# Global Information Assurance Certification Paper

# How to Configuring Local Logging on Solaris 8 and Use Symantec Intruder Alert for Centralized Logging

**Nolan Haisler**
**SANS GSEC v1.4c**
**January 24, 2005**

## Abstract

Logging is often a forgotten security friend for system administrators until a security breach has occurred. The security administrator then goes to look at the logs only to find that there are no logs, the logs are incomplete, or that the logs have been modified by the attacker himself to cover his tracks. To prevent this from happening, a system administrator should be prepared to have a good local logging system in place and perhaps even a central log server for archiving logs. In the case of a security breach or attempted security breach "complete and trustworthy system logs are critical for understanding what has happened on a given system" [1].

In this paper we will take a look at how to setup and configure a centralized logging system for a network of Solaris 8 machines and Windows 2000 machines. First, we will take advantage of Solaris' built in logging mechanisms, Syslog and BSM, and then we will install and configure Symantec Intruder Alert (SIA) to create a unique centralized logging scheme with powerful querying capabilities. The focus will be on centralizing the Solaris 8 logs while using the Windows machines for SIA Administrative purposes.

## I. Introduction

Logging is often a forgotten security friend for system administrators until a security breach has occurred. The security administrator then goes to look at the logs only to find that there are no logs, the logs are incomplete, or that the logs have been modified by the attacker himself to cover his tracks. To prevent this from happening, a system administrator should be prepared to have a good local logging system in place and perhaps even a central log server for archiving logs. In the case of a security breach or attempted security breach "complete and trustworthy system logs are critical for understanding what has happened on a given system" [1].

In this paper we will take a look at how to setup and configure a centralized logging system for a network of Solaris 8 machines and Windows 2000 machines. First, we will take advantage of Solaris' built in logging mechanisms, Syslog and BSM, and then we will install and configure Symantec Intruder Alert (SIA) to create a unique centralized logging scheme with powerful querying capabilities. The focus will be on centralizing the Solaris 8 logs while using the Windows machines for SIA Administrative purposes.

## II. Local Logging

Solaris has two methods for logging built in, Syslog and SunSHIELD Basic Security Module (BSM). Syslog is an auditing system where a daemon runs in the background to capture system and application messages. These messages are then logged according to the /etc/syslog.conf configuration file [11]. On the other hand, BSM captures kernel as well as user level events according to the configuration files in /etc/security and then records them in a binary log file. To begin our centralized audit logging system, let's set up local logging.

### A. Syslog

First let's set up Syslog. Open /etc/syslog.conf in a text editor and change the configuration commands to the following and save.

```
# syslog configuration file.
*.debug                         /var/adm/messages

*.alert                         root, operator
*.emerg                         *
```

"*.debug /var/adm/messages" tells the Syslog daemon to append messages from any facility and for any alert level (priority) above or at the debug level to /var/adm/messages. Since the "*" covers all facilities and since debug is the lowest priority, the Syslog daemon will log all messages and logs it receives to /var/adm/messages. The remaining 2 configuration commands tell the Syslog daemon to send any messages that have an alert or higher priority to root and the operator as well as any messages with a emergency priority to all users [10]. For more information on facilities and priorities see the syslog.conf man page referenced at the end of this paper.

Now let's change the permissions of the Syslog configuration file to protect against unauthorized changes. Execute:

```
chmod 0400 /etc/syslog.conf
```

To protect the logs from unauthorized access, execute:

```
chmod 0600 /var/adm/messages
```

On Solaris 8, Syslog by default accepts logs remotely on port 514. Since we will be using Symantec Intruder Alert (SIA) to forward and centralize logs, there is no need on most systems to have the Syslog daemon listening on port 514. Turning off this feature helps guard against a denial of service type attack where someone may try to flood a machine with Syslog messages and fill up the drive space. However, one machine (or as few as possible) should be designated to

accept remote Syslog messages in order to capture logs forwarded from devices that will not have an SIA Agent installed. These devices, including firewalls, switches, and perhaps intrusion detection sensors, should be configured to forward logs remotely to the designated machine (machines).

To disable Syslog from receiving remote logs, open /etc/init.d/syslog in a text editor and add the "-t" option as shown in the following line [11]:

```
/usr/sbin/syslogd –t >/dev/msglog 2>&1 &
```

For the newly made changes to take effect, the Syslog daemon must now be restarted. This can be done by executing:

```
/etc/init.d/syslog stop
/etc/init.d/syslog start
```

To test the Syslog configuration, execute the logger command.

```
logger –p daemon.debug "Testing Syslog configuration"
```

The logger command sends the message "Testing Syslog configuration" to the Syslog daemon with the facility "daemon" and the priority "debug." The Syslog daemon appends the message (as according to the syslog.conf file) to /var/adm/messages. Check that the log exists in /var/adm/messages.

```
cat /var/adm/messages | grep "Testing Syslog"
```

Now that Syslog is configured, we will be getting logs from everything we need, right? Not quite. Not every application or service logs to Syslog by default or even has Syslog logging capabilities. For those that do have the capability be sure to configure them to use Syslog and for those that do not, a wrapper script may help. For example, McAfee VirusScan v4.10 command line scanner does not have built in Syslog compatibility [9]. Appendix A shows a simple wrapper script that captures the scan summary generated by McAfee, formats it, and logs it to Syslog.

