# TechNote – EWS Kerberos-Authentifizierung in Load-Balancer-Umgebungen konfigurieren

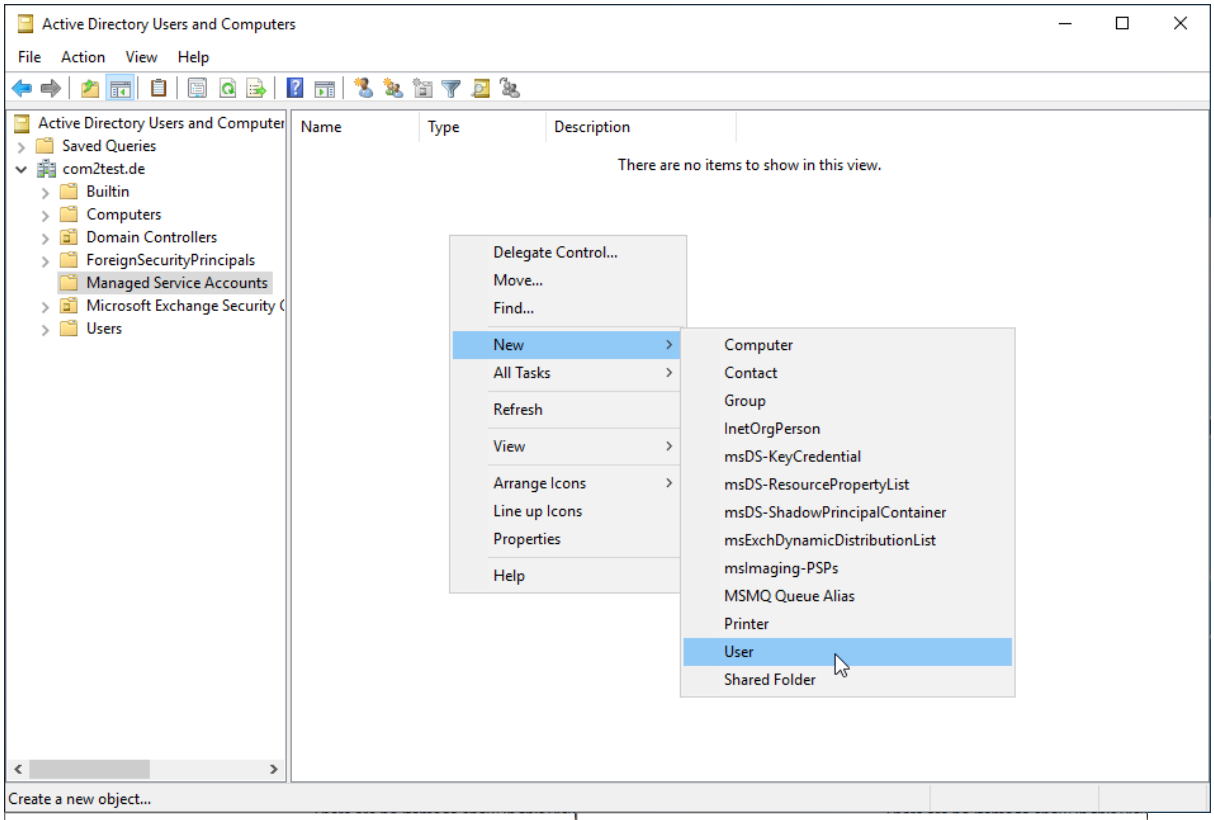
Produkt: NetOrchestra® MA

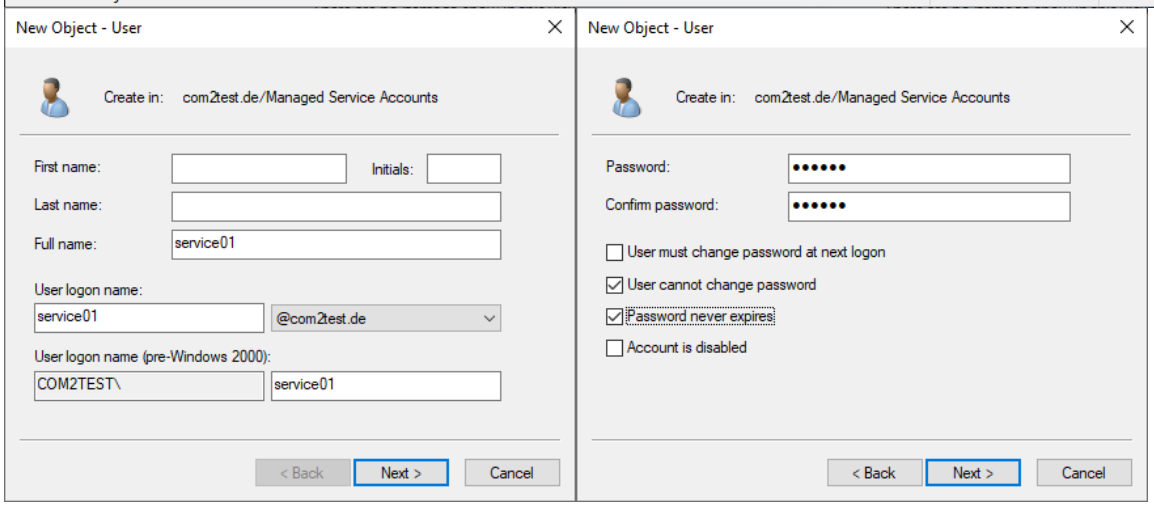
**Kurzbeschreibung:** ***EWS Kerberos-Authentifizierung in Load-Balancer-Umgebungen konfigurieren***

*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. Erstellung eines Service-Accounts

Öffnen Sie die Anwendung "Active Directory-Benutzer und -Computer" und legen für Ihre Domäne unter "Managed Service Accounts" einen neuen User an.



