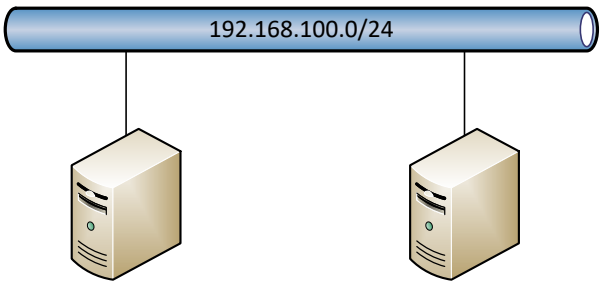
Inhalt

1. Szenario

IST-Zustand

Meine RDS-Infrastruktur besteht derzeit noch aus 2 Windows Server 2012R2:



WS-RDS1.ws.its
RDS(B,W,G,S,L),NLB
Win 2012R2
192.168.100.16/24
192.168.100.26/24

WS-RDS2.ws.its
RDS(W,G,S,L),NLB
Win 2012R2
192.168.100.21/24
192.168.100.26/24

Beide Server führen die Services RDS-Webserver, Lizenzserver, Gateway und Sessionhost aus. Auf WS-RDS1 läuft der SessionBroker mit einer lokalen Datenbank (WID). Beide Server bieten die Webservices über eine NLB-Clusteradresse an.

WS-RDS1 ist ein Mitglied der Collection RDS-RemoteApps. Hier veröffentliche ich nur Anwendungen. Auf WS-RDS2 wird eine komplette Desktop-Session über eine 2. Collection bereitgestellt.

Beide Server verwenden ein externes Zertifikat, dass nun abgelaufen ist. Der externe Zugriff läuft durch einen WebApplicationProxy-Cluster, der auf den VMs WS-RA1 und WS-RA2 installiert ist.

Auf WS-RDS1 laufen einige zentrale Scripte über Tasks.

Soll-Zustand

Die RDS-Infrastruktur soll verkleinert werden: zukünftig wird nur noch eine VM benötigt. Diese soll dann alle RDS-Funktionen übernehmen.

Das Betriebssystem soll ein Windows Server 2016 DC. Ein Upgrade wird ausgeschlossen.

Die alten Lizenzen sollen migriert werden.

Migrationsweg

WS-RDS2 kann im Vorfeld entfernt werden. Die Lizenzen sollen aber übernommen werden. Da alle neuen Funktionen auf WS-RDS1 ausgeführt werden sollen und dafür nur ein Wipe & Load in Frage kommt, ist dieser Migrationsweg möglich:

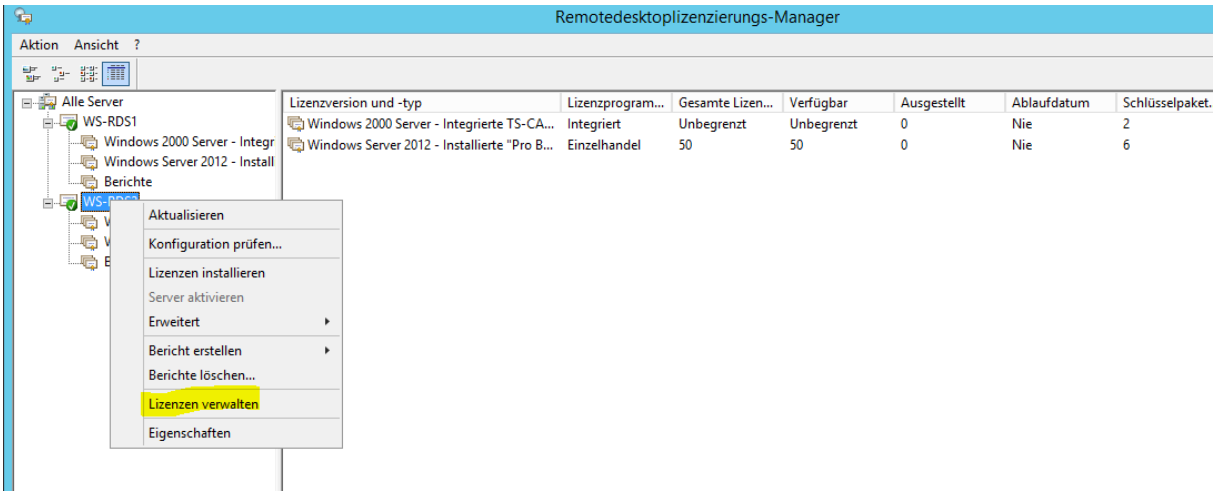
- WS-RDS2 man alle RDS-Rollen außer dem Lizenzserver deinstallieren
- Dann kann man die Lizenzen vom alten WS-RDS1 auf den alten WS-RDS2 übertragen,
- Nun kann WS-RDS1 komplett entfernt werden. Zu dieser Zeit existiert dann nur noch ein alter Lizenzserver mit allen Lizenzen
- Der neue Server wird ohne Übernahme der alten Konfigurationen mit allen RDS-Rollen neu installiert
- Nun kann man die alten Lizenzen auf den neuen WS-RDS1 verschieben und den alten WS-RDS2 deinstallieren

Während der Umstellung stehen die RD-Services nicht zur Verfügung.

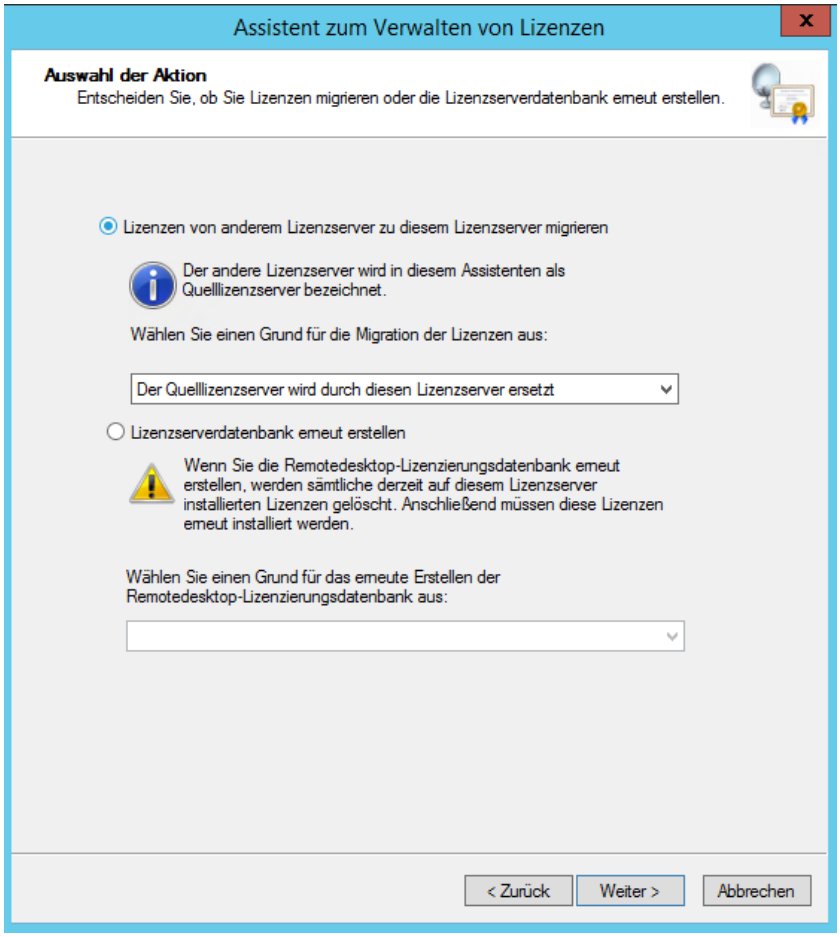
2. Vorbereitung der Migration

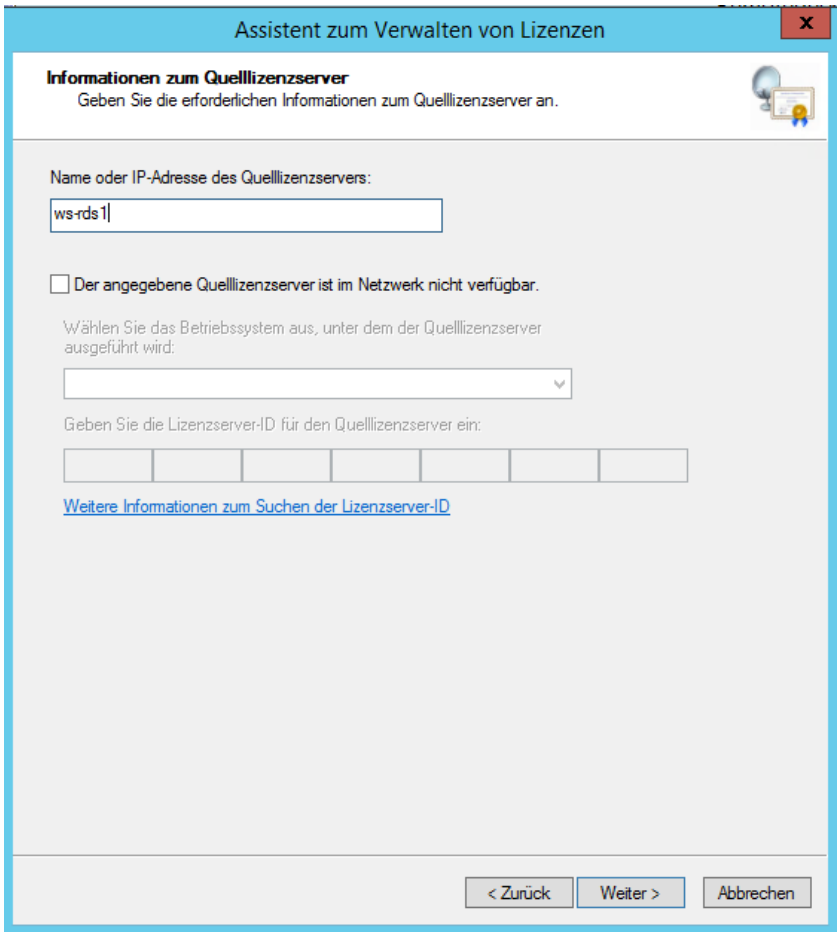
Verschieben aller Lizenzen von WS-RDS1 auf WS-RDS2

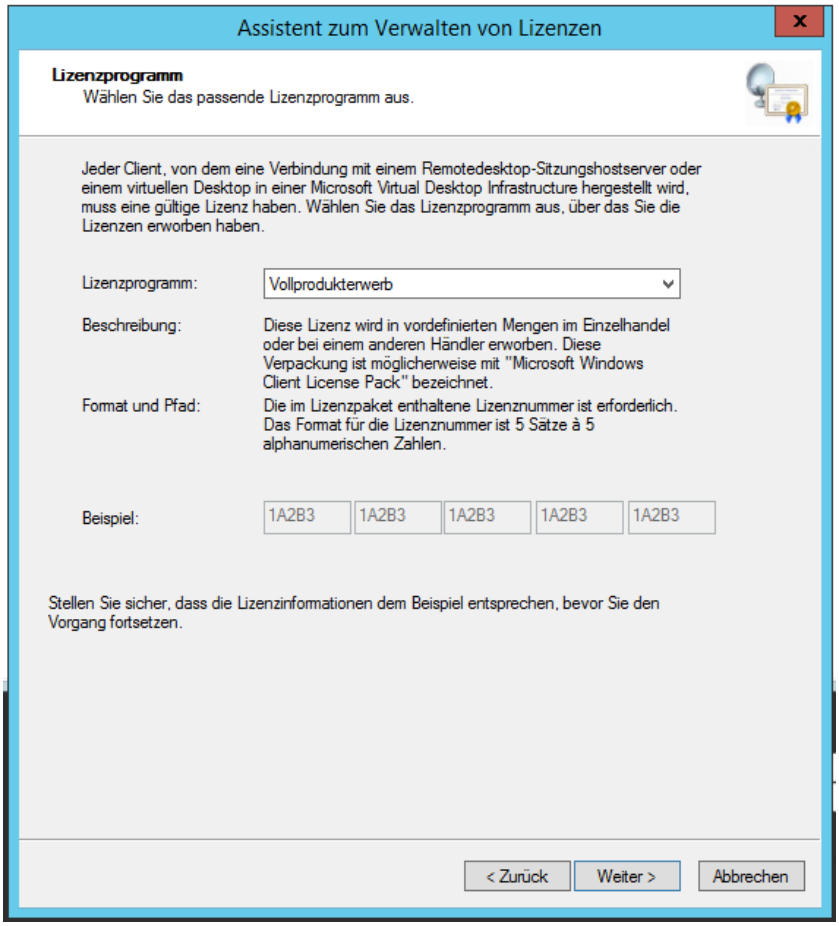
Die Lizenzen können mit der RD-Lizenzierungsmanager-MMC online verschoben werden. Dies muss auf dem Zielserver passieren:



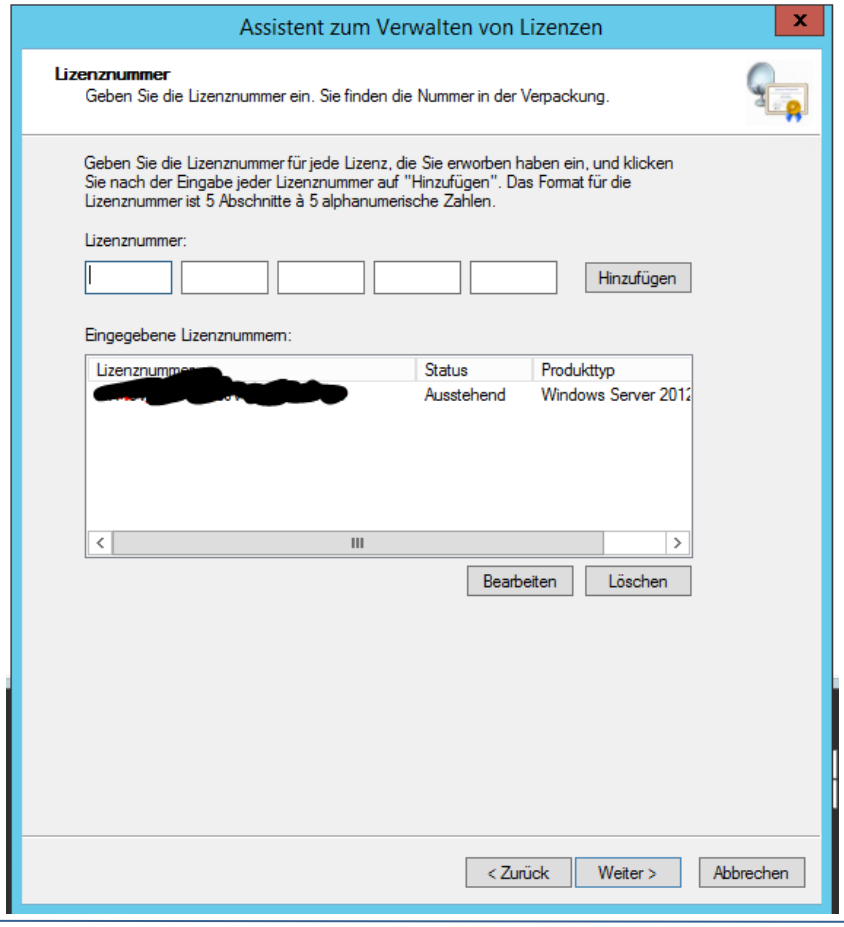
Der Dialog ist einfach aufgebaut:

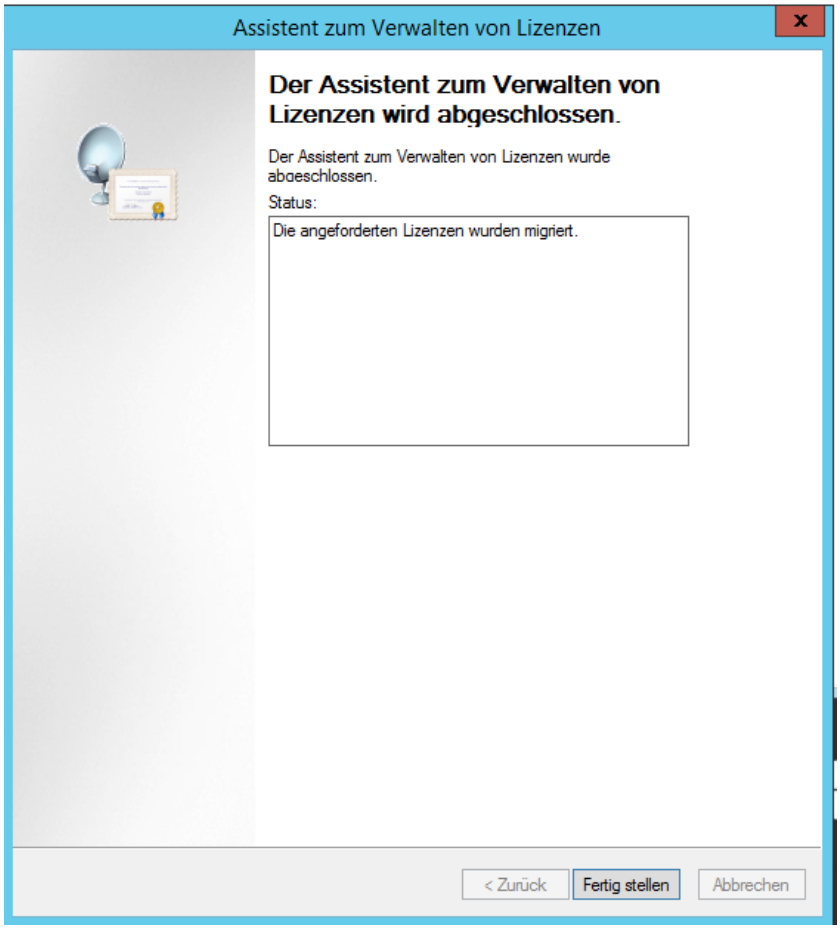

Assistent zum Verwalten von Lizenzen
Auswahl der Aktion
Entscheiden Sie, ob Sie Lizenzen migrieren oder die Lizenzserverdatenbank erneut erstellen.
Lizenzen von anderem Lizenzserver zu diesem Lizenzserver migrieren
Der andere Lizenzserver wird in diesem Assistenten als Quelllizenzserver bezeichnet.
Wählen Sie einen Grund für die Migration der Lizenzen aus:
Der Quelllizenzserver wird durch diesen Lizenzserver ersetzt
Lizenzserverdatenbank erneut erstellen
Wenn Sie die Remotedesktop-Lizenzierungsdatenbank erneut erstellen, werden sämtliche derzeit auf diesem Lizenzserver installierten Lizenzen gelöscht. Anschließend müssen diese Lizenzen erneut installiert werden.
Wählen Sie einen Grund für das erneute Erstellen der Remotedesktop-Lizenzierungsdatenbank aus:
< Zurück
Weiter >
Abbrechen


Assistent zum Verwalten von Lizenzen
Informationen zum Quelllizenzserver
Geben Sie die erforderlichen Informationen zum Quelllizenzserver an.
Name oder IP-Adresse des Quelllizenzservers:
ws-rds1
Der angegebene Quelllizenzserver ist im Netzwerk nicht verfügbar.
Wählen Sie das Betriebssystem aus, unter dem der Quelllizenzserver ausgeführt wird:
Geben Sie die Lizenzserver-ID für den Quelllizenzserver ein:
Weitere Informationen zum Suchen der Lizenzserver-ID
< Zurück
Weiter >
Abbrechen

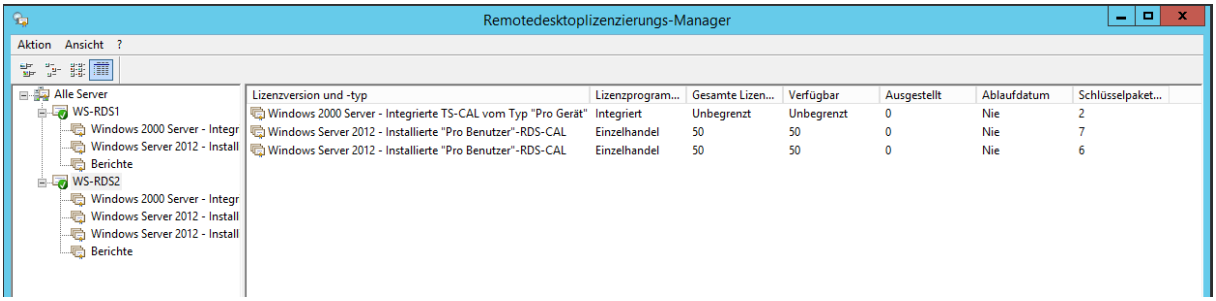


Die Lizenzschlüssel müssen dennoch bekannt sein. Sonst könnte ja jeder kommen ☺:



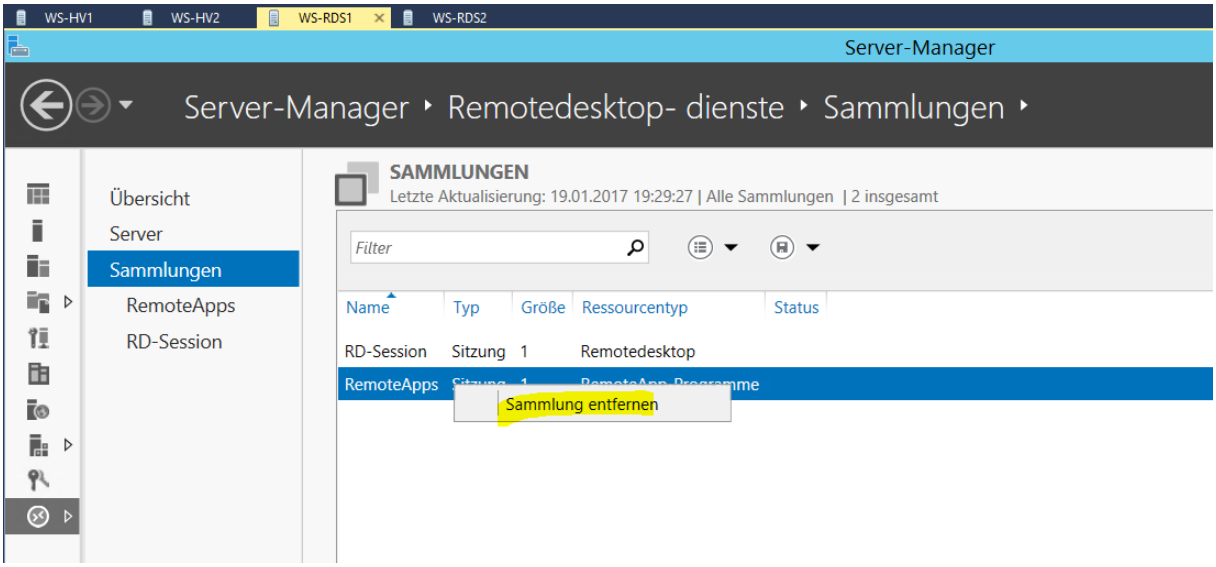


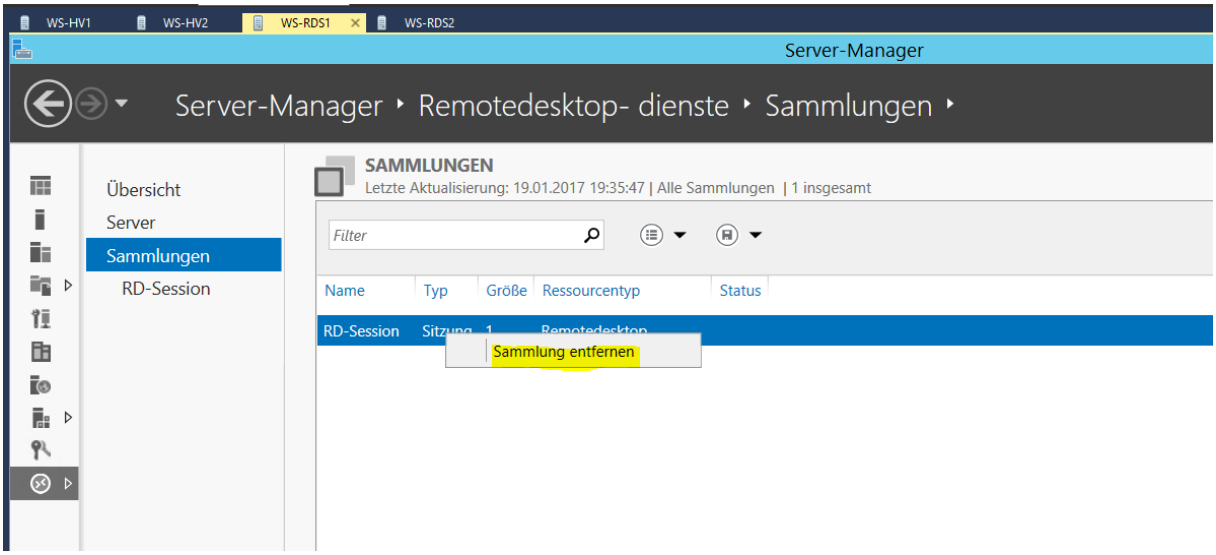
Das Ergebnis passt:



Entfernen aller Sammlungen zum Deinstallieren der RDS-Rollen

Ein RDS kann nicht deinstalliert werden, wenn er noch in Collections als SessionHost registriert ist. Da eine Collection nicht ohne Host betrieben werden kann muss ich diese löschen:

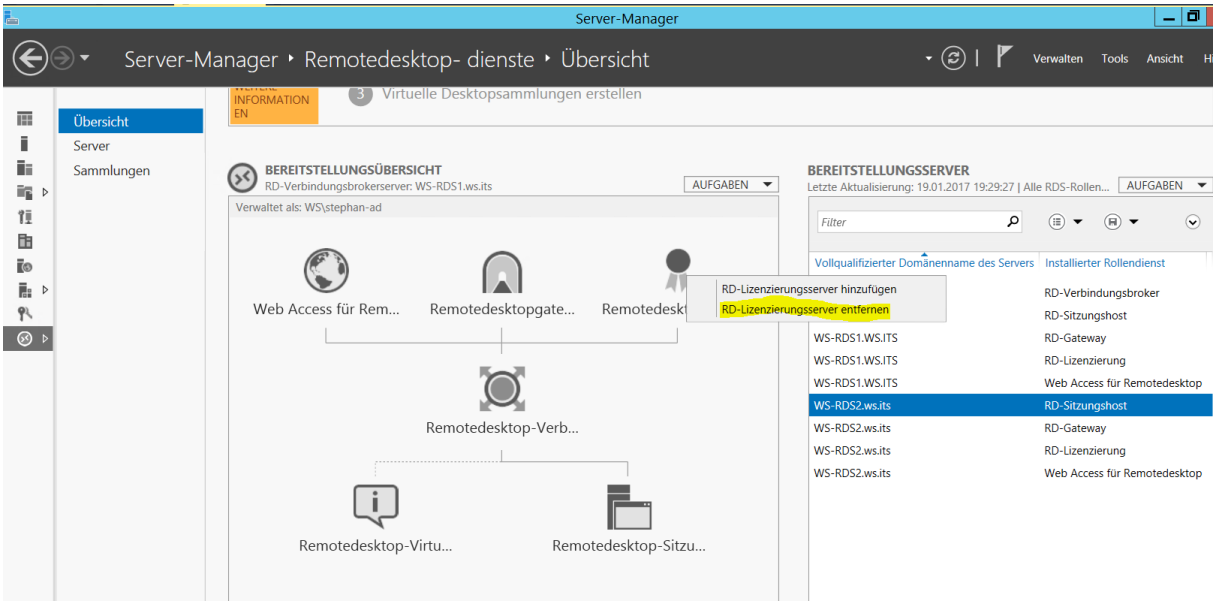


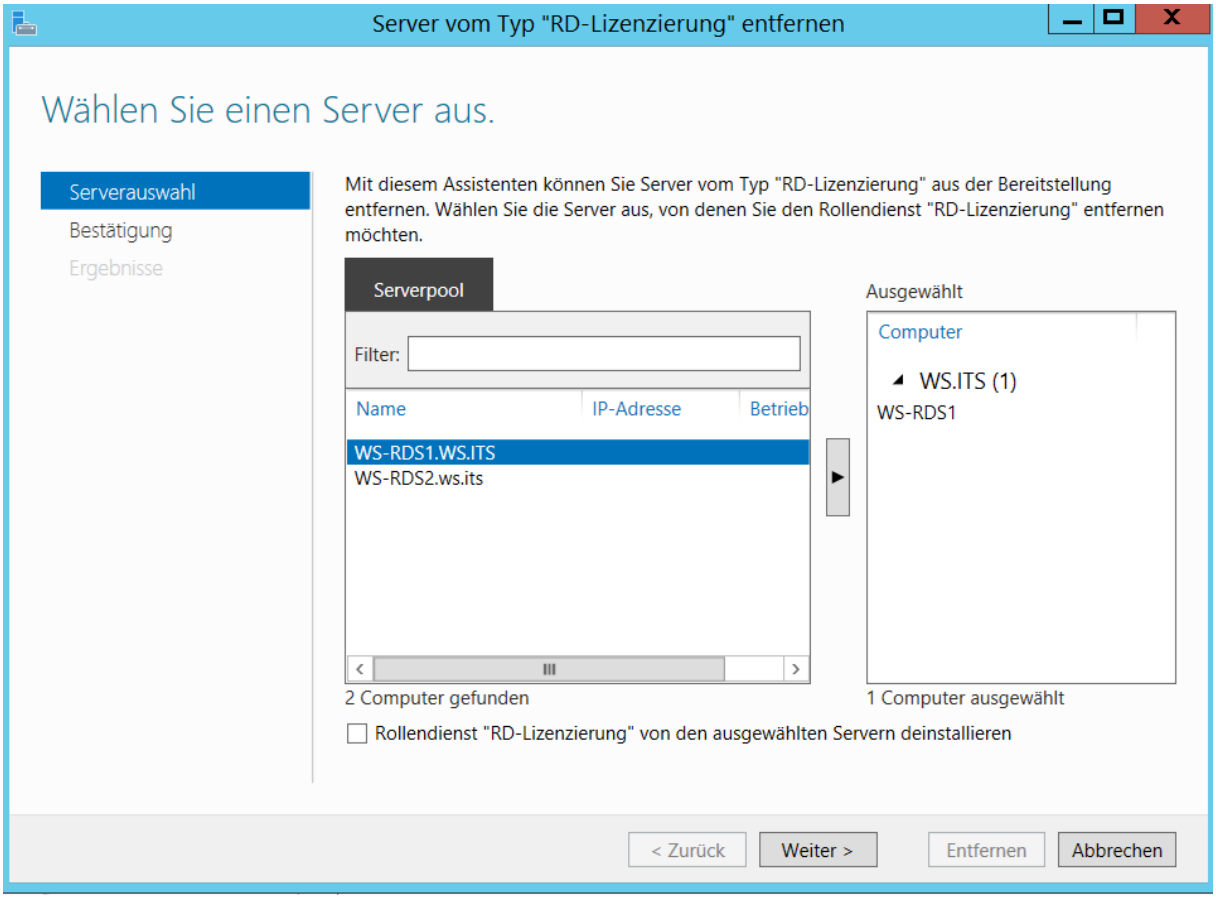


Ab jetzt stehen die RD-Services den Nutzern nicht mehr zur Verfügung!

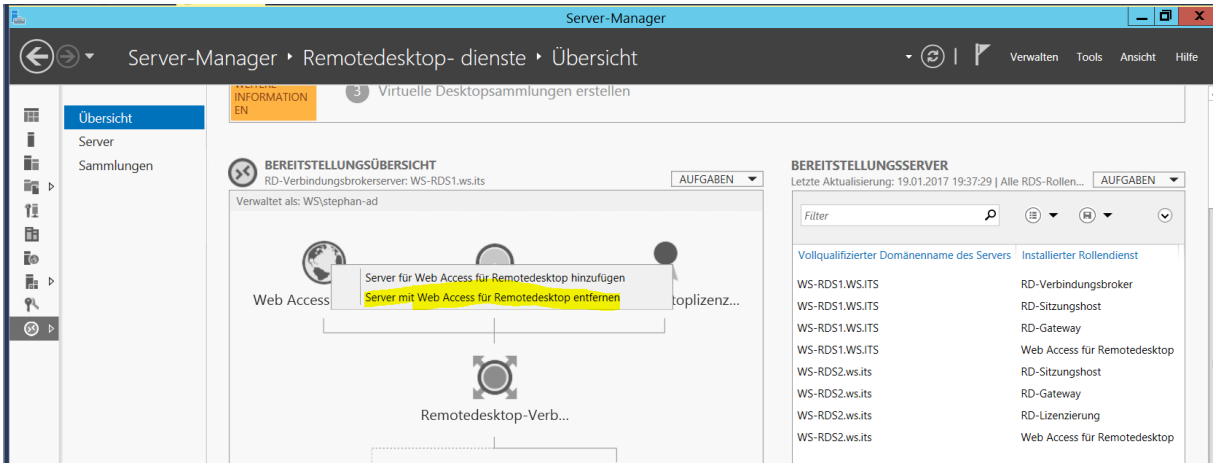
Entfernen aller nicht erforderlichen RDS-Rollen

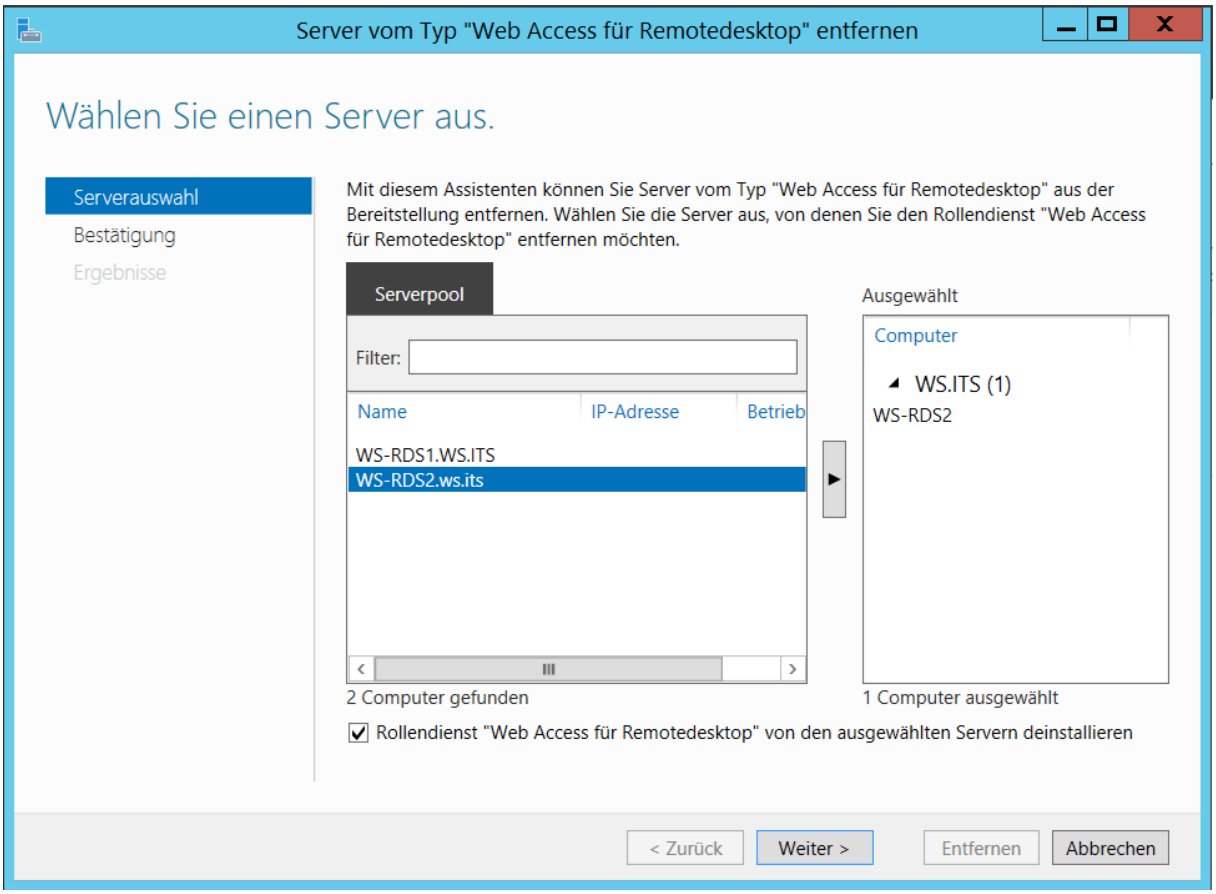
WS-RDS2 soll auch nach dem Entfernen des SessionBrokers als LizenzServer ansprechbar sein. Daher deinstalliere ich alle RDS-Rollen, um ihn aus der- Infrastruktur zu bereinigen. Ich beginne mit dem Lizenzserver auf dem alten WS-RDS1. Dieser kann über das Dashboard mit einem Rechtsklick entfernt werden:

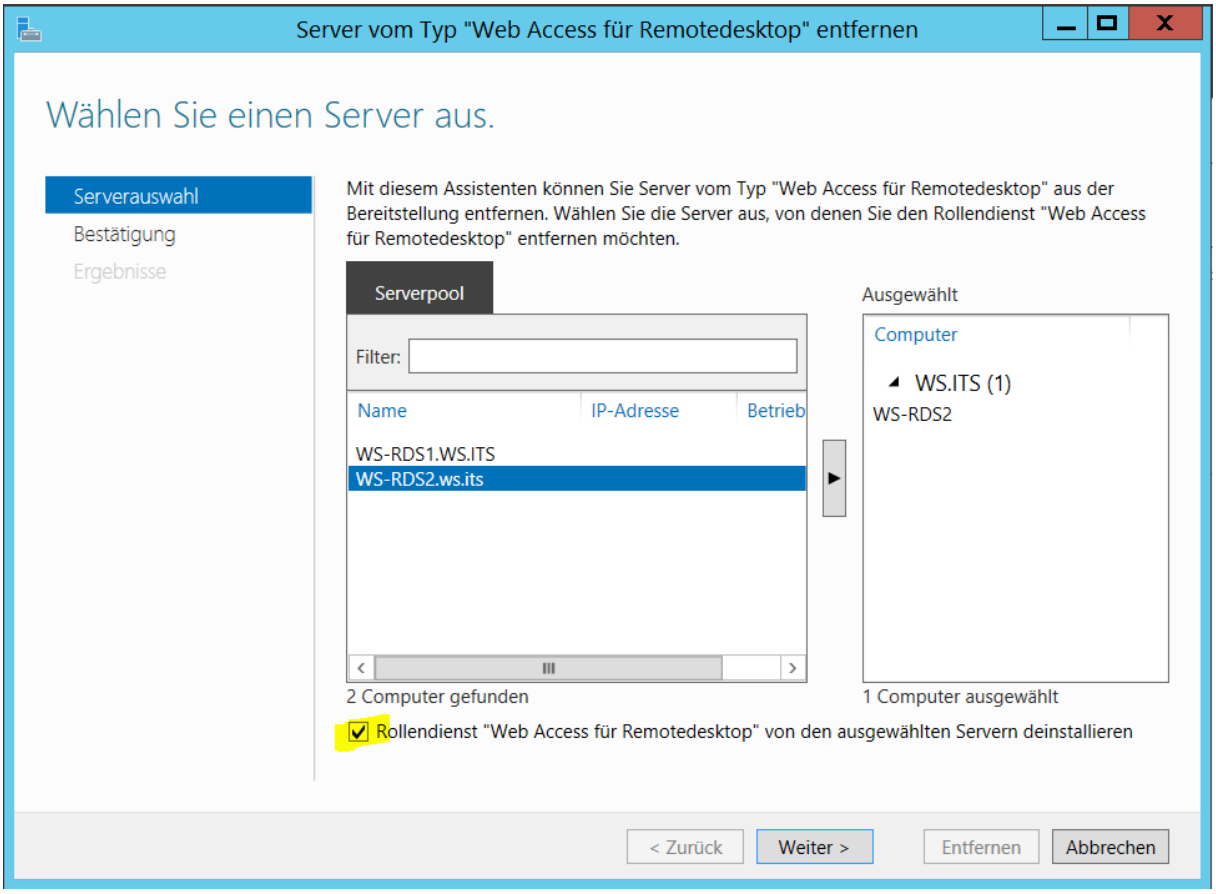

Server-Manager
Server-Manager ‣ Remotedesktop- dienste ‣ Übersicht
Verwalten
Tools
Ansicht
Übersicht
Server
Sammlungen
Virtuelle Desktopsammlungen erstellen
BEREITSTELLUNGSÜBERSICHT
RD-Verbindungsbrokerserver: WS-RDS1.ws.its
AUFGABEN
Verwaltet als: WS\stephan-ad
Web Access für Rem...
Remotedesktopgate...
RD-Lizenzierungsserver hinzufügen
RD-Lizenzierungsserver entfernen
Remotedesktop-Verb...
Remotedesktop-Virtu...
Remotedesktop-Sitzu...
BEREITSTELLUNGSSERVER
Letzte Aktualisierung: 19.01.2017 19:29:27 | Alle RDS-Rollen...
Filter
Vollqualifizierter Domänenname des Servers
Installierter Rollendienst
WS-RDS1.WS.ITS RD-Verbindungsbroker
WS-RDS1.WS.ITS RD-Sitzungshost
WS-RDS1.WS.ITS RD-Gateway
WS-RDS1.WS.ITS RD-Lizenzierung
WS-RDS1.WS.ITS Web Access für Remotedesktop
WS-RDS2.ws.its RD-Sitzungshost
WS-RDS2.ws.its RD-Gateway
WS-RDS2.ws.its RD-Lizenzierung
WS-RDS2.ws.its Web Access für Remotedesktop


