Vorbereitung des Active Directory Servers

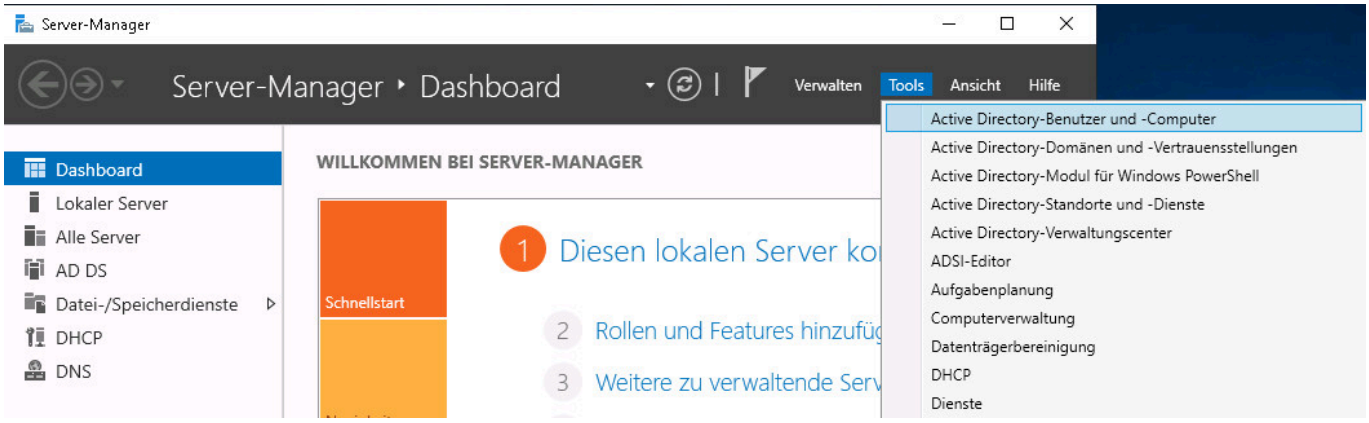
Der Windows Server, welcher als Active Directory verwendet werden soll, ist vor der Einrichtung der Anbindung eines TightGate-Pro grundsätzlich zur Verarbeitung von Domänendiensten vorzubereiten, falls noch nicht geschehen. Die Vorbereitung unterteilt sich in vier Schritte:

- Im ersten Schritt wird ein Computer-Account für TightGate-Pro auf dem AD-Server angelegt.
- Im zweiten Schritt wird eine Keytab-Datei für die Authentisierung von TightGate-Pro am AD-Server erzeugt.
- Im dritten Schritt sind die DNS-Einstellungen vorzunehmen, damit TightGate-Pro im Netzwerk von den TightGate-Klienten gefunden werden kann.
- Im vierten Schritt sind die AD-Sicherheitsgruppen anzulegen.

