

Inhalt

Zielsetzung	2
Entfernung von WS-RDS1	2
Neuinstallation von WS-RDS1	3
Installation des neuen Servers.....	3
Bereitstellung der RemoteDesktopServices (RDS)	6
Erweiterung auf den HTML5-WebClient	22
Installation des HTML5-Clients	22
Troubleshooting – Problem „Firewall“	23
Troubleshooting – Problem „RD-Gateway“	28
Troubleshooting – Problem „Authentifizierung“	32
Troubleshooting – Problem „Zertifikat“	33
Veröffentlichung im Web Application Proxy	40
Veröffentlichung im PFSense HA-Proxy	45
Finetuning und Absicherung.....	49
Integration der RemoteApps.....	49
Absicherung durch MFA	50
http-Umleitung.....	59
Voreinstellungen	60
Integration in die Maintenance-Infrastruktur	60
Umzug in das Client-Netzwerk	60
Zusammenfassung	64

Zielsetzung

Einer meiner Windows Server 2016 mit dem Namen WS-RDS1 war ursprünglich mein RDS-System für die Einwahl von außen. Nach einigen Experimenten lief der Server nicht mehr stabil. Kurzerhand hatte ich einen weiteren Server WS-RDS2 installiert und als alleinigen Endpunkt für die RDP-Einwahl definiert. Seitdem hatte WS-RDS1 außer der Ausführung von 2 Scriptaufgaben (1x pro Tag) nichts mehr zu tun.

Im Rahmen meiner Umstellung auf Windows Server 2019 wird es Zeit, diese Altlast zu bereinigen. Leider hat Microsoft mit Windows Server 2019 die Rolle RemoteDesktopService verschlechtert. Daher habe ich überlegt, wie ich das zum einen selber testen kann und zum anderen aber keine wertvolle Funktionalität verliere. Die Lösung ist einfach: Ich installiere mit WS-RDS1 auf Windows Server 2019 eine zusätzliche Farm zu meinem WS-RDS2.

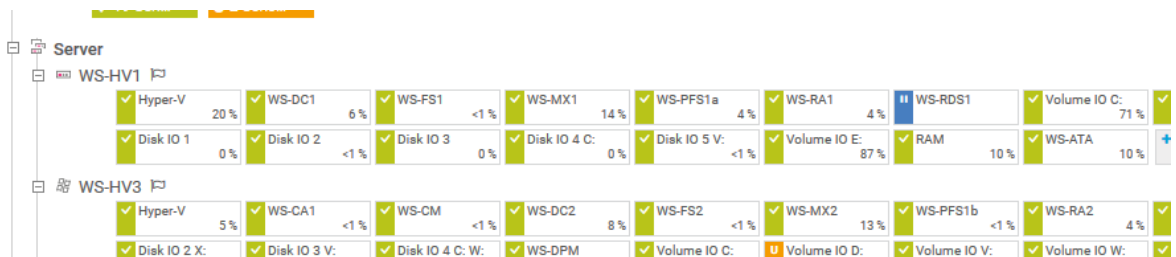
Zusätzlich möchte ich gerne zu meiner bestehenden RDS-RemoteApp-Verbindung für den Zugriff von außen auch einen HTML5-WebClient bereitstellen. Und diese Funktion wird der neue WS-RDS1 übernehmen.

Das Umstellungsszenario ist denkbar einfach: die beiden Scripte habe ich bereits auf einen anderen Server verschoben. WS-RDS1 kann also einfach entfernt und neu installiert werden. Die neue Installation erbt den Namen und die IPv4. So spare ich mir Anpassungen im Bereich Monitoring, Backup und Firewall.

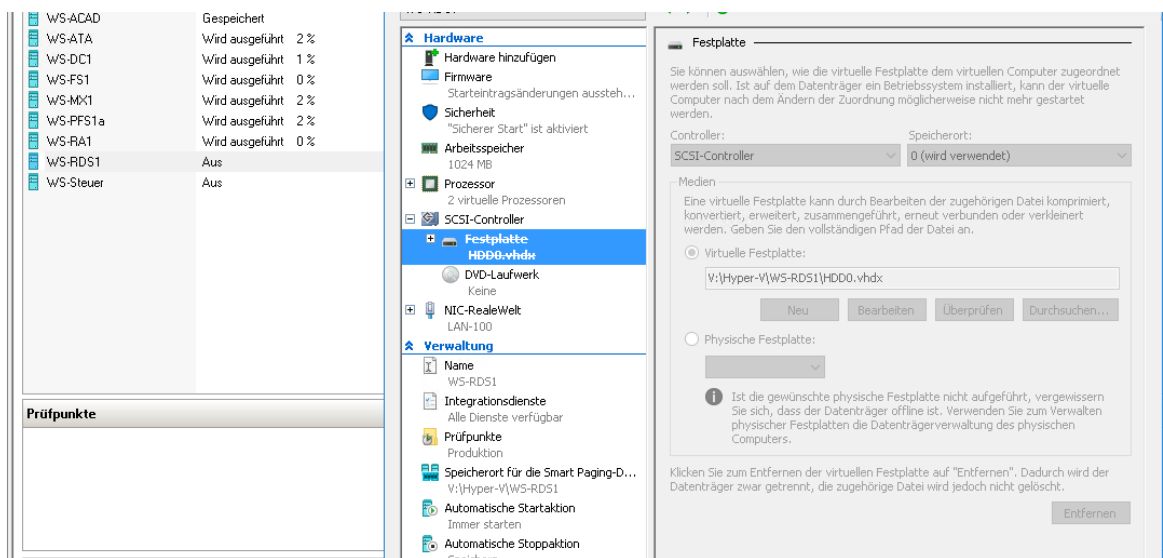
Entfernung von WS-RDS1

Ich prüfe noch einmal, ob auf dem System Daten oder Dienste liegen, die ich mitnehmen muss. Aber auf WS-RDS1 (alt) gibt es nichts mehr. Es kann also losgehen.

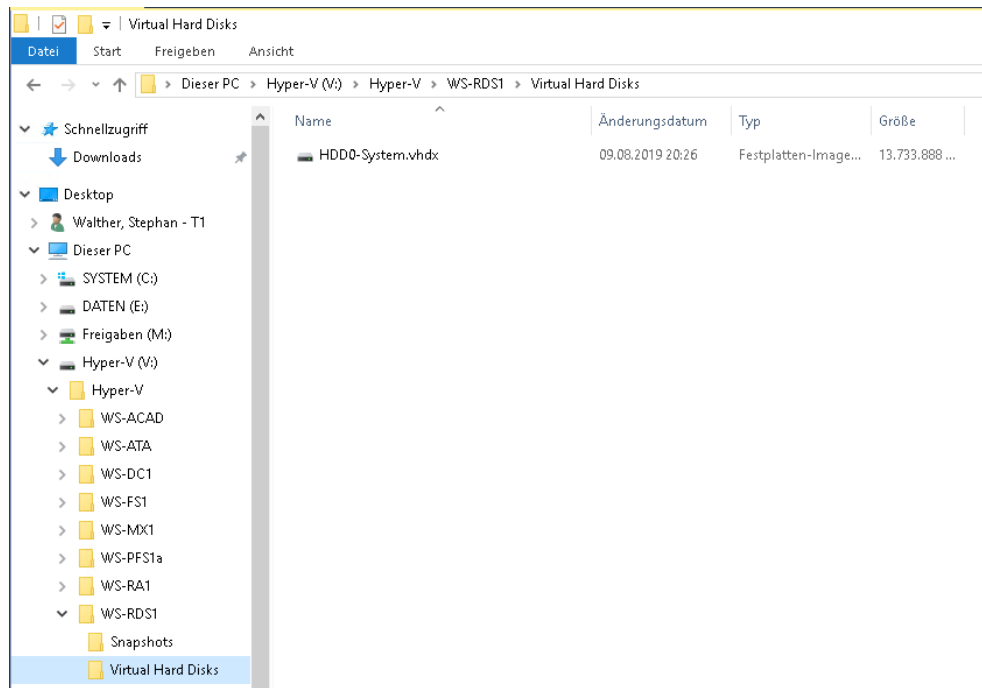
Ich pausiere das Monitoring:



Dann beende ich die VM aus im Hyper-V-Host WS-HV1 und entferne die alte VHDX-Festplatte:



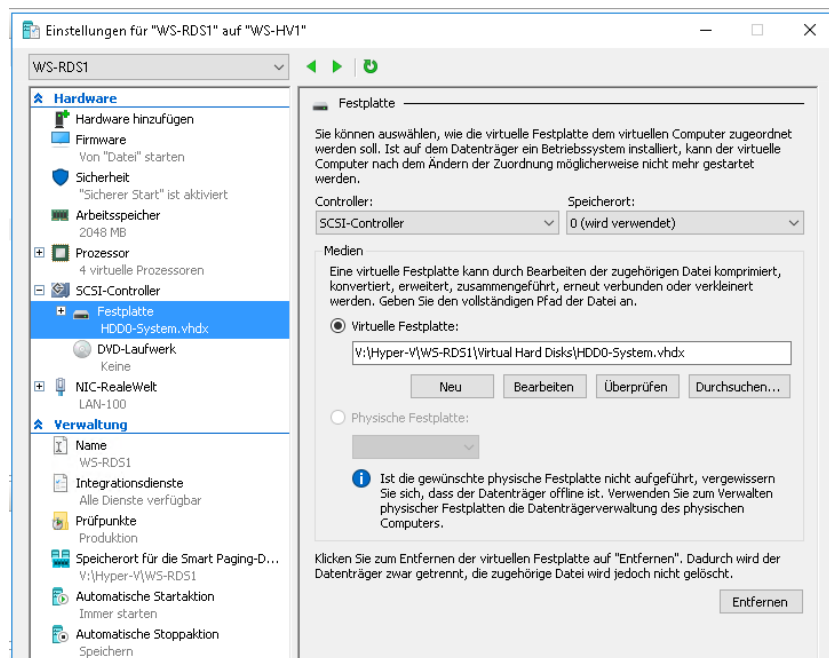
Die Datei entferne ich vom Datenträger und kopiere die vorbereitete VHDX-Datei mit Windows Server 2019 rein:



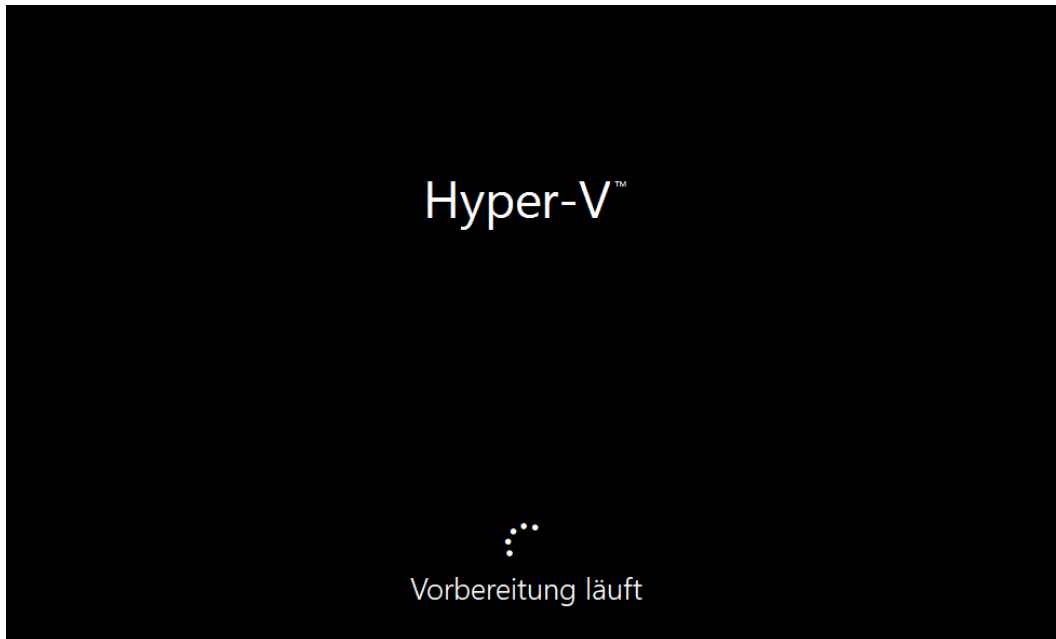
Neuinstallation von WS-RDS1

Installation des neuen Servers

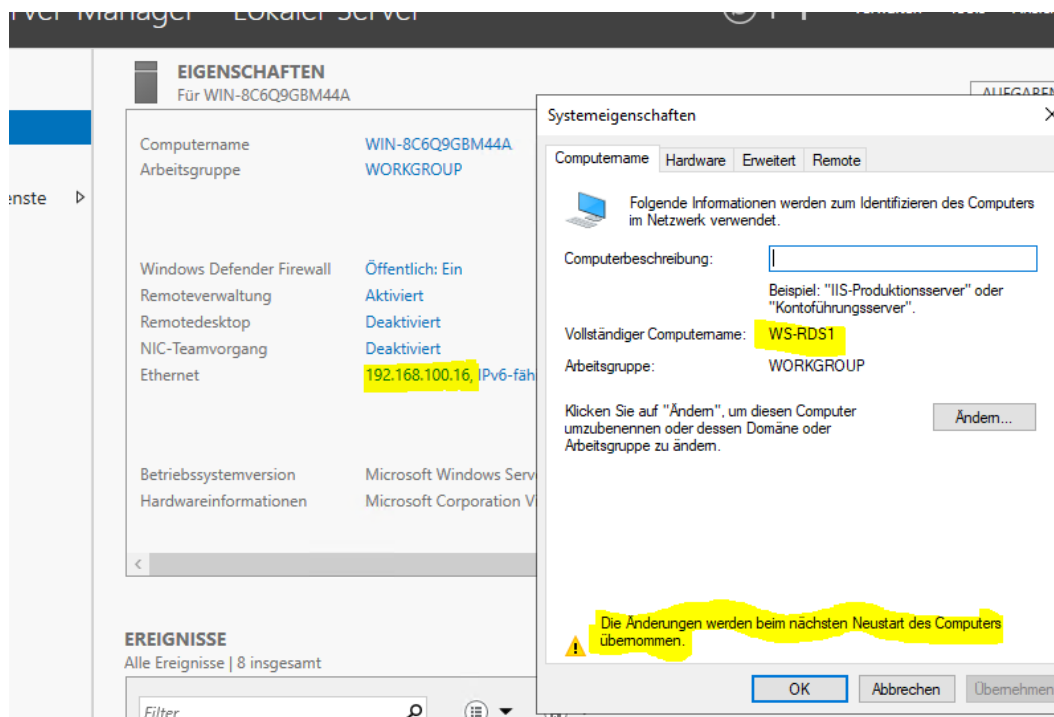
Die neue VHDX „installiere“ ich in die VM. Zusätzlich passe ich die „Hardware“ etwas an:



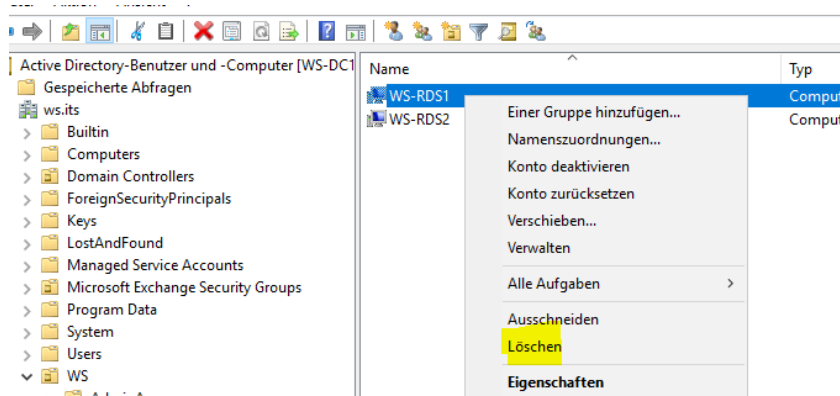
Nach dem Start der VM wird das Betriebssystem im OOBE-Modus vorbereitet:



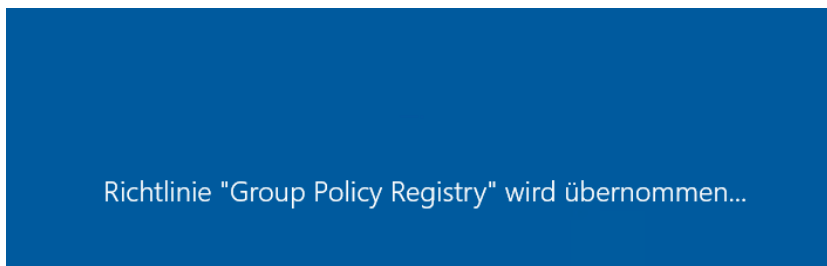
Ich definiere ein initiales Kennwort für den Administrator, konfiguriere die IPv4-Einstellungen und benenne das System um:



Vor dem DomainJoin lösche ich das alte Konto im ActiveDirectory:



Nun lasse ich das System in mein ActiveDirectory. Vor dem Neustart platziere ich das AD-Computerkonto in der richtigen Organisationseinheit. So wirken alle Gruppenrichtlinien direkt nach dem Neustart:



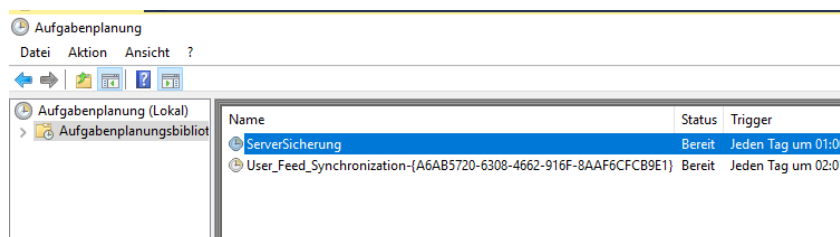
Jetzt fehlen noch die Windows Updates. Diese installiere brav im Hintergrund. Im WSUS meldet sich das System als Windows Server 2019:

ws-ipm.ws.its	192.168.100.14	Windows Server 2012 R2
ws-mon.ws.its	192.168.100.18	Windows Server 2019 Datacenter
ws-mx2.ws.its	192.168.100.13	Windows Server 2016 Datacenter
ws-ra2.ws.its	192.168.100.17	Windows Server 2016 Datacenter
ws-rds1.ws.its	192.168.100.16	Windows Server 2019 Datacenter
ws-rds3.ws.its	192.168.101.2	Windows Server 2016 Datacenter

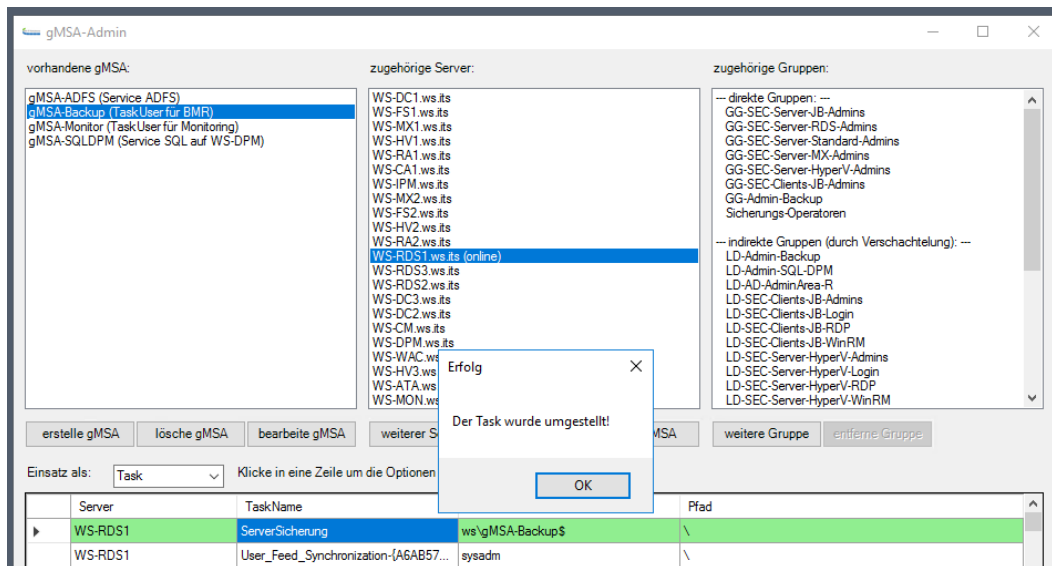
ws-rds1.ws.its			
Status	Updates mit Fehlern:	0	Gruppenmitgliedschaft: Alle Computer, Update-Verzoegert
	Erforderliche Updates:	0	Betriebssystem: Windows Server 2019 Datacenter
	Installierte/nicht zutreffende Updates:	825	Betriebssystemsprache: de-DE
	Updates ohne Status:	0	Service Pack: Keine
			IP-Adresse: 192.168.100.16
Zusätzliche Details			
Computerfabrikat: Microsoft Corporation			

Nach dem Update wird ein Neustart verlangt. Der ist schnell erledigt..

Nun fehlt noch das Backup. Auch bei diesem System setze ich auf die SystemState-Sicherung mit meinem Script. Dieses importiere ich als Scripttask:



Und wie schon mehrfach gezeigt passe ich den ausführenden Account mit meinem gMSA-Tool an:

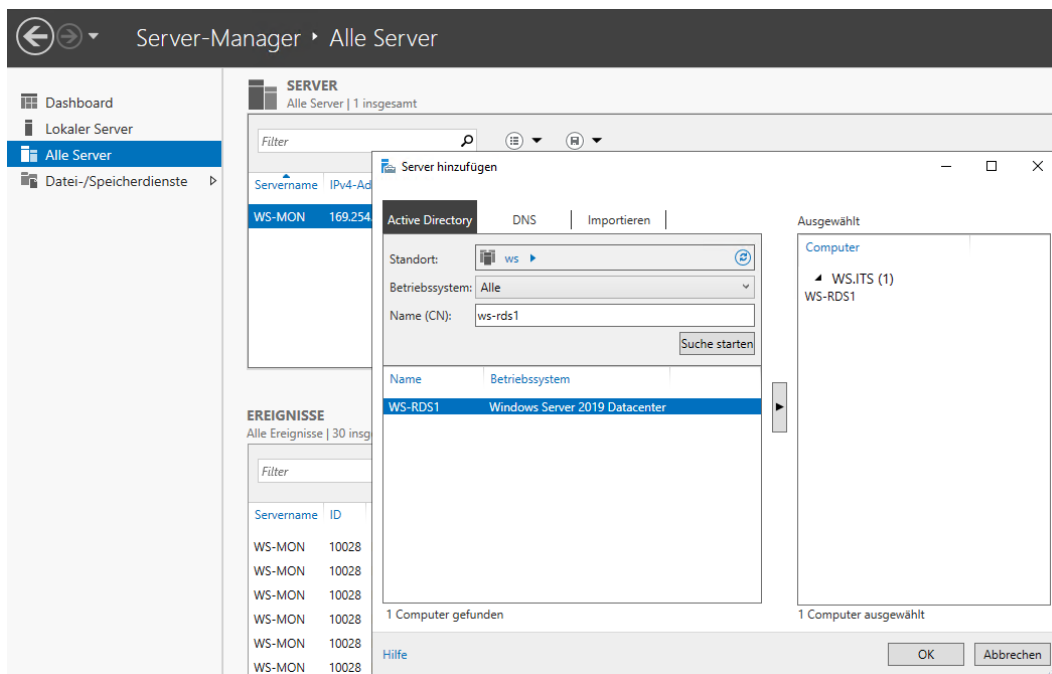


Das System ist einsatzbereit und wartet auf seine Aufgabe.

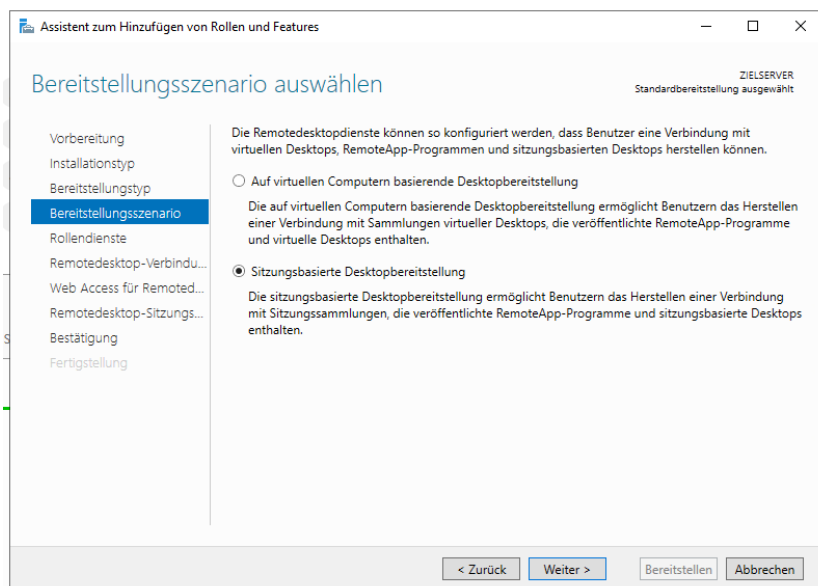
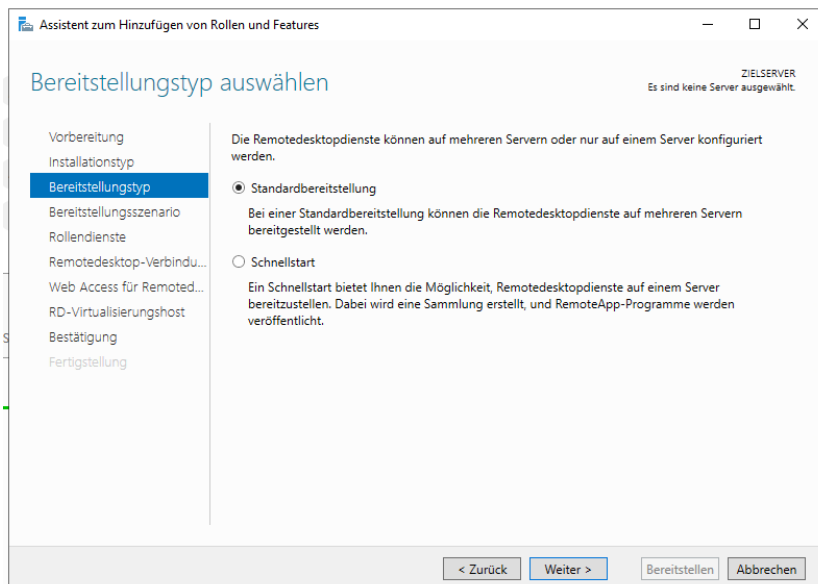
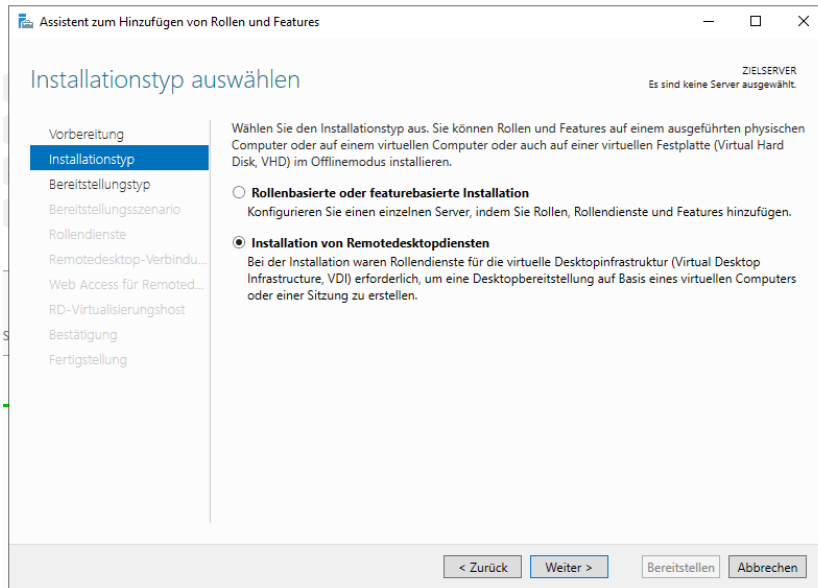
Bereitstellung der RemoteDesktopServices (RDS)

Der Server soll eine eigene RDS-Instanz bereitstellen. Daher werde ich die 4 Rollen: RD-ConnectionBroker, RD-Webservice, RD-SessionHost und RD-Gateway installieren. Den Zugriff auf die SessionCollection möchte ich mit HTML5 abbilden.

Das Setup der Instanz gleicht dem der vorherigen Betriebssysteme. Es wird über den Servermanager gestartet. Da der Vorgang aber einen Neustart erwartet werde ich die Installation von einem anderen Server ausführen. Hier wähle ich meinen neuen WS-MON. Auch dieser läuft schon mit Windows Server 2019. Im Servermanager füge ich den WS-RDS1 hinzu:



Und dann geht es mit der Rolleninstallation los:



Assistent zum Hinzufügen von Rollen und Features

ZIELSERVER
Standardbereitstellung ausgewählt

Rollendienste überprüfen

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

Für diese Bereitstellung werden die folgenden Rollendienste für Remotedesktopdienste installiert und konfiguriert:

- Remotedesktop-Verbindungsbroker**
Vom Remotedesktop-Verbindungsbroker wird ein Clientgerät mit RemoteApp-Programmen, sitzungsbasierten Desktops und virtuellen Desktops verbunden.
- Web Access für Remotedesktop**
Mit Web Access für Remotedesktop wird es Benutzern ermöglicht, über das Startmenü oder einen Webbrowser Verbindungen mit Ressourcen herzustellen, die von Sitzungssammlungen und Sammlungen virtueller Desktops bereitgestellt werden.
- Remotedesktop-Sitzungshost**
Mit dem Remotedesktop-Sitzungshost wird es einem Server ermöglicht, RemoteApp-Programme oder sitzungsbasierte Desktops zu hosten.

i Die Anmeldeinformationen des WS\stephan-T1-Kontos werden zum Erstellen der Bereitstellung verwendet.

< Zurück Weiter > Bereitstellen Abbrechen

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	Betriebsst...
WS-RDS1.ws.its	192.168.100.16	
WS-MON.ws.its	169.254.148.22...	

2 Computer gefunden

Ausgewählt

Computer

- WS.ITS (1)
- WS-RDS1

1 Computer ausgewählt

< Zurück Weiter > Bereitstellen Abbrechen

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-Verbindungsbrokerserver installieren

Serverpool

Filter:

Name	IP-Adresse	Betriebsst...
WS-RDS1.ws.its	192.168.100.16	
WS-MON.ws.its	169.254.148.22...	