Server vom Typ "RD-Lizenzierung" entfernen
Wählen Sie einen Server aus.
Serverauswahl
Bestätigung
Ergebnisse
Mit diesem Assistenten können Sie Server vom Typ "RD-Lizenzierung" aus der Bereitstellung entfernen. Wählen Sie die Server aus, von denen Sie den Rollendienst "RD-Lizenzierung" entfernen möchten.
Serverpool
Filter:
Name
IP-Adresse
Betrieb
WS-RDS1.WS.ITS
WS-RDS2.ws.its
2 Computer gefunden
Ausgewählt
Computer
WS.ITS (1)
WS-RDS1
1 Computer ausgewählt
Rollendienst "RD-Lizenzierung" von den ausgewählten Servern deinstallieren
< Zurück
Weiter >
Entfernen
Abbrechen

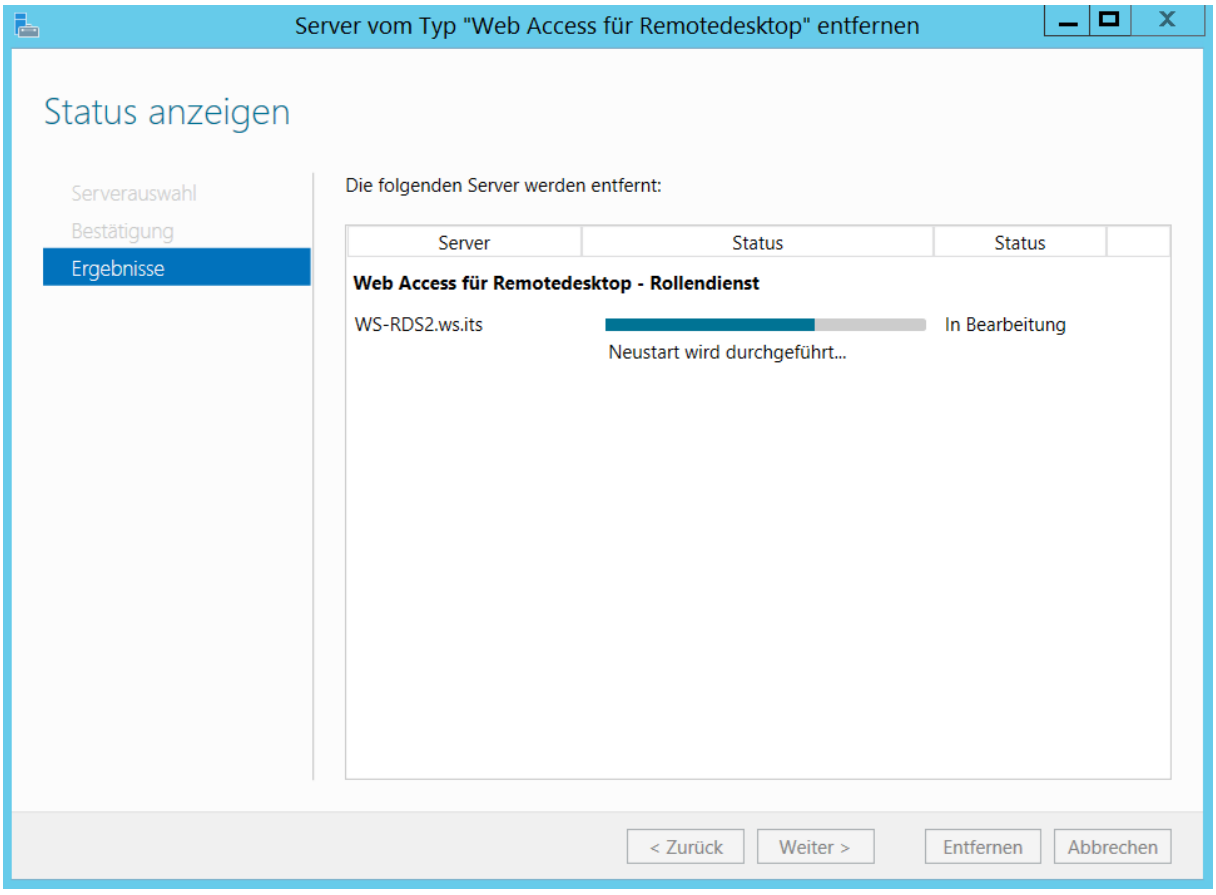
Weiter geht es mit dem WebService von WS-RDS2:



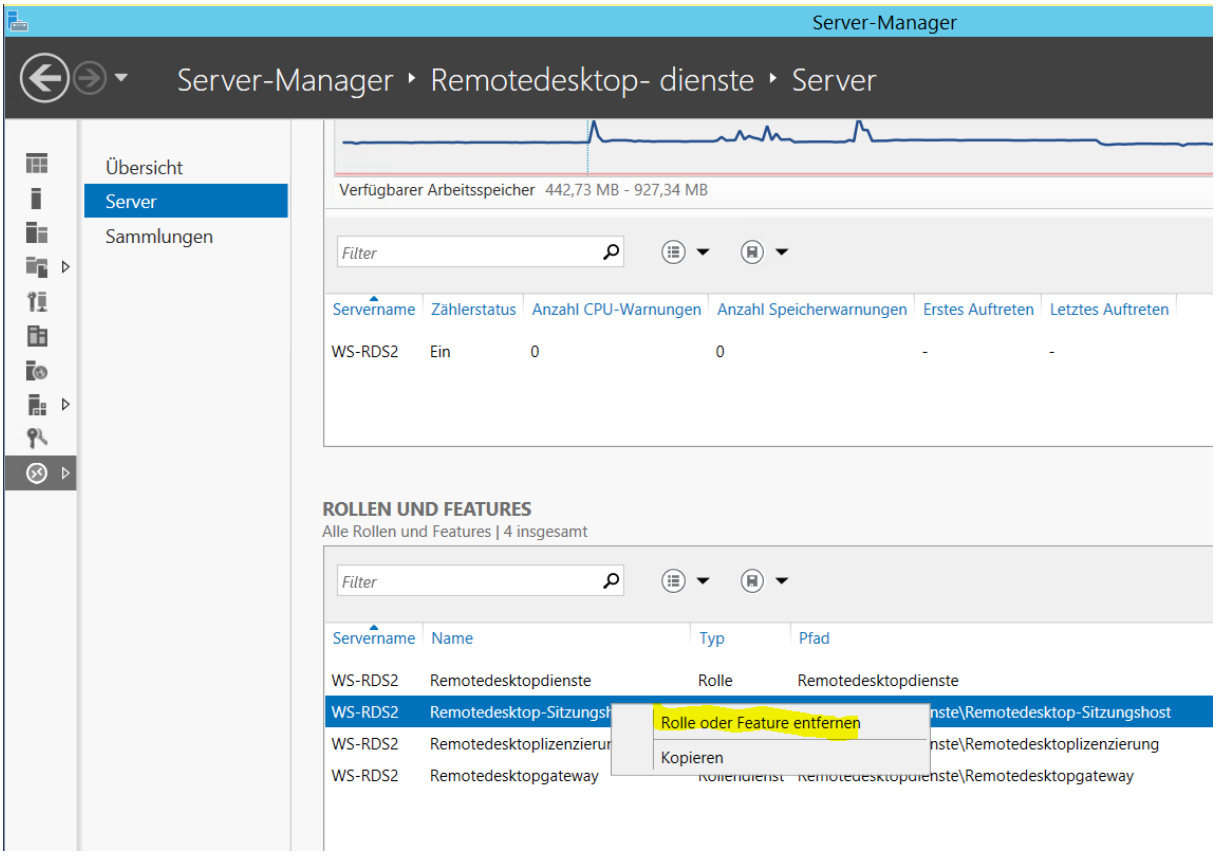




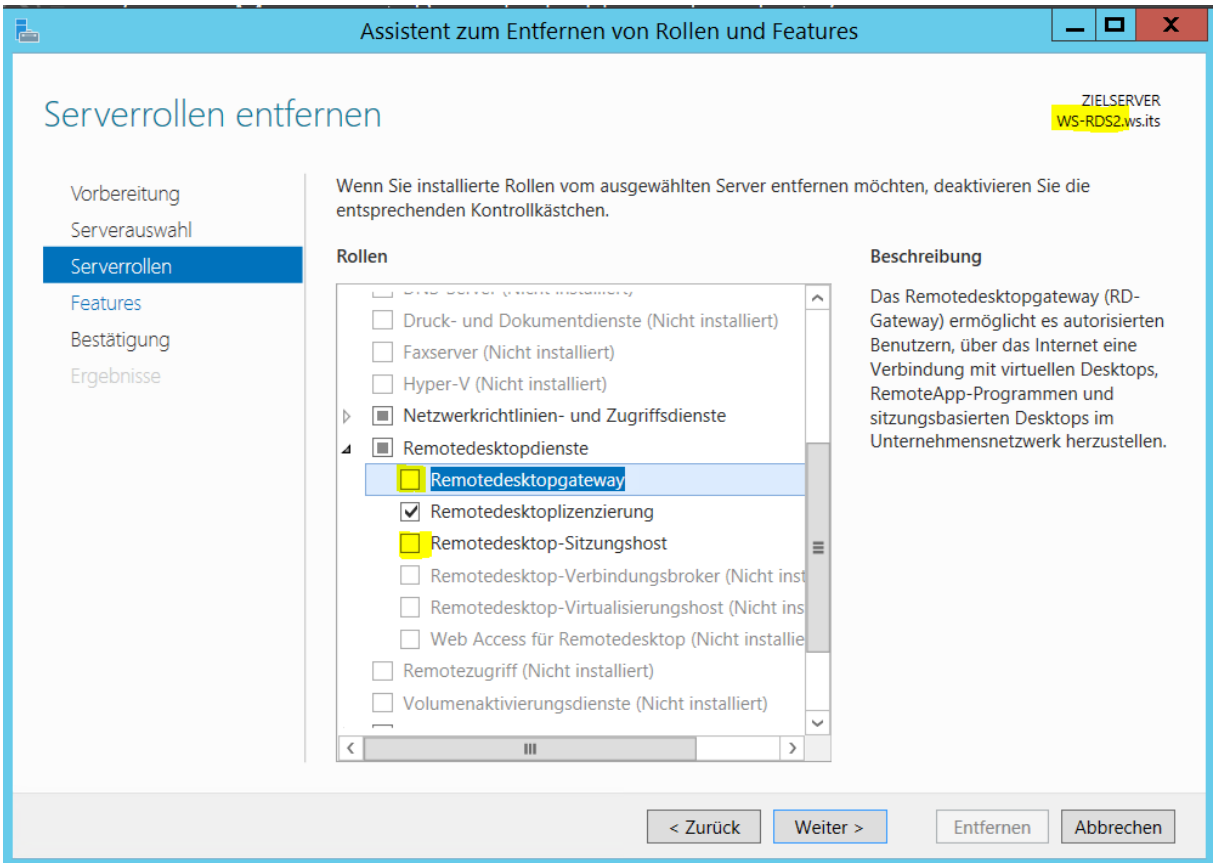
Dieses Feature benötigt bei der Deinstallation einen Neustart:

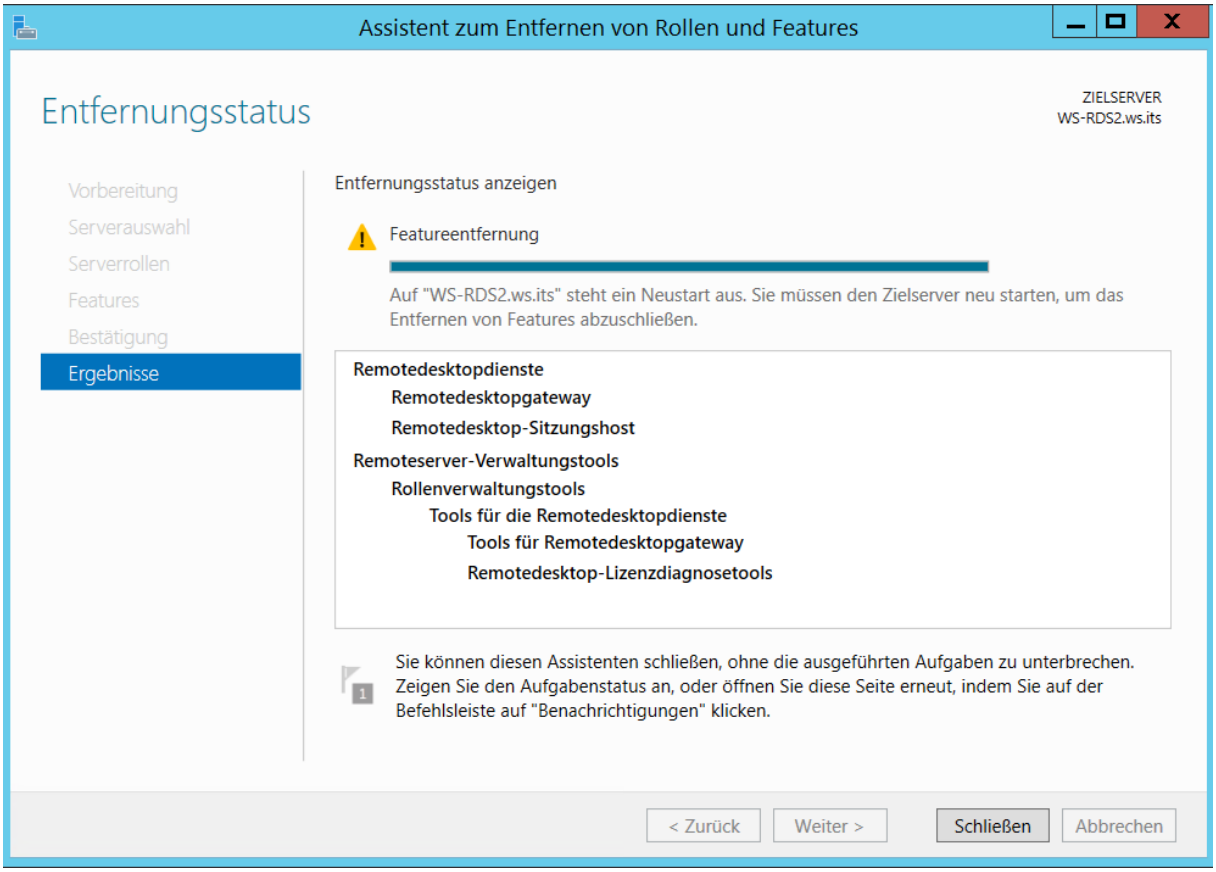


Jetzt kann der RD-Sessionhost und der Gateway vom WS-RDS2 entfernt werden:

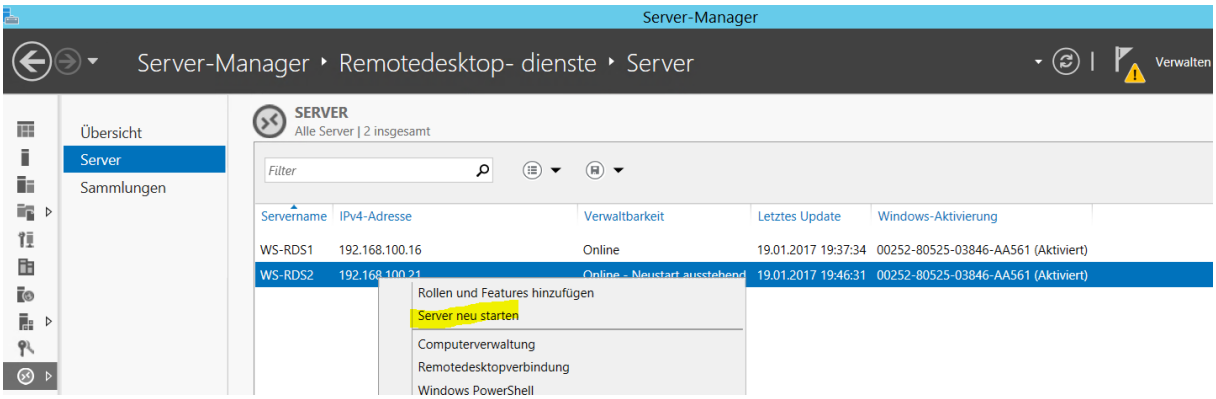


Nur der Lizenzserver verbleibt:

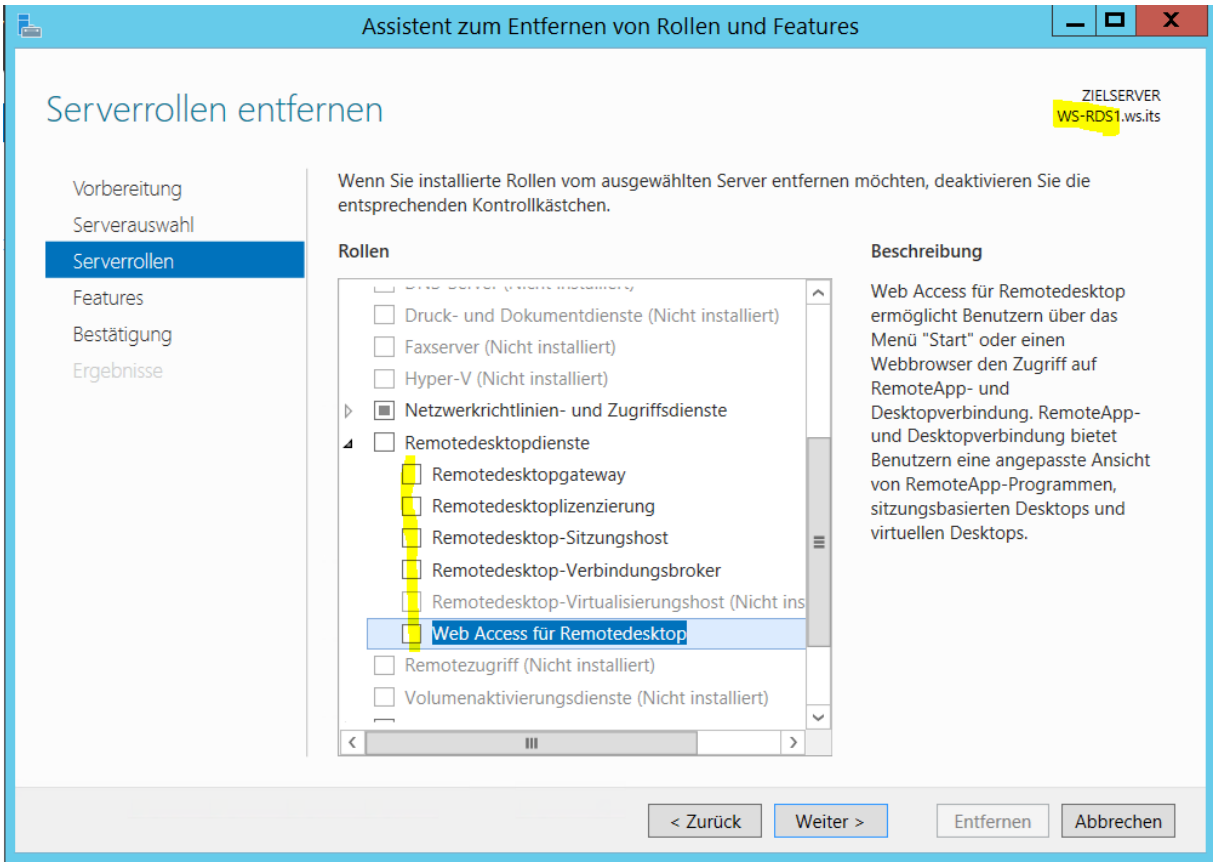


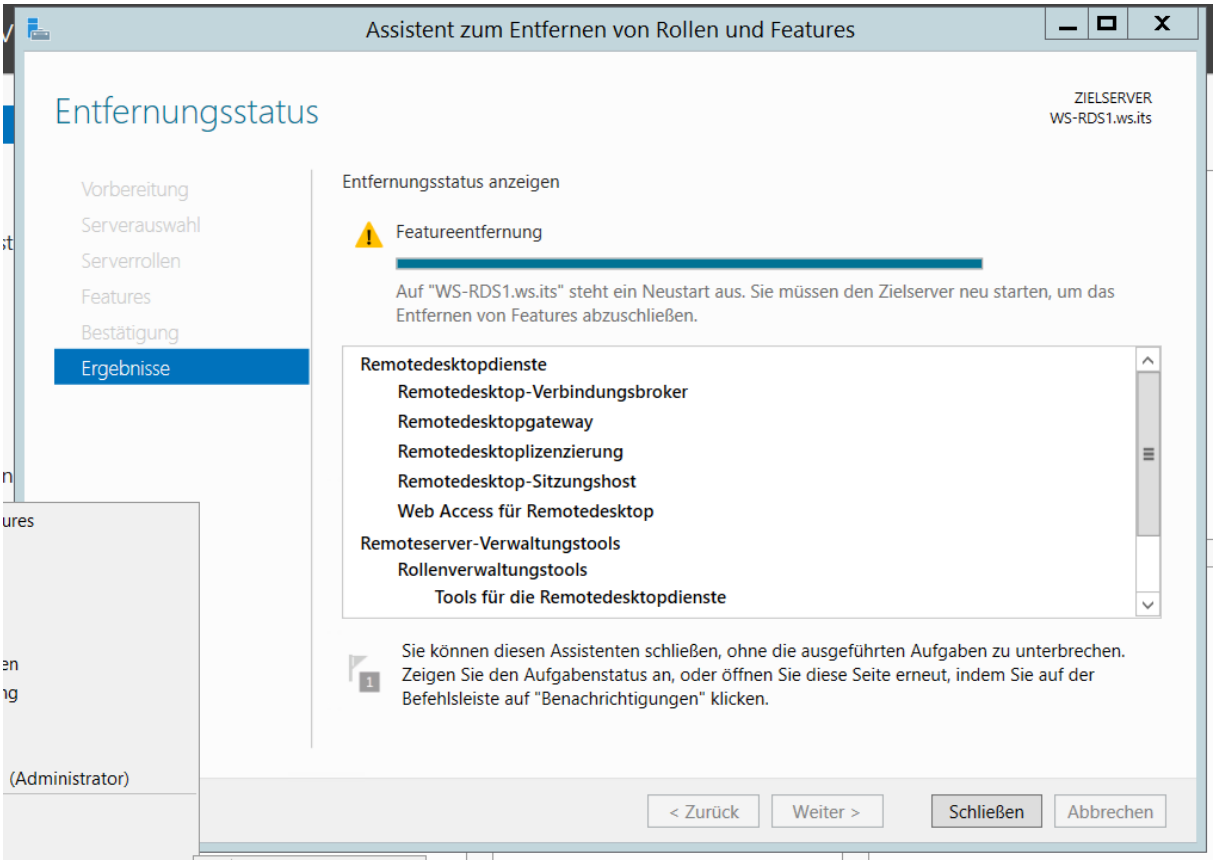


Der Server benötigt einen Neustart:



Auf WS-RDS1 können nun alle RDS-Rollen aufgelöst werden. Da es jetzt keine Abhängigkeiten mehr gibt kann dies in einer Aktion ausgeführt werden:



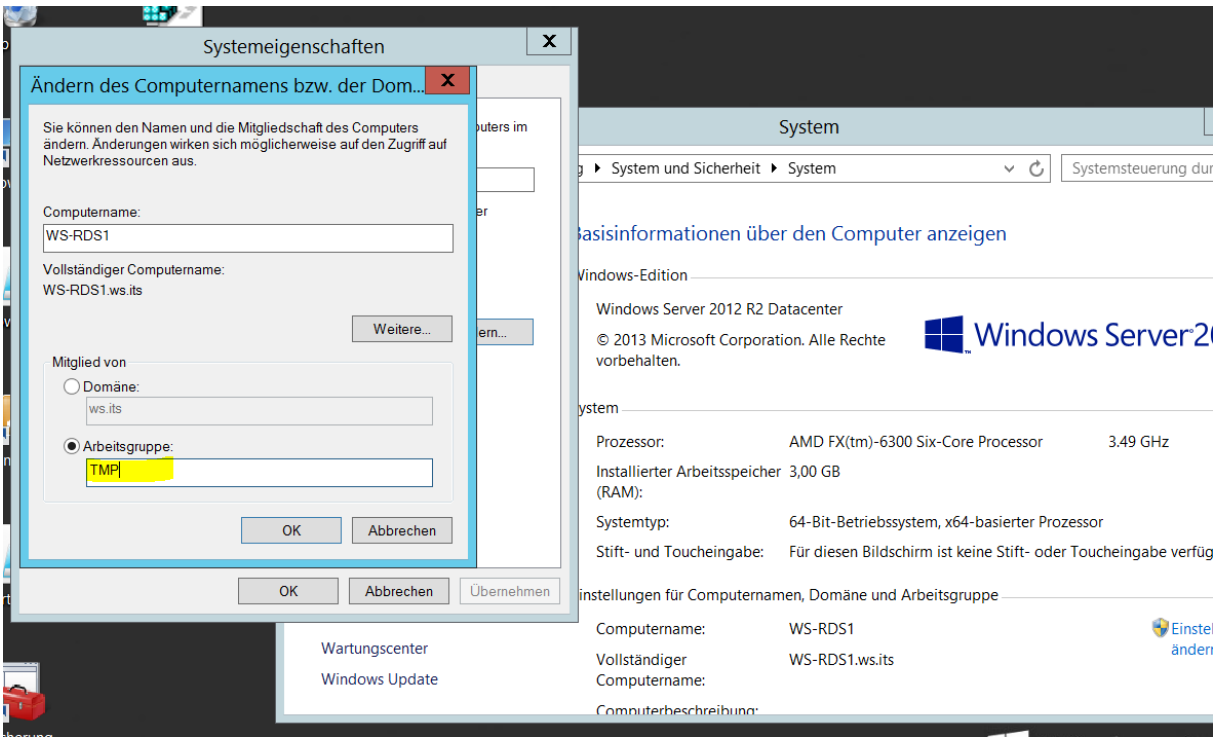


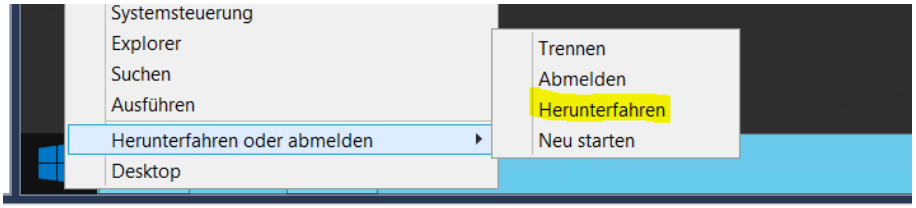
Abschalten des alten Servers WS-RDS1

Nach dem Neustart sichere ich noch einige Informationen des alten Servers:

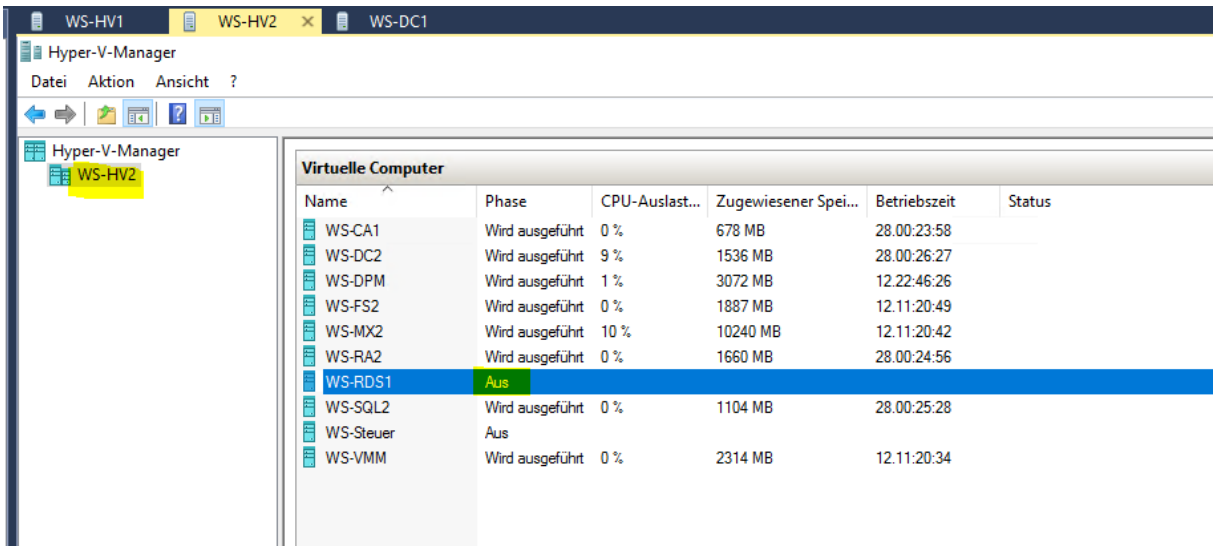
- Ich exportiere ScheduledTasks
- Ich kopiere die Script-Verzeichnisse auf einen FileServer

Jetzt kann der Server das Active Directory verlassen:

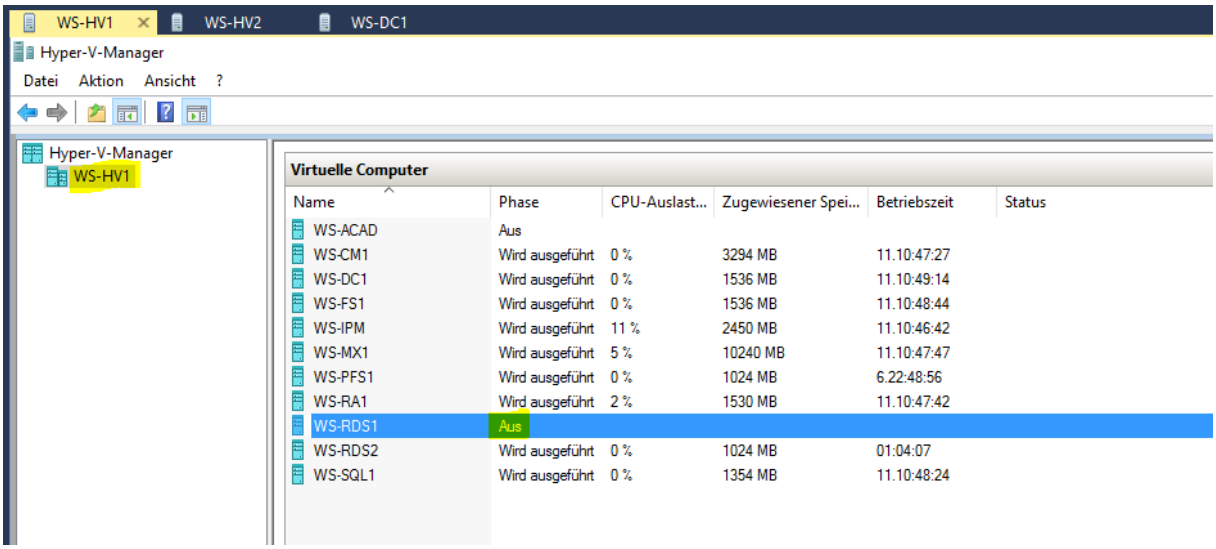




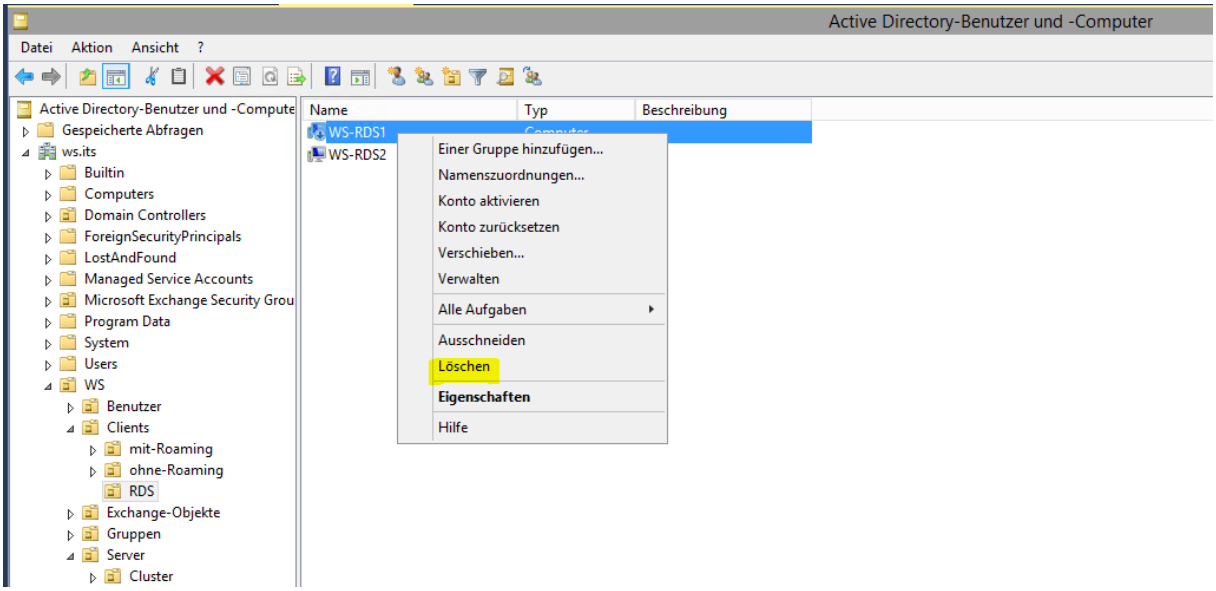
Die alte VM ist jetzt ausgeschaltet:



Auf meinem anderen Hyper-V-Host habe ich bereits eine neue VM mit dem Betriebssystem Windows Server 2016 und allen erforderlichen Anwendungen bereitgestellt. Es fehlt noch der DomainJoin:



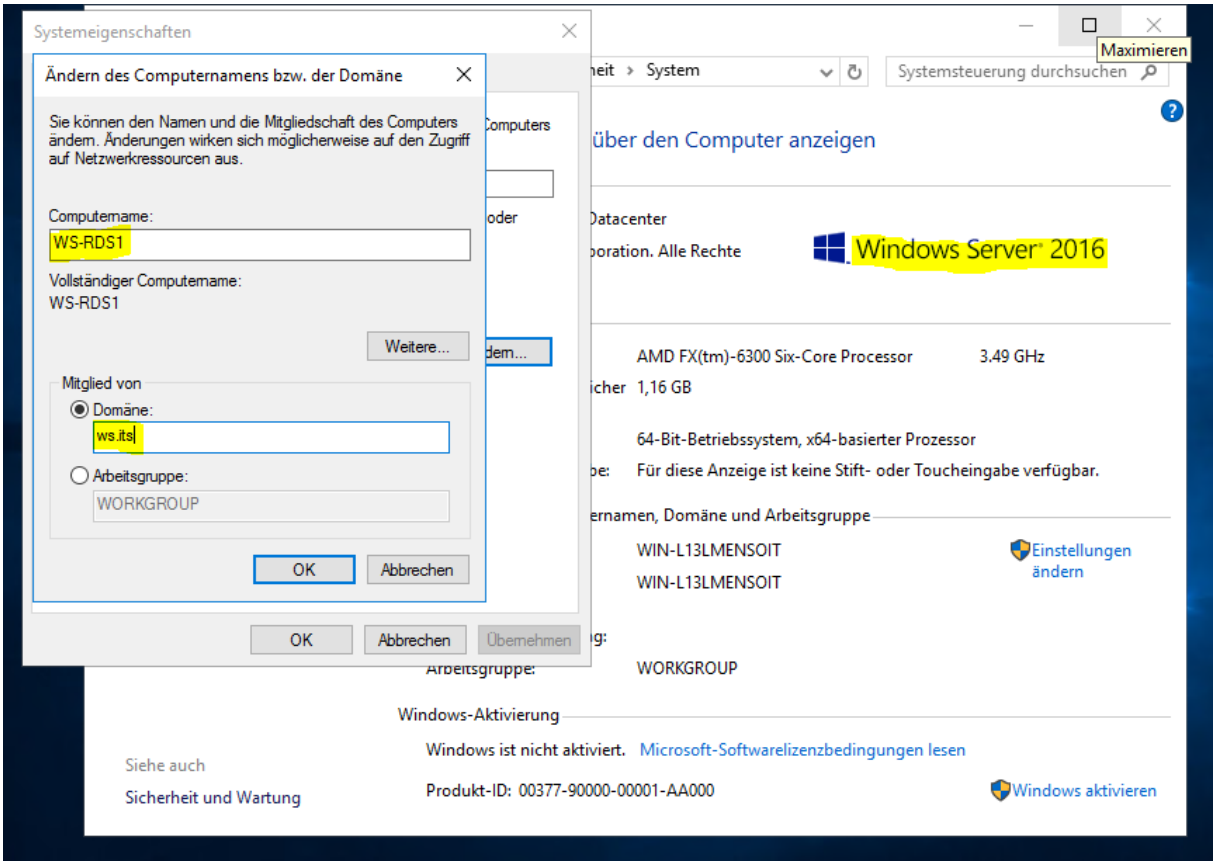
Im Active Directory lösche ich das AD-Computerkonto, damit der neue Server den gleichen Namen mit neuer SID verenden kann:



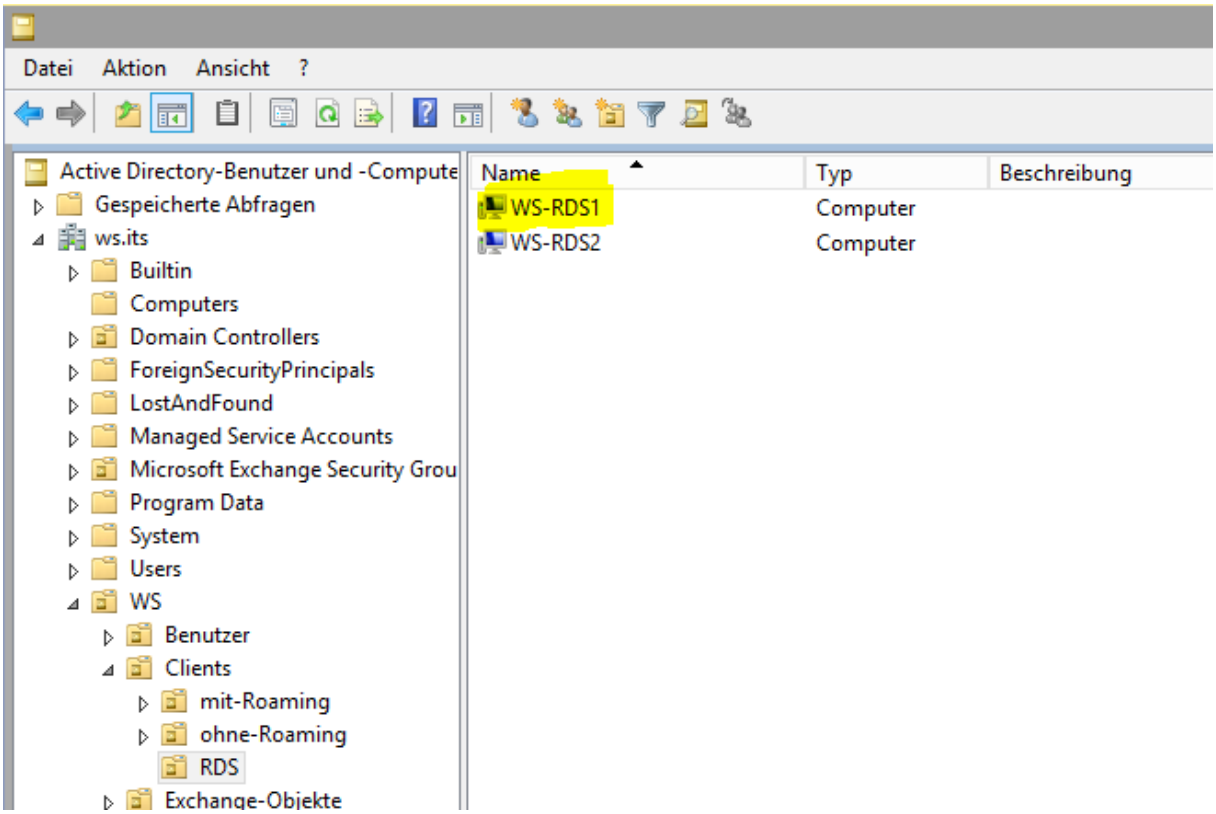
3. Aufbau der neuen RDS-Infrastruktur

Inbetriebnahme und Vorbereitung des neuen Servers WS-RDS1

Jetzt kann die neue VM eingeschaltet werden. Diese nehme ich nun auch in das Active Directory auf:



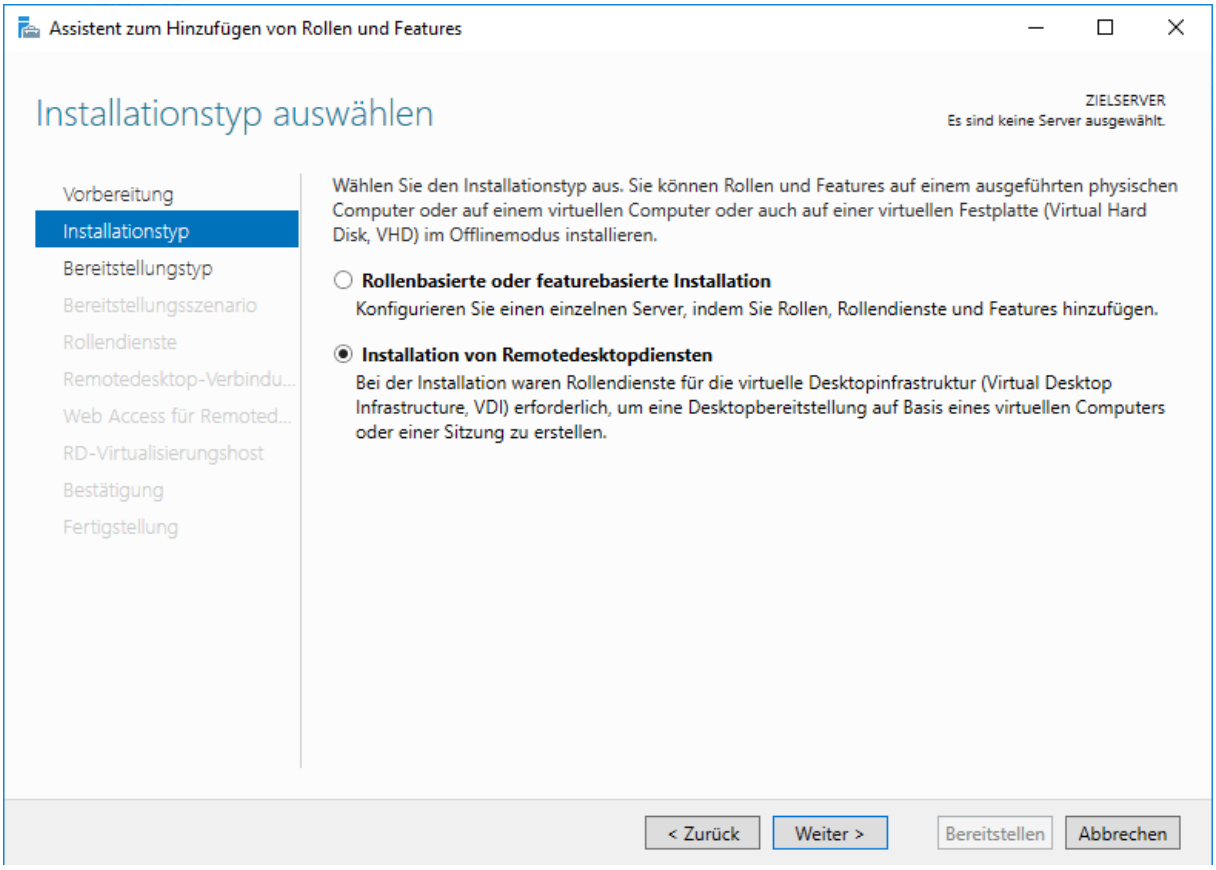
Das Computerkonto verschiebe ich nun in die richtige OU und starte dann den Server neu:



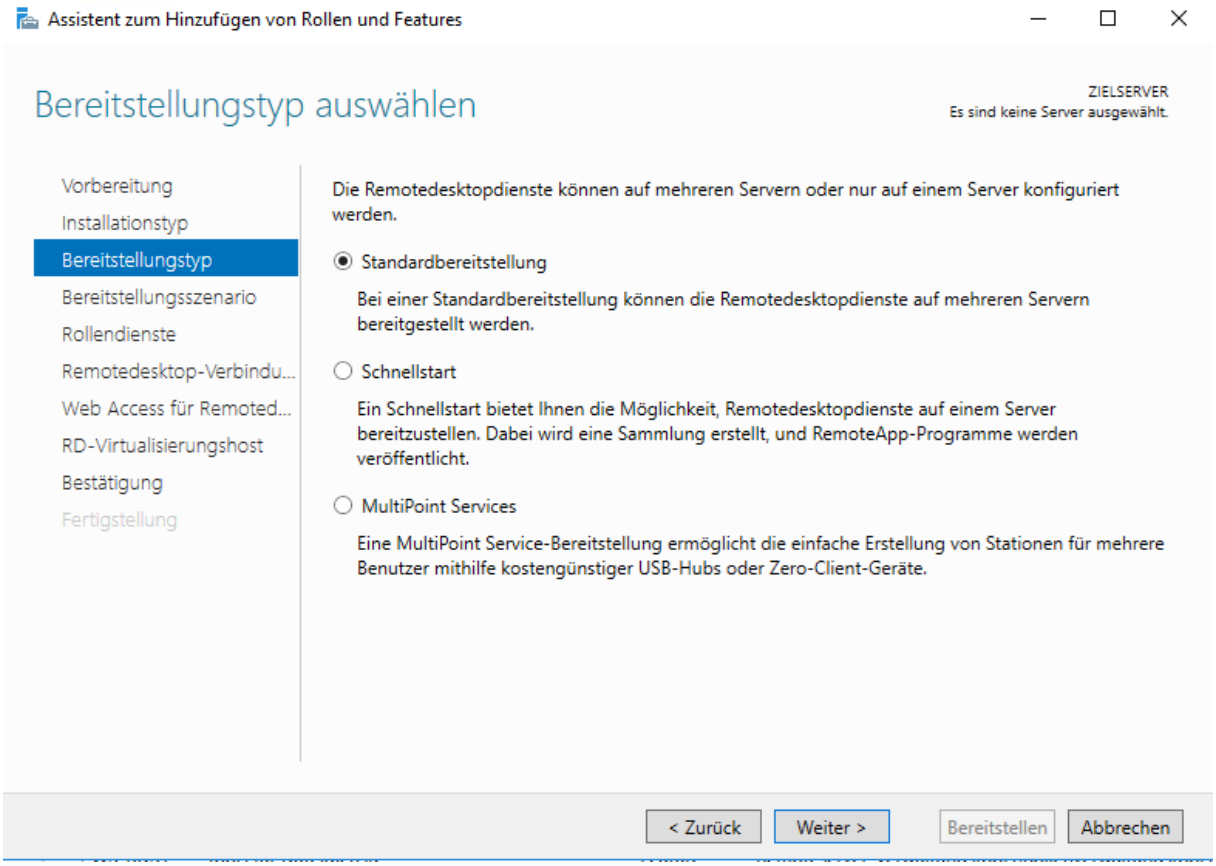
Die IP-Konfiguration entspricht schon der des alten Servers – lediglich den NLB benötige ich nicht mehr. Die dazugehörige IP-Adresse habe ich freigegeben.

Installation der neuen RDS-Infrastruktur

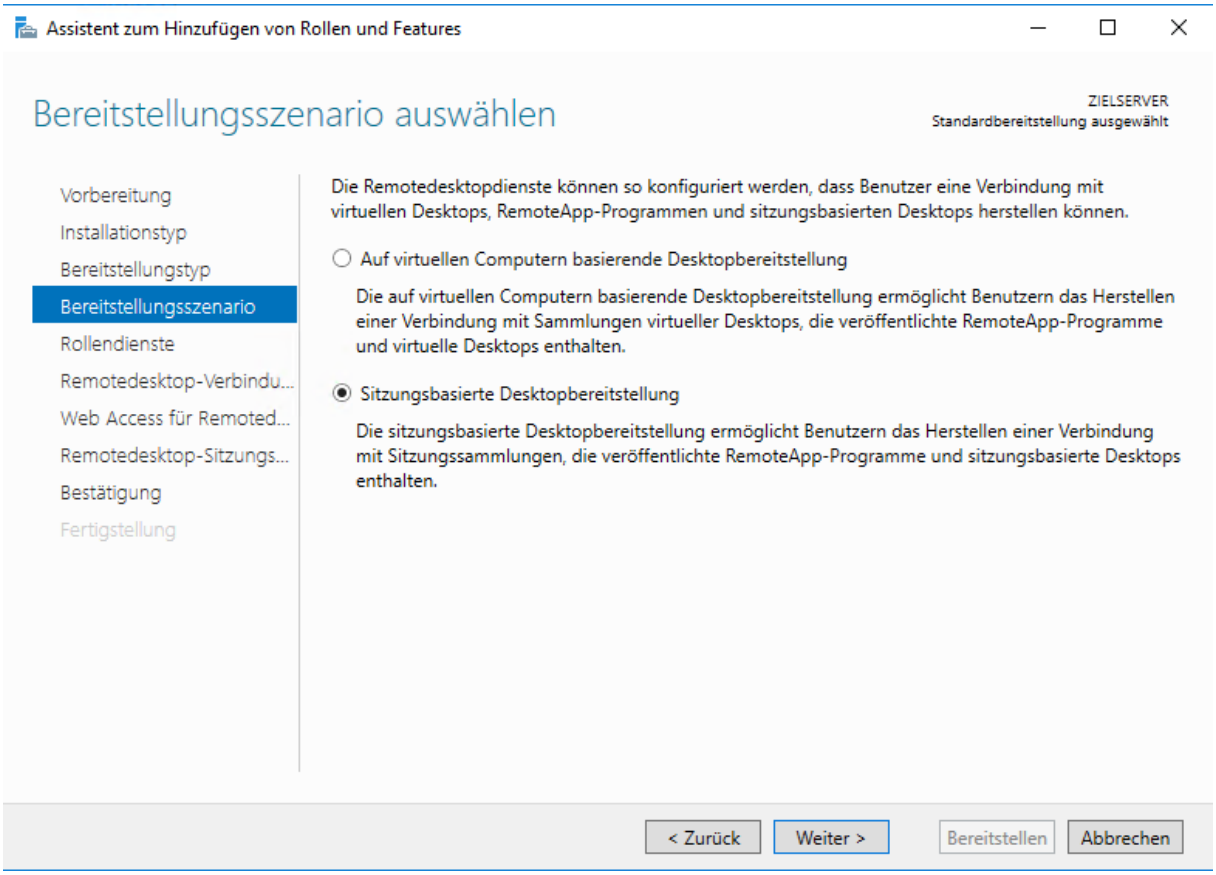
Auf dem neuen Server starte ich den Bereitstellungsassistenten für RDS:



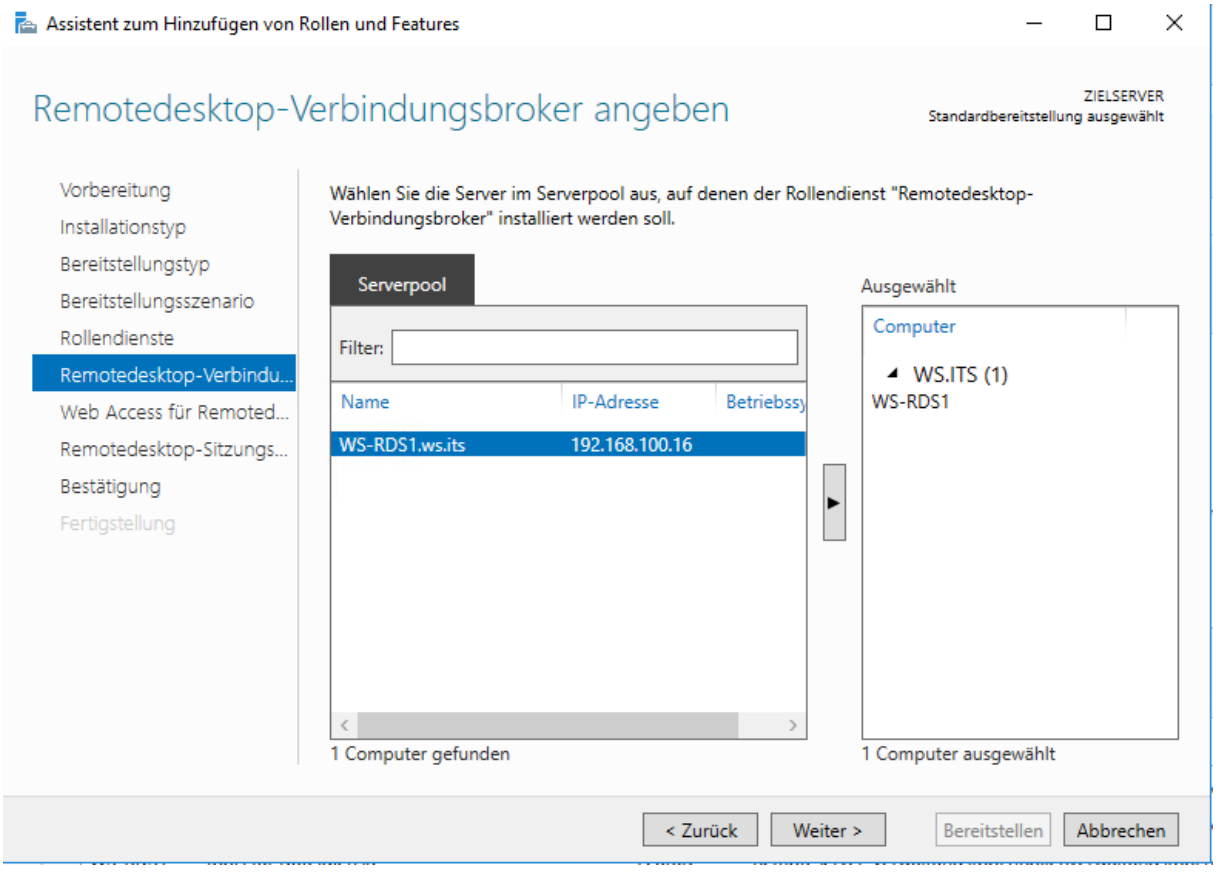
Eine Standard-Bereitstellung genügt:

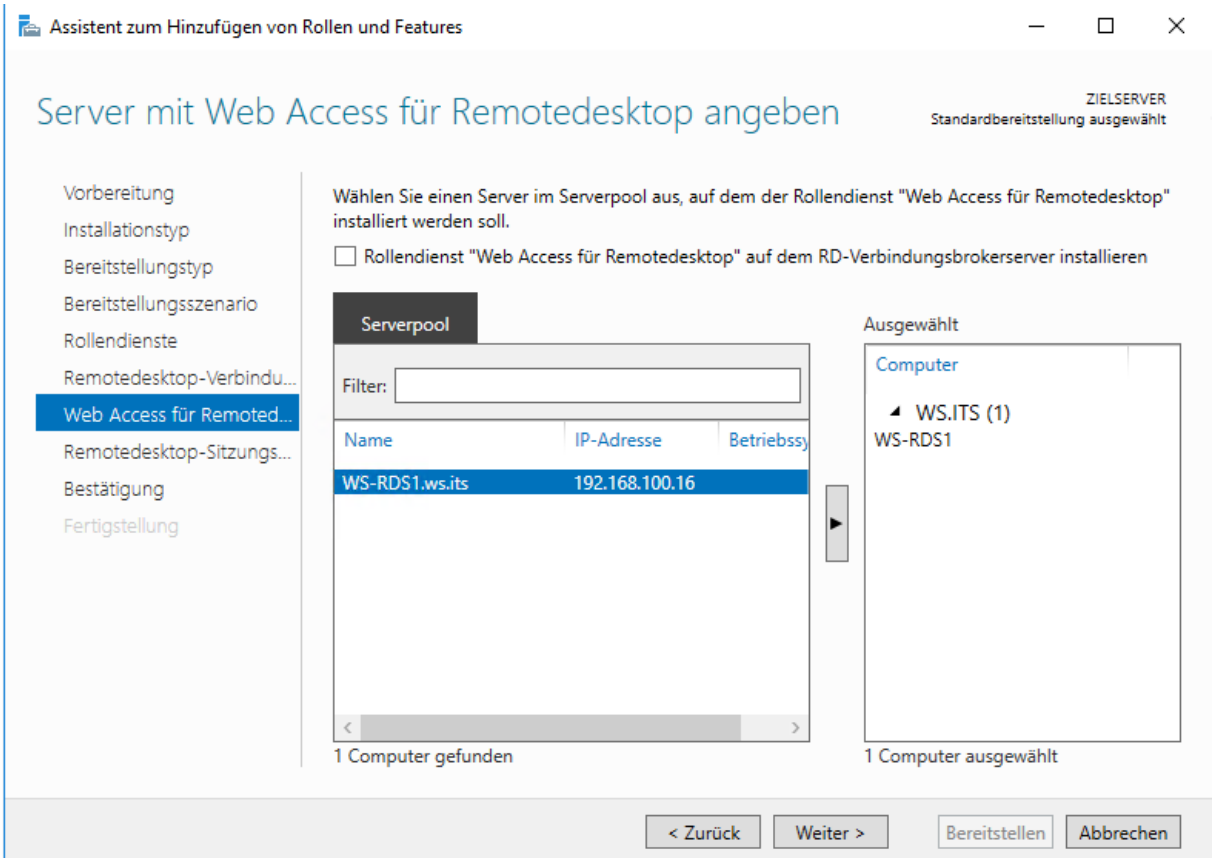


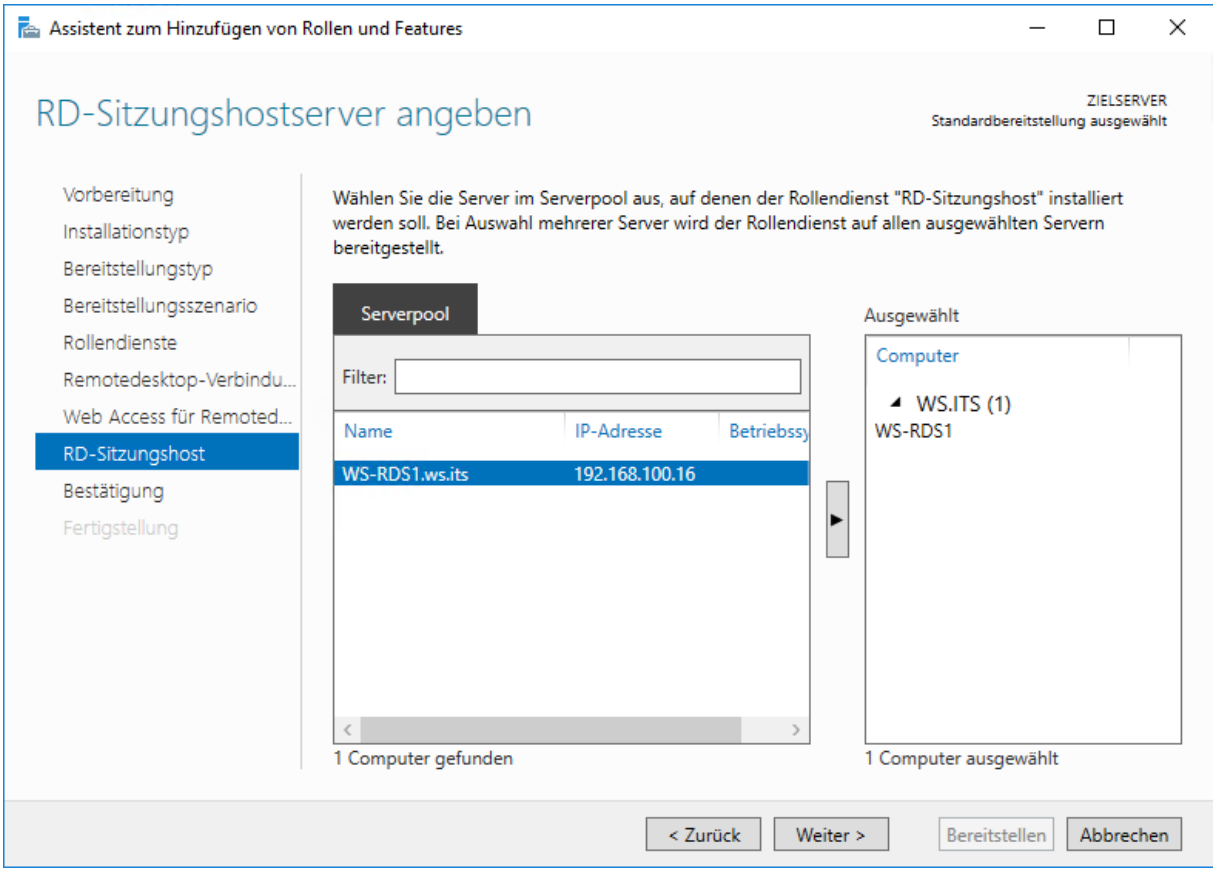
Zunächst soll eine SessionHost-Bereitstellung gestartet werden:

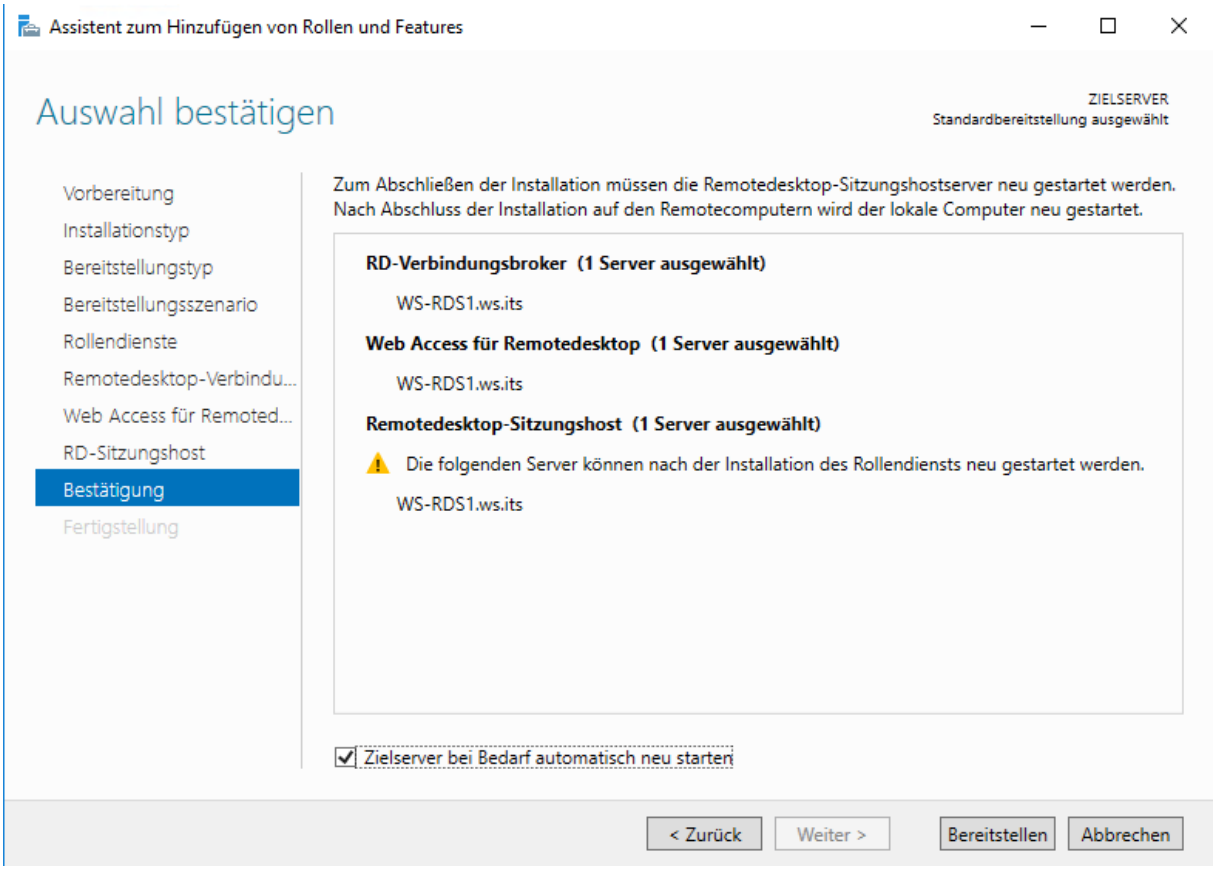


Der Server WS-RDS1 soll darin natürlich alle Rollen übernehmen, da nur noch ein Server geplant ist:

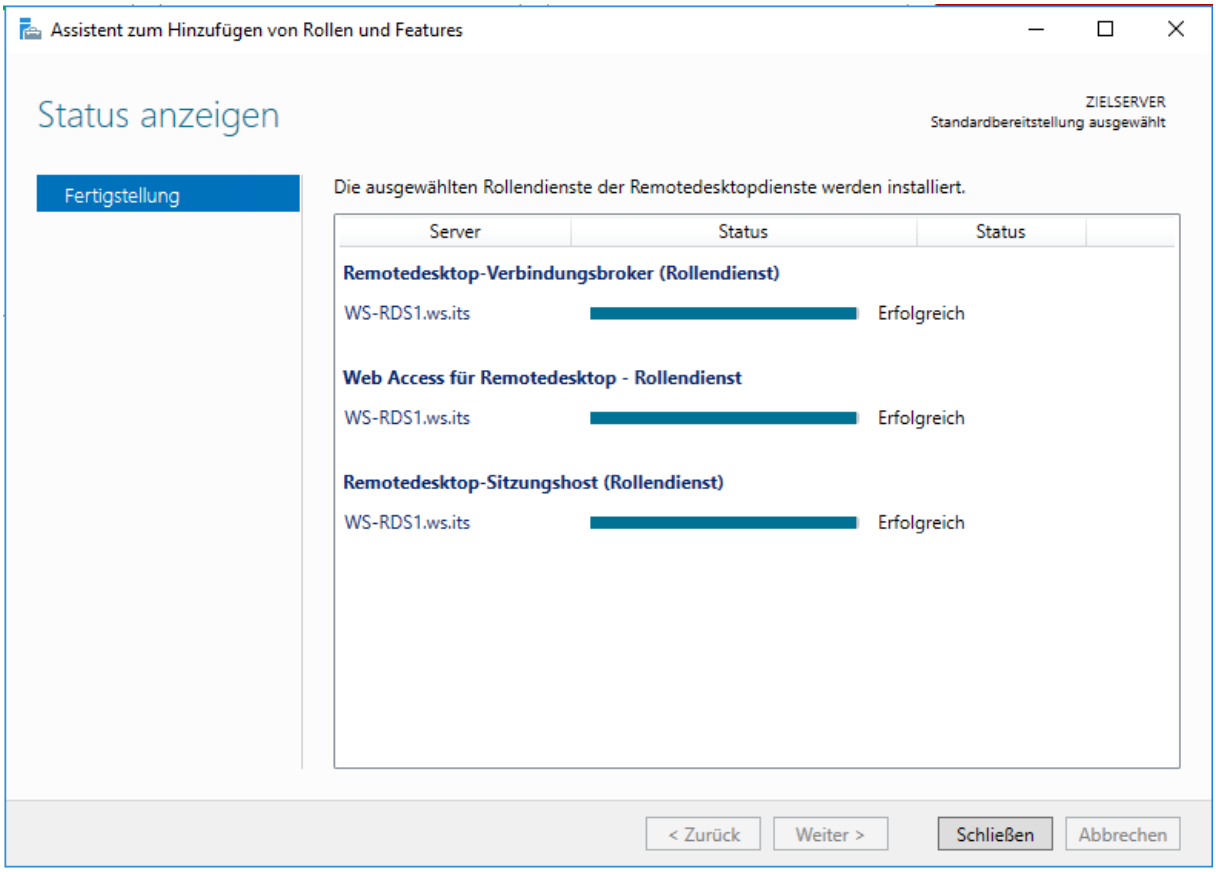



Assistent zum Hinzufügen von Rollen und Features
Server mit Web Access für Remotedesktop angeben
ZIELSERVER
Standardbereitstellung ausgewählt
Vorbereitung
Installationstyp
Bereitstellungstyp
Bereitstellungsszenario
Rollendienste
Remotedesktop-Verbindu...
Web Access für Remoted...
Remotedesktop-Sitzungs...
Bestätigung
Fertigstellung
Wählen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" installiert werden soll.
Rollendienst "Web Access für Remotedesktop" auf dem RD-Verbindungsbrokerserver installieren
Serverpool
Filter:
Name
IP-Adresse
Betriebssy
WS-RDS1.ws.its
192.168.100.16
1 Computer gefunden
Ausgewählt
Computer
WS.ITS (1)
WS-RDS1
1 Computer ausgewählt
< Zurück
Weiter >
Bereitstellen
Abbrechen

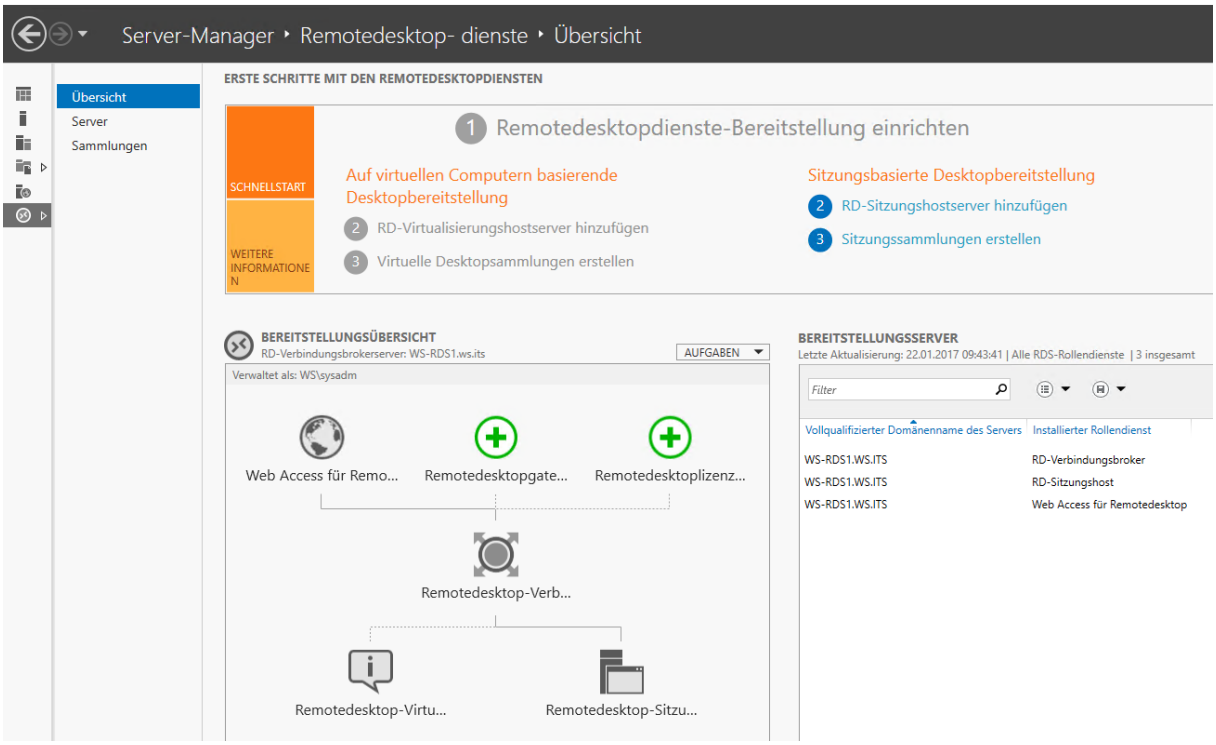

Assistent zum Hinzufügen von Rollen und Features
RD-Sitzungshostserver angeben
ZIELSERVER
Standardbereitstellung ausgewählt
Vorbereitung
Installationstyp
Bereitstellungstyp
Bereitstellungsszenario
Rollendienste
Remotedesktop-Verbindu...
Web Access für Remoted...
RD-Sitzungshost
Bestätigung
Fertigstellung
Wählen Sie die Server im Serverpool aus, auf denen der Rollendienst "RD-Sitzungshost" installiert werden soll. Bei Auswahl mehrerer Server wird der Rollendienst auf allen ausgewählten Servern bereitgestellt.
Serverpool
Filter:
Name
IP-Adresse
Betriebssy
WS-RDS1.ws.its
192.168.100.16
1 Computer gefunden
Ausgewählt
Computer
WS.ITS (1)
WS-RDS1
1 Computer ausgewählt
< Zurück
Weiter >
Bereitstellen
Abbrechen



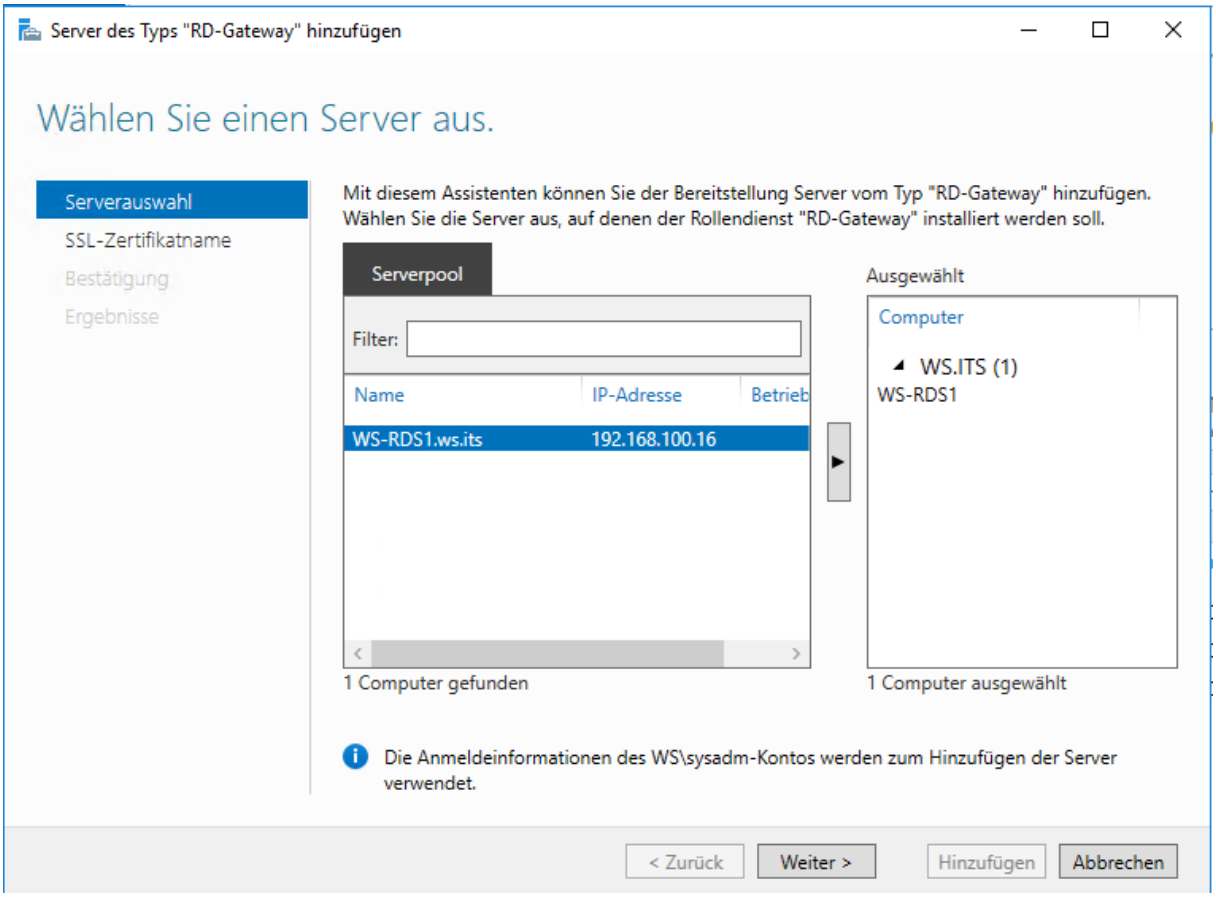
Der WorkFlow beginnt mit der Konfiguration und es wird ein automatischer Neustart ausgeführt:



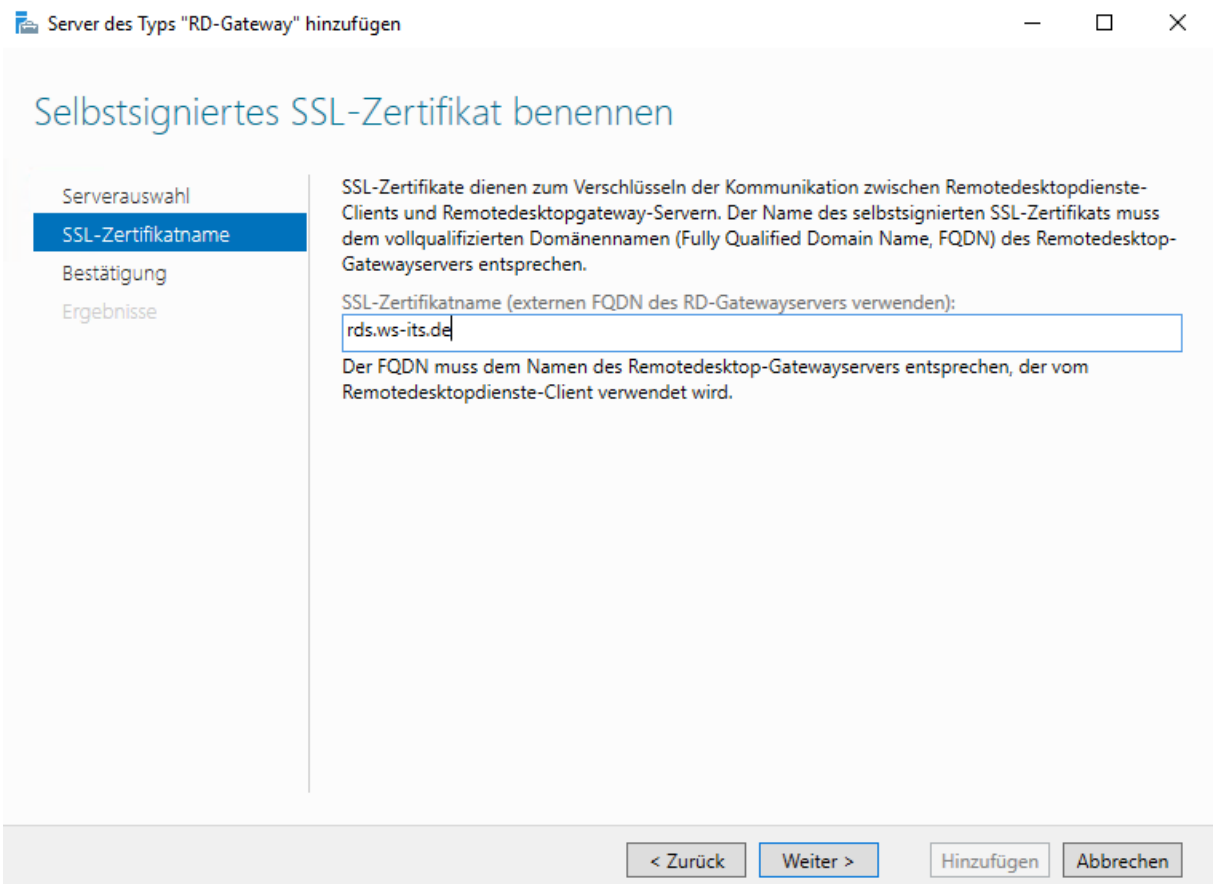
Nach der Neuanmeldung ist der Management-Client im Servermanager einsatzbereit.



