Windows Server: Erste Schritte

Autor: Schmid Tobias

Datum: 03.01.2021

Typ: Information

Version: 1.0

INHALT

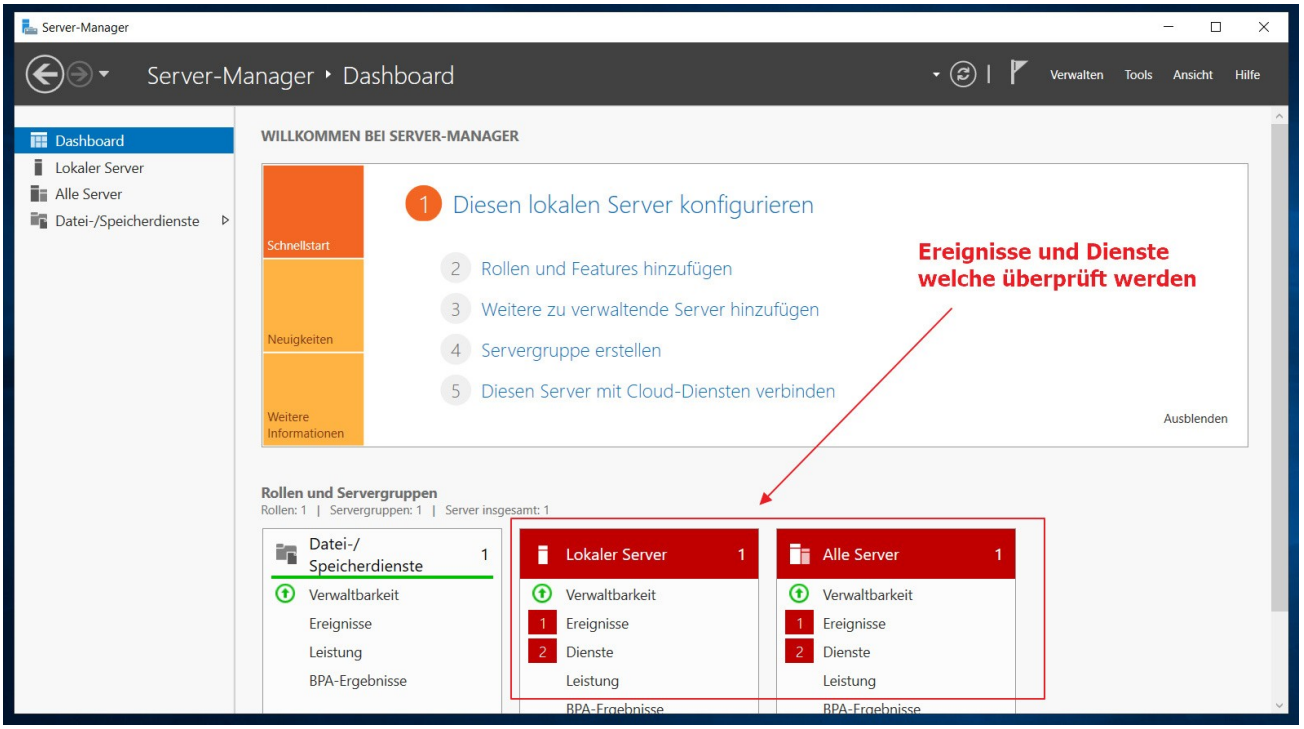
1 Einleitung

Das nachfolgende Dokument zeigt die ersten Schritte bei einer Servereinrichtung. Die wichtigsten Schritte haben wir während dem Unterricht angeschaut.

2 Überprüfung der Ereignisanzeige

Nachdem die Installation durchgelaufen ist und der neue Windows Server fertig installiert, sollte man auf alle Fälle mal einige Sachverhalte überprüfen. Hierzu gehört unbedingt die Ereignisanzeige. Sie erteilt Auskunft über verschiedene Betriebssystemdienste, bei welchen evtl. Fehler aufgetreten sind.

Direkt nach dem Öffnen des Server Managers werden auch dort in Rot mögliche Probleme und Fehler angezeigt. Ein Klick auf das entsprechende Ereignis öffnet automatisch die Detailanzeige. Jede später im Server installierte Rolle erhält im Server Manager eine eigene Seite für die Ereignisse. Daraus lässt sich leicht erkennen, wo bestimmte Probleme aufgetreten sind.

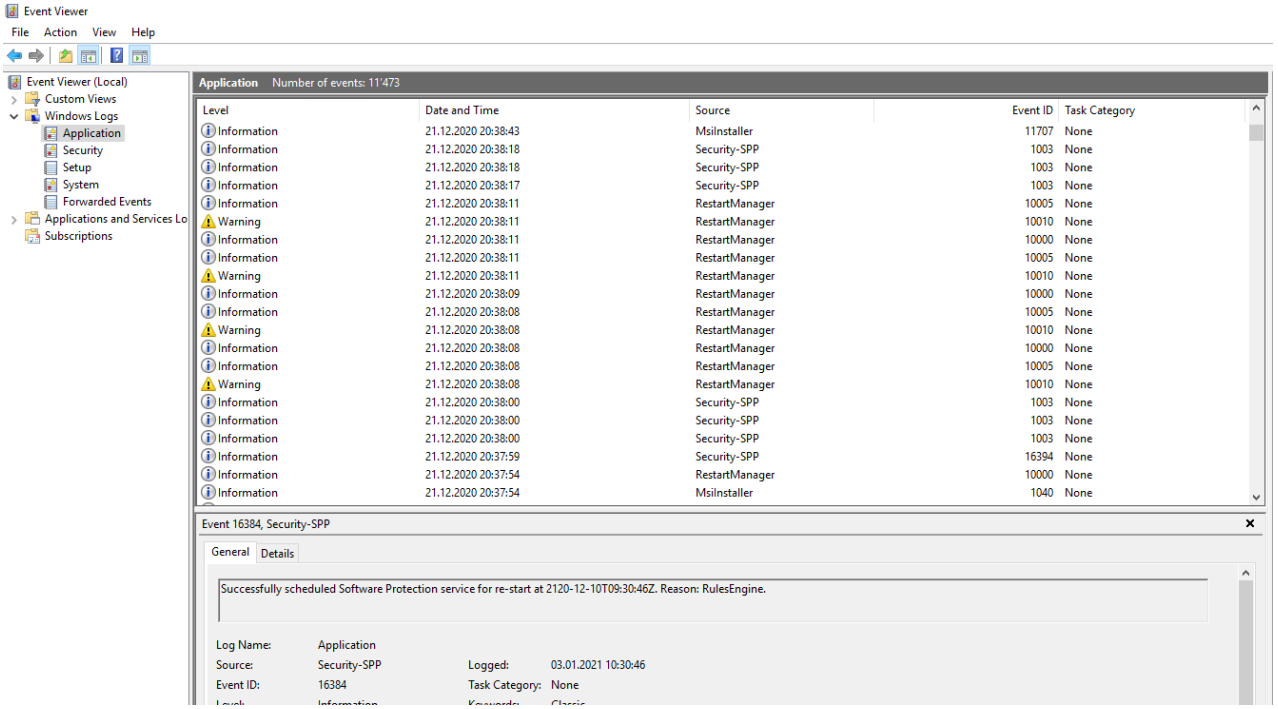


Eine weitere Anlaufstelle ist die Ereignisanzeige direkt. Geöffnet werden kann Sie per **eventvwr** im Startmenü. Aus dieser erhält man direkt aufgelistet die letzten aufgetretenen Fehler mit dessen Typ. Die unterschiedlichen Typen sind dabei z.B. Warnung, Fehler, Information oder Überwachung erfolgreich bzw. gescheitert.

Generell werden die Protokolle noch weiter unterteilt, wie man es im linken Navigationsmenü sehen kann. Wenn später am Server bestimmte Rollen und Features installiert werden, dann wird die Ereignissanzeige um diese Rolle bzw. dieses Feature ebenso erweitert.

Neben der Quelleund der Zeit wo bzw. wann das Problem aufgetreten ist, liefert die Detailansicht eine Ereignis-ID. Über diese ID kann man direkt eine Online Recherche starten.

Selbstverständlich bietet auch die Windows PowerShell Cmdlets an, um die Ereignisse auszulesen und ggf. weiterzuverarbeiten. Details zu den jeweiligen Befehlen erhält man durch das zusätzliche Cmdlet **Get-Help**.



