Lernen Online mit Moodle | Vorarlberger Bildungsservice

Probleme bei Moodle – Authentifizierung über ldaps

Besuchen Sie uns im Internet unter
http://www.vobs.at/

Probleme bei Moodle – Authentifizierung über ldaps

Zertifikat erneuern

Inhalt

1. Vorbemerkung

Die grundsätzliche Einrichtung der Moodle-Benutzerauthentifizierung mit dem Benutzerverzeichnis der jeweiligen Schule (z.B. Microsoft Active Directory Service – ADS) über ldap bzw. ldaps wird im Dokument „MoodleVobsLDAPsAnbindung.pdf“ erläutert:
http://moodle2.vobs.at/_allgInfos/MoodleVobsLDAPsAnbindung.pdf

In dieser Kurzanleitung geht es nur um die Erneuerung des selbstsignierten Zertifikates auf dem Domänencontroller der Schule. Mit der Migration der Moodleinstanzen auf den neuen Moodleserver moodle.vobs.at (193.171.140.14) und den notwendigen Sicherheitsupdates im Bereich ssl/tls gab/gibt es vor allem auf Windows Server 2012 (R2) basierten Domänencontrollern Probleme mit der Anbindung an das lokale ADS der Schule über ldap**s** (ldap funktioniert problemlos)**.**

2. Fehlerbild

Nach der Migration der Moodleinstanz auf den neuen Moodleserver und der notwendigen Änderung der IP-Adresse auf der Firewall der Schule (IP des alten Moodleservers 193.171.140.2; IP des neuen Moodleservers 193.171.140.**14):**

kommt beim Moodle-Loginversuch mit einem ADS-Account der Schule folgende Fehlermeldung:

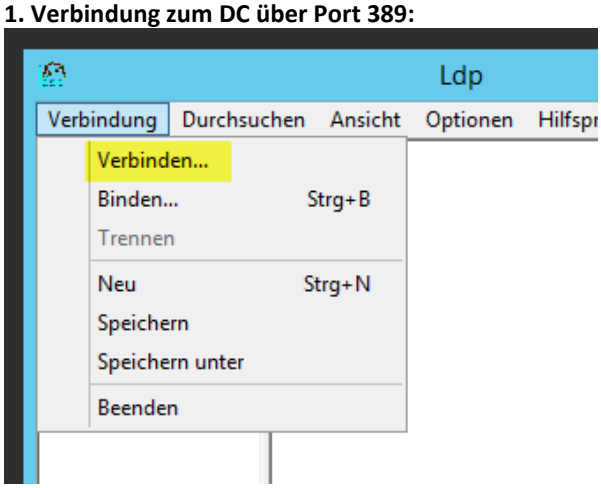
Das LDAP-Modul kann keine Serververbindung herstellen: Server: 'ldaps://193.171.141.18:636', Connection: 'Resource id #83', Bind result: "

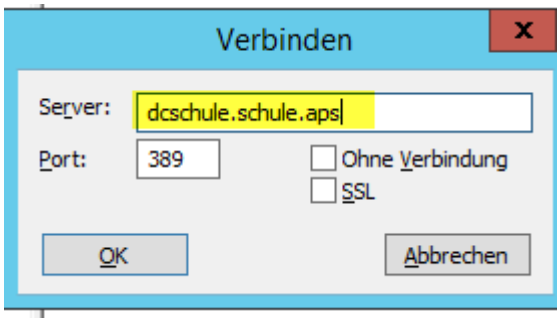
Das ist eine sehr allgemein gehaltene Fehlermeldung, die sehr viele Ursachen haben kann. In unserem Fall liegt es aber vermutlich an dem selbssignierten Zertifikat auf dem DC der Schule.

2.1. Fehlersuche

Wenn wir uns auf dem DC als Admin einloggen und das windowseigene Tool „ldp.exe“ starten, können wir der Sache etwas näher auf den Grund gehen:

1. Verbindung zum DC über Port 389:

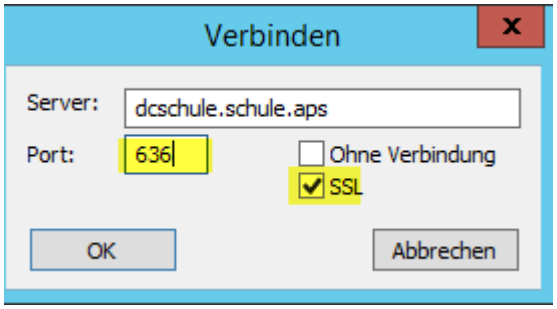




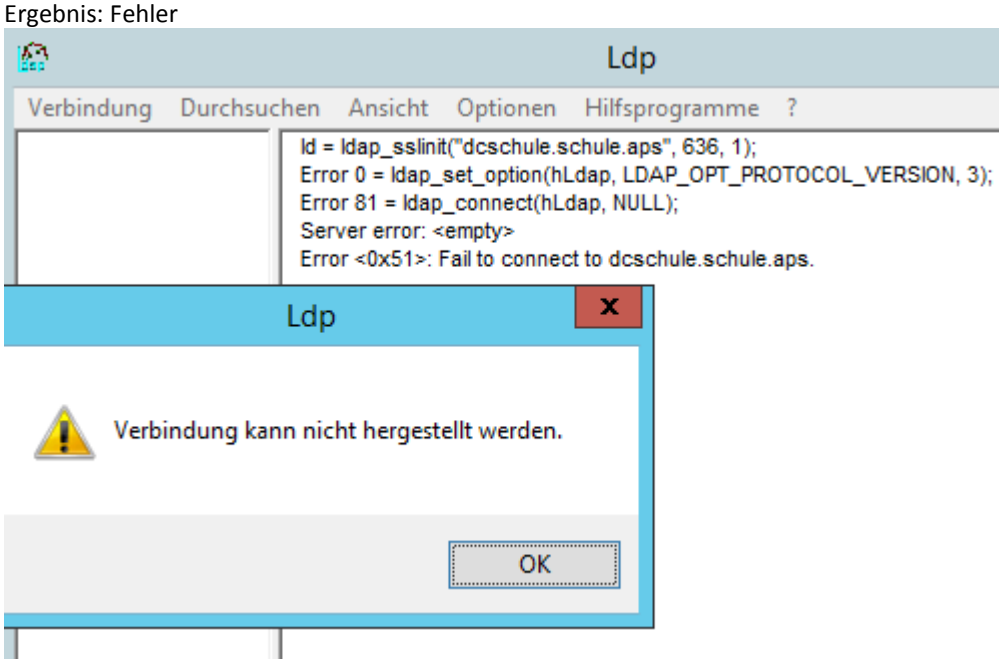
Verbindung passt – es werden AD-Daten abgerufen:

```
ld = ldap_open("dcschule.schule.aps", 389);
Established connection to dcschule.schule.aps.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
    configurationNamingContext: CN=Configuration,DC=schule,DC=aps;
    currentTime: 31.07.2015 12:09:26 Mitteleuropäische Somm;
    defaultNamingContext: DC=schule,DC=aps;
    dnsHostName: DCSchule.schule.aps;
    domainControllerFunctionality: 6 = ( WIN2012R2 );
```

