

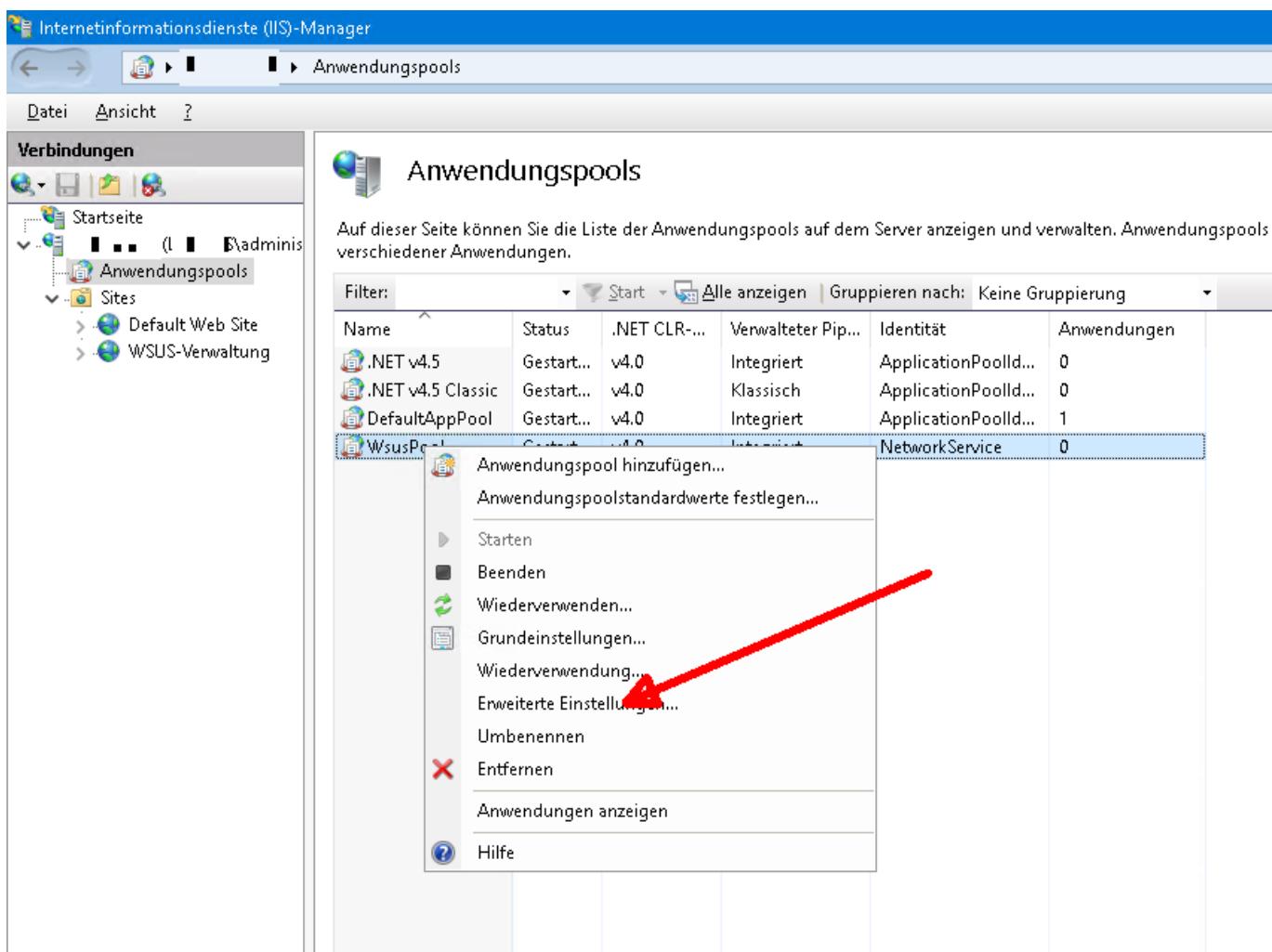
# Windows Server Update Services

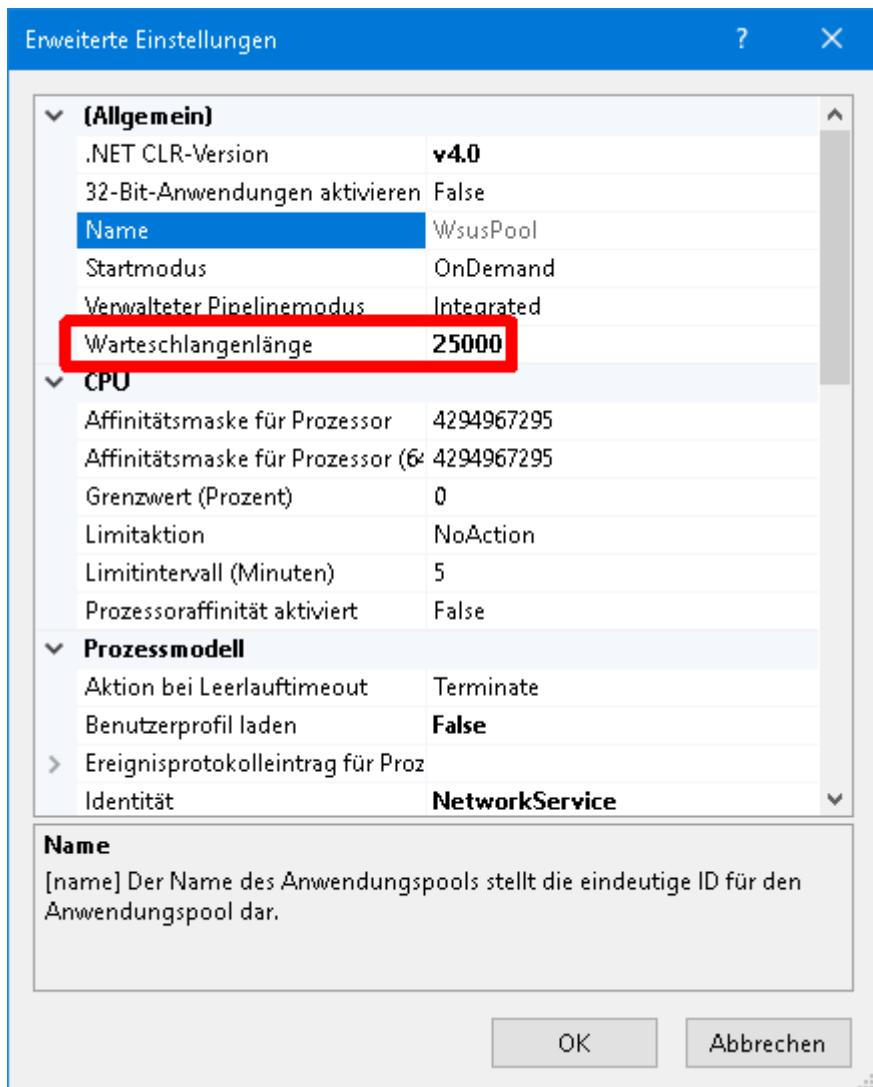
## Ressourcenoptimierung (w3wp.exe 100% CPU bei W10 Clients/Server 2016 Clients)

