Link: https://www.tecchannel.de/a/workshop-log-dateien-auf-windows-systemen-auswerten,2032597

Ereignisse suchen, finden und bewerten
Workshop - Log-Dateien auf Windows-Systemen auswerten

Datum: 09.10.2012
Autor(en): Frank-Michael Schlede

Der Blick in die Event-Logs der Windows-Systeme sollte zu den Standardprozeduren des Administrators gehören. Die Untersuchung dieser großen Datenmenge ist allerdings aufwendig. Dieser Workshop zeigt, wie Filterung und Scripts diese Aufgabe erleichtern können.

Auf einem Windows-Server sind standardmäßig immer mindestens drei Protokolldateien zu finden: das Anwendungs-, das System- und das Sicherheitsprotokoll. Die Anwendungen und Dienste auf einem System verwenden die Anwendungsprotokolldatei, während Gerätetreiber die Systemprotokolldatei für ihre Zwecke einsetzen.

Das gilt natürlich nicht nur für die Server, sondern auch für die Windows-Client-Systeme. Ist diese Überwachung aktiviert, so wird ein solches Windows-System sowohl Erfolgs- als auch entsprechende Fehlerüberwachungsereignisse im Sicherheitsprotokoll generieren.

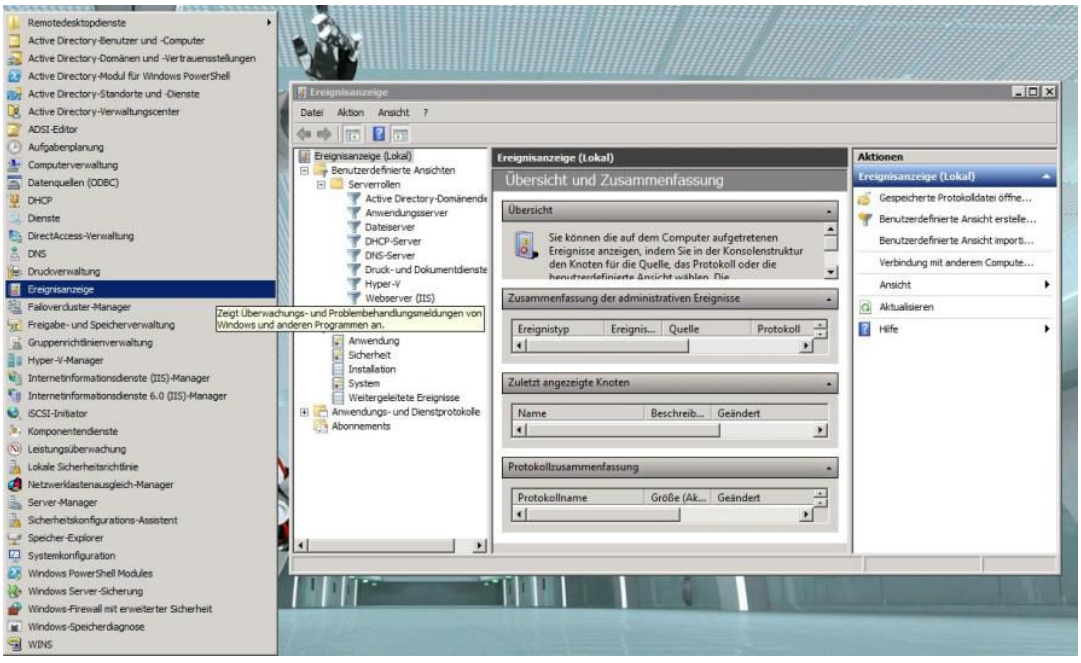
Im professionellen Einsatz werden zudem in der Regel noch eine Reihe anderer Anwendungen, wie beispielsweise der Verzeichnisdienst **Active Directory**[1] (AD), auf dem Server installiert sein, sodass auf diesen Rechnern mit großer Wahrscheinlichkeit noch weitere Standardprotokolldateien zu finden sind. Weiterhin haben die Administratoren die Möglichkeit, eigene selbst definierte Protokolldateien auf einem lokalen oder Remote-Computer zu erstellen.

[Hinweis auf Bildergalerie: **Bildergalerie:**] gal1

Geht man nun von einer nicht allzu großen Firma aus, die 20 Serversysteme besitzt, auf denen im Durchschnitt jeweils fünf verschiedene Log-Dateien 24 Stunden am Tag mit Ereignisdaten gefüllt werden, so kann man sich schnell die Dimension der zu verwaltenden Daten ausmalen, die es im Zweifelsfall zu durchforsten gilt. Der folgende Artikel hilft, diese Aufgabe ein wenig systematischer anzugehen.

1. Das Problem unterschiedlicher Formate

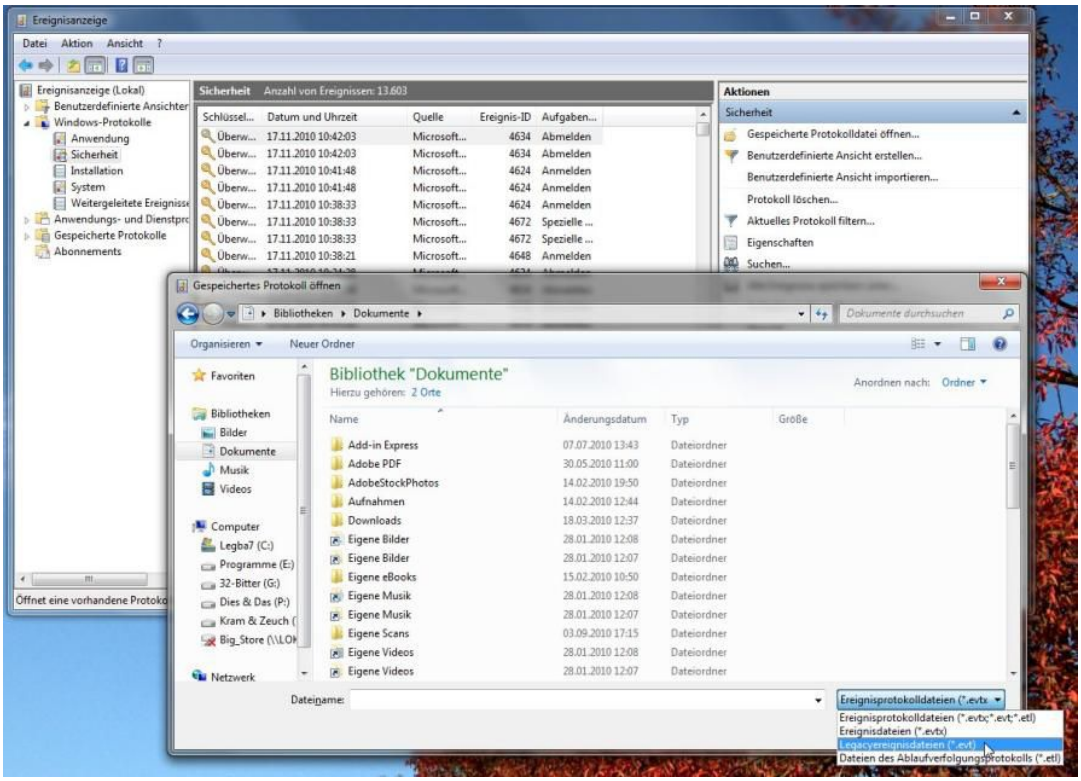
Leider macht es Microsoft den Systemverwaltern auch nicht einfacher: So kommt erschwerend hinzu, dass der Hersteller mit dem Erscheinen von **Windows Vista**[2] und **Windows Server 2008**[3] ein neues, erweitertes Dateiformat für die Protokolldateien eingeführt hat. Dabei wurde das alte EVT-Format, das schon seit Windows NT 4 für die Log-Dateien zum Einsatz kam, durch das neue EVTX-Format ersetzt.