2 Computer gefunden

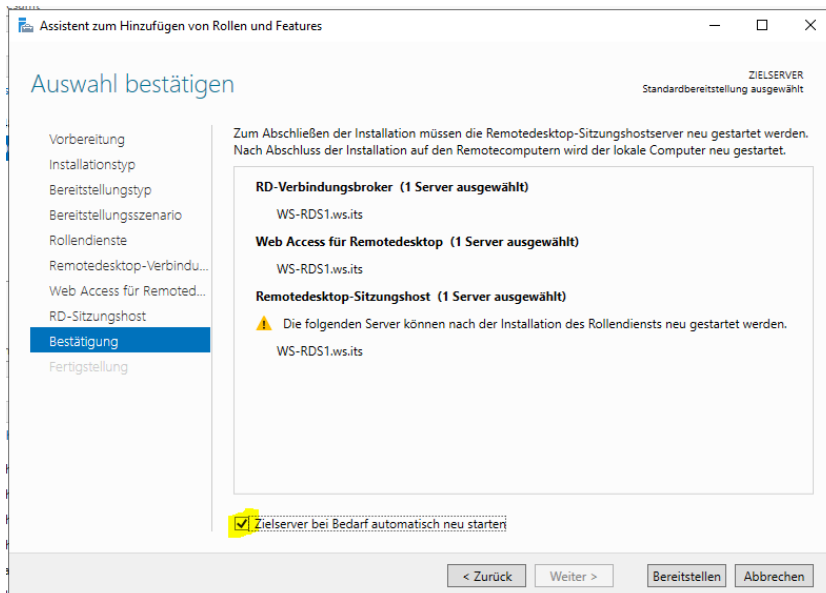
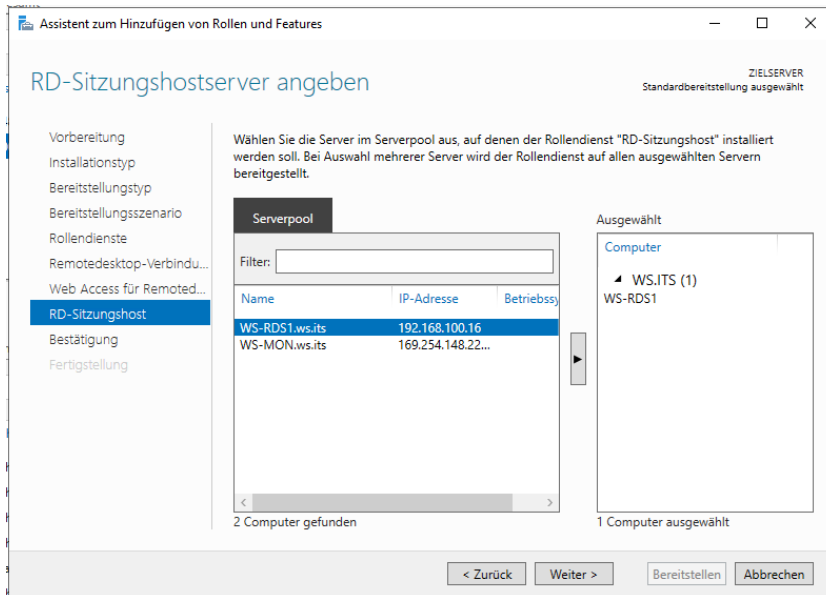
Ausgewählt

Computer

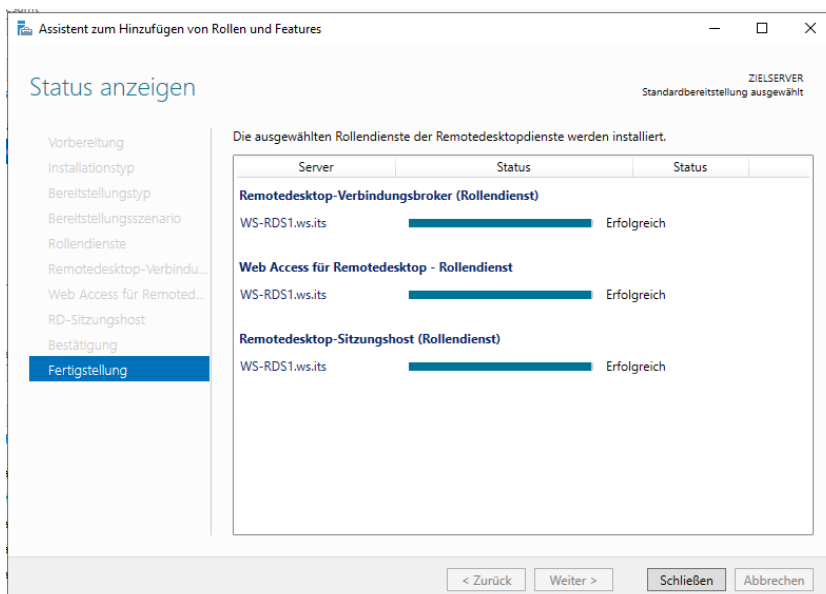
- WS.ITS (1)
- WS-RDS1

1 Computer ausgewählt

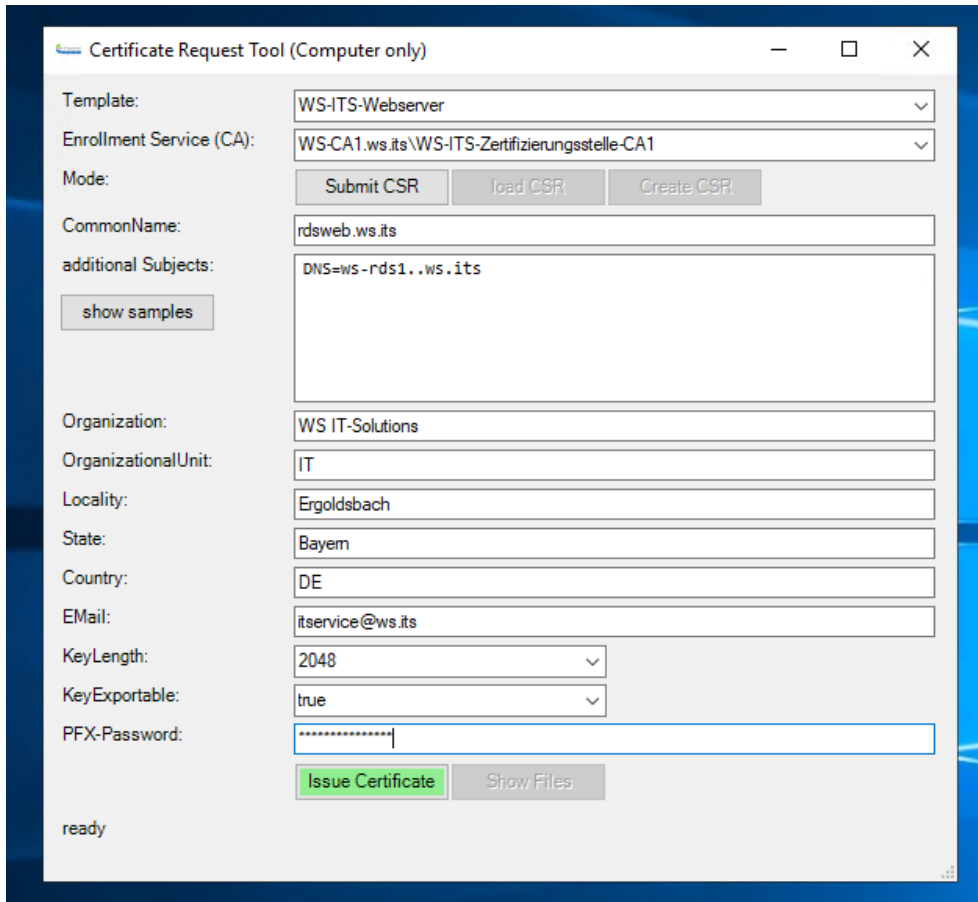
< Zurück Weiter > Bereitstellen Abbrechen



Das Setup läuft und ist nach wenigen Minuten erfolgreich abgeschlossen:



Für die verschiedenen Funktionen benötige ich ein internes Zertifikat. Dieses beantrage ich mit meinem PowerShell-Tool von meiner internen Windows-PKI:



Certificate Request Tool (Computer only)

Template: WS-ITS-Webserver

Enrollment Service (CA): WS-CA1.ws.its\WS-ITS-Zertifizierungsstelle-CA1

Mode: Submit CSR | load CSR | Create CSR

CommonName: rdswb.ws.its

additional Subjects: DNS=ws-rds1..ws.its

show samples

Organization: WS IT-Solutions

OrganizationalUnit: IT

Locality: Ergoldsbach

State: Bayern

Country: DE

EMail: itservice@ws.its

KeyLength: 2048

KeyExportable: true

PFX-Password:

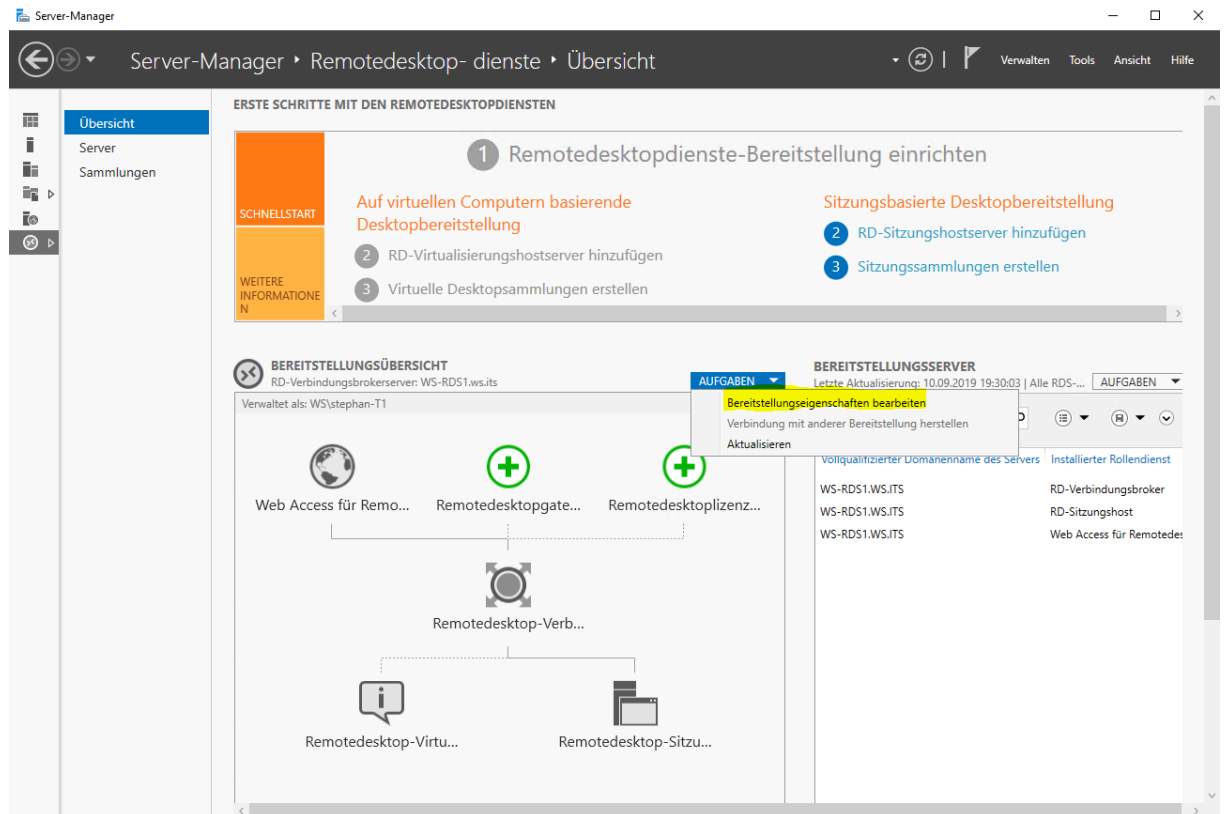
Issue Certificate | Show Files

ready

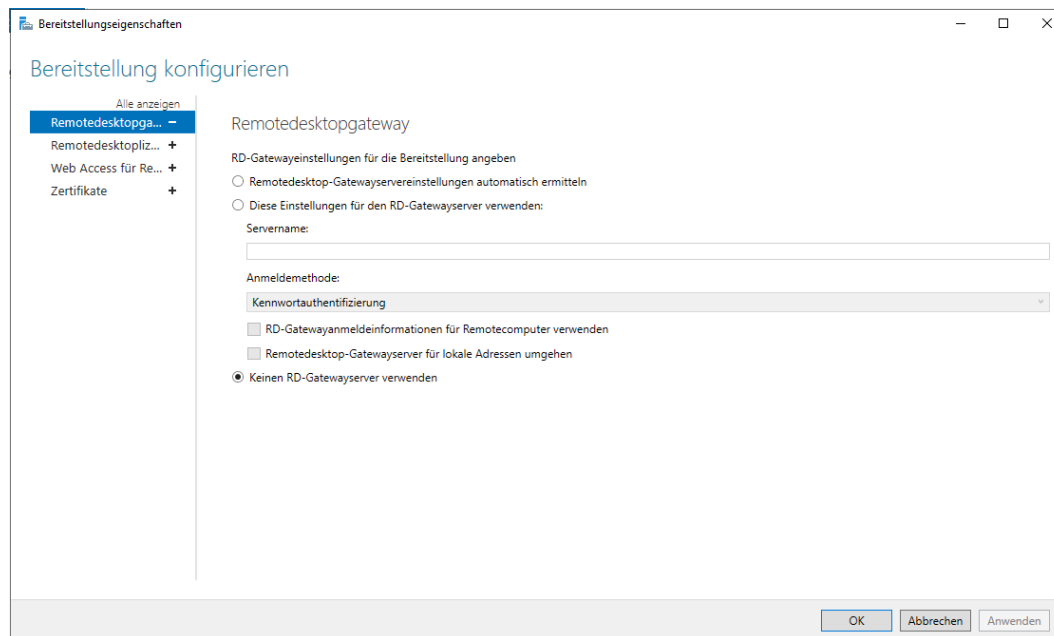


Warum ich kein öffentliches Zertifikat verwende? Der Server wird selber kein „Tageslicht“ sehen. Seine Webdienste leite ich durch einen WAP (Web Application Proxy). Nur dieser bekommt das vertrauenswürdige Zertifikat installiert...

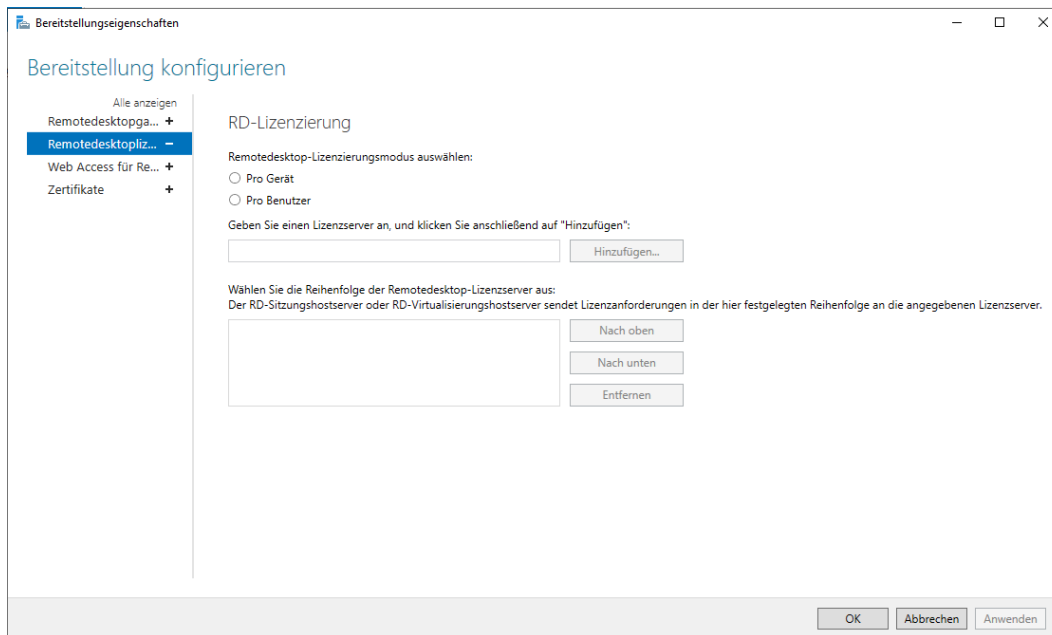
Nun kann die Bereitstellung beginnen:



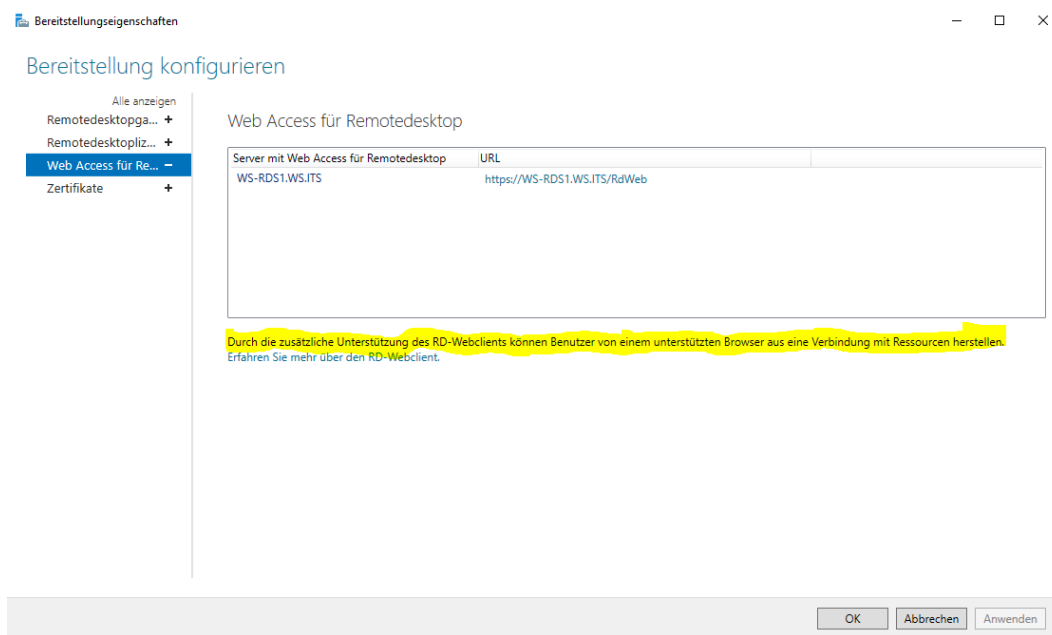
Noch ist kein Gateway installiert:



Den Lizenzserver installiere ich später, wenn die Lösung funktioniert. Bis dahin genügt mir der Evaluierungszeitraum:



Das ist die interessante Funktion:



In diesem Dialog gibt es keine Veränderung. Für jede Komponente müssen die Zertifikate installiert werden:

Bereitstellungseigenschaften

Bereitstellung konfigurieren

Alle anzeigen
 Remotedesktopga... +
 Remotedesktoppliz... +
 Web Access für Re... +
Zertifikate -

Zertifikate verwalten

Für eine Remotedesktopdienste-Bereitstellung sind Zertifikate für die Serverauthentifizierung, einmaliges Anmelden und Herstellen von sicheren Verbindungen erforderlich.

Die aktuelle Zertifikatsstufe der Bereitstellung ist **Nicht konfiguriert**
 Was ist eine Zertifikatsstufe?

Rolldienst	Stufe	Status	Status
Remotedesktop-Verbindungsbroker	Nicht konfiguriert	--	
Remotedesktop-Verbindungsbroker	Nicht konfiguriert	--	
Web Access für Remotedesktop	Nicht konfiguriert	--	
RD-Gateway	Unbekannt	--	

Antragstellername: Nicht verfügbar
 Details anzeigen

Dieses Zertifikat ist für die Serverauthentifizierung für die Remotedesktopdienste-Bereitstellung erforderlich.

Sie können dieses Zertifikat aktualisieren, indem Sie ein neues Zertifikat erstellen oder ein vorhandenes Zertifikat auswählen.

Neues Zertifikat erstellen... Vorhandenes Zertifikat auswählen...

OK Abbrechen Anwenden

Bereitstellungseigenschaften

Bereitstellung konfigurieren

Alle anzeigen
 Remotedesktopga... +
 Remotedesktoppliz... +
 Web Access für Re... +
Zertifikate -

Zertifikate

Für eine Remo...
 erforderlich.

Die aktuelle Z...
 Was ist eine Zi...

Rolldienst	Stufe	Status	Status
Remotedeskk	Nicht konfiguriert	--	
Remotedeskk	Nicht konfiguriert	--	
Web Access	Nicht konfiguriert	--	
RD-Gateway	Unbekannt	--	

Antragstellern...
 Details anzeig...

Dieses Zertifik...
 Sie können die...

Vorhandenes Zertifikat auswählen

Sie können das momentan auf dem RD-Verbindungsbrokerserver gespeicherte Zertifikat anwenden oder ein anderes Zertifikat in einer PKCS-Zertifikatsdatei auswählen.

Auf dem RD-Verbindungsbrokerserver gespeichertes Zertifikat anwenden
 Kennwort:

Anderes Zertifikat auswählen
 Zertifikatpfad:
 Kennwort:

Hinzufügen des Zertifikats zum Zertifikatspeicher "Vertrauenswürdige Stammzertifzierungsstellen" auf den Zielcomputern zulassen

OK Abbrechen

OK Abbrechen Anwenden

Bereitstellungseigenschaften

Bereitstellung konfigurieren

Daten werden gespeichert...
 Alle anzeigen
 Remotedesktopga... +
 Remotedesktoppliz... +
 Web Access für Re... +
Zertifikate -

Zertifikate verwalten

Für eine Remotedesktopdienste-Bereitstellung sind Zertifikate für die Serverauthentifizierung, einmaliges Anmelden und Herstellen von sicheren Verbindungen erforderlich.

⚠ Einem bestimmten Rollendienst kann jeweils nur ein einzelnes Zertifikat hinzugefügt werden. Wenn Sie weiteren Rollendiensten Zertifikate hinzufügen möchten, klicken Sie auf "Übernehmen" oder "OK".

Die aktuelle Zertifikatsstufe der Bereitstellung ist **Nicht konfiguriert**
 Was ist eine Zertifikatsstufe?

Rollendienst	Stufe	Status	Status
Remotedesktop-Verbindungsbroker	Nicht konfiguriert	--	Kann angewendet wer
Remotedesktop-Verbindungsbroker	Nicht konfiguriert	--	
Web Access für Remotedesktop	Nicht konfiguriert	--	
RD-Gateway	Unbekannt	--	

Antragstellername: Nicht verfügbar
 Details anzeigen

Dieses Zertifikat ist für die Serverauthentifizierung für die Remotedesktopdienste-Bereitstellung erforderlich.
 Sie können dieses Zertifikat aktualisieren, indem Sie ein neues Zertifikat erstellen oder ein vorhandenes Zertifikat auswählen.

Neues Zertifikat erstellen... Vorhandenes Zertifikat auswählen...

OK Abbrechen **Anwenden**

Das wiederhole ich für alle anderen Komponenten. Hier sehen wir das Ergebnis:

Bereitstellungseigenschaften

Bereitstellung konfigurieren

Daten werden gespeichert...
 Alle anzeigen
 Remotedesktopga... +
 Remotedesktoppliz... +
 Web Access für Re... +
Zertifikate -

Zertifikate verwalten

Für eine Remotedesktopdienste-Bereitstellung sind Zertifikate für die Serverauthentifizierung, einmaliges Anmelden und Herstellen von sicheren Verbindungen erforderlich.

Die aktuelle Zertifikatsstufe der Bereitstellung ist **Vertrauenswürdig**
 Was ist eine Zertifikatsstufe?

Rollendienst	Stufe	Status	Status
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	Erfolgreich
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	Erfolgreich
Web Access für Remotedesktop	Vertrauenswürdig	OK	Erfolgreich
RD-Gateway	Unbekannt	--	

Antragstellername: E=itservice@ws.its, CN=rdsweb.ws.its, OU=IT, O=WS IT-Solutions, L=Ergoldsbach, S=Bayern, C=DE
 Details anzeigen

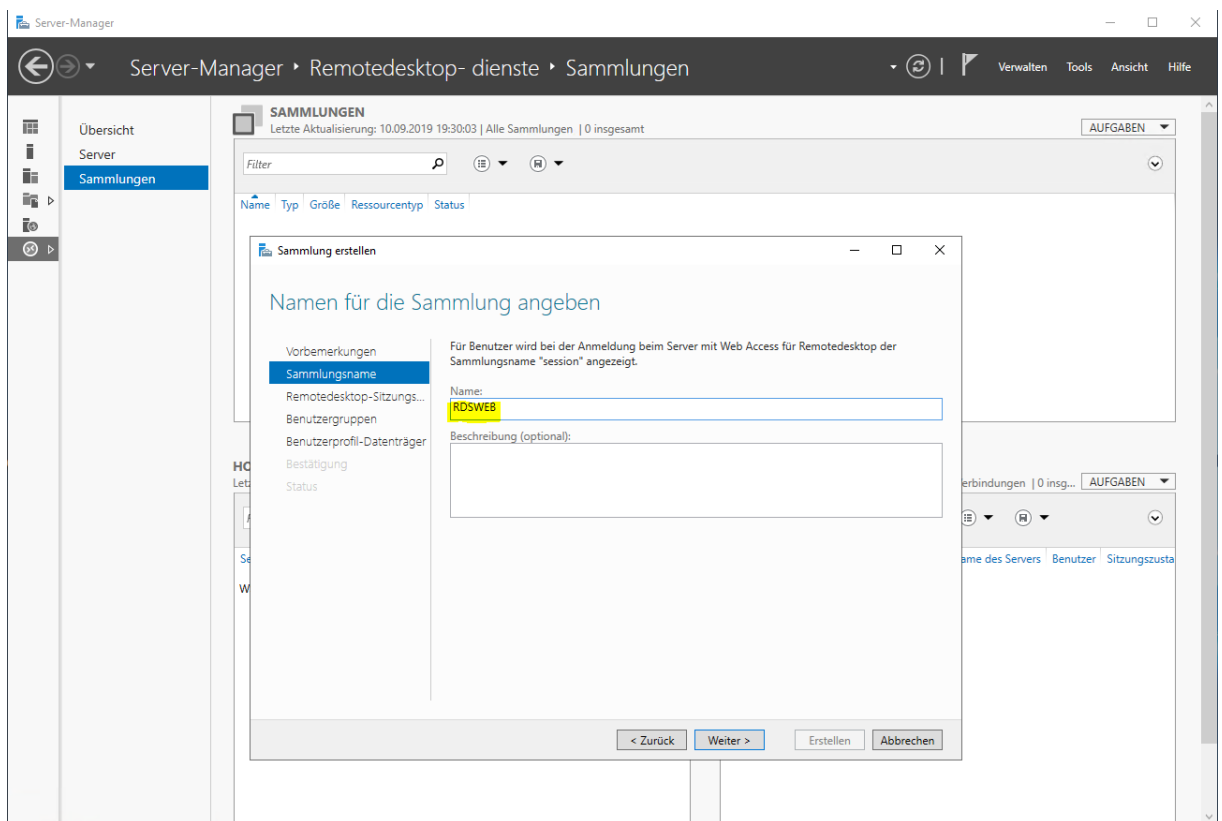
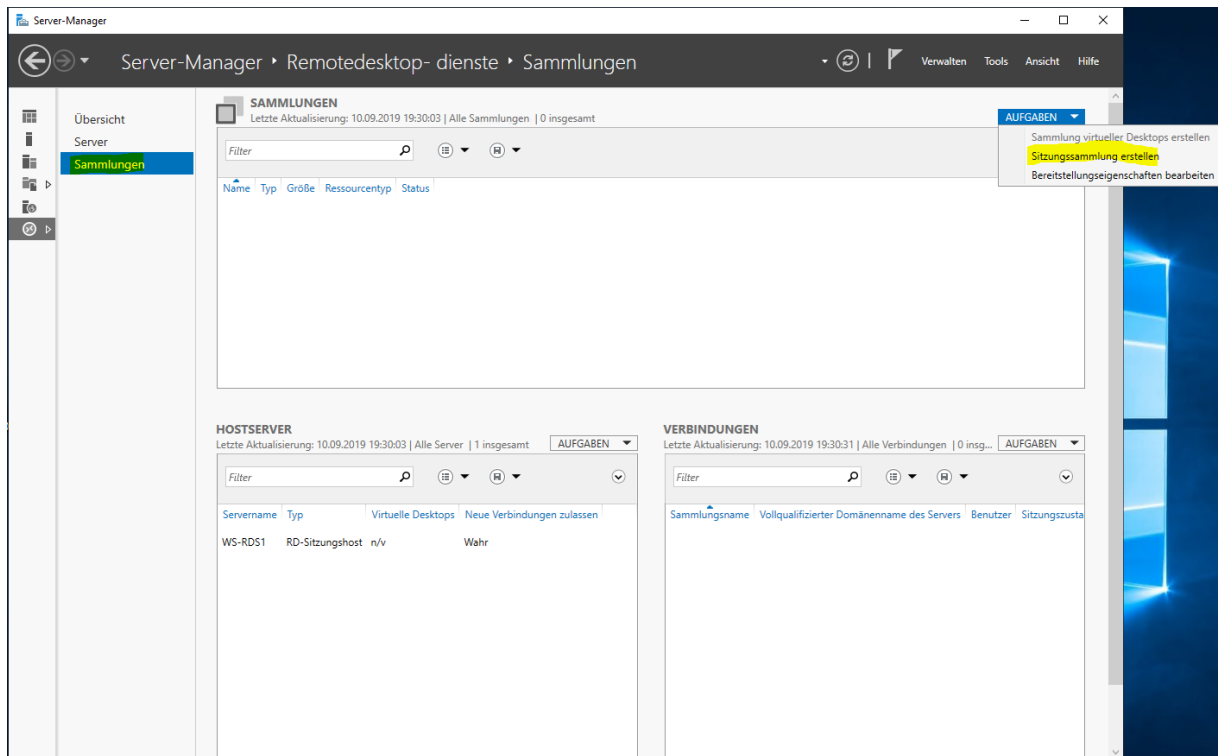
Dieses Zertifikat ist für die Aktivierung des RemoteApp- und Desktopverbindungsabonnements und für die Serverauthentifizierung für Web Access für Remotedesktop erforderlich.

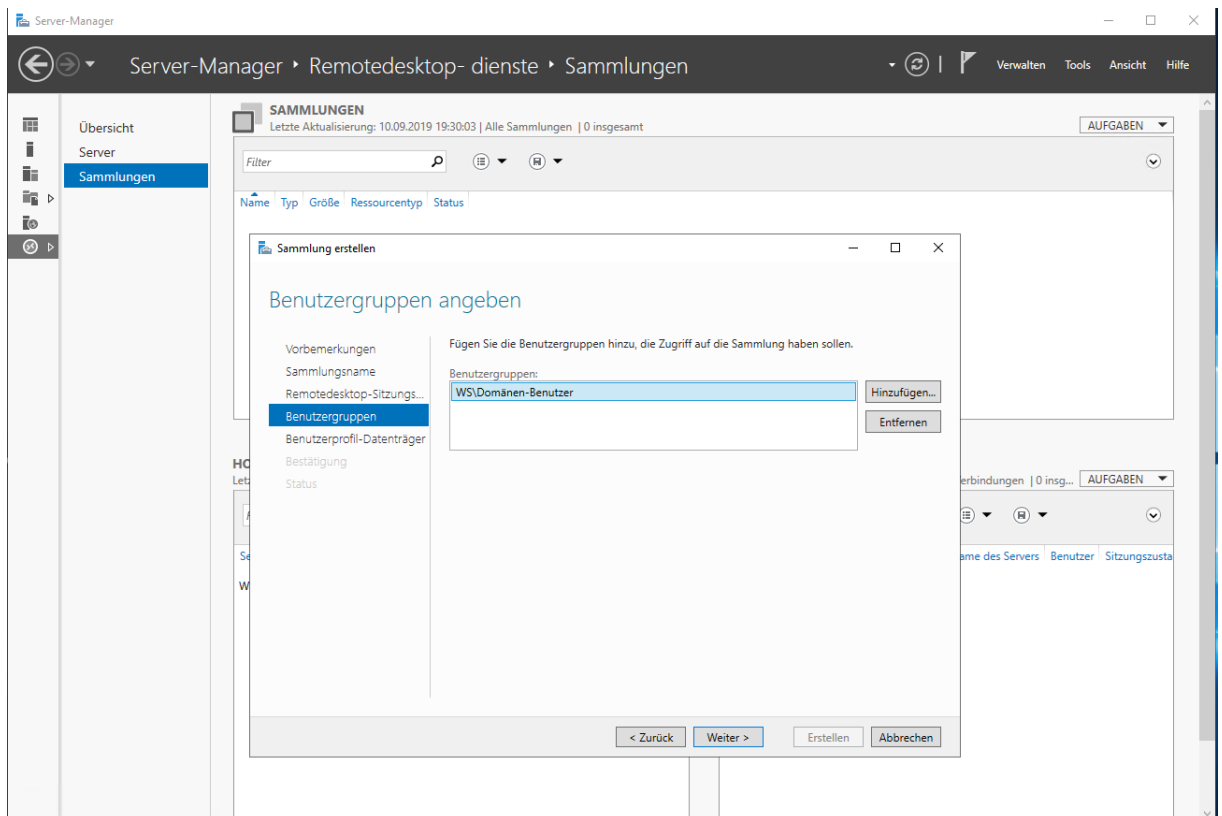
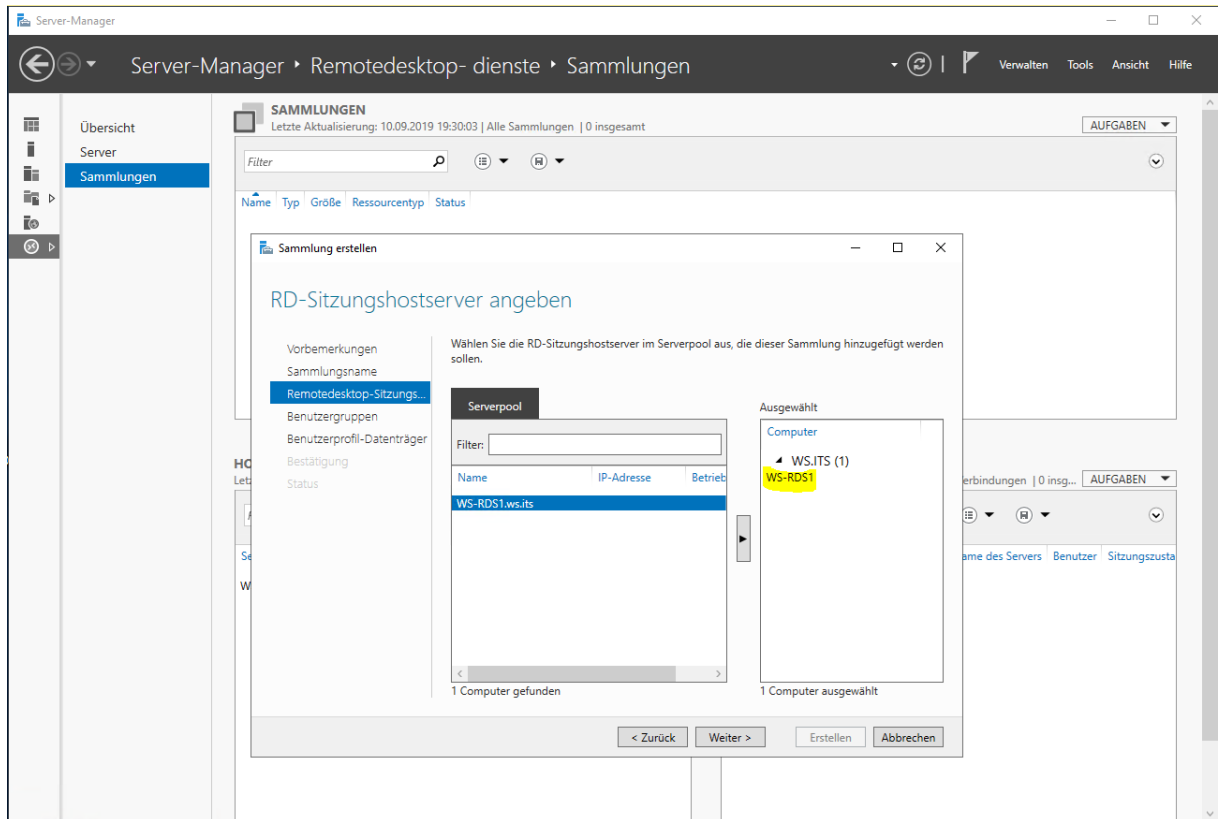
Sie können dieses Zertifikat aktualisieren, indem Sie ein neues Zertifikat erstellen oder ein vorhandenes Zertifikat auswählen.

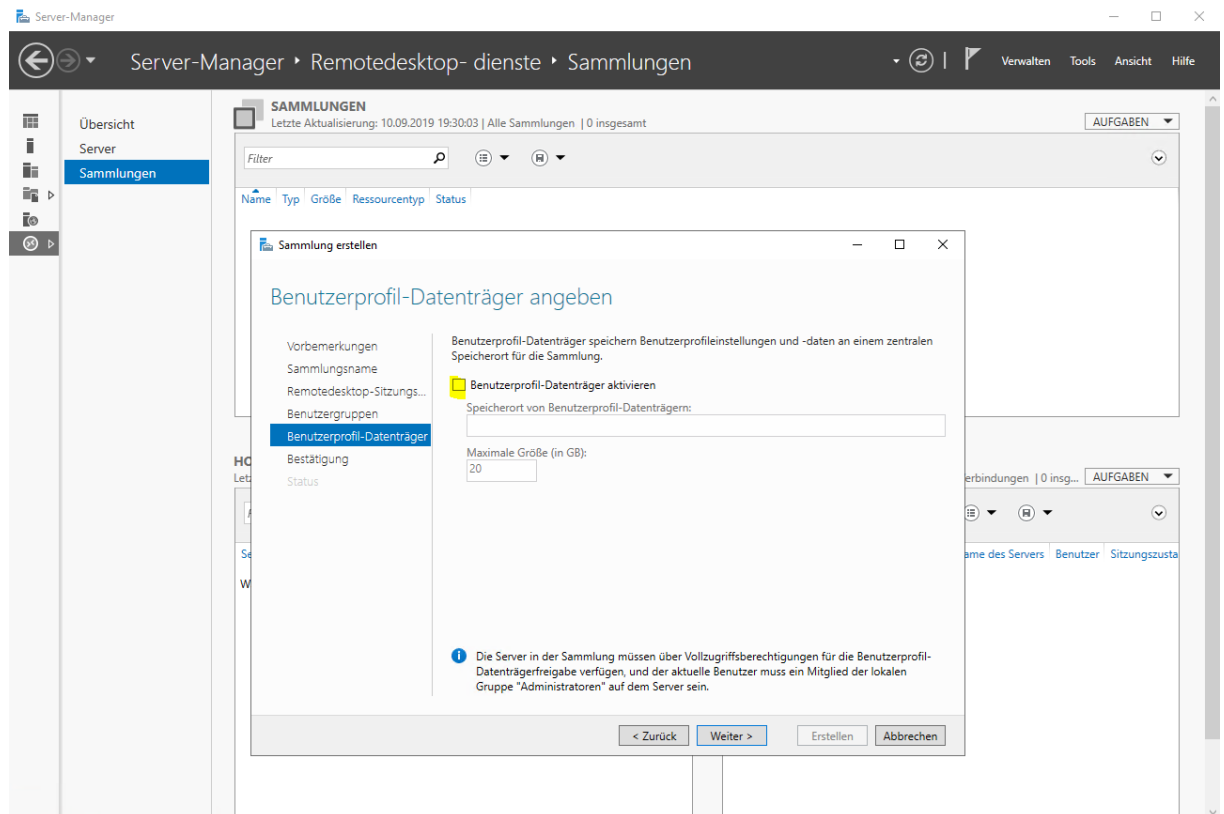
Neues Zertifikat erstellen... Vorhandenes Zertifikat auswählen...

