LDAP(S) Anbindung von außen

Windows Musterlösung
Daniel Wiesler, Stefan Kink
30.05.2017

1. Einführung

Das Lightweight Directory Access Protocol bietet vielfältige Kommunikationsmöglichkeiten für die aktuellen Bedürfnisse von schulischen Netzwerkumgebungen. So ist es möglich, die AD-Benutzer des pädagogischen Schulnetzwerks zur Authentifizierung in Moodle oder WebUntis zu nutzen um ein deutlich schlankeres Benutzermanagement pflegen zu können.

Die vorliegende Dokumentation basiert auf einer früheren Version zur paedML 2.x von Johannes Kühn.

2. LDAP Konfiguration

Zur Einrichtung eines Zugriffs von außen per LDAP(S), sind in der paedML3.x mehrere Schritte erforderlich:

1. Octogate Portweiterleitung einrichten
2. LDAP-Benutzer zur Kommunikation mit externem Service (z.B. Moodle) anlegen
3. Konfiguration des externen Dienstes (z.B. Moodle): LDAP Authentifizierung aktivieren und als Standard definieren
4. LDAPS: Rollenkonfiguration und Zertifikatsimport auf DC01.

2.1. Octogate konfigurieren

Die für LDAP(S) benötigten Ports 389 bzw. 636 müssen der Octogate Firewall zur Kommunikation nach außen bekannt gemacht werden. Dazu eignet sich insbesondere eine Portweiterleitung. Durch das Weiterleiten des Standard-LDAP-Ports auf abweichende, nicht standardisierte Werte ist die Öffnung des Systems nach außen mit einem geringeren Sicherheitsrisiko verbunden[1]. Dies soll im Folgenden angewandt werden (weiterführende Informationen finden siehe auch in den Fortbildungsunterlagen zu ***Portweiterleitungen in der paedML3.x***, auf eine bebilderte Anleitung wird daher an dieser Stelle verzichtet).

1 Damit ein Zugriff von außen erfolgen kann, muss der nach außen weitergeleitete Port im externen Hardwarerouter (z.B. von BelWü) freigeschaltet sein. Dazu müssen Sie u.U. Kontakt mit BelWü selbst aufnehmen (anschluss@belwue.de).

2.1.1. Weboberfläche aufrufen

1. Starten Sie die Weboberfläche der Octogate Firewall.
2. Melden Sie sich als Administrator an.
3. Wechseln Sie links im Menü zu dem Punkt: Firewall – Portweiterleitungen.

2.1.2. Portweiterleitung einrichten

1. Fügen Sie nun eine neue Weiterleitungsregel hinzu und benennen Sie sie nach ihrer Funktion: LDAP
2. Richten Sie so eine Weiterleitung des intern lauschenden Ports 389 auf DC01 (mit der IP 10.1.1.1) auf die externe IP (d.h. der IP der Schule) mit einem beliebigen anderen Port ein. Hier bieten sich hohe Zahlbereiche an, die nicht bereits reserviert sind, z.B. 45001.
3. Speichern Sie die Regel und aktualisieren (oben rechts) die Octogate Firewall, erst nach diesem Schritt wird die Weiterleitung auch funktionieren.

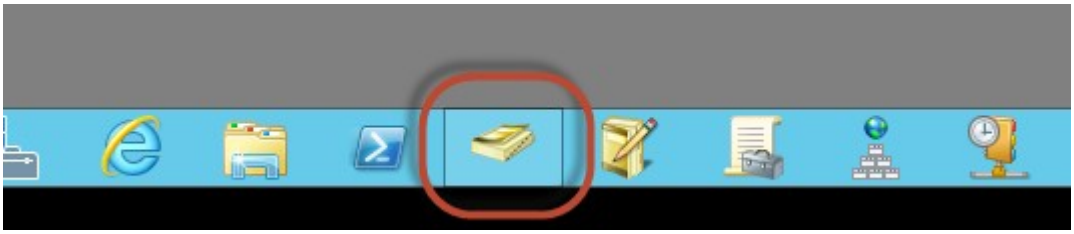
2.1.3. Übung: LDAPS-Weiterleitung einrichten

Führen Sie die obigen Schritte erneut durch, um eine Weiterleitung für das LDAPS Protokoll (Port 636) auf einen anderen, beliebigen Port nach außen freizuschalten.

2.2. LDAP-Benutzer einrichten

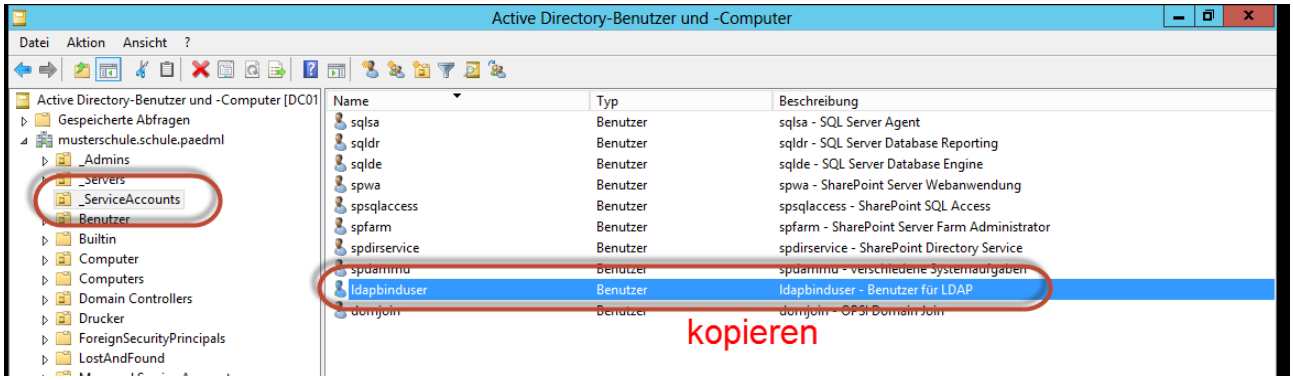
Als nächstes soll ein Service-Benutzer auf DC01 eingerichtet werden, der den alleinigen Zweck der Kommunikation einer externen Quelle über das LDAP Protokoll mit dem AD hat.

