How to Configure Windows Event Forwarding (WEF)

Task. Configure WEF.

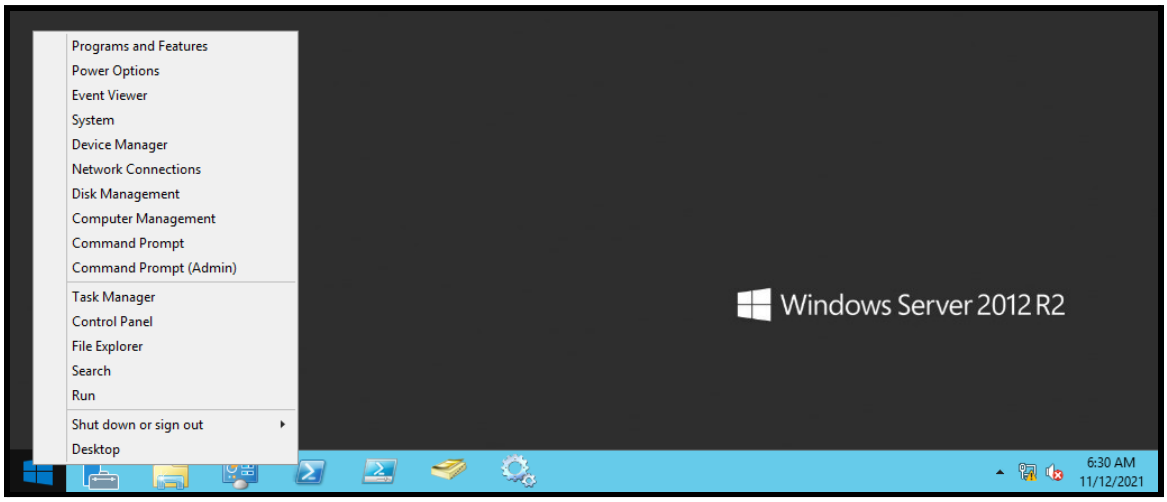
Purpose. WEF allows for Windows events (a.k.a “logs”) to be pushed/pulled to one or more Windows Event Collector (WEC) servers.

Conditions. You have domain administrator privileges and access to either a domain controller or a workstation with Remote Server Administration Tools (RSAT) installed.

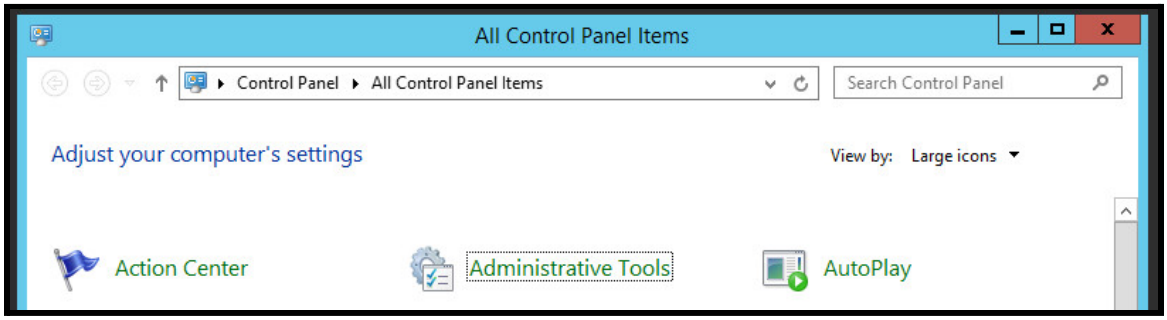
Standard. You were able to create a Group Policy Object (GPO) for WEF.

Step 1. Login to your domain administrator account on either a domain controller or a workstation with RSAT installed.