OK Abbrechen Anwenden

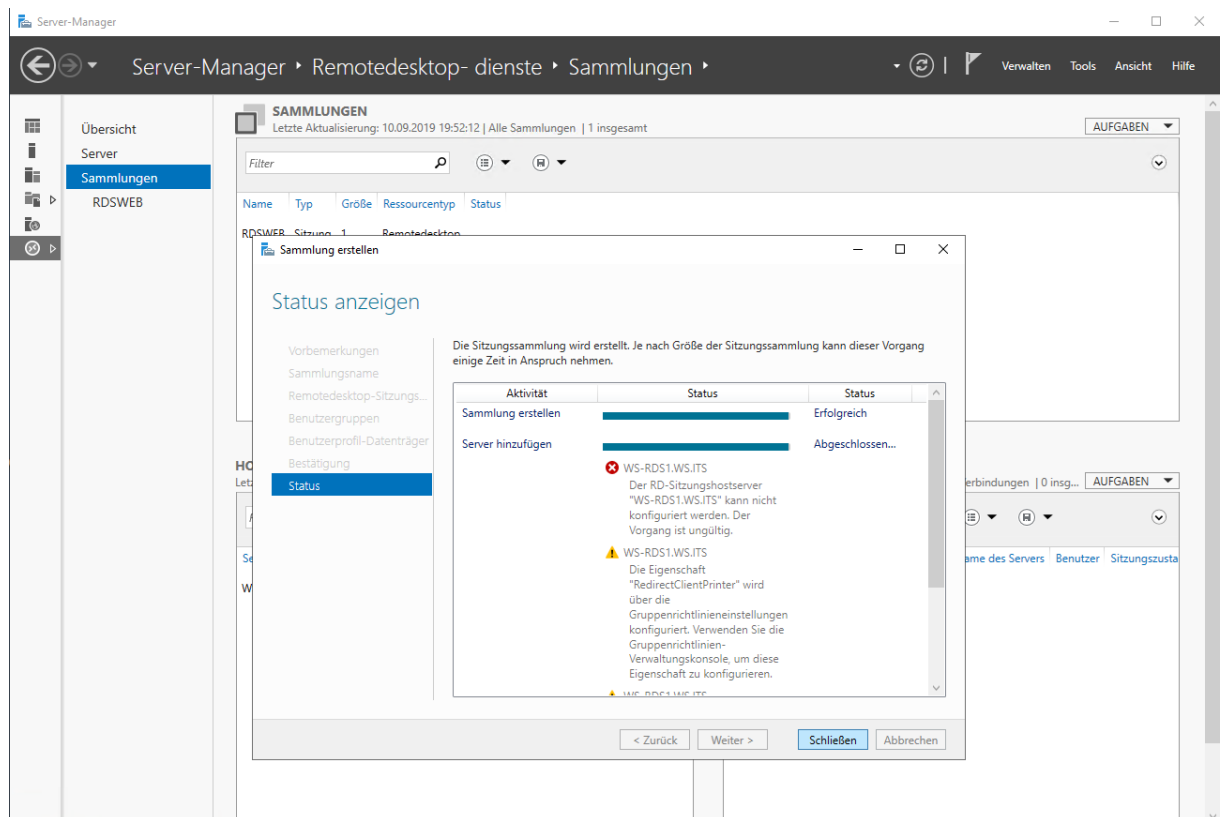
Jetzt erstelle ich eine Session-Collection. Früher haben wir das einfach Farm genannt. Gemeint sind SessionHosts, die alle die gleiche Funktion anbieten. Mitglied ist der WS-RDS1 selber:



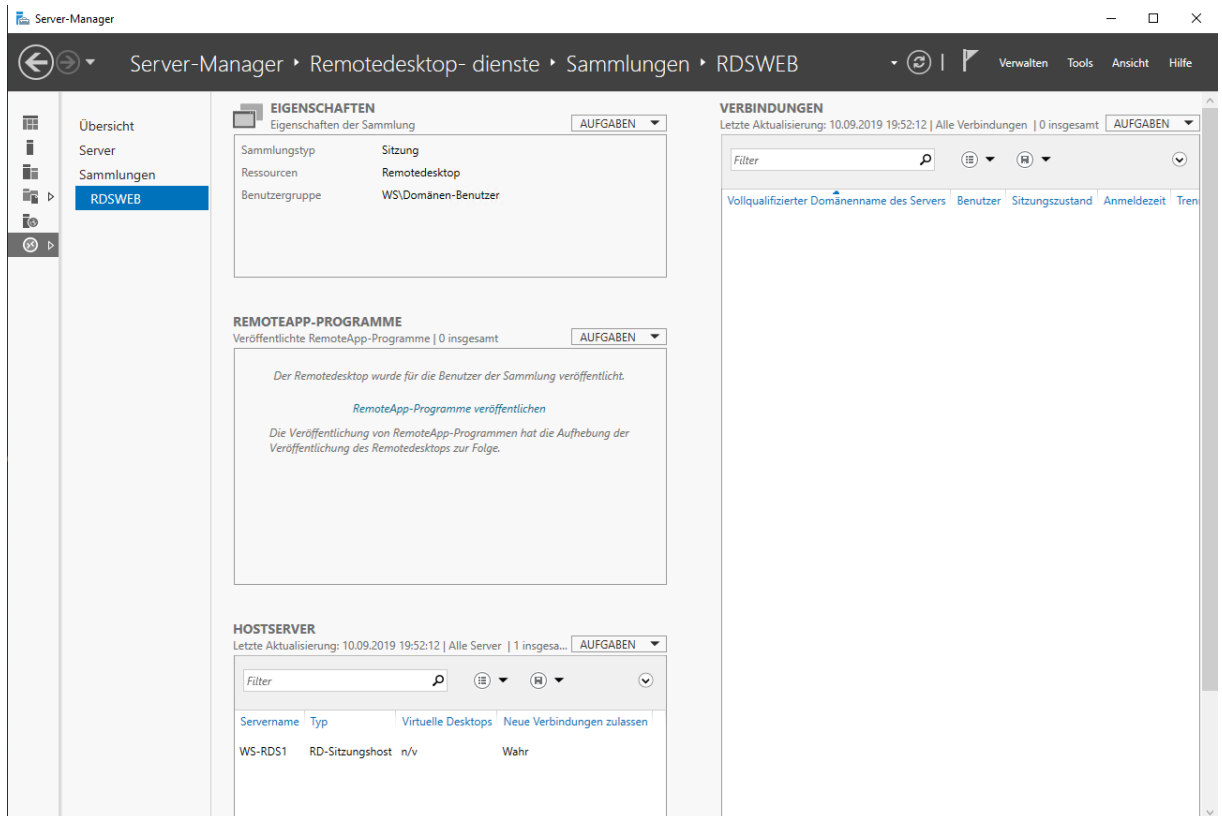




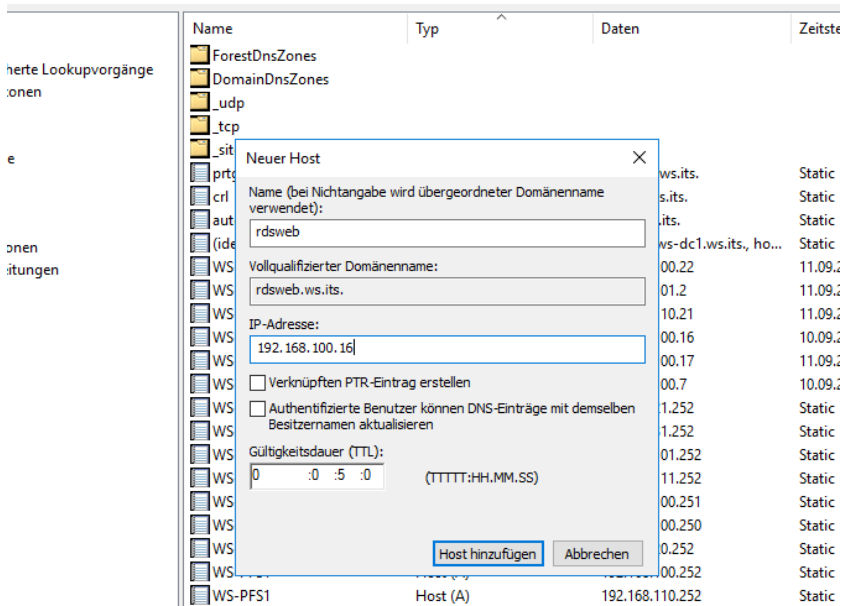
Hier ist eine meiner GPO gegen eine neue Collection am Wirken. Diese mag der RDS-Broker nicht:



Dennoch wurde sie erstellt:



Die Webseite möchte ich mit dem FQDN rdsweb.ws.its intern aufrufen können. Dazu ist ein neuer DNS-Record erforderlich:



Es wird Zeit für einen Test. Ich rufe die RD-Website von meinem Client aus auf. Leider ohne Erfolg:

Fehler: Netzwerk-Zeitüberschreitung

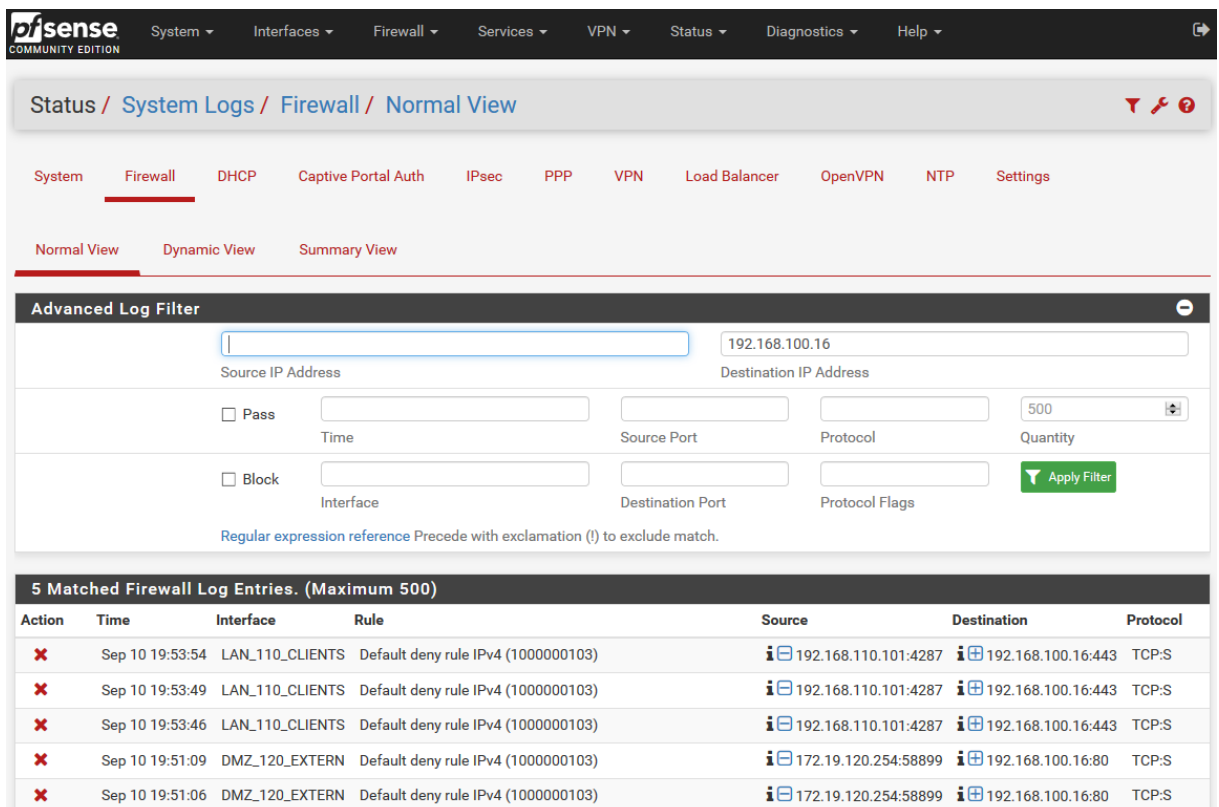
Der Server unter ws-rds1.ws.its braucht zu lange, um eine Antwort zu senden.



- Die Website könnte vorübergehend nicht erreichbar sein, versuchen Sie es bitte später nochmals.
- Wenn Sie auch keine andere Website aufrufen können, überprüfen Sie bitte die Netzwerk-/Internetverbindung.
- Wenn Ihr Computer oder Netzwerk von einer Firewall oder einem Proxy geschützt wird, stellen Sie bitte sicher, dass Firefox auf das Internet zugreifen darf.

Nochmals versuchen

Die Ursache ist schnell gefunden: Meine Firewall kennt den neuen Service noch nicht und blockt erwartungsgemäß:



The screenshot shows the pfSense Firewall Log Filter interface. The 'Advanced Log Filter' section is active, with 'Source IP Address' set to 192.168.100.16. The 'Pass' checkbox is checked, and the 'Quantity' is set to 500. Below the filter, a table displays 5 matched firewall log entries.

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Sep 10 19:53:54	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:4287	192.168.100.16:443	TCP:S
✗	Sep 10 19:53:49	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:4287	192.168.100.16:443	TCP:S
✗	Sep 10 19:53:46	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:4287	192.168.100.16:443	TCP:S
✗	Sep 10 19:51:09	DMZ_120_EXTERN	Default deny rule IPv4 (1000000103)	172.19.120.254:58899	192.168.100.16:80	TCP:S
✗	Sep 10 19:51:06	DMZ_120_EXTERN	Default deny rule IPv4 (1000000103)	172.19.120.254:58899	192.168.100.16:80	TCP:S

Also schreibe ich die IPv4-Adresse des neuen Servers in die passende Gruppe und versuche es erneut:

Firewall / Aliases / Edit

Properties

Name: ServerIn_HTTPS
The name of the alias may only consist of the characters *a-z, A-Z, 0-9 and _*.

Description: Services mit HTTPS
A description may be entered here for administrative reference (not parsed).

Type: Host(s)

Host(s)

Hint: Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	Service	Action
192.168.100.18	WS-MON (PRTG)	Delete
192.168.100.7	WS-RA1 (WAP)	Delete
192.168.100.17	WS-RA2 (WAP)	Delete
192.168.100.6	WS-CA1 (PKI+CES)	Delete
192.168.100.23	WS-ATA (ATA)	Delete
192.168.100.22	WS-WAC (WAC)	Delete
192.168.100.16	WS-RDS1 (RDSWEB)	Delete

Die Webseite lässt sich nun fehlerfrei aufrufen:

Web Access für Remotedesktop

https://rdsweb.ws.its/RDWeb/Pages/de-DE/login.aspx?ReturnUrl=/RC

Work Resources
RemoteApp- und Desktopverbindung

Hilfe

Domäne\Benutzername:

Kennwort:

Sicherheit

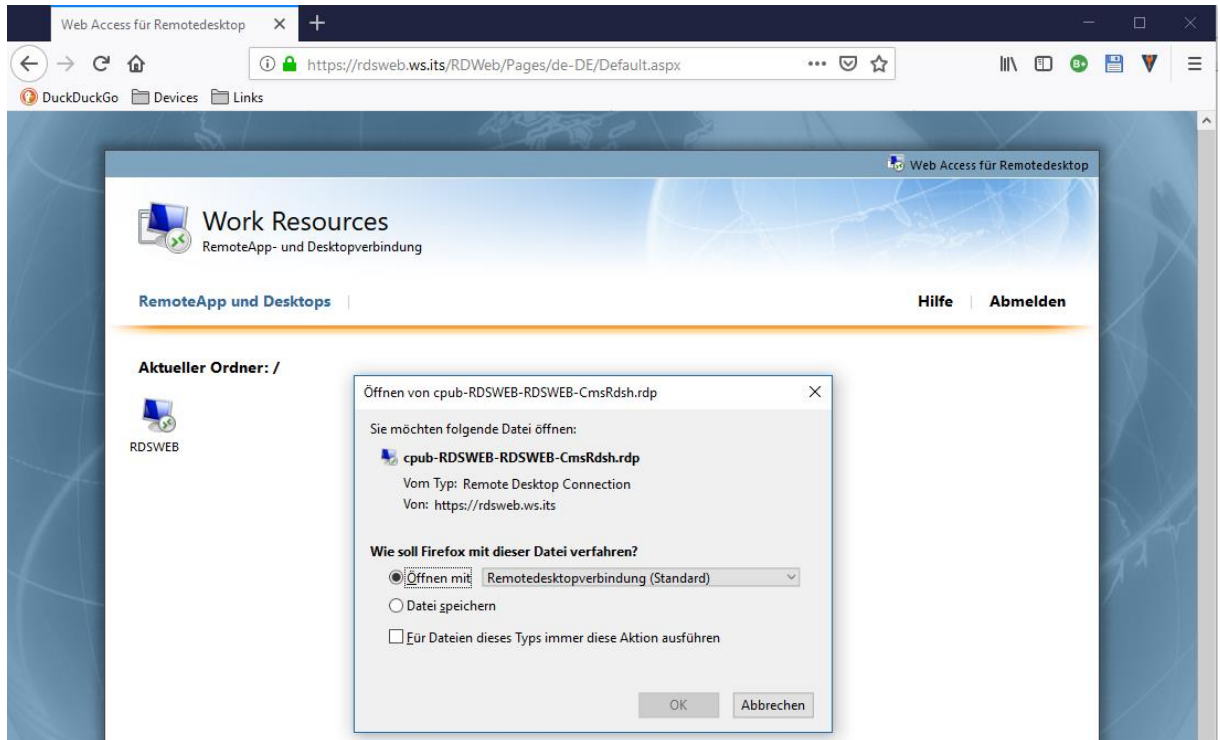
Warnung: Wenn Sie sich bei dieser Webseite anmelden, bestätigen Sie, dass dieser Computer die Sicherheitsrichtlinien Ihrer Organisation erfüllt.

Anmelden

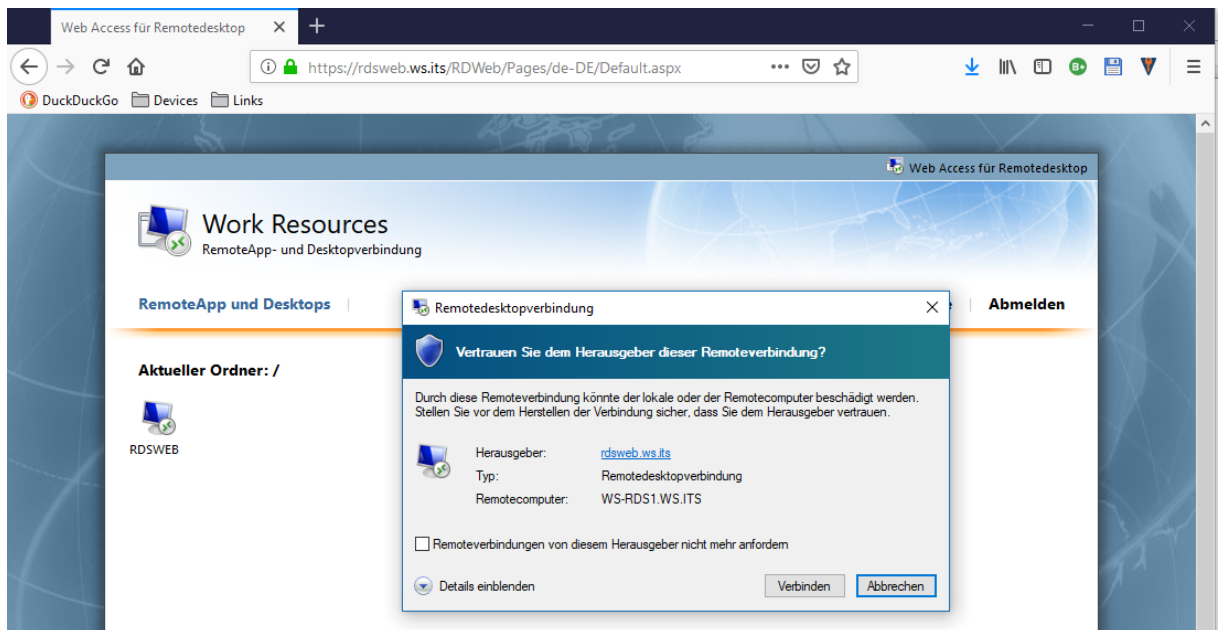
Zum Schutz vor unberechtigtem Zugriff tritt für die Sitzung von Web Access für Remotedesktop nach einem Zeitraum der Inaktivität automatisch eine Zeitüberschreitung ein. Wenn die Sitzung beendet wird, aktualisieren Sie den Browser, und melden Sie sich erneut an.

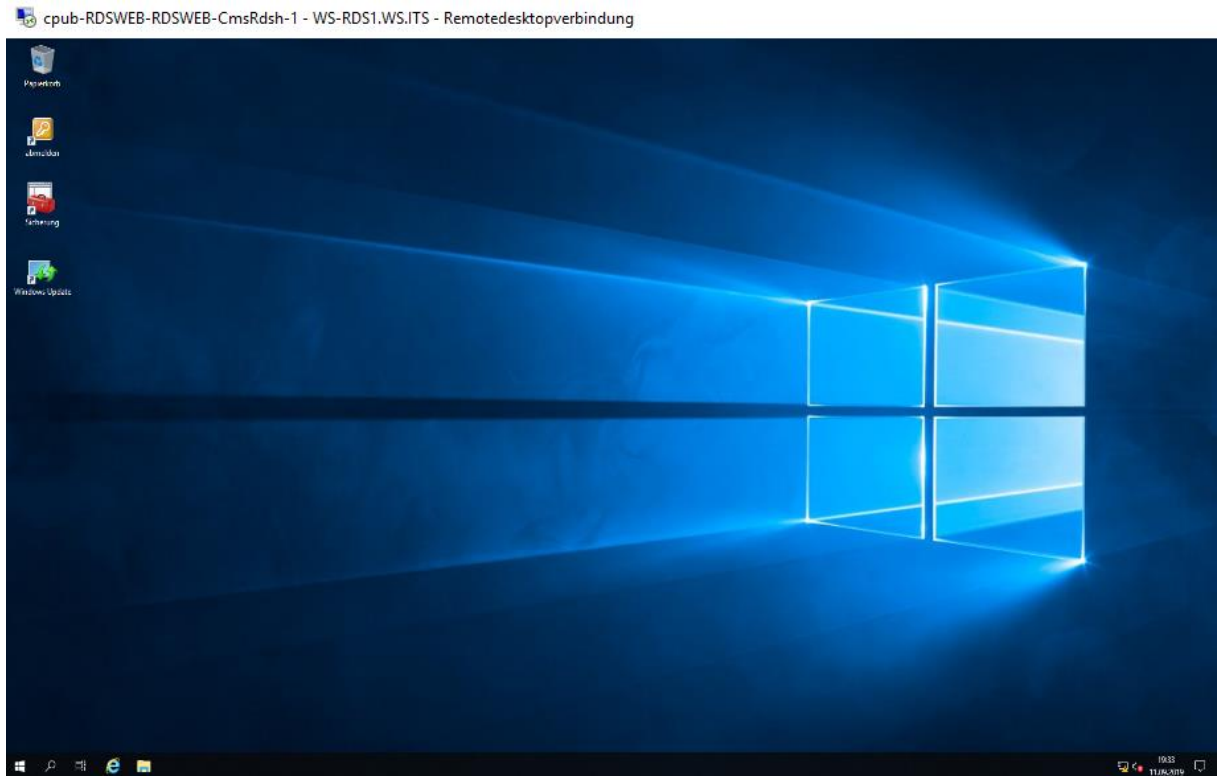
Windows Server 2019 Microsoft

Nach der Anmeldung wird die SessionCollection angezeigt:



Und über die RDP-Datei gelange ich auf meinen neuen Server. Natürlich noch ohne SingleSignOn:



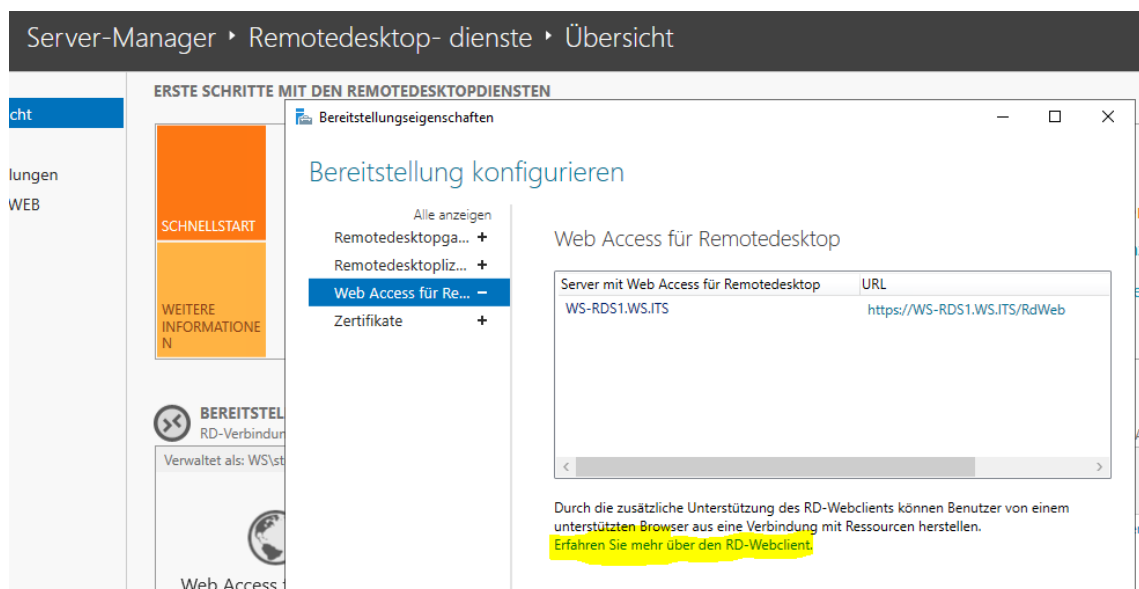


Das Grundgerüst steht.

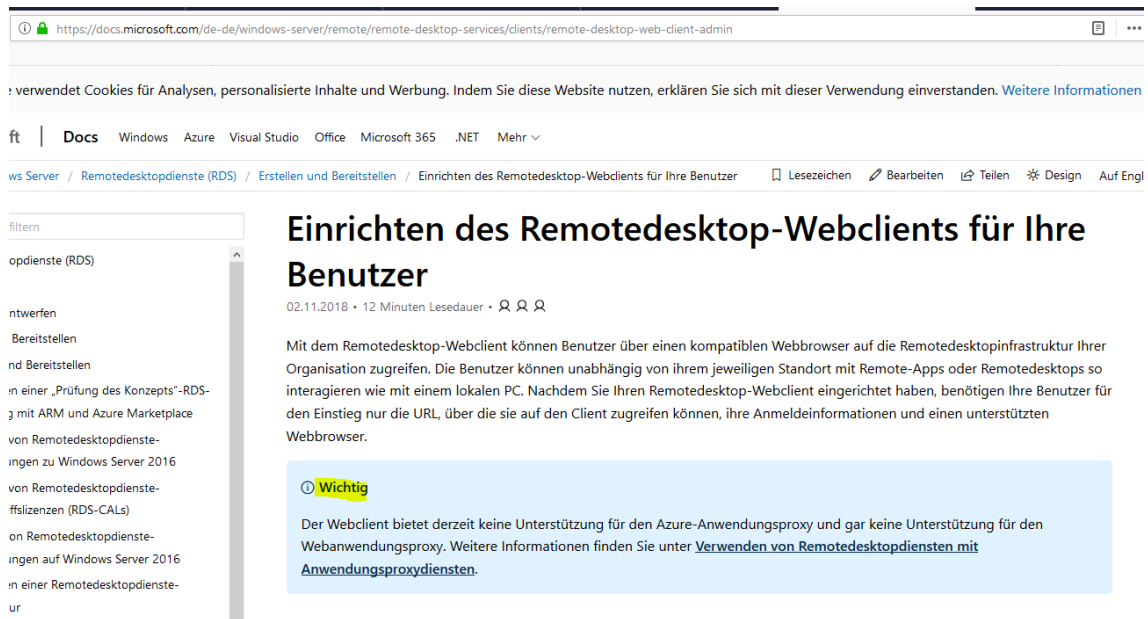
Erweiterung auf den HTML5-WebClient

Installation des HTML5-Clients

So eine Collection habe ich aber schon. Ich möchte den Zugriff über HTML5 im Browser ermöglichen. Im Servermanager stand vorhin dazu ein passender Hinweis:



Ich folge dem Link und gelange auf eine MSDocs-Seite. Gleich zu Beginn wird ein Hinweis angezeigt:



The screenshot shows a Microsoft documentation page in German. The title is "Einrichten des Remotedesktop-Webclients für Ihre Benutzer". The page includes a navigation menu with "Docs", "Windows", "Azure", "Visual Studio", "Office", "Microsoft 365", ".NET", and "Mehr". The breadcrumb trail is "ws Server / Remotedesktopdienste (RDS) / Erstellen und Bereitstellen / Einrichten des Remotedesktop-Webclients für Ihre Benutzer". The main content area has a search bar and a list of related articles on the left. The main text explains that the Remote Desktop Webclient allows users to access the Remote Desktop infrastructure through a compatible web browser. A blue callout box with a yellow "Wichtig" (Important) icon states: "Der Webclient bietet derzeit keine Unterstützung für den Azure-Anwendungsproxy und gar keine Unterstützung für den Webanwendungsproxy. Weitere Informationen finden Sie unter [Verwenden von Remotedesktopdiensten mit Anwendungsproxys](#)." The page footer shows "02.11.2018 • 12 Minuten Lesedauer • 2 2 2".

Der Webclient kann wohl nicht mit einem WebApplicationProxy konfiguriert werden. Manchmal weiß ich echt nicht, wie Microsoft sowas veröffentlichen kann. Es nerft. Ich probiere es dennoch aus. Kein Support muss ja nicht zwingend bedeuten, dass es nicht funktioniert. Und Support will ich von denen eh keinen haben...

Die Anleitung zeigt, wie das Setup über die PowerShell ausgeführt wird. Die relevanten Befehle habe ich hier zusammengestellt. Dazu habe ich einige Vereinfachungen geschrieben:

```
Install-Module -Name PowerShellGet -Force
# PowerShell neustarten

Install-Module -Name RDWebClientManagement
Install-RDWebClientPackage
Get-RDWebClientPackage

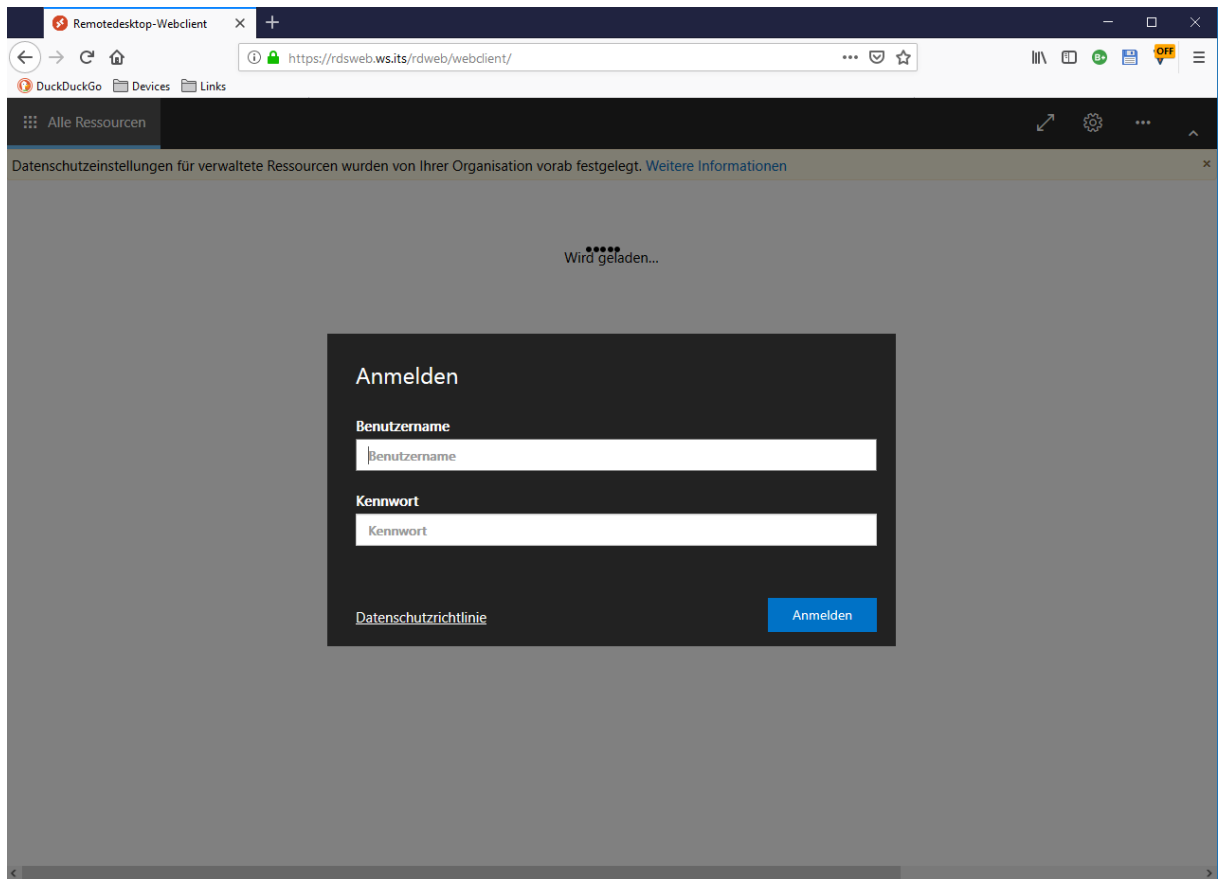
$BrokerCertThumbprint = (Get-RDCertificate -Role RDRedirector).Thumbprint
Get-ChildItem -Path "Cert:\LocalMachine\My\$BrokerCertThumbprint" |
    Export-Certificate -FilePath 'C:\Broker.cer' | Out-Null

Import-RDWebClientBrokerCert -Path 'C:\Broker.cer'
Publish-RDWebClientPackage -Type Production -Latest
```

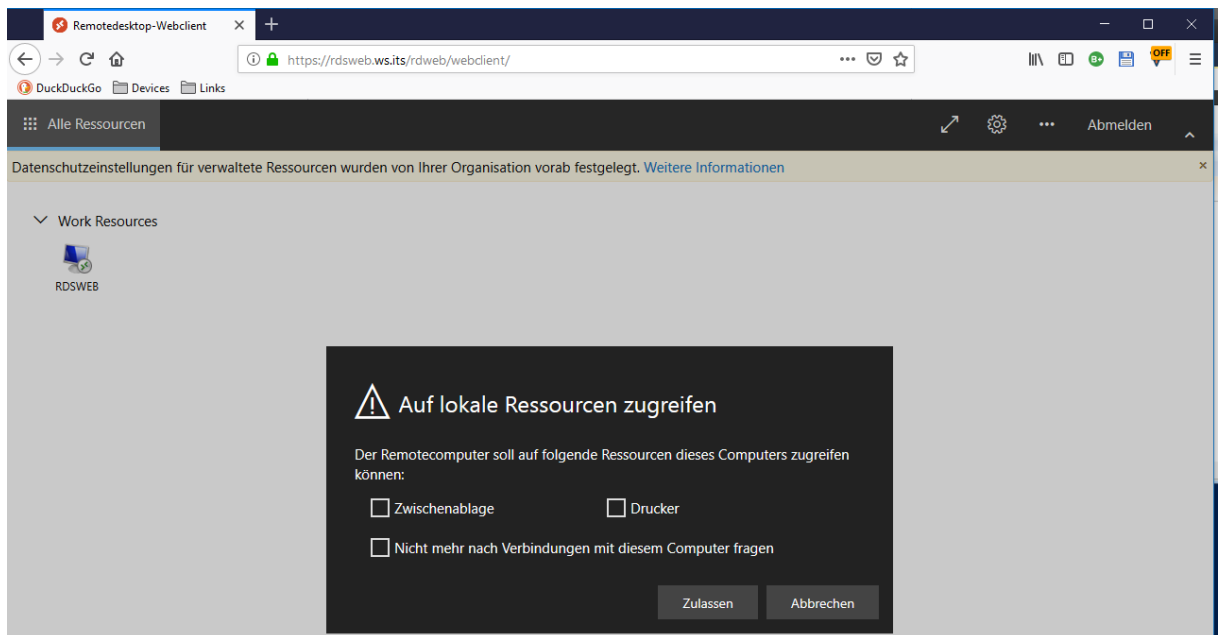
Dem Webclient muss das richtige Zertifikat zugewiesen werden. Dieses muss man aber vorher exportieren. Das Setup benötigt eine Internetverbindung. In der Anleitung gibt es zwar auch eine Offline-Variante, aber die lief bei mir nicht. Daher habe ich den Server für das Setup in der Firewall freigeschaltet. So lief es problemlos durch.