1. Starten Sie zu diesem Zweck die AD-Verwaltung auf dem Server DC01.

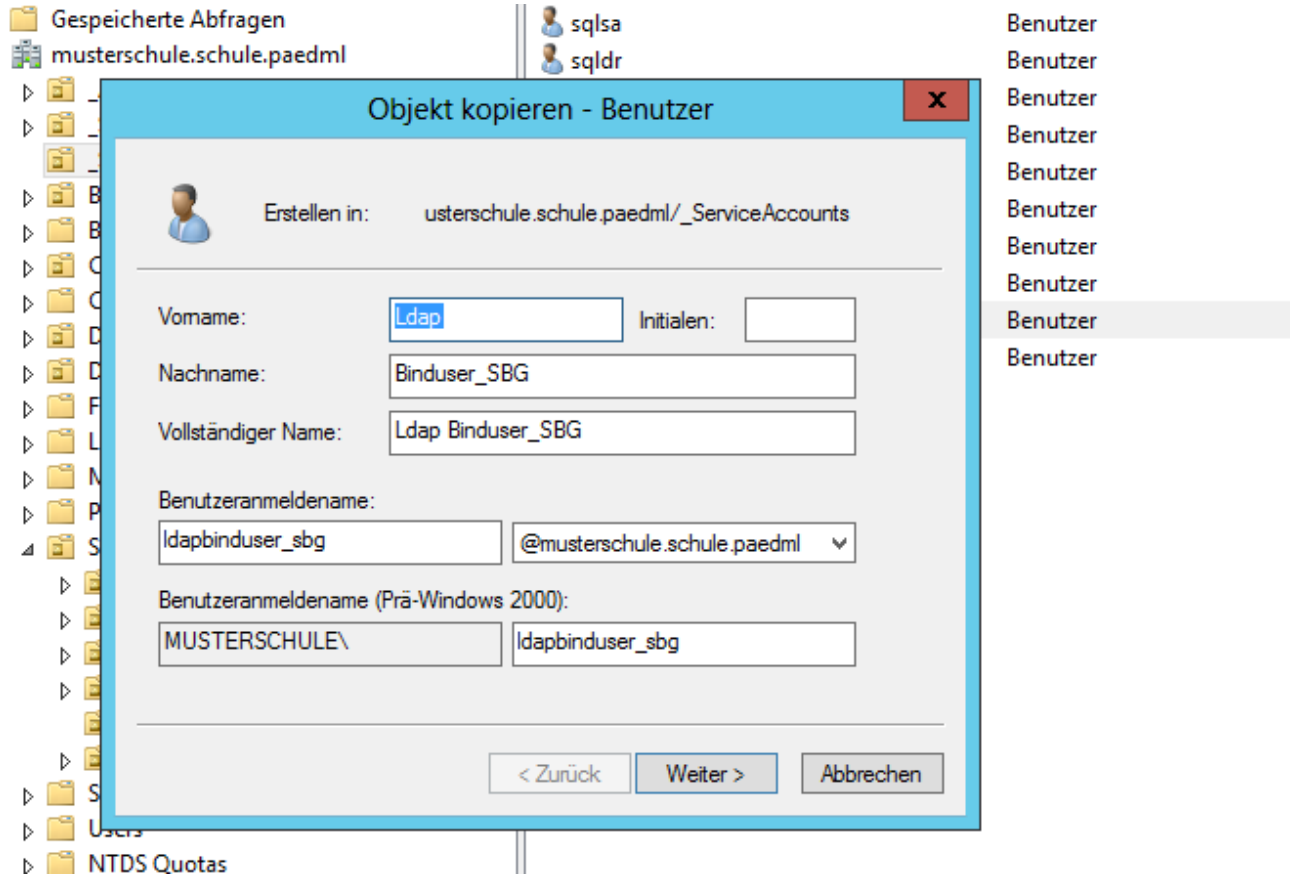


2. Gehen Sie in die OU „_ServiceAccounts“.

3. Kopieren Sie den existenten Benutzer „ldapbinduser“ und geben ihm einen eindeutigen Namen, z.B. „ldapbinduser_sbg“. Dieser ServiceAccount hat den einzigen Zweck: die Kommunikation mit einem extern gehosteten Dienst.



4. Der Benutzer hat keine besondere Eigenschaften, er muss lediglich Mitglied der Domäne sein.



2.3. Konfiguration des externen Dienstes

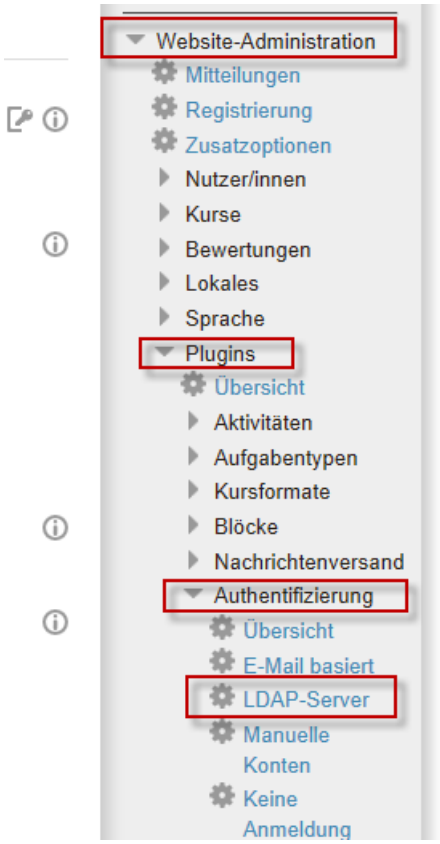
Für einen Zugriff von außen über das LDAP Protokoll soll am typischen Einsatzbeispiel Moodle besprochen werden, wie der externe Dienst konfiguriert werden muss, um auf die AD-Struktur der Domänenbenutzer zugreifen zu können. Diese Sektion ist damit stark auf diesen einen Spezialfall

zugeschnitten. Die Anbindung anderer Dienste kann sich mitunter deutlich von der hier gezeigten Lösung unterscheiden, auch wenn die logischen Schritte die gleichen sind.

2.3.1. LDAP Plugin aktivieren

Falls noch nicht geschehen, müssen Sie Moodle installieren.

1. Loggen Sie sich als Administrator in Moodle ein.
2. Gehen Sie zum Plugin-Bereich.
3. Aktivieren Sie das LDAP-Plugin (z.B. durch einen Klick auf das Auge.)



Das Bild zeigt die Einstellung in Moodle 2.x.

2.3.2. LDAP-Zugriff konfigurieren

Damit der Dienst, im vorliegenden Fall Moodle, erkennt, welche Benutzer in welcher Struktur des Verzeichnisses angelegt sind und auf diese zugreifen kann, müssen umfangreiche und detaillierte Einstellungen angegeben werden. Diese sind in untenstehender Tabelle angegeben.

LDAP Servereinstellungen	
Host URL	IP:389 *oder* ldap://<IP>:389 *(IP ist die externe IP des der Octogate oder der DYNDNS-Eintrag, 389 der Port, der evtl. dem der Weiterleitung entspricht)* *alternativ:* ldaps://IP:636 *(bzw. der Port, der bei der Weiterleitung eingerichtet wurde)*
Version	3
LDAP Codierung	utf-8
Einträge pro Seite	
Bind-Einstellungen	
Kennwörter verbergen	nein
Anmeldename	cn=ldapbinduser_sbg,ou=_serviceaccounts,dc=musterschule,dc=schule,dc=paedml *(alles ohne Leerzeichen!)*
Kennwort	*(Kennwort des ldapusers)*
Nutzersuche (user lookup)	
Nutzertyp	MS ActiveDirectory
Kontexte	ou=benutzer,dc=musterschule,dc=schule,dc=paedml
Subkontexte	ja
Alias berücksichtigen	Nein
Nutzermerkmal	sAMAccountName
Mitgliedsmerkmal	member
Mitgliedsattribut nutzt dn	*(leer)*
	Kennwort
Kennwortänderung verlangen	
Kennwortänderung verlangen	nein
Standardseite zur Kennwortänderung nutzen	nein
Kennwortformat	Reiner Text
URL zur Kennwortänderung	*(leer)*
Gültigkeitsablauf von Kennwörtern	
Gültigkeitsende	no

