Inhalt

1. Szenario

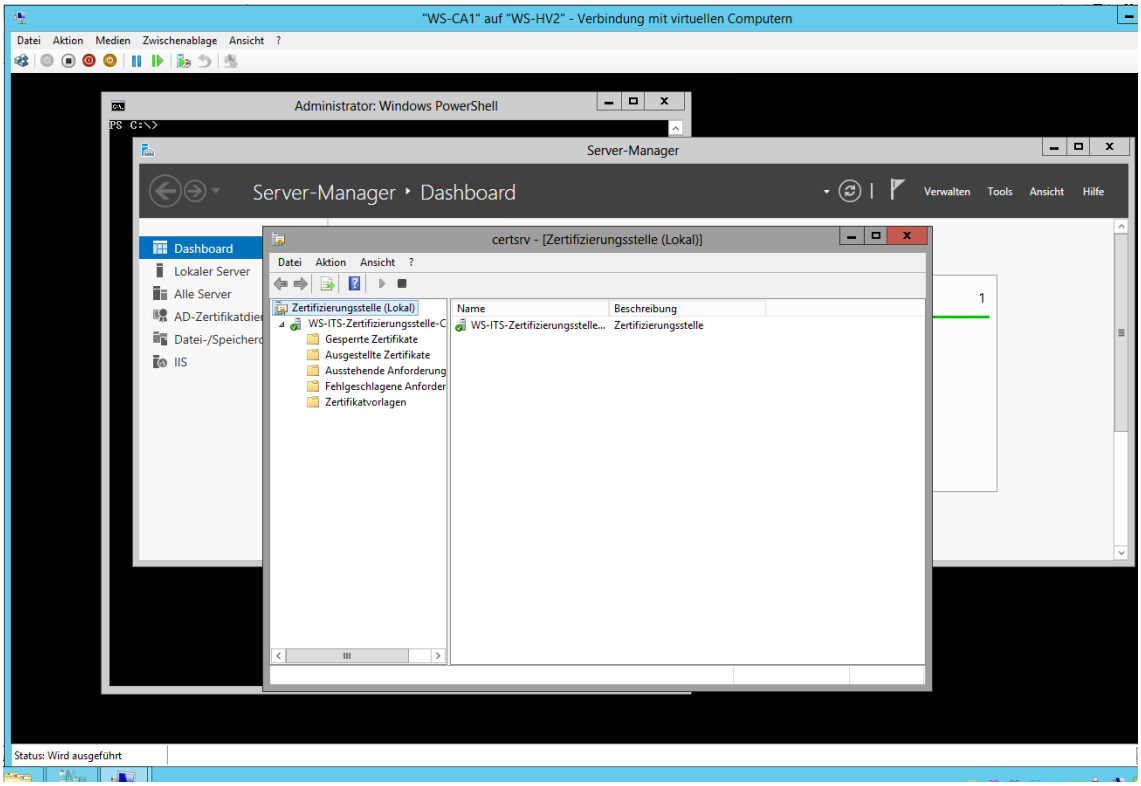
Aktuell wird in einer Windows Server 2012 R2 Gesamtstruktur eine Active Directory Zertifizierungsstelle auf dem DomainMember WS-CA1 AD-integriert betrieben. Der Server WS-CA1 läuft auf einem Windows Server 2012 als Server Core mit Mini-Shell-Oberfläche.

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

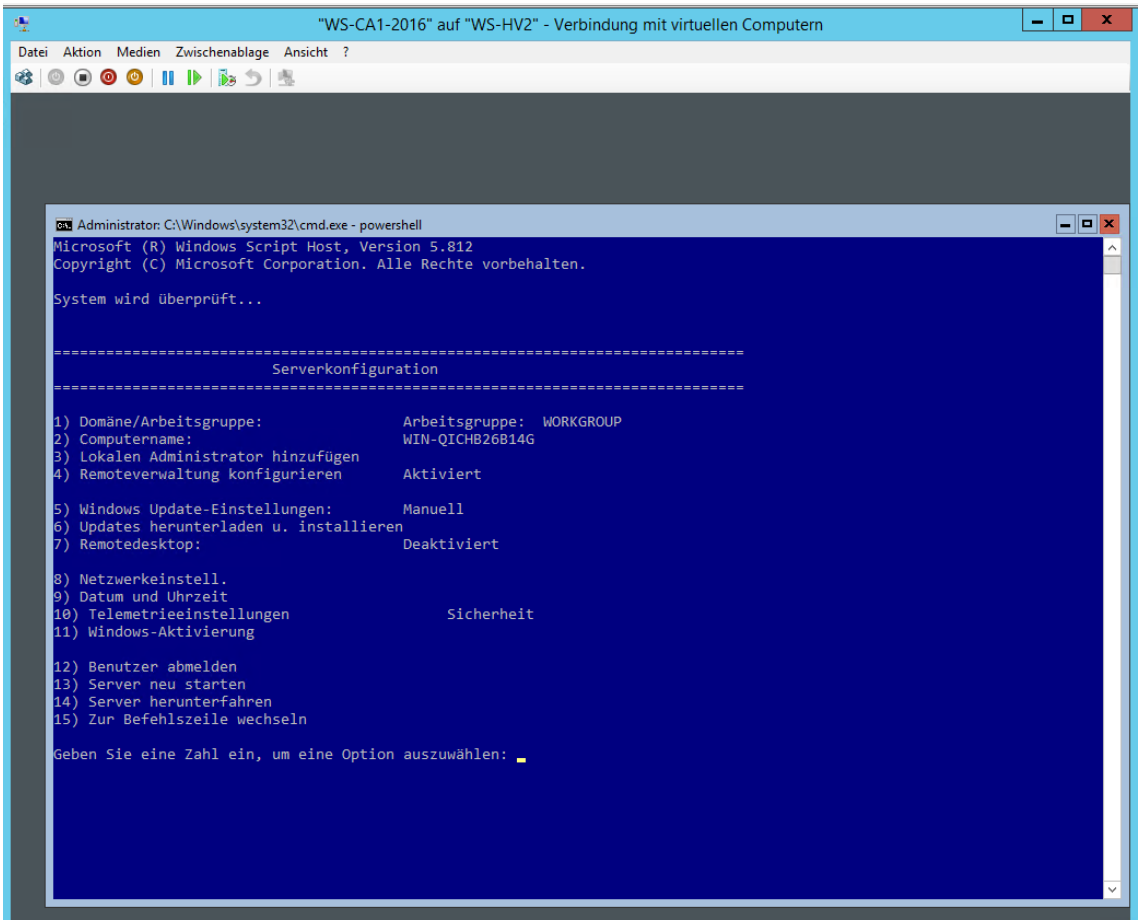
Als Migrationsverfahren wir ein klassisches Wipe & Load verwendet: der neue Server wird nach dem Umzug die CA unter der gleichen Identität (Name im AD, SID, IP, …) fortführen.

2. Auf dem alten Server

Kontrolle der alten CA

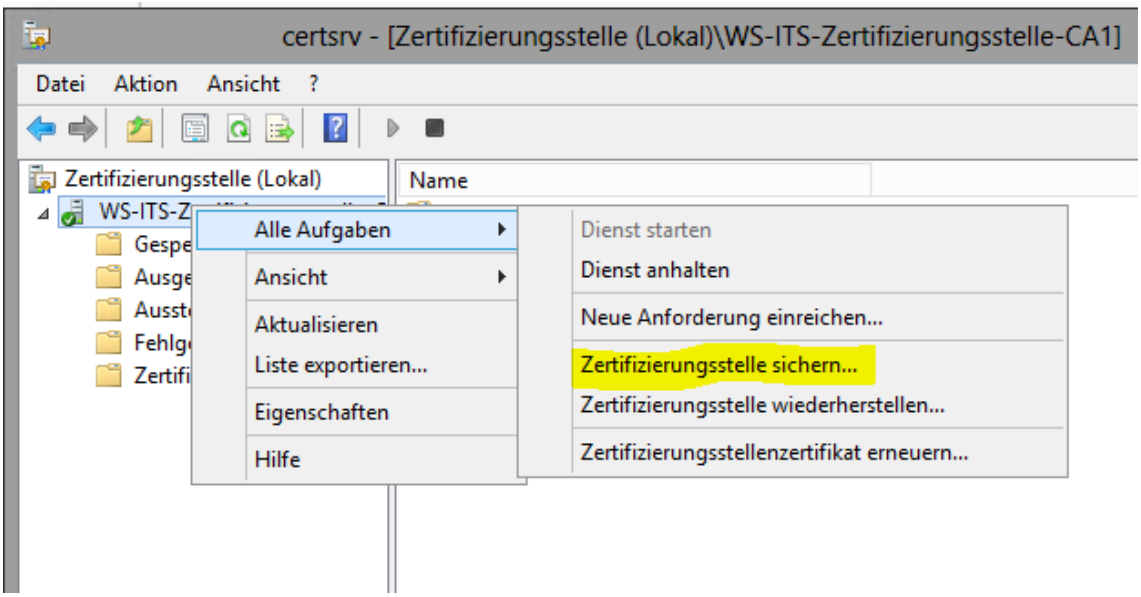


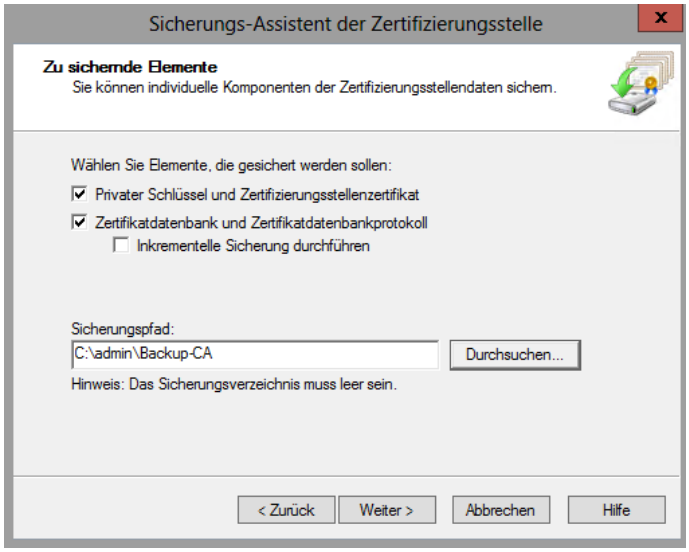
Aufsetzen des neuen Servers

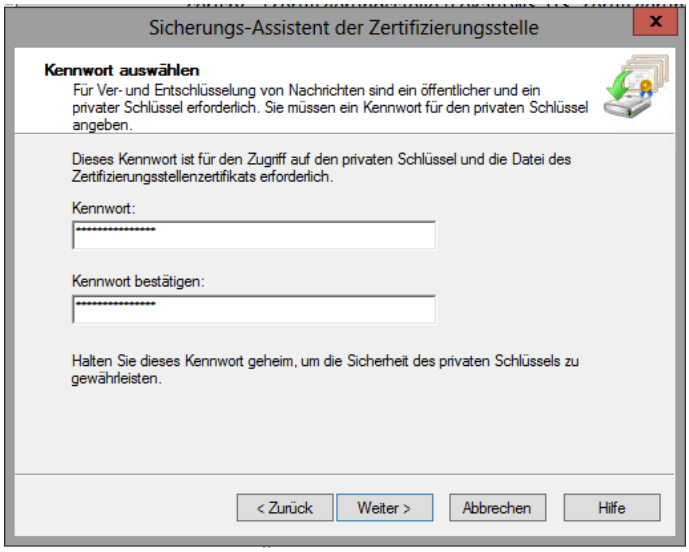


Sicherung des alten CA-Servers

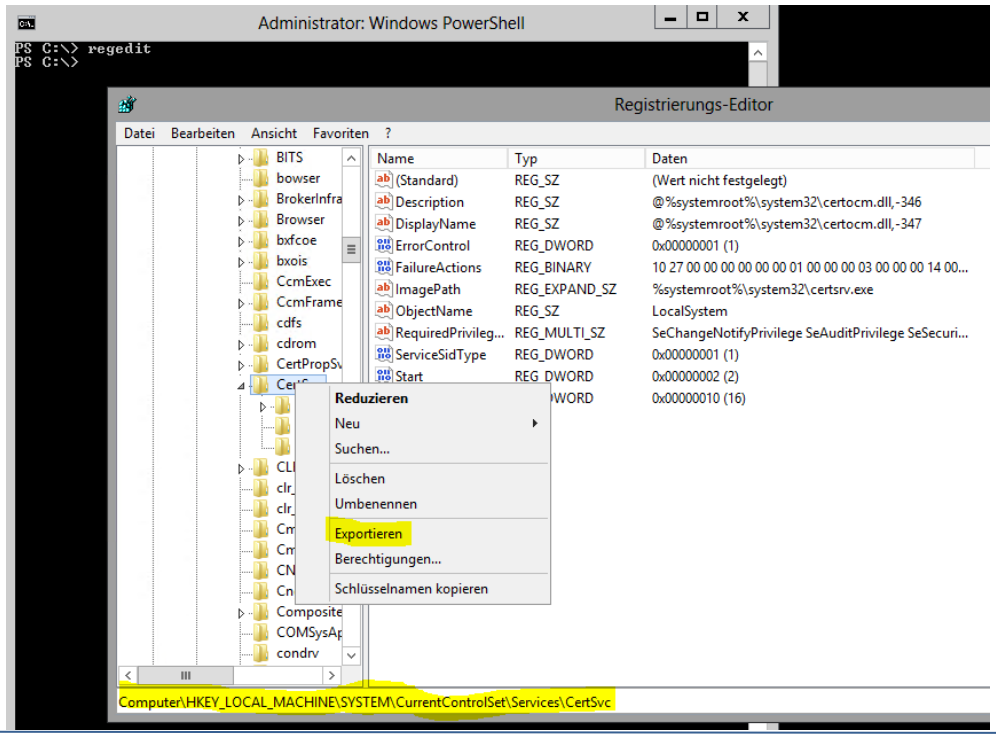
Auf dem alten Server stehen dank Mini-Shell die Servertools lokal zur Verfügung. Zuerst wird die CA mit den Zertifikaten lokal gesichert:

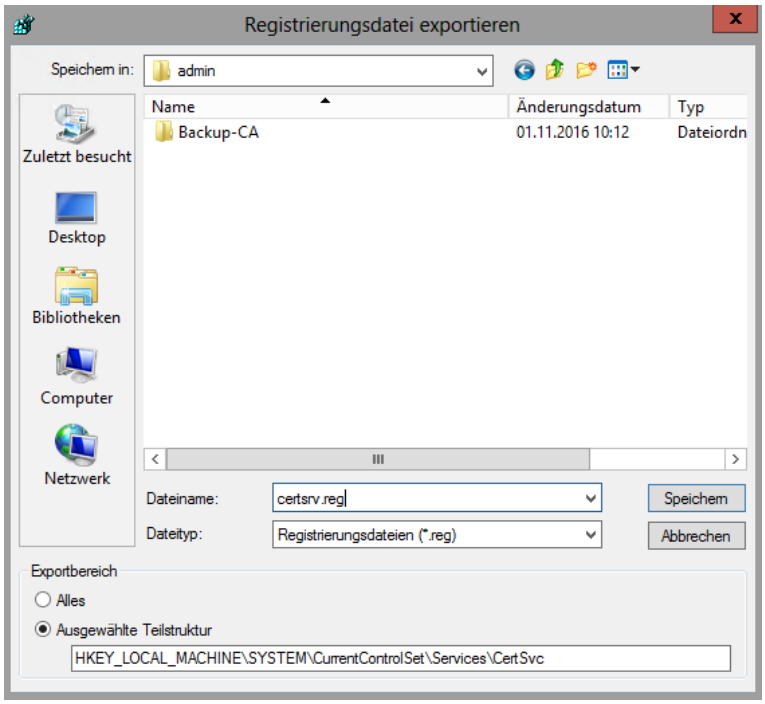




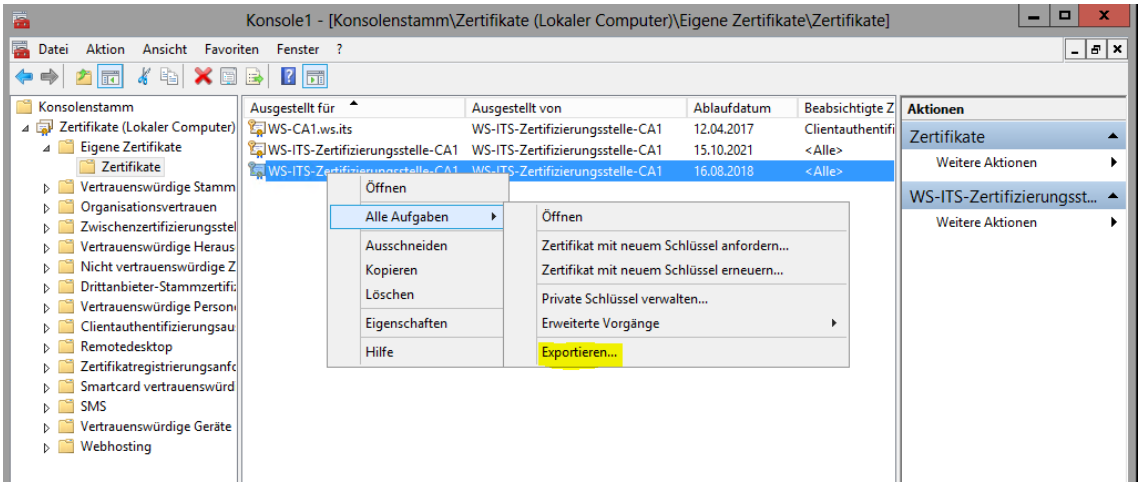


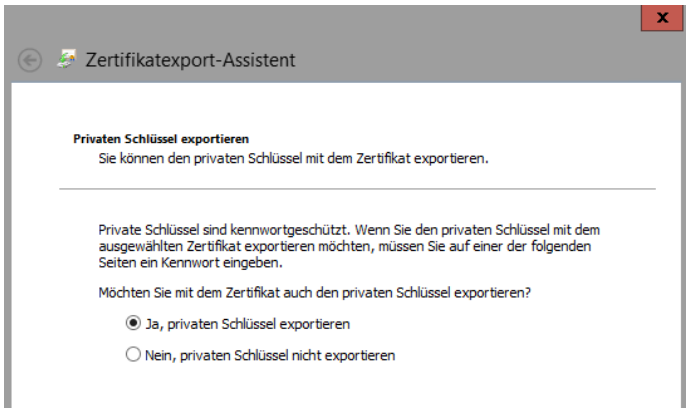
Zusätzlich muss die Konfiguration des CA-Services aus der Registry gesichert werden:

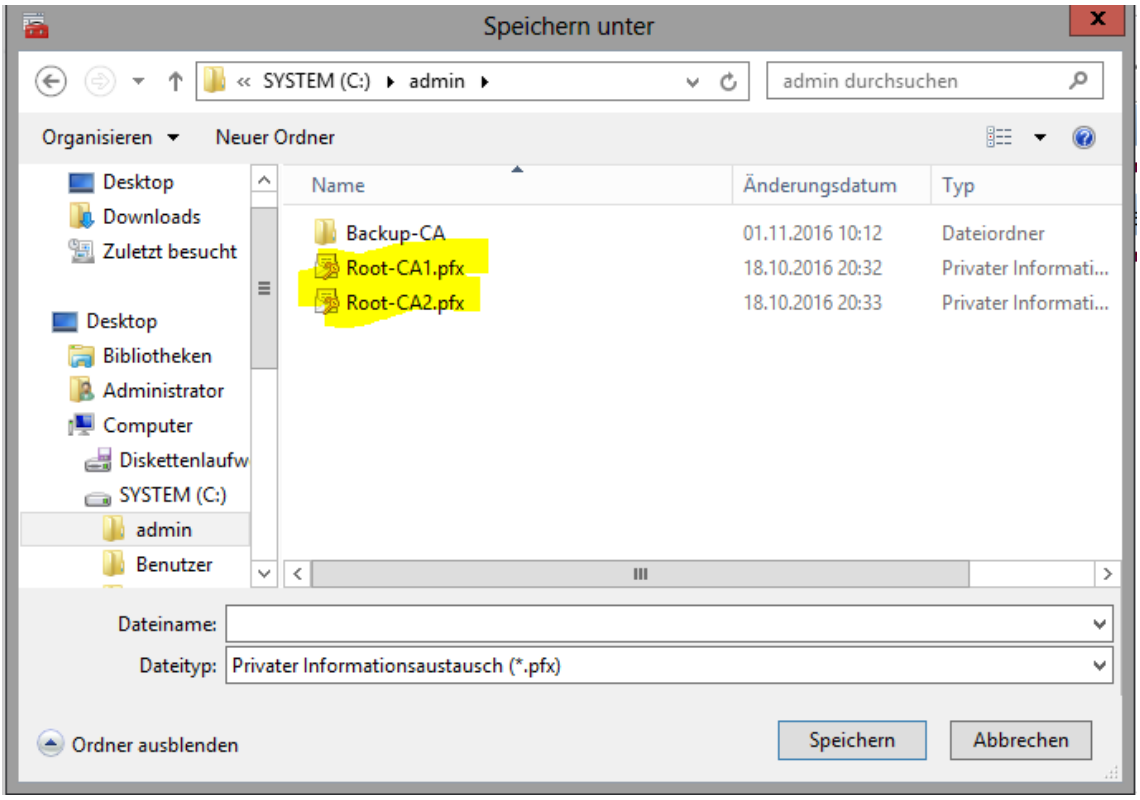




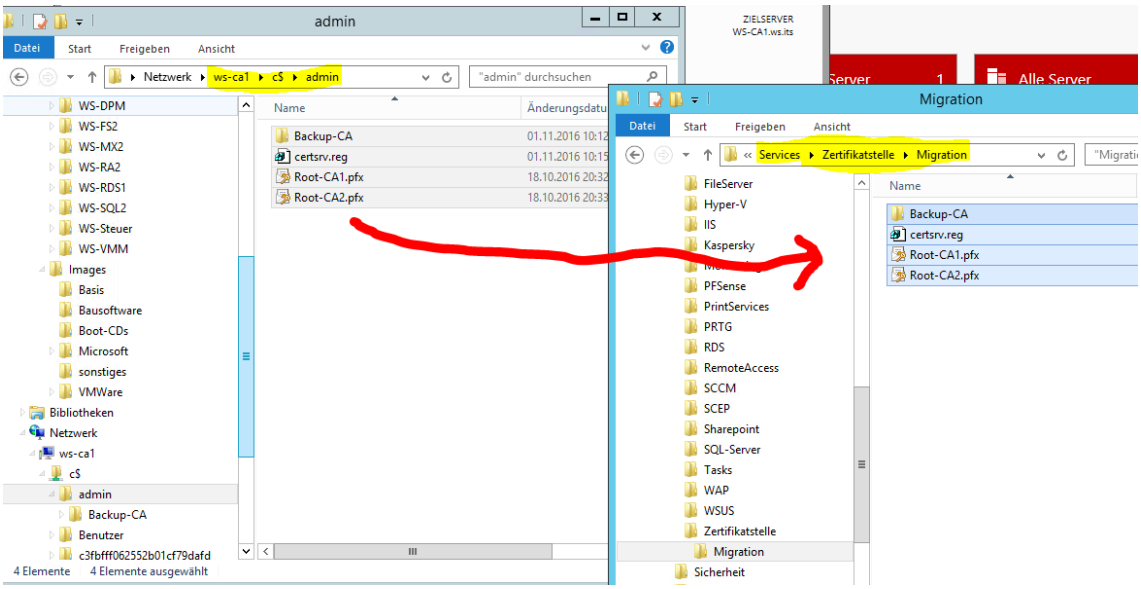
Es existieren 2 Root-CA-Zertifikate. Diese werden ebenfalls als PFX exportiert:





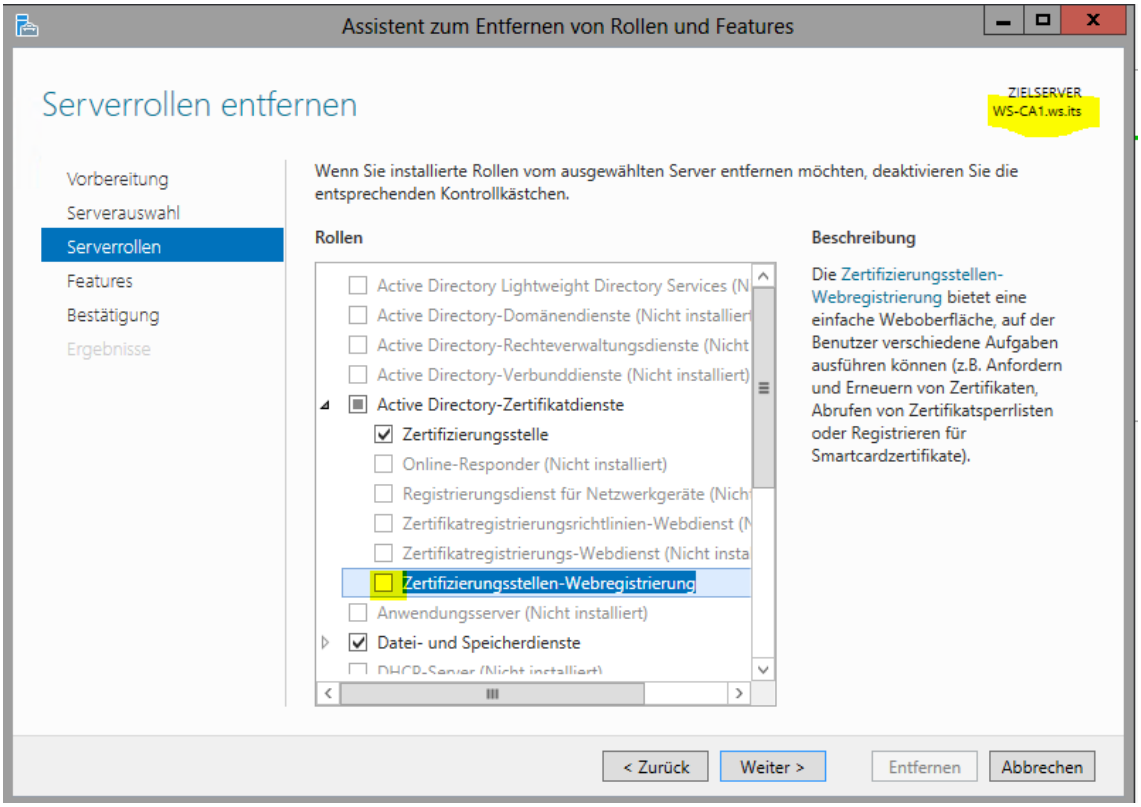


Alle Daten liegen nun auf dem alten Server unter C:\Admin. Da der Server gleich abgeschaltet wird, schiebe ich die Daten auf ein AdminShare:

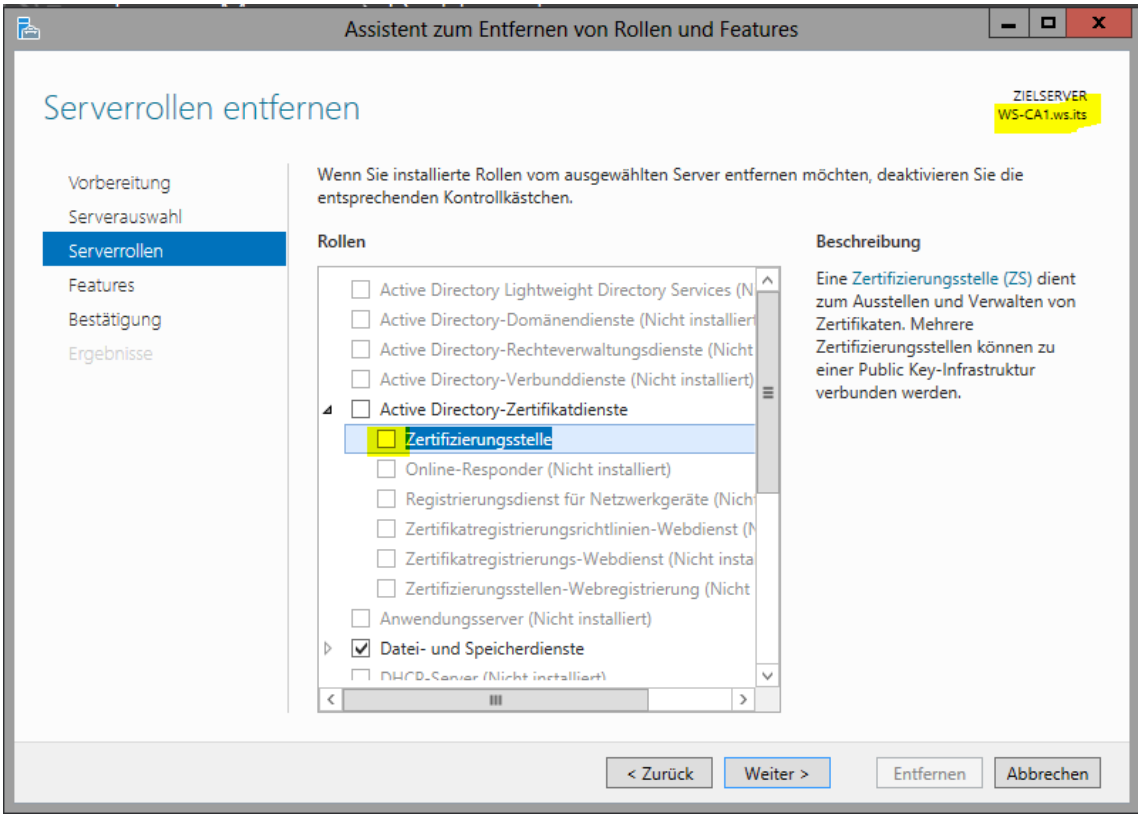


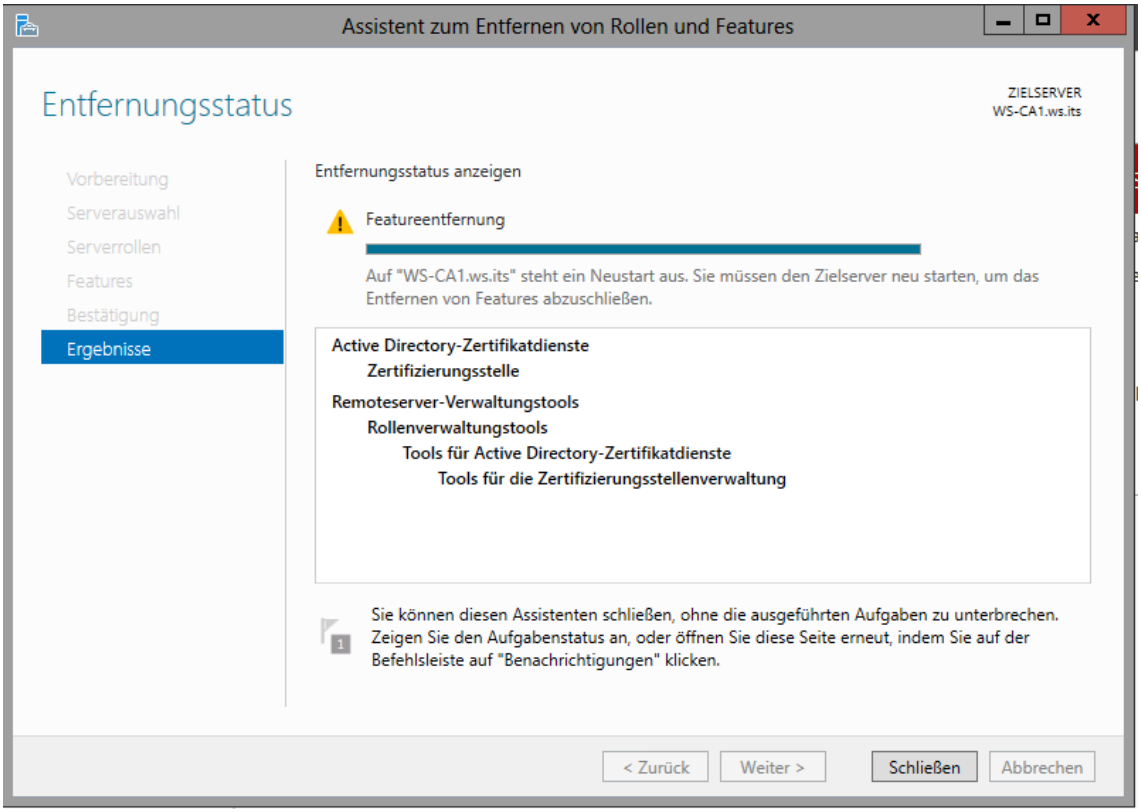
Entfernen des alten CA-Servers

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:

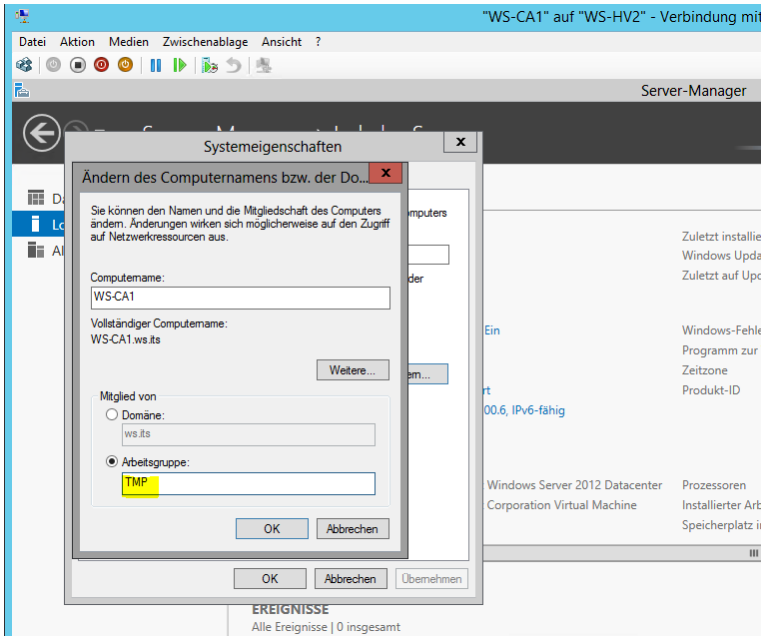


Jetzt kann die CA selbst deinstalliert werden:

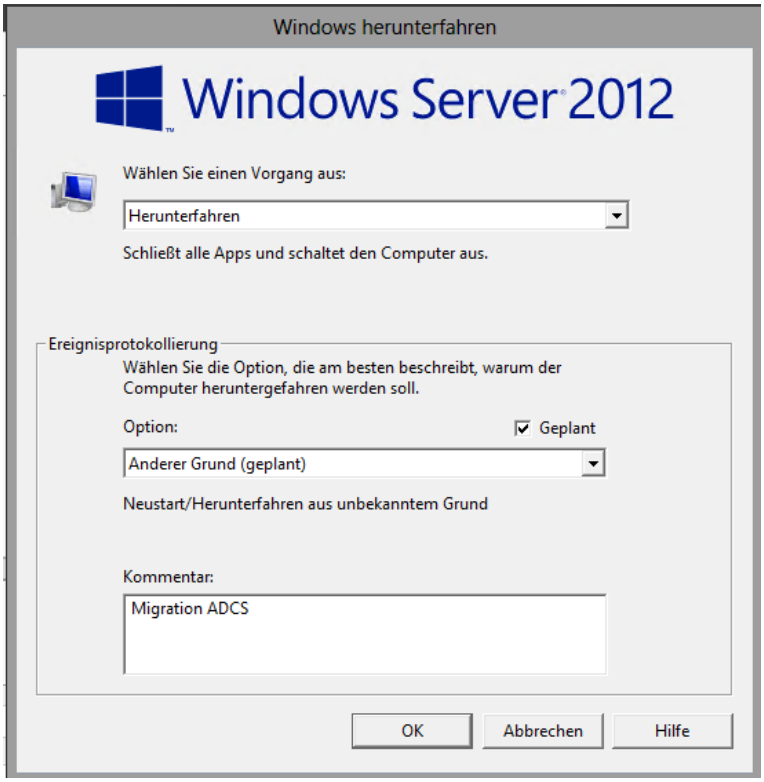




Nach dem Neustart kann der alte Server aus dem AD entfernt werden:



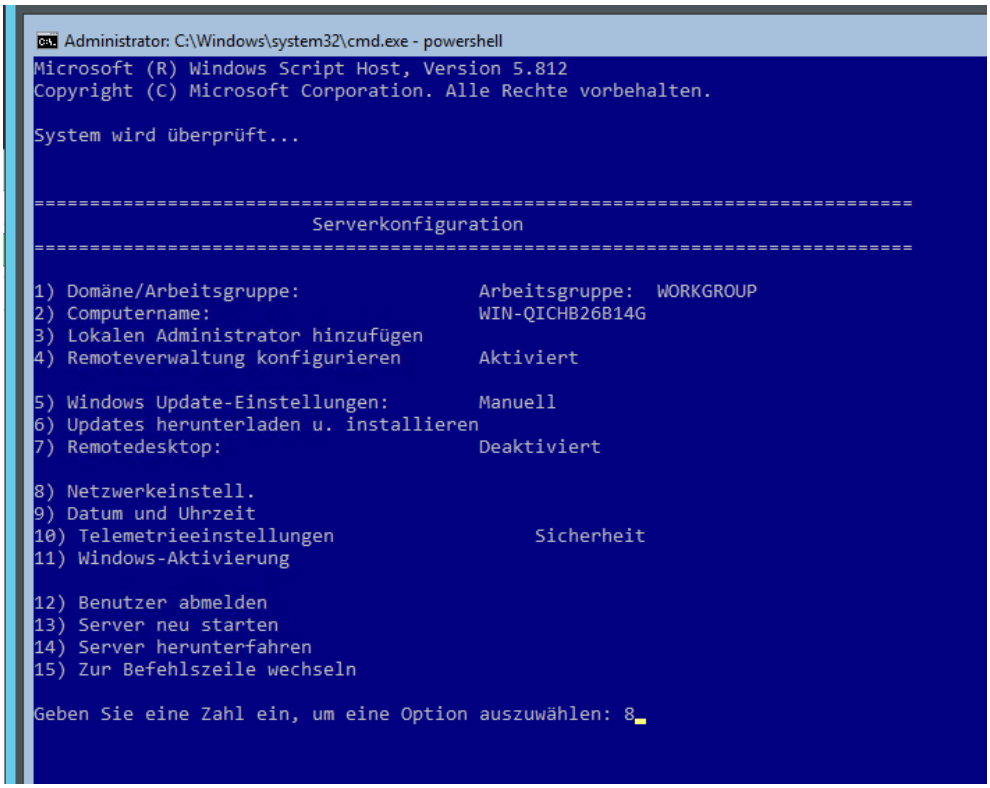
Ein Neustart ist nicht notwendig. Der alte CA-Server kann abgeschaltet werden:

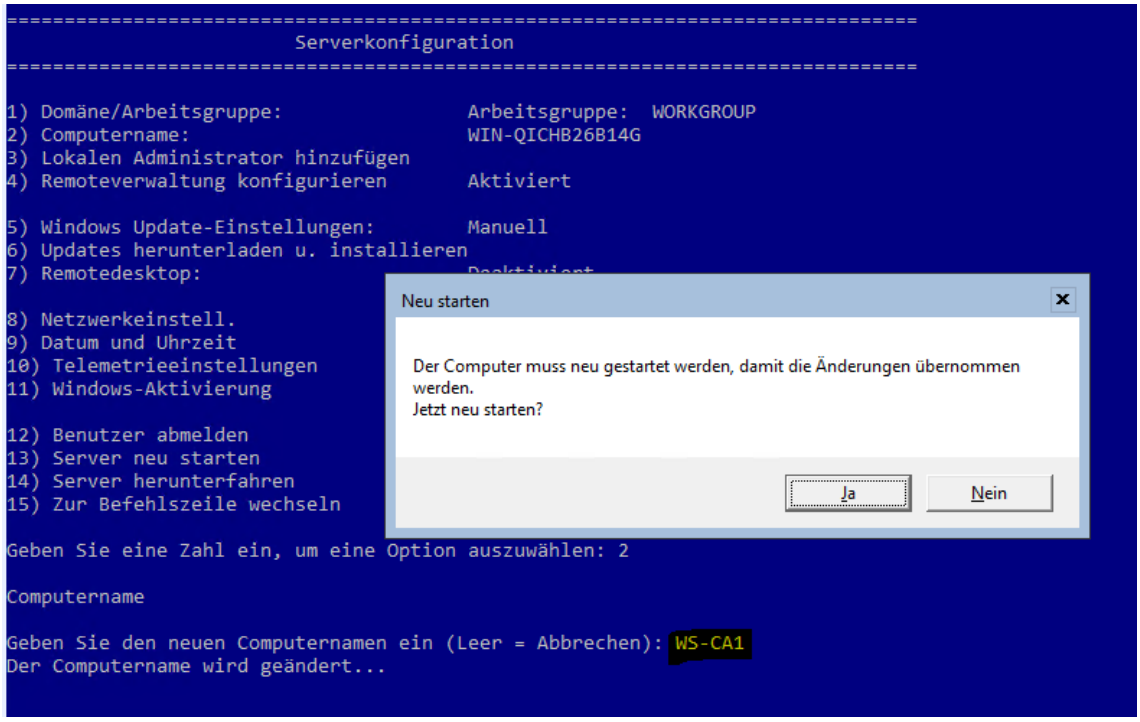


3. Auf dem neuen Server

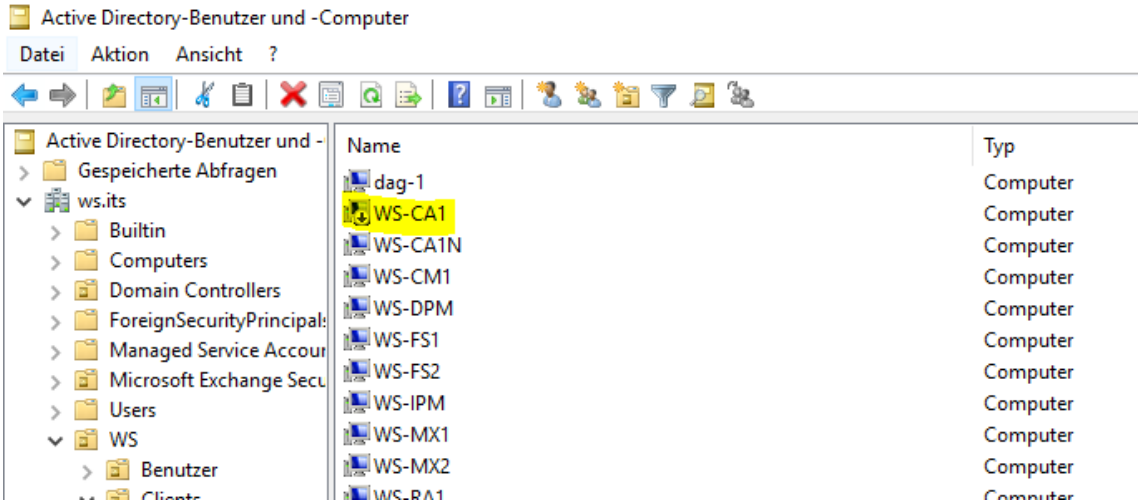
Aufbau des neuen Servers

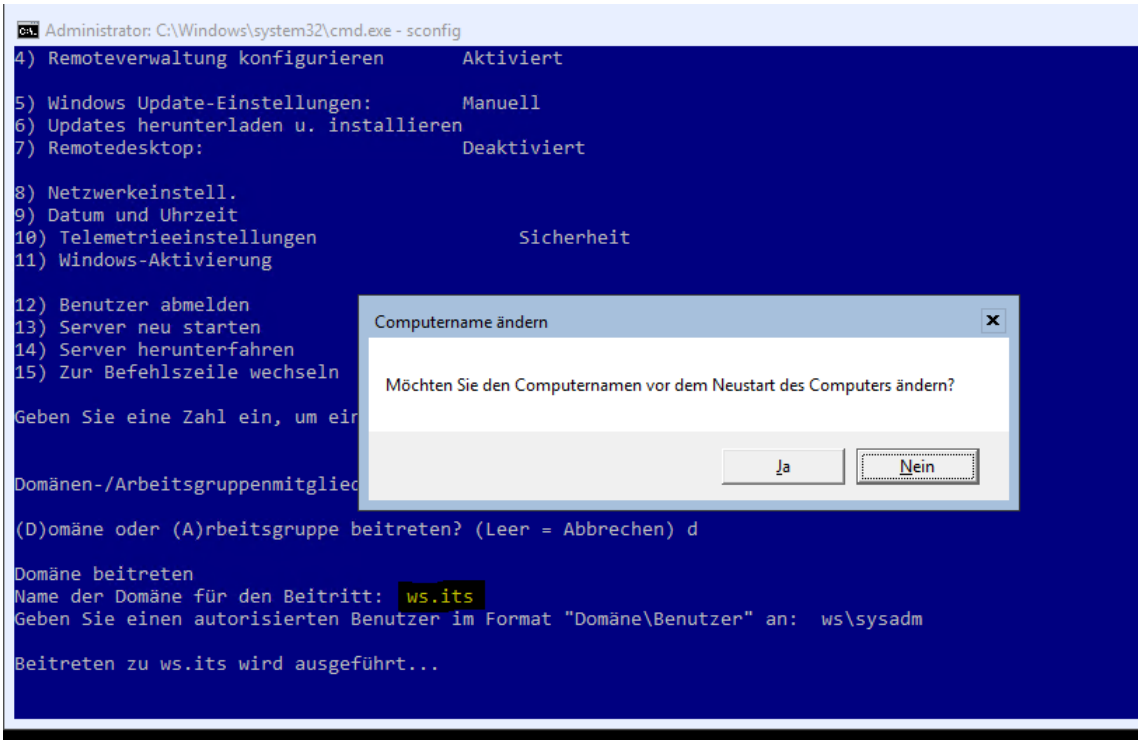
Der neue Server ist als Core-Server bereitgestellt worden. Zunächst sind die üblichen Aufgaben (IP-Konfiguration, Server benennen und DomainJoin) erforderlich:



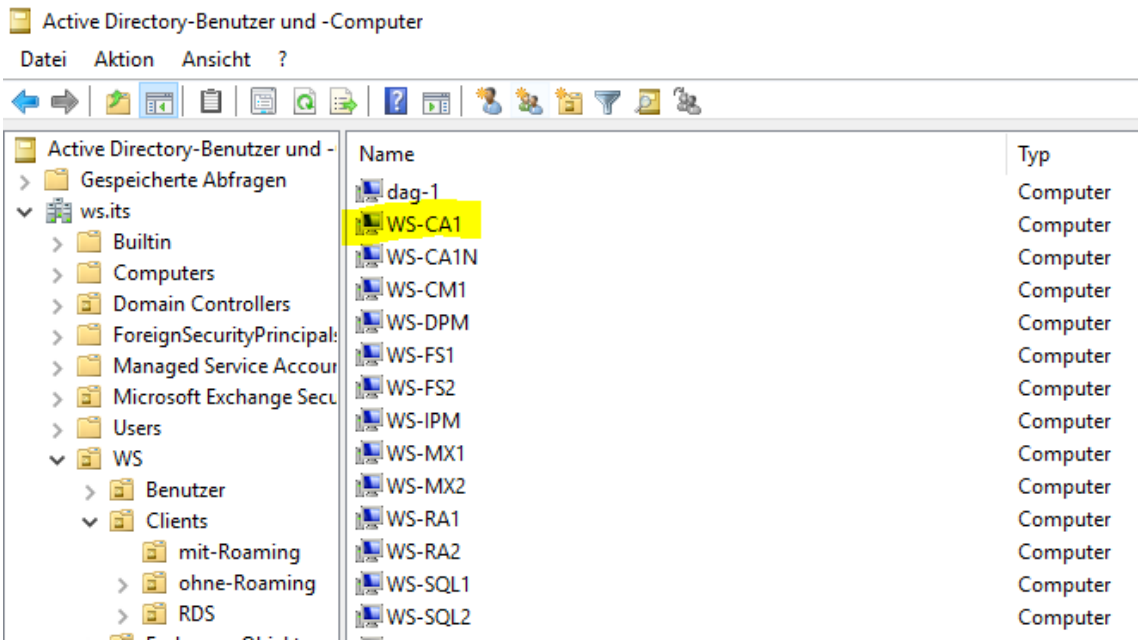


Das AD-Konto des alten Servers ist jetzt wieder frei:

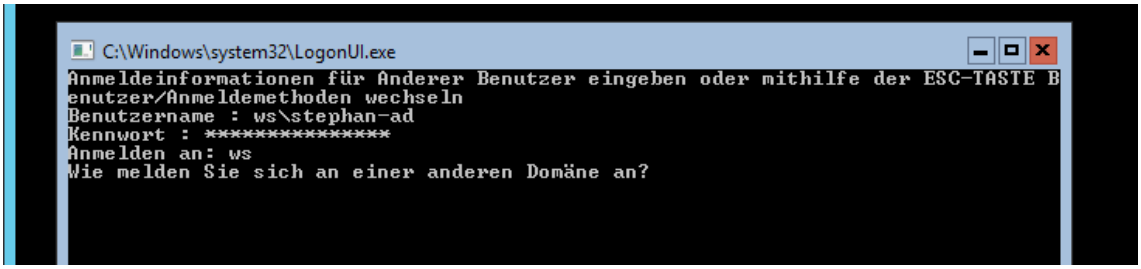




Nach dem DomainJoin ist das Konto wieder belegt:

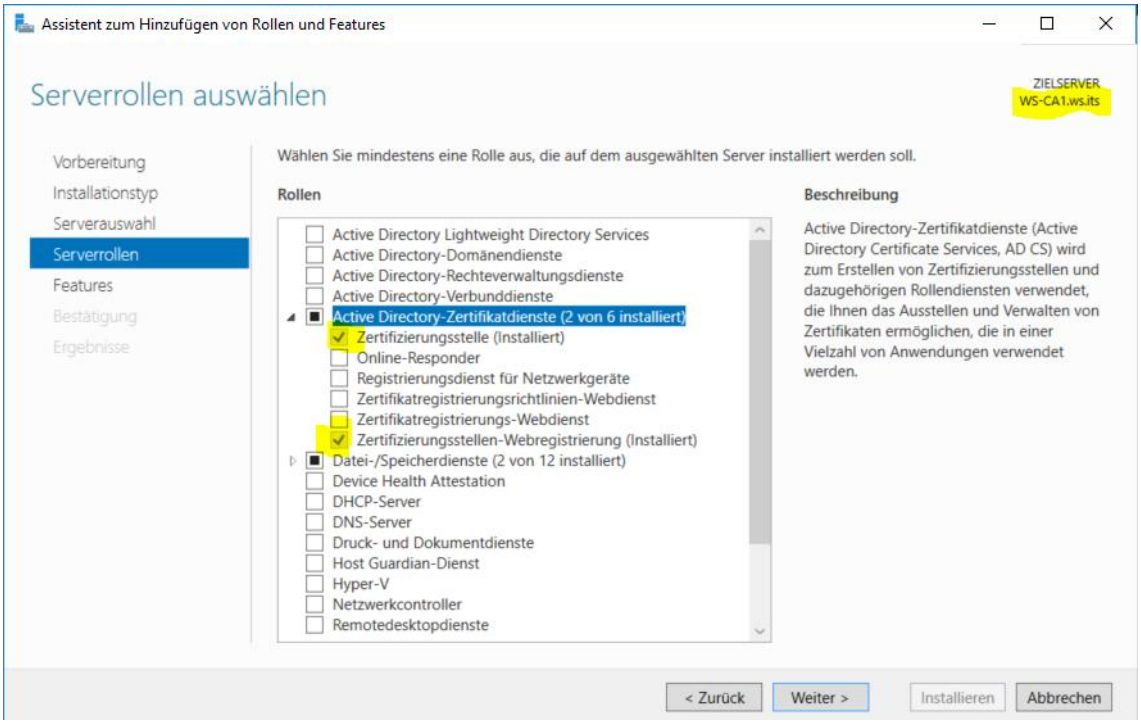


Der Anmelde-Account benötigt ausreichend Rechte:

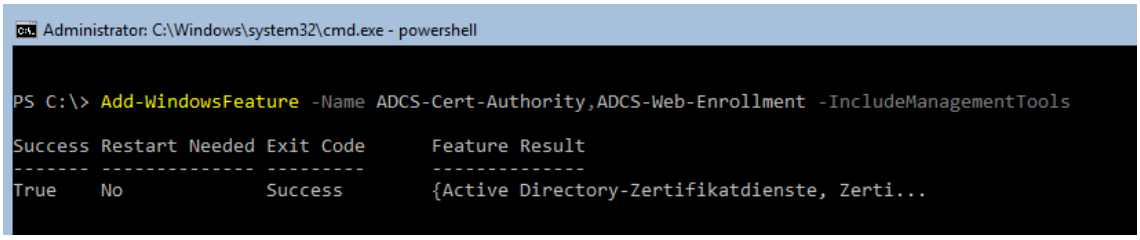


Installation der neuen CA

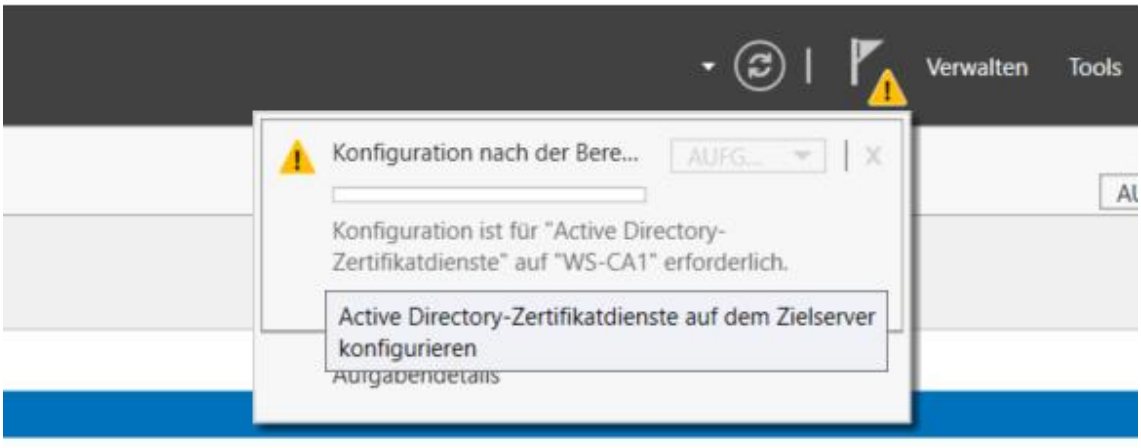
Jetzt kann die CA-Rolle installiert werden. Da der Server keine Management-Tools mehr hat kann entweder ein ServerManager eines kompatiblen Systems verwendet werden…



