Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Empfehlung zur Konfiguration der Protokollierung in Windows 10

Version: 1.0

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Telefon: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

1.1 Zusammenfassung

Dieses Dokument stellt das Ergebnis von Arbeitspaket 10 des Projekts „SiSyPHuS Win10: Studie zu Systemaufbau, Protokollierung, Härtung und Sicherheitsfunktionen in Windows 10“ dar. Das Projekt wird durch die Firma ERNW Enno Rey Netzwerke GmbH im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) durchgeführt.

Ziel dieses Arbeitspakets ist die Erstellung eines umfassenden Protokollierungskonzeptes für die Komponenten von Windows 10. Wie vom Bundesamt für Sicherheit in der Informationstechnik gefordert, ist Windows 10 LTSC 2019, 64 Bit in deutscher Sprache im Fokus dieses Dokuments.

2 Allgemeines

Aufbauend auf den in den Arbeitspaketen erarbeiteten Ergebnissen ist für Windows 10 eine Konfigurationsempfehlung zur Protokollierung erstellt worden, welche es ermöglicht, Angriffsversuche und unerwünschte Aktionen von Windows-Funktionalitäten zu erkennen, welche die Vertraulichkeit, Verfügbarkeit oder Integrität des IT-Systems bedrohen. Die Empfehlung richtet sich an fortgeschrittene Anwender und Administratoren und ist geeignet, die Konfigurationseinstellungen des Betriebssystems direkt umsetzen zu können.

2.1 Geltungsbereich

Das vorliegende Dokument und die darin enthaltenen Konfigurationsempfehlungen sind gültig für das Betriebssystem Microsoft Windows 10 Long Term Servicing Channel (LTSC), Version 2019. Die hierzu äquivalente Semi-Annual Channel (SAC) Version entspricht Windows 10, Version 1809 und ist zu Windows 10 LTSC Version 2019 hinsichtlich des Kernels und der Komponenten, die in beiden Versionen enthalten sind, funktionsgleich. Da LTSC-Versionen auf einen gleichbleibenden Funktionsumfang und Stabilität ausgelegt sind, werden von Microsoft keine Funktionsupgrades nach der Veröffentlichung bereitgestellt und Komponenten, die mit neuen Funktionalitäten versehen werden könnten, wurden entfernt. Zu den wichtigsten fehlenden Komponenten zählt der Edge-Browser, die virtuelle Assistentin Cortana und alle vorinstallierten Universal Windows Apps („Store-Apps“) inkl. dem Microsoft Store.

Die im Nachfolgenden beschriebenen Konfigurationsempfehlungen für die Protokollierung gehen von einem Standardnutzungsszenario, wie der Verwendung eines Windows 10-Systems zur Büroarbeit, aus. Sie können jedoch auch als Grundlage für die Definition von Protokollierungskonfigurationen für spezifischere Anwendungsfälle, wie einem Windows 10-System, das für administrative Tätigkeiten verwendet wird, herangezogen werden.

2.2 Rahmenbedingungen

Die nachfolgend beschriebenen Konfigurationsempfehlungen basieren auf den im Projekt erarbeiteten Analyseergebnissen, auf Security Best Practices sowie auf langjähriger Expertise von ERNW. Zu allen Empfehlungen erfolgt ein Abgleich mit den in der Security Baseline für Windows 10 1809 (ms_sec_bl_1809, 2020) von Microsoft enthaltenen Einstellungen sowie dem Center for Internet Security (CIS) Benchmark (cis_win10_1809, 2019) für Windows 10 Enterprise (Version 1809). Abweichungen von der Security Baseline oder dem CIS-Benchmark werden im Dokument für die betroffenen Einstellungen erläutert und begründet. Sofern Empfehlungen im Dokument mit dem CIS-Benchmark oder der Security Baseline übereinstimmen, wird auf den entsprechenden Abschnitt im CIS-Benchmark bzw. auf die Security Baseline verwiesen, um das Auffinden der jeweiligen Einstellung in den anderen Publikationen zu erleichtern.

Bei der Erstellung dieses Dokuments folgte die Auswahl der konkreten Konfigurationsempfehlungen den folgenden Grundprinzipien zur Erhöhung der Systemsicherheit:

- Erhebung von für die Entdeckung von bekannten und verbreiteten Angriffsszenarien relevanten Daten, so dass diese für eine aktive Überwachung zur Identifikation von versuchten und andauernden Angriffen nutzbar sind.
- Erhebung von für die Aufklärung von bekannten und verbreiteten Angriffsszenarien relevanten Daten, so dass diese für eine weitergehende Analyse im Zuge forensischer Untersuchungen auswertbar sind.
- Erhebung von relevanten Daten zu Konfigurationsänderungen an sicherheitsrelevanten Objekten und der Funktion von sicherheitsrelevanten Komponenten, so dass diese im Zuge einer kontinuierlichen Überwachung des Sicherheitsniveaus eines Systems nutzbar sind.
- Erzwingen von Einstellungen, um eine Modifikation durch den Benutzer zu verhindern.

- Erweitern der Standardkonfiguration, um die Generierung und Speicherung von relevanten Protokollierungsdaten sicherzustellen.
- Berücksichtigung des Datenschutzes, indem Konfigurationen, die zur Preisgabe von sensiblen Daten in Protokollierungsdateien führen können, als solche kenntlich gemacht werden.

Nicht betrachtet wurde die Erhebung von Protokollierungsdaten zur Überwachung und Sicherstellung der operationellen Zuverlässigkeit eines Systems. Ebenso nicht Teil dieses Dokuments ist die konkrete Auswertung der protokollierten Daten.

Ergänzend oder alternativ können die in diesem Dokument definierten Konfigurationsempfehlungen zum Teil auch durch *Sysmon* (ms_sysmon, 2020) abgedeckt werden, welches eine sehr feingranulare Konfiguration über die Bordmittel hinaus erlaubt.

Konfigurationsempfehlungen, die im Zusammenhang mit allgemeiner Härtung des Systems stehen, finden sich in der „Konfigurationsempfehlungen zur Härtung von Windows 10 mit Bordmitteln“ des Projekts SiSyPHuS (Arbeitspaket 11).

Gruppenrichtlinien-Objekte zu den Empfehlungen zur Konfiguration der Protokollierung (AP 10) und zur Härtung (AP 11) werden im Rahmen von Arbeitspaket 12 bereitgestellt.

3 Generelle Maßnahmenempfehlungen

Die folgenden Abschnitte beschreiben generelle Empfehlungen aus dem Bereich Informationssicherheit, die bei der Protokollierung auf einem Windows 10-System berücksichtigt werden sollten. Da diese nicht zwingend über technische Konfiguration (mit Bordmitteln) umsetzbar sind oder über den definierten Rahmen dieses Dokuments hinausgehen, werden diese Maßnahmen nur allgemein beschrieben.

3.1 Zeitsynchronisation der Systeme

In einer IT-Infrastruktur, an der mehrere Systeme beteiligt sind, ist eine zeitliche Korrelation von Protokollierungsdaten verschiedener Quellen essenziell für die Detektion von Angriffen sowie für die Rekonstruktion von Sicherheitsvorfällen im Zuge forensischer Untersuchungen.

Ist die Systemzeit der beteiligten Systeme nicht untereinander synchronisiert, kann dies dazu führen, dass die aus den Protokollierungsdaten hervorgehende Zeiten für Ereignisse deutlich voneinander abweichen, da für die verschiedenen Zeitstempel keine gemeinsame Basis gegeben ist. Somit wäre eine zeitliche Korrelation dieser Daten nicht sinnvoll möglich beziehungsweise würde potenziell falsche Ergebnisse liefern, insbesondere wenn die Protokollierungsdaten auf einem zentralen Protokollierungsserver gespeichert werden.

Aus diesem Grund sollte die Systemzeit aller an der Protokollierung beteiligten Systeme und Anwendungen synchron sein. Wenn sich die beteiligten Systeme in unterschiedlichen Zeitzonen befinden, bietet es sich an UTC als Basis für alle Quellen von Protokolldaten festzulegen. Für die Auswertung der Protokollierungsdaten ist jedoch nur notwendig, dass alle Systeme dieselbe Systemzeit verwenden.

Zeitsynchrone Netzwerke können durch den Einsatz von Zeitservern, z. B. NTP Servern, realisiert werden.

3.2 Zentrale Sammlung der Protokollierungsdaten

Sicherheitsvorfälle betreffen häufig nicht nur einzelne Systeme, sondern eine gesamte IT-Infrastruktur. Werden Protokollierungsdaten nur lokal auf den Systemen vorgehalten, auf denen sie erhoben werden, können diese nur mit hohem Aufwand korreliert werden, um Angriffe auf die gesamte Infrastruktur zu erkennen oder im Zuge forensischer Untersuchungen zu rekonstruieren. Des Weiteren kann ein Angreifer nach der erfolgreichen Kompromittierung eines Systems Manipulationen an den darauf vorgehaltenen Protokollierungsdaten vornehmen, um seine Handlungen zu verschleiern. Aus diesen Gründen sollten die erhobenen Protokollierungsdaten aller Systeme in einer Umgebung in einer zentralen Protokollierungsinfrastruktur gesammelt und vorgehalten werden.

Die Übermittlung der Protokollierungsdaten an die zentrale Protokollierungsinfrastruktur sollte über Betriebssystemmittel wie z. B. Windows Event Forwarding erfolgen. Es sollte jedoch sichergestellt werden, dass die Übermittlung der Daten auf eine Art und Weise erfolgt, die die Integrität und die Vertraulichkeit der Daten sicherstellt (z. B. durch Transportverschlüsselung).

Die zentrale Protokollierungsinfrastruktur ist für die gesamte Sicherheit einer IT-Infrastruktur von großer Bedeutung. Eine Kompromittierung oder ein Ausfall der Protokollierungsinfrastruktur könnte dazu führen, dass Angriffe nicht mehr erkannt und nachvollzogen werden können. Aus diesem Grund sollte sie entsprechend abgesichert werden:

- Um Verfügbarkeit, Integrität und Ausfallsicherheit der Protokollierungsinfrastruktur sicherzustellen, sollte diese aus mehreren verteilten Systemen, im Sinne eines Verbunds von Protokollierungsservern, platziert in einem eigenen Netzwerksegment, bestehen.
- Die Administration der Protokollierungsserver sollte von der Administration der restlichen IT-Infrastruktur separiert sein und den Vorgaben der Grundschutzverordnung für die Administration von Systemen mit erhöhtem Schutzbedarf folgen (siehe (bsi_adm_erh_schb, 2020)).

- Um unautorisierten Zugriff auf die Protokollierungsdaten zu verhindern, sollte ein Zugriffskonzept erstellt und umgesetzt werden, welches regelt, wer auf welche protokollierten Daten zugreifen darf. Die Berechtigungen sollten dabei so restriktiv wie möglich vergeben werden. Des Weiteren sollten eine Softwarelösung zur Verschlüsselung mindestens der Daten-Partitionen, auf denen die Protokollierungsdaten gespeichert werden, eingesetzt werden und die physische Sicherheit der Protokollierungsserver sichergestellt werden.
- Das erwartete Datenaufkommen ist abhängig von der Anzahl der Systeme, dem Nutzungsverhalten und der Konfiguration der Protokollierung. Um sicherzustellen, dass relevante Protokollierungsereignisse nicht verloren gehen oder überschrieben werden, sollte die Kapazität der Protokollierungsinfrastruktur so ausgelegt sein, dass sie die doppelte Menge des erwarteten Datenaufkommens verarbeiten kann und Protokollierungsereignisse für die doppelte Dauer der geplanten Speicherfrist im Datenspeicher vorgehalten werden können.
- Der Verbund von Protokollierungsservern sollte die Protokollierungsdaten von IT-Systemen und Anwendungen zeitnah nach Erzeugung erhalten. Dies soll sicherstellen, dass Ereignisdaten, die einer etwaigen Kompromittierung vorausgehen, bereits direkt nach Entstehung in einen sicheren und gegen Manipulation geschützten Protokollierungsspeicher übertragen werden. Beim Beispiel Windows Event Forwarding erfolgt dies typischerweise durch regelmäßige Weiterleitung der Ereignisdaten durch die Quellsysteme an die zugehörigen Protokollierungsserver. Dieses Vorgehen ist besonders für die flächendeckende Sammlung von Protokollierungsdaten geeignet. Für besonders schützenswerte Systeme sollten die Protokollierungsdaten nicht auf Initiative der Endgeräte an die Server übertragen werden, sondern auf Initiative der Protokollierungsserver auf den Endgeräten über z. B. ein spezifisches Benutzerkonto eingesammelt werden. Dadurch soll unter anderem sichergestellt werden, dass das Ausbleiben der Weiterleitung von Protokollierungsdaten nicht unbemerkt bleibt. Wie dies beispielhaft mit Bordmitteln über Windows Event Forwarding umsetzbar ist, wird von Microsoft hier beschrieben: (ms_ev_coll, 2020).
- Um einen Ausfall der Protokollierungsinfrastruktur zu vermeiden und somit sicherzustellen, dass keine Protokollierungsdaten verloren gehen, sollte die zentrale Protokollierungsinfrastruktur kontinuierlich auf Fehlerzustände hin überwacht werden.
- Um den Verlust von gespeicherten Protokollierungsdaten zu verhindern und die Integrität der gespeicherten Protokollierungsdaten sicherzustellen, sollte technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden können.

3.3 Umgang mit sensitiven Protokollierungsdaten

Protokollierungsdaten können sensitive Daten enthalten und bedürfen deshalb eines besonderen Schutzes. Dies können sowohl sensible Benutzerinformationen als auch für einen Angreifer potenziell wertvolle Informationen, wie Passwörter oder Informationen über die interne Struktur der IT-Infrastruktur, sein. Aus diesem Grund sollten Protokollierungsdaten nur verschlüsselt übertragen werden und es sollte sichergestellt werden, dass kein unautorisierter Zugriff auf gespeicherte Protokollierungsdaten erfolgt. Jeder Zugriff auf diese Daten sollte wiederum protokolliert werden. Des Weiteren sollte eine Speicherfrist für Protokollierungsdaten definiert werden, nach deren Ablauf diese einem festgelegten Prozess folgend gelöscht werden. Protokollierungsdaten, die personenbezogene Daten enthalten, sollten nur pseudonymisiert in einer zentralen Protokollierungsinfrastruktur gespeichert werden. Zur Analyse von Sicherheitsvorfällen sollte jedoch sichergestellt sein, dass eine Rückauflösung der Pseudonyme innerhalb der Speicherfrist möglich ist. Außerdem sollte bei der Verarbeitung und Speicherung von Protokollierungsdaten, die personenbezogenen Angaben enthalten (können), geprüft werden, welche gesetzlichen Bestimmungen und betriebsinternen Vorgaben ggf. zu berücksichtigen sind.

4 Konfigurationsempfehlungen: Systemweite Einstellungen

Die folgenden Abschnitte enthalten Konfigurationsempfehlungen in Form von Gruppenrichtlinien, die Einfluss auf das generelle Protokollierungsverhalten des Systems haben. Konfigurationsempfehlungen für spezifische Ereignisprotokolle und Überwachungsrichtlinien, finden sich in Kapitel 5.

4.1 Sicherheitsoptionen

Dieser Abschnitt enthält Empfehlungen für die Konfiguration von Sicherheitsoptionen.

4.1.1 Stellen Sie sicher, dass „Überwachung: System sofort herunterfahren, wenn Sicherheitsüberprüfungen nicht protokolliert werden können“ auf den Wert „Deaktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 2.3.2.2 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Standardwert
Deaktiviert (Das System fährt nicht herunter, wenn nicht protokolliert werden kann.)

Hinweis: Für den Fall, dass unter keinen Umständen Ereignisse des Sicherheit-Ereignisprotokolls verloren gehen dürfen, sollte diese Einstellung auf „Aktiviert“ gesetzt werden.

4.1.2 Stellen Sie sicher, dass „Überwachung: Unterkategorieeinstellungen der Überwachungsrichtlinie erzwingen (Windows Vista oder höher), um Kategorieeinstellungen der Überwachungsrichtlinie außer Kraft zu setzen“ auf den Wert „Aktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 2.3.2.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Sicherheitsoptionen

Standardwert
Aktiviert (Einstellungen der erweiterten Überwachungsrichtlinienkonfiguration werden verwendet.)

4.2 Windows Defender Firewall mit erweiterter Sicherheit

Dieser Abschnitt enthält Empfehlungen zur Konfiguration der Windows-Firewall.

4.2.1 Domänenprofil

Dieser Abschnitt enthält Empfehlungen für das Domänenprofil der Windows Defender Firewall.

4.2.1.1 Stellen Sie sicher, dass „Windows Firewall: Domänenprofil: Protokollierung: Name“ auf den Wert „%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.1.5 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Domänenprofil

Standardwert
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.1.2 Stellen Sie sicher, dass „Windows Firewall: Domänenprofil: Protokollierung: Größenlimit (KB)“ auf den Wert „16.384 KB oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.1.6 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Domänenprofil

Standardwert
4.096 KB

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

4.2.1.3 Stellen Sie sicher, dass „Windows Firewall: Domänenprofil: Protokollierung: Verworfene Pakete protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.1.7 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Domänenprofil

Standardwert
Nein (Informationen über verworfene Pakete werden nicht protokolliert.)

4.2.1.4 Stellen Sie sicher, dass „Windows Firewall: Domänenprofil: Protokollierung: Erfolgreiche Verbindungen protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.1.8 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Domänenprofil

Standardwert
Nein (Informationen über erfolgreiche Verbindungen werden nicht protokolliert.)

4.2.2 Privates Profil

Dieser Abschnitt enthält Empfehlungen für das Private Profil der Windows Defender Firewall.

4.2.2.1 Stellen Sie sicher, dass „Windows Firewall: Privates Profil: Protokollierung: Name“ auf den Wert „%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.2.5 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Privates Profil

Standardwert
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.2.2 Stellen Sie sicher, dass „Windows Firewall: Privates Profil: Protokollierung: Größenlimit (KB)“ auf den Wert „16.384 KB oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.2.6 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Privates Profil

Standardwert
4.096 KB

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem

solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

4.2.2.3 Stellen Sie sicher, dass „Windows Firewall: Privates Profil: Protokollierung: Verworfene Pakete protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.2.7 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Privates Profil

Standardwert
Nein (Informationen über verworfene Pakete werden nicht protokolliert.)

4.2.2.4 Stellen Sie sicher, dass „Windows Firewall: Privates Profil: Protokollierung: Erfolgreiche Verbindungen protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.2.8 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Privates Profil

Standardwert
Nein (Informationen über erfolgreiche Verbindungen werden nicht protokolliert.)

4.2.3 Öffentliches Profil

Dieser Abschnitt enthält Empfehlungen für das öffentliche Profil der Windows Defender Firewall.

4.2.3.1 Stellen Sie sicher, dass „Windows Firewall: Öffentliches Profil: Protokollierung: Name“ auf den Wert „%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.3.5 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Öffentliches Profil

Standardwert
%SystemRoot%\System32\logfiles\firewall\pfirewall.log

4.2.3.2 Stellen Sie sicher, dass „Windows Firewall: Öffentliches Profil: Protokollierung: Größenlimit (KB)“ auf den Wert „16.384 KB oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.3.6 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Öffentliches Profil

Standardwert
4.096 KB

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

4.2.3.3 Stellen Sie sicher, dass „Windows Firewall: Öffentliches Profil: Protokollierung: Verworfene Pakete protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.3.7 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Öffentliches Profil

Standardwert
Nein (Informationen über verworfene Pakete werden nicht protokolliert.)

4.2.3.4 Stellen Sie sicher, dass „Windows Firewall: Öffentliches Profil: Protokollierung: Erfolgreiche Verbindungen protokollieren“ auf den Wert „Ja“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 9.3.8 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Windows Defender Firewall mit erweiterter Sicherheit\Öffentliches Profil

Standardwert
Nein (Informationen über erfolgreiche Verbindungen werden nicht protokolliert.)

4.3 Administrative Vorlagen

Dieser Abschnitt enthält computerbasierte Empfehlungen von Administrativen Vorlagen der Gruppenrichtlinien (ADMX).

4.3.1 MSS (Legacy)

Dieser Abschnitt enthält Empfehlungen für die Konfiguration von Microsoft Solutions for Security (MSS).

Diese Einstellungen werden von der Gruppenrichtlinienvorlage `MSS-legacy.admx/adml` bereitgestellt, die von Microsoft veröffentlicht wurde (ms_sec_bl_1809, 2020) und ausschließlich in englischer Sprache verfügbar ist.

4.3.1.1 Stellen Sie sicher, dass „MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning“ auf den Wert „Aktiviert: 90% oder weniger“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.4.13 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\MSS (Legacy)

Standardwert
0 % (Es wird kein warnendes Ereignis erzeugt.)

Hinweis: Wenn das Ereignisprotokoll so konfiguriert ist, dass Ereignisse nach Bedarf oder nach einem gewissen Alter automatisch überschrieben werden, wird dieses Ereignis nicht erzeugt.

4.3.2 Ereignisprotokolldienst

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des Ereignisprotokolldienstes.

Dieser Abschnitt mit Gruppenrichtlinien wird von der Gruppenrichtlinienvorlage `EventLog.admx/adml` bereitgestellt, die in allen Versionen der Microsoft Windows Administrativen Vorlagen enthalten ist.

4.3.2.1 Anwendung

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des Anwendung-Ereignisprotokolls.

4.3.2.1.1 Stellen Sie sicher, dass „Maximale Protokolldateigröße (KB) angeben“ auf den Wert „32.768 oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.1.2 *des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Anwendung

Standardwert
Deaktiviert (Die Standardgröße der Protokolldatei beträgt 20.480 KB und kann lokal umkonfiguriert werden.)

4.3.2.1.2 Stellen Sie sicher, dass „Verhalten des Ereignisprotokolls steuern, wenn die Protokolldatei ihre Maximalgröße erreicht“ auf den Wert „Deaktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.1.1 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Anwendung

Standardwert
Deaktiviert (Wenn die Protokolldatei ihre maximale Größe erreicht, überschreiben neue Ereignisse alte Ereignisse.)

Hinweis: Alte Ereignisse können unter Umständen beibehalten werden, abhängig davon, wie die Einstellung „Volles Protokoll automatisch sichern“ konfiguriert ist.

4.3.2.2 Setup

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des Setup-Ereignisprotokolls.

4.3.2.2.1 Stellen Sie sicher, dass „Maximale Protokolldateigröße (KB) angeben“ auf den Wert „32.768 oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.3.2 *des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Setup

Standardwert
Deaktiviert (Die Standardgröße der Protokolldatei beträgt 20.480 KB und kann lokal umkonfiguriert werden.)

4.3.2.2.2 Stellen Sie sicher, dass „Verhalten des Ereignisprotokolls steuern, wenn die Protokolldatei ihre Maximalgröße erreicht“ auf den Wert „Deaktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.3.1 *des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Setup

Standardwert
Deaktiviert (Wenn die Protokolldatei ihre maximale Größe erreicht, überschreiben neue Ereignisse alte Ereignisse.)

Hinweis: Alte Ereignisse können unter Umständen beibehalten werden, abhängig davon, wie die Einstellung „Volles Protokoll automatisch sichern" konfiguriert ist.

4.3.2.3 Sicherheit

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des Sicherheit-Ereignisprotokolls.

4.3.2.3.1 Stellen Sie sicher, dass „Maximale Protokolldateigröße (KB) angeben" auf den Wert „524.288 oder größer" gesetzt ist.

Siehe auch 18.9.26.2.2 *des CIS Benchmark und die Konfigurationsempfehlung der Microsoft Security Baseline.*

Mit dieser Einstellung wird die maximale Protokollgröße des Protokolls *Sicherheit* konfiguriert.

Begründung

Für eine umfassende Protokollierung von sicherheitsrelevanten Ereignissen sind die gängigen Empfehlungen für die Größe des Protokolls *Sicherheit* noch nicht ausreichend und sollte somit mindestens auf den empfohlenen Wert angehoben werden. Insbesondere wenn u. a. auch die Prozesserstellung protokolliert wird.

Auswirkung

Die Größe der Protokolldatei für das Protokoll *Sicherheit* wird auf den empfohlenen Wert erhöht.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Sicherheit

Standardwert
Deaktiviert (Die Standardgröße der Protokolldatei beträgt 20.480 KB und kann lokal umkonfiguriert werden.)

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

4.3.2.3.2 Stellen Sie sicher, dass „Verhalten des Ereignisprotokolls steuern, wenn die Protokolldatei ihre Maximalgröße erreicht“ auf den Wert „Deaktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.2.1 *des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\Sicherheit

Standardwert
Deaktiviert (Wenn die Protokolldatei ihre maximale Größe erreicht, überschreiben neue Ereignisse alte Ereignisse.)

Hinweis: Alte Ereignisse können unter Umständen beibehalten werden, abhängig davon, wie die Einstellung „Volles Protokoll automatisch sichern“ konfiguriert ist.

4.3.2.4 System

Dieser Abschnitt enthält Empfehlungen für die Konfiguration des System-Ereignisprotokolls.

4.3.2.4.1 Stellen Sie sicher, dass „Maximale Protokolldateigröße (KB) angeben“ auf den Wert „32.768 oder größer“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.4.2 *des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\System

Standardwert
Deaktiviert (Die Standardgröße der Protokolldatei beträgt 20.480 KB und kann lokal umkonfiguriert werden.)

4.3.2.4.2 Stellen Sie sicher, dass „Verhalten des Ereignisprotokolls steuern, wenn die Protokolldatei ihre Maximalgröße erreicht“ auf den Wert „Deaktiviert“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 18.9.26.4.1 *des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Ereignisprotokolldienst\System

Standardwert
Deaktiviert (Wenn die Protokolldatei ihre maximale Größe erreicht, überschreiben neue Ereignisse alte Ereignisse.)

Hinweis: Alte Ereignisse können unter Umständen beibehalten werden, abhängig davon, wie die Einstellung „Volles Protokoll automatisch sichern" konfiguriert ist.

4.3.3 Prozesserstellung überwachen

Dieser Abschnitt enthält Einstellungen zur Überwachung von Ereignissen zur Prozesserstellung.

Dieser Abschnitt über Gruppenrichtlinien wird von der Gruppenrichtlinienvorlage `AuditSettings.admx/adml` bereitgestellt, die in den Administrativen Vorlagen für Microsoft Windows 8.1 & Server 2012 R2 (oder neuer) enthalten ist.

4.3.3.1 Stellen Sie sicher, dass „Befehlszeile in Prozesserstellungsereignisse einschließen" auf den Wert „Aktiviert" gesetzt ist.

Siehe auch 18.8.3.1 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Standardmäßig enthalten Prozesserstellungsereignisse (Ereignis-ID 4688 im Sicherheitsereignisprotokoll) keine Informationen darüber, mit welchen Argumenten ein Prozess aufgerufen wurde. Mit dieser Einstellung lässt sich dieses Verhalten beeinflussen.

Begründung

Die Standardkonfiguration der Prozesserstellungsereignisse liefert bereits wichtige Informationen zur Detektion von schadhaften Aktionen eines Angreifers. Dazu gehören z. B. der Prozess-Name oder der Name des ausführenden Kontos. Diese können aber unter Umständen nicht ausreichend sein, um einen aktiven Angriff zu detektieren bzw. in einer forensischen Analyse die tatsächlichen Aktionen nachzuvollziehen, da z. B. ein Prozess-Name leicht änderbar ist. Die zusätzliche Protokollierung der Prozessargumente kann Aufschluss darüber geben, was die tatsächliche Intention eines Prozessstarts war sowie welche Daten und Informationen an diesen Prozess übergeben wurden.

Auswirkung

Sobald diese Einstellung aktiviert ist, werden alle Befehlszeilenargumente bei einem Prozessstart aufgezeichnet und im Sicherheitsprotokoll gespeichert. Dies kann auch sensitive Informationen wie z. B. Passwörter umfassen, wenn diese im Klartext auf der Befehlszeile eingegeben wurden. Somit hat jeder Benutzer, der lesenden Zugriff auf das Sicherheitsprotokoll hat, auch die Möglichkeit diese sensitiven Informationen zu lesen. Dies gilt auch, wenn das Protokoll auf einem anderen System (z. B. zur Aufbewahrung) abgespeichert wurde.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\System\Prozesserstellung überwachen

Standardwert
Deaktiviert (Die Befehlszeile wird nicht in Prozesserstellungsereignisse eingeschlossen.)

4.3.4 Windows PowerShell

Da PowerShell über .NET auf viele Systemressourcen zugreifen kann und einfach zu verwenden ist, können Angreifer PowerShell für schadhafte Zwecke verwenden. Dazu zählt zum einen die vollständige Kompromittierung von Windows-Instanzen, zum anderen das anschließende Aufrechterhalten des Zugriffs auf dieses System. Die umfassende Protokollierung von PowerShell-Ereignissen und deren Analyse ist dabei von entscheidender Bedeutung, um die böswillige Verwendung frühzeitig zu erkennen.

Die folgenden Einstellungen (Abschnitte 4.3.4.1, 4.3.4.2 und 4.3.4.3) können, je nachdem wie PowerShell in einer bestimmten Windows-Instanz verwendet wird, eine erhebliche Menge an Protokolldaten erzeugen. Sie bieten jedoch die Möglichkeit, festzustellen, ob böswillige Aktivitäten stattgefunden haben. Wenn die Protokolldaten in Echtzeit verarbeitet werden, kann somit möglicherweise böswillige PowerShell-Aktivität zum Zeitpunkt der eigentlichen Ausführung erkannt werden. Mindestens hilft es jedoch bei einer forensischen Analyse den tatsächlichen Hergang zu rekonstruieren.

Es ist wichtig zu betonen, dass die Bewertung, ob eine bestimmte PowerShell-Aktivität schädlich ist oder nicht, davon abhängt, wie PowerShell auf einer bestimmten Windows-Instanz verwendet wird. Dies kann für verschiedene Fälle unterschiedlich sein. Sobald Aktivitäten identifiziert wurden, die für die Windows-Instanz nicht typisch sind, ist eine genauere Untersuchung der Protokolldaten erforderlich, um den genauen Grund der Aktivität zu ermitteln und zu bewerten, ob die Aktivität böswillig war oder nicht.

Es gibt einige allgemeine Indikatoren für böswillige PowerShell-Aktivitäten, die in Protokolldaten beobachtet werden können:

- Erstellen von PowerShell-Sitzungen (Ereignis-ID 8193, siehe Anhang, Absatz „Ereignis-IDs: Abs. 5.5.2.1“): Wenn ein Prozess, der keine PowerShell-Sitzungen erstellen soll, diese erstellt, weist dies möglicherweise darauf hin, dass es sich bei dem Prozess um Schadsoftware handelt;
- atypischer Inhalt von PowerShell-Skripten (Ereignis-ID 4104, siehe Anhang, Absatz „Ereignis-IDs: Abs. 5.5.2.1“): Ein Beispiel ist ein codierter Skriptinhalt oder ein in inkonsistenter Weise geschriebener Skriptinhalt (z. B. inkonsistente Groß- und Kleinschreibung). Dies weist auf die Ausführung eines schädlichen PowerShell-Skripts hin;
- atypische PowerShell-Befehle (ausgeführt als Teil eines Skripts oder vom Benutzer über die Befehlszeilenschnittstelle des PowerShell-Hostprozesses eingegeben): Ein Beispiel ist die Ausführung des PowerShell-Befehls `IEX` zum Herstellen einer Netzwerkverbindung, wenn solche Verbindungen normalerweise nicht über PowerShell hergestellt werden;
- atypische PowerShell/.NET-Aktivitäten: Diese Aktivitäten können durch Untersuchen der Protokolldaten identifiziert werden, die von der Microsoft-Windows-PowerShell / Operational-Protokollquelle erstellt wurden (z. B. Ereignis-ID 4103, siehe Anhang, Absatz „Ereignis-IDs: Abs. 5.5.2.1“). Auf hoher Ebene können solche Aktivitäten durch Zeichenfolgen identifiziert werden. Die Zeichenfolge *MiniDumpWriteDump* gibt beispielsweise an, dass PowerShell den einem Prozess zugewiesenen Speicherbereich extrahiert hat. Dieser Speicherbereich kann z. B. vertrauliche Benutzerdaten enthalten. Wenn diese Aktivität normalerweise nicht mit Hilfe der PowerShell ausgeführt wird, handelt es sich möglicherweise um eine böswillige PowerShell-Aktivität.

4.3.4.1 Stellen Sie sicher, dass „Modulprotokollierung aktivieren“ auf den Wert „Aktiviert“ und die Option „Modulnamen“ auf den Wert „*“ gesetzt ist.

Diese Einstellung aktiviert die Protokollierung von benutzerspezifizierten PowerShell-Modulen.

Hinweis: Abhängig von der Nutzung des Systems können die überwachten PowerShell-Module eingegrenzt werden (über die Option „Modulnamen“), um die Menge an Protokolldaten zu reduzieren.

Begründung

Mit der Modulprotokollierung werden für alle spezifizierten PowerShell-Module Ereignisse der Pipelineausführung aufgezeichnet. Dies umfasst die Befehle, die ausgeführt werden, einschließlich der genauen Befehlsaufrufe und einem Teil der ausgeführten Skripte. Daten, die für die Ausgabe bestimmt sind, werden ebenfalls zum Teil aufgezeichnet. Obwohl die Modulprotokollierung nicht alle Einzelheiten der Ausführung und der Ausgabeergebnisse enthält, stellt es eine sinnvolle Ergänzung zu den anderen PowerShell-Protokollmechanismen dar.

Auswirkung

Sobald diese Einstellung aktiviert ist, werden Teile von ausgeführten PowerShell-Befehlen und -Skripten sowie PowerShell-Ausgaben aufgezeichnet und im Protokoll *Microsoft-Windows-PowerShell/Operational* gespeichert. Dies kann auch sensitive Informationen wie z. B. Passwörter umfassen, wenn diese im Klartext eingegeben wurden. Somit hat jeder Benutzer, der lesenden Zugriff auf das Protokoll hat, auch die Möglichkeit diese sensitiven Informationen zu lesen. Dies gilt auch, wenn das Protokoll auf einem anderen System (z. B. zur Aufbewahrung) abgespeichert wurde.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows PowerShell

Standardwert
Deaktiviert (PowerShell-Module werden standardmäßig nicht protokolliert. Die *LogPipelineExecutionDetails*-Eigenschaft eines PowerShell-Moduls gibt vor, ob Ausführungsereignisse protokolliert werden.)

4.3.4.2 Stellen Sie sicher, dass „Protokollierung von PowerShell-Skriptblöcken aktivieren“ auf den Wert „Aktiviert“ gesetzt ist.

Siehe auch 18.9.95.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Diese Einstellung konfiguriert die Protokollierung des Inhalts von ausgeführten PowerShell-Skripten.

Hinweis: Die Option „Start-/Stoppereignisse für den Aufruf von Skriptblöcken protokollieren“ sollte nicht aktiviert werden, da diese Konfiguration zu einem hohen Ereignisaufkommen mit hohen Datenmengen führt.

Begründung

Die Protokollierung von Skriptblöcken erlaubt es, die Verarbeitung von allen Befehlen und Skripten aufzuzeichnen, so wie sie von der PowerShell ausgeführt werden. Somit werden z. B. nicht nur ausgeführte enkodierte Befehle (wie sie häufig bei Schadsoftware vorkommen) im Protokoll gespeichert, sondern zusätzlich auch die dekodierten Befehle, sobald sie ausgeführt werden. Die Aufzeichnung geschieht unabhängig davon, ob die Befehle oder Skripte interaktiv oder automatisiert aufgerufen werden. Die

Protokollierung der Skriptblöcke enthält jedoch keine Informationen über die Ausgabe des ausgeführten Codes.

Auswirkung

Sobald diese Einstellung aktiviert ist, werden alle ausgeführten PowerShell-Befehle und -Skripte aufgezeichnet und im Protokoll *Microsoft-Windows-PowerShell/Operational* gespeichert. Dies kann auch sensitive Informationen wie z. B. Passwörter umfassen, wenn diese im Klartext eingegeben wurden. Somit hat jeder Benutzer, der lesenden Zugriff auf das Protokoll hat, auch die Möglichkeit diese sensitiven Informationen zu lesen. Dies gilt auch, wenn das Protokoll auf einem anderen System (z. B. zur Aufbewahrung) abgespeichert wurde.

Hinweis: Die im CIS Benchmark enthaltene Warnung, dass alle angemeldeten Benutzer lesenden Zugriff auf das Protokoll „Microsoft-Windows-PowerShell/Operational" haben, ist nicht korrekt. Standardmäßig hat nur die Benutzergruppe der Administratoren (abgesehen von weiteren Systemkonten) die entsprechenden Berechtigungen (in diesem Fall Vollzugriff).

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows PowerShell

Standardwert
Aktiviert (PowerShell-Skriptblöcke werden protokolliert.)

4.3.4.3 Stellen Sie sicher, dass „PowerShell-Aufzeichnung aktivieren" auf den Wert „Aktiviert" gesetzt und die Option „Aufrufheader einschließen" aktiviert ist.

Siehe auch 18.9.95.2 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Diese Einstellung konfiguriert die Protokollierung von Benutzereingaben und PowerShell-Ausgaben, die auf der Befehlszeilenschnittstelle des PowerShell-Hostprozesses (`powershell.exe`) angezeigt werden. Die Protokollierung erfolgt in eine Textdatei, dessen Speicherverzeichnis durch diese Richtlinie konfiguriert wird.

Hinweis: In der Standardkonfiguration werden alle Aufzeichnungen als Textdateien im Verzeichnis „Dokumente" des jeweiligen ausführenden Benutzers gespeichert. Um die Aufzeichnungen zentral zu sichern und vor unautorisierter Modifikation zu schützen, sollte eine ausschließlich schreibbare Netzwerkfreigabe als Verzeichnis für die Aufzeichnungsausgabe konfiguriert werden.

Begründung

Die PowerShell-Aufzeichnung erzeugt für jeden Benutzer und jede PowerShell-Sitzung ein sog. Transkript, in dem alle Ein- und Ausgaben (inkl. Zeitstempel) der Sitzung aufgezeichnet werden. Ergänzend zu den anderen Protokollmechanismen, können diese Aufzeichnungen genutzt werden, um bei einer etwaigen Analyse auf einer hohen Ebene einen ersten Überblick über PowerShell-Aktivität zu erhalten, da diese Art der Protokollierung eine überschaubare Menge an Daten erzeugt. Es besteht jedoch die Einschränkung, dass

nur Informationen gesichert werden, die direkt auf der PowerShell-Befehlszeile sichtbar sind. Dies schließt Informationen im Kontext ausgeführter Skripte und Daten, die auf andere Weise ausgegeben wurden (z. B. direkt in eine Datei geschrieben wurden), aus.

Auswirkung

Mit dieser Einstellung werden alle PowerShell-Eingaben und -Ausgaben in der Aufzeichnungsdatei *PowerShell_transcript* gespeichert. Dies kann auch sensitive Informationen wie z. B. Passwörter umfassen, wenn diese im Klartext eingegeben wurden. Somit hat jeder Benutzer, der lesenden Zugriff auf die Aufzeichnungsdatei hat, auch die Möglichkeit diese sensitiven Informationen zu lesen. Dies gilt auch, wenn die Aufzeichnungsdatei auf einem anderen System (z. B. zur Aufbewahrung) abgespeichert wurde.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Administrative Vorlagen\Windows-Komponenten\Windows PowerShell

Standardwert

Deaktiviert (Eine Aufzeichnung aller PowerShell-Sitzungen findet nicht statt.)

5 Konfigurationsempfehlungen: Überwachungsrichtlinien und Ereignisprotokolle

Die folgenden Abschnitte enthalten Konfigurationsempfehlungen für spezifische Einstellungen der Ereignisprotokolle und Überwachungsrichtlinien. Empfehlungen, die Einfluss auf das generelle Protokollierungsverhalten des Systems haben, finden sich in Kapitel 4.

Sämtliche Konfigurationen der Überwachungsrichtlinie sind ausschließlich über die Erweiterte Überwachungsrichtlinienkonfiguration vorzunehmen. Eine Verwendung von sowohl der normalen Überwachungsrichtlinie (unter dem Gruppenrichtlinien-Pfad *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Überwachungsrichtlinie*) als auch der erweiterten Überwachungsrichtlinie (unter dem Gruppenrichtlinien-Pfad *Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration*) kann zu einem unerwarteten Verhalten der Protokollierung führen, da in einem solchen Fall die Einstellungen für das Betriebssystem nicht eindeutig sind (siehe (ms_audit_pol, 2020)).

Während die Empfehlungen aus der Microsoft Security Baseline durch die in diesem Dokument enthalten Empfehlungen vollständig abgedeckt sind, existiert für die folgenden Konfigurationsempfehlungen für die Überwachungsrichtlinie aus dem CIS Benchmark keine äquivalente Empfehlung:

Referenz CIS Benchmark	Name der Richtlinieneinstellung	Begründung
17.2.1	Anwendungsgruppenverwaltung überwachen	Anwendungsgruppen werden nur vom sog. Authorization Manager genutzt, der seit Windows Server 2012 nicht mehr von Microsoft unterstützt wird (siehe (ms_app_group, 2020)).
17.2.2	Computerkontoverwaltung überwachen	In der Ereigniskategorie Computerkontenverwaltung werden nur auf Domänencontrollern Einträge erzeugt (siehe (ms_comp_acc, 2020)).
17.9.1	IPsec-Treiber überwachen	Die Ereigniskategorie IPsec-Treiber enthält nur relevante Einträge, wenn IPsec eingesetzt wird. Dies geht über den Geltungsbereich dieses Dokuments hinaus.

Die empfohlenen Konfigurationen der Anwendungs- und Dienstprotokolle können auf unterschiedlichen Wegen umgesetzt werden. Zu den Hauptarten zählen die Konfiguration über die `Ereignisanzeige` (in den Eigenschaften der einzelnen Protokolle), über den `Registrierung-Editor` (unter dem Registrierung-Pfad *HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels*) und über die Kommandozeilenanwendung `wevtutil.exe` (im Verzeichnis *C:\Windows\System32*). Da eine Konfiguration über die `Ereignisanzeige` für das automatische Ausrollen der Einstellungen ungeeignet ist und die Konfiguration über die Registrierung sich als unzuverlässig herausgestellt hat (Einstellungen werden auch nach einem Neustart nicht immer korrekt angewendet), wird in diesem Dokument die Konfiguration über die Anwendung `wevtutil.exe` beschrieben. Bei der `wevtutil.exe` Anwendung handelt es sich um ein Befehlszeilenwerkzeug, mit dessen Hilfe unter anderem Anwendungs- und Dienstprotokolle aktiviert und konfiguriert werden können. `wevtutil.exe` wird mit Windows 10 ausgeliefert. Die folgenden Parameter werden benötigt, um die empfohlenen Einstellungen umzusetzen:

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

- `set-log` gibt an, dass die Eigenschaften eines Protokolls modifiziert werden sollen
- `$log` gibt den Namen des Ereignisprotokolls an
- `/enabled:true` gibt an, dass das Ereignisprotokoll aktiviert werden soll

- `/retention:false` gibt an, dass Ereignisse bei Bedarf überschrieben werden dürfen (älteste Ereignisse zuerst)
- `/maxsize:33554432` gibt die Maximalgröße (in Bytes) des Ereignisprotokolls an (in diesem Beispiel 32.768 KB)

Detaillierte Informationen zum `wevtutil.exe` finden sich unter (ms_wevtutil, 2020).

Die nachfolgenden Kapitel beschreiben die notwendige Konfiguration, um eine umfassende Protokollierung in den folgenden Bereichen von Systemaktivität zu ermöglichen:

- Aktivität von Konten (z. B. Anmeldungen von Benutzerkonten)
- Aktivität von Kernsystemkomponenten (z. B. Installation eines System-Dienstes)
- Konfigurationsänderungen (z. B. Änderung von Gruppenmitgliedschaften)
- Netzwerkaktivität (z. B. Fehler beim SMB-Verbindungsaufbau)
- Prozessaktivität (z. B. Erstellung neuer Prozesse)
- Registrierungsaktivität (z. B. Änderung eines Registrierungs-Schlüssels)

Die zugehörigen Tabellen im Anhang enthalten die Ereignis-IDs und die entsprechenden Beschreibungen (sogenannte Nachrichten), unter denen Windows 10 Ereignisse für die entsprechenden Protokolle generieren kann (Spalte *Ereignis-ID* bzw. *Nachricht*). Hier wurde ebenfalls die Anwendung `wevtutil.exe` verwendet, um mögliche Ereignis-IDs und Nachrichten anzuzeigen (siehe (ERNW_WP2), Abschnitt 4.3). In den Tabellen im Anhang kennzeichnen Zahlen mit vorangestelltem Prozentzeichen (%) den dynamischen Teil des Ereignisses, der zur Laufzeit generiert wird. Die Nachrichten in diesen Tabellen werden so dargestellt, wie sie von Microsoft bereitgestellt werden.

5.1 Aktivität von Konten

Konten im Kontext des Windows-Betriebssystems sind Benutzern, Computern oder Diensten zugeordnet. Jedes Konto hat eine im Verwendungskontext einzigartige Kennung, den Kontennamen, und Zugangsdaten mit sich verknüpft. Authentifizierung basiert auf der Prüfung der Kontenkennung, sowie der angegebenen Zugangsdaten. Die Autorisierung erfolgt in der Regel auf Basis des verwendeten Kontos.

Unter Kontenaktivität werden im folgenden Konfigurationsänderungen, die an Konten vorgenommen werden, Ereignisse, die im Zusammenhang mit der Authentifizierung und Autorisierung von Konten stehen, sowie die Verwendung von vertraulichen Berechtigungen verstanden. Nähere Informationen, welche Berechtigungen Microsoft als vertrauliche Berechtigungen definiert, befinden sich unter (ms_sens_priv, 2020).

Die Protokollierung von Kontenaktivitäten dient dazu sichtbar zu machen, welche Konten, wann und auf welche Weise versuchen sich an einem System anzumelden. Des Weiteren kann nachvollzogen werden welche Berechtigungen (Privilegien) sie besitzen und welche Änderungen an Konten und ihren Berechtigungen (Privilegien) vorgenommen werden. Dadurch kann die Protokollierung dazu beitragen ein System oder eine Umgebung auf verschiedenste Angriffe auf Konten hin zu überwachen, sowie die Verwendung potenziell kompromittierter Konten im Zuge forensischer Untersuchungen zu rekonstruieren.

