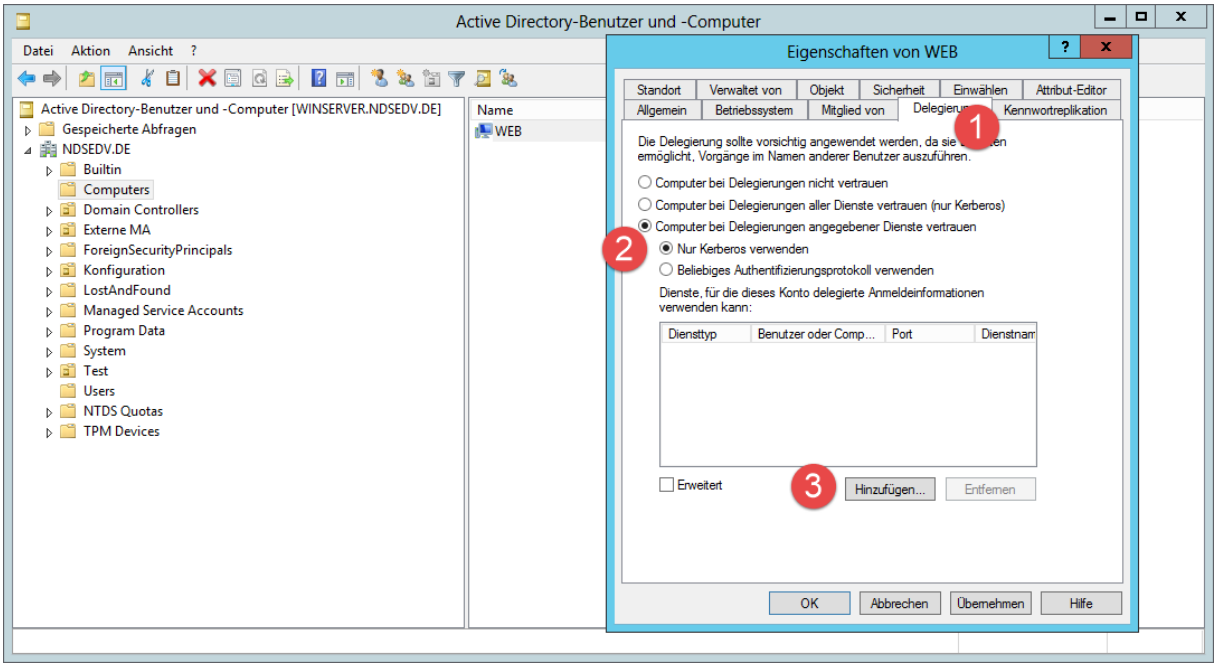
SPN und Kerberos Delegierung

Das Ziel ist die Delegierung einer Berechtigung auf ein weiteres System zur Ausführung einer Funktion (Dienst oder z.B. Applikation).

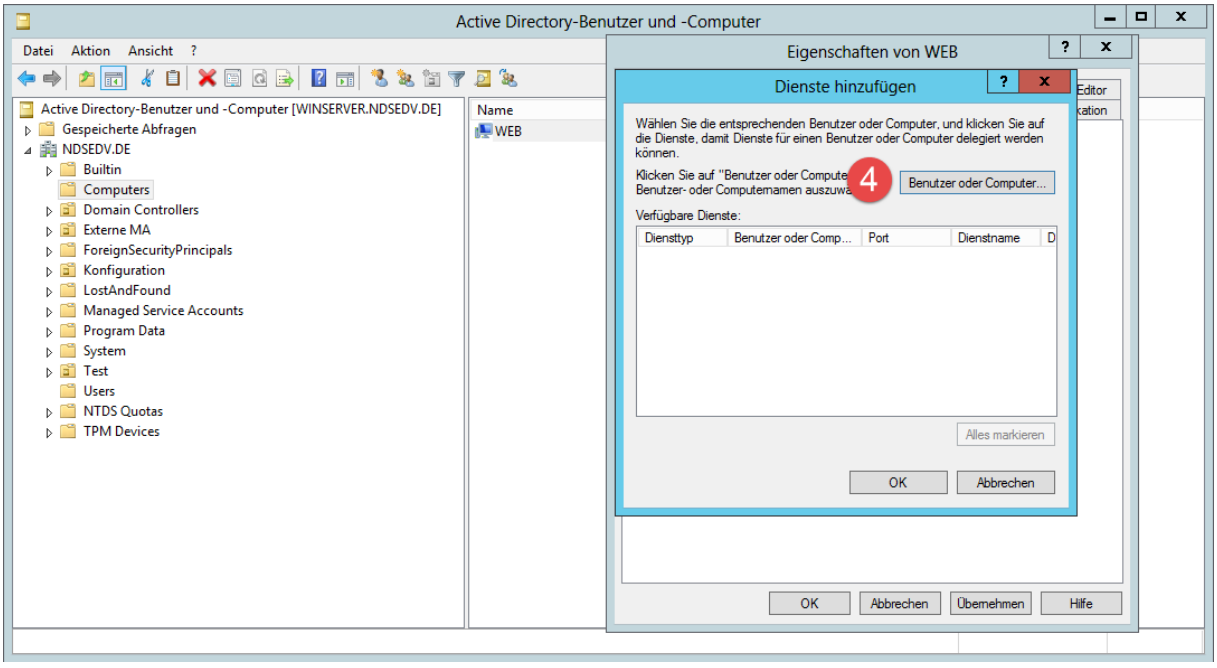
Damit Maschinen sich untereinander vertrauen bzw. Dienste weitergereicht oder genutzt werden können, ist es wichtig, dass der entsprechende Dienst auf dem Zielsystem ausgewählt und eingerichtet wird.