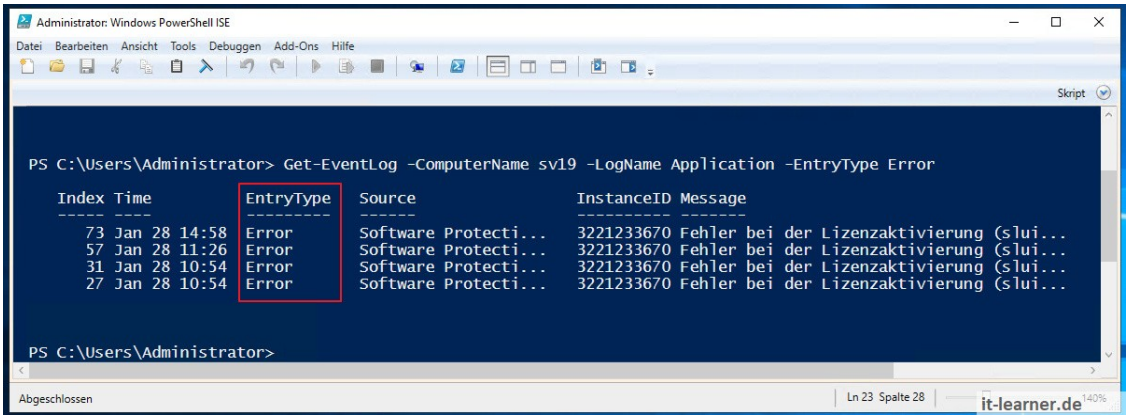
2.1 Mit der Windows PowerShell

```
Get-Eventlog

Get-WinEvent
```

Das folgende Windows PowerShell Beispiel zeigt, wie sämtliche Fehler aus dem Windows Protokoll „Anwendungen“ aufgelistet werden.

```
Get-EventLog -ComputerName sv19 -LogName Application -
EntryType Error
```



2.2 Der Best Practices Analyzer

Microsoft Server 2019 bietet auch einen sogenannten Best Practice Analyser an. Dieser hat die Aufgabe im Hintergrund verschiedene Serverrollen und Serverdienste zu überwachen. Im Prinzip lassen sich hiervon alle Serverrollen überwachen und dessen Ergebnisse anzeigen. Direkt im Servermanager sieht man das auch bei den einzelnen Kacheln. Ganz unten wird das BPA Ergebnis angezeigt.

2.3 Der Best Practice Analyser mit der Windows PowerShell

Natürlich lässt sich dieser Best Practice Analyzer durchaus auch mit der Windows PowerShell verwalten und steuern. Der grosse Vorteil liegt wieder darin, dass die Ergebnisse sofort weiterbearbeitet werden können

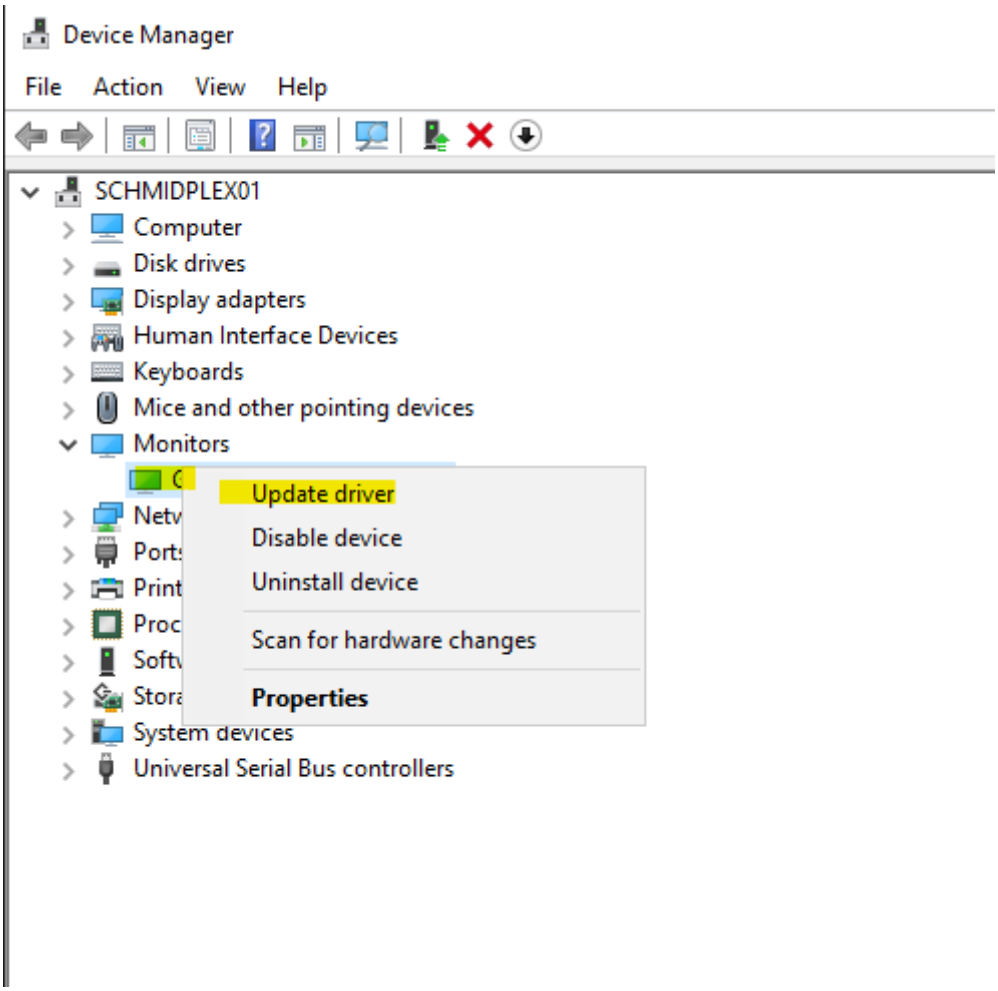
```
Get-BPAModel
```

Dieses Cmdlet liefert sämtliche IDs. Möchte man mehr Informationen für ein bestimmtes Modul, so kann man dabei folgendermassen vorgehen:

```
Get-BpaModel -ModelId Microsoft/Windows/FileServices
```

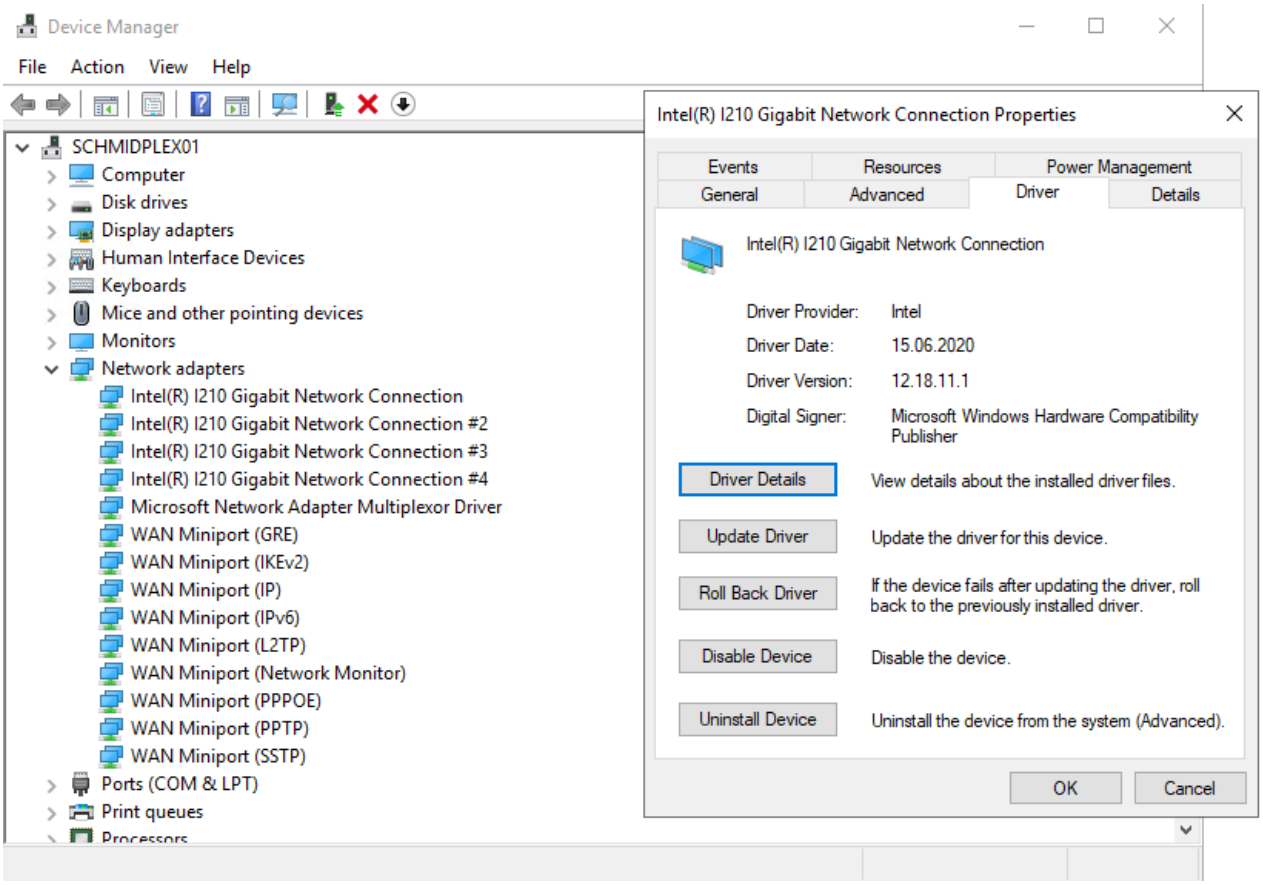
3 Server auf fehlende Treiber überprüfen

Nachdem nun diese Fehler beseitigt wurden, sollte man im nächsten Schritt alle Geräte auf die korrekten Treiber prüfen.



