

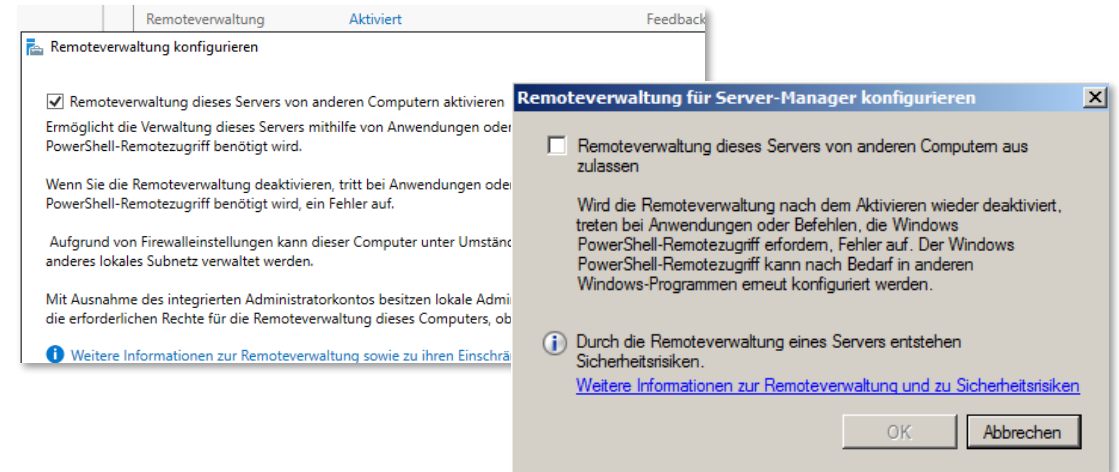
HWBS Windows Server - Remoteverwaltung

Agenda

- Kennen der Möglichkeiten zur Remoteverwaltung
- Konfiguration der Remoteverwaltung
- Verwendung der verschiedenen Tools

Aktivieren Remoteverwaltung

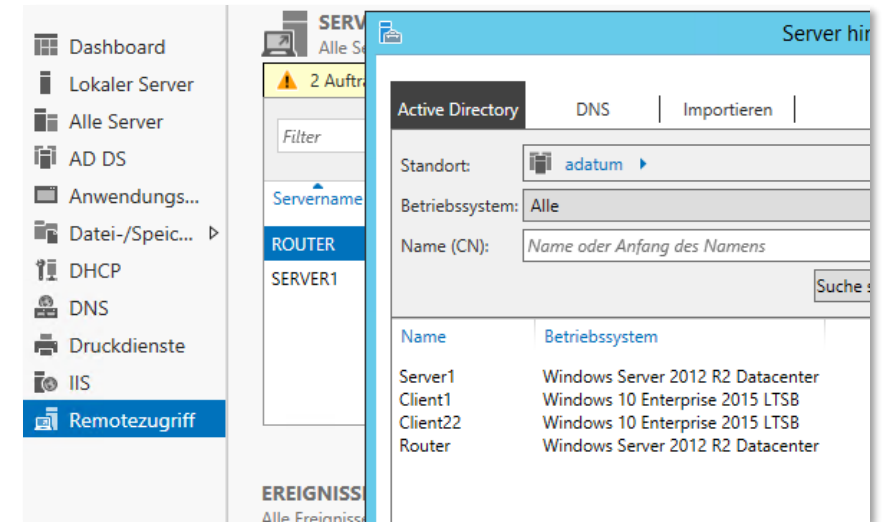
- Server-Manager
- ab Windows-Server 2012 Standard aktiv
- bis Windows-Server 2008 R2 deaktiviert
- Eingabeaufforderung
 - *winrm quickconfig*
- es werden die benötigten Dienste, Ausnahmen in der Firewall und WinRm-Listener konfiguriert



```
C:\Users\Administrator>winrm quickconfig
WinRM ist bereits zum Empfangen von Anforderungen auf diesem Computer konfiguriert.
WinRM wurde nicht für Verwaltungsremotenzugriff auf diesen Computer konfiguriert.
Folgende Änderungen müssen durchgeführt werden:
Erstellen Sie einen WinRM-Listener auf HTTP://*, um die WS-Verwaltungsanforderungen an eine beliebige IP-Adresse auf diesem Computer zu akzeptieren.
Aktivieren Sie die WinRM-Firewallausnahme.
Konfigurieren Sie "LocalAccountTokenFilterPolicy" so, dass lokalen Benutzern remote Administratorrechte gewährt werden.
Diese Änderungen durchführen [y/n]? _
```

