Preparing the Active Directory Server

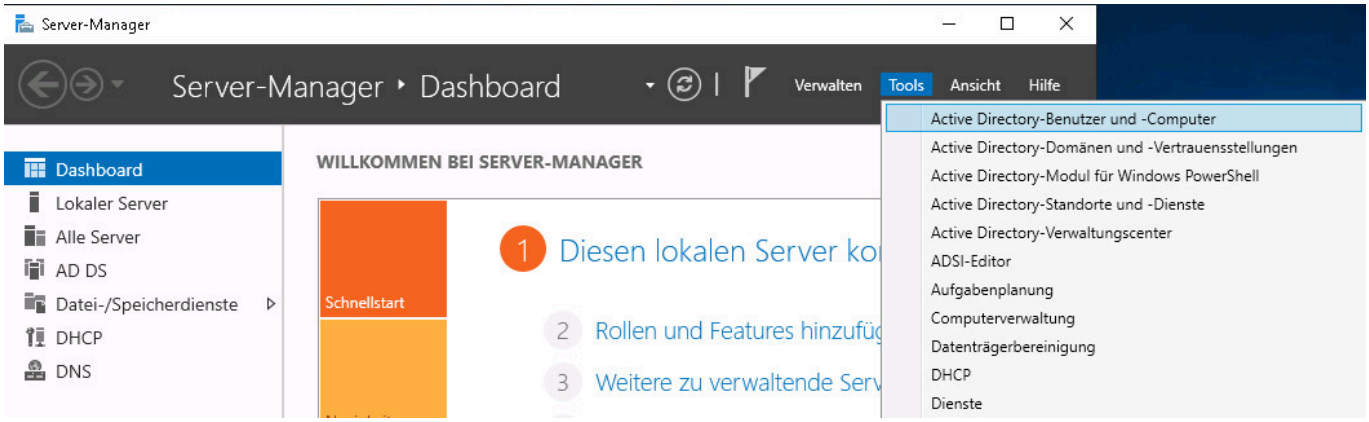
The Windows server that is to be used as the Active Directory must basically be prepared for processing domain services before setting up the connection of a TightGate-Pro, if it has not already been done. The preparation is divided into four steps:

- In the first step, a computer account for TightGate-Pro is created on the AD server.
- In the second step, a keytab file for the authentication of TightGate-Pro is created on the AD server.
- In the third step, the DNS settings are to be made so that TightGate-Pro can be found in the network by the TightGate clients.
- In the fourth step, the AD security groups are to be created.

