CYBRAICS

nLighten™

Configuring Your Environment for WEF & WEC

This document covers the steps necessary to configure the free, centralized logging solution built into Windows nodes. To do this, we will enable Windows Event Forwarding and the corresponding Windows Event Collection feature in a lab environment. These are native features built into Windows operating systems and do not require the installation of external agents. We will use one external agent to move the events from the Windows Event Collector to our analytics engines by way of the syslog protocol as the final step in the process.

The concepts described here are transferrable to larger environments but may require additional considerations for scheduling event collection, such as load balancing and fault tolerance. The goal of this configuration is to create a Global Policy Object for all capable members in the domain to automatically begin forwarding events to a single designated Windows Event Collector. Here is the general outline of the steps required to enable WEF & WEC and begin collecting events.

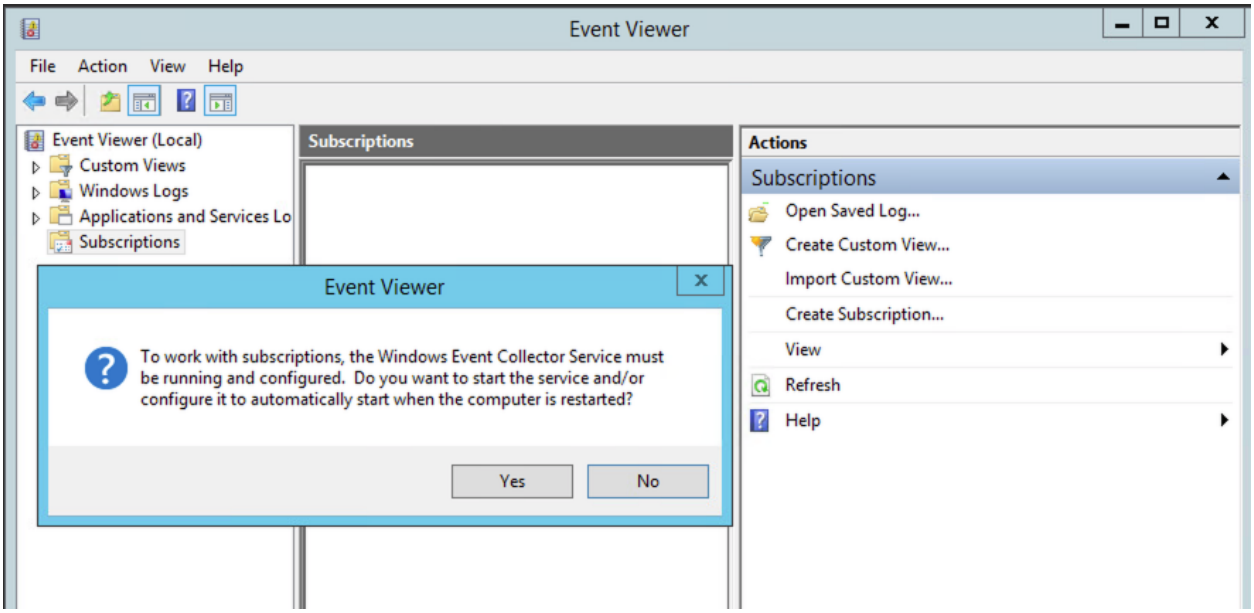
1. Select a machine to be the Windows Event Collector. For purposes of this example, where we are limited by the number of machines available in the lab, we will utilize the Domain Controller to also serve as our WEC.
2. Ensure that WinRM is enabled for all endpoints and our subscription manager which in this case will also be the Domain Controller.
3. Enable the Windows Event Collector Service on the WEC
4. Create a GPO to add the NETWORK SERVICE account to the built-in Event Log Readers group
5. Create a GPO to specify the URL of the WEF subscription manager, i.e., pointing to the Domain Controller, which is our WEC
6. Link our new Windows Event Forwarding GPO to the domain
7. Create a set of event log subscriptions that tell the endpoints which events to filter and forward. Note: We used Palantir's excellent guide as a baseline. See the references section at the end of this document.
8. Create corresponding GPOs to enable enhanced auditing on the endpoints to ensure they generate the events we are looking for. Note: many of these are disabled by default so this is a critical step to bring it all together.
9. Windows does not natively support syslog, so our final step will be to install and configure a syslog agent to forward all the windows events on the WEC to our analytics engines.

Step 1. We are working in a small lab environment, so we opted to have our Domain Controller also serve as the WEC. In the lab, the event volume will be relatively low, but you will need to take sizing into consideration for larger, high event volume deployments.

Step 2. We need to enable the WinRM service on the WEC. The lab VM we are using as the Domain Controller, and Windows Event Collector is running server 2012R2. To enable the WinRM service, which is used to send events to the WEC, open a command prompt with administrator access and type: **`winrm qc`**

Answer yes to both questions (yes to autostart winrm and yes to open firewall to allow access).

Step 3. Enable the Windows Event Collector Service on the WEC. Open the Event Viewer and click on Subscriptions.

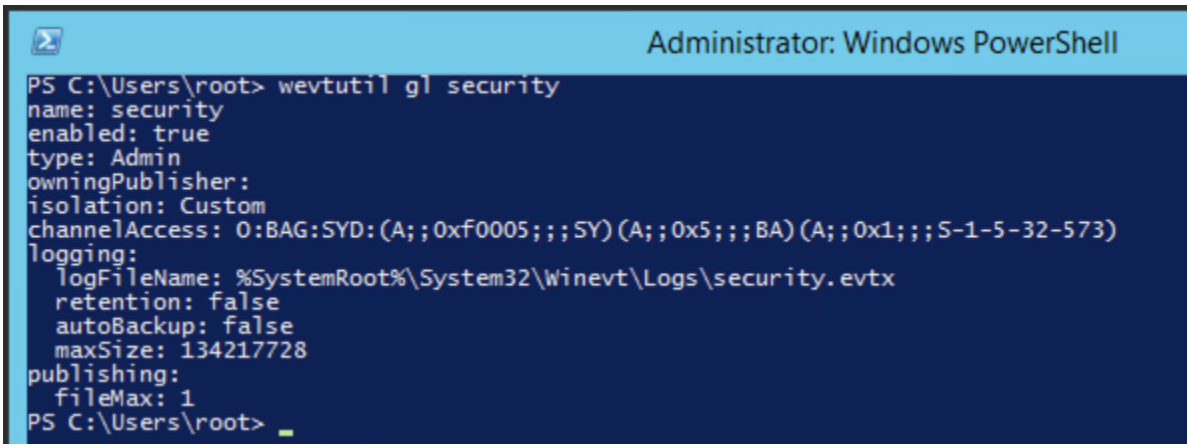


Click Yes to configure the service to start automatically.

At this point, we have enabled the WinRM protocol, which is used to securely transfer events over the network, and configured our WEC, Windows Event Collector, to automatically start and receive those events.

Step 4. Create GPO to allow reading of the Security log and to tell the endpoints where to get the Event Subscription details that tell them which events to forward.

