Vorbereitung des Active Directory

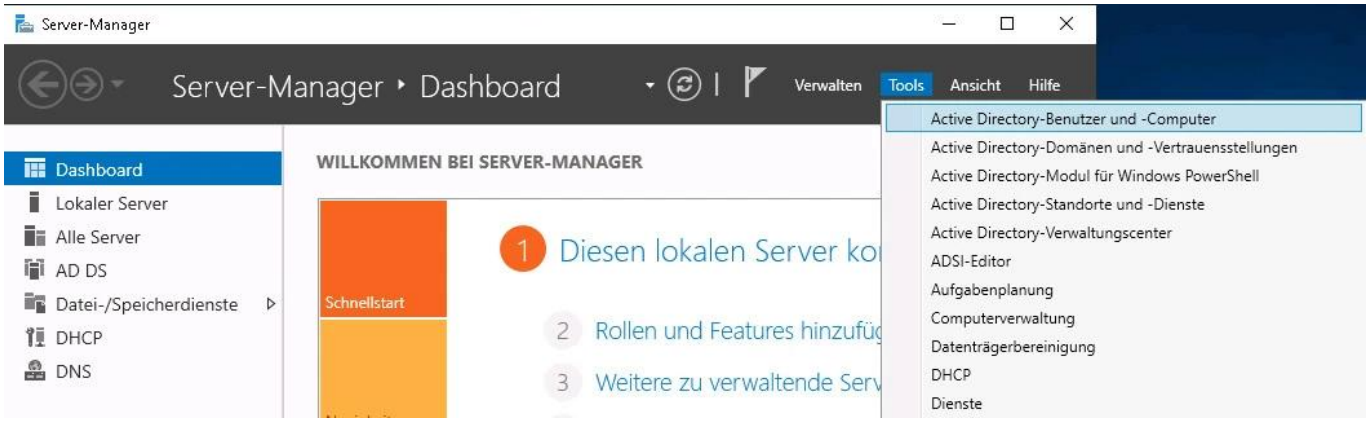
Am Active Directory (AD), welches zur Benutzerverwaltung des TightGate-Pro verwendet werden soll, sind für die Anbindung eines TightGate-Pro folgende Einstellungen vorzunehmen:

- Es ist ein Computer-Account für TightGate-Pro auf dem AD-Server anzulegen und zu konfigurieren.
- Danach ist die DNS-Einstellung vorzunehmen, damit TightGate-Pro im Netzwerk von den Klienten-PCs gefunden werden kann.
- Im nächsten Schritt ist eine Keytab-Datei für die Authentisierung des TightGate-Pro am AD-Server erzeugt.
- Im letzten Schritt sind die für TightGate-Pro notwendigen Sicherheitsgruppen im AD anzulegen.

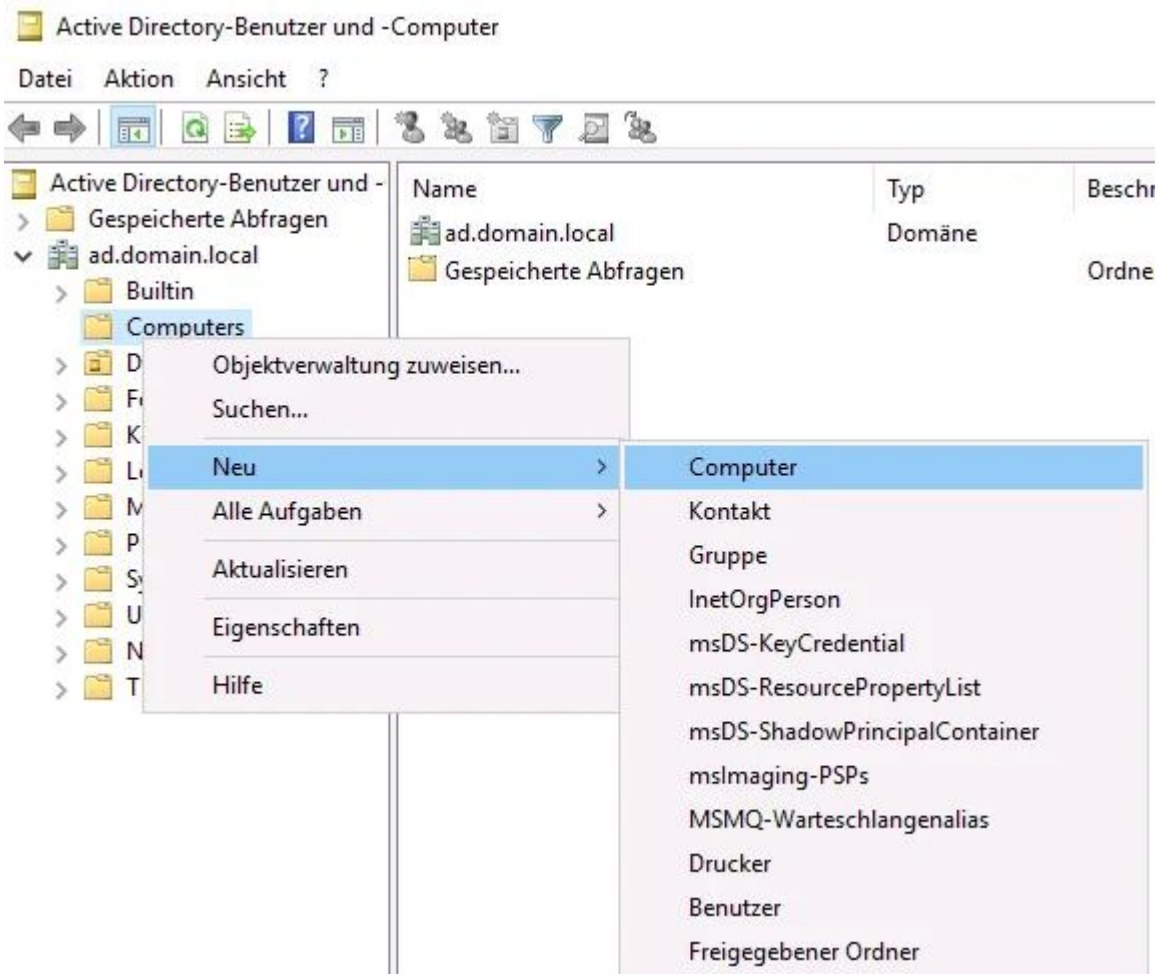
Anlegen eines Computer-Accounts

Zuerst ist auf dem AD-Server ein Computer-Account in der richtigen Domäne anzulegen. Dies gilt für Einzelsysteme wie auch für Clustersysteme gleichermaßen. In unserem Beispiel heißt der Computer-Account **tgpro**.

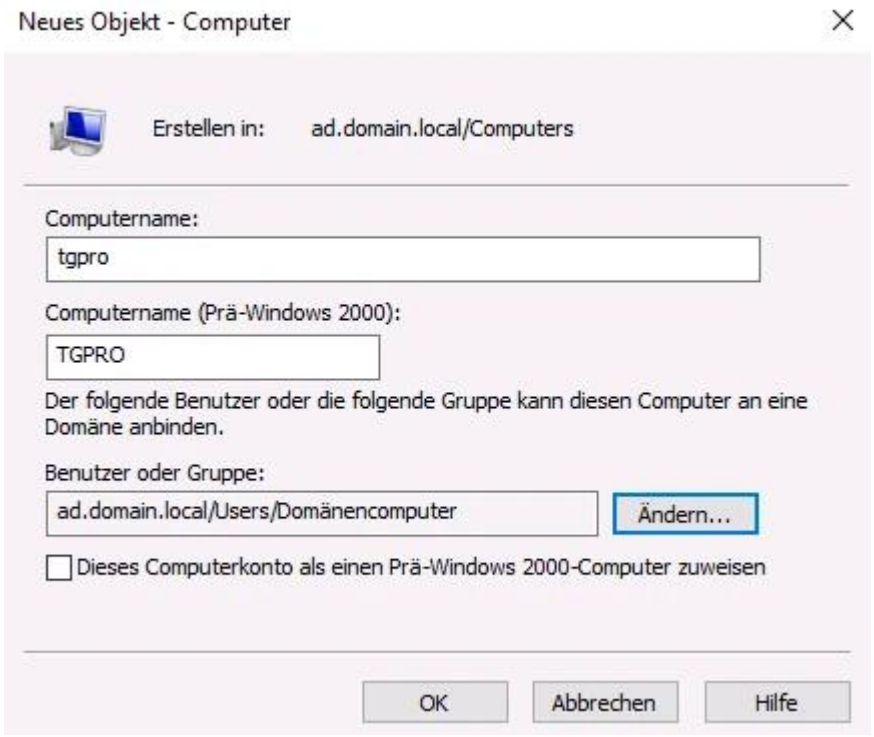
Ein Computer-Account wird im Server-Manager über den Menüpunkt **Tools > Active Directory-Benutzer und -Computer** angelegt, wie nachfolgende Abbildung verdeutlicht:



Dort ist (wie nachfolgende Abbildung zeigt) in der richtigen Domäne mit einem Rechtsklick auf **Computer** und anschließend im Kontextmenü unter **Neu > Computer** ein Dialogfenster zur Anlage eines neuen Computer-Accounts zu öffnen.

