Monitoring what matters - Windows Event Forwarding for everyone (even if you already have a SIEM.)

By kexugit

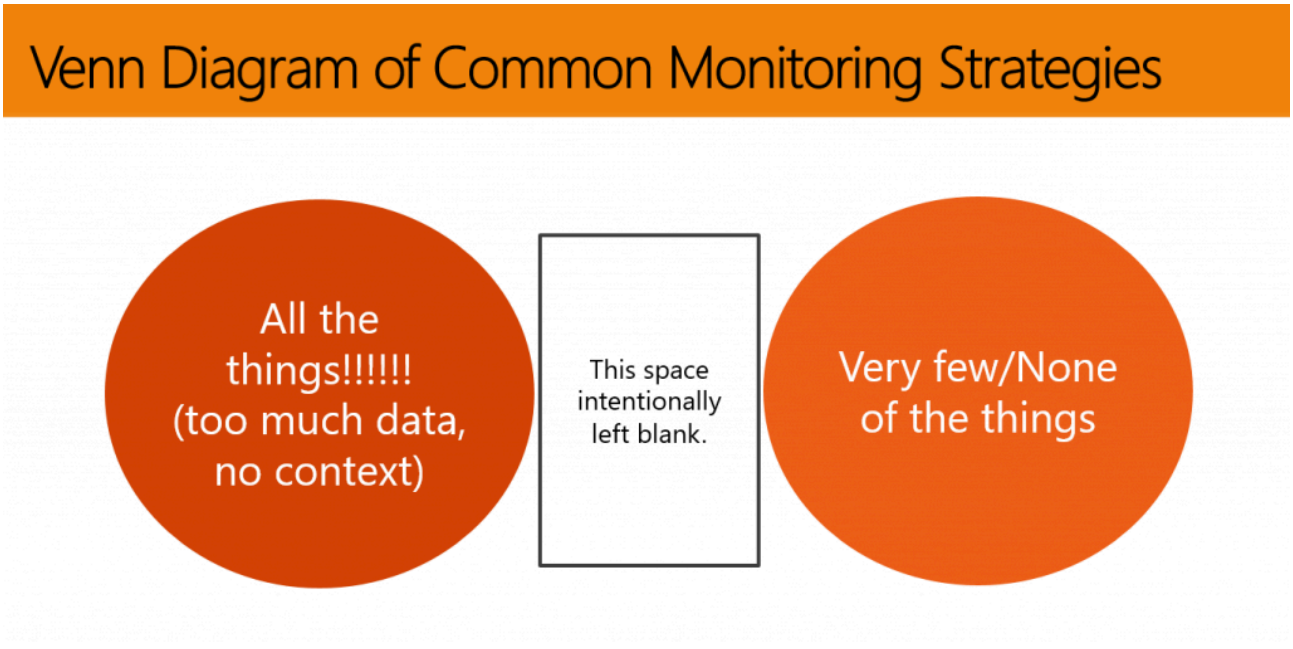
Archived: 2026-04-05 13:05:13 UTC

Last week at Ignite Australia I presented a session (available here) on something I don't think gets talked about enough - Windows Event Forwarding, or WEF. (*Edit: I've also since done an depthMicrosoft Virtual Academy sessionon Event Forwarding too!*).

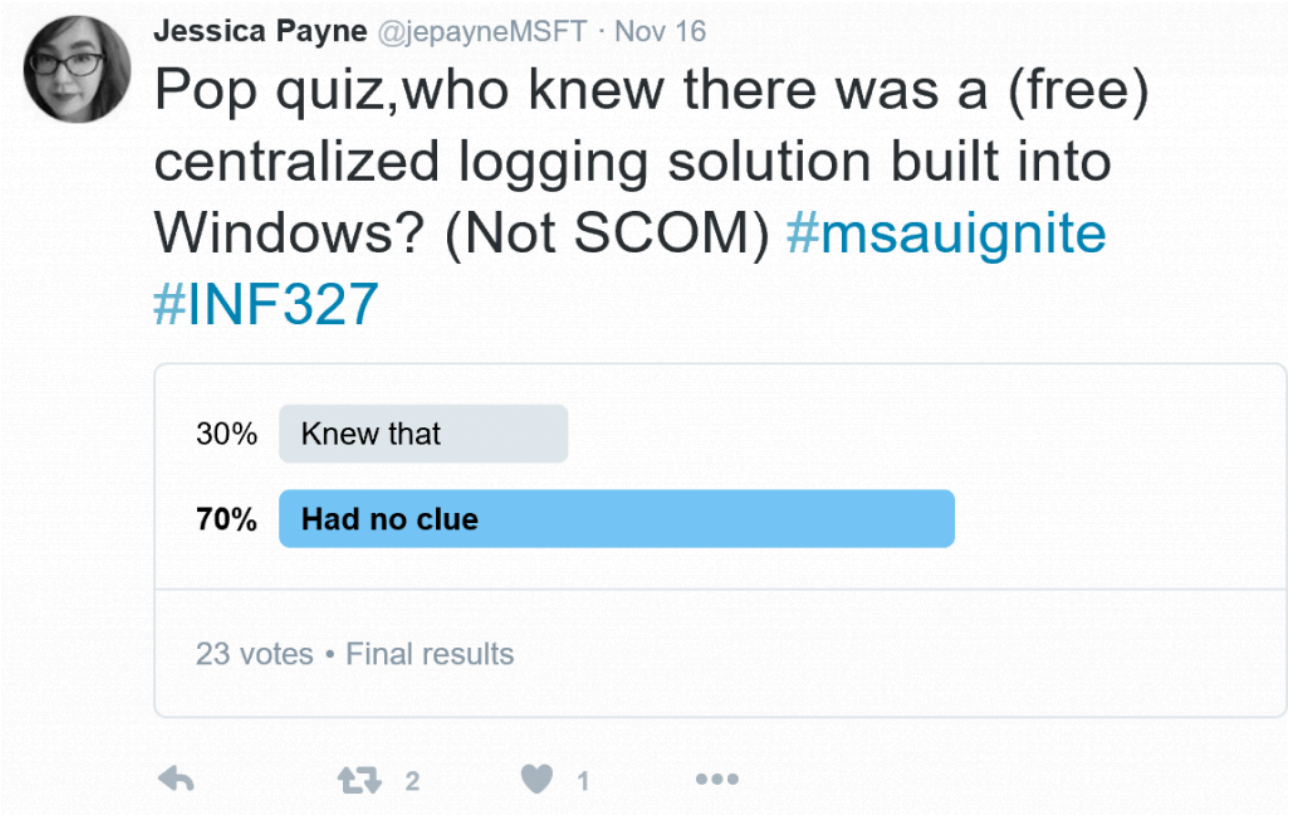
Often when we engage for an Incident Response, we find the customer :

- Has no centralized logging
- Are not monitoring endpoints/member servers (often just DCs)
- Spam logs with extra data
- Are not logging key events
- Logs roll too quickly
- Those with centralized logging still missing data, takes too long for IT admins to get reports

In Internet speak :



WEF's been part of the operating system for a while now, but not many people take advantage of it. Many people appear to not even be aware of it, as evidenced by this highly scientific poll.



WEF is not only free and built-in, it has some nice features when configured appropriately :