First, we need to create the permissions string for access to the Security logs. From a command prompt type: **`wevtutil gl security`**



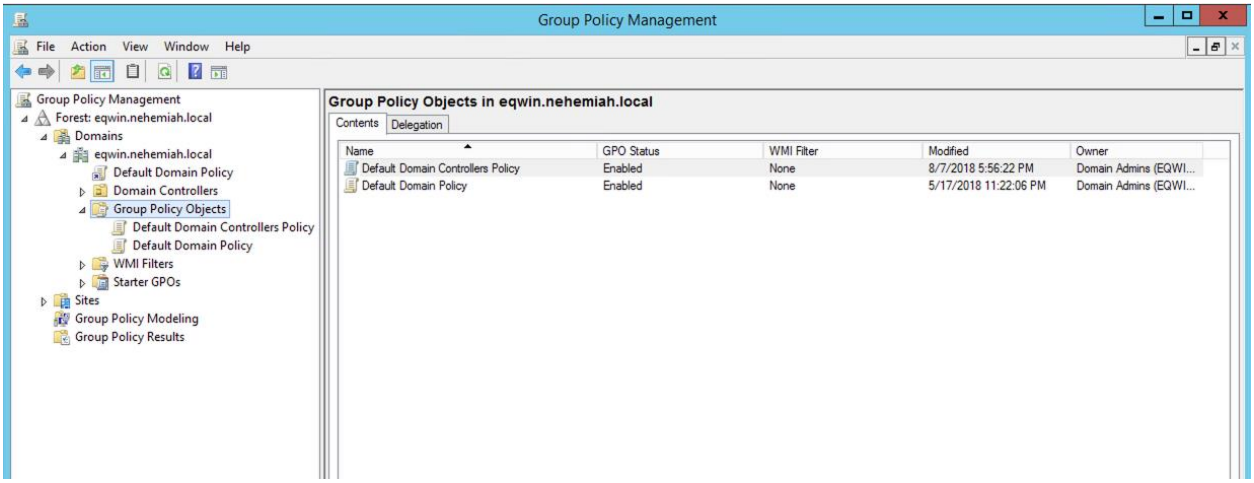
Copy the string from the channelAccess line that starts with O:BAG:SYD: and append it with the following string: **`(A;;0x1;;;NS)`**

The complete permission string should appear like this:
`O:BAG:SYD:(A;;0xf005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)`

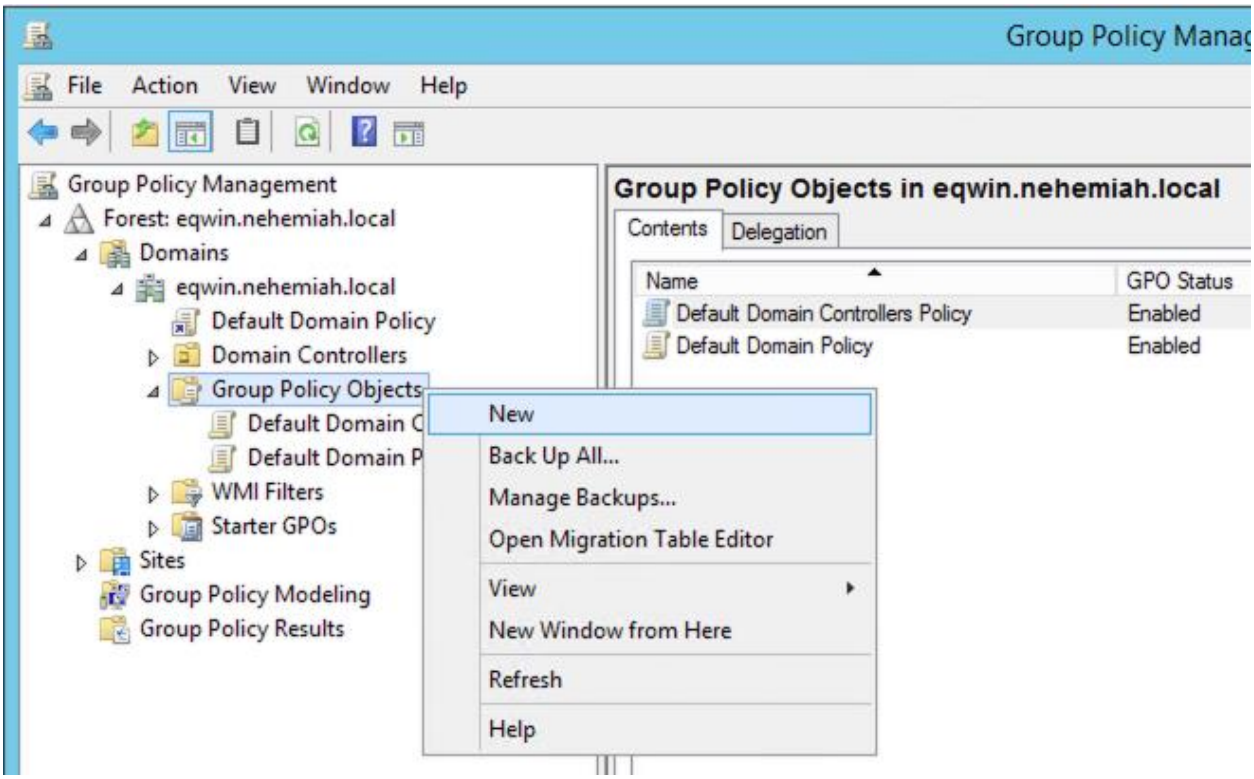
We also need the FQDN, Fully Qualified Domain Name, of the WEC. For our lab, we'll be using: **`dc.eqwin.nehemiah.local`**

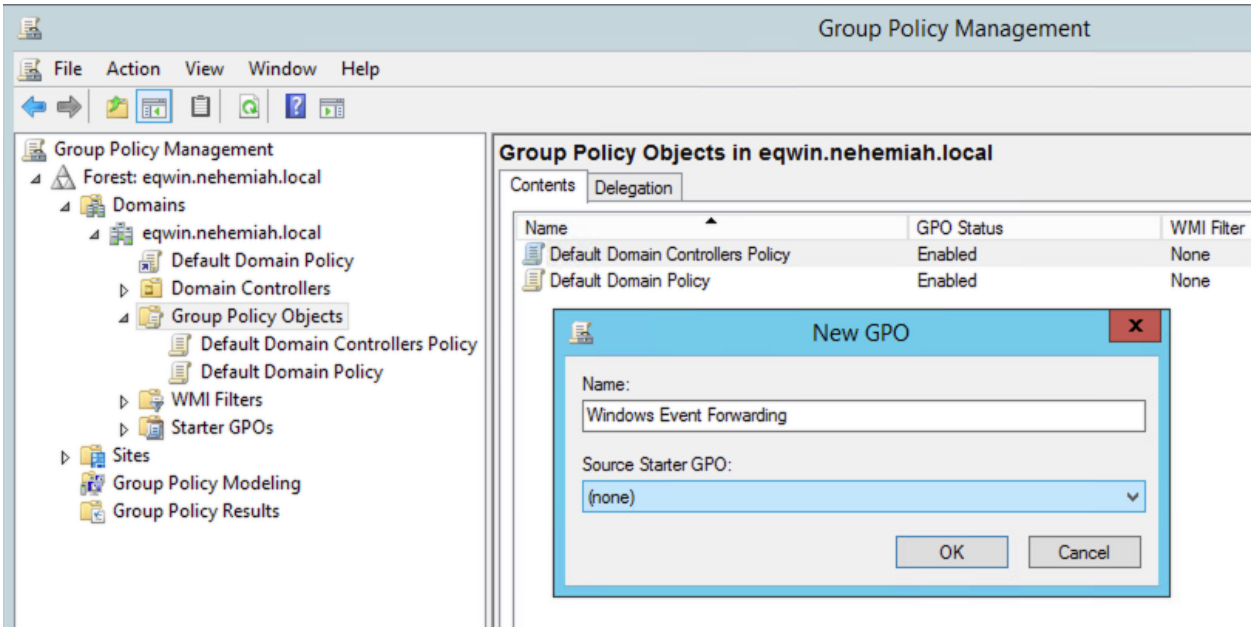
We use the FQDN in the URL that will enable the endpoints to find the WEC. We specify the permission string and the URL in the GPO we create.