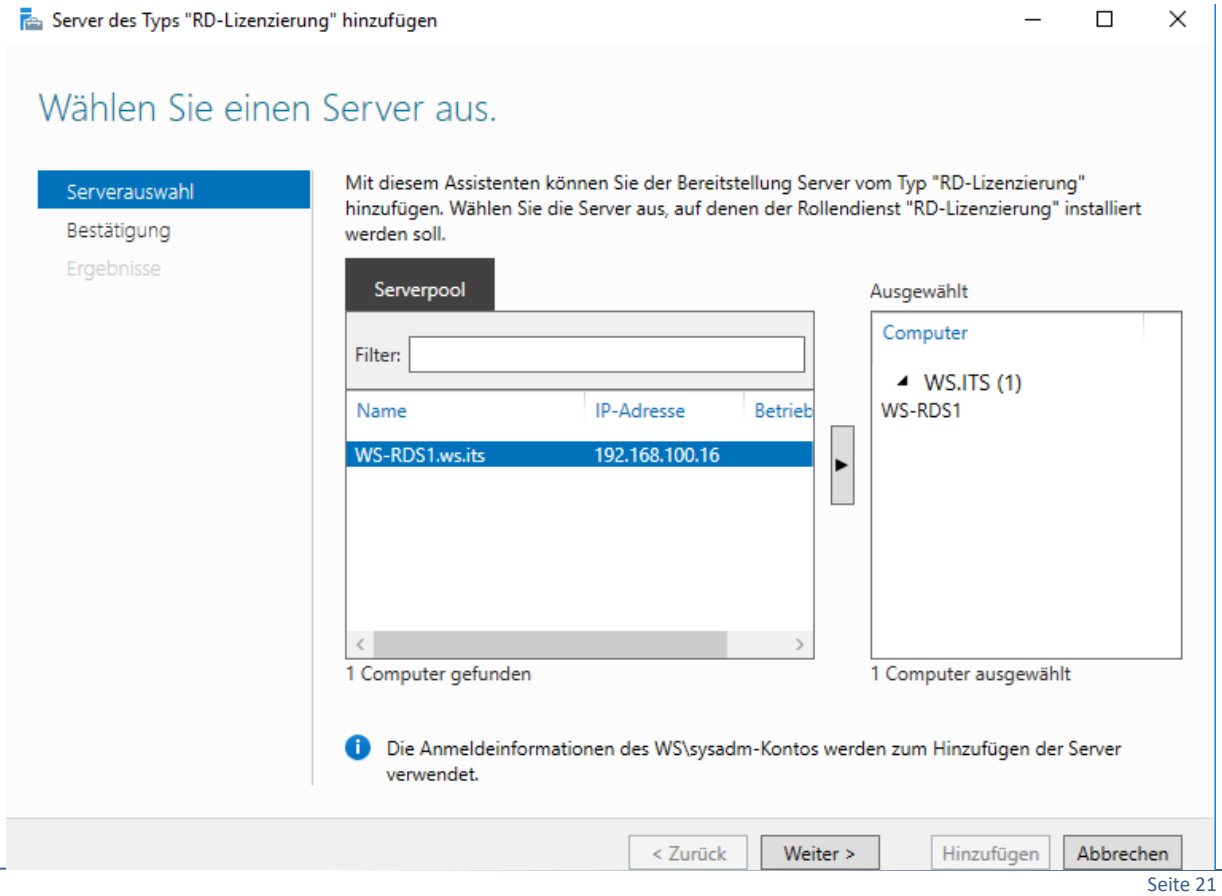
Zunächst installiere ich die fehlenden Rollen RD-Gateway und Lizenzserver:



Das Gateway stellt die Verbindung nach draußen durch einen https-Tunnel dar. Dafür ist ein externer Zugriffsname und auch ein Zertifikat nötig:



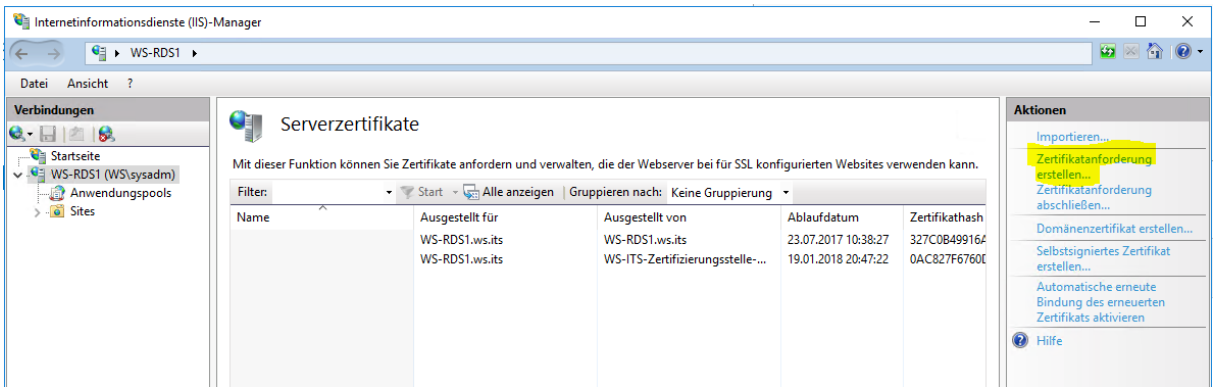
Der Lizenzierungsserver wird ähnlich installiert:



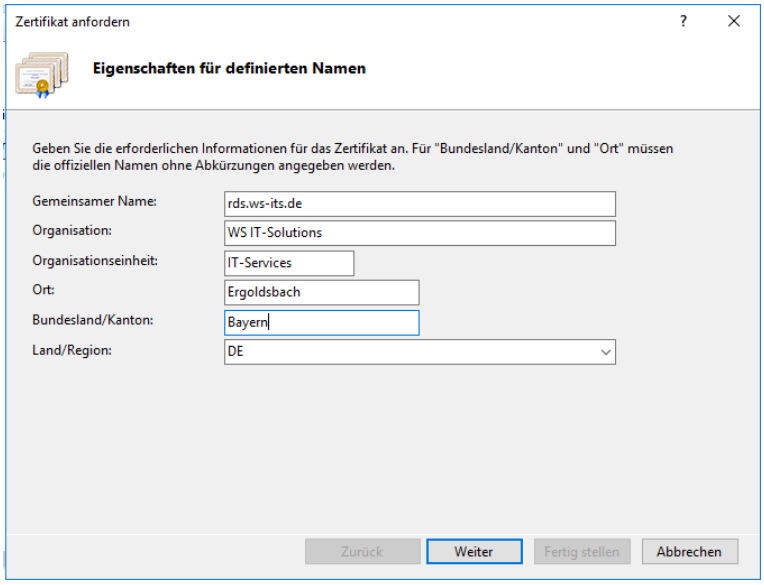
Jetzt stehen alle Rollen bereit. Es wird Zeit für die Konfiguration…

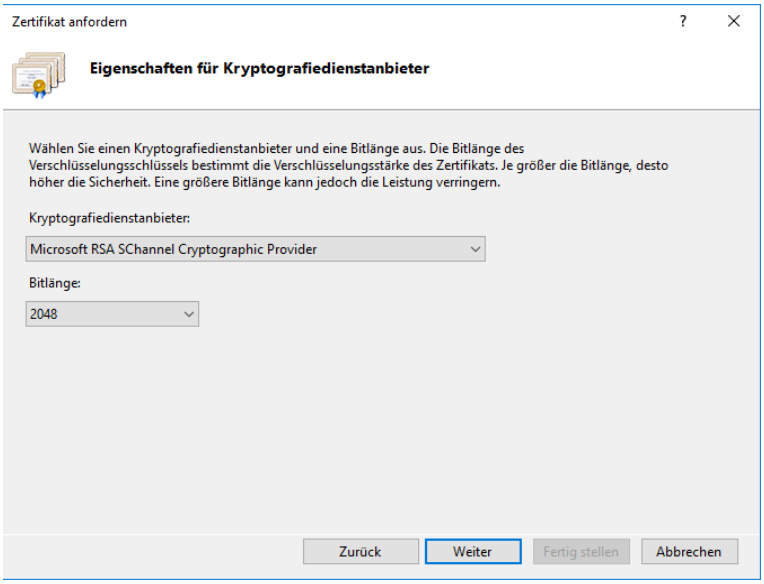
Beschaffung eines Zertifikates für die neue RDS-Infrastruktur

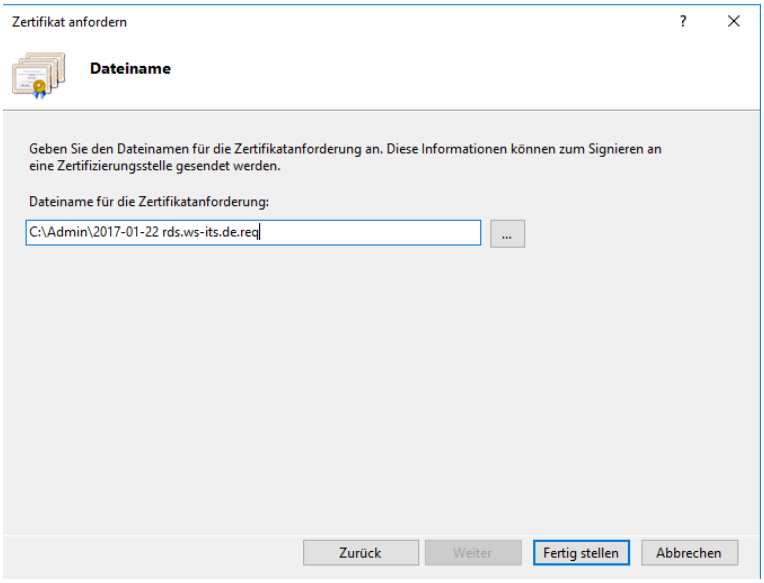
Auf dem WS-RDS1 nutze ich den IIS, um einen Certificate Signing Request zu erstellen:



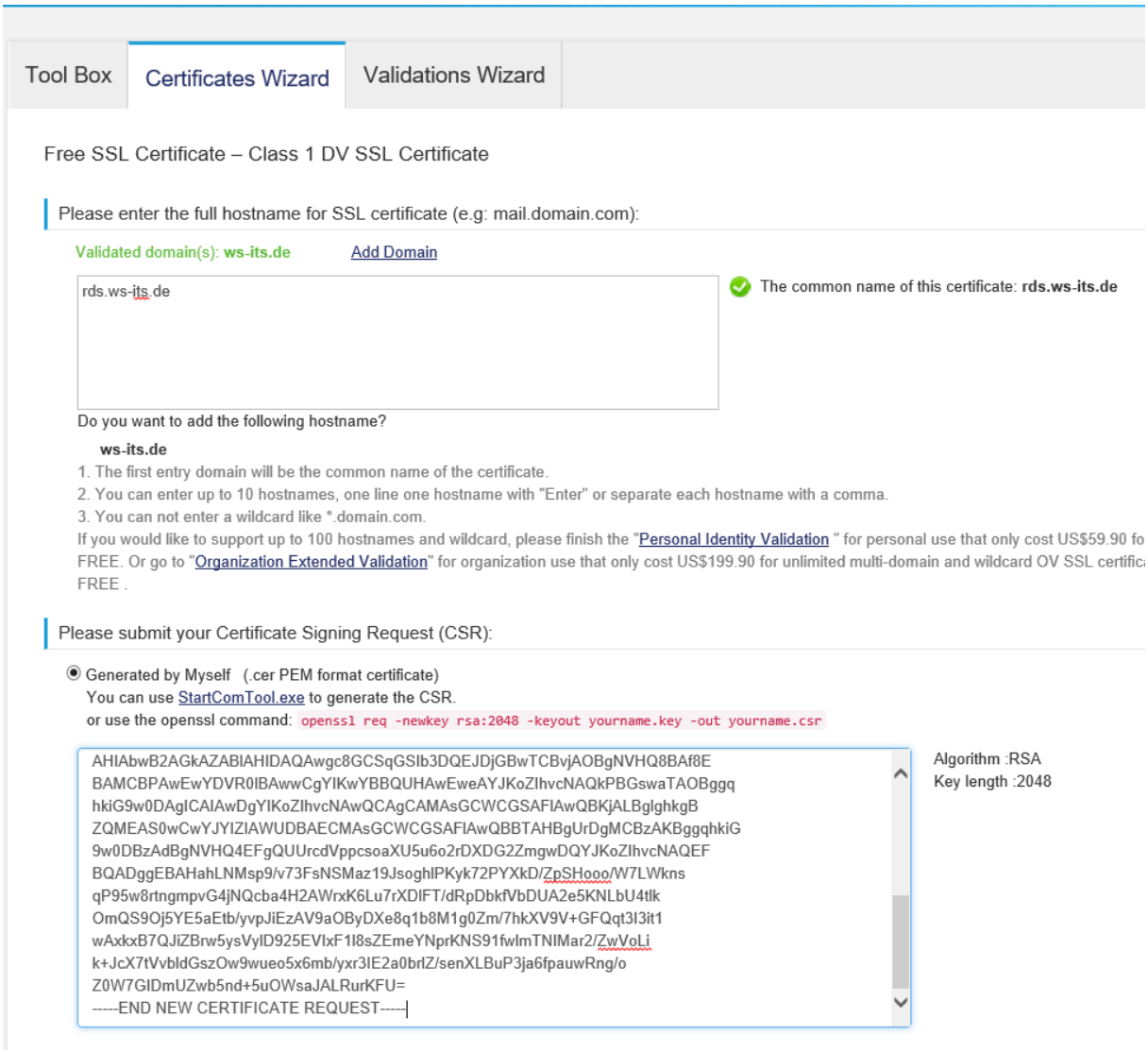
Der externe Name muss mit der Konfiguration des Gateways übereinstimmen.

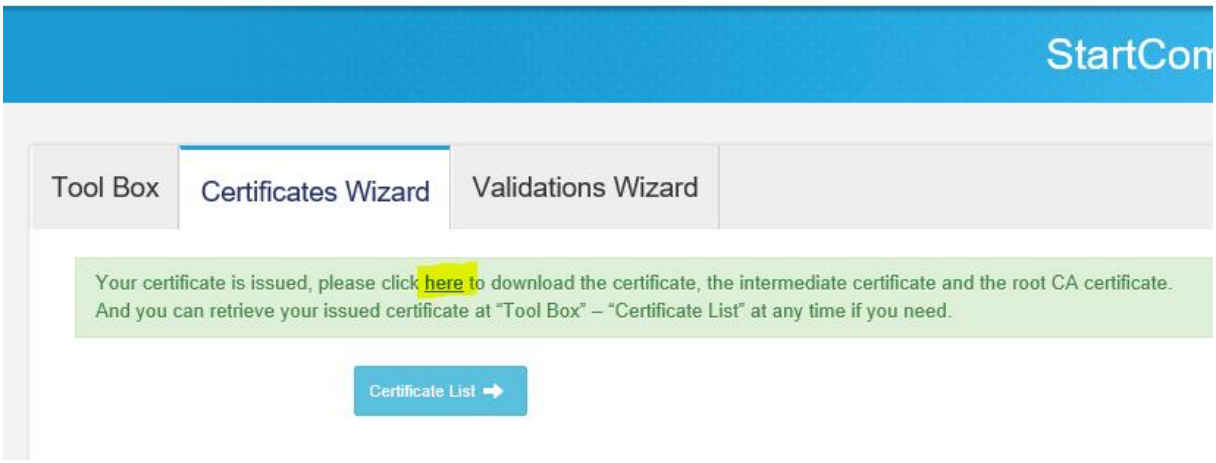




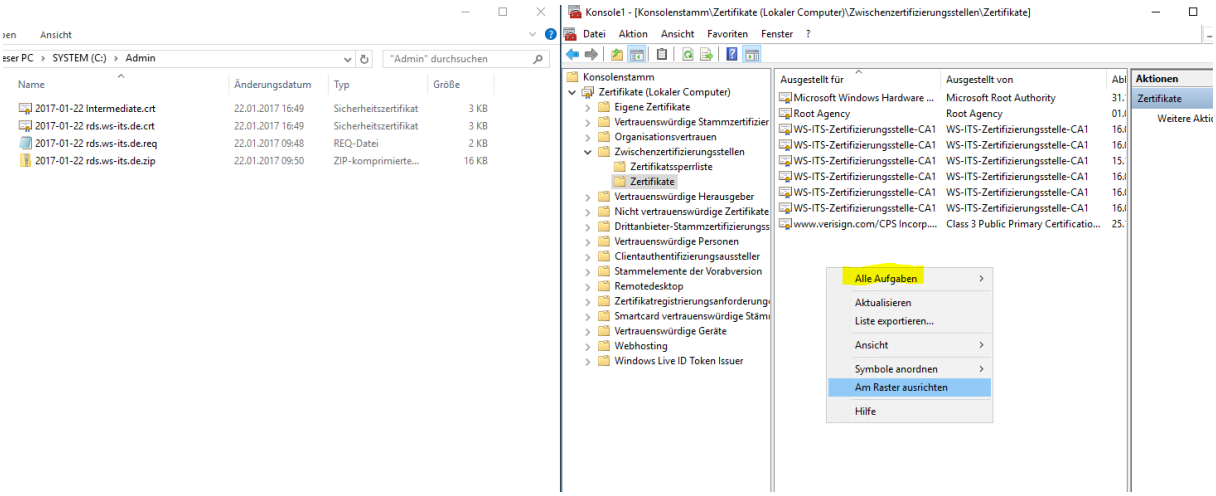


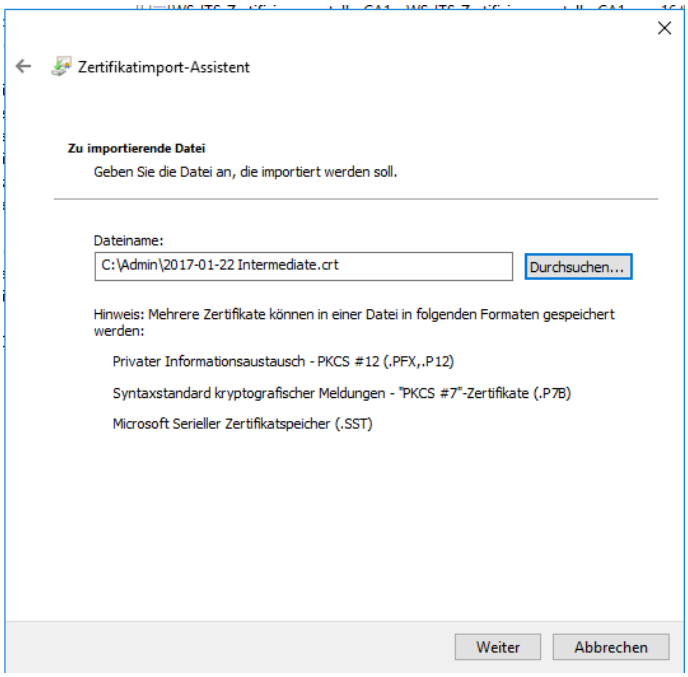
Den Request reiche ich bei der öffentlichen CA StartCom ein. Aktuell sind einige Consumer nicht von der Vertraulichkeit der CA überzeugt. Aber die Zugriffe sollen nur für meine Zwecke abgesichert werden und die Zertifikate sind kostenfrei ☺

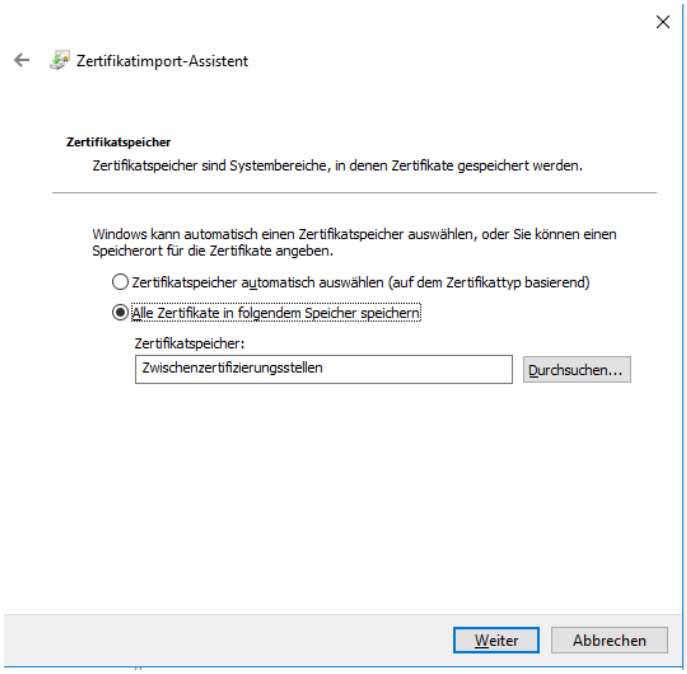




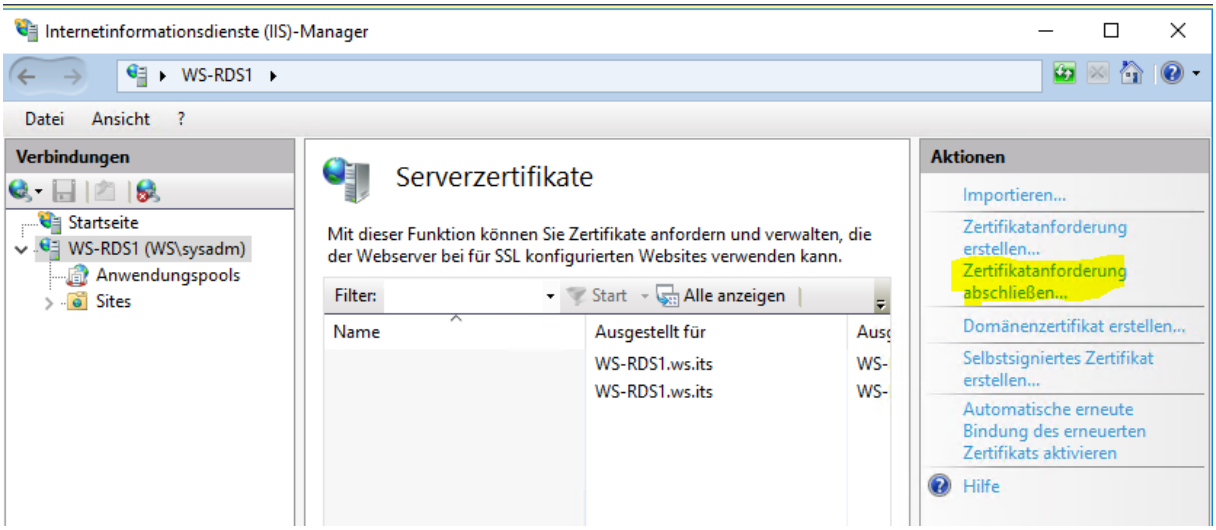
Das Intermediate-Zertifikat spiele ich noch manuell in den Speicher von WS-RDS1 ein:

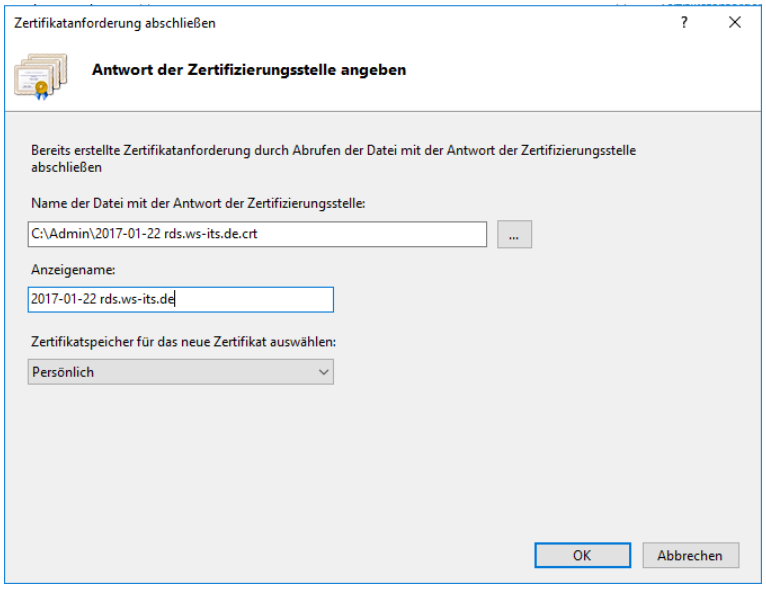




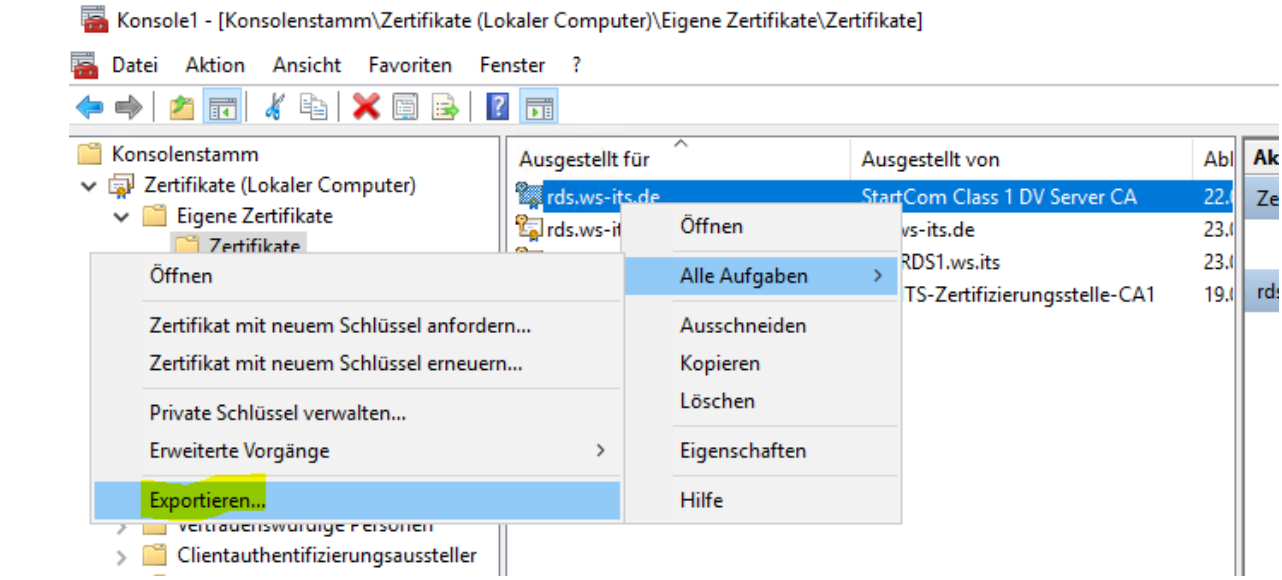


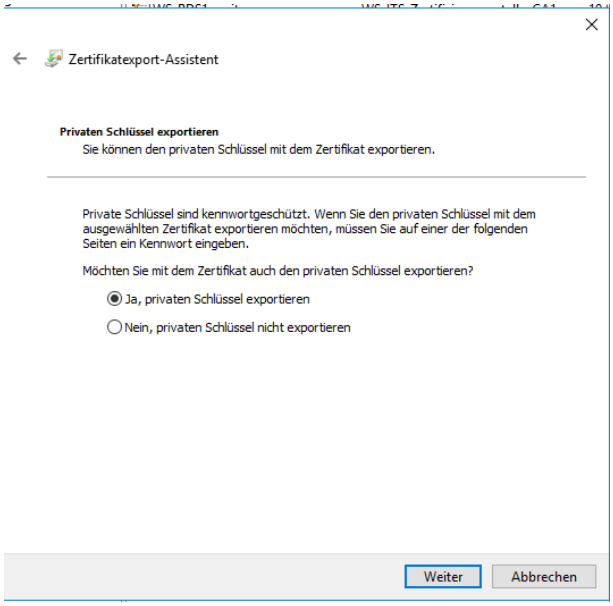
Das Zertifikat (der öffentliche Teil) wird dann im IIS mit dem Private Key zusammengeführt

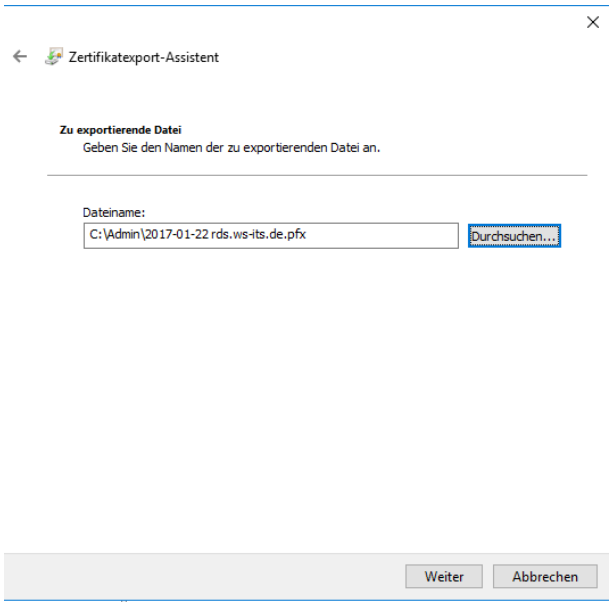




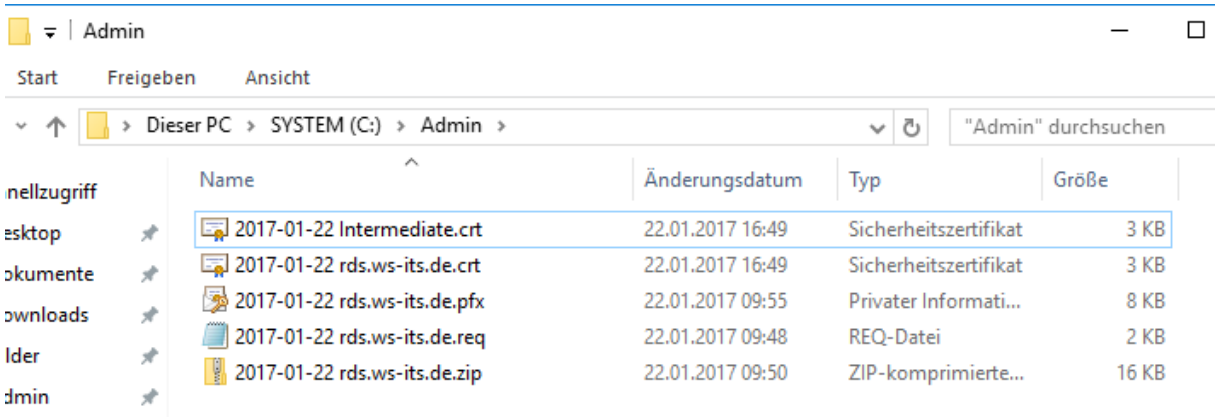
In dem Zertifikatspeicher von WS-RDS1 exportiere ich nun noch das fertige Zertifikat in eine PKCS#12 Datei. Diese wird gleich benötigt, um die RDS-Konfiguration abzuschließen. Zudem ist es nicht verkehrt, das komplette Zertifikat an einem sicheren Ort zusätzlich aufzubewahren:





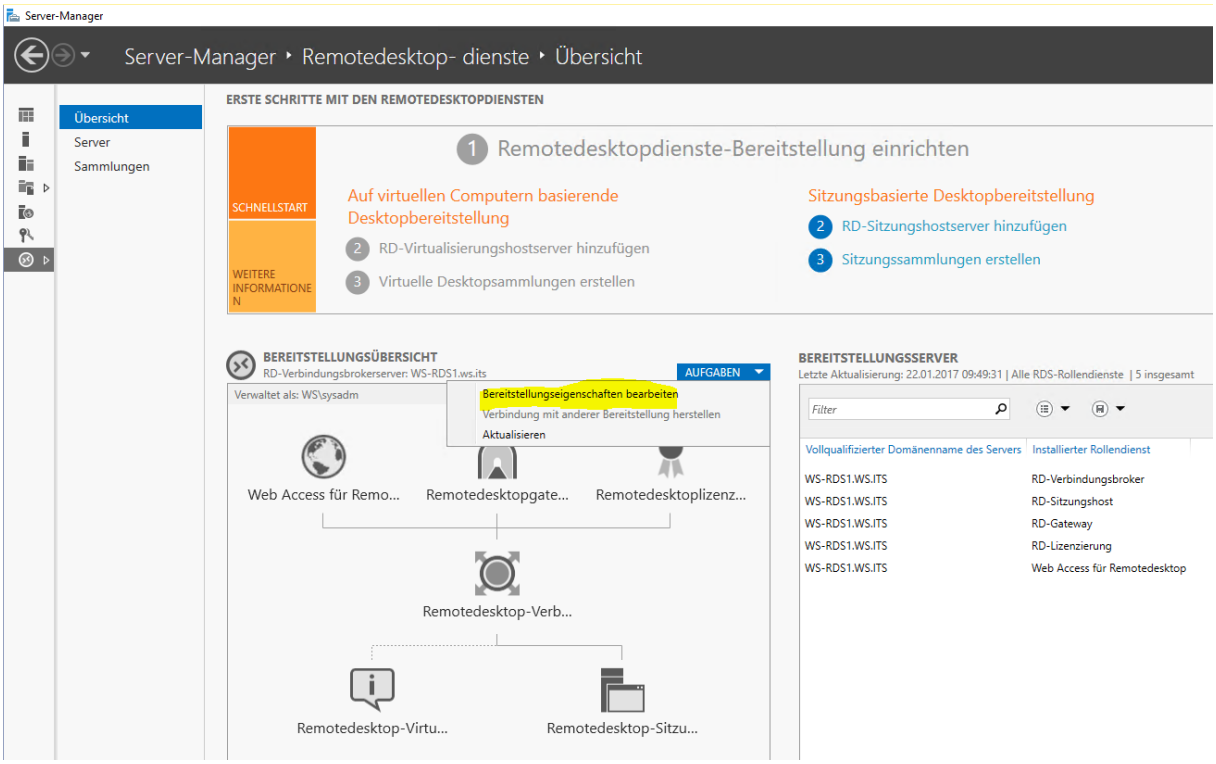


Jetzt liegen alle relevanten Dateien in einem Verzeichnis. Später verschiebe ich alles an einen sicheren Ort:

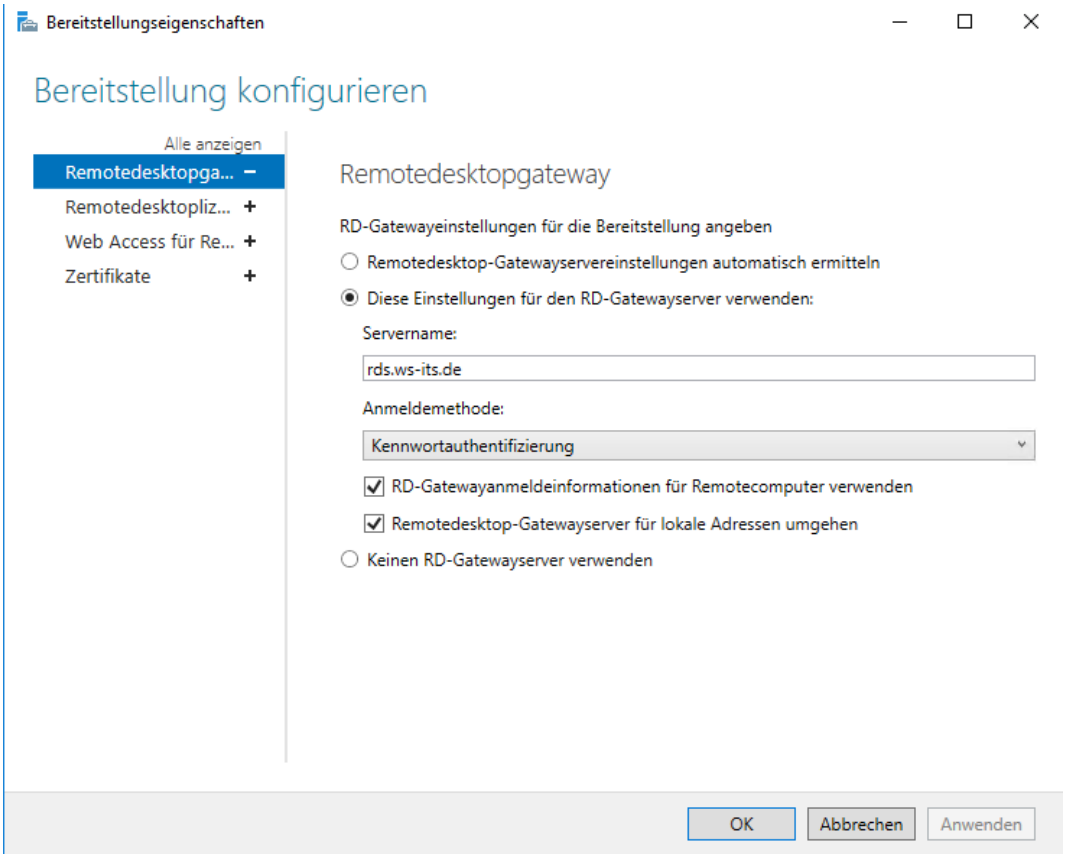


Konfiguration der RDS-Infrastruktur - allgemein

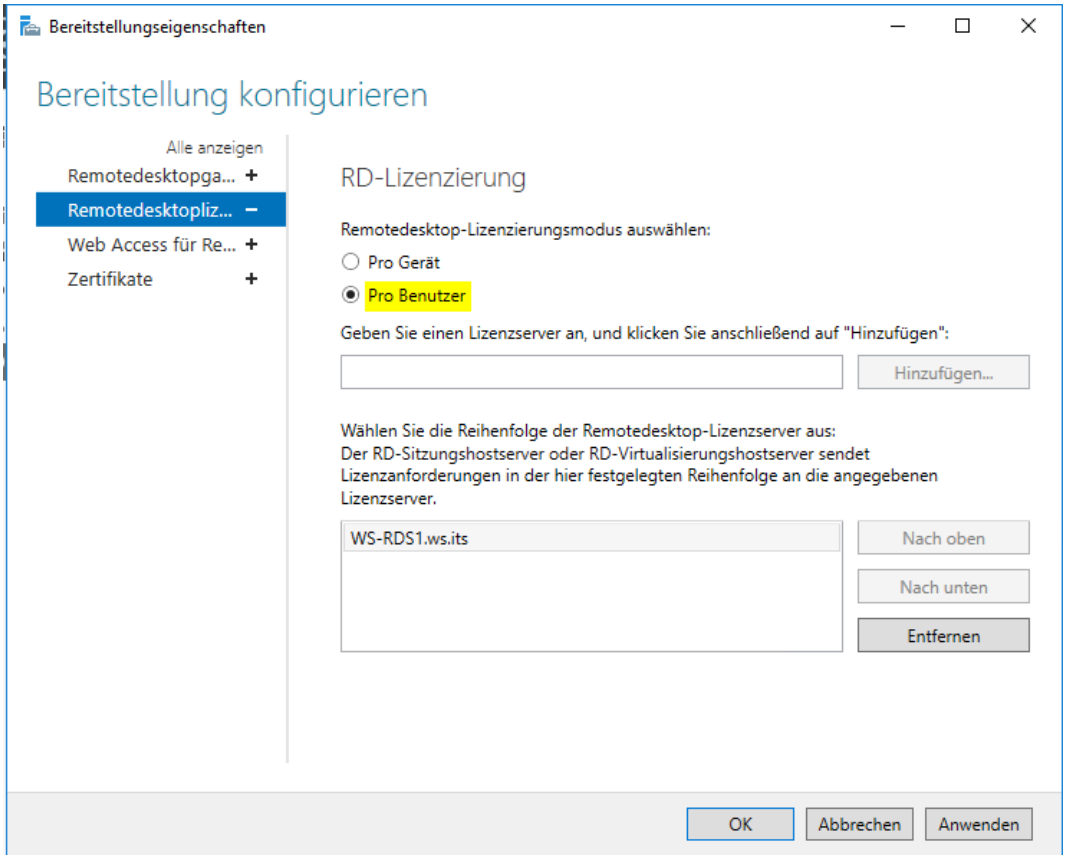
Im Servermanager starte ichh den erforderlichen Assistenten:



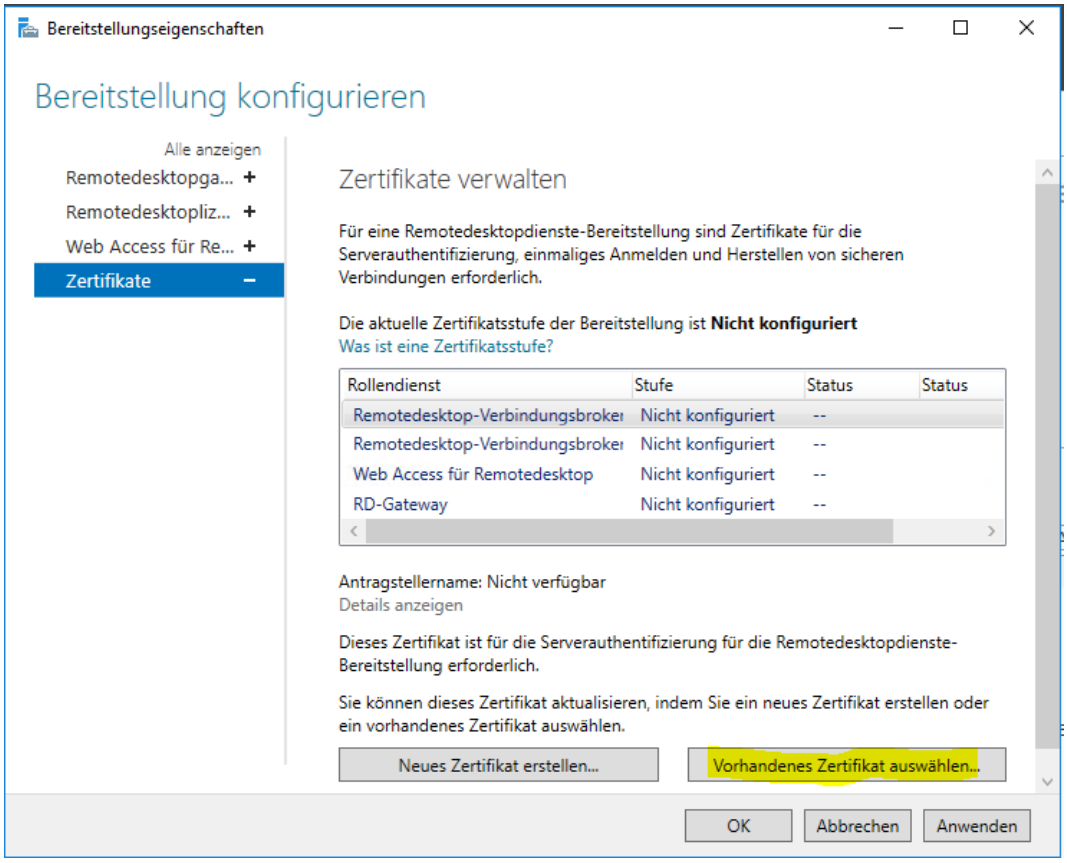
Die Adresse des Gateways passt bereits. Weitere Konfigurationen nehme ich später vor:



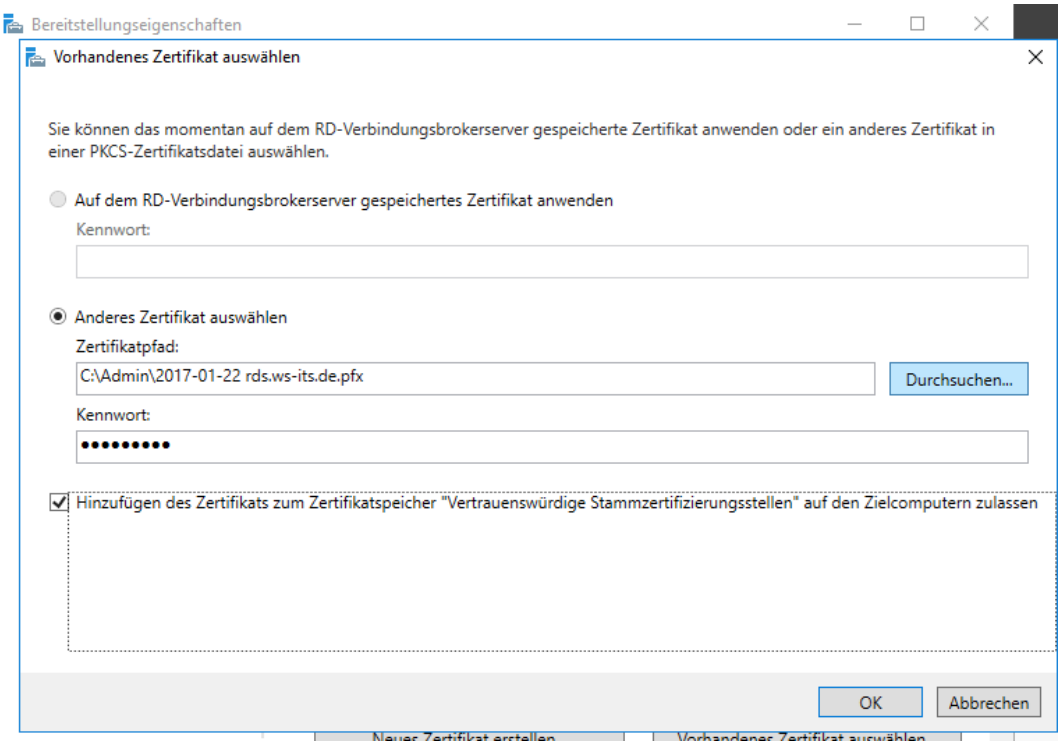
Die Lizenzierung stelle ich noch auf Pro Benutzer um. Der Lizenzserver benötigt ebenfalls separate Anpassungen:



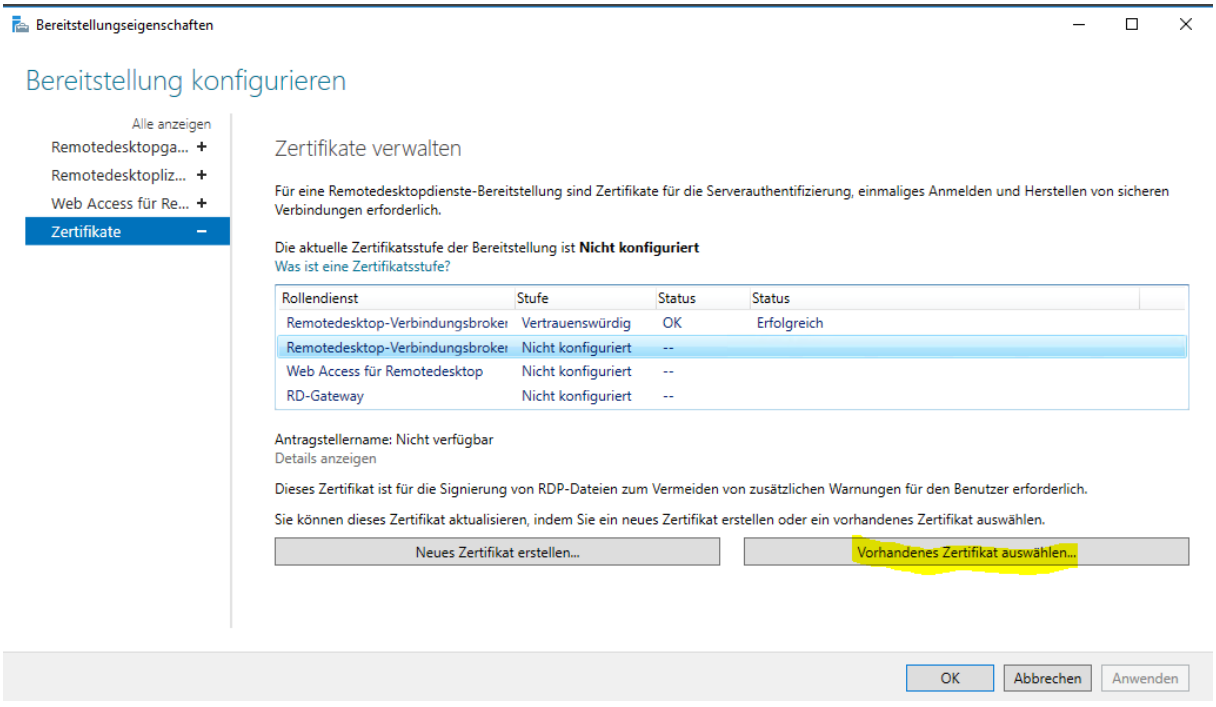
Im WebAccess kann man so nichts ändern. Dafür müssen die Zertifikatinformationen eingegeben werden:



Das vorhandene Zertifikat ist die zuvor exportierte PKCS#12-Datei des externen Zertifikates:

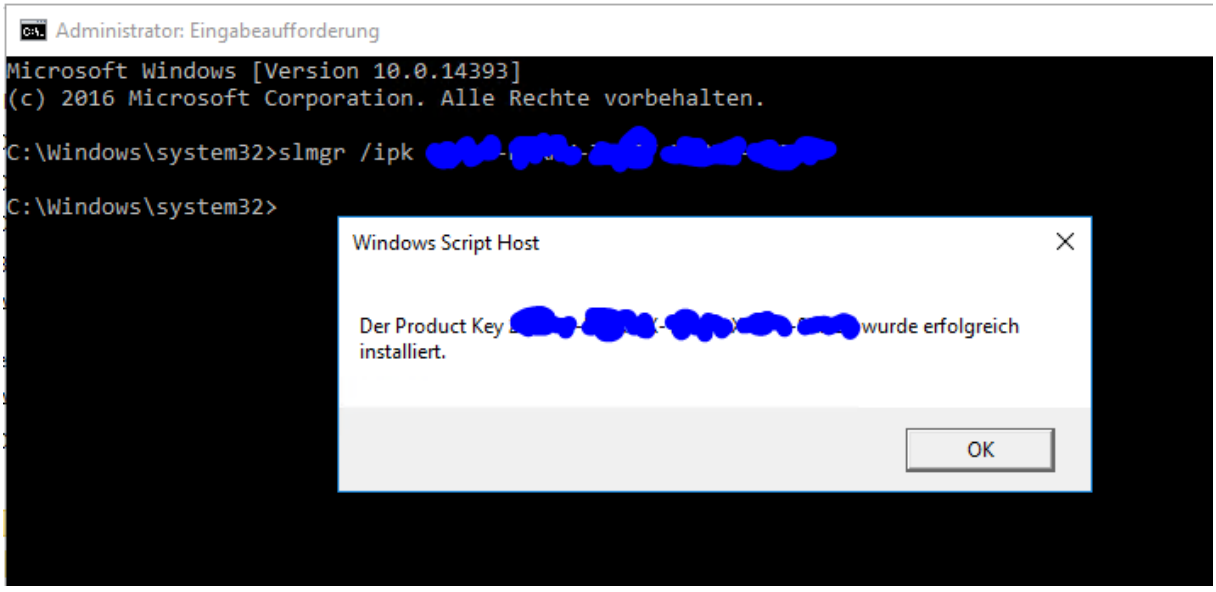


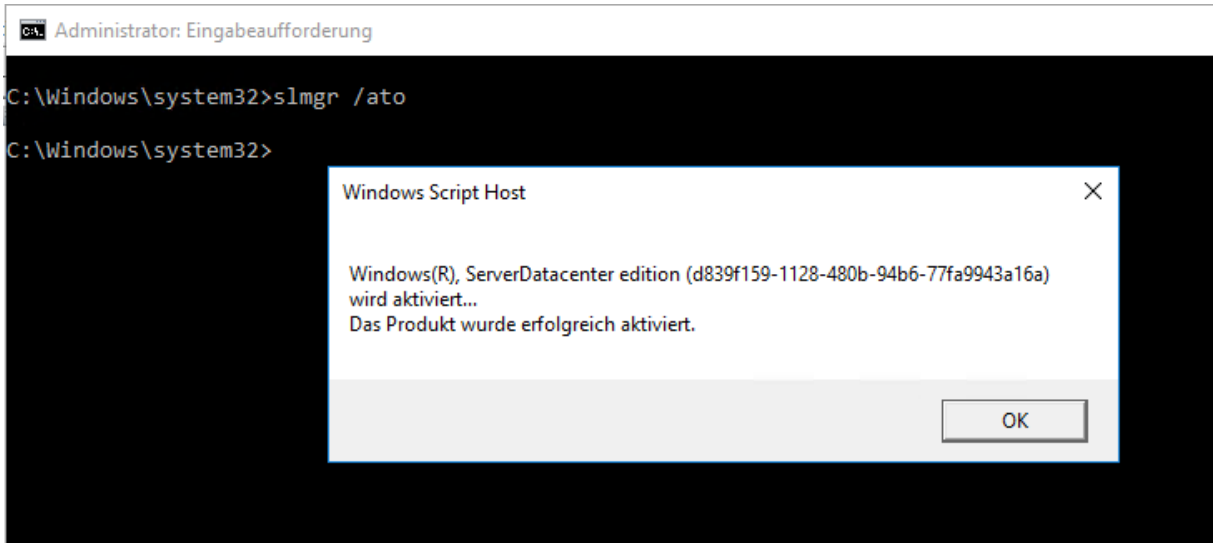
Der Arbeitsschritt ist für jedes Element in der Tabelle einzeln zu wiederholen…



… bis alle Einträge einen Status = OK aufweisen:

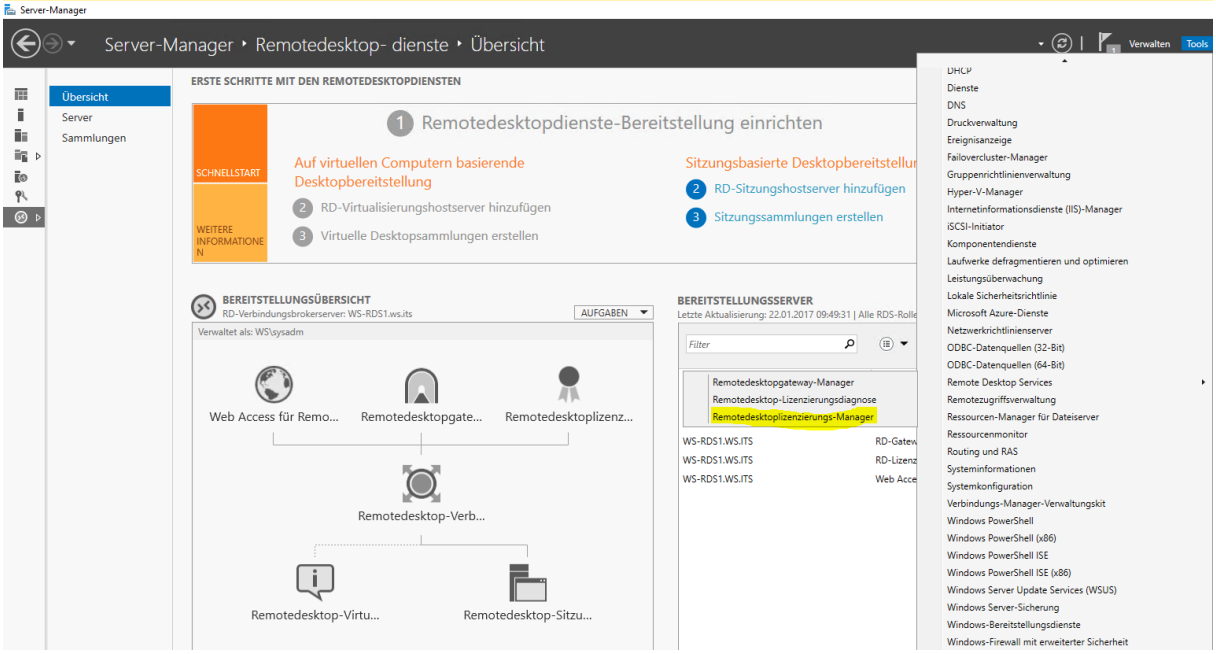
Damit ich den Lizenzserver des RDS aktivieren kann, muss ich das Windows Server 2016 Betriebssystem noch eben aktivieren:



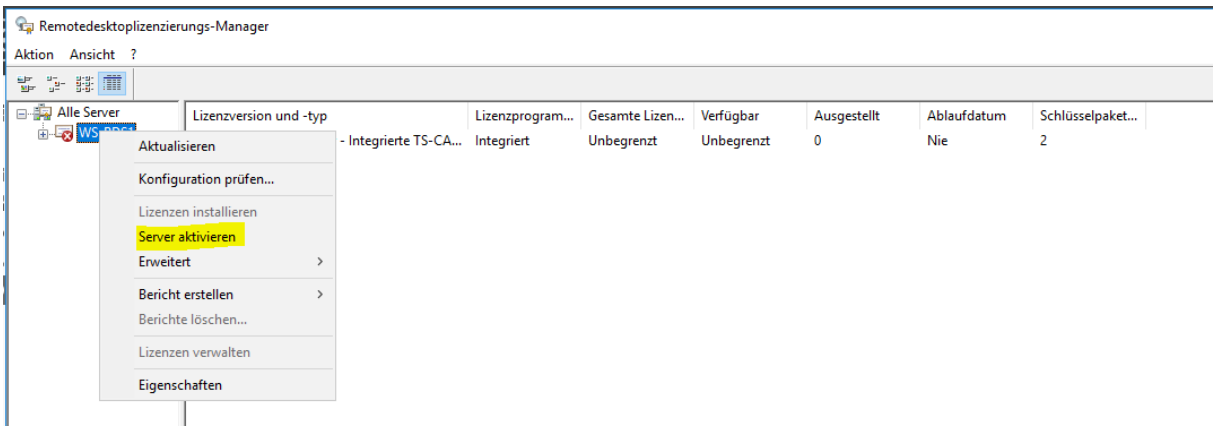


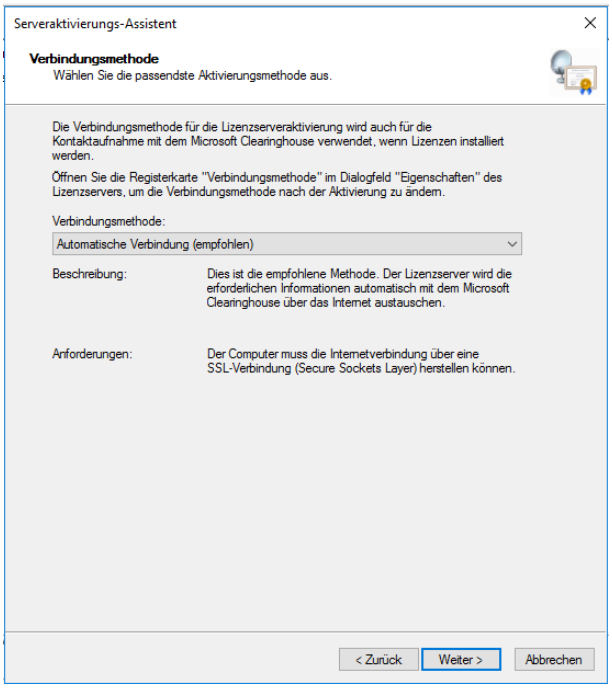
Konfiguration der Lizenzierung – Migration der bestehenden CALs

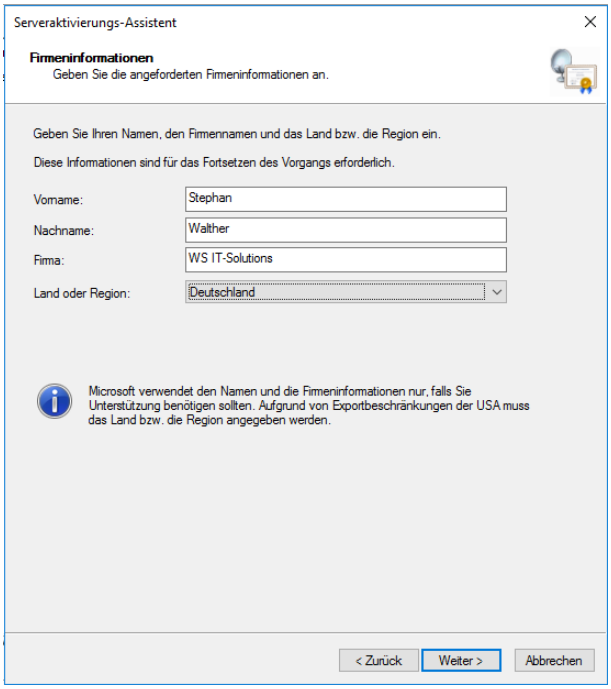
Im Servermanager gibt es einen Eintrag unter den Tools mit dem (endlich korrekten) Namen „Remote Desktop Services“. Darunter findet man die Lizenz-Management-Konsole:

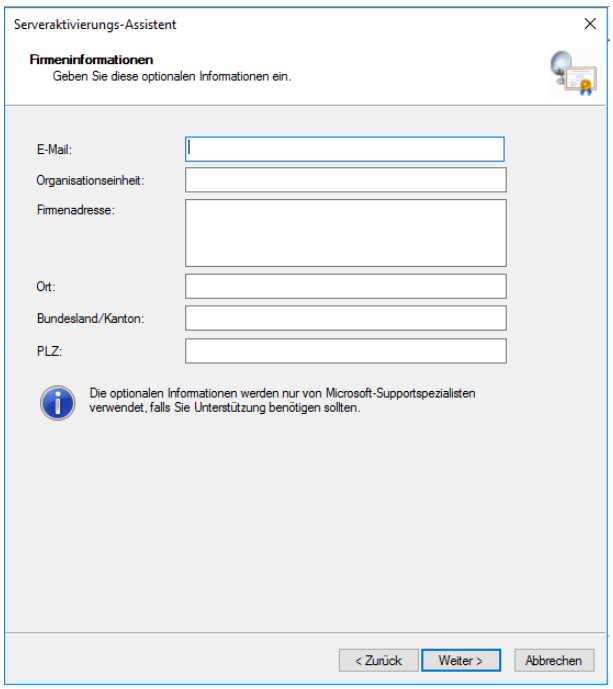


Zunächst aktiviere ich den neuen RDS-Lizenzserver:

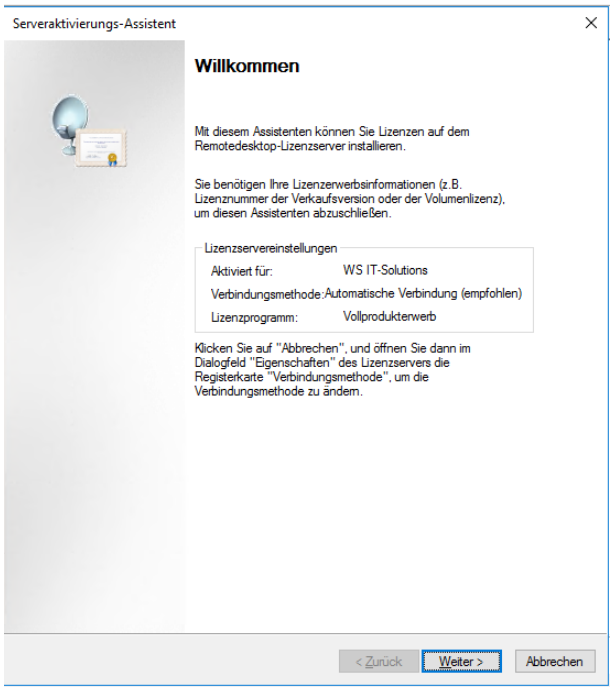


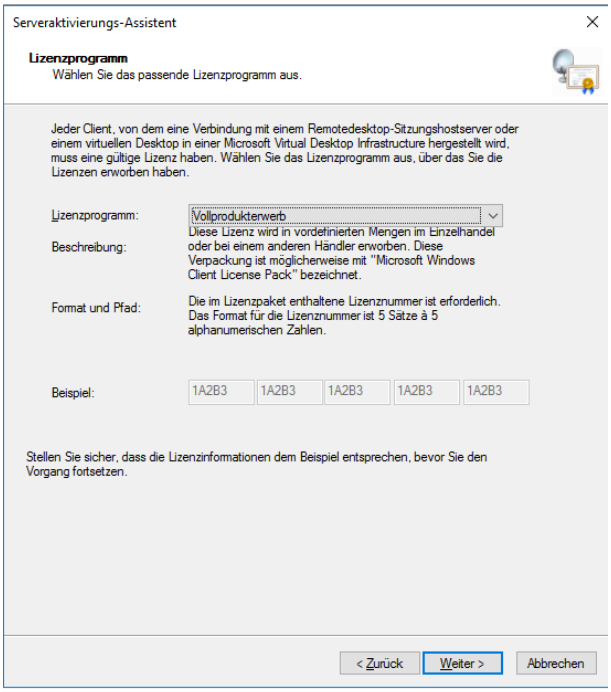




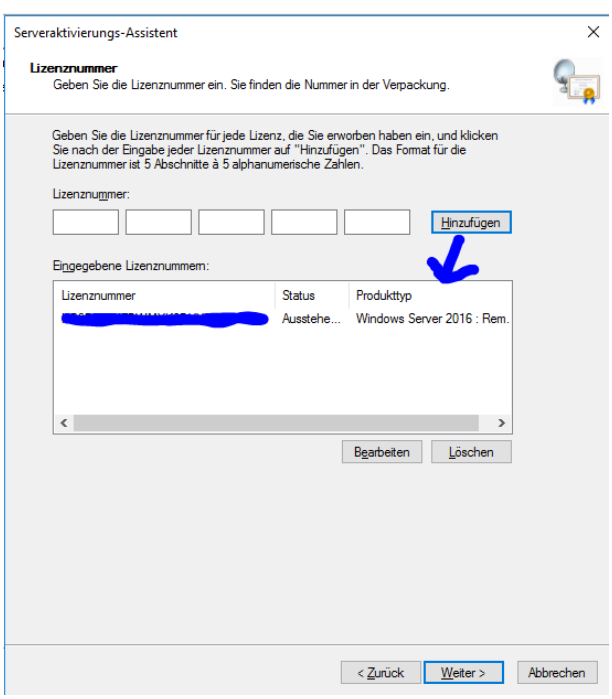


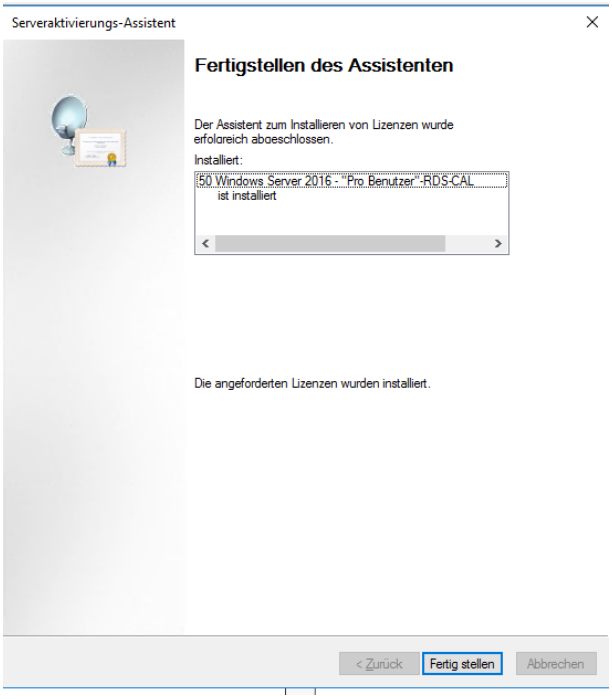
Danach lasse ich automatisch den Lizenzinstallations-Assistenten starten:



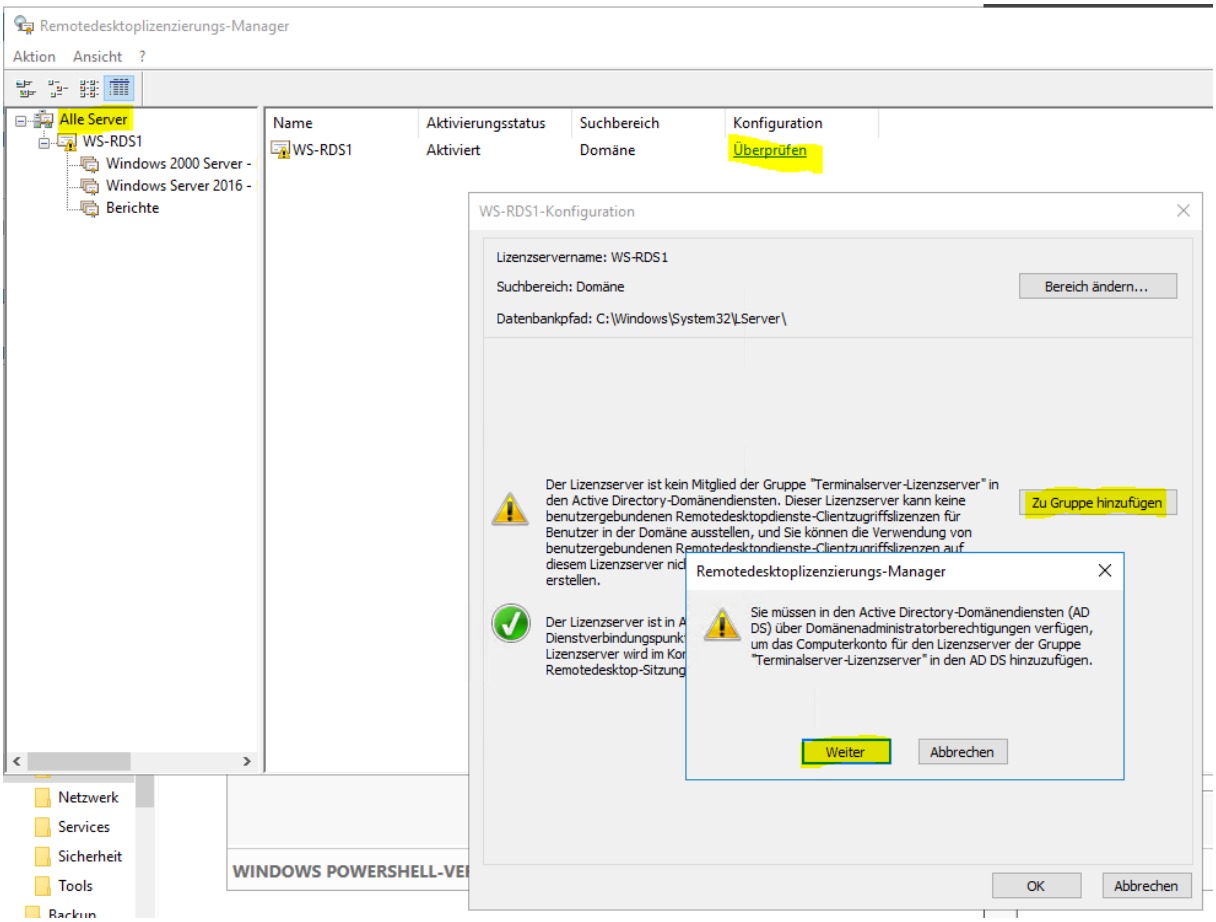


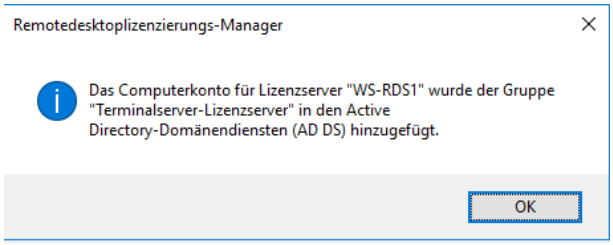
Ich installiere 50 neue CALs für Windows Server 2016:



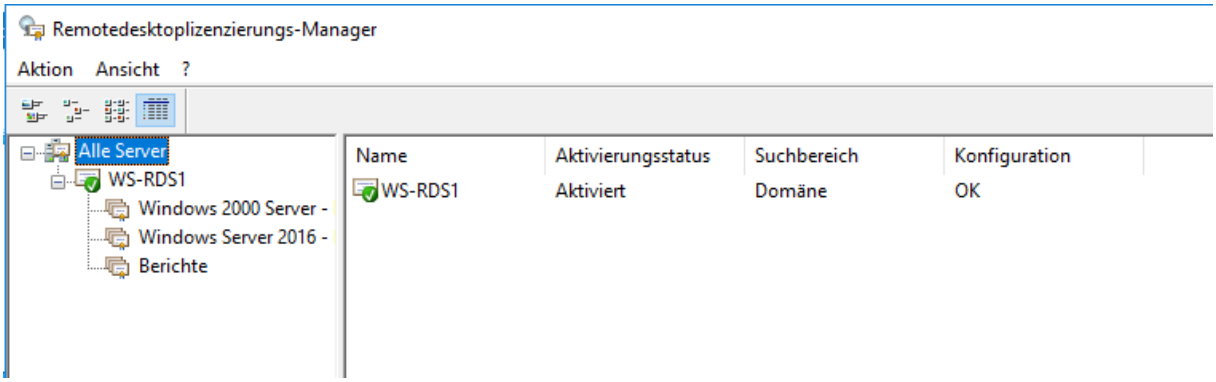


Ich starte nun die Serverprüfung. Dabei stellt das System fest, dass eine Gruppenmitgliedschaft im AD fehlt. Diese kann direkt über den Assistenten nachgeholt werden:

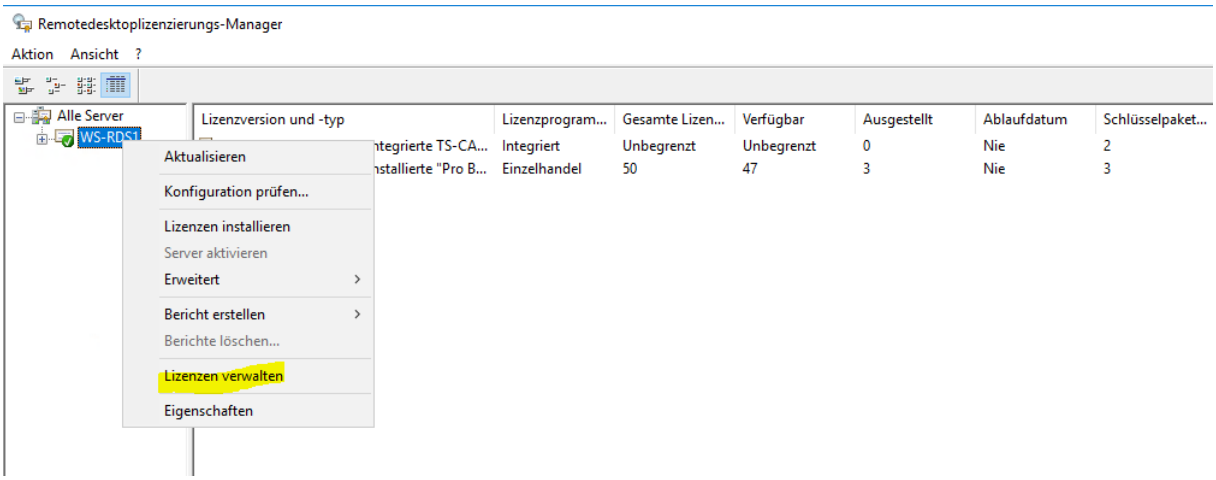


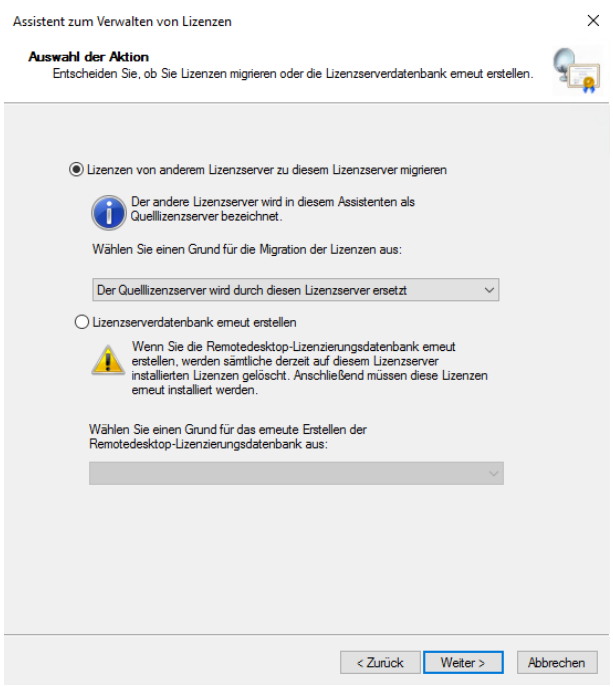


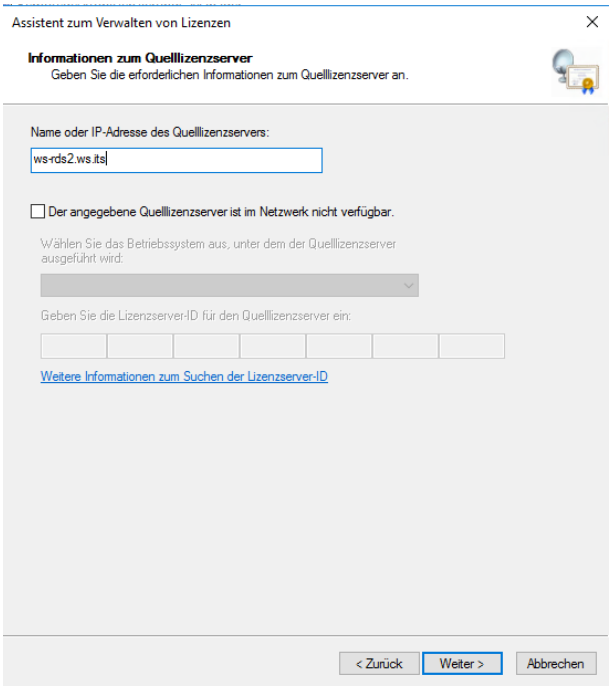
Der LIMA ist nun einsatzbereit:



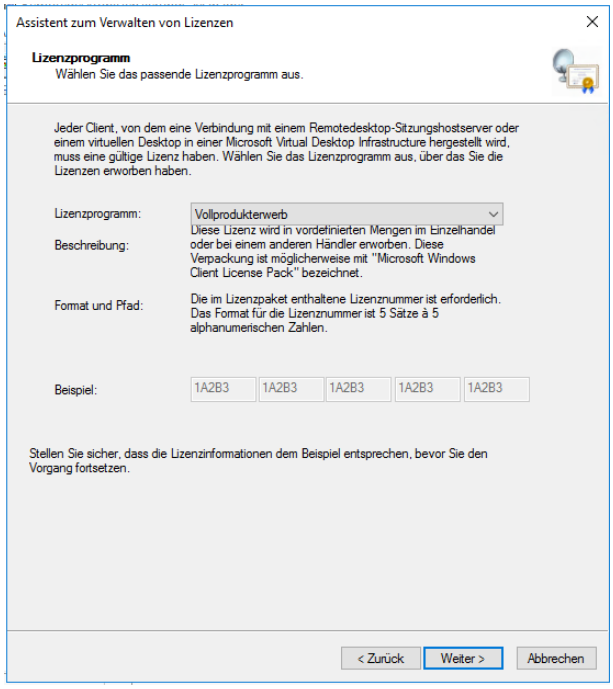
Die alten Lizenzen meiner Windows Server 2012 R2 Umgebung möchte ich aber auch portieren. Diese lagen ja zuerst jeweils als 50er Pakete auf beiden alten RDS-Servern. Im Rahmen der Vorbereitung verschob ich die 50 CAL des alten WS-RDS1 auf den alten WS-RDS2. Dessen 100 CALs hole ich nun auf den neuen WS-RDS1:

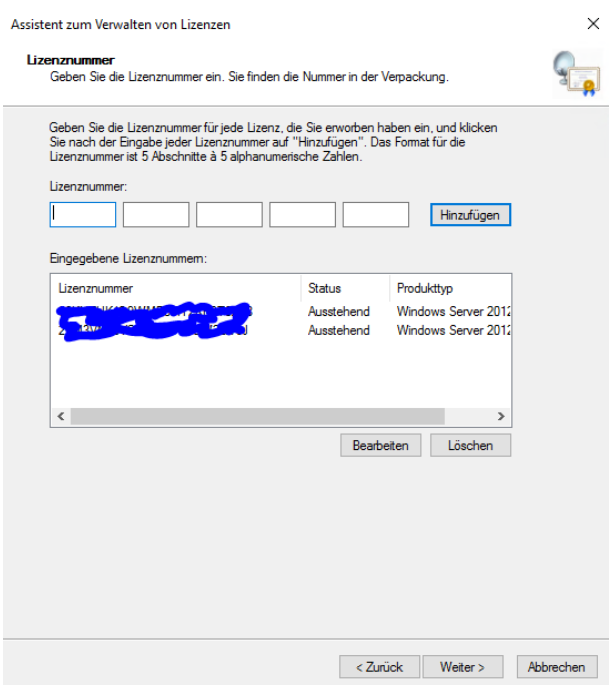




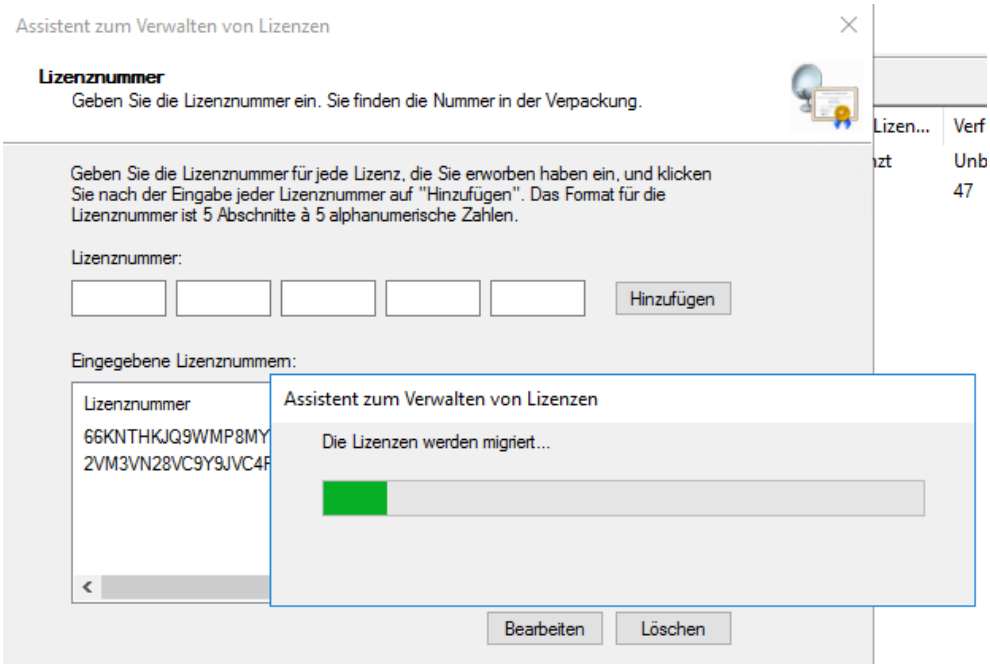


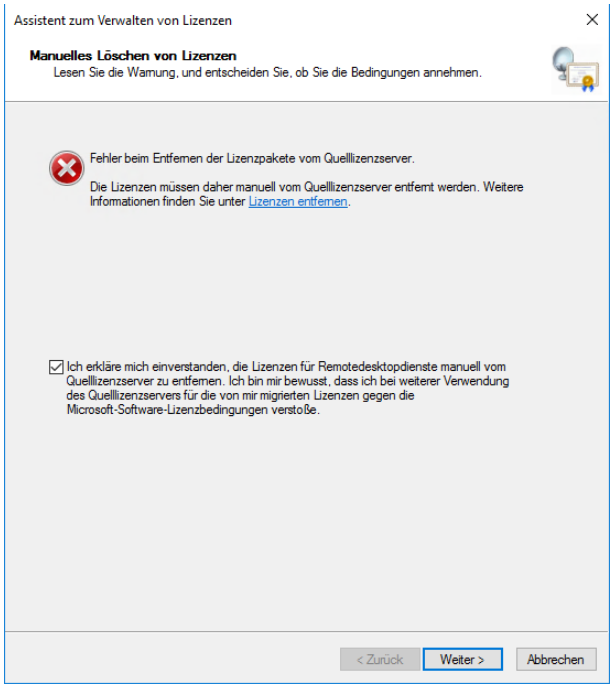
Auch hier müssen die CAL-Schlüssel eingegeben werden:

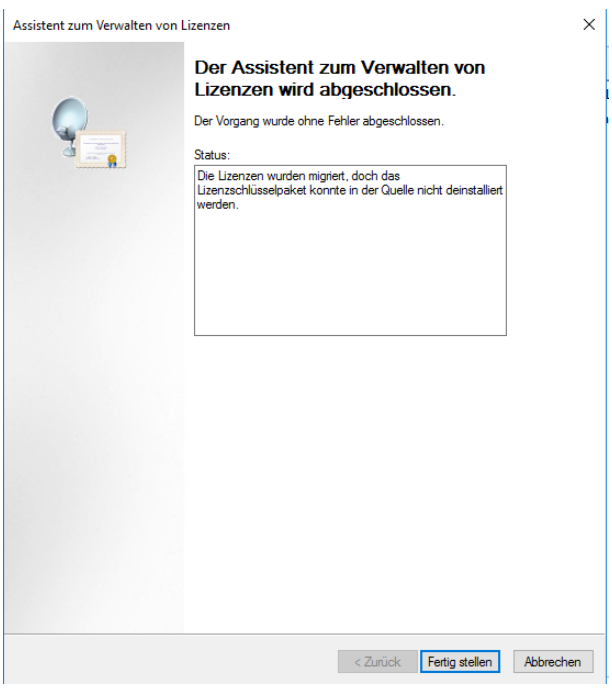




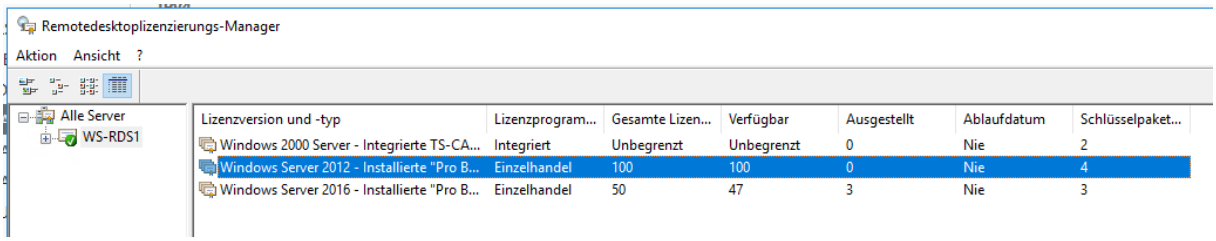
Die Übertragung der CALs läuft:



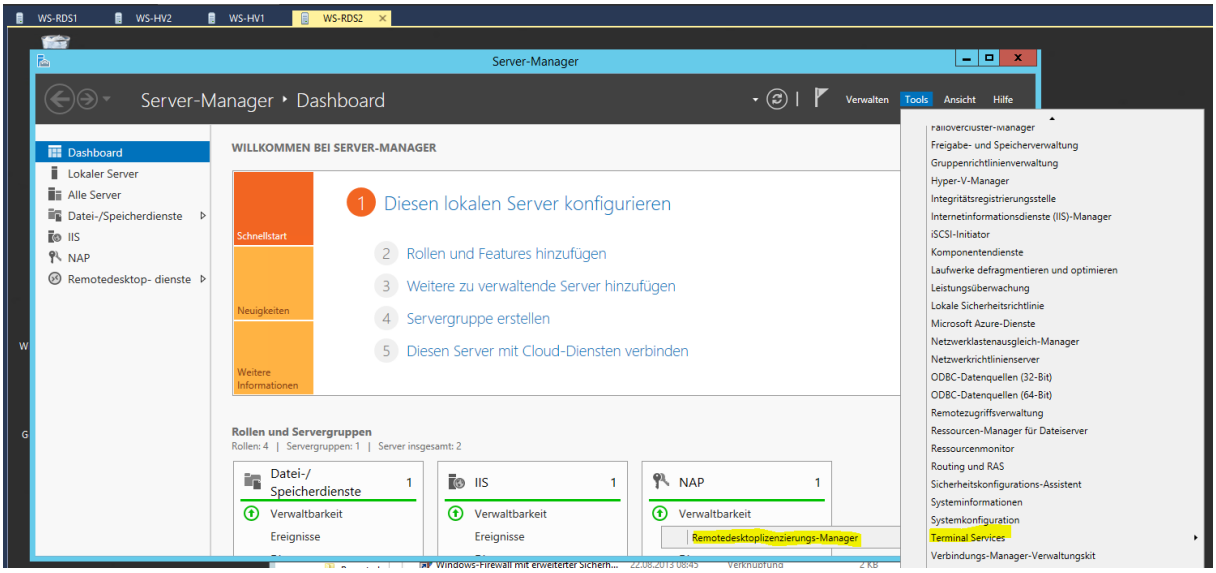


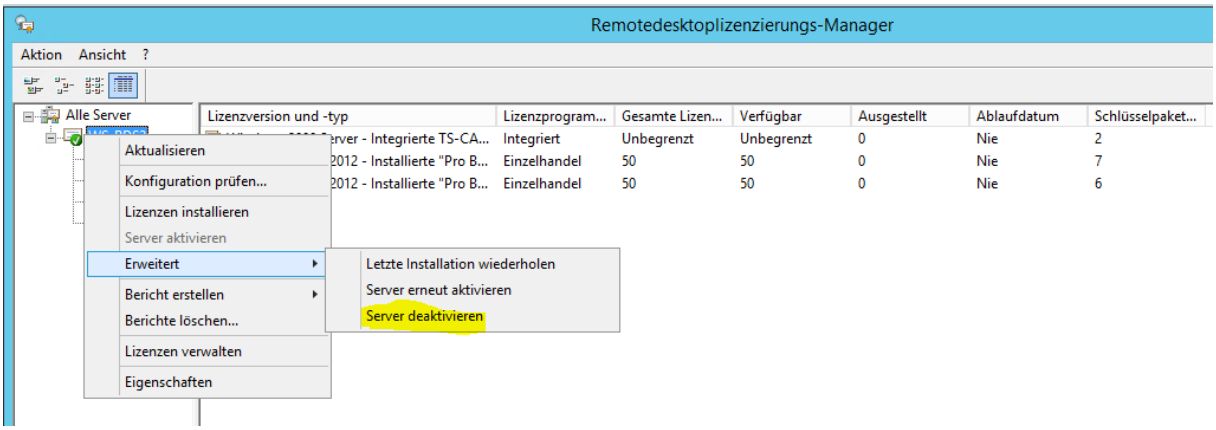


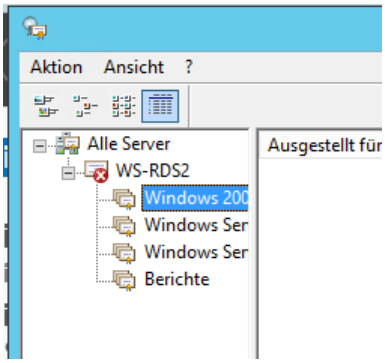
Beim Übertragen ist ein Fehler aufgetreten. Die CALs können dennoch eingespielt werden, wenn ich sicherstelle, dass der alte Server nicht weiter über die CALs verfügen kann:



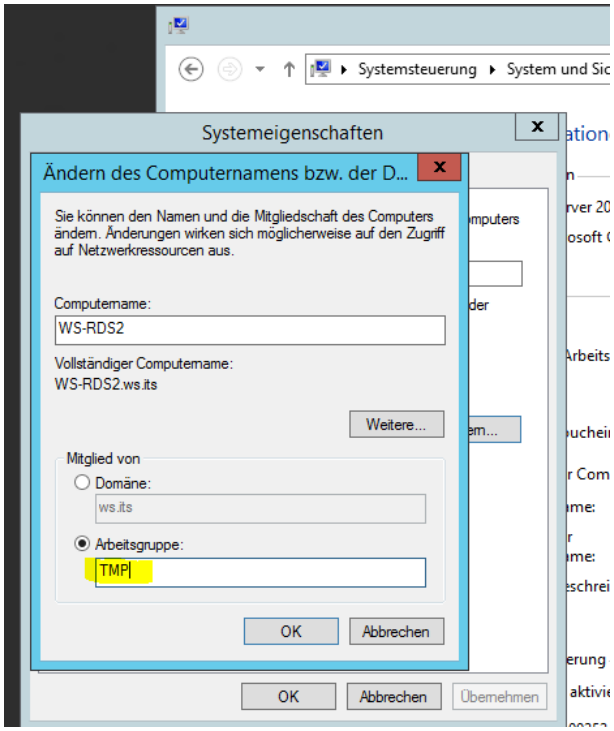
Um dies sicherzustellen (und meinem Ziel – nur ein RDS-Server – näher zu kommen), deinstalliere ich die Rolle vom alten Server. Zuvor deaktiviere ich ihn bei Microsoft:


WS-RDS1
WS-HV2
WS-HV1
WS-RDS2
Server-Manager
Server-Manager • Dashboard
Verwalten
Tools
Ansicht
Hilfe
Dashboard
Lokaler Server
Alle Server
Datei-/Speicherdienste
IIS
NAP
Remotedesktop- dienste
WILLKOMMEN BEI SERVER-MANAGER
Schnellstart
Neuigkeiten
Weitere Informationen
1 Diesen lokalen Server konfigurieren
2 Rollen und Features hinzufügen
3 Weitere zu verwaltende Server hinzufügen
4 Servergruppe erstellen
5 Diesen Server mit Cloud-Diensten verbinden
Rollen und Servergruppen
Rollen: 4 | Servergruppen: 1 | Server insgesamt: 2
Datei-/ Speicherdienste 1
IIS 1
NAP 1
Verwaltbarkeit
Ereignisse
Remotedesktoplizenzierungs-Manager
Terminal Services
Freigabe- und Speicherverwaltung
Gruppenrichtlinienverwaltung
Hyper-V-Manager
Integritätsregistrierungsstelle
Internetinformationsdienste (IIS)-Manager
iSCSI-Initiator
Komponentendienste
Laufwerke defragmentieren und optimieren
Leistungsüberwachung
Lokale Sicherheitsrichtlinie
Microsoft Azure-Dienste
Netzwerklastenausgleich-Manager
Netzwerkrichtlinienserver
ODBC-Datenquellen (32-Bit)
ODBC-Datenquellen (64-Bit)
Remotezugriffsverwaltung
Ressourcen-Manager für Dateiserver
Ressourcenmonitor
Routing und RAS
Sicherheitskonfigurations-Assistent
Systeminformationen
Systemkonfiguration
Verbindungs-Manager-Verwaltungskit


Remotedesktoplizenzierungs-Manager
Aktion
Ansicht
?
Alle Server
Lizenzversion und -typ
Lizenzprogram...
Gesamte Lizen...
Verfügbar
Ausgestellt
Ablaufdatum
Schlüsselpaket...
Integriert
Unbegrenzt
Unbegrenzt
0
Nie
2
Einzelhandel
50
50
0
Nie
7
Einzelhandel
50
50
0
Nie
6
Aktualisieren
Konfiguration prüfen...
Lizenzen installieren
Server aktivieren
Erweitert
Bericht erstellen
Berichte löschen...
Lizenzen verwalten
Eigenschaften
Letzte Installation wiederholen
Server erneut aktivieren
Server deaktivieren


Aktion
Ansicht
?
Alle Server
WS-RDS2
Windows 200
Windows Ser
Windows Ser
Berichte
Ausgestellt für

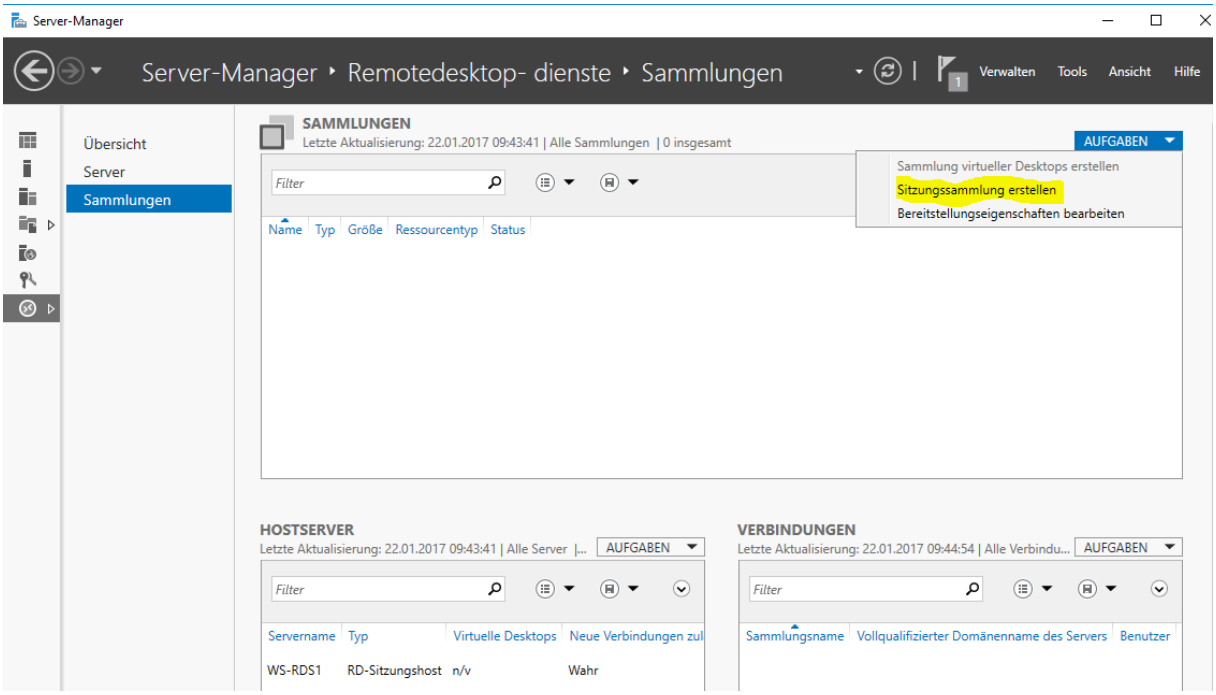
Jetzt entferne ich den alten WS-RDS2 aus der Domäne:



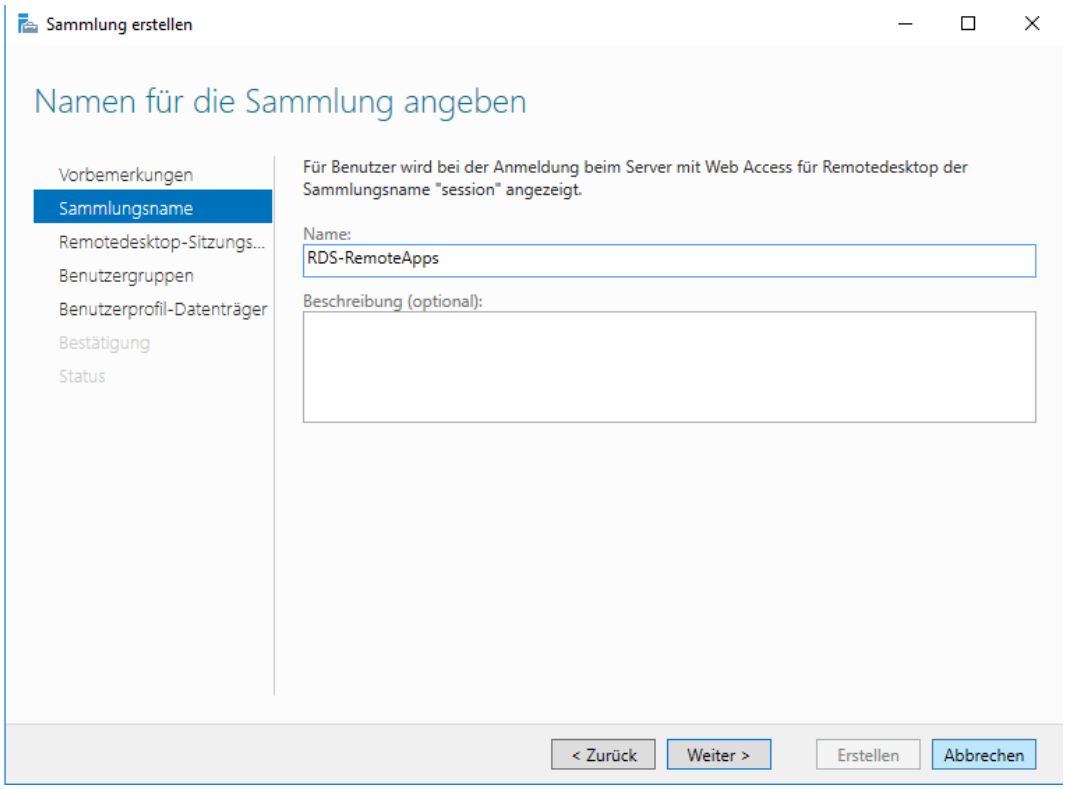
Abschließend entferne ich die VM aus dem Hyper-V-Host.

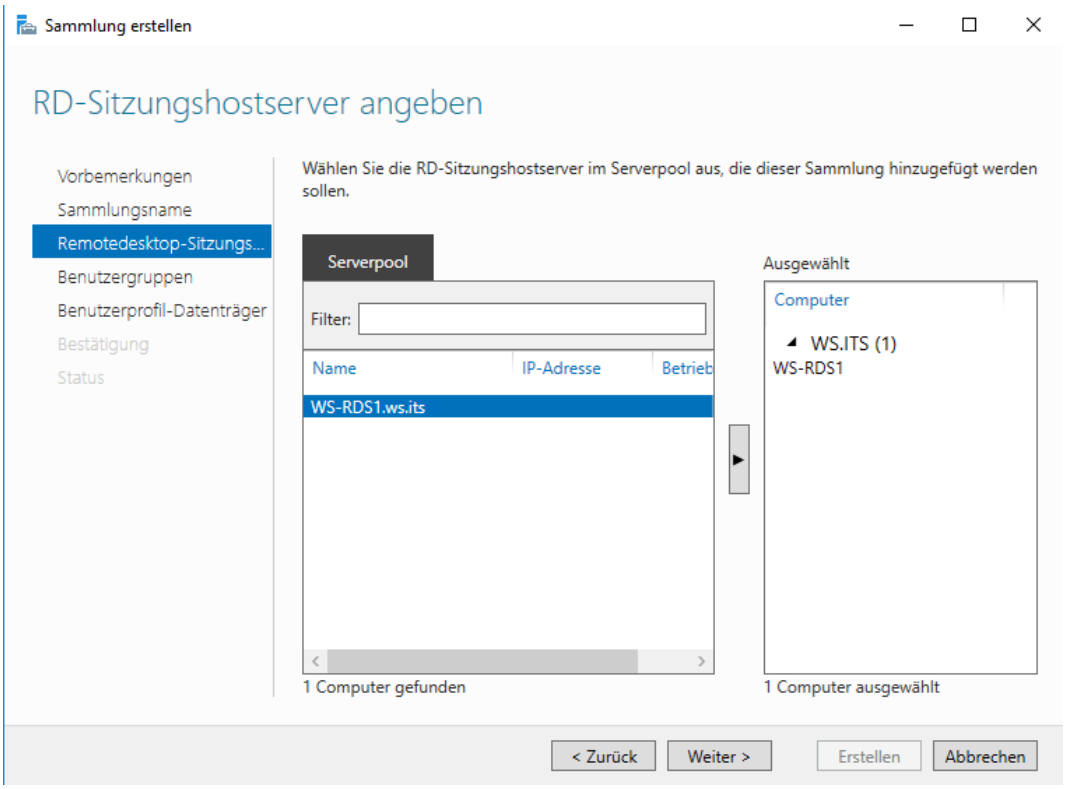
Konfiguration der SitzungsSammlung

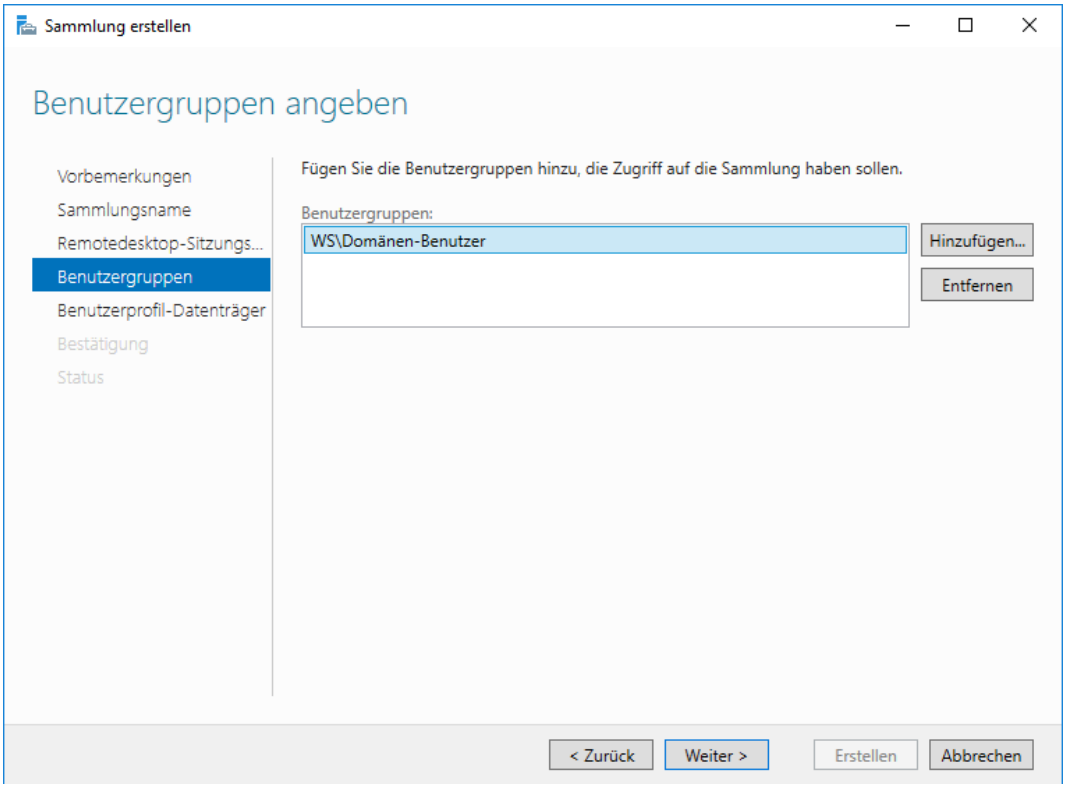
Ein Sessionhost benötigt weiter eine Collection zur Veröffentlichung:



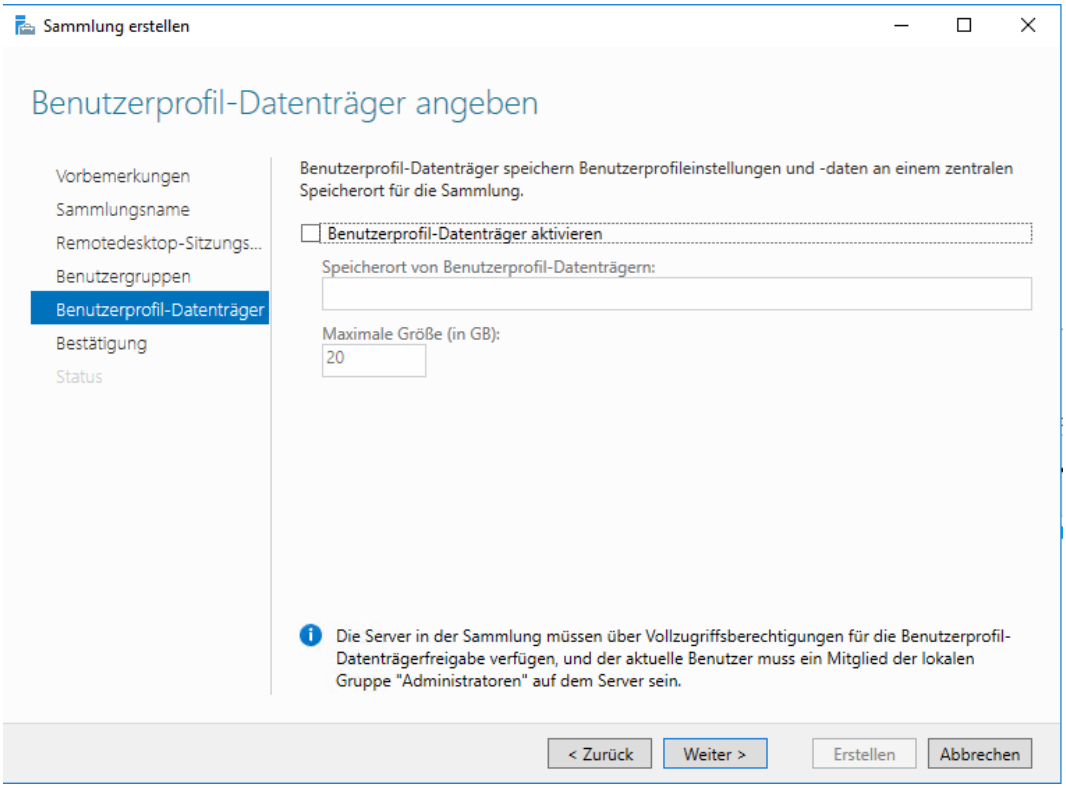
Auch der neue Server soll nur RemoteApps veröffentlichen. Die weiteren Optionen entsprechen denen einer Windows Server 2012 R2 Umgebung:



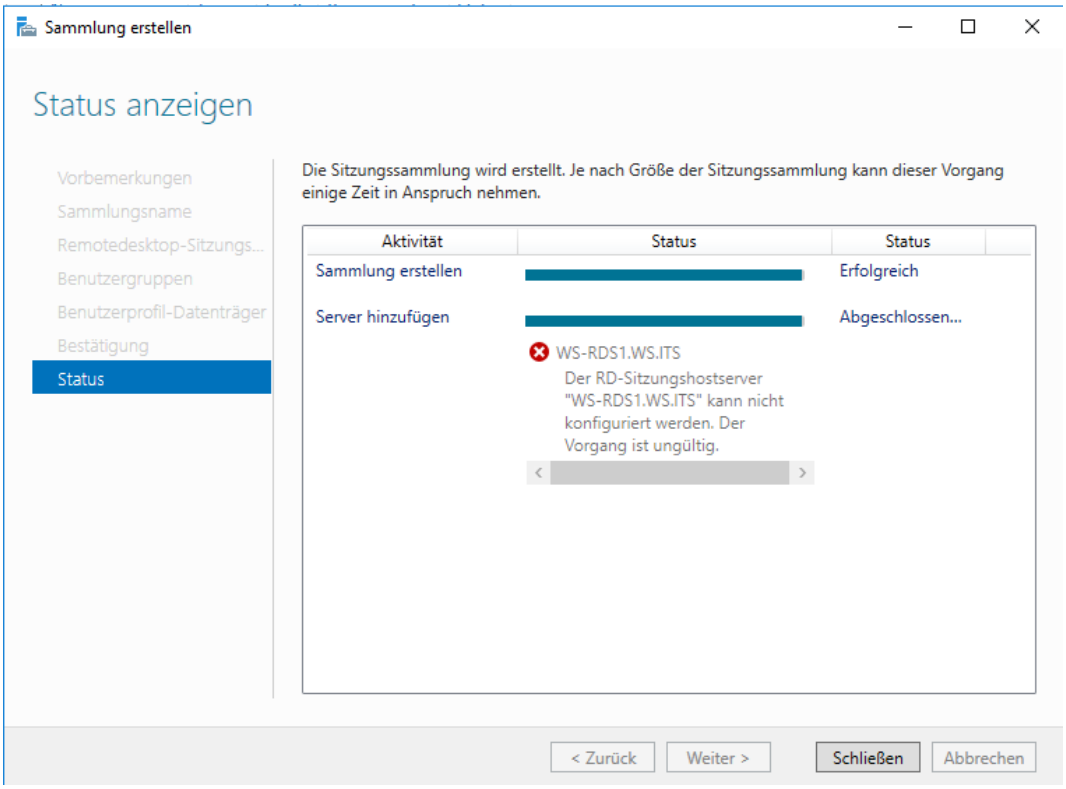




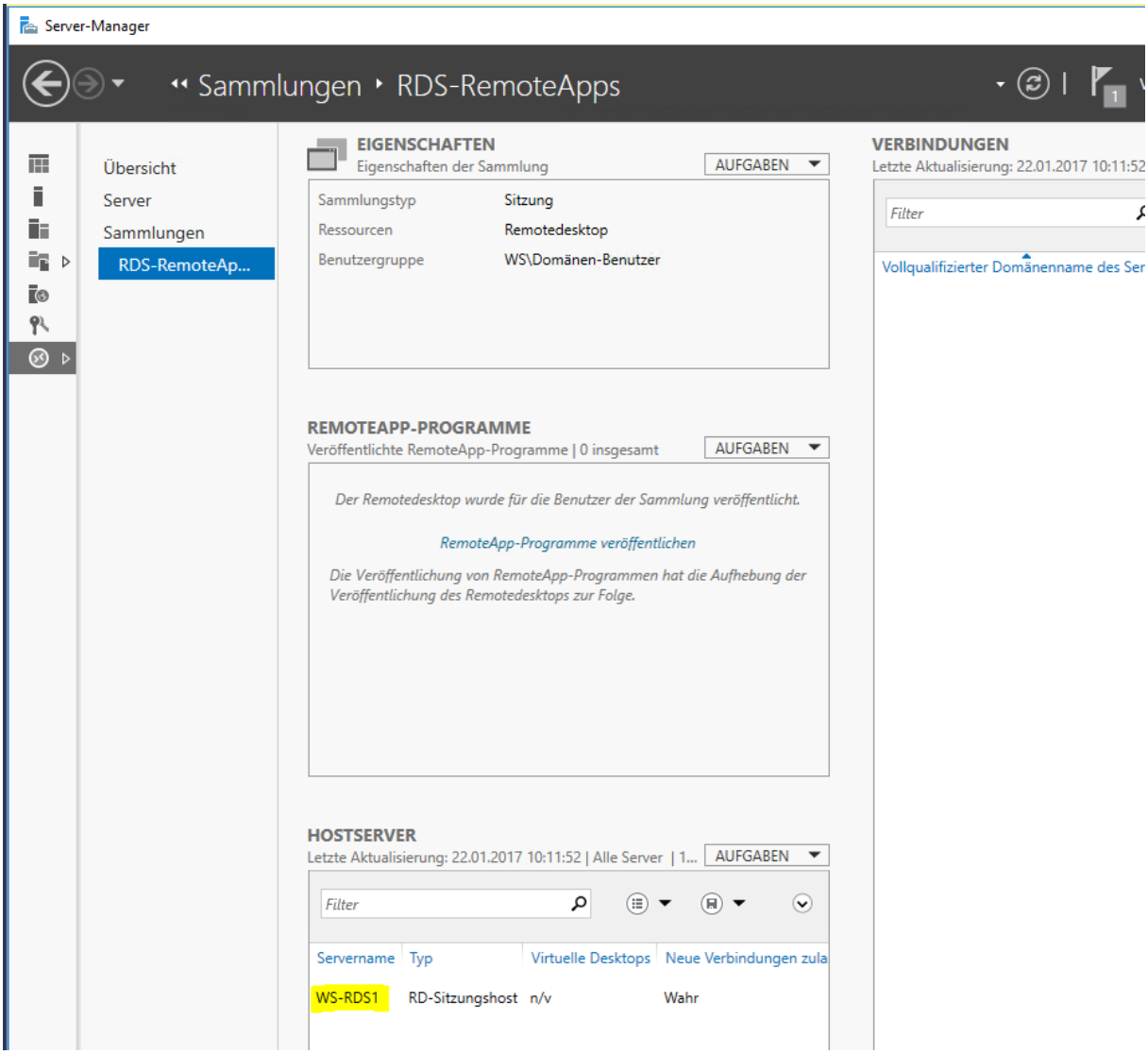
Den Benutzerprofildatenträger konfiguriere ich später:



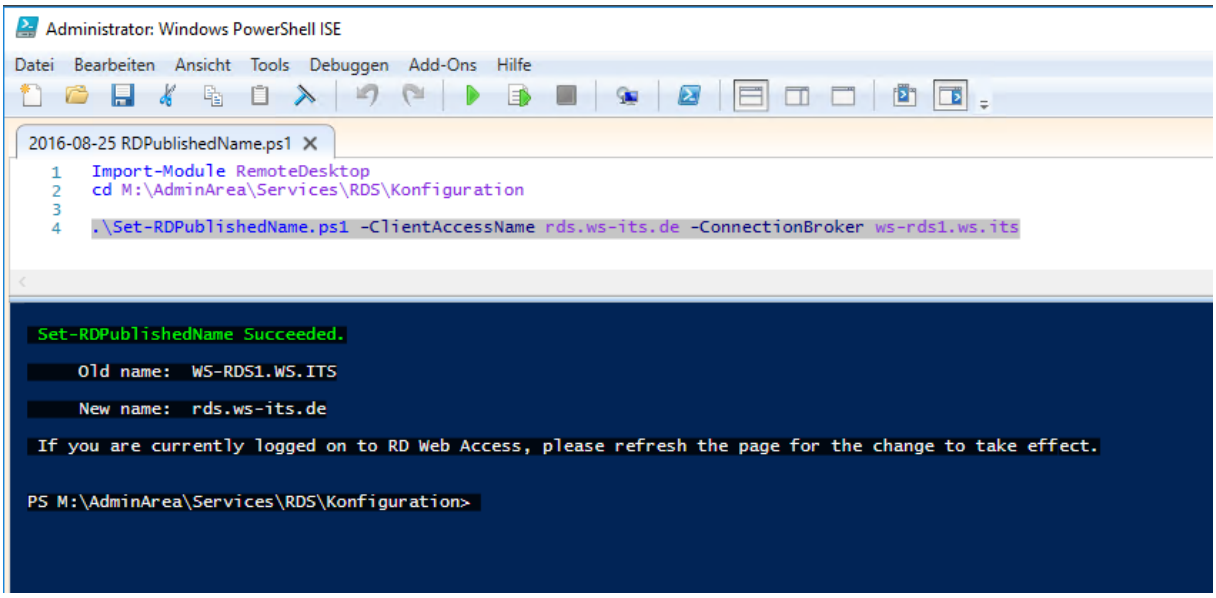
Beim Abschluss erhalte ich leider eine Fehlermeldung:



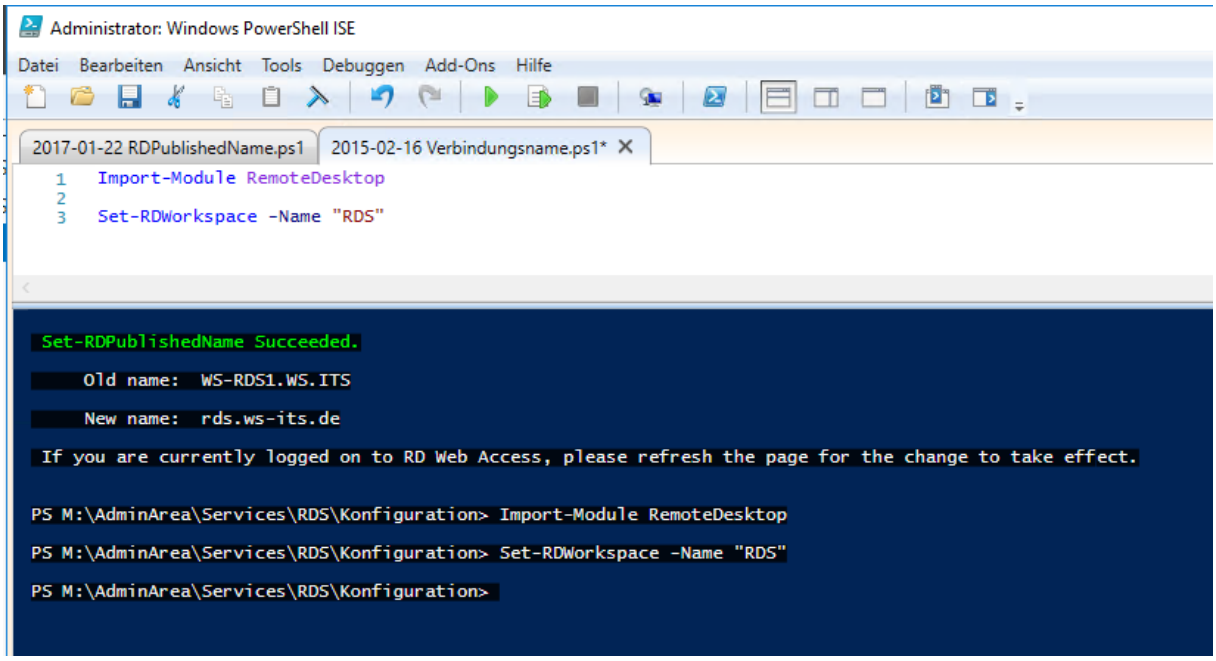
Diese ist nichtssagend. Ich prüfe, was der Servermanager anzeigt: Die Sammlung wurde erstellt. Ich entscheide mich, die Konfiguration fortzusetzen:



Der Server soll sich später beim Aufruf nicht mit seinem internen Namen, sondern mit dem externen Namen verwenden. Dafür gibt es in der PowerShell Script Gallery bei Microsoft ein Script, das den Zugriffsnamen ändert:

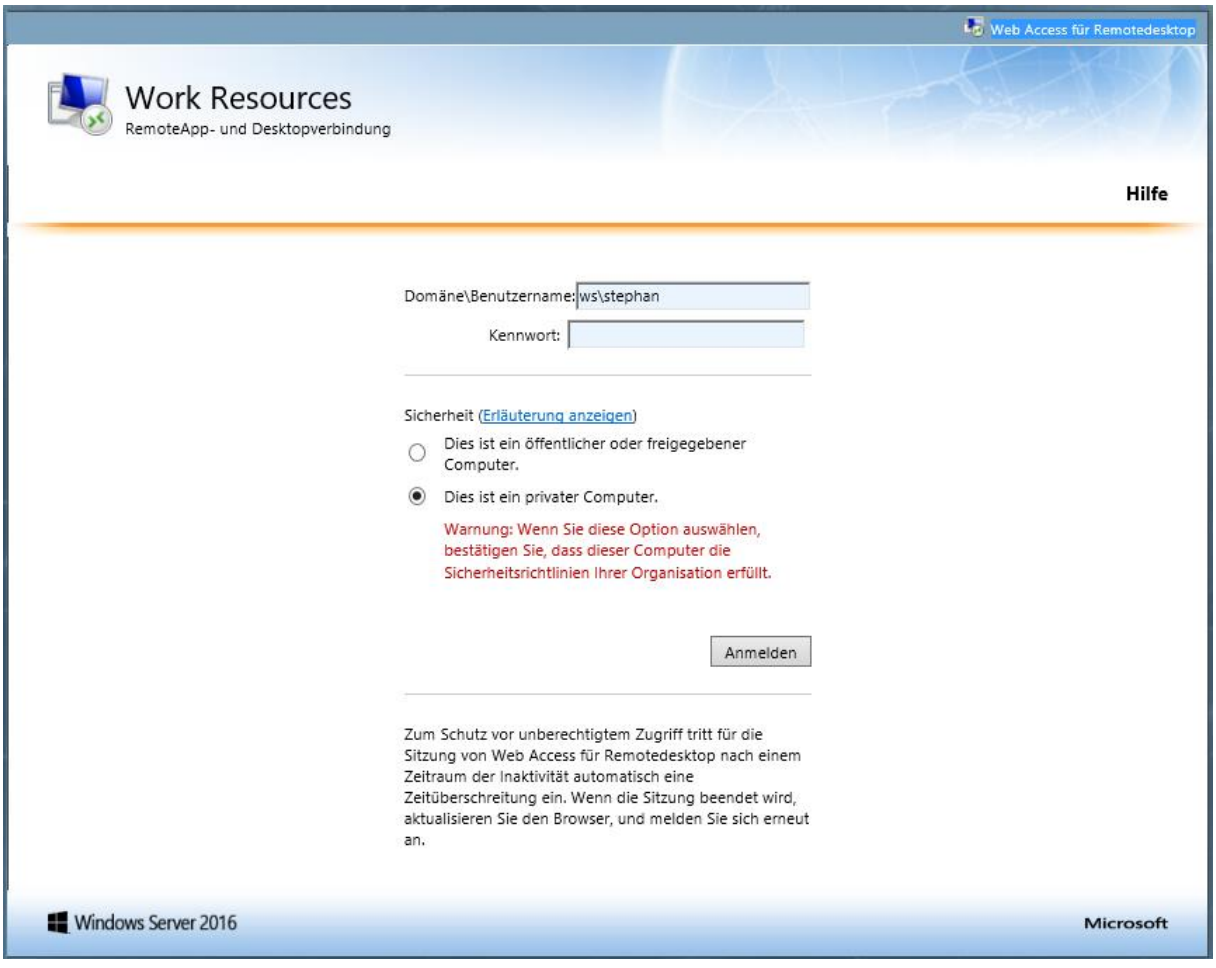


Die Sammlungen werden in den Clients in einem WorkSpace (Namensraum) dargestellt. Dieser ist mir per Default zu lang, daher ändere ich den Namen VOR der Veröffentlichung der Collection:

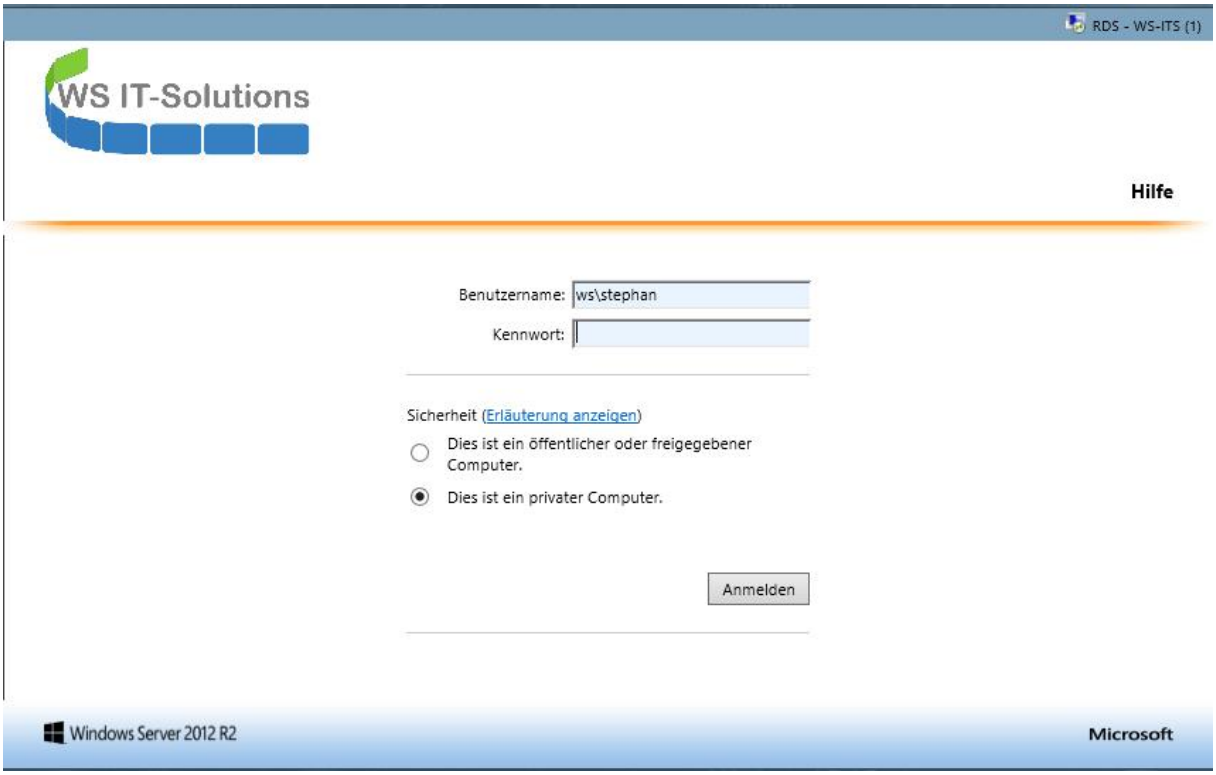


Konfiguration der RDS-Website

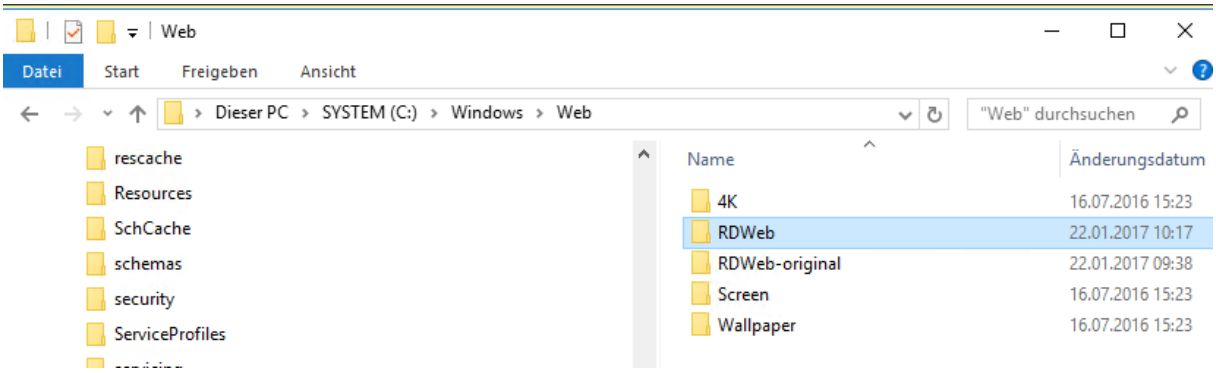
Das aktuelle Layout der RDS-Website hat Verbesserungsbedarf. Auf meinem alten RDS-Server hatte ich die Website bereits modifiziert. Ich tausche nun die Dateien unter dem IIS aus. Das ist vorher:



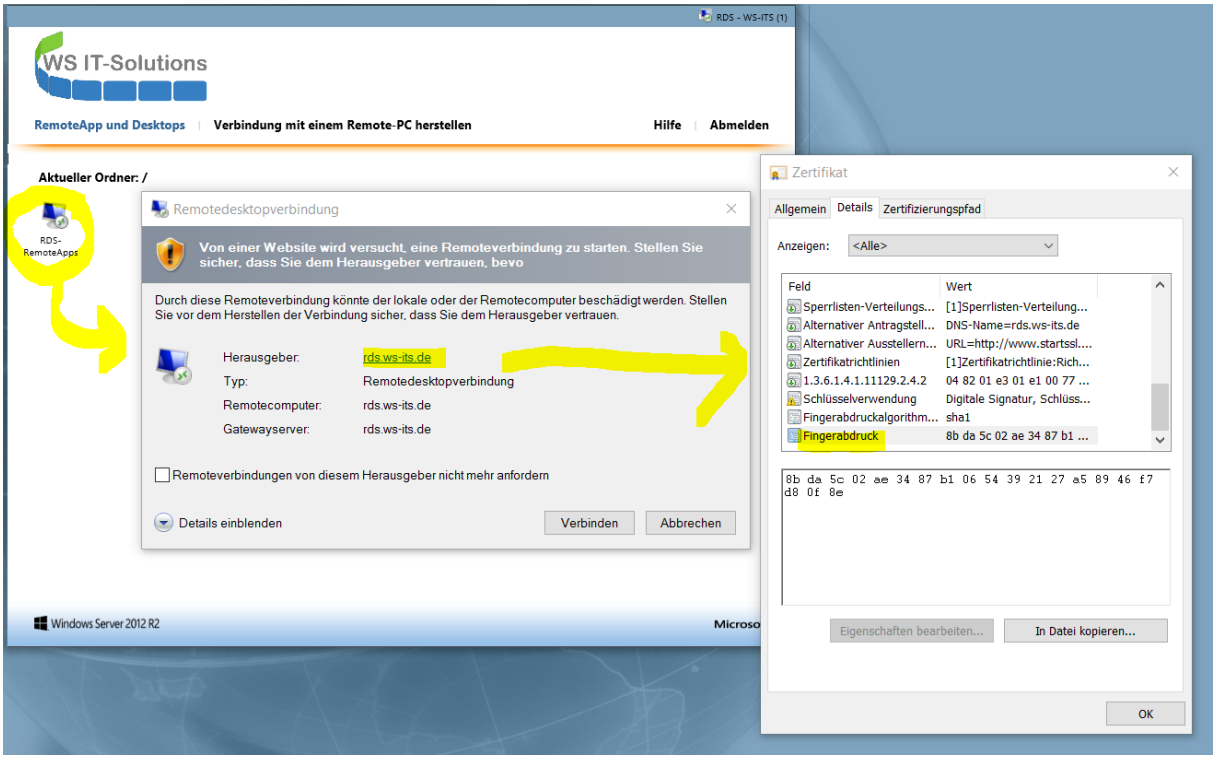
Und das ist nun die aktuelle Seite. Das Layout ist also kompatibel ☺:



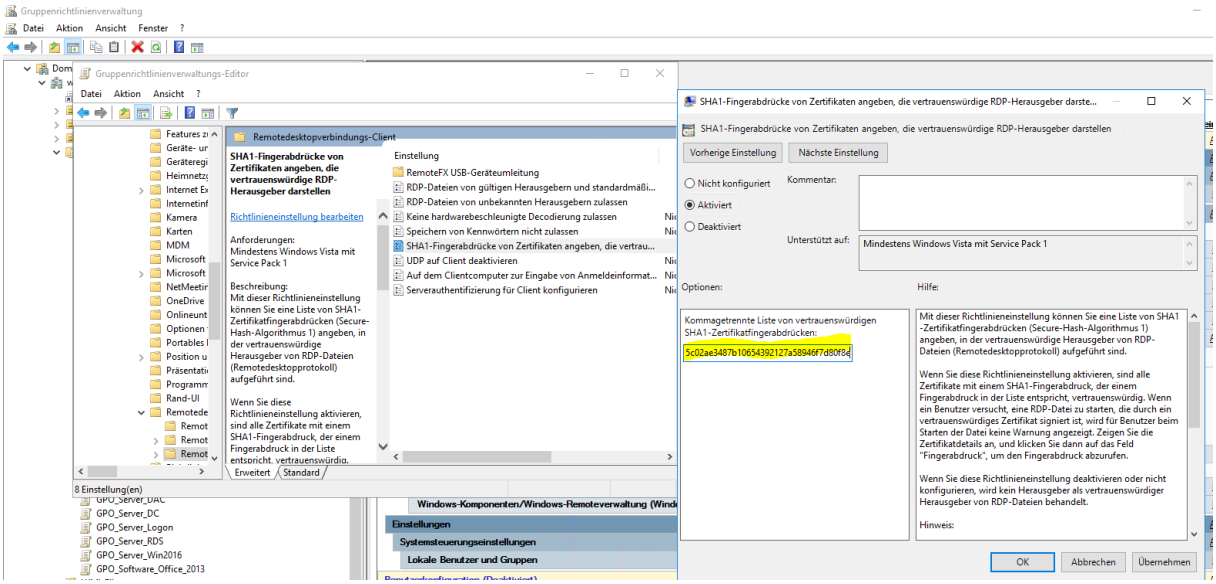
Hier liegt das Verzeichnis:



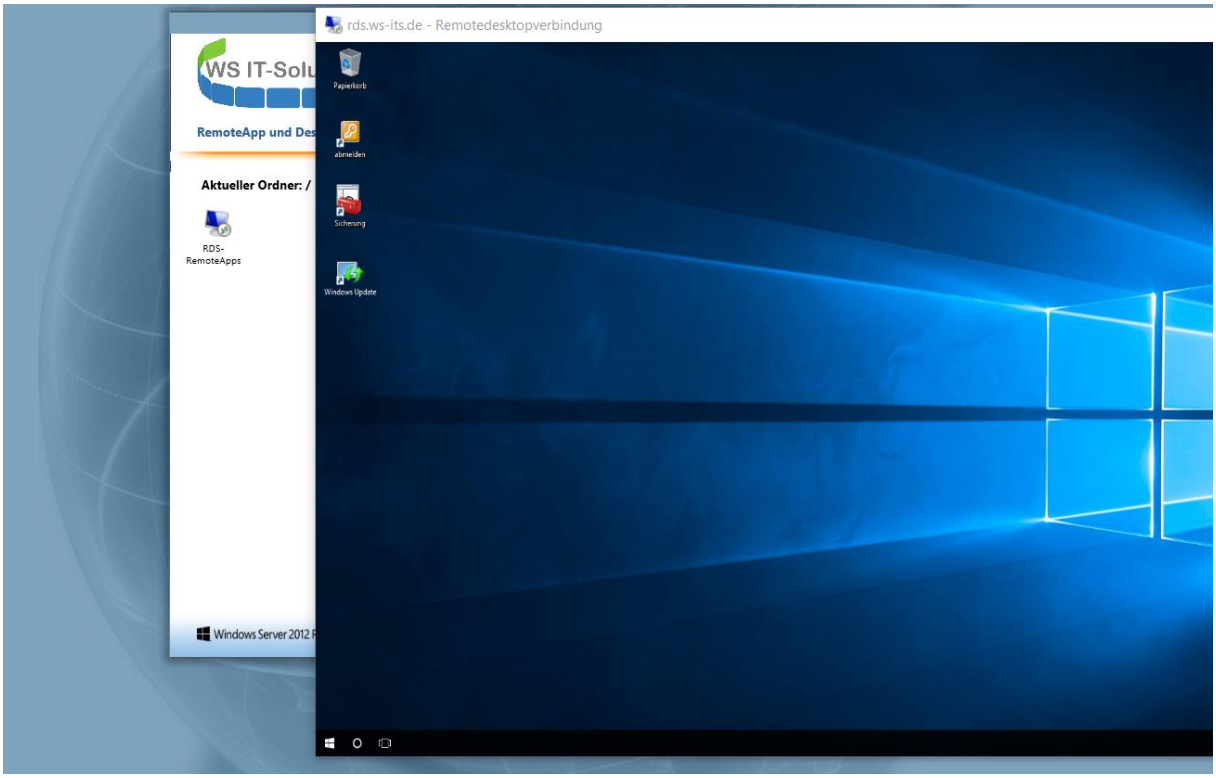
Ein Verbindungsaufbau zeigt aber, dass beim Start der RDP-Session eine Sicherheitsabfrage erscheint. Das Zertifikat ist zwar vertrauenswürdig, aber mein Client vertraut den rdp-Dateien noch nicht. Dies hatte ich bisher mit einer GPO erreicht, in der ich den Fingerabdruck des verwendeten Zertifikates als vertrauenswürdig deklariert habe. Vom neuen Zertifikat muss ich also nur den neuen Fingerabdruck mit in die GPO eintragen:



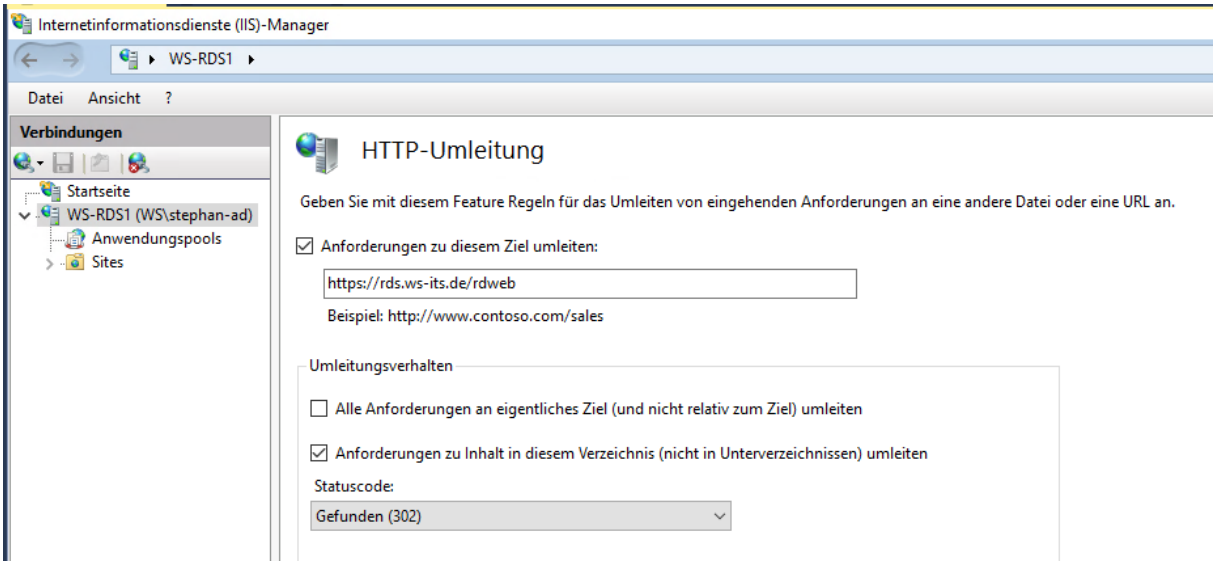
Das ist die GPO:



Ein gpupdate später baut mein Client die Verbindung ohne Meldungen auf:

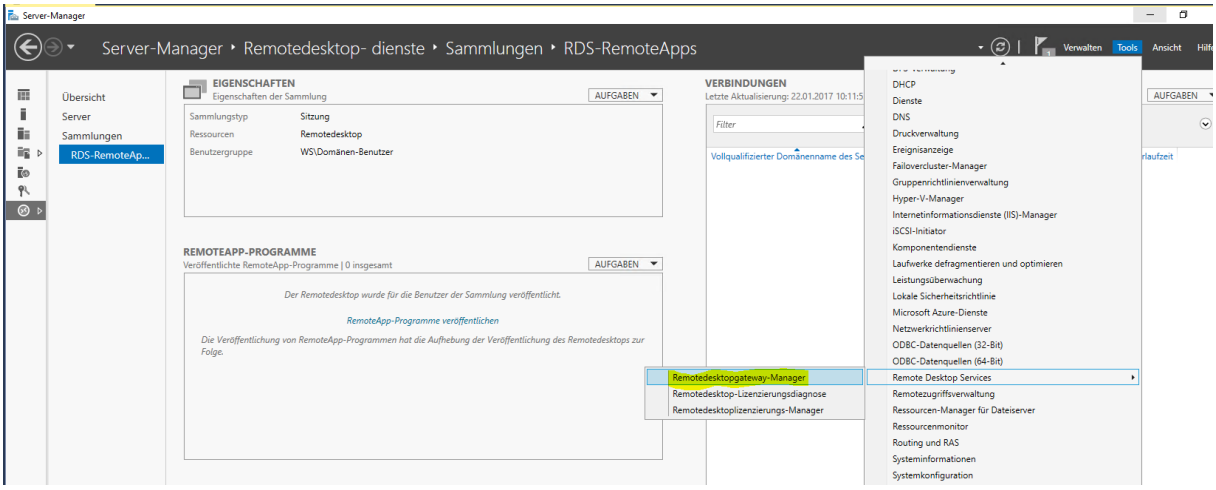


Nun noch etwas Bequemlichkeit: der Aufruf des Webportals benötigt die Angabe des Namens vom virtuellen Verzeichnis rdweb – es ist der Aufruf https://rds.ws-its.de/rdweb notwendig. Mit einer http-Redirect-Anweisung kann ich dem Benutzer ermöglichen, nur https://rds.ws-its.de aufzurufen:

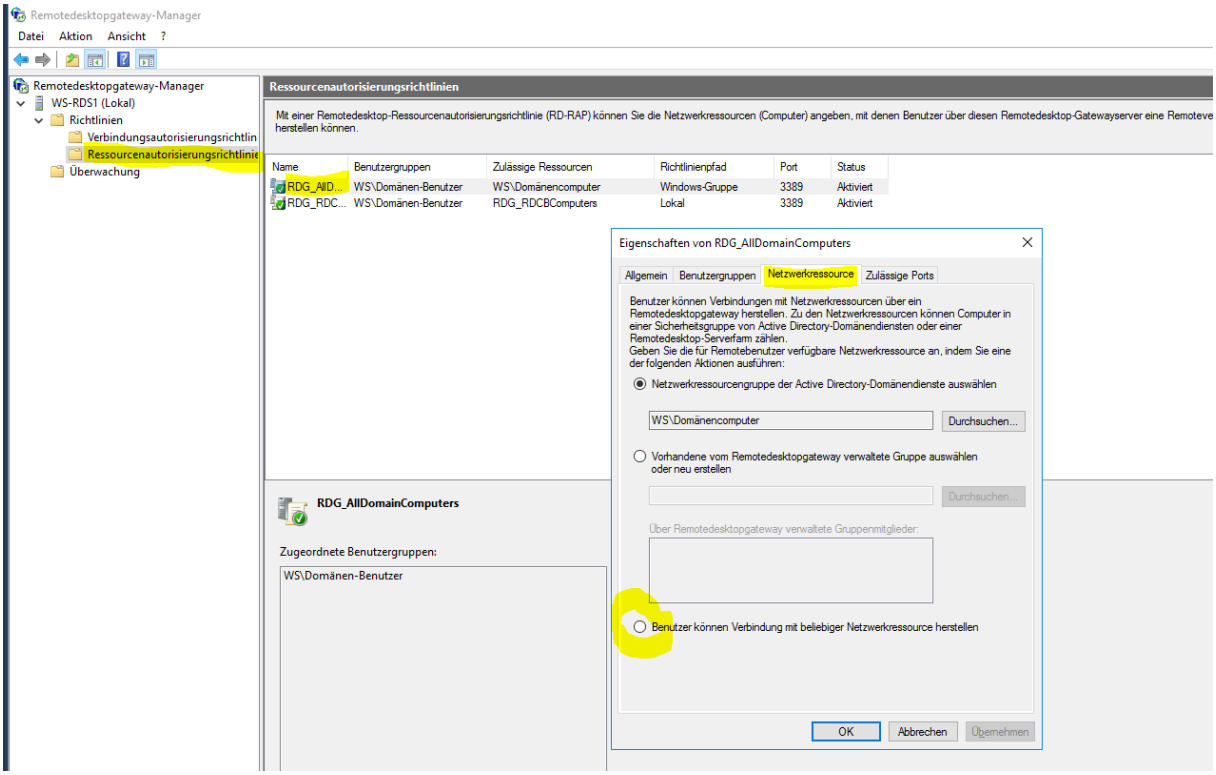


Konfiguration des RDS-Gateways

Das Gateway hat eine eigene Management-Konsole. Auch diese ist über die Servermanager-Tools erreichbar:

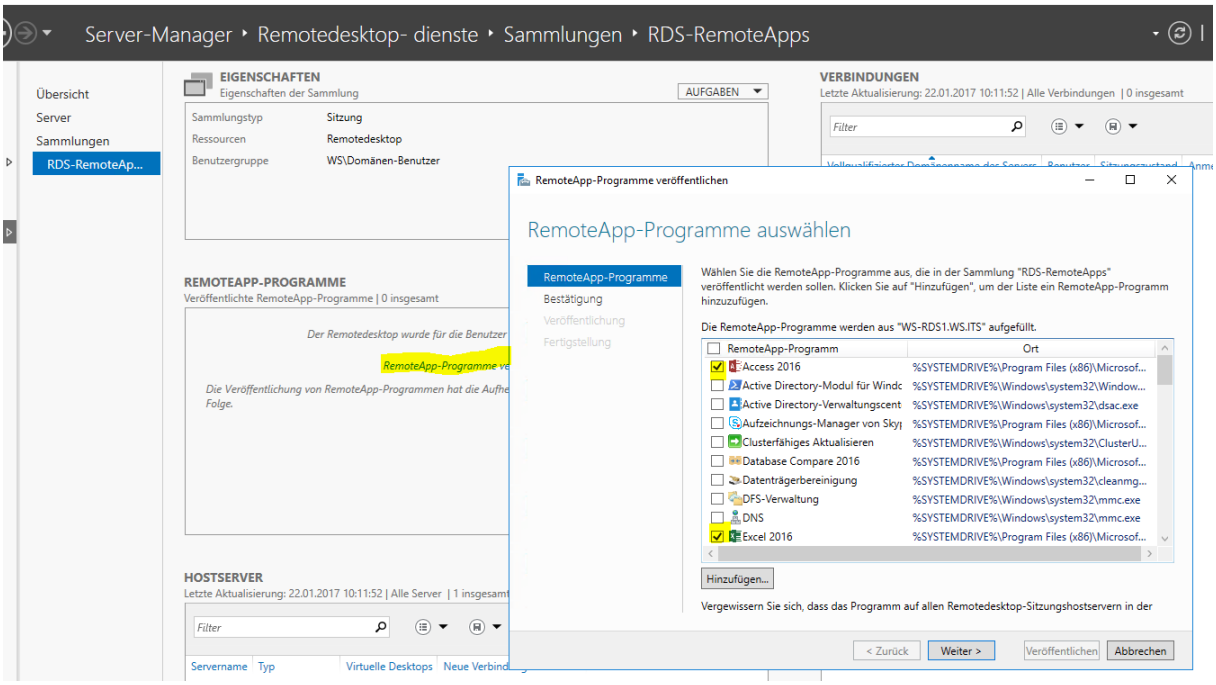


Hier werden ggf. Anpassungen bei den Autorisierungsrichtlinien notwendig, damit Benutzer eine RDP-Verbindung von außen über https aufbauen können:



Konfiguration der RemoteApps

Jetzt habe ich erfolgreich eine Vollsitzung erstellt. Ich möchte aber nur bestimmte Anwendungen veröffentlichen. Dafür muss ich nun in der SitzungsSammlung einzelne RemoteApps veröffentlichen. Die erforderlichen Setup habe ich bereits ausgeführt:

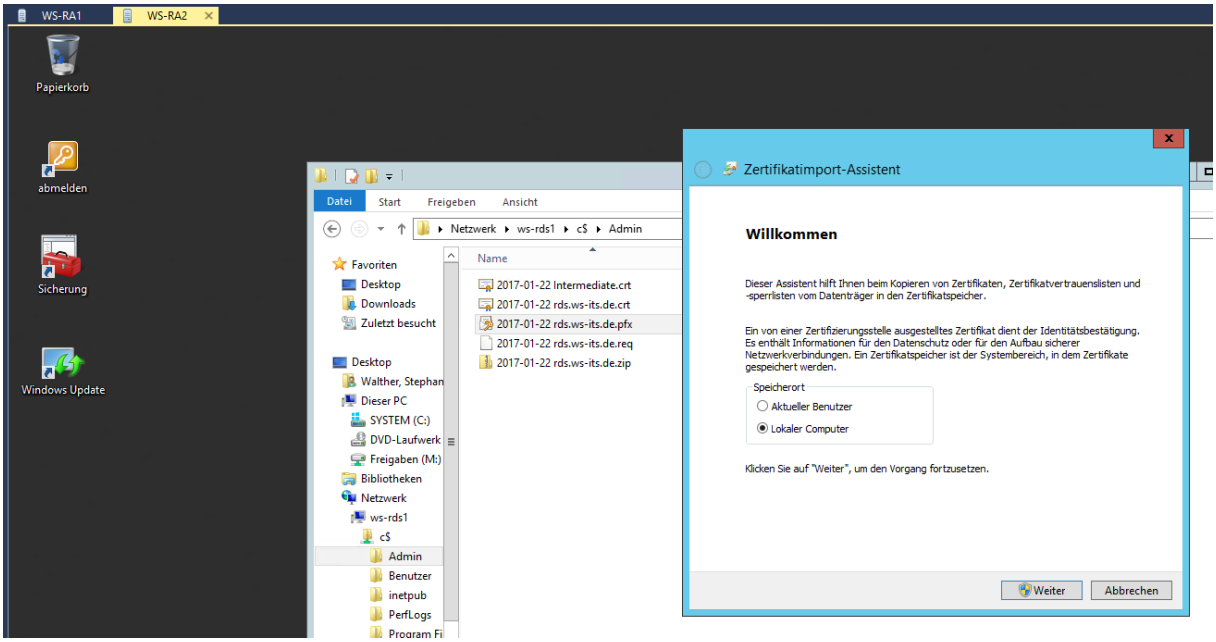


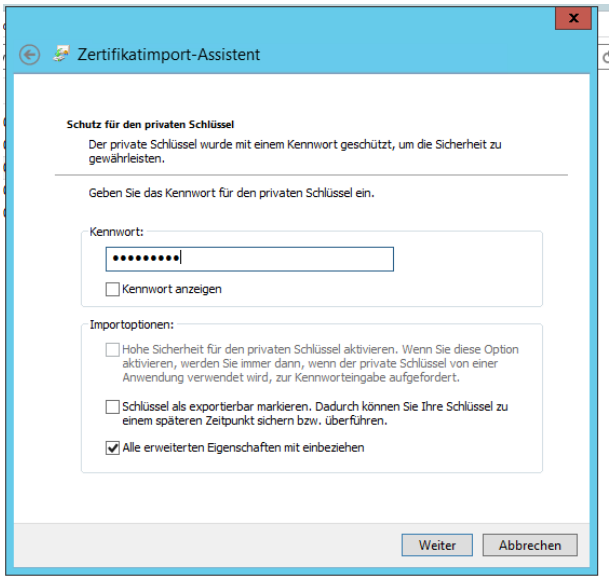
Konfiguration des Web Application Proxies

In meiner Umgebung ist der RDS-Gateway und das RDS-Webportal nicht direkt von außen erreichbar. Dazwischen steht unter Anderem ein Windows Server 2012 R2 Web Application Proxy Cluster. Dieser Cluster besteht aus 2 Systemen, die von außen auf dem Port 443 erreichbar sind. Beide analysieren den eigentlichen Aufruf und erkennen die URL, welche der externe Client angesprochen hat. Je nach URL wird dann ein Sicherheitszertifikat zur Serverauthentifizierung präsentiert. Dieses entspricht im Normalfall dem Zertifikat des Services, der hinter dem Cluster steht. Wenn alles geprüft wurde, leitet der WAP-Cluster die Anfrage an die interne Ressource weiter – in diesem Fall an den WS-RDS1.

Das Zertifikat wurde erneuert, da das alte vor wenigen Tagen (kontrolliert) abgelaufen ist. Ein externer Zugriff auf den RDS ist aktuell also wegen einem Zertifikatproblem nicht möglich.

