**Placement Empowerment Program**

***Cloud Computing and DevOps Centre***

**Write a Shell Script to Monitor Logs**Create a script that monitors server logs for errors and alerts you.

Name: Yasvanth Rajan E Department: AML



**Introduction and Overview**

In this Proof of Concept (POC), We are going to create a PowerShell script that checks the Windows System log for error events once every 12 hours. If errors matching a specific keyword ("error") are found, the script displays the error messages; otherwise, it outputs "Nothing found."

**Objectives**

* **Verification:**  
  If the script outputs "Nothing found" or displays errors when expected, it is working correctly.
* **Automation Consideration:**  
  Although this guide covers creating and testing the script, you can later schedule it to run every 12 hours using Task Scheduler if desired.
* **Customization:**  
  You can adjust the $errorKeyword or modify the script logic based on your monitoring needs.

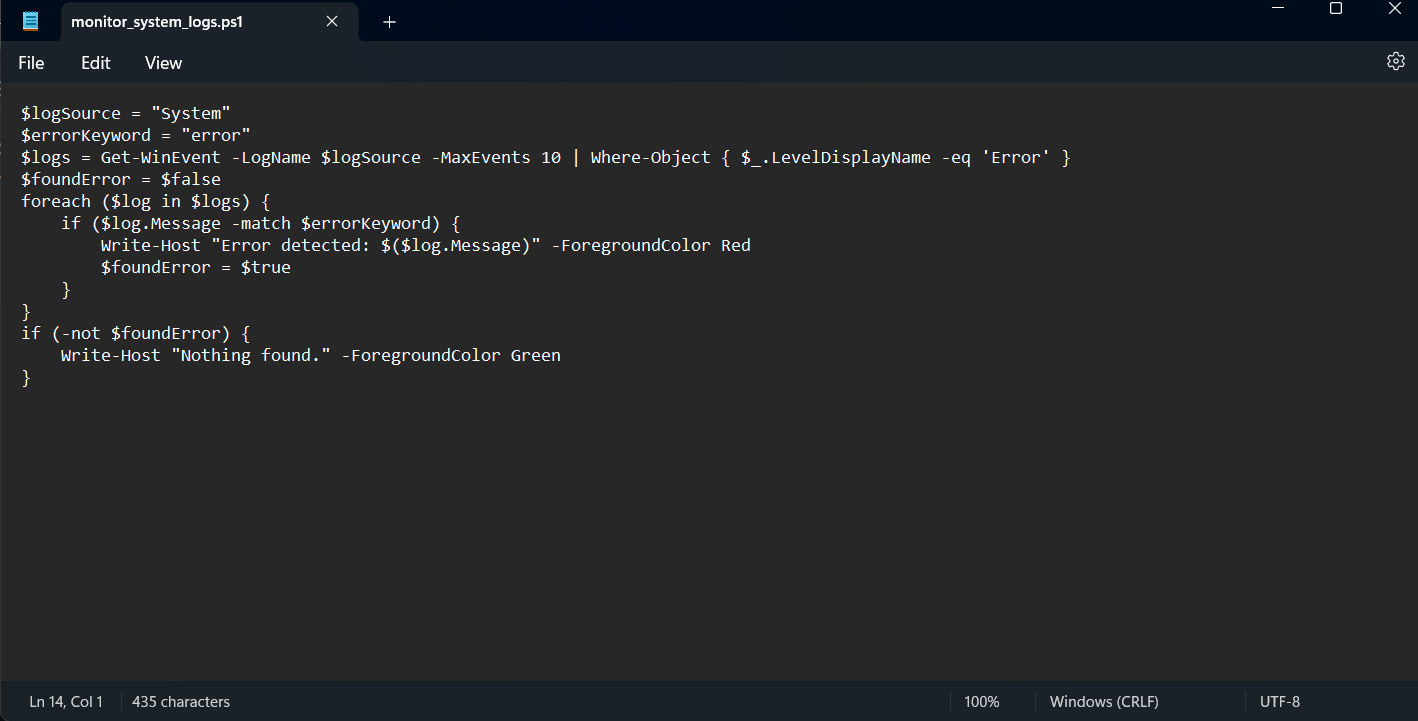
**Importance**

* Monitoring system logs is essential for proactive system management and troubleshooting.
* Regularly checking for errors can help you detect issues early, ensuring system stability and timely remediation.
* Automating this process with a PowerShell script makes monitoring consistent and efficient.

**STEPS:**

**STEP 1: Create the PowerShell Script**

* **Open a Text Editor:**  
  Use Notepad or your preferred text editor.
* **Copy the Script Code:**  
  Paste the following code into the editor:



* **Save the Script:**  
  Save the file with a .ps1 extension (e.g., monitor\_system\_logs.ps1). Note the file location (for example, C:\Scripts\monitor\_system\_logs.ps1).