Start the Group Policy Management gui on the Domain Controller.

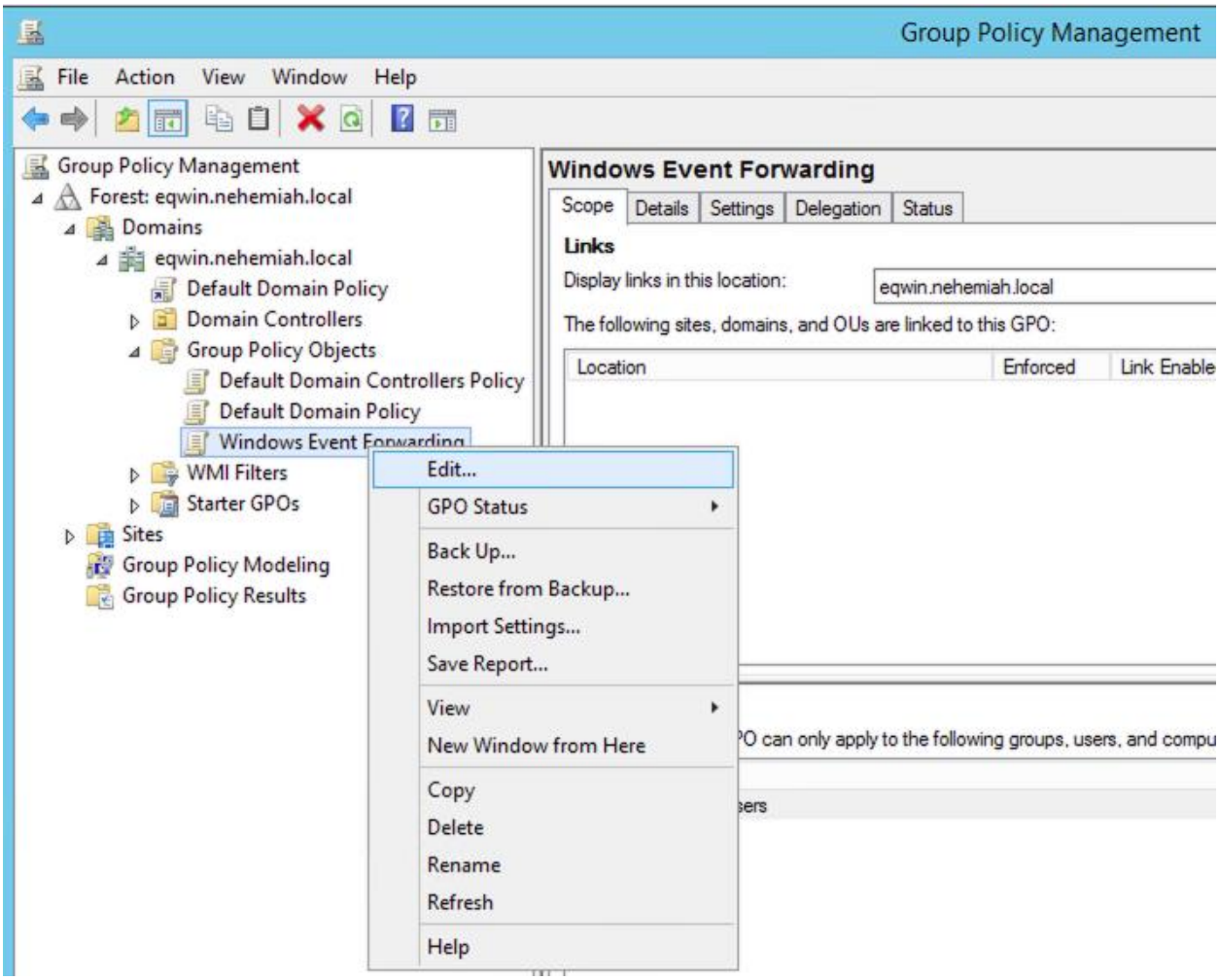


We are going to create a new GPO, which we will call: **`Windows Event Forwarding`**



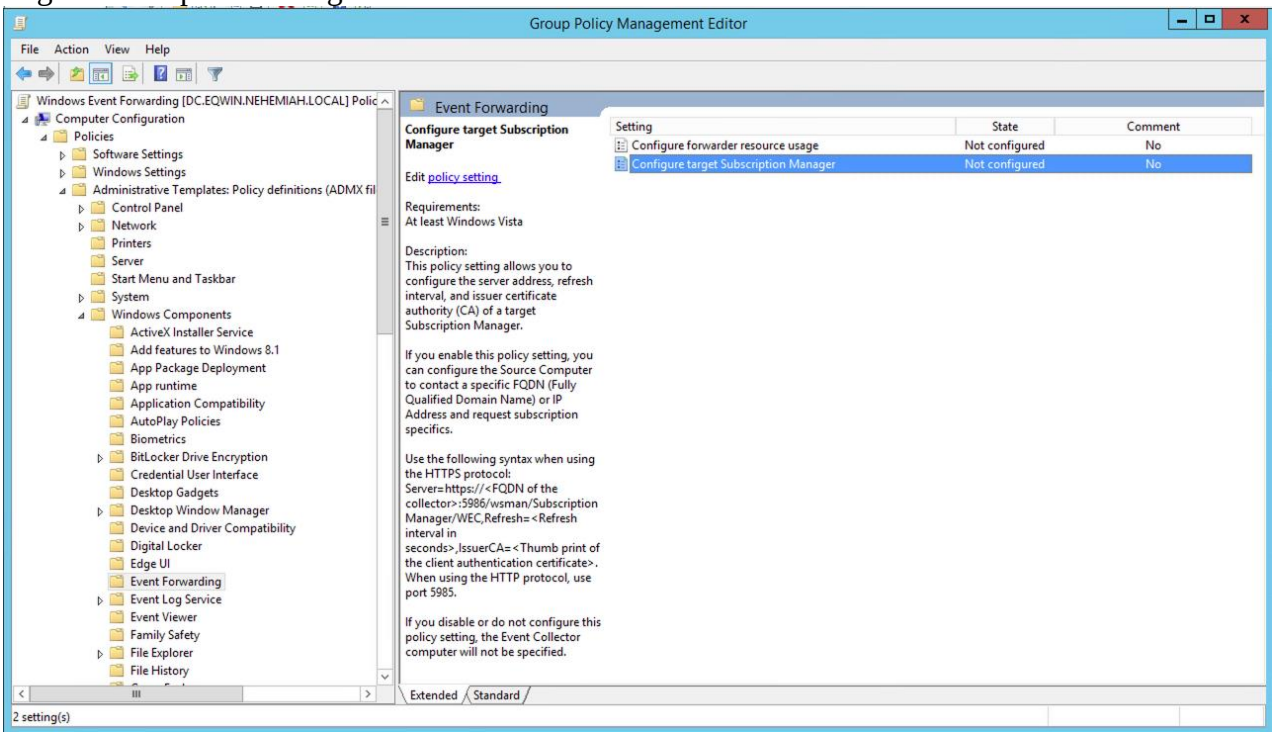


Next, we need to edit this new GPO and define our Event Subscription Manager string and configure local log access on the endpoints so the NETWORK SERVICE can read and forward the events.



