Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Windows Event Logging and Forwarding

APRIL 2019

Introduction

A common theme identified by the Australian Signals Directorate's Australian Cyber Security Centre (ACSC) while performing investigations is that organisations have insufficient visibility of activity occurring on their workstations and servers. Good visibility of what is happening in an organisation's environment is essential for conducting an effective investigation. It also aids incident response efforts by providing critical insights into the events relating to a cyber security incident and reduces the overall cost of responding to them.

This document has been developed as a guide to the setup and configuration of Windows event logging and forwarding. This advice has been developed to support both the detection and investigation of malicious activity by providing an ideal balance between the collection of important events and management of data volumes. This advice is also designed to complement existing host-based intrusion detection and prevention systems.

This document is intended for information technology and information security professionals. It covers the types of events which can be generated and an assessment of their relative value, centralised collection of event logs, the retention of event logs, and recommended Group Policy settings along with implementation notes.

This document does not contain detailed information about analysing event logs.

Accompanying this document is the ACSC's Windows event logging repository[1]. The repository contains configuration files and scripts to implement the recommendations in this document. All files and folders referred to in this document are available from this repository.

Considerations

This document's recommendations require the use of Microsoft Windows Server 2008 R2 and Microsoft Windows 7 SP1, or newer versions. Some Group Policy settings used in this document may not be available or compatible with Professional, Home or S editions of Windows.

To enable accurate correlation of events, accurate and consistent time stamps must be used. Organisations are recommended to ensure all devices in their environment (e.g. Windows hosts and network equipment) are configured to use an accurate time source.

As detailed in the ***Strategies to Mitigate Cyber Security Incidents***[2], the recommended event log retention time is at least 18 months; however, some organisations may have a regulatory requirement to retain event logs for a longer period.

[1] https://github.com/AustralianCyberSecurityCentre/windows_event_logging

[2] https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

To assist with the management of recommendations in this document, the Group Policy settings discussed should be placed in a separate Group Policy Object (GPO) with the scope set for all Windows hosts on the domain.

All changes made to systems should be fully tested to ensure there are no unintended side effects to an organisation's normal business processes. Testing should focus on the volume of logging generated and any impact on the network's performance, particularly where information may be transmitted across low bandwidth connections.

The recommended Group Policy settings in this document use advanced audit policies which may override existing legacy audit policies[3]. Care should be taken to ensure that existing legacy audit policies are migrated to advanced audit policies.

Sysmon (System Monitor)[4], a tool published by Microsoft, provides greater visibility of system activity on a Windows host than standard Windows logging. Organisations are recommended to use this tool in their Windows environment.

Event log retention

The Windows default settings have log sizes set to a relatively small size and will overwrite events as the log reaches its maximum size. This introduces risk as important events could be quickly overwritten. To reduce this risk, the Security log size needs to be increased from its default size of 20 MB. The Application and System log sizes should also be increased, but typically these do not contain as much data and hence do not need to be as large as the Security log. The default log sizes are acceptable in environments where local storage is limited (e.g. virtual infrastructure environments) provided logs are being forwarded.

The Group Policy settings provided in the table below will increase the maximum Security log size to 2 GB and the maximum Application and System log sizes to 64 MB. This will provide a balance between data usage, local log retention and performance when analysing local event logs. Note that these changes will increase the data storage requirements for each Windows host on the network.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 2097152
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System	
Specify the maximum log file size (KB)	Enabled Maximum Log Size (KB): 65536

[3] https://docs.microsoft.com/en-au/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff182311(v=ws.10)
[4] https://docs.microsoft.com/en-au/sysinternals/downloads/sysmon

Event categories

The default Windows settings provide only a subset of the desired logging events that assist in detecting and investigating malicious activity. This section covers the event categories that will significantly enhance technical analysis.

Each event category can be deployed independently and categories in the table below are ordered by the usefulness of the data source for detection and investigation. In general, most event categories are highly recommended. The list is not exhaustive and organisations should include additional event logs specific to their auditing requirements.

Each of the event categories below are accompanied by supplied subscription files. The subscriptions are used by Windows Event Forwarding to forward the locally generated events while filtering out the less valuable events.

