

Inhalt

1.	Szenario.....	1
2.	Auf dem alten Server.....	1
	Kontrolle der alten CA.....	1
	Aufsetzen des neuen Servers	2
	Sicherung des alten CA-Servers	2
	Entfernen des alten CA-Servers	5
3.	Auf dem neuen Server	8
	Aufbau des neuen Servers.....	8
	Installation der neuen CA	11
	Import der alten DB und der Konfiguration.....	16
	Absicherung der Web-Registrierungsstelle.....	18
	Anpassungen für SHA256.....	27
4.	Bereinigung	28

1. Szenario

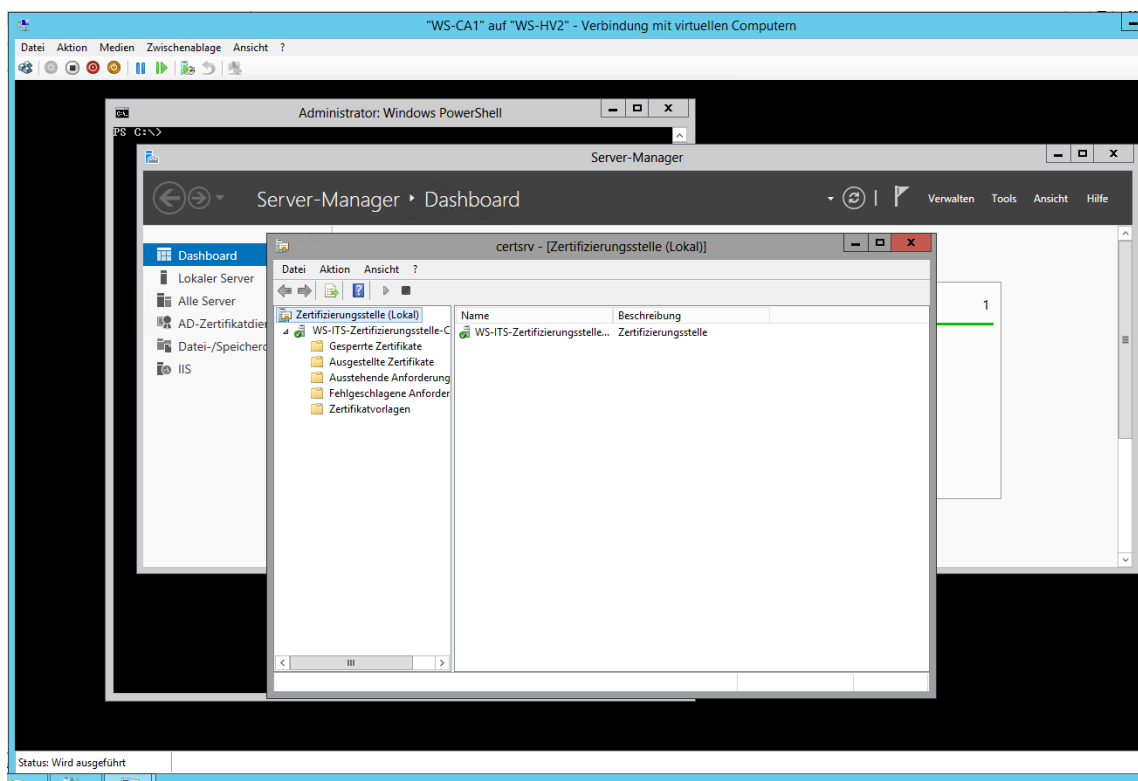
Aktuell wird in einer Windows Server 2012 R2 Gesamtstruktur eine Active Directory Zertifizierungsstelle auf dem DomainMember WS-CA1 AD-integriert betrieben. Der Server WS-CA1 läuft auf einem Windows Server 2012 als Server Core mit Mini-Shell-Oberfläche.

Im Rahmen der Migration aller Server soll die CA auf einen neuen Windows Server 2016 übertragen werden.

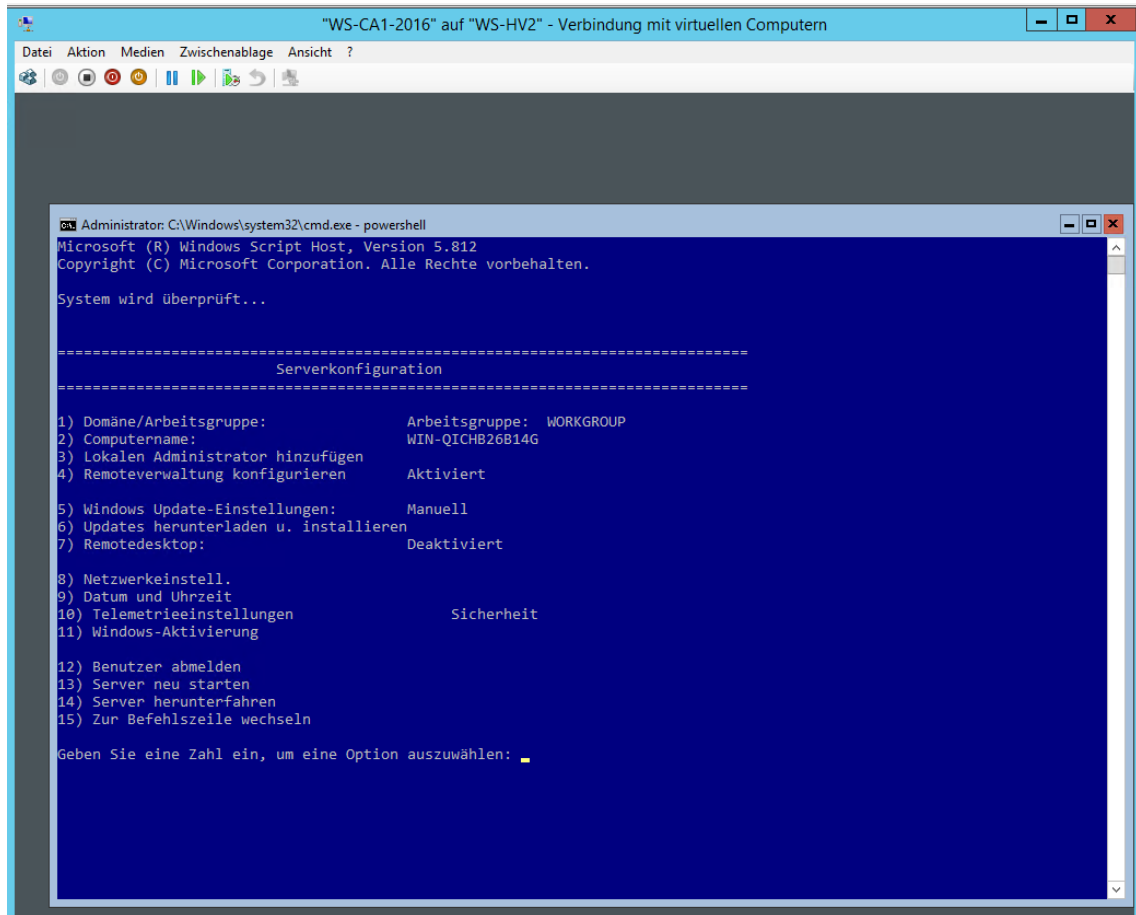
Als Migrationsverfahren wird ein klassisches Wipe & Load verwendet: der neue Server wird nach dem Umzug die CA unter der gleichen Identität (Name im AD, SID, IP, ...) fortführen.

2. Auf dem alten Server

Kontrolle der alten CA

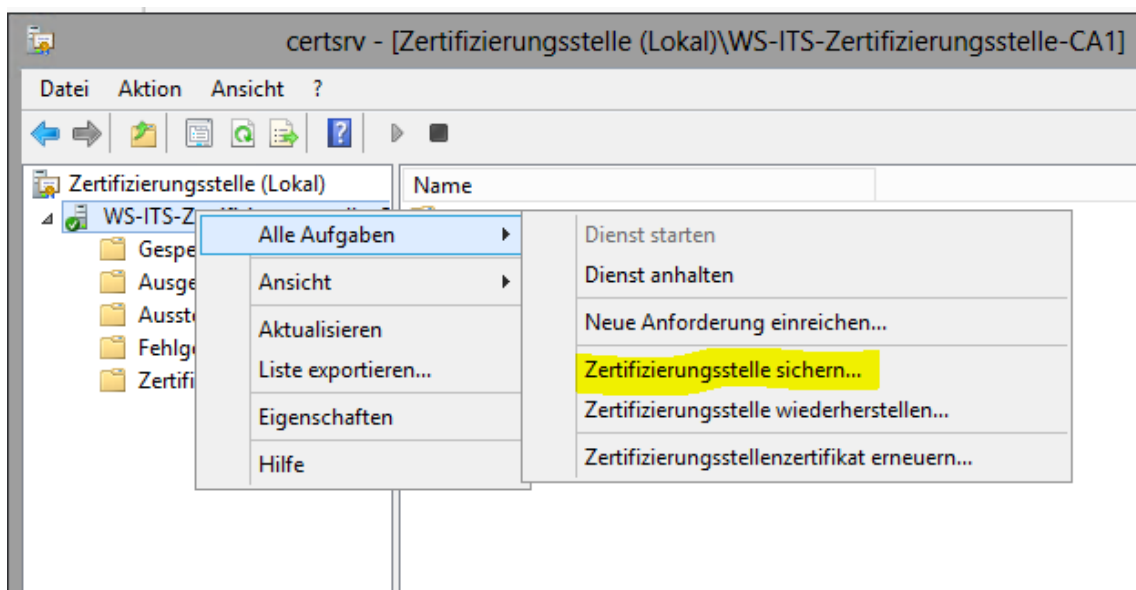


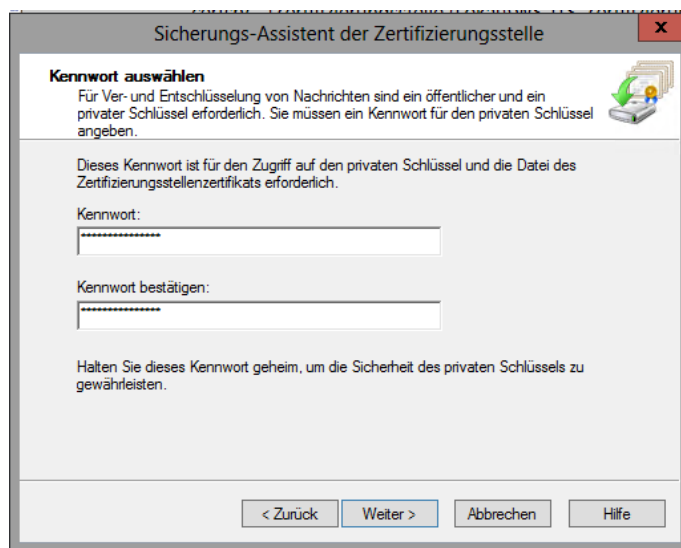
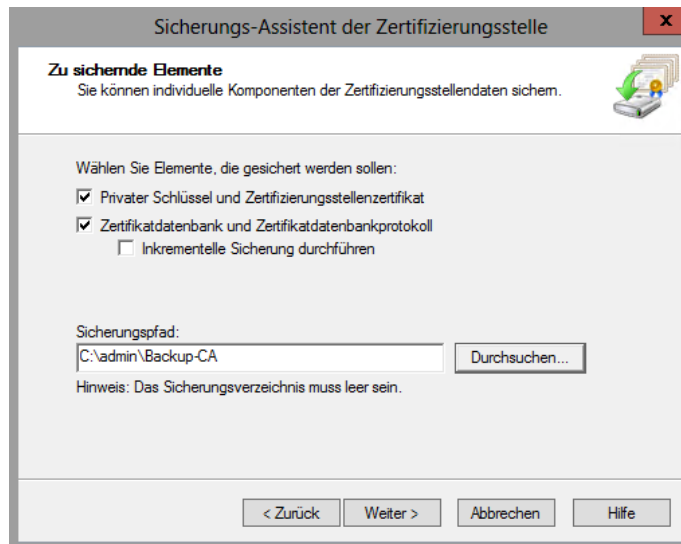
Aufsetzen des neuen Servers



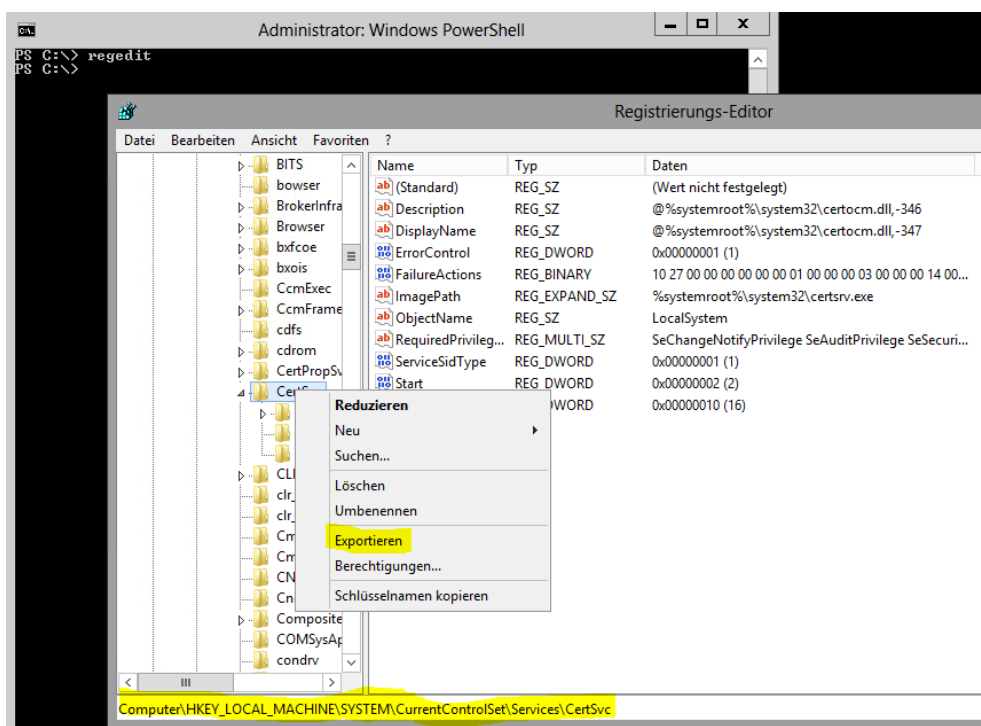
Sicherung des alten CA-Servers

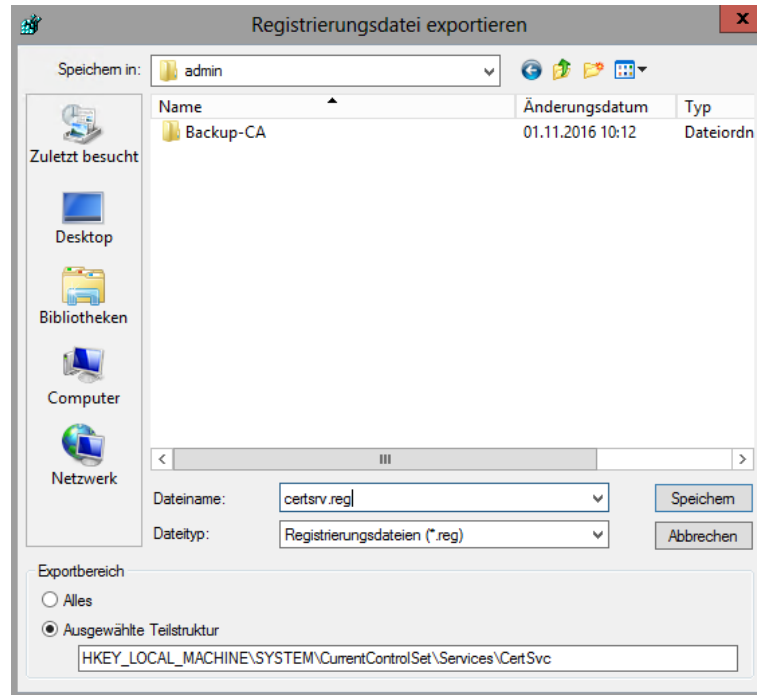
Auf dem alten Server stehen dank Mini-Shell die Servertools lokal zur Verfügung. Zuerst wird die CA mit den Zertifikaten lokal gesichert:



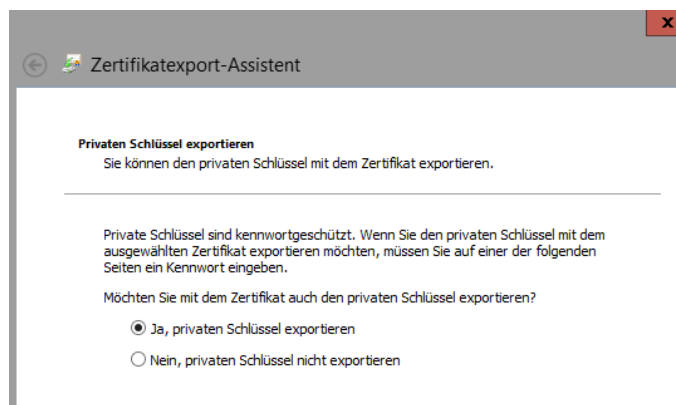
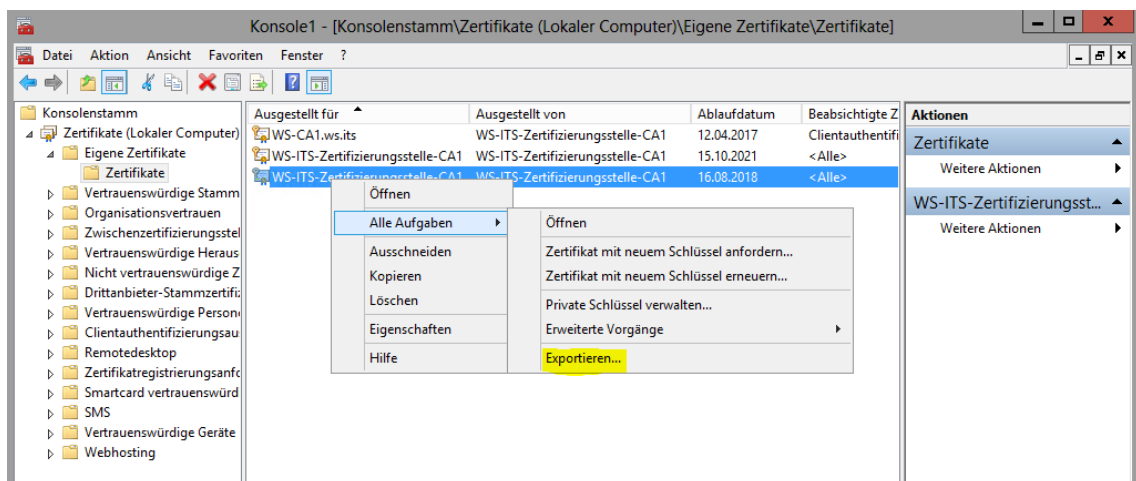


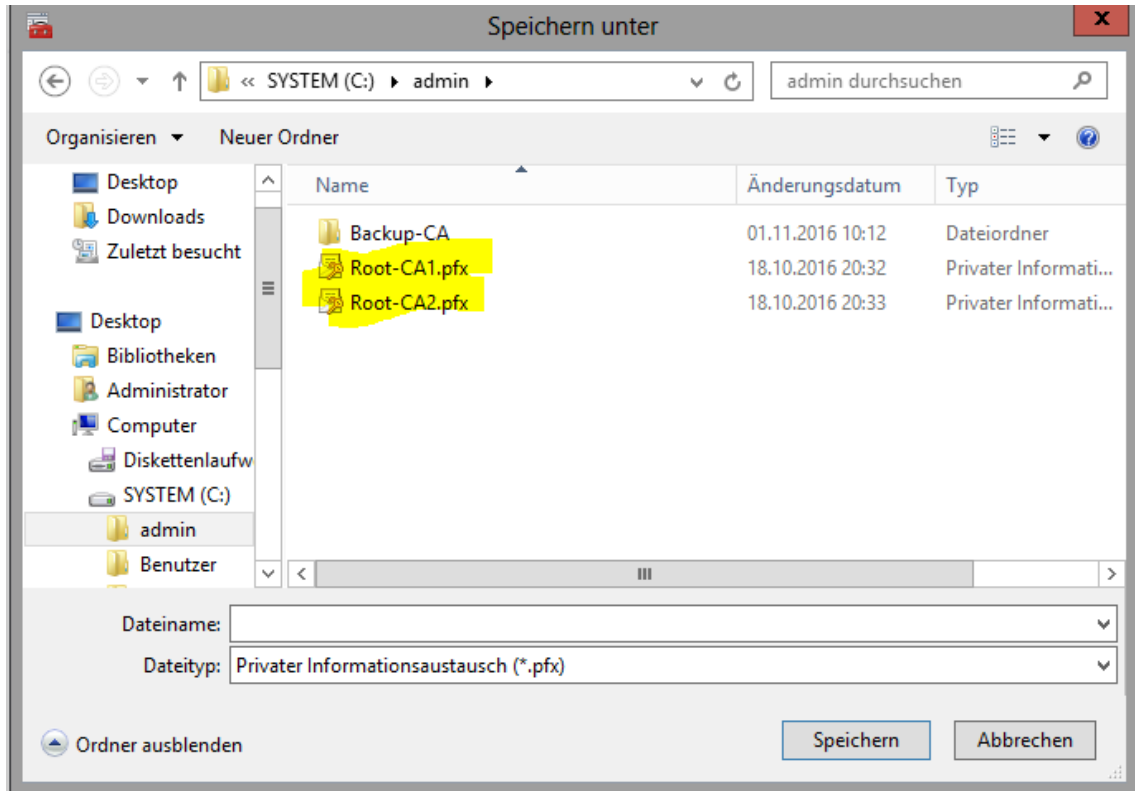
Zusätzlich muss die Konfiguration des CA-Services aus der Registry gesichert werden:



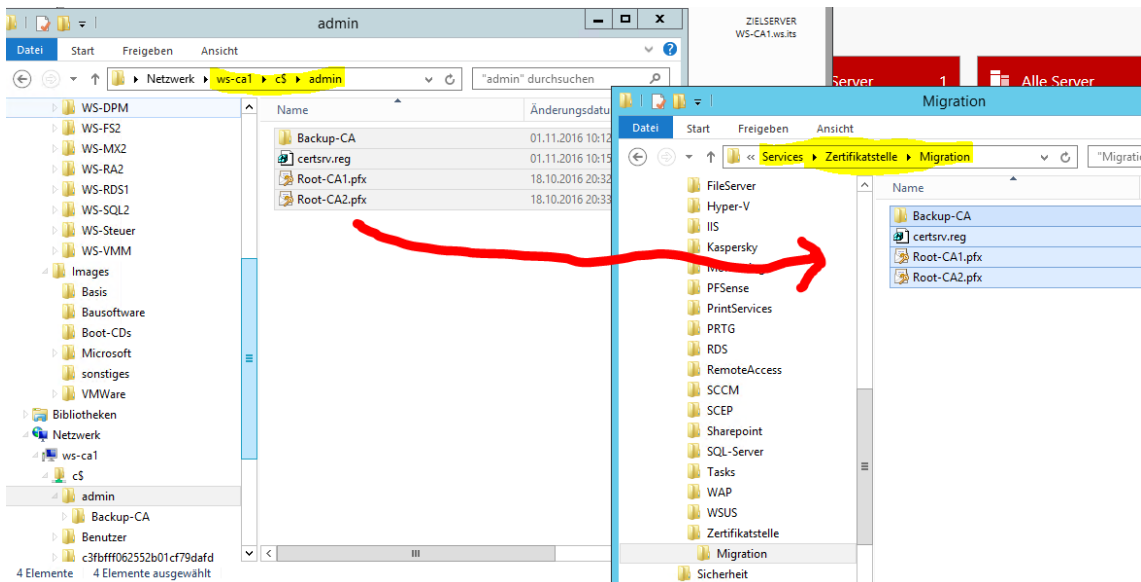


Es existieren 2 Root-CA-Zertifikate. Diese werden ebenfalls als PFX exportiert:



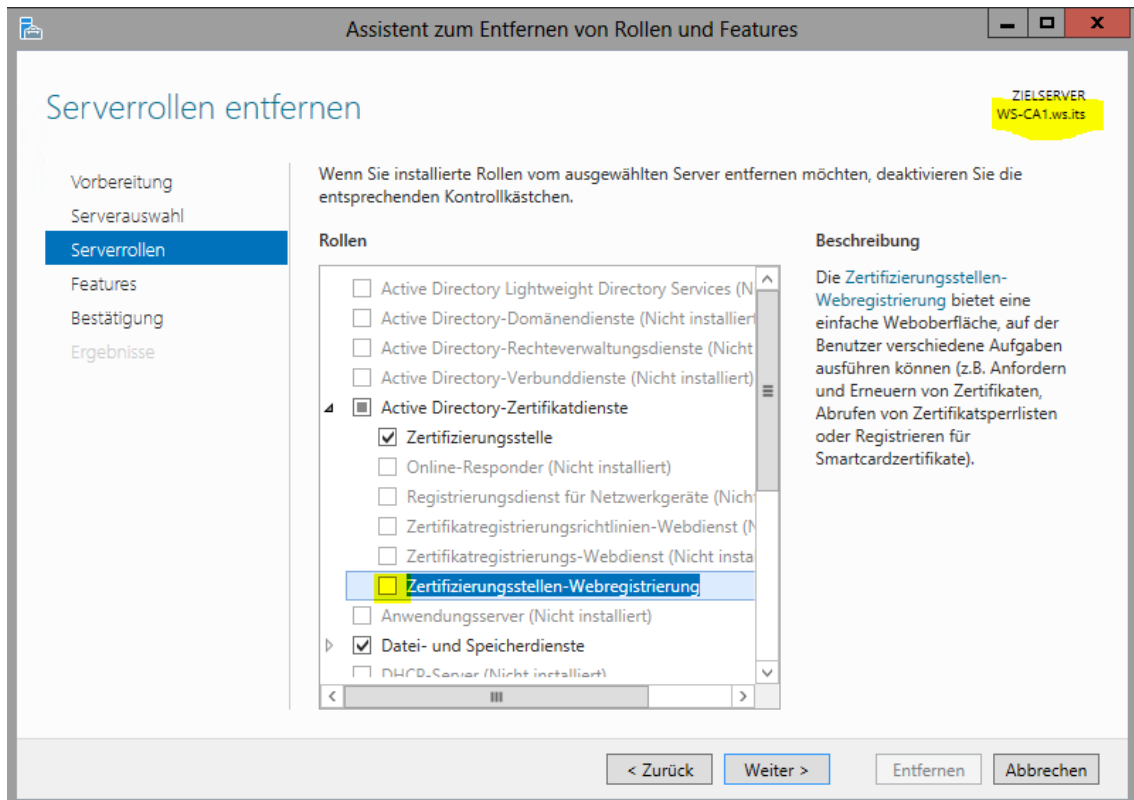


Alle Daten liegen nun auf dem alten Server unter C:\Admin. Da der Server gleich abgeschaltet wird, schiebe ich die Daten auf ein AdminShare:

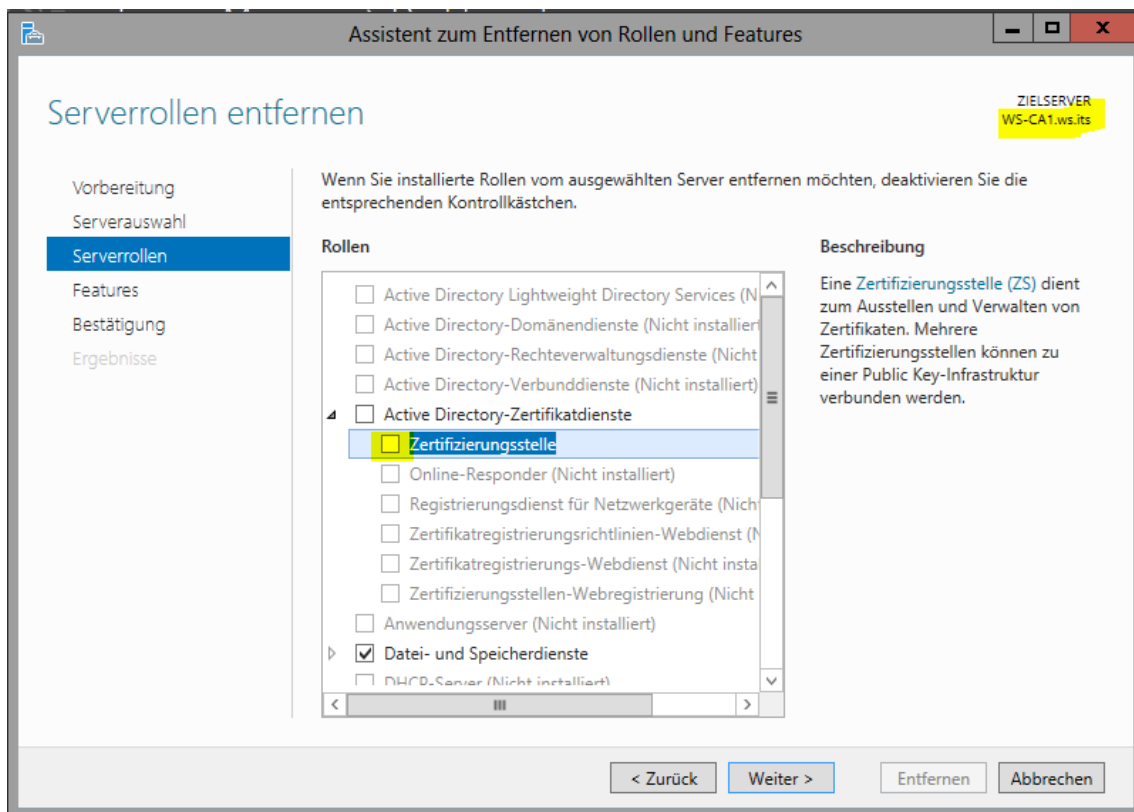


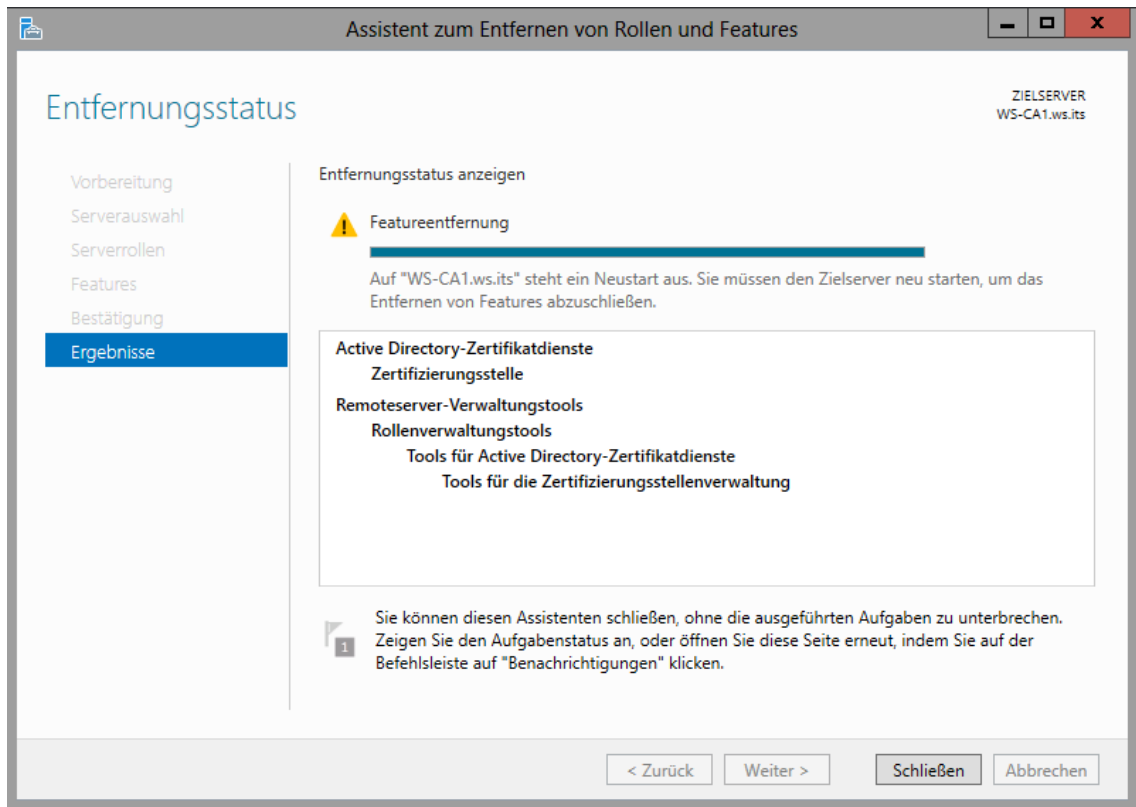
Entfernen des alten CA-Servers

Nachdem alle Daten gesichert wurden kann nun die CA-Rolle entfernt werden. Damit wird im AD die Position für den neuen Server frei. Da hier die Webregistrierung installiert ist muss diese zuerst entfernt werden:

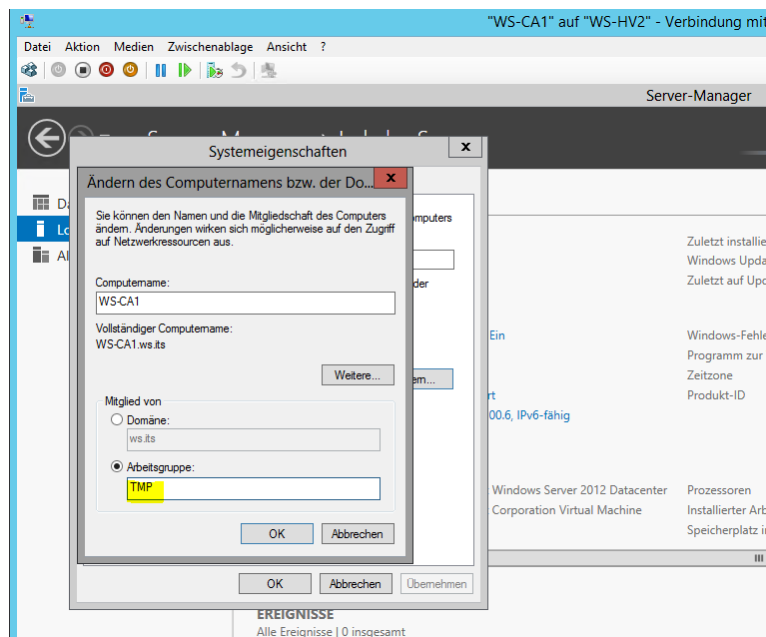


Jetzt kann die CA selbst deinstalliert werden:

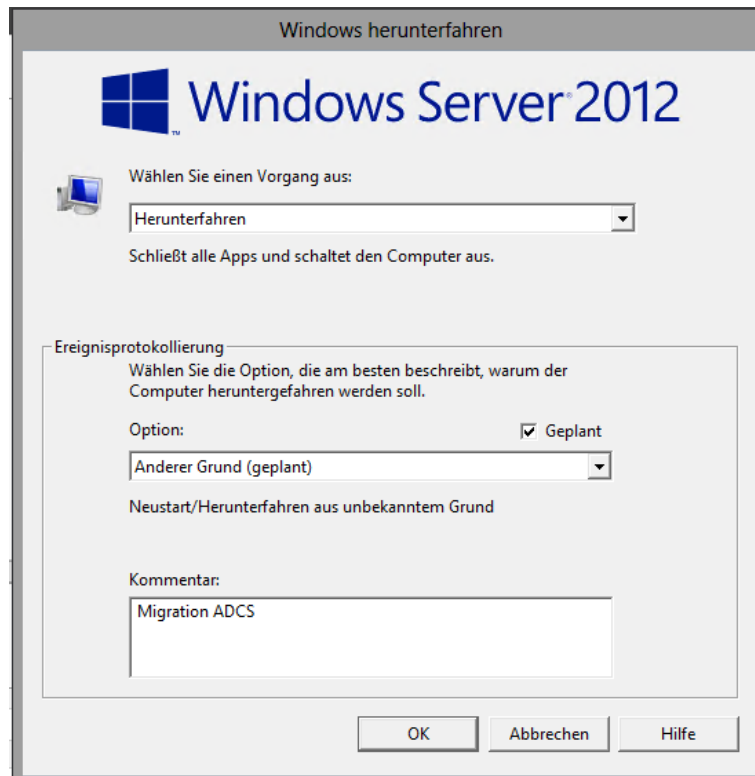




Nach dem Neustart kann der alte Server aus dem AD entfernt werden:



Ein Neustart ist nicht notwendig. Der alte CA-Server kann abgeschaltet werden:



3. Auf dem neuen Server

Aufbau des neuen Servers

Der neue Server ist als Core-Server bereitgestellt worden. Zunächst sind die üblichen Aufgaben (IP-Konfiguration, Server benennen und DomainJoin) erforderlich:

```

Administrator: C:\Windows\system32\cmd.exe - powershell
Microsoft (R) Windows Script Host, Version 5.812
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.

System wird überprüft...

=====
                          Serverkonfiguration
=====

1) Domäne/Arbeitsgruppe:           Arbeitsgruppe: WORKGROUP
2) Computername:                   WIN-QICHB26B14G
3) Lokalen Administrator hinzufügen
4) Remoteverwaltung konfigurieren  Aktiviert

5) Windows Update-Einstellungen:   Manuell
6) Updates herunterladen u. installieren
7) Remotedesktop:                  Deaktiviert

8) Netzwerkeinstell.
9) Datum und Uhrzeit
10) Telemetrieinstellungen         Sicherheit
11) Windows-Aktivierung

12) Benutzer abmelden
13) Server neu starten
14) Server herunterfahren
15) Zur Befehlszeile wechseln

Geben Sie eine Zahl ein, um eine Option auszuwählen: 8_

```



```

-----
Netzwerkkarteneinstellungen
-----

NIC-Index                0
Beschreibung             Microsoft Hyper-V Network Adapter
IP-Adresse               192.168.100.6   fe80::801c:af2e:b694:b87a
Subnetzmaske             255.255.255.0
DHCP aktiviert           Falsch
Standardgateway          192.168.100.252
Bevorzugter DNS-Server   192.168.100.2
Alternativer DNS-Server  192.168.100.1

1) Adresse der Netzwerkkarte festlegen
2) DNS-Server festlegen
3) DNS-Servereinstellungen löschen
4) Zurück zum Hauptmenü
  
```

```

=====
Serverkonfiguration
=====

1) Domäne/Arbeitsgruppe:           Arbeitsgruppe: WORKGROUP
2) Computernamen:                 WIN-QICHB26B14G
3) Lokalen Administrator hinzufügen
4) Remoteverwaltung konfigurieren   Aktiviert

5) Windows Update-Einstellungen:   Manuell
6) Updates herunterladen u. installieren
7) Remotedesktop:                 Deaktiviert

8) Netzwerkeinstell.
9) Datum und Uhrzeit
10) Telemetrieinstellungen
11) Windows-Aktivierung

12) Benutzer abmelden
13) Server neu starten
14) Server herunterfahren
15) Zur Befehlszeile wechseln

Geben Sie eine Zahl ein, um eine Option auszuwählen: 2

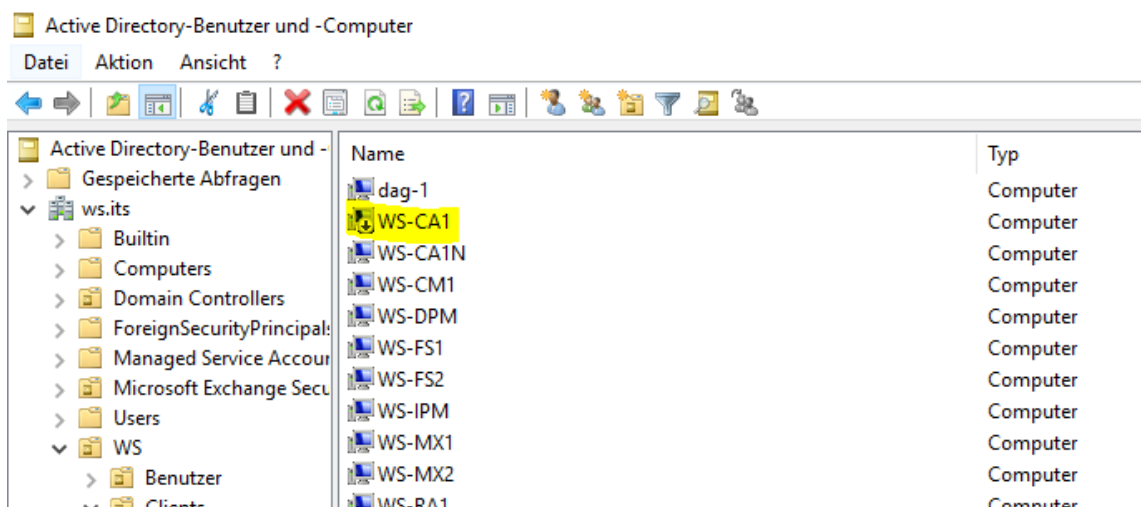
Computernamen

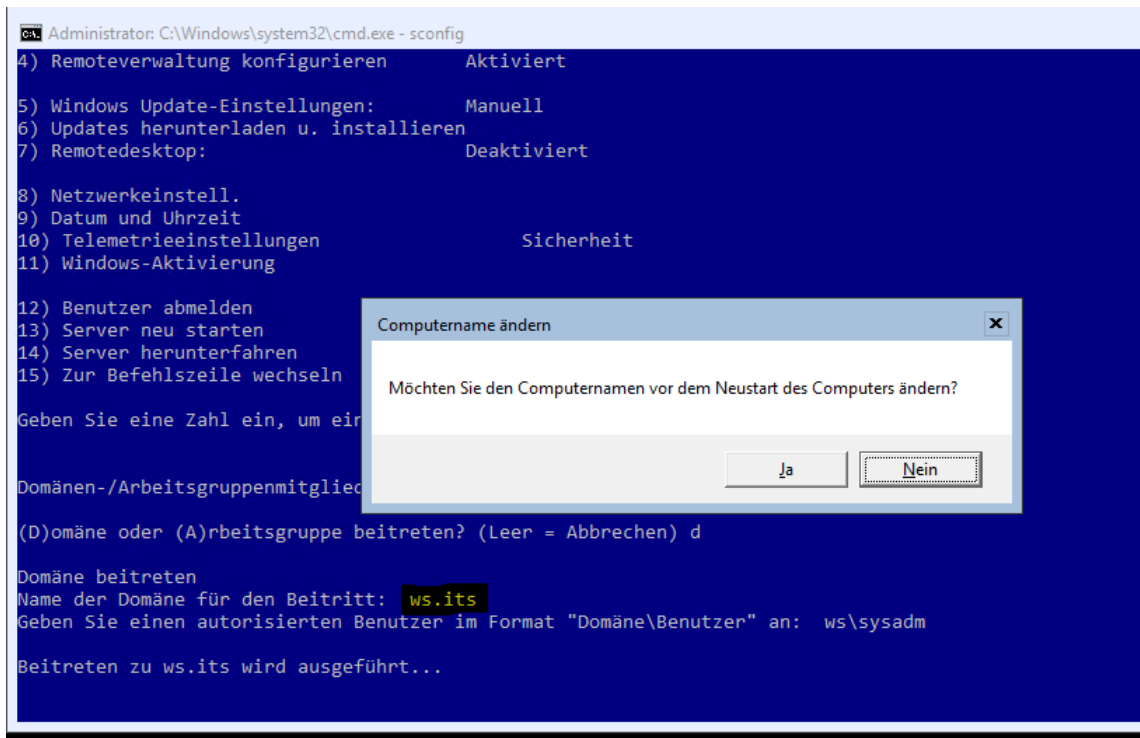
Geben Sie den neuen Computernamen ein (Leer = Abbrechen): WS-CA1
Der Computernamen wird geändert...
  
```

Neu starten

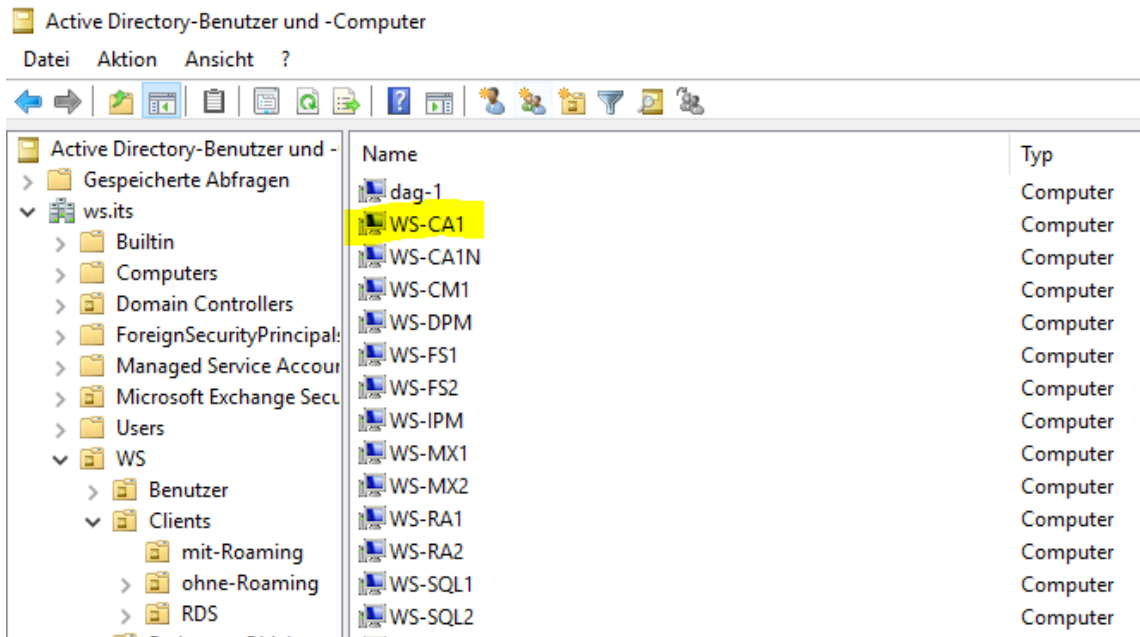
Der Computer muss neu gestartet werden, damit die Änderungen übernommen werden.
Jetzt neu starten?

Das AD-Konto des alten Servers ist jetzt wieder frei:

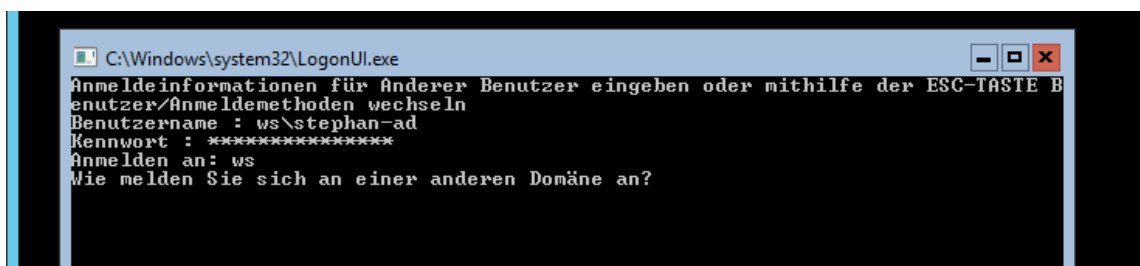




Nach dem DomainJoin ist das Konto wieder belegt:

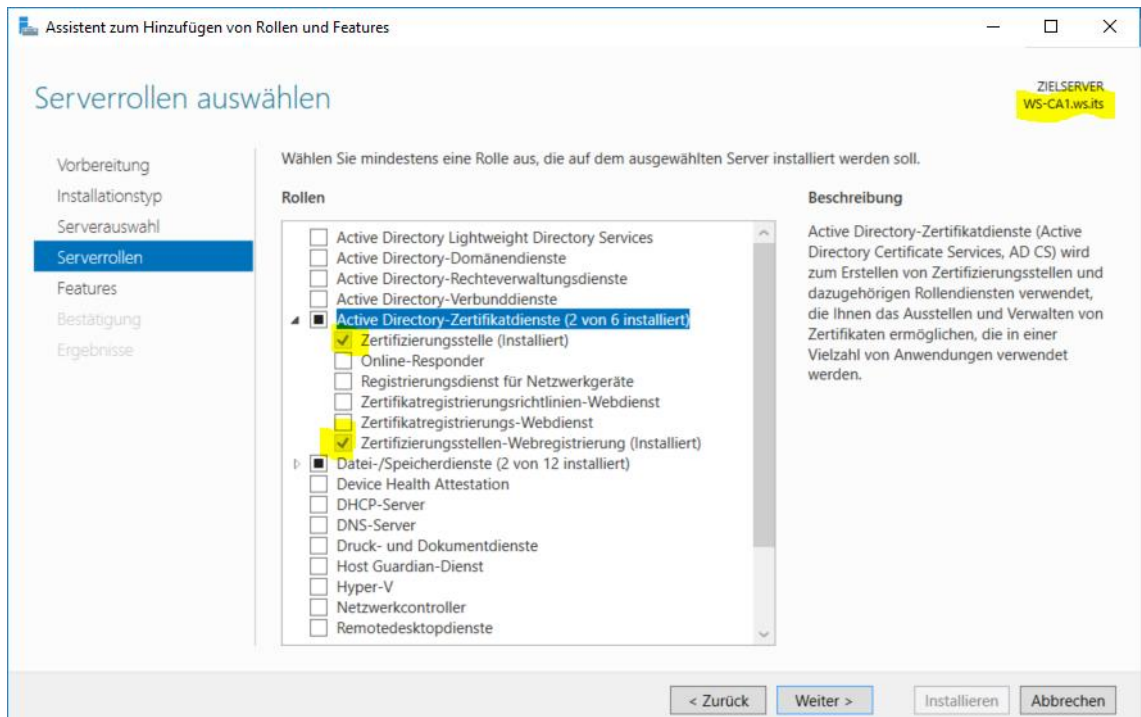


Der Anmelde-Account benötigt ausreichend Rechte:



Installation der neuen CA

Jetzt kann die CA-Rolle installiert werden. Da der Server keine Management-Tools mehr hat kann entweder ein ServerManager eines kompatiblen Systems verwendet werden...