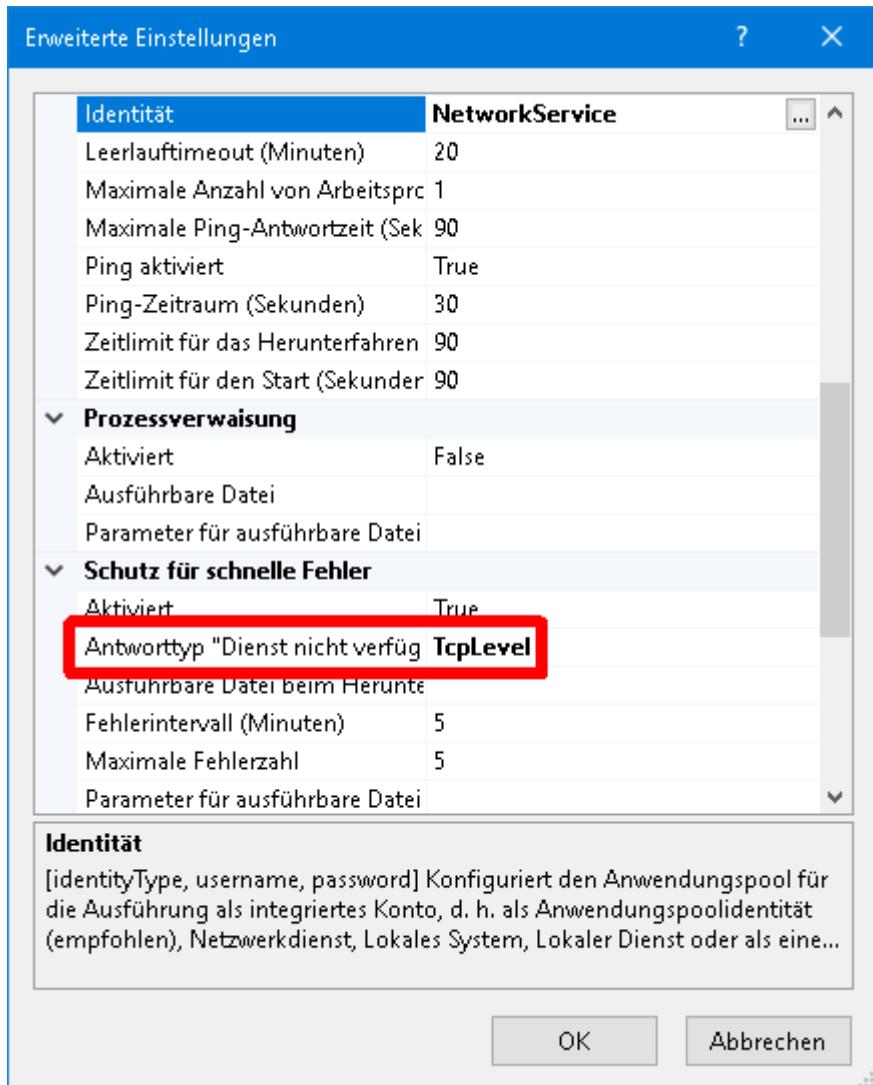
### Generelle Hardwareanforderungen bei Windows 10 Clients / Server 2016

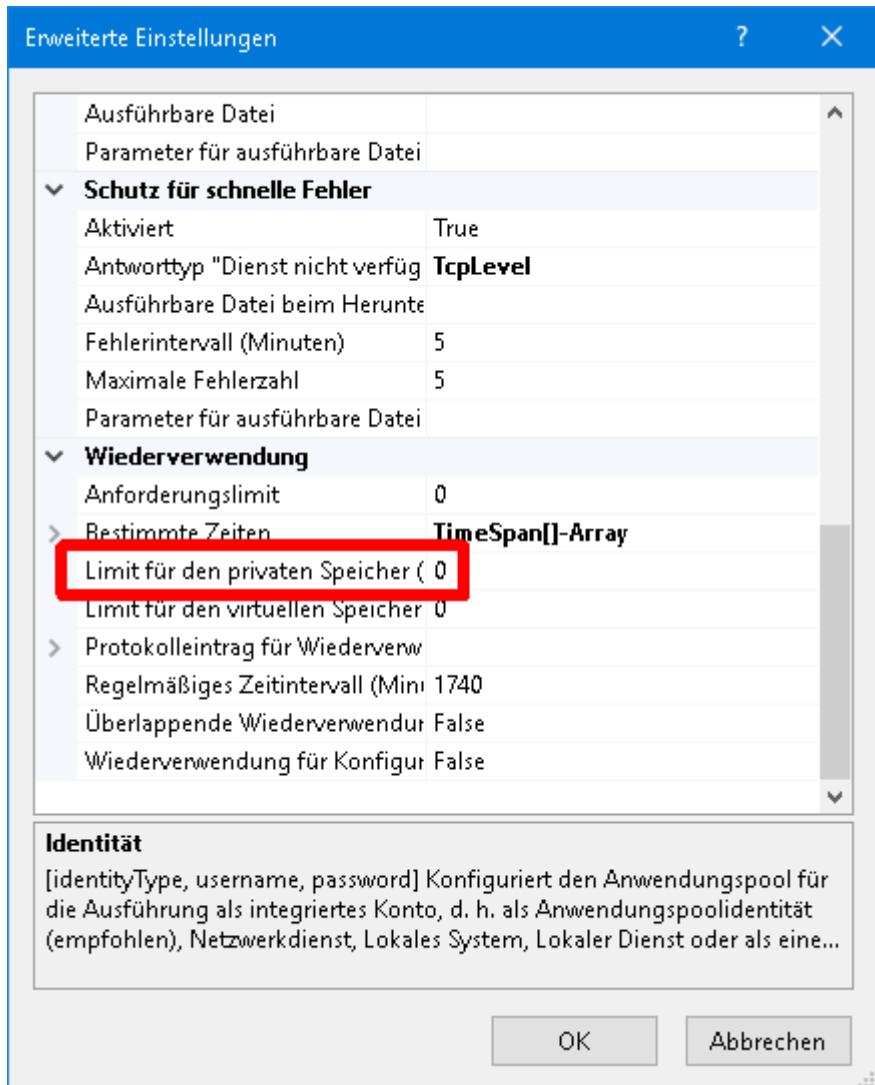
- Mindestens 8 GB RAM
- Mindestens 2 CPU-Kerne

