

Ereignisanzeige mit Remoteverwaltung, Abonnements und PowerShell

Event Manager

von Thomas Joos

Alle Fehler und Aktionen in Windows finden sich in den Ereignisanzeigen. So haben Administratoren eine im Prinzip hervorragende Quelle für das Troubleshooting, denn anhand des Ereignisprotokolls lassen sich problematische Events identifizieren. Doch leider ist das Ganze ungefiltert eine sehr unübersichtliche Angelegenheit, die erst mit Windows-Abonnements, der PowerShell oder Drittanbietertools wirklich zielführend wird.



Quelle: Sergi Lopez – 123RF

Die Ereignisanzeige hilft, nach Programm- und Systemaktionen zu suchen, die zu einem Problem führen und fördert Details zu Tage, die Ihnen bei der Ermittlung der Fehlerursache behilflich sind. Zugleich lassen sich anhand dieser Informationen auch Leistungsprobleme beurteilen und beheben. Sie sollten in regelmäßigen Abständen auf Server nach entsprechenden Einträgen suchen, da Sie so frühzeitig Fehler erkennen. Der Speicherort der Standardprotokolle in der Ereignisanzeige ist "%SystemRoot%\System32\winevt\Logs". Die Protokolldateien erhalten die Endung "EVTX", da diese XML-basiert sind.

Ereignisanzeige nutzen

Sie rufen die Ereignisanzeige durch Eingabe von *eventvwr.msc* im Startmenü auf. Unter Windows Server 2016 können Sie im Startmenü direkt *eventvwr.msc* eintippen oder über die Kombination der Tasten "Windows" und "R" das Dialogfeld "Ausführen" aufrufen und dort den Programmnamen eingeben. In Windows Server 2016 finden Sie die Ereignisanzeige im Menüpunkt "Tools" und unter dem Knoten "Windows-Protokolle" ist der Zugriff auf die Anwendungs-, System- und Sicherheitsprotokolle möglich.

Klicken Sie direkt auf den Knoten "Ereignisanzeige", sehen Sie eine Zusammenfassung aller Serverfehler im rechten Bereich und unter "Anwendungs- und Dienstprotokolle" finden Sie zahlreiche Protokolle zu den einzelnen Serverdiensten in Windows Server 2016. Einträge zu Serveranwendungen wie SQL Server oder Exchange beheimatet "Anwendungen". Mit "Benutzerdefinierte Ansichten" lassen Sie sich Filter für alle installierten Serverrollen anzeigen. Auf diese Weise können Sie auch Filter, zum Beispiel für die verschiedenen SQL-Instanzen, erstellen lassen oder für andere Serveranwendungen, die auf dem Server installiert sind.

Die "Benutzerdefinierten Ansichten" zeigen Ihnen auch administrative Ereignisse an. Hier finden sich alle Fehler und Warnungen aus den verschiedenen Protokolldateien, die für Administratoren von Interesse sind. Windows Server 2016 bietet dabei die Möglichkeit, weniger interessante Ereignisse herauszufiltern, sodass Sie sich auf jene Ereignisse konzentrieren können, die wichtig sind. Klicken Sie eine Meldung an, erhalten Sie im unteren Bereich ausführlichere Informationen rund um das Event.

Mit dem Windows-Aufgabenplaner können Sie einem Ereignis eine Aufgabe hinzufügen. Jedes Mal, wenn ein Ereignis erscheint, das der Abfrage entspricht, startet anschließend die entsprechende Aufgabe. Dazu klicken Sie mit der rechten Maustaste auf das Ereignis und wählen "Aufgabe an dieses Ereignis anfügen".

Fehler mit der Ereignisanzeige entdecken

Im mittleren Bereich des Ereignisprotokoll-Fensters finden Sie eine Zusammenfassung aller Einträge, deren detaillierte Informationen Sie per Doppelklick auf einzelne Meldungen anzeigen lassen können. Auf Basis dieser Fehlermeldung lässt sich erkennen, welche Probleme Windows Server 2016 mit einzelnen Komponenten erkannt hat. Sie sollten regelmäßig die Ereignisanzeigen auf Fehler überprüfen, da Sie hier schnell Probleme erkennen können, bevor diese gravierendere Auswirkungen haben.