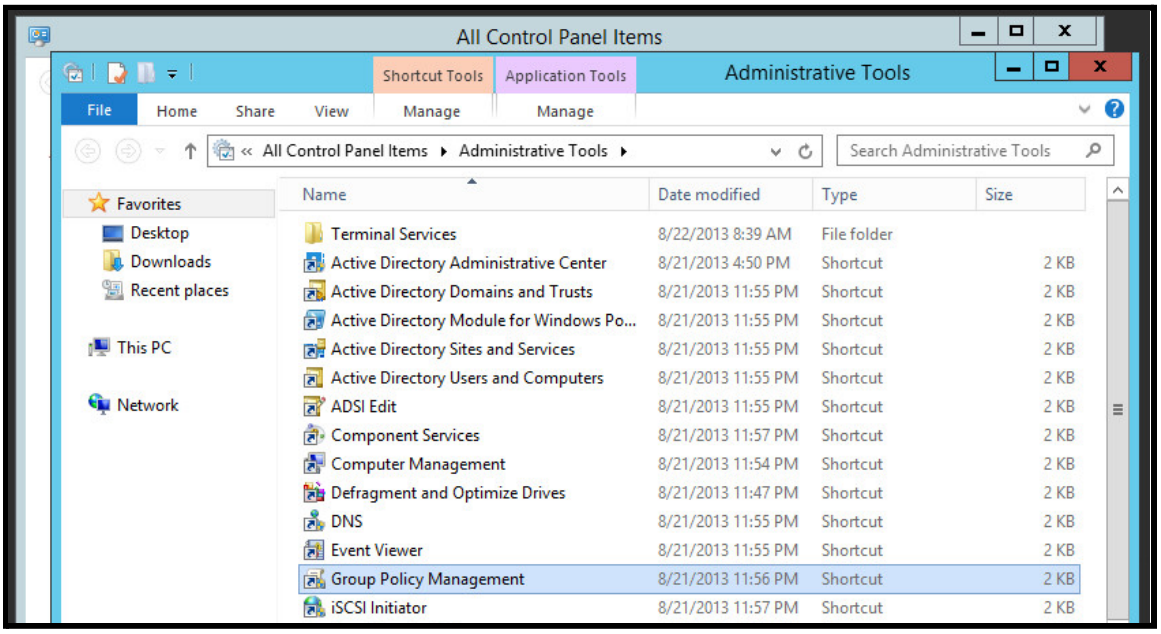
Step 2. Right-click on the Windows icon in the bottom-left corner and select “Control Panel.”



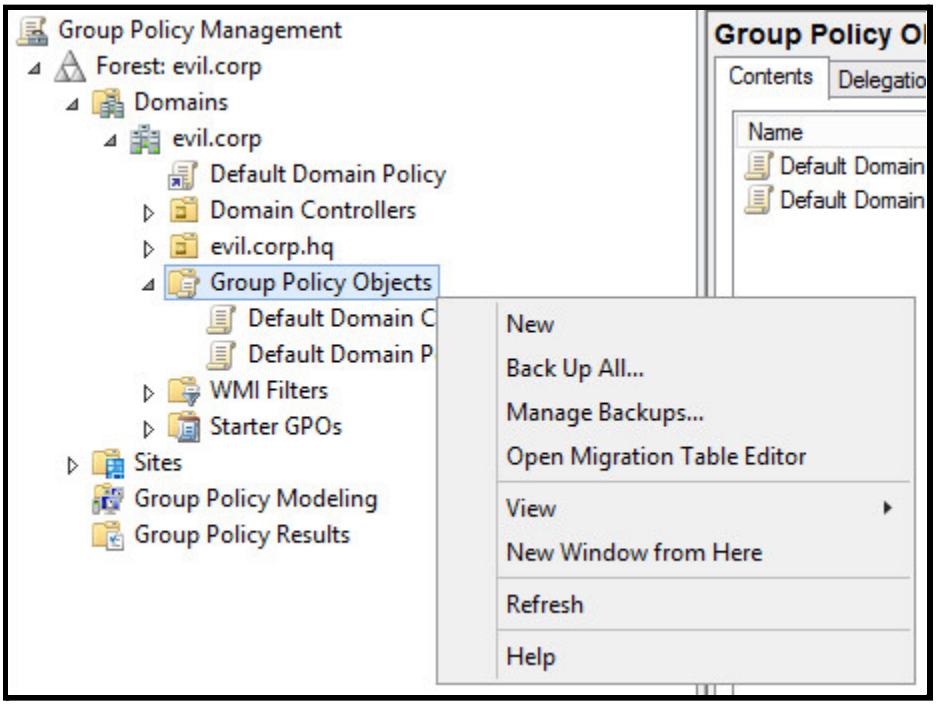
Step 3. Click-on “Administrative Tools.”