Event Category	Description	Why	Value	Noise	Implementation Notes
Sysmon	Provides visibility of process creation and termination, driver and library loads, network connections, file creation, registry changes, process injection, and more.	Detects many forms of malware execution, persistence and misuse of legitimate tools including application whitelisting bypasses. Detects process injection and some forms of credential and password hash access.	Very High	Very High	If Sysmon can't be deployed use process tracking instead.
Account lockout	Records account lockout activity.	Detects password brute-forcing attempts, which an adversary could use to access an account.	High	Low	None
Account modifications	Records creation and modification of accounts and groups.	Detects unauthorised creation or modification of accounts with administrative privileges.	High	Low	None
Event collection	Forwards changes and errors with auditing, event collection and event forwarding.	Verifies Windows hosts on the network are auditing, collecting and forwarding logs as expected. Detects attempts by an adversary to suppress logging evidence.	High	Low	None
Account logon	Records activity related to accounts logging in and out.	Detects unauthorised use of accounts, including indicators of an adversary moving laterally through the network.	High	Medium	None

Process tracking	Provides visibility of process creation and termination, including command line arguments (without requiring Sysmon).	Detects the execution of some forms of malware and misuse of legitimate tools, including some forms of application whitelisting bypasses.	High	High	Should only be implemented if Sysmon can't be deployed.
AppLocker	Provides visibility of programs blocked by application whitelisting.	Detects malware that has been prevented from executing by application whitelisting.	Medium	Low	Only beneficial if AppLocker is configured.
Enhanced Mitigation Experience Toolkit	Records Enhanced Mitigation Experience Toolkit (EMET) events relating to mitigations that have been applied.	Detects exploitation attempts that have been successfully blocked by EMET.	Medium	Low	Only applicable if EMET is installed and configured. EMET is not available on Microsoft Windows 10 version 1709 and later.
Services	Provides information about the installation of services.	Detects installation of services that are used for persistence or lateral movement by an adversary.	Medium	Low	None
Windows Defender	Records when exploit mitigations have been applied by Windows Defender Exploit Guard. Records Windows Defender Antivirus detection events and errors or problems with running or updating the software.	Detects exploitation attempts that have been successfully blocked. Detects malware that has been successfully blocked and verifies the software is running and updating correctly.	Medium	Low	If Windows Defender Antivirus is not used, logs from other antivirus software should be forwarded. Exploit Guard has been available since Microsoft Windows 10 version 1709.
Windows Error Reporting	Records when an application crashes.	Detects exploitation attempts and unstable applications, which may indicate malicious activity.	Medium	Low	None
Code Integrity	Records code integrity violations for drivers and protected processes. If Device Guard is configured, it also records system-wide code integrity violations.	Detects malware or restricted applications that are being audited or prevented from executing by code integrity checks.	Medium	Low or Medium (with Device Guard)	Visibility is increased if Device Guard is configured.

File shares	Records creation, modification and access of file shares.	Detects access and modification of file shares. This includes lateral movement and access to file shares used to exfiltrate data from the network.	Medium	Medium	None
Scheduled tasks	Records the creation and modification of scheduled tasks.	Detects scheduled tasks being added or modified. This may include tasks used for lateral movement, persistence or elevation to system privileges.	Medium	Medium	None
Windows Management Instrumentation auditing	Produces audit records for local and remote Windows Management Instrumentation (WMI) operations in sensitive paths.	Detects the use of WMI by an adversary for local or remote reconnaissance, lateral movement and persistence.	Medium	Medium	None
NTLM authentication	Records outgoing NTLM authentication usage.	Detects intentional or unintentional NTLM leaks that could be used by an adversary to authenticate remotely or to escalate privileges within a domain.	Low	Medium	Noise depends on NTLM use in the network.
Object access auditing	Produces auditing on file paths, registry keys and processes with pre-existing audit permissions.	Detects some forms of unauthorised changes to sensitive files and registry keys, and some forms of credential and password hash access.	Low	Medium	None
PowerShell	Records PowerShell activity including interactive and script usage.	Detects PowerShell being used by an adversary.	Low	High	None

Event category configuration

Sysmon

Sysmon records key events that will assist in an investigation of malware or the misuse of native Windows tools. These events include process creation and termination, driver and library loads, network connections, file creation, registry changes, process injection, named pipe usage and WMI-based persistence. Sysmon also supports filtering of events to keep logging at a manageable level.

