**Setting up Windows Event Log Collection**

**Setting up Collector on Windows Server (Must be 2008R2+ and Up)**

Step1: [start some services]

On the command line run these commands:

winrm qc

wecutil qc

Step 2: [Creating your Subscriptions]

Open up “Server Manager” -> “Diagnostics” -> “Event Viewer” -> “Subscriptions”

On the right hand side click on “Create Subscription…”

Enter a name for your subscription

Enter a Description

Destination Log: “Forwarded Events”

Click on “Select Source Computer initiated”

Click on “Select Computer Groups…”

Click on “Add Domain Computers”

In the “Enter the object name select” type in “domain computers” and select “check names”

Then Click okay

Next click on “Select Events”

Select “critical, warning, verbose, Error, Information”

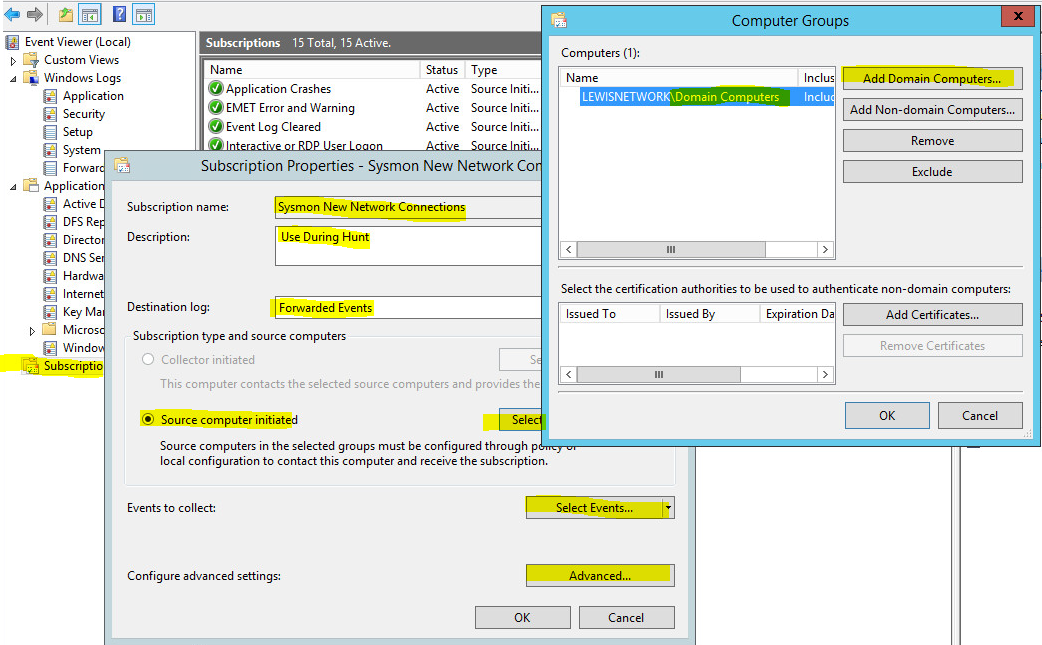
Select Radial button that says “By Log”

Select Drop down and Select whatever subscription you want. In my case I will select “application, system, and security” under the Windows Log section

Enter the event ID’s you want to receive comma separated (if are not specified the subscription will collect all events from al computers in the domain):

“4624,4625,4648,4723,4724,1102,7040,4697,7034,400,4670,4717,602,4649”

Select “OK”

****

Step3: [Setting up Filters to view the logs from your subscription (on the Collector)]

Open up “Server Manager” -> “Diagnostics” -> “Event Viewer” -> “Custom Views”

On the right side of the screen select “Create Custom View”

Select Radial button that says “By Log”

Select Drop down and Select “Forwarded Events” in the Windows Logs Drop down area

Select okay

Give it a name and description

Select Okay

Bata bing ☺

