2019 Core

- Remotemanagement
- Firewall
- Firewall - 2

Remotemanagement

Remote Management aktivieren

Der Core Server lässt sich über eine Arbeitsstation oder einen anderen Server Remote verwalten. Um auf dem entfernten Server Cmdlets ausführen zu können, muss folgendes vorbereitet werden.

Die Arbeitsstation/Server bereiten wir wie folgt vor, auf dem Core Server ist nichts weiter zu tun:

winrm quickconfig
winrm set winrm/config/client @{TrustedHosts=”*”}
chcp 65001

Enable-NetFirewallRule -DisplayGroup "Windows Remote Management" / Nicht sicher ob man dies braucht. Zuerst mit den unteren Befehlen testen

3

1

```
#  Enable Windows Firewall Remote Management
```

2

```
Set-NetFirewallRule –Name “RemoteFwAdmin-In-TCP” –Enabled True
```

3

```
Set-NetFirewallRule –Name “RemoteFwAdmin-RPCSS-In-TCP” –Enabled True
```

cmdkey /add:192.168.0.70 /user:Administrator -> mal als Info gespeichert

Firewall

Windows Firewall offers three firewall profiles:

- **Domain profile**: applies to networks where the host system can authenticate to a domain controller.
- **Private profile**: a user-assigned profile and is used to designate private or home networks.
- **Public profile**: this is the default profile. It is used to designate public networks such as Wi-Fi hotspots at coffee shops, airports, and other locations.

Get status of the Windows Firewall with PowerShell

First, let's get the current status of the Windows Firewall. We will be using the Get-NetFirewallProfile cmdlet.

```
PS C:\> Get-NetFirewallProfile | Format-Table Name, Enabled


Name    Enabled
----    -------
Domain     True
Private    True
Public     True
```

Copy

We have **three profiles**: Domain, Name, and Public. Windows Firewall is enabled on all three profiles.

Disable Windows Firewall in Windows Server 2012/2016/2019

Disable Windows Firewall on all three profiles.

```
PS C:\> Set-NetFirewallProfile -Profile Domain, Public, Private -Enabled False
```

Copy

Check Windows Firewall status

Check the status after you disable the Firewall on all three profiles. Run the **Get-NetFirewallProfile** cmdlet.

```
PS C:\> Get-NetFirewallProfile | Format-Table Name, Enabled


Name    Enabled
----    -------
Domain    False
Private   False
Public    False
```

Firewall - 2

There are actually a whole series of groups that you need to look at for remote administration, depending upon what you want to remotely manage. The name of the firewall group is Windows Firewall Remote Management.

You can find the names of the individual rules, if you want to ensure you just enable the specific ones you want, by issuing the following command:

Get-NetFirewallRule | Where { $_.DisplayGroup –Eq “firewall group”} | Format-Table
Replace firewall group with with the appropriate managment group. The ones that relate to remote management are:

group="File and Printer Sharing"

group="Remote Service Management"

group="Performance Logs and Alerts"

group="Remote Event Log Management"

group="Remote Scheduled Tasks Management"

group="Remote Volume Management"

group="Remote Desktop"

group="Windows Firewall Remote Management"

group="windows management instrumentation (wmi)"