The Subscription Service URL can be found here:

Computer Configuration>Policies>Admin Templates>Windows Components>Event Forwarding>Configure target Subscription Manager

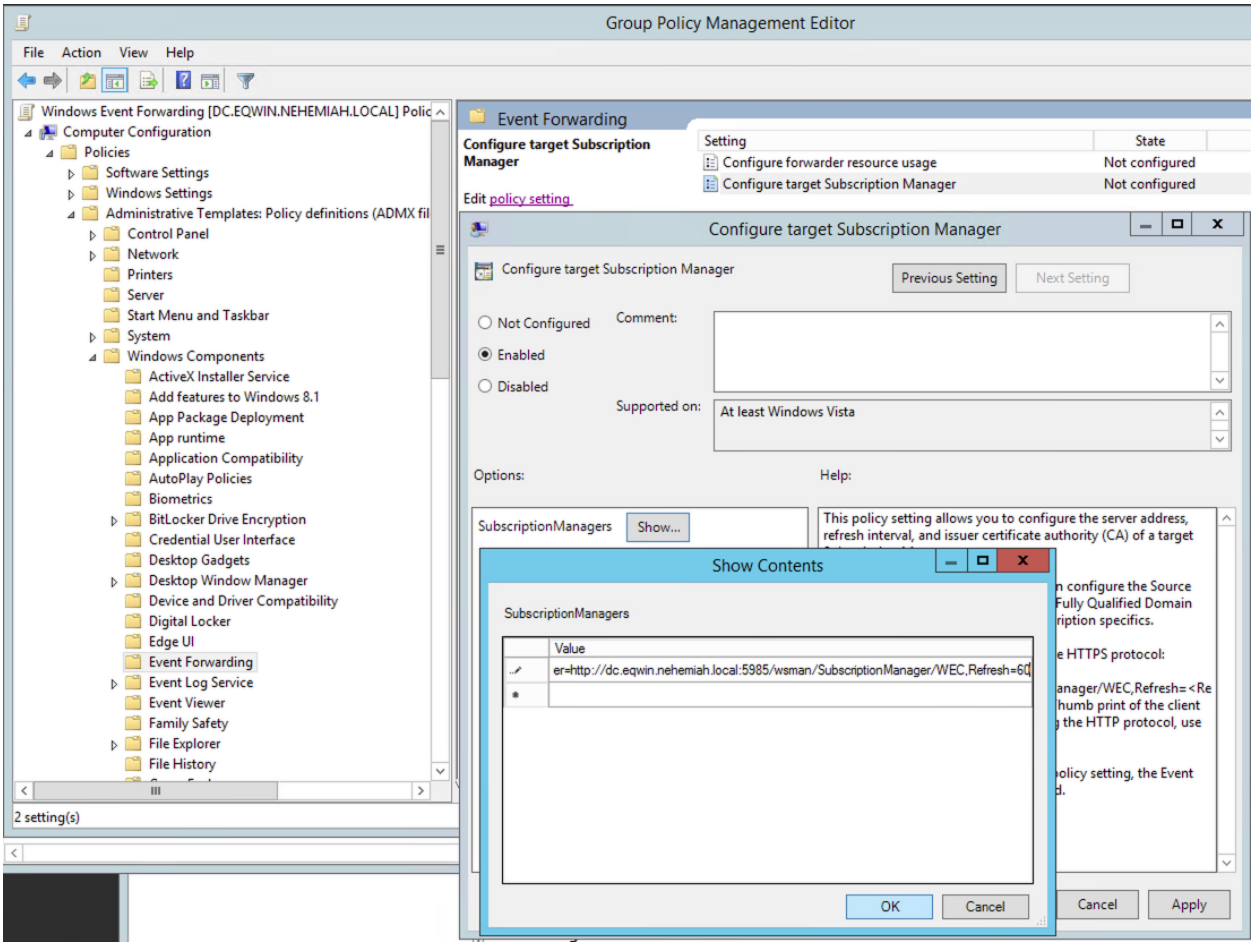


Click Edit **policy settings**, select **Enabled** and click **SubscriptionManagers Show…**

Enter the following for the Subscription Manager string:

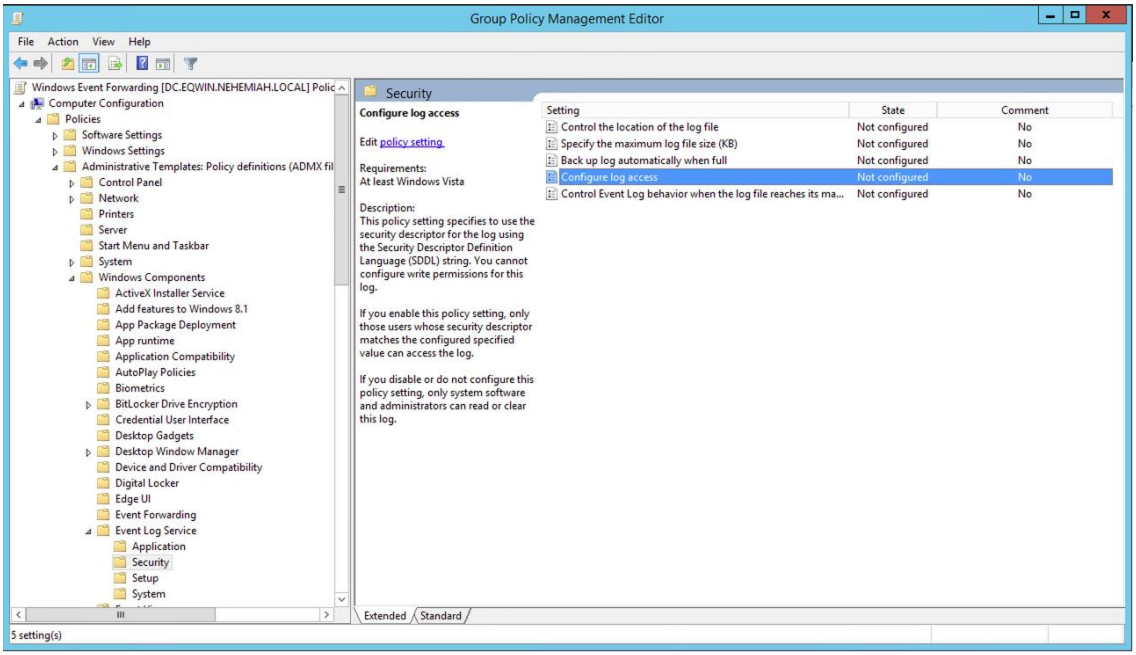
`Server=http://dc.eqwin.nehemiah.local:5985/wsman/SubscriptionManager/WEC,Refresh=60`

Note: Since we are using WinRM, events are encrypted via Kerberos by default, so we don't need to use the https protocol for any member nodes of the domain.



