

<u>Inhalt</u>

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



<u>Zielsetzung</u>

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:



📙 🛃 📙 🖛 Virtual Hard Disks						
Datei Start Freigeben A	Ansicht					
← → 🔹 🛧 📙 > Dieser PC → Hyper-V (V;) → Hyper-V → WS-RDS1 → Virtual Hard Disks						
👻 🚁 Schnellzugriff	^ Name	Änderungsdatum	Тур	Größe		
🕂 Downloads 🛛 🖈	🕳 HDD0-System.vhdx	09.08.2019 20:26	Festplatten-Image	13.733.888		
👻 🔜 Desktop						
> 🤱 Walther, Stephan - T1						
🗸 💻 Dieser PC						
> 🏪 System (C:)						
> 👝 DATEN (E:)						
> 👳 Freigaben (M:)						
👻 🕳 Hyper-V (V:)						
🗸 📙 Hyper-V						
> 📙 WS-ACAD						
> 📙 WS-ATA						
> 📙 WS-DC1						
> 📙 WS-FS1						
> 📙 WS-MX1						
> 📙 WS-PFS1a						
> 📙 WS-RA1						
🗸 📙 WS-RDS1						
📙 Snapshots						
📙 Virtual Hard Disks						
_						

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:

		1	Systemeigensch	haften				
te ⊳	Computername Arbeitsgruppe	WIN-8C6Q9GBM44A WORKGROUP	Computername Folg	Hardware ende Informa	Erweitert	Remote rden zum Identif	izieren des Co	omput
	Windows Defender Firewall Remoteverwaltung Remotedesktop NIC-Teamvorgang Ethernet Betriebssystemversion Hardwareinformationen	Öffentlich: Ein Aktiviert Deaktiviert 192.168.100.16, Pv6-fäh Microsoft Windows Serv Microsoft Corporation V	Computerbesch Vollständiger C Arbeitsgruppe: Klicken Sie auf umzubenenner Arbeitsgruppe :	hreibung: Computernam f "Åndern", (n öder desse zu ändern.	Beisp "Kon wOP wOP n Domäne	oiel: "IIS-Produkt toführungsserve <mark>RDS1</mark> RKGROUP Computer oder	tionsserver" c r". And	oder
	< EREIGNISSE Alle Ereignisse 8 insgesamt		Die Ande übernom	erungen werd men.	len beim n	ächsten Neusta	rt des Comput	ters be

Vor dem DomainJoin lösche ich das alte Konto im ActiveDirectory:

WS IT-Solutions



NS IT-Solutions

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-rds1.ws.its	192.168.100.16	Windows Server 2019 Datacenter
ws-rds3.ws.its	192.168.101.2	Windows Server 2016 Datacenter
vs-rds1.ws.its		
vs-rds1.ws.its	G 0 Bi 0 Bi 1 Bi 1 Bi 1 Bi 1 Bi 1 Bi 1 Bi 1 Bi 1	ruppenmitgliedschaft: Alle Computer, Update-Verzoegert triebssystem: Windows Server 2019 Datacenter etriebssystemsprache: de-DE rwice Pack: Keine

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:

Aufgabenplanung			
Datei Aktion Ansicht ?			
🗢 🄿 🞽 🖬 🚺 🖬			
Aufgabenplanung (Lokal)	Name	Status	Trigger
	ServerSicherung	Bereit	Jeden Tag um 01:00
	User_Feed_Synchronization-{A6AB5720-6308-4662-916F-8AAF6CFCB9E1}	Bereit	Jeden Tag um 02:01

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



🥌 gl	/ISA-Admin					- 0	×
vorha	ndene gMSA:		zugehörige Ser	ver:		zugehörige Gruppen:	
gMS/ gMS/ gMS/	vADFS (Service ADFS) <u>VBackup (TeskUserfür MMR)</u> <u>Monitor (TeskUserfür Monitoring</u> VSQLDPM (Service SQL auf WS)) DPM)	WS-DC1 ws.its WS-FC1 ws.its WS-MC1 ws.its WS-MA1 ws.its WS-RA1 ws.its WS-RA1 ws.its WS-RA2 ws.its WS-RA2 ws.its WS-RA2 ws.its WS-RDS3 ws.its WS-RD3 ws.its W	s (online) s s	X		*
ers	telle gMSA lösche gMSA	bearbeite gMSA	weiterer S	Der Task wurde umgestellt!	MSA	weitere Gruppe entferne Gruppe	
Einsa	tz als: Task ~	Klicke in eine Zeile um	die Optionen	ОК			
	Server	TaskName			Pf	fad	^
	WS-RDS1	ServerSicherung		ws\gMSA-Backup\$	X		
	WS-RDS1	User_Feed_Synchroniza	ation-{A6AB57	sysadm	N		

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:

Server-M	lanager > Alle Server
IIII Dashboard	Alle Server 1 insgesamt
Lokaler Server	Eilter O (E) Y (P) Y
Alle Server	
Datei-/Speicherdienste 🕨	Servername IPv4-Ad
	WS-MON 169.254 Active Directory DNS Importieren Ausgewählt
	Computer
	Standort:
	Betriebssystem: Alle WS-RDS1
	Name (CN): ws-rds1
	Suche starten
	Name Betriebssystem
	EREIGNISSE WS-RDS1 Windows Server 2019 Datacenter Alle Ereignisse 30 insg Filter Filter Servername WS-MON 10028 WS-MON 10028
	WS-MON 10028 1 Computer gefunden 1 Computer ausgewählt
	WS-MON 10028 WS-MON 10028 Hilfe OK Abbrechen

Und dann geht es mit der Rolleninstallation los:

Assistent zum Hinzufügen von I	lollen und Features	- Ц
Installationstyp au	swählen	ZIELSERVER Es sind keine Server ausgewählt.
Vorbereitung	Wählen Sie den Installationstyp aus. Sie können Rollen und Fea Computer oder auf einem virtuellen Computer oder auch auf ei	tures auf einem ausgeführten physische iner virtuellen Festplatte (Virtual Hard
Installationstyp Bereitstellungstyp	Disk, VHD) im Offlinemodus installieren.	
	Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, R	lollendienste und Features hinzufügen.
	 Installation von Remotedesktopdiensten Bei der Installation waren Rollendienste f ür die virtuelle Desk 	topinfrastruktur (Virtual Desktop
Web Access für Remoted	Infrastructure, VDI) erforderlich, um eine Desktopbereitstellu oder einer Sitzung zu erstellen.	ng auf Basis eines virtuellen Computers
	< Zurück Weite	r > Bereitstellen Abbrechen
Assistent zum Hinzufügen von	Rollen und Features	
Bereitstellungstyp	auswählen	ZIELSERVER Es sind keine Server ausgewählt.
Vorbereitung	Die Remotedesktopdienste können auf mehreren Servern oder	nur auf einem Server konfiguriert
Installationstyp Bereitstellungstyp	 Standardbereitstellung 	
Bereitstellungsszenario	Bei einer Standardbereitstellung können die Remotedesktop	dienste auf mehreren Servern
Rollendienste Remotedesktop-Verbindu	Schnellstart	
Web Access für Remoted	Ein Schnelstart bietet Ihnen die Möglichkeit, Remotedesktop	odienste auf einem Server
RD-Virtualisierungshost Bestätigung	veröffentlicht. Dabei wird eine sammlung erstellt, und kem veröffentlicht.	oteApp-Programme werden
Fertigstellung		
	< Zurück Weiter	r > Bereitstellen Abbrechen
Assistent zum Hinzufügen von I	Rollen und Features	>
Bereitstellungssze	nario auswählen	ZIELSERVER Standardbereitstellung ausgewählt
	Die Remotedesktondienste können so konfiguriert werden, dass	s Benutzer eine Verbindung mit
vorbereitung Installationstyp	virtuellen Desktops, RemoteApp-Programmen und sitzungsbasi	erten Desktops herstellen können.
Bereitstellungstyp	Auf virtuellen Computern basierende Desktopbereitstellung Die auf virtuellen Computern basierende Desktopbereitstellu	ing ermöglicht Reputzern das Herstellen
Bereitstellungsszenario Rollendienste	einer Verbindung mit Sammlungen virtueller Desktops, die vi und virtuelle Desktops enthalten.	eröffentlichte RemoteApp-Programme
Remotedesktop-Verbindu	 Sitzungsbasierte Desktopbereitstellung 	
Web Access für Remoted Remotedesktop-Sitzungs	Die sitzungsbasierte Desktopbereitstellung ermöglicht Benut mit Sitzungssammlungen, die veröffentlichte RemoteApp-Pri	tzern das Herstellen einer Verbindung ogramme und sitzungsbasierte Desktop:
Bestätigung	enthalten.	
	< Zurück Weiter	> Bereitstellen Abbrechen

WS IT-Solutions

<text></text>	📥 Assistent zum Hinzufügen von F	ollen und Features	>
Votereining Notareining Notareining </th <th>Rollendienste übe</th> <th>rprüfen standz</th> <th>ZIELSERVER irdbereitstellung ausgewählt</th>	Rollendienste übe	rprüfen standz	ZIELSERVER irdbereitstellung ausgewählt
Personal or approximate in the second or approximate in the secon	Vorbereitung	Für diese Bereitstellung werden die folgenden Rollendienste für Remotedeskto konfiguriert:	pdienste installiert und
Noncentration We have been been been been been been been be	Bereitstellungstyp Bereitstellungsszenario	Remotedesktop-Verbindungsbroker Vom Remotedesktop-Verbindungsbroker wird ein Clientgerät mit Remo sitzungsbasierten Desktops und virtuellen Desktops verbunden.	oteApp-Programmen,
Projections Projectio	Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Eertiostellung	Web Access für Remotedesktop Mit Web Access für Remotedesktop wird es Benutzern ermäglicht, über einen Webbrowser Verbindungen mit Ressourcen herzustellen, die von und Sammlungen virtueller Desktops bereitgestellt werden. Remotedesktop-Sitzungshost Mit dem Remotedesktop-Sitzungshost wird es einem Server ermäglicht Bronzmme oder sitwunchwärige Decktorg vur broten	das Startmenü oder Sitzungssammlungen t, RemoteApp-
< Zurick Wetter> Bereitsteller, Abbrechen Asstent zum Hinzufügen von Rollen und Festures		 Die Anmeldeinformationen des WS\stephan-T1-Kontos werden zum Erstel Bereitstellung verwendet. 	llen der
A skittent zum Hinzufügen von Rollen und Festures Remotedesktop-Verbindungsboroker angeben Vorbereitung instaliationstyp Bereitstellungsizenario Rollendienste Remotedesktop-Strzungel Bestägiging Ferligstellung Scoverpool Computer gefunden Verbindung Verbindu		< Zurück Weiter > Ben	eitstellen Abbrechen
Addetert zum Hinzufügen von Rollen und Festures Remotedesktop-Verbindungsboroker angeben Vorbereitung Instaliatonsyp Bereitstellungstop Bereits			
Computer suggewählt C	🖆 Assistent zum Hinzufügen von F	ollen und Features	- [] :
Vorbereitung Instalationstyp Bereitstellungsszenario Rollendienste Remotsdedstop-Strungs Bestätigung Perigstellung Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Strungs Bestätigung Perigstellung Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Strungs Bestätigung Perigstellung Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Verbindu Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Verbindu Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Verbindu Vorbereitung Instalatonstyp Bereitstellungsizenario Rollendienste Remotsdedstop-Verbindu Remotsdedstop-Strungs Bestätigung Perigstellung Perigstellung Dereitstellungsizenario Rollendienste Remotsdedstop-Strungs Bestätigung Perigstellung Perigstellung Dereitstellung Dereitstellung Dereitstellungsizenario Rollendienste Remotsdedstop-Strungs Bestätigung Perigstellung Dereitstellung Derei	Remotedesktop-V	erbindungsbroker angeben stand	ZIELSERVER ardbereitstellung ausgewählt
Installationstyp Verbindungsbroker*installieft werden soll. Bereitstellungsszenario Rollendienste Remotedesktop-Verbindungsbroker*installieft werden soll. Ausgewählt Remotedesktop-Verbindungsbroker*installieft werden soll. Verbindungsbroker*installieft werden soll. Remotedesktop-Verbindungsbroker*installieft werden soll. Ausgewählt Remotedesktop-Sitzungs. Verbindungsbroker*installieft werden soll. Bestätigung Fortigstellung Pertigstellungs Computer gefunden Installestonstyp Bereitstellung sollten und Features Assistent zum Hinzufügen von Rollen und Features - Server mit Web Access für Remotedesktop aug. auf dem der Rollendienst "Web Access für Remotedesktop" auf dem Rollendienst "Web	Vorbereitung	Wählen Sie die Server im Serverpool aus, auf denen der Rollendienst "Remoted	lesktop-
Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu. Bestatigung Perigszellung Perigszellung Ausgewählt Serverprod Mane IP-Adresse Betricksp Misch Sitzungs. Serverprod Serverprod Misch Sitzungs. Serverp	Installationstyp Bereitstellungstyp	Verbindungsbroker" installiert werden soll.	
Reliendenste Remoteddesktop-Verbindung Web Access für Remoted. Name IP-Adresse Betriebss Name IP-Adresse Betriebss WS.ITS (1) Web Access für Remoted. WS.ITS (1) WS.RDS1.ws.its 1992168.100.16 Web Access für Remoted. WS.ITS (1) Imagewählt Imagewählt Vorbereitung Imagewählt Zielsever Zielsever a Assistent zum Hinzufügen von Rollen und Festures Imagewählt Zielsever Vorbereitung Installationstyp Bereitstellung surgewählt Zielsever Bereitstellungstyp Remotedesktop-Sitzungs. Remotedesktop-Sitzungs. Ausgewählt Name IP-Adresse Betriebss Ausgewählt Vorbereitung Installeint werden soll. Remotedesktop-Sitzungs. Ausgewählt Bereitstellungstyp Bereitstellungstyp Serverpool Ausgewählt Pertigstellung Verbindungsbrokerserver installieren Ausgewählt Wei ACcess für Remotedesktop-Sitzungs. Serverpool Ausgewählt Iter Name IP-Adresse Betriebss Verligstellung Serverpool I Computer ausge	Bereitstellungsszenario	Serverpool Ausgewählt	
Remotedesktop-Vetrindu, Remotedesktop-Strungs Name IP-Adresse Betriebss Web Access für Remoted Remotedesktop-Strungs WS-RDS1 VS-RDS1 VS-RDS1 Betätigung Perigstellung VS-RDS1 VS-RDS1 VS-RDS1 VS-RDS1 Z Computer gefunden I Computer ausgewählt I Computer ausgewählt Assistent zum Hinzufügen von Rollen und Festures – I Server mit Web Access für Remotedesktop angeben Zielserver Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungszenario Rollendienste Remotedesktop-Verbindu Vwahlen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" auf dem Veb Access für Remotedesktop" auf dem Rol-Verbindungsbrokerserver installieren Serverpool Ausgewählt Web Access für Remotedesktop Strungs Bestätigung Perigstellungs MWS-RDS1 swits 192.108.100.16 NS-RDS1 swits Ausgewählt Vorbereitung Installertorestenster Remotedesktop-Verbindu MS-RDS1 swits 192.108.100.16 NS-RDS1 swits Ausgewählt Serverpool I Computer ausgewählt I Computer ausgewählt I Computer ausgewählt Vorbereitung VS-MON.ws.its 192.21.08.100.16 NS-RDS1 swits I Computer ausgewählt Vorbereitung I Computer ausgewählt I Computer ausgewählt I Comp	Rollendienste	Filter: Computer	
Web Access für Remotedesktop-Sitzungs Remotedesktop-Sitzungs Pertigstellung Vorbereitung Assistent zum Hinzufügen von Rollen und Festures Zerröck Weiter > Bereitstellungszerano Rollendienste Remotedesktop-Verbindu Web Access für Remotedesktop-Verbindu Web Access für Remotedesktop-Verbindu Web Access für Remotedesktop-Verbindu Server mit Web Access für Remotedesktop* auf dem der Rollendienst "Web Access für Remotedesktop" auf dem Rollendienst "Web Access für Remotedesktop" auf dem Rollendienstereinstalling ausgewählt Vorbereitung Installeit werden soll. Web Access für Remotedesktop - Verbindu Vorbereitung Pertigstellung Vorbereitung Vorbereitung Vorbereitung Vorbereitung Vorbereitung Vorbereitung Vorbereitung Verbereitung Verbereitung<	Remotedesktop-Verbindu	A WS.IT: Name IP-Adresse Betriebssy WS-RDS1	5 (1)
Bestätigung WS-MON.vs.its 169.254.148.22 Pertigstellung I Computer ausgewählt I Computer ausgewählt I Computer ausgewählt I Computer ausgewählt I Computer ausgewählt I Server mit Web Access für Remotedesktop angeben ZIELSEWER Vorbereitung installationstyp Wählen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" Vorbereitung installationstyp Wählen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" Verb Access für Remotedesktop-Sitzungs Bestätigung Pertigstellung Mishen Site einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" Verb Access für Remotedesktop-Sitzungs Bestätigung Pertigstellung Serverpool Verb Access für Remotedesktop Verbindung Ausgewählt Vier Direkting Serverpool Vorbereitung Name Verb Access für Remotedesktop-Sitzungs Bestätigung Ausgewählt Verboll weiter Verbindung Vorberigstellung I Computer ausgewählt Verboll weiter I Computer ausg	Web Access für Remoted Remotedesktop-Sitzungs	WS-RDS1.ws.its 192.168.100.16	
Pertigstellung I computer ausgewählt 2 Computer gefunden 2 Computer gefunden Assistent zum Hinzufügen von Rollen und Features - - Assistent zum Hinzufügen von Rollen und Features - Server mit Web Access für Remotedesktop angeben Züllstäviert Vorbereitung Installietn werden soll. Installationstyp Bereitstellungszenario Bereitstellungszenario I collendienst Remotedesktop-Verbindung Sandardbereitstellungs Verbe Access für Remotedesktop* auf dem RD-Verbindungsbrokerserver installieren Serverpool I kasgewählt Computer WS/RDS1 ws.its Verbackstop-Verbindung Nume Weiter - WS/RDS1 ws.its Verdigstellung I computer ausgewählt Computer WS/RDS1 ws.its Verdigstellung I computer ausgewählt	Bestätigung	WS-MON.ws.its 169.254.148.22	
Image: series of the remoted sktop - Verbindungsbrokerserver installieren Vorbereitung Instalationstyp Bereitstellungszenario Rollendienst Bereitstellungszenario Rollendienst Bereitstellungszenario Rollendienst Bestätigung Perligstellung Web Access für Remoted esktop * auf dem RD-Verbindungsbrokerserver installieren Server pool Serverpool			
Image: seriestellung seriesteriestellung seriestellung seriestellung seriestellung			
Image: state in the state			
Image: Computer gefunden 1 Computer ausgewählt Image: Computer gefunden Image: Computer ausgewählt Vorbereitung Image: Computer ausgewählt Image: Computer gefunden Image: Computer ausgewählt Vorbereitung Image: Computer ausgewählt Image: Computer gefunden Image: Computer ausgewählt Vorbereitung Image: Computer gefunden Image: Computer gefunden Image: Computer ausgewählt Image: Computer gefunden <t< td=""><td></td><td></td><td></td></t<>			
2 Computer gefunden 1 Computer ausgewählt < Zurück			
< Zurück		2 Computer gefunden 1 Computer a	usgewählt
Assistent zum Hinzufügen von Rollen und Features Server mit Web Access für Remotedesktop angeben Vorbereitung Installiationstyp Bereitstellungszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung Z Computer gefunden Ausgewählt Computer ausgewählt Compu		< Zurück Weiter > Ber	eitstellen Abbrechen
A Assistent zum Hinzufügen von Kollen und Features			
Server mit Web Access für Remotedesktop angeben Standardbereitstellung ausgewählt Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungszenario Rollendienste Remotedesktop-Verbindung Wahlen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Access für Remotedesktop" installiert werden soll. Web Access für Remotedesktop-Verbindungsbrokerserver installiert Rollendienst "Web Access für Remotedesktop" auf dem RD-Verbindungsbrokerserver installieren Serverpool Serverpool Filter: Name Name IP-Adresse Betriebssig WS-RDS1 (Ns.its) Serverpool Serverpool Verbreitung Serverpool Filter: Name Name IP-Adresse Betriebssig WS-RDS1 (Ns.its) Serverpool VS-RDS1 (Ns.its) VS-MON.ws.its 169.254.148.22 Verbreitung 1 Computer ausgewählt Zornick Weiter > Bereitstellen	Assistent zum Hinzufügen von H	ollen und Features	;
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remotedesktop" Bestätigung Fertigstellung WS-RDS1 //ws.its 169.254.148.22 Verbereitung Z computer gefunden Verbereitung Verbereitung Bestätigung Pertigstellung Z computer gefunden Z computer gefunden Z computer gefunden Z urück Weiter > Bereitstellen	Server mit Web A	ccess für Remotedesktop angeben standt	ZIELSERVER ardbereitstellung ausgewählt
Installationstyp Bereitstellungstyp Bereitstellungszenario Rollendienste Remotedesktop-Verbindu Web Access für Remotedesktop" auf dem RD-Verbindungsbrokerserver installieren Serverpool Filter: Name IP-Adresse Betriebss WS-RDS1.ws.its 192.168.100.16 WS-MON.ws.its 169.254.148.22 Ausgewählt Computer VS-RDS1 US-RDS1 US-RD	Vorbereitung	Wählen Sie einen Server im Serverpool aus, auf dem der Rollendienst "Web Acc installiert werden soll	ess für Remotedesktop:
Bereitstellen Bereitstellen	Bereitstellungstyp	Rollendienst "Web Access für Remotedesktop" auf dem RD-Verbindungsbra	okerserver installieren
Rollendienste Remotedesktop-Verbindu Ausgewählt Web Access für Remoted Filter:	Bereitstellungsszenario		
Remotedesktop-Verbindu Filter:	Rollendienste	Serverpool Ausgewählt	
Name IP-Adresse Betriebss Bestätigung WS-RDS1 ws.its 192.168.100.16 Fertigstellung VS-MON.ws.its 169.254.148.22 2 Computer gefunden 1 Computer ausgewählt	Remotedesktop-Verbindu	Filter	5 (1)
Bestätigung Fertigstellung 2 Computer gefunden	Remotedesktop-Sitzungs	Name IP-Adresse Betriebssy WS-RDS1	13.0
Fertigstellung WS-MUN.ws.its 169.254.148.22 C C C C C C C C C C C C C C C C	Bestätigung	WS-RDS1.ws.its 192.168.100.16	
2 Computer gefunden 1 Computer ausgewählt < Zurück Weiter > Bereitstellen Abbrechen		WS-MON.ws.its 169.254.148.22	
Computer gefunden Computer ausgewählt Computer ausgewählt Curück Weiter > Bereitstellen Abbrechen			
Computer gefunden Computer ausgewählt Computer ausgewählt Curück Weiter > Bereitstellen Abbrechen			
2 Computer gefunden 1 Computer ausgewählt			
< Zurück Weiter > Bereitstellen Abbrechen		2 Computer gefunden 1 Computer a	usgewählt
		< Zurück Weiter > Ber	eitstellen Abbrechen

