

How to Configure a Windows Event Collector (WEC) Server

Task. Configure a WEC server.

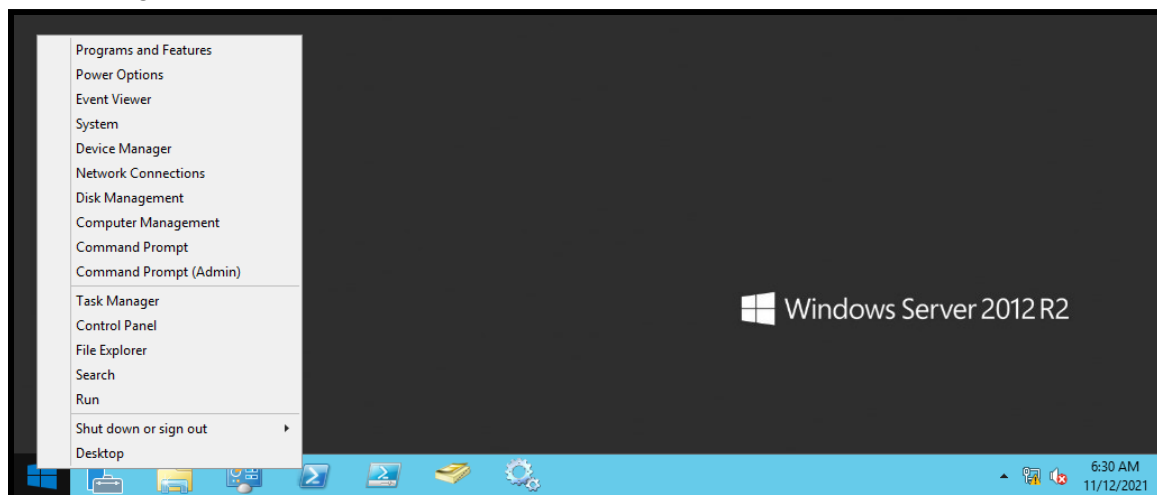
Purpose. System administrators have the option of reviewing Windows events (a.k.a. “logs”) one computer at a time or centralizing them using Windows Event Forwarding and a WEC server. A WEC server is a computer designated to store Windows events forwarded from other computers on the network. The specific events collected depend on the subscription configured.

Conditions. You have access and administrator privileges to a WEC server.

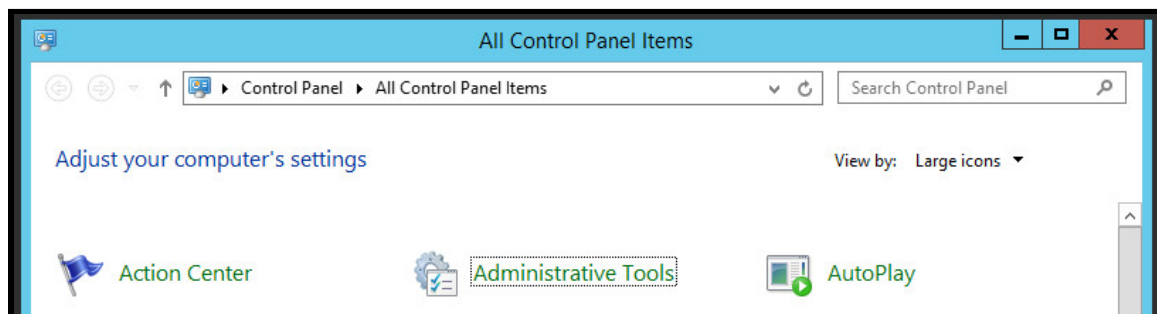
Standard. You were able to configure a WEC server.

Step 1. Login to the WEC server using your administrator account.