Troubleshooting – Problem „Firewall“

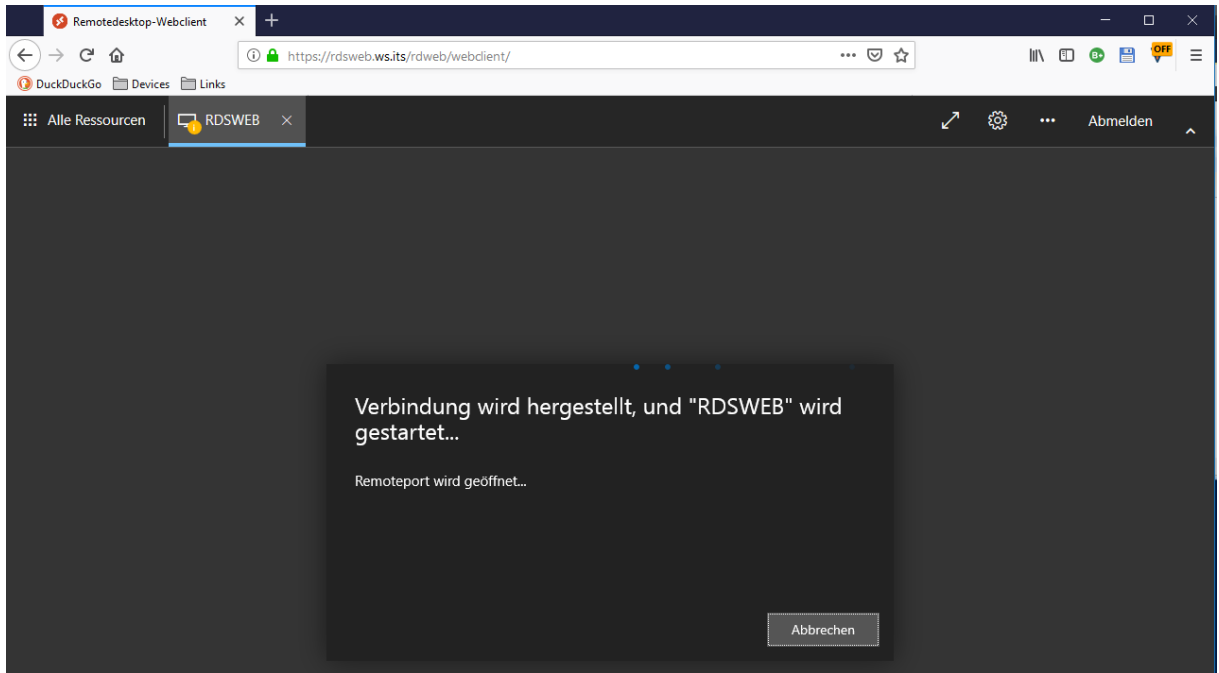
Dann teste ich den Webclient mal von intern. Im Browser muss diese Adresse aufgerufen werden: <https://rdsweb.ws.its/rdweb/webclient/>. Die Anmeldemaske sieht vielversprechend aus:



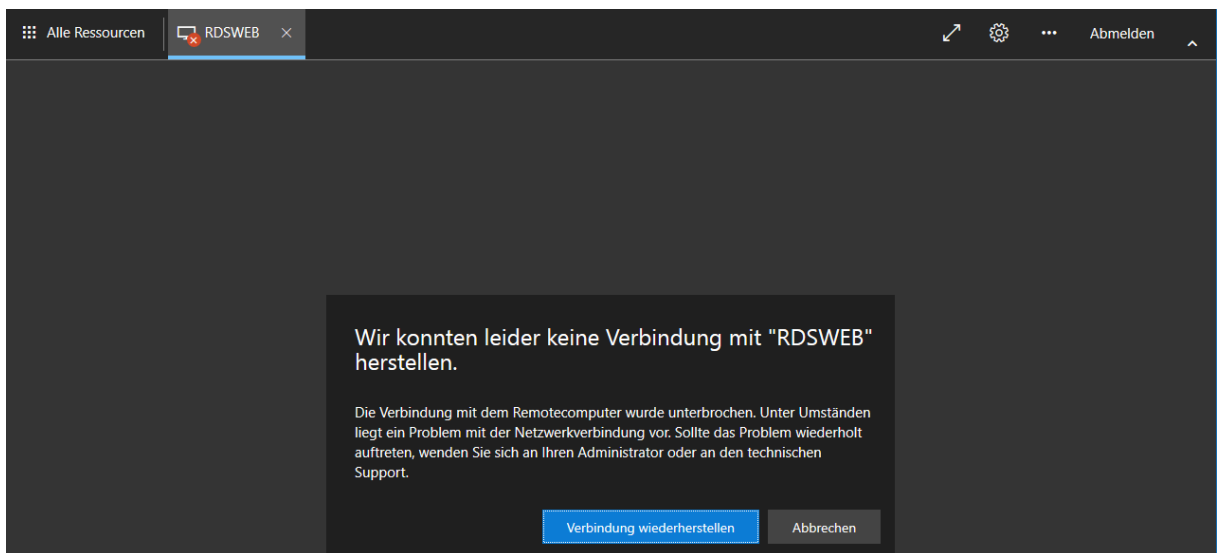
Auch die SessionCollection wird angezeigt. Und beim Start werden Verbindungsoptionen abgefragt:



Der Start dauert einige Sekunden:



Doch statt einem Desktop erhalte ich eine Fehlermeldung:



Mmh, das sieht mir nach einem Block in der Firewall aus. Ein Blick in die Logfiles meiner PFSense gibt mir Recht:

Status / System Logs / Firewall / Normal View

System Firewall DHCP Captive Portal Auth IPsec PPP VPN Load Balancer OpenVPN NTP Settings

Normal View Dynamic View Summary View

Advanced Log Filter

Source IP Address: 192.168.110.101 Destination IP Address: 192.168.100.16

Pass Time: [] Source Port: [] Protocol: [] Quantity: 500
 Block Interface: [] Destination Port: [] Protocol Flags: [] **Apply Filter**

Regular expression reference Precede with exclamation (!) to exclude match.

7 Matched Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✘	Sep 15 11:19:23	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1182	192.168.100.16:3392	TCP:S
✘	Sep 15 11:19:23	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1181	192.168.100.16:3392	TCP:S
✘	Sep 15 11:19:17	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1182	192.168.100.16:3392	TCP:S
✘	Sep 15 11:19:17	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1181	192.168.100.16:3392	TCP:S
✘	Sep 15 11:19:14	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1182	192.168.100.16:3392	TCP:S
✘	Sep 15 11:19:14	LAN_110_CLIENTS	Default deny rule IPv4 (1000000103)	192.168.110.101:1181	192.168.100.16:3392	TCP:S
✔	Sep 15 11:17:06	LAN_110_CLIENTS	Services HTTPS (1539840813)	192.168.110.101:1171	192.168.100.16:443	TCP:S

Da muss noch ein Port freigeschaltet werden. Das hole ich fix nach. Für jeden Port bzw. jede Applikation habe ich in meiner PFSense-Firewall eine Alias-Gruppe erstellt. Damit kann ich Anwendungen sehr einfach freigeben:

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / DMZ_120_EXTERN

Floating **DMZ_120_EXTERN** LAN_100_SERVER DMZ_130_INTERN LAN_110_CLIENTS DMZ_140_GAMEZONE DMZ_150_ISOLATION

Rules (Drag to Change Order)

<input type="checkbox"/>	✔	0 / 38 KiB	IPv4 TCP	Site_Neufahrn *	ServerIn_HTTP	Ports_HTTP	*	none	Zugriff HTTP	
<input type="checkbox"/>	✔	0 / 1.54 GiB	IPv4 TCP	Site_Neufahrn *	ServerIn_HTTPS	Ports_HTTP			Zugriff HTTPS	
<input type="checkbox"/>	✔	0 / 0 B	IPv4 TCP	Site_Neufahrn *	ServerIn_RDS	Ports_RDS			Zugriff RDS	
<input type="checkbox"/>	✔	0 / 33.90 MiB	IPv4 TCP	Netz_101 *	ServerIn_DPM	Ports_DPM			Zugriff DPM	

Alias details for Ports_RDS:

Value	Description
3389	RDS
443	WEB

Für diese Anwendung erweitere ich den bestehenden PortAlias „Ports_RDS“:

The screenshot shows the 'Firewall / Aliases / Edit' page in pfSense. The 'Properties' section is filled with the following information:

- Name:** Ports_RDS
- Description:** RDS (TCP&UDP)
- Type:** Port(s)

The 'Port(s)' section contains a table with the following entries:

Port	Alias	Action
3389	RDS	Delete
443	WEB	Delete
3392	RDS-Webclient	Delete

Buttons for 'Save' and '+ Add Port' are visible at the bottom.

Und jetzt nehme ich die IP-Adresse vom neuen Server in die AliasGruppe „ServerIn_RDS“ auf:

The screenshot shows the 'Firewall / Aliases / Edit' page in pfSense. The 'Properties' section is filled with the following information:

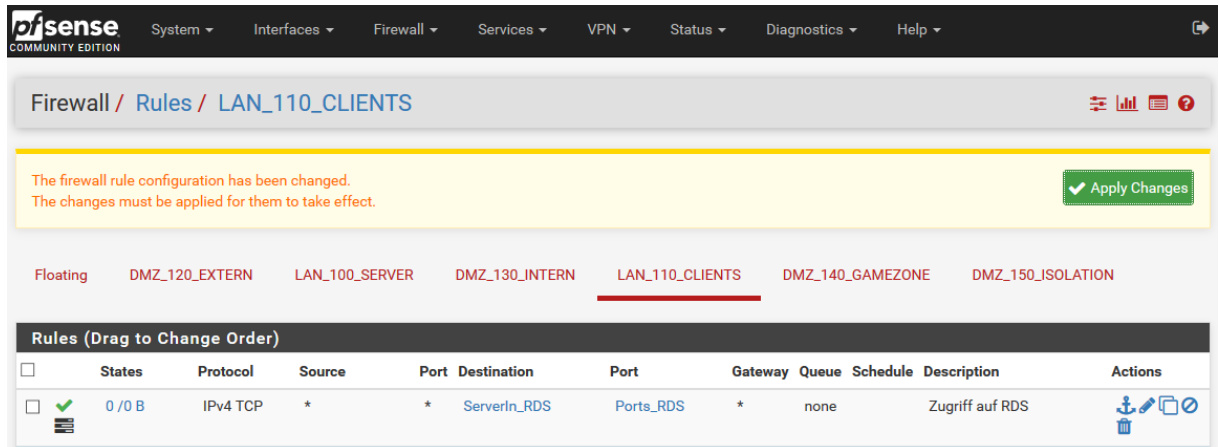
- Name:** ServerIn_RDS
- Description:** Server mit RDS
- Type:** Host(s)

The 'Host(s)' section contains a table with the following entries:

IP or FQDN	Alias	Action
192.168.110.21	WS-RDS2	Delete
192.168.100.16	WS-RDS1	Delete

Buttons for 'Save' and '+ Add Host' are visible at the bottom.

Aktuell steht der Server WS-RDS1 noch im Servernetz. Dieses kann mein Client so nicht erreichen. Also erstelle ich eine zusätzliche Ausnahme für den Zugriff:



Firewall / Rules / LAN_110_CLIENTS

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

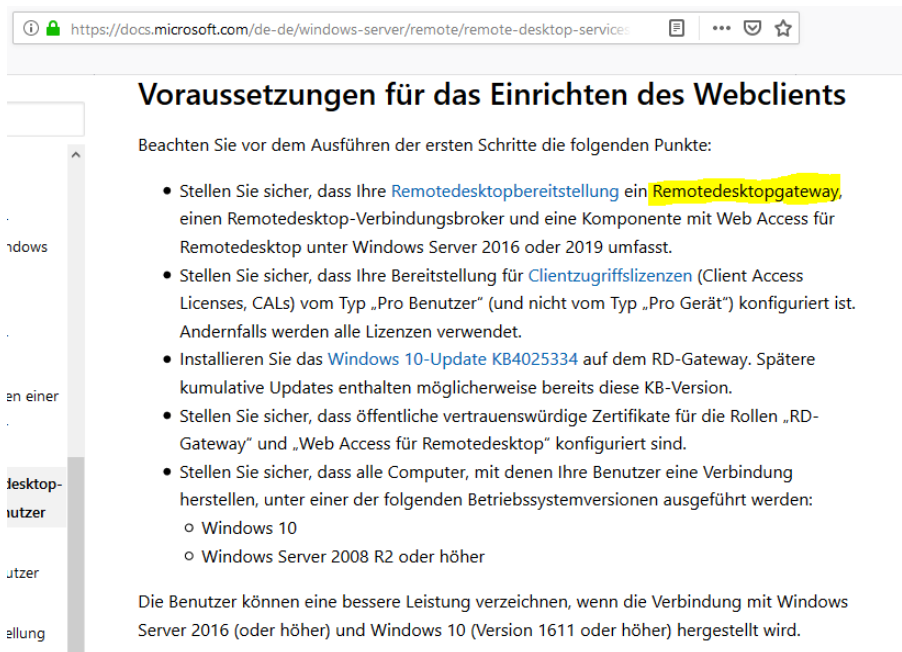
Apply Changes

Floating DMZ_120_EXTERN LAN_100_SERVER DMZ_130_INTERN LAN_110_CLIENTS DMZ_140_GAMEZONE DMZ_150_ISOLATION

Rules (Drag to Change Order)											
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
0/0 B	IPv4 TCP	*	*	ServerIn_RDS	Ports_RDS	*	none		Zugriff auf RDS	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	

Troubleshooting – Problem „RD-Gateway“

Es wird Zeit für einen weiteren Testlauf. Leider erscheint die gleiche Fehlermeldung. In der Firewall wird aber keine Verbindung mehr blockiert. Was ist da los? In der Anleitung von Microsoft finde ich den passenden Eintrag:



Voraussetzungen für das Einrichten des Webclients

Beachten Sie vor dem Ausführen der ersten Schritte die folgenden Punkte:

- Stellen Sie sicher, dass Ihre **Remotedesktopbereitstellung** ein **Remotedesktopgateway**, einen Remotedesktop-Verbindungsbroker und eine Komponente mit Web Access für Remotedesktop unter Windows Server 2016 oder 2019 umfasst.
- Stellen Sie sicher, dass Ihre Bereitstellung für **Clientzugriffslizenzen** (Client Access Licenses, CALs) vom Typ „Pro Benutzer“ (und nicht vom Typ „Pro Gerät“) konfiguriert ist. Andernfalls werden alle Lizenzen verwendet.
- Installieren Sie das **Windows 10-Update KB4025334** auf dem RD-Gateway. Spätere kumulative Updates enthalten möglicherweise bereits diese KB-Version.
- Stellen Sie sicher, dass öffentliche vertrauenswürdige Zertifikate für die Rollen „RD-Gateway“ und „Web Access für Remotedesktop“ konfiguriert sind.
- Stellen Sie sicher, dass alle Computer, mit denen Ihre Benutzer eine Verbindung herstellen, unter einer der folgenden Betriebssystemversionen ausgeführt werden:
 - Windows 10
 - Windows Server 2008 R2 oder höher

Die Benutzer können eine bessere Leistung verzeichnen, wenn die Verbindung mit Windows Server 2016 (oder höher) und Windows 10 (Version 1611 oder höher) hergestellt wird.

Mmh, ich meinte, dass für Windows Server 2019 kein RD-Gateway mehr nötig wäre. Und weiter unten in der Anleitung finde ich den passenden Abschnitt:



Herstellen einer Verbindung mit dem RD-Broker ohne RD-Gateway in Windows Server 2019

In diesem Abschnitt wird beschrieben, wie Sie eine Webclientverbindung mit einem Remotedesktop-Verbindungsbroker ohne RD-Gateway in Windows Server 2019 aktivieren.

OK, hier muss noch etwas verbogen werden. Die erforderlichen Befehle werden in der Anleitung beschrieben:

```
$BrokerCertThumbprint = (Get-RDCertificate -Role RDRedirector).Thumbprint
$BrokerCertThumbprint

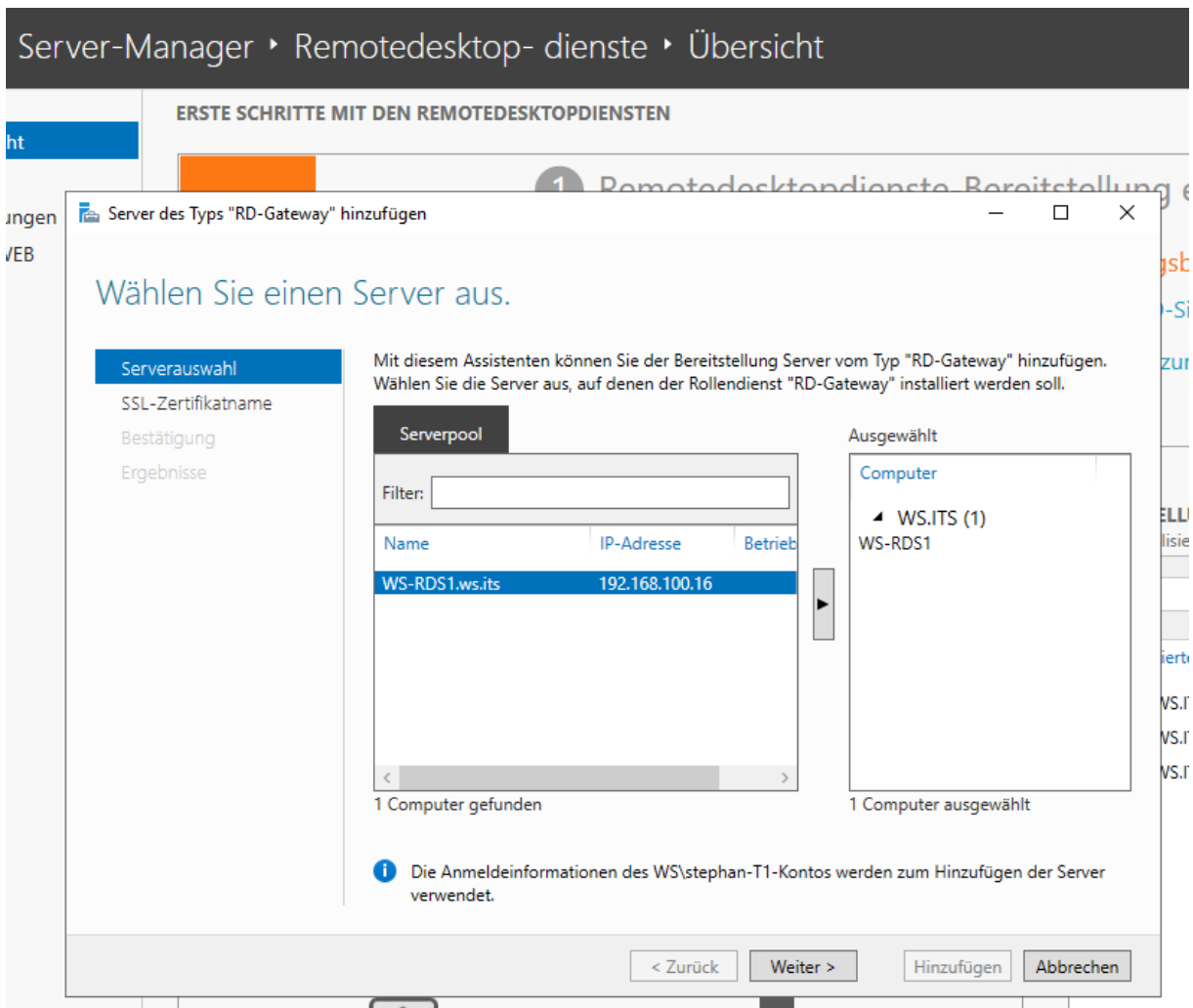
netsh http show sslcert
```

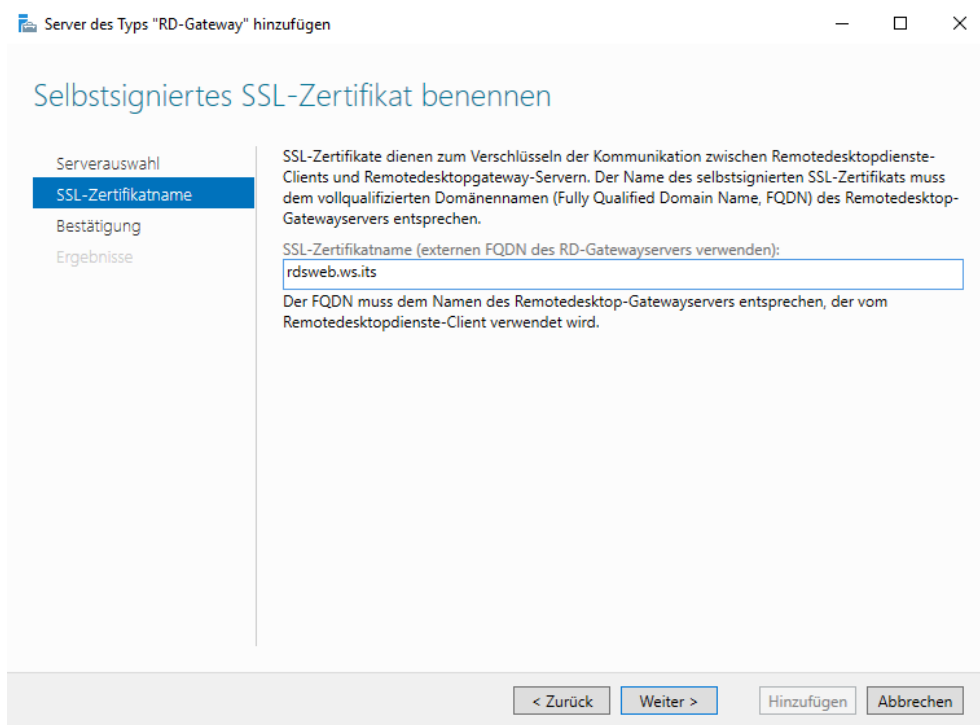
```
netsh http add sslcert ipport=0.0.0.0:3392 certhash="$BrokerCertThumprint" certstorename="Remote Desktop"appid="{00000000-0000-0000-0000-000000000000}"
netsh http show sslcert
```

Leider ergibt eine Vorprüfung, dass bei mir die Einstellungen bereits vorhanden sind:

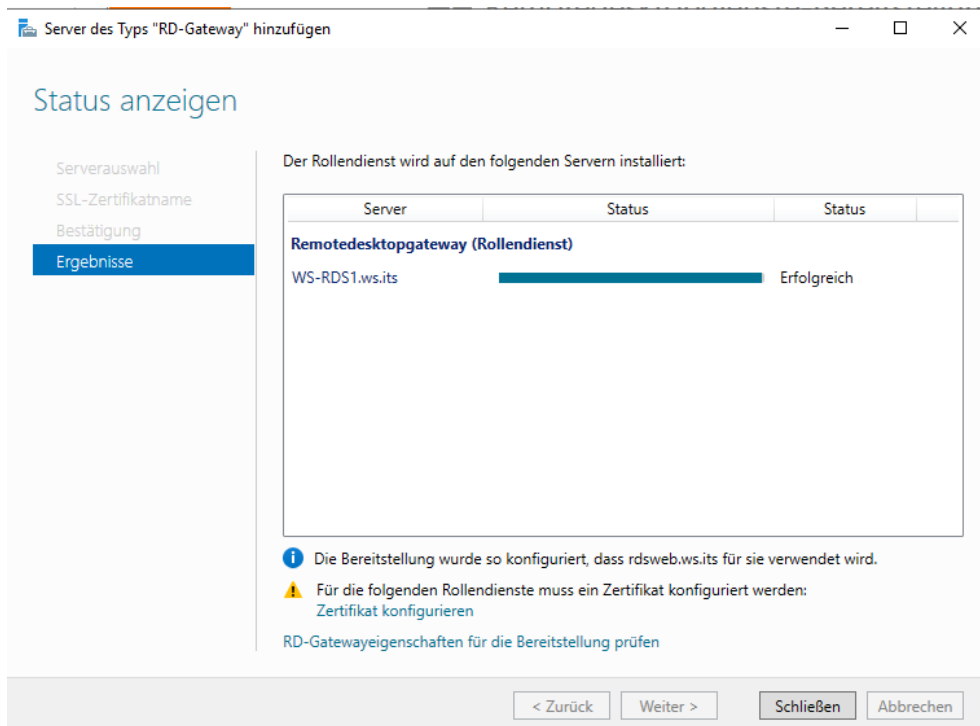
```
PS C:\Windows\system32> $BrokerCertThumprint = (Get-RDCertificate -Role RDRRedirector).Thumbprint
PS C:\Windows\system32> $BrokerCertThumprint
2BD435EF712678B6F00FFC3FF29BC1237E45512C
PS C:\Windows\system32> netsh http show sslcert
SSL-Zertifikatbindungen:
-----
IP:Port                : 0.0.0.0:3392
Zertifikathash         : 2bd435ef712678b6f00ffc3ff29bc1237e45512c
Anwendungs-ID         : {00000000-0000-0000-0000-000000000000}
Zertifikatspeichername : My
Clientzertifikatsperre berprfen : Enabled
Zur Sperrberprfung ausschlieälich zwischengespeichertes Clientzertifikat verwenden : Disabled
Verwendungsberprfung   : Enabled
Sperraktualisierungszeit : 0
Zeitlimit fr URL-Abruf   : 0
Steuerelement-ID      : (null)
Steuerelement-Speichername : (null)
```

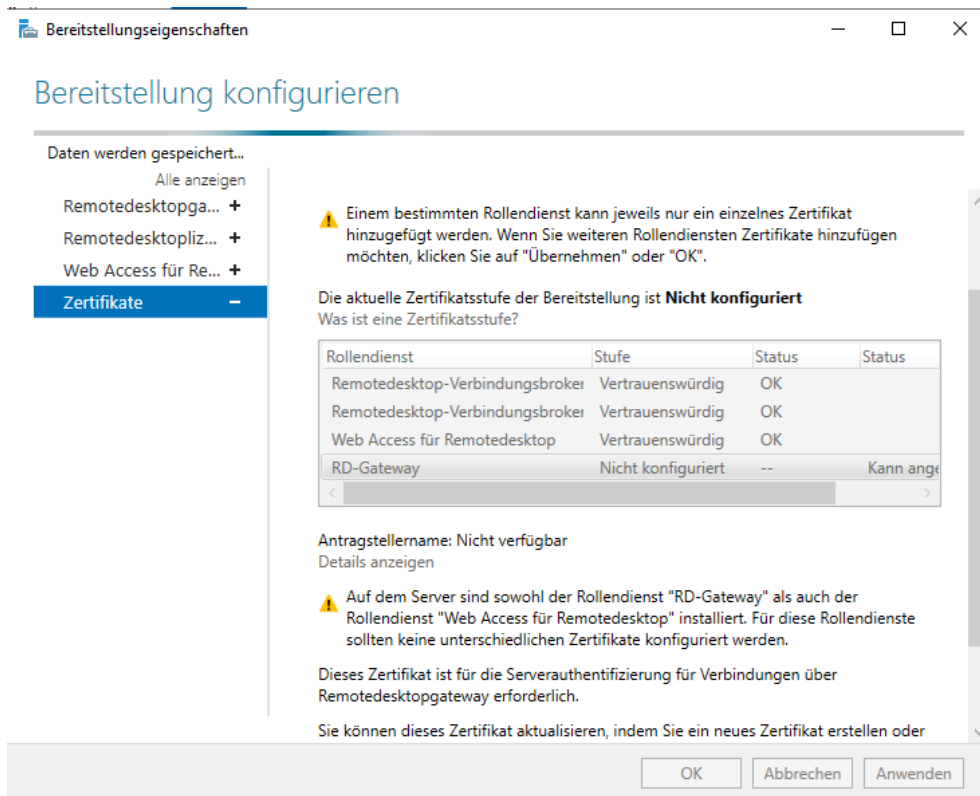
Da auch ein Versuch aus dem gleichen Netzwerksegment fehlschlägt installiere ich die Rolle RD-Gateway nach:



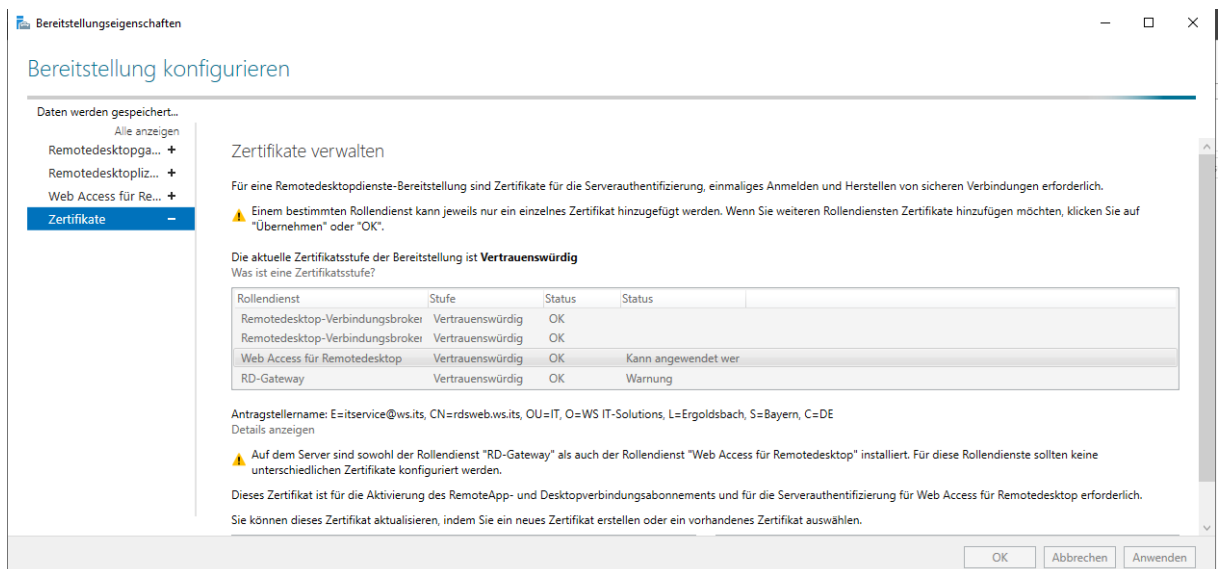


Noch belasse ich es bei dem internen Zertifikat.





