

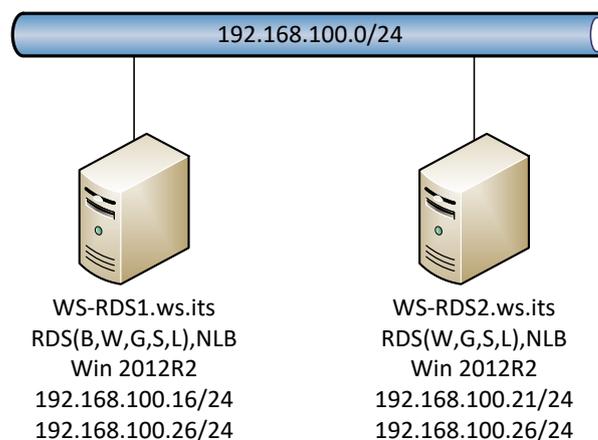
Inhalt

1.	Szenario.....	1
	IST-Zustand.....	1
	Soll-Zustand	2
	Migrationsweg.....	2
2.	Vorbereitung der Migration	2
	Verschieben aller Lizenzen von WS-RDS1 auf WS-RDS2	2
	Entfernen aller Sammlungen zum Deinstallieren der RDS-Rollen.....	5
	Entfernen aller nicht erforderlichen RDS-Rollen.....	6
	Abschalten des alten Servers WS-RDS1	13
3.	Aufbau der neuen RDS-Infrastruktur	14
	Inbetriebnahme und Vorbereitung des neuen Servers WS-RDS1	14
	Installation der neuen RDS-Infrastruktur	16
	Beschaffung eines Zertifikates für die neue RDS-Infrastruktur	22
	Konfiguration der RDS-Infrastruktur - allgemein.....	27
	Konfiguration der Lizenzierung – Migration der bestehenden CALs.....	30
	Konfiguration der SitzungsSammlung.....	38
	Konfiguration der RDS-Website	43
	Konfiguration des RDS-Gateways	46
	Konfiguration der RemoteApps.....	47
	Konfiguration des Web Application Proxies	48
	Konfiguration der Benutzerdatenträger	50
	Weitere GPOs:	51
	Absicherung der RDS-Infrastruktur.....	53
	Clientanbindung	54

1. Szenario

IST-Zustand

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



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, das 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 Skripte 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:

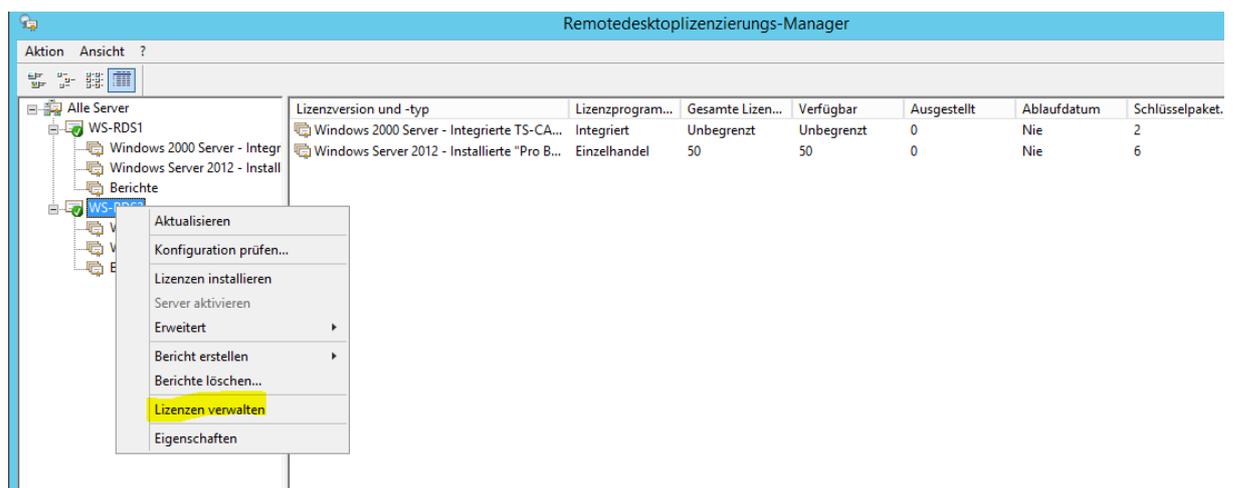
- WS-RDS2 man alle RDS-Rollen außer dem Lizenzserver deinstallieren
- Dann kann man die Lizenzen vom alten WS-RDS1 auf den alten WS-RDS2 übertragen,
- Nun kann WS-RDS1 komplett entfernt werden. Zu dieser Zeit existiert dann nur noch ein alter Lizenzserver mit allen Lizenzen
- Der neue Server wird ohne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

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:

Assistent zum Verwalten von Lizenzen ✕

Informationen zum Quelllizenzserver
Geben Sie die erforderlichen Informationen zum Quelllizenzserver an.

Name oder IP-Adresse des Quelllizenzservers:

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](#)

Assistent zum Verwalten von Lizenzen
✕

Lizenzprogramm
Wählen Sie das passende Lizenzprogramm aus.

Jeder Client, von dem eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder einem virtuellen Desktop in einer Microsoft Virtual Desktop Infrastructure hergestellt wird, muss eine gültige Lizenz haben. Wählen Sie das Lizenzprogramm aus, über das Sie die Lizenzen erworben haben.

Lizenzprogramm:

Beschreibung: Diese Lizenz wird in vordefinierten Mengen im Einzelhandel oder bei einem anderen Händler erworben. Diese Verpackung ist möglicherweise mit "Microsoft Windows Client License Pack" bezeichnet.

Format und Pfad: Die im Lizenzpaket enthaltene Lizenznummer ist erforderlich. Das Format für die Lizenznummer ist 5 Sätze à 5 alphanumerischen Zahlen.

Beispiel:

Stellen Sie sicher, dass die Lizenzinformationen dem Beispiel entsprechen, bevor Sie den Vorgang fortsetzen.

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

Assistent zum Verwalten von Lizenzen
✕

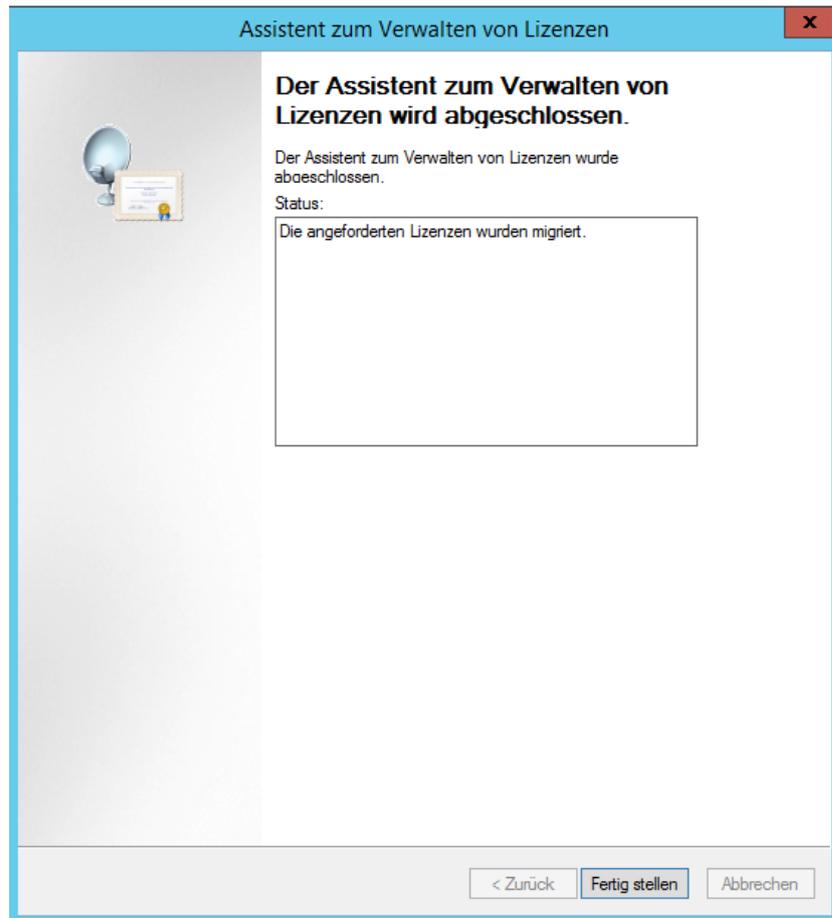
Lizenznummer
Geben Sie die Lizenznummer ein. Sie finden die Nummer in der Verpackung.

Geben Sie die Lizenznummer für jede Lizenz, die Sie erworben haben ein, und klicken Sie nach der Eingabe jeder Lizenznummer auf "Hinzufügen". Das Format für die Lizenznummer ist 5 Abschnitte à 5 alphanumerische Zahlen.

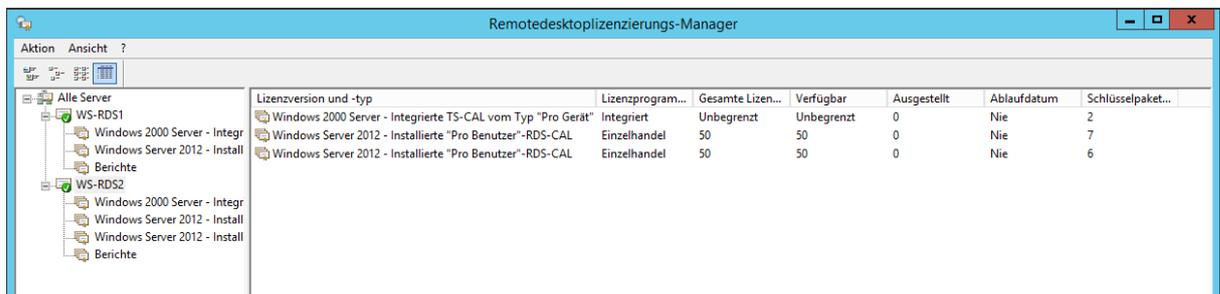
Lizenznummer:

Eingegebene Lizenznummern:

Lizenznummer	Status	Produkttyp
[REDACTED]	Ausstehend	Windows Server 2012

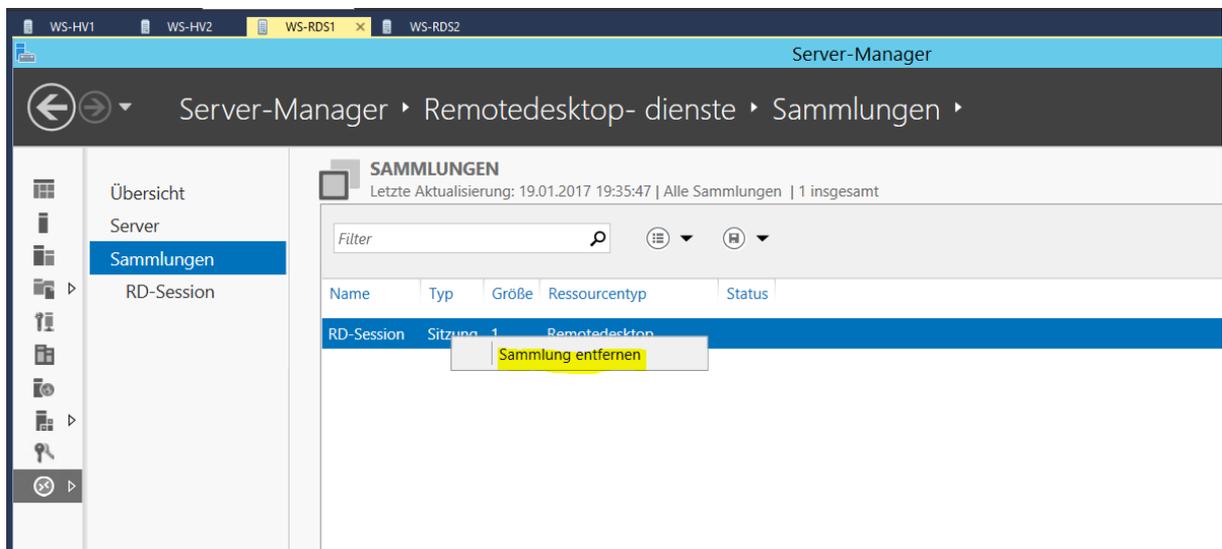
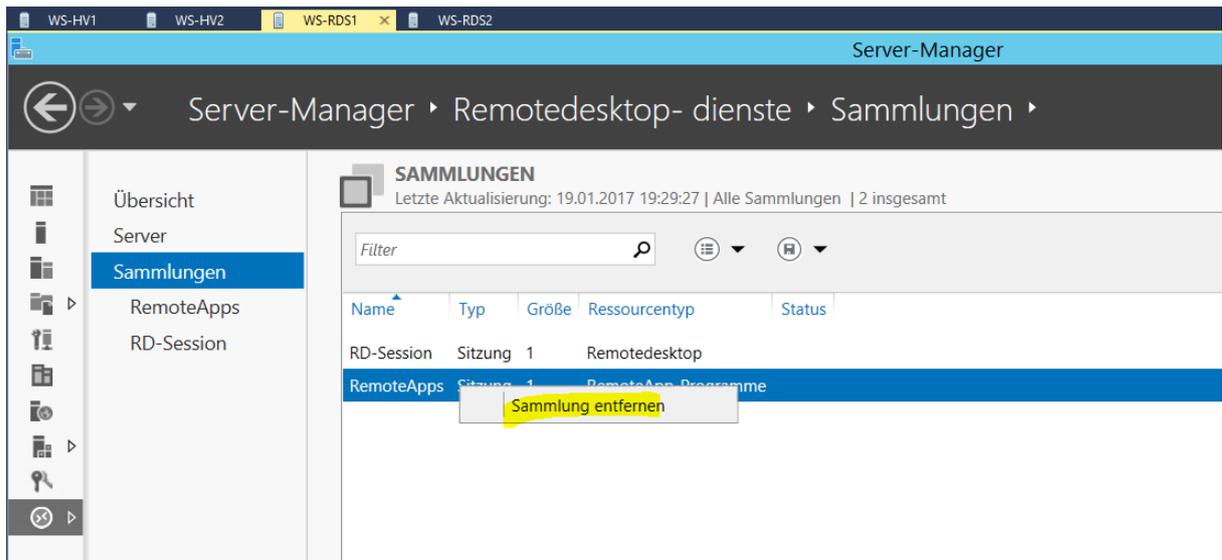


Das Ergebnis passt:



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 > Remotedesktop- dienste > Übersicht

BEREITSTELLUNGSÜBERSICHT
RD-Verbindungsbroker: WS-RDS1.ws.its

BEREITSTELLUNGSSERVER
Letzte Aktualisierung: 19.01.2017 19:29:27 | Alle RDS-Rollen...

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.

Name	IP-Adresse	Betrieb
WS-RDS1.WS.ITS		
WS-RDS2.ws.its		

2 Computer gefunden

Ausgewählt

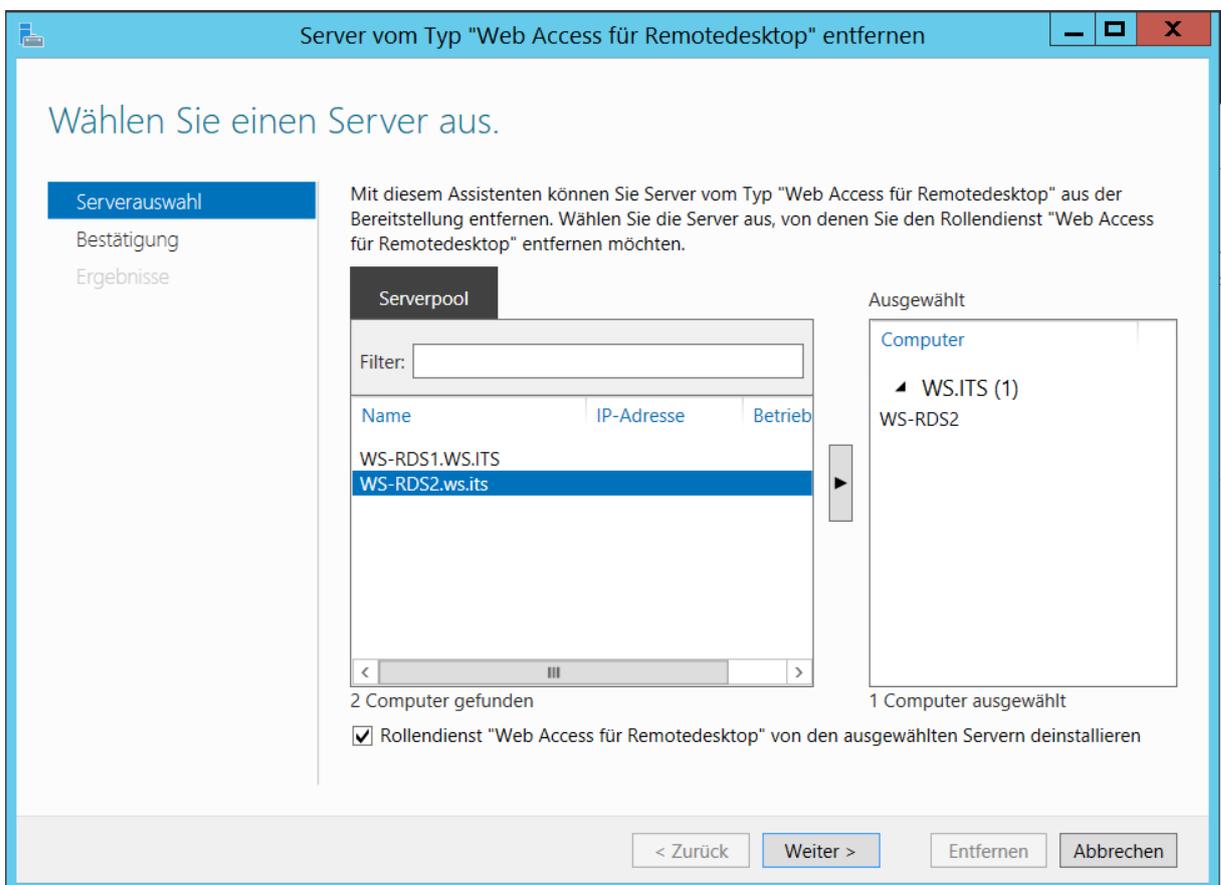
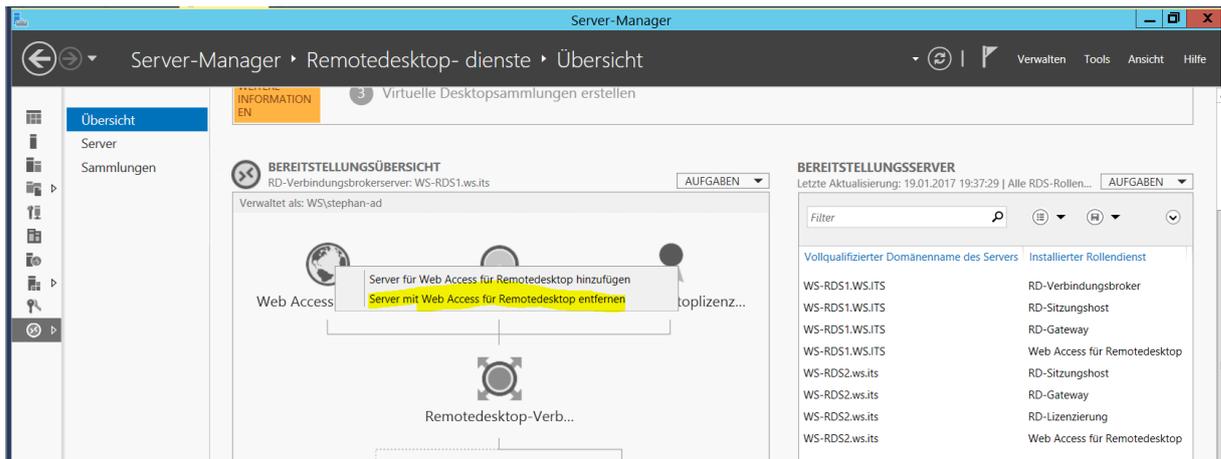
- Computer
 - WS.ITS (1)
 - WS-RDS1

1 Computer ausgewählt

Rollendienst "RD-Lizenzierung" von den ausgewählten Servern deinstallieren

< Zurück Weiter > Entfernen Abbrechen

Weiter geht es mit dem Webservice von WS-RDS2:



Server vom Typ "Web Access für Remotedesktop" entfernen

Wählen Sie einen Server aus.

Serverauswahl

Bestätigung
Ergebnisse

Mit diesem Assistenten können Sie Server vom Typ "Web Access für Remotedesktop" aus der Bereitstellung entfernen. Wählen Sie die Server aus, von denen Sie den Rollendienst "Web Access für Remotedesktop" entfernen möchten.

Serverpool

Filter:

Name	IP-Adresse	Betrieb
WS-RDS1.WS.ITS		
WS-RDS2.ws.its		

2 Computer gefunden

Rollendienst "Web Access für Remotedesktop" von den ausgewählten Servern deinstallieren

Ausgewählt

Computer

- WS.ITS (1)
 - WS-RDS2

1 Computer ausgewählt

< Zurück Weiter > Entfernen Abbrechen

Dieses Feature benötigt bei der Deinstallation einen Neustart:

Server vom Typ "Web Access für Remotedesktop" entfernen

Status anzeigen

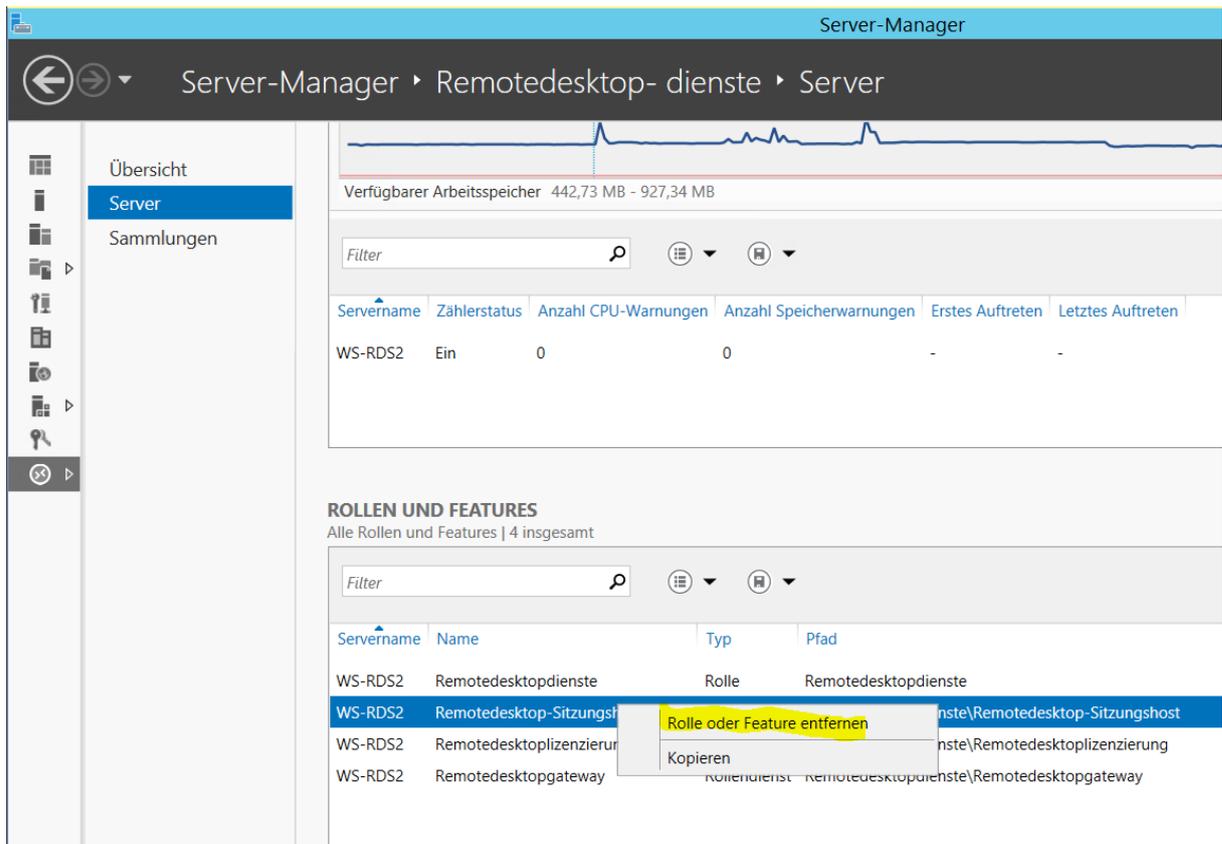
Serverauswahl
Bestätigung
Ergebnisse

Die folgenden Server werden entfernt:

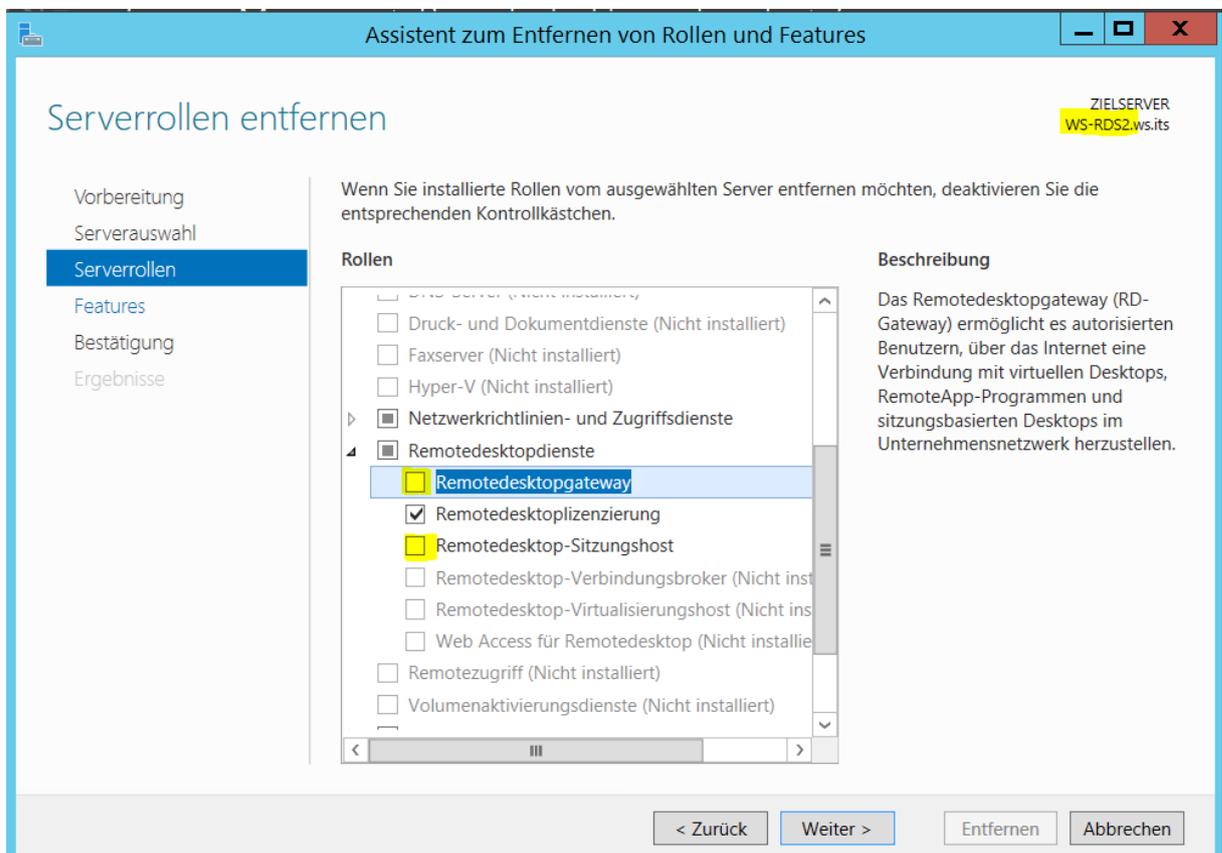
Server	Status	Status
Web Access für Remotedesktop - Rollendienst		
WS-RDS2.ws.its	<div style="width: 50%; background-color: #0070C0; height: 10px;"></div>	In Bearbeitung
	Neustart wird durchgeführt...	

