

<u>Inhalt</u>

Einleitung	2
Zielsetzung	2
Bereitgestellte Services	2
Web Application Proxy (WAP) & Active Directory Federation Service (ADFS)	2
Network Policy Service (NPS)	2
VPN-Service	2
Planung der Migration	2
Migration NPS	2
Aufbau der neuen VM	2
Installation der Rollen und Features	6
Migration der Rolle NPS	7
Konfiguration des Serverzertifikats	11
Konfiguration der Protokollierung	14
Austausch des NPS	16
Funktionsprüfung	17
Nacharbeiten	21
Datensicherung	21
Bereinigung der VMs	25
Windows Updates	28
Monitoring	29
Abhängigkeit zur PKI	29



<u>Einleitung</u>

<u>Zielsetzung</u>

Meine Serverumstellung auf Windows Server 2019 geht in die nächste Runde. Dieses Mal sind die beiden Server WS-RA1 und WS-RA2 dran. Beide laufen aktuell unter Windows Server 2016 als virtuelle Maschinen. Im folgenden Abschnitt prüfe ich, welche Services auf den Servern laufen und wie ich diese migrieren werde.

Bereitgestellte Services

Web Application Proxy (WAP) & Active Directory Federation Service (ADFS)

Die Umstellung auf den HAProxy habe ich bereits im Oktober durchgeführt und in einem anderen Artikel beschrieben. Diese spielt hier also keine Rolle mehr.

Network Policy Service (NPS)

Dazu stellt der Server WS-RA1 noch einen Network Policy Service (**NPS** – auch als Radius Server bekannt) bereit. Diesen nutzt ein WLAN-Accesspoint für WPA2-Enterprise-Anmeldungen meiner Clients. Die Funktion wird weiter benötigt und muss daher auf einen neuen Server migriert werden. Dabei halte ich mir eine Erweiterung auf eine hochverfügbare Lösung offen.

Die Migration wird mittels Wipe & Load vorgenommen, da ich aktuell keine Hochverfügbarkeitsanforderung gestellt habe. Für den Wechsel ist eine Downtime erforderlich.

VPN-Service

Die Namen der beiden Server habe ich aus dem Servicenamen RemoteAccess abgeleitet. Ich nutzte die Server als VPN-Server für die Einwahl von extern.

Die Formulierung in der Vergangenheitsform deutet es schon an: Ich nutze seit Ewigkeiten kein VPN mehr für die Arbeiten von außen. Diese Funktion bilde ich über meine Remote Desktop Services dank des RD-Gateways ab. Der Service VPN wird also nicht mehr benötigt und kann einfach entfernt werden.

Planung der Migration

Damit sind die Arbeitsschritte für die komplette Migration klar:

- Schritte im vorherigen Artikel
 - Zuerst entferne ich alle nicht mehr benötigten Services und deren Konfigurationen in der richtigen Reihenfolge.
 - Schritte in diesem Artikel
 - Danach migriere ich den Service NPS auf einen neuen Windows Server 2019 mit dem Namen WS-NPS1.
 - Zuletzt entferne ich die beiden alten Server aus meiner Infrastruktur..

Für die Migration des NPS werde ich den neuen Server neben dem alten synchron aufbauen. Der eigentliche Austausch wird durch die Übergabe der alten IPv4-Konfiguration an den neuen Server vorgenommen. Denn nur über diese IPv4 findet der WLAN-AccessPoint den NPS-Server. Damit spare ich mir die Rekonfiguration des WLAN-AccessPoints und die Anpassung der Firewall-Ausnahmen. Und ich könnte auch schnell wieder auf den alten Server zurückschwenken, indem ich die IP-Änderung wieder zurücknehme. Ein Rollback-Szenario ist immer gut.

Die Vorarbeiten sind bereits abgeschlossen. Dazu zählt die Entfernung des Web Application Proxy Clusters. Diese habe ich in einem anderen Artikel beschrieben. In diesem geht es daher nur noch um die Entfernung der beiden alten Server und um die Migration meines Network Protection Services (NPS)

Migration NPS

<u>Aufbau der neuen VM</u>

WAP, ADFS und VPN sind bereits entfernt. So bleibt nur noch die Rolle NPS. Diese möchte ich auf einen neuen Server migrieren. Den Namen leite ich aus der Funktion ab: WS-NPS1. Mit der Ziffer 1 halte ich die Option einer späteren



Skalierung um einen weiteren Server WS-NPS2 offen. Damit könnte ich einen hochverfügbaren Radius-Service konfigurieren.

Den neuen Server baue ich als VM in meinem Hyper-V-Host auf. Dazu kopiere ich zuerst ein Basefile (eine VHDX mit einem vorbereiteten Betriebssystem) in das VM-Verzeichnis. Diese VHDX enthält Windows Server 2019 mit der grafischen Oberfläche. Leider kann laut Microsoft der NPS-Service nicht auf einem Server Core betrieben werden:

 → × ↑	C > Tier-Gold (V:) > Hyper-V > WS-NPS1				
📌 Schnellzugriff	Name	^	Änderungsdatum	Тур	Größe	
📃 Desktop						Dieser Ordner ist lee
🤱 Walther, Stephan - T1						
🖉 💻 Dieser PC						
> 🏪 System (C:)						
> 👝 Daten (D:)		20% abgeschlossen			×	
> 🛖 Freigaben (M:)		,,				
🗸 👝 Tier-Gold (V:)		Ein Element wird von	Base nach WS-NPS1 kopiert			
Hyper-V		20% abgeschlos	sen	п	×	
> WS-ATA						
> WS-CM			Ge	schwindigkeit: 192 ME	B/s	
> WS-DC1						
> KVS-EVIL1		New				
> WS-FS1		Restdauer: Ungefähr (vnax i0 Sekunden			
> WS-MM		Verbleibende Element	e: 1 (10,4 GB)			
> WS-MX1		-				
WS-NPS1		(Weniger Details				
> WS-PFS1a						
> WS-RA1						
> WS-RDS1						
> 🛖 Tier-Silber (W:)						
🗧 🔒 Bibliotheken						
🖉 💣 Netzwerk						
🗸 💻 ws-hv3						
~ 🖵 w\$						
Base						
> Hyper-V						
					-	

Dann erstelle ich eine neue VM mit den passenden Spezifikationen. Der NPS-Service braucht nicht viel:



WS IT-Solutions

WSHowTo –Migration des NPS 2019-12-31 Migration auf Windows Server 2019

Dann bekommt die VM ihr Startsignal. Windows Server 2019 beginnt seine Erkennung und Ersteinrichtung:



Währen dessen bereite ich ein neues Computerobjekt im Active Directory vor:

WS IT-Solutions

Active Directory-Benutzer und -Computer					
Datei Aktion Ansicht ?					
🗢 🔿 📶 🗊 🗊 🖻 🗟 🖬 🕷 📚	i 🝸 🗾 🐍				
 Active Directory-Benutzer und -Computer [WS-DC1.ws.it Gespeicherte Abfragen Gespeicherte Abfragen Gespeicherte Abfragen Computers Computers Domain Controllers ForeignSecurityPrincipals Keys LostAndFound Managed Service Accounts Microsoft Exchange Security Groups Program Data System Users G AdminArea G AdminArea E Clients E Exchange-Objekte Gruppen 	Name WS-CA1 WS-CM WS-DPM WS-FS1 WS-FS2 WS-RA1 WS-RA2 WS-WAC		Typ Computer Computer Computer Computer Computer Computer	Objektverwaltung zuwei Verschieben Suchen	Beschreibung
 Cluster Cluster Server-HyperV Server-JB Server-MX Server-RDS Server-Standard Microsoft Exchange System Objects MTDS Quotas TPM Devices 		Computer Kontakt Gruppe InetOrgPerson msDS-ShadowPrincipalContainer msExchDynamicDistributionList msImaging-PSPs MSMQ-Warteschlangenalias Organisationseinheit Drucker Benutzer Freigegebener Ordner		Neu Alle Aufgaben Aktualisieren Liste exportieren Ansicht Symbole anordnen Am Raster ausrichten Eigenschaften Hilfe	>

Für den Domain Join delegiere ich das Recht an einen Setup-Adminaccount:



Nach der Eingabe eines Passwortes für den lokalen Admin kann der Server konfiguriert werden. Ich benenne das Betriebssystem um:



Systemeigenschaften Ändern des Computernamens bzw. der Domäne	×	ver	• 3) 🚩 Verwalten Tools Ansich	ht l
Sie können den Namen und die Mitgliedschaft des Comput ändem, Anderungen wirken sich möglicherweise auf den Zi auf Netzwerkressourcen aus.	ers Computers			AUFGABEI	N 🕶
Computername: WS-NPS1	oder	N-LVKQE870CUM)RKGROUP		Zuletzt installierte Updates Windows Update Zuletzt auf Updates geprüft	09.08 Nur U 09.08
Vollständiger Computername: WS-NPS1 Weitere	Ändern des Comp	uternamens bzw. der Domäne		Windows Defender Antivirus	Echtz
Mitglied von O Domäne:	Der Cor werden werden	mputer muss neu gestartet 1, damit die Änderungen wirksam 1.	ishiq	Verstärkte Sicherheitskonfiguration für IE Zeitzone	Aus (UTC-
Arbeitsgruppe: WORKGROUP	Speichern Sie alle Pr	Sie alle geöffneten Dateien, und schließen ogramme vor dem Neustart.	ang	FIGURED	00430
OK Abbrech		ОК		Prozessoren Installierter Arbeitsspeicher (RAM) Speicherplatz inspesamt:	AMD 2 GB

Und nach dem Neustart darf der Server der Domain beitreten:

Andem des computernamens bzw. der born	ine X	ALIEGABE	N
Sie können den Namen und die Mitgliedschaft de ändem. Änderungen wirken sich möglicherweise a auf Netzwerkressourcen aus.	Computers uf den Zugriff 21 Zuletzt in DOUD We down	Istallierte Updates	09.
Computername:	oder Zuletzt a	update uf Updates geprüft	09.
WS-NPS1	Windows-Sicherheit X		
Vollstandiger Computername: WS-NPS1	Ändern des Computernamens bzw. der	Defender Antivirus	Ech
	Domäne	e Sicherheitskonfiguration für IE	Aus
Mitglied von Omäne: ws.its	Geben Sie Namen und Kennwort eines Kontos ein, mit dem Sie dieser Domäne beitreten dürfen.	ID	(UT 004
O Arbeitsgruppe: WORKGROUP	ws\admin-setup	ren	AM
	••••••	er Arbeitsspeicher (RAM)	2 G
OK	1	platz insgesamt:	99,

Das sind alles Standardaufgaben. Eigentlich gehört auch die IP-Konfiguration dazu. Aber diese kommt für den Schwenk des NPS erst später.

Installation der Rollen und Features

Nun installiere ich die Rollen und Features. Das ist ebenfalls eine Standardaufgabe:

Assistent zum Hinzufügen von	Rollen und Features	-		×
nstallationsauswa	ahl bestätigen	W	ZIELSER\ 5-NPS1.ws	(ER Lits
Vorbereitung	Klicken Sie auf "Installieren", um die folgenden Rollen, Rollendienste und Features auf dem ausgewählten Server zu insta	llieren.		
Installationstyp	Zielserver bei Bedarf automatisch neu starten			
Serverauswahl	Optionale Features (z. B. Verwaltungstools) können auf dieser Seite angezeigt werden, da sie automatisch ausgewählt wu	irden. W	enn Sie	
Serverrollen	diese optionalen Features nicht automatisch installieren möchten, klicken Sie auf "Zurück", um die entsprechenden Kont deaktivieren	ollkästel	hen zu	
Features				
Netzwerkrichtlinien- und	Netzwerkrichtlinien- und Zugriffsdienste			
Bestätigung	Remoteserver-Verwaltungstools			
Ergebnisse	Featureverwaltungstools System Insights Module for Windows PowerShell			
	Rollenverwaltungstools			
	Tools für Netzwerkrichtlinien- und Zugriffsdienste			
	System Insights			
	Windows Server-Sicherung			

Das war kein Problem.

Migration der Rolle NPS

In meinem alten NPS-Server gibt es die Konfigurationen in der Konsole zu sehen. Bei mir ist es nicht viel. Das könnte ich eigentlich sogar einfach im neuen Server abtippen. Aber in großen Umgebungen ist das keine Option. Also wird das professioneller gehen dürfen. Hier ist eine Regel für mein WLAN:

Netzwerkrichtlinienserver				– 🗆 X
Datei Aktion Ansicht ?				
🗢 🄿 🙋 📰 🚺 🖬				
NPS (Lokal) Clients und -Serve Richtlinien Verbindungsanforderur Netzwerkrichtlinien Kontoführung	Verbindungsanforderungsrichtlinien Mithile von Richtlinien für Verbindungsanford werden. Richtlinienname	rungen kann festgelegt werden Status Verarbeitung	ob Verbindungsanforderungen lokal verarbeitet sreihenfolge Quelle	oder an RADIUS-Remoteserver weitergeleitet
> 🜉 Vorlagenverwaltung	Secure-WLAN	Aktiviert 1	Nicht angegeben	
			inu is digogoodi	
	Bedingungen - Wenn die folgenden Bedingungen er	üllt sind:		
	Bedingung Wert			
	Einstellungen - Dann werden folgende Einstellungen	angewendet:		
	Einstellung Wert			
< >				

Und das ist der eine WLAN-AccessPoint:



Microsoft hat eine Export-Funktion eingebaut. Diese nutze ich für den Transfer der Konfiguration. Wichtig ist aber, dass nach dem Export keine Änderungen am Altsystem mehr vorgenommen werden:

Netzwerkrich	itlinienserver					-		×				
Datei Aktion	Jatei Aktion Ansicht ?											
🗢 🔿 🔯 📷												
🚳 NPS (Lokal)	Verbindungsanforderungsr	ichtlinien										
> 🧮 RADI	Konfiguration importieren											
🗸 🧾 Richt	Konfiguration exportieren	ür Verbindungsanforderunger	kann fest	gelegt werden, ob Verbindur	ngsanforderungen lokal verarbeitet oder an RADIUS-Remotese	erver weite	argeleitet					
📑 Vi												
🚞 N	NPS-Dienst starten											
Nonte	NPS-Dienst beenden		Status	Verarbeitungsreihenfolge	Quelle							
> 🜉 Vorla	Server in Active Directory registrieren		Aktiviert	1	Nicht angegeben							
		· alle Benutzer verwenden	Aktiviert	1000000	Nicht angegeben							
	Eigenschaften											
	Hilfe											

Zwischen den Radius-Clients und dem Server wird verschlüsselt kommuniziert. Der Schlüssel wird im Klartext in der Exportdatei liegen. Das ist bei mir aber kein Problem, da die Datei nur für Administratoren sichtbar sein wird, die auch den Export erstellen können:





Der Assistent benötigt nur noch den Speicherpfad:

Netzwerkrichtliniens	erver			- 🗆 X
Datei Aktion Ansich	nt ?			
	NPS-Konfiguration exportieren		>	<
NPS (Lokal) ADIUS-Clients u	← → · · ↑ 📴 > Dieser PC → SYSTEM (C:) → Admin → Radius	5 V	"Radius" durchsuchen	
 Richtlinien Verbindungsi 	Organisieren 🔻 Neuer Ordner		8== ◄ (?	-Kemoteserver weitergeleitet
Sontoführung	Active Directory Name Admin System32 Desktop Walther, Stephar Dieser PC SYSTEM (C:) Admin PSTranscrip Radius	Änderungsdatum Ty	p Größe	
	Dateiname: config.xmi Dateityp: XML-Dateien (*.xml)		Speichern Abbrechen	
	Einstellung Wert			

Die Daten werden als xml-Datei gespeichert:

📕 🛃 🥃 🗸 Admin						-	×
Datei Start Freigeben Ansicht							~ 🕐
← → × ↑ 📙 > Netzwerk > ws-np	s1 → c\$ → Admin				~ Ō	"Admin" durchsuchen	P
a Walther, Stephan - T1 🔷	Name	Änderungsdatum	Тур	Größe			
💻 Dieser PC	PSTranscript	31.12.2019 17:18	Dateiordner				
SYSTEM (C:)	e config.xml	31.12.2019 17:19	XML-Dokument	68 KB			
PSTranscript							
Radius							
Benutzer							
CRLD							
inetpub							
PerfLogs							
Program Files (x86)							
Programme							
Windows							
🛖 Freigaben (M:)							
🐂 Bibliotheken							
Artzwerk							
ws-nps1							
cS							
Admin							



Während der alte NPS weiterläuft, importiere ich die xml-Datei im neuen Server. Hier hat sich mit Windows Server 2019 nicht wirklich etwas verändert. Daher erwarte ich auch eine entsprechende Kompatibilität der Exportdatei:

Netzwerkrichtlinienserve						- 🗆 ×
Datei Aktion Ansicht	1					
🗢 🔿 🙋 📰 🛛 🖬						
NPS (Lokal)	Verbindungsanforderungsrid	chtlinien				
RADIUS-Clients und -	erve	für Verbindungsanforderungen kann	festgelegt werden, ob Verbindungsa	nforderungen lokal verarbeitet oder an RADIU	S-Remoteserver weitergeleitet werden.	
RADIUS-Remotese	rverg					
✓ I Richtlinien	. Diskilations amo	Ci-tu	Versteit - amittanfalaa () u	-8-		
Verbindungsamor Verbindungsamor	n Hichtlinienname	ir alle Renutzer verwenden Aktiv	is verarbeitungsreinenioige oo ie# 999999 Nic	elle ht annenehen		
Nontoführung	THINK CAN BE AND A STOCK OF AND A ST	all dife periodzer verwenden	ieit 333333	ni drigogobon		
> 🛃 Vorlagenverwaltung						
	Bedingungen - Wenn die folge	enden Bedingungen erfüllt sind:				
	Bedingung V	Not				
	beangung	ven				
	Einstellungen - Dann werden f	folgende Einstellungen angewendet:				
	Finstellung	Nat				
	Enracolony .	ven				
<	>					I
Netzwerkrichtlinienserver						- 🗆 ×
Datei Aktion Ansicht						
(
🚯 NPS (Le 🖘 🔪		.htlinjen				
VPS (Letter)	n importieren	:htlinien	Votindunger	Colored and the second s		
NPS (Loten) The Market State Stat	n <mark>importieren</mark> n exportieren	chtlinien für Verbindungsanforderungen kann f	festgelegt werden, ob Verbindungsar	nforderungen lokal verarbeitet oder an RADIU:	S-Remoteserver weitergeleitet werden.	
NPS (Lc ^{k-N} RA(Konfiguratic Konfiguratic RA(NPS-Dienst	n <mark>importieren</mark> n exportieren tarten	chtlinien ür Verbindungsanforderungen kann f	festgelegt werden, ob Verbindungsar	nforderungen lokal verarbeitet oder an RADIU	S-Remoteserver weitergeleitet werden.	
NPS (Lr ^{k-N} Konfiguratic Rat Konfiguratic Ricl NPS-Dienst Structure A	n importieren n n exportieren n tarten ieenden	chtlinien für Verbindungsanforderungen kann f	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que	nforderungen lokal verarbeitet oder an RADIU	5-Remoteserver weitergeleitet werden,	
NPS (Lr ^{ken)} RAI Konfiguratic RAI RAI Konfiguratic Ricl NPS-Dienst NPS-Dienst Kor	n exportieren n tarten leenden ve Directory registrieren u	thtlinien Ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nicl	rforderungen lokal verarbeitet oder an RADIU alle tt angegeben	3-Remoteserver wetergeletet werden.	
NPS (Let-on) RAt Konfiguratis Rat Konfiguratis Ricl NPS-Dienst Server in Act Server in Act Vor	n exportieren n tarten eenden vir n n	htlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi	iestgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que et 999999 Nici	rforderungen lokal verarbeitet oder an RADIU elle ht angegeben	3-Remoteserver weitergeleitet werden.	
NPS (Let-on) RA(Konfiguratic Rorfiguratic NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Server in Act Server in Act Server Hat	n importieren forderen in n exportieren in tarten eenden ve Directory registrieren in n	thtlinien ür Verbindungsanforderungen kann f statu r alle Benutzer verwenden Aktivi	iestgelegt werden, ob Verbindungsar s Verarbeitungsreiherfolge Que et 999999 Nici	nforderungen lokal verarbeitet oder an RADIU slle ht angegeben	3-Remoteserver weitergeleitet werden.	
NPS (Let-on) RAt Konfiguratic NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Server in Act Server Hilfe	n importieren in a exportieren if tarten seenden ve Directory registrieren in n	thtlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi	iestgelegt werden, ob Verbindungsan s Verarbeitungsreiherfolge Que et 999999 Nici	rforderungen lokal verarbeitet oder an RADIU sle ht angegeben	3-Remoteserver weitergeleitet werden.	
NPS (Let-on) RAt Konfiguratic NPS-Dienst NPS-Dienst Server in Act Server in Act Server in Act Hilfe	n importieren in n exportieren if tarten eenden ve Directory registrieren in	thtlinien ür Verbindungsamforderungen kann f statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici	nforderungen lokal verarbeitet oder an RADIU slle ht angegeben	3-Remoteserver weitergeleitet werden.	
NPS (Let-on) RA(Konfiguratic Konfiguratic NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Server in Act Figenschaft Hilfe	n importieren in n exportieren if tarten eenden ive Directory registrieren ür	thtlinien ür Verbindungsamforderungen kann f statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsan s Verarbeitungsreihenfolge Que ert 999999 Nici	iforderungen lokal verarbeitet oder an RADIU slie ht angegeben	3-Remoteserver weitergeleitet werden.	×
NPS (Let-on) RA(Konfiguratio RA(Konfiguratio NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Server in Act Server in Act Hilfe Netzwerknichtlinienserver Datei Aktion Ansicht	n importieren in n exportieren if tarten seenden ive Directory registrieren ür	thtlinien ür Verbindungsamforderungen kann f statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici	iforderungen lokal verarbeitet oder an RADIU tile ht angegeben	5-Remoteserver weitergeleitet werden.	×
NPS (Let-s) ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■	n importieren in n exportieren if tarten seenden ive Directory registrieren ür	htlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici	rforderungen lokal verarbeitet oder an RADIU sle ht angegeben	3-Remoteserver weitergeleitet werden.	-
NPS (Let-on) RAt Konfigurati Konfigurati Konfigurati NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Eigenschafte Hilfe Netzwerkrichtlinienserver Datei Aktion Ansicht Aktion Ansicht NPS (Lokal)	Verbindungsanforderungsric	htlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi chtlinien	festgelegt werden, ob Verbindungsan s Verarbeitungsreihenfolge Que ert 999999 Nici	rforderungen lokal verarbeitet oder an RADIU sle ht angegeben	5-Remoteserver weitergeleitet werden.	×
NPS (Lettern) RAt Konfigurati Konfigurati Konfigurati NPS-Dienst NPS-Dienst Server in Act Server in Act Server in Act Eigenschaft Hilfe Netzwerkrichtlinienserver Datei Aktion Ansicht Set Market Aktion Ansicht Patei Aktion Ansicht Set Market Aktion Aktion	Verbindungsanforderungsric	htlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktiv chtlinien	festgelegt werden, ob Verbindungsan s Verarbeitungsreihenfolge Que ert 999999 Nicl	rforderungen lokal verarbeitet oder an RADIU sle ht angegeben	S-Remoteserver weitergeleitet werden.	×
NPS (Let=n): Konfigurati: ■ RAI Konfigurati: ■ ■ Konfigurati: ■ ■ NPS-Dienst ■ ■ NPS-Dienst ■ NPS-Dienst Server in Act ■ Vor Eigenschafte > ▼ Vor Eigenschafte Datei Aktion Ansicht Image: Server in Act ■ ● ■ ■ ■ ■ NPS (Let=n) ■ ■ ■ ● ● ■ ■ ■ ■ ● ● ■ ■ ■ ■ ■ ● ● ● ■ <	Verbindungsanforderungsric voe Verbindungsanforderungsric voe Verbindungsanforderungsric voe Verbindungsanforderungsric voe	htlinien ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi htlinien	festgelegt werden, ob Verbindungsar s Verarbeitungsreiherfolge Que ert 999999 Nicl	nforderungen lokal verarbeitet oder an RADIU sle ht angegeben	3-Remoteserver weitergeleitet werden.	×
NPS (Let-an) RA(Konfigurati Konfigurati Konfigurati NPS-Dienst NPS-Dienst Kor Vor Eigenschafte Hilfe Netzwerkrichtlinienserver Datei Aktion Ansicht Aktion Ansicht RAUUS-Clients RAUUS-Clients RAUUS-Clients Richtlinien	the start and a second for demonstrate in a seportieren if the second sec	thlinien ür Verbindungsanforderungen kann f statu r alle Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C:) > //	festgelegt werden, ob Verbindungsar s Verarbeitungsreiherfolge Que ert 999999 Nicl	forderungen lokal verarbeitet oder an RADIU sle ht angegeben v 0	S-Remoteserver weitergeleitet werden.	×
NPS (Let-on) RA(Konfigurati Konfigurati NPS-Dienst RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients Netzwerkrichtlinien Verbindungsanfor Netzwerkrichtlinien	Directory registrieren n Verbindungsanforderungsric Pre- Verbindungsanforderungsric Pre- Verbindungsanforderungsric Pre- Verbindungsanforderungsric Pre- Verbindungsanforderungsric Pre- Verbindungsanforderungsric Pre- Verbindungsanforderungsric	thtlinien ür Verbindungsanforderungen kann f r alle Benutzer verwenden Statu chtlinien > Lokaler Datenträger (C;) > / r	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nicl	forderungen lokal verarbeitet oder an RADIU alle ht angegeben	S-Remotesserver weitergeleitet werden.	×
NPS (Let-on) RAt Konfiguratio RAt Konfiguratio NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst Server in Act Server in Act Server in Act Rest Vor Eigenschafte Hilfe Netzwerkrichtlinienserver Datei Aktion Ansicht RADIUS-Clients and -5 RADIUS-Clients	the structure of a constraint of the importiseen of the structure of	thtlinien ür Verbindungsarforderungen kann f statu r alle Benutzer verwenden Aktivi thtlinien > Lokaler Datenträger (C;) > / r ne	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nicl Admin > Anderunosdatum	iforderungen lokal verarbeitet oder an RADIU sle tit angegeben ✓ ♂ ♂ "Admin" durchsuchen 目示 マ	S-Remoteserver weitergeleitet werden.	×
NPS (Let-on) RAt Konfiguratio RAt Konfiguratio NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac Server in Server in Ac Server in Ac	Verbindungsanforderungsric verbindungsanforderungsri	thtlinien Statu ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi chtlinien	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nicl Admin > Admin >	forderungen lokal verarbeitet oder an RADIU sle tit angegeben ✓ ♂	S-Remoteserver weitergeleitet werden.	X
NPS (Let-on) RAt Konfiguratio RAt Konfiguratio NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst RADIUS-Clients RADIUS-Cli	Verbindungsanforderungsric Preser PC Organiseren × Yerbindungsanforderungsric Preser PC Organiseren × Nes-Konfiguration importieren ✓ Yerbindungsanforderungsric NPS-Konfiguration importieren ✓ Yerbindungsanforderungsric Nes-Konfiguration importieren ✓ Yerbindungsanforderungsric Nes-Konfiguration importieren ✓ Yerbindungsanforderungsric Nes-Konfiguration importieren ✓ Yerbindungsanforderungsric Poskop Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric Yerbindungsanforderungsric	thtlinien ür Verbindungsarforderungen kann f statu r alle Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C;) > / r ne PSTranscript Stranuel	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici Admin > Änderungsdatum 31,12,2019 17;18 31,12,2019 17;18 31,12,2019 17;18	forderungen lokal verarbeitet oder an RADIU sle tit angegeben ✓ ♂ "Admin" durchsuchen IBEI ♥ Typ Größe Dateiordner ¥44-Dokument 68 KB	S-Remoteserver weitergeleitet werden.	×
NPS (Let-a) RA(Konfigurati Konfigurati Konfigurati NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac Server	Verbindungsanforderungsric verbindungsanforderungsri	thtlinien Statu ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Activi chtlinien	festgelegt werden, ob Verbindungsar s Verarbeitungsreiherfolge Que ert 999999 Nici Admin > Änderungsdatum 31.12.2019 17.18 31.12.2019 17.19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben v to "Admin" durchsuchen fill v Typ Größe Dateiordner XML-Dokument 68 KB	S-Remotesserver weitergeleitet werden.	×
NPS (Let-n) RAt Konfigurati Rat Konfigurati NPS-Dienst NPS-Dienst NPS-Dienst Kor Server in Ac Kor Vor Eigenschafte Hife Netzwerkrichtlinienserver Datei Aktion Ansicht More and ansicht RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Clients RADIUS-Remotes Vorlagenverwaltung	In the start of the start	chtlinien ür Verbindungsanforderungen kann f r alle Benutzer verwenden Statu chtlinien > Lokaler Datenträger (C:) > / r	festgelegt werden, ob Verbindungsar s Verarbeitungsreiherfölge Que ert 999999 Nicl Admin > Admin > Admin 31.12.2019 17:19 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben v č *Admin* durchsuchen jez v Typ Größe Dateiordner XML-Dokument 68 KB	S-Remotesserver weitergeleitet werden.	×
NPS (Let-n) RAt Konfigurati NPS-Dienst NPS-Dienst Kor WrS-Dienst Kor Wor Eigenschafte Hife Netzwerkrichtlinienserver Datei Aktion Ansicht RADUS-Clients RADUS-Clients RADUS-Clients RADUS-Clients RADUS-Clients RADUS-Clients Robults-Remotes Vorlagenverwaltung	Destrop Destrop The strop for the second sec	chtlinien ür Verbindungsarforderungen kann f statu r alle Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C:) > /r ne PSTranscript config.xml	ietgelegt werden, ob Verbindungsar Verarbeitungsreihenfolge Que ert 999999 Nicl Admin > Admin > Anderungsdatum 31.12.2019 17:19	forderungen lokal verarbetet oder an RADIU sle ht angegeben ✓ Č (*Admin* durchsuchen BE ▼ Typ Dateiordner XML-Dokument 68 KB	S-Remoteserver weitergeleitet werden.	×
NPS (Letan) RAI Konfiguration Konfiguration Konfiguration Konfiguration Kor Kor Eigenschafts Hife Netzwerkrichtlinienserver Date Aktion Ansicht Ansicht Ansicht Ansicht Ansicht Ansicht Kor Eigenschafts Eigenschafts Hife Netzwerkrichtlinienserver Date Aktion Ansicht Ansicht Ansicht Konto RaDIUS-Clients Richtlinien Kontoführung Vorlagenverwaltung	troportieren n exportieren n exportieren verbindungsanforderungsric envel Verbindungsanforderungsric envel e	htlinien Statu ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi - htlinien	festgelegt werden, ob Verbindungaar s Verarbetungsreihenfolge Que ert 999999 Nicl Admin > Admin > Änderungsdatum 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben ✓ © TAdmin" durchsuchen EEE ✓ Typ Größe Dateiordner XML-Dokument 68 KB	S-Remotesserver weitergeleitet werden.	×
NPS (Letan) Antipartition of the second	It bested uncover (and bested importieren, in exportieren, it atriten seenden ive Directory registrieren ive Directory reg	thlinien ür Verbindungsarforderungen kann f statu r alle Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C:) r ne PSTranscript config.xml	festgelegt werden, ob Verbindungsar s Verarbetungsreihenfolge Que et 999999 Nici Admin > Admin > Ånderungsdatum 31.12.2019 17:19	iforderungen lokal verarbeitet oder an RADIU sle til angegeben ✓ C TAdmin" durchsuchen IIII ✓ Typ Größe Dateiordner XML-Dokument 68 KB	S-Remoteserver weitergeleitet werden.	×
 NPS (Letter) RAI RAI Konfiguratii	It bested uncover (and bested importieren if intraction interes if ive Directory registrieren if	thtlinien Statu ür Verbindungsarforderungen kann f Statu r alle Benutzer verwenden Aktivi thtlinien Aktivi > Lokaler Datenträger (C3) > / / r	iestgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici Admin > Admin > Admin 31.12.2019 17:18 31.12.2019 17:19	iforderungen lokal verarbeitet oder an RADIU sle til angegeben ✓ © "Admin" durchsuchen I]EE ▼ Typ Große Dateiordner XML-Dokument 68 KB	S-Remoteserver weitergeleitet werden.	×
NPS (Letter) RAt RAt RAt Konfigurativ NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac Server in Ac Serve	Verbindungsanforderungsrie receiven Verbindungsanforderungsrie ve Directory registrieren ve Directory ve	thtlinien Statu ür Verbindungsarforderungen kann f Statu r alle Benutzer verwenden Aktivi	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Ned Admin > Admin > Admin 31.12.2019 17:18 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle tit angegeben ✓ ♂ "Admin" durchsuchen I]EE ♥ Typ Dateiordner XML-Dokument 68 KB	S-Remoteserver weitergeleitet werden.	X
 NPS (Let-n). RAI Konfigurati, Konfigurati, NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac Kor Eigenschaft Hilfe 	Verbindungsanforderungsric evel Verbindungsanforderungsric evel Verbindungsanforderungsric evel Verbindungsanforderungsric evel Verbindungsanforderungsric evel Verbindungsanforderungsric verbindungsanforderungsric	chtlinien Statu ür Verbindungsanforderungen kann f Statu r alle Benutzer verwenden Aktivi chtlinien Aktivi > Lokaler Datenträger (Ci) > / r ne PSTranscript config.xml	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici Admin > Änderungsdatum 31.12.2019 17:18 31.12.2019 17:19	tforderungen lokal verarbeitet oder an RADIU sle tit angegeben ✓ ひ (*Admin* durchsuchen (BEE ↓ Typ Größe Dateiordner XML-Dokument 69 KB	S-Remoteserver weitergeleitet werden.	
 NPS (Let-n) RAI Konfigurativ RIC NPS-Dienst NPS-Dienst NPS-Dienst Server in Ac Eigenschaft Hilfe 	Verbindungsanforderungsric evel Verbindungsanforderungsric	thtlinien ür Verbindungsarforderungen kann f Statu r alle Benutzer verwenden Activi chtlinien > Lokaler Datenträger (C:) > / r ne PSTranscript config.xml	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici Admin > Änderungsdatum 31.12.2019 17:19 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben ✓ ♂ "Admin" durchsuchen I]EE ↓ Typ Größe Dateiordner XML-Dokument 63 KB	S-Remoteserver weitergeleitet werden.	
NPS (Let-n) Antipartition of the second	In portieren in exportieren in exportieren in exportieren in exportieren in ive Directory registrieren i i ive Directory registrieren i i ive Directory registrieren ive ive Directory registrieren ive ive Directory registrieren ive Directory	Entlinien ür Verbindungsanforderungen kann f r alle Benutzer verwenden Aktivi Entlinien > Lokaler Datenträger (C:) > / r ne PSTranscript config.xml	festgelegt werden, ob Verbindungsar s Verarbeitungsreihenfolge Que ert 999999 Nici Admin > Änderungsdatum 31.12.2019 17:19 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben v 0 "Admin" durchsuchen EEE • Typ Größe Dateiordner XML-Dokument 68 KB	S-Remotesserver weitergeleitet werden.	
NPS (Letan) RAI Konfiguration Konfiguration Konfiguration NPS-Dienst Kor Eigenschaft NPS-Dienst Kor Eigenschaft Hiffe Netzwerkrichtlinienserver Datei Aktion Ansicht 1 Netzwerkrichtlinienserver Datei Aktion Ansicht 1 NPS (Lotal) NPS (Lotal) Kontoführung Vorlagenverwaltung	tryportieren ingoritieren ingoritieren ingoritieren ingoritieren ingoritieren in ive Directory registrieren i ive Directory registrieren ive ingoritieren ive Directory registrieren ive Desktop ive Directory ive Di	chtlinien ür Verbindungsarforderungen kann f statu r alle Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C:) > / r PSTranscript config.xml	festgelegt werden, ob Verbindungsar s Verarbeitungsreiherfölge Que ert 999999 Nici Admin > Admin 31.12.2019 17:19 31.12.2019 17:19	forderungen lokal verarbeitet oder an RADIU sle ht angegeben v Č "Admin" durchsuchen EE • Typ Größe Dateiordner XML-Dokument 68 KB	S-Remotesserver weitergeleitet werden.	
 NPS (Let-n). RAI RAI Konfiguratii	tripportieren n exportieren n exportieren inf inf portieren inf inf inf	chtlinien ür Verbindungsarforderungen kann f ale Benutzer verwenden Aktivi chtlinien > Lokaler Datenträger (C:) r ne PSTranscript config.xml	iestgelegt werden, ob Verbindungaar s Verarbetungsreihenfolge Que et 999999 Nei Admin > Admin > Admin 31.12.2019 17:18 31.12.2019 17:19	forderungen lokal verarbetet oder an RADIU sle til angegeben ✓ Č) "Admin" durchsuchen IEE ✓ Typ Größe Dateiordner XML-Dokument 68 KB ✓ XML files (*.xml) Öffnen Abb	S-Remoteserver weitergeleitet werden.	