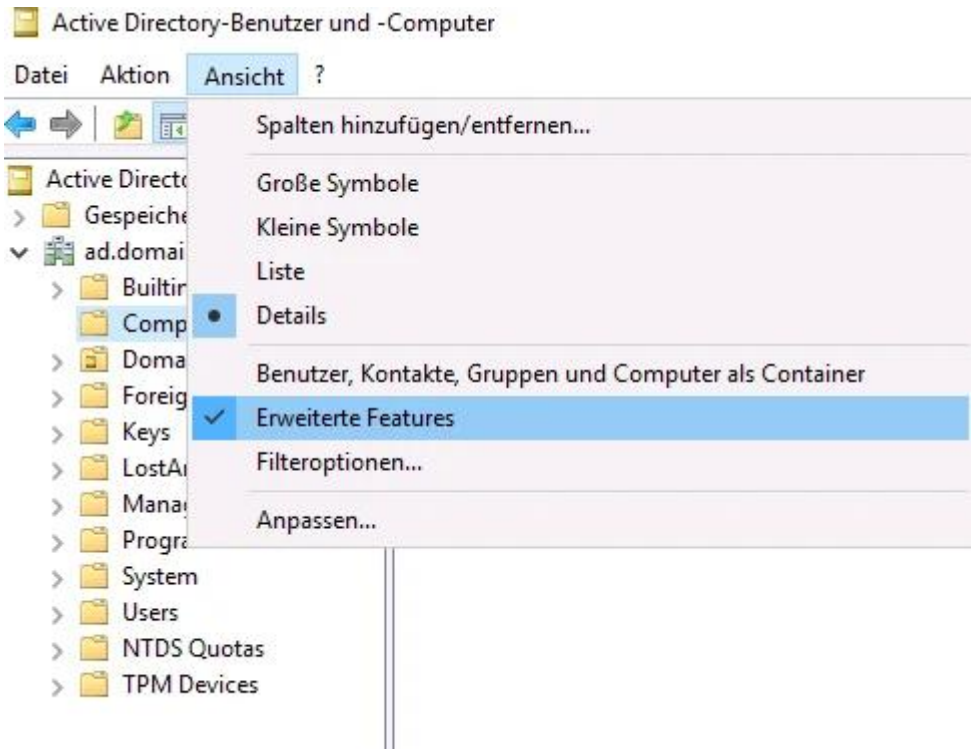


Der Name des Computer-Accounts kann frei gewählt werden, in unserem Beispiel bekommt der Computer den Namen **tgpro**.

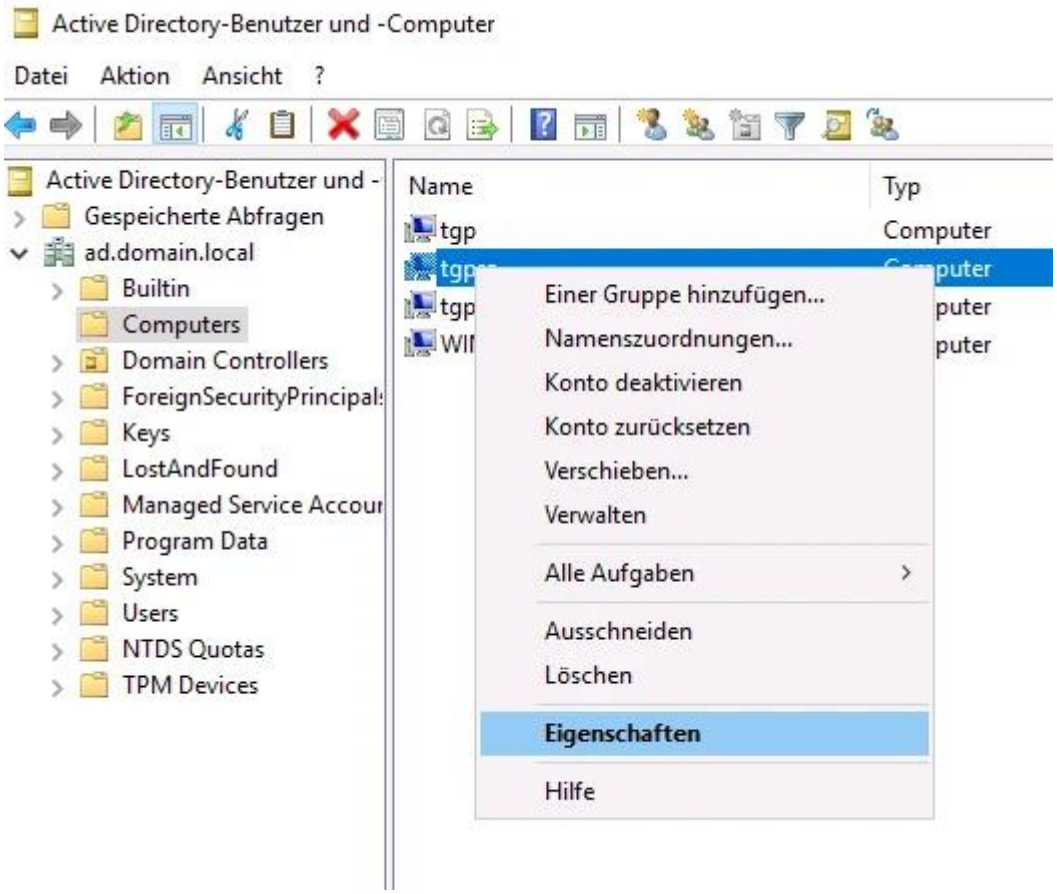


Nach der Anlage ist der Computer-Account weiter anzupassen und für die Kommunikation notwendige

Attribute zu setzen. Damit dies möglich ist, muss im Fenster **Active Directory-Benutzer und -Computer** unter **Ansicht** die Option **Erweiterte Features** ausgewählt werden.