... oder man verwendet lokal die PowerShell:

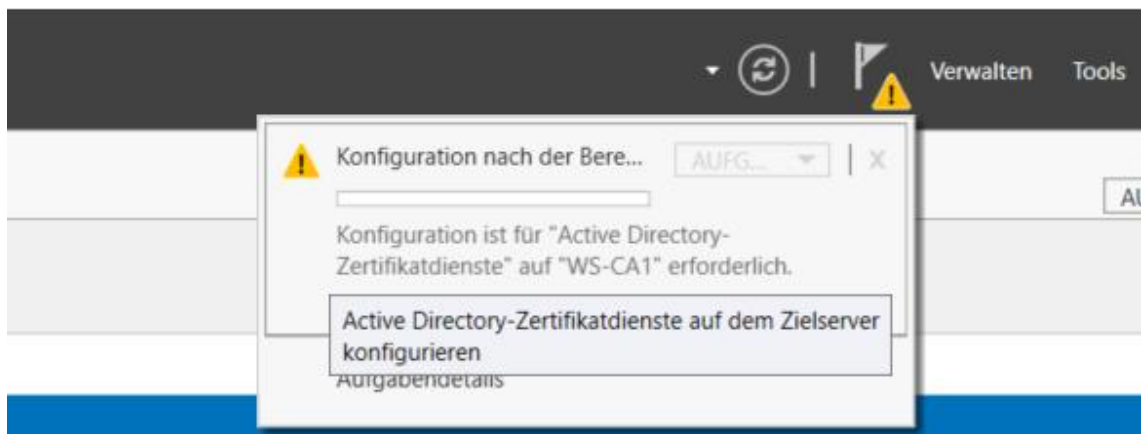
```

c:\> Administrator: C:\Windows\system32\cmd.exe - powershell

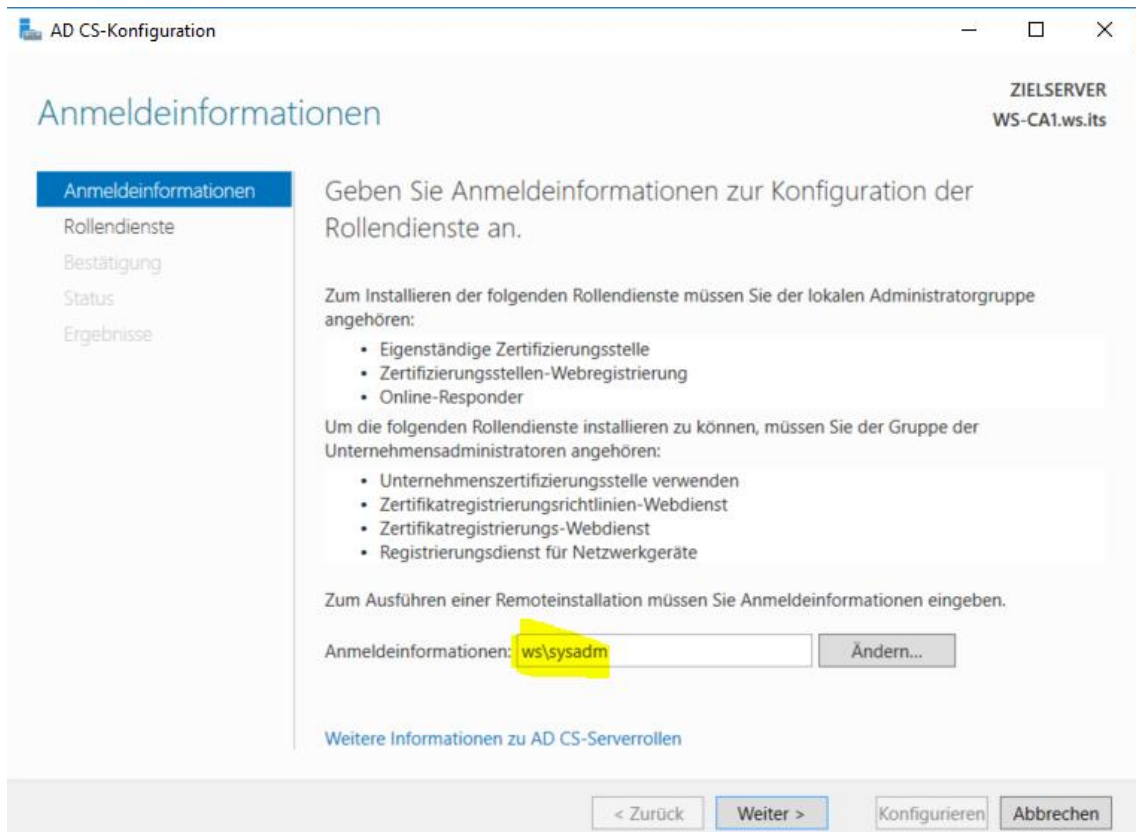
PS C:\> Add-WindowsFeature -Name ADCS-Cert-Authority,ADCS-Web-Enrollment -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
-----
True     No           Success      {Active Directory-Zertifikatdienste, Zerti...
  
```

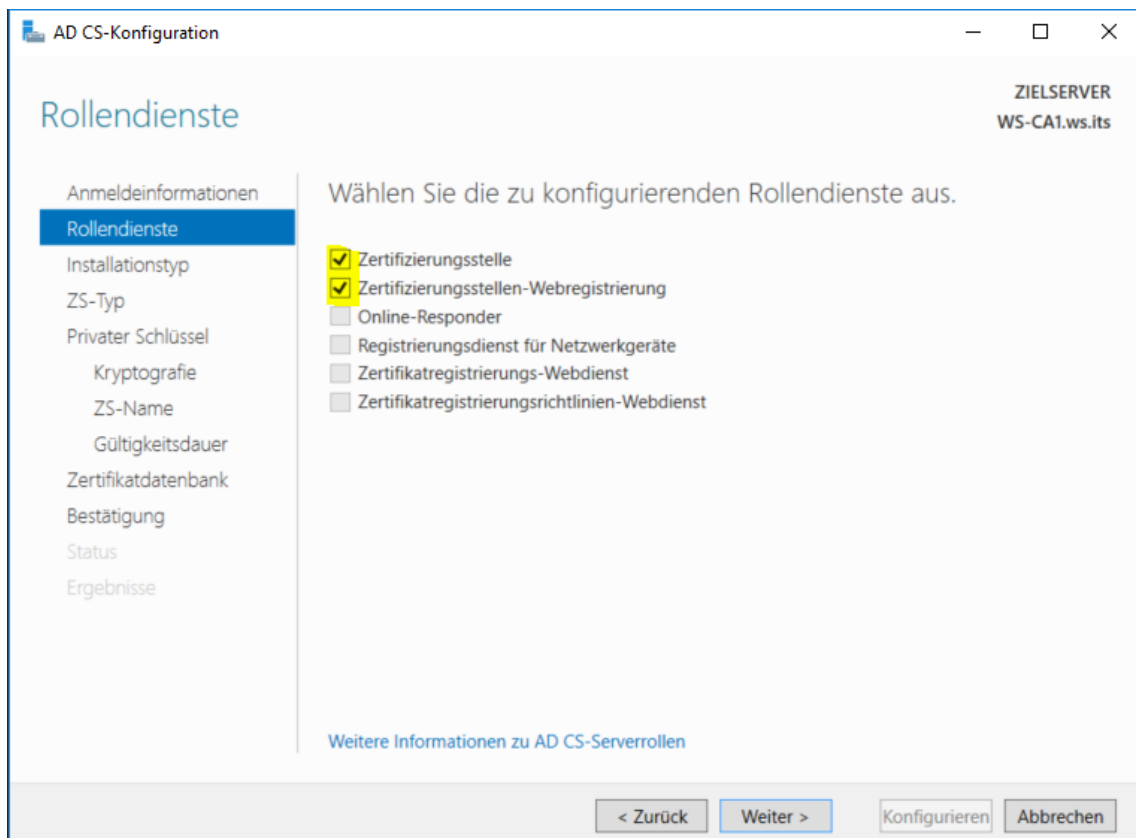
Mit dem Remote-Servermanager kann die Erstkonfiguration vorgenommen werden. Dabei wird eine neue CA mit dem alten Root-CA-Zertifikat aufgebaut:



Es werden AD-Rechte benötigt:



Es werden die beiden installierten Rollen vorbereitet:



AD CS-Konfiguration

ZIELSERVER
WS-CA1.ws.its

Setuptyp

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie den Installationstyp der Zertifizierungsstelle an.

Unternehmenszertifizierungsstellen können mithilfe von Active Directory-Domänendienste (Active Directory Domain Services, AD DS) die Verwaltung von Zertifikaten vereinfachen. Eigenständige Zertifizierungsstellen verwenden nicht AD DS, um Zertifikate auszustellen oder zu verwalten.

- Unternehmenszertifizierungsstelle**
Unternehmenszertifizierungsstellen müssen Domänenmitglieder sein. Sie sind normalerweise online, um Zertifikate oder Zertifikatrichtlinien auszustellen.
- Eigenständige Zertifizierungsstelle**
Eigenständige Zertifizierungsstellen können einer Arbeitsgruppe oder Domäne angehören. Eigenständige Zertifizierungsstellen erfordern kein AD DS und können ohne Netzwerkverbindung verwendet werden (offline).

[Weitere Informationen zum Setuptyp](#)

< Zurück Weiter > Konfigurieren Abbrechen

AD CS-Konfiguration

ZIELSERVER
WS-CA1.ws.its

Zertifizierungsstellentyp

Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse

Geben Sie den Typ der Zertifizierungsstelle an.

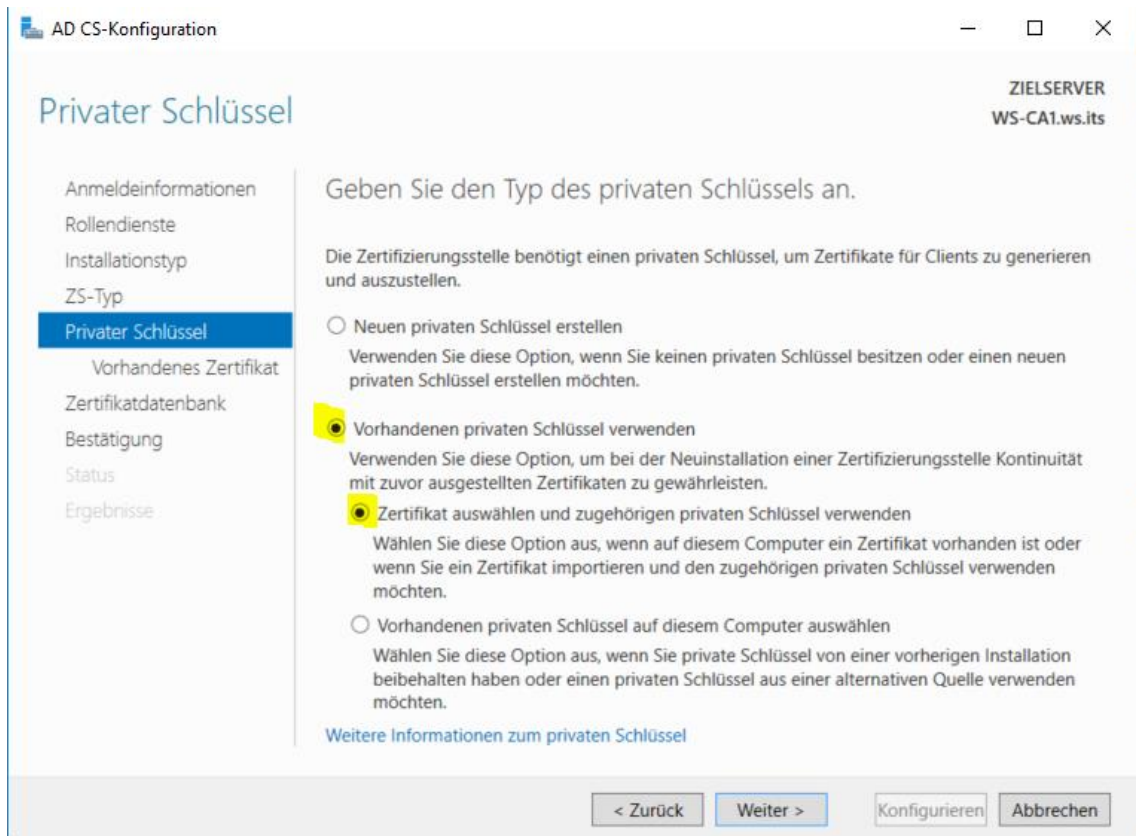
Wenn Sie Active Directory-Zertifikatdienste (Active Directory Certificate Services, AD CS) installieren, erstellen oder erweitern Sie eine Hierarchie der Public Key-Infrastruktur (PKI). Eine Stammzertifizierungsstelle befindet sich am Anfang der PKI-Hierarchie und stellt ein eigenes selbst signiertes Zertifikat aus. Eine untergeordnete Zertifizierungsstelle empfängt ein Zertifikat von der Zertifizierungsstelle, die in der PKI-Hierarchie darüber angesiedelt ist.

- Stammzertifizierungsstelle**
Stammzertifizierungsstellen sind die ersten und möglicherweise einzigen Zertifizierungsstellen, die in einer PKI-Hierarchie konfiguriert werden.
- Untergeordnete Zertifizierungsstelle**
Für untergeordnete Zertifizierungsstellen ist eine eingerichtete PKI-Hierarchie erforderlich. Sie sind zur Ausstellung von Zertifikaten berechtigt, die von der Zertifizierungsstelle stammen, die sich in der Hierarchie über den untergeordneten Zertifizierungsstellen befindet.

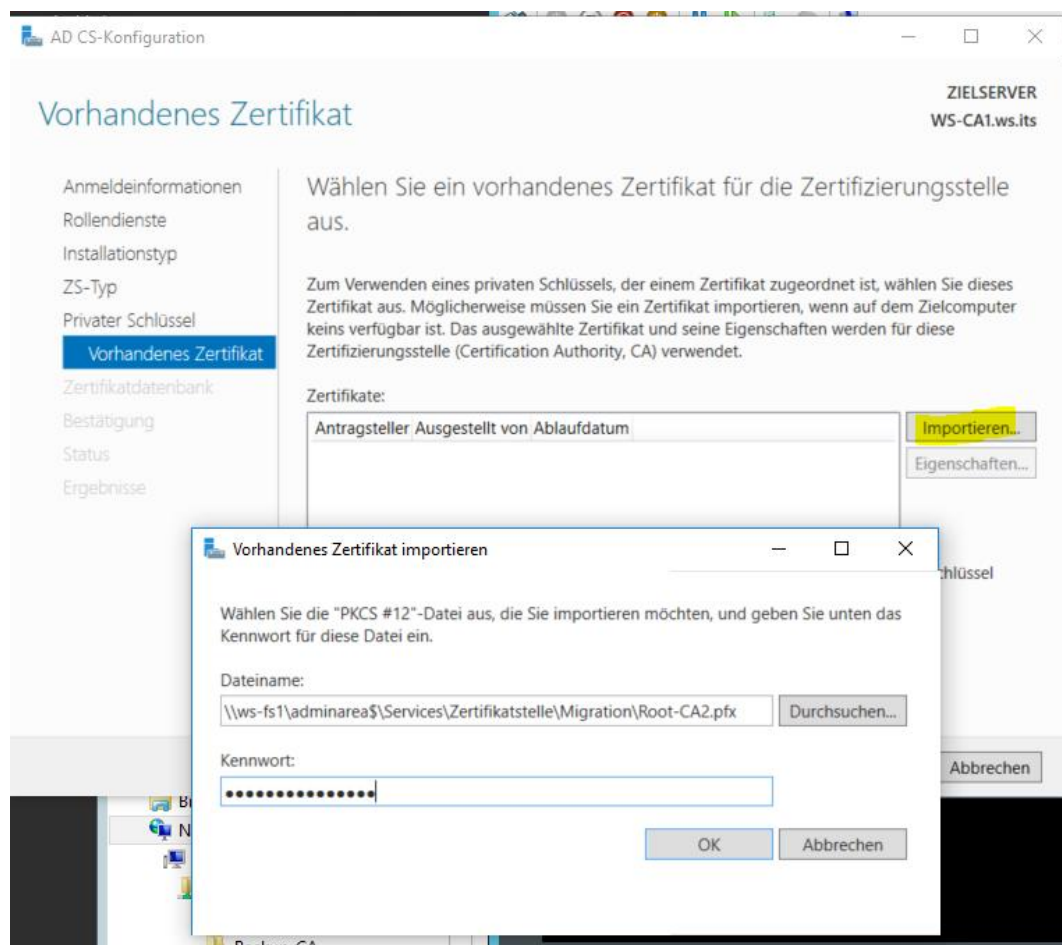
[Weitere Informationen zum Typ der Zertifizierungsstelle](#)

