



Global Distributed Storage Engineering

eTrust Audit - Storage Monitor

GDSE-05023-SG
Solutions Guide

Version 1.5

1. Version Control

Version	Date	Author	Reviewed	Comments
1.0	13-Jul-05	Kevin Hobaugh	GDSE	
1.1	22-Jul-05	Kevin Hobaugh	GDSE	Modified Policy Creation
1.2	4-Aug-05	Kevin Hobaugh	GDSE	Section 6 Section 8.1.1 Section 8.3.1
1.3	24-Oct-05	Gary Johnson	Kevin Hobaugh	Added HDS, Updated Ref.
1.3.1	25-Oct-05	Gary Johnson	Global Storage Community	Added "Audit" to eTrust
1.3.2	13-Apr-06	Kevin Hobaugh	Global Storage Community	Modified HDS Section 8.1.1, Logname. Section 13.3, MP File: log token
1.4	13-Nov-06	Gary Johnson	Kevin Hobaugh	Updated HDS methodology and MP files, Added Gen Recorder Maint.
1.5	22-Mar-06	Gary Johnson	Kevin Hobaugh	Updated HDS MP files, added syslog configs, updated references to GDSE website, Updated Citi logos

2. Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

3. Contact

Please address any comments or questions regarding the information contained in this document via email to the “*GT Global Distributed Storage Engineering” distribution list or alternatively to gdse@citigroup.com.

4. Latest Versions

It is recommended that the latest version of the document be used from the GDSE website <http://gdse.ny.ssmb.com>. Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

5. Table of Contents

1. VERSION CONTROL	2
2. LEGAL NOTICE	3
3. CONTACT	3
4. LATEST VERSIONS	3
5. TABLE OF CONTENTS	4
6. PREREQUISITES.....	6
7. EXECUTIVE SUMMARY	6
7.1. SYMMREMOTE/EMCREMOTE	7
7.2. SYMMWIN	7
7.3. NAVISPHERE.....	7
7.4. HDS STORAGE NAVIGATOR.....	7
7.4.1. <i>Client</i>	9
7.4.2. <i>Policy Manager</i>	10
7.4.3. <i>Data Tools</i>	10
7.5. HOW ETRUST AUDIT WORKS.....	12
7.6. WINDOWS GENERIC RECORDER MAINTENANCE.....	13
7.7. SOLARIS GENERIC RECORDER MAINTENANCE	13
8. INTEGRATION OF ETRUST AUDIT	14
8.1. ETRUST AUDIT CLIENT SOFTWARE INSTALLATION	14
8.1.1. <i>eTrust Audit Client Installation Steps</i>	15
8.1.2. <i>Installation Verification</i>	27
8.2. ETRUST AUDIT CLIENT SOFTWARE CONFIGURATION	28
8.2.1. <i>Client Configuration</i>	28
8.2.2. <i>Registry Settings</i>	29
8.3. ETRUST AUDIT POLICY MANAGER.....	30
8.3.1. <i>eTrust Audit Policy Creation and Activation</i>	30
8.3.2. <i>eTrust Audit Policy Rules</i>	42
9. APPENDIX A: FIREWALL PORTS.....	49
10. APPENDIX B: CLARIION LOG PROCESSING (NAVISPHERE).....	50
10.1. CLARIION SCRIPTS	50
10.2. CLARIION SP LOGS.....	52
11. APPENDIX C: EMC LOG PROCESSING (PERFORMED BY EMC)	56
11.1. DMX CONFIGURATION	56
11.1.1. <i>Log Pull Program</i>	56

11.1.2.	EMCRemote.....	58
11.1.3.	Private Wire (Firewall Software)	61
11.2.	SYMM5 CONFIGURATION	61
11.2.1.	Log Pull Program.....	61
11.2.2.	EMCRemote.....	63
11.2.3.	Private Wire (Firewall Software)	66
12.	APPENDIX D: CONNECTRIX LOG PROCESSING (PERFORMED BY EMC) 67	
12.1.	EMCREMOTE	67
13.	APPENDIX E: HDS USP LOG PROCESSING.....	70
13.1.	DEVICE MANAGER MONITORING	70
13.2.	ARRAY AUDIT LOG MONITORING (SYSLOG).....	71
13.3.	MESSAGE PARSING FILE FOR DEVICE MANAGER.....	74
13.4.	MESSAGE PARSING FILE FOR ARRAY AUDIT LOG (SYSLOG)	78
14.	REFERENCES.....	83
15.	RELEASE NOTES.....	84

6. Prerequisites

This document was written with the understanding that the eTrust storage infrastructure would connect to an eTrust infrastructure server running the eTrust Collector, Policy Manager and database. This eTrust server could be a newly configured eTrust server managed by Global Storage Management or another existing eTrust infrastructure environment. The regional storage team should coordinate with regional ISA team to determine the direction.

To connect to the eTrust infrastructure, you will need the following information from the Global Storage Management Group.

- eTrust Audit Policy Manager Server (hostname and IP)
- eTrust Audit Collector Server (hostname and IP)
- eTrust Audit Security Monitor Server (hostname and IP)

The following information will be required for the eTrust Audit Client installation.

- eTrust Audit Recorder Name (ie: EMCRemote / SymmWin_DMX / SymmWin_Symm5 / Navisphere)
- eTrust Audit Log Name (name of the eTrust log where events will be monitored ie: EMCRemote / SymmWin_DMX / SymmWin_Symm5 / Navisphere)
- Location of log being monitored
- eTrust Audit Message Parsing file location (*C:\location_path*)
- Hostname and IP address of the Service Processor or Navisphere Mgmt Server
- SMTP Mail Server (if required)

If you're required to build your own eTrust Audit Monitoring infrastructure, then you'll need to reference documents provided by UNIX Engineering (<http://unixeng.corp.smb.com/>).

The eTrust Audit Client server (Storage SP, Connectrix SP or Navisphere Mgr) will need to have network connectivity and the ability to ping the eTrust Audit Collector Server. If a firewall exists between the eTrust Collector Server and the eTrust Audit Client, see Appendix A for firewall ports needed for this product. Only EMC can make modifications to a Storage Array or Connectrix Service Processor.

7. Executive Summary

eTrust Audit has been a Citigroup standard for monitoring UNIX server access. GDSE has determined that it is technically feasible to use eTrust Audit to capture

and analyze logs generated by EMC SymmRemote, SymmWin and Navisphere Manager. EMC personnel use the SymmRemote application to remotely connect to the Symmetrix and Connectrix service processors. EMC uses the SymmWin application from the Symmetrix Service Processor to manage the Symmetrix storage array. Navisphere Manager is used to manage the CLARiiON storage array. Storage Navigator is used to manage the HDS USP storage array.

7.1. SymmRemote/EMCRemote

The SymmRemote application creates a log where it records date and time of when someone connected, and date and time of when they disconnected. Unauthorized remote access to the Symmetrix and Connectrix service processors can be tracked via this log. The SymmRemote application log is stored on the service processor. In order to access the log, GSMG (Global Storage Management Group) personnel need to physically visit each service processor. The eTrust Audit application will run on the service processor and will periodically send the log file to a designated log server.

7.2. SymmWin

The SymmWin application maintains a log of user activities on the service processor. Changes to the Symmetrix array by the vendor through the SymmWin application can be tracked via this log. In order to access the log, GSMG personnel need to physically visit each service processor. The eTrust Audit application will run on the service processor and will periodically send events to a designated log server.

7.3. Navisphere

The CLARiiON Navisphere Manager application maintains a log of user activities on each of the CLARiiON SPs and within the Windows Application Log on the off-array manager server. Changes to the CLARiiON arrays by the system administrator or vendor through the Navisphere application can be tracked via these logs. GSMG scripts will be used to automatically pull (via IP) logs from each CLARiiON SP (via Navicli), creating a copy of the individual log files on the off-array manager. The eTrust Audit client application will run on the off-array manager server and will periodically send events (from the copied log files and windows event log) to a designated log server.

7.4. HDS Storage Navigator

The HDS Storage Navigator server maintains fixed logs of user activities and system events on the USP storage array. Changes made to security or to the configuration of the array can be tracked via these logs. Once configured, audit

logs from the array and DeviceManager management systems will be sent to eTrust Audit (via agents running on the management servers) for log reporting and safekeeping. There is a windows-based server that is used as the DeviceManager server and a Solaris-based server that is used as a syslog repository. ETrust Audit agents on these servers will handle the translation and delivery to the eTrust Audit repository.

eTrust Audit

The eTrust Audit application consists of the following three components:

- Client
- Policy Manager
- Data Tools

7.4.1. Client

The Client component is comprised of several subcomponents that provide services that collect and forward audit event data, which can in turn result in the generation of actions and alerts.

The following list describes the subcomponents:

Standard System Recorder

This recorder taps into the event data sent to the Windows Event Log (on Windows platforms) and into event data sent into the syslog daemon on UNIX and on Linux platforms. This recorder enables any events sent to these standard system logging facilities to be harvested by eTrust Audit for processing.

Generic Log Scraper

The Generic Log Scraper is another recorder that can be configured to harvest (clear text) events from third party products that maintain their own logs as external “flat files.”

Portmapper

The portmapper (Windows platforms only) manages the logical communications channels required to provide a standard way for a Client to access RPC services that it might require.

Redirector

The Redirector (Windows platforms only) taps into local eTrust Audit logs (created by the eTrust Audit Standard System Recorder service) or logs created by eTrust Audit Access Control running on Windows systems, and automatically redirects that audit data to a Router component on the same or on another machine.

Router

The Router acts primarily as a filtered message forwarder. It analyzes the policies you create using the Policy Manager (which will eventually be deployed as .cfg files found in the installation_path\eTrust Audit\cfg directory), and then follows those policy imperatives to examine audit events that are sent to its attention. Based on the configuration instructions you provide, the router identifies those records that should be as follows:

- Filtered out
- Forwarded to the Action Manager
- Forwarded to other eTrust Audit components for additional processing or storage

Action Manager

The Action Manager processes events sent to it by the router. You can instruct the Action Manager to automatically perform a wide range of actions in response to receiving specific audit events. The Action Manager gets its instructions from the policies you create using the Policy Manager and executes those actions as necessary and appropriate to a specific audit event.

Distribution Agent

The Distribution Agent receives policy imperatives from the Policy Manager, and places these policies into effect. These policy imperatives are sent to the Distribution Agent by the Distribution Server.

7.4.2. Policy Manager

The Policy Manager component (available on Windows platforms only) includes the following subcomponents:

Policy Manager

The Policy Manager interface is a Windows GUI that you use to centrally manage eTrust Audit policies. Using the Policy Manager, you can create, implement, and distribute your organization's eTrust Audit policies.

Distribution Server

The Distribution Server communicates with the Distribution Agent and coordinates the delivery of eTrust Audit policies.

7.4.3. Data Tools

The Data Tools component is comprised of two major components:

- The Data Tools interface
- The Collector database

The Data Tools GUI

The Data Tools interface is available only on Windows platforms and is comprised of the following:

Viewer

The Viewer displays, sorts, and filters audit events retrieved from a Collector database. The viewer also lets you save your own customized filters for future use.

Reporter

The Reporter lets you view, create, and schedule detailed, graphic reports from information extracted from the Collector databases.

Security Monitor

The Security Monitor lets you do the following:

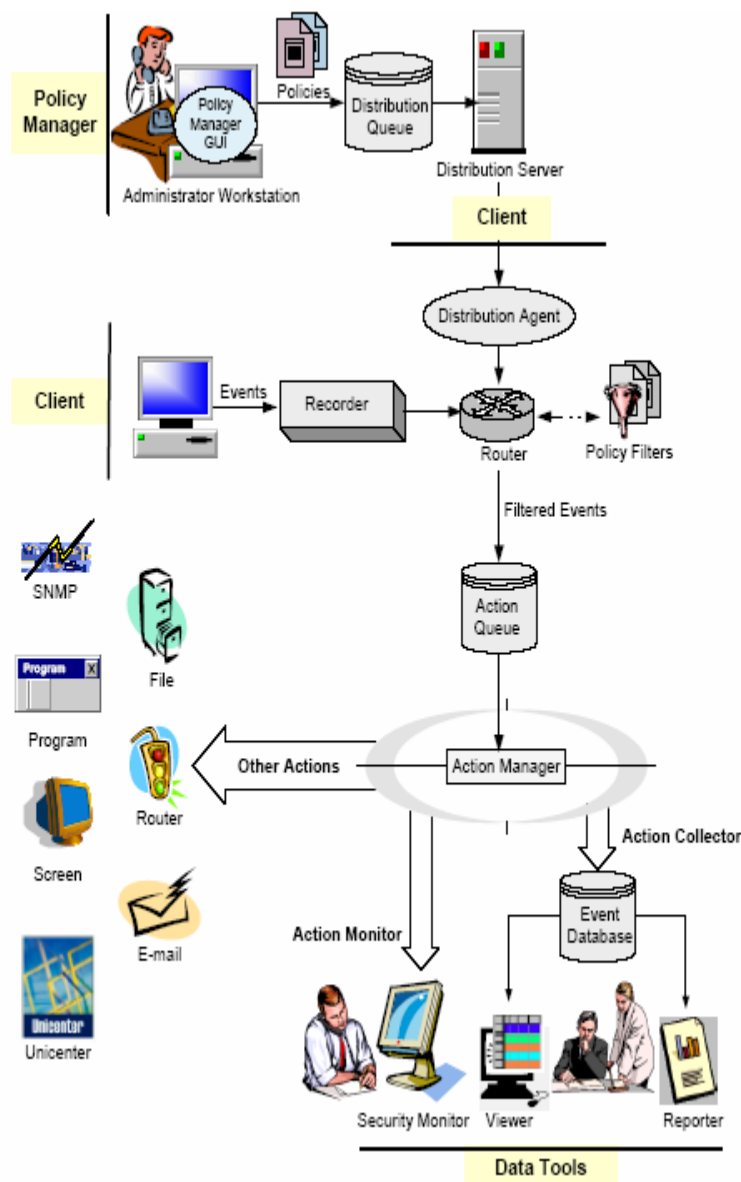
- Monitor specific events in near real time (designated important enough to monitor). The events can be sent from a variety of different recorders.
- Monitor eTrust Audit status and “self help” events. These are events related to the status of eTrust Audit components (for example, whether the Action Manager is started).

The Collector Database

The Collector database is where eTrust Audit stores all of the audit event data directed to it. eTrust Audit supports the following underlying databases:

- Microsoft SQL Server 7
- Microsoft SQL Server 2000
- Microsoft Access Database
- Oracle (on NT, Windows 2000, and UNIX)

7.5. How eTrust Audit Works



An administrator uses the Policy Manager to create, activate, and distribute policies that are stored in the policy distribution queue and routed to Distribution Agents on clients.

As events occur on clients, the Recorder harvests them and sends them to the Router for processing. Using the policies and filters created by the administrator, the Router stores events in the action queue for processing by the Action Manager.

The Action Manager, based on the policies you specify, can do the following:

- Take a direct action, such as executing a program, sending an email, or routing the message to Unicenter.
- Send the event to the Security Monitor so that an administrator can determine what action to take.
- Send the event to the Collector database where an administrator can use the Viewer to display events or use the Reporter to generate reports for later analysis.

7.6.Windows Generic Recorder Maintenance

The Generic recorder works as standard windows service named as “eTrust Audit Generic Recorder.”

To Stop/Start this service from Windows Service Control Manager:

1. Open Service control manager
2. Click on “eTrust Generic Recorder Service” use Start/ Stop service button from GUI to take corrective action depending on the requirement.

To Stop/Start from the command line interface:

1. Open command prompt
2. Go to eTrust Audit installed directory
 \Program Files\CA\eTrust Audit\bin
3. Issue command
 acrecorderd - start ----- to start Generic recorder service
 acrecorderd - stop ----- to stop Generic recorder service
 acrecorderd – help ----- for more options

7.7.Solaris Generic Recorder Maintenance

The Generic Recorder works as standard process named “acrecorderd”.

To Start/Stop this process

1. Switch to directory path “/export/opt/CAaudclnt/bin”
2. Issue command
 ./acrecorderd - start ----- to start Generic recorder service
 ./acrecorderd - stop ----- to stop Generic recorder service
 ./acrecorderd – help ----- for more options

8. Integration of eTrust Audit

In the Citigroup storage infrastructure, the eTrust client will be installed on every Symmetrix, DMX and Connectrix service processor. In addition, it will also be installed on all Navisphere Management stations. These clients will be configured to pass events back to the eTrust Collector database, for viewing by the Global Storage Management Group (GSMG).

8.1. eTrust Audit Client Software Installation

Only EMC authorized personnel are allowed to install and configure the client software on a DMX, Symm or Connectrix SP. Unapproved modifications to EMC code can invalidate the maintenance agreement. Storage Integration will install and configure the client software on the Navisphere management stations via package eacl1510.

The client consists of the following subcomponents/services (described above).

- Standard System Recorder
- Generic Log Scraper
- Portmapper
- Redirector
- Router
- Action Manager
- Distribution Agent

8.1.1. eTrust Audit Client Installation Steps

A copy of the message-parsing file is included in the appendix specific to the client platform and a zip file containing configuration files will be provided to EMC.

1. Manually create the directory where the MP file will reside. This will make sense later in the install when you select the MP file directory in step 9.

Click Start, Command Prompt

Enter "**c:**" to get to drive c.

Enter the following command to create the directory.

mkdir "Program Files\CA\Trust Audit\cfg"

Exit Command Prompt

Use Explorer to copy the MP file into the newly created directory.

PWHOST.mp for EMCRemote logs (create on DMX & Symm5)

Symm5_logall.mp for Symm5 SymmWin logs

DMX_logall.mp for DMX SymmWin logs

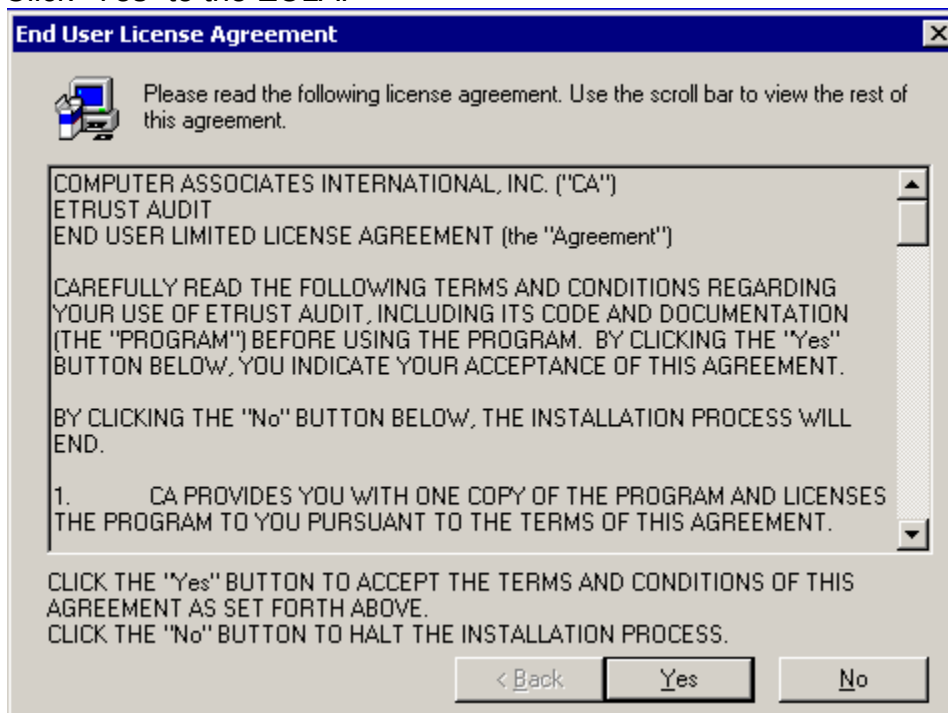
Navisphere.mp for Navisphere logs (create on Navisphere Mgmt Server)

HDSDevManager.mp for HDS Device Manager logs

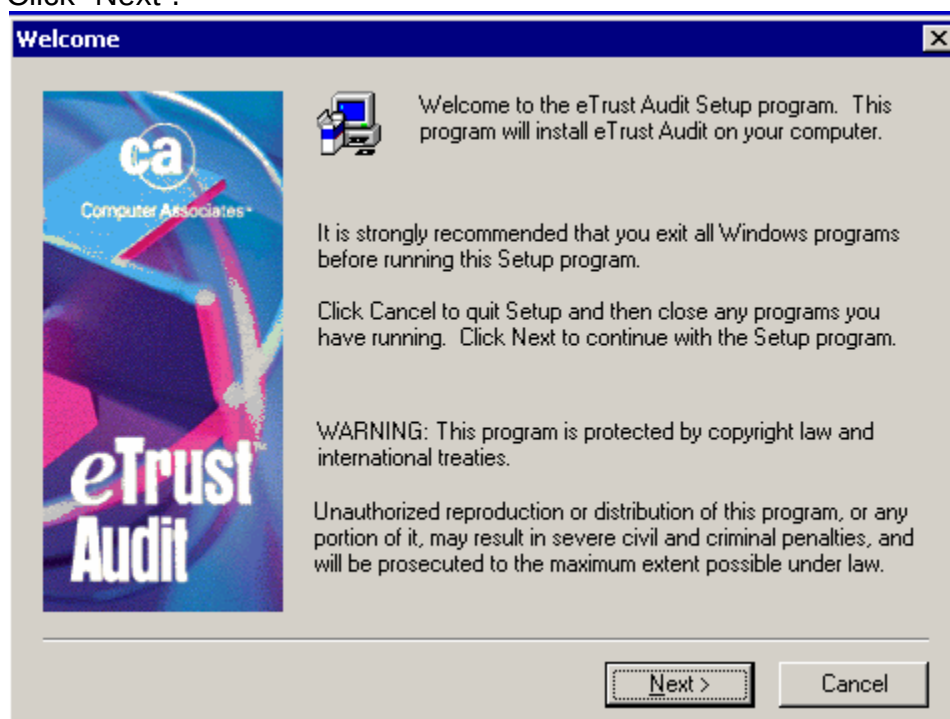
HDSStprageNav.mp for HDS Array Logs (Syslog)

2. EMC: Start installation via preferred startup method.
Integration: Start the installation via package eacl1510 (current to date).

Click "Yes" to the EULA.



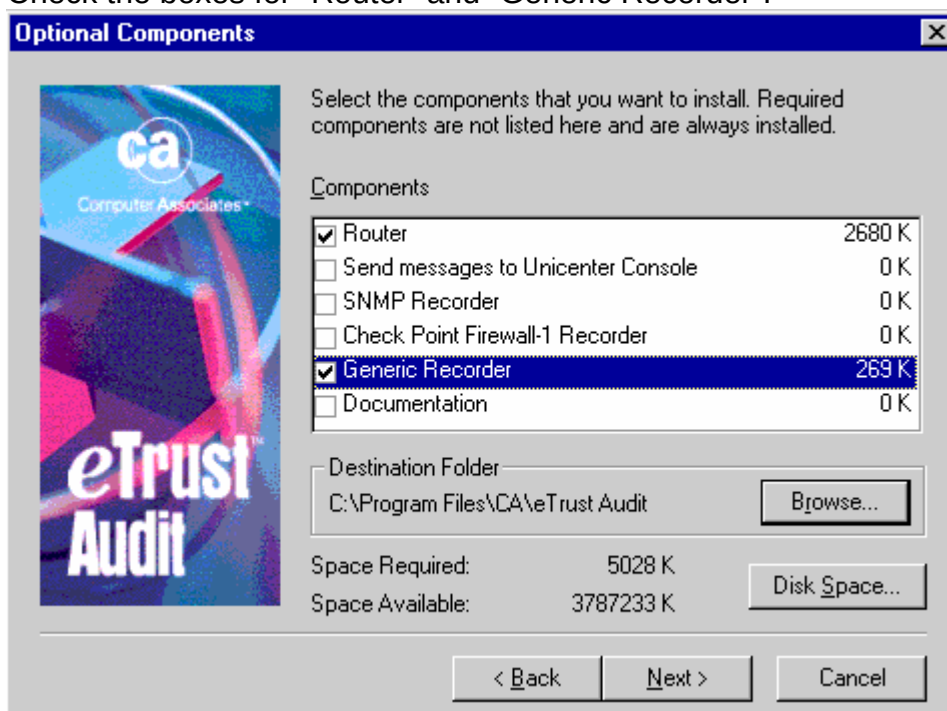
Click "Next".