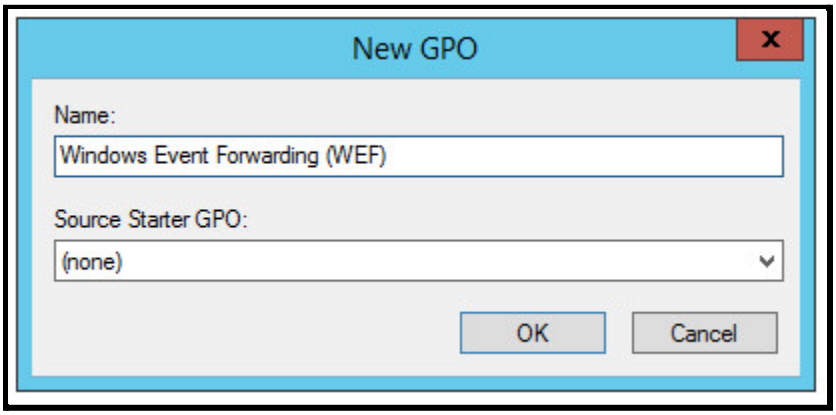
Step 4. Double-click “Group Policy Management.”



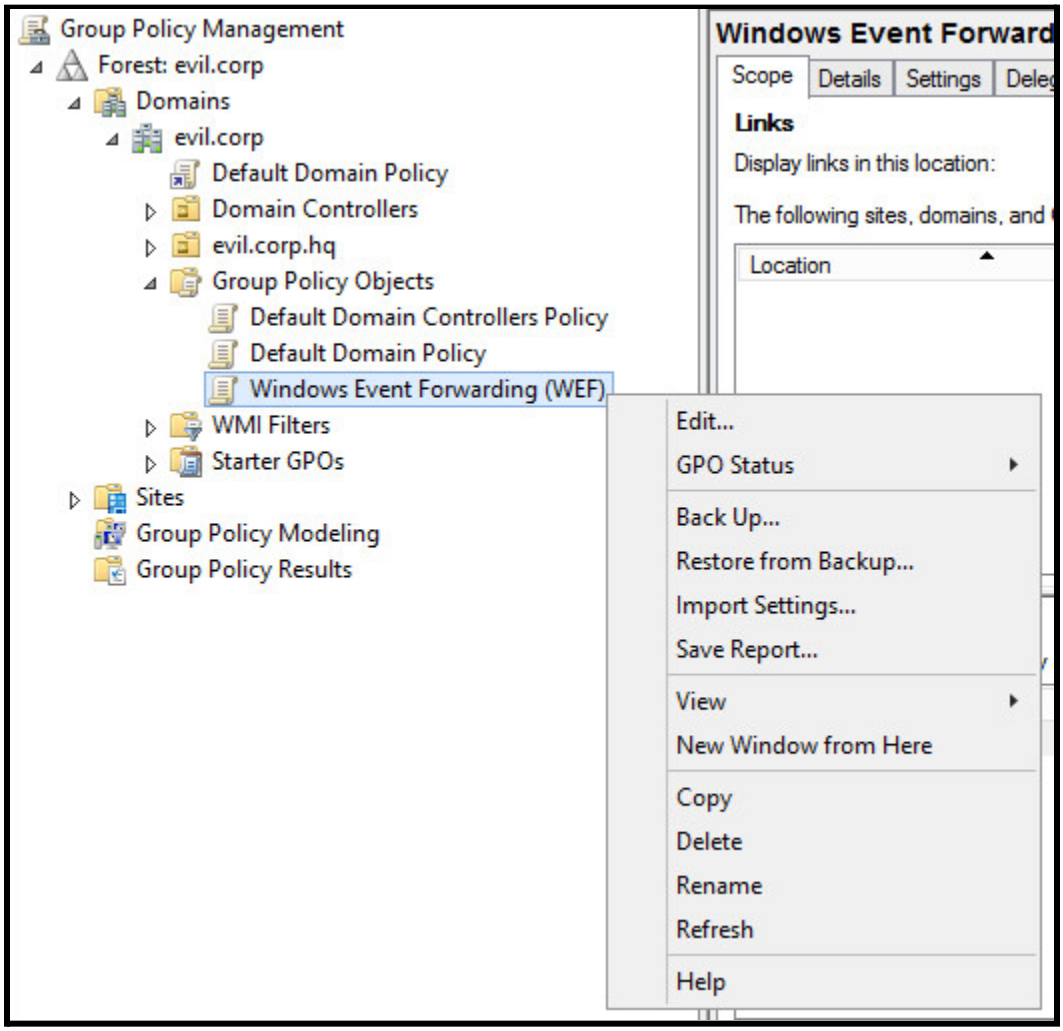
Step 5. Right-click the “Group Policy Objects” container and select “New.”