2. Verbindung zum DC über Port 636 und tls:



Ergebnis: Fehler

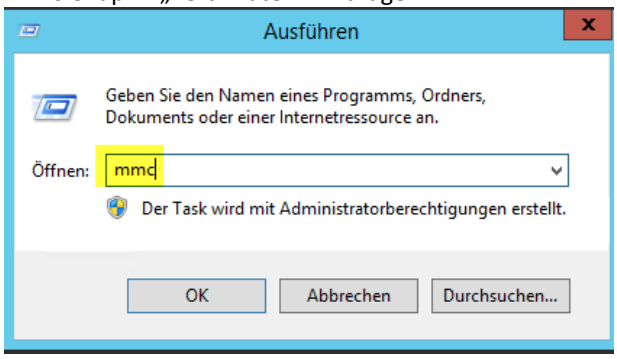


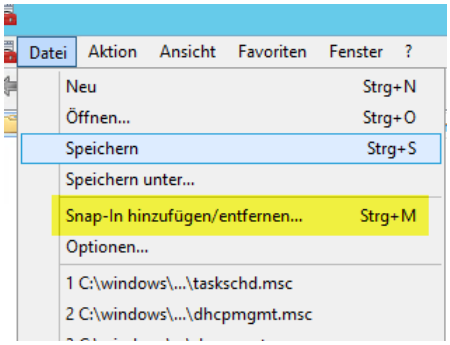
3. Problemlösung: Zertifikat erneuern

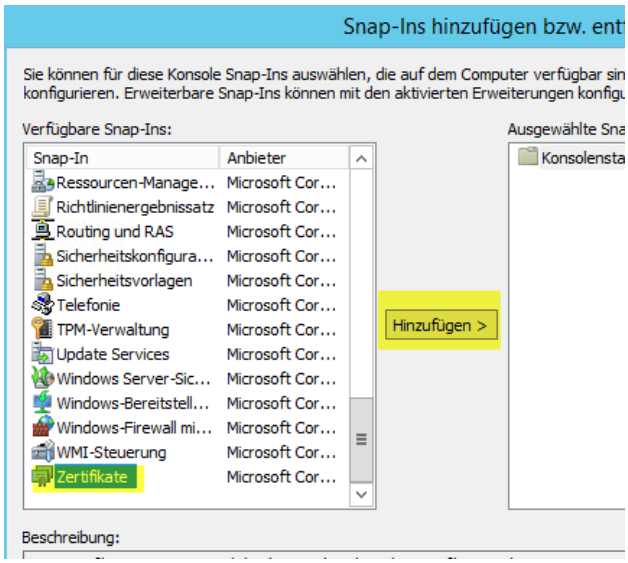
Hier wird eine mögliche Problemlösung erläutert. Da für die Suche nach der Problemursache schon sehr viel Zeit verbraten wurde, habe ich nicht mehr allzu viel Aufwand in verschiedene Wege der Problemlösung investiert. Wenn jemand einen einfacheren Weg zum Ziel kennt, dann bin ich für Hinweise dankbar ;-)
Mein Weg:

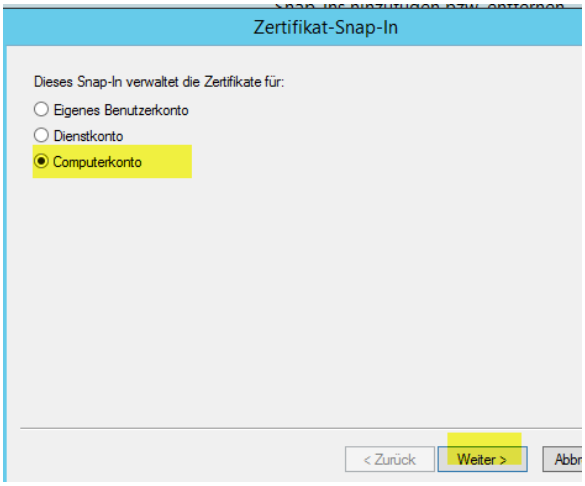
3.1. Alte Zertifikate löschen

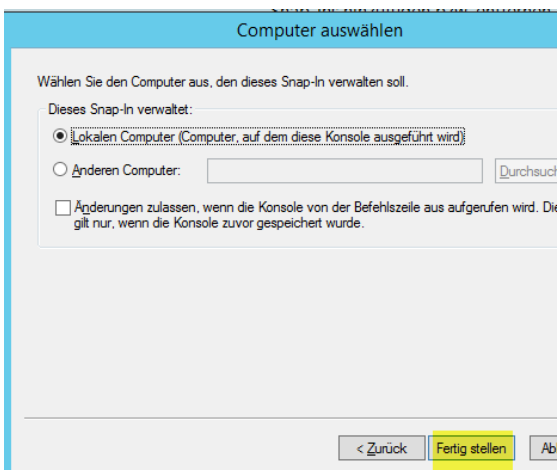
MMC-Snap-In „Zertifikate“ hinzufügen:

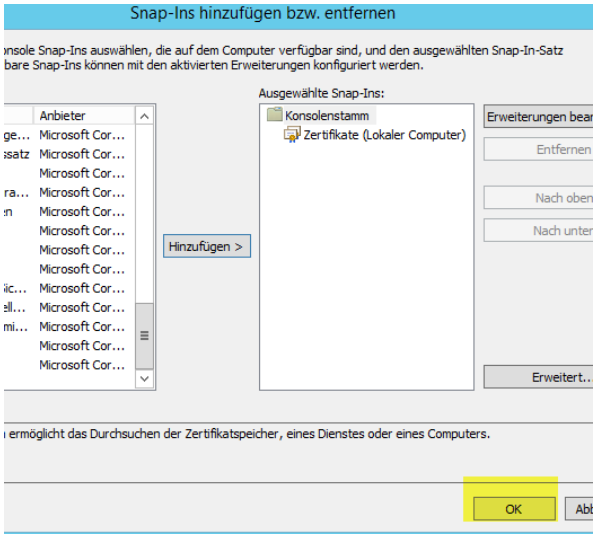




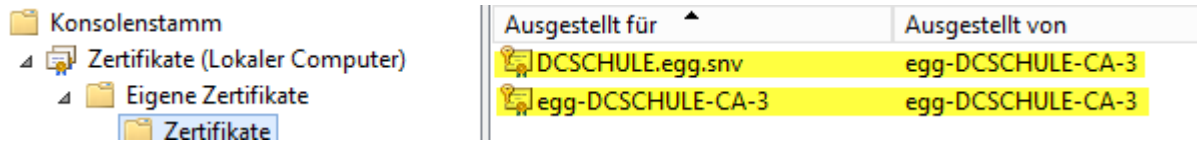


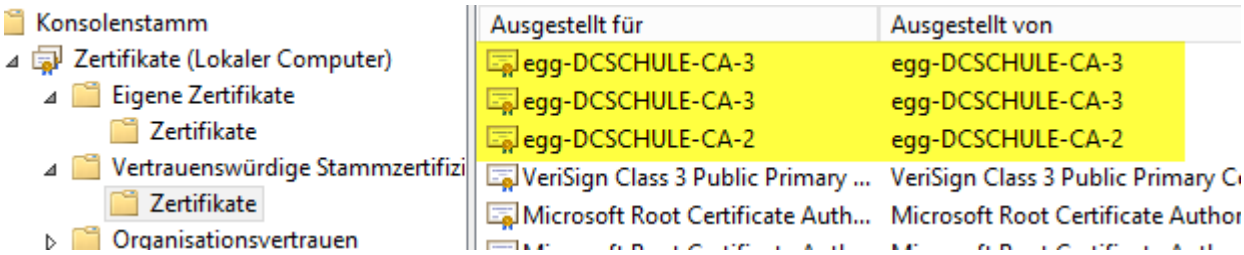






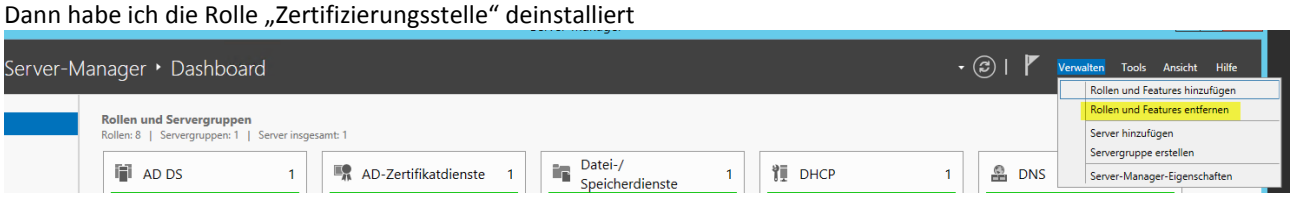
Alle vorhandenen selbstsignierte Zertifikate aus den verschiedenen Speicherbereichen löschen:

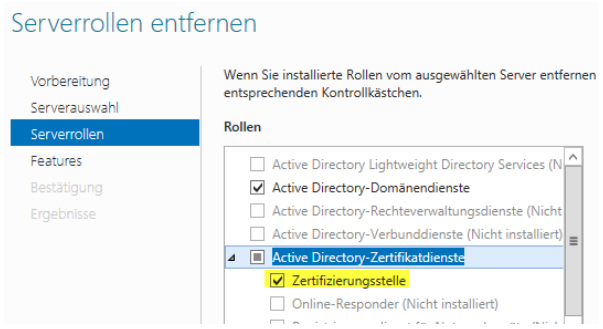


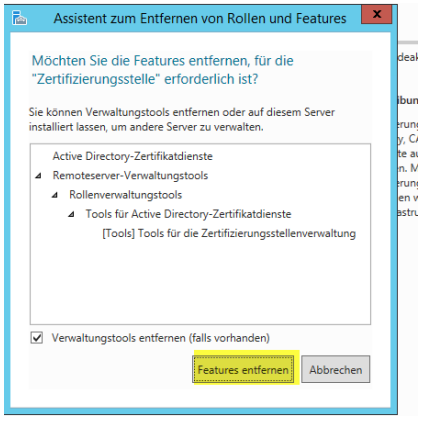


…

Dann habe ich die Rolle „Zertifizierungsstelle“ deinstalliert



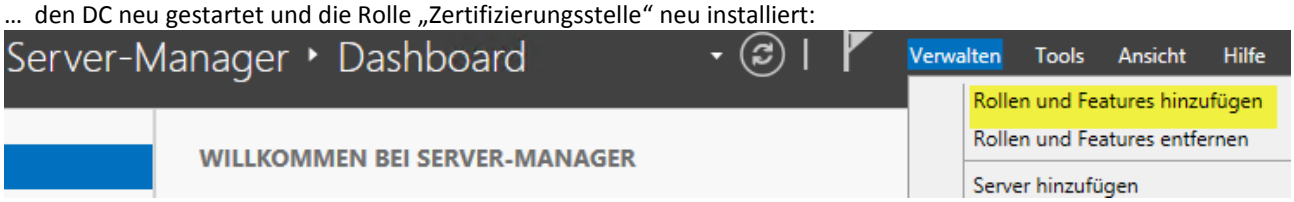


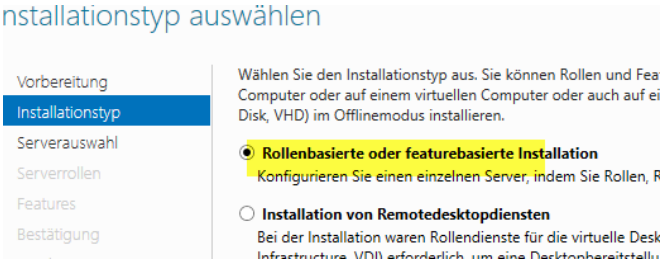


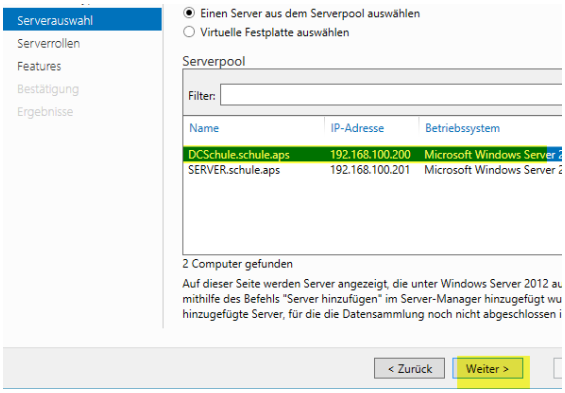
…

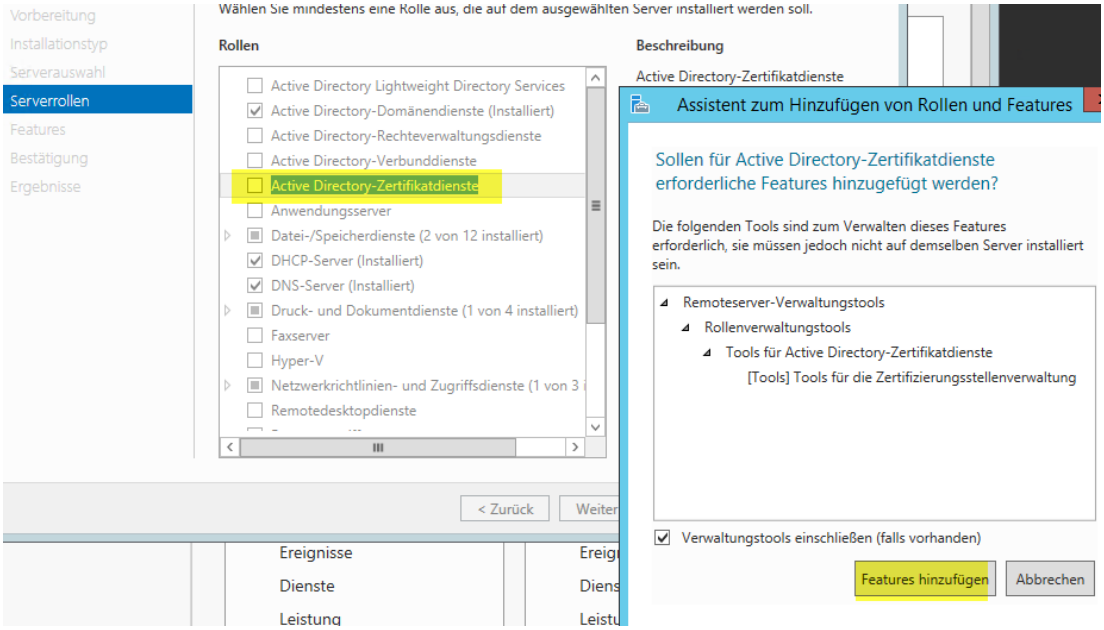
3.2. Zertifizierungsstelle neu installieren

