



St. JOSEPH'S
GROUP OF INSTITUTIONS
OMR, CHENNAI - 119



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: Nantha Krishnan.G.K.

Department:AML



Introduction

Log files are essential in IT systems as they capture activities and events generated by applications, servers, and network devices. Monitoring these logs is crucial for identifying issues such as errors, warnings, and suspicious activities that may require prompt attention. Automating the monitoring process increases efficiency and minimizes the risk of overlooking important information.

This PoC showcases the development of a PowerShell script to monitor logs in real-time. The script will continuously scan a log file for specific keywords (such as "error") and alert the user whenever such events are detected.

Overview

This project involves creating and executing a PowerShell script that continuously monitors a log file for specific keywords. The script will:

- Read the log file in real-time.
- Compare new entries in the log against predefined keywords (such as "error").
- Trigger an alert whenever a match is found.

This solution is both lightweight and efficient, making it an ideal tool 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.

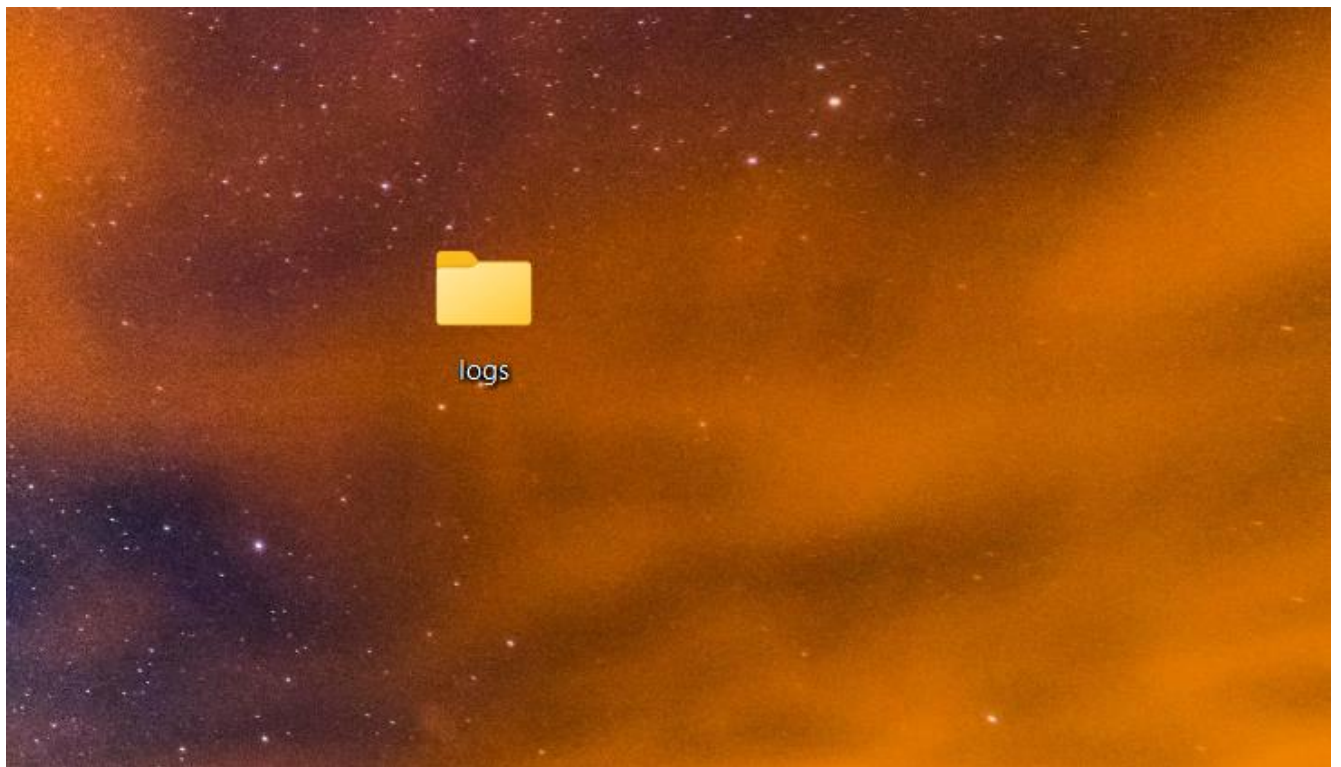
5. Scalability

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

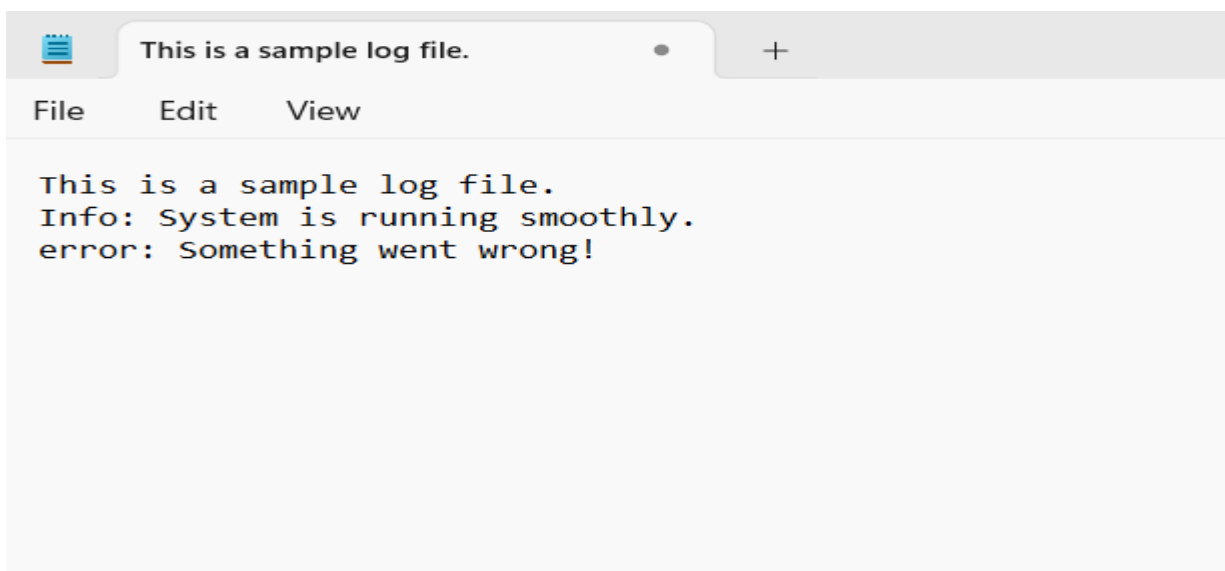
Step 1:

Create a Folder called logs for Your Logs and Script



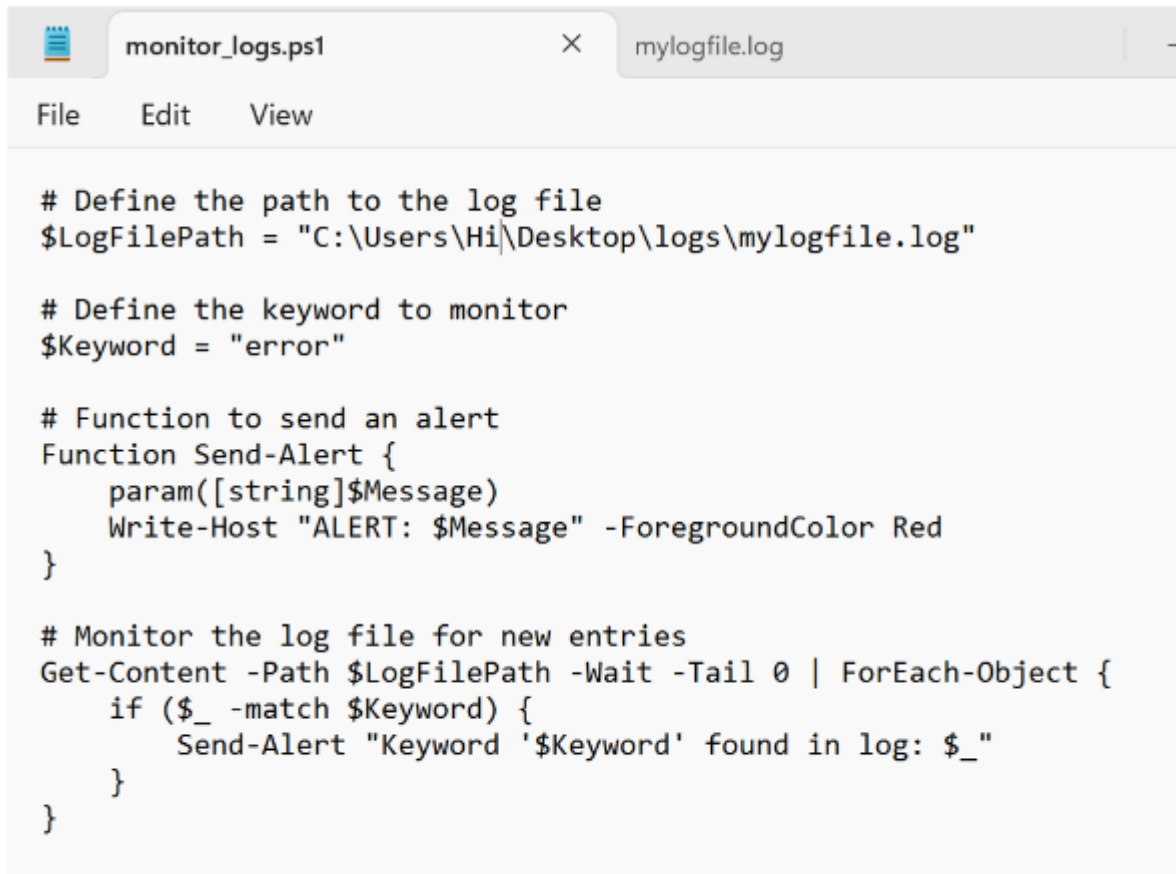
Step 2:

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



Step 3:

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

A screenshot of a Notepad application window. The title bar shows two tabs: 'monitor_logs.ps1' (active) and 'mylogfile.log'. The menu bar includes 'File', 'Edit', and 'View'. The script content is as follows:

```
# Define the path to the log file
$LogFilePath = "C:\Users\Hi\Desktop\logs\mylogfile.log"

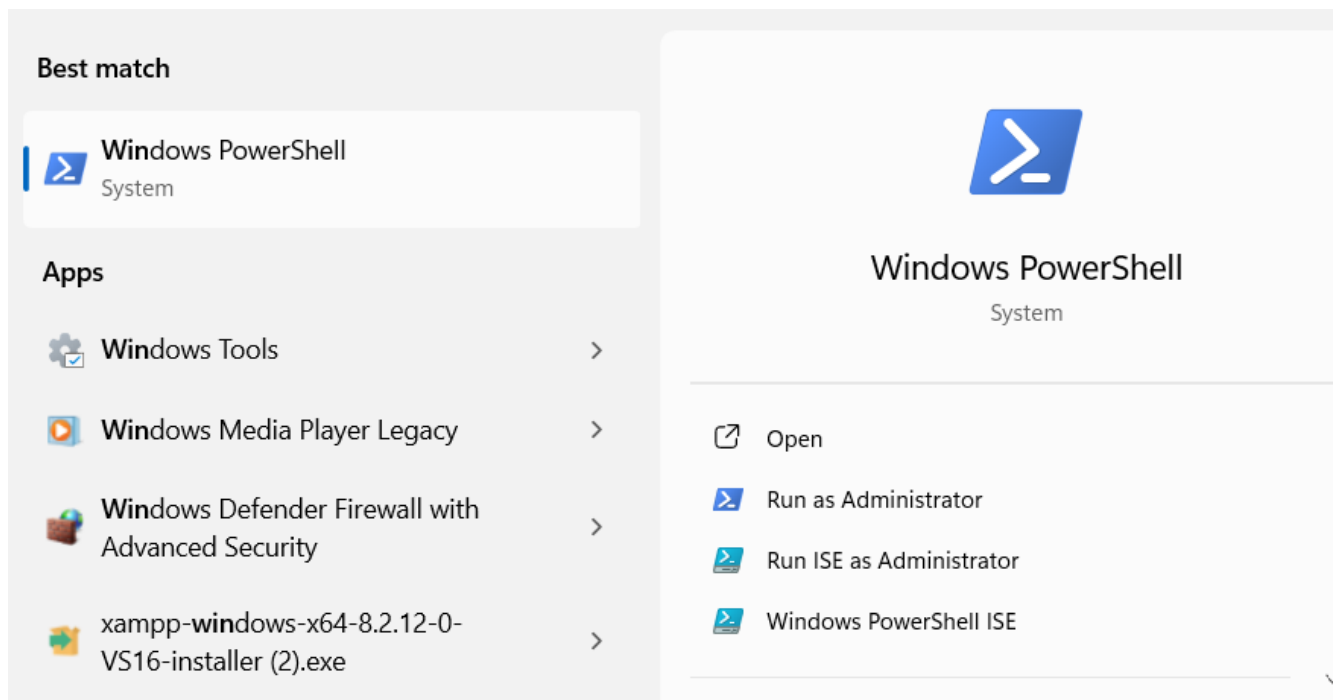
# Define the keyword to monitor
$Keyword = "error"

# 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: $_"
    }
}
```