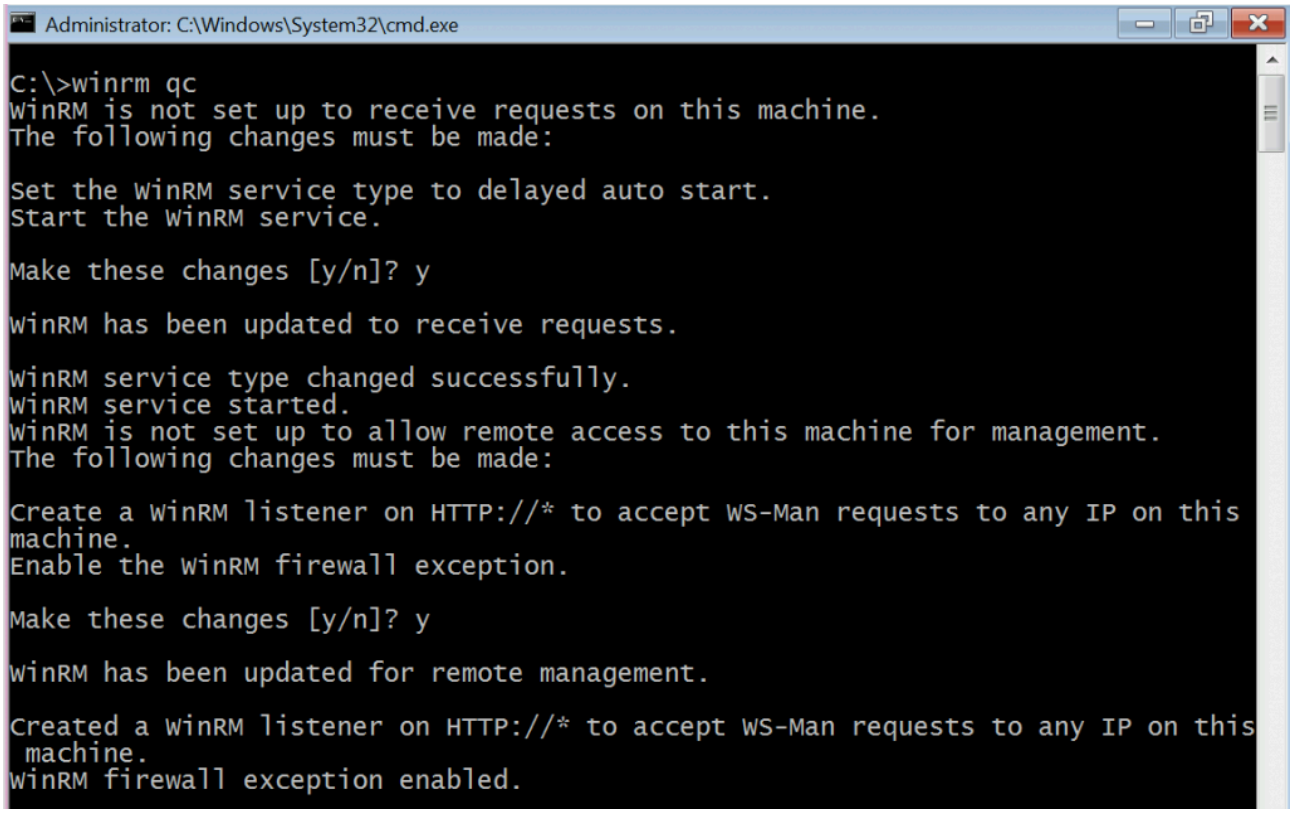
- Works nicely as a compliment to SCOM or SIEM products.
- Can dramatically increase your overall visibility in the environment. Frequently desktops aren't part of the centralized monitoring due to licensing costs - WEF can be setup (for free) to collect the key events from the desktops and then be forwarding on to the SIEM.
- Configured via GPO (easy!)
- Uses Windows Remote Management (Kerberos) to prevent man in the middle
- Can (and should be) targeted to specific events
- Native evtx (xml) log format
- “Push” log mode – less attack surface than adding a monitoring agent or account to a widely privileged group
- IT admins control their own logging destiny - AD guys looking to track down a certain service account don't have to wait on the security team.

Setting WEF up is really easy too. Prerequisites are essentially a server and a GPO. To collect security events, we'll also need to grant the local Network Service principal rights to read that log. This is just the Network Service on the machine itself, so it's not a wide privilege throughout the domain. The WinRM service will also need to be started on all the clients in the domain - just started though, not configured. This is key, as just starting the WinRM service doesn't leave it in a listening state, versus a quick config of the service would make it listening.

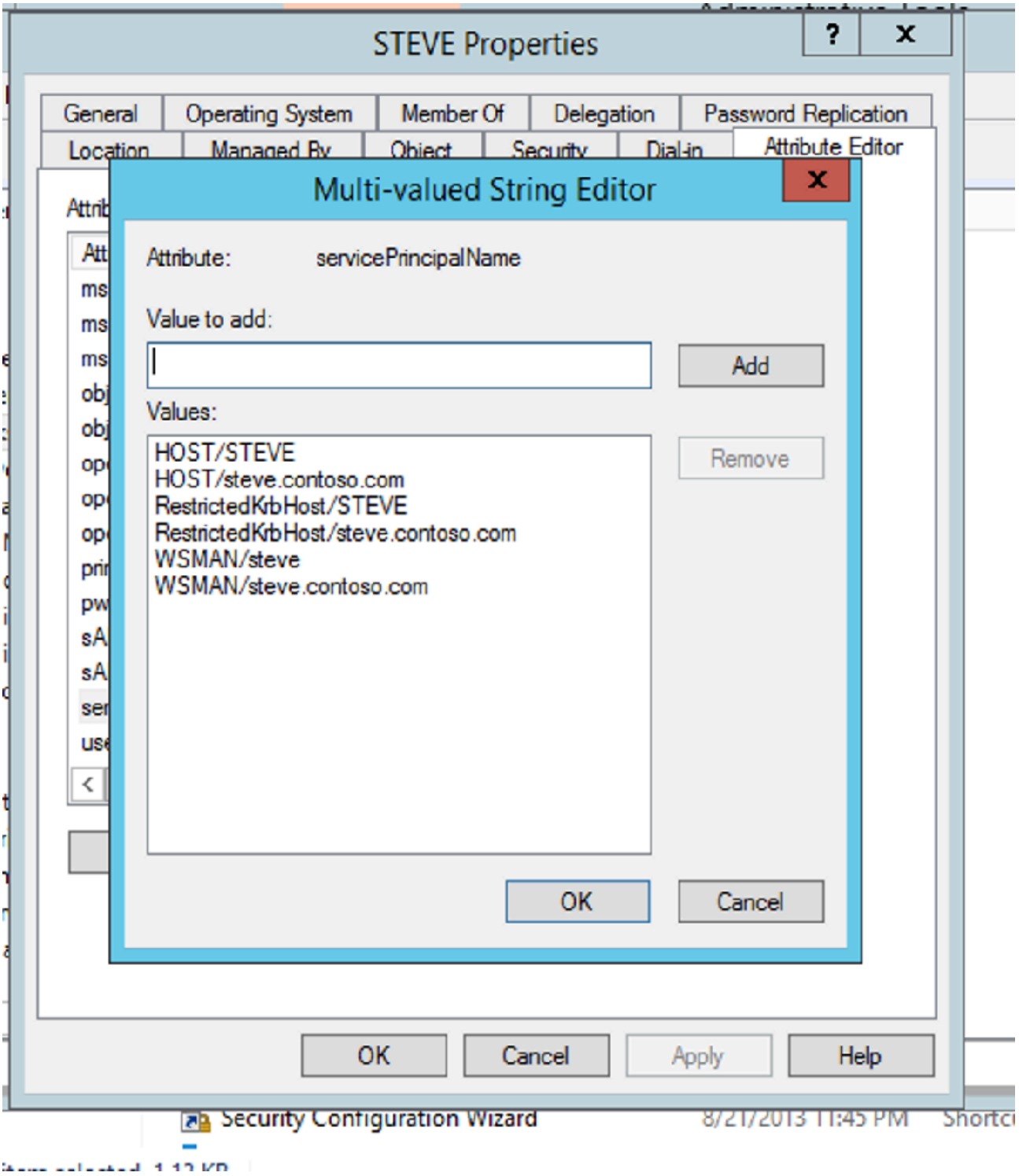
Recommendations for the collector server would be to use 2012R2, although you can even do this on Windows 7 if you have licensing restraints. The log files will be pretty small if you're just collecting targeted/critical events,

so you likely won't need much above and beyond your typical VM drive size but you may want to bump up the memory in the box a bit to avoid race conditions.