Computerkonten verfügen standardmäßig über den Tab Delegierung, welcher bei den Useraccounts ersteinmal aktiviert werden muss.

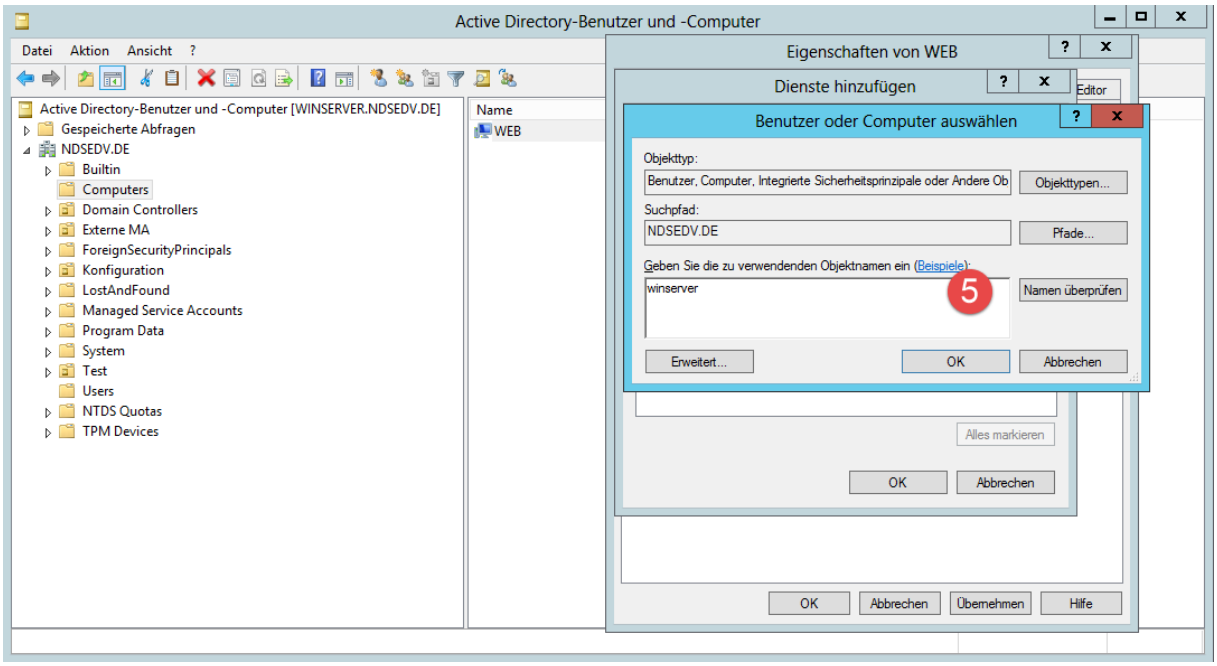
Damit die Maschine namens „Web" dem Server names „winserver" vertrauen kann gehen wir wie folgt vor. Als Beispiel kommt der Diensttyp CIFS zum Einsatz.



