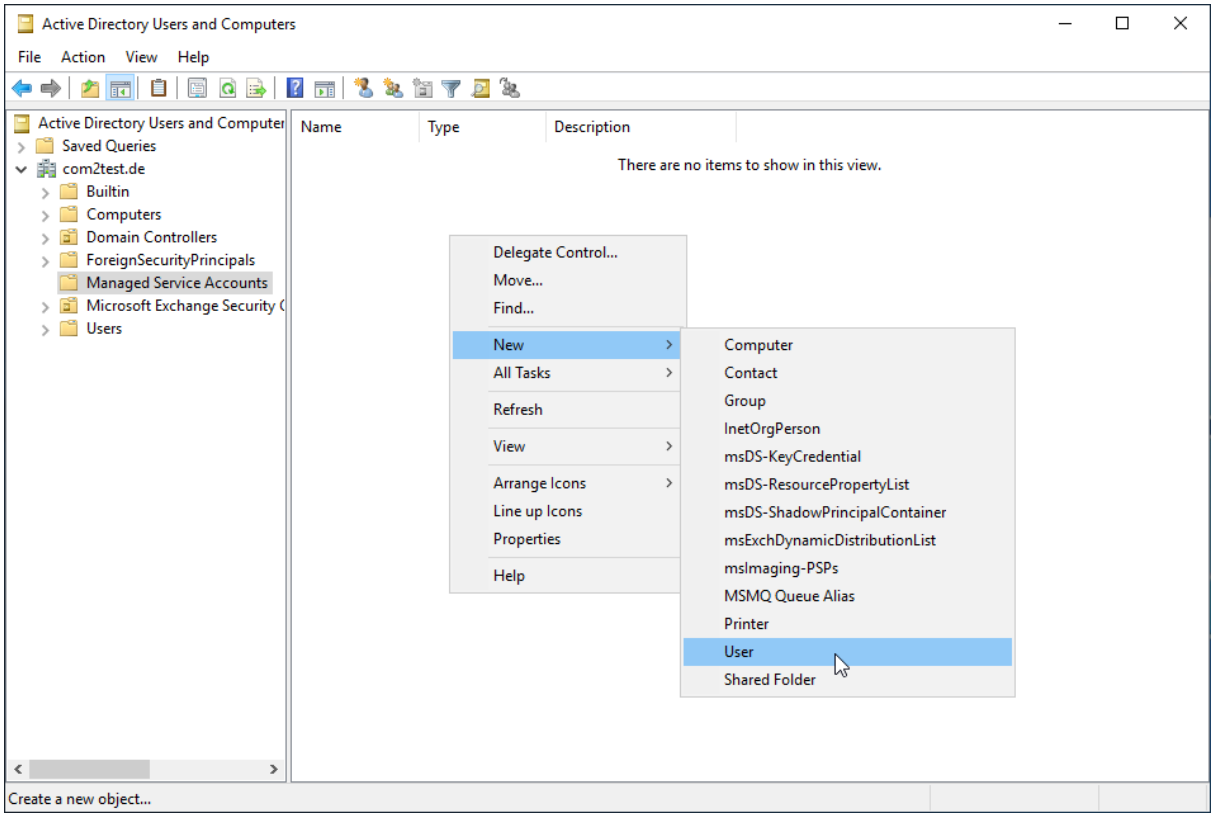
Produkt: NetOrchestra® MA

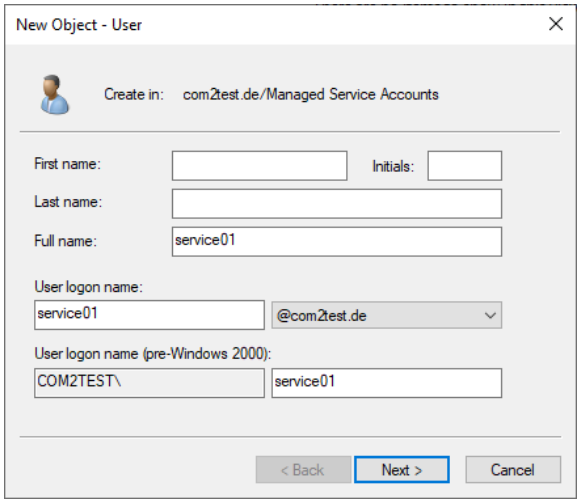
Kurzbeschreibung: Konfiguration der EWS Kerberos-Authentifizierung in Load-Balancer Umgebungen