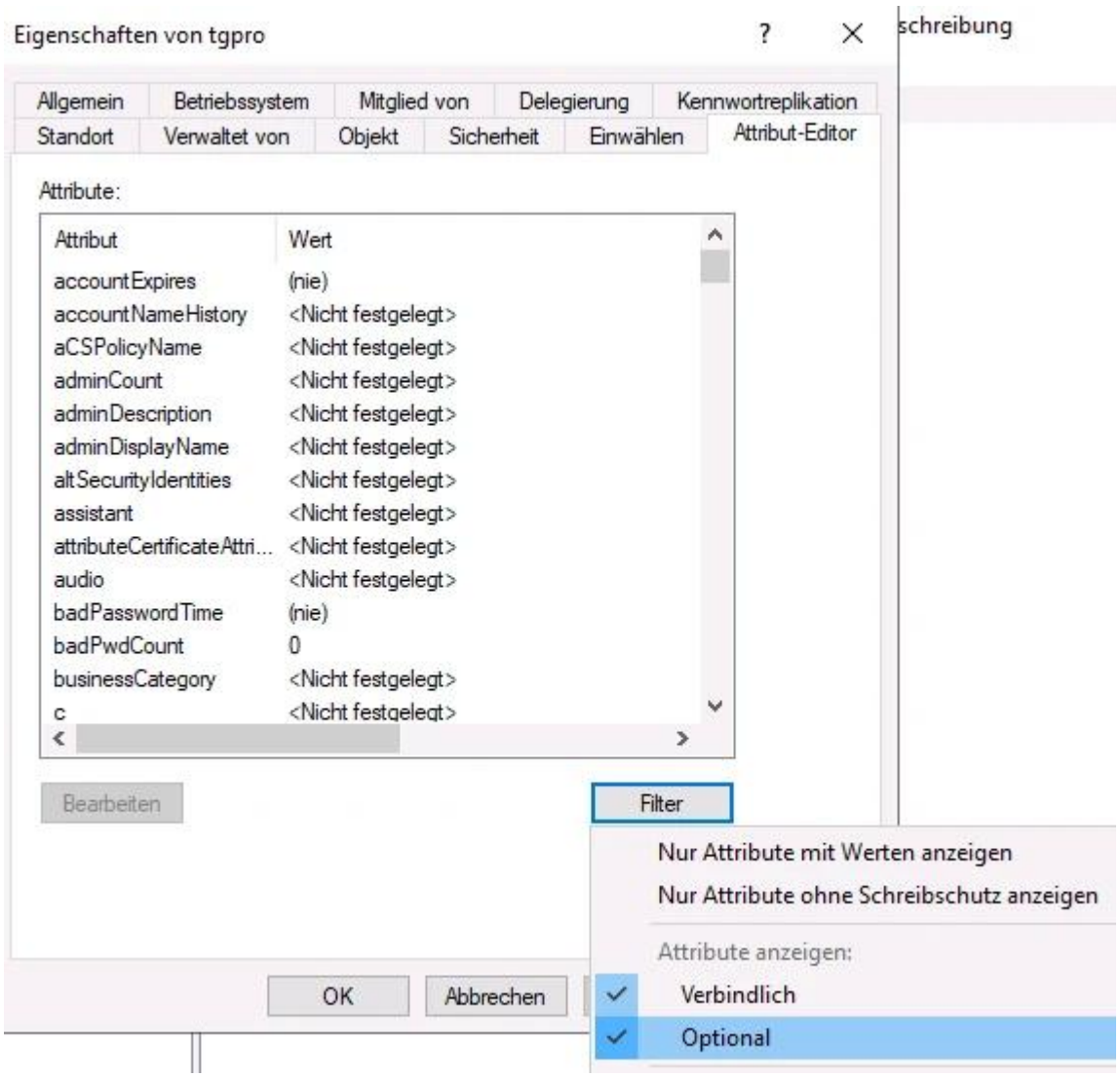


Nun ist aus der Liste der vorhandenen Computer (Computers) der neu angelegte Computer auszuwählen. Mit einem Kick der rechten Maustaste auf den Computer (in unserem Beispiel **tgpro**), öffnet das Kontextmenü, aus dem der Menüpunkt **Eigenschaften** aufzurufen ist.

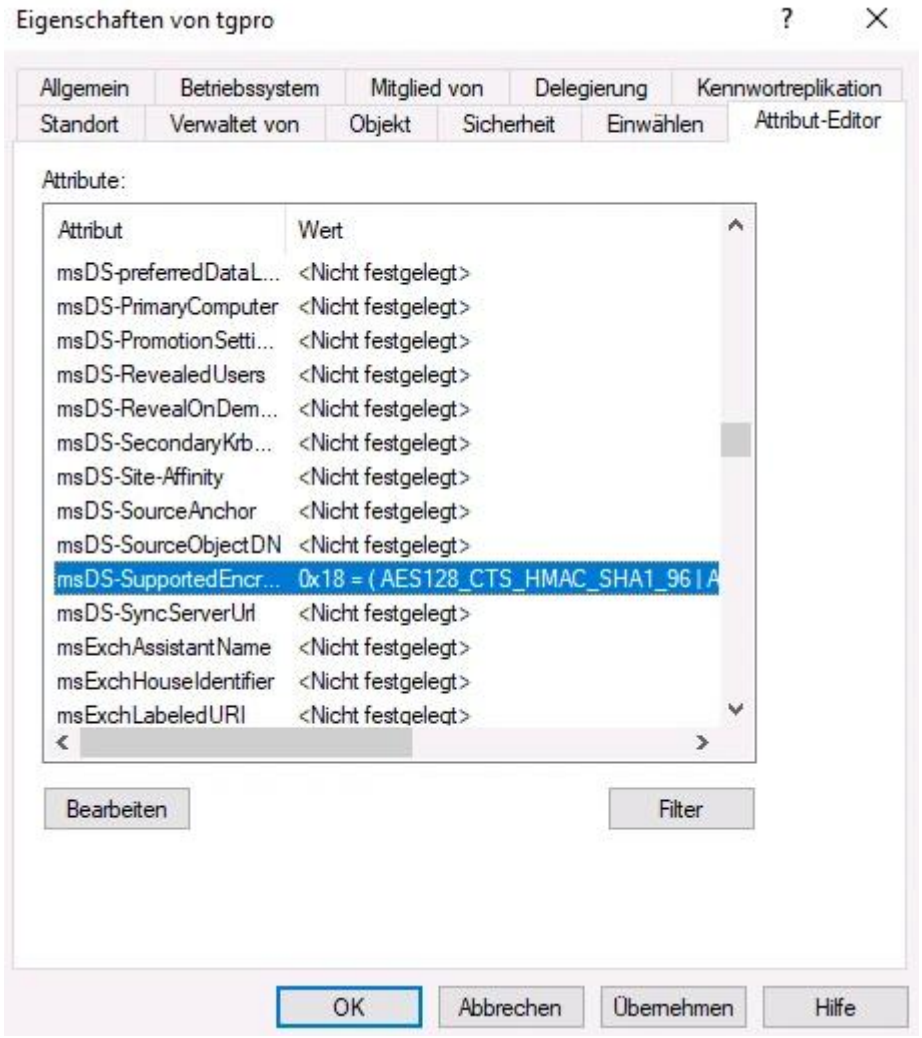


Es öffnet sich das Eigenschaften-Menü für den Computer-Account, in dem der Reiter **Attribut-Editor**

auszuwählen ist. Damit alle Attribut-Werte richtig gesetzt werden können, ist die Filter-Schaltfläche anzuklicken und sicherzustellen, dass unter **Attribute anzeigen > Optional** das Häkchen gesetzt ist.



In der Liste der Attribute ist nun das Attribut **msDS-SupportedEncryption Types** der Dezimalwert **24** (hexadezimal **0x18**) zu setzen. Hierzu wird der betreffende Parameter in der Auswahlliste durch Klick mit der linken Maustaste selektiert (farbige Unterlegung sichtbar) und mittels Klick auf die Schaltfläche **Bearbeiten** zur Änderung freigeschaltet. Ist der Wert gesetzt, so ist dieser über die Schaltfläche **Übernehmen** anzuwenden.

