Federal Office
for Information Security

Configuration Recommendations for Windows 10 Logging

Version: 1.0

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Table of Contents

1 Introduction

1.1 Executive Summary

This document outlines the result of work package 10 of the project “SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10” (orig., ger.). This project is being conducted by the company ERNW Enno Rey Netzwerke GmbH on behalf of the German Federal Office for Information Security (orig. ger.: Bundesamt für Sicherheit in der Informationstechnik (BSI)).

The objective of this work package is to create a comprehensive logging concept for the components of Windows 10. As required by the Federal Office for Information Security, Windows 10 LTSC 2019, 64 Bit in German language is the focus of this document.

2 General Concepts

Building on the results obtained in the preceding work packages a configuration recommendation for logging on Windows 10 has been created which allows to detect attempted attacks and unwanted actions of Windows functionalities that threaten the confidentiality, availability or integrity of the IT system. The recommendation is aimed at advanced users and administrators and is suitable for directly implementing the configuration settings of the operating system.

2.1 Scope

This document and the configuration recommendations it contains are valid for the Microsoft Windows 10 Long-Term Servicing Channel (LTSC) operating system, version 2019. The Semi-Annual Channel (SAC) version equivalent to this is Windows 10, version 1809. It is functionally identical to Windows 10 LTSC version 2019 both in terms of the kernel and components which are included in both versions. Because LTSC versions are designed to maintain a consistent feature set and stability, Microsoft does not provide post-release feature upgrades and components that could be added with new functionality have been removed. The most important missing components are the Edge browser, the virtual assistant Cortana as well as all preinstalled Universal Windows Apps (“Store Apps”) including the Microsoft Store.

The configuration recommendations for logging described in the following are based on a standard use case scenario, such as using a Windows 10 system for office work. However, the recommendations may also be used as a basis for defining logging configurations for more specific use cases, such as a Windows 10 system used for administrative tasks.

2.2 Scope Conditions

The configuration recommendations described in the following are based on the analysis conducted during the project, on security best practices, as well as on expertise by ERNW. All recommendations are both compared against the Center for Internet Security (CIS) Benchmark (cis_win10_1809, 2019) for Windows 10 Enterprise (Version 1809) as a globally known and widely adopted standard and the recommendations of the Security Baseline for Windows 10 1809 (ms_sec_bl_1809, 2021) by Microsoft. Deviations from the Security Baseline or the CIS Benchmark are explained and substantiated for the affected settings within this document. Where settings do not deviate, a reference is made to the relevant section in the CIS benchmark or to the Security Baseline to help in finding the setting inside the other publications.

While creating this document, decisions for specific configuration recommendations were led by the following basic principles for increasing system security:

- Collecting data relevant to the detection of known and widespread attack scenarios so that it can be used for an active monitoring to identify attempted and ongoing attacks
- Collecting data relevant for the analysis of known and widespread attack scenarios, so that it can be further evaluated in the course of forensic investigations.
- Collecting relevant data on configuration changes of security relevant objects and the function of security relevant components so that it can be used during a continuous monitoring of the security level of a system.
- Enforcing settings to prevent modifications by the user.
- Extending the default configuration to ensure the generation and storage of relevant logging data.
- Considering data privacy by identifying configurations that may lead to the disclosure of sensitive data in logging files.

For this document, the collection of logging data in order to monitor and ensure the operational reliability of a system was not considered. The concrete evaluation of the logged data as part of a monitoring solution is beyond the scope of this document, as well.

In addition, or alternatively, the configuration recommendations defined in this document can also be partially implemented by *Sysmon* (ms_sysmon, 2021) which allows for a very fine-grained configuration beyond the capabilities of built-in tools.

Hardening-related configuration recommendations can be found in the document “Configuration Recommendations for Hardening of Windows 10 Using Built-in Functionalities” (orig. ger.: “Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln”) of the SiSyPHuS project (work package 11).

The corresponding Group Policy objects for the recommendations regarding logging (work package 10) and hardening (work package 11) are provided as part of work package 12.

3 General Recommended Measures

The following sections describe general IT security recommendations that should be considered when logging events on a Windows 10 system. These measures are described only in general terms as not all of them can be implemented via technical configurations (respectively built-in Windows tools) or they are outside the scope of this document.

3.1 Time Synchronization

In an IT infrastructure that consists of multiple systems temporal correlation of logging data from different sources is essential for the detection of attacks as well as the reconstruction of security incidents during a forensic investigation.

If the system time of the involved systems is not synchronized, event occurrence times gathered from the logging data of different systems can deviate from each other, as there is no common basis for the generation of time stamps. Thus, a temporal correlation of this data would not be reasonably possible or would lead to false assumptions respectively, especially when the logging data is stored on a central logging server.

For this reason, the system time of all systems and applications involved in the logging procedure should be synchronized. If the involved systems are in different time zones, it is recommended to utilize UTC as a general time basis for all sources of logging data. For the purpose of logging data analyses, it is only required that all involved systems have a synchronized system time.

Time-synchronized networks can be achieved by utilizing time servers (e.g., NTP servers).

3.2 Central Collection of Logging Data

Security incidents often affect not only individual computer systems, but an entire IT infrastructure. If logging data is only kept locally on the systems on which the data is generated, it can only be correlated with great effort to detect attacks on the entire infrastructure or to reconstruct them during forensic investigations. Furthermore, an attacker that successfully compromised a system can manipulate the generated logging data to cover up their actions. For these reasons, the generated logging data from all systems in the environment should be collected and maintained in a central logging infrastructure.

Logging data should be transmitted to the central logging infrastructure via operating system mechanisms such as Windows Event Forwarding. However, it should be ensured that the data is transmitted in a manner that ensures the integrity and confidentiality of the data (e.g., through transport layer encryption).

The central logging infrastructure plays an essential role in the overall security of an IT infrastructure. A compromise or failure of the logging infrastructure could lead to attacks that can no longer be detected and tracked. For this reason, it should be secured accordingly:

- The logging infrastructure should consist of multiple distributed systems as part of a network of logging servers that are placed in a dedicated network segment to ensure availability, integrity, and reliability.
- The administration of the logging servers should be separated from the administration of the remaining IT infrastructure and should follow the requirements of proper IT administration for increased protection needs from the IT-Grundschutz Compendium (see (bsi_adm_erh_schb, 2021)).
- A concept for access control that regulates who can access which logging data should be designed and implemented to prevent unauthorized access. The permissions should be assigned as restrictively as possible. Furthermore, a software solution should be used to encrypt at least the data partition where the logging data is stored. In addition, the physical security of the logging servers should be ensured.

- The expected data volume depends on the number of systems, the usage patterns, and the logging configuration. To ensure that relevant logging events are not lost or overwritten, the capacity of the logging infrastructure should be designed to handle twice the expected volume of data and to store logging events in the data storage for twice the planned retention period.
- The network of logging servers should receive logging data of IT systems and applications in a timely manner. This is to ensure that event data that precedes a possible attack is transferred directly after the creation to a secure logging storage protected against tampering. In the example of Windows Event Forwarding, this is typically done by regular forwarding of event data by the source systems to the associated logging servers. This approach is especially suitable for an exhaustive collection of logging data. For systems that require increased protection, logging data should not be transferred to the servers on initiative of the end devices but should be collected on initiative of the logging servers on the end devices via, for example, a specific user account. This is to ensure, among other things, that the omission of forwarding logging data does not remain undetected. How this can be implemented using Windows Event Forwarding is described by Microsoft here: (ms_ev_coll, 2021).
- To prevent failure of the logging infrastructure and to ensure that no logging data is lost, the central logging infrastructure should be continuously monitored for failure states.
- To prevent the loss of stored logging data and to ensure the integrity of this data, it should be technically prevented that logging data can be deleted or modified in an unauthorized manner.

3.3 Handling of Sensitive Logging Data

Logging data can contain sensitive information and thus requires increased protection. This can be both sensitive user information and information potentially valuable to an attacker, such as passwords or information about the internal structure of the IT infrastructure. For this reason, logging data should only be transferred in encrypted form and it should be ensured that no unauthorized access is performed to stored logging data. In turn, all access to this data should be logged. Furthermore, a retention period should be defined for logging data after which it is deleted following a specified process. Logging data that contains individual-related data should only be stored pseudonymously in a central logging infrastructure. But for incident analysis it should be ensured that a reversal of the pseudonyms is possible within the retention period. In addition, when processing and storing logging data that (may) contain individual-related information, it should be verified which legal regulations and internal company policies may have to be taken into account.

4 Configuration Recommendations: System-wide Settings

The following sections contain configuration recommendations in the form of Group Policy settings that influence the general logging behavior of the system. Configuration recommendations for specific event logs and audit policies, can be found in Chapter 5.

4.1 Security Options

This section contains recommendations for the configuration of the Security Options.

4.1.1 Ensure “Audit: Shut down system immediately if unable to log security audits” is set to “Disabled”

Description, configuration recommendation and impact identical to 2.3.2.2 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Default Value
Disabled (The system will not be shut down if a security audit cannot be logged.)

Note: In case that under no circumstances events of the security event log should be lost, this setting should be set to “Enabled”.

4.1.2 Ensure “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” is set to “Enabled”

Description, configuration recommendation and impact identical to 2.3.2.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Default Value
Enabled (Configured settings of the Advanced Audit Policy subcategories are used.)

4.2 Windows Defender Firewall with Advanced Security

This section contains recommendations for the configuration of the Windows Defender Firewall.

4.2.1 Domain Profile

This section contains recommendations for the domain profile of the Windows Defender Firewall.

4.2.1.1 Ensure “Windows Firewall: Domain: Logging: Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log”

Description, configuration recommendation and impact identical to 9.1.5 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Domain Profile

Default Value
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.1.2 Ensure “Windows Firewall: Domain: Logging: Size limit (KB)” is set to “16,384 KB or greater”

Description, configuration recommendation and impact identical to 9.1.6 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Domain Profile

Default Value
4,096 KB

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

4.2.1.3 Ensure “Windows Firewall: Domain: Logging: Log dropped packets” is set to “Yes”

Description, configuration recommendation and impact identical to 9.1.7 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Domain Profile

Default Value
No (Information about dropped packets will not be logged.)

4.2.1.4 Ensure “Windows Firewall: Domain: Logging: Log successful connections” is set to “Yes”

Description, configuration recommendation and impact identical to 9.1.8 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Domain Profile

Default Value
No (Information about successful connections will not be logged.)

4.2.2 Private Profile

This section contains recommendations for the private profile of the Windows Defender Firewall.

4.2.2.1 Ensure “Windows Firewall: Private: Logging: Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log”

Description, configuration recommendation and impact identical to 9.2.5 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Private Profile

Default Value
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.2.2 Ensure “Windows Firewall: Private: Logging: Size limit (KB)” is set to “16,384 KB or greater”

Description, configuration recommendation and impact identical to 9.2.6 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Private Profile

Default Value
4,096 KB

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

4.2.2.3 Ensure “Windows Firewall: Private: Logging: Log dropped packets” is set to “Yes”

Description, configuration recommendation and impact identical to 9.2.7 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Private Profile

Default Value
No (Information about dropped packets will not be logged.)

4.2.2.4 Ensure “Windows Firewall: Private: Logging: Log successful connections” is set to “Yes”

Description, configuration recommendation and impact identical to 9.2.8 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Private Profile

Default Value
No (Information about successful connections will not be logged.)

4.2.3 Public Profile

This section contains recommendations for the public profile of the Windows Defender Firewall.

4.2.3.1 Ensure “Windows Firewall: Public: Logging: Name” is set to “%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log”

Description, configuration recommendation and impact identical to 9.3.7 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Public Profile

Default Value
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.3.2 Ensure “Windows Firewall: Public: Logging: Size limit (KB)” is set to “16,384 KB or greater”

Description, configuration recommendation and impact identical to 9.3.8 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Public Profile

Default Value
4,096 KB

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

4.2.3.3 Ensure “'Windows Firewall: Public: Logging: Log dropped packets” is set to “Yes”

Description, configuration recommendation and impact identical to 9.3.9 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Public Profile

Default Value
No (Information about dropped packets will not be logged.)

4.2.3.4 Ensure “Windows Firewall: Public: Logging: Log successful connections” is set to “Yes”

Description, configuration recommendation and impact identical to 9.3.10 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Settings\Windows Defender Firewall with Advanced Security\Windows Defender Firewall with Advanced Security\Windows Firewall Properties\Public Profile

Default Value
No (Information about successful connections will not be logged.)

4.3 Administrative Templates

This section contains computer-based recommendations from Group Policy Administrative Templates (ADMX).

4.3.1 MSS (Legacy)

This section contains recommendations for the configuration of Microsoft Solutions for Security (MSS).

These settings are provided by the Group Policy template `MSS-legacy.admx/adml` that was published by Microsoft (ms_sec_bl_1809, 2021).

4.3.1.1 Ensure "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning" is set to "Enabled: 90% or less"

Description, configuration recommendation and impact identical to 18.4.13 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\MSS (Legacy)

Default Value
0 % (No warning event is generated.)

Note: If the event log is configured to automatically overwrite events as needed or after a specific age, this event will not be generated.

4.3.2 Event Log Service

This section contains recommendations for the configuration of the Event Log Service.

These settings are provided by the Group Policy template `EventLog.admx/adml` that is included with all versions of the Microsoft Windows Administrative Templates.

4.3.2.1 Application

This section contains recommendations for configuration of the Application Event Log.

4.3.2.1.1 Ensure "Specify the maximum log file size (KB)" is set to "32,768 or greater"

Description, configuration recommendation and impact identical to 18.9.26.1.2 *of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application

Default Value
Disabled (The default log size is 20,480 KB and can be changed locally.)

4.3.2.1.2 Ensure “Control Event Log behavior when the log file reaches its maximum size” is set to “Disabled”

Description, configuration recommendation and impact identical to 18.9.26.1.1 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Application

Default Value
Disabled (When the event log file reaches its maximum size, new events overwrite old events.)

Note: Old events may be retained depending on how the “Backup log automatically when full” setting is configured.

4.3.2.2 Setup

This section contains recommendations for configuration of the Setup Event Log.

4.3.2.2.1 Ensure “Setup: Specify the maximum log file size (KB)” is set to “32.768 or greater”

Description, configuration recommendation and impact identical to 18.9.26.3.2 *of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Setup

Default Value
Disabled (The default log size is 20,480 KB and can be changed locally.)

4.3.2.2.2 Ensure “Control Event Log behavior when the logfile reaches its maximum size” is set to “Disabled”

Description, configuration recommendation and impact identical to 18.9.26.3.1 *of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Setup

Default Value
Disabled (When the event log file reaches its maximum size, new events overwrite old events.)

Note: Old events may be retained depending on how the “Backup log automatically when full” setting is configured.

4.3.2.3 Security

This section contains recommendations for configuration of the Setup Event Log.

4.3.2.3.1 Ensure “Specify the maximum log file size (KB)” is set to “524,288 or greater”

See also 18.9.26.2.2 *of the CIS Benchmark and the configuration recommendation of the Microsoft Security Baseline.*

This setting configures the maximum log size of the Security log.

Rationale

For comprehensive logging of security-relevant events, the common recommendations for the size of the Security log are not sufficient and should therefore be increased to at least the recommended value. Especially if, among others, the process creation is also logged.

Impact

The size of the log file for the Security log is increased to the recommended value.

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security

Default Value
Disabled (The default log size is 20,480 KB and can be changed locally.)

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

4.3.2.3.2 Ensure “Control Event Log behavior when the log file reaches its maximum size” is set to “Disabled”

Description, configuration recommendation and impact identical to 18.9.26.2.1 *of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\Security

Default Value
Disabled (When the event log file reaches its maximum size, new events overwrite old events.)

Note: Old events may be retained depending on how the “Backup log automatically when full” setting is configured.

4.3.2.4 System

This section contains recommendations for configuration of the System Event Log.

4.3.2.4.1 Ensure "Specify the maximum log file size (KB)" is set to "32,768 or greater"

Description, configuration recommendation and impact identical to 18.9.26.4.2 *of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System

Default Value
Disabled (The default log size is 20,480 KB and can be changed locally.)

4.3.2.4.2 Ensure "Control Event Log behavior when the log file reaches its maximum size" is set to "Disabled"

Description, configuration recommendation and impact identical to 18.9.26.4.1 *of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.*

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Event Log Service\System

Default Value
Disabled (When the event log file reaches its maximum size, new events overwrite old events.)

Note: Old events may be retained depending on how the "Backup log automatically when full" setting is configured.

4.3.3 Audit Process Creation

This section contains settings related to auditing of process creation events.

These settings are provided by the Group Policy template `AuditSettings.admx/adml` that is included with the Microsoft Windows 8.1 & Server 2012 R2 Administrative Templates (or newer).

4.3.3.1 Ensure "'Include command line in process creation events" is set to "Enabled"

See also 18.8.3.1 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

By default, process creation events (event ID 4688 in the Security event log) do not contain information about which arguments were used to invoke a process. This setting can be used to influence this behavior.

Rationale

The default configuration for process creation events already provides important information for detecting malicious actions by an attacker. This includes, for example, the process name or the name of the executing account. However, these may not be sufficient to detect an active attack or to trace the exact actions taken in a forensic analysis, since, for example, a process name is easily changeable. The additional logging of process arguments can provide information about what the actual intention of a process creation was as well as what data and information was passed to this process.

Impact

By enabling this setting, all process creation command line arguments are logged and saved in the Security event log. This may include sensitive information such as passwords if entered in plain text on the command line. Thus, every user that has read access on the Security event log can also read this sensitive information. This also applies if the log was saved on another system (e.g., for storage).

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\System\Audit Process

Default Value
Disabled (Command line arguments are not included in process creation events.)

4.3.4 Windows PowerShell

As PowerShell can access many system resources via .NET and is easy to use, attackers can use PowerShell for malicious purposes. These include completely compromising Windows instances and then maintaining access to that system. Comprehensive logging of PowerShell events and their analysis is critical in this regard to detect malicious use early.

The following settings (sections 4.3.4.1, 4.3.4.2 and 4.3.4.3) can generate a significant amount of log data. However, they provide the ability to detect malicious activity depending on how PowerShell is used on a particular Windows instance. Thus, if the log data is processed in real time, it may be possible to detect malicious PowerShell activity at the time of actual execution. At the very least, however, it helps to reconstruct what actually happened during a forensic analysis.

It is important to emphasize that the evaluation of whether a particular PowerShell activity is malicious or not depends on how PowerShell is used on a particular Windows instance. This may vary for different instances. Once activities are identified that are not typical for the specific Windows instance, a closer examination of the log data is required to determine the exact reason for the activity and to evaluate whether the activity was malicious or not.

There are some general indicators for malicious PowerShell activity that can be observed in the log data:

- Creation of PowerShell sessions (event ID 8193, see appendix, section “Event IDs: Section 5.5.2.1“): If a process that is not expected to create PowerShell sessions does create them, this may indicate that the process is malware;
- atypical content in PowerShell scripts (event ID 4104, see appendix, section “Event IDs: Section 5.5.2.1“): An example is encoded script content or script content written in an inconsistent manner (for example, inconsistent capitalization). This indicates the execution of a malicious PowerShell script;

- atypical PowerShell commands (executed as part of a script or entered by the user via the command line interface of the PowerShell host process): An example is the execution of the PowerShell command `IEX` to establish a network connection when such connections are not normally done via PowerShell;
- atypical PowerShell/.NET activities: These activities can be identified by examining the log data created by the Microsoft-Windows-PowerShell / Operational log source (for example, event ID 4103, see appendix, section “Event IDs: Section 5.5.2.1“). At a high level, such activities can be identified by strings. For example, the string *MiniDumpWriteDump* indicates that PowerShell has extracted the memory area allocated to a process. For instance, this memory area may contain confidential user data. If this activity is not normally performed using PowerShell, it may be a malicious PowerShell activity.

4.3.4.1 Ensure “Turn on Module Logging” is set to “Enabled” and the option “Modul Names” is set to “*”

This setting enables logging of user-specified PowerShell modules.

Note: Depending on the usage of the system, the monitored PowerShell modules can be narrowed down (via the "Module Names" option) to reduce the amount of log data.

Rationale

Module logging records pipeline execution events for all specified PowerShell modules. This includes the commands that are executed, including the exact command calls and a portion of the scripts that are executed. Data intended for output is also partially logged. Although module logging does not include all the details of execution and output results, it is a useful addition to the other PowerShell logging mechanisms.

Impact

Once this setting is enabled, portions of executed PowerShell commands and scripts, as well as PowerShell output, are recorded and stored in the log *Microsoft-Windows-PowerShell/Operational*. This may include sensitive information such as passwords if entered in plain text. Thus, every user that has read access on the Security event log can also read this sensitive information. This also applies if the log was saved on another system (e.g., for storage).

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell

Default Value
Disabled (By default, PowerShell modules are not logged. The property *LogPipelineExecutionDetails of a* PowerShell module specifies whether execution events are logged.)

4.3.4.2 Ensure “Turn on PowerShell Script Block Logging” is set to “Enabled”

See also 18.9.95.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

This setting configures logging of the contents of executed PowerShell scripts.

Note: The option "Log script block invocation start / stop events" should not be enabled, as this configuration leads to a high event volume with significant amounts of data.

Rationale

Logging of script blocks allows to record the processing of all commands and scripts as they are executed by PowerShell. Thus, for example, not only executed encoded commands (as they often occur in malware) are stored in the log, but additionally the decoded commands as soon as they are executed. Logging occurs regardless of whether the commands or scripts are invoked interactively or automatically. However, the logging of the script blocks does not contain any information about the output of the executed code.

Impact

Once this setting is enabled, all executed PowerShell commands and scripts are recorded and stored in the log *Microsoft-Windows-PowerShell/Operational*. This may include sensitive information such as passwords if entered in plain text. Thus, every user that has read access on the log file can also read this sensitive information. This also applies if the log was saved on another system (e.g., for storage).

Note: The warning in the CIS Benchmark that all logged-on users have read access to the log "Microsoft-Windows-PowerShell/Operational" is incorrect. By default, only the Administrators group (apart from other system accounts) has the appropriate permissions (in this specific case, Full Control).

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell

Default Value
Enabled (PowerShell script blocks are logged.)