Remoteverwaltung

- innerhalb der Domäne ohne zusätzliche Konfiguration
- Server in Server-Manager hinzufügen
- Server mit gleichen Rollen werden zusammen angezeigt
- Zugriff über Server-Manager oder Powershell
- je nach Version des Betriebssystems und ob der verwaltende Computer ein Server- oder Clientbetriebssystem ausführt kann sich die Konfiguration unterscheiden
- für Remoteverwaltung muss RSAT installiert sein



Remoteverwaltung

- innerhalb der Arbeitsgruppe ist zusätzliche Konfiguration nötig
- Vertrauensstellung zwischen Computern muss eingerichtet werden
- Konfiguration auf dem verwaltenden Computer
- Netzwerkprofil muss **Privat** sein
- *Set-Item Wsman:\localhost\Client\TrustedHosts -value **

```
PS C:\Users\Administrator> Set-Item Wsman:\localhost\Client\TrustedHosts -value *  
WinRM-Sicherheitskonfiguration.  
Mit diesem Befehl ändern Sie die TrustedHosts-Liste für den WinRM-Client. Die  
Computer in der TrustedHosts-Liste können möglicherweise nicht authentifiziert  
werden. Der Client sendet möglicherweise Anmeldeinformationen an diese Computer.  
Möchten Sie diese Liste wirklich ändern?  
[J] Ja [N] Nein [H] Anhalten [?] Hilfe (Standard ist "J"): j  
PS C:\Users\Administrator> Get-Item Wsman:\localhost\Client\TrustedHosts  
  
WSManConfig: Microsoft.WSMan.Management\WSMan::localhost\Client  
Type Name SourceOfValue Value  
----  
System.String TrustedHosts *
```

Remoteverwaltung

- Ändern des Netzwerkprofiles
- Powershell
 - *Get-NetConnectionProfile*
 - *InterfaceIndex* ermitteln
 - *Set-NetConnectionProfile*
 - *Set-NetConnectionProfile -InterfaceIndex ... -NetworkCategory Private*

```
PS C:\Users\Administrator> Get-NetConnectionProfile

Name                : Nicht identifiziertes Netzwerk
InterfaceAlias      : Ethernet
InterfaceIndex      : 2
NetworkCategory     : Public
IPv4Connectivity    : NoTraffic
IPv6Connectivity    : NoTraffic

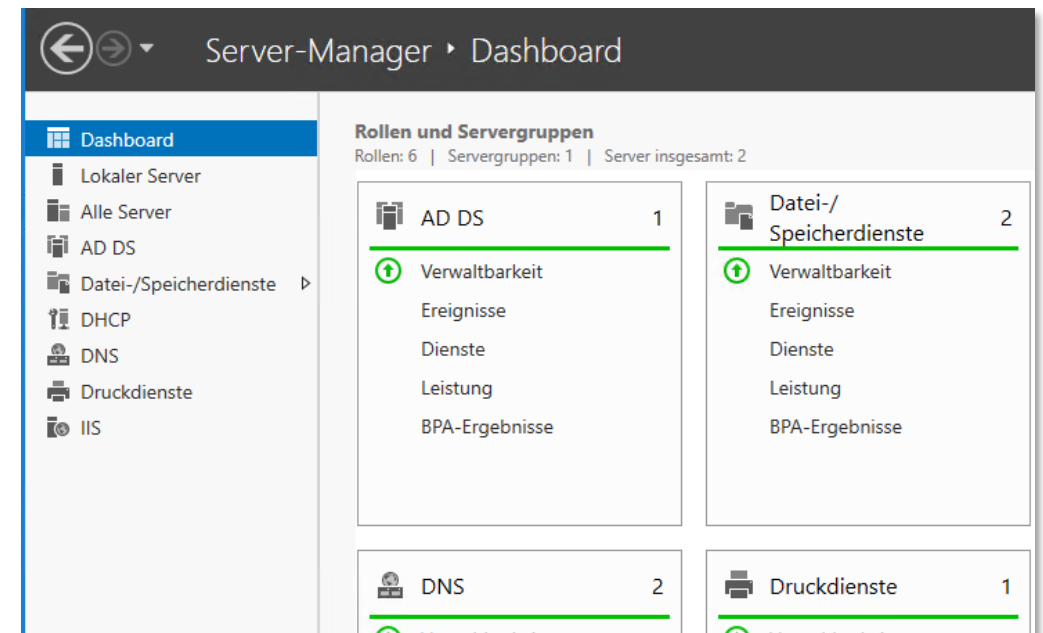
PS C:\Users\Administrator> Set-NetConnectionProfile -InterfaceIndex 2 -NetworkCategory Private
PS C:\Users\Administrator>
```