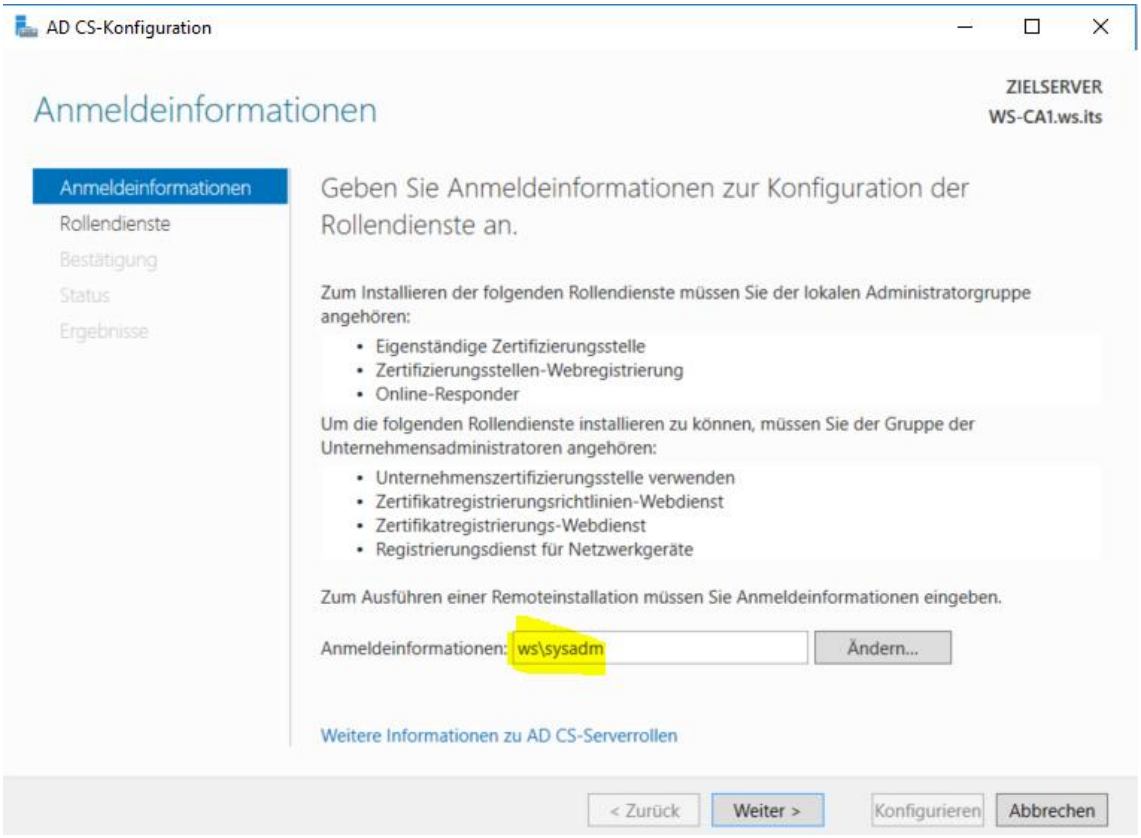
… oder man verwendet lokal die PowerShell:



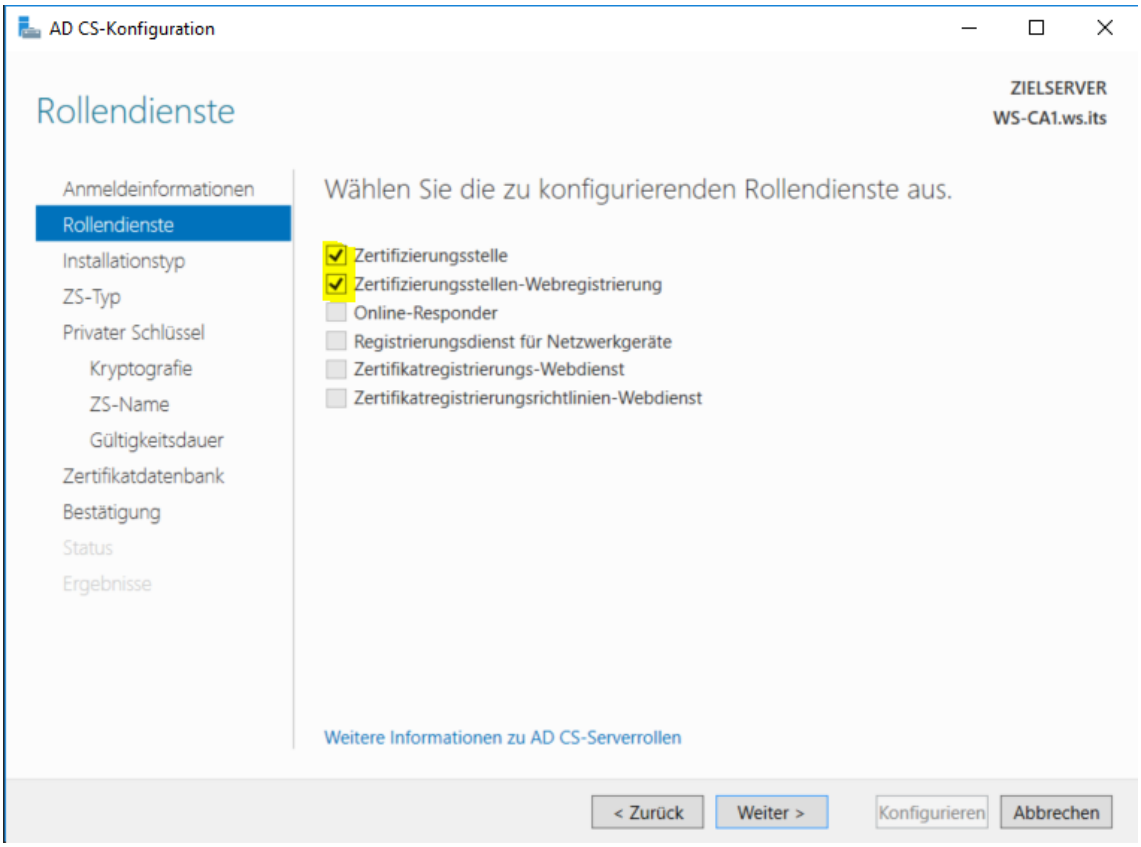
Mit dem Remote-Servermanager kann die Erstkonfiguration vorgenommen werden. Dabei wird eine neue CA mit dem alten Root-CA-Zertifikat aufgebaut:

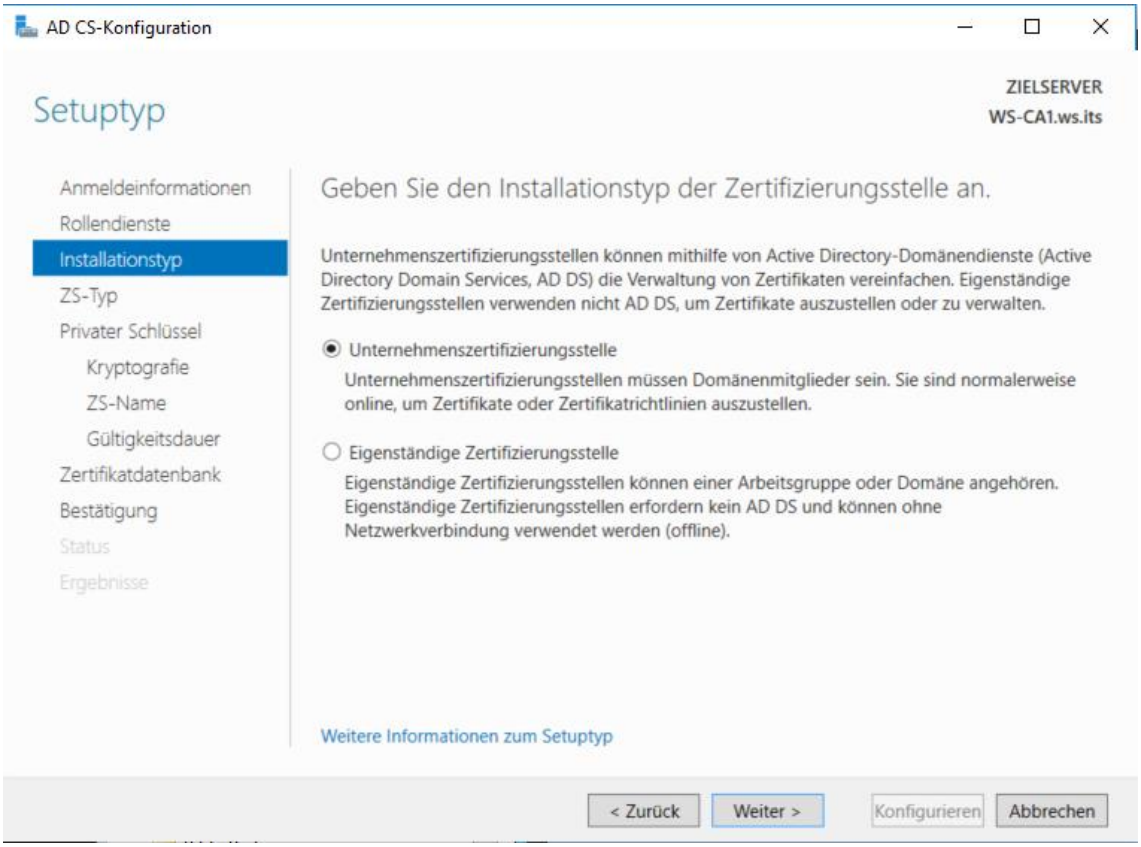


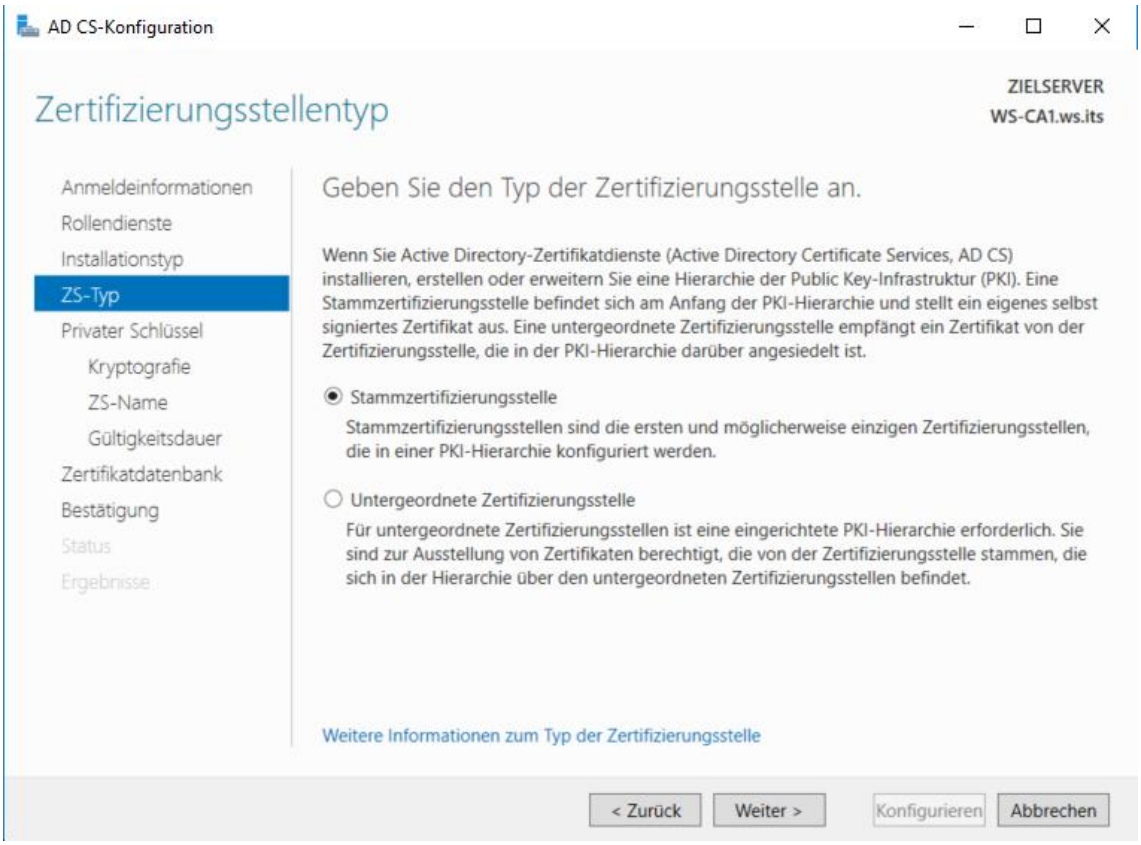
Es werden AD-Rechte benötigt:



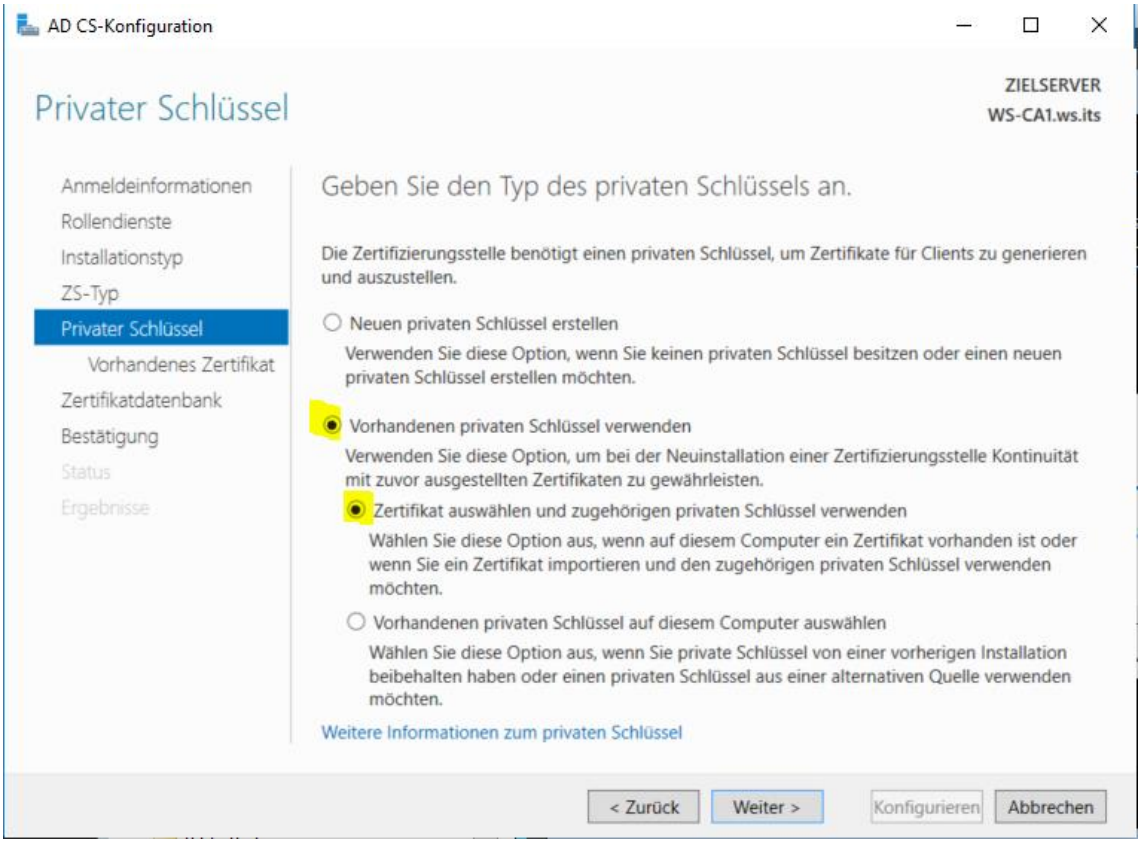
Es werden die beiden installierten Rollen vorbereitet:



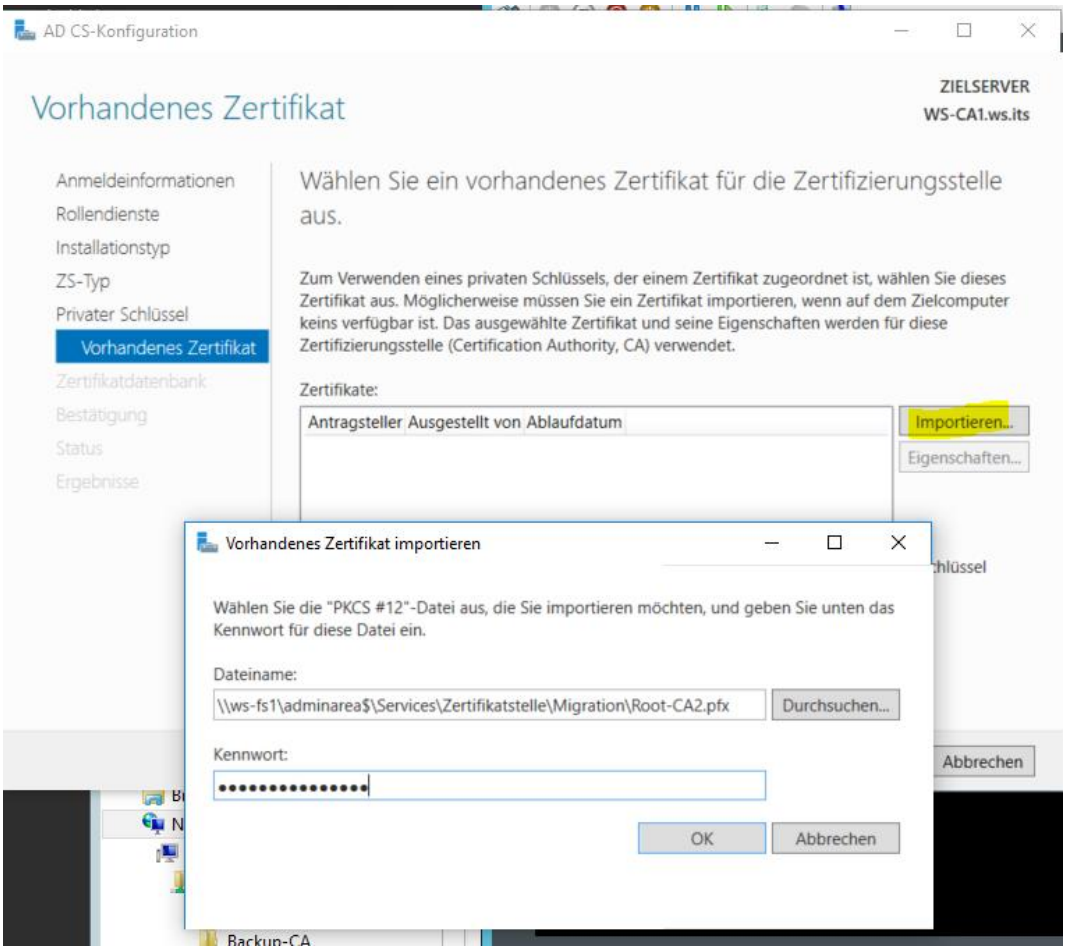




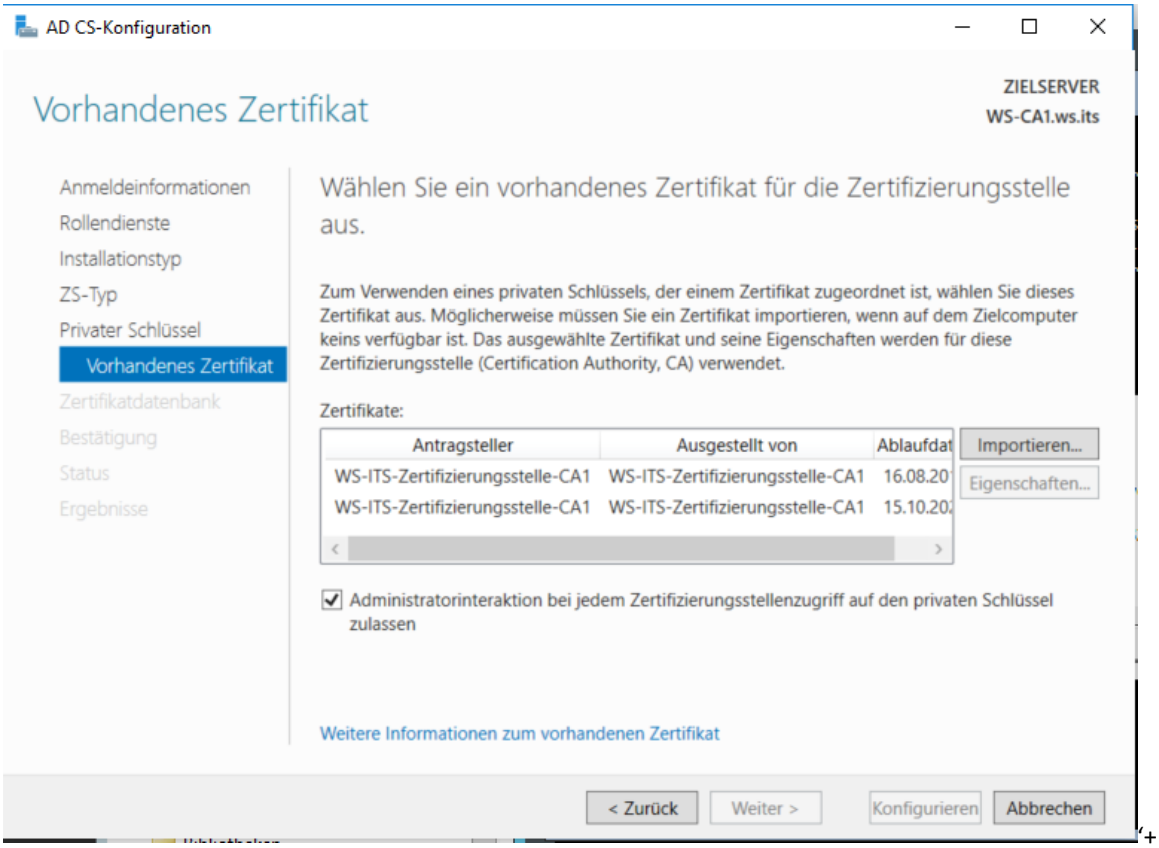
An dieser Stelle kann der Root-CA-Key der alten CA eingespielt werden:



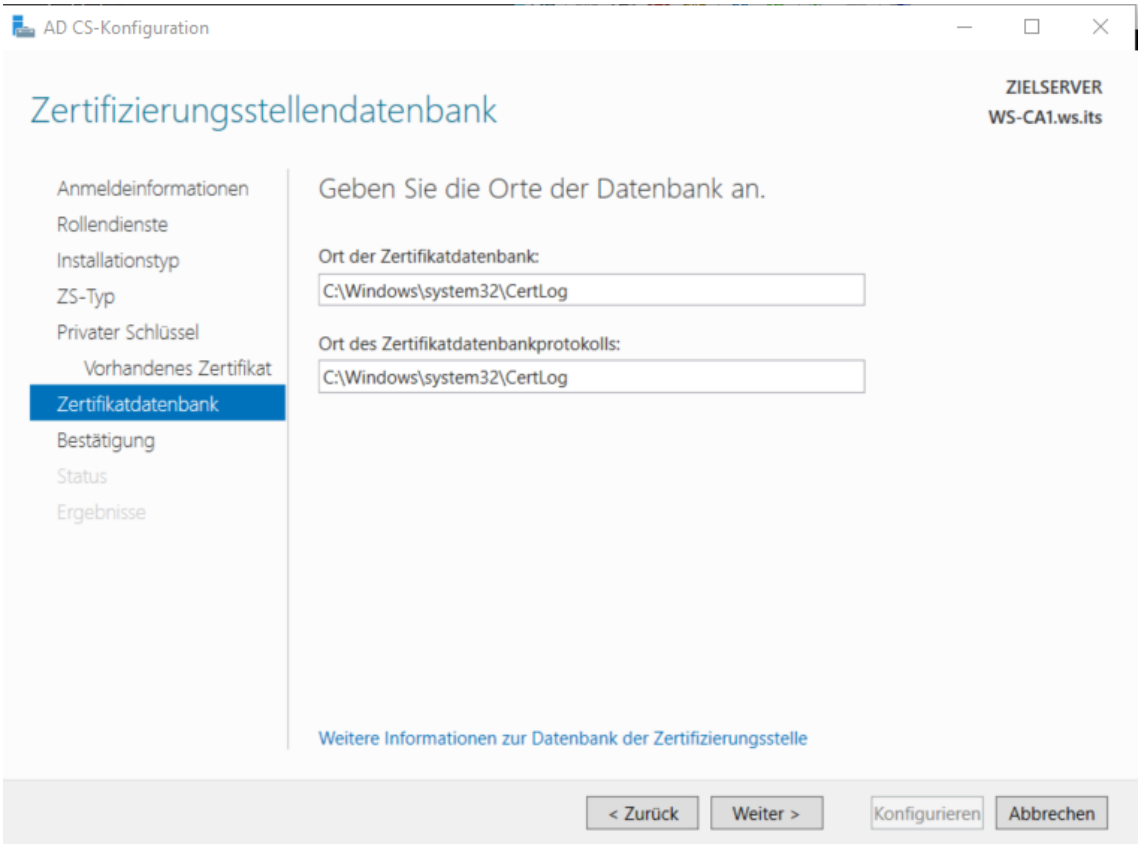
Das Zertifikat liegt im AdminShare:

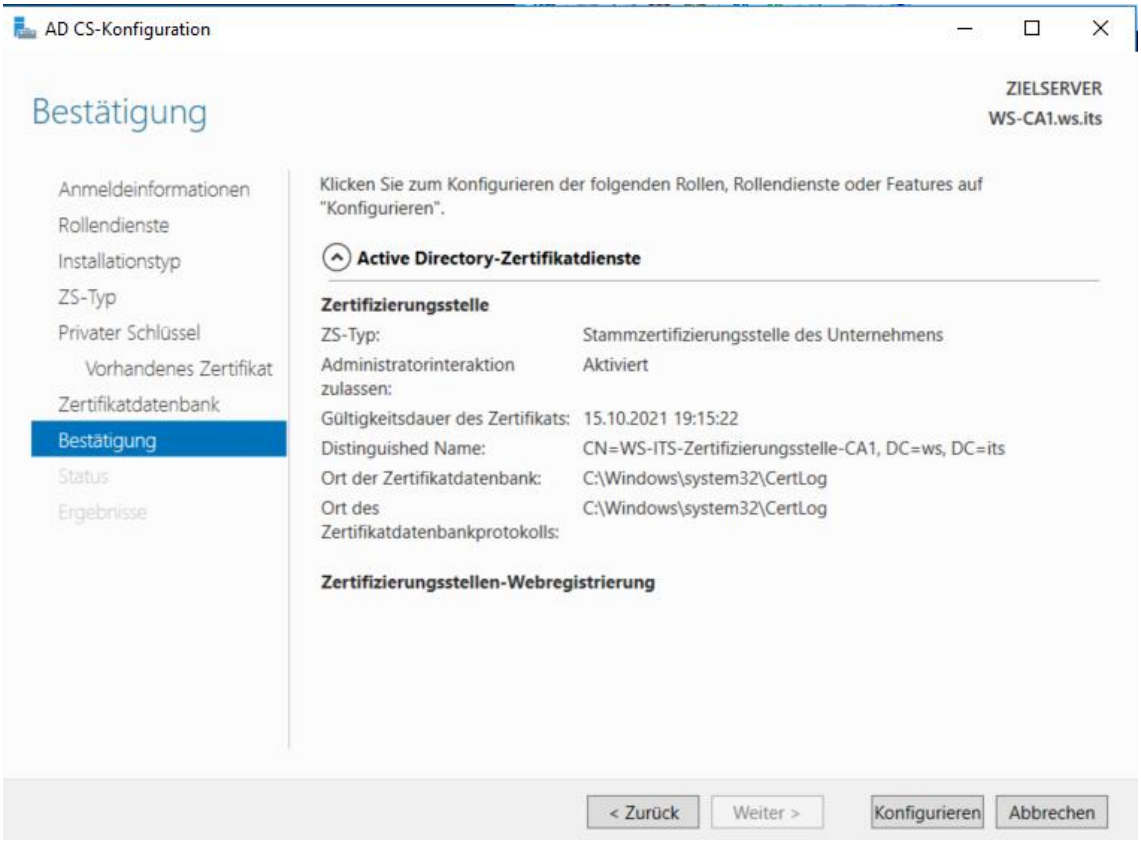


Es gab 2 alte Zertifikate. Beide werden eingespielt:

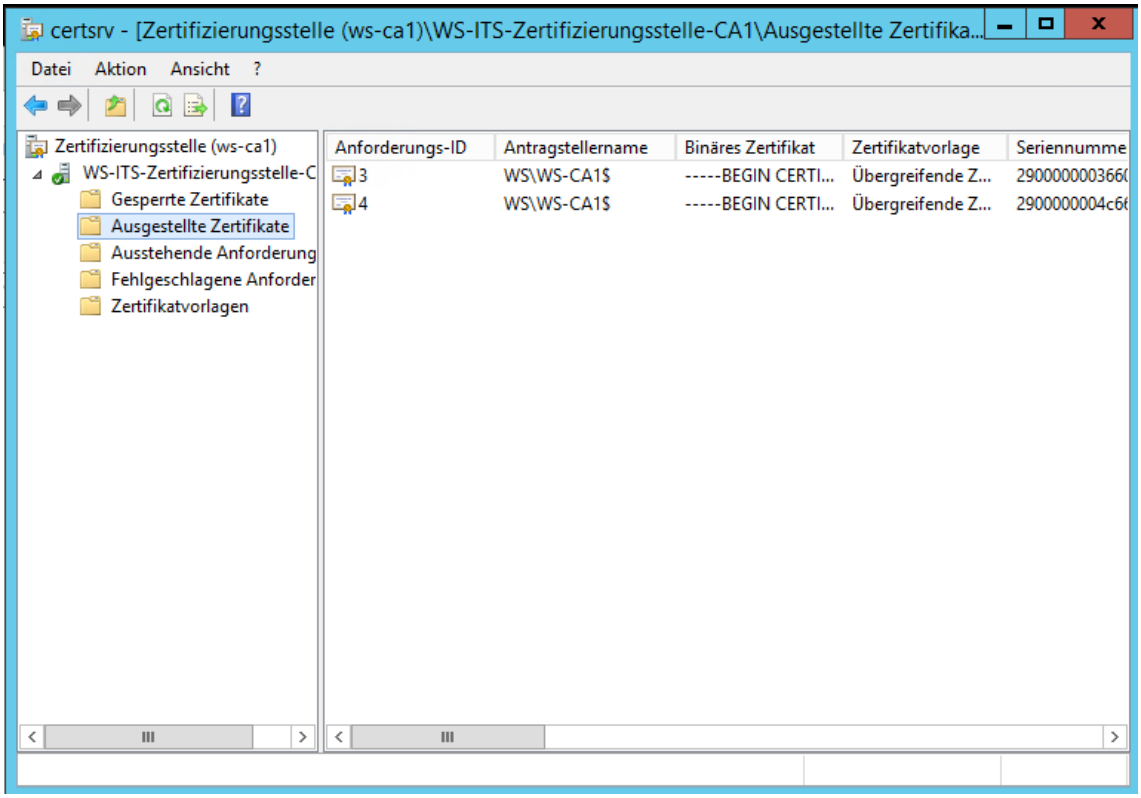


Die Pfade bleiben bestehen:



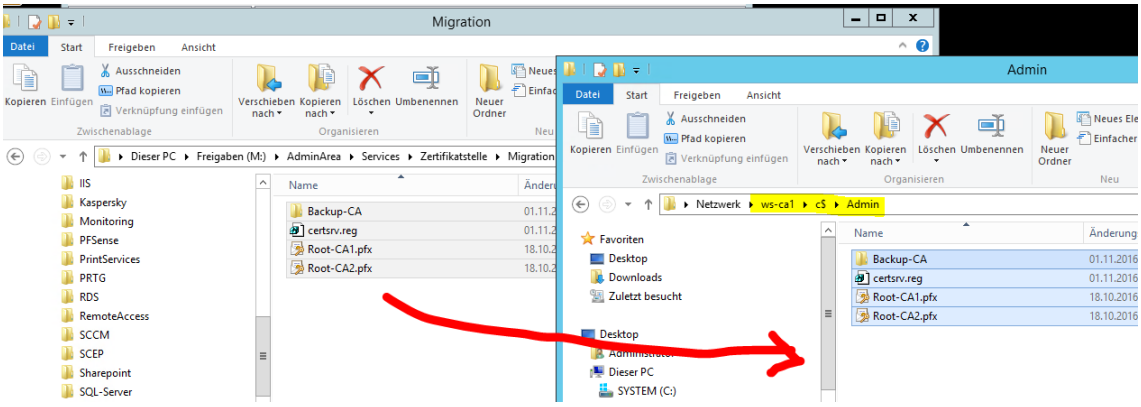


Das Ergebnis ist eine neue CA mit der alten Identität:

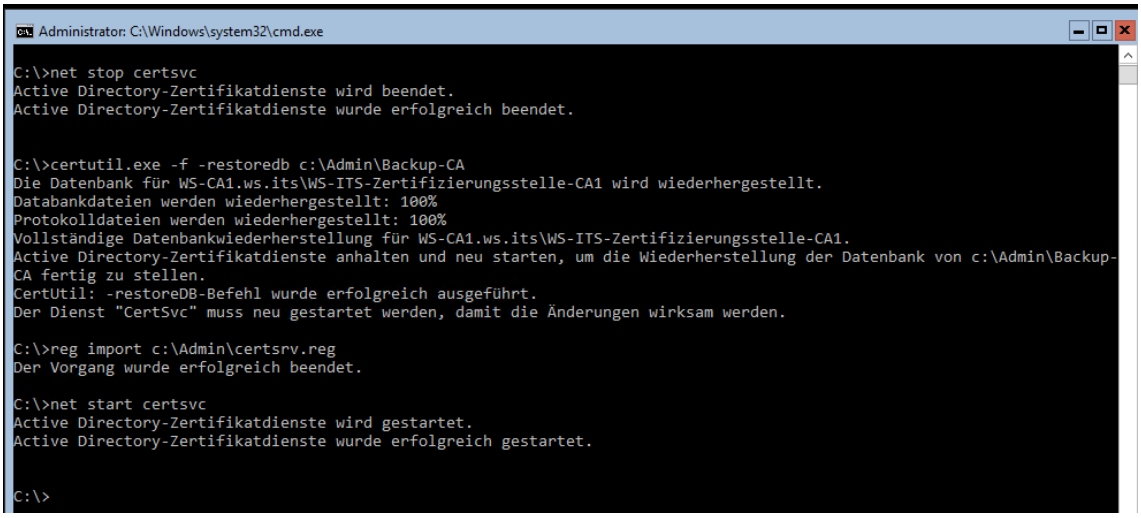


Import der alten DB und der Konfiguration

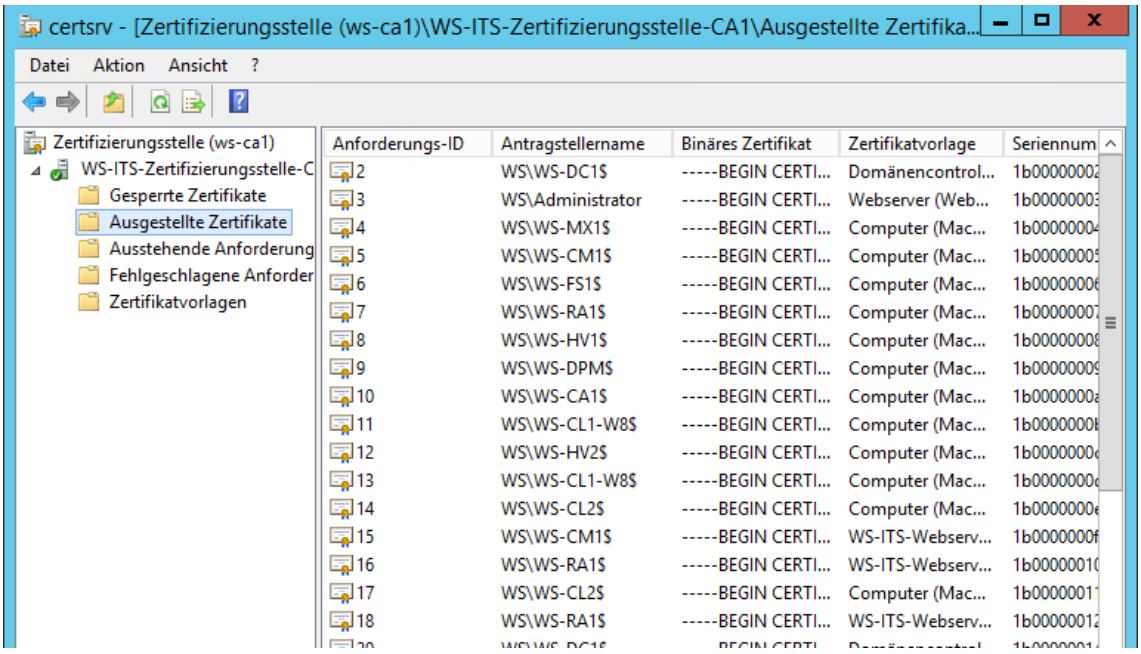
Zuerst kopiere ich die exportierten Daten auf den neuen Server:



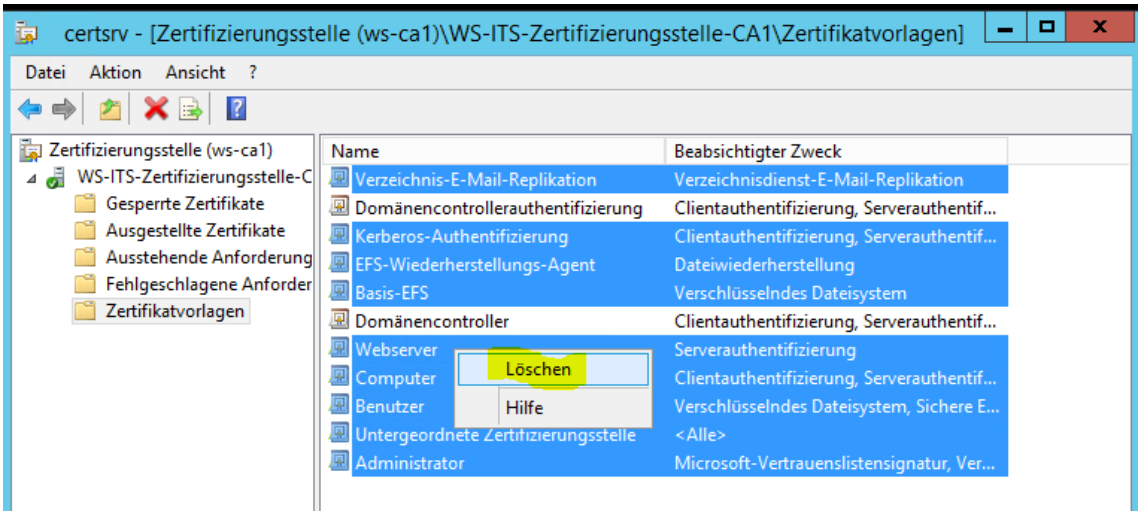
Mangels GUI-Tools verwende ich die cmd für den Import der CA-Datensicherung und der Service-Registry. Der Dienst der CA muss dafür natürlich aus sein:



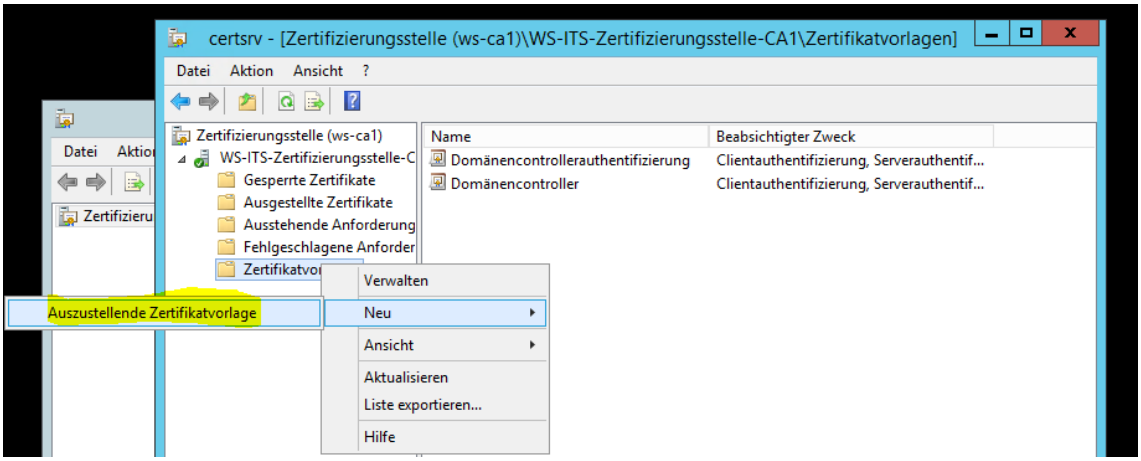
Das Ergebnis sind die alten Daten in der neuen CA:

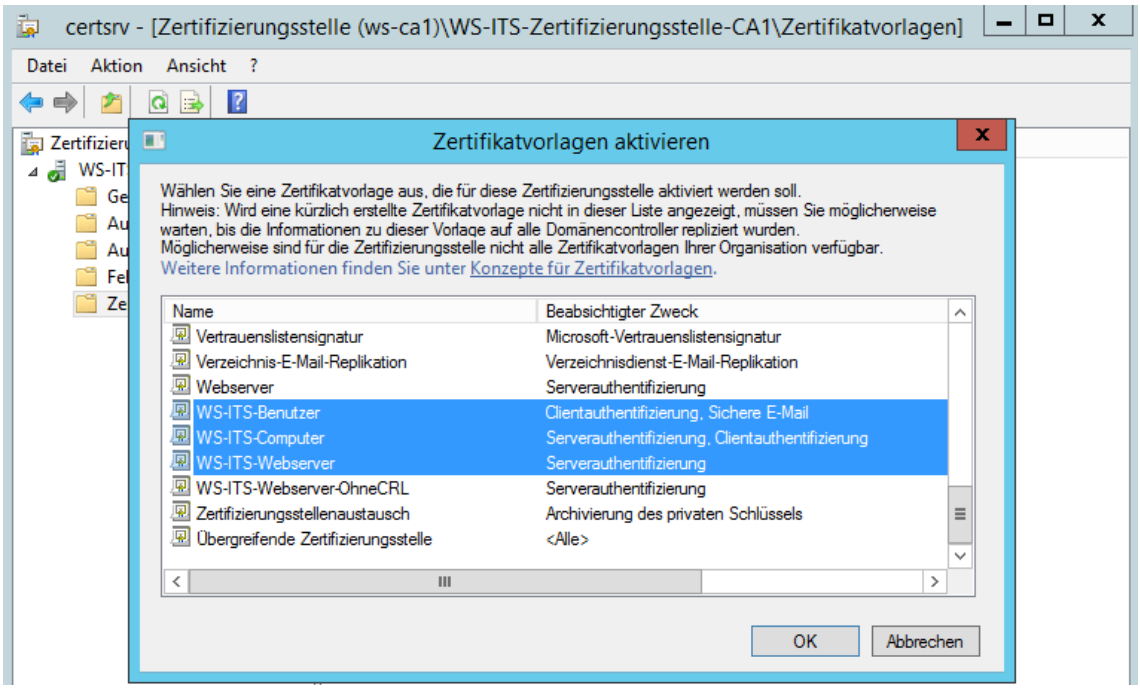


Jetzt fehlen noch die Vorlagen. Nicht verwendete Vorlagen entferne ich:



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





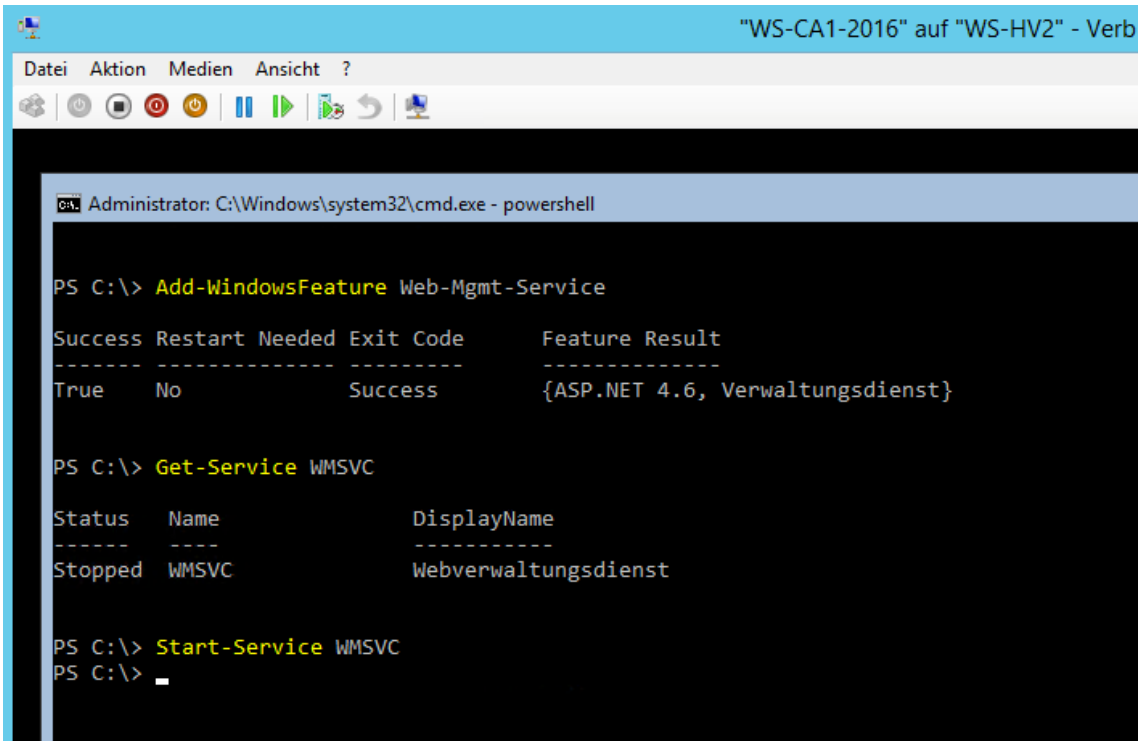
Absicherung der Web-Registrierungsstelle

Die Website ist nicht unter https erreichbar:

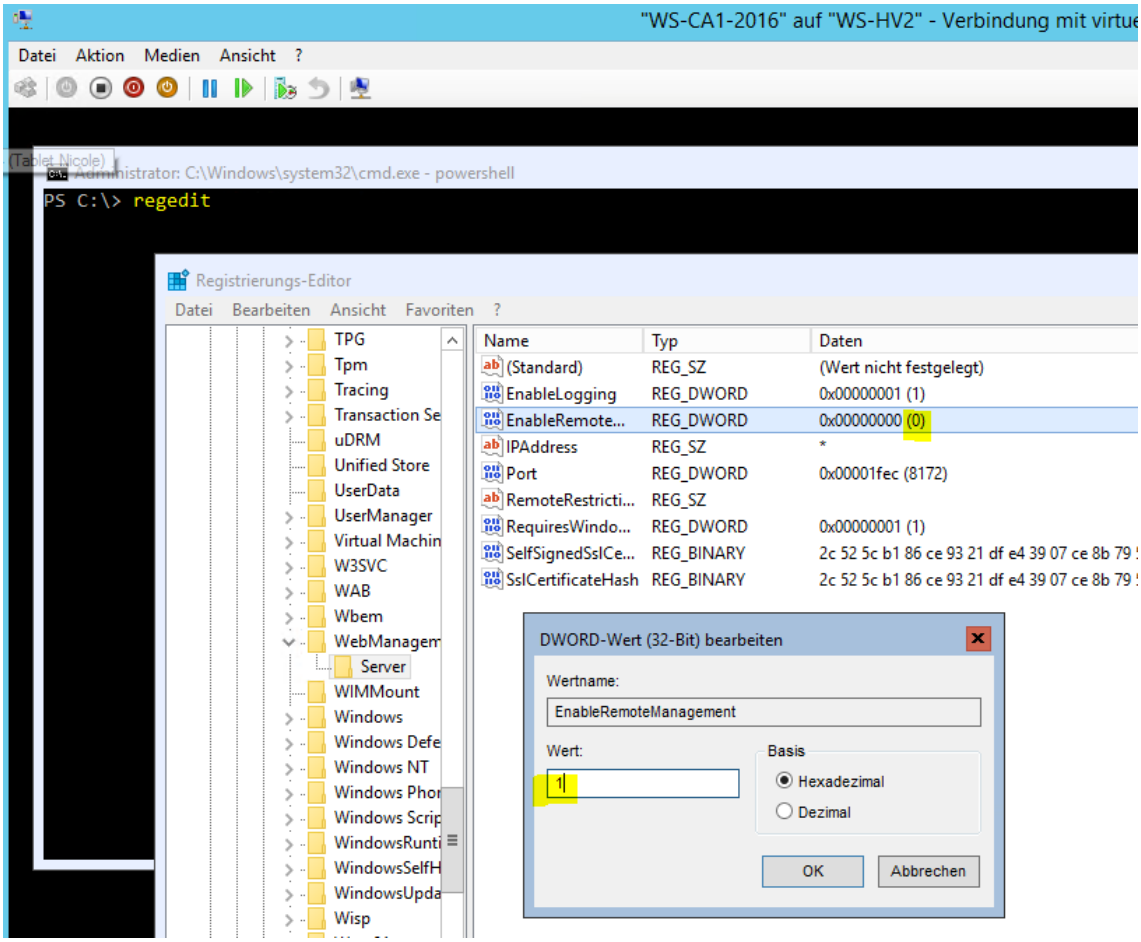
Die Seite kann nicht angezeigt werden.

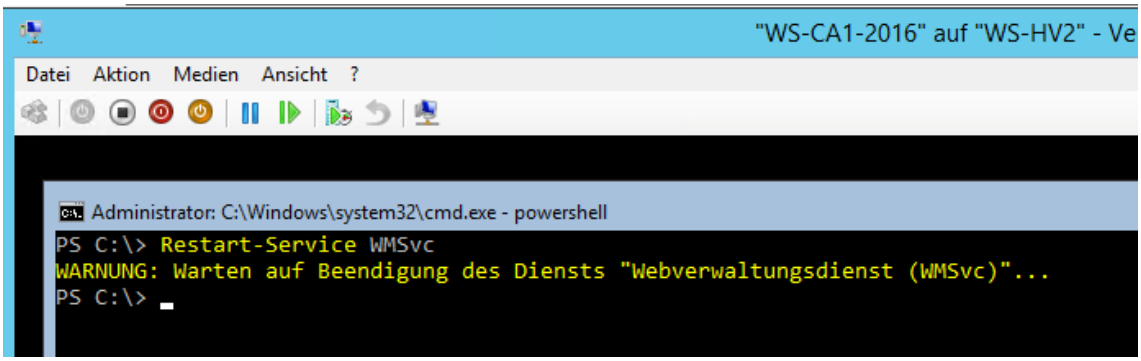
- Vergewissern Sie sich, dass die Webadresse https://ws-ca1.ws.its stimmt.
- Suchen Sie die Seite mit Ihrer Suchmaschine.
- Aktualisieren Sie die Seite in ein paar Minuten.

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

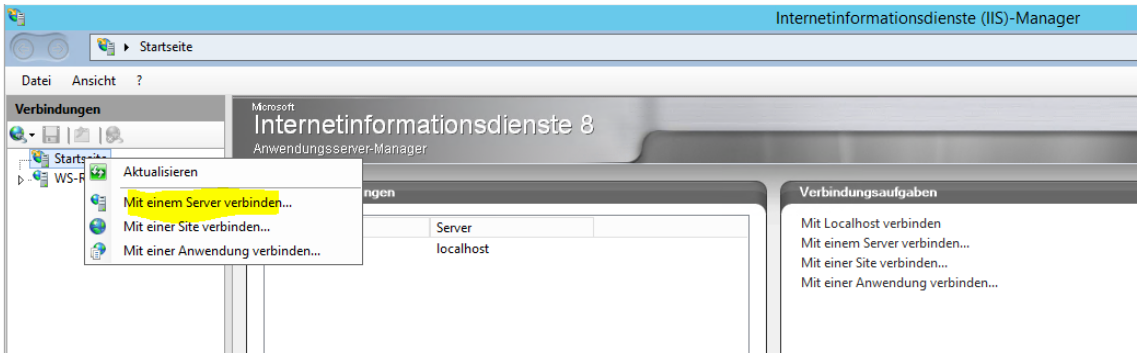


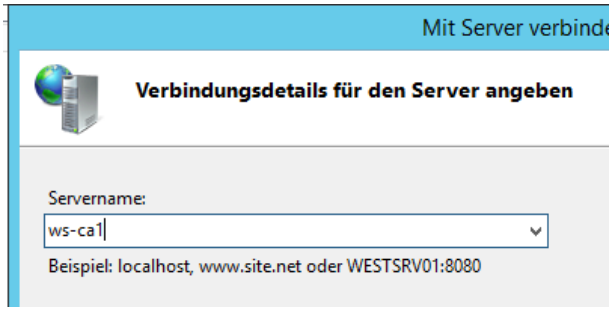
Die erforderliche Firewallausnahme setzt eine GPO. Dennoch ist eine Service-Konfiguration erforderlich:

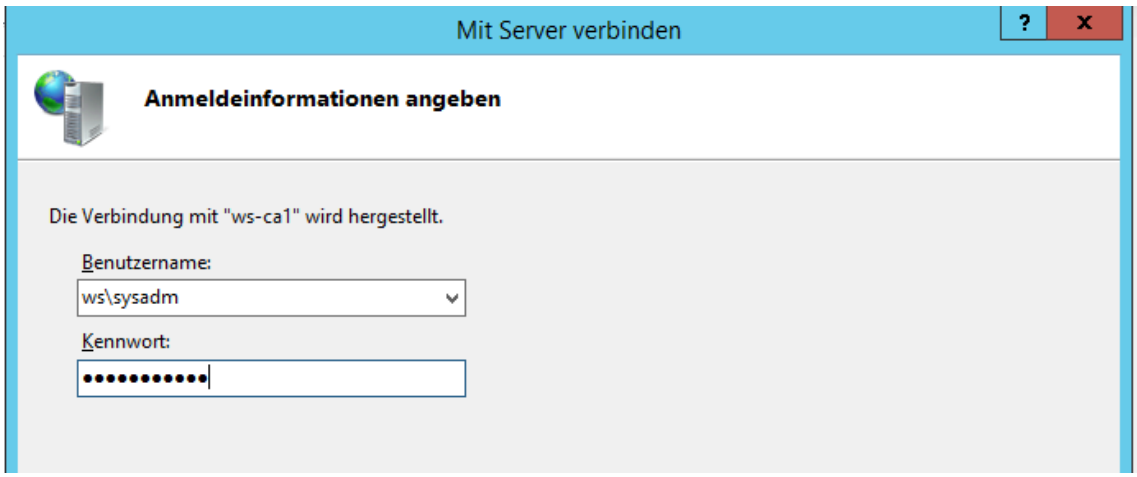




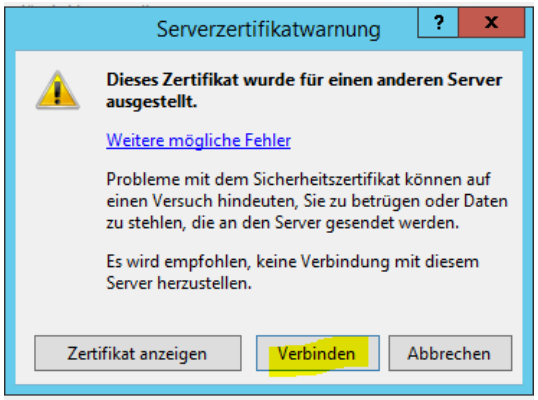
Von einem Server mit IIS-Management kann jetzt eine Verbindung hergestellt werden:



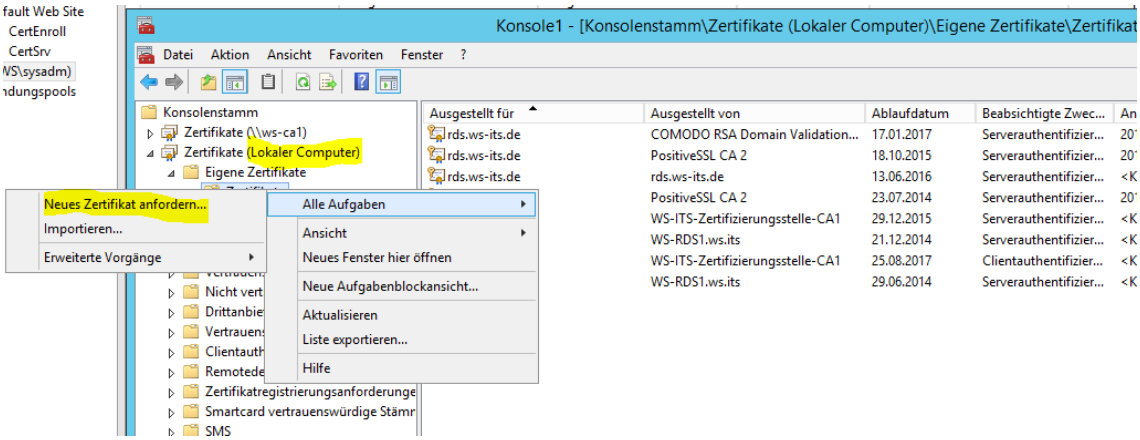


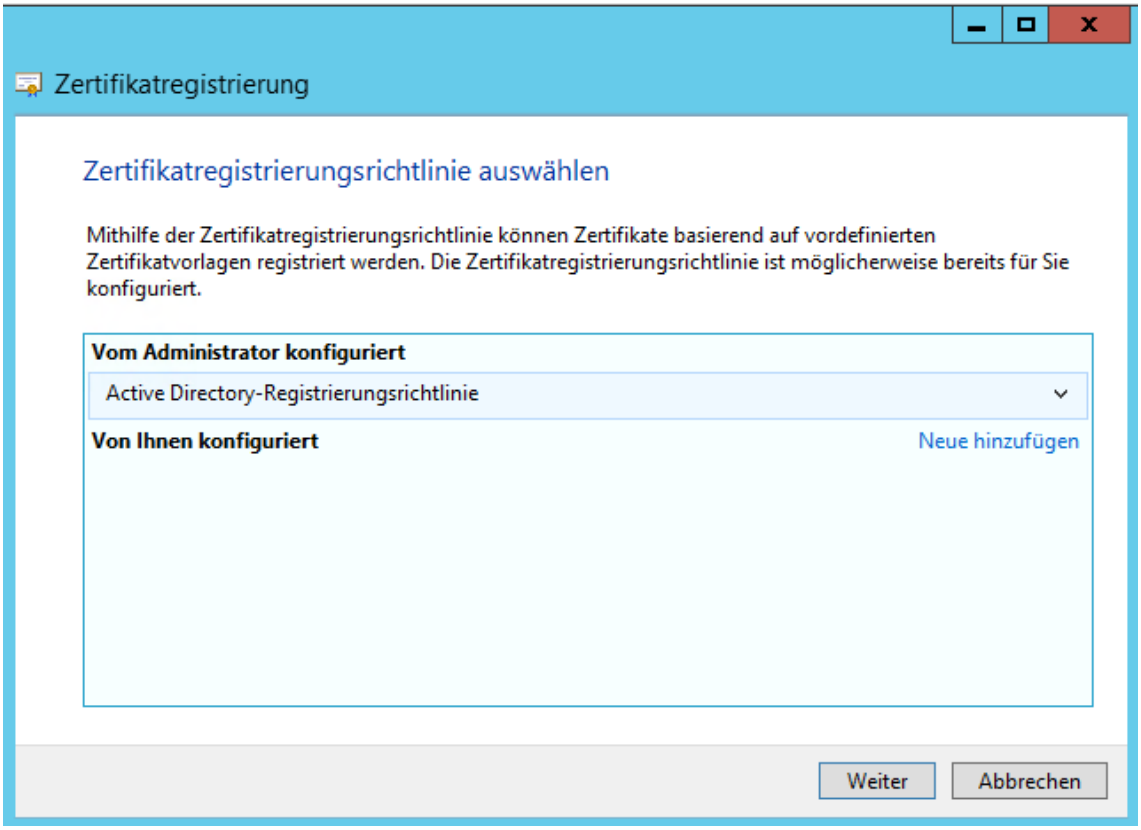


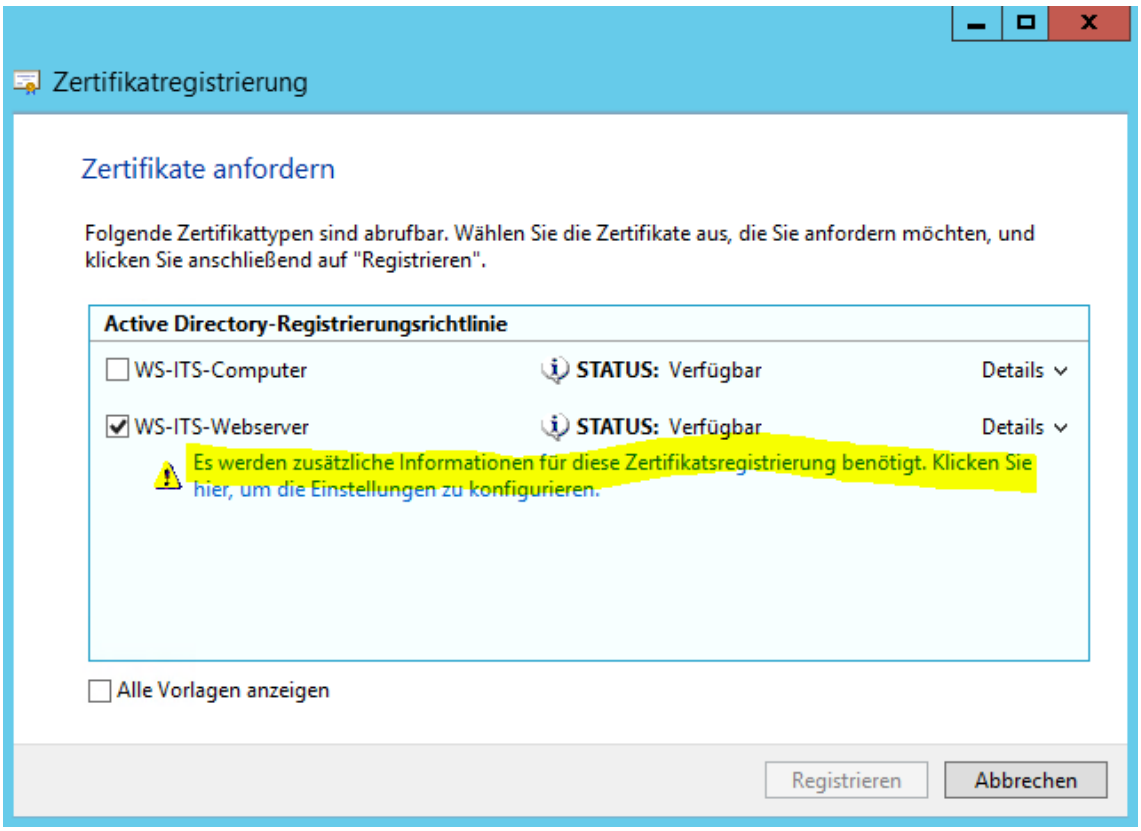
Natürlich passt das Zertifikat nicht…

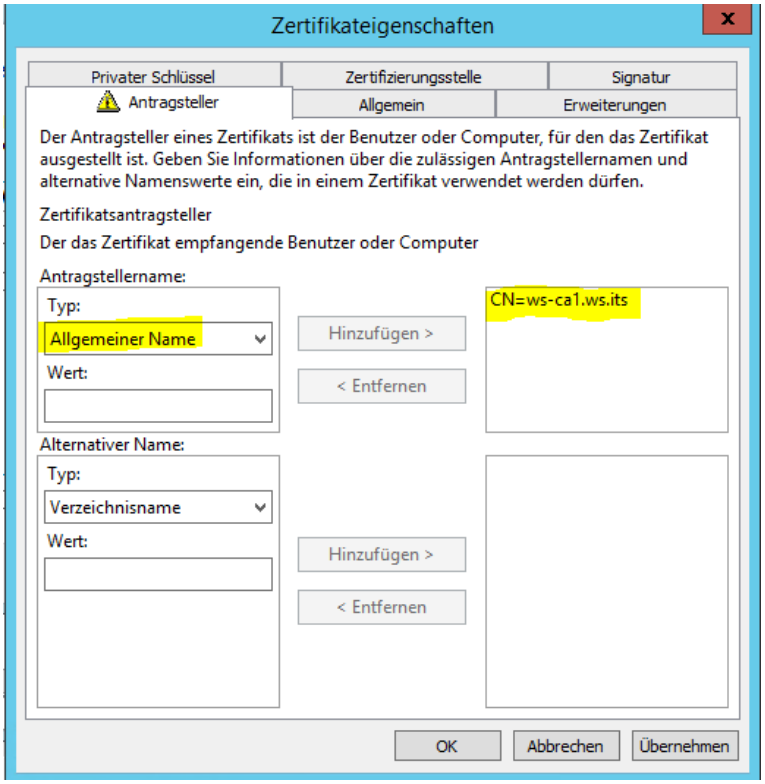


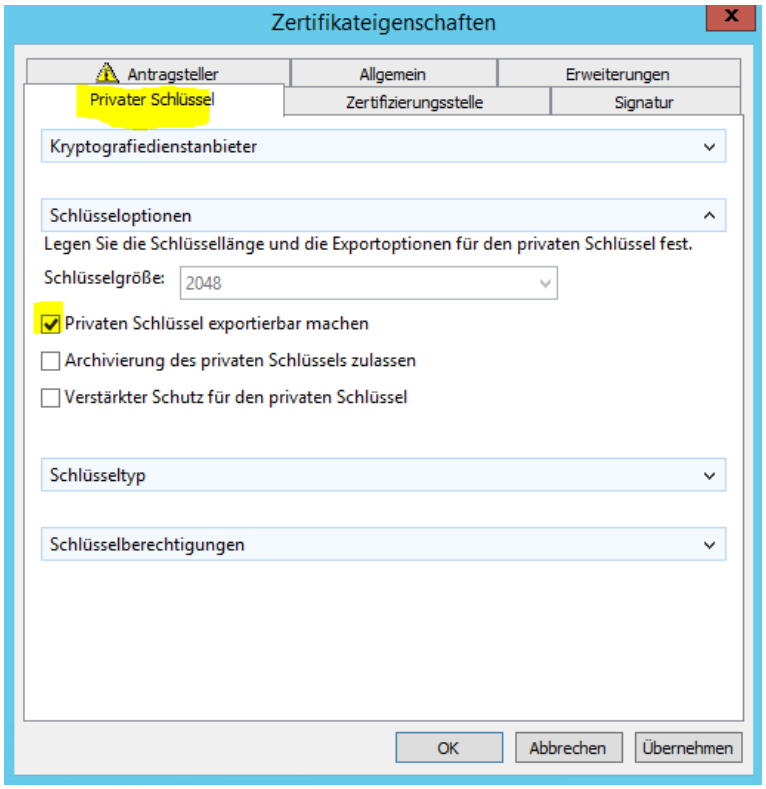
Die Verbindung steht. Aber es fehlt ein Webserver-Zertifikat. Dieses kann mit einer Zertifikate-MMC auf einem anderen Server angefordert werden. Sehr leicht geht das, indem man auf dem Management-Server ein Zertifikat mit dem richtigen Namen lokal anfordert, exportiert und dann auf dem Remote-Server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

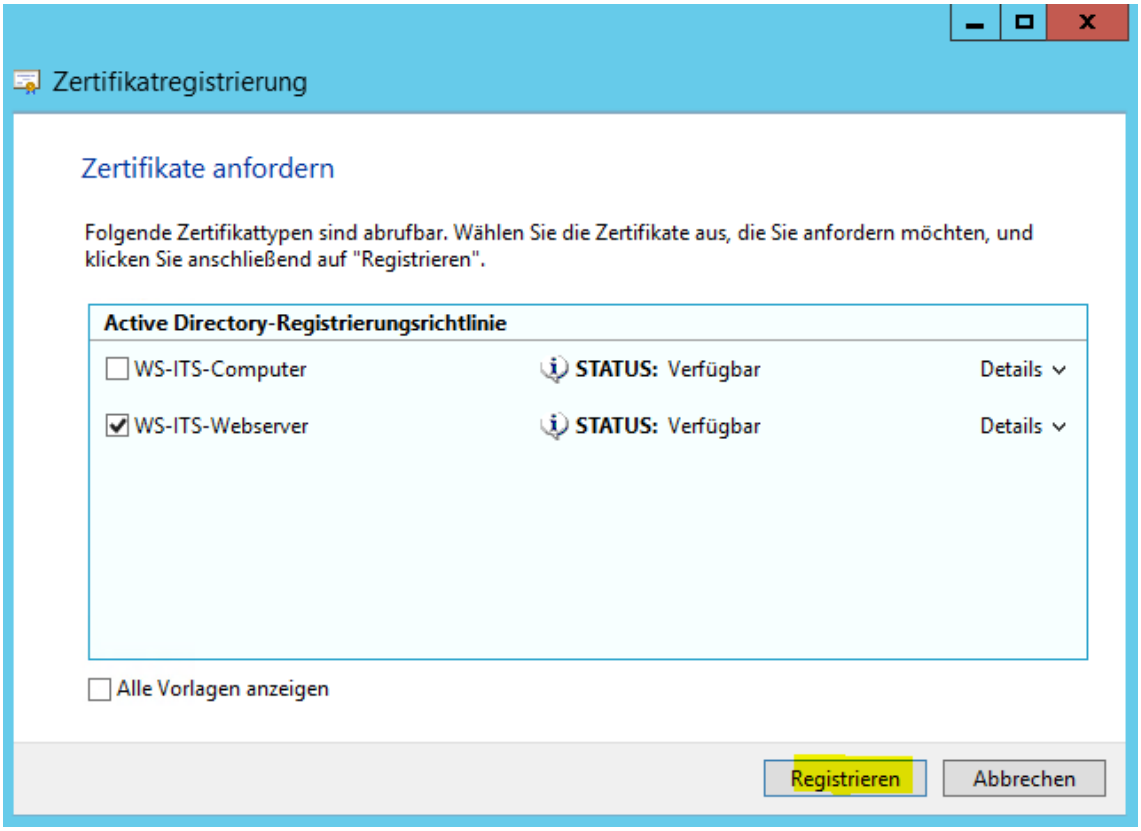


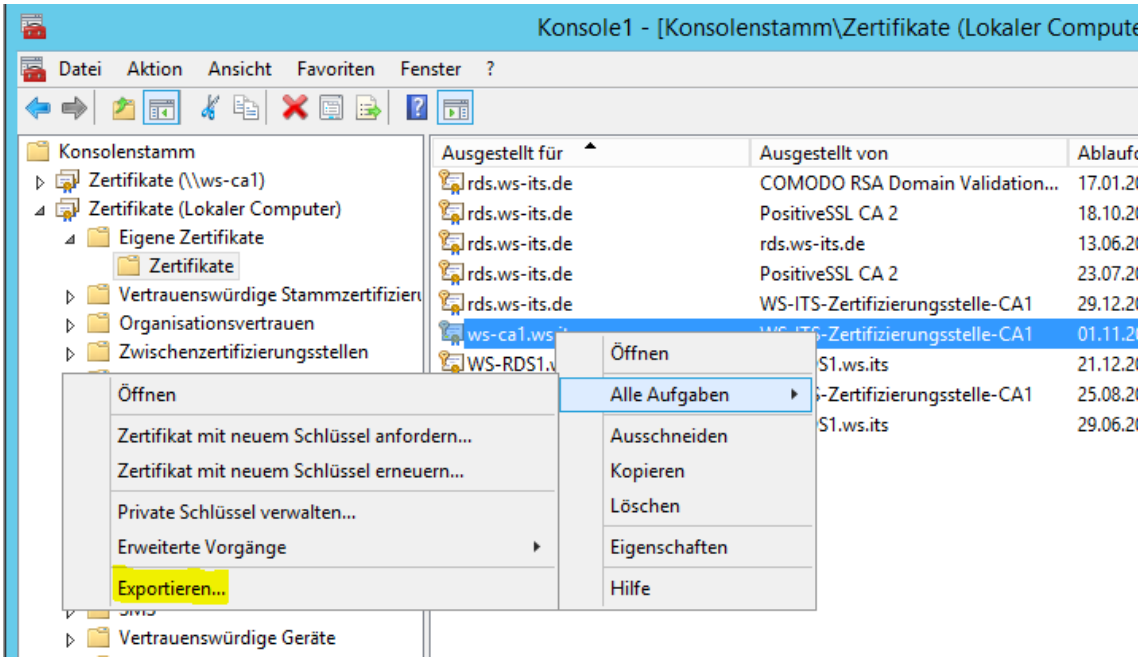

Zertifikatregistrierung
Zertifikatregistrierungsrichtlinie auswählen
Mithilfe der Zertifikatregistrierungsrichtlinie können Zertifikate basierend auf vordefinierten Zertifikatvorlagen registriert werden. Die Zertifikatregistrierungsrichtlinie ist möglicherweise bereits für Sie konfiguriert.
Vom Administrator konfiguriert
Active Directory-Registrierungsrichtlinie
Von Ihnen konfiguriert
Neue hinzufügen
Weiter
Abbrechen

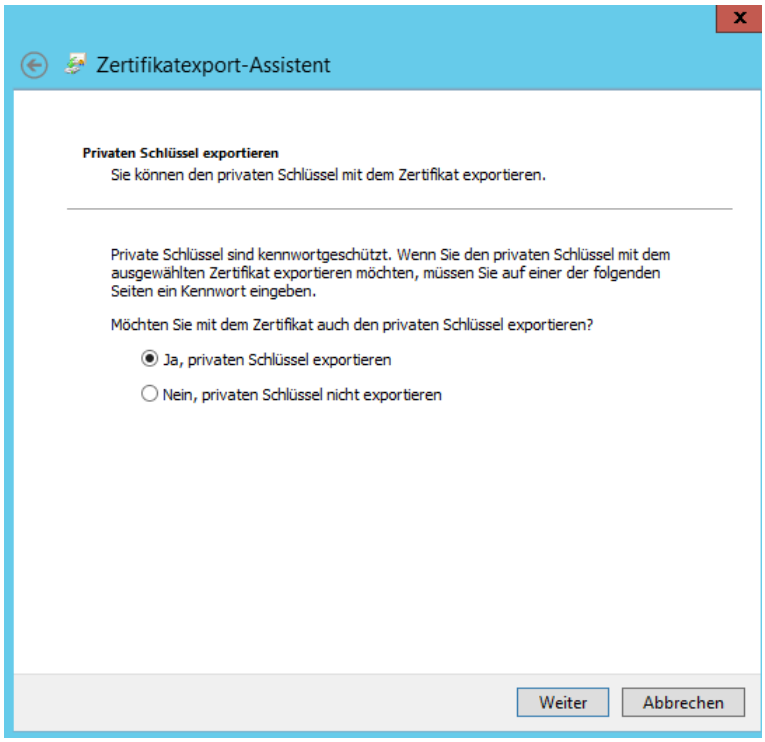

Zertifikatregistrierung
Zertifikate anfordern
Folgende Zertifikattypen sind abrufbar. Wählen Sie die Zertifikate aus, die Sie anfordern möchten, und klicken Sie anschließend auf "Registrieren".
Active Directory-Registrierungsrichtlinie
WS-ITS-Computer
STATUS: Verfügbar
Details
WS-ITS-Webserver
STATUS: Verfügbar
Details
Es werden zusätzliche Informationen für diese Zertifikatsregistrierung benötigt. Klicken Sie hier, um die Einstellungen zu konfigurieren.
Alle Vorlagen anzeigen
Registrieren
Abbrechen