The event log access configuration setting can be found here:

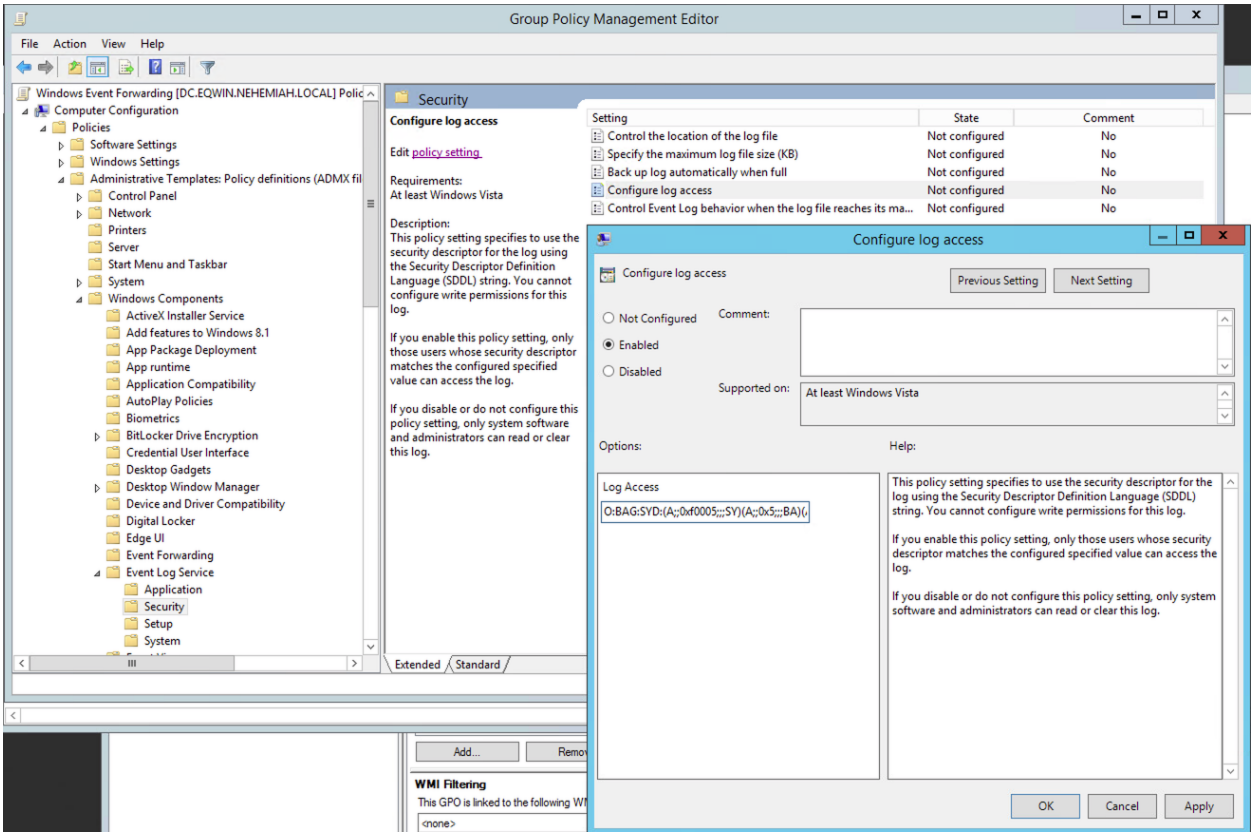
Computer Configuration>Policies>Admin Templates>Windows Components>Event Log Service>Security> Configure log access



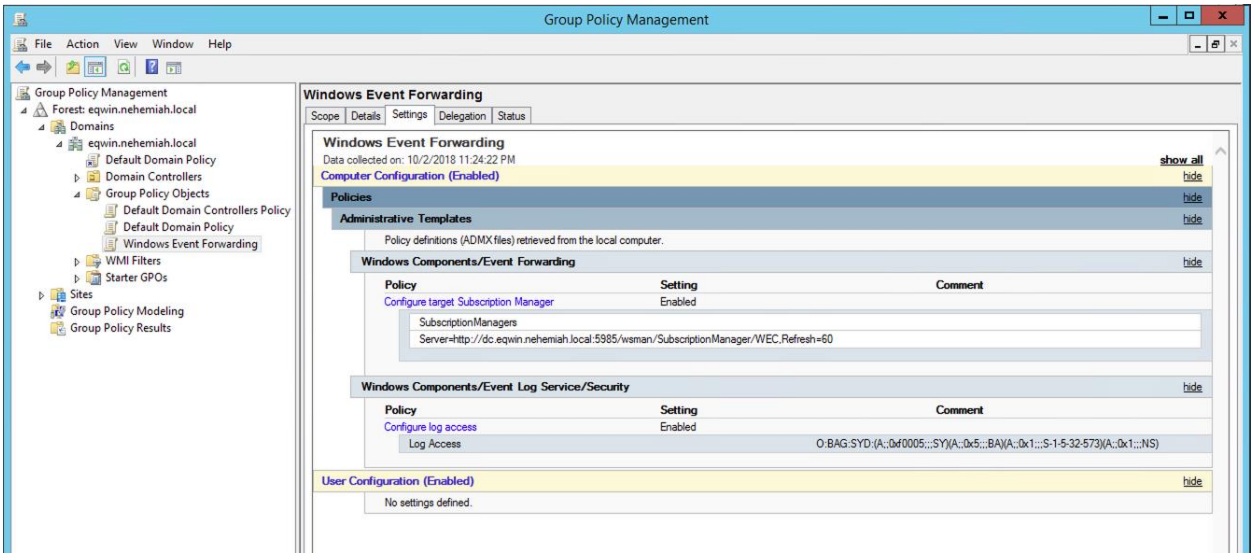
Click the Edit policy setting link or right click "Configure log access" and click edit.

Select enabled. Enter the SDDL, Security Descripto Definition Language, string we concatenated from the wevtutil gl security command in the box labled Log Access.