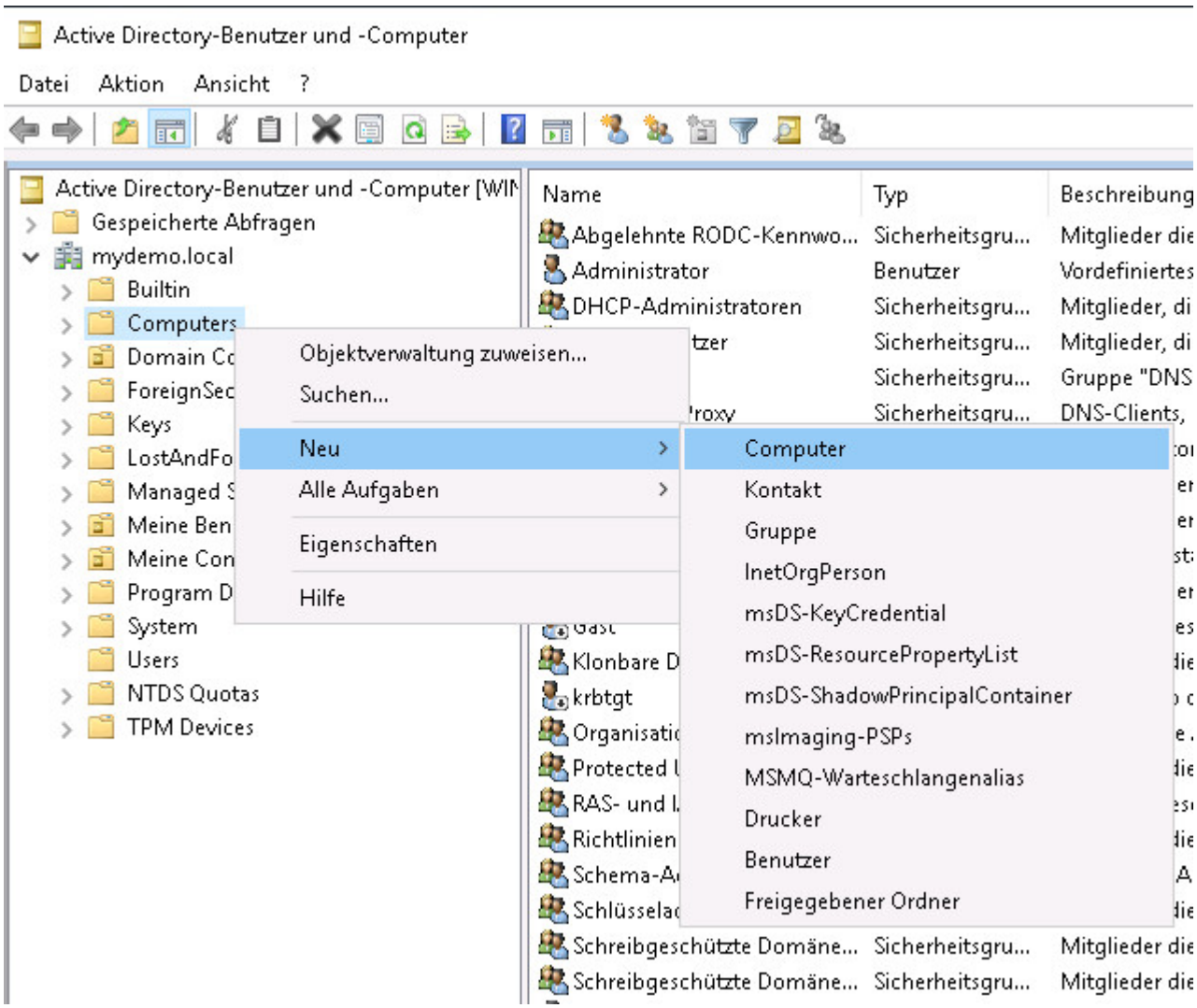
Anlegen eines Computer-Accounts

Zunächst ist TightGate-Pro auf dem AD-Server als sogenannter Computer-Account in der richtigen Domäne anzulegen. Dies gilt für Einzelsysteme wie auch für Clustersysteme gleichermaßen. Im Beispiel heißt der Computer-Account auf dem AD-Server im Fall eines Einzelsystems **TGPro** und im Fall eines Clustersystems **srv-TGPro**.

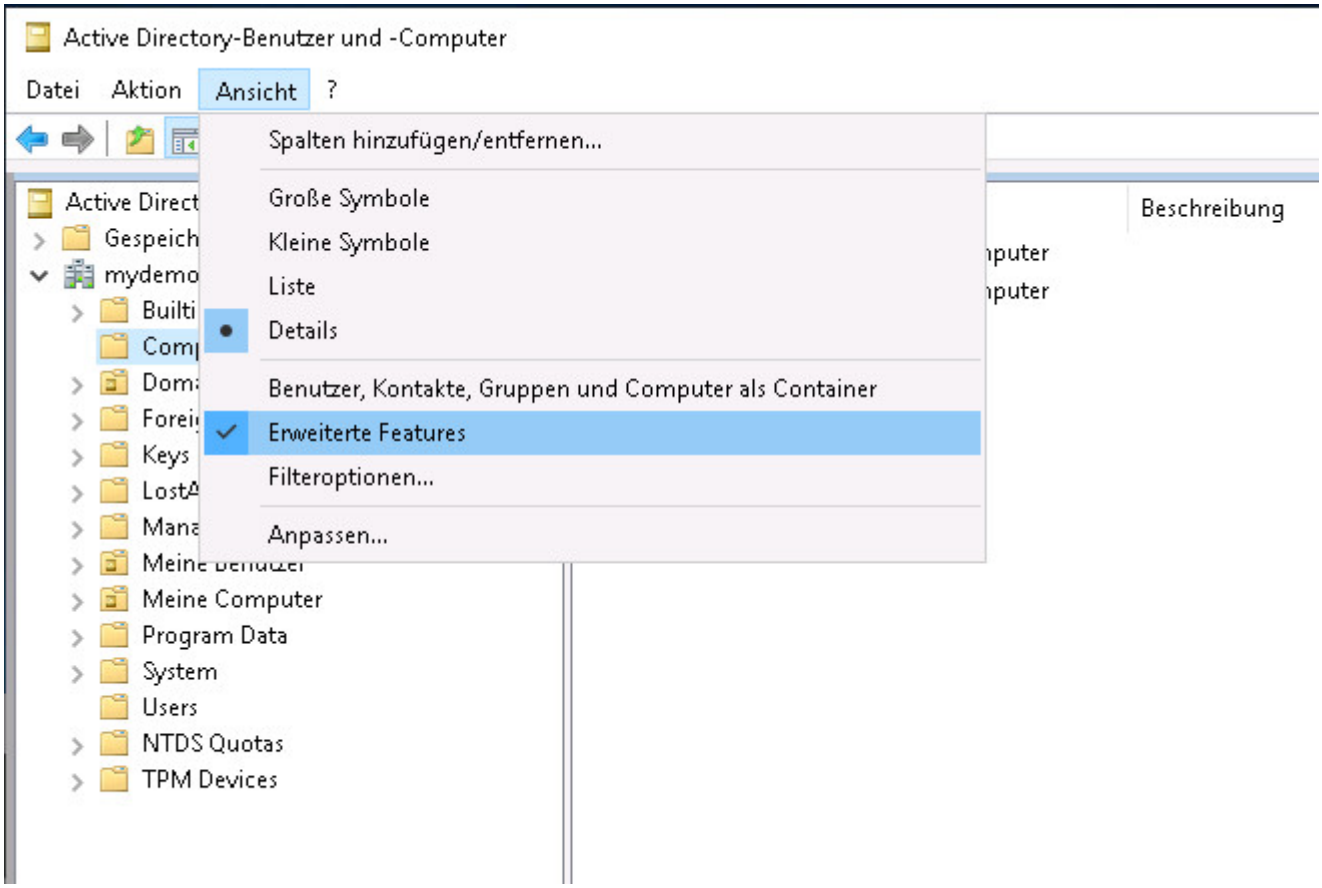
Den Computer-Account legen Sie an, indem Sie im Server-Manager auf **Tools > Active Directory-Benutzer und -Computer** klicken.



Klicken Sie im nächsten Fenster in Ihrer Domäne mit Rechtsklick auf **Computer** und anschließend im Kontextmenü auf **Neu > Computer**.