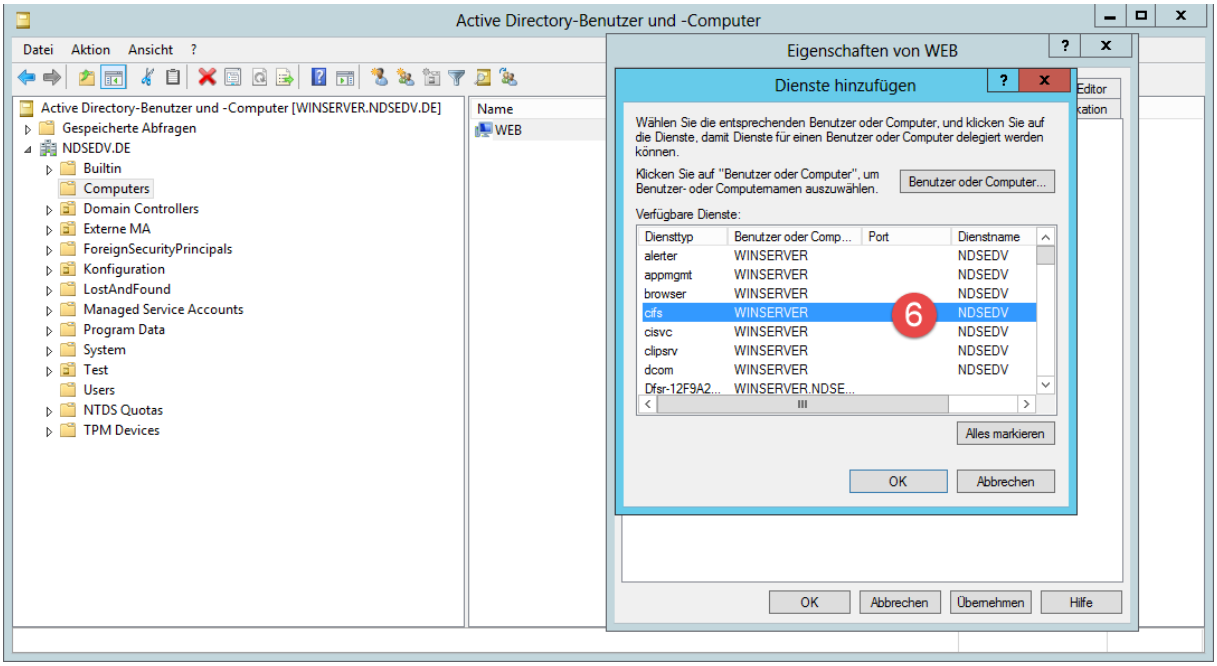
Unter beliebige Authentifizierung wird auch NTLM genutzt. Wer sicher gehen will nutzt nur Kerberos.



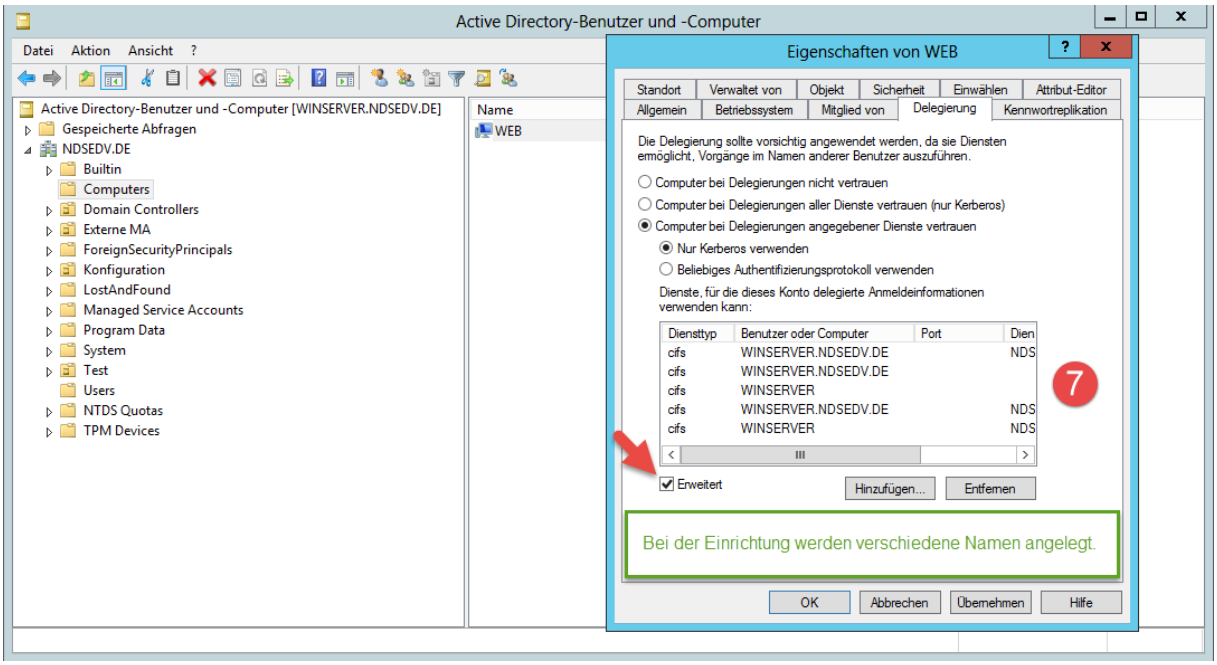
Maschine auswählen und übernehmen.