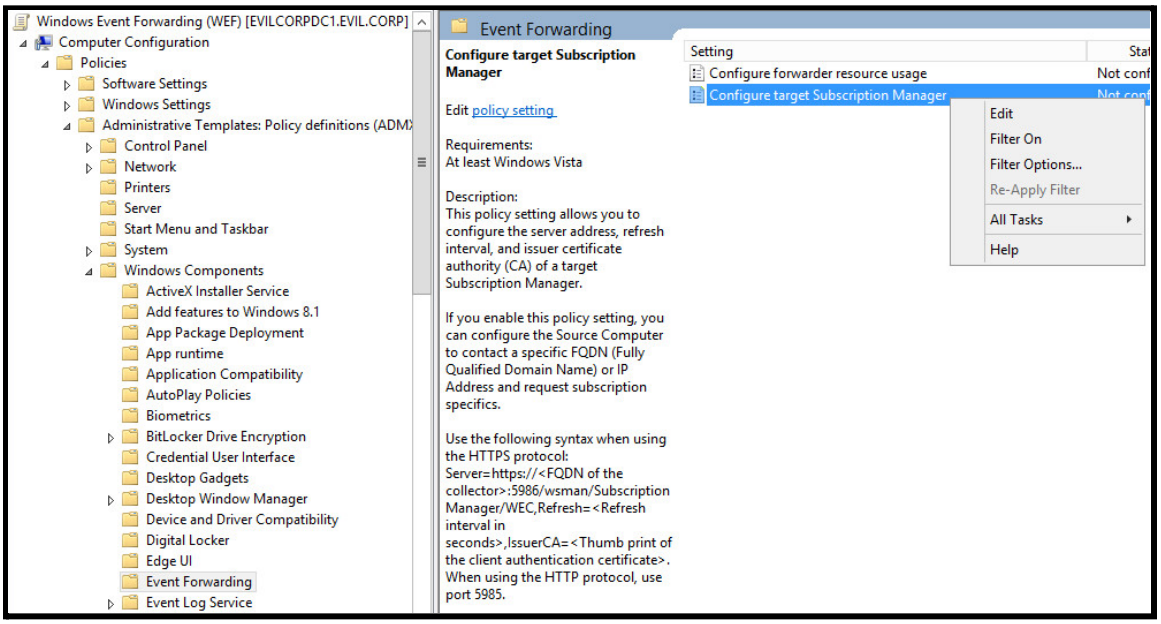
Step 6. Type “Windows Event Forwarding (WEF)” in the “Name” field.



