Windows Event Monitoring Guidance

Table of Contents

Table of Contents

1. Introduction

This document is to serve as a guide for security professionals and system administrators to configure Windows Event logging and forwarding on an enterprise network using Group Policy. The advice throughout this paper supports both the detection and investigation of malicious activity. Provided recommendations are an ideal balance between the collection of essential events and the management of data volumes. The tools discussed are either natively available in the Microsoft Windows Operating System (OS), available for free from Microsoft, or are open source projects. The event collection features discussed throughout the remainder of this paper do not require additional licensing costs.

The audience of this document is to be information security and information technology professionals. This document will cover Windows Event types, a general assessment of their value, a centralized collection of Windows Event logs, retaining Windows Event logs, and recommended Group Policy (GP GPO) settings for deployment as well notes for implementation.

This document consists of three main sections. The first section will be on Deployment Planning, which will have a focus on the configuration and deployment of a central log collection solution. The second section, Recommended Events to Collect, discusses a baseline of recommended events for security analysis. The final section, Recommended Events Group Policy, focuses on the specific policy objects that control the Windows Event logging identified in the second section. As this document ages, the Windows Event IDs mentioned may be deprecated or otherwise modified. Companion configurations, scripts, and information will be publicly available for future reference at https://github.com/hacks4snacks/windows-event-forwarding.

2. Requirements and Considerations

The development of the recommendations throughout this document took place on Windows 10 and Windows Server 2019 using WinRM 3.0 and PowerShell 5.1. All functionality discussed is backwards compatible to Windows 7 and Windows Server 2008, respectfully. There may be some Group Policy settings used throughout this document that may not be compatible or available with the Pro or lower-tier versions of Microsoft Windows.

In order to ensure accurate correlation of events and consistent, accurate time, timestamps are a must. Recommended practices (US-Cert, 2008) suggest that all devices (e.g., Windows Workstations and networking equipment) within an organization's environment use an accurate time source (e.g., NTP server).

All changes made to systems should be thoroughly tested in order to ensure there are no unintended outcomes to an Organization's standard operating procedures. While testing changes, the focus should be on the volume of logs generated, impact on the network's performance, and the performance of the hosts. Event collection hardening is not covered in this document; however, it is highly recommended that the proper steps are taken to ensure defense in a depth strategy when planning the deployment of the discussed logging solution.

Group Policy settings outlined in this document utilize the Windows Advanced Audit Policies, which may override any existing legacy audit policies. Please ensure that the existing audit policies are migrated into the advanced audit policies (Microsoft, 2017).

Sysmon (System Monitor) is a tool published by Microsoft that provides a greater depth of visibility into the system and network activity on a Windows host, much more than standard Windows logging. It is highly recommended that organizations use this tool in their Windows environment if and where possible (Microsoft, 2019).

3. Deployment Planning

3.1. Overview

The Windows Collector service serves as the mechanism that enables the ability to collect events from a domain, and non-domain joined machines to a central location for the exploration of a single system. Additionally, it can be used in the case of the necessity to forward to a Security Incident Event Manager (SIEM) in which the Collection Server can act as a single forwarding point. The Windows Collector Service Event Forwarding feature facilitates receiving or retrieving events from remote machines. The Event Forwarder can operate in two modes, Collector-Initiated (pull) or Source-Initiated(push).

The server that is collecting and archiving the Windows Events is known as the "Collector." The remote computer, where the events originate from, is known as the "Source." When and why to use one mode over the other (Collector-initiated vs. Source-Initiated) varies from environment to environment. However, the difference between the two is that a Source-Initiated subscription pushes its events (based on a pre-defined time) to the collector. The Collector-Initiated subscription necessitates that the collector itself reach out to each endpoint (based on a pre-defined time), which requires the collector to maintain names (IP or FQDN) of each endpoint which is much more challenging to maintain than the inverse. Micros oft's implementation of the Web Services-Management (WS-Management, WS-Man) protocol enables the communication between the collector and the sources. Throughout this document, the event forwarding configurations will assume a domain environment using the Source-Initiated(push) method.

3.2. Event Log Retention

By default, Windows log sizes are relatively small and configured to overwrite the previous events as the log exceeds the predefined maximum size. While this is less of a risk since the intent will be to have these logs forwarded to a central collector, it is good practice to increase these logs sizes. The increased log size reduces the risk of log loss if the computer falls off the domain or the user is on travel. The recommended changes below will increase the Security log from the default 20MB to 2GB. The Application and System logs increased to 64MB each. The intent of the sizes below is to provide a balance of data usage, local log retention, and performance when analyzing the local event logs when and if required.

Be advised; the changes will increase the data storage requirements for each Windows host in the environment if configured using Group Policy. In environments that local storage is limited, the default limits will suffice as the logs are forwarded to a centralized server for retention and analysis.

Group Policy Setting	Recommendation
Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Event Log Service -> Application	
	Enabled Maximum Log Size (KB): 65536
Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Event Log Service -> Security	
	Enabled Maximum Log Size (KB): 2097152
Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Event Log Service -> System	
	Enabled Maximum Log Size (KB): 65536

Table 1. Event Log location and sizing

3.3. Event Log Aggregation

The collector server should be a dedicated system for the sole purpose of collecting events in an environment (some environments may require more than one system depending on volume). Dedicating a system for collecting events helps avoid troubleshooting other services on the system. Additionally, it ensures the required amount of resources are available on the system to collect the events and alleviates some of the other security concerns that come with having multiple services running on one box.

Throughout this document, a Source-Initiated subscription is going to be assumed (same domain), and the event collector is going to be configured locally. It is worth noting that the event collector capabilities can be configured via GPO as well; however, this may lead to the Windows Event Collector service not to use subscriptions as expected. It is recommended that all collection servers be configured locally.

3.4. Configuring Collector Settings

The event collector needs to have both WinRM and the Windows Event Collector services enabled and set to automatically start (delay start). By default, on Windows Server 2008 and above, the WinRM service is enabled and set to automatically start. In the next section, the "quickconfig" option will be discussed as it is used to automatically configure both the WinRM and the Windows Event Collector services. The collector configuration can be completed by a domain administrator or a built-in administrator account. It is recommended to use the domain administrator account for configuration purposes only.

3.4.1. Collection Server Specifications

The 'recommended' resource specifications vary depending on specific use cases (how many hosts, log retention requirements, etc.). A general use recommendation is four (4) vCPUs, 16GB of RAM, and 500GB HDD to support an average load of 2,000 to 4,000 clients that have one or two subscriptions configured.

The memory usage of the Windows Event Collector service depends on the number of connections that are received by the client. The number of connections depends on the following factors:

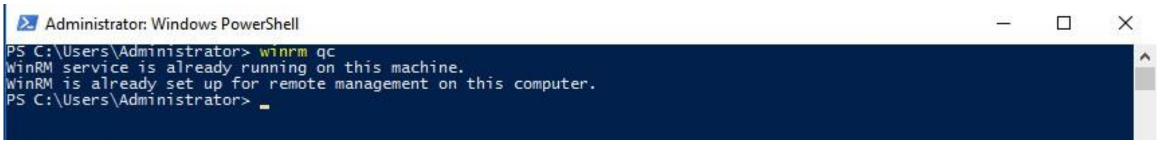
- The frequency of the connections
- The number of subscriptions
- The number of clients
- The operating system of the clients

3.4.2. Windows Remote Management Enablement

WinRM, is bundled with a command-line tool that provides the optional convenience to automatically configure WinRM (or to check if it is already configured). The tool is known as quick configure (qc). QC starts the WinRM service, sets it to Delay-Start, creates a listener using any IP address, and enables a firewall exception rule for WinRM. The default port for WinRM 2.0 and above is 5985

(HTTP) or 5986 (HTTPS). To configure WinRM on the collector, open PowerShell (can also use CMD) as an administrator or with administrator privileges and type the following command:

winrm qc



```
PS C:\Users\Administrator> winrm qc
WinRM service is already running on this machine.
WinRM is already set up for remote management on this computer.
PS C:\Users\Administrator> _
```

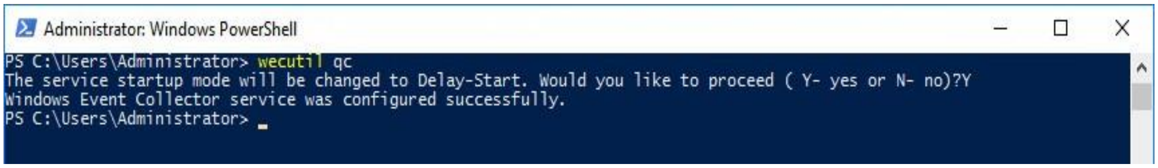
Figure 1. WinRM is already running on the machine.