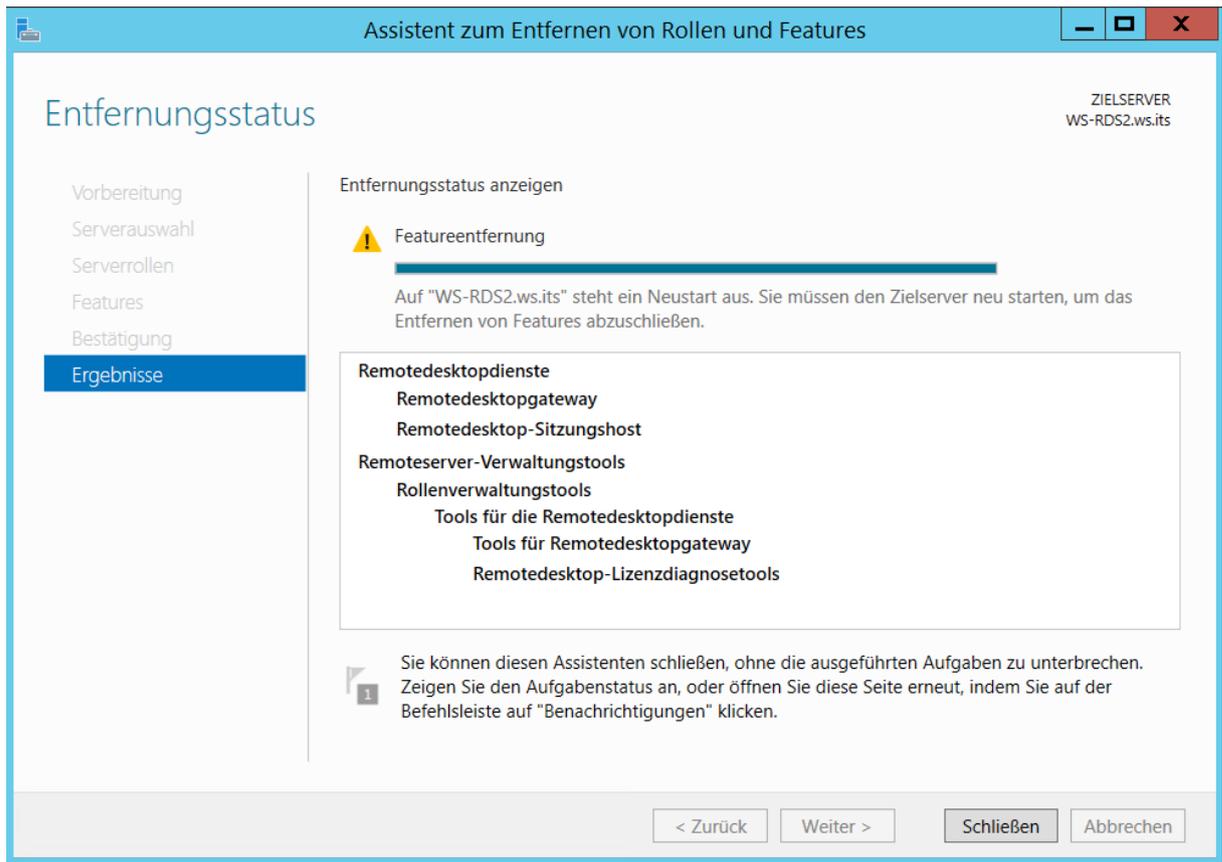
< Zurück Weiter > Entfernen Abbrechen

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

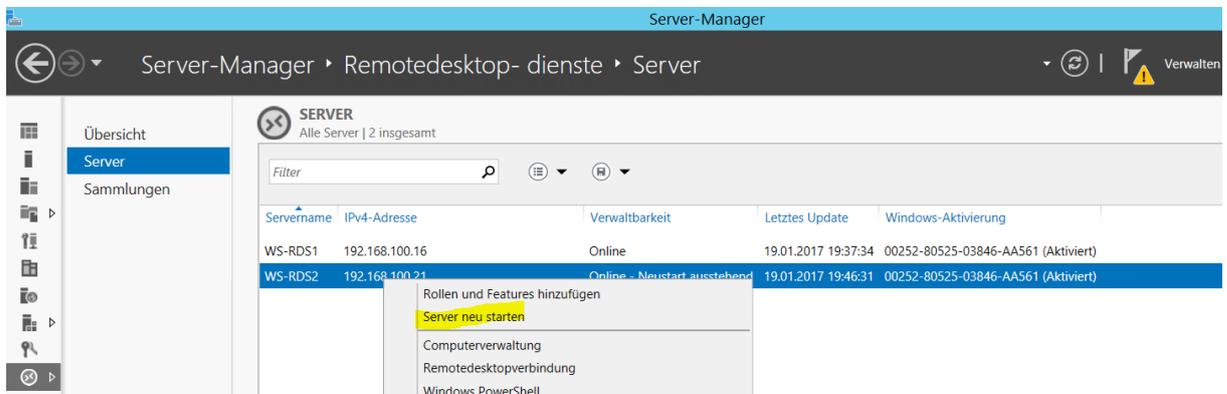


Nur der Lizenzserver verbleibt:

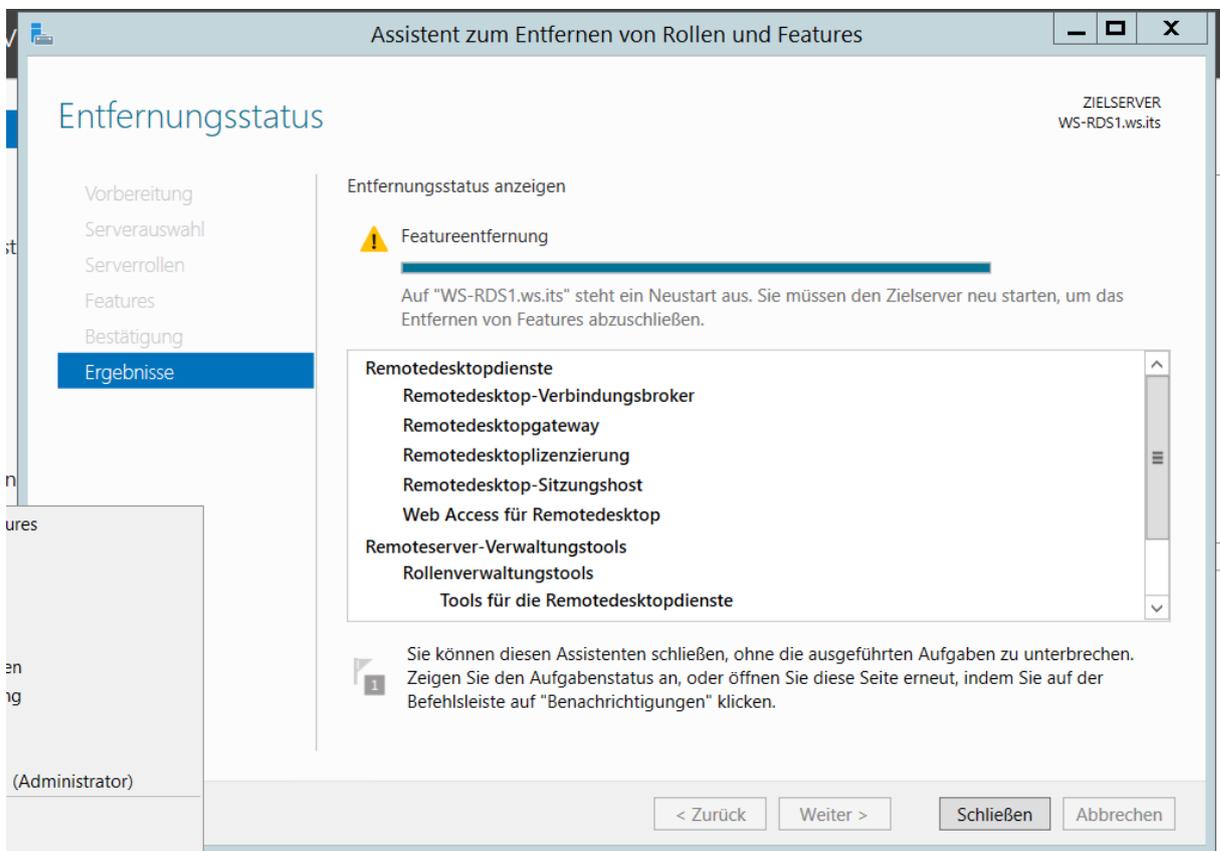
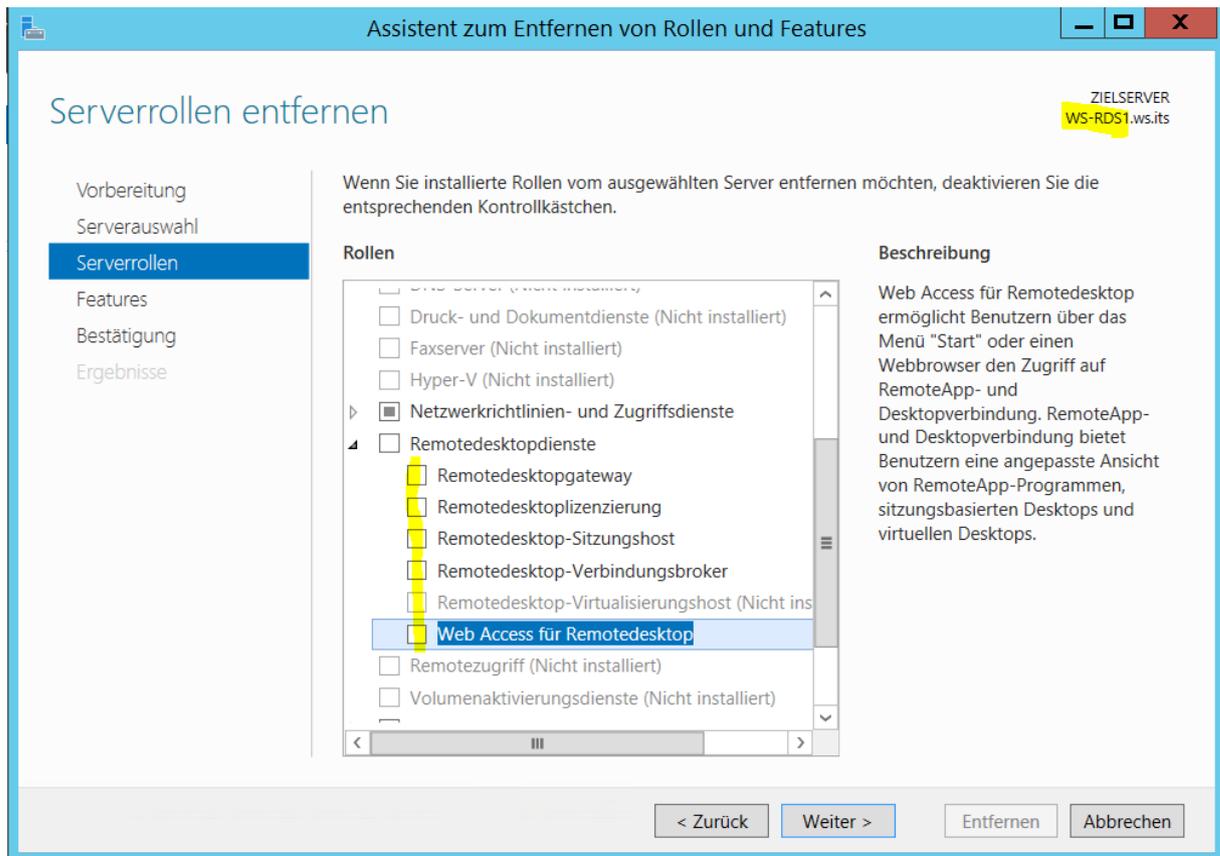




Der Server benötigt einen Neustart:



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

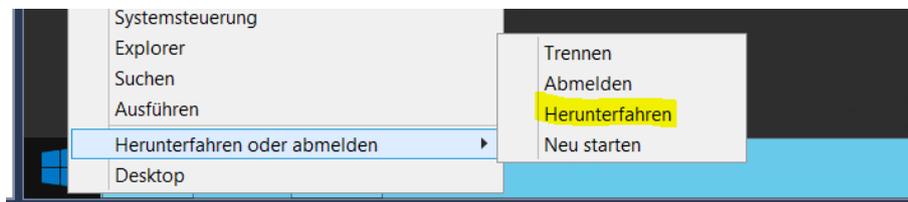
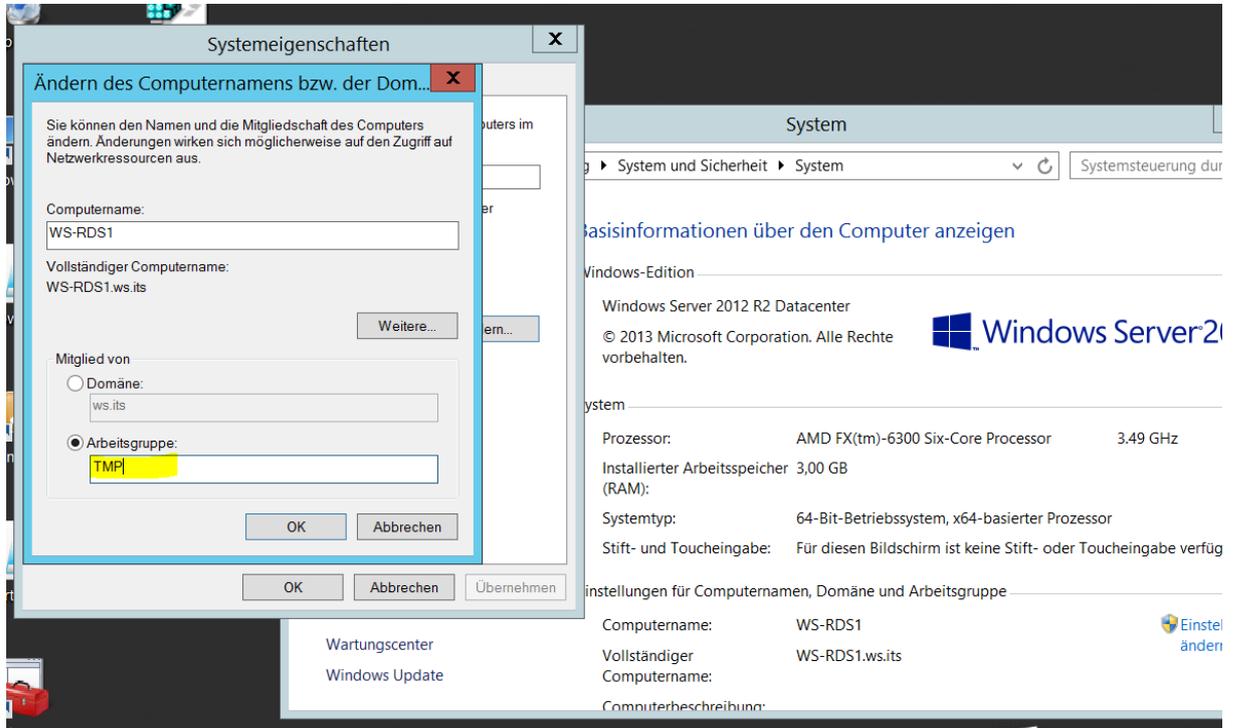


Abschalten des alten Servers WS-RDS1

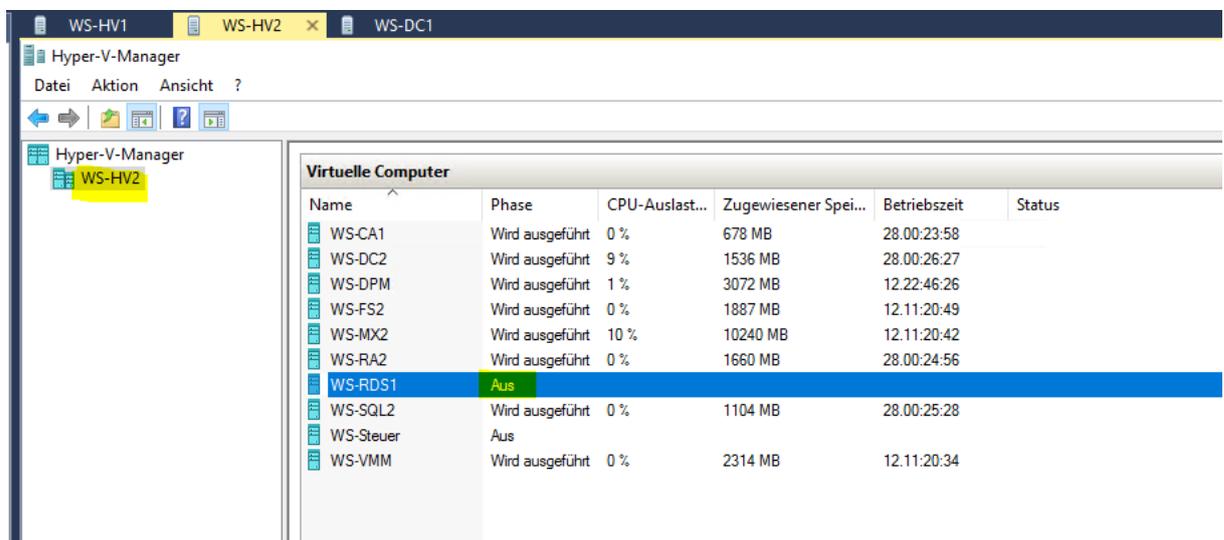
Nach dem Neustart sichere ich noch einige Informationen des alten Servers:

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

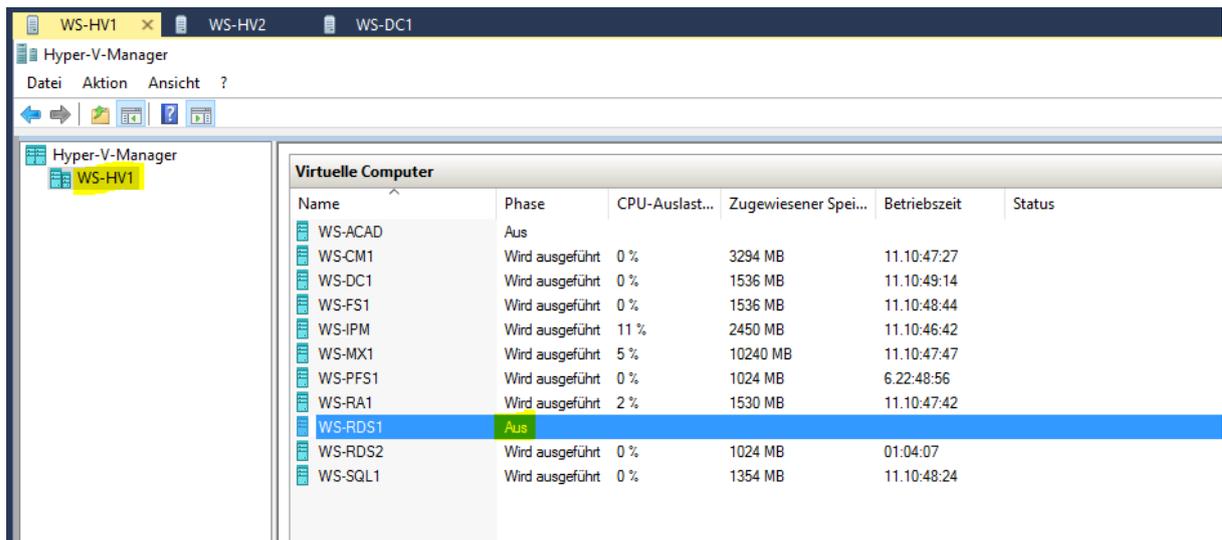
Jetzt kann der Server das Active Directory verlassen:



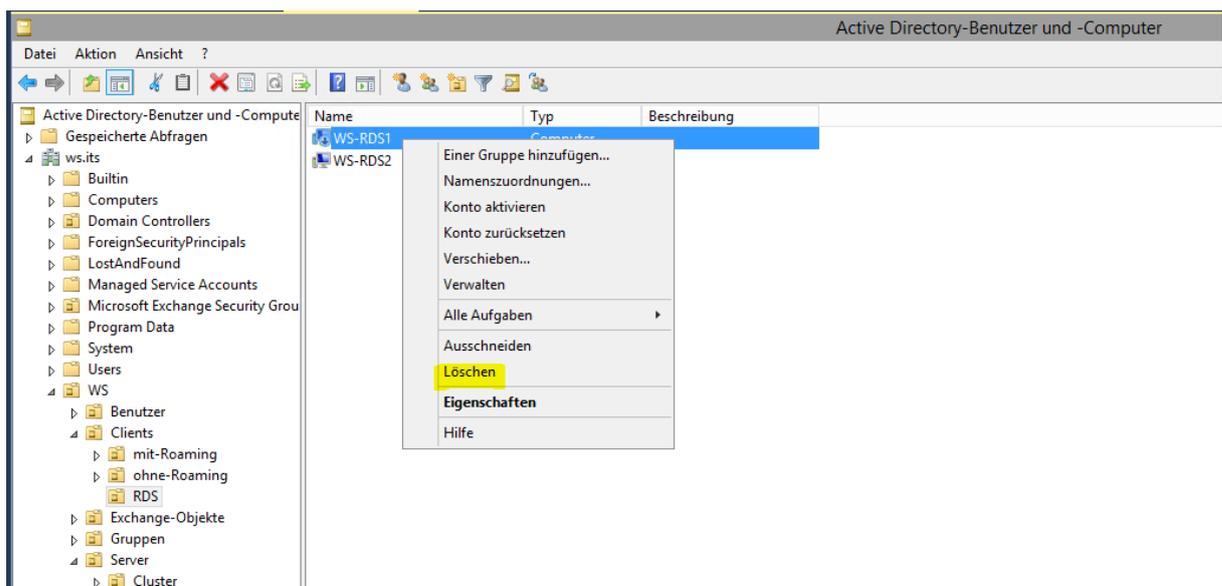
Die alte VM ist jetzt ausgeschaltet:



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:



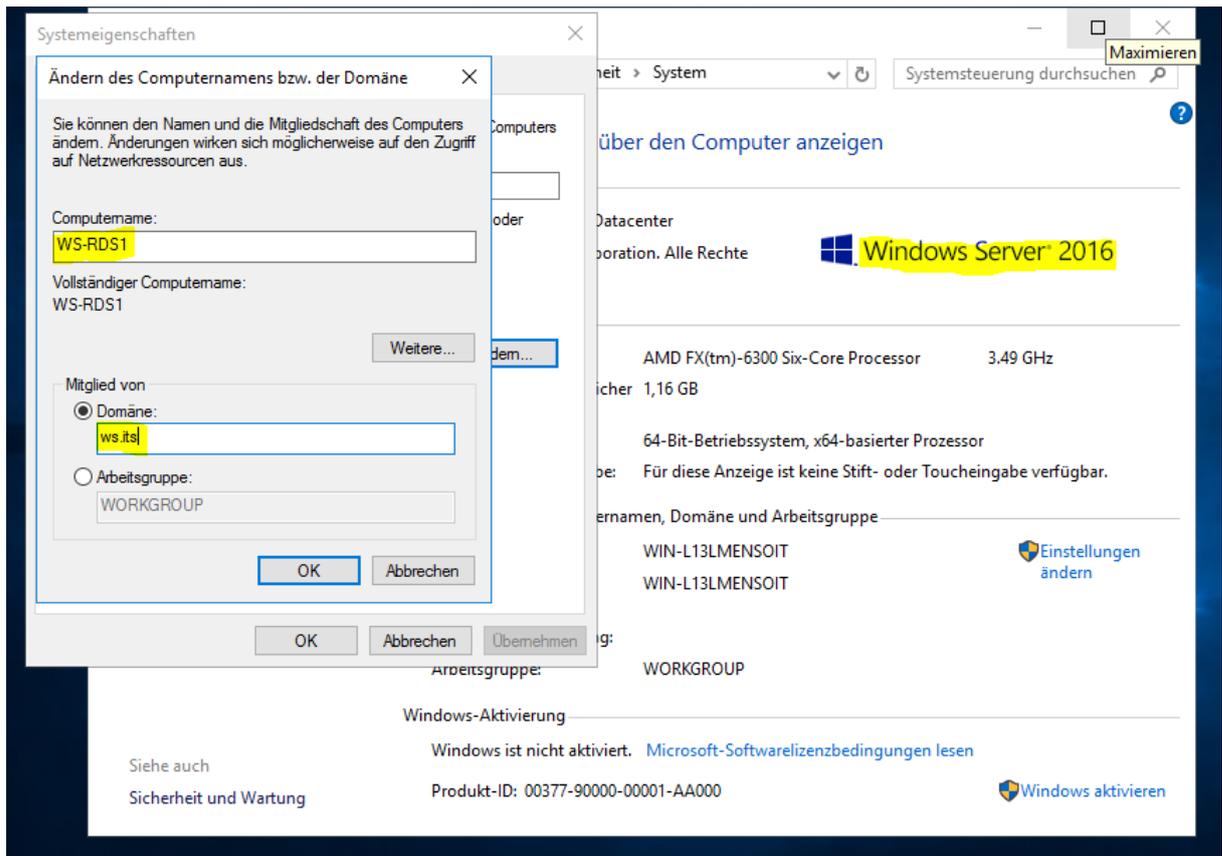
Im Active Directory lösche ich das AD-Computerkonto, damit der neue Server den gleichen Namen mit neuer SID verwenden kann:



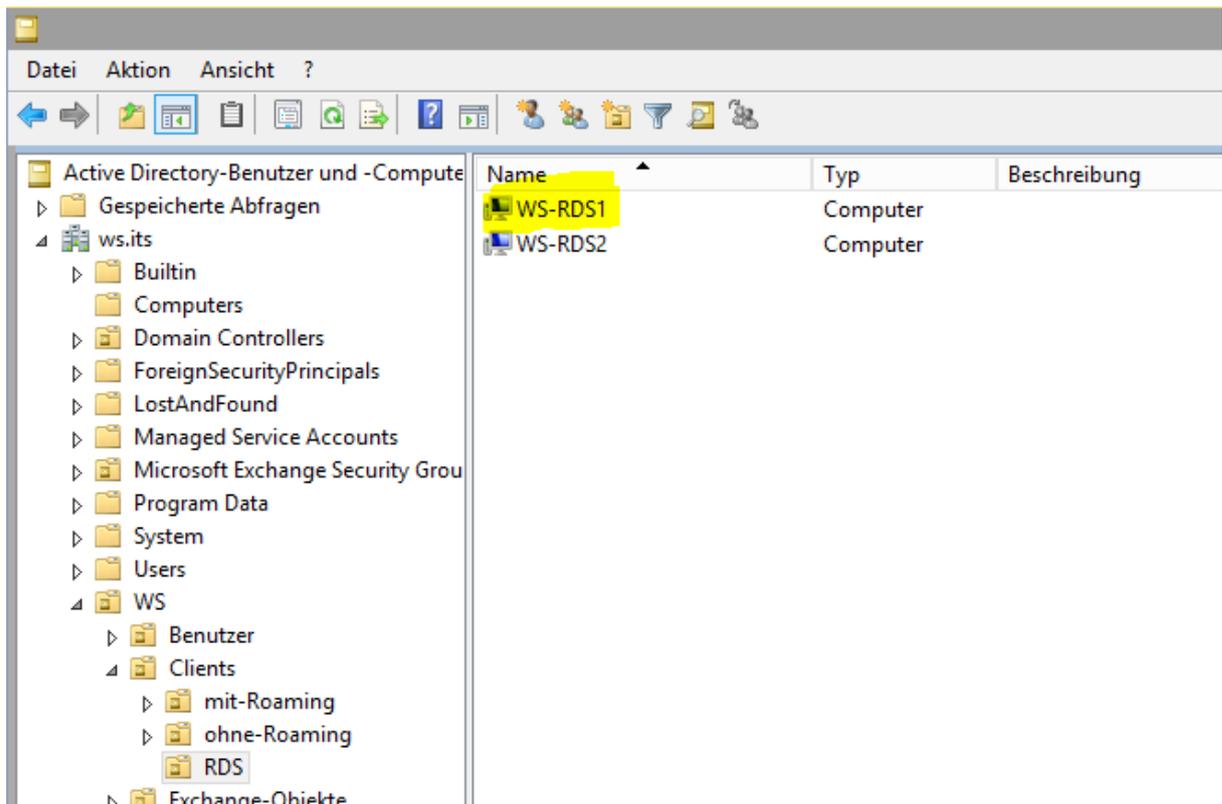
3. Aufbau der neuen RDS-Infrastruktur

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:



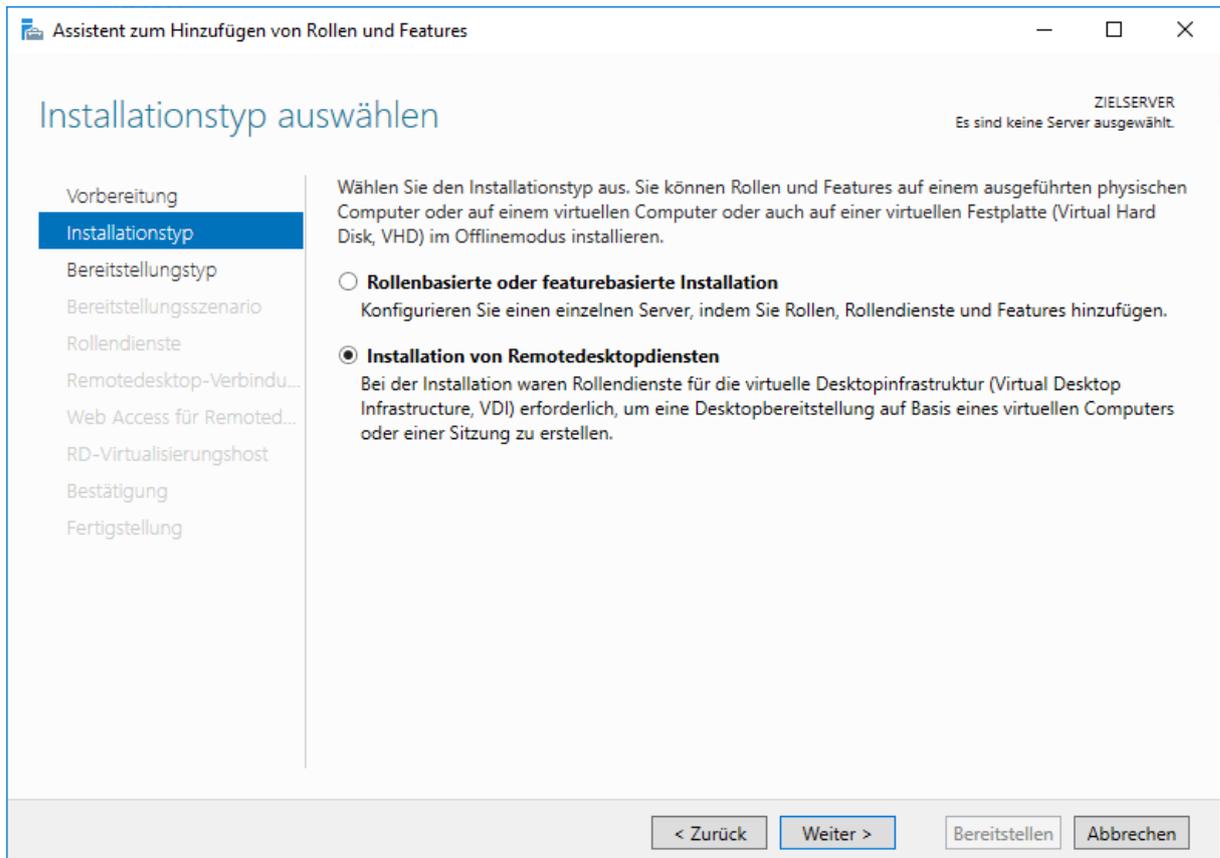
Das Computerkonto verschiebe ich nun in die richtige OU und starte dann den Server neu:



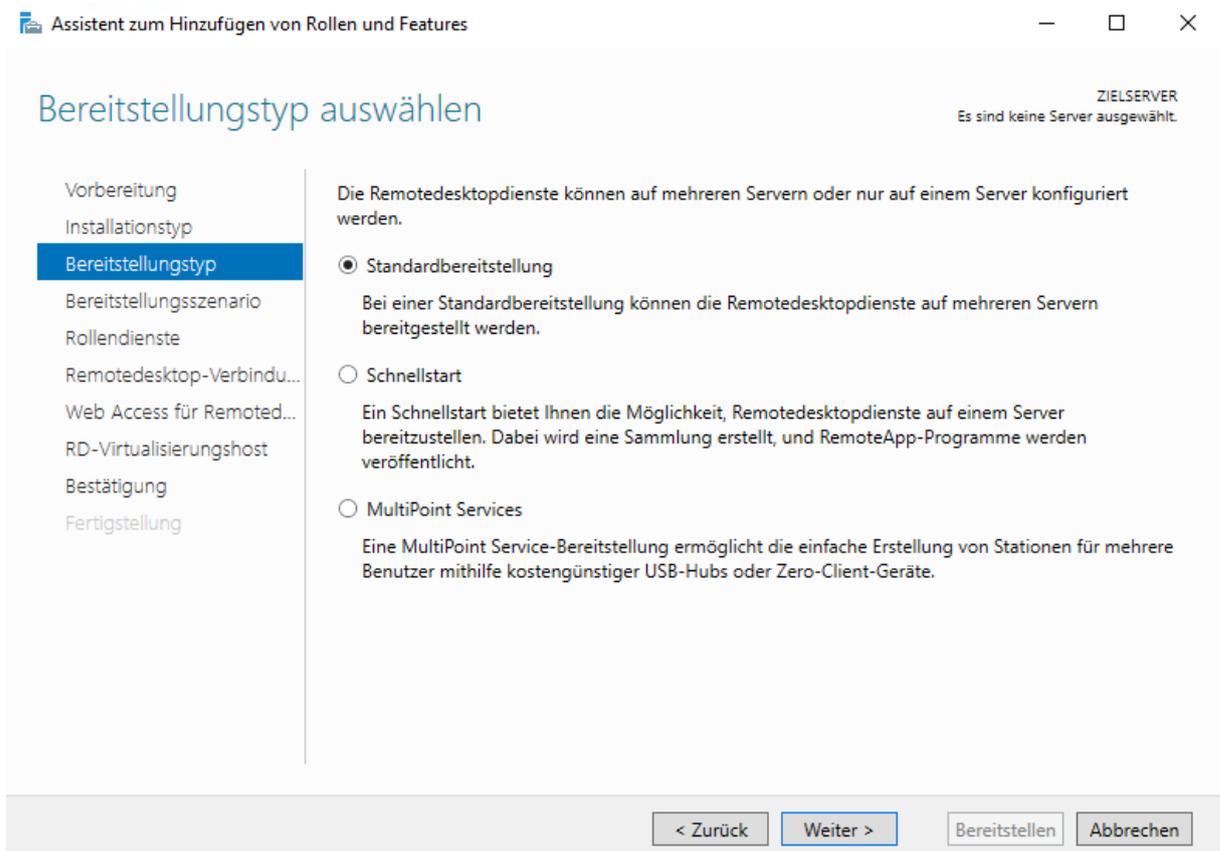
Die IP-Konfiguration entspricht schon der des alten Servers – lediglich den NLB benötige ich nicht mehr. Die dazugehörige IP-Adresse habe ich freigegeben.

Installation der neuen RDS-Infrastruktur

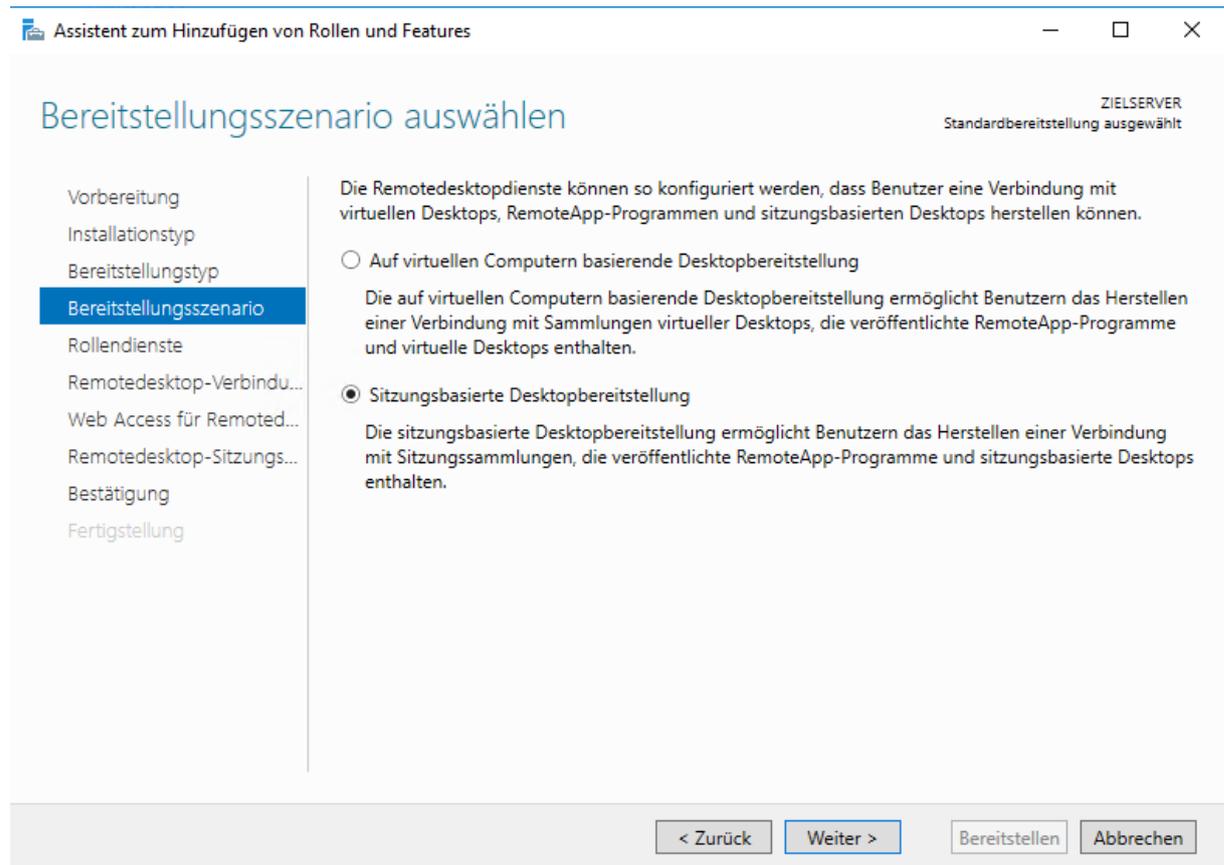
Auf dem neuen Server starte ich den Bereitstellungsassistenten für RDS:



Eine Standard-Bereitstellung genügt:



Zunächst soll eine SessionHost-Bereitstellung gestartet werden:



Assistent zum Hinzufügen von Rollen und Features ZIELSERVER
Standardbereitstellung ausgewählt

Bereitstellungsszenario auswählen

- Vorbereitung
- Installationstyp
- Bereitstellungstyp
- Bereitstellungsszenario**
- Rollendienste
- Remotedesktop-Verbindu...
- Web Access für Remoted...
- Remotedesktop-Sitzungs...
- Bestätigung
- Fertigstellung

Die Remotedesktopdienste können so konfiguriert werden, dass Benutzer eine Verbindung mit virtuellen Desktops, RemoteApp-Programmen und Sitzungs-basierten Desktops herstellen können.

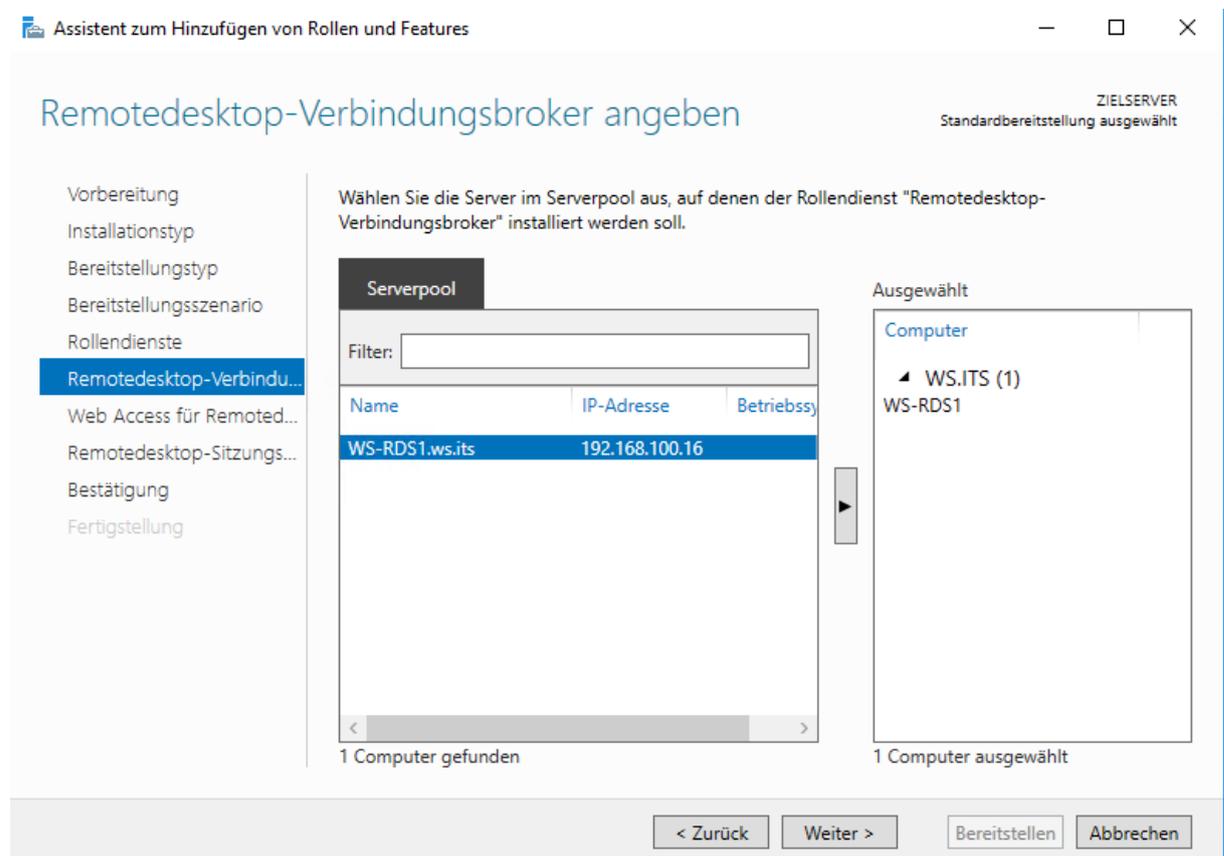
Auf virtuellen Computern basierende Desktopbereitstellung

Die auf virtuellen Computern basierende Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sammlungen virtueller Desktops, die veröffentlichte RemoteApp-Programme und virtuelle Desktops enthalten.

Sitzungs-basierte Desktopbereitstellung

Die Sitzungs-basierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungssammlungen, die veröffentlichte RemoteApp-Programme und Sitzungs-basierte Desktops enthalten.

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



Assistent zum Hinzufügen von Rollen und Features ZIELSERVER
Standardbereitstellung ausgewählt

Remotedesktop-Verbindungsbroker angeben

- Vorbereitung
- Installationstyp
- Bereitstellungstyp
- Bereitstellungsszenario
- Rollendienste
- Remotedesktop-Verbindu...**
- Web Access für Remoted...
- Remotedesktop-Sitzungs...
- Bestätigung
- Fertigstellung

Wählen Sie die Server im Serverpool aus, auf denen der Rollendienst "Remotedesktop-Verbindungsbroker" installiert werden soll.

Serverpool

Filter:

Name	IP-Adresse	Betriebsy
WS-RDS1.ws.its	192.168.100.16	

1 Computer gefunden

Ausgewählt

Computer

- WS.ITS (1)
 - WS-RDS1

1 Computer ausgewählt

Assistent zum Hinzufügen von Rollen und Features

ZIELSERVER
Standardbereitstellung ausgewählt

Server mit Web Access für Remotedesktop angeben

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-Verbindungsbroserserver installieren

Serverpool

Filter:

Name	IP-Adresse	Betriebsy
WS-RDS1.ws.its	192.168.100.16	

1 Computer gefunden

Ausgewählt

Computer

- WS.ITS (1)
- WS-RDS1

1 Computer ausgewählt

Assistent zum Hinzufügen von Rollen und Features

ZIELSERVER
Standardbereitstellung ausgewählt

RD-Sitzungshostserver angeben

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	Betriebsy
WS-RDS1.ws.its	192.168.100.16	

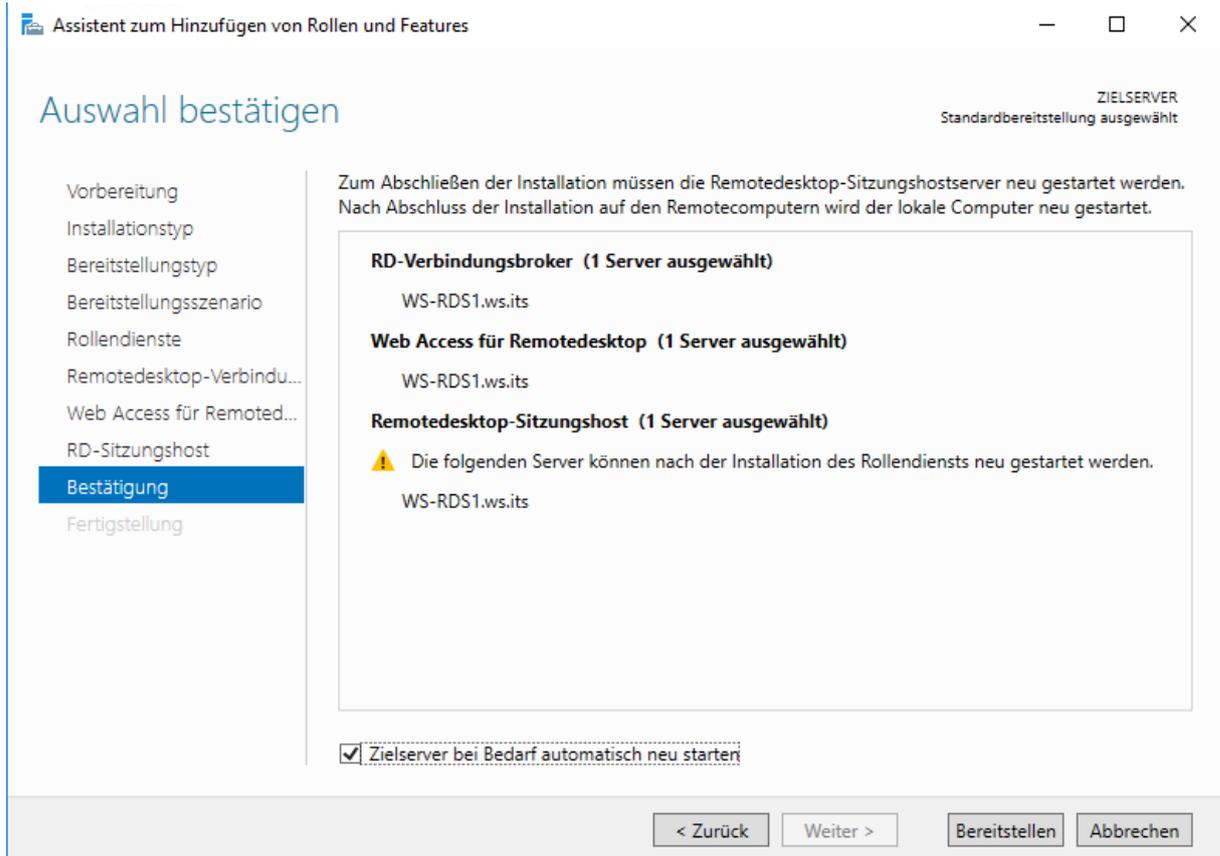
1 Computer gefunden

Ausgewählt

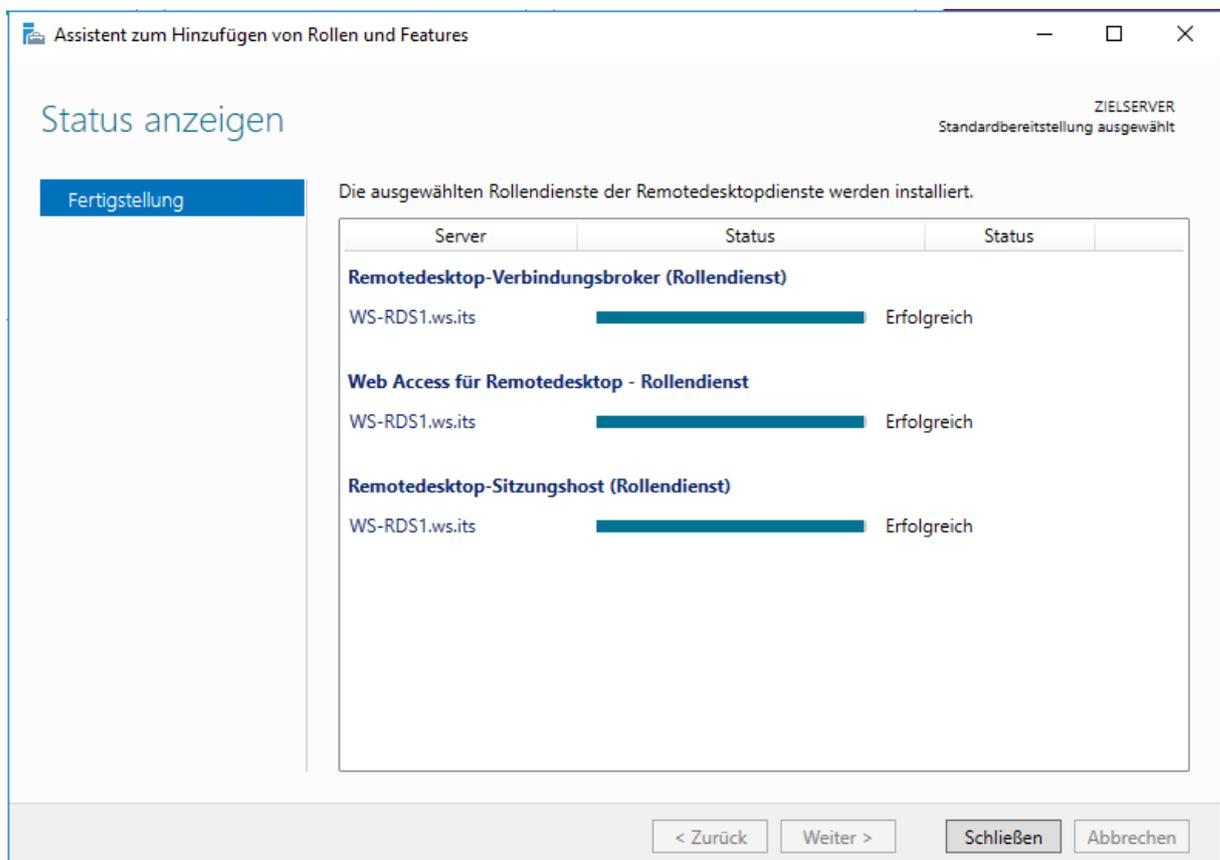
Computer

- WS.ITS (1)
- WS-RDS1

1 Computer ausgewählt



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



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

The screenshot shows the 'Server-Manager' console with the 'Remote Desktop Services' overview. The main heading is 'ERSTE SCHRITTE MIT DEN REMOTEDESKTOPDIENSTEN'. A large orange box indicates '1 Remotedesktopdienste-Bereitstellung einrichten'. Below this, it says 'Auf virtuellen Computern basierende Desktopbereitstellung' and lists three steps: '2 RD-Virtualisierungshostserver hinzufügen', '3 Virtuelle Desktopsammlungen erstellen', and 'Sitzungsbasierte Desktopbereitstellung' with steps '2 RD-Sitzungshostserver hinzufügen' and '3 Sitzungssammlungen erstellen'. A 'BEREITSTELLUNGSÜBERSICHT' section shows a diagram of the RDS architecture with components like 'Web Access für Remo...', 'Remotedesktopgate...', 'Remotedesktoplizen...', 'Remotedesktop-Verb...', 'Remotedesktop-Virtu...', and 'Remotedesktop-Sitzu...'. A 'BEREITSTELLUNGSSEVER' table lists installed roles for three servers.

Vollqualifizierter Domänenname des Servers	Installierter Rollendienst
WS-RDS1.WS.ITS	RD-Verbindungsbroker
WS-RDS1.WS.ITS	RD-Sitzungshost
WS-RDS1.WS.ITS	Web Access für Remotedesktop

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

The screenshot shows the 'Server des Typs "RD-Gateway" hinzufügen' wizard. The main heading is 'Wählen Sie einen Server aus.'. The wizard is in the 'Serverauswahl' step. It provides instructions: 'Mit diesem Assistenten können Sie der Bereitstellung Server vom Typ "RD-Gateway" hinzufügen. Wählen Sie die Server aus, auf denen der Rollendienst "RD-Gateway" installiert werden soll.' A 'Serverpool' table lists available servers, with 'WS-RDS1.ws.its' selected. An 'Ausgewählt' list shows 'Computer' > 'WS.ITS (1)' > 'WS-RDS1'. A note at the bottom states: 'Die Anmeldeinformationen des WS\sysadm-Kontos werden zum Hinzufügen der Server verwendet.' Navigation buttons at the bottom include '< Zurück', 'Weiter >', 'Hinzufügen', and 'Abbrechen'.

Name	IP-Adresse	Betrieb
WS-RDS1.ws.its	192.168.100.16	

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

Server des Typs "RD-Gateway" hinzufügen

Selbstsigniertes SSL-Zertifikat benennen

Serverauswahl

SSL-Zertifikatname

Bestätigung

Ergebnisse

SSL-Zertifikate dienen zum Verschlüsseln der Kommunikation zwischen Remotedesktopdienste-Clients und Remotedesktopgateway-Servern. Der Name des selbstsignierten SSL-Zertifikats muss dem vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) des Remotedesktop-Gatewayservers entsprechen.

SSL-Zertifikatname (externen FQDN des RD-Gatewayservers verwenden):

Der FQDN muss dem Namen des Remotedesktop-Gatewayservers entsprechen, der vom Remotedesktopdienste-Client verwendet wird.

< Zurück
Weiter >
Hinzufügen
Abbrechen

Der Lizenzierungsserver wird ähnlich installiert:

Server des Typs "RD-Lizenzierung" hinzufügen

Wählen Sie einen Server aus.

Serverauswahl

Bestätigung

Ergebnisse

Mit diesem Assistenten können Sie der Bereitstellung Server vom Typ "RD-Lizenzierung" hinzufügen. Wählen Sie die Server aus, auf denen der Rollendienst "RD-Lizenzierung" installiert werden soll.

Serverpool

Filter:

Name	IP-Adresse	Betrieb
WS-RDS1.ws.its	192.168.100.16	

1 Computer gefunden

Ausgewählt

Computer

- WS.ITS (1)
 - WS-RDS1

1 Computer ausgewählt

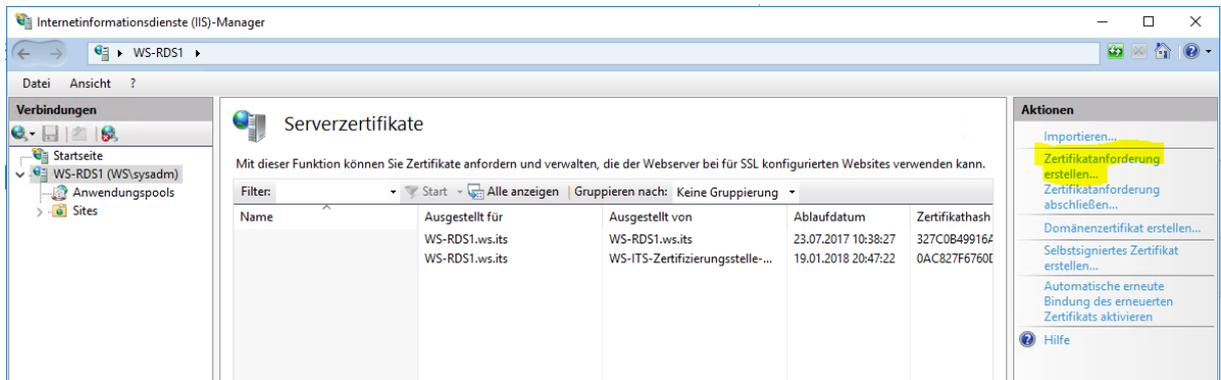
i Die Anmeldeinformationen des WS\sysadm-Kontos werden zum Hinzufügen der Server verwendet.