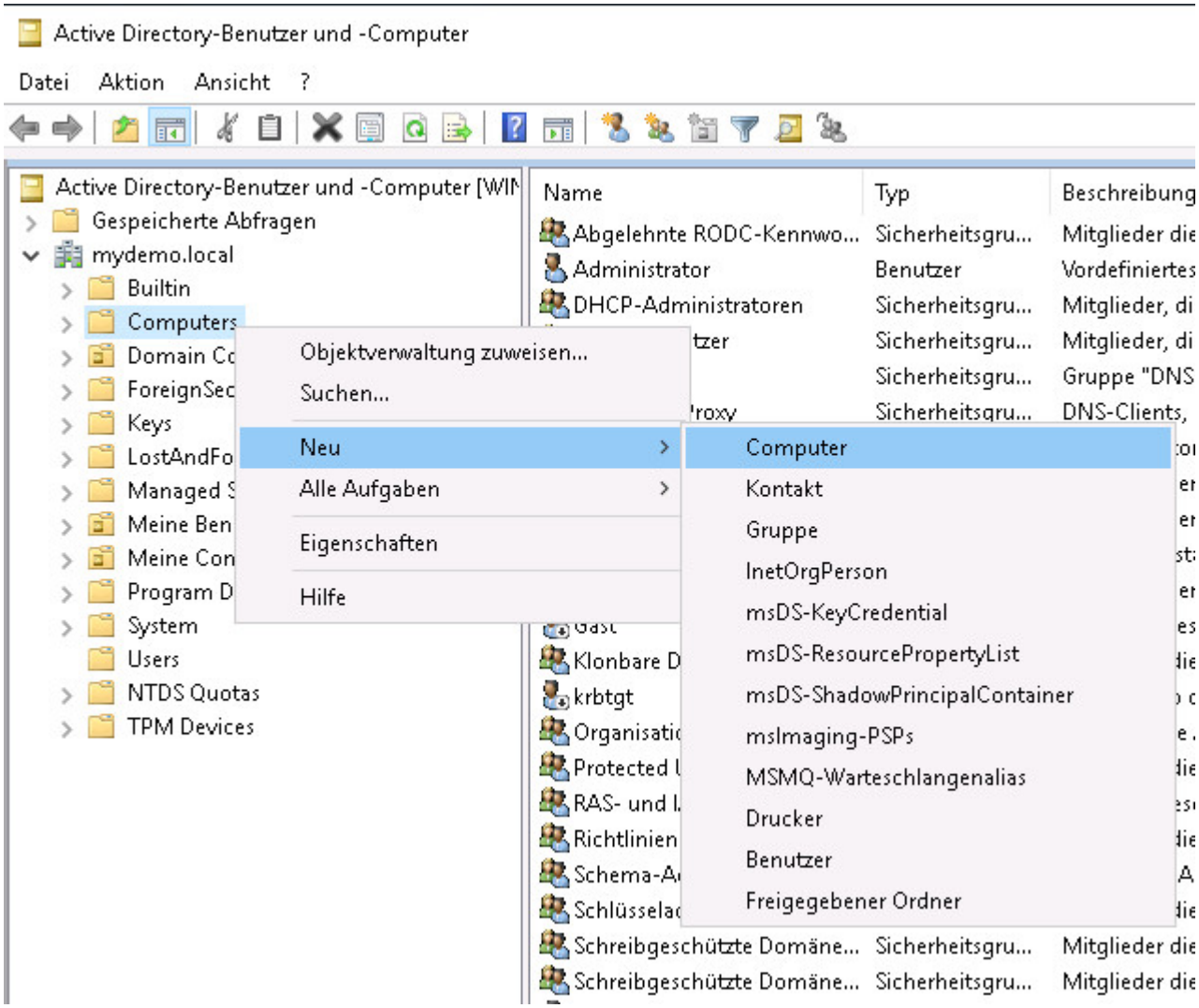
Creating a computer account

First, TightGate-Pro must be created on the AD server as a so-called computer account in the correct domain. This applies equally to single systems and cluster systems. In the example the computer account on the AD server is called **TGPro** in the case of a single system and **srv-TGPro** in the case of a cluster system.

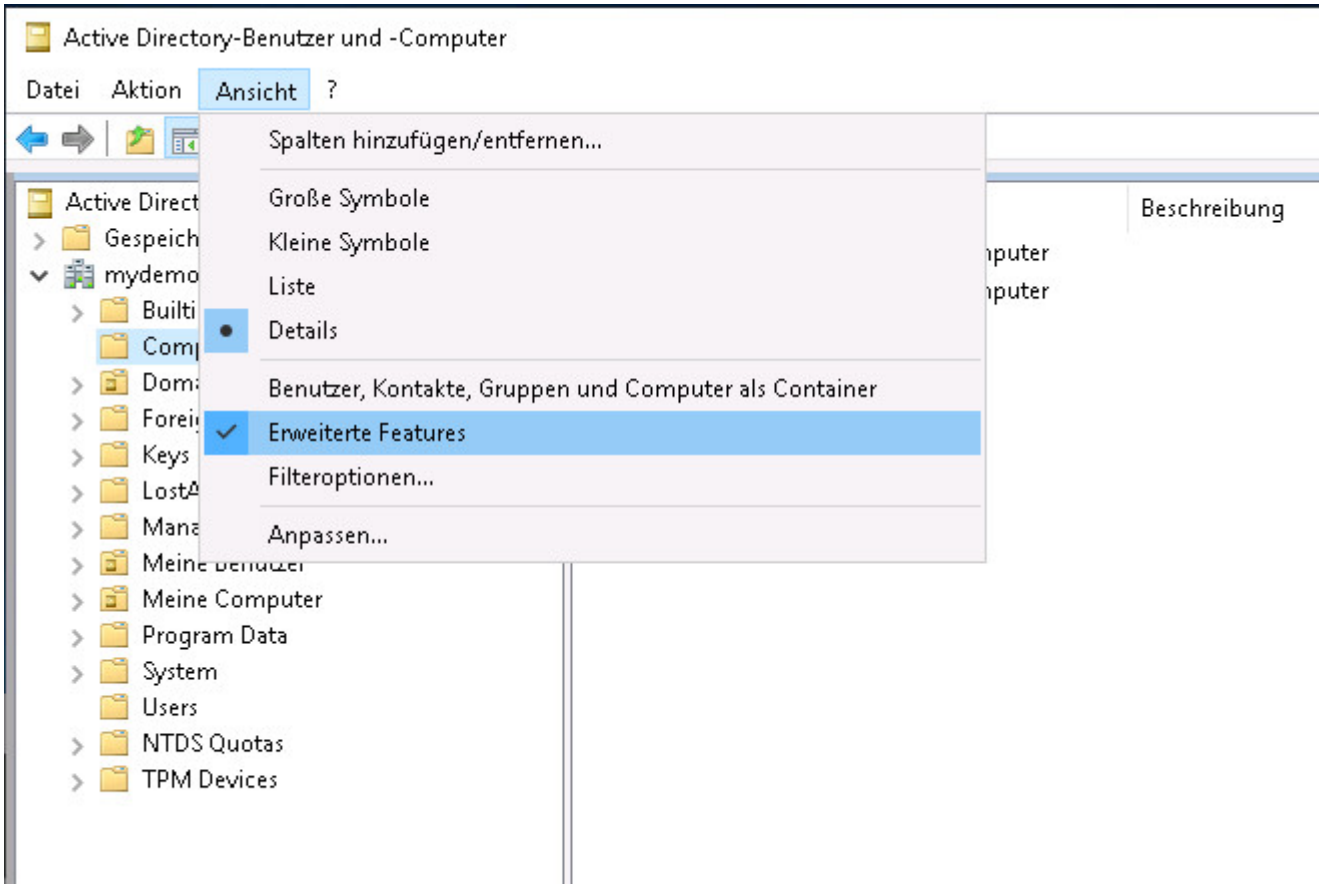
You create the computer account by clicking on **Tools > Active Directory Users and Computers** in the Server Manager.



In the next window, right-click on **Computer** in your domain and then click on **New > Computer** in the context menu.