Tools

- Server-Manager
- Powershell
- MMC
- Eingabeaufforderung
- Remotedesktop

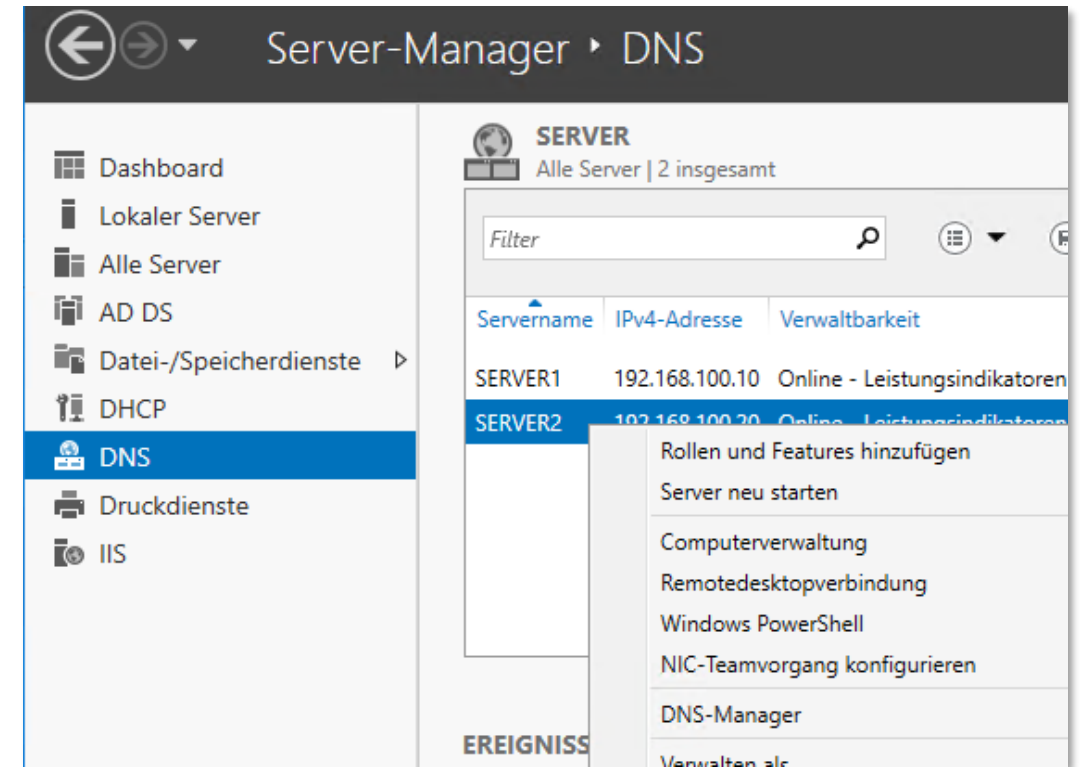
Server-Manager

- der Server-Manager ist seit Windows Server 2012 das wichtigste grafische Tool zur Verwaltung des Servers
- ist für die Verwaltung des lokalen Servers und von Remoteservern ausgelegt
- Remoteserver können gruppiert werden
- alle Server werden rollenbasiert angezeigt
- mit dem Server-Manager können bis Windows Server 2008 R2 verwaltet werden
- Windows Management Framework 5.1 und mind. .net Framework 4.5.2 müssen installiert werden