3.4.3. Windows Event Collector Enablement

Similar to WinRM, the Windows Event Collector service provides a QC option. The QC for Windows Event Collector sets the service startup type to Delay-Start and enables the ForwardedEvent channel. To configure the Windows Event Collector service on the collector, open PowerShell (can also use CMD) as an administrator or with administrator privileges and type the following command:

wecutil qc

Unlike WinRM, the WEC utility does not check if the service has already been set. So, every time it is run, the prompt is the same. Enter **Y** to have the service status modified to reflect Delay-Start.



```
PS C:\Users\Administrator> wecutil qc
The service startup mode will be changed to Delay-Start. Would you like to proceed ( Y- yes or N- no)?Y
Windows Event Collector service was configured successfully.
PS C:\Users\Administrator> _
```

Figure 2. Running wecutil qc to enable Windows Event Collector Services.

3.4.4. Collection Server Log Retention

It is recommended that the Forwarded Events log file on the server designated as the centralized log collector is set to a size of approximately 25GB and enable the Archive the log when full. Do not overwrite events policy to control the behavior when the event log has reach capacity. The theoretical maximum log file size for the forwarded events log on Windows Server 2008 R2 and later is two (2) terabytes. However, as the log file becomes more substantial in size, the Event Viewer UI takes longer to load and show results for custom views. Due to Event Viewer UI performance degradation when using a larger log file size, it is essential to review the log regularly (once a day) and set up archiving or feed the log data into a more extensive Security Information Event Management (SIEM) system.

To increase the default Windows log size on the collector, follow the steps below.

1. Open the Event Viewer.
2. Select Windows Logs in the left column.
3. Right-click on Forwarded Events in the center column and select Properties.
4. Change the Maximum log size from 20480 (20MB) to 10485760 (10GB).
    a. The log size can be any desired amount, however the primary performance bottleneck of WEF is the log size. Rule of thumb is log size + 5GB = total host memory.
5. Click **OK**.

It may be beneficial to have the Forwarded Events log file reside on a larger and separate disk. To modify the Event Viewer log files to another location, follow the steps outlined below.

1. Click **Start**, and then click **Run**.
2. In the Open box, type **regedit**, and then click **OK**.
3. Locate and click the following registry key:
    a. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog
4. Click the **subkey** that represents the event log to be moved.
5. In the right pane, double-click **File**.
6. Type the **complete path** to the new location (to include the log file name) in the **Value data** box, and then click **OK**.
7. When finished, **restart the computer**.

Alternatively, the path location can also be modified in the Event Viewer with the steps prescribed below.

1. Open **Event Viewer**.
2. Select the desired windows log and **right-click** the name.
3. Change the Log Path to specify the **absolute path** for the new log file

   a. Network-mapped drives must be specified by their names (e.g., **\\NetDrive\newdir\Fwd.evtx**)

4. Select **OK**.
5. When finished, **restart the computer**.

This modification may affect existing views and subscriptions until the machine is restarted.

3.4.5. Windows Event Subscriptions

Event subscriptions are used to organize event collection and identify the source of the collected events. Custom subscriptions can be crafted to tailor the event logs to assist in quickly identifying events of value. Subscriptions can be created through the command line or by using the Graphical User Interface (GUI) within the Event Viewer. One caveat to creating subscriptions through the GUI is that the interface does not allow complete customization. An example of complete customization of a subscription is the configuration of frequency and batch number of events to receive per delivery. The following section will demonstrate the creation of an example event subscription using the GUI.

To create a subscription:

1. Open the **Event Viewer**.
2. Select **Create Subscription**.
3. Provide a meaningful Subscription name.
4. Select **Source computer-initiated** option.
5. Select **Computer Groups** button.
   - Click **Add Domain Computers**, enter the desired group name.

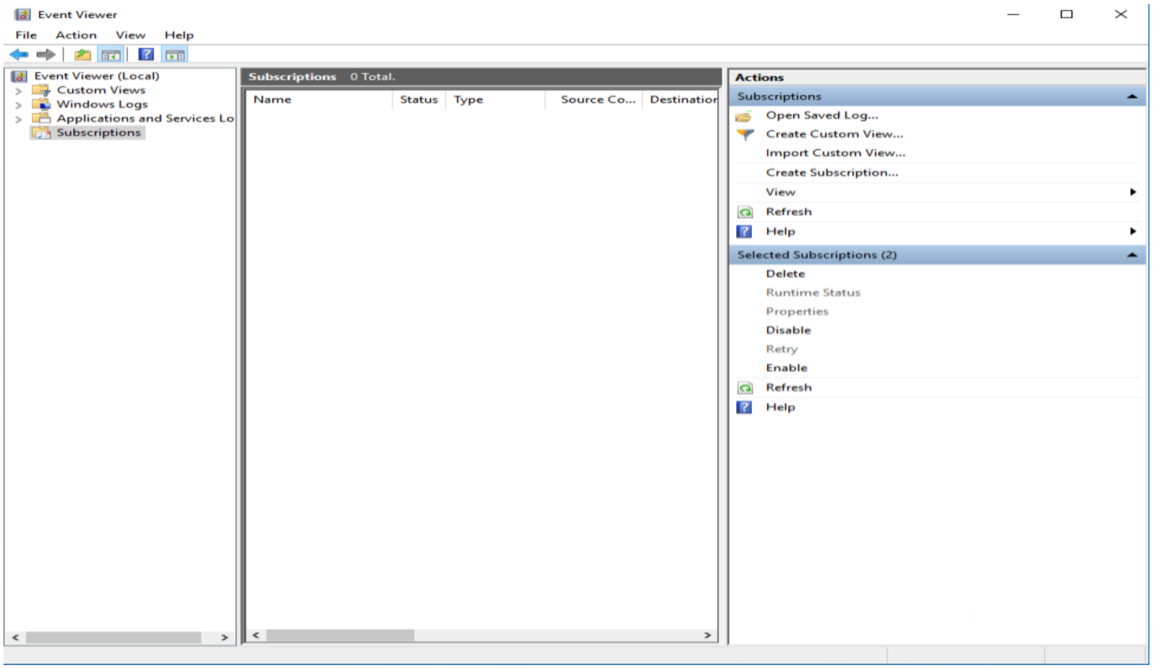
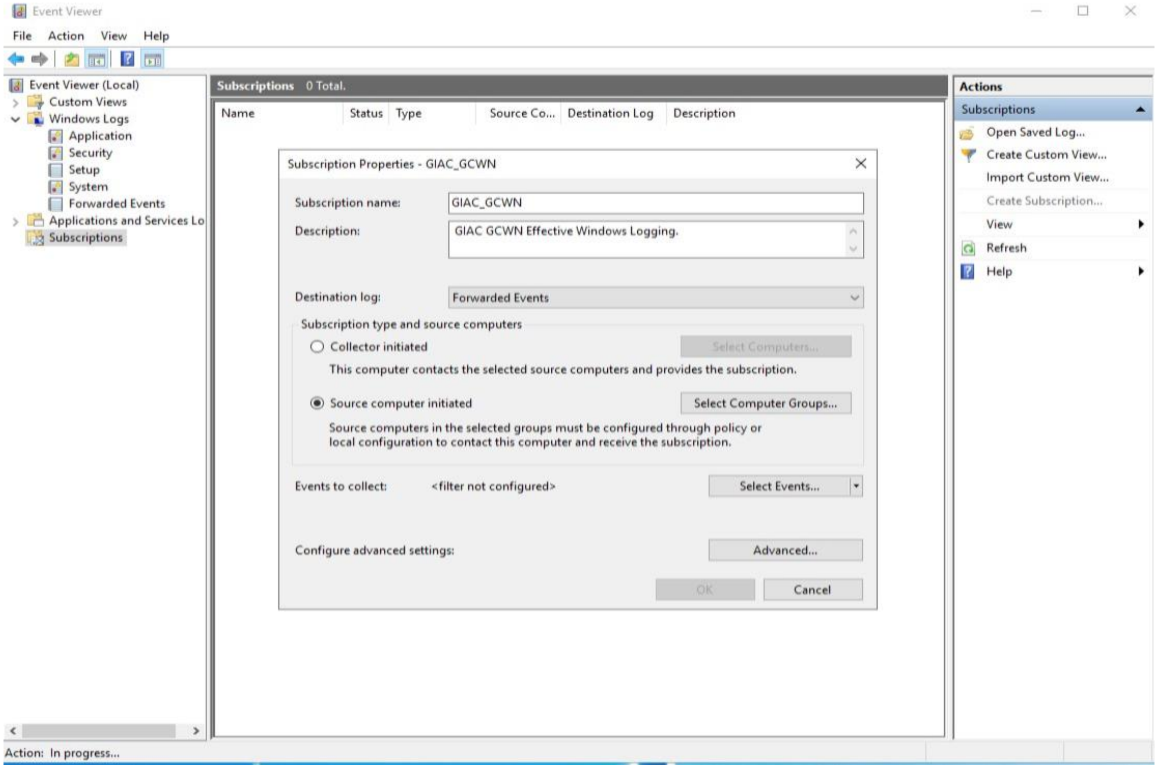