Der Event-Viewer auf einem Windows Server 2008 R2: Er kann auch mit dem alten EVT-Format der Protokolldateien vor Windows Vista umgehen und bietet eine entsprechende Konvertierung der Dateien an.

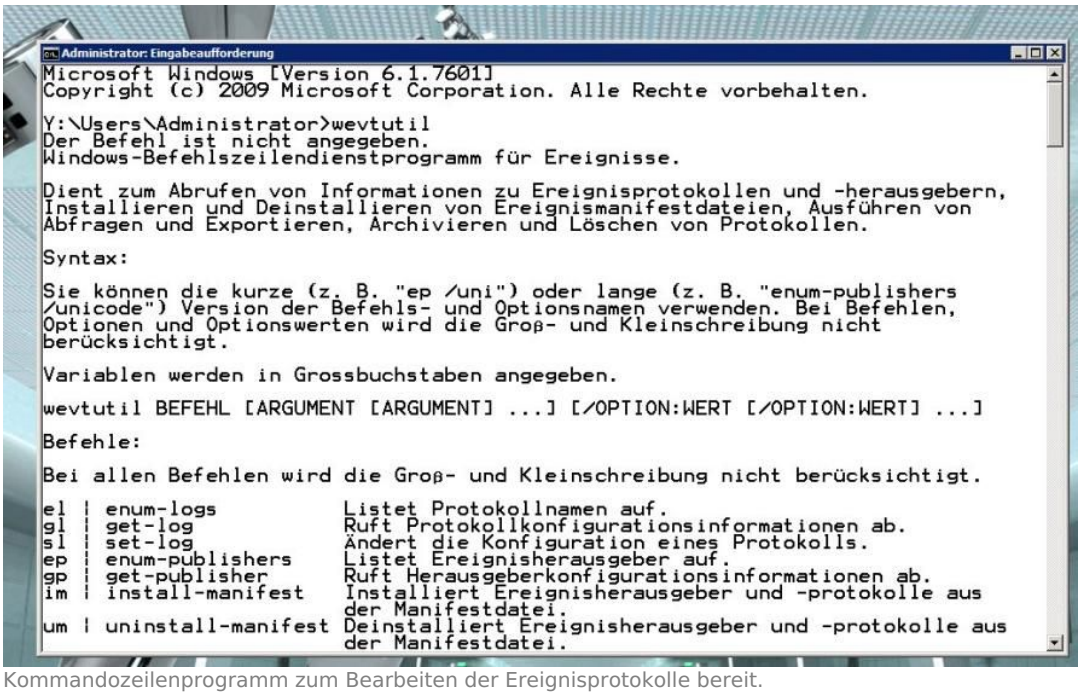
Was kann dieses Format besser? Es bietet nicht nur neue Ereigniseigenschaften (Event Properties), sondern ist zudem in der Lage, sogenannte Kanäle zum Ausgeben von Ereignissen zu verwenden. Ein weiterer Vorteil besteht sicherlich darin, dass dieses EVTX-Format nun zusätzlich auch das Speichern im XML-Format unterstützt.

Für den Administrator bedeuten diese Änderungen zunächst allerdings, dass er sich besonders in Systemumgebungen, in denen sowohl ältere als auch neue Windows-Systeme zum Einsatz kommen, mit einem zusätzlichen Arbeitsaufwand bei Bearbeitung, Verwaltung und Auswertung dieser Log-Dateien konfrontiert sieht.



Ein ähnliches Bild wie auf dem Server: Auch Windows-7-Systeme stellen eine Ereignisanzeige mit den entsprechenden Fähigkeiten zur Verfügung.

Allerdings ist es möglich, mit dem in der MMC (Microsoft Management Console) integrierten Event-Viewer eines aktuellen Windows-Systems eine alte EVT-Datei zu öffnen, die beispielsweise auf einem XP-System angelegt wurde - umgekehrt funktioniert das natürlich nicht. Die Software weist den Anwendern dann auch sogleich darauf hin, dass eine bessere Navigation in dieser Datei sowie eine Analyse im neuen EVTX-Format möglich sind, und bietet automatisch eine entsprechende Konvertierung an.



Sehr nützlich in Batch- und Script-Dateien: Auf den Windows-Systemen steht auch ein mächtiges Kommandozeilenprogramm zum Bearbeiten der Ereignisprotokolle bereit.

Weiterhin stellt Microsoft auf den aktuellen Windows-Systemen ein Kommandozeilen-Werkzeug mit dem Namen wevtutil.exe zur Verfügung. Es ermöglicht ebenfalls eine Konvertierung der Protokolldateien und kann zudem zur Analyse und Manipulation der Ereignisprotokolle verwendet werden. Allerdings sind diese beiden Standardmöglichkeiten der Windows-Betriebssysteme in der täglichen Praxis weder einfach einzusetzen noch besonders praktisch.

2. Werkzeuge für den Weg zur richtigen Information

So ist es auch kein Geheimnis, dass sich die Suche in den Ereignisprotokollen nicht gerade großer Beliebtheit bei Administratoren und Systembetreuern erfreut. Daher verwundert es kaum, dass Support-Mitarbeiter ihre Frage "Haben Sie schon im Ereignisprotokoll nachgeschaut?" zumeist mit einem "Nein" oder "Daran hab‘ ich nicht gedacht …" beantwortet bekommen.

Aber es existiert eine Reihe von Techniken, die eine Suche in den Log-Dateien vereinfachen können. Zudem bietet die Ereignisanzeige seit dem Erscheinen von Windows Server 2008 einige zusätzliche, sehr hilfreiche Fähigkeiten, und schließlich existiert ja auch noch die PowerShell, deren Einsatz als eine Art Universalwerkzeug für Systemverwalter auch in diesem Fall sehr hilfreich sein kann.

Die Ereignisanzeige ist auf einem Windows Server 2008 oder 2008 R2 zunächst einmal schnell und einfach zu erreichen:

1. Öffnen Sie das Startmenü des Servers.

2. Wählen Sie anschließend den Punkt "Verwaltung" auf, der Ihnen eine Liste mit den standardmäßig zur Verfügung stehenden Verwaltungsprogrammen anbietet.

3. Dort können Sie dann die Ereignisanzeige auswählen.

Schneller geht es auf einem Windows Server 2008, genauso wie auf den Windows-7-Systemen, wenn man im Suchfeld des Startmenüs einfach die ersten Buchstaben des gewünschten Programms eingibt und dann auf den vom System präsentierten Link zu klickt.

Nun stehen Sie als Systembetreuer aber vor dem Problem, beispielsweise nach einem Beweis für einen bestimmten Vorgang auf Ihrem Server oder gar für ein Sicherheitsvorkommnis in dieser riesigen Datenmenge zu suchen: Wonach soll man da am besten suchen, um schnell zu Ergebnissen zu kommen? Nach einem bestimmten String? Nach Nachrichten, Daten oder Event-Typen?

Schließlich stehen auch noch Dinge wie Event-Kategorien zur Verfügung, nach denen die Ereignisse gegliedert und - hoffentlich - gefunden werden könnten. In der Praxis wird es häufig so sein: Ein Administrator vermutet, dass ein Ereignis stattgefunden hat und dass sein System dazu auch einen Eintrag in einem Log angelegt hat, aber er weiß nicht sicher, welcher Beweis für das vermutete Ereignis in dieser Log-Datei existiert.

3. Der Schlüssel: Die Ereignis-ID führt zum Ziel

Für die Fehlersuche, beziehungsweise für die grundsätzliche Überwachung und Kontrolle eines Windows-Servers mithilfe der Ereignisprotokolle, ist es also sehr wichtig zu wissen, wonach man zu suchen hat: Dabei hat es sich in der Praxis als der effizienteste Weg erwiesen, jeweils mittels der Ereignis-ID (Event ID) nach einem bestimmten Vorfall Ausschau zu halten.

