Microsoft

Azure

CLI

Suche mit query im JSON Format mithilfe der JMESPATH Syntax

Quelle: https://adamraffe.com/2017/11/22/the-wonderful-world-of-azure-cli-jmespath-queries/

Alle VMs einer Ressourcen Gruppe auflisten

```
az vm list -g MeineRG --query
"[].{ResourceGroup:resourceGroup,VMName:name,VMSize:hardwareProfile.vmSize,StorageProfil:stora
geProfile.{OSDisk:osDisk.{Name:name,GB:diskSizeGb,OS:osType},DataDisk:dataDisks.[[].{Name:name
,GB:diskSizeGb}]}}"

Ausgabe:
[
  {
    "ResourceGroup": "MeineRG",
    "StorageProfil": {
      "DataDisk": [
        []
      ],
      "OSDisk": {
        "GB": 30,
        "Name": "adminsrv_OsDisk_1_randomID",
        "OS": "Linux"
      }
    },
    "VMName": "adminsrv",
    "VMSize": "Standard_B2s"
```

```
  },
  {
    "ResourceGroup": "MeineRG",
    "StorageProfil": {
      "DataDisk": [
        [
          {
            "GB": 80,
            "Name": "router-dataDisk"
          }
        ]
      ],
      "OSDisk": {
        "GB": 4,
        "Name": "router-osDisk",
        "OS": "Linux"
      }
    },
    "VMName": "router",
    "VMSize": "Standard_DS4_v2"
  }
]
```

Exchange2010

https://www.frankysweb.de/exchange-20102007-relay-ohne-authentifizierung-erlauben/

https://itler.net/exchange-server-relay-nach-extern-erlauben-smtp-relay/

ExchangeManagementPowershell

Exchange Management Powershell funktioniert nicht nach Exchange Update

Im Internet-Information-Server wird eine Einstellung mit falschem Parameter überschrieben wird. Nämlich der Pfad zu der Exe für die Exchange Shell.
Der falsche Wert:

```
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\PowerShell
```

Der richtige Wert:

```
C:\Program Files\Microsoft\Exchange Server\V15\ClientAccess\PowerShell
```

Wenn man das wieder ändert funktioniert auch die Exchange Shell wieder.

WindowsBefehlsaufforderung

Suchen nach einem Prozess mit PID

```
C:\>tasklist /FI "PID eq 1192" /FO TABLE
```

Prozesse abhören und anzeigen

```
C:\>netstat -?
Zeigt Protokollstatistiken und aktuelle TCP/IP-Netzwerkverbindungen an.

NETSTAT [-a] [-b] [-e] [-f] [-n] [-o] [-p Protokoll] [-r] [-s] [-t] [-v]
[Intervall]
-a  Zeigt alle Verbindungen und abhörenden Ports an.
-b  Zeigt die ausführbare Datei an, die beim Erstellen jeder
Verbindung bzw. jedes abhörenden Ports involviert ist. In
einigen Fällen enthalten bekannte ausführbare Dateien mehrere
unabhängige Komponenten. Dann wird die Reihenfolge der
Komponenten angezeigt, die beim Erstellen der Verbindung oder
des abhörenden Ports involviert sind. In diesem Fall befindet
sich der Name der ausführbaren Datei unten in []. Oben
befindet sich die aufgerufene Komponente usw., bis TCP/IP
erreicht wurde. Bedenken Sie, dass diese Option viel Zeit in
Anspruch nehmen kann und fehlschlägt, wenn Sie nicht über
ausreichende Berechtigungen verfügen.
-e  Zeigt die Ethernet-Statistik an. Kann mit der Option -s
kombiniert werden.
-f  Zeigt vollqualifizierte Domänennamen für Remoteadressen an.
-n  Zeigt Adressen und Portnummern numerisch an.
-o  Zeigt die mit jeder Verbindung verknüpfte, übergeordnete
Prozesskennung an.
-p  Protokoll Zeigt Verbindungen für das angegebene Protokoll an.
Protokoll kann sein: TCP, UDP, TCPv6 oder UDPv6.
Bei Verwendung mit der Option -s kann Protokoll Folgendes
Sein: IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP oder UDPv6.
```

```
-r □Zeigt den Inhalt der Routingtabelle an.
-s □Zeigt die Statistik protokollweise an. Standardmäßig werden
IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP und UDPv6 angezeigt.
Mit der Option -p können Sie dies weiter einschränken
-t □Zeigt den aktuellen Abladungsstatus der Verbindung an.
-v □In Verbindung mit -b wird die Reihenfolge der Komponenten
angezeigt, die beim Erstellen der Verbindung oder des
abhörenden Ports für alle ausführbaren Dateien involviert
sind.
Intervall Zeigt die gewählte Statistik nach der mit Intervall angege-
benen Anzahl von Sekunden erneut an. Drücken Sie STRG+C zum
Beenden der Intervallanzeige. Ohne Intervallangabe werden
die aktuellen Konfigurationsinformationen einmalig
angezeigt.
```

Das Ergebnis (Ausgabe des Befehls) in eine Datei speichern

`C:\>netstat -a > C:\netstat.txt`

Die Suche mit findstr() verfeinern

`C:\>netstat -ano | findstr /r 0.0:80 && netstat -ano | findstr :6066 TCP 0.0.0.0:80 0.0.0.0:0 ABHÖREN 4 TCP 0.0.0.0:808 0.0.0.0:0 ABHÖREN 4256 TCP 0.0.0.0:8008 0.0.0.0:0 ABHÖREN 5940 TCP 0.0.0.0:8009 0.0.0.0:0 ABHÖREN 5940`