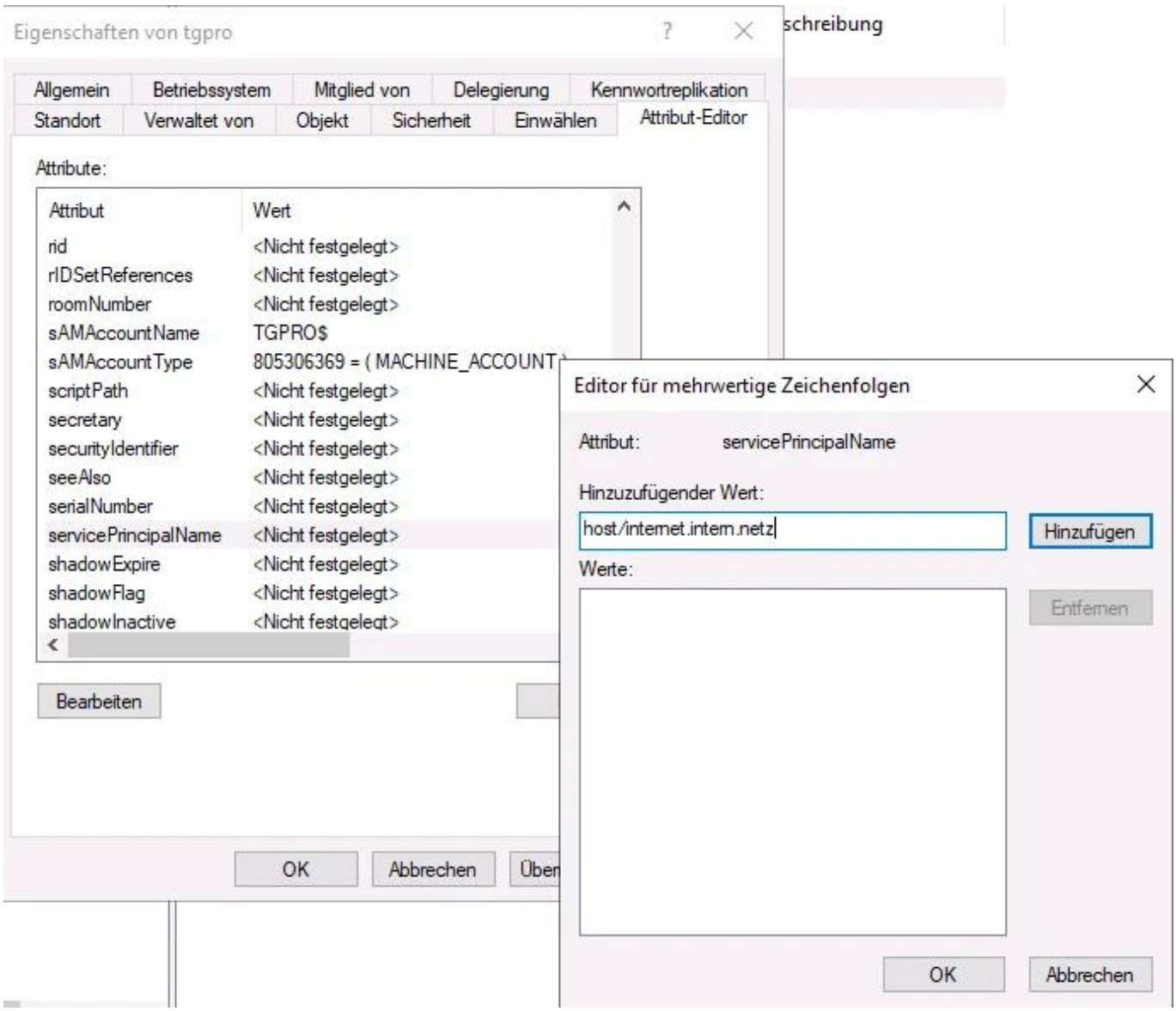


Im nächsten Schritt wird für das Attribut **servicePrincipalName** ein Wert gesetzt. Der Wert folgt dem Schema **host/[DNS-Name im Zertifikat]**. Der Eintrag lautet demzufolge für unser Beispiel: **host/internet.intern.netz**

Der Wert ist im Feld **Hinzuzufügender Wert** einzutragen und danach über die Schaltfläche **Hinzufügen** dem System hinzuzufügen. Danach kann über die Schaltfläche **OK** der Wert übernommen werden. Der **Attribut-Editor** kann danach mit der Schaltfläche **OK** ebenfalls beendet werden.

Hinweis

Der **DNS-Name im Zertifikat** ist der Wert, der im TightGate-Pro als Administrator ***config*** unter **Grundeinstellungen > DNS-Name im Zertifikat** gesetzt ist.



Keytab-Datei erzeugen

Damit sich TightGate-Pro am AD authentisieren kann, wird eine Keytab-Datei benötigt. Diese Keytab-Datei wird einmalig auf dem AD erzeugt und anschließend auf TightGate-Pro importiert.

Achtung

Bitte achten Sie darauf, dass Sie die **Keytab-Datei** mit einer Benutzerkennung erzeugen, die in der Standard-Sicherheitsgruppe **Administrator** des Active-Directory ist. Das Erzeugen einer Keytab aus einer anderen Sicherheitsgruppe heraus, wie z.B. Domänenadministratoren oder Enterprise Administratoren kann zwar durchgeführt werden, jedoch ist damit eine Authentifizierung von TightGate-Pro Anfragen am Active-Directory-Server nicht möglich.

Zur Erzeugung einer Keytab-Datei benötigen Sie entweder eine PowerShell oder einen

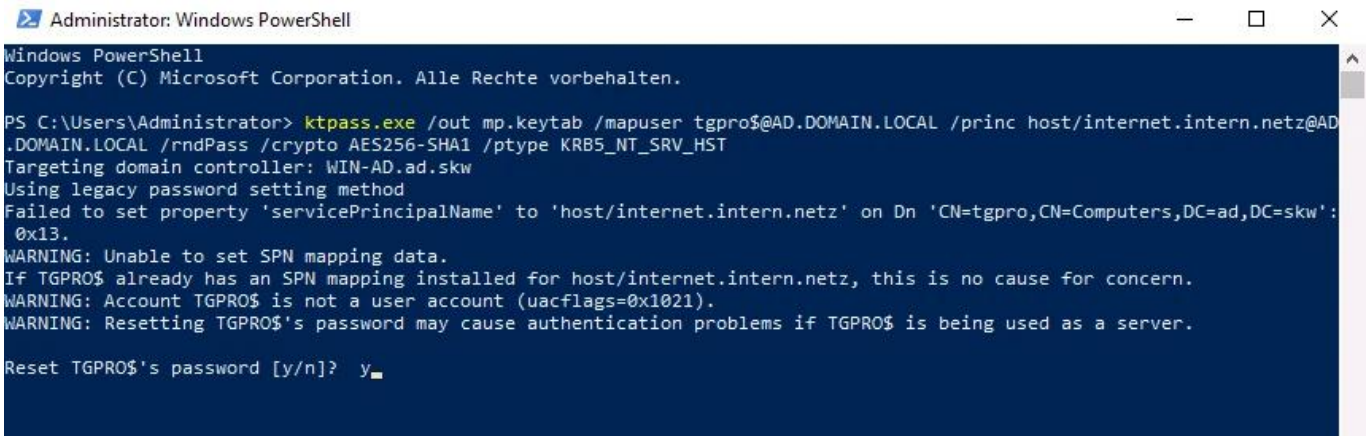
Eingabeaufforderung (CMD) mit administrativen Rechten. Der Befehl zur Erzeugung der Keytab-Datei auf dem AD-Server wird über die Windows Power Shell abgesetzt und hat folgendes Format:

```
ktpass.exe /out [Dateiname] /mapuser [Computer-Name von TightGate-Pro]$@[ADS-REALM] /princ host/[DNS-Name im Zertifikat]@[ADS-REALM] /rndPass /crypto AES256-SHA1 /ptype KRB5_NT_SRV_HST
```

Die Befehlszeile lautet entsprechend für unser Beispiel:

```
ktpass.exe /out mp.keytab /mapuser tgpro$@AD.DOMAIN.LOCAL /princ host/internet.intern.netz@AD.DOMAIN.LOCAL /rndPass /crypto AES256-SHA1 /ptype KRB5_NT_SRV_HST
```

Die Bestätigungsfrage ist mit **y** (Ja) zu beantworten.



Achtung

Der Befehl ist ohne Zeilenumbrüche und lediglich mit Leerzeichen zwischen Schlüsselworten und Parametern einzugeben. Die Groß-/Kleinschreibung ist unbedingt zu beachten.

Die folgende Übersicht erläutert die Bedeutung der Parameter bei der Erzeugung der Keytab-Datei:

Schlüsselwort	Beschreibung	Beispielwert
/out	Name der Ausgabedatei. **Achtung:** Dieser Dateiname muss immer mit .keytab enden.	mp.keytab
/mapuser	Spezifiziert das Zielsystem, für das die erzeugte Keytab-Datei gelten soll, in diesem Fall der TightGate-Pro.	tgpro@AD.DOMAIN.LOCAL
/princ	Spezifiziert den Principal-Namen	host/internet.intern.netz@AD.DOMAIN.LOCAL
/rndPass	Zufällig vom System erzeugtes Passwort.	Es muss kein Wert gesetzt werden.
/crypto	Spezifiziert die Verschlüsselung. **Achtung:** Nur der Wert AES256-SHA1 kann verwendet werden.	AES256-SHA1

Schlüsselwort	Beschreibung	Beispielwert
/ptype	Spezifiziert den Prinzipal-Typ. **Achtung:** Nur der Wert KRB5_NT_SRV_HST kann verwendet werden.	KRB5_NT_SRV_HST

Keytab-Datei zu TightGate-Pro übertragen

Nachdem die Keytab-Datei erzeugt wurde, ist diese zu TightGate-Pro zu übertragen. Die Übertragung erfolgt über das SFTP-Protokoll, am besten eignet sich dafür das Programm WinSCP. Öffnen Sie das WinSCP und erstellen Sie eine Verbindung zu einem TightGate-Pro. Als Benutzer verwenden Sie die Kennung ***config*** mit dem zugehörigen Passwort von Ihrer Passwortliste. Haben Sie die Verbindung erstellt, kopieren Sie die erzeugte Keytab-Datei direkt in das Transfer-Verzeichnis (/home/user/.transfer/config) von ***config*** und schließen Sie danach das WinSCP. Die Übernahme im TightGate-Pro, sowie das Testen der Einstellungen erfolgt wie nachfolgend beschrieben.

