**Windows Event Forwarding**

Event Collector : Windwows Server 2016

Collected Events from: Windows Server 2016

Set up WEF:

**Enable the collector service on the collector server:**

Run command: wecutil.exe qc

**(Optional) Create a group and place the monitored computers in it**

**Create a GPO**

What to set:

Computer Configuration -> Policies -> Admin Templates -> Windows Components -> Event Forwarding -> Configure Target Subscription Manager = Enabled + set subscription manager: Server=http://dc01:5985/wsman/SubscriptionManager/WEC,Refresh=60

Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Restricted Groups -> Add Group Event Log Readers with the Network Service user in it (WsMan runs as network service and it does not have access to the event logs by default)

**(Optional) In security filtering add the group created earlier**

**Link the GPO where you need it**

**Configure collector with what events it should get**

Go to Event Viewer to the Subscriptions pane. Add a subscription. Enter info and select source computer initiated (each computer contacts the server, not the server contacts all computers). Configure the group created earlier.