WS IT-Solutions

🚡 Assistent zum Hinzufügen von R	ollen und Features						×
RD-Sitzungshostse	erver angeber	ı			Standardbereitstellu	ZIELSER\ ung ausgewä	'ER ihlt
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted	Wählen Sie die Server in werden soll. Bei Auswah bereitgestellt. Serverpool Filter:	n Serverpool aus, auf d nl mehrerer Server wird	enen der Rol der Rollendi	llendienst "RD enst auf allen Ausgew Comp 4 V WS-RI	-Sitzungshost" in ausgewählten Se rählt uter VS.ITS (1) 251	stalliert rvern	
RD-Sitzungshost Bestätigung Fertigstellung	WS-RDS1.ws.its WS-MON.ws.its < 2 Computer gefunden	192.168.100.16 169.254.148.22	>	1 Comp	uter ausgewählt		
H		< Zun	ück W	eiter >	Bereitstellen	Abbrech	en
🚡 Assistent zum Hinzufügen von R	ollen und Features				_		×
, Auswahl bestätige	n				Standardbereitstellu	ZIELSERV ung ausgewä	'ER ihlt
Vorbereitung	Zum Abschließen der Ir Nach Abschluss der Ins	stallation müssen die R tallation auf den Remot	emotedeskte ecomputern	op-Sitzungsho wird der lokal	stserver neu ges le Computer neu	tartet werd gestartet.	len.
Bereitstellungstyp	RD-Verbindungsb	roker (1 Server ausgev	wählt)				
Bereitstellungsszenario Rollendienste	WS-RDS1.ws.its Web Access für Re	motedesktop (1 Serve	er ausgewäl	hlt)			
Remotedesktop-Verbindu	WS-RDS1.ws.its						
RD-Sitzungshost Bestätigung Fertigstellung	Remotedesktop-Si	tzungshost (1 Server Server können nach de	ausgewählt) des Rollendie	nsts neu gestarte	et werden.	
e l	Zielserver bei Bedar	f automatisch neu start	en				
1		< Zun	ück	eiter >	Bereitstellen	Abbrech	en

WS IT-Solutions

Das Setup läuft und ist nach wenigen Minuten erfolgreich abgeschlossen:

tatus anzeigen			Star	ndardbereitstellu	ZIELSEF ing ausgev
Vorbereitung	Die ausgewählten Kollendienste	der Remotedesktopdienste wer	den installier	t.	
	Server	Status		Status	
	Remotedesktop-Verbindungs	broker (Rollendienst)			
	WS-RDS1.ws.its		Erfolgreic	h	
			-		
	Web Access für Remotedeskt	op - Rollendienst			
Web Access für Remoted	WS-RDS1.ws.its		Erfolgreic	h	
RD-Sitzungshost					
	Remotedesktop-Sitzungshost	(Rollendienst)			
Fertiastelluna	WS-RDS1.ws.its		Erfolgreic	h	
5 5					



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		\sim	
	Mode:	Submit CSR load CSR Create CSR			
	CommonName:	rdsweb.ws.its			
	additional Subjects:	DNS=ws-rds1ws.its			
	show samples				
	Organization:	WS IT-Solutions			
	OrganizationalUnit:	IT			
	Locality:	Ergoldsbach			
	State:	Bayem			
	Country:	DE			
	EMail:	itservice@ws.its			
	KeyLength:	2048 ~			
	KeyExportable:	true 🗸			
	PFX-Password:	•••••			
		Issue Certificate Show Files			
	ready				
201	9-09-10_rdsweb.w s.its.pfx				

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:

WS IT-Solutions

WSHowTo – Neuinstallation eines RDS mit HTML5 (WS-RDS1) 2019-09-10 Migration auf Windows Server 2019



Noch ist kein Gateway installiert:

ereitstellungseigenschaften		-		×
ereitstellung kor	figurieren			
Alle anzeigen Remotedesktopga Remotedesktopliz + Web Access für Re + Zertifikate +	Remotedesktopgateway RD-Gatewayeinstellungen für die Bereitstellung angeben O Remotedesktop-Gatewayservereinstellungen automatisch ermitteln Diese Einstellungen für den RD-Gatewayserver verwenden: Servername:			
	Anmeldemethode: Kennwortauthentifizierung RD-Gatewayanmeldeinformationen für Remotecomputer verwenden Remotedesktop-Gatewayserver für lokale Adressen umgehen © Keinen RD-Gatewayserver verwenden			~
		OK Abbrechen	Anwende	

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



🚡 Bereitstellungseigenschaften	-
Bereitstellung konf	igurieren
Alle anzeigen	
Remotedesktopga +	RD-Lizenzierung
Remotedesktopliz –	Remotedeskton-lizenzierungsmodus auswählen:
Web Access für Re +	O Pro Gerät
Zertifikate +	O Pro Benutzer
	Geben Sie einen Lizenzserver an, und klicken Sie anschließend auf "Hinzufügen":
	Hinzufügen
	Wählen Sie die Reihenfolge der Remotedesktop-Lizenzserver aus: Der RD-Sitzungsbastenver oder RD-Virtualisienungsbastenversendet Lizenzanforderungen in der hier festgelegten Reihenfolge an die angegebenen Lizenzgener
	Der Korstizungsnossenen oder Korvirtuansierungsnosserver sendet Lizenzantorderungen in der mier resignegien nemennöge an die angegebenen Lizenzserver.
	Nach Oben
	Nach unten
	Entfernen
	OK åbbrechen ånwenden
	Internet Anternet

Das ist die interessante Funktion:

ᡖ Bereitstellungseigenschaften				-		×
Bereitstellung kor	nfigurieren					
Alle anzeigen Remotedesktopga + Remotedesktopliz +	Web Access für Remotedesktop					
Web Access für Re	Server mit Web Access für Remotedesktop	URL				
Zertifikate +	WS-RDS1.WS.ITS	https://WS-RDS1.WS.ITS/RdWeb				
	Durch die zusätzliche Unterstützung des RD-We Erfahren Sie mehr über den RD-Webclient.	ebclients können Benutzer von einem unterstützten Browser aus eine	e Verbindung mit Ressource	n herstel	len.	
						_
			UK Abbrech	nen /	Anwend	en

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



🚡 Bereitstellungseigenschaften							_	
Bereitstellung konfi	aurieren							
Alle anzeigen	5							
Remotedesktopga +	Zertifikate verwalten							
Remotedesktopliz +								
Web Access für Re +	erforderlich.	sereitstellung sind Zertifik	cate fur die Serv	rerauthentifizierung, i	inmaliges Anmelde	n und Herstellen von s	icheren Verbind	Jungen
Zertifikate –	Die aktuelle Zertifikatestufe der B	araitstallung ist Nicht kon	ofiquriert					
	Was ist eine Zertifikatsstufe?	erenstending ist Micht ko	ingunere					
	Rollendienst	Stufe	Status	Status				
	Remotedesktop-Verbindungsbr	oker Nicht konfiguriert						
	Remotedesktop-Verbindungsbr	oker Nicht konfiguriert						
	RD-Gateway	Unbekannt						
	Antragstellername: Nicht verfügb Details anzeigen	ar						
	Dieses Zertifikat ist für die Servera	authentifizierung für die F	Remotedesktop	dienste-Bereitstellun	g erforderlich.			
	Sie können dieses Zertifikat aktua	lisieren, indem Sie ein ne	ues Zertifikat er	rstellen oder ein vorh	andenes Zertifikat a	uswählen.		
	Neues	Zertifikat erstellen			Vorhand	lenes Zertifikat auswäh	len	
						OK AI	bbrechen A	nwenden
-								_
🚡 Bereitstellungseigenschaften							_	
Bereitstellung konfi	aurieren	ertifikat auswählen					>	<
Alle sessions	Sia kännan das	momentan auf dem PD)	Varbindungsbra	korroniar gospoisho	to Zostifikat anusau	dan adar ain andarar 7	ortifikat in	
Remotedesktopga +	Zertifikate einer PKCS-Zer	tifikatsdatei auswählen.	verbindungsbro	okerserver gespeiche	te zerunkat anwend	sen oder ein anderes z	erunkat in	
Remotedesktopliz +	Eür eine Remo)-Verbindungsbrokerserve	er gespeicherte	s Zertifikat anwender	1			200
Web Access für Re +	erforderlich. Kennwort:	-						gen
Zertifikate –	Die aktuelle Ze							
	Was ist eine Ze	rtifikat auswählen						
	Rollendienst Zertifikatpfa	ad:						
	Remotedesk Remotedesk Remotedesk	ephan-T1\Desktop\2019-	-09-10_rdsweb.v	ws.its.pfx		Di	urchsuchen	
	Web Access Kennwort:							
	RD-Gateway	•••••						
	Antragstellern 🗹 Hinzufügen	des Zertifikats zum Zertif	fikatspeicher "V	ertrauenswürdige Sta	mmzertifizierungss'	tellen" auf den Zielcom	putern zulasser	1
	Details anzeig							
	Dieses Zertifik							
	Sie können die							
						ОК	Abbrechen	1
								1
							hbrochon A	nwandan
						At	A	invenuen