Das bedeutet für den Administrator, dass er wissen muss, welche Ereignis-ID für ein spezifisches Ereignis steht. Alle Event-IDs des Windows Servers 2008 sind auf dem **TechNet**[4] von Microsoft dokumentiert, allerdings stehen keine kompletten Listen wirklich sämtlicher IDs, sondern nur nach Ereigniskategorien getrennte zur Verfügung. So können Sie beispielsweise bei Microsoft eine **Beschreibung der Sicherheitsereignisse und der ihnen zugeordneten Ereignis-IDs**[5] finden. Diese Liste bezieht sich explizit auf die neuen Windows-Systeme wie **Windows 7**[6] und Windows Server 2008 R2, denn auch hier hat Microsoft mal wieder einige Änderungen mit dem Wechsel des jeweilige Betriebssystem-Releases vorgenommen.

So verwenden die Ereignis-IDs auf Systemen unter Windows Server 2008 ein anderes System zur Nummerierung als die vorherigen Windows-Versionen. Beispielsweise wird ein "Account Lockout" (der Zugriff auf ein Nutzerkonto wird nach einer bestimmten Anzahl von Versuchen gesperrt) auf den Servern unter Windows 2000 und Windows 2003 mit der ID 644 notiert, während die neuen Windows-Systeme ab dem Windows Server 2008 dafür die ID 4740 vermerken.

Das bedeutet aber leider auch, dass bereits existierende Scripts, die bisher die **Ereignisprotokolle unter Windows Server 2003**[7] oder älteren Systemen nach einer bestimmten ID abgesucht haben, nun unter Windows Server 2008 nicht mehr eingesetzt werden können.

4. Übersicht wichtiger Ereignis-IDs

Die folgende Tabelle zeigt einige interessante und wichtige IDs, die von den neuen Windows-Systemen verwendet werden. Eine **ausführliche Auflistung**[8] ist wiederum bei Microsoft zu finden.

Die meisten Events, die wir beispielhaft in dieser Tabelle aufgeführt haben, stehen im Zusammenhang mit Sicherheitsvorfällen auf dem System. Einige dieser Ereignisse können sich zwar als völlig belanglos erweisen, wenn sie aber sehr häufig und regelmäßig auf einem oder mehreren Ihrer Server auftauchen, kann es sinnvoll sein, diese genauer zu untersuchen.

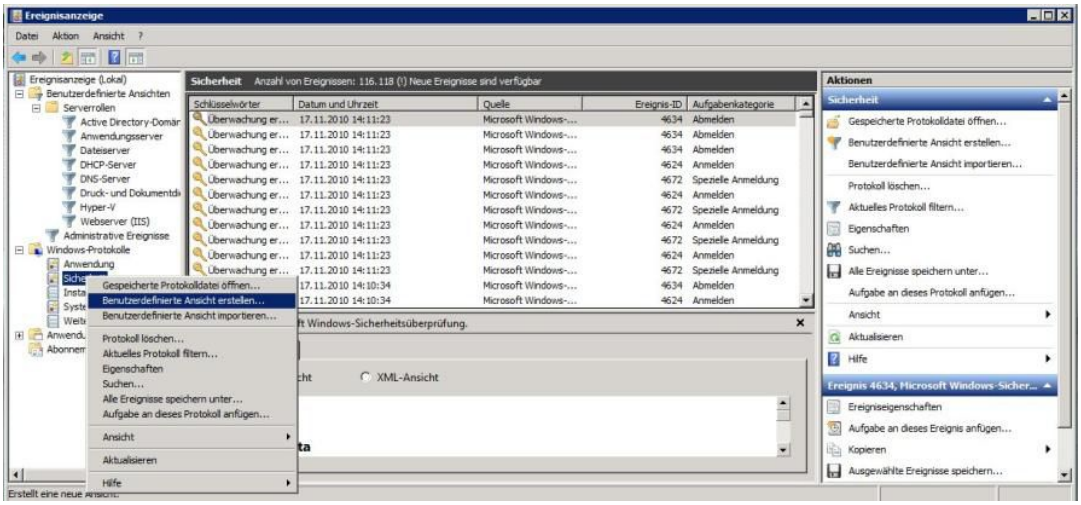
Wichtige Ereignis-IDs

ID	Meldung	Kategorie	Unterkategorie

4777	Ein Konto wurde für die Anmeldung zugeordnet	Kontoanmeldung	Überprüfung der Anmeldeinformation
4771	Kerberos-Vorbestätigung ist fehlgeschlagen	Kontoanmeldung	Kerberos-Authentifizierungsdienst
4772	Kerberos-Vorbestätigung ist fehlgeschlagen.	Kontoanmeldung	Kerberos-Authentifizierungsdienst
4723	Es wurde versucht, ein Kontokennwort zu ändern.	Kontoverwaltung	User Account Management
4738	Ein Benutzerkonto wurde geändert.	Kontoverwaltung	User Account Management
4740	Ein Benutzerkonto wurde gesperrt.	Kontoverwaltung	User Account Management
4780	Die ACL wurde für Konten festgelegt, die Mitglieder der Gruppenadministratoren sind.	Kontoverwaltung	User Account Management
4649	Ein Replay-Angriff wurde festgestellt.	Anmelden/Abmelden	Andere An-/Abmelde-Ereignisse
5378	Die angeforderte Anmeldeinformationen-Delegierung wurde durch die Richtlinie nicht zugelassen.	Anmelden/Abmelden	Andere An-/Abmelde-Ereignisse
4621	Administratorsystem vom CrashOnAuditFail wiederhergestellt. Benutzer, die keine Administratoren sind, können sich nun anmelden.	System	Security-Status ändern

5. Nützliches Werkzeug: Filtern und eigene Sichten

Einen schnellen und gangbaren Weg dazu bieten die Filtermöglichkeiten, die Sie an dieser Stelle verwenden können, um die Anzahl der angezeigten Daten in einer bestimmen Log-Datei deutlich zu reduzieren.



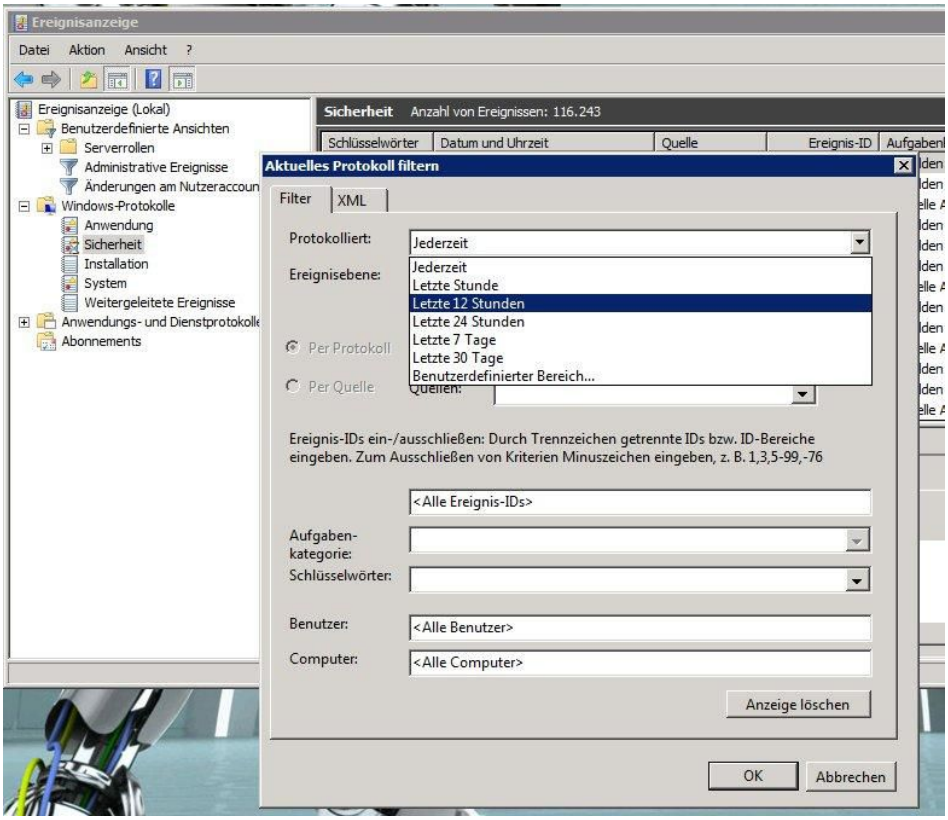
Erleichtert den Überblick enorm: Mithilfe der benutzerdefinierten Ansichten können die Daten aus den Ereignisprotokollen gefiltert werden.