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

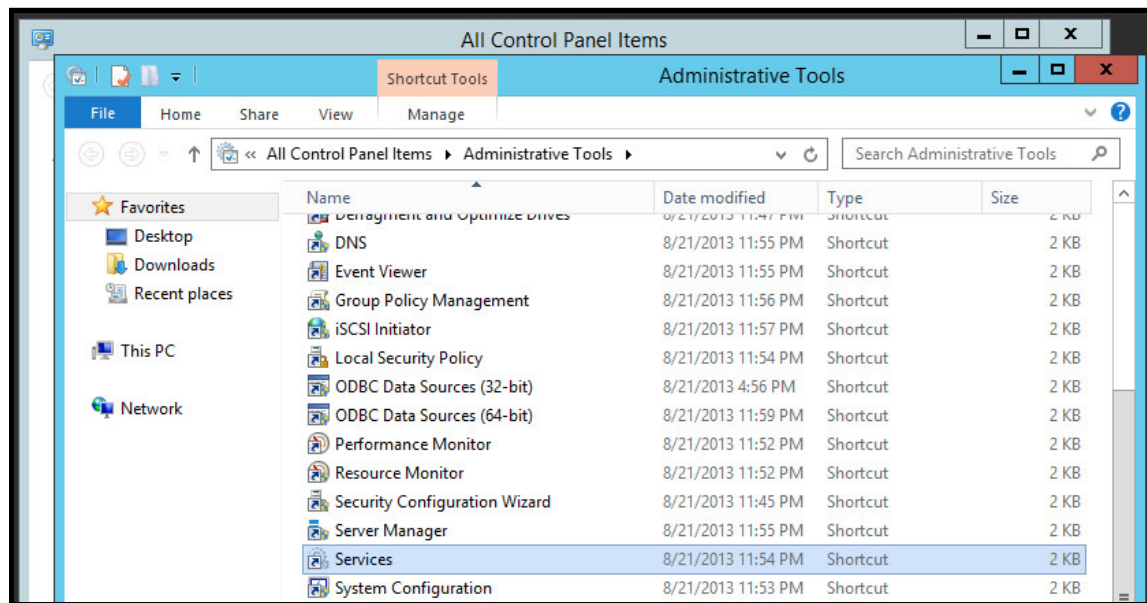


Step 3. Click-on “Administrative Tools.”