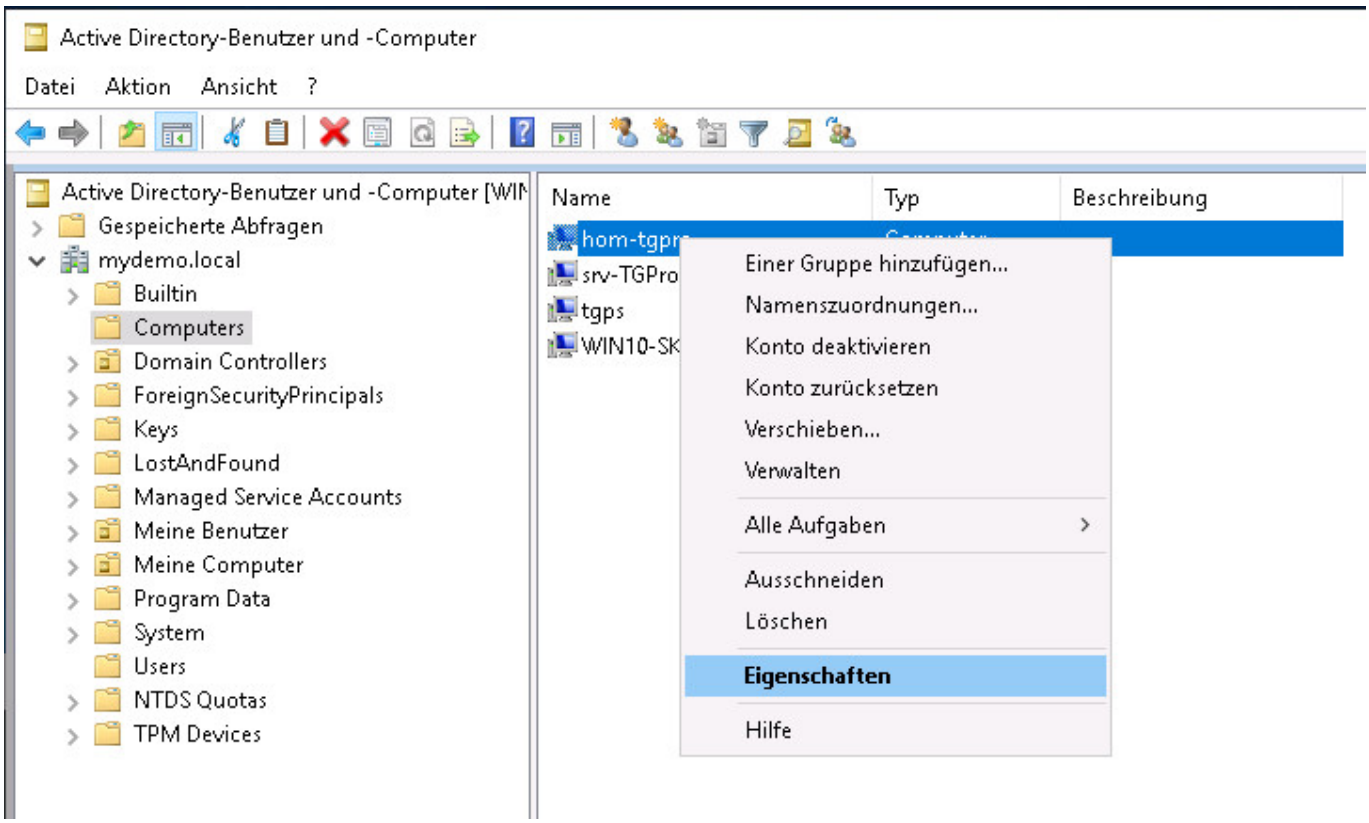


After creation, the computer account must be further customised. In the window **Active Directory Users and Computers** a more detailed list of the individual components of the domain of the AD server (ADS-REALM) can be displayed for this purpose under **View > Advanced Features**.

