Australian Government
Australian Cyber Security Centre

ASD
AUSTRALIAN SIGNALS DIRECTORATE

Technical Guidance For Windows Event Logging

JULY 2017

CONTENTS

Introduction

1. A common theme identified by the Australian Cyber Security Centre (ACSC) while performing investigations on networks, is that organisations have insufficient visibility of activity occurring on their workstations and servers. Good visibility of what is happening on an organisation's Microsoft Windows hosts 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 incidents.
2. This document has been developed by the Australian Signals Directorate (ASD) 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—including targeted cyber intrusions - by providing an ideal balance between the collection of important events and managing data volumes. This advice is also designed to complement existing host-based intrusion detection and prevention systems.
3. This document is intended for information technology and information security professionals.

Document overview

4. This document details:
    a. guidance to increase the retention of local event logs;
    b. guidance for the types of events which can be generated and an assessment of their relative value;
    c. guidance for forwarding event logs to a central location to allow for analysis and correlation of activity, and for a longer enterprise-wide retention period; and
    d. the specific Group Policy settings required to apply the recommended guidance with related implementation notes.
5. This document does not contain detailed information about analysing the collected event logs.

Why use Windows event logging?

6. Good visibility of host-based events is vital as adversaries increase their use of legitimate or native tools, capabilities and existing credentials to achieve their goals, rather than relying on the propagation of malware throughout a network.

7. Windows event logs provide an invaluable source of evidence of activity taking place on Microsoft Windows hosts. They can enable the detection and discovery of malicious activity and support incident response for cyber security incidents.

8. Event logging provides an in-built, standardised way of recording significant activity that has taken place on Microsoft Windows hosts. This information can then be centralised into a single source that can be interrogated for signs of malicious activity and used to correlate events across an enterprise's entire Microsoft Windows environment.

ACSC's Windows event logging repository

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

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

Considerations

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

10. To enable accurate correlation of events, accurate and consistent time stamps must be used throughout the network. ASD recommends that organisations ensure all devices (i.e. Windows hosts and network equipment) in their environment are configured to use an accurate time source.

11. As detailed in ASD's *Strategies to Mitigate Targeted Cyber Intrusions*[2], the recommended log retention time is at least 18 months. Some organisations will have a regulatory requirement to retain logs for a longer period, and organisations are encouraged to seek relevant advice.

12. To assist with the management of ASD's guidance, the Group Policy settings in this document should be placed in a separate Group Policy Object (GPO) with the scope set for all Microsoft Windows hosts on the domain. All changes made to systems as a result of ASD's guidance 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.

13. The recommended Group Policy settings in this document use the 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 the advanced audit policies.

14. Sysmon[4] (System Monitor), a tool published by Microsoft, provides greater visibility of system activity on a Microsoft Windows host than standard Window's logging. ASD recommends the use of this tool throughout an organisation's Microsoft Windows environment as part of this guidance. For more information, see Sysmon on page 10.

[2] https://www.asd.gov.au/infosec/mitigationstrategies.htm

[3] https://technet.microsoft.com/en-us/library/ff182311(v=ws.10).aspx#BKMK_3

[4] https://technet.microsoft.com/en-au/sysinternals/sysmon

Event log retention

15. 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 file size of 20 MB. The Application and System log file 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 event log file sizes are acceptable in environments where local storage is limited (e.g. virtual infrastructure environments), provided logs are being forwarded; see Event Forwarding on page 15.

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

Group Policy	Recommended Value
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

Event configuration

17. The default Windows settings provide only a subset of the desired logging events that assist in detecting and investigating malicious activity.

18. This section covers the event categories that will significantly enhance technical analysis. Each event category can be deployed independently and categories in the table on the following pages 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.

19. Each of the event categories 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. For more information and the guidance to configure the subscriptions, see Event Forwarding on page 15.

Event Category	Description	Why	Value	Noise	Implementation Notes
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 forwarding errors	Forwards errors related to event forwarding.	Verifies Microsoft Windows hosts on the network are forwarding logs as expected.	High	Low	None
Event log cleared	Records when the Windows event logs have been cleared.	Detects attempts by an adversary to delete 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
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. Detect process injection and some forms of credential and password hash access.	High	High	If Sysmon cannot be deployed use Process tracking instead.
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 (EMET)	Records EMET events relating to mitigations that have been applied.	Detects exploitation attempts that have been successfully blocked by EMET.	Medium	Low	Only beneficial if EMET is installed and configured.
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 Error Reporting	Records when an application crashes.	Detects exploitation attempts and unstable applications, which may indicate malicious activity.	Medium	Low	None

Event Category	Description	Why	Value	Noise	Implementation Notes
File shares	Records creation, modification and access of file shares.	Detects access and modification of file shares. This includes lateral movement and access of file shares 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 (WMI) auditing	Produces audit records for local and remote 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
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.	Medium	High	Should only be implemented if Sysmon cannot be deployed.
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
Windows PowerShell	Records PowerShell activity including interactive and script usage.	Detects PowerShell being used by an adversary.	Low	Medium	None

Account lockout

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

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon/Logoff	
Audit Account Lockout	Success

Account modifications

21. 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	Recommended Value
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 forwarding errors

22. This event category will forward errors and warnings resulting from problems with Windows Event Forwarding. These logs can detect errors related to incorrectly formed subscriptions and can assist with debugging.