4.3.4.3 Ensure "Turn on PowerShell Transcription" is set to "Enabled" and the option "Include invocation headers" is active

See also 18.9.95.2 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

This setting configures logging of user input and PowerShell output displayed on the command line interface of the PowerShell host process (`powershell.exe`). Logging is performed to a text file for which the storage location is configured by this policy.

Note: In the default configuration, all transcripts are stored as text files in the "Documents" directory of the respective executing user. To secure the transcripts centrally and protect them from unauthorized modification, a write-only network share should be configured as the directory for the transcript output.

Rationale

PowerShell transcription generates a so-called transcript for each user and each PowerShell session, in which all inputs and outputs (incl. timestamps) of the session are recorded. In addition to the other logging mechanisms, these transcripts can be used to get a first overview of PowerShell activity in the event of a

high-level analysis, as this type of logging generates a manageable amount of data. However, there is the limitation that only information directly visible on the PowerShell command line is logged. This excludes information in the context of executed scripts and data that was output in other ways (for example, written directly to a file).

Impact

With this setting, all PowerShell input and output is stored in the *PowerShell_transcript* log file. This may include sensitive information such as passwords if entered in plain text. Thus, every user that has read access on the transcript file can also read this sensitive information. This also applies if the log was saved on another system (e.g., for storage).

Configuration Path in the Group Policy Editor

Computer Configuration\Administrative Templates\Windows Components\Windows PowerShell

Default Value

Disabled (A transcription of all PowerShell sessions does not take place.)

5 Configuration Recommendations: Audit Policies and Event Logs

The following sections contain configuration recommendations for specific settings of event logs and audit policies. Recommendations that influence the general logging behavior of the system can be found in Chapter 4.

All configurations of the Audit Policy are to be done through the Advanced Audit Policy Configuration only. Using both the standard Audit Policy (under the Group Policy path *Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy*) and the Advanced Audit Policy (under the Group Policy path *Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration*) may result in unexpected logging behavior, as in such a case the settings for the operating system are not unambiguous (see (ms_audit_pol, 2021)).

While all recommendations from the Microsoft Security Baseline are also included in this document, the following configuration recommendations regarding the Audit Policy from the CIS Benchmark do not have an equivalent setting:

CIS Benchmark Reference	Policy Setting Name	Rationale
17.2.1	Audit Application Group Management	Application Groups are only used by the so-called. Authorization Manager which is no longer supported by Microsoft since Windows Server 2012 (see (ms_app_group, 2021)).
17.2.2	Audit Computer Account Management	Events of the category Computer Account Management are only generated on Domain Controllers (see (ms_comp_acc, 2021)).
17.9.1	Audit IPsec Driver	Events of the category IPsec Driver are only generated when IPsec is in use. This is beyond the scope of this document.

The recommended configurations for the Applications and Services Logs can be applied via various ways. The main methods are the configuration via the `Event Viewer` (in the properties of the individual logs), via the `Registry Editor` (under the Registry path *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*) and via the command line application `wevtutil.exe` (under the path *C:\Windows\System32*). As the configuration via the `Event Viewer` is not suitable for the automated deployment of settings and the configuration via the registry has proven to be unreliable (settings are not correctly applied, even after a reboot), this document describes the configuration via the application `wevtutil.exe`. The `wevtutil.exe` application is a command line tool with which, among others, the Applications and Services Logs can be configured. `wevtutil.exe` is included with Windows 10. The following parameters are required to apply the recommended settings:

```
wevtutil.exe set-log $log /enabled:true /retention:false /maxsize:33554432
```

- `set-log` specifies that the configuration of a specified log should be modified
- `$log` specifies the name of the event log
- `/enabled:true` specifies that the event log should be activated
- `/retention:false` specifies that events may be overwritten if necessary (oldest events first)
- `/maxsize:33554432` specifies the maximum size (in Bytes) of the event log (in this example 32,768 KB)

Detailed information about `wevtutil.exe` can be found here (ms_wevtutil, 2021).

The following sections describe the required configurations to allow a comprehensive logging in the following areas of system activity:

- Account activity (e.g., user account logons)
- Activity of core system components (e.g., installation of a system service)
- Configuration changes (e.g., group membership changes)
- Network activity (e.g., SMB connection errors)
- Process activity (e.g., process creation)
- Registry activity (e.g., changes to Registry keys)

The corresponding tables in the appendix contain the event IDs and the respective descriptions (so-called messages) under which Windows 10 can generate events for the corresponding logs (column *Event ID* or *Message*). In this case, the `wevtutil.exe` application was also used to display possible event IDs and messages (see (ERNW_WP2), section 4.3). In the tables in the appendix, numbers preceded by a percent sign (%) indicate the dynamic part of the event that is generated at runtime. The messages in these tables are presented as they are provided by Microsoft.

5.1 Account Activity

Accounts in the context of the Windows operating system are associated with users, computers, or services. Each account has in the context of its use a unique identifier, the account name, and credentials associated with it. Authentication is based on verification of the account identifier, as well as the credentials provided. Authorization is usually based on the account in use.

Account activity is defined herein as configuration changes made to accounts, events related to account authentication and authorization, and the use of sensitive privileges. For more information about which privileges Microsoft defines as sensitive privileges, see (ms_sens_priv, 2021).

The logging of account activities is used to make visible which accounts try to log on to a system, when and how. Furthermore, it can be traced which privileges they have, and which changes are made to accounts and their privileges. Thus, logging can help monitor a system or an environment for various attacks on accounts, as well as reconstruct the use of potentially compromised accounts during forensic investigations.

Since the compromise of accounts (as well as the associated credentials) and the subsequent reuse of them are among the main attack vectors in Windows environments, special attention is paid to logging account activity. As an example, the following log analysis scenarios can be stated, which are made feasible by the recommended settings:

- The attempt to compromise accounts via brute-force attacks or password spraying results in a high number of failed authentication attempts (of either individual or many accounts) and thus logon events within a short period of time.
- Unusual logon behavior, such as logons outside working hours or via logon types (logged in logon events) that are unusual for the account in question, can in turn be an indicator for the misuse of valid, but compromised, accounts.
- The use of sensitive privileges can indicate the execution of security-critical actions. These can occur during legitimate activities, but also during different attack techniques. Thus, the use of the so-called debug privilege could be indicative of the usage of the attack tool *mimikatz*.
- Logged account activity can also provide information about attempts by attackers to achieve persistence on a system or in an environment. The creation of new accounts, as well as changes to privileges or configurations of existing accounts, could represent such an attempt.

In Active Directory environments, the following additional exemplary scenarios also become relevant:

- Logging of account activity, in combination with events generated on Domain Controllers and servers, can also provide evidence of the use of stolen or forged Kerberos tickets on systems that are members of an Active Directory environment. For example, if an account does not have a valid *Ticket Granting Ticket* (TGT), i.e., the account did not logon via Kerberos authentication through a Domain Controller, or an account has logged out, but that account still authenticates to resources via a *Service Ticket*, this may indicate that an attacker has stolen Kerberos tickets or is able to create forged tickets for Kerberos services, so-called *Silver Tickets*.
- If an account's authorization does not match the privileges that the account has on a system or in Active Directory, this is an indication that forged Kerberos tickets are being used and thus that a service or even the entire Active Directory has been compromised. Such inconsistencies can be seen, for example, by event 4672 being logged for an account that does not have sensitive privileges.
- Indications of potential pass-the-hash attacks using stolen account password hashes to authenticate via the NTLM protocol can be provided by event 4624 in environments where Kerberos authentication is predominantly used. If logon type 9 is logged here, this means that a user has specified new credentials for outgoing connections that are different from their account. But even the general use of NTLM instead of Kerberos for authentication could be an indication of pass-the-hash (event 4776).

To cover the aforementioned scenarios, the recommended settings that enable logging of logon and logoff events (including group membership and assigned privileges), account lockout events, and account management events should be implemented.

5.1.1 Windows Logs

This section provides recommendations for the configuration of the System and Security logs that are configurable via Group Policy.

5.1.1.1 Ensure “Audit Credential Validation” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.1.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Account Logon

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4776: The computer attempted to validate the credentials for an account.	This event is generated when NTLM authentication information is verified and thus assists in tracking NTLM login attempts.

5.1.1.2 Ensure “Audit User Account Management” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.2.3 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Account Management

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4720: A user account was created.	This event is generated when a new user account object is created.
4722: A user account was enabled.	This event is generated when a user account object is activated.
4723: An attempt was made to change an account's password.	This event is generated when a user account attempts to change a password.
4724: An attempt was made to reset an account's password.	This event is generated when a user account attempts to reset a password.
4725: A user account was disabled.	This event is generated when a user account object is disabled.
4726: A user account was deleted.	This event is generated when a user account object is deleted.
4738: A user account was changed.	This event is generated when attributes of a user account object are changed.
4740: A user account was locked out.	This event is generated when a user account is locked.
4767: A user account was unlocked.	This event is generated when a user account is unlocked.
4781: The name of an account was changed.	This event is generated when the user account attribute *sAMAccountName* is changed.
4798: A user's local group membership was enumerated.	This event is generated when a process lists the security-enabled local groups of an account.
5376: Credential Manager credentials were backed up.	This event is generated when a user account successfully backs up the *Credential Manager* database.
5377: Credential Manager credentials were restored from a backup.	This event is generated when a user account successfully restores the *Credential Manager* database.

5.1.1.3 Ensure “Audit Account Lockout” is set to include “Failure”

Description, configuration recommendation and impact identical to 17.5.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Success events (see (ms_al, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4625: An account failed to log on.	This event is generated when an account is locked after a login attempt or when a login attempt is made for a locked account.

5.1.1.4 Ensure “Audit Group Membership” is set to include “Success”

Description, configuration recommendation and impact identical to 17.5.2 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4627: Group membership information.	This event is generated in conjunction with event ID 4624 (An account was successfully logged on) and displays the list of groups the logged-on account is a member of.

5.1.1.5 Ensure “Audit Logoff” is set to include “Success”

Description, configuration recommendation and impact identical to 17.5.3 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4634: An account was logged off.	This event is normally generated for all logon types except *Interactive* and *RemoteInteractive* when an account logoff occurs. Correlates with, for example, event ID 4624 (An account was successfully logged on).
4647: User initiated logoff.	This event is specific to *Interactive* and *RemoteInteractive* logon types and is generated when an account logoff is initiated. Correlates with, for example, event ID 4624 (An account was successfully logged on).

5.1.1.6 Ensure “Audit Logon” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.5.4 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
Success and Failure

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4624: An account was successfully logged on.	This event is generated when an account logon attempt was successful, and a logon session was created.
4625: An account failed to log on.	This event is generated when an account logon attempt has failed.
4648: A logon was attempted using explicit credentials.	This event is generated when an account attempts a logon with another account, such as when using the `runas.exe` application.

5.1.1.7 Ensure “Audit Other Logon/Logoff Events” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.5.5 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4778: A session was reconnected to a Window Station.	This event is generated when a user connects to an existing Window Station.
4779: A session was disconnected from a Window Station.	This event is generated when a user disconnects from an existing Window Station.
5378: The requested credentials delegation was disallowed by policy.	This event is generated when delegation of credentials via the CredSSP protocol has been attempted but prevented by policy.

5.1.1.8 Ensure “Audit Special Logon” is set to include “Success”

Description, configuration recommendation and impact identical to 17.5.6 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_sl, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Logon/Logoff

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4964: Special groups have been assigned to a new logon.	This event is generated when a member of a defined *Special Group* logs on.
4672: Special privileges assigned to new logon.	This event is generated when sensitive privileges are assigned to an account logon.

5.1.2 Application and Services Logs

This section provides recommendations for the configuration of the Applications and Services logs that are not configurable via Group Policy, but the settings can be distributed via Group Policy objects.

5.1.2.1 Ensure the log "Microsoft-Windows-LSA/Operational" is enabled and configured

This event log contains information about the Local Security Authority (LSA) of the Windows operating system. The LSA process performs all authentication and authorization activities and is thus an important source when monitoring logon activity.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-LSA/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Disabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
300	This event is generated when the login attempt of an account was successful, and a logon session was created. The event displays a list of groups which the logged-on account is a member of.

5.1.2.2 Ensure the log "Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational" is enabled and configured

This event log contains information about the Microsoft-Windows-TerminalServices-RemoteConnectionManager component of the Windows operating system. The logging data gathered here therefore includes information about incoming network connections from RDP clients.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
1149	This event is generated if a successful network authentication was performed before the actual user session.
258	This event is generated when the *TermService* service starts opening a port assigned to it.
259	This event is generated when the *TermService* service starts closing a port assigned to it.

5.1.2.3 Ensure the log "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational" is enabled and configured

This event log contains information about the Microsoft-Windows-TerminalServices-LocalSessionManager component of the Windows operating system, which is responsible for starting the computer and implementing Fast User Switching (FUS). The configuration of this component, as well as the Windows Defender Firewall, determine whether incoming RDP connections are allowed. If this is the case, this event log contains information about RDP sessions.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-TerminalServices-LocalSessionManager/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
40	This event is generated when an RDP session is interrupted.
41	This event is generated when the *TermService* service starts assigning a session.
42	This event is generated when the *TermService* service has completed the assignment of a session.
22	This event is generated when a shell is initialized after a successful RDP login.
21	This event is generated when a successful RDP login and session instantiation has been performed.
24	This event is generated when an RDP session is interrupted.
25	This event is generated when a user connects to an existing RDP session.
23	This event is generated when a logged-on user initiates a system logoff in an RDP session.
17	This event is generated when the *TermService* service startup failed.
39	This event is generated when a session is terminated by another session.

5.2 Activity of Core System Components

Events that are triggered by security-relevant system components and thus reflect the activities of these components and their correct or improper operation should be logged. This includes events triggered by the following core components of a Windows system:

- Local Security Authority (LSA)

- Security Account Manager (SAM)
- Windows Task Scheduler
- Windows Defender Firewall Service
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)
- Code Integrity Functionality
- Cryptography API: Next Generation

Additionally, events in the context of general operating system functionalities, such as file sharing, object access or application of Group Policies are covered by this section. Furthermore, the installation of new system services as well as devices and drivers were added to this category. The configuration recommendations for the logging of process creation and Registry activity events were moved to separate sections (see sections 5.5 and 5.6).

Events that are triggered by the aforementioned components (which are essential for the security of the operating system) can provide various indications for (attempted) attacks on the system as well as the security posture of a system.

If errors are reported by these components that are essential for the security of a system, this can mean that the overall security level of the system was lowered. These errors can be induced by an attacker or they can also be caused by component malfunctions, but in both cases, they can be security critical. Examples for this are:

- A deactivation of the Windows Defender Firewall (logged in event ID 5025) could be triggered by an attacker to establish unwanted network connections. Event ID 5030 that is generated when the Windows Defender Firewall service is not starting or was stopped unexpectedly can be an indicator for faulty behavior as well as actions of an attacker.
- The loss of logging data due to a logging queue overflow, logged in event ID 4612, can be provoked by an attacker to obfuscate their activities.

Events in this category can also provide evidence for (attempted) initial attacks:

- Event ID 5148 is logged when the Windows Filter Platform detects a presumed denial-of-service attack.
- The connection of external devices can be used to bring malware onto a computer. Event ID 400 is logged when a plug-and-play-capable device was successfully initialized.
- If the Code Integrity component reports that software does not meet the integrity requirements (e.g., loading an unsigned kernel module (event ID 3001)), it can be an indicator for the (attempted) execution of malware.

Information about the attack progression after a successful initial compromise can also be obtained by logging events generated by core system components:

- Unexpected processes that have debug privileges on core system components such as the Local Security Authority could be an indication for the execution of malware (e.g., *mimikatz*) with elevated privileges. In the example of *mimikatz* relevant key material is extracted via debugging of the Local Security Authority Subsystem Service (LSASS) to access encrypted memory areas containing credentials and authentication tokens.
- A new, unexpectedly installed system service (logged in event ID 4697) that is executed every system start could be a potential way for an attacker to gain persistence on a system after a successful compromise. As system services can be registered with administrative privileges but can possibly be executed with the rights of LOCAL SYSTEM, this can also be a way for an attacker to escalate their privileges.

To enable logging for the aforementioned system components and allow for monitoring of the exemplary scenarios, the following configuration recommendations should be implemented.

5.2.1 Windows Logs

This section provides recommendations for the configuration of the System and Security logs that are configurable via Group Policy.

5.2.1.1 Ensure “Audit Other System Events” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.9.2 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\System

Default Value
Success and Failure

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
5024: The Windows Firewall Service has started successfully.	This event is generated when the Windows Firewall service (*MpsSvc*) is started successfully.
5025: The Windows Firewall Service has been stopped.	This event is generated when the Windows Firewall service (*MpsSvc*) has been stopped.
5027: The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.	This event is generated when the Windows Firewall service (*MpsSvc*) cannot retrieve a new security policy and therefore cannot initialize it.
5028: The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.	This event is generated when the Windows Firewal l service (*MpsSvc*) cannot interpret and therefore initialize a new security policy.
5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy.	This event is generated when either the Windows Firewall service (*MpsSvc*) or its driver cannot be started or when they are terminated unexpectedly.
5030: The Windows Firewall Service failed to start.	This event is generated when the Windows Firewall service (*MpsSvc*) fails to start or when it terminates unexpectedly.
5033: The Windows Firewall Driver has started successfully.	This event is generated when the Windows Firewall driver is successfully started.
5034: The Windows Firewall Driver was stopped.	This event is generated when the Windows firewall driver is stopped.
5035: The Windows Firewall Driver failed to start.	This event is generated when the Windows firewall driver could not be started.
5037: The Windows Firewall Driver detected critical runtime error. Terminating.	This event is generated when the Windows Firewall driver fails to start or when it terminates unexpectedly.

5.2.1.2 Ensure “Audit Security State Change” is set to include “Success”

Description, configuration recommendation and impact identical to 17.9.3 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_ssc, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\System

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4608: Windows is starting up.	This event is generated when the *LSASS.EXE* process is started, and the auditing subsystem is initialized.
4616: The system time was changed.	This event is generated when the system time has been changed.

5.2.1.3 Ensure “Audit Security System Extension” is set to include “Success”

Description, configuration recommendation and impact identical to 17.9.4 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_sse, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\System

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4610: An authentication package has been loaded by the Local Security Authority.	This event is generated when an authentication package has been loaded by the *LSASS.EXE* process.
4611: A trusted logon process has been registered with the Local Security Authority.	This event is generated when the *LSASS.EXE* process confirms a valid logon process and logons can be processed by that logon process.
4614: A notification package has been loaded	This event is generated when a Notification Package DLL

Event ID: Name	Rationale
by the Security Account Manager.	has been loaded by the Security Account Manager and the initialization sequence for this DLL has been executed.
4622: A security package has been loaded by the Local Security Authority.	This event is generated when a Security Package DLL has been loaded by the Local Security Authority and the initialization sequence for this DLL has been executed.
4697: A service was installed in the system.	This event is generated when a new service is installed on the system.

5.2.1.4 Ensure "'Audit System Integrity" is set to "Success and Failure"

Description, configuration recommendation and impact identical to 17.9.5 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\System

Default Value
Success and Failure

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4612: Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.	This event is generated when the auditing queue overflows and events need to be discarded. This occurs most often when events are generated faster than they can be written to disk.
4816: RPC detected an integrity violation while decrypting an incoming message.	This event is generated when a Remote Procedure Call (RPC) has detected an integrity violation while decrypting an incoming message.
5038: Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error.	This event is generated when the code integrity functionality (ms_code_integrity, 2021) determines that the signature of a file is not valid.
5061: Cryptographic operation.	This event is generated when a cryptographic operation has been performed using a Key Storage Provider (KSP).
6281: Code Integrity determined that the page hashes of an image file are not valid. The file could be improperly signed without page hashes or corrupt due to unauthorized modification. The invalid hashes could indicate a potential disk device error.	This event is generated when the code integrity functionality (ms_code_integrity, 2021) determines that the page hash of an image is invalid.
6410: Code integrity determined that a file does not meet the security requirements to load into a process.	This event is generated when writable shared sections exist in a file image.

5.2.1.5 Ensure “Audit File Share” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.6.2 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Object Access

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
5140: A network share object was accessed.	This event is generated on the first access attempt when a network share object is accessed.
5142: A network share object was added.	This event is generated when a network share object is added.
5143: A network share object was modified.	This event is generated when a network share object is changed.
5144: A network share object was deleted.	This event is generated when a network share object is deleted.
5168: SPN check for SMB/SMB2 failed.	This event is generated when the SMB SPN check fails. The SPN is sent to the server only when the NTLMv2 or Kerberos protocols are used.

5.2.1.6 Ensure “'Audit Detailed File Share” is set to include “Failure”

Description, configuration recommendation and impact identical to 17.6.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Object Access

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
5145: A network share object was checked to see whether client can be granted desired access.	This event is generated when a network share object (file or folder) is accessed.

5.2.1.7 Ensure “Audit Other Object Access Events” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.6.3 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Object Access

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4671: An application attempted to access a blocked ordinal through the TBS.	This event is generated when a process tries to access a blocked TPM index via TPM Base Service (TBS) functionality.
5148: The Windows Filtering Platform has detected a DoS attack and entered a defensive mode; packets associated with this attack will be discarded.	This event is generated when an ICMP DoS attack starts or is detected.
5149: The DoS attack has subsided and normal processing is being resumed.	This event is generated when an ICMP DoS attack subsides or is terminated.
4698: A scheduled task was created.	This event is generated when a new Scheduled Task is created.
4699: A scheduled task was deleted.	This event is generated when a Scheduled Task is deleted.
4700: A scheduled task was enabled.	This event is generated when a Scheduled Task is enabled.
4701: A scheduled task was disabled.	This event is generated when a Scheduled Task is disabled.
4702: A scheduled task was updated.	This event is generated when a Scheduled Task is updated.
5888: An object in the COM+ Catalog was modified.	This event is generated when an object is changed in the COM+ Catalog.
5889: An object was deleted from the COM+ Catalog.	This event is generated when an object is deleted from the COM+ Catalog.
5890: An object was added to the COM+ Catalog.	This event is generated when an object is added to the COM+ Catalog.

5.2.1.8 Ensure “Audit Removable Storage” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.6.4 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Object Access

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4656: A handle to an object was requested.	This event is generated when a handle has been requested for an object.
4658: The handle to an object was closed.	This event is generated when a handle for an object has been closed.
4663: An attempt was made to access an object.	This event is generated when an attempt is made to access an object.