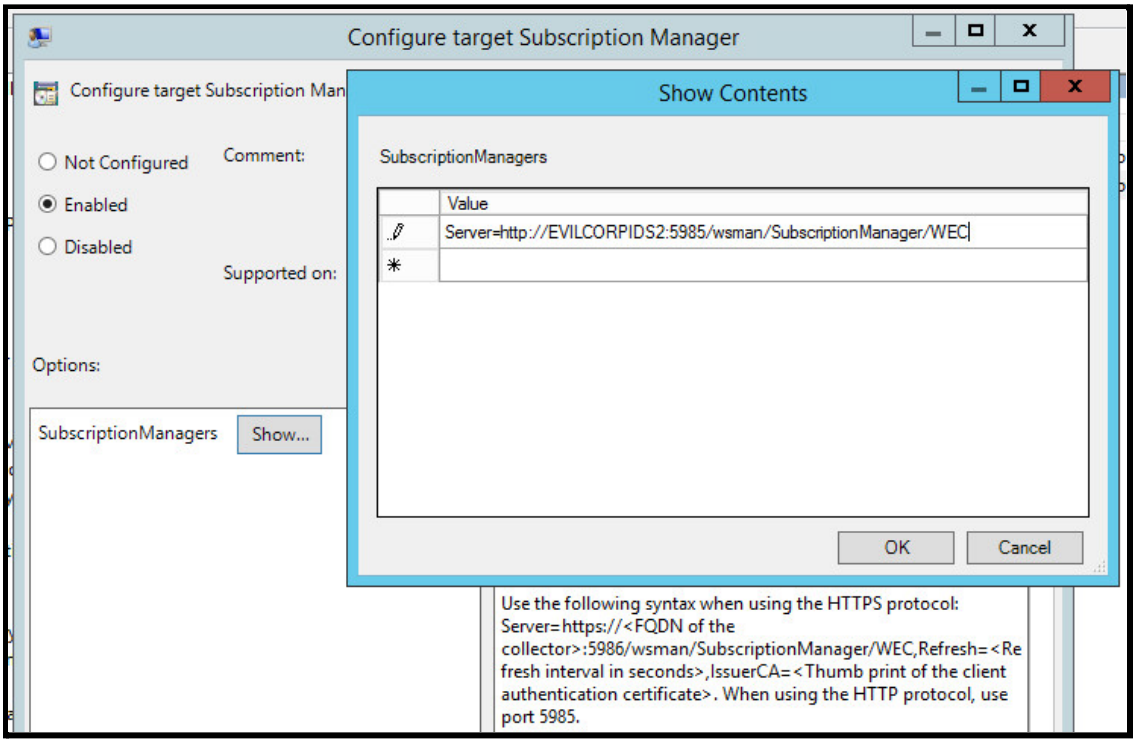
Step 7. Right-click the GPO you created and select “Edit.”



