SNARE

System iNtrusion Analysis & Reporting Environment

Guide to
SNARE for IRIX

INTERSECT
ALLIANCE

Documentation History

Version No.	Date	Edits	By whom
1.0	12 July 2004	First draft for the Guide to SNARE for IRIX documentation, in the updated format.	George Cora
2.0	2 April 2005	Minor rewording.	infofocus.com
2.1	30 November 2005	Formatting and minor changes	George Cora
2.2	15 May 2006	Included documentation for supported agents	David Mohr

About this guide

This guide introduces you to the functionality of the SNARE Agent for the IRIX operating system. SNARE for IRIX wraps the default IRIX auditing subsystem, and facilitates objective-based filtering, and remote audit event delivery. SNARE for IRIX will also allow a security administrator to fully remote control the application through a standard web browser if so desired.

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

The team at InterSect Alliance have experience with auditing and intrusion detection on a wide range of platforms - Solaris, Windows NT/2000/2003/XP, Netware, Tru64, Linux, 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 development of 'SNARE for IRIX' will now allow IRIX audit logs to be collected from the IRIX 6.5 or greater operating system, and forwarded to a remote audit event collection facility. SNARE for IRIX will also allow a security administrator to fully remote control the application through a standard web browser if so desired. SNARE has been designed in such a way as to allow the remote control functions to be readily effected manually, or by an automated process.

In the spirit of the release of the SNARE agents, InterSect Alliance are proud to release SNARE for IRIX as an open source initiative. Event audit modules for Solaris, Linux, Windows and other applications have been released under the terms of the GNU Public License. The overall project is called '**SNARE' - System iNtrusion Analysis & Reporting Environment**. The '*SNARE Server'* is a commercial release of software beneficial to organisations that wish to collect from a wide variety of SNARE agents and appliances such as firewalls or routers.

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 FOR IRIX

SNARE operates through the actions of one key application; the '*SnareCore*' process. SNARE interfaces with the IRIX 'Security Audit Trail' (sat) daemon, and will manage your IRIX audit selection configuration, based on the objectives defined in the SNARE configuration file. Logs generated by the IRIX audit subsystem are filtered using the SNARE objectives, and then passed over the network, using the UDP or TCP protocol, to a remote server for collection, analysis and archival, or saved locally to a file. *The TCP protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased a SNARE Server, through the supported agents. See Chapter 7 of this document for further details*. The *SnareCore* daemon is able to be remotely controlled using a standard web browser.

The text-format logs produced by SNARE are based generally on the output of the 'sat_interpret' command, which is described in detail by the IRIX manual pages. This format, is also discussed in the section on the *SnareCore* output format – Appendix A. The net result is that a *raw* event, as processed by the *SnareCore* daemon may appear as follows:

```
snare_irix        IrixSAT 4      86       sat_exec,Success TIME=(07/13/2004,12:47:15) SYSCALL=exece SATID= root
COMMAND=mail   CWD=/usr/root   DEVICE=15,1   PARENT_PID=1507   PID=1509   UGID=root,mail   UGID=root,sys
GID_LIST=sys,daemon,bin,adm,mail   CAP_SET=(all=)   UGID=root,mail   CAP_SET=(all=)   PATHNAME=/bin/mail
OBJECT=BEGIN  LOOKUP=/bin/@usr//bin//mail  FILE=20971839,0,76  UGID=root,mail  MODE=rwxr-xr-x  OBJECT=END
CAP_SET=(all=)        UGID=root,sys        UGID=root,sys        PATHNAME=/usr/lib32/libc.so.1        OBJECT=BEGIN
LOOKUP=/usr//lib32//libc.so.1/@..//..//lib32//libc.so.1   FILE=29809175,0,76   UGID=root,sys   MODE=r-xr-xr-x
OBJECT=END.
```

All of the fields in this record are sent to the remote server, whether this is a SNARE Server, or a custom tool. The SNARE Server will then interrogate some or all of the tokens in the log file to determine whether the event will be of interest to the security or system administrators.

3   INSTALLING AND RUNNING SNARE

3.1 SNARE INSTALLATION

SNARE includes an installation script to allow for easy installation and configuration of all critical components. The 'SnareIrix-Install archive includes the following key components:

• The *SnareCore* binary that performs all of the main SNARE functions.

• Configuration files necessary to allow *SnareCore* to work with the IRIX auditing subsystem.

• The installation script, *install.sh*, which enables the easy installation of all necessary components.

• A removal script – *snare-uninstall.sh*, which removes SNARE components from your system.

It is important to remember that a 'basic' IRIX installation does not normally contain the utilities necessary to run the auditing sub-system. As such, it must be separately installed on the IRIX host, before SNARE will run successfully. The next section details how the auditing sub-system may be installed on an IRIX workstation. Of note, the user will require the operating system CD's before proceeding, IF the auditing sub-system has not been enabled.

▶ **WHAT YOU NEED...**   • IRIX Audit Subsystem.

       • IRIX 'Foundation 1' CD.

▶ **HOW TO...**   Install the IRIX Audit Subsystem

   1. The *SnareCore* daemon can only work if the IRIX host has the basic IRIX 'Security Audit Trail' subsystem installed and enabled. The following steps detail how to check for, and install, the required auditing software.