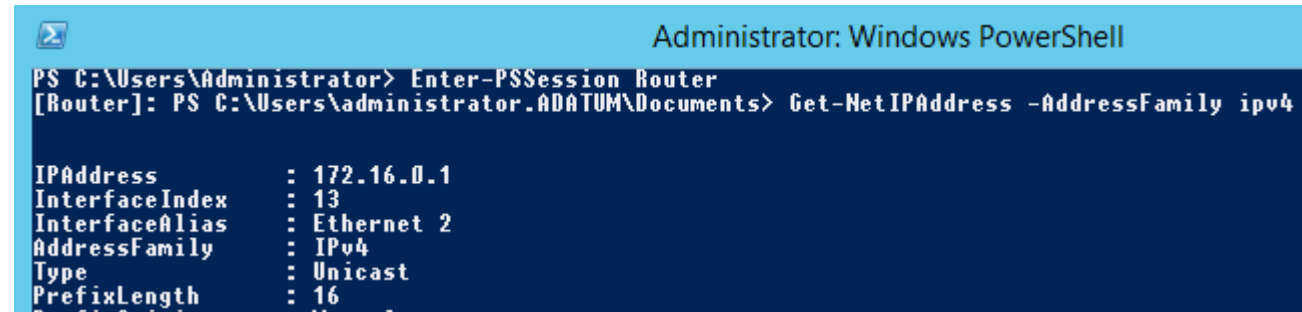
Server-Manager

- ausführbare Aufgaben
 - Hinzufügen von Rollen und Features
 - Starten von Powershell-Sitzungen
 - Anzeigen von Ereignissen
 - Serverkonfiguration



Powershell

- Powershell
 - Server-Manager
 - *Enter-PSSession Server*
- Cmdlet's werden wie am lokalen Computer ausgeführt



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Enter-PSSession Router
[Router]: PS C:\Users\administrator.ADATUM\Documents> Get-NetIPAddress -AddressFamily ipv4

IPAddress      : 172.16.0.1
InterfaceIndex  : 13
InterfaceAlias  : Ethernet 2
AddressFamily   : IPv4
Type            : Unicast
PrefixLength    : 16
```

Powershell

- Ausführungsrichtlinien steuern ob Powershellscripte auf Windows Computern ausgeführt werden dürfen
- auf Windows Clients und bis Server 2008 R2 ist die Ausführung grundsätzlich verboten
- ab Windows Server 2012 dürfen signierte heruntergeladene Scripte ausgeführt werden

```
PS C:\Users\Administrator> Get-ExecutionPolicy
RemoteSigned
```

- *Set-Executionpolicy*