Warnung zum Gültigkeitsende	10
Merkmal für Gültigkeitsende	*(leer)*
GraceLogins	nein
Merkmal für GraceLogin	*(leer)*
Nutzereinstellung aktivieren	
Nutzer extern anlegen	nein
Kontext für neue Nutzer	*(leer)*
Kursersteller/in	
Kursverwalter/innen	ou=Lehrer,ou=Benutzer,dc=musterschule,dc=schule,dc=paedml *(oder eben eine andere Gruppe, die Kurserstellerrechte erhalten soll)*
Cron-Synchronisierungsskript	
Entfernte externe Nutzer	nur intern zugänglich
NTLM SS	
Aktivieren	nein
Subnet	*(leer)*
MS IE fast path?	nein
Authentifikationsart	NTLM
Entfernter Nutzerdatenformat	*(leer)*
Datenzuordnung	
Vorname	givenName
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	bearbeitbar *(Hinweis: hier kann man auch "Gesperrt" angeben, dann können die Nutzer ihren Namen im Profil nicht ändern, was durchaus Sinn machen kann)*
Nachname	sn
lokal aktualisieren	beim Anlegen
extern aktualisieren	nie
Feld sperren	bearbeitbar *(Hinweis siehe Vorname)*
ID-Nummer	distinguishedName *(braucht man nur, wenn man AD-Gruppen automatisch Kursen zuweisen möchte)*

2.3.3. Hinweise

- Für die Authentifizierungsmethode müssen Sie nun eine Wahl treffen. War die Authentifizierungsmethode vorher "Manuelle Zugänge" läuft erst einmal alles weiter wie bisher, da die Authentifizierungs-Plugins von oben nach unten abgearbeitet werden. Verlief die Authentifizierung vorher emailbasiert, dann muss man sich entscheiden, in welcher Reihenfolge man die Authentifizierungsmethoden in der Übergangsphase bis zur kompletten Umstellung anordnen möchte.
- Bei jedem Anmelden eines Benutzers fragt der Moodleserver beim paedML-Server die Richtigkeit der Benutzerkennung ab. Das Kennwort wird nicht in der Moodledatenbank gespeichert. Beim ersten Anmelden werden Name und Vorname aus der Active Directory übernommen und zusammen mit den eingegebenen Profildaten in der Moodledatenbank gespeichert. Sind die Profildaten unvollständig, das heißt, fehlen Pflichtdaten wie z.B. die Mailadresse, erscheint das untenstehende Fenster, um die Daten zu ergänzen. Die Änderung der Daten muss durch eine Bestätigungsmail, die von Moodle automatisch verschickt wird, bestätigt werden. Erst danach ist ein Arbeiten in Moodle möglich.

2.4. LDAPS-Anbindung

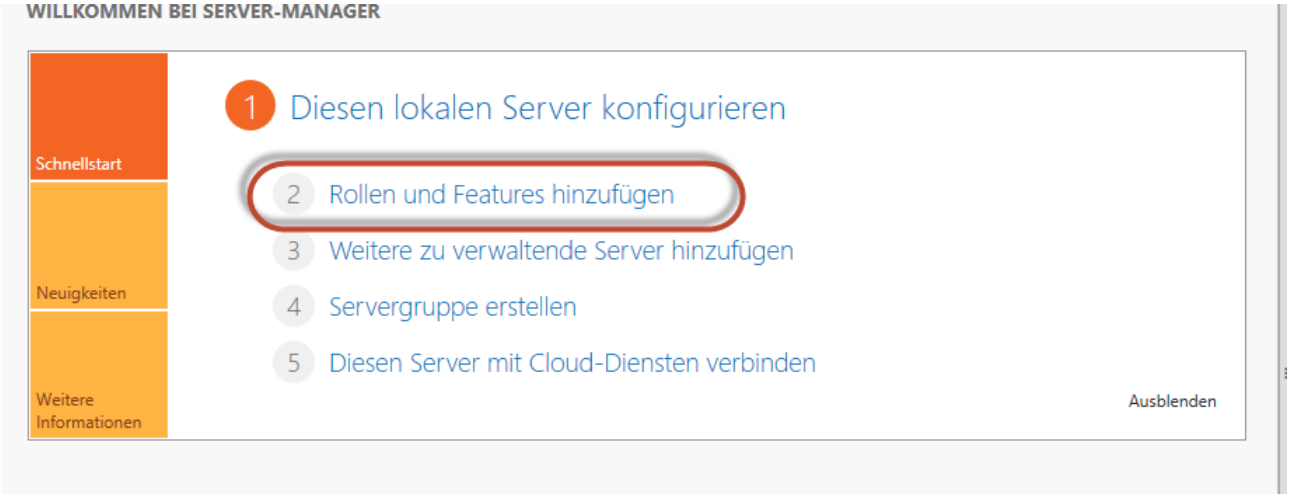
Um den verschlüsselten Austausch von LDAP-Informationen zu ermöglichen, wird das LDAPS Protokoll auf dem TCP Port 636 benötigt. Um dieses in der paedML3.x zu ermöglichen, bedarf es aber einiger Erweiterungen bzw. Änderungen am System über die bereits Beschriebenen hinaus. Im Einzelnen sind dies:

1. Rollenerweiterung von DC01
2. Zertifikatsimport

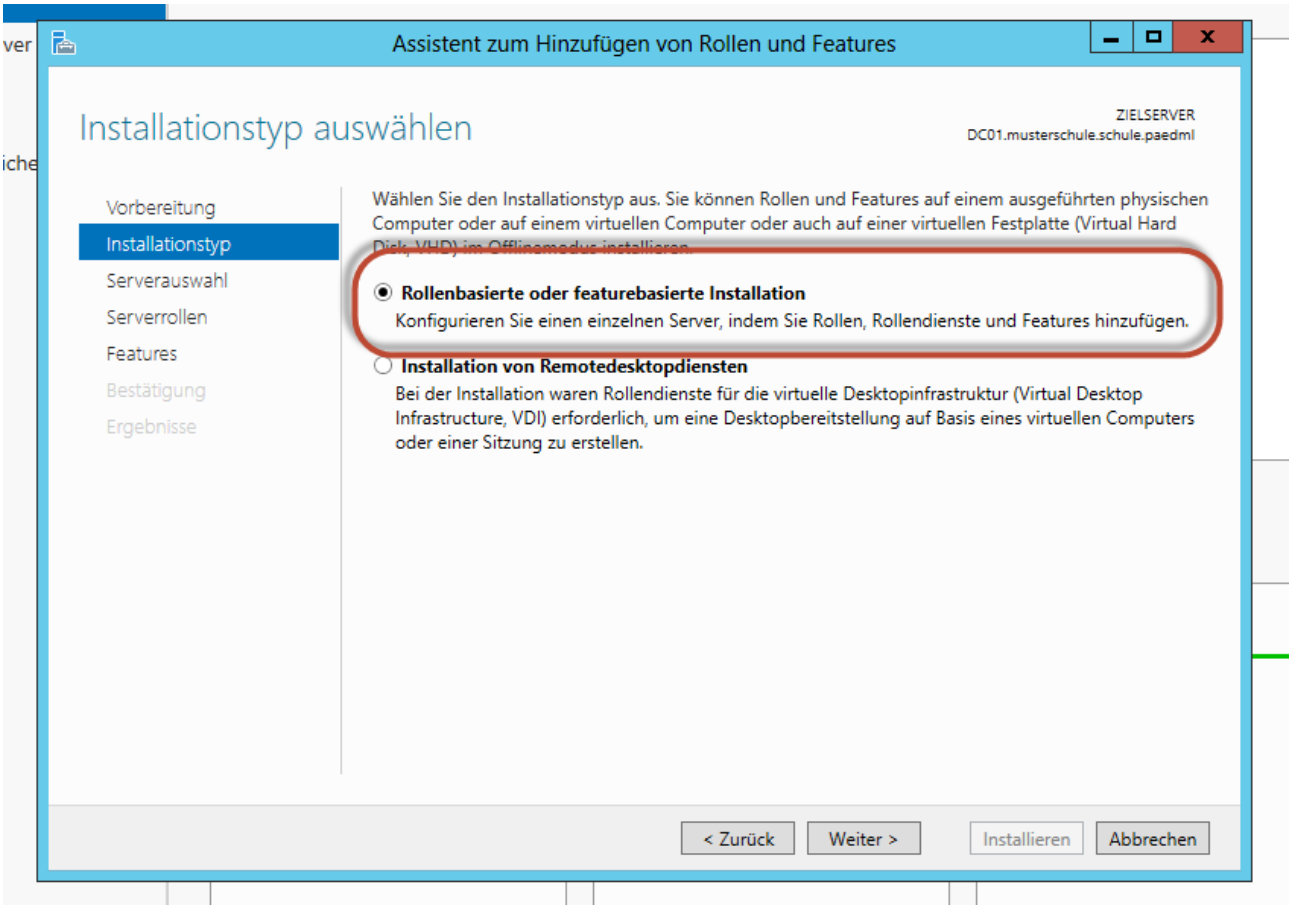
2.4.1. Rollenerweiterung von DC01

Um die Funktionalität von LDAPS zu aktivieren, muss dem Domänencontroller die SSL gesicherte Funktionalität zur Verfügung gestellt werden. Dazu muss dem das ActiveDirectory verwaltenden Windows Server 2012 DC01 die Rolle der AD-Zertifizierungsstelle hinzugefügt werden.

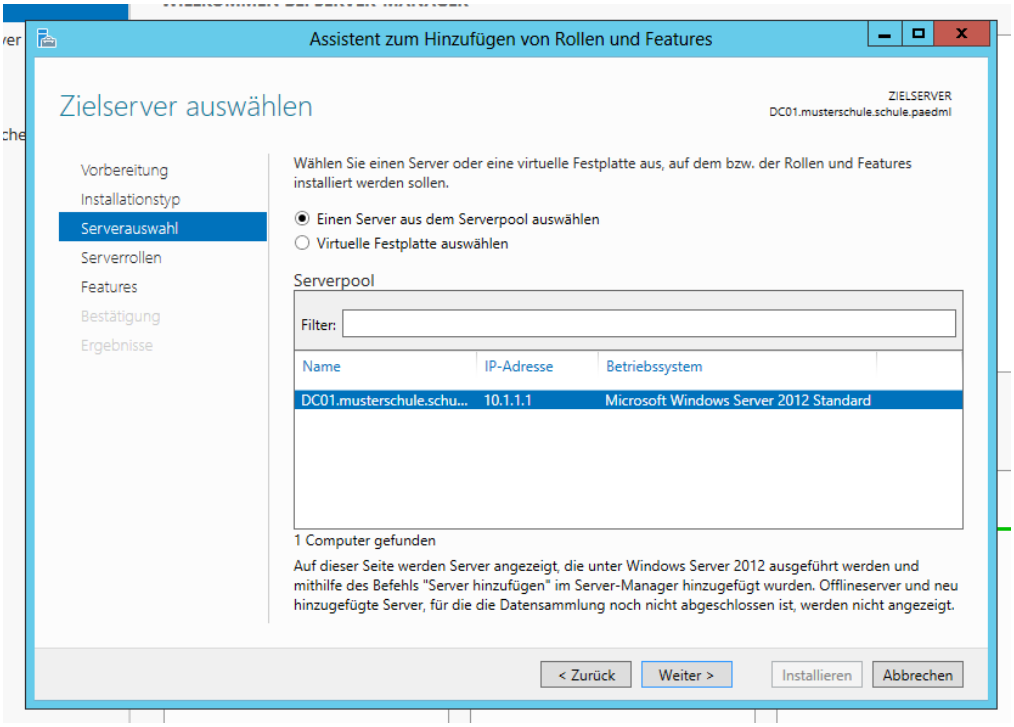
Dazu gehen Sie im Server Manager auf Rollen und Features hinzufügen.



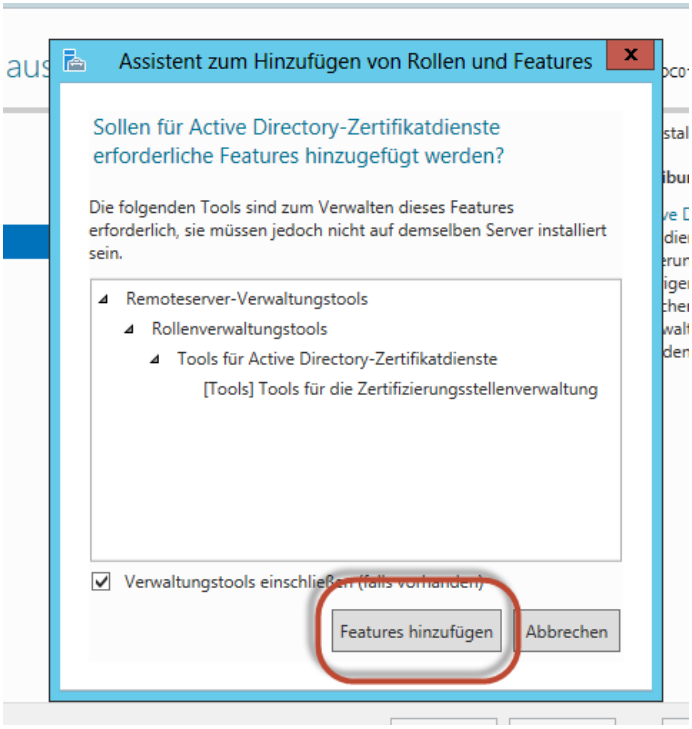
Wählen Sie den ersten Radiobutton zur Rollenbasierten oder featurebasierten Installation aus.



Wählen Sie den Domänencontroller DC01 als Server für die AD-Zertifikatsdienste aus.