Anlaufstelle hierfür ist der **Geräte- Manager.**

Es sollten dort nach Möglichkeit keine gelben Ausrufezeichen ersichtlich sein. Ist dies der Fall, so könnte hier ein Treiberproblem vorliegen?
Sollte es nicht möglich sein den Treiber direkt mit dem Geräte-Manager zuaktualisieren, dann müsste man auf die Herstellerseite der jeweiligen Komponente und dort den passenden Treiber herunterladen und manuell installieren.



Benötigt man mehr Informationen zu einem bestimmten Gerät, so liefert ein Rechtsklick auf die Eigenschaften des entsprechenden Gerätes noch wesentlich mehr Informationen. In diesem Kontextmenü würde sich der Treiber direkt aktualisieren lassen.

Übrigens wäre hier auch die Möglichkeit ein Gerät komplett zu deinstallieren oder auch zu deaktivieren. Dies ist sehr sinnvoll, bei Geräten, welche nicht verwendet werden.
Auch mit der Windows PowerShell und der Eingabeaufforderung lassen sich Treiber importieren. Die beiden wichtigsten Parameter bei der Windows PowerShell sind dabei *path* und *Driver*.
Eine detaillierte Hilfe zu den PowerShell Cmdlets erhält man immer mit **Get-Help** gefolgt vom gewünschtem Cmdlet. Bei der cmd ist die Hilfe (**/?**) sehr nützlich, um die Syntax des Befehls zu erhalten.

3.1 Mit der Windows PowerShell:

```
Get-Help Add-WindowsDriver
```

3.2 Mit der Kommandozeile cmd:

```
PnPutil.exe /?
```

4 Netzwerkeinstellungen prüfen

Bevor jetzt der Windows Server für seine eigentliche Aufgabe konfiguriert wird, sollte die Netzwerkkonfiguration überprüft werden. Gerade wenn man z.B. den Server als Domänencontroller in Betrieb nehmen möchte, ist es unerlässlich, dass diese Einstellungen richtig sind.

Ein späteres Ändern kann nämlich zu schwerwiegenden Problemen führen. Natürlich sollte man seine komplette Netzwerkinfrastruktur vorab ordentlich geplant haben.

Generell gibt es zwei Möglichkeiten, wie der Windows Server seine IP- Adresse erhält. Einmal über einen DHCP Server, welcher automatisch IP- Adressen verteilt oder die manuelle Vergabe der Adresse.

Ob ein DHCP Server sinnvoll ist, muss natürlich von Fall zu Fall unterschieden werden. Allerdings empfehle ich für Infrastrukturgeräte, wie eben einen Windows Server, generell statische IP-Adressen zu verwenden.

Abgesehen von dem Netzwerksymbol in der Taskleiste geht es mit der Eingabeaufforderung (cmd) oder der Windows PowerShell noch schneller. Die Kommandozeile bzw. die neue Windows PowerShell sind die Standardwerkzeuge jedes Administrators. Aus diesem Grund sollte man sich an sie gewöhnen und auch immer wieder verwenden.

4.1 Mit der Kommandozeile cmd:

```
ipconfig /all
```

Wenn der Server direkt im Netzwerk angeschlossen ist, so erhält er in der Regel von einem DHCP Server die IP-Konfiguration. Auch wenn kein eigenständiger DHCP Server installiert ist, so ist ein Gerät immer im Netzwerk vorhanden, welches normalerweise IP-Adressen verteilt.
Die Rede ist vom Router. In Unternehmensnetzwerken sollte diese Funktion allerdings beim Router deaktiviert werden und lieber ein dafür zuständiger Server oder spezieller Router verwendet werden.

4.2 Mit der Windows PowerShell:

```
Get-NetIPAdress

Get-NetAdapter
```

4.3 Die IP-Konfiguration über einen DHCP Server beziehen

Sollte allerdings über die obigen Befehle eine Adresse in der Form **169.254.x.x** auftauchen, so hat sich das Windows Server Betriebssystem selbst eine Adresse vergeben und es konnte keine von einem DHCP Server zugewiesen werden. Wenn es jedoch gewünscht ist, dass der Server eine Adresse vom DHCP erhält, so solltest du folgende Einstellungen prüfen:

- ✓ DHCP Server an! (Router oder Server läuft ordnungsgemäss)
- ✓ Kabel verbunden! (Stecker fest angeschlossen)
- ✓ Treiber für die Netzwerkschnittstellen vorhanden (Geräte-Manager im Windows aufrufen)
- ✓ Netzwerkkarte in Ordnung (ping auf die eigene Netzwerkkarte)

Wenn alle obigen Punkte geprüft wurden, kann man nochmal eine neue Adresse anfordern. Manuell geht das über den folgenden Befehl in der cmd:

```
ipconfig /renew
```

Übrigens nicht selten ist es so, dass der Server eine Adresse vom DHCP Dienst erhält, allerdings nicht irgendeine beliebige, sondern eine vorher bei diesem Dienst Festgelegte.

Im Fachjargon spricht man dabei von einer **DHCP Reservierung**. Hierbei kann für ein bestimmtes Gerät (Server, Drucker, PC etc.) im DHCP Modul eine feste Adresse anhand der MAC Adresse des Gerätes reserviert werden.

Dadurch hat man den Vorteil, dass die Adresse trotzdem über den DHCP Server bezogen wird, aber der Server dabei immer die gleiche erhält. Eine andere Variante wäre einen bestimmten Bereich an Adressen im DHCP- Modul auszuschliessen und diese nur für Infrastrukturgeräte zu verwenden. Auch dadurch hätte man eine bessere Übersicht und Planung.

Ob eine Verbindung mit dem Internet besteht, lässt sich sehr leicht prüfen. Auch hier kann dies mit der Eingabeaufforderung oder der Windows PowerShell getestet werden.

Klar geht das auch durch das Öffnen einer Internetseite im Browser. Sofern alle Pakete gesendet und empfangen wurden, besteht eine Verbindung.

4.4 Mit der Kommandozeile cmd:

```
Ping www.google.ch
```

4.5 Mit der Windows PowerShell:

```
Test-NetConnection www.google.ch
```

4.6 Statische IPv4 Adresse vergeben

In der Regel ist es sinnvoller für Infrastrukturgeräte wie u.a. einen Windows Server direkt eine feste IP-Adresse zu vergeben. Wie bereits oben erwähnt gibt es dazu mehrere mögliche Varianten.
Zum einen kann die Adresse über den DHCP Dienst bezogen werden, wobei dort die Adresse fest zugewiesen wird. Zum anderen kann die IP- Adresse manuell mit der grafischen Oberfläche, der Eingabeaufforderung oder der Windows PowerShell festgelegt werden.

4.7 Mit der Windows Eingabeaufforderung

```
netsh interface ipv4>set address name="Ethernet0" static
172.16.1.200 255.255.0.0 172.16.1.10
```

Mit dem obigen Befehl wurde noch keine DNS-Adresse eingetragen. Auch das wäre mit **netsh** möglich wie die folgende Befehlssequenz zeigt:

```
netsh dnsclient>add dnsserver name="Ethernet0"
address=172.16.1.200 validate=no
```

4.8 Mit der Windows PowerShell

```
Set-NetIPAddress -InterfaceIndex 6 -IPAddress 172.16.1.200
-PrefixLength 16
```

Auch mit der Windows PowerShell muss noch extra die Adresse für den DNS-Server angegeben werden.

```
Set-DnsClientServerAddress -InterfaceIndex 6 -
ServerAddresses 172.16.1.200
```

Ob die Namensauflösung über DNS korrekt funktioniert, lässt sich ebenso sehr einfach noch mit der PowerShell oder cmd prüfen.

4.9 Mit der Windows Eingabeaufforderung

```
Nslookup server1
```

4.10 Mit der Windows PowerShell

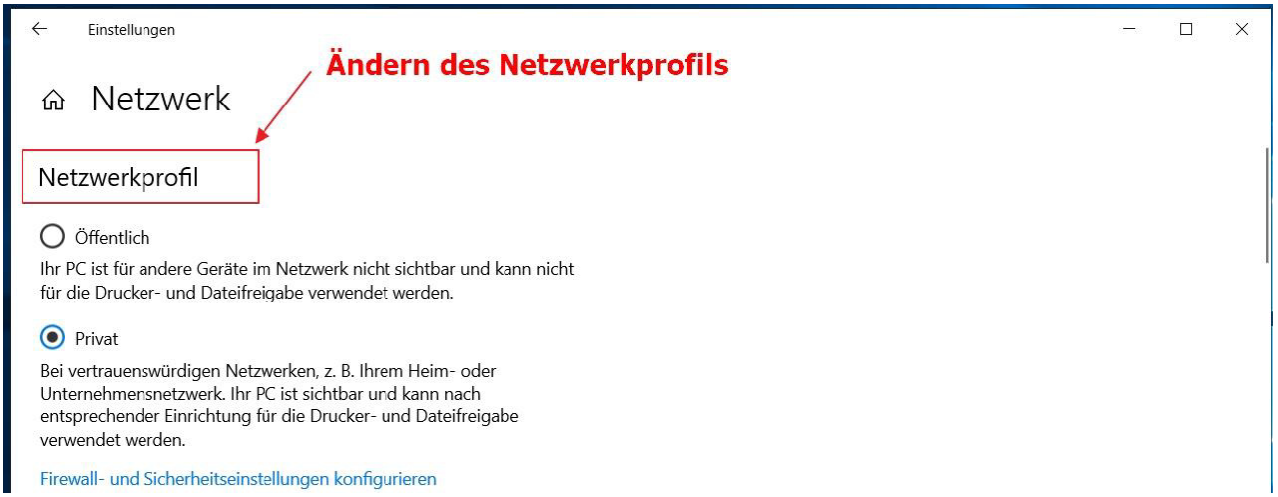
```
Resolve-DNSName server1
```

5 Firewalleinstellungen prüfen

Die Firewall ist im Prinzip die Schranke in andere Netzwerke. In der Regel hat man in grösseren Netzwerken eigenständige Geräte, welche als Firewall konfiguriert werden. Allerdings sollte man die Grundzüge der Windows Firewall kennen. Das wesentliche sind im Prinzip die folgenden drei Netzwerkprofile.