							-
Daten werden gespeichert							
Remotedesktopga +	Zertifikate verwalten						
Remotedesktopliz +	Zertinkate verwatern						
Web Access für Re +	Für eine Remotedesktopdienste-Bereit	stellung sind Zertifika	ate für die Sei	rverauthentifizierung, einmalig	ges Anmelden und Herstellen vo	on sicheren Verł	D
Test Close	erforderlich.						
	Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	tellung ist Nicht kon	figuriert				
	Rollendienst	Stufe	Status	Status			
	Remotedesktop-Verbindungsbroker	Nicht konfiguriert		Kann angewendet wer			
	Remotedesktop-Verbindungsbroker	Nicht konfiguriert					
	Web Access für Remotedesktop	Nicht konfiguriert					
	RD-Gateway	Unbekannt					
	RD-Gateway Antragstellemame: Nicht verfügbar Details anzeigen Dieses Zertifikat ist für die Serverauthe Sie können dieses Zertifikat aktualisier	Unbekannt entifizierung für die R en, indem Sie ein neu	emotedeskto Jes Zertifikat (pdienste-Bereitstellung erford erstellen oder ein vorhandene	derlich. es Zertifikat auswählen.		
	RD-Gateway Antragstellername: Nicht verfügbar Details anzeigen Dieses Zertifikat ist für die Serverauthe Sie können dieses Zertifikat aktualisier Neues Zerti	Unbekannt entifizierung für die R en, indem Sie ein neu fikat erstellen	emotedeskto ues Zertifikat (pdienste-Bereitstellung erford erstellen oder ein vorhandene	derlich. es Zertifikat auswählen. Vorhandenes Zertifikat ausv	vählen	

🛼 Bereitstellungseigenschaften

Remotedesktopga +	Zertifikate verwalten				
Remotedesktopliz + Web Access für Re + Zertifikate –	Für eine Remotedesktopdienste-Bereit erforderlich. Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	tstellung sind Zertifika stellung ist Vertraue n	ate für die Se swürdig	rverauthentifizierun	g, einmaliges Anmelden und Herstellen von sicheren Verbindunge
	Rollendienst	Stufe	Status	Status	
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	Erfolgreich	
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	Erfolgreich	
	Wah Accors für Pomotodoskton	Vertrauenswürdig	OK	Erfolgreich	
	web Access full Remotedesktop				
	RD-Gateway Antragstellername: E=itservice@ws.its, Details anzeigen	Unbekannt , CN=rdsweb.ws.its, C	 DU=IT, O=WS	IT-Solutions, L=Erg	oldsbach, S=Bayern, C=DE
	RD-Gateway Antragstellemame: E=itservice@ws.its Details anzeigen Dieses Zertifikat ist für die Aktivierung Remotedesktop erforderlich. Sie können dieses Zertifikat aktualisier	Unbekannt , CN=rdsweb.ws.its, C des RemoteApp- un en, indem Sie ein neu	 DU=IT, O=WS d Desktopver res Zertifikat	5 IT-Solutions, L=Erg rbindungsabonneme erstellen oder ein vo	oldsbach, S=Bayern, C=DE ents und für die Serverauthenbifizierung für Web Access für orhandenes Zertifikat auswählen.
	RD-Gateway Antragstellername: E=itservice@ws.its Details anzeigen Dieses Zertifikat ist für die Aktivierung Remotedesktop erforderlich. Sie können dieses Zertifikat aktualisier Neues Zerti	Unbekannt , CN=rdsweb.ws.its, C des RemoteApp- un en, indem Sie ein neu fikat erstellen	 DU=IT, O=WS d Desktopver res Zertifikat	i IT-Solutions, L=Erg rbindungsabonneme erstellen oder ein vo	oldsbach, S=Bayern, C=DE ents und für die Serverauthentifizierung für Web Access für orhandenes Zertifikat auswählen Vorhandenes Zertifikat auswählen
	RD-Gateway Antragstellername: E=istervice@ws.its Details ancigen Dieses Zertifikat ist für die Aktivierung Remotedesktop erforderlich. Sie können dieses Zertifikat aktualisier Neues Zerti	Unbekannt CN=rdsweb.ws.its, C des RemoteApp- und en, indem Sie ein neu fikat erstellen	 DU=IT, O=WS d Desktopver res Zertifikat	5 IT-Solutions, L=Erg ibindungsabonneme erstellen oder ein vo	oldsbach, S=Bayern, C=DE ents und für die Serverauthentifizierung für Web Access für orhandenes Zertifikat auswählen. Vorhandenes Zertifikat auswählen

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:

- 🗆 ×



🗟 Server-Manager		– 🗆 X
Server-	Manager • Remotedesktop- dienste • Sammlungen • ② 🚩 Verwalten Toc	ols Ansicht Hilfe
Üborricht	SAMMLUNGEN Lette Athulisianum: 10.09.2019.19.30/08.1 Alle Sammlungen, 1.0. insgesamt	
Server		Sammlung virtueller Desktops erstellen
Sammlungen		Sitzungssammlung erstellen Bereitstellungseigenschaften bearbeiten
© ⊘ ⊳		
	LIGTTERVER VERPINNUMEN	
	HOS IS ERVER VERSINUUNGEN Letze Aktualisierung: 10.09.2019 19:30:03 Alle Server 1 insgesamt AUFGABEN VERSINUUNGEN Letze Aktualisierung: 10.09.2019 19:30:31 Alle Verbindungen 0 insg	AUFGABEN V
	Filter ρ \blacksquare \checkmark \bigcirc Filter ρ \blacksquare \checkmark	\odot
	Servername Typ Virtuelle Desktops Neue Verbindungen zulassen Sammlungsname Vollqualifizierter Domänenname des Servers Benut	izer Sitzungszusta
	WS-RDS1 RD-Sitzungshost n/v Wahr	
		~
Server-Manager		- 🗆 X
Server	r-Manager • Remotedesktop- dienste • Sammlungen • 🕝 🚩	Verwalten Tools Ansicht Hilfe
Übersicht	SAMMLUNGEN Letzte Aktualisierung: 10.09.2019 19:30:03 Alle Sammlungen 0 insgesamt	AUFGABEN 💌
Server	Filter 👂 🗄 🔻 🔞 🕶	\odot
ir ⊳	Name Typ Größe Ressourcentyp Status	
	🚡 Sammlung erstellen — 🗆 X	
	Namen für die Sammlung angeben	
	Vorbemerkungen Für Benutzer wird bei der Anmeldung beim Server mit Web Access für Remotedesktop der Sammlungsname "session" angezeigt.	
	Sammlungsname Remotedesktop-SitzungsName:	
	Benutzergruppen Bechreihung (pational)	
	HC Bestätigung	
	Let Status erbindu	ungen 0 insg AUFGABEN 🔻
	Se arme de	s Servers Benutzer Sitzungszusta
	< Zurück Weiter > Erstellen Abbrechen	



🚵 Server-Manager		- 🗆 ×
Server-M	Nanager • Remotedesktop- dienste • Sammlungen 🛛 🔹 🕻	Verwalten Tools Ansicht Hilfe
Ü Übersicht Server Sammlungen	SAMMLUNGEN Letzte Aktualisierung: 10.09.2019 19:30:03 Alle Sammlungen 0 insgesamt Filter ⓐ ▼ ⓐ ▼ Name Typ Größe Ressourcentyp Status	AUFGABEN V
	Sammlung erstellen - × RD-Sitzungshostserver angeben Vorbemerkungen vallen Sie die RD-Sitzungshostserver im Serverpool aus, die dieser Sammlung hinzugefügt werden sollen. Benutzergruppen Benutzergruppen Benutzergruppen Status Status Serverpool W IP-Adresse Betritigung Status Status 1 Computer gefunden 1 Computer gefunden 1 Computer ausgewählt	rbindungen 0 insg AUFGABEN ▼ B ▼ (A) ▼ ⊙ me des Servers Benutzer Sitzungszusta

🔁 Serve	er-Manager	- C	1 ×
E		anager • Remotedesktop- dienste • Sammlungen 🛛 • 🕲 🏲 Verwalten Tools Ansicht	Hilfe
Übersicht Server Sammlungen ⊳		SAMMLUNGEN AUFGABEN Letzte Aktualisierung: 10.09.2019 19:30:03 Alle Sammlungen 0 insgesamt AUFGABEN Filter P ® ▼ © Name Tup, Größe Ressourcentup, Status ©	•
		Image: state state in the state sta	▼ ∂ usta





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

Übersicht	SAMML Letzte Ak	.UNGEN tualisierung: 10.09.2019 19:5	2:12 Alle Sammlungen	1 insgesamt			AUFGABEN
Server Sammlungen	Filter						۲
Þ	RDSWER_Sitzu Sammlu Statu Vorbe	ng erstellen s anzeigen merkungen	ie Sitzungssammlung wirr	d erstellt, Je nach Größe der Sitzungssammli	ung kann dieser Vorgang	×	
	HC Bestatus	lungsname :edesktop-Sitzungs :ergruppen zerprofil-Datenträger igung	Aktivität Sammlung erstellen Server hinzufügen	Status WS-RDS1.WS.ITS Der RD-Sitzungshostserver "WS-RDS1.WS.ITS" kann nicht konfguriert werden. Der Vorgang ist ungültig. WS-RDS1.WS.ITS Die Eigenschaft "RedirectlientPrinter" wird über die Grungenichtlinienteinstellungen	Status ^ Erfolgreich Abgeschlossen	erbindungen 0 insg B • B • sme des Servers Benut	AUFGABEN 🔹
	W			konfiguriert. Verwenden Sie die Gruppenrichtlinien- Verwaltungskonsole, um diese Eigenschaft zu konfigurieren.			

Dennoch wurde sie erstellt:



📥 Server-Manager		- 🗆 X
Serv	er-Manager + Remotedesktop- dienste + Sammlunger) • RDSWEB • 🕄 🚩 Verwalten Tools Ansicht Hilfe
Übersicht I Server I Sammlungen RDSWEB I I	EIGENSCHAFTEN Eigenschaften der Sammlung AUFGABEN Sammlungstyp Sitzung Ressourcen Remotedesktop Benutzergruppe WS\Domänen-Benutzer	VERBINDUNGEN Letzte Aktualisierung: 10.09.2019 19:52:12 Alle Verbindungen 0 insgesamt AUFGABEN ▼ Filter
	REMOTEAPP-PROGRAMME AUFGABEN Veröffentlichte RemoteApp-Programme 0 insgesamt AUFGABEN 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 Letzte Aktualisierung: 10.09.2019 19:52:12 Alle Server 1 insgesa AUFGABEN • Filter	
	Servername Typ Virtuelle Desktops Neue Verbindungen zulassen WS-RDS1 RD-Sitzungshost n/v Wahr	

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

	Name	Тур	Daten	Zeitste
	ForestDnsZones			
erte Lookupvorgange	DomainDnsZones			
nen	_udp			
	🚞_tcp			
	Neuer Host		×	
	prto		ws.its.	Static
	crl Name (bei Nic	htangabe wird übergeordneter Dom	nänenname s.its.	Static
	aut rdsweb		.its.	Static
en	(ide Lidsweb		vs-dc1.ws.its., h	o Static
ngen	WS Vollqualifiziert	er Domänenname:	00.22	11.09.
-	WS rdsweb.ws.i	ts.	01.2	11.09.
	WS TR-Adresses		10.21	11.09.
	WS 192 168 100	1.16	00.16	10.09.
	WS 192.100.100	7.10	00.17	11.09.
	WS Verknüpft	en PTR-Eintrag erstellen	00.7	10.09.
	WS Authentifi:	zierte Benutzer können DNS-Einträg	e mit demselben 1.252	Static
	WS Besitzerna	men aktualisieren	1.252	Static
	WS Gültigkeitsdau	ier (TTL):	01.252	Static
	WS 0 :0	:5 :0 (TTTTT:HH.MM.SS)	11.252	Static
	WS		00.251	Static
	WS		00.250	Static
	WS	Host hinzufügen	Abbrechen 0.252	Static
	ws	- Host Hinzardger	00.252	Static
	WS-PFS1	Host (A)	192.168.110.252	Static

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





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

	SC System	- Interfaces -	Firewall -	Services 🔻	VPN -	Status 🕶	Diagnostics 🔻	Help 👻		•
Statu	s / System I	Logs / Firewa	all / Normal V	liew						₹ <i>⊁</i> 0
System	Firewall	DHCP Captiv	e Portal Auth IP	sec PPP	VPN	Load Balar	ncer OpenV	PN NTP	Settings	
Normal	View Dynam	ic View Summ	ary View							
Advan	ced Log Filter									Θ
						192	.168.100.16			
		Source IP Address				Desti	nation IP Address			
		Pass							500	٢
		Tin	ne		Source	Port	Protoco	bl	Quantity	
									Y Apply Filter	
		Inte	erface		Destin	ation Port	Protoco	ol Flags		
		Regular expressior	n reference Precede w	ith exclamation	(!) to exclude	e match.				
5 Mato	ched Firewall L	og Entries. (Max	kimum 500)							
Action	Time	Interface	Rule				Source	0	estination	Protocol
×	Sep 10 19:53:54	LAN_110_CLIENTS	Default deny rule II	Pv4 (100000010	3)		192.168.11	0.101:4287	192.1 68.100.16:443	TCP:S
×	Sep 10 19:53:49	LAN_110_CLIENTS	Default deny rule II	Pv4 (100000010	3)		192.168.11	0.101:4287	192.168.100.16:443	TCP:S
×	Sep 10 19:53:46	LAN_110_CLIENTS	Default deny rule II	Pv4 (100000010	3)		192.168.11	0.101:4287	192.168.100.16:443	TCP:S
×	Sep 10 19:51:09	DMZ_120_EXTERM	Default deny rule II	Pv4 (100000010	3)		172.19.120	.254:58899	192.168.100.16:80	TCP:S
×	Sep 10 19:51:06	DMZ_120_EXTERM	Default deny rule II	Pv4 (100000010	3)		i = 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:



	r Interfaces ∓ Firewall ▼	Services - VPN -	Status 🕶	Diagnostics 👻	Help 🕶	•
Firewall / Aliases	/ Edit					0
Properties						
Name	ServerIn_HTTPS The name of the alias may only consist	t of the characters "a-z, A-	Z, 0-9 and _".			
Description	Services mit HTTPS A description may be entered here for a	administrative reference (r	not parsed).			
Туре	Host(s)		~			
Host(s) Hint	Enter as many hosts as desired. Hosts re-resolved and updated. If multiple IPs as 192.168.1.16/28 may also be entere	must be specified by thei s are returned by a DNS qu ed and a list of individual I	r IP address or ful iery, all are used. <i>A</i> P addresses will b	ly qualified domain An IP range such as re generated.	name (FQDN). FQDI 192.168.1.1-192.16	N hostnames are periodically 8.1.10 or a small subnet such
IP or FQDN	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 (RDSWE	B)		💼 Delete

Die Webseite lässt sich nun fehlerfrei aufrufen:



Nach der Anmeldung wird die SessionCollection angezeigt:



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

WS IT-Solutions

Web Acce	ss für Remotedesktop	× +									-	-		\times
(←) → C'	۵	🛈 🔒 https://rdswe	eb. ws.its /RDWeb/P	Pages/de-DE	/Default.aspx	•••	⊠ ☆		$\mathbf{\overline{1}}$	lii\	1		V	≡
OuckDuckGo	🗀 Devices 📋 Lin	nks												
1 Carllon	121		12	2355	0	a:	11			/				^
	. 147				<u></u>			📕 Web Ac	ress fü	r Remot	edesktor			
	Wor Remote	K Resources	dung			X	T							
	RemoteApp un	d Desktops	💀 Remotedeskt	opverbindung				×		Abme	den			
4	Aktueller Ordnu	er: /	Vertrauer Durch diese Remot Stellen Sie vor dem Urch diese Remote terraus Urch diese Remote Urch diese Remote	n Sie dem Her teverbindung kö i Herstellen der igeber: ecomputer:	rausgeber dieser F innte der lokale oder of Verbindung sicher, da rdsweb ws.its Remotedesktopverbi WS-RDS1.WS.ITS	Remoteverbind der Remotecomp ss Sie dem Hera indung mehr anfordem	lung? uter beschädigt usgeber vertraue	werden. m.						
1				nden	en nerausgeber hicht	Ve	rbinden Ab	brechen				A		



ntervision - State - S



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:

Server-N	lanager ∙ Rer	notedesktop- dienst	e • Übersicht	
cht	ERSTE SCHRITTE N	IIT DEN REMOTEDESKTOPDIENS	STEN	- 🗆 X .
lungen WEB	SCHNELLSTART WEITERE INFORMATIONE N	Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re Zertifikate +	figurieren Web Access für Remotedesktop Server mit Web Access für Remotedesktop WS-RDS1.WSJTS) URL https://WS-RDS1.WS.ITS/RdWeb
	BEREITSTEL RD-Verbindur Verwaltet als: WS\st		Curch die zusätzliche Unterstützung des RD-W unterstützten Browser aus eine Verbindung mi Erfahren Sie mehr über den RD-Webclient.	/ebclients können Benutzer von einem t Ressourcen herstellen.