Event log cleared

23. This event category will forward all events related to event logs being cleared. The event does not require any change to the Group Policy settings.

Account logon

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

25. 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	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Logon/Logoff	
Audit Logon	Success and Failure
Audit Logoff	Success
Audit Group Membership	Success (only available on Microsoft Windows 10 and Microsoft Windows Server 2016)
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success and Failure

Sysmon

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

27. 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. See Further information on page 20 for links containing more detailed documentation on Sysmon, including configuration and command-line options.

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

29. Guidance on the creation of an installation file (MSI) that may simplify the deployment 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. The end-user license agreement must be accepted beforehand.

    - Installed using sysmon -accepteula -i or sysmon -accepteula -i sysmon_config.xml
    - Configured using sysmon -c sysmon_config.xml
    - Uninstalled using sysmon -u

AppLocker

33. This event category will forward audit or deny events from AppLocker. AppLocker must be configured in either auditing or enforcement mode for events to be generated. See the *Application whitelisting* section of the ASD's Windows Hardening Guides[5] and ASD's *Implementing Application Whitelisting* publication[6] for recommendations on the implementation of application whitelisting.

34. 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.

[5] https://www.asd.gov.au/publications/index.htm

[6] https://asd.gov.au/publications/protect/application_whitelisting.htm

EMET

35. EMET is a tool developed by Microsoft to enable additional protection against software exploitation. Microsoft announced that it will cease support for EMET from mid-2018 as many of the controls provided by EMET have already been moved into the core of Microsoft Windows 10. EMET still provides significant security benefits by applying the application-specific mitigation measures to third-party applications[7].

36. This 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 ASD's Windows Hardening Guides[5].

Services

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

Windows Error Reporting

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

Scheduled tasks

39. The following Group Policy settings 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	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit Other Object Access Events	Success and Failure

File shares

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

Group Policy	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit Detailed File Share	Not Configured (enabling this is not recommended given the high noise level)
Audit File Share	Success and Failure

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

WMI auditing

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

42. Setting auditing records - System Access Control Lists (SACLs) - on WMI nodes cannot be done directly through Group Policy. 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 SCCM.

Group Policy	Recommended Value
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*.

Process tracking

43. The following Group Policy settings can be implemented to record process creation and termination events. ASD recommends organisations collect this information through Sysmon; if Sysmon cannot be used, process tracking events can be collected through this native Microsoft Windows logging.

44. 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, an update is available with security updates released in 2015. For more details see *Microsoft Security Advisory 3004375*[8] and *Update to improve Windows command-line auditing*[9].

Group Policy	Recommended Value
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

[8] https://technet.microsoft.com/en-us/library/security/3004375.aspx

[9] https://support.microsoft.com/en-us/kb/3004375

Object access auditing

45. Microsoft Windows 10 and Microsoft Windows Server 2016 have a default SACL on the Local Security Authority Subsystem Service (LSASS) process[10]. With kernel object access auditing enabled by the respective Group Policy setting below, this will record read and write access to the memory of LSASS and is valuable in detecting malicious activity like credential theft. Sysmon 4.10 and above contain the Process Access event, which can detect this activity on earlier versions of Microsoft Windows.

46. Microsoft Windows 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.

47. It is possible to define registry keys and file paths to be audited through Group Policy. 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.

48. 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	Recommended Value
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Object Access	
Audit File System	Success and Failure (Optional)
Audit Kernel Object	Success and Failure
Audit Registry	Success and Failure (Optional)
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Policy Change	
Audit Policy Change	Success and Failure

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

Windows PowerShell logging

49. The subscription will forward PowerShell engine start events and with the following Group Policy settings implemented, it will forward detailed logging of Windows 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. Refer to ASD's *Securing PowerShell in the Enterprise* publication[11] for more information about securing and logging Windows PowerShell.

50. The Microsoft Windows PowerShell *Script Block Tracing* feature requires PowerShell version 5 or above to be installed. A known bypass for this logging is to downgrade to an older version of PowerShell. ASD recommends that older versions of PowerShell be uninstalled or access restricted where possible.