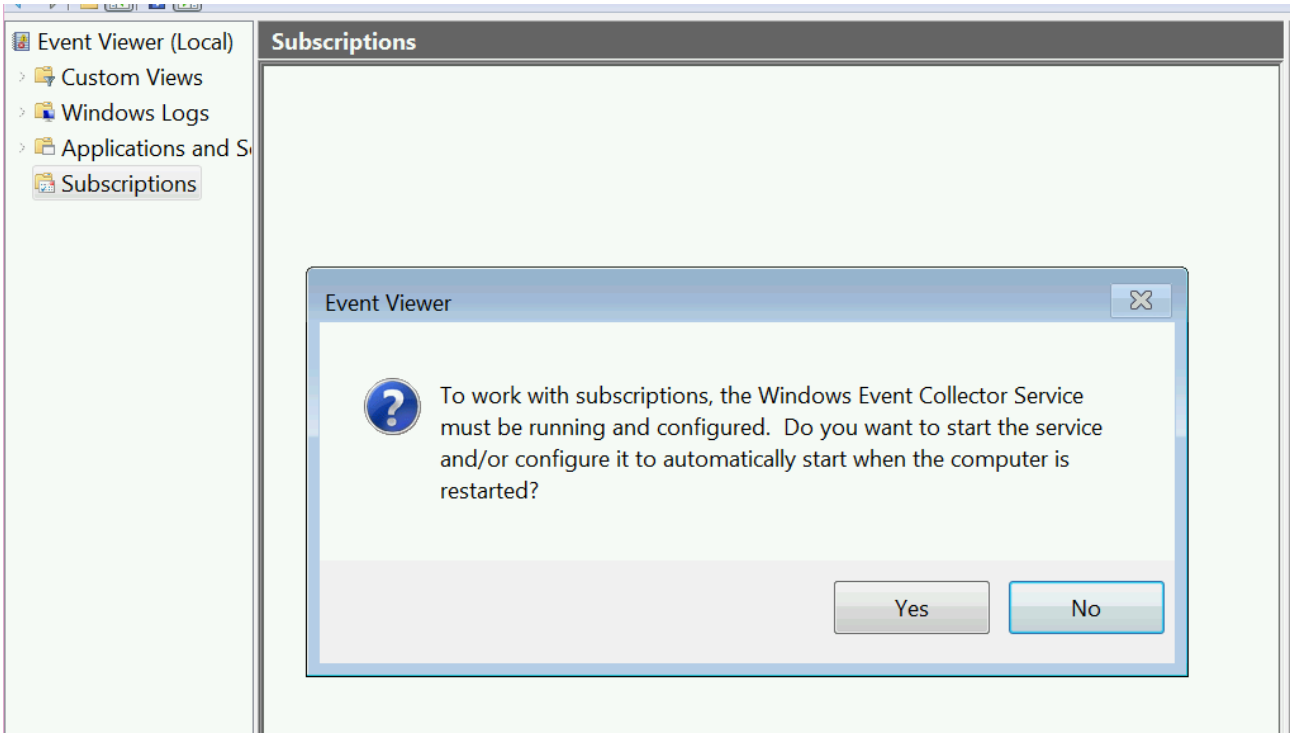
On your collector server, fire up an administrative command prompt (you do have UAC enabled, right? 🙂) and type in winrm qc. You'll then be asked two important questions - do you want the WinRM service to start automatically and do you want to poke a hole in the firewall for WinRM. I'd recommend controlling the firewall with a GPO as well, but go ahead and answer yes to both of these.



When that created the WinRM listener, it also created a Service Principal Name for Kerberos authentication to the service. If something goes flakey with WEF, this is usually where it happens. If the SPNs aren't right, Kerberos authentication can't happen which makes Event Forwarding not work. You may also have noticed the listener is on HTTP ://* - WinRM is at its core HTTP, so while the SPN is WSMAN for WinRM, if you try to install WEF on a server that already has an HTTP SPN Windows Event Forwarding will fail as if it's a duplicate SPN. If you're curious, you can check your SPNs out via attribute editor.



Once WinRM is setup (and hopefully after you've set the firewall via GPO) you can enable Event Forwarding. Open up Event Viewer on the Collector and navigate to the area called "Subscriptions" that you've probably never clicked on before. 🙂 If you haven't clicked on it before, you'll get prompted with this question:



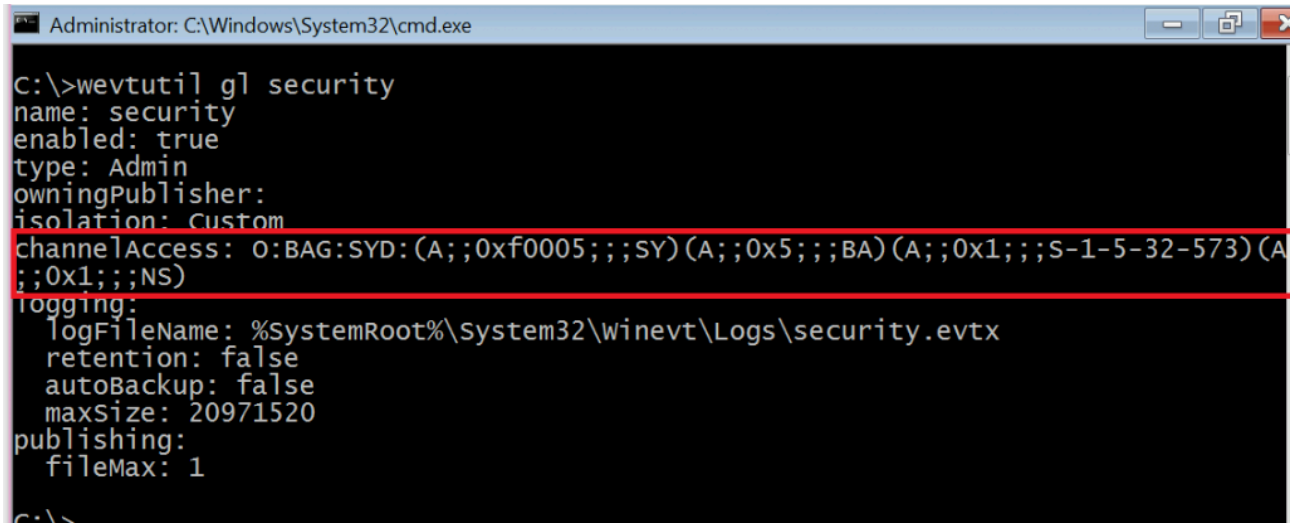
We do need/want the Windows Event Collector to start up automatically with the computer, so go ahead and click yes on that.

And that's it, you've configured a Windows Event Collector! The next trick is to get things report to it.

The best way to do that is via GPO. First things first, we'll need to give the local Network Service principal rights to read the security log. To make sure we don't break anything, run the following command on a server/workstation in your environment:

wevtutil gl security

That will spit out the information about the Security Event Log, as shown below. The weird "O:BAG:SYD:" line is where the permissions on the log are stored. Copy out that line from the O through the last parenthesis and stick it into Notepad. If yours doesn't have (A;;0x1;;;NS) on the end like mine does, append that in Notepad.



Copy the whole O:BAG:SYD line from Notepad, as we'll need it in the GPO. Create a new GPO in your domain to point the systems you want to monitor at the collector server - the same GPO can be used for both member systems and Domain Controllers in your environment, unless you want to point them at different collectors for delegation reasons.

You'll need to configure two settings :

Computer>Policies>Admin Templates>Windows Components>Event Forwarding>Configure target subscription manager

This will need to be populated with the address of your collector server in this format :

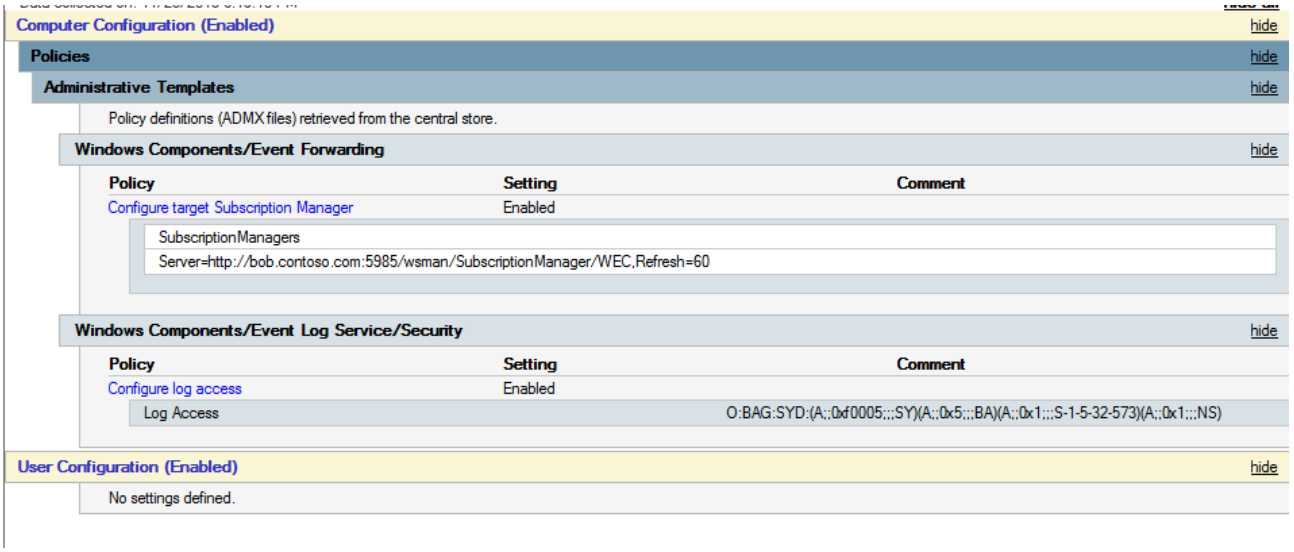
Server=https://fqdnofsubscriptionserver:5985/wsman/SubscriptionManager/WEC,Refresh=60

The refresh interval on the end indicates how often clients should check in to see if new subscriptions are there for them. 60 seconds might be a bit aggressive in production, but it helps out a lot when you're setting things up and testing.