Netsh

- Für HTTP
  - `>netsh http show urlacl - Lists DACLs for the specified reserved URL or all reserved URLs.`

WindowsEventlog

Anmeldetypen

- Typ2: Interactive
- Typ3: Netzwerk
- Typ4: Batch
- Typ5: Service
- Typ7: Unlock
- Typ8: NetworkCleartext
- Typ9: NewCredentials
- Typ10: RemoteInteractive
- Typ11: CachedInteractive

Quelle: http://techgenix.com/logon-types/

Beschreibung der Sicherheitsereignisse in Windows 7 und Windows Server 2008 R2

Auszug:
Einführung
Dieser Artikel beschreibt verschiedene Sicherheit und auditing Ereignisse in Windows 7 und Windows Server 2008 R2.
Dieser Artikel enthält außerdem Informationen dazu, wie diese Ereignisse zu interpretieren sind. Diese Ereignisse werden im Sicherheitsprotokoll angezeigt und mit Security Auditing protokolliert. Dieser Artikel beschreibt auch beschreibende Daten zu Ereignissen abrufen.

Quelle: https://support.microsoft.com/de-de/help/977519/description-of-security-events-in-windows-7-and-in-windows-server-2008

WindowsPowerShell

MD5 Hashwert erzeugen

Beispiel:

```
PS C:\Users\admin\Downloads> certutil.exe -hashfile 'Pfad zur Datei' MD5
MD5-Hash von DATEI:
e4a44f70a296a3507f292d48b94fde8a
```

WindowsServer2016

Vorwort

Der Windows Server Kompetenz Club hat ein Booklet zum Thema Windows Server 2016 entwickelt was ich jedem empfehle.

Hier der DL Link.

Lizenzierung

Die 4 Regeln

Es gibt 4 Regeln, die die Lizenzierung von Windows Server 2016 regeln:

Regel Nr. 1: Jeder physische Prozessor wird mit mindestens acht Kernen gewertet.

Regel Nr. 2: Jeder physische Server wird mit mindestens 16 Kernen gewertet.

Regel Nr. 3: Alle physischen und aktiven Kerne im Server müssen unter Berücksichtigung der Regeln 1 und 2 lizenziert werden, damit ein Standard Server zwei und ein Datacenter Server unlimitierte VM-Rechte besitzt. Nachdem die Hardware nach den Regeln 1 bis 3 ausreichend lizenziert wurde, hat der Kunde auf diesem Server mit der Datacenter-Edition unlimitierte VM-Rechte. Hat er mit der Standard-Editionlizenziert, darf er nun ZWEI virtuelle Windows Server Instanzen betreiben. Sollten mehr als zwei VMs benötigt werden, greift Regel Nr. 4.

Regel Nr. 4: Um mit der Standard Edition zwei weitere VM-Rechte zu erhalten, müssen alle physischen aktiven Kerne erneut lizenziert werden.

Ein Beispiel

Vorhandene Hardware:

- ein Hypervisor mit z.B. VM Ware ESX oder Windows Hyper-V
  - CPU: 2x Xeon E5-2620v2
    - je CPU 6 Kerne mit 1,9 Ghz

Anzahl benötigter Virtueller Maschinen:

- 3x Windows Server 2016 Standard

Berechnung der Lizenzen:

- 2x6 Kerne = 12 Kerne
  - Regel 2 besagt, dass immer mind. 16 Kernen angenommen werden. Also würden wir mit 1x Windows Server 2016 Standard Lizenz 16 Kerne abdecken und sind mit unseren 12 Kernen im Rahmen. Somit brauchen wir schon mal keine zusätzlichen Lizenzpakete kaufen. Also dürfen wir mit dieser einen Lizenz schon mal 2 Virtuelle Maschinen betreiben. Um jetzt aber noch die 3. Virtuelle Maschine betreiben zu dürfen, müssen wir eine weiter Windows Server 2016 Standard Lizenz kaufen für alle unsere 12 Kerne. damit dürften wir sogar noch eine 4. Virtuelle Maschine betreiben, die wir aber in dem Beispiel nicht benötigen.

WindowsTerminalServer

Fehlerbehebungen

User kann keine Dateien auf dem Desktop löschen

Die Ursache ist scheinbar ein Designfehler von Microsoft, denn die User haben keinen Schreibzugriff auf ihren Papierkorb. (Recyclebin unter C:\...)
Gibt man als Admin den einzelnen Usern, am besten per Script, die Schreibrechte auf ihren Papierkorb ist das Problem behoben.

WMI

Verbindung zu Remote-PC prüfen

Wenn man prüfen möchte, ob sich ein entfernter Rechner via WMI abfragen lässt, dann kann man das auf der Kommandozeile mit Hilfe eines einfachen wmic-Aufrufs machen, also beispielsweise mit `wmic /node:192.168.0.24 path win32_operatingsystem get caption`

WordSeitenzahlen

Seitenzahlen ab Seite 3

Gute Anleitung: http://www.pctipp.ch/tipps-tricks/kummerkasten/office/artikel/word-2007-2010-2013-erst-ab-seite-3-nummerieren-59535/