5.2.1.9 Ensure "Audit PNP Activity" is set to include "Success"

Description, configuration recommendation and impact identical to 17.3.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Detailed Tracking

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
6416: A new external device was recognized by the System.	This event is generated when a new external device is detected by the system, e.g., when a new external device is connected or activated.
6419: A request was made to disable a device.	This event is generated when a request to disable a device has been made.
6420: A device was disabled.	This event is generated when a request to disable a device was successful and the device was disabled.
6421: A request was made to enable a device.	This event is generated when a request to enable a device has been made.
6422: A device was enabled.	This event is generated when a request to enable a device was successful and the device was enabled.
6423: The installation of this device is forbidden by system policy.	This event is generated when the installation of a device has been prohibited by the device installation policies.
6424: The installation of this device was allowed, after having previously been forbidden by policy.	This event is generated when administrators are allowed to bypass the device installation policies.

5.2.2 Application and Services Logs

This section provides recommendations for the configuration of the Applications and Services logs that are not configurable via Group Policy, but the settings can be distributed via Group Policy objects.

5.2.2.1 Ensure the log "Microsoft-Windows-CAPI2/Operational" is enabled and configured

This event log contains events related to the "Cryptography API: Next Generation". This represents the cryptography platform of the Windows operating system and performs tasks such as the calculation of cryptographic operations. For example, errors generated during the usage of certificates can be found in this event log.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-CAPI2/Operational /enabled:true /retention:false /maxsize:201326592` to activate and configure the log.

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

Default Value
Disabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
10	This event is generated when a process has started the creation of a CERT_CONTEXT object (e.g., by using *CertGetCertificateChain*).
11	This event is generated when the creation of a CERT_CONTEXT object (e.g., by using *CertGetCertificateChain*) has been successfully completed.
30	This event is generated when the validity of a CERT_CONTEXT object (e.g., by using *CertVerifyCertificateChainPolicy*) has been verified by a process.
40	This event is generated when a process has started a lock status verification of a CERT_CONTEXT object (e.g., by using *CertVerifyRevocation*).
41	This event is generated when the lock status of a CERT_CONTEXT object has been verified (e.g., by using *CertVerifyRevocation*) by a process.
42	This event is generated when the revocation status verification information has been rejected (e.g., by *CertVerifyRevocation*).
50	This event is generated when a process has started retrieving a Public Key Infrastructure (PKI) object (see

Event ID	Rationale
	(ms_crypt_retrv_obj, 2021)) from a location specified by a URL.
51	This event is generated when a process completes the retrieval of a Public Key Infrastructure (PKI) object (see (ms_crypt_retrv_obj, 2021)) URL).
90	This event is generated when a CERT_CONTEXT object is created (e.g., by using *CertGetCertificateChain*).

5.2.2.2 Ensure the log "Microsoft-Windows-CodeIntegrity/Operational" is enabled and configured

This event log contains events related to kernel-side driver signature verification. The Operational event log can be used to obtain signature verification errors.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-CodeIntegrity/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
3001	This event is generated when the Code Integrity component detects that an unsigned kernel module is loaded into the system.
3002	This event is generated when the Code Integrity component cannot verify the integrity of a file.
3003	This event is generated when the system is in debug mode and the Code Integrity component cannot verify the integrity of a file.
3004	This event is generated when the Code Integrity component cannot verify the integrity of a file because the file hash is not found on the system.
3005	This event is generated when the system is in debug mode and the Code Integrity component cannot verify the integrity of a file because the file hash is not found on the system.
3010	This event is generated when the Code Integrity component failed to load a catalog file.
3033	This event is generated when the Code Integrity component detects that a process is attempting to load a file that does not meet the necessary signature requirements.

Event ID	Rationale
3076	This event is generated when a file is loaded as a result of a policy requirement, even though the Code Integrity component has determined that the necessary signature requirements are not met.
3077	This event is generated when the Code Integrity component detects that a process is attempting to load a file that does not meet the necessary policy requirement.
3089	This event is generated when the Code Integrity component interprets the signature information of a file.
3099	This event is generated when the Code Integrity component activates or updates an integrity policy.

5.2.2.3 Ensure the log "Microsoft-Windows-GroupPolicy/Operational" is enabled and configured

This event log contains events related to the use of Windows Group Policy. For example, if errors occur in the application of Group Policies, the events of this event log can be helpful.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-GroupPolicy/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 4,096 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
9001	This event is generated when Group Policy files are retrieved from a file share without *RequireMutualAuthentication* and *RequireIntegrity* attributes.
4126	This event is generated when the system starts requesting applicable Group Policies from a Domain Controller.
5126	This event is generated when the system has successfully requested applicable Group Policies from a Domain Controller.
7126	This event is generated when no applicable Group Policies could be requested from a Domain Controller.
4117	This event is generated when a Group Policy session is successfully initiated.
5117	This event is generated when a Group Policy session is successfully completed.

Event ID	Rationale
7117	This event is generated when a Group Policy session does not complete successfully.
4257	This event is generated when the system starts downloading Group Policy settings.
5257	This event is generated when the download of Group Policy settings is completed successfully.
7257	This event is generated when the download of Group Policy settings is not completed successfully.
4217	This event is generated when the system starts reading in Group Policy settings from the local datastore.
5217	This event is generated when the import of Group Policy settings from the local datastore is completed successfully.
7217	This event is generated when Group Policy settings could not be successfully read from the local datastore.
4016	This event is generated when a Client Side Extension (CSE) begins processing a Group Policy object.
5016	This event is generated when a Client Side Extension (CSE) successfully completes processing a Group Policy object.
4115	This event is generated when the Group Policy service is started successfully.
5115	This event is generated when the Group Policy service is stopped.
4017	This event is generated when the Group Policy service invokes system calls that retrieve, for example, account information or file information.
5017	This event is generated when the Group Policy Service successfully completes system calls that retrieve, for example, account information or file information.
5313	This event is generated when Group Policy objects have been filtered out and thus have not been applied.
5312	This event is generated when the list of applicable Group Policy objects is successfully queried.
5308	This event is generated when a connection to the Domain Controller has been established.
5310	This event is generated when the Group Policy service has successfully retrieved information about a *Security Principal* (ms_sec_principal, 2021) stored in the directory service.
4019	This event is generated when a script is started by the Group Policy service.
5019	This event is generated when the Group Policy service successfully completes the execution of a script.

5.2.2.4 Ensure the log "Microsoft-Windows-Kernel-PnP/Configuration" is enabled and configured

This event log contains information about plug-and-play device drivers loaded by the operating system kernel. Information about connected peripherals, such as Universal Serial Bus (USB) disks or keyboards, can be obtained from this event log.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-Kernel-PnP/Configuration /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
400	This event is generated when a PNP-capable device is detected and successfully initialized.
401	This event is generated when a PNP-capable device could be detected but not successfully initialized.
420	This event is generated when a PNP-capable device is successfully removed.
421	This event is generated when a PNP-capable device could not be successfully removed.
410	This event is generated when a PNP-capable device is successfully started after initialization.
411	This event is generated when a PNP-capable device cannot be started successfully after initialization.
430	This event is generated if further initialization steps are required after successful initialization of a PNP-capable device.

5.2.2.5 Ensure the log "Microsoft-Windows-TaskScheduler/Operational" is enabled and configured

This event log contains information about Windows Task Scheduling. Windows Task Scheduling is used to launch applications or scripts on a one-time or recurring basis. This is a popular method among attackers and malware to gain and maintain persistence on a system.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-TaskScheduler/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Disabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
100	This event is generated when a new task is successfully started by the Schedule service.
101	This event is generated when a task cannot be successfully started by the Schedule service.
102	This event is generated when a task is successfully completed by the Schedule service.
103	This event is generated when a task action (ms_task_action, 2021) cannot be started by the Schedule service.
104	This event is generated when a task action (ms_task_action, 2021) cannot be started by the Schedule service because the user cannot log on to the system.
106	This event is generated when a new task is created by a user.
107	This event is generated when a task is successfully started by the Schedule service due to a time trigger.
108	This event is generated when a task is successfully started by the Schedule service due to an event trigger.
109	This event is generated when a task is successfully started by the Schedule service due to a registration trigger.
110	This event is generated when a task is successfully started by the Schedule service for a user who is not logged in interactively.
111	This event is generated when a task is terminated by the Schedule service.
118	This event is generated when a task is successfully started by the Schedule service due to a system startup trigger.
119	This event is generated when a task is successfully started by the Schedule service due to a login trigger.
120	This event is generated when a task is successfully started by the Schedule service due to a user console login trigger.
121	This event is generated when a task is successfully started by the Schedule service due to a user console logout trigger.
122	This event is generated when a task is successfully started by the Schedule service due to a remote login condition.
123	This event is generated when a task is successfully started by the Schedule service due to a remote logoff condition.
124	This event is generated when a task is successfully started by the Schedule service due to a lock screen activation condition.
125	This event is generated when a task is successfully started by the Schedule service due to a lock screen

Event ID	Rationale
	deactivation condition.
129	This event is generated when a new task is successfully started by the Schedule service.
140	This event is generated when a user changes the attributes of an existing task.
141	This event is generated when a user deletes an existing task.
142	This event is generated when a user disables an existing task.

5.2.2.6 Ensure the log "Microsoft-Windows-WMI-Activity/Operational" is enabled and configured

This event log contains information about Windows Management Instrumentation (WMI) activity. WMI can be used to access Windows operating system settings locally or over the network and is therefore a commonly used component for administration and remote management.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-WMI-Activity/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
5857	This event is generated when WMI providers are loaded.
5858	This event is generated when a WMI query was not successful.
5860	This event is generated when a WMI event consumer is successfully registered.
5861	This event is generated when a WMI event filter is associated with an event consumer.

5.2.2.7 Ensure the log "Microsoft-Windows-WinRM/Operational" is enabled and configured

This event log contains information about the Windows Remote Management (WinRM) service of the Windows operating system. The WinRM service can be used to remotely manage Windows systems.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-WinRM/Operational /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
6	This event is generated when remote access to a target system has been initialized.
8	This event is generated when remote access to a target system has been stopped.
161	This event is generated when the system cannot connect to the target system.
162	This event is generated when the user authentication failed.
209	This event is generated when the WinRM service is started successfully.
212	This event is generated when the WinRM service has been successfully stopped.

5.3 Configuration Changes

Configuration changes to security-relevant policy objects, services, and groups can have far-reaching implications for the overall security of a system. Configuration recommendations and associated events in this section cover configuration changes to security-critical policy objects, such as the audit policy, the MPSSVC policy, the authentication policy, and the authorization policy, as well as configuration changes to the Trusted Platform Module (TPM) via Group Policy objects. Furthermore, configuration changes to groups and the Windows Defender Firewall itself as well as changes to the Access Control List (ACL) entries of objects fall into this category. Logging of configuration changes to accounts is not described in this section as it is covered by section 5.1. Configuration changes to the system that are implemented via the Registry are described in the separate section 5.6.

Configuration changes can provide evidence that a system has been compromised and that attackers are active. For configuration changes to be made to a system by an attacker, an initial compromise must have already occurred. However, configuration changes provide an attacker with many opportunities to achieve persistence on a compromised system.

Configuration changes should be logged not only to detect and reconstruct potential attacks, but also to monitor the security level of a system. Changes to security-critical policy objects, services, and groups are sometimes made by legitimate software products during installation. However, these changes can lower the security level of a system and undermine hardening measures.

Specific examples of configuration changes in the aforementioned areas can be the following:

- Adding (potentially compromised) accounts to privileged local groups could be an indicator for an attacker trying to gain persistence.

- Changes to the audit policy can be an indication for an attacker trying to cover their traces, for example, by preventing logging of specific events (logged in event ID 4719).
- Changes to the Windows Defender Firewall may indicate that an attacker or malware is trying to establish a communication channel (which may have been prevented by the current configuration) for data exfiltration or downloading additional malware modules.

To allow for the logging of configuration changes in the aforementioned areas (security groups, policies, Windows Defender Firewall), the following recommendations should be implemented.

5.3.1 Windows Logs

This section provides recommendations for the configuration of the System and Security logs that are configurable via Group Policy.

5.3.1.1 Ensure "'Audit Security Group Management" is set to "Success".

Description, configuration recommendation and impact identical to 17.2.3 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_sgm, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Account Management

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4731: A security-enabled local group was created.	This event is generated when a new security-enabled local group is created.
4732: A member was added to a security-enabled local group.	This event is generated when a new account is added to a security-enabled local group.
4733: A member was removed from a security-enabled local group.	This event is generated when an account is removed from a security-enabled local group.
4734: A security-enabled local group was deleted.	This event is generated when a security-enabled local group is deleted.
4735: A security-enabled local group was changed.	This event is generated when attributes of a security-enabled local group are changed.
4799: A security-enabled local group membership was enumerated.	This event is generated when a process attempts to list the members of a security-enabled local group.

5.3.1.2 Ensure "'Audit Audit Policy Change" is set to include "Success"

Description, configuration recommendation and impact identical to 17.7.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_apc, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Policy Change

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4715: The audit policy (SACL) on an object was changed.	This event is generated when the System Access Control List (SACL) of the local audit policy is changed.
4719: System audit policy was changed.	This event is generated when settings of the computer's audit policy are changed.
4817: Auditing settings on object were changed.	This event is generated when the global object access audit policy on a computer is changed.
4907: Auditing settings on object were changed.	This event is generated when the System Access Control List (SACL) of an object (for example, a Registry key or a file) has been changed.
4908: Special Groups Logon table modified.	This event is generated when the list of special groups is updated in the registry or via security policies.

5.3.1.3 Ensure “Audit Authentication Policy Change” is set to include “Success”

Description, configuration recommendation and impact identical to 17.7.2 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_authpc, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Policy Change

Default Value
Success

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4670: Permissions on an object were changed.	This event is generated when the Access Control List (ACL) of an object is changed.
4717: System security access was granted to an account.	This event is generated when the local logon user rights policy is changed, and an account is granted logon rights.

Event ID: Name	Rationale
4718: System security access was removed from an account.	This event is generated when the local logon user rights policy is changed, and the logon privilege is removed from an account.
4739: Domain Policy was changed.	This event is generated when any of the following changes are made to the local computer's security policy: • The settings under *Security Settings\Account Policies\Account Lockout Policy* were changed. • The settings under *Security Settings\Account Policies\Password Policy* were changed. • The Group Policy setting *Network security: Force logoff when logon hours expire* was changed. • Domain attributes, e.g., *ms-DS-MachineAccountQuota* (ms_domain_attribute_max_join, 2021) or *msDS-Behavior-Version* (ms_attribute_dfl, 2021), were changed.

5.3.1.4 Ensure “Audit Authorization Policy Change” is set to include “Success”

Description, configuration recommendation and impact identical to 17.7.3 of the CIS Benchmark. No configuration recommendation in the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Policy Change

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4703: A user right was adjusted.	This event is generated when token privileges are enabled or disabled.
4704: A user right was assigned.	This event is generated when privileges are added to a token.
4705: A user right was removed.	This event is generated when privileges are revoked from a token.
4670: Permissions on an object were changed.	This event is generated when the Access Control List (ACL) of an object (e.g., a Registry key or file) is changed.
4911: Resource attributes of the object were changed.	This event is generated when resource attributes of the file system object are changed
4913: Central Access Policy on the object was changed.	This event is generated when the central access policy for the file system object is changed. This event is generated regardless of the object's auditing policy settings.

5.3.1.5 Ensure “Audit MPSSVC Rule-Level Policy Change” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.7.4 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Policy Change

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4944: The following policy was active when the Windows Firewall started.	This event is generated when the Windows Firewall service (MpsSvc) is started. The event displays the public profile settings that were in effect at startup.
4945: A rule was listed when the Windows Firewall started.	This event is generated when the Windows Firewall service (MpsSvc) is started. The event displays the incoming and / or outgoing rule of the public profile that were effective at startup.
4946: A change has been made to Windows Firewall exception list. A rule was added.	This event is generated when a new local rule is added to the Windows Firewall. This event is not generated when a new rule is added by Group Policy.
4947: A change has been made to Windows Firewall exception list. A rule was modified.	This event is generated when a local Windows Firewall rule is changed. This event is not generated when the rule is changed by Group Policy.
4948: A change has been made to Windows Firewall exception list. A rule was deleted.	This event is generated when a local Windows Firewall rule is deleted. This event is not generated when the rule is deleted by Group Policy.
4949: Windows Firewall settings were restored to the default values.	This event is generated when the local Windows Firewall settings are reset to the default configuration.
4950: A Windows Firewall setting has changed.	This event is generated when the local Windows Firewall settings are changed. This event is not generated when the settings are changed by Group Policy.
4951: A rule has been ignored because its major version number was not recognized by Windows Firewall.	This event is generated when the version (i.e., structure) of a Windows Firewall rule cannot be interpreted and implemented by the firewall engine.
4952: Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced.	This event is generated when the version (i.e., structure) of a Windows Firewall rule can only be partially interpreted and implemented by the firewall engine.
4953: Windows Firewall ignored a rule because it could not be parsed.	This event is generated when a Windows firewall rule cannot be interpreted and implemented by the firewall engine.

Event ID: Name	Rationale
4954: Windows Firewall Group Policy settings have changed. The new settings have been applied.	This event is generated when the Windows Firewall Group Policy settings are changed or updated.
4956: Windows Firewall has changed the active profile.	This event is generated when Windows Firewall has changed the active profile.
4957: Windows Firewall did not apply the following rule.	This event is generated when Windows Firewall fails to apply a rule at startup or when applying a new rule.
4958: Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer.	This event is generated when Windows Firewall processes a rule that contains parameters that cannot be processed on the local computer.

5.3.1.6 Ensure “Audit Other Policy Change Events” is set to include “Failure”

Description, configuration recommendation and impact identical to 17.7.5 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Policy Change

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4826: Boot Configuration Data loaded.	This event is generated when the system boots and the current Boot Configuration Data (BCD) settings are read and implemented.
4909: The local policy settings for the TBS were changed.	This event is generated when a change is made to the TPM configuration in the computer's local policy object.
4910: The group policy settings for the TBS were changed.	This event is generated when a change is made to the TPM configuration via a Group Policy object.
6144: Security policy in the group policy objects has been applied successfully.	This event is generated when settings from the Security Options section of the Group Policy object could be applied to a computer without error.
6145: One or more errors occurred while processing security policy in the group policy objects.	This event is generated when settings from the Security Options section of the Group Policy object could not be applied to a computer without error.

5.3.1.7 Ensure the ETW Provider “TPM“ is enabled

This provider generates events related to the TPM chip.

Configuration Path in the Registry Editor

Ensure under the Registry path `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System\{1b6b0772-251b-4d42-917d-faca166bc059}` the entry:

- `Enabled` is set to `1` (enables the ETW Provider).

Default Value
Enabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
20	This event is generated when the TPM lock counter is reset.
21	This event is generated when the TPM returns an authorization error when executing a TPM command, which may result in a TPM lockout.
23	This event is generated when the execution of a TPM command is temporarily blocked due to too many previous authorization errors.

Note: The aforementioned events are stored in the Windows "System" log.

5.3.1.8 Ensure the ETW Provider “Microsoft-Windows-TPM-WMI“ is enabled

This provider generates events related to the TPM chip.

Configuration Path in the Registry Editor

Ensure under the Registry path `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System\{7d5387b0-cbe0-11da-a94d-800200c9a66}` the entry:

- `Enabled` is set to `1` (enables the ETW Provider).

Default Value
Enabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
769	This event is generated when the configuration of the so-called TPM Owner Authorization changes.
1025	This event is generated when the TPM is successfully provisioned.

Event ID	Rationale
1027	This event is generated when the TPM is taken possession of by the system with the help of the TPM command TakeOwnership.
1793	This event is generated when a deletion of the TPM is scheduled by the system.

Note: The aforementioned events are stored in the Windows "System" log.

5.3.2 Application and Services Logs

This section provides recommendations for the configuration of the Applications and Services logs that are not configurable via Group Policy, but the settings can be distributed via Group Policy objects.

5.3.2.1 Ensure the log "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" is enabled and configured

This event log contains events related to the configuration of Windows Defender Firewall. Windows Defender Firewall is a software firewall integrated into the Windows operating system.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log “Microsoft-Windows-Windows Firewall With Advanced Security/Firewall” /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 1,028 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
2032	This event is generated when the Windows Firewall local configuration is reset to the default configuration.
2002	This event is generated when a local Windows firewall setting is changed.
2006	This event is generated when a local Windows Firewall rule is deleted.
2033	This event is generated when all local Windows firewall rules are disabled.
2005	This event is generated when a local Windows firewall rule is changed.
2008	This event is generated when Windows Firewall Group Policy settings are successfully applied.
2009	This event is generated when Windows Firewall Group Policy settings fail to load.
2003	This event is generated when a local Windows firewall profile setting is changed.

Event ID	Rationale
2004	This event is generated when a new local rule is added to the Windows Firewall.
2010	This event is generated when the Windows firewall profile of a network adapter is changed.

5.3.2.2 Ensure the log "Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose" is enabled and configured

This event log contains events related to the operational state of Windows Defender Firewall. Windows Defender Firewall is a software firewall integrated into the Windows operating system.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log “Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose” /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Disabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
2001	This event is generated when a Windows Firewall profile setting is applied.
2007	This event is generated when the Windows Firewall service (MpsSvc) interprets a rule at startup.
2000	This event is generated when a Windows Firewall rule is read at system startup.

5.4 Network Activity

The following section describes configuration recommendations and associated events related to incoming and outgoing network traffic. The logging of network activity is used to make communication connections to other systems visible. This can enable the detection of initial (attempted) attacks by logging connections to known phishing websites or malware infected websites.

After a compromise has occurred, there may also be other noticeable network connections, such as malware or attacker communication to suspicious systems outside of their own network environment, such as (known) command and control servers (computer that issues instructions to malware-infected systems). Network connections within the internal network can also provide information about an ongoing attack in which malware or an attacker is spreading across the network. Here, it can be difficult to distinguish legitimate network connections from those of an attacker.

After the compromise of a system was identified, logging of network connections presents an important basis for the forensic analysis of the security incident.

