Manual descriptivo para búsqueda de eventos/sucesos en logs del gestor

Propiedades del script

- Búsqueda de información en logs.
- Ha sido modificado para integrar el directorio /omk en sus búsquedas.
- Nombre: Busqueda.pl
- Versión: 2.1
- Link de descarga: Busqueda.pl

¿Cuándo se debe emplear el script?

Puede utilizarse cuando se presenta alguna falla en el sistema de NMIS y se desea investigar todo evento relacionado con el nodo/grupo/evento, el cual proporcionará información detallada sobre la búsqueda que se ejecute.

Descripción y prerrequisitos

La función principal del script es realizar búsquedas en los directorios de logs del sistema de monitoreo, lo cual facilitará al usuario la investigación de algún suceso o evento que se haya presentado.

El script realiza una búsqueda avanzada, la cual le permite al usuario ingresar un string o un regex, según sea el caso. Esto efectuará una búsqueda en todos los ficheros que se encuentran en los directorios ya mencionados, incluyendo también los archivos .tar, .gz y .zip.

Ejemplo de búsquedas:

```
Ejemplo: search="router1|router2|switch3" logs=all
Ejemplo: search="Node Down|Node Up" logs=all
```

En primera instancia, debe descargarse el script **Busqueda.pl** del link proporcionado y subirlo al sistema mediante un FTP (FileZilla, por ejemplo) al directorio **/usr/local/nmis8/admin**.

Después de subirlo, se requiere la ejecución de la siguiente instrucción para solucionar algún tema de permisos que pueda presentarse:

```
/usr/local/nmis8/admin/fixperms.pl
```

Antes de ejecutar el script, se requiere una modificación en el archivo **/usr/local/nmis8/conf/Config.nmis** para que funcione de manera correcta. Debe agregarse la siguiente línea en el archivo en la sección **'directories'**:

```
...
 'omk_logs' => '/usr/local/omk/log',
...
```

El archivo **Config.nmis** debe de quedar de la siguiente manera:

```
...
 'database_root' => '<nmis_data>/database',
 'json_logs' => '<nmis_logs>/json',
 'log_root' => '<nmis_logs>',
 'omk_logs' => '/usr/local/omk/log',
 'mib_root' => '<nmis_base>/mibs',
 'plugin_root' => '<nmis_conf>/plugins',
...
```

Al terminar la edición, deben guardarse los cambios realizados en el archivo.

Ejecución de búsquedas

a) Búsqueda del string **NMIS is disabled**:

```
[root@cnvtmxomk01 admin]# perl Busqueda.pl search="NMIS is disabled" logs=all
Processing /usr/local/nmis8/logs/event.log

Processing /usr/local/nmis8/logs/event.log-20210509.gz

Processing /usr/local/nmis8/logs/event.log-20210919
16-Sep-2021 12:00:04,1631811604,localhost,Alert: NMIS IS LOCKED,Fatal,,NMIS is disabled! Server.prueba.LAB-OMK.
com 10.10.6.95 Delete the file NMIS_IS_LOCKED and run the command fpingd.pl
17-Sep-2021 12:00:03,1631898003,localhost,Alert: NMIS IS LOCKED,Fatal,,NMIS is disabled! Server.prueba.LAB-OMK.
com 10.10.6.95 Delete the file NMIS_IS_LOCKED and run the command fpingd.pl
18-Sep-2021 00:00:03,1631941203,localhost,Alert: NMIS IS LOCKED,Fatal,,NMIS is disabled! Server.prueba.LAB-OMK.
com 10.10.6.95 Delete the file NMIS_IS_LOCKED and run the command fpingd.pl
18-Sep-2021 12:00:03,1631984403,localhost,Alert: NMIS IS LOCKED,Fatal,,NMIS is disabled! Server.prueba.LAB-OMK.
com 10.10.6.95 Delete the file NMIS_IS_LOCKED and run the command fpingd.pl
19-Sep-2021 00:00:03,1632027603,localhost,Alert: NMIS IS LOCKED,Fatal,,NMIS is disabled! Server.prueba.LAB-OMK.
com 10.10.6.95 Delete the file NMIS_IS_LOCKED and run the command fpingd.pl

Processing /usr/local/omk/log/opCharts.log

Processing /usr/local/omk/log/opCharts.log-20210613.gz

[root@cnvtmxomk01 admin]#
```

b) Búsqueda del String **Node Configuration Change**:

```
[root@cnvtmxomk01 admin]#
[root@cnvtmxomk01 admin]# perl Busqueda.pl search="Node Configuration Change" logs=all
Processing /usr/local/nmis8/logs/event.log

Processing /usr/local/nmis8/logs/event.log-20210509.gz

Processing /usr/local/nmis8/logs/event.log-20210919
17-Sep-2021 15:15:04,1631909704,Ciudad_de_Mexico_TR04_DATACENTER,Node Configuration Change,Major,,Changed at
467 days 8:53:19
17-Sep-2021 15:15:04,1631909704,Cuernavaca_Central_RT01,Node Configuration Change,Major,,Changed at 73 days 18:
04:17
17-Sep-2021 15:20:02,1631910002,Firewall_CDMX_SDWAN01,Node Configuration Change,Major,,Changed at 5 days 5:46:59

Processing /usr/local/omk/log/opCharts.log

Processing /usr/local/omk/log/opCharts.log-20210613.gz

[root@cnvtmxomk01 admin]#
```