**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name: Jeslin Anista J

Department : EEE



**Introduction and Overview**

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 occurs.

**Objective**

The objective of this project is to:

1. Automate the process of monitoring log files for critical events.

2. Learn how to create and execute PowerShell scripts on a Windows system.

3. Demonstrate real-time detection of keywords like "error" in log files.

4. Enhance troubleshooting efficiency by providing immediate alerts for critical events.

**Importance of Storage Bucket(S3)**

1. **Proactive Issue Detection**

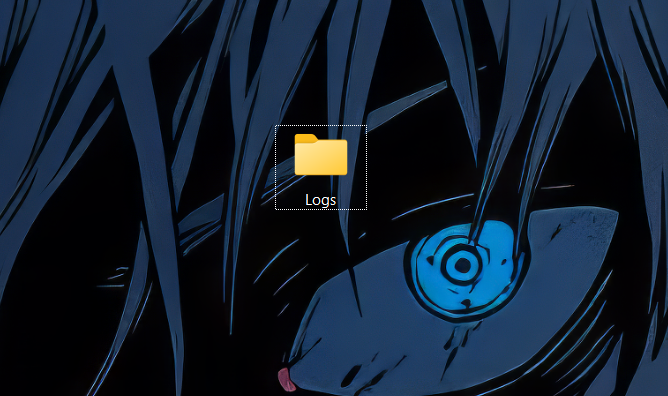
By monitoring logs in real time, this project helps detect errors and issues as they occur, reducing downtime and improving system reliability.

1. **Learning Automation Tools** This project introduces PowerShell scripting, a powerful automation tool, to beginners. It provides hands-on experience with practical applications.
2. **Cost-Effective Solution** Using PowerShell eliminates the need for expensive third-party monitoring tools while still achieving effective log monitoring.
3. **Time Efficiency** Automation saves significant manual effort in scanning logs, allowing IT professionals to focus on resolving issues.
4. **Scalability** The script can be adapted to monitor multiple log files or handle complex use cases, making it a foundational step toward advanced automation.

**Step-by-Step Overview**

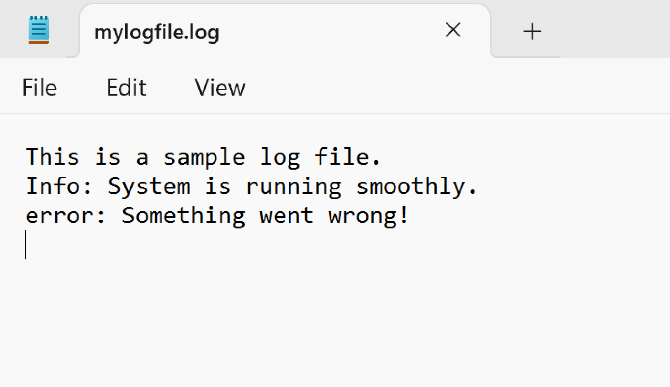
Step1:

Create a folder called logs for Your Logs and Script.

