**Log Files**

* Log means to make a record of something.
* Log file is the file which record of everything happens in system.
* The purpose of log file is to keep track of what happening with server.
* Logging is the act of keeping a log.
* Almost all Log files are generated automatically through system log (on behalf of system) and some are generated by applications.
* Log file is generally password protected so that only server administrator has a record of everything going on system.
* Common examples of Logs:
* Access log on web server: This log file keeps record of all individual files that people have requested from a website, number of visitors, number of request per page, the domain of visitors and so on.
* Transaction log in Microsoft exchange: This log keeps record of changes made to an exchange database. Any changes are first written in transaction log and afterwards written to database.
* Audit log: This log keeps record of any activity that could have affected a particular events. Activities like timestamp of resource access, source & destination addresses, and login information and so on.
* **Use of logs**:
* Logs are useful to troubleshoot the physical system and virtual system as well.
* Provides early warning sign of system abuse.
* When everything is failed including system crash, logs provide crucial data to recover system.
* Log file is in simple ASCII text format.
* Extension of log file: .log
* By default, logs are stored in /var/log.
* To view log files,

Command: ls –l /var/log

**Syslog:**

* Syslog is standard logging facility which collects messages from all other applications, services & kernel and store them under /var/log.
* Syslog term is often used to refer syslog daemon, syslog protocol or syslog messages.

Syslog daemon: (spell: daymun)

* Daemon (daemon process) is the program that runs in the background and does not connected with terminal.
* Daemon is started at system boot time and terminated when system is shutdown.
* Most of daemon names end with “d”.
* Daemon runs as root user/special privileged users.
* Daemon performs specified operation at predefined time or in respond to certain event.
* Daemon is not interactive and not under control of user.
* Daemon must be child process of INIT process and must not be connected to terminal.

Syslog protocol:

* Transport protocol that specifies how logs/messages can be sent over network.
* Standard UDP port : 514 for plain logs

6154 for encrypted logs

Syslog messages: Simply log messages

**Operation of Syslog:**

Applications send their log entries to syslogd (syslog daemon) which consults configuration file /etc/syslogd.conf OR /etc/syslog [Centralized logging program runs under these files, this file specifies rules for logging] and when match is found, writes the log message to desired log files.

Every logging rule consist of two fields, selector and action.

Format of Syslog:

&LT;%PRI%&GT;%PROTOCOL-VERSION% %TIMESTAMP:::DATE-RFC3339% %HOSTNAME% %APP-NAME% %PROCID% %MSGID% %MSG%N

E.g.,

&LT;34&GT;1 2003-10-11T22:14:15.003Z SERVER1.COM SSHD - - PAM\_UNIX(SSHD:AUTH): AUTHENTICATION FAILURE; LOGNAME= UID=0 EUID=0 TTY=SSH RUSER= RHOST=10.0.2.2

Timestamp: Indicates time & date on which message was generated on the system sending message. 2003-10-11 date & 22:14:15.003 on which message was generated.

Hostname: Name of host/system (server1) that sent a message.

App-name: Indicates name of application (sshd: auth) sent the message.

There are four terms related to Syslog:

1. Facility
2. Priority/ security level
3. Selector
4. Action
5. **Facility:**

* It specifies the application/process which submit log message.
* Facility code is used to specify type of application logging the message.

|  |  |  |
| --- | --- | --- |
| **Facility Code** | **Keyword** | **Description** |
| 0 | kern | kernel messages |
| 1 | user | user level messages |
| 2 | mail | mail system |
| 3 | daemon | system daemons |
| 4 | auth | security/authorization messages |
| 5 | syslog | messages generated internally by Syslogd |
| 6 | lpr | line printer subsystem |
| 7 | news | network news subsystem |
| 8 | uucp | UUCP subsystem |
| 9 |  | clock daemon |
| 10 | authpriv | security/authorization messages |
| 11 | ftp | FTP daemon |
| 12 |  | NTP subsystem |
| 13 |  | log audit |
| 14 |  | log alert |
| 15 | cron | scheduling daemon |
| 16 | local0 | local use 0 |
| 17 | local1 | local use 1 |
| 18 | local2 | local use 2 |
| 19 | local3 | local use 3 |
| 20 | local4 | local use 4 |
| 21 | local5 | local use 5 |
| 22 | local6 | local use 6 |
| 23 | local7 | local use 7 |

1. **Priority/ security level:**

* It indicates the importance of the message.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Value** | **Security** | **keyword** | **Description** | **Example** |
| 0 | Emergency | emerg | Emergency condition | System crash |
| 1 | Alert | alert | should be corrected immediately | corrupted system database |
| 2 | Critical | crit | critical condition | hardware error |
| 3 | Error | err | Ordinary error | storage limit exceeded |
| 4 | Warning | warn | indicates that error may occur if no action will be taken | non root file system has only 2 GB remaining |
| 5 | Notice | notice | Condition that is not error but should be handled in specific way. |  |
| 6 | Informational | info | Normal operational messages that requires no action. | Application started successfully. |
| 7 | Debug | debug | Messages used for debugging program. |  |

1. **Selector:**

* It is combination of one or more facilities and security level.
* When an incoming event matches a selector, an action is performed.

1. **Action:**

* Actions to be performed when an event matches a selector. Actions like writing message to a log file, echo message to a console and so on.