Haben Sie den Fehler genauer eingegrenzt und Fehlermeldungen in der Ereignisanzeige und der Diagnose festgestellt, suchen Sie auf [1] gezielt nach diesen Fehlern. Auf dieser Seite gibt es zu so gut wie jedem Eintrag der Ereignisanzeige Hin-

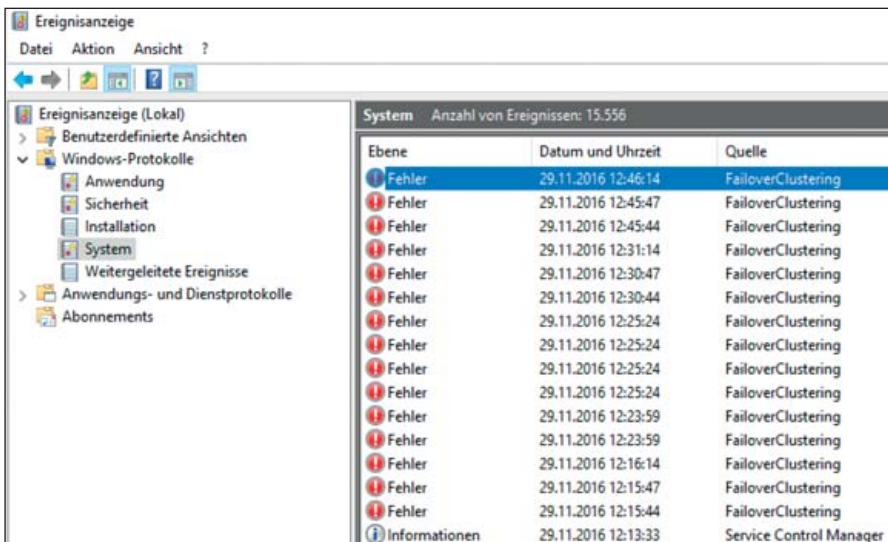


Bild 1: Zahlreiche Fehler in den Ereignisprotokollen von Windows Server 2016 sollten den Administrator hellhörig machen.

weise und mögliche Lösungsansätze. Außerdem können Sie den Fehler in einer Suchmaschine, auf speziellen Supportseiten [2] oder in der Microsoft Knowledge Base eingeben. Suchen Sie allerdings in der englischen Knowledge Base [3] immer nur nach englischen Begriffen, da Sie hier mehr Antworten erhalten.

Im Rahmen einer Fehlerbehebung sollten Sie in der Ereignisanzeige auch überprüfen, ob diese Fehler in anderen Protokollen meldet, die mit dem Problem in Zusammenhang stehen können. Überprüfen Sie etwa, ob parallel zu diesem Fehler in anderen Protokollen der Ereignisanzeige Fehler auftreten, die zur gleichen Zeit gemeldet werden, also unter Umständen auf einen Zusammenhang schließen lassen. Stellen Sie fest, wann der Fehler in der Ereignisanzeige das erste Mal aufgetreten ist und überlegen Sie genau, ob zu diesem Zeitpunkt irgendetwas verändert wurde (auch auf Basis der Ereignisprotokolle).

Untersuchen Sie auch in den anderen Protokollen der Ereignisanzeige, inwiefern der Fehler mit anderen Ursachen zusammenhängt. Ein Fehler tritt selten ohne vorherige Änderung der Einstellung oder aufgrund defekter Hardware auf, sondern meist durch Konfigurationen am System oder die Installation von Applikationen. Durch die Filtermöglichkeiten der Ereignisanzeige können Sie Fehler oft sehr genau eingrenzen.

Protokolle verwalten

Klicken Sie ein Protokoll mit der rechten Maustaste an, zeigt Ihnen das Kontextmenü zahlreiche Optionen an:

- Gespeicherte Protokolldatei öffnen: Hier öffnen Sie eine Protokolldatei, die Sie über "Ereignisse speichern unter" abgespeichert haben. Dadurch lassen sich Protokolle per E-Mail versenden.
- Benutzerdefinierte Ansicht erstellen: Erlaubt, die Anzeige der Ereignisanzeigen anzupassen und als benutzerdefinierter Filter abzulegen. In diesem Fall werden Ihnen nur noch die Ereignisse der gespeicherten Ansicht angezeigt.
- Benutzerdefinierte Ansicht importieren: Importiert zuvor exportierte Ansichten auf einem Server.
- Protokoll löschen: Wählen Sie diesen Menübefehl aus, wird nicht das Protokoll gelöscht, sondern der Inhalt des Protokolls. Sie erhalten zuvor noch eine Meldung, ob das Protokoll wirklich gelöscht werden soll und ob Sie es vorher speichern möchten (entspricht "Ereignisse speichern unter").
- Aktuelles Protokoll filtern: Dieser Befehl ist hilfreich, wenn Sie keine eigene Ansicht des Protokolls erstellen, sondern nur die aktuelle Ansicht filtern möchten. Dadurch können Sie zum Beispiel nach einem bestimmten Fehler suchen und überprüfen, wann dieser aufgetreten ist.
- Eigenschaften: Hier legen Sie die Größe der einzelnen Protokolle fest und bestimmen, wie sich Windows Server

- 2016 beim Erreichen der maximalen Ereignisprotokollgröße verhalten soll.
- Alle Ereignisse speichern unter: Speichert die Ereignisse in einer EVTX-Datei.
- Aufgabe an dieses Protokoll anfügen: Mit dieser Option können Sie über die Aufgabenplanung automatisch Aktionen und Skripte starten, wenn in den Ereignisanzeigen bestimmte Fehler auftauchen. Solche Aufgaben lassen sich auch an einzelne Ereignisse anfügen.