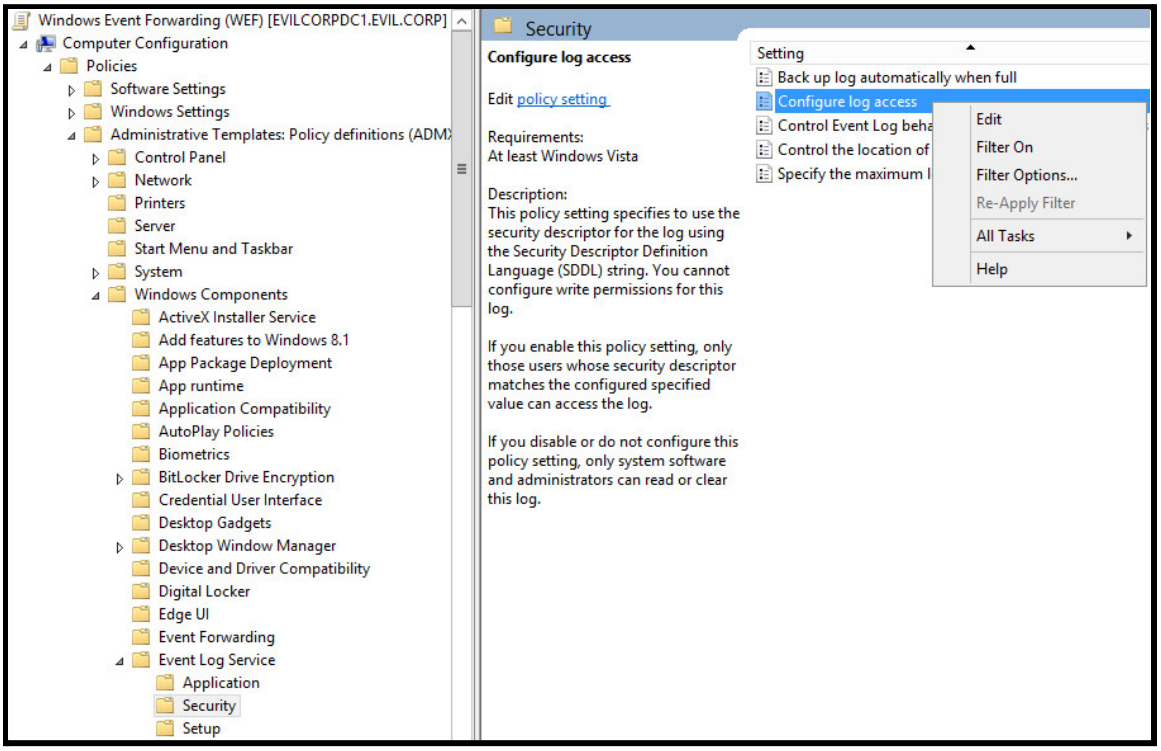
Step 8. With the GPO open, navigate to the following path: “Computer Configuration” > “Policies” > “Administrative Templates” > “Windows Components” > “Event Forwarding.” Right-click “Configure target Subscription Manager” and select “Edit.”



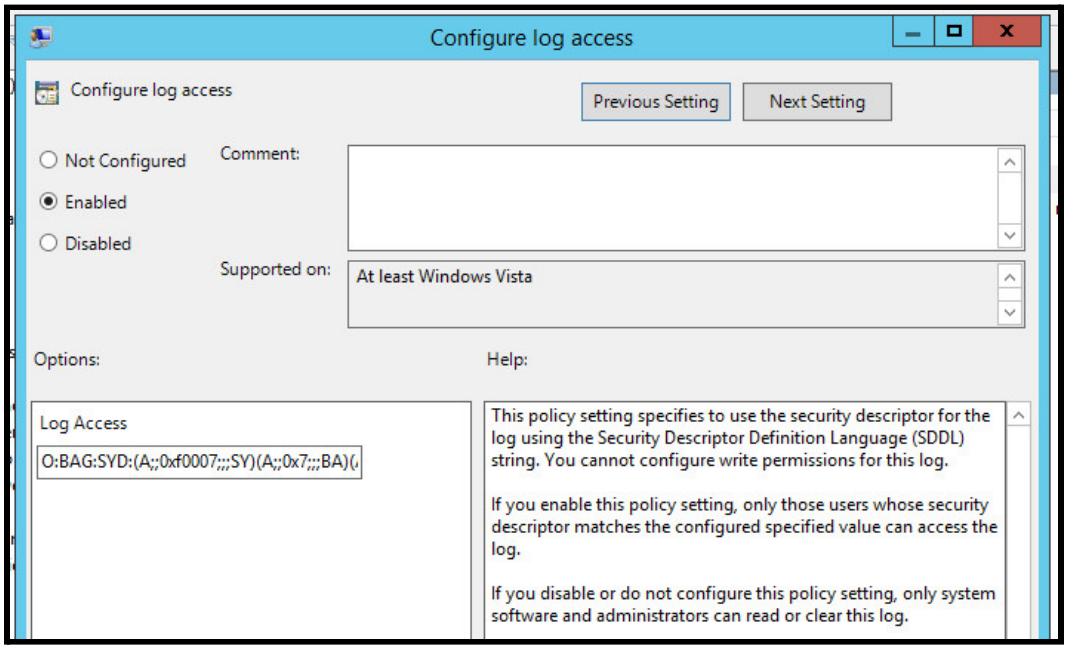
Step 9. Select “Enabled.” Click “Show…” and fill-in the SubscriptionManagers Value field using the correct syntax. For example, if the hostname of your WEC server is “EVILCORPIDS2,” you would type “http://EVILCORPIDS2:5985/wsman/SubscriptionManager/WEC.” Once complete, click “OK” to close the “Show Contents” window. Click “Apply” and “OK” to close the “Configure target Subscription Manager” window.



