Windows Event Viewer Hitchhiker's Guide to the Galaxy

Resources/Sources

Windows Event Types

- Error - A significant problem, such as loss of data or loss of functionality.
- Warning - An event that might not be significant, but might indicate a future problem.
- Information - An event that describes the successful operation of an application, driver, or service.
- Success Audit - An audited security access attempt that succeeds.
- Failure Audit - An audited security access attempt that fails.

Windows Logging Categories

- Application - Records events logged by program.
  - Developers decide what events get logged
- Security - Records security related events.
  - Invalid or valid logon by user.
- System - Records events logged by system components.
  - Failure of a driver to load at startup

Windows Event IDs

Resources/sources

- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx
- https://conf.splunk.com/session/2015/conf2015_MGough_MalwareArchaelogy_SecurityCompliance_FindingAdvnacedAttacksAnd.pdf

Important event IDs explained

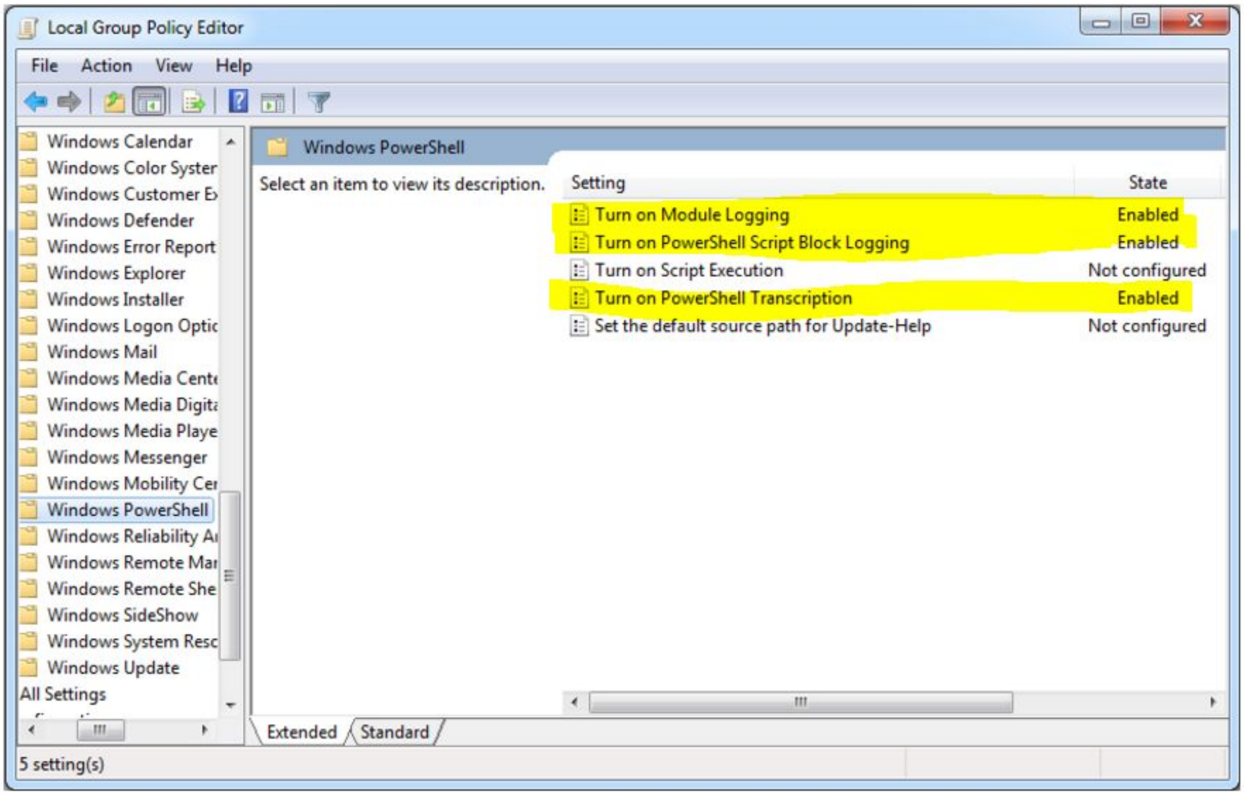
- 4688 - New process was created
- 4689 - Process has exited
- 4648 - Local user Login
    - 4626/4672 - Success network logon as admin
    - 4672 - Special/Admin Logon
    - 4634 - Logoff
- 4688 - Process Task Privilege Escalation
- 5140 - Shows share being mounted
- 106/200/201/141 - Scheduled tasks
    - 106 - Task scheduled
    - 200 - Task executed
    - 201 - Task complete
    - 141 - Task removed
        - Even if task is DELETED thank you logs, good luck bad guys
- 4657 - Registry key modified
- 5156 - Get the IP of a connection initiating to machine
- 7045 - New Windows Service created