Figure 3. Creating a Subscription.



Subscription Properties - GIAC_GCWN

Subscription name: GIAC_GCWN

Description: GIAC GCWN Effective Windows Logging.

Destination log: Forwarded Events

Subscription type and source computers

○ Collector initiated

This computer contacts the selected source computers and provides the subscription.

● Source computer initiated

Source computers in the selected groups must be configured through policy or local configuration to contact this computer and receive the subscription.

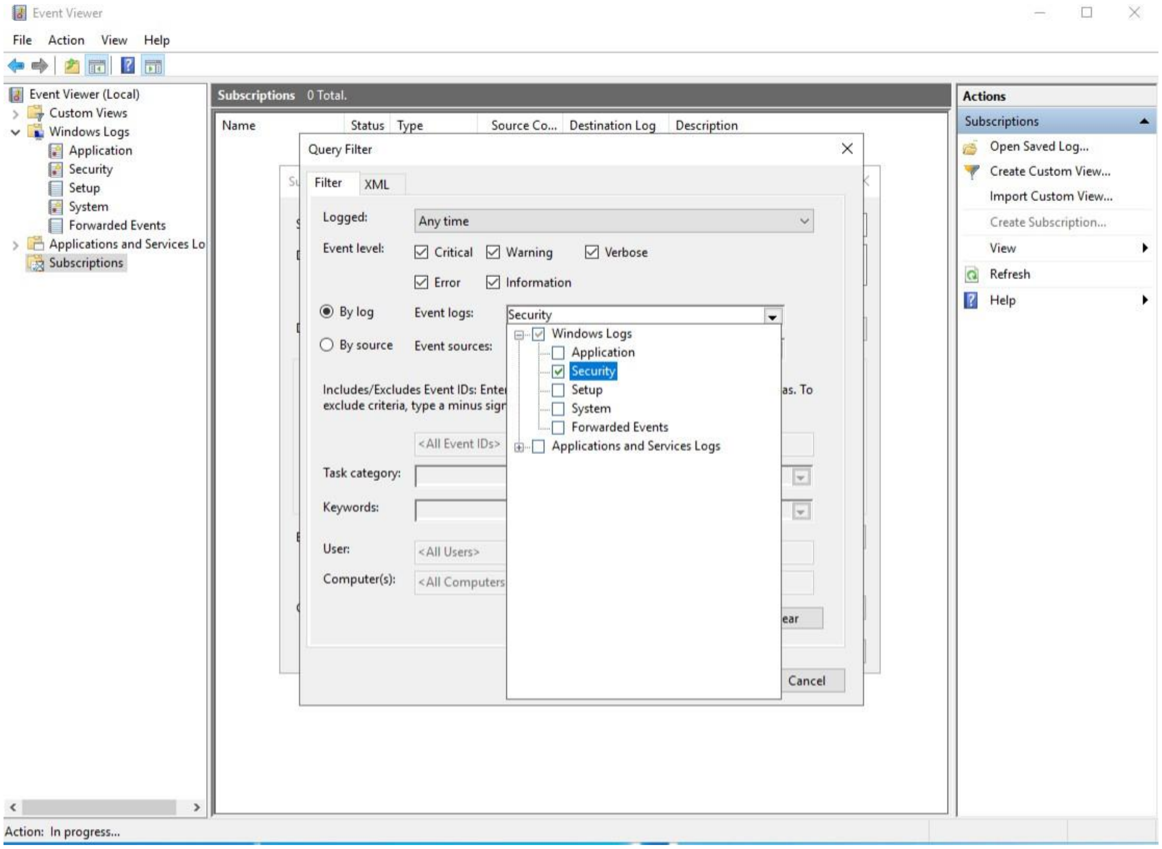
Events to collect: <filter not configured>

Configure advanced settings:

Figure 4. Configure Subscription Properties.

By default, Forwarded Events is selected as the predefined log location. This can be changed by selecting an alternate location from the dropdown.

6. Click **Select Events.**
7. Select the desired timeframe to retrieve logs from the sources retroactively.
8. Select **all levels** in Event Level.
    a. In more specially tailored subscriptions, only select the applicable event level.
9. Select **By log**.
10. From the drop-down **select.**
    - Windows Logs -> Security
11. Click **OK**.