O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)



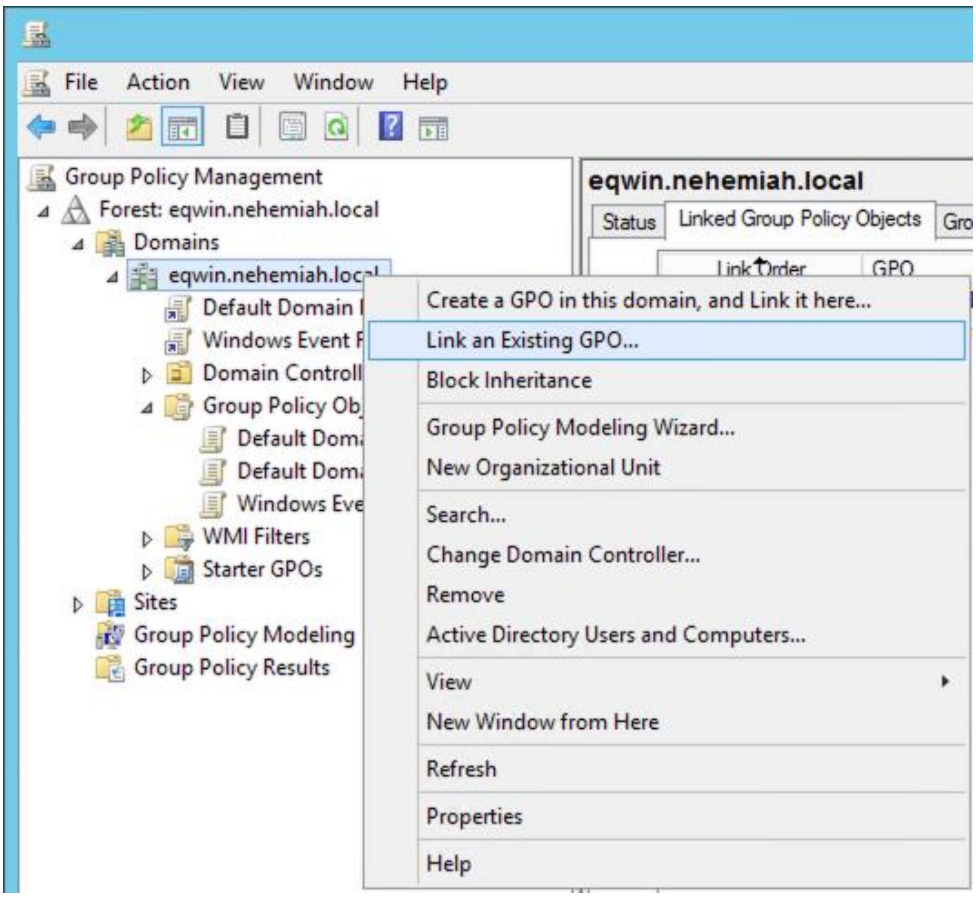
When you're done, you should be able to close the Group Policy Editor and return to the Group Policy Management GUI, select the new Windows Event Forwarding policy we created and then select the Settings to see a summary of our changes.



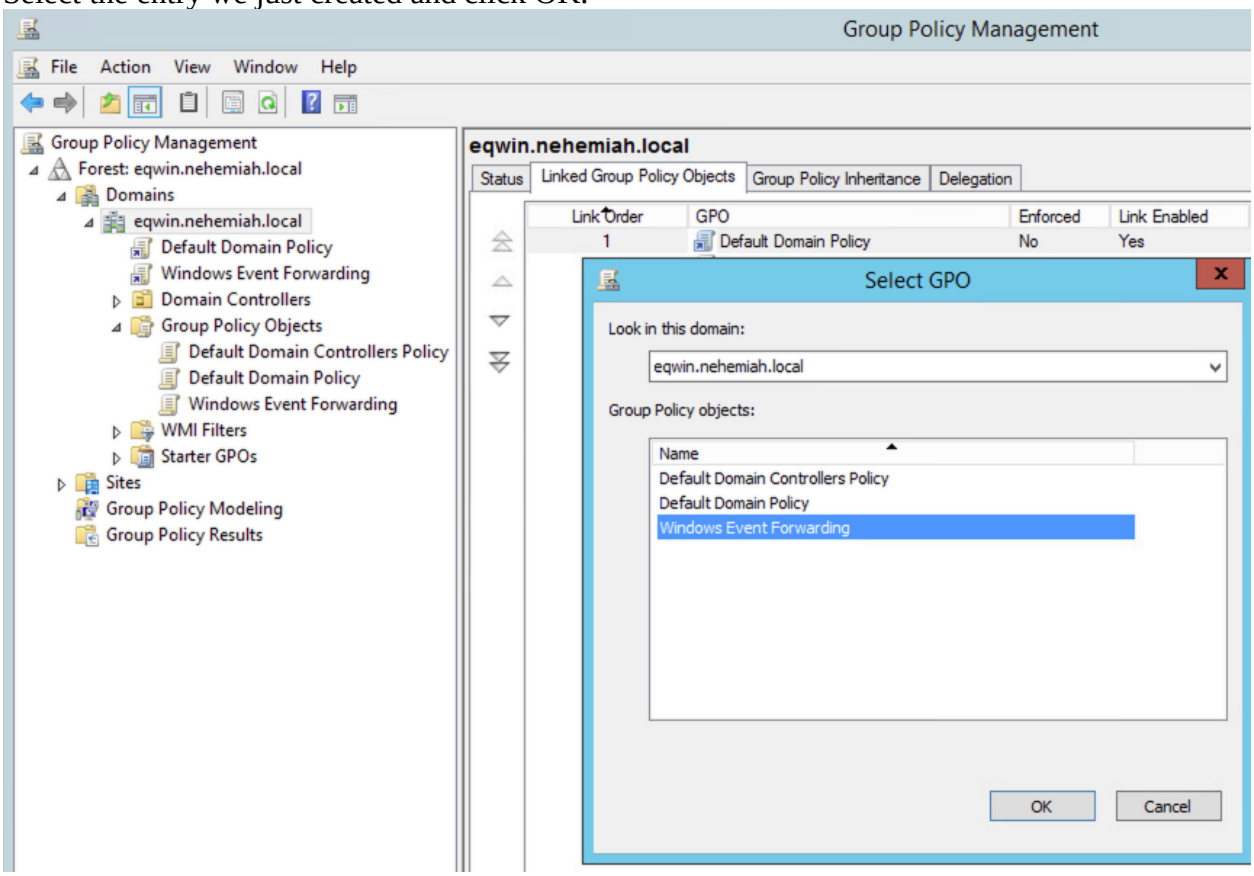
Step 6. Link the new Windows Event Forwarding GPO to the domain.

Select the domain we want to link our new GPO to. In this case, it's called eqwin.nehemiah.local.

Right-click and select "Link an Existing GPO…"



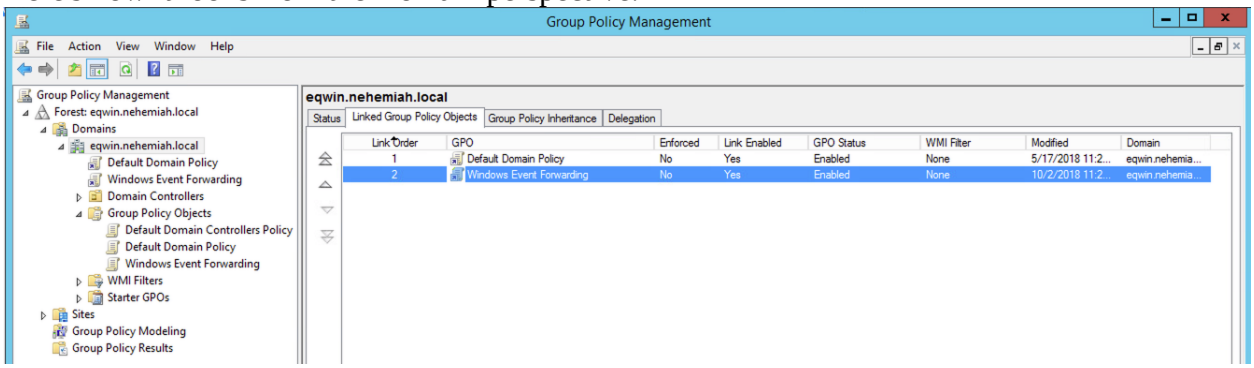
Select the entry we just created and click OK.