Windows Event Viewer Logging

Enable Powershell Logging

(Windows 7 is used for this example)

1. Run > gpedit.msc
2. Administrative Templates → Windows Components → Windows PowerShell
3. Double-click “Turn on Module Logging”
    a. Click Enable
    b. In the Options, type * to record all modules
    c. Click Ok
4. Double-click “Turn on PowerShell Script Block Logging ”
    a. Click Enable
    b. Click Ok
5. Double-click “Turn on PowerShell Transcription”
    a. Click Enable
    b. Click the checkbox “Include invocation headers”
    c. You can set a output directory if you want
    d. Click Ok



Select an item to view its description.

Setting	State
Turn on Module Logging	Enabled
Turn on PowerShell Script Block Logging	Enabled
Turn on Script Execution	Not configured
Turn on PowerShell Transcription	Enabled
Set the default source path for Update-Help	Not configured

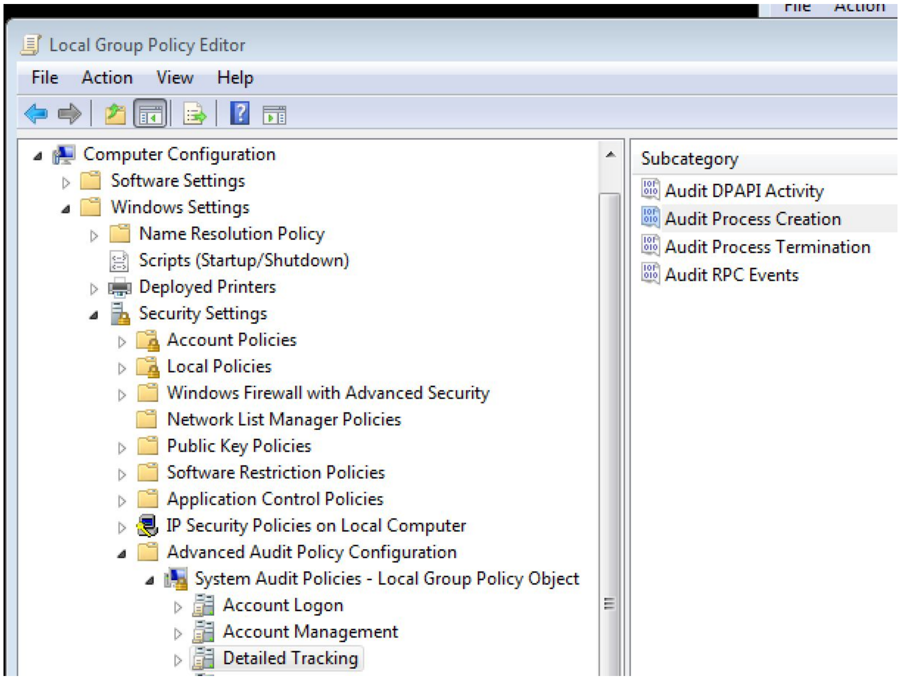
5 setting(s)