### B. BSM

Setting up BSM requires a little more effort but in return it provides very useful logging capabilities. A balance exists between logging every single event and process action, which can prove detrimental to a server's performance and drive space, and logging so little that the logs are all but worthless when trying to figure out what happened during a security breach. BSM is highly customizable and the configuration shown below provides a good place to start. Customize BSM according to your needs in order to capture what is needed while avoiding an overwhelming number of unnecessary logs. For more detailed information on the options available for BSM see the following resource.

http://docs-pdf.sun.com/806-1789/806-1789.pdf

To begin, let us configure the BSM audit configuration files in /etc/security. Open /etc/security/audit_class in a text editor and create a custom audit event flag as shown below.

```
0x01000000:cs:custom audit events
```

This custom flag is created so that we can specify exactly what events we want to log in the audit_event file [3]. Before we do this, let us first set up the audit_control file. Open /etc/security/audit_control in a text editor and make the following changes.

```
dir:/var/audit
minfree:20
flags:lo,ss,-fm,cs
naflags:lo
```

The “dir” entry specifies where the generated logs will be stored and the “minfree” entry specifies the percentage of free space that must be available (for storing logs in the “dir” directory) before the audit_warn script is executed. The “flags” entry sets the flags, which are mapped to events in the audit_event file. The entries lo (login/logout), ss (system state change), and cs (custom events) tells the BMS daemon to log all lo, ss, and cs events, successful and failed, while the “-“ sign in front of the fm flag (file modification) causes the BSM daemon only to log failed fm events. The BSM daemon will attempt to log all events specified in the audit_control file linked to a specific user. However if BSM cannot link the event to a specific user name then it will log the events specified by the “naflags” entry (ie. login/logouts only) [2].

Now that we have specified the flags in the audit_control file, let’s see which events the flags correspond to and set up our custom events to log. Open the audit_event file in a text editor. Appended to the end of each event are the flags that will cause that particular event to be logged if the flag is specified in the audit_control file. Add the cs flag to the end of the following events.

```
10:AUE_CHMOD:chmod(2):cs
11:AUE_CHOWN:chown(2):cs
24:AUE_CHROOT:chroot(2):pm,cs
38:AUE_FCHOWN:fchown(2):cs
39:AUE_FCHMOD:fchmod(2):cs
62:AUE_MOUNT:mount(2):as,cs
69:AUE_FCHROOT:fchroot(2):pm,cs
153:AUE_ENTERPROM:enter prom:na,cs
154:AUE_EXITPROM:exit prom:na,cs
```

```
237:AUE_LCHOWN:lchown(2):cs
268:AUE_UMOUNT2:umount2(2):as,cs
6200:AUE_allocate_succ:allocate-device success:ot,cs
6201:AUE_allocate_fail:allocate-device failure:ot,cs
6202:AUE_deallocate_succ:deallocate-device success:ot,cs
6203:AUE_deallocate_fail:deallocate-device failure:ot,cs
```

[3] BSM will now log the above events in addition to the lo, ss and fm events. The flags specified in the audit_control file are applied to all users. However, for the root (privileged) user we would like to log more than just the flags listed in the audit_control file. To do this, open the audit_user file in a text editor and add the following entry.

```
root:ex,lo:no
```

The audit_user file allows flags to be set only for a particular user. The “ex” flag tells the BSM daemon to log every command that is executed by root. Although every command name will be logged (along with the username of the user who su-ed to root) that root executes, the arguments to the command will not be logged by default. To log all arguments along with the command names, open the audit_startup file in a text editor and add the following line to the end of the startup script.

```
auditconfig -setpolicy +argv
```

When BSM is started the audit_startup file will be read and all command line arguments will be logged with the commands [2]. To help guard against unauthorized changes to the BSM configuration, change the BSM configuration file permissions to root read only.

```
chmod 0400 /etc/security/audit*
chmod 0700 /etc/security
```

To start BSM, first change to single user mode by executing “init s” (do not do this remotely or the remote connection will be closed). Then execute

```
/etc/security/bsmconv
init 6
```

bsmconv will prepare the system to begin logging, and “init 6” will reboot the machine. Once the machine has rebooted, verify that the BSM audit daemon is running by looking at the running processes. Execute

```
ps –ef | grep auditd
```

BSM security logs can be found in the /var/audit directory (remember we set “dir”

to /var/audit in the audit_control file). Change directories to the /var/audit directory and run "ls –l" to list the directory contents. The not_terminated file is the current log file. Execute "audit –n" to tell BSM to close the current log and start a new one. Then run "ls –l" again. Notice the previous log has been closed and a new not_terminated file has been created. The format for all closed log filenames is:

start_timestamp.end_timestamp.hostname

and the format for current log is

start_timestamp.not_terminated.hostname

The BSM log files are written in a binary format and require a tool to read. The built in tool for Solaris is the praudit command [2]. To view a log file execute

praudit –l <log filename>

The "-l" switch instructs praudit to print 1 record per line and to convert the record type and event fields into their ASCII representation [12]

BSM and Syslog have now been configured and the logs are ready to be centralized by Symantec Intruder Alert. The syslog.conf and BSM configuration must be carried out separately on all hosts in which logs are desired from. This can easily be done by either tar-ing up all the configuration files and writing a simple script to copy them into place and starting/restarting the necessary daemons or by creating a simple package and distributing the package to all machines.

## III. Symantec Intruder Alert

### A. Symantec Intruder Alert Components

Special consideration should be given to the organization of SIA throughout your network. SIA consists of 5 unique components that provide log management, centralization, and querying capabilities. The components are:

- Administrator
- Event Viewer
- Manager
- Agent
- Query Event Management Service (QEMS)

Figure 1 below shows a simple layout of these components.