Exemplary scenarios that can be detected by logging and evaluating network activity can include:

- Domain Name System-based attacks, such as local DNS hijacking, in which the IP address of the DNS server is set to a malicious value in the system's network settings, compromising communications, can follow initial attack steps.
- Indications of (attempted) man-in-the-middle attacks (an attack technique in which an attacker controls traffic between two or more network participants by logically or physically putting themselves in between them) on SMB connections on the internal network can be provided by events related to failed signature verification or encryption, such as an (attempted) downgrade to SMB 2.0.
- Anomalies such as unusual processes that accept or establish network connections as well as system services that are bound to an unintended port.

The following recommendations should be implemented to ensure the logging of events corresponding to DNS and SMB activity.

Note: Settings for logging data that is related to allowed and dropped packets by the Windows Defender Firewall are described in section 4.2.

5.4.1 Application and Services Logs

This section provides recommendations for the configuration of the Applications and Services logs that are not configurable via Group Policy, but the settings can be distributed via Group Policy objects.

5.4.1.1 Ensure the log "Microsoft-Windows-DNS Client Events/Operational" is enabled and configured

This event log contains events related to Windows Domain Name System (DNS) client. Among other things, all name resolutions and errors during name resolution are logged in this event log.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log “Microsoft-Windows-DNS Client Events/Operational” /enabled:true /retention:false /maxsize:201326592` to activate and configure the log.

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

Default Value
Disabled

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
1001	This event is generated when theDNS server information is configured on a network interface
3008	This event is generated when a DNS query is completed.
3009	This event is generated when a DNS query is indexed.

Event ID	Rationale
3010	This event is generated when a DNS query is sent to a DNS server.
3011	This event is generated when a DNS query is received from a DNS server.

5.4.1.2 Ensure the log "Microsoft-Windows-SMBClient/Connectivity" is enabled and configured

This event log contains information about monitoring the Windows Server Message Block (SMB) client. The Windows SMB client is required to access shares.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-SMBClient/Connectivity /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 8,192 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
30803	This event is generated when the system cannot establish a network connection to the target system.
30800	This event is generated when the system cannot successfully resolve the server name of the target system.
30804	This event is generated when the SMB connection to the target system is disconnected.
30816	This event is generated when the system and the target server cannot negotiate a common SMB version.

5.4.1.3 Ensure the log "Microsoft-Windows-SMBClient/Security" is enabled and configured

This event log contains information about monitoring the Windows Server Message Block (SMB) client. The Windows SMB client is required to access shares.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-SMBClient/Security /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value

Enabled (max. log size: 8,192 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
31002	This event is generated when a network token cannot be used for outgoing authentication (usually due to lack of delegation).
31010	This event is generated when the SMB client cannot connect to a share.
31012	This event is generated when the negotiated SMB parameters (such as the SMB version or supported SMB features) fail to be verified when a share is accessed.
31013	This event is generated when the signature verification of SMB messages fails during transfer between server and client.
31014	This event is generated when the client receives an unencrypted message but an encrypted one is expected.
31017	This event is generated when the server tries to log on the user as an unauthenticated guest.

5.4.1.4 Ensure the log "Microsoft-Windows-SMBServer/Operational" is enabled and configured

This event log contains information about monitoring the Windows Server Message Block (SMB) server. The Windows SMB server is required to provide shares.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-SMBServer/Security /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value

Enabled (max. log size: 8,192 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
1001	This event is generated when a client's attempt to access the server via SMB Version 1 is rejected.
1003	This event is generated when a client's attempt to send unencrypted data to the server is rejected.
1004	This event is generated when a client's attempt to send a incorrectly signed message to the server is rejected.
1005	This event is generated when verification of the negotiated SMB parameters (such as the SMB version or

Event ID	Rationale
	supported SMB features) between the client and server fails.

5.4.1.5 Ensure the log "Microsoft-Windows-SMBServer/Security" is enabled and configured

This event log contains information about monitoring the Windows Server Message Block (SMB) server. The Windows SMB server is required to provide shares.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-SMBServer/Security /enabled:true /retention:false /maxsize:33554432` to activate and configure the log.

Default Value
Enabled (max. log size: 8,192 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
551	This event is generated when authentication failed during a SMB connection attempt.
1006	This event is generated when access to a share has failed due to insufficient permissions.
1009	This event is generated when access to a share without credentials is attempted and denied by the server.

5.5 Process Activity

A process is the instantiation of a program at runtime under the control of the operating system. Ultimately, any execution of code leads to the creation of a process. The following section describes events that are generated when creating or starting processes, and in particular when using Windows PowerShell, which provides a way of interacting with the computer system that is also used by attackers. Logging these is intended to make activities of users and applications as well as attackers visible and allow an understanding of how a system is used. See also the sections 4.3.3 and 4.3.4.

Logging the process creation helps to understand which account created a process, as well as which token extension type (this indicates whether and how the User Account Control was used at the process start) and which integrity level (this controls, in addition to concrete object permissions, the access control) are assigned to a process. Furthermore, logging can be used to record in which folder a process was started. This can be used in exemplary log analysis scenarios as follows:

- The Token Elevation Type field of the 4688 event can be used to identify when accounts, for which User Account Control is disabled, trigger processes (TokenElevationTypeDefault (1)) and when processes were run with administrative privileges and User Account Control was enabled (TokenElevationTypeFull (2)). This can be useful for reconstructing the actions of an account after it has been compromised.

- Anomalies in execution, such as starting a privileged process from the temp folder, can be monitored. This can be useful for detecting or forensically reconstructing attacks based on malware execution.
- The execution of known standard versions of malware (e.g., *mimikatz*) can additionally be detected based on the process name and associated process parameters, which are also part of event ID 4688.

Logging Windows PowerShell activities, which can be used by attackers both to compromise a system and to subsequently continue accessing a system, provides the ability to track in detail actions performed via PowerShell. The logged information can be useful in gaining insight into an attacker's actions (see section 4.3.4). Moreover, depending on the legitimate use of a system, even the (attempted) use of Windows PowerShell can be suspicious.

To enable logging of necessary data for process creation and PowerShell activity, the following configuration recommendations should be implemented.

5.5.1 Windows Logs

This section provides recommendations for the configuration of the System and Security logs that are configurable via Group Policy.

5.5.1.1 Ensure “Audit Process Creation” is set to include “Success”

Description, configuration recommendation and impact identical to 17.3.2 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Note: This event category does not contain Failure events (see (ms_pc, 2021)*).*

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Detailed Tracking

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4688: A new process has been created.	This event is generated when a process is started.

5.5.1.2 Ensure “Audit Sensitive Privilege Use” is set to “Success and Failure”

Description, configuration recommendation and impact identical to 17.8.1 of the CIS Benchmark. Configuration recommendation identical to the Microsoft Security Baseline.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Privilege Use

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4673: A privileged service was called.	This event is generated when a process attempts to execute a privileged system service operation that requires one of the following privileges: *SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeCreateTokenPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege, SeLockMemoryPrivilege, SeSystemEnvironmentPrivilege, SeTcbPrivilege, SeEnableDelegationPrivilege*.
4674: An operation was attempted on a privileged object.	This event is generated when a process attempts to request an existing privileged object that requires one of the following privileges: *SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeCreateTokenPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege, SeLockMemoryPrivilege, SeSystemEnvironmentPrivilege, SeTcbPrivilege, SeEnableDelegationPrivilege*.

5.5.2 Application and Services Logs

This section provides recommendations for the configuration of the Applications and Services logs that are not configurable via Group Policy, but the settings can be distributed via Group Policy objects.

5.5.2.1 Ensure the log "Microsoft-Windows-PowerShell/Operational" is enabled and configured

This event log contains recordings of PowerShell activity if logging of PowerShell script blocks is enabled.

Note: This event log may contain sensitive information, as any processed code is logged. For example, if the code contains passwords, they will be logged in plain text.

Log Configuration via wevtutil.exe

Execute on a command line the following command `wevtutil.exe set-log Microsoft-Windows-PowerShell/Operational /enabled:true /retention:false /maxsize:536870912` to activate and configure the log.

Note: Depending on the usage of the system, the recommended log size configuration may not be sufficient as potentially a very high number of events are logged in a short time. In such a case, the log size should be increased beyond the recommended value or, ideally, the log data should be collected centrally.

Default Value
Enabled (max. log size: 15,360 KB)

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID	Rationale
4100	This event is generated when an error occurs during processing within PowerShell, for example, when a script cannot be executed due to the Execution Policy.
4103	This event is generated when a PowerShell command is invoked.
4104	This event is generated when PowerShell interprets a script block.
24577	This event is generated when the PowerShell Integrated Scripting Environment (ISE) executes a PowerShell script.
40961	This event is generated when a PowerShell console is indexed.
40962	This event is generated when a PowerShell console is ready to receive user input.

5.6 Registry Activity

The Registry of a Windows system is a hierarchical database in which all configuration parameters relevant to the administration of the system, as well as integrated system services and processes, and in some cases the settings for applications are stored. The integrity of the Registry is thus central to the health and security of a system, and changes to the Registry should be logged at relevant points.

This section describes the configuration of logging security-related changes to Registry objects that are not covered or only partially covered by other logging events described in the previous sections. Registry changes are a way for attackers to achieve persistence on a system after a successful compromise. Example scenarios that can be covered by analyzing logged data for specific registry keys include:

- Registry keys that trigger automatic execution of certain malware or commands every time a user logs on or boots the system.
- Registry keys that can be used for the registration of new system services or drivers.
- Registry keys that extend user authentication with new protocols or password filters.

Legitimate changes to these Registry key entries usually occur when legitimate software is installed. If this is not the case, it could have been triggered by the actions of an attacker or malware. Conspicuous Registry changes can also be correlated with other events, such as conspicuous network connections after a user logs on.

The following recommendations should be configured to enable logging of Registry activity in general and to monitor specific Registry keys for modification.

5.6.1 Windows Logs

This section provides recommendations for the configuration of the System and Security logs that are configurable via Group Policy.

5.6.1.1 Ensure “Audit Registry” is set to “Success”

This setting enables Registry auditing.

Note: A corresponding event in the log is generated only for objects for which a so-called System Access Control List (SACL) has been configured (see section 5.6.1.2).

Rationale

Since the registry is an essential part of the Windows operating system and holds security-critical configurations that are modified by attackers, e.g., for persistence, changes to relevant Registry objects should be logged.

Impact

When this setting is enabled, an event is generated for each successful attempt to access a Registry object with matching *System Access Control List* while using an account.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Advanced Audit Policy Configuration\Object Access

Default Value
No auditing

Relevant Event IDs

The following exemplary events are recorded by the recommended configuration:

Event ID: Name	Rationale
4657: A registry value was modified.	This event is generated when a value for a Registry key has been successfully changed.
4660: An object was deleted.	This event is generated when a Registry object is successfully deleted.
4670: Permissions on an object were changed.	This event is generated when the permissions on a Registry object have been successfully changed.

5.6.1.2 Ensure a SACL is Configured for Relevant Registry Objects

The following settings enable auditing for specific registry objects.

Rationale

To generate corresponding events for Registry auditing in the event log, the so-called *System Access Control List* (SACL) must be configured for security-relevant objects.

Impact

When these settings are enabled, an event is generated for each successful attempt to access the named Registry objects while using an account.

Configuration Path in the Group Policy Editor

Computer Configuration\Windows Settings\Security Options\Registry

Ensure for the following Registry keys that the following auditing entries (after selecting the Registry key click on “Advanced” and select the tab “Auditing”, then click on “Add”) are configured:

- Principal: “Everyone”
- Type: “Success”
- Applies to: “This key only” **or** “This key and subkeys”
- Advanced permissions: “Set value”, “Create Subkey”, “Delete”, “Write DAC”, “Write Owner”

Note: This configuration path exists only when modifying Group Policy objects in an Active Directory domain. On standalone systems, the following settings must be applied manually through the Registry Editor (using the permissions menu for registry keys) or through a PowerShell script (using the Set-Acl command). An example configuration would look as follows:

Execute the following commands in an administrative PowerShell session:

Specify the path to the Registry key to be configured:

```
$Path = "HKLM:\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Accessibility\ATs"
```

Read and temporarily store the current System Access Control List of the key to be configured:

```
$ACL = Get-Acl $Path -Audit
```

Create a new object that contains the relevant configuration for auditing:

```
$AuditRule = New-Object
System.Security.AccessControl.RegistryAuditRule("Everyone",
"SetValue,CreateSubKey,Delete,ChangePermissions,TakeOwnership","None","None"
, "Success")
```

Add the new audit entries to the temporarily stored Access Control List:

```
$ACL.AddAuditRule($AuditRule)
```

Apply the new configuration to the current Registry key:

```
Set-Acl -AclObject $ACL -Path $Path
```

For applying the setting “Applies to: This key and subkeys” the creation of the object carrying the audit entries must be modified as follows:

```
$AuditRule = New-Object
System.Security.AccessControl.RegistryAuditRule("Everyone",
"SetValue,CreateSubKey,Delete,ChangePermissions,TakeOwnership",
"ContainerInherit", "None", "Success")
```

Relevant Registry Objects

The following Registry keys should be audited via the recommended entries:

Registry Key	Rationale
Applies to: This key only	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs	When a new application is registered for ease of access, subkeys are generated at this location.
HKLM\SYSTEM\CurrentControlSet\Control\Lsa	When user authentication is extended with new protocols or password filters, subkeys are generated at this location.
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders	When a new cryptographic provider is registered, subkeys are generated at this location.
HKLM\SYSTEM\CurrentControlSet\Services	When a new service or driver is registered, subkeys are generated at this location.
Applies to: This key and subkeys	
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnceEx HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd (especially the Registry value *StartupPrograms*) HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp (especially the Registry value *InitialProgram*)	When an application is configured to run automatically when a user logs on, subkeys are created or registry values are modified at these locations.
HKLM\SOFTWARE\Microsoft\Active	When an application is configured to run

Registry Key	Rationale
Setup\Installed Components HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	automatically before loading the desktop via *Active Setup*, subkeys are generated at these locations.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	When configuring the behavior of the user logon process (including the configuration of which applications are initially launched), Registry values are modified at this location.
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot (especially the Registry value *AlternateShell*)	When the safe mode behavior is configured, this registry value is modified.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Shell HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logoff HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Startup HKLM\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Shutdown HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown	When a script or application is configured to run automatically via Group Policy, the configuration is stored in those locations.
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run HKCU\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Runonce HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunonceEx HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Load HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Run HKCU\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon (especially the	Similar to the system-wide configurations for applications that are automatically executed when a user logs on, subkeys are created or Registry values are modified at these locations for user-specific settings. *Note: These Registry paths are specific to each logged in user.*

Registry Key	Rationale
Registry value *Shell*) HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System (especially the Registry value *Shell*) HKCU\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon HKCU\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logoff	

Appendix

Tools Used

Tool	Availability and Description
Local Group Policy Editor	*Availability:* Included with Windows 10 *Description:* A tool for configuring Group Policy settings.
Event Viewer	*Availability:* Included with Windows 10 *Description:* A tool for viewing and configuring event logs.
Registry Editor	*Availability:* Included with Windows 10 *Description:* A tool for configuring the Registry.

Event IDs

Event IDs: Section 5.1.2.1

Event ID	Message
100	The security package does not cache the credentials needed to authenticate to the server. Package Name: %1 User Name: %2 Domain Name: %3 Server Name: %4 Protected User: %5 Error Code: %6
200	A security package received a network logon request after the logoff completed. User Name: %1 Domain Name: %2 Logon ID: %3 Logoff Time: %4 PID: %5 Program: %6 Principal Name: %7 Server Name: %8 Package Name: %9 Call Type: %10 Error Code: %11
300	Groups assigned to a new logon. New Logon: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon GUID: %5 Event in sequence: %6 of %7 Group Membership: %8
301	Claims assigned to a new logon. New Logon: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon GUID: %5 Logon Type: %6

Event ID	Message
	Event in sequence: %7 of %8 User Claims: %9 Device Claims: %10 This event is generated when a new logon session is created and the user token associated with it contains user and/or device claims. The New Logon fields indicate the account that was logged on. If all the user and device claims in the user token cannot be accommodated in a single event, multiple such events are generated. The Event in sequence field indicates how many more events are generated for this logon session. Each user or device claim is represented in the following format: ClaimID ClaimTypeID : Value1, Value2 à The common claim types are: 0 (Invalid Type), 1 (64-bit Integer, 2 (Unsigned 64-bit Integer), 3 (String), 4 (FQBN), 5 (SID), 6 (Boolean) and 16 (Blob). If the claim value exceeds the max allowed length then the string is terminated by ...
302	User %1 logged off notification is received. LogonId: %2 AuthorityName: %3 AccountName: %4 Timeout: %5 seconds
303	The security package does not cache the user's sign on credentials. Package Name: %1 User Name: %2 Domain Name: %3 Protected User: %4
320	Automatic restart sign on successfully configured the autologon credentials for: Account Name: %1 Account Domain: %2
321	Automatic restart sign on failed to configure the autologon credentials with error: %1
322	Automatic restart sign on successfully deleted autologon credentials from LSA memory.

Event IDs: Section 5.1.2.2

Event ID	Message
258	Listener %1 has started listening
259	Listener %1 has stopped listening
261	Listener %1 received a connection
262	Listener %1 has been asked to stop listening
1003	The remote desktop client '%1' has provided an invalid license.
1004	The Remote Desktop Session Host server cannot issue a client license. It was unable to issue the license due to a changed (mismatched) client license, insufficient memory, or an internal error. Further details for this problem may have been reported at the client's computer.
1011	The remote session could not be established from remote desktop client %1 because its temporary license has expired.
1136	RD Session Host Server role is not installed.
1137	The roaming user profile cache manager for Remote Desktop Services could not start. Error Code: %1
1140	The "Limit the size of the entire roaming user profile cache" Group Policy setting has been enabled, but the roaming user profile cache manager for Remote Desktop Services has encountered a problem. Error Code: %1

Event ID	Message
1141	The "Limit the size of the entire roaming user profile cache" Group Policy setting has been disabled, but the roaming user profile cache manager for Remote Desktop Services has encountered a problem. Error Code: %1
1142	The "Limit the size of the entire roaming user profile cache" Group Policy setting has been enabled.
1143	The "Limit the size of the entire roaming user profile cache" Group Policy setting has been disabled.
1145	The roaming user profile cache manager for Remote Desktop Services deleted the roaming user profile for the user %1 because the roaming user profile cache exceeded the %2 gigabyte limit.
1146	Remote Desktop Services: Remote control session initiated: %1 initiated a remote control session: User: %2 Domain: %3
1147	Remote Desktop Services: Remote control session connection succeeded: %1 initiated a remote control session: User: %2 Domain: %3
1148	Remote Desktop Services: Remote control session connection failed: %1 initiated a remote control session: User: %2 Domain: %3
1149	Remote Desktop Services: User authentication succeeded: User: %1 Domain: %2 Source Network Address: %3
1151	The remote user's connection was declined by the logged on user. User Account: %2 Domain: %1 Source IP Address: %3
1152	Failed to create KVP sessions string. Error Code %1
1153	Failed to write KVP sessions string. Error Code %1
1155	The Remote Connection Manager selected Kernel mode RDP protocol stack.
1156	The Remote Connection Manager selected User mode RDP protocol stack.
20503	Shadow View Session Started User %1 on computer %2 viewing user %3 (Session ID: %4)
20504	Shadow View Session Stopped User %1 on computer %2 viewing user %3 (Session ID: %4)
20506	Shadow Control Session Started User %1 on computer %2 controlling user %3 (Session ID: %4)
20507	Shadow Control Session Stopped User %1 on computer %2 controlling user %3 (Session ID: %4)

Event ID	Message
20508	Shadow View Permission Granted User %1 (Session ID: %3) granted permission to user %2
20509	Shadow View Permission Denied User %1 (Session ID: %3) denied permission to user %2
20510	Shadow Control Permission Granted User %1 (Session ID: %3) granted permission to user %2
20511	Shadow Control Permission Denied User %1 (Session ID: %3) denied permission to user %2
20512	Shadow Session Failure User %2 encountered error %3 trying to shadow user %1 (Session ID: %4)
20513	Shadow Session Failure User %2 was unable to shadow user %1 (Session ID: %3) because of group policy settings.
20514	Shadow Session Failure User %2 was unable to shadow user %1 (Session ID: %3) because that session is already being shadowed.
20522	Shadow Session Clipboard Copy Request User %1 on computer %2 controlling user %3 (Session ID: %4) Clipboard format: %5
20523	Connection from listener %1 will have terminal class of %2
50180	The remote session could not be established from remote desktop client %1 because its license could not be renewed.
50304	The Remote Desktop Virtualization Host server cannot issue a client license. It was unable to issue the license due to a changed (mismatched) client license, insufficient memory, or an internal error. Further details for this problem may have been reported at the client's computer.