The Sysmon configuration file defines what events will be recorded. A default Sysmon configuration file is supplied in *events/sysmon/sysmon_config.xml* and should be suitable for most environments. To further filter or control events that are forwarded, the Sysmon configuration may be customised and Sysmon subscriptions may be enabled or disabled.

As with all software, Sysmon should be installed by following the agreed software deployment practices for the network. Sysmon can be deployed by Group Policy settings or the System Centre Configuration Manager (SCCM). No other Group Policy setting changes are necessary as all Sysmon's configuration information is contained in the configuration file.

Guidance on the creation of an installation file (i.e. MSI file) that may simplify the deployment of Sysmon is supplied in *events/sysmon/msi/README.txt*. Alternatively, the following commands can be used to maintain Sysmon from a script or command line tool:

- Installation: *sysmon -accepteula -i or sysmon -accepteula -i sysmon_config.xml*
- Configuration: *sysmon -c sysmon_config.xml*
- Uninstallation: *sysmon –u*.

The end-user license agreement must be accepted before using Sysmon.

Account lockout

The following Group Policy setting can be implemented to record events related to accounts being locked and unlocked.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Logon/Logoff	
Audit Account Lockout	Success

Account modifications

The following Group Policy settings can be implemented to record events related to account creation or deletion, as well as modifications to account groups.

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

Event collection

This event category records and forwards auditing policy changes, when event logs are cleared and failures with event logging. Many of these events are recorded by default, but the following Group Policy settings further increase visibility.

The subscription will forward, if possible, warnings and errors resulting from problems with Windows Event Forwarding. These logs can detect errors related to incorrectly formed subscriptions and can assist with debugging.

Group Policy Setting	Recommendation Option
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

Account logon

The following Group Policy settings can be implemented to record logon and logoff events including interactive logons, network logons and logons using explicit credentials.

The subscription will not forward Kerberos logon events which produce a high level of noise on a typical network. This may obscure the misuse of Kerberos tickets; however, this information will still be available on each local machine.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon/Logoff	
Audit Group Membership *(only available on Microsoft Windows 10 and Microsoft Windows Server 2016)*	Success
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Process tracking

The following Group Policy settings can be implemented to record process creation and termination events. Organisations are recommended to collect this information through Sysmon. If Sysmon can't be used, process tracking events can be collected through this native Windows logging.

It is important to increase the value of the process creation events by including command line arguments with process creation events. This feature is enabled for Microsoft Windows 8.1 and Microsoft Windows Server 2012 R2, and newer versions. For earlier versions of Windows, an update is available. For more information see ***Microsoft Security Advisory 3004375***[5] and ***Update to improve Windows command-line auditing***[6].

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

AppLocker

This event category will forward audit or deny events from AppLocker[7]. AppLocker must be configured in either auditing or enforcement mode for events to be generated. For more information, see the application whitelisting section of the Microsoft Windows hardening guide publications[8] and the ***Implementing Application Whitelisting*** publication[9]. If a third party application whitelisting tool is used, follow the tool's documentation to enable and forward logging. At a minimum, blocked execution events should be logged.

Enhanced Mitigation Experience Toolkit

The Enhanced Mitigation Experience Toolkit (EMET)[10] was designed by the Microsoft Security Research Center (MSRC) to enable additional system-wide and application-specific protection against software exploitation. However, Microsoft has since ceased support for EMET as many of the mitigation measures have been incorporated into Windows Defender Exploit Protection[11].

[5] https://docs.microsoft.com/en-au/security-updates/SecurityAdvisories/2015/3004375

[6] https://support.microsoft.com/en-au/help/3004375/microsoft-security-advisory-update-to-improve-windows-command-line-aud#!en-us%2Fhelp%2F3004375%2Fmicrosoft-security-advisory-update-to-improve-windows-command-line-aud

[7] https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

[8] https://www.cyber.gov.au/publications

[9] https://www.cyber.gov.au/publications/implementing-application-whitelisting

[10] https://support.microsoft.com/en-au/help/2458544/the-enhanced-mitigation-experience-toolkit

[11] https://docs.microsoft.com/en-au/windows/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard

EMET still provides significant security benefits for versions of Windows prior to Microsoft Windows 10 version 1709, especially by applying application-specific mitigation measures to third-party applications[12].