Ich importiere zuerst das neue, externe Sicherheitszertifikat auf beiden RemoteAccess-Servern:





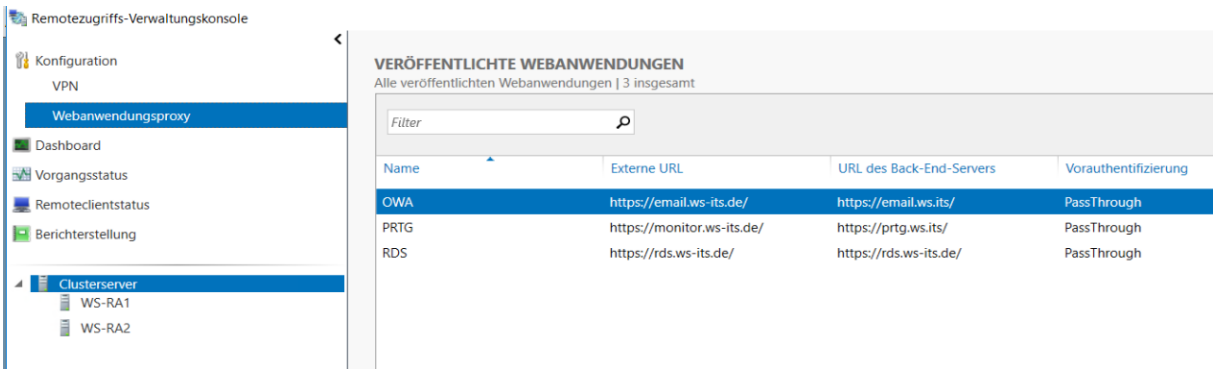
Den privaten Schlüssel markiere ich dabei als nicht exportierbar.

Jetzt kann ich über die PowerShell das neue Zertifikat an die bestehende Veröffentlichung meiner RDS-Infrastruktur binden. Dafür benötige ich den Fingerabdruck:

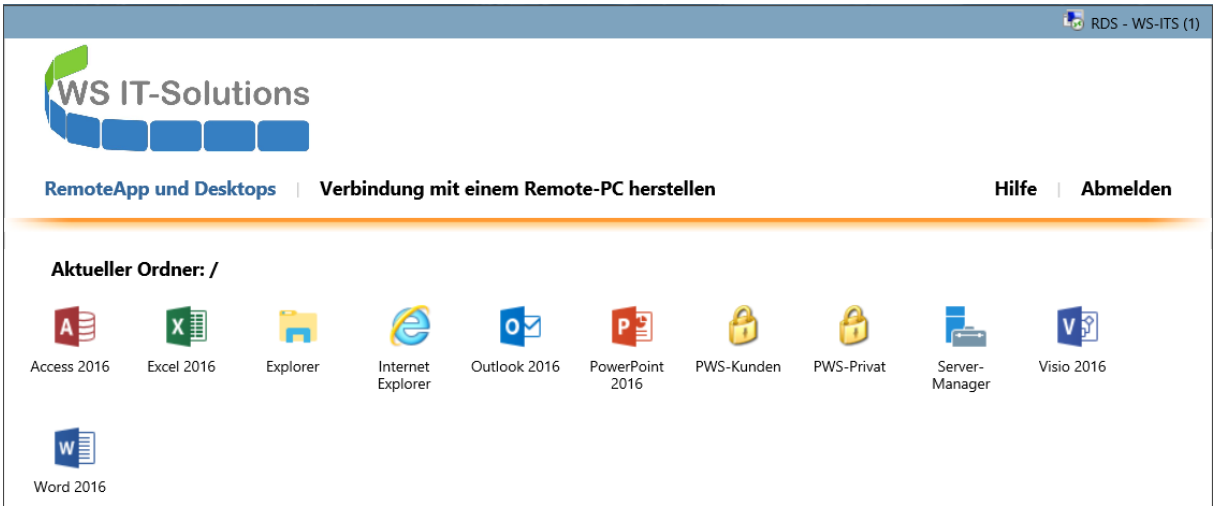
```
Unbenannt1.ps1 | 2017-01-22 Austausch RDS-Zertifikat.ps1

1  Get-ChildItem -Path Cert:\LocalMachine\My |
2      Where-Object {$_.subject -like '*rds*'} |
3          Format-Table -Property Thumbprint,Subject,NotBefore
4
5  get-WebApplicationProxyApplication -Name RDS |
6      Set-WebApplicationProxyApplication -ExternalCertificateThumbprint '8BDA5C02AE3487B10654392127A58946F7D80F8E'|
```

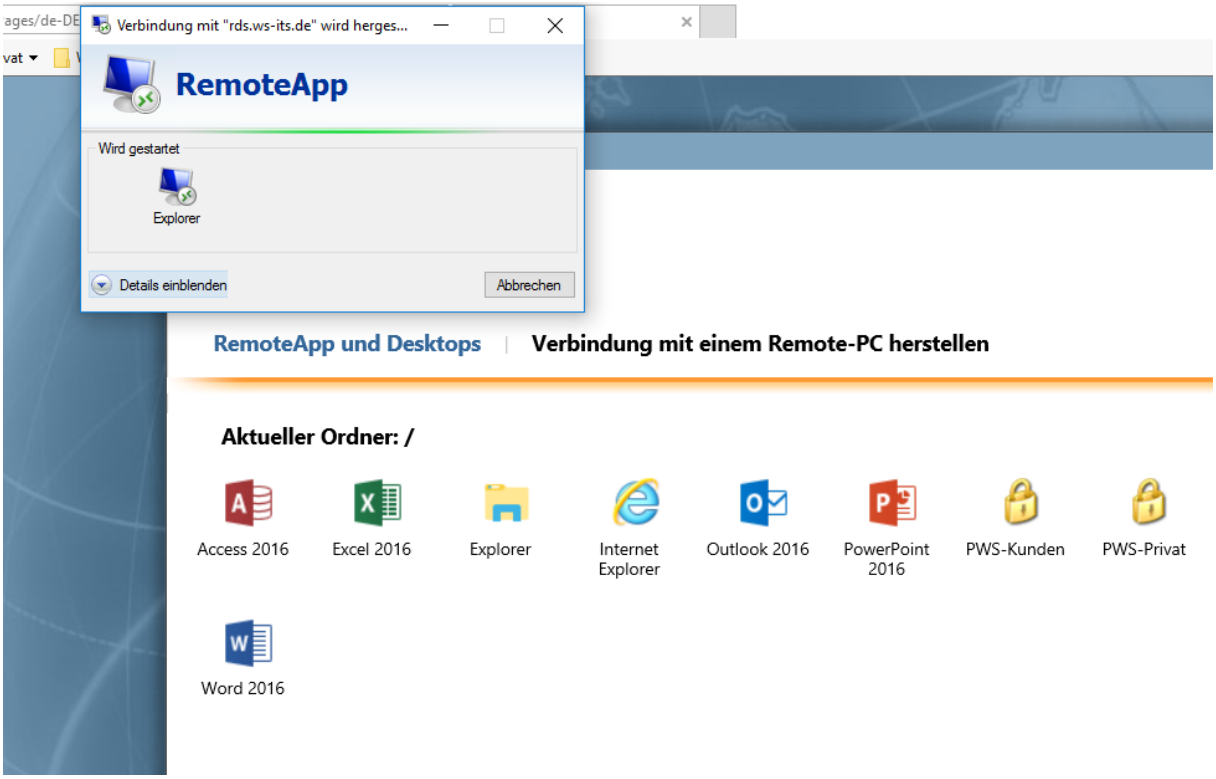
```
PS C:\Windows\system32> Get-ChildItem -Path Cert:\LocalMachine\My |
    Where-Object {$_.subject -like '*rds*'} |
        Format-Table -Property Thumbprint,Subject,NotBefore

Thumbprint                                Subject                                                 NotBefore
----------                                -------                                                 ---------
EAA63ABC7C2C6E1D544F75B0360469C55F399446  CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val... 19.10.2015 02:00:00
D60B05E28A7A1D322075444D56A88E0429921464  CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val... 19.07.2014 02:00:00
8BDA5C02AE3487B10654392127A58946F7D80F8E  CN=rds.ws-its.de, C=DE                                   22.01.2017 09:18:02
3405B0B9D51E7F1D2FBAD879EE1DC096C755F7EE  CN=rds.ws-its.de, OU=PositiveSSL Trial, OU=Domain Contr... 22.06.2014 02:00:00


PS C:\Windows\system32> get-WebApplicationProxyApplication -Name RDS |
    Set-WebApplicationProxyApplication -ExternalCertificateThumbprint '8BDA5C02AE3487B10654392127A58946F7D80F8E'

PS C:\Windows\system32>
```

In der Konsole für den RemoteZugriff ist die Änderung leider nicht möglich:



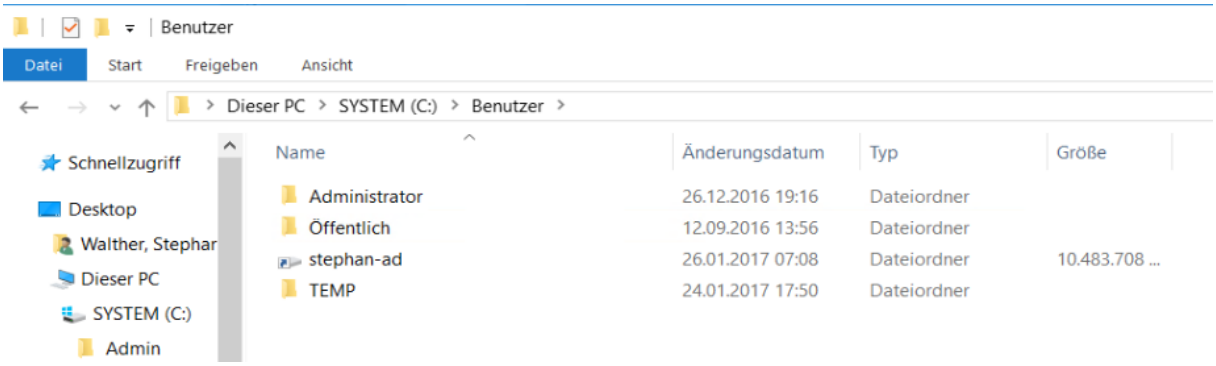
Ein Test von extern zeigt, dass nun sowohl das Web-Portal, als auch der Start der RemoteApps funktioniert:



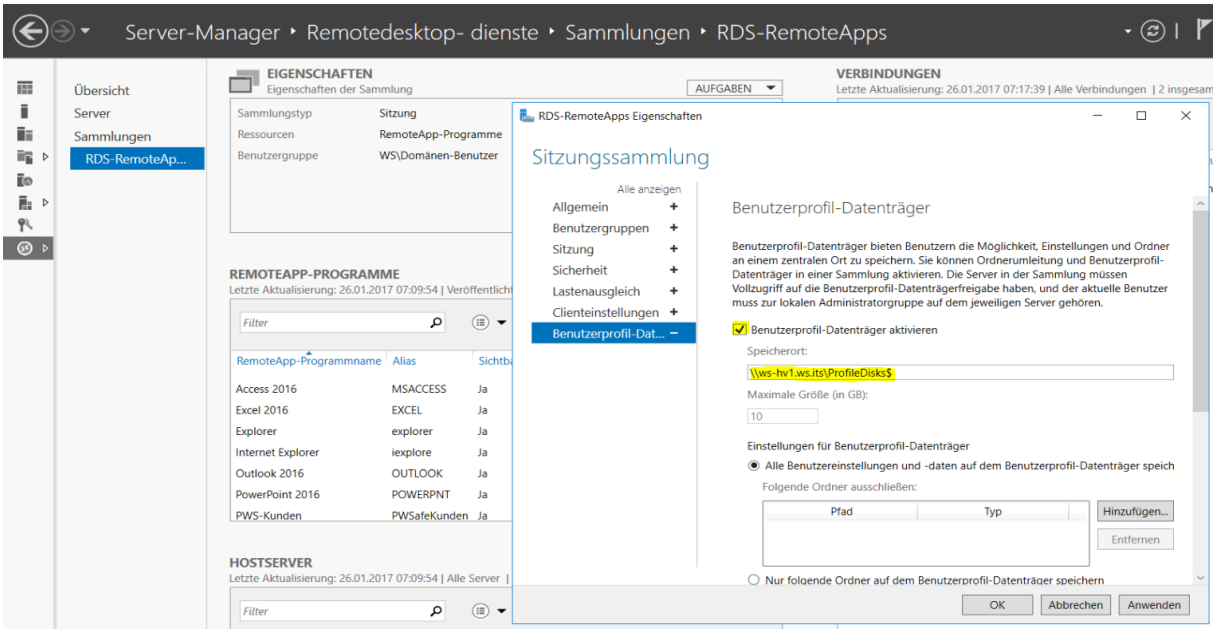


Konfiguration der Benutzerdatenträger

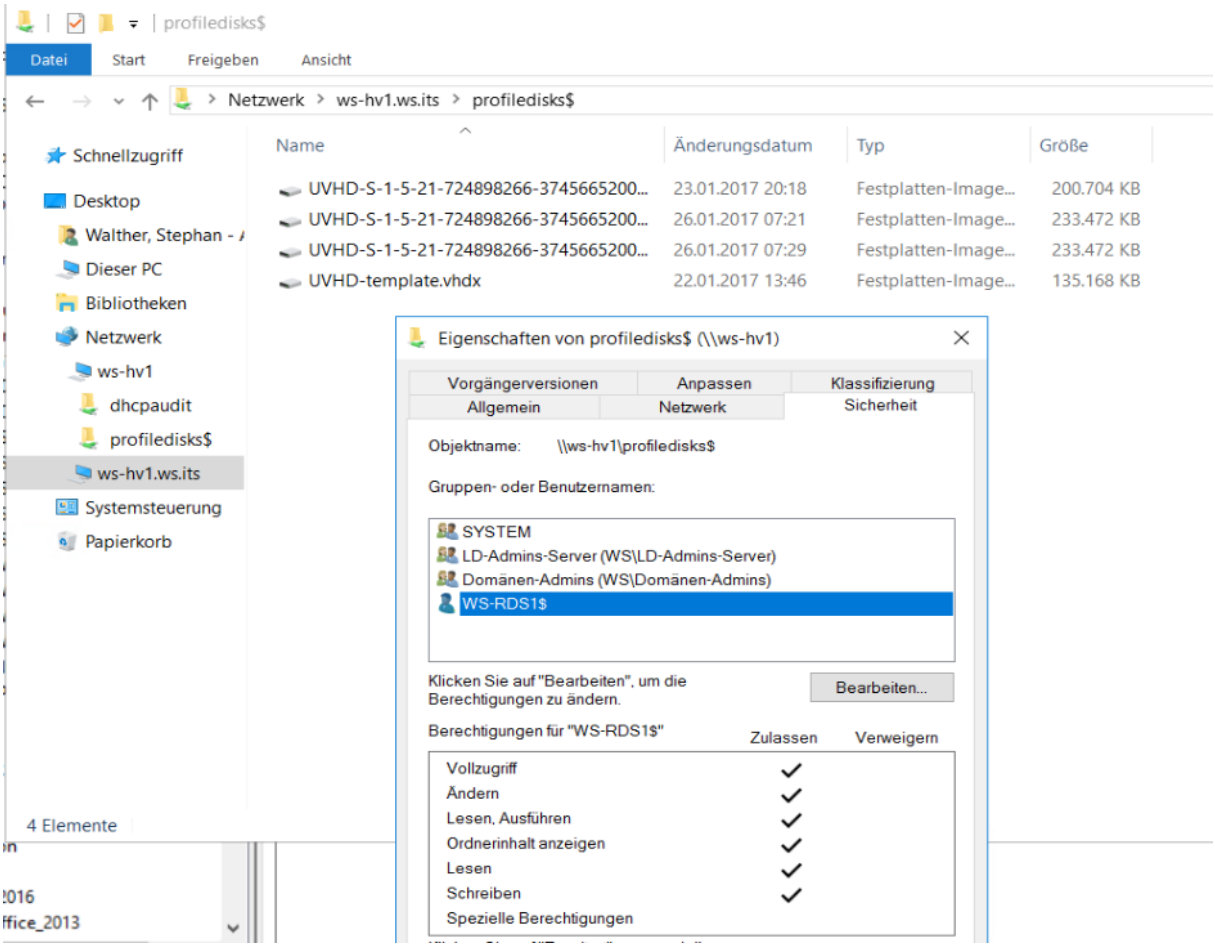
Der Benutzerdatenträger soll die Ladezeiten und den Speicherbedarf der Benutzerprofile minimieren, indem der Userstate in einer VHDX-Datei pro User gespeichert wird und diese bei der Anmeldung lokal als Benutzerprofilordner eingebunden wird:



Die Konfiguration kann in den Einstellungen der Sitzungssammlung vorgenommen werden:



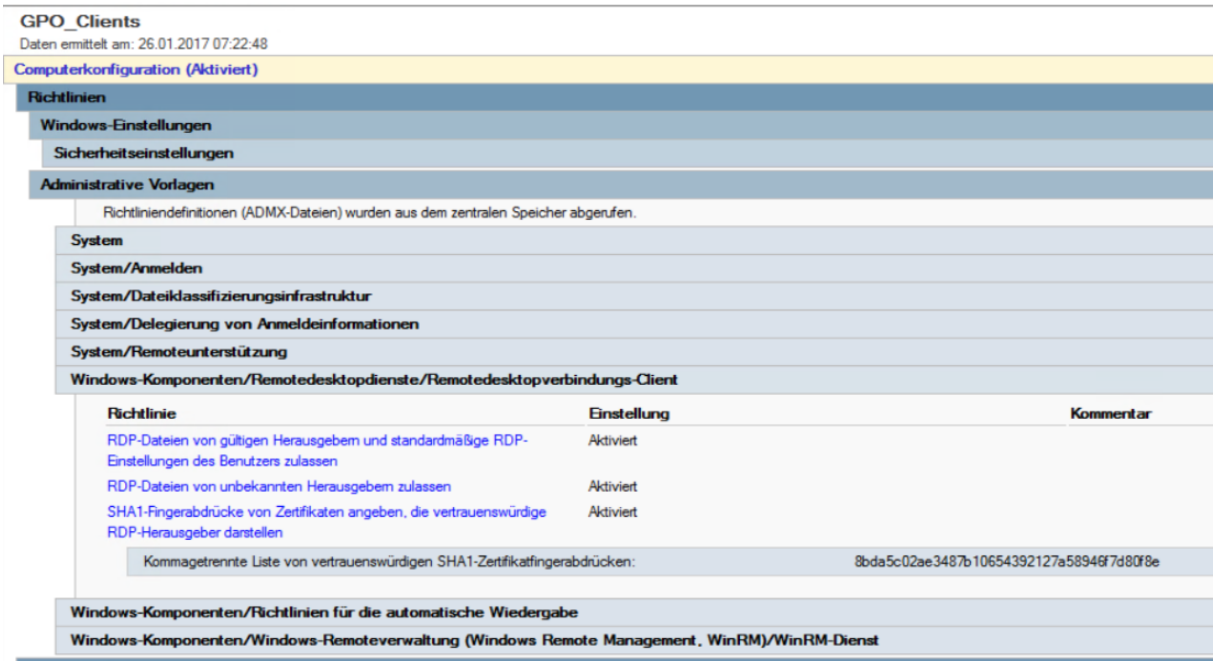
Die Freigabe, in der die VHDX-Dateien gespeichert werden, muss vorab erstellt werden. Die RDS-Server der Sammlung werden dabei vom Assistenten automatisch berechtigt, wenn der Administrator Vollzugriffsrechte hat:



Weitere GPOs:

Aus der Konfiguration der 2012 R2 RDS-Infrastruktur habe ich einige GPO übernommen. Abgesehen von den bisherigen Änderungen sind die Einstellungen mit Windows Server 2016 kompatibel.

Für jeden Client meiner Domain werden diese Einstellungen (für RDS) angewendet:



GPO_Clients
Daten ermittelt am: 26.01.2017 07:22:48

Computerkonfiguration (Aktiviert)

Richtlinien

Windows-Einstellungen

Sicherheitseinstellungen

Administrative Vorlagen

Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.

System

System/Anmelden

System/Dateiklassifizierungsinfrastruktur

System/Delegierung von Anmeldeinformationen

System/Remoteunterstützung

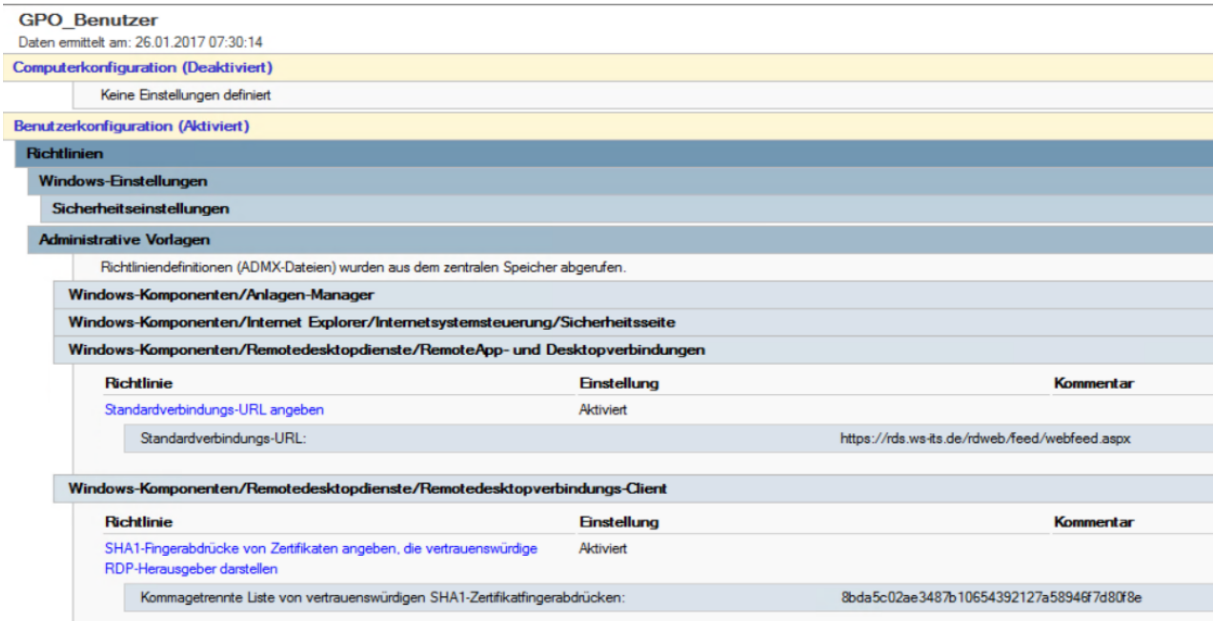
Windows-Komponenten/Remotedesktopdienste/Remotedesktopverbindungs-Client

Richtlinie	Einstellung	Kommentar
RDP-Dateien von gültigen Herausgebern und standardmäßige RDP-Einstellungen des Benutzers zulassen	Aktiviert	
RDP-Dateien von unbekannten Herausgebern zulassen	Aktiviert	
SHA1-Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen	Aktiviert	
Kommagetrennte Liste von vertrauenswürdigen SHA1-Zertifikatfingerabdrücken:	8bda5c02ae3487b10654392127a58946f7d80f8e	

Windows-Komponenten/Richtlinien für die automatische Wiedergabe

Windows-Komponenten/Windows-Remoteverwaltung (Windows Remote Management, WinRM)/WinRM-Dienst

Für die RDS-Benutzer werden folgende Einstellungen verwendet:



GPO_Benutzer
Daten ermittelt am: 26.01.2017 07:30:14

Computerkonfiguration (Deaktiviert)

Keine Einstellungen definiert

Benutzerkonfiguration (Aktiviert)

Richtlinien

Windows-Einstellungen

Sicherheitseinstellungen

Administrative Vorlagen

Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.

Windows-Komponenten/Anlagen-Manager

Windows-Komponenten/Internet Explorer/Internetsystemsteuerung/Sicherheitsseite

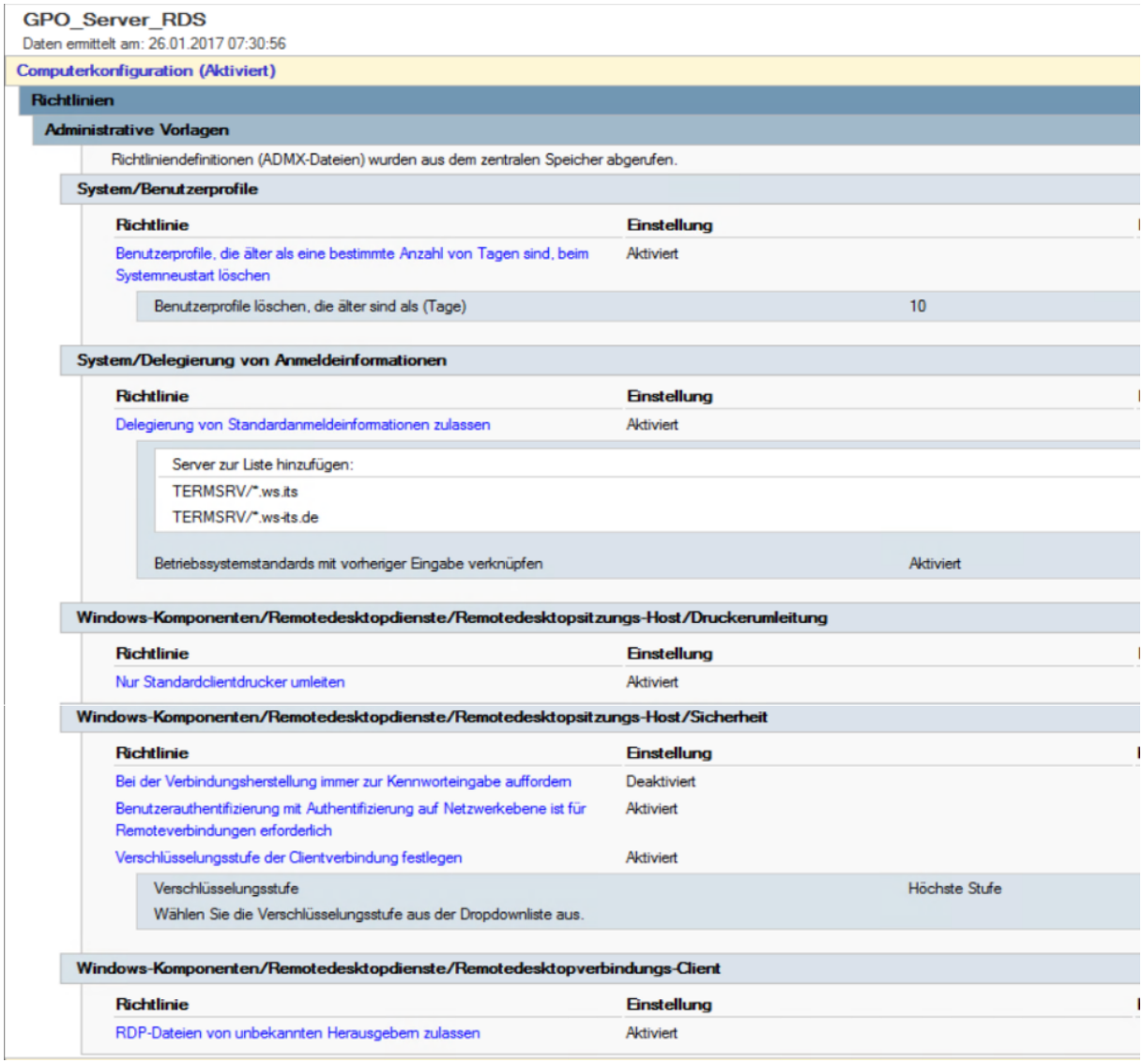
Windows-Komponenten/Remotedesktopdienste/RemoteApp- und Desktopverbindungen

Richtlinie	Einstellung	Kommentar
Standardverbindungs-URL angeben	Aktiviert	
Standardverbindungs-URL:	https://rds.ws-its.de/rdweb/feed/webfeed.aspx	

Windows-Komponenten/Remotedesktopdienste/Remotedesktopverbindungs-Client

Richtlinie	Einstellung	Kommentar
SHA1-Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen	Aktiviert	
Kommagetrennte Liste von vertrauenswürdigen SHA1-Zertifikatfingerabdrücken:	8bda5c02ae3487b10654392127a58946f7d80f8e	

Auch die (der) RDS-Server wird teilweise über GPO konfiguriert:



GPO_Server_RDS
Daten ermittelt am: 26.01.2017 07:30:56

Computerkonfiguration (Aktiviert)

Richtlinien

Administrative Vorlagen

Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.

System/Benutzerprofile

Richtlinie	Einstellung	
Benutzerprofile, die älter als eine bestimmte Anzahl von Tagen sind, beim Systemneustart löschen	Aktiviert	
Benutzerprofile löschen, die älter sind als (Tage)		10

System/Delegierung von Anmeldeinformationen

Richtlinie	Einstellung	
Delegierung von Standardanmeldeinformationen zulassen	Aktiviert	
Server zur Liste hinzufügen: TERMSRV/*.ws.its TERMSRV/*.ws-ts.de		
Betriebssystemstandards mit vorheriger Eingabe verknüpfen		Aktiviert

Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Druckerumleitung

Richtlinie	Einstellung
Nur Standardclientdrucker umleiten	Aktiviert

Windows-Komponenten/Remotedesktopdienste/Remotedesktopsitzungs-Host/Sicherheit

Richtlinie	Einstellung	
Bei der Verbindungsherstellung immer zur Kennworteingabe auffordern	Deaktiviert	
Benutzerauthentifizierung mit Authentifizierung auf Netzwerkebene ist für Remoteverbindungen erforderlich	Aktiviert	
Verschlüsselungsstufe der Clientverbindung festlegen	Aktiviert	
Verschlüsselungsstufe Wählen Sie die Verschlüsselungsstufe aus der Dropdownliste aus.		Höchste Stufe

Windows-Komponenten/Remotedesktopdienste/Remotedesktopverbindungs-Client

Richtlinie	Einstellung
RDP-Dateien von unbekannten Herausgebern zulassen	Aktiviert

Absicherung der RDS-Infrastruktur

Die Website und der Gateway sind über meine Firewall und den Web-Application-Proxy von extern erreichbar. Daher müssen einige lokale Sicherheitsvorkehrungen getroffen werden. Zu diesen zählen:

Sicherheitsebene	Erreicht durch
Patchmanagement	Automatisch durch WSUS mit GPO
AntiVirus	Automatisch durch Windows Defender (in 2016 m
Isolated User Mode / Secure Kernel / Virtualization Bases Security	Der Device Guard (neues Feature in 2016) ist durch eine GPO aktiv
Anwendungsisolation	Applocker-Regeln werden durch eine GPO angewendet
Windows Firewall	Aktiv durch GPO gesteuert
Deaktivierung unsicherer Cipher und Webserver-Protokolle	Ist in 2016 Server Standard!

Ich war überrascht, das Windows Server 2016 von außen betrachtet per default abgesichert war:

- es werden keine alten Webserver-Protokolle (SSLv1 bis SSLv3) verwendet
- TLS ist in der Version 1.2 aktiv
- Der unsichere Diffie-Hellman Key-Exchange ist nicht vorhanden
- Alle RC-Cipher sind deaktiviert

QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > rds.ws-its.de

SSL Report: rds.ws-its.de (87.138.129.242)

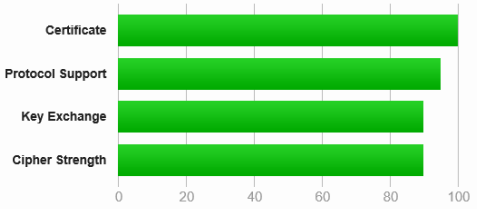
Assessed on: Thu, 26 Jan 2017 06:36:16 UTC | Hide | Clear cache

Scan Another »

Summary

Overall Rating

A



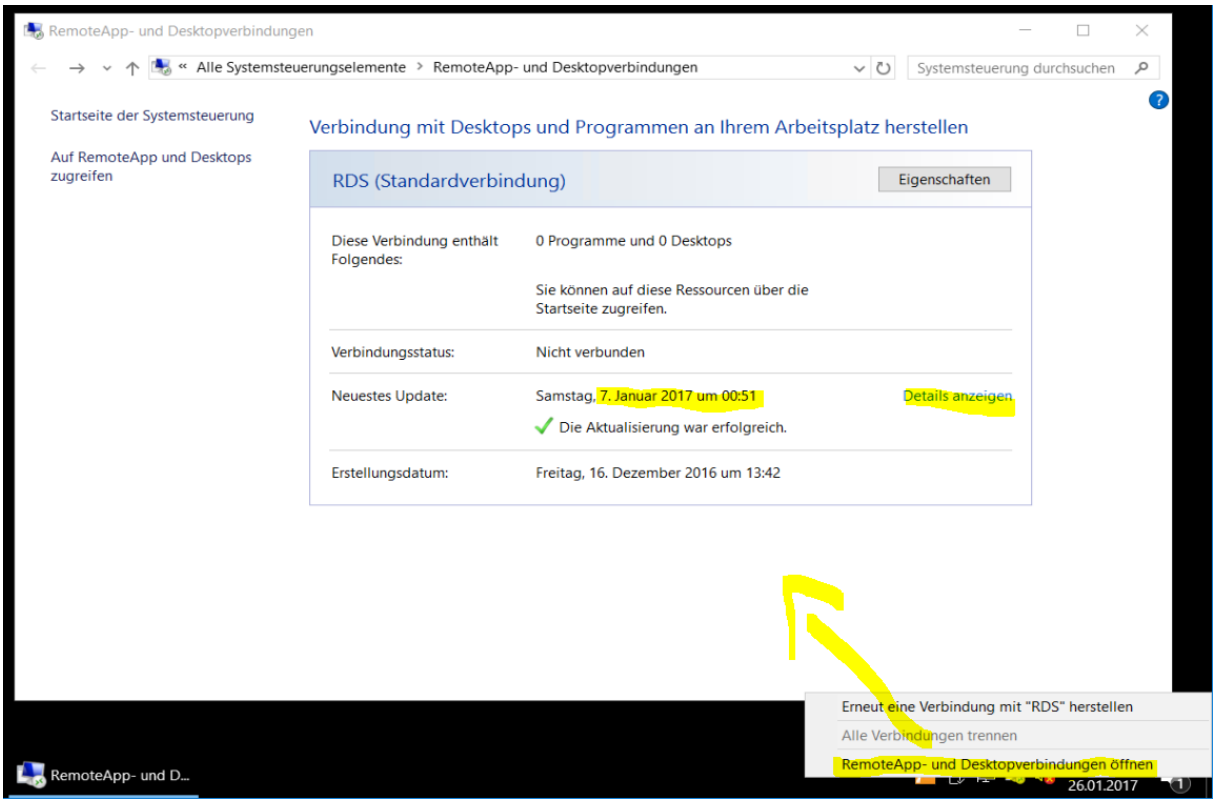
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

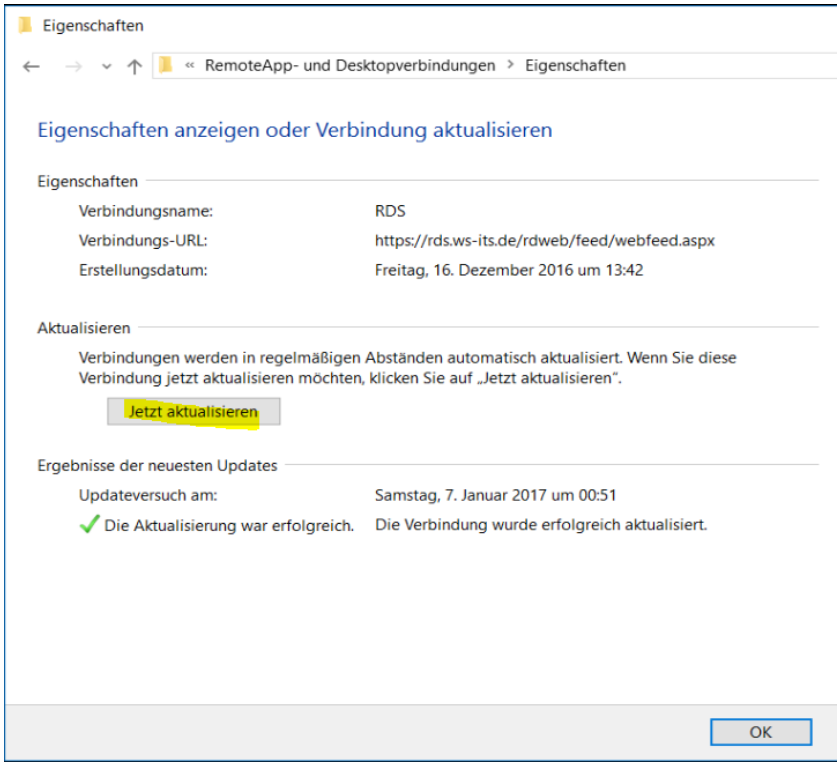
This site works only in browsers with SNI support.

Clientanbindung

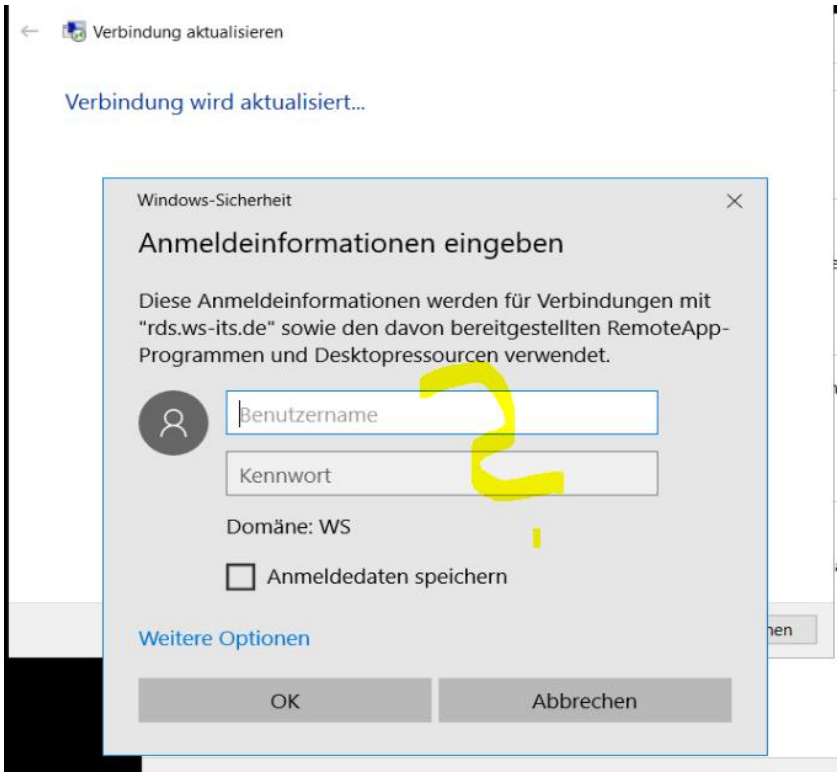
Die Benutzer werden über eine GPO angewiesen, die verfügbaren RemoteApps und Verbindungen automatisch zu erkennen. Diese Einstellung war bereits unter Windows Server 2012 R2 aktiv konfiguriert.

Leider aktualisiert sich der Client nicht mehr automatisch. Daher muss ich bei jedem Client nachhelfen:





Dabei erscheint ein Anmeldefenster. Dieses bestätige ich ohne Speicherung der Anmeldeinformationen:



Danach aktualisiert sich das System automatisch. ☺