Arbeiten mit Ereignis-Abonnements

Windows Server 2016 kann mit Bordmitteln die Ereignisanzeigen verschiedener Server im Netzwerk zusammentragen und anzeigen. Diese Funktion trägt die Bezeichnung "Abonnements" und lässt sich direkt in der Ereignisanzeige auf Basis des Systemdiensts "Windows-Ereignissammeldienst" einrichten. Dieser muss auf dem Server gestartet sein, der die verschiedenen Ereignisse sammeln soll, sowie auf allen beteiligten Servern. Damit die Sammlung von Ereignisanzeigen funktioniert, müssen Sie die beteiligten Computer vorbereiten, das Abonnement erstellen und dann in der Ereignisanzeige die Fehler der entsprechenden Server anzeigen. Die Sammlung von Ereignisanzeigen basiert auf zwei Grundlagen: Es gibt einen Server, der die Daten sammelt (Sammlungscomputer), und Server, die daran angebunden sind, die sogenannten Quellcomputer. Die Sammlung von Ereignisanzeigen führen Sie am besten auf Servern durch, die in einer gemeinsamen Active-Directory-Gesamtstruktur positioniert sind.

Im ersten Schritt aktivieren Sie die Remoteverwaltung auf den einzelnen Servern. Dazu geben Sie auf jedem Quell-

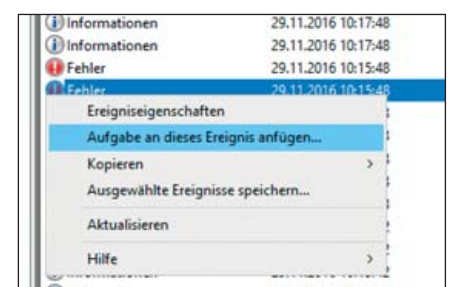


Bild 2: Wird eine Aufgabe an ein Ereignis angehängt, triggert es zuvor definierte Aktionen, wie etwa den Aufruf eines Skripts.

und dem Sammlungscomputer in einer Eingabeaufforderung mit Administratorrechten (über das Kontextmenü gestartet) die Befehle `winrm quickconfig` gefolgt von `wecutil qc` ein. Das Tool konfiguriert dann das Weiterleiten von Ereignissen über das Netzwerk zu einem Sammlungscomputer. Nehmen Sie anschließend das Computerkonto des Sammlungscomputers, auf dem Sie die Ereignisse aller angebotenen Server anzeigen wollen, in die lokalen Administratorgruppen der einzelnen Server auf, indem Sie die lokale Benutzerverwaltung starten (am schnellsten durch die Eingabe von `lusrmgr.msc` im Startmenü). Jetzt rufen Sie die Eigenschaften der lokalen Administratorgruppe auf, klicken dann auf die Schaltfläche "Hinzufügen" und im daraufhin geöffneten Dialogfeld auf den Button "Objekttypen", um auch Computerkonten in die Gruppe aufnehmen zu können.

Um Ereignisabonnements in Arbeitsgruppen zu erstellen, müssen Sie manuell eine Ausnahme in der Windows-Firewall für Remote-Ereignisprotokollverwaltung auf jedem Quellcomputer hinzufügen. Das Konto, mit dem Sie die Ereignisse auf den Quellcomputer sammeln, hinterlegen Sie anschließend bei der Einrichtung des Abonnements. Zusätzlich geben Sie auf dem Sammlungscomputer den folgenden Befehl ein:

```
> winrm set winrm/config/client
  @{TrustedHosts="Alle Quellcomputer, durch Komma getrennt"}
```

Die Sammlung nehmen Sie am besten mit einem Konto vor, das über Administratorrechte in der Domäne verfügt. Wollen Sie ein eigenes Konto dafür anlegen, müssen Sie dieses wie erwähnt in die lokale Administratorgruppe auf allen Quellcomputern aufnehmen. Normalerweise reicht es aus, wenn nur das Computerkonto des Sammlungscomputers Mitglied der Administratorgruppe auf den Quellcomputern ist.