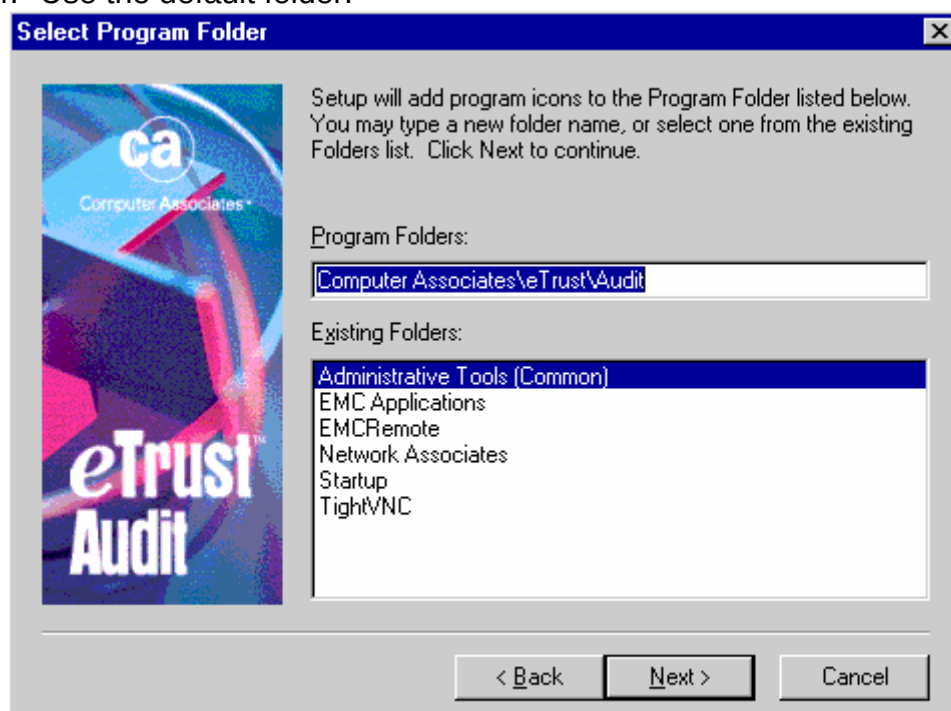
Select "Custom"



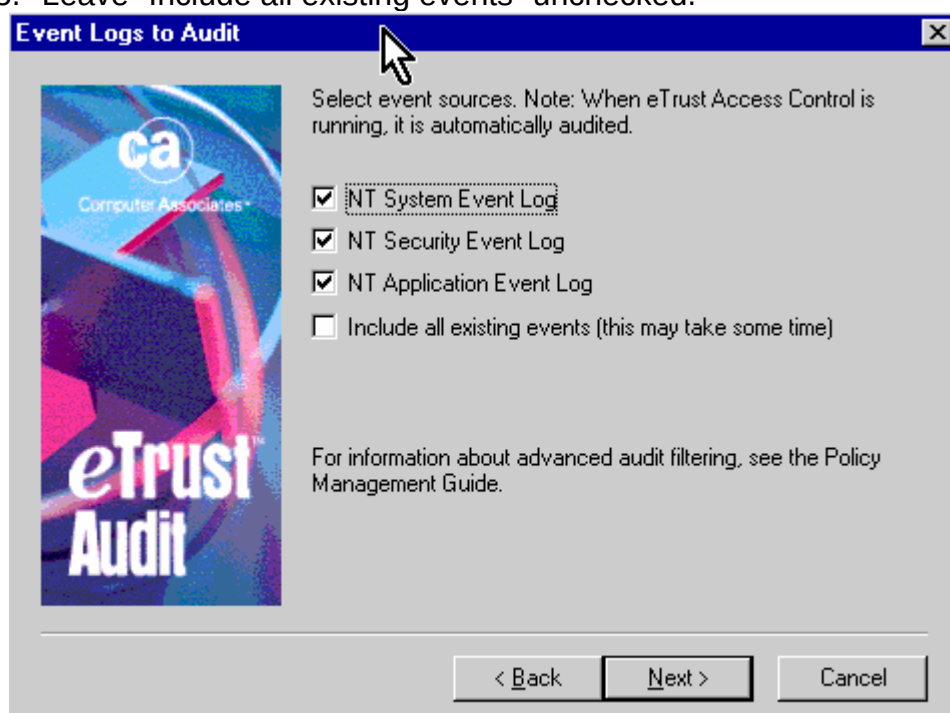
3. Check the boxes for “Router” and “Generic Recorder”.



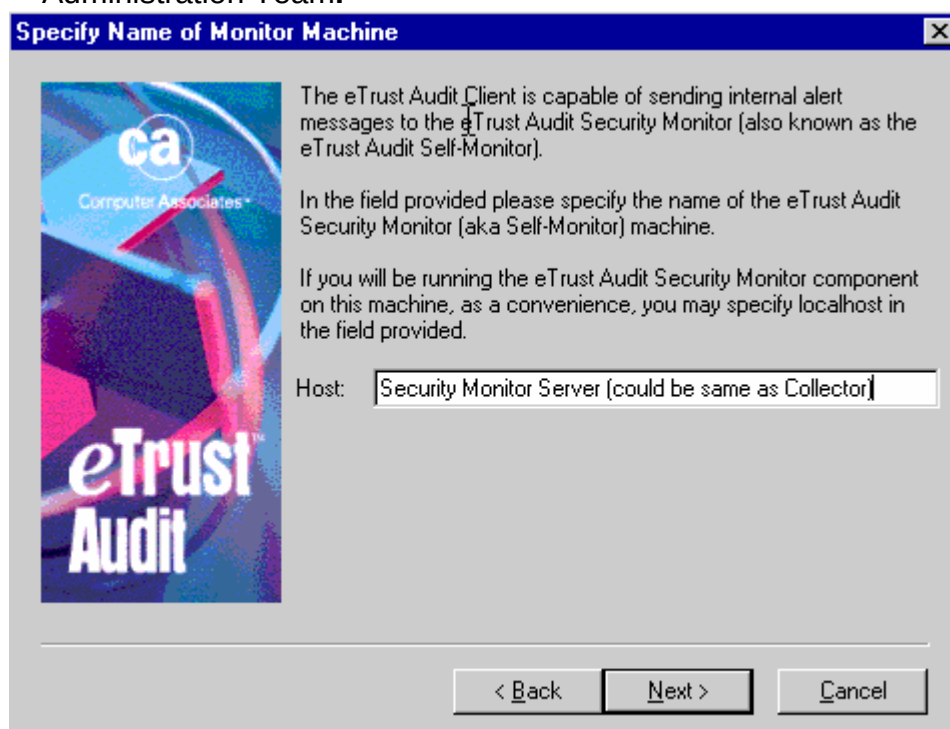
4. Use the default folder.



5. Leave "Include all existing events" unchecked.



6. Enter the Security Monitor server name provided by the Global eTrust Administration Team.





Please wait while detecting host ...

7. Enter the Policy Manager server name provided by Global eTrust Administration Team.

Specify Name of eTrust Audit Policy Manager Machine [X]

The eTrust Audit Client Components take direction from an eTrust Audit Policy Manager machine.

In the field provided please specify the name of the machine that will be running the eTrust Audit Policy Manager that this eTrust Audit Client accepts directions from.

If you will be running the eTrust Audit Policy Manager component on this machine, as a convenience, you may specify 'localhost' in the field provided.

Host:

< Back Next > Cancel



Please wait while detecting host ...

8. Click “Add” to configure Message Parsing.



9. Enter "Recorder Name", "Log Name", "MP File" and Log Files. Click OK.

For Navisphere log monitoring.

Recorder: Navisphere

Log Name: Navisphere

MP File: C:\Program Files\CA\e-trust Audit\cfg\Navisphere.mp

Log Files: C:\Logs*.log

For EMCRemote log monitoring

Recorder: EMCRemote

Log Name: EMCRemote

MP File: C:\Program Files\CA\e-trust Audit\cfg\PWHOST.mp

Log Files: C:\Program Files\EMC\SymmRemote\PWHOST.log

For DMX log monitoring

Recorder: SymmWin_DMX

Log Name: SymmWin_DMX

MP File: C:\Program Files\CA\e-trust Audit\cfg\DMX_logall.mp

Log Files: C:\EMC\swlfg\audit*.log

For Symm5 log monitoring

Recorder: SymmWin_Symm5

Log Name: SymmWin_Symm5

MP File: C:\Program Files\CA\e-trust Audit\cfg\Symm5_logall.mp

Log Files: C:\EMC\swlfg\audit*.log

For HDS Device Manager Monitoring

Recorder: HDSEvManager

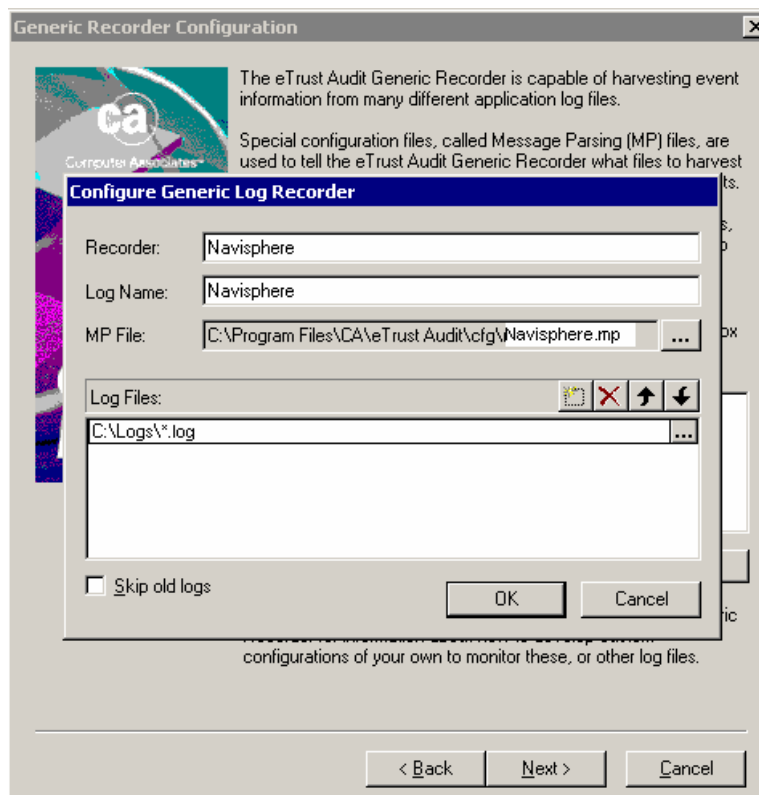
Log Name: HDSEvManager

MP File: C:\Program Files\CA\e-trust Audit\cfg\HDSEvManager.mp

Log Files: C:\Program Files\HiCommand\DeviceManager\HiCommandServer\logs\service.log

For HDS USP Array Monitoring (Syslog)

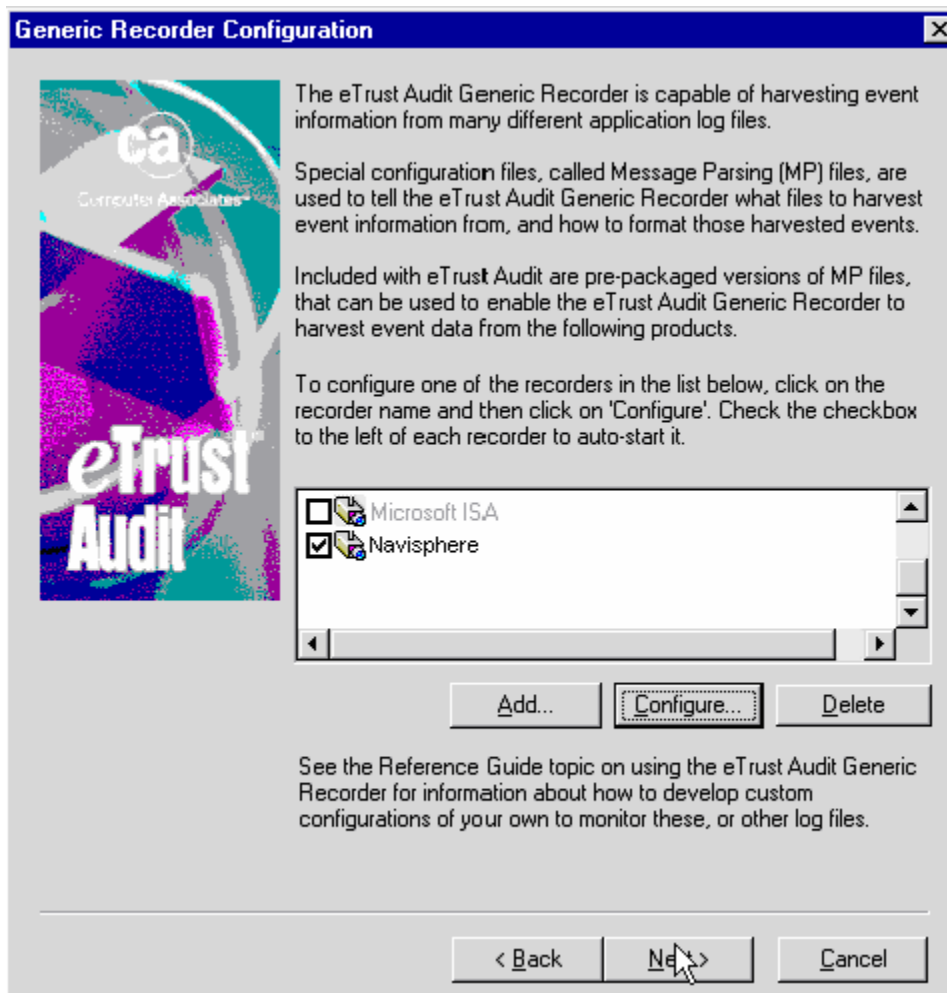
This will be configured through a non-gui interface. Please see Appendix E for details.



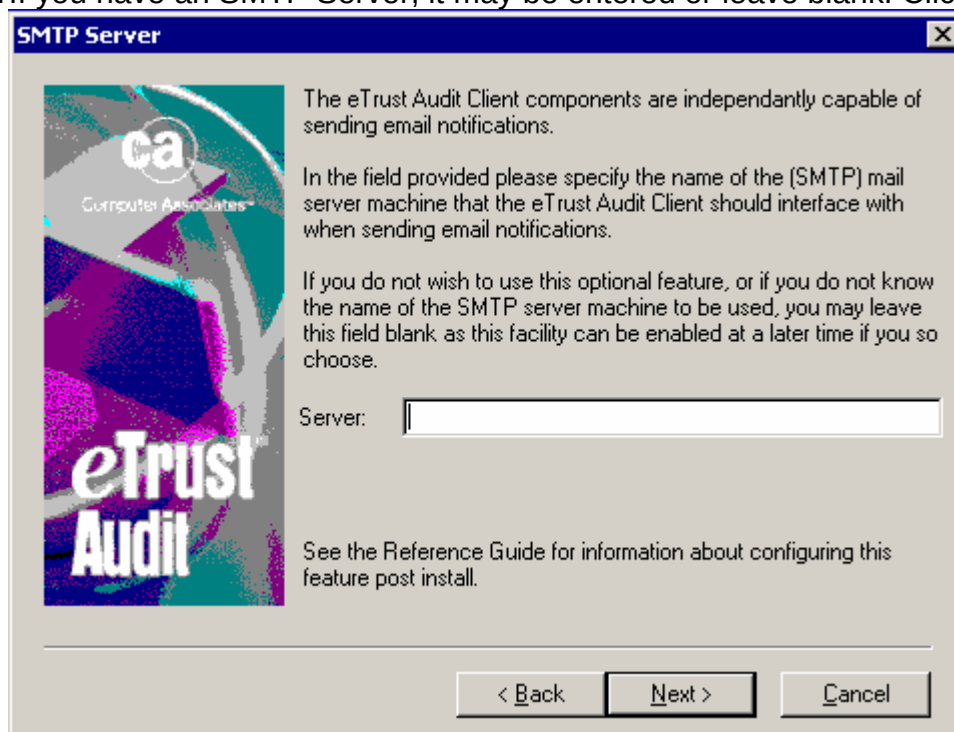
10. For Navisphere servers click "Next".

For EMC Service Processors, you add two different Generic Recorders (SymmWin and EMCRemote logs).

For Connectrix Service Processors, you add one Generic Recorder (EMCRemote logs). When complete, click "Next".



11. If you have an SMTP Server, it may be entered or leave blank. Click Next.



The eTrust Audit Client components are independently capable of sending email notifications.

In the field provided please specify the name of the (SMTP) mail server machine that the eTrust Audit Client should interface with when sending email notifications.

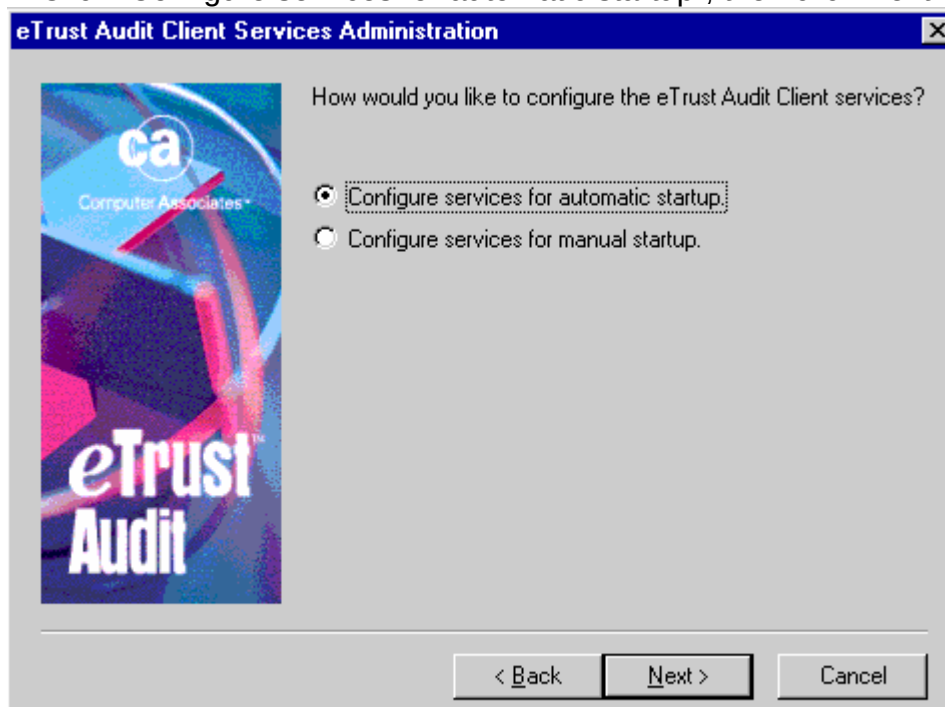
If you do not wish to use this optional feature, or if you do not know the name of the SMTP server machine to be used, you may leave this field blank as this facility can be enabled at a later time if you so choose.

Server:

See the Reference Guide for information about configuring this feature post install.

< Back Next > Cancel

12. Click “Configure services for automatic startup”, then click Next.



eTrust Audit Client Services Administration

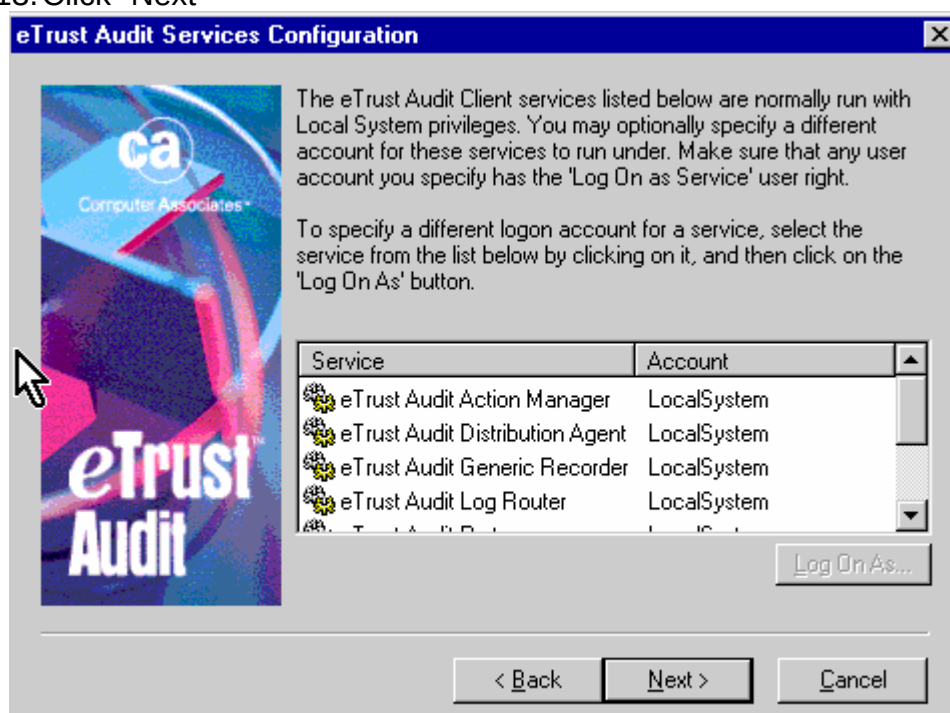
How would you like to configure the eTrust Audit Client services?

☒ Configure services for automatic startup.

☐ Configure services for manual startup.

< Back Next > Cancel

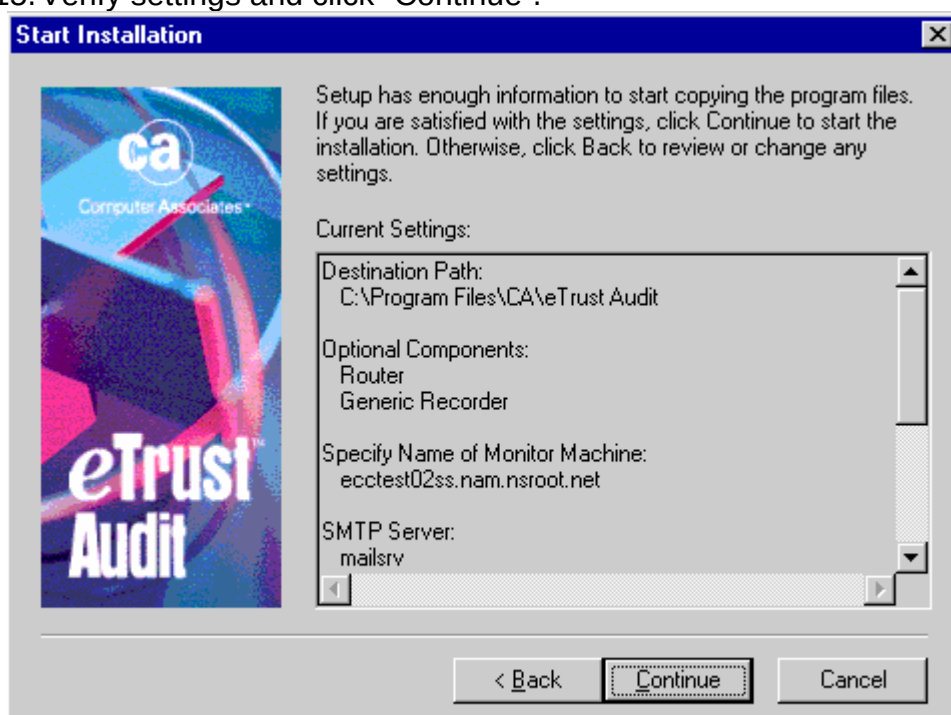
13. Click "Next"



14. Click "Next"



15. Verify settings and click “Continue”.

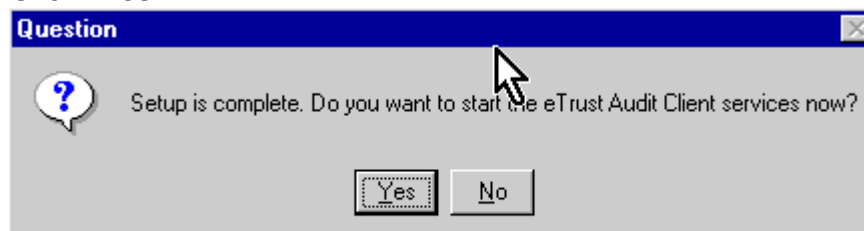


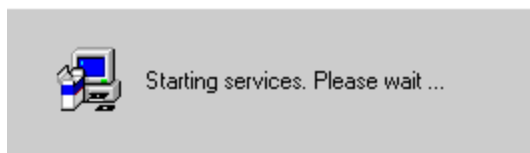
Setting up eTrust Audit infrastructure. This may take a few minutes.



Please wait while services are being set up ...

16. Click “Yes”





Client setup is complete.

8.1.2. Installation Verification

On Windows 2000 (DMX):

Click Start\Settings\Control Panel. Double click "Administrative Tools". Double click on "Services"

On Windows NT (Symm5 and older):

Click Start\Settings\Control Panel. Double click "Services"

Verify that the eTrust Services are started.

