☁️ AWS CloudWatch Log Downloader and Scanner

Author: Daniel Chisasura

Version: 1.0

Purpose:

This script uses the AWS CLI to download CloudWatch logs from a specified log group and scans them locally for suspicious keywords (e.g., `"Unauthorized"`, `"Failed"`).

📄 Overview

This Bash script helps cloud administrators monitor AWS EC2 or other services by pulling logs from CloudWatch and scanning them for signs of unauthorized access or errors. It's a simple tool for entry-level cloud engineers to demonstrate automation and log analysis using AWS CLI.

🛠️ Prerequisites

- **AWS CLI**: Must be installed on your system.
- **AWS Credentials**: Run aws `configure` to set up your Access Key ID, Secret Access Key, and default region.
- **IAM Permissions**: Ensure your IAM user or role has permissions like `logs:GetLogEvents`.

⚙️ Configuration

Before running, edit the following variables in the script:

```
LOG_GROUP_NAME="/aws/ec2/my-instance-logs"  # Your CloudWatch log group
KEYWORD_TO_FIND="Unauthorized"              # Keyword to search for
OUTPUT_FILE="downloaded_logs.txt"           # Output file name
```

💡 **Note for macOS users**:

Replace the Linux `date` command with:

```
START_TIME=$(date -v-1d +%s000)
```

🚀 How to Use

1. **Make the script executable**: chmod +x download_and_scan.sh
2. **Run the script**: ./download_and_scan.sh

The script will:

- Download logs from the last 24 hours.
- Save them to `downloaded_logs.txt`.
- Print any lines containing your specified keyword.

📋 Sample Output

```
☁️  Starting AWS CloudWatch log download...
Log Group: /aws/ec2/my-instance-logs
Log download complete. Saved to downloaded_logs.txt
------------------------------------------------
🔍 Scanning logs for keyword: 'Unauthorized'
🚨 ALERT: Suspicious keyword 'Unauthorized' found in logs.
```