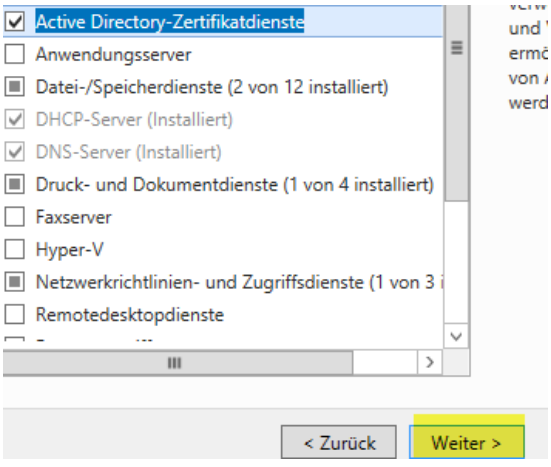
… den DC neu gestartet und die Rolle „Zertifizierungsstelle“ neu installiert:



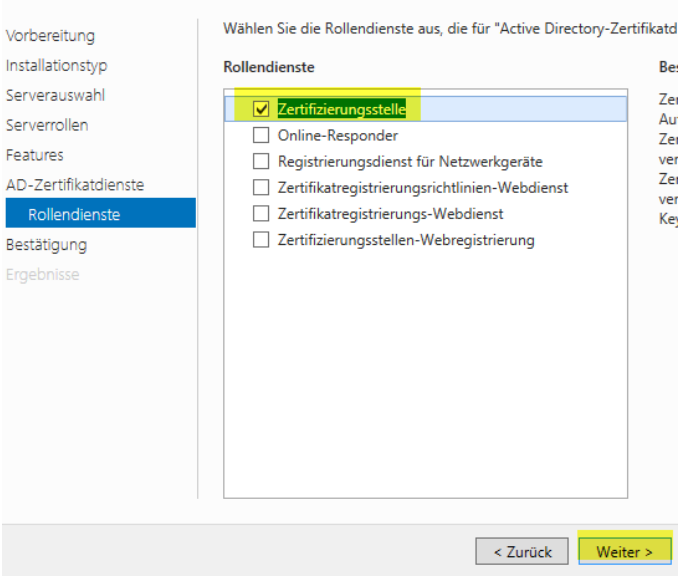

nstallationstyp auswählen
Vorbereitung
Installationstyp
Serverauswahl
Serverrollen
Features
Bestätigung
Wählen Sie den Installationstyp aus. Sie können Rollen und Fea
Computer oder auf einem virtuellen Computer oder auch auf ei
Disk, VHD) im Offlinemodus installieren.
Rollenbasierte oder featurebasierte Installation
Konfigurieren Sie einen einzelnen Server, indem Sie Rollen, R
Installation von Remotedesktopdiensten
Bei der Installation waren Rollendienste für die virtuelle Desk

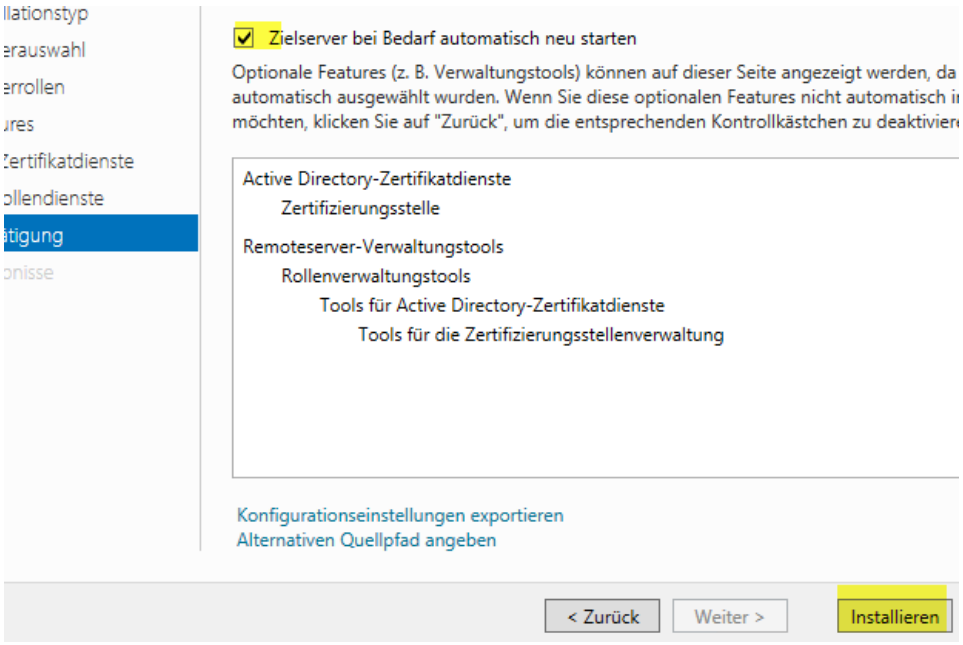

Serverauswahl
Serverrollen
Features
Bestätigung
Ergebnisse
Einen Server aus dem Serverpool auswählen
Virtuelle Festplatte auswählen
Serverpool
Filter:
Name
IP-Adresse
Betriebssystem
DCSchule.schule.aps
192.168.100.200
Microsoft Windows Server
SERVER.schule.aps
192.168.100.201
Microsoft Windows Server
2 Computer gefunden
Auf dieser Seite werden Server angezeigt, die unter Windows Server 2012 au
mithilfe des Befehls "Server hinzufügen" im Server-Manager hinzugefügt wu
hinzugefügte Server, für die die Datensammlung noch nicht abgeschlossen
< Zurück
Weiter >


Vorbereitung
Installationstyp
Serverauswahl
Serverrollen
Features
Bestätigung
Ergebnisse
Wählen Sie mindestens eine Rolle aus, die auf dem ausgewählten Server installiert werden soll.
Rollen
Active Directory Lightweight Directory Services
Active Directory-Domänendienste (Installiert)
Active Directory-Rechteverwaltungsdienste
Active Directory-Verbunddienste
Active Directory-Zertifikatdienste
Anwendungsserver
Datei-/Speicherdienste (2 von 12 installiert)
DHCP-Server (Installiert)
DNS-Server (Installiert)
Druck- und Dokumentdienste (1 von 4 installiert)
Faxserver
Hyper-V
Netzwerkrichtlinien- und Zugriffsdienste (1 von 3
Remotedesktopdienste
Beschreibung
Active Directory-Zertifikatdienste
Assistent zum Hinzufügen von Rollen und Features
Sollen für Active Directory-Zertifikatdienste erforderliche Features hinzugefügt werden?
Die folgenden Tools sind zum Verwalten dieses Features erforderlich, sie müssen jedoch nicht auf demselben Server installiert sein.
Remoteserver-Verwaltungstools
Rollenverwaltungstools
Tools für Active Directory-Zertifikatdienste
[Tools] Tools für die Zertifizierungsstellenverwaltung
Verwaltungstools einschließen (falls vorhanden)
Features hinzufügen
Abbrechen
< Zurück
Ereignisse
Dienste
Leistung