This event category will forward warnings and errors generated by EMET. EMET must be installed and configured correctly for events to be generated. For further information, see the Enhanced Mitigation Experience Toolkit section of the Microsoft Windows hardening guide publications[13].

Services

This event category will forward events when services have been installed. It does not require any change to Group Policy settings. This category will also forward events related to the event log service being shut down.

Windows Defender

This event category will forward configuration changes, update issues and malware detected by Windows Defender Antivirus. If third-party antivirus software is used, the vendor's documentation should be followed to enable and forward logging to a central location. At a minimum, configuration changes, update issues and malware detection events should be logged and forwarded.

Windows Defender Exploit Guard has been available since Microsoft Windows 10 version 1709, and this event category will forward exploit mitigations being applied. Audit mode events can also be forwarded by enabling the supplied audit subscription.

Windows Defender Exploit Protection, which superseded EMET and is a component of Windows Defender Exploit Guard, will still run if third-party antivirus software is used. Exploit Protection is enabled by default and can be configured as required[14].

Events from the Windows Defender Exploit Guard components, Attack Surface Reduction, Network Protection and Controlled Folder Access require Windows Defender Antivirus's real-time antivirus scanning engine to be enabled[15].

Windows Error Reporting

This event category will forward application crashes and it does not require any change to Group Policy settings.

Code integrity

This event category will forward code integrity violations, and the following Group Policy settings will increase integrity logging. Recorded events include unsigned or untrusted drivers and protected processes attempting to load untrusted code.

When Device Guard is configured, events will be generated for code integrity violations against a defined list of trusted executable hashes and signatures. Audit mode events can also be forwarded by the supplied subscription. For further information, see Microsoft's deployment guide for Device Guard[16].

[12] https://insights.sei.cmu.edu/cert/2016/11/windows-10-cannot-protect-insecure-applications-like-emet-can.html

[13] https://www.cyber.gov.au/publications

[14] https://docs.microsoft.com/en-au/windows/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard

[15] https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-antivirus/windows-defender-antivirus-in-windows-10

[16] https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control-deployment-guide

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

File shares

The following Group Policy settings can be implemented to record events for file share creation, modification and access.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit Detailed File Share *(Enabling this setting is not recommended due to the high noise level)*	Not Configured
Audit File Share	Success and Failure

Scheduled tasks

The following Group Policy setting can be implemented to record events associated with scheduled tasks being registered, modified or disabled. The subscription will not forward common task modification events.

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

Windows Management Instrumentation auditing

Windows Management Instrumentation (WMI) auditing, like file and registry auditing, is native to Windows and provides visibility of WMI activity on a Windows host. The following Group Policy settings can be implemented to record events from sensitive WMI paths including local and remote activity.

Setting auditing records (System Access Control Lists (SACLs)) on WMI nodes can't be done directly through Group Policy settings. Instead, this can be achieved by using the supplied PowerShell script *events/wmi_auditing/wmi_auditing.ps1* and through the respective Group Policy setting below, which will configure it to run on host startup. This script can also be deployed through software deployment services such as System Centre Configuration Manager (SCCM).

Microsoft Windows 10 version 1607 and newer includes WMI persistence logging by default. This feature is almost identical to Sysmon's WMI logging.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\ Object Access	
Audit Other Object Access Events	Success and Failure
Computer Configuration\Policies\Windows Settings\Security Settings\Scripts (Startup/Shutdown)	
Startup	Click 'Show Files...' and add the file wmi_auditing.ps1. Under 'Powershell Scripts', click 'Add...' and select the wmi_auditing.ps1.

NTLM authentication

The following Group Policy settings will log events for outgoing NTLM authentication, which can be vulnerable to relay and brute force attacks. The events generated include information on the user, process responsible and target server. To reduce logging if NTLM is commonly used on the domain (e.g. by servers that require proxy authentication) you can specify servers to be exempt from auditing.

Although the NTLM protocol has weaknesses, disabling NTLM is not recommended on a typical network[17].