- eTrust Audit Action Manager
- eTrust Audit Distribution Agent
- eTrust Audit Generic Recorder
- eTrust Audit Log Router
- eTrust Audit Portmap
- eTrust Audit Recorder
- eTrust Audit Redirector

If any of these services are NOT started, click on it and click the "Start" button.

8.2. eTrust Audit Client Software Configuration

For eTrust Audit Client software to function correctly there are several modifications that need to be made manually. The changes in this section will need to be made on all eTrust Audit Client nodes. For platform specific modifications, see the appendix for your installation type.

- Appendix A: Firewall Ports
- Appendix B: CLARiiON (Navisphere)
- Appendix C: EMC (DMX & Symm)
- Appendix D: Connectrix
- Appendix E: HDS USP

8.2.1. Client Configuration

Modification to file: "LogNames.txt". The numbers (Example: 150, 151, 152 and 153) will need to be consistent on all Clients, Collectors and Policy Mgr servers.



8.2.2. Registry Settings

The eTrust network ports have to be manually configured in the registry under eTrust (HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Ports).

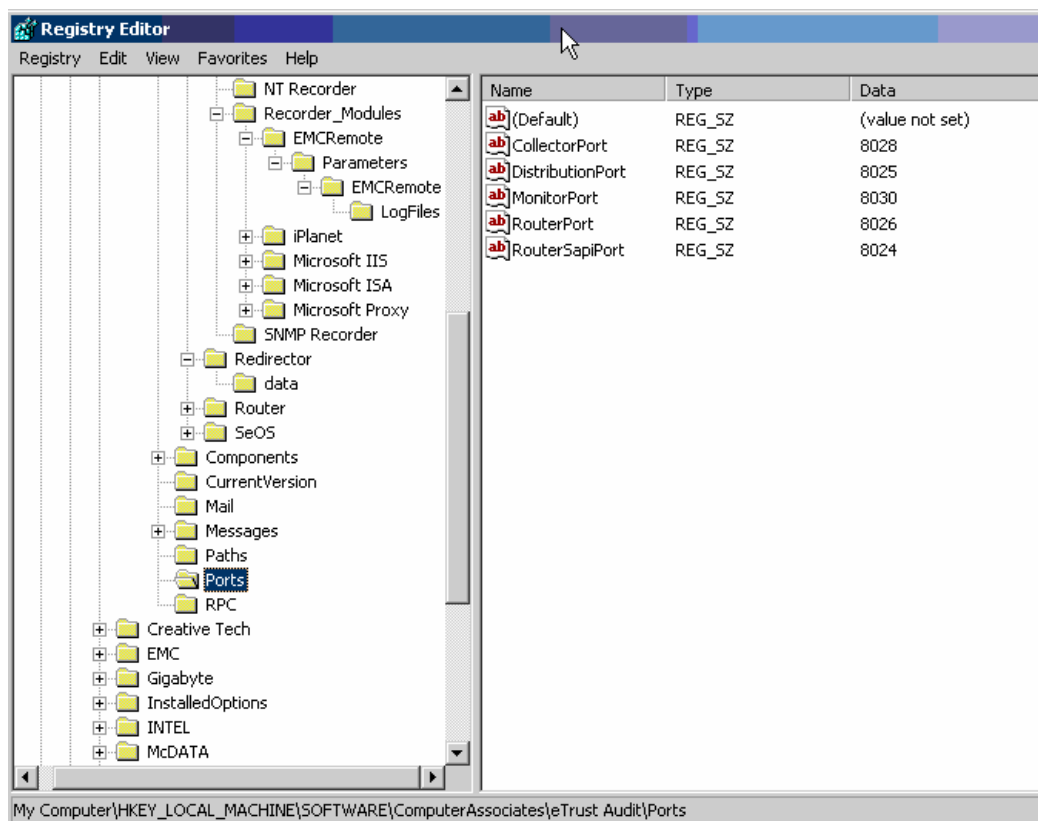
CollectorPort: 8028

DistributionPort: 8025

MonitorPort: 8030

RouterPort: 8026

RouterSapiPort: 8024





3. Enter Audit Node Type (ie: *EMCRemote*, *SymmWin_DMXX*, *SymmWin_Symm5*, *Navisphere* or *HDS*), Click Add.

Audit Node Types

Existing AN types

Name	Description
ACF2	ACF2
Apache	Apache Server
AS400	AS400 Recorder
AuditEngine	Audit Engine
BEA Weblogic	BEA Weblogic
BindView	BindView
CacheFlow	CacheFlow

Delete

New AN type

Name:

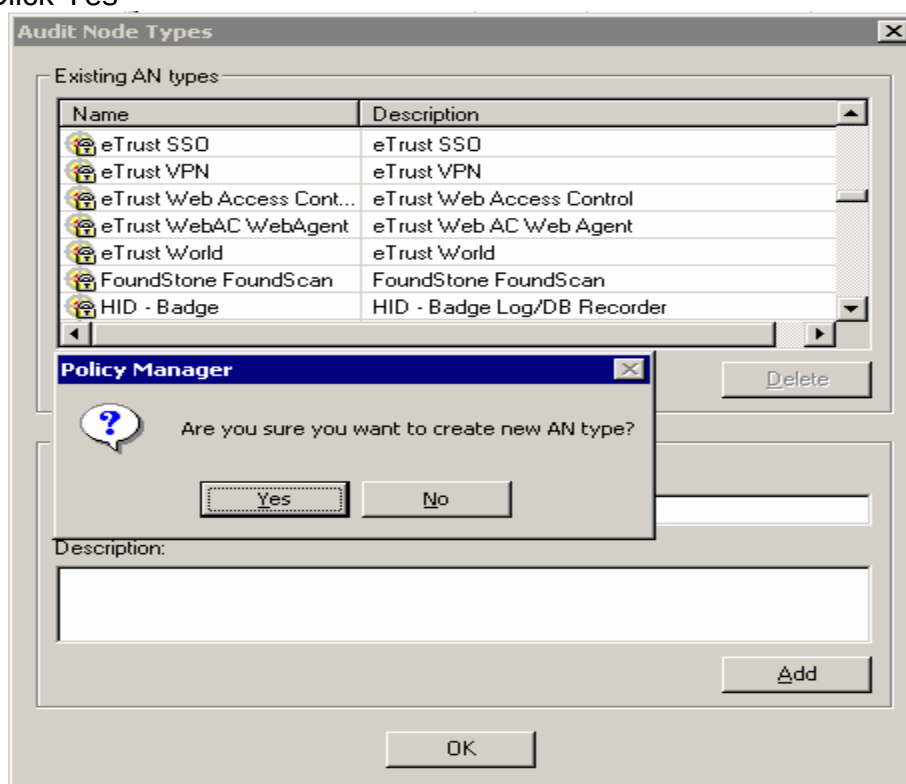
EMCRemote

Description:

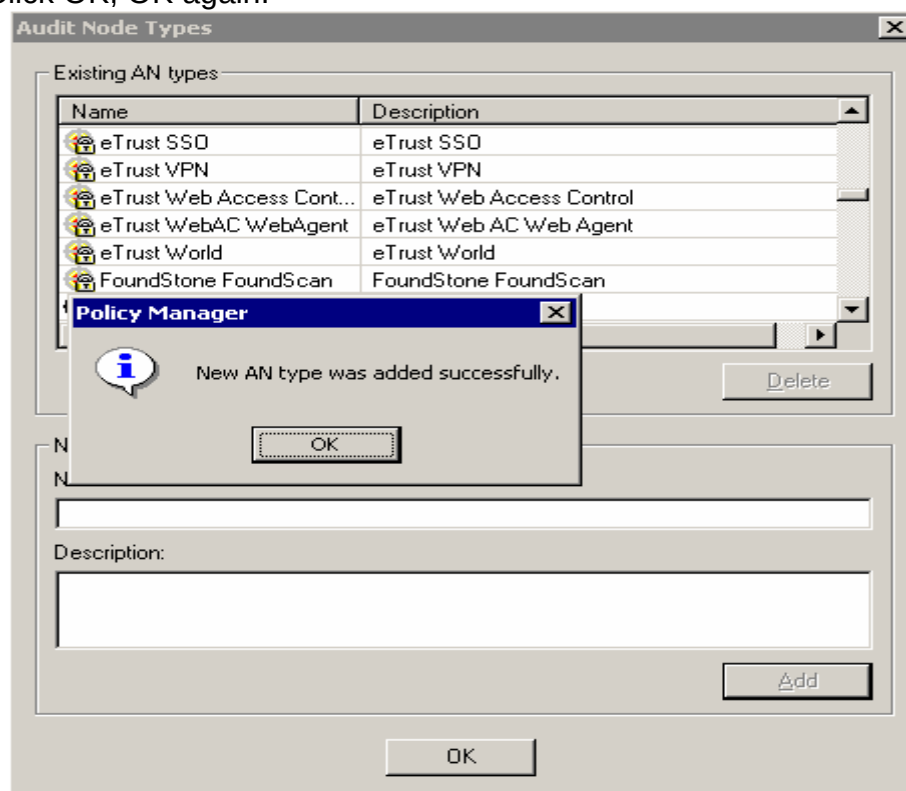
Add

OK

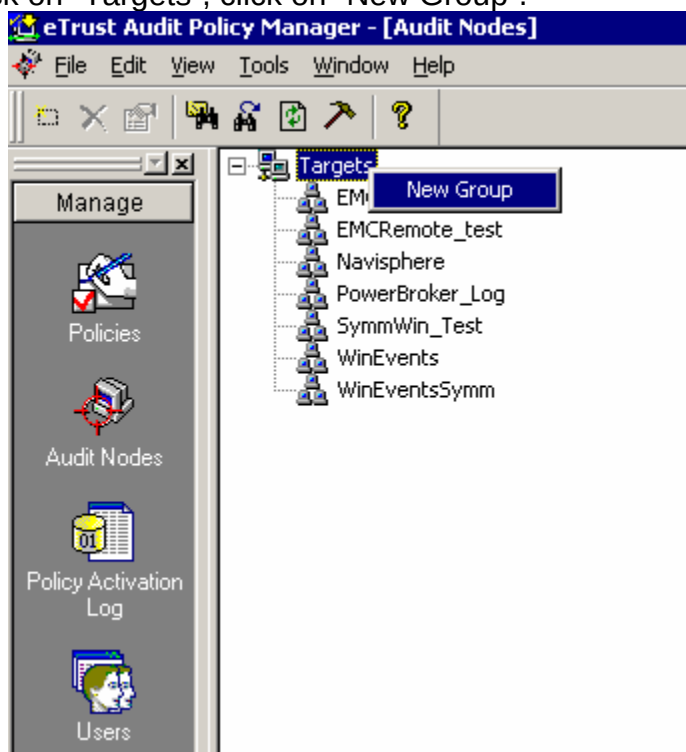
4. Click Yes



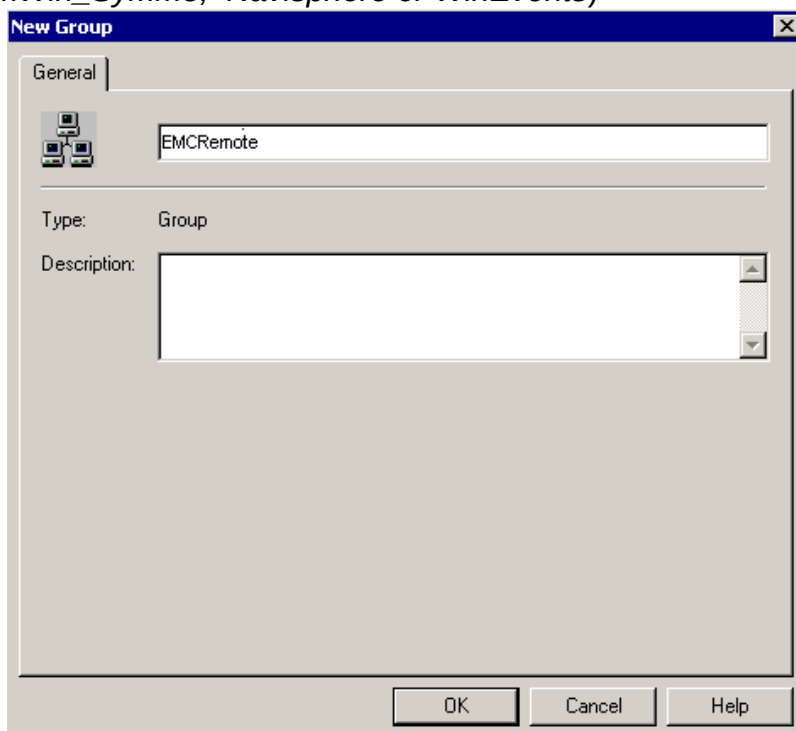
5. Click OK, OK again.



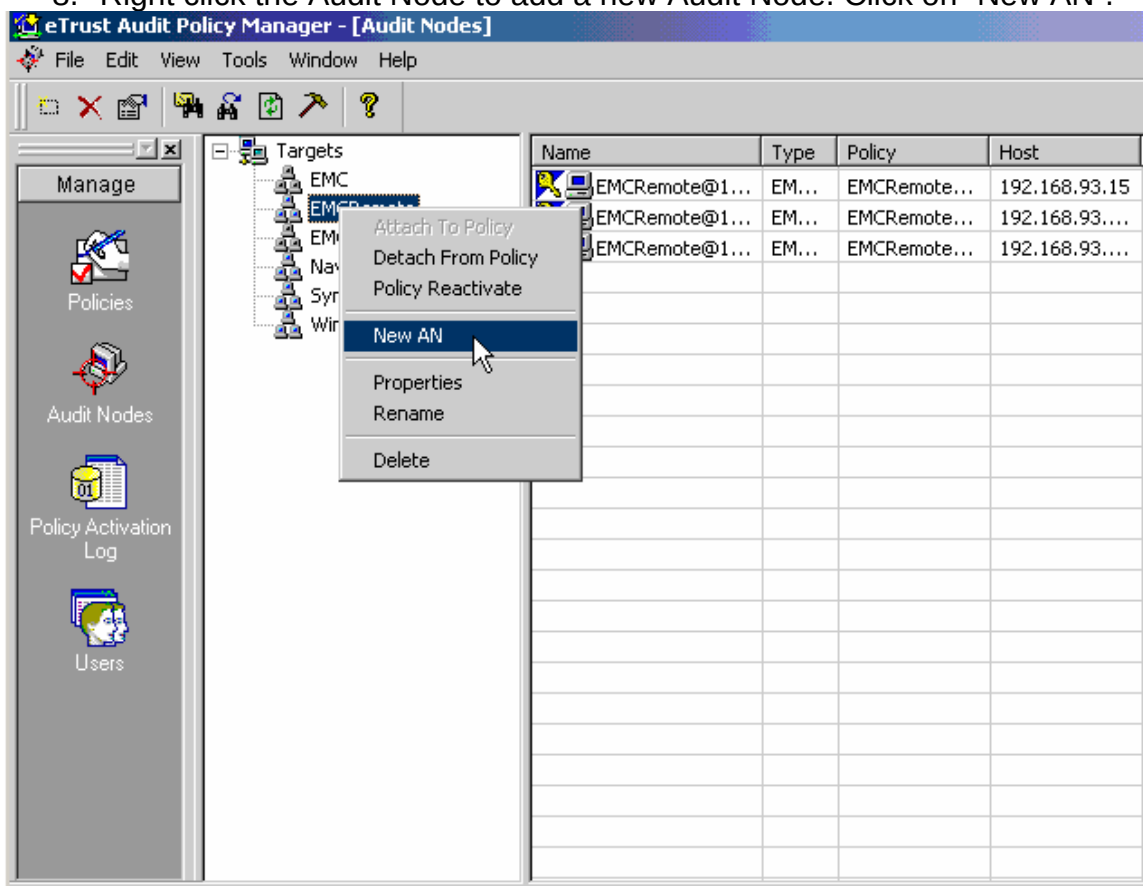
6. Right click on "Targets", click on "New Group".



7. Enter the Audit "Group Name". (Example: *EMCRemote*, *SymmWin_DMX*, *SymmWin_Symm5*, *Navisphere* or *WinEvents*)

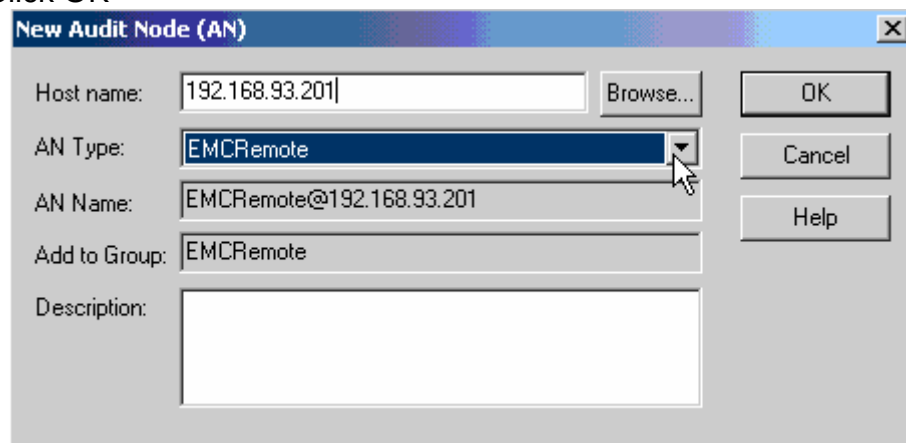


8. Right click the Audit Node to add a new Audit Node. Click on “New AN”.



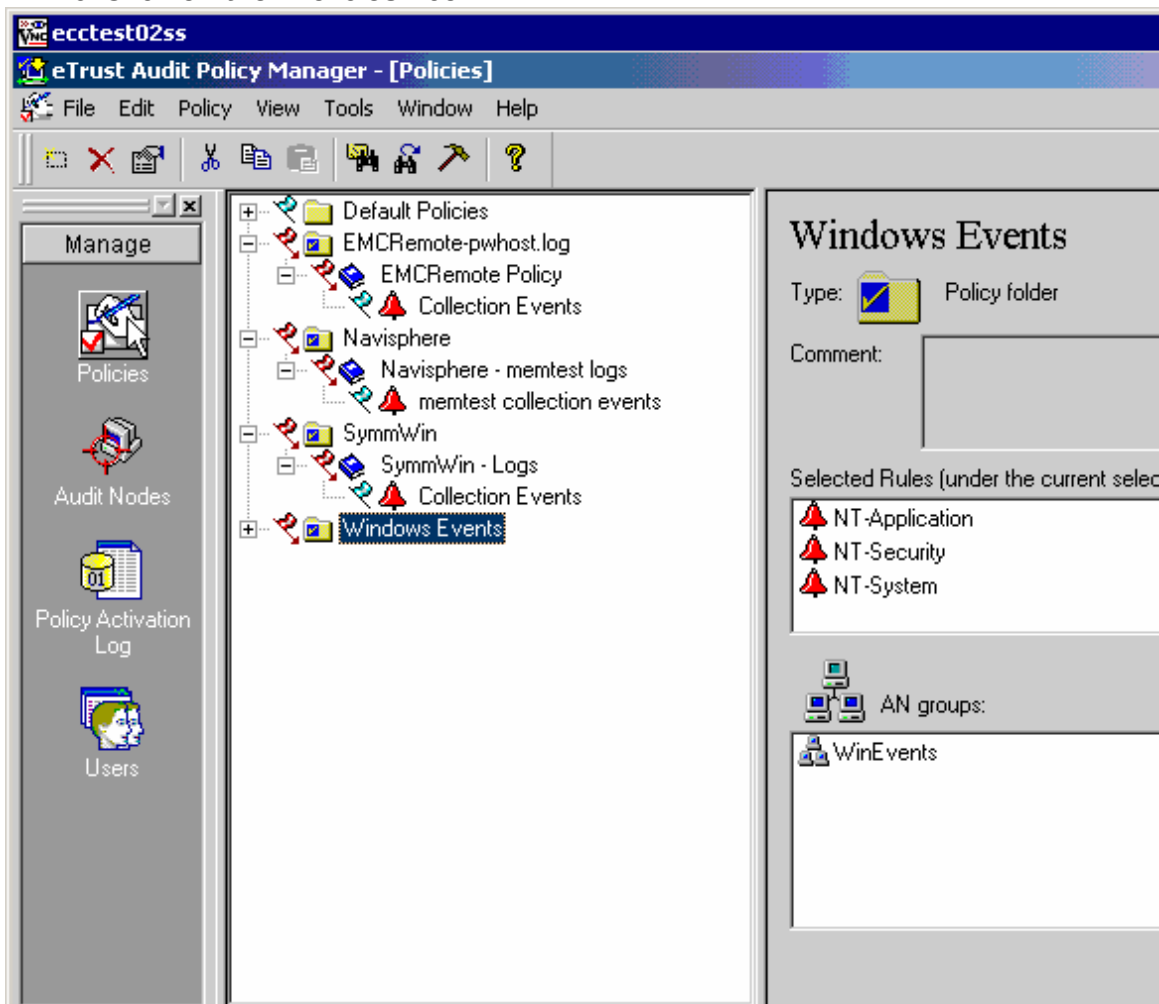
9. Enter Hostname or IP address of Navisphere Server, DMX, Symm or Connectrix SP. Use the dropdown to select AN Type (*EMCRemote*, *SymmWin_DMX*, *SymmWin_Symm5*, *Navisphere* or *NT* for WinEvents).

Note: WinEvents will only be collected for Navisphere Mgmt Station.
Click OK

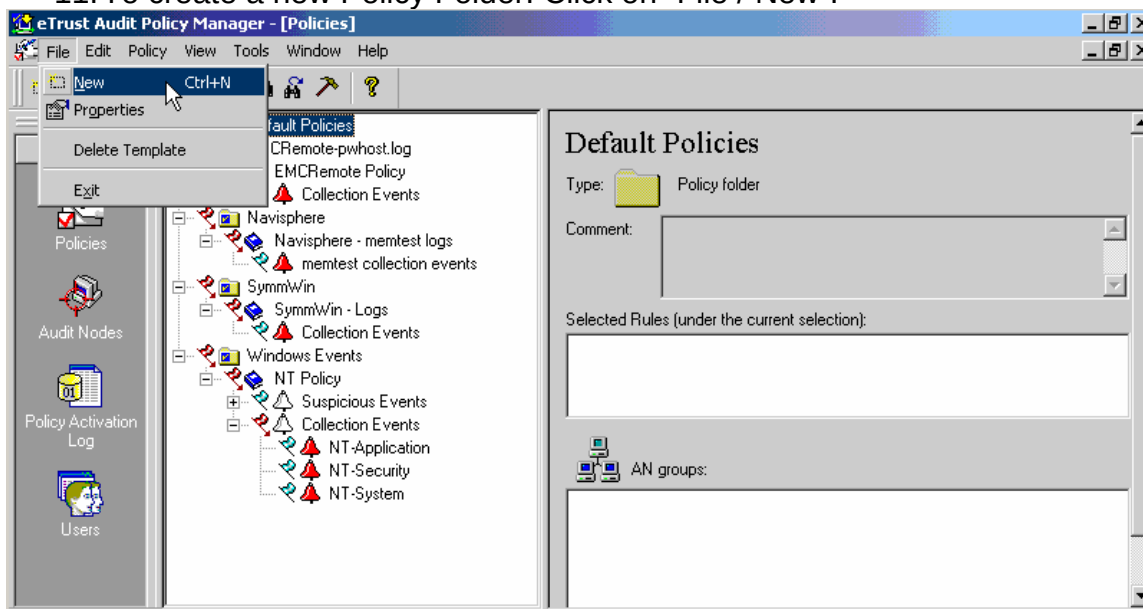


Create Policies.

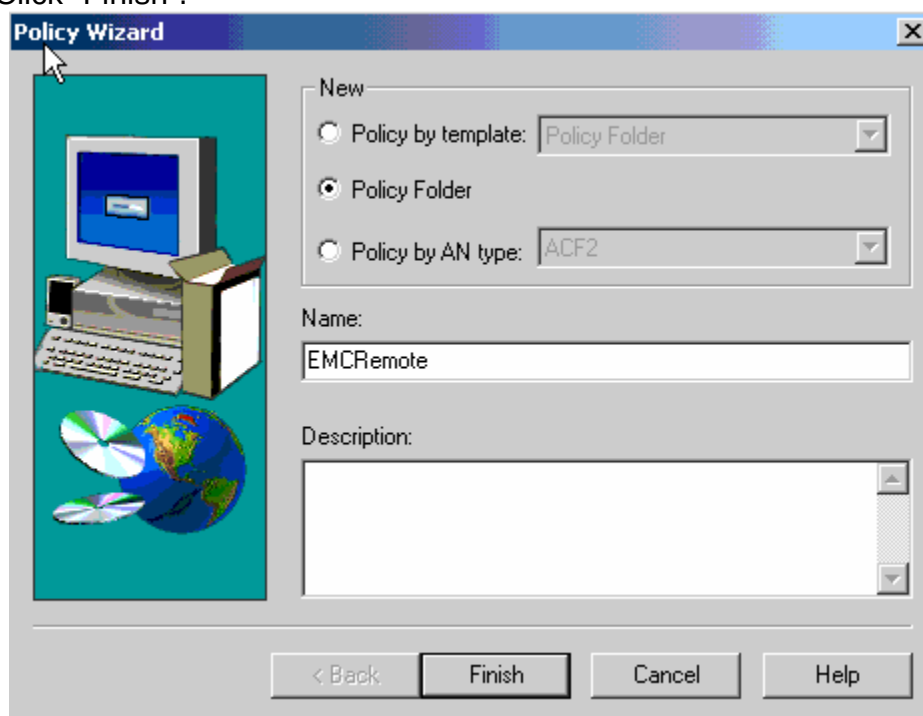
10. Click on the “Policies” icon.



