Inhalt

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

1. <u>Szenario</u>

IST-Zustand

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



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

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

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

Auf WS-RDS1 laufen einige zentrale Scripte über Tasks.

Soll-Zustand

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

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

Die alten Lizenzen sollen migriert werden.

<u>Migrationsweg</u>

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

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

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

2. Vorbereitung der Migration

Verschieben aller Lizenzen von WS-RDS1 auf WS-RDS2

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



Der Dialog ist einfach aufgebaut:



Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

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

Assistent zum Verwalten von Lizenzen	×
Informationen zum Quelllizenzserver Geben Sie die erforderlichen Informationen zum Quellizenzserver an.	9
Name oder IP-Adresse des Quelllizenzservers:	
m31u5 I]	
Der angegebene Quelllizenzserver ist im Netzwerk nicht verfügbar.	
Wählen Sie das Betriebssystem aus, unter dem der Quelllizenzserver ausgeführt wird:	
v	
Geben Sie die Lizenzserver-ID für den Quelllizenzserver ein:	
Weitere Informationen zum Suchen der Lizenzserver-ID	
< Zurück Weiter >	Abbrechen



	Assistent zu	m Verwa	lten von L	izenzen		x
Lizenzprogramm Wählen Sie das passo	ende Lizenzprogr	amm aus.				9
Jeder Client, von dem eine Verbindung mit einem Remotedesktop-Sitzungshostserver oder einem virtuellen Desktop in einer Microsoft Virtual Desktop Infrastructure hergestellt wird, muss eine gültige Lizenz haben. Wählen Sie das Lizenzprogramm aus, über das Sie die Lizenzen erworben haben.						
Lizenzprogramm:	Vollprodukt	erwerb			~	
Beschreibung:	Diese Lizenz oder bei eine Verpackung Client Licens	wird in vord manderen H ist möglicher e Pack" bez	efinierten Mer Händler erwor weise mit "M weichnet.	ngen im Einze ben. Diese icrosoft Windo	Ihandel ows	
Format und Pfad:	Die im Lizen: Das Format f alphanumeri:	zpaket entha ür die Lizenz schen Zahler	ltene Lizenzn nummer ist 5 n.	ummerist erfo Sätze à 5	orderlich.	
Beispiel:	1A2B3	1A2B3	1A2B3	1A2B3	1A2B3	
Stellen Sie sicher, dass die Vorgang fortsetzen.	Lizenzinformation	nen dem Bei	spiel entsprec	hen, bevor Si	ie den	
			< Zuri	ick We	eiter > A	bbrechen

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

Assistent zu	um Verwalten von I	izenzen	X
Lizenznummer Geben Sie die Lizenznummer ein. Sie f	finden die Nummer in der \	Verpackung.	9
Geben Sie die Lizenznummer für jede I Sie nach der Eingabe jeder Lizenznum Lizenznummer ist 5 Abschnitte à 5 alpł	Lizenz, die Sie erworben h 1mer auf "Hinzufügen". Da hanumerische Zahlen.	aben ein, und klicken Is Format für die	
Lizenznummer:		Hinzufügen	
Eingegebene Lizenznummem:	Status Ausstehend	Produkttyp Windows Server 2012	
<	III	>	
	Беар	Loschen	



A	ssistent zum Verwalten von Lizenzen	x
	Assistent zum Verwalten von Lizenzen Der Assistent zum Verwalten von Lizenzen wird abgeschlossen. Der Assistent zum Verwalten von Lizenzen wurde abgeschlossen. Status: Die angeforderten Lizenzen wurden migriert.	X
	< Zurück Fertig stellen Abbr	rechen

Das Ergebnis passt:

%	Remotedesktoplizenzierungs-Manager						
Aktion Ansicht ?							
🖃 🚔 Alle Server	Lizenzversion und -typ	Lizenzprogram	Gesamte Lizen	Verfügbar	Ausgestellt	Ablaufdatum	Schlüsselpaket
🖶 🐷 WS-RDS1	🖏 Windows 2000 Server - Integrierte TS-CAL vom Typ "Pro Gerät"	Integriert	Unbegrenzt	Unbegrenzt	0	Nie	2
	🖏 Windows Server 2012 - Installierte "Pro Benutzer"-RDS-CAL	Einzelhandel	50	50	0	Nie	7
	🖏 Windows Server 2012 - Installierte "Pro Benutzer"-RDS-CAL	Einzelhandel	50	50	0	Nie	6
Berichte							
E-Lo WS-RDS2							
Windows 2000 Server - Integr							
Windows Server 2012 - Install							
Windows Server 2012 - Install							
berichte							
1 1	1						

Entfernen aller Sammlungen zum Deinstallieren der RDS-Rollen

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



WS-H	V1 🔋 WS-HV2 🔋	WS-RDS1 × 🔋 WS-RDS2
4		Server-Manager
\mathbf{E}	∋• Server-N	∕lanager • Remotedesktop- dienste • Sammlungen •
	Übersicht Server Sammlungen RemoteApps RD-Session	SAMMLUNGEN Letzte Aktualisierung: 19.01.2017 19:29:27 Alle Sammlungen 2 insgesamt Filter
🔋 WS-H\	v1 🔋 WS-HV2 🔋 WS	-RDS1 × 🔹 WS-RDS2 Server-Manager
I ws-ht	v1 ∎ ws-Hv2 ⊡ ws	FRDS1 × I WS-RDS2 Server-Manager anager • Remotedesktop- dienste • Sammlungen •
VVS-HV	v1 🔹 ws-Hv2 💽 ws The server-Ma Übersicht	FRDS1 × WS-RDS2 Server-Manager anager • Remotedesktop- dienste • Sammlungen • Sammlungen • Letzte Aktualisierung: 19.01.2017 19:35:47 Alle Sammlungen 1 insgesamt
■ WS-HN	vı ∎ ws-нv2 ▣ ws → Server-Ma Übersicht Server Sammlungen	FRDS1 × WS-RDS2 Server-Manager anager • Remotedesktop- dienste • Sammlungen • SAMMLUNGEN Letzte Aktualisierung: 19.01.2017 19:35:47 Alle Sammlungen 1 insgesamt Filter • • • • • • • • • • • • • • • • • • •
	vı vı ws-Hvz i ws Server-Ma Übersicht Server Sammlungen RD-Session	RDS1 × WS-RDS2 Server-Manager anager Remotedesktop- dienste Sammlungen SAMMLUNGEN Letzte Aktualisierung: 19.01.2017 19:35:47 Alle Sammlungen 1 insgesamt Filter P E F F F F F F F F F F F F
8 ws+H	vi vs-Hv2 vs Server-Ma Übersicht Server Sammlungen RD-Session	SRDS1 × ■ WS-RDS2 Server-Manager anager • Remotedesktop- dienste • Sammlungen • SAMMLUNGEN Letzte Aktualisierung: 19.01.2017 19:35:47 Alle Sammlungen 1 insgesamt Fitter
WS+HY WS+HY I	vi vs-Hv2 i ws Server-Ma Übersicht Server Sammlungen RD-Session	SRDS1 × WS-RDS2 Server-Manager anager • Remotedesktop- dienste • Sammlungen • SAMMLUNGEN Letzte Aktualisierung: 19.01.2017 19:35:47 Alle Sammlungen 1 insgesamt Filter P E +

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

Entfernen aller nicht erforderlichen RDS-Rollen

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







Weiter geht es mit dem WebService von WS-RDS2:



6	Server vom Typ "Web Access für Remotedesktop" entfernen 📃 🗖 🗙
Wählen Sie Serverauswahl Bestätigung Ergebnisse	e einen Server aus. Mit diesem Assistenten können Sie Server vom Typ "Web Access für Remotedesktop" aus der Bereitstellung entfernen. Wählen Sie die Server aus, von denen Sie den Rollendienst "Web Access für Remotedesktop" entfernen möchten. Serverpool Filter: Name IP-Adresse Betrieb WS-RDS1.WS.ITS WS-RDS2.ws.its Computer Ausgewählt VS-RDS2.ws.its Computer ausgewählten Servern deinstallieren
	< Zurück Weiter > Entfernen Abbrechen

Dieses Feature benötigt bei der Deinstallation einen Neustart:

S	erver vom Typ "Web Ac	cess für Remotedesktop" entferner	
Status anzeigen			
Serverauswahl	Die folgenden Server wer	den entfernt:	
Bestätigung	Server	Status	Status
Ergebnisse	Web Access für Remote	edesktop - Rollendienst	
	WS-RDS2.ws.its	Neustart wird durchgeführt	In Bearbeitung
		< Zurück Weiter >	Entfernen Abbrechen



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

L		Server-Manager	
\mathbf{E}	€ Server-N	anager • Remotedesktop- dienste • Server	
	Übersicht Server Sammlungen	Verfügbarer Arbeitsspeicher 442,73 MB - 927,34 MB Filter P Image: Content of the second	
		Filter P Servername Name Typ Pfad WS-RDS2 Remotedesktopdienste Rolle Remotedesktopdienste WS-RDS2 Remotedesktop-Sitzungst WS-RDS2 Remotedesktop-Sitzungst WS-RDS2 Remotedesktoplizenzierur Kopieren nste\Remotedesktoplizenzierung WS-RDS2 Remotedesktoplizenzierung	
		ws-KDS2 kemotedesktopgateway konenciensi kemotedesktopgateway	

Nur der Lizenzserver verbleibt:

4	Assistent zum Entfernen von Rollen und Features
Serverrollen ent Vorbereitung Serverauswahl Serverrollen Features Bestätigung Ergebnisse	Assistent zum Entfernen von Rollen und Features
	Kennotedesktop-Virtualisterdingshost (Nicht installie Web Access für Remotedesktop (Nicht installie Remotezugriff (Nicht installiert) Volumenaktivierungsdienste (Nicht installiert) <

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

L	Assistent zum Entfernen von Rollen und Features	X
Entfernungsstatus	ZIELSERVER WS-RDS2.ws.its	t 5
Vorbereitung	Entfernungsstatus anzeigen	
Serverauswahl	1 Featureentfernung	
Serverrollen Features	Auf "WS-RDS2.ws.its" steht ein Neustart aus. Sie müssen den Zielserver neu starten, um das Entfernen von Features abzuschließen.	
Ergebnisse	Remotedesktopdienste Remotedesktopgateway Remotedesktop-Sitzungshost Remoteserver-Verwaltungstools Rollenverwaltungstools Tools für die Remotedesktopdienste Tools für Remotedesktopgateway Remotedesktop-Lizenzdiagnosetools	
	Sie können diesen Assistenten schließen, ohne die ausgeführten Aufgaben zu unterbrechen. Zeigen Sie den Aufgabenstatus an, oder öffnen Sie diese Seite erneut, indem Sie auf der Befehlsleiste auf "Benachrichtigungen" klicken.	
	< Zurück Weiter > Schließen Abbrecher	1

Der Server benötigt einen Neustart:

WS IT-Solutions

_					Server-Manage	er			
\mathbf{E}	Server-№	lanager •	Remote	edesktop- dier	nste • Server		• ©	Verwal	lten
ii ii	Übersicht Server Sammlungen	SERVI Alle Se	E R rver 2 insgesa	amt 🔅 🗸	. (₽) ►				
in ⊳ 11		Servername WS-RDS1	IPv4-Adresse	6	Verwaltbarkeit Online	Letztes Update 19.01.2017 19:37:34	Windows-Aktivierung 00252-80525-03846-AA561 (Aktiviert)		
III I⊗ III ▷ IN III ▷ IN		WS-RDS2	192.168 100 2	nt Rollen und Features hinzu Server neu starten Computerverwaltung Remotedesktopverbindur Windows PowerShell	Online - Neustart ausstehend fügen	19.01.2017 19:46:31	00252-80525-03846-AA561 (Aktiviert)		



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

<u> </u>	Assistent zum Entfernen von Rollen und Feature	s 🗖 🗖 🗙
Serverrollen entfer	nen	ZIELSERVER <mark>WS-RDS1</mark> .ws.its
Vorbereitung Serverauswahl Serverrollen	Wenn Sie installierte Rollen vom ausgewählten Server entfernen entsprechenden Kontrollkästchen. Rollen	möchten, deaktivieren Sie die Beschreibung
Features Bestätigung Ergebnisse	 Druck- und Dokumentdienste (Nicht installiert) Faxserver (Nicht installiert) Hyper-V (Nicht installiert) Metzwerkrichtlinien- und Zugriffsdienste Remotedesktopdienste Remotedesktoplizenzierung Remotedesktop-Sitzungshost Remotedesktop-Verbindungsbroker Remotedesktop-Virtualisierungshost (Nicht installiert) Web Access für Remotedesktop Remotezugriff (Nicht installiert) Volumenaktivierungsdienste (Nicht installiert) 	Web Access für Remotedesktop ermöglicht Benutzern über das Menü "Start" oder einen Webbrowser den Zugriff auf RemoteApp- und Desktopverbindung. RemoteApp- und Desktopverbindung bietet Benutzern eine angepasste Ansicht von RemoteApp-Programmen, sitzungsbasierten Desktops und virtuellen Desktops.
	< Zurück Weiter	> Entfernen Abbrechen
Entfernungsstatus	Assistent zum Entfernen von Rollen und Features	S ZIELSERVER WS-RDS1.ws.its
Vorbereitung	Entfernungsstatus anzeigen	
t Serverauswahl Serverrollen Features Bestätigung	Featureentfernung Auf "WS-RDS1.ws.its" steht ein Neustart aus. Sie müssen d Entfernen von Features abzuschließen.	den Zielserver neu starten, um das
n ures	Remotedesktopdienste Remotedesktop-Verbindungsbroker Remotedesktopgateway Remotedesktoplizenzierung Remotedesktop-Sitzungshost Web Access für Remotedesktop Remoteserver-Verwaltungstools Rollenverwaltungstools Tools für die Remotedesktopdienste	
en Ig	Sie können diesen Assistenten schließen, ohne die ausgef Zeigen Sie den Aufgabenstatus an, oder öffnen Sie diese Befehlsleiste auf "Benachrichtigungen" klicken.	tührten Aufgaben zu unterbrechen. Seite erneut, indem Sie auf der
(Auministrator)	< Zurück Weiter	> Schließen Abbrechen