51. The *Script Block Tracing* Group Policy setting may not be visible in the Group Policy editor. If it is not, this requires the Group Policy administrative templates be updated, or that organisations follow the registry method contained in Appendix C of ASD's *Securing PowerShell in the Enterprise* publication[11].

Group Policy	Recommended Value
Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell	
Turn on Module Logging	Enabled only if versions prior to PowerShell 5 are installed on the network. Enabled Module Names: *
Turn on PowerShell Script Block Logging	Enabled

[11] https://asd.gov.au/publications/protect/securing-powershell.htm

Event forwarding

52. Microsoft Windows has the native ability to forward events from hosts on the network to a log collection server, known as Windows Event Forwarding (WEF). WEF can operate in both a push and pull mode, and ASD's guidance uses Microsoft's recommended push method[12] 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.

53. This guidance 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.

54. To implement event forwarding the following is required:

    a. a dedicated event collection server, running Microsoft Windows Server and joined to the domain; and

    b. either a secure centralised logging facility where events can be forwarded for analysis; or

    c. adequate disk space available to the collection server for archival and backup purposes.

Scalability

55. The instructions provided in this document are for a Microsoft Windows domain with one log collection server. The Microsoft TechNet article *Use Windows Event Forwarding to help with intrusion detection*[13] mentions that, as a general rule, a log collection server on commodity hardware should be limited to 10,000 Microsoft Windows hosts and below a total of 10,000 events/second.

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

[12] https://docs.microsoft.com/en-us/windows/threat-protection/use-windows-event-forwarding-to-assist-in-instrusion-detection#is-wef-push-or-pull

[13] https://docs.microsoft.com/en-us/windows/threat-protection/use-windows-event-forwarding-to-assist-in-instrusion-detection

Client configuration

57. 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 Microsoft Windows hosts on the domain. In the case of multiple collection servers, GPOs need to be defined to direct the Microsoft Windows hosts to their respective log collection server (Subscription Manager).

58. 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 process is restarted. To restart the service process, 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 Microsoft Windows host.

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

    Alternatively, restarting each Microsoft 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 (Event ID 102 from the log *Microsoft-Windows-Forwarding/Operational*).

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

Group Policy	Recommended Value
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	Click **Enabled** – Click **Show…** under SubscriptionManagers and add the logging server in the following notation: server=nameofyourlogserver.yourdomain.gov.au:5985
Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups	
Add Group "Event Log Readers", with a member NETWORK SERVICE.	

Server configuration

60. 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 and these should be applied to the log collection servers as a separate GPO.

Group Policy	Recommended Value
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 this 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

Setting forwarded log size

61. To set forwarding log sizes:
    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator
    b. select the **Forwarded Events** log and click **Properties**
    c. set maximum log size to around 2 GB (2097152 KB)
    d. click **OK**.

Adding subscriptions

62. 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.

63. To add subscriptions:
    a. logon to the log collection server as an Administrator
    b. copy the supplied *events* folder to the log collection server
    c. open PowerShell (*powershell.exe*)

d. navigate to the *events* directory in the PowerShell console

e. 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.

64. 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.

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

    a. logon to the log collection server as an Administrator

    b. open PowerShell (*powershell.exe*)

    c. navigate to the *events* directory (as detailed above) in the PowerShell console

    d. run *./*set_subscriptions_source.ps1. If an error is returned due to the PowerShell script execution policy, run *powershell -exec bypass ./*set_subscriptions_source.ps1*.*

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

    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator

    b. 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**

    c. click **Properties**

    d. click **Select Computer Groups**

    e. 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**

    f. click **OK** and **OK**.

67. Source hosts will start forwarding events based on the updated subscriptions. To speed up the testing of subscriptions changes you can force hosts to perform a group policy update by running *gpupdate /force* on hosts that are forwarding events.

68. Subscriptions can be viewed and edited using the same Event Viewer interface (*eventvwr.msc*); this includes enabling or disabling subscriptions, or updating filters.

69. 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 Microsoft 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

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

    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator

    b. click **Windows Logs**

    c. click **Forwarded Events**.

71. Alternatively you can view which hosts are sending data per subscription:
    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator
    b. click **Subscriptions**
    c. select a subscription and click **Runtime Status**.
72. 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 and navigating to Applications and Services Logs/Microsoft/Windows.