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

WS IT-Solutions

WSHowTo – Neuinstallation eines RDS mit HTML5 (WS-RDS1) 2019-09-10 Migration auf Windows Server 2019



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
$BrokerCertThumprint = (Get-RDCertificate -Role RDRedirector).Thumbprint
Get-ChildItem -Path "Cert:\LocalMachine\My\$BrokerCertThumprint" |
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: <u>https://rdsweb.ws.its/rdweb/webclient/</u>. Die Anmeldemaske sieht vielversprechend aus:



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



Der Start dauert einige Sekunden:

WS IT-Solutions



Doch statt einem Desktop erhalte ich eine Fehlermeldung:

WS IT-Solutions

III Alle Ressourcen	RDSWEB ×		2	ŝ	 Abmelden	^
		Wir konnten leider keine Verbindung mit "RDSWEB" herstellen.				
		Die Verbindung mit dem Remotecomputer wurde unterbrochen. Unter Umständen liegt ein Problem mit der Netzwerkverbindung vor. Sollte das Problem wiederholt auftreten, wenden Sie sich an Ihren Administrator oder an den technischen Support.				
		Verbindung wiederherstellen Abbrechen				

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

WS	IT-S	olu	tior	۱S

	us / System I	_ogs / Fir	ewall / Norm	al View								T 7 6
System	n Firewall	DHCP C	Captive Portal Auth	IPsec	PPP	VPN	Load	Balancer	OpenVPN	NTP	Settings	
Norma	l View Dynam	ic View S	Summary View									
Advan	nced Log Filter											e
		192.168.110	0.101					192.168.10	0.16			
		Source IP Ad	dress				(Destination I	P Address			
		Dage									500	•
			Time			Source	Port		Protocol		Quantity	
		D Black									Apply Filter	
		DIOCK	Interface			Destinat	tion Port		Protocol Flag	3	A sppy million	
									-			
		Regular expre	ession reference Prec	ede with excl	amation (!) t	o exclude	match.					
		Regular expre	ession reference Prec	ede with excl	amation (!) t	o exclude	match.					
7 Mat	ched Firewall L	Regular expre	ession reference Prec (Maximum 500)	ede with excl	amation (!) t	o exclude	match.					
7 Mat	ched Firewall Lo Time	Regular expre og Entries. Interface	ession reference Prec (Maximum 500) Rule	ede with excl	amation (!) t	o exclude	match.	Source	_	Desti	nation	Protocol
7 Mat tion	ched Firewall Lo Time Sep 15 11:19:23	Regular expre og Entries. Interface LAN_110_CL	ession reference Prec (Maximum 500) Rule IENTS Default deny	ede with excl	amation (!) t 00000103)	o exclude	match.	Source	2.168.110.101:1	Destin 182 i 🕀	nation 192.168.100.16 <mark>;339;</mark>	Protocol TCP:S
7 Mat ction X X	ched Firewall L Time Sep 15 11:19:23 Sep 15 11:19:23	Regular expre og Entries. Interface LAN_110_CL LAN_110_CL	(Maximum 500) Rule IENTS Default deny IENTS Default deny	ede with excl rule IPv4 (10 rule IPv4 (10	amation (!) 1 00000103) 00000103)	o exclude	match.	Source i=19	2.168.110.101:1 2.168.110.101:1	Destir 182 i⊕1 181 i⊕1	nation 192.168.100.16 <mark>:339:</mark> 192.168.100.16:339:	Protocol 2 TCP:S 2 TCP:S
7 Mat ction X X	Ched Firewall L Time Sep 15 11:19:23 Sep 15 11:19:23 Sep 15 11:19:17	Regular expre	ession reference Prece (Maximum 500) Rule IENTS Default deny IENTS Default deny IENTS Default deny	ede with excl rule IPv4 (10) rule IPv4 (10) rule IPv4 (10)	amation (!) t 00000103) 00000103) 00000103)	o exclude	match.	Source i=19 i=19 i=19	2.168.110.101:1 2.168.110.101:1 2.168.110.101:1	Destin 182 i⊕ 181 i⊕ 182 i⊕	nation 192.168.100.16 <mark>:339;</mark> 192.168.100.16:339; 192.168.100.16:339;	Protocol 2 TCP:S 2 TCP:S 2 TCP:S
7 Mat ction × × ×	Ched Firewall L Time Sep 15 11:19:23 Sep 15 11:19:23 Sep 15 11:19:17 Sep 15 11:19:17	Regular expression og Entries. Interface LAN_110_CLL LAN_110_CLL LAN_110_CLL LAN_110_CL	(Maximum 500) Rule IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny	ede with excl rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10)	amation (!) 1 00000103) 00000103) 00000103) 00000103)	o exclude	match.	Source i = 19 i = 19 i = 19 i = 19 i = 19	2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1	Destin 182 i⊕ 181 i⊕ 182 i⊕ 182 i⊕	nation 192.168.100.16 <mark>:339</mark> ; 192.168.100.16:339; 192.168.100.16:339; 192.168.100.16:339;	Protocol 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S
7 Mat ction × × × ×	ched Firewall L Time Sep 15 11:19:23 Sep 15 11:19:23 Sep 15 11:19:17 Sep 15 11:19:17	Regular expression og Entries. Interface LAN_110_CL LAN_110_CL LAN_110_CL LAN_110_CL	(Maximum 500) Rule IENTS Default deny	rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10)	00000103) 00000103) 00000103) 00000103)	o exclude	match.	Source i = 19 i = 19 i = 19 i = 19 i = 19 i = 19	2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1	Destin 182 i ⊕ 1 181 i ⊕ 1 182 i ⊕ 1 181 i ⊕ 1 182 i ⊕ 1	nation 192.168.100.16; <mark>339;</mark> 192.168.100.16;339; 192.168.100.16;339; 192.168.100.16;339;	Protocol TCP:S TCP:S TCP:S TCP:S TCP:S
7 Mat etion X X X X X	Ched Firewall Li Time Sep 15 11:19:23 Sep 15 11:19:23 Sep 15 11:19:17 Sep 15 11:19:17 Sep 15 11:19:17 Sep 15 11:19:17 Sep 15 11:19:17	Regular expression og Entries. Interface LAN_110_CLL LAN_110_CLL LAN_110_CLL LAN_110_CLL	(Maximum 500) Rule IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny	rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10)	amation (!) 1 00000103) 00000103) 00000103) 00000103)	o exclude	match.	Source i = 19 i = 19 i = 19 i = 19 i = 19 i = 19	2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1	Destin 182 i + 1 181 i + 1 182 i + 1 181 i + 1 182 i + 1 182 i + 1	nation 192.168.100.16: <mark>339:</mark> 192.168.100.16:339: 192.168.100.16:339: 192.168.100.16:339:	Protocol 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S
7 Mat tion × × × × ×	Ched Firewall L Time Sep 15 11:19:23 Sep 15 11:19:23 Sep 15 11:19:17 Sep 15 11:19:17 Sep 15 11:19:17 Sep 15 11:19:14	Regular expression og Entries. Interface LAN_110_CL LAN_110_CL LAN_110_CL LAN_110_CL LAN_110_CL LAN_110_CL	IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny IENTS Default deny	rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10) rule IPv4 (10)	amation (!) 1 00000103) 00000103) 00000103) 00000103) 00000103) 00000103)	o exclude	match.	Source i 19 i 19 i 19 i 19 i 19 i 19 i 19 i 19 i 19 i 19	2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1 2.168.110.101:1	Destin 182 i ⊕ 1 181 i ⊕ 1 182 i ⊕ 1 181 i ⊕ 1 182 i ⊕ 1 181 i ⊕ 1 182 i ⊕ 1 183 i ⊕ 1 184 i ⊕ 1 185 i ⊕ 1	nation 192.168.100.16: <mark>3392</mark> 192.168.100.16:3392 192.168.100.16:3392 192.168.100.16:3392 192.168.100.16:3392	Protoco 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S 2 TCP:S 2 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:

	C System - ∾	Interfaces 👻	Firewall 🗸	Services -	VPN -	Status 🕶	Diagnostic	s • Help •		Þ
Firewal	I / Rules / D	MZ_120_EX	TERN							ŧ III ■ 6
Floating	DMZ_120_EXTE	RN LAN_100	SERVER	DMZ_130_INTERN	LAN_11	IO_CLIENTS	DMZ_14	0_GAMEZONE	DMZ_150_ISOLA	TION
Rules (D	rag to Change (Order)								
	0 /38 KiB IP	v4 TCP Site_Neu	ıfahrn * s	ServerIn_HTTP	Ports_HTTP	*	none	Zugri	iff HTTP	₺₡₢₡
	0 /1.54 GiB IP	v4 TCP Site_Neu	ıfahrn * s	ServerIn_HTTPS	Ports_HTTP	Alias deta	ils	Zugri	iff HTTPS	≟∥⊡⊘₫
	0 /0 B IP	v4 TCP Site_Neu	ıfahrn * s	ServerIn_RDS	Ports_RDS	Value De	escription	Zugri	iff RDS	₺₡₢₡
	0 /33.90 MiB IP	v4 TCP Netz_10	1 * 9	ServerIn_DPM	Ports_DPM	443 WI	EB	Zugri	iff DPM	₺₡₢₡

Für diese Anwendung erweitere ich den bestehenden PortAlias "Ports_RDS":



	System -	Interfaces 🗸	Firewall 👻	Services -	VPN -	Status 🗸	Diagnostics 👻	Help 👻		€
Firewall /	Aliases	/ Edit								0
Properties										
	<u>Name</u>	Ports_RDS The name of the alia	s may only cons	ist of the charact	ters "a-z, A-Z,	, 0-9 and _".				
De	escription	RDS (TCP&UDP) A description may be	entered here fo	r administrative	reference (no	ot parsed).				
	Туре	Port(s)				\sim				
Port(s)										
	Hint	Enter ports as desire	d, with a single p	port or port range	e per entry. P	ort ranges can	be expressed by sep	arating with a colo	۱.	
	Port	3389			R)S			î Delete	
		443			W	EB			🛅 Delete	
		3392			R	S-Webclient			💼 Delete	
		🖺 Save 🕇 Add	Port							

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

	System -	Interfaces 👻	Firewall 👻	Services -	VPN -	Status 🗸	Diagnostics 👻	Help 👻	¢
Firewall /	Aliases	/ Edit							0
Properties									
	Name	ServerIn_RDS							
		The name of the alia	as may only cons	sist of the charac	ters "a-z, A-Z	, 0-9 and _".			
De	scription	Server mit RDS							
		A description may b	e entered here fo	or administrative	reference (n	ot parsed).			
	Type	Host(s)				~			
Host(s)									
	Hint	Enter as many hosts re-resolved and upd as 192.168.1.16/28	as desired. Hos ated. If multiple may also be ent	ats must be spec IPs are returned ered and a list of	ified by their by a DNS que individual IP	IP address or f ry, all are used addresses will	ully qualified domain . An IP range such as I be generated.	name (FQDN). FQI 192.168.1.1-192.1	DN hostnames are periodically 68.1.10 or a small subnet such
IP	or FQDN	192.168.110.21			W	S-RDS2			🛍 Delete
		192.168.100.16				S-RDS1			🛍 Delete
		🖺 Save 🕇 Add	Host						

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:

		System -	Interf	aces 🔻	Firewall 👻	Services 🗸	VPN 👻	Status 🕶	Diagnostics	· ▼ Hel	p -	¢
Fire	wall /	Rules /	LAN_1	10_CLIE	NTS							‡ iii 🖬 🛛
The fi The c	rewall rule hanges m	configurations to configurations to configurations to configurations and configurations are configurated as a c	on has been ed for them t	changed. to take effec	t.							✓ Apply Changes
Float	ing [OMZ_120_E>	CTERN	LAN_100_S	SERVER	DMZ_130_INTERN	LAN_1	10_CLIENTS	DMZ_140)_GAMEZON	IE DMZ_15	0_ISOLATION
Rule	s (Drag	to Chang	e Order)									
	State	s Pr	otocol	Source	Port	Destination	Port	Gate	way Queue	Schedule	Description	Actions
	0 / 0	B IF	Pv4 TCP	*	*	ServerIn_RDS	Ports_F	RDS *	none		Zugriff auf RDS	≟∥⊡⊘ ≞

<u>Troubleshooting – Problem "RD-Gateway"</u>

VS IT-Solutions

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:

🛈 🔒 https	://docs.microsoft.com/de-de/windows-server/remote/remote-desktop-services 🛛 🔛 😒 🟠
	Voraussetzungen für das Einrichten des Webclients
^	Beachten Sie vor dem Ausführen der ersten Schritte die folgenden Punkte:
ndows	 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
en einer	 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.
lesktop- iutzer	 Stellen Sie sicher, dass alle Computer, mit denen Ihre Benutzer eine Verbindung herstellen, unter einer der folgenden Betriebssystemversionen ausgeführt werden: Windows 10
utzer	 Windows Server 2008 R2 oder h
ellung	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:



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

```
$BrokerCertThumprint = (Get-RDCertificate -Role RDRedirector).Thumbprint
$BrokerCertThumprint
netsh http show sslcert
```

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



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

			1 Romoto	docktor	dionsto Bor	aitstallu
🚡 Server d	es Typs "RD-Gateway	" hinzufügen			-	
Wähl	en Sie eine	n Server aus.				
Serve SSL-Z Bestär Ergeb	rauswahl ertifikatname igung nisse	Mit diesem Assisten Wählen Sie die Serv Serverpool Filter: Name WS-RDS1.ws.its	ten können Sie der Berei er aus, auf denen der Rol IP-Adresse 192.168.100.16	itstellung Server Ilendienst "RD-G	vom Typ "RD-Gateway" I Gateway" installiert werde Ausgewählt Computer WS-RDS1	ninzufügen. n soll.
		 Computer gefund Die Anmeldein verwendet 	en formationen des WS\stej	>	1 Computer ausgewäh werden zum Hinzufügen	lt 1 der Server

🛓 Server des Typs "RD-Gateway" hinzufügen 🛛 — 🗆 🗙						
Selbstsigniertes S	SL-Zertifikat benen	nen				
Serverauswahl SSL-Zertifikatname Bestätigung Ergebnisse	SSL-Zertifikate dienen zum Versa Clients und Remotedesktopgate dem vollqualifizierten Domänen Gatewayservers entsprechen. SSL-Zertifikatname (externen FQ rdsweb.ws.its Der FQDN muss dem Namen de Remotedesktopdienste-Client ver	chlüsseln der Kommunikation zwis way-Servern. Der Name des selbst namen (Fully Qualified Domain Na <u>DN des RD-Gatewayservers verwe</u> s Remotedesktop-Gatewayservers erwendet wird.	chen Remotedesktoj signierten SSL-Zerti me, FQDN) des Rem nden): entsprechen, der vo	pdienste- fikats mu notedeskt	:5 op-	
		< Zurück Weiter >	Hinzufügen	Abbrech	en	

Noch belasse ich es bei dem internen Zertifikat.