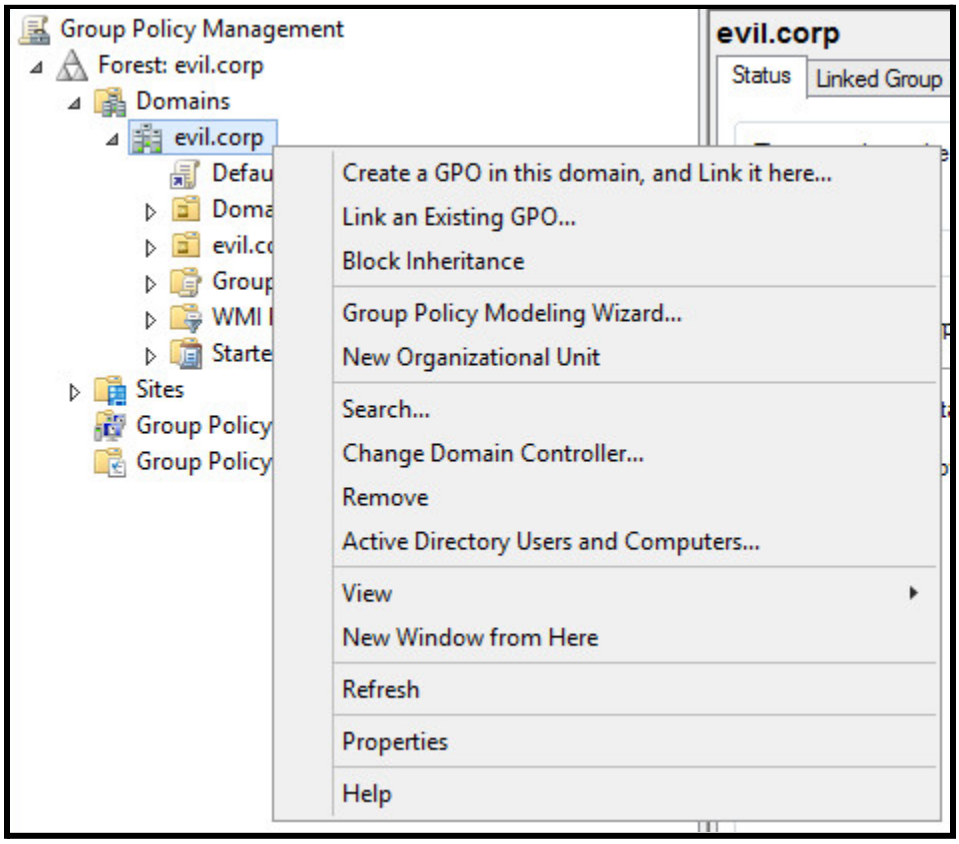
Step 10. With the GPO still open, navigate to the following path: “Computer Configuration” > “Policies” > “Administrative Templates” > “Windows Components” > “Event Log Service” > “Security.” Right-click “Configure log access” and select “Edit.”



Step 11. Select “Enabled” and type the following string in the “Log Access” field: O:BAG:SYD:(A;;0xf0007;;;SY)(A;;0x7;;;BA)(A;;0x1;;;BO)(A;;0x1;;;SO)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;S-1-5-20). Click “Apply,” click “OK,” and close the GPO.



Step 12. Right-click on your domain and select “Link an Existing GPO…”



Step 13. Select the GPO you created and click-on “OK.”