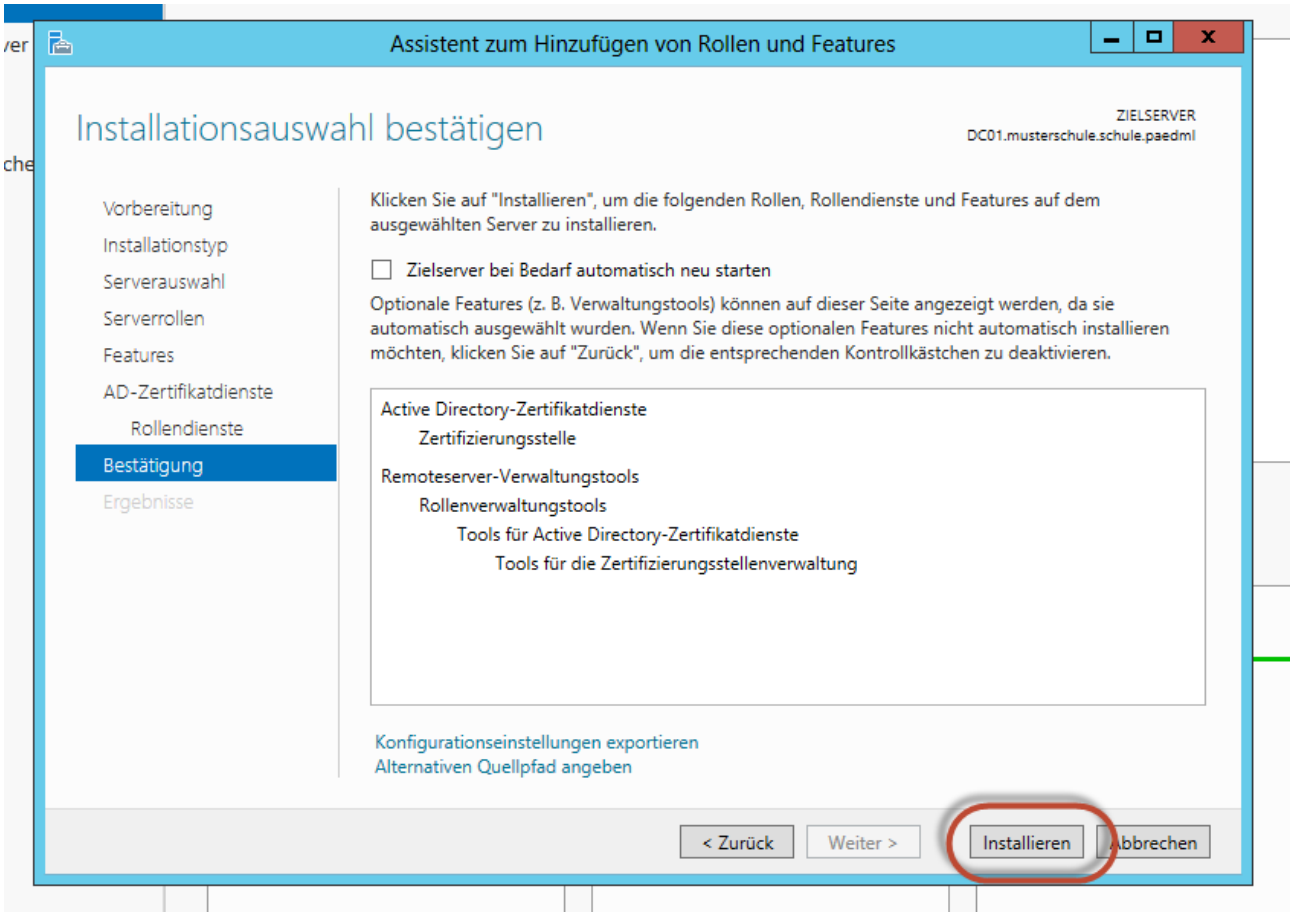


Bestätigen Sie die Auswahl durch ein Klick auf „Features hinzufügen“.



Drücken Sie abschließend auf „Installieren“. Die Installation erfolgt nun im Hintergrund, sie können das Fenster schließen. Ein erneutes Aufrufen des Server Managers bestätigt Ihnen nach kurzer Zeit den

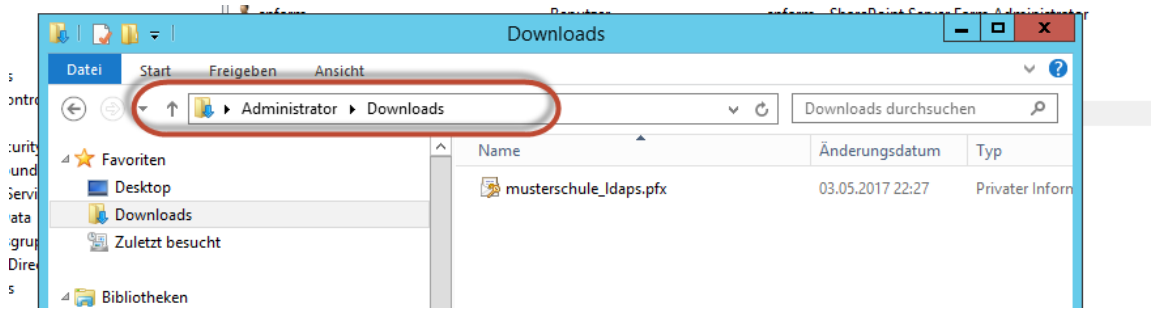
erfolgreichen Abschluss.



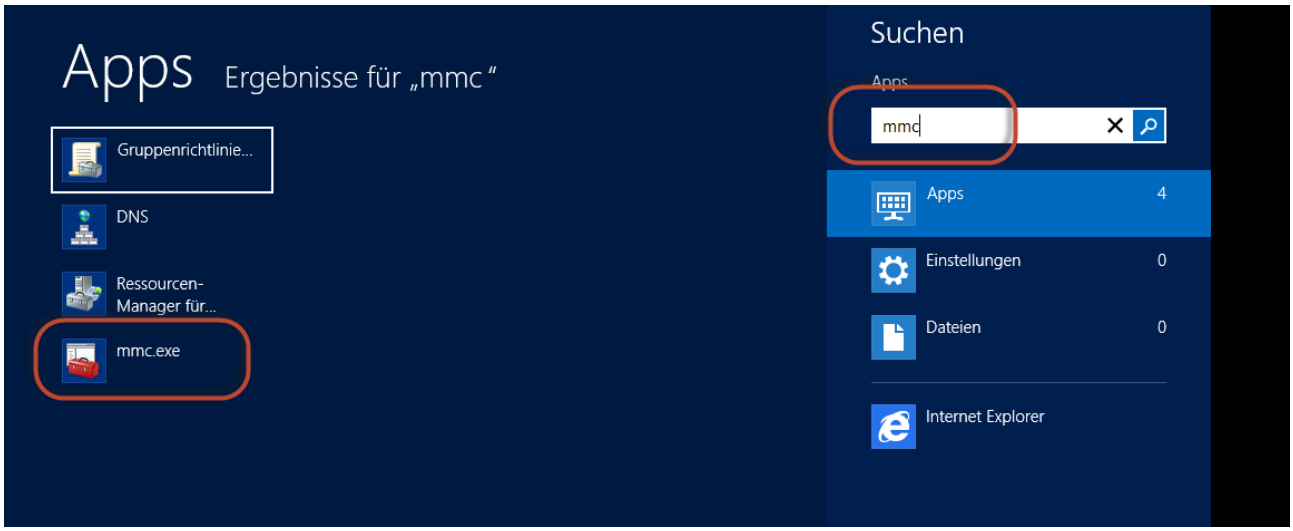
2.4.2. Zertifikatsimport

Das von Octogate[2] zur Verfügung gestellte Zertifikat „musterschule_ldaps.pfx“ wird im Folgenden im System hinterlegt und als Grundlage für die verschlüsselten LDAP Verbindungen verwendet. Dazu geht man wie folgt vor: zunächst wird die Datei auf dem Domänencontroller DC01 zwischengespeichert.