Zertifikateigenschaften
Privater Schlüssel
Zertifizierungsstelle
Signatur
Antragsteller
Allgemein
Erweiterungen
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.
Zertifikatsantragsteller
Der das Zertifikat empfangende Benutzer oder Computer
Antragstellername:
Typ:
Allgemeiner Name
Wert:
Hinzufügen >
< Entfernen
CN=ws-ca1.ws.its
Alternativer Name:
Typ:
Verzeichnisname
Wert:
Hinzufügen >
< Entfernen
OK
Abbrechen
Übernehmen

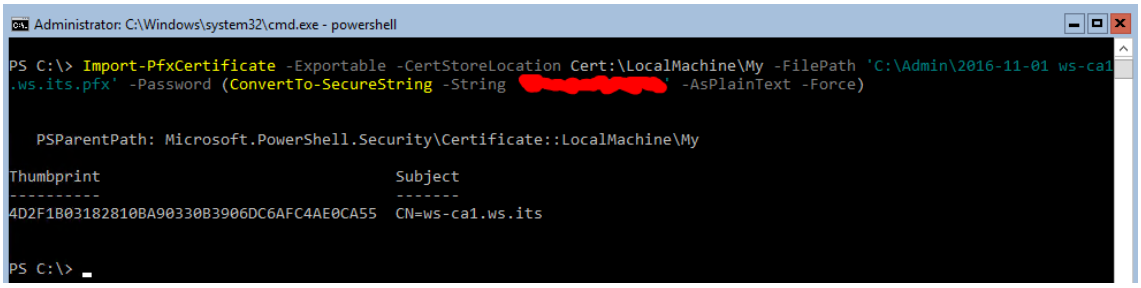

Zertifikateigenschaften
Antragsteller
Allgemein
Erweiterungen
Privater Schlüssel
Zertifizierungsstelle
Signatur
Kryptografiedienstanbieter
Schlüsseloptionen
Legen Sie die Schlüssellänge und die Exportoptionen für den privaten Schlüssel fest.
Schlüsselgröße:
2048
Privaten Schlüssel exportierbar machen
Archivierung des privaten Schlüssels zulassen
Verstärkter Schutz für den privaten Schlüssel
Schlüsseltyp
Schlüsselberechtigungen
OK
Abbrechen
Übernehmen


Zertifikatregistrierung
Zertifikate anfordern
Folgende Zertifikattypen sind abrufbar. Wählen Sie die Zertifikate aus, die Sie anfordern möchten, und klicken Sie anschließend auf "Registrieren".
Active Directory-Registrierungsrichtlinie
WS-ITS-Computer
STATUS: Verfügbar
Details
WS-ITS-Webserver
STATUS: Verfügbar
Details
Alle Vorlagen anzeigen
Registrieren
Abbrechen

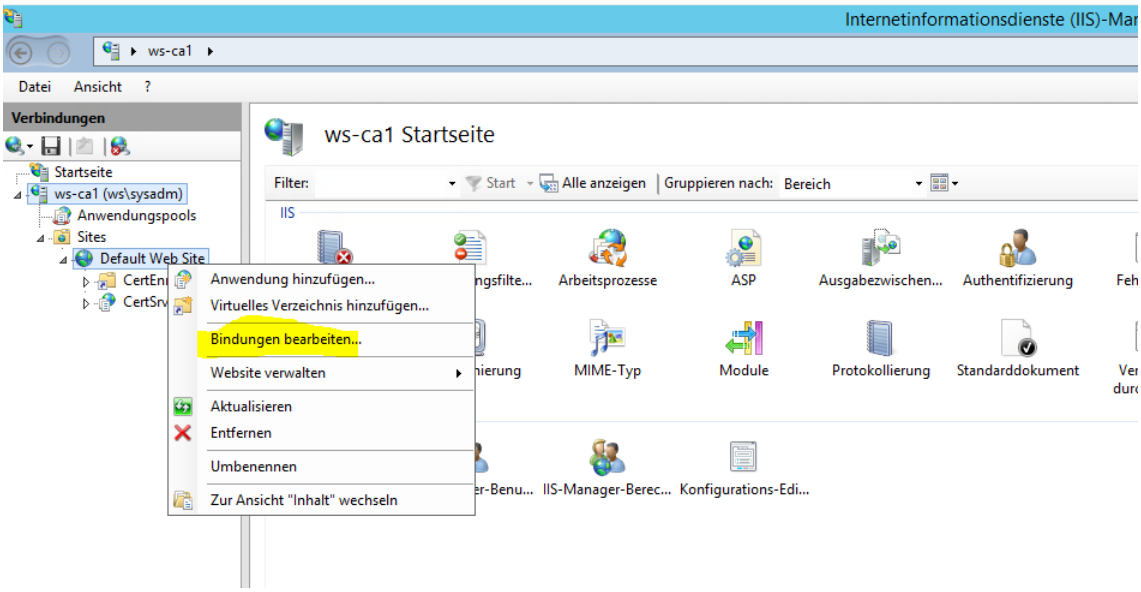

Konsole1 - [Konsolenstamm\Zertifikate (Lokaler Compute
Datei Aktion Ansicht Favoriten Fenster ?
Konsolenstamm
Zertifikate (\\ws-ca1)
Zertifikate (Lokaler Computer)
Eigene Zertifikate
Zertifikate
Vertrauenswürdige Stammzertifizieru
Organisationsvertrauen
Zwischenzertifizierungsstellen
Vertrauenswürdige Geräte
Ausgestellt für
Ausgestellt von
Ablauf
rds.ws-its.de
COMODO RSA Domain Validation...
17.01.2
rds.ws-its.de
PositiveSSL CA 2
18.10.2
rds.ws-its.de
rds.ws-its.de
13.06.2
rds.ws-its.de
PositiveSSL CA 2
23.07.2
rds.ws-its.de
WS-ITS-Zertifizierungsstelle-CA1
29.12.2
ws-ca1.ws
-Zertifizierungsstelle-CA1
01.11.2
WS-RDS1.
S1.ws.its
21.12.2
-Zertifizierungsstelle-CA1
25.08.2
S1.ws.its
29.06.2
Öffnen
Alle Aufgaben
Ausschneiden
Kopieren
Löschen
Eigenschaften
Hilfe
Öffnen
Zertifikat mit neuem Schlüssel anfordern...
Zertifikat mit neuem Schlüssel erneuern...
Private Schlüssel verwalten...
Erweiterte Vorgänge
Exportieren...

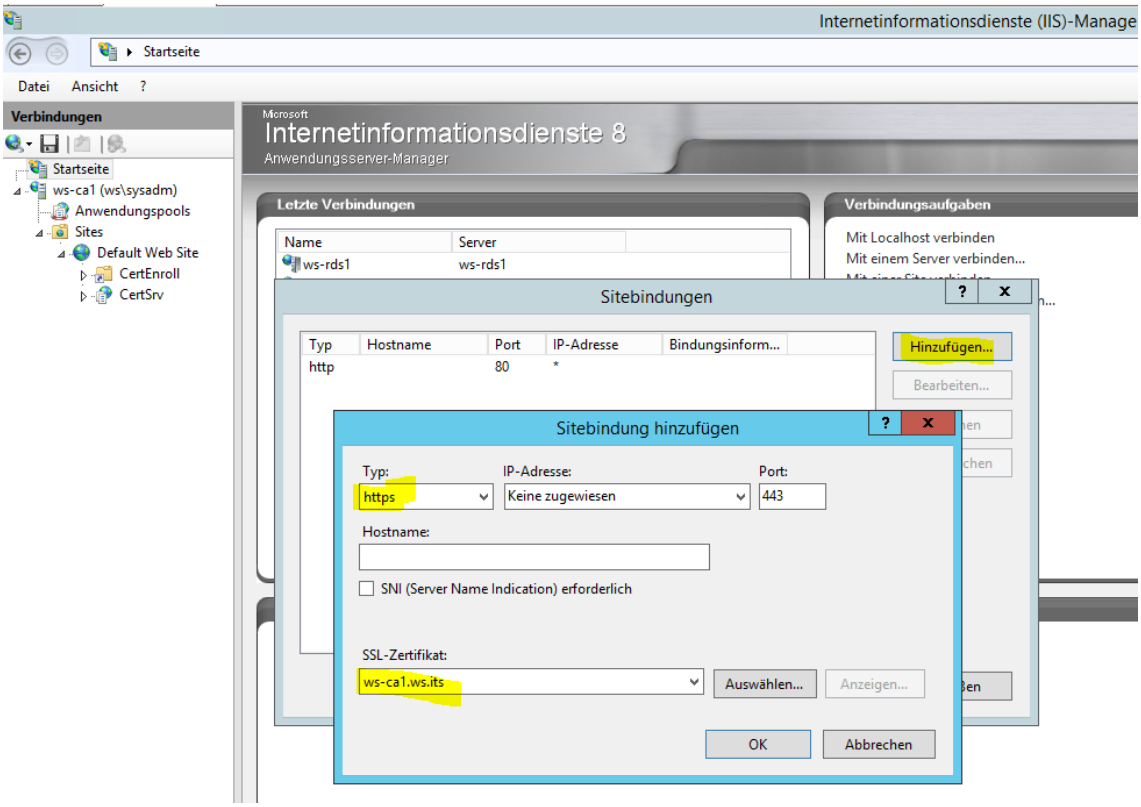


Nun kopiere ich das Zertifikat auf dem neuen CA-Server und importiere es mit der PowerShell:

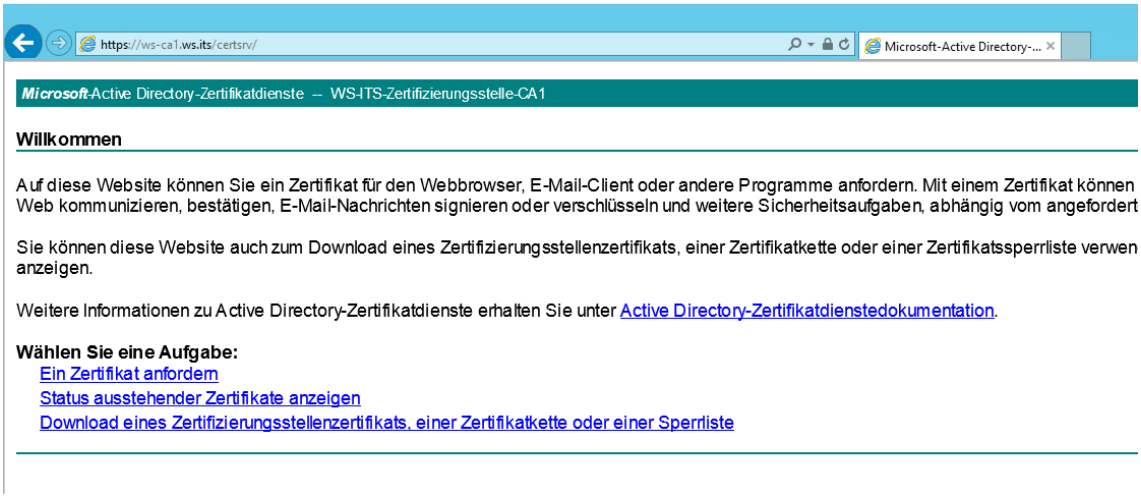


Im IIS-Manager kann ich nun das Zertifikat für die https-Bindung verwenden:



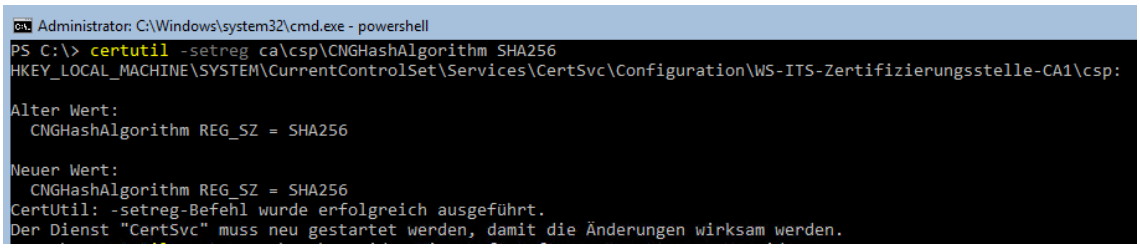


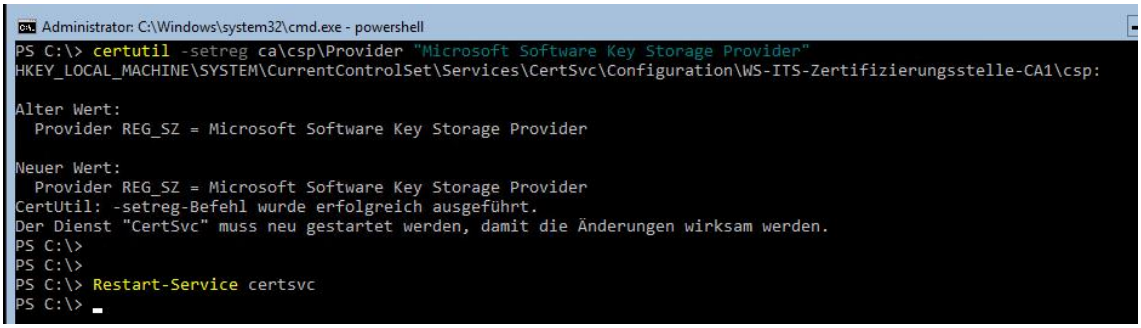
Jetzt ist der Webservice unter https erreichbar:



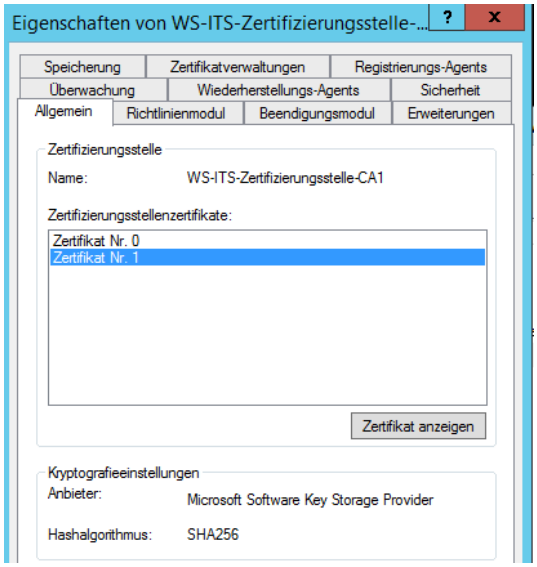
Anpassungen für SHA256

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

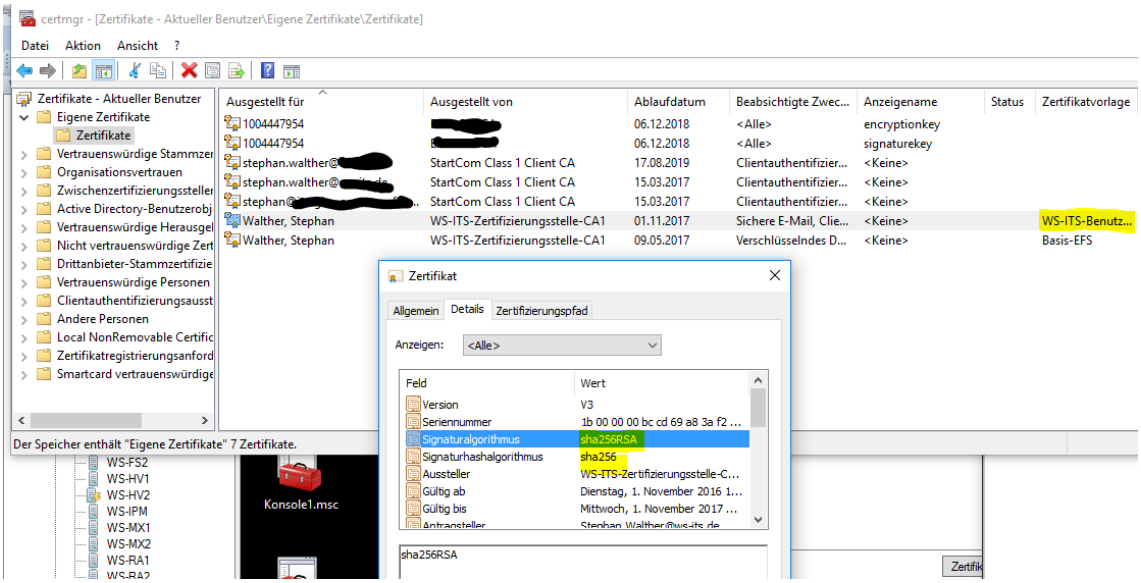




Das Ergebnis:

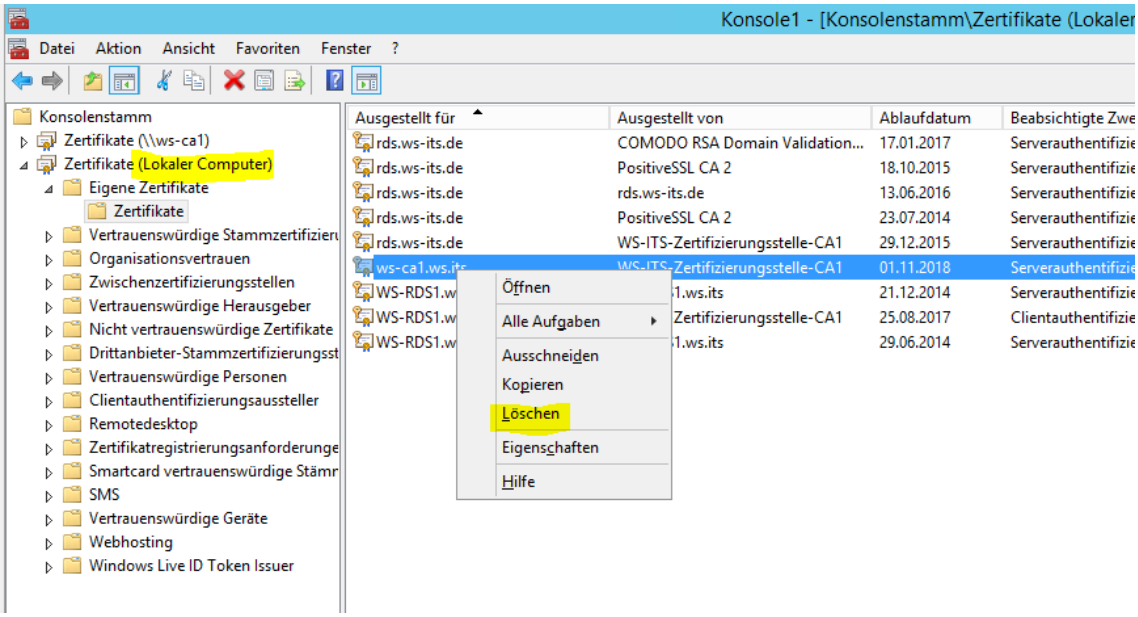


Ein Test zeigt, dass auch ausgestellte Zertifikate mit SHA256 abgesichert sind:



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.