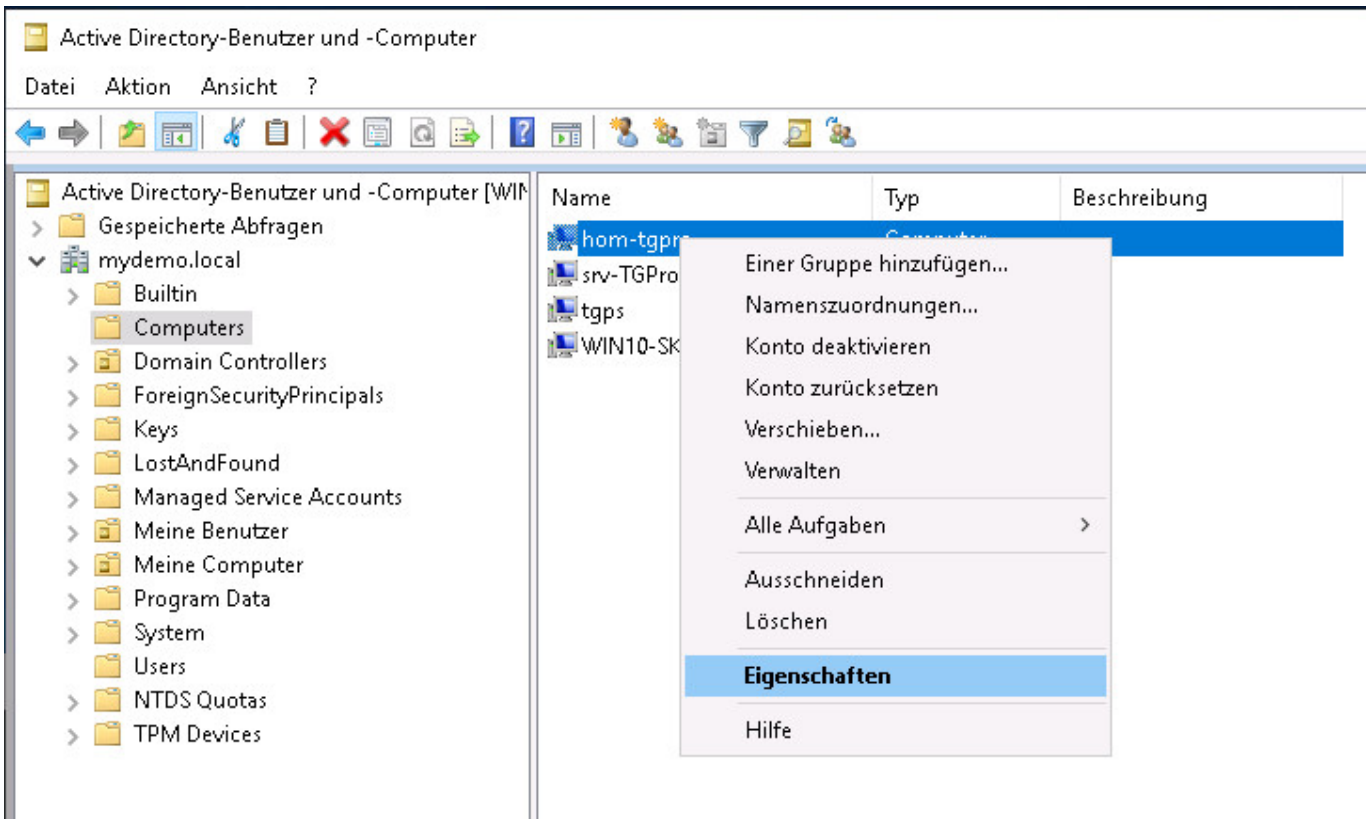


Nach der Anlage ist der Computer-Account weiter anzupassen. Im Fenster **Active Directory-Benutzer und -Computer** kann hierzu unter **Ansicht > Erweiterte Features** eine ausführlichere Liste der einzelnen Bestandteile der Domäne des AD-Servers (ADS-REALM) angezeigt werden.