Da die Kompromittierung von Konten (sowie den zugehörigen Zugangsdaten) und die darauffolgende Wiederverwendung dieser zu den Hauptangriffsvektoren in Windows-Umgebungen zählen, wird besonderes Augenmerk auf die Protokollierung von Kontenaktivität gelegt. Beispielhaft können die folgenden Szenarien der Protokollanalyse genannt werden, die durch die empfohlenen Einstellungen möglich sind:

- Der Versuch Konten durch Brute Force Angriffe oder Password Spraying zu kompromittieren wird sich in einer hohen Zahl von fehlgeschlagenen Authentifizierungsversuchen (einzelner oder vieler Konten) und somit Anmeldeereignissen innerhalb eines kurzen Zeitraumes niederschlagen.
- Ungewöhnliches Anmeldeverhalten, wie zum Beispiel das Anmelden außerhalb der Arbeitszeit oder unter Verwendung von Anmeldearten (protokolliert in Anmeldeereignissen), die untypisch für das verwendete Konto sind, können wiederum Hinweise auf den Missbrauch valider, jedoch kompromittierter, Konten sein.
- Die Verwendung von vertraulichen Berechtigungen kann auf das Ausführen von sicherheitskritischen Aktionen hinweisen. Diese können im Zuge legitimer Tätigkeiten auftreten, aber auch durch Angriffstechniken. So könnte die Verwendung des sog. Debug-Privilegs ein Hinweis auf die Verwendung des Angriffswerkzeugs *mimikatz* sein.
- Protokollierte Kontenaktivitäten können auch Hinweise auf Versuche von Angreifern Persistenz auf einem System oder in einer Umgebung zu erreichen geben. Die Erstellung neuer Konten, sowie Änderungen an Berechtigungen oder Konfigurationen von bestehenden Konten könnten einen solchen Versuch darstellen.

In Active Directory-Umgebungen werden zudem die folgenden zusätzlichen Beispielszenarien relevant:

- Die Protokollierung von Kontenaktivitäten kann bei Systemen, die Mitglied einer Active Directory-Umgebung sind, in Kombination mit Ereignissen, die auf Domain Controllern und Servern generiert werden, auch Hinweise auf die Verwendung von gestohlenen und gefälschten Kerberos-Tickets geben. Wenn für ein Konto z. B. kein gültiges *Ticket Granting Ticket* (TGT) existiert, das Konto sich also nicht per Kerberos-Authentifizierung über einen Domain Controller angemeldet hat, oder ein Konto sich abgemeldet hat, dieses Konto sich jedoch trotzdem Ressourcen gegenüber per *Service Ticket* authentifiziert, kann dies dafür sprechen, dass ein Angreifer Tickets gestohlen hat oder in der Lage ist gefälschte Tickets für Kerberos-Dienste, so genannte *Silver Tickets*, zu erstellen.
- Entspricht die Autorisierung eines Kontos nicht den Berechtigungen, die dieses Konto auf einem System oder im Active Directory hat, ist dies ein Hinweis auf die Verwendung von gefälschten Tickets und somit auf die Kompromittierung eines Dienstes oder gar des gesamten Active Directorys. Solche Inkonsistenzen können sich zum Beispiel dadurch zeigen, dass das Ereignis 4672 für ein Konto, das nicht über vertraulichen Berechtigungen verfügt, protokolliert wird.
- Hinweise auf potenzielle Pass-the-Hash-Angriffe, bei denen gestohlene Passwort-Hashes von Konten zur Authentifizierung über das NTLM-Protokoll verwendet werden, kann in Umgebungen, in denen vorrangig Kerberos-Authentifizierung eingesetzt wird, das Ereignis 4624 geben. Ist hier der Anmeldetyp 9 protokolliert, bedeutet dies, dass ein Benutzer neue und zu seinem Konto abweichende Anmeldeinformationen für ausgehende Verbindungen angegeben hat. Aber auch schon die generelle Verwendung von NTLM, anstatt Kerberos, zur Authentifizierung könnte ein Hinweis auf Pass-the-Hash sein (Ereignis 4776).

Um die genannten Szenarien abzudecken, sollten die empfohlenen Einstellungen, die die Protokollierung von Anmelde- und Abmeldeereignissen (inkl. Gruppenmitgliedschaft und zugewiesenen Privilegien), Kontensperrungsereignisse und Kontenverwaltungsereignisse aktivieren, umgesetzt werden.

5.1.1 Windows-Protokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der System- und Sicherheits-Protokolle, die über Gruppenrichtlinien konfigurierbar sind.

5.1.1.1 Stellen Sie sicher, dass „Überprüfen der Anmeldeinformationen überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.1.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Kontoanmeldung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4776: Der Computer hat versucht, die Anmeldeinformationen für ein Konto zu überprüfen.	Dieses Ereignis wird generiert, wenn NTLM-Authentifizierungsinformationen überprüft werden und unterstützt somit bei der Nachvollziehung von NTLM-Anmeldeversuchen.

5.1.1.2 Stellen Sie sicher, dass „Benutzerkontenverwaltung überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.2.3 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Kontenverwaltung

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4720: Ein Benutzerkonto wurde erstellt.	Dieses Ereignis wird generiert, wenn ein neues Benutzerkonto-Objekt erstellt wurde.
4722: Ein Benutzerkonto wurde aktiviert.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto-Objekt aktiviert wird.
4723: Es wurde versucht, das Kennwort eines Kontos zu ändern.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto versucht ein Kennwort zu ändern.
4724: Es wurde versucht, das Kennwort eines Kontos zurückzusetzen.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto versucht ein Kennwort zurückzusetzen.

Ereignis-ID: Name	Begründung
4725: Ein Benutzerkonto wurde deaktiviert.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto-Objekt deaktiviert wird.
4726: Ein Benutzerkonto wurde gelöscht.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto-Objekt gelöscht wird.
4738: Ein Benutzerkonto wurde geändert.	Dieses Ereignis wird generiert, wenn Attribute eines Benutzerkonto-Objekts geändert werden.
4740: Ein Benutzerkonto wurde gesperrt.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto gesperrt wird.
4767: Ein Benutzerkonto wurde entsperrt.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto entsperrt wird.
4781: Der Name eines Kontos wurde geändert.	Dieses Ereignis wird generiert, wenn das Benutzerkontoattribut *sAMAccountName* geändert wird.
4798: Die lokale Gruppenmitgliedschaft eines Benutzers wurde aufgelistet.	Dieses Ereignis wird generiert, wenn ein Prozess die sicherheitsfähigen lokalen Gruppen eines Kontos auflistet.
5376: Credential Manager-Anmeldeinformationen wurden gesichert.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto die Datenbank des *Credential Managers* erfolgreich sichert.
5377: Credential Manager-Anmeldeinformationen wurden aus einer Sicherung wiederhergestellt.	Dieses Ereignis wird generiert, wenn ein Benutzerkonto die Datenbank des *Credential Managers* erfolgreich wiederherstellt.

5.1.1.3 Stellen Sie sicher, dass „Kontosperrung überwachen“ den Wert „Fehler“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Erfolg-Ereignisse (siehe (ms_al, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4625: Ein Konto konnte nicht angemeldet werden.	Dieses Ereignis wird generiert, wenn ein Konto nach einem Anmeldeversuch gesperrt oder wenn ein Anmeldeversuch für ein gesperrtes Konto durchgeführt wurde.

5.1.1.4 Stellen Sie sicher, dass „Mitgliedschaft in der Überwachungsgruppe“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4627: Gruppenmitgliedschaftsinformationen.	Dieses Ereignis wird in Verbindung mit dem Ereignis 4624 (Ein Konto wurde erfolgreich angemeldet) generiert und zeigt die Liste der Gruppen an, zu denen das angemeldete Konto gehört.

5.1.1.5 Stellen Sie sicher, dass „Abmelden überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.3 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4634: Ein Konto wurde abgemeldet.	Dieses Ereignis wird normalerweise für alle Anmeldetypen außer *Interactive* und *RemoteInteractive* generiert, wenn eine Kontoabmeldung erfolgt. Korreliert mit z. B. dem Ereignis 4624 (Ein Konto wurde erfolgreich angemeldet).
4647: Benutzer initiierte Abmeldung.	Dieses Ereignis ist typisch für *Interactive* und *RemoteInteractive* Anmeldetypen und wird generiert, wenn eine Kontoabmeldung initiiert wird. Korreliert mit z. B. dem Ereignis 4624 (Ein Konto wurde erfolgreich angemeldet).

5.1.1.6 Stellen Sie sicher, dass „Anmelden überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.4 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Erfolg und Fehler

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4624: Ein Konto wurde erfolgreich angemeldet.	Dieses Ereignis wird generiert, wenn ein Anmeldeversuch eines Kontos erfolgreich war und eine Anmeldesitzung erstellt wurde.
4625: Ein Konto konnte nicht angemeldet werden.	Dieses Ereignis wird generiert, wenn ein Anmeldeversuch eines Kontos fehlgeschlagen ist.
4648: Es wurde versucht, eine Anmeldung mit expliziten Anmeldeinformationen zu verwenden.	Dieses Ereignis wird generiert, wenn ein Konto einen Anmeldeversuch für ein anderes Konto durchführt, wie z. B. bei Verwendung der Anwendung `runas.exe`.

5.1.1.7 Stellen Sie sicher, dass „Andere Anmelde-/Abmeldeereignisse überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.5 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4778: Eine Benutzersitzung wurde wieder mit einer *Window Station* verbunden.	Dieses Ereignis wird generiert, wenn ein Benutzer die Verbindung zu einer vorhandenen *Window Station* aufruft.

Ereignis-ID: Name	Begründung
4779: Eine Benutzersitzung wurde von einer *Window Station* getrennt.	Dieses Ereignis wird generiert, wenn ein Benutzer die Verbindung zu einer vorhandenen *Window Station* trennt.
5378: Die angeforderte Delegierung von Anmeldeinformationen wurde nach Richtlinie nicht zugelassen.	Dieses Ereignis wird generiert, wenn die Delegierung von Zugangsinformationen über das CredSSP-Protokoll versucht aber durch Richtlinien unterbunden wurde.

5.1.1.8 Stellen Sie sicher, dass „Spezielle Anmeldung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.5.6 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_sl, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Anmelden/Abmelden

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4964: Einer neuen Anmeldung wurden spezielle Gruppen zugewiesen.	Dieses Ereignis wird generiert, wenn ein Mitglied einer definierten speziellen Gruppe sich anmeldet.
4672: Besondere Privilegien, die der neuen Anmeldung zugewiesen sind.	Dieses Ereignis wird generiert, wenn einer Kontenanmeldung eine sensitive Berechtigung zugeordnet wird.

5.1.2 Anwendungs- und Dienstprotokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der Anwendungs- und Dienstprotokolle, die nicht über Gruppenrichtlinien konfigurierbar sind, aber über Gruppenrichtlinienobjekte verteilt werden können.

5.1.2.1 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-LSA/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Local Security Authority (LSA) des Windows-Betriebssystems. Der LSA-Prozess führt sämtliche Aktivitäten der Authentifizierung und Autorisierung durch und ist somit eine wichtige Quelle bei der Überwachung von Anmeldeaktivität.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-LSA/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Deaktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
300	Dieses Ereignis wird generiert, wenn der Anmeldeversuch eines Kontos erfolgreich war und eine Anmeldesitzung erstellt wurde. Das Ereignis zeigt die Liste der Gruppen an, zu denen das angemeldete Konto gehört.

5.1.2.2 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Komponente Microsoft-Windows-TerminalServices-RemoteConnectionManager des Windows-Betriebssystems. Die hier erhobenen Protokollierungsdaten enthalten somit Informationen zu eingehenden Netzwerkverbindungen von RDP-Clients.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
1149	Dieses Ereignis wird generiert, wenn vor der eigentlichen Benutzersitzung eine erfolgreiche Netzwerkauthentifizierung durchgeführt wurde.
258	Dieses Ereignis wird generiert, wenn der *TermService*-Dienst beginnt einen ihm zugeordneten Port zu öffnet.
259	Dieses Ereignis wird generiert, wenn der *TermService*-Dienst beginnt einen ihm zugeordneten Port zu schließen.

5.1.2.3 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-TerminalServices-LocalSessionManager/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Komponente Microsoft-Windows-TerminalServices-LocalSessionManager des Windows-Betriebssystems, welche für den Start des Computers und die Implementierung von Windows Fast User Switching (FUS) verantwortlich ist. Die Konfiguration dieser Komponente, sowie der Windows Firewall bestimmen, ob eingehende RDP Verbindungen erlaubt sind. Ist dies der Fall enthält dieses Ereignisprotokoll Informationen zu RDP Sitzungen.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-TerminalServices-LocalSessionManager/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
40	Dieses Ereignis wird generiert, wenn eine RDP-Sitzung unterbrochen wurde.
41	Dieses Ereignis wird generiert, wenn der *TermService*-Dienst beginnt eine Sitzung zuzuweisen.
42	Dieses Ereignis wird generiert, wenn der *TermService*-Dienst die Zuweisung eine Sitzung abgeschlossen hat.
22	Dieses Ereignis wird generiert, wenn nach der erfolgreichen RDP-Anmeldung eine Shell initialisiert wurde.
21	Dieses Ereignis wird generiert, wenn eine erfolgreiche RDP-Anmeldung und Sitzungsinstanziierung durchgeführt wurde.
24	Dieses Ereignis wird generiert, wenn eine RDP Sitzung unterbrochen wurde.
25	Dieses Ereignis wird generiert, wenn ein Benutzer eine Verbindung zu einer vorhandenen RDP-Sitzung hergestellt.
23	Dieses Ereignis wird generiert, wenn ein angemeldeter Benutzer eine Systemabmeldung in einer RDP Sitzung einleitet.
17	Dieses Ereignis wird generiert, wenn der Start des *TermService*-Diensts fehlgeschlagen ist.
39	Dieses Ereignis wird generiert, wenn eine Sitzung durch eine andere Sitzung beendet wurde.

5.2 Aktivität von Kernsystemkomponenten

Ereignisse, die von sicherheitsrelevanten Systemkomponenten ausgelöst werden und somit die Aktivitäten dieser Komponenten und ihre korrekte oder fehlerhafte Funktion abbilden, sollten protokolliert werden. Hierzu gehören Ereignisse, die von folgenden Kernkomponenten eines Windowssystems ausgelöst werden:

- Local Security Authority (LSA)
- Security Account Manager (SAM)
- Windows Aufgabenplanung
- Windows Firewall Dienst
- Windows Management Instrumentation (WMI)
- Windows Remote Management (WinRM)
- Code-Integritätsfunktionalität
- Cryptography API: Next Generation

Auch Ereignisse im Zusammenhang mit grundlegenden Funktionen des Betriebssystems, wie der Dateifreigabe, dem Objektzugriff oder der Anwendung von Windows Gruppenrichtlinien werden diesem Kapitel behandelt. Des Weiteren wurde die Protokollierung der Installation neuer Dienste oder Geräte und Treiber in diese Kategorie aufgenommen. Die Konfiguration der Protokollierung von Ereignissen zu Prozessaktivitäten und Registrierungsaktivitäten wurden in jeweils eigene Kapitel ausgelagert (siehe Abschnitte 5.5 und 5.6).

Ereignisse die von den obengenannten Komponenten, welche für die Sicherheit des Betriebssystems zentral sind, ausgelöst werden, können vielfältige Hinweise auf (versuchte) Angriffe auf das System, sowie Informationen über den Sicherheitszustand eines Systems liefern.

Werden Fehler in der Ausführung von diesen für die Sicherheit eines Systems essenziellen Komponenten gemeldet, kann dies bedeuten, dass die gesamte Sicherheit des Systems heruntergesetzt wurde Diese Fehler können durch einen Angreifer induziert sein oder auch durch Fehlfunktionen entstehen, können jedoch in beiden Fällen sicherheitskritisch sein. Beispiele hierfür sind:

- Das Anhalten der Windows Defender Firewall, protokolliert im Ereignis 5025, kann durch einen Angreifer veranlasst werden, um unerwünschte Netzwerkverbindungen aufzubauen. Ereignis 5030, das generiert wird, wenn der Windows Defender Firewall-Dienst nicht gestartet oder unerwartet beendet wird, kann sowohl auf eine Fehlfunktion als auch auf eine Aktion eines Angreifers hindeuten.
- Der Verlust von Protokollierungsdaten durch ein Überlaufen der Warteschlange der Protokollierung, protokolliert in Ereignis 4612, kann durch einen Angreifer provoziert werden, um seine Aktivitäten zu verschleiern.

Ereignisse in dieser Kategorie können zudem Hinweise auf (versuchte) initiale Angriffe liefern:

- Ereignis 5148 protokolliert, wenn die Windows Filter Plattform einen vermuteten Denial of Service-Angriff detektiert.
- Der Anschluss von externen Geräten, kann dazu genutzt werden Schadsoftware auf ein Gerät aufzubringen. Im Ereignis 400 wird protokolliert, wenn ein Plug-and-Play-fähiges Gerät erfolgreich initialisiert wurde.
- Wenn die Code-Integritätsfunktionalität meldet, dass Software nicht den Integritätsanforderungen entspricht (wie zum Beispiel das Laden eines nicht-signierten Kernel Moduls (Ereignis 3001)) kann dies ein Hinweis auf das (versuchte) Ausführen von Schadsoftware sein.

Auch Hinweise auf den Angriffsverlauf nach einer erfolgreichen ersten Kompromittierung können durch die Protokollierung von durch Kernsystemkomponenten generierten Ereignissen gewonnen werden:

- Unerwartete Prozesse, die Debug-Rechte auf Kernsystemkomponenten, wie der Local Security Authority, haben, können ein Hinweis auf die Ausführung von Schadsoftware (wie z. B. *mimikatz*) mit erhöhten Privilegien sein. Im Beispiel von *mimikatz* wird über Debugging des LSA-Subsystemdienst-Prozess (LSASS) relevantes Schlüsselmaterial extrahiert, um dann auf verschlüsselte Speicherbereiche des Prozesses zuzugreifen, in dem Zugangsdaten und Berechtigungsnachweise gespeichert sind.
- Ein neuer, unerwartet installierter Dienst (protokolliert im Ereignis 4697), der bei jedem Systemstart ausgeführt wird, könnte für einen Angreifer ein möglicher Weg sein, nach einer erfolgreichen Kompromittierung, Persistenz auf einem System zu erreichen. Da Dienste mit Administratorrechten erstellt werden können, aber unter Umständen mit SYSTEM-Rechten ausgeführt werden, kann dies auch ein Weg für einen Angreifer sein, seine Privilegien zu erhöhen.

Um die Protokollierung für die obengenannten Systemkomponenten zu aktivieren und eine Überwachung der Bespielszenarien zu ermöglichen, sollten die nachfolgenden Einstellungsempfehlungen umgesetzt werden.

5.2.1 Windows-Protokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der System- und Sicherheits-Protokolle, die über Gruppenrichtlinien konfigurierbar sind.

5.2.1.1 Stellen Sie sicher, dass „Andere Systemereignisse überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.9.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\System

Standardwert
Erfolg und Fehler

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
5024: Der Windows Firewall-Dienst wurde erfolgreich gestartet.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) erfolgreich gestartet wurde.
5025: Der Windows Firewall-Dienst wurde angehalten.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) gestoppt wurde.
5027: Der Windows Firewall-Dienst konnte die Sicherheitsrichtlinie nicht aus dem lokalen Speicher abrufen. Der Dienst wendet weiterhin die aktuelle Richtlinie an.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) eine neue Sicherheitsrichtlinie nicht abrufen und deshalb auch nicht initialisieren kann.
5028: Der Windows Firewall-Dienst konnte die neue Sicherheitsrichtlinie nicht	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) eine neue Sicherheitsrichtlinie

Ereignis-ID: Name	Begründung
verarbeiten. Der Dienst wendet weiterhin die aktuelle Richtlinie an.	nicht interpretieren und deshalb auch nicht initialisieren kann.
5029: Fehler beim Initialisieren des Treibers durch den Windows Firewall-Dienst. Der Dienst wendet weiterhin die aktuelle Richtlinie an.	Dieses Ereignis wird generiert, wenn entweder der Windows Firewall-Dienst (*MpsSvc*) oder sein Treiber nicht gestartet werden kann oder wenn sie unerwartet beendet werden.
5030: Der Windows Firewall-Dienst konnte nicht gestartet werden.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) nicht gestartet werden kann oder wenn er unerwartet beendet wird.
5033: Der Windows-Firewall-Treiber wurde erfolgreich gestartet.	Dieses Ereignis wird generiert, wenn der Windows-Firewall-Treiber erfolgreich gestartet wurde.
5034: Der Windows-Firewall-Treiber wurde angehalten.	Dieses Ereignis wird generiert, wenn der Windows-Firewall-Treiber gestoppt wird.
5035: Der Windows-Firewall-Treiber konnte nicht gestartet werden.	Dieses Ereignis wird generiert, wenn der Windows-Firewall-Treiber nicht gestartet werden konnte.
5037: Der Windows-Firewall-Treiber hat einen kritischen Laufzeit Fehler erkannt. Der Treiber wird beendet.	Dieses Ereignis wird generiert, wenn der Windows-Firewall-Treiber nicht gestartet werden kann oder wenn er unerwartet beendet wird.

5.2.1.2 Stellen Sie sicher, dass „Sicherheitsstatusänderung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.9.3 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_ssc, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\System

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4608: Windows startet.	Dieses Ereignis wird generiert, wenn der *LSASS.EXE*-Prozess gestartet und das Überwachungssubsystem initialisiert wird.
4616: Die Systemzeit wurde geändert.	Dieses Ereignis wird generiert, wenn die Systemzeit geändert wurde.

5.2.1.3 Stellen Sie sicher, dass „Sicherheitssystemerweiterung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.9.4 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_sse, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\System

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4610: Ein Authentifizierungspaket wurde von der *Local Security Authority* geladen.	Dieses Ereignis wird generiert, wenn ein Authentifizierungspaket vom *LSASS.EXE*-Prozess geladen wurde.
4611: Ein Anmeldeprozess wurde bei der *Local Security Authority* registriert.	Dieses Ereignis wird generiert, wenn der *LSASS.EXE*-Prozess einen validen Anmeldeprozess bestätigt und Anmeldungen von diesem Anmeldeprozess bearbeitet werden können.
4614: Ein *Notification Package* wurde vom *Security Account Manager* geladen.	Dieses Ereignis wird generiert, wenn eine *Notification Package* DLL vom *Security Account Manager* geladen und die Initialisierungssequenz für diese DLL ausgeführt wurde.
4622: Ein Sicherheitspaket wurde von der *Local Security Authority* geladen.	Dieses Ereignis wird generiert, wenn eine *Security Package* DLL von der *Local Security Authority* geladen und die Initialisierungssequenz für diese DLL ausgeführt wurde.
4697: Ein Dienst wurde im System installiert.	Dieses Ereignis wird generiert, wenn ein neuer Dienst auf dem System installiert wurde.

5.2.1.4 Stellen Sie sicher, dass „Systemintegrität überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.9.5 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\System

Standardwert
Erfolg und Fehler

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4612: Die internen Ressourcen, die für die Warteschlange von Überwachungs-Nachrichten reserviert wurden, wurden ausgeschöpft, was zum Verlust einiger Audits führte.	Dieses Ereignis wird generiert, wenn die Warteschlange der Protokollierung überläuft und Ereignisse verworfen werden müssen. Dies tritt am häufigsten auf, wenn Ereignisse schneller generiert als auf die Festplatte geschrieben werden können.
4816: RPC hat eine Integritätsverletzung erkannt, während eine eingehende Nachricht entschlüsselt wurde.	Dieses Ereignis wird generiert, wenn Remote Procedure Call (RPC) beim Entschlüsseln einer eingehenden Nachricht eine Integritätsverletzung festgestellt hat.
5038: Die Code Integrität hat festgestellt, dass der Imagehash einer Datei nicht gültig ist.	Dieses Ereignis wird generiert, wenn die Code-Integritätsfunktionalität (ms_code_integrity, 2020) feststellt, dass die Signatur einer Datei nicht gültig ist.
5061: Kryptografischer Vorgang	Dieses Ereignis wird generiert, wenn eine kryptografische Operation unter Verwendung eines *Key Storage Providers* (KSP) ausgeführt wurde.
6281: Die Code Integrität hat festgestellt, dass die Pagehashes einer Imagedatei ungültig sind.	Dieses Ereignis wird generiert, wenn die Code-Integritätsfunktionalität (ms_code_integrity, 2020) feststellt, dass der Page-Hash eines Images ungültig ist.
6410: Die Code Integrität hat festgestellt, dass eine Datei nicht die Sicherheitsanforderungen erfüllt, um in einen Prozess geladen zu werden.	Dieses Ereignis wird generiert, wenn schreibbare freigegebene Abschnitte (*Shared Sections*) in einem Dateiabbild (*File Image*) vorhanden sind.

5.2.1.5 Stellen Sie sicher, dass „Dateifreigabe überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.6.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Objektzugriff

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
5140: Zugriff auf ein Netzwerkfreigabe-Objekt.	Dieses Ereignis wird beim erste Zugriffsversuch generiert, wenn auf ein Netzwerkfreigabe Objekt zugegriffen wird.
5142: Ein Netzwerkfreigabe-Objekt wurde hinzugefügt.	Dieses Ereignis wird generiert, wenn ein Netzwerkfreigabe Objekt hinzugefügt wird.

Ereignis-ID: Name	Begründung
5143: Ein Netzwerkfreigabe-Objekt wurde geändert.	Dieses Ereignis wird generiert, wenn ein Netzwerkfreigabe Objekt geändert wird.
5144: Ein Netzwerkfreigabe-Objekt wurde gelöscht.	Dieses Ereignis wird generiert, wenn ein Netzwerkfreigabe-Objekt gelöscht wird.
5168: SPN-Prüfung für SMB-SMB2 fehlgeschlagen.	Dieses Ereignis wird generiert, wenn die SMB-SPN-Prüfung fehlschlägt. Der SPN wird nur an den Server gesendet, wenn NTLMv2- oder Kerberos-Protokolle verwendet werden.

5.2.1.6 Stellen Sie sicher, dass „Detaillierte Dateifreigabe überwachen“ den Wert „Fehler“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.6.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Objektzugriff

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
5145: Ein Netzwerkfreigabe Objekt wurde überprüft, um festzustellen, ob dem Client der gewünschte Zugriff gewährt werden kann.	Dieses Ereignis wird generiert, wenn auf ein Netzwerkfreigabeobjekt (Datei oder Ordner) zugegriffen wird.

5.2.1.7 Stellen Sie sicher, dass „Andere Objektzugriffsereignisse überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.6.3 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Objektzugriff

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4671: Eine Anwendung hat versucht, über die TBS auf einen blockierten Index zuzugreifen.	Dieses Ereignis wird generiert, wenn ein Prozess versucht über TPM Base Service (TBS) -Funktionalität auf einen blockierten TPM Index zuzugreifen.
5148: Die Windows-Filterplattform hat einen DoS-Angriff erkannt und in einen defensiven Modus versetzt; Pakete, die diesem Angriff zugeordnet sind, werden verworfen.	Dieses Ereignis wird generiert, wenn ein ICMP-DoS-Angriff startet oder erkannt wird.
5149: Der DoS-Angriff hat nach und nach die normale Verarbeitung fortgesetzt.	Dieses Ereignis wird generiert, wenn ein ICMP-DoS-Angriff abklingt oder beendet wurde.
4698: Ein geplanter Vorgang wurde erstellt.	Dieses Ereignis wird generiert, wenn ein neuer *Scheduled Task* erstellt wird.
4699: Ein geplanter Vorgang wurde gelöscht.	Dieses Ereignis wird generiert, wenn ein *Scheduled Task* gelöscht wird.
4700: Ein geplanter Vorgang wurde aktiviert.	Dieses Ereignis wird generiert, wenn ein *Scheduled Task* aktiviert wird.
4701: Ein geplanter Vorgang wurde deaktiviert.	Dieses Ereignis wird generiert, wenn ein *Scheduled Task* deaktiviert wird.
4702: Ein geplanter Vorgang wurde aktualisiert.	Dieses Ereignis wird generiert, wenn ein *Scheduled Task* aktualisiert wird.
5888: Ein Objekt im COM+-Katalog wurde geändert.	Dieses Ereignis wird generiert, wenn ein Objekt im COM+-Katalog geändert wird.
5889: Ein Objekt wurde aus dem COM+-Katalog gelöscht.	Dieses Ereignis wird generiert, wenn ein Objekt im COM+-Katalog gelöscht wird.
5890: Dem COM+-Katalog wurde ein Objekt hinzugefügt.	Dieses Ereignis wird generiert, wenn ein Objekt im COM+-Katalog hinzugefügt wird.

5.2.1.8 Stellen Sie sicher, dass „Wechselmedien überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.6.4 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Objektzugriff

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4656: Ein Handle für ein Objekt wurde angefordert.	Dieses Ereignis wird generiert, wenn ein Handle für ein Objekt angefordert wurde.
4658: Das Handle für ein Objekt wurde geschlossen.	Dieses Ereignis wird generiert, wenn ein Handle für ein Objekt geschlossen wurde.

Ereignis-ID: Name	Begründung
4663: Es wurde versucht, auf ein Objekt zuzugreifen.	Dieses Ereignis wird generiert, wenn versucht wird auf ein Objekt zuzugreifen.

5.2.1.9 Stellen Sie sicher, dass „PNP-Überwachungsaktivität“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.3.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Detaillierte Überwachung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
6416: Ein neues externes Gerät wurde vom System erkannt.	Dieses Ereignis wird generiert, wenn ein neues externes Gerät vom System erkannt wird, z. B. wenn ein neues externes Gerät angeschlossen oder aktiviert wird.
6419: Es wurde eine Anfrage zum Deaktivieren eines Geräts gestellt.	Dieses Ereignis wird generiert, wenn eine Anfrage zum Deaktivieren eines Geräts gestellt wurde.
6420: Ein Gerät wurde deaktiviert.	Dieses Ereignis wird generiert, wenn eine Anfrage zum Deaktivieren eines Geräts erfolgreich war und das Gerät deaktiviert wurde.
6421: Es wurde eine Anforderung zum Aktivieren eines Geräts gestellt.	Dieses Ereignis wird generiert, wenn eine Anfrage zum Aktivieren eines Geräts gestellt wurde.
6422: Ein Gerät wurde aktiviert.	Dieses Ereignis wird generiert, wenn eine Anfrage zum Aktivieren eines Geräts erfolgreich war und das Gerät aktiviert wurde.
6423: Die Installation dieses Geräts ist nach Systemrichtlinien untersagt.	Dieses Ereignis wird generiert, wenn die Installation eines Geräts gemäß den Geräteinstallationsrichtlinien untersagt wurde.
6424: Die Installation dieses Geräts war zulässig, nachdem es zuvor durch eine Richtlinie verboten wurde.	Dieses Ereignis wird generiert, wenn Administratoren gestattet wird, die Geräteinstallationsrichtlinien zu umgehen.

5.2.2 Anwendungs- und Dienstprotokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der Anwendungs- und Dienstprotokolle, die nicht über Gruppenrichtlinien konfigurierbar sind, aber über Gruppenrichtlinienobjekte verteilt werden können.

5.2.2.1 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-CAPI2/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse in Zusammenhang mit der „Cryptography API: Next Generation“. Dies stellt die Kryptografie Plattform des Windows-Betriebssystems dar und übernimmt Aufgaben wie die Berechnung kryptografischer Operationen. Diesem Ereignisprotokoll können beispielsweise Fehler bei der Verwendung von Zertifikaten entnommen werden.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-CAPI2/Operational /enabled:true /retention:false /maxsize:201326592` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

Standardwert
Deaktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
10	Dieses Ereignis wird generiert, wenn ein Prozess die Erstellung eines *CERT_CONTEXT* Objekt (z. B. mit Hilfe von *CertGetCertificateChain*) gestartet hat.
11	Dieses Ereignis wird generiert, wenn die Erstellung eines *CERT_CONTEXT* Objekt (z. B. mit Hilfe von *CertGetCertificateChain*) erfolgreich abgeschlossen wurde.
30	Dieses Ereignis wird generiert, wenn die Gültigkeit ein *CERT_CONTEXT* Objekt (z. B. mit Hilfe von *CertVerifyCertificateChainPolicy*) von einem Prozess überprüft wurde.
40	Dieses Ereignis wird generiert, wenn ein Prozess einen Sperrstatus Überprüfung eines *CERT_CONTEXT* Objekts (z. B. mit Hilfe von *CertVerifyRevocation*) gestartet hat.
41	Dieses Ereignis wird generiert, wenn der Sperrstatus eines *CERT_CONTEXT* Objekt (z. B. mit Hilfe von *CertVerifyRevocation*) von einem Prozess überprüft wurde.
42	Dieses Ereignis wird generiert, wenn die Informationen zur Sperrstatus Überprüfung abgelehnt wurden (z. B. von *CertVerifyRevocation*).
50	Dieses Ereignis wird generiert, wenn ein Prozess den Abruf eines Public Key Infrastructure (PKI) Objekts (siehe (ms_crypt_retrv_obj, 2020)) von einem durch eine URL angegebenen Speicherort gestartet hat.

Ereignis-ID	Begründung
51	Dieses Ereignis wird generiert, wenn ein Prozess den Abruf eines Public Key Infrastructure (PKI) Objekts (siehe (ms_crypt_retrv_obj, 2020)) von einem durch eine Uniform Ressource Locator (URL) angegebenen Speicherort abgeschlossen hat.
90	Dieses Ereignis wird generiert, wenn ein *CERT_CONTEXT* Objekt (z. B. mit Hilfe von *CertGetCertificateChain*) erstellt wird.

5.2.2.2 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-CodeIntegrity/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse in Zusammenhang mit kernelseitiger Treiber-Signaturprüfung. Dem Operational-Ereignisprotokoll können Fehler bei der Signaturprüfung entnommen werden.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-CodeIntegrity/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
3001	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente feststellt, dass ein nicht signiertes Kernelmodul in das System geladen wird.
3002	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente die Integrität einer Datei nicht überprüfen kann.
3003	Dieses Ereignis wird generiert, wenn das System sich im Debug-Modus befindet und die *Code Integrity*-Komponente die Integrität einer Datei nicht überprüfen kann.
3004	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente die Integrität einer Datei nicht überprüfen kann, da der Datei-Hash auf dem System nicht gefunden wird.
3005	Dieses Ereignis wird generiert, wenn das System sich im Debug-Modus befindet und die *Code Integrity*-Komponente die Integrität einer Datei nicht überprüfen kann, da der Datei-Hash auf dem System nicht gefunden wird.

Ereignis-ID	Begründung
3010	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente eine Katalog-Datei nicht laden konnte.
3033	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente feststellt, dass ein Prozess versucht eine Datei zu laden, welche die erforderlichen Signaturanforderungen nicht erfüllt.
3076	Dieses Ereignis wird generiert, wenn eine Datei aufgrund einer Richtlinienanforderung geladen wird, obwohl die *Code Integrity*-Komponente festgestellt hat, dass die erforderlichen Signaturanforderungen nicht erfüllt werden.
3077	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente feststellt, dass ein Prozess versucht eine Datei zu laden, welche die erforderlichen Richtlinienanforderung nicht erfüllt.
3089	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente die Signaturinformationen einer Datei interpretiert.
3099	Dieses Ereignis wird generiert, wenn die *Code Integrity*-Komponente eine Integritätsrichtlinie aktiviert oder aktualisiert.

5.2.2.3 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-GroupPolicy/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse in Zusammenhang mit der Nutzung von Windows Gruppenrichtlinien. Kommt es beispielsweise zu Fehlern in der Anwendung von Gruppenrichtlinien, können die Ereignisse dieses Ereignisprotokolls hilfreich sein.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-GroupPolicy/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert

Aktiviert (max. Protokollgröße: 4.096 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
9001	Dieses Ereignis wird generiert, wenn Gruppenrichtliniendateien ohne die Attribute *RequireMutualAuthentication* und *RequireIntegrity* von einer Dateifreigabe abgerufen werden.

Ereignis-ID	Begründung
4126	Dieses Ereignis wird generiert, wenn das System beginnt anwendbare Gruppenrichtlinien vom Domänencontroller anzufordern.
5126	Dieses Ereignis wird generiert, wenn das System anwendbare Gruppenrichtlinien vom Domänencontroller erfolgreich angefordert hat.
7126	Dieses Ereignis wird generiert, wenn keine anwendbaren Gruppenrichtlinien vom Domänencontroller angefordert werden konnten.
4117	Dieses Ereignis wird generiert, wenn eine Gruppenrichtliniensitzung erfolgreich initiiert wurde.
5117	Dieses Ereignis wird generiert, wenn eine Gruppenrichtliniensitzung erfolgreich abgeschlossen wurde.
7117	Dieses Ereignis wird generiert, wenn eine Gruppenrichtliniensitzung nicht erfolgreich abgeschlossen wurde.
4257	Dieses Ereignis wird generiert, wenn das System beginnt Gruppenrichtlinieneinstellungen herunterzuladen.
5257	Dieses Ereignis wird generiert, wenn das Herunterladen von Gruppenrichtlinieneinstellungen erfolgreich abgeschlossen wurde.
7257	Dieses Ereignis wird generiert, wenn das Herunterladen von Gruppenrichtlinieneinstellungen nicht erfolgreich abgeschlossen wurde.
4217	Dieses Ereignis wird generiert, wenn das System beginnt Gruppenrichtlinieneinstellungen aus dem lokalen Datenspeicher einzulesen.
5217	Dieses Ereignis wird generiert, wenn das Einlesen von Gruppenrichtlinieneinstellungen aus dem lokalen Datenspeicher erfolgreich abgeschlossen wurde.
7217	Dieses Ereignis wird generiert, wenn Gruppenrichtlinieneinstellungen aus dem lokalen Datenspeicher nicht erfolgreich eingelesen werden konnten.
4016	Dieses Ereignis wird generiert, wenn eine *Client Side Extension* (CSE) beginnt ein Gruppenrichtlinienobjekt zu verarbeiten.
5016	Dieses Ereignis wird generiert, wenn eine *Client Side Extension* (CSE) die Verarbeitung eines Gruppenrichtlinienobjekt erfolgreich abgeschlossen hat.
4115	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst erfolgreich gestartet wird.
5115	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst gestoppt wird.
4017	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst Systemaufrufe aufruft, die z. B. Kontoinformationen oder Dateieninformationen abrufen.
5017	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst die Systemaufrufe erfolgreich

Ereignis-ID	Begründung
	abgeschlossen hat, die z. B. Kontoinformationen oder Dateieninformationen abrufen.
5313	Dieses Ereignis wird generiert, wenn Gruppenrichtlinienobjekte herausgefiltert und somit nicht angewendet wurden.
5312	Dieses Ereignis wird generiert, wenn die Liste der anwendbaren Gruppenrichtlinienobjekte erfolgreich abgefragt wurde.
5308	Dieses Ereignis wird generiert, wenn eine Verbindung zum Domänencontroller aufgebaut wurde.
5310	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst erfolgreich Informationen zu einem *Security Principal* (ms_sec_principal, 2020), hinterlegt im Verzeichnisdienst, abgerufen hat.
4019	Dieses Ereignis wird generiert, wenn ein Skript vom Gruppenrichtliniendienst gestartet wird.
5019	Dieses Ereignis wird generiert, wenn der Gruppenrichtliniendienst die Ausführung eines Skripts erfolgreich abgeschlossen hat.

5.2.2.4 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-Kernel-PnP/Configuration" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zu vom Betriebssystem-Kern geladenen Plug-and-Play-Gerätetreibern. Diesem Ereignisprotokoll können Informationen zu angeschlossener Peripherie, wie beispielsweise Universal Serial Bus (USB)-Datenträgern oder -Tastaturen entnommen werden.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-Kernel-PnP/Configuration /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
400	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät erkannt und erfolgreich initialisiert wurde.
401	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät erkannt, aber nicht erfolgreich initialisiert werden konnte.
420	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät erfolgreich entfernt wird.

Ereignis-ID	Begründung
421	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät nicht erfolgreich entfernt werden konnte.
410	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät nach der der Initialisierung erfolgreich gestartet wird.
411	Dieses Ereignis wird generiert, wenn ein PNP-fähiges Gerät nach der der Initialisierung nicht erfolgreich gestartet werden kann.
430	Dieses Ereignis wird generiert, wenn nach der erfolgreichen Initialisierung eines PNP-fähigen Geräts weitere Initialisierungsschritte notwendig sind.

5.2.2.5 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-TaskScheduler/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Windows Aufgabenplanung. Die Windows Aufgabenplanung wird verwendet, um Anwendungen oder Skripte einmalig oder wiederkehrend zu starten. Unter Angreifern und bei Schadsoftware ist dies eine beliebte Methode, um sich Persistenz auf dem System zu verschaffen und beizubehalten.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-TaskScheduler/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Deaktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
100	Dieses Ereignis wird generiert, wenn ein neuer *Task* durch den *Schedule*-Dienst erfolgreich gestartet wird.
101	Dieses Ereignis wird generiert, wenn ein *Task* nicht erfolgreich durch den *Schedule*-Dienst gestartet werden kann.
102	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst erfolgreich abgeschlossen wird.
103	Dieses Ereignis wird generiert, wenn eine *Task Action* (ms_task_action, 2020) durch den *Schedule*-Dienst nicht gestartet werden kann.
104	Dieses Ereignis wird generiert, wenn eine *Task Action* (ms_task_action, 2020) durch den *Schedule*-Dienst nicht gestartet werden kann, da der Benutzer sich am System nicht anmelden kann.

Ereignis-ID	Begründung
106	Dieses Ereignis wird generiert, wenn ein neuer *Task* durch einen Benutzer angelegt wird.
107	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Zeitbedingung erfolgreich gestartet wird.
108	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Ereignisbedingung erfolgreich gestartet wird.
109	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Registrierungsbedingung erfolgreich gestartet wird.
110	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst für einen Benutzer, der nicht interaktiv angemeldet ist, erfolgreich gestartet wird.
111	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst beendet wird.
118	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Systemstartbedingung erfolgreich gestartet wird.
119	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Anmeldebedingung erfolgreich gestartet wird.
120	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Benutzerkonsole-Anmeldebedingung erfolgreich gestartet wird.
121	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Benutzerkonsole-Abmeldebedingung erfolgreich gestartet wird.
122	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Remote-Anmeldebedingung erfolgreich gestartet wird.
123	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Remote-Abmeldebedingung erfolgreich gestartet wird.
124	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Sperrbildschirm-Aktivierungsbedingung erfolgreich gestartet wird.
125	Dieses Ereignis wird generiert, wenn ein *Task* durch den *Schedule*-Dienst aufgrund einer Sperrbildschirm-Deaktivierungsbedingung erfolgreich gestartet wird.
129	Dieses Ereignis wird generiert, wenn ein neuer *Task* durch den *Schedule*-Dienst erfolgreich gestartet wird.
140	Dieses Ereignis wird generiert, wenn ein Benutzer die Attribute eines bestehenden *Tasks* ändert.
141	Dieses Ereignis wird generiert, wenn ein Benutzer einen bestehenden *Task* löscht.
142	Dieses Ereignis wird generiert, wenn ein Benutzer einen bestehenden *Task* deaktiviert.

5.2.2.6 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-WMI-Activity/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Aktivität der Windows Management Instrumentation (WMI). Mit Hilfe von WMI kann lokal oder über das Netzwerk auf Einstellungen des Windows-Betriebssystems zugegriffen werden und ist daher ein häufig genutzter Bestandteil für Administration und Fernverwaltung.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-WMI-Activity/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
5857	Dieses Ereignis wird generiert, wenn WMI-Provider geladen werden.
5858	Dieses Ereignis wird generiert, wenn eine WMI-Abfrage nicht erfolgreich war.
5860	Dieses Ereignis wird generiert, wenn ein WMI-Ereigniskonsument erfolgreich registriert wird.
5861	Dieses Ereignis wird generiert, wenn ein WMI-Event Filter mit einem Ereigniskonsument verbunden wird.

5.2.2.7 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-WinRM/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zum Windows Remote Management (WinRM)-Dienst des Windows-Betriebssystems. Der WinRM-Dienst kann zur Fernverwaltung von Windows-Systemen verwendet werden.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-WinRM/Operational /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
6	Dieses Ereignis wird generiert, wenn ein Fernzugriff auf ein Zielsystem initialisiert wurde.
8	Dieses Ereignis wird generiert, wenn ein Fernzugriff auf ein Zielsystem gestoppt wurde.
161	Dieses Ereignis wird generiert, wenn das System keine Verbindung zum Zielsystem herstellen kann.
162	Dieses Ereignis wird generiert, wenn die Authentifizierung des Benutzers fehlgeschlagen ist.
209	Dieses Ereignis wird generiert, wenn der *WinRM*-Dienst erfolgreich gestartet wurde.
212	Dieses Ereignis wird generiert, wenn der *WinRM*-Dienst erfolgreich gestoppt wurde.

5.3 Konfigurationsänderungen

Konfigurationsänderungen an sicherheitskritischen Richtlinienobjekten, Diensten und Gruppen können weitreichende Implikationen für die Gesamtsicherheit eines Systems haben. Konfigurationsempfehlungen und die daraus resultierenden Ereignisse in diesem Kapitel umfassen Konfigurationsänderungen an sicherheitsrelevanten Richtlinienobjekten, wie der Überwachungsrichtlinie, der MPSSVC-Richtlinien, der Authentifizierungsrichtlinie und der Autorisierungsrichtlinie, sowie Konfigurationsänderungen am Trusted Platform Module (TPM) über Richtlinienobjekte. Des Weiteren fallen Konfigurationsänderungen an Gruppen und der Windows Defender Firewall selbst, sowie Änderungen an der Access Control List (ACL)-Einträgen von Objekten und in diese Kategorie. Die Protokollierung von Konfigurationsänderungen an Konten werden jedoch nicht in diesem Kapitel beschrieben, da sie in dem Kapitel 5.1 behandelt werden. Konfigurationsänderungen am System, die über die Registrierung vorgenommen werden, werden in dem separaten Kapitel 5.6 beschrieben.

Konfigurationsänderungen können Hinweise auf eine erfolgte Kompromittierung eines Systems und Aktivitäten von Angreifern liefern. Damit Konfigurationsänderungen von einem Angreifer an einem System vorgenommen werden können, muss eine erste Kompromittierung bereits stattgefunden haben. Jedoch bieten Konfigurationsänderungen einem Angreifer viele Möglichkeiten Persistenz auf einem kompromittierten System zu erreichen.