       • As root, execute the command: */usr/sbin/versions | grep eoe.sw.audit*
       • It should return:

```
# /usr/sbin/versions | grep audit
I  eoe.sw.audit         07/07/2004   Security Audit Trail Software
```

       • If it doesn't, then the IRIX audit sub-system has not been installed. The following instructions detail how to install the auditing software; but be aware, they may vary depending on the IRIX Operating System version that is installed. Your IRIX operating system CD's will be required.

         • Load the IRIX 'Foundation 1' CD
         • As root, execute the command *inst*
         • At the Inst> prompt type '**from /CDROM/dist**'
         • type '**keep ***'
         • type '**install standard**'
         • type '**install eoe.sw.audit**' to install the auditing software
         • type '**go**'. Note that if any conflicts arise, then the full set of operating CD's may need to be scanned.
         • Type quit to exit the Inst program, and execute as root: */usr/sbin/versions | grep eoe.sw.audit*
         • The return from the above command should now show that auditing has been installed.

Once the IRIX audit subsystem has been installed and activated, the SNARE installation process can continue. There are three general components to the SNARE installation package:

● **SNARE**
The *SnareCore* daemon is contained in the '*SnareCore*' binary. This binary contains all the software to read the event log records, filter the events according to the 'objectives', provide a web based remote control interface, and configure the IRIX audit subsystem based on required objectives.

● **install.sh/snare-uninstall.sh**
These two scripts undertake the installation and uninstall functions required to ensure SNARE for IRIX works as required. The scripts prompt the user on the steps that need to be undertaken and the choices to be made (discussed in detail below).

● **Configuration Files**
A number of configuration files are required to correctly run the *SnareCore* audit sub-system. These configuration files have been tailored to meet the SNARE requirements, and include the files: sat_select.options, satd.filter*, satd.options and snare.conf. These configuration files are copied to the IRIX/etc/config/ directory during the installation process.

▶ How to...   Install the SNARE package for IRIX

1. Download the 'SnareIrix-Install' file from the Intersect Alliance website.

2. As 'root', type:
   # gzip -d SnareIrix-Install-*<version>*.tar.gz
   # tar xvf SnareIrix-Install-*<version>*.tar
   (where <version> is the version of SNARE for IRIX you wish to install)

3. A directory called SnareIrix-Install-*<version>* will be created. Enter this directory:
   # cd SnareIrix-Install-*<version>*

4. In order to commence the installation, type in './install.sh'. A series of prompts will then be displayed, requesting that various parameters be set. Read these settings carefully, using this manual as a reference. Most of the references are discussed later in this guide, so it pays to read this guide first, before installing the software.

5. Once the installation process has completed, the *SnareCore* daemon will start automatically, and will be integrated into your normal boot process.

3.2 Running SNARE

Upon installation of SNARE for IRIX, the *SnareCore* binary will be installed in the /usr/sbin directory. The *SnareCore* process will be controlled by the /etc/init.d/audit daemon control script, so there is no need to start or stop *SnareCore* directly.

The *SnareCore* daemon must be running, if the events are to be passed to a remote host. The *SnareCore* daemon may be stopped, started or restarted, by issuing the command: '/etc/init.d/audit stop', and '/etc/init.d/audit start', respectively.

▶ How to...   Run the *SnareCore* Daemon:

1. Login as root.

2. Execute the command '*/etc/init.d/audit start*'.

3. Execute the command '**ps -ef | grep snare'**, and check that there is one (or two if the micro-web server is active) process called '/usr/sbin/snarecore'.

How to...   Enable Remote Audit Control

If the **SnareCore** daemon is run on a system that has remote control enabled in the snare.conf file, then the audit subsystem may be remotely controlled using a standard web browser. Note that for this to work, the remote control facility should be set *(see the following section of the documentation for specific instructions on remote control settings)*, and the **/etc/config/snare.conf** MUST have AT LEAST the 'allow=1' line under the [Remote] configuration category specified:

```
[Remote]
        allow=1
        listen_port=6161
        restrict_ip=10.0.0.1
        accesskey=SnYLb.gT4Gk2k
```

If the 'restrict_ip' line is in the snare.conf file, then the only machines that are able to remote control the agent are those listed on that line. If the 'accesskey' line is specified, then a password is required to access the remote control function (the username for remote control is always '**snare**'). The password in the SNARE configuration file, is 'encrypted' using the standard UNIX 'crypt' function. Using a web browser type in the following on the URL bar:

```
http://<ip address or DNS hostname>:6161
```

(NOTE that '6161' will be the port number specified in the '**listen_port'** of the **/etc/config/snare.conf** file.

4   SETTING THE AUDIT CONFIGURATION

4.1 AUDIT CONFIGURATION

The audit configuration is stored as */etc/config/snare.conf*. This file contains all the details required by the audit daemon to successfully execute. Failure to have a correct configuration file available in this location will not 'crash' the daemon, but will result in events not being processed, or forwarded to your central log server.

> Tip: Manual editing of the snare.conf configuration file is possible, but care should be taken to ensure that it conforms to the required format for the audit daemon. Also, any use of the Remote Control SNARE capability to modify security objectives or selected events, may result in any manual configuration file changes being overwritten. Details on the configuration file format can be viewed in Appendix B – SNARE Configuration File.