- ✓ Domänen Netzwerk
- ✓ Privates Netzwerk
- ✓ Öffentliches Netzwerk

Darauf beruhen alle einzelnen Firewall Regeln.



Im Detail kann jede einzelne Regel in der Firewall manuell eingestellt werden. Die Konfiguration lässt sich dabei mit dem Befehl **wf.msc** öffnen.

5.1 Privates Netzwerk

Diese Einstellung sollte für das Netzwerk zu Hause verwendet werden, denn damit wird i. d. R. die ***Netzwerkerkennung*** sowie auch die ***Datei- und Druckerfreigabe*** aktiviert. Was bedeutet, dass der Server sehr schnell über den Netzwerkexplorer gefunden werden kann.

5.2 Öffentliches Netzwerk

Dieses Netzwerk ist das Gegenteil vom privaten. Hier werden alle Konfigurationen so eingestellt, als das der Server im Netzwerk nicht sichtbar ist.

5.3 Domänen-Netzwerk

Dieses Netzwerk wird verwendet, sobald der Server entweder selbst ein Domänencontroller ist oder er zum Mitglied einer Domäne wird.
Das Netzwerkprofil, sowie auch einzelne Regeln lassen sich ebenso mit der Kommandozeile oder der Windows PowerShell konfigurieren. Dazu wird entsprechend des folgenden Befehles, bzw. das folgende PowerShell Cmdlet benötigt. Details zu den einzelnen Parametern kann man wieder der Hilfe entnehmen.

5.4 Mit der Windows PowerShell

Mit dem ersten Cmdlet lässt sich das aktuelle Profil auslesen.

```
Get-NetConnectionProfile
```

Mit diesem Cmdlet würde für den Netzwerkadapter mit dem InterfaceIndex 5 das Profil auf Privat konfiguriert.

```
Set-NetConnectionProfile -InterfaceIndex 5 -
NetworkCategory Private
```

Das folgende Cmdlet gibt alle vorhanden Firewall Regeln aus.

```
Get-NetFirewallRule
```

Es wird die Regel erstellt, dass alle eingehenden IPv4 Pings blockiert werden.

```
New-NetFirewallRule -DisplayName "pingen-blockieren" -
Direction Inbound -Protocol icmpv4 -Action Block
```

5.5 Mit der Windows Kommandozeile

```
Netsh advfirewall
```

6 Servernamen prüfen und einstellen

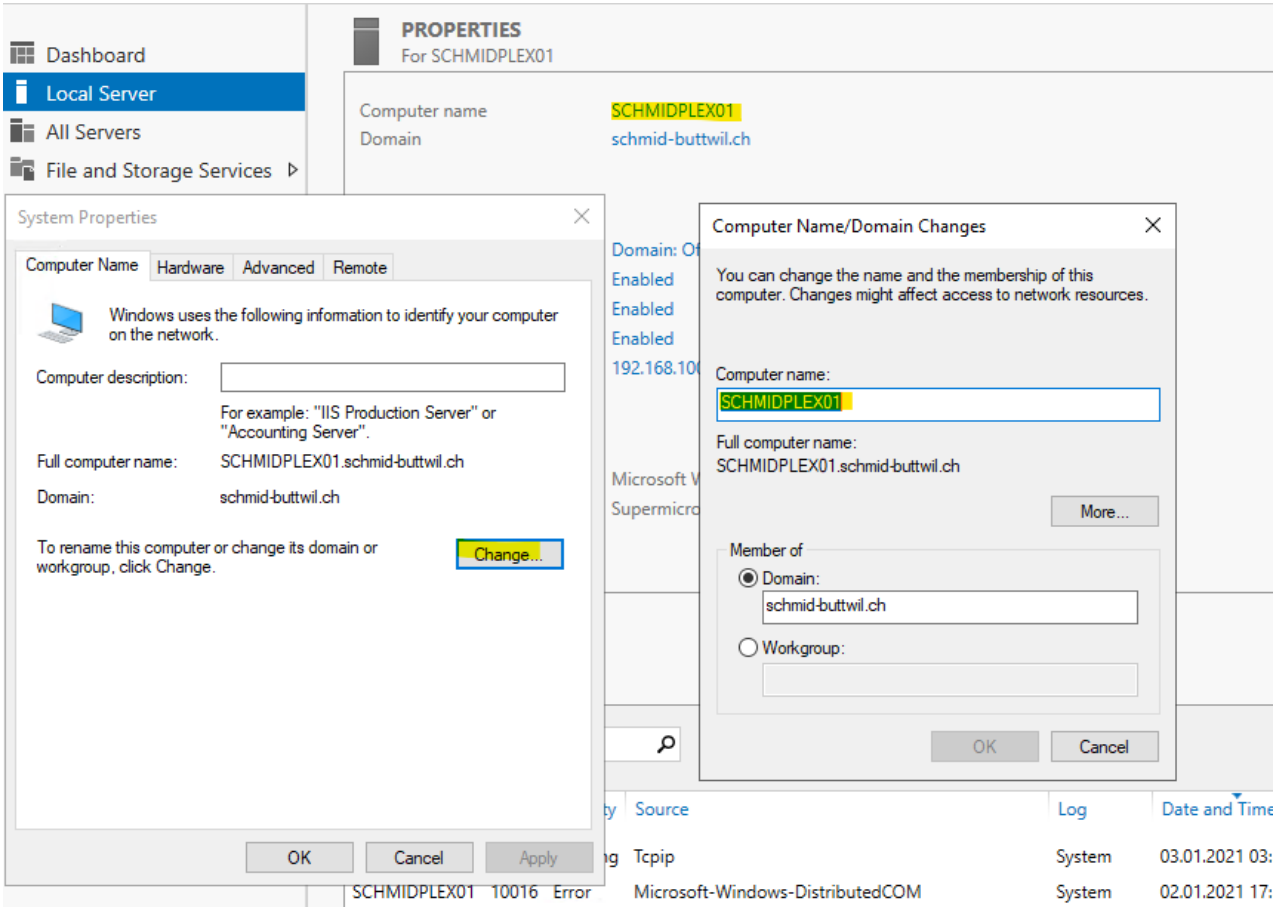
Eine weitere wichtige Grundkonfiguration des Servers ist der Name. Genauer gesagt handelt es sich dabei immer um den NetBios Namen. Dieser stammt noch aus der früheren Zeit und hat allerdings nichts mit dem BIOS zu tun, sondern wurde für die Vernetzung von Arbeitsgruppen entwickelt. Nach wie vor ist der 15 Zeichen lange Name im Windows Netzwerk fester Bestandteil und sollte eindeutig gewählt werden. Ein späteres Ändern führt häufig zu massiven Problemen.

Auch hier gilt die Devise. Vorab einen ordentlichen Plan für die Netzwerkinfrastruktur zu erstellen. Ein kürzerer Name ist meist auch sinnvoller als ein viel zu langer.

Der Server Manager liefert im ersten Überblick wieder diese wichtige Information. In der Regel hat man bereits bei der Installation des Servers einen eindeutigen Namen festgelegt. Falls dem nicht so ist, gibt es auch hier wieder mehrere verschiedene Varianten.

Die Erste ist jene über die grafische Oberfläche. Ein Klick im Server Manager auf den dort aktuellen Computernamen öffnet direkt die Systemeigenschaften. Dort lässt sich der Name des Servers ändern. Abschliessend wird ein Neustart benötigt.

Hinweis: Verwenden Sie für die wichtigsten Konfigurationseinstellungen immer den Server Manager und dort "local Server".



Eine zweite bzw. dritte Variante bietet wieder die Windows PowerShell sowie auch die Eingabeaufforderung.

