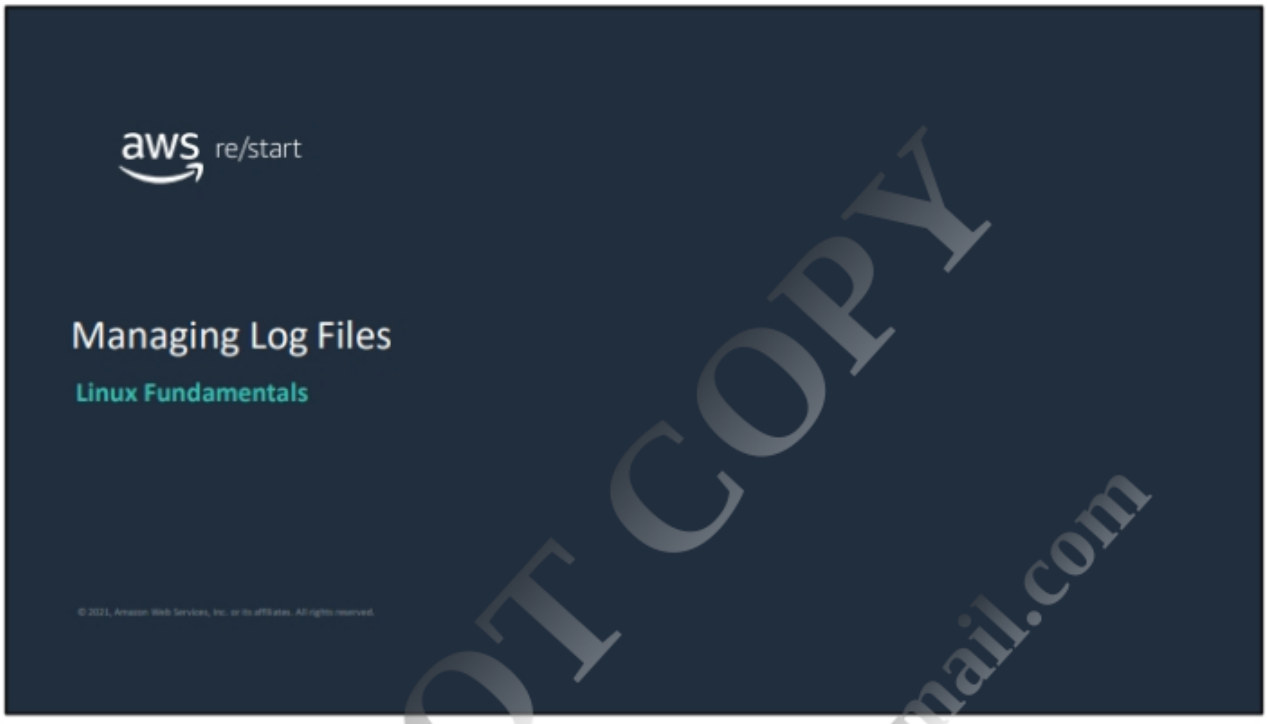


Welcome to Managing Log Files.

What you will learn

At the core of the lesson

You will learn how to:

