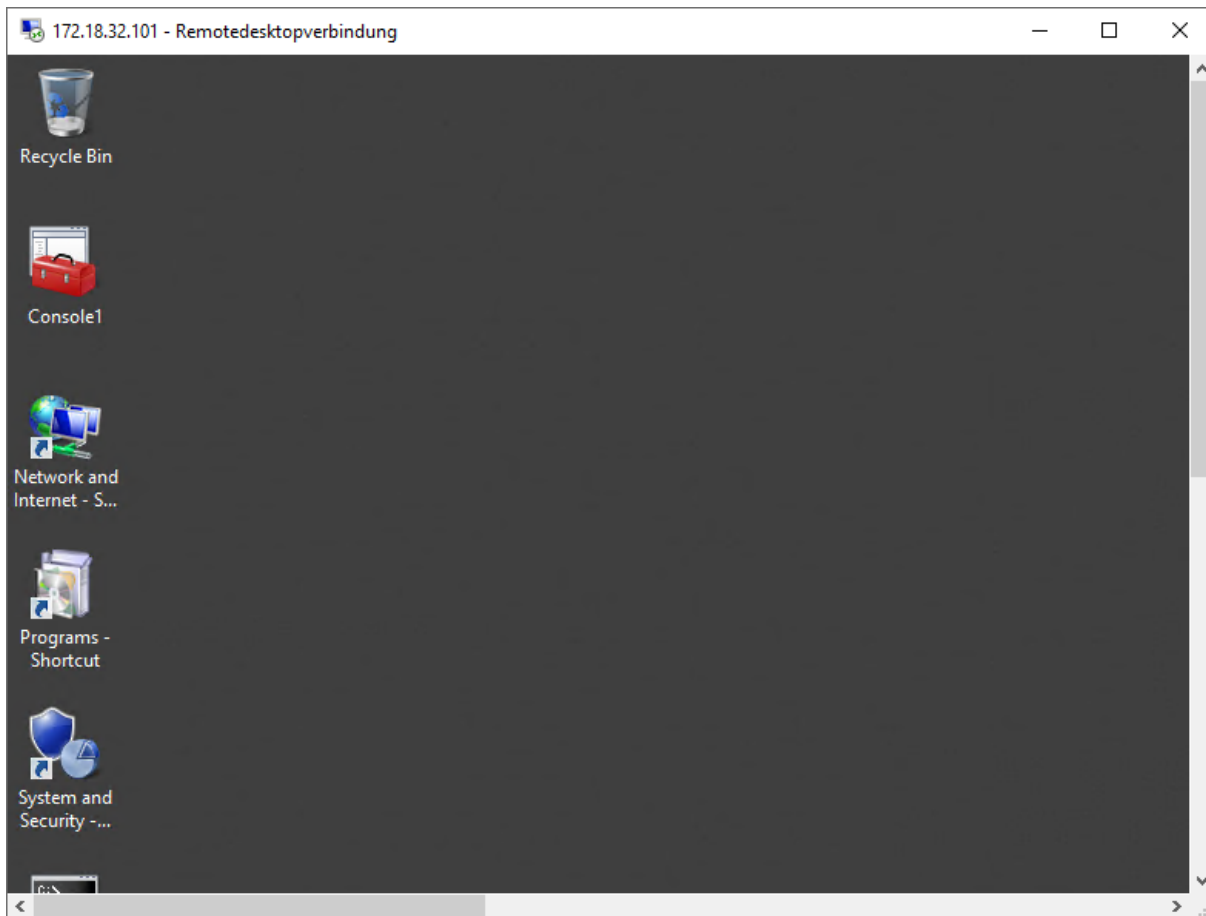




QWINSTA Remote abmelden

Angemeldete Remote-User von einem Server abmelden. Auf dem Server SRV02 (172.18.32.101) ist der Benutzer NDS angemeldet und blockiert eine benötigte Session.



Mit dem Tool qwinsta bekommen wir einen Überblick darüber, wer auf dem Server angemeldet ist.

Wir stellen vom DC01 eine Verbindung zu SRV02 her. Leider scheitert diese mangels benötigter Freischaltungen. Fehler 1722!

```
Administrator: Eingabeaufforderung
C:\Windows\system32>qwinsta.exe /Server:SRV02
Fehler 1722 beim Abrufen der Sitzungsnamen
Fehler [1722]:Der RPC-Server ist nicht verfügbar.

C:\Windows\system32>hostname
DC01

C:\Windows\system32>
```



QWINSTA Remote abmelden

Auf dem Zielsystem müssen Firewall-Regeln erstellt werden bzw. aktiviert werden.

Da ich ein Mensch der Konsole bin erstelle ich auf dem Server SRV02 gleich mal eben 4 Regeln:

```
netsh advfirewall firewall add rule name="Open Port 135 RPC" dir=in action=allow protocol=TCP localport=135
```

```
netsh advfirewall firewall add rule name="Open Port 135 RPC" dir=in action=allow protocol=UDP localport=135
```

```
netsh advfirewall firewall add rule name="Open Port 445 RPC" dir=in action=allow protocol=TCP localport=445
```

```
netsh advfirewall firewall add rule name="Open Port 445 RPC" dir=in action=allow protocol=UDP localport=445
```

```
C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 135 RPC" dir=in action=allow protocol=TCP localport=135
Ok.

C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 135 RPC" dir=in action=allow protocol=UDP localport=135
Ok.

C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 445 RPC" dir=in action=allow protocol=TCP localport=445
Ok.

C:\Windows\system32>netsh advfirewall firewall add rule name="Open Port 445 RPC" dir=in action=allow protocol=UDP localport=445
Ok.

C:\Windows\system32>hostname
SRV02

C:\Windows\system32>
```

Jetzt sollte der Zugriff funktionieren, korrekt.