Dieser Schritt war sehr einfach. Die Bestätigung klingt vielversprechend:





Meine Richtlinien sind alle angekommen:

Netzwerkrichtlinienserver						_		×
Datei Aktion Ansicht ?								
🗢 🔿 🙍 🖬								
NPS (Lokal) ADIUS-Clients und -Serve RADIUS-Clients ADIUS-Clients RADIUS-Remoteserverg Richtlinien	Netzwerkrichtlinien Netzwerkrichtlinien emöglichen das Festlegen der zur	Herstellung einer N	etzwerkverbindung berechti	gten Personen sowie	e der Bedingungen, unter denen sie eine V	ferbindung herstellen könne	n.	
🦉 📔 Verbindungsanforderur	Richtlinienname	Status	Verarbeitungsreihenfolge	Zugriffstyp	Quelle			
 Netzwerkrichtlinien Kontoführung Morlagenverwaltung 	VPN-Clents-Zetfikate VPN-Clents-Zetfikate VPN-clent volument Microsoft-Routing- und Remotezugriffser Verbindungen mit Microsoft-Routing- und Remotezugriffservern	Aktiviert Aktiviert Deaktiviert Aktiviert Aktiviert	1 2 3 999999 1000000	Zugriff gewähren Zugriff gewähren Zugriff gewähren Zugriff verweigem Zugriff verweigem	Nicht angegeben Nicht angegeben Nicht angegeben Nicht angegeben Nicht angegeben			
	Secure-WLAN							
	Bedingungen - Wenn die folgenden Bedingungen erfüllt sind Bedingung Wert NAS-Porttyp Drahtlos (sonstige) OR Drahtlos (IEEE 802.11)						
	Einstellungen - Dann werden folgende Einstellungen angewe	ndet:						
	Einstellung W EAP-Konfiguration (Extensible Authentication-Protokoll) Ko Benutzereihwähleigenschaften ignorieren W Zugriffsberechtigung Zu EAP-Methode (Extensible Authentication-Protokoll) M Authentifizierungsmethode E/	ert nfiguriert ahr griff gewähren crosoft: Smartcard- P	oder anderes Zertifikat					
< >								•

Und auch der Radius-Client wird angezeigt:

Netzwerkrichtlinienserver					-	×
Datei Aktion Ansicht ?						
🗢 🄿 🙋 📅 🚺						
🚳 NPS (Lokal)	RADIUS-Clients					
RADIUS-Clients und -Serve	RADIUS-C	lients emögliche	n die Angabe der Ne	tzwerkserver, die Zugriff auf das Netzwerk bieten.		
 Verbindungsanforderun Netzwerkrichtlinien Kontoführung Vorlagenverwaltung 	Anzeigename	IP-Adresse ws-ap1.ws.its	Gerätehersteller RADIUS Standard	Status Aktiviert		

Bevor es jetzt in die Umstellungsphase geht nutze ich die Gelegenheit, um etwas aufzuräumen. In den Netzwerkrichtlinien ist noch die Richtlinie für den VPN-Service gelistet. Da ich diesen Service nicht mehr bereitstelle, kann ich die Regel löschen:

Netzwerkrichtlinienserver								_		×
Datei Aktion Ansicht ?										1
🗢 🄿 🖄 📰 🚺 🖬										
🚯 NPS (Lokal)	Netzwerkrichtlinie	n								
 RADIUS-Clients und -Serve Richtlinien Verbindungsanforderur Netzwerkrichtlinien 	Netzwerkrich Verbindung ł	tlinien emöglichen das Festlegen de terstellen können.	er zur Herste	ellung einer N	etzwerkverbindung berechti	gten Personen sowie	der Bedingungen, unte	er denen s	ie eine	
Kontoführung	Richtlinienname			Status	Verarbeitungsreihenfolge	Zugriffstyp	Quelle			
> 💐 Vorlagenverwaltung	Secure-WLAN			Aktiviert	1	Zugriff gewähren	Nicht angegeben			· · · ·
	VPN-Clients-Zertifi	kate		Aktiviert	2	Zugriff gewähren	Nicht angegeben			
1 · · · · · · · · · · · · · · · · · · ·	VPN-Clients	Nach oben		Deaktiviert	3	Zugriff gewähren	Nicht angegeben			
1 · · · · · · · · · · · · · · · · · · ·	Verbindungen	Nachoben	erver	Aktiviert	999999	Zugriff verweigem	Nicht angegeben			
1 · · · · · · · · · · · · · · · · · · ·	Verbindungen	Nach unten		Aktiviert	1000000	Zugriff verweigem	Nicht angegeben			
· • · · · · · · · · · · · · · · · · · ·		Aktivieren								
· • · · · · · · · · · · · · · · · · · ·	VPN-Clients	Löschen								
1 · · · · · · · · · · · · · · · · · · ·		Umbenennen						_		
1 · · · · · · · · · · · · · · · · · · ·	Bedingungen -	Richtlinie duplizieren	nd:							
1 · · · · · · · · · · · · · · · · · · ·		Reference of application	_							
1 · · · · · · · · · · · · · · · · · · ·	Bedingung	Eigenschaften								
	Windows-Grup Zulässige EAP	Hilfe	AP)-Micro	osoft: Gesiche	rtes Kennwort (EAP-MSCH/	\P v2)				

Damit habe ich die Funktionalität des NPS im Hintergrund kopiert. Für die Umstellung fehlt aber noch ein wichtiges Detail.

Konfiguration des Serverzertifikats

IT-Solutions

Dieses Detail ist das Zertifikat für den Radius-Server. In meiner Gruppenrichtlinie für die mobilen Clients habe ich für den internen WLAN-Zugriff die gegenseitige Authentifizierung angefordert: So muss nicht nur der Client seine Identität beweisen, sondern auch der Radius-Server. Und das kann er mit einem Sicherheitszertifikat. Durch mein PKI-Zertifikat-AutoEnrollment hat der Server WS-NPS1 bereits ein Clientauthentifizierungszertifikat. Für den NPS-Service benötige ich aber ein anderes. Dieses frage ich manuell in der Konsole certlm.msc an:

👼 certlm - [Zertifikate - Lokaler Co	omputer\Eige	er/Eigene Zertifikate\Zertifikate} —								
Datei Aktion Ansicht ?										
🗢 🄿 🙋 📆 📋 🙆 🔒	?									
 Zertifikate - Lokaler Computer Eigene Zertifikate Zertifikate Vertrauenswürdige Stammze Organisationsvertrauen 	Ausgestel	lt für 2S1	Ausgest WS-ITS-	ellt von Zertifizierungsstelle-CA1	Ablaufdatum 30.12.2020	Beabsichtigte Zwec Clientauthentifizier	Anzeigename <keine></keine>	Status	Zertifikatvorla WS-ITS-Comp	ge
> Cwischenzertifizierungsstelle	a	Alle Aufgaben	>	Neues Zertifikat anfo	dern					
 Vertrauenswürdige Herausge Nicht vertrauenswürdige Zer Drittanbieter-Stammzertifizie 	el t	Aktualisieren Liste exportieren		Importieren Erweiterte Vorgänge	>					
 Vertrauenswürdige Personen Clientauthentifizierungsauss 	t	Ansicht	>							
Stammelemente der Vorabve Stämme testen Gemetedeskton		Symbole anordnen Am Raster ausrichter	>							
 Zertifikatregistrierungsanford 	d	Hilfe								
Smartcard vertrauenswürdige Geräte Windows Live ID Token Issue Windows Live ID Token Issue Oper Specific (1997)	e 31									

Der Assistent verbindet sich mit meiner PKI über den CEPCES-Endpunkt:

📓 certlm - [Zertifikate - Lokaler Con	puter\Eigene Zertifikate\Zertifikate]			- 0	\times
Datei Aktion Ansicht ?					
🗢 🔿 🙋 📅 📋 🙆 😽					
🙀 Zertifikate - Lokaler Computer	Ausgestell – – ×	me	Status	Zertifikatvorlage	
 Eigene Zertifikate Zertifikate 	🙀 WS-NP 🗔 Zertifikatregistrierung			WS-ITS-Comp	
> Vertrauenswürdige Stammzer					
> Organisationsvertrauen	Zertifikatregistrierungsrichtlinie auswählen				
Zwischenzertritizierungssteller Zwischenzertritizierungssteller Vertrauenswürdige Herausgel Nicht vertrauenswürdige Zert Dittanbieter-Stammzertifizie Vertrauenswürdige Despage	Mithilfe der Zertifikatregistrierungsrichtlinie können Zertifikate basierend auf vordefinierten Zertifikatvorlagen registriert werden. Die Zertifikatregistrierungsrichtlinie ist möglicherweise bereits für Sie konfiguriert.				
Clientauthentifizierungsausst	Vom Administrator konfiguriert				
> 📔 Stammelemente der Vorabve	WS IT-Solutions Zertifikatverteilung 🔹				
Stamme testen Externation Executed sktop Sectifikatregistrierungsanford Sonartcard vertrauenswürdige Wertrauenswürdige Geräte Windows Live ID Token Issuer	Von Ihnen konfiguriert Neue hinzufügen				
	Weiter Abbrechen				

Für NPS benötige ich ein Webserver-Zertifikat. Dafür habe ich bereits eine Vorlage erstellt. Der Subject-Wert muss manuell eingegeben werden:

🚟 certlm - [Zertifikate - Lokaler Com	puter\Eigene Zertifikate\Zertifikate]		- 0	\times
Datei Aktion Ansicht ?				
🗢 🄿 🙍 📰 📋 🙆 🕞				
Zertifikate - Lokaler Computer Eigene Zertifikate Zertifikate Yertrauenswürdige Stammzer Zvischenzertifizierungssteller Wertrauenswürdige Herausgel Wicht vertrauenswürdige Zert Dritanbieter-Stammzertifizie Vertrauenswürdige Personen Clientauthentifizierungsausst Stämme testen Sämme testen Sämmet edesktop Zertifikatregistrierungsanford Smartcard vertrauenswürdige Vertrauenswürdige Geräte Windows Live ID Token Issuer	Ausgestell <	me Status	Zertifikatvorlage WS-ITS-Comp	

Ich benenne den CN mit einem Alias nps.ws.its:

WS IT-Solutions

ᡖ certlm - [Zertifikate - Lokaler Com	nputer\Eige	ne Zertifikate	\Zertifikate]						- 0	×
Datei Aktion Ansicht ?										
🗢 🄿 🖄 📆 📋 🙆 🖌	?									
Zertifikate - Lokaler Computer Eigene Zertifikate Zertifikate Verturenswürdige Stammzer Organisationsvertrauen Zwischenzertifizierungssteller Verturenswürdige Heraussel	Ausgestell	Zertifik Zert	atregistrierung ifikate anfordern		-		me	Status	Zertifikatvorlage WS-ITS-Comp	
 Nicht vertrauenswürdige Zert Drittanbieter-Stammzertifizie 		klick	Privater Schlüssel	Zertifizierungsstelle	Signatur	. na				
> 📔 Vertrauenswürdige Personen		W	🛕 Antragsteller	Allgemein	Erweiterungen					
Clientauthentifizierungsausst Stammelemente der Vorabve Stamme testen Ernotedesktop Zertifikatregistrierungsanford Smartard vertrauenswürdige Wertrauenswürdige Geräte Windows Live ID Token Issuer			Der Antragsteller eines Zertifika ausgestellt ist. Geben Sie Inform alternative Namenswerte ein, d Zertifikatsantragsteller Der das Zertifikat empfangende Antragstellername: [Jyp: Altgemeiner Name Wegt: [ts ist der Benutzer oder Comput nationen über die zulässigen An ie in einem Zertifikat verwendet Benutzer oder Computer Hinzufügen > < Entfermen	ier, für den das Zertifikat tragstellernamen und werden dürfen. npsws.its	ails ¥ ails ¥ ie				
< >> >> Der Sneicher "Einene Zertifikate" enthä	it 1 Zertifik:	*	DNS Vgrt:	Hinzufügen >	ws.its					
Der Speicher Eigene Zertifikate" entha	it i Zertifika	it.		< Entfernen				_		_

WS IT-Solutions

So ausgefüllt kann der Request zur PKI gesendet werden:

🚪 certlm - [Zertifikate - Lokaler Cor	omputer\Eigene Zert	ifikate\Zertifikate]					- 0	\times
Datei Aktion Ansicht ?								
🗢 🔿 🙍 📆 📋 🧟 😹	?							
Zertifikate - Lokaler Computer Eigene Zertifikate Zertifikate Vertrauenswürdige Stammzer Grganisationsvertrauen Zvischenzertifizierungssteller Wicht vertrauenswürdige Zert	Ausgestell	ertifikatregistrierung Zertifikate anfordern Folgende Zertifikattypen sind abruf klicken Sie anschließend auf "Regist	bar. Wählen Sie die Zertifikate aus, die Sie anforden trieren".	− □ ×	me	Status	Zertifikatvorlage WS-ITS-Comp	
Drittanbieter-Stammzertifizie	2	WS IT-Solutions Zertifikatverte	iluna					
 Clientauthentifizierungsausst Stammelemente der Vorabve 	t	WS-ITS-Computer-V2	(1) STATUS: Verfügbar	Details 🗸				
Stämme testen Remotedesktop Zertifikatregistrierungsanford Sinartcard vertrauenswürdige Windows Live ID Token Issuer	al e	₩S-ITS-Webserver-V2	ن STATUS : Verfügbar	Details 💙				
		Alle Vorlagen anzeigen						
			Registrieren	Abbrechen				

Und dort wird er auch direkt genehmigt:

🚪 certlm - [Zertifikate - Lokaler Con	nputer\Eigene Zertif	kate\Zertifikate]					- 0	\times
Datei Aktion Ansicht ?								
🗢 🄿 🙍 📆 📋 🙆 😹	?							
Zertifikate - Lokaler Computer Gigene Zertifikate Zertifikate Vertrauenswürdige Stammzer Grganisationsvertrauen Vertrauenswürdige Herausgel Nicht vertrauenswürdige Herausgel Nicht vertrauenswürdige Herausgel Nicht vertrauenswürdige Herausgel	Ausgestell	tifikatregistrierung Iertifikatinstallationsergebnis: Jogende Zertifikate wurden registriert	Se und auf diesem Computer installiert.	– – ×	me	Status	Zertifikatvorlage WS-ITS-Comp	
Ortennorsvördige Personen Ortennorsvördige Personen Ortennorsvördige Personen Stämmelemente der Vorabve Stämme testen Remotedesktop Zertifikatregistrierungsanford Smartcard vertrauenswürdige Vertrauenswürdige Geräte Windows Live ID Token Issuer		WS-ITS-Webserver-V2	y STATUS: Erfolgreich	Details 💌				
				<u>F</u> ertig stellen]			

Das Zertifikat ist jetzt einsatzbereit:

藩 certlm - [Zertifikate - Lokaler Cor	nputer\Eigene Zertifikate\Zertifika	te]					- 0	×
Datei Aktion Ansicht ?								
-	?							
🙀 Zertifikate - Lokaler Computer	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwec	Anzeigename	Status	Zertifikatvorlage	
 Eigene Zertifikate Zertifikate Vertrauenswürdige Stammzer 	留nps.ws.its 留WS-NPS1	WS-ITS-Zertifizierungsstelle-CA1 WS-ITS-Zertifizierungsstelle-CA1	15.10.2021 30.12.2020	Serverauthentifizier Clientauthentifizier	<keine> <keine></keine></keine>		WS-ITS-Webse WS-ITS-Comp	
 Organisationsvertrauen Zwischenzertifizierungssteller Vertrauenswürdige Herausgel 								
Nicht vertrauenswürdige Zert Drittanbieter-Stammzertifizie Vertrauenswürdige Personen								
 Clientauthentifizierungsausst Stammelemete der Vorabve 								
Stamme testen Emotedesktop Zertifikatregistrierungsanford								
 Smartcard vertrauenswürdige Vertrauenswürdige Geräte Windows Live ID Token Issuei 								

Jetzt muss ich dem NPS noch mitteilen, dass er dieses neue Zertifikat verwenden soll. Dazu geht es in die NPS-Konsole in die Richtlinie für mein Secure-WLAN:



Netzwerkrichtlinienserver Datei Aktion Ansicht ?							- 🗆 ×
← ⇒ 2 □ 2 □							
Datei Aktion Ansicht ? NPS (Lokal) RADIUS-Clients und -Serve Richtlinien Verbindungsenforderur Netzwerkrichtlinien Kontoführung Vorlagenverwaltung Vorlagenverwaltung Vorlagenverwaltung 	Netzwerkricht Verbind Richtlinienname Verbindunge Verbindunge Verbindunge Verbindunge Secure-WL Bedingungen Bedingungen Bedingungen Einstellungen Einstellungen Enstellungen Einstellungen KAS-Porttyp	tlinien emöglichen das Festlegen der zur H ung herstellen können.	enstellung einer N Status Aktiviert Aktiviert Einstellungen ese Netzwerkrich- ngsanforderung, Zugriff nur für authentifizierei EAP-Typen vi Reihentörge a EAP-Typen vi Reihentörge a EAP-Typen vi Hinzufügen Weniger siche Benutzz Microsoft-w Benutzz Microsoft-	letzwerkverbindung berechti Verarbeitungsreihenfolge 1 2 timie. wird der Netzwerkzugriff ver Lients gewähren, die sich m 1. riden zwischen Netzwerkrick usgehandelt. nattcard-oder anderes Zertif 	igten Personen sowi Zugriff gewähren Zugriff gewähren zugriff gewähren it den angegebenen htlinienserver und Cl fikat Entfernen en: ng, Version 2 (MS-CL blaufdatum ändem ng (MS-CLAP) blaufdatum ändem) P SSAP)	e der Bedingungen, unter de Quelle Nicht angegeben Nicht angegeben Methoden ient in der angezeigten Nach oben Nach oben Nach unten	nen sie eine
			Clientverbi	idungen ohne Aushandlung	einer Authentifizieru	ngsmethode zulassen	
					ОК	Abbrechen Übe	mehmen

Der Server hat das Zertifikat sofort gefunden:

Netzwerkrichtlinienserver								×
Datei Aktion Ansicht ?								
🗢 🄿 🙍 🖬								
🚳 NPS (Lokal)	Netzwerkrichtlinien							
> 🧮 RADIUS-Clients und -Serve								
✓ I Richtlinien	Verbindung herstellen können.	estiegen der zur Herstell	ung einer ive	etzwerkverbindung berechtig	gten Personen sowie	e der Bedingungen, unter den	en sie eine	
Verbindungsanforderur								
Kontoführung	Richtlinienname		Status	Verarbeitungsreihenfolge	Zugriffstyp	Quelle		
> I Vorlagenverwaltung	Secure-WLAN		Aktiviert	1	Zugriff gewähren	Nicht angegeben		
·	VPN-Clients-Zertifikate		Aktiviert	2	Zugriff gewähren	Nicht angegeben		
	VPN-Clients Eigenschaften von Secure-	WLAN					\times	
	Verbindunge							
	Ubersicht Bedingungen	Einschränkungen Eins	stellungen					
	Secure-WL Konfigurieren Sie die Einsch Entspricht keine Einschränl	Smartcard- oder an	idere Zertifi	ikateigenschaften	×]		
	Bedingungen Einschränkungen:	Dieser Server identifi	ziert sich ger	enüber Aufnifem bevor ein	e Verbindung			
	Einschränkungen	hergestellt wird. Wäh	len Sie das	als Identitätsnachweis zu ve	rwendende	Vethoden		
	Bedingung Authentifizierungsme	Zertifikat aus.						
	NAS-Porttyp n	Zertifikat ausgestellt f	für: nps.	ws.its	~			
	🎭 Leerlaufzeitüberschr	Anzeigename:	nos v	vsits		nt in der angezeigten		
	🐝 Sitzungszeitübersch	, including and including a						
	🧾 Empfangs-ID	Aussteller:	WS-	TS-Zertifizierungsstelle-CA1				
	Tag- und	Ablaufdatum:	15.1	0.2021 18:15:22		Nach oben		
	Einstellungen Uhrzeiteinschränkur					Nach unten		
	Finstellung 👚 NAS-Porttyp			OK	Abbrechen	>		^
	FAP-Konfigu		Hinzufügen	Bearbeiten	Entfemen	1		

Damit steht dem Schwenk des NPS nur noch eine Kleinigkeit im Weg.

Konfiguration der Protokollierung

Ich bin durchaus ein Fan von Protokollen und Logfiles. Zu oft hatte ich schon Szenarien, in denen diese nicht oder nicht mehr zur Verfügung standen. So wird effizientes Troubleshooting, nachträgliche Forensik von Sicherheitsproblemen und



proaktives Monitoring ein Kraftakt. Daher überlege ich gerne, welcher Service welche Informationen auf welchem Wege zur Verfügung stellen kann.

Der NPS hat ein sogenanntes Accounting. Dieses ist per Default nicht aktiv. Also werde ich das in der Konsole jetzt anpassen:

Netzwerkrichtlinienserver	- 🗆 ×
Datei Aktion Ansicht ?	
🗢 🔿 🙍 🖬	
 NPS (Lokal) RADIUS-Clients und -Serve 	Kontoführung
RADIUS-Clients	Kontoführung
KADIUS-Kemoteserverg Kichtlinien Verbindungsanforderur Natzwackrightlinige	Wählen Sie die Option "Kontoführung konfigurieren" aus, wenn Sie den Kontoführungskonfigurations-Assistenten aufführen möchten. Mithälfe des Assistenten können Sie eine Auswahl aus vier verschiedenen Kontoführungskonfigurationen treffen und automatisch eine lokale oder eine Remotenstanz von SQL Server mit einer Datenbank für die NPS-Kontoführung konfigurieren.
Kontoführung	Koritofkinung konfiguteren Wetere Informationen
	Protokolldateieigenschaften
	Wählen Sie die Option "Protokolldateieigenschaften ändem" aus, wenn Sie die Einstellungen für die Textprotokollierung ändem möchten.
	Status: Konfigurient für C:\Windows\system32\LogFiles
	Protokoldateieigenschaften ändem Weitere Informationen
	SQL Server-Protokollierungseigenschaften
	Wählen Sie die Option "SQL Server-Protokollierungseigenschaften ändern" aus, wenn Sie die SQL Server-Protokollierungseinstellungen ändern möchten.
	Status: <pre>cnicht konfiguriet></pre>
	SQL Server-Protokollieungseigenschaften ändem

Aktuell ist der Server alleine. Daher könnte ein lokales Accounting in eine Textdatei genügen. Später wäre ein zentraler SQL-Server auf einem anderen Server die bessere Option:

Netzwerkrichtlinienserver			- 🗆 ×
Datei Aktion Ansicht ?			
🗢 🔿 🖄 🖬 🚺		Kantafilana akadima Anidan	1
🚯 NPS (Lokal)	Kontoführung	Kontorunrungskonrigurations-Assistent	
 RADIUS-Clients und -Serve RADIUS-Clients RADIUS-Remoteserverg Richtlinien 	Kontoführung Wählen Sie die Option "Ko Kontoführungskonfiguratio	Kontoführungsoptionen auswählen	s Assistenten können Sie eine Auswahl aus vier verschiedenen toführung konfigurieren.
 Veröindungsanlörderur Netzwerkrichtlinien Kontoführung Vorlagenverwaltung 	Kontoführung konfigu	Mithilfe von NPS können Kontoführungedaten in einer lokalen Textdatei bzw. in einer SQL Server-Datenbank protokolliet werden. Es ist außerdem möglich, dass die Protokollierung mit NPS nur in einer SQL Server-Datenbank enfolgt, in diesem Fäl wird anschließend die Protokollierung in einer Textdatei gestatet, wenn bei der SQL Server-Protokollierung Fehrer auftreten und es zu einem Fälover kommt.	
	Protokolldateieigen	Wählen Sie eine Option für die NPS-Kontoführungskonfiguration aus, und klicken Sie dann auf "Weiter": O Protokollierung in einer SQL Server-Datenbank.	
	Wählen Sie die Option "Pr	Protokollierung in einer Textdatei auf dem lokalen Computer.	
	Status: Konfiguriert für C	O Gleichzeitige Protokollierung in einer SQL Server-Datenbank und in einer lokalen Textdatei.	
	SOI Server Protoko	O Protokollierung in einer SQL Server-Datenbank mithilfe der Textdateiprotokollierung für Failover.	

Die Auswahl der möglichen Eintragstypen und die Angabe des Speicherpfades sind selbsterklärend:





Für einen Test brauche ich aktive Verbindungen.

Austausch des NPS

Der NPS ist vollständig konfiguriert. Der nächste Schritt kann also der eigentliche Austausch des alten NPS gegen den neuen sein. Wie eingangs geplant wird das von mir durch den Austausch der IPv4-Konfiguration erledigt, da mein Radius-Client nur die IP-Adresse des NPS kennt. Zuerst sichte ich auf dem alten Server die aktuelle Konfiguration:



Nun könnte ich dem alten Server eine neue IP-Adresse geben. Ich habe aber alle anderen Komponenten des Servers entfernt. Also schalte ich den Server einfach aus. Ein Vorteil: sollte der neue Server nicht funktionieren, dann kann ich den neuen einfach ausschalten und den alten wieder hochfahren. So kommt der WLAN-AccessPoint wieder am funktionalen NPS auf dem alten Server raus:

	.	Einstellungen	<u> </u>		
		Erleichterte Bedienung 🛛 🗸	Remotedeskt	Ereignisanzeige	Explorer
	s				
Wähle besch herun And	en Sie e ireibt, w iterfahr	inen Grund aus, der am bester varum Sie diesen Computer en möchten. und (geplant) ✓	ı		
		Windows Venualtungsprogra	eiter		
Φ		Windows-Zubehör			
-	Q	다 🤅 📃 🎐	2		

Natürlich muss ich sicherstellen, dass der alte und der neue Server nicht zeitgleich aktiv sind. Im neuen Server trage ich nun die statische IPv4-Konfiguration ein:

😰 Netzwerkverbindungen			- 🗆 X
← → ✓ ↑ 😰 > Systemsteuerung > Netzwerk und Internet.	Netzwerkverbindungen	~ Ū	"Netzwerkverbindungen" dur 🔎
Organisieren 🔻 Netzwerkgerät deaktivieren Verbindi	Eigenschaften von Ethernet	»	
Ethernet ws.its Microsoft Hyper-V Network Adap	tzwerk Eigenschaften von Internetprotokoll, Version 4 (TCP/IPv4) X Allgemein P-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen. O IP-Adresse automatisch beziehen Folgende IP-Adresse verwenden: IP-Adresse: 192.168.100.7 Subnetzmaske: 255.255.255.0 Standardgateway: 192.168.100.252 ONS-Serveradresse automatisch beziehen Folgende DNS-Server: @ Folgende DNS-Server: 192.168.100.2 Alternativer DNS-Server: 192.168.100.2 Alternativer DNS-Server: 192.168.100.1 Einstellungen beim Beenden überprüfen Erweitert		
1 Element 1 Element ausgewählt	OK Abbrechen		== 📼

Ab jetzt sollten neue Clientverbindungen über WLAN vom WS-NPS1 authentifiziert werden.

Funktionsprüfung

VS IT-Solutions

Das muss natürlich getestet werden. Damit die Zeit der Unterbrechung so gering wie möglich wird, habe ich bereits einen WLAN-Client zum Testen aufgebaut und mich von meinem Rechner aus mit dem Administrations-Portal meines WLAN-AccessPoints verbunden. Das WLAN mit der SSDI ws-ist verwendet WPA-Enterprise – also die Authentifizierung gegen den NPS-Server:

Pt	p-link					Access Poir	nt 🗸 🗲 ?)	
Network		Wirele	Wireless Monitoring		Managemer	Management System			
 Wireless Setting		s	Portal	MAC Filtering	Scheduler Qo		oS Rogue AP Deter		
								🔂 Add	
ID	SSI	D	Wireless VLAN I	D SSID Broadcast	Security Mode	Portal	SSID Isolation	Modify	
1	ws-g	ast	130	Enable	WPA-PSK	Enable	Enable	6	
2	ws-d	mz	130	Enable	WPA-PSK	Disable	Disable	6	
3	WS-	its	110	Enable	WPA-ENTERPRISE	Disable	Disable	C	

Wireless Advanced Settings

Beacon Interval:	100	ms (40-100)
DTIM Period:	1	(1-255)
RTS Threshold:	2347	(1-2347)
Fragmentation Threshold:	2346	(256-2346. This works only in 11b/g mode.)