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options	
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Audit all
Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	*<NTLM servers as fully qualified domain names or NetBIOS names>*

Object access auditing

Microsoft Windows 10 and Microsoft Windows Server 2016 have a default SACL on the Local Security Authority Subsystem Service (LSASS) process[18]. With kernel object access auditing enabled by the respective Group Policy settings below, this will record read and write access to the memory of LSASS and is valuable in detecting malicious activity such as credential theft.

Sysmon contains the Process Access event, which can detect this activity on earlier versions of Windows.

Windows also has registry keys and file paths for a number of pre-existing SACLs which can be logged if the respective Group Policy settings below are enabled. These can be valuable, but some may cause a significant number of low-value events to be created. To reduce the amount of data to a manageable level, the subscription will not forward object access auditing from the System, Local Service and Network Service accounts.

[17] https://blogs.technet.microsoft.com/askds/2009/10/08/ntlm-blocking-and-you-application-analysis-and-auditing-methodologies-in-windows-7/

[18] https://docs.microsoft.com/en-au/windows/whats-new/whats-new-windows-10-version-1507-and-1511#bkmk-lsass

It is possible to define registry keys and file paths to be audited through Group Policy settings. The value of this is reduced as it can be difficult to define and maintain rules and it may introduce security flaws by defining incorrect permissions. Given these potential issues, the Sysmon file creation and registry auditing features are preferred.

The following Group Policy settings can be implemented to record auditing policy changes, kernel object auditing and optionally file system and registry auditing.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit File System *(Optional setting)*	Success and Failure
Audit Kernel Object	Success and Failure
Audit Registry *(Optional setting)*	Success and Failure

PowerShell logging

This event category will forward PowerShell engine start events, and with the following Group Policy settings implemented it will forward detailed logging of PowerShell scripts and interactive access. It may produce an excessive level of noise if large PowerShell scripts are used frequently within the environment and it is recommended that testing is conducted before it is deployed across the enterprise. For information on securing and logging using PowerShell, see the ***Securing PowerShell in the Enterprise*** publication[19].

The *Turn on PowerShell Script Block Logging* Group Policy setting requires PowerShell version 5.0 or above to be installed. A known bypass for this feature is to downgrade to an older version of PowerShell. Organisations are recommended to uninstall or restrict access to older versions of PowerShell where possible.

The following Group Policy settings can be implemented to enable the PowerShell *Script Block Tracing* feature in PowerShell version 5 or above. If the Group Policy settings are not visible, this requires the Group Policy administrative templates be updated. Alternatively, organisations can follow the registry method contained in Appendix C of the ***Securing PowerShell in the Enterprise*** publication[20].

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on Module Logging *(Enable only if versions prior to PowerShell 5 are installed on the network)*	Enabled Module Names: *
Turn on PowerShell Script Block Logging	Enabled

[19] https://www.cyber.gov.au/publications/securing-powershell-in-the-enterprise

[20] https://www.cyber.gov.au/publications/securing-powershell-in-the-enterprise

Event forwarding

Windows has the native ability, known as Windows Event Forwarding (WEF), to forward events from Windows hosts on the network to a log collection server. WEF can operate either via a push method or a pull method. This document uses Microsoft's recommended push method[21] of sending events to the log collection server. Subscriptions are added to determine which events are to be transferred, the source hosts and how frequently they are transferred. From the log collection server, events may be forwarded to a secure centralised logging capability such as a Security Information and Event Management (SIEM) system. This will enable centralised detection, correlation and discovery of cyber security incidents.

This document addresses the most common deployment scenarios; but there are many ways to achieve a similar result. These instructions primarily use the Windows Event user interface, but it is possible to achieve a similar outcome using the *wevtutil* and *wecutil* command-line utilities.

To implement event forwarding, the following is required:

- a dedicated event collection server joined to the domain running Microsoft Windows Server
- either a secure centralised logging facility where events can be forwarded for analysis or adequate disk space available to the collection server for archival and backup purposes.

Scalability

The instructions provided in this document are for a Windows domain with one log collection server. The Microsoft ***Use Windows Event Forwarding to help with intrusion detection*** article[22] mentions that, as a general rule, a log collection server on commodity hardware should be limited to 10,000 Windows hosts and below a total of 10,000 events per second.