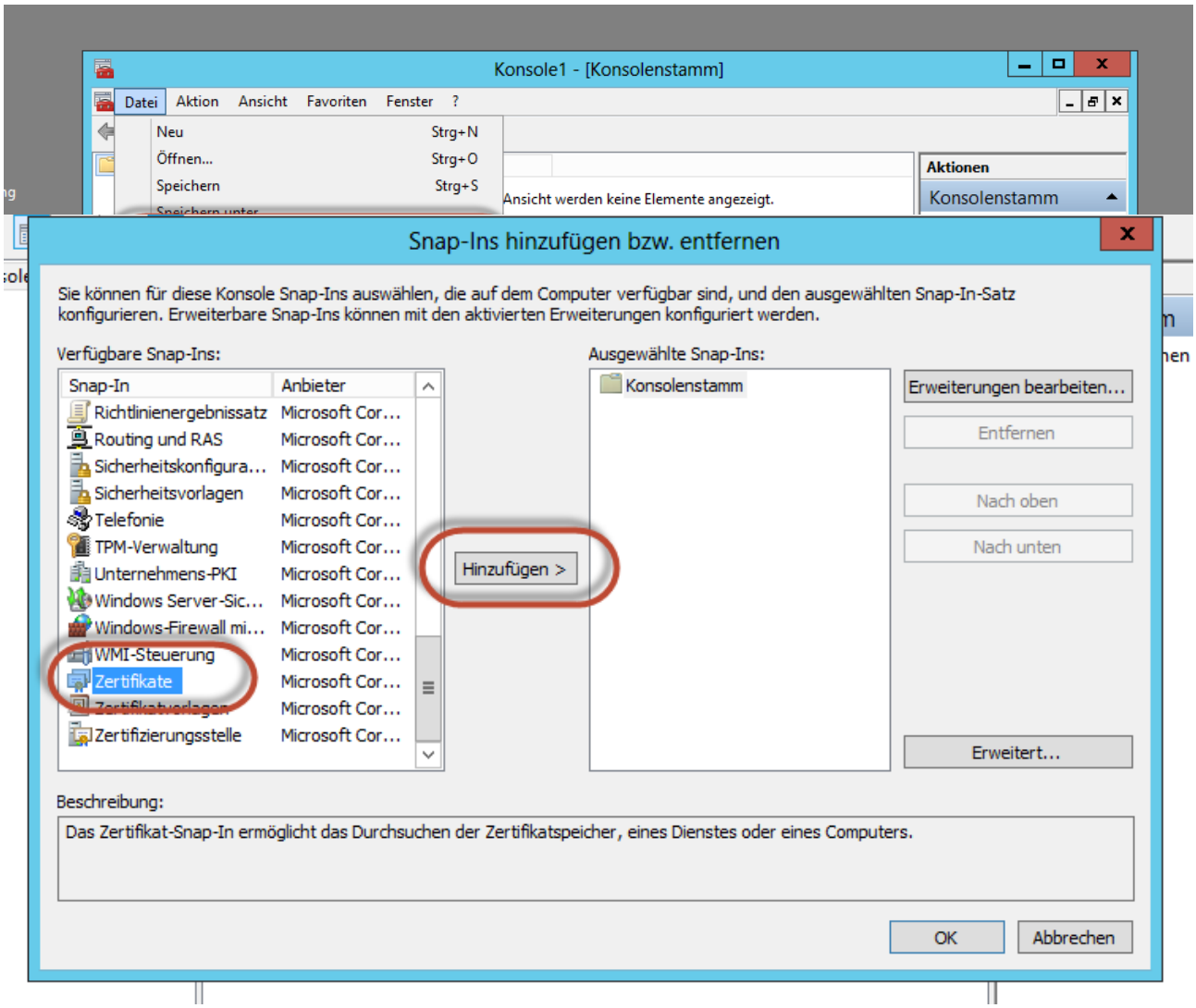
2 Das Zertifikat „musterschule_ldaps.pfx“ erhalten Sie auf Nachfrage von der Octogate Hotline.



Als nächstes muss das Zertifikat in einer Verwaltungsumgebung importiert werden. Dazu eignet sich die Microsoft Management Console (mmc), die Sie über die Windows Taste und anschließender Eingabe von „mmc“ erreichen.

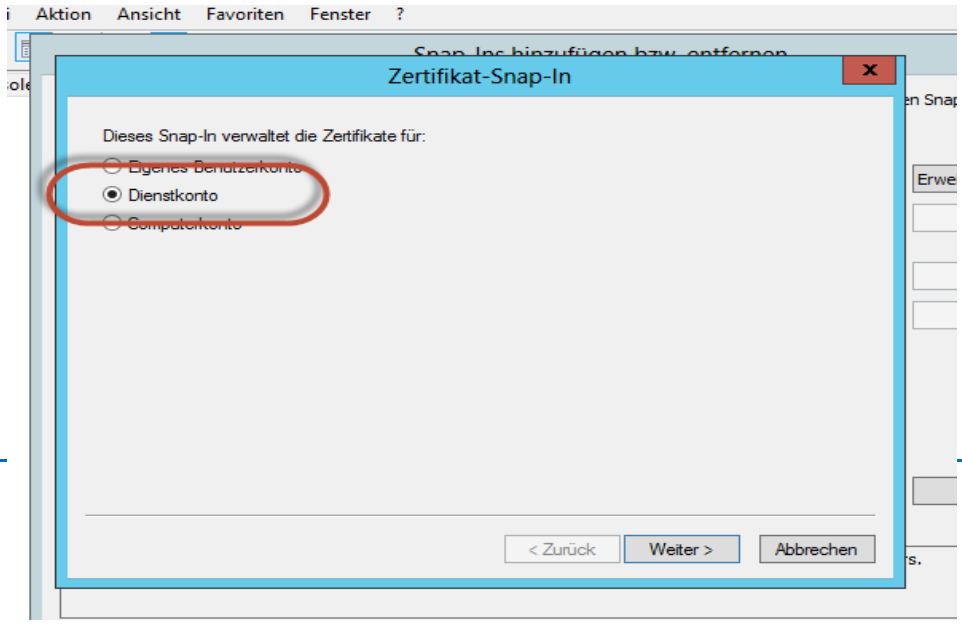


Nach Öffnen der Selbigen muss das Zertifikat Snap-In hinzugefügt werden.