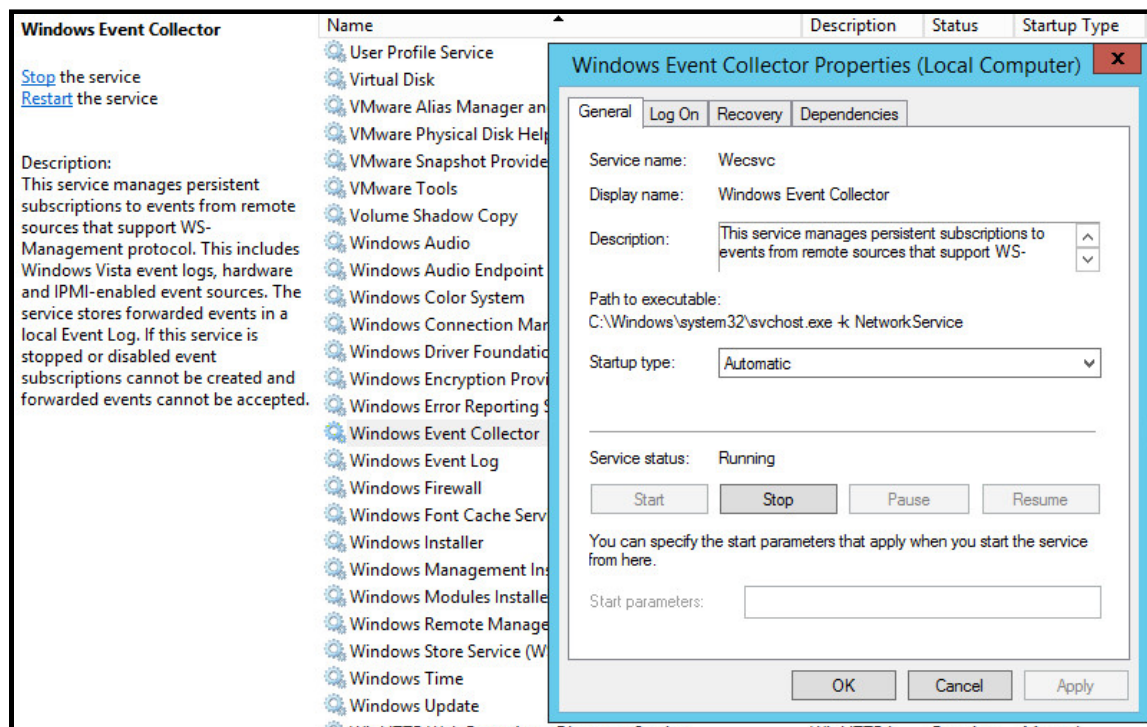


How to Configure a Windows Event Collector (WEC) Server

Step 4. Double-click “Services.”

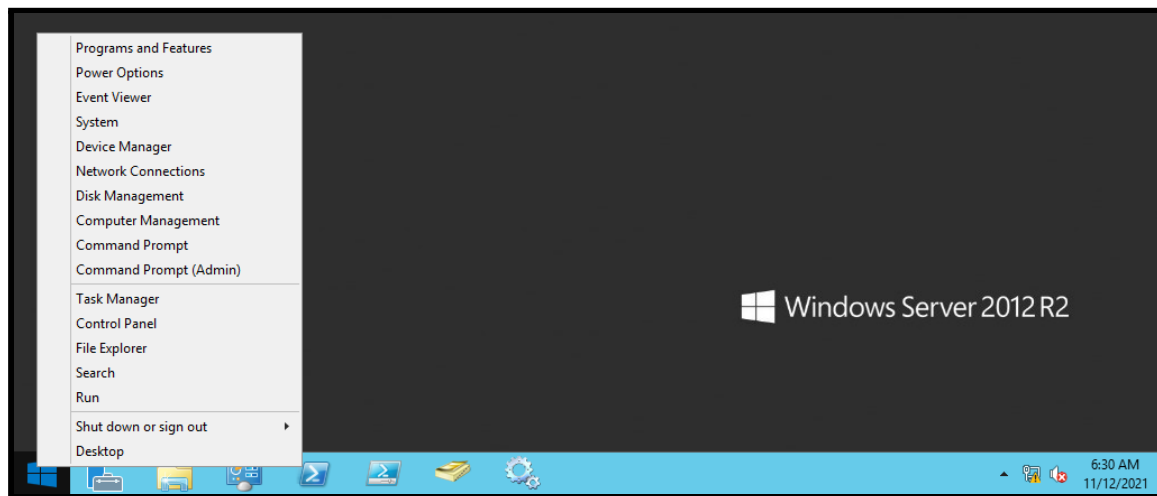


Step 5. Right-click the “Windows Event Collector” service, select “Properties,” set the “Startup type” to “Automatic,” click “Start,” and click “Apply.” Click “OK” and close all open windows.

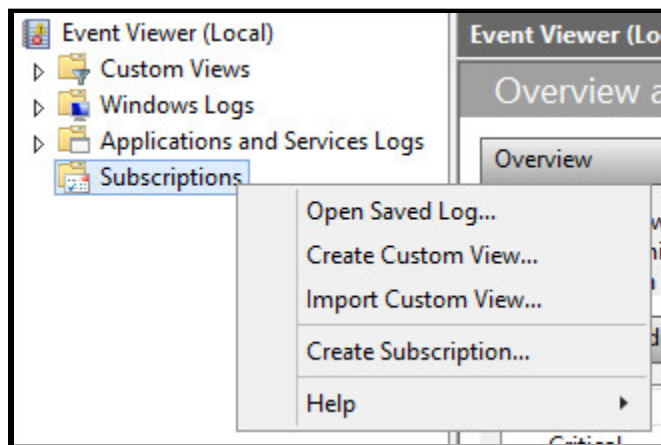


How to Configure a Windows Event Collector (WEC) Server

Step 6. Right-click on the Windows icon in the bottom-left corner and select “Event Viewer.”