To scale to multiple collection servers, the Group Policy settings can be modified to direct groups of Windows hosts to their closest available log collection server. These configurations need to consider the location of the collection server and bandwidth available from Windows hosts across Wide Area Network (WAN) links or remote access connections when forwarding event logs.

Client configuration

The event forwarding client configuration adjusts the Windows Remote Management (WinRM) configuration, which Windows Event Forwarding relies upon, and specifies the log collection server. The following Group Policy settings should be defined in a separate GPO, with the scope set for all Windows hosts on the domain. In the case of multiple collection servers, GPOs need to be defined to direct the Windows hosts to their respective log collection server (Subscription Manager).

To permit event log files to be read by the forwarding service the *Event Log Readers* group needs to be modified. This configuration does not take effect until the Windows Event Collector service is restarted. To restart the service, the Windows Event Collector service type needs to be set to start in a separate process, and then the service needs to be restarted. This can be achieved by running the below command on each Windows host.

```
sc config wecsvc type=own && sc stop wecsvc && sc start wecsvc
```

[21] https://docs.microsoft.com/en-au/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

[22] https://docs.microsoft.com/en-au/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection

Alternatively, restarting each Windows host will achieve the same result. Failure to do either of these will result in the Security and Sysmon logs not being forwarded and error events will be generated (i.e. Event ID 102 from the log *Microsoft-Windows-Forwarding/Operational*).

Forwarding will use global proxy settings on clients if enabled. The log collection server may need to be added to the proxy exclusion list unless this is required.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client	
Disallow Digest authentication	Enabled
Computer Configuration\Policies\Administrative Templates\Windows Components\Event Forwarding	
Configure target Subscription Manager	Enabled SubscriptionManagers: *<server=logserver.yourdomain:5985>*
Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups	
	Add Group 'Event Log Readers' with the NETWORK SERVICE.

Server configuration

The log collection server requires the Windows Event Collector service to be running, WinRM to be setup as a server and the firewall to be configured appropriately. This is implemented by the following Group Policy settings which should be applied to the log collection servers as a separate GPO.

Group Policy Setting	Recommendation Option
Computer Configuration\Policies\Windows Settings\Security Settings\System Services	
Windows Remote Management (WS-Management)	Startup Mode: Automatic
Windows Event Collector	Startup Mode: Automatic
Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Inbound Rules	
Windows Remote Management (HTTP-In)	(Right-Click) 'New Rule…', select 'Predefined' then 'Windows Remote Management'. Click 'Next' and ensure the rules are going to be created. Click 'Next' and ensure the option 'Allow the connection' is set. Click 'Finish'.

Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service	
Allow remote server management through WinRM	Enabled IPv4 Filter: * *(or the private IP address range(s) for the network)*
Specify channel binding token hardening level	Enabled Hardening Level: Strict
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Shell	
Allow Remote Shell Access	Disabled
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment	
Access this computer from the network	If this setting has been modified from its default and does not include the Everyone or Authenticated Users group, ensure that at a minimum the Domain Computers and Domain Controllers are included.

Setting forwarded log size

To set forwarding log sizes:

- open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator
- select the Forwarded Events log and click 'Properties'
- set maximum log size to around 2 GB (2097152 KB)
- click 'OK'.

Adding subscriptions

To collect each event category, a relevant subscription needs to be added and enabled. The subscriptions contain query filters that forward events of potential interest. In some cases query filters are based on full paths and these would need to be modified if non-standard paths or drives are used.

To add subscriptions:

- logon to the log collection server as an Administrator
- copy the supplied *events* folder to the log collection server
- open PowerShell (*powershell.exe*)
- navigate to the *events* directory in the PowerShell console
- run *./add_subscriptions.ps1*. If an error is returned due to the PowerShell script execution policy, run *powershell -exec bypass ./add_subscriptions.ps1*. Note, errors may be returned because no source hosts or computer groups have been defined, this will be resolved by completing the following instructions.

The default configuration should now be loaded and computer groups need to be added to enable the subscriptions on the domain. Typically, this would include both the *Domain Computers* and *Domain Controllers* groups. This can be customised to include or exclude specific computers or groups.

To subscribe the *Domain Computers* and *Domain Controllers* groups to all subscriptions:

- logon to the log collection server as an Administrator
- open PowerShell (*powershell.exe*)
- navigate to the *events* directory in the PowerShell console
- run *./set_subscriptions_source.ps1*. If an error is returned due to the PowerShell scriptexecution policy, run *powershell -exec bypass ./set_subscriptions_source.ps1*.

