# Placement Empowerment Program

***Cloud Computing and DevOps Centre***

Write the Shell Script to Monitor Logs : Create a script that monitors server logs for errors and alert you

Name: Jai Riyaz G

Department: ADS



# Introduction

Log files play a critical role in IT systems, as they record activities and events generated by applications, servers, and network devices. Monitoring these logs helps identify issues such as errors, warnings, and suspicious activities that may require immediate attention. Automating the monitoring process ensures efficiency and reduces the risk of missing critical information.

This PoC demonstrates the creation of a **PowerShell script** to monitor logs in real-time. The script will detect specific keywords (like "error") in a log file and alert the user when such events occur.

# Overview

This project involves writing and running a PowerShell script that continuously scans a log file for specific keywords. The script:

1. Reads the log file in real time.
2. Matches new entries in the log against predefined keywords (e.g., "error").
3. Triggers an alert when a match is found.

This solution is lightweight and practical for system administrators and IT professionals to monitor logs on Windows systems.

# Importance

## 1. Proactive Issue Detection

By monitoring logs in real time, this project helps detect errors and issues as they occur, reducing downtime and improving system reliability.

## 2. Learning Automation Tools

This project introduces PowerShell scripting, a powerful automation tool, to beginners. It provides hands-on experience with practical applications.

# Step-by-Step Overview

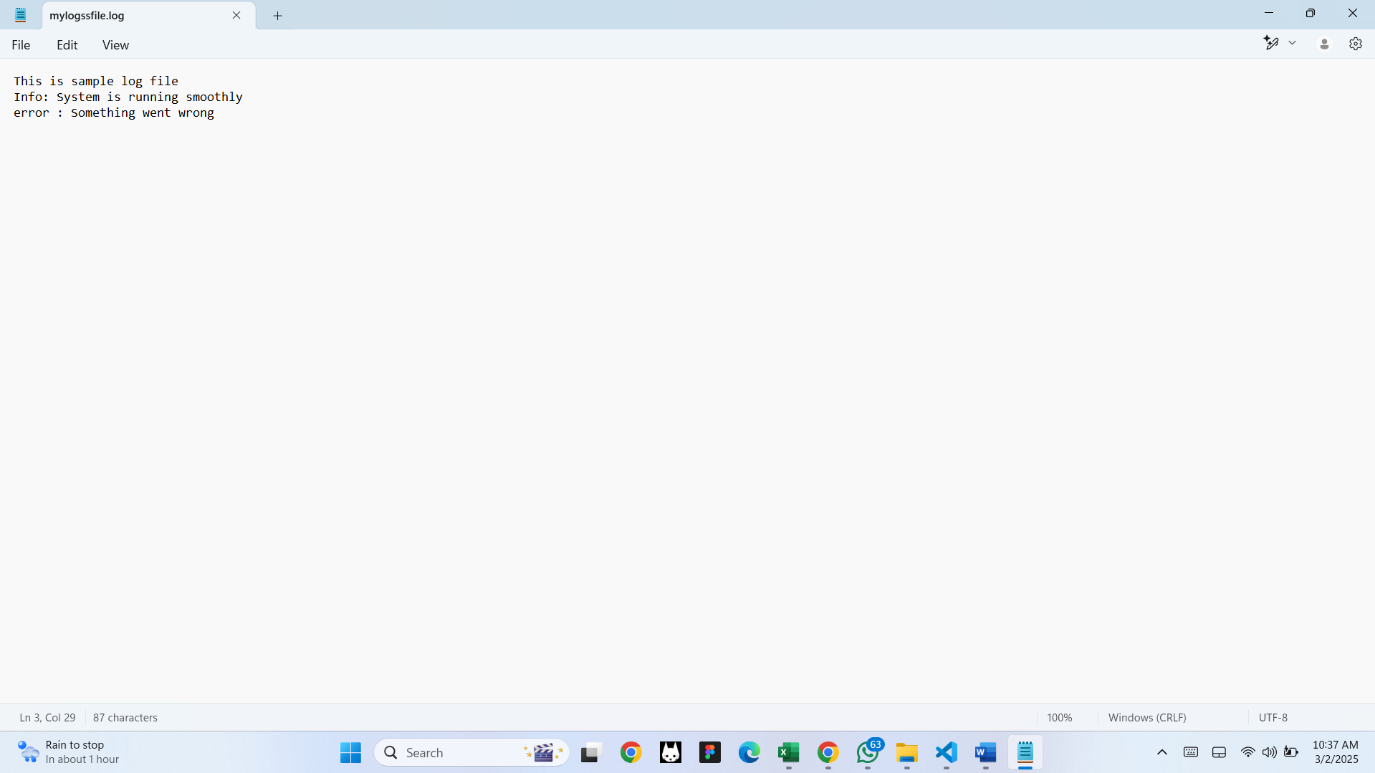
Step 1:

Create a Folder called logs for Your Logs and Script



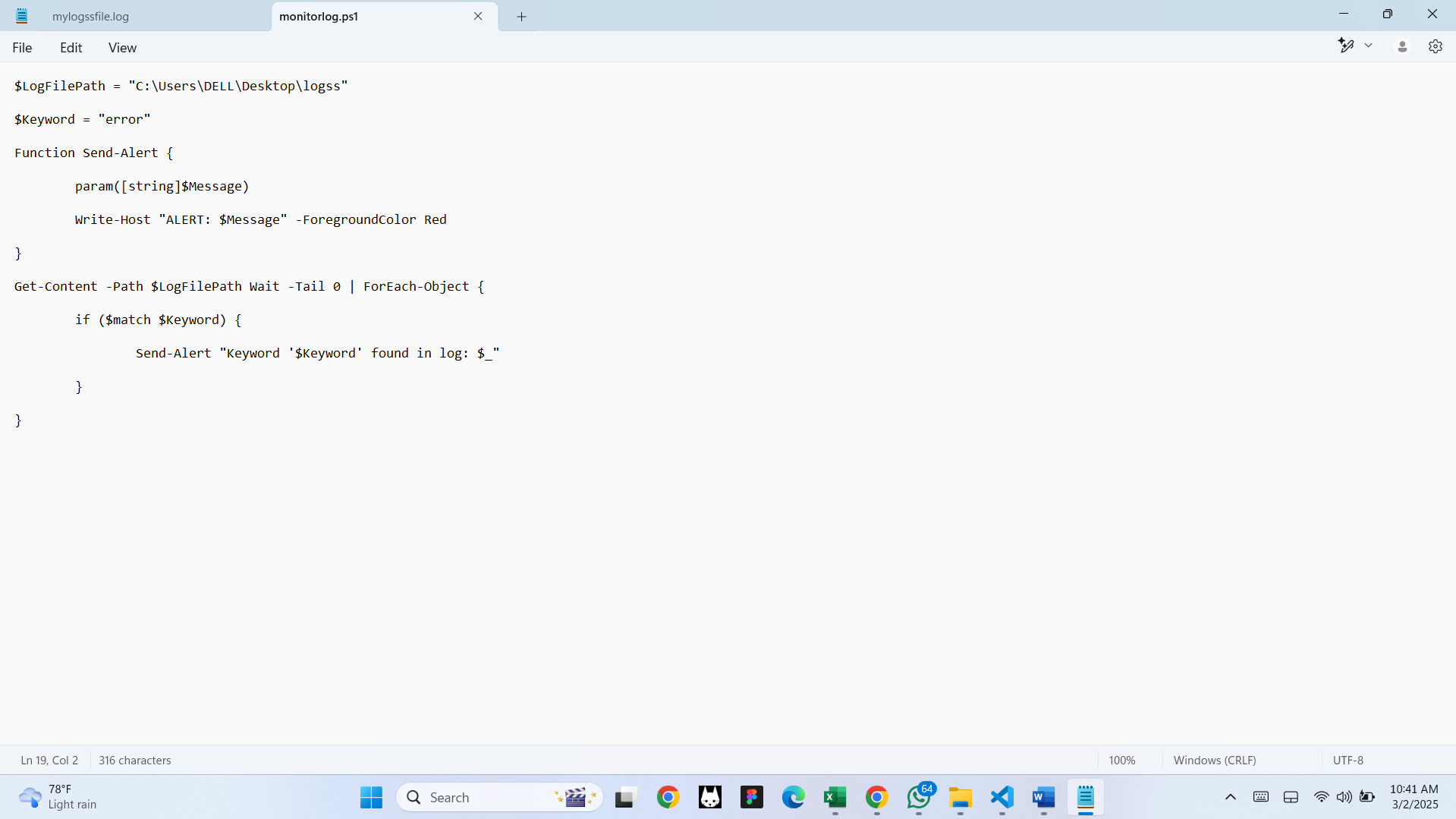
Step 2:

Open Notepad and Add the following sample text to it and Save the file as **mylogssfile.log** inside the logs folder



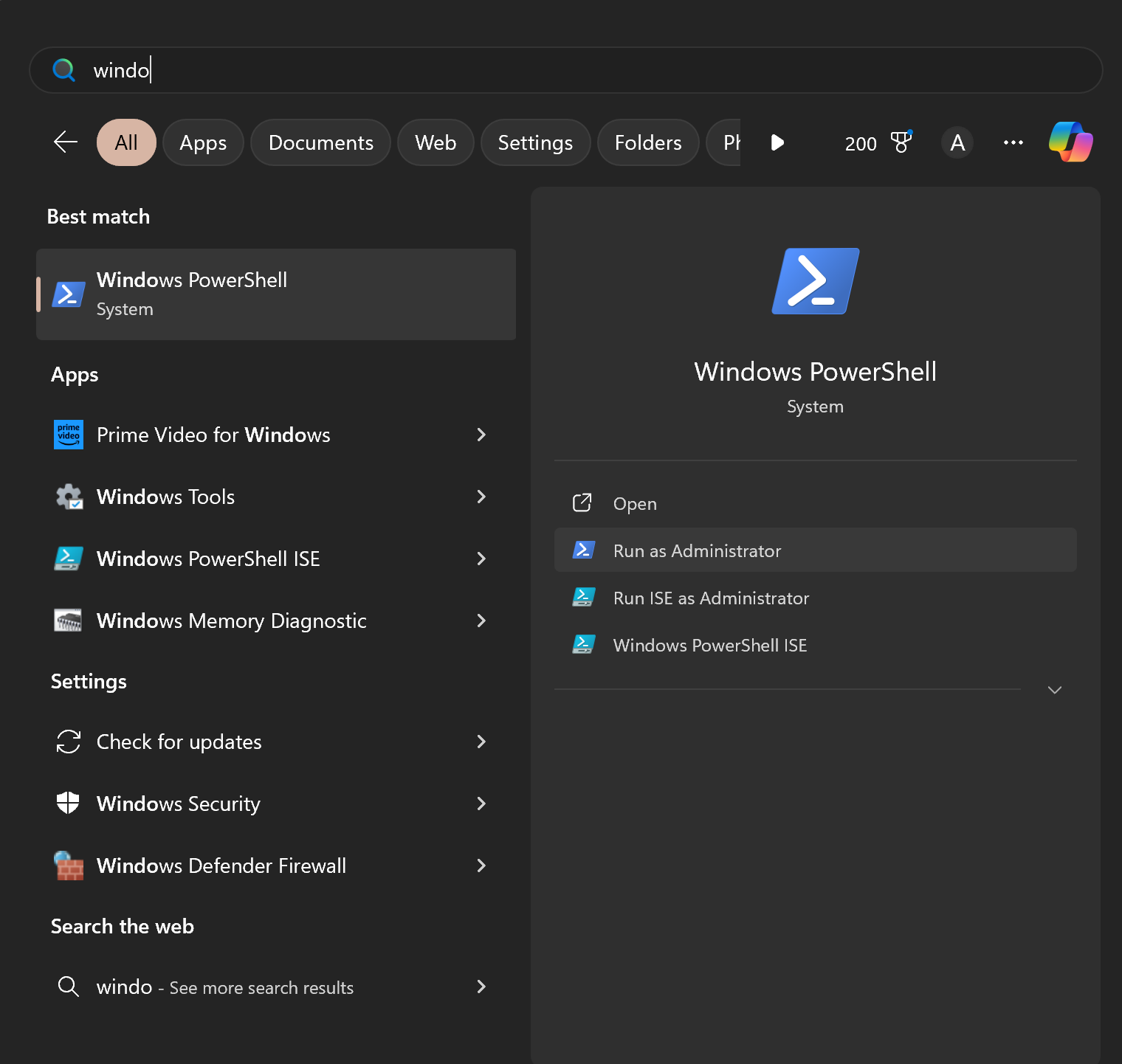
Step 3:

Open Notepad and Type the following PowerShell script into it and Set the $LogFilePath address to the mylogfile.log which you saved in logs folder. Save the file as monitorlog.ps1 inside the same logs folder



Step 4:

Click the Windows Key and Search for Windows PowerShell and click Run as Administrator.

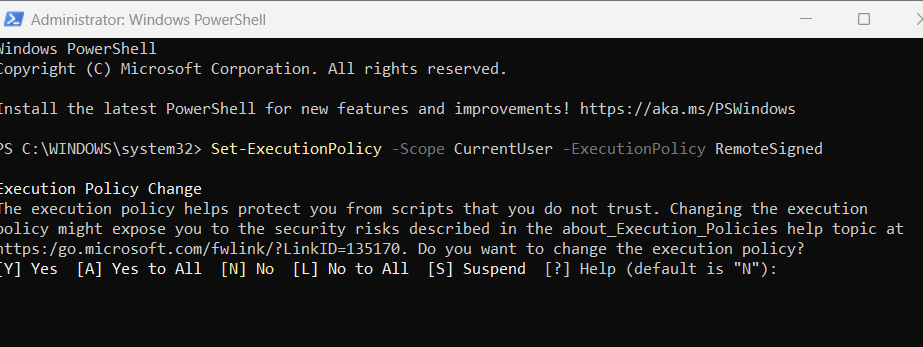


Step 5:

Run the following command to allow script execution:

## Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned

When prompted, type Y and press Enter.



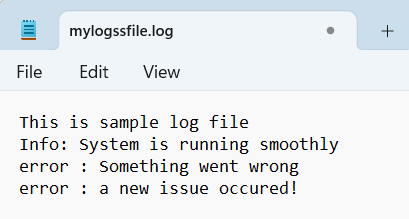
Step 6:



Step 7:

Open mylogfile.log in Notepad and Add a new line with the word

"error" and Save the file.



Step 9:

Check PowerShell — you should see an alert like:

**ALERT: Keyword 'error' found in log: error: A new issue occurred!**



Explanation:

1. When the script is running, it continuously monitors the log file.

1. If any line containing the keyword "error" is added to the file, it immediately triggers an alert in PowerShell.

Outcome:

By completing this Proof of Concept (PoC), we will:

* 1. Successfully create and execute a PowerShell script to monitor log files in real time.
  2. Detect and alert on predefined keywords (e.g., "error") to highlight critical events.
  3. Gain hands-on experience with PowerShell scripting and automation on a Windows system.
  4. Understand the importance of log monitoring in proactive system maintenance and troubleshooting.
  5. Learn to customize and scale the script for more advanced monitoring scenarios in future projects.