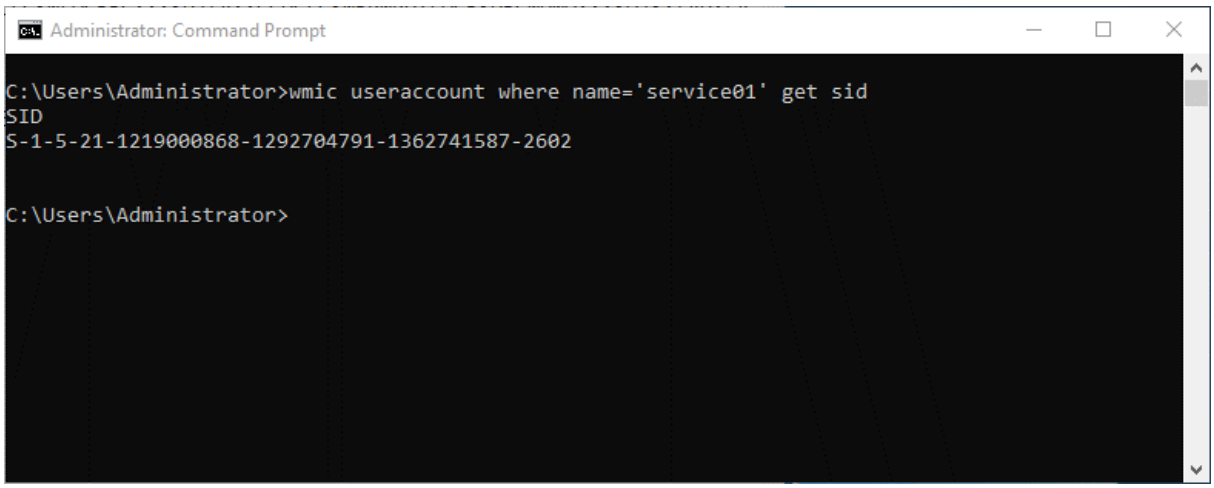



In den nachfolgenden Schritten wird dem Benutzer das Recht erteilt auf den Dienst "MSExchangeADTopology" zugreifen zu dürfen. Um den Befehl zum Erteilen des Rechts bilden zu können muss zunächst die SID des Benutzers sowie der Security Descriptor des Dienstes ermittelt werden.

Öffnen Sie dazu eine Kommandozeile mit Adminrechten, führen die nachfolgenden Befehle aus und notieren sich die Ausgaben.