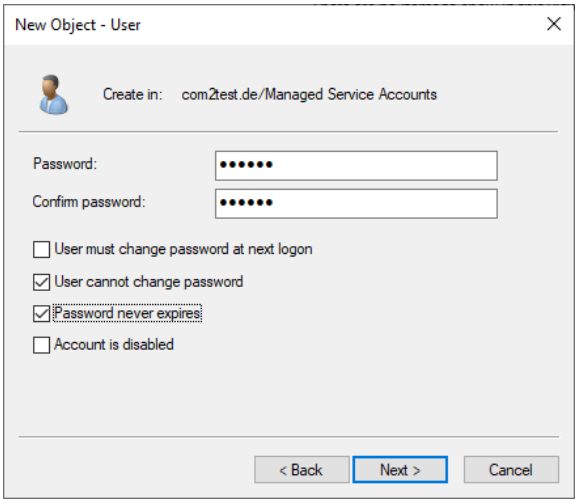
Diese Anleitung hilft Ihnen, das nachfolgend geschilderte Problem zu beheben. Dazu sollten Sie über gute bis sehr gute Kenntnisse im Betriebssystem Windows verfügen. Im Zweifelsfall empfehlen wir, einen Spezialisten hinzuzuziehen. ***Die com2 Communications & Security GmbH gibt keine Funktionsgarantie und übernimmt keine Haftung für Schäden oder Verlust an Hard- oder Software und/oder Datenbeständen, die durch Anwendung dieser Anleitung entstehen könnten.***

1. Service-Account erstellen

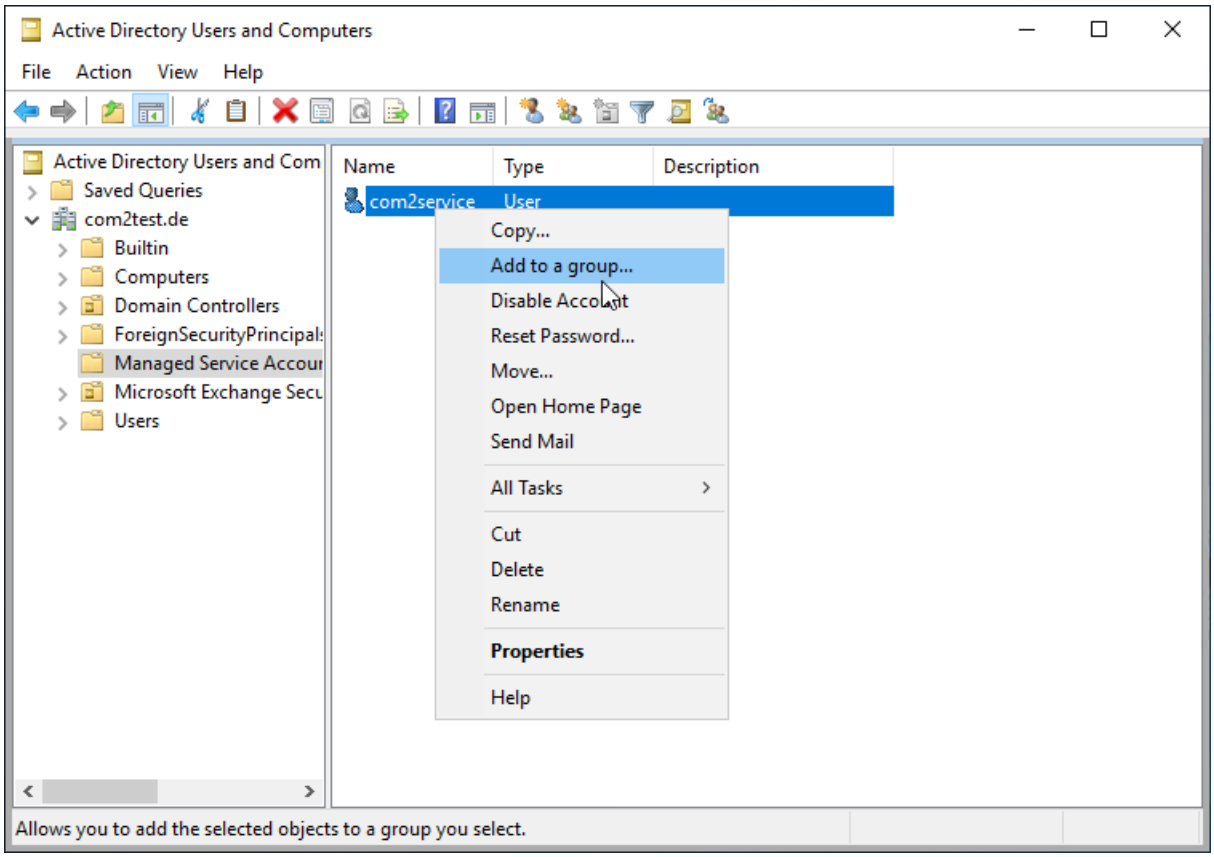
- Öffnen Sie die Anwendung `Active Directory-Benutzer und -Computer`.
- Legen Sie unter `Managed Service Accounts` einen neuen User an.