Diese Filter standen auch schon auf Windows Server 2003 zur Verfügung und können auf Server 2008 in der gleichen Art und Weise verwendet werden. Diese stellen Ihnen nur einen augenblicklichen "View" auf die Daten zur Verfügung, sind also nicht permanent. Das System bieten Ihnen aber die Möglichkeit, eine benutzerdefinierte Ansicht in eine XML-Datei abzuspeichern, die dann später wieder in die Ereignisanzeige importiert und auf die Daten angewendet werden kann.

Wenn Sie einen Filter auf einem Windows Server 2008 verwenden wollen, müssen Sie die folgenden Schritte durchführen:

1. Öffnen Sie, wie zuvor beschrieben, die Ereignisanzeige.

2. Wählen Sie das Log aus, das Sie filtern möchten. Sie können entweder über einen Klick auf den entsprechenden Eintrag im Bereich Aktionen der MMC oder durch einen Rechtsklick auf das Log aus dem KontextmenüAktuelles Protokoll filtern... auswählen.



Ein eigener "Blick" auf die vielen Daten wird entworfen: Durch die Filter ist es möglich, sehr viel genauer nach bestimmten Ereignissen zu suchen.

3. Daraufhin wird das Fenster "Aktuelles Protokoll filtern" geöffnet. Hier steht Ihnen nun eine ganze Reihe von Möglichkeiten zur Verfügung, wie sie filtern können. So können Sie beispielsweise nur die Ereignisse auswählen, die innerhalb der vergangenen zwölf Stunden auf dem System aufgetreten sind.

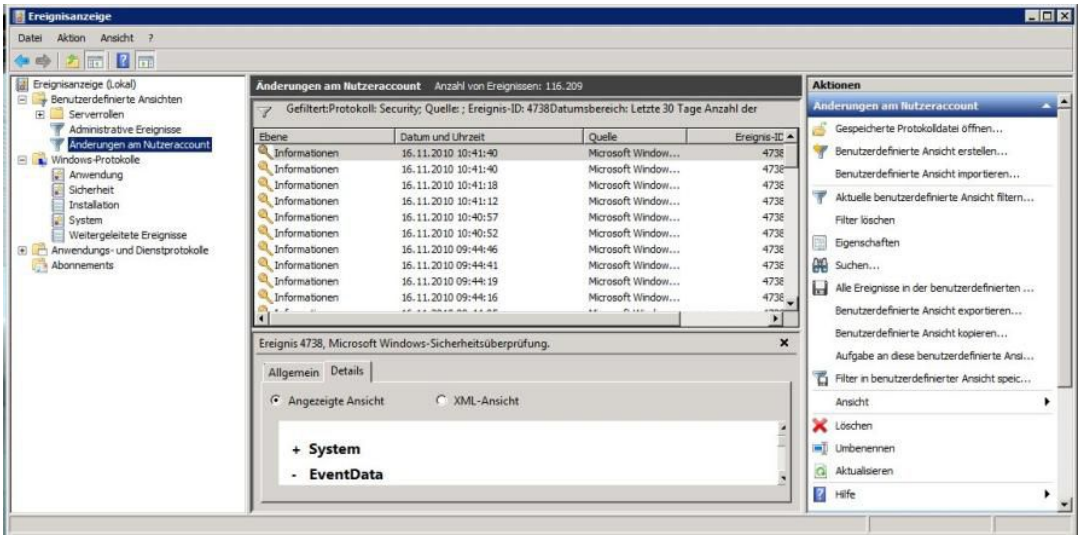
4. Weiterhin steht Ihnen an dieser Stelle die Möglichkeit offen, nach den unterschiedlichen Event-Quellen oder nach Schlüsselwörtern beziehungsweise Anwendern oder Systemen zu suchen. Hier können Sie auch nach einer ganz spezifischen Ereignis-ID suchen.

6. Benutzerdefinierte Ansichten - Suche eingrenzen

Wie bereits erwähnt, stellt sich die Suche nach einer genau spezifizierten Ereignis-ID in der Praxis zumeist als der beste Weg heraus, einem Vorfall auf einem Serversystem schnell auf die Spur zu kommen.

Der Nachteil dieses Ansatzes besteht darin, dass ein Administrator bereits die Ereignis-ID kennen muss, nach der suchen will. Die Möglichkeit, nach einem bestimmten Anwender zu suchen erscheint auf den ersten Blick als probates Mittel, die Aktivitäten eines Anwenders zu finden.

Leider zeigt diese Suchmethode nicht alle Ereignisse an, die einen bestimmten Nutzer auf diesem System betreffen. Ist beispielsweise ein "Anmelde-Ereignis" eines Kontos mit einem Anwender "N/A" verbunden, so können Sie den Nutzernamen, unter dem er angemeldet war, nur sehen, indem Sie im Datenfeld des entsprechenden Ereignisses nachschauen. Auch eine Suche nach Schlüsselwörtern bietet die Filterfunktionalität an, doch diese ist auf bestimmte vorgegebene Schlüsselwörter beschränkt, und eine freie Suche ist hier nicht möglich.



Eine benutzerdefinierte Ansicht - eine der Neuerungen, die mit Windows Server 2008 eingeführt wurden. Hier wurde eine solche Ansicht für alle Events mit der ID 4738 entworfen.

Erst mit Windows Server 2008 ist es schließlich möglich, die benutzerdefinierten Ansichten zu entwerfen, abzuspeichern und auf mehrere verschiedenen Ereignisprotokolle beliebig anzuwenden. Beim Anlegen einer solchen Ansicht gehen Sie folgendermaßen vor:

1. Öffnen Sie die Ereignisanzeige.

2. Mit einem Rechtsklick auf den Knoten Benutzerdefinierte Ansichten im linken Panel der Ereignisanzeige wählen Sie Benutzerdefinierte Ansicht erstellen... aus.

3. Das Fenster, das nun erscheint, gleicht im Prinzip dem zuvor geschilderten Filter. Allerdings besitzen Sie hier nun die Möglichkeit, Daten von mehreren Log-Dateien zu extrahieren. Die Optionen, die Ihnen zur Verfügung stehen, entsprechen dabei jenen, die auch von der Filterfunktionalität angeboten werden.

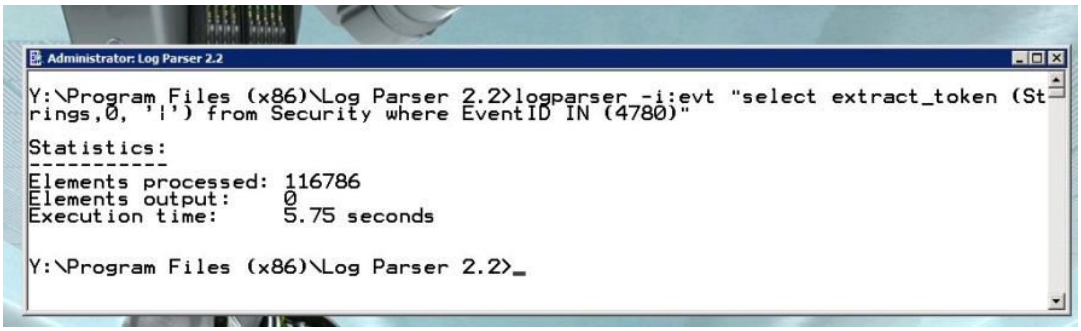
Der wichtigste Zusatznutzen, der mit diesem Feature für die Systembetreuer bereitgestellt wird, besteht ohne Zweifel darin, dass Sie entsprechende benutzerdefinierte Ansichten ex- und wieder importieren und so auch auf mehreren Maschinen im Netz problemlos einsetzen können.