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

Abschalten des alten Servers WS-RDS1

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

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

Jetzt kann der Server das Active Directory verlassen:

Systemeigenschaften	X			
Ändern des Computernamens bzw. der Dom 🗴				
Sie können den Namen und die Mitgliedschaft des Computers ändern. Anderungen wirken sich möglicherweise auf den Zugriff auf	outers im		System	
Netzwerkressourcen aus.		y ► System und Sicherheit ►	System v 🖒	Systemsteuerung dur
Computername:	er			
WS-RDS1		lasisinformationen übe	r den Computer anzeigen	
Vollständiger Computername:		Vindows-Edition		
W3 1103 1.W3.18		Windows Server 2012 R2 D	atacenter	
Weitere	ern	© 2013 Microsoft Corporat	ion. Alle Rechte 🗧 Wind	ows Server ²
Mitglied von		vorbehalten.		
U Domane:		vstem		
Arbeitsgruppe:		Prozessor:	AMD FX(tm)-6300 Six-Core Processor	3.49 GHz
		Installierter Arbeitsspeicher (RAM):	3,00 GB	
OK Abbrechen		Systemtyp:	64-Bit-Betriebssystem, x64-basierter P	rozessor
		Stift- und Toucheingabe:	Für diesen Bildschirm ist keine Stift- of	der Toucheingabe verfüg
OK Abbrechen	Übernehmen	instellungen für Computernan	nen, Domäne und Arbeitsgruppe	
		Computername:	WS-RDS1	😽 Einstel
Wartungscenter Windows Update		Vollständiger Computername:	WS-RDS1.ws.its	änderi
		Computerbeschreihung		

Systemsteuerung		
Explorer	Trennen	
Suchen	Abmelden	
Ausführen	Herunterfahren	
Herunterfahren oder abmelden	Neu starten	
Desktop		
Herunterfahren oder abmelden	Neu starten	

Die alte VM ist jetzt ausgeschaltet:

WS-HV1 WS-HV2 Hyper-V-Manager Datei Aktion Ansicht ? Hyper-V-Manager Patei	× 🛿 WS-DC1					
Hyper-V-Manager	Virtuelle Computer	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status
	WS_CA1	Wird ausgeführt	0 %	678 MB	28 00:23:58	
	WS-DC2	Wird ausgeführt	9%	1536 MB	28.00.26.27	
	WS-DPM	Wird ausgeführt	1%	3072 MB	12 22:46:26	
	WS-ES2	Wird ausgeführt	0%	1887 MB	12 11:20:49	
	WS-MX2	Wird ausgeführt	10 %	10240 MB	12.11:20:42	
	WS-RA2	Wird ausgeführt	0 %	1660 MB	28.00:24:56	
	WS-RDS1	Aus				
	WS-SQL2	Wird ausgeführt	0 %	1104 MB	28.00:25:28	
	WS-Steuer	Aus				
	WS-VMM	Wird ausgeführt	0 %	2314 MB	12.11:20:34	

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

🔋 WS-HV1 🗙 🔋 WS-HV2	🛛 WS-DC1					
Hyper-V-Manager						
Datei Aktion Ansicht ?						
🗢 🔿 🖄 📰 🛛 🖬						
Hyper-V-Manager	Virtuelle Computer					
	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status
	WS-ACAD	Aus				
	WS-CM1	Wird ausgeführt	0 %	3294 MB	11.10:47:27	
	WS-DC1	Wird ausgeführt	0 %	1536 MB	11.10:49:14	
	WS-FS1	Wird ausgeführt	0 %	1536 MB	11.10:48:44	
	🗧 WS-IPM	Wird ausgeführt	11 %	2450 MB	11.10:46:42	
	WS-MX1	Wird ausgeführt	5 %	10240 MB	11.10:47:47	
	WS-PFS1	Wird ausgeführt	0 %	1024 MB	6.22:48:56	
	🗧 WS-RA1	Wird ausgeführt	2 %	1530 MB	11.10:47:42	
	WS-RDS1	Aus				
	WS-RDS2	Wird ausgeführt	0 %	1024 MB	01:04:07	
	WS-SQL1	Wird ausgeführt	0 %	1354 MB	11.10:48:24	

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

				Active Directory-Benutzer und -Computer
Datei Aktion Ansicht ?				
🗢 🔿 🙋 📰 🔏 📋 🗙 🖬 🍳 🖻	🛛 🖬 🗏 🐮 👕 🖉	38		
Active Directory-Benutzer und -Compute Gespeicherte Abfragen	Name	Typ Bes	chreibung	
▲ W ws.its ▶ ■ Builtin ▶ ■ Computers ▶ ■ ForeignSecurityPrincipals ▶ ■ LostAndFound ▶ ■ Managed Service Accounts ▶ ■ Program Data ▶ ■ Vsstern ▶ ■ System ▶ ■ WS ▶ ■ Senutzer	WS-RDS2 Einer Grupp Namenszuc Konto aktiv Konto zurü Verschieber Verwalten Alle Aufgat Ausschneid Löschen Eigenschaf	er hinzutugen ordnungen ieren eksetzen h een ten		
 ▲ Clients ▶ a mit-Roaming ▶ a ohne-Roaming a RDS ▶ Exchange-Objekte ▶ G Gruppen ▲ Server ▶ Cluster 	Hilfe			

3. Aufbau der neuen RDS-Infrastruktur

Inbetriebnahme und Vorbereitung des neuen Servers WS-RDS1

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

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

WS IT-Solutions

Systemeigenschaften	×	
Ändern des Computernamens bzw. der Domäne 🛛 🗙]	reit → System → Č Systemsteuerung durchsuchen P
Sie können den Namen und die Mitgliedschaft des Computers ändem. Änderungen wirken sich möglicherweise auf den Zugriff auf Netzwerkressourcen aus.	Computers	über den Computer anzeigen
Computemame: WS-RDS1 Vollständiger Computername: WS-RDS1	oder	Datacenter poration. Alle Rechte H Windows Server [®] 2016
Weitere Mitglied von Domäne: ws.tsi Arbeitsgruppe: WORKGROUP OK Abbrechen	dem	AMD FX(tm)-6300 Six-Core Processor 3.49 GHz icher 1,16 GB 64-Bit-Betriebssystem, x64-basierter Prozessor be: Für diese Anzeige ist keine Stift- oder Toucheingabe verfügbar. ernamen, Domäne und Arbeitsgruppe WIN-L13LMENSOIT WIN-L13LMENSOIT
OK Abbrechen Arbeitsg	Übernehmen gruppe:	g: WORKGROUP
Windows-A Window Siehe auch	Aktivierung vs ist nicht akt	iviert. Microsoft-Softwarelizenzbedingungen lesen
Sicherheit und Wartung Produkt	t-ID: 00377-90	000-00001-AA000 💱 Windows aktivieren

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

Datei Aktion Ansicht ?			
🗢 🄿 📶 📋 🗐 🗟 🗟 🛙	1 🕺 🔌 🛅 🍸 🕹	2 (k)	
Active Directory-Benutzer und -Compute	Name 📩 📩	Тур	Beschreibung
Gespeicherte Abfragen	🖳 WS-RDS1	Computer	
⊿ 🙀 ws.its	🖳 WS-RDS2	Computer	
⊳ 🛗 Builtin			
Computers			
Domain Controllers			
ForeignSecurityPrincipals			
LostAndFound			
Managed Service Accounts			
Microsoft Exchange Security Grou			
Program Data			
System			
b Users			
⊿ III WS			
Denutzer			
A Clients			
A since Koaming			
▶ S Exchange-Objekte			

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

Installation der neuen RDS-Infrastruktur

WS IT-Solutions

Auf dem neuen Server starte ich den Bereitstellungsassistenten für RDS:

	Rollen und Features	-		2
nstallationstyp au	swählen Es sir	nd keine Serve	ZIELSER\ er ausgewä	/ER ihlt.
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted RD-Virtualisierungshost Bestätigung Fertigstellung	 Wählen Sie den Installationstyp aus. Sie können Rollen und Features auf einem at Computer oder auf einem virtuellen Computer oder auch auf einer virtuellen Fes Disk, VHD) im Offlinemodus installieren. Rollenbasierte oder featurebasierte Installation Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, Rollendienste und Installation von Remotedesktopdiensten Bei der Installation waren Rollendienste für die virtuelle Desktopinfrastruktur Infrastructure, VDI) erforderlich, um eine Desktopbereitstellung auf Basis eine oder einer Sitzung zu erstellen. 	ausgeführte stplatte (Vir I Features h (Virtual Des s virtuellen	en physise tual Harc ninzufüge sktop Comput	n.
lard-Bereitstellung genü	< Zurück Weiter > Bere	itstellen	Abbrech	ıen
lard-Bereitstellung genü Assistent zum Hinzufügen von F Sereitstellungstyp	< Zurück Weiter > Bere gt: Rollen und Features auswählen Es sir	itstellen 	Abbrech	ver ihlt.
ard-Bereitstellung genü Assistent zum Hinzufügen von R ereitstellungstyp Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted	 Zurück Weiter > Bere gt: Rollen und Features auswählen Es sin Die Remotedesktopdienste können auf mehreren Servern oder nur auf einem Se werden. Standardbereitstellung Bei einer Standardbereitstellung können die Remotedesktopdienste auf mehr bereitgestellt werden. Schnellstart Ein Schnellstart bietet Ihnen die Möglichkeit, Remotedesktopdienste auf eine bereitgestellt werden. 	itstellen (Abbrech	VEF

< Zurück

Weiter >

Bereitstellen Abbrechen

Zunächst soll eine SessionHost-Bereitstellung gestartet werden:

A skistent zum Hinzufügen von Rollen und Features – – – – – – – – – – – – – – – – – – –					
Descente Construction Appreciating Descente Appreciating Descente Bit Descente	Assistent zum Hinzufügen von R	ollen und Features	-		×
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungstyp Bereitstellungsternario Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung Fertigstellung Verbreitung Verbreitung Verbreitung Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktopbereitstellung Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktopbereitstellung Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktops enthalten. (*) Sitzungsbasierte Desktops enthalten.	Bereitstellungsszei	nario auswählen	Standardbereitstellu	ZIELSER ng ausgew	VER ählt
Instalationsyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung Pertigstellung Verbindug Verbindug Remotedesktop-Sitzungs Bestätigung Fertigstellung Verbindug Verbindug Verbindug Verbindug Verbindug Remotedesktop-Sitzungs Bestätigung Fertigstellung Verbindug Verbindug Verbindug Remotedesktop-Sitzungs Bestätigung Fertigstellung Verbindug Verbi	Vorbereitung	Die Remotedesktopdienste können so konfiguriert werden, dass Benut virtuellen Desktops, RemoteApp-Programmen und sitzungsbasierten D	zer eine Verbindung Jesktops herstellen k	mit :önnen.	
Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung Vertigstellung	Bereitstellungstyp	\bigcirc Auf virtuellen Computern basierende Desktopbereitstellung			
Rollendienste und virtuelle Desktops enthalten. Remotedesktop-Verbindu Image: Sitzungsbasierte Desktopbereitstellung Remotedesktop-Sitzungs Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktops enthalten. Bestätigung Fertigstellung Fertigstellung enthalten. (Image: Sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktopbereitstellung Die sitzungsbasierte Desktops enthalten. Fertigstellung Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktops enthalten. enthalten. Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktops enthalten. Sitzungsbasierte Desktops enthalten. Sitzungsbasierte De	Bereitstellungsszenario	Die auf virtuellen Computern basierende Desktopbereitstellung erm einer Verbindung mit Sammlungen virtueller Desktops, die veröffen	öglicht Benutzern d tlichte RemoteApp-I	as Herste Programr	ellen me
Web Access für Remoted Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern das Herstellen einer Verbindung mit Sitzungsbasierte Desktops Bestätigung Fertigstellung Fertigstellung Zurück Weiter > Bereitstellen Abbrechen	Rollendienste Remotedesktop-Verbindu	und virtuelle Desktops enthalten. Sitzungsbasierte Desktopbereitstellung			
Remotedesktop-Sitzungs mit Sitzungssammlungen, die veröffentlichte RemoteApp-Programme und sitzungsbasierte Desktops enthalten. Bestätigung Fertigstellung Fertigstellung Zurück Weiter > Bereitstellen Abbrechen	Web Access für Remoted	Die sitzungsbasierte Desktopbereitstellung ermöglicht Benutzern da	as Herstellen einer V	erbindun	g
Pertigstellung	Remotedesktop-Sitzungs	mit Sitzungssammlungen, die veröffentlichte RemoteApp-Programn	ne und sitzungsbasi	erte Desk	tops
Fertigstellung < Zurück	Bestätigung	enthalten.			
< Zurück Weiter > Bereitstellen Abbrechen	Fertigstellung				
< Zurück Weiter > Bereitstellen Abbrechen					
< Zurück Weiter > Bereitstellen Abbrechen					
< Zurück Weiter > Bereitstellen Abbrechen					
< Zurück Weiter > Bereitstellen Abbrechen					
< Zurück Weiter > Bereitstellen Abbrechen					
< Zurück Weiter > Bereitstellen Abbrechen					
		< Zurück Weiter >	Bereitstellen	Abbrec	hen

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

📥 Assistent zum Hinzufügen von Ro	llen und Features					-		\times
Remotedesktop-Ve	erbindungsbr	oker angebe	en		Standardberei	tstellun	ZIELSERV g ausgewä	/ER ählt
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted Remotedesktop-Sitzungs Bestätigung Fertigstellung	Wählen Sie die Server in Verbindungsbroker" ins Serverpool Filter: Name WS-RDS1.ws.its	m Serverpool aus, auf o stalliert werden soll. IP-Adresse 192.168.100.16	denen der Rol	I endie	Ausgewählt Computer WS.ITS (1) WS-RDS1 1 Computer ausgew	ō-		
		< Zu	ırück W	eiter >	Bereitstell	en	Abbrech	ien

