

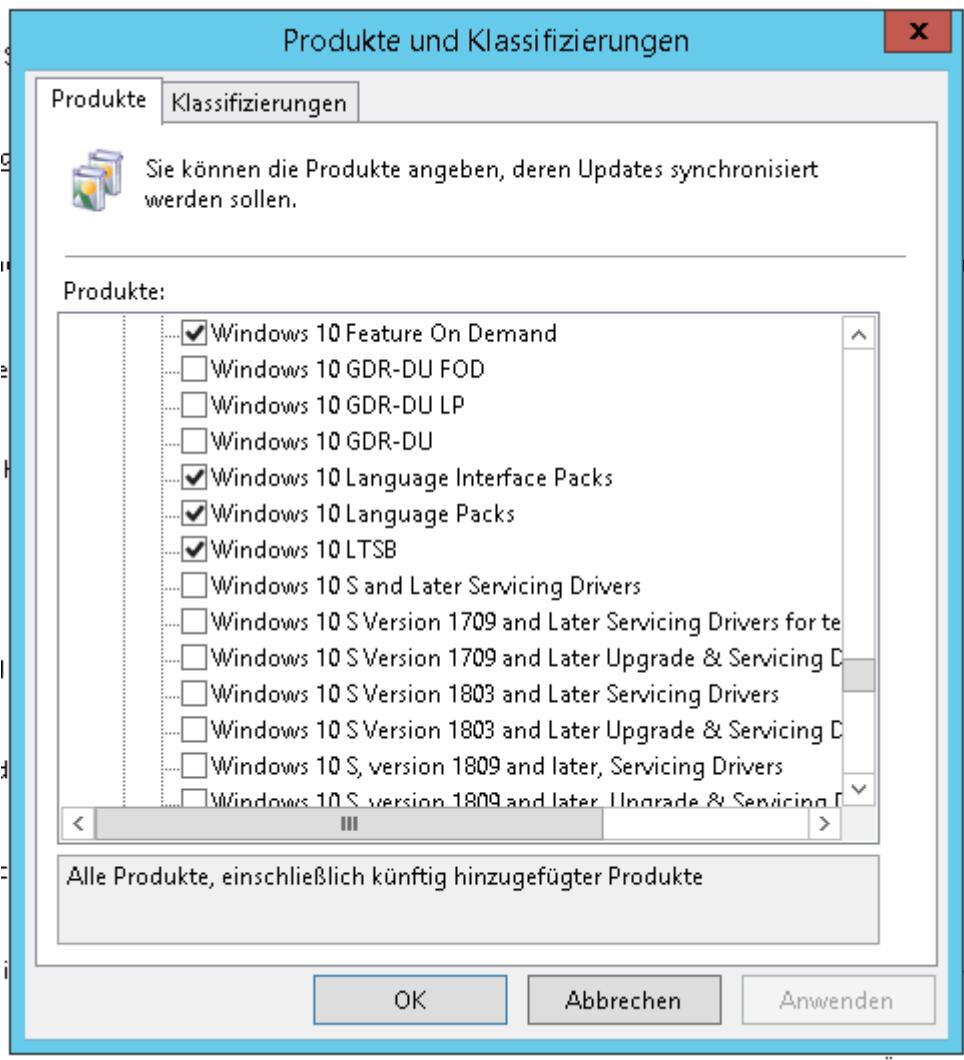
Windows Server Update Services

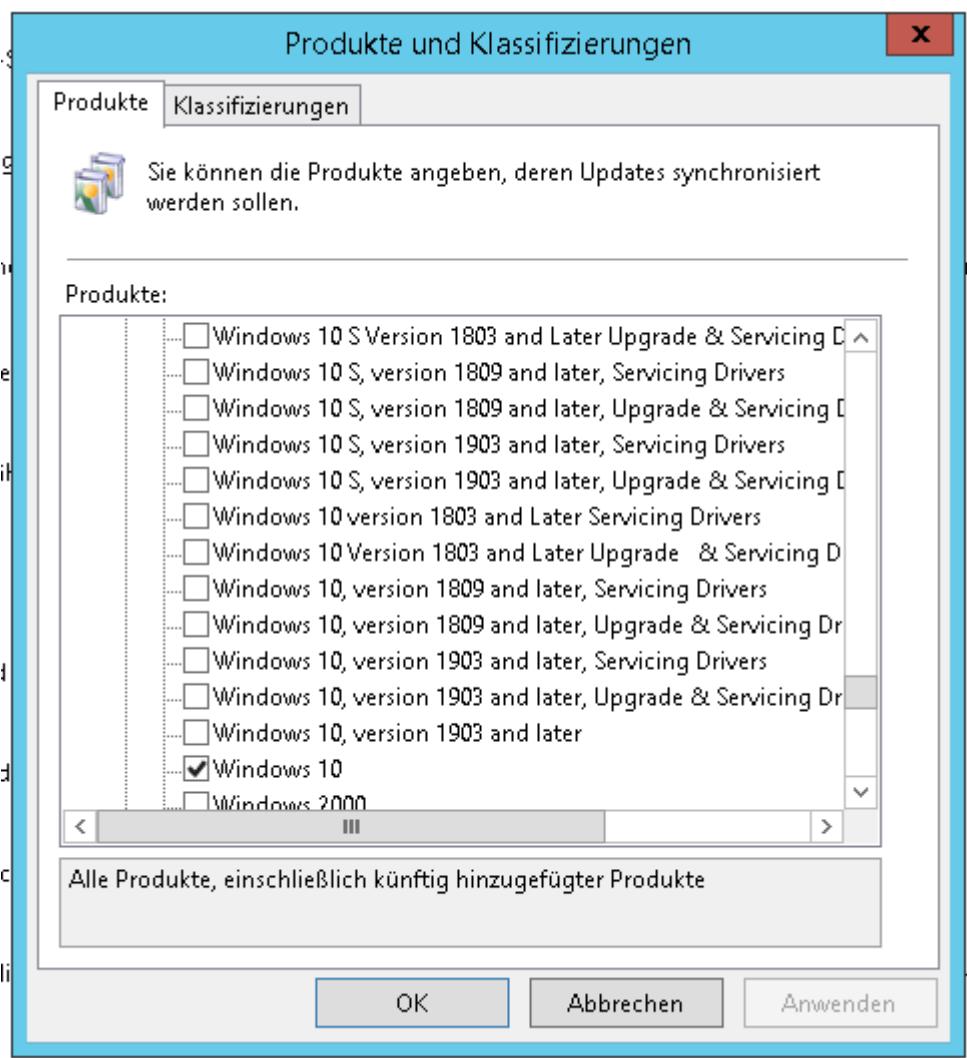
Installation und Ersteinrichtung (Vorgehen)

1. Produktauswahl treffen (siehe unten)
2. Automatische Genehmigungen konfigurieren oder entfernen
3. E-Mailbenachrichtigung aktivieren (falls gewünscht)
4. Automatische Synchronisierung konfigurieren und durchführen/prüfen
5. TLS aktivieren
6. Gruppenrichtlinie erstellen und verlinken