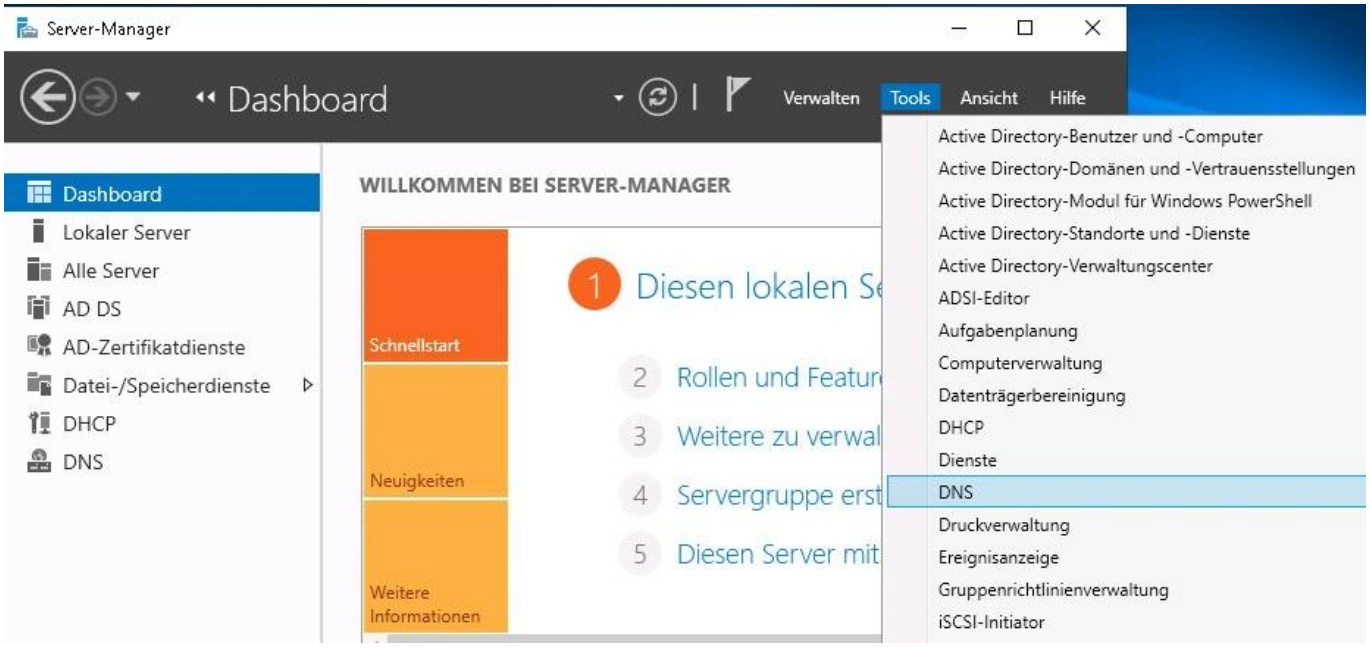
Legen Sie bitte nun wie nachfolgend beschrieben die AD-Sicherheitsgruppen an, danach kann TightGate-Pro wie hier beschrieben konfiguriert werden.

DNS-Einträge erstellen

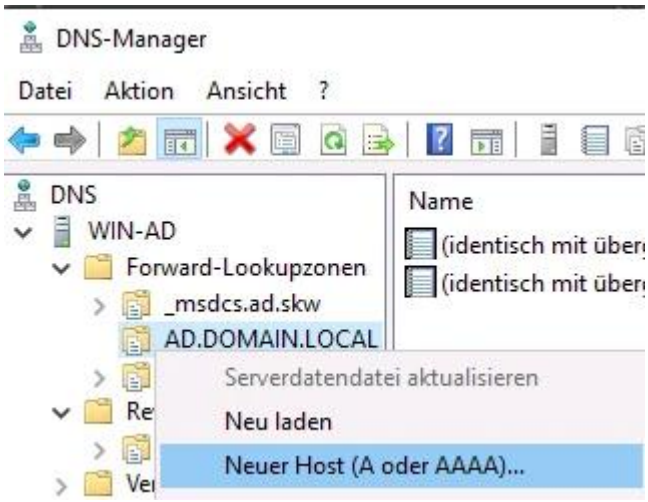
Die Art des DNS-Eintrags für TightGate-Pro unterscheidet sich je nachdem, ob TightGate-Pro als Einzelsystem oder als Clustersystem betrieben wird. Während für Einzelsysteme ein einfacher Host-Eintrag genügt, so ist für Cluster-Systeme ein DNS Zonen-Forwarding einzurichten, damit die Lastverteilung der Benutzer auf die einzelnen Knoten von TightGate-Pro richtig funktioniert.

DNS-Eintrag für TightGate-Pro Einzelsysteme

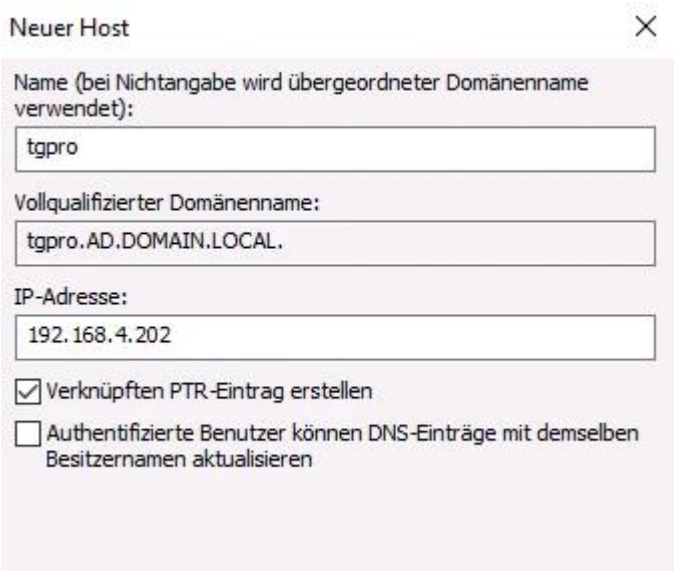
Klicken Sie im Server-Manager auf **Tools > DNS**.



Der Menübaum unter **DNS-Server** ist so weit auszuklappen, bis die verfügbaren *Forward-Lookupzonen* sichtbar sind. Nach Klick mit der rechten Maustaste auf der entsprechenden Domäne des AD (ADS-REALM), in diesem Beispiel AD.DOMAIN.LOCAL, kann über **Neuer Host (A oder AAAA) ...** ein Dialog aufgerufen werden, über den TightGate-Pro zugewiesen werden kann.



Als Name ist der auflösbare Name von TightGate-Pro anzugeben, ebenso wie die IPv4-Adresse des Servers. Das Kontrollkästchen **Verknüpften PTR-Eintrag erstellen** ist zu aktivieren, damit der Hostname automatisch auch in der Reverse-Lookup-Zone eingetragen wird. Das Dialogfeld ist über die Schaltfläche **Host hinzufügen** zu verlassen. Es empfiehlt sich eine Überprüfung, ob der Name von TightGate-Pro vorwärts und rückwärts korrekt aufgelöst werden kann.



DNS-Einrichtung für TightGate-Pro Cluster

Damit die Lastverteilung in TightGate-Pro Clustern einwandfrei arbeitet, dürfen die einzelnen Rechner im Verbund seitens der Klientenrechner nicht dediziert über deren IPv4-Adresse oder deren Host-Namen angesprochen werden. Stattdessen muss der gesamte Cluster von TightGate-Pro im internen Netzwerk als Einheit erscheinen. Es müssen alle Verbindungsanfragen zu TightGate-Pro an spezielle Nodes übergeben werden, welche die Aufgabe der Lastverteilung wahrnehmen.