Hier steht die IPv4 des NPS-Servers. Bei nur einem AP hätte ich hier auch einfach die neue IP des NPS eintragen können. Aber mit mehreren AP wäre ohne zentralen Server der Aufwand höher: WS IT-Solutions

WSHowTo – Migration des NPS 2019-12-31 Migration auf Windows Server 2019

₽	tp-link						Access Poir	nt v 🗲	?			
N	etwork W	'ireless	Monitoring			Managemer	nt Sy	stem				
Wir	eless Settings	Portal	Μ	1AC Filt	ering	Schedule	er Qe	oS	Rogue AP Detection			
2	ws-dmz	130)	Enab	le	WPA-PSK	Disable	Disable	Ø	1		
3	ws-its	110)	Enab	le	WPA-ENTERPRISE	Disable	Disable		W		
	SSID:	ws-its										
	Wireless VLAN ID:	110			(1-4094)						
	SSID Broadcast:	Enable										
	Security Mode:	WPA-Ent	erprise	Ŧ								
	Version:	\bigcirc Auto	O WPA-PS	K 💿	WPA2-PS	БК						
	Encryption:	\bigcirc Auto	⊖ TKIP	AES								
	RADIUS Server IP:	192.168	100.7									
	RADIUS Port: 0				(1-6553 which is	5. 0 means the defa 1812.)	ult port,					
	RADIUS Password:											
	Group Key Update Period: 0					seconds (30-8640000. 0 means no update.)						
	Portal:	Enable										

Jetzt versuche ich eine Verbindung zwischen meinem Testclient und dem WLAN. Der AccessPoint sieht die Verbindung:

P	tp-link				Access Point 🗸 🗧 ?						
N	Network Wireless Monitoring				Ma	nageme	nt	System			
			AF	0	SSID		Client				
										🕲 Refresh	
ID	MAC	Band	Access Point	SSID	SNR (dB)	CCQ(%)	Rate (Mbps)	Down (Byte)	Up (Byte)	Active Time	
1	20-39-56-0B-F9-86	2.4GHz	EAP245-50-c7-bf- 8b-46-d2	ws-dmz	27	100	53.1	633156k	459788k	0 days 18:25:24	
2	CC-9F-7A-59-39-32	2.4GHz	EAP245-50-c7-bf- 8b-46-d2	ws-dmz	26	100	52.5	90441k	3745k	0 days 06:29:44	
3	CC-9F-7A-42-FF-57	2.4GHz	EAP245-50-c7-bf- 8b-46-d2	ws-dmz	31	100	11.0	47758k	5577k	0 days 04:10:14	
4	B4-D5-BD-E8-9E-0A	2.4GHz	EAP245-50-c7-bf- 8b-46-d2	ws-its	42	100	171.5	430k	154k	0 days 00:00:14	

Portal Authenticated Guest

	🔘 Re											
ID	MAC	Band	Access Point	SSID	SNR (dB)	CCQ(%)	Rate (Mbps)	Down (Byte)	Up (Byte)	Active Time	Action	

Aber der Client kann sich nicht mit dem WLAN verbinden. Woran liegt das? Ich kenne das Problem bereits aus einem Projekt bei einem Kunden. Ein PowerShell-Command gibt mir recht. Mit dem Befehl

Get-Content -Path c:\windows\system32\logfiles\firewall\pfirewall.log -tail 10

WS IT-Solutions WSHowTo – Migration des NPS 2019-12-31 Migration auf Windows Server 2019

kann ich die letzten 10 Zeilen des Windows-Firewall-Logfiles ansehen. Dieses Logfile ist nicht standardmäßig aktiv. Bei mir wird es über eine Gruppenrichtlinie proaktiv eingeschaltet (wo wir ein schönes Beispiel für das erfolgreiche Troubleshooting mit zuvor aktivierten Logfiles haben). Man sieht schnell, dass es hier einige DROPs gibt. Die dazugehörigen Verbindungen auf UDP 1812 gehören zum Service NPS. Das sind die eingehenden Versuche vom WLAN-AccessPoint:

- P11			
📰 Bilder 🚿	Administrator: Windows PowerShell	_	×
Desktop	P5 C:\> auditpol /get /subcategory:"Netzwerkrichtlinienserver"		~
🤱 Walther, Stephar	Systemüberwachungsrichtlinie Kategorie/Unterkategorie Einstellung		
💻 Dieser PC	An-/Abmeldung		
🏪 System (C:)	PS C:\> cd .\Windows\System32\LogFiles\Firewall\		
Admin	PS C:\Windows\System32\LogFiles\Firewall> <mark>Get-Content</mark> -Path .\pfirewall.log -Tail 10 2019-12-31 17:55:24 ALLOW TCP 192.168.100.7 192.168.100.1 64193 88 0 - 0 0 0 SEND		
PSTranscrip	2019-12-31 17:55:29 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE		
Radius	2019-12-31 17:55:32 DROP UDP 192.108.100.254 192.108.100.7 59223 1812 202 RECEIVE		
Benutzer	2019-12-31 17:55:38 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE 2019-12-31 17:55:38 ALLOW TCP 192.168.100.18 192.168.100.7 64237 135 0 - 0 0 0 RECEIVE		
PerfLogs	2019-12-31 17:55:48 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE		
- Program Files	2019-12-31 17:55:57 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202		
	PS C:\Windows\System32\LogFiles\Firewall>		
- 11F 1			

Aber warum kommen diese Verbindungen nicht durch? Natürlich ist meine Windows Firewall aktiv. Aber normalerweise wird doch bei einer Rolleninstallation die erforderliche Ausnahme automatisch erstellt? So kenne ich das von fast allen anderen Rollen. Und ein Blick in die Regeln zeigt auch eine NPS-Regel für UDP 1812, die eingehenden Traffic erlaubt:

Eingehende Regeln											
Name	Gruppe	Profil	Aktiviert	Aktion	Außer Kraft setzen	Programm	Lokale Adresse	Remoteadresse	Protokoll	Lokaler Port	Remo
Wetzwerkrichtlinienserver (Legacy-RADIU	Netzwerkrichtlinienserver	Alle	Ja	Zulassen	Nein	%systemro	Beliebig	Beliebig	UDP	1645	Beliel
Wetzwerkrichtlinienserver (Legacy-RADIU	Netzwerkrichtlinienserver	Alle	Ja	Zulassen	Nein	%systemro	Beliebig	Beliebig	UDP	1646	Beliel
Netzwerkrichtlinienserver (RADIUS-Authe	Netzwerkrichtlinienserver	Alle	Ja	Zulassen	Nein	%systemro	Beliebig	Beliebig	UDP	1812	Belie
Wetzwerkrichtlinienserver (RADIUS-Konto	Netzwerkrichtlinienserver	Alle	Ja	Zulassen	Nein	%systemro	Beliebig	Beliebig	UDP	1813	Beliel
🥨 Netzwerkrichtlinienserver (RPC)	Netzwerkrichtlinienserver	Alle	Ja	Zulassen	Nein	%systemro	Beliebig	Beliebig	TCP	Dynamische	Beliel
🥑 Remotedesktop - Benutzermodus (TCP ei	Remotedesktop	Alle	Ja	Zulassen	Nein	%SystemR	Beliebig	Beliebig	ТСР	3389	Beliel
🚜 Remotederkton - Renutzermodur (TCD ei	Remotederbton	۸IIa	la la	7ulaccen	Nain	%SuctemP	Reliebia	Reliebin	TOD	2280	Ralial

Die Lösung des Rätzels ist interessant: die vordefinierte Regel funktioniert nicht. Man muss die Regel selber noch einmal erstellen. Das Phänomen kenne ich bisher nur beim NPS des Windows Server 2019. Gefixt wurde es bis heute wohl noch nicht. Egal, ich kann die neue Regel einfach selber lokal erstellen:

🔗 Windows Defender F	irewall mit	erweiterter Sicherheit									
Datei Aktion Ansic	:ht ?										
🗢 🄿 🚺 🔂 🔂	? 📷										
🔗 Windows Defender F	Firewall mit	t Eingehende Regelr	n								
🗱 Eingehende Rege	eln	Name	(Gruppe	`	Profil	Aktiviert	Aktion	Außer Kraft setzen	Programm	Lo
Ausgehende Reg	Jeln									%SystemR	Be
Verbindungssich	e 💣 Assi	istent für neue eingehe	ende Regel						×	System	Be
	Protol	kolle und Ports								System	Be
	Geben Si	ie die Protokolle und Ports	s an fürdie diese Regel gilt							%SystemR	Be
	Geberror		an, fai ale alese negergit.							%SystemR	Be
	Schritte:									System	Be
	Regel	typ	Betrifft diese Regel TCP	oder UDP?						System	Be
	Protok	colle und Ports								System	Be
	 Aktion 									%systemro	Be
	- Pacitor		0.001							%systemro	Be
	 From 			%systemro	Be						
	 Name 		Gilt diese Regel für alle le	okalen Ports ode	er für bestimmte lok	ale Ports	?			%systemro	Be
			Alle lokalen Port							%systemro	Be
			Pale lokaler i oli Pale lokaler	Dorto: 101	2 1012					%systemro	Be
			Destiminite lokale	Forts. Tot.	2,1013 miel: 80,443,500	0.5010				%SystemR	Be
				Den	spiel. 00, 443, 300	0.0010				%SystemR	Be
										%SystemR	Be
										%SystemR	Pe
										System	Be
										System	Be
										System	Be
										%SystemR	Be
										%SystemR	Be
										System	Be
										System	Be
										%SystemR	Be
					< Zu	rück	Weiter >	Abbred	chen	%SystemR	Be
										%SystemR	Be D-
1										%SystemR	ве





🔗 Windows Defender Firewall mit erweiterter Sicherheit

Date: Alle

WS IT-Solutions

Datei Aktion Ansich	nt (
🗢 🄿 🙍 📊 🗟	?								
🔗 Windows Defender Fi	irewall mit Eingehende Rege	In							
🗱 Eingehende Regel 🌠 Ausgehende Rege	In Name ein		Gruppe	Profil	Profil Aktiviert		Außer Kraft setzen	Programm	Lok
🛼 Verbindungssiche > 🍓 Überwachung	Assistent für neue eingeh Name Geben Sie den Namen und die B	ende Regel eschreibung dieser Regel an	L				×	%SystemR System %SystemR %SystemR	Beli Beli Beli Beli Beli
	Schritte:							System System	Beli Beli
	Protokolle und Ports							System System %systemro	Beli Beli
	 Profil 	Name:						%systemro %systemro	Beli Beli
	Name	Beschreibung (a	pptional):					%systemro %systemro	Beli Beli
								%systemro %SystemR	Beli Beli
								%SystemR %SystemR	Beli Beli
								%SystemR %SystemR	Beli Beli
								System System	Beli Reli



Die Regel wird sofort aktiv. Ich starte auf meinem Client einen weiteren Verbindungsversuch und dieses mal ist er erfolgreich. Auf dem NPS-Server sehe ich nun die erlaubten Verbindungen:

	🔁 Auswählen Administrator: Windows PowerShell —	\times
I 🖓 🔜 🔻 Radius	2019-12-31 18:02:52 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE 2019-12-31 18:02:55 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE	^
Datei Start Freigeben Ansicht	2019-12-31 18:03:01 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE 2019-12-31 18:03:10 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE	
← → ✓ ↑ → Dieser PC → System (C:) → Admin → Radius	2019-12-31 18:03:13 DROP UDP 192.108.100.254 192.108.100.7 59223 1812 202 RECEIVE 2019-12-31 18:03:13 DROP UDP 192.168.100.254 192.168.100.7 59223 1812 202 RECEIVE	
★ Schnellzugriff	2019-12-31 18:03:17 DROP UDP 192.168.100.12 192.168.100.255 138 138 229 RECEIVE 2019-12-31 18:03:17 DROP UDP 192.168.100.12 192.168.100.7 59223 1812 202 RECEIVE	
Desktop 🖈 📄 IN191206.log	2019-12-31 18:03:22 DROP UDP 192.168.100.2 192.168.100.7 55689 137 78 RECEIVE 2019-12-31 18:03:22 ALLOW TCP 192.168.100.2 192.168.100.7 51193 135 0 - 0 0 0 RECEIVE	
Dokumente	2019-12-31 18:03:23 DROP UDP 192.168.100.2 192.168.100.7 55689 137 78 RECEIVE 2019-12-31 18:03:42 ALLOW TCP 192.168.100.18 192.168.100.7 5826 135 0 - 0 0 0 RECEIVE	
📰 Bilder 🖈	2019-12-31 18:03:49 DROP UDP 192.168.100.13 192.168.100.255 138 138 229 RELEIVE 2019-12-31 18:03:49 DROP UDP 192.168.100.13 192.168.100.255 138 138 229 RELEIVE 2019-12-31 18:04:19 41.0W TCP 192.168.100.13 192.168.100.18 64198 5985 0 - 0 0 0 SEND	
Desktop	2019-12-31 18:04:19 ALLOW TCP 192.168.100.7 192.168.100.18 64199 5985 0 - 0 0 0 SEND 2019-12-31 18:04:40 DROP UDP 192.168.100.2 192.168.100.255 138 138 229 RECEIVE	
🔏 Walther, Stephar	2019-12-31 18:04:40 DROP UDP 192.168.100.2 192.168.100.255 138 138 229 RECEIVE 2019-12-31 18:04:57 ALLOW UDP 192.168.100.254 192.168.100.7 59223 1812 0 RECEIVE	
💻 Dieser PC	2019-12-31 18:04:57 ALLOW UDP 192.168.100.7 192.168.100.1 56569 389 0 SEND	
🏪 System (C:)	2019-12-31 18:04:57 ALLOW UDP 192.168.100.7 192.168.100.2 63709 53 0 SEND 2019-12-31 18:04:57 ALLOW UTP 192 168 100 7 192 168 100 1 64200 135 0 - 0 0 0 SEND	
Admin	2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.1 64201 49670 0 - 0 0 0 SEND	
PSTranscrip	2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.2 64202 88 0 - 0 0 0 SEND 2019-12-31 18:04:57 ALLOW IDP 192.168.100.7 192.168.100.2 51141 53 0 SEND	
Radius	2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.2 64203 389 0 - 0 0 0 SEND	
Benutzer	2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.2 64204 88 0 - 0 0 0 SEND 2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.2 64206 88 0 - 0 0 0 SEND 2019-12-31 18:04:57 ALLOW TCP 192.168.100.7 192.168.100.2 64206 88 0 - 0 0 0 SEND	
PerfLogs	PS C:\Windows\System32\LogFiles\Firewall> _	
Program Files		
Programme		
Windows		~

Zum Funktionalitätstest gehört auch die Prüfung des Accountings. Die eingehenden Authentifizierungen werden wie gewünscht in Text-Logfiles gespeichert:

IN191206.log - Editor	-		×
Datei Bearbeiten Format Ansicht Hilfe			
192.168.100.254, host/WS-CL7.ws.its, 12/31/2019, 18:04:57, IAS, WS-NPS1, 4, 192.168.100.254, 5, 0, 30, 12-C7-BF-8B-46-D2:ws-its, 31, B4-D5-BD-E8-9E-0A,	,12,140	90,61,	19, ^
192.168.100.254,host/WS-CL7.ws.its,12/31/2019,18:04:57,IAS,WS-NP51,25,311 1 192.168.100.7 12/31/2019 17:02:12 1,27,30,4149,Secure-WLAN,416	38,192 .	.168.10	00.
192.168.100.254, host/WS-CL7.ws.its, 12/31/2019, 18:04:57, IAS, WS-NPS1, 4, 192.168.100.254, 5, 0, 30, 12-C7-BF-8B-46-D2:ws-its, 31, B4-D5-BD-E8-9E-0A,	,12,140	9 0,61, :	19,
192.168.100.254, host/WS-CL7.ws.its, 12/31/2019, 18:04:57, IAS, WS-NP51, 25, 311 1 192.168.100.7 12/31/2019 17:02:12 2, 27, 30, 4108, 192.168.100.254	4,4116,	,0,412	8,w
192.168.100.254,host/WS-CL/.ws.its,12/31/2019,18:04:5/,185,WS-NP51,4,192.168.100.254,5,0,30,12-C/-BE-88-46-D2:ws-its,31,B4-D5-BD-E8-9E-0A,	,12,146	90,61,	19,
192.168.100.254,host/WS-CL7.ws.its,12/31/2019,18:04:57,1AS,WS-NP51,25,311 1 192.168.100.7 12/31/2019 17:02:12 3,27,30,4108,192.168.100.254	4,4116,	,0,412	8,W
122.106.100.224,105t/W3-LL/.W5.1t5,12/31/2019,16304:37,1A3,W3-Wr51,4,122.106.100.224,5,30,30,12-t/-DF-0B-04-D2:WS-1t5,31,D4-U5-DE-09-2-09-20-09-2-09-20-00-00-00-00-00-00-00-00-00-00-00-00-	,12,140	100 10	19,
122.100.100.224,105(M3-CL7.W5-1C,12/31/2015)10.04.37,1A3W-W53,23,311 1 122.100.100.7 12/31/2015 17.02.12 4,27,30,4149,36(U)=*WL4H3,41	12 1/(100,19	19
192.168.100.254, host/WS-C17.ws-its.123,1291,2019,18:04:57.16S.WS-WS-125.111.1.192.168.100.7.12/31/2019.17:02:15.27.30.4149. Secure-WiAN.411	27.5.4	108.19	2.1
192.168.100.254.host/WS-CL7.ws.its.12/31/2019.18:04:57.IAS.WS-NP51.4.192.168.100.254.5.0.30.12-C7-BF-88-46-D2:ws-its.31.B4-D5-BD-E8-9E-04	.12.14	0.61.	19.
192.168.100.254, host/WS-CL7.ws.its, 12/31/2019, 18:04:57, IAS, WS-NPS1, 25, 311 1 192.168.100.7 12/31/2019 17:02:12 6,4132, Microsoft: Smartcard	- oder	ander	es

Damit ist mein NPS-Service erfolgreich auf Windows Server 2019 migriert.

Nacharbeiten

Datensicherung

Zu den üblichen Nacharbeiten gehört natürlich die Einrichtung der Datensicherung. Der Server ist zwar mit der exportierten Konfiguration recht schnell wiederaufgebaut, aber mit einer Recovery geht es einfach schneller. Zudem sichere ich so auch die Logfiles des NPS mit.