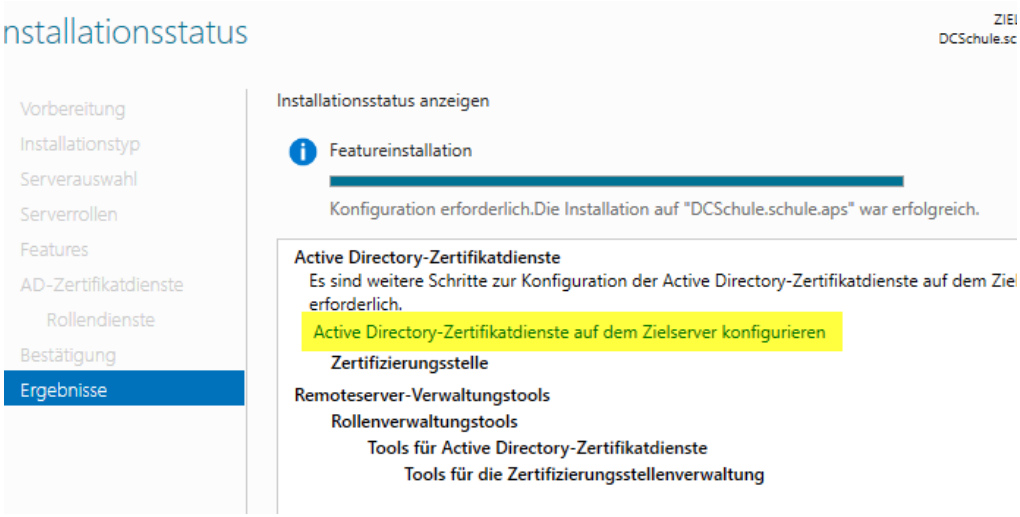

Active Directory-Zertifikatdienste
Anwendungsserver
Datei-/Speicherdienste (2 von 12 installiert)
DHCP-Server (Installiert)
DNS-Server (Installiert)
Druck- und Dokumentdienste (1 von 4 installiert)
Faxserver
Hyper-V
Netzwerkrichtlinien- und Zugriffsdienste (1 von 3
Remotedesktopdienste
< Zurück
Weiter >

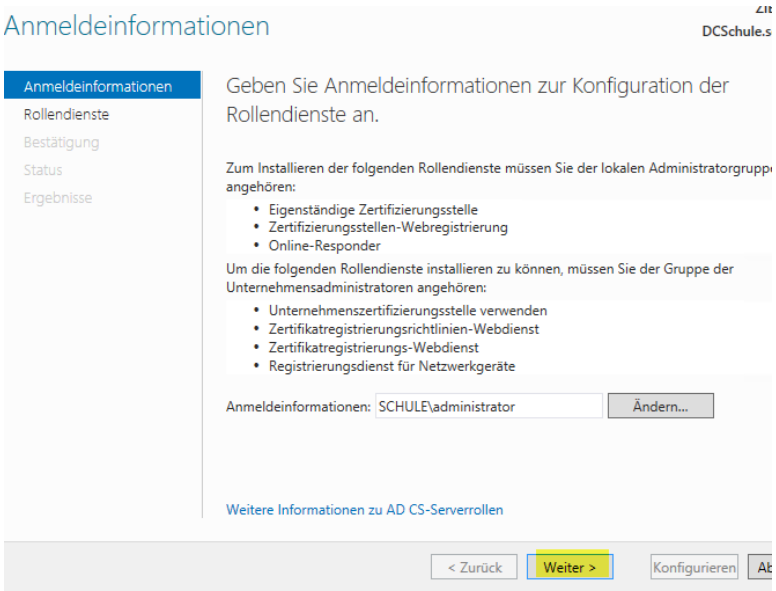
....

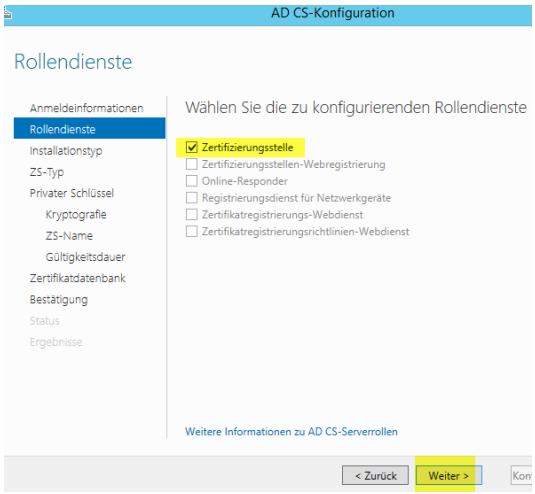

Vorbereitung
Installationstyp
Serverauswahl
Serverrollen
Features
AD-Zertifikatdienste
Rollendienste
Bestätigung
Ergebnisse
Wählen Sie die Rollendienste aus, die für "Active Directory-Zertifikatd
Rollendienste
Zertifizierungsstelle
Online-Responder
Registrierungsdienst für Netzwerkgeräte
Zertifikatregistrierungsrichtlinien-Webdienst
Zertifikatregistrierungs-Webdienst
Zertifizierungsstellen-Webregistrierung
< Zurück
Weiter >

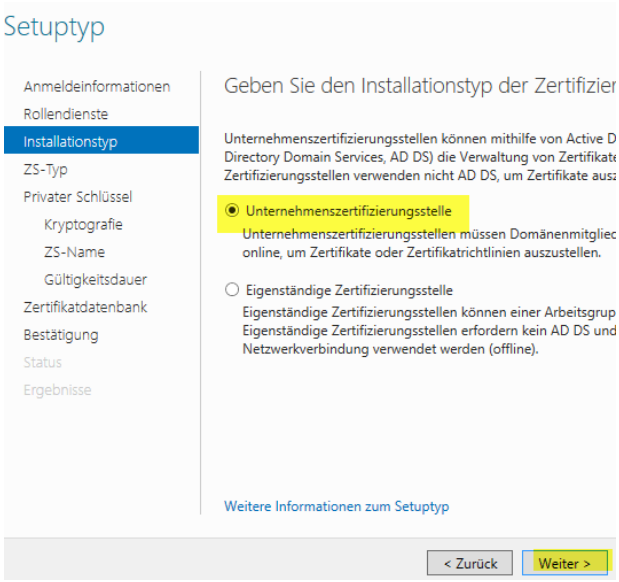

Zielserver bei Bedarf automatisch neu starten
Optionale Features (z. B. Verwaltungstools) können auf dieser Seite angezeigt werden, da
automatisch ausgewählt wurden. Wenn Sie diese optionalen Features nicht automatisch i
möchten, klicken Sie auf "Zurück", um die entsprechenden Kontrollkästchen zu deaktivier
Active Directory-Zertifikatdienste
Zertifizierungsstelle
Remoteserver-Verwaltungstools
Rollenverwaltungstools
Tools für Active Directory-Zertifikatdienste
Tools für die Zertifizierungsstellenverwaltung
Konfigurationseinstellungen exportieren
Alternativen Quellpfad angeben
< Zurück
Weiter >
Installieren