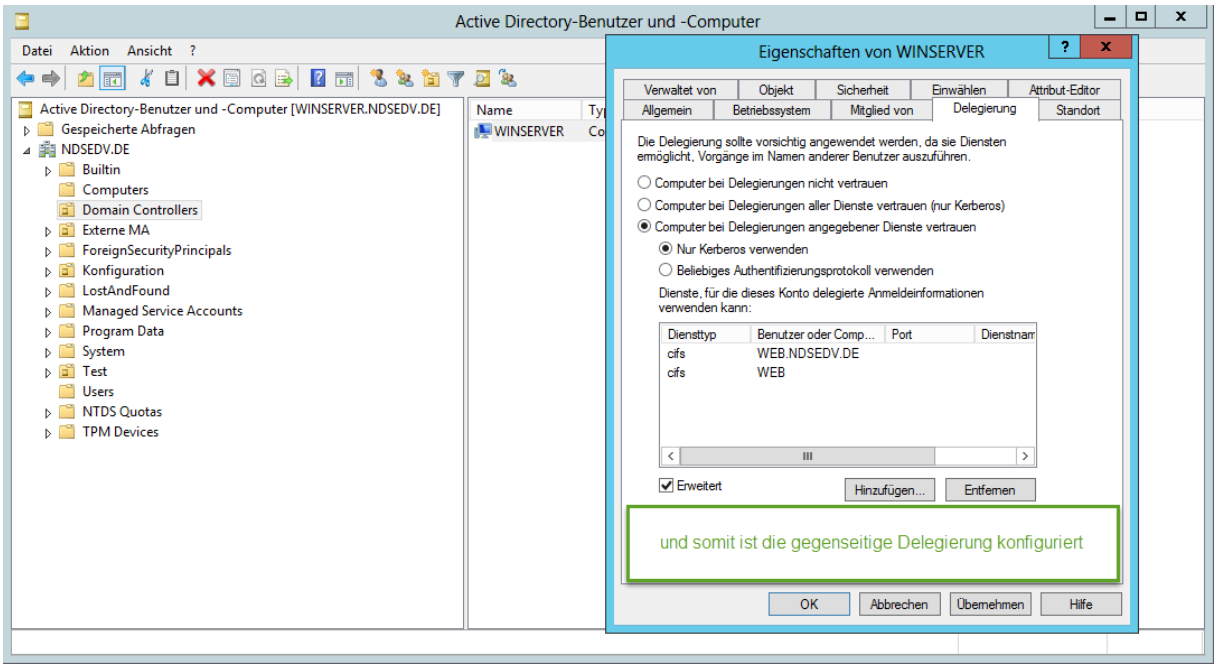
Protokoll bestimmen.



SPN und Kerberos Delegierung



Die gleiche Einrichtung muss nun auch für den „WINSERVER" vorgenommen werden.