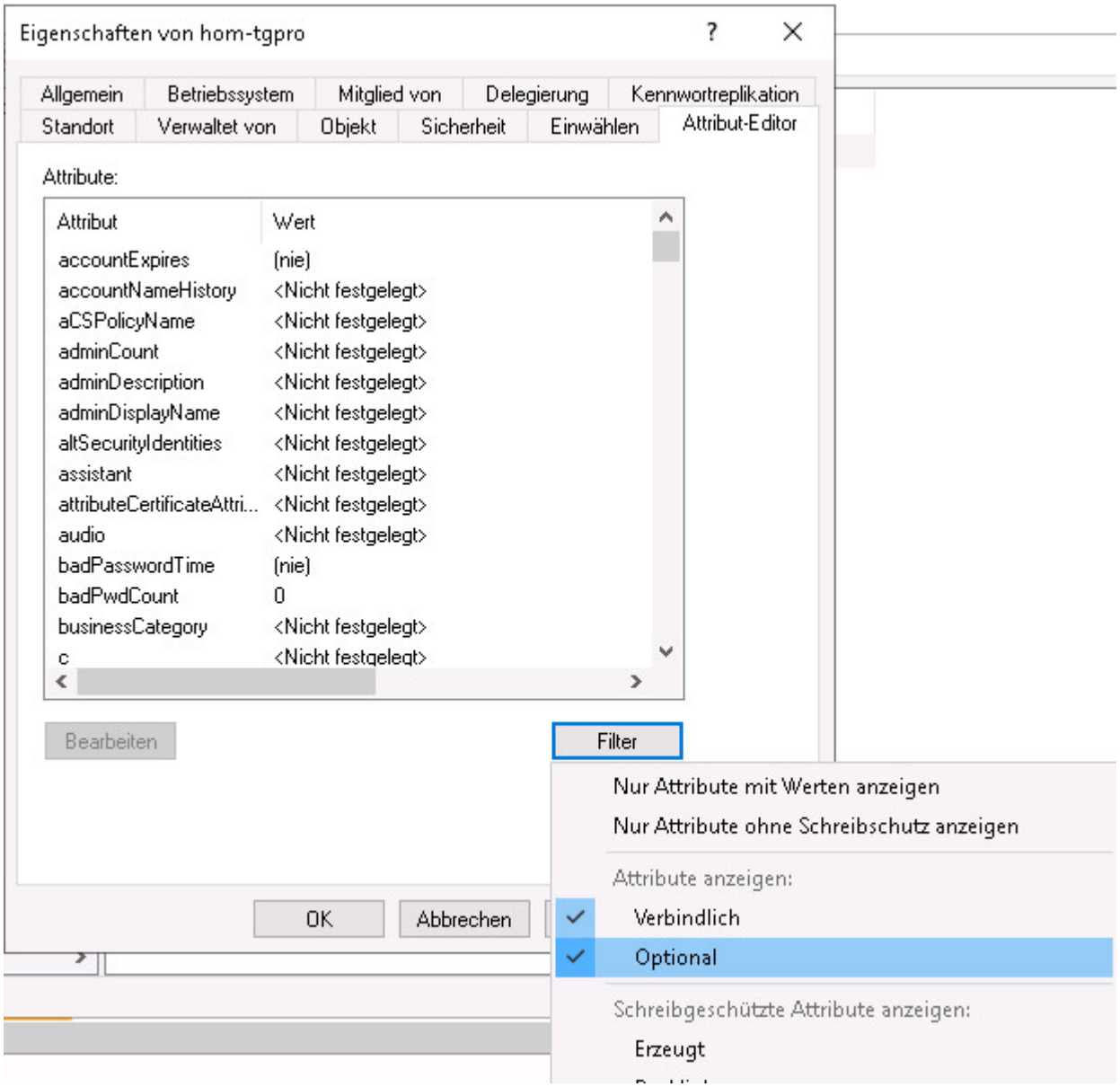


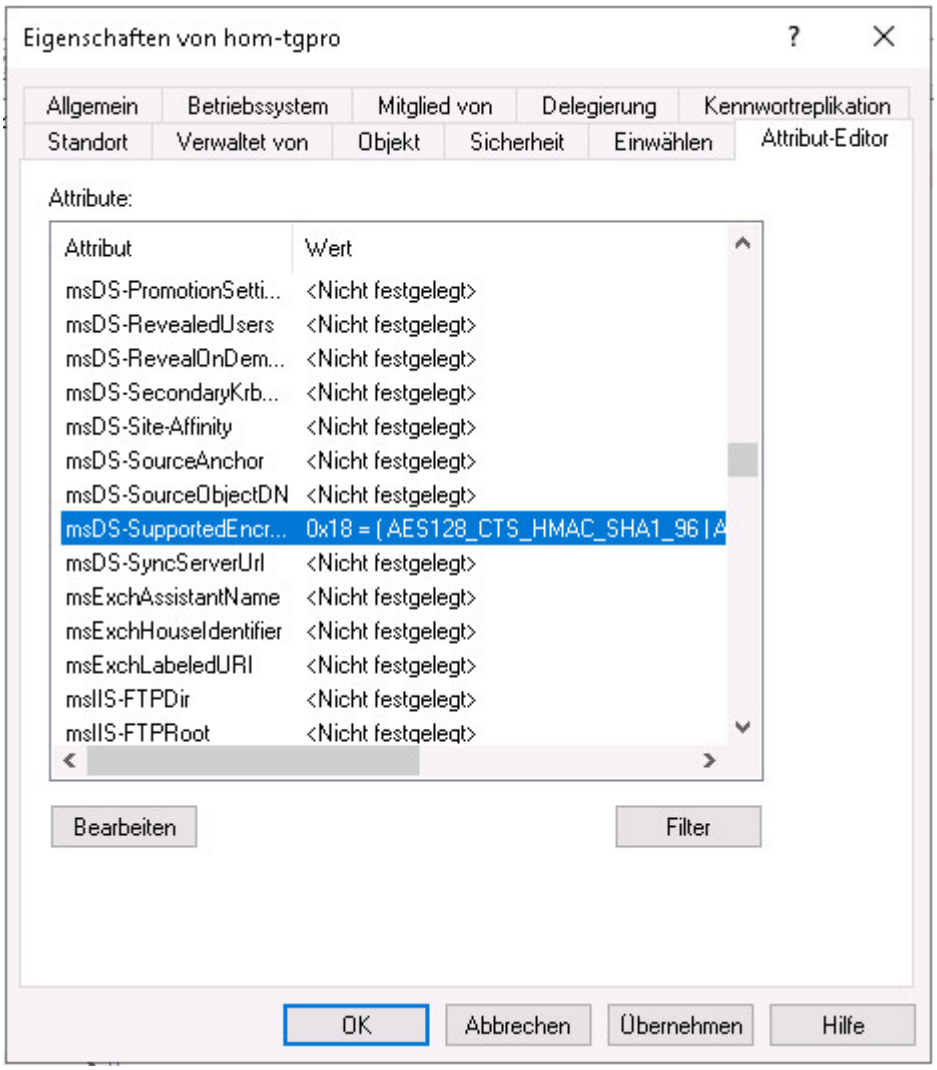
Verschlüsselung

Die Liste der vorhandenen Computer-Accounts wird nach Klick mit der linken Maustaste auf **Computers** angezeigt. Ein Klick mit der rechten Maustaste auf den Computer-Account von TightGate-Pro Server, im Beispiel entweder **TGPro** oder **srv-TGPro**, öffnet ein Kontextmenü, aus dem der Konfigurationsdialog über **Eigenschaften** aufzurufen ist.