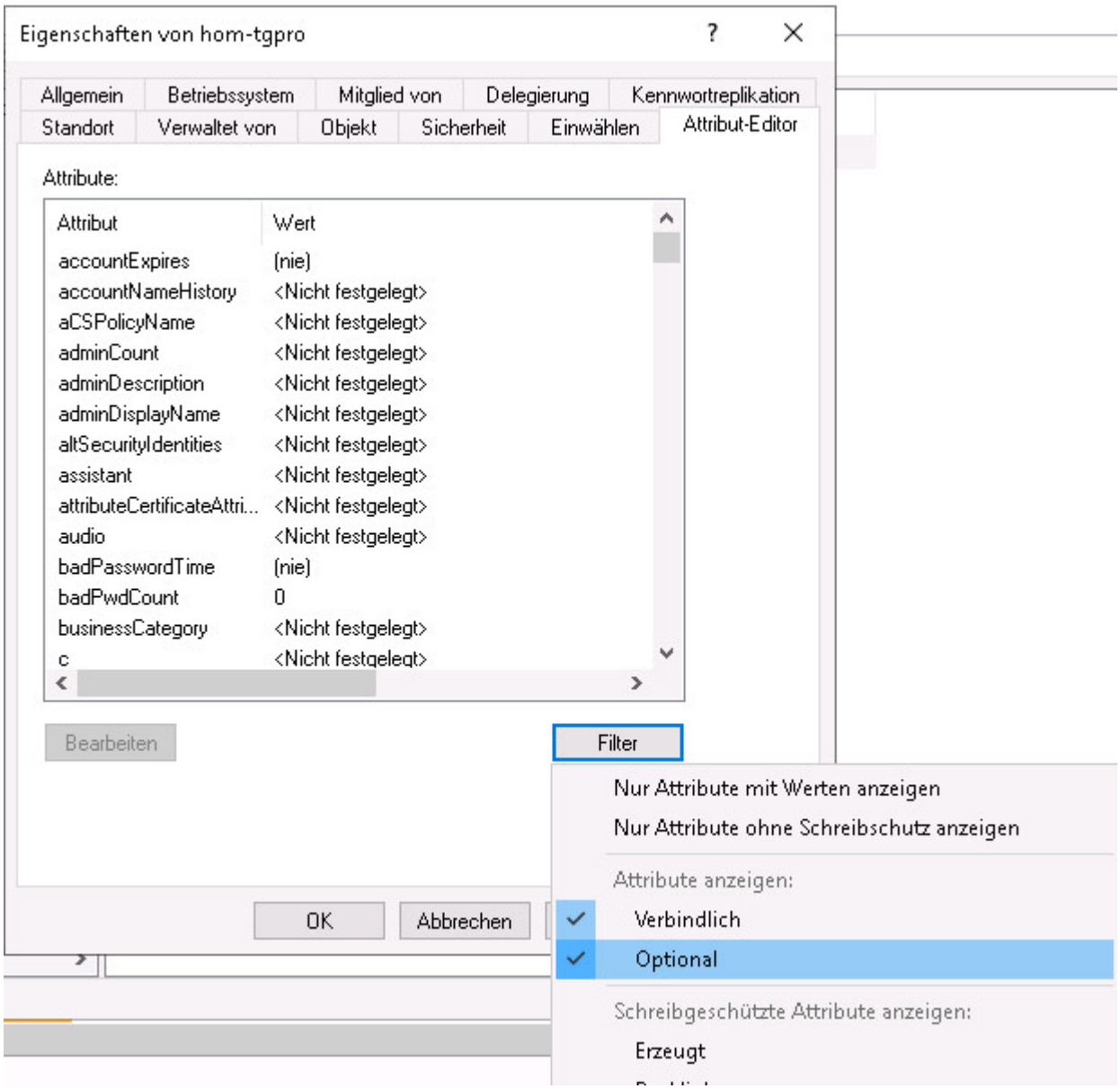


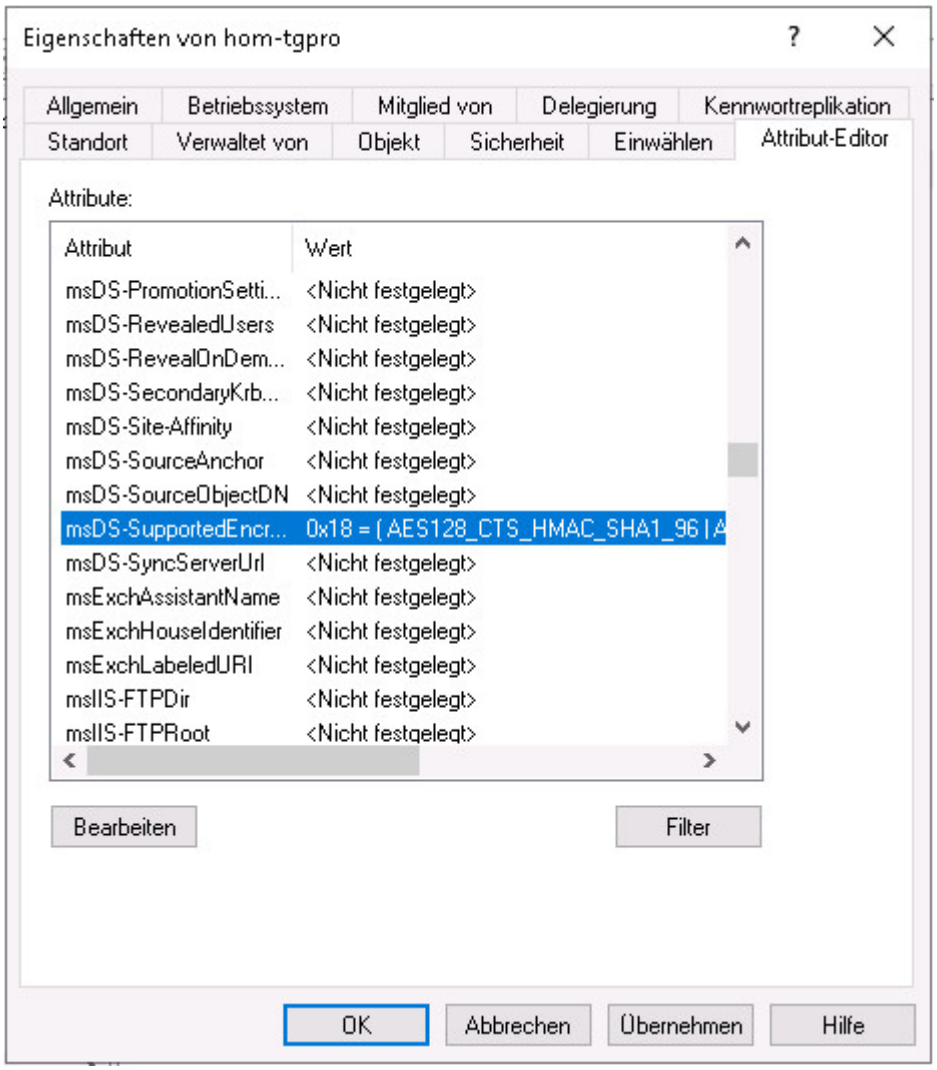
Encryption

The list of existing computer accounts is displayed after clicking with the left mouse button on **Computers**. A click with the right mouse button on the computer account of TightGate-Pro Server, in the example either **TGPro** or **srv-TGPro**, opens a context menu from which the configuration dialogue via **Properties** can be called up.