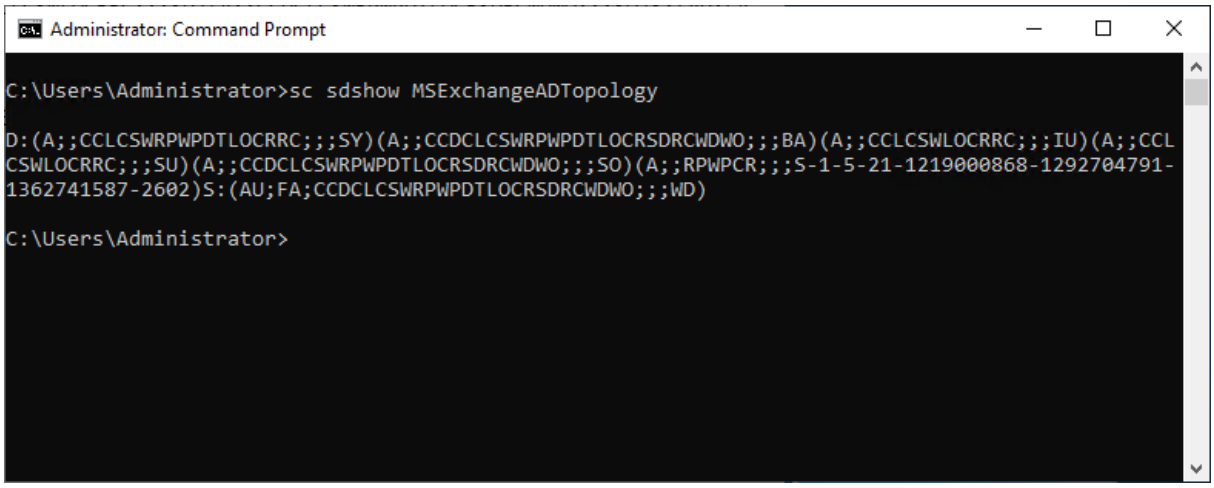
SID des neu erstellen Benutzers ermitteln:

```
wmic useraccount where name='service01' get sid
```




Security Descriptor des Dienstes "MSExchangeADTopology" ermitteln:

```
sc sdshow MSExchangeADTopology
```




Kombinieren Sie nun beide Ausgaben um somit den Befehl für das Erteilen des Rechtes bilden zu können. Wenn Sie sich den zuvor ermittelten Security Descriptor ansehen fällt Ihnen ggf. auf das es einen Block beginnend D: und einen mit S: gibt:

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

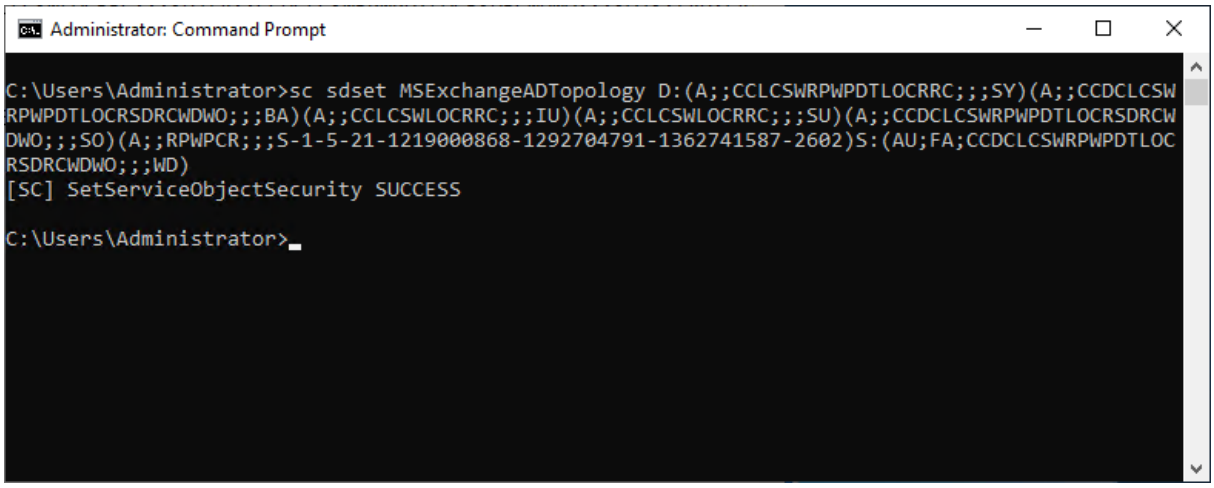
Zwischen diesen beiden Blöcken muss die SID des Benutzers in dem folgenden Format eingefügt werden:

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

In unserem Beispiel ergibt sich somit der folgende Befehl:

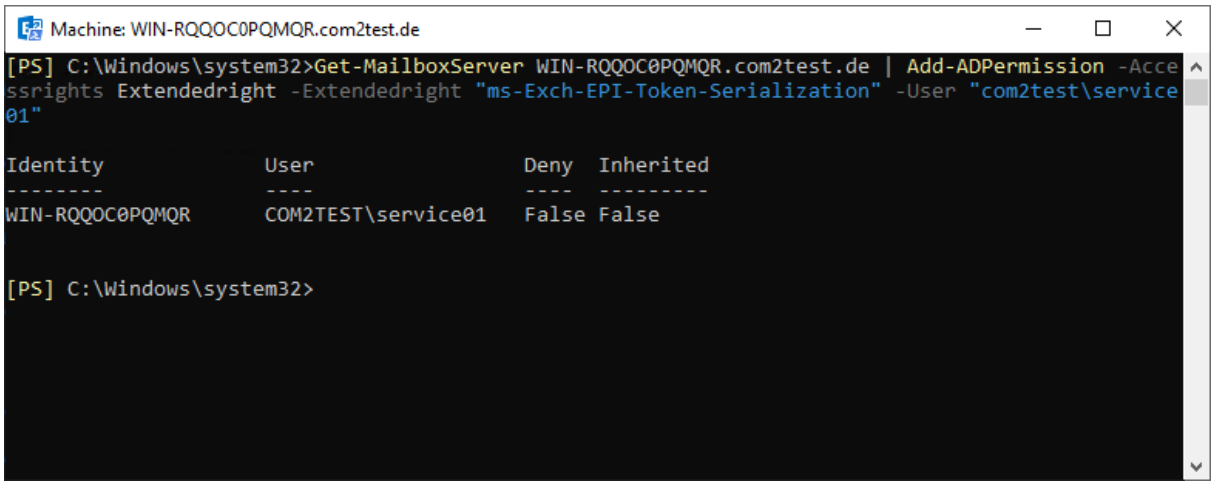
```
sc sdset MSExchangeADTopology
D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SO)(A;;RPWPCR;;;S-1-5-21-1219000868-1292704791-1362741587-2602)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
```