```
NAME
Set-ExecutionPolicy
```

SYNTAX

```
Set-ExecutionPolicy [-ExecutionPolicy] {Unrestricted | RemoteSigned | AllSigned | Restricted |
Default | Bypass | Undefined} [[-Scope] {Process | CurrentUser | LocalMachine | UserPolicy |
MachinePolicy}] [<CommonParameters>]
```

Powershell

- Remoteausführung eines Befehls auf mehreren Servern ohne Sitzung zu erstellen
- Invoke-Command
 - *Invoke-Command Server1,Server2 -Scriptblock {Cmdlet}*

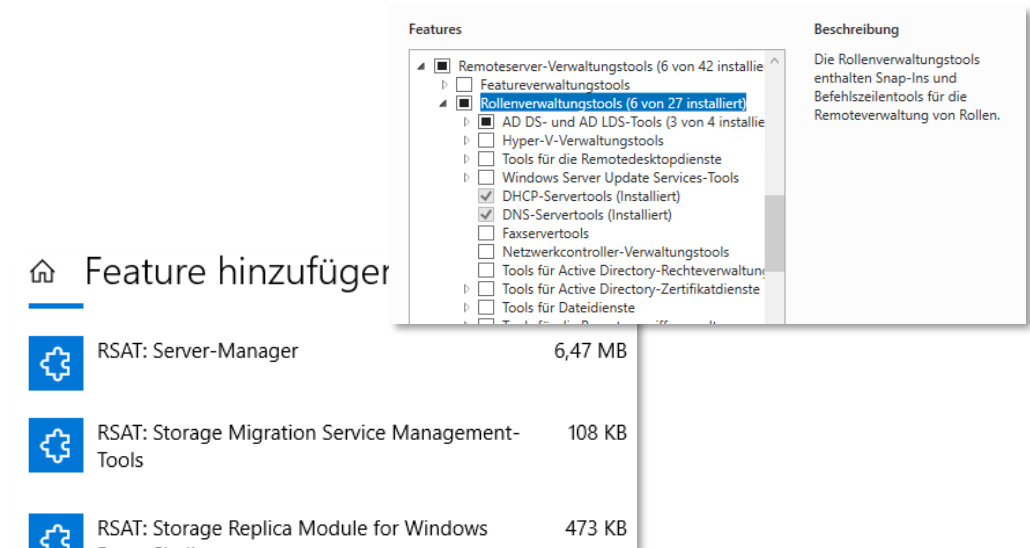
```
PS C:\Users\Administrator> Invoke-Command Server1,Server2 -ScriptBlock {Install-WindowsFeature xps-viewer}

PSComputerName : Server1
RunspaceId     : e308d995-b258-4dfc-b734-fedf8e8c63e4
Success        : True
RestartNeeded  : No
FeatureResult  : {XPS-Viewer}
ExitCode       : Success