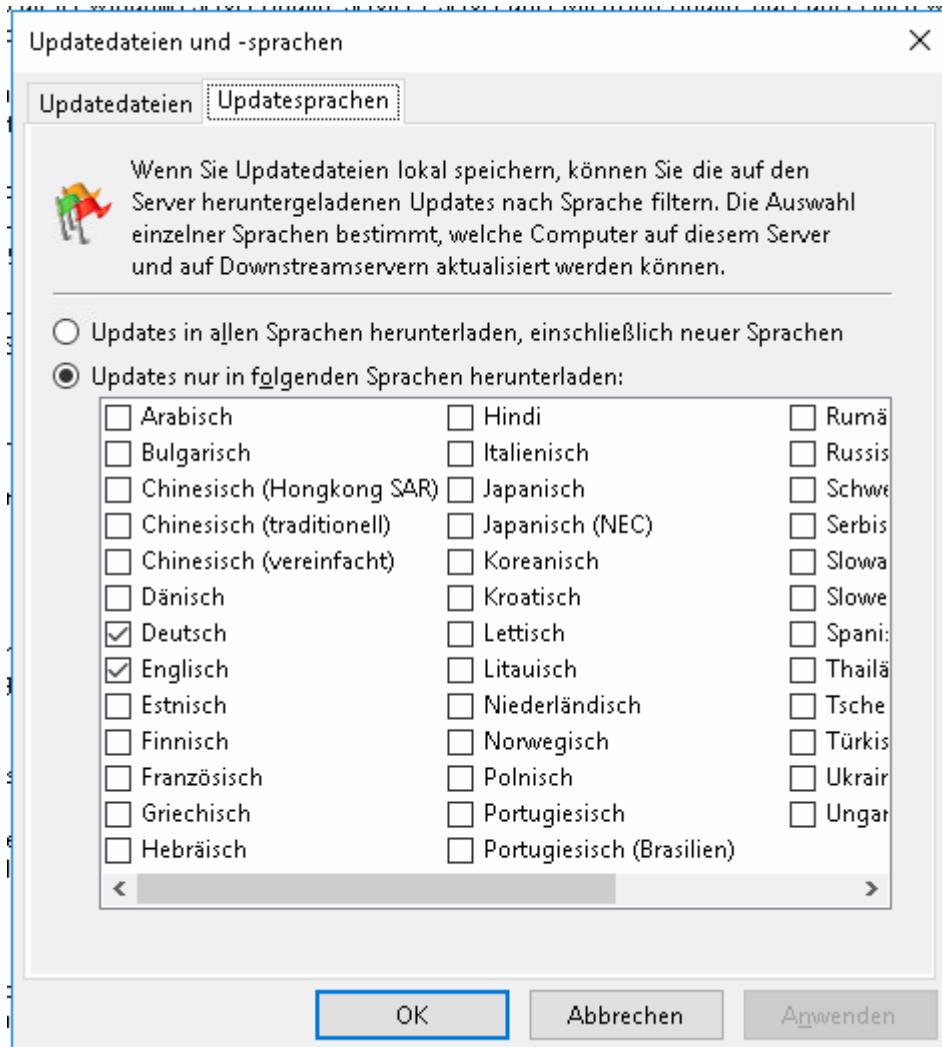
Produktauswahl bei Windows 10 Clients

Produkte





Sprachen



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

Internetinformationsdienste (IIS)-Manager

Anwendungspools

Verbindungen

Startseite | Anwendungspools | Administratoren | Anwendungen | Dokumente | Benutzer | Sicherheit | IIS-Manager

Anwendungspools

Auf dieser Seite können Sie die Liste der Anwendungspools auf dem Server anzeigen und verwalten. Anwendungspools verschiedener Anwendungen.