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



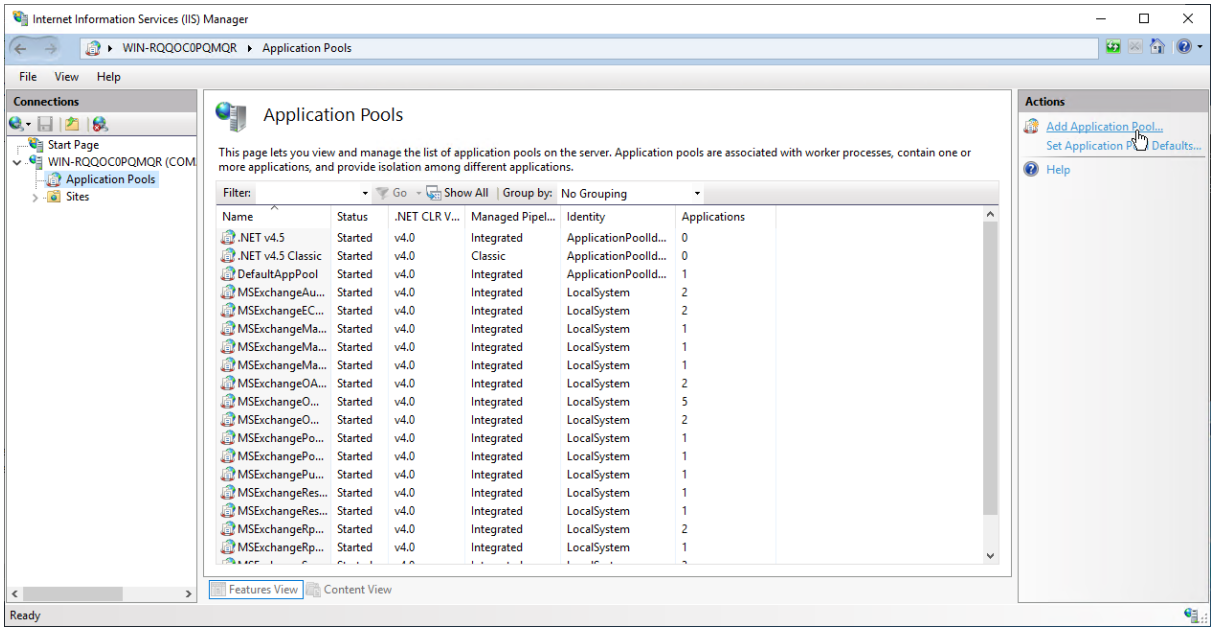

Nun muss dem Benutzer noch das Recht "ms-Exch-EPI-Token-Serialization" erteilt werden. Öffnen Sie hierfür die Exchange Management Shell und führen folgenden Befehl aus:

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

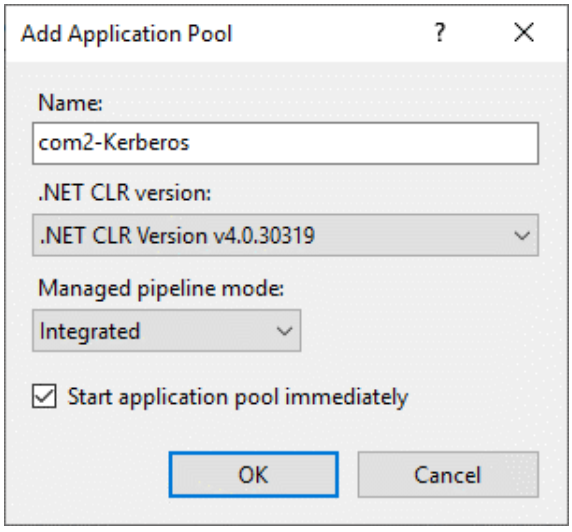


## 2. Erstellung eines neuen Application Pools im IIS

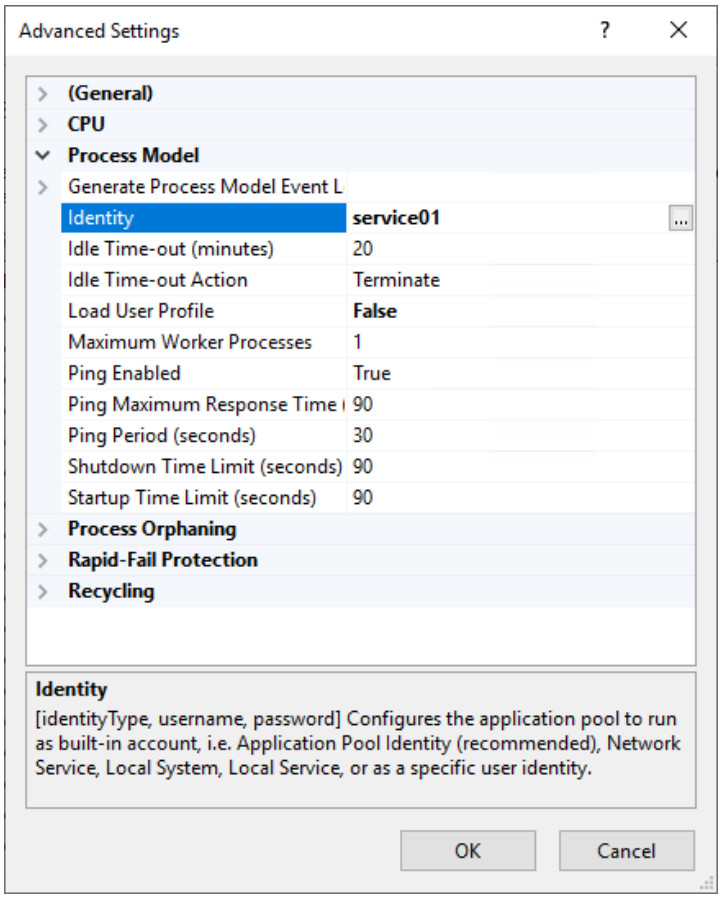
Öffnen Sie den Internet Information Services (IIS) Manager, wechseln über die Baumansicht unterhalb Ihres Servernamens zu den Application Pools und führen die Aktion "Add Application Pool" aus.




Geben Sie in dem nachfolgenden Dialog einen sinnvollen Namen an, belassen die Default-Einstellungen und klicken auf [OK].

