

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: **Priyadharshini S**

Department: **ADS**

Introduction

Log files are critical for IT systems as they record events and activities generated by applications, servers, and network devices. Monitoring these logs helps identify errors, warnings, and suspicious activities requiring immediate attention. Automating log monitoring ensures efficiency and reduces the risk of missing critical information.

This Proof of Concept (PoC) demonstrates the creation and execution of a PowerShell script to monitor log files in real-time. The script detects specific keywords (e.g., "error") in a log file and alerts the user upon finding such events.

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.

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

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.

3. Cost-Effective Solution

Using PowerShell eliminates the need for expensive third-party monitoring tools while still achieving effective log monitoring.

4. Time Efficiency

Automation saves significant manual effort in scanning logs, allowing IT professionals to focus on resolving issues.

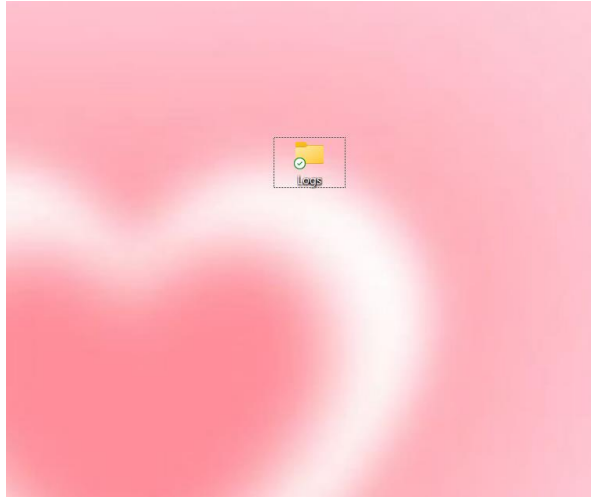
5. Scalability

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

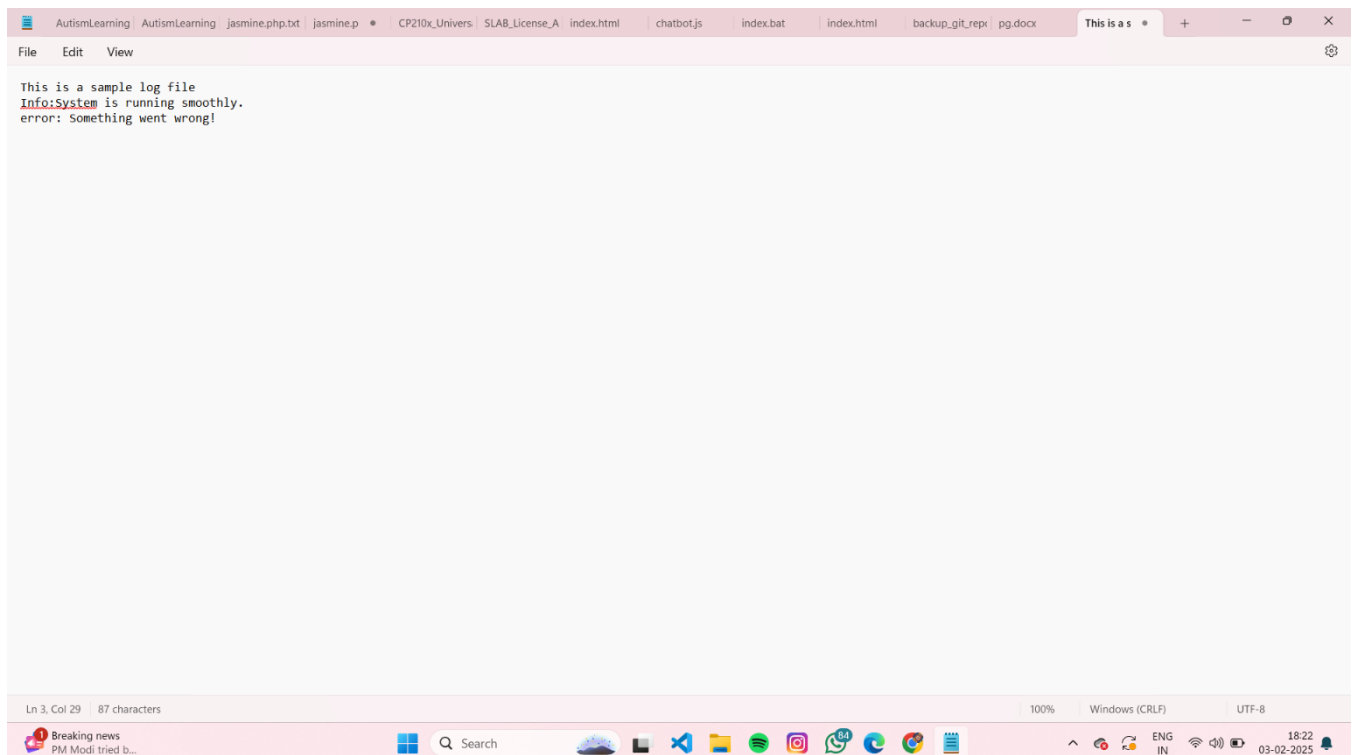
Step 1:

Create a Folder called logs for Your Logs and Script

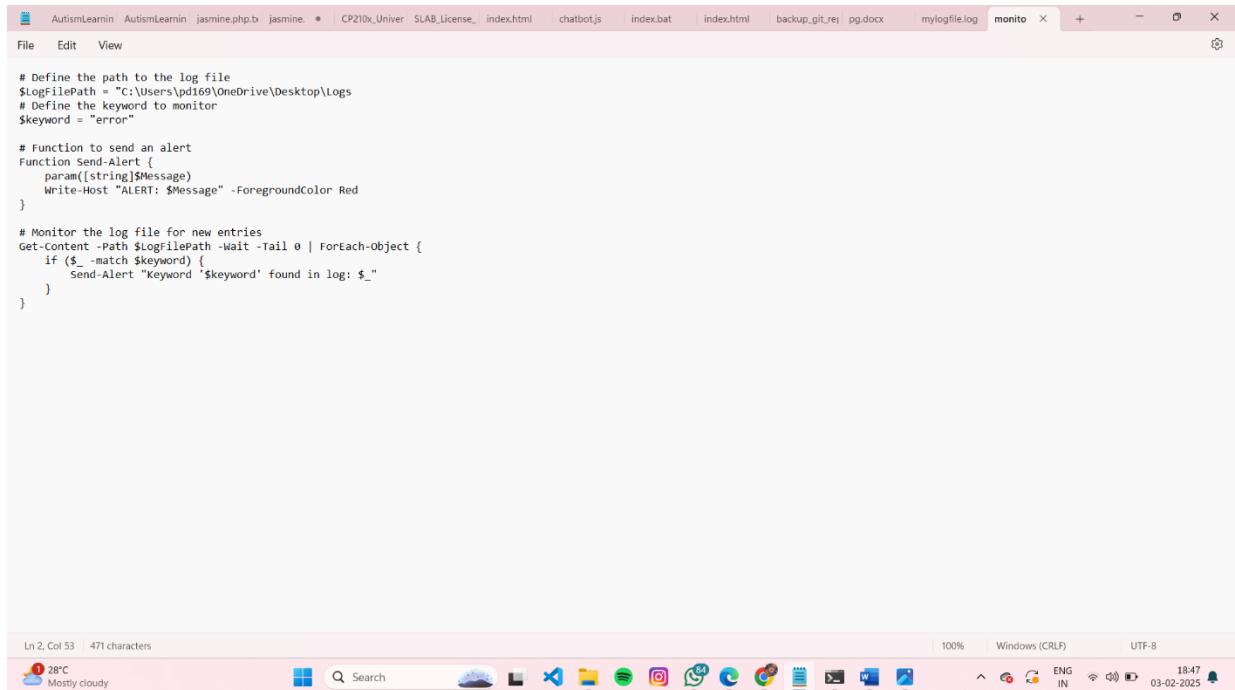


Step 2:

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



Step 3:



The screenshot shows a Notepad window with a tab titled 'monito'. The script is a PowerShell function designed to monitor a log file for a specific keyword and send an alert when it is found. The script is as follows:

```
# Define the path to the log file
$LogFilePath = "C:\Users\pd169\OneDrive\Desktop\Logs
# Define the keyword to monitor
$keyword = "error"

# Function to send an alert
function Send-Alert {
    param([string]$Message)
    Write-Host "ALERT: $Message" -ForegroundColor Red
}

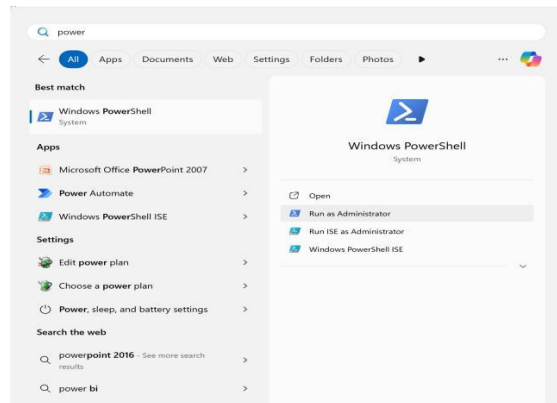
# Monitor the log file for new entries
Get-Content -Path $LogFilePath -Wait -Tail 0 | ForEach-Object {
    if ($_ -match $keyword) {
        Send-Alert "keyword '$keyword' found in log: $_"
    }
}
```

The status bar at the bottom of the Notepad window indicates 'Ln 2, Col 53', '471 characters', '100%' zoom, 'Windows (CRLF)' line endings, and 'UTF-8' encoding. The Windows taskbar is visible at the bottom, showing the date as 03-02-2025 and the time as 18:47.

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:

When prompted, type Y and press Enter.

```
PS C:\Users\pd169> cd "C:\Users\pd169\OneDrive\Desktop\Logs"
PS C:\Users\pd169\OneDrive\Desktop\Logs> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned
PS C:\Users\pd169\OneDrive\Desktop\Logs> cd "C:\Users\pd169\OneDrive\Desktop\Logs"
```

Step 6:

Navigate to the logs folder

```
PS C:\Users\pd169\OneDrive\Desktop\Logs> cd "C:\Users\pd169\OneDrive\Desktop\Logs"
```

Step 7:

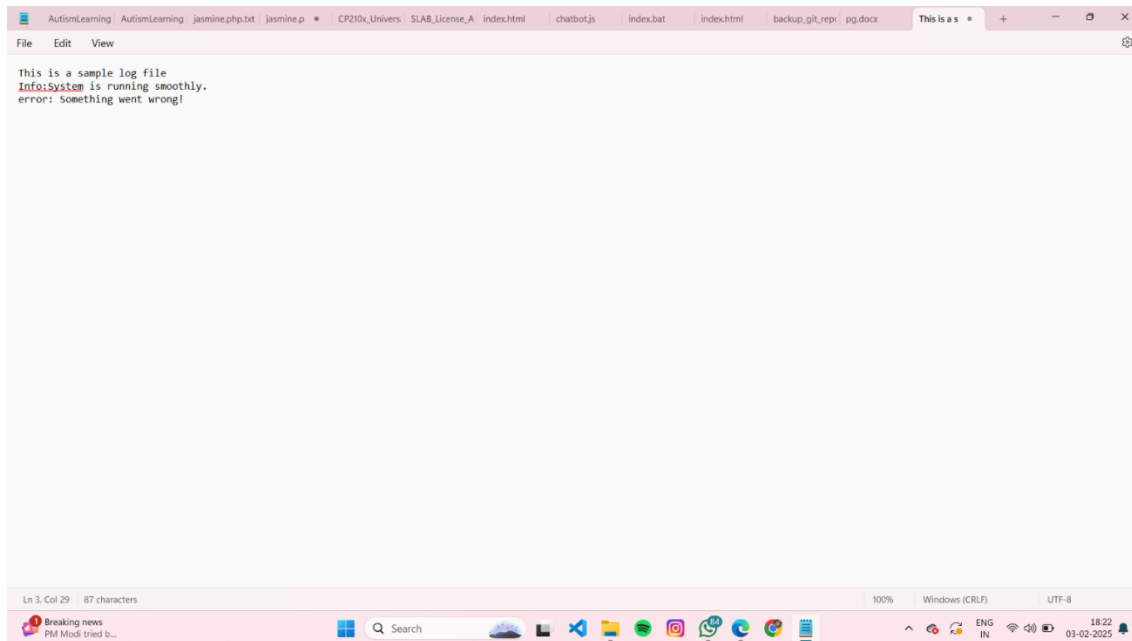
Run the script:

.\monitor_logs.ps1

```
PS C:\Users\pd169\OneDrive\Desktop\Logs> .\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!

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

Explanation:

1. When the script is running, it continuously monitors the log file.
2. 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.