Konfigurationsänderungen sollten nicht nur protokolliert werden, um potenzielle Angriffe erkennen und rekonstruieren zu können, sondern auch um das Sicherheitsniveau eines Systems zu überwachen. Änderungen an sicherheitskritischen Richtlinienobjekten, Diensten und Gruppen werden teilweise auch von legitimen Softwareprodukten während der Installation durchgeführt. Diese Änderungen können jedoch das Sicherheitsniveau eines Systems heruntersetzen und Härtungsmaßnahmen untergraben.

Konkrete Beispiele für Konfigurationsänderungsszenarien in den genannten Bereichen können sein:

- Das Hinzufügen von (potenziell kompromittierten) Konten in privilegierte lokale Gruppen, könnte darauf hindeuten, dass ein Angreifer versucht sich Persistenz zu verschaffen.
- Änderungen an der Überwachungsrichtlinie können ein Hinweis auf einen Angreifer sein, der versucht seinen Angriff und seine Aktionen zu verschleiern, indem er zum Bespiel die Protokollierung bestimmter Ereignisse unterbindet, was im Ereignis 4719 protokolliert wird.
- Änderungen an der Windows Defender Firewall, können ein Hinweis darauf sein, dass ein Angreifer oder Schadsoftware versuchen Kommunikationsverbindungen aufzubauen, die in der implementierten Konfiguration unterbunden wurden, um z. B. Daten abfließen zu lassen oder weitere Schadsoftware nachzuladen.

Um die Protokollierung von Konfigurationsänderungsereignissen in den genannten Bereichen (Sicherheitsgruppen, Richtlinien, Windows Defender Firewall) zu ermöglichen, sollten die folgenden Empfehlung umgesetzt werden.

5.3.1 Windows-Protokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der System- und Sicherheits-Protokolle, die über Gruppenrichtlinien konfigurierbar sind.

5.3.1.1 Stellen Sie sicher, dass „Sicherheitsgruppenverwaltung überwachen“ auf den Wert „Erfolg“ gesetzt.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.2.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_sgm, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Kontenverwaltung

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4731: Es wurde eine sicherheitsfähige lokale Gruppe erstellt.	Dieses Ereignis wird generiert, wenn eine neue sicherheitsfähige lokale Gruppe erstellt wird.
4732: Ein Mitglied wurde einer lokalen sicherheitsfähigen Gruppe hinzugefügt.	Dieses Ereignis wird generiert, wenn ein neues Konto einer sicherheitsfähigen lokalen Gruppe hinzugefügt wird.
4733: Ein Mitglied wurde aus einer lokalen sicherheitsfähigen Gruppe entfernt.	Dieses Ereignis wird generiert, wenn ein Konto aus einer sicherheitsfähigen lokalen Gruppe entfernt wird.
4734: Eine sicherheitsfähige lokale Gruppe wurde gelöscht.	Dieses Ereignis wird generiert, wenn eine sicherheitsfähige lokale Gruppe gelöscht wird.
4735: Eine sicherheitsfähige lokale Gruppe wurde geändert.	Dieses Ereignis wird generiert, wenn Attribute einer sicherheitsfähigen lokale Gruppe geändert werden.
4799: Die Mitgliedschaft einer lokalen sicherheitsfähigen Gruppe wurde aufgelistet.	Dieses Ereignis wird generiert, wenn ein Prozess die Mitglieder einer sicherheitsfähigen lokalen Gruppe versucht aufzulisten.

5.3.1.2 Stellen Sie sicher, dass „Überwachungsrichtlinienänderungen überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.7.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_apc, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Richtlinienänderung

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4715: Die Überwachungsrichtlinie (SACL) für ein Objekt wurde geändert.	Dieses Ereignis wird generiert, wenn die *System Access Control List* (SACL) der lokalen Überwachungsrichtlinie geändert wird.
4719: Die System-Überwachungsrichtlinie wurde geändert.	Dieses Ereignis wird generiert, wenn Einstellungen der Überwachungsrichtlinie des Computers geändert werden.
4817: Die Überwachungseinstellungen für das Objekt wurden geändert.	Dieses Ereignis wird generiert, wenn die Richtlinie für die globale Objektzugriffsüberwachung auf einem Computer geändert wird.
4907: Die Überwachungseinstellungen für das Objekt wurden geändert.	Dieses Ereignis wird generiert, wenn die *System Access Control List* (SACL) eines Objekts (z. B. eines Registrierungs-Schlüssels oder einer Datei) geändert wurde.
4908: Die Anmelde-Tabelle für spezielle Gruppen wurde geändert.	Dieses Ereignis wird generiert, wenn die Liste der speziellen Gruppen in der Registrierung oder über Sicherheitsrichtlinien aktualisiert wird.

5.3.1.3 Stellen Sie sicher, dass „Authentifizierungsrichtlinienänderung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.7.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_authpc, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Richtlinienänderung

Standardwert
Erfolg

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4670: Berechtigungen für ein Objekt wurden geändert.	Dieses Ereignis wird generiert, wenn die *Access Control List* (ACL) eines Objekts geändert wird.
4717: Anmelderechte wurden einem Konto gewährt.	Dieses Ereignis wird generiert, wenn die Richtlinie für die Benutzerrechte der lokalen Anmeldung geändert und einem Konto das Anmelderecht gewährt wird.
4718: Anmelderechte wurden einem Konto entzogen.	Dieses Ereignis wird generiert, wenn die Richtlinie für die Benutzerrechte der lokalen Anmeldung geändert und einem Konto das Anmelderecht entzogen wird.
4739: Die Domänenrichtlinie wurde geändert.	Dieses Ereignis wird generiert, wenn eine der folgenden Änderungen an der Sicherheitsrichtlinie des lokalen Computers vorgenommen wird: • Die Einstellungen für *Sicherheitseinstellungen \Kontorichtlinien\Kontosperrungsrichtlinien* des Computers werden geändert. • Die Einstellungen für *Sicherheitseinstellungen \Kontorichtlinien\Kennwortrichtlinie* des Computers werden geändert. • Die Gruppenrichtlinieneinstellung *Netzwerksicherheit: Abmeldung nach Ablauf der Anmeldezeit erzwingen* wird geändert. • Domänen-Attribute wie *ms-DS-MachineAccountQuota* (ms_domain_attribute_max_join, 2020) oder *msDS-Behavior-Version* (ms_attribute_dfl, 2020) werden geändert.

5.3.1.4 Stellen Sie sicher, dass „Autorisierungsrichtlinienänderung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.7.3 des CIS Benchmark. Keine Konfigurationsempfehlung in der Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Richtlinienänderung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4703: Ein Benutzerrecht wurde angepasst.	Dieses Ereignis wird generiert, wenn Token-Berechtigungen aktiviert oder deaktiviert werden.

Ereignis-ID: Name	Begründung
4704: Ein Benutzerrecht wurde zugewiesen.	Dieses Ereignis wird generiert, wenn Berechtigungen einem Token hinzugefügt werden.
4705: Ein Benutzerrecht wurde entfernt.	Dieses Ereignis wird generiert, wenn Berechtigungen einem Token entzogen werden.
4670: Die Berechtigungen für ein Objekt wurden geändert.	Dieses Ereignis wird generiert, wenn die *Access Control List* (ACL) eines Objekts (z. B. eines *Registry Key* oder einer Datei) geändert wird.
4911: Die Ressourcenattribute des Objekts wurden geändert.	Dieses Ereignis wird generiert, wenn Ressourcenattribute des Dateisystem-Objekts geändert werden
4913: Die zentrale Zugriffsrichtlinie für das Objekt wurde geändert.	Dieses Ereignis wird generiert, wenn die zentrale Zugriffsrichtlinie für das Dateisystem-Objekt geändert wird. Dieses Ereignis wird unabhängig von den Überwachungsrichtlinien-Einstellungen des Objekts generiert.

5.3.1.5 Stellen Sie sicher, dass „MPSSVC-Richtlinienänderung auf Regelebene überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.7.4 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Richtlinienänderung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4944: Die folgende Richtlinie war aktiv, als die Windows-Firewall gestartet wurde.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (MpsSvc) gestartet wird. Das Ereignis zeigt die Einstellungen des öffentlichen Profils an, die bei Start wirksam waren.
4945: Beim Starten der Windows-Firewall wurde eine Regel aufgelistet.	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (MpsSvc) gestartet wird. Das Ereignis zeigt die eingehende und / oder ausgehende Regel des öffentlichen Profils an, die beim Start wirksam waren.
4946: Es wurde eine Änderung an der Ausnahmeliste der Windows-Firewall vorgenommen. Eine Regel wurde hinzugefügt.	Dieses Ereignis wird generiert, wenn der Windows-Firewall eine neue lokale Regel hinzugefügt wird. Das Ereignis wird nicht generiert, wenn eine neue Regel per Gruppenrichtlinien hinzugefügt wird.
4947: Es wurde eine Änderung an der Ausnahmeliste der Windows-Firewall vorgenommen. Eine Regel wurde geändert.	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall Regel geändert wird. Das Ereignis

Ereignis-ID: Name	Begründung
	wird nicht generiert, wenn die Regel per Gruppenrichtlinien geändert wird.
4948: Es wurde eine Änderung an der Ausnahmeliste der Windows-Firewall vorgenommen. Eine Regel wurde gelöscht.	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall Regel gelöscht wird. Das Ereignis wird nicht generiert, wenn die Regel per Gruppenrichtlinien gelöscht wird.
4949: Die Windows-Firewall-Einstellungen wurden wieder auf die Standardwerte zurückgesetzt.	Dieses Ereignis wird generiert, wenn die lokale Einstellung der Windows-Firewall auf die Standardkonfiguration zurückgesetzt wird.
4950: Eine Windows-Firewall-Einstellung wurde geändert.	Dieses Ereignis wird generiert, wenn die lokale Einstellung der Windows-Firewall geändert wird. Das Ereignis wird nicht generiert, wenn die Einstellung per Gruppenrichtlinien geändert wird.
4951: Eine Regel wurde ignoriert, weil die Hauptversionsnummer von der Windows-Firewall nicht erkannt wurde.	Dieses Ereignis wird generiert, wenn die Version (d. h. die Struktur) der Windows-Firewall-Regel nicht von der Firewall-Engine interpretiert und implementiert werden kann.
4952: Teile einer Regel wurden ignoriert, weil die untergeordnete Versionsnummer von der Windows-Firewall nicht erkannt wurde. Die anderen Teile der Regel werden angewendet.	Dieses Ereignis wird generiert, wenn die Version (d. h. die Struktur) der Windows-Firewall-Regel nur teilweise von der Firewall-Engine interpretiert und implementiert werden kann.
4953: Eine Regel wurde von der Windows-Firewall ignoriert, da Sie die Regel nicht analysieren konnte.	Dieses Ereignis wird generiert, wenn eine Windows-Firewall-Regel nicht von der Firewall-Engine interpretiert und implementiert werden kann.
4954: Die Einstellungen für die Windows-Firewall-Gruppenrichtlinien wurden geändert. Die neuen Einstellungen wurden angewendet.	Dieses Ereignis wird generiert, wenn die Windows-Firewall-Gruppenrichtlinieneinstellungen geändert oder aktualisiert werden.
4956: Die Windows-Firewall hat das aktive Profil geändert.	Dieses Ereignis wird generiert, wenn die Windows-Firewall das aktive Profil geändert hat.
4957: Die Windows-Firewall hat die folgende Regel nicht angewendet.	Dieses Ereignis wird generiert, wenn die Windows-Firewall beim Start oder beim Anwenden einer neuen Regel, eine Regel nicht anwenden kann.
4958: Die Windows-Firewall hat die folgende Regel nicht angewendet, da die Regel auf Elemente verweist, die auf diesem Computer nicht konfiguriert sind.	Dieses Ereignis wird generiert, wenn die Windows-Firewall eine Regel verarbeitet, die Parameter enthält, die auf dem lokalen Computer nicht verarbeitet werden können.

5.3.1.6 Stellen Sie sicher, dass „Andere Richtlinienänderungsereignisse überwachen“ den Wert „Fehler“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.7.5 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Richtlinienänderung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4826: Startkonfigurationsdaten geladen.	Dieses Ereignis wird generiert, wenn das Systemstartet und die aktuellen BCD-Einstellungen (Boot Configuration Data) eingelesen und implementiert werden.
4909: Die lokalen Richtlinieneinstellungen für die TBS wurden geändert.	Dieses Ereignis wird generiert, wenn eine Änderung an der TPM-Konfiguration im lokalen Richtlinienobjekt des Computers durchgeführt wird.
4910: Die Gruppenrichtlinieneinstellungen für die TBS wurden geändert.	Dieses Ereignis wird generiert, wenn eine Änderung an der TPM-Konfiguration über ein Gruppenrichtlinienobjekt durchgeführt wird.
6144: Die Sicherheitsrichtlinie in den Gruppenrichtlinienobjekten wurde erfolgreich angewendet.	Dieses Ereignis wird generiert, wenn Einstellungen aus dem Abschnitt "Sicherheitseinstellungen" im Gruppenrichtlinienobjekt ohne Fehler auf einen Computer angewendet werden konnten.
6145: Bei der Verarbeitung der Sicherheitsrichtlinien in den Gruppenrichtlinienobjekten ist ein oder mehrere Fehler aufgetreten.	Dieses Ereignis wird generiert, wenn Einstellungen aus dem Abschnitt "Sicherheitseinstellungen" im Gruppenrichtlinienobjekt nicht ohne Fehler auf einen Computer angewendet werden konnten.

5.3.1.7 Stellen Sie sicher, dass der ETW-Provider „TPM“ aktiviert ist.

Dieser Provider generiert Ereignisse in Zusammenhang mit dem TPM-Chip.

Konfigurationspfad im Registrierungs-Editor

Stellen Sie sicher, dass unter dem Registrierungs-Pfad `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System\{1b6b0772-251b-4d42-917d-faca166bc059}` der Eintrag:

- `Enabled` auf den Wert `1` gesetzt ist (aktiviert den ETW-Provider).

Standardwert
Aktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
20	Dieses Ereignis wird generiert, wenn der Zähler für die TPM-Sperrung zurückgesetzt wird.
21	Dieses Ereignis wird generiert, wenn das TPM einen Autorisierungsfehler bei Ausführung eines TPM-Befehls zurückgibt, was zu einer TPM-Sperrung führen kann.

Ereignis-ID	Begründung
23	Dieses Ereignis wird generiert, wenn die Ausführung eines TPM-Befehls auf Grund zu vieler vorangegangener Autorisierungsfehler temporär blockiert wird.

Hinweis: Die genannten Ereignisse werden im Windows-Protokoll „System“ gespeichert.

5.3.1.8 Stellen Sie sicher, dass der ETW-Provider „Microsoft-Windows-TPM-WMI“ aktiviert ist.

Dieser Provider generiert Ereignisse in Zusammenhang mit dem TPM-Chip.

Konfigurationspfad im Registrierungs-Editor

Stellen Sie sicher, dass unter dem Registrierungs-Pfad
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\WMI\Autologger\EventLog-System\{7d5387b0-cbe0-11da-a94d-800200c9a66}` der Eintrag:

- `Enabled` auf den Wert `1` gesetzt ist (aktiviert den ETW-Provider).

Standardwert
Aktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
769	Dieses Ereignis wird generiert, wenn sich die Konfiguration der sog. TPM Owner Authorization ändert.
1025	Dieses Ereignis wird generiert, wenn das TPM erfolgreich provisioniert wird.
1027	Dieses Ereignis wird generiert, wenn mit Hilfe des TPM-Befehls TakeOwnership das TPM vom System in Besitz genommen wird.
1793	Dieses Ereignis wird generiert, wenn eine Löschung des TPM durch das System geplant ist.

Hinweis: Die genannten Ereignisse werden im Windows-Protokoll „System“ gespeichert.

5.3.2 Anwendungs- und Dienstprotokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der Anwendungs- und Dienstprotokolle, die nicht über Gruppenrichtlinien konfigurierbar sind, aber über Gruppenrichtlinienobjekte verteilt werden können.

5.3.2.1 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse, die sich auf die Konfiguration der Windows Defender Firewall beziehen. Die Windows Defender Firewall ist eine in das Betriebssystem Windows integrierte Software-Firewall.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log „Microsoft-Windows-Windows Firewall With Advanced Security/Firewall“ /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 1.028 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
2032	Dieses Ereignis wird generiert, wenn die lokale Konfiguration der Windows-Firewall auf die Standardkonfiguration zurückgesetzt wird.
2002	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall-Einstellung geändert wird.
2006	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall-Regel gelöscht wird.
2033	Dieses Ereignis wird generiert, wenn alle lokalen Windows-Firewall-Regel deaktiviert werden.
2005	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall-Regel geändert wird.
2008	Dieses Ereignis wird generiert, wenn Windows-Firewall-Gruppenrichtlinieneinstellungen erfolgreich angewendet werden.
2009	Dieses Ereignis wird generiert, wenn Windows-Firewall-Gruppenrichtlinieneinstellungen nicht geladen werden können.
2003	Dieses Ereignis wird generiert, wenn eine lokale Windows-Firewall-Profileinstellung geändert wird.
2004	Dieses Ereignis wird generiert, wenn der Windows-Firewall eine neue lokale Regel hinzugefügt wird.
2010	Dieses Ereignis wird generiert, wenn das Windows-Firewall-Profil eines Netzwerkadapters geändert wird.

5.3.2.2 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse, die sich auf den Betriebszustand der Windows Defender Firewall beziehen. Die Windows Defender Firewall ist eine in das Betriebssystem Windows integrierte Software-Firewall.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log „Microsoft-Windows-Windows Firewall With Advanced Security/FirewallVerbose“ /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Deaktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
2001	Dieses Ereignis wird generiert, wenn eine Windows-Firewall Profileinstellung angewendet wird.
2007	Dieses Ereignis wird generiert, wenn der Windows Firewall-Dienst (*MpsSvc*) beim Start eine Regel interpretiert.
2000	Dieses Ereignis wird generiert, wenn eine Windows-Firewall Regel beim Systemstart eingelesen wird.

5.4 Netzwerkaktivität

Im folgenden Kapitel werden Konfigurationsempfehlungen und zugehörige Ereignisse im Zusammenhang mit eingehendem und ausgehendem Netzwerkverkehr beschrieben. Die Protokollierung der Netzwerkaktivität dient dazu Kommunikationsverbindungen zu anderen Systemen sichtbar zu machen. Dies kann es ermöglichen, erste (versuchte) Angriffe zu erkennen, indem ein Kommunikationsaufbau zu bekannten Phishing-Webseiten oder mit Malware infizierten Webseiten protokolliert wird.

Nach einer erfolgten Kompromittierung kann es zudem zu weiteren auffälligen Netzwerkverbindungen kommen, wie der Kommunikation von Schadsoftware oder Angreifern zu verdächtigen Systemen außerhalb der eigenen Umgebung, wie zum Beispiel zu einem (bekannten) Command and Control Server (Computer, der Anweisungen an mit Malware infizierte Systeme ausgibt). Netzwerkverbindungen innerhalb des internen Netzwerks können auch Hinweise auf einen laufenden Angriff liefern, bei dem sich Schadsoftware oder ein Angreifer im Netzwerk ausbreitet. Dabei kann es schwierig sein, legitime Netzwerkverbindungen von denen eines Angreifers zu unterscheiden.

Wird die Kompromittierung eines Systems identifiziert, stellt die Protokollierung der Netzwerkverbindungen eine wichtige Grundlage für die forensische Analyse des Sicherheitsvorfalls dar.

Beispielhafte Szenarien, die durch die Protokollierung und Auswertung von Netzwerkaktivität detektiert werden können, können sein:

- Domain Name System-basierte Angriffe, wie Local DNS-Hijacking, bei dem in den Netzwerkeinstellungen eines Systems die IP-Adresse des DNS-Servers auf einen bösartigen Wert gesetzt wird und somit die Kommunikation kompromittiert wird, können auf erste Angriffsschritte folgen.
- Hinweise auf (versuchte) Man-in-the-Middle-Angriffe (eine Angriffstechnik, bei der ein Angreifer den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern kontrolliert in dem er sich logisch oder physisch dazwischen schaltet) auf SMB-Verbindungen im internen Netzwerk, können Ereignisse im Zusammenhang mit fehlgeschlagener Signaturprüfung oder Verschlüsselung, wie einem (versuchten) Herunterstufen auf SMB 2.0, liefern.

- Anomalien, wie ungewöhnliche Prozesse, die Netzwerkverbindungen annehmen oder aufbauen, oder Dienste, die an einen falschen Port gebunden sind.

Die folgenden Empfehlungen sollten umgesetzt werden, um die Protokollierung von Ereignissen in Bezug auf DNS- und SMB-Aktivität zu gewährleisten.

Hinweis: Die Einstellungen für die Protokollierung von Daten, die im Zusammenhang mit erlaubten und blockierten Paketen durch die Windows Defender Firewall stehen, werden in Kapitel 4.2 beschrieben.

5.4.1 Anwendungs- und Dienstprotokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der Anwendungs- und Dienstprotokolle, die nicht über Gruppenrichtlinien konfigurierbar sind, aber über Gruppenrichtlinienobjekte verteilt werden können.

5.4.1.1 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-DNS Client Events/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Ereignisse in Zusammenhang mit Windows Domain Name System (DNS) Client. In dieses Ereignisprotokoll werden unter anderem sämtliche Namensauflösungen und Fehler während der Namensauflösung protokolliert.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log „Microsoft-Windows-DNS Client Events/Operational“ /enabled:true /retention:false /maxsize:201326592` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

Standardwert
Deaktiviert

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
1001	Dieses Ereignis wird generiert, wenn die DNS-Server Informationen an einer Netzwerkschnittstelle konfiguriert werden
3008	Dieses Ereignis wird generiert, wenn eine DNS-Abfrage abgeschlossen wird.
3009	Dieses Ereignis wird generiert, wenn eine DNS-Abfrage indiziert wird.
3010	Dieses Ereignis wird generiert, wenn eine DNS-Abfrage an einen DNS-Server gesendet wird.
3011	Dieses Ereignis wird generiert, wenn eine DNS-Abfrage von einen DNS-Server empfangen wird.

5.4.1.2 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-SMBClient/Connectivity" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Überwachung des Windows Server Message Block (SMB)-Clients. Der Windows SMB-Client wird für den Zugriff auf Freigaben benötigt.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-SMBClient/Connectivity /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 8.192 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
30803	Dieses Ereignis wird generiert, wenn das System keine Netzwerkverbindung zum Zielsystem herstellen kann.
30800	Dieses Ereignis wird generiert, wenn das System den Servernamen des Zielsystems nicht erfolgreich auflösen kann.
30804	Dieses Ereignis wird generiert, wenn die SMB-Verbindung zum Zielsystem getrennt wird.
30816	Dieses Ereignis wird generiert, wenn das System und der Zielserver keine gemeinsame SMB-Version aushandeln können.

5.4.1.3 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-SMBClient/Security" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Überwachung des Windows Server Message Block (SMB)-Clients. Der Windows SMB-Client wird für den Zugriff auf Freigaben benötigt.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-SMBClient/Security /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 8.192 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
31002	Dieses Ereignis wird generiert, wenn ein Netzwerktoken nicht für eine ausgehende Authentifizierung genutzt werden kann (in der Regel auf Grund fehlender Delegierung).
31010	Dieses Ereignis wird generiert, wenn der SMB-Client keine Verbindung mit einer Freigabe herstellen kann.
31012	Dieses Ereignis wird generiert, wenn die Überprüfung der ausgehandelten SMB-Parameter (wie z. B. die SMB-Version oder unterstützten SMB-Funktionen) bei Zugriff auf eine Freigabe fehlschlägt.
31013	Dieses Ereignis wird generiert, wenn die Signaturprüfung der SMB-Nachrichten bei der Übertragung zwischen Server und Client fehlschlägt.
31014	Dieses Ereignis wird generiert, wenn der Client eine unverschlüsselte Nachricht erhält, aber eine verschlüsselte erwartet wird.
31017	Dieses Ereignis wird generiert, wenn der Server versucht, den Benutzer als nicht authentifizierten Gast anzumelden.

5.4.1.4 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-SMBServer/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Überwachung des Windows Server Message Block (SMB)-Server. Der Windows SMB-Server wird für die Bereitstellung von Freigaben benötigt.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-SMBServer/Security /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert

Aktiviert (max. Protokollgröße: 8.192 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
1001	Dieses Ereignis wird generiert, wenn der Versuch eines Clients über SMB Version 1 auf den Server zuzugreifen, abgelehnt wird.
1003	Dieses Ereignis wird generiert, wenn der Versuch eines Clients unverschlüsselt Daten an den Server zu senden, abgelehnt wird.

Ereignis-ID	Begründung
1004	Dieses Ereignis wird generiert, wenn der Versuch eines Clients eine falsch signierte Nachricht an den Server zu senden, abgelehnt wird.
1005	Dieses Ereignis wird generiert, wenn die Überprüfung der ausgehandelten SMB-Parameter (wie z. B. die SMB-Version oder unterstützten SMB-Funktionen) zwischen Client und Server fehlschlägt.

5.4.1.5 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-SMBServer/Security" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Informationen zur Überwachung des Windows Server Message Block (SMB)-Server. Der Windows SMB-Server wird für die Bereitstellung von Freigaben benötigt.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-SMBServer/Security /enabled:true /retention:false /maxsize:33554432` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Standardwert
Aktiviert (max. Protokollgröße: 8.192 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
551	Dieses Ereignis wird generiert, wenn die Authentifizierung beim SMB-Verbindungsaufbau fehlgeschlagen ist.
1006	Dieses Ereignis wird generiert, wenn der Zugriff auf eine Freigabe aufgrund unzureichender Berechtigungen fehlgeschlagen ist.
1009	Dieses Ereignis wird generiert, wenn ein Zugriff auf eine Freigabe ohne Anmeldeinformationen versucht und vom Server verweigert wird.

5.5 Prozessaktivität

Unter einem Prozess versteht man die Instanziierung eines Programms zur Laufzeit unter der Kontrolle des Betriebssystems. Letztlich führt somit jegliche Ausführung von Code zu der Erstellung eines Prozesses. Im folgenden Kapitel werden Ereignisse beschrieben, die beim Erstellen oder Starten von Prozessen, sowie im Speziellen bei der Verwendung der Windows PowerShell, die eine Möglichkeit zur Interaktion mit dem Computersystem bietet, die auch von Angreifern genutzt wird, generiert werden. Diese zu protokollieren soll Aktivitäten von Benutzern und Anwendungen sowie auch Angreifern sichtbar machen und erlauben nachzuvollziehen wie ein System verwendet wird. Siehe hierzu auch die Kapitel 4.3.3 und 4.3.4.

Die Protokollierung der Prozesserstellung hilft nachzuvollziehen, welches Konto einen Prozess erstellt hat, sowie welcher Tokenerweiterungstyp (dieser gibt an, ob und wie die Benutzerkontensteuerung beim Prozesstart zum Einsatz kam) und welche Integritätsebene (diese steuert, neben konkreten Objektberechtigungen, die Zugriffskontrolle) einem Prozess zugewiesen sind. Des Weiteren lässt sich mit der Protokollierung festhalten, in welchem Ordner ein Prozess gestartet wurde. Dies kann wie folgt in beispielhaften Protokollanalyseszenarien genutzt werden:

- Über das Feld Tokenerweiterungstyp im Ereignis 4688 lässt sich identifizieren, wenn Konten, für die die Benutzerkontensteuerung deaktiviert ist, Prozesse anstoßen (Standard-Tokenerweiterungstyp (1)) und wenn Prozesse als Administrator ausgeführt wurden und die Benutzerkontensteuerung aktiviert ist (Vollständiger Tokenerweiterungstyp (2)). Dies kann hilfreich sein, um nach einer entdeckten Kompromittierung eines Kontos, dessen Aktionen zu rekonstruieren.
- Auffälligkeiten in der Ausführung, wie das Starten eines privilegierten Prozesses aus dem Temp-Ordner, können überwacht werden. Dies kann hilfreich für das Erkennen oder die forensische Rekonstruktion von Angriffen sein, die auf der Ausführung von Malware basieren.
- Die Ausführung von bekannten Standardversionen von Malware (z. B. *mimikatz*) kann zusätzlich auch basierend auf dem Prozessnamen und zugehörigen Prozessparametern detektiert werden, die ebenfalls Teil von Ereignis 4688 sind.

Das Protokollieren von Aktionen der Windows PowerShell, welche von Angreifern sowohl für die Kompromittierung eines Systems als auch für einen anschließenden weiteren Zugriff auf ein System genutzt werden kann, bietet die Möglichkeit detailliert Aktivitäten, die mit der Windows PowerShell durchgeführt wurden, nachzuvollziehen. Die protokollierten Informationen können nützlich sein, um Einblick in die Aktionen eines Angreifers zu gewinnen (siehe auch 4.3.4). Außerdem kann je nach legitimer Nutzung eines Systems, schon die (versuchte) Verwendung der Windows PowerShell verdächtig sein.

Um die Protokollierung der notwendigen Daten für Prozesserstellung und PowerShell-Aktivität zu aktivieren, sollten die nachfolgenden Konfigurationsempfehlungen umgesetzt werden.

5.5.1 Windows-Protokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der System- und Sicherheits-Protokolle, die über Gruppenrichtlinien konfigurierbar sind.

5.5.1.1 Stellen Sie sicher, dass „Prozesserstellung überwachen“ den Wert „Erfolg“ enthält.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.3.2 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Hinweis: Diese Ereigniskategorie enthält keine Fehler-Ereignisse (siehe (ms_pc, 2020)*).*

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Detaillierte Überwachung

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4688: Ein neuer Prozess wurde erstellt.	Dieses Ereignis wird generiert, wenn ein Prozess gestartet wird.

5.5.1.2 Stellen Sie sicher, dass „Sensible Verwendung von Rechten überwachen“ auf den Wert „Erfolg und Fehler“ gesetzt ist.

Beschreibung, Konfigurationsempfehlung und Auswirkung identisch zu 17.8.1 des CIS Benchmark. Konfigurationsempfehlung identisch zu Microsoft Security Baseline.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Berechtigungen

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
4673: Ein privilegierter Dienst wurde aufgerufen.	Dieses Ereignis wird generiert, wenn ein Prozess versucht eine privilegierte Systemdienstfunktionalität auszuführen, die eine der folgenden privilegierten Berechtigungen erfordert: *SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeCreateTokenPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege, SeLockMemoryPrivilege, SeSystemEnvironmentPrivilege, SeTcbPrivilege, SeEnableDelegationPrivilege*.
4674: Ein Vorgang wurde für ein privilegiertes Objekt versucht.	Dieses Ereignis wird generiert, wenn ein Prozess versucht ein bereits bestehendes privilegiertes Objekt anzufordern, das eines der folgenden privilegierten Berechtigungen erfordert: *SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeCreateTokenPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeLoadDriverPrivilege, SeLockMemoryPrivilege, SeSystemEnvironmentPrivilege, SeTcbPrivilege, SeEnableDelegationPrivilege*.

5.5.2 Anwendungs- und Dienstprotokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der Anwendungs- und Dienstprotokolle, die nicht über Gruppenrichtlinien konfigurierbar sind, aber über Gruppenrichtlinienobjekte verteilt werden können.

5.5.2.1 Stellen Sie sicher, dass das Protokoll "Microsoft-Windows-PowerShell/Operational" aktiviert und konfiguriert ist.

Dieses Ereignisprotokoll enthält Mitschnitte der PowerShell-Aktivität, sofern Protokollierung von PowerShell-Skriptblöcken aktiviert ist.

Hinweis: Dieses Ereignisprotokoll kann sensitive Informationen enthalten, da jeglicher prozessierter Code mitgeschrieben wird. Enthält der Code beispielsweise Passwörter, werden diese im Klartext protokolliert.

Konfiguration des Protokolls über wevtutil.exe

Führen Sie in einer Kommandozeile den Befehl `wevtutil.exe set-log Microsoft-Windows-PowerShell/Operational /enabled:true /retention:false /maxsize:536870912` aus, um das Protokoll zu aktivieren und zu konfigurieren.

Hinweis: Abhängig von der Nutzung des Systems, kann die empfohlene Konfiguration der Protokollgröße nicht ausreichend sein, da potenziell eine sehr hohe Anzahl von Ereignissen in kurzer Zeit protokolliert wird. In einem solchen Fall sollte die Protokollgröße über den empfohlenen Wert hinaus erweitert werden oder die Protokolldaten idealerweise zentral gesammelt werden.

Standardwert
Aktiviert (max. Protokollgröße: 15.360 KB)

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID	Begründung
4100	Dieses Ereignis wird generiert, wenn ein Fehler bei der Verarbeitung innerhalb der PowerShell aufritt, z. B. wenn ein Skript aufgrund einer *Execution Policy* nicht ausgeführt werden kann.
4103	Dieses Ereignis wird generiert, wenn ein PowerShell Kommando aufgerufen wird.
4104	Dieses Ereignis wird generiert, wenn die PowerShell einen *Skriptblock* interpretiert.
24577	Dieses Ereignis wird generiert, wenn das PowerShell *Integrated Scripting Environment* (ISE) ein PowerShell-Skript ausführt.
40961	Dieses Ereignis wird generiert, wenn eine PowerShell-Konsole indiziert wird.
40962	Dieses Ereignis wird generiert, wenn eine PowerShell-Konsole bereit ist Benutzereingaben zu empfangen.

5.6 Registrierungsaktivität

Die Registrierung eines Windows-Systems ist eine hierarchische Datenbank, in welcher alle für die Verwaltung des Systems, sowie integrierter Systemdienste und -prozesse relevanten Konfigurationsparameter und teilweise auch die Einstellungen für Anwendungsprogramme gespeichert

sind. Die Integrität der Registrierung ist somit zentral für den Zustand und die Sicherheit eines Systems und Änderungen an der Registrierung sollten an relevanten Stellen protokolliert werden.

In diesem Kapitel wird die Konfiguration der Protokollierung von sicherheitsrelevanten Änderungen an Registrierungsobjekten beschrieben, die nicht durch andere, in den vorhergehenden Kapiteln beschriebene Protokollierungsereignisse abgedeckt oder nur zum Teil erfasst werden. Änderungen an der Registrierung sind eine Möglichkeit für Angreifer, nach einer erfolgreichen Kompromittierung Persistenz auf einem System zu erreichen. Beispielhafte Szenarien, die durch die Analyse der protokollierten Daten für bestimmte Registrierungsschlüssel abgedeckt werden können, sind:

- Registrierungsschlüssel, die die automatische Ausführung von bestimmter Malware oder Befehlen bei jeder Benutzeranmeldung oder beim Booten des Systems auslösen.
- Registrierungsschlüssel, die für die Registrierung neuer Dienste oder Treiber genutzt werden können.
- Registrierungsschlüssel, die die Benutzerauthentifizierung durch neue Protokolle oder Passwortfilter erweitern.

Legitime Änderungen an diesen Registrierungsschlüsseleinträgen treten normalerweise auf, wenn legitime Software installiert wird. Ist dies nicht der Fall, könnte dies durch die Aktionen eines Angreifers oder Schadsoftware ausgelöst worden sein. Auffällige Änderungen an der Registrierung können zudem mit anderen Ereignissen, wie auffälligen Netzwerkverbindungen nach einer Benutzeranmeldung, korreliert werden.

Die nachfolgenden Empfehlungen sollten konfiguriert werden, um die Protokollierung von Registrierungsaktivität generell zu aktivieren und bestimmte Registrierungsschlüssel hinsichtlich Modifikation zu überwachen.

5.6.1 Windows-Protokolle

Dieser Abschnitt enthält Empfehlungen für die Konfiguration der System- und Sicherheits-Protokolle, die über Gruppenrichtlinien konfigurierbar sind.

5.6.1.1 Stellen Sie sicher, dass „Registrierung überwachen“ auf den Wert „Erfolg“ gesetzt ist.

Diese Einstellung aktiviert die Registrierungsüberwachung.

Hinweis: Ein entsprechendes Ereignis im Protokoll wird nur für Objekte generiert, für die eine sog. System Access Control List (SACL) konfiguriert wurde (siehe Abschnitt 5.6.1.2).

Begründung

Da die Registrierung einen essenziellen Bestandteil des Windows-Betriebssystems bildet und sicherheitskritische Konfigurationen vorhält, die von Angreifern z. B. für Persistenz modifiziert werden, sollten Veränderungen an relevanten Registrierungsobjekten protokolliert werden.

Auswirkung

Wenn diese Einstellung aktiviert wird, wird für jeden erfolgreichen Versuch mit Hilfe eines Kontos auf ein Registrierungsobjekt mit übereinstimmender *System Access Control List* zuzugreifen, ein Ereignis erzeugt.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Erweiterte Überwachungsrichtlinienkonfiguration\Objektzugriff

Standardwert
Keine Überwachung

Relevante Ereignis-IDs

Die folgenden beispielhaften Ereignisse werden durch die empfohlene Konfiguration aufgezeichnet:

Ereignis-ID: Name	Begründung
4657: Ein Registrierungswert wurde geändert.	Dieses Ereignis wird generiert, wenn ein Wert für einen Registrierungs-Schlüssel erfolgreich geändert wurde.
4660: Ein Objekt wurde gelöscht.	Dieses Ereignis wird generiert, wenn ein Registrierungs-Objekt erfolgreich gelöscht wurde.
4670: Die Berechtigungen für ein Objekt wurden geändert.	Dieses Ereignis wird generiert, wenn die Berechtigungen auf einem Registrierungs-Objekt erfolgreich geändert wurden.

5.6.1.2 Stellen Sie sicher, dass für sicherheitsrelevante Registrierungsobjekte eine SACL konfiguriert ist.

Die folgenden Einstellungen aktivieren die Überwachung für bestimmte Registrierungsobjekte.

Begründung

Damit entsprechende Ereignisse für die Überwachung der Registrierung im Protokoll generiert werden, muss die sog. *System Access Control List* (SACL) für sicherheitsrelevante Objekte konfiguriert werden.

Auswirkung

Wenn diese Einstellungen aktiviert werden, wird für jeden erfolgreichen Versuch mit Hilfe eines Kontos auf die genannten Registrierungsobjekte zuzugreifen, ein Ereignis erzeugt.

Konfigurationspfad im Gruppenrichtlinien-Editor

Computerkonfiguration\Windows-Einstellungen\Sicherheitseinstellungen\Registrierung Stellen Sie sicher, dass für die nachfolgenden Registrierungs-Schlüssel die folgenden Überwachungseinträge (nach Auswahl des Registrierungsschlüssels auf „Erweitert“ klicken und den Reiter „Überwachung“ auswählen, danach auf „Hinzufügen“) konfiguriert sind: • Prinzipal: „Jeder“ • Typ: „Erfolgreich“ • Anwenden auf: „Nur diesen Schlüssel“ **oder** „Diesen und untergeordnete Schlüssel“ • Erweiterte Berechtigungen: „Wert festlegen“, „Unterschlüssel erstellen“, „Löschen“, „Berechtigungen ändern“, „Besitz übernehmen“

Hinweis: Dieser Konfigurationspfad existiert nur bei der Modifikation von Gruppenrichtlinienobjekten in einer Active Directory-Domäne. Auf Einzelsystemen müssen die nachfolgenden Einstellungen manuell über den Registrierungs-Editor (mit Hilfe des Berechtigungs-Menüs für Registrierungsschlüssel) oder über ein PowerShell-Skript (mit Hilfe des Befehls Set-Acl) angewendet werden. Eine beispielhafte Konfiguration würde wie folgt aussehen:

Führen Sie die folgenden Befehle in einer administrativen PowerShell-Sitzung aus:

Angabe des Pfads zum Registrierungs-Schlüssel, der konfiguriert werden soll:

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

Auslesen und Zwischenspeichern der aktuellen System Access Control List des zu konfigurierenden Schlüssels:

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

Erstellen eines neuen Objekts, das die relevante Konfiguration für die Überwachung beinhaltet:

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

Hinzufügen der neuen Überwachungseinträge zu der zwischengespeicherten Access Control List:

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

Anwenden der neuen Konfiguration auf den aktuellen Registrierungs-Schlüssel:

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

Für die Anwendung der Einstellung „Anwenden auf: Diesen und untergeordnete Schlüssel“ muss die Erstellung des Objekts, das die Überwachungseinträge trägt, wie folgt abgeändert werden:

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

Relevante Registrierungs-Objekte

Die folgenden Registrierungs-Schlüssel sollten durch die empfohlenen Einträge überwacht werden:

Registrierungs-Schlüssel	Begründung
Anwenden auf: Nur diesen Schlüssel	
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Accessibility\ATs	Wenn eine neue Anwendung für erleichterte Bedienung registriert wird, werden an dieser Stelle Unterschlüssel erzeugt.

Registrierungs-Schlüssel	Begründung
HKLM\SYSTEM\CurrentControlSet\Control\Lsa	Wenn die Benutzerauthentifizierung durch neue Protokolle oder Passwortfilter erweitert wird, werden an dieser Stelle Unterschlüssel erzeugt.
HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders	Wenn ein neuer kryptographischer Provider registriert wird, werden an dieser Stelle Unterschlüssel erzeugt.
HKLM\SYSTEM\CurrentControlSet\Services	Wenn ein neuer Dienst oder Treiber registriert wird, werden an dieser Stelle Unterschlüssel erzeugt.
Anwenden auf: Diesen und untergeordnete Schlüssel	
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 (vor allem der Registrierungswert *StartupPrograms*) HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp (vor allem der Registrierungswert *InitialProgram*)	Wenn eine Anwendung für die automatische Ausführung bei einer Benutzeranmeldung konfiguriert wird, werden an diesen Stellen Unterschlüssel erzeugt oder Registrierungs-Werte modifiziert.
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components	Wenn eine Anwendung für die automatische Ausführung vor dem Laden des Desktops über *Active Setup* konfiguriert wird, werden an diesen Stellen Unterschlüssel erzeugt.
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	Wenn das Verhalten des Benutzeranmeldevorgangs (inkl. der Konfiguration welche Anwendungen initial gestartet werden) konfiguriert wird, werden an dieser Stelle Registrierungs-Werte modifiziert.

Registrierungs-Schlüssel	Begründung
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot (vor allem der Registrierungswert *AlternateShell*)	Wenn das Verhalten des abgesicherten Modus konfiguriert wird, wird dieser Registrierungs-Wert modifiziert.
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	Wenn über Gruppenrichtlinien ein Skript oder eine Anwendung für die automatische Ausführung konfiguriert wird, wird die Konfiguration an diesen Stellen gespeichert.
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 (vor allem der Registrierungswert *Shell*) HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System (vor allem der Registrierungswert *Shell*)	Analog zu den systemweiten Konfigurationen für Anwendungen, die automatisch bei einer Benutzeranmeldung ausgeführt werden, werden an diesen Stellen für benutzerspezifische Einstellungen Unterschlüssel erzeugt oder Registrierungs-Werte modifiziert. *Hinweis: Diese Registrierungspfade sind spezifisch für jeden angemeldeten Benutzer.*

Registrierungs-Schlüssel	Begründung
HKCU\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logon HKCU\SOFTWARE\Policies\Microsoft\Windows\System\Scripts\Logoff	

Appendix

Werkzeuge

Werkzeug	Verfügbarkeit und Beschreibung
Gruppenrichtlinienverwaltungs-Editor	*Verfügbarkeit:* Verteilt mit Windows 10 *Beschreibung:* Ein Werkzeug zur Konfiguration von Gruppenrichtlinien.
Ereignisanzeige	*Verfügbarkeit:* Verteilt mit Windows 10 *Beschreibung:* Ein Werkzeug zur Einsicht und Konfiguration von Ereignisprotokollen.
Registrierungs-Editor	*Verfügbarkeit:* Verteilt mit Windows 10 *Beschreibung:* Ein Werkzeug zur Konfiguration der Registrierung.

Ereignis-IDs

Ereignis-IDs: Abs. 5.1.2.1

Ereignis-ID	Nachricht
100	Die Anmeldeinformationen, die für die Authentifizierung gegenüber dem Server erforderlich sind, werden vom Sicherheitspaket nicht zwischengespeichert. Paketname: %1 Benutzername: %2 Domänenname: %3 Servername: %4 Geschützter Benutzer: %5 Fehlercode: %6
200	Ein Sicherheitspaket hat eine Anforderung zur Netzwerkanmeldung empfangen, nachdem die Abmeldung abgeschlossen war. Benutzername: %1 Domänenname: %2 Anmelde-ID: %3 Abmeldezeit: %4 PID: %5 Programm: %6 Prinzipalname: %7 Servername: %8 Paketname: %9 Aufruftyp: %10 Fehlercode: %11
300	Die Gruppen wurden einer neuen Anmeldung zugewiesen. Neue Anmeldung: Sicherheits-ID: %1 Kontoname: %2 Kontodomäne: %3 Anmelde-ID: %4 Anmelde-GUID: %5 Ereignis in Sequenz: %6 von %7 Gruppenmitgliedschaft: %8
301	Die Ansprüche wurden einer neuen Anmeldung zugewiesen.