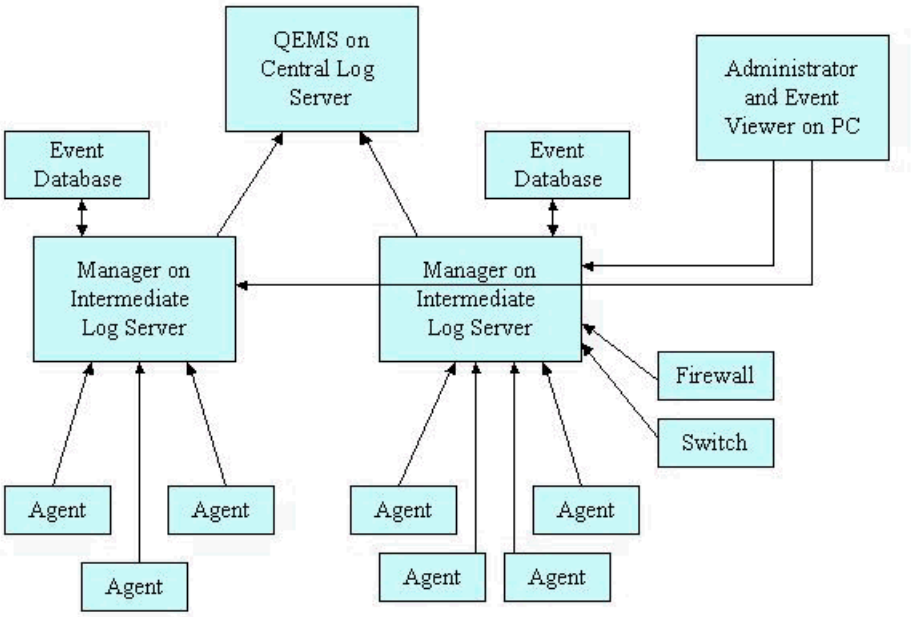


**Figure 1: Simple layout of SIA components**

The Agents run on every server and workstation collecting the local logs and then forwarding the logs to a Manager. Each Manager stores a local copy of the logs it receives (in the event database) and then forwards a copy to the Query Event Management Service (QEMS). The Administrator manages the Managers and Agents as well as the logging policies and the Event Viewer allows for running queries on each Manager's event database. The QEMS runs on the central log server and collects all logs it receives and stores them in plain text locally. Let's look at each component and its role in more detail.

### a. Agents

Agents are installed on every machine, UNIX and Windows, that is capable of running an agent. Examples of where an Agent normally would not be installed are firewalls and switches. Generally these types of devices would log via remote Syslog to a machine that is running an Agent and the logs would be picked up and centralized from there. Each Agent is responsible for watching and gathering logs from the local:

- wtmp
- BSM log files
- Syslog (which we set to log to /var/adm/messages)
- Any other ASCII log file that we specify

The logs are then filtered through a set policies and rules (which we will configure later) and then a copy is forwarded on to a Manager. The Agent runs as a UNIX daemon (or as a Windows service) nonstop gathering and forwarding logs as they are generated [5].

Note: The Agent does not modify or delete any local logs. It only watches and creates a copy. Thus even when a log is forwarded, the original log still resides on the local machine untouched.

The logs from Agents are forwarded encrypted on port 5051 by default to a manager [6].

### b. Managers and the Administrator console

The Manager provides a common link between Agents, the Administrator console, and the Event Viewer and serves as an intermediate centralized log collection center. The Manager's responsibilities include:

- Gathering all logs sent by its Agents
- Storing a copy of all the logs it receives from its Agents in a local encrypted database
- Sending a copy of the logs it receives to the Query Event Management Service

In addition the Manager is used to:

- Organize the Agents into groups
- Administer policies and rules

Agents can be grouped by which Manger they report to as well as internally inside each Manager. Within a single Manger, Agents can be divided into groups such that each group has its own set of policies and rules. A simple way to categorize Agents is to group them by operating system type (for example Solaris and Windows NT).

Although the Managers administer and maintain the organization of Agents as well as the policies and rules, the configuration of these cannot be accomplished directly. The Administrator is the key. The Administrator runs on a windows machine only and is used to log into the Managers. Once logged into a Manager (or Managers) you can then graphically configure the groupinp of Agents, the policies and rules, and user accounts [5]. The Managers and the Administrator console communicate on ports 5051 and 3833 by default [6].

### c. Event Viewer

The Event Viewer, which can be installed on the same machine as the Administrator, communicates with the Managers on ports 3834 and 5051 and allows you to view and query the logs in each Manager's event database [6]. It provides the capability to query logs by Agent (i.e. the originating machine), by policy or rule, by date and time, by keyword or signature or by any combination of the above [5]. For example, you can easily query for all failed logins that occurred on Jan 1st between 1 and 3 pm on a single particular workstation. At the same time you can also run a query for all traffic on Jan 1st between 1 and 1:30 pm that transversed your firewall if you have your firewall logging to a machine with an Agent. Event Viewer is a powerful tool!

### d. Accounts

Both the Administrator and the Event Viewer require that you have an account on the Manager before you can change or even view anything. Remember it is important to assign accounts to each user, rather than having group accounts. When the accounts are set up (covered in the installation section) privileges are also set. It is a good practice to give each user only the privileges they need to do their job. Account privileges include:

- View intruder configuration
- Modify policies/domains
- View event information (view logs stored on Manager)
- Change Manager configuration
- Change Agent configuration
- Register new Agent
- User account information (can modify user accounts) [5]

### e. Query Event Management Service

Lastly, let's talk about the Query Event Management Service (QEMS). The QEMS communicates with the Managers on ports 5051 and 3836 and is a multipurpose tool that can be used for storing the logs forwarded by Managers as well as for generating reports based on the logs [5][6].

In this setup, we are going to use the QEMS as a centralized log collector. Each Manager will forward all the logs they collect from their Agents to the QEMS. The QEMS will in turn format the logs and then write them into an ASCII text file. Ideally the Query Event Management Service should run on a hardened server by itself. The server will need the appropriate disk space to store all the logs it receives. The amount of space that will be needed is dependent upon several factors including the number of Agents that will be forwarding logs, the number of logs that are desired to be kept, as well as the aggressiveness of log rotation and archiving (log rotation and archiving is discussed later). The central log server should be locked down and if possible placed on the network in a lower security risk area. For example, it would be better to place the central log server inside the internal network rather than out in the DMZ. Remember the central log server will maintain a plain text copy of every log forwarded from every machine in your network, creating a very valuable resource.

## B. Installation and Configuration

The SIA components should be laid out in a manner that makes sense for your network architecture. Figure 2 shows an example layout.

