Linux Multi String , Multi Folder Log Search

By : Raz Goren

Date : 28-7-2014

Version : 1.01

# Preface

This tool/script was written to make searches on logs and cdrs easier .

It can search for multiple strings in multiple folders in text or gzipped files in the same time .

It can be used not only on any Linux system .

# Files

1. log-search.sh – Main script
2. list\_params.sh – Configuration script

# How to Use

To use the tool copy both files to a folder on the Linux machine .

Give both files executable permissions .

chmod +x \*.sh

## Configuration

Open the “list\_params.sh” with a text editor .

The following lines should be edited with the configuration you want :

1. STRINGS\_2\_SEARCH=(2013-12-30T19:19:30Z MIA-ACCESS69)
2. FOLDERS\_2\_SEARCH=(/var/log /OSS/oss/NexOSS\_5.8.0/ARCHIVE /OSS/oss/NexOSS\_5.8.0/LOG)
3. DATES\_2\_SEARCH=(8 12)
4. LOG\_NAME=searchresults.txt

In the parenthesis of the “STRINGS\_2\_SEARCH “ variable enter all strings you want to search for .  
There is no limitation on the number of strings you want to search for .

In the parenthesis of the “FOLDERS\_2\_SEARCH “ variable enter all paths of the files you plan to search in .  
There is no limitation on the number of folders you want to search for .

In the parenthesis of the “DATES\_2\_SEARCH” variable enter the number of days backward you want to search in .  
The 1st number is the minimum number of days and the 2nd number is the maximum number of days .  
Example : DATES\_2\_SEARCH=(8 12)  
 search files with dates between 8 to 12 days ago

All results will be shown on screen and in a log with default name : “searchresults.txt”  
Change the “LOG\_NAME” variable if you want a different logname .

## Running

It is recommended to run the script as root since there might be different folders we look at with different permissions .

CD into the folder where the scripts exist .

Run the command :

./log-search.sh

## Logs

The search results are written into a specific log file configured in the “list\_params.sh” file .

Each run the previous search log in the folder is renamed to a unique name .