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

📥 Assistent zum Hinzufügen von	Rollen und Features				_		×
Server mit Web A	ccess für Remo	otedesktop	angebe	en	Standardbereitstel	ZIELSER\ lung ausgewä	/ER ählt
Vorbereitung Installationstyp	Wählen Sie einen Server installiert werden soll.	im Serverpool aus, au	f dem der Ro	ollendienst	"Web Access für Re	motedeskt	op"
Bereitstellungstyp Bereitstellungsszenario		ccess für Kemotedeski	top auf dem	1 KD-verbir	ndungsbrokerserver	Installierer	1
Rollendienste	Serverpool				gewanit		
Remotedesktop-Verbindu	Filter:						
Remotedeskton-Sitzungs	Name	IP-Adresse	Betriebssy	w	- WS.ITS (1) S-RDS1		
Bestätigung Fertigstellung	WS-RDS1.ws.its	192.168.100.16		►			
	<		>				
	1 Computer gefunden			1 Cc	omputer ausgewählt	t	
		< 7u	rück W	/eiter >	Bereitstellen	Abbreck	nen
🖕 Assistent zum Hinzufügen von	Rollen und Features				-		>
RD-Sitzungshosts	erver angeber	I			Standardbereitstel	ZIELSER\ lung ausgewä	/ER ählt
Vorbereitung Installationstyp Bereitstellungstyp	Wählen Sie die Server in werden soll. Bei Auswah bereitgestellt.	n Serverpool aus, auf d I mehrerer Server wird	lenen der Ro der Rollend	llendienst ' ienst auf al	'RD-Sitzungshost" i len ausgewählten Si	nstalliert ervern	
Bereitstellungsszenario	Serverpool			Διιε	newählt		
Rollendienste				Co	mputer		
Remotedesktop-Verbindu	Filter:				WS ITS (1)		
Web Access für Remoted	Name	IP-Adresse	Betriebssy	ws	S-RDS1		
RD-Sitzungsnöst Restätigung	WS-RDS1.ws.its	192.168.100.16					
Fertigstellung				►			
	<		>				
	1 Computer gefunden			1 Co	omputer ausgewählt		
		< Zur	ruck N	/eiter >	Bereitstellen	Abbrech	ien

Auswahl bestätige	Rollen und Features — L X ZIELSERVER Standardbereitstellung ausgewählt
Vorbereitung Installationstyp Bereitstellungstyp Bereitstellungsszenario Rollendienste Remotedesktop-Verbindu Web Access für Remoted RD-Sitzungshost Bestätigung Fertigstellung	Zum Abschließen der Installation müssen die Remotedesktop-Sitzungshostserver neu gestartet werden. Nach Abschluss der Installation auf den Remotecomputern wird der lokale Computer neu gestartet. RD-Verbindungsbroker (1 Server ausgewählt) WS-RDS1.ws.its Web Access für Remotedesktop (1 Server ausgewählt) WS-RDS1.ws.its Remotedesktop-Sitzungshost (1 Server ausgewählt) M Die folgenden Server können nach der Installation des Rollendiensts neu gestartet werden. WS-RDS1.ws.its Zuelsenver bei Bedarf automatisch neu starteri
	< Zurück Weiter > Bereitstellen Abbrechen

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

_						(E.D.
Status anzeigen			Sta	andardbereitstellur	ng ausgewä	ihlt
Fertigstellung	Die ausgewählten Rollendienste	der Remotedesktopdienste we	rden installie	rt.		
	Server	Status		Status		
	Remotedesktop-Verbindungs	broker (Rollendienst)				
	WS-RDS1.ws.its		Erfolgrei	ch		
	Web Access für Remotedeskt	op - Rollendienst				
	WS-RDS1.ws.its		Erfolgrei	ch		
	Remotedesktop-Sitzungshost	(Rollendienst)				
	WS-RDS1.ws.its		Erfolgrei	ch		



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



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

🚡 Server des Typs "RD-Gateway" H	hinzufügen					-		×
Wählen Sie einen Serverauswahl SSL-Zertifikatname	Server aus. Mit diesem Assistenten Wählen Sie die Server au	können Sie der Bereit us, auf denen der Roll	stellung Serv endienst "RD	/er vor)-Gate	n Typ "RD-Gat way" installier	teway" h t werden	inzufüger soll.	n.
Bestätigung	Serverpool			A	usgewählt			
Ergebnisse	Filter:				Computer	(1)		
	Name	IP-Adresse	Betrieb		WS-RDS1			
	WS-RDS1.ws.its	192.168.100.16	>		0			
	 Computer getunden Die Anmeldeinform verwendet. 	nationen des WS\sysa	dm-Kontos v	1 verder	Computer au: 1 zum Hinzufü	sgewählt gen der	: Server	
		< Zurück	Weite	er >	Hinzuf	ügen	Abbrech	ien



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

	🚡 Server des Typs "RD-Gateway" ł	inzufügen		-		×
	Selbstsigniertes S	SL-Zertifikat benen	nen			
	Serverauswahl SSL-Zertifikatname Bestätigung Ergebnisse	SSL-Zertifikate dienen zum Vers Clients und Remotedesktopgate dem vollqualifizierten Domänen Gatewayservers entsprechen. SSL-Zertifikatname (externen FO rds.ws-its.de Der FQDN muss dem Namen de Remotedesktopdienste-Client w	chlüsseln der Kommunikation zwisc way-Servern. Der Name des selbsts namen (Fully Qualified Domain Nar 2DN des RD-Gatewayservers verwen es Remotedesktop-Gatewayservers e erwendet wird.	hen Remotedeskto ignierten SSL-Zert ne, FQDN) des Rer iden): entsprechen, der vi	opdienste- ifikats mus notedeskt	is op-
			< Zurück Weiter >	Hinzufügen	Abbrech	en
Der Liz	zenzierungsserver wird ähnli	ch installiert:				
	🚡 Server des Typs "RD-Lizenzierur	g" hinzufügen		-		×
	Wählen Sie einen	Server aus.				

Serverpool			Ausgewählt
Filter:			✓ WSJTS (1)
Name	IP-Adresse	Betrieb	WS-RDS1
WS-RDS1.ws.its	192.168.100.16		
<		>	
1 Computer gefunden			1 Computer ausgewählt
i Die Anmeldeinfor	mationen des WS\sysa	dm-Kontos we	rden zum Hinzufügen der Server

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

Beschaffung eines Zertifikates für die neue RDS-Infrastruktur

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

💐 Internetinformationsdienste (IIS)	-Manager					- 🗆 X
← → ♥∃ ► WS-RDS1 ►						🔤 🖾 🟠 🔞 -
Datei Ansicht ?						
Verbindungen	Serverzertifil Mit dieser Funktion können S Filter:	Kate iie Zertifikate anfordern und verwa - 🐨 Start - 🖼 Alle anzeigen	ilten, die der Webserver bei für SSL kon Gruppieren nach: Keine Gruppierung	figurierten Websites ve	rwenden kann.	Aktionen Importieren Zertifikatanforderung estellen Zertifikatanforderung
> - 🔊 Sites	Name	Ausgestellt für WS-RDS1.ws.its WS-RDS1.ws.its	Ausgestellt von WS-RD51.ws.its WS-ITS-Zertifizierungsstelle	Ablaufdatum 23.07.2017 10:38:27 19.01.2018 20:47:22	Zertifikathash 327C0B499164 0AC827F6760E	abschließen Domänenzertifikat erstellen Selbstigniertes Zertifikat erstellen Automatische erneute Bindung des erneuerten Zertifikats aktivieren

Der externe Name muss mit der Konfiguration des Gateways übereinstimmen.

Zertifikat anfordern					?	×
Eigenschafter	für definierter	Namen				
Geben Sie die erforderliche die offiziellen Namen ohne	n Informationen fü Abkürzungen ange	r das Zertifikat an. Fi :geben werden.	ir "Bundesland/Ka	nton" und "Ort" m	lüssen	
Gemeinsamer Name:	rds.ws-its.de					
Organisation:	WS IT-Solution	ons				
Organisationseinheit:	IT-Services					
Ort:	Ergoldsbach					
Bundesland/Kanton:	Bayern					
Land/Region:	DE			~		
		7 - 5 - 6	Welter	Partie Adve		-
		Zurück	Weiter	Fertig stellen	Abbreche	n
Zertifikat anfordern Eigenschaften	für Kryptogra	fiedienstanbiete	r		?	×
Wählen Sie einen Kryptogra Verschlüsselungsschlüssels höher die Sicherheit. Eine g Kryptografiedienstanbieter: Microsoft RSA SChannel Cr	fiedienstanbieter u bestimmt die Versc rößere Bitlänge kan votographic Provid	nd eine Bitlänge aus hlüsselungsstärke d n jedoch die Leistur er	. Die Bitlänge des es Zertifikats. Je gr 1g verringern.	ößer die Bitlänge,	desto	
Bitlänge:						
2048						
		7	Maitan.		Abberghe	-



Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

ertifikat anfordern	?	×
Dateiname		
Geben Sie den Dateinamen für die Zertifikatanforderung an. Diese Informationen können zum Signier eine Zertifizierungsstelle gesendet werden.	ren an	
Dateiname für die Zertifikatanforderung:		
C:\Admin\2017-01-22 rds.ws-its.de.req		
Zurück Weiter Fertig stellen	Abbrech	en

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

ol Box	Certificates Wizard	Validations Wizard				
ree SSL	. Certificate – Class 1 D\	/ SSL Certificate				
Please e	enter the full hostname for S	SL certificate (e.g: mail.dom	ain.com):			
Validat	ed domain(s): ws-its.de	Add Domain				
rds.ws	-i <u>ts</u> de			🤣 The common n	iame of t	this certificate: rds.ws-its.de
Do you	want to add the following host	name?				
1. The 2. You	first entry domain will be the co can enter up to 10 hostnames,	mmon name of the certificate. one line one hostname with "En	ter" or separate each	hostname with a com	ma.	
1. The 2. You 3. You If you v FREE. FREE Please s	first entry domain will be the co can enter up to 10 hostnames, can not enter a wildcard like *.c would like to support up to 100 h Or go to " <u>Organization Extende</u> submit your Certificate Signi rated by Myself (.cer PEM form	mmon name of the certificate. one line one hostname with "En lomain.com. iostnames and wildcard, please id <u>Validation</u> " for organization us ng Request (CSR): nat certificate)	ter" or separate each finish the " <u>Personal Ic</u> se that only cost US\$1	hostname with a com l <u>entity Validation</u> " for 99.90 for unlimited m	ma. persona ulti-doma	I use that only cost US\$59.9 ain and wildcard OV SSL ce
1. The 2. You 3. You If you v FREE. FREE Please s	first entry domain will be the co can enter up to 10 hostnames, can not enter a wildcard like *.c would like to support up to 100 h Or go to " <u>Organization Extende</u> submit your Certificate Signi rated by Myself (.cer PEM form can use <u>StartComTool.exe</u> to ge	mmon name of the certificate. one line one hostname with "En lomain.com. lostnames and wildcard, please <u>d Validation</u> " for organization us ng Request (CSR): nat certificate) nerate the CSR.	ter" or separate each finish the " <u>Personal Ic</u> se that only cost US\$1	hostname with a com l <u>entity Validation</u> " for 99.90 for unlimited m	ma. persona ulti-doma	Il use that only cost US\$59.9 ain and wildcard OV SSL ce

StartCom[®]

Fool Box	Certificates Wizard	Validations Wizard	
fool Box	Certificates Wizard	Validations Wizard	

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

en Ansicht				∣ × ~ (2)	Konsole1 - [Konsolenstamm\Zertifikate (Li Batei Aktion Ansicht Favoriten Fe	okaler Computer)\Zwischenzertifizierur :nster ?	ngsstellen\Zertifikate]	
ser PC > SYSTEM (C:) > Admin		∨ ບື "Admin	" durchsuchen	Q	🗢 🔿 🙍 🗊 📋 🗟 🗟 📆			
Name	Anderungsdatum 22.01.2017 1649 22.01.2017 1649 22.01.2017 0948 22.01.2017 0948 22.01.2017 09450	Typ Sicherheitszertifikat REQ-Date ZIP-komprimiette	Große 3 KB 3 K3 2 K8 16 K8		Konsolenstamm Veil Zetrifikate (Lokaler Computer) Eigene Zetrifikate Veil Zetrifikate (Lokaler Computer) Veil Zetrifikate (Lokaler Computer) Zetrifikatesperifiste Zetrifikatesperifiste Zetrifikatesperifiste Veitzuenswürdige Verausgeber Nicht vertrauenswürdige Zetrifikate Drinbidere Sammzesussteller Stammelemente der Vorabversion Stammelemente der Vorabversion Zetrifikatespistrierungsandrderung Smartcarl vertrauenswürdige Zetrif Wehosting Windows Live ID Token Issuer	Ausgetallt für Microsoft Windows Hardware Root Agency W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 W-ST-SZettfräterungsstelle-CA1 M-ST-SZettfräterungsstelle-CA1 Altaalisieren Liste oportieren Ansicht Symbole andrenen Ansket ausricht Hilfe	Ausgetall von Microoft Roch Authority Roct Agency WS-ITS-Zertifizierungstelle-CA1 WS-ITS-Zertifizierungstelle-CA1 WS-ITS-Zertifizierungstelle-CA1 WS-ITS-Zertifizierungstelle-CA1 WS-ITS-Zertifizierungstelle-CA1 Class 3 Public Primary Certificatio.	Abi Aktionen 31: Zertifikate 01.1 Weitere Aktion 16.3 Veitere Aktion 16.4 16.4 16.4 25.5
	< .	Zertifikatim Zu importieren Geben Sie	oort-Assister de Datei die Datei an, i	it die impor	Tiert werden soll.	×		
		Dateiname C:\Admin	: \2017-01-22 I	intermed	liate.crt	Durchsuchen		
		Hinweis: M werden: Privater Syntax: Microso	ehrere Zertifik [.] Informations standard kryp ft Serieller Zei	kate könn austaus tografisc rtifikatsp	nen in einer Datei in folgenden Forn ch - PKCS #12 (.PFX,.P12) cher Meldungen - "PKCS #7"-Zertifik eicher (.SST)	naten gespeichert ate (.P7B)		
				- ma ap				
					Weit	er Abbrechen		