7. Zugriff von der Kommandozeile und mithilfe der PowerShell

Wer die Ereignisprotokolldateien mithilfe von Scripts auslesen und auswerten möchte, kann dazu mehre Wege einschlagen. Viele Administratoren dürften ein spezielles Microsoft-Tool kennen, das schon eine ganze Zeit lang zur Verfügung steht: den Log Parser.

Aktuell steht diese Software in der Version 2.2 zum **kostenlosen Download**[9] bereit. Obwohl auf dieser Seite vermerkt wird, dass diese Software nur für Windows 2000, Windows XP und Server 2003 geeignet sei, arbeitet sie problemlos mit Windows Server 2008 R2 zusammen.

Der Vorteil dieser Lösung besteht darin, dass Sie damit eine Log-Datei mithilfe einer SQL-ähnlichen Syntax abarbeiten können. Allerdings sind Syntax und Einsatzmöglichkeiten dieser Software so umfangreich und damit entsprechend komplex, dass eine genauere Beschreibung ihres Einsatzes den Umfang dieses Artikels bei Weitem sprengen würde.



Das kostenlose Werkzeug Log Parser: Es bietet umfangreiche Möglichkeiten, die Ereignisprotokolle direkt von der Kommandozeile abzufragen, ist aber veraltet und besitzt eine sehr komplexe Syntax.

Neben Beispielen im **Script-Center des TechNets**[10] besitzt die Software selbst eine ganze Reihe von Hilfefunktionalitäten, die zudem eine ganze Reihe von - auch komplexeren - Beispielen beinhalten. Alle Systemadministratoren, die sich auf diese Software verlassen, sollten aber immer bedenken, dass sie seit 2005 kein Update mehr erfahren hat.

Deshalb ist es sicher weitaus sinnvoller, mit der PowerShell zu arbeiten. Sie bietet mit dem Cmdlet Get-Eventlog eine sehr gute Möglichkeit, auf die entsprechenden Daten zuzugreifen. War es bis zu Windows Server 2008 nicht möglich, sie auch auf den **Core-Systemen**[11] (Windows-Server-Installationen ohne grafische Oberfläche) einzusetzen, so ist diese Einschränkung seit der Verfügbarkeit der R2-Version von Windows Server 2008 aufgehoben: Mit der aktuellen PowerShell 2.0 können die entsprechenden Scripts nun auch auf dieser Plattform laufen - für Administratoren ein entscheidender Vorteil.

8. Log-Dateien untersuchen

Bevor Sie nun beginnen, mithilfe dieses PowerShell-Kommandos die verschiedenen Log-Dateien zu untersuchen, sollten Sie unbedingt noch einen wichtigen Hinweis beachten: Alle Cmdlets, die in ihrem Namen das Substantiv "EventLog" beinhalten, können nur mit dem klassischen Format der Ereignisprotokolle zusammenarbeiten; sie sind nicht in der Lage, die Erweiterungen des neuen EXVT-Formats zu verarbeiten. Dazu gehören auch die folgenden Kommandos:

Clear-Eventlog,

Limit-Eventlog,

New-Eventlog ,

RemoveEventlog,

ShowEventlog und

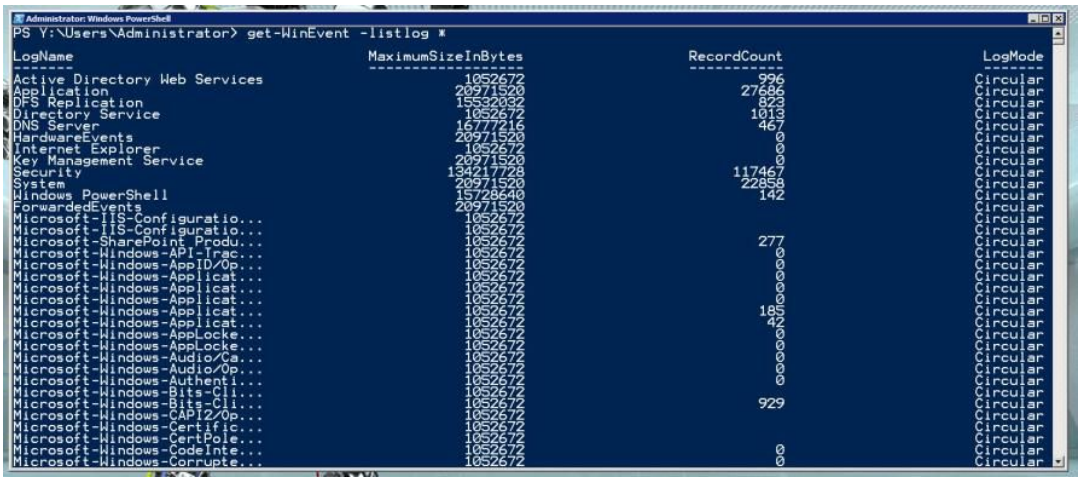
WriteEventlog.

Mit diesen Kommandos können Sie natürlich auch auf Windows Server 2008 R2 oder Windows 7 auf die "klassischen" Ereignisdateien wie System, Sicherheit und Anwendungen zugreifen. Wollen Sie hingegen auf die vielen speziellen Log-Dateien und neuere Features zugreifen, so sollten Sie dazu das Cmdlet Get-WinEvent einsetzen. Es erfordert den Einsatz von Windows Vista, Windows Server 2008 R2 oder eine höhere Version. Zudem wird das Microsoft .NET Framework in der Version 3.5 oder höher benötigt.

9. Beispiele

Ein einfacher Aufruf dieses Kommandos in der folgenden Form zeigt Ihnen dann all die Ereignisprotokolle an, die Sie auf dem System mit seiner Hilfe auslesen können:

```
Get-WinEvent -listlog *
```



Die komplette Liste: Der Get-WinEvent-Befehl zeigt alle vorhandenen Protokolle auf dem lokalen System an und steht nur auf den modernen Windows-Versionen zur Verfügung.

Dabei handelt es sich um eine ziemlich lange Liste, da auf einem aktuellen Windows-Server leicht mehr als 100 Protokolle angezeigt werden. Wie in unserem Beispiel gezeigt, veranlasst das Metazeichen "*" hinter dem Parameter -listlog den Befehl, alle auf dem aktuellen System vorhandenen Protokolle aufzulisten. Wollen Sie nur bestimmte Log-Dateien anzeigen, so gelingt das durch Modifikation des Befehls genauso leicht:

```
Get-WinEvent -listlog *Security *
```

Dieser Befehl wird Ihnen alle Protokolldateien anzeigen, in deren Namen an beliebiger Stelle der Begriff "security" auftaucht. Lassen Sie hingegen den Parameter -listlog weg, so werden Ihnen die eigentlichen Ereignisse in den Sicherheitsprotokollen aufgelistet:

```
Get-WinEvent Security
```

Auch bei diesem Aufruf sind es wieder sehr, sehr viele Ereignisse, die von der PowerShell auf dem Bildschirm angezeigt werden. Da ist es auf jeden Fall weitaus sinnvoller, entsprechende Einschränkungen direkt beim Aufruf des Cmdlets mitzugeben. Geben Sie ein:

```
Get-WinEvent Security -MaxEvents 5
```

und Sie bekommen nur noch die letzten fünf aktuellen Ereignisse aus der entsprechenden Protokolldatei (in diesem Fall "Sicherheit") aufgelistet.

