EMC²

TECHNICAL NOTES

EMC® VNX®
Version 8.1

Configuring and Using the Audit Tool on VNX for File

P/N 300-015-126 Rev 01
August, 2013

This technical note contains information on these topics:

Executive summary

The Audit tool provides a mechanism to monitor and collect events that are posted to log files.

This technical note explains how to configure and use the Audit tool for VNX for File systems and how to interpret the information it collects.

Introduction

The Audit tool runs on the Control Station, and monitors events posted in existing logs. It sends appropriate events to the local SYSlog service, which, in turn forwards the event records to a remote SYSlog server.

Audience

This technical note is aimed at administrators responsible for monitoring storage systems.

Overview

The Audit tool consists of several scripts that run on the Control Station. Each script monitors an assigned log file continuously for particular events. When one of these events occurs, the scripts post a standardized message using the Linux SYSlog functionality.

The scripts map the User ID to the LDAP name or local name as defined in the administrative database. Each instance of the script creates an internal mapping at startup and updates it periodically while running.

The scripts do not add new events to the logs; instead they monitor events posted in existing logs and then send the appropriate events to the local SYSlog service. The local SYSlog service is, in turn, configured to forward the event records to a remote SYSlog server.

The Audit tool monitors the following log files:

- `/nas/log/cmd_log`
- `/var/log/messages`

When a script detects an applicable message, it reformats it into the following format:

Date/time stamp, Time zone, System ID (Serial number), EVENTID, Operation, Username, User ID, Log name, Original Celera Log Entry

where:

- Date/Time Stamp = time on the Control Station
- Time zone = time zone in standard format from the Linux time zone functionality
- System ID = serial number of the system as reported by the/nas/sbin/serial command
- EVENTID = unique number to facilitate quick identification of events
- Operation = text describing the event
- Username = user name of the individual that executed the operation (The tool uses the name in the `/nas/site/user_db` file.)
- User ID = user ID as defined on the system
- Log Name = name of the log on the system where the event was posted
- Original Celera Log Entry = text of the original Celera Log Entry

Following is an example of Audit tool output from a remote SYSlog when the scripts are running, and an explanation of the information in the output:

```
May 18 18:32:14 nasdev244cs0 AUDIT_Messages.pl:
05/18/2010,18:32:14,EDT,ABC12345678901,1101,Succesful
Login,root(uid=0)@local,0,/var/log/messages,May 18
18:32:02 nasdev244cs0 sshd(pam_unix)[16132]: session
opened for user root by root(uid=0)
```

- Local SYSlog information = timestamp, hostname, and utility that provides the entry to the SYSlog utility on the Control Station. In this case, May 18 18:32:14 nasdev244cs0 AUDIT_Messages.pl.
- Date/Time Stamp = from AUDIT tool on 5/18/2010 at 18:32:14
- Time zone = EDT
- System ID = ABC12345678901
- Event ID = 1101
- Operation = Successful Login
- Username = root(uid=0)@local

- User ID = 0
- Log Name = /var/log/messages
- Original Celera Log Entry = May 18 18:32:02 nasdev244cs0 sshd(pam_unix)[16132]: session opened for user root by root(uid=0)

Two additional examples of Audit tool output are:

```
May 18 18:32:32 nasdev244cs0 sshd[16348]: Accepted
password for nasadmin from 128.222.7.47 port 2221 ssh2

May 18 18:32:39 nasdev244cs0 AUDIT_Messages.pl:
05/18/2010,18:32:39,EDT,ABC12345678901,1103,Password for
session accepted,root(uid=0)@local,0,/var/log/messages,May
18 18:32:32 nasdev244cs0 sshd[16348]: Accepted password
for nasadmin from 128.222.7.47 port 2221 ssh2
```

Add Audit tool scripts to your storage system

1. Log in to your system as root.
2. Copy the files and directories from the `AUDIT_tool` directory in the Zip file to the `/etc/AUDIT_tool` directory on your Control Station.

   ```
   cp –rf /<path>/AUDIT_tool/  /etc/AUDIT_tool/
   ```

3. Change directory (`cd`) to the `AUDIT_tool` directory. View (`ls`) the contents of the directory to verify that the following files are present:

   ```
   AUDIT_cmd_bs  AUDIT_messages.pl  auto
   custom_cmd_log.csv       File
   ReadMe.txt

   AUDIT_cmd.pl  AUDIT_ms_bs        cmd_log.csv
   custom_messages_log.csv  messages_log.csv  Time
   ```

4. Copy the file `AUDIT_ms_bs` to `/etc/.AUDIT_ms_bs` (the '.' makes it a hidden file) by typing:

   ```
   cp –f AUDIT_ms_bs /etc/.AUDIT_ms_bs
   ```

5. Copy the file `AUDIT_cmd_bs` to `/etc/.AUDIT_cmd_bs` (the '.' makes it a hidden file) by typing:

   ```
   cp –f AUDIT_cmd_bs /etc/.AUDIT_cmd_bs
   ```

6. Ensure that both scripts are executable by running the following commands in the `/etc directory` :

   ```
   chmod u+x .AUDIT_ms_bs
   chmod u+x .AUDIT_cmd_bs
   ```

7. Run the `.AUDIT_ms_bs` in the original console to ensure that it executes by typing:

   ```
   /etc/.AUDIT_ms_bs
   ```

   If the file fails to execute, refer to Appendix B: Troubleshooting.