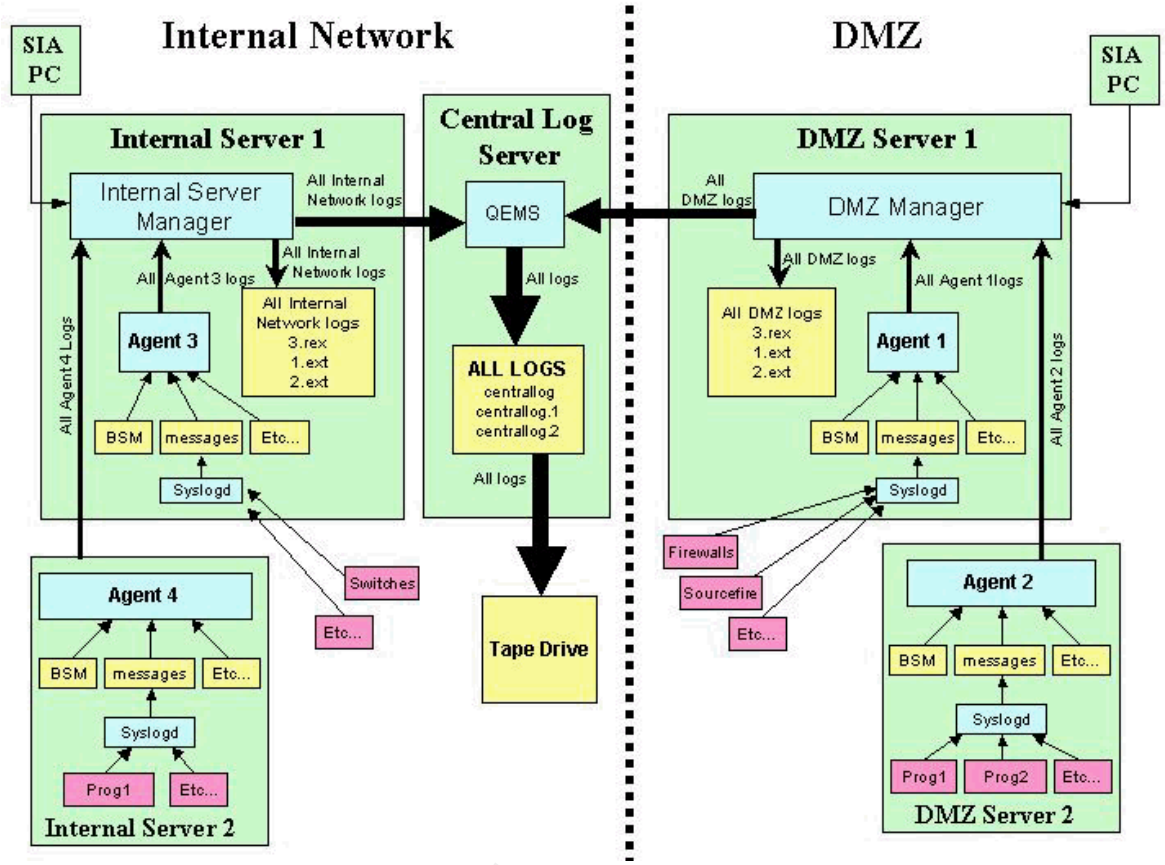


**Figure 2: Example SIA Layout**

Remember to keep in mind system capabilities such as disk space, memory, and processor speed when choosing a location for Managers. The Managers will be communicating and receiving logs from all its Agents as well as storing them locally. The amount of system capabilities depends largely on the number of Agents, the amount of logs you decide to keep, and how aggressive of a log rotation scheme you choose [4].

Now let us get to the installation and configuration. First install the Managers by following the steps below.

> Note: You do not need to install an Agent on the server running the Manager because an Agent is installed with the Manager.

### Installing SIA Manager

**Step 1)** Assume root privileges

**Step 2)** Extract the SIA install files into a temporary directory and then run "itasetup"

**Step 3)** Type '1' and press ENTER to do Basic installation

**Step 4)** Press SPACEBAR repeatedly until end of license agreement is reached

**Step 5)** Type 'yes' and press ENTER to agree with license agreement

**Step 6)** Type '2' and press ENTER to install a Manager
**Step 7)** Type '1' and press ENTER to specify absolute path
**Step 8)** Type where you want to install SIA (such as /opt/sia-3.6) and press ENTER
**Step 9)** Type '2' and press ENTER to select use agent's short hostname
**Step 10)** Type 'y' and press ENTER to okay the label
**Step 11)** Verify the location of the ita.tgz file and press ENTER
**Step 12)** Type in the 19-character license key WITH hyphens and press ENTER
**Step 13)** Type the number of licensed guests for that license and press ENTER
**Step 14)** Type in a administrator name for the Intruder Alert Administrator, press ENTER (Note: This account is used for SIA only)
**Step 15)** Type in a password and press ENTER
**Step 16)** NOTE: You must know this administrator name and password to configure the manager so be sure to remember it.
**Step 17)** Retype the password and press ENTER
**Step 18)** Press ENTER to select the TCP Manager port default (5051)
**Step 19)** Press ENTER to select the TCP Agent port default (5052)
**Step 20)** Press ENTER to select N
**Step 21)** Type '0' and press ENTER to select No Default Policies
**Step 22)** Setup Complete

Next lets secure the SIA files from unauthorized access. Execute:

```
chmod 0600 /axent/ita/system/`hostname`/*
```

To turn on SIA's capability to capture the logs from BSM and to use SIA to rotate the wtmp log files, open /axent/ita/system/`hostname`/ita.ini in a text editor and make the following changes.

```
WTMP_TRUNC = 1
 WTMP_LOG_MAX_SIZE = 1024

# Indicates if the C2 Audit Trail Daemon should start when the agent
starts
C2ATD_START = 1
# Options to be passed to the C2 Audit Trail Daemon
C2ATD_OPTIONS = -p1
```

After making these changes the Manger must be restarted. To restart, execute:

```
/axent/ita/bin/itarc stop
/axent/ita/bin/itarc start
```

When SIA is installed it makes an update to the syslog.conf file. Because we want all logs to go to /var/adm/messages and not to SIA's install directory, comment out the line SIA added. Open /etc/syslog.conf in a text editor and make the following change.