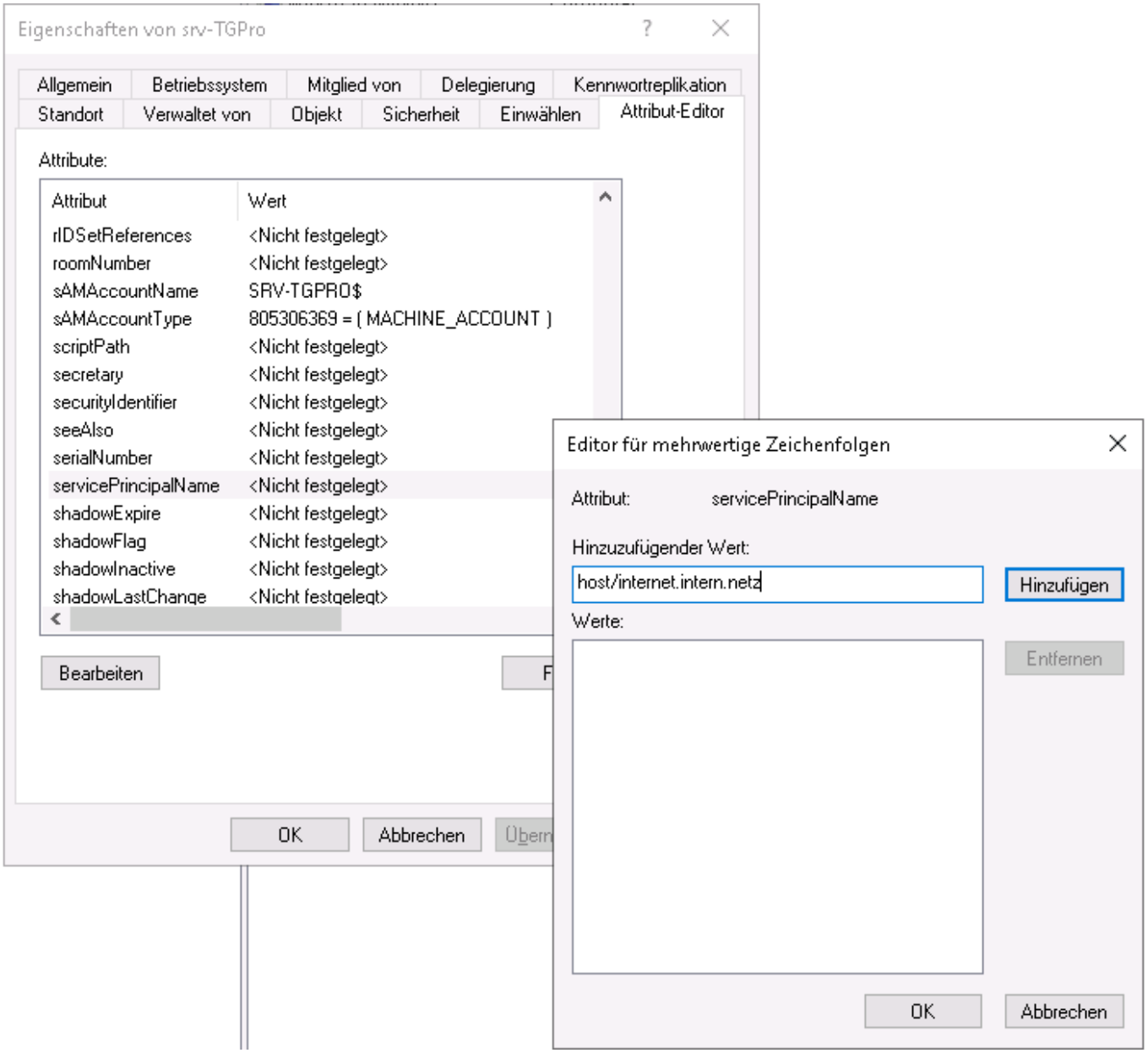
Im nächsten Schritt müssen Einstellungen im Attribut-Editor vorgenommen werden. Wechseln Sie zur Registertaste **Attribut-Editor** und vergewissern Sie sich zuerst mit einem Klick auf die Filter-Schaltfläche, dass unter **Attribute anzeigen > Optional** das Häkchen gesetzt ist.





Sowohl für Einzel- als auch für Clustersysteme sind auf der Registertaste **Attribut-Editor** die Verschlüsselungstypen für den Computer-Account von TightGate-Pro zu setzen. Dabei ist ausschließlich der Wert **msDS-SupportedEncryption Types** aus der Auswahlliste auf den 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.

Weiterhin muss das Attribut **servicePrincipalName** auf den Wert **host/[Domäne des TG-Pro-Clusters oder DNS-Name des Einzelsystems]** gesetzt werden. Der Eintrag lautet demzufolge im Beispiel: - Für den Cluster: **host/internet.intern.netz** - Für das Einzelsystem: **host/TGPro.sso.m-privacy.hom**.