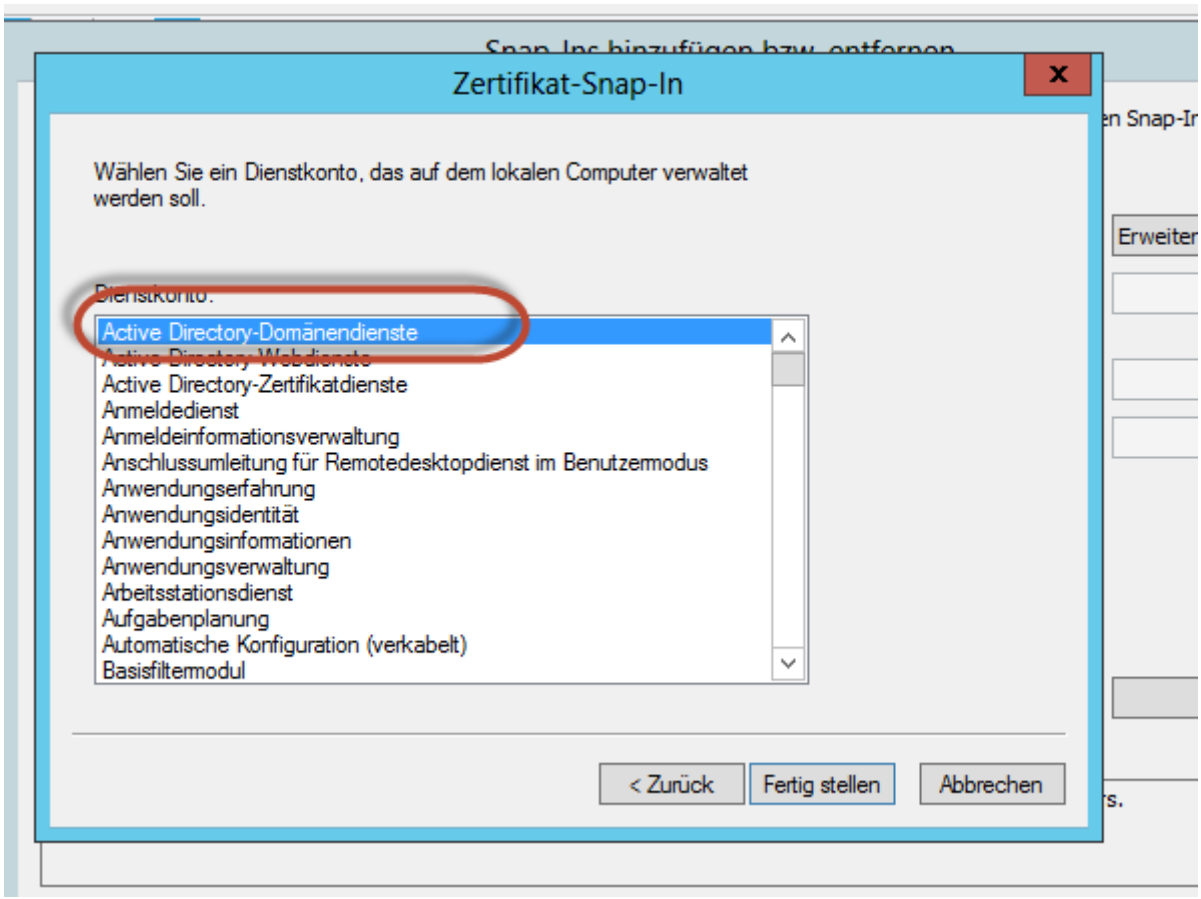


Als Snap-In wählen Sie Zertifikate aus und klicken auf OK.

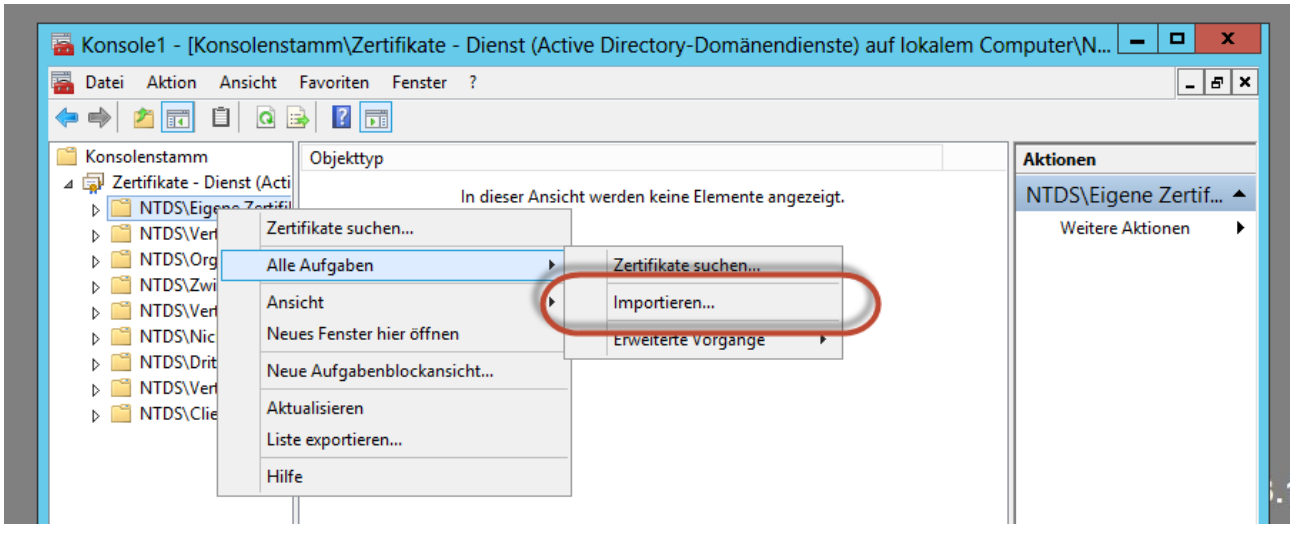
Wichtig ist das Hinzufügen als Dienstkonto, damit die Zertifikatverwaltung Benutzerunahängig funktioniert.



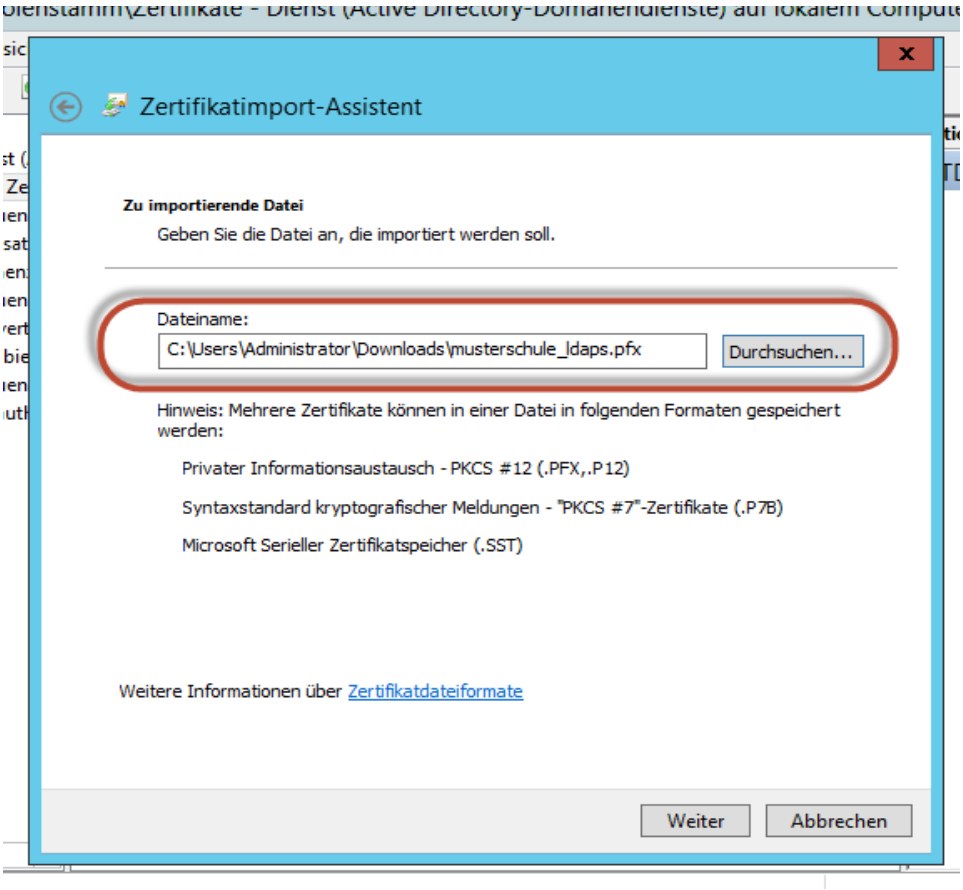
Wählen Sie die Active Directory-Domänendienste als Dienstkonto aus und schließen Sie das Hinzufügen des Snap-Ins ab.