Logged: Any time

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

● By log Event logs: Security

○ By source Event sources:

☑ Windows Logs
□ Application
☑ Security
□ Setup
□ System
□ Forwarded Events
□ Applications and Services Logs

Includes/Excludes Event IDs: Ente... exclude criteria, type a minus sign ... as. To

<All Event IDs>

Task category:

Keywords:

User: <All Users>

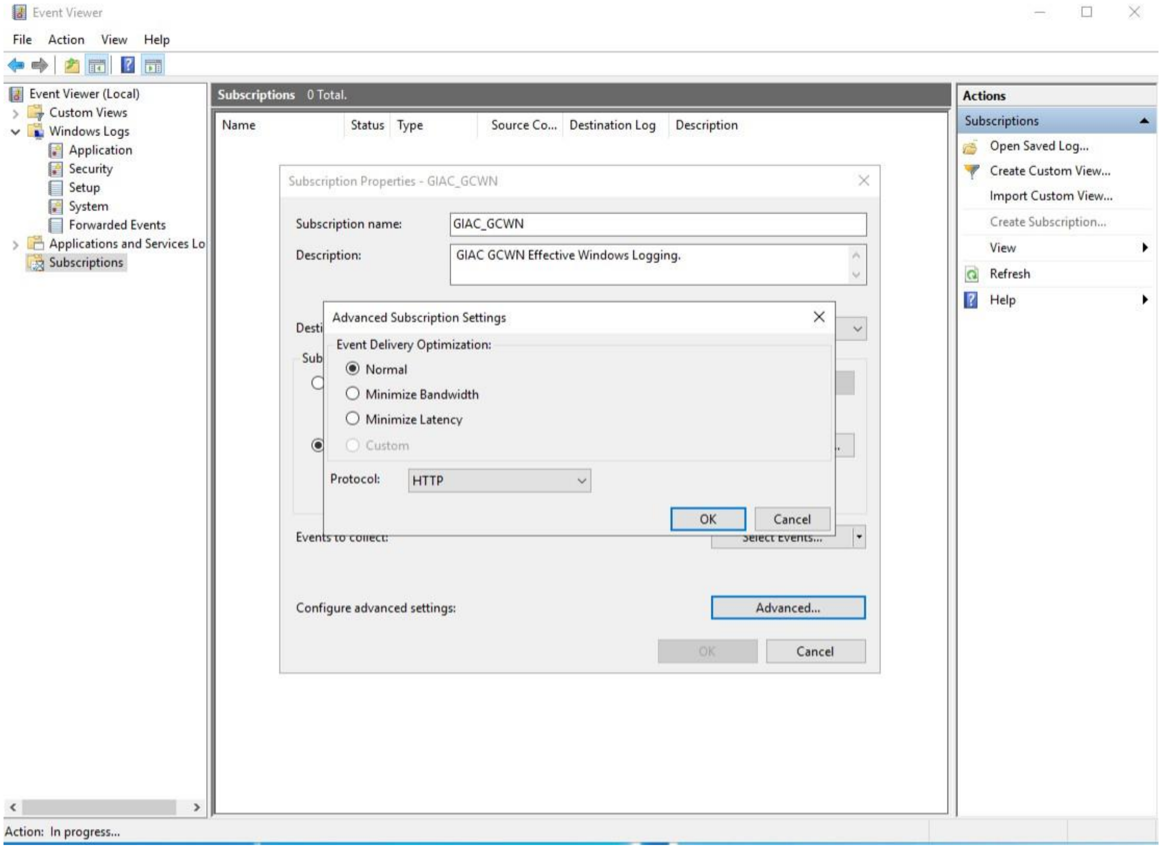
Computer(s): <All Computers

Figure 5. Select the Event Logs to collect.

The configuration of the advanced subscription settings sets the frequency of that event being received.

12. Click the **Advanced button.**
13. Select **Normal.**
    - Protocol HTTP (5985) or HTTPS (5986) can be selected

Event Delivery Optimization permits the collection of logs in 15-minute (normal), 6-hour (Minimize bandwidth), or 30 seconds (minimize latency) intervals.



Subscription Properties - GIAC_GCWN

Subscription name: GIAC_GCWN

Description: GIAC GCWN Effective Windows Logging.

Advanced Subscription Settings

Event Delivery Optimization:

● Normal

○ Minimize Bandwidth

○ Minimize Latency

○ Custom

Protocol: HTTP

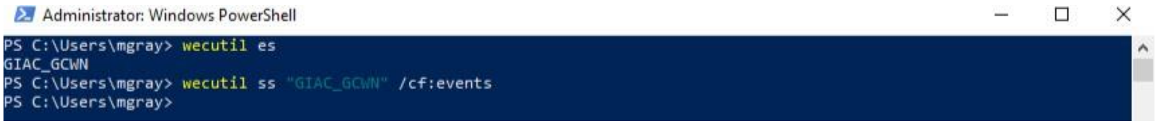
Figure 6. Configuring advanced subscription settings.

3.5. Modify Subscription Text

Windows provides two formats for the Windows Logs “Rendered Text” and “Events”. Rendered Text formatting offers a dynamically created “Message” within each log that gives a brief synopsis of what the event is trying to convey. While this is beneficial, it does require additional compute resources from the source host. Ultimately, “Rendered Text” takes up more space as these logs now contain additional information that is not a necessity. It is recommended to change the format to “Events” using the method below.

1. Open PowerShell as an **administrator**.
2. Run **wecutil es** to find the names of the current subscriptions.

3. Run **wecutil ss "Name of your subscription" /cf:events**



```
PS C:\Users\mgray> wecutil es
GIAC_GCWN
PS C:\Users\mgray> wecutil ss "GIAC_GCWN" /cf:events
PS C:\Users\mgray>
```

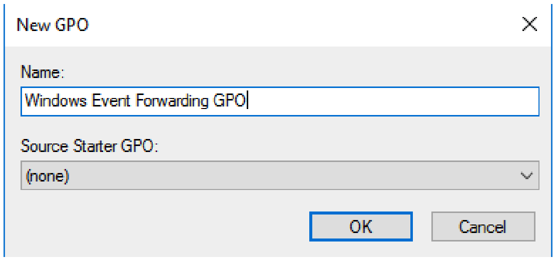
Figure 7. Modify Subscription text type.

3.6. Source Computer Policy Configuration

For hosts running Windows 7 or later, the recommended practice is to configure the Event Forwarding policies via Domain GP. The ability to read host Security logs and other default log files will be covered in the section below.

3.6.1. Source Group Policy Objects

When creating a new GPO for source configuration, it is a best practice that each identified source is created as part of a new group, and GPO named accordingly with the Event Source (source of events and domain users' groups). It is also common to create a baseline Event Forwarding configuration that spans the entire environment, and more specific configurations created for select hosts. The created GPOs should have both Enforced, and Link Enable setting applied after being properly configured for the in-scope source hosts.



Name:
Windows Event Forwarding GPO

Source Starter GPO:
(none)

Figure 8. Example Event Source GPO creation.

3.6.2. Windows Remote Management Policy Enablement

WinRM and Event Forwarding can be managed via GP for the member hosts, unlike the collector, which recommended a manual approach to the configuration. WinRM (if not enabled and started already) can be started using a System Service policy. To mitigate a host firewall blocking WinRM connectivity, Active Directory provides predefined WinRM firewall rules.

The WinRM service can be found in the path below:

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Windows Settings -> Security Settings -> System Services -> Windows Remote Management (WS-Management)	
	Set to Automatic

Table 2. WinRM GP system service location.

Inbound connection listeners are required for WinRM functionality. The Allow remote server management through WinRM policy will create listeners on port 5985 for WinRM 2.0 and above. With the IP values set to *, WinRM will start running and listen on the "any" IP address.

The Allow remote server management through WinRM can be found and enabled in the path below:

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service -> Allow remote server management through WinRM	
	Enabled IPv4 Filter: * (optional)IPv6 Filter: *

Table 3. Enable WinRM listeners.

3.6.3. Event Forwarding Policy Enablement

All sources must be configured to forward events to the subscription manager (Windows Event Collector Server). The subscription manager controls all subscriptions that are created on it (collector server). Each source must be able to contact the manager in order to retrieve a list of all subscriptions. Each subscription specifies what events to forward.

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Administrative Templates -> Windows Components -> Event Forwarding -> Configure Target Subscription manager	

	Enabled *configure SubscriptionManagers within settings*

Table 4. Subscription manager server location.

To configure SubscriptionManager:

1. After enabling the policy, click **on show**.
2. Set the Server option using the syntax below:
Server=[http|https]://FQDN[:PORT][/wsman/SubscriptionManager/WEC[, Refresh=SECONDS]
3. Once the SubscriptionManager value has been set, click **OK**.