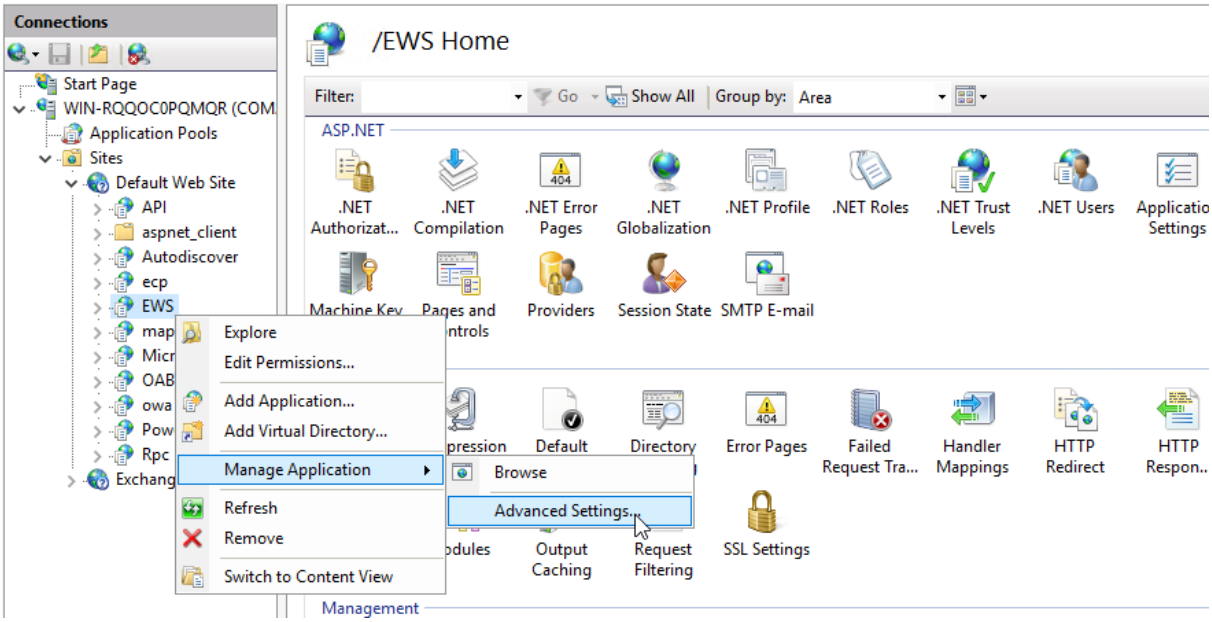


Wählen Sie nun den neuen Application Pool in der Liste aus und öffnen die erweiterten Einstellungen. Für die Einstellung Process Model > Identity muss der ServiceAccount-Benutzer angegeben werden.