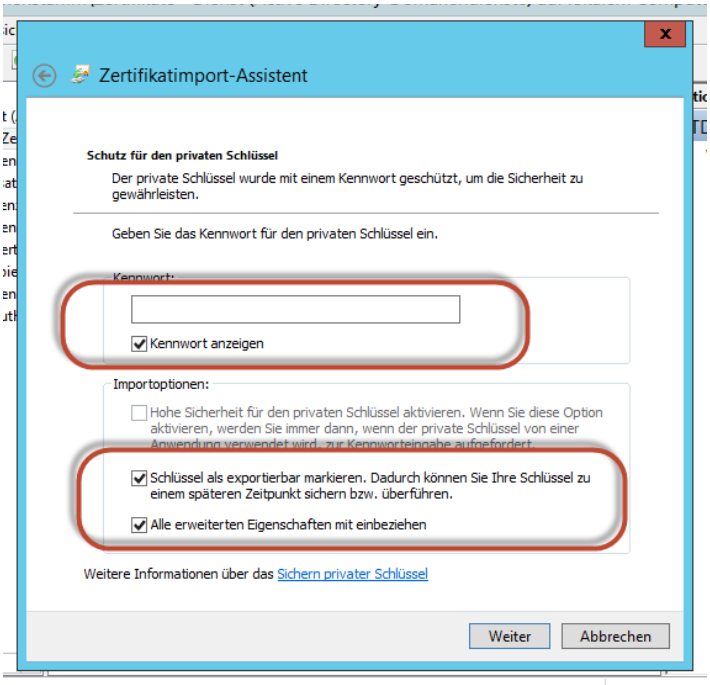
Im nächsten Schritt importieren Sie im neuen Reiter Zertifikate der MMC das Octogatezertifikat



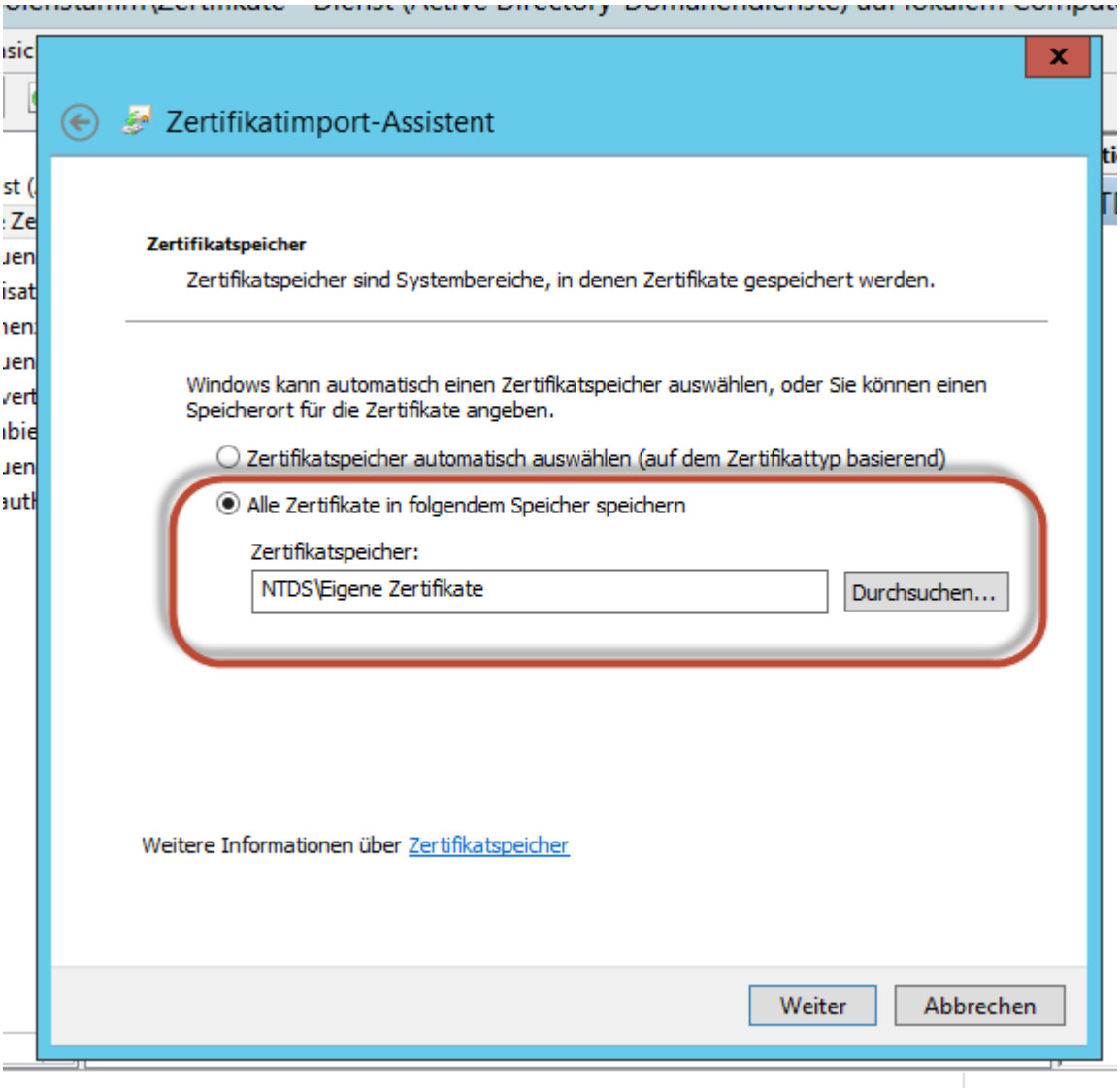
Als Quelle wählen Sie die oben abgelegte Datei mit dem entsprechenden Speicherort.



Der private Schlüssel für die Musterschule ist ein leeres Passwort, der zweite Reiter sollte aktiviert werden.



Abschließend legen Sie den Zertifikatsspeicher fest.



Damit ist das Importieren des Zertifikats und die interne Einrichtung von LDAPS abgeschlossen.

Nun lässt sich nach Erstellen einer entsprechenden Portweiterleitung wie bereits oben beschrieben durch eine gesicherte Verbindung zwischen dem externen Dienst (z.B. Moodle) und dem lokalen Domänencontroller der Schule aufbauen.