Keytab-Datei für TightGate-Pro erzeugen

Damit sich TightGate-Pro am AD-Server authentisieren kann, benötigt ersterer ein spezielles Zertifikat, das in einer sogenannten keytab-Datei enthalten ist. Diese keytab-Datei wird einmalig auf dem AD-Server unter Angabe bestimmter Parameter erzeugt und TightGate-Pro zur Verfügung gestellt.

Warnung

Bitte achten Sie darauf, dass Sie die **keytab** mit dem 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.

Der Befehl **für Einzelsysteme** auf dem AD-Server zur Erzeugung der keytab-Datei wird über die Windows Power Shell abgesetzt und hat folgendes Format:

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

Der Befehl für ***Clustersysteme (Verbundrechner)*** auf dem AD-Server zur Erzeugung der keytab-Datei hat folgendes Format:

```
ktpass.exe /out [Dateiname] /mapuser [Computer-Name von TG-Pro
Cluster]$@[ADS-REALM] /princ host/[Domäne TG-Pro Cluster]@[ADS-REALM]
/rndPass /crypto AES256-SHA1 /ptype KRB5_NT_SRV_HST
```

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

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.	TGPro.keytab
/mapuser	Spezifiziert das Zielsystem, für das die erzeugte keytab-Datei gelten soll, in diesem Fall TightGate-Pro Server, im Format [Computer-Name von TG-Pro]$@[ADS-REALM]	TGPRO$@SSO.M-PRIVACY.HOM
/princ	Spezifiziert den Principal-Namen	**Für Einzelsysteme:** host/TGPro.sso.m-privacy. hom@SSO.M-PRIVACY.HOM **Für Clustersysteme:** host/internet.intern.netz@SSO.M-PRIVACY.HOM
/rndPass	Zufällig vom System erzeugtes Passwort.	Es muss kein Wert gesetzt werden.
/crypto	Spezifiziert die Schlüssel, welche in der keytab-Datei eingebettet werden. **Achtung:** Nur der kryptografische Typ AES256-SHA1 wird von TightGate-Pro Server unterstützt.	AES256-SHA1
/ptype	Spezifiziert den Prinzipal-Typ, es wird nur der HOST-Service benötigt. **Achtung:** Es muss der angegebene Wert gesetzt werden.	KRB5_NT_SRV_HST

Die Befehlszeile **für Einzelsysteme** lautet entsprechend der beispielhaft gesetzten Werte:

```
ktpass.exe /out TGPro.keytab /mapuser TGPro$@SSO.M-PRIVACY.HOM /princ
host/TGPro.sso.m-privacy.hom@SSO.M-PRIVACY.HOM /rndPass /crypto AES256-SHA1
/ptype KRB5_NT_SRV_HST
```

Die Befehlszeile für **Clustersysteme** lautet entsprechend der beispielhaft gesetzten Werte:

```
ktpass.exe /out srv-TGPro.keytab /mapuser srv-TGPro$@SSO.M-PRIVACY.HOM
/princ host/internet.intern.netz@SSO.M-PRIVACY.HOM /rndPass /crypto AES256-
SHA1 /ptype KRB5_NT_SRV_HST
```

Die Bestätigungsfrage ist mit **Ja / Yes** zu beantworten.

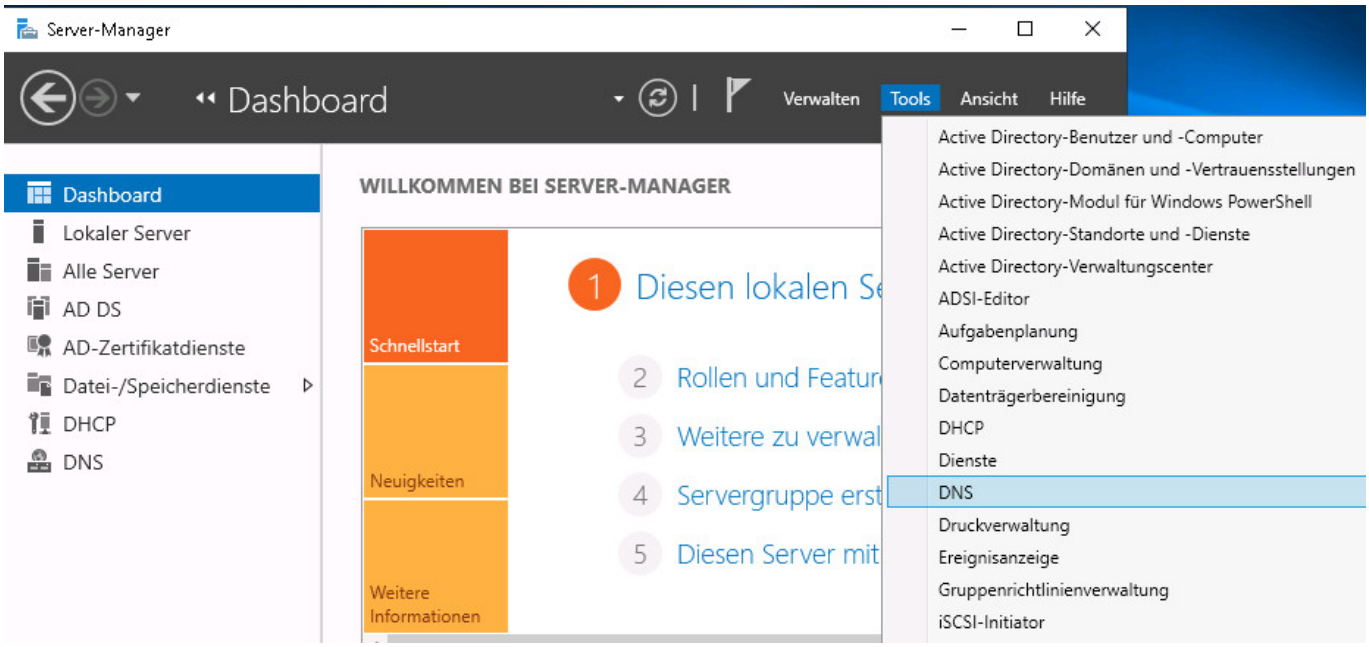
Abschließend ist die erzeugte keytab-Datei im Transfer-Verzeichnis des Administrators ***config*** auf TightGate-Pro zu hinterlegen.

