

# Verwalten von Ereignisprotokollen mit EventCompTM

Beigesteuert von Frank Solinske

## Verwalten von Ereignisprotokollen mit Event Comp

Warum schwer, wenn es auch Einfach geht ?

Jeder kennt das Problem, wenn es darum geht, die Eventlogs der Server zu überwachen oder zu überprüfen. Sicher kann man so etwas auch mit automatischen Tools wie SMS 2003 oder MOM 2005 erledigen, es geht aber auch deutlich günstiger !

Microsoft hat ein kostenfreies Tool dafür, mit dem man alle Server (auch DC's) abfragen kann. Es heisst Event Comp

Downloadlink:

<http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e>

Um das Tool benutzen zu können muss man Administratorenrechte besitzen. Oder das Recht zum Auslesen der Eventlogs muss delegiert worden sein.

Es werden Windows Windows 2000, Windows XP und Server 2003 unterstützt.

Event Comp bietet eine einfache und gut strukturierte GUI:

Im Feld Domain, wird die lokale Domäne automatisch angezeigt. Will man andere Domänen erfassen, dann kann man die erkannte Domäne einfach überschreiben.

Hinzufügen der zu scannenden Server:

Mit einem Rechtsklick öffnet sich das Auswahlménü:

Add a Single Server : Manuelles hinzufügen von Workstations oder Servern

Add DCs in Domain : Automatisches hinzufügen aller Domain Controller

Add DCs in a Site : Automatisches hinzufügen aller Domain Controller des Standortes

Add all GCs : Automatisches hinzufügen aller Domain Controller die GC sind

All Server from Browse : manuelles hinzufügen aller Server die per Netbios gefunden werden

Add Servers from File: auslesen einer Textdatei mit allen Servernamen

Add Comp from Dom : Automatisches hinzufügen aller PC's und Memberservern

Nach der Auswahl werden die entsprechenden Server angezeigt. Man kann mehrere Server gleichzeitig durchsuchen lassen.

Man kann einzelne oder mehrere Logdateien gleichzeitig durchsuchen.

Bei der Auswahl der Ereignisse sind auch ein Mehrfachauswahl möglich.

Im Feld Event IDs, kann man gezielt nach einer ID suchen, oder mehrere durch Kommata getrennte IDs suchen. Will man einen Bereich (600 - 700) durchsuchen, dann trägt man diese in die beiden hinteren Felder ein.

Im Bereich Sources kann man die Ursprungsquelle definieren. Standardeinstellung ist: All Sources. Durch das Dropdown Feld kann man die Quelle dediziert einschränken.

Im Menüpunkt: Searches - Built in Searches sind die wichtigsten Events vorkonfiguriert. Das GUI wird entsprechend angepasst.

Mit Search wird die Analyse gestartet und das Ergebnis wird in dem Output Directory als EventCompMT.txt Datei gespeichert. Je nach Menge der Server und Größe der Logdateien kann die Analyse einige Minuten dauern.

Mit dem Event Comp Tool bekommt man ein mächtiges Hilfsmittel an die Hand, dass einem die tägliche Arbeit sehr erleichtert.

© 2006 by Frank Solinske - Unterwegs-im.net