Ereignis-ID	Nachricht
	Neue Anmeldung: Sicherheits-ID: %1 Kontoname: %2 Kontodomäne: %3 Anmelde-ID: %4 Anmelde-GUID: %5 Anmeldetyp: %6 Ereignis in Sequenz: %7 von %8 Benutzeransprüche: %9 Geräteansprüche: %10 Dieses Ereignis wird generiert, wenn eine neue Anmeldesitzung erstellt wird und das zugeordnete Benutzertoken Benutzer- und/oder Geräteansprüche enthält. Die Felder für die neue Anmeldung enthalten das angemeldete Konto. Passen nicht alle Benutzer- und Geräteansprüche in ein einzelnes Ereignis, werden mehrere entsprechende Ereignisse generiert. Das Feld "Ereignis in Sequenz" gibt Aufschluss darüber, wie viele weitere Ereignisse für diese Anmeldesitzung generiert werden. Jeder Benutzer- oder Geräteanspruch wird im folgenden Format dargestellt: Anspruchs-ID Anspruchstyp-ID : Wert1, Wert2 à Häufig verwendete Anspruchstypen: 0 (ungültiger Typ), 1 (ganze 64-Bit-Zahl), 2 (unsignierte ganze 64-Bit-Zahl), 3 (Zeichenfolge), 4 (FQBN), 5 (SID), 6 (Boolesch) und 16 (BLOB). Übersteigt der Anspruch die maximal zulässige Länge, endet die Zeichenfolge auf "...".
302	Für den Benutzer "%1" wurde eine Abmeldebenachrichtigung empfangen. Anmelde-ID: %2 Name der Zertifizierungsstelle: %3 Kontoname: %4 Zeitlimit: %5 Sekunden
303	Die Anmeldeinformationen des Benutzers werden vom Sicherheitspaket nicht zwischengespeichert. Paketname: %1 Benutzername: %2 Domänenname: %3 Geschützter Benutzer: %4
320	Die Anmeldeinformationen für die automatische Anmeldung nach einem Neustart wurden für Folgendes erfolgreich konfiguriert: Kontoname: %1 Kontodomäne: %2
321	Die Anmeldeinformationen für die automatische Anmeldung nach einem Neustart konnten nicht konfiguriert werden. Fehler: %1
322	Bei der Anmeldung nach einem automatischen Neustart wurden die Anmeldeinformationen für das automatische Anmelden erfolgreich aus dem LSA-Speicher gelöscht.
5000	Das Sicherheitspaket "%1" verursachte eine Ausnahme. Daten: Ausnahmeinformationen.
6027	Das globale Kennwort %1 konnte nicht aktualisiert werden. Überprüfen Sie den Status aller Dienste im System.
6033	Eine anonyme Sitzung mit hergestellter Verbindung von %1 hat versucht, einen LSA-Richtlinienhandle auf diesem Computer zu öffnen. Der Versuch wurde mit STATUS_ACCESS_DENIED zurückgewiesen, um die Verbreitung von sicherheitssensitiven Informationen an einen anonymen Anrufer zu verhindern. Der Anwendungsfehler, der

Ereignis-ID	Nachricht
	diesen Versuch verursacht hat, sollte behoben werden. Wenden Sie sich an den Hersteller der Anwendung. Als temporären Workaround kann diese Sicherheitserkennung durch Setzen des DWORD Werts \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\TurnOffAnonymousBlock auf 1 aufgehoben werden. Diese Meldung wird höchstens einmal pro Tag protokolliert.
6035	Während eines Anmeldeversuchs hat der Sicherheitskontext des Benutzers zu viele Sicherheits-IDs angesammelt. Dies ist eine sehr ungewöhnliche Situation. Entfernen Sie den Benutzer von einigen globalen oder lokalen Gruppen, um die Anzahl der Sicherheits-IDs zu reduzieren und in den Sicherheitskontext aufgenommen zu werden. Benutzer-SID: %1 Wenn es sich hier um ein Administratorkonto handelt, werden durch die Anmeldung im sicheren Modus Gruppenmitgliedschaften automatisch eingeschränkt.
6036	Das Programm %2 mit der zugewiesenen Prozess-ID %1 stellte beim Aufruf der InitializeSecurityContext- API zur Initialisierung eines ausgehenden NTLM-Sicherheitskontexts einen NULL-Namen oder leeren Zielnamen für den PSZ-Zielnamenparameter zur Verfügung. Dies stellt ein Sicherheitsrisiko dar, wenn die gegenseitige Authentifizierung erforderlich ist. Zum Schutz vor bösartigen Angriffen muss der Code sicherer gemacht werden. Dazu muss das Programm geändert werden, sodass ein Zielname im PSZ-Zielnamen-Parameterfeld angegeben und der Code anschließend neu kompiliert wird.
6037	Das Programm %2 mit der zugewiesenen Prozess-ID %1 konnte sich mit dem Zielnamen %3 nicht lokal authentifizieren. Der verwendete Zielname ist ungültig. Ein Zielname muss sich auf einen der lokalen Computernamen beziehen, z. B. den DNS-Hostnamen. Wählen Sie einen anderen Zielnamen.
6038	Von Microsoft Windows Server wurde festgestellt, dass momentan zwischen Clients und diesem Server die NTLM-Authentifizierung verwendet wird. Dieses Ereignis tritt einmal pro Serverstart auf, wenn NTLM von einem Client erstmalig für den Server verwendet wird. NTLM ist ein relativ schwacher Authentifizierungsmechanismus. Prüfen Sie Folgendes: Von welchen Anwendungen wird die NTLM-Authentifizierung verwendet? Liegen Konfigurationsprobleme vor, die verhindern, dass ein stärkerer Authentifizierungsmechanismus (etwa Kerberos) verwendet wird? Wenn NTLM unterstützt werden muss: Ist der erweiterte Schutz konfiguriert? Ausführliche Informationen zum Ausführen dieser Überprüfungen finden Sie unter "http://go.microsoft.com/fwlink/?LinkId=225699".
6039	Von Microsoft Windows Server wurde festgestellt, dass momentan zwischen Clients und diesem Server die NTLM-Authentifizierung verwendet wird. Dieses Ereignis tritt einmal pro Serverstart auf, wenn NTLM von einem Client erstmalig für den Server verwendet wird. NTLM ist ein relativ schwacher Authentifizierungsmechanismus. Prüfen Sie Folgendes: Von welchen Anwendungen wird die NTLM-Authentifizierung verwendet? Liegen Konfigurationsprobleme vor, die verhindern, dass ein stärkerer Authentifizierungsmechanismus (etwa Kerberos) verwendet wird? Wenn NTLM unterstützt werden muss: Ist der erweiterte Schutz konfiguriert? Ausführliche Informationen zum Ausführen dieser Überprüfungen finden Sie unter "http://go.microsoft.com/fwlink/?LinkId=225699".
6040	Eine Authentifizierungsanforderung für das Paket "%1" wurde abgelehnt, weil die Zielinformationen ungültig waren. Die Authentifizierungsanforderung stimmte nicht mit dem Zielnamen von "%2" überein.
6041	Eine CredSSP-Authentifizierung für %1 konnte keine gemeinsame Protokollversion aushandeln. Der Remotehost hat die Version %2 angeboten, die gemäß Encryption Oracle-Abwehr nicht zugelassen ist. Weitere Informationen finden Sie unter https://go.microsoft.com/fwlink/?linkid=866660.

Ereignis-ID	Nachricht
6144	Ein geheimes Objekt, das für LSA privat ist, wurde von einem Client abgefragt. Aus Sicherheitsgründen wurde das Objekt im verschlüsselten Format zurückgegeben.
6145	Fehler beim Abrufen neuer zentraler Zugriffsrichtlinien für diesen Computer. Für die folgenden DNs konnten keine Richtlinien abgerufen werden: %1
6146	Fehler beim Verarbeiten neuer zentraler Zugriffsrichtlinien für diesen Computer. Folgende zentrale Zugriffsregel, auf die von mindestens einer zentralen Zugriffsrichtlinie verwiesen wird, konnte nicht überprüft werden: Fehler: %1 Name: %2 Beschreibung: %3
6147	Credential Guard ist für die Ausführung konfiguriert, aber nicht lizenziert. Credential Guard wurde nicht gestartet.
6182	LogonSession alive after interactive user logoff. Indicates a possible token leak in one of the services. Logon ID:%1 Account Name:%2 Domain Name:%3
6225	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6226	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6227	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6228	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6229	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6230	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6231	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
6232	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
32773	Es wurde eine Lookupanforderung ausgeführt, die eine Verbindung mit einem Domänencontroller in der Domäne %1 erfordert. Es konnte kein Domänencontroller in dieser Domäne gefunden werden. Fehler bei der Anforderung. Überprüfen Sie die Verbindung und die Installation des sicheren Kanals zwischen diesem Domänencontroller und der Domäne %2.
32774	Es wurde eine Lookupanforderung ausgeführt, die eine Verbindung mit einem Domänencontroller %1 erfordert. Es konnte kein Domänencontroller in dieser Domäne gefunden werden. Fehler bei der Anforderung. Überprüfen Sie die Verbindung und die Installation des sicheren Kanals zwischen diesem Domänencontroller und der Domäne %2.
32775	Es wurde eine Lookupanforderung ausgeführt, die Lookupdienste auf dem Remotedomänencontroller %1 erfordert. Fehler bei der Anforderung auf dem Remotedomänencontroller. Fehler bei der ursprünglichen Anforderung bei dem lokalen LSA. Überprüfen Sie die Verbindung und die Installation des sicheren Kanals zwischen diesem Domänencontroller und der Domäne %2.
32777	LSA konnte die RPC-Schnittstelle nicht über die TCP/IP-Schnittstelle registrieren. Stellen Sie sicher, dass das Protokoll ordnungsgemäß installiert ist.
32779	
32780	Die LSA konnte den UBPM beim Starten nicht mit Status %1 benachrichtigen.
40960	Das Sicherheitssystem hat einen Authentifizierungsfehler für den Server %1 festgestellt. Der Fehlercode des Authentifizierungsprotokolls %2 lautete %3.
40961	Das Sicherheitssystem konnte keine sichere Verbindung mit dem Server %1 herstellen. Es war kein Authentifizierungsprotokoll verfügbar.

Ereignis-ID	Nachricht
40962	Das Sicherheitssystem konnte sich nicht am Server %1 authentifizieren, da die Authentifizierung am Server abgeschlossen ist, aber das Clientauthentifizierungsprotokoll %2 noch nicht.
40964	Das Sicherheitssystem hat einen Authentifizierungsversuch mit einem unbekannten Authentifizierungsprotokoll empfangen. Fehler bei der Anforderung.
40965	Das Sicherheitssystem hat %2 als Authentifizierungsprotokoll mit dem Server %1 ausgewählt.
40966	Das Sicherheitssystem hat einen Authentifizierungsversuch empfangen und festgestellt, dass das vom Client bevorzugte Protokoll %1 angenommen werden kann.
40967	Das Sicherheitssystem hat eine Authentifizierungsanforderung direkt für das Protokoll %1 empfangen.
40968	Das Sicherheitssystem hat eine Authentifizierungsanforderung empfangen, die nicht decodiert werden konnte. Fehler bei der Anforderung.
40969	Das Sicherheitssystem hat einen Authentifizierungsversuch empfangen und festgestellt, dass es sich bei dem Protokoll %1 um das gemeinsam verwendete Protokoll handelt.
45056	Der Anmeldecache wurde deaktiviert. Ggf. treten während Netzwerklatenzen oder periodische Authentifizierungsfehler Unterbrechungen auf. Wenden Sie sich an den Systemadministrator.
45057	Durch einen Fehler bei einem Anmeldeversuch wurde ein Anmeldecacheeintrag für Benutzer %1 gelöscht. Das Authentifizierungspaket lautete %2 und die Fehlermeldung %3.
45058	Ein Anmeldecacheeintrag für Benutzer %1 war der älteste Eintrag und wurde entfernt. Der Zeitstempel dieses Eintrags lautete %2.

Ereignis-IDs: Abs. 5.1.2.2

Ereignis-ID	Nachricht
258	Listener %1 hat mit dem Abhören begonnen.
259	Listener %1 hat das Abhören beendet.
261	Listener %1 hat eine Verbindung empfangen.
262	Listener %1 wurde aufgefordert, das Abhören zu beenden.
1003	Vom Remotedesktopclient "%1" wurde eine ungültige Lizenz übermittelt.
1004	Vom Remotedesktop-Hostserver kann keine Clientlizenz erteilt werden. Die Clientlizenz konnte wegen einer geänderten (nicht übereinstimmenden) Clientlizenz, unzureichendem Arbeitsspeicher oder einem internen Fehler nicht erteilt werden. Weitere Informationen über diesen Fehler wurden möglicherweise auf dem Clientcomputer berichtet.
1011	Die Remotesitzung konnte vom Remotedesktopclient "%1" aus nicht erstellt werden, da dessen temporäre Lizenz abgelaufen ist.
1136	Die Rolle für Remotedesktop-Sitzungshostserver ist nicht installiert.
1137	Die Cacheverwaltung für Roamingbenutzerprofile für Remotedesktopdienste konnte nicht gestartet werden. Fehlercode: %1
1140	Die Gruppenrichtlinieneinstellung "Gesamtgröße des Caches für Roamingbenutzerprofile begrenzen" wurde aktiviert, jedoch ist in der Cacheverwaltung für Roamingbenutzerprofile für Remotedesktopdienste ein Problem aufgetreten. Fehlercode: %1
1141	Die Gruppenrichtlinieneinstellung " Gesamtgröße des Caches für Roamingbenutzerprofile begrenzen" wurde deaktiviert, jedoch ist in der Cacheverwaltung für Roamingbenutzerprofile für Remotedesktopdienste ein Problem aufgetreten. Fehlercode: %1
1142	Die Gruppenrichtlinieneinstellung "Gesamtgröße des Caches für Roamingbenutzerprofile begrenzen" wurde aktiviert.

Ereignis-ID	Nachricht
1143	Die Gruppenrichtlinieneinstellung "Gesamtgröße des Caches für Roamingbenutzerprofil begrenzen" wurde deaktiviert.
1145	Das Roamingbenutzerprofil für den Benutzer "%1" wurde von der Cacheverwaltung für Roamingbenutzerprofile für Remotedesktopdienste gelöscht, da der Cache für Roamingbenutzerprofile den Grenzwert von %2 Gigabyte überstiegen hat.
1146	Remotedesktopdienste: Eine Remotesteuerungssitzung wurde initiiert: %1 hat eine Remotesteuerungssitzung initiiert: Benutzer: %2 Domäne: %3.
1147	Remotedesktopdienste: Die Verbindung für die Remotesteuerungssitzung wurde erfolgreich hergestellt: %1 hat eine Remotesteuerungssitzung initiiert: Benutzer: %2 Domäne: %3.
1148	Remotedesktopdienste: Fehler beim Herstellen der Verbindung für die Remotesteuerungssitzung: %1 hat eine Remotesteuerungssitzung initiiert: Benutzer: %2 Domäne: %3.
1149	Remotedesktopdienste: Die Benutzerauthentifizierung war erfolgreich: Benutzer: %1 Domäne: %2 Quellnetzwerkadresse: %3.
1151	Die Verbindung des Remotebenutzers wurde vom angemeldeten Benutzer verweigert. Benutzerkonto: %2 Domäne: %1 Quell-IP-Adresse: %3
1152	Fehler beim Erstellen der KVP-Sitzungszeichenfolge. Fehlercode "%1"
1153	Fehler beim Schreiben der KVP-Sitzungszeichenfolge. Fehlercode "%1"
1155	Der vom Remoteverbindungs-Manager ausgewählte RDP-Protokollstapel für den Kernelmodus.
1156	Der vom Remoteverbindungs-Manager ausgewählte RDP-Protokollstapel für den Benutzermodus.
20503	Spiegelungsansichtssitzung gestartet Benutzer "%1" auf Computer "%2" zeigt Benutzer "%3" an (Sitzungs-ID: %4)
20504	Spiegelungsansichtssitzung beendet Benutzer "%1" auf Computer "%2" zeigt Benutzer "%3" an (Sitzungs-ID: %4)
20506	Spiegelungssteuerungssitzung gestartet Benutzer "%1" auf Computer "%2" steuert Benutzer "%3" an (Sitzungs-ID: %4)
20507	Spiegelungssteuerungssitzung beendet Benutzer "%1" auf Computer "%2" steuert Benutzer "%3" an (Sitzungs-ID: %4)

Ereignis-ID	Nachricht
20508	Berechtigung für Ansichtsspiegelung gewährt Benutzer "%1" (Sitzungs-ID: %3) wurde die Berechtigung für Benutzer "%2" erteilt.
20509	Berechtigung für Ansichtsspiegelung verweigert Benutzer "%1" (Sitzungs-ID: %3) wurde die Berechtigung für Benutzer "%2" verweigert.
20510	Berechtigung für Steuerungsspiegelung gewährt Benutzer "%1" (Sitzungs-ID: %3) wurde die Berechtigung für Benutzer "%2" erteilt.
20511	Berechtigung für Steuerungsspiegelung verweigert Benutzer "%1" (Sitzungs-ID: %3) wurde die Berechtigung für Benutzer "%2" verweigert.
20512	Fehler bei der Spiegelungssitzung Bei Benutzer "%2" ist beim Spiegeln von Benutzer "%1" der Fehler "%3" aufgetreten. (Sitzungs-ID: %4)
20513	Fehler bei der Spiegelungssitzung Der Benutzer "%2" konnte Benutzer "%1" (Sitzungs-ID: %3) aufgrund der Richtlinieneinstellungen nicht spiegeln.
20514	Fehler bei der Spiegelungssitzung Der Benutzer "%2" konnte Benutzer "%1" (Sitzungs-ID: %3) nicht spiegeln, weil die Sitzung bereits gespiegelt wird.
20522	Spiegelungssitzung: Kopieranforderung für Zwischenablage Benutzer %1 auf Computer %2 steuert Benutzer %3 (Sitzungs-ID: %4) Zwischenablageformat: %5
20523	Die Verbindung von Listener %1 verfügt über die Terminalklasse %2.
50180	Die Remotesitzung konnte vom Remotedesktopclient "%1" aus nicht erstellt werden, da die Lizenz nicht erneuert werden konnte.
50304	Vom Remotedesktop-Virtualisierungshostserver kann keine Clientlizenz erteilt werden. Die Clientlizenz konnte wegen einer geänderten (nicht übereinstimmenden) Clientlizenz, unzureichendem Arbeitsspeicher oder einem internen Fehler nicht erteilt werden. Weitere Informationen über diesen Fehler wurden möglicherweise auf dem Clientcomputer berichtet.

Ereignis-IDs: Abs. 5.1.2.3

Ereignis-ID	Nachricht
16	Der lokale Mehrfachbenutzersitzungs-Manager konnte nicht gestartet werden. Relevanter Statuscode: %1.
17	Fehler beim Starten des Remotedesktopdiensts. Relevanter Statuscode: %1.
18	Der Remotedesktopdienst wurde aus einem unbekannten Grund heruntergefahren. Der Dienst wird in einer Minute wiederhergestellt.
19	Fehler bei der Registrierung beim Dienststeuerungs-Manager zur Statusüberwachung für den Remotedesktopdienst mit %1. Wiederholen Sie den Vorgang in 10 Minuten.
20	Fehler beim Senden der %1-Nachricht an das Windows-Videosubsystem. Der relevante Statuscode lautete %2.

Ereignis-ID	Nachricht
21	Remotedesktopdienste: Die Sitzungsanmeldung war erfolgreich: Benutzer: %1 Sitzungs-ID: %2 Quellnetzwerkadresse: %3.
22	Remotedesktopdienste: Es wurde eine Shellstartbenachrichtigung empfangen: Benutzer: %1 Sitzungs-ID: %2 Quellnetzwerkadresse: %3.
23	Remotedesktopdienste: Die Sitzungsabmeldung war erfolgreich: Benutzer: %1 Sitzungs-ID: %2.
24	Remotedesktopdienste: Die Sitzung wurde getrennt: Benutzer: %1 Sitzungs-ID: %2 Quellnetzwerkadresse: %3.
25	Remotedesktopdienste: Die erneute Verbindungsherstellung für die Sitzung war erfolgreich: Benutzer: %1 Sitzungs-ID: %2 Quellnetzwerkadresse: %3.
32	Das Plug-In "%1" wurde erfolgreich initialisiert.
33	Fehler beim Initialisieren des Plug-Ins "%1". Fehlercode: %2.
34	Von den Remotedesktopdiensten werden keine Anmeldungen akzeptiert, da Setup gerade ausgeführt wird.
35	Das Ereignis "Sitzungsänderungsbenachrichtigung", das vom Remotedesktop-Dienst gesendet wurde, konnte vom Clientprozess mit der ID "%1" nicht abgeschlossen werden. Vom Remotedesktop-Dienst werden keine Sitzungsänderungsbenachrichtigungen mehr gesendet.
36	Fehler beim Übergang von "%3" in Reaktion auf "%5". (Fehlercode: %6)
37	Ungültiger Statusübergang von "%3" in Reaktion auf "%5". (Fehlercode: %6)
39	Die Sitzung "%1" wurde von Sitzung "%2" getrennt.
40	Sitzung "%1" wurde getrennt. Ursachencode: %2
41	Sitzungsvermittlung starten: Benutzer: %1 Sitzungs-ID: %2
42	Sitzungsvermittlung beenden: Benutzer: %1 Sitzungs-ID: %2
43	Die Verarbeitung des Connect-Ereignisses für die Sitzung "%1" durch das Windows-Subsystem hat zu lange gedauert.
44	Die Verarbeitung des Disconnect-Ereignisses für die Sitzung "%1" durch das Windows-Subsystem hat zu lange gedauert.
45	Die Verarbeitung des Terminate-Ereignisses für die Sitzung "%1" durch das Windows-Subsystem hat zu lange gedauert.

Ereignis-ID	Nachricht
48	Die Verarbeitung der Anmeldungsnachricht für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
49	Die Vorbereitung der Sitzungsvermittlung für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
50	Die Verarbeitung der Verbindungsstartnachricht für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
51	Die Verarbeitung der Verbindungsbeendigungsnachricht für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
52	Die Verarbeitung der Trennungsstartnachricht für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
53	Die Verarbeitung der Trennungsbeendigungsnachricht für die Sitzung "%1" durch den Remoteverbindungs-Manager hat zu lange gedauert.
54	Der lokale Mehrbenutzersitzungs-Manager hat eine Nachricht zum Herunterfahren des Systems empfangen.
55	Das Starten der Remotedesktopdienste hat zu lange gedauert.
56	Das Herunterfahren der Remotedesktopdienste hat zu lange gedauert.
59	%s von %S(#0x%x/0x%x)
60	Die Glas-Sitzung %1 wurde mit einem Remoteprotokoll erneut verbunden. Diese Sitzung kann jetzt nur lokal oder über dasselbe Remoteprotokoll erneut verbunden werden.

Ereignis-IDs: Abs. 5.2.2.1

Ereignis-ID	Nachricht
10	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
11	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
12	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
13	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
14	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
15	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
16	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
17	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
18	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
19	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
20	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
21	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
22	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
23	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
24	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
30	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
40	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
41	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
42	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
50	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
51	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"

Ereignis-ID	Nachricht
52	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
53	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
60	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
70	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
71	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
80	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
81	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
82	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
90	Für weitere Informationen über dieses Ereignis, wenden Sie sich an den Abschnitt "Details"
256	Vom Kryptografiedienst konnte die Katalogdatenbank nicht initialisiert werden. Fehler: %1 : %2.
257	Vom Kryptografiedienst konnte die Katalogdatenbank nicht initialisiert werden. "ESENT"-Fehler: %1.
512	Vom Kryptografiedienst konnte das VSS-Sicherungsobjekt "System Writer" nicht initialisiert werden.%1.
513	Fehler beim Kryptografiedienst während der Verarbeitung des "OnIdentity()"-Aufrufobjekts "System Writer".%1.
4097	Die automatische Aktualisierung des Drittanbieterstammzertifikats wurde erfolgreich ausgeführt: Antragsteller: <%1> Sha1-Fingerabdruck: <%2>.
4098	Der automatische Aktualisierungsabruf der Drittanbieterstammlisten-CAB-Datei wurde erfolgreich ausgeführt von <%1>.
4099	Fehler bei der automatischen Aktualisierung der CAB-Datei mit Drittanbieterstammlisten von <%1>. Fehler: %2.
4100	Der automatische Aktualisierungsabruf des Drittanbieterstammzertifikats wurde erfolgreich ausgeführt von <%1>.
4101	Fehler bei der automatischen Aktualisierung des Drittanbieterstammzertifikats von <%1>. Fehler: %2.
4102	Der crypt32-Schwellenwert von %1 Ereignissen wurde erreicht. Die Protokollierung wird für %2 Minuten ausgesetzt.
4103	Der automatische Aktualisierungsabruf der Drittanbieterstammlisten-Sequenznummer wurde erfolgreich ausgeführt von <%1>.
4104	Fehler bei der automatischen Aktualisierung der Sequenznummer der Drittanbieterstammlisten von <%1>. Fehler: %2.
4105	Nicht vertrauenswürdiges Stammzertifikat:: Antragsteller: <%1> Sha1-Fingerabdruck: <%2>
4106	Teilkette:: Aussteller: <%1> Antragsteller Sha1-Fingerabdruck: <%2>
4107	Fehler beim Extrahieren der Drittanbieterstammliste aus der automatischen Aktualisierungs-CAB-Datei bei <%1>. Fehler: %2.
4108	Erfolgreiches automatisches Löschen des Zertifikats des Drittanbieters:: Antragsteller: <%1> Sha1-Fingerabdruck: <%2>.
4109	Erfolgreiche automatische Eigenschaftsaktualisierung des Stammzertifikats des Drittanbieters:: Antragsteller: <%1> Sha1-Fingerabdruck: <%2>.
4110	Fehler beim Hinzufügen des Zertifikats zu Drittanbieter-Stammzertifizierungsstellen. Fehler: %2
4111	Erfolgreiche automatische Aktualisierung der Drittanbieterstammliste mit Gültigkeitsdatum: %1.
4112	Erfolgreiche automatische Aktualisierung der unzulässigen Zertifikatliste mit Gültigkeitsdatum: %1.
4113	Automatische Aktualisierung der Pin-Regeln erfolgreich. Gültig ab: %1.

Ereignis-ID	Nachricht
4114	Der Server "%1" weist nicht erwartete Zertifikate unter der vertrauenswürdigen Stelle "<%2>" mit Fingerabdruck "%3" auf. Konflikt der Pin-Regeln für Domäne "%4" mit Gültigkeitsdatum "%5" und Sequenznummer "%6".
4115	PKP (Public Key Pinning)-Regel für Domäne %1 mit Headerfingerabdruck %2 wurde hinzugefügt.
4116	Der Server "%1" weist nicht erwartete Zertifikate unter der vertrauenswürdigen Stelle <%2> mit Fingerabdruck %3 auf. Konflikt der PKP (Public Key Pinning)-Regel für Domäne %4, hinzugefügt am %5, Headerfingerabdruck %6. Zertifikate wurden unter <%7> gespeichert.
4117	Der Server "%1" weist nicht erwartete Zertifikate unter der vertrauenswürdigen Stelle <%2> mit Fingerabdruck %3 auf. Konflikt der PKP (Public Key Pinning)-Regel für Domäne %4, hinzugefügt am %5, Headerfingerabdruck %6. Zertifikate wurden unter <%7> gespeichert. Allerdings gab es auch eine Übereinstimmung mit Domäne %8, hinzugefügt am %9, Headerfingerabdruck %10.
4128	Die Zertifikatssperrliste wurde erfolgreich vorab aus "<%1>" abgerufen.
4129	Fehler beim Vorabrufen der Zertifikatssperrliste aus "<%1>". Fehler: %2.
4176	Fehler beim PFX-Vorgang, da AuthSafes-Anzahl außerhalb des erwarteten Bereichs liegt. Maximal zulässiger Wert: %1. Fehlerhafter Wert: %2.
4177	Fehler beim PFX-Vorgang, da die Iterationsanzahl außerhalb des erwarteten Bereichs liegt. Maximal zulässiger Wert: %1. Fehlerhafter Wert: %2.
4178	Fehler beim PFX-Vorgang, da die SafeBags-Anzahl außerhalb des erwarteten Bereichs liegt. Maximal zulässiger Wert: %1. Fehlerhafter Wert: %2.
8192	Die Katalogdatei "%2" wird dem Subsystem %1 hinzugefügt.
8193	Das Hinzufügen der Katalogdatei ist abgeschlossen. Status: %1
8194	Die Katalogdatei "%2" wird aus dem Subsystem %1 entfernt.
8195	Das Entfernen der Katalogdatei ist abgeschlossen. Status: %1.
8196	Die Katalogdatei "%2" wird mit dem Subsystem %1 synchronisiert.
8197	Die Synchronisierung der Katalogdatei ist abgeschlossen. Status: %1.
8198	Die Katalogdatenbank wird für das Subsystem %1 neu erstellt.
8199	Die Neuerstellung der Katalogdatenbank für das ausgewählte Subsystem ist abgeschlossen. Status: %1.
8200	Im Subsystem "%1" wird nach einem Hash mit Typ "%2", Länge %3 und Wert "%4" gesucht.
8201	Die Hashsuche ist abgeschlossen. Der Hash wurde in %2 Katalogen gefunden. Status: %1.
8202	Die Synchronisierung des Subsystems "%1" hat begonnen.
8203	Die Synchronisierung des Subsystems ist abgeschlossen. Status: %1.

Ereignis-IDs: Abs. 5.2.2.2

Die Nachrichten sind nicht in deutscher Sprache verfügbar.

Ereignis-ID	Nachricht
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.
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.

Ereignis-ID	Nachricht
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.
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.

Ereignis-ID	Nachricht
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.
3085	Code Integrity will disable WHQL driver enforcement for this boot session. Settings %1.

Ereignis-ID	Nachricht
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.

Ereignis-IDs: Abs. 5.2.2.3

Ereignis-ID	Nachricht
1002	Die Verarbeitung der Gruppenrichtlinie war aufgrund eines Systemzuordnungsfehlers nicht erfolgreich. Stellen Sie sicher, dass auf dem Computer ausreichend Ressourcen zur Verfügung stehen (Arbeitsspeicher, verfügbarer Festplattenspeicher). Die Gruppenrichtlinienverarbeitung wird beim nächsten Aktualisierungszyklus versucht.
1006	Fehler bei der Verarbeitung der Gruppenrichtlinie. Die Authentifizierung von Windows war für den Active Directory-Dienst auf einem Domänencontroller nicht möglich. (Fehler beim Aufruf der Funktion zur LDAP-Bindung). Den Fehlercode und eine Beschreibung finden Sie auf der Registerkarte "Details".
1007	Fehler bei der Verarbeitung der Gruppenrichtlinie. Die mit diesem Computer verknüpfte Site, die zur Gruppenrichtlinienverarbeitung erforderlich ist, konnte nicht ermittelt werden.
1030	Fehler bei der Verarbeitung der Gruppenrichtlinie. Es wurde versucht, neue Gruppenrichtlinieneinstellungen für diesen Benutzer oder Computer abzurufen. Den Fehlercode und eine Beschreibung finden Sie auf der Registerkarte "Details". Dieser Vorgang wird automatisch beim nächsten Aktualisierungszyklus wiederholt. Computer, die der Domäne beigetreten sind, müssen über eine geeignete Namensauflösung sowie über eine Netzwerkverbindung zu einem Domänencontroller zum Ermitteln von neuen Gruppenrichtlinienobjekten und -einstellungen verfügen. Wenn die Gruppenrichtlinie erfolgreich ist, wird ein Ereignis protokolliert.
1052	Die Verarbeitung der Gruppenrichtlinie ist fehlgeschlagen. Die Funktion dieses Computers konnte nicht festgestellt werden. Funktionsinformation (Arbeitsgruppe, Mitgliedsserver oder Domänencontroller) ist erforderlich um die Gruppenrichtlinie zu verarbeiten.

Ereignis-ID	Nachricht
1053	Fehler bei der Verarbeitung der Gruppenrichtlinie. Der Benutzername konnte nicht aufgelöst werden. Dies kann mindestens eine der folgenden Ursachen haben: a) Fehler bei der Namensauflösung mit dem aktuellen Domänencontroller. b) Active Directory-Replikationswartezeit (ein auf einem anderen Domänencontroller erstelltes Konto hat nicht auf dem aktuellen Domänencontroller repliziert).
1054	Fehler beim Verarbeiten der Gruppenrichtlinie. Der Name eines Domänencontrollers konnte nicht abgerufen werden. Dies kann auf einen Fehler bei der Namensauflösung zurückzuführen sein. Überprüfen Sie, ob DNS (Domain Name System) konfiguriert ist und richtig ausgeführt wird.
1055	Fehler bei der Verarbeitung der Gruppenrichtlinie. Der Computername konnte nicht aufgelöst werden. Dies kann mindestens eine der folgenden Ursachen haben: a) Fehler bei der Namensauflösung mit dem aktuellen Domänencontroller. b) Active Directory-Replikationswartezeit (ein auf einem anderen Domänencontroller erstelltes Konto hat nicht auf dem aktuellen Domänencontroller repliziert).
1058	Fehler bei der Verarbeitung der Gruppenrichtlinie. Der Versuch, die Datei "%9" von einem Domänencontroller zu lesen, war nicht erfolgreich. Die Gruppenrichtlinieneinstellungen dürfen nicht angewendet werden, bis dieses Ereignis behoben ist. Dies ist möglicherweise ein vorübergehendes Problem, das mindestens eine der folgenden Ursachen haben kann: a) Namensauflösung/Netzwerkverbindung mit dem aktuellen Domänencontroller. b) Wartezeit des Dateireplikationsdienstes (eine auf einem anderen Domänencontroller erstellte Datei hat nicht auf dem aktuellen Domänencontroller repliziert). c) Der DFS-Client (Distributed File System) wurde deaktiviert.
1065	Fehler bei der Verarbeitung der Gruppenrichtlinie. Der WMI-Filter (Windows Management Instrumentation) für das Gruppenrichtlinienobjekt "%8" konnte nicht ausgewertet werden. Dies kann darauf zurückzuführen sein, dass RSoP deaktiviert ist, oder dass der WMI-Dienst deaktiviert oder angehalten wurde, bzw. andere WMI-Fehler aufgetreten sind. Stellen Sie sicher, dass der WMI-Dienst gestartet ist und dass der Starttyp auf automatischen Start festgelegt ist. Neue Gruppenrichtlinienobjekte oder -einstellungen werden nicht verarbeitet, bis dieses Ereignis behoben wurde.
1068	Die Verarbeitung der Gruppenrichtlinie wurde unterbrochen. Das Ermitteln und Erzwingen der Gruppenrichtlinieneinstellungen wurde vorzeitig beendet, da das Herunterfahren des Computers angefordert wurde oder der Benutzer sich abgemeldet hat. Die Verarbeitung der Gruppenrichtlinie wird beim nächsten Aktualisierungszyklus, beim nächsten Computerneustart oder bei der nächsten Benutzeranmeldung wiederholt.
1079	Fehler bei der Verarbeitung der Gruppenrichtlinie. Die Liste der Gruppenrichtlinienobjekte, die auf diesen Computer oder Benutzer angewendet werden können, konnte nicht abgerufen werden. Weitere Informationen finden Sie in den Ereignisdetails.
1080	Fehler bei der Verarbeitung der Gruppenrichtlinie. Die Hierarchie der Active Directory-Organisationseinheiten konnte nicht durchsucht werden. Weitere Informationen finden Sie in den Ereignisdetails.
1085	Fehler beim Anwenden der "%8"-Einstellungen. Die "%8"-Einstellungen besitzen möglicherweise eine eigene Protokolldatei. Klicken Sie auf den Link "Weitere Informationen".
1088	Fehler bei der Verarbeitung der Gruppenrichtlinie. Beim Abfragen der Liste der Gruppenrichtlinienobjekte wurde das maximale Limit (999) überschritten.
1089	Fehler beim Aufzeichnen der RSoP-Informationen (Resultant Set of Policy), die den Bereich der Gruppenrichtlinienobjekte beschreiben, die auf den Computer oder den Benutzer angewendet wurden. Dies kann darauf zurückzuführen sein, dass RSOP deaktiviert ist oder dass der WMI-Dienst (Windows Management Instrumentation) deaktiviert oder angehalten wurde bzw. andere WMI-Fehler aufgetreten sind. Die Richtlinieneinstellungen wurden erfolgreich auf den Computer oder Benutzer angewendet. Die Meldung durch die Verwaltungstools ist möglicherweise nicht genau.

Ereignis-ID	Nachricht
1090	Fehler beim Aufzeichnen der RSoP-Informationen (Resultant Set of Policy), die den Bereich der Gruppenrichtlinienobjekte beschreiben, die auf den Computer oder den Benutzer angewendet wurden. Dies kann darauf zurückzuführen sein, dass der WMI-Dienst (Windows Management Instrumentation) deaktiviert oder angehalten wurde bzw. andere WMI-Fehler aufgetreten sind. Die Richtlinieneinstellungen wurden erfolgreich auf den Computer oder Benutzer angewendet. Die Meldung durch die Verwaltungstools ist möglicherweise nicht genau.
1091	Die RSoP-Informationen (Resultant Set of Policy) für die Gruppenrichtlinienerweiterung <%8> konnten nicht aufgezeichnet werden. Gruppenrichtlinieneinstellungen wurden erfolgreich auf den Computer oder Benutzer angewendet. Die Meldung durch die Verwaltungstools ist möglicherweise nicht genau.
1095	Fehler beim Aufzeichnen der RSoP-Informationen (Resultant Set of Policy), die den Bereich der Gruppenrichtlinienobjekte beschreiben, die auf den Computer oder den Benutzer angewendet wurden. Die Richtlinieneinstellungen wurden erfolgreich auf den Computer oder Benutzer angewendet. Die Meldung durch die Verwaltungstools ist möglicherweise nicht genau.
1096	Fehler bei der Verarbeitung der Gruppenrichtlinie. Es wurde versucht, registrierungsbasierte Richtlinieneinstellungen für das Gruppenrichtlinienobjekt "%8" zu lesen. Die Gruppenrichtlinieneinstellungen dürfen nicht erzwungen werden, bis dieses Ereignis behoben ist. Weitere Informationen über den Dateinamen und -pfad, der den Fehler verursacht hat, können den Ereignisdetails entnommen werden.
1097	Fehler bei der Verarbeitung der Gruppenrichtlinie. Das Computerkonto zum Erzwingen der Gruppenrichtlinieneinstellungen konnte nicht bestimmt werden. Dies ist möglicherweise ein vorübergehender Fehler. Gruppenrichtlinieneinstellungen, einschließlich Computerkonfiguration, werden für diesen Computer nicht erzwungen.
1101	Fehler bei der Verarbeitung der Gruppenrichtlinie. Das Verzeichnisobjekt "%8" wurde nicht gefunden. Die Gruppenrichtlinieneinstellungen dürfen nicht erzwungen werden, bis dieses Ereignis behoben ist. Weitere Informationen zu diesem Fehler können den Ereignisdetails entnommen werden.
1104	Die WMI-Filterinformationen (Windows Management Instrumentation), die mit dem Gruppenrichtlinienobjekt "%8" verknüpft sind, konnten nicht gelesen werden. Dies kann auf einen gelöschten WMI-Filter zurückzuführen sein, der in der Domäne definiert ist, die noch von Gruppenrichtlinienobjekten verwendet wird. Die Gruppenrichtlinieneinstellungen für dieses Gruppenrichtlinienobjekt werden nicht erzwungen. Andere Gruppenrichtlinienobjekte werden möglicherweise weiter angewendet. Es wird versucht, diese Informationen beim nächsten Richtlinienzyklus abzurufen. Sie können dieses spezielle Problem lösen, indem Sie alle Gruppenrichtlinienobjekte identifizieren, die auf diesen WMI-Filter verweisen, und diese Verweise entfernen. Wenden Sie sich an den Administrator, wenn dieses Ereignis über mehrere Stunden wiederholt auftritt.
1109	Das Benutzerkonto befindet sich in einer anderen Gesamtstruktur als das Computerkonto. Das Verarbeiten einer Gruppenrichtlinie aus einer anderen Gesamtstruktur ist nicht zulässig. Die Gruppenrichtlinie wird mithilfe des Loopback-Ersetzen-Modus verarbeitet. Der Bereich der Benutzerrichtlinieneinstellungen wird vom Speicherort des Computerobjekts in Active Directory bestimmt. Die Einstellungen werden von der Benutzerkonfiguration dieser Richtlinien abgerufen.
1110	Fehler bei der Verarbeitung der Gruppenrichtlinie. Es konnte nicht bestimmt werden, ob sich Benutzer- und Computerkonto in der gleichen Gesamtstruktur befinden. Stellen Sie sicher, dass der Benutzerdomänenname mit dem Namen einer vertrauenswürdigen Domäne übereinstimmt, die sich in der gleichen Gesamtstruktur wie das Computerkonto befindet.
1112	Die clientseitige Erweiterung "%8" der Gruppenrichtlinie konnte mindestens eine Einstellung nicht anwenden, da die Änderungen vor dem Systemstart oder der

Ereignis-ID	Nachricht
	Benutzeranmeldung verarbeitet werden müssen. Das System wartet vor dem nächsten Startvorgang oder der nächsten Benutzeranmeldung darauf, dass die Gruppenrichtlinienverarbeitung vollständig abgeschlossen ist. Dies kann zu einem langsamen Start und zu einer niedrigen Startleistung führen.
1125	Die Gruppenrichtlinie konnte aufgrund eines internen Systemfehlers nicht verarbeitet werden. Eine spezifische Fehlermeldung hierzu finden Sie im Betriebsprotokoll der Gruppenrichtlinie. Es wird versucht, die Gruppenrichtlinie beim nächsten Aktualisierungszyklus erneut zu verarbeiten.
1126	Es konnte nicht festgestellt werden, ob die vom Netzwerkadministrator definierten neuen Gruppenrichtlinieneinstellungen für diesen Benutzer oder Computer erzwungen werden sollen, da die Systemuhr dieses Computers nicht mit der Uhr eines der Domänencontroller für die Domäne synchronisiert ist. Aufgrund dieses Problems erfüllt dieses Computersystem möglicherweise nicht die Anforderungen des Netzwerkadministrators, und die Benutzer dieses Systems können möglicherweise einige Netzwerkfunktionen nicht nutzen. Windows versucht regelmäßig, diesen Vorgang zu wiederholen. Es ist möglich, dass die Zeiteinstellungen entweder von diesem System oder dem Domänencontroller korrigiert werden, ohne dass der Administrator eingreifen muss, und das Problem dadurch behoben wird. Wenn dieses Problem für mehr als eine Stunde weiterhin auftritt, besteht eine Möglichkeit zum Beheben des Problems darin, die Uhrzeiteinstellungen des lokalen Systems zu prüfen, um sicherzustellen, dass sie korrekt sind und mit den Uhren auf den Netzwerkdomänencontrollern synchronisiert sind. Wenn das Problem trotz Korrektur der Uhrzeiteinstellungen des lokalen Systems weiterhin besteht, kann das Problem möglicherweise nur durch einen Netzwerkadministrator behoben werden.
1127	Die Gruppenrichtlinie konnte aufgrund eines internen Systemfehlers nicht verarbeitet werden. Die spezifische Fehlermeldung hierzu finden Sie im Betriebsprotokoll der Gruppenrichtlinie. Es wird versucht, die Gruppenrichtlinie beim nächsten Aktualisierungszyklus erneut zu verarbeiten.
1128	Die clientseitige Erweiterung "%3" der Gruppenrichtlinie hat möglicherweise dazu geführt, dass der Gruppenrichtliniendienst unerwartet beendet wurde. Um weitere Fehler beim Gruppenrichtliniendienst zu vermeiden, wurde diese Erweiterung vorübergehend deaktiviert. Die Erweiterung wird erst nach dem nächsten Systemneustart wieder aktiviert. Die von dieser Erweiterung verwalteten Gruppenrichtlinieneinstellungen dürfen erst wieder nach einem Neustart des Systems erzwungen werden. Wenden Sie sich an den Lieferanten dieser Erweiterung, wenn dieses Problem erneut auftritt.
1129	Bei der Verarbeitung der Gruppenrichtlinie ist aufgrund fehlender Netzwerkkonnektivität mit einem Domänencontroller ein Fehler aufgetreten. Dies kann eine vorübergehende Bedingung sein. Es wird eine Erfolgsmeldung generiert, wenn die Verbindung des Computers mit dem Domänencontroller wiederhergestellt wurde und wenn die Gruppenrichtlinie erfolgreich verarbeitet wurde. Falls für mehrere Stunden keine Erfolgsmeldung angezeigt wird, wenden Sie sich an den Administrator.
1130	%5 war nicht erfolgreich. Name des Gruppenrichtlinienobjekts: %6 Dateisystempfad des Gruppenrichtlinienobjekts: %7 Skriptname: %8
1500	Die Gruppenrichtlinieneinstellungen für den Computer wurden erfolgreich verarbeitet. Es wurden keine Änderungen seit der letzten erfolgreichen Gruppenrichtlinienverarbeitung erkannt.

Ereignis-ID	Nachricht
1501	Die Gruppenrichtlinieneinstellungen für den Benutzer wurden erfolgreich verarbeitet. Es wurden keine Änderungen seit der letzten erfolgreichen Gruppenrichtlinienverarbeitung erkannt.
1502	Die Gruppenrichtlinieneinstellungen für den Computer wurden erfolgreich verarbeitet. Es wurden neue %6-Gruppenrichtlinienobjekte erkannt und angewendet.
1503	Die Gruppenrichtlinieneinstellungen für den Benutzer wurden erfolgreich verarbeitet. Es wurden neue %6-Gruppenrichtlinienobjekte erkannt und angewendet.
4000	Die Verarbeitung der Computerstartrichtlinie für %2 wird gestartet. Aktivitäts-ID: %1
4000	Die Verarbeitung der Computerstartrichtlinie für %2 wird gestartet. Aktivitäts-ID: %1
4001	Die Verarbeitung der Benutzeranmeldungsrichtlinie für %2 wird gestartet. Aktivitäts-ID: %1: %1
4001	Die Verarbeitung der Benutzeranmeldungsrichtlinie für %2 wird gestartet. Aktivitäts-ID: %1: %1
4002	Die Richtlinienverarbeitung wird aufgrund einer Netzwerkstatusänderung für Computer %2 gestartet. Aktivitäts-ID: %1
4002	Die Richtlinienverarbeitung wird aufgrund einer Netzwerkstatusänderung für Computer %2 gestartet. Aktivitäts-ID: %1
4003	Die Richtlinienverarbeitung wird aufgrund einer Netzwerkstatusänderung für Benutzer %2 gestartet. Aktivitäts-ID: %1
4003	Die Richtlinienverarbeitung wird aufgrund einer Netzwerkstatusänderung für Benutzer %2 gestartet. Aktivitäts-ID: %1
4004	Die manuelle Verarbeitung der Richtlinie für Computer %2 wird gestartet. Aktivitäts-ID: %1
4004	Die manuelle Verarbeitung der Richtlinie für Computer %2 wird gestartet. Aktivitäts-ID: %1
4005	Die manuelle Verarbeitung der Richtlinie für Benutzer %2 wird gestartet. Aktivitäts-ID: %1
4005	Die manuelle Verarbeitung der Richtlinie für Benutzer %2 wird gestartet. Aktivitäts-ID: %1
4006	Die regelmäßige Richtlinienverarbeitung für Computer %2 wird gestartet. Aktivitäts-ID: %1
4006	Die regelmäßige Richtlinienverarbeitung für Computer %2 wird gestartet. Aktivitäts-ID: %1
4007	Die regelmäßige Richtlinienverarbeitung für Benutzer %2 wird gestartet. Aktivitäts-ID: %1
4007	Die regelmäßige Richtlinienverarbeitung für Benutzer %2 wird gestartet. Aktivitäts-ID: %1
4017	%1 %2
4018	%2 für %1 wird gestartet
4019	Das Skript mit dem Namen %1 wird ausgeführt.
4115	Der Gruppenrichtliniendienst wurde gestartet.
4116	Die Initialisierungsphase des Gruppenrichtliniendiensts wurde gestartet.
4117	Die Gruppenrichtliniensitzung wurde gestartet.