Haben Sie alle Vorbereitungen getroffen, öffnen Sie auf dem Sammlungscomputer die Ereignisanzeige und klicken auf "Abonnements". Ist der Systemdienst "Windows-Ereignissammlungsdienst" nicht gestartet,

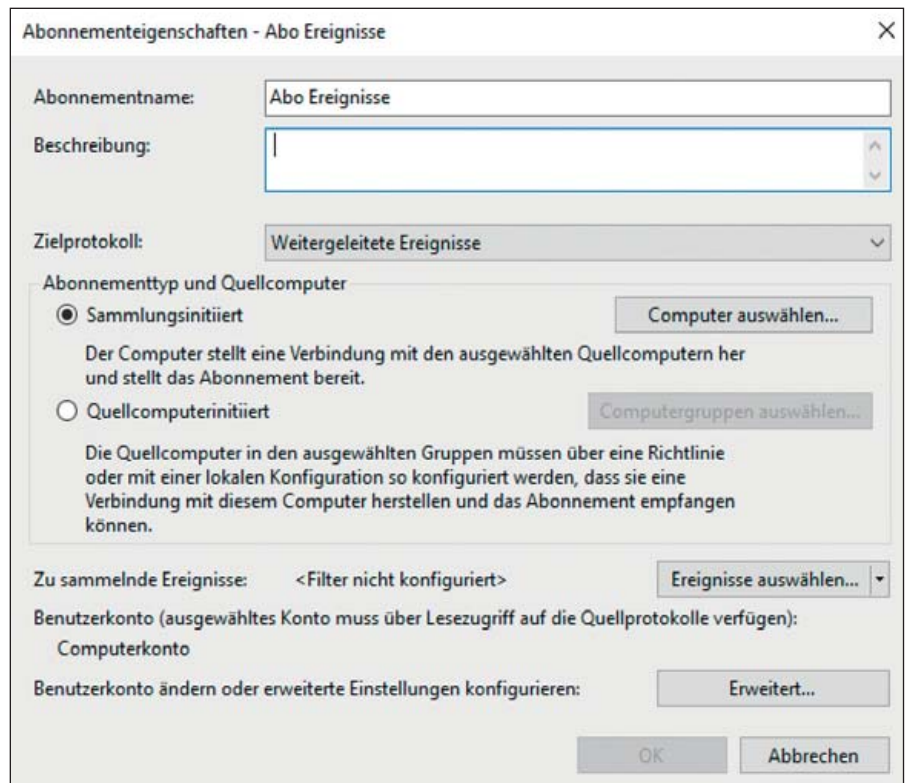


Bild 3: Über eine einfache Oberfläche konfigurieren Administratoren ein neues Abonnement für die Sammlung von Ereignissen auf Rechnern im Netzwerk.

erhalten Sie eine entsprechende Meldung. Lassen Sie in diesem Fall den Dienst starten. Anschließend klicken Sie mit der rechten Maustaste auf "Abonnements" und dann auf "Abonnement erstellen", alternativ gehen Sie über das Menü "Aktionen" und "Abonnement erstellen".

Im neuen Fenster konfigurieren Sie jetzt das Abonnement. Bei "Abonnementname" geben Sie eine Bezeichnung und auf Wunsch auch eine Beschreibung ein, während "Zielprotokoll" definiert, wo auf dem Sammlungscomputer die Ereignisse der Quellcomputer gesammelt werden sollen. Standardmäßig ist hier das Protokoll "Weitergeleitete Ereignisse" ausgewählt. Anschließend wählen Sie die Art des Abonnements aus. Aktivieren Sie die Option "Sammlungsinitiiert" und klicken Sie auf die Schaltfläche "Computer auswählen", um die Quellcomputer für das Abonnement festzulegen. Sie sollten für jeden Computer, den Sie hinzufügen, auf die Schaltfläche "Testen" klicken, um sicherzustellen, dass der Sammlungscomputer eine Verbindung aufbauen kann.

Über die Schaltfläche "Ereignisse auswählen" erstellen Sie neue Filter, über die Sie

festlegen, welche Ereignisse auf den Quellcomputern der Sammlungscomputer anzeigen soll. Grundsätzlich beinhaltet dies die Auswahl, welche Ereignisse von welchen Protokollen zu erfassen sind. Haben Sie den Filter angelegt, klicken Sie auf "OK". Bevor Sie weitere Einstellungen vornehmen, klicken Sie erneut auf "OK", um das Abonnement zu überprüfen. Das Abonnement muss jetzt als "Aktiv" gekennzeichnet sein. Auf diesem Weg können Sie mehrere Abonnements erstellen, die verschiedene Computer mit verschiedenen Abfragefiltern erfassen.

Nun ist der Sammlungscomputer in der Lage, die Ereignisse im ausgewählten Protokoll anzuzeigen. Haben Sie das Standardprotokoll "Weitergeleitete Ereignisse" ausgewählt, finden Sie dieses im Bereich "Windows-Protokolle". Bis die ersten Ereignisse eintreffen, kann es allerdings eine Weile dauern. Von welchem Server die Ereignisse stammen, sehen Sie in der Spalte "Computer".