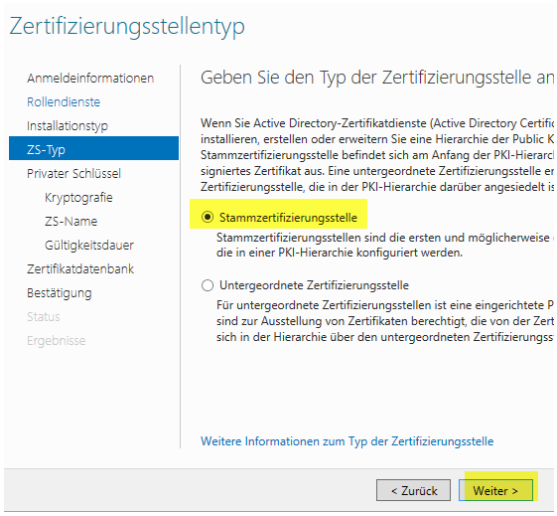
… warten …

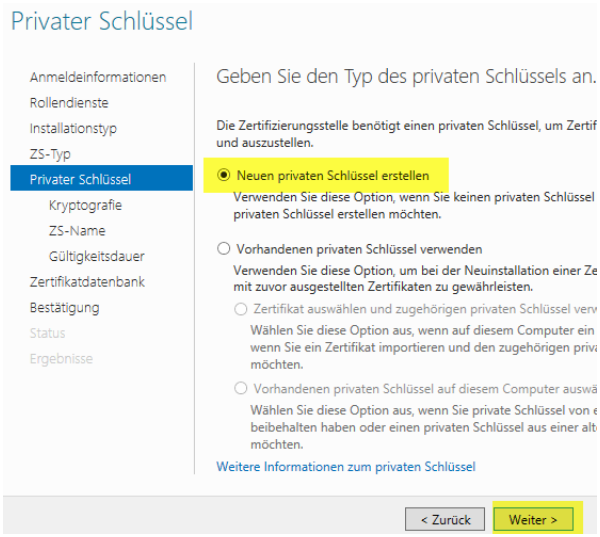

nstallationsstatus
Vorbereitung
Installationstyp
Serverauswahl
Serverrollen
Features
AD-Zertifikatdienste
Rollendienste
Bestätigung
Ergebnisse
Installationsstatus anzeigen
Featureinstallation
Konfiguration erforderlich.Die Installation auf "DCSchule.schule.aps" war erfolgreich.
Active Directory-Zertifikatdienste
Es sind weitere Schritte zur Konfiguration der Active Directory-Zertifikatdienste auf dem Ziel
erforderlich.
Active Directory-Zertifikatdienste auf dem Zielserver konfigurieren
Zertifizierungsstelle
Remoteserver-Verwaltungstools
Rollenverwaltungstools
Tools für Active Directory-Zertifikatdienste
Tools für die Zertifizierungsstellenverwaltung

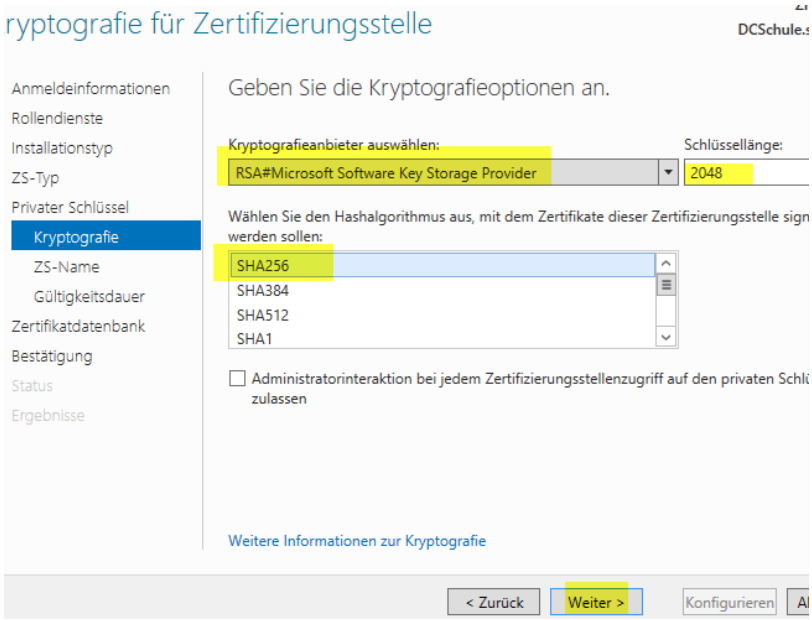

Anmeldeinformationen
Anmeldeinformationen
Rollendienste
Bestätigung
Status
Ergebnisse
Geben Sie Anmeldeinformationen zur Konfiguration der Rollendienste an.
Zum Installieren der folgenden Rollendienste müssen Sie der lokalen Administratorgrupp
angehören:
Eigenständige Zertifizierungsstelle
Zertifizierungsstellen-Webregistrierung
Online-Responder
Um die folgenden Rollendienste installieren zu können, müssen Sie der Gruppe der
Unternehmensadministratoren angehören:
Unternehmenszertifizierungsstelle verwenden
Zertifikatregistrierungsrichtlinien-Webdienst
Zertifikatregistrierungs-Webdienst
Registrierungsdienst für Netzwerkgeräte
Anmeldeinformationen: SCHULE\administrator
Ändern...
Weitere Informationen zu AD CS-Serverrollen
< Zurück
Weiter >
Konfigurieren

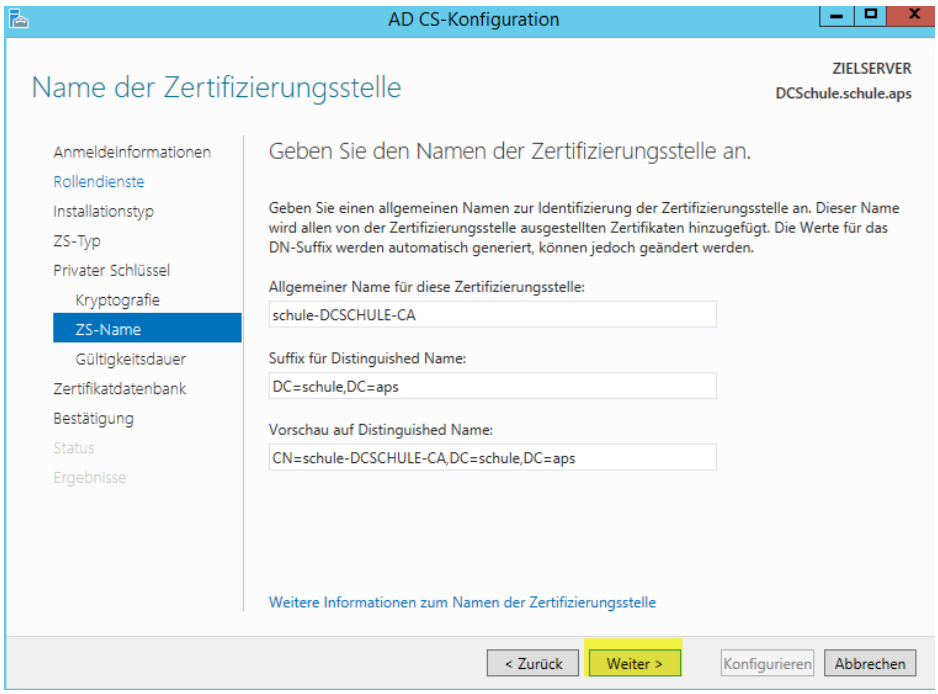

AD CS-Konfiguration
Rollendienste
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Wählen Sie die zu konfigurierenden Rollendienste
Zertifizierungsstelle
Zertifizierungsstellen-Webregistrierung
Online-Responder
Registrierungsdienst für Netzwerkgeräte
Zertifikatregistrierungs-Webdienst
Zertifikatregistrierungsrichtlinien-Webdienst
Weitere Informationen zu AD CS-Serverrollen
< Zurück
Weiter >