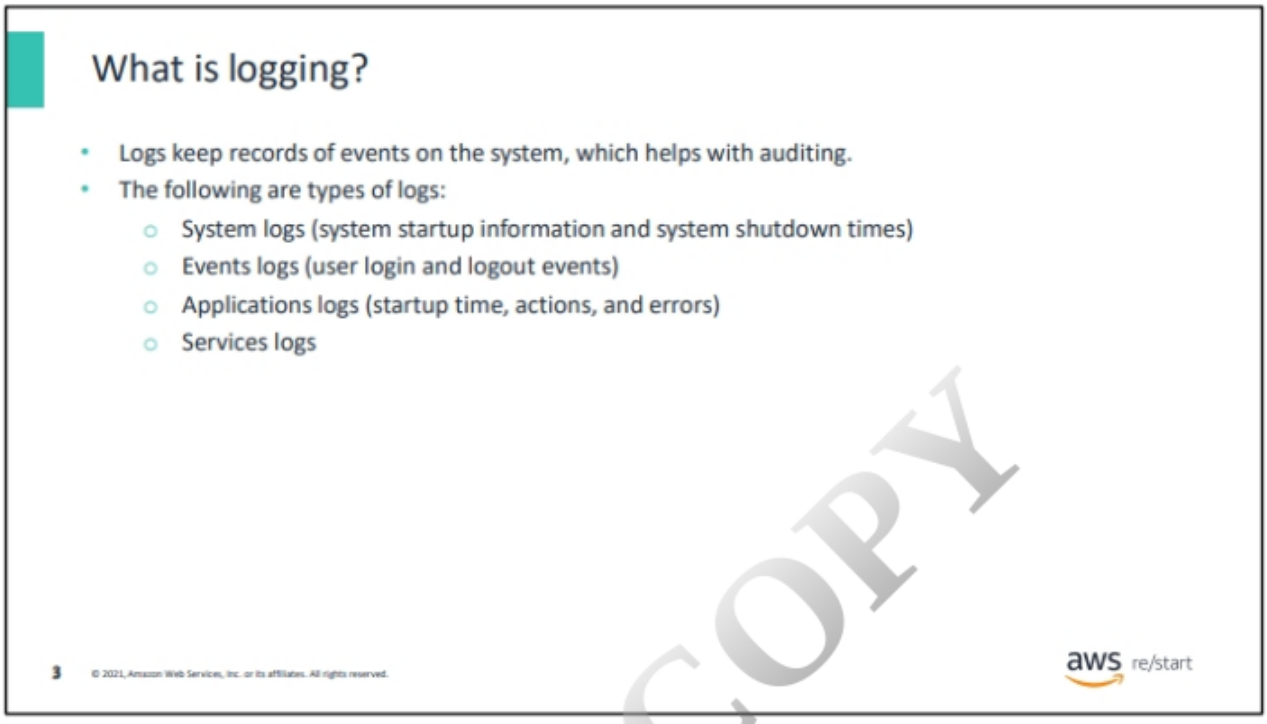
- Define log files
- Use commands to read different types of messages in a log file
- Recognize the benefits of log rotation

2

aws re/start

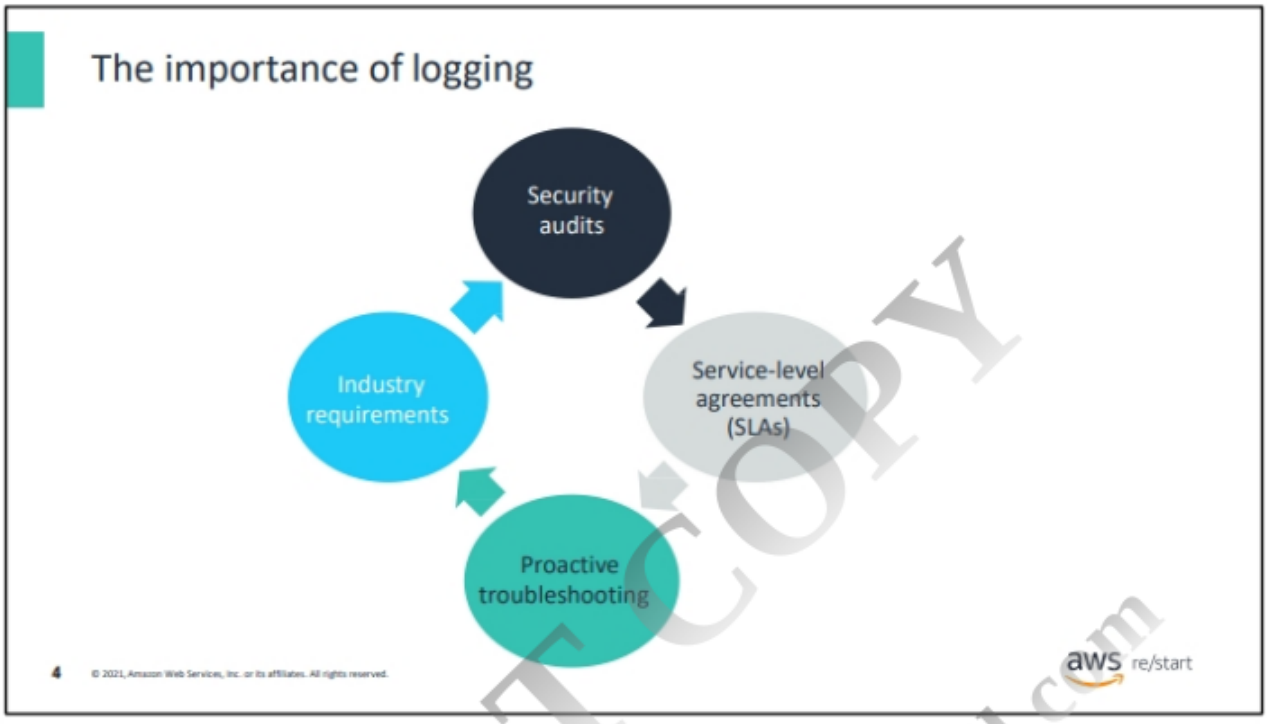
You will learn how to:

- Define log files
- Use commands to read different types of messages in a log file
- Recognize the benefits of log rotation



Logs are a record of what happened in the operating system or an application.

They are particularly useful if an issue occurs. Administrators, developers, and others can trace which application triggered an error, which user made a wrong action, or which outside host accessed the server.



Logging can help troubleshoot issues: What or who caused an error? Did anyone wrongfully access a file, a database, or a server?

Logs are a key to security audits (gathering information about the system) and service-level agreements (troubleshooting must start within *x* hours after an issue occurs).

Example of a log file

```
[ec2-user]$ sudo cat /var/log/yum.log
May 28 08:35:38 Updated: glibc-minimal-langpack-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-common-2.26-45.amzn2.x86_64
May 28 08:35:39 Updated: glibc-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: libcrypt-2.26-45.amzn2.x86_64
May 28 08:35:40 Updated: python3-pip-20.2.2-1.amzn2.0.2.noarch
May 28 08:35:41 Updated: python3-setuptools-49.1.3-1.amzn2.0.2.noarch
May 28 08:35:41 Updated: python3-3.7.9-1.amzn2.0.3.x86_64
May 28 08:35:43 Updated: python3-libs-3.7.9-1.amzn2.0.3.x86_64
May 28 08:35:43 Updated: 32:bind-license-9.11.4-26.P2.amzn2.5.noarch
May 28 08:35:43 Updated: 32:bind-libs-lite-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-libs-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-utils-9.11.4-26.P2.amzn2.5.x86_64
May 28 08:35:43 Updated: 32:bind-export-libs-9.11.4-26.P2.amzn2.5.x86_64
```

```
[ec2-user]$ sudo cat /var/log/httpd/error_log-20210620
[Sun Jun 13 03:49:01.840870 2021] [lbmethod_heartbeat:notice] [pid 2901] AH02282: No slotmem from mod_heartmonitor
[Sun Jun 13 03:49:01.840916 2021] [http2:warn] [pid 2901] AH10034: The mpm module (prefork.c) is not supported by mod_
http2. The mpm determines how things are processed in your server. HTTP/2 has more demands in this regard and the curr
ently selected mpm will just not do. This is an advisory warning. Your server will continue to work, but the HTTP/2 pr
otocol will be inactive.
[Sun Jun 13 03:49:01.840922 2021] [http2:warn] [pid 2901] AH02951: mod_ssl does not seem to be enabled
[Sun Jun 13 03:49:01.841367 2021] [mpm_prefork:notice] [pid 2901] AH00163: Apache/2.4.46 () configured -- resuming nor
mal operations
[Sun Jun 13 03:49:01.841374 2021] [core:notice] [pid 2901] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Tue Jun 15 12:23:06.907911 2021] [mpm_prefork:notice] [pid 2901] AH00170: caught SIGWINCH, shutting down gracefully
[Tue Jun 15 12:23:56.143046 2021] [suexec:notice] [pid 2899] AH01232: suEXEC mechanism enabled (wrapper: /usr/sbin/su
exec)
```


aws re/start

The first log in the /var/log/YUM.log log file lists programs that were installed or updated. (YUM is a package management utility to install, update, and remove software.)

The second is the log file of the httpd, a web server service.