DNS-Einträge erstellen

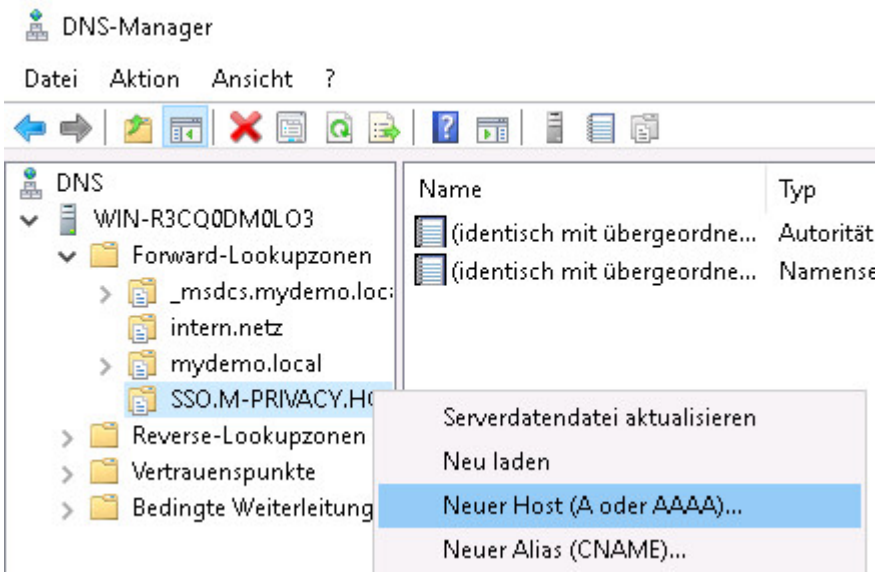
Die Art des DNS-Eintrags für TightGate-Pro unterscheidet sich je nachdem, ob TightGate-Pro als Einzelsystem oder als Clustersystem betrieben wird. Während für Einzelsysteme ein einfacher Host-Eintrag genügt, so ist für Cluster-Systeme ein DNS Zonen-Forwarding einzurichten, damit die Lastverteilung der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

DNS-Eintrag für Einzelsysteme

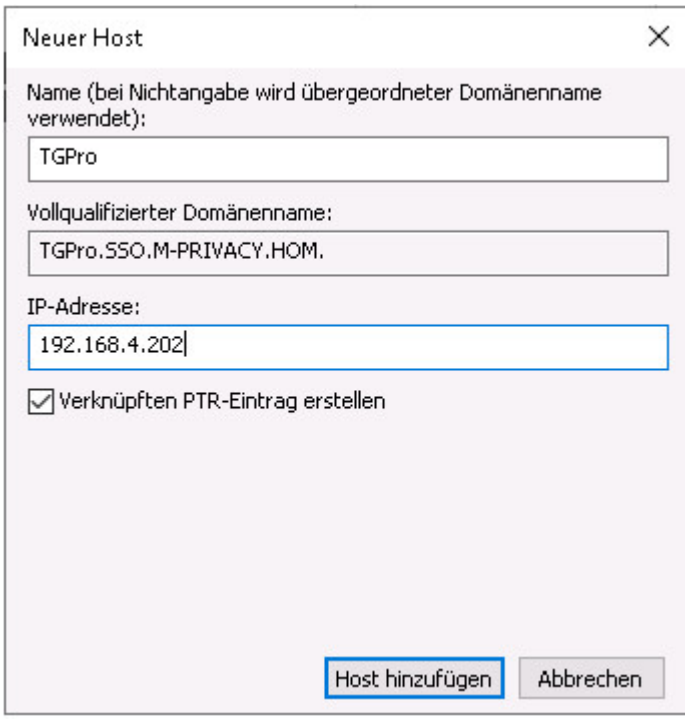
Klicken Sie im Server-Manager auf **Tools > DNS**.



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-Servers (ADS-REALM), in diesem Beispiel SSO.M-PRIVACY.HOM, 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 in jedem Fall 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 Clustersysteme

Leistungsstarke ReCoB-Server der TightGate-Pro-Produktlinie werden aus Kapazitätsgründen im

Clusterverbund ausgeliefert. Dieser Verbund besteht aus mehreren Einzelrechnern, die "Nodes" genannt werden. Innerhalb des Verbundes verfügt TightGate-Pro über eine automatische Lastverteilung. Diese Lastverteilung, auch "Load Balancing" genannt, ist die Grundlage eines optimierten Systembetriebs.