6. Resource: https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html

Enable process creation tracking

1. Run > gpedit.msc

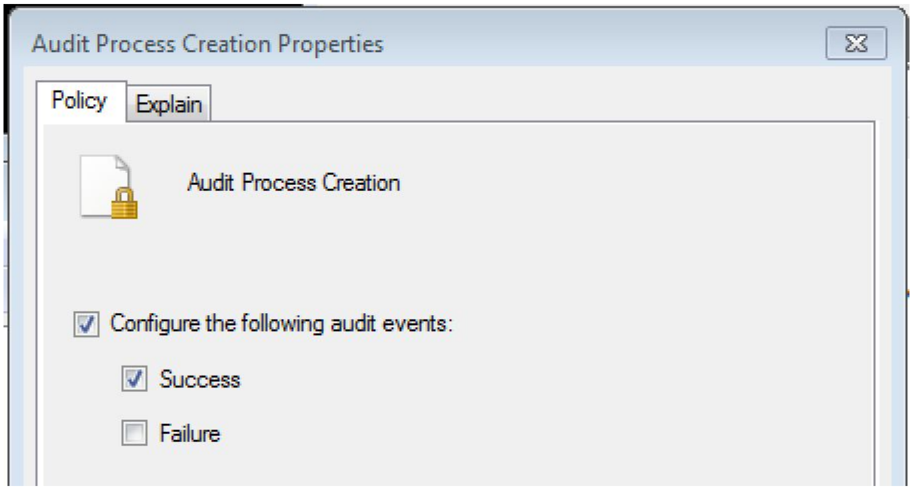
2. Local Computer Policy > Windows Settings > Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Detailed tracking



Computer Configuration
  Software Settings
  Windows Settings
    Name Resolution Policy
    Scripts (Startup/Shutdown)
    Deployed Printers
    Security Settings
      Account Policies
      Local Policies
      Windows Firewall with Advanced Security
      Network List Manager Policies
      Public Key Policies
      Software Restriction Policies
      Application Control Policies
      IP Security Policies on Local Computer
      Advanced Audit Policy Configuration
        System Audit Policies - Local Group Policy Object
          Account Logon
          Account Management
          Detailed Tracking

Subcategory
Audit DPAPI Activity
Audit Process Creation
Audit Process Termination
Audit RPC Events

3. Double-click "Audit process creation"
    a. Check "Configure the following audit events"
    b. Select "Enable"



Audit Process Creation

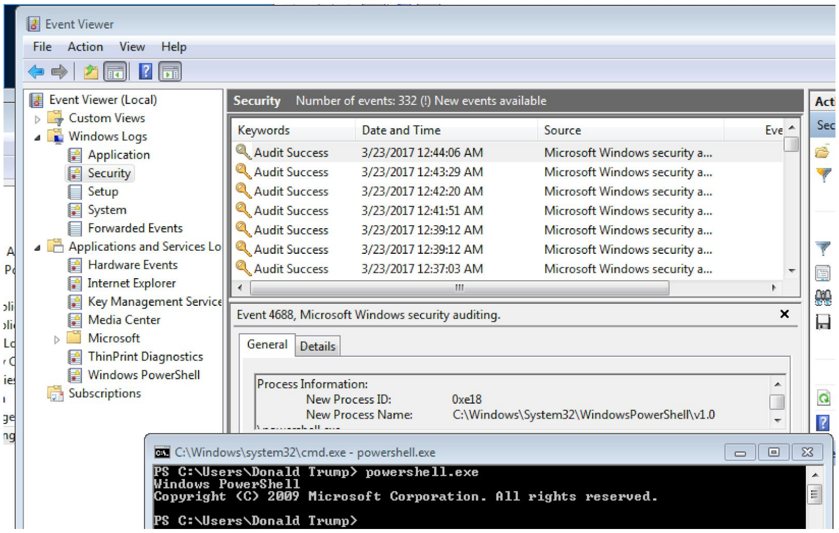
☑ Configure the following audit events:

☑ Success

☐ Failure

    c. Select "apply, "ok"
4. Open command prompt and run "powershell.exe"
5. Open "Event Manager"
    a. Windows Logs > Security

b. Look for event ID 4688



Security Number of events: 332 (!) New events available

Keywords	Date and Time	Source	Eve
Audit Success	3/23/2017 12:44:06 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:43:29 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:42:20 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:41:51 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:39:12 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:39:12 AM	Microsoft Windows security a...	
Audit Success	3/23/2017 12:37:03 AM	Microsoft Windows security a...	