The most effective and simplest way to configure the SNARE audit daemon is to use the remote control capability. Additionally, the installation script will ensure that a correct format *snare.conf* file is generated, based on broad user requirements when initially installing the SNARE tool.

The installation script will request the choice of 3 installation profiles. The description of each one, along with the system calls that it audits are detailed below.

Option 1: 'General Administrative and Login Events'. This will collect all the *sat_ae_identity* and

sat_chroot,sat_mount,sat_clock_set,sat_hostname_set,sat_domainname_set,sat_hostid_set,sat_control,sat_bsdipc_snoop_ok,sat_bsdipc_snoop_fail,sat_ae_audit,sat_ae_mount system calls.

Option 2: 'General Administrative, Login and process execution events'. In addition to the above, all the *sat_exec*, and *sat_exit* system calls will also be collected.

Option 3: 'General Administrative, Login and process execution events and file events related to system configuration files'. In addition to the above, all the sat_open_ro, sat_access_denied, sat_access_failed, sat_open, and sat_file_attr_write system calls will be audited but only for files and directories within /etc/ (the IRIX system configuration directory).

4.2 AUDITING CONTROL

The initial audit configuration parameters to consider are:

• The hostname, IP address and UDP or TCP port of the remote collection servers,

• The requirement to maintain a log file, or send the events to a remote server or servers, or both, and

• The location of the logfile.

• Note that the TCP and multiple server features are only available to users who purchase a SNARE Server. This is not part of the Open Source toolset. See Chapter 7 below for more details on the supported versions of the SNARE agents.

These three parameters are shown in the '*Network Configuration*' menu, shown in Figure 1 below. Note that the figure below shows all the menus for other features, such as 'Objectives Configuration' and 'Remote Control Configuration'. This and other functions are discussed later in this documentation.
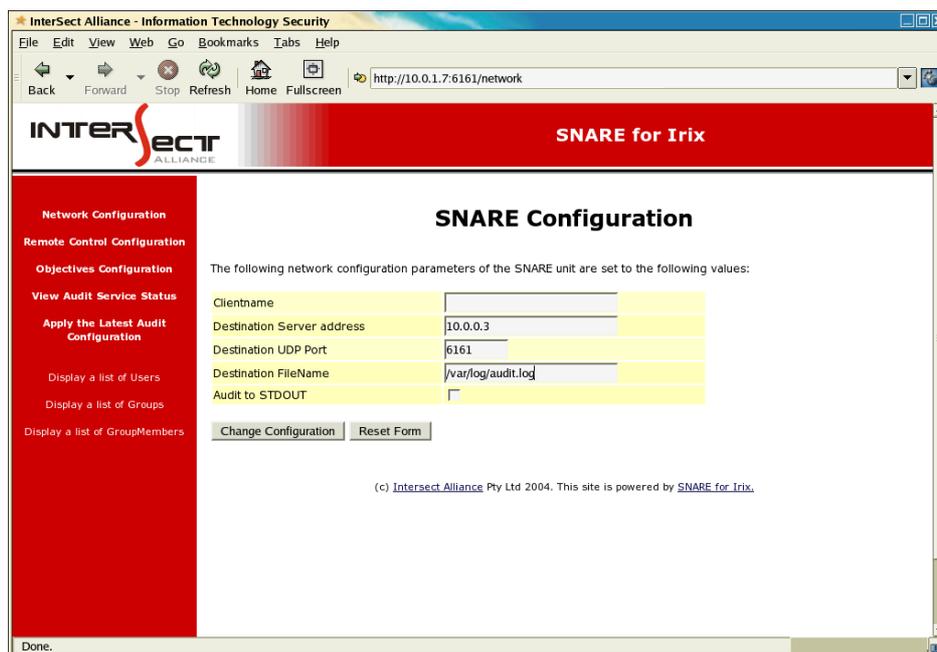
Figure 1 Network Configuration

The hostname field can be used to override the fully qualified domain name of the host system, which will be used by SNARE if this field is blank. Note that executing the command 'hostname' on a command prompt will display the current host name allocated to the host.

The 'port' shown in Figure 1 is the SNARE Server's port that will be used to collect the events. If, for example, the Intersect Alliance SNARE Server is used, then this is the default port which will be used. Since SNARE for IRIX converts the binary log file entries into text, a copy of these events may be saved locally to a file, if it is required that a facility be provided to log events to a text file. This is shown in Figure 1. Leaving this entry blank will pass events directly over the network, and NOT write them to disk. Supported agents will have an additional options to enable TCP and configure multiple hosts. See Chapter 7 below for more details on the supported versions of the SNARE agents.