PSComputerName : Server2
RunspaceId     : b7085e43-9ab0-49fe-b49f-5d3d082b92b5
Success        : True
RestartNeeded  : No
FeatureResult  : {XPS-Viewer}
ExitCode       : Success
```

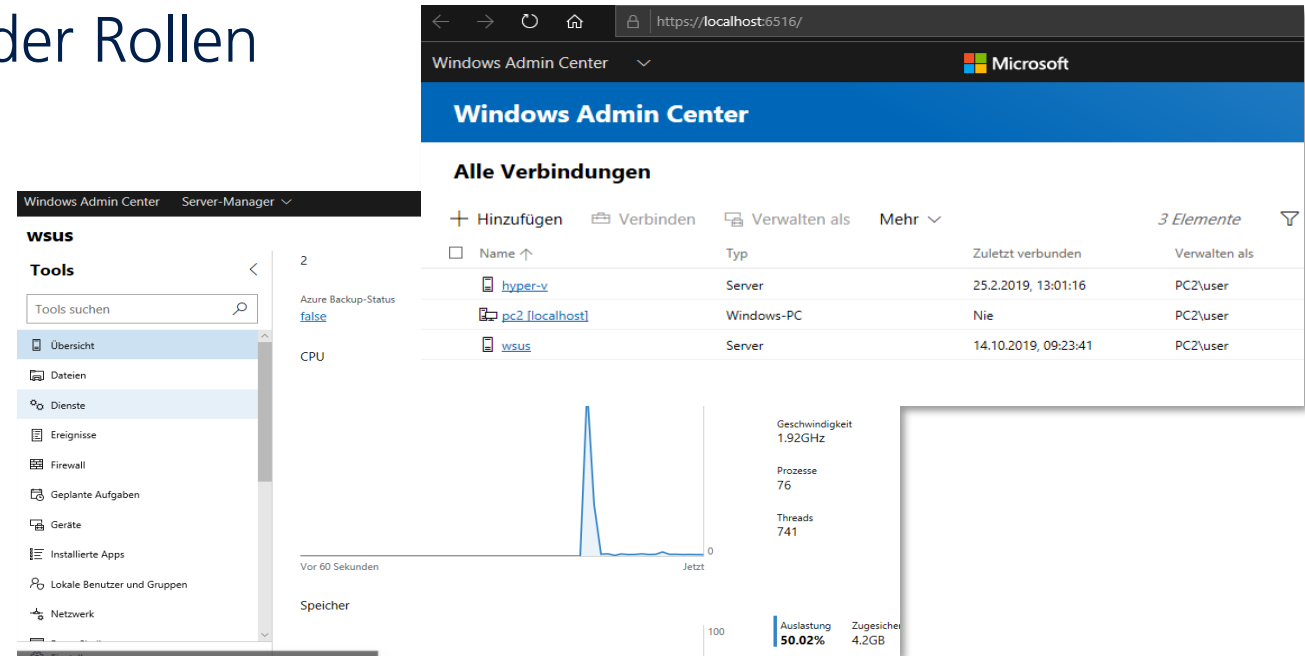
Remote Server Administration Tools

- für die Verwaltung einer Rolle müssen die Verwaltungstools auf dem verwaltenden Computer installiert sein
- bei der lokalen Installation schlägt der Server-Manager deren Auswahl mit vor
- bei Installation mit der Powershell und Remoteinstallation müssen sie ausgewählt werden
- auf Server in Features
- auf Clientcomputern als separates Update vom Microsoft herunterladen
- seit Windows 10 1809 als Optionales Feature in Apps&Features
- RSAT sind angepasst an Server Version



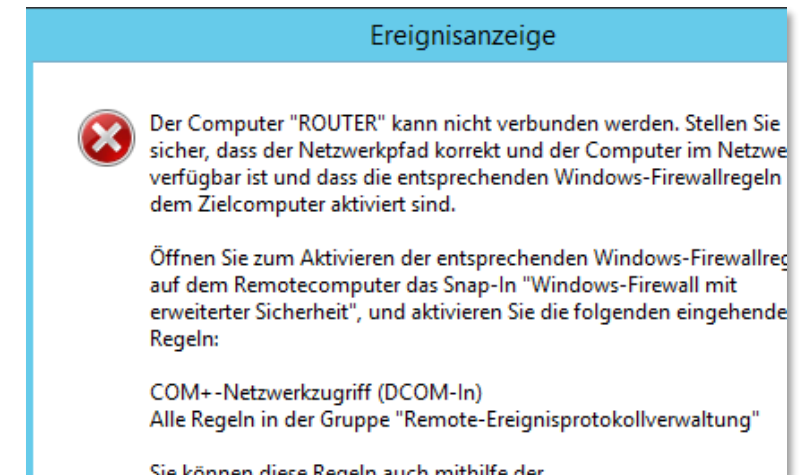
Windows Server Admin Center

- steht seit Windows Server 2019 als separates Download zur Verfügung
- Verwaltung der Server über einen Browser
- Übersicht über den Zustand der Server
- Installation und Verwaltung der Rollen



Firewall – MMC und CMD

- für Remoteverwaltung mit MMC und Eingabeaufforderung muss Firewall angepasst werden
- ggf. sind Regeln für die jeweilige Verwaltungsaufgabe zu aktivieren
- verwenden andere Protokolle als Server-Manager oder Powershell
 - Firewall mit erweiterter Sicherheit
 - netsh



Firewall – MMC und CMD

■ Firewall mit erweiterter Sicherheit


Windows-Firewall mit erweiterter Sicherheit

Eingehende Regeln

Ausgehende Regeln

Verbindungssicherheit

Überwachung

