
Eventsammler

Geschrieben von ChrisBox - 2007/11/26 15:45

Hi,

Ich habe mir mal den Eventsammler angesehen und muss sagen: Holla! Supper Teil.

Das teil sammelt mir schonmal einige Events ein.

- Bei Windows XP64 bleibt das Script einfach hängen und nichts passiert weiter.
Nach 15 Minuten und keinem Anwachsen der DB habe ich unterbrochen.
Netzwerkverkehr war auch bei 0.

Muss ich was an der XP64 Maschine drehen oder hat sich WMI so verändert, dass es eine 2. Routine braucht?
Firewall ist nicht installiert auf der Maschine.

- Wir haben POP3/smtp intern verbannt. Es gibt also keine möglichkeit eMails per smtp zu versenden.
Exchange und IMAP habe ich. Gibt es dazu eine Idee/kommt da was?

- Das createDB Script erzeugt eine DB auf C:\. Das will ich aber nicht.

(aus einem Tool:)

```
CREATE DATABASE ON
(FILENAME = 'E:\MSSQL\MyEvents.mdf'),
(FILENAME = 'E:\MSSQL\MyEvents_log.LDF')
FOR ATTACH
GO
```

Danke,
chris

Re:Eventsammler

Geschrieben von Potsdam - 2007/11/26 20:56

mmh - gegen und mit XP64 hab ich noch nicht getestet.

Scannst du eine XP64-Box oder läuft das Script darauf?
Erinnere mich noch an Probleme mit x64 bei meinem VMWare-BAckupscript. Das musste glaub ich nur mit der richtigen Scriptengine aufgerufen werden - dann gings. (die VMWare-APIs gibbet nur für 32bit)

Create DB lief bei mir richtig!? Habe allerdings meinem SQL2005 die Standard Pfade für Datenbanken und Logs auf separate Laufwerke voreingestellt. Werds mal mit deinem Tipp testen.

Ansonsten bin ich dabei das ganze ins Inventory zu integrieren.

Mail per IMAP - auch da werden die Nachrichten per SMTP versendet - oder irre ich mich??

Re:Eventsammler

Geschrieben von Adben - 2007/11/27 10:34

Potsdam schrieb:

Mail per IMAP - auch da werden die Nachrichten per SMTP versendet - oder irre ich mich??

IMAP oder POP3 dienen zum E-Mail-Empfang, sind aber seit 2003 standardmäßig nicht aktiviert. Der Zugriff erfolgt normal aus Outlook heraus über die MAPI-Schnittstelle und dafür hat MS was eigenes.

SMTP ist der Standardversandweg, dieser ist auch bei Exchange aktiv. Möglicherweise ist eine Authentifizierung notwendig oder der versendende Webserver hat keine Berechtigung (Server-Protokolle-SMTP-Default SMTP Virtual Server-Eigenschaften, Access-Relay) Nachrichten über den Exchangeserver auszuliefern. Outlook verwendet auch hierfür die MAPI-Schnittstelle. Änderungen dieser Einstellungen können dazu führen, dass der Exchange als OpenRelay im Netz steht.

=====

Re:Eventsammler

Geschrieben von ChrisBox - 2007/11/27 12:29

Uiuiui, Da war ich aber durcheinander.

eMails:

Gut, nochmal. Wir haben POP3 abgeschaltet. Hat auch nichts damit zu tun;-)
Der eMail Empfang geht auch über IMAP. Hat aber auch nichts damit zu tun;-)
Vollkommener Quatsch den ich gefragt habe.

Mein Problem war:

Da wir also eMailtechnisch recht panisch sind, kamen wir auf die Idee den Port 25 dicht zu machen. Für SMTP haben wir dann SSL eingeschaltet (=Port 465).

Port 25 ist intern komplett dicht wegen den Viren und den Vertriebs-Kollegen:

"Aaah, schön, eine .pdf.exe. Hab ich ja noch nie gesehen. Wie die wohl geöffnet wird..."

Hinweis

Für mich hat sich das Problem erstmal gelöst, aber vielleicht hat es jemand anderes...
Ich habe mit unserem Linux-Admin gesprochen und den Port 25 für ein paar Server-IP aufgemacht.
So ist es nicht mehr ein Problem, sondern nur noch ein Hinweis:-)

XP64:

Das Script läuft auf einer XP32Bit Maschine... und es läuft gut!
Wenn ich von der XP32 Kiste die AD scannen lasse, bleibt es bei dem XP64Rechner einfach stehen.
Auch admins-eventsammler.vbs -PC:XP64Rechner liefert das selbe Bild.

Der letzte Logeintrag:

Uhrzeit: 666 Events von Rechner LOCALHORST eingelesen

Uhrzeit: Rechner XP64 ist online

Dann passiert (mind.) 15 Minuten lang nichts.

Rechnernamen

Ich habe die AD scannen lassen.

Dann einen Testrechner per Hand einscannen lassen, der vorher aus war.

Allerdings habe ich den Computernamen klein geschrieben und nicht wie das Script es ausliest, GROSS.

Wenn ich das in der Datenbank einsehe, sieht das -für mich- unschön aus:-))

Jammern auf hohem Niveau:-))

Domäne/Arbeitsgruppe

Es wäre gut, die Möglichkeit zu haben, auch Arbeitsgruppen-Rechner (Laptops, VMWare) zu scannen. Dazu muss ein Useraccount und Passwort eingegeben werden.

Gruß,
chris

=====