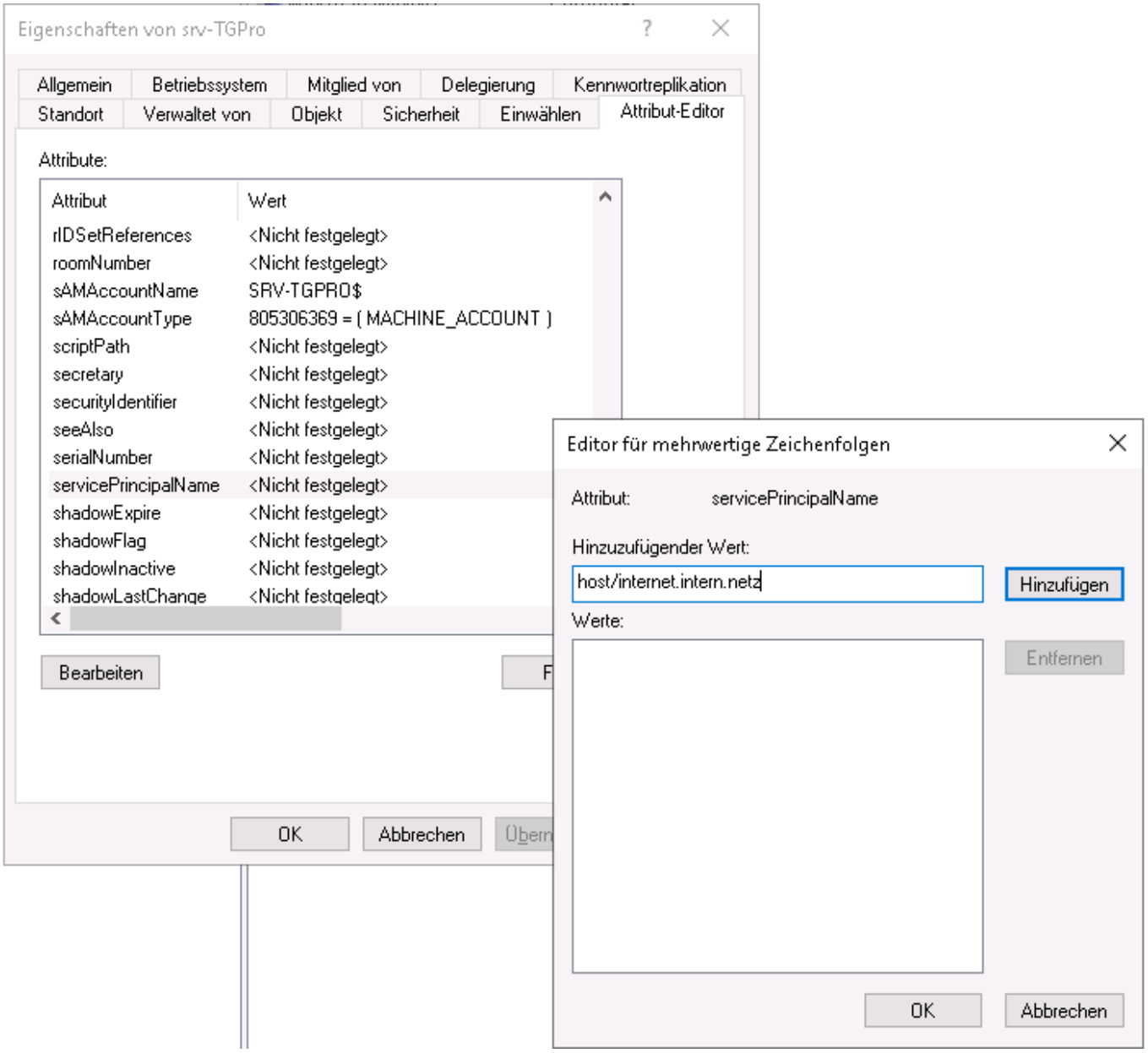
In the next step, settings must be made in the attribute editor. Switch to the tab button **Attribute Editor** and first make sure by clicking on the filter button that the check mark is set under **Show Attributes > Optional**.





For both single and cluster systems, the encryption types for the computer account of TightGate-Pro are to be set on the tab key **Attribute Editor**. Only the value **msDS-SupportedEncryption Types** from the selection list is to be set to the decimal value **24** (hexadecimal **0x18**). To do this, select the relevant parameter in the selection list by clicking on it with the left mouse button (coloured background visible) and enable it for modification by clicking on the button **Edit**.