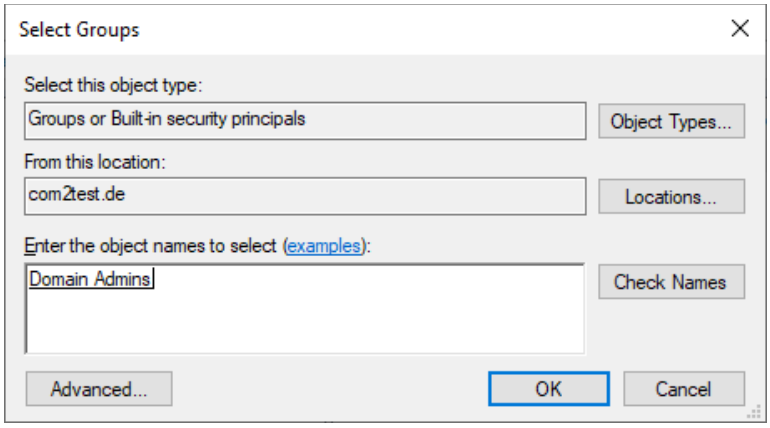






- Fügen Sie den User der Gruppe der Domänenadministratoren hinzu.

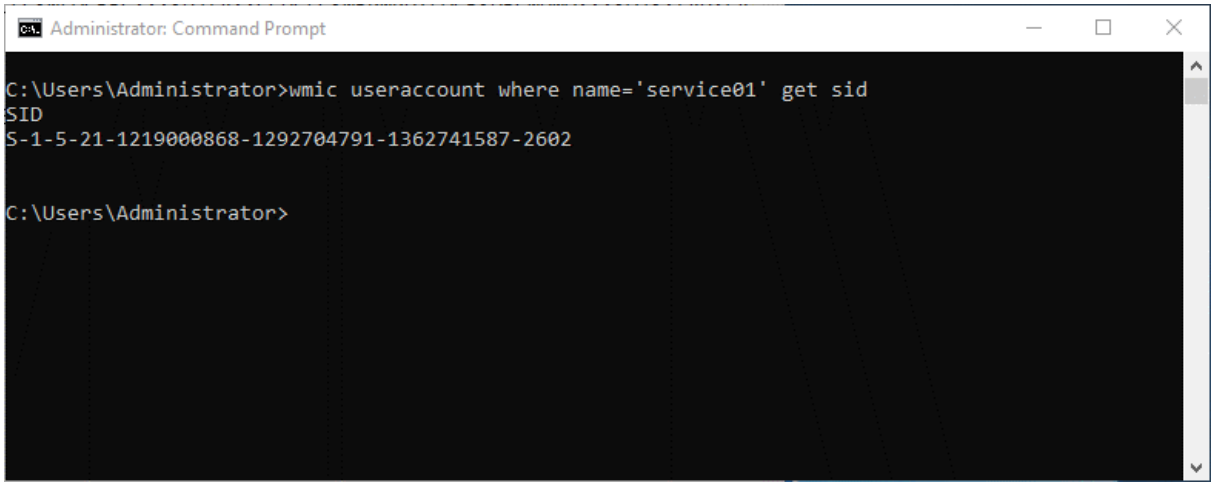




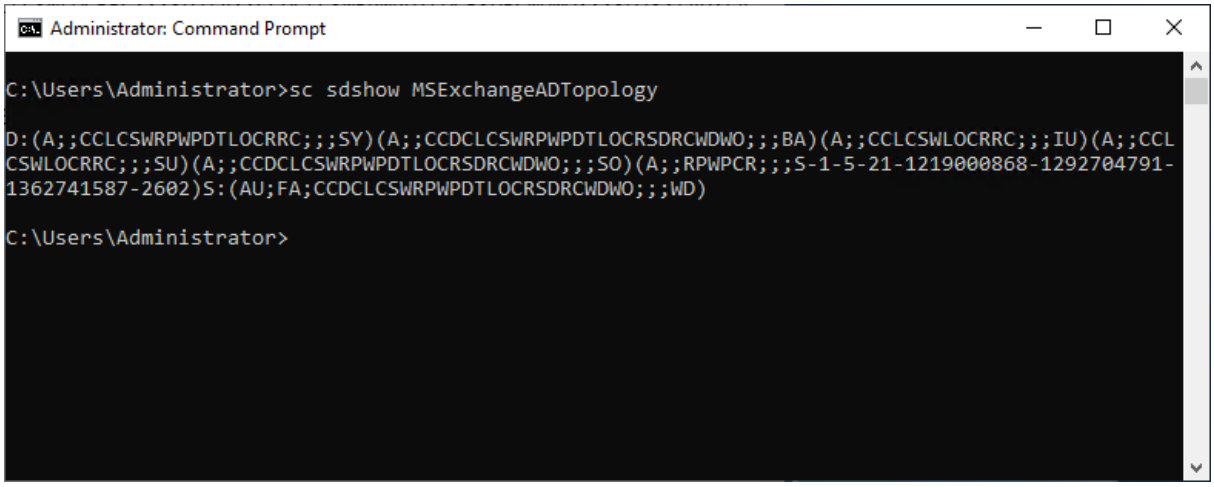
Nun muss dem neuen User das Recht erteilt werden auf den Dienst `MSExchangeADTopology` zugreifen zu dürfen. Hierfür muss zunächst die SID des Benutzers und der Security Descriptor des Dienstes ermittelt werden.

- Öffnen Sie eine Kommandozeile mit Adminrechten
- Führen Sie die nachfolgenden Befehle aus und notieren sich die Ausgaben:

SID des neu erstellen Benutzers ermitteln:
`wmic useraccount where name='service01' get sid`



Security Descriptor des Dienstes "MSExchangeADTopology" ermitteln:
`sc sdshow MSExchangeADTopology`



Mit den beiden Informationen kann nun der Befehl zum Erteilen des Rechts vorbereitet werden.

- Der zuvor ermittelte Security Descriptor beinhaltet einen Block beginnend mit D: und einen mit S:

  `D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDT-LOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)`

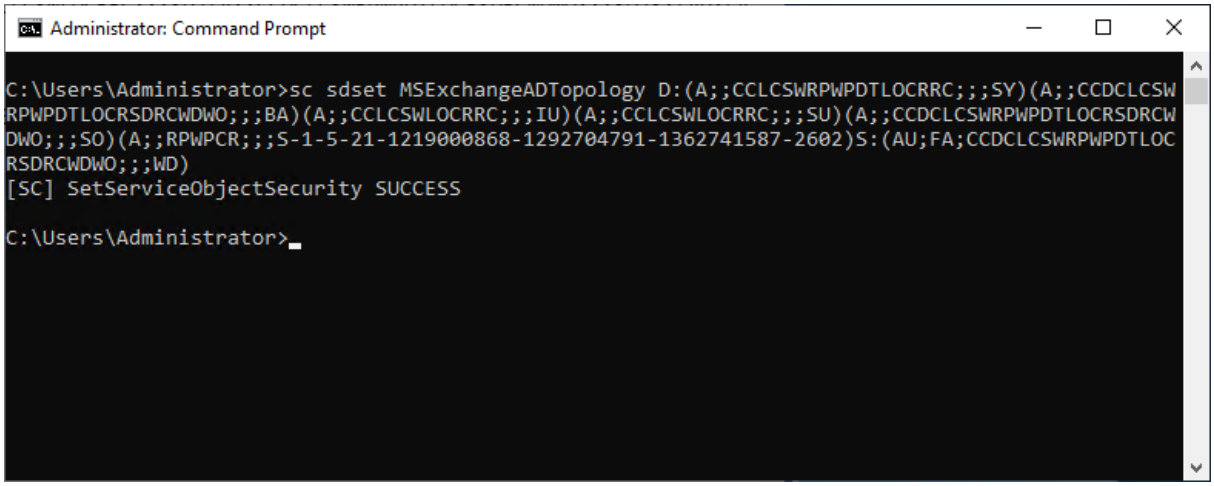
- Fügen Sie vor dem Block der mit S: beginnt die SID des Benutzers im folgenden Format ein:

  `(A;;RPWPCR;;;SID-DES-BENUTZERS)`

Somit ergibt sich in unserem Beispiel folgender Befehl:

```
sc sdset MSExchangeADTopology D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDT-
LOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDT-
LOCRSDRCWDWO;;;SO)(A;;RPWPCR;;;S-1-5-21-1219000868-1292704791-1362741587-
2602)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

- Führen Sie den Befehl aus, um dem ServiceAccount-Benutzer das Recht zu erteilen:



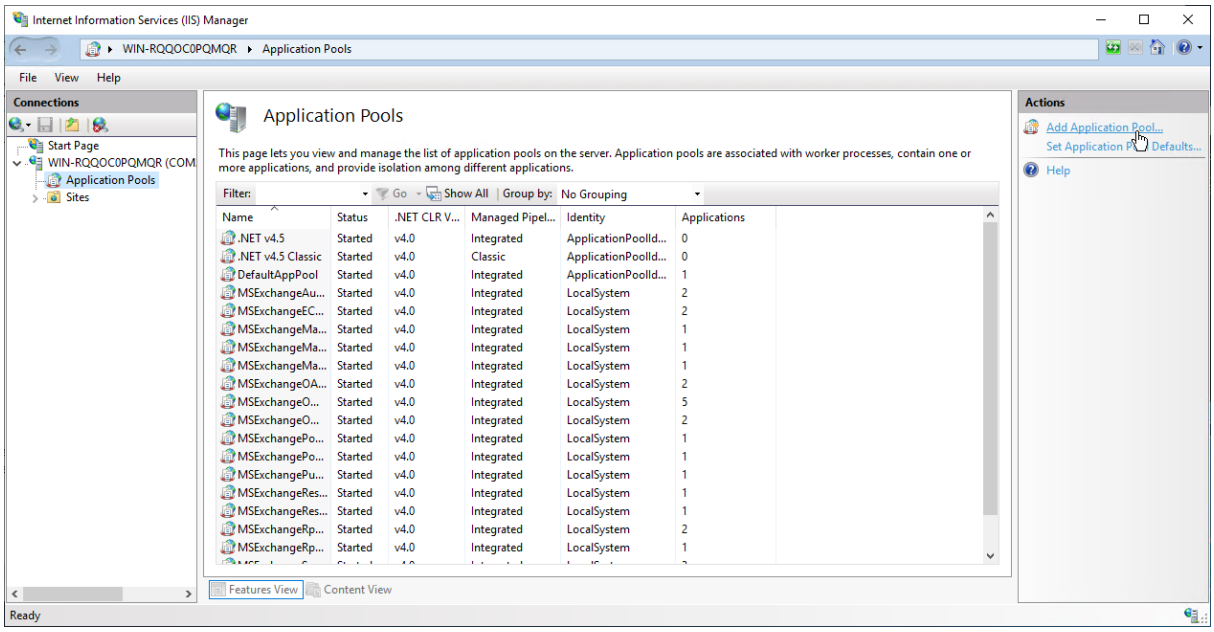
Nun muss dem Benutzer noch das Recht `ms-Exch-EPI-Token-Serialization` erteilt werden.

- Öffnen Sie die Exchange Management Shell und führen folgenden Befehl aus:

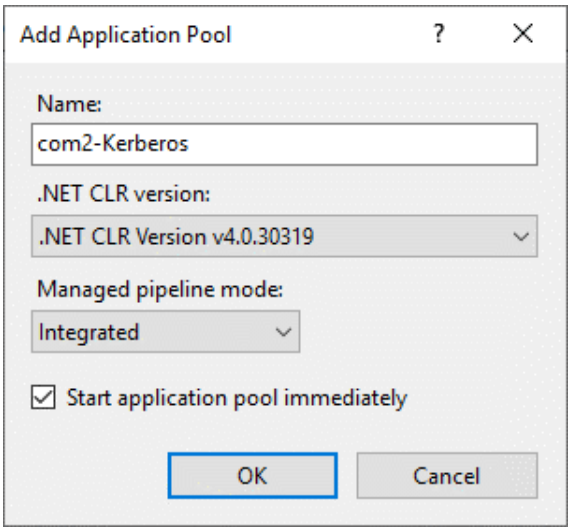
```
Get-MailboxServer <Rechnername> | Add-ADPermission -Accessrights Extendedright -
Extendedright "ms-Exch-EPI-Token-Serialization" -User "<Domäne>\<Kontoname>"
```

2. Neuen Application Pool in IIS erstellen

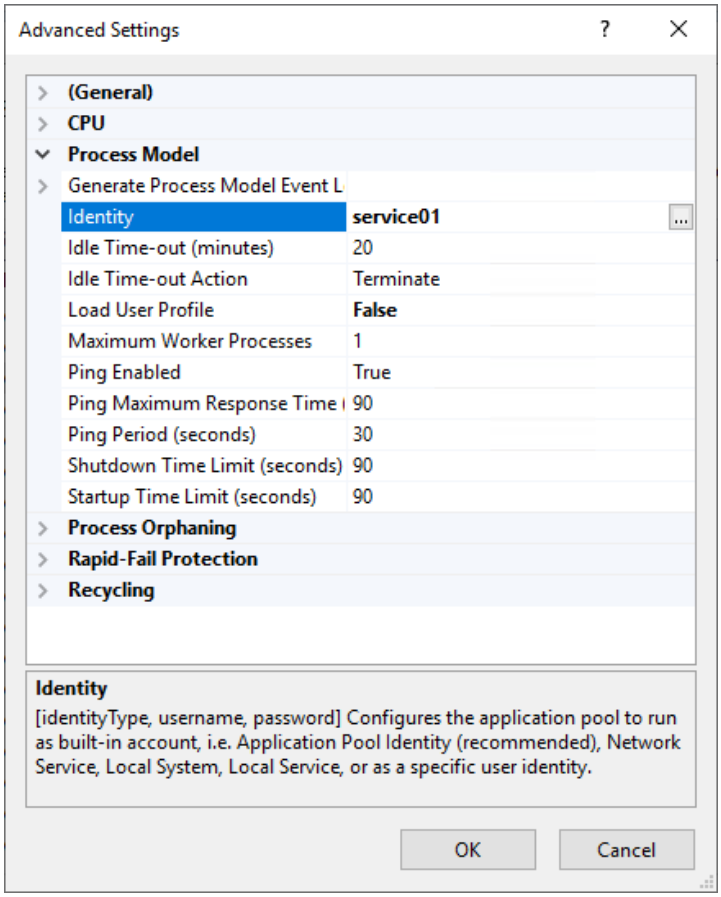
- Öffnen Sie den Internet Information Services (IIS) Manager.
- Wechseln Sie zu den Application Pools.
- Klicken Sie auf `Add Application Pool`.



- Geben Sie einen sinnvollen Namen an
- Belassen Sie die restlichen Einstellungen und klicken auf `[OK]`.

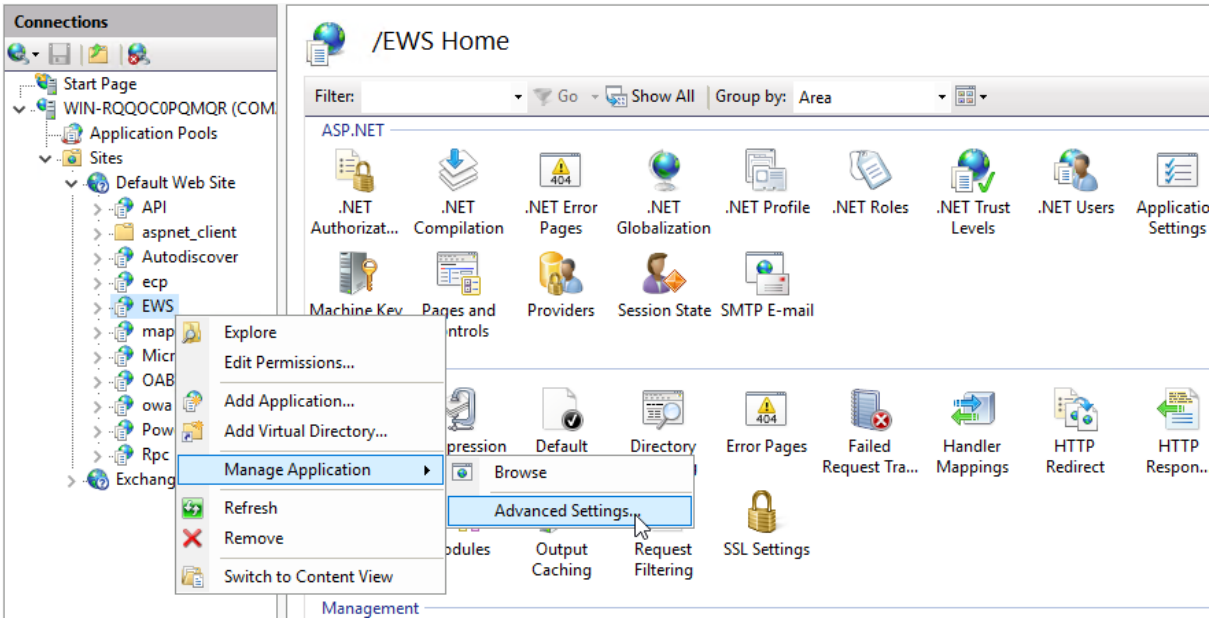


- Wählen Sie den neuen Application Pool in der Liste aus und öffnen die erweiterten Einstellungen.