Neben den Standardeinstellungen für Abonnements können Sie über die Schaltfläche "Erweitert" in den Eigenschaften des Abonnements individuelle Anpassungen vornehmen.

sungen vornehmen. Zum Beispiel lässt sich festlegen, dass die Abfrage der Ereignisse nicht durch das Computerkonto des Servers erfolgt, sondern mit einem speziellen Benutzerkonto, dessen Daten Sie in den erweiterten Einstellungen des Abonnements hinterlegen. Achten Sie aber auch hier darauf, dieses Konto in die lokale Administratorengruppe der Quellcomputer aufzunehmen.

Außerdem konfigurieren Sie in den erweiterten Einstellungen, wie der Sammlungscomputer die Daten abrufen soll. Hier stehen die drei Optionen "Normal", "Bandbreite minimieren" und "Wartezeit minimieren" zur Verfügung. Bei der Standardeinstellung "Normal" verwendet das Abonnement den Pull-Zustellungsmodus. Dabei fasst das Abo immer fünf Elemente zusammen und überträgt diese vom entsprechenden Quellcomputer auf den Sammlungsserver. Die Option "Bandbreite minimieren" begrenzt die Bandbreite, die dem Abo zur Verfügung steht und "Wartezeit minimieren" stellt sicher, dass Ereignisse möglichst schnell auf dem Sammlungsserver zur Verfügung stehen. In den erweiterten Einstellungen legen Sie auch den Port und die Übertragungsart fest. Wenn Sie diese ändern, müssen Sie in den Firewall-Einstellungen der Quellcomputer ebenfalls entsprechende Regeln definieren, was sich in Active-Directory-Umgebungen auch mit Gruppenrichtlinien umsetzen lässt.

Remote-Zugriff auf Ereignisse ohne Abonnements

Neben den Abonnements lassen sich auch mit der Standardereignisanzeige problemlos Ereignisanzeigen von Computern im Netzwerk abrufen. Dazu dient Ihnen die Ereignisanzeige selbst oder das Befehlszeilentool "Wevtutil". Für Ersteres starten Sie die Ereignisanzeige und klicken Sie mit der rechten Maustaste auf "Ereignisanzeige (Lokal)". Anschließend öffnen Sie durch Auswahl von "Verbindung mit anderem Computer herstellen" die Ereignisanzeige beliebiger Server. Wollen Sie auf diesem Weg eine Verbindung mit mehreren Servern aufbauen, müssen Sie eine neue Management-Konsole erstellen und das Snap-in der Ereignisanzeige mehrmals integrieren. Um nun eine Ver-

bindung mit einem anderen Benutzerkonto aufzubauen, aktivieren Sie noch die Option "Verbindung unter anderem Benutzerkonto herstellen" und wählen das entsprechende Konto aus. Sie können den Benutzernamen und das Kennwort für die Verbindung festlegen. Sie können die Ereignisanzeige eines Servers auch direkt durch Eingabe von *eventvwr Computername* öffnen.

Um mit dem erwähnten Tool eine Verbindung zur Ereignisanzeige eines anderen Servers aufzubauen, verwenden Sie den folgenden Befehl:

```
> wevtutil Option /r:Computername /u:Benutzername /p:Kennwort
```

Verwenden Sie die Optionen "/u" und "/p" nicht, verbindet Sie Wevtutil mit dem Benutzer, mit dem Sie angemeldet sind. Welche Optionen zur Verfügung stehen, sehen Sie, wenn Sie *wevtutil* eingeben. Das Tool dient nicht dazu, die Ereignisanzeige über das Netzwerk zu öffnen, sondern Einstellungen vorzunehmen oder das Protokoll zu löschen. Mit

```
> wevtutil el /r:sbs.contoso.local
```

lassen Sie sich zum Beispiel alle verfügbaren Protokolle auf dem Remotecomputer anzeigen. Sie können auf diesem Weg auch Ereignisanzeigen ohne Rückfrage löschen:

```
> wevtutil cl Name des Protokolls
```

Der Befehl

```
> wevtutil cl system /r:sql
```

löscht zum Beispiel das Systemprotokoll auf dem Server "sql" ohne weitere Rückmeldung. Natürlich können Sie mit dem Tool über *wevtutil epl* auch Protokolle über das Netzwerk auf den lokalen Computer in EVT-X-Dateien exportieren.

Ereignisanzeige mit der PowerShell anzeigen

In der PowerShell lassen Sie sich die Ereignisanzeige auf Computern über das Cmdlet *Get-Eventlog* anzeigen. Mit den Optionen "system", "application" und

"security" definieren Sie, welche der einzelnen Ereignisanzeigen Sie öffnen. Zugriff auf das Sicherheitsprotokoll erhalten Sie allerdings nur, wenn die PowerShell-Sitzung mit Administratorrechten gestartet wurde.