Archiving

73. 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.
74. To ensure all forwarded events are archived on the event collection server:
    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator
    b. select the **Forwarded Events** log and click **Properties**
    c. click **Archive the log when full, do not overwrite events**
    d. click **OK**.
75. 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:
    a. 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
    b. System - Full control
    c. Administrators - Full control.
76. To set the forwarded events log to use the alternative path:
    a. open Event Viewer (*eventvwr.msc*) on the log collection server as an Administrator
    b. select the **Forwarded Events** log and click **Properties**
    c. Set the *Log path* to the alternative path - e.g. *D:\Logs\ForwardedEvents.evtx* and click **OK**.
77. 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.
78. 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 the *%SYSTEMROOT%\System32\winevt\Logs* and they will have a format similar to *Archive-ForwardedEvents-2016-05-18-05-23-46-723*.
79. 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

80. The *Australian Government Information Security Manual* (ISM), available at https://www.asd.gov.au/infosec/ism/, assists in the protection of information that is processed, stored or communicated by Australian government systems. The following ISM section can be consulted in relation to advice in this publication:

    a. the *Event Logging and Auditing* section of the *Access Control* chapter

    b. the *Managing Cyber Security Incidents* section of the *Cyber Security Incidents* chapter.

81. ASD's *Strategies to Mitigate Cyber Security Incidents* publication complements the advice in the ISM, and is available at https://www.asd.gov.au/infosec/mitigationstrategies.htm.

82. ASD's *Cyber security incidents: are you ready?* publication contains additional recommendations for event logging to enable an investigation into a security incident. It can be found at https://www.asd.gov.au/publications/protect/cyber-security-incidents-are-you-ready.htm.

83. ASD's *Implementing Application Whitelisting* publication contains guidance on whitelisting implementation and logging recommendations. It can be found at https://www.asd.gov.au/publications/protect/application_whitelisting.htm.

84. ASD's *Securing PowerShell in the Enterprise* publication contains additional information on logging and securing Windows PowerShell. It can be found at https://www.asd.gov.au/publications/protect/securing-powershell.htm.

85. ASD's *Hardening Microsoft Windows 10 Workstations*, *Hardening Microsoft Windows 8.1 Update Workstations* and *Hardening Microsoft Windows 7 SP1 Workstations* publications include hardening advice for logging under the sections *Audit event management* and *Centralised audit event logging*. These publications can be found at https://asd.gov.au/publications/index.htm.

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

    a. *Spotting the Adversary with Windows Event Log Monitoring*, https://www.iad.gov/iad/library/ia-guidance/security-configuration/applications/spotting-the-adversary-with-windows-event-log-monitoring.cfm.

    b. *NSA Information Assurance guidance for Windows Event Forwarding and Windows Event Log monitoring*, https://github.com/iadgov/Event-Forwarding-Guidance.

    c. *Advanced security audit policy settings (Windows 10)*, https://technet.microsoft.com/en-us/itpro/windows/keep-secure/advanced-security-audit-policy-settings.

    d. *Use Windows Event Forwarding to help with intrusion detection*, https://docs.microsoft.com/en-us/windows/threat-protection/use-windows-event-forwarding-to-assist-in-instrusion-detection.

    e. *Sysmon*, https://technet.microsoft.com/en-au/sysinternals/sysmon.

    f. *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.

    g. *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.

    h. *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/.

i. *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/.

j. *What's new in security auditing?*, https://docs.microsoft.com/en-us/windows/whats-new/whats-new-windows-10-version-1507-and-1511#security-auditing.

k. *Recommended settings for event log sizes in Windows*, https://support.microsoft.com/en-au/help/957662/recommended-settings-for-event-log-sizes-in-windows.

l. *Advanced Security Auditing FAQ*, https://technet.microsoft.com/en-us/library/ff182311(v=ws.10).aspx.

m. *Greater Visibility Through PowerShell Logging*, https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html.

n. *Microsoft Security Advisory 3004375,* https://technet.microsoft.com/en-us/library/security/3004375.aspx.

o. *Update to improve Windows command-line auditing,* https://support.microsoft.com/en-us/kb/3004375.

p. *Detecting Security Incidents Using Windows Workstation Event Logs*, https://www.sans.org/reading-room/whitepapers/logging/detecting-security-incidents-windows-workstation-event-logs-34262.

q. *Windows Logon Forensics*, https://www.sans.org/reading-room/whitepapers/forensics/windows-logon-forensics-34132.

r. *Detecting Advanced Threats with Sysmon, WEF and ElasticSearch,* https://www.root9b.com/sites/default/files/whitepapers/R9B_blog_005_whitepaper_01.pdf.

s. *Centralizing Windows Events with Event Forwarding*, http://www.aspirantinfotech.com/sg/download/avecto/brochure/EventCentralization.pdf.

t. *Attacks on Software Publishing Infrastructure and Windows Detection Capabilities*, https://www.first.org/resources/papers/conf2016/FIRST-2016-101.pdf.

u. *Detecting Lateral Movement through Tracking Windows Event Logs*, https://www.jpcert.or.jp/english/pub/sr/20170612ac-ir_research_en.pdf.

Contact details

87. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

88. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.