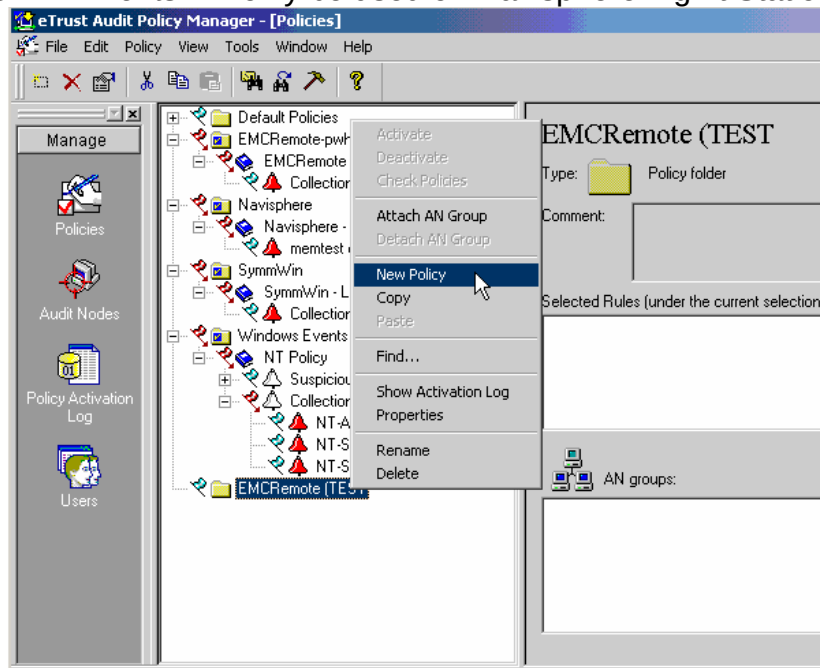
11. To create a new Policy Folder. Click on “File / New”.



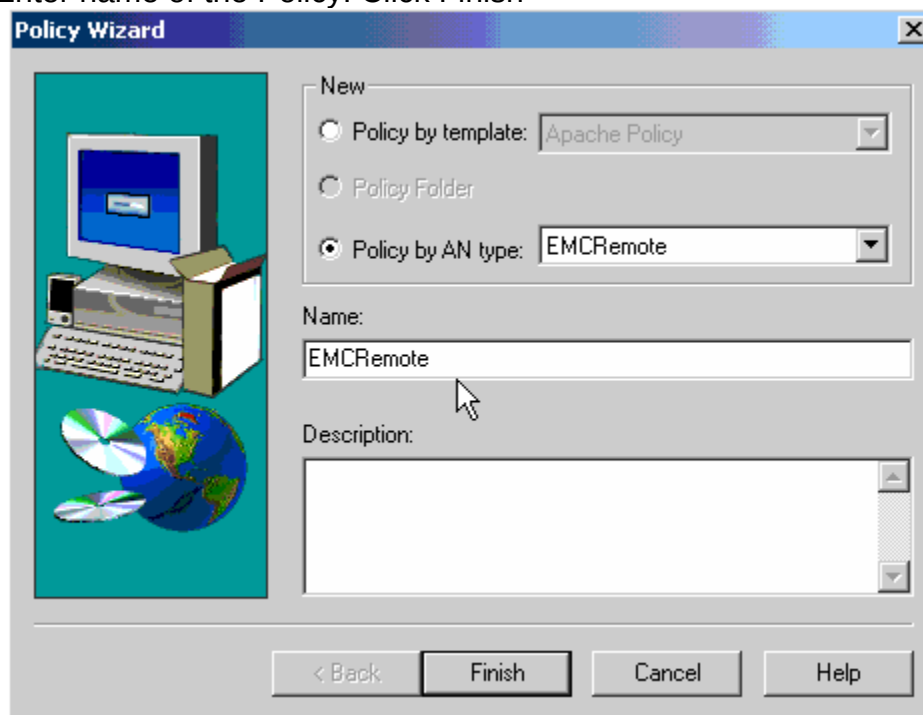
12. Click Policy Folder and enter the name of the folder (ie: *EMCRemote*, *SymmWin_DMx*, *SymmWin_Symm5*, *Navisphere*, *HDS* or *WinEvents*)
Click “Finish”.



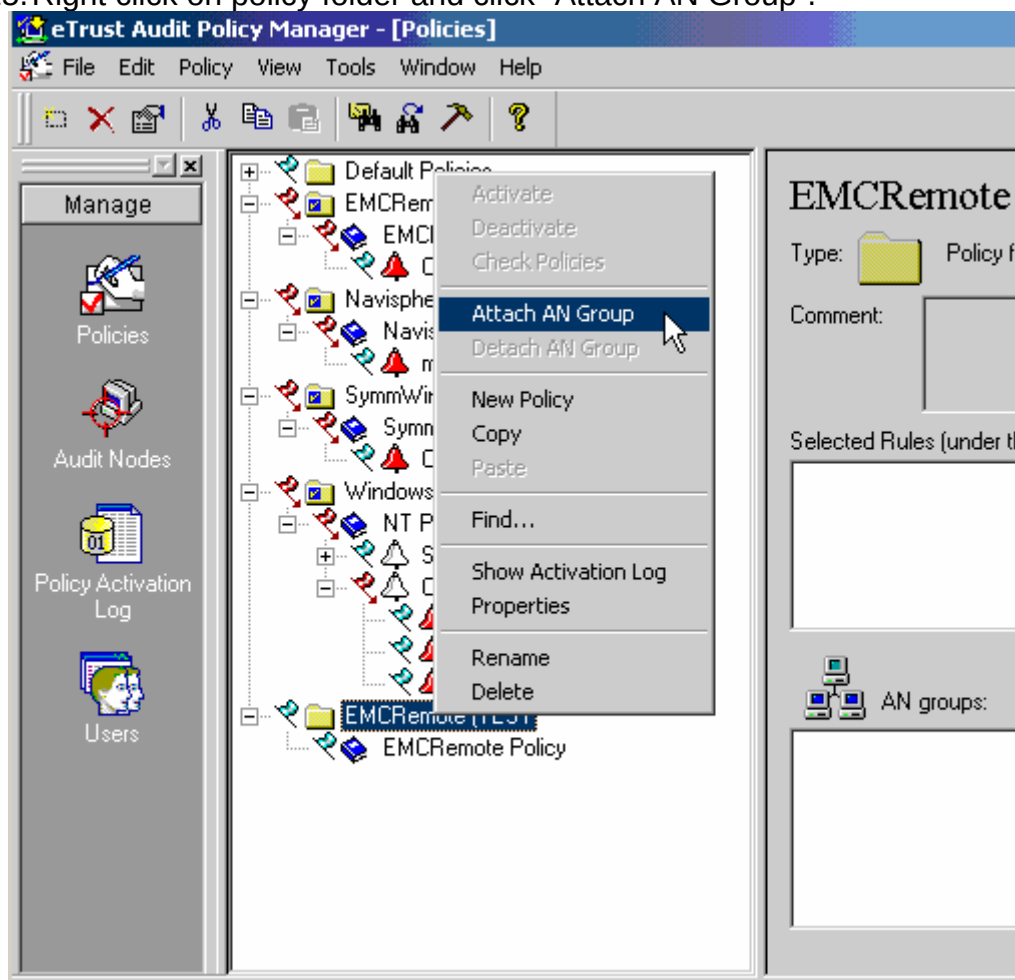
13. Right Click on the Policy Folder you just created and Click “New Policy”.
For *WinEvents*, you can copy/paste the *NT Policy* under Default Policies.
Note: *WinEvents* will only be used on Navisphere Mgmt Station.



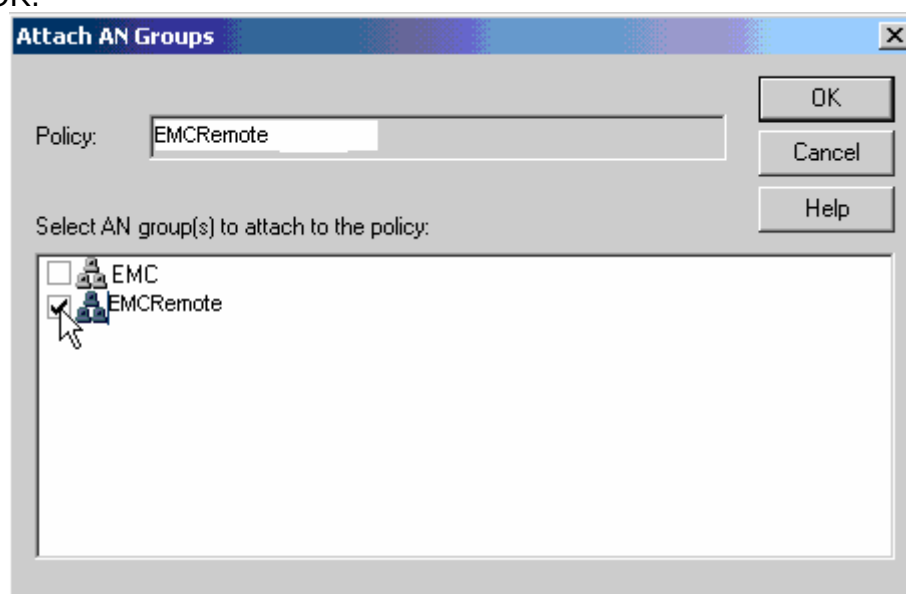
14. Click on “Policy by AN type:” and select Type from dropdown menu.
Enter name of the Policy. Click Finish



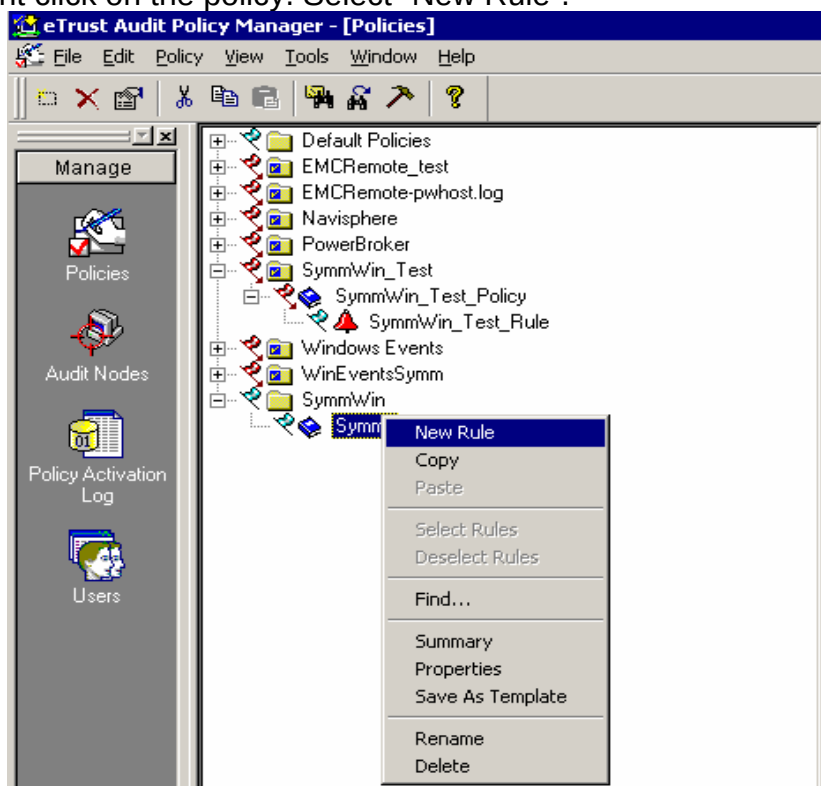
15. Right click on policy folder and click “Attach AN Group”.



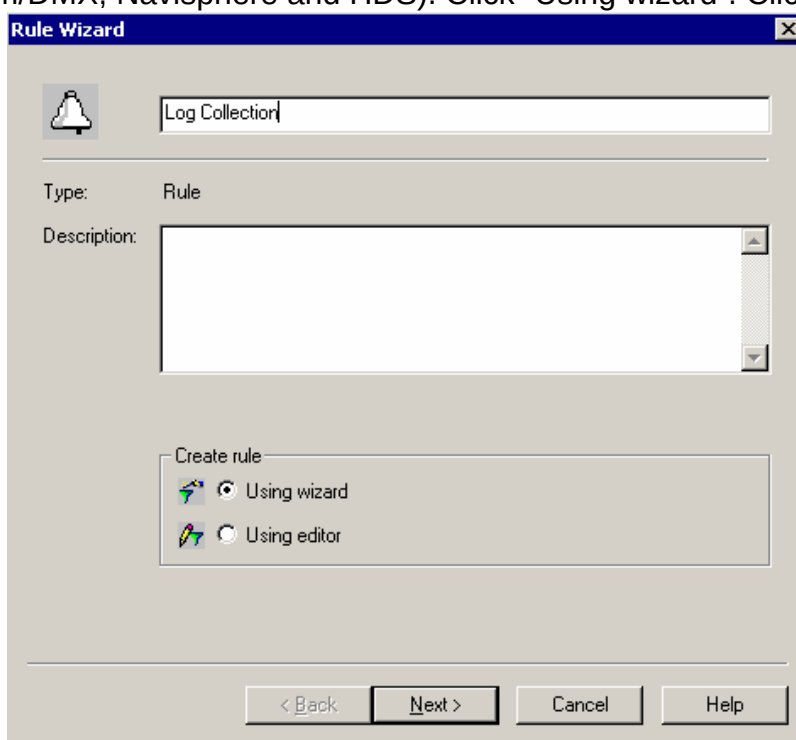
16. Check the box next to the relevant AN Group to attach to the Policy. Click OK.



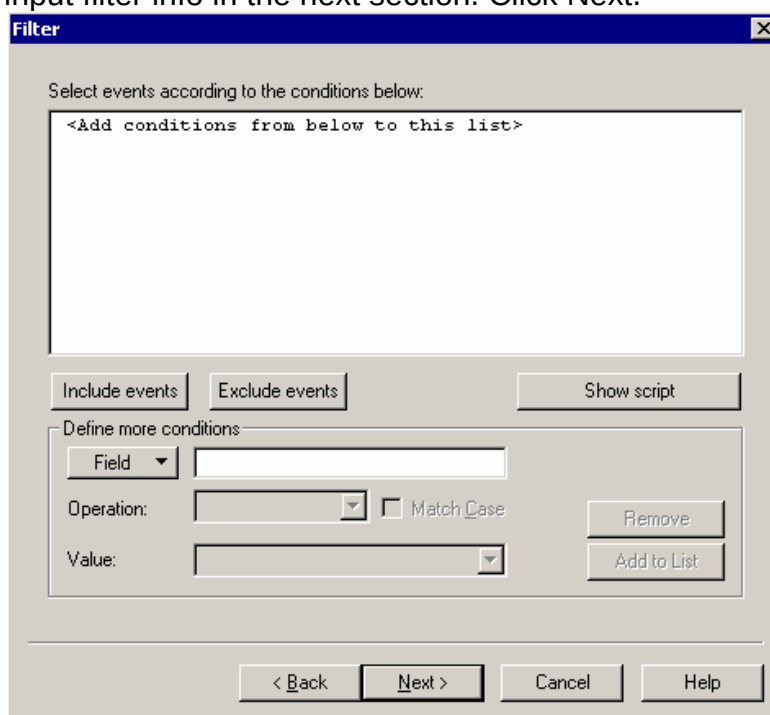
17. Right click on the policy. Select “New Rule”.



18. Enter the name of the rule (Example: *Log Collection* for EMCRremote, Symm/DMX, Navisphere and HDS). Click “Using wizard”. Click Next.

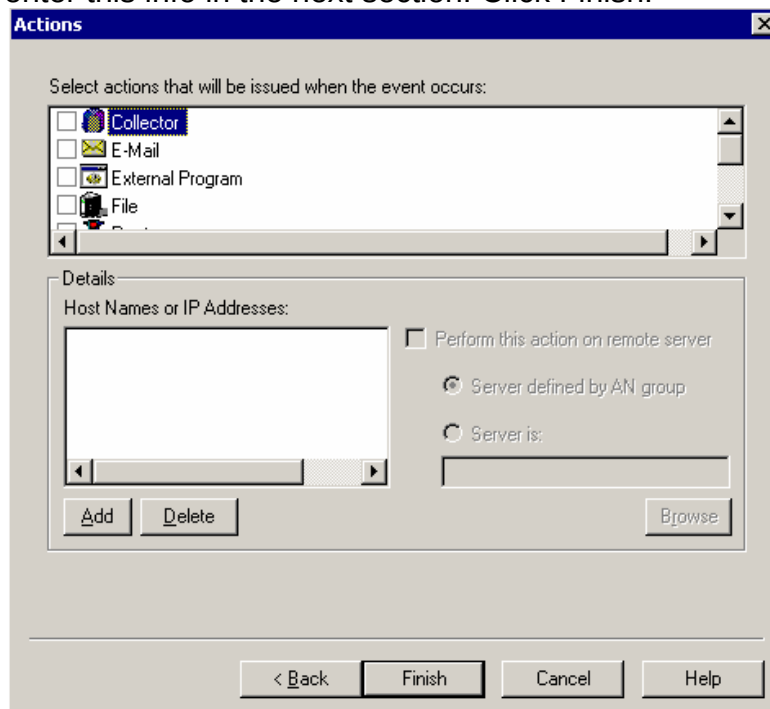


19. We'll input filter info in the next section. Click Next.



The 'Filter' dialog box is shown. It has a title bar with 'Filter' and a close button. The main area contains a text box with the placeholder '<Add conditions from below to this list>'. Below this are three buttons: 'Include events', 'Exclude events', and 'Show script'. Underneath is a section titled 'Define more conditions' which includes a 'Field' dropdown, an 'Operation' dropdown, a 'Value' dropdown, and a 'Match Case' checkbox. There are also 'Remove' and 'Add to List' buttons. At the bottom are navigation buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

20. We'll enter this info in the next section. Click Finish.



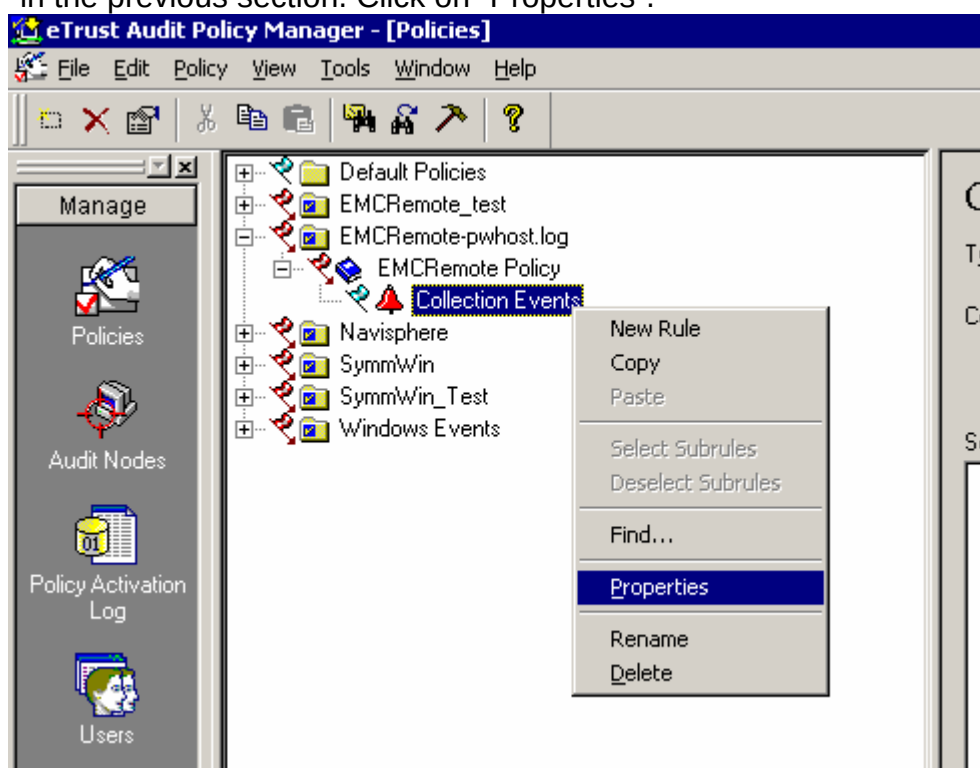
The 'Actions' dialog box is shown. It has a title bar with 'Actions' and a close button. The main area contains a list box with the following items: 'Collector', 'E-Mail', 'External Program', and 'File'. Below the list box is a section titled 'Details' which includes a text box for 'Host Names or IP Addresses:', a 'Perform this action on remote server' checkbox, and radio buttons for 'Server defined by AN group' and 'Server is:'. There are also 'Add', 'Delete', and 'Browse' buttons. At the bottom are navigation buttons: '< Back', 'Finish', 'Cancel', and 'Help'.

8.3.2. eTrust Audit Policy Rules

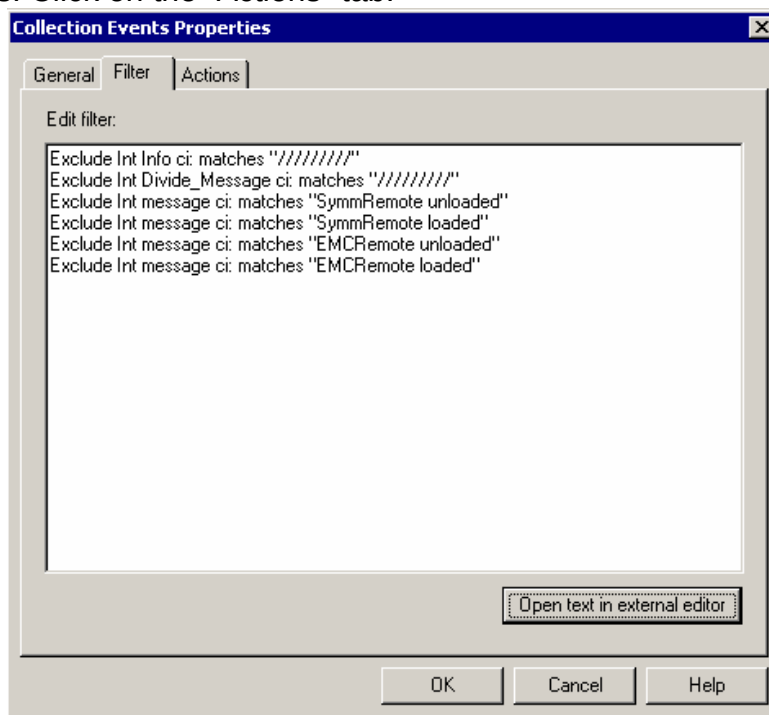
A Policy rule is similar to a script of commands that are triggered by the events received by the router component of the Audit Client. Each event that passes through the Audit Client (Router) is tested against the Policy Rules that are created and distributed by the Policy Manager. Policy rules are defined as sequences of Include (Select) or Exclude (Ignore) filters, and each event must pass through these filters before the event is selected for Audit Action destinations.

The following steps detail how to add “exclude” and “include” filters to a policy.