If desired, the source hosts or computer groups for a specific subscription can be edited:

- logon to the log collection server as an Administrator
- open Event Viewer (*eventvwr.msc*)
- click ‘Subscriptions’, which will list all the added subscriptions, and select a desired subscription. Note, an initial error may be returned as the ‘Windows Event Collector’ service needs to be configured and running, although the service should be running with the above group policy configuration. Click ‘Yes’
- click ‘Properties’
- click ‘Select Computer Groups’
- add the desired computer groups or individual hosts using ‘Add Domain Computers’. It is also possible to exclude hosts or computer groups as desired. When finished click ‘OK’
- click ‘OK’ and ‘OK’.

To speed up the testing of subscriptions changes you can force hosts to perform a Group Policy update by running *gpupdate /force* on Windows hosts that are forwarding events. Subscriptions can also be viewed and edited using the Event Viewer (*eventvwr.msc*) interface. This includes enabling or disabling subscriptions, or updating filters.

By default, the subscriptions are enabled to read existing events in the log archive. This may cause a higher than average number of events to be forwarded and place additional load on the network where Windows hosts are forwarding events for the first time. The *ReadExistingEvents* subscription setting can be modified for each subscription to enable or disable the forwarding of previous events by using the command-line utility *wecutil*.

Verification and debugging

To verify that event logs are being forwarded to the log collection server:

- logon to the log collection server as an Administrator
- open Event Viewer (*eventvwr.msc*)
- click ‘Windows Logs’
- click ‘Forwarded Events’.

Alternatively you can view which hosts are sending data per subscription:

- logon to the log collection server as an Administrator
- open Event Viewer (*eventvwr.msc*)
- click ‘Subscriptions’
- select a subscription and click ‘Runtime Status’.

To diagnose potential errors, the event collection server has the EventCollector log (*Microsoft-Windows-EventCollector/Operational*) and the clients have the Eventlog-ForwardingPlugin log (*Microsoft-Windows-Forwarding/Operational*). These logs are forwarded where possible and can also be accessed using the Event Viewer (*eventvwr.msc*) and navigating to *Applications and ServicesLogs/Microsoft/Windows*.

Archiving

Events should be archived if they are not going to be forwarded to a secure centralised logging facility. Regular backups of the event collection server's archived logs can help mitigate the risk of data loss.

To ensure all forwarded events are archived on the event collection server:

- logon to the log collection server as an Administrator
- open Event Viewer (*eventvwr.msc*)
- select the Forwarded Events log and click 'Properties'
- click 'Archive the log when full, do not overwrite events'
- click 'OK'.

An alternative log path may optionally be set. This is useful in situations where log files are being stored on a separate high capacity drive. The path must first have an access control list defined on the folder to match the permissions on the default Windows event log path, as listed below:

- EventLog: Traverse folder, List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Delete subfolders and files, Read permissions
- System: Full control
- Administrators: Full control.

To set the Forwarded Events log to use the alternative path:

- logon to the log collection server as an Administrator
- open Event Viewer (*eventvwr.msc*)
- select the Forwarded Events log and click 'Properties'
- Set the *Log path* to the alternative path (e.g. *D:\Logs\ForwardedEvents.evtx*) and click 'OK'.

Organisations must appropriately secure their Windows event log archives to ensure only authorised users and services are able to access these files. Unauthorised access to these files could provide an adversary with sensitive information or an opportunity to remove or tamper with event logs.

When the ForwardedEvents log is full, archive files will be created. This should occur when they are approximately 2 GB. By default, this will be in *%SystemRoot%\System32\winevt\Logs* and will have a format similar to *Archive-ForwardedEvents-2016-05-18-05-23-46-723*.

Over time archive logs will be created and not overwritten or deleted. Adequate disk space needs to be allocated to the server and disk usage should be monitored. It is recommended that a procedure is created to backup or move archived logs on a regular basis, or when the disk is reaching capacity.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents.

The ***Implementing Application Whitelisting*** publication contains guidance on whitelisting implementation and logging recommendations. It can be found at https://www.cyber.gov.au/publications/implementing-application-whitelisting.