Example:
Server=http://mdc0.gcwn.lab:5985/wsman/SubscriptionManager/WEC,Refresh=60

To permit event log files to be read by the forwarding service, the Event Log Readers group needs to be modified to include the NETWORK SERVICE account.

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Windows Settings -> Security Settings -> Restricted Groups	
	Add Group 'Event Log Readers' with the 'NETWORK SERVICE' account as a member

Table 5. Adding NETWORK SERVICE to Event Log Readers Restricted Group.

The final step is adding the appropriate rights for the NETWORK SERVICE principle to read security logs.This is done by finding the channelAccess string on the collector and adding the string to the appropriate GPO setting.

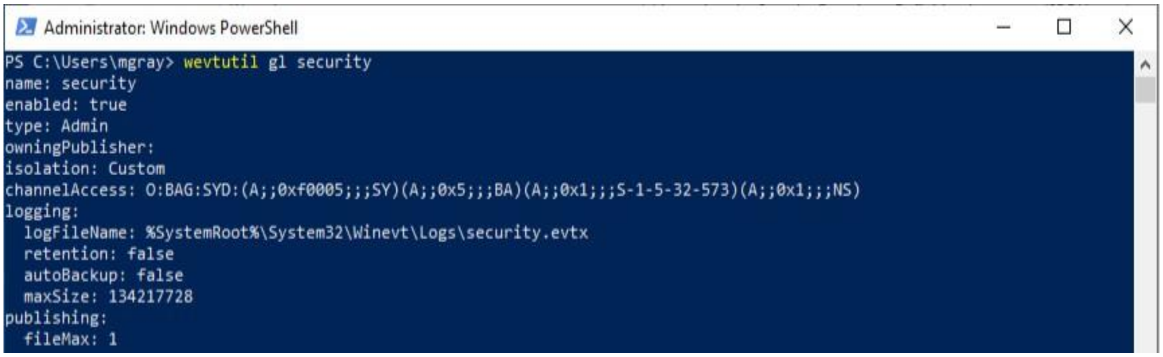
To Find channelAccess string:

1. On the Collector **open PowerShell** as an Administrator.
2. Run the command: **wevtutil gl security**
3. **Copy** the channelAccess string stating with the "O".
   a. **O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)**
   b. If the **channelAccess** string in the command output does not include **(A;;0x1;;;NS)**, it will need to be appended in the GPO.
4. Paste the string in a text editor and **append** the string if necessary.
5. Navigate to the GPO setting below and add the **channelAccess value** to the applicable Event Log Service access.

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Administrative Templates -> Windows Components -> Event Log Service -> Security -> Configure log access	

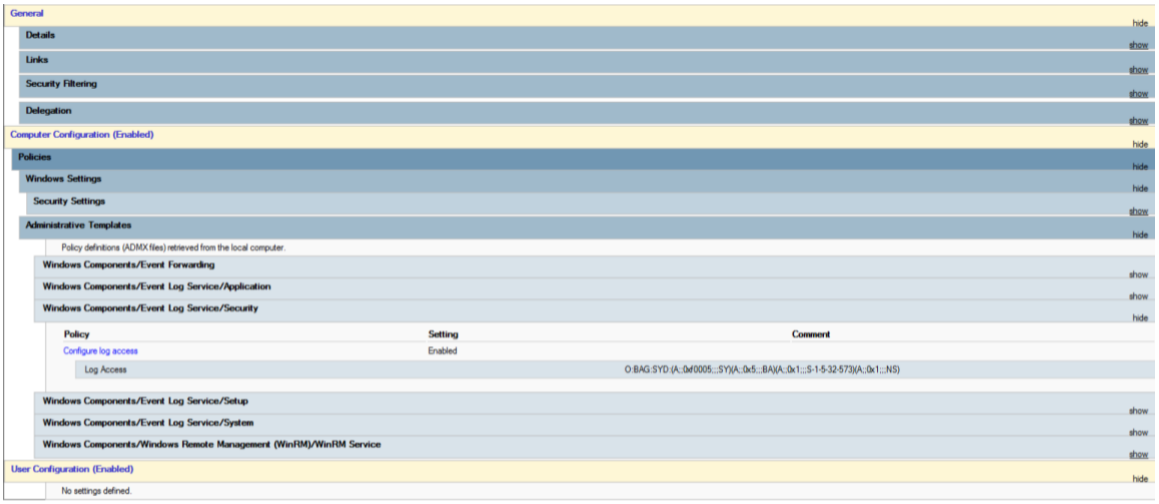
	Enabled *configure log access option with channelAccess*

Table 6. Configure log access permission.



```
PS C:\Users\mgray> wevtutil gl security
name: security
enabled: true
type: Admin
owningPublisher:
isolation: Custom
channelAccess: O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)
logging:
  logFileName: %SystemRoot%\System32\Winevt\Logs\security.evtx
  retention: false
  autoBackup: false
  maxSize: 134217728
publishing:
  fileMax: 1
```

Figure 9. Getting channelAccess value for log access.



General

Details

Links

Security Filtering

Delegation

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Event Forwarding

Windows Components/Event Log Service/Application

Windows Components/Event Log Service/Security

Policy	Setting	Comment
Configure log access	Enabled	
Log Access		O:BAG:SYD:(A;;0xf0005;;;SY)(A;;0x5;;;BA)(A;;0x1;;;S-1-5-32-573)(A;;0x1;;;NS)

Windows Components/Event Log Service/Setup

Windows Components/Event Log Service/System

Windows Components/Windows Remote Management (WinRM)/WinRM Service

User Configuration (Enabled)

No settings defined.

Figure 10. Log access configured in GPO.

3.7. System Monitor (Sysmon){Optional}

“System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time” (Mark & Thomas, 2019). This is an optional install but highly recommended as it provides analysts an additional source to derive information for analysis.

If there is no endpoint management software in the environment, Sysmon can be deployed via GPO to close the gap on the lack of visibility. Deploying Sysmon at scale is out of scope for this document; however, instructions and resource links will be provided in the appendix.

3.8. NXLog Configuration

NXLog is an excellent log source collection tool for forwarding logs to a SIEM. NXLog is an open source tool that is available on various platforms and is flexible enough to fit the needs of capturing and normalizing logs for our purposes. The provided patterndb file will limit the events collected and sent to the sensor (Windows Event IDs not present in patterndb.xml are not forwarded).

Because there is a centralized collector, NXLog only needs to be installed and configured for the collector host as this will be the host transforming and sending the logs to the sensor.

To Install NXLog:

1. Download the applicable binary and place on the collector. Link: https://nxlog.co/products/nxlog-community-edition/download
2. Once installed navigate to the **conf** folder located **in C:\Program Files (x86)\nxlog** or **C:\Program Files\nxlog** (depending on 64 vs 32 bit installer)
3. Rename the **nxlog.conf** file to **nxlog.conf.old**
4. Copy the provided configuration into the **conf** folder
5. Copy the provided **patterndb.xml** file into the **conf** folder
6. Open an administrative PowerShell Windows and run the command **Start-Service nxlog** (or start from services panel)
7. Check the **nxlog.log** file located in the **C:\Program Files (x86)\nxlog\data** folder for errors.

If no errors are present, check the portal for incoming logs.

Windows Event Collector, Event Subscription(s), and GPO configuration is now complete. The next sections are optional to review but recommended.