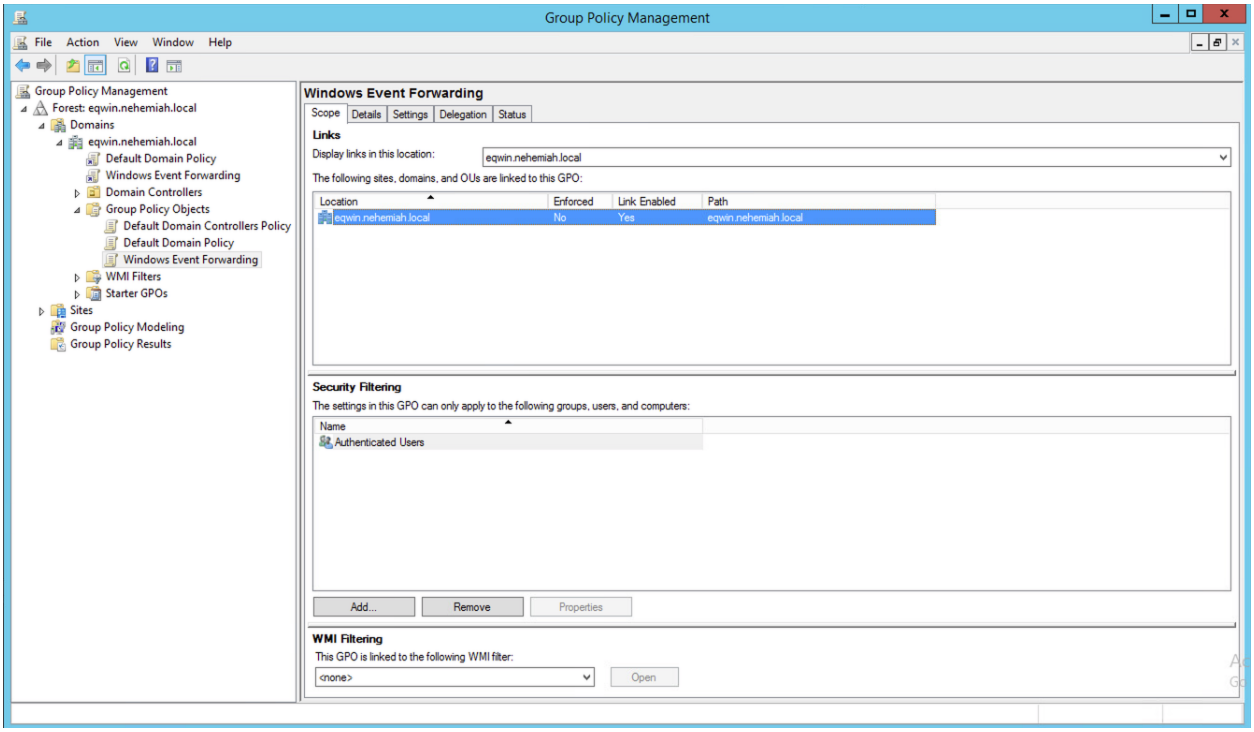
This will ensure that all machines in the domain follow our Windows Event Forwarding policy which means they can find the Subscription link and permit the Network Service to access the events and forward them to our Windows Event Collector.

When you're done with the configuration, you'll be able to see the Windows Event Forwarding policy we created under the domain and vice-versa from the perspective of the GPO.

Here's how it looks from the Domain perspective.



Here's how it looks from the GPO perspective.



Step 7. We will now setup our WEF event channels and subscriptions using the tools from Palantir as a starting point. They include instructions for customization, but I started with the defaults.
To create the corresponding custom event channels for all the subscriptions we will create, run these commands.

Disable the Windows Even Collector Service:

```
net stop wecsvc
```

If you already have a custom event channel, unload it first:

```
wevtutil um c:\windows\system32\CustomEventChannels.man
```

Copy and replace the new custom event channel description files on the WEF server under c:\Windows\system32

```
CustomEventChannels.dll
CustomEventChannels.man
```

Load the new Event Channel file:

```
wevtutil im c:\windows\system32\CustomEventChannels.man
```

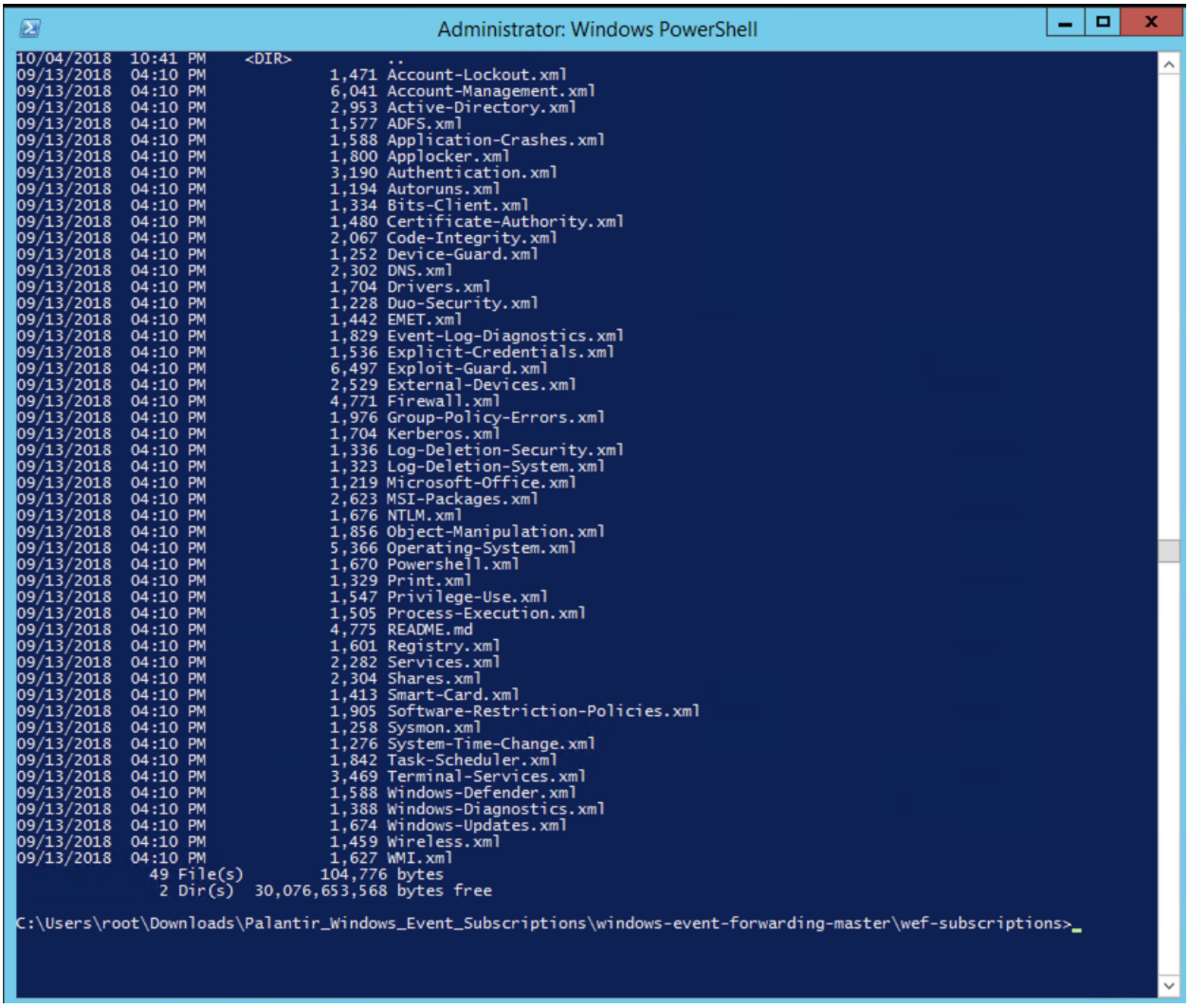
From a powershell prompt, Resize the log files:

```
$xml = wevtutil el | select-string -pattern "WEC"
foreach ($subscription in $xml) {
  wevtutil sl $subscription /ms:4194304
}
```