< Zurück
Weiter >
Hinzufügen
Abbrechen

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.

Zertifikat anfordern

Eigenschaften für definierten Namen

Geben Sie die erforderlichen Informationen für das Zertifikat an. Für "Bundesland/Kanton" und "Ort" müssen die offiziellen Namen ohne Abkürzungen angegeben werden.

Gemeinsamer Name:

Organisation:

Organisationseinheit:

Ort:

Bundesland/Kanton:

Land/Region:

Zurück Weiter Fertig stellen Abbrechen

Zertifikat anfordern

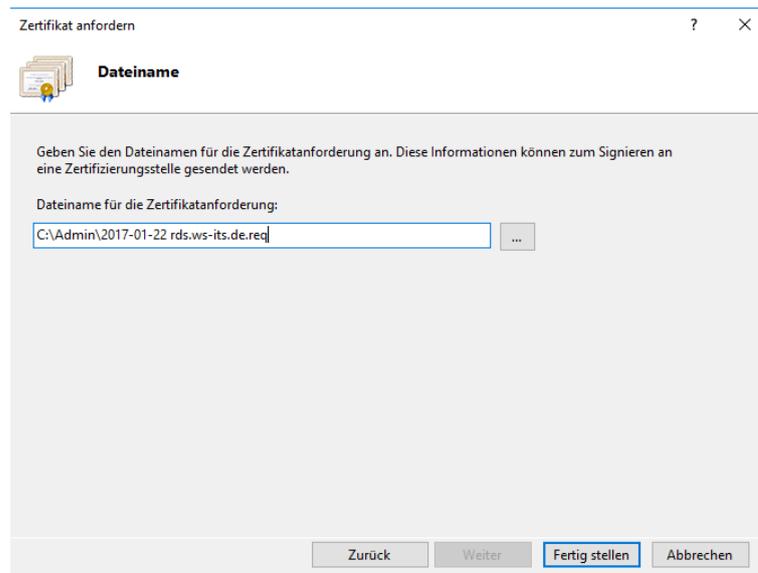
Eigenschaften für Kryptografiedienstanbieter

Wählen Sie einen Kryptografiedienstanbieter und eine Bitlänge aus. Die Bitlänge des Verschlüsselungsschlüssels bestimmt die Verschlüsselungsstärke des Zertifikats. Je größer die Bitlänge, desto höher die Sicherheit. Eine größere Bitlänge kann jedoch die Leistung verringern.

Kryptografiedienstanbieter:

Bitlänge:

Zurück Weiter Fertig stellen Abbrechen



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 😊

Tool Box

Certificates Wizard

Validations Wizard

Free SSL Certificate – Class 1 DV SSL Certificate

Please enter the full hostname for SSL certificate (e.g: mail.domain.com):

Validated domain(s): ws-its.de [Add Domain](#)

rds.ws-its.de

✔ The common name of this certificate: rds.ws-its.de

Do you want to add the following hostname?

ws-its.de

- The first entry domain will be the common name of the certificate.
- You can enter up to 10 hostnames, one line one hostname with "Enter" or separate each hostname with a comma.
- You can not enter a wildcard like *.domain.com.

If you would like to support up to 100 hostnames and wildcard, please finish the "[Personal Identity Validation](#)" for personal use that only cost US\$59.90 for FREE. Or go to "[Organization Extended Validation](#)" for organization use that only cost US\$199.90 for unlimited multi-domain and wildcard OV SSL certificate FREE.

Please submit your Certificate Signing Request (CSR):

Generated by Myself (.cer PEM format certificate)
 You can use [StartComTool.exe](#) to generate the CSR.
 or use the openssl command: `openssl req -newkey rsa:2048 -keyout yourname.key -out yourname.csr`

```
AHIAbwB2AGkAZABIAHIDAQAwwgc8GCSqGSIb3DQEJJjGBwTCBvjAObGNVHQ8BAf8E
BAMCBPAwEwYDVR0IBAwWCgYIKwYBBQUHAWEwEwAYJKoZIhvcNAQkPBGswTAOBggq
hkiG9w0DAgICAIAwDgYIKoZIhvcNAwQCAgCAMAsGCWCGSAFIAwQBKjALBglghkgB
ZQMEAS0wCwYJIZIAWUDBAECMAAsGCWCGSAFIAwQBBAHBBgUrDgMCBzAKBggqhkig
9w0DBzAdBgNVHQ4EFgQUUrcdVppcsoaXU5u6o2rDXDG2ZmgwDQYJKoZIhvcNAQEF
BQADggEBAHahLNMsp9/v73FsNSMaz19JsoghIPkyk72PYXkd/ZpSHooo/W7LWkns
qP95w8rtngmpvG4jNqcba4H2AWrxK6Lu7rXDIFT/dRpDbkfvbDUA2e5KNLbU4tlk
OmQS9Oj5YE5aEtb/yvpJIeZAV9aOByDXe8q1b8M1g0Zm/7hkXV9V+GFQqt3I3it1
wAxxB7QJiZBrw5ysVylD925EVlxF1I8sZEmeYNprKNS91fwlmTNIMar2/ZwVoLi
k+JcX7tVvldGszOw9wueo5x6mb/yxr3IE2a0brlZ/senXLBuP3ja6pauwRng/o
Z0W7GIDmUZwb5nd+5uOWsaJALRurKFU=
-----END NEW CERTIFICATE REQUEST-----
```

Algorithm :RSA
Key length :2048

StartCom

Tool Box

Certificates Wizard

Validations Wizard

Your certificate is issued, please click [here](#) to download the certificate, the intermediate certificate and the root CA certificate. And you can retrieve your issued certificate at "Tool Box" – "Certificate List" at any time if you need.

Certificate List →

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

Name	Änderungsdatum	Typ	Größe
2017-01-22 Intermediate.crt	22.01.2017 16:49	Sicherheitszertifikat	3 KB
2017-01-22 rds.ws-its.de.crt	22.01.2017 16:49	Sicherheitszertifikat	3 KB
2017-01-22 rds.ws-its.de.req	22.01.2017 09:48	REQ-Datei	2 KB
2017-01-22 rds.ws-its.de.zip	22.01.2017 09:50	ZIP-komprimierte...	16 KB

← Zertifikatimport-Assistent
✕

Zu importierende Datei
Geben Sie die Datei an, die importiert werden soll.

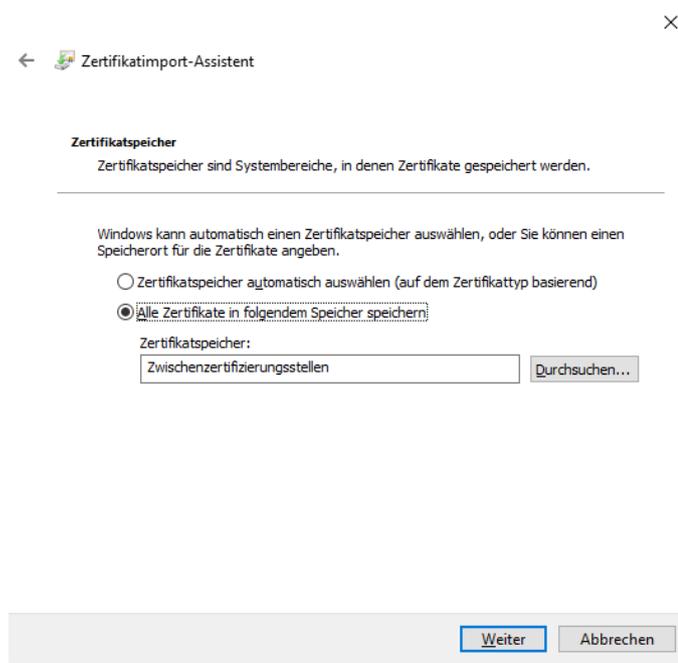
Dateiname:

Durchsuchen...

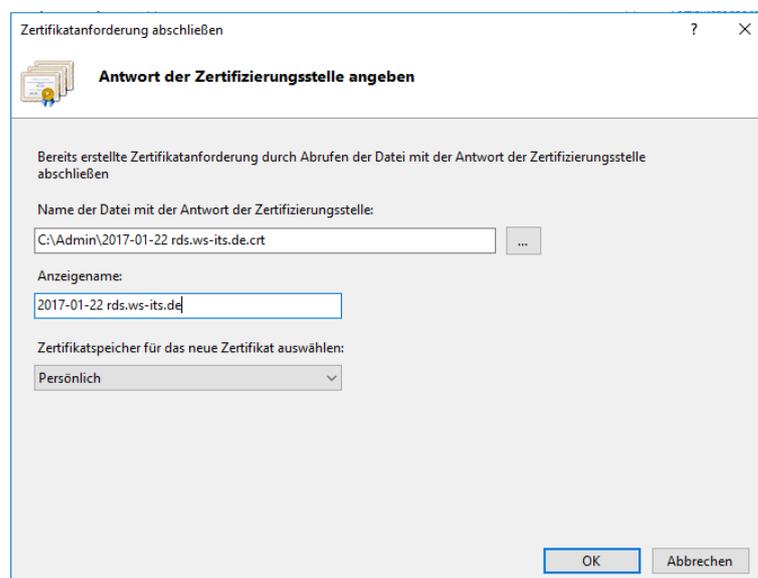
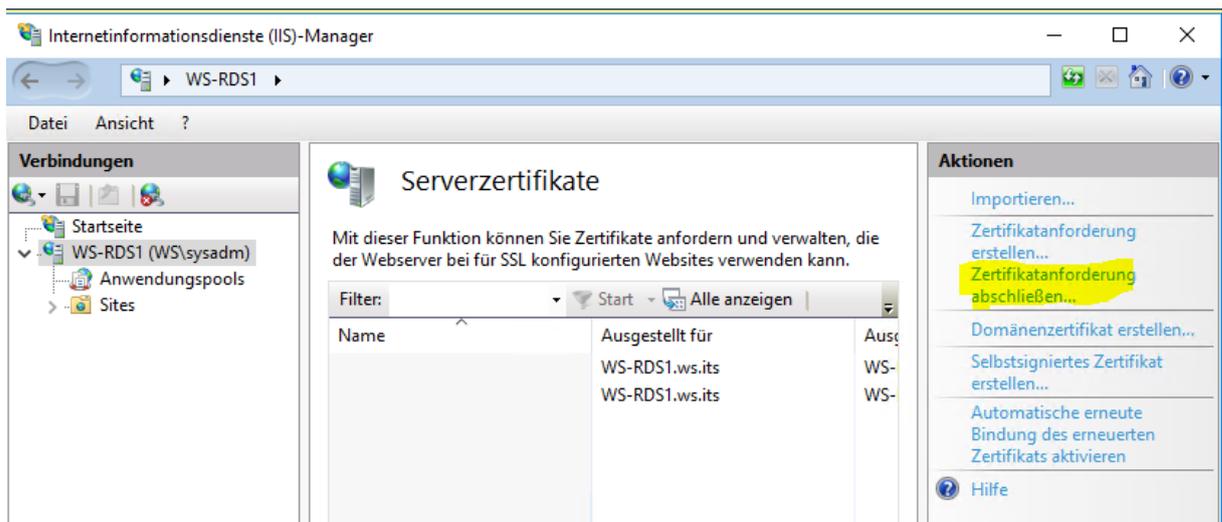
Hinweis: Mehrere Zertifikate können in einer Datei in folgenden Formaten gespeichert werden:

- Privater Informationsaustausch - PKCS #12 (.PFX,.P12)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
- Microsoft Serieller Zertifikatspeicher (.SST)

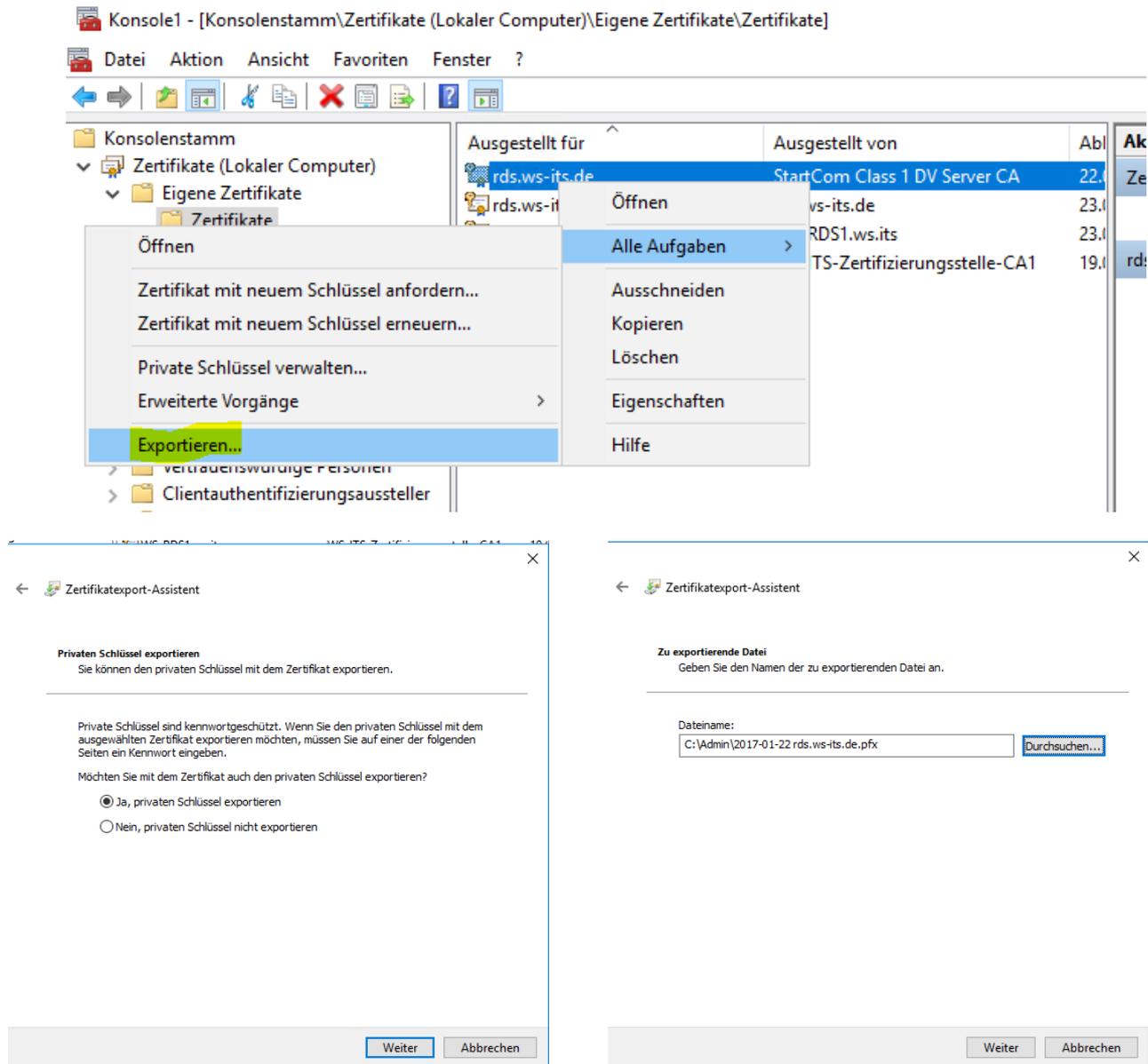
Weiter
Abbrechen



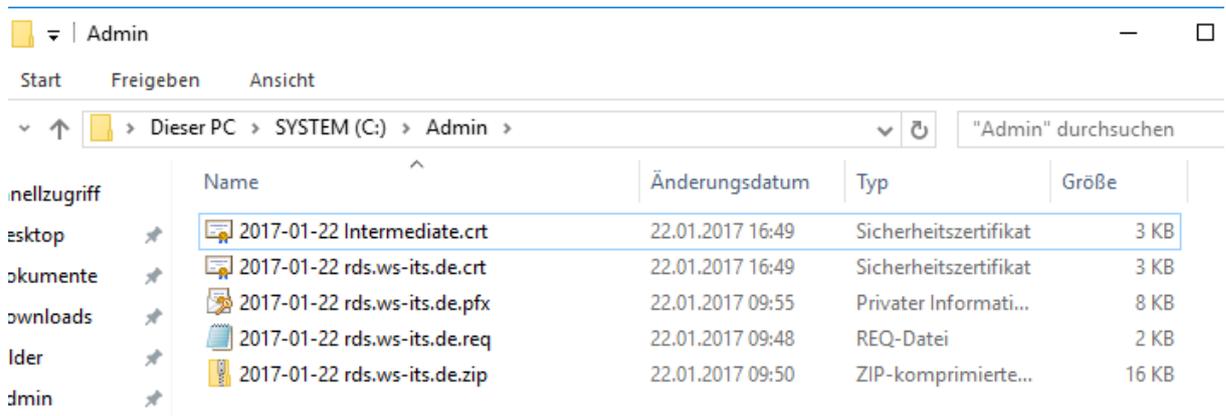
Das Zertifikat (der öffentliche Teil) wird dann im IIS mit dem Private Key zusammengeführt



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:

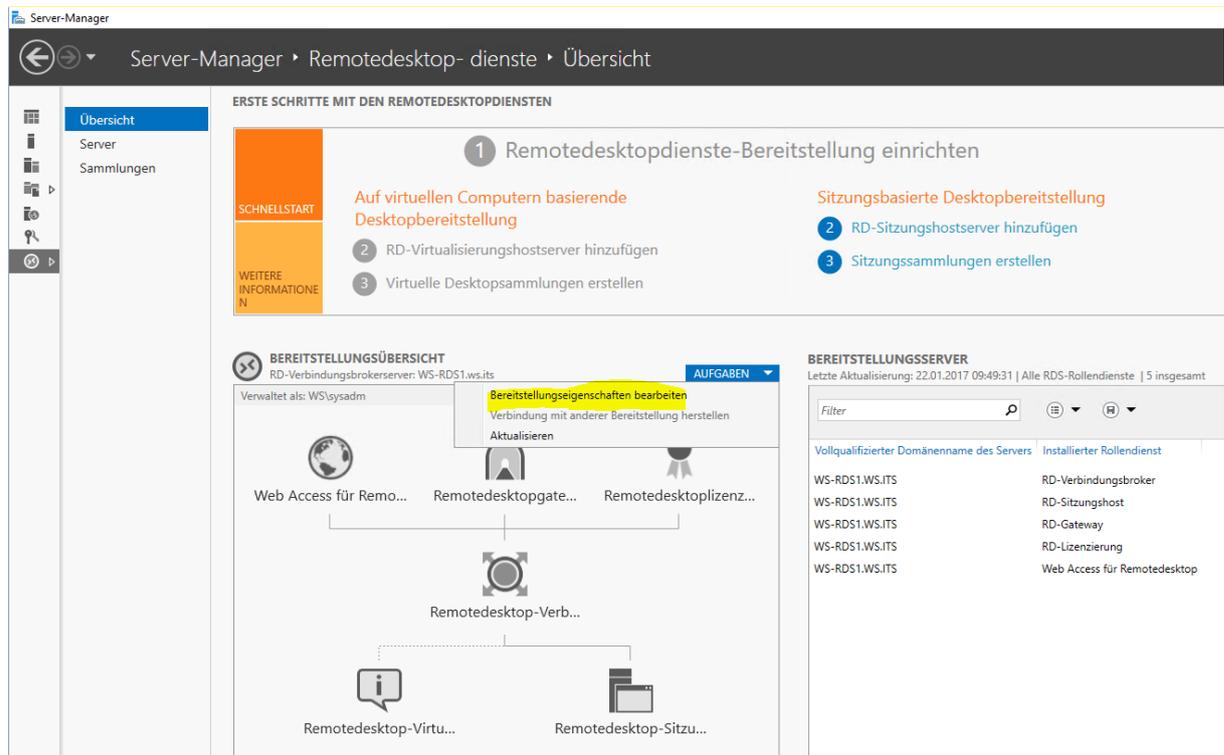


Jetzt liegen alle relevanten Dateien in einem Verzeichnis. Später verschiebe ich alles an einen sicheren Ort:

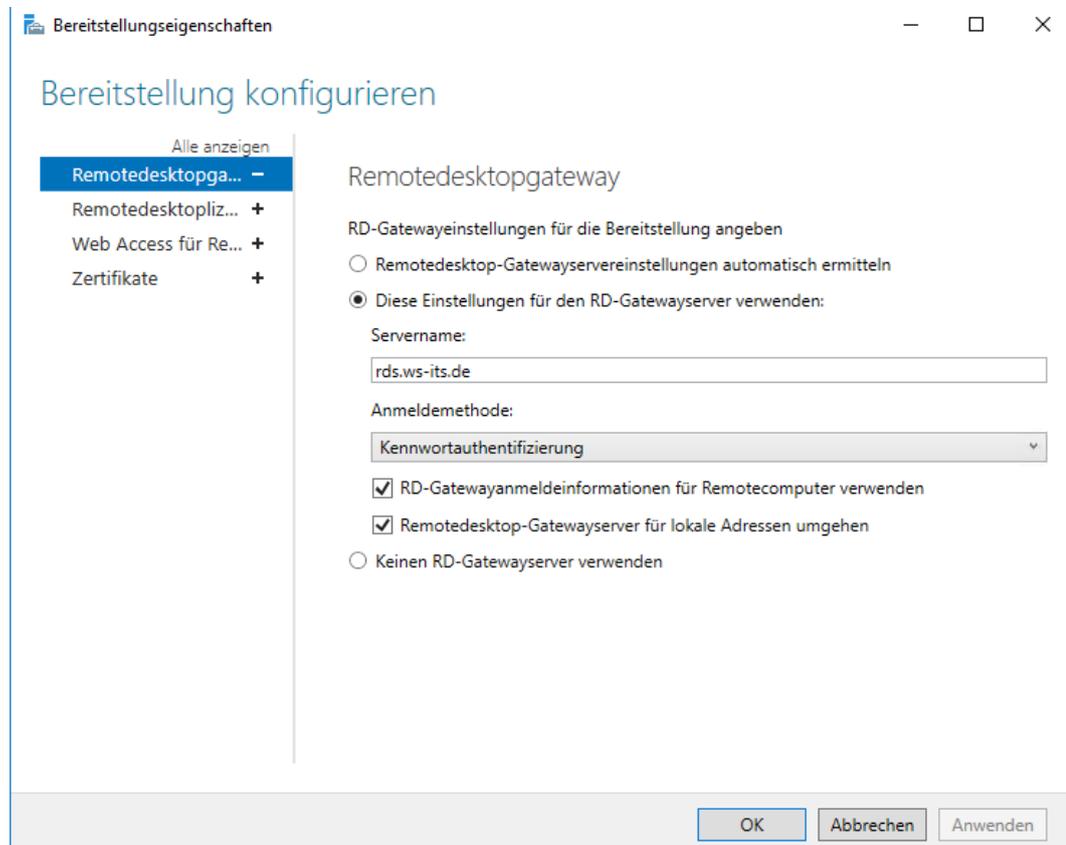


Konfiguration der RDS-Infrastruktur - allgemein

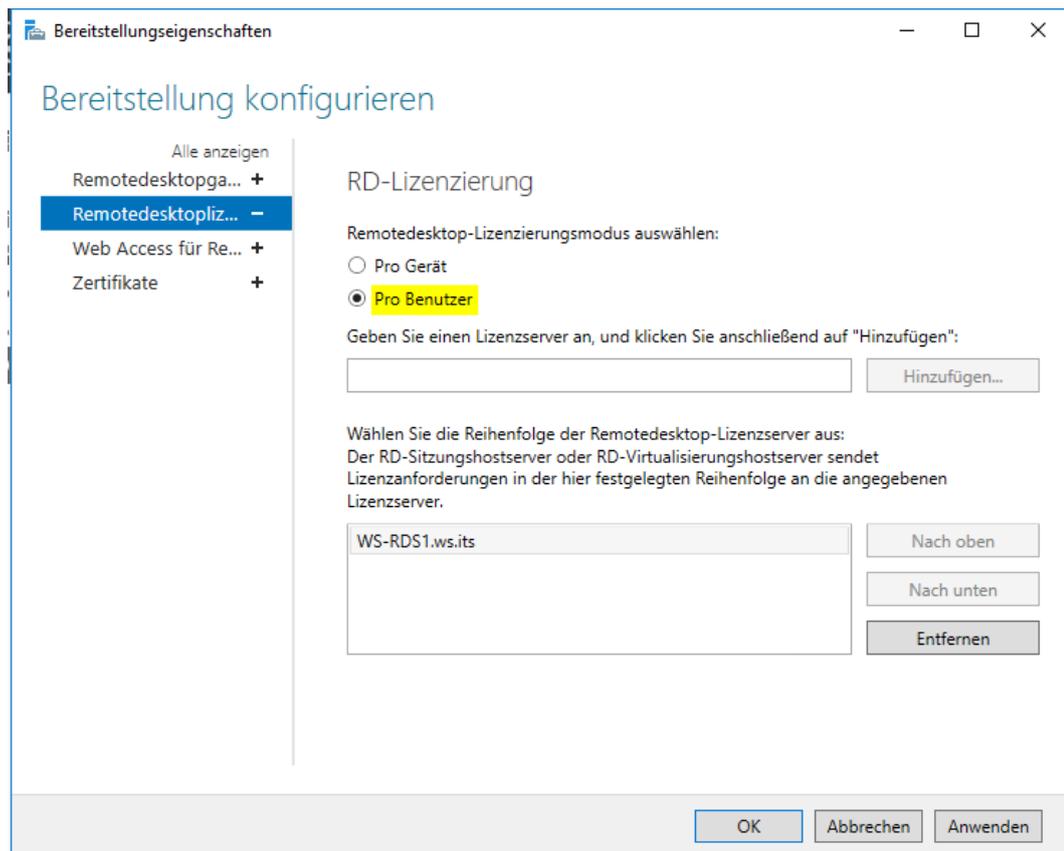
Im Servermanager starte ich den erforderlichen Assistenten:



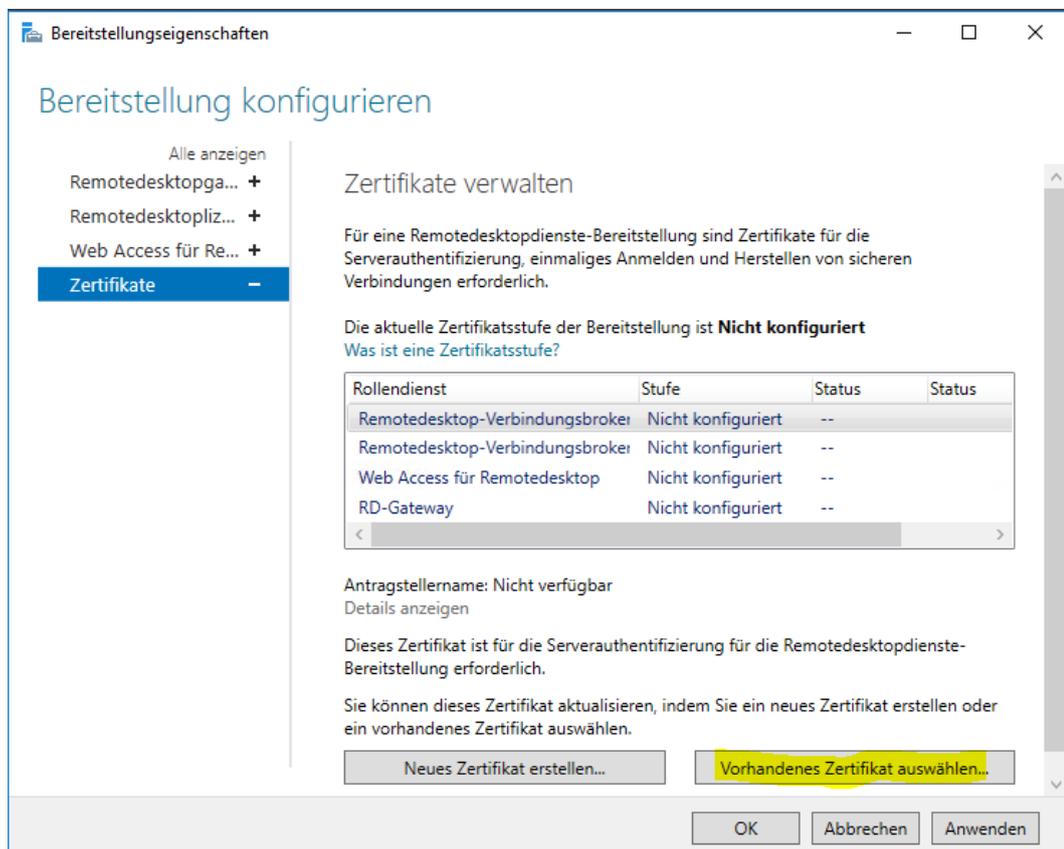
Die Adresse des Gateways passt bereits. Weitere Konfigurationen nehme ich später vor:



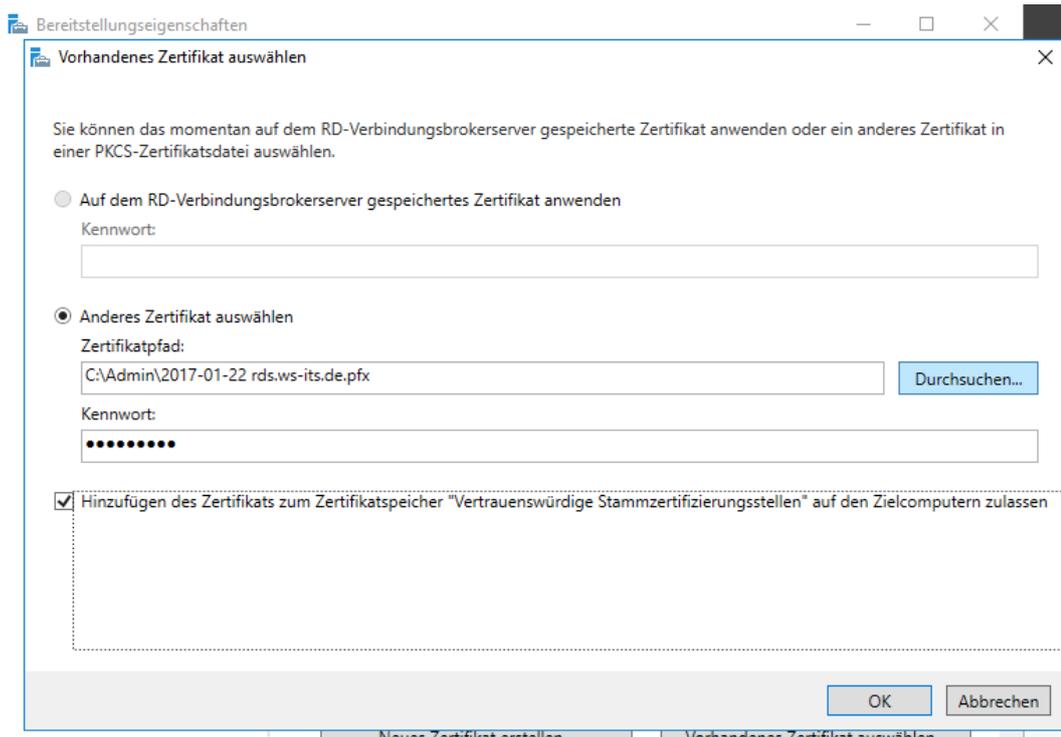
Die Lizenzierung stelle ich noch auf Pro Benutzer um. Der Lizenzserver benötigt ebenfalls separate Anpassungen:



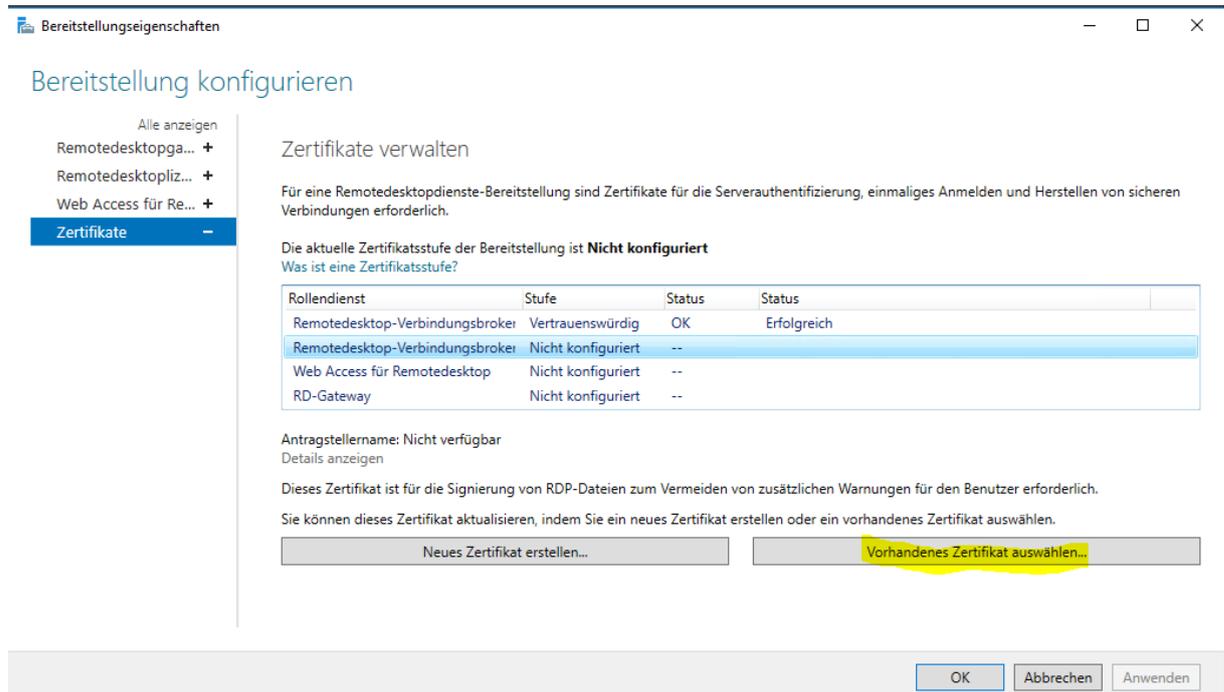
Im WebAccess kann man so nichts ändern. Dafür müssen die Zertifikatinformationen eingegeben werden:



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



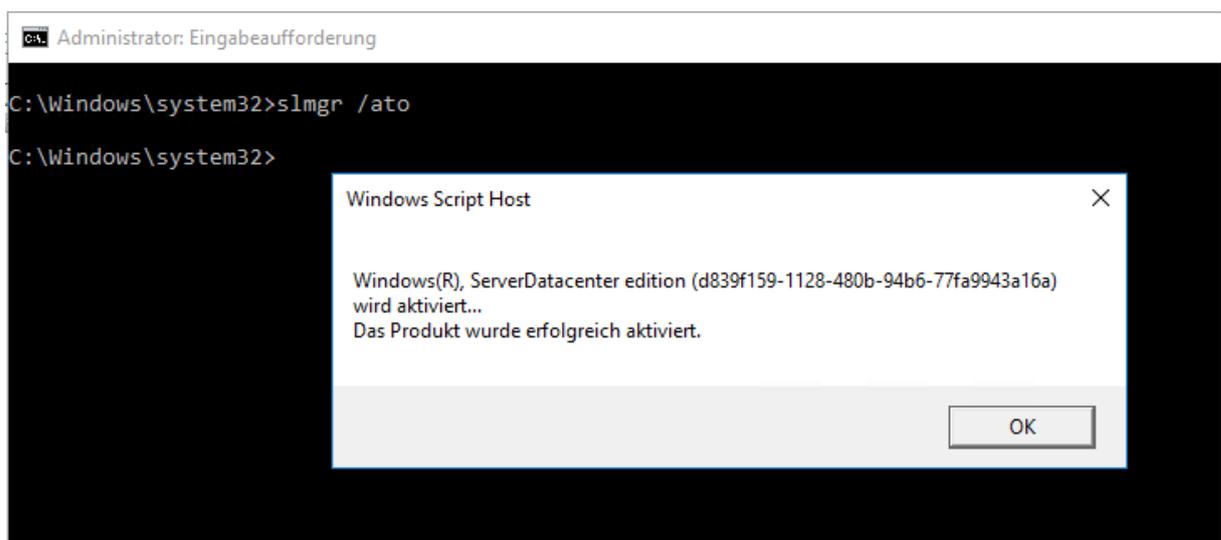
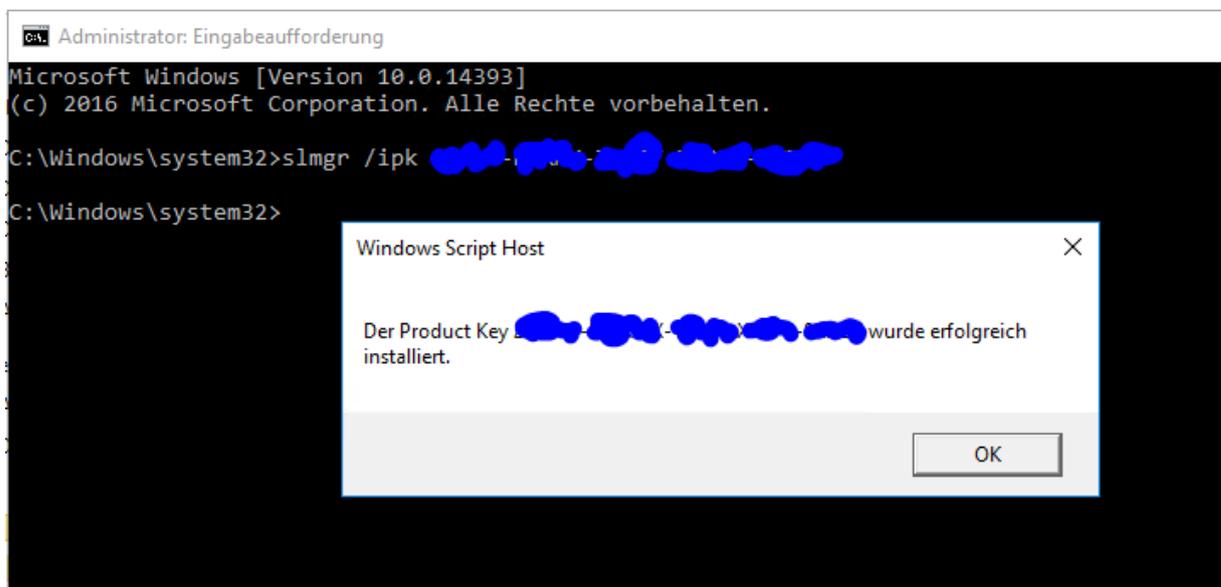
Der Arbeitsschritt ist für jedes Element in der Tabelle einzeln zu wiederholen...



... bis alle Einträge einen Status = OK aufweisen:

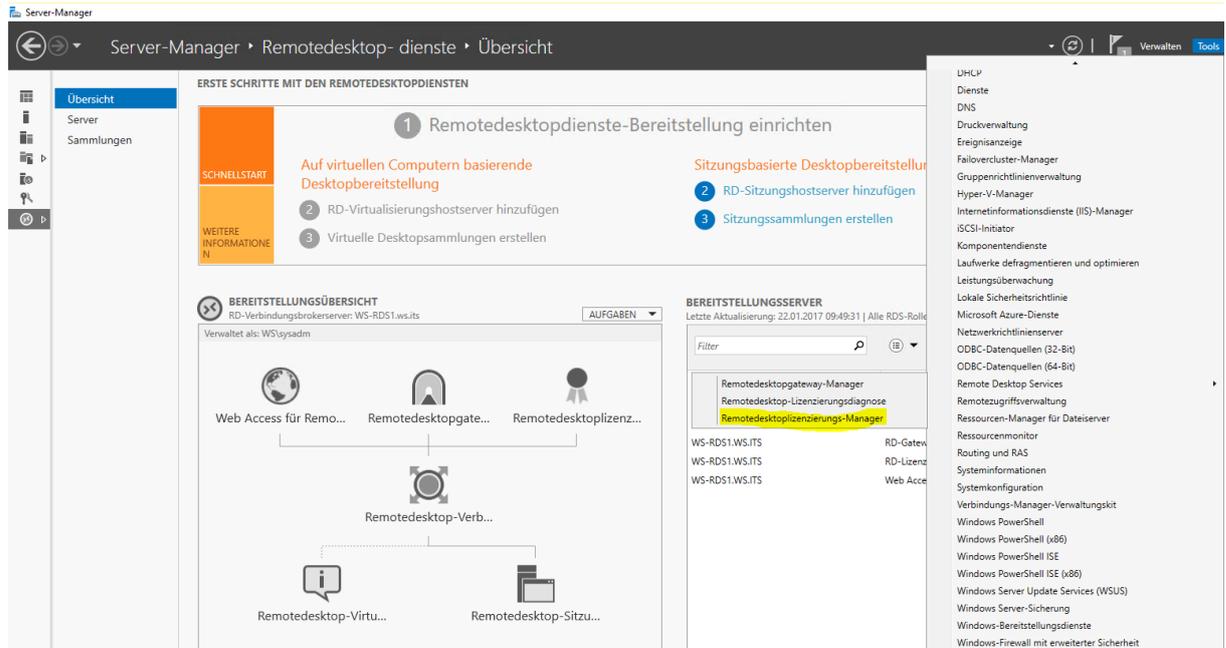


Damit ich den Lizenzserver des RDS aktivieren kann, muss ich das Windows Server 2016 Betriebssystem noch eben aktivieren:

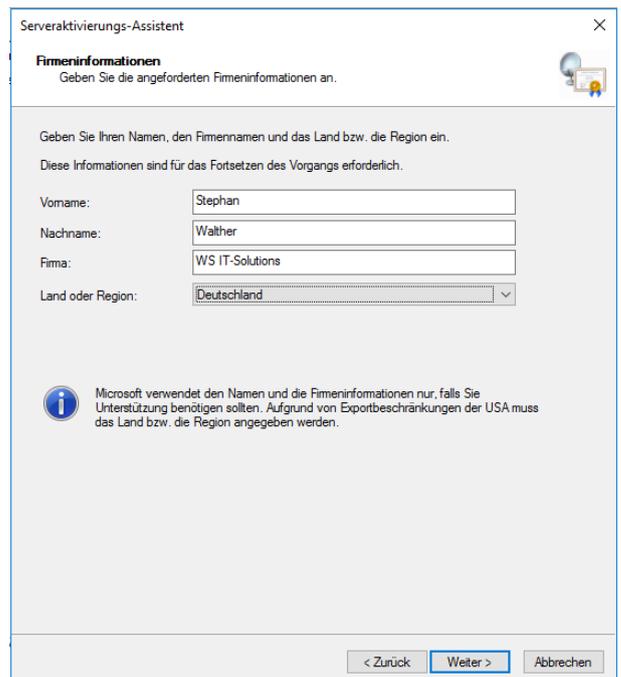
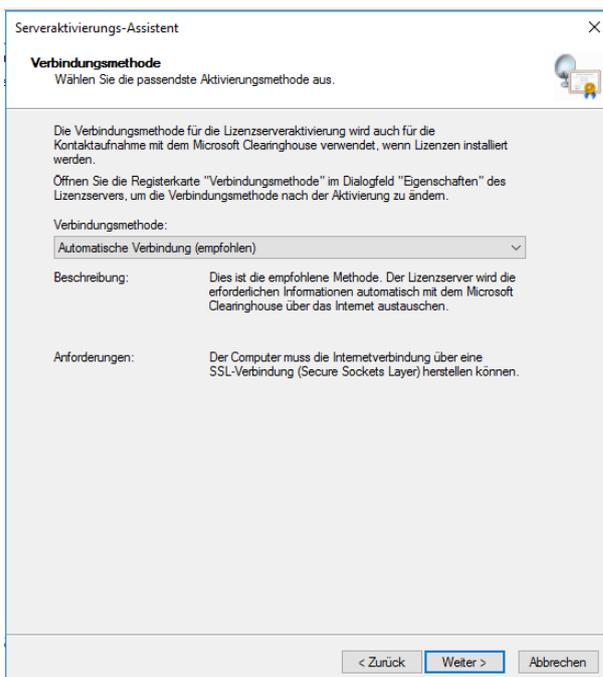
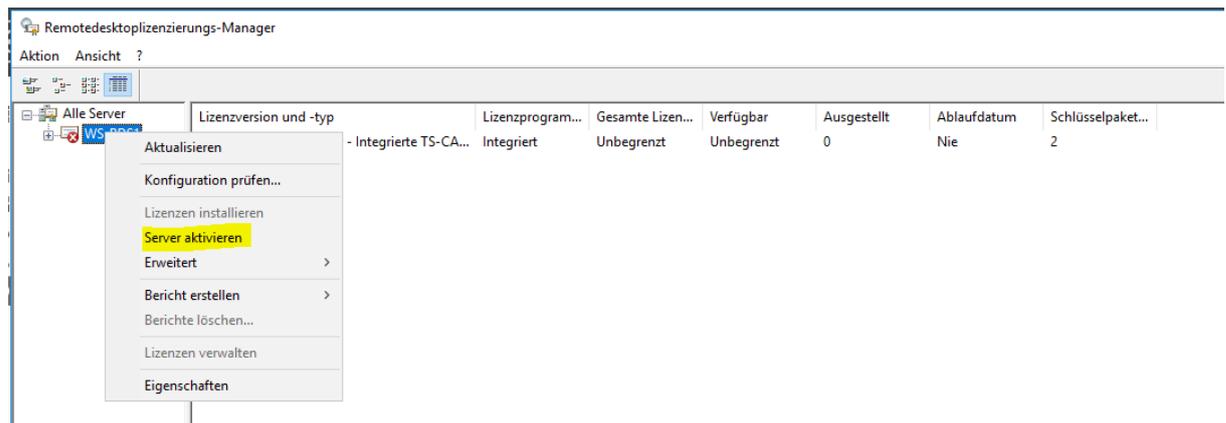


Konfiguration der Lizenzierung – Migration der bestehenden CALs

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:



Serveraktivierungs-Assistent

Firmeninformationen
Geben Sie diese optionalen Informationen ein.

E-Mail:

Organisationseinheit:

Firmenadresse:

Ort:

Bundesland/Kanton:

PLZ:

 Die optionalen Informationen werden nur von Microsoft-Supportspezialisten verwendet, falls Sie Unterstützung benötigen sollten.

< Zurück **Weiter >** Abbrechen

Serveraktivierungs-Assistent

Fertigstellen des Assistenten

Der Assistent zur Serveraktivierung wurde erfolgreich abgeschlossen.

Status:
Der Lizenzserver wurde aktiviert.
Klicken Sie auf "Weiter", um Lizenzen zu installieren.

Deaktivieren Sie das Kontrollkästchen "Assistent für die Lizenzinstallation starten", und klicken Sie anschließend auf "Fertig stellen", um die Lizenzinstallation zu verschieben.

Assistent für die Lizenzinstallation starten

< Zurück **Weiter >** Abbrechen

Danach lasse ich automatisch den Lizenzinstallations-Assistenten starten:

Serveraktivierungs-Assistent

Willkommen

Mit diesem Assistenten können Sie Lizenzen auf dem Remotedesktop-Lizenzserver installieren.

Sie benötigen Ihre Lizenzverbinformationen (z.B. Lizenznummer der Verkaufsversion oder der Volumenlizenz), um diesen Assistenten abzuschließen.

Lizenzereinstellungen

Aktiviert für: WS IT-Solutions

Verbindungsmethode: Automatische Verbindung (empfohlen)

Lizenzprogramm: Vollprodukterwerb

Klicken Sie auf "Abbrechen", und öffnen Sie dann im Dialogfeld "Eigenschaften" des Lizenzservers die Registerkarte "Verbindungsmethode", um die Verbindungsmethode zu ändern.

< Zurück **Weiter >** Abbrechen

Serveraktivierungs-Assistent

Lizenzprogramm
Wählen Sie das passende Lizenzprogramm aus.

Jeder Client, von dem eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder einem virtuellen Desktop in einer Microsoft Virtual Desktop Infrastructure hergestellt wird, muss eine gültige Lizenz haben. Wählen Sie das Lizenzprogramm aus, über das Sie die Lizenzen erworben haben.

Lizenzprogramm:

Beschreibung: Diese Lizenz wird in vordefinierten Mengen im Einzelhandel oder bei einem anderen Händler erworben. Diese Verpackung ist möglicherweise mit "Microsoft Windows Client License Pack" bezeichnet.

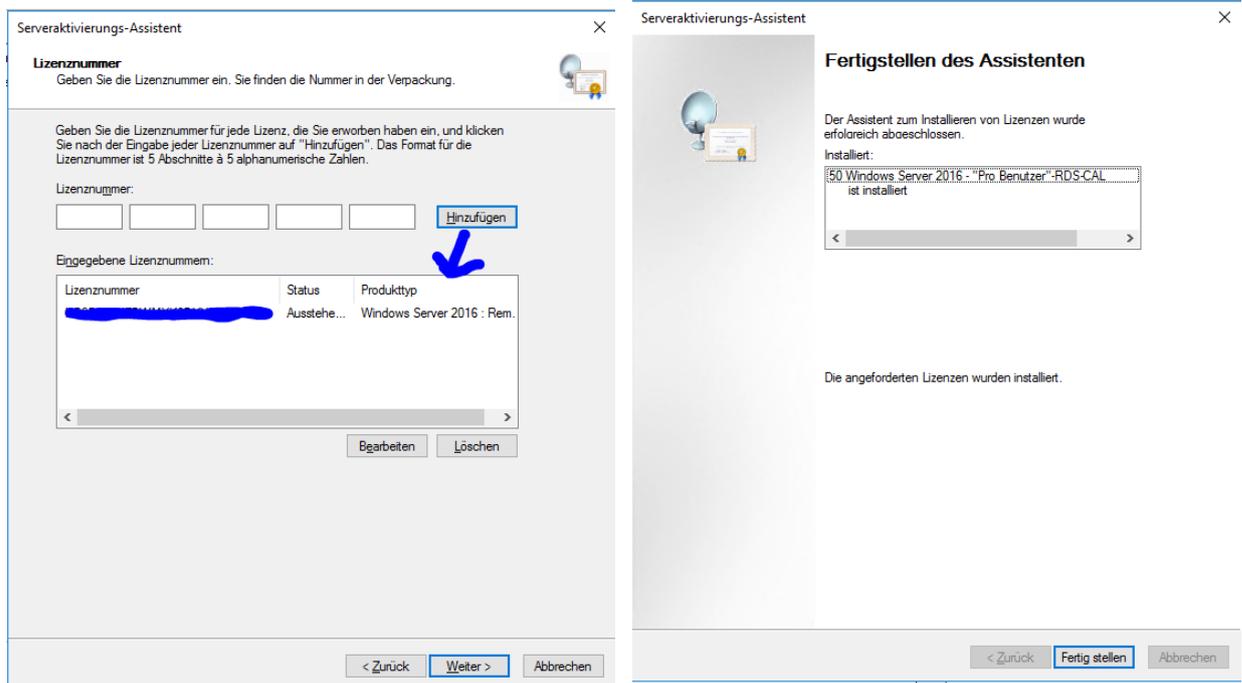
Format und Pfad: Die im Lizenzpaket enthaltene Lizenznummer ist erforderlich. Das Format für die Lizenznummer ist 5 Sätze à 5 alphanumerischen Zahlen.

Beispiel:

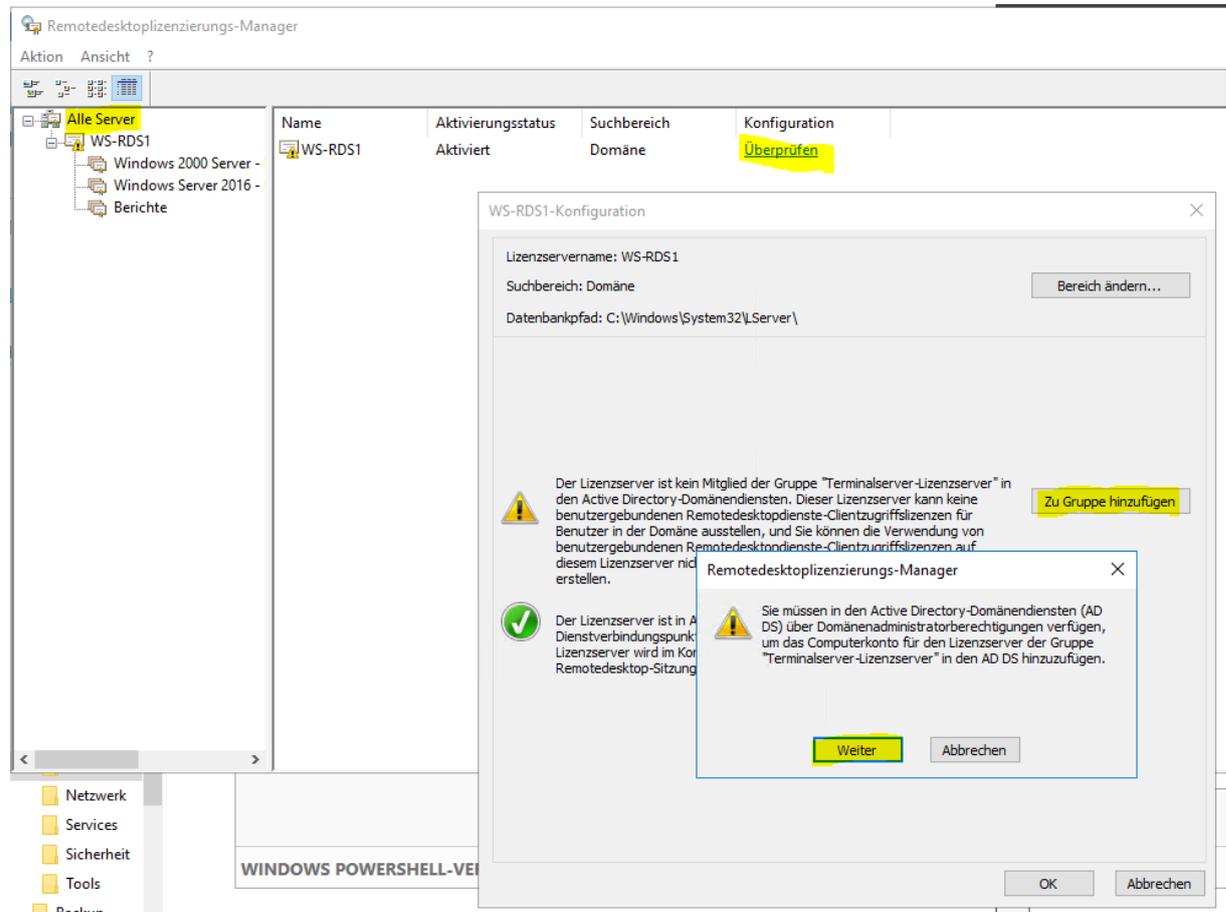
Stellen Sie sicher, dass die Lizenzinformationen dem Beispiel entsprechen, bevor Sie den Vorgang fortsetzen.