Ereignis-ID	Nachricht
4126	Die Gruppenrichtlinie empfängt anwendbare Gruppenrichtlinienobjekte vom Domänencontroller.
4216	Das Speichern von Richtlinien im lokalen Datenspeicher wird gestartet.
4217	Das Laden von Richtlinien aus dem lokalen Datenspeicher wird gestartet.
4218	Die erste WMI-Abfrage für die Richtlinie wird gestartet.
4257	Das Herunterladen von Richtlinien wird gestartet.
4326	Die Gruppenrichtlinie versucht, Domänencontrollerinformationen zu ermitteln.
5016	Die Verarbeitung der %3-Erweiterung wurde in %1 Millisekunden abgeschlossen.
5017	%3 %4 Der Aufruf wurde in %1 Millisekunden abgeschlossen.
5018	%4 wurde für %3 in %1 Sekunden abgeschlossen.
5019	%3 in %1 Sekunde(n) abgeschlossen
5115	Der Gruppenrichtliniendienst wurde beendet.
5116	Die Initialisierungsphase des Gruppenrichtliniendiensts wurde erfolgreich abgeschlossen.
5117	Die Gruppenrichtliniensitzung wurde erfolgreich abgeschlossen.
5126	Die Gruppenrichtlinie hat anwendbare Gruppenrichtlinienobjekte vom Domänencontroller erhalten.
5216	Die Richtlinien wurden erfolgreich im lokalen Datenspeicher gespeichert.
5217	Die Richtlinien wurden erfolgreich aus dem lokalen Datenspeicher geladen.
5218	Die erste WMI-Abfrage wurde erfolgreich abgeschlossen.
5257	Das Herunterladen von Richtlinien wurde erfolgreich abgeschlossen.
5308	Domänencontrollerdetails: Domänencontrollername: %1 Domänencontroller-IP-Adresse: %2
5309	Computerdetails: Computerrolle: %1 Netzwerkname: %2
5310	Kontodetails: Kontoname: %1 Kontodomänenname: %2 DC-Name: %3 DC-Domänenname: %4
5311	Der Loopback-Richtlinienverarbeitungsmodus ist %1.
5312	Liste der anwendbaren Gruppenrichtlinienobjekte: %1
5313	Die folgenden Gruppenrichtlinienobjekte wurden nicht angewendet, da sie herausgefiltert wurden: %1
5314	Eine %6-Verbindung wurde erkannt. Die geschätzte Bandbreite ist %1 KBit/s. Der Schwellenwert der langsamen Verbindung ist %3 KBit/s.
5315	Die nächste Richtlinienverarbeitung für %1 wird in %2 %3 versucht.
5320	%1
5321	%1 Parameter: %2
5322	Die Gruppenrichtlinie hat beim Computerstart %3 Millisekunden lang auf das Netzwerksubsystem gewartet.
5323	Ungültige Fehlermeldung.

Ereignis-ID	Nachricht
5324	Die Gruppenrichtlinie hat die Benachrichtigung %1 von Winlogon für Sitzung %2 empfangen.
5325	Die Gruppenrichtlinie hat die Benachrichtigung %1 vom Service Control Manager (SCM) empfangen.
5326	Die Gruppenrichtlinie hat den Domänencontroller erfolgreich in %1 Millisekunden ermittelt.
5327	Geschätzte Netzwerkbandbreite einer der Verbindungen: %1 KBit/s.
5331	Es wurde versucht, die Dienstkonfiguration auf einen eigenständigen Dienst zu aktualisieren, da die Gruppenrichtlinienclient-Erweiterung "%1" vorhanden ist, die nicht Teil des Betriebssystems ist. Dieser Vorgang wurde mit Status "%3" beendet.
5332	Die Gruppenrichtlinie hat beim Computerstart %3 Millisekunden lang auf die CorpNet-Konnektivität für DirectAccess gewartet.
5340	Der Verarbeitungsmodus für Gruppenrichtlinien ist "%1".
5351	Die Gruppenrichtliniensitzung ist zur Windows-Anmeldung zurückgekehrt.
6000	Ungültige Fehlermeldung.
6001	Ungültige Fehlermeldung.
6002	Ungültige Fehlermeldung.
6003	Ungültige Fehlermeldung.
6004	Ungültige Fehlermeldung.
6005	Ungültige Fehlermeldung.
6006	Ungültige Fehlermeldung.
6007	Ungültige Fehlermeldung.
6016	Die Verarbeitung der %3-Erweiterung wurde in %1 Millisekunden abgeschlossen.
6017	Ungültige Fehlermeldung.
6018	Ungültige Fehlermeldung.
6019	Ungültige Fehlermeldung.
6033	Wegen der clientseitigen Verarbeitungsregeln für die Gruppenrichtlinie wurde die %1-Erweiterung übersprungen. Weitere Informationen finden Sie im RSoP-Bericht (Resultant Set of Policy).
6034	Die Gruppenrichtlinie wurde auf der Grundlage der Erkennung langsamer Verbindungen von der synchronen Vordergrundverarbeitung auf die asynchrone Vordergrundverarbeitung festgelegt.
6035	Die Verarbeitung wurde von der Erweiterung "%1" bis zur nächsten synchronen Vordergrundverarbeitung zurückgestellt. Weitere Informationen finden Sie in einem Ergebnissatz des Richtlinienberichts.
6226	Ungültige Fehlermeldung.
6308	Ungültige Fehlermeldung.
6309	Ungültige Fehlermeldung.
6310	Ungültige Fehlermeldung.
6311	Ungültige Fehlermeldung.
6312	Ungültige Fehlermeldung.
6313	Ungültige Fehlermeldung.
6314	Fehler beim Schätzen der Bandbreite der Gruppenrichtlinie. Die Verarbeitung der Gruppenrichtlinie wird fortgesetzt. Es wird eine %6-Verbindung angenommen.
6315	Ungültige Fehlermeldung.
6320	Warnung: %1 Warnungscode %2.
6321	Warnung: %1 Parameter: %3: Warnungscode %2.
6322	Ungültige Fehlermeldung.

Ereignis-ID	Nachricht
6323	Die Gruppenrichtlinienabhängigkeiten (%1) konnten nicht gestartet werden. Die netzwerkbezogenen Features der Gruppenrichtlinien [Schätzung der Bandweite und Antwort auf Netzwerkveränderungen] funktionieren daher nicht.
6324	Ungültige Fehlermeldung.
6325	Ungültige Fehlermeldung.
6326	Ungültige Fehlermeldung.
6327	Ungültige Fehlermeldung.
6330	Es wurde ein nicht beendeter Aufruf der clientseitigen Erweiterung "%1" der Gruppenrichtlinie aus einer vorherigen Instanz des Gruppenrichtliniendiensts erkannt. Dies kann darauf hinweisen, dass der Gruppenrichtlinienclient-Dienst durch die Erweiterung unerwartet beendet wurde.
6331	Ungültige Fehlermeldung.
6332	Ungültige Fehlermeldung.
6337	Die Netzwerkverbindung der Gruppenrichtlinie wurde per Direktzugriff hergestellt.
6338	Die Berichterstellung für den Windows-Anmeldungsstatus der Gruppenrichtlinie wurde abgeschlossen.
6339	Die Behandlung der Startshell für die Windows-Anmeldung der Gruppenrichtlinie wurde abgeschlossen.
6341	Die Erkennung von schnellen/langsamen Verbindungen wurde mit einer Gruppenrichtlinieneinstellung außer Kraft gesetzt.
6342	Die Netzwerkverbindung verwendet ein WWAN-Gerät für Konnektivität.
6344	Die Gruppenrichtlinie hat während der Verarbeitung im synchronen Modus eine langsame Verbindung erkannt.
6345	Bei der Domänencontrollerverbindung ist während des Prozesses im synchronen Modus der Gruppenrichtlinie eine Zeitüberschreitung aufgetreten.
6346	Die Gruppenrichtlinie ist vom Prozess im synchronen Modus in den asynchronen Modus gewechselt.
7000	Fehler bei der Verarbeitung der Computerstartrichtlinie für %3 in %1 Sekunden.
7000	Fehler bei der Verarbeitung der Computerstartrichtlinie für %3 in %1 Sekunden.
7001	Fehler bei der Verarbeitung der Benutzeranmeldungsrichtlinie für %3 in %1 Sekunden.
7001	Fehler bei der Verarbeitung der Benutzeranmeldungsrichtlinie für %3 in %1 Sekunden.
7002	Fehler bei der Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Computer %3 in %1 Sekunden.
7002	Fehler bei der Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Computer %3 in %1 Sekunden.
7003	Fehler bei der Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Benutzer %3 in %1 Sekunden.
7003	Fehler bei der Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Benutzer %3 in %1 Sekunden.
7004	Fehler bei der manuellen Verarbeitung der Richtlinie für Computer %3 in %1 Sekunden.
7004	Fehler bei der manuellen Verarbeitung der Richtlinie für Computer %3 in %1 Sekunden.
7005	Fehler bei der manuellen Verarbeitung der Richtlinie für Benutzer %3 in %1 Sekunden.
7005	Fehler bei der manuellen Verarbeitung der Richtlinie für Benutzer %3 in %1 Sekunden.
7006	Fehler bei der regelmäßigen Verarbeitung der Richtlinie für Computer %3 in %1 Sekunden.
7006	Fehler bei der regelmäßigen Verarbeitung der Richtlinie für Computer %3 in %1 Sekunden.
7007	Fehler bei der regelmäßigen Verarbeitung der Richtlinie für Benutzer %3 in %1 Sekunden.
7007	Fehler bei der regelmäßigen Verarbeitung der Richtlinie für Benutzer %3 in %1 Sekunden.
7016	Die Verarbeitung der %3-Erweiterung wurde in %1 Millisekunden abgeschlossen.
7017	%3 %4

Ereignis-ID	Nachricht
	Fehler beim Aufruf nach %1 Millisekunden.
7018	Skript für %3 in %1 Sekunde(n) fehlgeschlagen
7019	Ungültige Fehlermeldung.
7117	Die Gruppenrichtliniensitzung wurde mit einem Fehler abgeschlossen.
7126	Die Gruppenrichtlinie konnte keine anwendbaren Gruppenrichtlinienobjekte vom Domänencontroller abrufen.
7216	Fehler beim Speichern von Richtlinien im lokalen Datenspeicher.
7217	Fehler beim Laden vorn Richtlinien aus dem lokalen Datenspeicher.
7257	Fehler beim Herunterladen von Richtlinien.
7308	Ungültige Fehlermeldung.
7309	Ungültige Fehlermeldung.
7310	Ungültige Fehlermeldung.
7311	Ungültige Fehlermeldung.
7312	Ungültige Fehlermeldung.
7313	Ungültige Fehlermeldung.
7314	Ungültige Fehlermeldung.
7315	Ungültige Fehlermeldung.
7320	Fehler: %1 Fehlercode %2.
7321	Fehler: %1 Parameter: %3: Fehlercode %2.
7322	Ungültige Fehlermeldung.
7323	Ungültige Fehlermeldung.
7324	Ungültige Fehlermeldung.
7325	Ungültige Fehlermeldung.
7326	Die Gruppenrichtlinie konnte die Domänencontrollerdetails nicht in %1 Millisekunden ermitteln.
7327	Ungültige Fehlermeldung.
7331	Es wurde versucht, die Dienstkonfiguration auf einen eigenständigen Dienst zu aktualisieren, da die Gruppenrichtlinienclient-Erweiterung "%1" vorhanden ist, die nicht Teil des Betriebssystems ist. Dieser Vorgang wurde mit Status "%3" beendet.
7332	Ungültige Fehlermeldung.
8000	Die Verarbeitung der Computerstartrichtlinie für %3 wurde in %1 Sekunden abgeschlossen.
8000	Die Verarbeitung der Computerstartrichtlinie für %3 wurde in %1 Sekunden abgeschlossen.
8001	Die Verarbeitung der Benutzeranmeldungsrichtlinie für %3 wurde in %1 Sekunden abgeschlossen.
8001	Die Verarbeitung der Benutzeranmeldungsrichtlinie für %3 wurde in %1 Sekunden abgeschlossen.
8002	Die Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Computer %3 wurde in %1 Sekunden abgeschlossen.
8002	Die Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Computer %3 wurde in %1 Sekunden abgeschlossen.
8003	Die Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Benutzer %3 wurde in %1 Sekunden abgeschlossen.
8003	Die Richtlinienverarbeitung aufgrund einer Netzwerkstatusänderung für Benutzer %3 wurde in %1 Sekunden abgeschlossen.
8004	Die manuelle Verarbeitung der Richtlinie für Computer %3 wurde in %1 Sekunden abgeschlossen.
8004	Die manuelle Verarbeitung der Richtlinie für Computer %3 wurde in %1 Sekunden abgeschlossen.
8005	Die manuelle Verarbeitung der Richtlinie für Benutzer %3 wurde in %1 Sekunden abgeschlossen.

Ereignis-ID	Nachricht
8005	Die manuelle Verarbeitung der Richtlinie für Benutzer %3 wurde in %1 Sekunden abgeschlossen.
8006	Die regelmäßige Richtlinienverarbeitung für Computer %3 wurde in %1 Sekunden abgeschlossen.
8006	Die regelmäßige Richtlinienverarbeitung für Computer %3 wurde in %1 Sekunden abgeschlossen.
8007	Die regelmäßige Richtlinienverarbeitung für Benutzer %3 wurde in %1 Sekunden abgeschlossen.
8007	Die regelmäßige Richtlinienverarbeitung für Benutzer %3 wurde in %1 Sekunden abgeschlossen.
8016	Die Erweiterung "%1" (%2) fordert einen Prozess im synchronen Modus an.
9001	Dieser Computer ist so konfiguriert, dass Gruppenrichtliniendateien auf unsichere Weise aus einer Dateifreigabe abgerufen werden.

Ereignis-IDs: Abs. 5.2.2.4

Die Nachrichten sind nicht in deutscher Sprache verfügbar.

Ereignis-ID	Nachricht
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 stellt für diese Ereignis-ID keine Nachricht bereit>*
206	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
207	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
208	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
209	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
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
219	Fehler beim Laden des Treibers %5 für das Gerät %2.
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
225	Die Anwendung %3 mit der Prozess-ID %1 hat das Entfernen oder Auswerfen für das Gerät %5 beendet.

Ereignis-ID	Nachricht
226	Begin calling driver initialization routine for driver %2
227	End calling driver initialization routine for driver %2. Status: %3
228	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
229	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
230	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
231	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
232	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
233	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
234	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
235	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
236	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
240	Ein Vorgang zum Ersetzen einer Partitionseinheit wurde initiiert.
241	Fehler bei einem Vorgang zum Ersetzen einer Partitionseinheit.
241	Fehler bei einem Vorgang zum Ersetzen einer Partitionseinheit.
242	Eine Partitionseinheit wurde erfolgreich ersetzt.
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
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 stellt für diese Ereignis-ID keine Nachricht bereit>*
277	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
278	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
300	Begin starting initialization of drivers
301	End starting initialization of drivers
400	Das Gerät %1 wurde konfiguriert. Treibername: %2 Klassen-GUID: %3 Treiberdatum: %4 Treiberversion: %5 Treiberanbieter: %6 Treiberabschnitt: %8 Treiberrang: %9 Passende Geräte-ID: %10 Treiber mit niedrigerem Rang: %11 Gerät wurde aktualisiert: %12 Übergeordnetes Gerät: %14

Ereignis-ID	Nachricht
401	Fehler bei der Konfiguration des Geräts %1. Treibername: %2 Klassen-GUID: %3 Treiberdatum: %4 Treiberversion: %5 Treiberanbieter: %6 Treiberabschnitt: %8 Treiberrang: %9 Passende Geräte-ID: %10 Treiber mit niedrigerem Rang: %11 Gerät wurde aktualisiert: %12 Status: %13 Übergeordnetes Gerät: %14
402	Die Konfiguration des Geräts %1 wurde durch eine Richtlinie blockiert. Treibername: %2 Klassen-GUID: %3 Treiberdatum: %4 Treiberversion: %5 Treiberanbieter: %6 Treiberabschnitt: %8 Treiberrang: %9 Passende Geräte-ID: %10 Treiber mit niedrigerem Rang: %11 Gerät wurde aktualisiert: %12 Status: %13 Übergeordnetes Gerät: %14
403	Für das Gerät %1 muss ein Systemneustart ausgeführt werden, um die Konfiguration abzuschließen. Treibername: %2 Klassen-GUID: %3 Treiberdatum: %4 Treiberversion: %5 Treiberanbieter: %6 Treiberabschnitt: %8 Treiberrang: %9 Passende Geräte-ID: %10 Treiber mit niedrigerem Rang: %11 Gerät wurde aktualisiert: %12 Status: %13 Übergeordnetes Gerät: %14
410	Das Gerät %1 wurde gestartet. Treibername: %2 Klassen-GUID: %3 Dienst: %4 Untere Filter: %5 Obere Filter: %6
411	Beim Start des Geräts %1 ist ein Problem aufgetreten.

Ereignis-ID	Nachricht
	Treibername: %2 Klassen-GUID: %3 Dienst: %4 Untere Filter: %5 Obere Filter: %6 Problem: %7 Problemstatus: %8
412	Für das Gerät %1 muss ein Systemneustart ausgeführt werden, bevor es gestartet werden kann. Treibername: %2 Klassen-GUID: %3 Dienst: %4 Untere Filter: %5 Obere Filter: %6 Problem: %7 Problemstatus: %8
420	Das Gerät %1 wurde gelöscht. Klassen-GUID: %2
421	Das Gerät %1 konnte nicht gelöscht werden. Klassen-GUID: %2 Problem: %3 Status: %4
430	Das Gerät "%1" erfordert weitere Installationen.
440	Das Gerät "%1" wurde migriert. ID der letzten Gerätinstanz: %2 Klassen-GUID: %3 Speicherortpfad: %4 Migrationsrang: %5 Vorhanden: %6
441	Das Gerät "%1" konnte nicht migriert werden. ID der letzten Geräteinstanz: %2 Klassen-GUID: %3 Speicherortpfad: %4 Migrationsrang: %5 Vorhanden: %6 Status: %7
442	Das Gerät %1 wurde aufgrund einer teilweisen oder mehrdeutigen Übereinstimmung nicht migriert. ID der letzten Geräteinstanz: %2 Klassen-GUID: %3 Speicherortpfad: %4 Migrationsrang: %5 Vorhanden: %6 Status: %7

Ereignis-ID	Nachricht
500	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
501	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
502	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
503	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
600	A start type override of %3 was set for driver %2 in hardware configuration %1
700	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
701	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
702	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
703	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
704	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
705	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
800	Begin processing new device (%1)
801	Processing device %2 (%1)
802	End processing new device (%1)
803	Verarbeitung von Phase %1 des Starts von Gerät "%2" beginnen
804	Verarbeitung von Phase %1 des Starts von Gerät "%2" beenden
805	Verarbeitung von Phase %1 des Neustarts von Gerät "%2" beginnen
806	Verarbeitung von Phase %1 des Neustarts von Gerät "%2" beenden
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 stellt für diese Ereignis-ID keine Nachricht bereit>*
820	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
821	*<Wevtutil stellt für diese Ereignis-ID keine Nachricht bereit>*
830	Removal of %1 has been queued.
831	Begin removal of %1.
832	End removal of %1.
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.

Ereignis-IDs: Abs. 5.2.2.5

Ereignis-ID	Nachricht
100	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" für den Benutzer "%2" gestartet.
101	Die Aufgabenplanung konnte die Aufgabe "%1" für den Benutzer "%2" nicht starten. Zusätzliche Daten: Fehlerwert: %3

Ereignis-ID	Nachricht
102	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" für den Benutzer "%2" erfolgreich fertig gestellt.
103	Die Aufgabenplanung konnte die Instanz "%2" der Aufgabe "%1" für den Benutzer "%3" nicht starten. Zusätzliche Daten: Fehlerwert: %4
104	Die Aufgabenplanung konnte die Anmeldung an "%1" nicht ausführen. Der Fehler ist in "%2" aufgetreten. Benutzeraktion: Vergewissern Sie sich, dass die Anmeldeinformationen für die Aufgabe richtig angegeben wurden. Zusätzliche Daten: Fehlerwert: %3
105	Die Aufgabenplanung konnte die Identität von "%1" nicht annehmen. Zusätzliche Daten: Fehlerwert: %2
106	Die Aufgabe "%1" wurde vom Benutzer "%2" registriert.
107	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" aufgrund einer Zeitauslöserbedingung gestartet.
108	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" gemäß eines Ereignisauslösers gestartet.
109	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" gemäß eines Registrierungsauslösers gestartet.
110	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" für den Benutzer "%3" gestartet.
111	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" beendet.
112	Die Aufgabenplanung konnte die Aufgabe "%1" nicht starten, weil das Netzwerk nicht verfügbar war. Benutzeraktion: Stellen Sie sicher, dass der Computer mit dem in der Aufgabe angegebenen Netzwerk verbunden ist. Entfernen Sie die Netzwerkbedingung aus der Aufgabenkonfiguration, wenn die Aufgabe das Vorhandensein eines Netzwerks nicht erfordert.
113	Die Aufgabe "%1" ist registriert, wird aber nicht von allen angegebenen Triggern gestartet. Benutzeraktion: Stellen Sie sicher, dass alle Aufgabentrigger gültig konfiguriert sind. Zusätzliche Daten: Fehlerwert: %2
114	Die Aufgabenplanung konnte die Aufgabe "%1" nicht wie geplant starten. Die Instanz "%2" wird jetzt entsprechend der Konfigurationsoption gestartet (Start der Aufgabe bei Verfügbarkeit, wenn der Plan nicht eingehalten wurden).
115	Die Aufgabenplanung konnte eine Transaktion beim Aktualisieren oder Löschen einer der Aufgabe nicht zurücksetzen. Zusätzliche Daten: Fehlerwert: %1
116	Die Aufgabenplanung hat die Konfiguration für die Aufgabe "%1" überprüft, es konnten jedoch keine Anmeldeinformationen gespeichert werden. Benutzeraktion: Registrieren Sie die Aufgabe erneut, und stellen Sie dabei sicher, dass die Anmeldeinformationen richtig sind. Zusätzliche Daten: Fehlerwert: %2
117	Die Aufgabenplanung konnte die Instanz "%2" der Aufgabe "%1" aufgrund einer Leerlaufbedingung nicht starten.
118	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" aufgrund eines Systemstarts gestartet.
119	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" aufgrund der Anmeldung des Benutzers "%2" gestartet.
120	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" eine Verbindung mit dem Konsolentrigger hergestellt hat.
121	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" die Verbindung mit dem Konsolentrigger getrennt hat.
122	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" eine Remoteverbindung mit dem Trigger hergestellt hat.
123	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" die Remoteverbindung mit dem Trigger getrennt hat.

Ereignis-ID	Nachricht
124	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" den Computertrigger gesperrt hat.
125	Die Aufgabenplanung hat die Instanz "%3" der Aufgabe "%1" gestartet, weil der Benutzer "%2" den Computertrigger entsperrt hat.
126	Die Aufgabenplanung konnte die Aufgabe "%1" nicht ausführen. Ein Neustart wird ausgeführt. Zusätzliche Daten: Fehlerwert: %2
127	Die Aufgabenplanung konnte die Aufgabe "%1" aufgrund einer Racebedingung beim Herunterfahren nicht ausführen. Ein Neustart wird ausgeführt.
128	Die Aufgabenplanung hat die Aufgabe "%1" nicht gestartet, weil die aktuelle Uhrzeit nach der konfigurierten Aufgabenendzeit liegt. Benutzeraktion: Verlängern Sie ggf. die Endzeit für die Aufgabe.
129	Die Aufgabenplanung hat die Aufgabe "%1", Instanz "%2" mit der Prozess-ID %3 gestartet.
130	Die Aufgabenplanung konnte die Aufgabe "%1" nicht starten, weil der Dienst ausgelastet ist.
131	Die Aufgabenplanung konnte die Aufgabe "%1" nicht starten, weil die Anzahl von Aufgaben in der Aufgabenwarteschlange das derzeit konfigurierte Kontingent von %2 überschreitet. Benutzeraktion: Reduzieren Sie die Anzahl von ausgeführten Aufgaben, oder erhöhen Sie das konfigurierte Warteschlangenkontingent.
132	Die Aufgabe, durch die das Warteschlangenkontingent gestartet wurde, hat das voreingestellte Aufgabenlimit von momentan %1 fast erreicht. Benutzeraktion: Reduzieren Sie die Anzahl der ausgeführten Aufgaben, oder erhöhen Sie das konfigurierte Warteschlangenkontingent.
133	Die Aufgabenplanung konnte die Aufgabe "%1" im Aufgabenmodul "%2" für den Benutzer "%3" nicht starten. Benutzeraktion: Reduzieren Sie die Anzahl ausgeführter Aufgaben im angegebenen Benutzerkontext.
134	Das Aufgabenmodul "%1" für den Benutzer "%2" hat das voreingestellte Aufgabenlimit fast erreicht. Benutzeraktion: Reduzieren Sie die Anzahl ausgeführter Aufgaben im angegebenen Benutzerkontext.
135	Die Aufgabenplanung konnte die Aufgabe "%1" nicht starten, da der Computer nicht im Leerlauf war.
140	Die Aufgabe "%1" wurde vom Benutzer "%2" aktualisiert.
141	Die Aufgabe "%1" wurde vom Benutzer "%2" gelöscht.
142	Die Aufgabe "%1" wurde vom Benutzer "%2" deaktiviert.
145	Die Aufgabenplanung hat den Computer zur Ausführung einer Aufgabe aktiviert.
146	Aufgabe "%1" konnte vom Aufgabenplanungsdienst beim Start nicht geladen werden. Zusätzliche Daten: Fehlerwert: %2.
147	Das Abbild der Aufgabe "%1" konnte nach einer Beschädigung, die bei einem Betriebssystemupgrade aufgetreten ist, von der Aufgabenplanung werden.
148	Das Abbild der Aufgabe "%1" konnte nach einer Beschädigung, die bei einem Betriebssystemupgrade aufgetreten ist, von der Aufgabenplanung nicht wiederhergestellt werden. Zusätzliche Daten: Fehlerwert: 0x%2.
149	Von der Aufgabe "%1" wird eine Kombination von Eigenschaften verwendet, die mit dem Planungsmodul nicht kompatibel ist.
150	Die Aufgabenplanung konnte den Ereignisauslöser für die Aufgabe "%1" nicht abonnieren. Zusätzliche Daten: Fehlerwert: %2.
151	Fehler bei der Aufgabeninstanziierung: %1. Prüfpunkt: %2. Fehlerwert: %3.
152	Die Aufgabe "%1" wurde an ein Legacyplanungsmodul umgeleitet.
153	Von der Aufgabenplanung wurde die Aufgabe "%1" nicht gestartet, da der Zeitplan nicht ausgeführt wurde. Verwenden Sie ggf. die Konfigurationsoption zum Starten der Aufgabe, wenn der Zeitplan nicht ausgeführt wurde.

Ereignis-ID	Nachricht
155	Die Aufgabenplanung wartet derzeit auf die Fertigstellung der Aufgabe "%1".
200	Die Aufgabenplanung hat die Aktion "%2" in der Instanz "%3" der Aufgabe "%1" gestartet.
200	Die Aufgabenplanung hat die Aktion "%2" in der Instanz "%3" der Aufgabe "%1" gestartet.
201	Die Aufgabenplanung hat die Aufgabe "%1", Instanz "%3", Instanz "%3", Aktion "%2" erfolgreich abgeschlossen.
201	Die Aufgabenplanung hat die Aufgabe "%1", Instanz "%2", Aktion "%3" mit Rückgabecode %4 erfolgreich abgeschlossen.
201	Die Aufgabenplanung hat die Aufgabe "%1", Instanz "%2", Aktion "%3" mit Rückgabecode %4 erfolgreich abgeschlossen.
202	Die Aufgabenplanung konnte die Aufgabe "%1", Instanz "%2", Aktion "%3" nicht abschließen. Zusätzliche Daten: Fehlerwert: %4
202	Die Aufgabenplanung konnte die Aufgabe "%1", Instanz "%2", Aktion "%3" nicht abschließen. Zusätzliche Daten: Fehlerwert: %4
203	Die Aufgabenplanung konnte die Aktion "%3" in der Instanz "%2" der Aufgabe "%1" nicht starten. Zusätzliche Daten: Fehlerwert: %4
204	Die Aufgabenplanung konnte die auslösenden Ereigniswerte für die Aufgabe "%1" nicht abrufen. Das Ereignis wird ignoriert. Zusätzliche Daten: Fehlerwert: %2
205	Die Aufgabenplanung konnte das Muster der Ereignisse für die Aufgabe "%1" nicht zuordnen. Die Ereignisse werden ignoriert. Zusätzliche Daten: Fehlerwert: %2
300	Die Aufgabenplanung hat das Aufgabenmodul "%1" mit der Prozess-ID %2 gestartet.
301	Die Aufgabenplanung beendet das Aufgabenmodul "%1".
303	Die Aufgabenplanung beendet das Aufgabenmodul "%1" aufgrund eines Fehlers in "%2". Zusätzliche Daten: Fehlerwert: %3
304	Die Aufgabenplanung hat die Aufgabe "%1" an das Aufgabenmodul "%2" gesendet. Aufgabeninstanz-ID: "%3"
305	Die Aufgabenplanung hat die Aufgabe "%1" nicht an das Aufgabenmodul "%2" gesendet. Zusätzliche Daten: Fehlerwert: %3
306	Der Threadpool konnte die Nachricht für das Aufgabenmodul "%1" nicht verarbeiten. Zusätzliche Daten: Fehlerwert: %2
307	Die Aufgabenplanungdienst konnte die Verbindung mit dem Aufgabenmodul "%1" nicht herstellen. Zusätzliche Daten: Fehlerwert: %2
308	Die Aufgabenplanungdienst hat eine Verbindung mit dem Prozess des Aufgabenmoduls "%1" hergestellt.
309	Die Aufgaben "%1" der Aufgabenplaung sind beim Beenden des Aufgabenmoduls "%2" verwaist. Benutzeraktion: Machen Sie den von dieser Aufgabe ausgeführten Prozess im Task-Manager ausfindig, und beenden Sie ihn manuell.
310	Die Aufgabenplanung hat den Prozess des Aufgabenmoduls "%1" gestartet. Befehl="%2", Prozess-ID=%3, Thread-ID=%4
311	Die Aufgabenplanung konnte den Prozess des Aufgabenmoduls "%1" aufgrund eines Fehlers in "%3" nicht starten. Befehl="%2". Zusätzliche Daten: Fehlerwert: %4
312	Die Aufgabenplanung hat das Win32-Auftragsobjekt für das Aufgabenmodul "%1" erstellt.
313	Die Aufgabenplanungkanal mit dem Aufgabenmodul "%1" ist bereit zum Senden und Empfangen von Nachrichten.
314	Die Aufgabenplanung führt keine Aufgaben für das Aufgabenmodul "%1" aus, und der Leerlaufzeitgeber wurde gestartet.
315	Der Prozess des Aufgabenmoduls "%1" konnte keine Verbindung mit dem Aufgabenplanungsdienst herstellen. Zusätzliche Daten: Fehlerwert: %2
316	Das Aufgabenmodul "%1" konnte keine Nachricht an den Aufgabenplanungsdienst senden. Zusätzliche Daten: Fehlerwert: %2

Ereignis-ID	Nachricht
317	Die Aufgabenplanung hat den Prozess des Aufgabenmoduls "%1" gestartet.
318	Die Aufgabenplanung hat den Prozess des Aufgabenmoduls "%1" beendet.
319	Das Aufgabenmodul "%1" hat eine Nachricht vom Aufgabenplanungsdienst empfangen, in der das Starten der Aufgabe "%2" angefordert wird.
320	Das Aufgabenmodul "%1" hat eine Nachricht vom Aufgabenplanungsdienst empfangen, in der das Beenden der Aufgabe "%2" angefordert wird.
322	Die Aufgabenplanung hat die Aufgabe "%1" nicht gestartet, weil die Instanz "%2" de gleichen Aufgabe bereits ausgeführt wird.
323	Die Aufgabenplanung hat die Instanz "%1" der Aufgabe "%2" beendet, um die neue Instanz "%3" zu starten.
324	Die Aufgabenplanung hat die neue Instanz "%2" der Aufgabe "%1" in die Warteschlange eingereiht. Die Instanz wird gestartet, sobald die Instanz "%3" abgeschlossen ist.
325	Die Instanz "%2" der Aufgabe "%1" wurde von der Aufgabenplanung in die Warteschlange eingereiht.
326	Die Aufgabenplanung hat die Aufgabe "%1" nicht gestartet, weil der Computer mit Akkus betrieben wird. Benutzeraktion: Ändern Sie das entsprechende Kennzeichen in der Aufgabekonfiguration, wenn die Aufgabe im Akkubetrieb gestartet werden muss.
327	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" beendet, weil der Computer auf Akkubetrieb umschaltet.
328	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" beendet, weil der Computer sich nicht mehr im Leerlauf befindet.
329	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" aufgrund einer Überschreitung der zugeordneten Ausführungszeit (Aufgabendefinition) beendet. Benutzeraktion: Erhöhen Sie das konfigurierte Aufgabenzeitlimit, oder überprüfen Sie, ob externe Ursachen für die Verzögerung verantwortlich sind.
330	Die Aufgabenplanung hat die Instanz "%2" der Aufgabe "%1" auf Anforderung des Benutzers "%3" beendet.
331	Die Aufgabenplanung führt die Instanz "%2" der Aufgabe "%1" nach der vorgesehenen Zeitüberschreitung weiter aus, weil der Zeitüberschreitungsmechanismus nicht erstellt werden konnte. Zusätzliche Daten: Fehlerwert: %3
332	Die Aufgabenplanung hat die Aufgabe "%1" nicht gestartet, weil der Benutzer "%2" nicht angemeldet war, als die Startbedingungen erfüllt wurden. Benutzeraktion: Vergewissern Sie sich, dass der Benutzer angemeldet ist, oder ändern Sie die Aufgabendefinition, um den Start ohne Anmeldung des Benutzers zuzulassen.
333	Die Aufgabenplanung hat die Aufgabe "%1" nicht gestartet, da die Zielsitzung eine RemoteApp-Sitzung ist. Benutzeraktion: Wenn die Aufgabe in RemoteApp-Sitzungen gestartet werden muss, ändern Sie das entsprechende Kennzeichen in der Aufgabenkonfiguration.
334	Die Aufgabe "%1" wurde von der Aufgabenplanung nicht gestartet, weil die Zielsitzung eine WORKER-Sitzung ist.
400	Die Aufgabenplanungdienst wurde gestartet.
401	Die Aufgabenplanungdienst konnte aufgrund eines Fehlers in "%1" nicht gestartet werden. Zusätzliche Daten: Fehlerwert: %2
402	Die Aufgabenplanungdienst wird heruntergefahren.
403	Beim Ausführen des Aufgabenplanungsdiensts ist ein Fehler in"%1" aufgetreten. Zusätzliche Daten: Fehlerwert: %2
404	Beim Ausführen des Aufgabenplanungsdiensts ist ein RPC-Initialisierungsfehler in "%1" aufgetreten. Zusätzliche Daten: Fehlerwert: %2
405	Die Aufgabenplanungdienst konnte COM nicht initialisieren. Zusätzliche Daten: Fehlerwert: %1

Ereignis-ID	Nachricht
406	Die Aufgabenplanungdienst konnte den Anmeldeinformationsspeicher nicht initialisieren. Zusätzliche Daten: Fehlerwert: %1
407	Die Aufgabenplanungdienst konnte LSA nicht initialisieren. Zusätzliche Daten: Fehlerwert: %1
408	Die Aufgabenplanungdienst konnte das Leerlaufstatuserkennungs-Modul nicht initialisieren. Leerlaufaufgaben können nicht wie erforderlich gestartet werden Zusätzliche Daten: Fehlerwert: %1
409	Die Aufgabenplanungdienst konnte die Zeitänderungsbenachrichtigung nicht initialisieren. Aktualisierungen der Systemzeit werden möglicherweise nicht vom Dienst übernommen, und Aufgabenpläne werden nicht aktualisiert. Zusätzliche Daten: Fehlerwert: %1
410	Die Aufgabenplanungdienst konnte keinen Reaktivierungszeitgeber einstellen. Einige Aufgaben werden daher möglicherweise während einer Unterbrechung des Systems nicht ausgeführt. Zusätzliche Daten: Fehlerwert: %1
411	Die Aufgabenplanungdienst hat eine Benachrichtigung über eine Systemzeitänderung empfangen.
412	Die Aufgabenplanungdienst konnte durch den Computerstart ausgelöste Aufgaben nicht starten. Zusätzliche Daten: Fehlerwert: %1.
413	Beim Start des Aufgabenplanungsdiensts konnten Aufgaben nicht geladen werden. Zusätzliche Daten: Fehlerwert: %1.
414	Der Aufgabenplanungsdienst hat eine fehlerhafte Konfiguration in Definition %1gefunden. Zusätzliche Daten: Fehlerwert: %2.
500	Prozess-ID %2 hat die Leerlaufaufgaben-ID %1 registriert.
501	Prozess-ID %2 hat die Leerlaufaufgaben-ID %1 abgeschlossen.
502	Ausführung der Leerlaufaufgaben-ID %1 wurde gestartet.
503	Ausführung der Leerlaufaufgaben-ID %1 wurde beendet.
504	Leerlaufaufgaben-ID %1 wurde benachrichtigt, dass die ausdrückliche Verarbeitung angefordert wurde.
505	Leerlaufaufgaben-ID %1 hat eine Rückmeldung von ihrer ausdrücklichen Verarbeitungsbenachrichtigung zurückgegeben.
506	Die ausdrückliche Ausführung aller Leerlaufaufgaben wurde angefordert.
507	Die ausdrückliche Ausführung aller Leerlaufaufgaben wurde fertig gestellt.
508	Derzeit findet die ausdrückliche Ausführung aller Leerlaufaufgaben statt.
509	Energiebenachrichtigung für Leerlaufaufgabe empfangen: %1 (%2)
510	
511	
512	Leerlaufprüfpunkt: Zustand: %1; Ursache: %2.
700	Die Aufgabenplanungdienst hat das Aufgabenkompatibilitätsmodul gestartet.
701	Die Aufgabenplanungdienst konnte das Aufgabenkompatibilitätsmodul nicht starten. Unter älteren Windows-Versionen können Aufgaben möglicherweise nicht registriert werden. Zusätzliche Daten: Fehlerwert: %1
702	Die Aufgabenplanung konnte den RPC-Server zum Starten des Aufgabenkompatibilitätsmoduls nicht initialisieren Unter älteren Windows-Versionen können Aufgaben möglicherweise nicht registriert werden. Zusätzliche Daten: Fehlerwert: %1
703	Die Aufgabenplanung konnte die Netzplanungs-API zum Starten des Aufgabenkompatibilitätsmoduls nicht initialisieren. Unter älteren Windows-Versionen können Aufgaben möglicherweise nicht registriert werden. Zusätzliche Daten: Fehlerwert: %1

Ereignis-ID	Nachricht
704	Die Aufgabenplanung konnte LSA zum Starten des Aufgabenkompatibilitätsmoduls nicht initialisieren. Unter älteren Windows-Versionen können Aufgaben möglicherweise nicht registriert werden. Zusätzliche Daten: Fehlerwert: %1
705	Die Aufgabenplanung konnte die Verzeichnisüberwachung für das Aufgabenkompatibilitätsmodul nicht starten. Zusätzliche Daten: Fehlerwert: %1
706	Das Aufgabenkompatibilitätsmodul konnte die Aufgabe "%1" nicht auf den erforderlichen Status "%2" aktualisieren. Zusätzliche Daten: Fehlerwert: %3
707	Das Aufgabenkompatibilitätsmodul konnte die Aufgabe "%1" nicht löschen. Zusätzliche Daten: Fehlerwert: %2
708	DasAufgabenkompatibilitätsmodul konnte die Sicherheitsbeschreibung "%1" für die Aufgabe "%2" nicht einstellen. Zusätzliche Daten: Fehlerwert: %3
709	Das Aufgabenkompatibilitätsmodul konnte die Aufgabe "%1" nicht aktualisieren. Zusätzliche Daten: Fehlerwert: %2
710	Das Aufgabenkompatibilitätsmodul konnte vorhandene Aufgaben nicht aktualisieren. Der Upgradeversuch wird beim nächsten Start des Aufgabenplanungsdiensts wiederholt. Zusätzliche Daten: Fehlerwert: %1
711	Das Aufgabenkompatibilitätsmodul konnte das NetSchedule-Konto "%1" nicht aktualisieren. Zusätzliche Daten: Fehlerwert: %2
712	Das Aufgabenkompatibilitätsmodul konnte den vorhandenen Speicher zum Aktualisieren von Aufgaben nicht lesen. Zusätzliche Daten: Fehlerwert: %1.
713	Das Aufgabenkompatibilitätsmodul konnte die Aufgabe "%1" nicht für das Upgrade laden. Zusätzliche Daten: Fehlerwert: %2
714	Das Aufgabenkompatibilitätsmodul konnte die Aufgabe "%1" nicht für das Upgrade registrieren. Zusätzliche Daten: Fehlerwert: %2
715	Das Aufgabenkompatibilitätsmodul konnte den LSA-Speicher nicht für das Upgrade löschen. Zusätzliche Daten: Fehlerwert: %1
716	Das Aufgabenkompatibilitätsmodul konnte vorhandene geplante Aufgaben nicht aktualisieren. Zusätzliche Daten: Fehlerwert: %1
717	Das Aufgabenkompatibilitätsmodul konnte nicht feststellen, ob ein Upgrade erforderlich ist. Zusätzliche Daten: Fehlerwert: %1
718	Die Aufgabenplanung konnte den Anmeldeinformationsspeicher aus der Beta 2-Version nicht aktualisieren. Möglicherweise müssen Aufgaben, die Kennwörter erfordern, erneut registriert werden. Zusätzliche Daten: Fehlerwert: %1.
719	Aus Gründen der Leistungsoptimierung wurde die Protokollierung automatisch deaktiviert. Verwenden Sie die Ereignisanzeige, um sie wieder zu aktivieren.
800	Der Wartungszustand wurde in "%1" geändert. (Letzte Ausführung: %2).
801	Fehler beim Starten der Wartung. Zusätzliche Fehlerinformationen: %1.
802	Fehler beim Ändern der Wartungskonfiguration. Zusätzliche Fehlerinformationen: %1.
803	Auf die Aufgabe "%1" des Wartungsplanungsmoduls konnte nicht zugegriffen werden. Zusätzliche Fehlerinformationen: %2.
804	Von der Wartungsplanung wurde für die folgenden Wartungsaufgaben eine zyklische Abhängigkeit erkannt: %1.
805	Bei der Wartungsaufgabe "%1" ist die Frist abgelaufen.
806	Verarbeitungsfehler bei der Wartungsaufgabe "%1". Zusätzliche Fehlerinformationen: %2.
807	Die Wartung wurde abgeschlossen. (Starttyp: %1)
808	Von der Wartungsaufgabe "%1" wird beim nächsten regulären Wartungslauf die Reaktivierung des Computers angefordert.
809	Für %1 wurden keine ordnungsgemäßen Gruppenrichtlinieneinstellungen für den Wartungszeitplan angegeben. Die Standardeinstellungen werden verwendet.

Ereignis-ID	Nachricht
998	DEBUG! (%3:%4) "%1" fehlgeschlagen. (%2).
999	DEBUG! "%1".