A major function of the SNARE audit subsystem is the capability to filter events. This is accomplished via the advanced auditing 'objectives' function. Any number of objectives may be specified, and are displayed within the 'Objectives Configuration' menu on the remote control browser page, as shown in Figure 2 below.
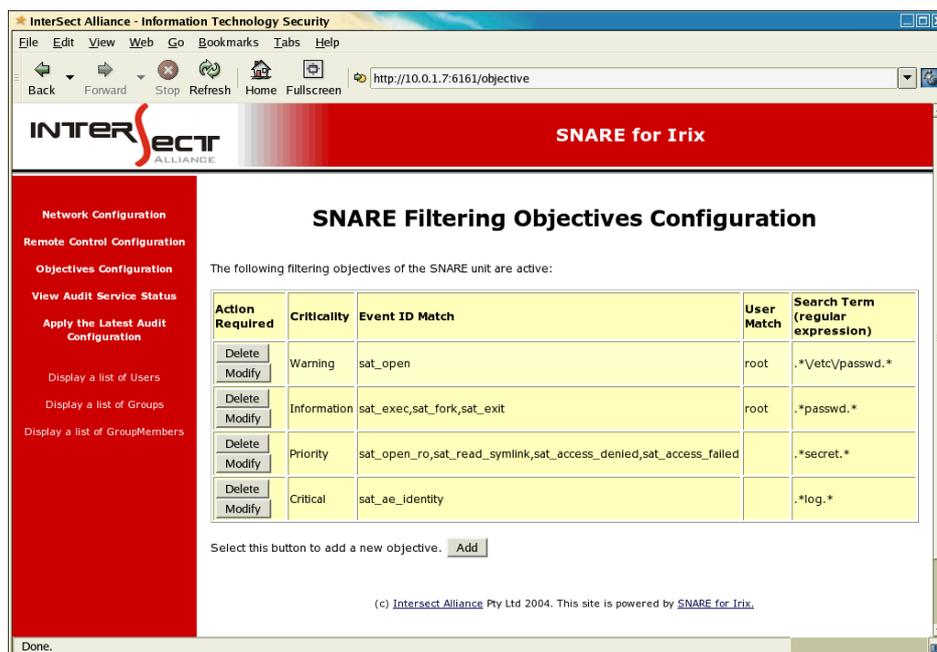
Figure 2 Objectives Configuration

Each of the objectives provides a high level of control over which events are selected and reported. Events are selected from a group of high level requirements, and further refined using selected filters. Users can choose from pre-defined 'groups' of objectives (eg. 'Start or stop a program execution'), or can select any valid IRIX auditable system call (as shown by the 'sat_select -h' command). The 'high level' groups are as follows:

- Read, write or create a file or directory,

- Modify system, file or directory attributes,

- Start or stop a program execution,

- Administrative Events,

- Open a file/directory for reading only,

- User logon or logoff,

- Any event(s).

Note that the groups above are provided to cover the most common security objectives that most organisations are interested in. If other event types are required, then the 'Any event(s)' objective will allow fully tailored objectives to be set, AND the relevant audit event type should be entered in the '*Event ID Search Term*'. As an example, if the IRIX specific 'sat_exec' audit event is to be audited, then the objective shown in Figure 3 should be specified. Note that this example, also shows that only the users '*root, red or george*' will be audited for both successes or failures.
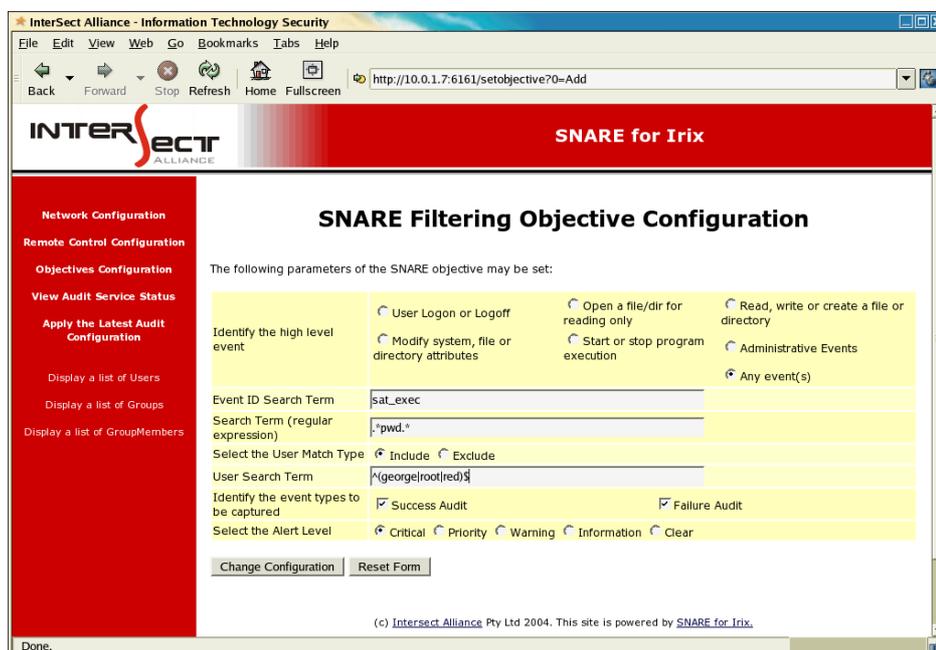
Figure 3 Specific Objective Configuration

From each of these groups, a criticality level can be applied. These criticality levels are *critical*, *priority*, *warning*, *information* and *clear*, as shown at the bottom of Figure 3. These security levels are provided to enable the SNARE user to map audit events to their most pressing business security objectives.