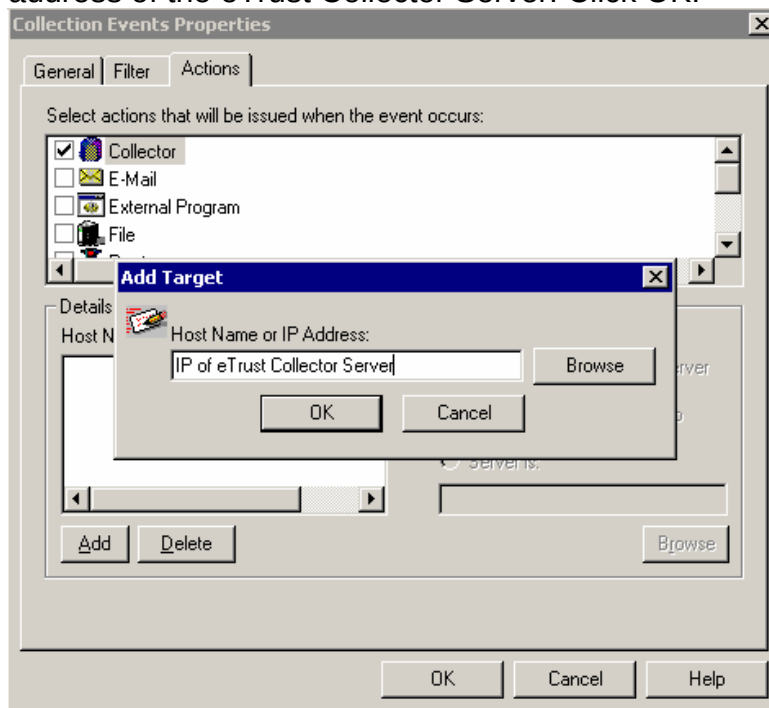
1. Right click on the policy collection event (*Log Collection*) that was created in the previous section. Click on “Properties”.



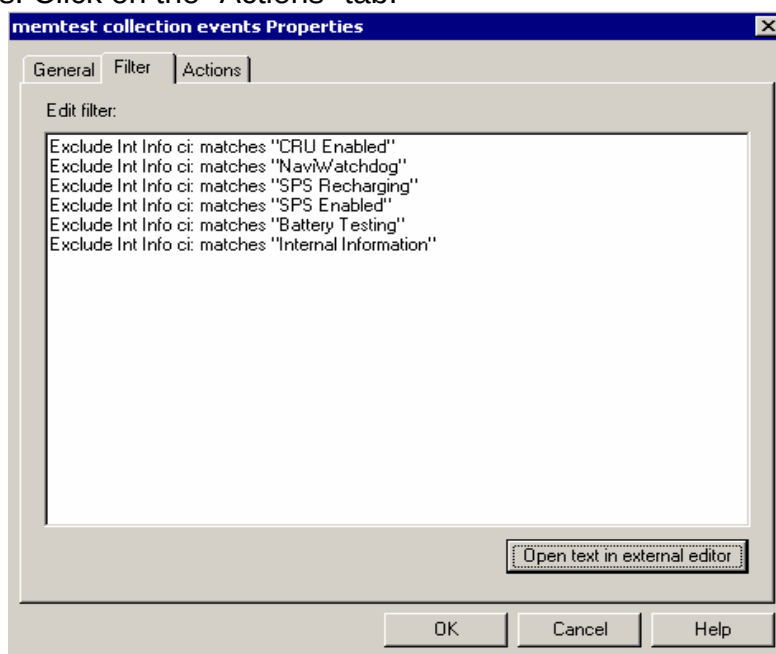
2. For the EMCRemote policy, click on the “Filter” tab and add the following entries. Click on the “Actions” tab.



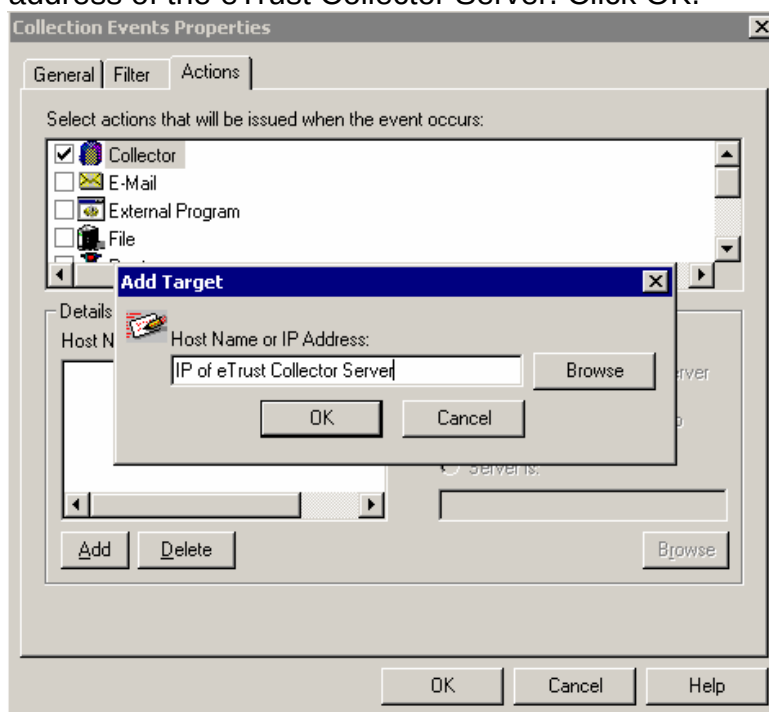
From the “Actions” tab. Check the “Collector” box and click on “Add”. Enter the IP address of the eTrust Collector Server. Click OK.



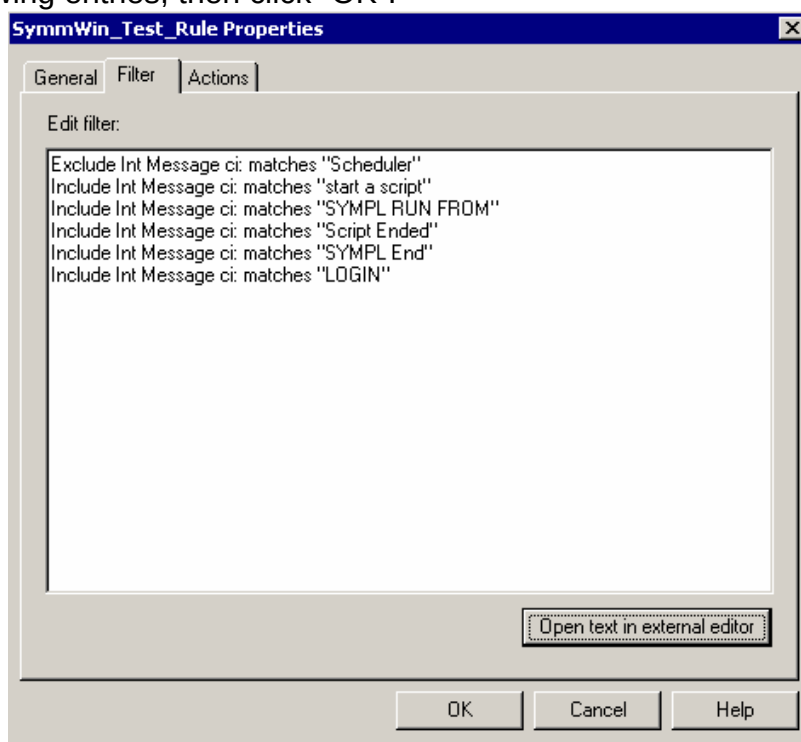
3. For the Navisphere policy, click on the “Filter” tab and add the following entries. Click on the “Actions” tab.



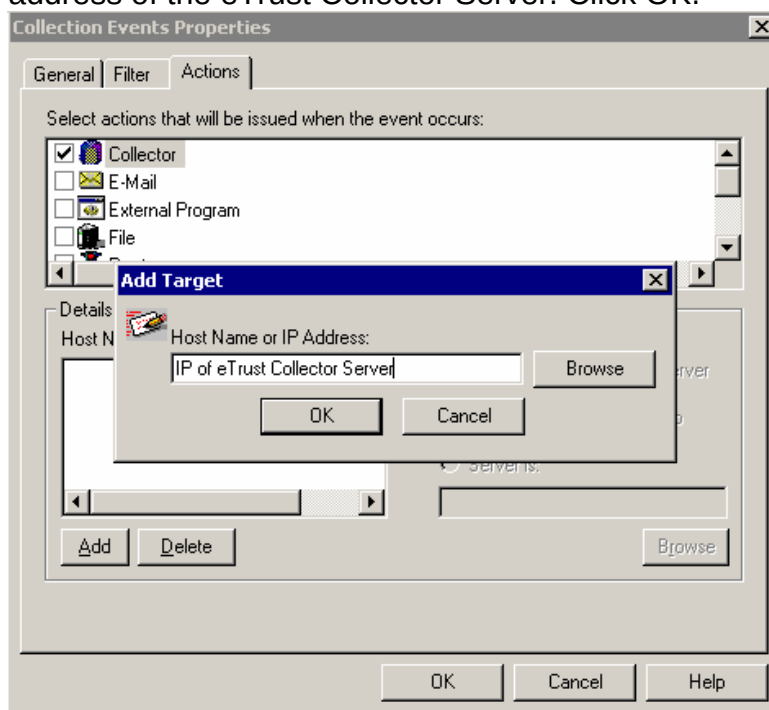
From the “Actions” tab, check the “Collector” box and click on “Add”. Enter the IP address of the eTrust Collector Server. Click OK.



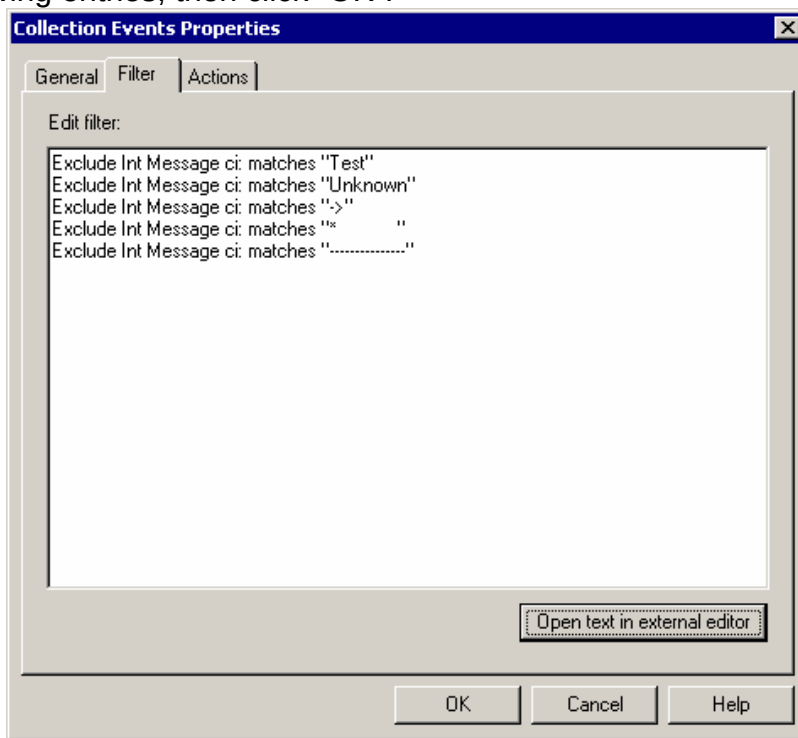
4. For the SymmWin_DMx policy, click on the “Filter” tab and add the following entries, then click “OK”.



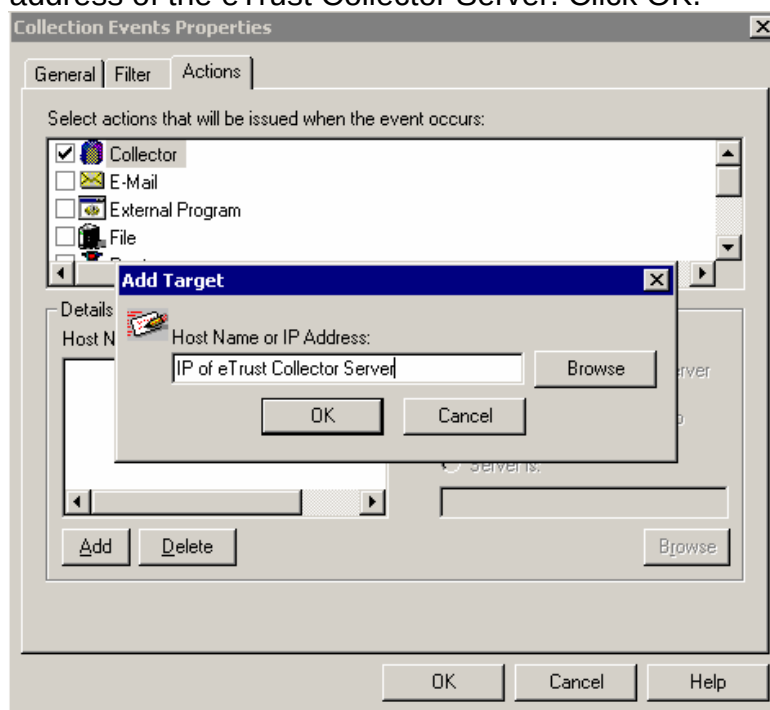
From the “Actions” tab, check the “Collector” box and click on “Add”. Enter the IP address of the eTrust Collector Server. Click OK.



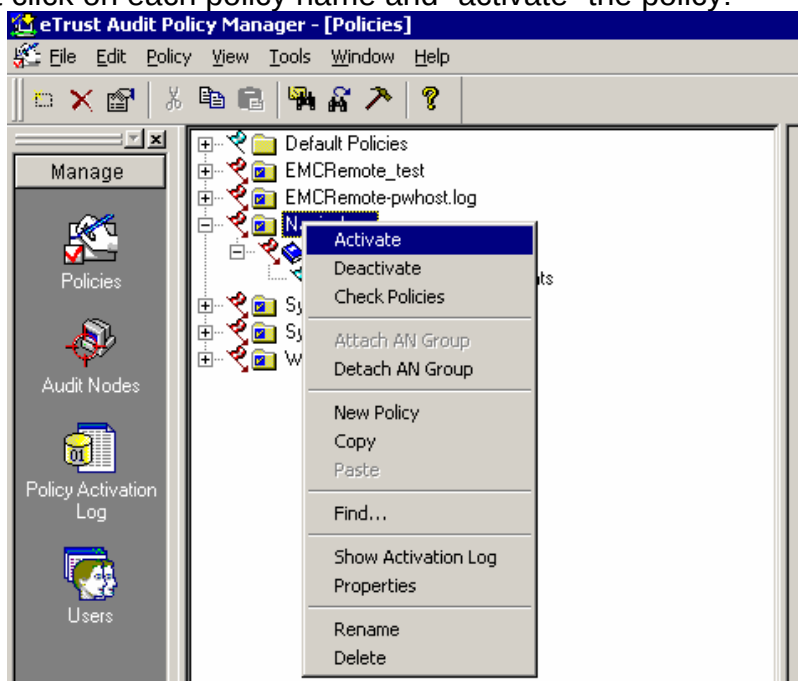
5. For the SymmWin_Symm5 policy, click on the “Filter” tab and add the following entries, then click “OK”.



From the “Actions” tab, check the “Collector” box and click on “Add”. Enter the IP address of the eTrust Collector Server. Click OK.

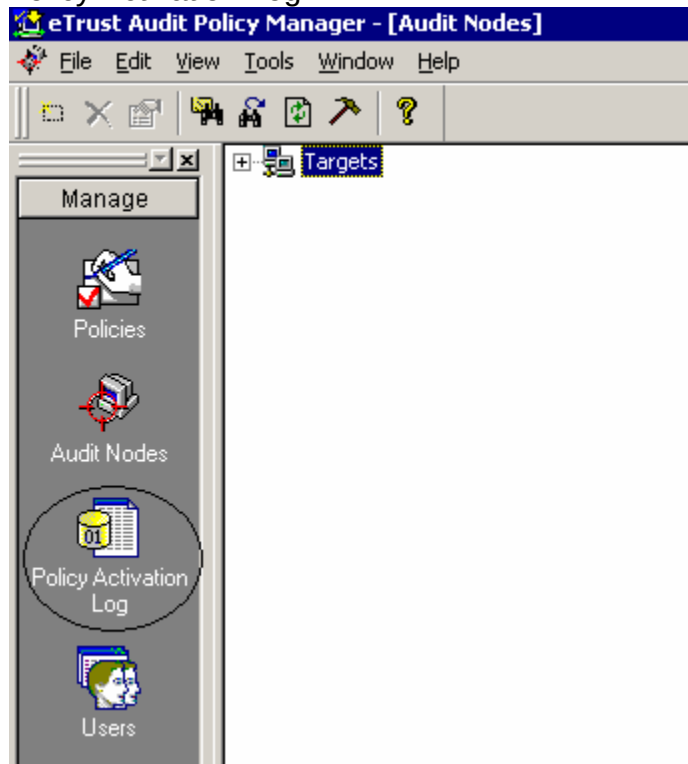


6. Right click on each policy name and “activate” the policy:



Verify Policy Activation:

7. Click on Policy Activation Log



8. Check to make sure the policies distributed successfully to all the clients.

Time	AN Name	Policy Name	Type	Message Text
07/22/2005 08:07:05 AM	SymmWin@192.168.93.202	SymmWin	Policy application	Policy was successfully distributed to the AN.
07/22/2005 08:07:05 AM	SymmWin@192.168.93.202	SymmWin	Policy application	Policy was successfully applied to the AN.
07/22/2005 08:06:57 AM	SymmWin@192.168.93.202	SymmWin	Policy application	Distribution command will be sent
07/21/2005 02:08:14 PM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy application	Policy was successfully applied to the AN.
07/21/2005 02:08:14 PM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy application	Policy was successfully distributed to the AN.
07/21/2005 02:08:07 PM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy application	Distribution command will be sent
07/21/2005 02:07:43 PM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy removing	Policy was successfully removed from the AN.
07/21/2005 02:07:43 PM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy removing	Policy was successfully distributed to the AN.
07/21/2005 09:37:42 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Policy was successfully applied to the AN.
07/21/2005 09:37:42 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Policy was successfully distributed to the AN.
07/21/2005 09:37:31 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Distribution command will be sent
07/21/2005 09:37:31 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Policy was successfully applied to the AN.
07/21/2005 09:37:31 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Policy was successfully distributed to the AN.
07/21/2005 09:37:21 AM	EMCRemote_test@192.168.93.202	EMCRemote_test	Policy application	Distribution command will be sent
07/21/2005 09:36:51 AM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy removing	Policy was successfully removed from the AN.
07/21/2005 09:36:51 AM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy removing	Policy was successfully distributed to the AN.
07/20/2005 05:28:23 PM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy application	Policy was successfully applied to the AN.
07/20/2005 05:28:23 PM	EMCRemote@192.168.93.202	EMCRemote-pwghost.log	Policy application	Policy was successfully distributed to the AN.

9. Appendix A: Firewall Ports

For the eTrust Audit client to communicate with the collector database through a firewall the following TCP and UDP ports are required to be open.

TCP Ports: 8025

UDP Ports: 8024, 8026, 8028 and 8030

10. Appendix B: CLARiiON Log Processing (Navisphere)

Monitoring of CLARiiON arrays is accomplished via a Navisphere Manager server. The following information is required:

- Name and IP addresses of storage arrays (will be used in the scripts)
- Location and name of the log files.
- Message Parsing file (Navisphere.mp).

10.1. CLARiiON Scripts

In order to generate log entries that can be sent to the eTrust logging system, the following scripts were implemented on a NAVICLI capable machine. This machine is typically the off-array management station. These scripts are designed to run on a Windows 2000/2003 platform.

Note: Enable "Windows Task Scheduler", if it's not enabled already.

Run_navi_logs.bat – main batch file for log processing
(schedule this script to run 1x / day)

```
@echo off
rem *****
rem * run_navi_logs.bat *
rem * Gary Johnson GDSE 04/08/05 *
rem * last updated: 06/08/05 GJ *
rem * *
rem * This batch file calls the main batch file navi_logs.bat and creates *
rem * a reused log file every time it run. *
rem * *
rem * It should be scheduled to repeat every 24 hours. *
rem * *
rem * Logs are circular files and are not cleared *
rem * *
rem * sample entry for AT: *
rem * at 07:15 /EVERY:M,t,w,th,f,s,su "c:\logs\batchjobs\run_navi_logs.bat" *
rem *****
@echo on
CALL "c:\logs\batchjobs\navi_logs.bat" > "c:\logs\batchjobs\navi_logs.log"
```

Navi_logs.bat – main logic loop for log processing

```
@echo off
rem *****
rem * navi_logs.bat *
rem * Gary Johnson GDSE 04/08/05 *
rem * last updated: 06/16/05 GJ *
rem * *
rem * This batch file pulls the log file from CX-series arrays *
rem * as defined in navi_logs.ini, stops and starts the eTrust process, *
rem * and renames the old file. It also calls utilities called fc and findstr *
rem * that provides etrust with the (difference) only new records since *
rem * the last pull and places it in the .log file. *
rem * *
rem * Logs on CLARiiON SP's are circular files and are not cleared *
rem * *
rem *****
@echo --begin processing-----
CALL net stop "eTrust Audit Generic Recorder"
```

```

SETLOCAL
FOR /F "eol=# tokens=1,2 delims=, " %i IN (c:\logs\batchjobs\navi_logs.ini) DO (
    @echo %j %i
    @echo filename will be: %j.new
    @echo copy old file to %j.old
    CALL copy c:\logs\%j.new c:\logs\%j.old
    @echo Pulling log from %j
    CALL navicli -h %i getlog > c:\logs\%j.new
    @echo creating difference file: %j.log
    CALL fc /L c:\logs\%j.old c:\logs\%j.new > c:\logs\%j.tmp
    CALL findstr /B "[0-9]" c:\logs\%j.tmp > c:\logs\%j.log
    @echo clean up temporary file
    CALL del c:\logs\%j.tmp
    @echo +++)
ENDLOCAL
CALL net start "eTrust Audit Generic Recorder"
@echo --end of processing----

```

Navi_logs.ini – definition file for list of arrays and ip addresses – include both SPs

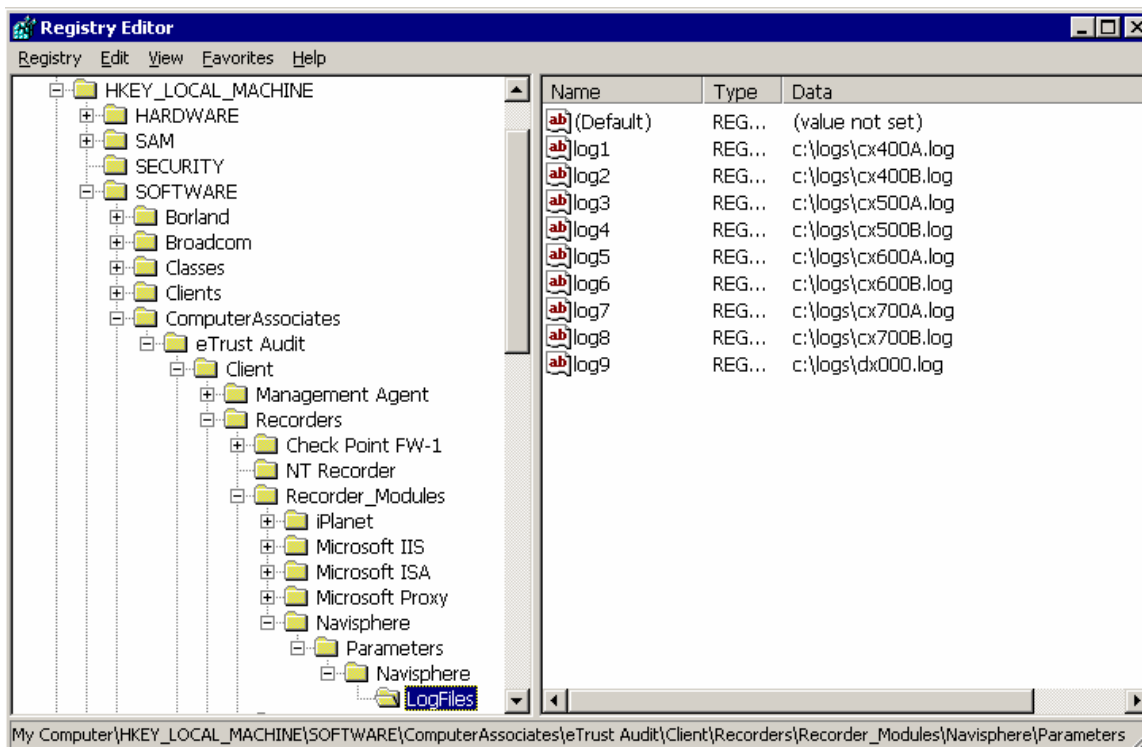
```

# *****
# * navi_logs.ini *
# * Gary Johnson GDSE 04/08/05 *
# * last updated: 06/08/05 GJ *
# * *
# * This is a configuration file for the automated pull *
# * of Navisphere activity logs from CX-series arrays. *
# * *
# * List ip addresses (SPA & SPB) of cx-series arrays,name of array *
# * 192.168.93.40,cx400 (example) *
# *****
192.168.93.40,cx400A
192.168.93.41,cx400B
192.168.93.60,cx600A
192.168.93.61,cx600B
192.168.93.30,cx500A
192.168.93.31,cx500B
192.168.93.70,cx700A
192.168.93.71,cx700B