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

This is where you'll need to paste your O:BAG:SYD line from Notepad. Remember this is an authoritative setting, so if you had permissions set some other way on a system in your environment this would replace them.

When you're done, your GPO should look like this:



Now any system that has this GPO will know to check into the web service running on the Windows Event Collector to see if there are any subscriptions for it. Computers only send events when they get a subscription telling them to do so.

So what should you monitor?

You absolutely could configure WEF to collect all the security logs in your domain - and maybe if you don't have any other centralized logging in your domain you should do this for forensic reasons - but the real value of WEF is targeted alerts, filtering out what really matters. This is also where WEF is a great compliment to a SIEM you already have in your environment - let the SIEM do the heavy lifting of collecting every single event and use WEF for targeted visibility, and use WEF to get important security events from workstations/member servers in your environment you may not have covered by the SIEM. The SIEM can then collect them from the WEF server, still providing you with the "single pane of glass" view.

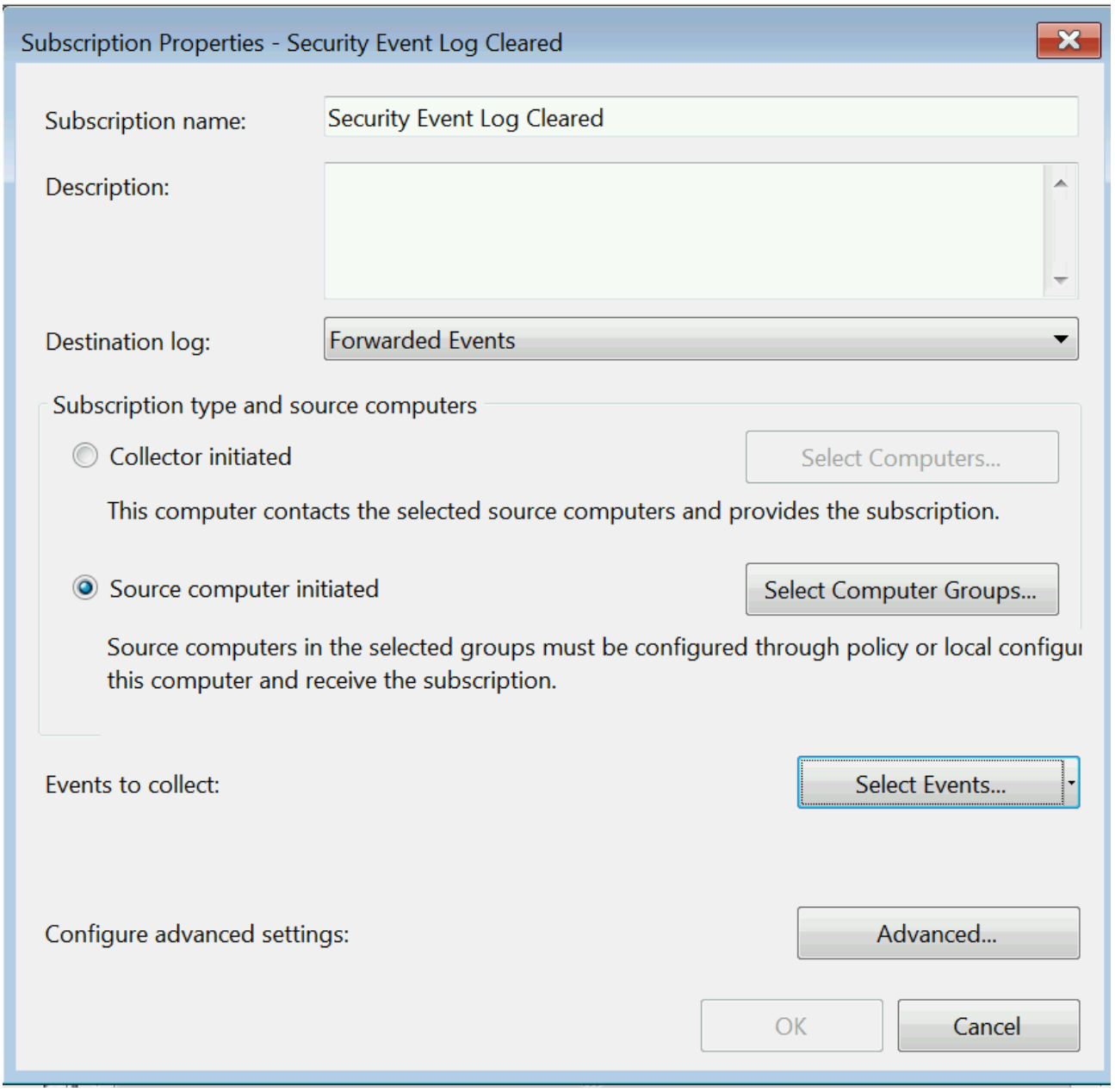
The five basic things I think everyone should start with for monitoring in their domain (if they aren't already) are :

- Security Event Logs being cleared
- High value groups like Domain Admins being Changed
- Local administrator groups being changed
- Local users being created or deleted on member systems
- New Services being installed, particularly on Domain Controllers (as this is often an indicator of malware or lateral movement behavior.)

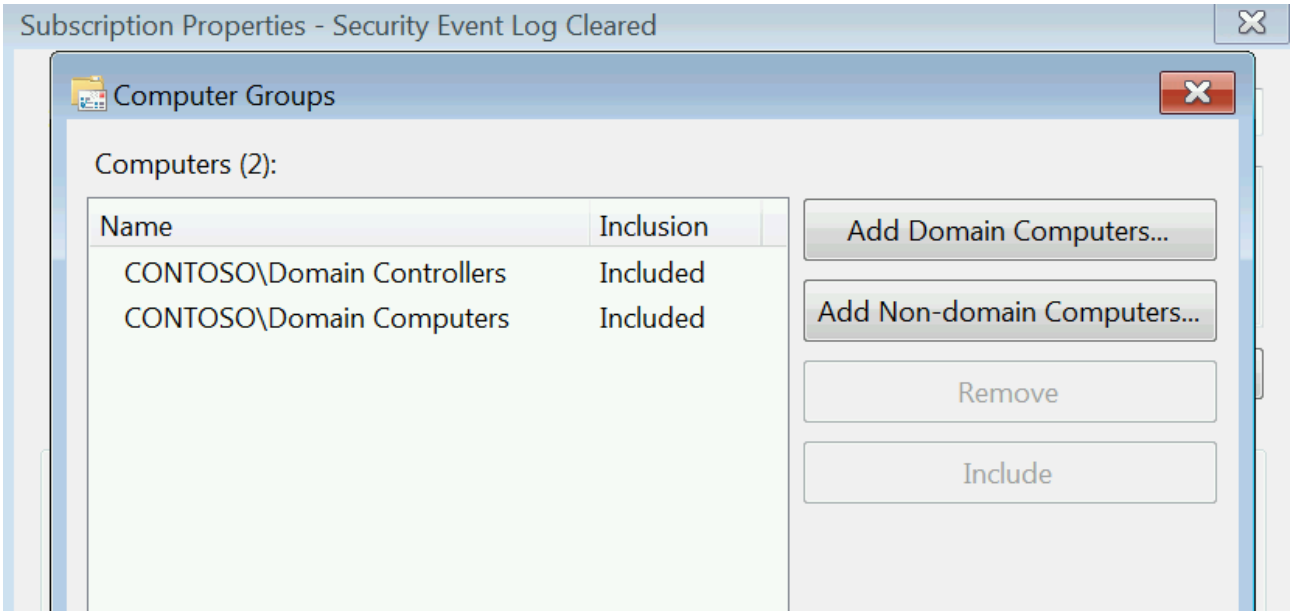
Configuring subscriptions can be done via the GUI (easy mode) or via XPath filters (lots more flexibility.) The settings for the subscriptions do matter though, as this is where you configure the logs to be in "push" mode versus "pull."