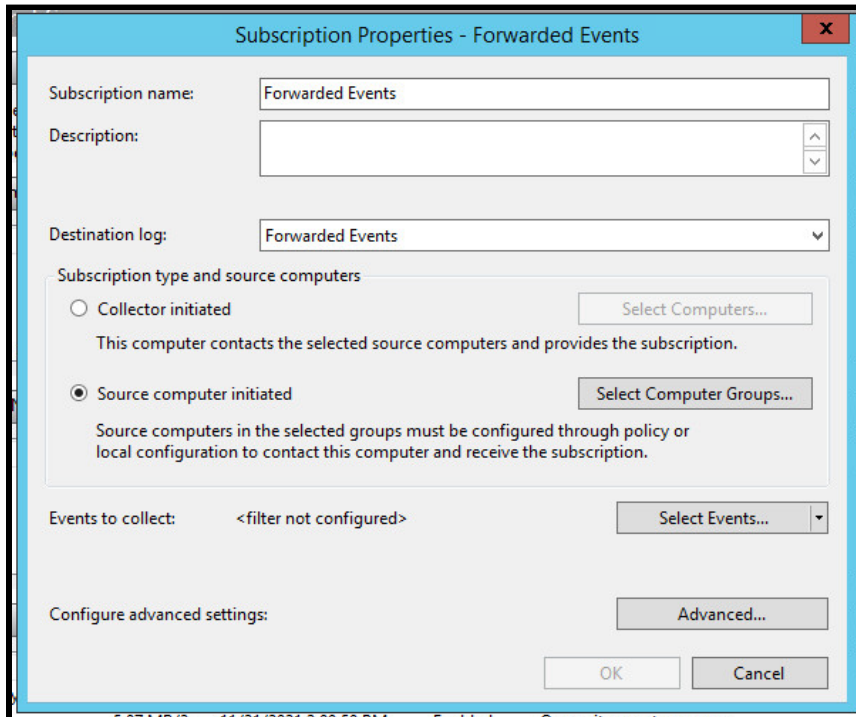


Step 7. Right-click “Subscriptions” and select “Create Subscription...”



How to Configure a Windows Event Collector (WEC) Server

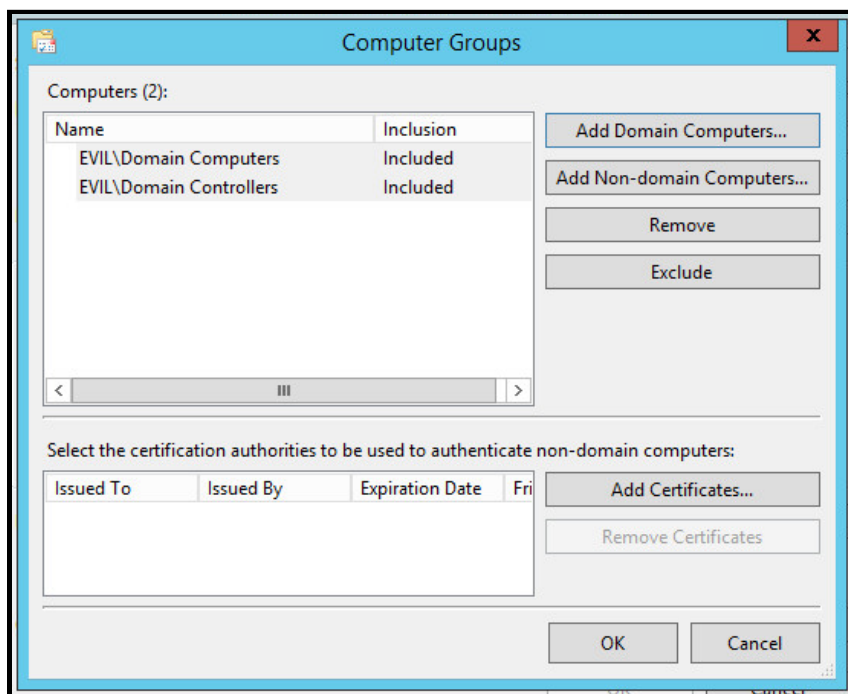
Step 8. Type “Forwarded Events” in the “Subscription name” field. For the “Destination log,” select “Forwarded Events.” For the “Subscription type,” select “Source computer initiated.”