The following filters can be applied to incoming audit events:

1. Filter on the event-specific matchable item

Each event contains a particular piece of information that represents the core data that needs to be communicated. For the 'Open a file/directory for reading only' group, for example, this would be the name of the file and/or directory opened or created. For the 'Start or stop a program execution' group, this would be the name of the program in question (including the fully qualified path, where available). The event match allows a 'regular expression' match term to check against the event-specific matchable item. Regular expressions are an advanced form search filter. For example, the term '.*[Pp]ass(word|wd).*' would match the following:

- /etc/passwd

- /tmp/PasswordFile

but would not match

- /etc/PASSWD/

- /home/red/PaSsWoRd .txt

The regular expression will only match on selected tokens within a string. In the case of audit events related to file access or program execution, the *SnareCore* daemon will scan the combination of 'CWD' and 'PATHNAME' tokens (eg. CWD=/tmp, and PATHNAME=../home/../etc/passwd, will be scanned as /etc/passwd). For all other events, the search term will be used to search the entire string. So for example, this means that the 'Search Term' field seen in Figure 3, will apply to the pathname such as */sbin/pwd* when the command '*pwd'* is executed and audited by the IRIX audit sub-system.

2. Filter on user

Any number of users can be selected, and should be entered as a regular expression. If no users are entered, ALL users are assumed to be audited. Alternatively, specific users may be EXCLUDED from any individual objective, leading to objectives such as "tell me whenever any user except 'root' or 'red' generate an event". If the user exclusion function is selected, SNARE will only report users that DO NOT match the supplied list of users. Note that multiple users may be selected, but since it is a regular expression field, the users must be separated by the pipe symbol '|'. So in the case of specifying the users '*root'* and '*red'*, this must be written as '*^(root|red)$'*.

3. Filter on return value

An audit event will either return a success or failure return code. SNARE allows a user to filter on the return value.

Once the above settings have been finalised, clicking 'Change Configuration on the remote control page' will save the configuration to the SNARE Configuration file. However, to ensure the *SnareCore* daemon has received the new configuration, the *SnareCore* daemon MUST be restarted via the 'Apply the Latest Audit Configuration' menu item, or alternatively, by issuing the commands: '/etc/init.d/audit stop', '/etc/init.d/audit start', respectively.

A word of caution: The IRIX audit sub-system has a tendency to 'cache' events. In other words, an event record generated by (say) a particular command execution may sit in an internal buffer of the operating system, UNTIL, another event is received and pushed out. The Intersect Alliance team have noticed this behaviour on occasions, especially with (but not limited to) file modification events.

5 RETRIEVING USER AND GROUP INFORMATION

The *SnareCore* daemon also has the ability to retrieve users, groups and group membership from accounts local to the host that is running the agent. In those cases where the primary authentication source is defined as a NIS+ domain or an LDAP directory, then the users, groups and group membership retrieved will be those defined in the remote domain.

This feature is available through the remote control web page, and can be accessed through any standard web browser. The menu structure on the remote web pages (as shown in Figure 3) shows the selections 'Display a list of Users', 'Display a list of Groups', 'Display a list of GroupMembers'. Selecting any of these items will then display the relevant details. For example, Figure 4 below shows the output of selecting 'Display a list of Users'. The output from these commands has been designed with no HTML markup, so as to assist automated services, such as the SNARE Server, to interrogate the users, groups and group membership.

Figure 4: Output of 'Display a list of Users'

In the case of 'Display a list of Users', the output shows a number of tab delimited entries, per line. These entries should be interpreted as follows:

a. *Username*; *UID*; *Description*; Password Expired (token will be: PASSWD_EXPIRED); Account Inactive (token will be: ACCOUNT_INACTIVE); Account Expired (token will be: ACCOUNT_EXPIRED); Account Disabled (token will be: ACCOUNT_DISABLED); Account Locked (token will be: ACCOUNT_LOCKED); No Password (token will be: NO_PASSWD).

The first three entries of username, UID and description shown in bold and italics above will be displayed and be tab delimited. The remaining tokens will only be shown if they exist on a particular account.

In the case of Groups and Group Membership, the attributes displayed are *Groupname*; *GID*; *Group Members*. Obviously, the group member list will only be shown when selecting the 'Display a list of GroupMembers' menu item from the remote control web page. Additionally, the group members will be displayed as a comma separated list of usernames. As stated previously, the groups and associated membership displayed via the web browser may relate to NIS+ or LDAP users and groups, if the local host that is running the SNARE for IRIX agent has been configured to derive users and groups information from a domain.

6 REMOTE CONTROL AND MANAGEMENT

The *SnareCore* service is a separate standalone component of the SNARE system, as described in *2 Overview of SNARE for IRIX on page 5*. The audit configuration can be developed and set using the remote control web browser, set via the installation script, or configured manually as per the exact requirements detailed in Appendix B: SNARE Configuration File.

The *SnareCore* daemon can be restarted remotely from the menu item *Apply the Latest Audit Configuration*. This will instruct the audit daemon to re-read the configuration file, clear the buffers and restart. This function is useful when changes to the audit configuration have simply been saved to the configuration file, without being 'applied'. The user can therefore select when to activate a new configuration by selecting this link. This restart process can also be executed via the command line as follows:

- As root, execute the command: *ps -ef | grep snare*
- It should return something like:

    ```
    # ps -ef | grep snare
        root     3540        1  0 09:12:04 pts/0   0:00 /usr/sbin/snarecore
        root     3543     3540  0 09:12:09 pts/0   0:00 /usr/sbin/snarecore
        root     3616     3580  0 10:20:47 pts/1   0:00 grep snare
    ```

- As root, execute the command: */etc/init.d/audit stop*
- As root, execute the command: */etc/init.d/audit start*
- As root, execute the command: *ps -ef | grep snare*, and check that the processes have been restarted by ensuring the '*SnareCore*' processes have new process IDs.