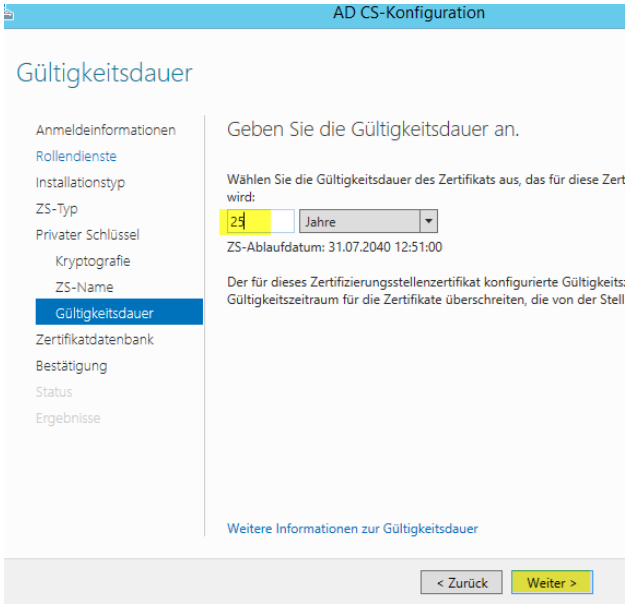

Setuptyp
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Installationstyp der Zertifizier
Unternehmenszertifizierungsstellen können mithilfe von Active D
Directory Domain Services, AD DS) die Verwaltung von Zertifikat
Zertifizierungsstellen verwenden nicht AD DS, um Zertifikate aus
Unternehmenszertifizierungsstelle
Unternehmenszertifizierungsstellen müssen Domänenmitglied
online, um Zertifikate oder Zertifikatrichtlinien auszustellen.
Eigenständige Zertifizierungsstelle
Eigenständige Zertifizierungsstellen können einer Arbeitsgrup
Eigenständige Zertifizierungsstellen erfordern kein AD DS und
Netzwerkverbindung verwendet werden (offline).
Weitere Informationen zum Setuptyp
< Zurück
Weiter >

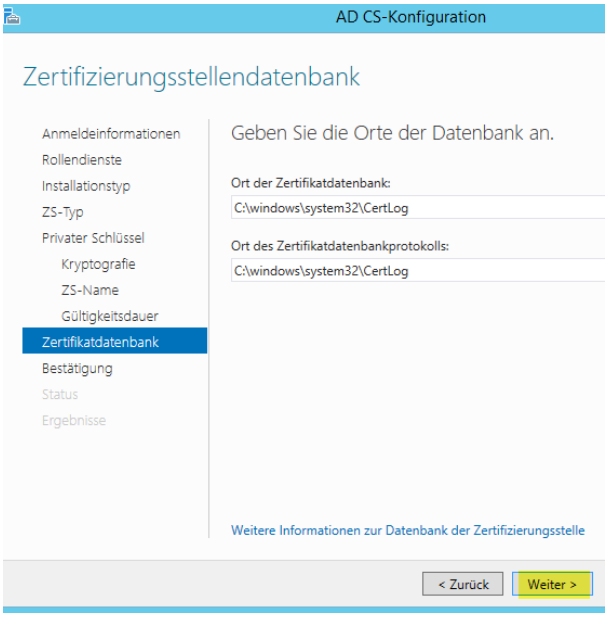

Zertifizierungsstellentyp
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Typ der Zertifizierungsstelle an
Wenn Sie Active Directory-Zertifikatdienste (Active Directory Certifi
installieren, erstellen oder erweitern Sie eine Hierarchie der Public K
Stammzertifizierungsstelle befindet sich am Anfang der PKI-Hierarc
signiertes Zertifikat aus. Eine untergeordnete Zertifizierungsstelle er
Zertifizierungsstelle, die in der PKI-Hierarchie darüber angesiedelt is
Stammzertifizierungsstelle
Stammzertifizierungsstellen sind die ersten und möglicherweise
die in einer PKI-Hierarchie konfiguriert werden.
Untergeordnete Zertifizierungsstelle
Für untergeordnete Zertifizierungsstellen ist eine eingerichtete P
sind zur Ausstellung von Zertifikaten berechtigt, die von der Zert
sich in der Hierarchie über den untergeordneten Zertifizierungss
Weitere Informationen zum Typ der Zertifizierungsstelle
< Zurück
Weiter >

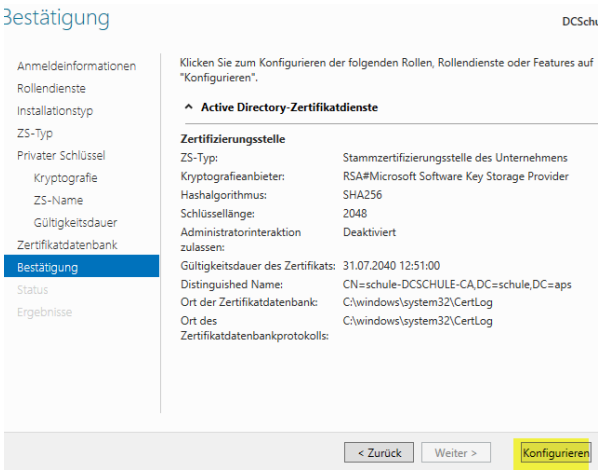

Privater Schlüssel
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Typ des privaten Schlüssels an.
Die Zertifizierungsstelle benötigt einen privaten Schlüssel, um Zertif
und auszustellen.
Neuen privaten Schlüssel erstellen
Verwenden Sie diese Option, wenn Sie keinen privaten Schlüssel
privaten Schlüssel erstellen möchten.
Vorhandenen privaten Schlüssel verwenden
Verwenden Sie diese Option, um bei der Neuinstallation einer Ze
mit zuvor ausgestellten Zertifikaten zu gewährleisten.
Zertifikat auswählen und zugehörigen privaten Schlüssel verw
Wählen Sie diese Option aus, wenn auf diesem Computer ein
wenn Sie ein Zertifikat importieren und den zugehörigen priv
möchten.
Vorhandenen privaten Schlüssel auf diesem Computer auswä
Wählen Sie diese Option aus, wenn Sie private Schlüssel von
beibehalten haben oder einen privaten Schlüssel aus einer alt
möchten.
Weitere Informationen zum privaten Schlüssel
< Zurück
Weiter >

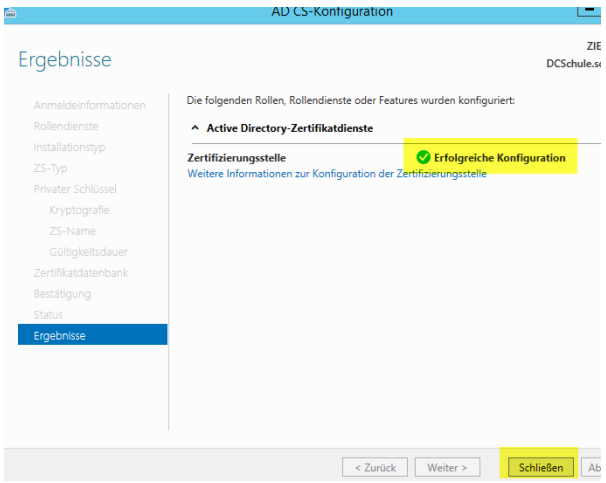

ryptografie für Zertifizierungsstelle
DCSchule.
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie die Kryptografieoptionen an.
Kryptografieanbieter auswählen:
Schlüssellänge:
RSA#Microsoft Software Key Storage Provider
2048
Wählen Sie den Hashalgorithmus aus, mit dem Zertifikate dieser Zertifizierungsstelle sign
werden sollen:
SHA256
SHA384
SHA512
SHA1
Administratorinteraktion bei jedem Zertifizierungsstellenzugriff auf den privaten Schl
zulassen
Weitere Informationen zur Kryptografie
< Zurück
Weiter >
Konfigurieren