Dies wird erreicht, indem die Verbindungsanfragen an einen zentralen Rechnernamen (eigene DNS-Zone) gestellt werden, der den Rechnerverbund repräsentiert.

Die nachfolgende Anleitung beschreibt die Einrichtung einer DNS-Zonenweiterleitung (DNS Zone Forwarding).

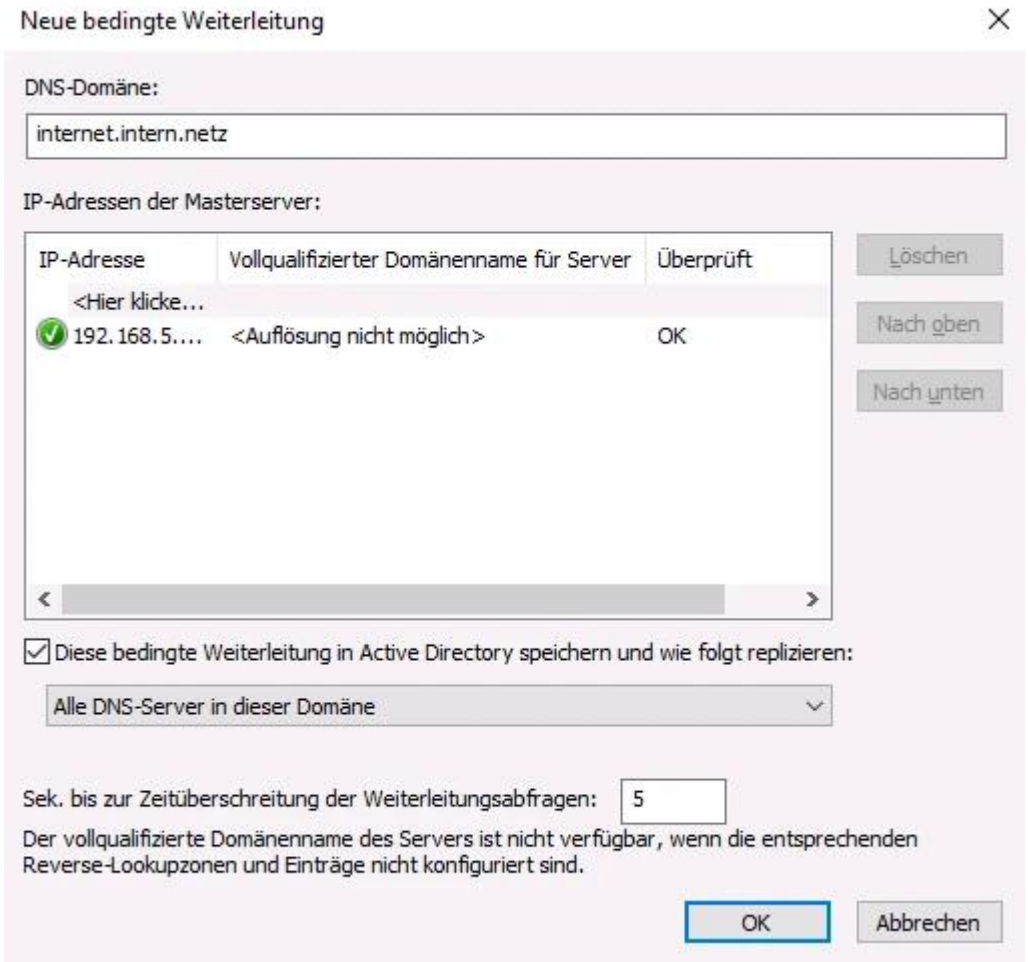
Hinweis

Unter diesem Link finden Sie eine Erklärung und schematische Darstellung der Verbindungswege für die Nutzung des "DNS Zone Forwarding". Dort ist auch beschrieben was zu konfigurieren ist, wenn es zwischen internem Netzwerk und TightGate-Pro eine NAT-Umsetzung gibt.

Bedingte Weiterleitung einrichten

Eine neue bedingte Weiterleitung wird über den DNS-Manager in der betreffenden Domäne erzeugt über den Menüpunkt **Bedingte Weiterleitungen > Neue bedingte Weiterleitung…**

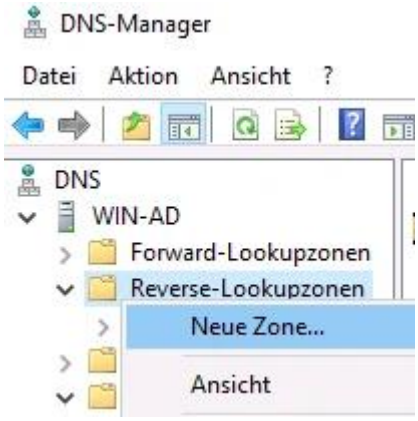
In dem sich öffnenden Dialogfenster ist unter **DNS-Domäne** der Domänenname des TightGate-Pro Clusters (im Beispiel: internet.intern.netz) einzutragen. Zusätzlich sind die IPv4-Adressen der definierten Load Balancer des TightGate-Pro Clusters als **IP-Adressen der Masterserver** hinzuzufügen. Im Beispiel werden die IPv4-Adressen der LAN-Interfaces der ersten beiden TightGate-Pro hinzugefügt, da diese im Beispiel als Load Balancer fungieren.



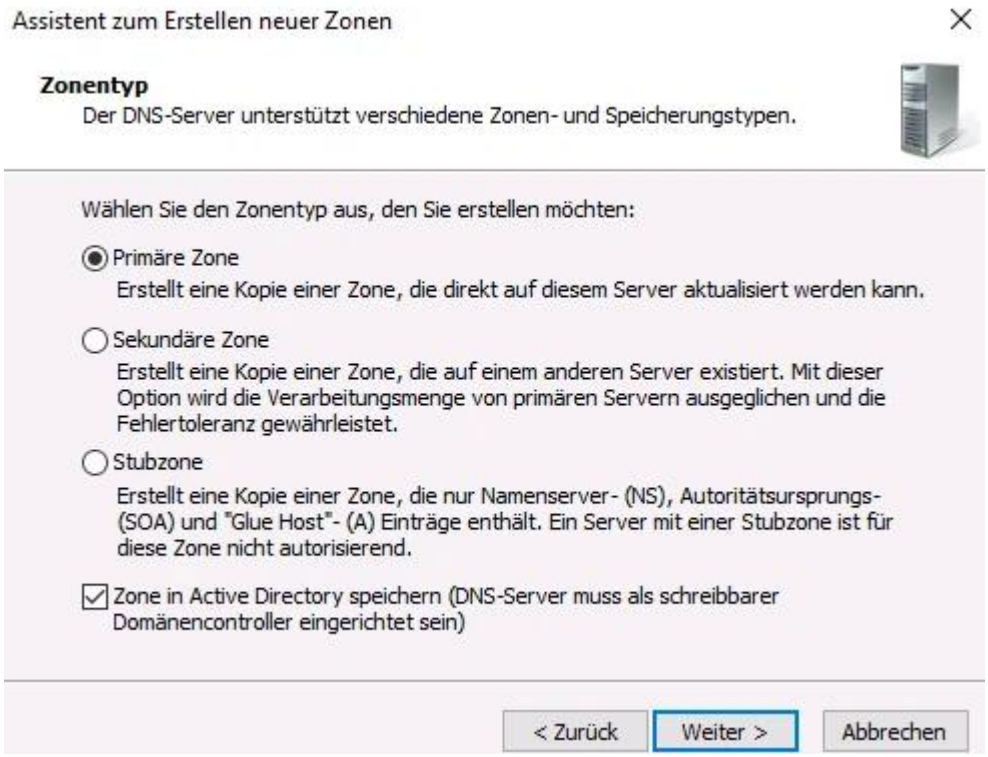
Als Nächstes ist in den Kasten neben den **Sek. bis zur Zeitüberschreitung der Weiterleitungsabfragen** eine **5** zu setzen. Abschließend sind die Einstellungen mit **OK** anzuwenden und das Dialogfenster zu verlassen.