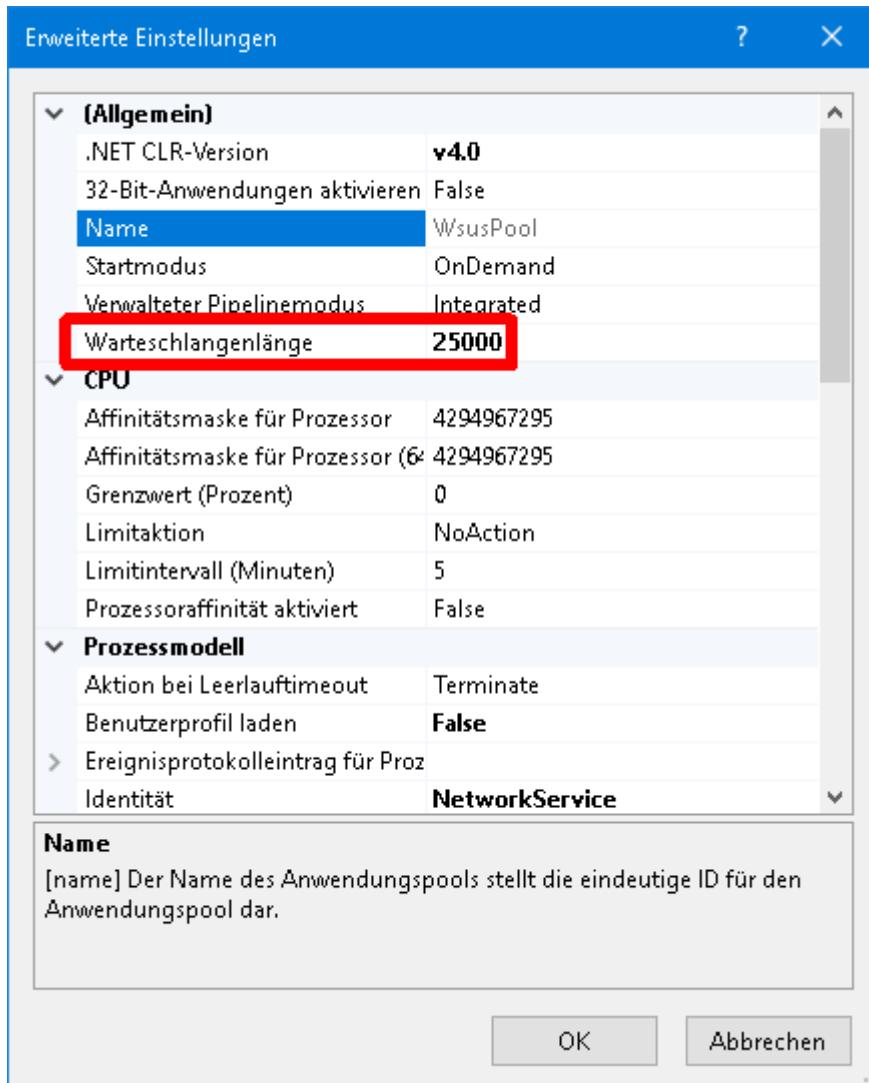
Filter: Alle anzeigen | Gruppieren nach: Keine Gruppierung

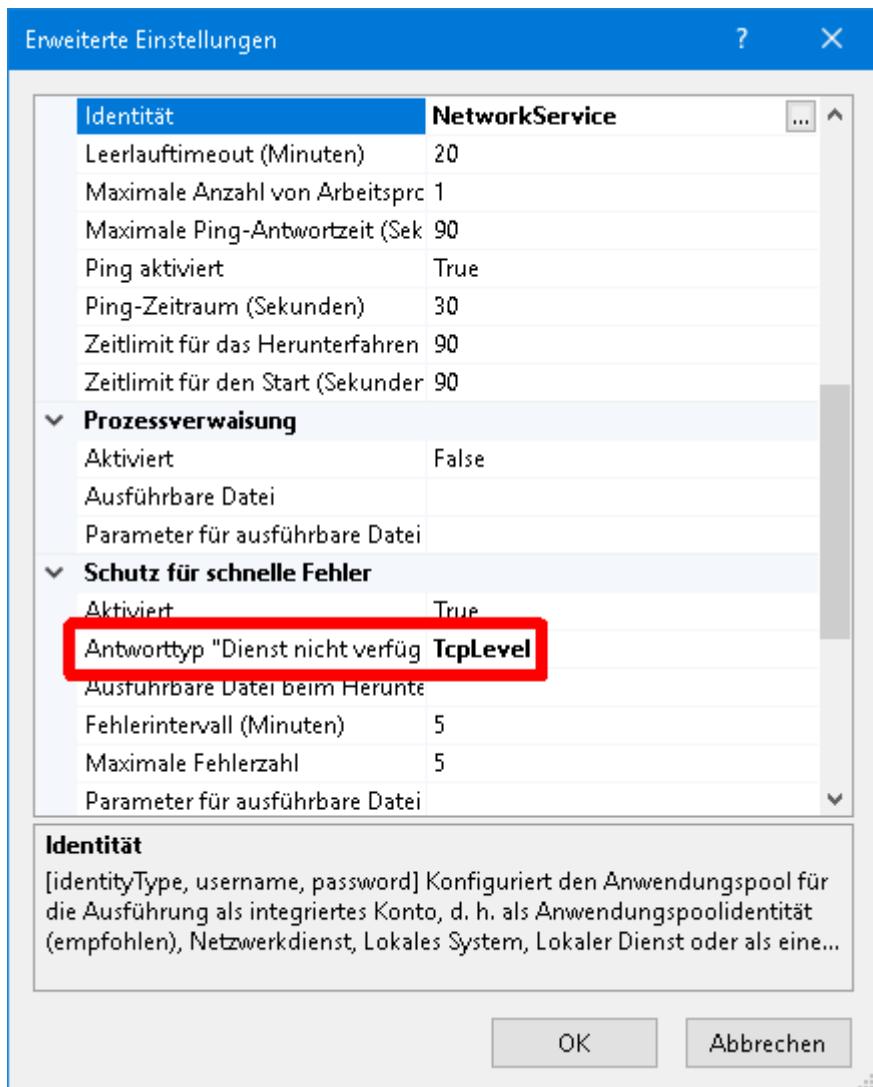
Name	Status	.NET CLR...	Verwalteter Pip...	Identität	Anwendungen
.NET v4.5	Gestart...	v4.0	Integriert	ApplicationPoolId...	0
.NET v4.5 Classic	Gestart...	v4.0	Klassisch	ApplicationPoolId...	0
DefaultAppPool	Gestart...	v4.0	Integriert	ApplicationPoolId...	1
WsusP	Gestart...	v4.0	Integriert	NetworkService	0