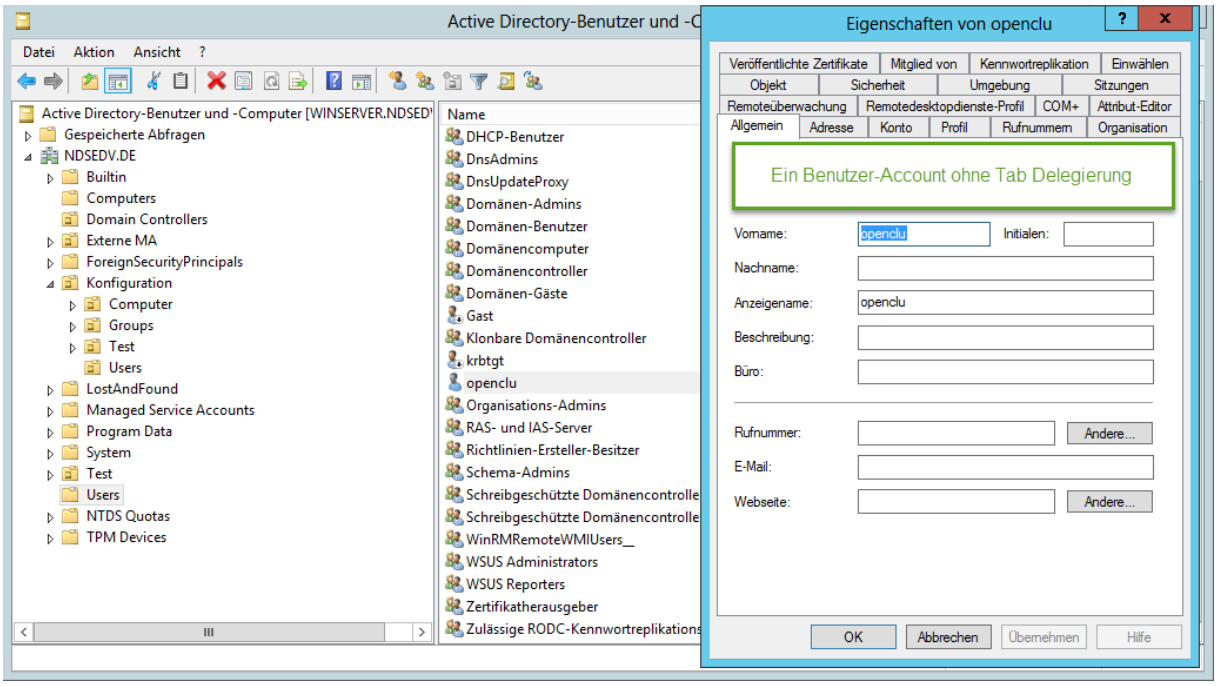


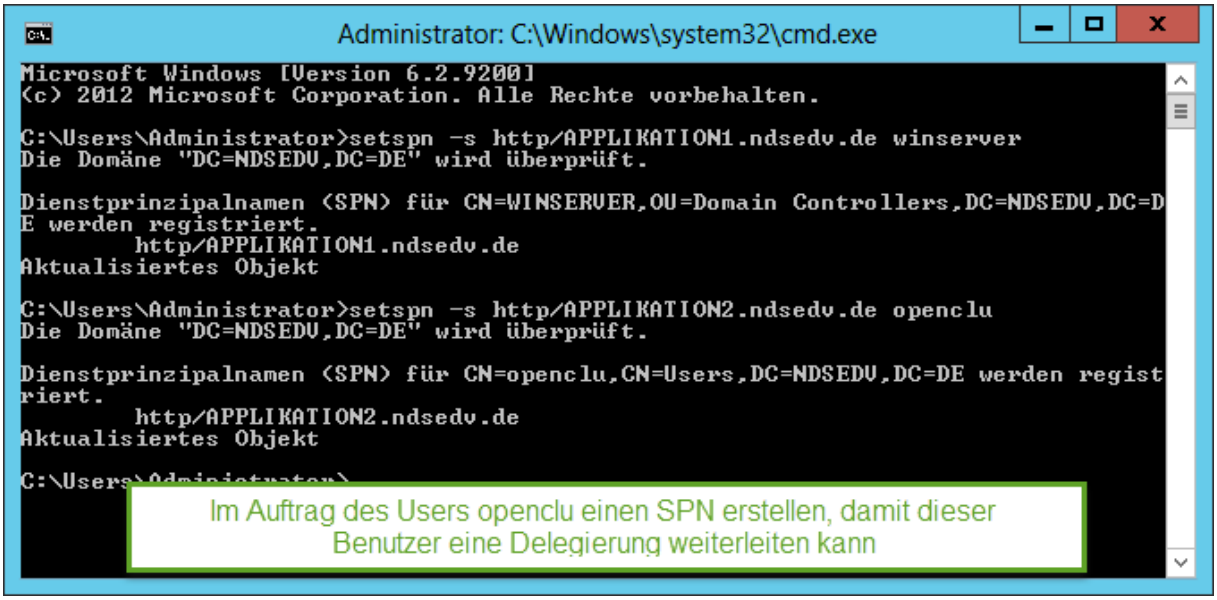
SPN und Kerberos Delegierung

Bei Useraccounts gehen wir wie folgt vor:

Damit man einem Useraccount eine Delegierung weiterleiten kann müssen wir als erstes einen SPN im Auftrag des Users openclu erstellen.

Das Ziel ist die Durchreichung einer Berechtigung an eine Applikation oder Service.