6.1 REMOTE CONTROL

A significant function of the *SnareCore* service is its ability to be remote controlled. This facility has been incorporated to allow all the functions normally available through the front end SNARE tool (in the case of Linux, Solaris and Windows only), to also be available through a standard web browser. The *SnareCore* daemon employs a custom micro-web server to facilitate configuration through a browser, or via an automated custom designed tool such as the SNARE Server. Figure 5 below shows a web browser connecting to a SNARE agent. Note that the default web browser supplied with IRIX does not correctly display the SNARE remote control pages as of version 1.0 of the SNARE agent. Newer versions of Mozilla, Firefox or Internet Explorer display the pages correctly, and we have found a workaround for versions of the SNARE for IRIX agent above 1.0.
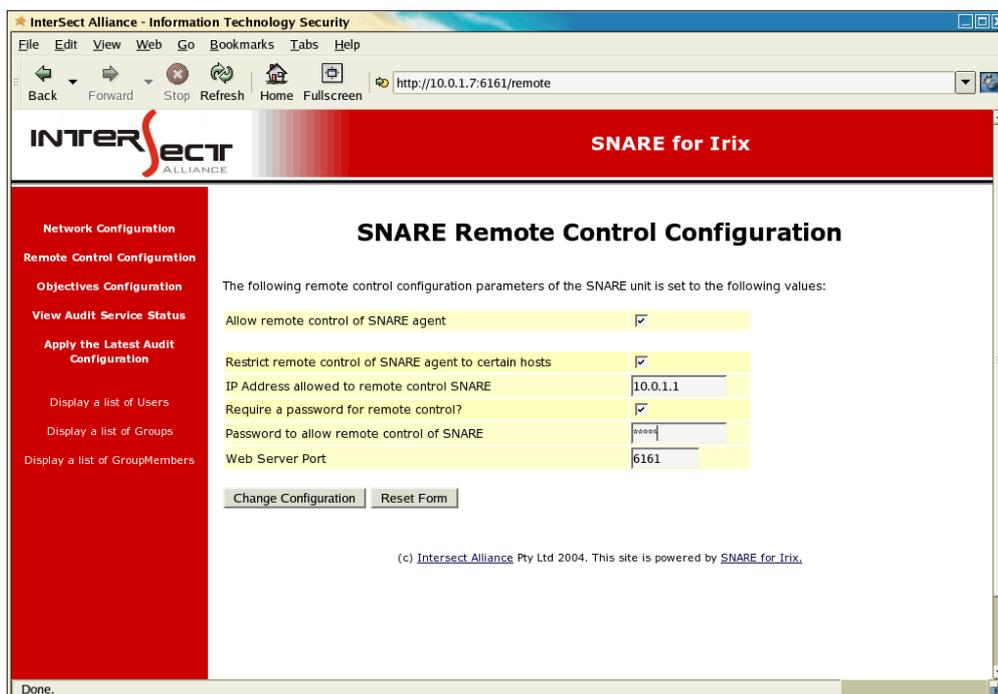
Figure 5 Remote Control Configuration

The functions available through the web browser are identical to those available on the SNARE configuration file. The parameters which may be set for remote control operation are shown in Figure 5, and are discussed in detail below:

- **Allow remote control of SNARE agent**. Selecting this checkbox will allow the SNARE agent to be remotely controlled from a web browser. This host may be independent from the central audit collection server. If the remote control function is disabled, and you wish to enable the facility, follow the instructions detailed in 'Enable Remote Audit Control' in Section 3.2 of this document.

- **IP Address allowed to remote control SNARE**. Remote control actions may be limited to a given host. This host, entered as an IP address in this field, will only allow remote connections to be effected from the stated IP address. Note that access control based on source IP address is prone to spoofing, and should be considered as a security measure to be used in conjunction with other countermeasures (such as ensuring your organisational firewall does not allow external connections to the SNARE micro-web server port).

- **Password to allow remote control of SNARE**. A password may be set so that only authorised individuals may access the remote control functions. If accessing the remote control functions through a browser or batch-mode tool (such as 'curl' or 'wget'), note that the UserID is always '*snare'*, and the password is whatever has been set through this setting. This password is not encrypted when being transmitted via the http session, but is encrypted when stored in the *snare*.*conf* file.

- **Web Server Port**. Normally, a traditional web server operates on port 80. If this is the case, then a user need only type the address into the browser to access the site. If however, a web server is operating on a port other than 80 (eg. 8085), then the user needs to type **http://mysite.gov:8085** to reach the web server. The default *SnareCore* web server port may be changed using this setting, if it conflicts with an established web server. However, care should be taken to note the new server port, as it will need to be placed in the URL needed to access the SNARE agent.