The ***Securing PowerShell in the Enterprise*** publication contains additional information on logging and securing PowerShell. It can be found at https://www.cyber.gov.au/publications/securing-powershell-in-the-enterprise.

The ***Hardening Microsoft Windows 10 version 1709 Workstations***, ***Hardening Microsoft Windows 8.1 Update Workstations*** and ***Hardening Microsoft Windows 7 SP1 Workstations*** publications include hardening advice for logging. These publications can be found at https://www.cyber.gov.au/publications.

External references and further reading about Windows event logging and forwarding can be found at:

- ***Spotting the Adversary with Windows Event Log Monitoring (version 2)***, https://apps.nsa.gov/iaarchive/library/reports/spotting-the-adversary-with-windows-event-log-monitoring.cfm.
- National Security Agency guidance for Windows Event Forwarding and Windows Event Log monitoring, hhttps://github.com/nsacyber/Event-Forwarding-Guidance.
- ***Advanced security audit policy settings***, https://docs.microsoft.com/en-au/windows/security/threat-protection/auditing/advanced-security-audit-policy-settings.
- ***Use Windows Event Forwarding to help with intrusion detection***, https://docs.microsoft.com/en-au/windows/security/threat-protection/use-windows-event-forwarding-to-assist-in-intrusion-detection.
- ***Sysmon v9.0***, https://docs.microsoft.com/en-au/sysinternals/downloads/sysmon.
- ***Tracking Hackers on Your Network with Sysinternals Sysmon***, https://www.rsaconference.com/writable/presentations/file_upload/hta-w05-tracking_hackers_on_your_network_with_sysinternals_sysmon.pdf.
- ***How to Go From Responding to Hunting with Sysinternals Sysmon***, https://www.rsaconference.com/writable/presentations/file_upload/hta-t09-how-to-go-from-responding-to-hunting-with-sysinternals-sysmon.pdf.
- ***Monitoring what matters – Windows Event Forwarding for everyone (even if you already have a SIEM.)***, https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/.
- ***DIY Client Monitoring – Setting up Tiered Event Forwarding***, https://blogs.msdn.microsoft.com/canberrapfe/2015/09/21/diy-client-monitoring-setting-up-tiered-event-forwarding/.
- ***What's new in Windows 10, versions 1507 and 1511***, https://docs.microsoft.com/en-au/windows/whats-new/whats-new-windows-10-version-1507-and-1511#security-auditing.
- ***Recommended settings for event log sizes in Windows***, https://support.microsoft.com/en-au/help/957662/recommended-settings-for-event-log-sizes-in-windows.
- ***Advanced Security Auditing FAQ***, https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff182311(v=ws.10).
- ***Greater Visibility Through PowerShell Logging***, https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html.
- ***Microsoft Security Advisory 3004375***, https://docs.microsoft.com/en-au/security-updates/SecurityAdvisories/2015/3004375.

- ***Microsoft security advisory: Update to improve Windows command-line auditing: February 10, 2015***, https://support.microsoft.com/en-au/help/3004375/microsoft-security-advisory-update-to-improve-windows-command-line-aud.
- ***Detecting Security Incidents Using Windows Workstation Event Logs***, https://www.sans.org/reading-room/whitepapers/logging/detecting-security-incidents-windows-workstation-event-logs-34262.
- ***Windows Logon Forensics***, https://www.sans.org/reading-room/whitepapers/forensics/windows-logon-forensics-34132.
- ***Detecting Advanced Threats with Sysmon, WEF and ElasticSearch***, https://www.root9b.com/sites/default/files/whitepapers/R9B_blog_005_whitepaper_01.pdf.
- ***Centralizing Windows Events with Event Forwarding***, http://www.aspirantinfotech.com/sg/download/avecto/brochure/EventCentralization.pdf.
- ***Attacks on Software Publishing Infrastructure and Windows Detection Capabilities***, https://www.first.org/resources/papers/conf2016/FIRST-2016-101.pdf.
- ***Detecting Lateral Movement through Tracking Windows Event Logs***, https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf.

Contact details

Organisations or individuals with questions regarding this advice can email asd.assist@defence.gov.au or call 1300 CYBER1 (1300 292 371).