Lesen Sie jedoch auf diesem Weg die ganze Ereignisanzeige aus, wird es schnell unübersichtlich. Sie können aber zum Beispiel auch nur die aktuellsten Meldungen anzeigen:

```
> Get-Eventlog system -Newest 100
```

Reicht dieser Filter nicht aus, lässt er sich noch so erweitern, dass er nur die Fehlermeldungen anzeigt:

```
> Get-Eventlog system -Newest 100 | here-Object {$_.entryType -Match "Error"}
```

Weiter ausgebaut zeigt der Filter die Meldungen optimal formatiert und beinhaltet nur die gewünschten Informationen:

```
> Clear-Host
> $Event = Get-Eventlog -Logname system -Newest 1000
> $logError = $Event | where {$_.entryType -Match "Error"}
> $logError | Sort-Object EventID | Format-Table EventID, Source, TimeWritten, Message -auto
```

Interessant in diesem Zusammenhang ist auch die Möglichkeit, nach ganz bestimmten Quellen

```
> Get-EventLog System -Newest 10 -Source "Service*" | Format-Table TimeWritten, Source, EventID, Message -auto
```

oder nach der ID zu filtern:

```
> Get-EventLog -Logname system -InstanceId 7040 -Newest 10
```

Ereignismeldungen selbst erzeugen

Über die Eingabeaufforderung mit dem Befehl *eventcreate.exe* lassen sich eigene Einträge in den verschiedenen Ereignisanzeigen erstellen, beispielsweise für ei-

Optionen von PsLogList

Option	Auswirkung
@Datei	Führt den Befehl auf allen Computern aus, die in der Datei aufgelistet sind. Jeder Computer muss dazu in einer eigenen Spalte in der Textdatei stehen. Die entsprechenden Ereignisse der Computer werden also hierüber gesammelt.
-a	Zeigt die Einträge nach dem genannten Datums an. Als Format kommt "dd/mm/yy" zum Einsatz.
-b	Zeigt die Einträge vor dem genannten Datum an.
-c	Löscht die entsprechenden Ereignisanzeigen nach der Anzeige über PsLogList. Dies ist zum Beispiel bei der Abfrage über eine Batchdatei sinnvoll.
-d	Zeigt nur die Einträge der letzten n Tage an. Dabei werden die letzten Tage als "<n>" hinter der Option angegeben.
-e	Filtert Einträge mit definierten IDs aus. Die Syntax entspricht der Option "-i".
-f	Filtert Ereignisse mit bestimmten Typen aus ("-f w" beispielsweise filtert Warnungen). Sie können beliebige Buchstaben verwenden, wobei nur Ereignisse auftauchen, die mit den entsprechenden Buchstaben anfangen.
-h	Liefert Einträge der letzten n Stunden. Die Syntax entspricht der Option "-d".
-i	Sucht nur Einträge mit den hier definierten IDs. Es können auch mehrere IDs kommagetrennt angezeigt werden.
-l	Speichert Einträge der definierten Ereignisanzeige.
-m	Liefert die Einträge der letzten n Minuten.
-n	Zeigt nur die aktuellsten definierten Einträge an.
-o	Sucht nur die Einträge der spezifizierten Ereignisquelle (zum Beispiel "\-o cdrom"). Diese Option schließt in der Ausgabe also zusätzliche Informationen ein.
-p	Gibt das Kennwort für den konfigurierten Benutzer an. Geben Sie kein Passwort ein, fragt das Tool notfalls nach. Dabei wird das Kennwort nicht in Klartext angezeigt oder über das Netzwerk geschickt.
-q	Zeigt die Einträge der spezifizierten Ereignisquelle nicht an (zum Beispiel "\-q cdrom"). Benutzerdefinierte Einträge werden so von der Ausgabe ausgeschlossen. Sollen mehrere Quellen von der Ausgabe ausgeschlossen werden, müssen Sie diese durch Komma voneinander trennen.
-r	Speichert die Einträge aufsteigend ab.
-s	Hier werden die Einträge kommabasiert angezeigt, um diese zum Beispiel in einer Excel-Tabelle oder SQL-Datenbank zu speichern. Nach der Auswertung kann zum Beispiel über den Befehl <i>start</i> die CSV-Datei sofort geöffnet und angezeigt werden.
-t	Definiert das Trennzeichen.
-u	Legt den Benutzernamen fest, mit dem Sie auf die Server zugreifen.
-w	Wartet auf neue Einträge und speichert diese, sobald diese in der Ereignisanzeige angezeigt werden. Das funktioniert aber nur für das lokale System.
-x	Speichert erweiterte Daten, die standardmäßig nicht angezeigt werden. Hierbei handelt es sich meistens um binäre Rohdaten.