Die Konfiguration braucht einen weiteren Testlauf. Das Ergebnis ist aber unverändert. In der Anleitung von Microsoft steht, der RD-Gateway-Service muss mit einem öffentlichen Zertifikat ausgestattet sein. OK, für meinen alten RDS-Service habe ich noch eins. Das importiere ich im nächsten Schritt. Unterschiedliche Zertifikate für RD-Web und RD-Gateway sind nicht erlaubt. Daher ändere ich beide ab:



Damit nun aber die Namensauflösung passt, ändere ich den DNS-Record für rds.ws-ist.de auf meinem DC:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[25], ws-dc1.ws.its., hostm...	Static
(identisch mit übergeordne...	Host (A)	192.168.110.21	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc1.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc2.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc3.ws.its.	Static

Host (A)	Sicherheit
Host (bei Nichtangabe wird übergeordnete Domäne verwendet): (identisch mit übergeordnetem Ordner)	
Vollqualifizierter Domänenname: rds.ws-its.de	
IP-Adresse: 192.168.100.16	
<input type="checkbox"/> Entsprechenden Zeigereintrag (PTR) aktualisieren	
<input type="checkbox"/> Eintrag löschen, sobald er verfällt	
Zeitstempel des Eintrags: <input type="text"/>	
Gültigkeitsdauer (TTL): 0 :0 :5 :0 (TTTT.HH.MM.SS)	

Troubleshooting – Problem „Authentifizierung“

Aber selbst jetzt kommt diese Fehlermeldung! Logfiles mit Fehlern oder passende Eventlogs suche ich vergebens. Vielleicht sind es die Gruppenrichtlinien, die ich auf das System anwende? Ich deaktiviere alle GPOs, starte das System neu und versuche es wieder. Das Problem bleibt aber bestehen

Die Ursache liegt woanders. Es muss eine Einschränkung sein. Im Netzwerk kann sie nicht liegen, da ist nun alles freigeschaltet. Ist es ein Authentifizierungsproblem? Ich hatte vor einiger Zeit NTLMv2 aus meiner AD-Infrastruktur verbannt. Auf meinen Domain Controllern habe ich für genau diesen Fall das Logging aktiviert. Mit einem PowerShell-Script kann ich die Eventlogs aller DCs prüfen:

```

1 cls;
2 Invoke-Command -ComputerName (Get-ADDomain).ReplicaDirectoryServers -ScriptBlock {
3   Get-WinEvent -Path C:\Windows\System32\Winevt\Logs\Microsoft-Windows-NTLM%4Operational.evtx -MaxEvents 20 -ErrorAction SilentlyContinue |
4   Select-Object -Property @{ n='DC' ; e={ $env:COMPUTERNAME } };
5   @{} |>> {
6     @{ n='Datetime' ; e={ (Get-Date -Date $_.TimeCreated -Format u) -replace 'z' } };
7     @{ n='Client' ; e={ ((($_.Message -split "n" | select-string 'Arbeitsstationsname') -split ':')[1].trim() ) } };
8     @{ n='Server' ; e={ ((($_.Message -split "n" | select-string 'Name des sicheren Kanals') -split ':')[1].trim() ) } };
9     @{ n='Domain' ; e={ ((($_.Message -split "n" | select-string 'Domänenname') -split ':')[1].trim() ) } };
10    @{ n='User' ; e={ ((($_.Message -split "n" | select-string 'Benutzername') -split ':')[1].trim() ) } };
11 } | Sort-Object -Property Datetime |
Format-Table -Property DC,Datetime,Client,Server,Domain,User

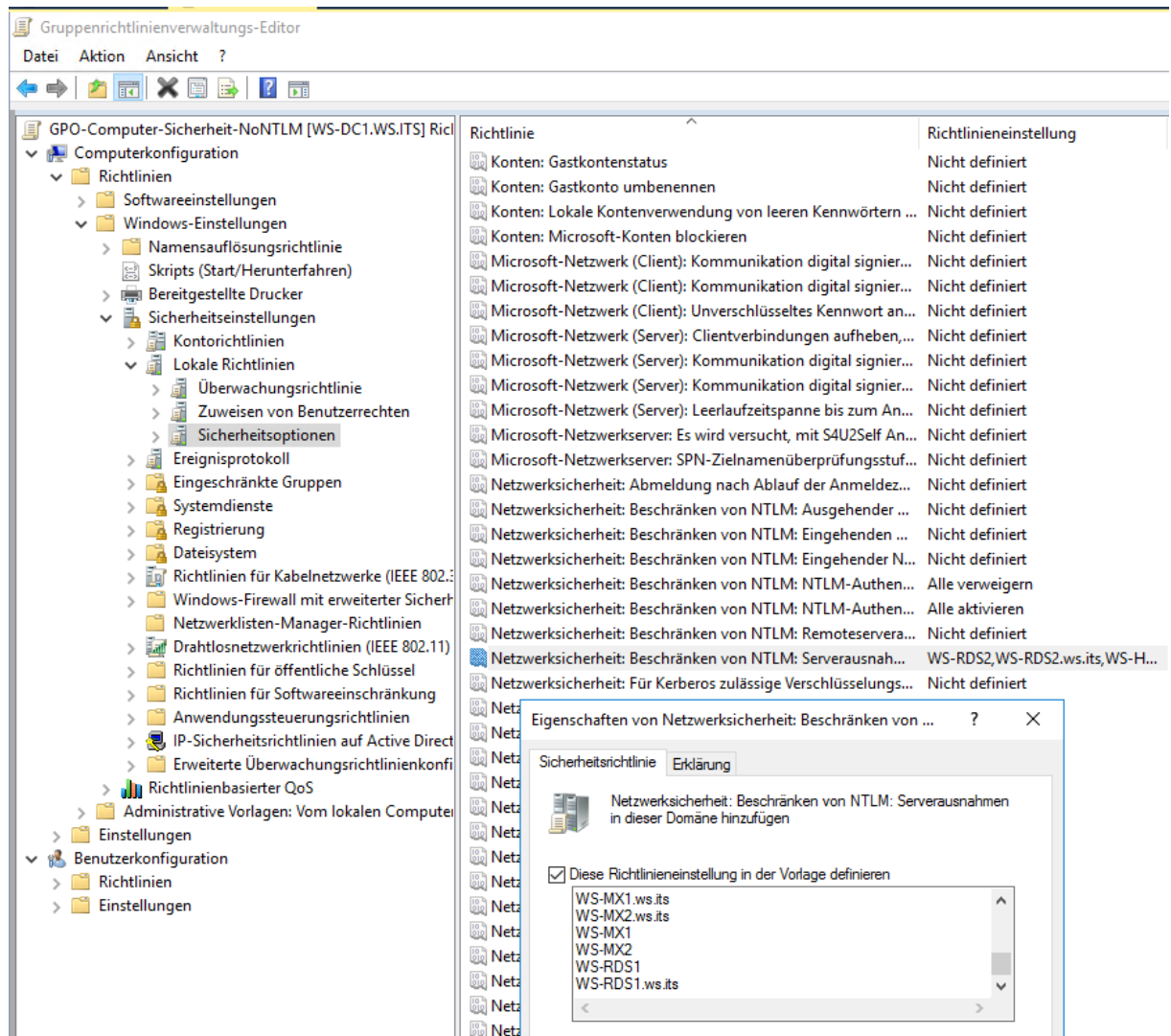
```

```

WS-DC1 2019-09-16 05:17:32 \\WS-MON WS-NAS1 ws sysadm
WS-DC1 2019-09-16 05:17:32 \\WS-MON WS-NAS1 ws sysadm
WS-DC3 2019-09-16 06:50:36 WS-ATA WS-CL3 ws.its service-ata
WS-DC3 2019-09-16 11:07:40 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:40 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:40 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:41 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:41 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:41 WS-MON WS-CL3 ws sysadm
WS-DC3 2019-09-16 11:07:41 WS-MON WS-CL3 ws sysadm
WS-DC2 2019-09-16 12:24:22 WS-ATA WS-CA1 ws.its service-ata
WS-DC2 2019-09-16 19:08:42 WS-ATA WS-CM ws.its service-ata
WS-DC1 2019-09-16 19:44:08 NULL WS-RDS1 ws stephan
WS-DC1 2019-09-16 19:45:42 NULL WS-RDS1 ws stephan
WS-DC1 2019-09-16 19:47:19 NULL WS-RDS1 ws stephan

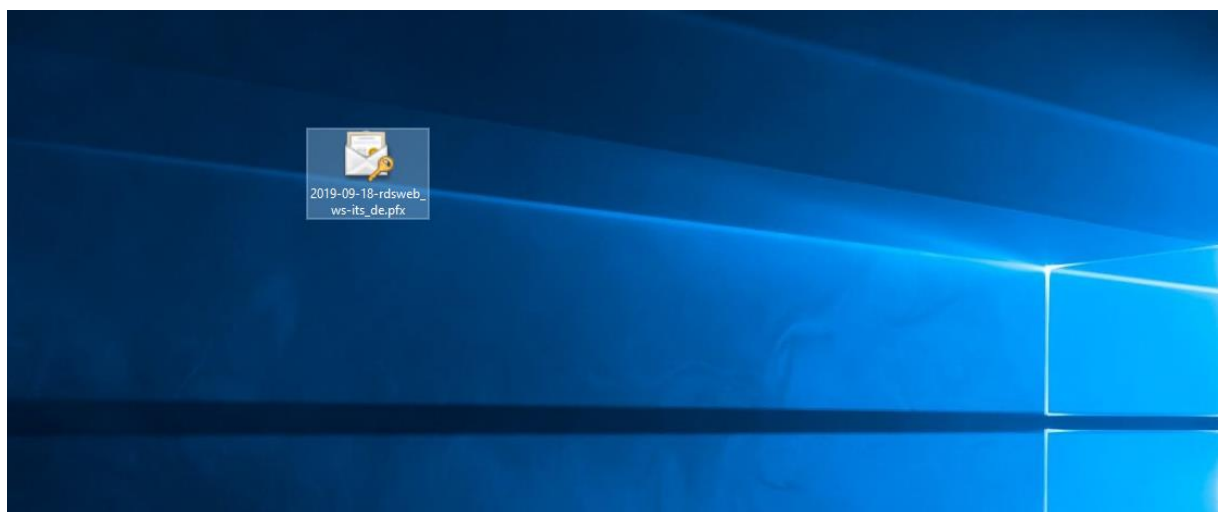
```

Das ist ein Volltreffer: Der Domain Controller blockiert die Authentifizierung, die offenbar mit NTLM forciert wird... In der GPO, mit der ich NTLM deaktiviert habe, gibt es auch eine Ausnahme-Einstellung: Hier trage ich den Server WS-RDS1 mit ein:



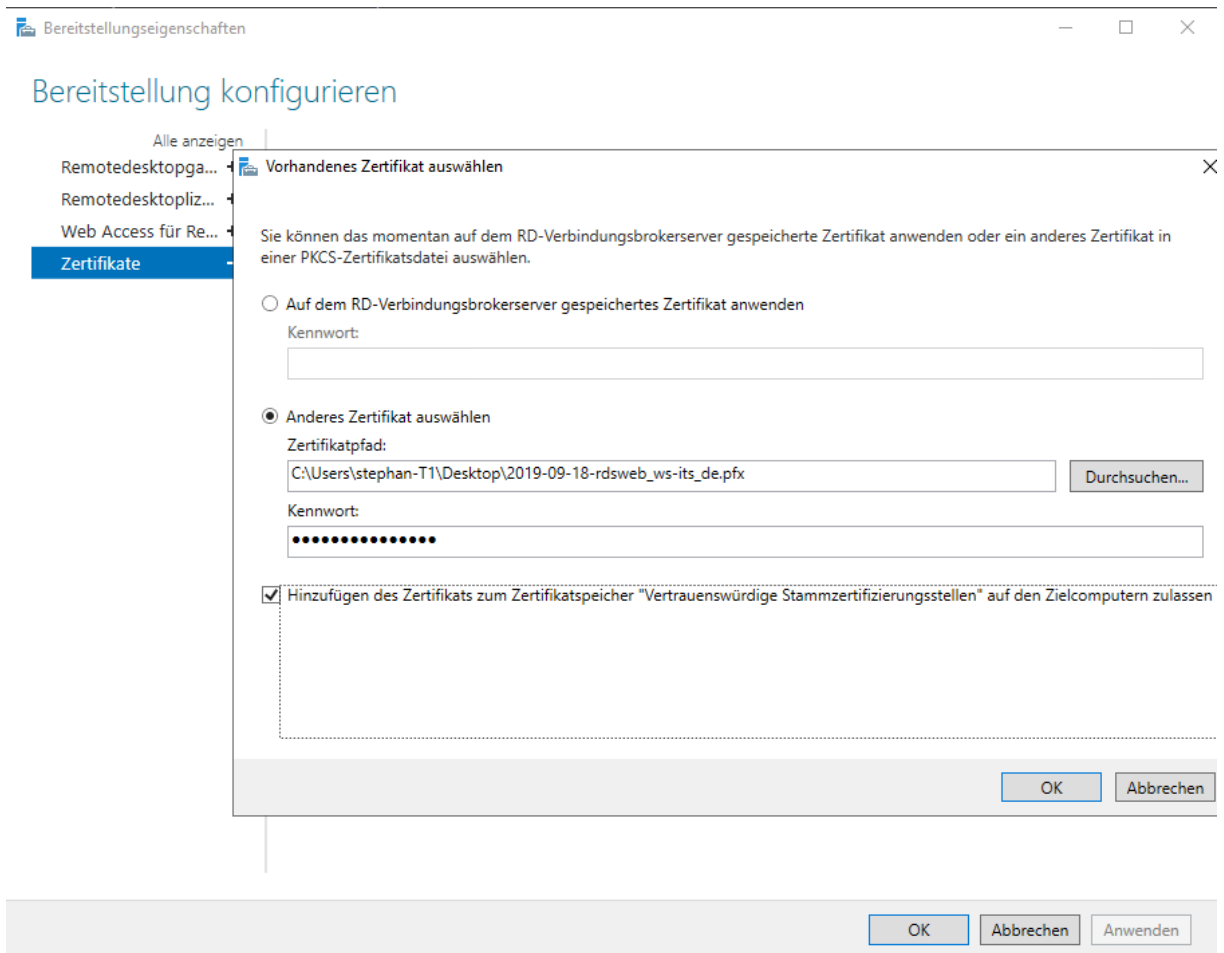
Troubleshooting – Problem „Zertifikat“

Doch das Problem besteht weiter. Da es aber nicht meine erste RDS-Infrastruktur ist, fällt mir die Lösung (etwas spät) ein: Das RD-Gateway benötigt ein öffentliches Zertifikat. Na klar! In der Anleitung stand es ja auch drin... Aber bevor ich eines kaufe, erstelle ich ein öffentlich gültiges Testzertifikat für 30 Tage bei PSW. Der Request ist leicht erstellt und das Zertifikat ist einsatzbereit:



Den Namen habe ich auf eine öffentliche Subdomain rdsweb.ws-its.de erstellt. Diese konfiguriere ich noch fix bei meinem Provider.

Nun installiere ich das Zertifikat im RD-Gateway:



Bereitstellung konfigurieren

- Alle anzeigen
- Remotedesktopga... +
- Remotedesktoppliz... +
- Web Access für Re... +
- Zertifikate -**

Zertifikate verwalten

Für eine Remotedesktopdienste-Bereitstellung sind Zertifikate für die Serverauthentifizierung, einmaliges Anmelden und Herstellen von sicheren Verbindungen erforderlich.

⚠ Einem bestimmten Rollendienst kann jeweils nur ein einzelnes Zertifikat hinzugefügt werden. Wenn Sie weiteren Rollendiensten Zertifikate hinzufügen möchten, klicken Sie auf "Übernehmen" oder "OK".

Die aktuelle Zertifikatsstufe der Bereitstellung ist **Vertrauenswürdig**

Was ist eine Zertifikatsstufe?

Rollendienst	Stufe	Status	Status
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	
Web Access für Remotedesktop	Vertrauenswürdig	OK	Kann angewendet werden
RD-Gateway	Vertrauenswürdig	OK	

Antragstellername: E=itservice@ws.its, CN=rdsweb.ws.its, OU=IT, O=WS IT-Solutions, L=Ergoldsbach, S=Bayern, C=DE
[Details anzeigen](#)

⚠ Auf dem Server sind sowohl der Rollendienst "RD-Gateway" als auch der Rollendienst "Web Access für Remotedesktop" installiert. Für diese Rollendienste sollten keine unterschiedlichen Zertifikate konfiguriert werden.

Dieses Zertifikat ist für die Aktivierung des RemoteApp- und Desktopverbindungsabonnements und für die Serverauthentifizierung für Web Access für Remotedesktop erforderlich.

Sie können dieses Zertifikat aktualisieren, indem Sie ein neues Zertifikat erstellen oder ein vorhandenes Zertifikat auswählen.

Bereitstellung konfigurieren

- Alle anzeigen
- Remotedesktopga... +
- Remotedesktoppliz... +
- Web Access für Re... +
- Zertifikate -**

Zertifikate verwalten

Für eine Remotedesktopdienste-Bereitstellung sind Zertifikate für die Serverauthentifizierung, einmaliges Anmelden und Herstellen von sicheren Verbindungen erforderlich.

Die aktuelle Zertifikatsstufe der Bereitstellung ist **Vertrauenswürdig**

Was ist eine Zertifikatsstufe?

Rollendienst	Stufe	Status	Status
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	
Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	
Web Access für Remotedesktop	Vertrauenswürdig	OK	Erfolgreich
RD-Gateway	Vertrauenswürdig	OK	Erfolgreich

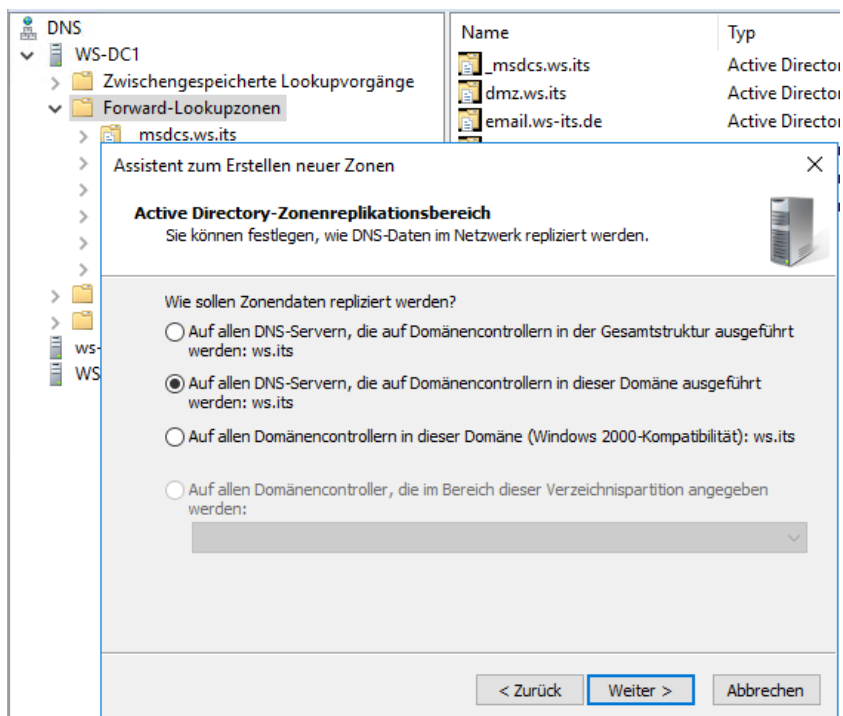
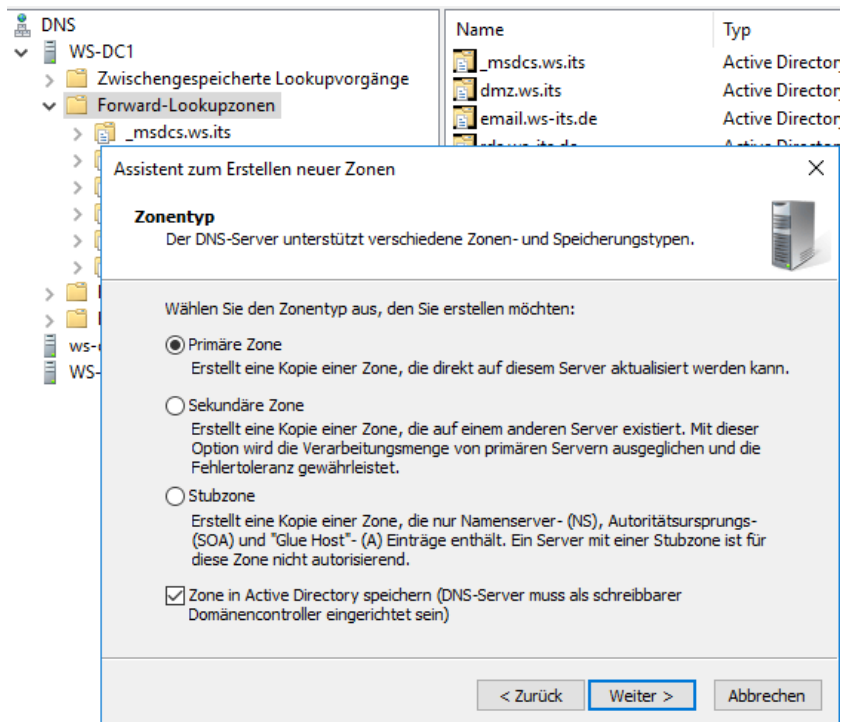
Antragstellername: CN=rdsweb.ws-its.de, OU=Domain Control Validated
[Details anzeigen](#)

⚠ Auf dem Server sind sowohl der Rollendienst "RD-Gateway" als auch der Rollendienst "Web Access für Remotedesktop" installiert. Für diese Rollendienste sollten keine unterschiedlichen Zertifikate konfiguriert werden.

Dieses Zertifikat ist für die Serverauthentifizierung für Verbindungen über Remotedesktopgateway erforderlich.

Sie können dieses Zertifikat aktualisieren, indem Sie ein neues Zertifikat erstellen oder ein vorhandenes Zertifikat auswählen. Wenn Sie dieses Zertifikat ändern, müssen Sie den Remotedesktop-Gatewaydienst auf allen RD-Gatewayservern neu starten.

Für die interne Namensauflösung verwende ich eine neue DNS-Zone mit dem Namen rdsweb.ws-its.de, die ohne Hostname direkt auf die IPv4 des Servers WS-RDS1 zeigt:



The screenshot shows the DNS console with the following table:

Name	Typ
_msdcs.ws.its	Active Director
dmz.ws.its	Active Director
email.ws-its.de	Active Director

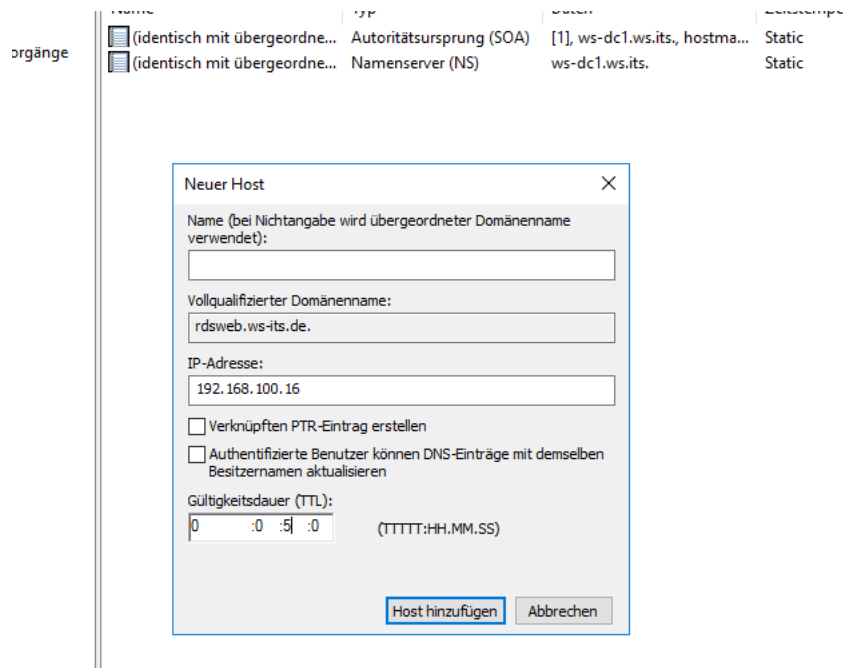
The dialog box 'Assistent zum Erstellen neuer Zonen' is open. The 'Zonenname' field contains 'rdswb.ws-its.de'. Below the field, there is explanatory text: 'Der Zonenname bestimmt den Teil des DNS-Namespace, für den dieser Server autorisierend ist. Normalerweise wird der Firmendomenenname (wie z. B. "microsoft.com") oder ein Teil des Domänennamens (wie z. B. "neuezone.microsoft.com") verwendet. Der Zonenname ist nicht der Name des DNS-Servers.'

The screenshot shows the same DNS console as above. The dialog box 'Assistent zum Erstellen neuer Zonen' is now on the 'Dynamisches Update' step. The text reads: 'Sie können festlegen, dass diese DNS-Zone sichere, unsichere oder keine dynamische Updates zulässt.'

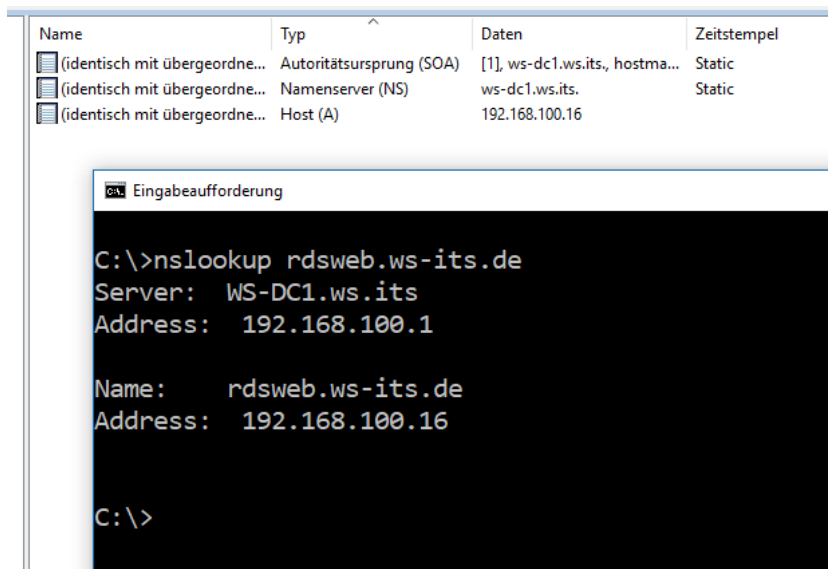
Below this, there is explanatory text: 'Dynamische Updates ermöglichen DNS-Clientcomputern, sich zu registrieren und die eigenen Ressourceneinträge dynamisch mit einem DNS-Server bei Änderungen zu aktualisieren. Bestimmen Sie den Typ des dynamischen Updates, der verwendet werden soll.'

Three radio button options are listed:

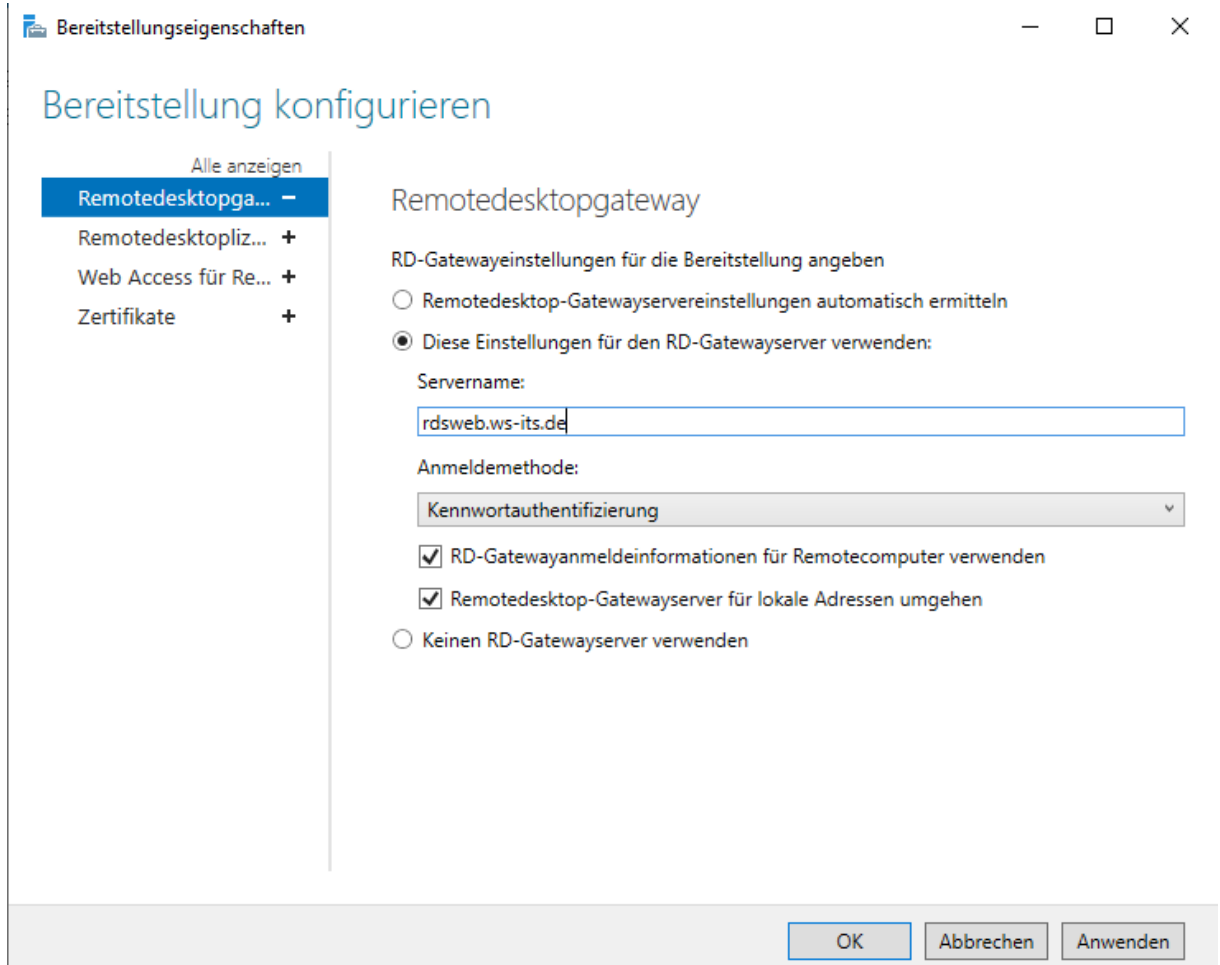
- Nur sichere dynamische Updates zulassen (für Active Directory empfohlen)
Diese Option ist nur für Active Directory-integrierte Zonen verfügbar.
- Nicht sichere und sichere dynamische Updates zulassen
Dynamische Updates von Ressourceneinträgen werden von allen Clients zugelassen.
! Durch diese Option besteht ein hohes Sicherheitsrisiko, da Updates von nicht vertrauenswürdigen Quellen angenommen werden können.
- Dynamische Updates nicht zulassen
Dynamische Updates von Ressourceneinträgen werden von dieser Zone nicht zugelassen. Diese Einträge müssen manuell aktualisiert werden.



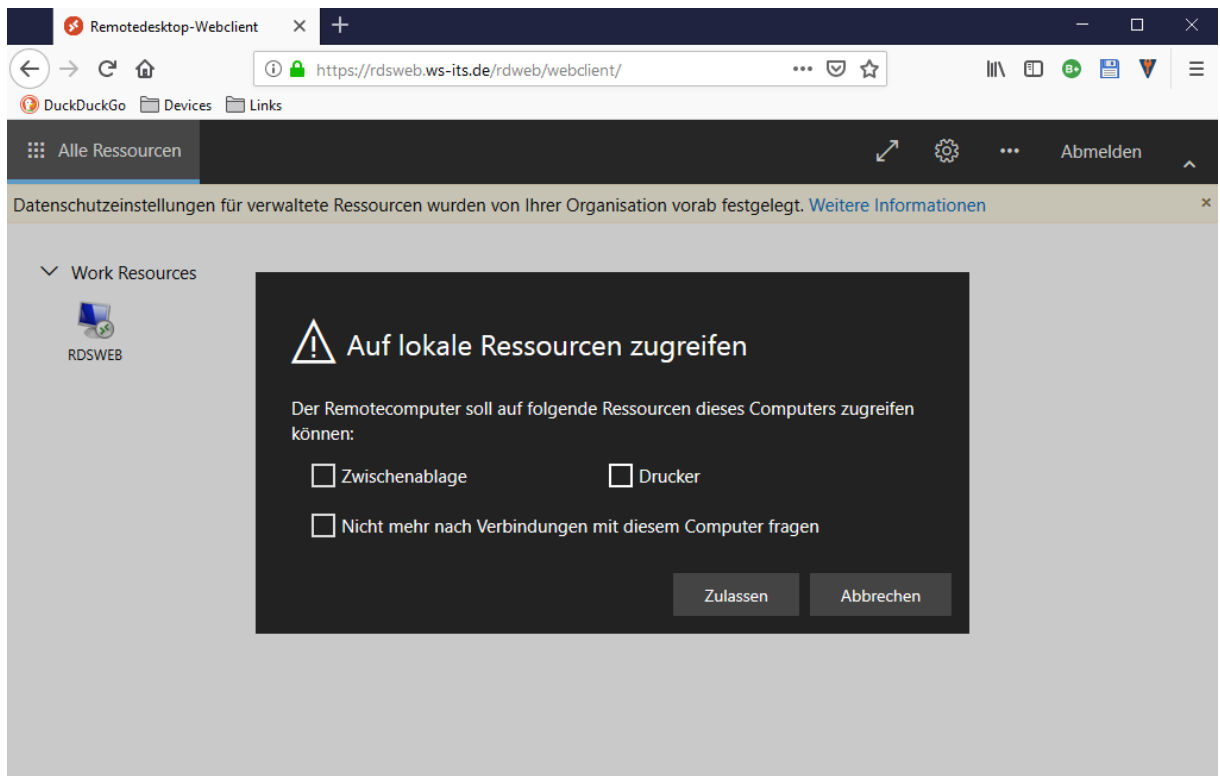
Das Ergebnis kann einfach geprüft werden: Der externe Name löst intern auf die IPv4 des Servers auf:



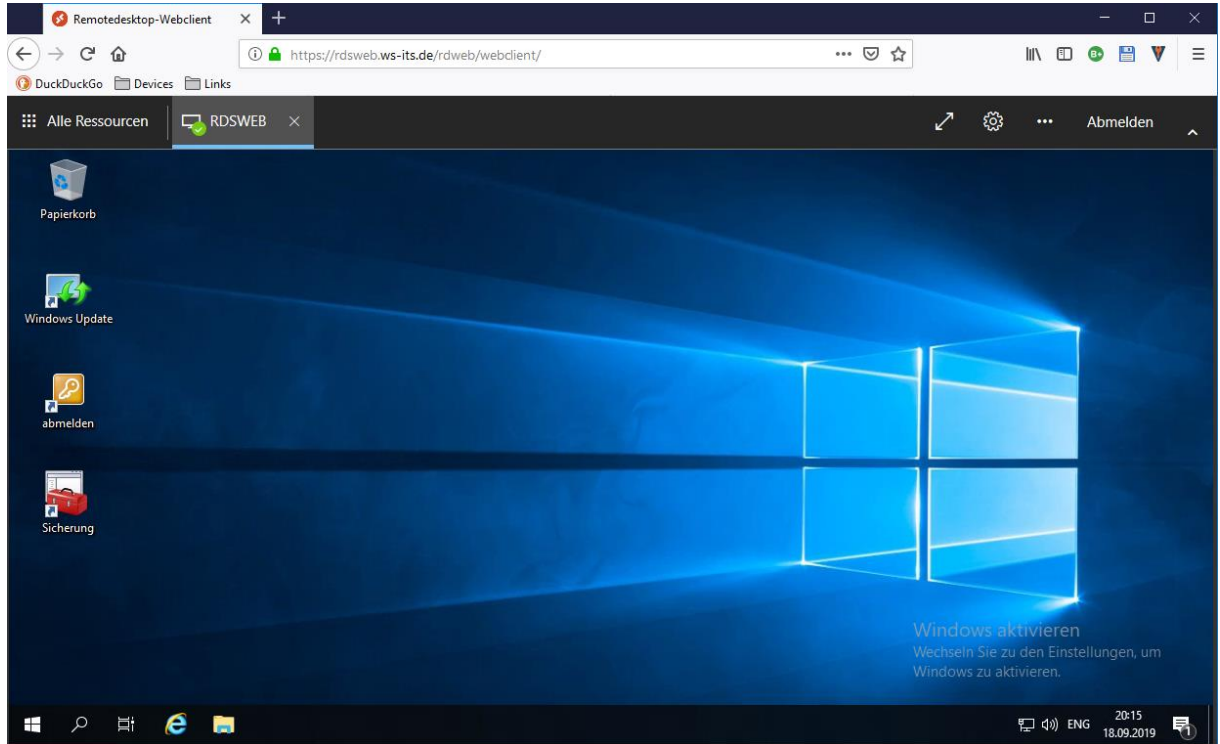
Nun muss aber auch das RD-Gateway von diesem Namen erfahren. Dazu starte ich den Bereitstellungsassistenten im Servermanager:



So. Jetzt kann wieder getestet werden. Nach der Anmeldung kommt statt der Fehlermeldung die Konfiguration der lokalen Ressourcen:



Und die Session wird im Browser angezeigt:



So hab ich mir das vorgestellt!

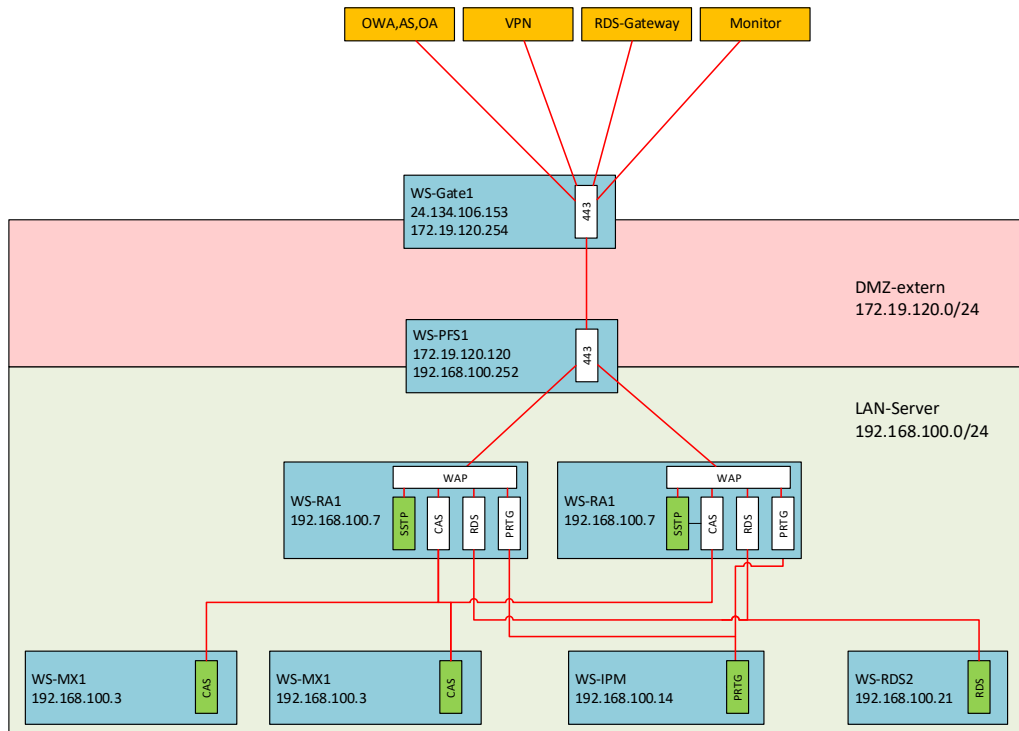
Veröffentlichung im Web Application Proxy

Der interne Zugriff funktioniert. Ich möchte die Ressource aber nach extern veröffentlichen. Und wie eingangs erwähnt verwende ich bisher einen Web Application Proxy im Clusterverbund (2x WAP und 2x ADFS auf insgesamt 4 Servern). Laut Microsoft wird dieses Szenario eigentlich nicht unterstützt. Ich will es dennoch einmal versuchen.