6.2 Log rotation

Depending on the SNARE configuration, the log file may be small or large. In any case, it is normal housekeeping practice that logs either be rotated or archived. Depending on the site requirements, a rotation scheme that keeps old copies of the last (say) 7 days may be sufficient. In this case, it may be sufficient to simply include a CRON job, and use a program such as logrotate to ensure the current log file does not grow to an unmanageable size. Alternatively, you may wish to archive all log files to backup media such as tape or CDROM. This may be scheduled using CRON or undertaken manually. In either case, it is important to note that the audit daemon should be restarted, so that it opens the new log file for writing the events. Users of the 'SNARE Server' software that do not save data locally, will have collection and archival of data managed and scheduled for them.

6.3 Remote distribution

SNARE provides the facility to send events to a remote host, using UDP or TCP (supported agents only). *The TCP protocol capability, and the ability to send events to multiple hosts is only available to those users that have purchased a SNARE Server, through the supported agents. See Chapter 7 of this document for further details.*

In conjunction with the audit log archive script (auditserver.pl) provided on the InterSect Alliance web site, this will facilitate the remote storage of audit logs for later analysis. The purpose of the SNARE agents is to filter the local events, and send them in real time to a remote server. It is recommended that a local log file not be maintained, but if one is required, then the housekeeping tasks detailed above should be undertaken.

The remote server may be a SNARE Server (discussed in the next section), or a custom tool that listens on port 6161 for SNARE events.

7   S N A R E   S e r v e r

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, 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 Syslog Data of any variety.

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 not offered through *any* other channels.
- 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 60,000 events per minute using a low end, workstation class, Intel based PC on a 100Mbps network.
- Automatic archiving of events to compressed text format after a configurable event time period. This is to prevent the database from slowing down due to storage of old events.
- Ability to drill down from top level reports. This reduces the amount of data "clutter" 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 and its ability to use a myriad of stable and functional open source tools. 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.

There are supported versions of the SNARE agents which are only available through the purchase of a SNARE Server. Functionality includes, but is not limited to, ability to send events via TCP as well as UDP, and the ability to send events to many destinations, not just one host.
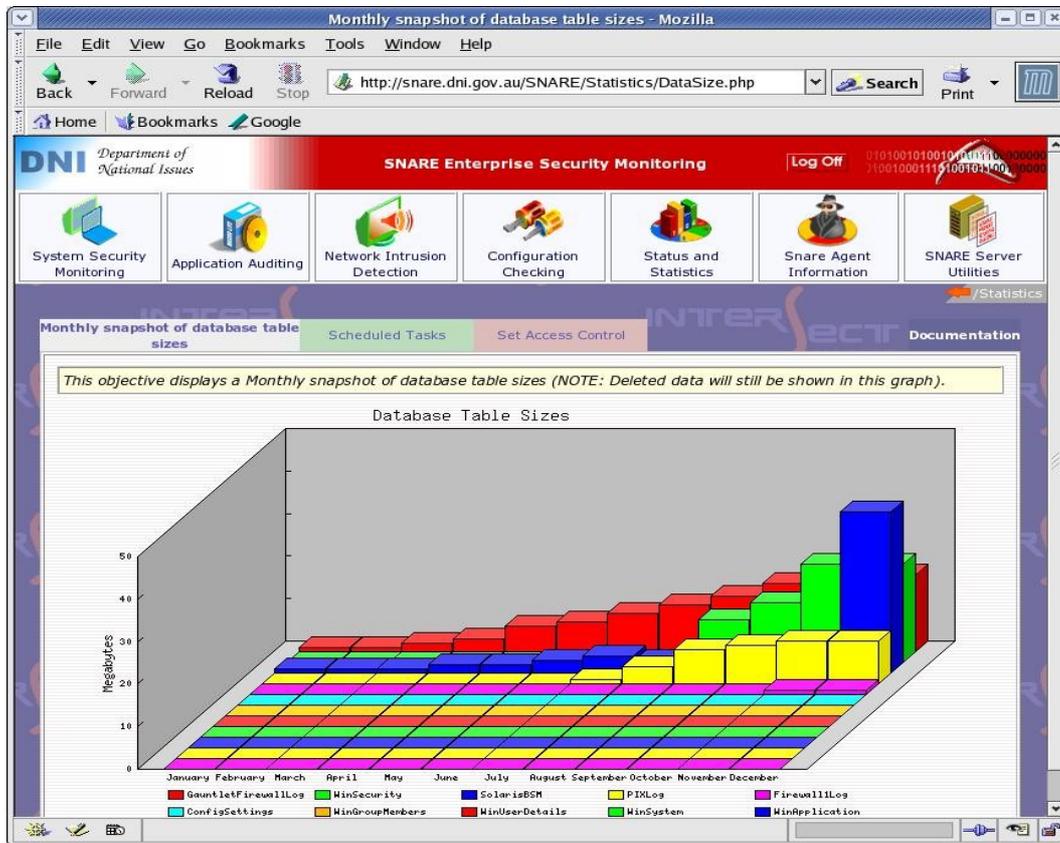
Figure 6 Screen shot from the SNARE Server

8   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 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.

Appendix A - Event Output Format

The *SnareCore* daemon reads data from the IRIX binary audit file, via published APIs. It converts the binary audit data into text format using the '*sat_interpret'* utility, and separates information out into a series of token/data groups. Three different field separators are used in order to facilitate follow-on processing - TABS separate 'tokens', COMMAS separate data within each token, and SPACES separate elements within data.

