# Solución de problemas opFlow



## Verifique que el demonio de recolección de flujo se esté ejecutando

En OpFlow 3, se le avisará de los problemas del demonio en la página principal del panel, de forma similar a la siguiente captura de pantalla:

### Verificar que se está ejecutando "flowd"

opFlow  usa la herramienta "flowd" para recibir (y almacenar temporalmente) datos de flujo:

```
ps -ef | grep flowd
```

Debería ver algunas entradas además del grep, la relevante aquí son las dos líneas " ":

```
[root@thor opmantek]# ps -ef | grep flowd

root 13356 1 0 Jun18 ? 00:00:10 flowd: monitor

_flowd 13357 13356 0 Jun18 ? 00:00:30 flowd: net

root 27114 1 0 12:40 ? 00:00:00 NMIS opflowd debug=0

root 32567 27106 0 12:51 pts/5 00:00:00 grep flowd
```

Para iniciar un flujo perdido / muerto, simplemente ejecuta

```
sudo service flowd start
```

## Verificar que se está ejecutando "nfcapd"

En opFlow 3, hemos cambiado a un colector de flujo más moderno, "nfcapd" del paquete "nfdump"; OpFlow 3 también incluye un script de inicio más conveniente para este demonio:

```
sudo service nfdump status
```

Debe informar que nfcapd se está ejecutando con un PID particular; puede comprobar siguiendo este parámetro:

```
ps -ef|fgrep nfcapd
```

Si no hay nfcapd activo, ejecuta

```
sudo service nfdump start
```

## Verificar que el demonio principal de opFlow se está ejecutando

opFlow requiere que `opflowd` se ejecute para recuperar periódicamente y procesar nuevos datos de flujo de la herramienta correspondiente del colector de flujo.

```
sudo service/opflowd status
```

Debería de informar que opFlowd está activo, sino ejecutar el siguiente comando

```
sudo service opflowd start
```

## Verificar que MongoDB se esté ejecutando

Sin un funcionamiento MongoDB opFlow no puede operar; con toda probabilidad, usará un servidor MongoDB local, en la misma máquina que opFlow. En este caso, debería ser suficiente para verificar un servidor de mongod Activo.

```
sudo service mongod status y/o ps -ef | fgrep mongod
```

(Si no está utilizando la configuración predeterminada, sino una instancia de mongod remota, deberá usar el `mongo` shell para verificar que esté accesible y funcionando). Al igual que en el `mongod` ejemplo anterior, activar una instancia faltante es fácil:

```
sudo service mongod start
```

Tenga en cuenta que mongod puede negarse a iniciar por una serie de razones (por ejemplo, configuración incorrecta, falta de espacio en disco, etc.); si el inicio del servicio indica falla, tendrá que investigar usando los registros de MongoDB (que generalmente están en `/var/log/mongodb/`).

# Verificar la configuración de la carpeta de origen de datos

opFlow necesita saber dónde buscar nuevos datos de flujo, y es evidente que la herramienta de recolección de flujo necesita saber dónde guardar los datos para que los consumidores los encuentren.

## Directorios de flujo (opFlow 2)

Verifique que todas las carpetas sean iguales. Ejecute estos comandos y asegúrese de que todo apunte al lugar correcto.

```
grep logfile /usr/local/etc/flowd.conf

grep opflow_dir /usr/local/opmantek/conf/opFlow.nmis
```

Es especialmente importante que opFlow, que es la configuración de "flowd_data", recoja el archivo de registro que fluye, y este se combina con "<dir_o_flujo>" para obtener la ruta

```
grep logfile /usr/local/etc/flowd.conf

logfile "/data/opflow/flowd"

 grep opflow_dir /usr/local/opmantek/conf/opFlow.nmis

  '<opflow_dir>' => '/data/opflow',

  'flowd_data' => '<opflow_dir>/flowd',
```

## Directorio nfcapd / nfdump (opFlow 3)

La configuración predeterminada para nfcapd se utiliza `/var/lib/nfdump` para el almacenamiento de datos de flujo, y opFlowd necesita usar el mismo directorio.

```
grep opflow_dir  /usr/local/omk/conf/opCommon.nmis

  '<opflow_dir>' => '/var/lib/nfdump',

 cat /etc/default/nfdump /etc/sysconfig/nfdump

#...at most one of these files exists; if not the default in /etc/init.d/nfdump will be used

# in all cases the relevant line looks like this:

DATA_BASE_DIR="/var/lib/nfdump"
```

# Espacio de disco duro

## Verifica tu espacio de disco (principalmente opFlow 2)

Asegúrese de que donde quiera que esté poniendo los datos de flujo y el Mongo DB, tenga bastante espacio en disco; Los datos de flujo son muy voluminosos. En opFlow 3, las colecciones de la base de datos normalmente tienen un "límite" de tamaño y no aumentan.

```
df -h /data
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg_data-lv_data
           247G  86G  148G  37% /data
```

# Ejecute una purga manualmente (solo opFlow 2)

Purgue los datos de flujo binario del flujo sin procesar y los datos de la base de datos anterior, suponga que desea mantener 7 días de datos binarios de flujo y se encuentra en / var / opflow.

```
/usr/local/opmantek/bin/opflw_purge_raw_files.sh /var/opflow 7
/usr/local/opmantek/bin/opflowd.pl type=purge
```