**Linux System**

# Vendor List:

* Linux

# Security Audit Configuration & Compliance

## **1.Linux**

### **Privileged User Activity Monitoring and Auditing:**

Configuration:

1. Login to the linux box and assume root

sudo su -

1. Edit **/etc/profile** and add the following lines to the bottom of the file:

# command line audit logging

function log2syslog

{

declare COMMAND

COMMAND=$(fc -ln -0)

logger -p local1.notice -t bash -i -- "${USER}:${COMMAND}"

}

trap log2syslog DEBUG

1. Save and exit **/etc/profile**
2. Edit **/etc/rsyslog.conf** and add the following lines to the bottom of the file:

# command line audit logging

#local1.\* -/var/log/cmdline

local1.\* @@10.19.151.51:514

###OR According to server site main/DR

local1.\* @@10.10.151.51:514

1. Save and exit **/etc/rsyslog.conf**
2. Either restart the rsyslog service, or restart the whole machine to release all user sessions - forcing a reload of the bash profile and enacting the changes

/etc/init.d/rsyslog restart

1. The audit logging will be visible under **/var/log/syslog**and**/var/log/cmdline** and will look like this:

Aug 22 15:04:39 ip-10-10-34-56 bash[15856]: jsmith:

Aug 22 15:04:40 ip-10-10-34-56 bash[15859]: jsmith:#011 sudo su -

Aug 22 15:04:43 ip-10-10-34-56 bash[15893]: root:

Aug 22 15:04:49 ip-10-10-34-56 bash[15903]: root:#011 ls -lart /var/log

Aug 22 15:05:01 ip-10-10-34-56 CRON[15927]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)

Aug 22 15:05:06 ip-10-10-34-56 bash[15937]: root:#011 ls -lart /var/log | grep cmd

Aug 22 15:15:01 ip-10-10-34-56 CRON[17254]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1 1 1)

Aug 22 15:17:01 ip-10-10-34-56 CRON[17513]: (root) CMD ( cd / && run-parts --report /etc/cron.hourly)

Aug 22 15:20:02 ip-10-10-34-56 bash[17921]: root:#011 cd /var/log

Aug 22 15:20:03 ip-10-10-34-56 bash[17924]: root:#011 ls

Aug 22 15:20:16 ip-10-10-34-56 bash[17969]: root:#011 service confluence restart

1. You may consider saving the log on an NFS mount and/or pushing the syslog logs to another machine.
2. The following list consider to IP addresses need to apply above configuration on them:

**DR Site:**

* + - 1. 10.19.100.12
      2. 10.19.150.34
      3. 10.19.207.28

**Main Site:**

* + - 1. 10.10.100.176
      2. 10.10.100.12
      3. 10.10.100.177
      4. 10.10.150.36
      5. 10.10.103.11
      6. 10.10.107.23
      7. 10.10.107.24

1. The Testing required after configuring. the following command need to be testing by SysAdmin User:
   * + 1. Pwd
       2. Netstat
       3. Cd

# Locally Retention Logs & Rotation Period

The primary way to manage logging is to set up the system to create all necessary logs and alerts and a minimum of unnecessary log entries

## **Set Log File Retention Policies**

the guidelines to apply the log file retention policy in CIS Hardening report .

## **Store Log Files on a Separate Drive**

Log files are written constantly, which can lead to high disk I/O on busy systems. As a best practice, you should mount /var/log on a separate storage device. This prevents log file writes from interfering with the performance of your applications, especially on disk-based storage. This also prevents log files from filling up the entire drive in case they become too large.

# System Owner Configuration Check

## **1.Linux**

The System Admin has to check syslog structure and format

### **Auditing the Log Review Status**

*date time hostname facility:priority username: message\_body.*

1. A selector to determine the log message priorities which is the *facility.priority* pair.
2. A log destination (file path) for the above selector.
3. Rotation (optional)

The *facility* must be one of the values from the following list:

* kern - kernel messages
* user - random user-level messages (recommended for the **db2audit extract** command)
* mail - mail system messages
* daemon - system daemons
* auth - security/authorization messages (recommended for the **db2audit extract** command)
* syslog - messages generated internally by syslogd
* lpr - line printer subsystem
* news - news subsystem
* uucp - uucp subsystem
* cron - clock daemon
* caa - Cluster aware AIX® subsystem
* local0 ~ local7 - reserved for local use (recommended for the **db2audit extract** command)
* \* - (all facilities- used only in the configuration file and not in the commands or API)

The *priority* must be one of the values from the following list (from high to low):

* emerge or panic - system is unusable
* alert - action must be taken immediately
* crit - critical conditions
* err or error - error conditions
* warn or warning - warning conditions
* notice - normal but significant condition
* info - informational
* debug - debug-level messages

Syslog messages are logged usually in the format:

*date time hostname facility:priority username: message\_body.*

# Reference

## <https://www.ibm.com/docs/en/db2/11.5?topic=logs-configuring-system-error-event-log-syslog>

## https://confluence.atlassian.com/confkb/how-to-enable-command-line-audit-logging-in-linux-956166545.html