Ereignis-IDs: Abs. 5.2.2.6

Ereignis-ID	Nachricht
1	Gruppenvorgangs-ID: %1; Vorgangs-ID: %2; Vorgang: %3; Clientcomputer: %4; Benutzer: %5; Clientprozess-ID: %6; Namespacename: %7
2	Anbieterinformationen für Gruppenvorgangs-ID: %1; Vorgang: %2; Anbietername: %3; Anbieter-GUID: %4; Pfad: %5
3	Stoppvorgangs-ID: %1
11	Korrelations-ID: %1; Gruppenvorgangs-ID: %2; Vorgangs-ID: %3; Vorgang: %4; Clientcomputer: %5; Benutzer: %7; Clientprozess-ID: %8; Namespacename: %9
12	Anbieterinformationen für Gruppenvorgangs-ID: %1; Vorgang: %2; Host-ID: %3; Anbietername: %4; Anbieter-GUID: %5; Pfad: %6
13	Stoppvorgangs-ID: %1; Ergebniscode: %2
14	Vorgangs-ID: %1; Vorgang: %2; Kanal: %3; Meldung: %4
15	Vorgangs-ID: %1; Vorgang: %2; Fehler-ID: %3; Fehlerkategorie: %4; Meldung: %5; Zielname: %6
16	Vorgangs-ID: %1; Vorgang: %2; Fehler-ID: %3; Meldung: %4
17	Korrelations-ID: %1; Vorgangs-ID: %2; Protokoll: %3; Vorgang: %4; Benutzer: %5; Namespace: %6
18	WMI-Ereignisse wurden verworfen. ConsumerType = %1; mögliche Ursache: %2
19	Löschvorgang für das WMI-Repository wird ausgeführt. Vorgangs-ID: %1; Vorgang: %2
20	Updatevorgang für das WMI-Repository wird ausgeführt. Vorgangs-ID: %1; Vorgang: %2; Kennzeichnungen: %3
21	WMI-Ereignisse wurden gebunden. ConsumerType = %1; mögliche Ursache: %2
22	Korrelations-ID: %1; Gruppenvorgangs-ID: %2; Vorgangs-ID: %3; Klassenname: %4; Methodenname: %5; Implementierungsklasse: %6; Clientcomputer: %7; Benutzer: %9; Clientprozess-ID: %10; Namespacename: %12
23	CorrelationId = %1; GroupOperationId = %2; OperationId = %3; Commandline= %4; CreatedProcessId = %5; ClientMachine = %6; User = %8; ClientProcessId = %9
50	Aktivitätsübertragung
100	Komponentenname: %1; Meldungsdetails: %2; Dateiname: %3

Ereignis-ID	Nachricht
101	Komponentenname: %1; Fehler-ID: %2; Fehlerdetails: %3; Dateiname: %4
5857	Der Anbieter "%1" wurde mit dem Ergebniscode "%2" gestartet. Hostprozess: %3; Prozess-ID: %4; Anbieterpfad: %5
5858	ID: %1; Clientcomputer: %2; Benutzer: %3; Clientprozess-ID: %4; Komponente: %5; Vorgang: %6; Ergebniscode: %7; mögliche Ursache: %8
5859	Namespace = %1; NotificationQuery = %2; OwnerName = %3; HostProcessID = %4; Provider= %5, queryID = %6; mögliche Ursache = %7
5860	Namespace = %1; NotificationQuery = %2; UserName = %3; ClientProcessID = %4, ClientMachine = %5; mögliche Ursache = %6
5861	Namespace = %1; Eventfilter = %2 (siehe die aktive Ereignis-ID: 5859); Consumer = %3; PossibleCause = %4

Ereignis-IDs: Abs. 5.2.2.7

Ereignis-ID	Nachricht
2	WSMan-API wird initialisiert.
3	Fehler bei der Initialisierung der WSMan-API. Fehlercode: %1
4	Initialisierung der WSMan-API wird aufgehoben.
5	Fehler beim Aufheben der Initialisierung der WSMan-API. Fehlercode: %1
6	WSMan-Sitzung wird erstellt. Verbindungszeichenfolge:%1
7	Fehler beim WSMan-Sitzungserstellungsvorgang. Fehlercode: %1
8	WSMan-Sitzung wird geschlossen.
9	Fehler beim Schließen der WSMan-Sitzung. Fehlercode: %1
10	WSMan-Sitzungsoption ("%1") - "%2" mit dem Wert ("%3") wurde erfolgreich festgelegt.
11	WSMan-Shell wird mit Ressourcen-URI "%1" und Shell-ID "%2" erstellt.
12	Fehler bei der WSMan-Shellerstellung. Fehlercode: %1
13	WSMan-Befehl wird mit Befehls-ID "%1" ausgeführt.
14	Fehler beim Ausführen des WSMan-Befehls. Fehlercode: %1
15	WSMan-Befehl wird geschlossen.
16	WSMan-Shell wird geschlossen.
28	Fehler aufgrund verweigerten Zugriffs: Der API-Aufrufer "%1" entspricht nicht dem Ersteller des Anwendungsobjekts.
29	Initialisierung der WSMan-API wurde abgeschlossen.
30	Die Initialisierung der WSMan-API wurde aufgehoben.
31	WSMan-Sitzungserstellung wurde abgeschlossen.
32	Fehler beim Festlegen der WSMan-Sitzungsoption (%1) - %2. Fehlercode: %3.
33	Die WSMan-Sitzung wurde geschlossen.
37	Fehler beim Schließen des WSMan-Shells. Fehlercode: %1
38	Fehler beim Schließen des WSMan-Befehls. Fehlercode: %1
40	Fehler beim Schließen von WSMan-Vorgang "%1". Fehlercode: %2
41	Es wurde mit dem Laden des WinRM-Protokollhandlers für die Anwendung %1 begonnen.
42	Das Entladen des WinRM-Protokollhandlers wurde abgeschlossen.
43	Der WinRM-Protokollhandler wurde wegen des folgenden Fehlers vorzeitig entladen: %2.
44	Der WinRM-Protokollhandler hat damit begonnen, am folgenden Ziel eine Sitzung zu erstellen: %1

Ereignis-ID	Nachricht
45	Der WinRM-Protokollhandler hat die Sitzung geschlossen.
46	Die WinRM-Protokollsitzung wurde wegen des folgenden Fehlers vorzeitig geschlossen: %2.
47	Die WinRM-Protokollsitzung hat auf dem Server einen Vorgang vom Typ "%1" gestartet. In dem Vorgang wird auf die Klasse "%3" unter dem Namespace "%2" zugegriffen.
48	Die WinRM-Protokollsitzung hat den Vorgang erfolgreich abgeschlossen.
49	Der WinRM-Protokollvorgang konnte wegen des folgenden Fehlers nicht ausgeführt werden: %2.
84	Die maximale zulässige Anzahl von Benutzern (%1), die Shellvorgänge ausführen, wurde überschritten. Wiederholen Sie den Vorgang später, oder erhöhen Sie die Quote für gleichzeitig aktive Shellbenutzer.
85	Der %1-Benutzer darf maximal %2 gleichzeitige Shells ausführen. Diese Zahl wurde jedoch überschritten. Schließen Sie vorhandene Shells, oder erhöhen Sie die Quote für diesen Benutzer.
86	Ein Hostprozess zur Verarbeitung der angegebenen Anforderung konnte nicht gestartet werden. Stellen Sie sicher, dass der Hostserver des WSMan-Anbieters und der Proxy ordnungsgemäß registriert sind. Fehlercode: %1
87	Der WSMan-Hostprozess wurde unerwarteterweise beendet. Fehlercode: %1
90	"RunAs" wurde durch die Gruppenrichtlinie deaktiviert. Der WSMan-Dienst hat alle "RunAs"-Anmeldeinformationen gelöscht.
91	WSMan-Shell wird mit folgender Ressourcen-URI auf dem Server erstellt: %1
131	Der Umleitungsstatuscode aus der Vermittlungsschicht wurde empfangen; Status: 302 (HTTP_STATUS_REDIRECT); Speicherort: %1
132	WSMan-Vorgang "%1" wurde abgeschlossen.
135	Die Anforderung wird aufgrund von ERROR_WINHTTP_CANNOT_CONNECT erneut gesendet. Dabei wird der nächste Proxy verwendet.
136	Die Anforderung wird aufgrund von ERROR_WINHTTP_NAME_NOT_RESOLVED erneut gesendet. Dabei wird der nächste Proxy verwendet.
137	Von der Vermittlungsschicht wurde "ERROR_WINHTTP_NAME_NOT_RESOLVED" zurückgegeben - Der Servername kann nicht aufgelöst werden. Der Vorgang wird abgebrochen.
138	Der Client empfing eine Zeitüberschreitung von der Vermittlungsschicht (ERROR_WINHTTP_TIMEOUT).
139	Der Client empfing einen Anmeldefehler von der Vermittlungsschicht (ERROR_WINHTTP_LOGIN_FAILURE).
142	Fehler bei WSMan-Vorgang "%1". Fehlercode: %2
145	Der WSMan-Vorgang "%1" wurde mit der Ressourcen-URI "%2" gestartet.
161	%1
162	Fehler beim Authentifizieren des Benutzers. Die Anmeldeinformationen wurden nicht akzeptiert.
163	Der vom Client angeforderte Authentifizierungsmechanismus (%1) wird vom Server nicht unterstützt. Mögliche vom Server gemeldete Authentifizierungsmechanismen: %2 %3 %4 %5 %6
164	Vom Zielcomputer (%1) wurde ein Fehler aufgrund verweigerten Zugriffs zurückgegeben. Überprüfen Sie, ob Ihre Anmeldeinformationen korrekt sind.
165	Der vom Proxy angeforderte Authentifizierungsmechanismus (%1) wird vom Client nicht unterstützt. Unterstützt werden nur die Authentifizierungsmechanismen: Negotiate, Basic oder Digest. Mögliche vom Proxy gemeldete Authentifizierungsmechanismen: %1 %2 %3 %4 %5

Ereignis-ID	Nachricht
171	Fehler beim Authentifizieren des Benutzers beim Proxy. Die Anmeldeinformationen funktionierten nicht.
172	Das Serverzertifikat auf dem Zielcomputer (%1:%2) enthält folgende Fehler: %3 %4 %5 %6 %7 %8 %9 %10. Beheben Sie die Fehler im Serverzertifikat, und wiederholen Sie den Vorgang.
173	Der Dienst "Windows-Remoteverwaltung" hat in den letzten %2 Minuten %1 nicht authentifizierte Verbindungen beendet, um den fehlerfreien Systemstatus aufrechtzuerhalten Wahrscheinliche Ursache hierfür ist eine Überlastung des Diensts oder eine auf Authentifizierung basierende Attacke auf den Dienst. Aktion: Aktivieren Sie das WinRM-Protokoll (Windows Remote Management, Windows-Remoteverwaltung) "Analytisch", und suchen Sie im Protokoll nach Warnereignissen mit der ID 1843. Diese Ereignisse enthalten weitere Informationen zu den Clients, die plötzlich beendet wurden.
192	Fehler bei der Autorisierung des Benutzers. Fehler: %1
193	Die Anforderung für Benutzer "%1" (%2) wird unter Verwendung des virtuellen WinRM-Kontos %3 (%4) ausgeführt.
208	Der Winrm-Dienst wird gestartet.
209	Der Winrm-Dienst wurde gestartet.
210	Der WinRM-Dienst kann aufgrund eines Initialisierungsfehlers nicht gestartet werden. Fehlercode: %1
211	Der Winrm-Dienst wird beendet.
212	Der Winrm-Dienst wurde beendet.
213	Die aktuellen Konfigurationseinstellungen konnten nicht vom WSMan-Dienst geladen werden, da die Einstellungen beschädigt sind. Der Dienst wird stattdessen mit den Standardeinstellungen gestartet. Benutzeraktion Verwenden Sie zum Wiederherstellen der Standardeinstellungen den folgenden Befehl: winrm invoke Restore winrm/config @{}
214	Die aktuellen Konfigurationseinstellungen konnten nicht vom WSMan-Client geladen werden, da die Einstellungen beschädigt sind. Der Client wird stattdessen mit den Standardeinstellungen ausgeführt. Benutzeraktion Starten Sie den WinRM-Dienst, und verwenden Sie zum Wiederherstellen der Standardeinstellungen den folgenden Befehl: winrm invoke Restore winrm/config @{}
215	Die Konfiguration des folgenden Plug-Ins konnte vom WSMan-Dienst nicht gelesen werden: %1. Empfangener Fehler: %2: %%%2 %3. Benutzeraktion Stellen Sie sicher, dass diese Plug-In-Konfiguration gültig ist.
216	Fehler im WSMan-Dienst beim Neustart der Plug-Ins, die für automatischen Neustart gekennzeichnet sind. Es wurde folgender Fehlercode empfangen: %1.
217	Fehler im WSMan-Dienst beim Neustart des %1-Plug-Ins beim Dienststart. Es wurde folgender Fehlercode empfangen: %2
218	Der WSMan-Dienst hat das folgende Plug-In beim Dienststart erfolgreich neu gestartet: %1.
219	Die WSMan-Shellinstanz "%1" unterstützt nicht länger die Funktionalität zum Trennen und Wiederherstellen von Verbindungen, weil der Client eine nicht unterstützte Anforderung gesendet hat.
224	%1
229	Fehler beim Registrieren von WinRM "%1" für Benachrichtigungen über Gruppenrichtlinienänderungen. Der Fehlercode lautet %2.
230	Das Löschen des Registrierungsschlüssels "%1" hat dazu geführt, dass der Zugriff verweigert wird. Ist dieser Registrierungseintrag nicht speziell als schreibgeschützt markiert, scheint dies ein mögliches Problem zu sein.

Ereignis-ID	Nachricht
254	Aktivitätsübertragung
255	Aktivitätsübertragung
283	Plug-In, von dem Kontext für Vorgang "%1" gemeldet wird
284	Plug-In, von dem das Datenobjekt für Vorgang "%1" gemeldet wird
285	Plug-In, von dem ein Datenobjekt und EPR für Vorgang "%1" gemeldet wird
286	Plug-In, von dem ein Datenobjekt und Lesezeichen für Vorgang "%1" gemeldet wird
287	Plug-In, von dem Daten für den Vorgang "Empfangen" gemeldet werden
288	Plug-In, von dem der Abschluss des Vorgangs für "%1" gemeldet wird
289	Plug-In, von dem Vorgangsinformationen für Parameter "%1" und Vorgang "%2" gemeldet werden
290	Plug-In, von dem gemeldet wird, dass die Autorisierung für Benutzer "%1" mit Fehlercode "%2" abgeschlossen wurde
291	Plug-In, von dem gemeldet wird, dass der Autorisierungsvorgang mit Fehler "%1" für Vorgang "%2" und Ressourcen-URI "%3" abgeschlossen wurde
292	Das Kontingent für Benutzer "%1" mit Fehlercode "%2 " wird aktualisiert. Maximal zulässige gleichzeitige Shells=%3 Maximal zulässige gleichzeitige Vorgänge=%4 Größe des Zeitrahmens=%5 Maximal zulässige Vorgänge pro Zeitrahmen=%6
306	Das folgende Plug-In wurde geladen: %1 (%2)
307	Das folgende Plug-In wurde entladen: %1 (%2)
308	"WSManPluginGetConfiguration" wurde vom Plug-In mit dem Parameter "%1" aufgerufen, und es wurde der Rückgabewert "%2" empfangen.
309	"WSManPluginReportCompletion" wurde vom Plug-In mit dem Parameter "%1" aufgerufen, und es wurde der Rückgabewert "%2" empfangen.
310	Das Plug-In "%1" wird heruntergefahren, weil es länger im Leerlauf war, als im Kontingent "HostIdleTimeoutSecs" konfiguriert ist.
311	Fehler beim Signalisieren des WSMan-Befehls. Fehlercode: %1
312	WSMan-Befehl wird signalisiert.
313	Eingabe wird an den Befehl gesendet.
314	Eingabe wird an Shell wird gesendet.
315	Fehler beim Vorgang zum Senden von Eingabe. Fehlercode: %1
316	WSMan wird aufgerufen, um Ausgabe von der Shell zu empfangen.
317	Fehler beim WSMan-Empfangsvorgang. Fehlercode: %1
318	WSMan wird aufgerufen, um Ausgabe vom Befehl zu empfangen.
319	Das Abrufen der Meldung für den Fehlercode "%1" wurde erfolgreich abgeschlossen. Der Sprachcodeparameter war: %2
320	WSMan-Sitzungsoption (%1) - %2 wird abgerufen.
321	WSMan-Shell wird signalisiert.
322	WSMan-Shell wird signalisiert. Fehlercode: %1
323	WSMan-Vorgang wird geschlossen.
324	WSMan-Vorgang "%1" wurde erfolgreich abgeschlossen.
325	Die Verbindung mit der Shell mit ID "%1" wird getrennt.
326	Fehler beim Trennen der Shell, Fehlercode "%1".
327	Die Verbindung mit der Shell mit ID "%1" wird wiederhergestellt.
328	Fehler beim Wiederherstellen der Verbindung mit der Shell, Fehlercode "%1".
329	Die Verbindung mit der Shell mit ID "%1" wird hergestellt.
330	Fehler beim Herstellen der Verbindung mit der Shell, Fehlercode "%1".

Ereignis-ID	Nachricht
331	Die Verbindung mit dem Shellbefehl mit ID "%1" wird wiederhergestellt.
332	Fehler beim Wiederherstellen der Verbindung mit dem Shellbefehl, Fehlercode "%1".
333	Die Verbindung mit dem Shellbefehl mit ID "%1" wird hergestellt.
334	Fehler beim Herstellen der Verbindung mit dem Shellbefehl, Fehlercode "%1".
512	Automatisches Erkennen von Proxyeinstellungen
513	Automatische Proxyerkennung wurde abgeschlossen. Proxyliste: %1 Umgehungsliste: %2
514	Proxyinformationen werden festgelegt Proxyliste: %1 Umgehungsliste: %2
771	SOAP [Von Client wird Index "%1" von insgesamt %2 Abschnitten gesendet (%3 Byte)] %4
772	SOAP [Von Listener wird Index "%1" von insgesamt %2 Abschnitten empfangen (%3 Byte)] %4
774	Der %1-Benutzer darf gleichzeitig bis zu %2 Vorgänge ausführen. Diese Anzahl wurde jedoch überschritten. Schließen Sie für diesen Benutzer bestehende Vorgänge, oder erhöhen Sie das Kontingent für den Benutzer.
775	Das Lastenkontingent von %1 Anforderungen pro %2 Sekunden wurde überschritten. Senden Sie künftige Anforderungen mit einer geringeren Übertragungsrate, oder erhöhen Sie das Kontingent für den %3-Benutzer. Die nächste Anforderung dieses Benutzers wird mindestens %4 Millisekunden lang nicht genehmigt.
776	Das Systemlastenkontingent von %1 Anforderungen pro %2 Sekunden wurde überschritten. Senden Sie künftige Anforderungen mit einer geringeren Übertragungsrate, oder erhöhen Sie das Systemkontingent. Die nächste Anforderung von Benutzer "%3" wird mindestens %4 Millisekunden lang nicht genehmigt.
779	SOAP [Von Client wird Index "%1" von insgesamt %2 Abschnitten gesendet (%3 Byte)] %4
780	Von WinRM "%1" wurden Probleme mit der Netzwerkkonnektivität erkannt.
781	Es wird vom WinRM-Client versucht, die Netzwerkverbindung wiederherzustellen.
782	Der WinRM-Dienst hat eine neue Netzwerkverbindung vom Client erkannt.
783	WinRM "%1" hat erfolgreich eine Netzwerkverbindung wiederhergestellt.
784	WinRM "%1" konnte keine Netzwerkverbindung wiederherstellen und protokolliert den Fehler.
785	Der WSMan-Hostprozess wurde für den Benutzer "%1" gestartet.
786	Der WSMan-Hostprozess wurde für den Benutzer "%1" beendet.
787	Die Anforderung für Vorgang "%1" wird an folgenden Zielcomputer und -port gesendet: %2:%3
788	Clientanforderung für Vorgang "%1" wird verarbeitet.
789	Das Plug-In für Vorgang "%1" mit der Ressourcen-URI <%2> wird eingegeben.
790	Das Plug-In für Vorgang "%1" wird verlassen.
791	Fehler im WinRM-Dienst beim Durchlaufen der DASH/SMASH-Spezifikationen. MI-Fehler: %1.
1025	Antwortfehlerpaket für folgende Aktions-URI wird gesendet: %1
1026	SOAP [Von Client wird Index "%1" von insgesamt %2 Abschnitten empfangen (%3 Byte)] %4
1027	SOAP [Von Listener wird Index "%1" von insgesamt %2 Abschnitten gesendet (%3 Byte)] %4
1041	Aufzählung wird heruntergefahren
1043	Abonnement wird heruntergefahren
1044	SOAP [Von Listener wird Index "%1" von insgesamt %2 Abschnitten gesendet (%3 Byte)] %4
1045	Die Antwort von der Vermittlungsschicht wurde empfangen; Status: 200 (HTTP_STATUS_OK)

Ereignis-ID	Nachricht
1046	Für den %1-Vorgang wurde das Zeitlimit für einen Rückruf für erweiterte Semantik erreicht.
1047	Antwort aus Vermittlungsschicht wurde empfangen; Status: %1
1048	Der HTTP-Fehler wird aufgrund eines Transportfehlers an den Client zurückgesendet. Der HTTP-Statuscode lautet "%1". Der Fehlercode lautet "%2".
1049	Für folgenden Vorgang wird eine Zeitlimitantwort gesendet: %1
1050	Antwort für Vorgang "%1" wird gesendet.
1051	Antwort aus Vermittlungsschicht wurde empfangen; Status: %1
1052	WSMan-Vorgang "%1" wurde abgeschlossen.
1053	Der WSMan-Vorgang "%1" wurde angehalten, weil die Verbindung mit der WSMan-Shell getrennt wurde.
1054	WSMan-Vorgang "%1" wird fortgesetzt, weil die Verbindung mit der WSMan-Shell wiederhergestellt wurde.
1291	Die Vermittlungsschichtrichtlinie für automatische Anmeldung wurde infolge einer HTTP 401-Antwort von WinHttp auf "Niedrig" festgelegt.
1292	Die Vermittlungsschichtrichtlinie für automatische Anmeldung wurde auf "Hoch" festgelegt.
1293	Der ausgewählte Authentifizierungsmechanismus ist "%1".
1294	Eine HTTP 401-Antwort wird an den Client gesendet. Die Verbindung wird nach dem Senden der Antwort getrennt.
1295	Benutzer "%1" wurde mithilfe der %2-Authentifizierung authentifiziert.
1296	Die Authentifizierung mithilfe des Clientzertifikats mit Betreff %1 wurde vorgenommen.
1297	Der Benutzer wird mithilfe des %1-Mechanismus authentifiziert.
1536	Der Benutzer wird autorisiert.
1537	Die Autorisierung des Benutzers war erfolgreich.
1840	Fehler beim Verarbeiten eines Vorgangs. Fehlercode: %1 Fehlerzeichenfolge:%2
1841	Fehler beim Verarbeiten eines Vorgangs. Fehlercode: %1
1842	Weitere Informationen: In den Angaben zu den XML-Parametern finden Sie weitere Details.
1843	Eine nicht authentifizierte Verbindung vom Client "%1" wird beendet.
2048	[Dateiname:- %1; Zeile:- %2; Funktion:- %3;] %4
2049	[Dateiname:- %1; Zeile:- %2; Funktion:- %3; Fehlercode:- %4] %5
468853	Vom WinRM-Dienst werden keine Anforderungen abgehört, da beim Abhören mindestens einer Adresse und eines Ports ein Fehler aufgetreten ist. Fehler bei der Remoteverwaltung mittels WinRM. Benutzeraktion Konfigurieren Sie die Listener, indem Sie die automatische Konfiguration von Listenern durch eine Gruppenrichtlinie ermöglichen, oder verwenden Sie das WinRM-Befehlszeilenprogramm, um einen Listener manuell zu erstellen.
468854	Vom WinRM-Dienst werden keine %1-Anforderungen abgehört, da beim Binden an die URL (%2) in HTTP.SYS ein Fehler aufgetreten ist. Ein anderer Prozess ist zum Abhören des URL-Präfixes des WinRM-Dienstes registriert. Benutzeraktion Beheben Sie das Problem, indem Sie den anderen Prozess beenden, sein URL-Präfix ändern oder die Konfiguration für die Listeningadresse der WS-Verwaltung ändern.
468855	Der WS-Verwaltungsclient lauscht auf keine gepushten Ereignisse, da ein Fehler bei der Bindung an die URL (%1) in HTTP.SYS aufgetreten ist. Ein anderer Prozess ist zum Lauschen auf das URL-Präfix des WinRM-Clients registriert. Benutzeraktion Beheben Sie dieses Problem, indem Sie den anderen Prozess anhalten und sein URL-Präfix ändern oder indem Sie die Konfiguration für die Lauschadresse der WS-Verwaltung ändern.

Ereignis-ID	Nachricht
468856	Vom WinRM-Dienst werden keine HTTP-Anforderungen abgehört, weil ein Fehler beim Binden an die URL (%1) in HTTP.SYS aufgetreten ist. An dieser URL werden keine Remoteanforderungen bedient. Benutzeraktion Verwenden Sie "netsh http", um zu überprüfen, ob die ACL für die URL (%1) auf "Network Service" festgelegt ist. Zusätzliche Daten Der von HTTP.sys empfangene Fehlercode ist %2: %%%2
468857	Vom WS-Verwaltungsclient werden keine Pushereignisse abgehört, weil ein Fehler beim Binden an die URL (%1) in HTTP.SYS aufgetreten ist. Benutzeraktion Verwenden Sie "netsh http", um zu überprüfen, ob die ACL für die URL (%1) auf "Network Service" festgelegt ist. Zusätzliche Daten Der von HTTP.sys empfangene Fehlercode ist %2: %%%2
468862	Der WinRM-Dienst kann das Clientzertifikat nicht überprüfen, da der Sperrstatus des Zertifikats oder eines Zertifikats in der Zertifikatkette entweder offline oder veraltet ist. Benutzeraktion Stellen Sie sicher, dass auf die Zertifikatssperrliste zugegriffen werden kann und dass die Zertifikatssperrliste auf dem neuesten Stand ist.
468863	Die Benutzerauthentifizierung mittels der Standardauthentifizierung war nicht möglich. Zusätzliche Daten Unerwarteter Fehler von LogonUser "%1" empfangen: %%%1.
468864	Das Clientzertifikat hat die maximale Größe überschritten, die für den WinRM-Dienst zulässig ist. Benutzeraktion Verwenden Sie ein anderes Clientzertifikat oder eine andere Authentifizierungsmethode.
468865	Fehler beim Verarbeiten einer Anforderung, weil der WinRM-Dienst eine Daten- oder Ereignisquelle nicht laden kann: DLL="%1" Benutzeraktion Prüfen Sie, ob "%1" vorhanden ist. Zusätzliche Daten Fehler "%2" (%%%2) beim Laden von "%1".
468866	Die SSL-Konfiguration für die IP-Adresse %1 und den Port %2 wird gemeinsam mit einem anderen Dienst, z. B. Internetinformationsdienste (IIS), verwendet.
468871	Der WinRM-Dienst konnte aufgrund eines Fehlers bei der Initialisierung nicht gestartet werden. Zusätzliche Daten Der Fehlercode ist %1.
468872	Der WinRM-Dienst hat eine unsichere HTTP-Verbindung von "%1" erhalten. Diese Konfiguration ist nicht sicher. Benutzeraktion Legen Sie in der WinRM-Konfiguration "AllowUnencrypted" auf "False" fest, um sicherzustellen, dass Pakete bei der Übertragung verschlüsselt werden.
468873	Die Konfiguration des WinRM-Dienstes sieht vor, dass die Standardauthentifizierung bei unsicheren HTTP-Verbindungen zulässig ist. Diese Konfiguration ist nicht sicher. Benutzeraktion Legen Sie in der WinRM-Konfiguration "AllowUnencrypted" auf "False" fest, um sicherzustellen, dass Pakete bei der Übertragung verschlüsselt werden.
468880	Vom WinRM-Dienst werden keine HTTP-Anforderungen abgehört, weil ein Fehler beim Binden an die URL (%1) in HTTP.SYS aufgetreten ist. An dieser URL werden keine Remoteanforderungen bedient. Benutzeraktion Verwenden Sie "netsh http", um zu überprüfen, ob die ACL für die URL (%1) auf "Network Service" festgelegt ist. Zusätzliche Daten Der von HTTP.sys empfangene Fehlercode ist %2: %%%2
468881	Vom WS-Verwaltungsclient werden keine Pushereignisse abgehört, weil ein Fehler beim Binden an die URL (%1) in HTTP.SYS aufgetreten ist. Benutzeraktion Verwenden Sie "netsh http", um zu überprüfen, ob die ACL für die URL (%1) auf "Network Service" festgelegt ist. Zusätzliche Daten Der von HTTP.sys empfangene Fehlercode ist %2: %%%2
468882	Der IP-Filter %1, der in der Gruppenrichtlinie für die automatische Konfiguration von Listenern angegeben wurde, ist ungültig und wird ignoriert. Aufgrund dieses Problems kann der automatisch konfigurierte Listener vom WinRM-Dienst nicht verwendet werden. Mit "*" wird angezeigt, dass der Dienst alle verfügbaren IP-Adressen auf diesem Computer abhören soll. Wenn "*" verwendet wird, können keine anderen Bereiche im Filter angegeben werden. Benutzeraktion Entfernen Sie ggf. andere IP-Bereiche wenn "*" in den IP-Filter eingeschlossen werden muss.
468883	Der IP-Bereich "%1" ist ungültig und wird ignoriert. Bereiche müssen mit der Syntax IP1-IP2 angegeben werden. Mehrere Bereiche werden durch Komma getrennt. IPv4-

Ereignis-ID	Nachricht
	Beispielbereiche: 2.0.0.1-2.0.0.20, 24.0.0.1-24.0.0.22 IPv6-Beispielbereiche: 3FFE:FFFF:7654:FEDA:1245:BA98:0000:0000-3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562 Benutzeraktion Korrigieren Sie den IP-Filter "%1", indem Sie die oben beschriebene Syntax verwenden.
468884	Vom WinRM-Dienst werden keine Richtlinienänderungen abgehört, da beim Registrieren für Änderungen am Inhalt des Richtlinienschlüssels der WS-Verwaltung ein Fehler aufgetreten ist. Gruppenrichtlinienänderungen werden nicht verarbeitet. Benutzeraktion Beenden Sie den WinRM-Dienst, und starten Sie ihn neu. Zusätzliche Daten Der Fehlercode ist %1.
468888	Vom WinRM-Dienst wurde ein schwerwiegender Sicherheitsfehler festgestellt. Der Dienst kann nicht mehr in seinem Sicherheitskontext ausgeführt werden. Benutzeraktion Beenden Sie den WinRM-Dienst, und starten Sie ihn neu. Zusätzliche Daten Der Fehlercode ist %1.
468889	Der WinRM-Dienst kann den Listener mit der IP-Adresse %1 und dem Anschluss %2 nicht migrieren, da die IP-Adresse auf dem Zielcomputer nicht vorhanden ist. Dieser Listener wurde während der Migration ignoriert. Benutzeraktion Erstellen Sie den Listener erneut mit der korrekten IP-Adresse.
468890	Der WinRM-Dienst kann den Listener mit der IP-Adresse %1 und der Transporteinstellung "%2" nicht migrieren, da die IP-Adresse %3 auf dem Zielcomputer nicht vorhanden ist. Dieser Listener wurde während der Migration ignoriert. Benutzeraktion Erstellen Sie den Listener erneut mit der korrekten IP-Adresse.
468891	Der WinRM-Dienst kann den Listener mit der IP-Adresse %1 und dem Anschluss %2 nicht migrieren, da die MAC-Adresse %3 auf dem Zielcomputer nicht vorhanden ist. Dieser Listener wurde während der Migration ignoriert. Benutzeraktion Erstellen Sie den Listener erneut mit der korrekten MAC-Adresse.
468892	Der WinRM-Dienst kann den Listener mit der IP-Adresse %1 und der Transporteinstellung "%2" nicht migrieren, da die MAC-Adresse %3 auf dem Zielcomputer nicht vorhanden ist. Dieser Listener wurde während der Migration ignoriert. Benutzeraktion Erstellen Sie den Listener erneut mit der korrekten MAC-Adresse.
468893	Der WinRM-Dienst kann den Listener mit der IP-Adresse %1, dem Anschluss %2 und der Transporteinstellung "%3" nicht migrieren. Ein Listener, für den die Adresse %4 und die Transporteinstellung "%5" konfiguriert sind, ist bereits vorhanden.
468894	Der WinRM-Dienst kann den Listener mit der Adresse %1 und der Transporteinstellung "%2" nicht migrieren. Ein Listener mit dieser Adress- und Transportkonfiguration ist bereits vorhanden.
468895	Bei der Migration ist im WinRM-Dienst ein Fehler aufgetreten. Benutzeraktion Erstellen Sie die Konfiguration mithilfe des WinRM-Befehlszeilenprogramms erneut. Zusätzliche Daten Der Fehlercode ist: %1 %%%1
468896	Beim Lesen der aktuellen Konfiguration ist im WinRM-Dienst ein Fehler aufgetreten. Der Dienst wurde beendet. Benutzeraktion Verwenden Sie die folgende Befehlszeile, um die Standardeinstellungen wiederherzustellen: winrm invoke Restore winrm/config @{} Fügen Sie dann alle gewünschten benutzerdefinierten Konfigurationseinstellungen hinzu, und starten Sie den Dienst erneut. Zusätzliche Daten Der Fehlercode ist: %1 %%%1
468897	Beim Anwenden der aktuellen Konfiguration ist ein Fehler im WinRM-Dienst aufgetreten. Der Dienst wurde beendet. Benutzeraktion Überprüfen Sie das Ereignisprotokoll im Hinblick auf zuvor protokollierte Meldungen, und starten Sie den Dienst erneut.
468898	Beim Lesen der aktuellen Konfiguration ist im WinRM-Dienst ein Fehler aufgetreten. Der Dienst wurde beendet. Benutzeraktion Verwenden Sie die folgende Befehlszeile, um die Standardeinstellungen wiederherzustellen: winrm invoke Restore winrm/config @{} Fügen Sie dann alle gewünschten benutzerdefinierten Konfigurationseinstellungen hinzu, und starten Sie den Dienst erneut. Zusätzliche Daten Der Fehlercode ist: %1 %%%1

Ereignis-ID	Nachricht
468899	Das Hostnamensmuster "%1" ist ungültig und wird ignoriert. Hostnamensmuster dürfen nicht leer sein und dürfen maximal einen Platzhalter ("*") enthalten. Mit dem Muster "*" kann auf alle Hosts verwiesen werden. Wenn dieses Muster verwendet wird, darf die Liste kein anderes Muster enthalten. Mit der speziellen Zeichenfolge "<local>" kann auf alle Hostnamen verwiesen werden, die keinen Punkt enthalten. Benutzeraktion Korrigieren Sie das Hostnamensmuster, indem Sie die oben beschriebene Syntax verwenden.
468900	Der WinRM-Dienst hört WS-Verwaltungsanforderungen ab. Benutzeraktion Verwenden Sie den folgenden Befehl, um die spezifischen IP-Adressen anzuzeigen, die der WinRM-Dienst abhört: winrm enumerate winrm/config/listener
468901	Der WinRM-Dienst hört keine WS-Verwaltungsanforderungen ab. Benutzeraktion Wenn Sie den Dienst nicht unbeabsichtigt beendet haben, verwenden Sie folgenden Befehl, um die WinRM-Konfiguration anzuzeigen: winrm enumerate winrm/config/listener
468902	Der WinRM-Dienst konnte den folgenden Listener nicht zum Empfangen von WS-Verwaltungsanforderungen verwenden. Der Listener ist aktiviert, aber für den Listener ist keine IP-Adresse konfiguriert. Benutzeraktion Prüfen Sie die zugrunde liegende Netzwerkkonfiguration, um festzustellen, ob dieser Listener mindestens eine gültige IP-Adresse hat. Wenn die IP-Adresse gültig ist, stellen Sie sicher, dass die WinRM-Konfiguration diese IP-Adresse nicht ausschließt, indem Sie den folgenden Befehl verwenden: winrm get winrm/config/service Zusätzliche Daten Listenertransport: %1 Listeneradresse: %2
468903	Beim Lesen der Konfiguration während der Benachrichtigung über eine IP-Adressänderung ist im WinRM-Dienst ein Fehler (%1) aufgetreten. Der Dienst wird weiterhin mit der alten Konfiguration ausgeführt. Benutzeraktion Wenn sofortige Änderungen erforderlich sind, starten Sie den Dienst manuell neu.
468904	Der WinRM-Dienst hat erfolgreich eine Adressänderungsbenachrichtigung verarbeitet.
468905	Die Konfiguration konnte vom WSMan-IIS-Modul nicht gelesen werden. Empfangener Fehler: %1: %%%1 %2. Benutzeraktion Stellen Sie sicher, dass sowohl die Schema- als auch die Überprüfungsdatei vorhanden und gültig sind.
468906	Die folgenden SPNs konnten vom WinRM-Dienst nicht erstellt werden: %1; %2. Zusätzliche Daten Empfangener Fehler: %3: %%%3. Benutzeraktion Die SPNs können von einem Administrator mithilfe des Hilfsprogramms "setspn.exe" erstellt werden.
468907	Die Konfiguration des folgenden Plug-Ins konnte vom WSMan-Dienst nicht gelesen werden: %1. Empfangener Fehler: %2: %%%2 %3. Benutzeraktion Stellen Sie sicher, dass diese Plug-In-Konfiguration gültig ist.
468908	"CredSSP" konnte vom WinRM-Dienst nicht initialisiert werden. Zusätzliche Daten Empfangener Fehler: %1. Benutzeraktion Konfigurieren Sie die CertificateThumbprint-Einstellung unter der WinRM-Konfiguration für den Dienst. Verwenden Sie den Fingerabdruck eines gültigen Zertifikats, und stellen Sie sicher, dass der Netzwerkdienst über Zugriff auf den privaten Schlüssel des Zertifikats verfügt.
468909	Vom WinRM-Dienst wurde beim Entladen einer Daten- oder Ereignisquelle ein Fehler empfangen: DLL="%1" Benutzeraktion Überprüfen Sie, ob eine aktualisierte Version der folgenden Datei verfügbar ist: "%1". Zusätzliche Daten Fehler beim Herunterfahren von "%1". Fehler="%2" (%%%2).
468910	Am standardmäßigen %1-Port "%2" und am %1-Port "%3" (Kompatibilität) für WS-Verwaltungsanforderungen findet ein Abhörvorgang statt. Der %1-Port "%3" ist nicht mehr der Standardport für den WinRM-Dienst. Falls Sie den Listener am Port "%3" (Kompatibilität) deaktivieren möchten, führen Sie den folgenden Befehl aus: Winrm set winrm/config/service @{%4="False"}
468911	Der Dienst "Windows-Remoteverwaltung" hat in den letzten %2 Minuten %1 nicht authentifizierte Verbindungen beendet, um den fehlerfreien Systemstatus aufrechtzuerhalten Wahrscheinliche Ursache hierfür ist eine Überlastung des Diensts oder

Ereignis-ID	Nachricht
	eine auf Authentifizierung basierende Attacke auf den Dienst. Aktion: Aktivieren Sie das WinRM-Protokoll (Windows Remote Management, Windows-Remoteverwaltung) "Analytisch", und suchen Sie im Protokoll nach Warnereignissen mit der ID 1843. Diese Ereignisse enthalten weitere Informationen zu den Clients, die plötzlich beendet wurden.
3221734403	Der WinRM-Dienst wird aufgrund eines Fehlers beim Registrieren für Änderungen an den IP-Adressen beendet. Benutzeraktion Starten Sie den WinRM-Dienst neu. Zusätzliche Daten Der Fehlercode ist %1.
3221734404	Der WinRM-Dienst wird aufgrund eines Fehlers beim Registrieren für Änderungen an der Konfiguration beendet. Benutzeraktion Starten Sie den WinRM-Dienst neu. Zusätzliche Daten Der Fehlercode ist %1.

Ereignis-IDs: Abs. 5.3.1.7

Ereignis-ID	Nachricht
2	Fehler des TPM-Selbsttestbefehls.
12	Beim Gerätetreiber für das Trusted Platform Module (TPM) ist ein Fehler in der TPM-Hardware aufgetreten, der dazu führen kann, dass einige Anwendungen, die TPM-Dienste verwenden, nicht ordnungsgemäß ausgeführt werden. Starten Sie den Computer neu, um die TPM-Hardware zurückzusetzen. Wenn Sie weitere Unterstützung benötigen, wenden Sie sich an den Computerhersteller, um weitere Informationen zu erhalten.
14	Beim Gerätetreiber für das Trusted Platform Module (TPM) ist ein nicht behebbarer Fehler in der TPM-Hardware aufgetreten, der die Verwendung der TPM-Dienste (z. B. Datenverschlüsselung) verhindert. Wenden Sie sich an den Computerhersteller, um weitere Hilfe zu erhalten.
15	Beim Gerätetreiber für das Trusted Platform Module (TPM) ist ein nicht behebbarer Fehler in der TPM-Hardware aufgetreten, der die Verwendung der TPM-Dienste (z. B. Datenverschlüsselung) verhindert. Wenden Sie sich an den Computerhersteller, um weitere Hilfe zu erhalten.
16	Es wurde kein kompatibles TPM gefunden.
17	Die TPM-Hardware (Trusted Platform Module) konnte einen TPM-Befehl nicht ausführen.
18	Dieses Ereignis löst die Ausführung der TPM-Bereitstellung/-Statusprüfung aus.
19	Von der Systemfirmware konnte die Überschreibung des Systemspeichers beim Neustart nicht aktiviert werden. Die ACPI-Anforderung konnte nicht von der Firmware interpretiert werden. Für die Firmware sollte ein Upgrade vorgenommen werden.
20	An das TPM (Trusted Platform Module) wurde ein Befehl gesendet, der die TPM-Sperrlogik erfolgreich zurückgesetzt hat. Dieses Ereignis wird generiert, wenn ein an das TPM gesendeter Befehl die TPM-Sperrlogik erfolgreich zurückgesetzt hat. Nach diesem Ereignis werden alle früheren TPM-Autorisierungsfehler für Standardbenutzer ignoriert, sodass letztere das TPM sofort wieder normal verwenden können.
21	Ein von einem Standardbenutzer ausgegebener TPM-Befehl hat einen Autorisierungsfehler zurückgegeben. Dieses Ereignis wird generiert, wenn ein von einem Standardbenutzer an das TPM gesendeter Befehl eine Antwort zurückgibt, die auf einen Autorisierungsfehler hinweist. Bei zu vielen Autorisierungsfehlern können Standardbenutzer möglicherweise vorübergehend keine TPM-Befehle senden, für die eine Autorisierung erforderlich ist. Dadurch wird eine Hardwaresperre des TPM aufgrund zu vieler Autorisierungsfehler vermieden. Benutzersicherheits-ID:%1. Prozesspfad %2.

Ereignis-ID	Nachricht
22	TPM-Basisdienste (TBS) befindet sich gemäß Konfiguration bis zum nächsten vollen Neustart in einem Testmodus. Von TBS wird bis zum nächsten vollen Neustart keine TPM-Ressourcenvirtualisierung oder eine TPM-Befehlssperre ausgeführt.
23	Ein TPM-Befehl eines Standardbenutzers wurde gesperrt, da der Standardbenutzer die maximal zulässige Anzahl an Autorisierungsfehlern überschritten hat. Dieses Ereignis wird generiert, wenn zu viele kürzlich an das TPM gesendete TPM-Befehle eine Antwort zurückgegeben haben, die auf einen Autorisierungsfehler hinweist. Der Standardbenutzer kann vorübergehend keine TPM-Befehle senden, für die eine Autorisierung erforderlich ist. Dadurch wird eine Hardwaresperre des TPM aufgrund zu vieler Autorisierungsfehler vermieden. Benutzersicherheits-ID:%1.
24	Status des Trusted Platform Module (TPM): "%1" und "%2".
25	Fehler beim Erstellen des Windows AIK-Verzeichnisses.
26	Fehler beim Erstellen eines Bereitstellungsereignisses
27	Fehler bei der Initialisierung des TPMs (Trusted Platform Module). Das TPM befindet sich möglicherweise im Fehlermodus. Wenden Sie sich zu Diagnosezwecken unter Angabe der angefügten Informationen an den TPM-Hersteller.

Ereignis-IDs: Abs. 5.3.1.8

Ereignis-ID	Nachricht
513	Die TPM-Besitzerautorisierungsinformationen wurden erfolgreich in den Active Directory-Domänendiensten gesichert.
514	Fehler beim Sichern der TPM-Besitzerautorisierungsinformationen in den Active Directory-Domänendiensten. Fehlercode: %1 Überprüfen Sie, ob Ihr PC mit der Domäne verbunden ist. Falls er mit der Domäne verbunden ist, bitten Sie den Domänenadministrator zu überprüfen, ob das Active Directory-Schema für die Sicherung von TPM-Besitzerautorisierungsinformationen für Windows 8 geeignet ist und das aktuelle Computerobjekt über Schreibberechtigungen für das TPM-Objekt verfügt. Für Installationen von Windows Server 2008 R2 oder ältere Versionen ist eine Schemaerweiterung erforderlich, um TPM-Besitzerautorisierungsinformationen für Windows 8 sichern zu können. Weitere Informationen zum Einrichten der Active Directory-Domänendienste für TPM finden Sie in der Onlinedokumentation.
515	Für die TPM (Trusted Platform Module)-Hardware auf diesem Computer konnten die Wörterbuchangriff-Parameter nicht auf den Legacymodus festgelegt werden.
516	Die Anforderung der physischen Anwesenheit zum Löschen des Trusted Platform Module (TPM) wurde erfolgreich gesendet.
517	Fehler beim Senden der Anforderung der physischen Anwesenheit zum Löschen des Trusted Platform Module (TPM)
518	Fehler beim Abrufen des isOwned Status vom Trusted Platform Module (TPM). Das Löschen des TPMs wird in der Annahme fortgesetzt, dass das TPM über einen Besitzer verfügt. Fehlercode: %1
769	Die TPM-Besitzerautorisierungskonfiguration wurde von "%1" in "%2" geändert.
1025	Das TPM wurde erfolgreich bereitgestellt und kann jetzt verwendet werden.
1026	Die Trusted Platform Module-Hardware auf diesem PC kann nicht automatisch zur Verwendung bereitgestellt werden. Richten Sie das TPM mithilfe der TPM-

Ereignis-ID	Nachricht
	Verwaltungskonsole (Start->tpm.msc) interaktiv ein, und verwenden Sie die Aktion zum Vorbereiten des TPMs. Fehler: %1 Weitere Informationen: %2
1027	Der Besitz an der Trusted Platform Module-Hardware auf diesem PC wurde erfolgreich vom System übernommen (TPM-Befehl "TakeOwnership").
1028	Der Task für die NGC-Schlüsselgenerierung wurde erfolgreich ausgelöst.
1029	Fehler beim Auslösen des Tasks für die NGC-Schlüsselgenerierung.
1030	Der Task für die NGC-Zertifikatregistrierung wurde erfolgreich ausgelöst.
1031	Fehler beim Auslösen des Tasks für die NGC-Zertifikatregistrierung.
1281	Durch dieses Ereignis wird die TBS-Gerätebezeichnergenerierung ausgelöst.
1282	Der TBS-Gerätebezeichner wurde generiert.
1537	Das Geräteintegritätszertifikat wurde erfolgreich von %1 bereitgestellt.
1538	Bei der Bereitstellung des Geräteintegritätszertifikats konnte keine Verbindung mit %1 hergestellt werden. %2
1539	Das Geräteintegritätszertifikat konnte von %1 nicht bereitgestellt werden. HTTP-Statuscode %2: %3
1793	Für die TPM (Trusted Platform Module)-Hardware auf diesem Computer ist eine Löschung durch das System geplant.
1794	Bei der TPM (Trusted Platform Module)-Firmware auf diesem PC liegt ein bekanntes Sicherheitsproblem vor. Erkundigen Sie sich bei Ihrem PC-Hersteller nach einem Update. Weitere Informationen finden Sie unter https://go.microsoft.com/fwlink/?linkid=852572.