Event IDs: Section 5.1.2.3

Event ID	Message
16	Local Multi-User session manager failed to start. The relevant status code was %1.
17	Remote Desktop Service start failed. The relevant status code was %1.
18	Remote Desktop Service is shutdown for unknown reason. Will recover in one minute.
19	Registering with Service Control Manager to monitor Remote Desktop Service status failed with %1, retry in ten minutes.
20	Attempt to send %1 message to Windows video subsystem failed. The relevant status code was %2.
21	Remote Desktop Services: Session logon succeeded: User: %1 Session ID: %2 Source Network Address: %3
22	Remote Desktop Services: Shell start notification received: User: %1 Session ID: %2

Event ID	Message
	Source Network Address: %3
23	Remote Desktop Services: Session logoff succeeded: User: %1 Session ID: %2
24	Remote Desktop Services: Session has been disconnected: User: %1 Session ID: %2 Source Network Address: %3
25	Remote Desktop Services: Session reconnection succeeded: User: %1 Session ID: %2 Source Network Address: %3
32	Plugin %1 has been successfully initialized
33	Plugin %1 failed to initialize, error code %2
34	Remote Desktop Services is not accepting logons because setup is running.
35	The client process ID %1 could not complete the session change notification event sent by the Remote Desktop service. The Remote Desktop service will not send any more session change notifications.
36	An error occurred when transitioning from %3 in response to %5. (ErrorCode %6)
37	Invalid state transition from %3 in response to %5. (ErrorCode %6)
39	Session %1 has been disconnected by session %2
40	Session %1 has been disconnected, reason code %2
41	Begin session arbitration: User: %1 Session ID: %2
42	End session arbitration: User: %1 Session ID: %2
43	Windows Subsystem has taken too long to process Connect event for session %1
44	Windows Subsystem has taken too long to process Disconnect event for session %1
45	Windows Subsystem has taken too long to process Terminate event for session %1
48	Remote Connection Manager has taken too long to process logon message for session %1
49	Remote Connection Manager has taken too long to prepare for session arbitration for session %1
50	Remote Connection Manager has taken too long to process begin-connect-message for session %1
51	Remote Connection Manager has taken too long to process end-connect-message for session %1
52	Remote Connection Manager has taken too long to process begin-disconnect-message for session %1
53	Remote Connection Manager has taken too long to process end-disconnect-message for session %1
54	Local multi-user session manager received system shutdown message
55	Remote Desktop Service has taken too long to start up

Event ID	Message
56	Remote Desktop Service has taken too long to shutdown
59	%s from %S(#0x%x/0x%x)
60	Glass session %1 has been reconnected to a remote protocol, this session can now only be reconnect locally or from same remote protocol

Event IDs: Section 5.2.2.1

Event ID	Message
10	For more details for this event, please refer to the "Details" section
11	For more details for this event, please refer to the "Details" section
12	For more details for this event, please refer to the "Details" section
13	For more details for this event, please refer to the "Details" section
14	For more details for this event, please refer to the "Details" section
15	For more details for this event, please refer to the "Details" section
16	For more details for this event, please refer to the "Details" section
17	For more details for this event, please refer to the "Details" section
18	For more details for this event, please refer to the "Details" section
19	For more details for this event, please refer to the "Details" section
20	For more details for this event, please refer to the "Details" section
21	For more details for this event, please refer to the "Details" section
22	For more details for this event, please refer to the "Details" section
23	For more details for this event, please refer to the "Details" section
24	For more details for this event, please refer to the "Details" section
30	For more details for this event, please refer to the "Details" section
40	For more details for this event, please refer to the "Details" section
41	For more details for this event, please refer to the "Details" section
42	For more details for this event, please refer to the "Details" section
50	For more details for this event, please refer to the "Details" section
51	For more details for this event, please refer to the "Details" section
52	For more details for this event, please refer to the "Details" section
53	For more details for this event, please refer to the "Details" section
60	For more details for this event, please refer to the "Details" section
70	For more details for this event, please refer to the "Details" section
71	For more details for this event, please refer to the "Details" section
80	For more details for this event, please refer to the "Details" section
81	For more details for this event, please refer to the "Details" section
82	For more details for this event, please refer to the "Details" section
90	For more details for this event, please refer to the "Details" section

Event IDs: Section 5.2.2.2

Event ID	Message
3001	Code Integrity determined an unsigned kernel module %2 is loaded into the system. Check with the publisher to see if a signed version of the kernel module is available.

Event ID	Message
3002	Code Integrity is unable to verify the image integrity of the file %2 because the set of per-page image hashes could not be found on the system.
3003	Code Integrity is unable to verify the image integrity of the file %2 because the set of per-page image hashes could not be found on the system. The image is allowed to load because kernel mode debugger is attached.
3004	Windows is unable to verify the image integrity of the file %2 because file hash could not be found on the system. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source.
3005	Code Integrity is unable to verify the image integrity of the file %2 because a file hash could not be found on the system. The image is allowed to load because kernel mode debugger is attached.
3010	Code Integrity was unable to load the %2 catalog. Status %3.
3021	Code Integrity determined a revoked kernel module %2 is loaded into the system. Check with the publisher to see if a new signed version of the kernel module is available.
3022	Code Integrity determined a revoked kernel module %2 is loaded into the system. The image is allowed to load because kernel mode debugger is attached.
3023	Windows is unable to verify the integrity of the file %2 because the signing certificate has been revoked. Check with the publisher to see if a new signed version of the kernel module is available.
3024	Windows was unable to update the boot catalog cache file. Status %1.
3026	Code Integrity was unable to load the %2 catalog because the signing certificate for this catalog has been revoked. This can result in images failing to load because a valid signature cannot be found. Check with the publisher to see if a new signed version of the catalog and images are available.
3032	Code Integrity determined a revoked image %2 is loaded into the system. Check with the publisher to see if a new signed version of the image is available.
3033	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements.
3034	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3035	Code Integrity determined a revoked image %2 is loaded into the system. The image is allowed to load because kernel mode debugger is attached.
3036	Windows is unable to verify the integrity of the file %2 because the signing certificate has been revoked. Check with the publisher to see if a new signed version of the kernel module is available.
3037	Code Integrity determined an unsigned image %2 is loaded into the system. Check with the publisher to see if a signed version of the image is available.
3050	Code Integrity completed retrieval of file cache. Status %1.
3051	Code Integrity completed retrieval of file cache. Status %1.
3052	Code Integrity completed retrieval of file cache. Status %1.
3057	Code Integrity completed retrieval of file cache. Status %1.
3058	Code Integrity completed retrieval of file cache. Status %1.
3063	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the security requirements for %5.
3065	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the security requirements for %5. However, due to system policy, the image was allowed to load.

Event ID	Message
3066	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3067	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3068	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy.
3069	Code Integrity was unable to load the weak crypto policy value from registry. Status %1.
3070	Code Integrity was unable to load the weak crypto policy from registry store. Status %1.
3071	Code Integrity was unable to load the weak crypto policies. Status %1.
3072	Code Integrity determined that the kernel module %2 is not compatible with hypervisor enforcement due to it having non-page aligned sections.
3073	Code Integrity determined that the kernel module %2 is not compatible with strict mode hypervisor enforcement due to it having an executable section that is also writable.
3074	Code Integrity was unable to verify a page for a module verified using hypervisor enforcement. Status %1.
3076	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3077	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy.
3078	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3079	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy.
3080	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy. However, due to code integrity auditing policy, the image was allowed to load.
3080	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated Advanced Threat Protection policy. However, due to code integrity auditing policy, the image was allowed to load.
3080	Code Integrity determined that a process (%4) attempted to load %2 that violated Driver policy. However, due to code integrity auditing policy, the image was allowed to load.
3080	Code Integrity determined that a process (%4) attempted to load %2 that violated Driver policy. However, due to code integrity auditing policy, the image was allowed to load.
3081	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated code integrity policy.
3081	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the %5 signing level requirements or violated Advanced Threat Protection policy.
3081	Code Integrity determined that a process (%4) attempted to load %2 that violated Driver policy.
3082	Code Integrity determined kernel module %2 that did not meet the WHQL requirements is loaded into the system. However, due to code integrity auditing policy, the image was allowed to load.
3083	Code Integrity determined kernel module %2 that did not meet the WHQL requirements is loaded into the system. Check with the publisher to see if a WHQL compliant kernel module is available.
3084	Code Integrity will enable WHQL driver enforcement for this boot session. Settings %1. Exemption %2.

Event ID	Message
3085	Code Integrity will disable WHQL driver enforcement for this boot session. Settings %1.
3086	Code Integrity determined that a process (%4) attempted to load %2 that did not meet the signing requirements for Isolated User Mode.
3087	Code Integrity determined that the kernel module %2 is not compatible with hypervisor enforcement. Status %3.
3089	Signature information for another event. Match using the Correlation Id.
3090	Code Integrity testing module %2 against policy %11. Status %3
3091	Code Integrity testing module %2 against policy %11. Status %3
3092	Code Integrity testing module %2 against policy %11. Status %3
3093	other (see event data)
3094	other (see event data)
3095	other (see event data)
3096	other (see event data)
3097	other (see event data)
3098	other (see event data)
3099	other (see event data)
3100	other (see event data)
3101	other (see event data)
3102	other (see event data)
3103	other (see event data)
3104	Windows blocked file %2 which has been disallowed for protected processes.

Event IDs: Section 5.2.2.3

Event-ID	Message
4000	Starting computer boot policy processing for %2. Activity id: %1
4000	Starting computer boot policy processing for %2. Activity id: %1
4001	Starting user logon Policy processing for %2. Activity id: %1
4001	Starting user logon Policy processing for %2. Activity id: %1
4002	Starting policy processing due to network state change for computer %2. Activity id: %1
4002	Starting policy processing due to network state change for computer %2. Activity id: %1
4003	Starting policy processing due to network state change for user %2. Activity id: %1
4003	Starting policy processing due to network state change for user %2. Activity id: %1
4004	Starting manual processing of policy for computer %2. Activity id: %1
4004	Starting manual processing of policy for computer %2. Activity id: %1
4005	Starting manual processing of policy for user %2. Activity id: %1
4005	Starting manual processing of policy for user %2.

Event-ID	Message
	Activity id: %1
4006	Starting periodic policy processing for computer %2. Activity id: %1
4006	Starting periodic policy processing for computer %2. Activity id: %1
4007	Starting periodic policy processing for user %2. Activity id: %1
4007	Starting periodic policy processing for user %2. Activity id: %1
4016	Starting %2 Extension Processing. List of applicable Group Policy objects: (%5) %6
4017	%1 %2
4018	Starting %2 for %1.
4019	Running script name %1.
4115	Group Policy Service started.
4116	Started the Group Policy service initialization phase.
4117	Group Policy Session started.
4126	Group Policy receiving applicable GPOs from the domain controller.
4216	Starting to save policies to the local datastore.
4217	Starting to load policies from the local datastore.
4218	Starting the first WMI query for the policy.
4257	Starting to download policies.
4326	Group Policy is trying to discover the Domain Controller information.
5016	Completed %3 Extension Processing in %1 milliseconds.
5017	%3 %4 The call completed in %1 milliseconds.
5018	Completed %4 for %3 in %1 seconds.
5019	Completed %3 in %1 seconds.
5115	Group Policy Service stopped.
5116	Successfully completed the Group Policy Service initialization phase.
5117	Group policy session completed successfully.
5126	Group Policy successfully got applicable GPOs from the domain controller.
5216	Successfully saved policies to the local datastore.
5217	Successfully loaded policies from the local datastore.
5218	Successfully completed the first WMI query.
5257	Successfully completed downloading policies.
5308	Domain Controller details: Domain Controller Name : %1 Domain Controller IP Address : %2
5309	Computer details: Computer role : %1 Network name : %2
5310	Account details: Account Name : %1 Account Domain Name : %2 DC Name : %3 DC Domain Name : %4
5311	The loopback policy processing mode is %1.
5312	List of applicable Group Policy objects:

Event-ID	Message
	%1
5313	The following Group Policy objects were not applicable because they were filtered out : %1
5314	A %6 link was detected. The Estimated bandwidth is %1 kbps. The slow link threshold is %3 kbps.
5315	Next policy processing for %1 will be attempted in %2 %3.
5320	%1
5321	%1 Parameter: %2
5322	Group Policy waited for %3 milliseconds for the network subsystem at computer boot.
5323	Invalid Error Message.
5324	Group Policy received the notification %1 from Winlogon for session %2.
5325	Group Policy received %1 notification from Service Control Manager.
5326	Group Policy successfully discovered the Domain Controller in %1 milliseconds.
5327	Estimated network bandwidth on one of the connections: %1 kbps.
5331	Service configuration update to standalone was attempted due to the presence of Group Policy client extension %1 that is not part of the operating system and completed with status %3.
5332	Group Policy waited for %3 milliseconds for the Direct Access CorpNet connectivity at computer boot.
5340	The Group Policy processing mode is %1.
5351	Group policy session returned to winlogon.
6000	Invalid Error Message.
6001	Invalid Error Message.
6002	Invalid Error Message.
6003	Invalid Error Message.
6004	Invalid Error Message.
6005	Invalid Error Message.
6006	Invalid Error Message.
6007	Invalid Error Message.
6016	Completed %3 Extension Processing in %1 milliseconds.
6017	Invalid Error Message.
6018	Invalid Error Message.
6019	Invalid Error Message.
6033	Skipped %1 Extension based on Group Policy client-side processing rules. Refer to a Resultant Set of Policy report for more information.
6034	Group Policy changed from synchronous foreground to asynchronous foreground based on slow link detection.
6035	%1 Extension deferred processing until next synchronous foreground. Refer to a Resultant Set of Policy report for more information.
6226	Invalid Error Message.
6308	Invalid Error Message.
6309	Invalid Error Message.
6310	Invalid Error Message.
6311	Invalid Error Message.
6312	Invalid Error Message.
6313	Invalid Error Message.
6314	Group Policy bandwidth estimation failed. Group Policy processing will continue. Assuming %6 link.
6315	Invalid Error Message.

Event-ID	Message
6320	Warning: %1 Warning code %2.
6321	Warning: %1 Parameter: %3 : Warning code %2.
6322	Invalid Error Message.
6323	Group Policy dependency (%1) did not start. As a result, network related features of Group Policy such as bandwidth estimation and response to network changes will not work.
6324	Invalid Error Message.
6325	Invalid Error Message.
6326	Invalid Error Message.
6327	Invalid Error Message.
6330	An unfinished invocation of the Group Policy Client Side Extension %1 from a previous instance of the Group Policy Service was detected. This may indicate that the extension caused the Group Policy Client Service to terminate unexpectedly.
6331	Invalid Error Message.
6332	Invalid Error Message.
6337	Group Policy network connection is via Direct Access.
6338	Group Policy Winlogon status reporting has completed.
6339	Group Policy Winlogon Start Shell handling completed.
6341	A Group Policy setting was used to override the fast/slow link detection.
6342	The network connection is using a WWAN device for connectivity.
6344	Group Policy detected a slow link during sync mode processing.
6345	The connection to DC timed out during the Group Policy sync mode process.
6346	Group Policy switched the sync mode process to async mode.
7000	Computer boot policy processing failed for %3 in %1 seconds.
7000	Computer boot policy processing failed for %3 in %1 seconds.
7001	User logon policy processing failed for %3 in %1 seconds.
7001	User logon policy processing failed for %3 in %1 seconds.
7002	Policy processing due to network state change failed for computer %3 in %1 seconds.
7002	Policy processing due to network state change failed for computer %3 in %1 seconds.
7003	Policy processing due to network state change failed for user %3 in %1 seconds.
7003	Policy processing due to network state change failed for user %3 in %1 seconds.
7004	Manual processing of policy failed for computer %3 in %1 seconds.
7004	Manual processing of policy failed for computer %3 in %1 seconds.
7005	Manual processing of policy failed for user %3 in %1 seconds.
7005	Manual processing of policy failed for user %3 in %1 seconds.
7006	Periodic policy processing failed for computer %3 in %1 seconds.
7006	Periodic policy processing failed for computer %3 in %1 seconds.
7007	Periodic policy processing failed for user %3 in %1 seconds.
7007	Periodic policy processing failed for user %3 in %1 seconds.
7016	Completed %3 Extension Processing in %1 milliseconds.
7017	%3 %4 The call failed after %1 milliseconds.
7018	Script for %3 failed in %1 seconds.
7019	Invalid Error Message.
7117	Group policy session completed with error.
7126	Group Policy could not get applicable GPOs from the domain controller.
7216	Saved policies to the local datastore with error.
7217	Loaded policies from the local datastore with error.
7257	Downloaded policies with error.
7308	Invalid Error Message.

Event-ID	Message
7309	Invalid Error Message.
7310	Invalid Error Message.
7311	Invalid Error Message.
7312	Invalid Error Message.
7313	Invalid Error Message.
7314	Invalid Error Message.
7315	Invalid Error Message.
7320	Error: %1 Error code %2.
7321	Error: %1 Parameter: %3 : Error code %2.
7322	Invalid Error Message.
7323	Invalid Error Message.
7324	Invalid Error Message.
7325	Invalid Error Message.
7326	Group Policy failed to discover the Domain Controller details in %1 milliseconds.
7327	Invalid Error Message.
7331	Service configuration update to standalone was attempted due to the presence of Group Policy client extension %1 that is not part of the operating system and completed with status %3.
7332	Invalid Error Message.
8000	Completed computer boot policy processing for %3 in %1 seconds.
8000	Completed computer boot policy processing for %3 in %1 seconds.
8001	Completed user logon policy processing for %3 in %1 seconds.
8001	Completed user logon policy processing for %3 in %1 seconds.
8002	Completed policy processing due to network state change for computer %3 in %1 seconds.
8002	Completed policy processing due to network state change for computer %3 in %1 seconds.
8003	Completed policy processing due to network state change for user %3 in %1 seconds.
8003	Completed policy processing due to network state change for user %3 in %1 seconds.
8004	Completed manual processing of policy for computer %3 in %1 seconds.
8004	Completed manual processing of policy for computer %3 in %1 seconds.
8005	Completed manual processing of policy for user %3 in %1 seconds.
8005	Completed manual processing of policy for user %3 in %1 seconds.
8006	Completed periodic policy processing for computer %3 in %1 seconds.
8006	Completed periodic policy processing for computer %3 in %1 seconds.
8007	Completed periodic policy processing for user %3 in %1 seconds.
8007	Completed periodic policy processing for user %3 in %1 seconds.
8016	%1 Extension (%2) requests a sync mode process.
9001	This machine is configured to retrieve Group Policy files from a file share in an insecure way. UNC Path: %1 Mutual Authentication Enforced: %2 Integrity Enforced: %3 Guidance: The UNC path contains logon scripts and/or files that control system security policies. Microsoft recommends configuring Windows to require both mutual authentication and integrity when accessing files on this UNC path. For details on configuring Windows machines to require additional security when accessing specific UNC paths, visit http://support.microsoft.com/kb/3000483.

Event IDs: Section 5.2.2.4

Event ID	Message
200	Begin boot start drivers phase
201	End boot start drivers phase
202	Begin system start drivers phase
203	End system start drivers phase
204	OS Loader Start: %1 OS Loader End: %2
204	OS Loader Start: %1 OS Loader End: %2
205	*<Wevtutil does not provide message text for this event ID>*
206	*<Wevtutil does not provide message text for this event ID>*
207	*<Wevtutil does not provide message text for this event ID>*
208	*<Wevtutil does not provide message text for this event ID>*
209	*<Wevtutil does not provide message text for this event ID>*
210	Begin initializing boot start driver %2
211	End initializing boot start driver %2. Status: %3
212	Begin loading driver %2
213	End loading driver %5. Status: %3
214	Begin unloading driver %2
215	End unloading driver %5. Status: %3
216	Begin starting device %2
217	Pending start of device %2
218	End starting device %2 using driver %5. Status: %3
220	Begin querying bus relations for device %2
221	Pending querying bus relations for device %2
222	End querying bus relations for device %2
223	Begin attempting to eject device %2
224	End attempting to eject device %2. Status: %3
226	Begin calling driver initialization routine for driver %2
227	End calling driver initialization routine for driver %2. Status: %3
228	*<Wevtutil does not provide message text for this event ID>*
229	*<Wevtutil does not provide message text for this event ID>*
230	*<Wevtutil does not provide message text for this event ID>*
231	*<Wevtutil does not provide message text for this event ID>*
232	*<Wevtutil does not provide message text for this event ID>*
233	*<Wevtutil does not provide message text for this event ID>*
234	*<Wevtutil does not provide message text for this event ID>*
235	*<Wevtutil does not provide message text for this event ID>*
236	*<Wevtutil does not provide message text for this event ID>*
250	Begin configuration of device %2
251	Pending configuration of device %2
252	End configuration of device %2. Status: %3
260	Begin starting system start drivers part 1
261	End starting system start drivers part 1
262	Begin starting system start drivers part 2
263	End starting system start drivers part 2
264	Begin processing reinitialization requests for boot start drivers
265	End processing reinitialization requests for boot start drivers
266	Begin processing reinitialization requests for system start drivers

Event ID	Message
267	End processing reinitialization requests for system start drivers
270	Begin loading driver database %2
271	Pending loading driver database %2
272	End loading driver database %2
273	Begin unloading driver database %2
274	Pending unloading driver database %2
275	End unloading driver database %2
276	*<Wevtutil does not provide message text for this event ID>*
277	*<Wevtutil does not provide message text for this event ID>*
278	*<Wevtutil does not provide message text for this event ID>*
300	Begin starting initialization of drivers
301	End starting initialization of drivers
400	Device %1 was configured. Driver Name: %2 Class Guid: %3 Driver Date: %4 Driver Version: %5 Driver Provider: %6 Driver Section: %8 Driver Rank: %9 Matching Device Id: %10 Outranked Drivers: %11 Device Updated: %12 Parent Device: %14
401	Device %1 failed configuration. Driver Name: %2 Class Guid: %3 Driver Date: %4 Driver Version: %5 Driver Provider: %6 Driver Section: %8 Driver Rank: %9 Matching Device Id: %10 Outranked Drivers: %11 Device Updated: %12 Status: %13 Parent Device: %14
402	Device %1 had its configuration blocked by policy. Driver Name: %2 Class Guid: %3 Driver Date: %4 Driver Version: %5 Driver Provider: %6 Driver Section: %8 Driver Rank: %9 Matching Device Id: %10 Outranked Drivers: %11 Device Updated: %12 Status: %13

Event ID	Message
	Parent Device: %14
403	Device %1 requires a system reboot to complete configuration. Driver Name: %2 Class Guid: %3 Driver Date: %4 Driver Version: %5 Driver Provider: %6 Driver Section: %8 Driver Rank: %9 Matching Device Id: %10 Outranked Drivers: %11 Device Updated: %12 Status: %13 Parent Device: %14
410	Device %1 was started. Driver Name: %2 Class Guid: %3 Service: %4 Lower Filters: %5 Upper Filters: %6
411	Device %1 had a problem starting. Driver Name: %2 Class Guid: %3 Service: %4 Lower Filters: %5 Upper Filters: %6 Problem: %7 Problem Status: %8
412	Device %1 requires a system reboot before it can be started. Driver Name: %2 Class Guid: %3 Service: %4 Lower Filters: %5 Upper Filters: %6 Problem: %7 Problem Status: %8
420	Device %1 was deleted. Class Guid: %2
421	Device %1 could not be deleted. Class Guid: %2 Problem: %3 Status: %4
430	Device %1 requires further installation.
440	Device %1 was migrated. Last Device Instance Id: %2

Event ID	Message
	Class Guid: %3 Location Path: %4 Migration Rank: %5 Present: %6
441	Device %1 could not be migrated. Last Device Instance Id: %2 Class Guid: %3 Location Path: %4 Migration Rank: %5 Present: %6 Status: %7
442	Device %1 was not migrated due to partial or ambiguous match. Last Device Instance Id: %2 Class Guid: %3 Location Path: %4 Migration Rank: %5 Present: %6 Status: %7
500	*<Wevtutil does not provide message text for this event ID>*
501	*<Wevtutil does not provide message text for this event ID>*
502	*<Wevtutil does not provide message text for this event ID>*
503	*<Wevtutil does not provide message text for this event ID>*
600	A start type override of %3 was set for driver %2 in hardware configuration %1
700	*<Wevtutil does not provide message text for this event ID>*
701	*<Wevtutil does not provide message text for this event ID>*
702	*<Wevtutil does not provide message text for this event ID>*
703	*<Wevtutil does not provide message text for this event ID>*
704	*<Wevtutil does not provide message text for this event ID>*
705	*<Wevtutil does not provide message text for this event ID>*
800	Begin processing new device (%1)
801	Processing device %2 (%1)
802	End processing new device (%1)
807	Begin device add operation for driver %3, device %4
808	End device add, status (%1)
810	Reenumeration of device tree below %1 has been queued.
811	Begin reenumeration of device tree below %1.
812	End reenumeration of device tree below %1.
813	Reenumeration of %1 has been queued.
814	Begin reenumeration of %1.
815	End reenumeration of %1.
816	Configuration of device %1 for configuration type %2 has been queued.
817	Begin configuration of device %1 for configuration type %2.
818	End configuration of device %1 for configuration type %2. Result is %3
819	*<Wevtutil does not provide message text for this event ID>*
820	*<Wevtutil does not provide message text for this event ID>*
821	*<Wevtutil does not provide message text for this event ID>*
830	Removal of %1 has been queued.
831	Begin removal of %1.
832	End removal of %1.