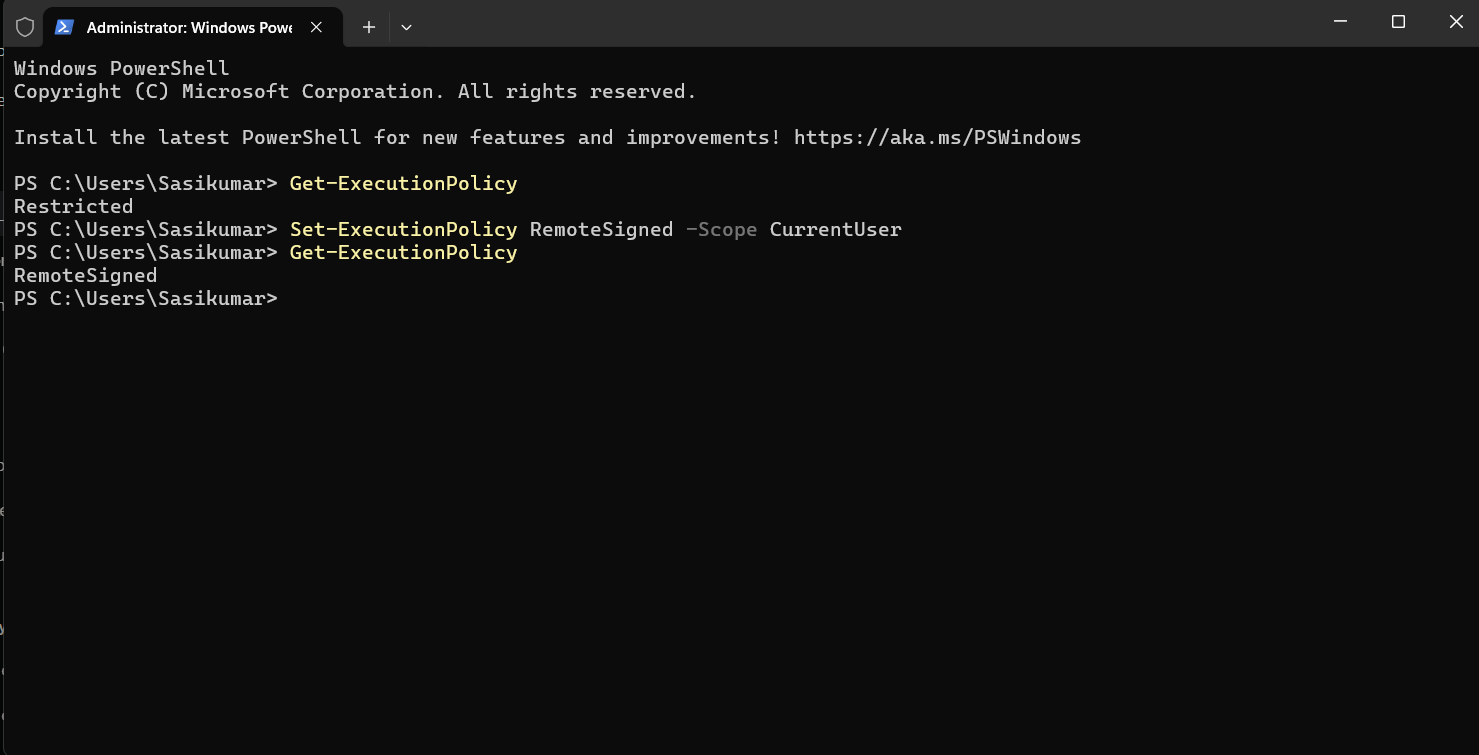
**STEP 2: Configure the Windows Execution Policy (if needed)**

* **Check the Current Policy:**  
  In PowerShell, run:
  + - Get-ExecutionPolicy
    - If it returns Restricted, you need to change it.
* **Set the Execution Policy:**  
  To allow script execution, change the policy to RemoteSigned (which permits locally created scripts):

Set-ExecutionPolicy RemoteSigned -Scope CurrentUser

* + - Confirm the change when prompted.
* **Verify the Change:**  
  Run the following again:
  + - Get-ExecutionPolicy

It should now display RemoteSigned.



**STEP 3: Test the PowerShell Script**

* **Open PowerShell:**  
   Press **Win + X** and select **Windows PowerShell** (or **PowerShell (Admin)** if required).
* **Navigate to the Script’s Directory:**  
   Change to the directory where you saved your script:

cd "C:\Path\To\Your\Script"

* **Run the Script:**  
   Execute the script by typing:

.\monitor\_system\_logs.ps1

* **Expected Output:**
  + 1. If no matching error events exist, you should see:

Nothing found.

* + 1. If matching errors are found, the script will display each error message in red.