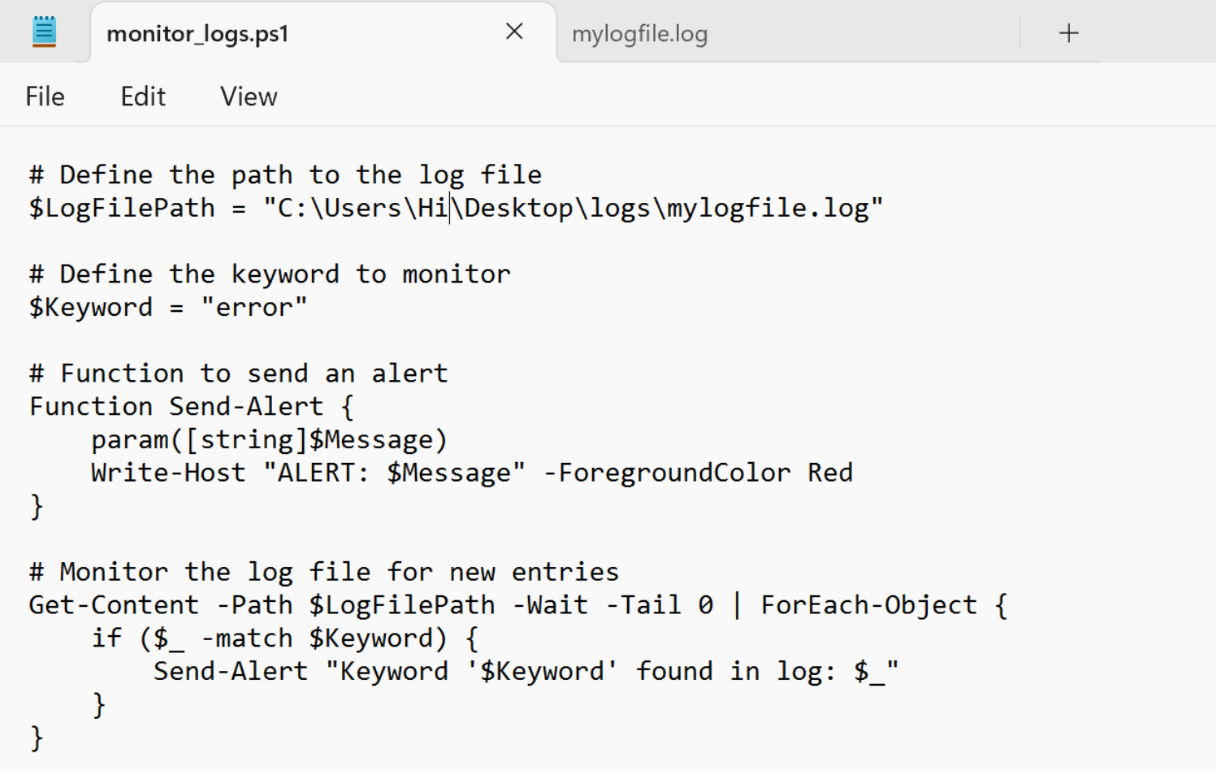


Step 2 :

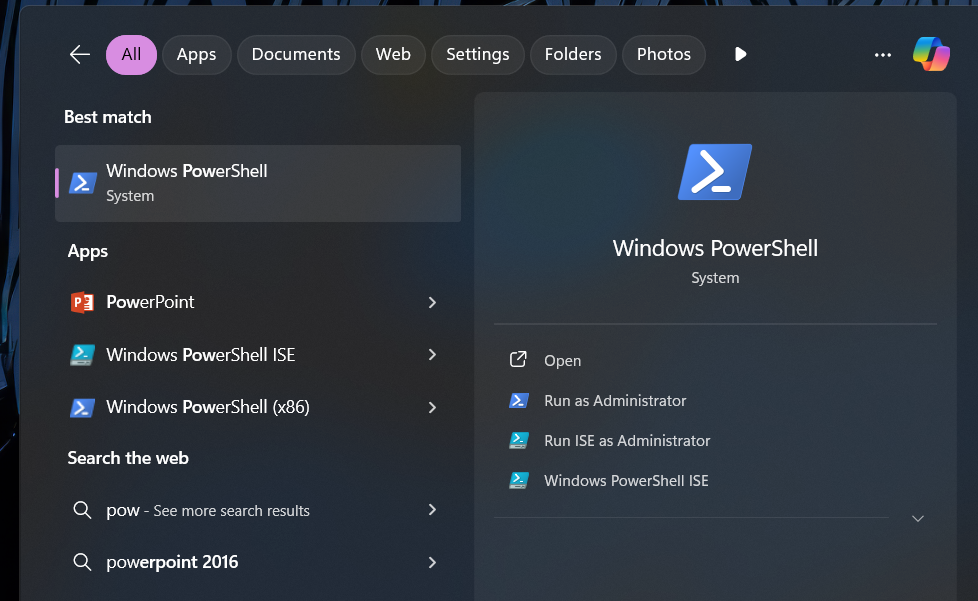
Open Notepad and Add the following sample text to it and Save the file as **mylogfile.log** inside the logs folder).



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 monitor\_logs.ps1 inside the same logs folder

Step 4 :

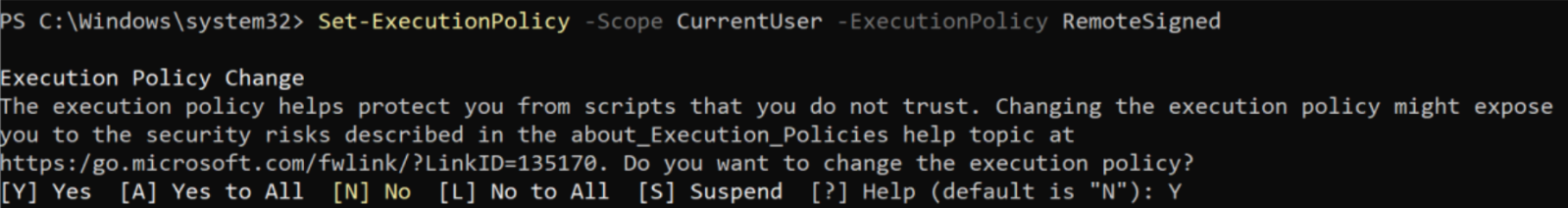
Click the Windows Key and Search for Windows PowerShell and click Run as Administrator.

Step 5 :

Run the following command to allow script execution:

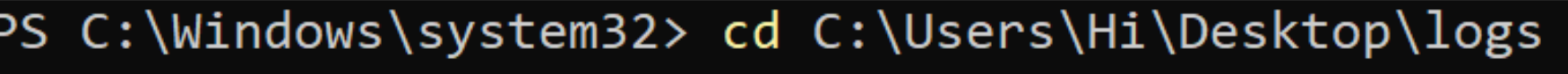
**Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned**

When prompted, type Y and press Enter.