#*.info;mail.err;mark.none /axent/ita/system/<hostname>/syslog

To restart the Syslog daemon for the changes to take effect execute:

kill –HUP `cat /etc/syslog.pid`

Now that the Manager is installed we must install the Administrator next so we can set up the user accounts we will need. While were at it, let's install the Event Viewer and an Agent also.

**Installing SIA Administrator and Event Viewer**

**Step 1)** Log onto Windows 2000 with Administrator privileges
**Step 2)** Exit all Windows programs
**Step 3)** Copy the SIA install file to the Desktop and unzip it to C:\temp\sia

**MS-DAO installation**

**Step 4)** In the Start menu, choose Run
**Step 5)** Type C:\temp\sia\dao\disk1\setup.exe
**Step 6)** Click OK in the Run dialog box
**Step 7)** When the Welcome dialog box appears, read the text then click Next
**Step 8)** After the Select Components dialog box appears, select the Jet and ODBCdirect components and click Next
**Step 9)** Select all optional formats for Jet and then click Next
**Step 10)** After installation of MS-DAO, an information dialog box appears. Click OK

**Agent/Administrator/Event Viewer Installation**

**Step 11)** In the Start menu, choose Run
**Step 12)** Type C:\temp\sia\setup.exe
**Step 13)** Click OK in the Run dialog box
**Step 14)** At the Welcome dialog box, read the text and click Next
**Step 15)** At the Software License Agreement, read the text and click Yes to accept
**Step 16)** At the Select Components dialog box, select the check boxes for:
- ITA Agent for Windows
- ITA Administrator for Windows
- ITA Event Viewer
- Policy Library

**Step 17)** At the Choose Destination Location dialog box, click Next
**Step 18)** At the Intruder Alert Service Ports dialog box, click Next to accept defaults 5051 and 5052

**Step 19)** At the Intruder Alert Agent Label dialog box, select the 'Use system's Short Name as Agent Label' option and click Next

**Step 20)** At the Register Agent to Manager dialog box, type in the Manager's name. Then type in the Manager's username and password used when the manager was installed

**Step 21)** Click the → to add the Manager to the list, click Next

**Step 22)** At the Select Program Folder dialog box, type in Symantec under 'Program Folders:' and click Next

**Step 23)** At the Choose Platforms dialog box, select No Policies

**Step 24)** If auditing on the Windows machine is off, the System Configuration dialog appears asking to enable Windows auditing. Click Yes to enable Windows audit logging.

**Step 25)** Click Finish to exit the installation program

An account is needed on every Manager to register Agents as well as for the QEMS service.
Note: The administrator account created at the time of Manager installation could be used to register new Agents as well as for the QEMS service but this not recommended by Symantec [7]. It is good practice to only give each account the privileges needed.

Follow the instructions below to add the accounts to each Manager.

**Adding the "Register a new agent" and QEMS accounts to a Manager.**

**Step 1)** Log on to the PC with the Administration Console

**Step 2)** Open the Administration Console

**Step 3)** Right click "Manager" on the left hand bar and select Connect to Manager

**Step 4)** In the popup window, type in the IP address of the server the Manager is installed on. Then type in the username and password that were used during the Manager installation. Click OK.

**Step 5)** When the Manager's IP address appears on the left hand bar, right click on it and select User Manager

**Step 6)** Click Add, then type in "QEMS" for Username and "SIA Query Event Mgmt Serv" for Full name. Type in a password for QEMS

**Step 7)** Check "View Event Information" box ONLY.

**Step 8)** Click Commit

**Step 9)** Click Add, then type in "regAgnt" for Username and "Register New Agent Account" for Full name. Type in a password for "regAgnt.

**Step 10)** Check "Register New Agent" box ONLY.

**Step 11)** Click Commit

**Step 12)** Click OK to close the User Manger

After setting up the user accounts on every Manager, we are ready to install the Agents. To install the Agents follow the instructions below on every machine that will have an Agent.

**Installing SIA Agents**

SIA Agents must be installed separately on each machine. To install, assume root privileges and then extract the SIA install files into a temporary directory. Run the silent install script:

```
./sinstall /D: <Install Dir> /G:root /U:root /V: /A:<Manager
IP>:<Username>:<Password>:5052
```

where

<Install Dir> is the directory to install SIA
<Manager IP> is the IP address of the Manager this Agent will report to
<Username> is the username created to register new Agents
<Password> is the password created to register new Agents

Next lets secure the SIA files from unauthorized access. Execute:

```
chmod 0600 /axent/ita/system/`hostname`/*
```

To turn on SIA's capability to capture the logs from BSM and to use SIA to rotate the wtmp log files, open /axent/ita/system/`hostname`/ita.ini in a text editor and make the following changes.

```
WTMP_TRUNC = 1
 WTMP_LOG_MAX_SIZE = 1024

# Indicates if the C2 Audit Trail Daemon should start when the agent
starts
C2ATD_START = 1
# Options to be passed to the C2 Audit Trail Daemon
C2ATD_OPTIONS = -p1
```

After making these changes the Agent must be restarted. To restart, execute:

```
/axent/ita/bin/itarc stop
/axent/ita/bin/itarc start
```

When SIA is installed it makes an update to the syslog.conf file. Because we want all logs to go to /var/adm/messages and not to SIA's install directory, comment out the line SIA added. Open /etc/syslog.conf in a text editor and make the following change.

```
#*.info;mail.err;mark.none /axent/ita/system/<hostname>/syslog
```

To restart the Syslog daemon for the changes to take effect execute:

```
kill –HUP `cat /etc/syslog.pid`
```

After installing all the Agents, they must now be configured to capture the desired logs. The configuration is accomplished through the Administrator. Follow the steps below to configure the Agents to capture logs from /var/adm/messages and BSM. This must be done on each Manager and to every Agent.

**Configure Agents for var/adm/messages, BSM**

**Step 1)** Log on to the PC with the Administration Console

**Step 2)** Open the Administration Console

**Step 3)** Right click “Manager” on the left hand bar and select Connect to Manager

**Step 4)** In the popup window, type in the IP address of the server the Manager is installed on. Then type in the username and password that were used during the Manager installation. Click OK.