```

10.2. CLARiiON SP Logs

The scripts run nightly to pull the log off of each SP and places the data in a log file in directory C:\logs\arrayname.log. The eTrust registry entries need to be updated with the location and name of each of these logs. There should be two logs for each array (one per SP). The log name should be the same name that was defined in the “Navi_logs.ini” file with a “.log” extension (file type). For example:

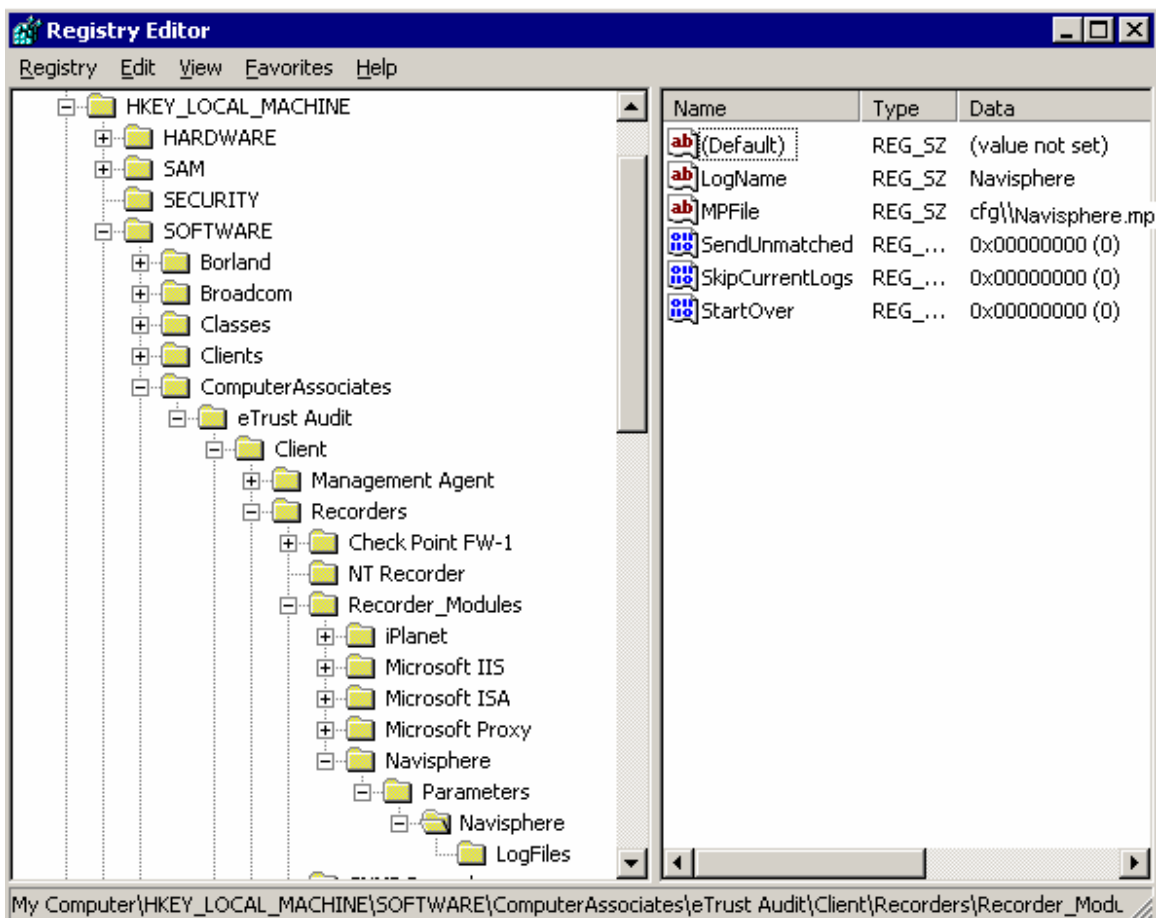


Any files listed in this area will be scanned for new entries on a frequent basis. If the file does not exist (i.e. wrong file name) an error in the windows application log will be generated and should be sent to the eTrust log.

Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for CLARiiON (Navisphere.mp):

```
; ini file for Navisphere Log
Tokens
{
    Date
    {
        Type = datetime
        Format = [0-9]*\[0-9]*\[0-9]* [0-9]*\:[0-9]*\:[0-9]*
        DateTimeFormat = %m/%d/%Y %T
    }
    Enclosure
    {
        format = [0-9]*
    }
    Disk
    {
        format = [0-9]*
    }
    SPS
    {
        format = [0-9A-Za-z]*
    }
    ErrorCode
    {
        format = [0-9a-zA-Z]*
    }
    Message1
    {
```

```

    format = [0-9a-zA-Z\ ]*
  }
  Info
  {
    format = .+
  }
  HexCode
  {
    format = [0-9a-fA-Fx]*
  }
}

TranslateTbl
{
}

Records
{
;
;
;Records
;*****;
;
;
; DiskEnclosure Messages
;
;
;
; 03/03/2004 08:19:25 Enclosure 1 Disk 13 (a07) CRU Powered Down [0x00] 0
920c
;
; DiskEnclosure_Message1
; {
;   Name = DiskEnclosure_Message1
;   KeyVal = 0
;   Type = RECORD
;   Regex = <Date> Enclosure <Enclosure> Disk <Disk>[ ]+[\(\]<ErrorCode>[\)] [ ]+<Info>[
]+[\<HexCode>\][ ]*<Code1>[ ]*<Code2><_rest>
;   Key = DiskEnclosure_Message1
;   ReplaceSpace = TRUE
;   AddToken1 = Category:Clariion
;   AddToken2 = Log:Navisphere
;   AddToken3 = Taxonomy:
;   AddToken4 = Status:S
;   AddToken5 = EventCategory:DiskEnclosure1
;   <Code1> = <ErrorCode>
;   <Code2> = <ErrorCode>
; }
;
; 03/03/2004 08:19:26 Enclosure 0 SPS B (90d) SPS Removed [0x00] 0
20000
;
; DiskEnclosure_Message2
; {
;   Name = DiskEnclosure_Message2
;   KeyVal = 0
;   Type = RECORD
;   Regex = <Date> Enclosure <Enclosure> SPS <SPS>[ ]+[\(\]<ErrorCode>[\)] [ ]+<Info>[
]+[\<HexCode>\][ ]*<Code1>[ ]*<Code2><_rest>
;   Key = DiskEnclosure_Message2
;   ReplaceSpace = TRUE
;   AddToken1 = Category:Clariion
;   AddToken2 = Log:Navisphere
;   AddToken3 = Taxonomy:
;   AddToken4 = Status:S
;   AddToken5 = EventCategory:DiskEnclosure2
;   <Code1> = <ErrorCode>
;   <Code2> = <ErrorCode>
; }
;
;
;
; Basic2
{

```

```
Name = Basic_Message2
KeyVal = 0
Type = RECORD
Regex = <Date><Message1>[\\(<ErrorCode>\\)]<Info><_rest>
Key = Basic_Message
ReplaceSpace = TRUE
AddToken1 = Category:Clariion
AddToken2 = Log:Navisphere
AddToken3 = Taxonomy:
AddToken4 = Status:S
}
Basic
{
  Name = Basic_Message
  KeyVal = 0
  Type = RECORD
  Regex = <Date>[ ]+[\\(<ErrorCode>\\)]<Info><_rest>
  Key = Basic_Message
  ReplaceSpace = TRUE
  AddToken1 = Category:Clariion
  AddToken2 = Log:Navisphere
  AddToken3 = Taxonomy:
  AddToken4 = Status:S
}
;
; Records
;*****;
;
}
```

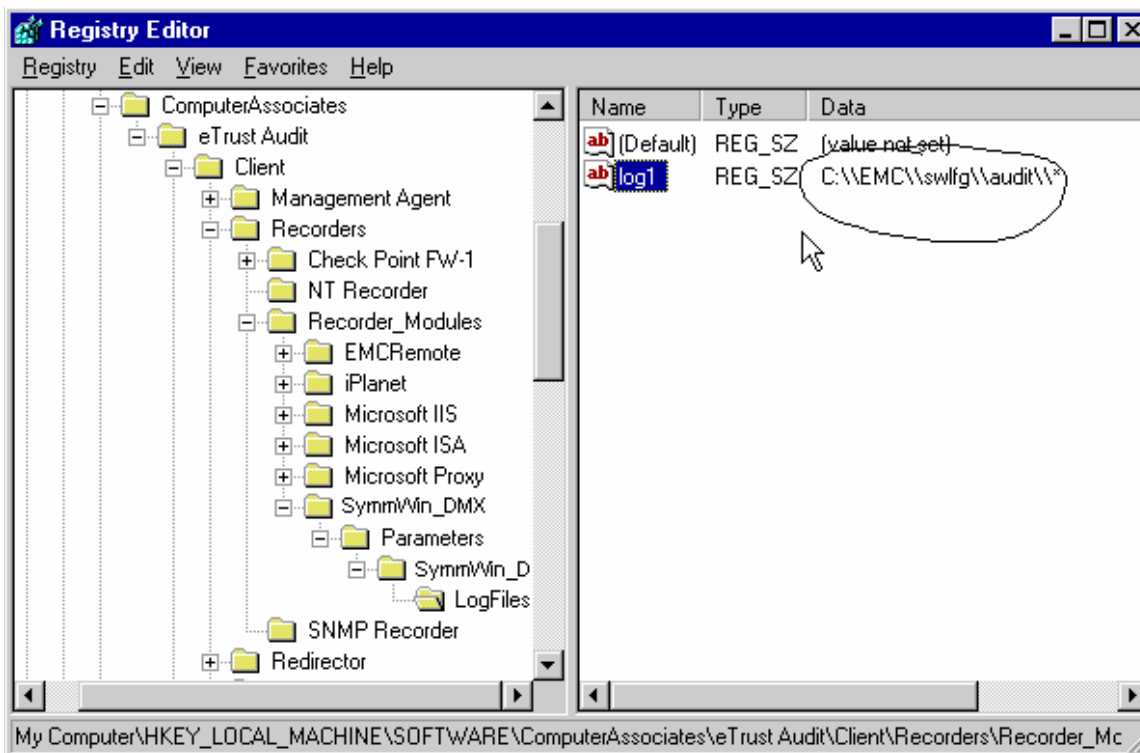
11. Appendix C: EMC Log Processing (performed by EMC)

11.1. DMX Configuration

11.1.1. Log Pull Program

The EMC Log Pull program (swlfg.exe) will be installed by EMC on the DMX service processors. This program will extract data from the SymmWin log and place it in a format that eTrust can read. The program is located in directory: C:\EMC\swlfg. The logs that it generates are located in directory: C:\EMC\swlfg\audit under filenames: logall_dateyymmdd_timexxxxxx.log.

The eTrust registry entry needs to be updated with the location of this file. If the log file locations were specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.

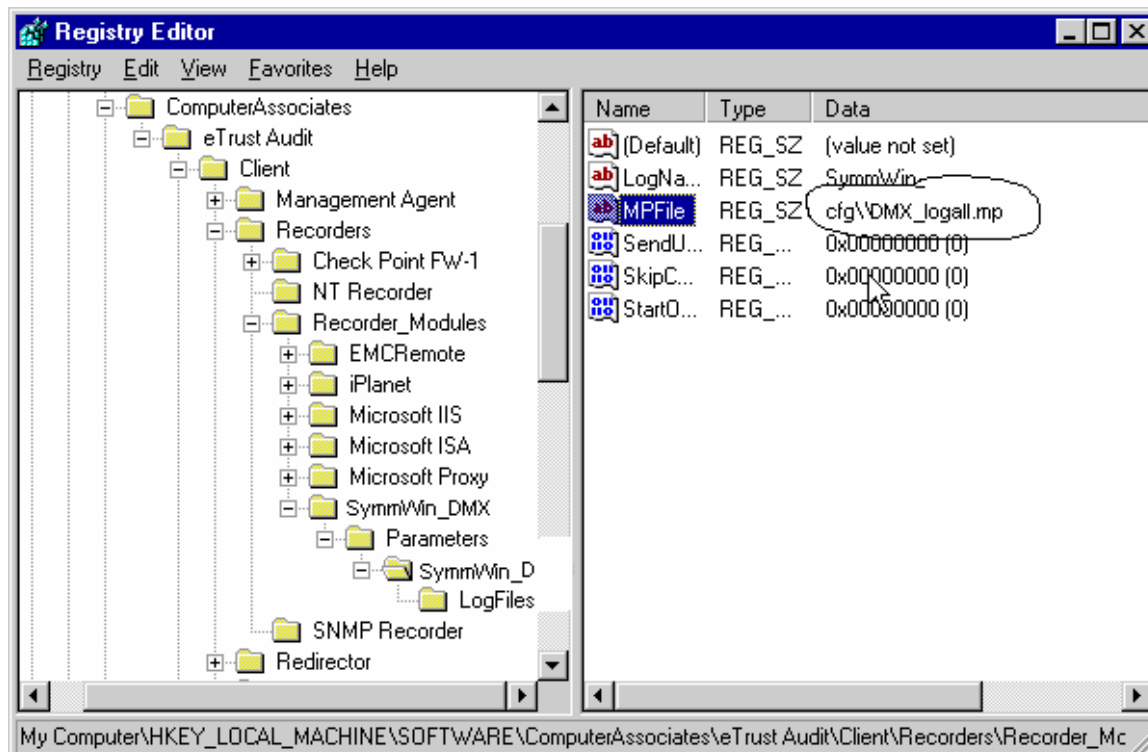


Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this

file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for DMX (DMX_logall.mp):

```
; ini file for the EMC Log
Tokens
{
  Date
  {
    Type = datetime
    Format = [0-9]*\[0-9]*\[0-9]* [0-9]*\:[0-9]*\:[0-9]*
    DateTimeFormat = %m/%d/%Y %T
  }
  System
  {
    format = [a-zA-Z0-9]*
  }
  Facility
  {
    format = \[[a-zA-Z0-9]+\]
  }
  <Message> = <_rest>
}

TranslateTbl
{
}

Records
{

;Categories
;*****;
```

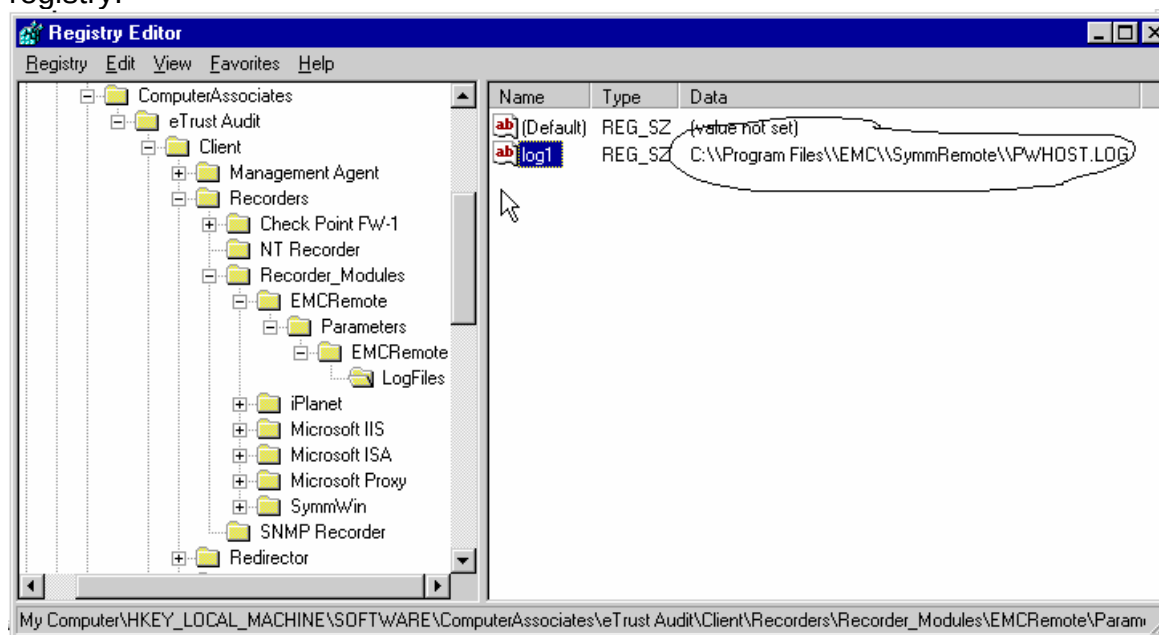
```

;BasicMessage
{
  Basic
  {
    Name = Basic_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = .. <Date> <System> <_rest>
    Key = Basic_Message
    ReplaceSpace = TRUE
  }
;
; Records
;*****;
;
; Basic_Record
{
  Name = Basic_Record
  KeyVal = Basic_Message
  Type = RECORD
  Regex = <Facility> <Message>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:EMC
  AddToken2 = Log:SymmWin_DMx
  AddToken6 = Taxonomy:
  AddToken7 = Status:S
}
}

```

11.1.2. EMCRemote

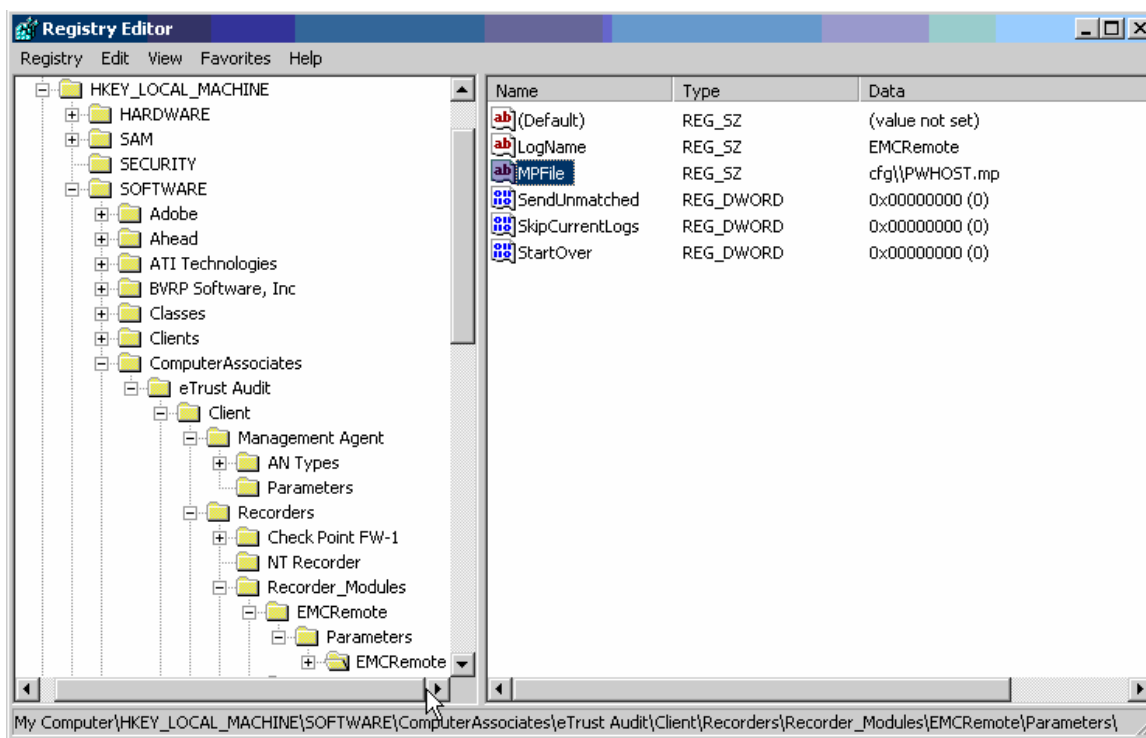
Remote access to the EMC storage array is accomplished using EMCRemote. It has a log file (PWHOST.log) that logs successful and unsuccessful attempts to access the storage array. The eTrust registry entry needs to be updated with the location of this file. If the log file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for EMCRemote (PWHOST.mp):

```
; ini file for PWHOST Log
Tokens
{
  Date
  {
    Type = datetime
    Format = [0-9]*\/[0-9]*\/[0-9]* [0-9]*\:[0-9]*\:[0-9]* [A-Z]*
    DateTimeFormat = %m/%d/%Y %I:%M:%S %p
  }
  Message
  {
    format = [a-zA-Z0-9\.\'\ \" ]*
  }
  Divide
  {
    format = [\/]
  }
}
```

```

    }
    DivideMessage
    {
        format = [\/]*
    }
}

TranslateTbl
{
}

Records
{

;Categories
;*****;

;BasicMessage
Basic
{
    Name = Basic_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = <Date> <_rest>
    Key = Basic_Message
    ReplaceSpace = TRUE
}
Divider
{
    Name = Divider_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = <Divide><_rest>
    Key = Divide_Message
    ReplaceSpace = TRUE
}
;
; Records
;*****;
;
Basic_Record
{
    Name = Basic_Record
    KeyVal = Basic_Message
    Type = RECORD
    Regex = <Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
Divide_Record
{
    Name = Divide_Record
    KeyVal = Divide_Message
    Type = RECORD
    Regex = <Divide_Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
}

```

11.1.3. Private Wire (Firewall Software)

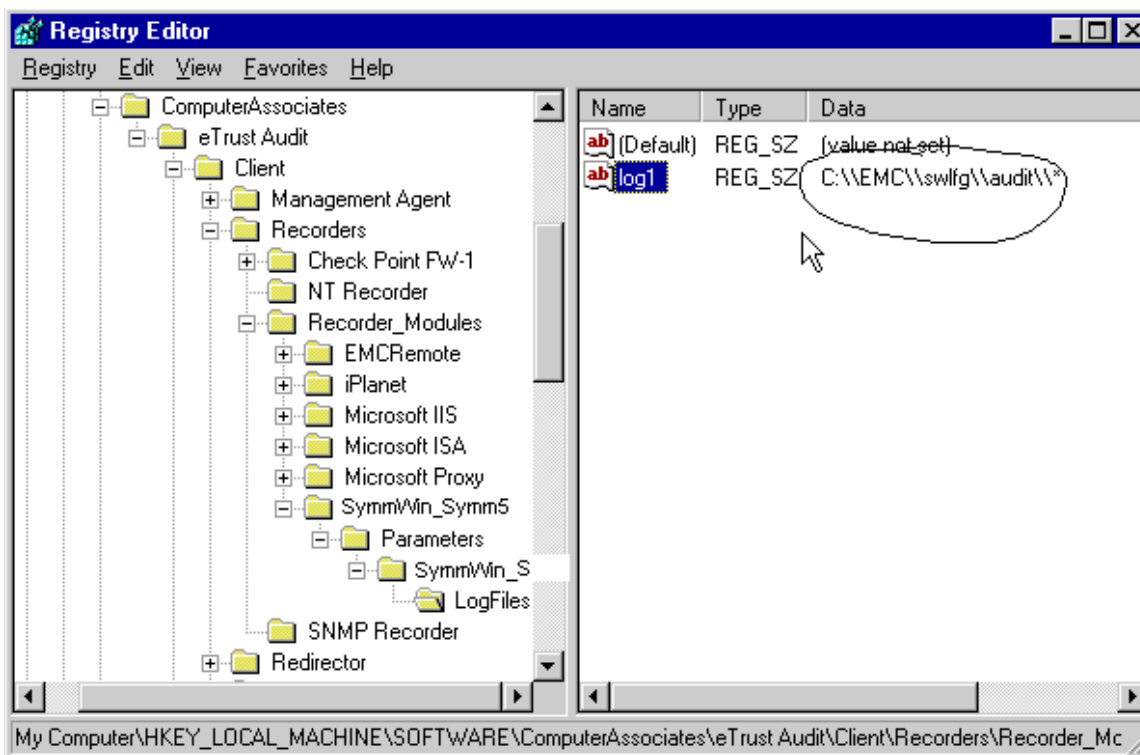
EMC will configure the firewall software on the DMX to allow eTrust traffic. Ports are listed in Appendix A.

11.2. Symm5 Configuration

11.2.1. Log Pull Program

The EMC Log Pull program (swlfg.exe) will be installed by EMC on the DMX service processors. This program will extract data from the SymmWin log and place it in a format that eTrust can read. The program is located in directory: C:\EMC\swlfg. The logs that it generates are located in directory: C:\EMC\swlfg\audit under filenames: logall_dateymmdd_timexxxxxx.log.

The eTrust registry entry needs to be updated with the location of this file. If the log file locations were specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.