6.1 Mit der Windows PowerShell

```
Rename-Computer-NewName sv1

Restart -Computer
```

6.2 Mit der Windows Eingabeaufforderung

```
WMIC computersystem where caption='Aktueller Name' rename
'Neuer Name'
```

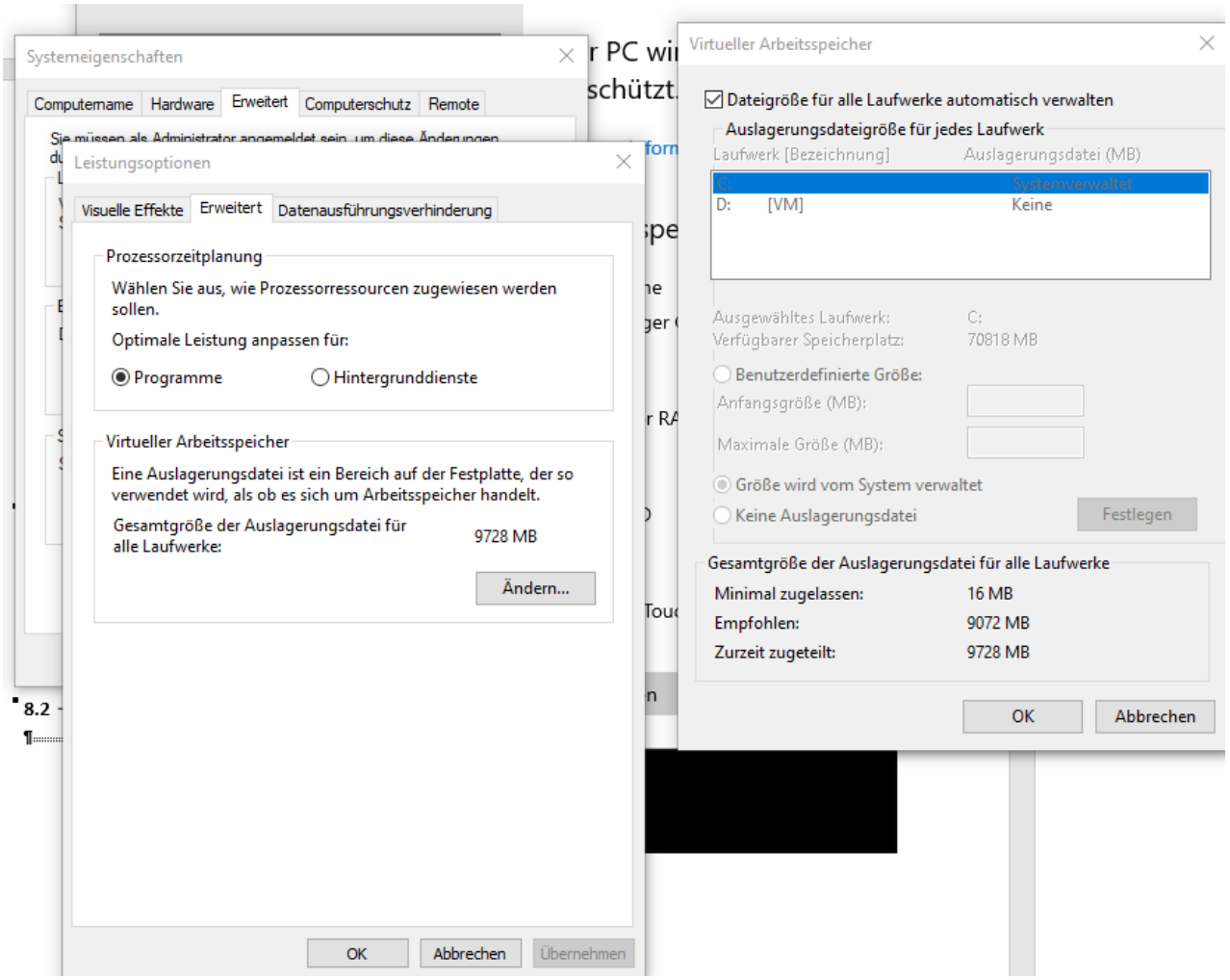
7 Konfiguration der Auslagerungsdatei

Die Auslagerungsdatei mit dem Namen **PAGEFILE.SYS** dientlaufenden Anwendungen als zusätzlicher Speicherplatz. In der Regel hat diese heutzutage keine zu grosse Bedeutung mehr, da die Server meist hardwaretechnisch sehr gut ausgestattet sind.

Für ältere Server kann die Konfiguration allerdings noch sehr sinnvoll sein. Zunächst kann die Verwaltung dem Server überlassen werden oder man konfiguriert diese manuell.

Bei der manuellen Konfiguration ergibt sich der Vorteil, dass die Datei auch auf einer anderen Partition als auf der c:\ Festplatte liegen kann.Aus diesem Grund wird sie häufig per Hand eingestellt. Bzgl. der Dimensionierung gibt es die Faustformel:

PAGEFILE = RAM x 1,5.



8 Windows Server auf neue Updates prüfen und aktivieren

Ein Windows Server stellt meist immer ein sehr wichtiges Infrastrukturgerät dar, was im Netzwerk essenziell ist. Aus diesem Grund muss er stehts besonders geschützt sein. Dazu gehört unbedingt, dass der Server die neuesten Updates besitzt.

Neue Updates bringen bekanntlich nicht nur neue Features, sondern schliessen auch evtl. vorhandene Sicherheitslücken oder lösen Probleme bei einem fehlerhaften Code. Der Update Prozess sollte so konfiguriert werden, dass der Server nicht automatisch neu startet. Das wäre fatal, gerade wenn es sich dabei um einen Produktivserver handeln würde. Aus diesem Grund ist es sinnvoll, wenn man vom Betriebssystem den Hinweis auf neue Updates erhält, aber den Zeitpunkt der Installation selbst bestimmen kann.

Auch mit der Kommandozeile sowie der Windows PowerShell, kann der Update Prozess gesteuert werden. Wobei für die Windows PowerShell explizit ein Modul installiert werden muss.

Ein Modul ist dabei im Prinzip nur ein Paket mit einer Sammlung von verschiedenen Befehlen für eine bestimmte Konfiguration.

Die obige Beschreibung bezieht sich darauf, dass der Server selbstständig die Updates herunterlädt. Grössere Unternehmen haben aber in der Regel einen sogenannten WSUS-Server, also einen Windows Service Update Server, welcher zentral alle Updates verwaltet. Wenn man den Server dafür konfigurieren möchte, so muss man ihm die Adresse des WSUS Servers in den Gruppenrichtlinien mitteilen.

8.1 Mit der Windows PowerShell

```
Install-Module PSWindowsUpdate

Get-WindowsUpdate
```

8.2 Mit der Windows Eingabeaufforderung

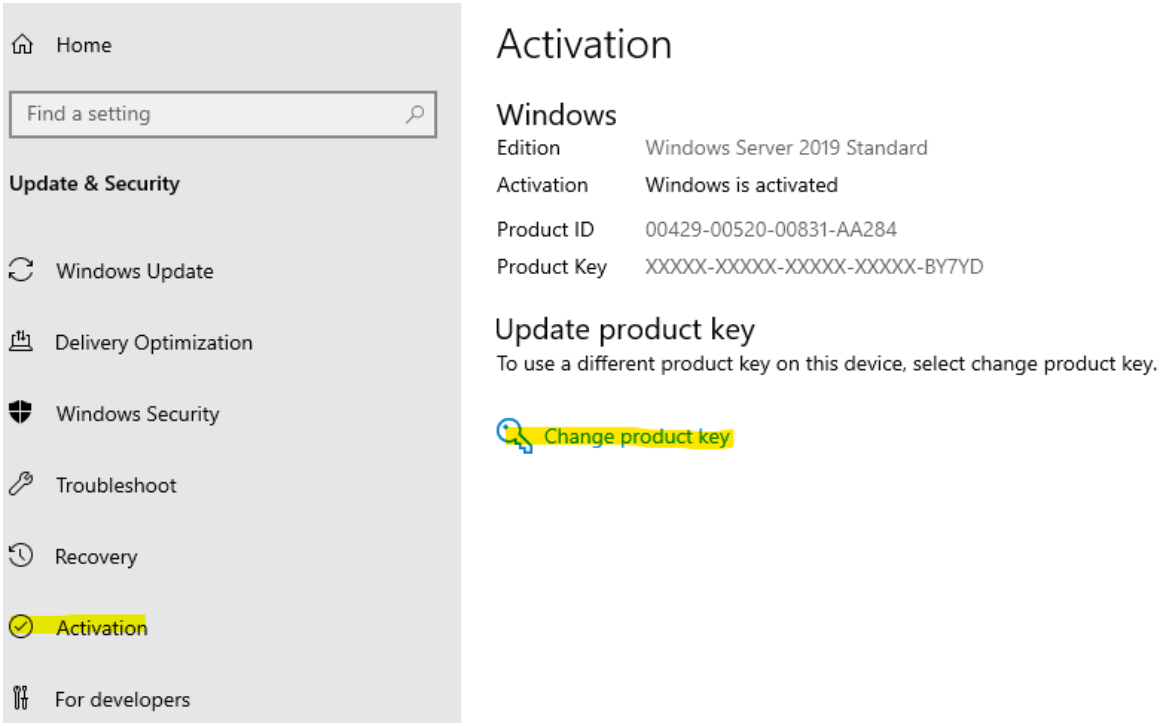
```
wuauclt /detectnow

wuauclt /updatenow
```

9 Aktivieren des Windows Servers

Für den korrekten Betrieb eines Windows Servers, gehört natürlich auch dessen Lizenzierung. Zunächst muss man die richtige Lizenz erworben haben. Welche benötigt wird, hängt vom Einsatzgebiet ab. Wenn man z.B. viel virtualisieren möchte und mehr als zwei Server im Hyper-V benötigt, so reicht die Standardlizenz nicht mehr aus. Auch gilt es wieder vorab die Infrastruktur gut zu planen und auch hier bereits an die Zukunft zu denken.