Event 4688, Microsoft Windows security auditing.

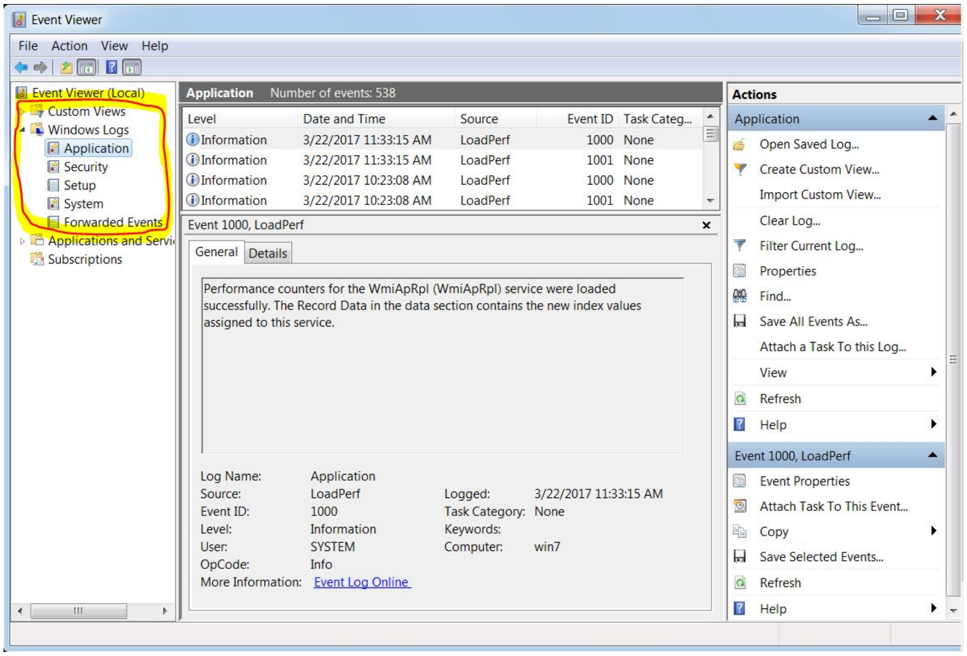
```
Process Information:
        New Process ID:        0xe18
        New Process Name:      C:\Windows\System32\WindowsPowerShell\v1.0
```

```
PS C:\Users\Donald Trump> powershell.exe
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Donald Trump>
```

Windows Event Manager Filter/Search

1. Run > eventvwr.msc
2. Choose a log to filter



Application Number of events: 538

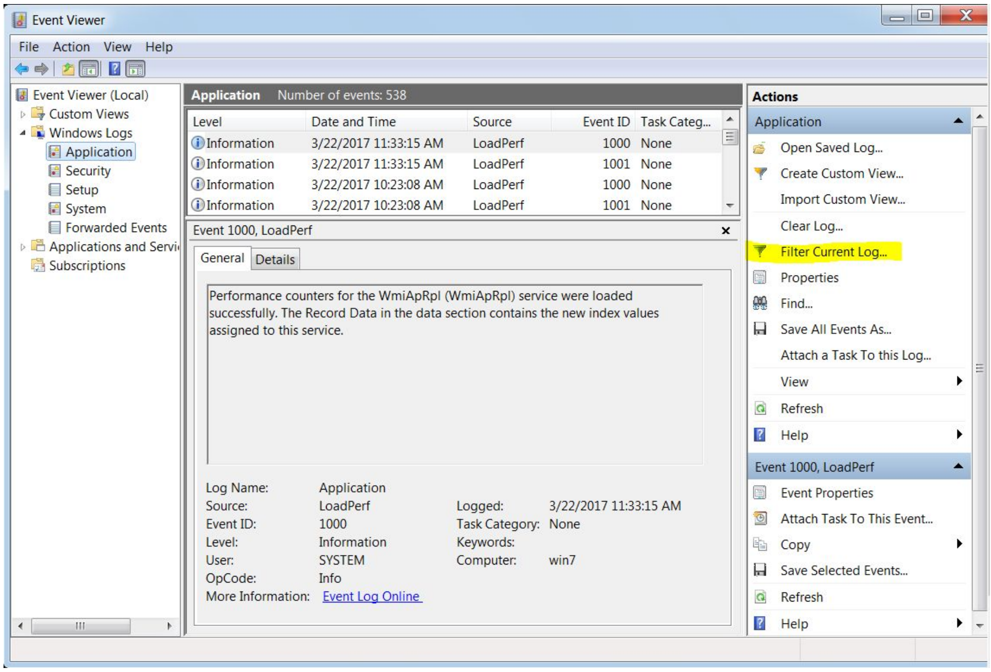
Level	Date and Time	Source	Event ID	Task Categ...
Information	3/22/2017 11:33:15 AM	LoadPerf	1000	None
Information	3/22/2017 11:33:15 AM	LoadPerf	1001	None
Information	3/22/2017 10:23:08 AM	LoadPerf	1000	None
Information	3/22/2017 10:23:08 AM	LoadPerf	1001	None