Ereignis-IDs: Abs. 5.3.2.1, 5.3.2.2

Ereignis-ID	Nachricht
2000	Die folgenden Einstellungen wurden beim Start auf die Windows Defender Firewall angewendet. Aktuelles Profil: %1 IPsec-SA-Leerlaufzeit: %2 IPsec-Verschlüsselung vorinstallierter Schlüssel: %3 IPsec-Ausnahme: %4 IPsec-Zertifikatsperrlistenüberprüfung: %5 IPsec über NAT: %6 Unterstützte Richtlinienversion: %7 Richtlinienversion: %8 Unterstützte Binärversion: %9 Statusbehaftetes FTP: %10 Angewendete Gruppenrichtlinie: %11 Remotecomputer-Autorisierungsliste: %12 Remotebenutzer-Autorisierungsliste: %13
2001	Die folgenden profilbezogenen Einstellungen wurden von der Windows Defender Firewall angewendet. Profil: %1 Betriebsmodus: %2 Geschützter Modus: %3 Alle eingehenden Verbindungen blockieren: %4 Unicastantwort auf Multicastbroadcast: %5 Verworfene Pakete protokollieren: %6 Erfolgreiche Verbindungen protokollieren: %7 Ignorierte Regeln protokollieren: %8 Eingehende Benachrichtigungen: %9 Zusammenführen von lokalen Richtlinien zulassen: %12 Zusammenführen von lokalen IPsec-Richtlinien zulassen: %13 Ausgehende Standardaktion: %14 Eingehende Standardaktion: %15 Remoteverwaltung: %16 Geschützter Modus - Ausnahme für IPsec-geschützte Pakete: %21 Maximale Protokolldateigröße: %17 Protokolldateipfad: %18 Benutzerdefiniertes Zusammenführen von autorisierten Anwendungen zulassen: %10 Benutzerdefiniertes Zusammenführen von global geöffneten Ports zulassen: %11
2002	Eine Windows Defender Firewall-Einstellung wurde geändert. Neue Einstellung: Typ: %1 Wert: %4 Ändernder Benutzer: %6 Ändernde Anwendung: %7
2003	Eine Windows Defender Firewall-Einstellung im Profil %1 wurde geändert. Neue Einstellung: Typ: %2 Wert: %5 Ändernder Benutzer: %7 Ändernde Anwendung: %8

Ereignis-ID	Nachricht
2004	Eine Regel wurde der Ausnahmeliste der Windows Defender Firewall hinzugefügt. Hinzugefügte Regel: Regel-ID: %1 Regelname: %2 Ursprung: %3 Aktiv: %18 Richtung: %6 Profile: %11 Aktion: %10 Anwendungspfad: %4 Dienstname: %5 Protokoll: %7 Sicherheitsoptionen: %21 Edgeausnahme: %19 Ändernder Benutzer: %22 Ändernde Anwendung: %23
2005	Eine Regel in der Ausnahmeliste der Windows Defender Firewall wurde geändert. Geänderte Regel: Regel-ID: %1 Regelname: %2 Ursprung: %3 Aktiv: %18 Richtung: %6 Profile: %11 Aktion: %10 Anwendungspfad: %4 Dienstname: %5 Protokoll: %7 Sicherheitsoptionen: %21 Edgeausnahme: %19 Ändernder Benutzer: %22 Ändernde Anwendung: %23
2006	Eine Regel in der Ausnahmeliste der Windows Defender Firewall wurde gelöscht. Gelöschte Regel: Regel-ID: %1 Regelname: %2 Ändernder Benutzer: %3 Ändernde Anwendung: %4
2007	Beim Start der Windows Defender Firewall wurde eine Regel aufgelistet. Hinzugefügte Regel: Regel-ID: %1 Regelname: %2 Ursprung: %3 Aktiv: %18 Richtung: %6 Profile: %11 Aktion: %10 Anwendungspfad: %4 Dienstname: %5 Protokoll: %7 Sicherheitsoptionen: %21 Edgeausnahme: %19
2008	Die Windows Defender Firewall-Gruppenrichtlinieneinstellungen wurden geändert. Die neuen Einstellungen wurden angewendet.
2009	Fehler beim Laden der Gruppenrichtlinie durch den Windows Defender Firewall-Dienst. Fehler: %1
2010	Das Netzwerkprofil wurde für eine Schnittstelle geändert. Adapter-GUID: %1 Adaptername: %2 Altes Profil: %3 Neues Profil: %4
2011	Die Windows Defender Firewall konnte den Benutzer nicht darüber benachrichtigen, dass eine Anwendung blockiert wurde und dass sie keine eingehenden Verbindungen im Netzwerk akzeptieren kann. Grund: %1 Anwendungspfad: %2 IP-Version: %3 Protokoll: %4 Port: %5 Prozess-ID: %6 Benutzer: %7
2032	Die Windows Defender Firewall wurde auf die Standardkonfiguration zurückgesetzt. ModifyingUser: %1 ModifyingApplication: %2
2033	Alle Regeln wurden aus der Windows Defender Firewall-Konfiguration auf dem Computer gelöscht. Speichertyp: %1 ModifyingUser: %2 ModifyingApplication: %3

Ereignis-IDs: Abs. 5.4.1.1

Ereignis-ID	Nachricht
1000	Momentan sind für die Schnittstellen auf dem Host keine IPv4-DNS-Server konfiguriert. Konfigurieren Sie DNS-Servereinstellungen, oder legen Sie die dynamischen IP-Einstellungen neu fest.
1001	Schnittstelle: %1 Anzahl DNS-Server gesamt: %2 Index: %3 Adresse: %6 (%4)
1002	Der für die Schnittstelle %1 abgefragte DNS-Server wurde in %3 geändert.
1003	Die folgenden DNS-Server wurden erfolgreich als aktive Server überprüft, die diesen Client bedienen können. %2
1005	Die folgenden Server konnten vom Client nicht als aktive DNS-Server überprüft werden. Die Server sind möglicherweise vorübergehend nicht verfügbar oder wurden falsch konfiguriert. %2
1007	Kein primäres DNS-Suffix für den Computer vorhanden. Bei nicht vorhandenem primären DNS-Suffix werden kurze, unvollständige Namen möglicherweise nicht in DNS aufgelöst.
1008	Kein primäres DNS-Suffix für den Computer vorhanden. Bei nicht vorhandenem primären DNS-Suffix werden kurze, unvollständige Namen möglicherweise nicht in DNS aufgelöst.
1009	Das primäre DNS-Suffix für den Computer (%1) stimmt nicht mit der Active Directory-Domäne (%2) überein, zu der er momentan gehört.

Ereignis-ID	Nachricht
1010	Das primäre DNS-Suffix für den Computer (%1) stimmt nicht mit der Active Directory-Domäne (%2) überein, zu der er momentan gehört.
1011	Fehler beim Lesen der Datei für lokale Hosts.
1012	Fehler beim Lesen der Datei für lokale Hosts.
1013	Zeitüberschreitung bei der Namensauflösung für den Namen %1, nachdem keiner der konfigurierten DNS-Server geantwortet hat.
1014	Zeitüberschreitung bei der Namensauflösung für den Namen %1, nachdem keiner der konfigurierten DNS-Server geantwortet hat.
1015	Zeitüberschreitung bei der Namensauflösung für den Namen %1, nachdem der DNS-Server %3 nicht geantwortet hat.
1016	Fehler beim Namen "%1": Der Name wurde nicht gefunden. Überprüfen Sie den Namen, um sicherzustellen, dass er richtig ist. Die Antwort wurde vom Server um %3 gesendet.
1017	Die Antwort des DNS-Servers auf eine Abfrage für den Namen %1 zeigt, dass für den angefragten Typ keine Datensätze verfügbar sind. Sie könnte jedoch darauf hindeuten, dass für denselben Namen andere Datensätze vorhanden sind.
1018	Die Antwort für die Abfrage %1 war eine verbindungslokale IP-Adresse %3. Die Antwort wurde vom Server um %5 gesendet.
1019	Momentan sind für die Schnittstellen auf dem Host keine IPv6-DNS-Server konfiguriert. Konfigurieren Sie DNS-Servereinstellungen, oder legen Sie die dynamischen IP-Einstellungen neu fest.
1020	Richtlinientabelle für die DNS-Namensauflösung lesen: Schlüsselname %1: DNS-Sicherheitseinstellungen: DNS-Überprüfung erforderlich %2, DNS-Abfrage über IPSec %3, DNS-Verschlüsselung %4 DirectAccess-Einstellungen: DirectAccess-Serverliste %5, Remote-IPSEC aktivieren%6 Remoteverschlüsselung %7 Proxytyp %8 Proxyname %9
1021	Übereinstimmende effektive Richtlinie für den Abfragenamen "%1": Schlüsselname: %2, DNSSEC-Überprüfung erforderlich: %3, DNS-Anfrage über IPSec: %4, DNS-Verschlüsselung: %5, DirectAccess-Serverliste: %6, Proxytyp: %7, Proxyname: %8
1022	Bei der Namensauflösung für den Namen %1 wird nicht LLMNR oder NetBIOS verwendet.
1023	Die Richtlinientabelle für die Namensauflösung ist beschädigt. Die DNS-Auflösung ist so lange fehlerhaft, bis das Problem behoben wird. Wenden Sie sich an den Netzwerkadministrator. Weitere Informationen: Fehler %2 beim Lesen der Richtlinientabelle für die Regel %1.
1024	Die Transaktions-ID der Antwort für die Abfrage %1 von Server %3 stimmte nicht überein.
1025	Die DNS-Server-IP %3 der Antwort für die Abfrage %1 ist auf dem Client nicht konfiguriert.
1026	Die Frage (%2) in der Antwort von Server %4 stimmt nicht mit der ursprünglichen Frage %1 überein.
1027	Fehler bei der DNS-Namensauflösung für den Namen %1, da der Client keine Verbindung mit dem DNS-Server herstellen konnte. Mindestens eine der Schnittstellen befindet sich nicht in einem privaten Netzwerk, und bei der Namensauflösung werden LLMNR oder NetBIOS nicht verwendet.
1028	Übereinstimmende effektive Richtlinie für den Abfragenamen "%1": Schlüsselname: %2, DNSSEC-Überprüfung erforderlich: %3, DNS-Abfrage über IPSec: %4, DNS-Verschlüsselung: %5, DirectAccess-Serverliste: %6, Proxytyp: %7, Proxyname: %8, generische Serverliste: %9, IDN-Konfiguration: %10
3000	Eine DNS-Abfrage wird für den Namen "%1" und den Typ "%2" mit den Abfrageoptionen "%3" eingeleitet.
3001	Der DNS-Abfragevorgang wurde mit dem Ergebnis "%1" abgeschlossen.
3002	Eine DNS-Cachesuche wird für den Namen "%1" und den Typ "%2" mit den Abfrageoptionen "%3" eingeleitet.

Ereignis-ID	Nachricht
3003	Ein DNS-Cachesuchvorgang für den Namen "%1" und den Typ "%2" wurde mit dem Ergebnis "%3" abgeschlossen.
3004	Eine DNS-Abfrage nach dem FQDN wird für den Namen "%1" und den Typ "%2" mit den Abfrageoptionen "%3" eingeleitet.
3005	Ein DNS-Abfragevorgang nach dem FQDN für den Namen "%1" und den Typ "%2" wurde mit dem Ergebnis "%3" abgeschlossen.
3006	Für den Namen "%1" wird eine DNS-Abfrage aufgerufen. Typ: %2, Abfrageoptionen: %3, Serverliste: %4, Netzwerkabfrage: %5, Netzwerkindex: %6, Schnittstellenindex: %7, asynchrone Abfrage: %8
3007	"DnsQueryEx" für den Namen "%1" steht aus.
3008	Die DNS-Abfrage für den Namen "%1" ist abgeschlossen. Typ: %2, Abfrageoptionen: %3, Status: %4. Ergebnisse: %5
3009	Für den Namen "%1" wird eine Netzwerkabfrage initiiert. Parallele Abfrage: %2, Netzwerkindex: %3, Schnittstellenanzahl: %4, erster Schnittstellenname: %5, lokale Adressen: %6, DNS-Server: %7
3010	An den DNS-Server "%3" wurde eine DNS-Abfrage für den Namen "%1" und den Typ "%2" gesendet.
3011	Vom DNS-Server "%3" wurde eine Antwort für den Namen "%1" und den Typ "%2" empfangen. Antwortstatus: %4
3012	Für den Namen "%1" wird eine NetBIOS-Abfrage initiiert. Netzwerkindex: %2, Schnittstellenanzahl: %3, erster Schnittstellenname: %4, lokale Adressen: %5
3013	Die NetBIOS-Abfrage für den Namen "%1" wurde abgeschlossen. Status: %2, Ergebnisse: %3
3014	Die NetBIOS-Abfrage für den Namen "%1" steht aus.
3015	"DnsQueryEx" für den Namen "%1" wurde abgebrochen.
3016	Für den Namen "%1" (Typ: %2, Optionen: %3, Schnittstellenindex: %4) wurde ein Cachesuchvorgang aufgerufen.
3018	Vom Cachesuchvorgang für den Namen "%1" (Typ: %2, Option: %3) wurde "%4" zurückgegeben. Ergebnisse: %5
3019	Für den Namen "%1" (Typ: %2, Schnittstellenindex: %3, Netzwerkindex: %4) wurde eine Abfrage aufgerufen.
3020	Von der Abfrageantwort für den Namen "%1" (Typ: %2, Schnittstellenindex: %3, Netzwerkindex: %4) wurde "%5" zurückgegeben. Ergebnisse: %6
8001	Der DNS-Clientdienst konnte nicht gestartet werden. Die Schnittstelle des Remoteprozeduraufrufs (Remote Procedure Call, RPC) für den Dienst konnte nicht gestartet werden. Sie können die RPC- und DNS-Clientdienste neu starten, um das Problem zu beheben. Verwenden Sie hierfür an der Eingabeaufforderung einen der folgenden Befehle: (1) Geben Sie "net start rpc" ein, um den RPC-Dienst zu starten. (2) Geben Sie "net start dnscache" ein, um den DNS-Clientdienst zu starten. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8002	Der DNS-Clientdienst konnte nicht gestartet werden, weil kein Arbeitsspeicher zugewiesen wurde und möglicherweise kein Arbeitsspeicher verfügbar ist. Schließen Sie alle derzeit nicht verwendeten Anwendungen, oder starten Sie den Computer neu. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8003	Fehler beim Registrieren des Netzwerkadapters mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5

Ereignis-ID	Nachricht
	IP-Adressen: %6 Die Ursache für den DNS-Registrierungsfehler war eine Zeitüberschreitung der DNS-Updateanforderung, nachdem sie an den angegebenen DNS-Server gesendet wurde. Möglicherweise wird der autoritative DNS-Server für den aktualisierenden Namen nicht ausgeführt. Sie können versuchen, den Netzwerkadapter und seine Einstellungen manuell zu konfigurieren, indem Sie in der Befehlszeile "ipconfig /registerdns" eingeben. Wenden Sie sich bezüglich des Netzwerkzustands an den Netzwerksystemadministrator, falls das Problem weiterhin besteht.
8004	Der Netzwerkadapter konnte mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese DNS-Registrierung ist aufgrund eines DNS-Serverfehlers fehlgeschlagen. Mögliche Ursache ist eine Zonenübertragung, die den DNS-Server für die anwendbare Zone, die der Computer zum Registrieren benötigt, blockiert. (Die anwendbare Zone sollte mit dem oben angegebenen adapterspezifischen Domänensuffix übereinstimmen.) Sie können versuchen, den Netzwerkadapter und seine Einstellungen manuell zu konfigurieren, indem Sie in der Befehlszeile "ipconfig /registerdns" eingeben. Wenden Sie sich bezüglich des Netzwerkzustands an den Netzwerksystemadministrator, falls das Problem weiterhin besteht.
8005	Der Netzwerkadapter konnte mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Die Registrierung ist aufgrund der folgenden Ursachen fehlgeschlagen: (a) Der DNS-Server unterstützt das Protokoll für das dynamische DNS-Update nicht. (b) Die primäre autorisierende Zone für die Namensregistrierung lässt zurzeit keine dynamischen Updates zu. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um einen Ressourceneintrag für einen DNS-Host (A oder AAAA) mit dem spezifischen DNS-Namen für diesen Adapter hinzuzufügen oder zu registrieren.

Ereignis-ID	Nachricht
8006	Der Netzwerkadapter konnte mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Die Registrierung ist fehlgeschlagen, weil der DNS-Server die dynamische Updateanforderung verweigert hat. Mögliche Ursachen sind: (a) Die aktuellen DNS-Updaterichtlinien lassen das Update für den für diesen Adapter konfigurierten DNS-Domänennamen nicht zu. (b) Der autorisierende DNS-Server für diesen DNS-Domänennamen unterstützt das Protokoll für das dynamische DNS-Update nicht. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um einen (A oder AAAA) Ressourceneintrag des DNS-Hosts mit dem spezifischen DNS-Domänennamen für diesen Adapter zu registrieren.
8007	Fehler beim Registrieren des Netzwerkadapters mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Die DNS-Updateanforderung konnte aufgrund von Sicherheitsproblemen nicht registriert werden. Mögliche Ursachen sind: (a) Der Domänenname, unter dem der Computer registriert werden soll, konnte aufgrund ungenügender Berechtigungen nicht aktualisiert werden. (b) Bei der gültigen Anmeldeinformationen mit dem zu aktualisierenden DNS-Server ist möglicherweise ein Problem aufgetreten. Sie können versuchen, den Netzwerkadapter und seine Einstellungen manuell zu konfigurieren, indem Sie in der Befehlszeile "ipconfig/registerdns" eingeben. Wenden Sie sich an den Netzwerksystemadministrator, falls das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8008	Fehler beim Registrieren des Netzwerkadapters mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6

Ereignis-ID	Nachricht
	Die DNS-Updateanforderung konnte aufgrund eines Systemproblems nicht abgeschlossen werden. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8009	Fehler beim Registrieren der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Die Ressourceneinträge konnten aufgrund einer Zeitüberschreitung der Updateanforderung, die an den angegebenen DNS-Server gesendet wurde, nicht registriert werden. Möglicherweise wird der autoritative DNS-Server für den zu registrierenden Namen nicht ausgeführt. Sie können versuchen, die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell auszuführen, indem Sie in der Befehlszeile "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, falls das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8010	Fehler beim Registrieren der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Das Problem wurde durch einen DNS-Serverfehler verursacht. Dies ist möglicherweise darauf zurückzuführen, dass die Reverse-Lookupzone ausgelastet ist oder auf dem vom Computer zu aktualisierenden DNS-Server fehlt. In den meisten Fällen ist dies ein geringfügiges Problem, da die normale(vorwärtsgerichtete) Namensauflösung nicht beeinträchtigt wird. Wenn für den Computer die rückwärtsgerichtete Auflösung (Adresse-in-Name) erforderlich ist, können Sie die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder

Ereignis-ID	Nachricht
	Netzwerksystemadministrator, wenn das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8011	Die Pointerressourceneinträge konnten für den Netzwerkadapter mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Die Ressourceneinträge konnten aufgrund der folgenden Ursachen nicht registriert werden: (a) Der DNS-Server unterstützt das Protokoll für das dynamische DNS-Update nicht. (b) Die autorisierende Zone, wo die Einträge registriert werden sollen, lässt keine dynamischen Updates zu. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um DNS-Pointerressourceneinträge mit dem spezifischen DNS-Domänennamen und IP-Adressen für diesen Adapter zu registrieren.
8012	Die Pointerressourceneinträge konnten für den Netzwerkadapter mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese Ressourceneinträge konnten nicht registriert werden, weil der DNS-Server die Updateanforderung verweigert hat. Mögliche Ursachen sind: (a) Der Computer darf den adapterspezifischen DNS-Domänenname nicht aktualisieren. (b) Der autorisierende DNS-Server unterstützt das Protokoll für das dynamische DNS-Update nicht. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um DNS-Pointerressourceneinträge mit dem spezifischen DNS-Domänennamen und IP-Adressen für diesen Adapter zu registrieren.
8013	Fehler beim Registrieren der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6

Ereignis-ID	Nachricht
	Diese Ressourceneinträge konnten aufgrund von Sicherheitsproblemen nicht registriert werden. Mögliche Ursachen sind: (a) Der Computer verfügt nicht über ausreichend Berechtigungen, um den spezifischen DNS-Domänennamen für diesen Adapter zu registrieren und aktualisieren. (b) Beim Aushandeln der Anmeldeinformationen mit dem DNS-Server während der Verarbeitung der Updateanforderung ist ein Fehler aufgetreten. Sie können versuchen, die DNS-Registrierung des Netzwerkadapters und seiner Einstellungen manuell auszuführen, indem Sie in der Befehlszeile "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server oder Netzwerksystemadministrator, falls das Problem weiterhin besteht.
8014	Fehler beim Registrieren der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Die Ressourceneinträge konnten während der Updateanforderung aufgrund eines Systemproblems nicht registriert werden. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8015	Fehler beim Registrieren der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Diese Ressourceneinträge konnten aufgrund einer Zeitüberschreitung der Updateanforderung, die an den DNS-Server gesendet wurde, nicht registriert werden. Wahrscheinlich wird der für die Registrierung oder Aktualisierung autoritative DNS-Server nicht ausgeführt. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht.

Ereignis-ID	Nachricht
8016	Fehler beim Registrieren der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Diese Ressourceneinträge konnten nicht registriert werden, weil die Updateanforderung auf dem DNS-Server fehlgeschlagen ist. Wahrscheinlich hat der für die Verarbeitung der Updateanforderung erforderliche DNS-Server eine Sperre auf dieser Zone, weil zurzeit eine Zonenübertragung ausgeführt wird. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht.
8017	Fehler beim Registrieren der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Entweder unterstützt der DNS-Server das Protokoll für das dynamische DNS-Update nicht oder die autoritative Zone unterstützt keine dynamischen Updates. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um die Ressourceneinträge für den DNS-Host (A oder AAAA) mit dem spezifischen DNS-Domänennamen und IP-Adressen für diesen Adapter zu registrieren.
8018	Die Ressourceneinträge für Host (A oder AAAA) konnten für den Netzwerkadapter mit folgenden Einstellungen nicht registriert werden: Adaptername : %1 Hostname : %2 Primäres Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) :

Ereignis-ID	Nachricht
	%6 Diese Ressourceneinträge konnten nicht registriert werden, weil der DNS-Server die Updateanforderung verweigert hat. Mögliche Ursachen sind: (a) Sie sind nicht dazu berechtigt den adapterspezifischen DNS-Domänenname zu aktualisieren. (b) Der autorisierende DNS-Server unterstützt das Protokoll für das dynamische DNS-Update nicht. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, um die Ressourceneinträge für den DNS-Host (A oder AAAA) mit dem spezifischen DNS-Domänennamen und IP-Adressen für diesen Adapter zu registrieren.
8019	Fehler beim Registrieren der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Diese Ressourceneinträge konnten aufgrund eines Sicherheitsproblems nicht registriert werden. Mögliche Ursachen sind: (a) Der Computer verfügt nicht über ausreichend Berechtigungen, um den spezifischen DNS-Domänennamensatz für diesen Adapter zu registrieren oder aktualisieren. (b) Beim Aushandeln der Anmeldeinformationen mit dem DNS-Server während des Verarbeitens der Updateanforderung ist ein Fehler aufgetreten. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8020	Fehler beim Registrieren der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Die Ressourceneinträge konnten aufgrund eines Systemproblems nicht während der Updateanforderung registriert werden. Sie können die DNS-Registrierung des Netzwerkadapters und der dazugehörigen Einstellungen manuell ausführen, indem Sie an der Eingabeaufforderung "ipconfig /registerdns" eingeben. Wenden Sie sich an den DNS-

Ereignis-ID	Nachricht
	Server- oder Netzwerksystemadministrator, wenn das Problem weiterhin besteht. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8021	Die Registrierung des Netzwerkadapters konnte mit folgenden Einstellungen nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Die Registrierung konnte aufgrund einer Zeitüberschreitung des DNS-Servers, an den die Updateanforderung gesendet wurde, nicht aktualisiert oder aufgehoben werden. Wahrscheinlich wird der autorisierende DNS-Server für die Zone, wo die Registrierung ursprünglich durchgeführt wurde, nicht ausgeführt oder ist über das Netzwerk zurzeit nicht erreichbar.
8022	Die Registrierung des Netzwerkadapters konnte mit folgenden Einstellungen nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n) : %6 Das Registrierungsupdate bzw. -aufhebung ist fehlgeschlagen, weil die Updateanforderung auf dem DNS-Server fehlgeschlagen ist. Wahrscheinlich hat der für die Updateanforderung verarbeitende erforderliche DNS-Server eine Sperre auf dieser Zone, weil eine Zonenübertragung zurzeit ausgeführt wird.
8023	Die Registrierung des Netzwerkadapters konnte mit folgenden Einstellungen nicht aktualisiert oder aufgehoben werden: Adaptername: %1 Hostname : %2 Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Der Vorgang ist fehlgeschlagen, weil (a) der DNS-Server, an den das Update gesendet wurde, das Protokoll für das dynamische DNS-Update nicht unterstützt, oder (b) die autorisierende Zone für den angegebenen DNS-Domänennamen zurzeit keine dynamischen DNS-Updates unterstützt.

Ereignis-ID	Nachricht
8024	Die Registrierung für den Netzwerkadapter mit seinen Einstellungen konnte nicht aktualisiert und entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Die Updateanforderung ist fehlgeschlagen, weil der DNS-Server die Anforderung verweigert hat. Mögliche Ursachen sind: (a) Der Computer darf den angegebenen DNS-Domänennamen nicht aktualisieren. (b) Der autorisierende DNS-Server für die zu aktualisierende Zone unterstützt das Protokoll für das dynamische DNS-Update nicht.
8025	Die Registrierung des Netzwerkadapters konnte mit folgenden Einstellungen nicht aktualisiert oder entfernt werden: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Das Update ist aufgrund eines Sicherheitsproblems fehlgeschlagen. Mögliche Ursachen sind: (a) Der Computer verfügt nicht über ausreichend Berechtigungen, um den spezifischen DNS-Domänennamensatz für diesen Adapter zu registrieren oder aktualisieren. (b) Beim Aushandeln der Anmeldeinformationen mit dem DNS-Server während des Verarbeitens der Updateanforderung ist ein Fehler aufgetreten. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8026	Fehler beim Aktualisieren und Entfernen der DNS-Registrierung für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Das Update zum Entfernen der DNS-Registrierung konnte aufgrund eines Systemproblems nicht ausgeführt werden. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8027	Die Pointerressourceneinträge für Netzwerkadapter

Ereignis-ID	Nachricht
	mit den folgenden Einstellungen konnten nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese Pointerressourceneinträge konnten aufgrund einer Zeitüberschreitung der Updateanforderung während der DNS-Serverrückmeldung nicht entfernt werden. Wahrscheinlich wird der autorisierte DNS-Server für die Zone, die ein Update erfordert, nicht ausgeführt.
8028	Die Pointerressourceneinträge für Netzwerkadapter mit den folgenden Einstellungen konnten nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese Pointerressourceneinträge konnten nicht entfernt werden, weil die Updateanforderung aufgrund des DNS-Servers fehlgeschlagen ist. Möglicherweise wird eine Zone gerade übertragen, so dass eine Zonensperrung beim DNS-Server, der zum Aktualisieren der Ressourceneinträge autorisiert ist, aufgetreten ist.
8029	Die Pointerressourceneinträge für Netzwerkadapter mit den folgenden Einstellungen konnten nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Die Pointerressourceneinträge konnten nicht entfernt werden, weil der DNS-Server das Protokoll für das dynamische DNS-Update nicht unterstützt. Andernfalls, verweigert die autorisierende Zone, die die Ressourceneinträge enthält, dynamische Updates.
8030	Die Pointerressourceneinträge für Netzwerkadapter mit den folgenden Einstellungen konnten nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Adapterspezifisches Domänensuffix : %3 DNS-Serverliste : %4

Ereignis-ID	Nachricht
	Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese Pointerressourceneinträge konnten nicht entfernt werden, weil der DNS-Server die Updateanforderung verweigert hat. Mögliche Ursachen sind: (a) Der durch diese angegebene Einstellungen angegebene DNS-Domänenname darf von diesem Computer nicht aktualisiert werden. (b) Der autorisierende DNS-Server, der das Update für die Ressourceneinträge enthaltene Zone ausführen darf, unterstützt das Protokoll für das dynamische DNS-Update nicht.
8031	Fehler beim Aktualisieren und Entfernen der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Die Zeigerressourceneinträge konnten aufgrund eines sicherheitsbedingten Problems nicht entfernt werden. Mögliche Ursachen: (a) Der Computer verfügt nicht über die Berechtigungen, um den für den Adapter konfigurierten spezifischen DNS-Domänennamen oder die für den Adapter konfigurierten IP-Adressen zu entfernen und zu aktualisieren. (b) Beim Verhandeln der gültigen Anmeldeinformationen mit dem DNS-Server während der Verarbeitung der Updateanforderung ist möglicherweise ein Problem aufgetreten. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8032	Fehler beim Aktualisieren und Entfernen der Zeigerressourceneinträge für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Adapterspezifisches Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Die Zeigerressourceneinträge konnten aufgrund eines Systemproblems nicht entfernt werden. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8033	Fehler beim Aktualisieren und Entfernen der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4

Ereignis-ID	Nachricht
	Server, an den das Update gesendet wurde: %5 IP-Adresse: %6 Diese Ressourceneinträge des Hosts (A oder AAAA) konnten aufgrund einer Zeitüberschreitung der Updateanforderung während der DNS-Serverrückmeldung nicht entfernt werden. Wahrscheinlich wird der autoritative DNS-Server für die Zone, wo die Ressourceneinträge aktualisiert werden müssen, nicht ausgeführt oder ist nicht über das Netzwerk erreichbar.
8034	Die Ressourceneinträge für Host (A oder AAAA) konnten für den Netzwerkadapter mit folgenden Einstellungen nicht aktualisiert und entfernt werden: Adaptername : %1 Hostname : %2 Primäres Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Diese Ressourceneinträge des Hosts (A oder AAAA) konnten nicht entfernt werden, weil die Updateanforderung aufgrund des DNS-Servers fehlgeschlagen ist. Möglicherweise wird eine Zone gerade übertragen, so dass eine Zonensperrung beim DNS-Server, der zum Aktualisieren der Ressourceneinträge autorisiert ist, aufgetreten ist.
8035	Die Ressourceneinträge für Host (A oder AAAA) für Netzwerkadapter mit folgenden Einstellungen konnten nicht registriert oder aufgehoben werden: Adaptername : %1 Hostname : %2 Primäres Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) : %6 Mögliche Ursachen für diesen Fehler sind, dass der DNS-Server, an den das Update gesendet wurde, entweder (a) das Protokoll für das dynamische DNS-Update nicht unterstützt oder (b) die autorisierende Zone für den in den Ressourceneinträgen des Hosts (A oder AAAA) angegebenen DNS-Domänenname zurzeit keine dynamischen DNS-Updates zulässt.
8036	Die Ressourceneinträge für Host (A oder AAAA) für Netzwerkadapter mit den folgenden Einstellungen konnten nicht aktualisiert oder entfernt werden: Adaptername : %1 Hostname : %2 Primäres Domänensuffix : %3 DNS-Serverliste : %4 Server, an den das Update gesendet wurde : %5 IP-Adresse(n) :

Ereignis-ID	Nachricht
	%6 Diese Ressourceneinträge konnten nicht entfernt werden, weil der DNS-Server die Updateanforderung verweigert hat. Mögliche Ursachen sind: (a) Der durch diese angegebene Einstellungen angegebene DNS-Domänenname darf von diesem Computer nicht aktualisiert werden. (b) Der autorisierende DNS-Server, der die Updates für die Ressourceneinträge enthaltene Zone ausführen darf, unterstützt das Protokoll für das dynamische DNS-Update nicht.
8037	Fehler beim Aktualisieren und Entfernen der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Die Ursache für den Fehler war ein sicherheitsbedingtes Problem. Mögliche Ursachen: (a) Der Computer verfügt nicht über die Berechtigungen, um den für den Adapter konfigurierten spezifischen DNS-Domänennamen oder die für den Adapter konfigurierten IP-Adressen zu entfernen und zu aktualisieren. (b) Beim Verhandeln der gültigen Anmeldeinformationen mit dem DNS-Server während der Verarbeitung der Updateanforderung ist möglicherweise ein Problem aufgetreten. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
8038	Fehler beim Aktualisieren und Entfernen der Hostressourceneinträge (A oder AAAA) für den Netzwerkadapter mit den folgenden Einstellungen: Adaptername: %1 Hostname: %2 Primäres Domänensuffix: %3 DNS-Serverliste: %4 Server, an den das Update gesendet wurde: %5 IP-Adresse(n): %6 Die Ursache für den Updateanforderungsfehler war ein Systemproblem. Genauere Fehlercodeinformationen finden Sie in den Ereignisdetails.
60004	Fehler: %1 Speicherort: %2 Kontext: %3
60005	Warnung: %1 Speicherort: %2 Kontext: %3
60006	Gewechselt in Status: %1 Kontext: %2
60007	Aktualisierter Kontext: %1 Ursache für Update: %2
60008	Die Richtlinientabelle für die Namensauflösung ist beschädigt. Die DNS-Auflösung ist so lange fehlerhaft, bis das Problem behoben wird. Wenden Sie sich an den Netzwerkadministrator. Weitere Informationen: Fehler %2 beim Lesen der Richtlinientabelle für die Regel %1.

Ereignis-ID	Nachricht
60101	Quelladresse: %1 Quellport: %2 Zieladresse: %3 Zielport: %4 Protokoll: %5 Referenzkontext: %6
60102	Quelladresse: %1 Quellport: %2 Zieladresse: %3 Zielport: %4 Protokoll: %5 Referenzkontext: %6
60103	Schnittstellen-Guid: %1 Schnittstellen-Index: %2 Schnittstellen-LUID: %3 Referenzparameter: %4

Ereignis-IDs: Abs. 5.4.1.2, 5.4.1.3

Ereignis-ID	Nachricht
30800	Der Servername kann nicht aufgelöst werden. Fehler: %2 Servername: %4 Erläuterung: Der Client kann die Serveradresse nicht in DNS oder WINS auflösen. Dieses Problem tritt oft unmittelbar nach dem Hinzufügen eines Computers zur Domäne auf, wenn die DNS-Registrierung des Clients möglicherweise noch nicht an alle DNS-Server verteilt wurde. Dieses Ereignis tritt auch beim Systemstart auf einem DNS-Server (z.B. ein Domänencontroller) auf, der für den primären DNS auf sich selbst verweist. Sie sollten die DNS-Clienteinstellungen auf diesem Computer mithilfe von IPCONFIG /ALL und NSLOOKUP überprüfen.
30801	%1. Fehler: %2 Servername: %4
30802	%1. Fehler: %2 Servername: %4
30803	Fehler bei der Einrichtung einer Netzwerkverbindung. Fehler: %2 Servername: %4 Serveradresse: %6 Verbindungstyp: %7 Erläuterung: Dies ist ein Hinweis auf ein Problem mit dem zugrunde liegenden Netzwerk oder dem Transportprotokoll, z.B. mit TCP/IP, und nicht auf ein Problem mit SMB. Eine Firewall, die den TCP-Port 445 oder 5445 bei Verwendung eines iWARP-RDMA-Adapters blockiert, kann dieses Problem ebenfalls verursachen.
30803	Fehler bei der Einrichtung einer Netzwerkverbindung. Fehler: %2

Ereignis-ID	Nachricht
	Servername: %4 Serveradresse: %6 Instanzname: %9 Verbindungstyp: %10 Erläuterung: Dies weist auf ein Problem mit dem zugrunde liegenden Netzwerk- oder Transportprotokoll (z. B. TCP/IP) und nicht auf ein Problem mit SMB hin. Eine Firewall, die den TCP-Port 445 oder 5445 bei Verwendung eines iWARP-RDMA-Adapters blockiert, kann dieses Problem ebenfalls verursachen.
30804	Eine Netzwerkverbindung wurde getrennt. Servername: %4 Serveradresse: %6 Verbindungstyp: %7 Erläuterung: Dies weist darauf hin, dass die Verbindung zwischen Client und Server getrennt wurde. Wenn bei Verwendung eines RoCE (RDMA over Converged Ethernet)-Adapters häufig unerwartete Trennungen auftreten, kann eine falsche Netzwerkkonfiguration vorliegen. RoCE setzt voraus, dass PFC (Priority Flow Control) für jeden Host, Switch und Router im RoCE-Netzwerk konfiguriert wird. Eine nicht ordnungsgemäße PFC-Konfiguration kann zu Paketverlusten, häufig auftretenden Trennungen und schlechter Leistung führen.
30805	Die Sitzung mit dem Server wurde für den Client unterbrochen. Fehler: %1 Servername: %5 Sitzungs-ID: %2 Erläuterung: Falls es sich bei dem Server um einen Windows-Failovercluster-Dateiserver handelt, wird diese Meldung ausgegeben, wenn die Dateifreigabe zwischen Clusterknoten verschoben wird. Es sollte auch das Anti-Ereignis 30806 vorhanden sein, das angibt, dass die Sitzung mit dem Server wiederhergestellt wurde. Falls es sich bei dem Server nicht um einen Failovercluster handelt, war der Server zuvor wahrscheinlich online, aber nun ist über das Netzwerk kein Zugriff mehr auf den Server möglich.
30806	Der Client hat die Sitzung mit dem Server wiederhergestellt. Servername: %5 Serveradresse: %7 Sitzungs-ID: %2 Erläuterung: Dieses Ereignis tritt auf, wenn zuvor das Ereignis 30805 vorhanden war, aber der Client die zwischengespeicherte Verbindung erfolgreich wiederhergestellt hat, bevor die Zeitüberschreitung eintrat.
30807	Die Verbindung mit der Freigabe wurde unterbrochen. Fehler: %1

Ereignis-ID	Nachricht
	Freigabename: %5 Sitzungs-ID: %2 Struktur-ID: %3 Erläuterung: Falls es sich bei dem Server um einen Windows-Failovercluster-Dateiserver handelt, wird diese Meldung ausgegeben, wenn die Dateifreigabe zwischen Clusterknoten verschoben wird. Es sollte auch das Anti-Ereignis 30808 vorhanden sein, das angibt, dass die Sitzung mit dem Server wiederhergestellt wurde. Falls es sich bei dem Server nicht um einen Failovercluster handelt, war der Server zuvor wahrscheinlich online, aber nun ist über das Netzwerk kein Zugriff mehr auf den Server möglich.
30808	Die Verbindung mit der Freigabe wurde wiederhergestellt. Freigabename: %5 Serveradresse: %7 Sitzungs-ID: %2 Struktur-ID: %3 Erläuterung: Dieses Ereignis tritt auf, wenn zuvor das Ereignis 30807 vorhanden war, aber der Client die zwischengespeicherte Verbindung erfolgreich wiederhergestellt hat, bevor die Zeitüberschreitung eintrat.
30809	Bei einer Anforderung ist eine Zeitüberschreitung aufgetreten, da der Server nicht antwortete. Servername: %6 Sitzungs-ID:%3 Baum-ID:%4 Nachrichten-ID:%2 Befehl: %1 Instanzname: %9 RetryCount: %10 ElapsedTime(ms): %11 Erläuterung: Der Server antwortet über TCP, aber nicht über SMB. Stellen Sie sicher, dass der Serverdienst ausgeführt wird und reagiert und dass die Datenträger keine hohe Pro-E/A-Latenz aufweisen, wodurch die Datenträger für SMB scheinbar nicht mehr reagieren. Stellen Sie außerdem sicher, dass der Server insgesamt reagiert und nicht angehalten ist. Vergewissern Sie sich beispielsweise, dass Sie sich an dem Server anmelden können.
30810	Eine TCP/IP-Transportschnittstelle wurde hinzugefügt. Name: %2 InterfaceIndex: %3 Erläuterung: Eine TCP/IP-Bindung wurde dem angegebenen Netzwerknetwork für den SMB-Client hinzugefügt. Der SMB-Client kann nun SMB-Datenverkehr auf diesem Netzwerkadapter mithilfe von TCP/IP senden und empfangen. Dieses Ereignis tritt auf, wenn ein Computer neu gestartet wird oder wenn ein zuvor deaktivierter Netzwerkadapter erneut aktiviert wird. Es ist keine Benutzeraktion erforderlich.

Ereignis-ID	Nachricht
30811	Eine TCP/IP-Transportschnittstelle wurde gelöscht. Name: %2 InterfaceIndex: %3 Erläuterung: Eine TCP/IP-Bindung wurde auf dem angegebenen Netzwerkadapter für den SMB-Client entfernt. Dieses Ereignis tritt auf, wenn ein Computer heruntergefahren wird oder wenn ein zuvor aktivierter Netzwerkadapter deaktiviert wird. Es ist keine Benutzeraktion erforderlich.
30812	Eine TDI-Transportschnittstelle wurde hinzugefügt. Name: %2 Erläuterung: Eine TDI (NetBIOS)-Bindung wurde dem angegebenen Netzwerkadapter für den SMB-Client hinzugefügt. Der SMB-Client kann nun SMB-Datenverkehr auf diesem Netzwerkadapter mithilfe von TDI senden und empfangen. Dieses Ereignis tritt auf, wenn ein Computer neu gestartet wird oder wenn ein zuvor deaktivierter Netzwerkadapter erneut aktiviert wird. Es ist keine Benutzeraktion erforderlich.
30813	Eine TDI-Transportschnittstelle wurde gelöscht. Name: %2 Erläuterung: Eine TDI (NetBIOS)-Bindung wurde auf dem angegebenen Netzwerkadapter für den SMB-Client entfernt. Dieses Ereignis tritt auf, wenn ein Computer heruntergefahren wird oder wenn ein zuvor aktivierter Netzwerkadapter deaktiviert wird. Es ist keine Benutzeraktion erforderlich.
30814	Die Zeugenregistrierung ist abgeschlossen. Status: %1 Clusterfreigabename: %4 Clusterfreigabetyp: %2 Adresse des Dateiserverclusters: %6 Erläuterung: Der Client wurde erfolgreich beim SMB-Zeugen über RPC mithilfe von TCP registriert (Port 135, anschließend ein Endpunktport über 1023). Es ist keine Benutzeraktion erforderlich.
30815	Die Aufhebung der Zeugenregistrierung ist abgeschlossen. Status: %1 Clusterfreigabename: %4 Clusterfreigabetyp: %2 Erläuterung: Die Registrierung des Clients beim SMB-Zeugen über RPC mithilfe von TCP wurde erfolgreich aufgehoben (Port 135, anschließend ein Endpunktport über 1023). Es ist keine Benutzeraktion erforderlich.
30816	Aushandlungsanforderungsfehler beim Server.

Ereignis-ID	Nachricht
	Fehler: %2 Servername: %4 Erläuterung: Der Server unterstützt keinen Dialekt, den der Client auszuhandeln versucht. Beispielsweise könnte auf dem Client SMB2/SMB3 deaktiviert sein, und auf dem Server könnte SMB1 deaktiviert sein.
30817	Fehler bei der Anforderung zum Schließen. Fehler: %2 Pfad: %4%6 Erläuterung: Ein beständiges Handle (Fortlaufende Verfügbarkeit) oder ein stabiles Handle konnte nicht geschlossen werden.
30818	RDMA-Schnittstellen sind verfügbar, aber der Client konnte keine Verbindung mit dem Server mittels RDMA-Transport herstellen. Servername: %2 Erläuterung: Sowohl der Client als auch der Server verfügen über RDMA (SMB Direct)-Adapter, aber es ist ein Problem bei der Verbindung aufgetreten, und der Client musste auf die Verwendung von TCP/IP SMB (Nicht-RDMA) zurückgreifen.
30819	Der SMB-Client hat eine Anforderung erhalten, auf einen anderen Knoten in einem Dateiservercluster umzustellen. Name des Dateiserverclusters: %4 Neue Adresse des Dateiserverclusters: %6 Erläuterung: Die fortlaufende Verfügbarkeit (transparentes Failover) wird verwendet, und der Clientcomputer wird nach einer SMB-Zeugenanforderung über RPC mithilfe von TCP auf einen anderen Knoten umgestellt (zuerst wird der Port 135 und anschließend ein Endpunktport über 1023 kontaktiert). Es ist keine Benutzeraktion erforderlich.
30820	Der SMB-Client wurde erfolgreich auf einen anderen Knoten in einem Dateiservercluster umgestellt. Name des Dateiserverclusters: %4 Neue Adresse des Dateiserverclusters: %6 Erläuterung: Die fortlaufende Verfügbarkeit (transparentes Failover) wird verwendet, und der Clientcomputer wurde nach einer SMB-Zeugenanforderung über RPC mithilfe von TCP erfolgreich auf einen anderen Knoten umgestellt (zuerst wird der Port 135 und anschließend ein Endpunktport über 1023 kontaktiert). Es ist keine Benutzeraktion erforderlich.
30821	Der SMB-Client konnte nicht auf einen anderen Knoten in einem Dateiservercluster umgestellt werden. Fehler: %1

Ereignis-ID	Nachricht
	Name des Dateiserverclusters: %4 Erläuterung: Die fortlaufende Verfügbarkeit (transparentes Failover) wird verwendet, und der Clientcomputer konnte nach einer SMB-Zeugenanforderung über RPC mithilfe von TCP nicht auf einen anderen Knoten umgestellt werden (zuerst wird der Port 135 und anschließend ein Endpunktport über 1023 kontaktiert). Der Verbindungsversuch mit dem Zielserver ist fehlgeschlagen, was in der Regel auf einen Netzwerkkonfigurationsfehler zurückzuführen ist. Dieses Problem kann beispielsweise auftreten, falls die IP-Adresse des Zielknotens nicht aufgelöst werden kann, falls sich der Zielknoten hinter einer Firewall befindet oder falls keine Netzwerkroute vom Client zum Knoten vorhanden ist.
30822	Fehler beim Herstellen einer SMB Multichannel-Netzwerkverbindung. Fehler: %2 Servername: %4 Serveradresse: %6 Clientadresse: %7 Instanzname: %9 Verbindungstyp: %10 Erläuterung: Dies weist auf ein Problem mit dem zugrunde liegenden Netzwerk- oder Transportprotokoll (z. B. TCP/IP) und nicht auf ein Problem mit SMB hin. Eine Firewall, die den TCP-Port 445 oder 5445 bei Verwendung eines iWARP-RDMA-Adapters blockiert, kann dieses Problem ebenfalls verursachen. Da der Fehler beim Versuch aufgetreten ist, eine Verbindung mit zusätzlichen Kanälen herzustellen, wird kein Anwendungsfehler gemeldet. Dieses Ereignis dient nur zu Diagnosezwecken.
30823	Die Verbindung wurde aufgrund eines oder mehrerer IO-Anfrage-Timeouts beendet. Fehler: %2 Name: %4 Serveradresse: %6 Clientadresse: %7 Instanzname: %9 Verbindungstyp: %10 Erläuterung: Dies weist auf ein Problem mit dem zugrunde liegenden Netzwerk oder dem Speicherstapel auf dem Remoteserver hin. IO-Operationen wurden nicht innerhalb der vorgegebenen Zeit abgeschlossen. Der Fehler tritt möglicherweise nicht in der Anwendung auf, da IO-Operationen normalerweise auf einer anderen Verbindung wiederholt werden. Dieses Ereignis dient nur zur Diagnose.
31000	%1. Fehler: %2 Sicherheitsstatus: %3 Benutzername: %10 Anmelde-ID: %4 Servername: %6
31001	%1. Fehler: %2 Sicherheitsstatus: %3 Benutzername: %10 Anmelde-ID: %4

Ereignis-ID	Nachricht
	Servername: %6 Prinzipalname: %8
31002	Bei der ausgehenden Authentifizierung konnte ein Netzwerktoken nicht verwendet werden. Fehler: %2 Servername: %4 Erläuterung: Dies ist in der Regel ein Hinweis darauf, dass die Delegierung für ein Kerberos Doppel-Hop-Szenario konfiguriert werden muss. Falls die Delegierung konfiguriert ist, bestätigen Sie, ob die Services auf dem Server auf mittlerer Ebene ordnungsgemäß konfiguriert sind.
31003	Der Wert für "LmCompatibilityLevel" weicht vom Standardwert ab. Konfigurierter LM-Kompatibilitätsgrad: %2 Standardmäßiger LM-Kompatibilitätsgrad: 3 Erläuterung: Bei der LAN-Manager (LM)-Authentifizierung handelt es sich um das Protokoll, mit dem Windows-Clients für den Netzwerkbetrieb authentifiziert werden. Dies beinhaltet das Hinzufügen einer Domäne, das Zugreifen auf Netzwerkressourcen und das Authentifizieren von Benutzern oder Computern. Dies bestimmt, welches Abfrage/Rückmeldung-Authentifizierungsprotokoll zwischen den Client- und Servercomputern ausgehandelt wird. Im Einzelnen bestimmt die LAN-Manager-Authentifizierungsebene, welche Authentifizierungsprotokolle der Client auszuhandeln versucht oder der Server akzeptiert. Der für "LmCompatibilityLevel" festgelegte Wert bestimmt, welches Abfrage/Rückmeldung-Authentifizierungsprotokoll für Netzwerkanmeldungen verwendet wird. Dieser Wert hat Auswirkungen auf die von Clients verwendete Authentifizierungsprotokollebene, die ausgehandelte Sitzungssicherheitsebene sowie die von Servern akzeptierte Authentifizierungsebene. Wert (Einstellung) - Beschreibung 0 (LM- und NTLM-Antworten senden) - Clients verwenden die LM- und NTLM-Authentifizierung, und sie verwenden niemals die NTLMv2-Sitzungssicherheit. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 1 (LM- und NTLM-Antworten senden - NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt) - Clients verwenden die LM- und NTLM-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 2 (Nur NTLM-Antworten senden) - Clients verwenden nur die NTLM-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 3 (Nur NTLMv2-Antworten senden) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 4 (Nur NTLMv2-Antwort senden/LM ablehnen) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller lehnen LM ab und akzeptieren nur die NTLM- und NTLMv2-Authentifizierung.