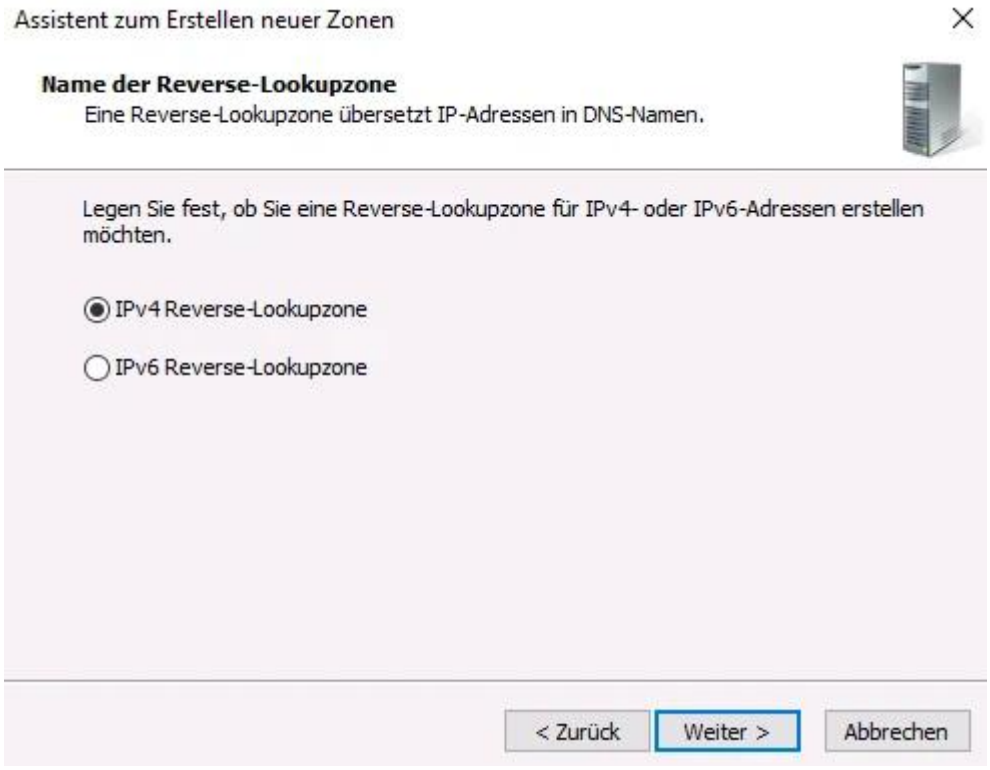
Zugehörige Rückwärtsauflösung einrichten (Reverse Lookupzone)

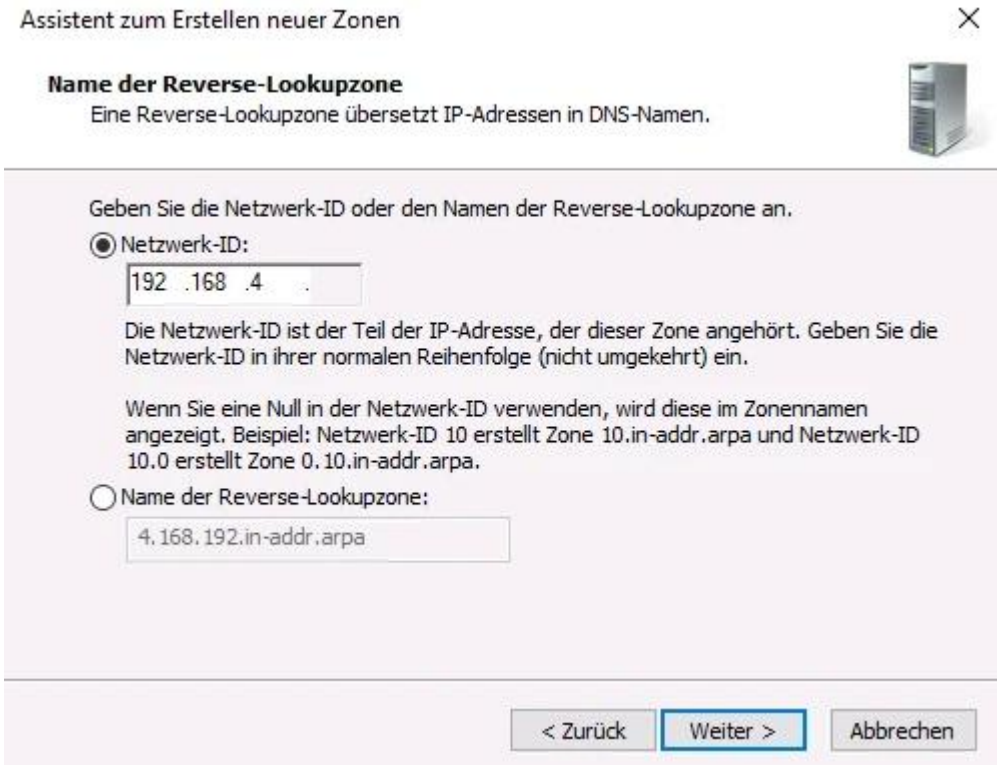
Eine zugehörige Rückwärtsauflösung wird über den DNS-Manager in der betreffenden Domäne erzeugt über den Menüpunkt **Reverse Lookupzonen > Neue Zone…**



Dem Assistenten zur Erstellung einer Reverse Lookupzone für die Domäne des Clusters von TightGate-Pro (im Beispiel internet.intern.netz) ist zu folgen.




Assistent zum Erstellen neuer Zonen
Name der Reverse-Lookupzone
Eine Reverse-Lookupzone übersetzt IP-Adressen in DNS-Namen.
Legen Sie fest, ob Sie eine Reverse-Lookupzone für IPv4- oder IPv6-Adressen erstellen möchten.
IPv4 Reverse-Lookupzone
IPv6 Reverse-Lookupzone
< Zurück
Weiter >
Abbrechen


Assistent zum Erstellen neuer Zonen
Name der Reverse-Lookupzone
Eine Reverse-Lookupzone übersetzt IP-Adressen in DNS-Namen.
Geben Sie die Netzwerk-ID oder den Namen der Reverse-Lookupzone an.
Netzwerk-ID:
192 .168 .4 .
Die Netzwerk-ID ist der Teil der IP-Adresse, der dieser Zone angehört. Geben Sie die Netzwerk-ID in ihrer normalen Reihenfolge (nicht umgekehrt) ein.
Wenn Sie eine Null in der Netzwerk-ID verwenden, wird diese im Zonennamen angezeigt. Beispiel: Netzwerk-ID 10 erstellt Zone 10.in-addr.arpa und Netzwerk-ID 10.0 erstellt Zone 0.10.in-addr.arpa.
Name der Reverse-Lookupzone:
4.168.192.in-addr.arpa
< Zurück
Weiter >
Abbrechen

AD-Sicherheitsgruppen anlegen

Damit die Gruppenverwaltung von TightGate-Pro korrekt auf das Active Directory übertragen wird, müssen die entsprechenden Sicherheitsgruppen auf dem Active Directory angelegt sein. Das Anlegen bzw. Ändern eines Benutzers (oder Gruppe von Benutzern) erfolgt durch das Hinzufügen oder Entfernen zu den definierten Sicherheitsgruppen im AD. Ist ein Benutzer z. B. Mitglied der Sicherheitsgruppe **TGProUser**, so kann er sich anmelden. Die weiteren Optionen für den Benutzer werden durch die Mitgliedschaft in entsprechenden Sicherheitsgruppen definiert.

Warnung

Die Namen (Gruppennamen) der Sicherheitsgruppen von TightGate-Pro im Active Directory müssen den Gruppennamen enthalten. Davor und danach können Zeichen hinzugefügt werden. Ist der Gruppenname nicht im Namen der Sicherheitsgruppe enthalten, schlägt die Anmeldung des TightGate-Viewers am TightGate-Pro fehl.