Event 1000, LoadPerf

Performance counters for the WmiApRpl (WmiApRpl) service were loaded successfully. The Record Data in the data section contains the new index values assigned to this service.

Log Name:	Application		
Source:	LoadPerf	Logged:	3/22/2017 11:33:15 AM
Event ID:	1000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	win7
OpCode:	Info		
More Information:	Event Log Online		

3. After choosing which log to filter, click Filter Current Log...

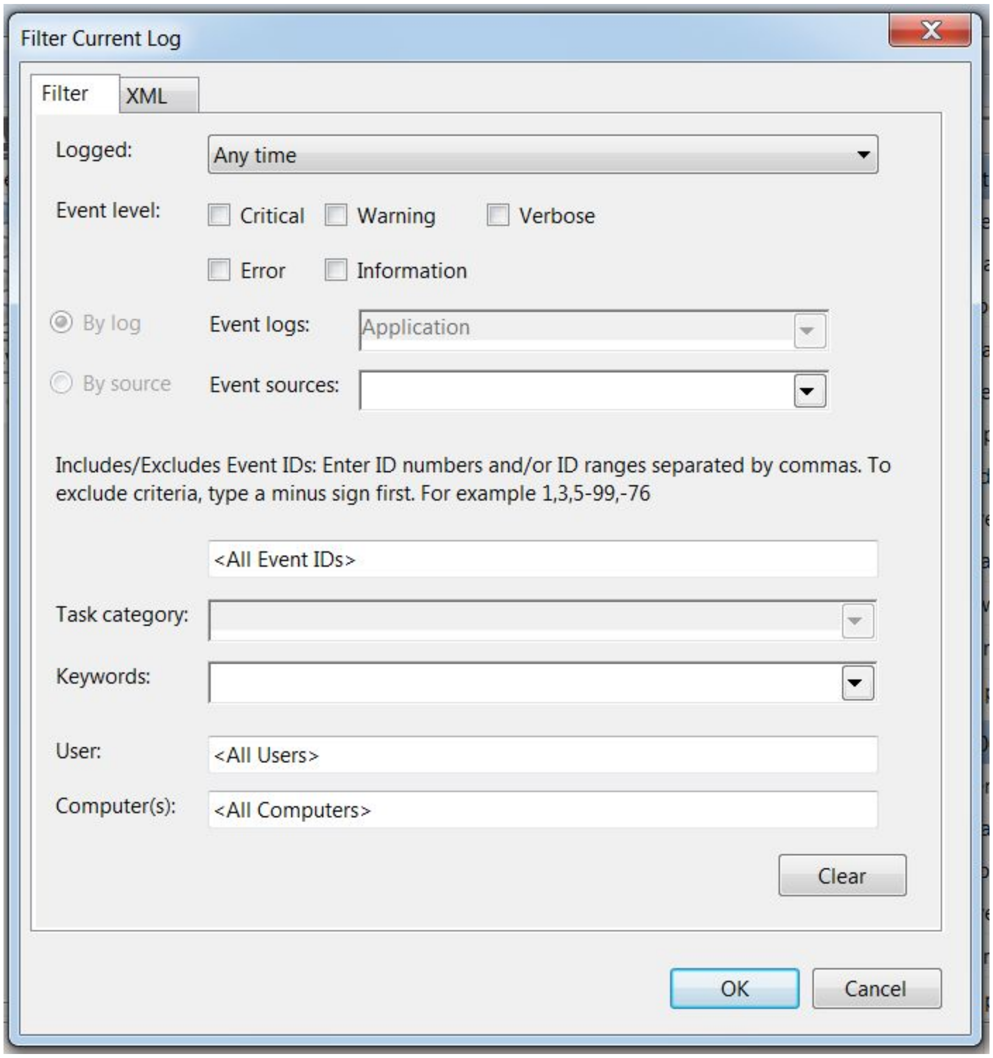


Level	Date and Time	Source	Event ID	Task Categ...
Information	3/22/2017 11:33:15 AM	LoadPerf	1000	None
Information	3/22/2017 11:33:15 AM	LoadPerf	1001	None
Information	3/22/2017 10:23:08 AM	LoadPerf	1000	None
Information	3/22/2017 10:23:08 AM	LoadPerf	1001	None

Event 1000, LoadPerf