A 'Token' is a group of related data, comprising a 'header', and a series of comma separated fields which make up data that relates to the header. For example, the 'CWD' token in a text version of an IRIX event refers to the current working directory, and will be displayed as: *CWD=/usr/root*

Groups of tab separated tokens make up an audit event, which may look something like this:

```
snare_irix.IrixSAT      4       86      sat_exec,Success TIME=(07/13/2004,12:47:15) SYSCALL=exece SATID= root
COMMAND=mail    CWD=/usr/root   DEVICE=15,1     PARENT_PID=1507   PID=1509    UGID=root,mail    UGID=root,sys
GID_LIST=sys,daemon,bin,adm,mail    CAP_SET=(all=)    UGID=root,mail    CAP_SET=(all=)    PATHNAME=/bin/mail
OBJECT=BEGIN  LOOKUP=/bin/@usr//bin//mail  FILE=20971839,0,76  UGID=root,mail  MODE=rwxr-xr-x  OBJECT=END
CAP_SET=(all=)          UGID=root,sys          UGID=root,sys          PATHNAME=/usr/lib32/libc.so.1          OBJECT=BEGIN
LOOKUP=/usr//lib32//libc.so.1/@..//..//lib32//libc.so.1    FILE=29809175,0,76    UGID=root,sys    MODE=r-xr-xr-x
OBJECT=END.
```

The exact contents of all the tokens in the above event record are described in the satd(4) man page, and related pages such as the sat_interpret. The information in blue however, as shown in the above record, is information added by the *SnareCore* daemon. The format of this information is as follows:

<hostname> IrixSAT   <criticality>   <event counter>

The criticality is as set via the remote control tool, or via the configuration file (see Appendix B). The event counter is a sequential integer starting from 1, and recycling after a count of about 2 billion, on most systems.

Appendix B - SNARE Configuration File

Details on the audit configuration were discussed previously. The purpose of this section is to discuss the makeup of the configuration file. The SNARE configuration file on IRIX hosts is located at **/etc/config/snare.conf**, and this location may not be changed. If the configuration file does not exist, the audit daemon will execute, but will not actively audit events until a correctly formatted configuration file is present, or unless specific instructions are passed to the audit module at load time.

SNARE can be configured in several different ways, namely:

- Via the installation script (*Recommended*), or

- Via the web server (*Recommended*), or

- By manually editing the configuration file.

The format of the audit configuration file is discussed below.

`[HostID]`	This item stores the hostname, if it is different from the assigned IRIX hostname.
`name=<hostname>`	This is the name of the host.
`[Output]`	By default, if no output section exists within the configuration file, the audit daemon will send audit data out to standard out (STDOUT). Note that audit events will be sent to all valid destinations specified in the Output section. As such, events can be sent to one or all of a file, standard output and to a remote network destination (Only one file destination is supported however).

`network=hostname:port:tcp`
 	
`network=hostname:port`
	Audit data can be sent to a remote system using the UDP (default) or TCP protocol. Data will be sent to the remote host, and network port specified here. Each additional host must be specified on a new line. Caching will be enabled for the first host only if TCP is enabled.

`network=stdout`	If stdout is specifically defined within the Output section, the audit daemon will send data to standard out.
`file=stdout`	If stdout is specifically defined within the Output section, the audit daemon will send data to standard out.
`file=/fully/qualified/file/name`	The audit daemon will send data to the fully qualified filename specified within the [Output] section. Note that if the audit daemon is not running as root, the file must be writable by the user under which the audit daemon is running.
`[Objectives]`	This section describes the format of the objectives. Objectives are composed of: 1. Criticality - an integer between 0 and 4 that indicates the severity of the event. 0 is "clear", 4 is "critical. 2. The event ID - this must either correspond to a valid auditable event, or be set to "*" for any event. Note that the web server will convert the generic "groups" in the Audit Configuration window to the required events. For example, the abstracted group "Start or stop program

	execution", will result in the event entry "event=sat_exec,sat_exit" being written, with the events comma delimited. Note also that additional filter flags may be specified, as discussed in section 4 above.
	3. The return code defines whether to report event (system call) if it is a success, failure or both ("*")
	4. The user list is listed is used to audit events for selected users, and is in extended regular expression format.
	5. The match term is the filter expression, and is again defined in extended regular expression format.
	Note that whitespace will be trimmed from the start and end of items, but will be assumed to be valid when bracketed by other characters.
`criticality=1   event=sat_exec   return=* user=^(red|george)$  match=^more$`	Report at criticality level 1, whenever the users "red" or "george", execute the exact command "more".
`[Remote]`	This subkey stores all the remote control parameters.
`allow=1`	"Allow" is an integer, and set to either 0 or 1 to allow remote control. 1= allow remote, 0=do not allow.
`listen_port=6161`	This value is the web server port. A missing "listen_port" will default the web server to port 80.
`restrict_ip=10.0.0.1`	This is an IP address, that will be used so that this address will be the only host that is allowed to connect to the web server. If this item does not exist, then the web server will not restrict by IP address.
`accesskey=snare`	This value is the password that is used to log into the SNARE web server. If this item does not exist, then a password will not be requested when connecting to the web server. The password is encrypted when stored in the snare.conf, using the standard UNIX "crypt" facility, with salt.