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.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\windows\system32> Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy RemoteSigned

Execution Policy Change
The execution policy helps protect you from scripts that you do not trust. Changing the execution policy might expose
you to the security risks described in the about_Execution_Policies help topic at
https://go.microsoft.com/fwlink/?LinkID=135170. Do you want to change the execution policy?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "N"): Y
```

Step 6:

Navigate to the logs folder

```
PS C:\windows\system32> cd "C:\Users\Nantha Krishnan\Downloads\logs"  
PS C:\Users\Nantha Krishnan\Downloads\logs> █
```

Step 7:

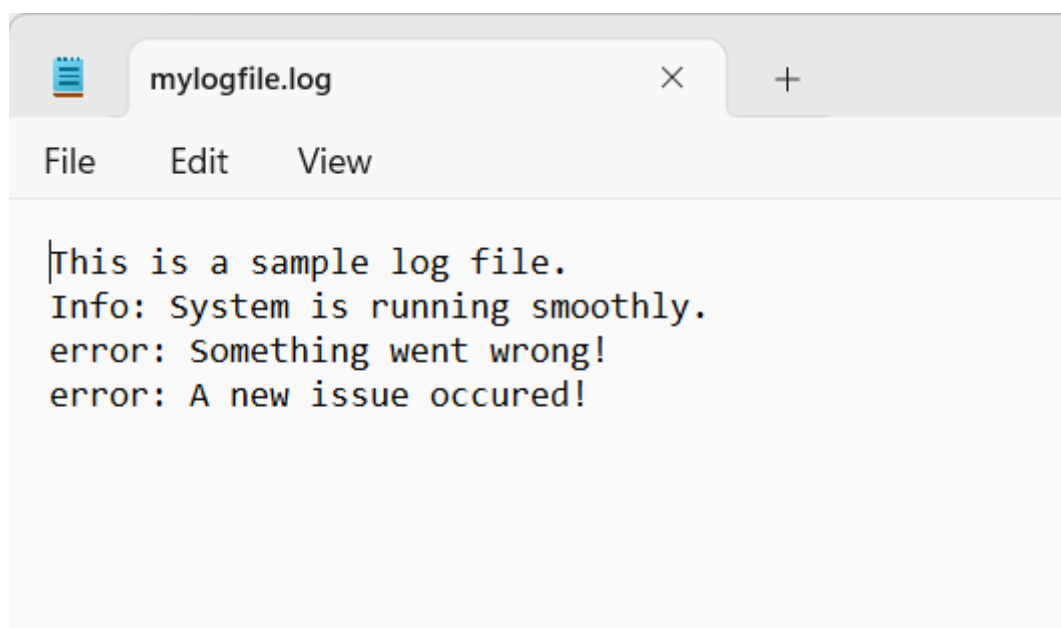
Run the script:

.\monitor_logs.ps1

```
PS C:\Users\Nantha Krishnan\Downloads\logs> .\monitor_logs.ps1
```

Step 8:

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



mylogfile.log

File Edit View

```
|This is a sample log file.  
Info: System is running smoothly.  
error: Something went wrong!  
error: A new issue occurred!
```

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!
```

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.
6. Detect and alert on predefined keywords (e.g., "error") to highlight critical events.
7. Gain hands-on experience with PowerShell scripting and automation on a Windows system.
8. Understand the importance of log monitoring in proactive system maintenance and troubleshooting.
9. Learn to customize and scale the script for more advanced monitoring scenarios in future projects.