Performance counters for the WmiApRpl (WmiApRpl) service were loaded successfully. The Record Data in the data section contains the new index values assigned to this service.

Log Name:	Application		
Source:	LoadPerf	Logged:	3/22/2017 11:33:15 AM
Event ID:	1000	Task Category:	None
Level:	Information	Keywords:	
User:	SYSTEM	Computer:	win7
OpCode:	Info		
More Information:	Event Log Online		



Filter Current Log

Logged: Any time

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

● By log Event logs: Application

○ 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

<All Event IDs>

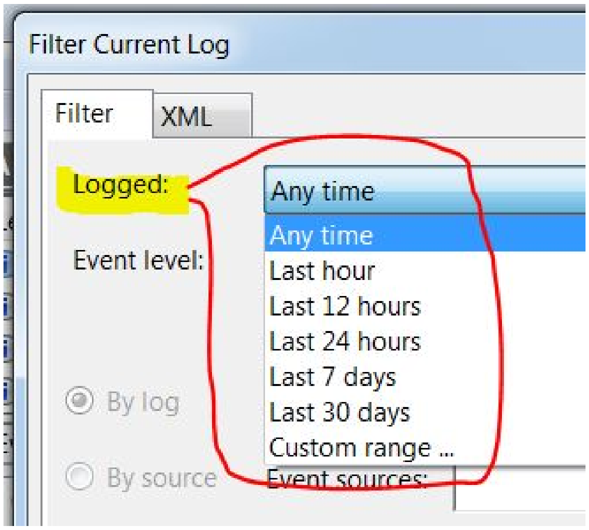
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

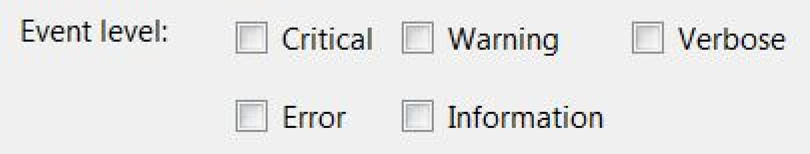
4. Here you can customize your filter
   a. Pick an option from Logged: to view a time span or create your own