Das "alte" Kommando Get-Eventlog bietet Ihnen hier noch eine breitere Auswahl an Parametern an, mit deren Hilfe beispielsweise nur die Einträge nach einem bestimmten Datum angezeigt werden können:

```
Get-Eventlog Security -after 16/11/2010
```

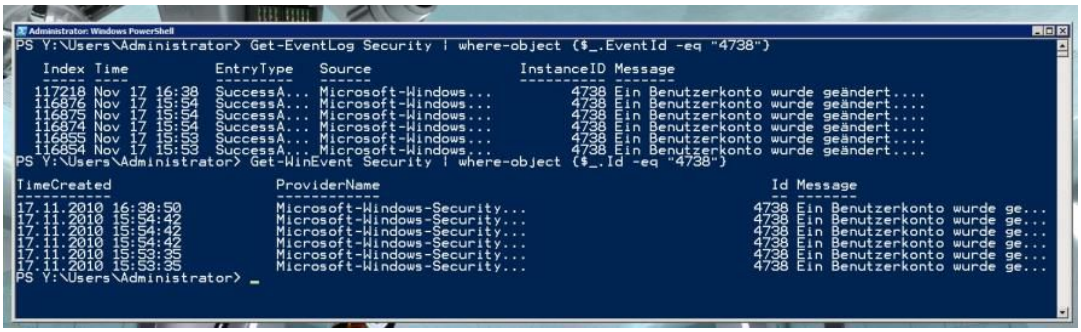
Aber nicht nur bei den Parametern haben die Entwickler der PowerShell zwischen den Versionen und zwischen den beiden eigentlich so ähnlichen Befehlen Get-EventLog und Get-WinEvent doch deutliche Unterschiede eingebaut, die bei einer Portierung oder beim Einsatz in Umgebungen mit alten und neuen Windows-Systemen zu Problemen führen können.

Auch die Eigenschaften (Properties) der einzelnen Objekte haben sich geändert. Der Aufruf:

```
Get-Eventlog Security |where-object {$_.EvenId -eq "4738"}
```

muss beim Einsatz des Get-WinEvent Cmdlets ein wenig anders lauten:

```
Get-WinEvent Security | where-object {$_.Id -eq "4738"}
```



Kleine, aber wichtige Unterschiede: Auch wenn beide Befehle auf dem aktuellen Window-Server funktionieren, sollte man vor ihrem Einsatz unbedingt die Details bei Syntax, Parametern und Eigenschaften beachten.

Administratoren und Systemverwalter, die diese Art von PowerShell-Befehlen in ihren Verwaltungs-Scripts auf den Serversystemen einsetzen wollen, sollten also vorher ganz genau evaluieren, auf welche Systeme mit welchen Windows-Versionen sie diese "loslassen".

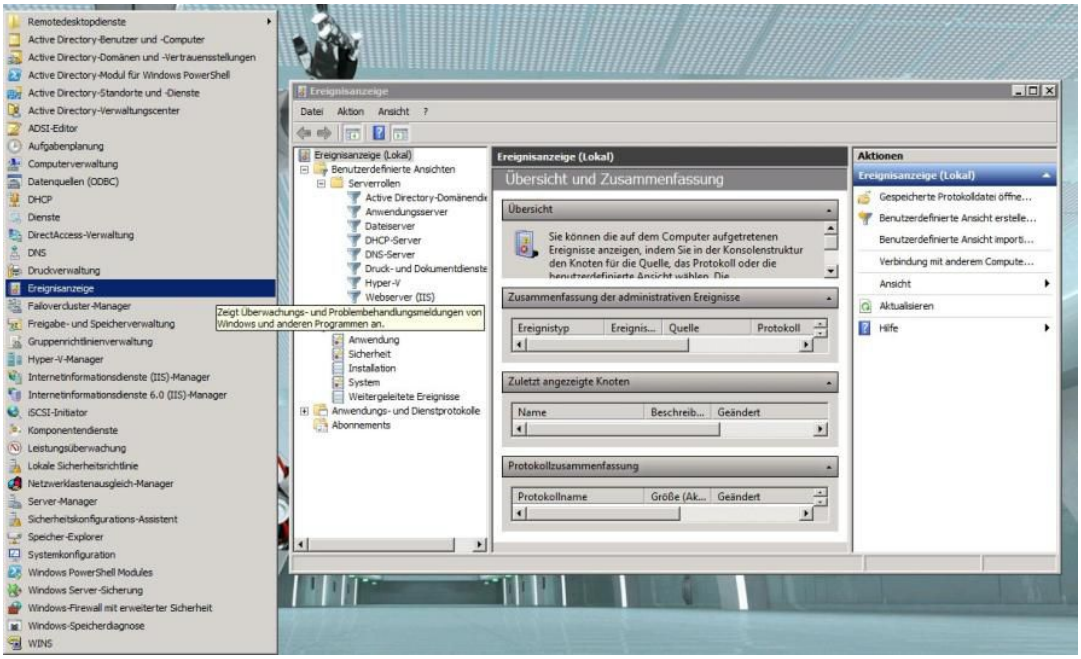
Wie immer beim Einsatz von PowerShell-Befehlen empfiehlt sich auch hier ein genaues Studium der Online-Hilfe mittels des Get-Help-Befehls, der durch die Erweiterung -examples immer anschauliche und gut erklärte Beispiele zu bieten hat. (mje)

Links im Artikel:

[1] **https://www.tecchannel.de/server/windows/2021722/windows_server_2008_r2_active_directory_windows_7_fuer_server/**
[2] **https://www.tecchannel.de/produkte/pc-mobil/betriebssystem/microsoft-windows-vista/**
[3] **https://www.tecchannel.de/produkte/server/betriebssystem/microsoft-windows-server-2008-r2/**
[4] **http://technet.microsoft.com/de-de/default.aspx**
[5] **http://support.microsoft.com/kb/977519/en-us**
[6] **https://www.tecchannel.de/produkte/pc-mobil/betriebssystem/microsoft-windows-7/**
[7] **https://www.tecchannel.de/server/windows/402510/windows_server_2003_ueberwachen_die_ereignisprotokolle/**
[8] **http://support.microsoft.com/kb/947226/de**
[9] **http://www.microsoft.com/downloads/en/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07&displaylang=en**
[10] **http://technet.microsoft.com/de-de/scriptcenter/default.aspx**
[11] **https://www.tecchannel.de/server/windows/481641/windows_server_2008_abgespeckt_die_core_installation/**

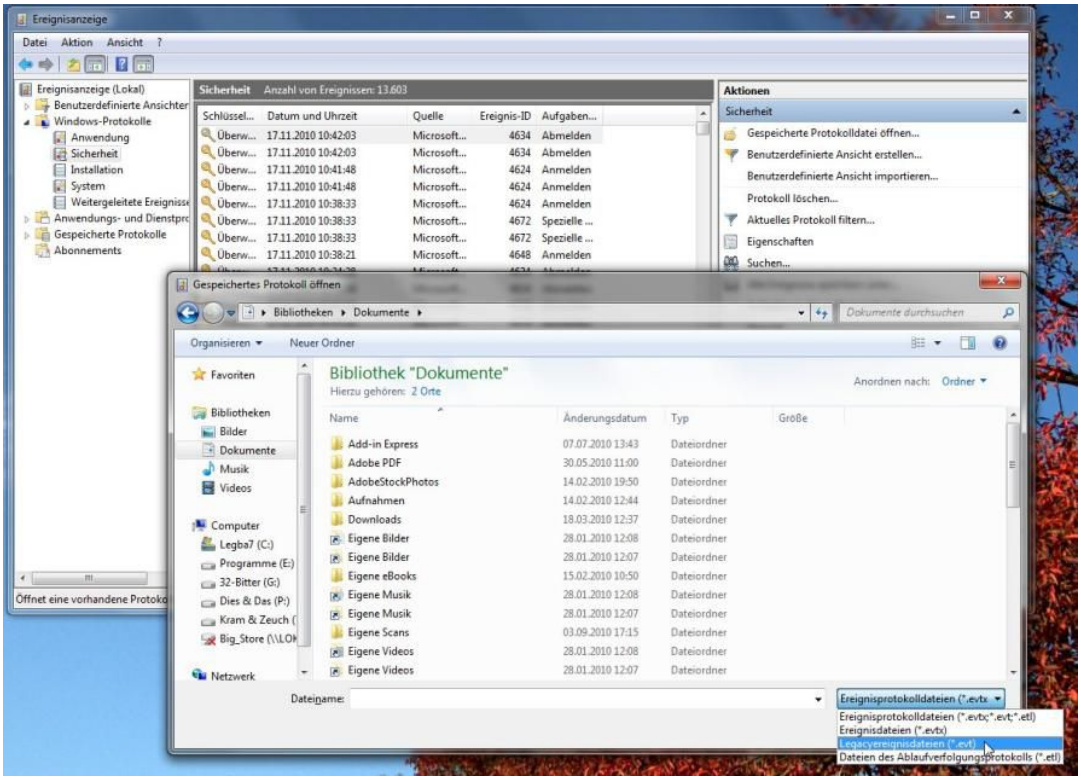
Bildergalerien im Artikel:

gal1 **Bildergalerie:**



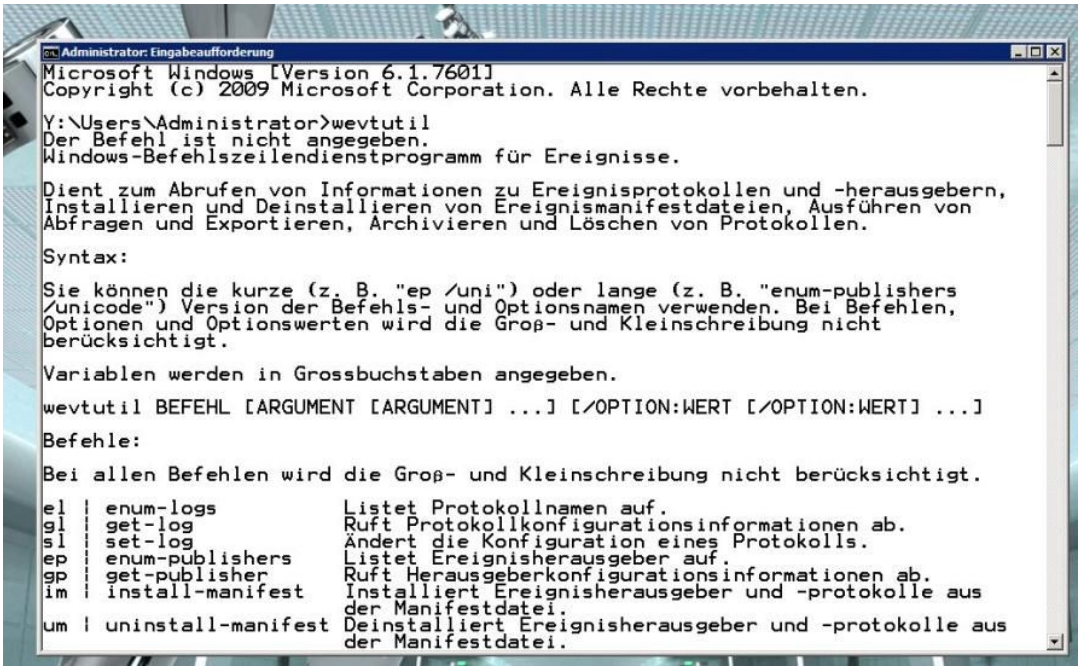
Log-Dateien auswerten

Der Event-Viewer auf einem Windows Server 2008 R2: Er kann auch mit dem alten EVT-Format der Protokoll-Dateien vor Windows Vista umgehen und bietet eine entsprechende Konvertierung der Dateien an.



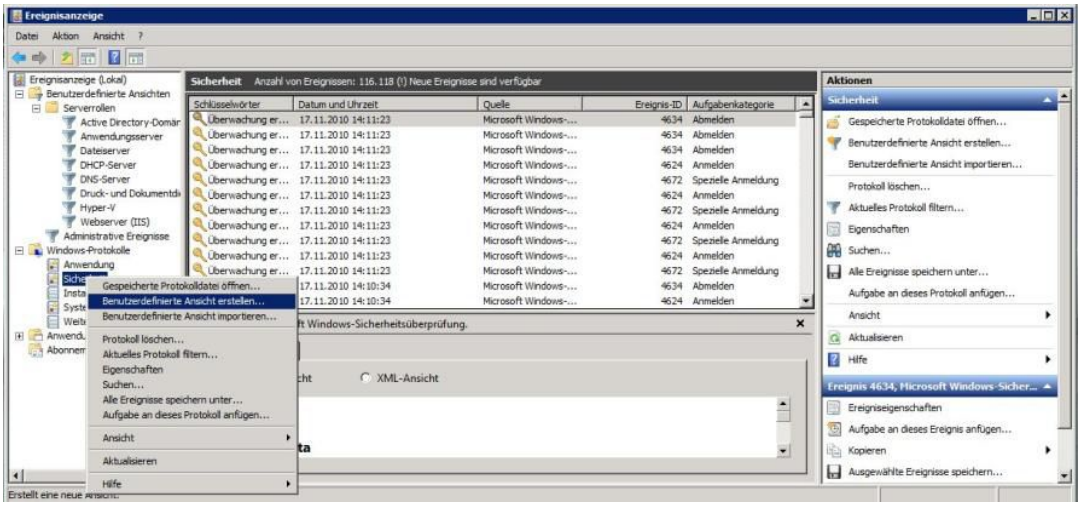
Log-Dateien auswerten

Ein ganz ähnliches Bild wie auf dem Server: Auch Windows-7-Systeme stellen natürlich eine Ereignisanzeige mit den entsprechenden Fähigkeiten zur Verfügung.

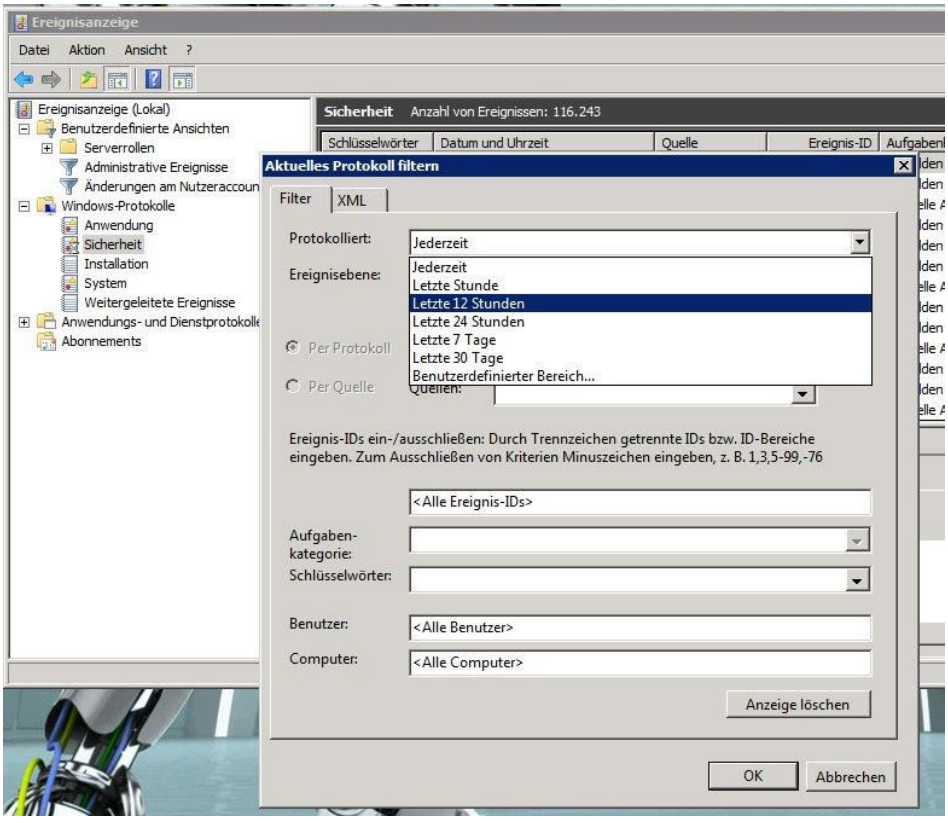


Kommandozeilenprogramm zum Bearbeiten der Ereignisprotokolle bereit.