Event ID	Message
840	Begin resetting device %2.
841	End resetting device %2 with status %3, veto type %4, veto name %6.
850	Begin assigning resources to device tree below %1.
851	End assigning resources to device tree below %1.
852	Begin rebalancing resources for device %2.
853	End rebalancing resources for device %2.

Event IDs: Section 5.2.2.5

Event ID	Message
100	Task Scheduler started "%3" instance of the "%1" task for user "%2".
101	Task Scheduler failed to start "%1" task for user "%2". Additional Data: Error Value: %3.
102	Task Scheduler successfully finished "%3" instance of the "%1" task for user "%2".
103	Task Scheduler failed to start instance "%2" of "%1" task for user "%3" . Additional Data: Error Value: %4.
104	Task Scheduler failed to log on "%1" . Failure occurred in "%2" . User Action: Ensure the credentials for the task are correctly specified. Additional Data: Error Value: %3.
105	Task Scheduler failed to impersonate "%1" . Additional Data: Error Value: %2.
106	User "%2" registered Task Scheduler task "%1"
107	Task Scheduler launched "%2" instance of task "%1" due to a time trigger condition.
108	Task Scheduler launched "%2" instance of task "%1" according to an event trigger.
109	Task Scheduler launched "%2" instance of task "%1" according to a registration trigger.
110	Task Scheduler launched "%2" instance of task "%1" for user "%3" .
111	Task Scheduler terminated "%2" instance of the "%1" task.
112	Task Scheduler could not start task "%1" because the network was unavailable. User Action: Ensure the computer is connected to the required network as specified in the task. If the task does not require network presence, remove the network condition from the task configuration.
113	Task registered task "%1" , but not all specified triggers will start the task. User Action: Ensure all the task triggers are valid as configured. Additional Data: Error Value: %2.
114	Task Scheduler could not launch task "%1" as scheduled. Instance "%2" is started now as required by the configuration option to start the task when available, if schedule is missed.
115	Task Scheduler failed to roll back a transaction when updating or deleting a task. Additional Data: Error Value: %1.
116	Task Scheduler validated the configuration for task "%1" , but credentials could not be stored. User Action: Re-register the task ensuring the credentials are valid. Additional Data: Error Value: %2.
117	Task Scheduler launched "%2" instance of task "%1" due to an idle condition.
118	Task Scheduler launched "%2" instance of task "%1" due to system startup.
119	Task Scheduler launched "%3" instance of task "%1" due to user "%2" logon.
120	Task Scheduler launched "%3" instance of task "%1" due to user "%2" connecting to the console trigger.
121	Task Scheduler launched "%3" instance of task "%1" due to user "%2" disconnecting from the console trigger.
122	Task Scheduler launched "%3" instance of task "%1" due to user "%2" remotely connecting trigger.
123	Task Scheduler launched "%3" instance of task "%1" due to user "%2" remotely disconnecting trigger.

Event ID	Message
124	Task Scheduler launched "%3" instance of task "%1" due to user "%2" locking the computer trigger.
125	Task Scheduler launched "%3" instance of task "%1" due to user "%2" unlocking the computer trigger.
126	Task Scheduler failed to execute task "%1" . Attempting to restart. Additional Data: Error Value: %2.
127	Task Scheduler failed to execute task "%1" due to a shutdown race condition. Attempting to restart.
128	Task Scheduler did not launch task "%1" , because current time exceeds the configured task end time. User Action: Extend the end time boundary for the task if required.
129	Task Scheduler launch task "%1" , instance "%2" with process ID %3.
130	Task Scheduler failed to start task "%1" due to the service being busy.
131	Task Scheduler failed to start task "%1" because the number of tasks in the task queue exceeding the quota currently configured to %2. User Action: Reduce the number of running tasks or increase the configured queue quota.
132	Task Scheduler task launching queue quota is approaching its preset limit of tasks currently configured to %1. User Action: Reduce the number of running tasks or increase the configured queue quota.
133	Task Scheduler failed to start task %1" in TaskEngine "%2" for user "%3". User Action: Reduce the number of tasks running in the specified user context.
134	Task Engine "%1" for user "%2" is approaching its preset limit of tasks. User Action: Reduce the number of tasks running in the specified user context.
135	Task Scheduler could not start task "%1" because the machine was not idle.
140	User "%2" updated Task Scheduler task "%1"
141	User "%2" deleted Task Scheduler task "%1"
142	User "%2" disabled Task Scheduler task "%1"
145	Task Scheduler woke up the computer to run a task.
146	Task Scheduler failed to load task "%1" at service startup. Additional Data: Error Value: %2.
147	Task Scheduler recovered sucessfully the image of task "%1" after a corruption occured during OS upgrade.
148	Task Scheduler failed to recover the image of task "%1" after a corruption occured during OS upgrade. Additional Data: Error Value: 0x%2.
149	Task "%1" is using a combination of properties that is incompatible with the scheduling engine.
150	Task Scheduler failed to subscribe for the event trigger for task "%1". Additional Data: Error Value: %2.
151	Task instantiation failed "%1". Check point: %2. Error Value: %3.
152	Task "%1" was re-directed to legacy scheduling engine.
153	Task Scheduler did not launch task "%1" as it missed its schedule. Consider using the configuration option to start the task when available, if schedule is missed.
155	Task Scheduler is currently waiting on completion of task "%1".
200	Task Scheduler launched action "%2" in instance "%3" of task "%1".
200	Task Scheduler launched action "%2" in instance "%3" of task "%1".
201	Task Scheduler successfully completed task "%1" , instance "%3" , action "%2" .
201	Task Scheduler successfully completed task "%1" , instance "%2" , action "%3" with return code %4.
201	Task Scheduler successfully completed task "%1" , instance "%2" , action "%3" with return code %4.

Event ID	Message
202	Task Scheduler failed to complete task "%1" , instance "%2" , action "%3" . Additional Data: Error Value: %4.
202	Task Scheduler failed to complete task "%1" , instance "%2" , action "%3" . Additional Data: Error Value: %4.
203	Task Scheduler failed to launch action "%3" in instance "%2" of task "%1". Additional Data: Error Value: %4.
204	Task Scheduler failed to retrieve the event triggering values for task "%1" . The event will be ignored. Additional Data: Error Value: %2.
205	Task Scheduler failed to match the pattern of events for task "%1" . The events will be ignored. Additional Data: Error Value: %2.
300	Task Scheduler started Task Engine "%1" with process ID %2.
301	Task Scheduler is shutting down Task Engine "%1"
303	Task Scheduler is shutting down Task Engine "%1" due to an error in "%2" . Additional Data: Error Value: %3.
304	Task Scheduler sent "%1" task to Task Engine "%2" . The task instance Id is "%3" .
305	Task Scheduler did not send "%1" task to Task Engine "%2" . Additional Data: Error Value: %3.
306	For Task Scheduler Task Engine "%1" , the thread pool failed to process the message. Additional Data: Error Value: %2.
307	Task Scheduler service failed to connect to the Task Engine "%1" process. Additional Data: Error Value: %2.
308	Task Scheduler connected to the Task Engine "%1" process.
309	Task Scheduler %1 tasks orphaned during Task Engine "%2" shutdown. User Action: Find the process run by this task in the Task Manager and kill it manually.
310	Task Scheduler started Task Engine "%1" process. Command="%2" , ProcessID=%3, ThreadID=%4
311	Task Scheduler failed to start Task Engine "%1" process due to an error occurring in "%3" . Command="%2" . Additional Data: Error Value: %4.
312	Task Scheduler created the Win32 job object for Task Engine "%1" .
313	Task Scheduler channel with Task Engine "%1" is ready to send and receive messages.
314	Task Scheduler has no tasks running for Task Engine "%1" , and the idle timer has started.
315	Task Engine "%1" process failed to connect to the Task Scheduler service. Additional Data: Error Value: %2.
316	Task Engine "%1" failed to send a message to the Task Scheduler service. Additional Data: Error Value: %2.
317	Task Scheduler started Task Engine "%1" process.
318	Task Scheduler shutdown Task Engine "%1" process.
319	Task Engine "%1" received a message from Task Scheduler service requesting to launch task "%2" .
320	Task Engine "%1" received a message from Task Scheduler service requesting to stop task instance "%2" .
322	Task Scheduler did not launch task "%1" because instance "%2" of the same task is already running.
323	Task Scheduler stopped instance "%2" of task "%1" in order to launch new instance "%3" .
324	Task Scheduler queued instance "%2" of task "%1" and will launch it as soon as instance "%3" completes.
325	Task Scheduler queued instance "%2" of task "%1".
326	Task Scheduler did not launch task "%1" because computer is running on batteries. User Action: If launching the task on batteries is required, change the respective flag in the task configuration.

Event ID	Message
327	Task Scheduler stopped instance "%2" of task "%1" because the computer is switching to battery power.
328	Task Scheduler stopped instance "%2" of task "%1" because computer is no longer idle.
329	Task Scheduler terminated "%2" instance of the "%1" task due to exceeding the time allocated for execution, as configured in the task definition. User Action: Increase the configured task timeout or investigate external reasons for the delay.
330	Task Scheduler stopped instance "%2" of task "%1" as request by user "%3" .
331	Task Scheduler will continue to execute Instance "%2" of task "%1" even after the designated timeout, due to a failure to create the timeout mechanism. Additional Data: Error Value: %3.
332	Task Scheduler did not launch task "%1" because user "%2" was not logged on when the launching conditions were met. User Action: Ensure user is logged on or change the task definition to allow launching when user is logged off.
333	Task Scheduler did not launch task "%1" because target session is RemoteApp session. User Action: If launching the task on RemoteApp sessions is required, change the respective flag in the task configuration.
334	Task Scheduler did not launch task "%1" because target session is a WORKER session.
400	Task Scheduler service has started.
402	Task Scheduler service is shutting down.
403	Task Scheduler service has encountered an error in "%1" . Additional Data: Error Value: %2.
700	Task Scheduler service started Task Compatibility module.
706	Task Compatibility module failed to update task "%1" to the required status %2. Additional Data: Error Value: %3.
707	Task Compatibility module failed to delete task "%1" . Additional Data: Error Value: %2.
708	Task Compatibility module failed to set security descriptor "%1" for task "%2" . Additional Data: Error Value: %3.
709	Task Compatibility module failed to update task "%1" . Additional Data: Error Value: %2.
710	Task Compatibility module failed to upgrade existing tasks. Upgrade will be attempted again next time 'Task Scheduler' service starts. Additional Data: Error Value: %1.
711	Task Compatibility module failed to upgrade NetSchedule account "%1" . Additional Data: Error Value: %2.
712	Task Compatibility module failed to read existing store to upgrade tasks. Additional Data: Error Value: %1.
713	Task Compatibility module failed to load task "%1" for upgrade. Additional Data: Error Value: %2.
714	Task Compatibility module failed to register task "%1" for upgrade. Additional Data: Error Value: %2.
715	Task Compatibility module failed to delete LSA store for upgrade. Additional Data: Error Value: %1.
717	Task Compatibility module failed to determine if upgrade is needed. Additional Data: Error Value: %1.

Event IDs: Section 5.2.2.6

Event ID	Message
5857	%1 provider started with result code %2. HostProcess = %3; ProcessID = %4; ProviderPath = %5
5858	Id = %1; ClientMachine = %2; User = %3; ClientProcessId = %4; Component = %5; Operation = %6; ResultCode = %7; PossibleCause = %8
5859	Namespace = %1; NotificationQuery = %2; OwnerName = %3; HostProcessID = %4; Provider= %5, queryID = %6; PossibleCause = %7

Event ID	Message
5860	Namespace = %1; NotificationQuery = %2; UserName = %3; ClientProcessID = %4, ClientMachine = %5; PossibleCause = %6
5861	Namespace = %1; Eventfilter = %2 (refer to its activate eventid:5859); Consumer = %3; PossibleCause = %4

Event IDs: Section 5.2.2.7

Event ID	Message
2	Initializing WSMan API
3	Initialization of WSMan API failed, error code %1
4	Deinitializing WSMan API
5	Deinitialization of WSMan API failed, error code %1
6	Creating WSMan Session. The connection string is: %1
7	WSMan Create Session operation failed, error code %1
8	Closing WSMan Session
9	Closing WSMan Session failed, error code %1
10	Setting WSMan Session Option (%1) - %2 with value (%3) completed successfully.
11	Creating WSMan shell with the ResourceUri: %1 and ShellId: %2
12	WSMan shell creation failed, error code %1
13	Running WSMan command with CommandId: %1
14	Running WSMan command failed, error code %1
15	Closing WSMan command
16	Closing WSMan shell
28	Access Denied error: the %1 API caller does not match the creator of the application object
29	Initialization of WSMan API completed successfuly
30	Deinitialization of WSMan API completed successfuly
31	WSMan Create Session operation completed successfuly
32	Setting WSMan Session Option (%1) - %2 failed, error code %3.
33	Closing WSMan Session completed successfuly
37	Closing WSMan shell failed, error code %1
38	Closing WSMan command failed, error code %1
40	Closing WSMan %1 operation failed, error code %2
41	The WinRM protocol handler has began loading for application %1.
42	The WinRM protocol handler completed unloading.
43	The WinRM protocol handler unloaded prematurely due to the following error: %2.
44	The WinRM protocol handler started to create a session at the following destination: %1.
45	The WinRM protocol handler closed the session.
46	The WinRM protocol session closed prematurely due to the following error: %2.
47	The WinRM protocol session began an operation of type %1 to the server. The operation accesses class %3 under the %2 namespace.
48	The WinRM protocol session successfully completed the operation.
49	The WinRM protocol operation failed due to the following error: %2.
84	The maximum number of users (%1) executing shell operations has been exceeded. Retry after sometime or raise the quota for concurrent shell users.
85	The %1 user is allowed a maximum number of %2 concurrent shells, which has been exceeded. Close existing shells or raise the quota for this user.

Event ID	Message
86	The WSMan service could not launch a host process to process the given request. Make sure the WSMan provider host server and proxy are properly registered. Error code %1
87	The WSMan host process was unexpectedly terminated. Error code %1
90	RunAs was disabled by Group Policy; WSMan service has erased all RunAs credentials.
91	Creating WSMan shell on server with ResourceUri: %1
131	Received redirect status code from Network layer; status: 302 (HTTP_STATUS_REDIRECT); location: %1
132	WSMan operation %1 completed successfully
135	Re-sending the request as a result of ERROR_WINHTTP_CANNOT_CONNECT, using next proxy
136	Re-sending the request as a result of ERROR_WINHTTP_NAME_NOT_RESOLVED, using next proxy
137	Network layer returned ERROR_WINHTTP_NAME_NOT_RESOLVED - The server name cannot be resolved. Aborting the operation
138	The client got a timeout from the network layer (ERROR_WINHTTP_TIMEOUT)
139	The client got a login failure from the network layer (ERROR_WINHTTP_LOGIN_FAILURE)
142	WSMan operation %1 failed, error code %2
145	WSMan operation %1 started with resourceUri %2
161	%1
162	Authenticating the user failed. The credentials didn't work.
163	The authentication mechanism (%1) requested by the client is not supported by the server. Possible authentication mechanisms reported by server: %2 %3 %4 %5 %6
164	The destination computer (%1) returned an 'access denied' error. Verify your credentials are correct.
165	The authentication mechanism requested by the proxy is not supported by the client. The only proxy authentication mechanism supported are Negotiate, Basic or Digest. Possible authentication mechanisms reported by proxy: %1 %2 %3 %4 %5
171	Authenticating the user with the proxy failed. The credentials didn't work.
172	The server certificate on the destination computer (%1:%2) has the following errors: %3 %4 %5 %6 %7 %8 %9 %10. Fix the server certificate and try again.
173	The WinRM service has terminated %1 unauthenticated connections over the past %2 minutes to maintain healthy system state. This will likely happen if the service is overloaded or if the service is under an authentication based attack. Action: Enable and observe Windows Remote Management Analytic log and look for warning events with Id 1843. These include additional information about the clients that got abruptly terminated.
192	The authorization of the user failed with error %1
193	Request for user %1 (%2) will be executed using WinRM virtual account %3 (%4)
208	The Winrm service is starting
209	The Winrm service started successfully
210	The WinRM service is unable to start because of a failure during initialization. The error code is %1
211	The Winrm service is stopping
212	The Winrm service was stopped successfully
213	The WSMan service could not load current configuration settings as the settings are corrupted. The service is started with default settings instead. User Action Use the following command to restore defaults: winrm invoke Restore winrm/config @{}
214	The WSMan client could not load current configuration settings as the settings are corrupted. The client is operating with default settings instead. User Action Start the

Event ID	Message
	WinRM service and use the following command to restore defaults: winrm invoke Restore winrm/config @{}
215	The WSMan service failed to read configuration of the following plugin: %1. The error received was %2: %%%2 %3. User Action Make sure this plugin configuration is valid.
216	The WSMan service failed to restart the plugins marked for AutoRestart. The error code received was %1.
217	The WSMan service failed to restart the %1 plugin on service startup. The error code received was %2.
218	The WSMan service successfully restarted the following plugin on service startup: %1.
219	The WSMan shell instance %1 will no longer support disconnect reconnect functionality because a non-supported request was sent by the client.
224	%1
229	The WinRM %1 failed to register for group policy change notifications. The error code is %2.
230	Deletion of registry key %1 resulted in access denied. If this registry entry is not marked specifically as read only, this seems like a potential issue.
254	Activity Transfer

Event IDs: Section 5.3.1.7

Event ID	Message
2	The TPM self test command failed.
12	The device driver for the Trusted Platform Module (TPM) encountered an error in the TPM hardware, which might prevent some applications using TPM services from operating correctly. Please restart your computer to reset the TPM hardware. For further assistance on this hardware issue, please contact the computer manufacturer for more information.
14	The device driver for the Trusted Platform Module (TPM) encountered a non-recoverable error in the TPM hardware, which prevents TPM services (such as data encryption) from being used. For further help, please contact the computer manufacturer.
15	The device driver for the Trusted Platform Module (TPM) encountered a non-recoverable error in the TPM hardware, which prevents TPM services (such as data encryption) from being used. For further help, please contact the computer manufacturer.
16	A compatible TPM is not found.
17	The Trusted Platform Module (TPM) hardware failed to execute a TPM command.
18	This event triggers the Trusted Platform Module (TPM) provisioning/status check to run.
19	The system firmware failed to enable overwriting of system memory on restart. The ACPI request could not be interpreted by the firmware. The firmware should be upgraded.
20	A command was sent to the Trusted Platform Module (TPM) successfully resetting the TPM lockout logic. This event is generated when a successful command sent to the TPM resets the TPM lockout logic. With this event, all prior standard user TPM authorization failures are ignored; allowing standard users to use the TPM normally again immediately.
21	A standard user issued Trusted Platform Module (TPM) command returned an authorization failure. This event is generated when a command sent to the TPM by a standard user returns a response indicating an authorization failure. If too many authorization failures occur, standard users may be temporarily prevented from sending TPM commands requiring authorization. This helps prevent the TPM from entering a hardware lockout because of too many authorization failures. User Security ID:%1. Process Path %2.

Event ID	Message
22	TPM Base Services (TBS) has been configured in a test mode until the next full restart. The TBS will not perform TPM resource virtualization or TPM command blocking until the next full restart.
23	A standard user Trusted Platform Module (TPM) command was blocked because the standard user has exceeded the maximum authorization failures permitted. This event is generated when too many recent TPM commands sent to the TPM by a standard user returned a response indicating an authorization failure. The standard user is currently temporarily prevented from sending TPM commands requiring authorization. This helps prevent the TPM from entering a hardware lockout because of too many authorization failures. User Security ID:%1.
24	The Trusted Platform Module (TPM) status: %1 and %2.
25	Creation of the Windows AIK directory failed.
26	Creation of provisioning event has failed.
27	The initialization of the Trusted Platform Module (TPM) failed. The TPM may be in failure mode. To allow diagnosis, contact the TPM manufacturer with the attached information.

Event IDs: Section 5.3.1.8

Event ID	Message
513	TPM Owner Authorization information was backed up successfully to Active Directory Domain Services.
514	Failed to backup TPM Owner Authorization information to Active Directory Domain Services. Errorcode: %1 Check that your computer is connected to the domain. If your computer is connected to the domain, have your Domain Administrator check that the Active Directory schema is appropriate for backup of Windows 8 TPM Owner Authorization information and that the current Computer object has write permission to the TPM object. Installations of Windows Server 2008 R2 or before need a schema extension in order to be ready for backup of Windows 8 TPM Owner Authorization information. Consult online documentation for more information about setting up Active Directory Domain Services for TPM.
515	The Trusted Platform Module (TPM) hardware on this computer has failed to set its Dictionary Attack Parameters to legacy mode.
516	Successfully sent physical presence request to clear the Trusted Platform Module(TPM).
517	Failed to send physical presence request to clear the Trusted Platform Module(TPM).
518	Failed to get isOwned status from Trusted Platform Module(TPM), proceeding to clear TPM assuming that TPM is owned. Error code:%1
519	The TPM has been cleared. Reason: %1.
769	TPM Owner Authorization configuration changed from '%1' to '%2'.
1025	The TPM was successfully provisioned and is now ready for use.
1026	The Trusted Platform Module (TPM) hardware on this computer cannot be provisioned for use automatically. To set up the TPM interactively use the TPM management console (Start->tpm.msc) and use the action to make the TPM ready. Error: %1 Additional Information: %2
1027	The Ownership of the Trusted Platform Module (TPM) hardware on this computer was successfully taken (TPM TakeOwnership command) by the system.
1028	The NGC key generation task was successfully triggered.