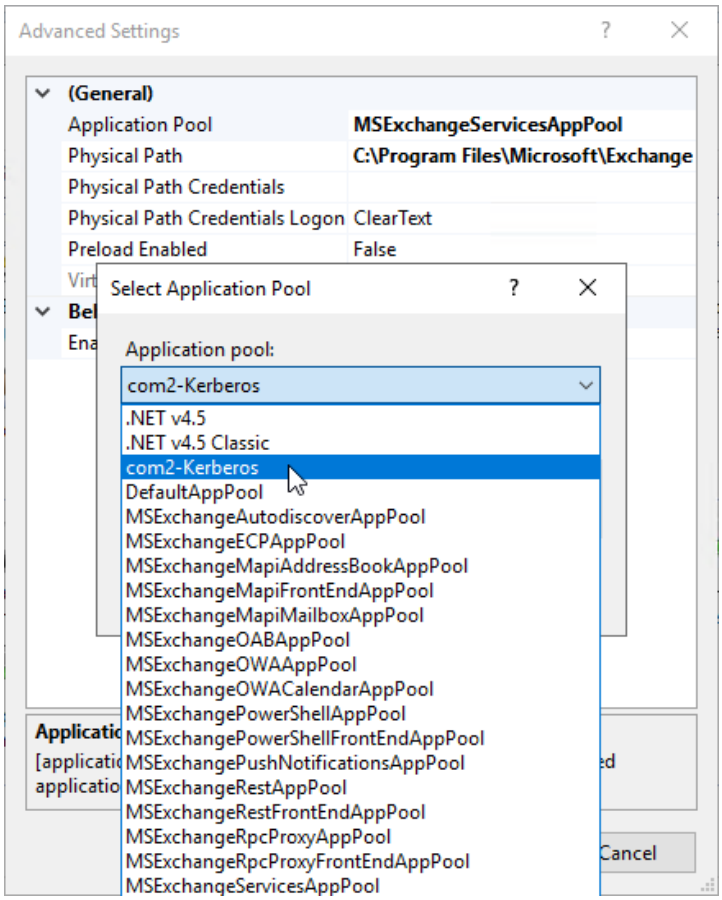



### 3. Zuweisung der des neuen Application Pools an die EWS-Applikation

Hierfür werden die erweiterten Einstellungen der EWS-Applikation benötigt.



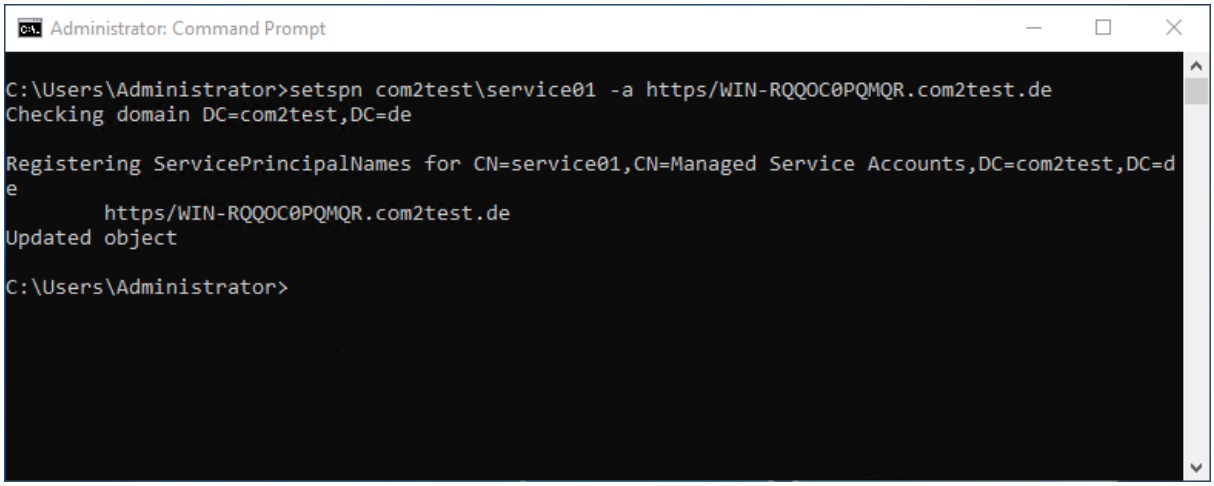
Wählen Sie unterhalb der Sektion General als Application Pool den neuen Pool aus.




### 4. Erstellung eines SPNs für den erstellten Service

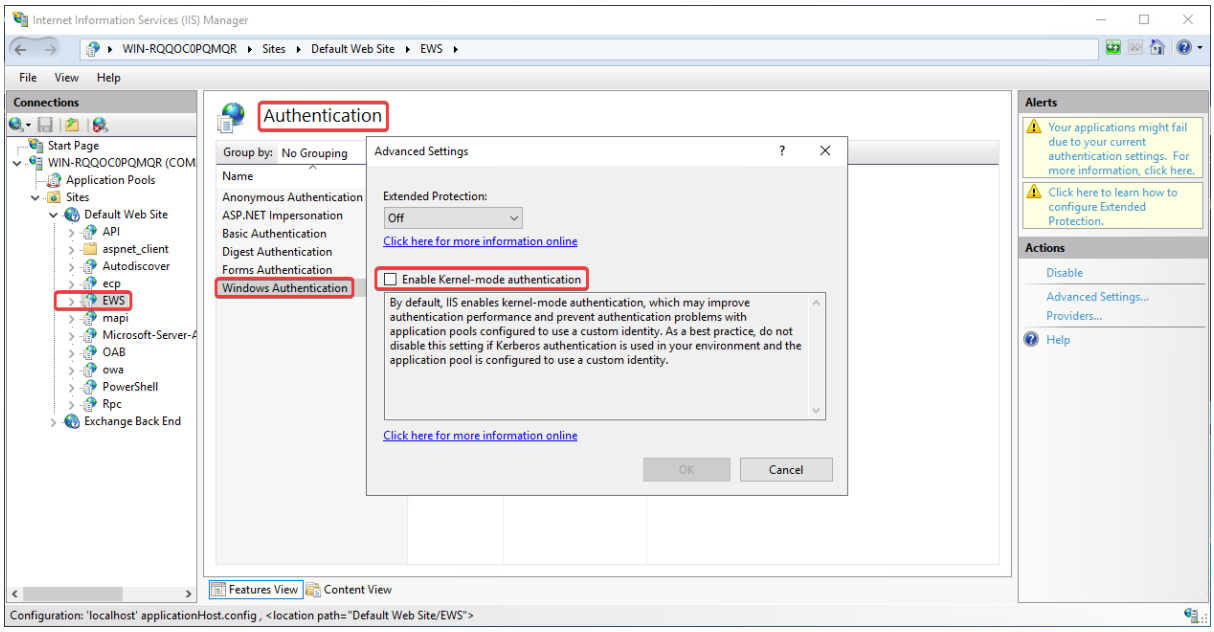
Öffnen Sie wieder eine Kommandozeile mit Adminrechten und führen setspn mit folgender Syntax auf:

```
setspn <Domäne>\<Kontoname> -a https/<FQDN des Loadbalancers>
```