Let's configure the Security Event log cleared alert via the GUI:

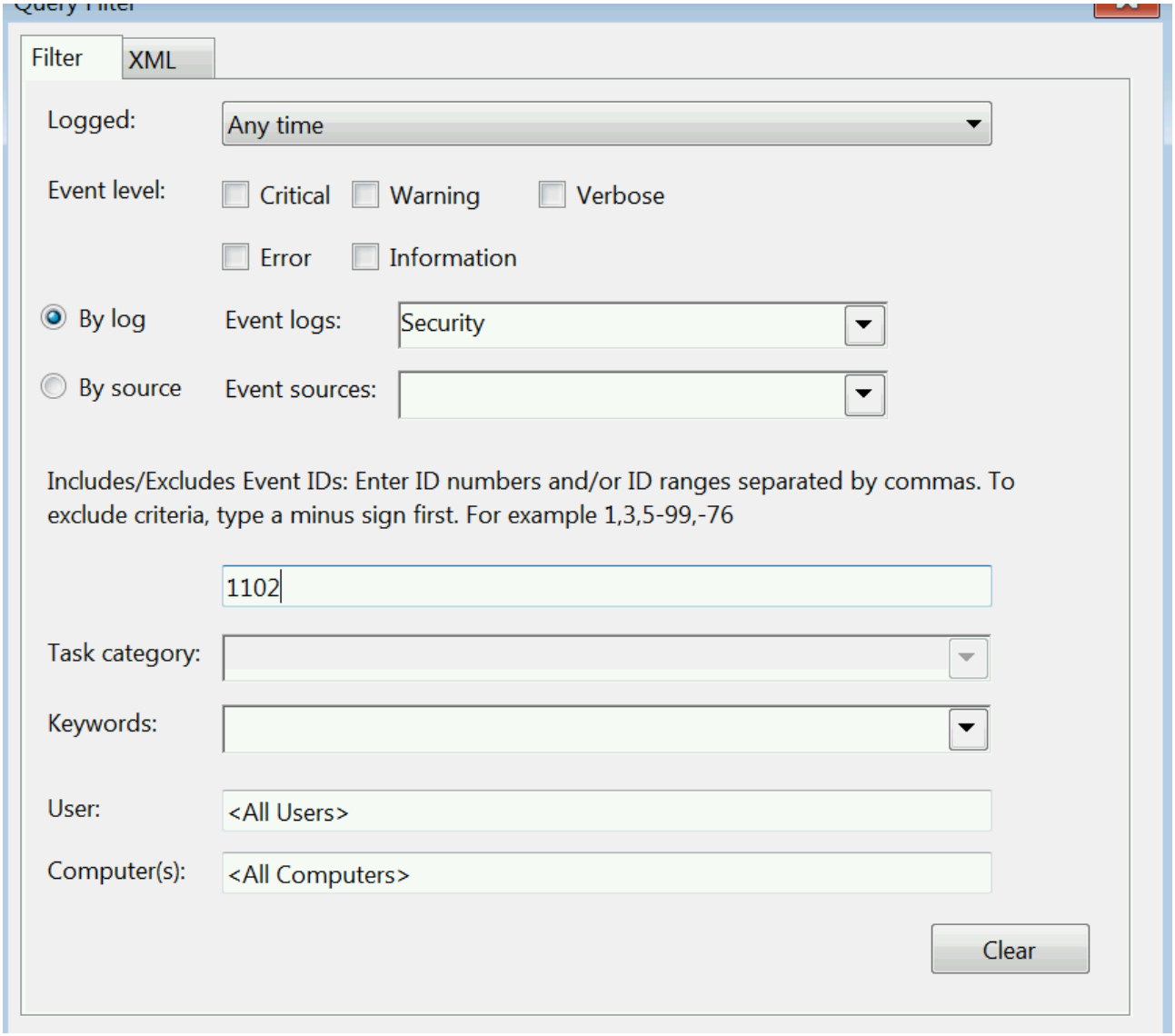
Right click on Subscriptions, then select Create Subscription. We'll need to give the subscription a name and pick "Source Computer Initiated" as that's what makes it "push."



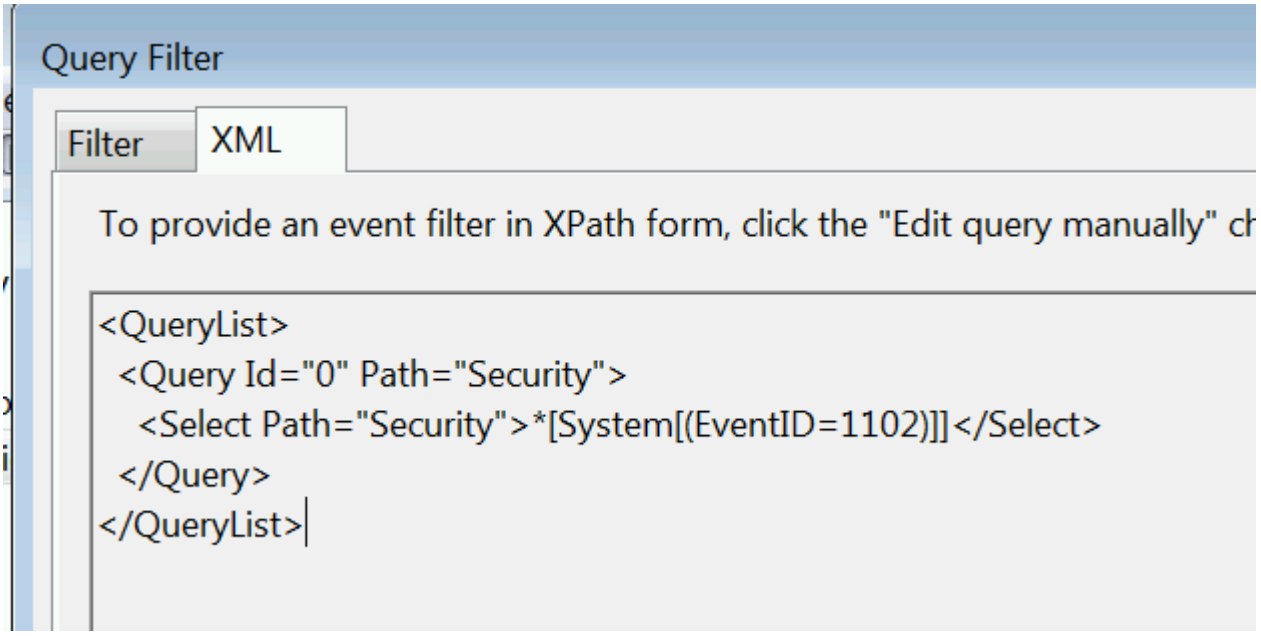
Select Computer Groups next, as this will define which computers send us the events we're interested in. Since we want to know whenever anyone anywhere clears a security log, we're going to use the two built-in/auto populating groups in AD, "Domain Controllers" and "Domain Computers."



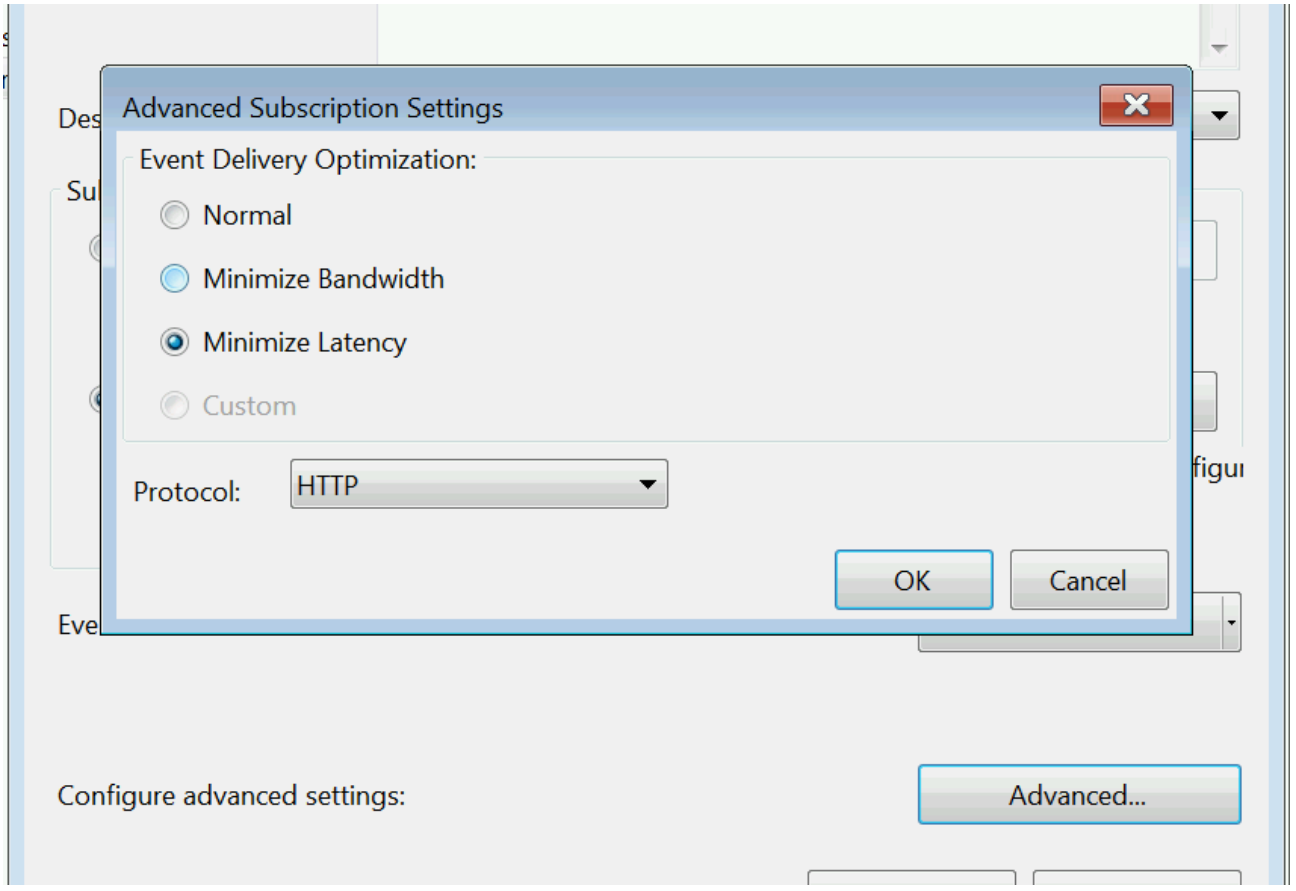
Next we click Select Events to define what we're monitoring. This alert is pretty straight forward, we're looking for Event ID 1102 in the Security log, so we can do it all via the GUI. 🙂