🚡 Server des Typs "RD-Gateway" h	inzufügen		- 🗆 ×
Status anzeigen	Der Rollendienst wird auf den folg	jenden Servern installiert:	
SSL-Zertifikatname	Server	Status	Status
Ergebnisse	Remotedesktopgateway (Rolle WS-RDS1.ws.its	ndienst)	Erfolgreich
	 Die Bereitstellung wurde so k Für die folgenden Rollendien Zertifikat konfigurieren RD-Gatewayeigenschaften für die 	onfiguriert, dass rdsweb.ws.its für sie ste muss ein Zertifikat konfiguriert v Bereitstellung prüfen	e verwendet wird. verden:
		< Zurück Weiter >	Schließen Abbrechen

📥 Bereitstellungseigenschaften \times Bereitstellung konfigurieren Daten werden gespeichert... Alle anzeigen Remotedesktopga... + Linem bestimmten Rollendienst kann jeweils nur ein einzelnes Zertifikat hinzugefügt werden. Wenn Sie weiteren Rollendiensten Zertifikate hinzufügen Remotedesktopliz... + möchten, klicken Sie auf "Übernehmen" oder "OK". Web Access für Re... + Die aktuelle Zertifikatsstufe der Bereitstellung ist Nicht konfiguriert Zertifikate Was ist eine Zertifikatsstufe? Rollendienst Stufe Status Status Remotedesktop-Verbindungsbroker Vertrauenswürdig OK Remotedesktop-Verbindungsbroker Vertrauenswürdig OK Web Access für Remotedesktop Vertrauenswürdig OK RD-Gateway Kann ang Nicht konfiguriert Antragstellername: Nicht verfügbar 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 OK Abbrechen Anwenden

VS IT-Solutions

Die Konfiguration braucht einen weiteren Testlauf. Das Ergebnis ist aber unverändert. In der Anleitung von Microsoft steht, der RD-Gatewayservice 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:

aten werden gespeichert Alle anzeigen Remotedesktopga +	Zertifikate verwalten								
Remotedesktopliz + Web Access für Re +	Für eine Remotedesktopdienste-Bereit	stellung sind Zertifika	ate für die Ser	verauthentifizierung, einmali	iges Anmelden und F	Herstellen von sicherer	n Verbindungen erforde	lich.	,
	"Übernehmen" oder "OK". Die aktuelle Zertifikatsstufe der Bereits	tellung ist Vertrauen	swürdig						
	Was ist eine Zertifikatsstufe?		Swarang						
	Was ist eine Zertifikatsstufe?	Stufe	Status	Status					
	Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker	Stufe Vertrauenswürdig	Status OK	Status					
	Was ist eine Zertrifikatsturfe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker	Stufe Vertrauenswürdig Vertrauenswürdig	Status OK OK	Status					
	Wasiste ine Zertifikasstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway	Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig	Status OK OK OK OK	Status Kann angewendet wer Warnung					

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

Daten 25], ws 192.168 vs-dc1 vs-dc2	s-dc1.ws.its., 3.110.21 we its	hostm	Zeitster Static
25], ws 192.168 vs-dc1 vs-dc2	s-dc1.ws.its., 3.110.21 ws.its	hostm	Static
92.168 vs-dc1 vs-dc2	3.110.21		
vs-dc1 vs-dc2	we ite		Static
vs-dc2	10021121		Static
	.ws.its.		Static
vs-dc3	.ws.its.		Static
?	×		
	_		
нммз	55)		
	557		
Demeh	hmen		
	? 	! X	! X

<u>Troubleshooting – Problem "Authentifizierung"</u>

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:\Wind	ws\System32\Winevt\Logs\Microsoft-Windows-NTLM%4Operational.evtx -MaxEvents 20 -ErrorAction SilentlyContinue
4 Select-Object -Propert	v @{ n='DC' : e={ \$env:COMPUTERNAME } }}.
6 n='Datetim	' : e={ (Get-Date - Date \$ TimeCreated - Format u) - replace 'z'
6 Of n='Client'	, e-{ ((f. Marshare -shift ")n" - salit (f. Salits thing 'Achaits things ame') -salit '(')[1] thim() } }
et la crienc	, e-(((f
/ et a 'Densia'	; e={ ((5
8 @{ n= Domain	; e={ ((3message -spirt n select-string Domanenname) -spirt ;)[1].trim() } },
9 @{ n= User	; e={ ((\$Message -split " n" select-string "Benutzername") -split ':')[1].trim() } }
10 [} Sort-Object -Property Date	et me
11 Format-Table -Property DC	,Datetime,Client,Server,Domain,User
	When we set all the set of the se
WS-DC1 2019-09-16 05:17:32 \\WS-MON	MS-NAS1 ws system
WS-DC3 2019-09-16 06:50:36 WS-ATA	NS-F13 ws its convice-ata
WS-DC3 2019-09-16 11:07:40 WS-MON	MS-C13 we evendm
WS DC3 2019-09-10 11:07:40 WS HON	NGCL3 NG System
WS-DC3 2019-09-16 11:07:40 WS-MON	WS-CLS WS System
WS-DC3 2019-09-16 11:07:40 WS-MUN	WS-CL5 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-RD51 ws stephan
WS-DC1 2019-09-16 19:45:42 NULL	WS-RDS1 wsstephan
WS-DC1 2019-09-16 19:47:19 NULL	WS-RD51 wsstephan
	no host no scephan

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:



Gruppenrichtlinienverwaltungs-Editor		
Datei Aktion Ansicht ?		
🗢 🔿 🔀 🔀 🖼 🕞		
GPO-Computer-Sicherheit-NoNTLM [WS-DC1.WS.ITS] Ricl	Richtlinie	Richtlinieneinstellung
🗸 擾 Computerkonfiguration	🐻 Konten: Gastkontenstatus	Nicht definiert
✓	Konten: Gastkonto umbenennen	Nicht definiert
> Softwareeinstellungen	Konten: Lokale Kontenverwendung von leeren Kennwörtern	Nicht definiert
V Windows-Einstellungen	Konten: Microsoft-Konten blockieren	Nicht definiert
Namensautiosungsrichtlinie	Microsoft-Netzwerk (Client): Kommunikation digital signier	Nicht definiert
Skripts (start/Herunterranren)	Microsoft-Netzwerk (Client): Kommunikation digital signier	Nicht definiert
Sicherheitseinstellungen	Microsoft-Netzwerk (Client): Unverschlüsseltes Kennwort an	Nicht definiert
Schemeissenstellungen	Microsoft-Netzwerk (Server): Clientverbindungen aufheben,	Nicht definiert
V 🗟 Lokale Richtlinien	Microsoft-Netzwerk (Server): Kommunikation diaital signier	Nicht definiert
> 🗃 Überwachungsrichtlinie	Microsoft-Netzwerk (Server): Kommunikation diaital signier	Nicht definiert
> Zuweisen von Benutzerrechten	Microsoft-Netzwerk (Server): Leerlaufzeitspanne bis zum An	Nicht definiert
> Sicherheitsoptionen	Microsoft-Netzwerkserver: Es wird versucht, mit S4U2Self An	Nicht definiert
> 📑 Ereignisprotokoll	Microsoft-Netzwerkserver: SPN-Zielnamenüberprüfungsstuf	Nicht definiert
> 🔀 Eingeschränkte Gruppen	Retzwerksicherheit: Abmeldung nach Ablauf der Anmeldez	Nicht definiert
> 🙀 Systemdienste	Netzwerksicherheit: Beschränken von NTLM: Ausgehender	Nicht definiert
> 済 Registrierung	Retzwerksicherheit: Beschränken von NTLM: Eingehenden	Nicht definiert
> 済 Dateisystem	Netzwerksicherheit: Beschränken von NTLM: Eingehender N	Nicht definiert
> 📷 Richtlinien für Kabelnetzwerke (IEEE 802.:	Netzwerksicherheit: Beschränken von NTLM: NTLM-Authen	Alle verweigern
> 🧮 Windows-Firewall mit erweiterter Sicherh	Netzwerksicherheit: Beschränken von NTLM: NTLM-Authen	Alle aktivieren
Netzwerklisten-Manager-Richtlinien	Detzwerksicherheit: Beschränken von NTLM: Remoteservera	Nicht definiert
> and Drahtlosnetzwerkrichtlinien (IEEE 802.11)	Netzwerksicherheit: Beschränken von NTLM: Serverausnah	WS-RDS2,WS-RDS2.ws.its,WS-H
Richtlinien für öffentliche Schlüssel	Netzwerksicherheit: Für Kerberos zulässige Verschlüsselungs	Nicht definiert
Richtlinien f ür Softwareeinschr änkung	Netz	2
Anwendungssteuerungsrichtlinien	Eigenschaften von Netzwerksicherheit: Beschränken von	f X
Enveiterte Überwachungsrichtlinienkonfi	Netz Sicherheitsrichtlinie, Erkläning	
Richtlinienbasierter OoS	like Netz	
Administrative Vorlagen: Vom Jokalen Computer	Netz Netzwerksicherheit: Beschränken von NTLM: Ser	verausnahmen
> 📔 Einstellungen	Netz In dieser Domane ninzurugen	
V 🥵 Benutzerkonfiguration	Di Netz	
> 📋 Richtlinien	₩ Netz Diese Richtlinieneinstellung in der Vorlage definieren	
> 🚞 Einstellungen	WS-MX1.ws.its WS-MX2.ws.ite	^
	WS-MX1	
	WS-MX2	
	WS-RDS1 WS-RDS1.ws.its	*
	💹 Netz 🧹	>
	💹 Neta	

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:

🔁 Bereitstellungseigenschafte	en		- []	\times	
Bereitstellung k	onfig	gurieren				
Alle anzeige	en l					
Remotedesktopga	ᡖ Vorl	nandenes Zertifikat auswählen			×	
Remotedesktopliz						
Web Access für Re	Sie können das momentan auf dem RD-Verhindungsbrokerserver gespeicherte Zertifikat anwenden oder ein anderes Zertifikat in					
Zertifikate -	eine	PKCS-Zertifikatsdatei auswählen.				
	04	uf dem RD-Verbindungsbrokerserver gespeichertes Zertifikat anwenden				
	k	(ennwort:				
	• A	nderes Zertifikat auswählen				
	2	Zertifikatpfad:				
		C:\Users\stephan-T1\Desktop\2019-09-18-rdsweb_ws-its_de.pfx	Durch	suche	n	
	ŀ	kennwort:				
		•••••				
		inzufügen des Zertifikats zum Zertifikatsgeicher "Vertrauenswürdige Stammzertifizierungsstellen" auf den Zi	elcompute	ern 7u	lassen	
			licomput		iossen	
	·					
		OK		Abbre	chen	
		OK Abbreche	n Anv	vende	n	

					_	
Bereitstellung kon	figurieren					
Alle anzeigen Remotedesktopga	Zertifikate verwalten					
Remotedesktopliz +	Zer linkale ver walleri					
Web Access für Re +	Für eine Remotedesktopdienste-Bereit	stellung sind Zertifika	ate für die Se	erverauthentifizierung, ein	imaliges Anme	lden und
Zertifikate –	Finance bestimmten Pallandiaset la	errordenich.			Ween Cin unit	
	Rollendiensten Zertifikate hinzufüg	en möchten, klicken	Sie auf "Übe	rnehmen" oder "OK".	wenn sie weit	eren
	Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	tellung ist Vertrauen	swürdig			
	Rollendienst	Stufe	Status	Status		
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK			
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK			
	Web Access für Remotedesktop	Vertrauenswürdig	OK	Kann angewendet	werden	
	Actorectellergener Eliteration@usite	CNL adamaticum its C		TT Caludiana I. Faraldal	and C Davias	C . D.
	Antragstellername: E=itservice@ws.its, Details anzeigen	CN=rdsweb.ws.its, C	U=IT, O=WS	5 IT-Solutions, L=Ergolds	bach, S=Bayern	, C=DE
	Auf dem Server sind sowohl der Ro installiert. Für diese Rollendienste	ollendienst "RD-Gatev sollten keine untersch	way" als auch niedlichen Ze	n der Rollendienst "Web A ertifikate konfiguriert werd	Access für Remo den.	otedeskt
	Dieses Zertifikat ist für die Aktivierung Serverauthentifizierung für Web Acces	des RemoteApp- und s für Remotedesktop	d Desktopver erforderlich	rbindungsabonnements u	und für die	
	Sie können dieses Zertifikat aktualisien auswählen.	en, indem Sie ein neu	es Zertifikat	erstellen oder ein vorhan	idenes Zertifika	t
	Neues Zertifikat erste	llen		Vorhandenes Zertifik	at auswählen	
				ΟΚ Α	bbrechen	Anwend
a Bereitstellungseigenschaften				ΟΚ Α	lbbrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon	figurieren			OK A	Abbrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga +	figurieren Zertifikate verwalten			ΟΚ Α	Abbrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re +	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen	stellung sind Zertifika erforderlich.	te für die Se	OK A	Nobrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	stellung sind Zertifika erforderlich. tellung ist Vertrauen	te für die Se swürdig	OK A	Nobrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe	ste für die Se swürdig Status	OK A	Nobrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig	ste für die Se swürdig Status OK	OK A	Mobrechen	Anwend
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig	ste für die Se swürdig Status OK OK	OK A	Mobrechen	den und
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig	swürdig Status OK OK OK	OK A erverauthentifizierung, ein Status Erfolgreich	Mobrechen	den und
a Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig	swürdig Status OK OK OK OK	OK A erverauthentifizierung, ein Status Erfolgreich Erfolgreich	wbbrechen	Anwend
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-its. Details anzeigen	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Con	swürdig Status OK OK OK OK Trol Validated	OK A erverauthentifizierung, ein Status Erfolgreich Erfolgreich	Mobrechen	den und
Bereitstellungseigenschaften Bereitstellung kon Alie anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-its.J Details anzeigen Auf dem Server sind sowohl der Re	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Com	ste für die Se swürdig Status OK OK OK Trol Validated vay" als auch	OK A	Nobrechen	Anwend den und
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-its. Details anzeigen ▲ Auf dem Server sind sowohl der Ro installiert. Für diese Rollendienste s Dieses Zertifikat ist für die Serverauthe	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Con ollendienst "RD-Gatex sollten keine untersch ntifizierung für Verbii	ste für die Se swürdig Status OK OK OK trol Validated vay" als auch iedlichen Ze ndungen übe	OK A	Mobrechen	den und
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-itsJ Details anzeigen ▲ Auf dem Server sind sowohl der Ro installiert. Für diese Rollendienste s Dieses Zertifikat ist für die Serverauthe Sie können dieses Zertifikat aktualisierr auswählen. Wenn Sie dieses Zertifikat a neu starten.	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Con ollendienst "RD-Gatew sollten keine untersch ntifizierung für Verbii en, indem Sie ein neu sindern, müssen Sie d	ste für die Se swürdig Status OK OK OK OK trol Validated vay" als auch iedlichen Ze ndungen übe es Zertifikat en Remotede	OK A	Access für Remo den. y erforderlich. idenes Zertifika f allen RD-Gate	Anwend den und otedeskt: t t wwayserv
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-its.J Details anzeigen ▲ Auf dem Server sind sowohl der Re installiert. Für diese Rollendienste s Dieses Zertifikat ist für die Serverauthe Sie können dieses Zertifikat aktualisiere auswählen. Wenn Sie dieses Zertifikat ineu starten. Neues Zertifikat erstel	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Com ollendienst "RD-Gatev sollten keine untersch ntifizierung für Verbii en, indem Sie ein neu ändern, müssen Sie d	ete für die Se swürdig Status OK OK OK OK OK OK OK iedlichen Ze ndungen übe es Zertifikat en Remotede	OK A	Access für Remo Access für Remo den. In erforderlich. Idenes Zertifika f allen RD-Gate	Anwend den und otedeskt t
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	figurieren Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Herstellen von sicheren Verbindungen Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe? Rollendienst Remotedesktop-Verbindungsbroker Web Access für Remotedesktop RD-Gateway Antragstellername: CN=rdsweb.ws-its. Details anzeigen ▲ Auf dem Server sind sowohl der Ro installiert. Für diese Rollendienste s Dieses Zertifikat ist für die Serverauthe Sie können dieses Zertifikat aktualisiere auswählen. Wenn Sie dieses Zertifikat arstel	stellung sind Zertifika erforderlich. tellung ist Vertrauen Stufe Vertrauenswürdig Vertrauenswürdig Vertrauenswürdig de, OU=Domain Con ollendienst "RD-Gatev sollten keine untersch ntifizierung für Verbii en, indem Sie ein neu sindern, müssen Sie d len	ete für die Se swürdig Status OK OK OK OK trol Validatec vay" als auch iedlichen Ze ndungen übe es Zertifikat en Remotede	OK A	Access für Remo den. y erforderlich. idenes Zertifika f allen RD-Gate	Anwend den und otedeskt



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:

✓ ✓ ✓	Active Director
 > ☐ Zwischengespeicherte Lookupvorgänge ✓ ☐ Forward-Lookupzonen ☐ dmz.ws.its A 	Active Director
V 📋 Forward-Lookupzonen	ACTIVE DIRECTOR
A amazil una ita da	Activic Director
> 🛐 _msdcs.ws.its	Active Director
Assistent zum Erstellen neuer Zonen	×
Zonentyp Der DNS-Server unterstützt verschiedene Zonen- und Sneicherungstynen	- 100 A
Wählen Sie den Zonentyp aus, den Sie erstellen möchten:	
ws-	
WS- Erstellt eine Kopie einer Zone, die direkt auf diesem Server aktualisiert werde	en kann.
🔿 Sekundäre Zone	
Erstellt eine Kopie einer Zone, die auf einem anderen Server existiert. Mit die Option wird die Verarbeitungsmenge von primären Servern ausgeglichen und Enligteternen gewährlichtet.	eser d die
Stubzone	
Erstellt eine Kopie einer Zone, die nur Namenserver- (NS), Autoritätsursprun (SOA) und "Glue Host"- (A) Einträge enthält. Ein Server mit einer Stubzone is diese Zone nicht autorisierend.	ngs- st für
Zone in Active Directory speichern (DNS-Server muss als schreibbarer Domänencontroller eingerichtet sein)	
< Zurück Weiter > A	Abbrechen
DNS News	T
WS-DC1	тур
The second secon	Active Director
V Torward-Lookupzonen	Active Director
> 🛐 msdcs.ws.its 🛛 🔤 email.ws-its.de 🗸	Active Director
> Assistent zum Erstellen neuer Zonen	×
Active Directory Zananyanlikationsharaish	
Sie können festlegen, wie DNS-Daten im Netzwerk repliziert werden.	
>	
Vie sollen Zonendaten repliziert werden?	
 Auf allen DNS-Servern, die auf Domänencontrollern in der Gesamtstruktur aus werden: ws.its 	ısgeführt
WS O Auf allen DNS-Servern, die auf Domänencontrollern in dieser Domäne ausgefü werden: ws.its	führt
O Auf allen Domänencontrollern in dieser Domäne (Windows 2000-Kompatibilität	it): ws.its
 Auf allen Domänencontroller, die im Bereich dieser Verzeichnispartition angeg werden: 	jeben
	\sim
< Zurück Weiter > A	Abbrechen

-	DN	VS		Name	Тур
~	-	WS	-DC1	msdcs.ws.its	Active Directo
	>	<u> </u>	Zwischengespeicherte Lookupvorgänge	dmz.ws.its	Active Directo
	~		Forward-Lookupzonen	email ws-its de	Active Directo
		>	🛅 msdcs.ws.its		Active Directo
		>	Assistent zum Erstellen neuer Zonen		×
		>			-
		>	Zonenname		30
		>	Wie lautet der Name der neuen Zone?		1
		>			
	>		Der Zonenname bestimmt den Teil des l	DNS-Namesnaces, für den dieser Serv	er
	>		autorisierend ist. Normalerweise wird d	er Firmendomänenname (wie z. B. "mie	crosoft.com")
	=	WS	oder ein Teil des Domänennamens (wie	z. B. "neuezone.microsoft.com") verv	vendet. Der
	Ξ	WS	Zonenname ist nicht der Name des DNS	S-Servers.	
	_				
			Zonenname:		
			rdsweb.ws-its.de		
				< Zurück Weiter >	Abbrechen
	DN	NS.		Name	Turn
		ws	-DC1		чур
	7		7wischengesneicherte Lookunvorgänge	_msdcs.ws.its	Active Directo
	1		Ennuard Lookunzonen	📑 dmz.ws.its	Active Directo
	~		medes ws its	🛐 email.ws-its.de	Active Directo
		2	e msdcs.ws.its		
		2	Assistent zum Erstellen neuer Zonen		×
		>	Barran I. Januarya		-
		>	Sie köppen festlagen, dass diese DNS	Zana aichara, unaichara adar kaina	
		>	dvnamische Updates zulässt.	zone sichere, unsichere oder keine	
		>			
	>		Dynamische Updates ermöglichen DNS-	Clientcomputern, sich zu registrieren u	und die
	>		eigenen Ressourceneinträge dynamisc	h mit einem DNS-Server bei Änderunge	en zu
	Ξ	WS	aktualisieren.		
	Ξ	WS	Bestimmen Sie den Tvp des dvpamische	en Updates, der verwendet werden so	Ш.
	_			lassen (für Active Directory omefahler	1
			Diese Option ist nur für Active Direc	ctory-integrierte Zonen verfügbar.	v
			 Nicht sichere und sichere dynamisch 	ne Updates zulassen	
			Dynamische Updates von Kessourd	eneintragen werden von allen Clients :	zugelassen.
			vertrauenswürdigen Ouellen	an nones sichemeitsrisiko, da updates angenommen werden können.	von nicht
			Dynamische Updates nicht zulassen Dynamische Updates von Deserver	aneinträgen werden von dieser Zooo a	icht
			zugelassen. Diese Einträge müssen	manuell aktualisiert werden.	inci i t
					Although
				< zuruck Weiter >	Abbrechen

WS IT-Solutio	WSHowTo – Neuinstallation e 2019-09-10 Migration auf Wi	ines RDS mit HTML5 (WS-RDS1) ndows Server 2019
orgänge	(identisch mit übergeordne Autoritätsursprung (SOA) [1], ws-dc1 (identisch mit übergeordne Namenserver (NS) ws-dc1.ws	Lws.its., hostma Static .its. Static
	Neuer Host X Name (bei Nichtangabe wird übergeordneter Domänenname verwendet):	
	Verknüpften PTR-Eintrag erstellen Authentifizierte Benutzer können DNS-Einträge mit demselben Besitzernamen aktualisieren Gültigkeitsdauer (TTL): 0 :0 :5 :0 (TTTTT:HH.MM.SS) Host hinzufügen Abbrechen	

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:

Alle anzeigen Remotedesktopga Remotedesktopliz + Web Access für Re + Zertifikate + Desse Einstellungen für die Bereitstellung angeben O Eise Einstellungen für den RD-Gatewayserver verwenden: Servername: rdsweb.ws-its.de Anmeldemethode: Kennwortauthentifizierung RD-Gatewayserver für lokale Adressen umgehen Remotedesktop-Gatewayserver verwenden	Bereitstellung konf	igurieren	
	Alle anzeigen Remotedesktopga Remotedesktopliz Web Access für Re Zertifikate	Remotedesktopgateway RD-Gatewayeinstellungen für die Bereitstellung angeben Aemotedesktop-Gatewayservereinstellungen automatisch ermitteln Diese Einstellungen für den RD-Gatewayserver verwenden: Servername: rdsweb.ws-its.de Anmeldemethode: Kennwortauthentifizierung RD-Gatewayanmeldeinformationen für Remotecomputer verwenden Remotedesktop-Gatewayserver für lokale Adressen umgehen Keinen RD-Gatewayserver verwenden	~

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.



WS IT-Solutions

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.wsits.de:

🔋 WS-RA1 🗙 🔋 WS-RA2			
🏪 🛃 📙 🔫 SYSTEM (C:)			
Datei Start Freigeben	Ansicht		×
← → × ↑ 🐂 > Dieser PC	> SYSTEM (C:)	🗧 🐓 Zertifikatimport-Assistent	
📌 Schnellzugriff 🛄 Desktop	▲ Nar	Zu importierende Datei	
🕂 Downloads	*	Geben Sie die Datei an, die importiert werden soll.	
 Dokumente Bilder Active Directory Admin System32 Desktop Walther, Stephan - T1 Dieser PC SYSTEM (C:) Freigaben (M:) Bibliotheken Netzwerk 	*	Dateiname: C:\2019-09-18-rdsweb_ws-its_de.pfx 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)	
😰 Systemsteuerung			
Alle Systemsteuerungselen	nente		_
Senutzerkonten		Weiter Abbrechen	
E Darstellung und Annassung	a		

Seite 41 von 64



a state of the sta	
er private Schlüssel wurde mit einem Kennwort geschützt, um die Sic ewährleisten.	herheit zu
eben Sie das Kennwort für den privaten Schlüssel ein.	
ennwort:	
•••••	
Kennwort anzeigen	
nportoptionen:	
Hohe Sicherheit für den privaten Schlüssel aktivieren. Wenn Sie aktivieren, werden Sie immer dann, wenn der private Schlüssel Anwendung verwendet wird, zur Kennworteingabe aufgeforder	diese Optior von einer t.
Schlüssel als exportierbar markieren. Dadurch können Sie Ihre S einem späteren Zeitpunkt sichern bzw. überführen.	chlüssel zu
Alle erweiterten Eigenschaften mit einbeziehen	

	í.	1		1	
Name	Anderungsdatum	Тур		Größe	
Admin	03.08.2019 12:23	Dateiordner			
Benutzer	17.06.2017 04:46	Dateiordner			
📑 inetpub	16.06.2017 08:57	Dateiordner			
PerfLogs	16.03.2018 05:44	Dateiordner			
Program Files (x86)	16.06.2017 08:57	Dateiordner			
- Programme	16 06 2017 00.57	Detainedeas			
Windows	Zertifikatimport-Assistent	×			
3 2019-09-18-rdsweb_ws-its_	d		nati	5 KB	
	Der Importvorgang war er	folgreich.			
		OK			

Nun kann die neue Anwendung veröffentlicht werden:

💐 Remotezugriffs-Verwaltungskonsole						- 0	x c
Konfiguration VPN	VERÖFFENT Alle veröffentli	LICHTE WEBANWENDUNG chten Webanwendungen 3 insg	GEN gesamt			> Aufgaben Allgemein	^
Webanwendungsproxy Dashboard	Filter	م			۲	Veröffentlichen Aktualisieren	
Vorgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung		Monitor	^
💻 Remoteclientstatus	Monitor	https://	https://	PassThrough	1	Bearbeiten	a war th
Berichterstellung Gustenenver WS-RA1 WS-RA2	MX RDS	https:// casus /	https://rds.ws-its.de/	PassThrough PassThrough		Entfernen	y veron

WS IT-Solutions

Vorauthentifizieru	INC MIT AD FS VERBUNDE adfs.ws.i
	5
Willkommen	Geben Sie die Vorauthentifizierungsmethode an:
Vorauthentifizierung	 Active Directory-Verbunddienste (Active Directory Federation Services, AD FS)
Bestätigung Ergebnisse	 Alle Internationauterter unanforderungen werden an den Verbindserver ungeleter. 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 ne	< Zurück Weiter > Veröffentlichen Abbreche euer Anwendungen MIT AD FS VERBUNDE
Assistent zum Veröffentlichen ne Veröffentlichungs	euer Anwendungen MIT AD FS VERBUNDE adfs.vs.i
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen	< Zurück Weiter > Veröffentlichen Abbreche euer Anwendungen einstellungen Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an.
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung	Zurück Weiter > Veröffentlichen Abbreche euer Anwendungen einstellungen Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name:
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu	< Zurück Weiter > Veröffentlichen Abbreche euer Anwendungen MIT AD FS VERBUNDE adfs.ws.i Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung	Veröffentlichen Abbreche euer Anwendungen euer Anwendungen MIT AD FS VERBUNDE adfs.ws.i Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt.
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	Veröffentlichen Abbrech euer Anwendungen euer Anwendungen MIT AD FS VERBUNDE adfs.ws. Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt. Externe URL: https://rdsweb.ws-its.de/ Externes Zertifikat: rdsweb.ws-its.de Yanzeigen
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	 < Zurück Weiter > Veröffentlichen Abbrech euer Anwendungen MIT AD FS VERBUNDE adfs.ws.i Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt. Externe URL: https://rdsweb.ws-its.de/ Externes Zertifikat: rdsweb.ws-its.de ✓ HTTP-zu-HTTPS-Umleitung aktivieren URL des Back-End-Servers:
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	Zurück Weiter > Veröffentlichen Abbrech euer Anwendungen MIT AD FS VERBUNDE adfs.ws. Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt. Externe URL: https://rdsweb.ws-its.de/ Externes Zertifikat: rdsweb.ws-its.de URL des Back-End-Servers: https://rdsweb.ws-its.de/
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	 < Zurück Weiter > Veröffentlichen Abbreche euer Anwendungen MIT AD FS VERBUNDE adfa.wa.i Geben Sie die Veröffentlichungseinstellungen für diese Webanwendung an. Name: RDSWEB Dieser Name wird in der Liste der veröffentlichten Webanwendungen angezeigt. Externe URL: https://rdsweb.ws-its.de/ Externes Zertifikat: rdsweb.ws-its.de ✓ Anzeigen WIT P-zu-HTTPS-Umleitung aktivieren URL des Back-End-Servers: https://rdsweb.ws-its.de/
Assistent zum Veröffentlichen ne Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück
Assistent zum Veröffentlichen na Veröffentlichungs Willkommen Vorauthentifizierung Veröffentlichungseinstellu Bestätigung Ergebnisse	< Zurück



Das war einfach:

💱 Remotezugriffs-Verwaltungskonsole							- 0	\times
👔 Konfiguration	< VERÖFFENT	LICHTE WEBANWENDUNGE	N			> Aufga	ben	
VPN Webanwendungsproxy	Filter	ncmen menanwendungen (* insges	amu		۲	Veröffentlichen		
Dashboard Vorgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung		Monitor		
Remoteclientstatus	Monitor	https://www.automatical.org	https://	PassThrough		Bearbeiten Basierend auf dieser Au	owendung ver	röff
📴 Berichterstellung	MX RDS	https://rds.ws-its.de/	https://tds.ws-its.de/	PassThrough PassThrough		Entfernen	initendung ven	
Clusterserver WS-RA1 WS-RA2	RDSWEB	https://rdsweb.ws-its.de/	https://rdsweb.ws-its.de/	PassThrough				

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

🙆 Remotedesktop-Webclient 🗙 🕂			- a ×
(←) → C ^a	dweb/webclient/	··· 🖂 🕁	III\ 🗊 💿 🔛 👎 ≡
🚺 DuckDuckGo 🗎 Devices 🗎 Links			
III Alle Ressourcen			
Datenschutzeinstellungen für verwaltete Ressourcen wurden von Ihre	r Organisation vorab festgelegt. Weitere Informationen		×
	Wird geladen		
	Anmelden		
	Panutzername		
	ws\stephan		
	Kennwort		
	Datenschutzrichtlinie Anmelde	n	
🚱 Remotedesktop-Webclient 🗙 🕂			- ð ×
← → C ^e ŵ	lweb/webclient/	··· 🖂 🕁	III\ 🛈 💿 💾 👎 ≡
🚺 DuckDuckGo 🛅 Devices 🛅 Links			
III Alle Ressourcen		∠ &	3 ••• Abmelden 🔨
Datenschutzeinstellungen für verwaltete Ressourcen wurden von Ihre	Organisation vorab festgelegt. Weitere Informationen		×
V Work Resources			
KDSWEB			
	<u>/!\</u> Auf lokale Ressourcen zugreifen		
	Der Remotecomputer soll auf folgende Ressourcen dieses Computers zugreifer	n	
	können:		
	Zwischenablage Drucker		
	Nicht mehr nach Verbindungen mit diesem Computer fragen		
	7 Jacob Atlant		
	Zolassen Addreche		

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

WS IT-Solutions

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 Micosoft 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:

	System -	Interf	aces -	Firewall -	Services -	VPN - S	tatus - Dia	agnostics -	Help 🗸		
Services	/ HAProx	ky / Ba	ckend ,	/ Edit						Co	≆ 🔟 🔳
Settings	Frontend	Backend	Files	s Stats	Stats FS	Templates					
Edit HAPro	xy Backeno	l server p	bool				_				
	Name	RDSWEB									
	Server list	Table									
			Mode	Name	Forwardto	Address	Port	Encrypt(SSL)	SSL checks	Weight	Actions
		⊔₺	active	WS-RDS1	Address+Port:	<mark>192.168.100</mark>	.16 443	no	no	10	e 🖉 🖉 🖉
		. 🕀									
		•		A							
		Field expl	anations:								

Nun kann ich das Frontend editieren:

WS IT-Solutions

	SC Sys	tem -	Interfaces	✓ Firewall ✓	Services -	VPN 🗸	Status 🗸	Diagnostics 🗸	Help 🗕		•
Services / HAProxy / Frontend Co 😤 🛄 🖬 😧											
Settings	Fronte	nd	Backend	Files Stats	Stats FS	Templates					
Primary	Shared	On	Advanced	Name	Descriptio	on Add	ress	Туре	Backen	d	Actions
□ <u></u> ‡		~		HTTPS-Proxy		172	2.19.120.120:44	43 ssl/http	ps HTTPS	G (default)	d
⊔₺		~		SMTP-Proxy		172	2.19.120.120:25	5 tcp	SMTP	(default)	e 🖞 🖉
										l Add 🔟 D	elete 💾 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:

COMMUNITY EDITION	✓ Interfaces	Firewall 🗕	Services -	VPN -	Status -	Diagnostics 🗸	Help 🗕		۵
Services / HAPro	xy / Frontend /	Edit						C @ ‡ Ш ≡	0
Settings Frontend	Backend Files	Stats	Stats FS	Templates					
Edit HAProxy Fronten	d								
Name	HTTPS-Proxy								
Description									
Status	Active				\checkmark				
Shared Frontend	☐ This can be used Use this setting to co All settings of which The frontend settings	to host a second nfigure multiple b only 1 can exist w ; will be merged in	or more websit backends/acce vill be hidden. nto 1 set of fro	te on the same sslists for a si ntend configu	PIP:Port combi ngle frontend. ation.	nation.			
External address	Define what ip:port co Table	ombinations to lis	sten on for inco	mming conne	ctions.				
	Listen address		Custom add	ress	Port		SSL Offloading	Advanced	Action
	Use custom a	ddress: ~	172.19.120	.120	443				D (
									>

WS IT-Solutions

WSHowTo – Neuinstallation eines RDS mit HTML5 (WS-RDS1) 2019-09-10 Migration auf Windows Server 2019

	NOTE: You must add a firewall rules pe If you want this rule to apply to another addresses on the first). Also note that i specify multiple ports, separate them w you would likely want to check the SSL-	rmitting access to the listen po IP address than the IP address f you are trying to redirect conr ith a comma (,). EXAMPLE: 80, offloading checkbox.	rts above. of the interface chosen al ections on the LAN select 8000 Or to listen on both 8	oove, select it the "any" opti 0 and 443 cr	here (you need to define on. In the port to listen to eate 2 rows in the table w	Virtual IP , if you want to 'here for the 443
Max connections	Sets the maximum amount of connecti	ons this frontend will accent	av he left empty			
		ons this nontend will accept, in				
Туре	ssl / https(TCP mode)		×			
	This defines the processing type of HAI Please note that for https encryption/d	Proxy, and will determine the av ecryption on HAProxy with a ce	ailabe options for acl cheorem rtificate the processing typ	ks and also s e needs to b	several other options. e set to "http".	
Default backend, acc	ess control lists and actions					
Access Control lists	Use these to define criteria that will be Table	used with actions defined belo	v to perform them only wh	en certain co	nditions are met.	
	Name	Expression		CS Not	Value	Actions
	□ 🕹 RDSWEB	Server Name Indication TLS	extension matches: ~		rdsweb.ws-its.de	D
	±					
Actions	Name Expression Backend1acl Host matches addHeaderAciSSL Client certificate val acl's with the same name will be 'comb For more information about ACL's pleas NOTE Important change in behaviour, s -acl's are no longer combined with logic -acl's alone no longer implicitly generate Use these to select the backend to use	Cl Not Value www.yourdomain.tld id see See HAProxy Documentation ince package version 0.32 al AND operators, list multiple e use_backend configuration. A or perform other actions like ca	Section 7 - Using ACL's acl's below where needed. dd 'actions' below to accor Illing a lua script, blocking	nplish this b	ehaviour. ests or others available.	
	Table		Parameters Co	dition acl na	mas	Actions
	Use Backend	~	See below R	SWEB		
	backend RDSWEB		L			
	T HTTPS					
	Example: RDSWEB					
	Action SMTP	Condi Rooka	ion			
	http-request header set New logformat	HEADER-ClientCertValid value: YES	aderAcl			
Default Backend	HTTPS		~			
	If a backend is selected with actions ab	ove or in other shared frontend	s, no default is needed and	l 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 "rdsweb.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:

WS IT-Solutions

	COMMUNITY EDITION	Firewall - Services -	VPN - Status - Diagnostics	✓ Help ✓	•	
Status /	' Dashboard					+ 0
System In	nformation 🖋 🖨 😒	Traffic Graphs	۶ 🗢 🛙	HAProxy		⊁⊖⊗
Name	WS-PFS1a.ws.its	DMZ_120_EXTERN	🔵 wan (in) 🛛 😑 wan (out)	Backend(s)/Server(s)	0	Otation
User	admin@192.168.110.21 (Local Database)			Server(s)	(cur/max)	Status /
Manalan			0.0	Client(s) addr.port	age/id	Actions
version	2.4.4-RELEASE-P3 (amdo4) built on Wed May 15 18:53:44 EDT 2019		• • • • • • • • • • • • • • • • • • •	RDSWEB_ipvANY	1 / 200	0
	FreeBSD 11.2-RELEASE-p10	· · ·	-200	WS-RDS1	1	
				109.41.192.198:10792	25s / 0x80250e400	-
	The system is on the latest version.		-400	HTTPS_ipvANY	3 / 200	
	Version information updated at Fri Sep 20 16:48:32			WS-RA1	3 4m40a / 0x80250aa00	0
	CEST 2019 💭		-600	109.41.192.198.23220	3m35s / 0x80242bc00	
Kernel PTI	Disabled	56:43 58:20	00:00 01:40 02:52	109.41.192.198:13552	3m26s / 0x80250e000	
Untime	26 Days 02 Hours 45 Minutes 04 Seconds	LAN 100 SERVER	🔵 lan (in) 🛛 😑 lan (out)	WS-RA2	0	0
opuno	20 Days 62 Hours 45 Minutes 64 Seconds			SMTP_ipv4	0 / 200	0
Current	Fri Sep 20 17:02:50 CEST 2019		500k	WS-MX1	0	Q
date/time			400k	WS-MX2	0	Ø

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:

→ ~ ↑ 🐯 > Systemsteuerung >	Alle Systemsteuerungselemente > RemoteApp- und Desktopverbindungen			~ Ö	Systemsteuerung durchsuchen	<i>م</i>
tartseite der Systemsteuerung		-	×			
Auf RemoteApp und Desktops 🤟	🐻 Auf RemoteApp und Desktops zugreifen					
	Geben Sie Ihre E-Mail-Adresse oder Verbindungs-URL ein					
	E-Mail-Adresse oder Verbindungs-URL:					
	https://rds.ws-its.de/rdweb/feed/webfeed.aspx		7			
	Beispiele: https://contoso.com https://contoso.com/api/feeddiscovery/webfeeddiscovery.aspx https://contoso.com/rdweb/feed/webfeed.aspx john@contoso.com					

Eine Anmeldung später werden die RemoteApps integriert:

← → × ↑ 🛂 > Systemsteue	erung > Alle System	nsteuerungselemente > RemoteApp- und D	lesktopverbindungen		~ Q	Systemsteuerung durchsuchen	٩
Startseite der Systemsteuerung				×			?
Auf RemoteApp und Desktops	🔶 🐻 Auf Ren	noteApp und Desktops zugreifen					
zugreifen		Windows-Sicherheit	×				
	Verbind	Mit den Anmeldeinforma	tionen konnte keine				
		Verbindung hergestellt w	erden.				
		Mit den zum Herstellen der Verbind verwendeten Anmeldeinformationen hergestellt werden. Geben Sie neue	ung mit rds.ws-its.de n konnte keine Verbindung Anmeldeinformationen ein.				
		ws\stephan					
		•••••	୕				
		Domäne: ws					
		Anmeldedaten speichern					
		Der Benutzername bzw. das Kennwo	ort ist falsch.				
			Sallaria de la contra de la con				



Ich starte testweise meine Outlook-RemoteApp:

III Alle Ressourcen				2	<u>نې</u>	 Abmelden	^
Papierkorb	RemoteApp App wird gestartet	- 🗆 X					
Windows Update	Outlook 2016 Remotesitzung wird konfiguriert	_					
abmelden	Details einblenden	At					
Sicherung							

Das sieht gut aus:

WS IT-Solutions

💈 Remotedesktop-Webclient 🗙 🕂					– a ×
(←) → C [*] ŵ (i) ≜ http	… ☑ ☆			o 😬 🏴 =	
O DuckDuckGo 🛅 Devices 🛅 Links					
III Alle Ressourcen 🛛 🗔 RDSWEB 🛛 🗙			2 🐵		Abmelden
0					
Papierkorb	🔂 🗇 💲 🔹 Posteingang - Stephan W., 🛛 🚽 🗆 🗙				
	Datei Start Senden/Empfangen Ordner Ansicht 🖓 Sie wünschen				
	- Antworten				
Windows Update	Neue Loschen Gebreiten Bernete Loschen Arbeiten Guiddsteps Versch Neu Löschen Arbeiten Quiddsteps Versch				
	▲ Favoriten Altuelles Postfach durchsuche Altuelles Postfach -			-	
	Posteingang 3 - Striphan Alle Ungelesen - Neuestes Element	1E			
abmelden	Posteingang - strephant@ju				
	Posteingang - stephan@wi service-mailing@ws-it !				
	▲ Stephan.Walther@nicht antworten@kund				
	Posteingang 3 Ihre Vodafone Kabel Deutsc 16:42				
Sicherung	Entwurfe service-mailing@ws-it !			-	
	Geher/Mo Flamanta 53 service-mailing⊚ws-it ! ■ 조 Ⅲ 炎 ···· Snort-Monitor 1437				
	Online mit Microsoft Exchange 🔲 🕸+ 10 %				

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, dass 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:

D410	Q Search for users, groups, application	is, or devices	sw stept	nan.waither ID:	Stephan Walther 🗸
Dashboard	Dashboard > Applications				
Policies	Applications				Protect an Application
Applications	Applications				
Protect an Application					
Users				Export V	search
2FA Devices	Name 🔺	Туре	Application Policy	Group Policies	
Groups					
Administrators	RD-Gateway	Microsoft RD Gateway			

Der Katalog bietet reichlich Auswahl:

DUƏ	Q Search for use	ers, groups, applications, or devices	👩 stephan.waither ID: 🍏 Stephan Waither 🗸
Dashboard	Dashboard > App	lications > Protect an Application	
Policies	Protect	an Application	
Applications	remotel	an Application	
Protect an Application	Temote		
Users			
2FA Devices	BOMGAR	Bomgar	Protect this Application Read the documentation C
Groups			
Administrators	_		
Reports		Microsoft RD Gateway	Protect this Application Read the documentation C
Settings			
Billing		Microsoft RD Web	Protect this Application Read the documentation of
Support			

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



	Search for u	users, groups,	applications, or d	levices			511	stephan.walt	her ID: 🗨		Stephan Walt	ther 🗸
Dashboard Policies	Successfully	added Micros	soft RD Web to p	rotected applica	ations. Add anoth	ner.						
Applications	Dashboard > A	pplications >	Microsoft RD Web									
Users	Micros	soft R	D Web						Authentical	ion Log f	Remove Appli	ication
2FA Devices	See the Micr	rosoft RD Wel	odocumentation	ocumentation of to integrate Duo into your RD Web App logins.								
Groups Administrators				, end								
Reports	Details										Reset Secret	Кеу
Settings	ntegration key				•	sel	ect					
Billing	Secret key		Click to view	,		sel	ect					
Support Upgrade your plan for support.			Don't write dow	n your secret key	or share it with anyor	ie.						
Account ID A	API hostname					sel	ect					
Deployment ID	Policv											
					2	-						
Product	Use Cases	s Pricin	g About	Partners	Resources	Docs	Support		Co	ntact Sales	Free Iri	al
Contents		Prere	quisites									
Overview		Make sur	e to complet	e these req	uirements be	fore insta	Illing Duo A	uthenticatio	n for RD W	/eb.		
Deployment Tip		1 Cheo	k your serve	er version. T	hese instruct	ions are	for installing	g Duo Authe	entication f	or RD Web	on Window	/S
First Steps		Serv	er 2012, 201	2 R2, 2016	, and 2019. If	you are	running Wi	ndows 2008	R2, see th	ne <u>RD Web</u>	2008 R2	
Test Your Setup		Instri	lctions.									
Updating Duo for RD Web Troubleshooting		2 Make	e sure you ha	ave installe	d .NET Frame	ework 4.5	. You can d	lo this, for e	xample, by	running th	e following	
Related		Pow	erShell comr	nands:								
≓∣ Duo Authentication for RDS Overview		Imp Ado	oort-Modul l-WindowsF	e Server Geature N	Manager ET-Framewo	rk-Core	2					
■ Duo Authentication for RD V RD Gateway 2012+	Web and	3 Also	make sure y	vou have ins	talled ASP.N	ET 4.5 sı	apport for II	S. The Pow	erShell cor	nmands fo	r this are:	
■ Duo Authentication for RD V RD Gateway 2008 R2	Web and	Imp	ort-Modul	le Server Teature N	Manager ET-Framewo	rk-45-7	ASPNET					
Duo Authentication for RD V 2012+ Only	Web	-Hac		LIVUIC N								
E Duo Authentication for RD V 2008 R2 Only	Web	4 Ensu	ire that the II	IS Manager	nent Scripts a	ind Tools	feature is t	urned on as	well. Pow	erShell exa	imple:	
■ Duo Authentication for RD G 2012+ Only	Gateway	Imp Ado	oort-Modul I-WindowsF	e Server Peature W	Manager eb-Scripti	ng-Tool	ls					
■ Duo Authentication for RD G 2008 R2 Only	Gateway											
RDS FAQ												
E Release Notes		Co Th re ra av	onnectivity his applicatio strict outbou nges aren't r vailability. If y	Requireme on communi- nd access t recommend rour organiz	nts cates with Du o Duo's servi ed, since thes ation requires	o's servic ce with ru se may cl s IP-base	ce on TCP iles using d hange over d rules, ple	port 443. Fir lestination II time to mai ase review	ewall confi P addresse ntain our s this Duo K	gurations t es or IP ado ervice's hig B article.	hat Iress Jh	

OK, ich prüfe die Voraussetzungen:







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

	Administrator Windows PouwsShell	- D X
	PS C:\Users\stephan-T1\Desktop> .\duo-rdweb-2.3.0.msi PS C:\Users\stephan-T1\Desktop>	^
duo-rdweb-2.3.0.msi	Duo Security Integration Details Duo Security Integration Details Enter the details of your Duo Security integration Integration Key: Secret Key: API Hostname:	
	Bypass Duo authentication when offline Use UPN username format Back Next Cancel	



<u>ک</u>	Administrator: Windows PowerShell	_	×
PS PS	C:\Users\stephan-T1\Desktop> .\ <mark>duo-rdweb-2.3.0.msi</mark> C:\Users\stephan-T1\Desktop>		^
duo-rdweb-2.3.0.msi	Duo Security Session Key Duo Security Session Key Configure your Duo Security session key Select whether to enter an existing session key or to generate a new one. If this IIS server is part of an application farm, all of the IIS servers in the farm should have the Duo integration installed, and all of these installations must share a session key. Session key: One Generate new session key One Generate new session key Back Next Cancel		

P P	Administrator: Windows PowerShell S C: \Users\stephan-T1\Desktop> .\duo-rdweb-2.3.0.msi S C: \Users\stephan-T1\Desktop>	
duo-rdweb-2.3.0.msi	Duo for Remote Desktop Web Access Setup — X Completed the Duo for Remote Desktop Web Access Setup Wizard Click the Finish button to exit the Setup Wizard.	
	Back Finish Cancel	

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



-							UUP				ш
Ausnahme	en extern										Ŵ
	18 /288.00 MiB	IPv4 UDP	ServerOut_UDF	P53 *	Devic	e_WS_Gate1	Ports_DNS	*	none	DNS-Forwarder erlaubt	±∥⊡0 ∎
	1 /4.84 MiB	IPv4 UDP	ServerOut_UDF	>53 *	Devic	e_WS_Gate2	Ports_DNS	*	none	DNS-Forwarder erlaubt	±∥⊡0 ∎
	0 /336 KiB	IPv4 UDP	ServerOut_UDF	2123 *	*		Ports_NTP	*	none	NTP erlaubt	±∥⊡0 ∎
	0 /8.39 MiB	IPv4 TCP	ServerOut_TCF	25 *	*		Ports_SMTP	*	none	SMTP erlaubt	±∥⊡0 ∎
	4 /1.51 GiB	IPv4 TCP	ServerOut_TCF	9443 *	*		Ports_HTTPS	*	none	HTTPS ins Internet erlaubt	±∥⊡0 ∎
	0 /14.54 GiB	IPv4 TCP	ServerOut_TCF	* 08	*		Ports_HTTP	*	none	HTTP ins Internet erlaubt	±∥⊡0 ∎
	0 /0 B	IPv4 UDP	ServerIn_WDS	Alias deta	ails	• 11	*	*	none	WDS Callback	±∕©0 ∎
	0 /267 KiB	IPv4 TCP	ServerOut_ DuoSecurity	Value 192.168.1	100.16	Description WS-RDS1	Ports_HTTPS	*	none	Zugriff DuoSecurity	±∥⊡0 ∎
	0 /2.39 MiB	IPv4 TCP	ServerOut_ MXServer	192.168.1	100.10	WS-HV2	Ports_HTTPS	*	none	MXUpdate HTTPS	±∥⊡0 ∎

Es sollte also alles funktionieren. Oder?