Die Aktivierung kann regulär über die grafische Oberfläche erfolgen. Dazu braucht man entsprechend den Produktkey. Die Aktivierung kann schon direkt bei der Installation erfolgen.



Sollte Sie allerdings nicht funktionieren, so gibt es das Tool **slmgr.vbs**, mit welchem Windows Systeme anhand der Cmd aktiviert werden können.

10 Das Standard Administratorkonto ändern

Schon bei der Installation muss man für das Administratorkonto ein Passwort vergeben. Dieses Konto hat sämtliche Rechte auf dem Server. Umso wichtiger ist der sorgsame Umgang damit. Das bedeutet, dass man auf alle Fälle ein gutes Passwort verwenden soll.

Hierzu zählt, dass das Passwort mindestens 8 Zeichen enthält und diese aus Gross und -Kleinbuchstaben, sowie Zahlen und Sonderzeichen bestehen. Besser wäre es auch noch, wenn man für administrative Zwecke nicht den Standardadministrator Account verwendet, sondern einen komplett neuen Benutzer erstellt, welcher natürlich die gleichen Rechte erhält wie der Standardadministrator. Den zum einem kann jetzt der vordefinierte Administrator Benutzer deaktiviert werden und zum anderem ist der neue Benutzer nicht bekannt.

Für einen Angriff müssen schliesslich zwei Sachverhalte herausgefunden werden. Dazu zählt der Name des Benutzers sowie sein Passwort.

Als letzter Hinweis wäre noch zu erwähnen, dass man zum einem das Passwort sicher aufbewahren sollte, wie z.B. in einem Safe und zum anderem ist es durchaus sinnvoll das Passwort von Zeit zu Zeit zuändern. Bei der Benutzerverwaltung sollte man noch bedenken, ob es sich um lokale Benutzer handelt oder um Benutzer in einer Active Directory. Mit den folgenden Befehlen wird der lokale Benutzer verwaltet.

10.1 Benutzerverwaltung mit der Windows PowerShell

Im folgendem wird zuerst ein neues Passwort erstellt, welches dann dem neuen Benutzer (Chef) übergeben wird. Gleichzeitig wird dieserBenutzer Mitglied der Gruppe Administratoren. Per **Disable-LocalUser** könnte als letztes noch der Standardadministrator Administrator deaktiviertwerden.

```
$pass = Read-Host -AsSecureString

New-LocalUser -Name Chef -Password $pass |

Add-LocalGroupMember -Group Administratoren

Disable-LocalUser -Name Administrator
```

10.2 Benutzerverwaltung mit der Eingabeaufforderung

```
net user
```

10.3 Gut zu merkendes Passwort erzeugen

Heutzutage benötigt man sehr viele Passwörter. Die grosse Gefahr liegt dabei darin, dass man einfache Namen etc. verwendet und meistens auch immer das gleiche Passwort. Dabei gibt es aber einen sehr einfachen Trick, wie man schwierige Passwörter, welche man sich leicht merken kann, erzeugt.

Man verwendet einen Satz und nimmt daraus nur die Anfangsbuchstaben. So erhält man ein sicheres und auch gut zu merkendesPasswort. Beispiel: Satz: **J**eden **T**ag **u**m **09:30 U**hr **g**ibt **e**s **f**rische **L**eberkässemmeln**!** Passwort: JTu09:30UgefL!

11 Windows Sicherung einrichten

Im nächsten Schritt sollte man sich unbedingt noch Gedanken um eine vernünftige Backupstrategie machen. Zu diesem Aspekt gehören zwei Sachverhalte. Zum einem der Hardwareausfall und zum anderem das eigentliche Backup.

Im ersten Fall wäre hier z.B. eine defekte Festplatte zu erwähnen. Generell ist es Ratsam gegen Hardwareausfälle redundante Komponenten zu verwenden. Dazu zählen u.a. Netzgeräte, Festplatten, RAID Controller, etc. Für Festplatten erstellt man in der Regel ein RAID Level. Aber hier gilt es unbedingt zu beachten, dass ein **RAID kein Backup** ist.

Wenn man z.B. ein RAID Level fünf mit drei Festplatten verwendet, so hat man die Redundanz, dass eine Festplatte ausfallen darf. Wenn allerdings Daten überschrieben werden, sind diese trotzdem verloren.

Hierfür benötigt man ein Backup, welches die Daten aus unterschiedlichen Zeitpunkten sichert.

Mögliche Varianten bzw. Softwareprodukte für eine Backupstrategie wären u.a. die Windows Server Sicherung, Acronis Backup oder auch Veeam Backup.

Generell lässt sich ein RAID Level 0, 1 oder 5 und natürlich auch eine Kombination wie 10 erstellen. Das RAID Level 0 bietet allerdings keinen Schutz vor Datenverlust. Dieses Level ist im Prinzip ein stripeset, was bedeutet, die Daten werden jeweils auf einen Datenträger geschrieben. Dadurch erhöht sich die Performance, allerdings erhält man keine Ausfallsicherheit. Bei einem RAID Level 1 würde man auf jeden Fall die Ausfallsicherheit von mindestens einer Festplatte haben, denn bei einem RAID Level 1 werden zwei Festplatten verwendet , welche gespiegelt sind, was bedeutet, dass die Daten sowohl auf der linken als auch auf der rechten Seite sind.

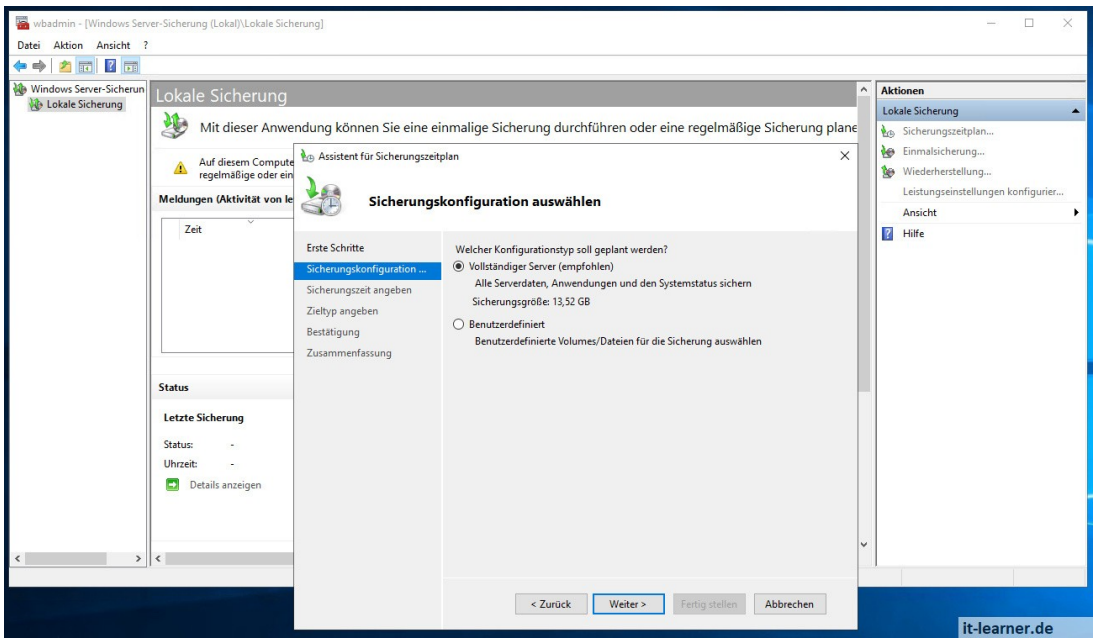
Eine bessere wäre ein RAID Level 5. Hier hat man mindestens drei Festplatten. Daraus wird ein sogenanntes Paritätsbit gebildet, was bedeutet, man hat zusätzlich eine bessere Performance und den Ausfallschutz von einer Festplatte. Kombinationen, wie z.B. RAID 10 benötigen dann Minimum vier Festplatten, wobei jeweils zwei in Kombination zu einem Raid 0 und die zwei gegenüberliegenden dann z.B. zu einem Raid 1 zusammengefasst werden. Generell lässt sich auch noch unterscheiden zwischen

Einem Software-RAID und einem Hardware-RAID.

Ein physikalischer Server besitzt in der Regel immer einen Hardware RAID Controller, dies hat den Vorteil, dass sämtliche Performance nicht vom eigentlichen Betriebssystem weggerechnet wird. Ausserdem bietet es auch einen besseren Schutz. Im Server selbst kann ein Software-RAID angelegt werden. Wenn man ein Hardware RAID verwenden möchte, so muss man sich dessen Konfiguration vor der Installation überlegen.