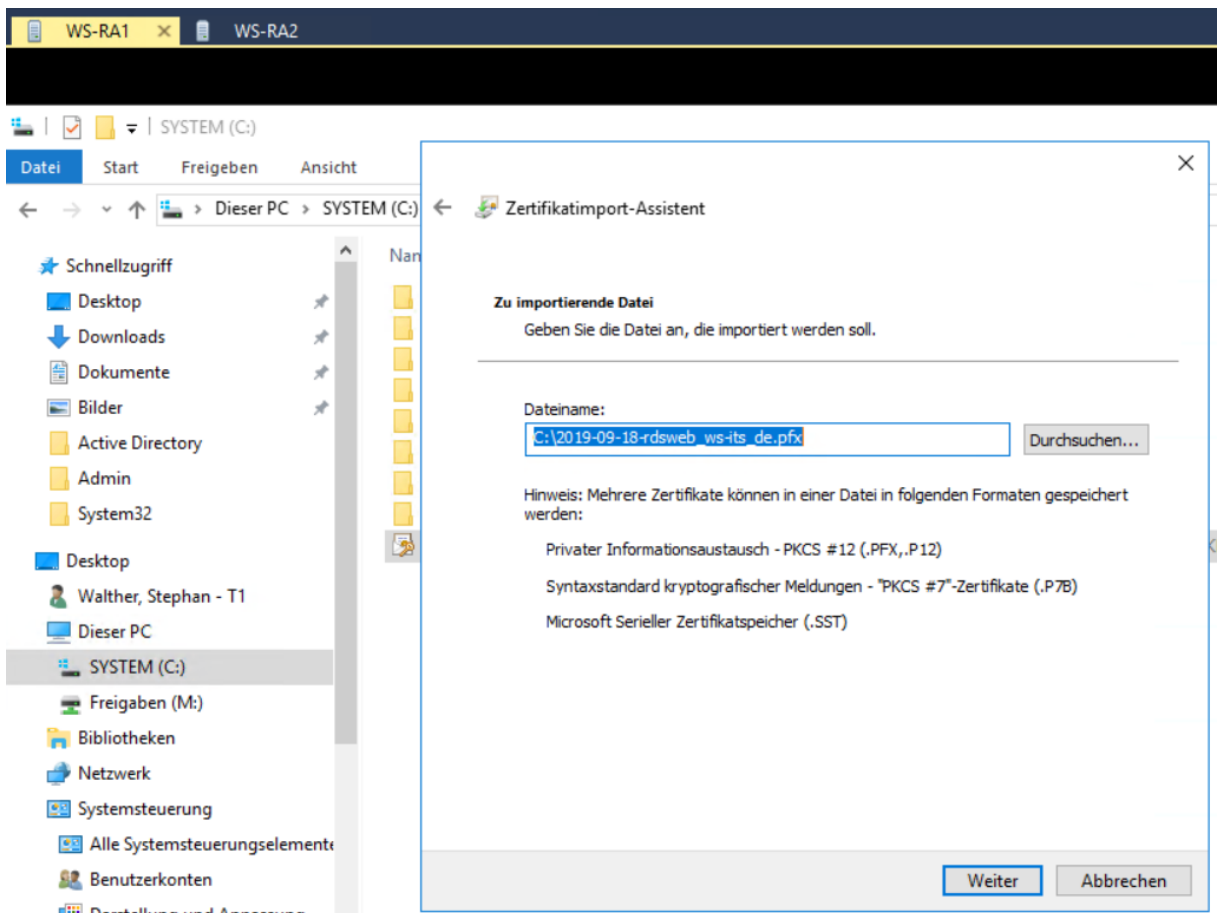
Warum so kompliziert? Ganz einfach: Ich habe von meinem Internet-Provider nur eine IPv4-Adresse erhalten. Und an dieser kann ich den Port 443 für https nur einmal anbinden. Da ich aber mehrere Webanwendungen nach extern veröffentlichen möchte (Exchange, RDS, VPN, Monitoring, ...) leite ich die Verbindungen am Router auf den WAP-Cluster weiter. Dieser analysiert die SNI und redirected im Hintergrund auf die internen Server.

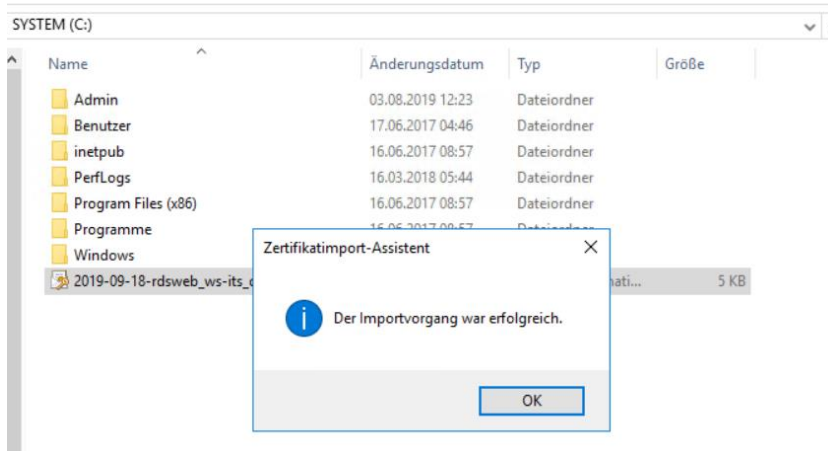
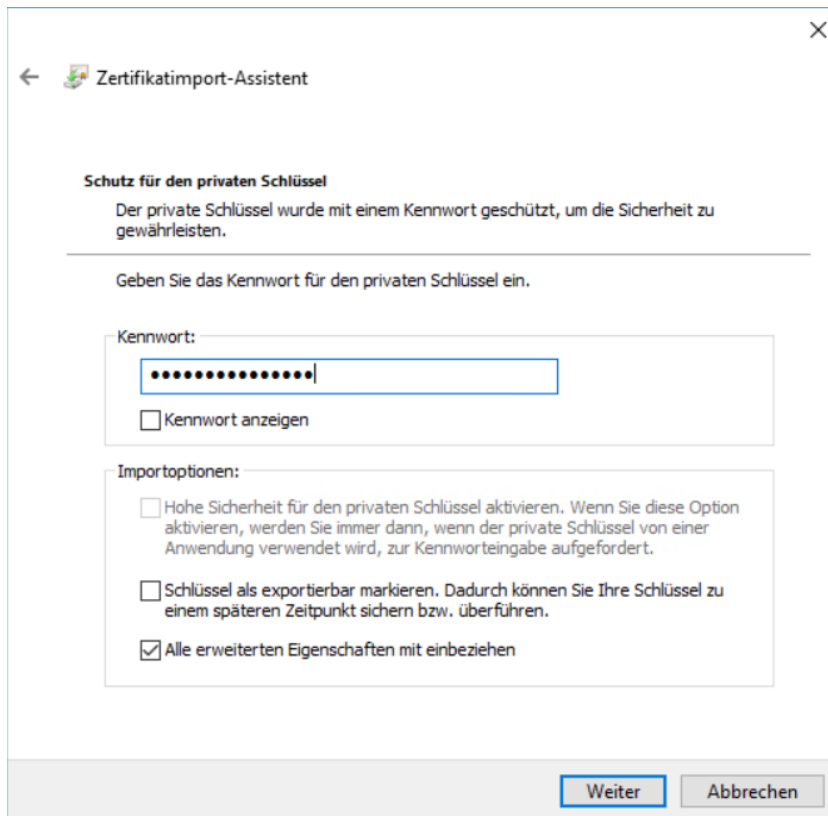
Es ist immer noch zu kompliziert? Stimmt. Hier kann Visio helfen. Zur Erläuterung:

- mein WS-Gate1 ist der Internet-Router. Dieser hat eine externe, feste IPv4 und eine interne IPv4 in meine externe DMZ
- WS-PFS1 ist meine Firewall. Diese verbindet die externe DMZ mit dem Servernetzwerk. Auf der PFSense läuft ein HA-Proxy. Dieser bekommt den externen Traffic vom Internet für HTTPS weitergeleitet. Dieser Reverse-Proxy leitet die Verbindungen an beide WAP-Server (WS-RA1 und WS-RA2) weiter.
- Die WAP-Systeme analysieren nun den SNI der Verbindungsabfrage (das ist der Servername in der URL) und leiten die Verbindung an das passende Zielsystem weiter.

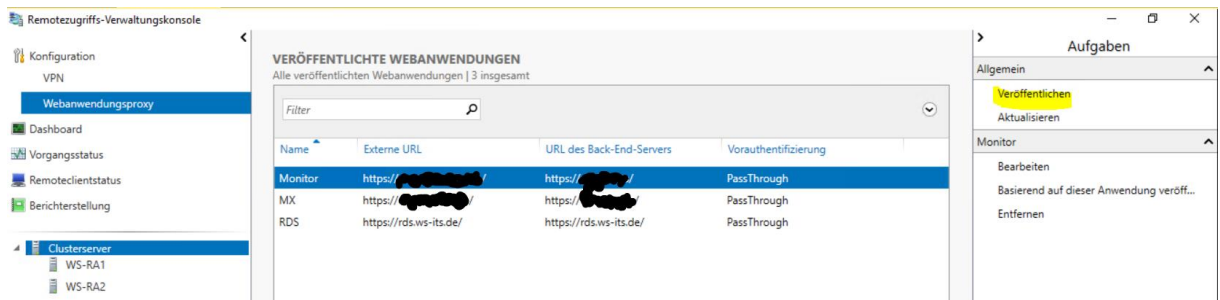


Der Web Application Proxy ist der Endpunkt für die Client-Kommunikation von extern. Daher benötigt er das gleiche Zertifikat wie der interne Service. Ich installiere also auf beiden WAP-Servern das öffentliche Zertifikat für rdsweb.ws-its.de:





Nun kann die neue Anwendung veröffentlicht werden:



Assistent zum Veröffentlichen neuer Anwendungen

MIT AD FS VERBUNDEN
adfs.ws.its

Vorauthentifizierung

Willkommen

Vorauthentifizierung

Veröffentlichungseinstellu...

Bestätigung

Ergebnisse

Geben Sie die Vorauthentifizierungsmethode an:

Active Directory-Verbinddienste (Active Directory Federation Services, AD FS)

Alle nicht authentifizierten Clientanforderungen werden an den Verbundserver umgeleitet. Nach der erfolgreichen Authentifizierung durch AD FS werden Clientanforderungen an den Back-End-Server weitergeleitet. Zudem können Back-End-Servern, die für die Verwendung der integrierten Windows-Authentifizierung konfiguriert wurden, vom Webanwendungsproxy Anmeldeinformationen bereitgestellt werden.

PassThrough

Der Webanwendungsproxy führt keine Vorauthentifizierung aus. Alle Anforderungen werden an den Back-End-Server weitergeleitet.

Assistent zum Veröffentlichen neuer Anwendungen

MIT AD FS VERBUNDEN
adfs.ws.its

Veröffentlichungseinstellungen

Willkommen

Vorauthentifizierung

Veröffentlichungseinstellu...

Bestätigung

Ergebnisse

Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an.

Name:

Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt.

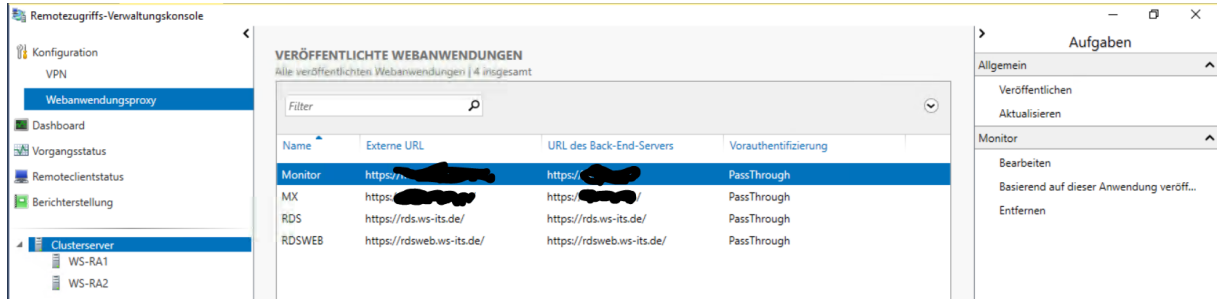
Externe URL:

Externes Zertifikat:

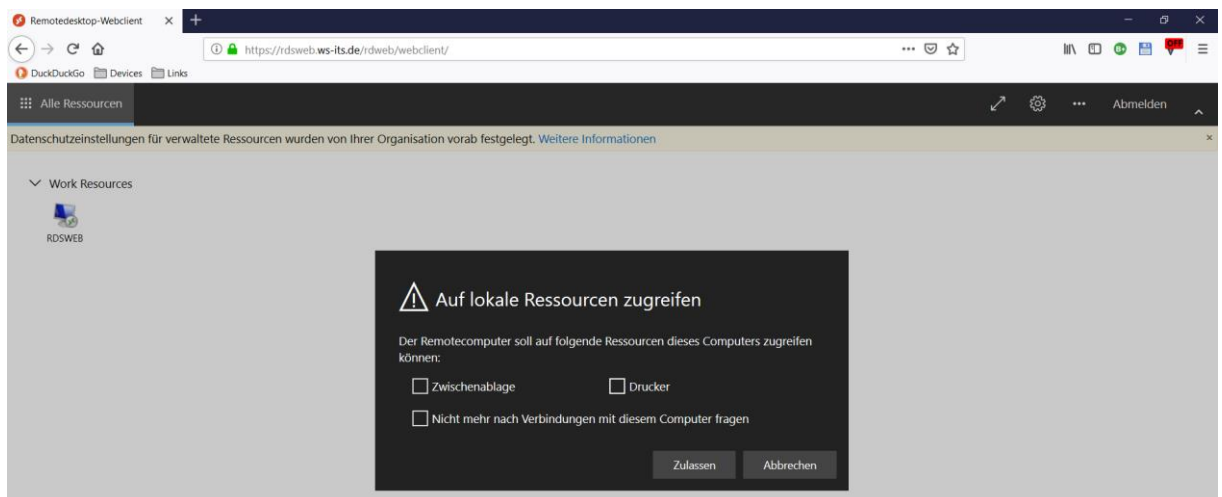
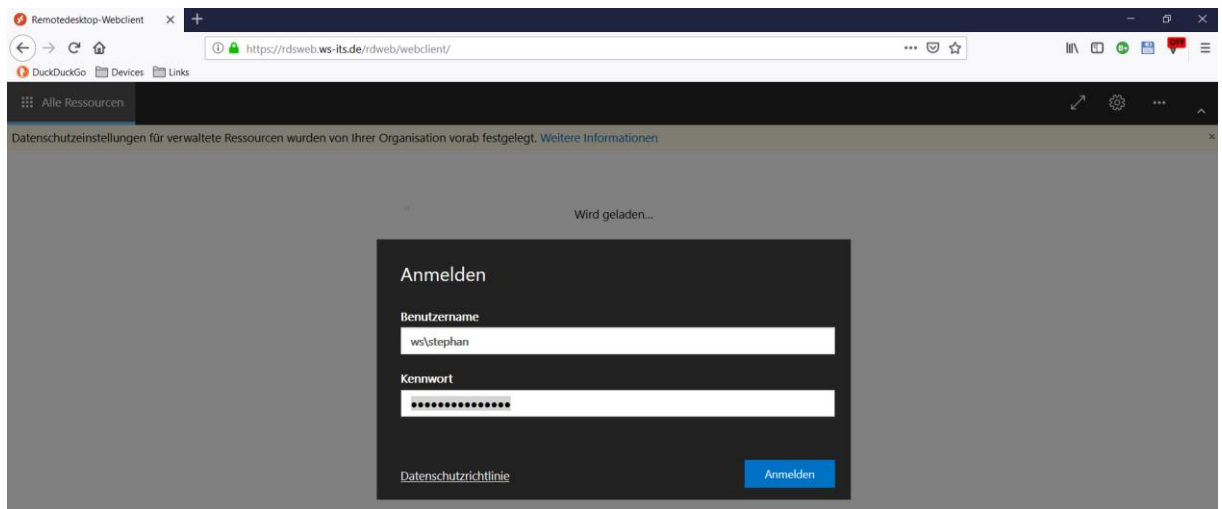
HTTP-zu-HTTPS-Umleitung aktivieren

URL des Back-End-Servers:

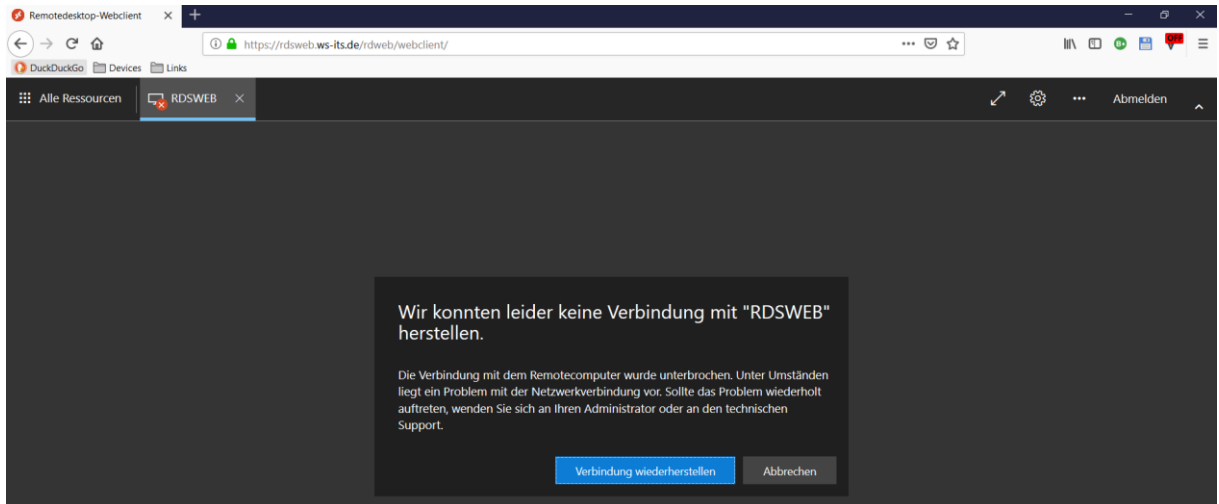
Das war einfach:



Es wird Zeit für einen Test. Dafür verbinde ich mein Notebook mit meinem Handy und rufe die RDS-Website von außen auf:



Bis hier sieht es gut aus. Doch die Verbindung wird nicht aufgebaut:



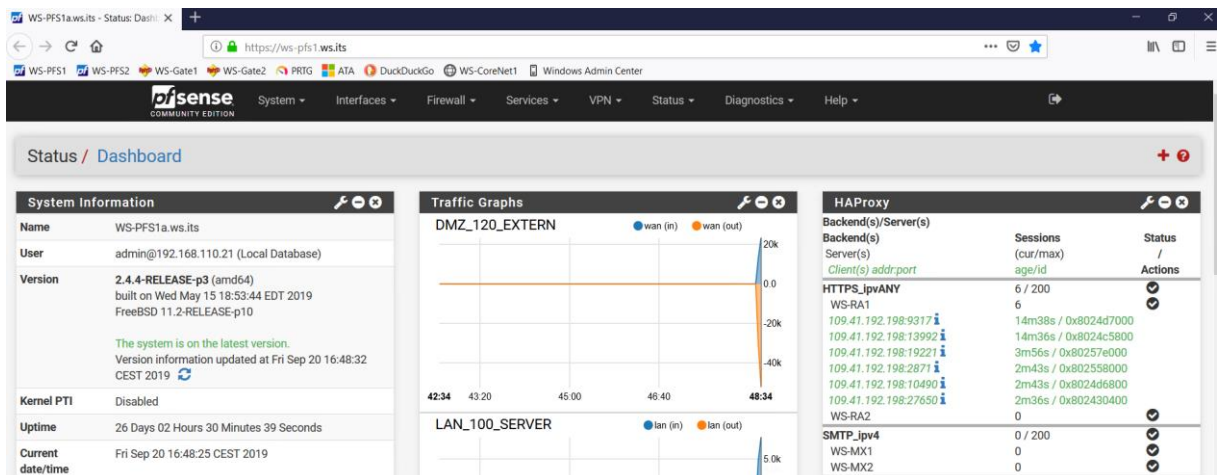
In den WAP-Servern finde ich keine Hinweise. Laut der Firewall wird der Traffic korrekt zugestellt. Das RD-Gateway mag also keine Unterbrechung des Traffics... Der Hinweis aus dem Microsoft-Artikel stimmt also.

Veröffentlichung im PfSense HA-Proxy

Die Konstruktion mit den beiden WAP-Servern hinter dem HA-Proxy ist historisch gewachsen: Zuerst stellten die WAP-Server einen NLB-Cluster mit einer einzelnen IPv4 bereit, Diese konnte ich in meinem Router als Ziel für eingehende HTTPS-Verbindungen auf Port 443 definieren. Da ein Microsoft NLB aber immer schon etwas buggy war, hatte ich dann den HAProxy eingestellt. Dieser arbeitete also als reiner LoadBalancer.

Aber mit dem HA-Proxy kann auch eine Vorfilterung und eine Steuerungslogik eingesetzt werden. Vielleicht funktioniert diese mit einem RDS-Webclient?

Aktuell schlägt externer HTTPS-Traffic auf dem HA-Proxy-Frontend auf. Dieses leitet weiter an WS-RA1 und WS-RA2 – meine beiden Backend-Systeme (WAP):



Zuerst benötige ich ein neues Backend mit der IP-Adresse meines WS-RDS1. Dieses ist mit der WebGUI recht schnell aufgebaut:

Services / HAProxy / Backend / Edit

Settings Frontend **Backend** Files Stats Stats FS Templates

Edit HAProxy Backend server pool

Name: RDSWEB

Server list

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
active	WS-RDS1	Address+Port:	192.168.100.16	443	no	no	10	

Field explanations:

Loadbalancing options (when multiple servers are defined)

Nun kann ich das Frontend editieren:

Services / HAProxy / Frontend

Settings **Frontend** Backend Files Stats Stats FS Templates

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	HTTPS-Proxy		172.19.120.120:443	ssl/https	HTTPS (default)	
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	SMTP-Proxy		172.19.120.120:25	tcp	SMTP (default)	

Add Delete Save

Hier muss eine ACL angelegt werden. Mit dieser wird ein Filter auf den SNI definiert und eine Aktion, wenn die Bedingung des Filters erfüllt ist:

Services / HAProxy / Frontend / Edit

Settings Frontend **Backend** Files Stats Stats FS Templates

Edit HAProxy Frontend

Name: HTTPS-Proxy

Description:

Status: Active

Shared Frontend This can be used to host a second or more website on the same IP:Port combination. Use this setting to configure multiple backends/accesslists for a single frontend. All settings of which only 1 can exist will be hidden. The frontend settings will be merged into 1 set of frontend configuration.

External address Define what ip:port combinations to listen on for incoming connections.

Listen address	Custom address	Port	SSL Offloading	Advanced	Action
<input type="checkbox"/>	Use custom address: <input type="text" value="172.19.120.120"/>	<input type="text" value="443"/>	<input type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
 If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define **Virtual IP** addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (.). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Name	Expression	CS	Not	Value	Actions
<input type="checkbox"/> <input type="button" value="Anchor"/> RDSWEB	Server Name Indication TLS extension matches: <input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="rdswb.ws-its.de"/>	<input type="button" value="Trash"/> <input type="button" value="Copy"/>

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld will not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched
 Example:

Name	Expression	CS	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

acl's with the same name will be 'combined' using OR criteria.
 For more information about ACL's please see [HAProxy Documentation](#) Section 7 - Using ACL's

NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Action	Parameters	Condition acl names	Actions
<input type="checkbox"/> <input type="button" value="Anchor"/> Use Backend	See below	<input type="text" value="RDSWEB"/>	<input type="button" value="Trash"/> <input type="button" value="Copy"/>

backend:

Example:

Action	SMTP	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend

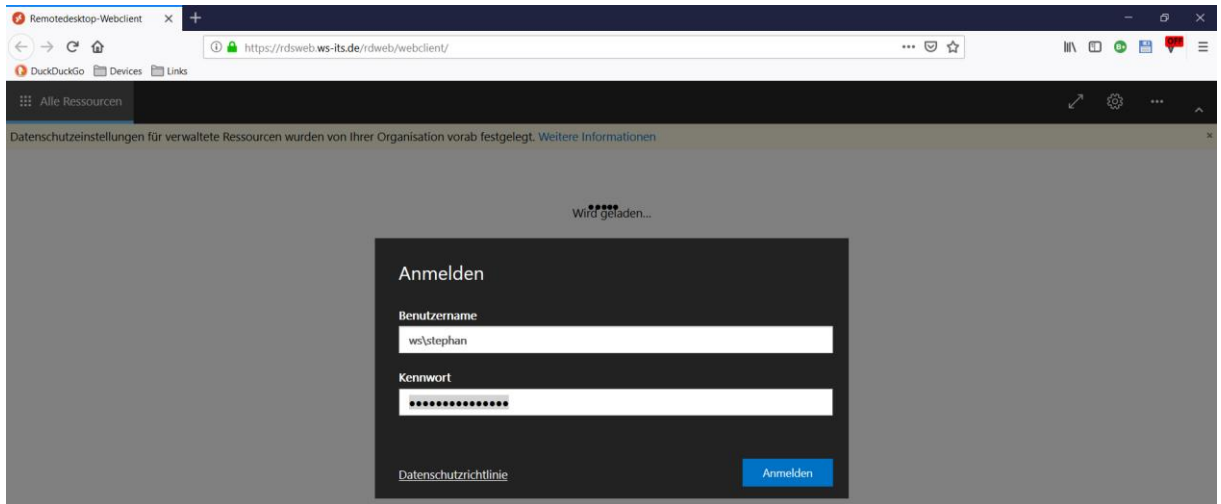
If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

Stats options

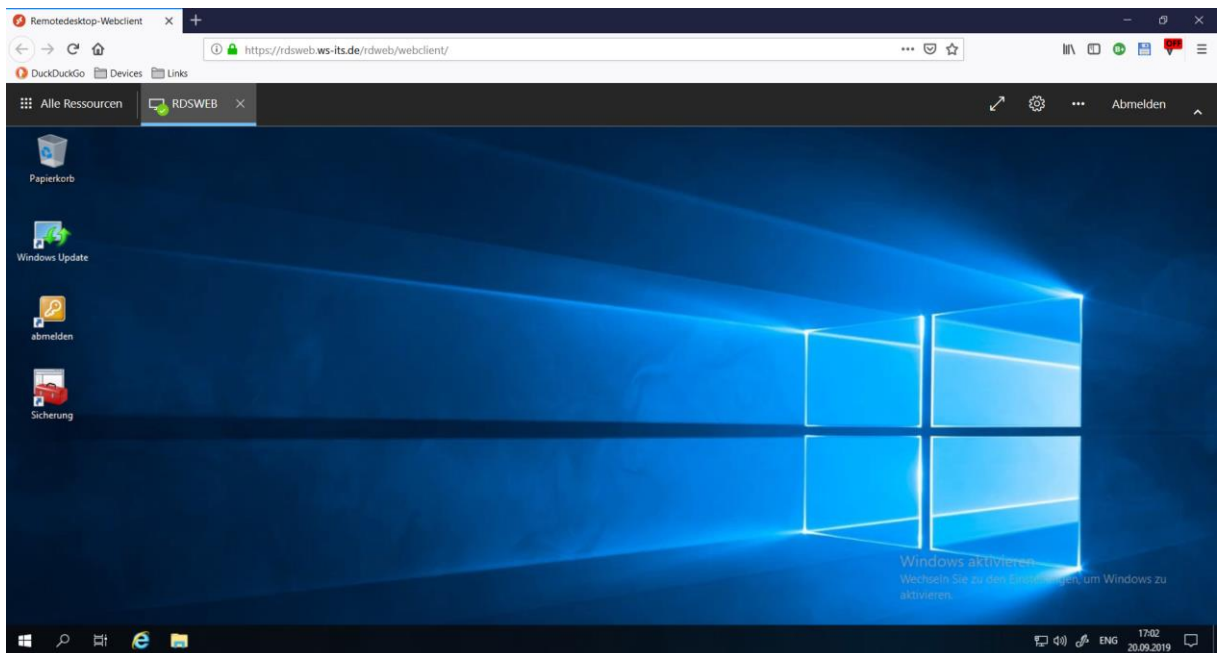
Im Detail arbeitet der HA-Proxy also nach diesem Muster:

- Eingehender Traffic wird nach dem SNI (Server Name Indication) untersucht.
- Entspricht der SNI dem Muster „rdswb.ws-ist.de“, dann wird das Backend „RDSWEB“ gewählt.
- Ist der SNI anders, dann wird das Default Backend „HTTPS“ gewählt. Das ist der WAP-Cluster mit WS-RA1 und WS-RA2

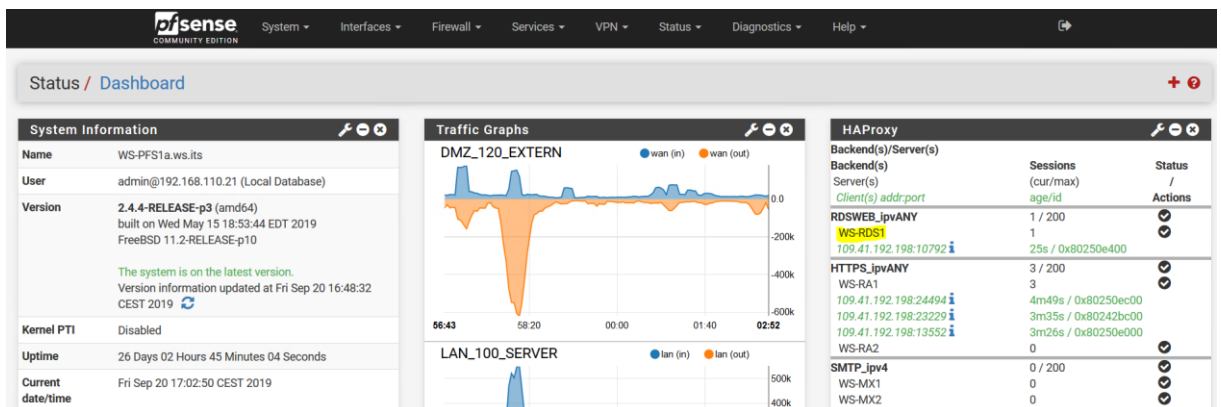
Soweit sollte nun alles passen. Es wird Zeit für einen weiteren Test von extern. Also verbinde ich mein Notebook wieder mit meinem Handy und wähle mich von außen auf das Portal des RDS-Webclients:



Es funktioniert jetzt auch von extern! Der Traffic wird ja vom HA-Proxy nicht geöffnet bzw. terminiert. Das RD-Gateway ist direkt erreichbar:



Im Dashboard von der PfSense ist der Datenstrom gut sichtbar:

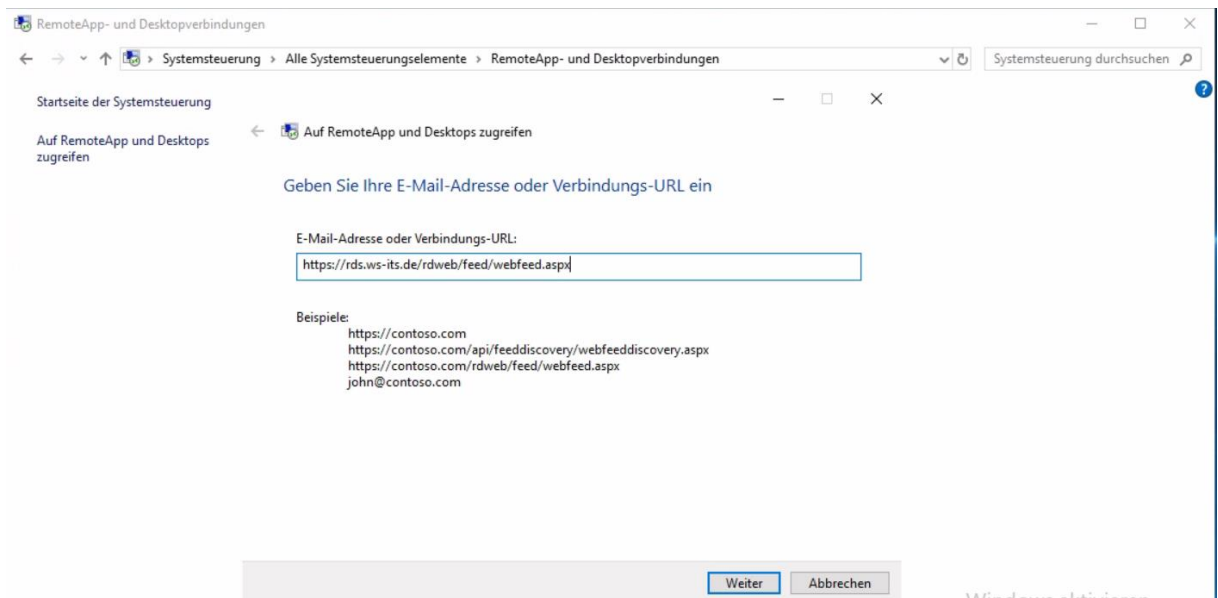


Finetuning und Absicherung

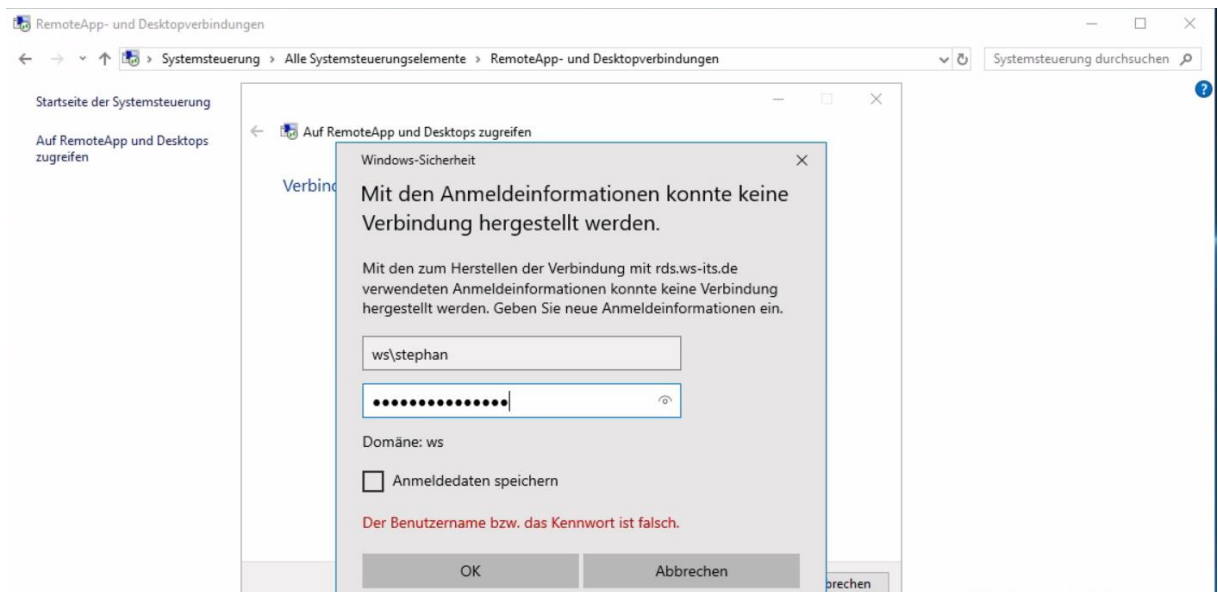
Integration der RemoteApps

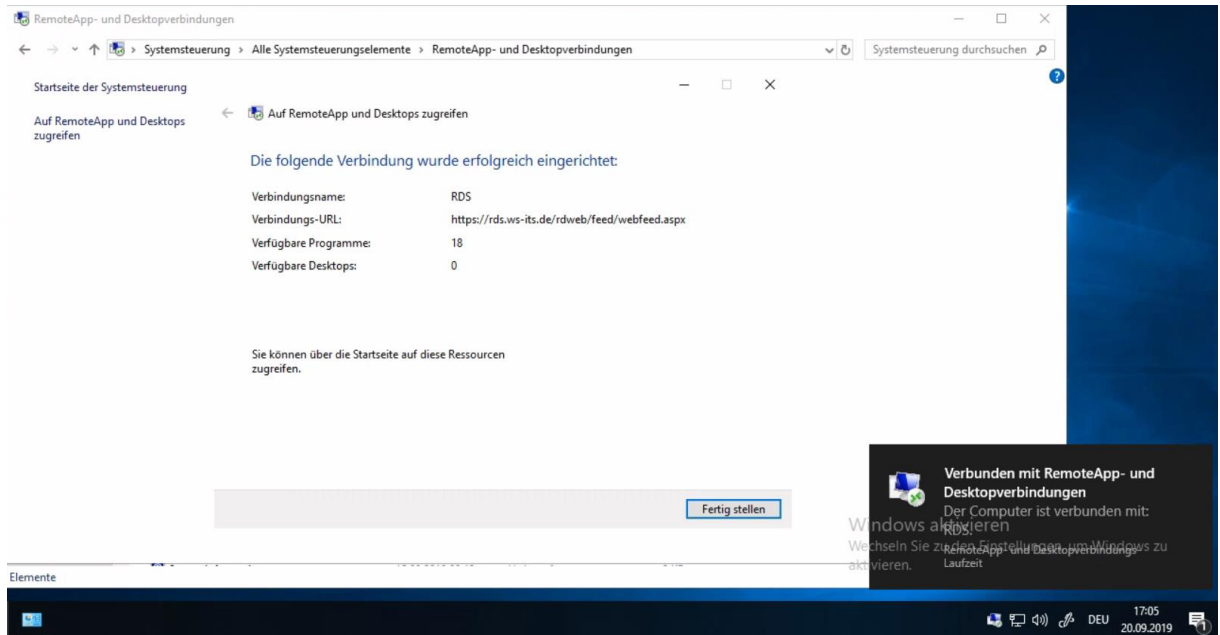
Ich kann mich über das Webportal auf meine Infrastruktur aufschalten. Schön wären jetzt noch einige Anwendungen auf dem RDS-Server. Eigentlich hatte ich hierfür meine erste RDS-Farm mit einer RemoteApp-Sammlung vorgesehen. Auf dem neuen Server könnte ich die gleichen Anwendungen installieren.