< Zurück Weiter > Konfigurieren Abbrechen

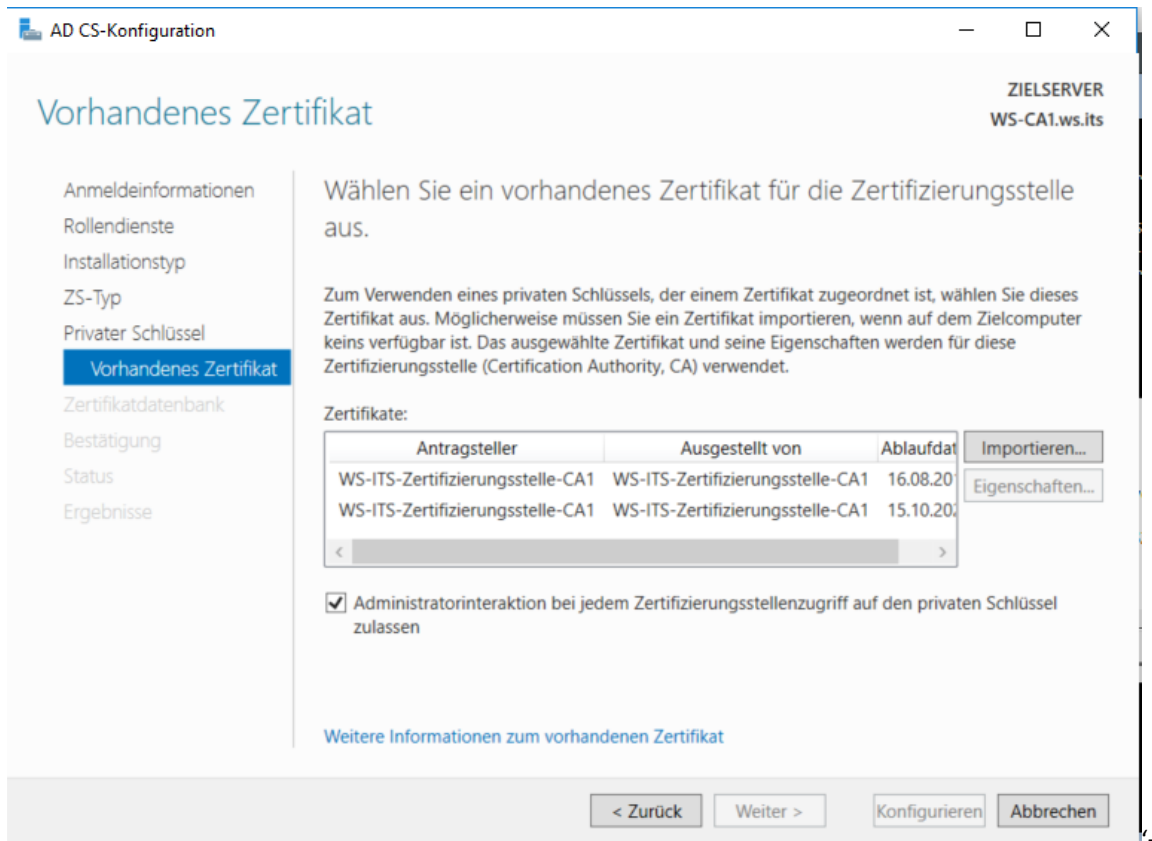
An dieser Stelle kann der Root-CA-Key der alten CA eingespielt werden:



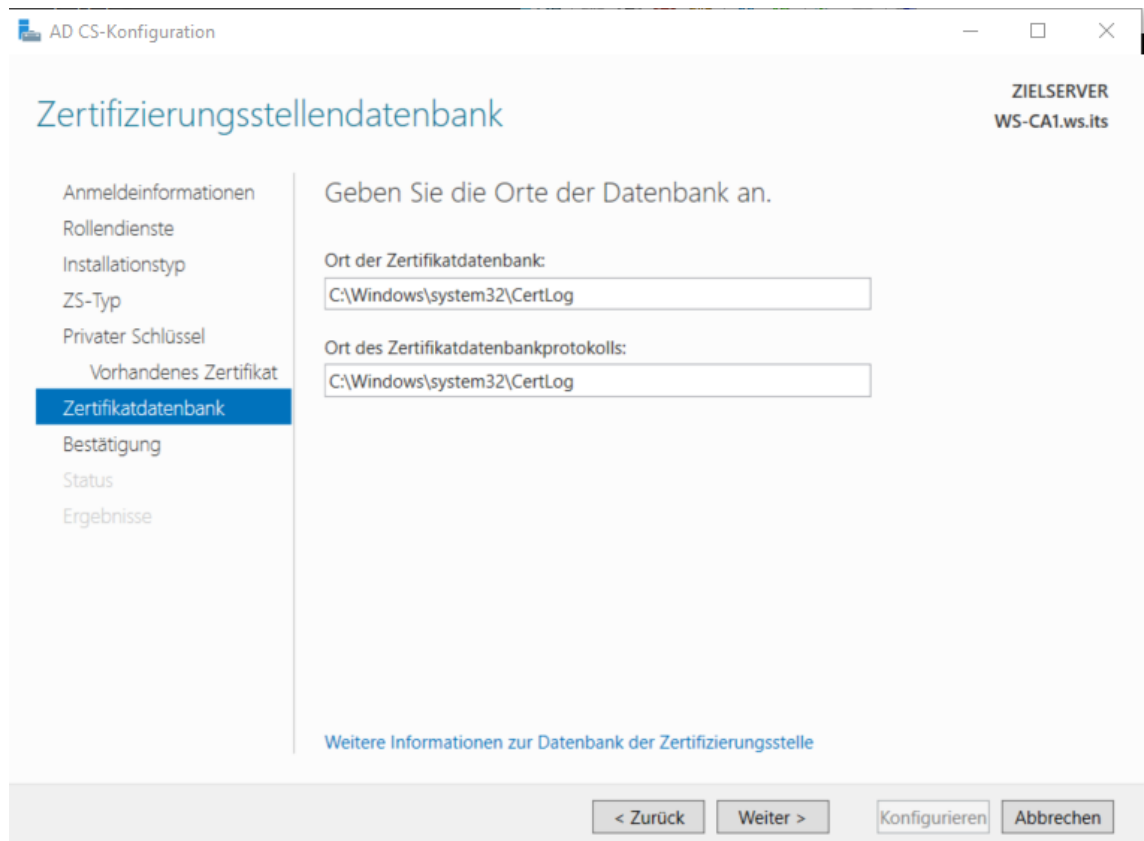
Das Zertifikat liegt im AdminShare:

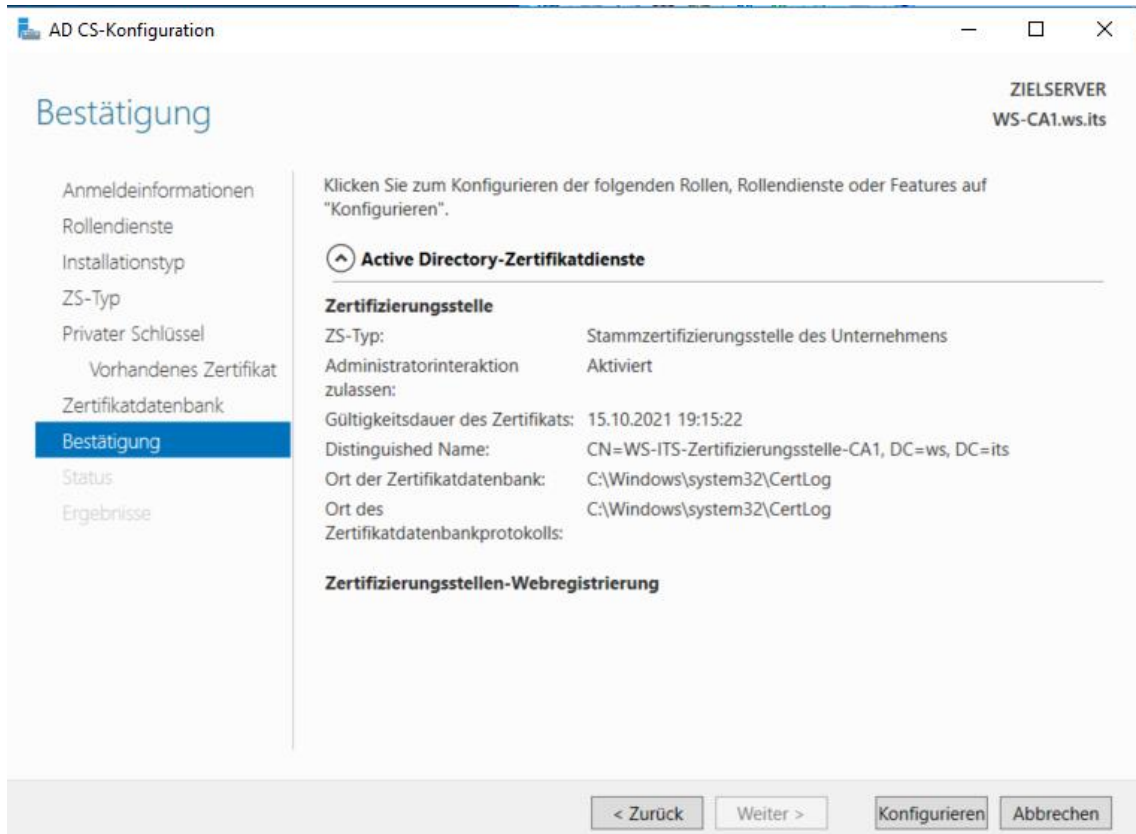


Es gab 2 alte Zertifikate. Beide werden eingespielt:

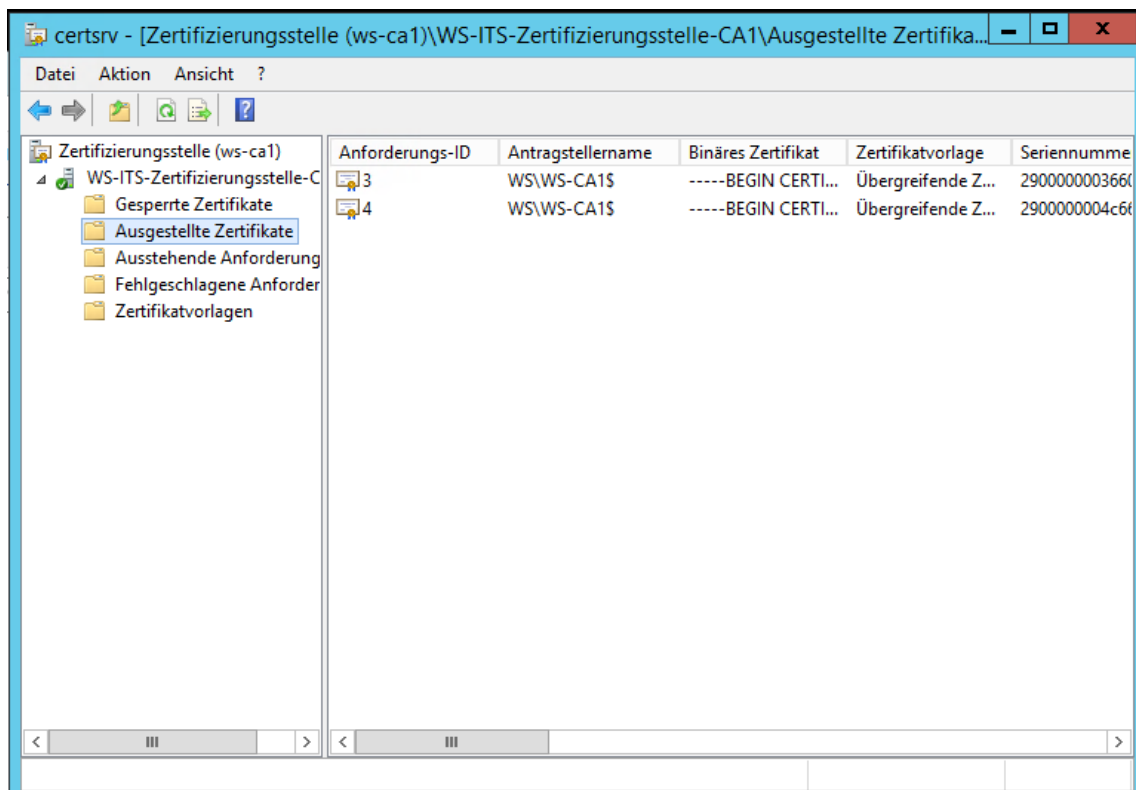


Die Pfade bleiben bestehen:



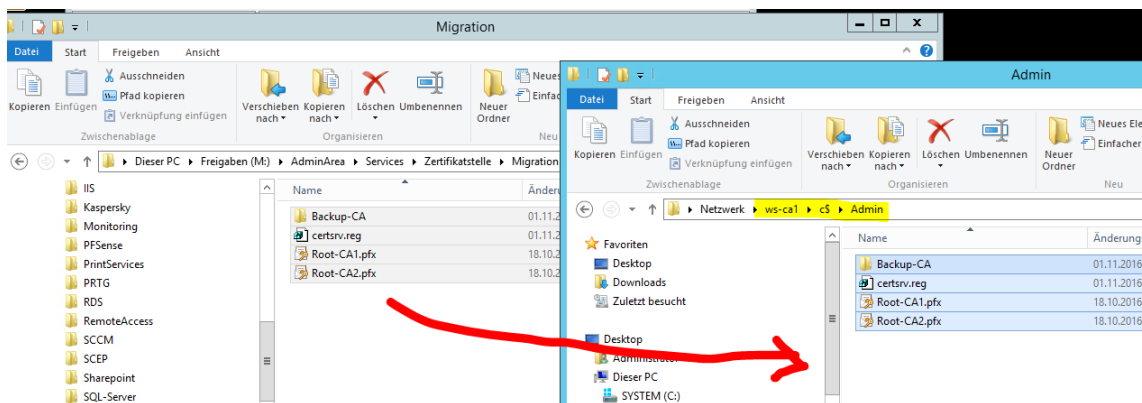


Das Ergebnis ist eine neue CA mit der alten Identität:



Import der alten DB und der Konfiguration

Zuerst kopiere ich die exportierten Daten auf den neuen Server:



Mangels GUI-Tools verwende ich die cmd für den Import der CA-Datensicherung und der Service-Registry. Der Dienst der CA muss dafür natürlich aus sein:

```

Administrator: C:\Windows\system32\cmd.exe

C:\>net stop certsvc
Active Directory-Zertifikatdienste wird beendet.
Active Directory-Zertifikatdienste wurde erfolgreich beendet.

C:\>certutil.exe -f -restoredb c:\Admin\Backup-CA
Die Datenbank für WS-CA1.ws.its\WS-ITS-Zertifizierungsstelle-CA1 wird wiederhergestellt.
Databankdateien werden wiederhergestellt: 100%
Protokolldateien werden wiederhergestellt: 100%
Vollständige Datenbankwiederherstellung für WS-CA1.ws.its\WS-ITS-Zertifizierungsstelle-CA1.
Active Directory-Zertifikatdienste anhalten und neu starten, um die Wiederherstellung der Datenbank von c:\Admin\Backup-CA fertig zu stellen.
CertUtil: -restoreDB-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.

C:\>reg import c:\Admin\certsrv.reg
Der Vorgang wurde erfolgreich beendet.

C:\>net start certsvc
Active Directory-Zertifikatdienste wird gestartet.
Active Directory-Zertifikatdienste wurde erfolgreich gestartet.

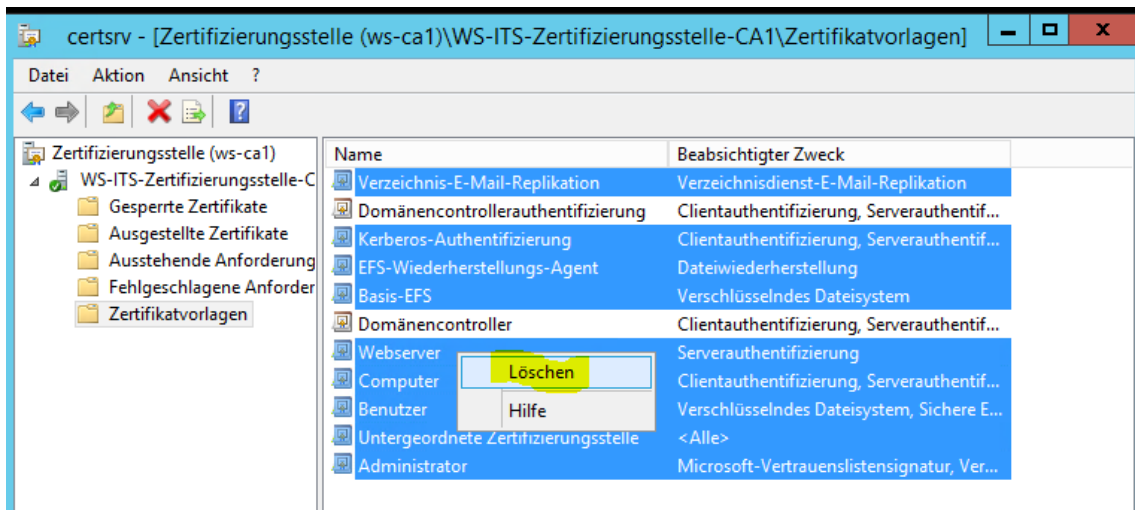
C:\>
    
```