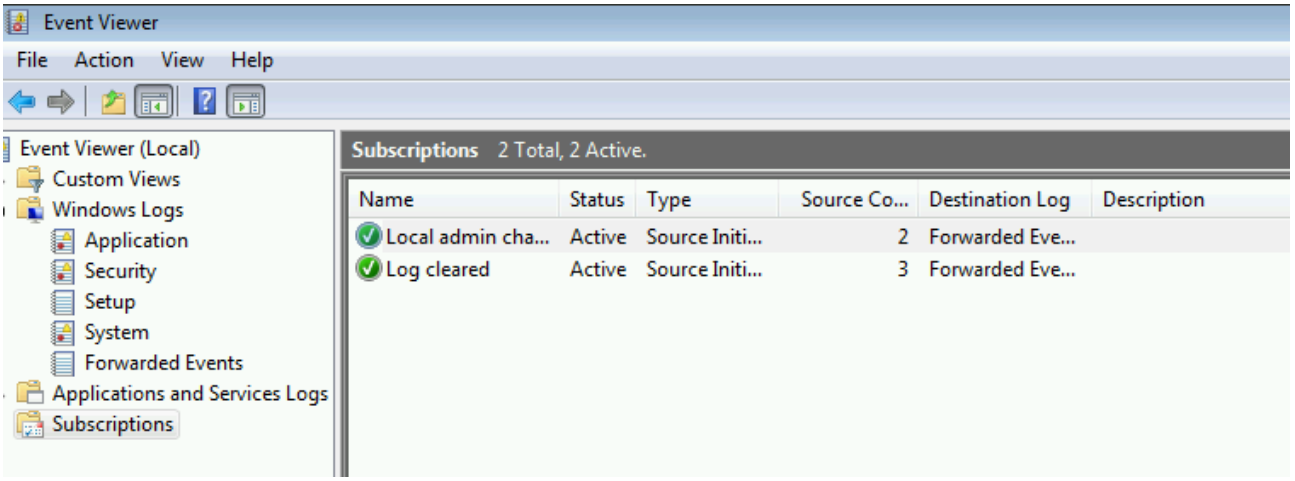
If we click on the XML tab we can see what the XPath filter we just created looks like.



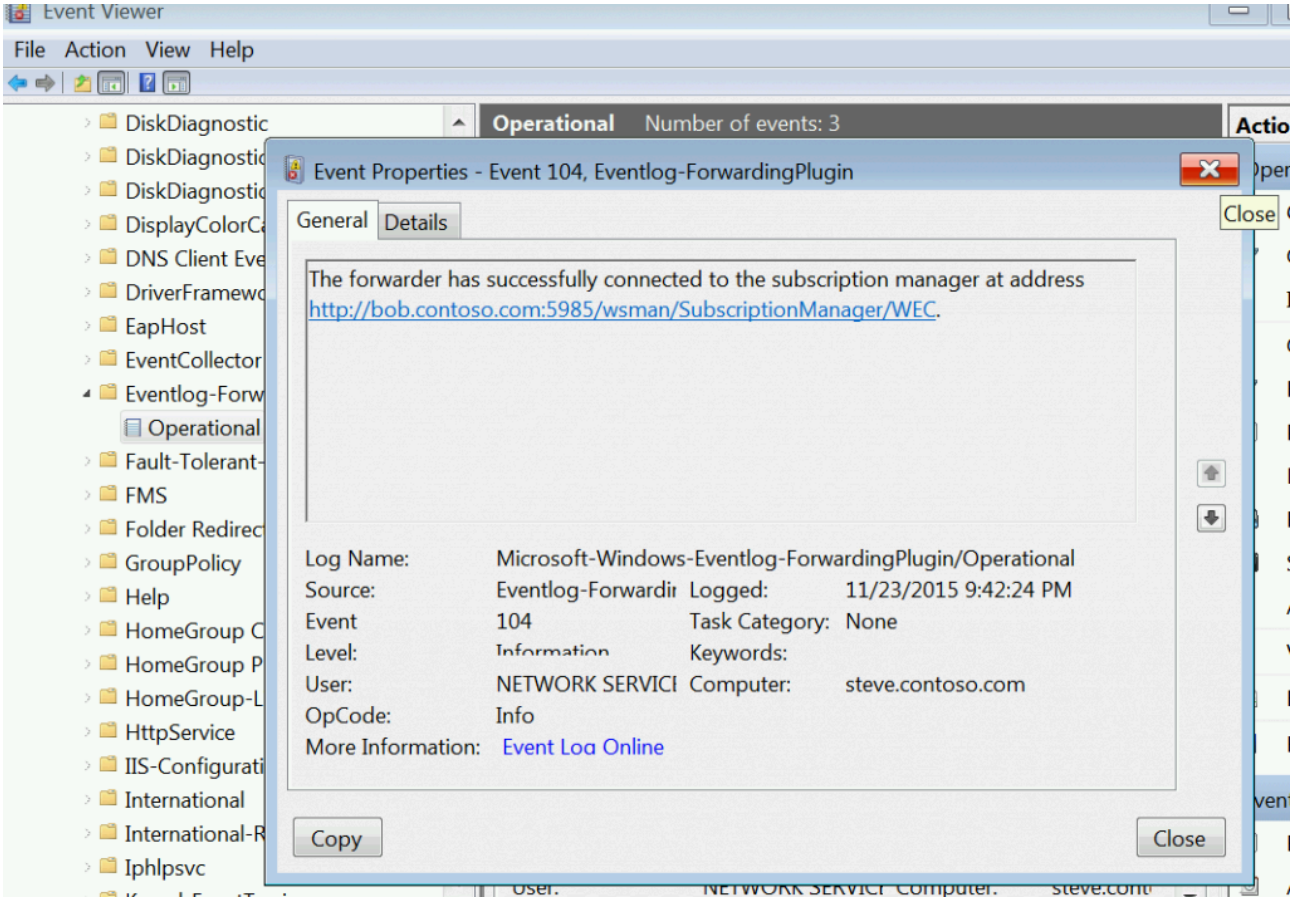
Click okay on that and then click Advanced on the main page. We want to set the subscription to Minimize Latency, to make sure we get events as soon as possible and also to help it catch up if we miss any.



You can troubleshoot that things have actually checked in by checking the Source Computers column on the main Subscriptions page :



You can also check the Event Forwarding Plugin Operational log under Applications and Services on the client to make sure everything is happy. This is where you'll see descriptive errors if something has gone awry with Kerberos or Firewalls.



Click okay and you've got a subscription. Find a low-value test VM, clear the Security log and see if you get an alert. 🙂

Configure those 5 events with cut and paste for two commands? Yes you can!

Thanks to Australian PFE Russell Tomkins, you can do just that. Below are two XML files that contain the appropriate subscriptions for Domain Computers and Domain Controllers. The subscriptions here are maybe a bit

wider than you want in your production domain to start with, as it's collecting services installing on workstations too, but give it a go. We'll want that data if we ever have to do an IR for you.