🚱 Remotedesktop-Webclient 🗙 🕂				– ø ×
(←) → C ^a			··· 🖂 🕁	👱 II\ 🗊 💿 🔛 🔻 🗏
O DuckDuckGo 🗎 Devices 🗎 Links				
III Alle Ressourcen				~ ~ ^
Datenschutzeinstellungen für verwaltete Ressourcen wurden von Ihrer Organisation vorab festgelegt	. Weitere Informationen			×
	Wird geladen			
	Anmelden			
	Ramidaan awa			
	ws\stephan	V		
	eren fremelierennen			
	Kennwort			
	•••••	•		
	Datenschutzrichtlinie	Anmelden		

🚱 Remotedesktop-Webclient 🛛 🗙 Web Access für Remotedesktop	× +	
← → C ŵ ① ♣ https://rdsweb.ws-it	s.de/RDWeb/webdient/	🖂 🖕 🔝 🐨 🗮 🗮 =
O DuckDuckGo 🛅 Devices 🛅 Links		
III Alle Ressourcen		
Datenschutzeinstellungen für verwaltete Ressourcen wurden vor	Ihrer Organisation vorab festgelegt. Weitere Informationen	· · · · · · · · · · · · · · · · · · ·
	* Wird geladen	
	Anmelden Berutzername ws/utrphan Konnwort ▲ fehier beim Anmelden. Überprüfen Sie ihren Berutzernamen und ih Konnwoft, und versuchen Sie ei dann noch mal. Daterschutzrichtlinise	

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:

instellungen	
û Startseite	Apps & Features
Einstellung suchen	Installationsquellen
pps	Wählen Sie aus, von wo Apps abgerufen werden können. Wenn Sie nur Apps aus dem Store installieren, tragen Sie dazu bei, dass Ihr PC geschützt ist und reibungslos funktioniert.
Apps & Features	App-Vorschläge deaktivieren $$
T Standard-Apps	
Apps für Websites	Apps & Features
¹ Autostart	Optionale Features verwalten
	Aliase für App-Ausführung verwalten
	Sie können nach Laufwerken suchen, sortieren und filtern. Wenn Sie eine App deinstallieren oder verschieben möchten, wählen Sie sie aus der Liste aus.
	Diese Liste durchsuchen
	Sortieren nach: Name $ \lor $ Filtern nach: Alle Laufwerke $ \lor $
	Duo for Remote Desktop Web Access 1,75 MB 20.09.2019
	2.3.0.188
	Ändern Deinstallieren

Ich versuche es mit der klassischen "Microsoft RDP"-Application:

NS IT-Solutions

DUO	Q Search for us	ers, groups, applications, or devices	stephan.walther ID: Stephan Wal	ther 🗸
Dashboard	Dashboard > App	lications > Protect an Application		
Policies	Protect	an Application		
Applications	remotel			
Protect an Application	Tenlotoq			
Users				
2FA Devices	BOMGAR	Bomgar	Protect this Application Read the documentation ⊑	
Groups				
Administrators				
Reports		Microsoft RD Gateway	Protect this Application Read the documentation [5	
Settings				
Billing		Microsoft RD Web	Protect this Application Read the documentation E	
	-			
Support Upgrade your plan for support.				
Account ID		Microsoft RDP	Protect this Application Read the documentation 🗗	
Deployment ID				

WS IT-Solutions

WSHowTo – Neuinstallation eines RDS mit HTML5 (WS-RDS1) 2019-09-10 Migration auf Windows Server 2019

Das Setup ist fast identisch mit dem ersten:

	還 Duo Authentication for Windows Logon x64 - InstallShield Wizard 🛛 🗙
	Duo Connectivity Check Please enter the hostname for your integration to verify connectivity
duo-win-login-4.0	API Hostname: This hostname can be found in the <u>Duo Admin Panel</u> under Applications, configure or
	select a Microsoft KDP application. Configure manual proxy for Duo traffic (Uses System settings if unspecified) Proxy Host: Proxy Port: Proxy Port:
	InstallShield < Back Next > Cancel

	🕼 Duo Authentication for Windows Logon x64 - InstallShield Wizard 🛛 🗙
	Duo Security Account Details
	Please enter the keys provided by Duo Security
	Integration Key:
duo-win-login-4.0	
	Secret Key:
	These keys can be found in the <u>Duo Admin Panel</u> under Applications, configure or select a Microsoft RDP application.
	Please refer to the Duo Windows Logon documentation for more information.
	InstallShield
	< Back Next > Cancel
	🖟 Duo Authentication for Windows Logon x64 - InstallShield Wizard 🛛 🗙
	Duo integration options
	Configure the integration below
	Bypass Duo authentication when offline (FailOpen)
duo-win-login-4.0	Enable this option to allow user logon without completing two-factor authentication if the Duo Security doud service is unreachable. If you plan to enable offline access with MFA consider disabling FailOpen to prevent un-enrolled users from logging in.
	✓ Use auto push to authenticate if available
	Automatically send a Duo Push or phone call authentication request after primary credential validation.
	✓ Only prompt for Duo authentication when logging in via RDP
	Leave this option unchecked to require Duo two-factor authentication for local logon and RDP sessions. If enabled, local logons do not require 2FA approval.
	Please refer to the Duo Windows Logon documentation for more information.

< Back Next >

Cancel

WS IT-Solutions



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:

🛃 Administrator: Windows PowerShell ISE
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe
Unbenannt1.ps1* ×
1 Set-RDWebClientDeploymentSetting -Name "SuppressTelemetry" <pre>\$true</pre>
2 Set-RDWebClientDeploymentSetting -Name "LaunchResourceInBrowser" <pre>\$true</pre>
PS C:\Windows\system32> Set-RDWebClientDeploymentSetting -Name "SuppressTelemetry" \$true
PS C+\Windows\system32\ Set_DDWebClientDenloymentSetting _Name "LaunchDesourceTnBrowser" \$true
rs C. (withdows (system) 22 set-towebc rient be royment setting - Name Laurent Resource introviser set ac
PS C:\Windows\system32>

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:



😰 Netzwerkverbindungen	
$\leftarrow \ ightarrow \ ightarrow \ ightarrow $	Internet > Netzwerkverbindungen
Organisieren 🔻 Netzwerkgerät deaktivieren Verbind	dung unterruchen Verbindung umbenennen Statuc der Verbindung anzeigen »
Ethernet ws.its Microsoft Hyper-V Network Adap	Image: Figureschaften von Ethernet × Netzwerk Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4) × Allgemein IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Bie sich andernfälls an den Netzwerk deninstrator, um die geeigneten P-Einstellungen zu beziehen. ● IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Bie sich andernfälls an den Netzwerkkadministrator, um die geeigneten P-Einstellungen zu beziehen. ● IP-Adresse automatisch beziehen ● Folgende IP-Adresse verwenden: IP-Adresse: 192 . 168 . 100 . 16 Subnetzmaske: Subnetzmaske: 255 . 255 . 05 Standardgateway: 192 . 168 . 110 . 252 DNS-Serveradresse automatisch beziehen ● Folgende DNS-Server: 192 . 168 . 100 . 1 Alternativer DNS-Server: 192 . 168 . 100 . 1 Alternativer DNS-Server: 192 . 168 . 100 . 1
1 Element 🔰 1 Element ausgewählt	Erweitert
	OK Abbrechen

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:

Virtuelle Computer			[Einstellungen f ür "WS-RDS1" auf "WS-HV	n. – – X
Name	Phase Gespeichert	CPU-Auslast	Zu	WS-RDS1 ~	< ► 0
WS-ATA WS-DC1 WS-FS1 WS-MX1 WS-PFS1a	Wird ausgeführt Wird ausgeführt Wird ausgeführt Wird ausgeführt Wird ausgeführt	3 % 0 % 0 % 3 % 1 %	301 301 101 102 512	Hardware Hardware hinzufügen Firmware Von 'Datel'' starten Siderheit Ladefehler	Vetzwerkkarte Konfigurieren Sie die Netzwerkkarte, oder entfernen Sie sie. Virtueller Switch: LAN-110,DMZ
WS-RAT WS-RDS1 WS-Steuer	Wird ausgeführt Wird ausgeführt Aus	0%	172	Arbeitsspeicher 2048 MB Zota MB Avituelle Prozessoren Avituelle Prozessoren SCSI-Controller E Festplatte HDD0-System.vhdx	VLAN-ID // Identifizierung virtueller LANs aktivieren Mithilfe der VLAN-ID wird das virtuelle LAN angegeben, das von diesem virtuellen Computer für die gesamte Netzwerkkommunikation über diese Netzwerkkarte verwendet wird. 110
				IVIC-RealeWelt LAN-110,DMZ Verwaltung Name We proct	Bandbreitenverwaltung Bandbreitenverwaltung aktivieren Geben Sie an, wie die Netzwerkbandbreite von diesem Netzwerkadapter

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

	COMMUNITY EDITION System - Interfac	es • Firewall • Services •	VPN - Status - Diagnostic	s∓ He	ielp 👻	•	
Status / Da	shboard						+ 0
System Inform	nation 🗲 🗢 🕄	Traffic Graphs	J.	• 🗢 😣	HAProxy		80 م
Name	WS-PFS1a.ws.its	DMZ_120_EXTERN	🔵 wan (in) 🛛 😑 wan (out)		Backend(s)/Server(s)	Sassions	Statue
User	admin@192.168.110.101 (Local Database)			2.01	Server(s)	(cur/max)	/
Version	2.4.4.DELEASE-p2 (amd64)			3.0K	Client(s) addr:port	age/id	Actions
Tersion	built on Wed May 15 18:53:44 EDT 2019			2.0k	RDSWEB_ipvANY	DOWN	0
	FreeBSD 11.2-RELEASE-p10			1.04	WS-RDS1	DOWN	0
				I.UK	HTTPS_ipvANY	0 / 200	e e e e e e e e e e e e e e e e e e e
	The system is on the latest version.			0.0	WS-RAT	0	ĕ
	Version information updated at Sun Oct 6 12:07:19 CEST 2019			4.0%	SMTD inve	0 / 200	
	0	01.02	05-00	-1.0K	WS-MX1	0/200	ĕ
Kernel PTI	Disabled	01:33 03.20	05.00 06.40	07:33	WS-MX2	0	õ
Uptime	19 Hours 08 Minutes 16 Seconds	LAN_100_SERVER	🔵 lan (in) 🛛 🔴 lan (out)	1451	Sport Alerts		600
Current date/time	Sun Oct 6 12:07:29 CEST 2019			10k	Interface/Time Src/Dst Addres	s Description	
Last config change	Sat Oct 5 12:31:53 CEST 2019			5.0k	DMZ_120_EXTERN 192.168.110.1 Oct 06 12:07:15 104.90.156.18	6:54828 ET USER_A 9:80 Device Met	GENTS Microsoft tadata Retrieval
0 I I				0.0			

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

T-Solution	ws 201	HowTo 19-09-10	– Neuin Migra	istallati tion au	ion ein f Wind	es RD lows S	S mit HTI erver 20	ML5 (\ 19	NS-RDS	1)
	C System -	- Interfaces -	Firewall 🗸	Services -	VPN -	Status 👻	Diagnostics 👻	Help 🛨		
Service	s / HAPro	xy / Backen	d						C®	£ III ■
Settings	Frontend	Backend F	Files Stats	Stats FS	Templates					
Backend	s Advanced		Name	Servers	s	Check	Frontend		Actions	
			SMTP	2		SMTP	SMTP-Proxy			e 1
□.₺			HTTPS	2		Basic	HTTPS-Proxy			e 1
			RDSWEB	1		Basic	HTTPS-Proxy			1
COMMUNITY EDITION	System -	Interfaces -	Firewall →	Services 🗸	VPN 🕶	Status 🕶	Diagnostics 🗸	Help 🔻	Co	후 교 🗉
Settings	Frontend	Backend F	Files Stats	Stats FS	Templates					
Edit HAP	roxy Backen	d server pool								
	Name	RDSWEB								
	Server list	Table	Neme		Forwardto	Address		Dent En	SSL	o Weight
		active	WS-RDS1		Address+Po	192.168	<mark>.110</mark> .16	443 C	нуµ((ЭЭС) СЛӨСК	10

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

COMMUNITY EDITION	ystem -	Interfaces 🕶	Firewall 👻	Services -	VPN 🗸	Status 🕶	Diagnostics -	Help 🛨		۵
Firewall / Ali	ases / IF)							[.iii]	0
IP Ports	URLs A	Ш								
Firewall Aliases	s IP									
Device_WS_PFS2	192.168.1	101.252, 192.168.1	11.252, 172.19	.121.252, 172.19	.131.252			Gerät WS-P	FS2 🔗	Û
Device_WS_RDS1	192.168.1	100.16						Server WS-	RDS1 🥏 🖉	<u>ش</u>
Device_WS_RDS2	192.168.1	10.21						Server WS-F	RDS2 🖋 1	۵.

WS IT-Solutions

WSHowTo – Neuinstallation eines RDS mit HTML5 (WS-RDS1) 2019-09-10 Migration auf Windows Server 2019

COMMUNITY EDITION	← Interfaces ← Firewall ←	Services - VPN -	Status 🕶 Diagnostics		()		
Firewall / Aliases	J Edit				0		
Properties							
Name	Device_WS_RDS1 The name of the alias may only consi	ist 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).						
Туре	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	192.168.110.16	WS	-RDS1				
	🖺 Save 🕂 Add Host						

Weitere Aliase warten auf die Editierung:

COMMUNITY EDITION	tem 👻 Interfaces	← Firewall ←	Services -	VPN 👻	Status 🕶	Diagnostics 🗸	Help 👻		¢
Firewall / Alia	ses / IP								<u>m</u> 6
IP Ports U	IRLs All								
Firewall Aliases I	Ρ								
ServerIn_HTTPS	192.168.100.18, 192.	168.100.7, 192.168.	100.17, 192.168.1	00.6, 192.16	8.100.23, 192.1	168.100.22, 1 92.168	.100.16	Services mit HTTPS	e 🖉
ServerIn_MXRemoting	192.168.100.3, 192.1	68.100.13						Server mit MX	e 🖉 🖉
ServerIn_Print	192.168.100.11, 192.	168.100.51						Services Print	e 🖉 🕯
ServerIn_RDS	192.168.110.21, 192.	168. <mark>100.16</mark>						Server mit RDS	e 🖉 🕯
ServerIn_SMB	192.168.100.11, 192.	168.100.12, 192.168	8.100.10, 192.168	.100.5, 192.1	68.101.2, 192.1	168.100.8, 192.168.1	100.41	Services SMB	e 🖉
ServerIn_WDS	192.168.100.4							Services WDS	e 🖉 🖉
ServerIn_WSUS	192.168.100.4							Services WSUS	e 🖉 🕯
ServerOut_Anywhere	192.168.99.99, 172.1	9.130.113						ServerOut Anywhere	e 🖉 🕯
ServerOut_DuoSecurity	192.168. <mark>100.16</mark> , 192.	168.100.9, 192.168.	100.10					Server mit DuoSecurity	e 🖉

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



Ein finaler Test von intern und extern war erfolgreich!

Zusammenfassung

NS IT-Solutions

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!