Furthermore, the attribute **servicePrincipalName** must be set to the value **host/[domain of the TG-Pro cluster or DNS name of the individual system]**. The entry in the example is therefore: - For the cluster: **host/internet.intern.netz** - For the individual system: **host/TGPro.sso.m-privacy.hom**.



Create keytab file for TightGate-Pro

In order for TightGate-Pro to authenticate itself on the AD server, the former requires a special certificate that is contained in a so-called keytab file. This keytab file is generated once on the AD server by specifying certain parameters and made available to TightGate-Pro.

Warnung

Please make sure that you generate the **keytab** with that of a user ID that is in the default security group **Administrator** of the Active Directory. Creating a keytab from another security group, such as Domain Administrators or Enterprise Administrators, can be done, but it will not authenticate TightGate-Pro requests to the Active Directory server.

The command **for individual systems** on the AD server to create the keytab file is issued via the Windows Power Shell and has the following 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
```

The command for ***cluster systems (federated computers)*** on the AD server to create the keytab file has the following 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
```

Attention: The command is to be entered without line breaks and only with spaces between keywords and parameters. The upper/lower case must be observed.

The following overview explains the meaning of the parameters when creating the keytab file:

Keyword	Description	Example value
/out	Name of the output file. **Attention:** This file name must always end with .keytab.	TGPro.keytab
/mapuser	Specifies the target system for which the generated keytab file is to apply, in this case TightGate-Pro Server, in the format [computer name of TG-Pro]$@[ADS-REALM]	TGPRO$@SSO.M-PRIVACY.HOM
/princ	Specifies the principal name	**For single systems:** host/TGPro.sso.m-privacy. hom@SSO.M-PRIVACY.HOM **For cluster systems:** host/internet.intern.netz@SSO.M-PRIVACY.HOM
/rndPass	Random password generated by the system.	No value needs to be set.
/crypto	Specifies the keys that are embedded in the keytab file. **Attention:** Only the cryptographic type AES256-SHA1 is supported by TightGate-Pro Server.	AES256-SHA1
/ptype	Specifies the headmaster type, only the HOST service is required. **Attention:** The specified value must be set.	KRB5_NT_SRV_HST

The command line **for single systems** is according to the values set as an example:

```
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
```

The command line for **cluster systems** is according to the values set as examples:

```
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
```

The confirmation question must be answered with **Yes** / **Yes**.

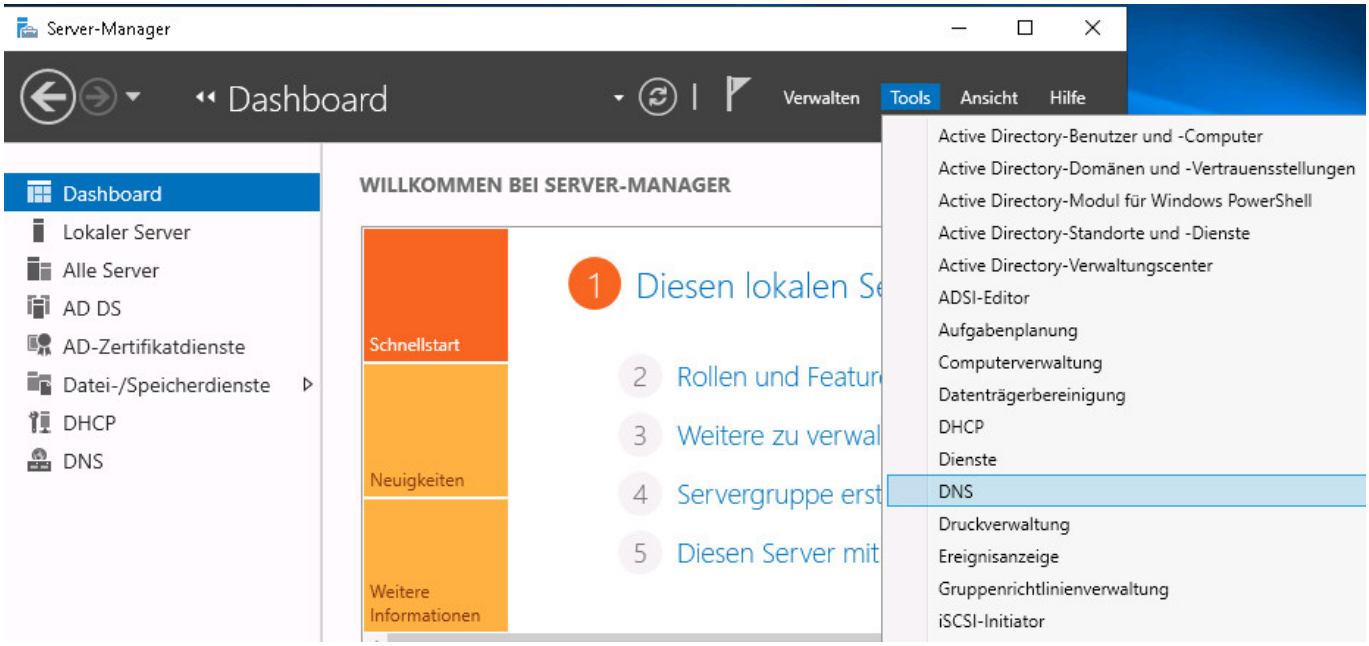
Finally, the generated keytab file must be deposited in the administrator's transfer directory ***config*** on TightGate-Pro.