Step 6 :

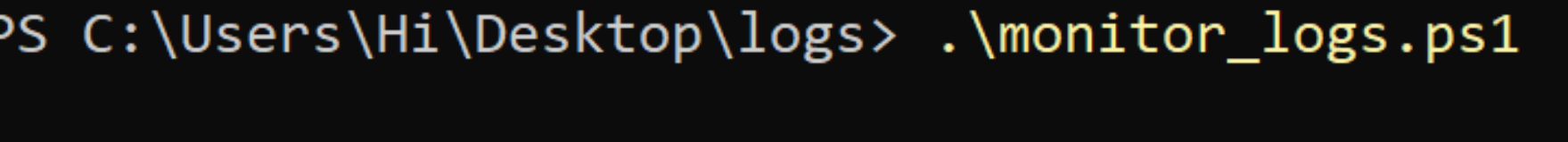
Navigate to the logs folder.



Step 7 :

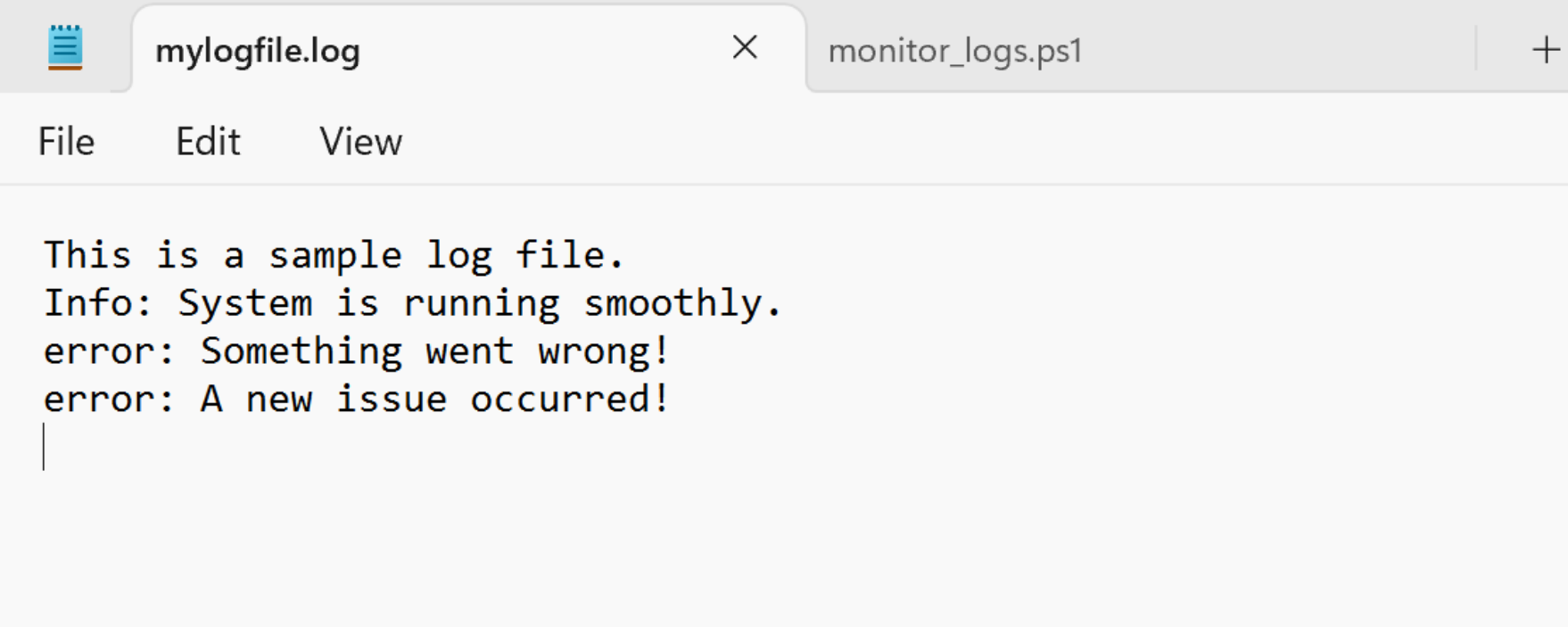
Run the script:

**.\monitor\_logs.ps1**



Step 8 :

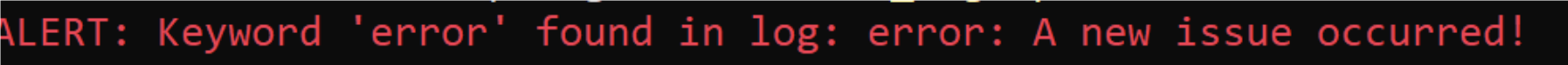
Open mylogfile.log in Notepad and Add a new line with the word "error" and Save the file.



Step 9 :

Check PowerShell — you should see an alert like:

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



**Expected 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.