Das Ergebnis sind die alten Daten in der neuen CA:

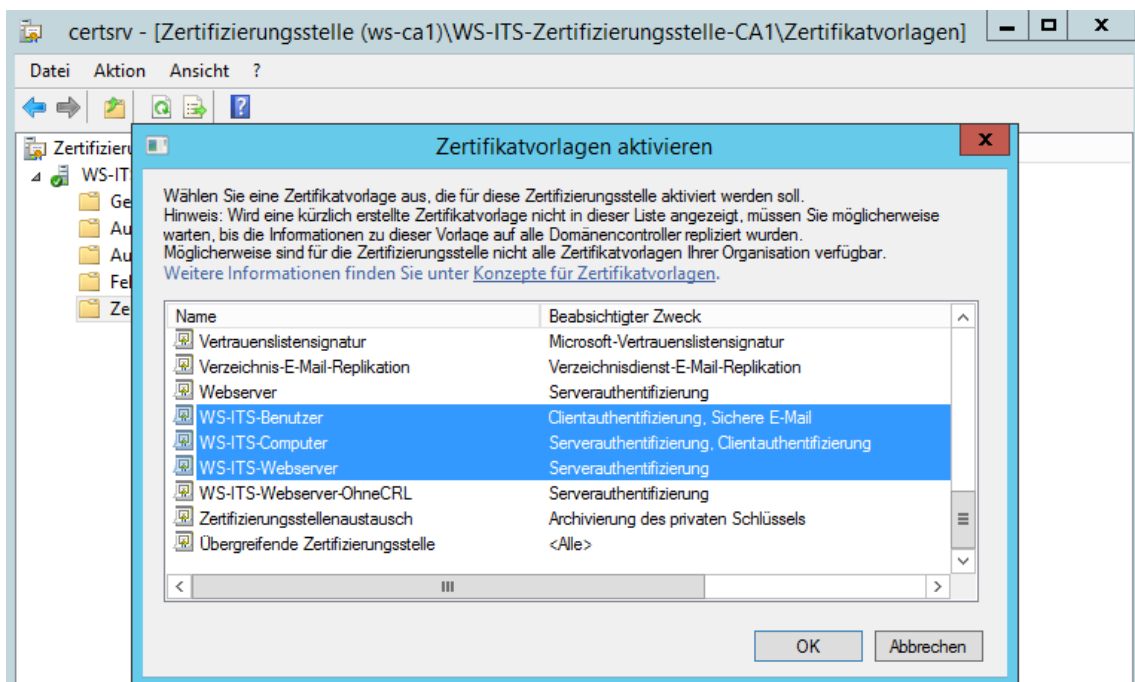
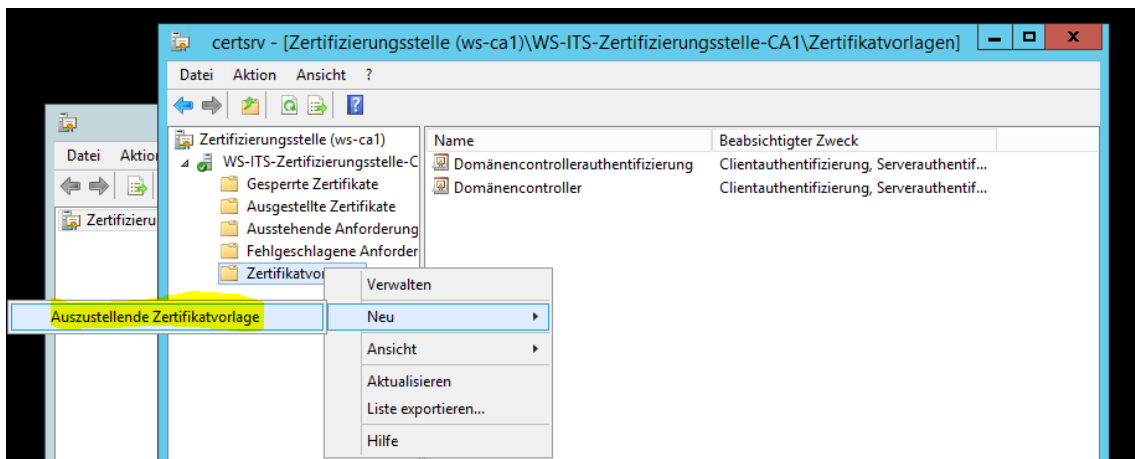
The screenshot shows the Certificate Authority console for 'Zertifizierungsstelle (ws-ca1)'. The 'Ausgestellte Zertifikate' folder is selected, displaying a list of certificates with columns for 'Anforderungs-ID', 'Antragstellername', 'Binäres Zertifikat', 'Zertifikatvorlage', and 'Seriennum'.

Anforderungs-ID	Antragstellername	Binäres Zertifikat	Zertifikatvorlage	Seriennum
2	WS\WS-DC1\$	-----BEGIN CERTI...	Domänencontrol...	1b00000002
3	WS\Administrator	-----BEGIN CERTI...	Webserver (Web...	1b00000003
4	WS\WS-MX1\$	-----BEGIN CERTI...	Computer (Mac...	1b00000004
5	WS\WS-CM1\$	-----BEGIN CERTI...	Computer (Mac...	1b00000005
6	WS\WS-FS1\$	-----BEGIN CERTI...	Computer (Mac...	1b00000006
7	WS\WS-RA1\$	-----BEGIN CERTI...	Computer (Mac...	1b00000007
8	WS\WS-HV1\$	-----BEGIN CERTI...	Computer (Mac...	1b00000008
9	WS\WS-DPMS	-----BEGIN CERTI...	Computer (Mac...	1b00000009
10	WS\WS-CA1\$	-----BEGIN CERTI...	Computer (Mac...	1b0000000a
11	WS\WS-CL1-W8\$	-----BEGIN CERTI...	Computer (Mac...	1b0000000b
12	WS\WS-HV2\$	-----BEGIN CERTI...	Computer (Mac...	1b0000000c
13	WS\WS-CL1-W8\$	-----BEGIN CERTI...	Computer (Mac...	1b0000000d
14	WS\WS-CL2\$	-----BEGIN CERTI...	Computer (Mac...	1b0000000e
15	WS\WS-CM1\$	-----BEGIN CERTI...	WS-ITS-Webserv...	1b0000000f
16	WS\WS-RA1\$	-----BEGIN CERTI...	WS-ITS-Webserv...	1b00000010
17	WS\WS-CL2\$	-----BEGIN CERTI...	Computer (Mac...	1b00000011
18	WS\WS-RA1\$	-----BEGIN CERTI...	WS-ITS-Webserv...	1b00000012

Jetzt fehlen noch die Vorlagen. Nicht verwendete Vorlagen entferne ich:



Dafür kommen die Vorlagen aus dem AD wieder in die CA:



Absicherung der Web-Registrierungsstelle

Die Website ist nicht unter https erreichbar:



Die Seite kann nicht angezeigt werden.

- Vergewissern Sie sich, dass die Webadresse <https://ws-ca1.ws.its> stimmt.
- Suchen Sie die Seite mit Ihrer Suchmaschine.
- Aktualisieren Sie die Seite in ein paar Minuten.

Für eine leichte Administration installiere ich auf dem neuen Server den Management-Service:

```
Administrator: C:\Windows\system32\cmd.exe - powershell

PS C:\> Add-WindowsFeature Web-Mgmt-Service

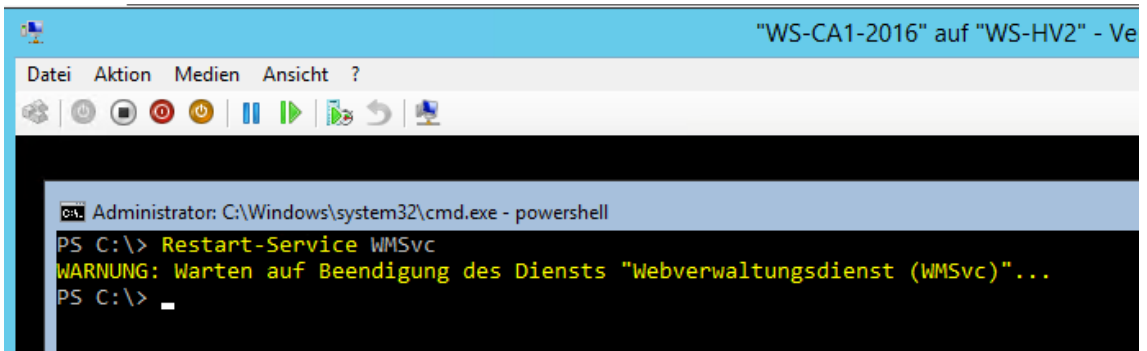
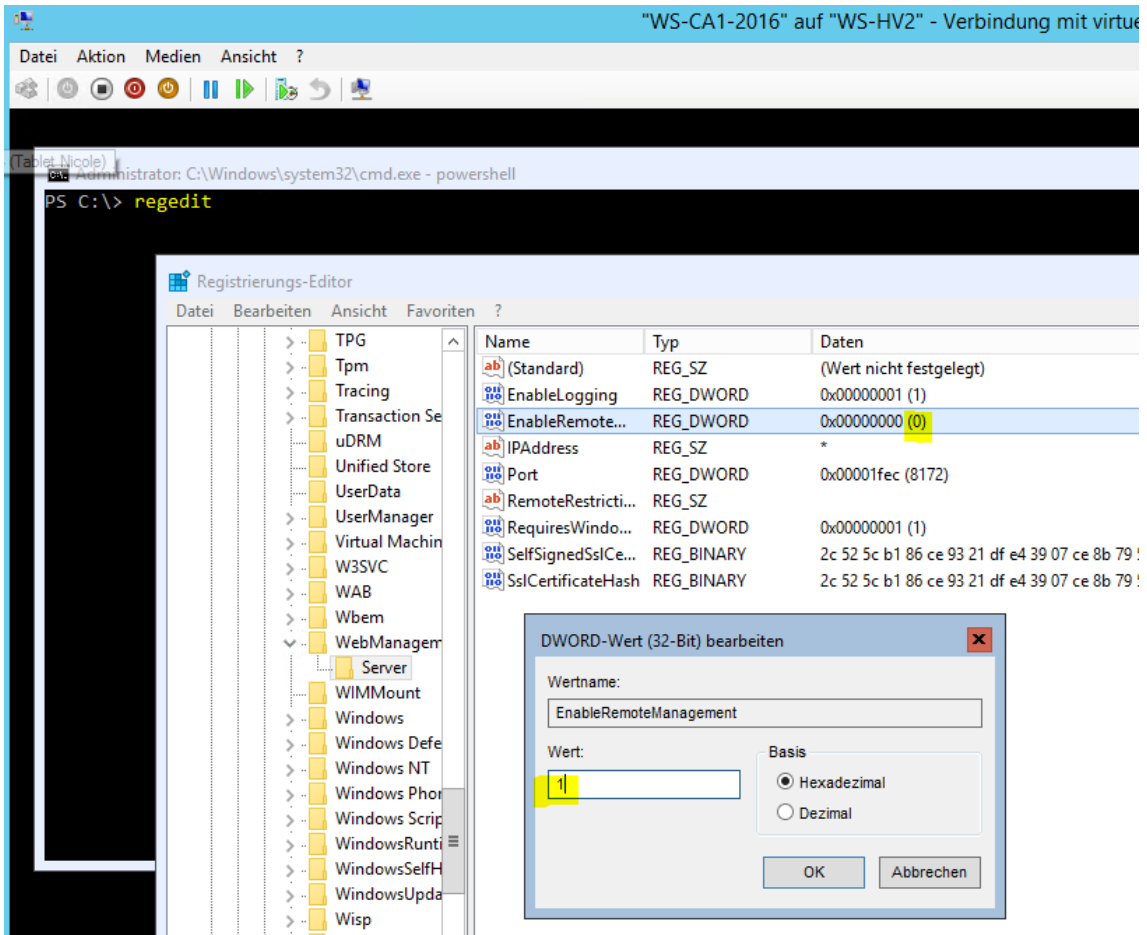
Success Restart Needed Exit Code      Feature Result
-----
True    No           Success      {ASP.NET 4.6, Verwaltungsdienst}

PS C:\> Get-Service WMSVC

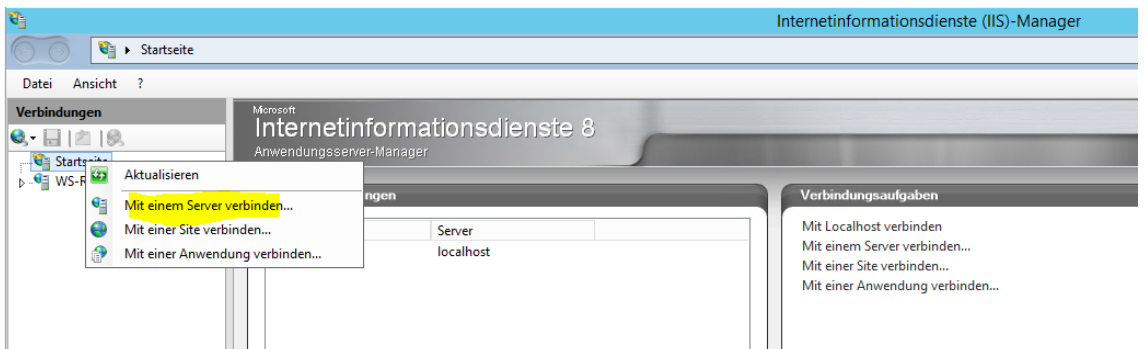
Status  Name      DisplayName
-----
Stopped WMSVC     Webverwaltungsdienst

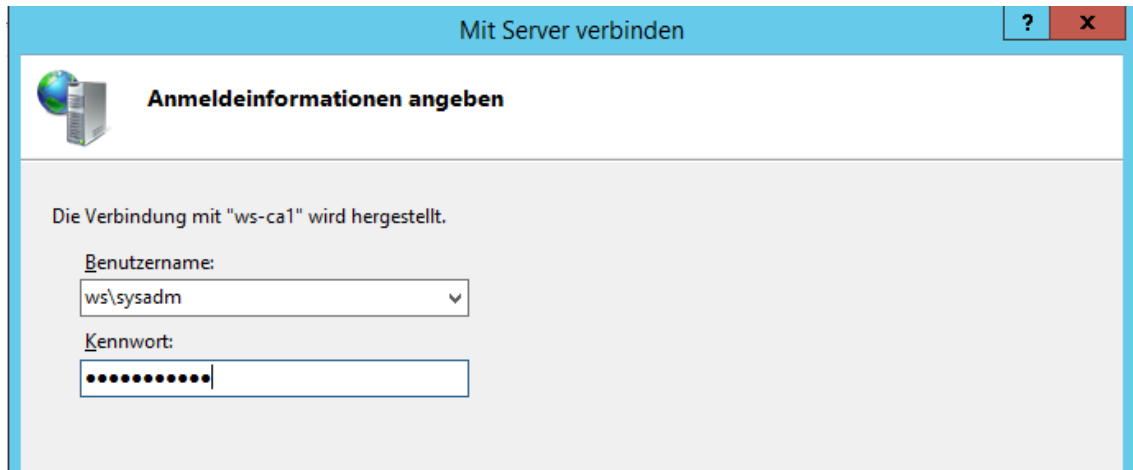
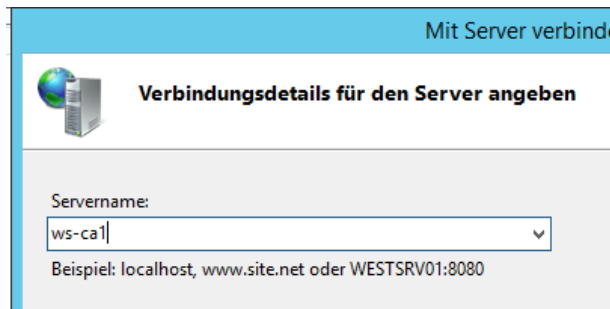
PS C:\> Start-Service WMSVC
PS C:\> _
```