Eingehende Regeln					
Name	Profil	Aktiviert	Aktion	Gruppe	
 COM+ -Netzwerkzugriff (DCOM-In)	Alle	Ja	Zulassen	COM+ -Netzwerkzugriff	
COM+ -Remoteverwaltung (DCOM-In)	Alle	Nein	Zulassen	COM+ -Remoteverwaltung	
Datei- und Druckerfreigabe (Echoanforderung - ICMPv4)	Alle	Nein	Zulassen	Datei- und Druckerfreigabe	
Datei- und Druckerfreigabe (Echoanforderung - ICMPv6)	Alle	Nein	Zulassen	Datei- und Druckerfreigabe	

Windows-Firewall mit erweiterter Sicherheit

Eingehende Regeln

Ausgehende Regeln

Verbindungssicherheit

Überwachung

Eingehende Regeln					
Name	Profil	Aktiviert	Aktion	Gruppe	
Remote-Ereignisprotokollverwaltung (NP eingehend)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (NP eingehend)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (NP eingehend)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (RPC)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (RPC)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (RPC-EPMAP)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remote-Ereignisprotokollverwaltung (RPC-EPMAP)	Alle	Nein	Zulassen	Remote-Ereignisprotokollverwaltung	
Remoteereignisüberwachung (RPC)	Alle	Nein	Zulassen	Remoteereignisüberwachung	

Firewall – MMC und CMD

- netsh

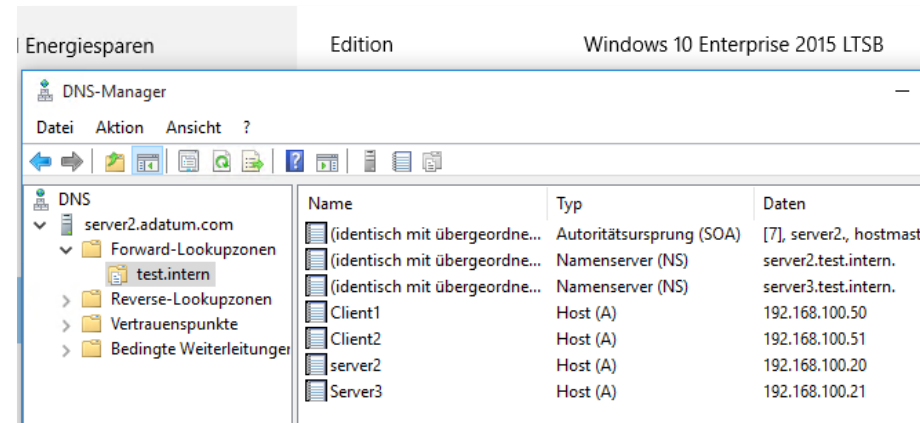
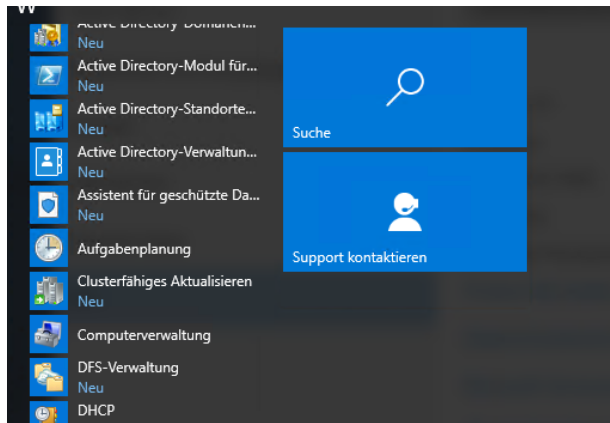
- *netsh advfirewall firewall set rule group="Remote-Ereignisprotokollverwaltung" new enable=yes*
- *netsh advfirewall firewall set rule group="COM+-Netzwerkzugriff" new enable=yes*

