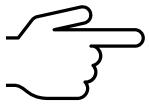
AUDIT OPERATING SYSTMS

DAILY, WEEKLY, MONTHLY

Asfaw Gedamu Haileselasie



Caution: Please use the commands with care, try them on test environments first.

Here are some Linux scripts that you can use to audit daily, weekly, and monthly OS server activities:

Daily audit

```
# Get a list of all users who have logged in today
echo "Getting a list of all users who have logged in today..."

lastlog | awk '{print $1}' | sort | uniq

# Get a list of all processes that are running today
echo "Getting a list of all processes that are running today..."

ps -ef | awk '{print $1}' | sort | uniq

# Get a list of all files that have been modified today
echo "Getting a list of all files that have been modified
today..."

find . -type f -mtime -1

# Get a list of all logins that have failed today
echo "Getting a list of all logins that have failed today..."

faillog | awk '{print $1}' | sort | uniq
```

Weekly audit

```
# Get a list of all users who have logged in this week
echo "Getting a list of all users who have logged in this
week..."
```

```
lastlog | awk '{print $1}' | sort | uniq -c | sort -n

# Get a list of all processes that are running this week
echo "Getting a list of all processes that are running this
week..."

ps -ef | awk '{print $1}' | sort | uniq -c | sort -n

# Get a list of all files that have been modified this week
echo "Getting a list of all files that have been modified this
week..."

find . -type f -mtime -7

# Get a list of all logins that have failed this week
echo "Getting a list of all logins that have failed this
week..."

faillog | awk '{print $1}' | sort | uniq -c | sort -n
```

Monthly audit

```
# Get a list of all users who have logged in this month
echo "Getting a list of all users who have logged in this month..."

lastlog | awk '{print $1}' | sort | uniq -c | sort -n | head -10

# Get a list of all processes that are running this month
echo "Getting a list of all processes that are running this month..."

ps -ef | awk '{print $1}' | sort | uniq -c | sort -n | head -10

# Get a list of all files that have been modified this month
echo "Getting a list of all files that have been modified this month..."

find . -type f -mtime -30

# Get a list of all logins that have failed this month
echo "Getting a list of all logins that have failed this month..."

faillog | awk '{print $1}' | sort | uniq -c | sort -n | head -10
```

These scripts will run the same Linux commands that I mentioned earlier, but they will be run from a Linux shell script. This allows you to run the scripts from a cron job or other scheduling mechanism.

To run the scripts, you will need to save them as `daily_audit.sh`, `weekly_audit.sh`, and `monthly_audit.sh`. You will also need to create a user account with the appropriate permissions to run the scripts.

Once you have done that, you can run the scripts by running the following commands:

Bash

```
# Run the daily audit script
./daily_audit.sh

# Run the weekly audit script
./weekly_audit.sh

# Run the monthly audit script
./monthly_audit.sh
```

The scripts will output the results of the audit to the console. You can also save the results to a file by redirecting the output of the script to a file.

For example, to save the results of the daily audit to a file called `daily_audit.log`, you would run the following command:

Bash

```
./daily_audit.sh > daily_audit.log
```