Event ID	Message
1029	The triggering of the NGC key generation task failed.
1030	The NGC certificate enrollment task was successfully triggered.
1031	The triggering of the NGC certificate enrollment task failed.
1281	This event triggers the TBS device identifier generation.
1282	The TBS device identifier has been generated.
1537	The Device Health Certificate was successfully provisioned from %1.
1538	The Device Health Certificate provisioning could not connect to %1. %2
1539	The Device Health Certificate could not be provisioned from %1. HTTP status code %2: %3
1793	The Trusted Platform Module (TPM) hardware on this computer is scheduled to be cleared by the system.
1794	The Trusted Platform Module (TPM) firmware on this PC has a known security problem. Please contact your PC manufacturer to find out if an update is available. For more information please go to https://go.microsoft.com/fwlink/?linkid=852572

Event IDs: Section 5.3.2.1, 5.3.2.2

Event ID	Message
2000	The following settings were applied to the Windows Defender Firewall at startup Current Profile: %1 IPsec SA Idle time: %2 IPsec preshared key encoding: %3 IPsec Exempt: %4 IPsec CRL Check: %5 IPsec Through NAT: %6 Policy Version Supported: %7 Policy Version: %8 Binary Version Supported: %9 Stateful FTP: %10 Group Policy Applied: %11 Remote Machine Authorization List: %12 Remote UserAuthorization List: %13
2001	The following per profile settings were applied by Windows Defender Firewall Profile: %1 Operational Mode: %2 Stealth Mode: %3 Block all Incoming Connections: %4 Unicast response to multicast broadcast: %5 Log dropped packets: %6 Log successful connections: %7 Log ignored rules: %8 Inbound Notifications: %9 Allow Local Policy Merge: %12 Allow Local IPsec Policy Merge: %13 Default Outbound Action: %14 Default Inbound Action: %15 Remote Administration: %16 Stealth Mode IPsec Secured Packet Exemption: %21 Maximum Log file size: %17 Log File path: %18 Allow User preferred merge of Authorized Applications: %10 Allow User preferred merge of Globally open ports: %11
2002	A Windows Defender Firewall setting has changed. New Setting: Type: %1 Value: %4 Modifying User: %6 Modifying Application: %7
2003	A Windows Defender Firewall setting in the %1 profile has changed. New Setting: Type: %2 Value: %5 Modifying User: %7 Modifying Application: %8
2004	A rule has been added to the Windows Defender Firewall exception list. Added Rule: Rule ID: %1 Rule Name: %2 Origin: %3 Active: %18 Direction: %6 Profiles: %11 Action: %10 Application Path: %4 Service Name: %5 Protocol: %7 Security Options: %21 Edge Traversal: %19 Modifying User: %22 Modifying Application: %23
2005	A rule has been modified in the Windows Defender Firewall exception list. Modified Rule: Rule ID: %1 Rule Name: %2 Origin: %3 Active: %18 Direction: %6 Profiles: %11 Action: %10 Application Path: %4 Service Name: %5 Protocol: %7 Security Options: %21 Edge Traversal: %19 Modifying User: %22 Modifying Application: %23
2006	A rule has been deleted in the Windows Defender Firewall exception list. Deleted Rule: Rule ID: %1 Rule Name: %2 Modifying User: %3 Modifying Application: %4
2007	A rule has been listed when the Windows Defender Firewall started. Added Rule: Rule ID: %1 Rule Name: %2 Origin: %3 Active: %18 Direction: %6 Profiles: %11 Action: %10 Application Path: %4 Service Name: %5 Protocol: %7 Security Options: %21 Edge Traversal: %19
2008	Windows Defender Firewall Group Policy settings have changed. The new settings have been applied

Event ID	Message
2009	The Windows Defender Firewall service failed to load Group Policy. Error: %1
2010	Network profile changed on an interface. Adapter GUID: %1 Adapter Name: %2 Old Profile: %3 New Profile: %4
2011	Windows Defender Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. Reason: %1 Application Path: %2 IP Version: %3 Protocol: %4 Port: %5 Process Id: %6 User: %7
2032	Windows Defender Firewall has been reset to its default configuration. ModifyingUser: %1 ModifyingApplication: %2
2033	All rules have been deleted from the Windows Defender Firewall configuration on this computer. Store Type: %1 ModifyingUser: %2 ModifyingApplication: %3

Event IDs: Section 5.4.1.1

Event ID	Message
1000	There are currently no IPv4 DNS servers configured for any interface on this host. Please configure DNS server settings, or renew your dynamic IP settings.
1001	Interface: %1 Total DNS Server Count: %2 Index: %3 Address: %6 (%4)
1002	The DNS server being queried for interface %1 has changed to %3
1003	The following DNS server(s) were successfully validated as active servers that can service this client. %2
1005	The client was unable to validate the following as active DNS server(s) that can service this client. The server(s) may be temporarily unavailable, or may be incorrectly configured. %2
1007	The primary DNS suffix for this machine is missing. In the absence of a primary DNS suffix, short unqualified names may not resolve through DNS
1009	The primary DNS suffix for this machine (%1) does not match the Active Directory domain (%2) that it is currently joined to.
1011	There was an error while attempting to read the local hosts file.
1013	Name resolution for the name %1 timed out after none of the configured DNS servers responded.
1015	Name resolution for the name %1 timed out after the DNS server %3 did not respond.
1016	A name not found error was returned for the name %1. Check to ensure that the name is correct. The response was sent by the server at %3.
1017	The DNS server's response to a query for name %1 indicates that no records of the type queried are available, but could indicate that other records for the same name are present.
1018	The response for the query %1 was a Link Local IP address %3. The response was sent by the server at %5.
1019	There are currently no IPv6 DNS servers configured for any interface on this host. Please configure DNS server settings, or renew your dynamic IP settings.
1020	Read DNS Name Resolution Policy Table: Key Name %1: DNSSEC Settings: DnsSecValidationRequired %2, DnsQueryOverIPSec %3, DnsEncryption %4 Direct Access Settings: DirectAccessServerList %5, EnableRemoteIPSEC %6 RemoteEncryption %7 ProxyType %8 ProxyName %9
1021	Matched Effective policy for query name %1: Key Name %2: DnsSecValidationRequired %3, DnsQueryOverIPSec %4, DnsEncryption %5 DirectAccessServerList %6, ProxyType %7 ProxyName %8
1022	Name resolution for the name, %1, will not fall back to LLMNR or NetBIOS
1024	Transaction ID of the response for query %1 from server %3 did not match
1025	The DNS server IP %3 of the response for query %1 is not configured on the client
1026	The question (%2) in the response from server %4 does not match the original question %1

Event ID	Message
1027	DNS Name resolution for the name, %1, failed because the client was unable to contact DNS servers. At least one of the interfaces is not in a private network and name resolution will not fall back to LLMNR or NetBIOS
1028	Matched effective policy for query name %1: Key Name %2: DnsSecValidationRequired %3, DnsQueryOverIPSec %4, DnsEncryption %5 DirectAccessServerList %6, ProxyType %7 ProxyName %8 GenericServerList %9 IdnConfig %10
3000	DNS Query is initiated for the name %1 and for the type %2 with query options %3
3001	DNS Query operation is completed with result %1
3002	DNS Cache lookup is initiated for the name %1 and for the type %2 with query options %3
3003	DNS Cache lookup operation for the name %1 and for the type %2 is completed with result %3
3004	DNS FQDN Query is initiated for the name %1 and for the type %2 with query options %3
3005	DNS FQDN Query operation for the name %1 and for the type %2 is completed with result %3
3006	DNS query is called for the name %1, type %2, query options %3, Server List %4, isNetwork query %5, network index %6, interface index %7, is asynchronous query %8
3007	DnsQueryEx for the name %1 is pending
3008	DNS query is completed for the name %1, type %2, query options %3 with status %4 Results %5
3009	Network query initiated for the name %1 (is parallel query %2) on network index %3 with interface count %4 with first interface name %5, local addresses %6 and Dns Servers %7
3010	DNS Query sent to DNS Server %3 for name %1 and type %2
3011	Received response from DNS Server %3 for name %1 and type %2 with response status %4
3012	NETBIOS query is initiated for name %1 on network index %2 with inteface count %3 with first interface name %4 and local addresses %5
3013	NETBIOS query is completed for name %1 with status %2 and results %3
3014	NETBIOS query for the name %1 is pending
3015	DnsQueryEx is canceled for the name %1
3016	Cache lookup called for name %1, type %2, options %3 and interface index %4
3018	Cache lookup for name %1, type %2 and option %3 returned %4 with results %5
3019	Query wire called for name %1, type %2, interface index %3 and network index %4
3020	Query response for name %1, type %2, interface index %3 and network index %4 returned %5 with results %6
60004	Error: %1 Location: %2 Context: %3
60005	Warning: %1 Location: %2 Context: %3
60006	Transitioned to State: %1 Context: %2
60007	Updated Context: %1 Update Reason: %2
60008	Name resolution policy table has been corrupted. DNS resolution will fail until it is fixed. Contact your network administrator. For more information: read policy table for rule %1 failed with error %2
60101	SourceAddress: %1 SourcePort: %2 DestinationAddress: %3 DestinationPort: %4 Protocol: %5 ReferenceContext: %6
60102	SourceAddress: %1 SourcePort: %2 DestinationAddress: %3 DestinationPort: %4 Protocol: %5 ReferenceContext: %6
60103	Interface Guid: %1 IfIndex: %2 Interface Luid: %3 ReferenceContext: %4

Event IDs: Section 5.4.1.2, 5.4.1.3

Event ID	Message
30800	The server name cannot be resolved. Error: %2 Server name: %4 Guidance: The client cannot resolve the server address in DNS or WINS. This issue often manifests immediately after joining a computer to the domain, when the client's DNS registration may not yet have propagated to all DNS servers. You should also expect this event at system startup on a DNS server (such as a domain controller) that points to itself for the primary DNS. You should validate the DNS client settings on this computer using IPCONFIG /ALL and NSLOOKUP.
30801	%1. Error: %2 Server name: %4
30802	%1. Error: %2 Server name: %4
30803	Failed to establish a network connection. Error: %2 Server name: %4 Server address: %6 Connection type: %7 Guidance: This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue.
30803	Failed to establish a network connection. Error: %2 Server name: %4 Server address: %6 Instance name: %9 Connection type: %10 Guidance: This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue.
30804	A network connection was disconnected. Server name: %4 Server address: %6

Event ID	Message
	Connection type: %7 Guidance: This indicates that the client's connection to the server was disconnected. Frequent, unexpected disconnects when using an RDMA over Converged Ethernet (RoCE) adapter may indicate a network misconfiguration. RoCE requires Priority Flow Control (PFC) to be configured for every host, switch and router on the RoCE network. Failure to properly configure PFC will cause packet loss, frequent disconnects and poor performance.
30805	The client lost its session to the server. Error: %1 Server name: %5 Session ID: %2 Guidance: If the server is a Windows Failover Cluster file server, then this message occurs when the file share moves between cluster nodes. There should also be an anti-event 30806 indicating the session to the server was re-established. If the server is not a failover cluster, it is likely that the server was previously online, but it is now inaccessible over the network.
30806	The client re-established its session to the server. Server name: %5 Server address: %7 Session ID: %2 Guidance: You should expect this event if there was a previous event 30805, but the client successfully resumed the cached connection before the timeout expired.
30807	The connection to the share was lost. Error: %1 Share name: %5 Session ID: %2 Tree ID: %3 Guidance: If the server is a Windows Failover Cluster file server, then this message occurs when the file share moves between cluster nodes. There should also be an anti-event 30808 indicating the session to the server was re-established. If the server is not a failover cluster, it is likely that the server was previously online, but it is now inaccessible over the network.
30808	The connection to the share was re-established. Share name: %5 Server address: %7 Session ID: %2 Tree ID: %3 Guidance: You should expect this event if there was a previous event 30807, but the client successfully resumed the cached connection before the timeout expired.
30809	A request timed out because there was no response from the server. Server name: %6 Session ID:%3 Tree ID:%4

Event ID	Message
	Message ID:%2 Command: %1 Instance Name: %9 RetryCount: %10 ElapsedTime(ms): %11 Guidance: The server is responding over TCP but not over SMB. Ensure the Server service is running and responsive, and the disks do not have high per-IO latency, which makes the disks appear unresponsive to SMB. Also, ensure the server is responsive overall and not paused; for instance, make sure you can log on to it.
30810	Added a TCP/IP transport interface. Name: %2 InterfaceIndex: %3 Guidance: A TCP/IP binding was added to the specified network adapter for the SMB client. The SMB client can now send and receive SMB traffic on this network adapter using TCP/IP. You should expect this event when a computer restarts or when a previously disabled network adaptor is re-enabled. No user action is required.
30811	Deleted a TCP/IP transport interface. Name: %2 InterfaceIndex: %3 Guidance: A TCP/IP binding was removed from the specified network adapter for the SMB client. You should expect this event when a computer shuts down or when a previously enabled network adaptor is disabled. No user action is required.
30812	Added a TDI transport interface. Name: %2 Guidance: A TDI (NetBIOS) binding was added to the specified network adapter for the SMB client. The SMB client can now send and receive SMB traffic on this network adapter using TDI. You should expect this event when a computer restarts or when a previously disabled network adaptor is re-enabled. No user action is required.
30813	Deleted a TDI transport interface. Name: %2 Guidance: A TDI (NetBIOS) binding was removed from the specified network adapter for the SMB client. You should expect this event when a computer shuts down or when a previously enabled network adaptor is disabled. No user action is required.
30814	Witness registration has completed. Status: %1 Cluster share name: %4 Cluster share type: %2 File server cluster address: %6 Guidance: The client successfully registered with the SMB Witness through RPC using TCP (port 135, then an endpoint port above 1023). No action is required.

Event ID	Message
30815	Witness deregistration has completed. Status: %1 Cluster share name: %4 Cluster share type: %2 Guidance: The client successfully de-registered with the SMB Witness through RPC using TCP (port 135, then an endpoint port above 1023). No action is required.
30816	The server failed the negotiate request. Error: %2 Server name: %4 Guidance: The server does not support any dialect that the client is trying to negotiate, such as the client has SMB2/SMB3 disabled and the server has SMB1 disabled.
30817	Close request failed. Error: %2 Path: %4%6 Guidance: A persistent handle (Continuous Availability) or a resilient handle failed to close.
30818	RDMA interfaces are available but the client failed to connect to the server over RDMA transport. Server name: %2 Guidance: Both client and server have RDMA (SMB Direct) adaptors but there was a problem with the connection and the client had to fall back to using TCP/IP SMB (non-RDMA).
30819	The SMB client received a request to move to a different node on a file server cluster. File server cluster name: %4 New file server cluster address: %6 Guidance: Continuous Availability (Transparent Failover) is in use and the client computer is going to move to a different node after an SMB witness request over RPC using TCP (first contacting port 135, then contacting an endpoint port above 1023). No user action is required.
30820	The SMB client successfully moved to a different node on a file server cluster. File server cluster name: %4 New file server cluster address: %6 Guidance: Continuous Availability (Transparent Failover) is in use and the client computer successfully moved to a different node after an SMB witness request over RPC using TCP (first contacting port 135, then contacting an endpoint port above 1023). No user action is required.
30821	The SMB client failed to move to a different node on a file server cluster. Error: %1 File server cluster name: %4

Event ID	Message
	Guidance: Continuous Availability (Transparent Failover) is in use and the client computer failed to move to a different node after an SMB witness request over RPC using TCP (first contacting port 135, then contacting an endpoint port above 1023). The attempt to connect to the destination server failed, which is typically due to a network configuration issue. For example, this issue may occur if the destination node's IP address cannot be resolved, if the destination node is behind a firewall, or if there is no network route from the client to the node.
30822	Failed to establish an SMB multichannel network connection. Error: %2 Server name: %4 Server address: %6 Client address: %7 Instance name: %9 Connection type: %10 Guidance: This indicates a problem with the underlying network or transport, such as with TCP/IP, and not with SMB. A firewall that blocks TCP port 445, or TCP port 5445 when using an iWARP RDMA adapter, can also cause this issue. Since the error occurred while trying to connect extra channels, it will not result in an application error. This event is for diagnostics only.
30823	The connection was terminated due to one or more IO request timeouts. Error: %2 Name: %4 Server address: %6 Client address: %7 Instance name: %9 Connection type: %10 Guidance: This indicates a problem with the underlying network or the storage stack on the remote server. IO operations were not completed within the allotted time. The application may not see this failure because IOs are usually retried on a different connection. This event is for diagnostics only.
31000	%1. Error: %2 Security status: %3 User name: %10 Logon ID: %4 Serrver name: %6
31001	%1. Error: %2 Security status: %3 User name: %10 Logon ID: %4 Server name: %6 Principal name: %8
31002	The outbound authentication failed using a network token.

Event ID	Message
	Error: %2 Server name: %4 Guidance: This typically indicates that delegation must be configured for a Kerberos double-hop scenario. If delegation is configured, confirm that the services are configured correctly on the middle-tier server.
31003	The LmCompatibilityLevel value is different from the default. Configured LM Compatibility Level: %2 Default LM Compatibility Level: 3 Guidance: LAN Manager (LM) authentication is the protocol used to authenticate Windows clients for network operations. This includes joining a domain, accessing network resources, and authenticating users or computers. This determines which challenge/response authentication protocol is negotiated between the client and the server computers. Specifically, the LM authentication level determines which authentication protocols the client will try to negotiate or the server will accept. The value set for LmCompatibilityLevel determines which challenge/response authentication protocol is used for network logons. This value affects the level of authentication protocol that clients use, the level of session security negotiated, and the level of authentication accepted by servers. Value (Setting) - Description 0 (Send LM & NTLM- responses) - Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 1 (Send LM & NTLM - use NTLMv2 session security if negotiated) - Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 2 (Send NTLM response only) - Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 3 (Send NTLM v2 response only) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 4 (Send NTLMv2 response only/refuse LM) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and accept only NTLM and NTLMv2 authentication. 5 (Send NTLM v2 response only/refuse LM & NTLM) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM and accept only NTLMv2 authentication. Incompatibly configured LmCompatibility levels between a client and server (such as 0 on a client and 5 on a server) prevent access to the server. Non-Microsoft clients and servers also provide these configuration settings.
31010	The SMB client failed to connect to the share.