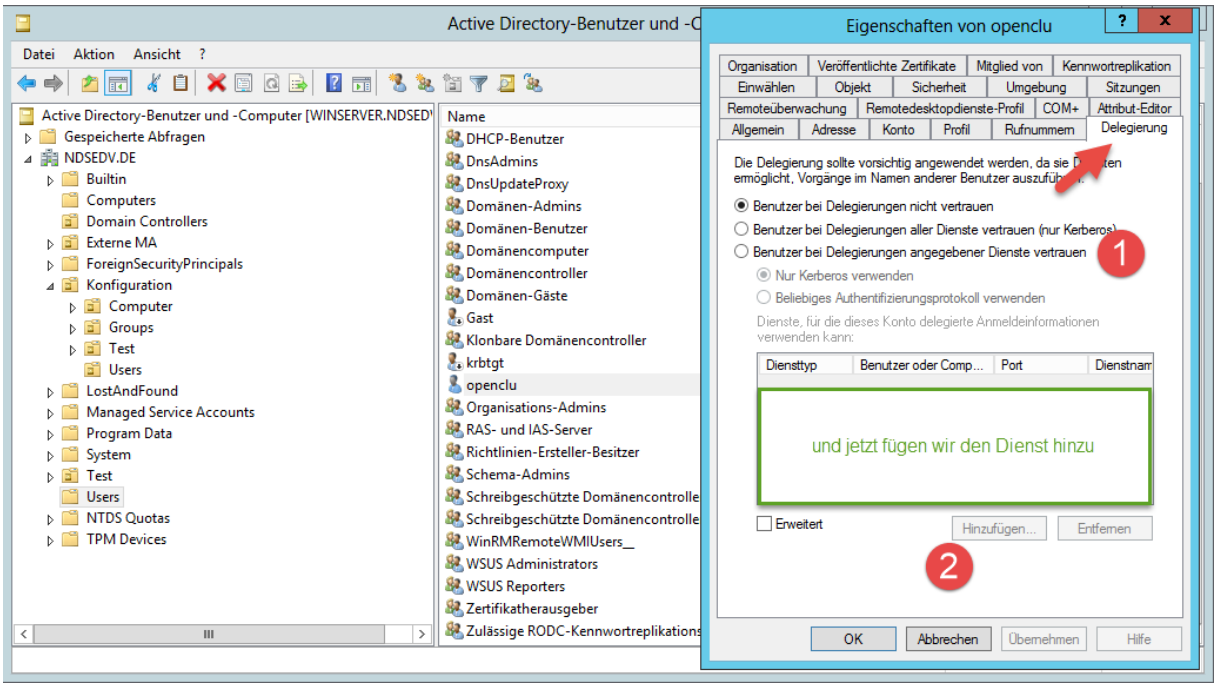




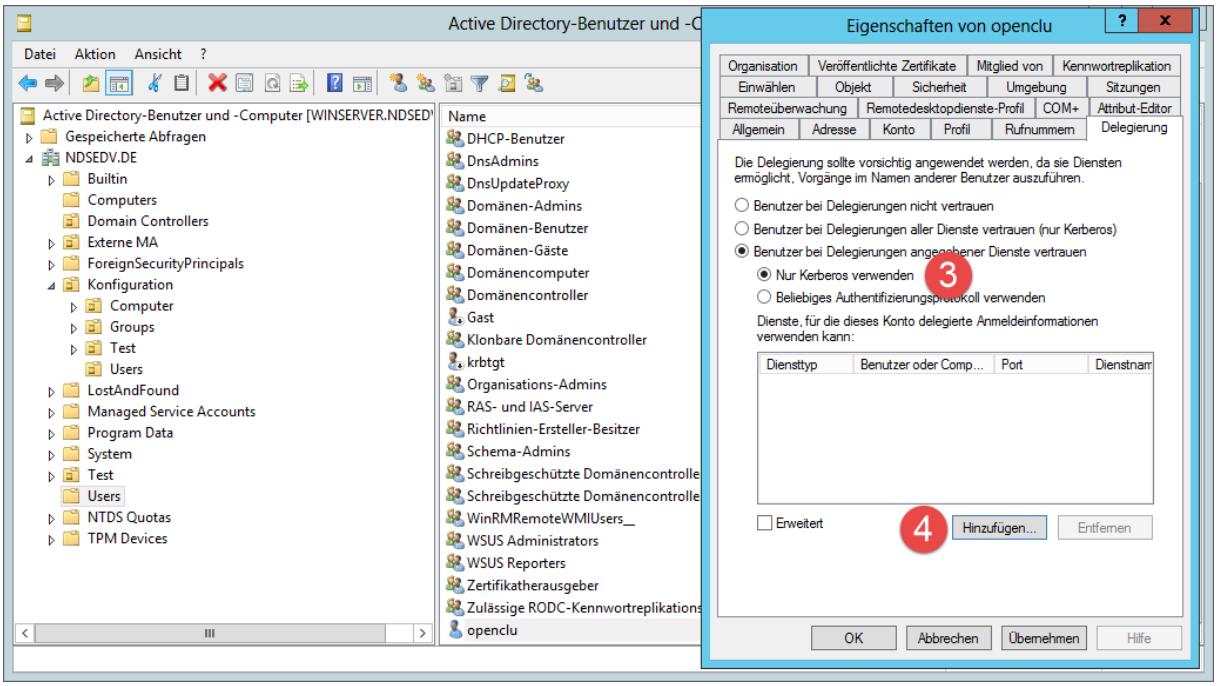
Zur Erklärung:

Der Befehl **setspn** setzt den Service Principal Namen, danach folgt das **Protokoll**, gefolgt vom **Namen der Applikation** und wo diese ausgeführt wird, in diesem Fall **winserver**. Das Gleiche gilt für einen Useraccount.

Daraufhin erscheint der Tab Delegierung.