Ereignis-ID	Nachricht
	5 (Nur NTLMv2-Antwort senden/LM & NTLM ablehnen) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller lehnen LM und NTLM ab und akzeptieren nur die NTLMv2-Authentifizierung. Inkompatibel konfigurierte LmCompatibility-Grade zwischen einem Client und einem Server (z.B. 0 auf einem Client und 5 auf einem Server) verhindern den Zugriff auf den Server. Andere als Microsoft-Clients und -Server weisen diese Konfigurationseinstellungen ebenfalls auf.
31010	Der SMB-Client konnte keine Verbindung mit der Freigabe herstellen. Fehler: %2 Pfad: %4%6
31012	Fehler bei der Überprüfung des Aushandelns. Von Verhandlungsantwort: Dialekt: %1 Sicherheitsmodus: %2 Funktionen: %3 Server-GUID: %4 Von FSCTL_VALIDATE_NEGOTIATE_INFO-Antwort: Dialekt: %5 Sicherheitsmodus: %6 Funktionen: %7 Server-GUID: %8 Erläuterung: Der Client hat den SMB-Dialekt, den Sicherheitsmodus, die Funktionen und die Server-GUID erfolgreich mit dem Server ausgehandelt, aber die Überprüfung dieser Werte ist dann nach dem Herstellen einer Verbindung mit einer Freigabe fehlgeschlagen. Dies kann auf einen "Man-in-the-Middle"-Angriffsversuch zurückzuführen sein.
31013	Fehler bei der Signaturüberprüfung. Fehler:%7 Servername: %6 Sitzungs-ID:%3 Struktur-ID:%4 Nachrichten-ID:%2 Befehl: %1 Erläuterung: Dieser Fehler weist darauf hin, dass SMB-Nachrichten bei der Übertragung im Netzwerk vom Server zum Client geändert werden. Dies kann zurückzuführen sein auf die Beendigung der Sitzung auf dem Server, ein Problem mit dem Netzwerk, ein Problem mit einem SMB-Server von einem Drittanbieter oder einen "Man-in-the-Middle"-Angriffsversuch. PacketFragment:%9
31014	Der Client hat eine unverschlüsselte Nachricht erhalten, als die Verschlüsselung erwartet wurde. Servername: %6 Sitzungs-ID:%3 Baum-ID:%4 Nachrichten-ID:%2 Befehl: %1 Instanzname: %9

Ereignis-ID	Nachricht
	Erläuterung: Dieser Fehler weist darauf hin, dass SMB-Nachrichten bei der Übertragung im Netzwerk vom Server zum Client geändert werden. Dies kann zurückzuführen sein auf die Beendigung der Sitzung auf dem Server, ein Problem beim Netzwerk, ein Problem mit einem SMB-Server von einem Drittanbieter oder einen äMan-in-the-Middleö-Angriffsversuch.
31015	Fehler beim Entschlüsseln einer verschlüsselten SMB-Nachricht. Fehler:%7 Servername: %6 Sitzungs-ID:%3 Instanzname: %9 Erläuterung: Der Client hat eine verschlüsselte SMB-Nachricht empfangen, kann aber die Daten nicht entschlüsseln. Dies bedeutet in der Regel, dass die Nachricht von einer früheren Sitzung stammt, die nicht mehr vorhanden ist. Möglicherweise wurde auch der Verschlüsselungsheader bei der Übertragung im Netzwerk zwischen dem Client und dem Server beschädigt oder manipuliert.
31016	Für den SBM-Signatur-Registrierungswert sind nicht die Standardeinstellungen konfiguriert. Standardregistrierungswert: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "EnableSecuritySignature"=dword:1 Konfigurierter Registrierungswert: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "EnableSecuritySignature"=dword:0 Erläuterung: Sie können zwar die SMB-Signatur deaktivieren, aktivieren oder als erforderlich festlegen, aber die Aushandlungsregeln wurden ab SMB2 geändert und nicht alle Kombinationen funktionieren wie in SMB1. Das tatsächliche Verhalten für SMB2/SMB3 sieht wie folgt aus: Client erforderlich und Server erforderlich = Signiert Client nicht erforderlich und Server erforderlich = Signiert Server erforderlich und Client nicht erforderlich = Signiert Server nicht erforderlich und Client nicht erforderlich = Nicht signiert Wenn die SMB-Verschlüsselung erforderlich ist, wird die SMB-Signatur nicht verwendet, und zwar unabhängig von den Einstellungen. Die SMB-Verschlüsselung bietet implizit dieselben Integritätsgarantien wie die SMB-Signatur.
31017	Eine unsichere Gastanmeldung wurde zurückgewiesen. Benutzername: %2 Servername: %4 Erläuterung: Dieses Ereignis gibt an, dass der Server versucht hat, den Benutzer als nicht authentifizierten Gast anzumelden, was vom Client verweigert wurde. Gastanmeldungen unterstützen keine Standardsicherheitsfunktionen wie die Signierung und Verschlüsselung. Folglich sind Gastanmeldungen gefährdet für Man-in-the-Middle-Angriffe, durch die vertrauliche Daten im Netzwerk verfügbar gemacht werden können. Unsichere Gastanmeldungen werden von Windows standardmäßig deaktiviert. Die Aktivierung unsicherer Gastanmeldungen wird von Microsoft nicht empfohlen.
31018	Der Registrierungsschlüssel %1 ist nicht mit Standardeinstellungen konfiguriert.

Ereignis-ID	Nachricht
	Standardregistrierungswert: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "%1"=dword:0 Konfigurierter Registrierungswert: [HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters] "%1"=dword:%2 Erläuterung: Dieses Ereignis gibt an, dass unsichere Gastanmeldungen von einem Administrator aktiviert wurden. Eine unsichere Gastanmeldung tritt auf, wenn der Benutzer vom Server als nicht authentifizierter Gast angemeldet wird, was in der Regel nach einem Authentifizierungsfehler erfolgt. Gastanmeldungen unterstützen keine Standardsicherheitsfunktionen wie die Signierung und Verschlüsselung. Folglich sind Gastanmeldungen gefährdet für Man-in-the-Middle-Angriffe, durch die vertrauliche Daten im Netzwerk verfügbar gemacht werden können. Unsichere Gastanmeldungen werden von Windows standardmäßig deaktiviert. Die Aktivierung unsicherer Gastanmeldungen wird von Microsoft nicht empfohlen.
31019	Die gegenseitige Authentifizierung wurde nach der erneuten Authentifizierung unerwartet ungültig: %6 Benutzer %8 LogonID %4 Status %2 AuthProtocol alt %9 Neu %10 MutualAuthState alt %11 Neu %12 Gruppiert %13

Ereignis-IDs: Abs. 5.4.1.4, 5.4.1.5

Ereignis-ID	Nachricht
551	Fehler bei der Authentifizierung der SM-Sitzung Clientname: %11 Clientadresse: %6 Benutzername: %9 Sitzungs-ID: %7 Status: %4 (%3) Erläuterung: Dieser Fehler kann auftreten, wenn Sie versuchen, mithilfe falscher Anmeldeinformationen eine Verbindung mit Freigaben herzustellen. Dieser Fehler ist nicht immer ein Hinweis auf ein Problem bei der Autorisierung, sondern in erster Linie bei der Authentifizierung. Er tritt eher bei Nicht-Windows-Clients auf. Dieser Fehler kann zurückzuführen sein auf die Verwendung falscher Benutzernamen und Kennwörter für NTLM, nicht übereinstimmende Einstellungen für "LmCompatibility" zwischen Client und Server, doppelte Prinzipalnamen für den Kerberos-Dienst, falsche Kerberos-Diensttickets für die Vergabe von Tickets oder aber auf Gastkonten ohne aktivierten Gastzugriff.
551	Fehler bei der Authentifizierung der SMB-Sitzung Clientname: %11 Clientadresse: %6 Benutzername: %9

Ereignis-ID	Nachricht
	Sitzungs-ID: %7 Status: %4 (%3) SPN: %12 SPN-Überprüfungsrichtlinie: %13 Erläuterung: Dieser Fehler kann auftreten, wenn Sie versuchen, mithilfe falscher Anmeldeinformationen eine Verbindung mit Freigaben herzustellen. Dieser Fehler ist nicht immer ein Hinweis auf ein Problem bei der Autorisierung, sondern in erster Linie bei der Authentifizierung. Er tritt eher bei Nicht-Windows-Clients auf. Dieser Fehler kann zurückzuführen sein auf: die Verwendung falscher Benutzernamen und Kennwörter für NTLM, nicht übereinstimmende LmCompatibility-Einstellungen zwischen Client und Server, einen falschen Dienstprinzipalnamen, doppelte Prinzipalnamen für den Kerberos-Dienst, falsche Kerberos-Diensttickets für die Vergabe von Tickets oder Gastkonten ohne aktivierten Gastzugriff
658	Das Dateihandle für die Datei "%8\%2" wurde durch den Benutzer "%4" über den Computer "%6" ungültig gemacht.
1000	S4U2Self-Authentifizierungsfehler - Der Client konnte mit S4U2Self nicht erneut authentifiziert werden, um Ansprüche anzufordern. Dieses Verhalten kann erwartet werden, wenn das Konto kein Domänenkonto ist.
1001	SRV deaktiviert - Fehler bei der SMB1-Aushandlungsanforderung, weil SMB1 deaktiviert ist.
1001	Ein Client hat versucht, über SMB1 auf den Server zuzugreifen und wurde abgelehnt, weil die Unterstützung der SMB1-Dateifreigabe deaktiviert oder deinstalliert ist. Erläuterung: Die Serverunterstützung für SMB1 wurde von einem Administrator deaktiviert oder deinstalliert. Clients, auf denen Windows XP/Windows Server 2003 R2 oder eine frühere Version ausgeführt wird, können nicht auf diesen Server zugreifen. Clients, auf denen Windows Vista/Windows Server 2008 oder eine höhere Version ausgeführt wird, benötigen kein SMB1 mehr. Um die Clients zu ermitteln, die über SMB1 auf diesen Server zugreifen, aktivieren Sie die SMB1-Zugriffsüberprüfung mit dem Windows PowerShell-Cmdlet "Set-SmbServerConfiguration".
1002	RKF-Fehler - SRV2 kann keine Bestätigung für die Anforderung eines permanenten Handles vom Fortsetzungsschlüsselfilter (RKF) abrufen.
1003	Der Server hat eine unverschlüsselte Nachricht vom Client "%4" empfangen. Die Nachricht wurde abgelehnt. Erläuterung: Dieses Ereignis weist darauf hin, dass ein Client unverschlüsselte Daten sendet, obwohl die SMB-Freigabe die Verschlüsselung erfordert.
1003	Der Server hat eine unverschlüsselte Nachricht vom Client empfangen, obwohl die Verschlüsselung erforderlich ist. Die Nachricht wurde abgelehnt. Clientname: %4 Clientadresse: %8 Benutzername: %6 Sitzungs-ID: %9 Freigabename: %2 Erläuterung: Dieses Ereignis weist darauf hin, dass ein Client unverschlüsselte Daten sendet, obwohl die SMB-Freigabe die Verschlüsselung erfordert.
1004	Der Server hat eine falsch signierte Nachricht vom Client "%2" empfangen. Die Nachricht wurde abgelehnt. Erläuterung: Dieses Ereignis weist darauf hin, dass ein Client eine falsch signierte Anforderung sendet.
1004	Der Server hat eine falsch signierte Nachricht abgelehnt. Clientname: %2 Clientadresse: %6 Benutzername: %4 Sitzungs-ID: %7 Erläuterung: Dieses Ereignis ist ein Hinweis darauf, dass ein Client eine falsch signierte Anforderung sendet.
1005	Der Server konnte die Aushandlung vom Client "%2" nicht überprüfen. Die Verbindung wurde beendet.
1005	Der Server hat eine ungültige Aushandlungsanforderung abgelehnt. Die Verbindung wurde beendet. Clientname: %2 Clientadresse: %6 Benutzername: %4 Sitzungs-ID: %13 Erwarteter Dialekt: %7 Erwartete Funktionen: %8 Erwarteter Sicherheitsmodus: %9 Empfangener Dialekt: %10 Empfangene Funktionen: %11 Empfangener Sicherheitsmodus: %12 Erläuterung: Dieses

Ereignis-ID	Nachricht
	Ereignis ist ein Hinweis darauf, dass ein Client versucht, eine zweite Verbindung mithilfe eines nicht übereinstimmenden Dialekts oder nicht übereinstimmender Funktionen auszuhandeln.
1005	Fehler beim Aushandeln der Integritätsprüfung. Status: %2 Clientname: %4 Clientadresse: %8 Benutzername: %6 Sitzungs-ID: %9 Erläuterung: Dieses Ereignis zeigt an, dass die Aushandlungsanforderung des Clients für das Netzwerk zwischen dem Client und dem Server aufgrund von Fehlern oder eines "Man-in-the-Middle"-Angriffsversuchs geändert wurde. Die Clientverbindung wurde getrennt, um ein Herabsetzen der Sicherheit zu verhindern.
1006	Die Freigabe hat den Zugriff auf den Client verweigert. Clientname: %10 Clientadresse: %6 Benutzername: %8 Sitzungs-ID: %17 Freigabename: %2 Freigabepfad: %4 Status: %16 (%15) Zugeordneter Zugriff: %11 Gewährter Zugriff: %12 Sicherheitsbeschreibung: %14 Erläuterung: Zugriffsverweigerungsfehler treten auf, wenn ein Prinzipal ohne die erforderlichen Berechtigungen auf eine Freigabe zugreift. Dies ist in der Regel ein Hinweis darauf, dass der Prinzipal nicht über die direkten Sicherheitsberechtigungen verfügt oder dass ihm die Mitgliedschaft in einer Gruppe fehlt, die über direkte Zugriffsberechtigungen verfügt. Um die Berechtigungen für die angegebene Freigabe zu bestimmen und zu korrigieren, kann ein Administrator die Registerkarte "Sicherheit" im Eigenschaftendialogfeld des Datei-Explorers, das Windows PowerShell-Modul SMBSHARE oder den Befehl NET SHARE verwenden. Darüber hinaus können Sie mithilfe der Registerkarte "Effektiver Zugriff" im Datei-Explorer das Problem diagnostizieren. Anwendungen genieren möglicherweise Zugriffsverweigerungsfehler beim Versuch, Dateien zunächst in einem Schreibmodus zu öffnen und anschließend in einem schreibgeschützten Modus erneut zu öffnen. In diesem Fall ist keine Benutzeraktion erforderlich. Falls der Zugriff auf die Freigabe verweigert wird und dieses Ereignis nicht protokolliert wird, können Sie die Datei- und Ordnerberechtigungen für NTFS/REFS analysieren. Dieser Fehler ist kein Hinweis auf ein Problem bei der Authentifizierung, sondern nur bei der Autorisierung.
1007	Die Freigabe hat den anonymen Zugriff auf den Client verweigert. Clientname: %8 Clientadresse: %6 Freigabename: %2 Freigabepfad: %4 Erläuterung: Dieser Fehler kann auftreten, wenn ein Client eine Verbindung mit Freigaben herzustellen versucht und keine Anmeldeinformationen eingibt. Dies ist ein Hinweis darauf, dass der Client keinen Benutzernamen (und ggf. Domänenanmeldeinformationen) eingibt. Standardmäßig wird der anonyme Zugriff auf Freigaben verweigert. Dieser Fehler ist nicht immer ein Hinweis auf ein Problem bei der Autorisierung, sondern in erster Linie bei der Authentifizierung. Er tritt eher bei Nicht-Windows-Clients auf.
1009	Der Server hat den anonymen Zugriff auf den Client verweigert. Clientname: %4 Clientadresse: %2

Ereignis-ID	Nachricht
	Sitzungs-ID: %5 Erläuterung: Dieser Fehler kann auftreten, wenn ein Client eine Verbindung mit Freigaben herzustellen versucht und keine Anmeldeinformationen eingibt. Dies ist ein Hinweis darauf, dass der Client keinen Benutzernamen (und ggf. Domänenanmeldeinformationen) eingibt. Standardmäßig verweigert Windows Server den anonymen Zugriff auf Freigaben. Dieser Fehler ist nicht immer ein Hinweis auf ein Problem bei der Autorisierung, sondern in erster Linie bei der Authentifizierung. Er tritt eher bei Nicht-Windows-Clients auf.
1010	Ein Endpunkt wurde hinzugefügt. Name: %2 Domänenname: %4 Transportname: %6 Transportkennzeichen: %7 Erläuterung: Dieser Fehler kann auftreten, wenn der Server mit dem Überwachen einer Schnittstelle beginnt, wie beispielsweise beim Neustart des Systems oder beim Aktivieren eines Netzwerkadapters. Es ist keine Benutzeraktion erforderlich.
1011	Ein Endpunkt wurde entfernt. Name: %2 Domänenname: %4 Transportname: %6 Erläuterung: Dieser Fehler kann auftreten, wenn der Server die Überwachung einer Schnittstelle beendet, wie beispielsweise beim Herunterfahren oder beim Deaktivieren eines Netzwerkadapters. Es ist keine Benutzeraktion erforderlich.
1012	Die Informationen zum Netzwerknamen wurden geändert. Änderungstyp: %1 Netzwerkname: %3 IP-Adresse: %9 Kennzeichen: %4 Schnittstellenindex: %5 Funktion: %6 Übertragungsrate: %7 Erläuterung: Dieses Ereignis kann bei einem Windows-Failoverclusterknoten bei Failovervorgängen, beim Systemstart oder bei der Netzwerkkonfiguration auftreten. Es ist keine Benutzeraktion erforderlich.
1013	Ein Endpunkt wird online geschaltet. Endpunktname: %2 Transportname: %4 Erläuterung: Dieses Ereignis kann bei einem Windows-Failoverclusterknoten bei Failovervorgängen auftreten. Es ist keine Benutzeraktion erforderlich.
1014	Ein Endpunkt wird offline geschaltet. Endpunktname: %2 Transportname: %4

Ereignis-ID	Nachricht
	Erläuterung: Dieses Ereignis kann bei einem Windows-Failoverclusterknoten bei Failovervorgängen auftreten. Es ist keine Benutzeraktion erforderlich.
1015	Fehler beim Entschlüsselungsaufruf. Clientname: %2 Clientadresse: %4 Sitzungs-ID: %7 Status: %6 (%5) Erläuterung: Dieses Ereignis tritt in der Regel auf, da eine frühere SMB-Sitzung nicht mehr vorhanden ist. Es kann auch durch Pakete verursacht werden, die im Netzwerk zwischen den Computern aufgrund von Fehlern oder eines "Man-in-the-Middle"-Angriffsversuchs geändert werden.
1016	Fehler beim erneuten Íffnen. Clientname: %7 Clientadresse: %9 Benutzername: %13 Sitzungs-ID: %14 Freigabename: %11 Dateiname: %16 Fortsetzungsschlüssel: %20 Status: %2 (%1) RKF-Status: %4 (%3) Permanent: %17 Stabil: %18 Beständig: %19 Grund: %21 Erläuterung: Der Client hat versucht, ein fortlaufend verfügbares Handle erneut zu öffnen, aber der Versucht ist fehlgeschlagen. Dies ist in der Regel ein Hinweis auf ein Problem beim Netzwerk oder dass die zugrunde liegende Datei erneut geöffnet wird.
1017	Das Handle wurde bereinigt. Freigabename: %7 Dateiname: %9 Fortsetzungsschlüssel: %5 Beständige Datei-ID: %3 Flüchtige Datei-ID: %4 Permanent: %1 Stabil oder beständig: %2 Erläuterung: Der Server hat ein Handle, das zuvor für einen Client reserviert wurde, nach 60 Sekunden geschlossen. Dieses Ereignis kann auf einem fortlaufend verfügbaren Computer auftreten, wenn die Sitzung von einem Client nicht ordnungsgemäß beendet wird. Beispielsweise, wenn der Client unerwartet neu gestartet wurde.
1018	Backchannelinvalidierung der Sitzung wurde abgeschlossen. Sitzungs-ID: %1 Status: %3 (%2) Aufgabenstatus: %5 (%4)

Ereignis-ID	Nachricht
	Erläuterung: Dieses Ereignis kann auf einem fortlaufend verfügbaren Computer auftreten. Es ist keine Benutzeraktion erforderlich.
1019	Backchannelinvalidierung der Datei wurde abgeschlossen. Fortsetzungsschlüssel: %1 Status: %3 (%2) Aufgabenstatus: %5 (%4) Erläuterung: Dieses Ereignis kann auf einem fortlaufend verfügbaren Computer auftreten. Es ist keine Benutzeraktion erforderlich.
1020	Der Dateisystemvorgang hat länger als erwartet gedauert. Clientname: %8 Clientadresse: %10 Benutzername: %6 Sitzungs-ID: %3 Freigabename: %12 Dateiname: %14 Befehl: %1 Dauer (in Millisekunden): %15 Warnungsschwellenwert (in Millisekunden): %16 Erläuterung: Das zugrunde liegende Dateisystem hat zu lange für die Reaktion auf einen Vorgang benötigt. Dies ist in der Regel ein Hinweis auf ein Problem mit dem Speicher, und nicht mit SMB.
1020	Der Dateisystemvorgang hat länger als erwartet gedauert. Clientname: %8 Clientadresse: %10 Benutzername: %6 Sitzungs-ID: %3 Freigabename: %12 Dateiname: %14 Befehl: %1 Dauer (in Millisekunden): %15 Warnungsschwellenwert (in Millisekunden): %16 Erläuterung: Das zugrunde liegende Dateisystem hat zu lange für die Reaktion auf einen Vorgang benötigt. Dies ist in der Regel ein Hinweis auf ein Problem mit dem Speicher, und nicht mit SMB.
1021	Der Wert für "LmCompatibilityLevel" weicht vom Standardwert ab. Konfigurierter LM-Kompatibilitätsgrad: %1 Standardmäßiger LM-Kompatibilitätsgrad: %2 Erläuterung: Bei der LAN-Manager (LM)-Authentifizierung handelt es sich um das Protokoll, mit dem Windows-Clients für den Netzwerkbetrieb authentifiziert werden. Dies beinhaltet das Hinzufügen einer Domäne, das Zugreifen auf Netzwerkressourcen und das Authentifizieren von Benutzern oder Computern. Dies bestimmt, welches Abfrage/Rückmeldung-Authentifizierungsprotokoll zwischen den Client- und

Ereignis-ID	Nachricht
	Servercomputern ausgehandelt wird. Im Einzelnen bestimmt die LAN-Manager-Authentifizierungsebene, welche Authentifizierungsprotokolle der Client auszuhandeln versucht oder der Server akzeptiert. Der für "LmCompatibilityLevel" festgelegte Wert bestimmt, welches Abfrage/Rückmeldung-Authentifizierungsprotokoll für Netzwerkanmeldungen verwendet wird. Dieser Wert hat Auswirkungen auf die von Clients verwendete Authentifizierungsprotokollebene, die ausgehandelte Sitzungssicherheitsebene sowie die von Servern akzeptierte Authentifizierungsebene. Wert (Einstellung) - Beschreibung 0 (LM- und NTLM-Antworten senden) - Clients verwenden die LM- and NTLM-Authentifizierung, und sie verwenden niemals die NTLMv2-Sitzungssicherheit. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 1 (LM- und NTLM-Antworten senden - NTLMv2-Sitzungssicherheit verwenden, wenn ausgehandelt) - Clients verwenden die LM- und NTLM-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 2 (Nur NTLM-Antworten senden) - Clients verwenden nur die NTLM-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 3 (Nur NTLMv2-Antworten senden) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller akzeptieren die LM-, NTLM- und NTLMv2-Authentifizierung. 4 (Nur NTLMv2-Antwort senden/LM ablehnen) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller lehnen LM ab und akzeptieren nur die NTLM- und NTLMv2-Authentifizierung. 5 (Nur NTLMv2-Antwort senden/LM & NTLM ablehnen) - Clients verwenden nur die NTLMv2-Authentifizierung, und sie verwenden die NTLMv2-Sitzungssicherheit, falls dies vom Server unterstützt wird. Domänencontroller lehnen LM und NTLM ab und akzeptieren nur die NTLMv2-Authentifizierung. Inkompatibel konfigurierte LmCompatibility-Grade zwischen einem Client und einem Server (z.B. 0 auf einem Client und 5 auf einem Server) verhindern den Zugriff auf den Server. Anderes als Microsoft-Clients und -Server weisen diese Konfigurationseinstellungen ebenfalls auf.
1023	Für mindestens eine Freigabe auf diesem Server ist die zugriffsbasierte Aufzählung aktiviert. Erläuterung: Dieses Ereignis kann auftreten, wenn Sie die zugriffsbasierte Aufzählung für mindestens eine Freigabe mit dem Server-Manager oder dem Windows PowerShell-Cmdlet Set-SmbShare aktivieren. Durch die zugriffsbasierte Aufzählung kann die CPU-Auslastung zunehmen, wenn Clients Verbindungen mit Freigaben herstellen, die Ordner mit vielen Ressourcen auf Peerebene enthalten, auf die der Benutzer keinen Zugriff hat. Die CPU-Auslastung können Sie durch Konfigurieren des Werts "ABELevel" in der Windows-Registrierung steuern: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\ABELevel [DWORD]

Ereignis-ID	Nachricht
	Sie können für "ABELevel" mehr Ebenen festlegen, um die CPU-Auslastung zu minimieren. Dadurch nimmt aber auch Effektivität der zugriffsbasierten Aufzählung ab: Wert = 0: die zugriffsbasierte Aufzählung ist für alle Ebenen aktiviert Wert = 1: die zugriffsbasierte Aufzählung ist für eine Ebene aktiviert (Beispiel: \server\share) Wert = 2: die zugriffsbasierte Aufzählung ist für zwei Ebenen aktiviert (Beispiel: \server\share\folder) Sie können weitere Werte für mehrere Tiefenebenen festlegen.
1024	SMB2 und SMB3 wurden auf diesem Server deaktiviert. Dies bedeutet eine Beeinträchtigung der Funktionalität und Leistung. Registrierungsschlüssel: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registrierungswert: Smb2 Standardwert: 1 (oder nicht vorhanden) Aktueller Wert: 0 Erläuterung: Dieses Ereignis kann auftreten, wenn Sie SMB2/SMB3 deaktivieren. Microsoft rät davon ab, SMB2/SMB3 zu deaktivieren. Die Deaktivierung von SMB3 verhindert die Verwendung von Features wie etwa SMB Transparent Failover, SMB Scale Out, SMB Multichannel, SMB Direct (RDMA), SMB Encryption, VSS for SMB File Shares sowie SMB Directory Leasing. SMB bietet in den meisten Fällen eine Möglichkeit der Problembehandlung als Alternative zur Deaktivierung von SMB2/SMB3. Verwenden Sie das Windows PowerShell-Cmdlet Set-SmbServerConfiguration zum Aktivieren von SMB2/SMB3.
1025	Mindestens eine Named Pipe oder Freigabe wurde für den Zugriff durch anonyme Benutzer gekennzeichnet. Dadurch erhöht sich das Sicherheitsrisiko des Computers, da nicht authentifizierte Benutzer eine Verbindung mit diesem Server herstellen können. Registrierungsschlüssel: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registrierungswerte: NullSessionPipes, NullSessionShares Standardwert: leer (oder nicht vorhanden) Aktueller Wert: nicht leer Erläuterung: Dieses Ereignis kann auftreten, wenn Sie die Standardwerte von "NullSessionShares" und "NullSessionPipes" ändern. Auf einem typischen Dateiserver sind diese Einstellungen nicht vorhanden oder enthalten keine Werte, was die sicherste Konfiguration darstellt. Standardmäßig füllen Domänencontroller den Eintrag "NullSessionShares" mit "netlogon", "samr" und "lsarpc" auf, um Legacyzugriffsmethoden zuzulassen.
1026	Das Dateileasing wurde für die SMB2- und SMB3-Protokolle deaktiviert. Dies bedeutet eine Beeinträchtigung der Funktionalität und möglicherweise der Leistung. Registrierungsschlüssel: HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters Registrierungswert: DisableLeasing Standardwert: 0 (oder nicht vorhanden) Aktueller Wert: ungleich Null Erläuterung: Dieses Ereignis kann auftreten, wenn Sie SMB 3 Leasing deaktivieren. Microsoft rät davon ab, SMB Leasing zu deaktivieren. Wenn Sie diese Option deaktivieren, kann der Datenverkehr vom Client zum Server zunehmen, da Metadaten und Daten nicht mehr aus einem lokalen Cache abgerufen werden können.

Ereignis-ID	Nachricht
1027	Die Firewallports für die Datei- und Druckerfreigabe sind aktuell geschlossen. Dies entspricht der Standardkonfiguration für ein System, von dem keine Inhalte freigegeben werden oder das sich in einem öffentlichen Netzwerk befindet. Erläuterung: Dieses Ereignis kann auftreten, wenn für die Windows-Firewall die Regel für die Datei- und Druckerfreigabe deaktiviert ist, wodurch eingehender SMB-Datenverkehr zugelassen wird. Dieses Ereignis tritt auf einem Computer auf, für den keine benutzerdefinierten Freigaben konfiguriert sind. Clients können erst auf SMB-Freigaben auf diesem Computer zugreifen, wenn SMB-Datenverkehr über die Firewall zulässig ist.
1028	Der maximal vom Cluster unterstützte SMB-Dialekt hat sich geändert. NewMaxDialect: %1 OldMaxDialect: %2 Erläuterung: Dieses Ereignis tritt gewöhnlich während eines Upgrades des Windows-Failoverclusters auf. Es ist keine Benutzeraktion erforderlich.
1029	Die Richtlinieneinstellung für die Gruppe 'Reihenfolge der Verschlüsselungssammlung' ist ungültig. Erläuterung: Das Ereignis gibt an, dass ein Administrator einen ungültigen Wert für die Gruppenrichtlinieneinstellung "Computerkonfiguration\Administrative Vorlagen\Netzwerk\LanMan-Server\Reihenfolge der Verschlüsselungssammlung" angegeben hat. Der Server verwendet so lange die Standardreihenfolge der Verschlüsselungssammlung "%1", bis der Fehler behoben ist.
1030	Fehler bei der Anforderung zum Abschluss eines MDL-Lese- oder -Schreibvorgangs. Servername: %2 Freigabename: %4 Dateiname: %6 IsRead: %7 Status: %8 Erläuterung: Der SMB-Server sendet MDL-Abschlussanforderungen bei Beendigung einer gepufferten E/A an ein Dateisystem, um Systemressourcen freizugeben. MDL-Abschlussanforderungen dürfen keine Fehler im Dateisystem und dessen Filtertreibern verursachen. Fehler können zu Speicherverlusten und verschlechterter Systemleistung und -stabilität führen. Filtertreiber eines Nicht-Microsoft-Dateisystems sind die häufigste Ursache für fehlerhafte MDL-Abschlussanforderungen.
1031	Der Server hat ein Problem festgestellt und ein Live-Kernelspeicherabbild zur Sammlung von Debuginformationen erfasst. Ursache: %1 Abbildpfad: %SystemRoot%\LiveKernelReports Erläuterung: Der Server unterstützt das Live Dump-Feature, das bei Erkennung eines Problems ein Kernelspeicherabbild, aber keinen Fehlercode erstellt und keinen Neustart ausführt. Dadurch kann der Microsoft-Support Speicherabbilder ohne Neustart oder manuelle Eingriffe untersuchen. Der Ursachencode gibt den festgestellten Problemtyp an. Verzögerte E/A Der Abschluss eines E/A-Vorgangs dauert unverhältnismäßig lange. Nicht ordnungsgemäß funktionierende Minifiltertreiber von Drittanbieter-Dateisystemen sind eine

Ereignis-ID	Nachricht
	häufige Ursache dieses Problems. Weitere Ursachen sind fehlerhafte Festplatten oder eine clientgesteuerte E/A-Arbeitslast, die weit über die Serverkapazität hinausgeht.
1032	Der Server hat ein Problem festgestellt, konnte jedoch kein Live-Kernelspeicherabbild zur Sammlung von Debuginformationen erfassen. Ursache: %1 Erläuterung: Der Server unterstützt das Live Dump-Feature, das bei Erkennung eines Problems ein Kernelspeicherabbild, aber keinen Fehlercode erstellt und keinen Neustart ausführt. Dadurch kann der Microsoft-Support Speicherabbilder ohne Neustart oder manuelle Eingriffe untersuchen. Der Ursachencode gibt den festgestellten Problemtyp an. In diesem Fall wurde die Serveranforderung zum Erstellen eines Live-Kernelspeicherabbilds zurückgewiesen. Dies ist normalerweise auf die Drosselung von Live-Kernelspeicherabbildern zurückzuführen, wodurch verhindert wird, dass häufige Speicherabbilder zu viel Speicherplatz belegen. Warten Sie entweder, bis die Drosselungsgrenze (normalerweise sieben Tage) abgelaufen ist, oder wenden Sie sich an den Microsoft-Support, um zu erfahren, wie der Drosselungswert überschrieben wird. Dieses Ereignis wird höchstens einmal pro Tag in das Protokoll geschrieben. Das Problem, das zur Anforderung eines Live-Kernelspeicherabbilds durch den Server geführt hat, kann häufiger auftreten. Verzögerte E/A Der Abschluss eines E/A-Vorgangs dauert unverhältnismäßig lange. Nicht ordnungsgemäß funktionierende Minifiltertreiber von Drittanbieter-Dateisystemen sind eine häufige Ursache dieses Problems. Weitere Ursachen sind fehlerhafte Festplatten oder eine clientgesteuerte E/A-Arbeitslast, die weit über die Serverkapazität hinausgeht.
1041	Fehler beim Lesen von FSCTL-Eigenschafteninformationen aus der Registrierung. Der Registrierungswerteintrag %3 wird ignoriert. Fehler: %1
1043	RDMA-Verbindung getrennt. Transportname: %3 Für das Schließen der Verbindung aufgewendete Millisekunden: %1 Anleitung: Das Schließen einer RDMA-Verbindung sollte nicht länger als 2 Minuten dauern. Ein RDMA-E/A, dessen Ausführung ungewöhnlich lange dauert, weist auf ein Problem mit den RDMA-Netzwerkadaptern auf diesem Computer oder dessen Remotehost hin. Wenden Sie sich an Ihren RDMA-Anbieter, um einen aktualisierten Treiber und weitere Informationen zur Problembehandlung zu erhalten.
1800	ZS-Fehler - Fehler beim Festlegen einer ständig verfügbaren Eigenschaft für eine neue oder vorhandene Dateifreigabe, da die Dateifreigabe keine Clusterfreigabe ist.
1801	ZS-Fehler - Fehler beim Festlegen einer ständig verfügbaren Eigenschaft für eine neue oder vorhandene Dateifreigabe, da der Fortsetzungsschlüsselfilter nicht gestartet wurde oder das zugrunde liegende Volume nicht anfügen konnte.
1802	Der Server konnte den nächsten ID-Bereich in der Clusterregistrierung nicht reservieren.
1803	Die Sicherheitsbeschreibung unterscheidet sich vom Standardwert. Pfad: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\%1 Erläuterung: Dies liegt häufig daran, dass die Objektsicherheit durch einen Administrator oder Drittanbieter manuell geändert wurde. Um die Sicherheitseinstellung wieder auf den Standardwert zurückzusetzen, löschen Sie den oben angezeigten Pfad. Microsoft rät davon ab,

Ereignis-ID	Nachricht
	die Standardsicherheit von %1 zu ändern, da Anwendungsinkompatibilitäten oder Sicherheitsprobleme entstehen können.
1905	Der Sever hat die Sitzung im Rahmen einer regelmäßigen Systembereinigung geschlossen. Sitzungs-ID: %1 Instanz-ID: %2 Ursache: %3

Ereignis-IDs: Abs. 5.5.2.1

Ereignis-ID	Nachricht
4100	%3 Kontext: %1 Benutzerdaten: %2
4101	%3 Kontext: %1 Benutzerdaten: %2
4102	%3 Kontext: %1 Benutzerdaten: %2
4103	%3 Kontext: %1 Benutzerdaten: %2
4104	ScriptBlock-Text (%1 von %2) wird erstellt: %3 ScriptBlock-ID: %4 Pfad: %5
4105	Der Aufruf der ScriptBlock-ID wurde gestartet: %1 Runspace-ID: %2
4106	Der Aufruf der ScriptBlock-ID wurde abgeschlossen: %1 Runspace-ID: %2
8193	Das Runspace-Objekt wird erstellt. Instanz-ID: %1
8194	Das RunspacePool-Objekt wird erstellt. InstanceId %1 MinRunspaces %2 MaxRunspaces %3
8195	RunspacePool wird geöffnet.
8196	Die Aktivitäts-ID wird geändert und zugeordnet.
8197	Runspacezustand wurde in %1 geändert.
8198	Es wird versucht, die Sitzungserstellung '%1' für Fehlercode '%2' für Sitzungs-ID %3 zu wiederholen.
12039	Die Aktivitäts-ID wird geändert und zugeordnet.
24577	Von Windows PowerShell ISE wurde begonnen, Skriptdatei "%1" auszuführen.
24578	Von Windows PowerShell ISE wurde begonnen, ein vom Benutzer ausgewähltes Skript aus der Datei "%1" auszuführen.
24579	Der aktuelle Befehl wird durch Windows PowerShell ISE angehalten.
24580	Der Debugger wird durch Windows PowerShell ISE fortgesetzt.
24581	Der Debugger wird durch Windows PowerShell ISE angehalten.
24582	Debuggen wird durch Windows PowerShell ISE schrittweise ausgeführt.
24583	Debuggen wird durch Windows PowerShell ISE übersprungen.
24584	Debuggen wird von Windows PowerShell ISE verlassen.
24592	Sämtliche Haltepunkte werden durch Windows PowerShell ISE aktiviert.
24593	Sämtliche Haltepunkte werden durch Windows PowerShell ISE deaktiviert.
24594	Sämtliche Haltepunkte werden durch Windows PowerShell ISE entfernt.

Ereignis-ID	Nachricht
24595	Der Haltepunkt wird durch Windows PowerShell ISE in Zeilennr. "%1" der Datei "%2" festgelegt.
24596	Der Haltepunkt wird durch Windows PowerShell ISE in Zeilennr. "%1" der Datei "%2" entfernt.
24597	Der Haltepunkt wird durch Windows PowerShell ISE in Zeilennr. "%1" der Datei "%2" aktiviert.
24598	Der Haltepunkt wird durch Windows PowerShell ISE in Zeilennr. "%1" der Datei "%2" deaktiviert.
24599	Der Haltepunkt wurde durch Windows PowerShell ISE in Zeilennr. "%1" der Datei "%2" getroffen.
32784	Runspace-ID: %1 Pipeline-ID: %2. WSMan hat einen Fehler gemeldet mit dem Fehlercode: %3. Fehlermeldung: %4 StackTrace: %5
40961	PowerShell-Konsole wird gestartet.
40962	PowerShell-Konsole ist für Benutzereingaben bereit.
46358	Der Persistenzspeicher hat die angegebene maximale Größe erreicht.
53249	Der geplante Auftrag "%1" wurde zu diesem Zeitpunkt gestartet: %2.
53250	Der geplante Auftrag "%1" wurde zum Zeitpunkt %2 mit dem Zustand "%3" abgeschlossen.
53251	Ausnahme für geplanten Auftrag %1: Meldung: %2 Stapelverfolgung: %3 Interne Ausnahme: %4
53504	Windows PowerShell hat einen IPC-Listeningthread für den Prozess %1 in AppDomain %2 gestartet.
53505	Windows PowerShell hat einen IPC-Listeningthread für Prozess %1 in AppDomain %2 beendet.
53506	Fehler beim Windows PowerShell IPC-Listeningthread für Prozess %1 in AppDomain %2. Fehlermeldung: %3.
53507	Windows PowerShell IPC stellt eine Verbindung mit Prozess %1 in AppDomain %2 für Benutzer %3 her.
53508	Windows PowerShell IPC trennt eine Verbindung mit Prozess %1 in AppDomain %2 für Benutzer %3.

Referenzen

bsi_adm_erh_schb. (28. September 2020). Von https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_2_Ordnungsgem%C3%A4%C3%9Fe_IT-Administration.html abgerufen

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

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

ms_al. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-account-lockout abgerufen

ms_apc. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-audit-policy-change abgerufen

ms_app_group. (4. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-application-group-management abgerufen

ms_attribute_dfl. (28. September 2020). Von https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/d7422d35-448a-451a-8846-6a7def0044df abgerufen

ms_audit_pol. (21. Oktober 2020). Von 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 abgerufen

ms_authpc. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-authentication-policy-change abgerufen

ms_code_integrity. (28. September 2020). Von https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd348642(v=ws.10) abgerufen

ms_comp_acc. (4. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-computer-account-management abgerufen

ms_crash_on_audit_fail. (28. September 2020). Von https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc963220(v=technet.10) abgerufen

ms_crypt_retrv_obj. (28. September 2020). Von https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptretrieveobjectbyurlw abgerufen

ms_domain_attribute_max_join. (28. September 2020). Von https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd391926(v=ws.10) abgerufen

ms_ev_coll. (23. September 2020). Von https://docs.microsoft.com/en-us/windows/win32/wec/creating-an-event-collector-subscription abgerufen

ms_pc. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-process-creation abgerufen

ms_sec_bl_1809. (17. Juli 2020). Von https://www.microsoft.com/en-us/download/details.aspx?id=55319 abgerufen

ms_sec_principal. (28. September 2020). Von https://docs.microsoft.com/en-us/windows/security/identity-protection/access-control/security-principals abgerufen

ms_sens_priv. (21. September 2020). Von https://docs.microsoft.com/de-de/windows/security/threat-protection/auditing/audit-sensitive-privilege-use abgerufen

ms_sgm. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-group-management abgerufen

ms_sl. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-special-logon abgerufen

ms_ssc. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-state-change abgerufen

ms_sse. (16. September 2020). Von https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-security-system-extension abgerufen

ms_sysmon. (10. November 2020). Von https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon abgerufen

ms_task_action. (28. September 2020). Von https://docs.microsoft.com/en-us/windows/win32/taskschd/task-actions abgerufen
ms_wevtutil. (16. September 2020). Von https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/wevtutil abgerufen

Abkürzungen

ACL: Access Control List, 47, 50, 51
ADMX: Administrativen Vorlagen der Gruppenrichtlinien, 13
BSI: Bundesamts für Sicherheit in der Informationstechnik, 3
COM: Component Object Model, 38, 98
CredSSP: Credential Security Support Provider, 29, 71, 110
CSE: Client Side Extension, 43
DLL: Dynamic-link Library, 35, 107, 110
DNS: Domain Name System, 57, 58, 71, 82, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129
FUS: Fast User Switching, 31
IO: Eingabe/Ausgabe, 134
IPSec: Internet Protocol Security, 114, 115
LSA: Local Security Authority, 29, 70, 71, 72, 98, 99, 100
LTSC: Long Term Servicing Channel, 4; long-term servicing channel, 3
MSS: Microsoft Solutions for Security, 13
NTLM: NT (New Technology) LAN Manager, 24, 25, 71, 135, 138, 143
NTP: Network Time Protocol, 6
PKI: Public Key Infrastructure, 40
PNP: Plug-and-Play, 38, 44
RDP: Remote Desktop Protocol, 30, 31
RPC: Remote Procedure Call, 35
SAC: Semi-Annual Channel, 4
SMB: Server Message Block, 23, 36, 57, 58, 59, 60, 129, 131, 132, 133, 135, 136, 137, 138, 139, 141, 142, 144, 145
SPN: Service Principal Name, 36, 138
TBS: TPM Base Service, 37, 53, 111, 112
TGT: Ticket Granting Ticket, 24
TPM: Trusted Platform Module, 37, 47, 53, 54
URL: Uniform Ressource Locator, 40
USB: Universal Serial Bus, 43
UTC: Coordinated Universal Time, 6
WinRM: Windows Remote Management, 102, 103, 104, 106, 107, 108, 109, 110
WMI: Windows Management Instrumentation, 32, 46, 53, 54, 82, 83, 84, 86, 101