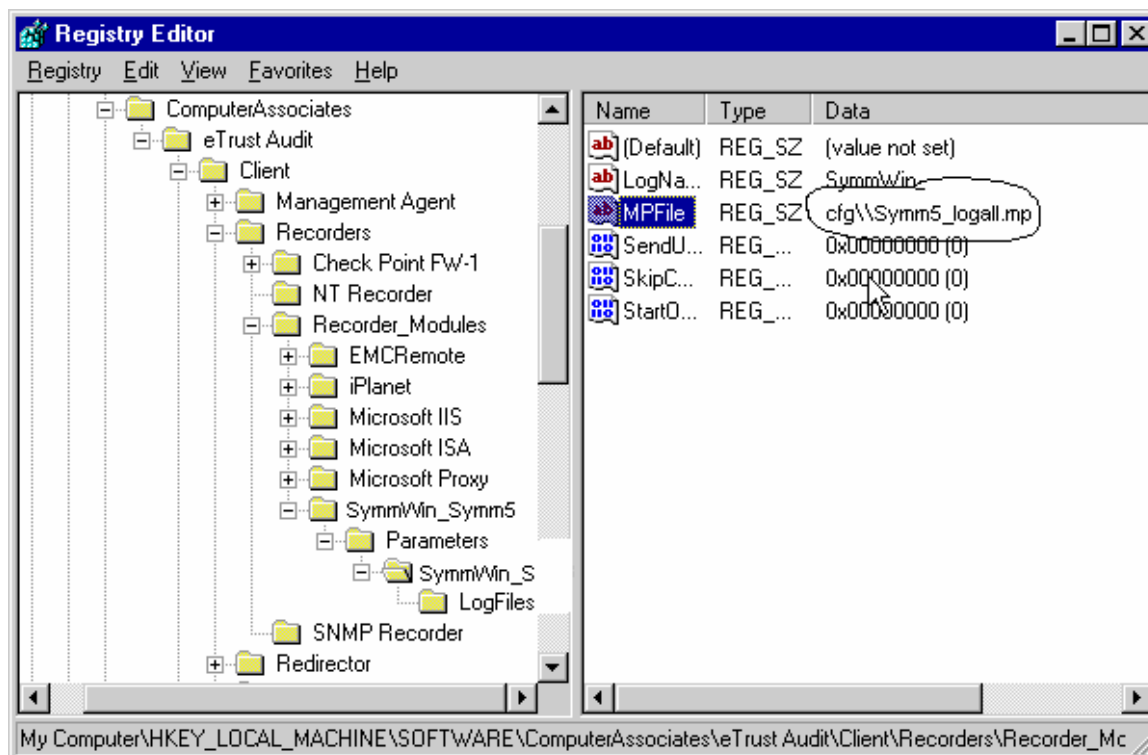


Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records,

before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for Symm5 (Symm5_logall.mp):

```
; ini file for the EMC Log
Tokens
{
  Date
  {
    Type = datetime
    Format = [0-9]*\[0-9]*\[0-9]* [0-9]*\[0-9]*\[0-9]*
    DateTimeFormat = %m/%d/%y %T
  }
  Facility
  {
    format = \[[a-zA-Z0-9]+\]
  }
  <Message> = <_rest>
}

TranslateTbl
{
}

Records
{

}

;Categories
```

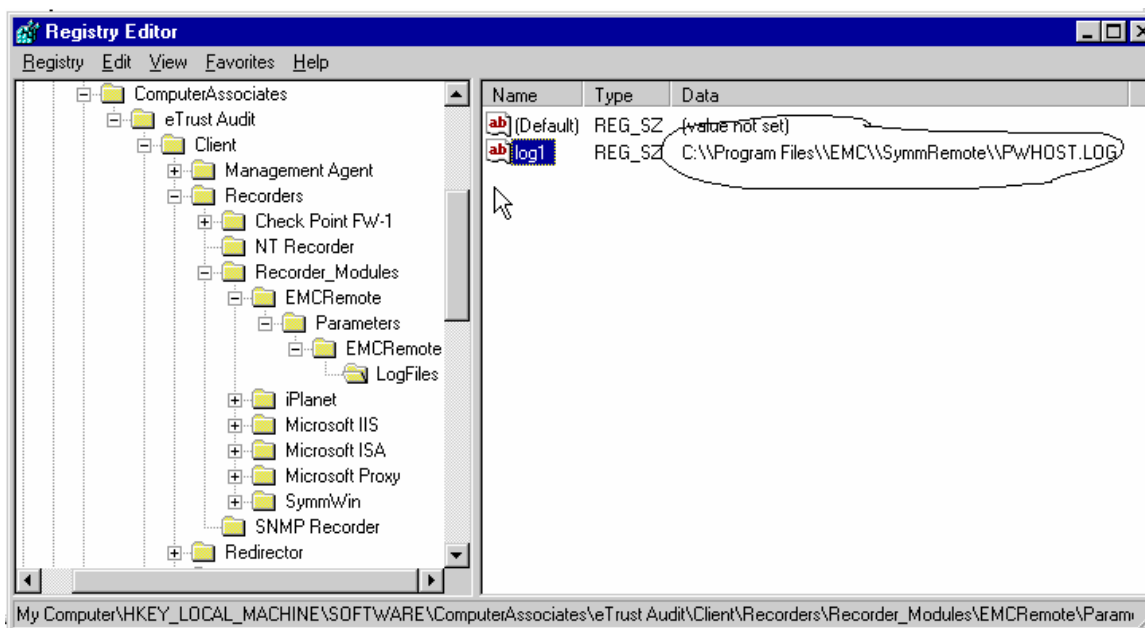
```

;*****;
;
;BasicMessage
;  Basic
;  {
;    Name = Basic_Message
;    KeyVal = 0
;    Type = CATEGORY
;    Regex = <Date><_rest>
;    Key = Basic_Message
;    ReplaceSpace = TRUE
;  }
;
; Records
;*****;
;
;Basic_Record
;  {
;    Name = Basic_Record
;    KeyVal = Basic_Message
;    Type = RECORD
;    Regex = <Facility> <Message>
;    Key =
;    ReplaceSpace = TRUE
;    AddToken1 = Category:EMC
;    AddToken2 = Log:SymmWin_Symm5
;    AddToken6 = Taxonomy:
;    AddToken7 = Status:S
;  }
;
;Default_Record
;  {
;    Name = Default_Record
;    KeyVal = Basic_Message
;    Type = RECORD
;    Regex = <Message>
;    Key =
;    ReplaceSpace = TRUE
;    AddToken1 = Category:EMC
;    AddToken2 = Log:SymmWin_Symm5
;    AddToken6 = Taxonomy:
;    AddToken7 = Status:S
;  }
;
}

```

11.2.2. EMCRemote

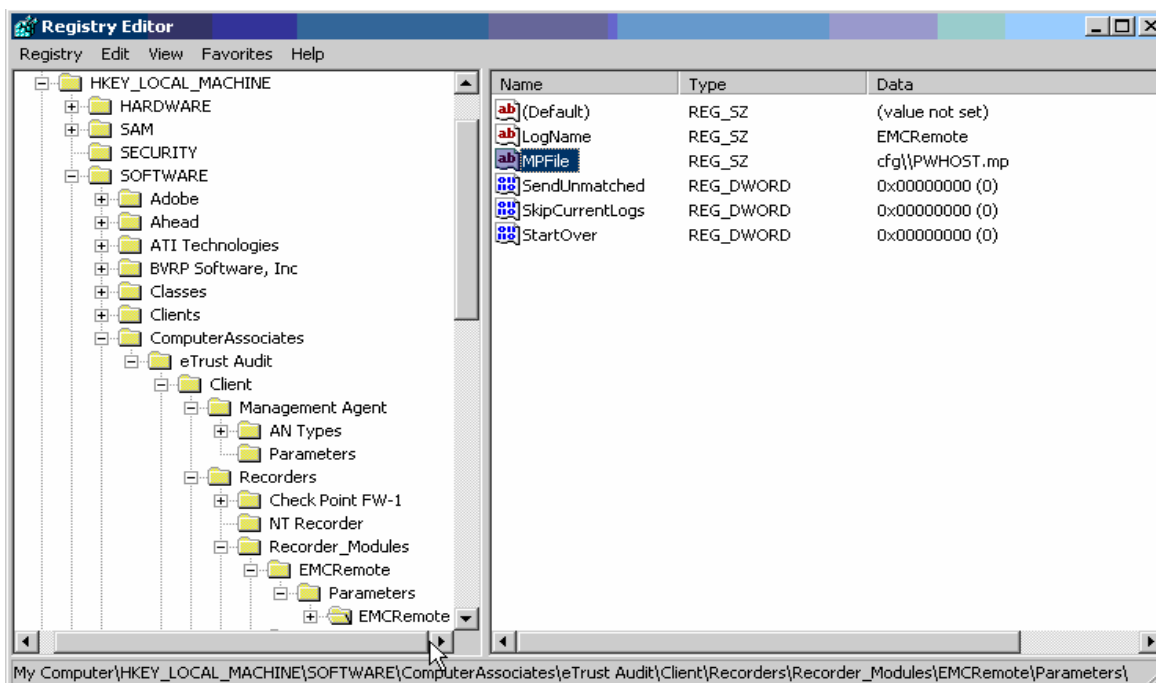
Remote access to the EMC storage array is accomplished using EMCRemote. It has a log file (PWHOST.log) that logs successful and unsuccessful attempts to access the storage array. The eTrust registry entry needs to be updated with the location of this file. If the log file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for EMCRemote (PWHOST.mp):

```
; ini file for PWHOST Log
Tokens
{
    Date
    {
        Type = datetime
        Format = [0-9]*\[0-9]*\[0-9]* [0-9]*\:[0-9]*\[0-9]* [A-Z]*
        DateTimeFormat = %m/%d/%Y %I:%M:%S %p
    }
    Message
    {
        format = [a-zA-Z0-9\.\'\\" ]*
    }
    Divide
    {
        format = [\\/]
    }
    DivideMessage
    {
        format = [\\/]
    }
}

TranslateTbl
{
}

Records
{

;Categories
;*****;

;BasicMessage
Basic
{
    Name = Basic_Message
    KeyVal = 0
}
```

```

    Type = CATEGORY
    Regex = <Date> <_rest>
    Key = Basic_Message
    ReplaceSpace = TRUE
}
Divider
{
    Name = Divider_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = <Divide><_rest>
    Key = Divide_Message
    ReplaceSpace = TRUE
}
;
; Records
;*****;
;
Basic_Record
{
    Name = Basic_Record
    KeyVal = Basic_Message
    Type = RECORD
    Regex = <Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
Divide_Record
{
    Name = Divide_Record
    KeyVal = Divide_Message
    Type = RECORD
    Regex = <Divide_Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
}

```

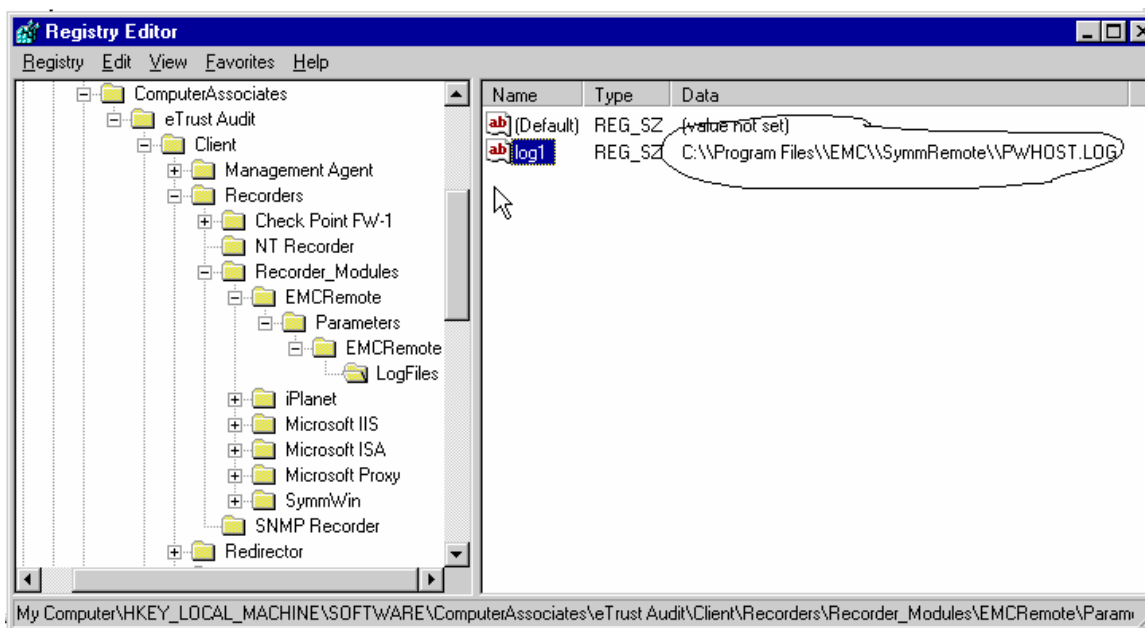
11.2.3. Private Wire (Firewall Software)

EMC will configure the firewall software on the DMX to allow eTrust traffic.

12. Appendix D: Connectrix Log Processing *(performed by EMC)*

12.1. EMCRemote

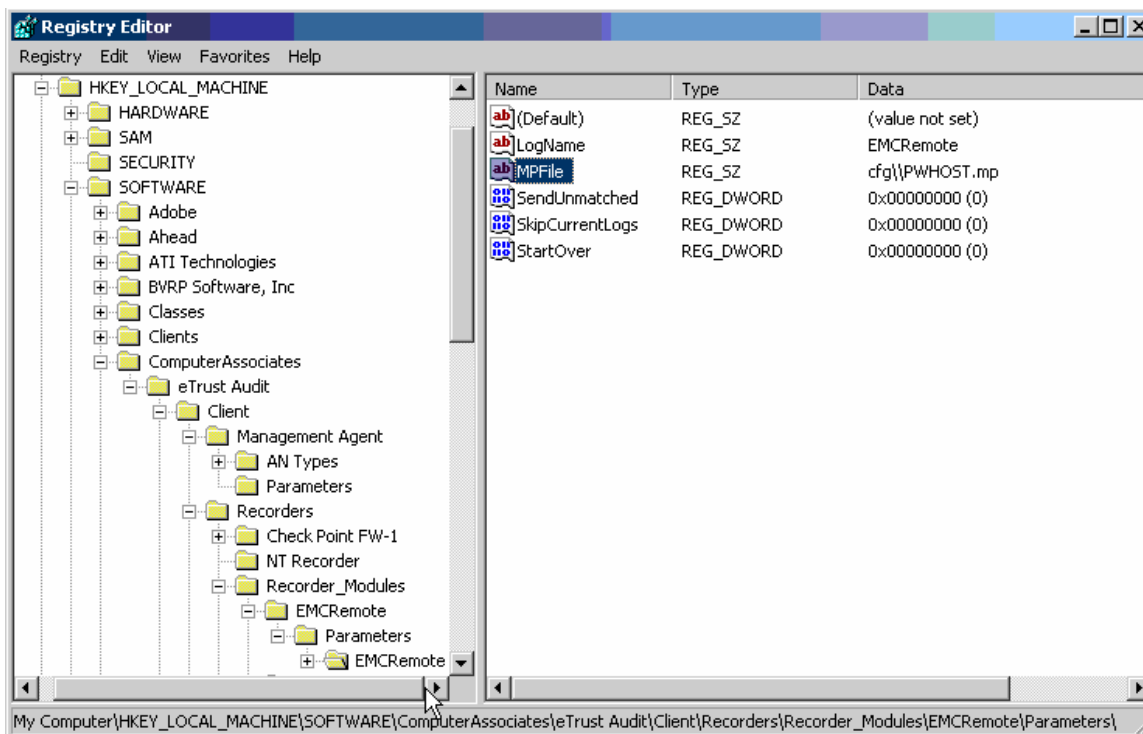
Remote access to the EMC storage array is accomplished using EMCRemote. It has a log file (PWHOST.log) that logs successful and unsuccessful attempts to access the storage array. The eTrust registry entry needs to be updated with the location of this file. If the log file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.



Message Parsing File for EMCRemote (PWHOST.mp):

```
; ini file for PWHOST Log
Tokens
{
    Date
    {
        Type = datetime
        Format = [0-9]*\[0-9]*\[0-9]* [0-9]*\:[0-9]*\:[0-9]* [A-Z]*
        DateTimeFormat = %m/%d/%Y %I:%M:%S %p
    }
    Message
    {
        format = [a-zA-Z0-9\.\'\ \ ]*
    }
    Divide
    {
        format = [\/]
    }
    DivideMessage
    {
        format = [\/]*
    }
}

TranslateTbl
{
}

Records
{

;Categories
;*****;

;BasicMessage
    Basic
    {
```

```

    Name = Basic_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = <Date> <_rest>
    Key = Basic_Message
    ReplaceSpace = TRUE
}
Divider
{
    Name = Divider_Message
    KeyVal = 0
    Type = CATEGORY
    Regex = <Divide><_rest>
    Key = Divide_Message
    ReplaceSpace = TRUE
}
;
; Records
;*****;
;
Basic_Record
{
    Name = Basic_Record
    KeyVal = Basic_Message
    Type = RECORD
    Regex = <Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
Divide_Record
{
    Name = Divide_Record
    KeyVal = Divide_Message
    Type = RECORD
    Regex = <Divide_Message>
    Key =
    ReplaceSpace = TRUE
    AddToken1 = Category:Process
    AddToken2 = Log:EMCRemote
    AddToken6 = Taxonomy:
    AddToken7 = Status:S
}
}

```

13. Appendix E: HDS USP Log Processing

There are two methods of monitoring for the HDS USP Array. These two methods are HDS Device Manager monitoring and USP Array monitoring. To fully capture all of the audit events, both must be configured.

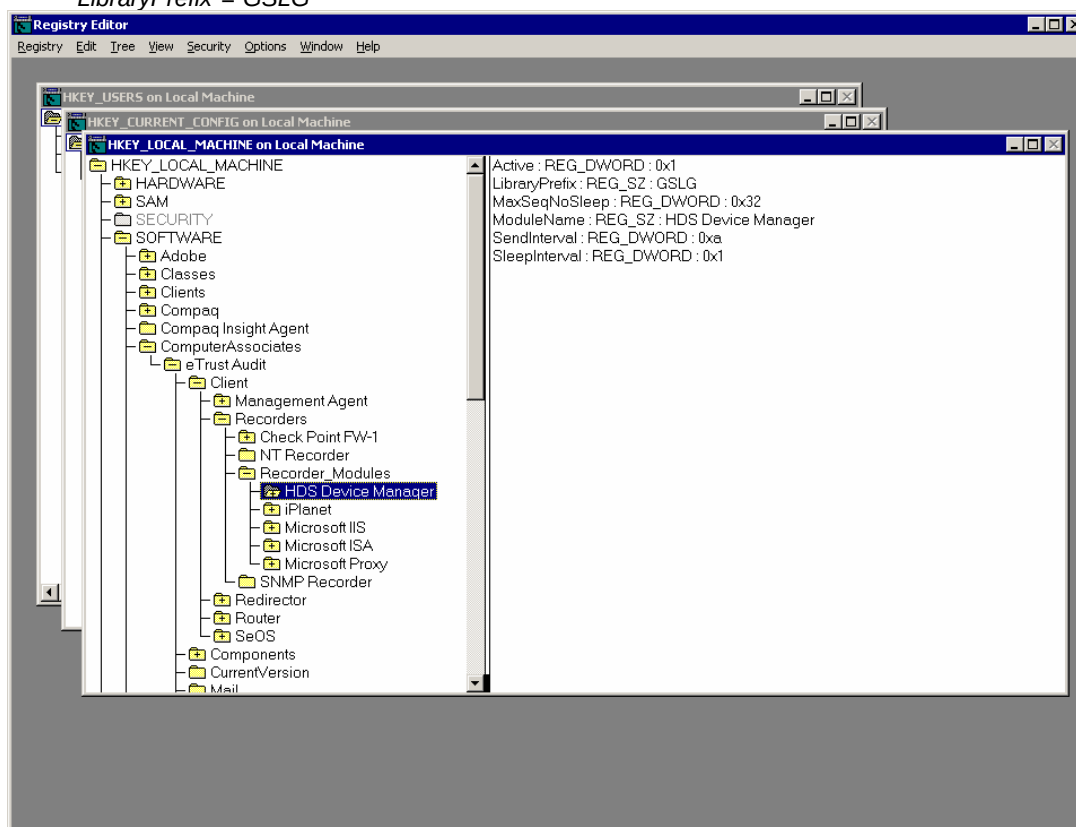
13.1. Device Manager Monitoring

HDS Device Manager is typically installed on a windows based machine. Set up of the windows agent is described earlier in this document.

Device Manager has a log file (service.log) that logs major function calls and events within Device Manager against the storage array. The eTrust registry entry needs to be updated with the location of this file. If the log file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry. Under normal circumstances, you have no reason to change these registry entries.

To validate the installation, check following registry settings:

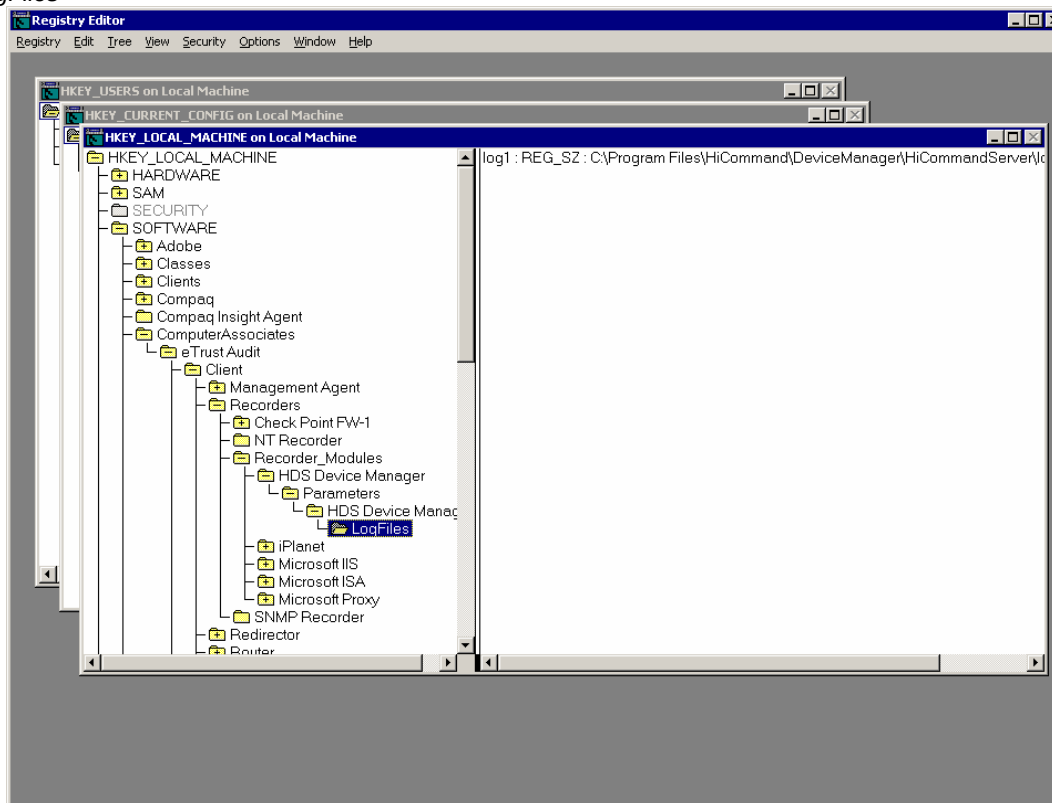
*HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Trust
Audit\Client\Recorders\Recorder_Modules\HDS Device Manager*
"Active"=dword:00000001
"LibraryPrefix"="GSLG"



To change log file name or to add more log files change following registry setting:

*HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Trust
Audit\Client\Recorders\Recorder_Modules\HDS Device Manager\Parameters\HDS Device Manager*

LogFiles



The default location to the Device Manager log file is:

C:\Program Files\HiCommand\DeviceManager\HiCommandServer\logs\service.log

The message-parsing file for Device Manager is described in [Message Parsing File for Device Manager](#).

13.2. Array Audit Log Monitoring (Syslog)

The HDS USP array should be configured to send its audit log to a syslog server. The procedure for this is described in the [HDS USP Array Solutions Guide](#).

Once the audit records are being sent to a syslog server, the generic recorder on the syslog server must be configured to accommodate a new message parsing file (MP). Installation of the HDS Syslog Recorder requires modifications in pre installed "Recorder.ini" file. This only applies to Solaris servers running the eTrust client.