- Geben Sie als `Identity` (unter `Process Model`) den neuen Service-Account an.

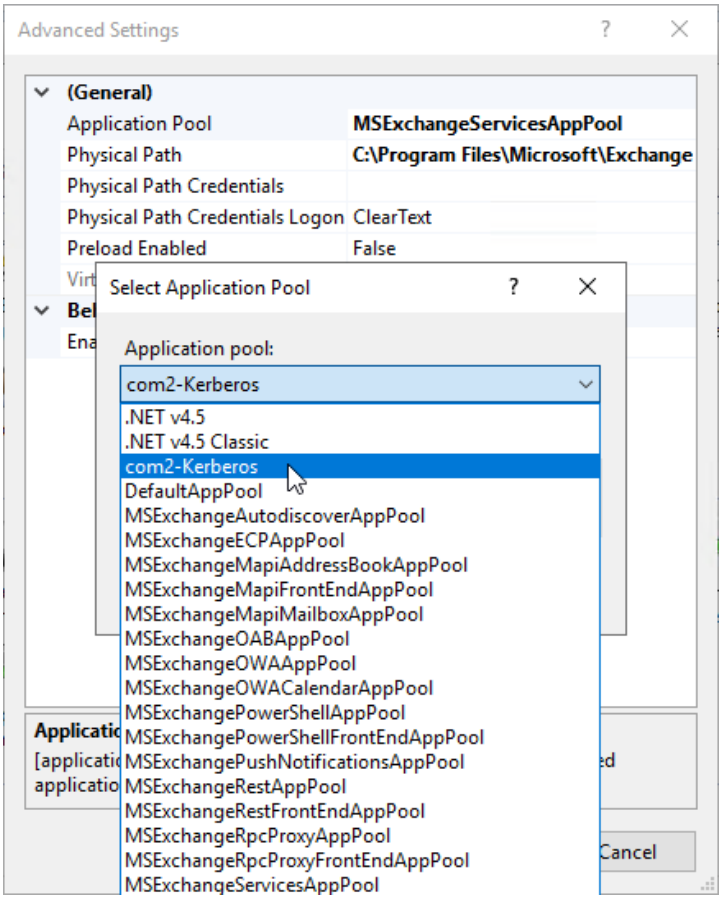


3. Neuen Application Pool der EWS-Application zuweisen

- Öffnen Sie die erweiterten Einstellungen der EWS-Applikation.

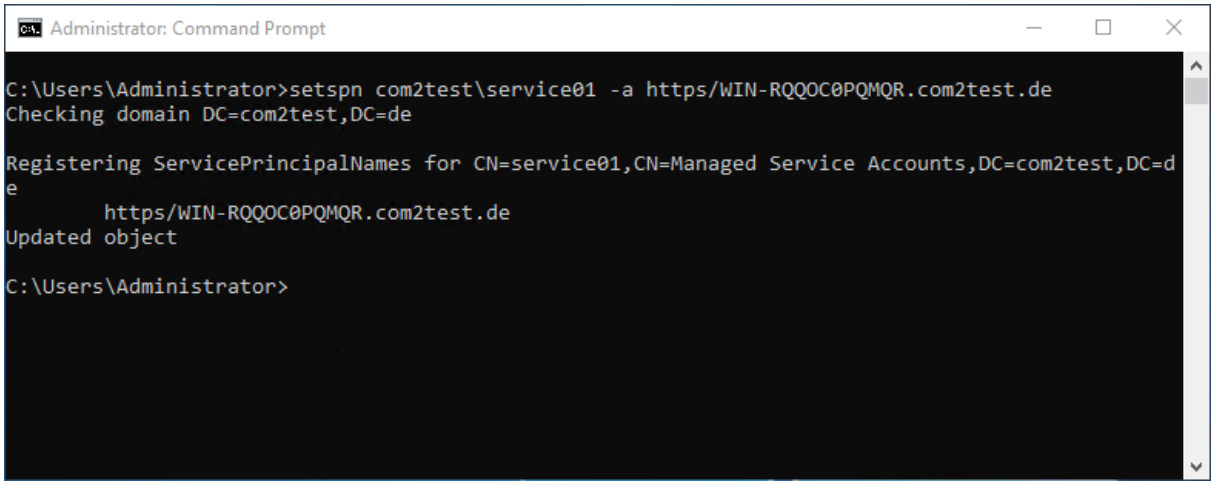


- Wählen Sie als `Application Pool` (unter `General`) den neuen Pool aus.



4. SPN für den neu erstellten Service erzeugen

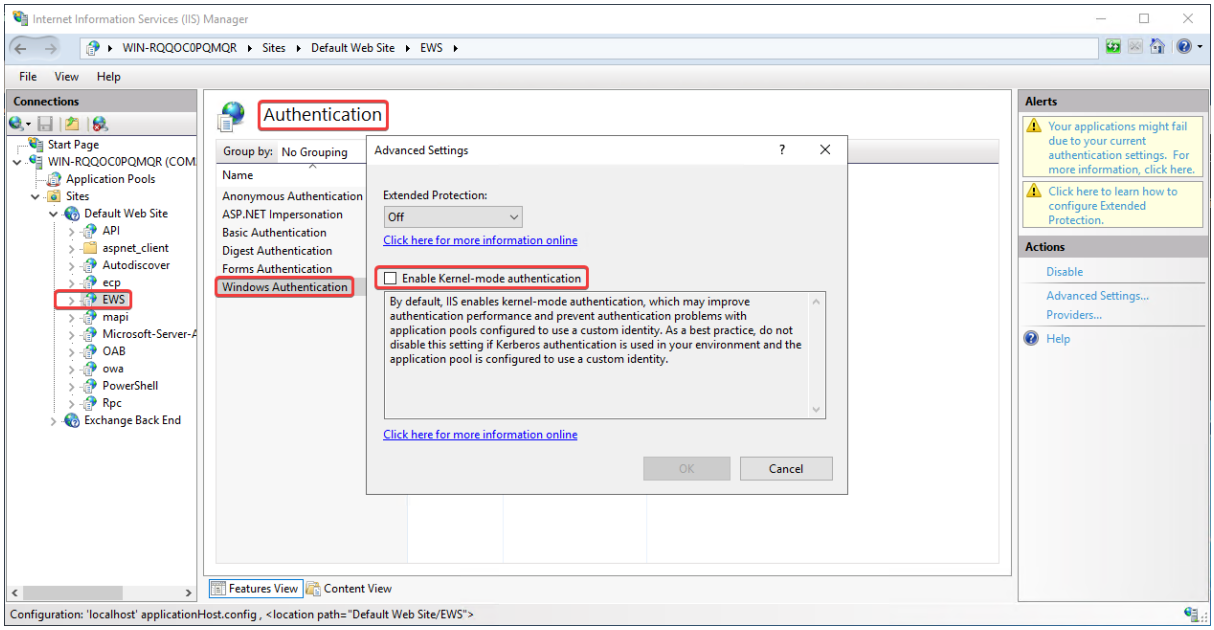
- Öffnen Sie eine Kommandozeile mit Adminrechten
- Führen Sie folgenden Befehl aus:
  `setspn <Domäne>\<Kontoname> -a https/<FQDN des Loadbalancers>`



5. Notwendige Einstellungen bei Kernelmodus-Authentifizierung

Wenn Sie die Kernelmodus-Authentifizierung für EWS nicht verwenden, können Sie diesen Schritt überspringen. Gehen Sie wie folgt vor um dies zu prüfen:

- Wechseln Sie in der EWS-Applikation zu `Authentication` > `Windows Authentication` > `Advanced Settings`.
- Anhand der Checkbox `Enable Kernel-mode authentication` erkennen Sie ob Sie den Modus verwenden.



Gehen Sie wie folgt vor, wenn der Modus verwendet wird:

- Öffnen Sie Datei `C:\Windows\System32\inetsrv\Config\applicationhost.config`.
- Ergänzen Sie diese um `useAppPoolCredentials="true"`.

6. Weitere CAS-Server konfigurieren

Die Schritte 2. 3. und 5. sowie die Rechtezuweisungen sind auf jedem beteiligten CAS-Server auszuführen.