Die erforderliche Firewallausnahme setzt eine GPO. Dennoch ist eine Service-Konfiguration erforderlich:

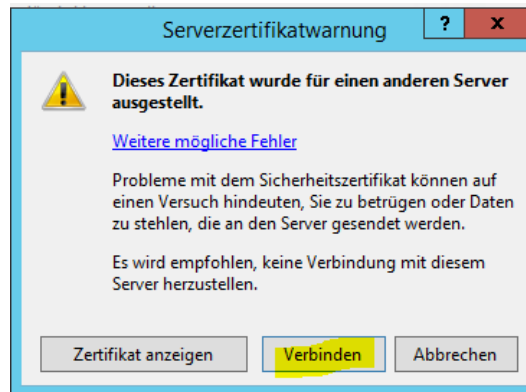


Von einem Server mit IIS-Management kann jetzt eine Verbindung hergestellt werden:

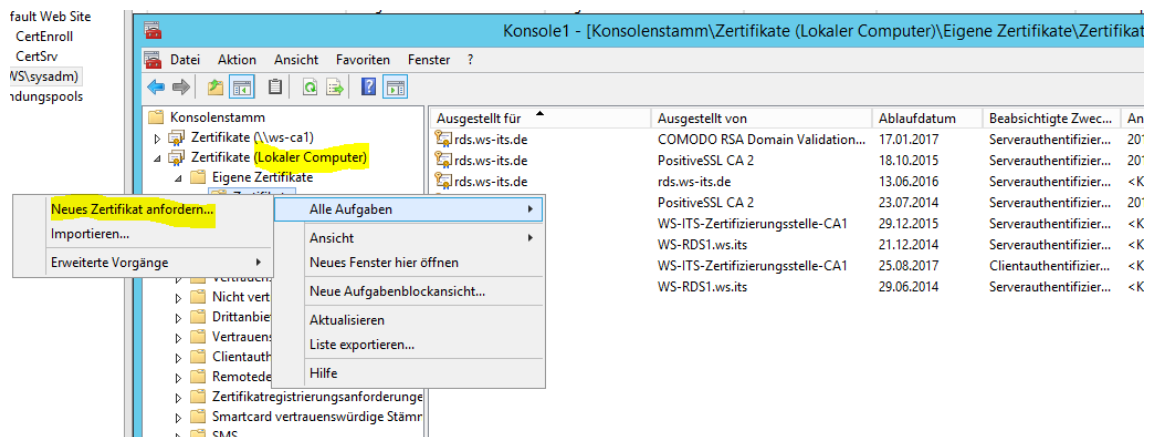


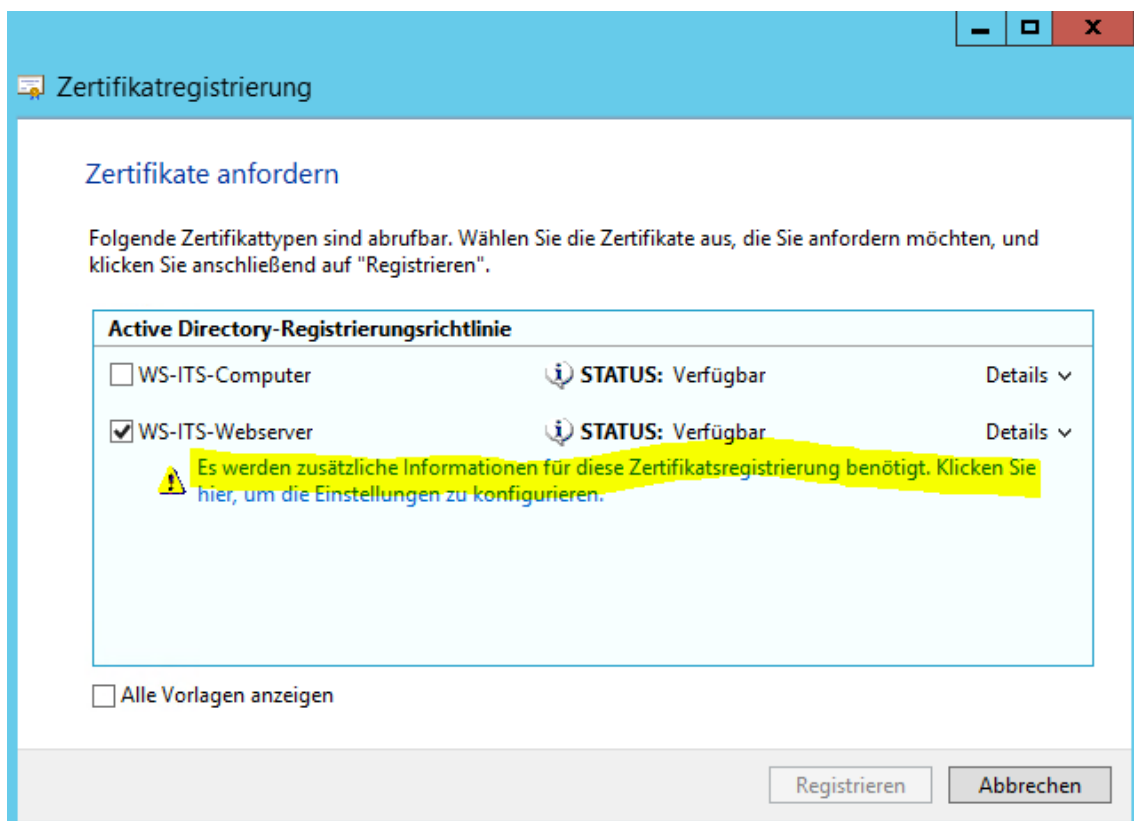
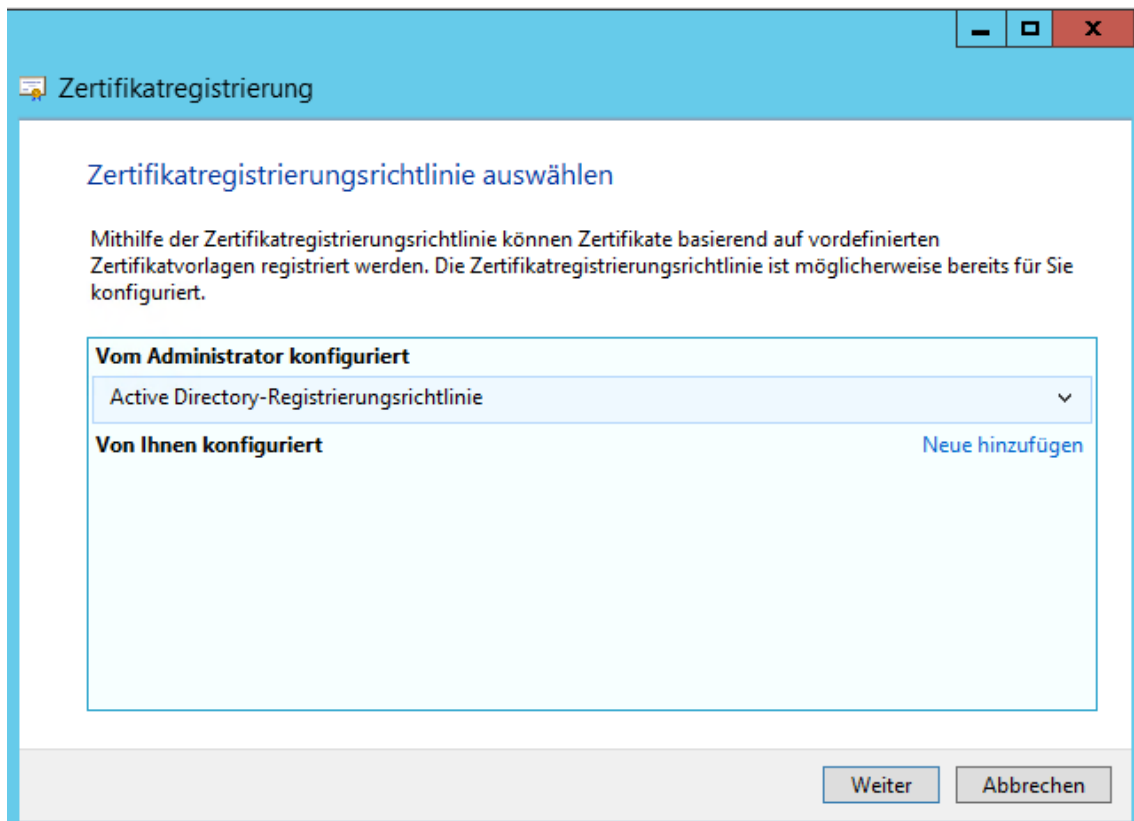


Natürlich passt das Zertifikat nicht...



Die Verbindung steht. Aber es fehlt ein Webserver-Zertifikat. Dieses kann mit einer Zertifikate-MMC auf einem anderen Server angefordert werden. Sehr leicht geht das, indem man auf dem Management-Server ein Zertifikat mit dem richtigen Namen lokal anfordert, exportiert und dann auf dem Remote-Server importiert:



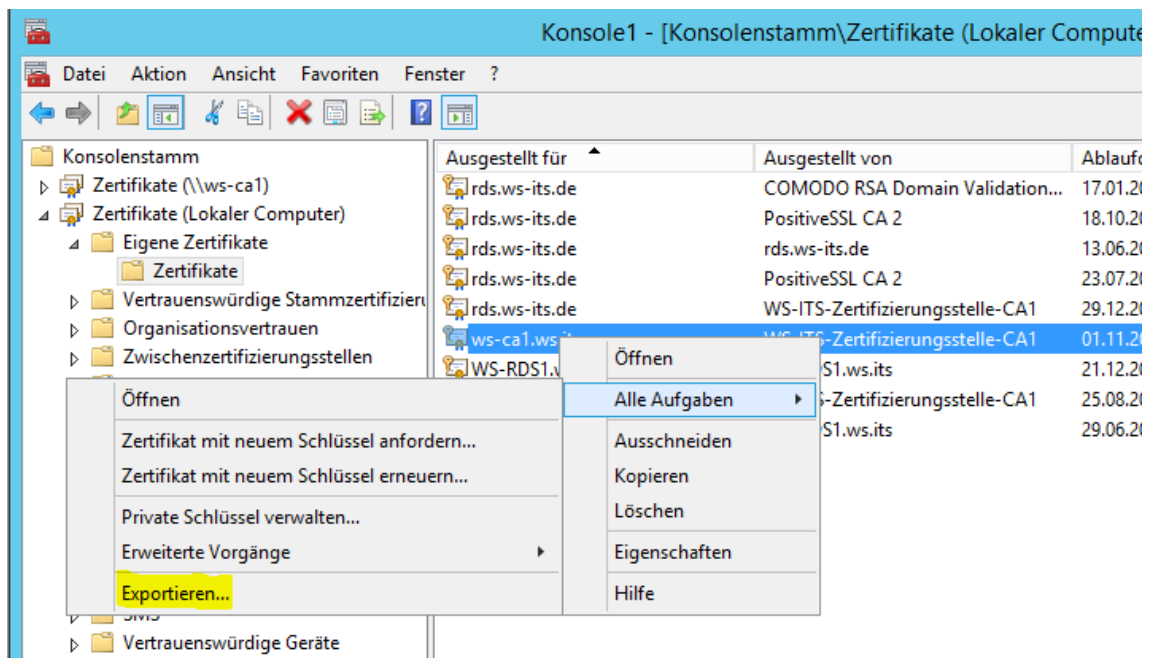
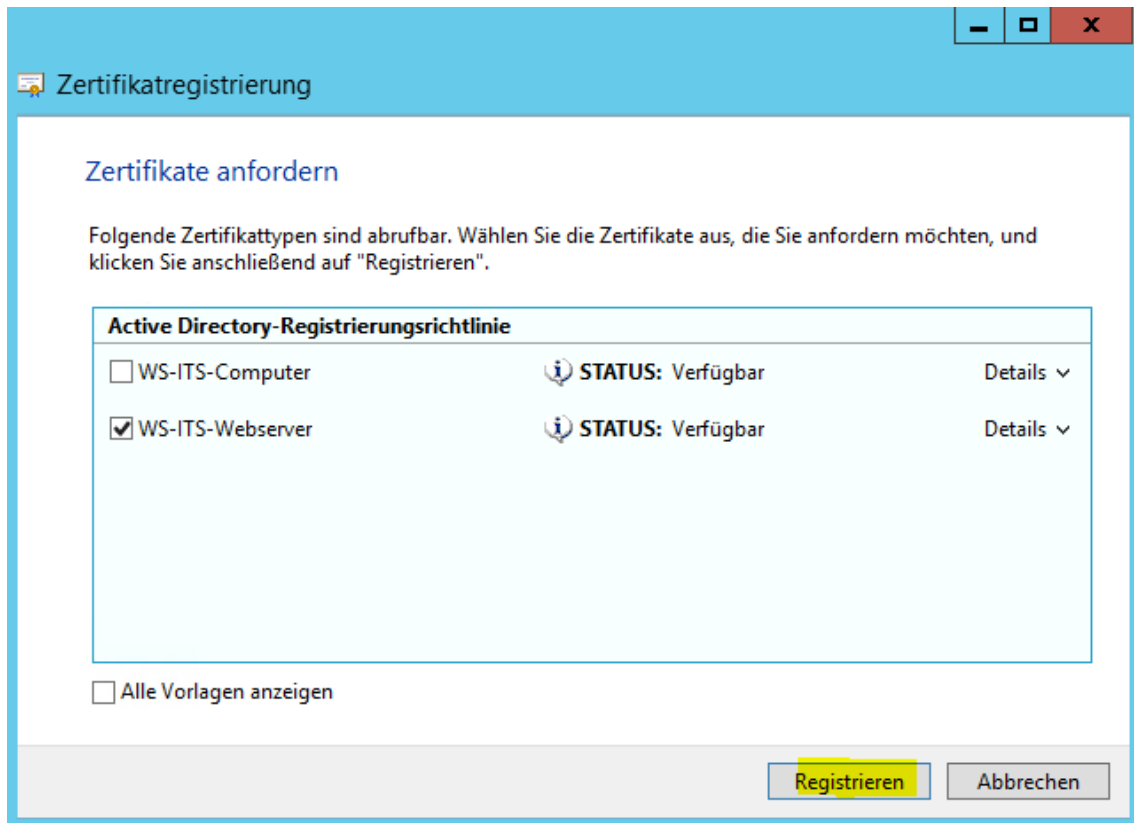


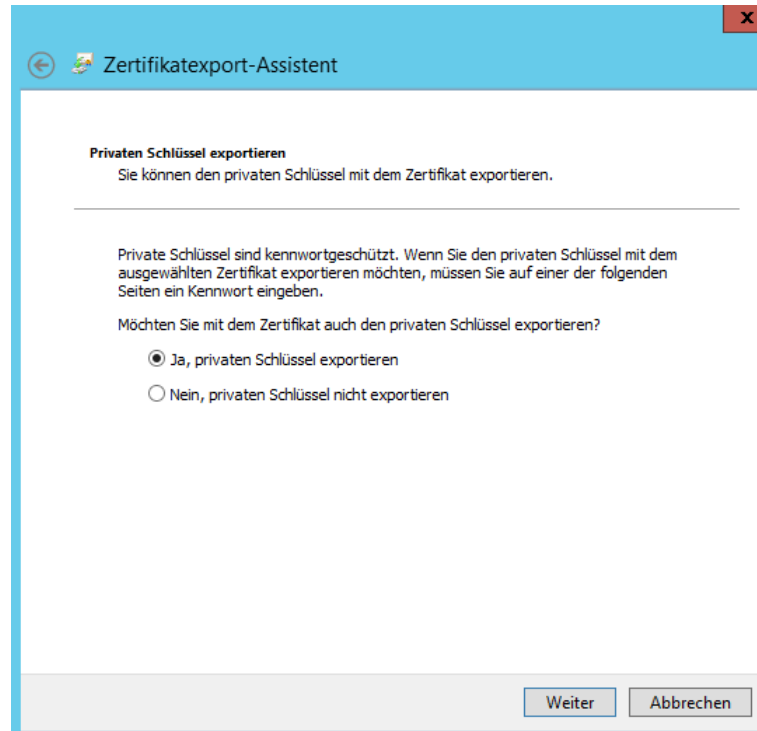
Zertifikateigenschaften x

Privater Schlüssel	Zertifizierungsstelle	Signatur
Antragsteller	Allgemein	Erweiterungen
<p>Der Antragsteller eines Zertifikats ist der Benutzer oder Computer, für den das Zertifikat ausgestellt ist. Geben Sie Informationen über die zulässigen Antragstellernamen und alternative Namenswerte ein, die in einem Zertifikat verwendet werden dürfen.</p> <p>Zertifikatsantragsteller Der das Zertifikat empfangende Benutzer oder Computer</p> <p>Antragstellername:</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Typ: Allgemeiner Name</p> <p>Wert: <input style="width: 90%;" type="text"/></p> </div> <div style="width: 10%; text-align: center;"> <p>Hinzufügen ></p> <p>< Entfernen</p> </div> <div style="width: 40%; border: 1px solid black; padding: 5px;"> <p>CN=ws-ca1.ws.its</p> </div> </div> <p>Alternativer Name:</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 45%;"> <p>Typ: Verzeichnisname</p> <p>Wert: <input style="width: 90%;" type="text"/></p> </div> <div style="width: 10%; text-align: center;"> <p>Hinzufügen ></p> <p>< Entfernen</p> </div> <div style="width: 40%; border: 1px solid black; padding: 5px;"> </div> </div>		
<p>OK Abbrechen Übernehmen</p>		