Event ID	Message
	Error: %2 Path: %4%6
31012	The negotiate validation failed. From negotiate response: Dialect: %1 SecurityMode: %2 Capabilities: %3 ServerGuid: %4 From FSCTL_VALIDATE_NEGOTIATE_INFO response: Dialect: %5 SecurityMode: %6 Capabilities: %7 ServerGuid: %8 Guidance: The client successfully negotiated SMB dialect, security mode, capabilities and server GUID with the server, but the validation of these values then failed after connecting to a share. This may be due to a "man-in-the-middle" compromise attempt.
31013	The signing validation failed. Error:%7 Server name: %6 Session ID:%3 Tree ID:%4 Message ID:%2 Command: %1 Guidance: This error indicates that SMB messages are being modified in transit across the network from the server to the client. This may be due to the session ending on the server, a problem with the network, a problem with a third-party SMB server, or a "man-in-the-middle" compromise attempt. PacketFragment:%9
31014	The client received an unencrypted message when encryption was expected. Server name: %6 Session ID:%3 Tree ID:%4 Message ID:%2 Command: %1 Instance Name: %9 Guidance: This error indicates that SMB messages are being modified in transit across the network from the server to the client. This may be due to the session ending on the server, a problem with the network, a problem with a third-party SMB server, or a "man-in-the-middle" compromise attempt.
31015	Failed to decrypt an encrypted SMB message. Error:%7 Server name: %6 Session ID:%3

Event ID	Message
	Instance Name: %9 Guidance: The client received an encrypted SMB message but cannot decrypt the data. This typically means that the communication came from a previous session that no longer exists. The encryption header may also have been damaged or tampered with on the network between the client and server.
31016	The SMB Signing registry value is not configured with default settings. Default Registry Value: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "EnableSecuritySignature"=dword:1 Configured Registry Value: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "EnableSecuritySignature"=dword:0 Guidance: Even though you can disable, enable, or require SMB Signing, the negotiation rules changed starting with SMB2 and not all combinations operate like SMB1. The effective behavior for SMB2/SMB3 is: Client Required and Server Required = Signed Client Not Required and Server Required = Signed Server Required and Client Not Required = Signed Server Not Required and Client Not Required = Not Signed When requiring SMB Encryption, SMB Signing is not used, regardless of settings. SMB Encryption implicitly provides the same integrity guarantees as SMB Signing.
31017	Rejected an insecure guest logon. User name: %2 Server name: %4 Guidance: This event indicates that the server attempted to log the user on as an unauthenticated guest and was denied by the client. Guest logons do not support standard security features such as signing and encryption. As a result, guest logons are vulnerable to man-in-the-middle attacks that can expose sensitive data on the network. Windows disables insecure guest logons by default. Microsoft does not recommend enabling insecure guest logons.
31018	The %1 registry value is not configured with default settings. Default Registry Value: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "%1"=dword:0 Configured Registry Value: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "%1"=dword:%2 Guidance: This event indicates that an administrator has enabled insecure guest logons. An insecure guest logon occurs when a server logs the user on as an unauthenticated guest, typically in response to an authentication failure. Guest logons do not support standard security features such as signing and encryption. As a result, allowing guest logons makes the client vulnerable to man-in-the-middle attacks that can expose sensitive data on the network. Windows disables insecure guest logons by default. Microsoft does not recommend enabling insecure guest logons.
31019	Mutual authentication was unexpectedly lost after re-authenticating to %6 User %8

Event ID	Message
	LogonID %4 Status %2 AuthProtocol Old %9 New %10 MutualAuthState Old %11 New %12 Clustered %13

Event IDs: Section 5.4.1.4, 5.4.1.5

Event ID	Message
551	SMB Session Authentication Failure Client Name: %11 Client Address: %6 User Name: %9 Session ID: %7 Status: %4 (%3) Guidance: You should expect this error when attempting to connect to shares using incorrect credentials. This error does not always indicate a problem with authorization, but mainly authentication. It is more common with non-Windows clients. This error can occur when using incorrect usernames and passwords with NTLM, mismatched LmCompatibility settings between client and server, duplicate Kerberos service principal names, incorrect Kerberos ticket-granting service tickets, or Guest accounts without Guest access enabled
551	SMB Session Authentication Failure Client Name: %11 Client Address: %6 User Name: %9 Session ID: %7 Status: %4 (%3) SPN: %12 SPN Validation Policy: %13 Guidance: You should expect this error when attempting to connect to shares using incorrect credentials. This error does not always indicate a problem with authorization, but mainly authentication. It is more common with non-Windows clients. This error can occur when using incorrect usernames and passwords with NTLM, mismatched LmCompatibility settings between client and server, an incorrect service principal name, duplicate Kerberos service principal names, incorrect Kerberos ticket-granting service tickets, or Guest accounts without Guest access enabled
658	File handle for file "%8\%2" was invalidated by user %4 from computer %6
1000	S4U2Self authentication failure - The client could not be reauthenticated with S4U2Self to obtain claims. This may be expected if the account is not a domain account.
1001	SRV Disabled - The SMB1 negotiate request fails due to SMB1 is disabled.
1001	A client attempted to access the server using SMB1 and was rejected because SMB1 file sharing support is disabled or has been uninstalled. Guidance: An administrator has disabled or uninstalled server support for SMB1. Clients running Windows XP / Windows Server 2003 R2 and earlier will not be able to access this

Event ID	Message
	server. Clients running Windows Vista / Windows Server 2008 and later no longer require SMB1. To determine which clients are attempting to access this server using SMB1, use the Windows PowerShell cmdlet Set-SmbServerConfiguration to enable SMB1 access auditing.
1002	RKF failure - SRV2 failed to get acknowledgement from Resume Key filter for persistent handle request.
1003	The server received an unencrypted message from client %4. Message was rejected. Guidance: This event indicates that a client is sending unencrypted data even though the SMB share requires encryption.
1003	The server received an unencrypted message from client when encryption was required. Message was rejected. Client Name: %4 Client Address: %8 User Name: %6 Session ID: %9 Share Name: %2 Guidance: This event indicates that a client is sending unencrypted data even though the SMB share requires encryption.
1004	The server received an incorrectly signed message from client %2. Message was rejected. Guidance: This event indicates that a client is sending an incorrectly signed request.
1004	The server rejected an incorrectly signed message. Client Name: %2 Client Address: %6 User Name: %4 Session ID: %7 Guidance: This event indicates that a client is sending an incorrectly signed request.
1005	The server failed to validate negotiation from client %2. Connection was terminated.
1005	The server rejected an invalid negotiation request. Connection was terminated. Client Name: %2 Client Address: %6 User Name: %4 Session ID: %13 Expected Dialect: %7 Expected Capabilities: %8 Expected Security Mode: %9 Received Dialect: %10 Received Capabilities: %11 Received Security Mode: %12 Guidance: This event indicates that a client is attempting to negotiate a second connection using a mismatched dialect or capabilities.
1005	Negotiate integrity check failed. Status: %2 Client Name: %4 Client Address: %8 User Name: %6

Event ID	Message
	Session ID: %9 Guidance: This event indicates that the client's negotiate request was altered on the network between the client and server due to errors or a "man-in-the-middle" attack. The client has been disconnected to prevent a security downgrade.
1006	The share denied access to the client. Client Name: %10 Client Address: %6 User Name: %8 Session ID: %17 Share Name: %2 Share Path: %4 Status: %16 (%15) Mapped Access: %11 Granted Access: %12 Security Descriptor: %14 Guidance: You should expect access denied errors when a principal accesses a share without the necessary permissions. Usually, this indicates that the principal does not have direct security permissions or lacks membership in a group that has direct access permissions. To determine and correct the permissions on the specified share, an administrator can use the Security tab in File Explorer Properties dialog, the SMBSHARE Windows PowerShell module, or the NET SHARE command. You can also use the Effective Access tab in File Explorer to help diagnose the issue. Applications may generate access denied errors if they attempt to open files in a writable mode first, and then reopen the files in a read-only mode. In this case, no user action is required. If access to the share is denied and this event is not logged, you can examine the file and folder NTFS/REFS permissions. This error does not indicate a problem with authentication, only authorization.
1007	The share denied anonymous access to the client. Client Name: %8 Client Address: %6 Share Name: %2 Share Path: %4 Guidance: You should expect this error when a client attempts to connect to shares and does not provide any credentials. This indicates that the client is not providing a user name (and domain credentials, if necessary). By default, anonymous access to shares is denied. This error does not always indicate a problem with authorization, but mainly authentication. It is more common with non-Windows clients.
1009	The server denied anonymous access to the client. Client Name: %4 Client Address: %2 Session ID: %5 Guidance: You should expect this error when a client attempts to connect to shares and does not provide any credentials. This indicates that the client is not providing a user name (and domain credentials, if necessary). By default, Windows Server denies anonymous access to shares. This error does not always indicate a problem with authorization, but mainly authentication. It is more common with non-Windows clients.

Event ID	Message
1010	Endpoint added. Name: %2 Domain Name: %4 Transport Name: %6 Transport Flags: %7 Guidance: You should expect this event when the server starts listening on an interface, such as during system restart or when enabling a network adaptor. No user action is required.
1011	Endpoint removed. Name: %2 Domain Name: %4 Transport Name: %6 Guidance: You should expect this event when the server stops listening on an interface, such as during shutdown or when disabling a network adaptor. No user action is required.
1012	The network name information changed. Change Type: %1 Net Name: %3 IP Address: %9 Flags: %4 Interface Index: %5 Capability: %6 Link Speed: %7 Guidance: You should expect this event on a Windows Failover Cluster node during failover operations, at system startup, or during network configuration. No user action is required.
1013	Endpoint coming online. Endpoint Name: %2 Transport Name: %4 Guidance: You should expect this event on a Windows Failover Cluster node during failover operations. No user action is required.
1014	Endpoint going offline. Endpoint Name: %2 Transport Name: %4 Guidance: You should expect this event on a Windows Failover Cluster node during failover operations. No user action is required.
1016	Reopen failed. Client Name: %7 Client Address: %9 User Name: %13 Session ID: %14 Share Name: %11 File Name: %16 Resume Key: %20

Event ID	Message
	Status: %2 (%1) RKF Status: %4 (%3) Durable: %17 Resilient: %18 Persistent: %19 Reason: %21 Guidance: The client attempted to reopen a continuously available handle, but the attempt failed. This typically indicates a problem with the network or underlying file being re-opened.
1017	Handle scavenged. Share Name: %7 File Name: %9 Resume Key: %5 Persistent File ID: %3 Volatile File ID: %4 Durable: %1 Resilient or Persistent: %2 Guidance: The server closed a handle that was previously reserved for a client after 60 seconds. You should expect this event on a computer that is continuously available where a client did not gracefully close its session. For instance, this may occur when the client unexpectedly restarted.
1018	Backchannel invalidation of session completed. Session ID: %1 Status: %3 (%2) Task Status: %5 (%4) Guidance: You should expect this event on a computer that is continuously available. No user action is required
1019	Backchannel invalidation of file completed. Resume Key: %1 Status: %3 (%2) Task Status: %5 (%4) Guidance: You should expect this event on a computer that is continuously available. No user action is required
1020	File system operation has taken longer than expected. Client Name: %8 Client Address: %10 User Name: %6 Session ID: %3 Share Name: %12 File Name: %14 Command: %1 Duration (in milliseconds): %15 Warning Threshold (in milliseconds): %16 Guidance: The underlying file system has taken too long to respond to an operation. This typically indicates a problem with the storage and not SMB.

Event ID	Message
1020	File system operation has taken longer than expected. Client Name: %8 Client Address: %10 User Name: %6 Session ID: %3 Share Name: %12 File Name: %14 Command: %1 Duration (in milliseconds): %15 Warning Threshold (in milliseconds): %16 Guidance: The underlying file system has taken too long to respond to an operation. This typically indicates a problem with the storage and not SMB.
1021	LmCompatibilityLevel value is different from the default. Configured LM Compatibility Level: %1 Default LM Compatibility Level: %2 Guidance: LAN Manager (LM) authentication is the protocol used to authenticate Windows clients for network operations. This includes joining a domain, accessing network resources, and authenticating users or computers. This determines which challenge/response authentication protocol is negotiated between the client and the server computers. Specifically, the LM authentication level determines which authentication protocols the client will try to negotiate or the server will accept. The value set for LmCompatibilityLevel determines which challenge/response authentication protocol is used for network logons. This value affects the level of authentication protocol that clients use, the level of session security negotiated, and the level of authentication accepted by servers. Value (Setting) - Description 0 (Send LM & NTLM responses) - Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 1 (Send LM & NTLM - use NTLMv2 session security if negotiated) - Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 2 (Send NTLM response only) - Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 3 (Send NTLM v2 response only) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. 4 (Send NTLMv2 response only/refuse LM) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and accept only NTLM and NTLMv2 authentication.

Event ID	Message
	5 (Send NTLM v2 response only/refuse LM & NTLM) - Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM and accept only NTLMv2 authentication. Incompatibly configured LmCompatibility levels between a client and server (such as 0 on a client and 5 on a server) prevent access to the server. Non-Microsoft clients and servers also provide these configuration settings.
1023	One or more shares present on this server have access based enumeration enabled. Guidance: You should expect this event when enabling access-based enumeration on one or more shares by using either Server Manager or the Set-SmbShare Windows PowerShell cmdlet. Access-based enumeration can raise CPU utilization when clients connect to shares with folders containing many peer-level resources to which a user does not have access. You can control the CPU utilization by configuring the ABELevel value in the Windows registry: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\ABELevel [DWORD] You can set the value for ABELevel to greater depths to minimize CPU overhead, but doing so diminishes the effectiveness of access-based enumeration: Value = 0: access-based enumeration is enabled for all levels Value = 1: access-based enumeration is enabled for a depth of 1 (example: \server\share) Value = 2: access-based enumeration is enabled for a depth of 2 (example: \server\share\folder) You can continue setting values for multiple depth levels.
1024	SMB2 and SMB3 have been disabled on this server. This results in reduced functionality and performance. Registry Key: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registry Value: Smb2 Default Value: 1 (or not present) Current Value: 0 Guidance: You should expect this event when disabling SMB2/SMB3. Microsoft does not recommend disabling SMB2/SMB3. When SMB3 is disabled, you cannot use features such as SMB Transparent Failover, SMB Scale Out, SMB Multichannel, SMB Direct (RDMA), SMB Encryption, VSS for SMB file shares, and SMB Directory Leasing. In most scenarios, SMB provides a troubleshooting workaround as an alternative to disabling SMB2/SMB3. Use the Set-SmbServerConfiguration Windows PowerShell cmdlet to enable SMB2/SMB3.
1025	One or more named pipes or shares have been marked for access by anonymous users. This increases the security risk of the computer by allowing unauthenticated users to connect to this server. Registry Key: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registry Values: NullSessionPipes, NullSessionShares Default Value: Empty (or not present) Current Value: Non-empty Guidance: You should expect this event when modifying the default values of NullSessionShares and NullSessionPipes. On a typical file server, these settings do not exist or do not contain values, which is the most secure configuration. By default, domain controllers

Event ID	Message
	populate the NullSessionShares entry with netlogon, samr, and lsarpc to allow legacy access methods.
1026	File leasing has been disabled for the SMB2 and SMB3 protocols. This reduces functionality and can decrease performance. Registry Key: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registry Value: DisableLeasing Default Value: 0 (or not present) Current Value: non-zero Guidance: You should expect this event when disabling SMB 3 Leasing. Microsoft does not recommend disabling SMB Leasing. Once disabled, traffic from client to server may increase since metadata and data may no longer be retrieved from a local cache.
1027	The file and printer sharing firewall ports are currently closed. This is the default configuration for a system that is not sharing content or is on a Public network. Guidance: You should expect this event when Windows Firewall is not configured to enable the File and Printer Sharing rule, which allows inbound SMB traffic. This event occurs on a computer that does not have custom shares configured. Clients cannot access SMB shares on this computer until SMB traffic is allowed through the firewall.
1028	The maximum cluster-supported SMB dialect has changed. NewMaxDialect: %1 OldMaxDialect: %2 Guidance: You should expect this event during a Windows Failover Cluster upgrade. No user action is required.
1029	The Cipher Suite Order group policy setting is invalid. Guidance: This event indicates that an administrator has configured an invalid value for the "Computer Configuration\Administrative Templates\Network\Lanman Server\Cipher Suite Order" group policy setting. The server will use the default cipher suite order "%1" until this error is resolved.
1030	An MDL read or write completion request failed. Server Name: %2 Share Name: %4 File Name: %6 IsRead: %7 Status: %8 Guidance: The SMB server sends MDL completion requests to a file system upon completion of a buffered I/O to release system resources. The file system and its filter drivers must not fail MDL completion requests. Failures may result in memory leaks and degraded system performance and stability. Non-Microsoft file system filter drivers are the most common cause of failed MDL completion requests.
1031	The server detected a problem and has captured a live kernel dump to collect debug information. Reason: %1 Dump Location: %SystemRoot%\LiveKernelReports

Event ID	Message
	Guidance: The server supports the Live Dump feature, where the detection of a problem results in a kernel memory dump, but no bugcheck and reboot. This allows Microsoft Support to examine memory dumps without requiring a reboot or manual intervention. The reason code indicates the type of problem that was detected. Stalled I/O An I/O is taking an unreasonably long time to complete. Malfunctioning third-party file system minifilter drivers are a common source of this problem. Other causes include failed disks or a client-driven I/O workload that greatly exceeds the server's capacity.
1032	The server detected a problem but was unable to capture a live kernel dump to collect debug information. Reason: %1 Guidance: The server supports the Live Dump feature, where the detection of a problem results in a kernel memory dump, but no bugcheck and reboot. This allows Microsoft Support to examine memory dumps without requiring a reboot or manual intervention. The reason code indicates the type of problem that was detected. In this case, the server's request to create a live kernel dump was rejected. This is usually due to the live kernel dump throttle, which prevents frequent dumps from consuming too much disk space. Either wait for the throttle limit to expire (by default, 7 days), or contact Microsoft Support for steps to override the throttle. This event is written to the log no more than once per day. The problem that caused the server to the request a live kernel dump may be occuring more frequently. Stalled I/O An I/O is taking an unreasonably long time to complete. Malfunctioning third-party file system minifilter drivers are a common source of this problem. Other causes include failed disks or a client-driven I/O workload that greatly exceeds the server's capacity.
1041	Error reading FSCTL properties information from the registry. Registry value entry %3 will be ignored. Error: %1
1800	CA failure - Failed to set continuously available property on a new or existing file share as the file share is not a cluster share.
1801	CA failure - Failed to set continuously available property on a new or existing file share as Resume Key filter is not started or has failed to attach to the underlying volume.
1802	The server failed to reserve the next ID region in the cluster registry.
1803	The security descriptor differs from the default value. Path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\%1 Guidance: This is typically caused by an administrator or a third party changing the security on the object manually. To reset the security back to the default value, delete the path shown above. Microsoft does not recommend changing the default security of %1 as it may cause application incompatibilities or security concerns.
1905	The server closed the session as part of periodic system cleanup. Session Id: %1 Instance Id: %2 Reason: %3

Event IDs: Section 5.5.2.1

Ereignis-ID	Nachricht
4100	%3 Context: %1 User Data: %2
4101	%3 Context: %1 User Data: %2
4102	%3 Context: %1 User Data: %2
4103	%3 Context: %1 User Data: %2
4104	Creating Scriptblock text (%1 of %2): %3 ScriptBlock ID: %4 Path: %5
4105	Started invocation of ScriptBlock ID: %1 Runspace ID: %2
4106	Completed invocation of ScriptBlock ID: %1 Runspace ID: %2
8193	Creating Runspace object Instance Id: %1
8194	Creating RunspacePool object InstanceId %1 MinRunspaces %2 MaxRunspaces %3
8195	Opening RunspacePool
8196	Modifying activity Id and correlating
8197	Runspace state changed to %1
8198	Attempting session creation retry %1 for error code %2 on session Id %3
12039	Modifying activity Id and correlating
24577	Windows PowerShell ISE has started to run script file %1.
24578	Windows PowerShell ISE has started to run a user-selected script from file %1.
24579	Windows PowerShell ISE is stopping the current command.
24580	Windows PowerShell ISE is resuming the debugger.
24581	Windows PowerShell ISE is stopping the debugger.
24582	Windows PowerShell ISE is stepping into debugging.
24583	Windows PowerShell ISE is stepping over debugging.
24584	Windows PowerShell ISE is stepping out of debugging.
24592	Windows PowerShell ISE is enabling all breakpoints.
24593	Windows PowerShell ISE is disabling all breakpoints.
24594	Windows PowerShell ISE is removing all breakpoints.
24595	Windows PowerShell ISE is setting the breakpoint at line #: %1 of file %2.
24596	Windows PowerShell ISE is removing the breakpoint on line #: %1 of file %2.
24597	Windows PowerShell ISE is enabling the breakpoint on line #: %1 of file %2.
24598	Windows PowerShell ISE is disabling the breakpoint on line #: %1 of file %2.
24599	Windows PowerShell ISE has hit a breakpoint on line #: %1 of file %2.
32777	An unhandled exception occurred in the appdomain. Exception Type: %1 Exception Message: %2

Ereignis-ID	Nachricht
	Exception StackTrace: %3
32784	Runspace Id: %1 Pipeline Id: %2. WSMan reported an error with error code: %3. Error message: %4 StackTrace: %5
40961	PowerShell console is starting up
40962	PowerShell console is ready for user input
46358	Persistence store has reached its maximum specified size
53249	Scheduled Job %1 started at %2
53250	Scheduled Job %1 completed at %2 with state %3
53251	Scheduled Job Exception %1: Message: %2 StackTrace: %3 InnerException: %4
53504	Windows PowerShell has started an IPC listening thread on process: %1 in AppDomain: %2.
53505	Windows PowerShell has ended an IPC listening thread on process: %1 in AppDomain: %2.
53506	An error has occurred in Windows PowerShell IPC listening thread on process: %1 in AppDomain: %2. Error Message: %3.
53507	Windows PowerShell IPC connect on process: %1 in AppDomain: %2 for User: %3.
53508	Windows PowerShell IPC connect on process: %1 in AppDomain: %2 for User: %3.

References

bsi_adm_erh_schb. (2021, March 11). Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/04_OPS_Betrieb/OPS_1_1_2_Ordnungsgemaesse_IT_Administration_Edition_2021.pdf

cis_win10_1809. (2019, November 22). *CIS Microsoft Windows 10 Enterprise (Release 1809) Benchmark v1.6.1*. Retrieved from https://www.cisecurity.org/cis-benchmarks/

ERNW_WP2. (n.d.). SiSyPHuS Win10 (Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10): Work Package 2.

ms_al. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-account-lockout

ms_apc. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-audit-policy-change

ms_app_group. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-application-group-management

ms_attribute_dfl. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/d7422d35-448a-451a-8846-6a7def0044df

ms_audit_pol. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/advanced-security-auditing-faq#what-is-the-interaction-between-basic-audit-policy-settings-and-advanced-audit-policy-settings

ms_authpc. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-authentication-policy-change

ms_code_integrity. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd348642(v=ws.10)

ms_comp_acc. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-computer-account-management

ms_crash_on_audit_fail. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc963220(v=technet.10)

ms_crypt_retrv_obj. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptretrieveobjectbyurlw

ms_domain_attribute_max_join. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd391926(v=ws.10)

ms_ev_coll. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/win32/wec/creating-an-event-collector-subscription

ms_pc. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-process-creation

ms_sec_bl_1809. (2021, March 11). Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=55319

ms_sec_bl_1809. (2021, March 11). Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=55319

ms_sec_principal. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-principals

ms_sens_priv. (2021, March 11). Retrieved from https://docs.microsoft.com/de-de/windows/security/threat-protection/auditing/audit-sensitive-privilege-use

ms_sgm. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management

ms_sl. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-special-logon

ms_ssc. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-state-change

ms_sse. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-system-extension

ms_sysmon. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

ms_task_action. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows/win32/taskschd/task-actions

ms_wevtutil. (2021, March 11). Retrieved from https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil

Abbreviations

ACL: Access Control List 44, 46, 47
BSI: Bundesamts für Sicherheit in der Informationstechnik 3
COM: Component Object Model 35
CredSSP: Credential Security Support Provider 27
CSE: Client Side Extension 40
DLL: Dynamic-link Library 33
DNS: Domain Name System 52, 53, 89, 90, 91
DoS: Denial-of-Service 35
FUS: Fast User Switching 29
ICMP: Internet Control Message Protocol 35
IO: Input/Output 95
LSA: Local Security Authority 27, 65, 84
LTSC: Long-Term Servicing Channel 4
MSS: Microsoft Solutions for Security 13
NTLM: NT (New Technology) LAN Manager 23, 96, 97, 99, 100, 104, 105
NTP: Network Time Protocol 6
PKI: Public Key Infrastructure 37, 38
PNP: Plug-and-Play 36, 41
RDP: Remote Desktop Protocol 28, 29
RPC: Remote Procedure Call 33
SAC: Semi-Annual Channel 4
SMB: Server Message Block 22, 34, 52, 53, 54, 55, 56, 92, 93, 94, 95, 97, 98, 100, 104, 105, 106
SPN: Service Principal Name 34
TBS: TPM Base Service 35, 49, 87, 88
TGT: Ticket Granting Ticket 23
TPM: Trusted Platform Module 35, 44, 49, 50
URL: Uniform Resource Locator 38
USB: Universal Serial Bus 40
UTC: Coordinated Universal Time 6
WinRM: Windows Remote Management 85, 86
WMI: Windows Management Instrumentation 30, 43, 49, 50, 73