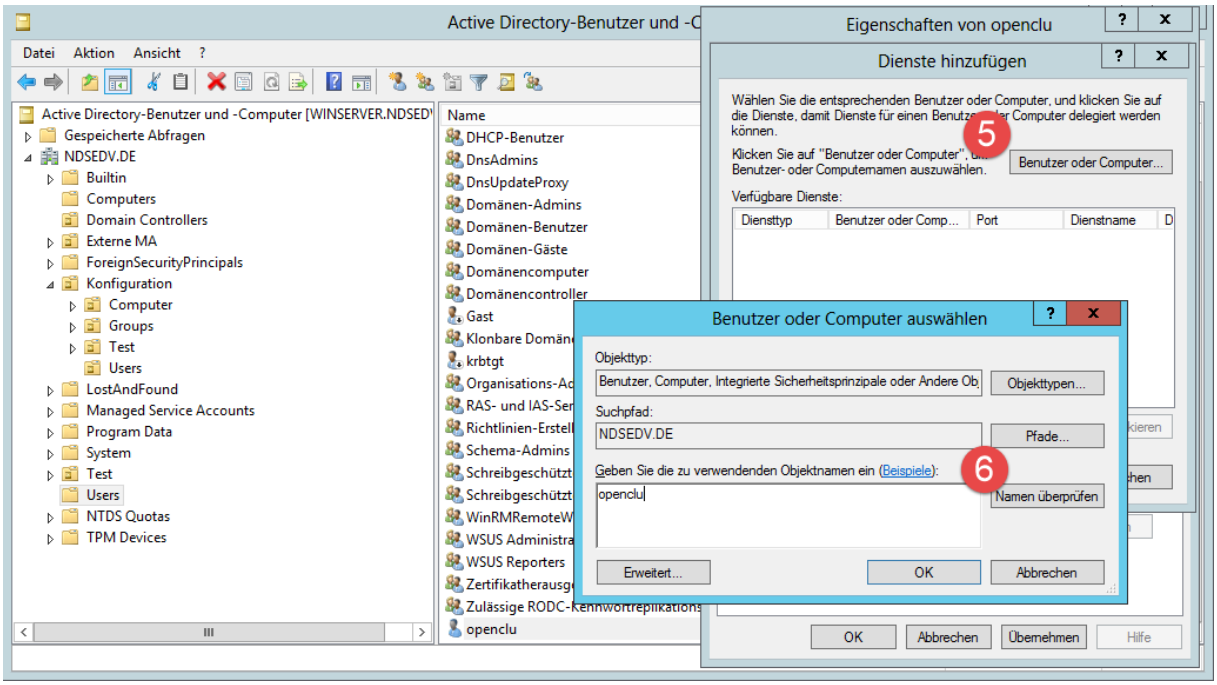


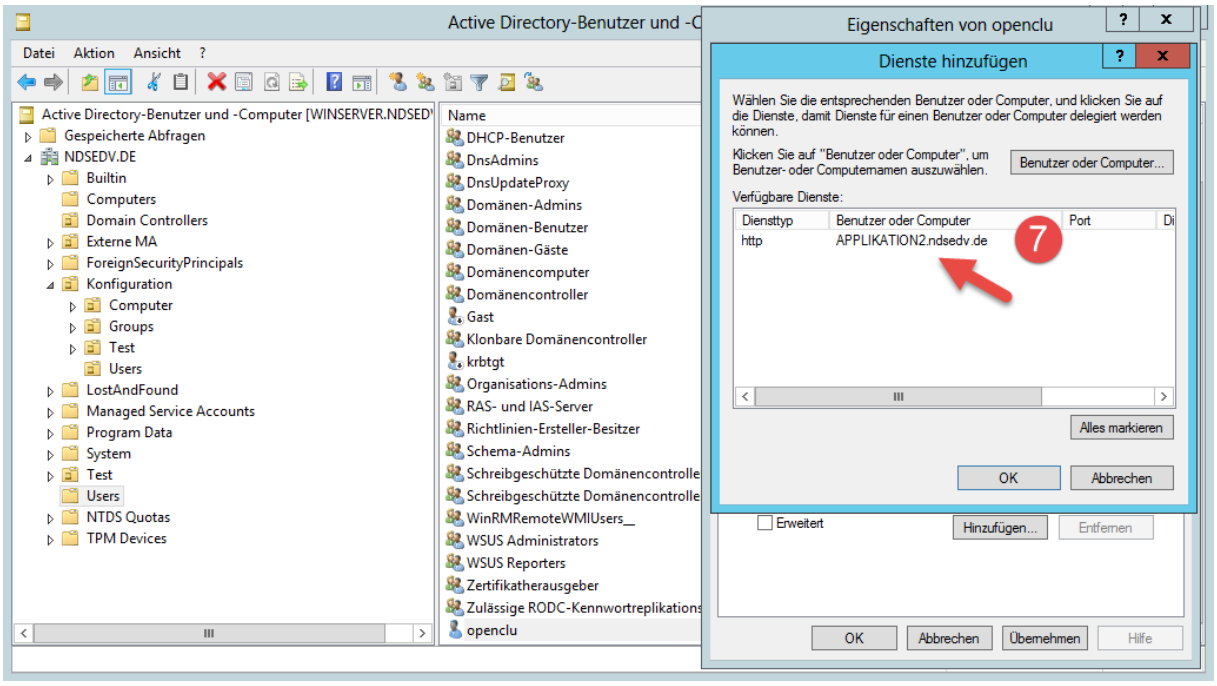
Auch hier wieder Kerberos auswählen.