**Types of logs:**

|  |  |  |
| --- | --- | --- |
| **Sr. no** | **Log file** | **Description** |
| 1 | /var/log/messages | general system messages(daemons)  i.e., message during system startup |
| 2 | /var/log/auth.log  /var/log/secure | Authentication logs |
| 3 | /var/log/kern.log | kernel logs |
| 4 | /var/log/cron.log | cron daemons logs  i.e., started job, terminated job, failure job |
| 5 | /var/log/mail.log  /var/log/maillog | Mail server logs |
| 6 | /var/log/daemon.log | Information logged by various daemons run on the system |
| 7 | /var/log/user.log | Information about all user level logs |
| 8 | /var/log/wtmp | All login and logout information |
| 9 | /var/log/btmp | Records failed login attempts. |
| 10 | /var/run/utmp | Present login state of each user |
| 11 | /var/log/dmesg | Contains kernel information about hardware & devices detected during boot process.  Will be overwritten during next boot |
| 12 | /var/log/mysql | MYSQL database logs |
| 13 | /var/log/audit/audit.log | Activities performed by user |
| 14 | /var/log/boot | Information regarding boot process (after kernel is loaded)  i.e., system file check, starting firewall, network devices, staring services and so on |
| 15 | /var/log/dpkg.log | Information regarding package installation/uninstallation |
| 16 | /var/log/yum.log | Information regarding package installation/uninstallation |
| 17 | /var/log/cups | All printer and printing related logs |
| 18 | /var/log/anaconda.log | Linux Installation related logs |
| 19 | /var/log/httpd  /var/log/apache2 | Apache web server access\_log and error\_log |
| 20 | /var/log/lighttpd | Light HTTPD access\_log and error\_log |
| 21 | /var/log/Xorg.x.log | log messages from X |

**Analyzing Logs:**

* Log analyzing is useful to troubleshoot the problem.
* It is useful to search particular text from big log files and filter particular texts from log files.
* Different commands/tools used for analyzing log files:

1. head

Monitoring purpose

1. tail
2. grep
3. cut
4. more
5. less
6. sort
7. uniq
8. awk
9. **head:**

* head command is used to display few lines from beginning/top end.
* By default, it displays first 10 lines.
* It is used with piping (|) only.
* e.g.,

ls –l /var/log | head : displays first 10 lines

ls –l /var/log | head -5 : display first 5 lines

1. **tail:**

* tail command is used to display few lines from bottom end.
* By default, it displays last 10 lines.
* It is used with piping (|) only.
* It is real time stream reading.
* e.g.,

ls –l /var/log | tail : display last 10 lines

ls –l /var/log | tail -5 : display last 5 lines

ls –l /var/log | tail –n +22 : display lines starting from 22 to last lines.

1. **grep:**

* grep command is used to filter lines according to required words/data row wise.
* Command: grep condition/word to be searched file/directory
* e.g.,

grep vaibhav v2 : display lines containing word “vaibhav”

grep --color vaibhav v2 : display lines containing word “vaibhav” in red color

grep –n vaibhav v2 : number the lines containing that word

grep –c vaibhav v2: gives total count of lines containing that word

grep –v vaibhav v2: display lines those not containing that word

grep –n --color ‘vaibha..’ v2

grep –n --color ‘v\*’ v2

grep –n --color ‘^vaibhav’ v2

grep –n --color ‘india$’ v2

Regular Expressions:

* . (Dot) : Single character
* [ ] (Square bracket): range of characters to match one or more characters
* \* (Asterisk) : one or more than one characters
* ^ : Following text must appear at the beginning of line
* $ : Preceding text must appear at the end of the line

1. **cut:**

* cut command is used to filter lines column wise.
* Command: **cut** **-d**<‘delimiter’> **-f**<column\_number> <file/directory>
* e.g., cut -d: -f1,2 v2: display the 1st and 1nd column content

1. **more:**

* It is used to view text file one page at a time.
* Press spacebar key to go to next page. Press enter key to navigate line by line.
* We can’t move backward from current page.
* Command: more file/directory
* e.g.,

more v2: display text file one page at a time

more -5 v2: display 5 lines per page at a time

more +30 v2 : display lines from 30th to end line.

1. **less:**

* It displays same output as more does.
* It allows forward/backward navigation through up/down keys.
* Press enter key to navigate line by line.
* Command: less file/directory
* By default, only way to exit less command, press q key. To make it automatically,

less -e v2 OR less -E v2

* e.g.,

less v2: display text files

less +30 v2 : display lines from 30th to end line.

less –N v2 : Number the output lines

less +/<word> v2: to highlight word in output

1. **sort:**

* sort command sorts contents of a text file line by line.
* Command: sort file/directory
* e.g.,

sort v2: sort contents of v2 file in the 1st field

sort -t: v2: used to separate fields by a colon character

sort -r v2 : sort in a reverse order

sort -k2 v2: sort by 3rd field

**Log Rotation:**

* As more and more information gets logged to log files, log files use more and more spaces. At some point of time, log files running out of disk space.
* Several problems arise when log files get bigger and bigger. e.g., larger files are hard tyo manipulate, disk space running out of space and so on.
* To get rid of these problems, log rotation technique is used.
* It moves existing log file to some other log file, starting fresh with empty log file and delete old log files over period time.
* It also takes care of log file compression.
* Log rotation activity is performed on predefined time (hourly, daily, nightly, weekly, monthly, yearly).