8. Tail the log file from a different console window to verify the Audit tool is operating by typing:

   ```
   tail –f /var/log/messages
   ```

   Examine the log for the events you wanted to collect.

8. Add the following lines to the `/etc/initab` file. The scripts are added to `inittab` to ensure that the scripts are restarted in case of a system restart.

   ```
   # Run the Audit tool shell scripts
   aml:3:respawn:/etc/.AUDIT_ms_bs
   acl:3:respawn:/etc/.AUDIT_cmd_bs
   ```

9. Restart the `inittab` by typing:

   ```
   telinit q
   ```

View messages on remote SYSlog server

1. Add the loghost information to the `/etc/hosts` file on the Control Station. For example:

   ```
   #log host
   # Ipaddress (###.###.###) -- Fully qualified
     DNS name -- "loghost"
   128.001.1.1   rsyslog_host.company.com   loghost
   ```

2. Add the following lines to the `/etc/syslog.conf` file:

   ```
   # write audit to remote log
   auth.notice            @loghost
   ```

3. Restart the SYSlog service by typing:

   ```
   /etc/service syslog restart
   ```

Ensure that remote SYSlog server can receive messages

1. Ensure that the remote SYSlog server is configured to receive the log entries. Examine the `/etc/sysconfig/syslog` file and determine if the `-r` option is set on the SYSLOGD_OPTIONS line. Enter the following command:

   ```
   cat /etc/sysconfig/syslog
   ```

   If the `–r` is on the on the SYSLOGD_OPTIONS line, the line will appear as follows:

   ```
   SYSLOGD_OPTIONS="-m 0 -r"
   ```

2. If this entry does not exist, add it.
3. Restart the SYSlog service on the remote server, if necessary by typing:

   ```
   /etc/service syslog restart
   ```

Appendix A: Audit_messages command options

You can modify Audit tool settings by using the Audit_messages command with the following options:

`-help`

Prints a brief help message and exits.

`-scaninterval=<`*filename*`>`

The default is 20 (Minimum = 10, Maximum = 300).

`-userfile=<`*filename*`>`

The name of the file where the user specified messages are stored. The default is `custom_messages_log.csv`.

The format of the file where the messages are stored is as follows:

```
EVENTID, UID_Valid, Operation, message_text
```

where:

- `EVENTID` = a unique number to facilitate quick identification of events that are deemed important
- `UID_Valid` = an indication that the UID on this command is the operator that issues the command. In some cases, the event does not have an associated UID.
- Operation = text describing the event
- `message_text` = actual text that will be used to scan the log

`-logfilename=<`*filename*`>`

The name of log file to monitor. The default is `/var/log/messages`.

`-syslog_severity=<`*severity_level*`>`

The severity setting used to post events from the Audit tool so that the event is sent to the remote SYSlog server. The default is `LOG_NOTICE`.

Additional valid severity options include:

- `LOG_EMERG` -- system is unusable
- `LOG_ALERT` -- action must be taken immediately
- `LOG_CRIT` -- critical conditions

- LOG_ERR -- error conditions
- LOG_WARNING -- warning conditions
- LOG_NOTICE -- normal, but significant, condition
- LOG_INFO -- informational message
- LOG_DEBUG -- debug-level message

-syslog_facility=<*facility_name*>

The SYSlog facility where events are posted. The default is LOG_AUTH.

Additional valid facility options:

- LOG_AUDIT -- audit daemon
- LOG_AUTH – security authorization messages
- LOG_AUTHPRIV – security authorization messages (private)
- LOG_CONSOLE -- /dev/console output
- LOG_CRON -- clock daemons (cron and at)
- LOG_DAEMON -- system daemons without separate facility value
- LOG_FTP -- FTP daemon
- LOG_KERN -- kernel messages
- LOG_INSTALL -- installer subsystem
- LOG_LAUNCHD -- launchd - general bootstrap daemon
- LOG_LFMT -- logalert facility; falls back to LOG_USER
- LOG_LOCAL0 through LOG_LOCAL7 -- reserved for local use
- LOG_LPR -- line printer subsystem
- LOG_MAIL -- mail subsystem
- LOG_NETINFO -- NetInfo subsystem
- LOG_NEWS -- USENET news subsystem
- LOG_NTP -- NTP subsystem
- OG_RAS -- Remote Access Service (VPN / PPP)
- LOG_REMOTEAUTH -- remote authentication/authorization

- LOG_SECURITY -- security subsystems (firewalling, etc.)
- LOG_SYSLOG -- messages generated internally by syslogd
- LOG_USER (default) -- generic user-level messages
- LOG_UUCP -- UUCP subsystem

-man

Prints the manual page and exits.

-debug

Displays debug information during operation.

Appendix B: Troubleshooting

It is possible that the `.AUDIT_ms_bs` script was edited on an operating system that uses end-of-line characters that differ from those used in Linux. This could happen if the file was edited on a Mac or PC, or if the file was converted when it was packaged. In this case, you get the misleading bad interpreter message, such as: No such file or directory message. To correct this problem, do the following:

1. Open the script with the `vi` editor. If you are unfamiliar with `vi`, follow these steps carefully. Type the following:

   ```
   vi .AUDIT_ms_bs
   ```

2. After the file opens, set the file type to UNIX by typing the following:

   ```
   :set fileformat=unix
   ```

3. Press **Enter**.

   You will not notice any change, but the end-of-line character problem is fixed.

4. Save and exit by typing the following:

   ```
   :wq!
   ```