Logging levels

Severity Level	Identification	Description
0	EMERGENCY	Logs messages when the system becomes unstable
1	ALERT	Logs when immediate action is needed
2	CRITICAL	Logs only messages for critical errors; the system may become unusable
3	ERROR	Logs only messages that indicate non-critical error conditions or more serious messages
4	WARN	Logs only messages that are warnings or more serious messages (usually the default log level on Linux distributions)
5	NOTICE	Logs messages for normal events but of significant importance
6	INFO	Logs all informational messages and more serious messages
7	DEBUG	Logs all debug-level and INFO messages

6

aws re/start

These logging levels are the logs that the Linux operating system offers. Some programs or libraries may offer fewer logging levels, such as debug, info, warning, and error, with a default logging level set to info.

The logs of the current logging level and higher levels are displayed. For example, when choosing WARN, level 4, the logs of NOTICE, INFO and DEBUG are also displayed.

cat, less, more, tail, and **head** are all commands that are useful to read logs. Using the pipe redirector **|** and **grep** is an efficient way to look for a specific pattern in a log.

You can also open the files using editors such as vi or gedit.

Using grep to search log files

- The grep command searches the given file for lines that contain a match to the specified strings or words.
- Add the grep command when you look for a specific string of text in log files.
- grep is one of the most useful commands in Linux.
- The following are examples:
  - `cat yourlog.log | grep ERROR`
  - `tail -f yourlog.log | grep error`
  - `sudo cat /tmp/log/secure | grep LOGIN > SharedFolders/logins.csv`

```
[ec2-user]$ sudo tail /var/log/secure | grep "invalid user"
Jun 22 14:45:45 ip-172-31-27-186 sshd[1131]: input_userauth_request: invalid user ec3-user [preauth]
Jun 22 14:45:59 ip-172-31-27-186 sshd[1137]: input_userauth_request: invalid user ec4-user [preauth]
[ec2-user]$
```

8

aws re/start

The following are some more details on these errors.

- **cat yourlog.log | grep ERROR**: searches for the ERROR message in the yourlog.log file and displays the matching lines of the file in the console (reads the content of the yourlog.log file and redirects it to the grep command that searches for the word ERROR).
- **tail -f yourlog.log | grep error**: searches the word error in the last 10 lines of the yourlog.log file and displays the matching lines of the file in the console (reads the last 10 lines of the yourlog.log file and redirects it to the grep command that searches for the word error; remember that without any additional option, tail reads the last 10 lines of a file).
- **sudo cat /var/log/secure | grep LOGIN > SharedFolders/logins.csv**: searches the word LOGIN in the file /var/log/secure and writes the matching lines of the file in the file SharedFolders/logins.csv. Sudo is required to access the /var/log/secure file.

Where does Linux store log files?

- Linux and applications normally store log files in the /var/log directory.
- The /var directory is used to store files that might rapidly and unpredictably change in size.

```
[ec2-user]$ ls /var/log
amazon                btmp-20210601          grubby                 messages-20210530  spooler-20210530
audit                 chrony                 grubby_prune_debug     messages-20210606  spooler-20210606
boot.log              cloud-init.log         httpd                  messages-20210613  spooler-20210613
boot.log-20210616     cloud-init-output.log  journal                messages-20210620  spooler-20210620
boot.log-20210617     cron                   lastlog                sa                 tallylog
boot.log-20210618     cron-20210530          maillog                secure             wtmp
boot.log-20210619     cron-20210606          maillog-20210530       secure-20210530    yum.log
boot.log-20210620     cron-20210613          maillog-20210606       secure-20210606
boot.log-20210621     cron-20210620          maillog-20210613       secure-20210613
boot.log-20210622     dmesg                  maillog-20210620       secure-20210620
btmp                  dmesg.old              messages               spooler
[ec2-user]$
```

9

aws re/start

Linux usually stores log files in the /var/log directory.