To import the XML files, save them to a directory on the server and then run the following commands from the same directory on your Windows Event Collector.

wecutil cs DomainComputers.xml

wecutil cs DomainControllers.xml

DomainComputers.xml

```
<Subscription xmlns="https://schemas.microsoft.com/2006/03/windows/events/subscription">
<SubscriptionId>Domain Computer Events</SubscriptionId>
<SubscriptionType>SourceInitiated</SubscriptionType>
<Description>Important Domain Controller Events</Description>
<Enabled>True</Enabled>
<Uri>https://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
<ConfigurationMode>MinLatency</ConfigurationMode>
<Query>
<![CDATA[<QueryList>
<Query Id="0" Path="Security">
<!-- Local Admins Changed -->
<Select Path="Security">
*[EventData[Data[@Name='TargetUserName'] and (Data='Administrators')]]
and
*[System[(EventID='4732') or (EventID='4733')]]
</Select>
<!-- Local user created or deleted -->
<Select Path="Security">*[System[(EventID='4720') or (EventID='4726')]]</Select>
<!-- New Service Installed -->
<!-- Event Log Cleared -->
<Select Path="Security">*[System[(EventID='1102')]]</Select>
</Query>
</QueryList>]]>
</Query>
<ReadExistingEvents>true</ReadExistingEvents>
<TransportName>http</TransportName>
<ContentFormat>RenderedText</ContentFormat>
<Locale Language="en-US"/>
<LogFile>ForwardedEvents</LogFile>
<AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
<AllowedSourceDomainComputers>O:NSG:NSD:(A;;GA;;;DC)(A;;GA;;;DD)
```

```
</AllowedSourceDomainComputers>
</Subscription>
```

DomainControllers.xml

```
<Subscription xmlns="https://schemas.microsoft.com/2006/03/windows/events/subscription">
<SubscriptionId>Domain Controller Events</SubscriptionId>
<SubscriptionType>SourceInitiated</SubscriptionType>
<Description>Important Domain Controller Events</Description>
<Enabled>True</Enabled>
<Uri>https://schemas.microsoft.com/wbem/wsman/1/windows/EventLog</Uri>
<ConfigurationMode>MinLatency</ConfigurationMode>
<Query>
<![CDATA[<QueryList>
<Query Id="0" Path="Security">
<!-- New Service Installed -->
<Select Path="System">*[System[(EventID='7045')]]</Select>
<!-- Member Added or Removed from an AD Domain Local, Universal or  Global Security Group -->
<Select Path="Security">
(*[EventData[Data[@Name="TargetUserName"] = "Administrators"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Domain Admins"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Schema Admins"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Enterprise Admins"]]) or
(*[EventData[Data[@Name="TargetUserName"] =  "Print Operators"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Server Operators"]]) or
(*[EventData[Data[@Name="TargetUserName"] = "Backup Operators"]])
and
*[System[(EventID='4732') or (EventID='4733') or (EventID='4756') or (EventID='4757') or (EventID='4728') or
(EventID='4729')]]
</Select>
<!-- Event Log Cleared -->
<Select Path="Security">*[System[(EventID='1102')]]</Select>
</Query>
</QueryList>]]>
</Query>
<ReadExistingEvents>True</ReadExistingEvents>
<TransportName>http</TransportName>
<ContentFormat>RenderedText</ContentFormat>
<Locale Language="en-US"/>
<LogFile>ForwardedEvents</LogFile>
<AllowedSourceNonDomainComputers></AllowedSourceNonDomainComputers>
<AllowedSourceDomainComputers>O:NSG:NSD:(A;;GA;;;DD)</AllowedSourceDomainComputers>
</Subscription>
```

If you have more than one domain, you'll need to specify the SIDs of Domain Computers/Domain Controllers in the <AllowedSourceDomainComputers> line as well as the DC (Domain Computers) and DD (Domain Controlls) SDDLs that are in there.

Hope this helps. Be sure to check out my post on tracking Special Groups with WEF and look forward to more things you can do with WEF in future blog posts! Happy Logging!

-Jessica @jepayneMSFT

- **Anonymous**
  November 23, 2015
  The comment has been removed
- **Anonymous**
  November 24, 2015
  The video of the presentation has now been posted, well worth watching.
  https://channel9.msdn.com/Events/Ignite/Australia-2015/INF327
- **Anonymous**
  November 26, 2015
  Lateral Movement - the moving of an attacker from one compromised host throughout your domain until they
- **Anonymous**
  November 30, 2015
  Sounds like a great session!
- **Anonymous**
  December 02, 2015
  Thanks again Jessica. I watched this at Ignite and watched the recording to refresh.
- **Anonymous**
  December 24, 2015
  Hallo - is this traffic sent plaintext across the network?
- **Anonymous**
  December 24, 2015
  The comment has been removed
- **Anonymous**
  December 28, 2015
  Hey Jessica. I've been using this method since you led a POP-SLAM engagement a few months back. Glad to see you blogging!

  I wanted to throw this in for people interested. I started to work on a PowerShell module for Event Subscriptions, but it still needs a lot of work. It's basically a wrapped for wecutil, but was made with automation in mind.

  https://github.com/davidhowell-tx/PS-WinEventSubscriptions

I also have a script posted that uses the module. It queries AD for Domain Admins membership and updates a subscription with the members' SamAccountName for monitoring.

- **Anonymous**
  December 28, 2015
  Hi, Jessica Payne from Microsoft Enterprise Cybersecurity Group's Global Incident Response and Recovery
- **Anonymous**
  December 30, 2015
  Hi David - glad you've been able to put the SLAM stuff into practice! You guys were super fun. (Embrace the 500 account!)

  Spoiler alert for the posts ahead, there's a Powershell logging module at the end of it that ties into the PowerBI dashboards - the fact you made your own is super cool too!

  Keep up the good work and innovation. :)

  -Jessica

- **Anonymous**
  January 11, 2016
  This is really handy and I'm in the middle of implementing it however, we use group policy preferences to change the local admins group so everytime a machine boots up, it changes the membership of the group and forwards and event, meaning we have 300 events every morning just from powering up. is there anyway to filter xpath to not monitor the groups added to local admin?
- **Anonymous**
  January 11, 2016
  More great stuff from you, Jessica, thanks so much! I'm wondering if there's a benefit or negative to creating separate subscriptions vs. combining the filters into one event in terms of processing or traffic for either the source or destination servers? For example, if I also want to monitor the special groups (I do!) I could create a new subscription or I could modify the existing subscriptions with the additional filter elements. Is one solution empirically "better" or "worse" than another, or is it purely dealer's choice?
- **Anonymous**
  January 12, 2016
  Tom - there's a way to filter based on who is doing the change, GPO should be done by SYSTEM so you could "suppress" those (knowing you might miss something.) The dashboard at the end of the series should help too. Are you doing adds or Restricted Groups? I'm a bigger fan of Restricted Groups.

  -Jessica

- **Anonymous**
  January 12, 2016
  Tony - I like to use different subscriptions so I can track if something goes wrong in the Event Forwarding Plugin operational log, but you can also use one big "security stuff" or "operational stuff" subscription for

simplicity too. So sort of your choice? :)
-Jessica

- **Anonymous**
  January 15, 2016
  We're adding a security group of I.T. staff to the local admins group by GPP. Not sure how restricted groups work but if you could point me in the direction of a good article I can certain start researching.
  - **Anonymous**
    May 18, 2016
    The comment has been removed
    - **Anonymous**
      May 20, 2016
      The comment has been removed
    - **Anonymous**
      May 20, 2016
      Suppress Path="Security">*[EventData[Data[@Name="SubjectUserSid"] = "S-1-5-18"]]
      </Suppress
- **Anonymous**
  January 25, 2016
  Hi, The Captain here from Microsoft Enterprise Cybersecurity Group's Global Incident Response and
- **Anonymous**
  February 23, 2016
  Jessica - great post and glad this topic seems to be getting more coverage. I have a OneNote notebook full of references trying to piece together a best practice approach.

  In all my research it would appear you can create an event log on the collector server other than the Forwarded Events, but I never seen a post on how. The reasoning behind this would be to push domain controller logs at one log with the corresponding file on a dedicated and performant disk (we generate around 750GB per day) and create other event logs for member servers and clients (again spreading out the disk IO load). Is this possible and if so how?