11.1 Die Windows Server-Sicherung

Neben den vielen Programmen, welche es für das Backup gibt, bietet der Windows Server direkt die



Windows Server Sicherung an. Diese kann als Feature zum Server hinzugefügt werden. Anschliessend lässt sich dadurch eine Einmalsicherung durchführen, oder aber auch ein kontinuierlicher Backupjob einrichten. Zweiteres ist natürlich sinnvoller. Die Sicherung kann dabei auf eine externe Festplatte, sowie aber auch über das Netzwerk erfolgen.

11.2 Windows Server-Sicherung mit der cmd

Die Windows Server Sicherung lässt sich auch über die cmd bzw. Windows PowerShell verwalten. Der Befehl dazu lautet **wbadmin**. Dieses Beispiel zeigt, wie man die komplette Festplatte c:\ auf die Festplatte b:\ sichert.

```
wbadmin start backup -backuptarget:b: -include:c:
```

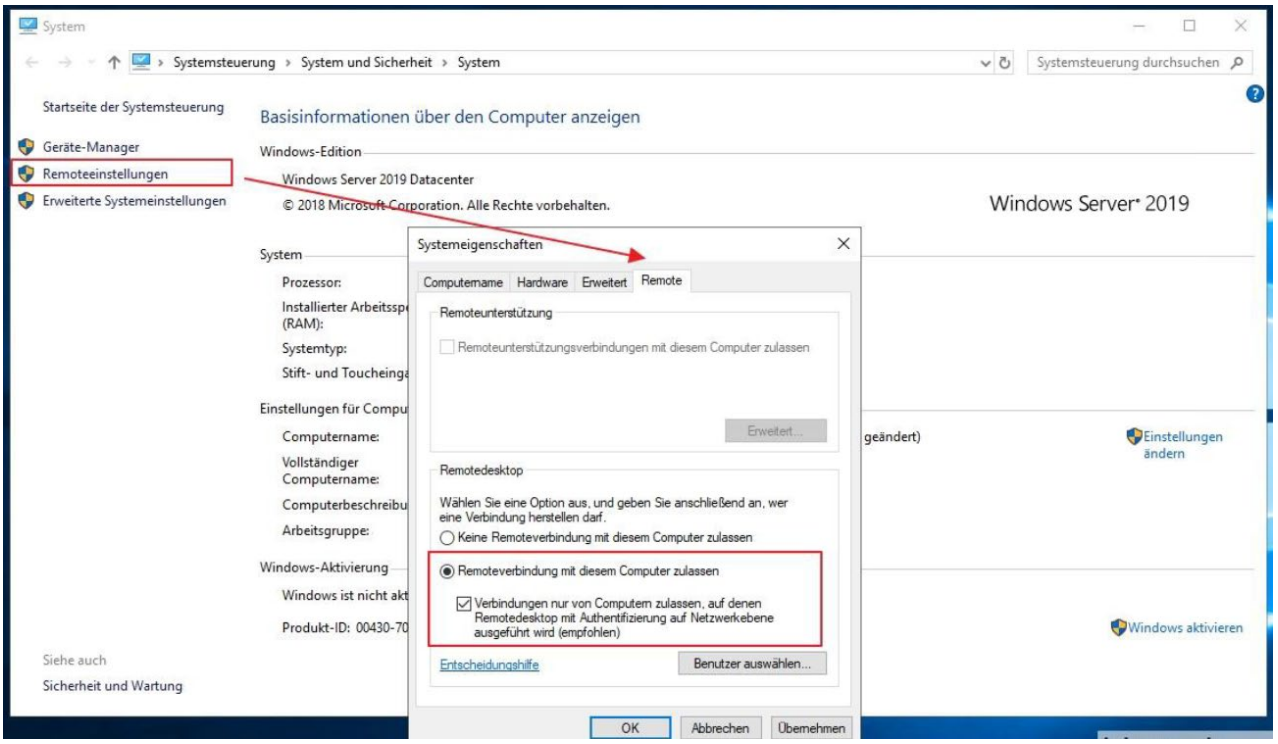
12 Den Server Remote verwalten

12.1 Remotedesktopverbindung einrichten

In der Regel verwaltet man den Server nicht direkt vor Ort. Sondern ausgehend von einem zweiten Rechner per Remote. Diese Remotedesktopverwaltung sollte man natürlich auch unbedingt noch einrichten. Grundsätzlich lässt sich das relativ leicht bewerkstelligen. Zunächst wechselt man in das Menü Systemsteuerung „System und Sicherheit“. Dieses erreicht man auch schnell über die Tastenkombination Windows + Pause Taste. Anschliessend klickt man dort auf die „Remoteeinstellungen“. Hier findet man ganz rechts im oberen Menü unter Remote die Möglichkeit Remote Desktop zu konfigurieren.

Grundsätzlich ist kein Zugriff erlaubt, sondern er muss explizit eingerichtet werden. Infolgedessen klickt man auf „Remoteverbindung mit diesem Computer“ zulassen. Es besteht auch direkt dort die Möglichkeit noch entsprechende Benutzer auszuwählen.

Für eine sichere Verbindung sollte man noch die Authentifizierung auf der Netzwerkebene aktivieren. Dies bedeutet aber auch, dass alle Updates auf dem Client installiert sind, sonst kann keine Verbindung hergestellt werden.

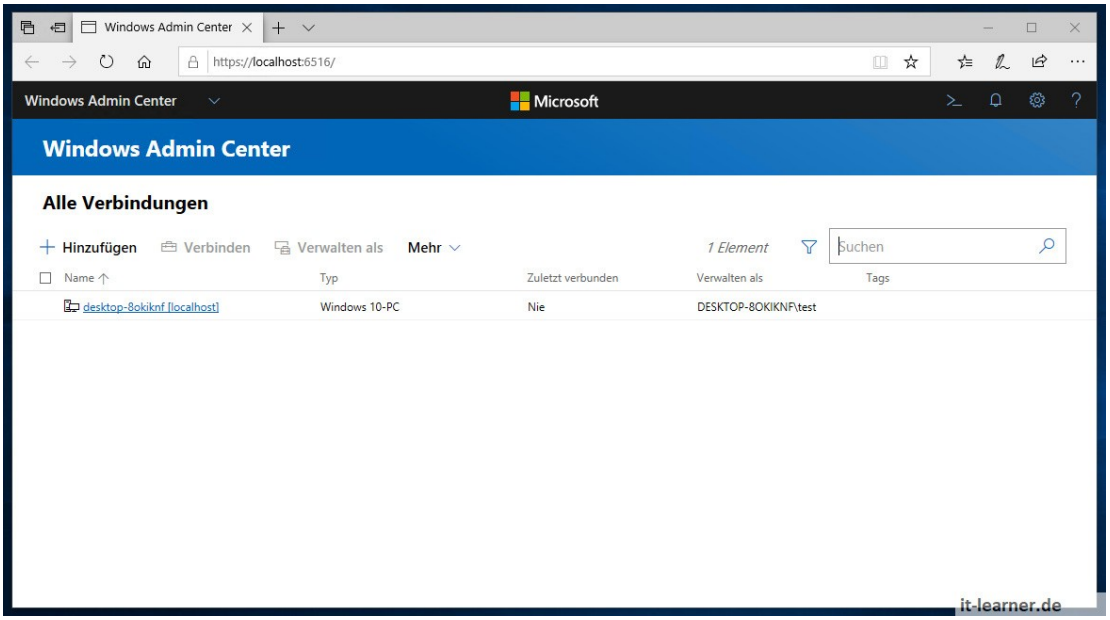


Jetzt kann man ganz einfach testen, ob man sich von einem entfernten Rechner (Natürlich muss sich dieser im gleichen Netz befinden) verbinden kann.

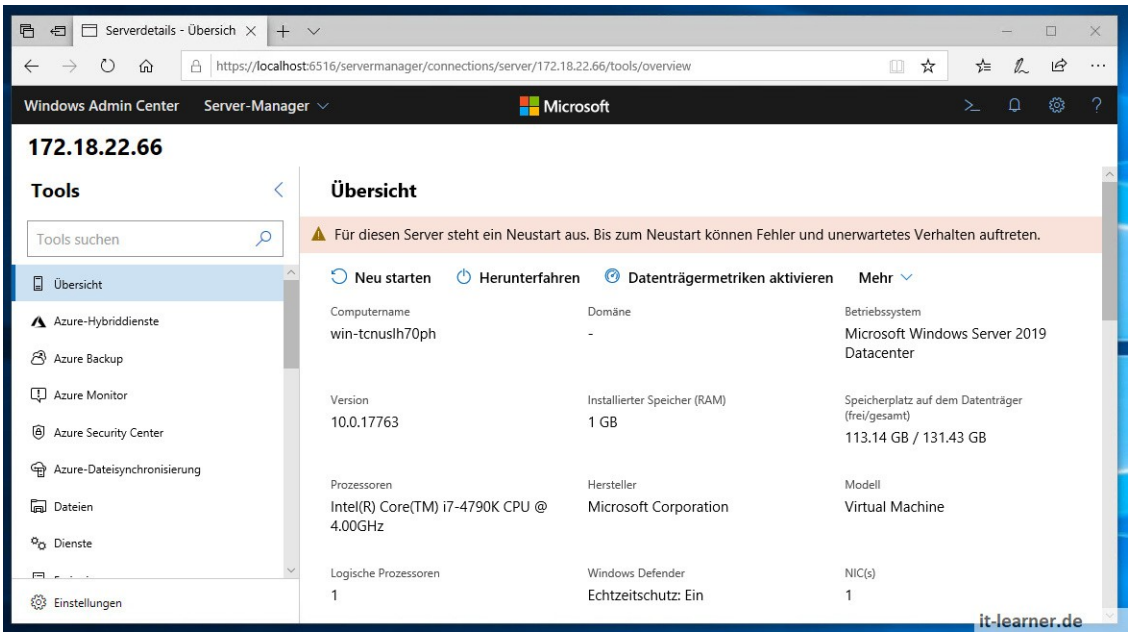
Per Tastenkürzel **mstsc.exe** erreicht man ebenso sehr schnell die Remotedesktopverbindung. Mit den korrekten Anmeldedaten kann man sich nun am Server Remote anmelden. Sofern auch schon ein Namensauflösungssystem wie DNS eingerichtet wurde, kann direkt der Servername verwendet werden. Falls nicht, so muss die IP-Adresse eingetragen werden.