**Step 5)** Click “+” to expand Registered Agents

**Step 6)** Select EACH UNIX Agent under Registered Agents and complete Steps a-o

- **a)** (After selecting the UNIX Agent in the left pane) Click New under the Audit Logs box
- **b)** For Description, type “C2 Audit”
- **c)** For Filename, type “/axent/ita/system/<hostname>/C2atd.pipe” where <hostname> is the hostname of the selected Agent
- **d)** Select Multiple Line
- **e)** For Delim String, type “return”
- **f)** Check “Include Delim” box
- **g)** Click OK
- **h)** Click New under the Audit Logs box
- **i)** For Description, type “var_adm_messages”
- **j)** For Filename, type “/var/adm/messages”
- **k)** Select Multiple Line
- **l)** For Delim String, type “\n”
- **m)** Check “Include Delim” box
- **n)** Click OK
- **o)** Click Save in right panel

After completing the previous steps SIA Agents are ready to send logs to their respective Managers from /var/adm/messages and BSM. Additional ASCII log files can be added simply by following steps a-o and substituting in the information for the additional log. The specific logs that SIA chooses to forward

from /var/adm/messages and BSM (as well as any additional logs specified) are decided by rules maintained in each Manager. Let's take a look at policies and rules.

### Adding Policies and Rules

There are two ways to filter the local logs to find which logs are desired to be forwarded from the Agents to the Managers. A catch all rule can be created that says to grab all logs except ones that contain any of these, <sig1,sig2,sig3>, signatures. On the other hand a rule or a set of rules can be created to define each signature that a log must have before it can be forwarded. In this procedure, we will set up a variance of the first option: forward all logs without exception. Don't be hesitant to set up your own rules. See the SIA User Guide reference at the end of this paper for detailed information on setting up policies and rules.

**Set up Catch All Rule and Policy**

**Step 1)** Log on to the PC with the Administration Console
**Step 2)** Create the file catchall.pol on the Desktop, See Appendix D for file contents
**Step 3)** Open the Administration Console
**Step 4)** Right click "Manager" on the left hand bar and select Connect to Manager
**Step 5)** In the popup window, type in the IP address of the server the Manager is installed on. Then type in the username and password that were used during the Manager installation. Click OK.
**Step 6)** Highlight "Policies" in the left pane
**Step 7)** Click File->Import Policy
**Step 8)** In popup box select the catchall.pol file and click open
**Step 9)** Click the "+" to expand Policies in left pane
**Step 10)** Click the "+" to expand Catch All Policy in left pane
**Step 11)** Right click Applied Domains and select Apply to Domain
**Step 12)** Select "Default-All Agents" and click OK
**Step 13)** Remove catchall.pol from the Desktop

### File Watch Bonus Feature

In addition to gathering logs, SIA agents also have a file watch feature. Symantec "Intruder Alert can determine if a file (text file, program, configuration file, etc.) or directory has disappeared, reappeared, or changed (been accessed or modified)" [5]. The files that are watched by default are listed in 2 files:

ita/system/<hostname>/uxcrit_L.lst,uxcrit_L
ita/system/<hostname>/uxcrit_S.lst,uxcrit_S

When a file or directory that is listed in one of the two above files changes in any way, the SIA Agent creates a log entry that is forwarded to its Manager. Additional files can be monitored by either adding them to the above files or

more properly by creating a new watch file list. See the SIA User Guide for more information [5].

### Symantec Intruder Alert Query Event Management Service

We are now ready to set up the Query Event Management Service on the central log server. Symantec supplies the QEMS as a single binary so we will need to create the other necessary files. The QEMS is controlled by two configuration files, iaquery.cfg and iaquery.fmt. Let's create each of these. Open a new file, /axent/ita/bin/iaquery.cfg, in a text editor and add the following configuration commands.

```
#Global parameters
output = /var/centrallog/centrallog
query_port = 5055
poll_interval = 1
format_file = /axent/ita/bin/iaquery.fmt
truncate_output = no

#UNIX managers
"managers = <ManIP>
"mgr_port = 5051
"user = <Username>
"password = <Password>
"query = (value >= 0)
"mode = real_time
```

where

<ManIP> is a comma separated list of all Manger IP addresses that will forward to QEMS
<Username> is the username created for QEMS
<Password> is the password for the QEMS account

To secure this file execute

```
chmod 0400 /axent/ita/bin/iaquery.cfg
```

Now let's create the format file. Open a new file, /axent/ita/bin/iaquery.fmt in a text editor and add the following configuration commands

```
#format of central log file
.equate EventTime
"%e_month%/%e_monthday%/%e_century%%e_year%
%e_hour%:%e_minute%:%e_second%"
.equate CurrentTime
"%c_month%/%c_monthday%/%c_century%%c_year%
%c_hour%:%c_minute%:%c_second%"
```

```
.record
.field delimiter 10 13
.field "EVENT TIME: %EventTime%   CURRENT TIME: %CurrentTime%
MANAGER: %manager%"
.field "MESSAGE: %text%"
.field "************************************************************"
.endrecord
```

[8] The configuration is ready for QEMS and we are almost ready to go. First let's copy the QEMS binary into /axent/ita/bin and give it permissions 0500. To start and stop QEMS, create a startup script in /etc/init.d. An example script is located in Appendix C. Be sure to create links into the rc* directories so that QEMS will stop and start with system state changes. For example:

```
ln –s /etc/rc2.d/K99init_iaquery /etc/init.d/iaquery_daemon
ln –s /etc/rc3.d/S99init_iaquery /etc/init.d/iaquery_daemon
```

Before starting the Query Event Management Service let's create the directory where the central log files will collect.

```
mkdir /var/centrallog
chmod 0700 /var/centrallog
```

After starting the Query Event Management Service, a file named centrallog will be created to store all the logs received from each Manager listed in the configuration file. Set the permissions on this file to 0600. For more information on configuring QEMS and about the commands in the configuration files, see the QEMS User Guide referenced at the end of this paper.