gene Skripte oder Batchdateien. Die Syntax dabei lautet:

```
> Eventcreate [/S Computername
  [/U Benutzername [/P Kennwort]]
  /ID Ereignis-ID [/L Protokollname]
  [/SO Quelle] } /T Typ
  /D Beschreibung
```

Als "Typ" stehen "SUCCESS", "ERROR", "WARNING" und "INFORMATION" zur

Verfügung. Ein Beispielsevent könnte wie folgt aufgebaut sein:

```
> Eventcreate /T Information /ID 523
  /L System /D "Anwendung Thomas 1
  erfolgreich installiert"
```

Diese Informationen lassen sich dann auch wieder mit der PowerShell auslesen. Soll nur der Text der Ereignismeldung angezeigt werden, filtern Sie wie folgt:

```
> get-eventlog system -newest 1 | fl
  Message
```

Ereignisanzeigen sammeln mit PsLogList

Mit PsLogList [4] aus der PsTools-Sammlung von Sysinternals können Sie in der Eingabeaufforderung die Ereignisanzeigen verschiedener Computer einsammeln, anzeigen und vergleichen. Rufen Sie das Tool ohne Optionen auf, zeigt es Einträge des lokalen Systemereignisprotokolls an, der Befehl *psloglist application* liefert das Anwendungsprotokoll. Sollen nur die aktuellsten fünf Einträge angezeigt werden, verwenden Sie

```
> psloglist system -n 5
```

Nur Fehlermeldungen erfassen Sie mit

```
> psloglist system -f e
```

Fehler und Warnungen erhalten Sie mit der Option "-f ew". Mit PsLogList können Sie auch die Ereignisanzeigen von Computern im Netzwerk auslesen:

```
> psloglist \\Computer
```

Alle Optionen finden Sie in der Tabelle "Optionen von PsLogList".

PsLogList liest auch die Ereignisanzeigen von Computern im Netzwerk aus. Dazu verwenden Sie zunächst *psloglist \\Computer* und dann die verschiedenen Optionen des Tools, um die Anzeige zu aktivieren. Dabei gehen Sie genauso vor wie bei der Abfrage lokaler Ereignisanzeigen.

Eine Option, die in der Tabelle fehlt, ist "eventlog": Standardmäßig verwendet das Tool das Systemereignisprotokoll. Sie können die Ereignisanzeige auswählen, wenn Sie die ersten Buchstaben oder die entsprechende Abkürzung angeben. Allerdings müssen Sie auch auf deutschen Windows-Servern die englischen Abkürzungen, also beispielsweise "sec" für "security", eingeben, wenn das Ereignisprotokoll "Sicherheit" geöffnet werden soll. Eine wichtige Funktion des Tools ist, dass das Programm in der Lage ist, direkt auf die Quell-DLLs auf den Remotesystemen zuzugreifen. Allerdings muss dazu auf

dem entfernten System die administrative Freigabe ("Admin\$") aktiviert sein.

Ereignisanzeigen im Netz durchsuchen

Microsoft EventCombMT [5] aus den kostenlosen "Microsoft Account Lockout and Management Tools" hat zwar schon einige Jahre auf dem Buckel, kann aber auch bei aktuellen Serverversionen noch helfen, auf einer von Ihnen festgelegten Anzahl von Servern nach bestimmten Ereignissen zu suchen, diese zu exportieren und dann in einer Textdatei anzuzeigen. Sie erhalten mit dem kostenlosen Tool einen sehr schnellen Überblick zu bestimmten Ereignissen im Netzwerk.

Sie müssen das Werkzeug nur starten, eine Installation ist nicht notwendig. EventCombMT zeigt für alle Server eine TXT- oder CSV-Datei an. Nach Eingabe der Domäne wählen Sie die entsprechenden Server aus, das Ereignisprotokoll, den Typ und andere Informationen. Sie können auch nach Ereignis-IDs und Texten filtern lassen. Um Ereignisanzeigen auszulesen, starten Sie die EXE-Datei, wählen die Domäne aus und fügen danach über das Kontextmenü die gewünschten Server hinzu. Danach geben Sie im unteren Bereich an, nach welchen Ereignissen Sie suchen wollen und klicken auf "Search". Im Anschluss finden Sie im Verzeichnis Textdateien mit den entsprechenden Daten.

Über den Menüpunkt "Options" können Sie die Ausgabedateien auch als CSV formatieren. In den Optionen steuern Sie auch, in welchem Zeitraum EventCombMT nach den Ereignissen suchen soll. Alle weiteren Filtermethoden steuern Sie auf der Startseite. Erhalten Sie zu viele Daten, können Sie die EventIDs einschränken sowie die Quelle und den Text, der in der Ereignismeldung erscheinen soll.