### Anpassungen des IIS Anwendungspools









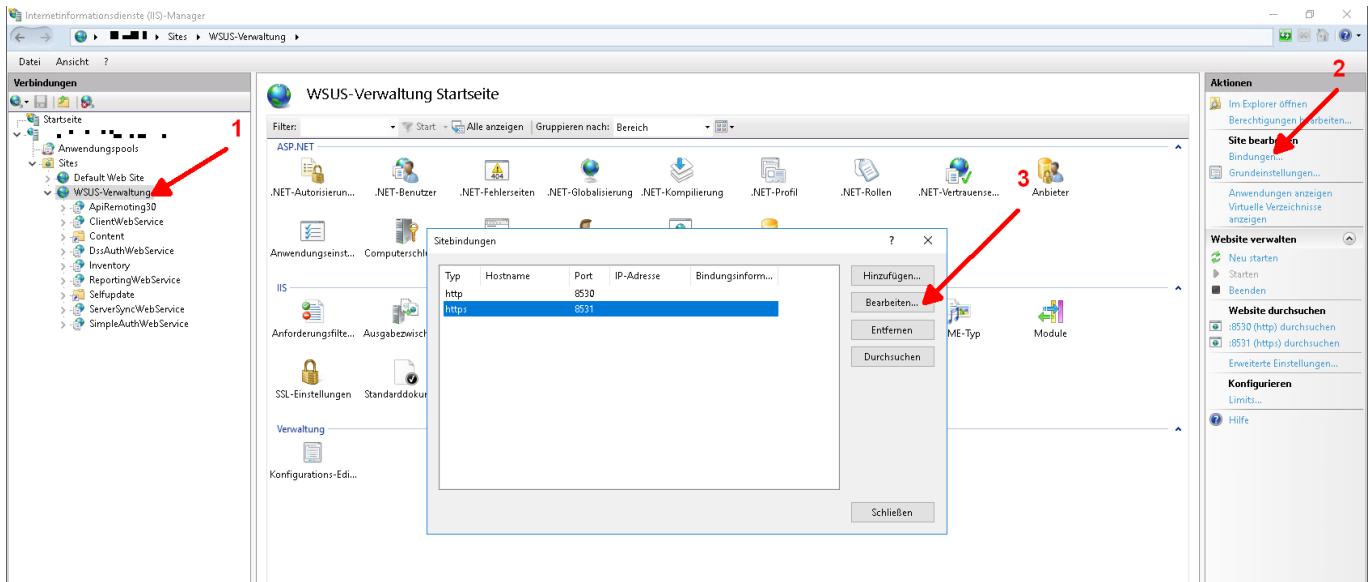
## Server 2012: Feature Updates nicht möglich

Folgender MIME-Typ muss hinzugefügt werden:

.esd application/vnd.ms-cab-compressed

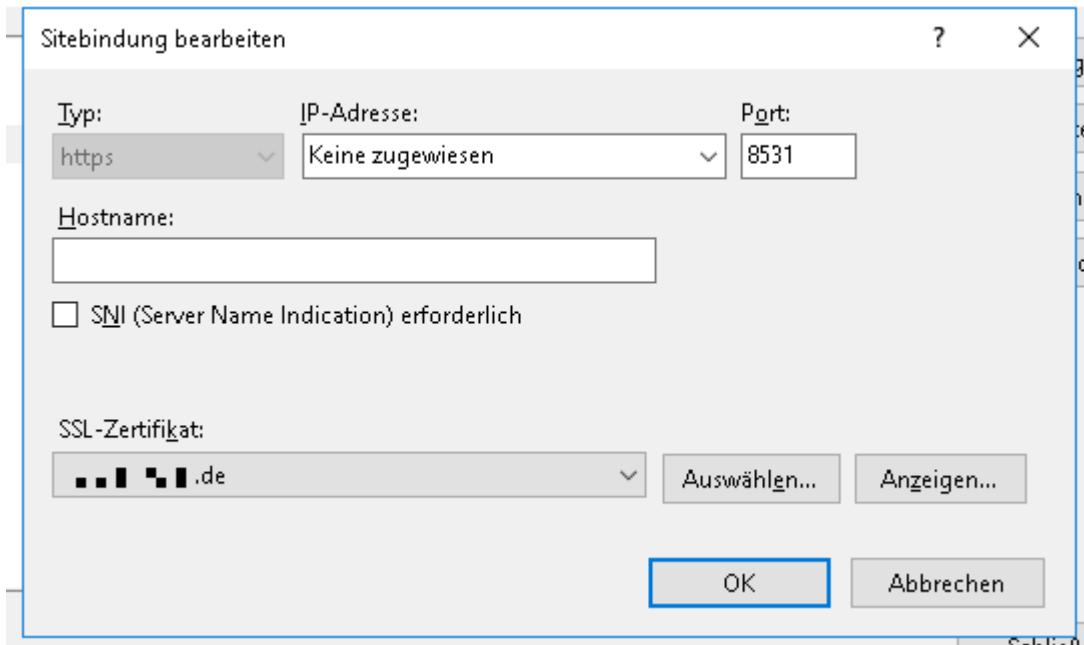
## WSUS über TLS

An dieser Stelle gehe ich davon aus, dass ein Zertifikat einer AD-CA für den Server bereits vorliegt.



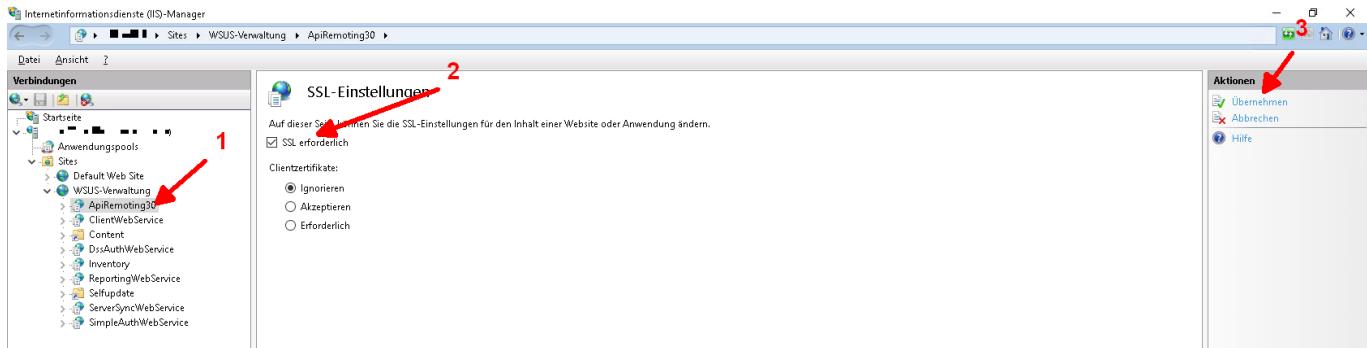
Innerhalb der IIS-Konsole:

1. Die Site „WSUS-Verwaltung“ auswählen.
2. Im rechten Frame „Bindungen“ wählen.
3. Die HTTPS-Bindung auf den Port 8531 bearbeiten, darin das korrekte Zertifikat zuweisen.



Für folgende virtuelle Verzeichnisse sollte nun die Kommunikation über SSL erzwungen werden:

- APIremoting30
- ClientWebService
- DSSAuthWebService
- ServerSyncWebService
- SimpleAuthWebService



Dann bringen wir dem WSUS über seine API bei, dass er von nun an via SSL/TLS kommunizieren muss. Dazu geben wir in einer Admin-CMD folgende Befehle ein. Es muss der FQDN des Servers angegeben werden, auf den auch das Zertifikat ausgestellt worden ist.

```
cd %ProgramFiles%\Update Services\Tools\  
wsusutil.exe configssl FQDN-des-Servers
```

## Verbindung zur WID über das Management Studio

Die Datenbank ist über folgenden Socket erreichbar:

```
\.\.\pipe\microsoft##wid\tsql\query
```

From:  
<https://wiki.sebastianhetzel.net/> - **Sebastians IT-Wiki**



Permanent link:  
[https://wiki.sebastianhetzel.net/win\\_server:wsus?rev=1556013347](https://wiki.sebastianhetzel.net/win_server:wsus?rev=1556013347)

Last update: **2019/04/23 11:55**