```
C:\Windows\system32>netsh advfirewall firewall set rule group="Remote-Ereignisprotokollverwaltung" new enable=yes
7 Regel(n) wurde(n) aktualisiert.
OK.

C:\Windows\system32>netsh advfirewall firewall set rule group="Com+-Netzwerkzugriff" new enable=yes
1 Regel(n) wurde(n) aktualisiert.
OK.
```

Microsoft Management Console

- Snap-In muss hinzugefügt werden
- Snap-In sind die Verwaltungstools für Rollen und Features – RSAT
- RSAT für Client enthalten auch den Server-Manager



Eingabeaufforderung

- Eingabeaufforderung auf dem lokalen Computer
- Befehle werden remote wie lokal ausgeführt
- *winrs -r:server Befehl*

```
C:\Windows\system32>winrs -r:router ipconfig
Windows-IP-Konfiguration

Ethernet-Adapter Ethernet 2:

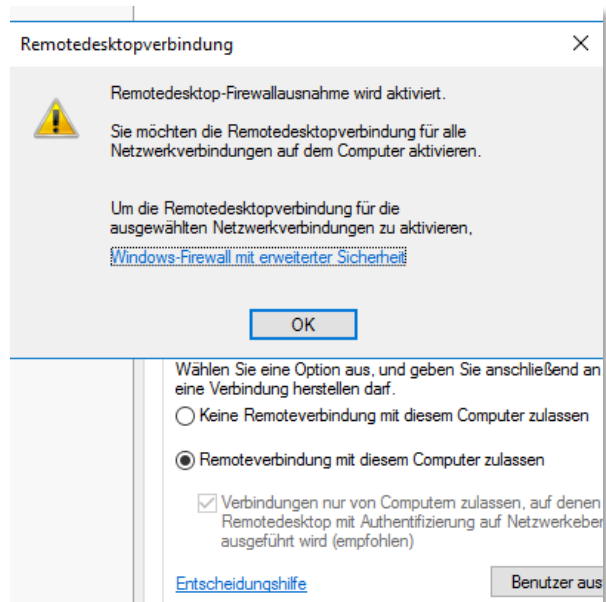
    Verbindungsspezifisches DNS-Suffix:
    Verbindungslokale IPv6-Adresse . . : fe80::2901:b30
    IPv4-Adresse . . . . . : 172.16.0.1
    Subnetzmaske . . . . . : 255.255.0.0
    Standardgateway . . . . . :
```

Remotedesktop

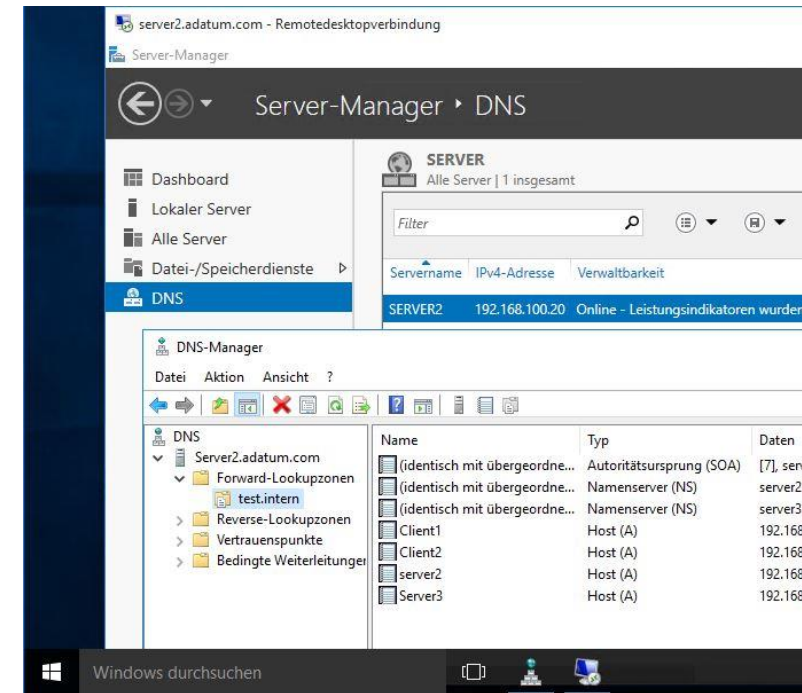
- wie lokale Anmeldung an Remoteserver
- standardmäßig deaktiviert
- bei Aktivierung festlegen der Sicherheit
 - Authentifizierung auf Netzwerkebene ab Windows Vista / Server 2008
 - ohne Authentifizierung auf Netzwerkebene bis Windows XP / Server 2003
- Ausnahme in der Firewall wird für TCP Port 3389 aktiviert
- Benutzer muss Mitglied der lokalen Gruppe Remotedesktopbenutzer sein
- Benutzer benötigt lokale Rechte zur Verwaltung

Remotedesktop

Aktivieren Remotedesktop



Remotedesktopverbindung





**VIELEN DANK
FÜR IHRE
AUFMERKSAMKEIT!**