Zertifikateigenschaften x

Privater Schlüssel	Zertifizierungsstelle	Signatur
Antragsteller	Allgemein	Erweiterungen
<p style="text-align: center;">Privater Schlüssel</p> <p>Kryptografiedienstleister v</p> <p>Schlüsselloptionen ^</p> <p>Legen Sie die Schlüssellänge und die Exportoptionen für den privaten Schlüssel fest.</p> <p>Schlüsselgröße: 2048</p> <p><input checked="" type="checkbox"/> Privaten Schlüssel exportierbar machen</p> <p><input type="checkbox"/> Archivierung des privaten Schlüssels zulassen</p> <p><input type="checkbox"/> Verstärkter Schutz für den privaten Schlüssel</p> <p>Schlüsseltyp v</p> <p>Schlüsselberechtigungen v</p>		
<p>OK Abbrechen Übernehmen</p>		





Nun kopiere ich das Zertifikat auf dem neuen CA-Server und importiere es mit der PowerShell:

```

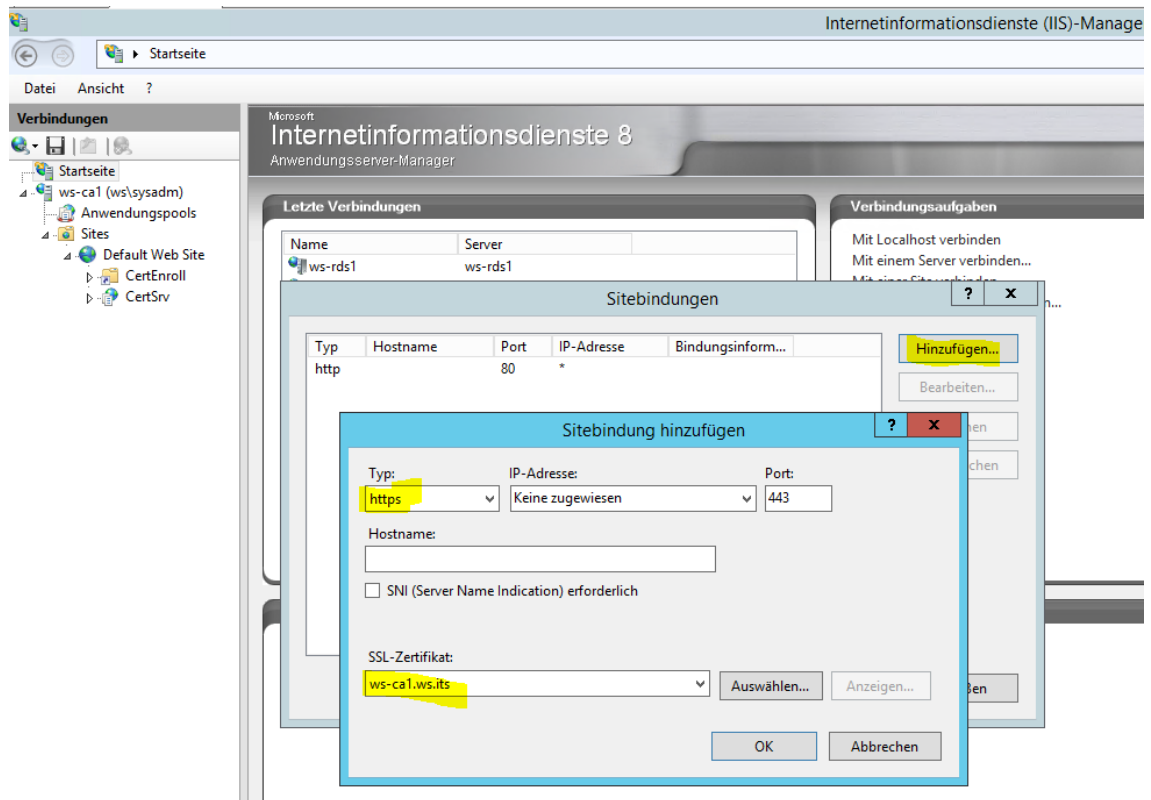
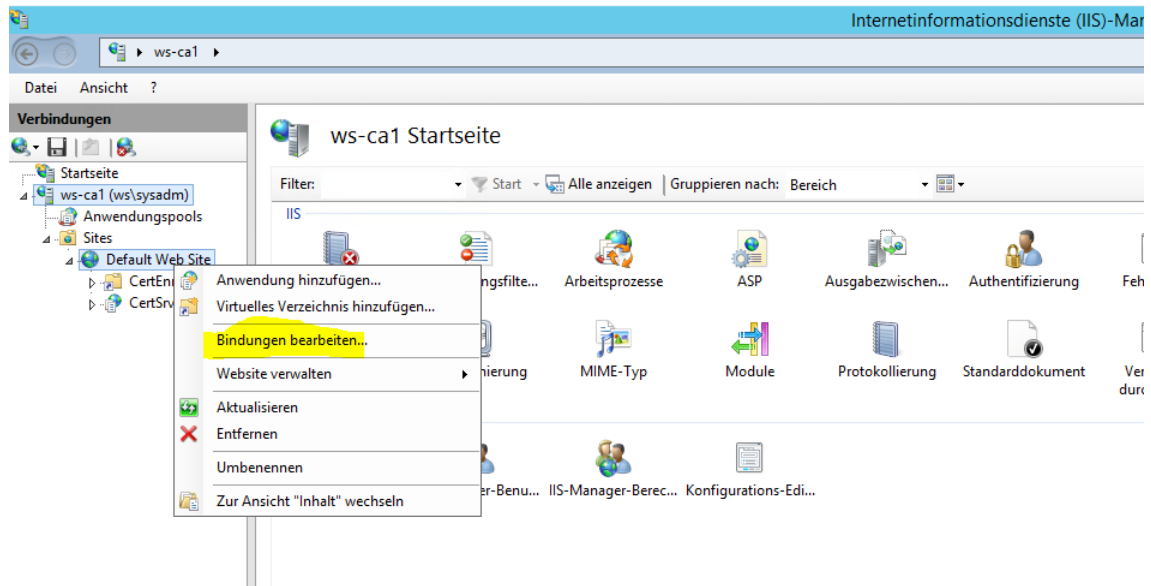
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\> Import-PfxCertificate -Exportable -CertStoreLocation Cert:\LocalMachine\My -FilePath 'C:\Admin\2016-11-01 ws-ca1.ws.its.pfx' -Password (ConvertTo-SecureString -String [REDACTED] -AsPlainText -Force)

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\My

Thumbprint                               Subject
-----
4D2F1B03182810BA90330B3906DC6AFC4AE0CA55  CN=ws-ca1.ws.its

PS C:\>
    
```

Im IIS-Manager kann ich nun das Zertifikat für die https-Bindung verwenden:



Jetzt ist der Webservice unter https erreichbar:



Microsoft-Active Directory-Zertifikatdienste – WS-ITS-Zertifizierungsstelle-CA1

Willkommen

Auf diese Website können Sie ein Zertifikat für den Webbrowser, E-Mail-Client oder andere Programme anfordern. Mit einem Zertifikat können Web kommunizieren, bestätigen, E-Mail-Nachrichten signieren oder verschlüsseln und weitere Sicherheitsaufgaben, abhängig vom angefordert

Sie können diese Website auch zum Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Zertifikatssperrliste verwenden anzeigen.

Weitere Informationen zu Active Directory-Zertifikatdienste erhalten Sie unter [Active Directory-Zertifikatdienstedokumentation](#).

Wählen Sie eine Aufgabe:

- [Ein Zertifikat anfordern](#)
- [Status ausstehender Zertifikate anzeigen](#)
- [Download eines Zertifizierungsstellenzertifikats, einer Zertifikatkette oder einer Sperrliste](#)

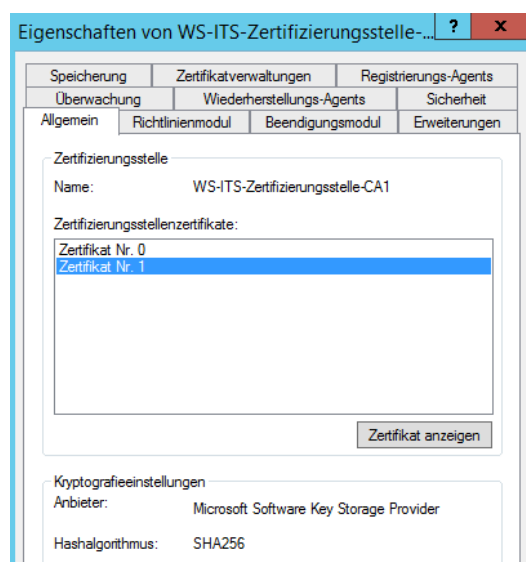
Anpassungen für SHA256

Das neue Zertifikat der Root-CA war bereits für SHA256 erstellt worden. Es sind nur noch einige Feinheiten erforderlich:

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\> certutil -setreg ca\csp\CNGHashAlgorithm SHA256
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\WS-ITS-Zertifizierungsstelle-CA1\csp:
Alter Wert:
    CNGHashAlgorithm REG_SZ = SHA256
Neuer Wert:
    CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.
```

```
Administrator: C:\Windows\system32\cmd.exe - powershell
PS C:\> certutil -setreg ca\csp\Provider "Microsoft Software Key Storage Provider"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\WS-ITS-Zertifizierungsstelle-CA1\csp:
Alter Wert:
    Provider REG_SZ = Microsoft Software Key Storage Provider
Neuer Wert:
    Provider REG_SZ = Microsoft Software Key Storage Provider
CertUtil: -setreg-Befehl wurde erfolgreich ausgeführt.
Der Dienst "CertSvc" muss neu gestartet werden, damit die Änderungen wirksam werden.
PS C:\>
PS C:\> Restart-Service certsvc
PS C:\>
```

Das Ergebnis:



Eigenschaften von WS-ITS-Zertifizierungsstelle-... ? X

Speicherung	Zertifikatverwaltungen	Registrierungs-Agents
Überwachung	Wiederherstellungs-Agents	Sicherheit
Allgemein	Richtlinienmodul	Beendigungsmodul
		Erweiterungen

Zertifizierungsstelle

Name: WS-ITS-Zertifizierungsstelle-CA1

Zertifizierungsstellenzertifikate:

Zertifikat Nr. 0
Zertifikat Nr. 1

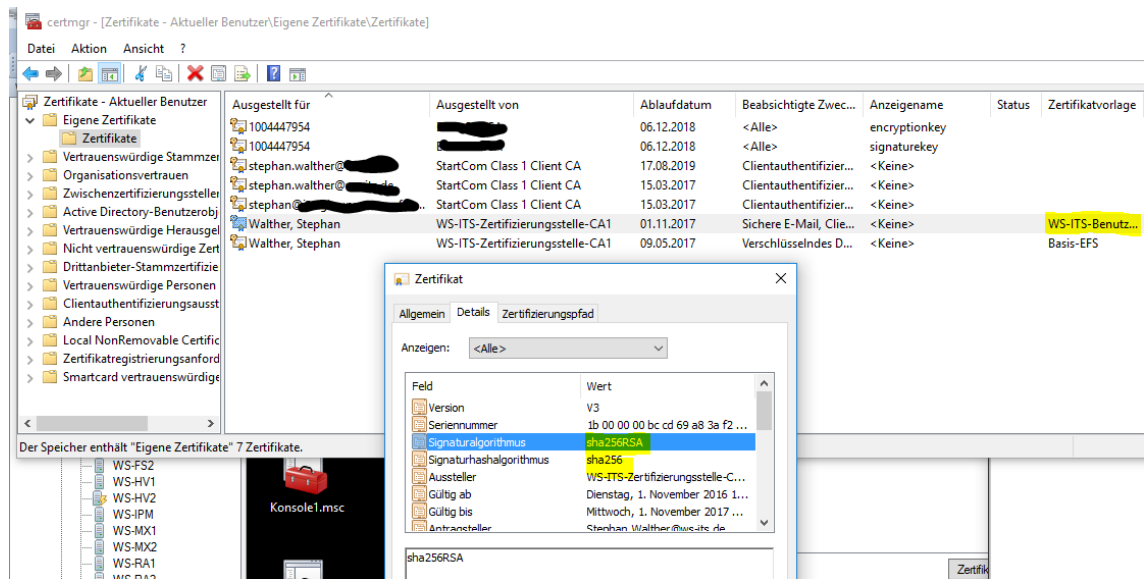
Zertifikat anzeigen

Kryptografieeinstellungen

Anbieter: Microsoft Software Key Storage Provider

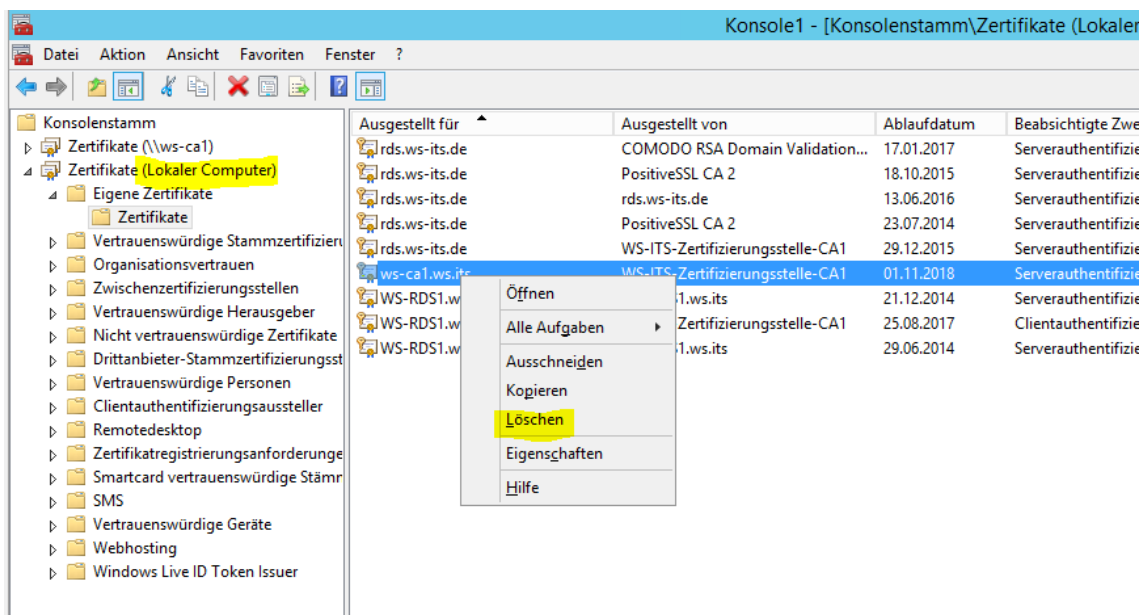
Hashalgorithmus: SHA256

Ein Test zeigt, dass auch ausgestellte Zertifikate mit SHA256 abgesichert sind:



4. Bereinigung

Auf dem Management-Server steht noch das Zertifikat im Speicher. Das wird gelöscht:



Sowohl der alte als auch der neue Server sind virtuelle Maschinen unter Hyper-V. Die alte VM wird nun entfernt, die neue wird dem Namen der alten angepasst. Ebenso passe ich noch die Hyper-V-Konfiguration an (Integrationsdienste, automatische Startaktion, ...)

Alle Arbeitsdateien werden in das AdminShare verschoben.

Der neue Server wird aktiviert.

Das Backup ist bereits über eine GPO konfiguriert. Ein Test der Sicherung zeigt einen Erfolg.

Als letzter Schritt wird das Monitoring angepasst.