4. Recommended Events to Collect

4.1. Overview

To alleviate the log data volume fatigue mentioned earlier in this document, an "output-driven" (Chuvakin, 2012) approach to log collection is the logical choice. The output-driven methodology drives focus on collecting artifacts that have a known or expected utilization, offering the ability for seamless prioritization. This process is tedious, time-consuming, and requires security practitioners to have the knowledge and expertise to define specific use cases for evidence collection. While the barrier to entry is more difficult than an input-driven approach, the result is an efficient, cost inducive, augmentation to security operations. The purpose of this section is to provide a basic set of events recommended for collection to bolster security analysis capabilities. This is a non-exhaustive list of suggestions; it is highly recommended to reference other industry publications released from varying organizations to assist in defining the best security posture for each distinctive environment.

4.2. Windows Firewall

In environments where the built-in host-based firewalls an enabled and in use, it is of great value to collect Firewall status events. In a scenario where the Windows Firewall is turned offed by a Normal user, this event should be collected for further analysis.

Event ID	Name	Level	Event Log
2004	Firewall Rule Add	Information	Microsoft-Windows-Windows Firewall with Advanced Security/Firewall
2005	Firewall Rule Change	Information	Microsoft-Windows-Windows Firewall with Advanced Security/Firewall
2006,2033	Firewall Rules Deleted	Information	Microsoft-Windows-Windows Firewall with

			Advanced Security/Firewall
2009	Firewall Failed to load Group Policy	Information	Microsoft-Windows-Windows Firewall with Advanced Security/Firewall

Table 7. Recommended Windows Firewall Events.

4.3. Operating System Security, Stability, Change

Operating System Security, Stability, and Change events are comprised of a number of varying conditions that may be irregular and have the potentiality to disrupt operations or act as an indicator of potential targeting of specific services or systems. These events may also serve as a method for reviewing newly installed software and system services.

Event ID	Name	Level	Event Log
7000,7023,7024,7026, 7031,7032,7034,7013,1069	A Service Failed to Start	Error	System
1000	Application Error	Error	Application
1001	Application Hang	Error	Application
1001	Blue Screen	Error	System
6422	A Device was Enabled	Information	System
1074	Shutdown Initiate Failed	Warning	User32
1022,1033	New MSI File Installed	Information	System
903,904	New Application Installed	Information	Program Inventory
907,908	Removed Application	Information	Program Inventory
7000	The Service Failed to Start	Error	System
7045	New Windows Service	Information	System

4657	Registry Modification	Information	Security
4616	System Time Changed	Information	Security
4618	A Monitored Security Event Pattern Has Occurred	Warning	Security
4719	System Audit Policy Was Changed	Warning	Security
4649	Reply Attack Detected	Warning	Security

Table 8. Operating System Security, Stability, and Change events for monitoring.

4.4. Windows Update Monitoring

For large environments, these events may be voluminous; however, it is important to track when hosts are unable to successfully update to avoid prolonged exposure of an application issue or vulnerability.

Event ID	Name	Level	Event Log
20, 24, 25, 31, 34, 35	Windows Update Failed	Error	Microsoft-Windows-WindowsUpdateClient/Operational
1009	Hotpatching Failed	Information	Setup
19	Windows Update Installed	Information	System

Table 9. Windows Update events for monitoring.

4.5. Clearing Event Logs

The clearing of event logs should rarely if ever occur in an environment. The reasons for an individual to legitimately clear logs can be controlled by compensating configurations. When an event log is cleared, it is immediately suspicious and should be investigated.

Event ID	Name	Level	Event Log
104	Event Log was Cleared	Information	System

1102	Audit Log was Cleared	Information	Security
1100	Event Log Service Shutdown	Information	Security

Table 10. Log cleared events for monitoring.

4.6. Windows Account Usage

Domain and Standalone system user account information to include, but not limited to, account lockout, remote desktop login, users authenticating as an elevated user, amongst other details can be collected and audited. Tracking local and domain account usage can help identify unauthorized account usage.

Event ID	Name	Level	Event Log
4728,4732,4756	User Added to Privileged Group	Information	Security
4735	Security-Enabled group Modification	Information	Security
4624	Successful User Account Login	Information	Security
4625	Failed User Account Login	Information	Security
4648	Account Login with Explicit Credentials	Information	Security
4740	A User Account was Locked Out	Information	Security
4672	Logon with Special Privileges	Information	Security
4782	Password Hash Accessed	Information	Security
4964	Special Groups Have Been Assigned To A New Logon	Information	Security

Table 11. Account Activity Events

Lockout events for domain accounts are generated on the domain controller whereas lockout events for local accounts are generated on the local computer.

4.6.1. Windows Account Logon Types

Account activity events may contain numerous fields describing the specification action that was taken as well as the user. Specifically, Event ID 4624 (Successful User Account Login) contains several fields and types that are essential to context and analysis.

Event ID	Name	Level	Type
4720	User Account Created	Information	2: Interactive 3: Network 4: Batch or Scheduled Task 5: Service 7: Screen Unlock 8: NetworkCleartext 9: New credentials such as RunAs 10: Remote Desktop, Terminal Services, or Remote Assistance 11: Cached credentials
4720	User Account Created	Information	Subject: Who requested logon Logon Type: How logon occurred New Logon: Provides information about origin of request Process Information: Identify requesting process Network Information: Provides information about origin of request Detailed Authentication Information: Authentication mechanism used

Table 12. Account Logon Types and Fields.

4.7. Kernel Driver Signing

Any indication of a protected driver being altered may indicate malicious activity or a disk error and warrants investigation.

Event ID	Name	Level	Event Log

5038	Detected an invalid image hash of file	Information	Security
6281	Detected an invalid page hash of an image file	Information	Security
3001,3002,3003,3004,3010,3023	Code Integrity Check	Warning, Error	Microsoft-Windows-CodeIntegrity/Operational
6	New Kernel Filter Driver	Information	System
219	Failed Kernel Driver Loading	Warning	System

Table 13. Kernel Driver Signing Events for monitoring.

4.8. Windows Defender Activities

In environments that leverage Windows Defender, it is of value to collect events as Windows Defender events can provide information on the detection, removal, and prevention of Spyware and Malware. Additionally, administrative events are also generated for operational abnormality identification.

Event ID	Name	Level	Event Log
1000	An antimalware scan started	Information	Microsoft-Windows-Windows Defender/Operational
1001	An antimalware scan finished	Information	Microsoft-Windows-Windows Defender/Operational
1002	Scan Terminated	Information	Microsoft-Windows-Windows Defender/Operational
1005	Scan Failed	Error	Microsoft-Windows-Windows Defender/Operational
1006	Detected Malware	Warning	Microsoft-Windows-Windows Defender/Operational
1008	Action on Malware Failed	Error	Microsoft-Windows-Windows Defender/Operational

1010	Failed to remove item from quarantine	Error	Microsoft-Windows-Windows Defender/Operational
2001	Failed to update signatures	Error	Microsoft-Windows-Windows Defender/Operational
2003	Failed to update engine	Error	Microsoft-Windows-Windows Defender/Operational
2004	Reverting to last known good set of signatures	Warning	Microsoft-Windows-Windows Defender/Operational
3002	Real-Time protection failed	Error	Microsoft-Windows-Windows Defender/Operational
5008	Unexpected Error	Error	Microsoft-Windows-Windows Defender/Operational

Table 14. Windows Defender Events for monitoring.

4.9. Mobile Device Activities

The capability to monitor network connectivity activity for an increasingly mobile workforce is paramount for the identification of a potential compromise. The frequency of events identified below is dependent on how often a device connects and disconnects to wireless networks.