Section,	aumport Assistent	
Zertifikal Zerti	speicher likatspeicher sind Systembereiche, in denen Zertifikate gespeich	nert werden.
Wind	ows kann automatisch einen Zertifikatspeicher auswählen, oder herort für die Zertifikate angeben.	Sie können einen
C) Zertifikatspeicher a <u>u</u> tomatisch auswählen (auf dem Zertifikatt	yp basierend)
	Alle Zertifikate in folgendem Speicher speichern	
	Zertifikatspeicher:	
	Zwischenzertifizierungsstellen	Durchsuchen

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

Internetinformationsdienste (IIS)	-Manager			– 🗆 X
← → ♥ WS-RDS1 →				📴 🖂 🟠 🔞 -
Datei Ansicht ?				
Verbindungen	Server:	zertifikate		Aktionen
Startseite WS-RDS1 (WS\sysadm)	Mit dieser Funktion der Webserver bei fi	können Sie Zertifikate anfordern und verw ür SSL konfigurierten Websites verwenden	alten, die kann.	Zertifikatanforderung erstellen Zertifikatanforderung
> 🔞 Sites	Filter:	🝷 🖤 Start 👒 🔙 Alle anzeigen 🛛	Ŧ	abschließen
	Name	Ausgestellt für WS-RDS1.ws.its WS-RDS1.ws.its	Aus <u>e</u> WS- WS-	Domänenzertifikat erstellen Selbstsigniertes Zertifikat erstellen Automatische erneute Bindung des erneuerten Zertifikats aktivieren
Zertifikat Eercitt abschi Name C:\Adu Anzeig 2017-C Zertifii Persön	anforderung abschließen Antwort der Zertifizie serstellte Zertifikatanforderung ließen der Datei mit der Antwort der Z min\2017-01-22 rds.ws-its.de.cr gename: D1-22 rds.ws-its.de N1-22 rds.ws-its.de katspeicher für das neue Zertifik hlich	erungsstelle angeben durch Abrufen der Datei mit der Antwort der Zertifizier Zertifizierungsstelle: tt	? ungsstelle	×

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

🚟 Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Computer)\Eigene Zertifikate\Zertifikate]

Kon	isolenstamm Zertifikate (Lokaler Computer)		Ausgestellt für		Aus	sgestellt von	Ab
~	Eigene Zertifikate		rds.ws-its.de	Öffnen	Sta	rtCom Class 1 DV Server CA vs-its.de	22. 23.
	Öffnen		a	Alle Aufgaben	>	RDS1.ws.its TS-Zertifizierungsstelle-CA1	23.
	Zertifikat mit neuem Schlüssel an Zertifikat mit neuem Schlüssel err	forder neuern	n	Ausschneiden Kopieren			15.
	Private Schlüssel verwalten			Löschen			
	Exportieren		/	Hilfe			
> (Clientauthentifizierungsausste	ller	× ***				
Zertifikatexpo ivaten Schlüss Sie können	ort-Assistent æl exportieren den privaten Schlüssel mit dem Zertifikat exportieren.			Certifikatexport Zu exportierende I Geben Sie der	t-Assistent Datei 1 Namen de	r zu exportierenden Datei an.	
Private Sch ausgewählt Seiten ein K	lüssel sind kennwortgeschützt. Wenn Sie den privaten S ten Zertifikat exportieren möchten, müssen Sie auf einer kennwort eingeben.	chlüssel mi der folger	t dem Iden	Dateiname: C:\Admin\20	17-01-22 rc	ds.ws-its.de.pfx Durch	nsuchen
Möchten Sie	e mit dem Zertifikat auch den privaten Schlüssel exportie privaten Schlüssel exportieren n, privaten Schlüssel nicht exportieren	ren?					

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

<mark> </mark>	nin [:] reigeb	en Ansicht			- 0
· ↑ 📙	> Die	ser PC > SYSTEM (C:) > Admin >		✓ ♂ "Admin	" durchsuchen
nellzugriff		Name	Änderungsdatum	Тур	Größe
esktop	*	🔄 2017-01-22 Intermediate.crt	22.01.2017 16:49	Sicherheitszertifikat	3 KB
okumente	*	🔄 2017-01-22 rds.ws-its.de.crt	22.01.2017 16:49	Sicherheitszertifikat	3 KB
ownloads		👼 2017-01-22 rds.ws-its.de.pfx	22.01.2017 09:55	Privater Informati	8 KB
	1	🗐 2017-01-22 rds.ws-its.de.req	22.01.2017 09:48	REQ-Datei	2 KB
laer dmin	*	2017-01-22 rds.ws-its.de.zip	22.01.2017 09:50	ZIP-komprimierte	16 KB



Konfiguration der RDS-Infrastruktur - allgemein

Im Servermanager starte ichh den erforderlichen Assistenten:

📥 Server	-Manager									
\mathbf{E}	● ✓ Server-Ma	anager • Rer	notedesktop- dier	nste ∙ Üb	ersicht					
	Übersicht	ERSTE SCHRITTE N	IIT DEN REMOTEDESKTOPDI	ENSTEN						
i is	Server Sammlungen		0	Remoted	lesktopdienste	-Bereits	tellung einrichte	ən		
i∎ ⊳ i© ? ⊗ ⊳		SCHNELLSTART WEITERE INFORMATIONE	Auf virtuellen Compu Desktopbereitstellun 2 RD-Virtualisierung 3 Virtuelle Desktops	utern basien 19 shostserver h ammlungen e	ende ninzufügen erstellen		Sitzungsbasierte De 2 RD-Sitzungshost 3 Sitzungssammlu	esktopbere server hinzungen erstell	itstellung ufügen en	g
		BEREITSTELL RD-Verbindun Verwaltet als: WS\sy	LUNGSÜBERSICHT Igsbrokerserver: WS-RDS1.ws.its sadm Ber Ver	eitstellungseigen: bindung mit ande	AUFGAE schaften bearbeiten erer Bereitstellung herstellen	BEN 🔻	BEREITSTELLUNGSSERVE Letzte Aktualisierung: 22.01.20 Filter	R 17 09:49:31 Alla P	e RDS-Rollen	ndienste 5 insgesamt (A) 💌
		Web Access t	jür Remo Remotedes	ktopgate	Remotedesktoplizer	nz	Vollqualifizierter Domänennai WS-RDS1.WS.ITS WS-RDS1.WS.ITS WS-RDS1.WS.ITS WS-RDS1.WS.ITS WS-RDS1.WS.ITS	ne des Servers	Installierter RD-Verbind RD-Sitzung RD-Gatewa RD-Lizenzie Web Access	Rollendienst Jungsbroker Ishost IV erung s für Remotedesktop
		Remo)tedesktop-Virtu	Remo	otedesktop-Sitzu					

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

🚡 Bereitstellungseigenschaften		-		×
Bereitstellungseigenschaften Bereitstellung kon Alle anzeigen Remotedesktopga – Remotedesktopliz + Web Access für Re + Zertifikate +	figurieren Remotedesktopgateway RD-Gatewayeinstellungen für die Bereitstellung angeben Remotedesktop-Gatewayservereinstellungen automatisch ermit Ervername: rds.ws-its.de Anmeldemethode: Kennwortauthentifizierung RD-Gatewayanmeldeinformationen für Remotecomputer ver RD-Gatewayanmeldeinformationen für Remotecomputer ver Remotedesktop-Gatewayserver für lokale Adressen umgeher	 teln wenden n		×
	OK Abb	rechen	Anwenc	len



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

🚡 Bereitstellungseigenschaften		-		×
Bereitstellung konfig	gurieren			
Alle anzeigen Remotedesktopga + Remotedesktopliz Web Access für Re + Zertifikate +	RD-Lizenzierung Remotedesktop-Lizenzierungsmodus auswählen: O Pro Gerät © Pro Benutzer			
	Geben Sie einen Lizenzserver an, und klicken Sie anschließend auf "h	linzufüge Hinz	n": ufügen	
	Wählen Sie die Reihenfolge der Remotedesktop-Lizenzserver aus: Der RD-Sitzungshostserver oder RD-Virtualisierungshostserver send Lizenzanforderungen in der hier festgelegten Reihenfolge an die ang Lizenzserver.	et Jegebene	n	
	WS-RDS1.ws.its	Nac	th oben	
		Nac	h unten	
		Ent	tfernen	
	OK Abbr	echen	Anwend	en

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

ᡖ Bereitstellungseigenschaften			-		×
Bereitstellung kon	figurieren				
Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Serverauthentifizierung, einmaliges An Verbindungen erforderlich. Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	istellung sind Zertifika imelden und Herstelle stellung ist Nicht kon t	te für die In von sicheren figuriert		^
	Rollendienst	Stufe	Status	Status	
	Remotedesktop-Verbindungsbroker	Nicht konfiguriert			
	Remotedesktop-Verbindungsbroker	Nicht konfiguriert			
	Web Access für Remotedesktop	Nicht konfiguriert			
	RD-Gateway	Nicht konfiguriert			
	<				>
	Antragstellername: Nicht verfügbar Details anzeigen Dieses Zertifikat ist für die Serverauthe Bereitstellung erforderlich. Sie können dieses Zertifikat aktualisier ein vorhandenes Zertifikat auswählen. Neues Zertifikat erstellen	entifizierung für die Re en, indem Sie ein neu Vorhander	emotedesktopd es Zertifikat ers <mark>nes Zertifikat au</mark>	ienste- tellen oder <mark>swählen</mark> .	
		OK	Abbrechen	Anwen	den



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

ereitstellungseigenschaften		\times
Vorhandenes Zertifikat auswählen		
Sie können das momentan auf dem RD-Verbindungsbrokerserver gespeic einer PKCS-Zertifikatsdatei auswählen	herte Zertifikat anwenden oder ein anderes Zertifikat	t in
Auf dem RD-Verbindungsbrokerserver gespeichertes Zertifikat anwend	den	
Kennwort:		
 Anderes Zertifikat auswählen 		
Zertifikatpfad:		
C:\Admin\2017-01-22 rds.ws-its.de.pfx	Durchsuc	hen
Kennwort:		
•••••		
Hinzufügen des Zertifikats zum Zertifikatspeicher "Vertrauenswürdige	Stammzertifizierungsstellen" auf den Zielcomputern	zulas
	OK Abt	orech

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

🚡 Bereitstellungseigenschaften					_		×		
Bereitstellung konfig	gurieren								
Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Verbindungen erforderlich. Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	stellung sind Zertifika stellung ist Nicht kon	ate für die Serv figuriert	rerauthentifizierung, einmaliges Anmelden und Herste	ellen vor	n sicherer	n		
	Rollendienst	Stufe	Status	Status					
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	ОК	Erfolgreich					
	Remotedesktop-Verbindungsbroker	Nicht konfiguriert							
	Web Access für Remotedesktop	Nicht konfiguriert							
	RD-Gateway	Nicht konfiguriert							
	Antragstellername: Nicht verfügbar Details anzeigen Dieses Zertifikat ist für die Signierung Sie können dieses Zertifikat aktualisier	von RDP-Dateien zun en, indem Sie ein neu	n Vermeiden v	on zusätzlichen Warnungen für den Benutzer erforder rstellen oder ein vorhandenes Zertifikat auswählen.	lich.				
	Neues Zertifika	Neues Zertifikat erstellen							

Abbrechen Anwenden

OK

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

🚡 Bereitstellungseigenschaften				- 0	×
Bereitstellung konfig	urieren				
Alle anzeigen Remotedesktopga + Remotedesktopliz + Web Access für Re + Zertifikate –	Zertifikate verwalten Für eine Remotedesktopdienste-Bereit Verbindungen erforderlich. Die aktuelle Zertifikatsstufe der Bereits Was ist eine Zertifikatsstufe?	tstellung sind Zertifika stellung ist Vertrauen	ite für die Se swürdig	rverauthentifizierung, einmaliges Anmelden und Herstellen von sicher	en
	Rollendienst	Stufe	Status	Status	
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	ОК	Erfolgreich	-
	Remotedesktop-Verbindungsbroker	Vertrauenswürdig	OK	Erfolgreich	
	Web Access für Remotedesktop	Vertrauenswürdig	OK	Erfolgreich	
	RD-Gateway	Vertrauenswürdig	OK	Erfolgreich	

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

Administrator: Eingabeaufforde	erung	
Microsoft Windows [Versi (c) 2016 Microsoft Corpo	on 10.0.14393] ration. Alle Rechte vorbehalten.	
C:\Windows\system32>slmg	r /ipk	
C:\Windows\system32>	Windows Script Host	×
2	Der Product Key Ander State State	
	ОК	
Administrator: Eingabeaufforde	rung	
C:\Windows\system32≻slmgr	r /ato	
C:\Windows\system32>		
	Windows Script Host	×
	Windows(R), ServerDatacenter edition (d839f159-1128-480b-94b6-77fa9943a16a wird aktiviert Das Produkt wurde erfolgreich aktiviert.	a)
	OK	

Konfiguration der Lizenzierung – Migration der bestehenden CALs

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





Zunächst aktiviere ich den neuen RDS-Lizenzserver:

🙀 Remotedesktop	olizenzierungs-Manager								
Aktion Ansicht	?								
107 17- 173 III									
🖃 🛱 Alle Server	Lizenzversion und	-typ	Lizenzprogram	Gesamte Lizen	Verfügbar	Ausgestellt	Ablaufdatum	Schlüsselpaket	
	Aktualisieren	- Integrierte TS-CA	Integriert	Unbegrenzt	Unbegrenzt	0	Nie	2	
	Konfiguration prüfen								
	Lizenzen installieren								
1	Server aktivieren								
	Erweitert	>							
	Bericht erstellen	>							
	Berichte löschen								
	Lizenzen verwalten								
	Eigenschaften								
Serveraktivierungs-A	ssistent			× Serverakti	vierungs-Assisten	t			×
Verbindungsmeth	node		Q	Firmen	informationen				Q
Wahlen Sie die	passendste Aktivierungsmethode	aus.	a	Sei Gei	ben Sie die angefon	derten Firmeninformat	ionen an.		बिः
Die Verbindung Kontaktaufnahn werden.	smethode für die Lizenzserveraktiv ne mit dem Microsoft Clearinghous	vierung wird auch für die e verwendet, wenn Lizenzen in	stalliert	Geben	Sie Ihren Namen, d	len Firmennamen und	das Land bzw. die Reg	gion ein.	
Öffnen Sie die F	Registerkarte "Verbindungsmethod	de" im Dialogfeld "Eigenschafte der Aktivienung zu ändern	n" des	Diese i			vorgangs enordenien.		
Verbindungsmei	thode:	der Aktivierung zu andern.		Voman	ne:	Stephan			
Automatische	Verbindung (empfohlen)		\sim	Nachna	ame:	Walther			
Beschreibung:	Dies ist die empfohl	ene Methode. Der Lizenzserve	wird die	Fima:		WS IT-Solutions			
	erforderlichen Inforr Clearinghouse über	nationen automatisch mit dem N das Internet austauschen.	Aicrosoft .	Land o	der Region:	Deutschland		~	
Anforderungen:	Der Computer muss SSL-Verbindung (Si	: die Internetverbindung über ei ecure Sockets Layer) hersteller	ie können.	()	Microsoft verwe Unterstützung b das Land bzw. c	ndet den Namen und enötigen sollten. Aufg die Region angegebei	die Firmeninformationer rund von Exportbeschr n werden.	n nur, falls Sie änkungen der USA muss	
		< Zinjirk Wate	r > Abbrechen				- 710°irl	c Weters 4	hhrechen
		< Zuruck Weite	r > Abbrechen				< Zurück	Weiter >	obrecher

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 WS IT-Solutions 2017-01-19

Serveraktivierungs-Assistent		×	Serveraktivierungs-Assistent		×
Firmeninformationen Geben Sie diese optionale	en Informationen ein.	9		Fertigstellen des Assistenten	
E-Mail: Organisationseinheit: Firmenadresse: Ort: Bundesland/Kanton: PLZ: With Die optionalen Info Verwendet, falls Sir	I mationen werden nur von Microsoft-Supportspezialisten Unterstützung benötigen sollten.			Der Assistent zur Serveraktivierung wurde erfolgreich aboeschlossen. Status: Der Lizenzserver wurde aktiviert. Klicken Sie auf "Weiter", um Lizenzen zu installieren. Deaktivieren Sie das Kortollkächchen "Assistent für die Lizenzinstallation starten", um die Lizenzinstallation zu verschieben. ✓ Assistent für die Lizenzinstallation starten	
	< Zurück Weiter >	Abbrechen		< Zurück Weiter >	Abbrechen

Danach lasse ich automatisch den Lizenzinstallations-Assistenten starten:

Serveraktivierungs-Assistent		×	Sen	veraktivierungs-Assiste	nt					
	Willkommen		1	L izenzprogramm Wählen Sie das pass	ende Lizenzpr	ogramm aus.				q.
	Mit diesem Assistenten können Sie Lizenzen auf dem Remotedesktop-Lizenzserver installieren.			Jeder Client, von dem einem virtuellen Desk muss eine gültige Lize Lizenzen enworben ha	eine Verbindu top in einer Mi nz haben. Wä aben.	ing mit einem F crosoft Virtual ihlen Sie das L	Remotedeskto Desktop Infra izenzprogram	op-Sitzungshos structure herge m aus, über da	tserver oder estellt wird, as Sie die	
	Sie benötigen ihre Lizenzerwerbeinformationen (z. B. Lizenznurmer der Verkadzversion oder der Volumenilzenz), um diesen Assistenten abzuschließen. Lizenzservereinstellungen			Lizenzprogramm: Beschreibung:	Vollprod Diese Liz oder bei	ukterwerb enz wird in vor einem anderen	definierten Me Händler erwo	engen im Einze orben. Diese		
	Aktiviert für: WS IT-Solutions Verbindungsmethode:Automatische Verbindung (empfohlen) Lizenzprogramm: Vollprodukterwerb			Format und Pfad:	Verpackung ist möglicherweise mit "Microsoft Windows Client License Pack" bezichnet. Die im Lizenzpaket enthaltene Lizenznummer ist erforderlic Das Format für die Lizenznummer ist 5 Sätze à 5 alphanumerischen Zahlen.			ows orderlich.		
	Klicken Sie auf "Abbrechen", und öffnen Sie dann im Dialogfeld "Eigenschaften" des Lizenzservers die Registerkarte "Verbindungsmethode", um die Verbindungsmethode zu ändern.			Beispiel:	1A2B3	1A2B3	1A2B3	1A2B3	1A2B3	
			s V	itellen Sie sicher, dass die Vorgang fortsetzen.	Lizenzinforma	tionen dem Be	eispiel entspre	chen, bevor Si	ie den	
	< Zurück Weiter > Abb	rechen					< <u>Z</u> u	rück <u>W</u> e	eiter >	Abbrech



Ich installiere 50 neue CALs für Windows Server 2016:

raktivierungs-Assistent	× Serveraktivierungs-Assistent	
zen znummer Geben Sie die Lizenznummer ein. Sie finden die Nummer in der Verpackung.	Fertigstellen	des Assistenten
Geben Sie die Lizenznummer für jede Lizenz, die Sie erworben haben ein, und klicken Sie nach der Eingabe jeder Lizenznummer auf "Hinzufügen". Das Format für die Lizenznummer ist 5 Abschnitte à 5 alphanumerische Zahlen. Lizenznugmer:	Der Assistent zum Insta erfolgreich abeschlos Installiert: (50 Windows Server 2 ist Installiert <	allieren von Lizenzen wurde sen. 016 - "Pro Benutzer"-RDS-CAL
Uzenznummer Status Produkttyp Ausstehe Windows Server 2016 : Rei		
	Die angeforderten Lize	nzen wurden installiert.
< Bgarbeten Löschen	Die angeforderten Lize	nzen wurden installiert.
<bgabeitenlöschen< td=""><td>Die angefordetten Lize</td><td>nzen wurden installiert.</td></bgabeitenlöschen<>	Die angefordetten Lize	nzen wurden installiert.
< Bgarbeten Löschen	Die angeforderten Lize	nzen wurden installiert.

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

🗣 Remotedesktoplizenzierungs-Mar	nager					
Aktion Ansicht ?						
 ⇒ Alle Server → Alle Server → Alle Server → Windows 2000 Server - → Windows Server 2016 - 	Name A	ktivierungsstatus .ktiviert	Suchbereich Domäne	Konfiguration Überprüfen		
🖳 🕞 Berichte		WS-RDS1-Ko	nfiguration			×
		Lizenzserve Suchbereich Datenbankp	rname: WS-RDS1 n: Domäne ofad: C:\Windows\Sys	em32\LServer\	Bereic	h ändern
 Netzwerk Services Sicherheit Tools 	NDOWS POWERSHELL	Der der ber ber der ber die ers Die Die Lizz Rei	r Lizenzserver ist kein 1 Active Directory-Dom nutzergebundenen Rer sem Lizenzebundenen Rer sem Lizenzserver nich tellen. r Lizenzserver ist in A nstverbindungspunk enzserver wird im Kor motedesktop-Sitzung	Aitglied der Gruppe "Terminalse änendiensten. Dieser Lizenzse notedesktopdienste-Clientzugr Remotedesktoplizenzierung Sie müssen in den Ac DS) über Domänenad DS) über Domänenad mas Computerkon "Terminalserver-Lizen Weiter	rver-Lizenzserver" in rver kann keine Zu Grup Iffslizenzen für /erwendung von Iffslizenzen auf s-Manager tive Directory-Domänendiensten (A ministratorberechtigungen verfüge to für den Lizenzserver der Gruppe izserver" in den AD DS hinzuzufüge Abbrechen OK	pe hinzufügen
					OK	Abbrechen
Backup						

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

Remotedesktoplizenzierungs-Manager	×
Das Computerkonto für Lizenzserver "WS-RDS1" wurde der Gruppe "Terminalserver-Lizenzserver" in den Active Directory-Domänendiensten (AD DS) hinzugefügt.	
ОК	

Der LIMA ist nun einsatzbereit:

😪 Remotedesktoplizenzierungs-Man Aktion Ansicht ?	ager				
Alle Server WS-RDS1 Windows 2000 Server - Windows Server 2016 - Berichte	Name	Aktivierungsstatus Aktiviert	Suchbereich Domäne	Konfiguration OK	

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

🙀 Remotedesktopliz	enzierungs-Manager							
Aktion Ansicht ?								
Alle Server	Lizenzversion und -typ		Lizenzprogram	Gesamte Lizen	Verfügbar	Ausgestellt	Ablaufdatum	Schlüsselpaket
	Aktualisieren	ntegrierte TS-CA nstallierte "Pro B	Integriert Einzelhandel	Unbegrenzt 50	Unbegrenzt 47	0 3	Nie Nie	2 3
	Konfiguration prüfen							
	Lizenzen installieren							
	Server aktivieren							
	Erweitert	>						
	Bericht erstellen	>						
	Berichte löschen							
	Lizenzen verwalten							
	Eigenschaften							

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

ssistent zum Verwalten von Lizenzen	×	Assistent zum Verwalten von Lizenzen	×
Auswahl der Aktion Entscheiden Sie, ob Sie Lizenzen migrieren oder die Lizenzserverdatenbank erneut erstellen.		Informationen zum Quelllizenzserver Geben Sie die erforderlichen Informationen zum Quellizenzserver an.	
		Name oder IP-Adresse des Queillizenzservers:	
Lizenzen von anderem Lizenzserver zu diesem Lizenzserver migrieren		ws-rds2.ws.its	
Der andere Lizenzserver wird in diesem Assistenten als Gueillizenzserver bezeichnet.		Der angegebene Queillizenzserver ist im Netzwerk nicht verfügbar.	
Wählen Sie einen Grund für die Migration der Lizenzen aus:		Wählen Sie das Betriebssystem aus, unter dem der Quelllizenzserver ausgeführt wird:	
Der Quelllizenzserver wird durch diesen Lizenzserver ersetzt $\qquad \lor$		~	
O Lizenzserverdatenbank erneut erstellen		Geben Sie die Lizenzserver-ID für den Quelllizenzserver ein:	
Wenn Sie die Remotedesktop-Lizenzierungsdatenbank erneut erstellen, werden sämtliche derzeit auf diesem Lizenzserver installierten Lizenzen gelöscht. Anschließend müssen diese Lizenzen erneut installiet werden.		Weitere Informationen zum Suchen der Lizenzserver-ID	
Wählen Sie einen Grund für das erneute Erstellen der Remotedesktop-Lizenzierungsdatenbank aus:			
~ ~			
<zurück weiter=""> Ab</zurück>	brechen	< Zurück Weiter >	Abbrechen

Auch hier müssen die CAL-Schlüssel eingegeben werden:

WS IT-Solutions

Assistent zum Verwalten v	on Lizenzen					×	Assistent zum Verv	walten von	Lizenzen				×
Lizenzprogramm Wählen Sie das passende Lizenzprogramm aus.					9	Lizenznummer Geben Sie di	ie Lizenznun	mmer ein. Sie	finden die N	Nummer in der 1	/erpackung.		
Jeder Client, von dem einem virtuellen Desk muss eine gültige Lize Lizenzen erworben ha	n eine Verbindung top in einer Micro enz haben. Wähl aben.	g mit einem Re osoft Virtual De en Sie das Lize	emotedeskto, esktop Infras enzprogramr	p-Sitzungshos tructure herge n aus, über da	tserver oder estellt wird, as Sie die		Geben Sie di Sie nach der Lizenznumme	ie Lizenznum Eingabe jed er ist 5 Absch er:	nmer für jede der Lizenznur hnitte à 5 alp	Lizenz, die mmer auf "H vhanumerisch	Sie erworben h inzufügen". Da he Zahlen.	aben ein, und klicken is Format für die	
Lizenzprogramm:	Vollprodukt	terwerb			\sim							Hinzufügen	1
Beschreibung:	Diese Lizen oder bei ein Verpackung Client Licen	z wird in vorde em anderen H g ist möglichen se Pack'' beze	stinierten Me ländler erwo weise mit "M eichnet.	ngen im Einze rben. Diese licrosoft Winde	ihandel ows		Eingegebene	e Lizenznum	mem:				-
Format und Pfad:	Die im Lizen Das Format alphanumer	Die in Lizense rack, bezeichne Lizenznummer ist erforderlich. Die im Lizenzpaket enthaltene Lizenznummer ist 5 Satze à 5 alphanumerischen Zahlen.			orderlich.				alftil Tr	1	Status Ausstehend Ausstehend	Produkttyp Windows Server 201 Windows Server 201	2
Beispiel:	1A2B3	1A2B3	1A2B3	1A2B3	1A2B3								
Stellen Sie sicher, dass die Vorgang fortsetzen.	a Lizenzinformatio	onen dem Beis	piel entspred	shen, bevor Si	ie den		¢				Bearb	eiten Löschen	
			< Zur	ück We	siter > Abb	rechen					< Zur	ück Weiter >	Abbrechen

Die Übertragung der CALs läuft:

Assistent zum Verwalten von Li	zenzen		\times	
Lizenznummer Geben Sie die Lizenznumm	ner ein. Sie finden die Nummer	in der Verpackung.	9 ₁	Lizen Verf
Geben Sie die Lizenznumm Sie nach der Eingabe jede Lizenznummer ist 5 Abschr Lizenznummer: Eingegebene Lizenznummer G6KNTHKJQ9WMP8MY 2VM3VN28VC9Y9JVC4F	er für jede Lizenz, die Sie erw Lizenznummer auf "Hinzufüg litte à 5 alphanumerische Zahl em: Assistent zum Verwalten v Die Lizenzen werden m	orben haben ein, und klick en". Das Format für die en. Hinzufüg /on Lizenzen igriert	en gen	izt Unb 47
		Bearbeiten Lösche	en	
Assistent zum Verwalten von Lizenzen Manuelles Löschen von Lizenzen Lesen Sie die Wamung, und entscheiden Sie, ob Sie die Beding	ungen annehmen.	Assistent zum Verwalten von L	Lizenzen Der Assistent zum	Verwalten von
Fehler beim Entfernen der Lizenzpakete vom Quellizenzse Die Lizenzen müssen daher manuell vom Quellizenzserve Informationen finden Sie unter <u>Lizenzen entfernen</u> .	arver.		Lizenzen wird abge Der Vorgang wurde ohne Fehler Status: Die Lizenzen wurden migriert, d Lizenzachlüsselpaket konnte in werden.	eschlossen. abgeschlossen. och das der Guelle nicht deinstalliert
☐ Ich ektäre mich einverstanden, die Lizenzen für Remotedeskt Quellizenzserver zu entfemen. Ich bin mir bewusst, dass Ich b des Quellizenzservers für die von mir migrierten Lizenzen gege Microsoft-Software-Lizenzbedingungen verstoße.	opdienste manuell vom i wetterer Verwendung n die			
< Zur	ick Weiter > Abbrechen		<	Zurück Fertig stellen Abbrechen

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

	Remotedesktoplizenzierungs-Manager							
E	Aktion Ansicht ?							
)								
Alle Server Lizenzversion und -typ Lizenzp		Lizenzprogram	Gesamte Lizen	Verfügbar	Ausgestellt	Ablaufdatum	Schlüsselpaket	
2	in Ling WS-RDS1	🕼 Windows 2000 Server - Integrierte TS-CA	Integriert	Unbegrenzt	Unbegrenzt	0	Nie	2
		👼 Windows Server 2012 - Installierte "Pro B	Einzelhandel	100	100		Nie	4
-		🖶 Windows Server 2016 - Installierte "Pro B	Einzelhandel	50	47	3	Nie	3

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



Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19







WS IT-Solutions Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

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

ا ن ان				
ເ⊖ 🔄 マ ↑ 🗗 Systemsteueru	ng 🕨 System und Sic			
Systemeigenschaften	× ation			
Ändern des Computernamens bzw. der D	n			
Sie können den Namen und die Mitgliedschaft des Computers ändem. Änderungen wirken sich möglicherweise auf den Zugriff auf Netzwerkressourcen aus	mputers rver 20 osoft (
Computername:	der			
WS-RDS2 Vollständiger Computername: WS-RDS2.ws.its	Arbeits			
Weitere	em ucheii			
Mitglied von O Domäne:	r Com			
ws.its	ime:			
Arbeitsgruppe:	r			
	eschrei			
OK Abbrechen				
	erung			
OK Abbrechen	Obemehmen aktivie			

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

Konfiguration der SitzungsSammlung

Ein Sessionhost benötigt weiter eine Collection zur Veröffentlichung:

📥 Server-Manager		>
Server-M	1anager • Remotedesktop- dienste • Sammlungen 🛛 • 🕄 l 🍢 Verwalten Tool	ls Ansicht Hilfe
Ubersicht Server Sammlungen	SAMMLUNGEN Filter ⓐ ▼ ⓐ ▼ ⓐ ▼	AUFGABEN stellen arbeiten AUFGABEN AUFGABEN stellen arbeiten AUFGABEN stellen stelle

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

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

🚡 Sammlung erstellen		– 🗆 X			
Namen für die Sammlung angeben					
Vorbemerkungen Sammlungsname Remotedesktop-Sitzungs Benutzergruppen Benutzerprofil-Datenträger Bestätigung Status	Für Benutzer wird bei der Anmeldung beim Server mit Web Access fr Sammlungsname "session" angezeigt. Name: RDS-RemoteApps Beschreibung (optional):	ir Remotedesktop der			
	< Zurück Weiter >	Erstellen Abbrechen			
🚡 Sammlung erstellen — 🗆 🗙					
RD-Sitzungshostse	erver angeben				
Vorbemerkungen Sammlungsname	Wählen Sie die RD-Sitzungshostserver im Serverpool aus, die dieser sollen.	Sammlung hinzugefügt werden			
Remotedesktop-Sitzungs Benutzergruppen	Serverpool	ewählt			
Benutzerprofil-Datenträger Bestätigung Status	Filter: Com Name IP-Adresse Betrieb WS-RDS1.ws.its	ws.ITS (1) RDS1			
	< >> 1 Computer gefunden 1 Com	nputer ausgewählt			
	< Zurück Weiter >	Erstellen Abbrechen			

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

è 5	Sammlung erstellen	-			×	
В	enutzergruppen	angeben				
	Vorbemerkungen	Fügen Sie die Benutzergruppen hinzu, die Zugriff auf die Sammlung haben sollen.				
	Sammlungsname	Benutzergruppen:				
	Remotedesktop-Sitzungs	WS\Domänen-Benutzer	Hi	inzufüge	n	
	Benutzergruppen			Entferne	n	
	Benutzerprofil-Datenträger					
	Bestätigung					
	Status					
		< Zurück Weiter > Erstellen		Abbrech	en	

Den Benutzerprofildatenträger konfiguriere ich später:

📥 Sammlung erstellen				-		×
Sammlung erstellen Benutzerprofil-Dat Vorbemerkungen Sammlungsname Remotedesktop-Sitzungs Benutzergruppen Benutzerprofil-Datenträger Bestätigung Status	enträger angeben Benutzerprofil-Datenträger speic Speicherort für die Sammlung. Benutzerprofil-Datenträger e Speicherort von Benutzerprof Maximale Größe (in GB): 20 Die Server in der Sammlung	chern Benutzerprofileinstellunge iktivieren fil-Datenträgern:	n und -daten an	n einem	zentrale	×
	Gruppe "Administratoren" a	auf dem Server sein.				
		< Zurück Weiter >	Erstelle	n	Abbrech	en

Beim Abschluss erhalte ich leider eine Fehlermeldung:

Vorbemerkungen	Die Sitzungssammlung wird	d erstellt. Je nach Größe der Sitzungssamm	ung kann dieser Vorga
Sammlungsname Remotedesktop-Sitzungs	Aktivität	Status	Status
Benutzergruppen Benutzerprofil-Datenträger	Sammlung erstellen		Erfolgreich
Bestätigung Status		 WS-RDS1.WS.ITS Der RD-Sitzungshostserver "WS-RDS1.WS.ITS" kann nicht konfiguriert werden. Der Vorgang ist ungültig. 	

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



📥 Serve	r-Manager		
\mathbf{E}	. ✓ Samm	nlungen • RDS-RemoteApps	• ② 🍢
■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	Übersicht Server Sammlungen RDS-RemoteAp	EIGENSCHAFTEN Eigenschaften der Sammlung Sammlungstyp Sitzung Ressourcen Remotedesktop Benutzergruppe WS\Domänen-Benutzer	VERBINDUNGEN Letzte Aktualisierung: 22.01.2017 10:11:52 <i>Filter</i> Vollqualifizierter Domânenname des Ser
		REMOTEAPP-PROGRAMME Veröffentlichte RemoteApp-Programme 0 insgesamt Der Remotedesktop wurde für die Benutzer der Sammlung veröffentlicht. RemoteApp-Programme veröffentlichen Die Veröffentlichung von RemoteApp-Programmen hat die Aufhebung der Veröffentlichung des Remotedesktops zur Folge.	
		HOSTSERVER Letzte Aktualisierung: 22.01.2017 10:11:52 Alle Server 1 AUFGABEN ▼ Filter Filter Servername Typ Virtuelle Desktops Neue Verbindungen zula WS-RDS1 RD-Sitzungshost n/v Wahr	

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

😫 Administrator: Windows PowerShell ISE					
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe					
2016-08-25 RDPublishedName.ps1 ×					
1 Import-Module RemoteDesktop 2 cd M:\AdminArea\Services\RDS\Konfiguration					
<pre>3 4 .\Set-RDPublishedName.ps1 -ClientAccessName rds.ws-its.de -ConnectionBroker ws-rds1.ws.its</pre>					
Set-RDPublishedName Succeeded.					
Set-RDPublishedName Succeeded.					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de If you are currently logged on to RD Web Access, please refresh the page for the change to take effect.					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de If you are currently logged on to RD Web Access, please refresh the page for the change to take effect.					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de If you are currently logged on to RD Web Access, please refresh the page for the change to take effect. PS M:\AdminArea\Services\RDS\Konfiguration>					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de If you are currently logged on to RD Web Access, please refresh the page for the change to take effect. PS M:\AdminArea\Services\RDS\Konfiguration>					
Set-RDPublishedName Succeeded. Old name: WS-RDS1.WS.ITS New name: rds.ws-its.de If you are currently logged on to RD Web Access, please refresh the page for the change to take effect. PS M:\AdminArea\Services\RDS\Konfiguration>					

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

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

Administrator: Windows PowerShell ISE					
Datei Bearbeiten Ansicht Tools Debuggen Add-Ons Hilfe					
1 🙆 🖬 🐇 1 🔪 🔊 🔍 🕨 📑 🔳 🐼 🖉 🔚 🖬 🖬 🖉					
2017-01-22 RDPublishedName.ps1 2015-02-16 Verbindungsname.ps1* X					
1 Import-Module RemoteDesktop					
2 3 Set-RDWorkspace -Name "RDS"					
Set-RDPublishedName Succeeded.					
Old name: W5-RDS1.W5.ITS					
New name: rds.ws-its.de					
If you are currently logged on to RD Web Access, please refresh the page for the change to take effect.					
PS M:\AdminArea\Services\RDS\Konfiguration> Import-Module RemoteDesktop					
PS M:\AdminArea\Services\RDS\Konfiguration> Set-RDWorkspace -Name "RDS"					
PS M:\AdminArea\Services\RDS\Konfiguration>					

Konfiguration der RDS-Website

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

Work Resourc	es rbindung	Web Access für Remotedesktop
		Hilfe
	Domäne\Benutzername: ws\stephan Kennwort:	
	 Sicherheit (<u>Erläuterung anzeigen</u>) Dies ist ein öffentlicher oder freigegebener Computer. Dies ist ein privater Computer. Warnung: Wenn Sie diese Option auswählen, bestätigen Sie, dass dieser Computer die Sicherheitsrichtlinien Ihrer Organisation erfüllt. 	
	Anmelden Zum Schutz vor unberechtigtem Zugriff tritt für die Sitzung von Web Access für Remotedesktop nach einem Zeitraum der Inaktivität automatisch eine Zeitüberschreitung ein. Wenn die Sitzung beendet wird, aktualisieren Sie den Browser, und melden Sie sich erneut an.	
Windows Server 2016		Microsoft



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

		💀 RDS - WS-ITS (1)
WS IT-Solutions		Hilfe
	Benutzername: ws\stephan Kennwort:	
	Sicherheit (<u>Erläuterung anzeigen</u>) O Dies ist ein öffentlicher oder freigegebener Computer.	
	Dies ist ein privater Computer. Anmelden	
Windows Server 2012 R2		Microsoft

Hier liegt das Verzeichnis:

- 🖓 📑 🖛 Web				_		×
Datei Start Freigeben Ansicht						~ 🕐
\leftarrow \rightarrow \checkmark \uparrow \Box \rightarrow Dieser PC \rightarrow SYSTEM (C:) \rightarrow Windows \rightarrow Web			~ Ū	"Web" durch	suchen	Q
rescache	^	, Name	^	Ä	nderung	sdatum
Resources		4K		1	6.07.2016	15:23
SchCache		RDWeb		2	2.01.2017	10:17
schemas		RDWeb-original		2	2.01.2017	09:38
security		Screen		1	6.07.2016	15:23
ServiceProfiles		Wallpaper		1	6.07.2016	15:23

Ein Verbindungsaufbau zeigt aber, dass beim Start der RDP-Session eine Sicherheitsabfrage erscheint. Das Zertifikat ist zwar vertrauenswürdig, aber mein Client vertraut den rdp-Dateien noch nicht. Dies hatte ich bisher mit einer GPO erreicht, in der ich den Fingerabdruck des verwendeten Zertifikates als vertrauenswürdig deklariert habe. Vom neuen Zertifikat muss ich also nur den neuen Fingerabdruck mit in die GPO eintragen: Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

RemoteApp und Desktops Verbindung mit einem Remote-PC hers	tellen Hilfe Abmeld	den	
Aktueller Ordner: /	X Remoteverbindung zu starten. Stellen Sie rtrauen, bevo der der Remotecomputer beschädigt werden. Stellen sie dem Herausgeber vertrauen. opverbindung nicht mehr anfordem Verbinden Abbrechen	Allgemein Details Zertifizierungspfad Anzeigen: Feld Wert Sperriisten-Verteilungs [1]Sperrlisten-Verteilung Galternativer Antragstell DNS-Name=rds.ws-its.de Galternativer Aussellern URL=http://www.startssl Galternativer Aussellern URL=http://www.startssl Galternativer Aussellern URL=http://www.startssl Galternativer Aussellern URL=http://schluss Fingerabdruckalgorithm shal Fingerabdruckalgorithm shal Boda 5c 02 ae 34 87 b1 06 54 39 21 27 a5 89 46 f7 d8 0f 8e	×
Windows Server 2012 R2	Micros	Eigenschaften bearbeiten In Datei kopieren	

Das ist die GPO:

📓 Gruppenrichtlinienverwaltung	_
📓 Datei Aktion Ansicht Fenster ?	
← → 2 m	
- C >	
Datei Aktion Ansicht ?	💭 SHA1-Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darste — 🔲 🗙
Festures 21 A is Remotedesktopyerbindungs-Client	SHA1-Fingerabdrücke von Zerüfikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen
Geräte- un SHA1-Fingerabdrücke von Einstellung	Vorherige Einstellung Nächste Einstellung
Ertifikaten angeben, die vertrauenswürdige RDP- Heimnetze vertrauenswürdige RDP- Den Deteine ver villeren Hennenden und stendenden	O Nicht konfiguriert Kommentar:
Internet Ex Herausgeber darstellen Distornetion Distornetion Distornetion Distornetion	Altiviat
Kamera Richtlinieneinstellung bearbeiten	Nic O Truck
□ Karten Anforderungen: E Speichern von Kennwörtern nicht zulassen	Nic O Deaktiviert
MDM Mindestens Windows Vista mit Mindestens Windows Vista mit B HAP er Gene dealkfürke von Zertifikaten angeben, die vertrau	Mindestens Windows Vista mit Service Pack 1
Microsoft Service Pack 1 Dev au Client deaktivieren Auf dem Clientomputer zur Fingabe von Anmeldeinformat	Nic
NetMeetir Beschreibung:	Nic Optionen: Hilfe:
OneDrive Mit dieSer Michtlinenenstellung Können Sie eine Liste von SHA1-	
Otionen	Kommagetrennte Liste von vertrauenswürdigen SUA1 7-4-Einefersenklichten: Kommagetrennte Liste von SHA1 A -Zertifikatfingerabdrücken (Secure-Hash-Algorithmus 1)
Portables I der vertrauenswürdige	angeben, in der vertrauenswürdige Herausgeber von RDP-
> Position u Herausgeber von RDP-Dateien	bcl/2ae348/b10b5439212/ab894bf/d8078q
Prasentatii Udinocecescoprotocon	Wenn Sie diese Richtlinieneinstellung aktivieren, sind alle Zweifikete wit einem SHA1. Einenscheltrick, der einem
Rand-UI Wenn Sie diese	Fingerabdruck in der Liste entspricht, vertrauenswürdig. Wenn
🗸 🛅 Remotede 🛛 Richtlinieneinstellung aktivieren,	ein Benutzer versucht, eine RDP-Datei zu starten, die durch ein vertrauenswürdiges Zertifikat signiert ist wird für Benutzer beim
Remot Sind alle Zertrikate mit einem	Starten der Datei keine Warnung angezeigt. Zeigen Sie die
Remot Fingerabdruck in der Liste	Zertifikatdetails an, und klicken Sie dann auf das Feld "Fingerabdruck", um den Fingerabdruck abzurufen.
A second	
8 Einstellung(en)	Wenn Sie diese Richtlinieneinstellung deaktivieren oder nicht konfigurieren, wird kein Herausgeber als vertrauenswürdiger
GPU_Server_DAC Windows-Komponenten/Windows-Remoteverwaltung (W	nde Herausgeber von RDP-Dateien behandelt.
GPO Server Logon Einstellungen	Hinweis:
GPO_Server_RDS Systemsteuerungseinstellungen	
GPO_Server_Win2016 Lokale Benutzer und Gruppen	OK Abbrechen Übernehmen
Bouchardina Contraction (Desktinier)	

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

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19



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

ध Internetinformationsdienste (IIS)-N	lanager
← → ♥ WS-RDS1 →	
Datei Ansicht ?	
Verbindungen	WITTP-Umleitung Geben Sie mit diesem Feature Regeln für das Umleiten von eingehenden Anforderungen an eine andere Datei oder eine URL an. Anforderungen zu diesem Ziel umleiten: https://rds.ws-its.de/rdweb Beispiel: http://www.contoso.com/sales Umleitungsverhalten Alle Anforderungen an eigentliches Ziel (und nicht relativ zum Ziel) umleiten Statuscode: Gefunden (302)

Konfiguration des RDS-Gateways

WS IT-Solutions

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



0	EIGENSCHAFTEN	-	VERBINDUNGEN	DHCP	
Ubersicht	Ligenschaften der Sammlung AUPGABEN	•	Letzte Aktualisierung: 22.01.2017 10:11:5	Dienste	
Server	Sammlungstyp Sitzung		Filter	DNS	
Sammlungen	Ressourcen Remotedesktop			Druckverwaltung	
RDS-RemoteAp	Benutzergruppe WS\Domänen-Benutzer		Vollqualifizierter Domanenname des Se	Ereignisanzeige	rlau
				Failovercluster-Manager	
				Gruppenrichtlinienverwaltung	
				Hyper-V-Manager	
				Internetinformationsdienste (IIS)-Manager	
				iSCSI-Initiator	
	REMOTEAPP-PROGRAMME			Komponentendienste	
	Veröffentlichte RemoteApp-Programme 0 insgesamt AUFGABEN	•		Laufwerke defragmentieren und optimieren	
				Leistungsüberwachung	
	Der Kemoteaesktop wurde für die Benutzer der Sammlung veröffentlicht.			Lokale Sicherheitsrichtlinie	
	RemoteApp-Programme veröffentlichen			Microsoft Azure-Dienste	
	Die Veröffentlichung von RemoteAnn-Programmen hat die Aufhehung der Veröffentlichung des Remotedesktons zur			Netzwerkrichtlinienserver	
	Folge.			ODBC-Datenquellen (32-Bit)	
				ODBC-Datenquellen (64-Bit)	
		Remote	desktopgateway-Manager	Remote Desktop Services	•
		Remote	desktop-Lizenzierungsdiagnose	Remotezugriffsverwaltung	
		Remote	desktoplizenzierungs-Manager	Ressourcen-Manager für Dateiserver	

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

Image: Section of the section of t	Ressourcenaut	torisierungsrichtlinien						
 ✓ ■ WS-RDS1 (Lokal) ✓ ■ Richtlinien ■ Verbindungsautorisierungsrichtlini ■ Ressourcenautorisierungsrichtlinit 	Mit einer Remot herstellen könn	edesktop-Ressourcenautoris en.	ierungsrichtlinie (RD-RAP) kö	nnen Sie die Netzwerkressourcen	(Computer) ar	ngeben, mit denen Be	enutzer über diesen Remoted	esktop-Gatewayserver eine Remoter
	Name	Benutzergruppen	Zulässige Ressourcen	Richtlinienpfad	Port	Status		
opennenning	RDG_AID	WS\Domänen-Benutzer	WS\Domänencomputer	Windows-Gruppe	3389	Aktiviert		
	RDG_RDC	WS\Domänen-Benutzer	RDG_RDCBComputers	Lokal	3389	Aktiviert		
				Eigenschaften von RDG_AII	DomainCom	puters	×	
				Allgemein Benutzergruppen	Netzwerkre	ssource Zulässige	Ports	
				Benutzer können Verbindung Remotedesktoogateway here einer Sicherhetsgruppe von Remotedesktoo-Severfam Geben Sie die für Remotebe der folgenden Aktionen austi	gen mit Netzw stellen. Zu der Active Directo rählen. nutzer verfügb ühren: ppe der Activu r tedesktopgate	erkressourcen über n Netzwerkressource ny-Domänendienster vare Netzwerkressou e Directory-Domänen sway verwaltete Grup	an n oder einer roce an, indem Sie eine ndienste auswählen Durchauchen ppe auswählen	
	RDG_AllDomainComputers Zugeordnete Benutzergruppen:		Ober Remotedesktopgat	ieway verwalti	ete Gruppenmitgliede	Durchsuchen		
	WS\Domäne	n-Benutzer		O Benutzer können Verbir	ndung mit belie	ebiger Netzwerkresso	urce herstellen	
					[ОК АЫ	brechen Obernehmen	

Konfiguration der RemoteApps

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



Server	sammungstyp sitzung		Filter	▼ (ii) ▼ (iii) Q	
Sammlungen	Ressourcen Remotedesktop				
▶ RDS-RemoteAp	Benutzergruppe WS\Domanen-Benutzer	a RemoteApp-Programme veröffentlichen	Vollouslifiziortor	DomBacanona das Sanars Romutras Sitrumasa — —	×
•		RemoteApp-Programme a	auswählen		
	REMOTEAPP-PROGRAMME Veroffentlichte RemoteApp-Programme 0 insgesamt	RemoteApp-Programme Wählen Sie or veröffentlich hinzuzufüge	lie RemoteApp-Programme au t werden sollen. Klicken Sie au n.	is, die in der Sammlung "RDS-RemoteApps" f "Hinzufügen", um der Liste ein RemoteApp-Progra	amm
	Der Remotedesktop wurde für die Benutzer	Fertigstellung	App-Programme werden aus	ws-RDS1.WS.ITS' autgetuilt.	
	RemoteApp-Programme ve		eApp-Programm	%SVSTEMDRIVE%\Program Files (x86)\Microsof	
	Die Veröffentlichung von RemoteApp-Programmen hat die Aufhe Folge.	Constraints of the second sec	ve Directory-Modul für Windc ve Directory-Verwaltungscent tecichnungs-Manager von Sky terfähiges Aktualisieren abase Compare 2016 enträgerebereinigung -Verwaltung 3 2 2016	SKYSTEMDRIVE%Windows/bystem32/windows/ SKYSTEMDRIVE%Windows/bystem32/windows/ SKYSTEMDRIVE%Windows/bystem32/windows/ SKYSTEMDRIVE%Windows/bystem32/windows/ SKYSTEMDRIVE%Windows/bystem32/windows/ SKYSTEMDRIVE%Windows/bystem32/wincexe SKYSTEMDRIVE%Windows/bystem32/wincexe SKYSTEMDRIVE%Windows/bystem32/wincexe SKYSTEMDRIVE%Windows/bystem32/wincexe	~
	HOSTSERVER Letzte Aktualisierung: 22.01.2017 10:11:52 Alle Server 1 insgesamt	Hinzufügen Vergewissen	 n Sie sich, dass das Programm	auf allen Remotedesktop-Sitzungshostservern in de	er
	Filter D (E) Virtuelle Desktops Neue Verbind		< Zurüc	k Weiter > Veröffentlichen Abbred	:hen

Konfiguration des Web Application Proxies

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

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

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

🔋 WS-RA1 🔋 WS-RA2 🗙		
Papierkorb		
- Amerikan	📕 🔁 🕼 = I	Zertifikatimport-Assistent
abmelden Sicherung Windows Update	Date Start Freigeben Ansicht	Willkommen Deser Assistent hift Ihnen beim Kopieren von Zertifikaten, Zertifikatvertrauenslisten und sperifisten von Datenträger in den Zertifikatspeicher. En von einer Zertifikatongestelle zusgestellte Zertifikat dent der Identitätbeetätigung. En enthält Informationen für den Datenschutz oder für den Aufbau ücherer Netwerkverbindungen. En Zertifikatspeicher ist der Systembereich, in dem Zertifikate speicher ur verden

• 🗷 I

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

) 🔄 🛃 Zertifikatimport-Assistent	X	0
Schutz für den privaten Schlüssel Der private Schlüssel	um die Sicherheit zu	
gewährleisten. Geben Sie das Kennwort für den privaten Schlüssel ein.		
Kennwort:		
Importoptionen: Hohe Sicherheit für den privaten Schlüssel aktivieren aktivieren, werden Sie immer dann, wenn der private Anwendung verwendet wird, zur Kennworteingabe a	. Wenn Sie diese Option 2 Schlüssel von einer ufgefordert.	
 Schlüssel als exportierbar markieren. Dadurch könne einem späteren Zeitpunkt sichern bzw. überführen. Alle erweiterten Eigenschaften mit einbeziehen 	n Sie Ihre Schlüssel zu	
	Weiter Abbrechen	

Den privaten Schlüssel markiere ich dabei als nicht exportierbar.

VS IT-Solutions

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

Unbenannt1.ps1 2017-01-22 Austausch RDS-Zertifikat.ps1 ×							
1 Get-ChildItem -Path Cert:\LocalMachine\My 2 Where-Object {\$subject -like '*rds*'} 3 Format-Table -Property Thumbprint,Subject,N	NotBefore						
5 get-WebApplicationProxyApplication -Name RDS 6 Set-WebApplicationProxyApplication -ExternalCer	⁴ get-WebApplicationProxyApplication -Name RDS 6 Set-WebApplicationProxyApplication -ExternalCertificateThumbprint '8BDA5C02AE3487B10654392127A58946F7D80F8E'						
٢							
PS C:\Windows\system32> Get-ChildItem -Path Cert:\LocalMa Where-Object {\$subject -like '*rds*'} Format-Table -Property Thumbprint,Subject,NotBefo Thumbprint	uchine\My ore Subject	NotBefore					
EAA63ABC7C2C6E1D544F75B0360469C55F399446 D60B05E28A7A1D322075444D56A88E0429921464 8BDA5C02AF3487E10654392127A58946F70806F8E 3405B0B9D51E7F1D2FBAD879EE1DC096C755F7EE	CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val CN=rds.ws-its.de, OU=PositiveSSL, OU=Domain Control Val CN=rds.ws-its.de, C=DE CN=rds.ws-its.de, OU=PositiveSSL Trial, OU=Domain Contr	19.10.2015 02:00:00 19.07.2014 02:00:00 22.01.2017 09:18:02 22.06.2014 02:00:00					
PS C:\Windows\system32> get-WebApplicationProxyApplicatio Set-WebApplicationProxyApplication -ExternalCertifica	n -Name RDS hteThumbprint '8BDA5C02AE3487B10654392127A58946F7D80F8E'						
PS C:\Windows\system32>							

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

Remotezugriffs-Verwaltungskonsole									
Konfiguration VPN	VERÖFFENTLICHTE V Alle veröffentlichten Web	VERÖFFENTLICHTE WEBANWENDUNGEN Alle veröffentlichten Webanwendungen [3 insgesamt							
Webanwendungsproxy	Filter	م							
Dashboard									
Worgangsstatus	Name	Externe URL	URL des Back-End-Servers	Vorauthentifizierung					
Remoteclientstatus	OWA	https://email.ws-its.de/	https://email.ws.its/	PassThrough					
Remoteclientstatus Berichterstellung	OWA PRTG	https://email.ws-its.de/ https://monitor.ws-its.de/	https://email.ws.its/ https://prtg.ws.its/	Pass Through Pass Through					
Remoteclientstatus Berichterstellung Image: Comparison of Compariso	OWA PRTG RDS	https://email.ws-its.de/ https://monitor.ws-its.de/ https://rds.ws-its.de/	https://email.ws.its/ https://prtg.ws.its/ https://rds.ws-its.de/	PassThrough PassThrough PassThrough					