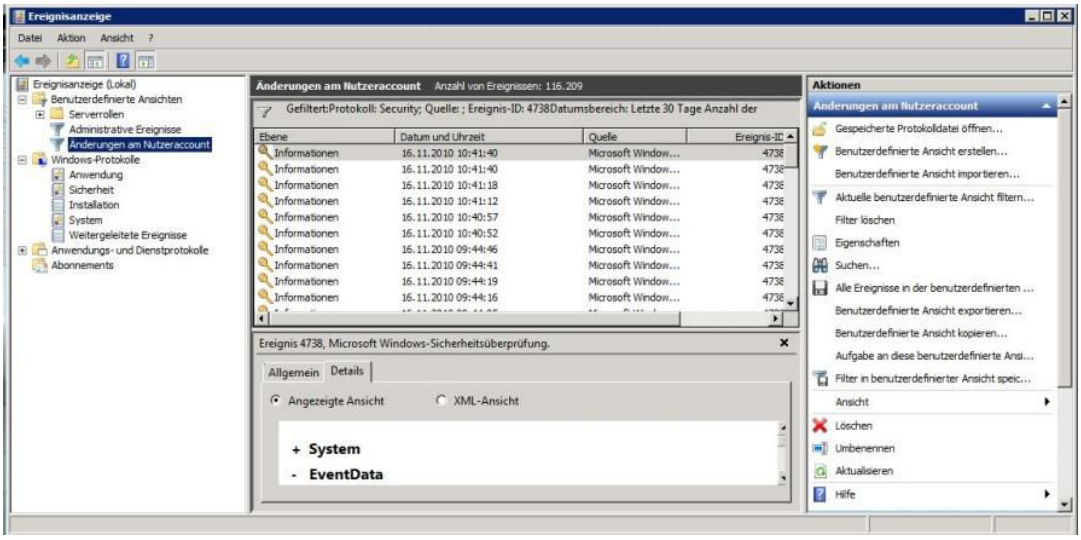
Log-Dateien auswerten
Sehr nützlich in Batch- und Script-Dateien: Auf den Windows-Systemen steht auch ein mächtiges



Log-Dateien auswerten
Erleichtert den Überblick ganz enorm: Mit Hilfe der benutzerdefinierten Ansichten können die Daten aus den Ereignisprotokollen gefiltert werden.

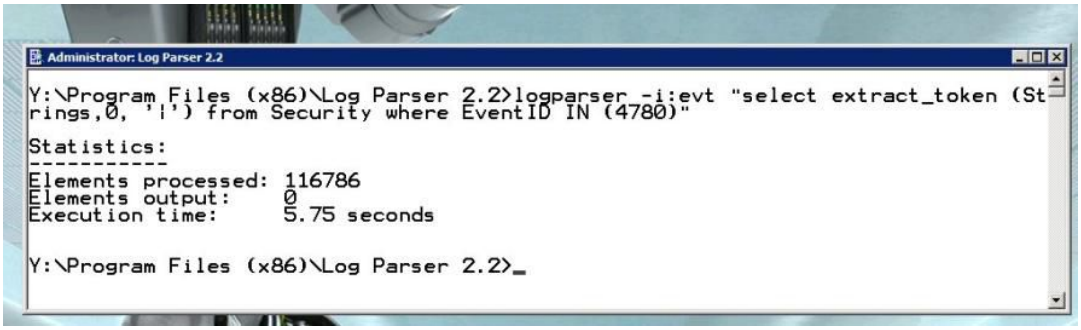


Log-Dateien auswerten
Ein eigener „Blick“ auf die vielen Daten wird entworfen: Durch die Filter ist es möglich, sehr viel genauer nach bestimmten Ereignissen zu suchen.



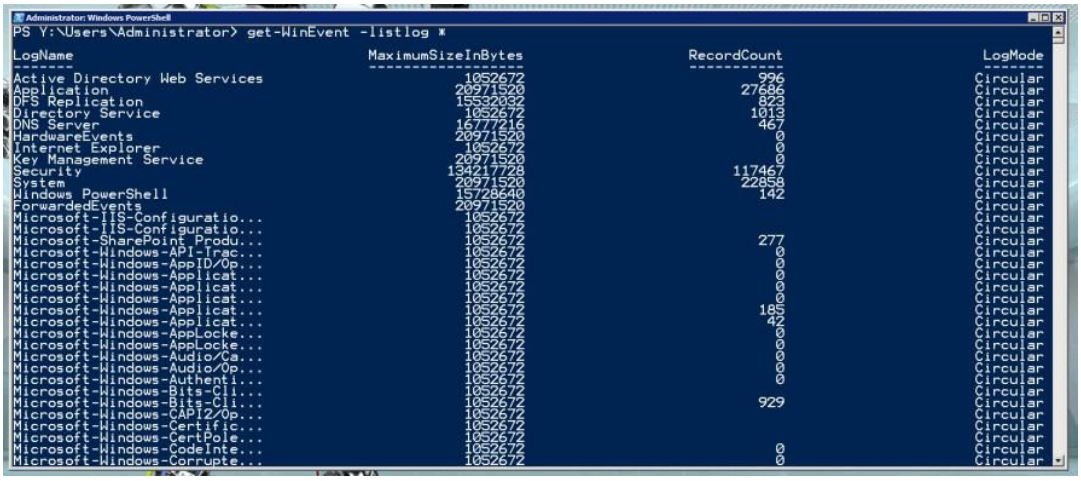
Log-Dateien auswerten

Eine benutzerdefinierte Ansicht – eine der Neuerung, die mit Windows Server 2008 eingeführt wurde: Hier wurde eine solche Ansicht für alle Events mit der ID 4738 entworfen.



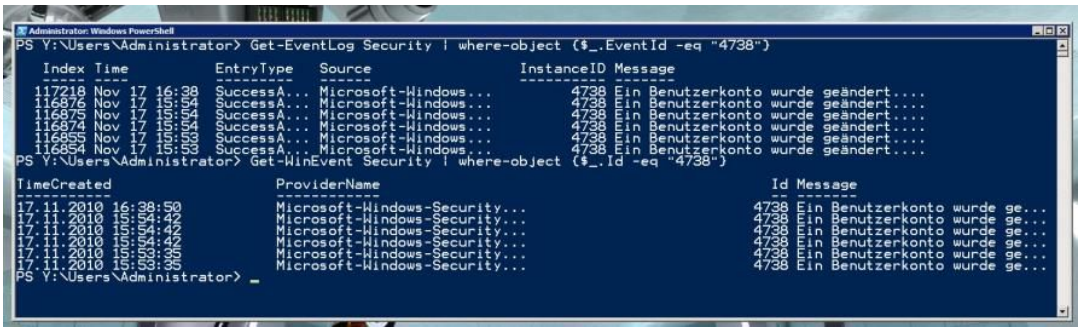
Log-Dateien auswerten

Das kostenlose Werkzeug Log Parser: Es bietet umfangreiche Möglichkeiten, die Ereignisprotokolle direkt von der Kommandozeile abzufragen, ist aber veraltet und besitzt eine sehr komplexe Syntax.



Log-Dateien auswerten

Die komplette Liste: Der Get-WinEvent-Befehl zeigt alle vorhandenen Protokolle auf dem lokalen System an und steht nur auf den modernen Windows-Versionen zur Verfügung.



Log-Dateien auswerten

Kleine, aber wichtige Unterschiede: Auch wenn beide Befehle auf dem aktuellen Window-Server funktionieren, sollte man vor ihrem Einsatz unbedingt die Details bei Syntax, Parametern und Eigenschaften beachten.