The "Subscription Properties - Forwarded Events" dialog box is shown. It contains the following fields and options:

- Subscription name:** Forwarded Events
- Description:** (empty text box)
- Destination log:** Forwarded Events (dropdown menu)
- Subscription type and source computers:**
 - ☐ Collector initiated (disabled button: Select Computers...)
 - ☒ Source computer initiated (button: Select Computer Groups...)
- Events to collect:** <filter not configured> (button: Select Events...)
- Configure advanced settings:** (button: Advanced...)
- Buttons:** OK, Cancel

Step 9. Click “Select Computer Groups...” Click “Add Domain Computers...” Type “Domain Computers” in the provided text-box and click “OK.” Click “Add Domain Computers...” again. Type “Domain Controllers” in the provided text-box and click “Check Names.” Click “OK” to close the “Computer Groups” window.



The "Computer Groups" dialog box is shown. It contains the following elements:

- Computers (2):**

Name	Inclusion
EVIL\Domain Computers	Included
EVIL\Domain Controllers	Included
- Buttons:** Add Domain Computers..., Add Non-domain Computers..., Remove, Exclude
- Select the certification authorities to be used to authenticate non-domain computers:**

Issued To	Issued By	Expiration Date	Fri
-----------	-----------	-----------------	-----
- Buttons:** Add Certificates..., Remove Certificates
- Buttons:** OK, Cancel

How to Configure a Windows Event Collector (WEC) Server

Step 10. Click “Select Events...” For the “Event level,” select all available options. Click “By log.” Using the “Event logs” drop-down menu, select “Application,” “Security,” and “System” under “Windows Logs” and “Microsoft-Windows-Powershell/Operational” under “Applications and Services Logs.” Ensure to select the correct PowerShell log (this will require navigating to the following path: “Applications and Services Logs” > “Microsoft” > “Windows” > “PowerShell” > “Operational.” Finally, select “AppLocker” under “Applications and Services Logs” > “Microsoft” > “Windows.” In the “Includes/Excludes” Event IDs field, type the following Event IDs: 4103, 4104, 4720, 4722, 4723, 4724, 4728, 4732, 4756, 4688, 4624, 4625, 4672, 5140, 5145, 4663, 5156, 5157, 4698, 6416, 4719, 4697, 8004, 8007. FYI, these Event IDs should match those generated by your audit policy. Click “OK” to close the “Query Filter” window. Click “OK” to close the “Subscription Properties” window.

Query Filter

Filter XML

Logged: Any time

Event level: ☒ Critical ☒ Warning ☒ Verbose ☒ Error ☒ Information

☒ By log Event logs: Application, Security, System, Microsoft-Windows-PowerShell/Operational

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4720, 4722, 4723, 4724, 4728, 4732, 4756, 4688, 4624, 4625, 4672, 5140, 5145, 4663, 5156, 5157, 4698, 6416, 4719, 4697, 8004, 8007

Task category:

Keywords:

User: <All Users>

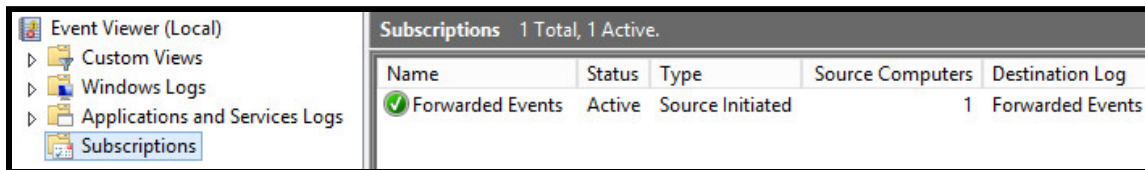
Computer(s): <All Computers>

Clear

OK Cancel

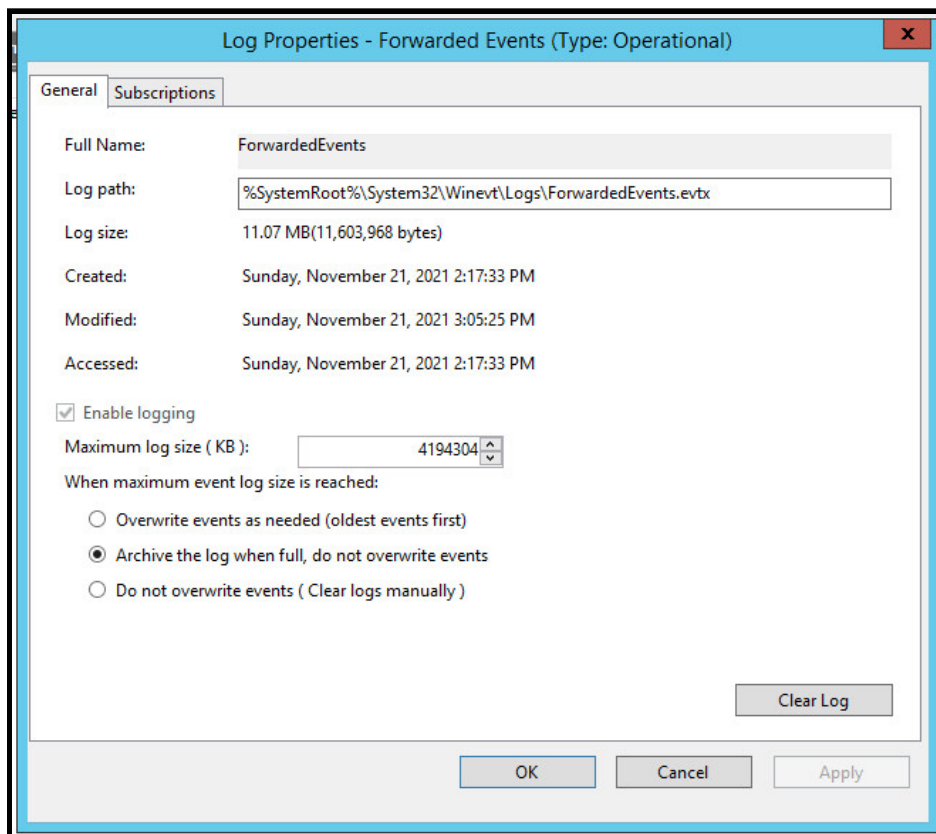
How to Configure a Windows Event Collector (WEC) Server

Step 11. Click “Subscriptions.” Wait a few minutes and click “Refresh” under the “Subscriptions” section on the right-hand side. You should begin to see the “Source Computers” counter change from 0 to however many computers you have configured to forward events to your WEC server. To expedite this process, perform a Group Policy update on the computers within your domain.



If the “Source Computers” counter does not change, begin troubleshooting by looking at the “Eventlog-ForwardingPlugin” log on a computer that should be forwarding Windows events. To access this log, open “Event Viewer” and navigate to “Applications and Services Logs” > “Microsoft” > “Windows” > “Eventlog-ForwardingPlugin.”

Step 12. With “Event Viewer” still open, right-click “Forwarded Events” under “Windows Logs.” Select “Properties.” Set the “Maximum log size” to 4,194,304 KBs (roughly 4 GBs). Click “Archive the log when full, do not overwrite old events” in the “When maximum event log size is reached” section. Click “Apply” and “OK” to close the “Log Properties” window.



Routinely check the WEC server’s disk space to prevent losing the ability to collect Windows events (all archives of the “Forwarded Events” log can be found under the “Log path” shown in the screenshot above).