Congratulations, we have now set up a centralized logging system. Agents will now forward their logs to their respective Managers. The Managers will store a local copy and then forward one to the central log server where QEMS will capture it and log it to the centrallog file. All forwarded logs will now reside in /var/centrallog!

However, an important topic still remains – log rotation.

## IV. Log Rotation and Archiving

Many factors play into how aggressively logs should be rotated. These factors include, how long logs should be kept, the amount of logs generated, and the amount of disk space available. We will assume in the following explanations that local logs must be kept for seven days and that ample disc space is available.

### A. Local Logs

The easiest way to maintain local logs is via a cron job. A simple cron entry like the one shown below can be made to run a script that will rotate the logs nightly.

10 0 * * * /opt/auditlog_scripts/24hr-log-rotate.pl #log rotation

An example script is located in Appendix B, that if run nightly by cron, will keep 7 days worth of /var/adm/messages and BSM logs.

### B. Event Database

The intermediate logs that are stored by each Manager reside in the installation directory at /axent /ita/system/`hostname`/. The files are rotated by SIA after reaching a size specified in the ita.ini file. How much space is available as well as how long of a log history is desired to be kept in the event database will decide how often the old logs should be removed. The current log has a .rex extension while all archived logs have a .ext extension. The oldest logs are the logs with the numerically smallest filename. Remember once the logs are removed, they will be available on the central log server but not for querying with the Event Viewer.

### C. Centralized Logs on central log server

The /var/centrallog/centrallog file has the potential to grow very rapidly. A cron job that runs a script hourly to check the centrallog's file size and rotate it if its is too large will be sufficient for most systems. The centralized logs can be easily archived from the central log server to tape or other method for long-term storage if necessary.

## V. Conclusion

Setting up and configuring a central audit system is not a trivial task but the benefits provided generally out-weigh the cost. Symantec Intruder Alert provides a good backbone for centralizing logs and can reduce the amount of time spent looking for logs greatly with its querying capabilities. Remember this tutorial is a guide and you should configure local logging as well as the policies and rules for log forwarding according to your requirements.

## Appendix A: Wrapper script for McAfee VirusScan v4.10

```
#!/bin/sh
################################################
#Author: Nolan Haisler
#
#   A simple wrapper script to run the host-based anti-virus
#   software from the command line and send the results
#   to the local syslog
################################################
quarantine_directory=/var/quarantine
tmp_file=/tmp/mvs-output.txt
tmp_file_for=/tmp/mvs-formatted.txt

if [ $# -eq 1 ]; then
    /usr/local/bin/uvscan --summary -m $quarantine_directory -r $1 > $tmp_file
    #report if an error has occured
    code="$?"
    if [ "$code" -ne "0" ]; then
      echo "Error running /usr/local/bin/uvscan: $?" >> $tmp_file
    fi
else
    echo ""
    /usr/bin/echo "Enter the directory or file to scan:  \c"
    read scan_file
    /usr/local/bin/uvscan --summary -m $quarantine_directory -r $scan_file | tee
$tmp_file
    #report if an error has occured
    code="$?"
    if [ "$code" -ne "0" ]; then
      echo "Error running /usr/local/bin/uvscan: $?" | tee -a $tmp_file
    fi
fi

#add comment to scan summary
/usr/bin/echo "McAfeeVirusScan: \c" > $tmp_file_for

#format uvscan output for syslog
sed -e 's/  //g' $tmp_file | tr -d "." | tr "\n" ";" >> $tmp_file_for

#send scan summary to local syslogd
logger -p "daemon.debug" -f $tmp_file_for

#clean up
rm $tmp_file $tmp_file_for
exit "$code"
```

## Appendix B: Rotating /var/adm/messages and BSM logs

```
#!/bin/perl -w

#####################################################################
#
#  Name:         24hr-log-rotate.pl
#
#  Author:       Nolan Haisler
#
#  Description:  This script rotates:
#                messages log files in the /var/adm directory
#                BSM log files in the /var/audit directory
#
#               This script replaces /usr/lib/newsyslog script for rotating
#               /var/adm/messages.
#
#               BSM logs older than 7 days are removed
#
#               This script should be called nightly (after midnight) by cron.
#
#####################################################################
use File::Copy;
sub rotate
{
  my($sfile, $dfile) = @_;
  if (-e $sfile)
  {
    move($sfile, $dfile) ||
      die "24hr-log-rotate.pl: Could not move $sfile to $dfile: $!\n";
  }
}

sub system_error_handler
{
  my($code, $string) = @_;
  $code = $code >> 8;
  print STDERR "System call Error for $string: $code\n";
  exit;
}
#####################################################################
#               Rotate /var/adm/messages logs
#####################################################################
&rotate("/var/adm/messages.6", "/var/adm/messages.7");
&rotate("/var/adm/messages.5", "/var/adm/messages.6");
&rotate("/var/adm/messages.4", "/var/adm/messages.5");
```

```
&rotate("/var/adm/messages.3", "/var/adm/messages.4");
&rotate("/var/adm/messages.2", "/var/adm/messages.3");
&rotate("/var/adm/messages.1", "/var/adm/messages.2");
&rotate("/var/adm/messages.0", "/var/adm/messages.1");
&rotate("/var/adm/messages", "/var/adm/messages.0");
copy("/dev/null", "/var/adm/messages") ||
  die "24hr-log-rotate.pl: Could not copy /dev/null to /var/adm/messages: $!\n";
chmod 0600, "/var/adm/messages";

#Restart the syslog daemon
system("kill -HUP `cat /etc/syslog.pid`") == 0
  || &system_error_handler($?, "kill -HUP `cat /etc/syslog.pid`");

#####################################################################
#                   Rotate the bsm logs
#####################################################################
system("audit -n") == 0
  || &system_error_handler($?, "audit -n");

#####################################################################
#           Remove BSM log files older than 7 days
#####################################################################
#Grab all BSM log files in /var/audit
opendir(DIR, "/var/audit/") ||
  die "24hr-log-rotate.pl: Couldn't open /var/audit/ directory: $!\n";
my $sysname = `hostname`;
chomp $sysname;
my @files = grep /$sysname/o, readdir DIR;
closedir(DIR);

###assemble 7 day old file name###
#grab current date and time
my ($sec,$min,$hour,$day,$month,$year,$wday,$yday,$isdst);
($sec,$min,$hour,$day,$month,$year,$wday,$yday,$isdst) = localtime(time);
$month++;
$year+= 1900;

#go back 7 days
$day = $day - 7;

#if day is in previous month
if ($day <= 0)
{
  $month--;
  #if day is in previous year
  if ($month == 0)
```

```
  {
    $year--;
    $month = 12;
  }

  #Add the number of days according to the month
  SWITCH:
  {
    if ($month =~ /4|6|9|11/)  { $day += 30; last SWITCH; }
    if ($month =~ /1|3|5|7|8/) { $day += 31; last SWITCH; }
    #ignore leap year
    $day += 28;
  }
}
#add leading zeros if needed
if ($month < 10) { $month = "0" . $month; }
if ($day < 10)   { $day = "0" . $day; }
if ($hour < 10)  { $hour = "0" . $hour; }
if ($min < 10)   { $min = "0" . $min; }
if ($sec < 10)   { $sec = "0" . $sec; }

#assemble file name
my $deciding_date = $year . $month . $day . $hour . $min . $sec;
###end assemble 7 day old file name###

#remove files older than 7 days
foreach my $file (@files)
{
  my @fields = split(/\./, $file);
  if ($fields[0] < $deciding_date)
  {
    unlink("/var/audit/$file") ||
      die "24hr-log-rotate.pl: Can't unlink /var/audit/$file: $!\n";
  }
}
```