Filter Current Log

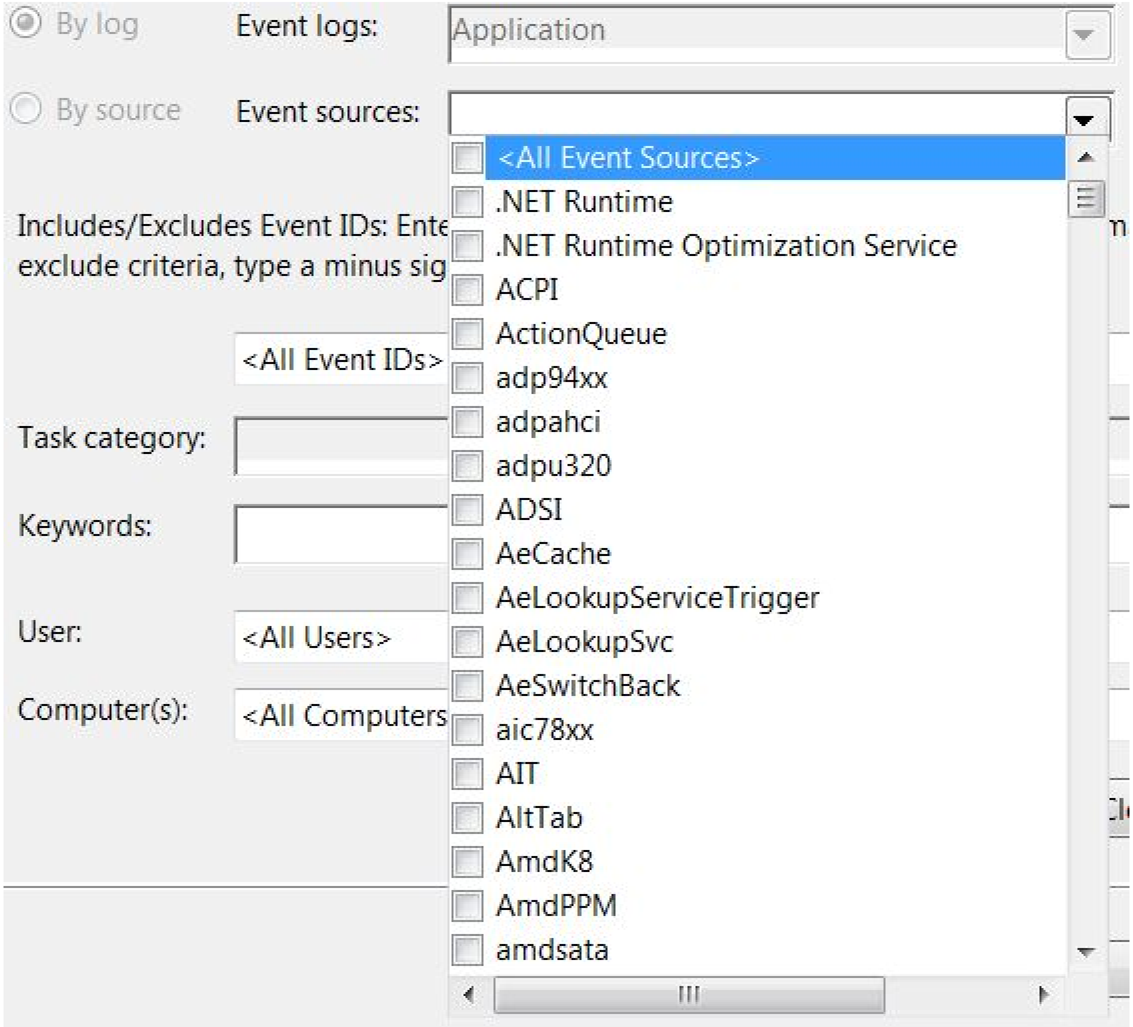
Logged: Any time

   b. Choose the event level



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

c. Choose event source(s) from the drop down menu



● By log Event logs: Application

○ By source Event sources:

Includes/Excludes Event IDs: Ente
exclude criteria, type a minus sig

<All Event IDs>

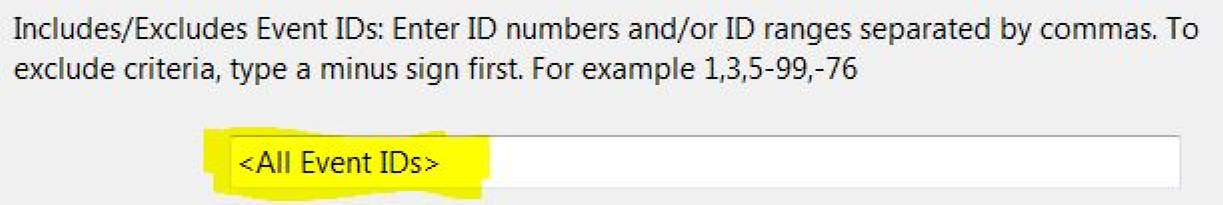
Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers

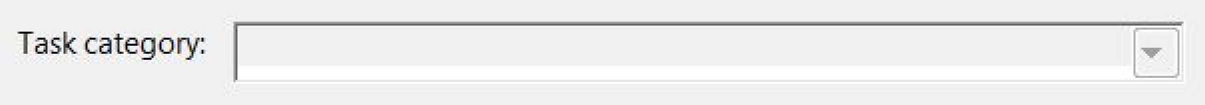
d. Enter Event IDs or leave the default of all Event IDs



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

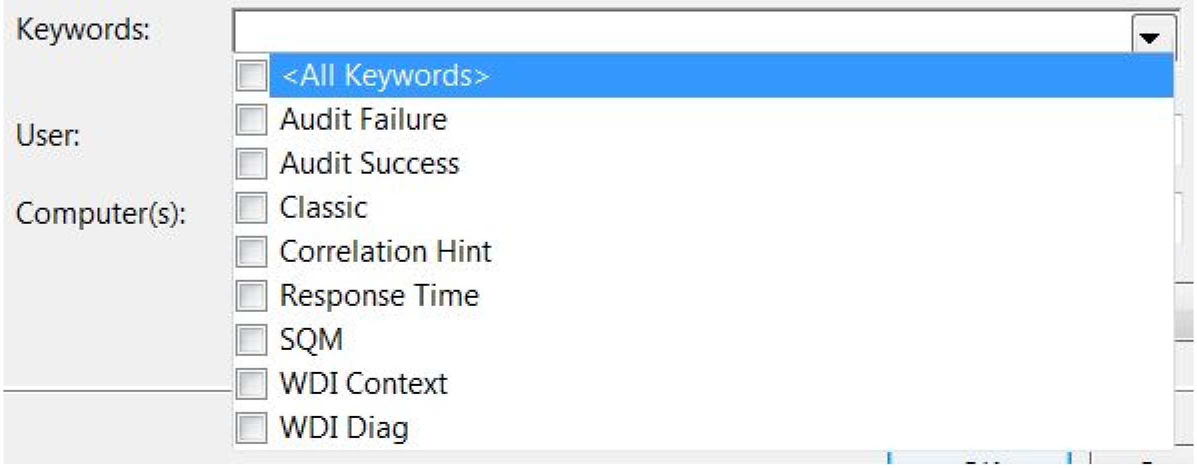
<All Event IDs>

e. For Task category



Task category:

f. For keywords, select from the dropdown menu for click “All Keywords>



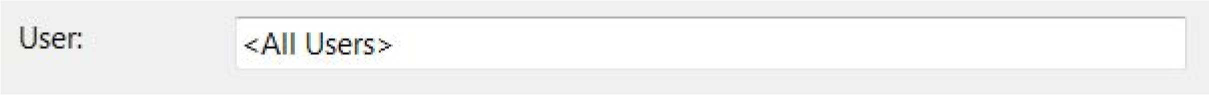
Keywords:

User:

Computer(s):

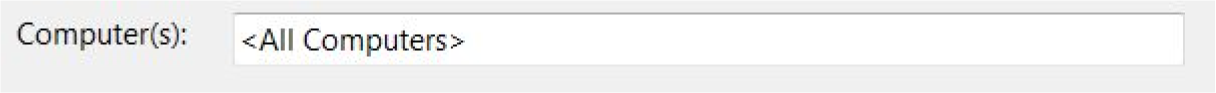
- ☐ <All Keywords>
- ☐ Audit Failure
- ☐ Audit Success
- ☐ Classic
- ☐ Correlation Hint
- ☐ Response Time
- ☐ SQM
- ☐ WDI Context
- ☐ WDI Diag

g. For Users, enter the user(s) you want to see



User: <All Users>

h. For Computer(s), enter the source computer(s)



Computer(s): <All Computers>

5. Click OK to apply your filtering

Resource: https://technet.microsoft.com/en-us/library/cc722058(v=ws.11).aspx