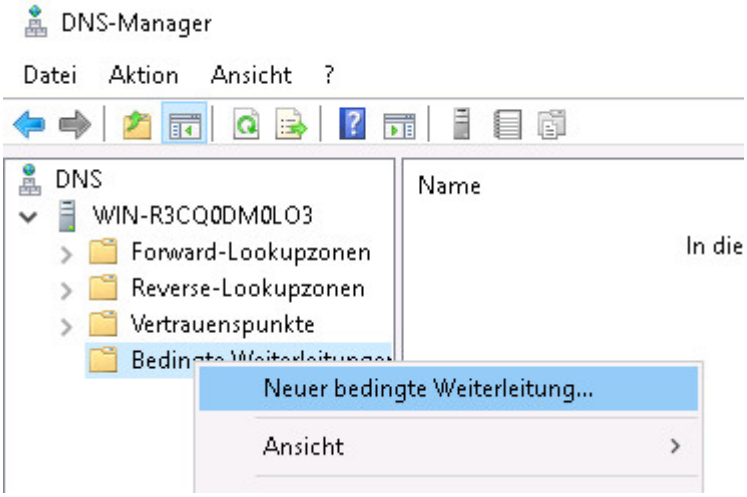
Damit die Lastverteilung einwandfrei arbeitet, dürfen die einzelnen Rechner im Verbund seitens der Klientenrechner nicht dediziert über deren IPv4-Adresse oder deren Host-Namen angesprochen werden. Stattdessen muss der gesamte Cluster von TightGate-Pro im internen Netzwerk als Einheit erscheinen. Es 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.

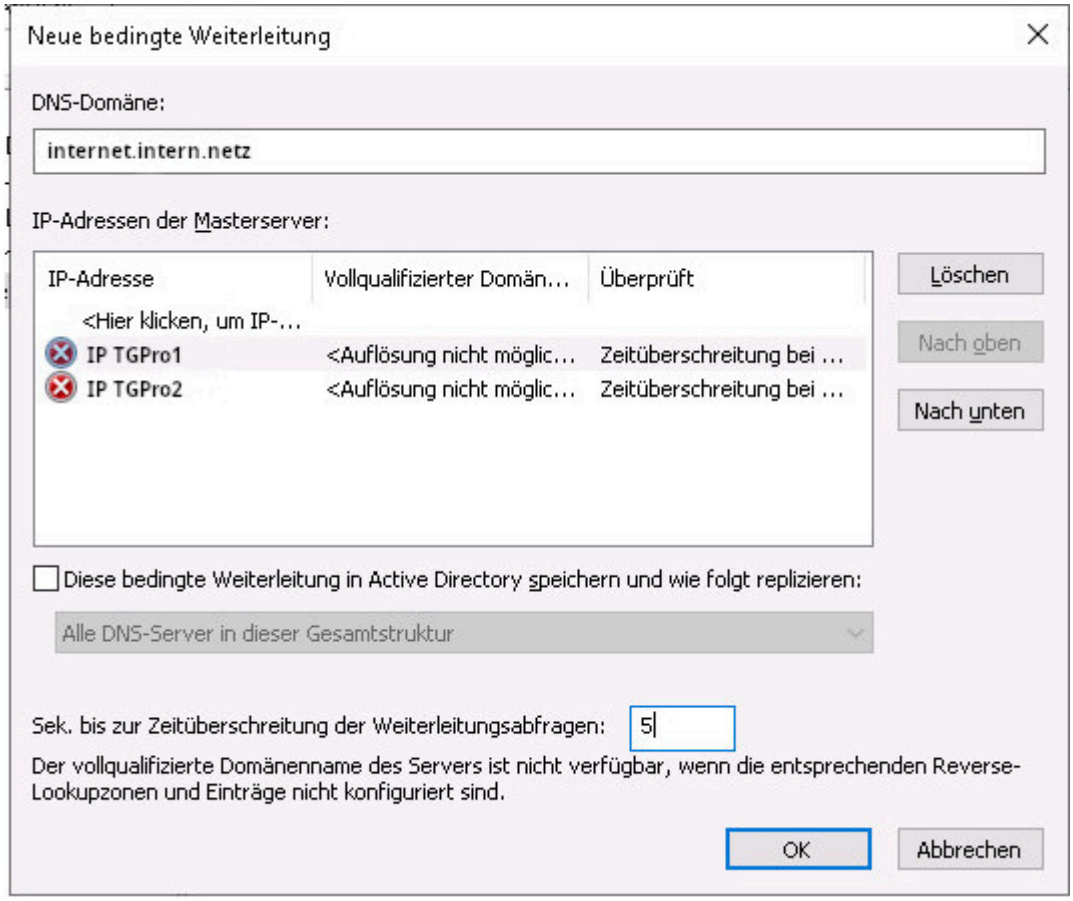
Die nachfolgende Anleitung beschreibt die Einrichtung einer DNS-Zonenweiterleitung (DNS Zone Forwarding) unter Microsoft Windows.

a) Einstellungen am DNS-Server

- Auswahl des Menüpunkts **Bedingte Weiterleitung > 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 Knoten hinzugefügt, da diese in diesem Fall als Load Balancer fungieren.



- Als Nächstes ist in den Kasten neben den "Sek. bis zur Zeitüberschreitung der Weiterleitungsabfragen" eine **5** zu setzen.
- Abschließend die Einstellungen das Dialogfeld mit **OK** verlassen.

b) Rückwärtsauflösung einrichten (Reverse Lookupzone)

- Auswahl des Menüpunkts **Reverse Lookupzonen > Neue Zone...**
- Dem Assistenten zur Erstellung einer Reverse Lookupzone für die Domäne des Clusters von TightGate-Pro (im Beispiel internet.intern.netz) folgen.

AD-Sicherheitsgruppen anlegen

Damit die Gruppenverwaltung von TightGate-Pro korrekt auf das Active Directory übertragen wird, müssen die entsprechenden Sicherheitsgruppen auf dem zentralen Verzeichnisdienst angelegt sein. Bitte legen Sie die benötigten Sicherheitsgruppen in Ihrem Active Directory System an. Die Entscheidung, welche Sicherheitsgruppen zu verwenden sind, kann anhand dieser Tabelle entschieden werden.