Create DNS entries

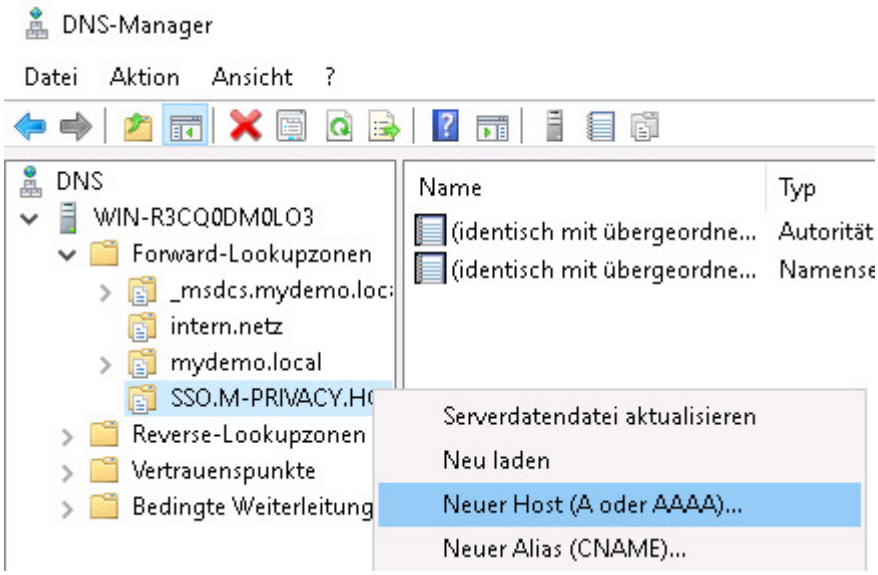
The type of DNS entry for TightGate-Pro differs depending on whether TightGate-Pro is operated as a single system or as a cluster system. While a simple host entry is sufficient for single systems, DNS zone forwarding must be set up for cluster systems so that the load distribution of the users to the individual nodes of TightGate-Pro functions correctly.

DNS entry for individual systems

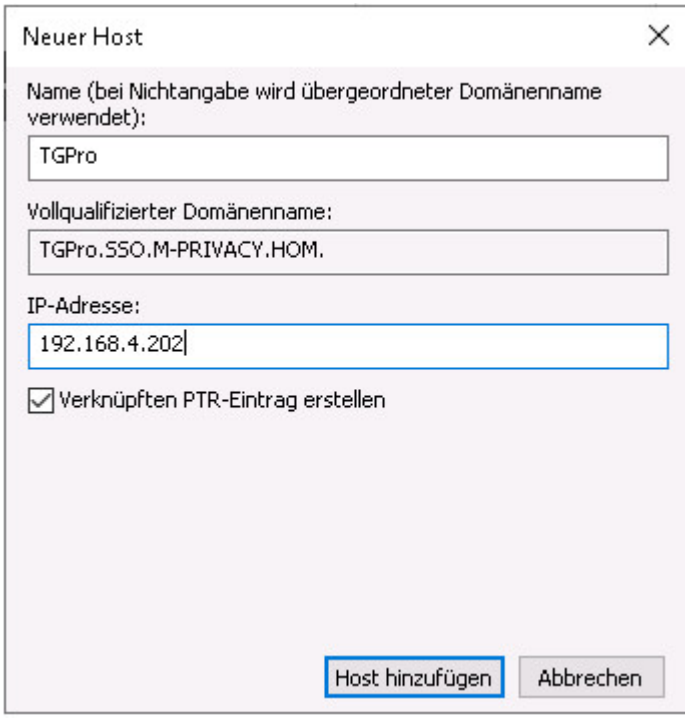
In the Server Manager, click on **Tools > DNS**.



The menu tree at **DNS server** must be expanded until the available **forward lookup zones** are visible. After clicking with the right mouse button on the corresponding domain of the AD server (ADS-REALM), in this example SSO.M-PRIVACY.HOM, a dialogue can be called up via **New Host (A or AAAA) ...**, via which TightGate-Pro can be assigned.



The resolvable name of TightGate-Pro must be entered as the name, as well as the IPv4 address of the server. The checkbox **Create linked PTR entry** must be activated in any case so that the host name is automatically entered in the reverse lookup zone as well. The dialogue box is to be left via the button **Add host**. It is recommended to check whether the name of TightGate-Pro can be resolved correctly forwards and backwards.



DNS Setup for Cluster Systems

Powerful ReCoB servers of the TightGate-Pro product line are delivered in a cluster system for capacity reasons. This network consists of several individual computers called "nodes". Within the network, TightGate-Pro has an automatic load distribution. This load distribution, also called "load balancing", is the basis for optimised system operation.