Restart the Windows Event Collector

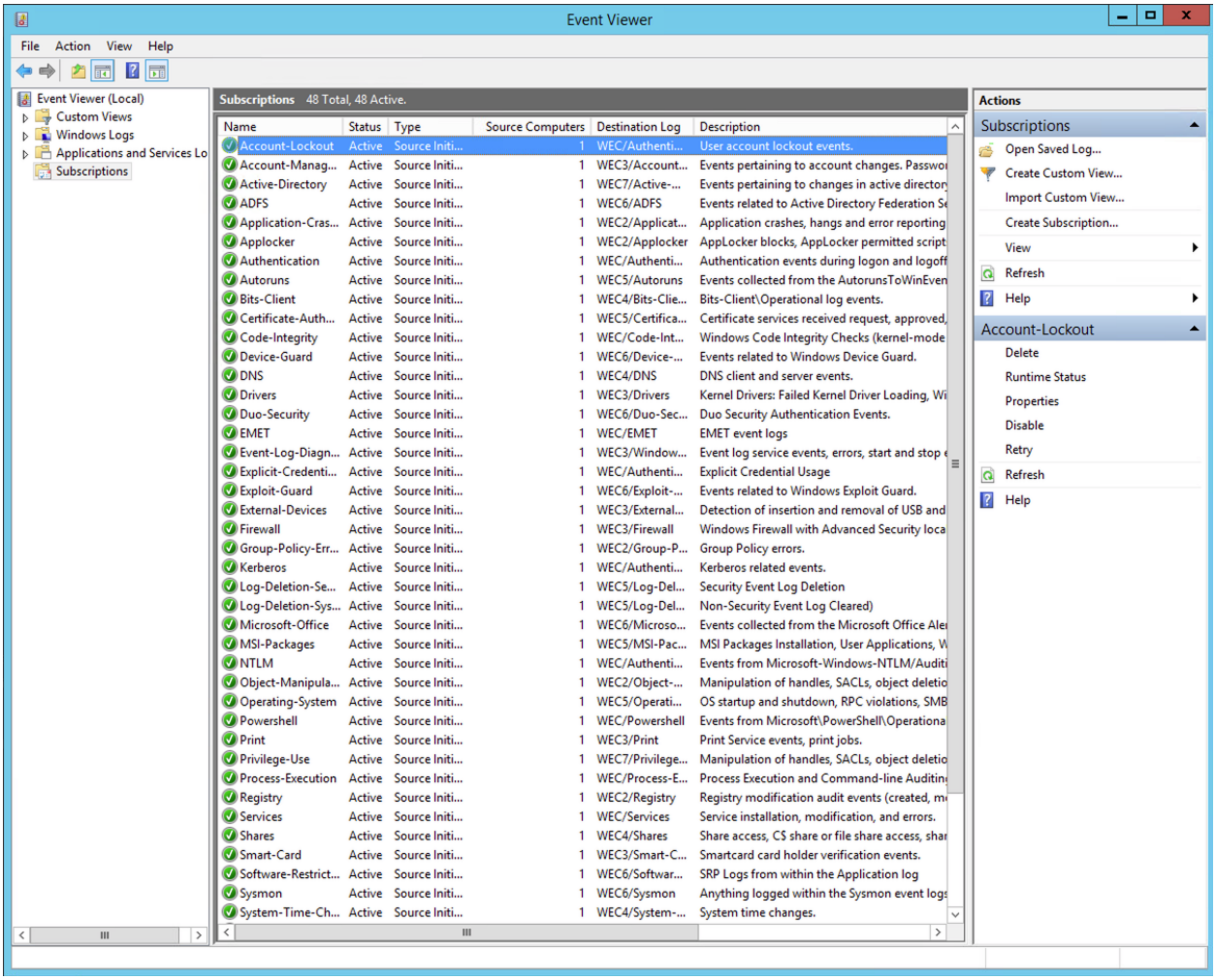
```
net start Wecsvc
```

To create all the subscriptions, cd to the directory containing all the xml files and run this command from a cmd prompt:




```
for /r %i in (*.xml) do wecutil cs %i
```

That should do it. We can fire up the Event Viewer, and we should be able to see all the new subscriptions now, and if any machines in the domain are running, we see them reflected in the subscriber count.



Step 8. The Palantir guidance includes recommendations for which GPOs to create to enable associated auditing policies for the events we can now log. In our case, where we run experiments in a lab, we need the flexibility to enable and disable individual policies on the fly to measure results. Therefore, we configure auditing policies per experiment rather than creating a constant GPO.

Step 9. We need to get these events to the Cybraics analytics engines to get the full benefit that WEF and WEC centralization provides us. We do this by installing a syslog agent on the WEC which in our case also happens to be the Domain Controller for the lab. We use the rsyslog agent to extract the events from the WEC and forward them to the Cybraics DCA, Data Collection Appliance, which in turn feeds them to the Cybraics analytics engines.

Cybraics customers will be provided a link to download the agent and license details and a configuration guide.

References:
Note: These links were immensely helpful and formed the basis of this guide.

The Windows Event Forwarding Survival Guide
https://hackernoon.com/the-windows-event-forwarding-survival-guide-2010db7a68c4

Monitoring what matters – Windows Event Forwarding for everyone (even if you already have a SIEM.)
https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/

Palantir's Windows Event Forwarding Guidance
https://github.com/palantir/windows-event-forwarding

https://medium.com/palantir/windows-event-forwarding-for-network-defense-cb208d5ff86f

Advanced Security Audit Policy Settings
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn319056(v=ws.11)