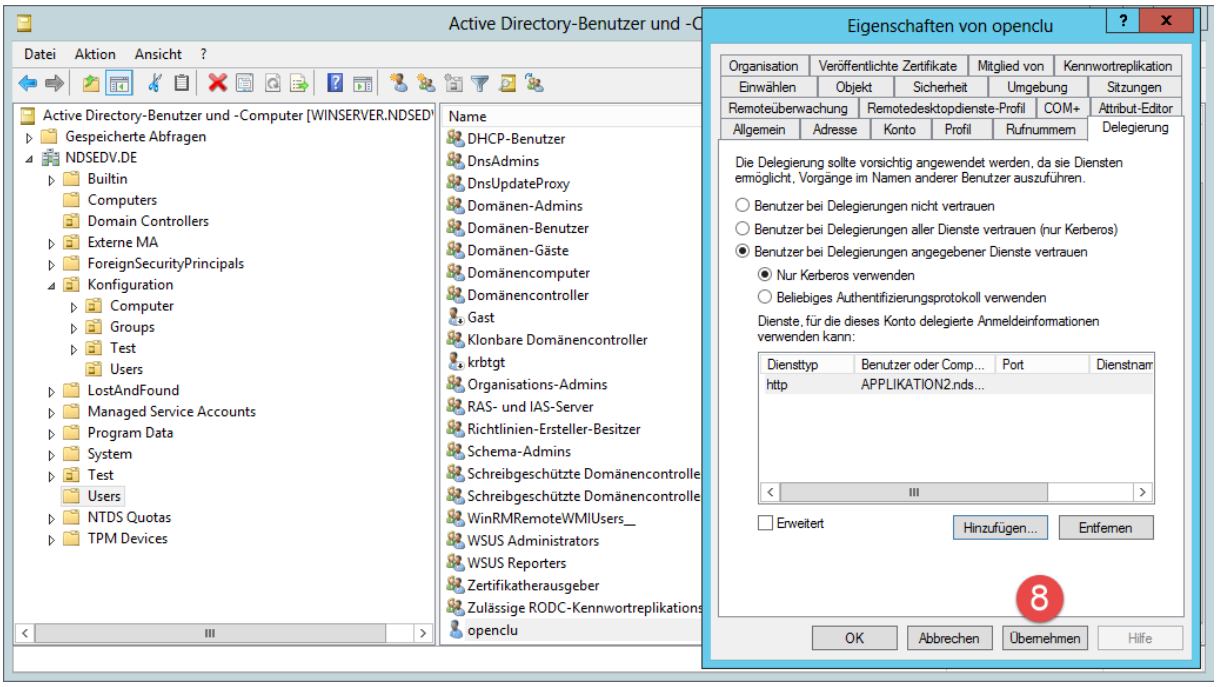


Die Delegierung muss immer an allen Objekten durchgeführt werden, die sich untereinander vertrauen sollen.

SPN und Kerberos Delegierung







Das war es auch schon.

Was ist denn nun genau ein SPN?

Also, ein Dienstprinzipalname (Service Principal Name) SPN, ist ein eindeutiger Name der eine Instanz eines Services identifiziert und ist verbunden mit dem Login-Konto unter dem die Instanz läuft.

Es stellt eine Zuordnung zwischen dem AD-Account und der Dienstinstanz her. Er besteht aus einem mehrteiligen Namensformat wie z.B. http/webserver.ndsedv.de.

Der SPN wird in den Prozess der gegenseitigen Authentifizierung zwischen einem Client und einem Server eingesetzt der einen bestimmten Dienst verwendet.

Ein SPN kann aber auch an ein Benutzer- (Dienst-) Konto verknüpft werden, wenn ein Dienst oder eine Anwendung unter diesem Benutzer ausgeführt wird.

Das würde dann z.B. so aussehen:
setspn -A HTTP/benutzer1.ndsedv.de@ndsedv.de benutzer1

Eingesetzt werden SPNs ganz stark im SQL-Server Umfeld. Dort läuft der SQL-Server-Dienst in der Regel unter einem Dienstkonto anstatt unter „LocalSystem".

Das Ganze würde dann z.B. so aussehen: MSSQLSvc/sqlsrvr.ndsedv.de:1433

Um einen Überblick über die SPNs zu bekommen, kann man den Befehl setspn –L einsetzen. Es werden einem alle registrierten SPNs aufgelistet. Der Befehl klist wäre eine Alternative.

Zur Abfrage kann aber auch LDP oder LDIFDE eingesetzt werden.