So geht's

Zur Änderung der für einen Benutzer oder eine Benutzergruppe gewünschten Attribute müssen die Mitgliedschaften der betreffenden Benutzer oder Benutzergruppen aus den Sicherheitsgruppen hinzugefügt bzw. entfernt werden. Bei der nächsten Anmeldung des Benutzers mit dem TightGate-Viewer werden die Attribute wirksam. Eine Übersicht über alle für TightGate-Pro verfügbaren Sicherheitsgruppen gibt nachfolgende Tabelle mit Beschreibung und Empfehlung:

Gruppenname	Berechtigung auf TightGate-Pro	Empfehlung für normale Nutzer
TGProUser	Benutzungsberechtigung von TightGate-Pro	Ja
TGtransfer	Benutzungsberechtigung für die Dateischleuse. Die Berechtigung kann über diese Gruppe nur erteilt oder entzogen werden. Eine weitergehende Konfiguration hinsichtlich Übertragungsrichtungen und erlaubter Dateitypen ist nur über die Mitgliedschaft in der/den Gruppen **TGtransferN** möglich.	Ja
TGtransferN	Transfergruppe N, zur Definition erlaubter MIME-TYPEN für den Dateitransfer. Beispiel: tgtransfer1, Groß- und Kleinschreibung ist dabei egal, tgtransfer01 mit führender 0 funktioniert nicht. Ist ein Benutzer in mehreren Transfergruppen, so werden die Rechte der einzelnen Gruppen kumuliert. Die Mitgliedschaft in der Gruppe **TGtransfer** ist zu Nutzung obligatorisch. Es können bis zu 99 Transfer-Gruppen auf TightGate-Pro definiert werden.	Ja
TGaudio	Berechtigung für die Soundübertragung vom Internet	Ja
TGtransferSpool	Berechtigung für die automatische Druckausgabe auf dem Windows Arbeitsplatzrechner.	Ja
TGunfiltered	Berechtigung ohne Inhaltsfilter von TightGate-Pro das Internet nutzen können.	Ja
TGchromeicon	Anzeige des Chrome-Browsers in der Menüleiste des TightGate-Viewers	Optional
TGmailicon	Anzeige des Mailprogramms Thunderbird in der Menüleiste des TightGate-Viewers	Optional
TGopswat	Zuweisung der Dateischleuse über OPSWAT. Die Mitgliedschaft in dieser Gruppe ist zwingend erforderlich, sofern OPSWAT verwendet werden soll. Ist eine Kennung nicht in dieser Gruppe, wird OPSWAT nicht verwendet und alle Gruppen-Mitgliedschaften in den **TGopswatN**-Gruppen werden ignoriert. Damit OPSWAT wirksam verwendet werden kann, ist zusätzlich noch eine Mitgliedschaft in einer **TGopswatN**-Gruppe zu setzen. Ist keine Mitgliedschaft in einer **TGopswatN**-Gruppe vorhanden wird immer die Standard-Regel des OPSWAT verwendet.	Optional
TGopswatN	OPSWAT-Gruppe 1-9 zur Zuweisung der zu verwenden OPSWAT-Regel. Die Gruppe **TGopswatN** weißt einem Benutzer die zu verwendende OPSWAT-Regel zu. Es darf pro Benutzer nur eine **TGopswatN**-Gruppe verwendet werden, da es sonst zu Fehlern kommen kann. Die **TGoposwatN**-Gruppen korrelieren mit den als ***config*** angelegten OPSWAT-Rules. Beispiel: tgopswat1, Groß- und Kleinschreibung ist egal, tgopswat01 mit führender 0 funktioniert nicht.	Optional
TGtoricon	Anzeige des TOR-Browsers in der Menüleiste des TightGate-Viewers –> Anleitung zur Nutzung des TOR-Browsers in TightGate-Pro	Optional
TGbebpoicon	Anzeige des beBPo-Klienten in der Menüleiste des TightGate-Viewers –> Anleitung zur Nutzung des besonderen elektronischen Behördenpostfachs (beBPo) in TightGate-Pro	Optional

Gruppenname	Berechtigung auf TightGate-Pro	Empfehlung für normale Nutzer
TGfiltergroupN	Webfilter-Gruppe N; zur Zuweisung der zwangsweisen Nutzung des Webfilters. Es wird pro Benutzer nur eine Webfilter-Gruppe verwendet. Ist ein Benutzer in mehreren Webfilter-Gruppen, so verwendet TightGate-Pro automatisch nur die Rechte aus der höchsten Webfilter-Gruppe. Eine Kumulierung von Rechten aus mehreren Gruppen findet nicht statt. Es können bis zu 99 Webfilter-Gruppen definiert werden. Beispiel: tgfiltergroup1, Groß- und Kleinschreibung ist dabei egal, tgfiltergroup01 mit führender 0 funktioniert nicht.	Optional
TGmaxfilesize	Mitglieder in dieser Gruppe dürfen Dateien verarbeiten, die größer als 4GB sind.	Optional
TGtransferAuto	Berechtigung zur Nutzung der automatischen Dateischleuse.	Optional
TGnoidleTimeout	Auswahl, ob die Kennung von der Zwangstrennung bei Inaktivität ausgenommen wird. Die Trennung beim Erreichen der Maximalen Sitzungsdauer wird damit nicht aufgehoben.	Optional
TGstartpdf	Mitgliedern dieser Gruppe wird bei jeder Anmeldung mit dem TightGate-Viewer eine PDF-Datei angezeigt, um (vom Betreiber erstellte) Nutzungsbedingungen zur Kenntnis zu nehmen. Die PDF-Datei ist vorab auf TightGate-Pro zu hinterlegen. –> Anleitung zur Anzeige von kundenspezifischen Nutzungsbedingungen	Optional
TGbandwidth	Nutzung der Bandbreitenoptimierung des TightGate-Viewers. Die Darstellungsqualität ist um eine Stufe herabgesetzt, dafür wird die benötigte Bandbreite deutlich reduziert.	Empfohlen für WAN
TGbandwidthhigh	Nutzung der maximalen Bandbreitenoptimierung des TightGate-Viewers. Es wird maximal am TightGate-Pro komprimiert. Die Bandbreitennutzung schrumpft bei dieser Komprimierung auf ein fünftel der normalen Bandbreite, dafür steigt der CPU-Verbrauch am TightGate-Pro stark an. **Warnung:** Diese Kompressionsstufe benötigt sehr hohe CPU-Ressourcen am TightGate-Pro UND auf dem lokalen Arbeitsplatz-PC, was die Leistungsfähigkeit des gesamten TightGate-Pro Systems beeinträchtigen Kann. Bitte nehmen Sie vor der Umsetzung dieser Kompression Kontakt mit dem technischen Kundendienst der m-privacy GmbH auf und lassen sich dazu beraten.	Nein
TGprivileged	Zusätzliche Berechtigung sich als privilegierter Benutzer anzumelden. Es ist zusätzlich immer die Mitgliedschaft in der Sicherheitsgruppe **TGProUser** erforderlich sowie eine TightGate-Pro Lizenz, welche privilegierte Benutzer zulässt.	Nein
TGadminMaint	Anmeldung als Administrator ***maint***	Nein
TGadminConfig	Anmeldung als Administrator ***config***	Nein
TGadminUpdate	Anmeldung als Administrator ***update***	Nein
TGadminBackuser	Anmeldung als Administrator ***backuser***	Nein
TGadminRoot	Anmeldung als Administrator ***root***	Nein
TGadminSecurity	Anmeldung als Administrator ***security***	Nein

Hinweis

Abgelaufene Passworte sperren auch Benutzerkonten, die sich mit Single Sign-on (SSO) via Active Directory anmelden. Sofern SSO per Active Directory verwendet wird, wird empfohlen das lokale Passwort nicht zu verwenden, bzw. zu deaktivieren.

Benutzer entfernen/löschen

Entfernt wird ein Benutzer, indem er aus allen Sicherheitsgruppen von TightGate-Pro im AD entfernt wird. Nach dem Entfernen aus den Sicherheitsgruppen kann sich der Benutzer nicht mehr am TightGate-Pro anmelden. Soll der Benutzeraccount auf TightGate-Pro komplett gelöscht werden, so folgenden Sie bitte dieser Anleitung.

Hinweise zum Löschen bei einer Benutzerverwaltung mittels Active Directory Die komplette Löschung eines Benutzers ist nur dann wirksam, wenn der Benutzer ebenfalls aus den Sicherheitsgruppen **TGProUser** und **TGtransfer** im Active Directory entfernt wurde. Andernfalls wird der Benutzer automatisch neu angelegt, wenn der betreffenden Benutzer eine Anmeldung versucht.