12.2 Remoteverwaltung per Windows Admin Center

Die oben beschriebene Vorgehensweise ist eine Routine Konfiguration. Aber es gibt auch noch neuere Varianten. Eine davon wäre das Windows Admin Center, was man direkt von Microsoft downloaden kann. Dabei erhält man ein msi Paket, welches auf einem Windows 10 oder Windows Server installiert werden kann. Zu beachten ist dabei, dass das Windows Admin Center nicht auf einen Domänencontroller installiert werden kann.



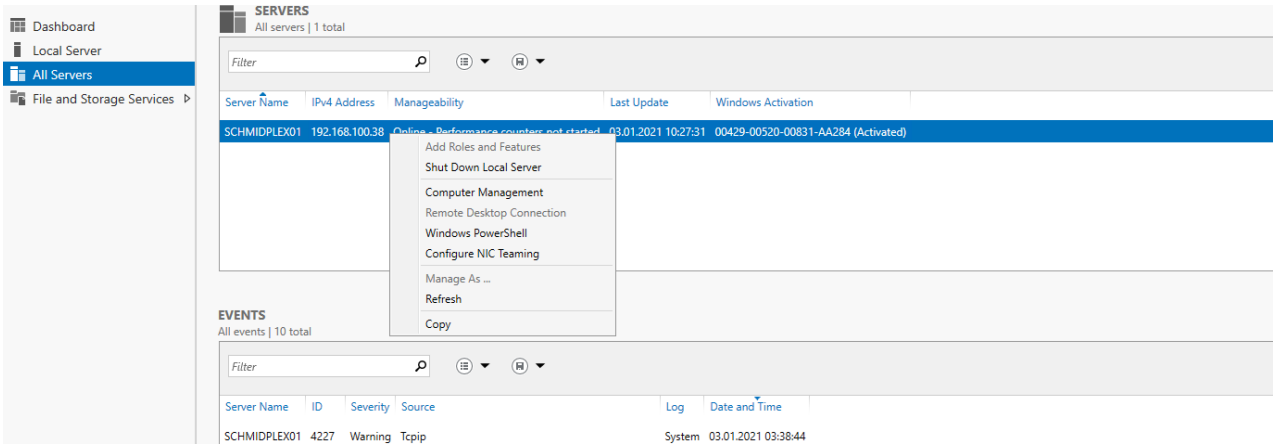
Die Verwaltung basiert anschliessend dann auf einer Browseroberfläche, welche im Webbrowser ausgeführt wird. Für die Installation wird ein Zertifikat benötigt. Dabei ist es am sinnvollsten, wenn ein Zertifikat einer Zertifizierungsstelle der vorhandenen Infrastruktur verwendet wird. Die sonstigen Zertifikate sind in der Regel nur 60 Tage gültig. Nach dem Öffnen des Admin Centers können die Server hinzugefügt werden. Anschliessend hat man auch damit die Möglichkeit sämtliche Konfigurationen vorzunehmen. Wie das folgende Bild zeigt, steht bei dem soeben hinzugefügten Server ein Neustart aus.



Sinnvoll ist das Windows Admin Center dann, wenn man mehrere Server zentral verwalten möchte.

12.3 Remoteverwaltung mittels RSAT Tools

Eine Möglichkeit zur Remoteverwaltung sind die Remoteserver- Verwaltungstools (RSAT). Auch diese können direkt für das entsprechende Betriebssystem von Microsoft downgeloadet werden. Dabei handelt es sich im Prinzip um Optionale Windows Features, welche dem System hinzugefügt werden. Nach der Installation sind bereits alle Features vorhanden. Über den Server Manager unter Windows 10 kann jetzt ein zu verwaltender Server hinzugefügt werden. Darüber lassen sich dann z.B. Rollen und Features installieren.



12.4 Remoteverwaltung mit der Windows PowerShell

Zu guter Letzt wäre noch eine Variante zu nennen. Diese beinhaltet die Verwaltung des Servers über eine Windows PowerShell Konsole. Im Prinzip ist das hauptsächlich für Windows Core Server gedacht. Also Windows Server, welche keine Grafische Oberfläche besitzen. Der Zugriff erfolgt dabei über das folgende Windows PowerShell Cmdlet.

```
Enter-PSSession
```

Allerdings muss vorab der Windows PC sowie der Windows Server für eine Remoteverwaltung vorbereitet werden. Ebenso muss die Authentifizierung eingerichtet werden. Da sich dieses Buch an Einsteiger richtet, möchte ich an dieser Stelle nicht tiefer in dessen Konfiguration eingehen.

13 Windows Server Sicherheit

Standardmässig hat der Server auch Sicherheitsfeatures OnBoard. Diese erreicht man über das Einstellungsmenü anschliessend auf „Update und Sicherheit“ dort auf der linken Seite findet man den Reiter Windows- Sicherheit.

Generell gibt es vier verschiedene Schutzbereiche, welche auf dem sogenannten Windows Defender basieren.

Wenn man keine Drittanbieter Software verwendet, sollte man zu mindestens diesen Schutz aktivieren. Bevor der Server seinen eigentlichen Betrieb startet, wäre ein Virenscan durchaus sinnvoll.

14 Checkliste 10 Punkte nach der Server Installation

Nr.		Beschreibung	Cmd Befehl	PowerShell Befehl
1	☐	Ereignissanzeige überprüfen	Eventvwr.exe	Get-Eventlog
2	☐	Treiber überprüfen	PnPutil.exe	Add-WindowsDriver
3	☐	IP-Konfiguration prüfen Erreichbarkeit prüfen IP-Adressvergabe manuell	 ipconfig /all Ping netsh	 Get-NetIPAdress Test-NetConnection Set-NetIPAddress
4	☐	Servernamen prüfen	WMIC	Rename-Computer
5	☐	Auslagerungsdatei prüfen		
6	☐	Windows Updates prüfen	Wuauclt /detectnow	Install-Module PSWindowsUpdate
7	☐	Windows Firewall prüfen	Netsh advfirewall	Get- NetConnectionProfile
8	☐	Administratorkonto ändern	Net user	New-LocalUser
9	☐	Server aktivieren	Slmgr.vbs	
10	☐	Backup und Ausfallstrategie		

15 Checkliste 10 Tipps für mehr Sicherheit am Server

Nr.		Tipp	Beschreibung
1	☐	Updates prüfen	Den Server regelmässig auf neue Updates prüfen.
2	☐	Backup prüfen	Das Backup kontinuierlich prüfen und auch testen, ob es erfolgreich zurück gesichert werden kann. Am besten mit Hilfe eines Zeitplans
3	☐	Sichere Passwörter	Sichere Passwörter verwenden und diese auch regelmässig wechseln
4	☐	Benutzer anlegen	Am besten einen neuen Administrator Account erstellen und den Default Account deaktivieren
5	☐	Rechtevergabe	Bei der Vergabe von Zugriffsrechten darauf achten, wer Rechte hat und auch wieviel dieser benötigt.
6	☐	Rollen & Feature Installation	Nur die Rollen und Features auf einen Server installieren, welche auch wirklich benötigt werden.
7	☐	Rollen & Features aufteilen	Jeder Server sollte im Prinzip nur eine Aufgabe erfüllen. Also prinzipiell alle Dienste auf verschiedene Server aufsplitten 1x Server DNS 1x Server Domänencontroller 1x Server DHCP etc.
8	☐	Server Replikation	Jeder Server sollte zur Sicherheit einen Replikationsserver besitzen.
9	☐	Neueste Sicherheitsfeatures nutzen	Für die Laufwerksverschlüsselung z.B. Bitlocker oder für VPN z.B. L2TP Over IPSec.
10	☐	Skript Ausführung verbieten	Es sollten keine Skripte auf dem Server ausgeführt werden dürfen. Falls doch, sollten Sie signiert sein.