Important log files

Log File	Description
/var/log/syslog	Stores system information
/var/log/secure	Stores authentication information for Red Hat-derived distributions
/var/log/kern	Stores Linux kernel information
/var/log/boot.log	Stores startup messages
/var/log/maillog	Stores mail messages
/var/log/daemon.log	Stores information about running background services
/var/log/auth.log	Stores authentication information for Debian-derived distributions
/var/log/cron.log	Stores cron messages for scheduled tasks
/var/log/httpd	Stores Apache information for Red Hat-derived distributions

aws re/start

Other important log files include the following:

- /var/log/YUM: Stores YUM installer information for Red Hat-derived distributions
- /var/log/apache2/access.log: Stores Apache authentication information for Debian-derived distributions
- /var/log/lastlog: Stores information about successful logins to the host

The `lastlog` command

Reports recent login information for the system

Can report all logins or login information for a specific user

All users

```
Username         Port     From             Latest
ec2-user         pts/0    72-21-198-64.ama Wed Jun 23 08:10:16 +0000 2021
mmajor           pts/0                     Tue Jun 22 09:31:07 +0000 2021
jdoe             pts/0                     Mon Jun 21 08:25:22 +0000 2021
```

Specific user

```
Username         Port     From             Latest
ec2-user         pts/0    72-21-198-64.ama Wed Jun 23 08:10:16 +0000 2021
```

11

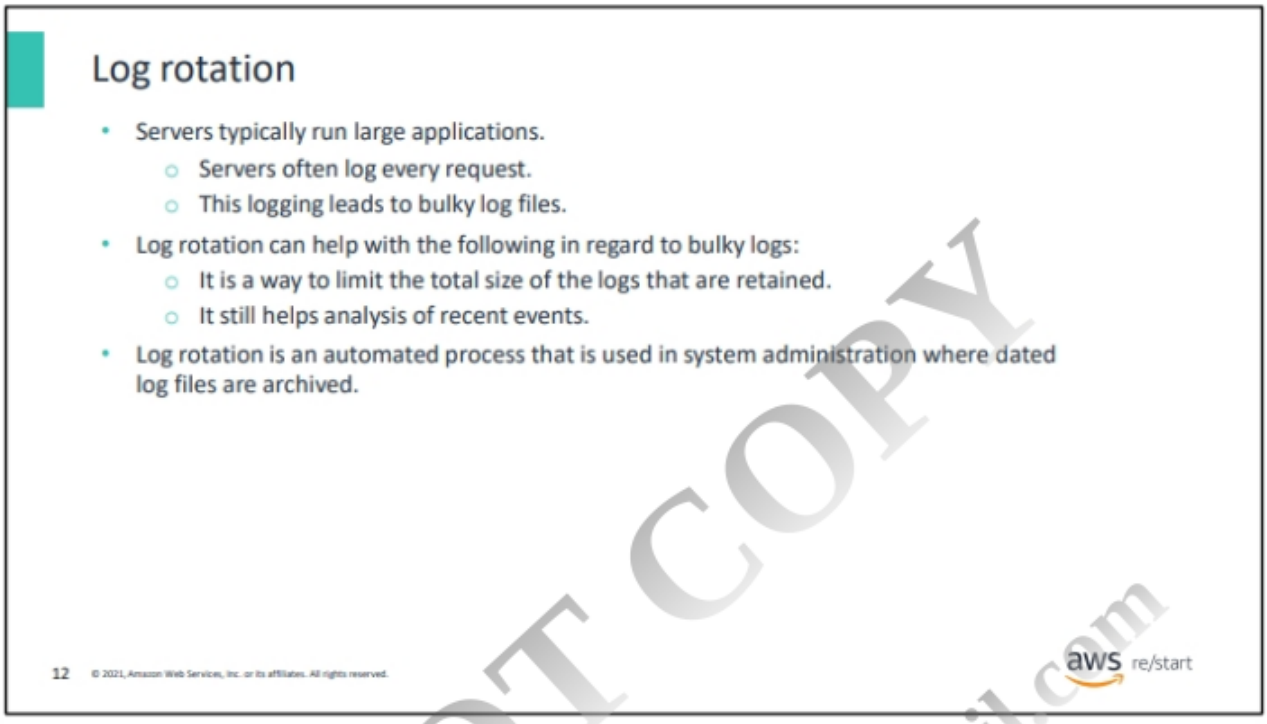
aws re/start

The **lastlog** command retrieves user information from the **/var/log/lastlog** file and outputs it in the console.

lastlog –u ec2-user displays information of the ec2-user only.

lastlog –t 1 displays login information more recent than 1 day ago.