Ich konfiguriere meine zentral gesteuerte SystemState-Sicherung mit Windows Server Backup. Das Feature ist bereits installiert. Es fehlt nur noch die geplante Aufgabe. Diese importiere ich als xml-Datei in der Konsole "Aufgabenplanung":

Aufgabenplanung		– 🗆 X
Datei Aktion Ansicht ?		
🗢 🔿 🖄 📰 🚺		
 Aufgabenplanung (Lokal) Aufgabenplanungsbibliot 	Name Status Trigger Nächste Laufzeit @ Urar Feed S Rereit Jeden Tan um 02:01 Ubr - Trigger Liuft um 10:08 2020 02:01:17 ab. 01:01 2020 01:01:17	Aktionen Aufgabenplanungsbibliothek
		 Einfache Aufgabe erstellen Aufgabe erstellen Aufgabe importieren
	Einfache Aufgabe erstellen Neue Aufgabe erstellen	Auguste imposeren Alle aktiven Aufgaben anzeigen Verlauf für alle Aufgaben deaktivieren
	< Aktualisieren >	 Neuer Ordner Ansicht
1 1		Aktualicieren

Aufgabenplanung										- 0	×
Datei Aktion Ansicht	?										
🗢 🄿 🖄 🖬 🚺											
Aufgabenplanung (Lokal)) Name	Status	Trigger		Nächste Lau	fzeit	Aktionen				
	Öffnen								×		•
	$\leftarrow \rightarrow \checkmark \uparrow$	v Ö	"Admin	" durchsuchen		Q					
	Organisieren 🔻	Veuer Ord	ner				8== ▼		?		
	🖈 Schnellzugriff	^ N	ame	Änderungsdatum	Тур		Größe			izeigen deaktivieren	
	📃 Desktop 刘		PSTranscript	31.12.2019 17:18	Dateiord	her					
	👆 Downloads 刘		Radius	31.12.2019 18:04	Dateiord	her					
	付 Dokumente 🕫		🖞 config.xml	31.12.2019 17:19	XML-Dok	ument	68 KB				
	📰 Bilder 刘		ServerSicherung.xml	31.12.2019 18:14	XML-Dok	tument	4 KB				
	E Desktop										
	👗 Walther, Steph	ar									
	💻 Dieser PC										
	🏪 System (C:)										
	📙 Admin										
	PSTranscri	p'									
	Radius	~									
	1	Datei <u>n</u> ame	ServerSicherung.xml		~	XML-D	ateien (*.xml)		\sim		
			<u> </u>		,	Ö <u>f</u> f	inen Ab	breche	n		
L L							1			1	

Der ausführende Account ist wieder ein Group Managed Service Account, denn ich wie bei den anderen Migrationen auch von meinem Domain Controller aus mit einer selbst programmierten PowerShell-GUI einrichte. Zuerst entferne ich hier aber noch die alten ServerAccounts WS-RA1 und WS-RA2:

🦕 gMSA-Admin		– 🗆 ×
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:
gMSA-ADFS (Service ADFS) <u>oMSA-Backup (TaskUser für BMR)</u> gMSA-Hontor (TaskUser für Montoring) gMSA-SQLDPM (Service SQL auf WS-DPM)	WS-DC1.ws.its WS-HX1.ws.its WS-MX1.ws.its (offline) WS-MX1.ws.its (offline) WS-MX1.ws.its WS-MX1.ws.its WS-RA2.ws.its WS-RA2.ws.its WS-RDS1.ws.its WS-RDS3.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC2.ws.its WS-DC3.ws.its WS-DC4.ws.its WS-VD4.ws.its WS-HV3.ws.its WS-HV3.ws.its WS-HV3.ws.its WS-HV4.ws.its WS-HV4.ws.its WS-HV4.ws.its	
Einsatz als:		
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:
gMSA-ADFS (Service ADFS) MSA-Backup (TeakUser für BMR) gMSA-Montor (TeakUser für Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM)	WS-DC1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX1.ws.its WS-MX2.ws.its WS-RDS1.ws.its WS-RDS1.ws.its WS-RDS1.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-RDS2.ws.its WS-CQ.ws.its WS-DC4.ws.its WS-PDW.ws.its WS-HV3.ws.its WS-HV3.ws.its WS-HV4.ws.its WS-HV4.ws.its WS-HV4.ws.its	
erstelle gMSA lösche gMSA bearbeite gMSA	weiterer Server entferne Server teste gMSA	weitere Gruppe entferne Gruppe

Dann erlaube ich die Passwortübertragung zum WS-NPS1:



🛥 gMSA-Admin		- 0	\times
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:	
gMSA-ADFS (Service ADFS) gMSA-Backup (TaskUser für BMR) gMSA-Monitor (TaskUser für Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM)	WS-DC1.ws.its WS-FS1.ws.its WS-MX1.ws.its WS-K32.ws.its WS-FS2.ws.its WS-FS2.ws.its W neuer Server für gMSA V Geben Sie den Namen (nicht den FQDN) des zusätzlichen Servers ein V V v v v v v v v v v v v v v		~
erstelle gMSA lösche gMSA bearbeite gMSA	weiterer Server entferne Server teste gMSA	weitere Gruppe entferne Gruppe	
Einsatz als:			

Über das PowerShell-Remoting kann ich dann auf dem Server WS-NPS1 die geplante Aufgabe remote umkonfigurieren:

드 gMSA-Admin					-	- 🗆	×		
vorhandene gMSA:	zug	zugehörige Server:			zugehörige Gruppen:	zugehörige Gruppen:			
gMSA-ADFS (Service ADFS) WS-DC1.ws gMSA-Backup (TaskUser für BMR) WS-FS1.ws gMSA-SQLDPM (Service SQL auf WS-DPM) WS-KS1.ws WS-RDS1.ws WS-RDS2.ws WS-RDS2.ws WS-RDS2.ws WS-DC3.ws WS-CC3.ws WS-NC1.ws WS-CC3.ws WS-RDS1.ws WS-RDS1.ws WS-RDS2.ws WS-RDS2.ws WS-DC3.ws WS-CC3.ws WS-NC4.ws WS-NC4.ws WS-NC5.ws WS-NC4.ws WS-NC5.ws WS-NC4.ws WS-NC4.ws WS-NC4.ws WS-NC4.ws <th>(online)</th> <th></th> <th colspan="3"> direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-Rb-Admins GG-SEC-Server-Rb-Admins GG-SEC-Server-MyperV-Admins GG-SEC-Clients-JB-Admins GG-SEC-Clients-JB-Admins GG-Admin-Backup Sicherungs-Operatoren indirekte Gruppen (durch Verschachtelung): LD-Admin-Backup LD-Admin-SQL-DPM LD-D-Admin-Area-R LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-RDP LD-SEC-Clients-JB-RDP</th>			(online)		direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-Rb-Admins GG-SEC-Server-Rb-Admins GG-SEC-Server-MyperV-Admins GG-SEC-Clients-JB-Admins GG-SEC-Clients-JB-Admins GG-Admin-Backup Sicherungs-Operatoren indirekte Gruppen (durch Verschachtelung): LD-Admin-Backup LD-Admin-SQL-DPM LD-D-Admin-Area-R LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-Admins LD-SEC-Clients-JB-RDP LD-SEC-Clients-JB-RDP				
erstelle gMSA lösche gMSA Einsatz als: Task	bearbeite gMSA w	veiterer Serve Optionen zu a	er entferne Server	teste gMSA	weitere Gruppe entferne Gruppe				
Server	TaskName		Account		Pfad		^		
WS-NPS1	ServerSicherung		admin-setup		\ \				
WS-NPS1	User_Feed_Synchronization	ion-{A6AB57 svsadm			X				
WS-NPS1	Server Initial Configuration Ta	ask	SYSTEM		\Microsoft\Windows\				
WS-NPS1	.NET Framework NGEN v4.	0.30319	SYSTEM		\Microsoft\Windows\.NET Framework\				
WS-NPS1	WS-NPS1 .NET Framework NGEN v4.0.		SYSTEM		\Microsoft\Windows\.NET Framework\				
WS-NPS1 .NET Framework NGEN v4.0.30319 6		0.30319 6	SYSTEM		\Microsoft\Windows\.NET Framework\				
WS-NPS1	.NET Framework NGEN v4.	0.30319 C	SYSTEM		\Microsoft\Windows\.NET Framework\				
WS-NPS1	WS-NPS1 AD RMS Rights Policy Template Man				\Microsoft\Windows\Active Directory Rights M	anagement Se	··· 🗸		
lese alle Server setze gMSA ein bereit							.:1		



🛥 gMSA-Admin				— 🗆	\times
vorhandene gMSA:	zugehörige Sen	ver:		zugehörige Gruppen:	
gMSA-ADFS (Service ADFS) gMSA-Backup (TaskUserfür BMR) gMSA-Monitor (TaskUserfür Monitoring) gMSA-SQLDPM (Service SQL auf WS-DPM) erstelle gMSA lösche gMSA bearbei Einsatz als: Task V Klicke in ei	WS-DC1.ws.its WS-FS1.ws.its WS-FS1.ws.its WS-CA1.ws.its WS-CA1.ws.its WS-RDS2.ws.it WS-RDS3.ws.it WS-RDS3.ws.it WS-RDS3.ws.its WS-DC3.ws.its WS-DC3.ws.its WS-DC3.ws.its WS-DC4.ws.its WS-DC4.ws.its WS-DC4.ws.its WS-DC4.ws.its WS-HV4.ws.its W	s s rfolg Der Task wurde umgestellt!	X	direkte Gruppen: GG-SEC-Server-Monitoring-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-RDS-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Server-HyperV-Admins GG-SEC-Server-HyperV-Admins GG-Admin-Backup Sicherungs-Operatoren	~
Server TaskName	e	UK		Pfad	^
WS-NPS1 ServerSich	erung	ws\gMSA-Backup\$		N	
WS-NPS1 User_Feed	_Synchronization-{A6AB57	sysadm		X	
WS-NPS1 Server Initia	al Configuration Task	SYSTEM		\Microsoft\Windows\	
WS-NPS1 .NET Frame	ework NGEN v4.0.30319	SYSTEM		\Microsoft\Windows\.NET Framework\	
WS-NPS1 .NET Frame	ework NGEN v4.0.30319 64	SYSTEM		\Microsoft\Windows\.NET Framework\	
WS-NPS1 .NET Frame	ework NGEN v4.0.30319 6	SYSTEM		\Microsoft\Windows\.NET Framework\	
WS-NPS1 .NET Frame	ework NGEN v4.0.30319 C	SYSTEM		\Microsoft\Windows\.NET Framework\	
WS-NPS1 AD RMS R	ights Policy Template Mana			\Microsoft\Windows\Active Directory Rights Management Se	~
lese alle Server setze gMSA ein bereit		·			

Die geplante Aufgabe startet ein zentral abgelegtes Script. Dessen Konfiguration ist eine simple ini-Datei. Hier entferne ich die Sicherungsjobs der alten Server:

Sicherun	g.ini - Editor							-	×
Datei Bearb	eiten Forn	nat Ansicht	Hilfe						
recipient	s2=								^
mailserve	r2=								
[Sicherun	gen]								
'Optionen	: -ohneT	ag							
'Server	# Dela	/ # Tage	# JobName	# JobDefinition	# Dest	: # Optionen			
WS-CM	# 0	# 3@135	# BMR	<pre># c: -systemstate -allCritical -vssFu</pre>	11 # 1	#			
WS-DC1	# 20	# 6@135	# BMR	# c: -systemstate -allCritical -vssFu	11 # 1	#			
WS-FS1	# 40	# 3@135	# BMR	<pre># c: -systemstate -allCritical -vssFu</pre>	11 # 1	#			
WS-HV4	# 60	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFu</pre>	11 # 3	#			
WS-RA1	# 80	# 6@135	# BMR	# c: -systemstate -allCritical -vssFu	11 #1	#			
WS-MON	# 100	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFu</pre>	11 # 1	#			
WS-RDS1	# 120	# 6@135	# BMR	<pre># c: -systemstate -allCritical -vssFu</pre>	11 # 1	#			
WS-WAC	# 140	# 3@135	# BMR	# c: -systemstate -allCritical -vssFu	11 # 1	#			
WS-MX1	# 160	# 6@135	# BMR	# c: -systemstate -allCritical -vssFu	11 # 1	#			
WS_HV3	# 0	# 60246	# RMR	# c: _systemstate _all(ritical _yssE	11 # 3	#			
WS-DC2	# 20	# 60246	# BMR	# c: _systemstate _all(ritical _vssFi	11 # 1	#			
WS-ES2	# 10	# 30246	# BMR	# c: _systemstate _all(ritical _vssFi	11 # 1	#			
WS-RA2	# 60	# 60246	# BMR	# c: -systemstate -allCritical -vsst	11 #1	#			
WS-RDS2	# 80	# 60246	# BMR	# c: _systemstate _all(nitical _vsst	11 #1	#			
WS-DPM	# 110	# 60246	# BMR	# c: _systemstate _all(ritical _vssFi	11 # 3	#			
WS-CA1	# 130	# 30246	# BMR	# c: _systemstate _all(ritical _vssFi	11 # 1	#			
WS-ATA	# 150	# 30246	# BMR	# c: _systemstate _all(ritical _vssFi	11 # 1	#			
	# 170	# 60240	# BMR	# c: systemstate allChitical vsst	11 #1	#			
ND-11/2	# 170	# 0@240	# Dritt	# csystemstate -artchititar -vssh		π			
WS-DC3	# 0	# 3@246	# BMR	# C: -systemstate -allcritical -yssFu	11 # 2	#			
WS-RDS3	# 0	# 3@135	# BMR	# C: -systemstate -allcritical -vssFu	11 # 2	#			
		c		· · · · · · · · · · · · · · · · · · ·					
[Export]									~
<									>
					Windows (CRLE)		Zeile 1 Snalte 1	100%	

Und dann konfiguriere ich die Datensicherung für den neuen WS-NPS1:

WS IT-Solutions

Sicherung	g.ini - Editor									-	×
Datei Bearb	eiten Form	at Ansicht Hill	fe								
recipient	s2=										^
mailserve	r2=										
[Sicherun	gen]										
'Optionen	: -ohneTa	g									
'Server	# Delay	/ # Tage	# JobName	<pre># JobDefinition</pre>		# Dest	# Optionen				
WS-CM	# 0	# 3@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-DC1	# 20	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-FS1	# 40	# 3@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-HV4	# 60	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full # 3	#				
WS-NPS1	# 80	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-MON	# 100	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-RDS1	# 120	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-WAC	# 140	# 3@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS-MX1	# 160	# 6@135	# BMR	<pre># c: -systemstate</pre>	-allCritical -vss	Full #1	#				
WS_HV3	# 0	# 60246	# BMR	# c: _svstemstate	-allCritical -vss	Eu11 # 3	#				
WS-DC2	# 20	# 6@246	# BMR	# c: _systemstate	-allCritical -vss	Full # 1	#				
WS-ES2	# 10	# 3@246	# BMR	# c: _systemstate	-allCritical -vss	Full # 1	#				
WS-RDS2	# 90	# 6@246	# BMR	# c: _systemstate	-allCnitical -vss	Gull # 1	" #				
WS-DPM	# 110	# 6@246	# BMR	# c: _systemstate	-all(ritical -ves	Full # 3	#				
WS-CA1	# 130	# 3@246	# BMR	# c: _systemstate	-all(ritical -vss	Full # 1	#				
WS-ATA	# 150	# 3@246	# BMR	# c: -systemstate	-allCritical -vss	Full # 1	#				
WS-MX2	# 170	# 6@246	# BMR	# c: _systemstate	-allCritical -vss	Full # 1	#				
NJ-102	# 1/0	# 0@240	# Dritt	# csystemstate	-arrenterear -vss						
WS-DC3	# 0	# 3@246	# BMR	# C: -systemstate	-allcritical -vss	Full # 2	#				
WS-RDS3	# 0	# 3@135	# BMR	# C: -systemstate	-allcritical -vss	Full # 2	#				
		Ū.		<u>,</u>							
[Export]											
Server	# Tage	# lohname	# Temn	# 7iel							~
<											>
						Windows (CRLF)		Zeile 47, Spalte 96	100%		

Die alten Server hatten natürlich Sicherungen erstellt. Diese benötige ich nicht mehr. Daher entferne ich sie aus dem Sicherungsverzeichnis:

📙 💆 📙 🗢 Serversicherung						- 0	×
Datei Start Freigeben Ansicht							~ 🕐
← → → ↑ 📙 → Dieser PC → BMR (E	:) > Backup > Serversicherung	>			~ ∿	"Serversicherung" durchsuche	en 🔎
📌 Schnellzugriff	Name	Änderungsdatum	Тур	Größe			
🛄 Desktop	WS-ATA	03.10.2019 13:18	Dateiordner				
🤱 Walther, Stephan - T1	WS-CAT	27.08.2019 03:30	Dateiordner				
💻 Dieser PC	WS-DC1	26.08.2019 20:27	Dateiordner				
🏪 System (C:)	WS-DC2	27.08.2019 01:20	Dateiordner				
BMR (E:)	WS-FS1	28.08.2019 01:40	Dateiordner				
Backup	WS-FS2	27.08.2019 01:40	Dateiordner				
Serversicherung	WS-MON	09.09.2019 02:40	Dateiordner				
DPM (G:)	WS-MX2	27.08.2019.02:20	Dateiordner				
🛖 Freigaben (M:)	WS-RA1	28.08.2019 02:50	Dateiordner				
🐂 Bibliotheken	WS-RA2	Öffnen	ordner				
💣 Netzwerk	WS-RDS1	In neuem Fenster öffnen	ordner				
😰 Systemsteuerung	WS-RDS2	An Schnellzugriff anheften	ordner				
🔯 Papierkorb	WS-WAC	Zugriff gewähren auf	> ordner				
		Senden an	>				
		Ausschneiden					
		Kopieren					
		Verknüpfung erstellen					
15 Elemente 2 Elemente ausgewählt Sta	tus: 🎎 Freigegeben	<mark>Löschen</mark> Umbenennen					
		Eigenschaften					

Morgen kann ich die Datensicherung des neuen Servers in der Monitor-Email sehen. Die Sicherung umfasst den gesamten Server. Eine zusätzliche Nutzdatensicherung ist nicht erforderlich.