Event ID	Name	Level	Event Log
10000,10001	Network Connection and Disconnection Status (Wired and Wireless)	Information	Microsoft-Windows-NetworkProfile/Operational
8000,8011	Starting a Wireless connection	Information	Microsoft-Windows-WLAN-AutoConfig/Operational
8001	Successfully connected to Wireless connection	Information	Microsoft-Windows-WLAN-AutoConfig/Operational
8003	Disconnect from Wireless connection	Information	Microsoft-Windows-WLAN-AutoConfig/Operational

11000,11001,11002	Wireless Association Status	Information, Error	Microsoft-Windows-WLAN-AutoConfig/Operational
11004,11005,11010,11006	Wireless Security Started, Stopped, Successful, or Failed	Information, Error	Microsoft-Windows-WLAN-AutoConfig/Operational
8002	Wireless Connection Failed	Error	Microsoft-Windows-WLAN-AutoConfig/Operational
12011,12012,12013	Wireless Authentication Started and Failed	Information, Error	Microsoft-Windows-WLAN-AutoConfig/Operational

Table 15. Mobile Device activities for monitoring.

4.10. External Media Detection

For sensitive networks, the detection of USB device utilization may be important. The events below can be used to proactively detect USB usage. For a more robust external device detection capability, it is recommended that the organization looks at specialized software.

Event ID	Name	Level	Event Log
43	New Device Information	Information	Microsoft-Windows-USB-USBHUB3-Analytic
400	New Mass Storage Installation	Information	Microsoft-Windows-Kernel-PnP/Device Configuration
410	New Mass Storage Installation	Information	Microsoft-Windows-Kernel-PnP/Device Configuration
2100,2102,2105,2106	Pnp or Power Management Operation	Information	Microsoft-Windows-DriverFrameworks-UserMode-Operational
2003,2010,2004,2006	Loading Drivers to Control a Newly Discovered Deivce	Information	Microsoft-Windows-DriverFrameworks-UserMode-Operational
6416	A New External Device was Recognized by the System	Information	Microsoft-Windows-DriverFrameworks-UserMode-Operational
6422	A Device was Enabled	Information	Microsoft-Windows-DriverFrameworks-UserMode-Operational

6423	The Installation of this Device is forbidden by system policy	Information	Microsoft-Windows-DriverFrameworks-UserMode-Operational

Table 16. External Media detection activities for monitoring.

4.11. Process Tracking

If workstations in an environment do not have an endpoint detection and response agent, Windows can natively collect process invocation and command line data. For increased log verbosity without precuring any paid software, Sysmon can be configured and deployed.

Event ID	Name	Level	Event Log
4688	A new process has been created	Information	Security
1	Process creation	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
2	A process changed a file creation time	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
3	Network Connection	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
10	Process Access	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
11	File Create	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational
12,13,14	Registry Event	Information	Applications and Services Logs/Microsoft/Windows/Sysmon/Operational

Table 17. Process tracking and Sysmon events for monitoring.

4.12. Network Host Activities

Windows hosts natively generate network log artifacts that can be valuable for network troubleshooting, detecting suspicious network traffic, unauthorized network policy change identification, and unusual network resource manipulation.

Event ID	Name	Level	Event Log
5140	Network Share Accessed	Information	Security
5142	Network Share Created	Information	Security
5144	Network Share Deleted	Information	Security
4706	New Trust for Domain	Information	Security
4769	Kerberos Service Ticket Request Failed	Information	Security
6273	Network Policy Server Denied Access	Information	Security
6279	Network Policy Server Locked Account	Information	Security
6272	Network Policy Server Granted Full Access	Information	Security
6276	Network Policy Quarantined User	Information	Security

Table 18. Network Host Activities for monitoring.

4.13. PowerShell Activities

PowerShell is included by default in modern versions of Windows. PowerShell events may provide value when identifying malicious activity that relies on PowerShell to run or download additional payloads.

Event ID	Name	Level	Event Log
800	Get-MessageTrackingLog cmdlet	Information	Powershell
169	Remote Connection	Information	Powershell
4103	Exception Raised	Information	Microsoft-Windows-Powershell/Operational
4104	Script block contents	Information	Microsoft-Windows-Powershell/Operational
4105	Script block start	Information	Microsoft-Windows-Powershell/Operational

4106	Script block end	Information	Microsoft-Windows-Powershell/Operational

Table 19. Windows PowerShell activities for monitoring.

4.14. Scheduled Tasks

The scheduling or deletion of tasks can be a sign of malicious activity. It has been observed that particular malware variants create a scheduled task to wait for specific conditions prior to downloading additional malicious payloads or conduct additional activity.

Event ID	Name	Level	Event Log
106	New Task Registered	Information	Microsoft-Windows-TaskScheduler/Operational
141	Task Deleted	Information	Microsoft-Windows-TaskScheduler/Operational
142	Task Disabled	Information	Microsoft-Windows-TaskScheduler/Operational
200	Task Launched	Information	Microsoft-Windows-TaskScheduler/Operational

Table 20. Scheduled Task events for monitoring.

4.15. Windows Account Life Cycle

The following events can be used to record new account creation, account modification, account deletion, account disablement, and account enablement activities. The analysis of these events can ensure proper account management procedures in the environment.

Event ID	Name	Level	Event Log
4720	User Account Created	Information	Security
4722	A User Account was enabled	Information	Security
4723	An attempt was made to change an account’s password	Information	Security

4724	An attempt was made to reset an account’s password	Information	Security
4725	A user account was disabled	Information	Security
4726	A user account was deleted	Information	Security
4738	A user account was changed	Information	Security
4781	The name of an account was changed	Information	Security

Table 21. Windows Account Life Cycle events for monitoring.

4.16. Windows Audit CVE

Audit CVE logs are generated on Windows 10 and later systems when there is an attempt to exploit a known, patched vulnerability. Monitoring audit CVE events can provide insight into attempted exploitations in an environment.

Event ID	Name	Level	Event Log
1	Microsoft-Windows-Audit-CVE	Warning	Application

Table 22. Windows Audit CVE events for monitoring.

4.17. Microsoft Cryptography API

Certificate verification and encryption/decryption of data is performed using the Microsoft CryptoAPI. There are a number of interesting events that should be logged for suspicious behavior or for future auditing.

Event ID	Name	Level	Event Log
11	Cert Trust Chain Build Failed	Information	Microsoft-Windows-CAPI2/Operational
70	Private Key Accessed	Information	Microsoft-Windows-CAPI2/Operational
90	X.509 Object	Information	Microsoft-Windows-CAPI2/Operational

Table 23. Microsoft Cryptography API events for monitoring.

5. Recommended Events Group Policy

5.1. Overview

The following section defines the required changes within Group Policy that must be made in order to collect the events identified in the previous section. Not all events that were mentioned require any additional configuration changes so that they will be excluded from this section.

5.2. Operating System Security, Stability, Change GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Policy Change	
Audit Audit Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System	
Audit System Integrity	Success and Failure

Table 24. Required GPO settings for the Windows Account Usage and Life Cycle events.

5.3. Windows Account Usage and Account Life Cycle GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon/Logoff	
Audit Account Lockout	Success
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Account Management	
Audit Computer Account Management	Success and Failure
Audit Security Group Management	Success and Failure
Audit Other Account Management Events	Success and Failure
Audit User Account Management	Success and Failure

Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon/Logoff	
Audit Group Membership	Success
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Table 25. Required GPO settings for the Windows Account Usage and Life Cycle events.

5.4. Process Tracking GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Detailed Tracking	
Audit Process Creation	Success
Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation	
Include command line in process creation events	Enabled

Table 26. Required GPO settings for the Process Tracking events.

5.5. Network Host Activities GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit File Share	Success and Failure

Table 27. Required GPO settings for the Process Network Host Activities events.

5.6. PowerShell Activities GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	

Turn on Module Logging	Enabled *Requires PowerShell 5*
Turn on PowerShell Script Block Logging	Enabled

Table 28. Required GPO settings for the PowerShell Activities events.