AD CS-Konfiguration
Name der Zertifizierungsstelle
ZIELSERVER
DCSchule.schule.aps
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie den Namen der Zertifizierungsstelle an.
Geben Sie einen allgemeinen Namen zur Identifizierung der Zertifizierungsstelle an. Dieser Name wird allen von der Zertifizierungsstelle ausgestellten Zertifikaten hinzugefügt. Die Werte für das DN-Suffix werden automatisch generiert, können jedoch geändert werden.
Allgemeiner Name für diese Zertifizierungsstelle:
schule-DCSCHULE-CA
Suffix für Distinguished Name:
DC=schule,DC=aps
Vorschau auf Distinguished Name:
CN=schule-DCSCHULE-CA,DC=schule,DC=aps
Weitere Informationen zum Namen der Zertifizierungsstelle
< Zurück
Weiter >
Konfigurieren
Abbrechen


AD CS-Konfiguration
Gültigkeitsdauer
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie die Gültigkeitsdauer an.
Wählen Sie die Gültigkeitsdauer des Zertifikats aus, das für diese Zert wird:
25
Jahre
ZS-Ablaufdatum: 31.07.2040 12:51:00
Der für dieses Zertifizierungsstellenzertifikat konfigurierte Gültigkeits: Gültigkeitszeitraum für die Zertifikate überschreiten, die von der Stell
Weitere Informationen zur Gültigkeitsdauer
< Zurück
Weiter >

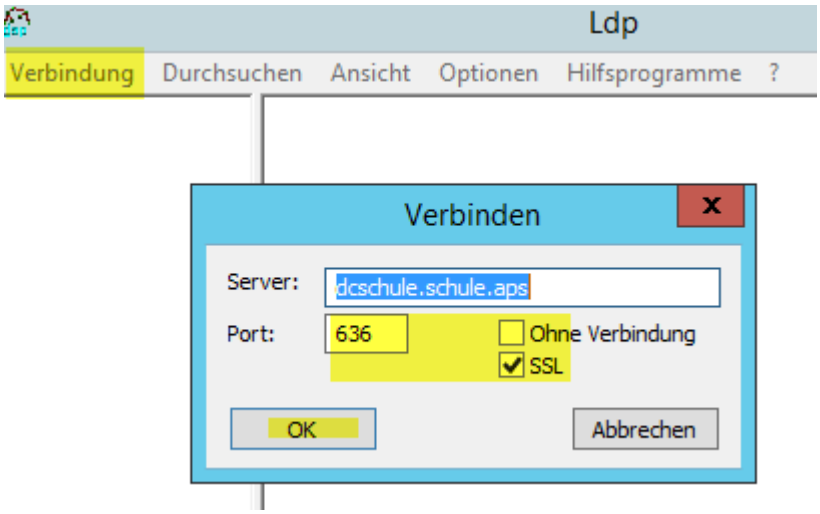

AD CS-Konfiguration
Zertifizierungsstellendatenbank
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Geben Sie die Orte der Datenbank an.
Ort der Zertifikatdatenbank:
C:\windows\system32\CertLog
Ort des Zertifikatdatenbankprotokolls:
C:\windows\system32\CertLog
Weitere Informationen zur Datenbank der Zertifizierungsstelle
< Zurück
Weiter >


Bestätigung
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Klicken Sie zum Konfigurieren der folgenden Rollen, Rollendienste oder Features auf "Konfigurieren".
Active Directory-Zertifikatdienste
Zertifizierungsstelle
ZS-Typ: Stammzertifizierungsstelle des Unternehmens
Kryptografieanbieter: RSA#Microsoft Software Key Storage Provider
Hashalgorithmus: SHA256
Schlüssellänge: 2048
Administratorinteraktion zulassen: Deaktiviert
Gültigkeitsdauer des Zertifikats: 31.07.2040 12:51:00
Distinguished Name: CN=schule-DCSCHULE-CA,DC=schule,DC=aps
Ort der Zertifikatdatenbank: C:\windows\system32\CertLog
Ort des Zertifikatdatenbankprotokolls: C:\windows\system32\CertLog
< Zurück
Weiter >
Konfigurieren

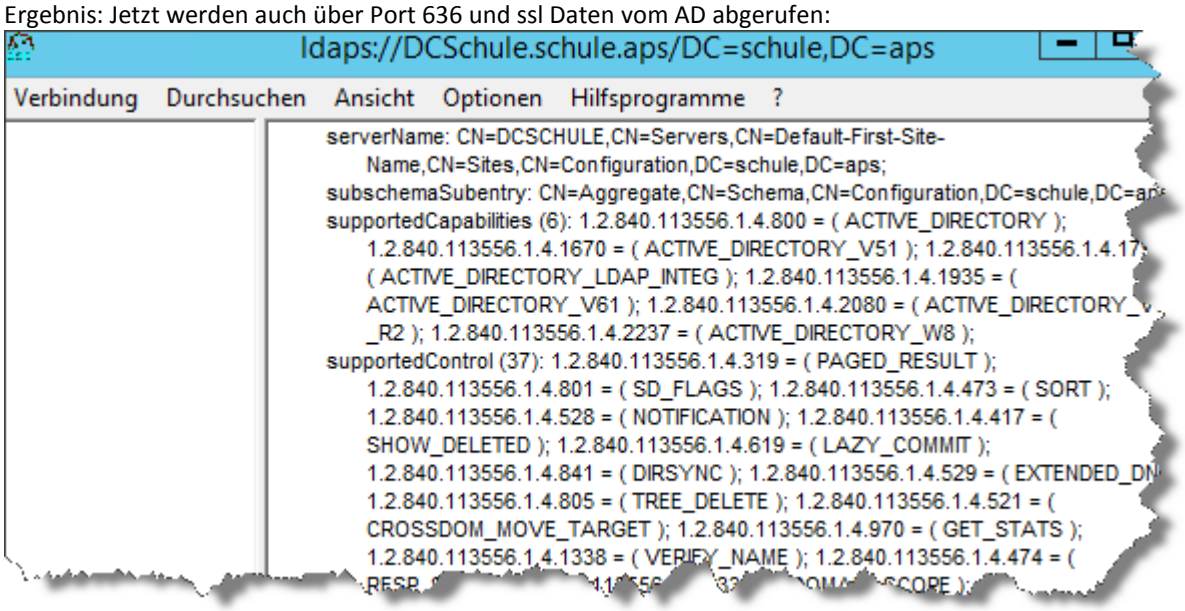

AD CS-Konfiguration
Ergebnisse
Anmeldeinformationen
Rollendienste
Installationstyp
ZS-Typ
Privater Schlüssel
Kryptografie
ZS-Name
Gültigkeitsdauer
Zertifikatdatenbank
Bestätigung
Status
Ergebnisse
Die folgenden Rollen, Rollendienste oder Features wurden konfiguriert:
Active Directory-Zertifikatdienste
Zertifizierungsstelle
Erfolgreiche Konfiguration
Weitere Informationen zur Konfiguration der Zertifizierungsstelle
< Zurück
Weiter >
Schließen

DC neu starten!

Kontrolle mit ldp.exe:



Ergebnis: Jetzt werden auch über Port 636 und ssl Daten vom AD abgerufen:



Damit sollte auch die ldaps – Anbindung der Moodleinstanz wieder funzen ☺.