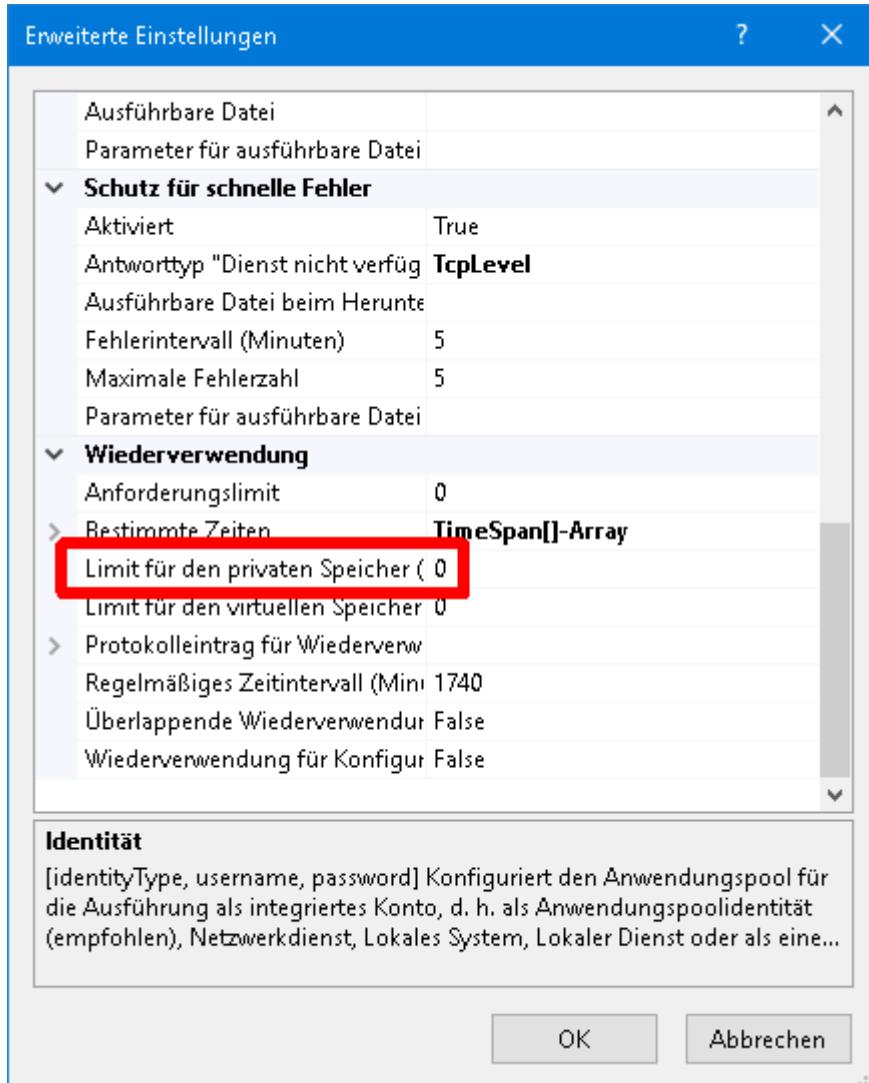
WsusP Kontext

Anwendungspool hinzufügen...
Anwendungspoolstandardwerte festlegen...
Starten
Beenden
Wiederverwenden...
Grundeinstellungen...
Wiederverwendung...
Erweiterte Einstellungen...
Umbenennen
Entfernen
Anwendungen anzeigen
Hilfe









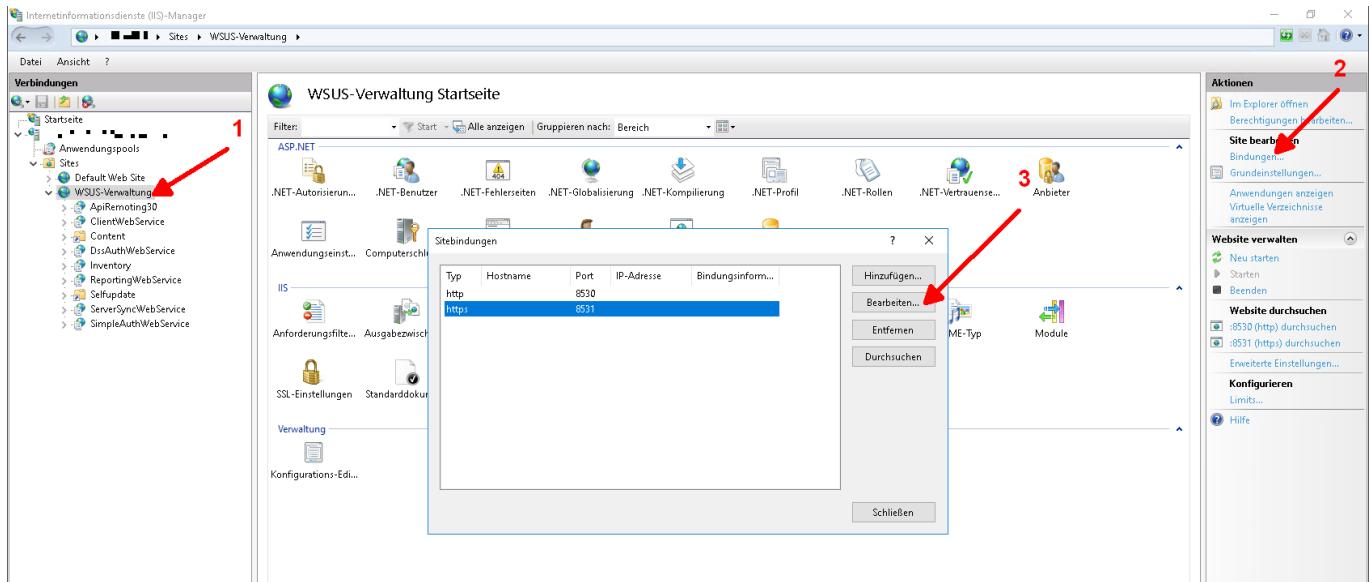
Server 2012: Feature Updates nicht möglich

Folgender MIME-Typ muss hinzugefügt werden:

.esd **application/vnd.ms-cab-compressed**

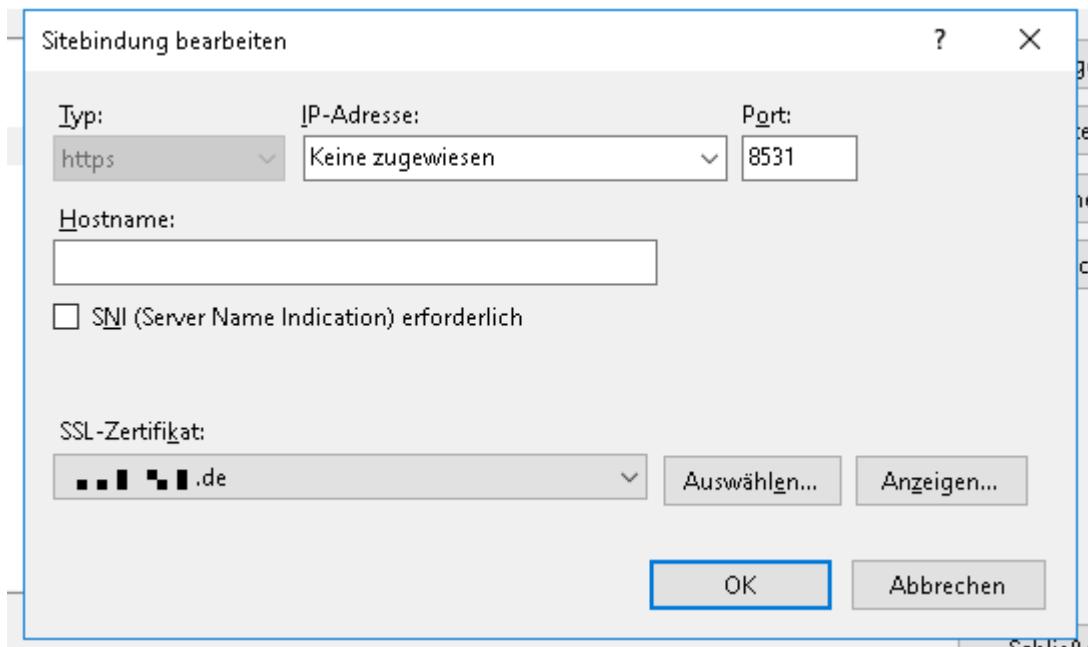
WSUS über TLS

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



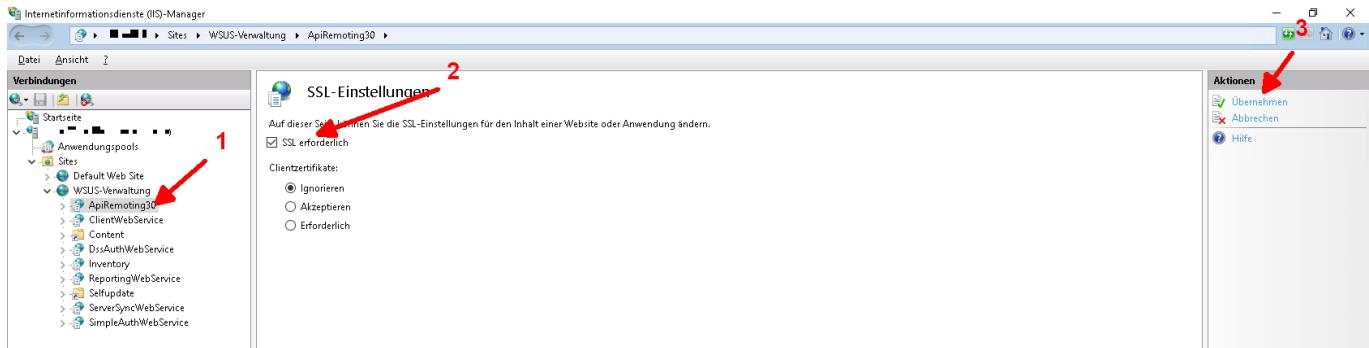
Innerhalb der IIS-Konsole:

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://wikinet.webby.hetzel-netz.de/> - **Sebastians IT-Wiki**



Permanent link:
https://wikinet.webby.hetzel-netz.de/win_server:wsus?rev=1559038683

Last update: **2019/05/28 12:18**