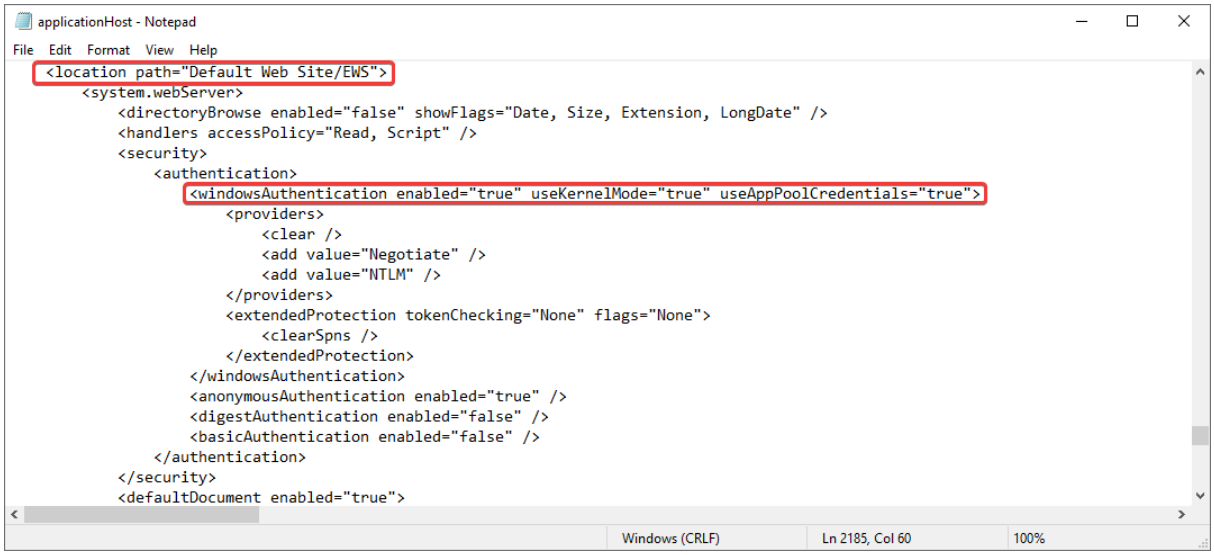


## 5. Notwendige Einstellungen bei Kernelmodus-Authentifizierung

Wenn Sie für EWS die Kernelmodus-Authentifizierung nicht verwenden, können Sie diesen Schritt überspringen. Um dies zu prüfen wechseln Sie in der EWS-Applikation zu Authentication > Windows Authentication > Advanced Settings und prüfen den Status der Checkbox "Enable Kernel-mode authentication"




Wird für EWS die Kernelmodus-Authentifizierung benutzt, ist es noch notwendig die Datei `C:\Windows\System32\inetsrv\Config\applicationhost.config` um `useAppPoolCredentials="true"` wie folgt zu ergänzen:




## 6. Weitere CAS-Server konfigurieren

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