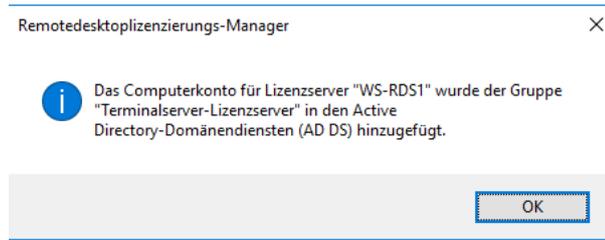
< Zurück **Weiter >** Abbrechen

Ich installiere 50 neue CALs für Windows Server 2016:

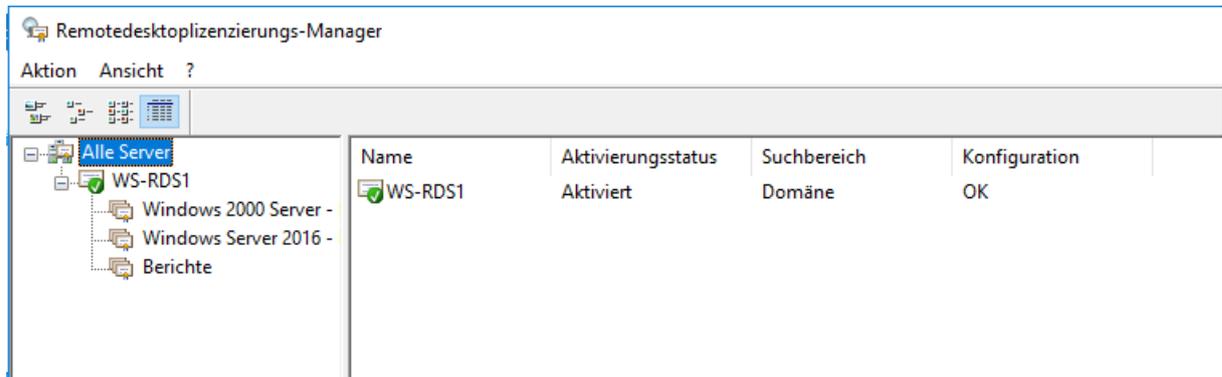


Ich starte nun die Serverprüfung. Dabei stellt das System fest, dass eine Gruppenmitgliedschaft im AD fehlt. Diese kann direkt über den Assistenten nachgeholt werden:

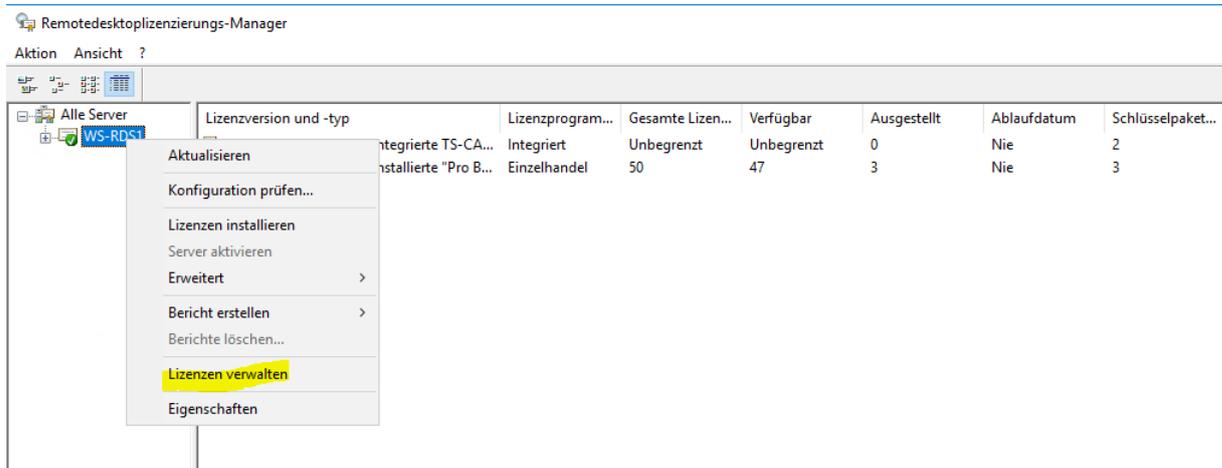




Der LIMA ist nun einsatzbereit:



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:



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

i 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

w 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-rds2.ws.its

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

Auch hier müssen die CAL-Schlüssel eingegeben werden:

Assistent zum Verwalten von Lizenzen

Lizenzprogramm
Wählen Sie das passende Lizenzprogramm aus.

Jeder Client, von dem eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder einem virtuellen Desktop in einer Microsoft Virtual Desktop Infrastructure hergestellt wird, muss eine gültige Lizenz haben. Wählen Sie das Lizenzprogramm aus, über das Sie die Lizenzen erworben haben.

Lizenzprogramm: Vollprodukterwerb

Beschreibung: Diese Lizenz wird in vordefinierten Mengen im Einzelhandel oder bei einem anderen Händler erworben. Diese Verpackung ist möglicherweise mit "Microsoft Windows Client License Pack" bezeichnet.

Format und Pfad: Die im Lizenzpaket enthaltene Lizenznummer ist erforderlich. Das Format für die Lizenznummer ist 5 Sätze à 5 alphanumerischen Zahlen.

Beispiel: 1A2B3 1A2B3 1A2B3 1A2B3 1A2B3

Stellen Sie sicher, dass die Lizenzinformationen dem Beispiel entsprechen, bevor Sie den Vorgang fortsetzen.

< Zurück Weiter > Abbrechen

Assistent zum Verwalten von Lizenzen

Lizenznummer
Geben Sie die Lizenznummer ein. Sie finden die Nummer in der Verpackung.

Geben Sie die Lizenznummer für jede Lizenz, die Sie erworben haben ein, und klicken Sie nach der Eingabe jeder Lizenznummer auf "Hinzufügen". Das Format für die Lizenznummer ist 5 Abschnitte à 5 alphanumerische Zahlen.

Lizenznummer:

Hinzufügen

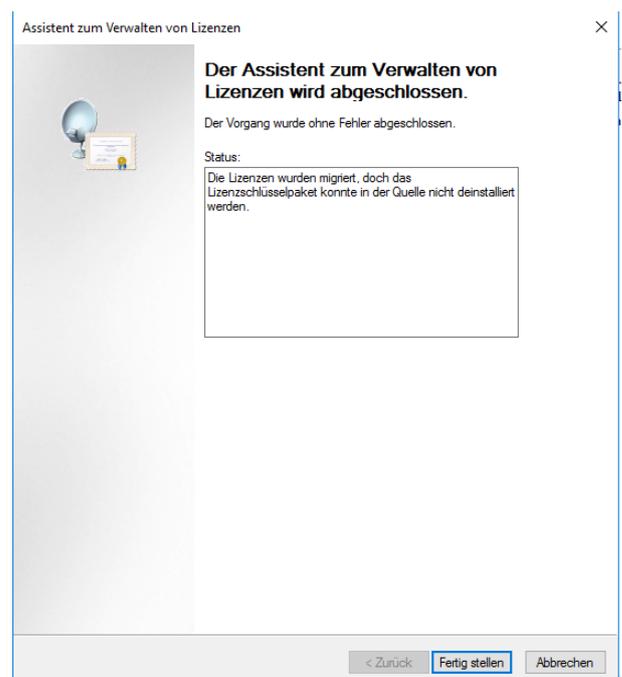
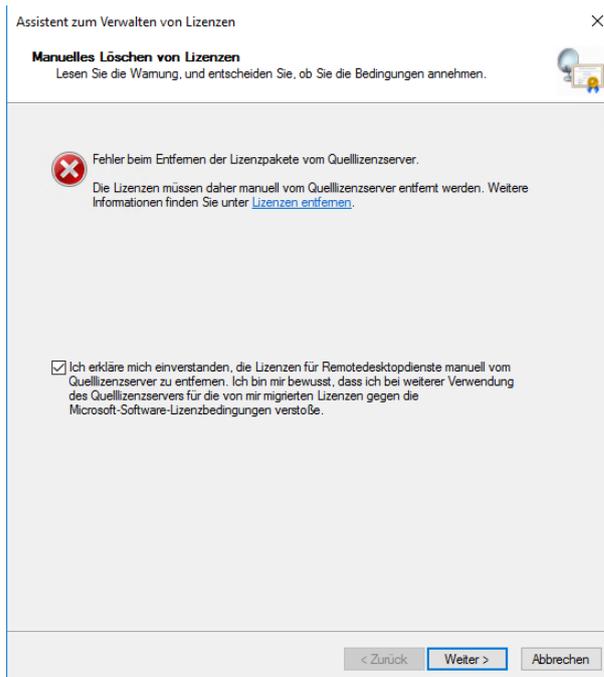
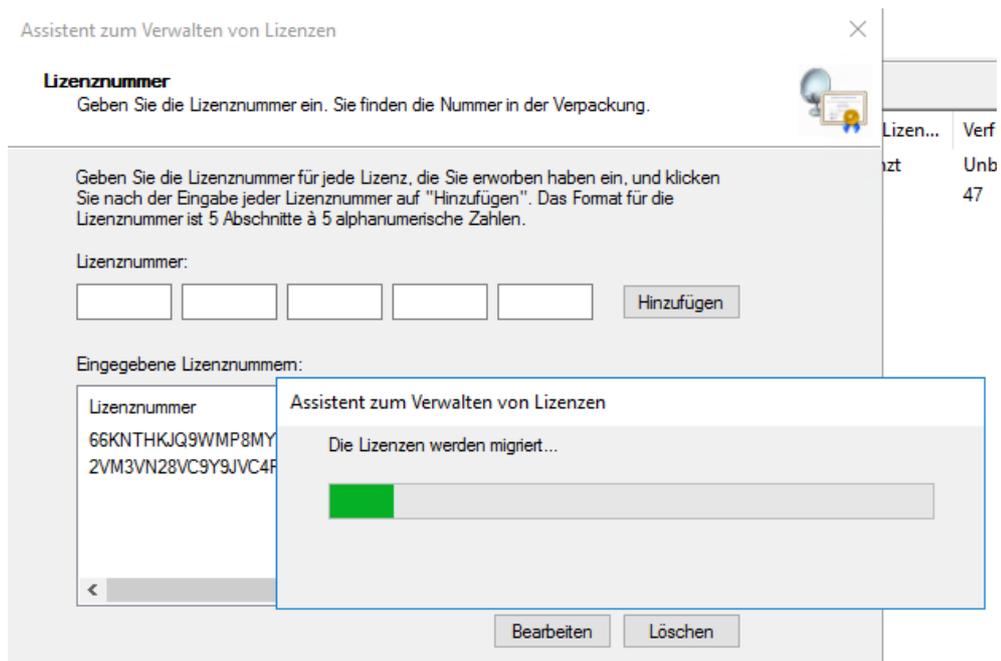
Eingegebene Lizenznummern:

Lizenznummer	Status	Produkttyp
[blurred]	Ausstehend	Windows Server 2012
[blurred]	Ausstehend	Windows Server 2012

Bearbeiten Löschen

< Zurück Weiter > Abbrechen

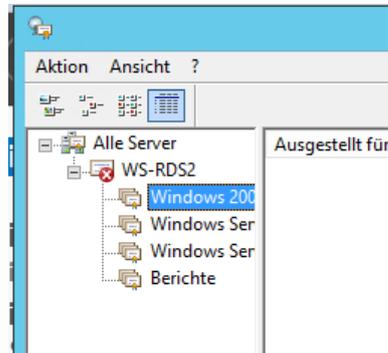
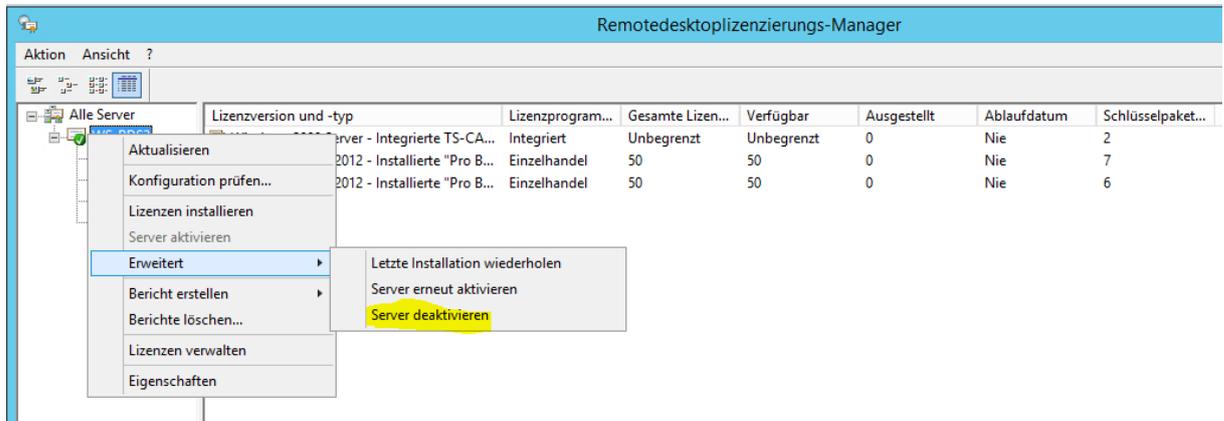
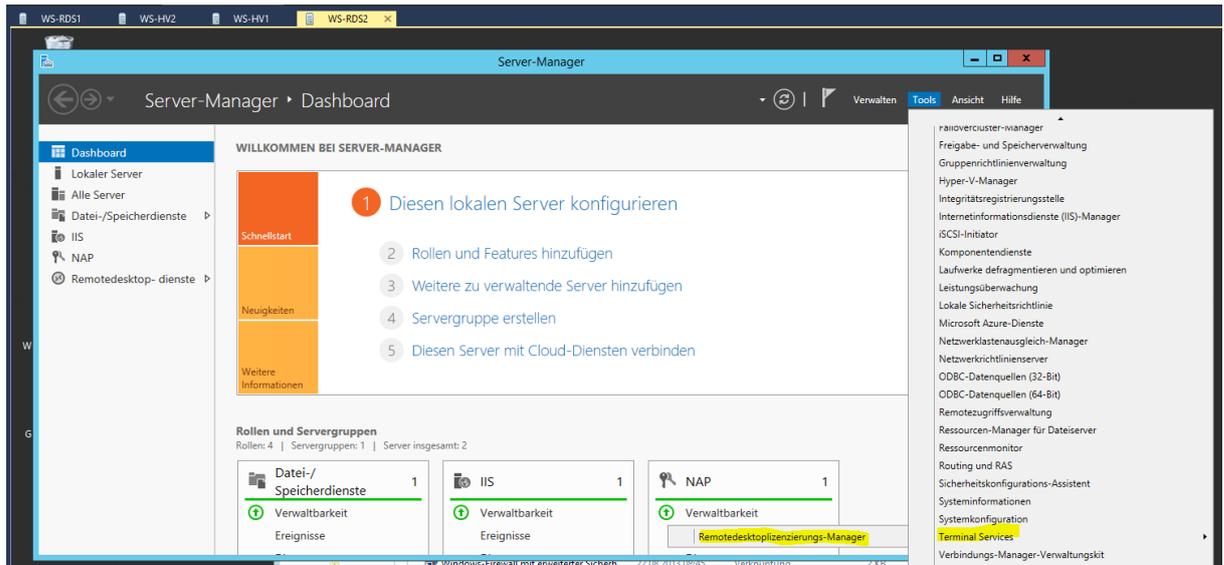
Die Übertragung der CALs läuft:



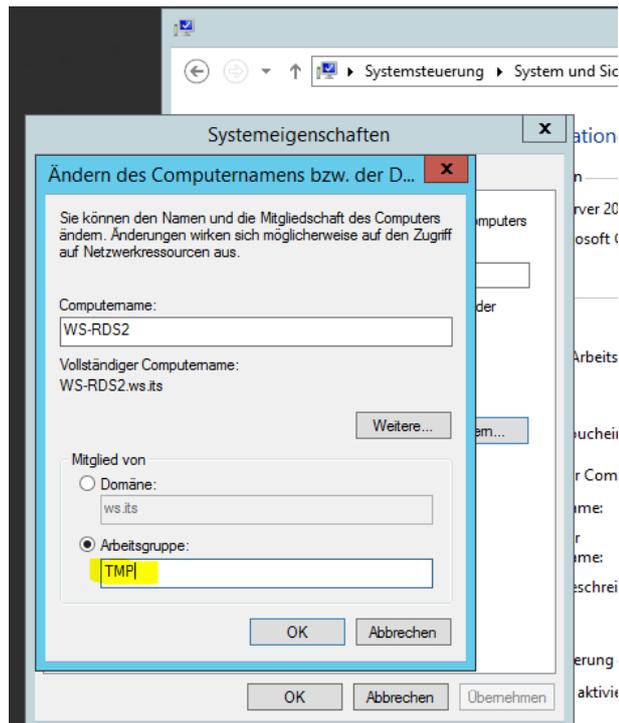
Beim Übertragen ist ein Fehler aufgetreten. Die CALs können dennoch eingespielt werden, wenn ich sicherstelle, dass der alte Server nicht weiter über die CALs verfügen kann:

Aktion	Ansicht	?	Lizenzversion und -typ	Lizenzprogramm...	Gesamte Lizen...	Verfügbar	Ausgestellt	Ablaufdatum	Schlüsselpaket...
			Windows 2000 Server - Integrierte TS-CA...	Integriert	Unbegrenzt	Unbegrenzt	0	Nie	2
			Windows Server 2012 - Installierte "Pro B...	Einzelhandel	100	100	0	Nie	4
			Windows Server 2016 - Installierte "Pro B...	Einzelhandel	50	47	3	Nie	3

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:



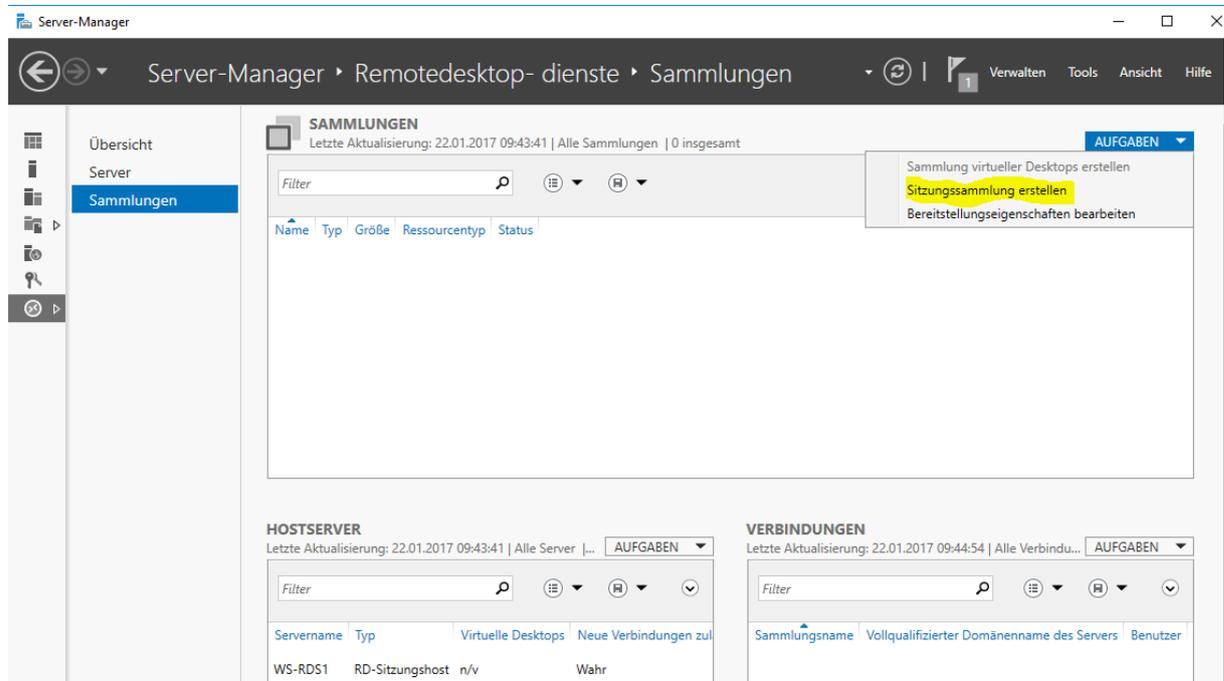
Jetzt entferne ich den alten WS-RDS2 aus der Domäne:



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:

Sammlung erstellen

Namen für die Sammlung angeben

Vorbemerkungen
Sammlungsname
 Remotedesktop-Sitzungs...
 Benutzergruppen
 Benutzerprofil-Datenträger
 Bestätigung
 Status

Für Benutzer wird bei der Anmeldung beim Server mit Web Access für Remotedesktop der Sammlungsname "session" angezeigt.

Name:

Beschreibung (optional):

< Zurück Weiter > Erstellen Abbrechen

Sammlung erstellen

RD-Sitzungshostserver angeben

Vorbemerkungen
 Sammlungsname
Remotedesktop-Sitzungs...
 Benutzergruppen
 Benutzerprofil-Datenträger
 Bestätigung
 Status

Wählen Sie die RD-Sitzungshostserver im Serverpool aus, die dieser Sammlung hinzugefügt werden sollen.

Serverpool

Filter:

Name	IP-Adresse	Betrieb
WS-RDS1.ws.its		

1 Computer gefunden

Ausgewählt

Computer

- ▲ WS.ITS (1)
- WS-RDS1

1 Computer ausgewählt

< Zurück Weiter > Erstellen Abbrechen

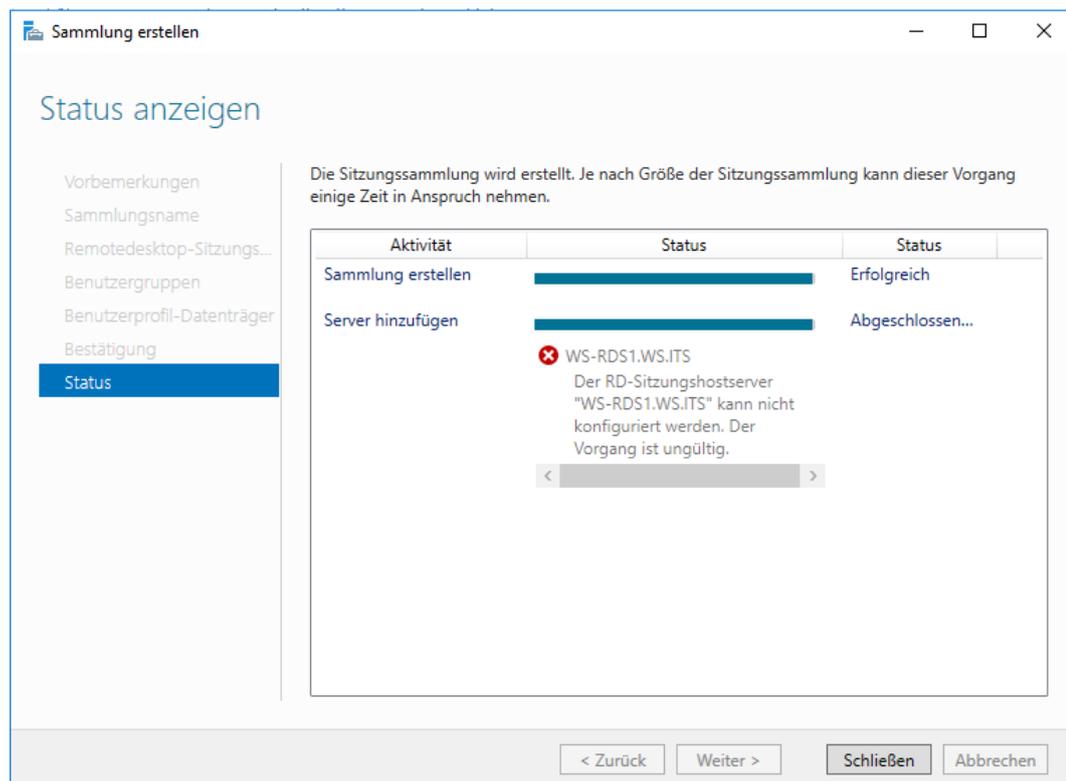
The screenshot shows the 'Sammlung erstellen' wizard at the 'Benutzergruppen angeben' step. The left sidebar contains a list of steps: 'Vorbemerkungen', 'Sammlungsname', 'Remotedesktop-Sitzungs...', 'Benutzergruppen' (highlighted), 'Benutzerprofil-Datenträger', 'Bestätigung', and 'Status'. The main area has the title 'Benutzergruppen angeben' and the instruction 'Fügen Sie die Benutzergruppen hinzu, die Zugriff auf die Sammlung haben sollen.' Below this is a list box labeled 'Benutzergruppen:' containing 'WS\Domänen-Benutzer'. To the right of the list box are two buttons: 'Hinzufügen...' and 'Entfernen'. At the bottom of the wizard are four buttons: '< Zurück', 'Weiter >', 'Erstellen', and 'Abbrechen'.

Den Benutzerprofil-Datenträger konfiguriere ich später:

The screenshot shows the 'Sammlung erstellen' wizard at the 'Benutzerprofil-Datenträger angeben' step. The left sidebar contains a list of steps: 'Vorbemerkungen', 'Sammlungsname', 'Remotedesktop-Sitzungs...', 'Benutzergruppen', 'Benutzerprofil-Datenträger' (highlighted), 'Bestätigung', and 'Status'. The main area has the title 'Benutzerprofil-Datenträger angeben' and the instruction 'Benutzerprofil-Datenträger speichern Benutzerprofileinstellungen und -daten an einem zentralen Speicherort für die Sammlung.' Below this is a checkbox labeled 'Benutzerprofil-Datenträger aktivieren' which is currently unchecked. Underneath is a text box labeled 'Speicherort von Benutzerprofil-Datenträgern:'. Below that is a label 'Maximale Größe (in GB):' followed by a text box containing the value '20'. At the bottom of the wizard are four buttons: '< Zurück', 'Weiter >', 'Erstellen', and 'Abbrechen'. A blue information icon is present at the bottom left of the main area.

i Die Server in der Sammlung müssen über Vollzugriffsberechtigungen für die Benutzerprofil-Datenträgerfreigabe verfügen, und der aktuelle Benutzer muss ein Mitglied der lokalen Gruppe "Administratoren" auf dem Server sein.

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:

The screenshot shows the Server-Manager console with the following sections:

- EIGENSCHAFTEN** (Properties):

Sammlungstyp	Sitzung
Ressourcen	Remotedesktop
Benutzergruppe	WS\Domänen-Benutzer
- REMOTEAPP-PROGRAMME** (RemoteApp Programs):

Veröffentlichte RemoteApp-Programme | 0 insgesamt

Der Remotedesktop wurde für die Benutzer der Sammlung veröffentlicht.

[RemoteApp-Programme veröffentlichen](#)

Die Veröffentlichung von RemoteApp-Programmen hat die Aufhebung der Veröffentlichung des Remotedesktops zur Folge.
- HOSTSERVER** (Host Servers):

Letzte Aktualisierung: 22.01.2017 10:11:52 | Alle Server | 1...