Haben Sie komplizierte Abfragen erstellt, können Sie diese über "Searches / Save This Search" speichern und mit "Searches / Load A Search" laden. In EventCombMT sind bereits standardmäßig Abfragen und Suchen enthalten, zum Beispiel Fehlermeldungen von Festplatten, gesperrte Konten im Active Directory und mehr. Diese finden Sie über "Searches / BuiltIn Searches".

Ereignisse mit Drittanbietertools verwalten

Das Tool "Event Log Explorer" [6] von FS Pro Labs stellt Ereignisanzeigen von bis zu drei Computer im Netzwerk kostenlos dar. Sie können für einzelne Computer getrennte Anmeldeinformationen hinterlegen. Zusätzlich können Sie Computergruppen erstellen, zum Beispiel für Domänencontroller, Datenbank-Server oder Server in Niederlassungen. Event Log Explorer bietet auch Filter an.

Der "GFI Events Manager" [7] steht zwar nicht kostenlos zur Verfügung, lässt sich aber kostenlos testen. Die Preise hängen von den angebundenen Servern ab. Sie können aus den vorgefertigten Überwachungsregeln auswählen oder eigene erstellen. Das Tool kann auch Systemdienste in Windows, Linux und anderen Betriebssystemen sowie Anwendungs-Server wie Exchange oder SQL-Server überwachen.

"EventSentry" [8] ist eine Monitoring-Software für die Ereignisanzeige. Sie bietet unter anderem die Möglichkeit, Informationen per E-Mail zu versenden, wenn bestimmte Ereignismeldungen in den Protokollen der Server auftauchen. In der E-Mail ist die auslösende Ereignismeldung mit allen Daten enthalten. Die Lizenz der Anwendung für einen Host kostet 85 US-Dollar. Es gibt jedoch auch eine kostenlose, aber etwas eingeschränkte Light-Variante. Diese kann Ereignisanzeigen überwachen und E-Mails versenden. Das Tool benötigt Agenten auf den Zielsystemen sowie einen Computer im Netzwerk als Installationsziel der Verwaltungsoberfläche. In dieser finden Sie die Ereignisanzeigen der angebundenen Rechner und können Aktionen durchführen. So legen Sie etwa über "Packages / Event Log Packages / Default" fest, welche Ereignisse das Tool überwachen soll. Auf diesem Weg können Sie auch direkt nach einzelnen IDs oder nach Ereignisquellen filtern. Im Bereich "Actions" konfigurieren Sie, wie das Tool reagieren soll, wenn bestimmte Ereignisse auftreten.


Mit der Freeware "MyEventViewer" [9] von Nirsoft erhalten Sie ein Werkzeug, das Ereignisse übersichtlicher darstellt als

die Standardanzeige in Windows. Das Tool muss nicht installiert werden und verbindet sich nach dem Start mit dem lokalen Rechner, zeigt die Ereignisse an und bietet eine übersichtliche Arbeitsoberfläche. Starten Sie das Werkzeug über die Befehlszeile oder eine Verknüpfung, lassen sich auch Ereignisanzeigen über das Netzwerk auslesen:

```
MyEventViewer.exe /remote
\\Computername
```

Seine Vorteile spielt MyEventViewer vor allem durch die verschiedenen Filter und die einfache Anzeige aus. Über den Bereich "Logs" in der Menüleiste blenden Sie uninteressante Protokolle aus oder setzen über "Options" verschiedene Filter.

Fazit

Hat Ihr Windows-Server Probleme, sagt er Bescheid. Das Problem für Sie als Admin ist nur, die Hilferufe auch wahrzunehmen, wenn sie im allgemeinen Rauschen der Ereignisprotokolle untergehen. Mit den hier gezeigten Maßnahmen und Werkzeugen lässt die Wahrscheinlichkeit, ein wichtiges Ereignis zu verpassen, deutlich reduzieren. So erreichen Sie nicht nur ein besseres Troubleshooting, vielmehr steigt auch die Chance, Probleme so früh zu erkennen, dass sie sich abstellen lassen, bevor ein gravierendes Ereignis eintritt. (jp) 

Link-Codes

- [1] **Eventid**
CS1F1
- [2] **Experts Exchange**
CS1F2
- [3] **Microsoft-Support (englisch)**
DS1S3
- [4] **Microsoft PsLogList**
C2P15
- [5] **Microsoft EventCombMT**
FS147
- [6] **Event Log Explorer**
FS148
- [7] **GFI Events Manager**
FS149
- [8] **EventSentry**
C2P12
- [9] **MyEventViewer**
GS2Z2