The recorder.ini file (/export/opt/CAaudclnt/ini/) will need an entry for HDSNavigator added (see **red** text):

```
Recorder_Modules
{
  File Spooler
  {
    ModuleName = syslog
    LibraryPrefix = GSLG
    DWORD:Active = 1
```

```

DWORD:SleepInterval = 1
DWORD:SendInterval = 10
DWORD:MaxSeqNoSleep = 50
Parameters
{
    DatFilePath = dat/recorders/syslog.dat
    DWORD:MPDebug = 1
    Syslog
    {
        LogName = Unix
        DWORD:StartOver = 0
        DWORD:ReloadLogs = 0
        DWORD:SendUnmatched = 0
        DWORD:SkipCurrentLogs = 0
        MPFile = cfg/syslog.mp
        ConfigFile = /etc/syslog.conf
        DWORD:Source = 1
        LogFiles
        {
            ;
        }
    }
    su
    {
        LogName = Unix
        DWORD:StartOver = 0
        DWORD:ReloadLogs = 0
        DWORD:SendUnmatched = 0
        DWORD:SkipCurrentLogs = 0
        MPFile = cfg/sulog.mp
        LogFiles
        {
            log1 = /var/log/sulog
        }
    }
}
HDSNavigator
{
    LogName = HDSStorageNav
    DWORD:StartOver = 0
    DWORD:ReloadLogs = 0
    DWORD:SendUnmatched = 0
    DWORD:SkipCurrentLogs = 0
    MPFile = cfg/HDSStorageNav.mp
    LogFiles
    {
        log1 = /var/adm/HDS_messages
    }
}
}
Apache
{
    ModuleName = Apache
    LibraryPrefix = GSLG
    DWORD:Active = 0
    DWORD:SleepInterval = 1
    DWORD:SendInterval = 10
    DWORD:MaxSeqNoSleep = 50
    Parameters
    {
        DatFilePath = dat/recorders/apache.dat
        DWORD:MPDebug = 1
        Apache
        {
            LogName = Apache
            DWORD:StartOver = 0
            DWORD:ReloadLogs = 0
            DWORD:SendUnmatched = 0
            DWORD:SkipCurrentLogs = 0
            MPFile = cfg/Apache.mp
        }
    }
}

```

```

        LogFiles
        {
            ;
        }
    }
}
Oracle
{
    ModuleName = oracle
    LibraryPrefix = ORMD
    DWORD:Active = 0
    DWORD:SleepInterval = 1
    DWORD:SendInterval = 10
    DWORD:MaxSeqNoSleep = 50
    ORACLE_HOME =
    Parameters
    {
        ORACLE_SID =
        TWO_TASK =
        MPFile = cfg/oracle.mp
        DatFilePath = dat/recorders/oracle.dat
        BINARY:Password = $(ORACLE_PASSWORD)
        BINARY:Username = $(ORACLE_USER)
    }
}
Netscape
{
    ModuleName = netscape
    LibraryPrefix = GSLG
    DWORD:Active = 0
    DWORD:SleepInterval = 1
    DWORD:SendInterval = 10
    DWORD:MaxSeqNoSleep = 50
    Parameters
    {
        DatFilePath = dat/recorders/netscape.dat
        DWORD:MPDebug =
        Netscape
        {
            LogName = Netscape
            DWORD:StartOver = 0
            DWORD:ReloadLogs = 0
            DWORD:SendUnmatched = 0
            DWORD:SkipCurrentLogs = 0
            MPFile = cfg/netscape.mp
            LogFiles
            {
                ;
            }
        }
    }
}
}

```

The message parsing file is described in [Message Parsing File for Array Audit Log \(Syslog\)](#).

It is important to create the file `/var/adm/HDS_messages`. This can be any blank file. The SA should set up any file handling such that this file does not become too large or difficult to manage. The `syslog.conf` describes the name and location of this file. Additional scripting may be required for file handling of older copies.

The syslog.conf (/etc/syslog.conf) file should be configured to accommodate the HDS syslog messages (user.info messages). A sample modified excerpt is shown below:

```
#Start of HDS Syslog modification
user.info                                /var/adm/HDS_messages
#End of HDS Syslog modificationRecorder_Modules
```

On the Citigroup SOE build for Solaris systems, the syslog daemon needs to be configured to receive external logging (on port 514). In order to turn this feature back on, the syslog daemon (/etc/syslog/init.d/syslog) needs to be modified to remove the “- t” option from the syslogd command. A sample modified lines is shown below.

```
#!/sbin/sh
#
# Copyright (c) 1991-1999 by Sun Microsystems, Inc.
# All rights reserved.
#
#ident "@(#)syslog      1.13      99/09/06 SMI"
#
# Changed call to syslogd from /usr/sbin/syslogd -t to /usr/sbin/syslog
# to allow for remote messages to be sent to syslog.

case "$1" in
'start')
    if [ -f /etc/syslog.conf -a -f /usr/sbin/syslogd ]; then
        echo 'syslog service starting.'
        #
        # Before syslogd starts, save any messages from previous
        # crash dumps so that messages appear in chronological order.
        #
        /usr/bin/savecore -m
        if [ -r /etc/dumpadm.conf ]; then
            . /etc/dumpadm.conf
            [ "x$DUMPADM_DEVICE" != xswap ] && \
                /usr/bin/savecore -m -f $DUMPADM_DEVICE
        fi
        if [ ! -f /var/adm/messages ]; then
            /usr/bin/cp /dev/null /var/adm/messages
            /usr/bin/chmod 0644 /var/adm/messages
        fi
        /usr/sbin/syslogd >/dev/msglog 2>&1 &
    fi
    ;;
'stop')
    if [ -f /etc/syslog.pid ]; then
        syspid=`/usr/bin/cat /etc/syslog.pid`
        [ "$syspid" -gt 0 ] && kill -15 $syspid
    fi
    ;;
*)
    echo "Usage: $0 { start | stop }"
    exit 1
    ;;
esac
```

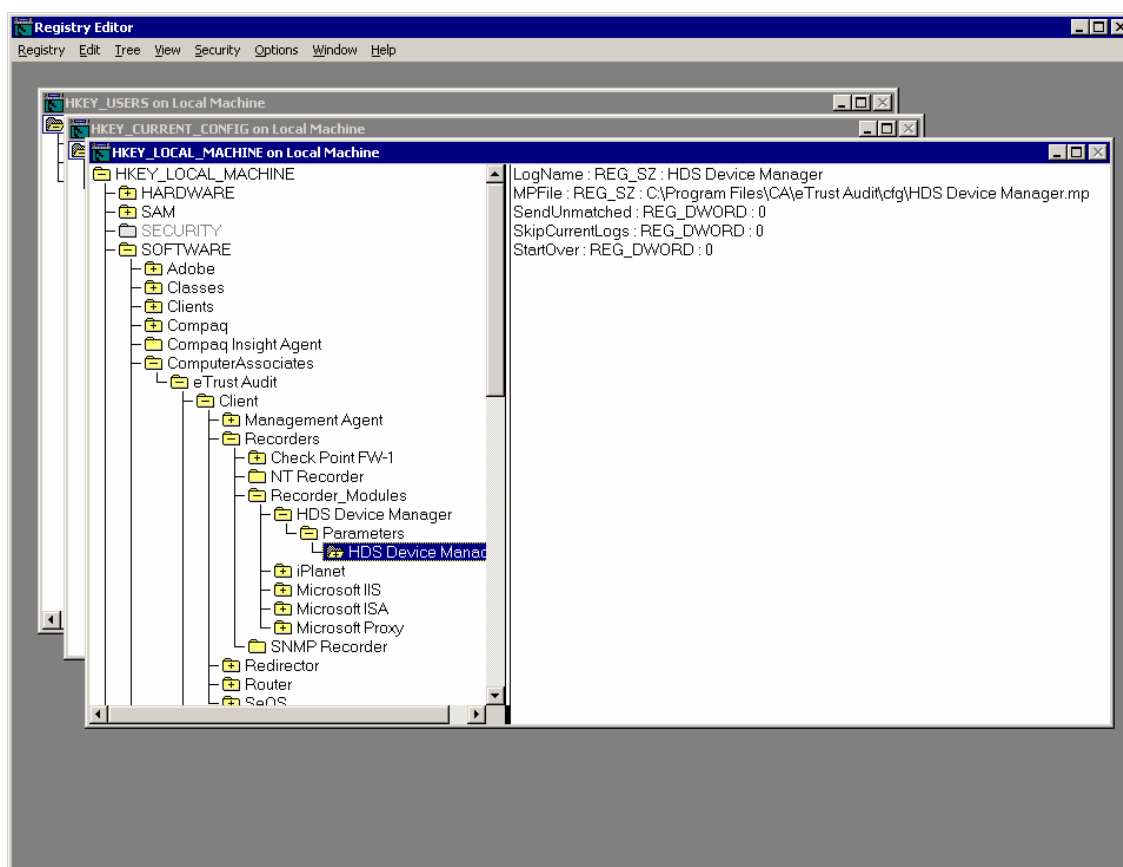
13.3. Message Parsing File for Device Manager

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these

records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The message-parsing file needs to be copied to C:\Program Files\CA\eTrust Audit\cfg. The eTrust registry entry needs to be updated with the location of this file. If the MP file location was specified during the install of eTrust Client, then you will not have to update the registry. Verify by checking the registry.

HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\eTrust Audit\Client\Recorders\Recorder_Modules\HDS Device Manager\Parameters\HDS Device Manager\MPFile= C:\Program Files\CA\eTrust Audit\cfg\HDSDevManager.mp



Sample Message Parsing File for HDS Device Manager (HDSDevManager.mp) that should reside in \Program Files\CA\eTrust Audit\cfg\

```

*****
;Project : eTrust Audit 1.5 SP3
;Module : HDS Device Manager Version 4.x, tested up to DM V5.5
;File : DevManager.mp
;Purpose :Message parsing file
*****
;Developed By : Kery Hines
;Modified By : Kery Hines Feb 23, 2007
*****
;
;
;-----

```

```

Tokens
{
  Date
  {
    Type = datetime
    format = [0-9]+/[0-9]+/[0-9]+:[0-9]+:[0-9]+:[0-9]+
    DateTimeFormat = %d/%m/%Y:%T
  }
  User
  {
    format = [a-zA-Z0-9]*
  }
  Agent
  {
    format = [a-zA-Z0-9]*
  }
  Command
  {
    format = [a-zA-Z0-9]*
  }
  Frame
  {
    format = [a-zA-Z0-9/]*
  }
  Info
  {
    format = .*
  }
  IPAddress
  {
    format = [0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
  }
  HDSAgent
  {
    format = [a-zA-Z0-9/\. ]*
  }
  MessNum
  {
    format = [0-9]+
  }
  <Misc> = <_rest>
}
;-----
TranslateTbl
{
}
;-----
Records
{
;
;
;Categories
;
;Pattern 1 -----
;
; 02/01/2007:11:57:49 -0500 -
;
Device_Manager_Master
{
  Name = Device_Manager_Master
  KeyVal = 0
  Type = CATEGORY
  Regex = <Date> -[0-9]+ - <_rest>
  Key = Device_Manager_Master
  ReplaceSpace = TRUE
}
;
;Records
;
;Pattern User1 -----
;

```

```

;StorageManager: created message #361108221,
user=system@127.0.0.1/Hitachi:HiCommandClient:DV1170954655234G, cmd=GetStorageArray,
storage=USP/10192
;
Key_User_1
{
  Name = Key_User_1
  KeyVal = Device_Manager_Master
  Type = RECORD
  Regex = <Agent>: <Info> #<MessNum>, user=<User>@<IPAddress><HDSAgent>, cmd=<Command>,
storage=<Frame>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:<Agent>
  AddToken2 = Log:DevManager
  AddToken3 = Src:Command - <Command>, Issued from <IPAddress>, Against frame <Frame>,
<Info> #<MessNum>
}
;
;Pattern User2 -----
;
;StorageManager: created message #361108221,
user=system@127.0.0.1/Hitachi:HiCommandClient:DV1170954655234G, cmd=GetStorageArray
;
Key_User_2
{
  Name = Key_User_2
  KeyVal = Device_Manager_Master
  Type = RECORD
  Regex = <Agent>: <Info> #<MessNum>, user=<User>@<IPAddress><HDSAgent>, cmd=<Command>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:<Agent>
  AddToken2 = Log:DevManager
  AddToken3 = Src:Command - <Command>, Issued from <IPAddress>, <Info> #<MessNum>
}
;
;Pattern User3 -----
;
;HostManager: successfully expired in COMPLETED
XmlMsg#360936207,usr=system,cmd=GetStorageArray
;
Key_User_3
{
  Name = Key_User_3
  KeyVal = Device_Manager_Master
  Type = RECORD
  Regex = <Agent>: <Info> #<MessNum>, usr=<User>,cmd=<Command>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:<Agent>
  AddToken2 = Log:DevManager
  AddToken3 = Src:Command - <Command>, <Info> #<MessNum>
}
;
;Pattern Agent1 -----
;
;GroupManager: loading AddLUNScan class
;
Key_Agent_1
{
  Name = Key_Agent_1
  KeyVal = Device_Manager_Master
  Type = RECORD
  Regex = <Agent>: <Info>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:<Agent>
  AddToken2 = Log:DevManager
  AddToken3 = Src:Command - <Info>
}

```

```
;
;Pattern Misc Records -----
;
;GetRequestStatus finished #358793662 status=PROCESSING cmd=AddStorageArray
target=#358793557
;
Key_Misc_Rec
{
  Name = Key_Misc_Rec
  KeyVal = Device_Manager_Master
  Type = RECORD
  Regex = <Misc>
  Key =
  ReplaceSpace = TRUE
  AddToken1 = Category:Misc Record
  AddToken2 = Log:DevManager
  AddToken3 = Src:Command - <Misc>
}
}
```

13.4. Message Parsing File for Array Audit Log (Syslog)

The Message Parsing file is used to describe the format of the records that are in the log file, so that the eTrust Audit generic log scraper can interpret these records. The MP file also tells the eTrust Audit generic log scraper how these records should be (re)formatted, what categories to assign to these records, before these records are sent on to the rest of eTrust Audit for processing/storage.

The following is a sample listing of the mp file for the USP Array Audit Log when it has been sent to a Solaris syslog server (HDSStorageNav.mp) that should reside in /export/opt/CAaudclnt/cfg/

```
*****
;
;Project : eTrust Audit 1.5 SP3
;Module : HDS Audit Log via Syslog
;File : HDSStorageNav.mp
;Purpose : Message parsing file for syslog
*****
;
;Developed By : Kery Hines for WinSyslog Product
;Modified By : Kery Hines March 31, 2007 (add space to basic record def)
*****
;
;
;-----
Tokens
{
  Date
  {
    Type = datetime
    format = [0-9]+\-[0-9]+\-[0-9]+T[0-9]+:[0-9]+:[0-9]+
    DateTimeFormat = %Y-%m-%dT%T
  }
  Detail_End_Type
  {
    format = [a-zA-Z0-9 _](-)*
  }
  Frame
  {
    format = [a-zA-Z0-9 ]*
  }
  Info
  {
    format = .*
  }
  IPAddress
```

```

{
  format = [0-9]+\.[0-9]+\.[0-9]+\.[0-9]*+
}
Log_In
{
  format = [a-zA-Z0-9 ](-)*
}
Status
{
  format = [a-zA-Z0-9 ]*
}
User
{
  format = [a-zA-Z0-9 ]*
}
J1
{
  format = [0-9><]+
}
<Misc> = <_rest>
}
;
-----
TranslateTbl
{
}
;
-----
Records
{
;
;Categories
;
;Pattern 1 -----
;
;<14>      Jan      16      15:06:51      SVP      Storage:      CELFSS,1.1,285024,,2007-01-
16T15:06:51.1Z,Storage,SVP,Authentication,
;
  HDS_Navigator_Auth
  {
    Name = HDS_Navigator_Auth
    KeyVal = 0
    Type = CATEGORY
    Regex = <J1> [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+ [a-zA-Z0-9]* [a-zA-Z0-9]*: [a-zA-Z0-
9]*,[0-9]+\.[0-9]+,[0-9]+,,<Date>\.[a-zA-Z0-9]*,[a-zA-Z0-9]*,[a-zA-Z0-
9]*,Authentication,<_rest>
    Key = HDS_Navigator_Auth
    ReplaceSpace = TRUE
  }
;
;Pattern 2 -----
;
;<14>      Jan      16      15:18:40      SVP      Storage:      CELFSS,1.1,285025,,2007-01-
16T15:18:40.8Z,Storage,SVP,ConfigurationAccess,
;
  HDS_Navigator_Config
  {
    Name = HDS_Navigator_Config
    KeyVal = 0
    Type = CATEGORY
    Regex = <J1> [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+ [a-zA-Z0-9]* [a-zA-Z0-9]*: [a-zA-Z0-
9]*,[0-9]+\.[0-9]+,[0-9]+,,<Date>\.[a-zA-Z0-9]*,[a-zA-Z0-9]*,[a-zA-Z0-
9]*,ConfigurationAccess,<_rest>
    Key = HDS_Navigator_Config
    ReplaceSpace = TRUE
  }
;
;Pattern Catch all record -----
;
  HDSCatch_All
  {
    Name = HDSCatch_All
    KeyVal = 0

```

```

Type = CATEGORY
Regex = <J1> [a-zA-Z]+ [0-9]+ [0-9]+:[0-9]+:[0-9]+ [a-zA-Z0-9]* [a-zA-Z0-9]*: [a-zA-Z0-9]*, [0-9]+\.[0-9]+, [0-9]+, <Date>\.[a-zA-Z0-9]*, <_rest>
Key = HDS_Catch_All
ReplaceSpace = TRUE
}
;
;Records
;
;Pattern 1 in1 -----
;
;Success,uid=DeviceMgr,R500:10192,,Local_USP@Warren_Lab10,,,,,,,,,266755,BasicLog,,,99,[BASE],Login ,IP=10.40.42.47*,Normal end,Seq.=386381
;
Key_HDS_Navigator_Auth_In1
{
Name = Key_HDS_Navigator_Auth_In1
KeyVal = HDS_Navigator_Auth
Type = RECORD
Regex = <Status>,uid=<User>,[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-9]*,[a-zA-Z0-9 ]*,,, [a-zA-Z0-9]*,\[[a-zA-Z0-9]*\],<Log_In>,IP=<IPAddress>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:User Login
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Storage Navigator <Log_In> <Status> on Frame <Frame> from IP Address <IPAddress>
}
;
;Pattern 1 in2 -----
;
;Success,uid=DeviceMgr({COMPONENT-POLLER}:DvM_Srv),R500:10192,,388GX10HU@WarrenNJ,,,,,,,,,284670,BasicLog,,,99,[BASE],Login ,IP=10.40.42.19*,Normal end,Seq.=393547
;
Key_HDS_Navigator_Auth_In2
{
Name = Key_HDS_Navigator_Auth_In2
KeyVal = HDS_Navigator_Auth
Type = RECORD
Regex = <Status>,uid=<User>(.*) , [a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-9]*,[a-zA-Z0-9 ]*,,, [a-zA-Z0-9]*,\[[a-zA-Z0-9]*\],<Log_In>,IP=<IPAddress>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:User Login
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Storage Navigator <Log_In> <Status> on Frame <Frame> from IP Address <IPAddress>
}
;
;Pattern 1 out1 -----
;
;Success,uid=DeviceMgr,R500:10192,,Local_USP@Warren_Lab10,,,,,,,,,266759,BasicLog,,,99,[BASE],Logout,,Normal end,Seq.=386382
;
Key_HDS_Navigator_Auth_Out1
{
Name = Key_HDS_Navigator_Auth_Out1
KeyVal = HDS_Navigator_Auth
Type = RECORD
Regex = <Status>,uid=<User>,[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-9]*,[a-zA-Z0-9 ]*,,, [a-zA-Z0-9]*,\[[a-zA-Z0-9]*\],<Log_In>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:User Logout
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Storage Navigator <Log_In> <Status> on Frame <Frame>
}
;
;Pattern 1 out2 -----
;

```

```

;Success,uid=DeviceMgr({COMPONENT-
POLLER}:DvM_Srv),R500:10192,,388GX10HU@WarrenNJ,,,,,,,,,284673,BasicLog,,,99,[BASE],Logout
,,Normal end,Seq.=393548
;
Key_HDS_Navigator_Auth_Out2
{
Name = Key_HDS_Navigator_Auth_Out2
KeyVal = HDS_Navigator_Auth
Type = RECORD
Regex = <Status>,uid=<User>(.*),[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-
9]*,[a-zA-Z0-9 ]*,,,[a-zA-Z0-9]*,\[[a-zA-Z0-9 ]*\],<Log_In>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:User Logout
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Storage Navigator <Log_In> <Status> on Frame <Frame>
}
;
;Pattern 2 bas1 -----
;
;Success,uid=DeviceMgr,R500:10192,,Local_USP@Warren_Lab10,,,,,,,,,266756,BasicLog,,,99,[BA
SE],ChangeMode,Modify,Normal end,Seq.=515508
;
Key_HDS_Navigator_Config_Basic1
{
Name = Key_HDS_Navigator_Config_Basic1
KeyVal = HDS_Navigator_Config
Type = RECORD
Regex = <Status>,uid=<User>,[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-
9]*,BasicLog,,,[a-zA-Z0-9]*,\[[a-zA-Z0-9 ]*\],<Log_In>,<Detail_End_Type>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:Config Change Basic
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Configuration Change <Log_In> <Detail_End_Type> <Status> on Frame
<Frame>
}
;
;Pattern 2 bas2 -----
;
;Failed,uid=DeviceMgr({COMPONENT-
POLLER}:DvM_Srv),R500:10192,,388GX10HU@WarrenNJ,,,,,,,,,284671,BasicLog,,,99,[BASE],Change
Mode,Modify,Error(2-9000),Seq.=526257
;
Key_HDS_Navigator_Config_Basic2
{
Name = Key_HDS_Navigator_Config_Basic2
KeyVal = HDS_Navigator_Config
Type = RECORD
Regex = <Status>,uid=<User>(.*),[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-
9]*,BasicLog,,,[a-zA-Z0-9]*,\[[a-zA-Z0-9 ]*\],<Log_In>,<Detail_End_Type>,. *<000>
Key =
ReplaceSpace = TRUE
AddToken1 = Category:Config Change Basic
AddToken2 = Log:HDSStorageNav
AddToken3 = Src:Configuration Change <Log_In> <Detail_End_Type> <Status> on Frame
<Frame>
}
;
;Pattern 2 det1 -----
;
;Success,uid=DeviceMgr,R500:10192,,388GX10HU@WarrenNJ,,,,,,,,,283456,DetailLog,,,+Operatio
n=Add
;
Key_HDS_Navigator_Config_Detail1
{
Name = Key_HDS_Navigator_Config_Detail1
KeyVal = HDS_Navigator_Config
Type = RECORD
Regex = <Status>,uid=<User>,[a-zA-Z0-9]*:<Frame>,,[a-zA-Z0-9@_.-]*,,,,,,,,[a-zA-Z0-
9]*,DetailLog,,,[+-]+<Info><000>

```

```
Key =  
ReplaceSpace = TRUE  
AddToken1 = Category:Config Change Detail  
AddToken2 = Log:HDSStorageNav  
AddToken3 = Src:<Info>  
}  
;  
;Pattern Catch all record -----  
;  
KeyHDSCatch_All  
{  
Name = KeyHDSCatch_All  
KeyVal = HDSCatch_All  
Type = RECORD  
Regex = <Misc>  
Key =  
ReplaceSpace = TRUE  
AddToken1 = Category:SN Catch All  
AddToken2 = Log:HDSStorageNav  
AddToken3 = Src:<Misc>  
}  
}
```

14. References

Document	Location
GDSE Website	http://engineering.ti.citigroup.net/gdse/
Unix Engineering	http://unixeng.corp.smb.com/
EMC DMX Solutions Guide	http://engineering.ti.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/03038-sg.pdf
EMC CLARiiON Solutions Guide	http://engineering.ti.citigroup.net/gdse/products/platforms/clariion/stdsdocs/05010-sg.pdf
HDS TagmaStore USP Solutions Guide	http://engineering.ti.citigroup.net/gdse/products/platforms/tagmastore/stdsdocs/05015-sg.pdf

15. Release Notes

Version

1.4

Comment

Created Release Notes section. Updated HDS to reflect new syslog based audit log. Updated HDS to reflect new Device Manager audit log. Deleted old GUI-based HDS information. Added eTrust process management for Solaris and Windows. Removed the following old entries from version table:

Version	Date	Author	Reviewed	Comments
Draft .01	13-Jun-05	Kevin Hobaugh	Gary Johnson	
Draft .02	21-Jun-05	Kevin Hobaugh	Project Team	
Draft .03	24-Jun-05	Kevin Hobaugh	Project Team	
Draft .04	5-Jul-05	Kevin Hobaugh	RFC	1. Changed title. 2. Modified Sect 8 with additional screen shots. 3. Reorganized some of the sections.

1.5

Appendix E changes (HDS): Updated both mp file listings, added syslog.conf and syslog daemon definitions, updated recorder.ini listings. Updated all external document references to reflect new GDSE website. Updated Citigroup logo to reflect new Citi logo.