  Thanks

  Paul

- **Anonymous**
  February 23, 2016
  Paul - yes you can do that! It was hard to get working reliably but we got some help from MSIT on how they do it and have it being tested at some customers now. Should be part of an upcoming post once we make sure it is still reliable at 500k+ endpoints.
  - **Anonymous**
    March 10, 2016
    The comment has been removed
    - **Anonymous**
      May 23, 2016

For those wishing to create custom event logs, Russell Tomkins has blogged about the way we do it inside of Microsoft : https://blogs.technet.microsoft.com/russellt/2016/05/18/creating-custom-windows-event-forwarding-logs/

- **Anonymous**
  March 09, 2016
  Hi Jessica, I am looking forward to implementing WEF in my current company after seeing this presentation. We have been reviewing SIEM providers for sometime now and it's a minefield for sure. I agree with some of your comments from the presentation that one needs to be clear about the type of events that are being logged. I believe there are a key list that everyone should focus as essential but each company should know what's important to them beyond that. Can you recommend how to create a dashboard for the events?
- **Anonymous**
  May 18, 2016
  Thanks for this article Jessica, it is extremely helpful.This is simple but I stumbled so I thought I would share to help anybody else doing this.I glossed over the whole “WinRM must be started” part so my first attempt did nothing.Add this to your GPO to get it up and running:Computer > Policies > Windows Settings > Security Settings > System Services > Windows Remote Management (WS-Management) Startup = Automatic@dconsec
- **Anonymous**
  May 24, 2016
  Hi Jessica,I had a similar issue with HTTP SPN.And I had concluded that to make a denial of service of Event Forwarding you just have to do a setspn...What's your thoughts on that ?How do you monitor that clients are still sending events to collector ?RegardsGreg
- **Anonymous**
  June 30, 2016
  Thanks for this post. Very easy to follow. Thank you! One thing -- The tag in the DomainComputers.xml section looks like it might be incorrect as it mentions domain controllers.
- **Anonymous**
  July 22, 2016
  Thank you so much, Jessica! You just fixed the last issue I was having setting this up.The MSDN docs don't mention the access restrictions on the Security logfile, so I was a bit confused when some of our servers didn't send their Security logs (but others did, go figure).So that other people can Google the error I was having now to find this article: Event 101, Eventlog-ForwardingPluginStatus SubscribePartialSuccess returned status data which included:
  - **Anonymous**
    August 23, 2016
    The comment has been removed
    - **Anonymous**
      September 15, 2016
      Hi David - check out my reply to Joel for a fix, this is a known issue between versions.

- **Anonymous**
  September 13, 2016
  The comment has been removed
  - **Anonymous**
    September 15, 2016
    There's an error in the XML schema for 2012R2 since it was made on 2008R2. Best way to ensure it imports is to make a new subscription via GUI and export using :wecutil gs "%subscriptionname%" /f:xml >>"C:\Temp%subscriptionname%.xml"You can then use that one as a template and just change the XPath portion.
    - **Anonymous**
      November 10, 2016
      This isn't working for me still Jessica. I've created the subscription on a 2012R2 host, exported it, but then can't import it again (even if i dont change the exported file!). Any ideas?
      - **Anonymous**
        December 13, 2016
        Does the import display any error? -Jessica
- **Anonymous**
  October 07, 2016
  The comment has been removed
- **Anonymous**
  October 20, 2016
  Thanks for the article. Works fine, however occasionally the source computers will turn into an inactive state for apparantly no reason. See my reply to a thread about this here: https://social.technet.microsoft.com/Forums/en-US/3d62d46b-33e7-4db6-b672-8555fd6a9f35/event-log-forwarding-subscription-is-unsubscribed
- **Anonymous**
  November 17, 2016
  What about environments where there are thousands of users forwarding events per day, is there built in options for load balancing between multiple WEC servers?
  - **Anonymous**
    December 13, 2016
    Load balancing in WEF/WEC (in a supported way) is achieved by putting multiple collectors in the GPO - then it will send a copy of the event to each server, while maintaining the "bookmark" of which was sent last. While network load balancing solutions are possible, due to the bookmark manner or operation it will have the same net result of sending a copy to each server leading to duplicates. -Jessica
    - **Anonymous**
      January 30, 2017
      We're attempting this via network load balancing right now. We also have a single virtual address (VIP + FQDN + SPN) which fronts four event collectors on the backend.If the setup is source-initiated, I'm hoping that this wont mean that the backend servers would get

duplicate events, since any bookmark being maintained by each client would only point to the virtual address.@Jessica - is this correct? is one bookmark maintained by the client for the last event sent, or is it maintained per last event sent to each server?

- **Anonymous**
  August 07, 2017
  did you get network load balancing working ?

- **Anonymous**
  January 12, 2017
  Hi Jessica, I decided to roll with WEF after reading this post! Any ideas as to what would give an eventid of 102 with error 5004? I'm testing the collection of sysmon logs from Microsoft-Windows-Sysmon/Operational but it keeps erroring with: The subscription Collect Sysmon Logs can not be created. The error code is 5004.
- **Anonymous**
  February 22, 2017
  I assume there is no way to do wildcards since Microsoft is using XPath 1.0?
- **Anonymous**
  March 28, 2017
  Hi Everybodyquick question...Is it possible to implement a WEC server to address multiple forest ? If yes, is there any technical aspects I should take care of ? (We had implemented a WEC servers, we can subscriptions from other forest, but logs are not forwarded..;despite GPO is applied)Thanks in advance for your inputs / Cheers / Kristoff
- **Anonymous**
  April 19, 2017
  Thanks for the Jessica! I am monitoring security logs for changes (4728, 4729) and it does not work with security groups under the 'Builtin' OU (e.g. Administrators) and also the 'Users' OU (e.g. Domain Admins) although the respective audit policies are enabled for these OUs. Any suggestions on how to deal with this quirk gracefully with WEF?
  - **Anonymous**
    April 19, 2017
    Ah - found the problem. I was just forwarding events for domain global groups. Added the respective event log IDs for universal and domain local groups. See https://technet.microsoft.com/en-us/library/dn311500(v=ws.11).aspx
- **Anonymous**
  May 30, 2017
  Great article and video. One question/comment - my understanding is that running WinRM with the quick config (qc) switch also starts WinRS by default, which may be an unintended security issue if admins aren't aware and haven't explicitly blocked WinRS through GPO (assuming they don't need it).
- **Anonymous**
  July 27, 2017
  The comment has been removed
- **Anonymous**
  August 08, 2017

Hello Jessica,I have (2) Windows 2012 R2 servers setup as WEF Collectors and I have several Source Initiated Subscriptions in place. One of the Source Initiated Subscriptions is dedicated to pulling Security Log information from (14 Domain Controllers.)This subscription is setup using HTTPS and collects Security Log Events only.When I check the Runtime Status, one of the DC's shows as "Inactive" and no event log information is being captured for the DC.I believe this was working when it was initially setup. The WEF GPO that is assigned to the Domain Controllers OU is configured correctly:server=https://ServerName.DomainName:5986/wsman/SubscriptionManager/WEC,Refresh=60Can you please tell what I am missing in order to get this one DC to show up as Active"Thank youGlenn

- **Anonymous**
  August 31, 2017
  The comment has been removed
- **Anonymous**
  September 15, 2017
  These instructions are great! They got me up and running in no time. I've just started experimenting with WEF for use in the enterprise and I've come across an odd scenario that I have not seen documented elsewhere. I have WEF setup with a simple Powershell subscription that includes 4103 and 4104 event IDs. I've tried it with a few simple PS scripts, and everything works as expected.However, I got a little more ambitious and ran a 2MB mimikatz script that had Base64 encoded executables embedded in it. The appropriate 4103 and 4104 (script block logging) events were generated on the endpoint. However, instead of forwarding the events to my collector, the subscription for Powershell events started 'flapping' and alternating between the subscription being created and removed (event IDs 100 and 103, respectively in the Eventlog-ForwardingPlugin channel). There are 200+ sizable 4104 events being generated by the script, so I wonder if the size/number of the events is causing an issue. One other detail…if I remove 4104 events from the subscription, and run the mimikatz script, everything works as expected and the 4103 events appear on the collector.
- **Anonymous**
  December 11, 2017
  Jessica,You deleted the content on the last update.
  - **Anonymous**
    December 12, 2017
    Woops, fixed. Thanks for catching it.
  - **Anonymous**
    December 18, 2017
    JPayne,This content is too outrageous to not be on the internet! I was looking for it during an incident after i changed jobs and had to pull it from memory. Keep up the awesome work.
- **Anonymous**
  December 16, 2017
  Hello Jessica - Great read!!One question I have is amount of space I need to factor for my central server to collect the security logs. I am looking to collect these events from around 15000 endpoints. On an average how many events per sec are generated from the Win10 machines and what would be size of each event
- **Anonymous**
  December 19, 2017

Great post Jessica! I will be forwarding this to all of my customers.

- **Anonymous**

  April 10, 2018

  Is it possible to forward the whole Windows eventlog? (Not only: Application, Security, Setup, System, for example "Applications and Services Logs/Microsoft/Windows/Hyper-V Worker")