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

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 WS IT-Solutions 2017-01-19 🐻 RDS - WS-ITS (1) WS IT-Solutions Hilfe Abmelden RemoteApp und Desktops | Verbindung mit einem Remote-PC herstellen Aktueller Ordner: / A хI 0 V Access 2016 Excel 2016 Outlook 2016 PWS-Privat Visio 2016 Internet PowerPoint PWS-Kunden Explorer Server-2016 Explorer Manager w Word 2016 × ages/de-DE Nerbindung mit "rds.ws-its.de" wird herges... _ Х vat 🔻 RemoteApp Wird gestartet 400 Explorer Details einblenden Abbrechen RemoteApp und Desktops Verbindung mit einem Remote-PC herstellen Aktueller Ordner: / 0 A х Access 2016 Excel 2016 Explorer PowerPoint PWS-Kunden PWS-Privat Internet Outlook 2016 Explorer 2016 w Word 2016

Konfiguration der Benutzerdatenträger

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

📙 🗹 📜 🔻 🛛 Benutzer				
Datei Start Freigebe	n Ansicht			
← → ~ ↑ 📜 > Di	eser PC > SYSTEM (C:) > Benutzer	>		
★ Schnellzugriff	Name	Änderungsdatum	Тур	Größe
Deskton	Administrator	26.12.2016 19:16	Dateiordner	
Malthan Stanhan	Öffentlich	12.09.2016 13:56	Dateiordner	
Waither, Stephar	🔊 stephan-ad	26.01.2017 07:08	Dateiordner	10.483.708
S Dieser PC	ETEMP	24.01.2017 17:50	Dateiordner	
SYSTEM (C:)				
Admin				

Die Konfiguration kann in den Einstellungen der Sitzungssammlung vorgenommen werden:

 Übersicht	EIGENSCHAFTEN Eigenschaften der Sam	mlung		AUF	GABEN 🔻	VERBINDUNGEN Letzte Aktualisierung: 26.01.2017 07:17:39 Alle	e Verbindungen 2 in	nsgesan
Übersicht Server Sammlungen RDS-RemoteAp	Eigenschaften der Sam Sammlungstyp Eigenschaften der Sam Sammlungstyp Ressourcen Benutzergruppe RemoteApp-PROGRAM Letzte Aktualisierung: 26.01.20 Filter RemoteApp-Programmame Access 2016 Excel 2016 Explorer Internet Explorer Outlook 2016 PwS-Kunden	Mung Sitzung RemoteApp-Prog WS/Domanen-Be 17 07:09:54 Ven 17 07:09:54 Ven 17 Alias MSACCESS EXCEL explorer iexplorer iexplorer iexplorer POWERPNT PWSafeKunder	offentlicht (IIII)	RDS-RemoteApps Eigenschaften	Benutzerprofi Benutzerprofil-Data an einem zentralen Datenträger in eine Voltzugriff auf die B muss zur lokalen Ai Speicherort: [ws-hv1.ws.tb] Maximale Größe 10 Einstellungen fü Einstellungen fü Folgende Ore	ini-Datenträger enträger bieten Benutzern die Möglichkeit, Einste off zugen von die Möglichkeit, Einste von zugenbern. Sie können Ordnerumleitung ur sammlung aktiveren. Die Sevore in der Sammlung renträger aktivieren. Profite/Disks\$ (in GB): reinstellungen und -daten auf dem Benutzerprofidiner Profite/Disks\$ (in GB): reinstellungen und -daten auf dem Benutzerprofidiner ausschließen: Pfad Typ	Verbindungen 2 in Verbindungen und Ordner Illungen und Ordner Ind Benutzerprofil- Ing müssen er aktuelle Benutzer hören. II-Datenträger speich Hinzufügen Entfernen	x
	HOSTSERVER Letzte Aktualisierung: 26.01.20	17 07:09:54 Alle	Server		O Nur folgende	e Ordner auf dem Benutzerprofil-Datenträger spe	eichern	~

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

堤 🕑 📜 ∓ profiledisks Datei Start Freigeben	\$ Ansicht				
; ← → ∽ ↑ 💄 > Net	zwerk > ws-hv1.	ws.its > profiledisks\$			
: 🖈 Schnellzugriff	Name	^	Änderungsdatum	Тур	Größe
 Desktop Walther, Stephan - A Dieser PC Bibliotheken 	UVHD-S-1- UVHD-S-1- UVHD-S-1- UVHD-S-1-	5-21-724898266-3745665200 5-21-724898266-3745665200 5-21-724898266-3745665200 plate.vhdx	23.01.2017 20:18 26.01.2017 07:21 26.01.2017 07:29 22.01.2017 13:46	Festplatten-Image Festplatten-Image Festplatten-Image Festplatten-Image	200.704 KB 233.472 KB 233.472 KB 135.168 KB
I Netzwerk		💄 Eigenschaften von profiled	sks\$ (\\ws-hv1)	×	
 ws-hv1 dhcpaudit profiledisks\$ ws-hv1.ws.its Systemsteuerung Papierkorb 		Vorgängerversionen Allgemein Objektname: \\ws-hv1\profil Gruppen- oder Benutzernamen: & SYSTEM & LD-Admins-Server (WS\LD & Domänen-Admins (WS\Do & WS-RDS15	Anpassen Netzwerk edisks\$ -Admins-Server) mänen-Admins)	Klassifizierung Sicherheit	
4 Elemente		Klicken Sie auf "Bearbeiten", un Berechtigungen zu ändern. Berechtigungen für "WS-RDS1\$ Vollzugriff Åndern Lesen, Ausführen Ordnerinhalt anzeigen	die "Zulassen V V V V	Bearbeiten Verweigern	
1016 ffice_2013 🗸 🗸		Lesen Schreiben Spezielle Berechtigungen	~		

Weitere GPOs:

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

_

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

PO_Clients		
en ermittelt am: 26.01.2017 07:22:48		
puterkonfiguration (Aktiviert)		
chtlinien		
Nindows-Einstellungen		
Sicherheitseinstellungen		
Administrative Vorlagen		
Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher	abgerufen.	
System		
System/Anmelden		
System/Dateiklassifizierungsinfrastruktur		
System/Delegierung von Anmeldeinformationen		
System/Remoteunterstützung		
Windows-Komponenten/Remotedesktopdienste/Remotedesktopverb	indungs-Client	
Richtlinie	Einstellung	Kommentar
RDP-Dateien von gültigen Herausgebern und standardmäßige RDP- Einstellungen des Benutzers zulassen	Aktiviert	
RDP-Dateien von unbekannten Herausgebern zulassen	Aktiviert	
SHA1-Fingerabdrücke von Zertifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen	Aktiviert	
Kommagetrennte Liste von vertrauenswürdigen SHA1-Zertifikatfingera	bdrücken:	8bda5c02ae3487b10654392127a58946f7d80f8e
Windows Konsonantes (Disklinies 67, die automatische Windowskie)	-	
windows-tomponenten/rsichtlinien für die automatische Wiedergab	8	
Windows-Komponenten/Windows-Remoteverwaltung (Windows Rem	ote Management, Wi	inRM)/WinRM-Dienst

Für die RDS-Benutzer werden folgende Einstellungen verwendet:

GPO_Benutzer		
Daten ermittelt am: 26.01.2017 07:30:14		
Computerkonfiguration (Deaktiviert)		
Keine Einstellungen definiert		
Benutzerkonfiguration (Aktiviert)		
Richtlinien		
Windows-Einstellungen		
Sicherheitseinstellungen		
Administrative Vorlagen		
Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher a	bgerufen.	
Windows-Komponenten/Anlagen-Manager		
Windows-Komponenten/Internet Explorer/Internetsystemsteuerung/S	icherheitsseite	
Windows-Komponenten/Remotedesktopdienste/RemoteApp- und Des	sktopverbindungen	
Richtlinie	Einstellung	Kommentar
Standardverbindungs-URL angeben	Aktiviert	
Standardverbindungs-URL:		https://rds.ws-its.de/rdweb/feed/webfeed.aspx
Windows-Komponenten/Remotedesktopdienste/Remotedesktopverbi	ndungs-Client	
Richtlinie	Einstellung	Kommentar
SHA1-Fingerabdrücke von Zettifikaten angeben, die vertrauenswürdige RDP-Herausgeber darstellen	Aktiviert	
Kommagetrennte Liste von vertrauenswürdigen SHA1-Zertifikatfingerab	drücken:	8bda5c02ae3487b10654392127a58946f7d80f8e

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

GPO_9	Server_RDS		
Daten erm	nittelt am: 26.01.2017 07:30:56		
Computer	rkonfiguration (Aktiviert)		
Richtlin	nien		
Admin	nistrative Vorlagen		
	Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher a	abgerufen.	
S	ystem/Benutzerprofile		
	Richtlinie	Einstellung	1
	Benutzerprofile, die älter als eine bestimmte Anzahl von Tagen sind, beim Systemneustart löschen	Aktiviert	
	Benutzerprofile löschen, die älter sind als (Tage)		10
S	ivstem/Delegierung von Anmeldeinformationen		
	Richtlinie	Einstellung	
	Delegierung von Standardanmeldeinformationen zulassen	Aktiviert	
	Server zur Liste hinzufügen:		
	TERMSRV/*.ws.its		
	TERMSRV/*.ws-its.de		
	Betriebssystemstandards mit vorheriger Eingabe verknüpfen		Aktiviert
W	Vindows-Komponenten/Remotedesktopdienste/Remotedesktopsitzu	ngs-Host/Druckerumleitung	
	Richtlinie	Einstellung	1
	Nur Standardclientdrucker umleiten	Aktiviert	
W	Vindows-Komponenten/Remotedesktopdienste/Remotedesktopsitzu	ngs-Host/Sicherheit	
	Richtlinie	Einstellung	1
	Bei der Verbindungsherstellung immer zur Kennworteingabe auffordem	Deaktiviert	
	Benutzerauthentifizierung mit Authentifizierung auf Netzwerkebene ist für Remoteverbindungen erforderlich	Aktiviert	
	Verschlüsselungsstufe der Clientverbindung festlegen	Aktiviert	
	verschlusselungsstufe		Hochste Stufe
	verschlusselungssture Wählen Sie die Verschlüsselungsstufe aus der Dropdownliste aus.		Hochste Stufe
w	verschlusselungssture Wählen Sie die Verschlüsselungsstufe aus der Dropdownliste aus. Vindows-Komponenten/Remotedesktopdienste/Remotedesktopverb	indungs-Client	Hochste Stufe
W	Verschlusselungssture Wählen Sie die Verschlüsselungsstufe aus der Dropdownliste aus. Vindows-Komponenten/Remotedesktopdienste/Remotedesktopverb Richtlinie	indungs-Client Einstellung	Hochste Stufe

Absicherung der RDS-Infrastruktur

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

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

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

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

Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

	<u>Projects</u> > <u>SSL Server Test</u> > rds.ws-its.de					
SSL Repo	rt: rds.ws-its.de (87.1	38.129.242)				
Assessed on: Thu, 26	3 Jan 2017 06:36:16 UTC <u>Hide</u> <u>Clear cache</u>				<u>Scan A</u>	noth
Summa	ary					
	Overall Rating					
		Certificate				
		Protocol Support				
		Key Exchange				
		Cipher Strength				
					•	

<u>Clientanbindung</u>

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

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

😹 RemoteApp- und Desktopverbindunger	1			_		\times
← → × ↑ 🍓 « Alle Systemsteue	rungselemente > RemoteApp-	und Desktopverbindungen	νŪ	Systemsteuerung	durchsuchen	P
Startseite der Systemsteuerung Auf RemoteApp und Desktops	Verbindung mit Desktop	s und Programmen an Ihrem Arbeit	splatz he	erstellen		?
zugreifen	RDS (Standardverbing	dung)	I	Eigenschaften		
	Diese Verbindung enthält Folgendes:	0 Programme und 0 Desktops				
		Sie können auf diese Ressourcen über die Startseite zugreifen.				
	Verbindungsstatus:	Nicht verbunden				
	Neuestes Update:	Samstag, <mark>7. Januar 2017 um 00:51</mark>		Details anzeigen		
	Erstellungsdatum:	Freitag, 16. Dezember 2016 um 13:42				
		R	Erneut ei	ne Verbindung mit "f	RDS" herstelle	n
			Alle Verb	indungen trennen		
RemoteApp- und D			RemoteA	pp- und Desktopver	26.01.20	fnen 17 - (1



Migration der RDS-Infrastruktur von 2012 R2 auf 2016 2017-01-19

📜 Eigenschaften	
\leftarrow \rightarrow \checkmark \uparrow 📜 « RemoteApp- und Des	sktopverbindungen > Eigenschaften
Eigenschaften anzeigen oder Verb	indung aktualisieren
Eigenschaften	
Verbindungsname:	RDS
Verbindungs-URL:	https://rds.ws-its.de/rdweb/feed/webfeed.aspx
Erstellungsdatum:	Freitag, 16. Dezember 2016 um 13:42
Verbindungen werden in regelmäßigen Verbindung jetzt aktualisieren möchten Jetzt aktualisieren Ergebnisse der neuesten Updates	Abständen automatisch aktualisiert. Wenn Sie diese , klicken Sie auf "Jetzt aktualisieren".
Updateversuch am:	Samstag, 7. Januar 2017 um 00:51
Die Aktualisierung war erfolgreich.	Die Verbindung wurde erfolgreich aktualisiert.
	ОК

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

Windo	ows-Sicherheit	×
Anr	neldeinformationen eingebe	n
"rds. Prog	ws-its.de" sowie den davon bereitgeste rammen und Desktopressourcen verw βenutzername	ellten RemoteApp- endet.
	Kennwort	
	Domäne: WS	

Danach aktualisiert sich das System automatisch. $\ensuremath{\textcircled{\sc o}}$