# LAB-06. Reviewing System Logs and Updating the journald Configuration

## Introduction

In this hands-on lab, you will be reviewing the secure log located in the /var/log directory to check for any critical issues and will make a backup copy of the current log file in your home directory. After backing up the secure log, you will check to see if the system journals are configured to be persistent. If not, update the configuration to be persistent and limit the size of the journal files.

## Solution

Log in to the lab server using the credentials provided:

ssh cloud\_user@<PUBLIC\_IP\_ADDRESS>

**Note:** *When copying and pasting code into Vim from the lab guide, first enter :set paste (and then i to enter insert mode) to avoid adding unnecessary spaces and hashes. To save and quit the file, press* ***Escape*** *followed by :wq. To exit the file* ***without*** *saving, press* ***Escape*** *followed by :q!.*

**Review the /var/log/secure Log File for Any Critical Authorization Issues**

1. Use the less command to view the file:

sudo less /var/log/secure

1. Scroll down the file screen by screen by using the PAGE DOWN key.
2. Jump to the end of the file and tail it for a bit to view inbound traffic(**Note:** Press Ctrl+C to interrupt and q to quit in less):

Shift + F

**Create a Backup of the /var/log/secure Log File**

1. Create a log\_archive directory in your home directory:

mkdir log\_archive

1. Copy the /var/log/secure file to the log\_archive directory while preserving attributes and contexts:

sudo cp --preserve=context /var/log/secure log\_archive

**Determine If Journals Are Configured to Be Persistent**

1. Confirm the /var/log/journal directory exists:

ls -l /var/log

1. Create the /var/log/journal directory:

sudo mkdir /var/log/journal

1. Confirm journal data is being written to the directory:

ls -l /var/log/journal

**Update the journald Configuration to Limit the Size of Journal Files**

1. Review the /etc/systemd/journald.conf.

sudo vi /etc/systemd/journald.conf

1. Add SystemMaxUse=50M to the end of the configuration file:

SystemMaxUse=50M

1. Write out and close the file:

:wq

1. Cycle the journald service:

sudo systemctl restart systemd-journald

## Conclusion

Congratulations — you've completed this hands-on lab!