- 1) Verbindung herstellt
- 2) Verbindung des Benutzer NDS mit der ID 1 wurde erfolgreich getrennt

```
C:\Windows\system32>qwinsta.exe /Server:SRV02
Fehler 1722 beim Abrufen der Sitzungsnamen
Fehler [1722]:Der RPC-Server ist nicht verfügbar.

C:\Windows\system32>hostname
DC01

C:\Windows\system32>qwinsta.exe /Server:SRV02 1
SITZUNGSNAME  BENUTZERNAME  ID  STATUS  TYP  GERÄT
services     0  Getr.
rdp-tcp#2     NDS             1  Aktiv
console      3  Verb.
rdp-tcp      65536  Abhör.

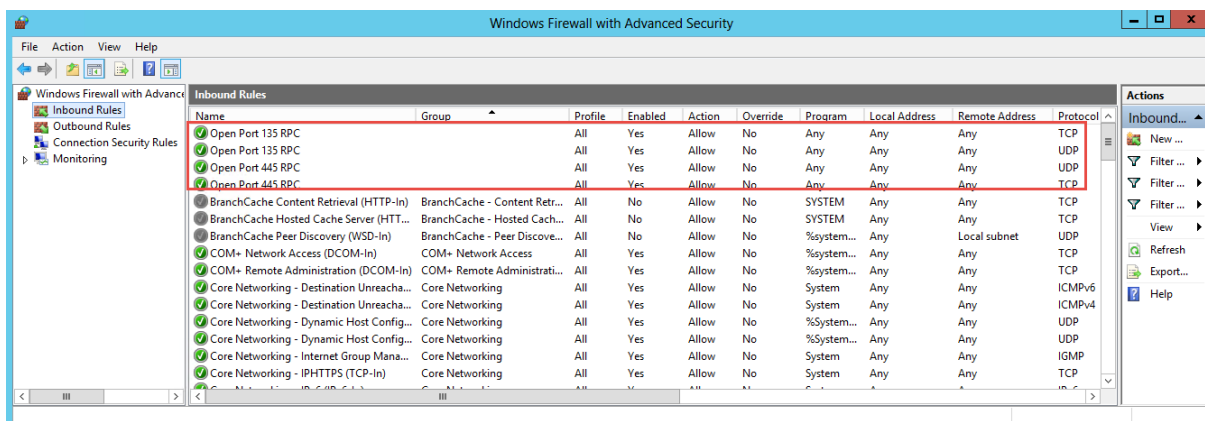
C:\Windows\system32>logoff 1 /Server:SRV02 2

C:\Windows\system32>
```



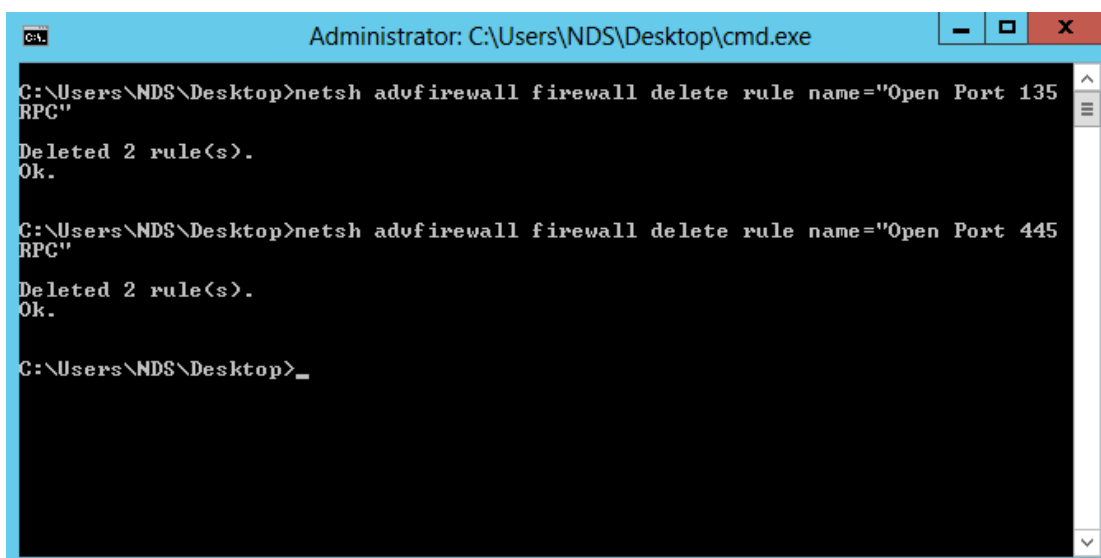
QWINSTA Remote abmelden

Die Firewall-Regeln lassen sich genauso schnell wieder löschen:



```
netsh advfirewall firewall delete rule name="Open Port 135 RPC"
```

```
netsh advfirewall firewall delete rule name="Open Port 445 RPC"
```



Befehle:

qwinsta = Query WINDows STAtion = zeigt Terminalsitzungen an

rwinsta = Reset WINDows STAtion = setzt Terminalsitzungen zurück

/Server:Servername	Abzufragender Server (Standard ist der aktuelle Server). IP-Adresse ist auch möglich.
/MODE	Zeigt aktuelle Leitungseinstellungen der RDP-Sitzungen an.
/FLOW	Zeigt aktuelle Flusssteuerungseinstellungen an.
/CONNECT	Zeigt aktuelle Verbindungseinstellungen der RDP-Sitzungen an.
/COUNTER	Aktuelle Zählerinformationen für die Remotedesktopdienste anzeigen.
/VM	Zeigt Informationen zu Sitzungen innerhalb von virtuellen Computern an.