5.7. Scheduled Tasks GPO

Group Policy Setting	Recommendation
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit Other Object Access Events	Success and Failure

Table 29. Required GPO settings for the Scheduled Tasks events.

References and Further Reading

Chuvakin, A. (2012, September 24). On “Output-driven” SIEM. Retrieved from https://blogs.gartner.com/anton-chuvakin/2012/09/24/on-output-driven-siem/

Windows Event Logging and Forwarding. (n.d.). Retrieved from https://www.cyber.gov.au/publications/windows-event-logging-and-forwarding

Spotting the Adversary with Windows Event Log Monitoring. (n.d.). Retrieved from https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm

Change the event log size to what Microsoft recommended Blog. (n.d.). Retrieved from https://www.jqit.com.au/blog/change-the-event-log-size-to-what-microsoft-recommended/

Microsoft (n.d.). Appendix L - Events to Monitor. Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor

Deploy Sysmon with GPO. (2017, September 5). Retrieved from https://natesec.com/deploy-sysmon-with-gpo/

Windows Events, Sysmon and Elk…oh my! (Part 2). (2018, June 26). Retrieved from https://silentbreaksecurity.com/windows-events-sysmon-elk-part-2/

Windows Event Log Forwarding In Windows Server 2016 [Tutorial]. (2019, October 10). Retrieved from https://adamtheautomator.com/windows-event-log-forwarding/

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

Windows Security Log Encyclopedia. (n.d.). Retrieved from https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/Default.aspx

Nsacyber/Event-Forwarding-Guidance. (2019, April 12). Retrieved from https://github.com/nsacyber/Event-Forwarding-Guidance/tree/master/Events

Murdoch, D. (2019). *Blue Team Handbook: SOC, SIEM, and Threat Hunting (V1. 02): A Condensed Guide for the Security Operations Team and Threat Hunter*.

Stevewhims. (n.d.). About Windows Remote Management. Retrieved from https://docs.microsoft.com/en-us/windows/win32/winrm/about-windows-remote-management

Log Analysis and the Challenge of Processing Big Data. (2020, January 22). Retrieved from https://www.graylog.org/post/log-analysis-and-the-challenge-of-processing-big-data

Creating Cyber Forensics Plans for Control Systems. (2008). Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/Forensics_RP.pdf

Microsoft. (n.d.). Audit Policy Recommendations. Retrieved from https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations

Microsoft. (2018). Accurate Time for Windows Server 2016. Retrieved from https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/accurate-time

451 Research. (2019). 451 Research: Tackling the Visibility Gap in Information Security. Retrieved from https://info.reliaquest.com/451RQBatemanVisibilityGapStudy

Finding Cyber Threats with ATT&CK-Based Analytics. (2019, October 11). Retrieved from https://www.mitre.org/publications/technical-papers/finding-cyber-threats-with-attck-based-analytics

Microsoft. (2013). Configure Advanced Subscription Settings. Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc749167(v=ws.11)?

Infocyte. (2018, March 7). Challenges of Threat Hunting with Endpoint Detection (EDR). Retrieved from https://www.infocyte.com/blog/2018/03/07/3-challenges-of-threat-hunting-with-edr/

6. Appendix A – Common Troubleshooting Steps

Below are some common troubleshooting steps to resolve any underlying issues experienced while attempting to deploy Windows Event Forwarding into an environment. The error below can be found in the **Application and Service Logs -> Microsoft -> Windows -> Eventlog-ForwardingPlugin** channel on the source computer. Be advised, this is not an exhaustive list and may exclude some environmental abnormalities causing connectivity issues.

6.1. All Subscriptions Have 0 Active Forwarders

Description: All settings (GPO + steps above) appear correct and system event log shows error event 10128 and 10129 (also helpful when eventforwarding log has error 105 with code 2150859027). Run the below steps on the Windows Event Collectors demonstrating the issue.

Step 1: Run the command (as administrator) **netsh http show urlacl**
-This will find and list URL ACLs running on the host. Take note of the URL mentioned in the 10128 error code and record the SDDL.

Step 2: If the output does not equal **SDDL: D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)**
Continue with the steps below.

Step 3: Run the command (as administrator) **netsh http delete urlacl url=http://+:5985/wsman/**
-This will remove the current entry from the system,

Step 4: Run the command (as administrator) **netsh http add urlacl url=http://+:5985/wsman/ sddl=D:(A;;GX;;;S-1-5-80-569256582-2953403351-2909559716-1301513147-412116970)(A;;GX;;;S-1-5-80-4059739203-877974739-1245631912-527174227-2996563517)**

Step 5: Restart the **winrm** and **wec** service (may require a reboot).

Step 6: Refresh the subscription status in event viewer.

6.2. Testing Connectivity

1. Make sure “Windows Remote Management” is running.

2. Run command to make sure the host is LISTENING on port 5985:
    a. netstat -an | findstr 5985
3. Test “Windows Remote Management” connectivity:
    a. Test-WSMan -ComputerName <IP or host name>
4. Verify Network Connection profile:
    a. Get-NetConnectionProfile

6.3. Check Collector to Source Computer Connectivity

Verify connectivity from Collector to Source Computer via WinRM.

1. Run command on Collector: winrm id /r:<Source Computer> /a:none

6.4. Source Computer Registration Check

List all registered Source Computers as well as the last heartbeat time.

1. Run command on Collector: wecutil gr <subscription name>

6.5. Windows Event Error 105

Check the Windows Forwarding/Operational event log on the Source Computer for errors. Event ID 105 “The forwarder is having a problem communicating with the subscription manager address” is often a result of the Windows Firewall on the Event collector blocking communication.

Ensure the following rules are accepting incoming connection:

- Windows Firewall port(s) Windows Remote Management (HTTP-In) Port 5985 configured for inbound communication.
- Windows Firewall port(s) Windows Remote Management (HTTP-In) – Compatibility Mode - Port 80 configured for inbound communication.
- Windows Firewall port(s) Windows Remote Management (HTTPs-In) configured for inbound communication.

Ensure there is no proxy interference.

- Run the following commands on source host(s) experiencing the error.
    1. netsh winhttp show proxy
    2. netsh winhttp reset proxy
- Retest connectivity.
    3. winrm id /:<IP or FQDN of Collector> -a:none

6.6. Windows Event Error 102

Event error 102 with Error code 5004 indicates that event cannot be created. This is often the result of the “Network Service” Account not having permissions to the security logs. Please ensure that the “Network Service” user has been added to the “Event Log Readers” group.

7. Appendix B – Sysmon

In order for the GPO to process correctly, the Sysmon binary, Sysmon configuration, and the startup script will need to be placed within the SYSVOL folder on a domain controller. Within the SYSVOL folder on the domain controller complete the steps below:

1. Within **SYSVOL** create a folder titled **Sysmon**
2. Download the latest copy of Sysmon and **place Sysmon.exe and Sysmon64.exe** in the **Sysmon folder**
3. Place the provided **Sysmon configuration** in the **Sysmon folder** and rename it to **Sysmonconfig.xml**
4. Place the provided **SysmonStartup.bat** in the **Sysmon folder**
5. Edit the **DC and FQDN lines** in the **SysmonStartup.bat** file to reflect the environment

Sysmon Group Policy Object

Create a new GPO and title it appropriately. Once created configure the setting below:

Group Policy Setting	Recommendation
Computer Configuration -> Polices -> Windows Scripts (Startup/Shutdown)	Right Click Startup, select Properties Select Add then Browser to navigate to the SysmonStartup.bat

After the GPO is created ensure it is linked to all of the OUs in scope for the Sysmon deployment. Be advised each host will need to be rebooted after the GPO is applied in order to initiate the Sysmon installation.