Servername	Typ	Virtuelle Desktops	Neue Verbindungen zula
WS-RDS1	RD-Sitzungshost	n/v	Wahr

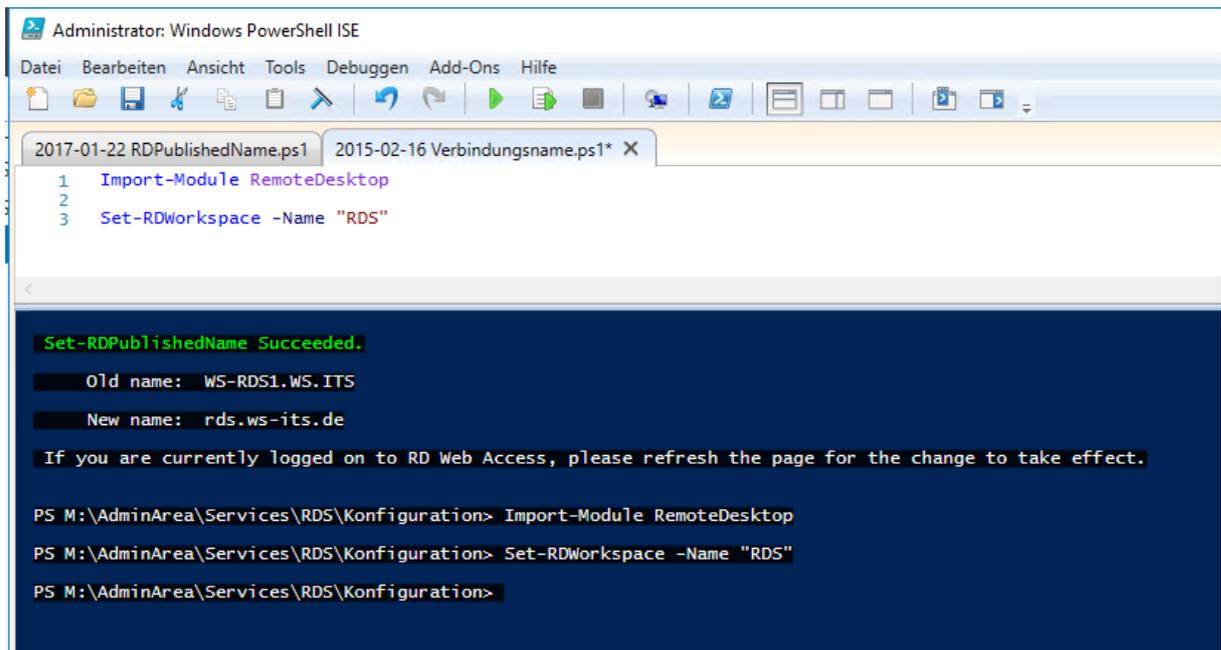
Der Server soll sich später beim Aufruf nicht mit seinem internen Namen, sondern mit dem externen Namen verwenden. Dafür gibt es in der PowerShell Script Gallery bei Microsoft ein Script, das den Zugriffsnamen ändert:

```

Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
2016-08-25 RDPublishedName.ps1 X
1 Import-Module RemoteDesktop
2 cd M:\AdminArea\Services\RDS\Konfiguration
3
4 .\Set-RDPublishedName.ps1 -ClientAccessName rds.ws-its.de -ConnectionBroker ws-rds1.ws.its

Set-RDPublishedName Succeeded.
Old name: WS-RDS1.WS.ITS
New name: rds.ws-its.de
If you are currently logged on to RD Web Access, please refresh the page for the change to take effect.
PS M:\AdminArea\Services\RDS\Konfiguration>
    
```

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:



```

Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe

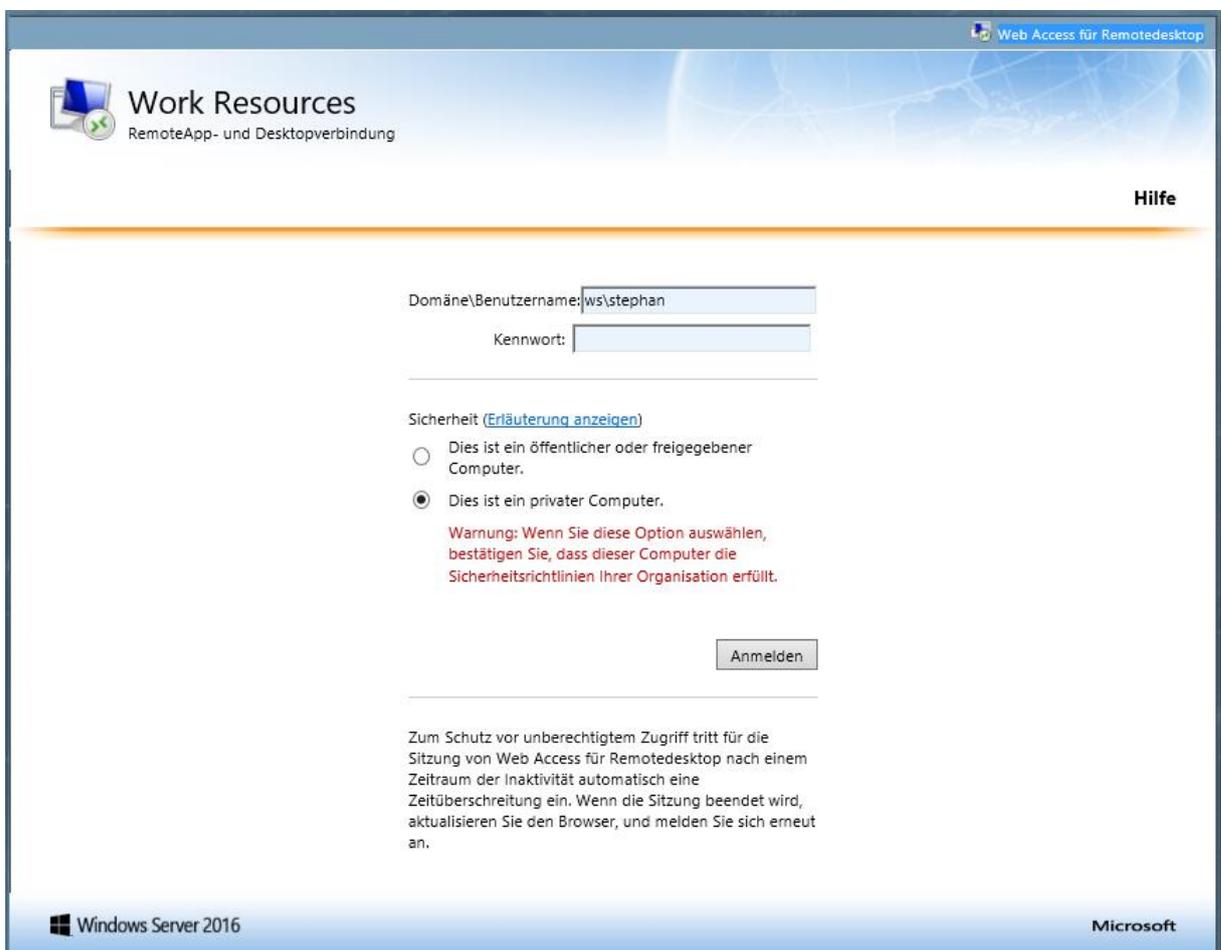
2017-01-22 RDPublishedName.ps1 2015-02-16 Verbindungsname.ps1* X
1 Import-Module RemoteDesktop
2
3 Set-RDWorkspace -Name "RDS"

Set-RDPublishedName Succeeded.
Old name: WS-RDS1.WS.ITS
New name: rds.ws-its.de
If you are currently logged on to RD Web Access, please refresh the page for the change to take effect.

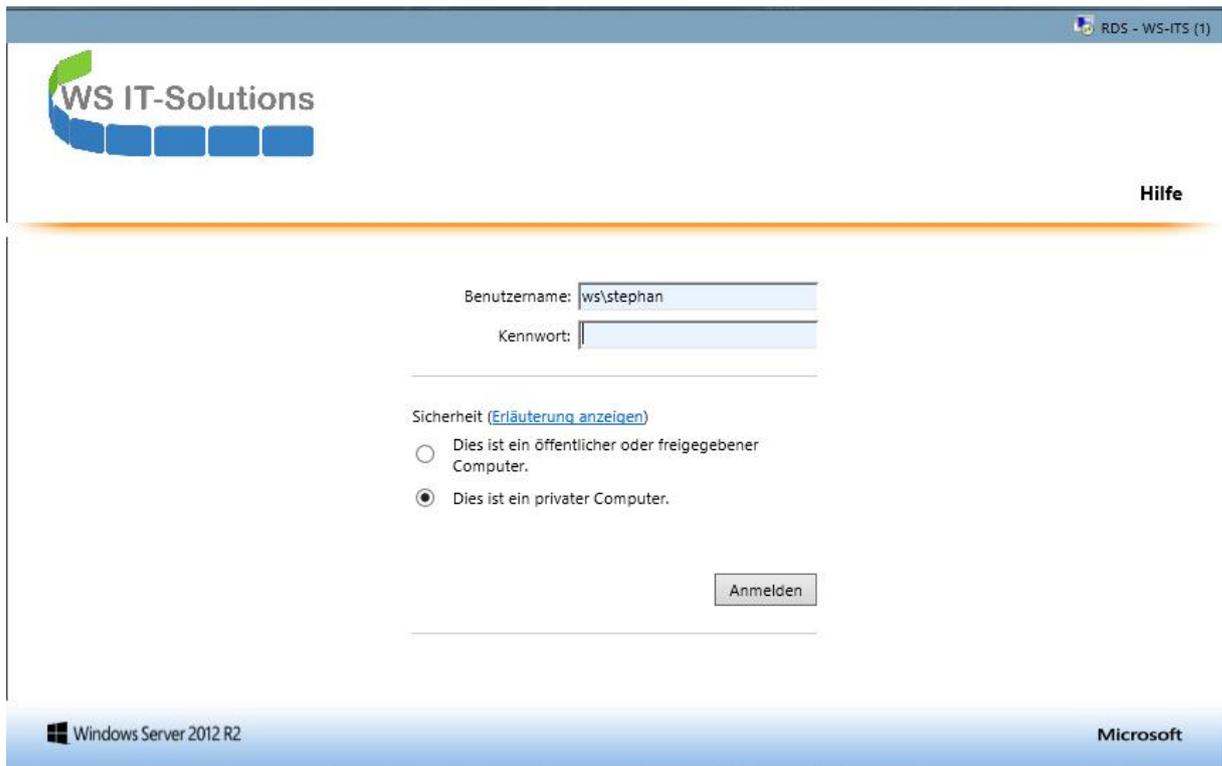
PS M:\AdminArea\Services\RDS\Konfiguration> Import-Module RemoteDesktop
PS M:\AdminArea\Services\RDS\Konfiguration> Set-RDWorkspace -Name "RDS"
PS M:\AdminArea\Services\RDS\Konfiguration>
  
```

Konfiguration der RDS-Website

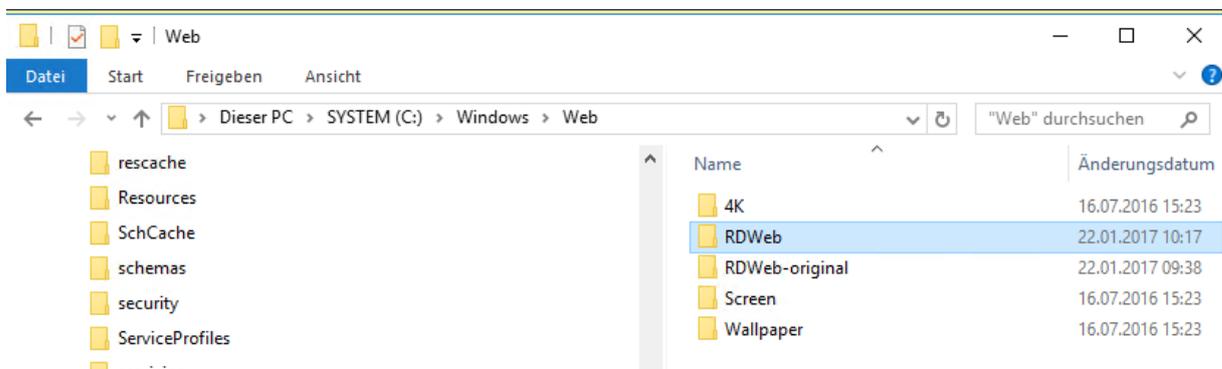
Das aktuelle Layout der RDS-Website hat Verbesserungsbedarf. Auf meinem alten RDS-Server hatte ich die Website bereits modifiziert. Ich tausche nun die Dateien unter dem IIS aus. Das ist vorher:



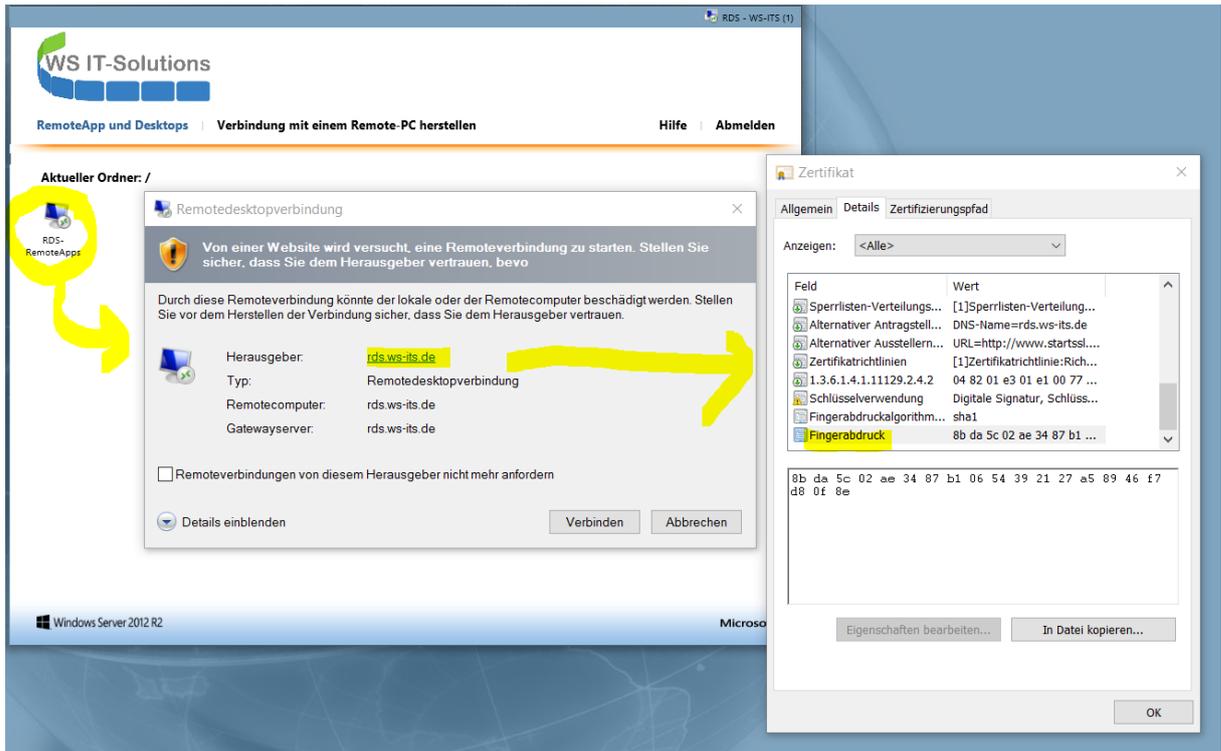
Und das ist nun die aktuelle Seite. Das Layout ist also kompatibel ☺:



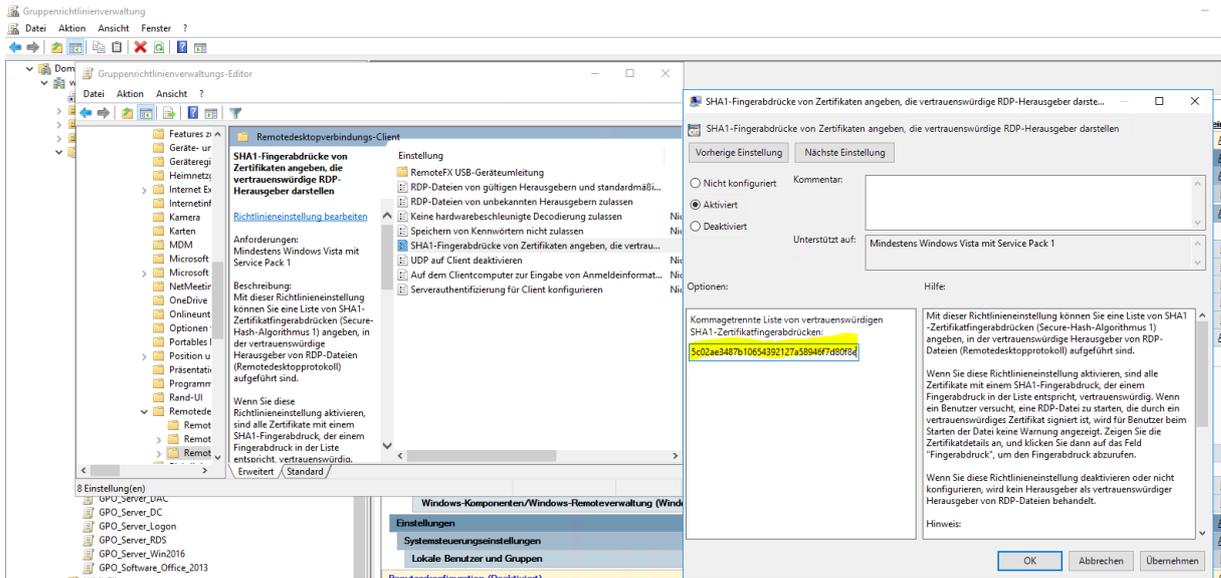
Hier liegt das Verzeichnis:



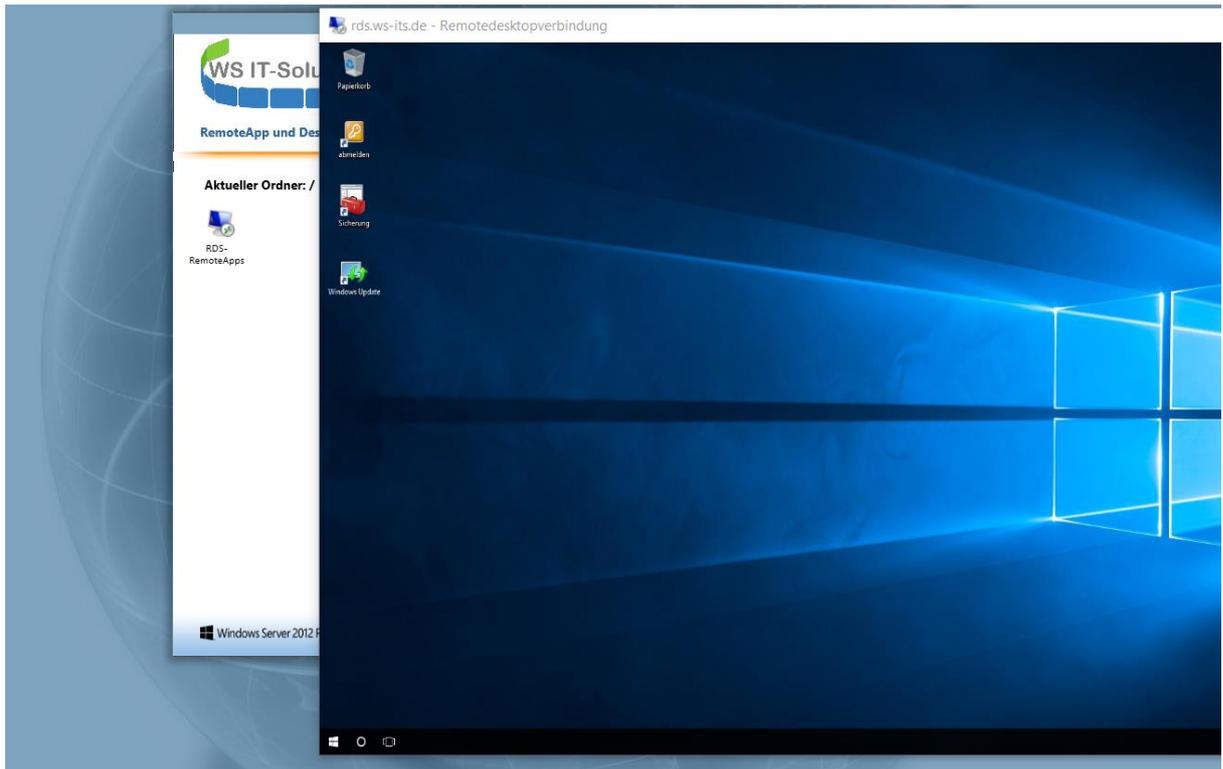
Ein Verbindungsaufbau zeigt aber, dass beim Start der RDP-Session eine Sicherheitsabfrage erscheint. Das Zertifikat ist zwar vertrauenswürdig, aber mein Client vertraut den rdp-Dateien noch nicht. Dies hatte ich bisher mit einer GPO erreicht, in der ich den Fingerabdruck des verwendeten Zertifikates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



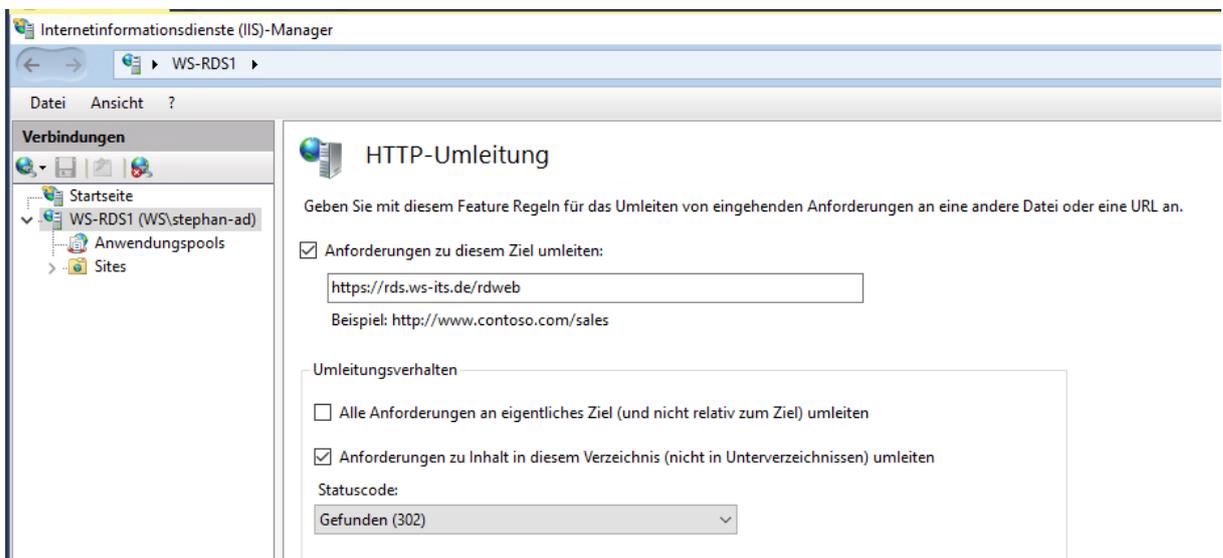
Das ist die GPO:



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

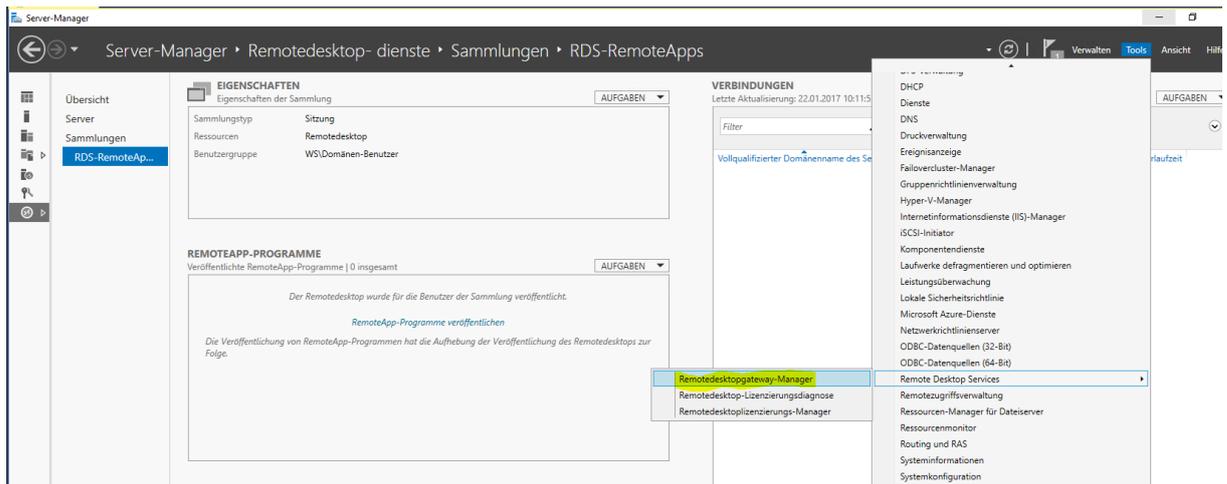


Nun noch etwas Bequemlichkeit: der Aufruf des Webportals benötigt die Angabe des Namens vom virtuellen Verzeichnis rdweb – es ist der Aufruf <https://rds.ws-its.de/rdweb> notwendig. Mit einer http-Redirect-Anweisung kann ich dem Benutzer ermöglichen, nur <https://rds.ws-its.de> aufzurufen:

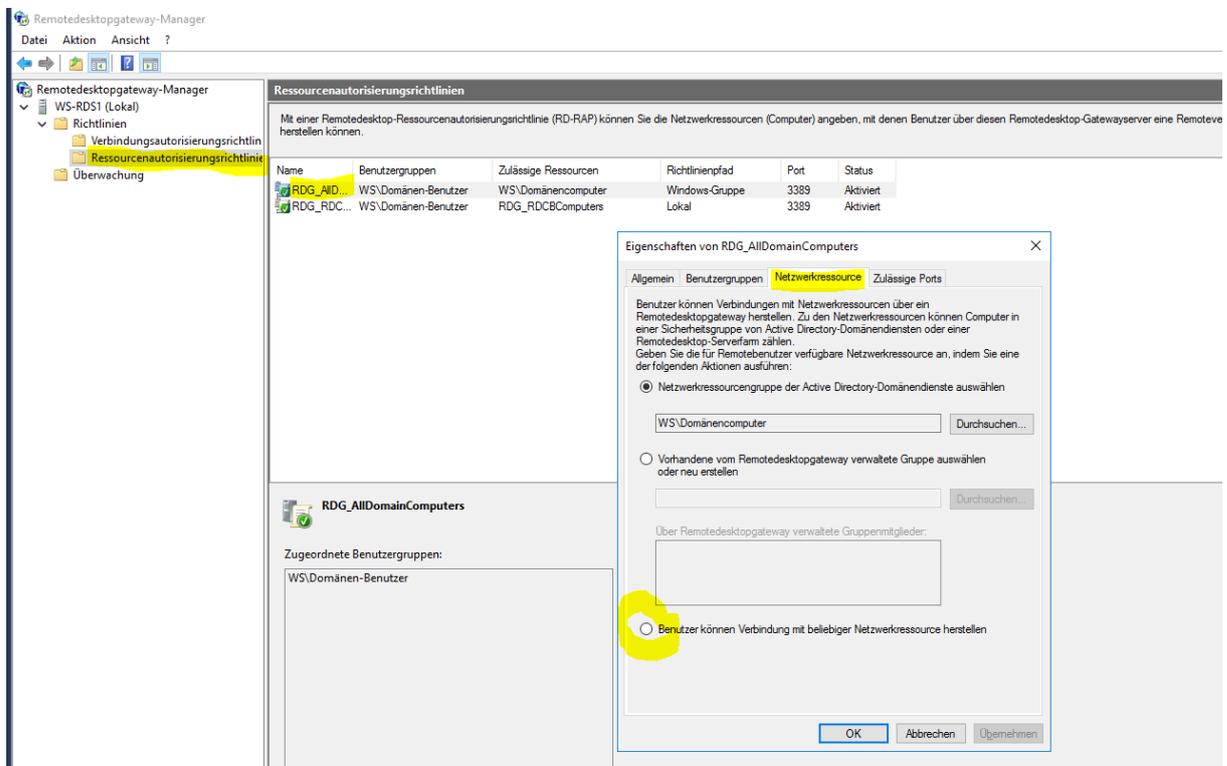


Konfiguration des RDS-Gateways

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

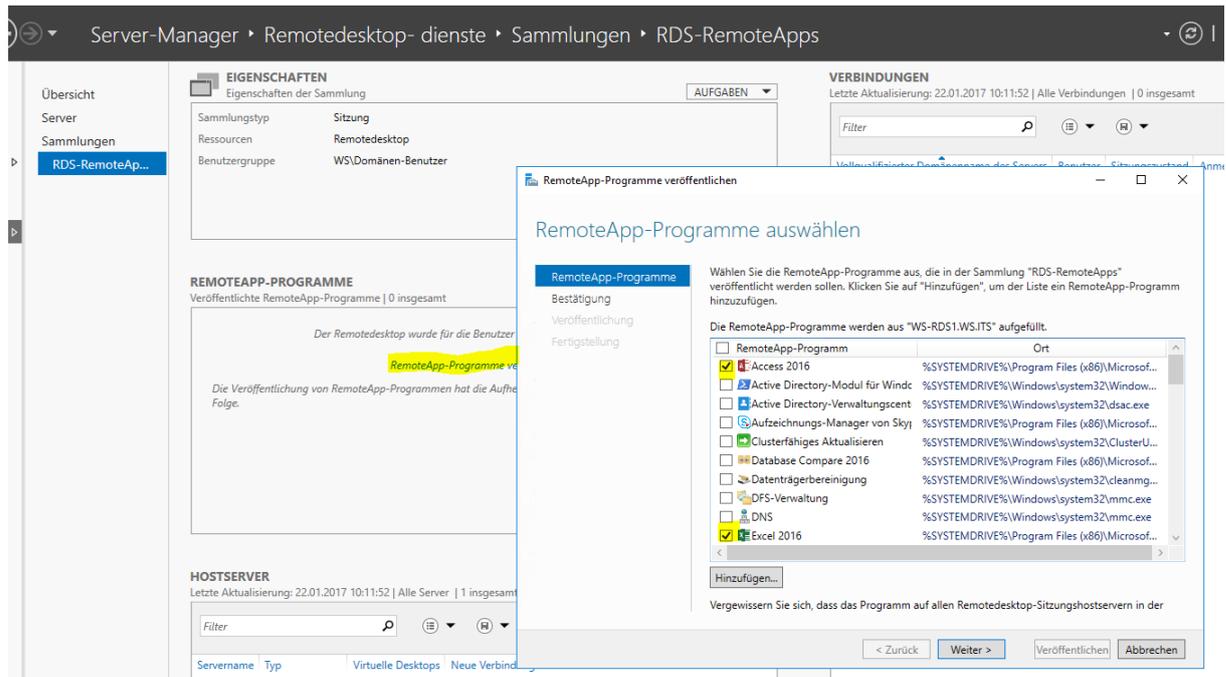


Hier werden ggf. Anpassungen bei den Autorisierungsrichtlinien notwendig, damit Benutzer eine RDP-Verbindung von außen über https aufbauen können:



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:

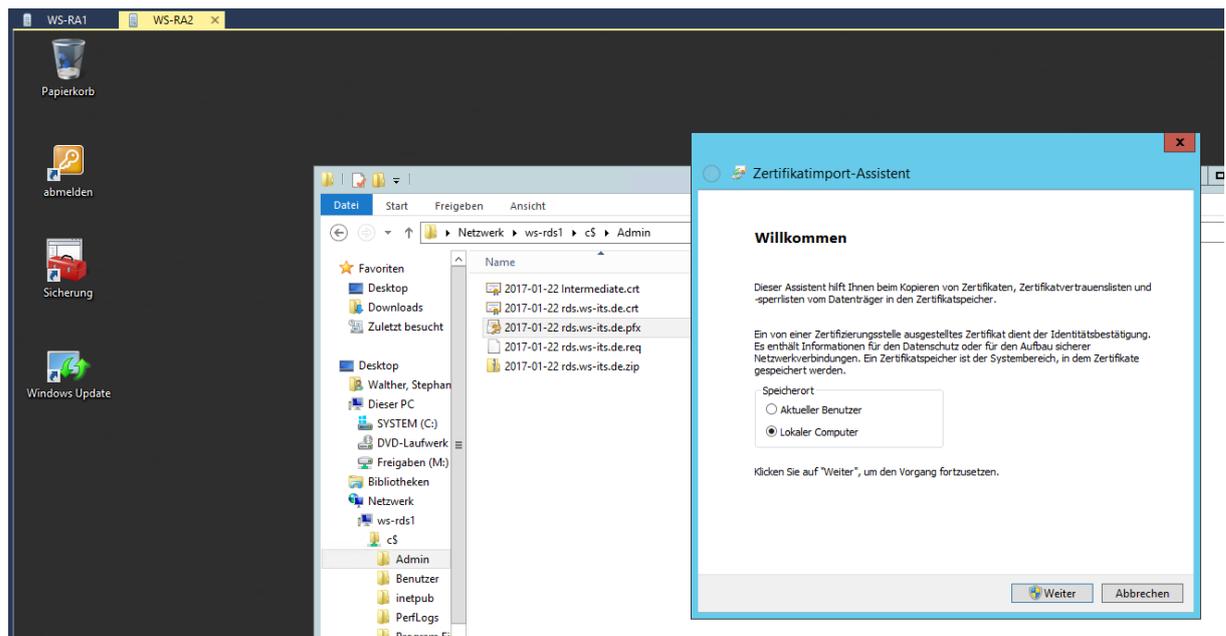


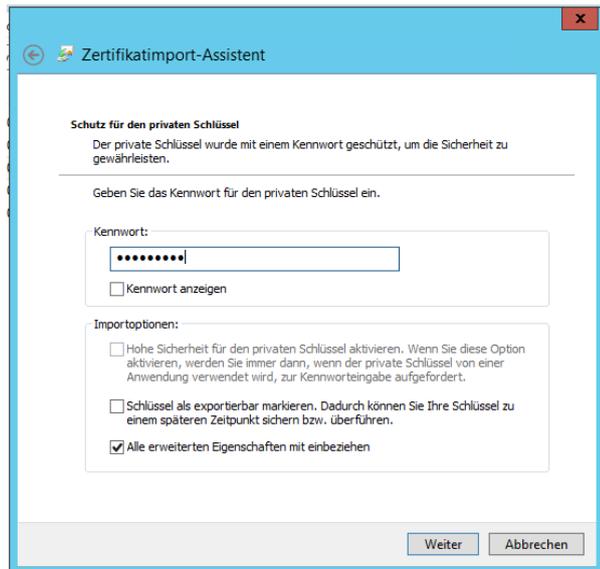
Konfiguration des Web Application Proxies

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 X
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

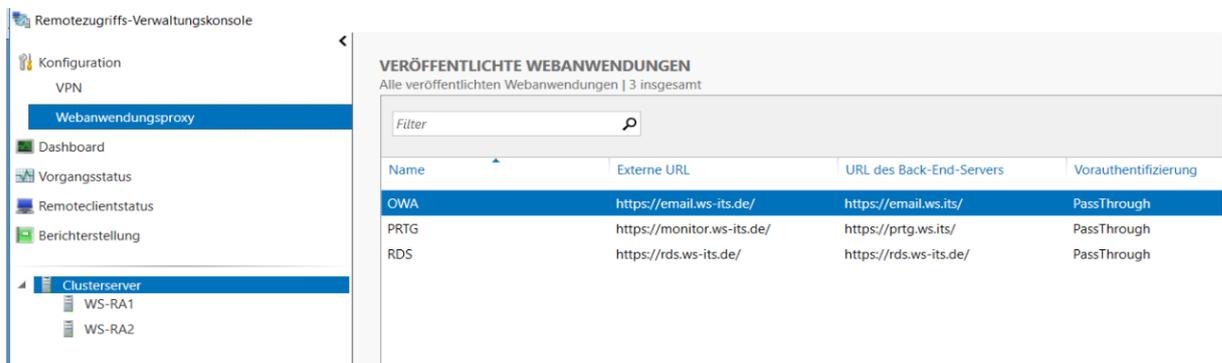
Thumbprint Subject NotBefore
-----
EAA63ABC7C2C6E1D544F75B0360469C55F399446 CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val... 19.10.2015 02:00:00
D60B05E28A7A1D322075444D56A88E0429921464 CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val... 19.07.2014 02:00:00
8BDASC02AE3487B10654392127A58946F7D80F8E CN=rds.ws-its.de, C=DE 22.01.2017 09:18:02
340580B9D51E7F1D2FBAD879EE1DC096C755F7EE CN=rds.ws-its.de, OU=PositiveSSL Tria], OU=Domain Contr... 22.06.2014 02:00:00

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

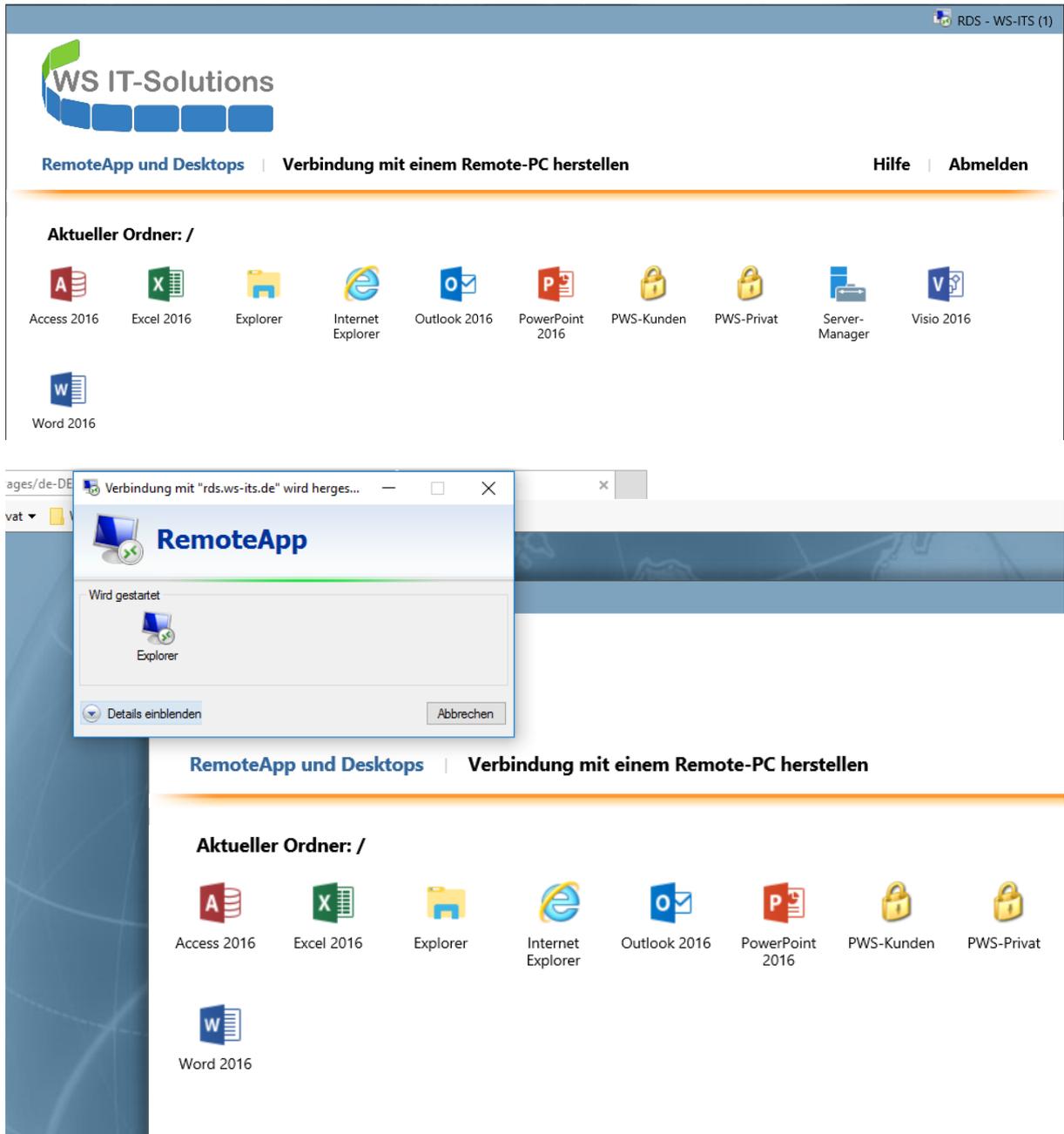
PS C:\windows\system32>

```

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

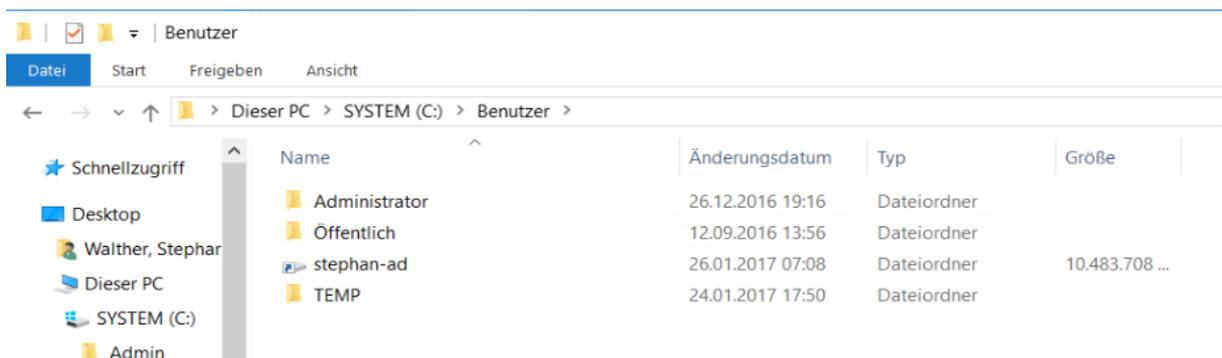


Ein Test von extern zeigt, dass nun sowohl das Web-Portal, als auch der Start der RemoteApps funktioniert:

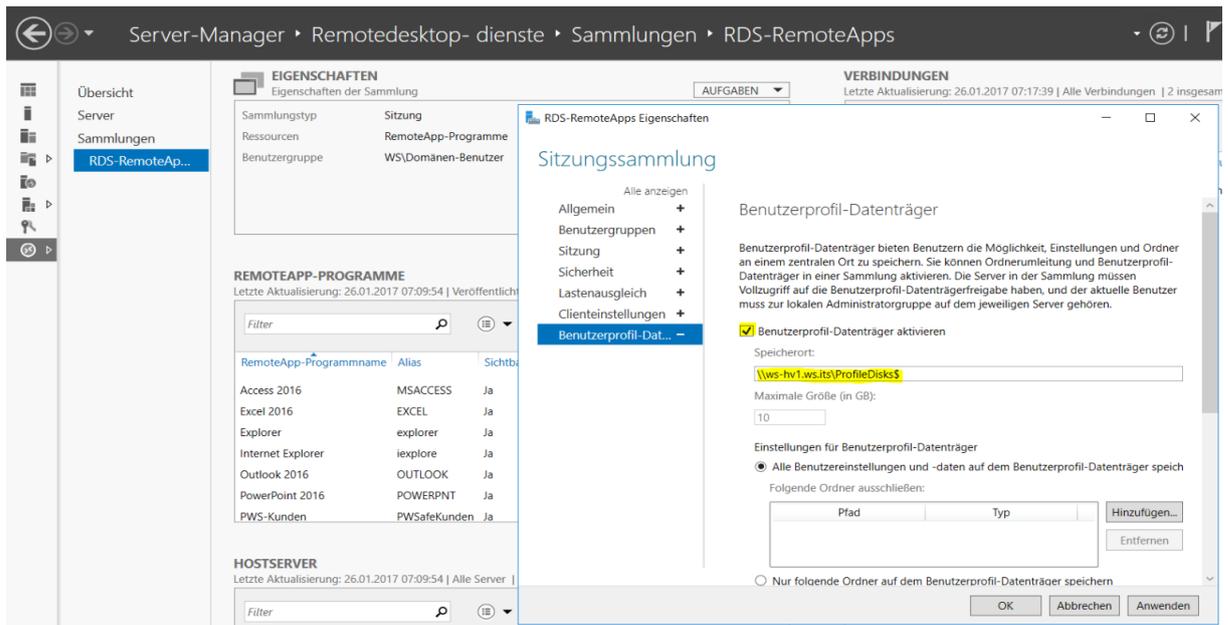


Konfiguration der Benutzerdatenträger

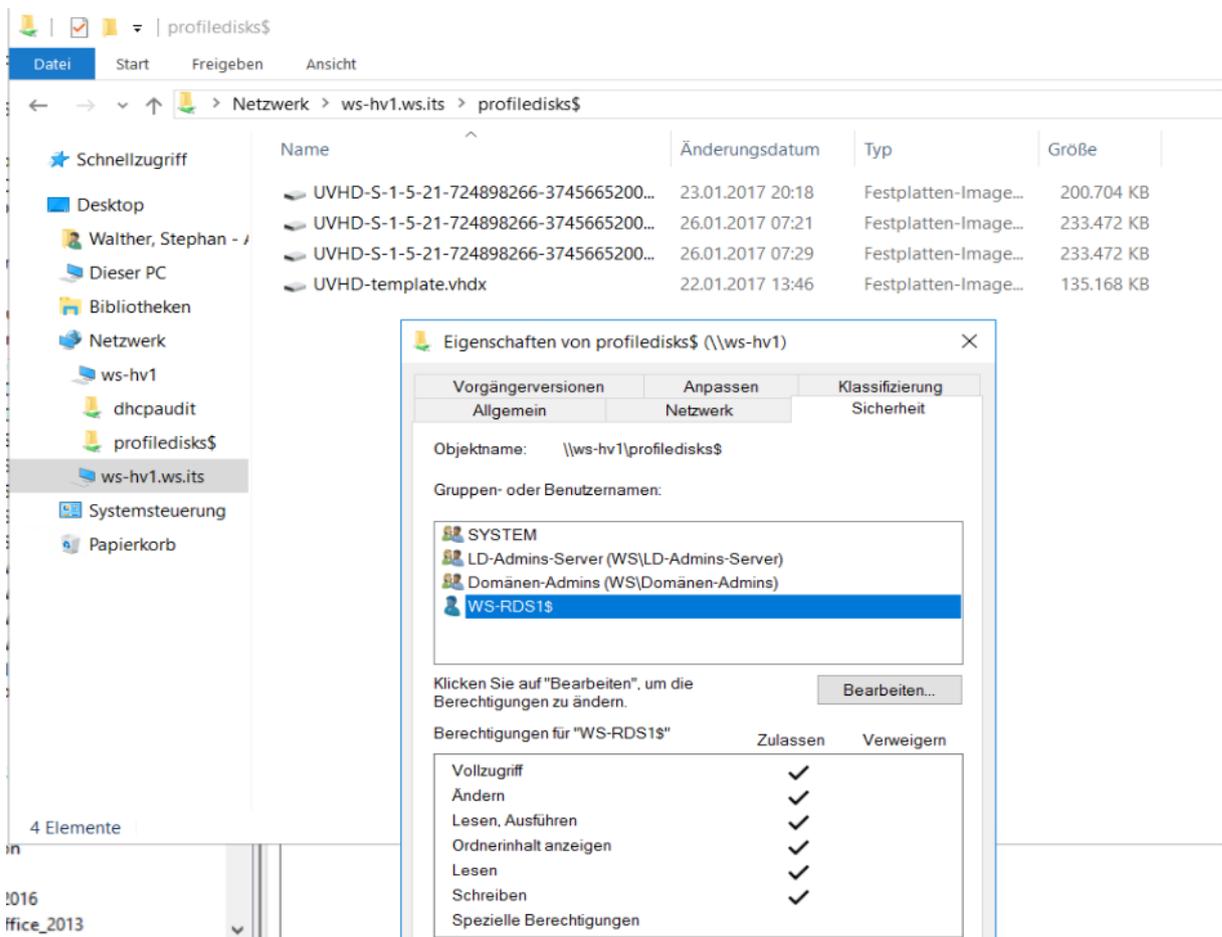
Der Benutzerdatenträger soll die Ladezeiten und den Speicherbedarf der Benutzerprofile minimieren, indem der Userstate in einer VHDX-Datei pro User gespeichert wird und diese bei der Anmeldung lokal als Benutzerprofilordner eingebunden wird:



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 unbekanntem Herausgeber 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/Internetssystemsteuerung/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-its.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 unbekanntem Herausgeber 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
Anwendungsisolierung	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:

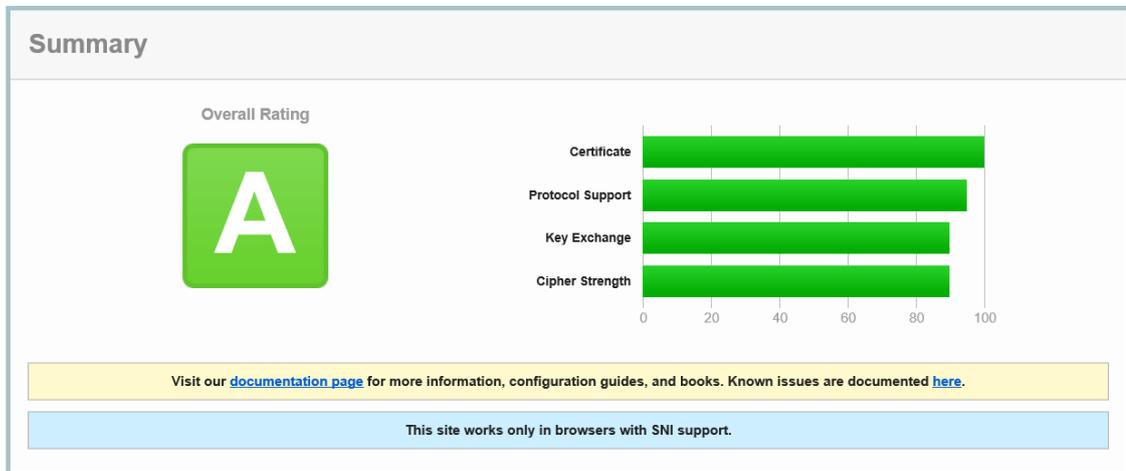
- es werden keine alten Webserver-Protokolle (SSLv1 bis SSLv3) verwendet
- TLS ist in der Version 1.2 aktiv
- Der unsichere Diffie-Hellman Key-Exchange ist nicht vorhanden
- Alle RC-Cipher sind deaktiviert

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 08:36:16 UTC | [Hide](#) | [Clear cache](#)

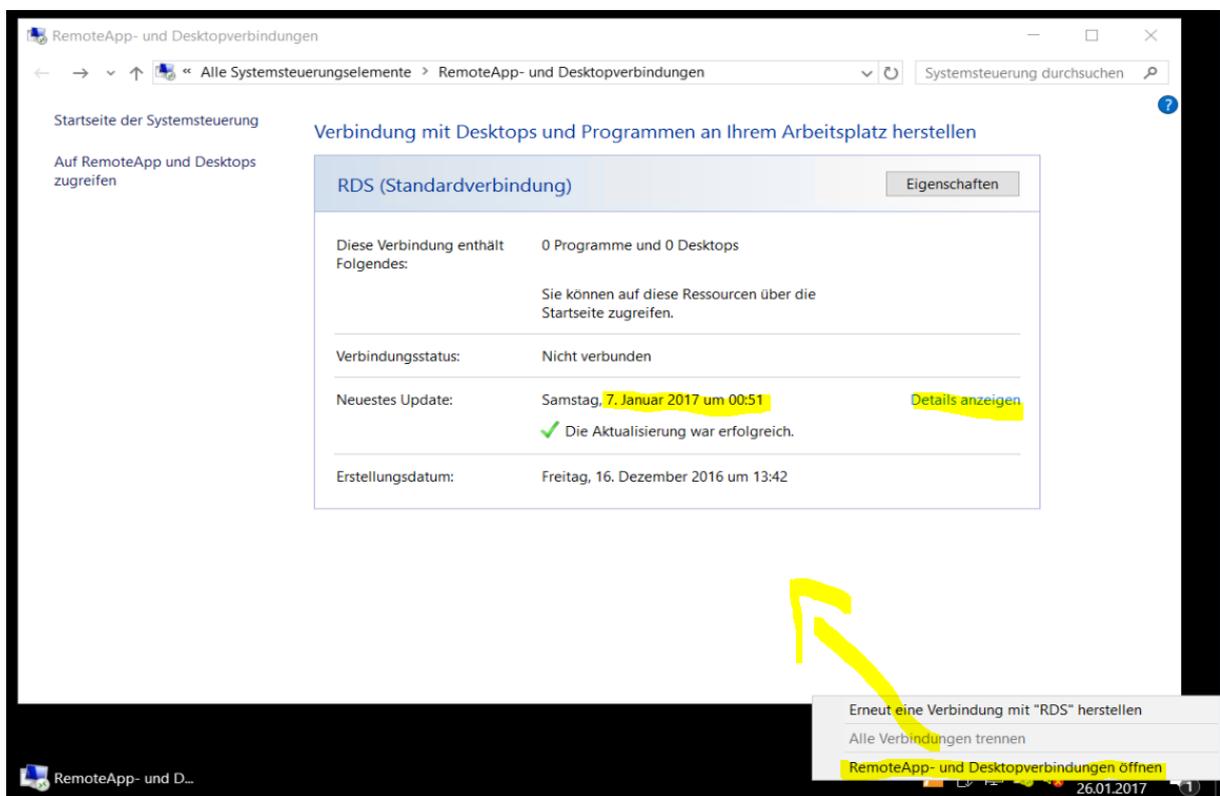
[Scan Another »](#)

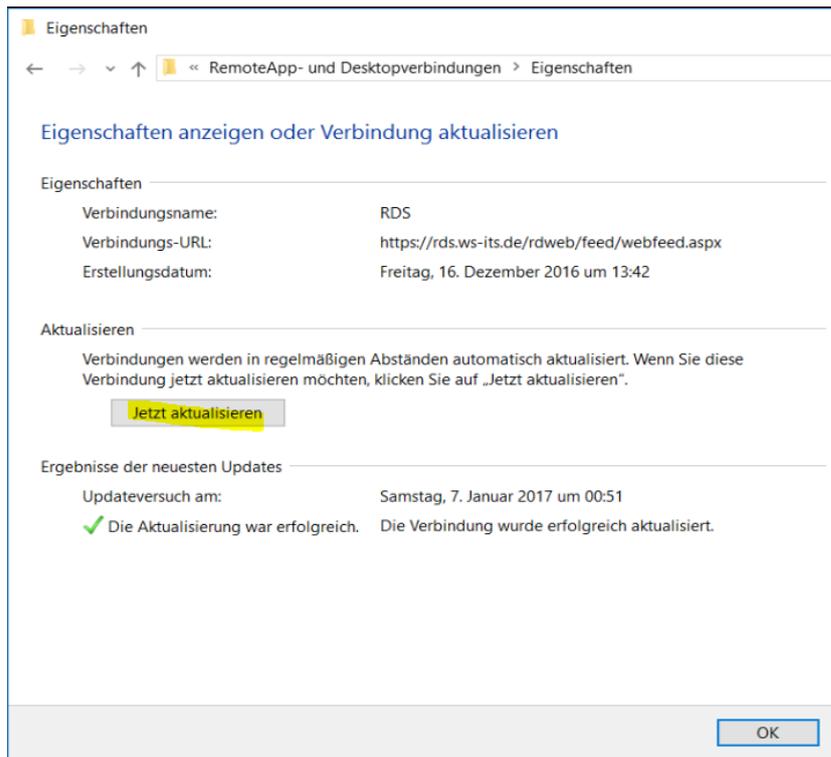


Clientanbindung

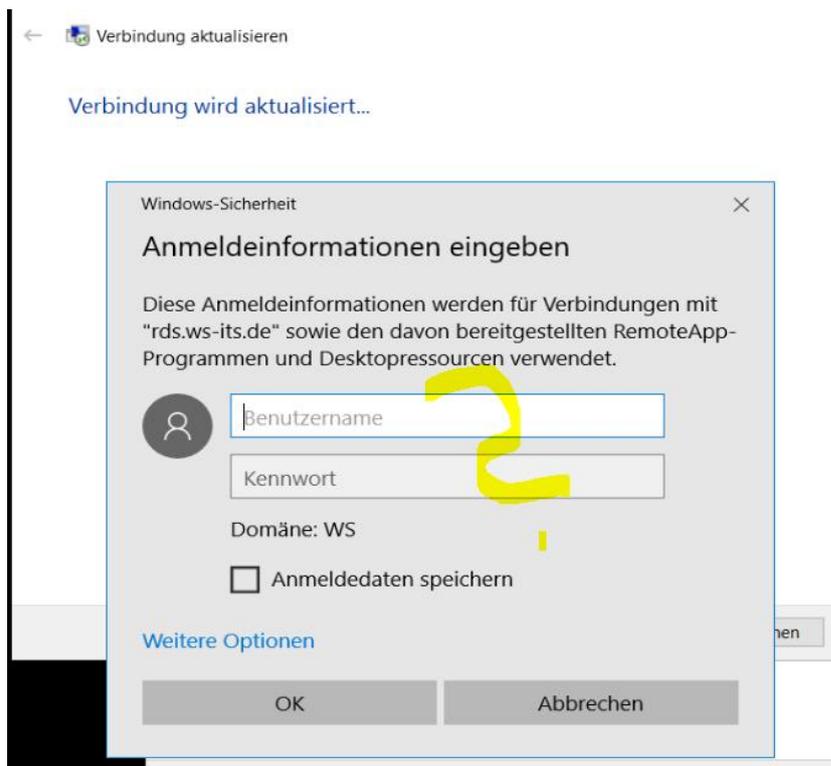
Die Benutzer werden über eine GPO angewiesen, die verfügbaren RemoteApps und Verbindungen automatisch zu erkennen. Diese Einstellung war bereits unter Windows Server 2012 R2 aktiv konfiguriert.

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. ☺