Aber warum eigentlich? Ich könnte diese RemoteApps auch in die WebSession integrieren. Dafür muss ich nur den RD-Webfeed eintragen. Dieser versteckt sich immer noch in der alten Systemsteuerung. Alternativ kann auch die GPO verwendet werden:

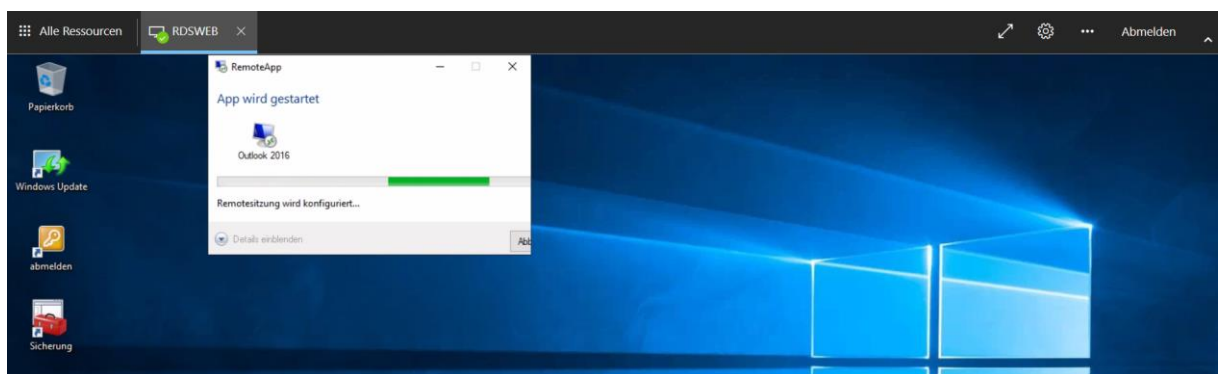


Eine Anmeldung später werden die RemoteApps integriert:

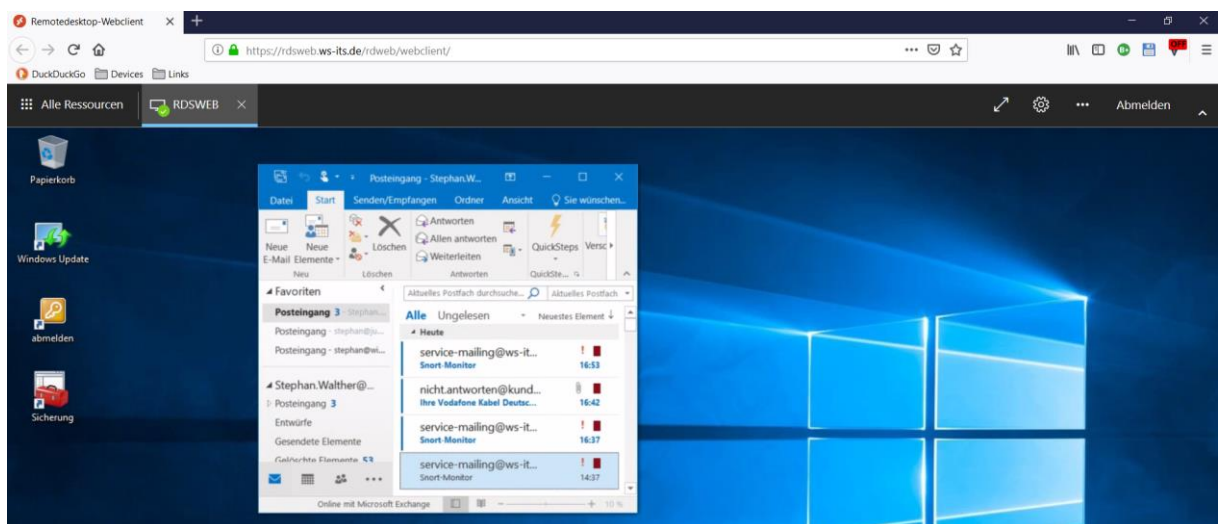




Ich starte testweise meine Outlook-RemoteApp:



Das sieht gut aus:



Absicherung durch MFA

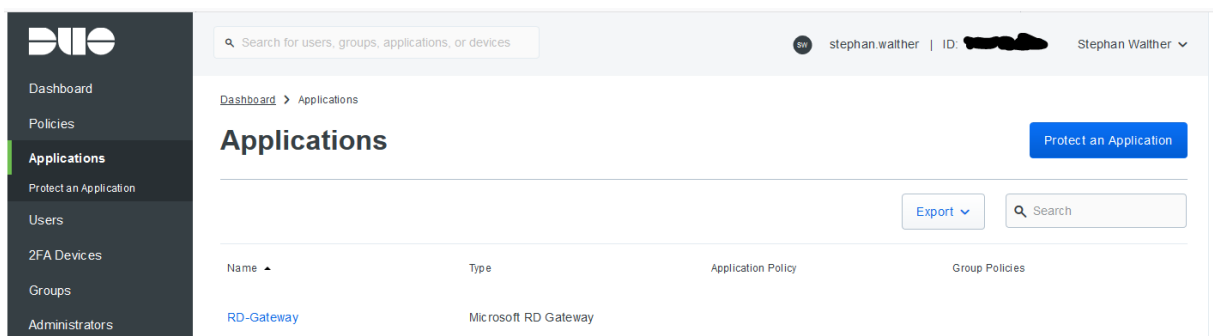
Vielleicht habt ihr euch schon gefragt, warum ich hier so offen mit meinen Konfigurationen umgehe? Ein Angreifer könnte darin eine Schwachstelle erkennen und durch z.B. diesen neuen HTML5-Webclient in meine Infrastruktur eindringen.

Da möchte ich 2 Punkte dagegenhalten: Zum ersten ist Security by Obscurity nicht wirklich sinnvoll. Ein Angreifer kann öffentlich erreichbare Endpunkte analysieren und die gleichen Erkenntnisse gewinnen. Und zum zweiten belasse ich die Absicherung nicht bei einem Kennwort. Den Zugriff von extern gewähre ich nur nach erfolgreicher Zweifaktor-Authentifizierung!

Als Anbieter verwende ich DUO, das mittlerweile von Cisco übernommen wurde. DUO bietet eine freie Lizenz für bis zu 10 Accounts an. Ideal für mich, wenn ich benötige natürlich weniger.

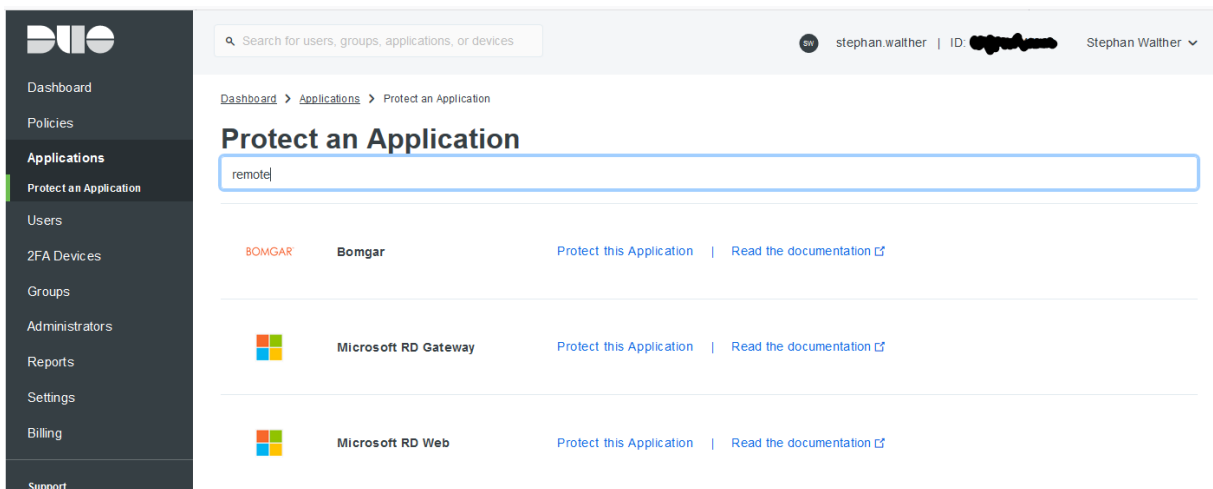
Die Authentifizierung wird nach der Anmeldung am Zielsystem durch eine Erweiterung an den DUO-Server gesendet. Mein Smartphone hält mit der App permanent die Verbindung mit diesem Server und wird via Push-Notification zur Bestätigung aufgefordert. Eine feine Sache!

Für die Integration muss ich bei DUO eine Application erstellen:



The screenshot shows the DUO web interface. On the left is a dark sidebar with navigation options: Dashboard, Policies, Applications (highlighted), Protect an Application, Users, 2FA Devices, Groups, and Administrators. The main content area is titled 'Applications' and includes a search bar, an 'Export' button, and a search input. A table lists applications with columns for Name, Type, Application Policy, and Group Policies. One application is visible: 'RD-Gateway' with Type 'Microsoft RD Gateway'.

Der Katalog bietet reichlich Auswahl:



The screenshot shows the 'Protect an Application' page in the DUO interface. The sidebar is similar to the previous screenshot but includes 'Reports', 'Settings', 'Billing', and 'Support'. The main content area has a search bar containing 'remote'. Below the search bar, there is a list of application templates with icons and links to 'Protect this Application' and 'Read the documentation'. The visible templates are: 'BOMGAR Bomgar', 'Microsoft RD Gateway', and 'Microsoft RD Web'.

Ich entscheide mich für das „Microsoft RD Web“-Template. Dazu gibt es auf der Seite einige Hinweise für die Bereitstellung:

- Dashboard
- Policies
- Applications
- Protect an Application
- Users
- 2FA Devices
- Groups
- Administrators
- Reports
- Settings
- Billing
- Support
- Upgrade your plan for support.
- Account ID
- Deployment ID

stephan.walther | ID: [REDACTED]
Stephan Walther ▾

Successfully added Microsoft RD Web to protected applications. [Add another.](#)

Dashboard > Applications > Microsoft RD Web
Authentication Log | Remove Application

Microsoft RD Web

See the [Microsoft RD Web documentation](#) to integrate Duo into your RD Web App logins.

Reset Secret Key

Details

Integration key	[REDACTED]	select
Secret key	Click to view	select
Don't write down your secret key or share it with anyone.		
API hostname	[REDACTED]	select

- Product
- Use Cases
- Pricing
- About
- Partners
- Resources
- Docs
- Support

Contact Sales
Free Trial

Contents

- Overview
- Deployment Tip
- Prerequisites
- First Steps
- Test Your Setup
- Updating Duo for RD Web
- Troubleshooting

Related

- [Duo Authentication for RDS Overview](#)
- [Duo Authentication for RD Web and RD Gateway 2012+](#)
- [Duo Authentication for RD Web and RD Gateway 2008 R2](#)
- [Duo Authentication for RD Web 2012+ Only](#)
- [Duo Authentication for RD Web 2008 R2 Only](#)
- [Duo Authentication for RD Gateway 2012+ Only](#)
- [Duo Authentication for RD Gateway 2008 R2 Only](#)
- [RDS FAQ](#)
- [Release Notes](#)

Prerequisites

Make sure to complete these requirements before installing Duo Authentication for RD Web.

- 1 Check your server version. These instructions are for installing Duo Authentication for RD Web on Windows Server 2012, 2012 R2, 2016, and 2019. If you are running Windows 2008 R2, see the [RD Web 2008 R2 instructions](#).
- 2 Make sure you have installed .NET Framework 4.5. You can do this, for example, by running the following PowerShell commands:


```
Import-Module ServerManager
Add-WindowsFeature NET-Framework-Core
```
- 3 Also make sure you have installed ASP.NET 4.5 support for IIS. The PowerShell commands for this are:


```
Import-Module ServerManager
Add-WindowsFeature NET-Framework-45-ASPNET
```
- 4 Ensure that the IIS Management Scripts and Tools feature is turned on as well. PowerShell example:


```
Import-Module ServerManager
Add-WindowsFeature Web-Scripting-Tools
```

Connectivity Requirements

This application communicates with Duo's service on TCP port 443. Firewall configurations that restrict outbound access to Duo's service with rules using destination IP addresses or IP address ranges aren't recommended, since these may change over time to maintain our service's high availability. If your organization requires IP-based rules, please review [this Duo KB article](#).

OK, ich prüfe die Voraussetzungen:

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

PS C:\Windows\system32> Add-WindowsFeature NET-Framework-Core
Add-WindowsFeature : Fehler bei der Anforderung zum Hinzufügen oder Entfernen von Features auf dem angegebenen Server.
Fehler beim Installieren mindestens einer Rolle, eines Rollendiensts oder eines Features. Fehler: 0x800f0954
In Zeile:1 Zeichen:1
+ Add-WindowsFeature NET-Framework-Core
+ ~~~~~
+ CategoryInfo          : InvalidOperation: (@{Vhd=; Credent...Name=localhost}:PSObject) [Install-WindowsFeature],
  Exception
+ FullyQualifiedErrorId : DISMAPI_Error__Failed_To_Enable_Updates,Microsoft.Windows.ServerManager.Commands.AddWind
  owsFeatureCommand

Success Restart Needed Exit Code      Feature Result
-----
False No                Failed          {}

PS C:\Windows\system32> Get-WindowsFeature net*core

Display Name                                     Name                               Install State
-----
[ ] .NET Framework 3.5 (enthält .NET 2.0 und 3.0) NET-Framework-Core                 Removed
[X] .NET Framework 4.7                           NET-Framework-45-Core              Installed

PS C:\Windows\system32>
  
```

```

Administrator: Windows PowerShell
PS C:\Windows\system32> Add-WindowsFeature NET-Framework-45-ASPNET

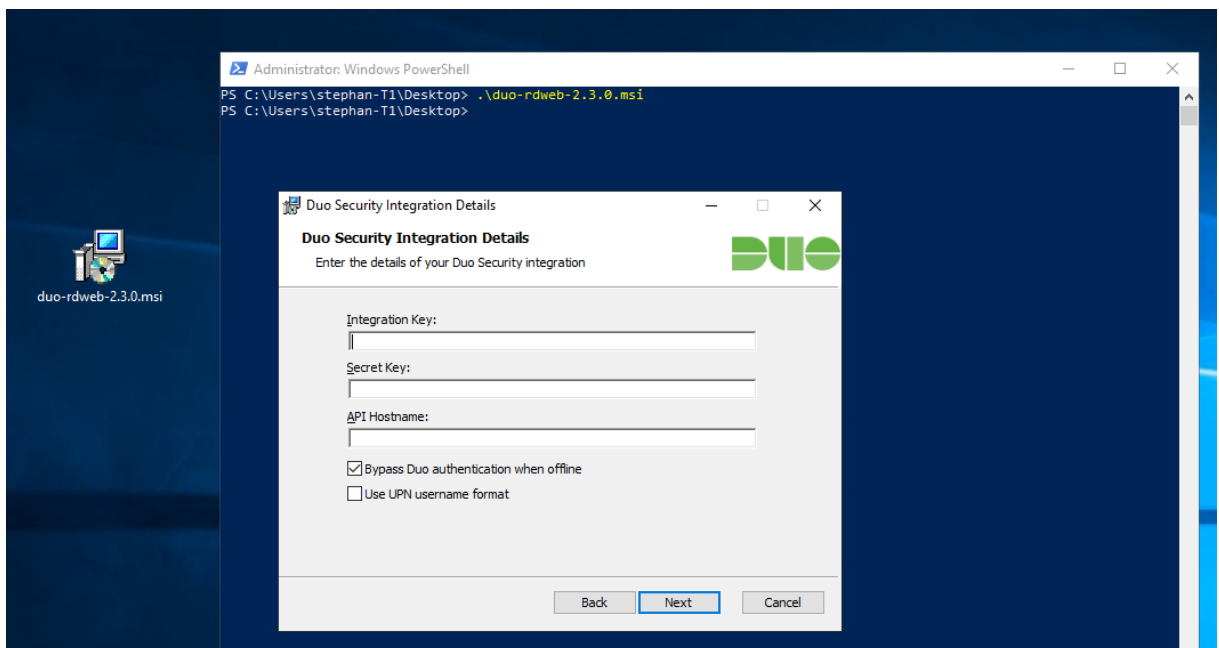
Success Restart Needed Exit Code      Feature Result
-----
True No                NoChangeNeeded {}

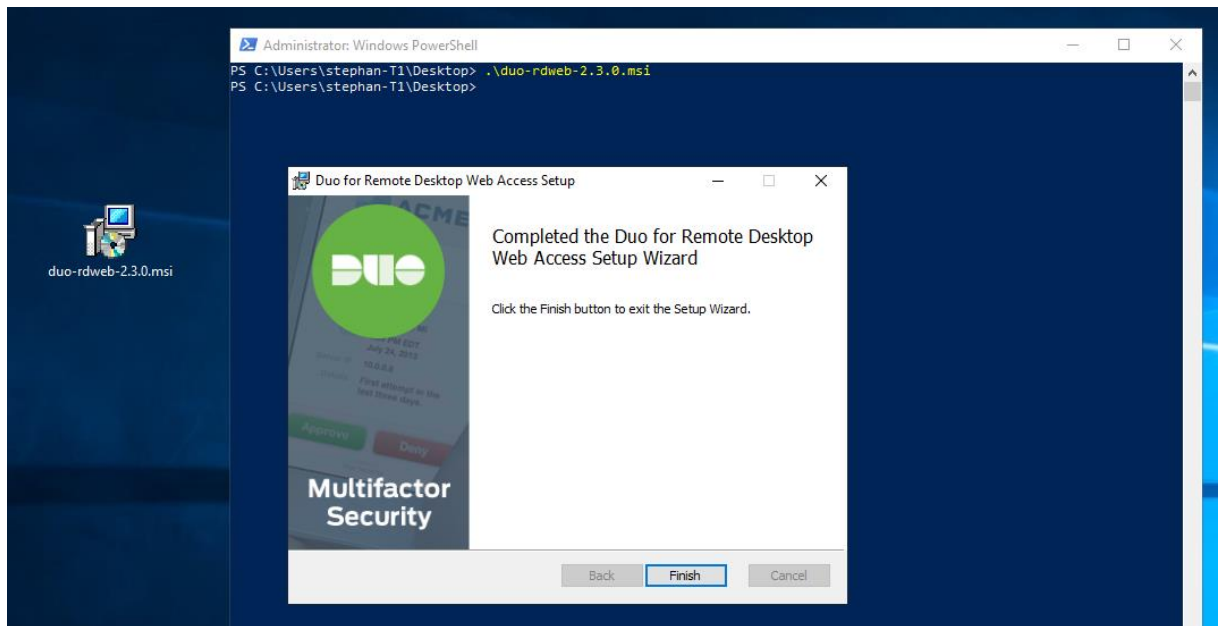
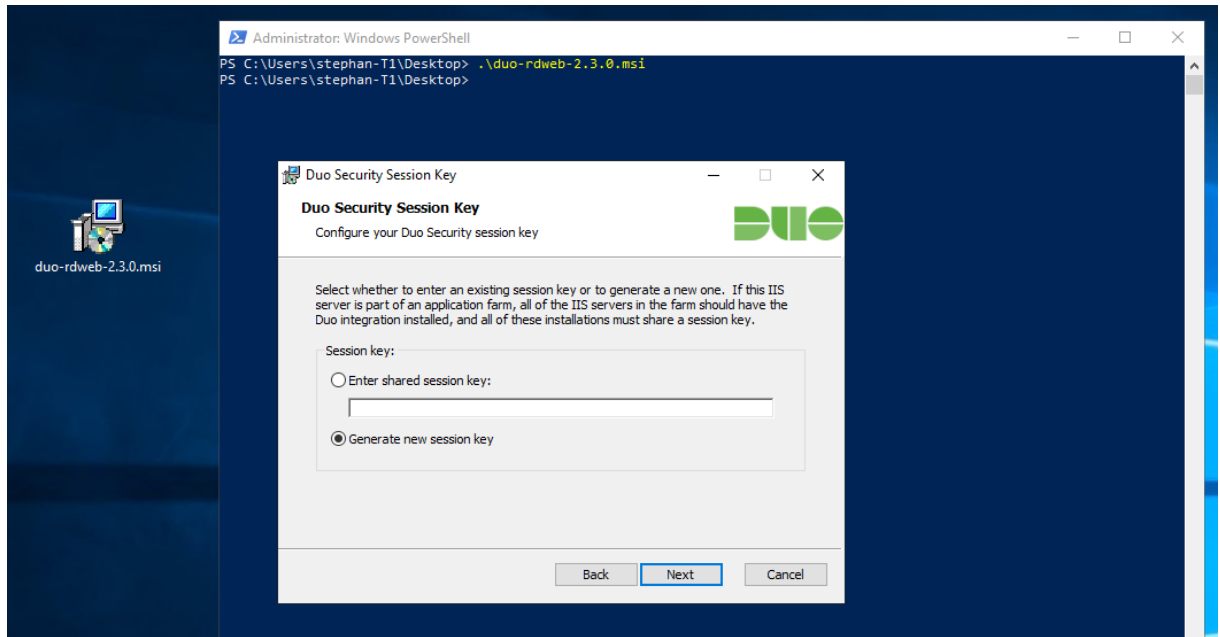
PS C:\Windows\system32> Add-WindowsFeature Web-Scripting-Tools

Success Restart Needed Exit Code      Feature Result
-----
True No                NoChangeNeeded {}

PS C:\Windows\system32>
  
```

Jetzt kann ich die MSI-Datei installieren. Die 3 Informationen liefert die Anweisung im DUO-Dashboard gleich mit:





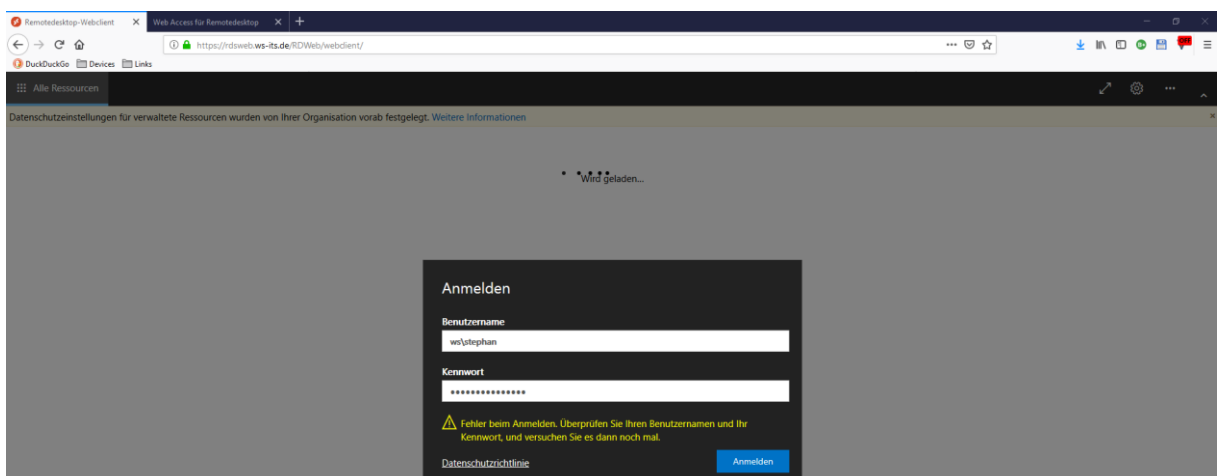
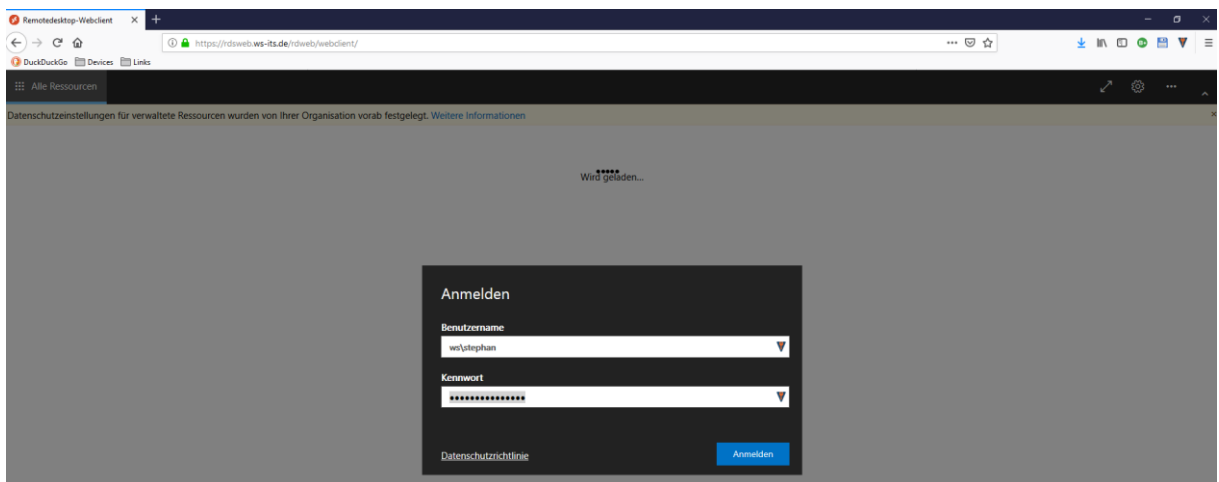
Die erforderliche Firewall-Ausnahme zum DUO-Server existiert bereits:

Ausnahmen extern										
<input type="checkbox"/>	✓	18 /288.00 MiB	IPv4 UDP	ServerOut_UDP53	*	Device_WS_Gate1	Ports_DNS	*	none	DNS-Forwarder erlaubt
<input type="checkbox"/>	✓	1 /4.84 MiB	IPv4 UDP	ServerOut_UDP53	*	Device_WS_Gate2	Ports_DNS	*	none	DNS-Forwarder erlaubt
<input type="checkbox"/>	✓	0 /336 KiB	IPv4 UDP	ServerOut_UDP123	*	*	Ports_NTP	*	none	NTP erlaubt
<input type="checkbox"/>	✓	0 /8.39 MiB	IPv4 TCP	ServerOut_TCP25	*	*	Ports_SMTP	*	none	SMTP erlaubt
<input type="checkbox"/>	✓	4 /1.51 GiB	IPv4 TCP	ServerOut_TCP443	*	*	Ports_HTTPS	*	none	HTTPS ins Internet erlaubt
<input type="checkbox"/>	✓	0 /14.54 GiB	IPv4 TCP	ServerOut_TCP80	*	*	Ports_HTTP	*	none	HTTP ins Internet erlaubt
<input type="checkbox"/>	✓	0 /0 B	IPv4 UDP	ServerIn_WDS	*	*	*	*	none	WDS Callback
<input type="checkbox"/>	✓	0 /267 KiB	IPv4 TCP	ServerOut_DuoSecurity	*	*	Ports_HTTPS	*	none	Zugriff DuoSecurity
<input type="checkbox"/>	✓	0 /2.39 MiB	IPv4 TCP	ServerOut_MXServer	*	*	Ports_HTTPS	*	none	MXUpdate HTTPS

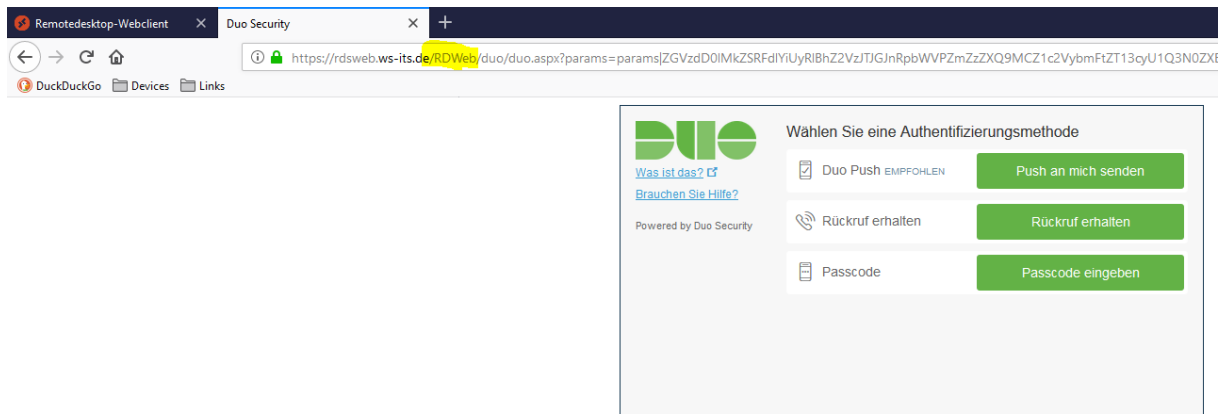
Alias details

Value	Description
192.168.100.16	WS-RDS1
192.168.100.9	WS-HV1
192.168.100.10	WS-HV2

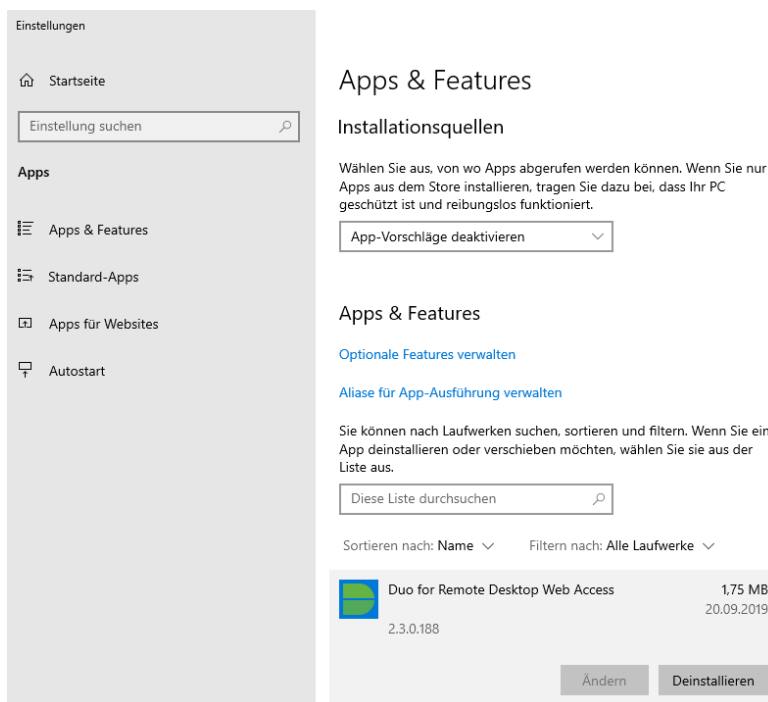
Es sollte also alles funktionieren. Oder?