Bereinigung der VMs

Jetzt kann ich den Speicherplatz in den Hyper-V-Servern freigeben. Dazu lösche ich die beiden alten VMs:



Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🔿 🙍 📊 🛛 🗊							
Hyper-V-Manager							
WS-HV3	Virtuelle Computer						
WS-HV4	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
	WS-ATA	Wird ausgeführt	1 %	6144 MB	12.12:45:07		8.0
	🗧 WS-CM	Wird ausgeführt	0 %	4096 MB	13.14:27:49		8.0
	WS-DC1	Wird ausgeführt	0 %	2352 MB	01:30:31		8.0
	WS-EVIL1	Aus					8.0
	WS-FS1	Wird ausgeführt	0 %	2994 MB	12.14:36:45		8.0
	WS-MM	Wird ausgeführt	0%	898 MB	3.21:50:51		9.0
	WS-MX1	Wird ausgeführt	3%	14336 MB	12.14:19:55		8.0
	WS-NPS1	Wird ausgeführt	1%	1518 MB	12 14:27:29		9.0
	WS-RA1	Aus	1 /6	5120 MB	13.14.37.33		8.0
	WS-RDS1	Wird auso	Verbinden		4:35:51		8.0
			Finstellungen				
			cinstendigen				
			Konfigurationsv	ersion upgraden			
			Starten				
			Prüfpunkt				
			Variabishan				
			Functioner				
			Exportieren				
			Umbenennen				
			Loschen				
			Replikation aktiv	vieren			
	Dellfoundate		Hilfe				
	rruipuikte						
_							
Hyper-V-Manager							
Datei Aktion Ansicht ?							
🗢 🔿 📶 🔽 🖬							
Hunor V Managor							
WS-HV3	Virtuelle Computer						
WS-HV4	Name	Phase	CPU-Auslast	Zugewiesener Spei	Betriebszeit	Status	Konfiguratio
	WS-ACAD	Aus		5 1			80
	WS-CA1	Wird ausgeführt	0%	828 MB	3 21:47:12		8.0
	WS-CL6	Wird ausgeführt	0%	890 MB	05:16:08		9.0
	WS-DC2	Wird ausgeführt	0 %	2524 MB	01:33:51		8.0
	WS-DPM	Wird ausgeführt	0%	3714 MB	3.21:49:01		9.0
	WS-FS2	Wird ausgeführt	0 %	1068 MB	3.21:48:57		9.0
	WS-MON	Wird ausgeführt	6 %	2504 MB	03:03:17		8.0
	WS-MX2	Wird ausgeführt	1 %	14336 MB	3.21:47:41		8.0
	WS-PFS1b	Wird ausgeführt	0 %	5120 MB	3.21:49:41		8.0
	WS-RA2	Aus					8.0
	WS-RDS2	Wird ausgefü	Verbinden		:12		8.0
	WS-Steuer	Aus	Einstellungen				8.0
	WS-WAC	Wird ausgefü	Konfiguration	sversion ungraden	:41		9.0
			a	sreision apgradenin			
			starten				
			Prüfpunkt				
			Verschieben				
			Exportieren				
			exportieren				
			Umbenennen				
			Umbenennen Löschen				

Die virtuellen Festplatten bleiben dabei erhalten. Diese lösche ich manuell mit dem Windows Explorer:



📙 🛛 🛃 🖬 🖛 🗍 Hyper-V					
Datei Start Freigeben	Ansicht				
\leftarrow \rightarrow \checkmark \uparrow \square \rightarrow Diese	r PC → Tier-Gold (V:) → H	lyper-V >			
🖈 Schnellzugriff	Name	Änderur	ngsdatum Typ	Größe	
— — — —	WS-ATA	25.08.20	19 17:12 Dateiordner		
Desktop	WS-CM	28.11.20	19 15:23 Dateiordner		
🤱 Walther, Stephan - T1	WS-DC1	29.03.20	18 16:20 Dateiordner		
💻 Dieser PC	WS-EVIL1	28.11.20	19 18:48 Dateiordner		
🏪 System (C:)	WS-FS1	15.11.20	19 16:28 Dateiordner		
Daten (D:)	WS-MM	26.12.20	19 10:21 Dateiordner		
Ereigaben (M:)	WS-MX1	24.01.20	19 07:26 Dateiordner		
Tier-Gold (\/r)	WS-NPS1	31.12.20	19 17:05 Dateiordner		
	WS-PFS1a	03.01.20	19 16:39 Dateiordner		
Hyper-V	WS-RA1	16.09.20	19 06:43 Dateiordner		
WS-ATA	WS-RDS1	Öffnen	ner		
WS-CM		In neuem Fenster öffnen			
WS-DC1		An Schnellzugriff anheften			
WS-EVIL1		Zugriff gewähren auf	>		
WS-FS1		Vorgängerversionen wiederh	erstellen		
WS-MM		In Bibliothek aufnehmen	\		
WS-MX1		An "Start" anheften			
WS-NDS1		- An start annerten			
WS DEST.		Senden an	>		
WS-PFSTa		Ausschneiden			
WS-RAT		Kopieren			
WS-RDS1		Verknünfung erstellen			
🛖 Tier-Silber (W:)		Löschen			
🐂 Bibliotheken		Umbenennen			
i Netzwerk					
🔝 Systemsteuerung		Eigenschaften			
-					
📙 🛃 🥃 🗧 Hyper-V					
Datei Start Freigeben	Ansicht				
← → × ↑ 📘 > Netzwerk	> ws-hv3 > v\$ > Hyper-V	>			
📌 Schnellzugriff	Name	Änderungsdatum	Typ Größe		
	WS-CA1	06.08.2019 14:44	Dateiordner		
Desktop	WS-DC2	06.08.2019 16:08	Dateiordner		
Walther, Stephan - 11	WS-DPM	16.08.2019 08:48	Dateiordner		
Uleser PC	WS-FS2	15.11.2019 11:51	Dateiordner		
Daten (C:)	WS-MUN	08.09.2019 10:31	Dateiordner		
Ereigaben (Mt)	WS-PFS1b	07.08.2019 07.28	Dateiordner		
Tier-Gold (//)	WS-RA2	06.00.2010.14.66	Pateiordner		
Tier-Silber (W)	WS-RDS2 Öffnen		ateiordner		
Bibliotheken	WS-WAC In neuer	m Fenster öffnen	ateiordner		
Netzwerk	Vorgăno	nenzugrin annerten nerversionen wiederherstellen			
ws-hv3	An "Star	rt" anheften			
VS	Sendon	an			
Hyper-V					
Systemsteuerung	Ausschr	neiden			
Papierkorb					
	Verknüp	n n n n n n n n n n n n n n n n n n n			
	Umben	ennen			
		haften			
	Eigensc	naten			

Im Active Directory finde ich die beiden verwaisten Computerkonten. Diese lösche ich:



Damit sind die alten Server bereinigt.

Windows Updates

WS IT-Solutions

Der neue Server darf natürlich auch Updates über meinen WSUS erhalten. Da er aber noch nicht hochverfügbar ist, kommt er in die Gruppe mit der verzögerten Update-Genehmigung. Sollte mal ein Update Probleme bereiten, dann erkenne ich das an Servern der Gruppe "Update-Sofort" und habe dann die Möglichkeit, die Verteilung aufzuhalten:



Der Server holt die Updates automatisch nach. Ich starte die Installation aber manuell, damit ich deren Ausführung überwachen kann:

Einstellungen	- 0	×
☆ Startseite	Windows Update	
Einstellung suchen	*Einige Einstellungen werden von Ihrer Organisation verwaltet. Konfigurierte Updaterichtlinien anzeigen	
Update und Sicherheit	Es sind Updates verfügbar.	
📿 Windows Update		
些 Übermittlungsoptimierung	2019-12 Kumulatives Update für .NET Framework 3.5, 4.7.2 und 4.8 für Windows Server 2019 für x64 (KB4533094) Status : Neustart ausstehend	
Windows-Sicherheit	2019-12 Kumulatives Update für Windows Server 2019 für x64-basierte Systeme (KB4530715) Status: Wird installiert – 74%	
Problembehandlung	Windows-Tool zum Entfernen bösartiger Software x64 - Dezember 2019 (KB890830) Status: Installation ausstehend	
S Wiederherstellung	Updateverlauf anzeigen	
O Aktivierung	Erweiterte Optionen	

Einen Neustart später ist der Server up-to-date.

Monitoring

VS IT-Solutions

Mittlerweile hat mich mein PRTG-Monitoring via Push-Benachrichtigung informiert, dass 2 virtuelle Computer fehlen und die WAP-Dienste nicht erreichbar sind. Daher wird es Zeit, die Konfiguration anzupassen. Ich entferne die alten VMs und trage dafür die neue VM ein. Dann entferne ich noch alle Sensoren für ADFS und WAP:



Abhängigkeit zur PKI

Unmittelbar nach dem Abschluss einer Migration kann eigentlich noch keine Aussage über deren Erfolg getroffen werden. Manche Abhängigkeiten und Probleme bemerkt man erst im Anschluss. So ist es mir einen Tag später auch gegangen. Ich erhalte jeden Morgen einige Mails, mit denen ich verschiedene Funktionalitäten prüfen kann. Eine Mail davon sendet mir eine Auswertung der letzten 24 Stunden, in der verdächtige Anmeldeaktivitäten aufgezeigt werden. Mit der PowerShell hab ich dazu eine hübsche grafische Darstellung gerendert: WS IT-Solutions



Interessant ist dabei der Zeitpunkt. Ab 13:00 des Vortages hat es vermehrt Authentifizierungsversuche gegeben, die aber alle geblockt wurden. Diese Anfragen kamen von meiner PKI, die auf WS-CA1 läuft. Was will denn die PKI von meinem WS-NPS1? Ha, ganz einfach: ich hatte ganz vergessen, dass auf WS-RA1 auch ein Sperrlistenverteilungspunkt platziert war. Diesen konnten die Clients über http ansprechen und die Sperrliste meiner PKI herunterladen. Dazu muss der WS-CA1 aber zuvor seine Sperrlistendatei auf dem Server speichern können. Und dafür ist wiederum eine Anmeldung erforderlich.

Ein Blick in die Konfiguration der Zertifizierungsstelle zeigt den jetzt falschen Eintrag:



Gleichzeitig ist damit auch klar, dass ich im DNS noch die beiden alten Hostnames mit ihren IP's registriert habe. Denn sonst würde die Verbindung nicht funktionieren:

PS C:\> Resolve-DnsName ws-np	os1						^
Name			Туре	TTL Section	IPAddress		
 ws-nps1.ws.its				1200 Answer	192.168.100.7		
PS C:\> Resolve-DnsName crl.w	s.its						
Name	Туре	TTL	Section	NameHost			
crl.ws.its	CNAME	3600	Answer	ws-ral.ws.its			
Name : ws-ra1.ws.its							
TTL : 1200							
Section : Answer							
IP4Address : 192.168.100.7							

OK, diese Funktion muss angepasst werden. Der alte WS-RA1 war auch ein Webserver durch seine VPN-Funktionalität. Daher konnte er auch die CRL-Datei veröffentlichen. Der neue NPS-Server ist aber kein Webserver mehr. Abgesehen davon macht diese Kombination von PKI und NPS keinen Sinn. Daher verschiebe ich den Endpunkt auf die Zertifizierungsstelle selbst. Das kann ich ja bei der Migration der PKI wieder anpassen.

Mein Server WS-CA1 ist ein Server Core mit Windows Server 2016. Dort lege ich ein Verzeichnis für die Sperrlisten an:



Lokal editiere ich nun den Wert in der Registry. Das geht deutlich schneller als der Umweg über den grafischen Assistenten (dort wäre ein Abändern des Pfades nicht vorgesehen):

ninistrator: C:\Windows\system32	\cmd.exe - powershell				- - X	
<pre>\> regedit \></pre>					^	
Registrierungs-Editor Datei Bearbeiten Ar	r nsicht Favoriten ?					- - ×
· · · · · · · · · · · · · · · · · · ·	Configuration	~	Name	Тур	Daten	^
	WS-ITS-Zertifizierungsstelle-CA1 CSP EncryptionCSP >	-	CRLDeltaOverlapPeriod CRLDeltaOverlapUnits CRLDeltaOverlapUnits CRLDeltaPeriod CRLDeltaPeriodUnits	REG_SZ REG_DWO REG_SZ REG_DWO	Mehrteilige Zeichenfolge bearbeiten Wertname: CRLPublicationURLs	
	A - PolicyModules Performance Security cht4vbd CLFS ClipSVC clr_optimization_v4.0.30319_32 clr_optimization_v4.0.30319_64 CmBatt CMU	=	Image: CRLEditFlags Image: CRLEditFlags Image: CRLOverlapPeriod Image: CRLOverlapUnits Image: CRLOverlapUnits	REG_DWO REG_DWO REG_BINA REG_SZ REG_DWO REG_SZ REG_DWO REG_MULT REG_SZ REG_SZ	Vert: 79:1dap:///CN=%7%8.CN=%2,CN=CDP 6:http://crt.ws.ts2/crtd/%3%8%9.crt 65:c:\admin/PKI%3%6%9.crt	CN=Public Key Services,
	CngHwAssist CompositeBus COMSysApp ConDrv CoreMessagingRegistrar		EKUOIDsForPublishExpiredCertInCRL Enabled ForceX500NameLengths ForceTeletex HighSerial	REG_MULT REG_DWO REG_DWO REG_DWO REG_DWO	< III	OK Abbrech
	crypt32 CryptSvc DCLocator DcomLaunch	~	₩ InterfaceFlags ₩ KRACertCount	REG_DWOF REG_DWOF REG_MULT	RD 0x00000641 (1601) RD 0x00000000 (0) I_SZ	~
Computer\HKEY_LOCAL	MACHINE\SYSTEM\CurrentControlSet\Service	es\Cei	rtSvc\Configuration\WS-ITS-Zertifizierung	sstelle-CA1		

Die Zertifizierungsstelle muss als Service neustarten, damit diese Konfiguration geladen wird:



🔤 Administrator: C:\Windows\system32\cmd.exe - powershell	_ 0	×
PS C:\> Restart-Service CertSvc PS C:\> _		^
		\sim

Der Wert wird korrekt in der Verwaltungskonsole angezeigt:

certsrv - [Zertifizierungsstelle (ws-ca1.ws.its)\WS-IT	Zertifizierungsstelle-CA1]	– 🗆 X
Datei Aktion Ansicht ?		
Datei Aktion Ansicht ?	Eigenschaften von WS-ITS-Zertifizierungsstelle-CA1 ? × fikate nfikate en forderung Speicherung Zertifikatverwaltungen Registrierungs-Agents Gberwachung Wiederherstellungs-Agents Sicherheit Allgemein Richtlinienmodul Beendigungsmodul Erweiterungen Erweiterung auswählen: Sperifisten-Verteilungspunkt V Geben Sie Standorte an, von denen Benutzer eine Zertifikatssperifiste Von Von	
	ematen konnen. Idap:///CN= <catuncstedname><crlnamesuffix>:CN=<servershotnar http://crtws.ts/cdd/<caname><crlnamesuffix>CDetaCRLAIowed>:cf cxadminVFKIxCaName><crlnamestfix><detacrlaiowed>:cf Hinzufügen Entfemen</detacrlaiowed></crlnamestfix></crlnamesuffix></caname></servershotnar </crlnamesuffix></catuncstedname>	
	John alle Speritisten einbeziehen. Legt fest, wo dies bei manueller Veröffentlichung im Active Directory veröffentlicht werden soll In Speritisten einbeziehen. Wird z. Suche von Deltasperlisten verwendet In CDP-Erweiterung des ausgestellten Zertfikats einbeziehen Deltasperlisten an diesem Ott veröffentlichen In die IDP-Erweiterung ausgestellter CRLs einbeziehen	

Und auch die Sperrlistendateien tauchen korrekt auf:

ſ	ov. Admi	nistrator: C:\Windows\syst	em32\cmd.exe - po	wershell		 ×
I	PS C:\:	certutil -crl				^
	CertUt:	.1: -CRL-Betehl wu	irde ertolgrei	ch ausgetuhr	٠t.	
		dir C:\Admin\PKT				
1		dill of (Admini (Ad				
	Ver	zeichnis: C:\Admi	n\PKI			
I	Mode	Last	WriteTime	Length	Name	
		62 61 2626	16:04	760	WS_ITS_Zentifizienungsstelle_CA1(1)+ cnl	
	-a	02.01.2020	16:04	1037	WS-ITS-Zertifizierungsstelle-CA1(1).crl	
	-a	02.01.2020	16:04	755	WS-ITS-Zertifizierungsstelle-CA1+.crl	
	-a	02.01.2020	16:04	1024	WS-ITS-Zertifizierungsstelle-CA1.crl	
	PS C:\:					

Aber wie sollen meine Clients und Server diese Dateien finden und herunterladen? Ganz einfach: Bisher war der Verteilungspunkt ein Webservice hinter einem CNAME. Dieser zeigte auf meinen alten WS-RA1. Im DNS kann ich den Record nun auf meine Windows PKI zeigen lassen:



🍰 DNS-Manager								_		×
Datei Aktion Ansicht ?	20									
	1									_
 DNS WS-DC1 ws-dc2 Zivischengespeicherte Lookupvorgänge Forward-Lookupzonen Grunsdcs.ws.its Grunz.ws.its 	Name admin ata autodiscover crl DAG-1		Typ Host (A) Host (A) Alias (CNAMI Alias (CNAMI Host (A)	;) ;)	Daten 192.168.100.22 192.168.100.23 email.ws.its. ws-ra1.ws.its. 192.168.100.15			Zeitstempel Static Static Static Static Static 01.01.2020 21:00:00		^
 Genail.ws-its.de Ids.ws-its.de Ids.ws-its.de Ids.ws-its.de Ids.ws-its Werrese-Lookupzonen Bedingte Weiterleitungen WS-DC3 	Drucker-1 Drucker-2 email ForestDnsZon ntopng prtg wac wac WS-AP1 WS-ATA WS-CA1	Eigenschaften Alias (CNAME) Aliasname (br orl Vollqualifiziert orl.ws.its Vollqualifiziert ws.calt.ws.its	Host (A) von crl Sicherheit ei Nichtangabe w er Domänennam s.	ird übergeordne e: e des Zielhosts:	192.168.100.51 te Domäne verw	? endet): urchsucher	×	Static Static Static Static Static Static Static Static Static Static 02.01.2020 05:00:00 02.01.2020 13:00:00		
	WS-CL1	Entrag lör Zeitstemp Gültigkeitsda	ichen, sobald er el des Eintrags: uer (TTL):	verfällt 0 :0 <u>5</u> 0K) :0 (TTTTT: Abbrechen	HH.MM.SS	5) men	02.01.2020 09:00:00		~

Dazu muss ich dort aber auch ein virtuelles Verzeichnis im IIS erstellen. Dieses fungiert als eine Art http-Freigabe auf den lokalen Ordner. Der Name ist bereits allen Systemen bekannt. Den muss ich also beibehalten. Der IIS ist bereits auf meiner Windows PKI installiert. Aber die Verwaltungstools fehlen, da es ja ein Server Core ist. Also verwende ich die Konsole auf meinem Admin Server und stelle aus dieser eine Verbindung zur PKI her:

🍋 Internetinforma	tionsdienste (IIS)-Manager				- 0	×
	Startseite				🔯 😣	🔓 🔞 🗸
Datei Ansicht	?					
Verbindungen		Merrosoft Internetinform:	ationedianeta	10		
🔍 - 🔒 🖄 😥		Anwendungsserver-Manage		10		
> Startser	Aktualisieren					
•	Mit einem Server verbinden	tzte Verbindungen		Verbindungsaufgaben	Onlineressourcen	
	Mit einer Site verbinden	lame	Server	Mit Localhost verbinden Mit einem Server verhinden	IIS-News und -Informationen	
	Mit einer Anwendung verbinden	ws-ca1.ws.its	ws-ca1.ws.its	Mit einer Site verbinden	IIS-Foren	
		110 HAC	localitose	Mit einer Anwendung verbinden	TechNet MSDN	
					ASP.NET-News	
					Microsoft-Webplattform	
		<	>			
		IIS-News			IIS News aktive	
		IIS News sind deaktiviert, k	licken Sie auf den Link "IIS N	aver aktivieren" um die aktuellen Online-News zu erk	alten	
		ino reeves sind deaktiviere, k	incken sie auf den eink ins fo	ews aktivitient, unt die aktivelien online news zu en	biten.	
Bereit						



📬 Internetinformationsdienste (IIS)-Man	ager	— 🗆 X
← → Viartseite		🗰 🖂 🙆 i 🔞 -
Datei Ansicht ?	Mit Server verbinden	? ×
Verbindungen Q • 🔛 🖄 🖗 	Verbindungsdetails für den Server angeben	
> 📲 WS-WAC (WS\stephan-T1)	Servername: ws-ca1jws.its v Beispiel: localhost, www.site.net oder WESTSRV01:8080	nlineressourcen 5-News und -Informationen 5-Downloads 5-Foren
internetinformationsdienste (IIS)-Mar	ager	×
Datei Ansicht ?	Mit Server verbinden	? ×
Verbindungen	Anmeldeinformationen angeben	
Statistice WS-wAC (WS\stephan-T1)	Die Verbindung mit "ws-ca1.ws.its" wird hergestellt. Benutzername:	nlineressourcen 5-News und -Informationen 5-Dewnloads
	ws\stephan-t1 ~ Kennwort:	>Forn schNet

Das virtuelle Verzeichnis hänge ich direkt in die Root des IIS:



Der Name "crl" ist bereits veröffentlicht, daher muss ich den beibehalten. Der Eintrag zeigt auf das zuvor erstellte Verzeichnis mit den CRL-Dateien:

📬 Internetinformationsdienste (IIS)-Manager		- 🗆 X
← → ♥ ws-ca1.ws.its ►		😰 🔤 🏠 😰 -
Datei Ansicht ?		
Date: Ansicht ? Verbindungen Verbindungen Vstartseite Vstartseitee	Ws-ca1.ws.its Startseite Filter: Virtuelles Verzeichnis hinzufügen ? × ASP.NET Sitename: Default Web Site Pfad: / .NET-Autorisien Anwendungsein Beispiel: Bilder Bysischer Pfad:	Aktionen Server verwalten Neu starten Estarten Anwendungspools anzeigen Sites anzeigen
	Ablaufverfolgun für Anforder Pass-Through-Authentifizierung Ablaufverfolgun für Anforder Verbinden als Ehelreseiten OK Abbrechen Abbrechen nd ISAPI-Filter	



Nach einem Klick auf OK ist alles erledigt. Aber ich kontrolliere immer gerne mit pkiview.msc, ob alle Einstellungen auch aus der Perspektive des Clients erreichbar sind. Daher starte ich das Tool auf meinem Admin Server:

	.	D	٥					Filter 🗸		
ش ^н	löchst	e Überei	instimmung							
and the second	i,	pkiviev Microso	w.msc oft Common Cons	ole-Dokument						
Č3										
	Aktive A	Anwendu	ingen							
	Q	Bł	ê 📄	I	1					

Und der Blick wird mit einem Fehler belohnt. Das ist wohl die Deltasperrliste nicht erreichbar:

🏥 pkiview - [Unternehmens-P	PKI\WS-ITS-Zertifizierungsstelle-CA1 (V1.1)]					-		×
Datei Aktion Ansicht ?								
🗢 🔿 🖄 🙆 👔								
Unternehmens-PKI	Name	Status	Ablaufdatum	Ort		Aktionen		
WS-ITS-Zertifizierungs:	Zertifizierungsstellenzertifikat	ОК	15.10.2021 18:15			WS-ITS-Zertifi	ierungs	🔺
	AIA-Speicherort #1	ОК	15.10.2021 18:15	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1,CN=AIA,CN	=Pu	Weitere A	dionen	•
	AIA-Speicherort #2	ОК	15.10.2021 18:15	http://ws-ca1.ws.its/CertEnroll/WS-CA1.ws.its_WS-ITS-Zer	rtifizi		concin	
	E Speicherort für Sperrlisten-Verteilungspunkte #1	OK	10.01.2020 04:14	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-C	CA1,			
	DeltaCRL-Speicherort #1	ОК	04.01.2020 04:14	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-C	CA1,			
	DeltaCRL-Speicherort #2	Download nicht möglich.		http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1)+.	<mark>.crl</mark>			
	Speicherort f ür Sperrlisten-Verteilungspunkte #2	OK	10.01.2020 04:14	http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1).cr	rl h			
< >								
	L							

Die Ursache ist klar, wenn man schon einmal mit PKI zu tun hatte: Die Deltasperrliste wird mit einem Pluszeichen im Namen gekennzeichnet. Dieses Zeichen hat aber in einer URL eine andere Bedeutung. Daher reagiert der IIS nicht auf die Anfrage. Das Verhalten lässt sich mit einer IIS-Option anpassen. Diese kann im Konfigurationseditor vorgenommen werden:



🖏 Internetinformationsdienste (IIS)-Manager		- 🗆 X
Image: State in the state i		🖸 🐼 🟠 🔞 🗸
Datei Ansicht ?		
Verbindungen		Aktionen Grundeinstellungen
Filter: Image: Start in the start in	eiten	 Gundeandebungen Virtuelles Verzeichnis durchsuchen *80 (http) durchsuchen *40 (http) durchsuchen *413 (https) durchsuchen Virtuelles Verzeichnis bearbeiten Erweitette Einstellungen Hilfe
Konfigurations-Edi	v	

Der anzupassende Wert ist das DoubleEscaping im RequestFiltering:



Dieses muss aktiviert werden:

 → ws-cal.ws.its → Sites → Defa 	ult Web Site 🖡 crid 🖡			
Datei Ansicht ?				
erbindungen • 🔜 🖄 😓	Konfigurations-Editor	Filtering		Aktionen
■ WS-WAC (WS\stephan-T1) ■ ws-ca1.ws.its (ws\stephan-t1)	✓ Unterste Pfadebene: MACHINE/WEBRO	Skript generieren		
Anwardungspools Gistes Gefault Web Site ADPolicyProvider_CEP_Kerberos	allowDoubleEscaping allowHighBitCharacters	True True	~	Konfiguration Konfiguration suchen
	alwaysAllowedQueryStrings alwaysAllowedUrls	(Count=0) (Count=0)		Abschnitt
> - aspnet_client > - 💭 CertEnroll	denyQueryStringSequences denyUrlSequences	(Count=0) (Count=0)		'allowDoubleEscaping'-Attri
> - [] CertSrv > - [] WS-ITS-Zertifizierungsstelle-CA1_Cl	> fileExtensions filteringRules	(Count=0)		Attribut sperren
2 <u>2</u> 00	hiddenSegments removeServerHeader request limits	False		Hilfe
	unescapeQueryString	True		
	allowDoubleEscaping Datentyp:bool			



Nach einem IIS-Reset ist die Datei dann im pkiview erreichbar und alles ist grün:

pkiview - [Unternehmens-F Datei Aktion Ansicht ?	PKI\WS-ITS-Zertifizierungsstelle-CA1 (V1.1)]				- 🗆 X
🗢 🔿 🖄 🔯					
🝰 Unternehmens-PKI	Name	Status	Ablaufdatum	Ort	Aktionen
WS-ITS-Zertifizierungs:	Zertifizierungsstellenzertifikat	Verifizierung			WS-ITS-Zertifizierungs 🔺
	AIA-Speicherort #1	ОК	15.10.2021 18:15	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1,CN=AIA,CN=Pu	Weitere Aktionen
	AIA-Speicherort #2	OK	15.10.2021 18:15	http://ws-ca1.ws.its/CertEnroll/WS-CA1.ws.its_WS-ITS-Zertifizi	
	E Speicherort für Sperrlisten-Verteilungspunkte #1	ОК	10.01.2020 04:14	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-CA1,	
	E DeltaCRL-Speicherort #1	OK	04.01.2020 04:14	Idap:///CN=WS-ITS-Zertifizierungsstelle-CA1(1),CN=WS-CA1,	
	E DeltaCRL-Speicherort #2	ОК	04.01.2020 04:14	http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1)+.crl	
	E Speicherort für Sperrlisten-Verteilungspunkte #2	ОК	10.01.2020 04:14	http://crl.ws.its/crld/WS-ITS-Zertifizierungsstelle-CA1(1).crl	

Der Admin Server kann die Datei und den dazugehörigen Server direkt ansprechen. Meine Clients stehen aber in anderen Subnets. Für den Zugriff muss der Zertifizierungsserver über TCP Port 80 (http) erreichbar sein. Dazu habe ich in meiner Firewall entsprechende Regeln definiert. Die aktuelle Regel verweist noch auf den alten WS-RA1:

	SC System	n v Inter	faces 🔻 Firew	all -	Services -	VPN - Status -	Diagn	ostics -	- Help	•	¢
Firewa	all / Rules	/ LAN_1	10_CLIENTS	;							± Ш ■ 0
Floating	DMZ_120_	EXTERN	LAN_100_SERVER	R [DMZ_130_INTERN	LAN_110_CLIENT	s dm	IZ_140_(GAMEZONE	DMZ_150_ISOL	ATION
Rules (Drag to Char	ige Order)									
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	0 /478 KiB	IPv4 ICMP any	*	*	*	*	*	none		TEST	≟ℐ⊡⊘ ฃ
Ausnahme	en intern										Ê
	0 /0 B	IPv4 TCP	*	*	ServerIn_RDS	Ports_RDS	*	none		Zugriff auf RDS	≟ℐ⊡⊘ ฃ
	3 /146.79 MiB	IPv4 TCP	*	*	ServerIn_AD	Ports_AD_TCP	*	none		Services AD	≟ℐ⊡⊘ Ճ
	6 /50.95 MiB	IPv4 UDP	*	*	ServerIn_AD	Ports_AD_UDP Alias details	*	none		Services AD	≟ℐ⊡⊘ Ճ
	0 /3 KiB	IPv4 TCP	*	*	ServerIn_HTTP	Value Desc 192.168.100.7 WS-I	cription RA1 (CRL)	ione		Services HTTP	≟ℐ⊡⊘ ฃ
Π 🥑	15 /337 60	IPv/I TCP	*	*	Serverin HTTPS	Porte HTTPS	*	none		Services HTTPS	. ₽ .▲□0

Hinter der Regel steht ein Alias. In diesem gebe ich nun die IP-Adresse meines WS-CA1 an:

Sense System	- Interfaces - Firewall -	Services - VPN -	Status 🔻	Diagnostics -	Help 🗕	€
Firewall / Aliases	/ Edit					Θ
Properties						
Name	ServerIn_HTTP The name of the alias may only con	sist of the characters "a-z, A-z	Z, 0-9 and _".			
Description	Services mit HTTP A description may be entered here f	for administrative reference (n	not parsed).			
Туре	Host(s)		~			
Host(s)						
Hint	Enter as many hosts as desired. Ho re-resolved and updated. If multiple as 192.168.1.16/28 may also be en	sts must be specified by their IPs are returned by a DNS qu tered and a list of individual IF	IP address or fu ery, all are used. P addresses will	Illy qualified domain An IP range such as be generated.	name (FQDN). FQE 192.168.1.1-192.1	0N hostnames are periodically 68.1.10 or a small subnet such
IP or FQDN	192.168.100.6		VS-CA1 (CRL)			
	🖺 Save 🕂 Add Host					

Nun wird es Zeit für einen Test von einem Client aus. Dazu nutze ich mein Notebook. Hier sind einige interne Zertifikate vorhanden. Ich exportiere eines davon in eine cer-Datei:

WS IT-Solutions



Mit certutil kann ich nun einen Sperrlisten-Test vornehmen:

<pre>\> certutil -url E:\test</pre>	.cer			
URL-Abrufprogramm			×	
Status Typ	URL	Abrufzeit Fingerabd	Iruck	
Zeitlimit (Sek.)	Hinweis: Heruntergeladene Sperfisten und	Abrufen		
Zeitiimi (Jert.)	Zertifikate werden nur bis zu einem gewisser Maß überprüft. Die Sperrliste bzw. das	n C Zertifikate (vom Al.	A)	
🗌 LDAP-Verkehr signieren	Zertifikat ist möglicherweise nicht ordnungsgemäß signiert oder verfügt nicht	Spentisten (vom Cl	OP)	
Zettilletesteretel	über entsprechende Erweiterungen für eine ordnungsgemäße Überprüfung.	C OCSP (von AIA)		
Walther, Stephan	Auswählen Beenden	Abrufen		
		-		

Das Tool prüft, ob die Sperrlistendaten von den Servern geladen werden können:



> Windows PowerShell		-	\times
PS E:\> PS E:\> certutil -url E:\tes	t.cen		Ŷ
URL-Abrufprogramm Status Typ Deprüft Basissperils. Öbeprüft Detasperils. Öbeprüft Detasperils. Öbeprüft Detasperils. Öbeprüft Detasperils.	URL Abrufzeit Fingerabdruck [0.0] Idap:///CN=WS-ITS-Zertifizierum 0 560cb4d6f9 [0.0.1] http://cl.ws.its/crid/WS-ITS-Zer 975fe-3a662 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 975fe-3a662 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 560cb4d6f9 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 975fe-3a662 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 0 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 0 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 0 975fe-3a662 0 [1.0] http://cl.ws.its/crid/WS-ITS-Zer 0 975fe-3a662 0		
Zettlinit (Sek.) 15 LDAP-Verkehr signieren Zertifikatantragstel Waither, Stephan URL für Download	Hinweis: Heruntergeladene Spenisten und Zertifikat werden nur bis zu einem gewissen Maß Überprüft. Die Speniste bzw. das Zertifikat im die Gicherweise nicht ordnungsgemäß signeit oder verfügt nicht über entsprechende Erweitenungen für eine ordnungsgemäße Überprüfung. Abrufen Auswählen Beenden C Zertifikat (vom AIA) Auswählen Beenden OCSP (von AIA)		

Das sieht gut aus. Damit sollte diese Migration abgeschlossen sein.