## Appendix C: Query Event Management Service start/stop script

```
#!/bin/sh

#####################################################################
#
#  Name:         iaquery_daemon
#
#  Author:       Nolan Haisler
#
#  Description:  Start and stop init script for the QEMS daemon
#
#####################################################################

case "$1" in
'start')
  if [ -f /axent/ita/bin/iaquery ]; then
     echo "Starting iaquery daemon..."
     cd /axent/ita/bin
     ./iaquery -f /axent/ita/bin/iaquery.cfg
  fi
  ;;

'stop')
  if [ -f /axent/ita/bin/iaquery ]; then
     echo "Stopping iaquery daemon..."
     cd /axent/ita/bin
     ./iaquery stop
  fi
  ;;

*)
   echo "Usage: $0 { start | stop }"
   exit 1
   ;;
esac
```

## Appendix D: Catch All Policy and Rule

```
.N Catch All Policy  #Policy Name
.L 2     #Policy structure
.D Catches all logs  #Policy Description
.V 1098711975        #Policy revision number
.Z 50  #Policy ID
.Z 50  #Policy ID
.R Catch All Rule    #Rule Definition
..D Catches all logs          #Rule Description
..Z 51  #Rule ID
..V 50 #Rule Value
..S      #Select Clause(s)
...G System Message        #System Message
....T *  #Regular text
....C 0          #Case sensitivity
....Z 52         #ID of the clause
..A      #Action Clause(s)
...E Record to Event Viewer        #Record Event
....Z 54         #ID of the clause
```

## References


1. Eric Cole, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials and the CISSP 10 Domains Version 2.2, Unix Security. SANS PRESS, 2004.

2. Sun Microsystems, Inc. "SunSHIELD Basic Security Module Guide" February 2000. URL: http://docs-pdf.sun.com/806-1789/806-1789.pdf

3. Osser, William; Noordergraaf, Alexander. "Auditing in the Solaris 8 Operating Environment" February 2001. URL: http://www.sun.com/blueprints/0201/audit_config.pdf

4. Symantec Corporation. "Installation Guide, Intruder Alert Version 3.6" December 2001. URL: ftp://ftp.symantec.com/public/english_us_canada/products/intruder_alert/3.6/manuals/ita36installguide_updated_2001.pdf

5. Symantec Corporation. "User's Guide, Intruder Alert Version 3.6" January 2002. URL: ftp://ftp.symantec.com/public/english_us_canada/products/intruder_alert/3.6/manuals/ita36userguide_updated_2002.pdf

6. Symantec Corporation. Knowledge Base Document: "List of TCP communication ports used by Intruder Alert" May 2004. URL: http://service1.symantec.com/SUPPORT/intrusiondetectkb.nsf/e922810fa3c8172285256b12004d0728/2cc20b2d3d1dd4ac88256d0a005a5476?OpenDocument&prod=Symantec%20Intruder%20Alert&ver=3.6&src=ent&pcode=intruder_alert&dtype=corp&svy=&prev=&miniver=ia_36_netware

7. Symantec Corporation. Knowledge Base Document: "Using an Intruder Alert user name and password to register agents to a manager" October 2002. URL: http://service1.symantec.com/SUPPORT/intrusiondetectkb.nsf/e922810fa3c8172285256b12004d0728/ce231bb7c4e31f8887256b330054e6e2?OpenDocument&prod=Symantec%20Intruder%20Alert&ver=3.6&src=ent&pcode=intruder_alert&dtype=corp&svy=&prev=&miniver=ia_36_netware

8. Symantec Corporation. "User's Guide, IA Query Event Management Service Version 3.5 for Intruder Alert Versions 3.6" September 2001. URL: ftp://ftp.symantec.com/public/english_us_canada/products/intruder_alert/3.6/manuals/iaquery.pdf

9. Network Associates, McAfee. "VirusScan for UNIX Administrator's Guide 4.10.0" URL: http://www.networkassociates.com/common/media/mcafeeb2b/support/unx410

0.pdf

10. Sun Product Documentation. “Syslog.conf” man page. January 1997. URL: http://docs.sun.com/app/docs/doc/806-0633/6j9vn6q7g?q=syslog&a=view

11. Sun Product Documentation. “Syslogd” man page. May 1999. URL: http://docs.sun.com/app/docs/doc/816-3319/6m9k06rfb?a=view

12. Sun Product Documentation. “praudit” man page. December 2002. URL: http://docs.sun.com/app/docs/doc/817-0880/6mglau84p?a=view