In order for the load balancing to work properly, the individual computers in the network must not be

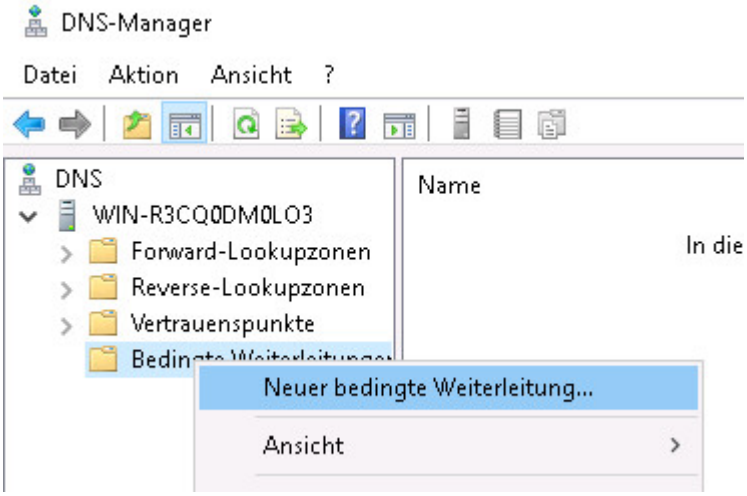
addressed by the client computers via their IPv4 address or their host name. Instead, the entire cluster of TightGate-Pro must appear as a unit in the internal network. All connection requests to TightGate-Pro must be transferred to special nodes that perform the task of load distribution.

This is achieved by sending the connection requests to a central computer name (own DNS zone) which represents the computer cluster.

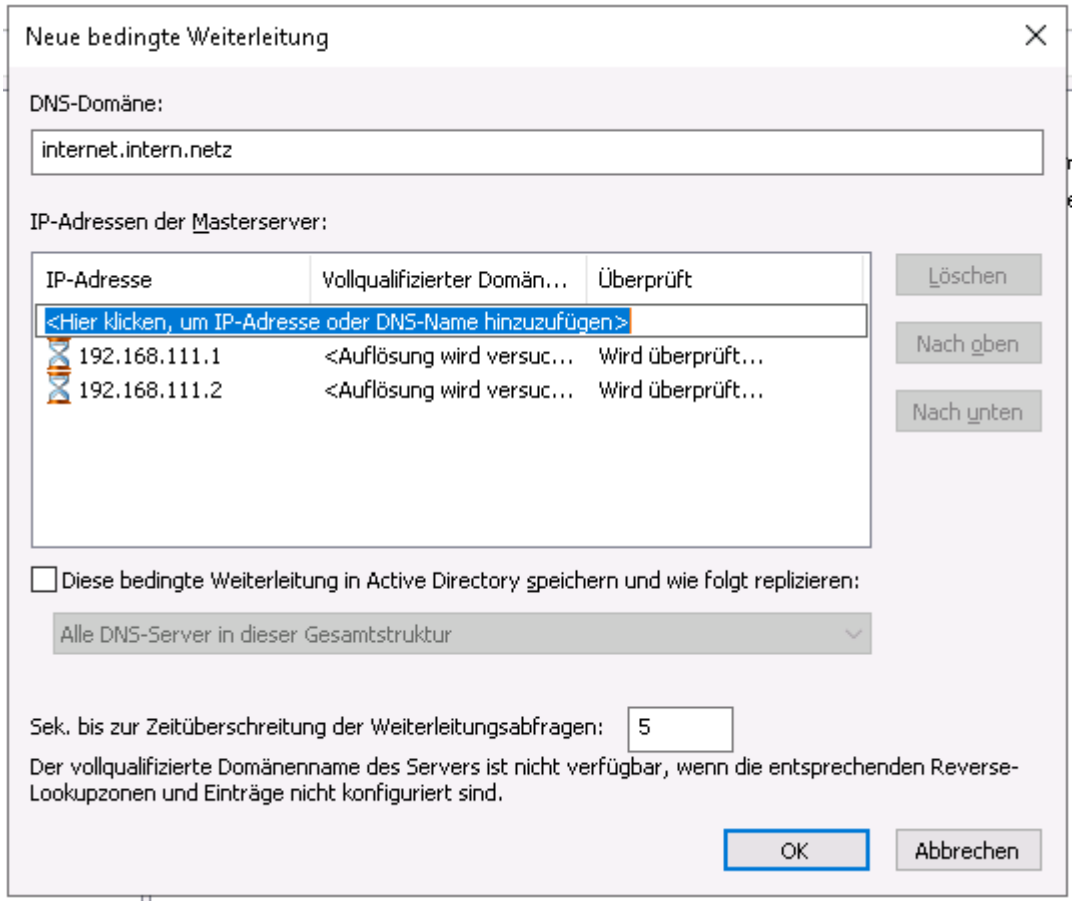
The following instructions describe how to set up DNS zone forwarding under Microsoft Windows.

a) Settings on the DNS server

- Select the menu item **Conditional Forwarding > New Conditional Forwarding…**



- In the dialogue window that opens, enter the domain name of the TightGate-Pro cluster (in the example: internet.intern.netz) under "DNS domain". In addition, the IPv4 addresses of the defined load balancers of the TightGate-Pro cluster are to be added as "IP addresses of the master servers".
  In the example, the IPv4 addresses of the nodes 192.168.111.1 and 192.168.111.2 are added, as these act as load balancers in this case.



- Next, set a **5** in the box next to the "Sec. until forwarding queries time out".
- Finish the settings by leaving the dialogue box with **OK**.

b) Set up reverse resolution (Reverse Lookupzone)

- Select the menu item **Reverse Lookupzones > New Zone...**
- Follow the wizard to create a reverse lookup zone for the domain of the cluster of TightGate-Pro (in the example internet.intern.netz).

Create AD security groups

In order for the group management of TightGate-Pro to be correctly transferred to the Active Directory, the corresponding security groups must be created on the central directory service. Please create the required security groups in your Active Directory system. The decision which security groups to use can be made using this table.