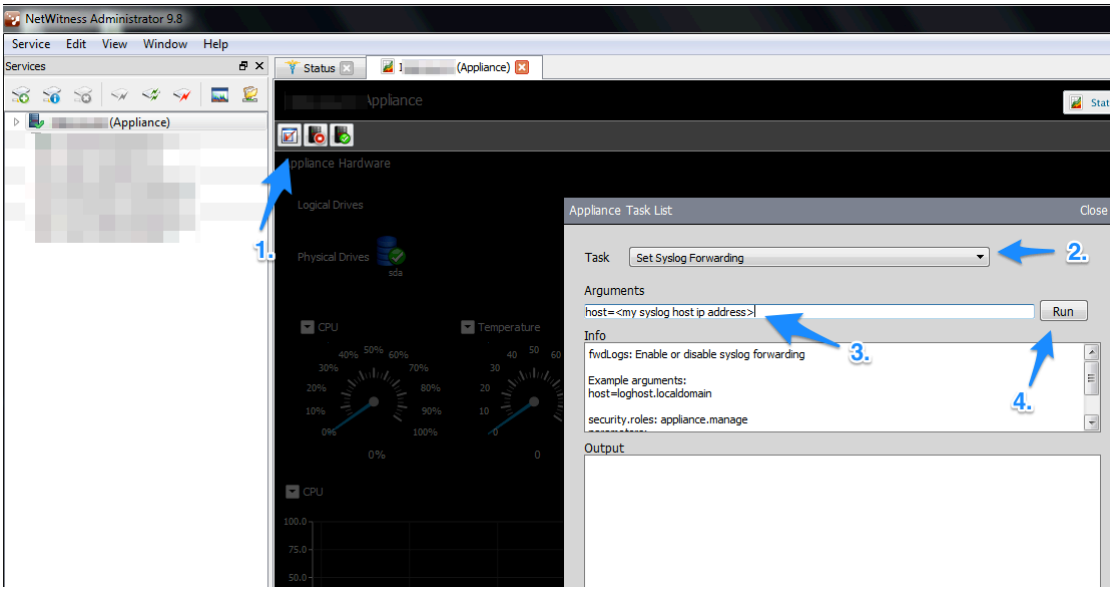
## How to configure Syslog Forwarding on your NextGen devices

Start by using NW Administrator and connecting to the Appliance Service of your device. Select your device and open its Appliance service tab and then:

1. Click the “Appliance Tasks” button
2. Select “Set Syslog Forwarding” from the drop-down
3. Enter the details of your syslog server with “host=<your syslog server IP address>”
4. Click “Run”




On CentOS 6.x based devices a /etc/rsyslog.nw.conf file will be created with the following contents.

```
[root@          ~]# cat /etc/rsyslog.nw.conf
:programname, contains, "nw"    @       .172
# This file is generated automatically.  Do not edit it!
[root@          ~]#
```

Which only forwards your NextGen relevant messages to the syslog server.

On CentOS 5.x based devices “*.*” will be added to the end of your /etc/syslog.conf

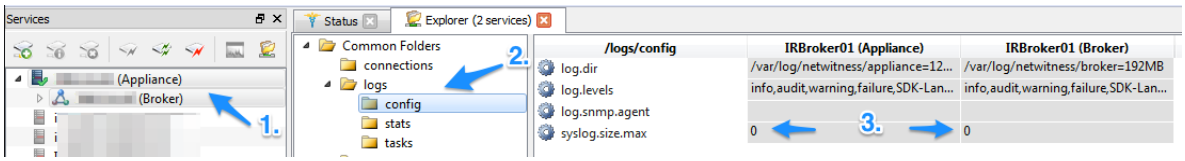
```
[root@          ~]# tail -2 /etc/syslog.conf
*.*      @       172

[root@          ~]#
```

In this case all syslog messages, including standard OS messages will be forwarded to your syslog server.

Before closing NW Administrator, select both your device's Appliance and its own product service (Decoder,Log Decoder, Concentrator or Broker) and

1. Open "Explorer" for both services
2. Navigate to "/logs/config"
3. Set "syslog.size.max" to 0




The default is "255" but that will truncate most of your audit messages for user activity, so it is strongly encouraged that you change this setting.

## Configuring your Syslog Server using rsyslog to filter NW messages

If using rsyslog to receive your forwarded log messages (in my case it comes by default with CentOS 6), here's some additional configuration to help route messages to an NW only log file and also to filter the constant login/logout messages generated by the other Splunk Apps.

```
[root@splunkdev netwitness_admin]# cat /etc/rsyslog.d/10-nwappliances.conf

# provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

:msg, regex, "<your Splunk Server IP>.* has logged"      ~
:programname, contains, "nw"  /var/log/netwitness.log
&~
:HOSTNAME, isequal, "[redacted]240"    /var/log/netwitness-linux.log
:HOSTNAME, isequal, "[redacted]241"    /var/log/netwitness-linux.log
&~
```



Item 1. above shows how to filter out messages that contain your Splunk server IP and the "has logged" wording, this should help exclude the regular messages generated by Splunk Apps login in to each device every minute. These look something like the below examples:

```
Sep  6 09:52:23 Broker01 nw[4699]: [Engine] [audit] User splk
(session 972295 [::ffff:x.x.x.172]:65087) has logged out
Sep  6 09:52:22 Broker01 nw[4700]: [Engine] [audit] User splk
(session 972295, [::ffff:x.x.x.172]:65087) has logged in
```

Item 2. will forward all “nw” messages to the “/var/log/netwitness.log” file so it can easily be monitored by Splunk and the correct sourcetype set.

```
[monitor:///var/log/netwitness.log]
sourcetype = netwitness_log
```

The last 3 lines will forward other syslog messages mostly from CentOS 5 based devices to a separate log file that will mostly contain OS messages (i.e. not “nw” related) to a separate log file.