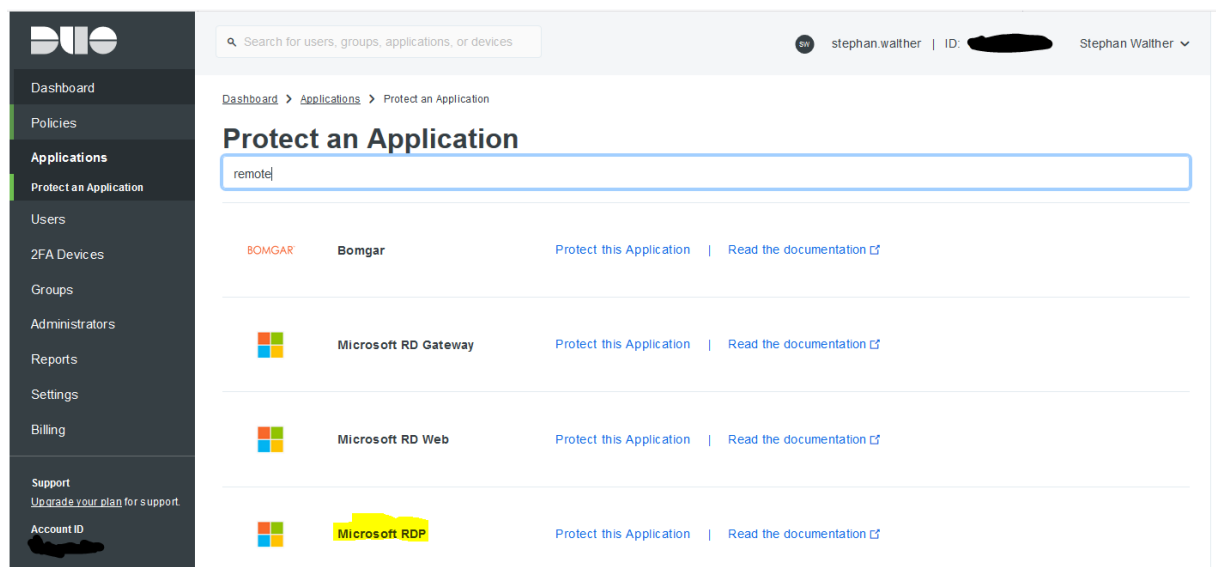
Das funktioniert so nicht! Der Name der Application klingt auch eher nach dem RDWeb-Portal. Und so ist es leider auch:



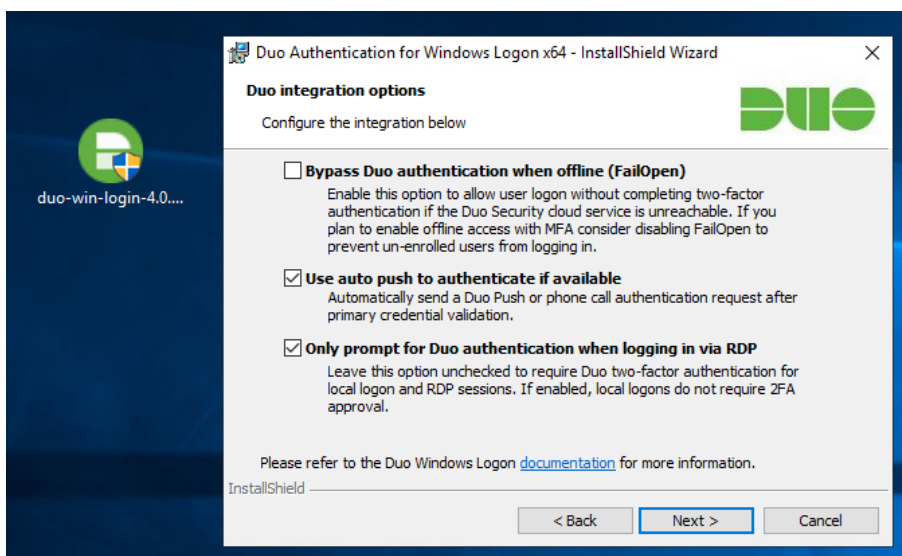
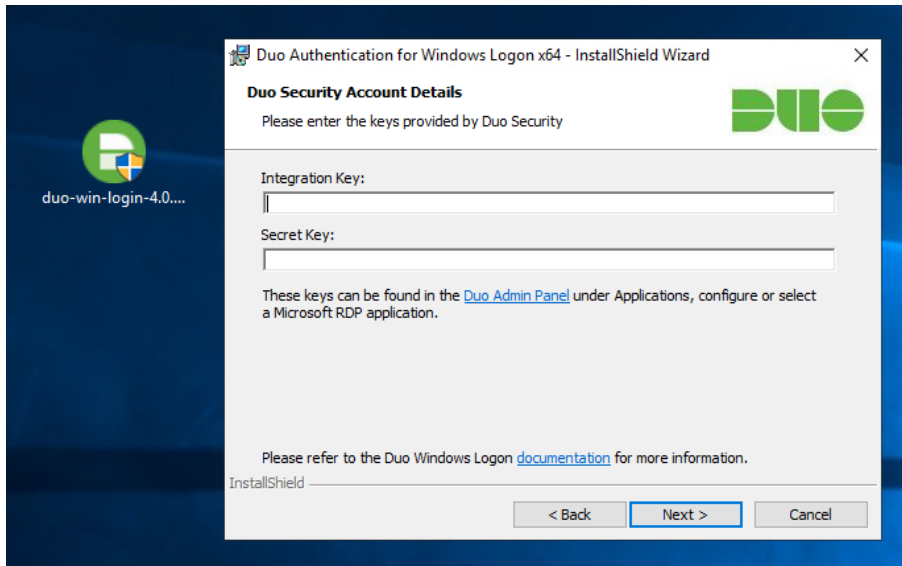
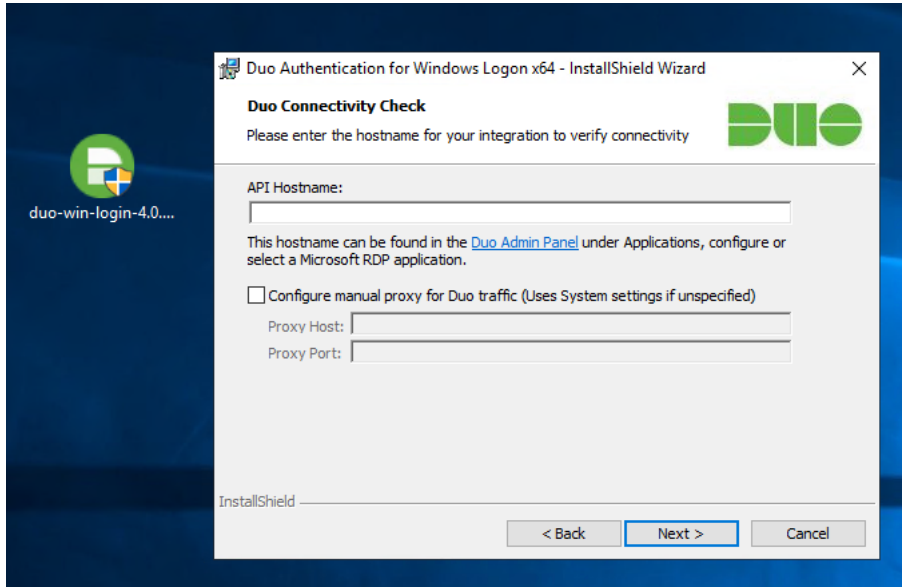
Auf der Support-Seite von DUO steht weiter unten, dass der HTML5-Client nicht unterstützt wird. War ja klar. Also entferne ich die Installation:

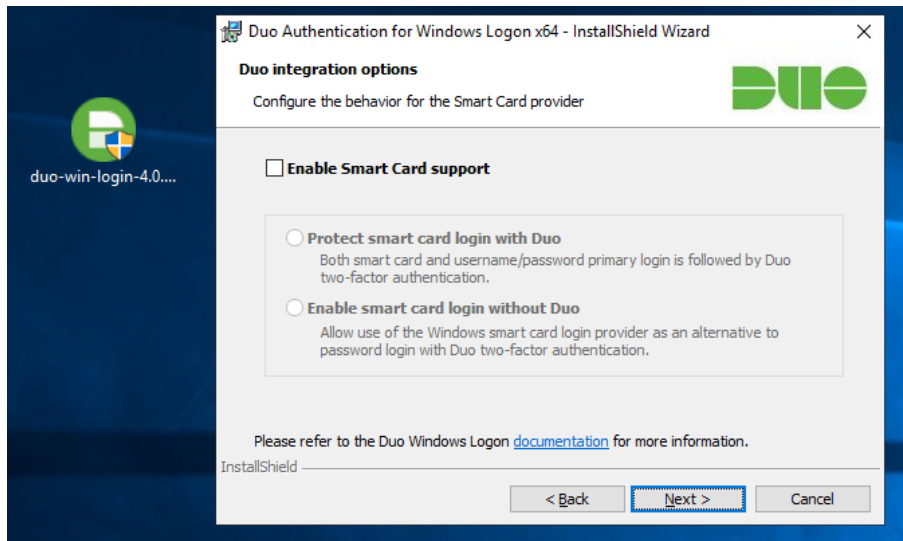


Ich versuche es mit der klassischen „Microsoft RDP“-Application:

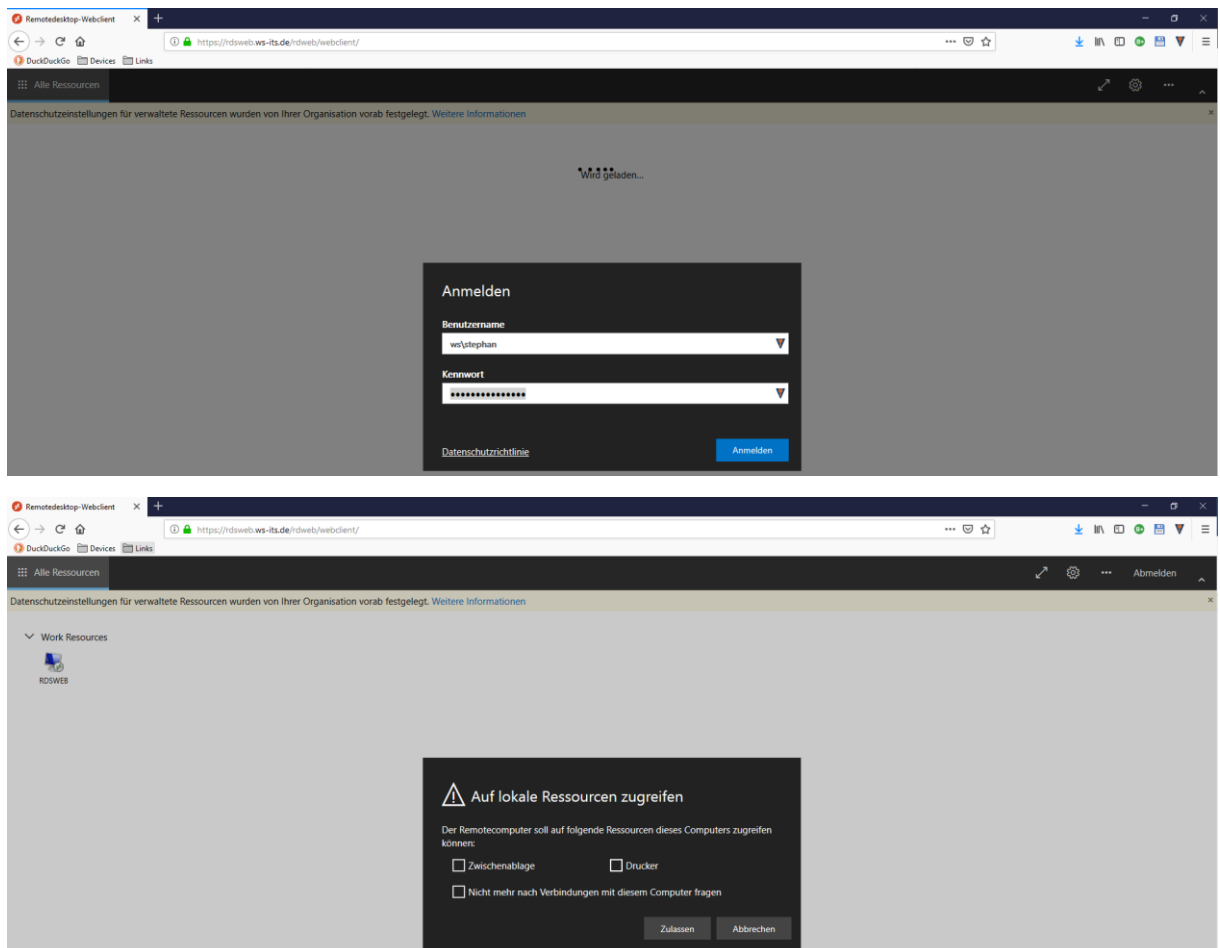


Das Setup ist fast identisch mit dem ersten:

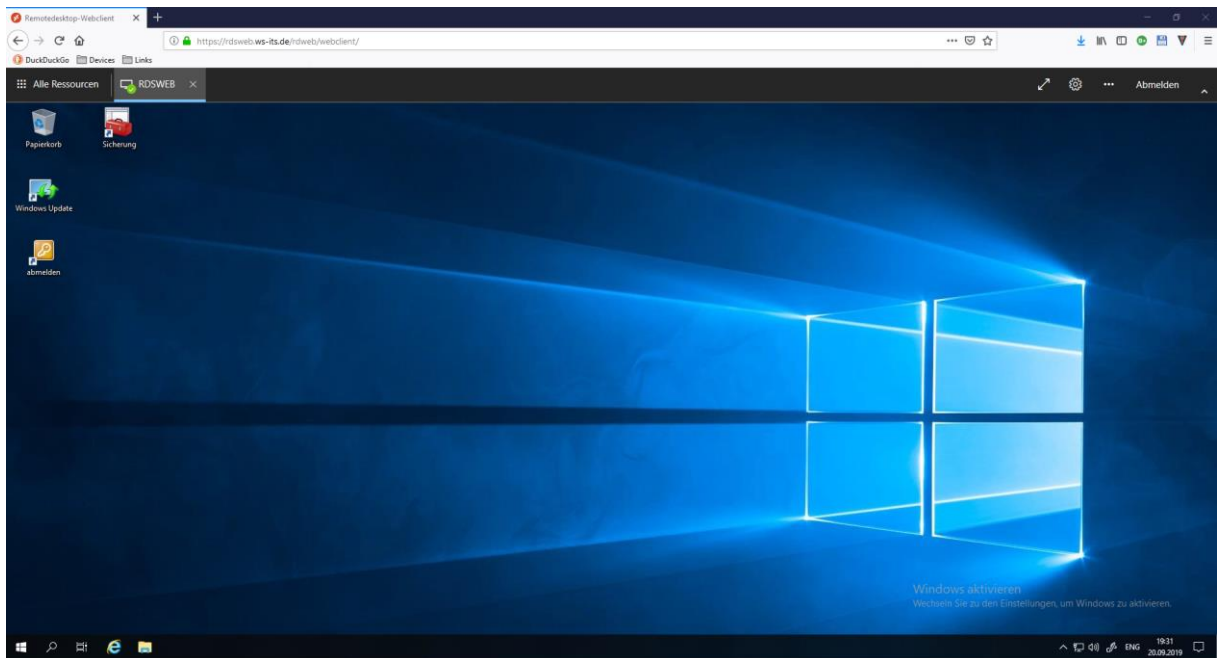
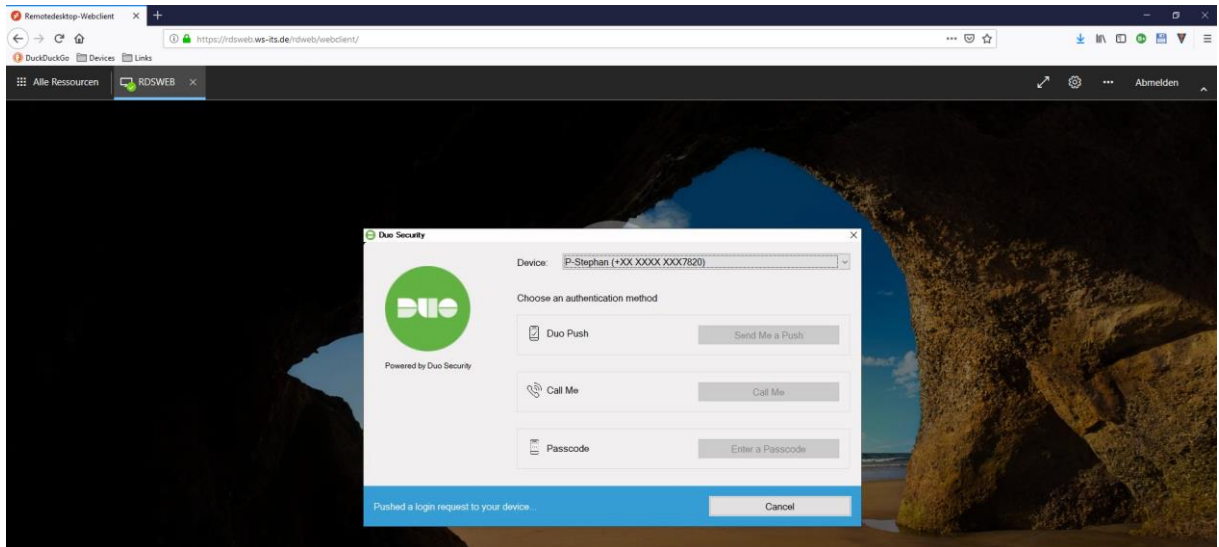




Nun muss die Anmeldung vollständig sein, damit der zweite Faktor angefordert wird. Aber es ist immer noch besser als nur ein Passwort. Und auch das muss erst einmal gefunden werden!

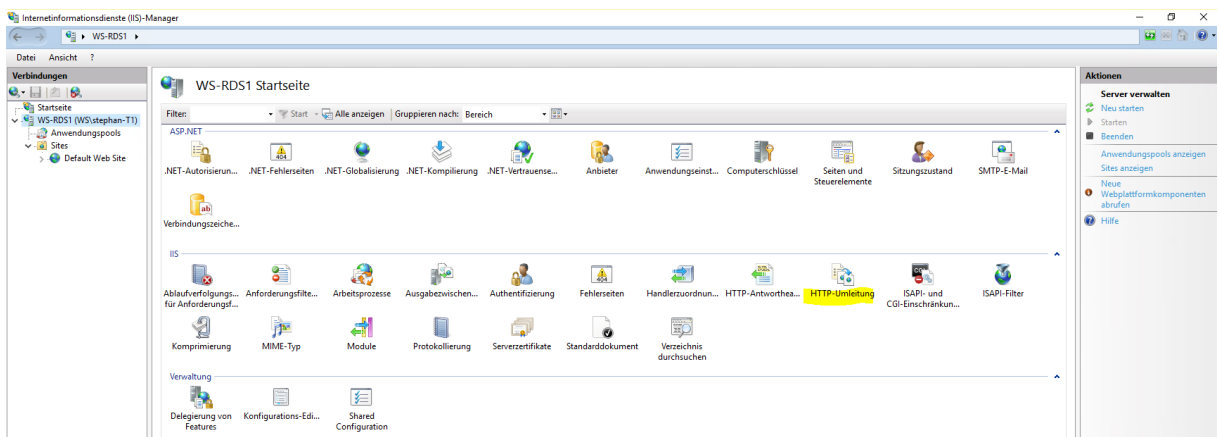


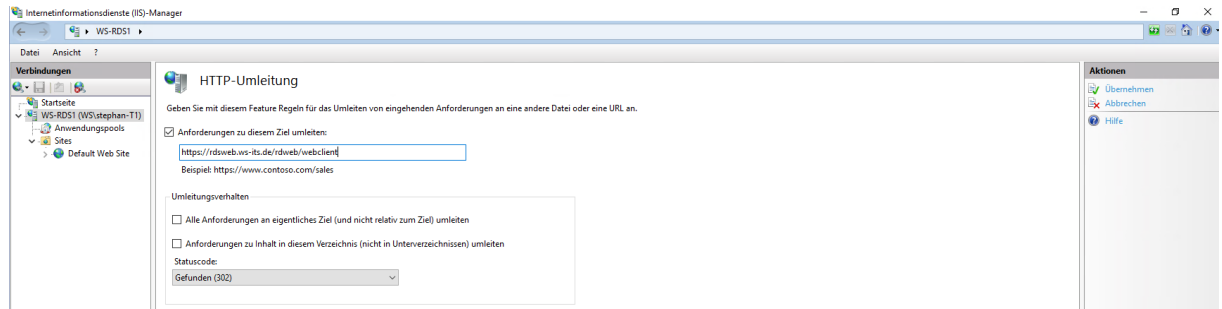
Jetzt wird das Smartphone kontaktiert.:



http-Umleitung

Der Webclient wird nur aktiv, wenn man im Browser die richtige URL einträgt. Die mag ich mir nicht merken. Ebenso mag ich sie nicht tippen. Also stelle ich im IIS auf meinem neuen WS-RDS1 die http-Umleitung ein

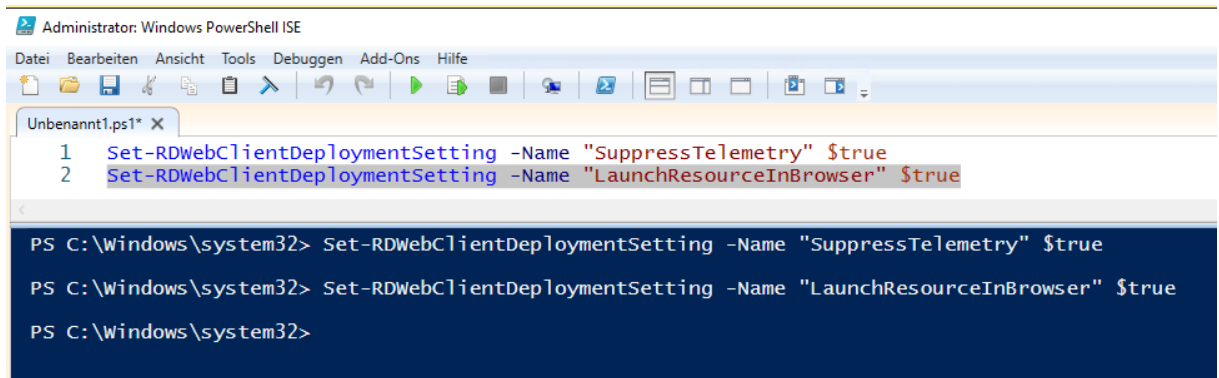




Nun genügt die URL `https://<FQDN>` für die Verbindung.

Voreinstellungen

Über die PowerShell können einige Optionen definiert werden. Die klingen ganz gut:



Integration in die Maintenance-Infrastruktur

Der Server wird in die Datensicherung integriert. Ein Testlauf erstellte eine vollständige Sicherung der VM im laufenden Betrieb.

Ebenso aktiviere ich das Monitoring des Systems in meinem PRTG.

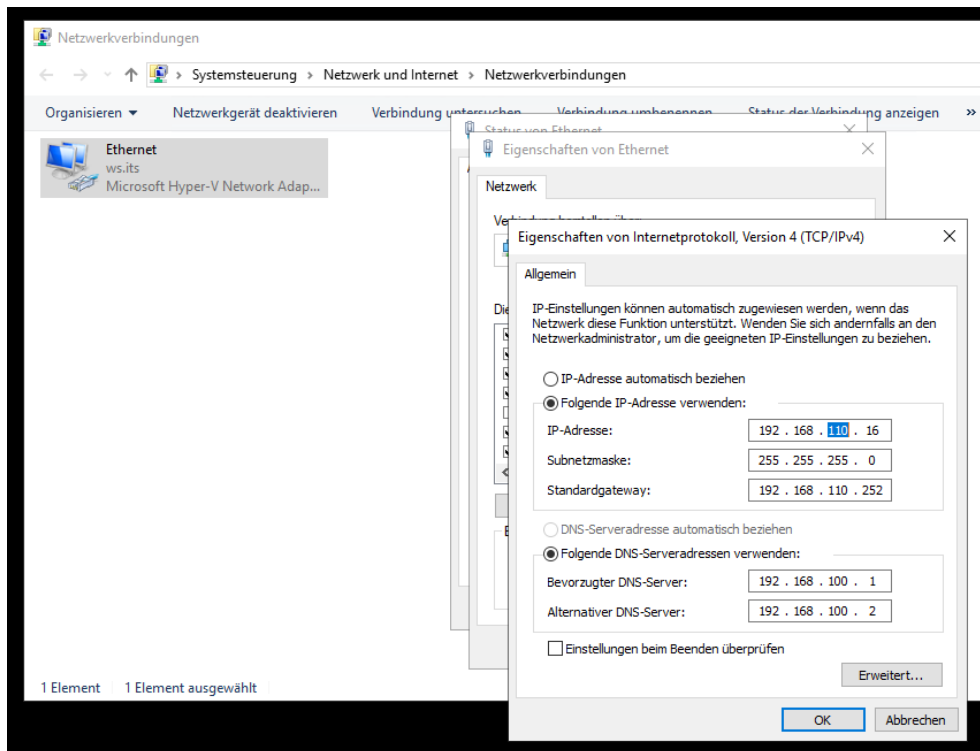
Die Windows Updates laufen dank der GPO-Konfiguration automatisch an.

Umzug in das Client-Netzwerk

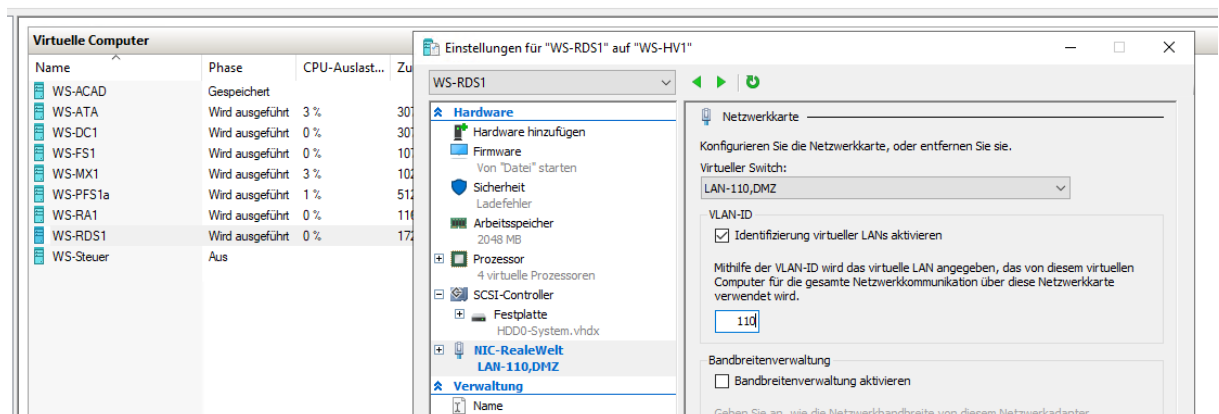
Nachdem die Lösung funktioniert möchte ich die Absicherung weiter verbessern. Aktuell würde ein Angreifer nach der erfolgreichen Anmeldung am Server direkt im Servernetzwerk 192.168.100.0/24 rauskommen. Danach nützt mir meine Firewall zwischen den Clientnetzen und dem Servernetzwerk nichts mehr.

RDS-Server werden im Gegensatz zu anderen Servern von Endanwendern verwendet. Daher gehören sie in ein eigenes Netzwerksegment oder in das Clientnetzwerk. Ich entscheide mich für mein Clientnetz 192.168.110.0/24.

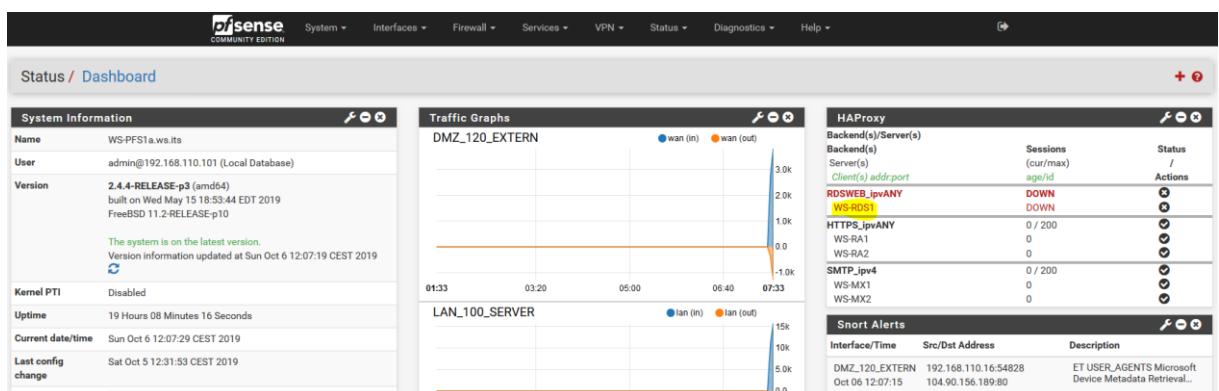
Zuerst ändere ich die IPv4-Konfiguration des Servers WS-RDS1:



Da es eine virtuelle Maschine ist, wird die Anpassung des Netzwerkadapters recht einfach ausfallen: Ich ändere den vSwitch und die VLAN-ID im Hyper-V-Manager:



Aber auch die PfSense muss über den Wechsel informiert werden. Der HA-Proxy prüft permanent die Verfügbarkeit. Er vermisst den Server bereits:



Die Anpassung nehme ich im Backend des HA-Proxy vor:

The screenshot shows the pfSense HAProxy Backend configuration page. The breadcrumb trail is Services / HAProxy / Backend. The 'Backend' tab is selected. Below the navigation tabs, there is a table of Backends:

Advanced	Name	Servers	Check	Frontend	Actions
<input type="checkbox"/>	SMTP	2	SMTP	SMTP-Proxy	
<input type="checkbox"/>	HTTPS	2	Basic	HTTPS-Proxy	
<input type="checkbox"/>	RDSWEB	1	Basic	HTTPS-Proxy	

At the bottom right, there are buttons for Add, Delete, and Save.

The screenshot shows the 'Edit HAProxy Backend server pool' page for the 'RDSWEB' backend. The 'Name' field contains 'RDSWEB'. Below, the 'Server list' table is shown:

Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Action
active	WS-RDS1	Address+Port	192.168.110.16	443	<input type="checkbox"/>	<input type="checkbox"/>	10	

Field explanations are available at the bottom.

Die Firewall besteht bei mir aus etlichen Alias-Einträgen, die in diversen Regeln angewendet werden. Diese müssen nun ebenfalls angepasst werden:

The screenshot shows the pfSense Firewall Aliases IP page. The breadcrumb trail is Firewall / Aliases / IP. The 'IP' tab is selected. Below, the 'Firewall Aliases IP' table is shown:

Device	IPs	Device	Actions
Device_WS_PFS2	192.168.101.252, 192.168.111.252, 172.19.121.252, 172.19.131.252	Gerät WS-PFS2	
Device_WS_RDS1	192.168.100.16	Server WS-RDS1	
Device_WS_RDS2	192.168.110.21	Server WS-RDS2	

Firewall / Aliases / Edit

Properties

Name Device_WS_RDS1
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description Server WS-RDS1
A description may be entered here for administrative reference (not parsed).

Type Host(s)

Host(s)

Hint Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN	Alias
192.168.110.16	WS-RDS1

Save Add Host

Weitere Aliase warten auf die Editierung:

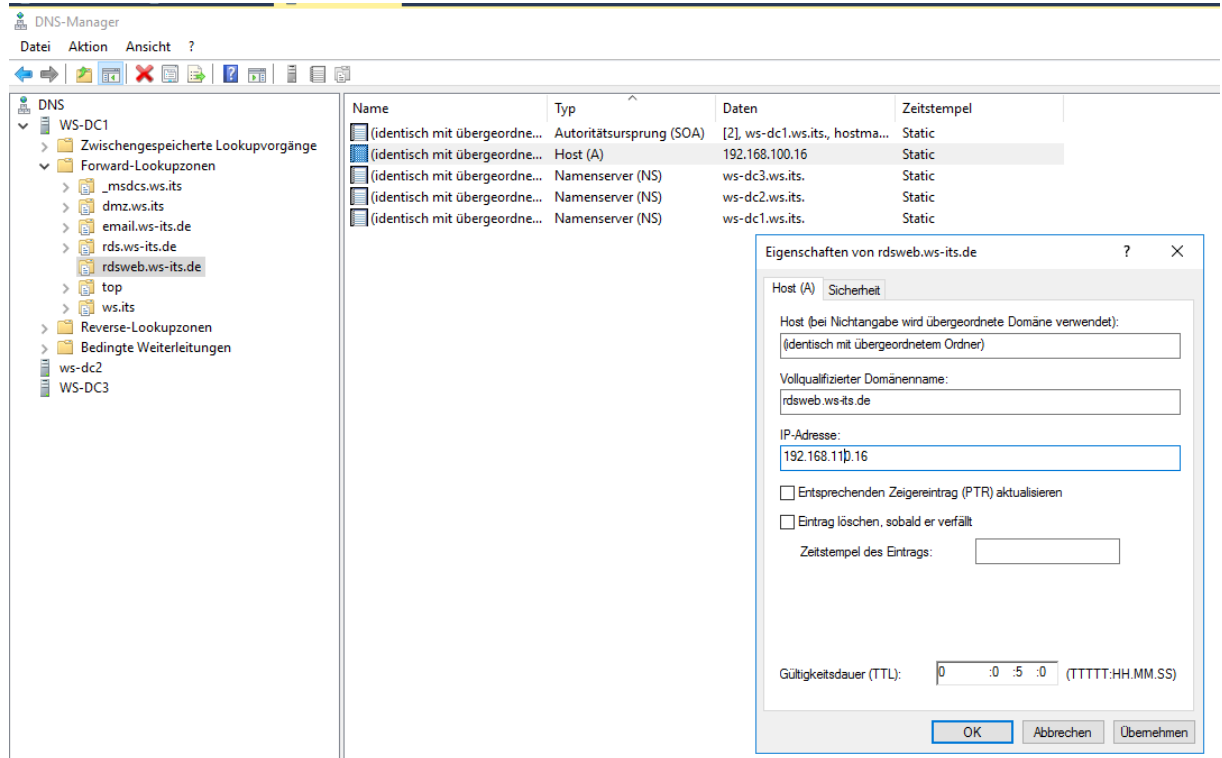
Firewall / Aliases / IP

IP Ports URLs All

Firewall Aliases IP

ServerIn_HTTPS	192.168.100.18, 192.168.100.7, 192.168.100.17, 192.168.100.6, 192.168.100.23, 192.168.100.22, 192.168.100.16	Services mit HTTPS	
ServerIn_MXRemoting	192.168.100.3, 192.168.100.13	Server mit MX	
ServerIn_Print	192.168.100.11, 192.168.100.51	Services Print	
ServerIn_RDS	192.168.110.21, 192.168.100.16	Server mit RDS	
ServerIn_SMB	192.168.100.11, 192.168.100.12, 192.168.100.10, 192.168.100.5, 192.168.101.2, 192.168.100.8, 192.168.100.41	Services SMB	
ServerIn_WDS	192.168.100.4	Services WDS	
ServerIn_WSUS	192.168.100.4	Services WSUS	
ServerOut_Anywhere	192.168.99.99, 172.19.130.113	ServerOut Anywhere	
ServerOut_DuoSecurity	192.168.100.16, 192.168.100.9, 192.168.100.10	Server mit DuoSecurity	

Zuletzt muss auch der DNS-Record in meinen DNS-Servern angepasst werden:



The screenshot shows the DNS Manager interface. On the left, the tree view shows the hierarchy: DNS > WS-DC1 > Forward-Lookupzonen > rdsweb.ws-its.de. The main pane displays a list of DNS records:

Name	Typ	Daten	Zeitstempel
(identisch mit übergeordne...	Autoritätsursprung (SOA)	[2], ws-dc1.ws.its., hostma...	Static
(identisch mit übergeordne...	Host (A)	192.168.100.16	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc3.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc2.ws.its.	Static
(identisch mit übergeordne...	Namenserver (NS)	ws-dc1.ws.its.	Static

An 'Eigenschaften von rdsweb.ws-its.de' dialog box is open, showing the configuration for a Host (A) record:

- Host (bei Nichtangabe wird übergeordnete Domäne verwendet): (identisch mit übergeordnetem Ordner)
- Vollqualifizierter Domänenname: rdsweb.ws-its.de
- IP-Adresse: 192.168.11.16
- Entsprechenden Zeigereintrag (PTR) aktualisieren
- Eintrag löschen, sobald er verfällt
- Zeitstempel des Eintrags: []
- Gültigkeitsdauer (TTL): 0 :0 :5 :0 (TTTT:HH.MM.SS)

Ein finaler Test von intern und extern war erfolgreich!

Zusammenfassung

Die Umstellung des Servers WS-RDS1 von Windows Server 2016 auf Windows Server 2019 ist abgeschlossen. Das 30 Tage gültige Testzertifikat wird später noch gegen ein gekauftes Zertifikat ersetzt.

Und auch die Erweiterung um den HTML5-Webclient verlief fast ohne Probleme. So macht eine Migration Spass!