Use **man lastlog** for more options.



Log rotation is not activated by default.

With the **logrotate** utility, you can compress, rename, or clean up the log files.

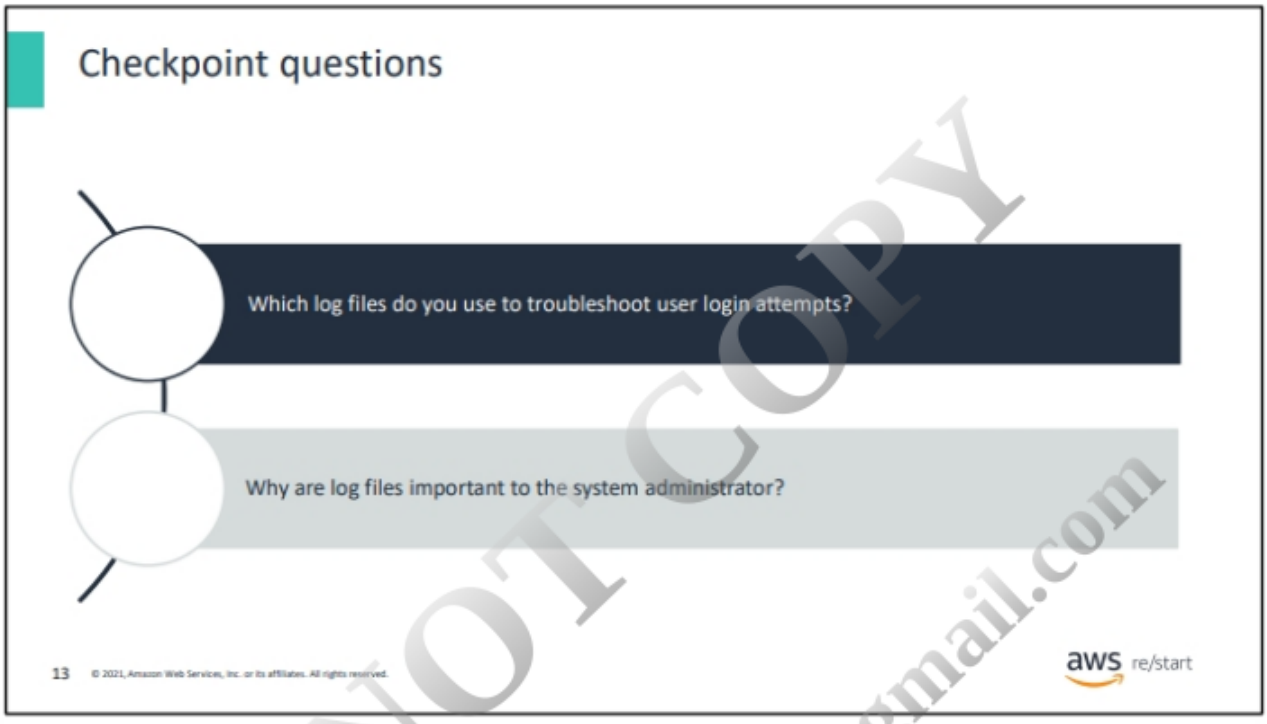
You can activate log rotation according to the log file size: if the log file is more than a specific size, it will be renamed xxxxx.log-20210612 (if it is renamed on June 21, 2021). The default date format is **yyyymmdd**.

It can also be activated on a regular basis (weekly, daily or monthly).

A maximum number of log files to keep can be set: if the maximum number of logs is reached, the logs are erased, moved, or emailed.

You can also compress log files.

You can individually tailor log rotation for different kinds of logs.



1. You use either **/var/log/auth.log** or **/var/log/secure** depending on whether the system is Debian-derived or Red Hat-derived.
2. Log files are running records of what is occurring on a system. These records include authentication and also logs from programs, status of services, and many other server events.

Some key takeaways from this lesson include:

- You use logging to record events that are happening with the system.
- Log files can become large. To keep the logs manageable, use log rotation to routinely save files.
- You can control the amount of detail in the logs with logging levels.