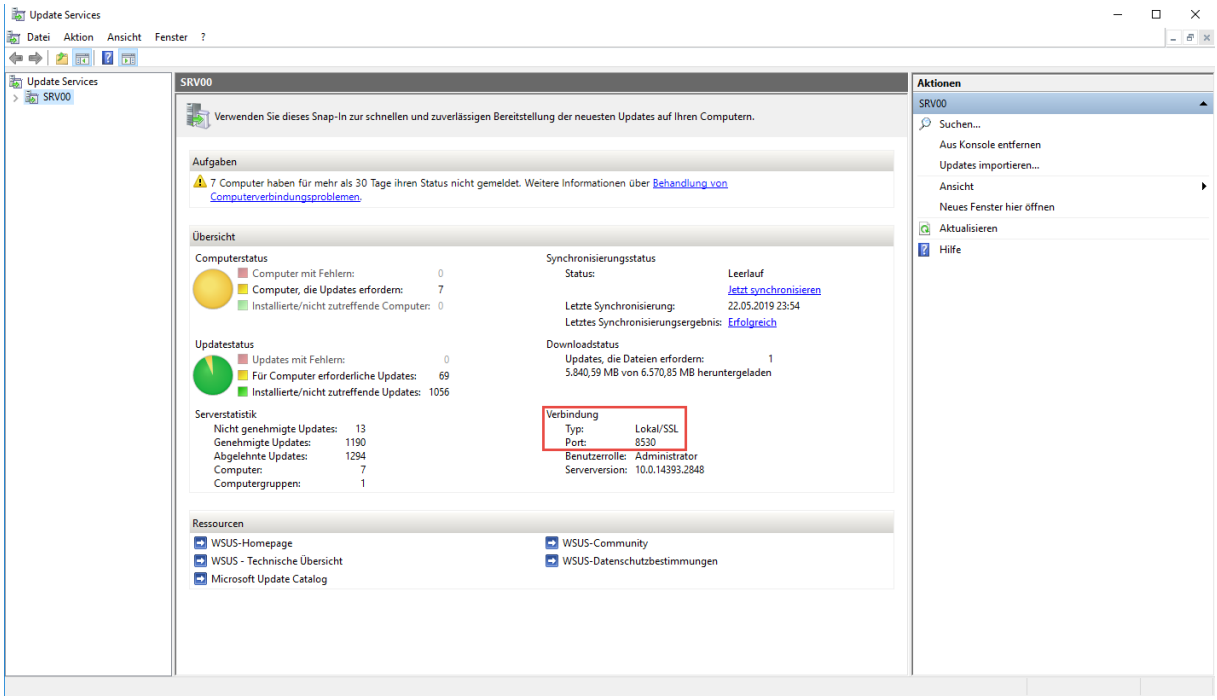
Erweiterte Sicherheit beim Anmeldeprozess

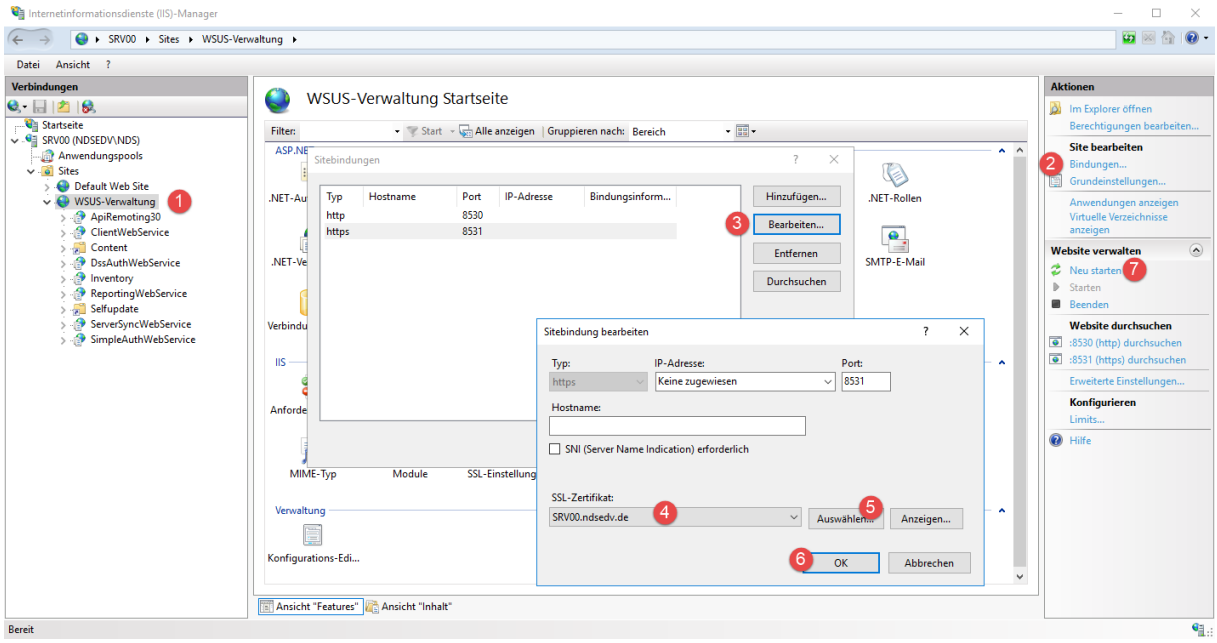
In diesem Dokument gehe ich auf die Umstellung der WSUS-Kommunikation ein. Das Ziel ist die HTTP Verbindung auf HTTPS umzustellen. Also von dem Standard Port 8530 auf 8531.

Im Moment ist der Service noch immer unter http zu erreichen.



Über die interne CA besorgen wir uns ein SSL-Zertifikat. Bitte denkt an eventuelle Subject Alternative Namens (SAN).

Starten den IIS und durchlaufen folgende Zahlen, um der WSUS-Verwaltung ein Zertifikat zuzuweisen und daran zu binden.

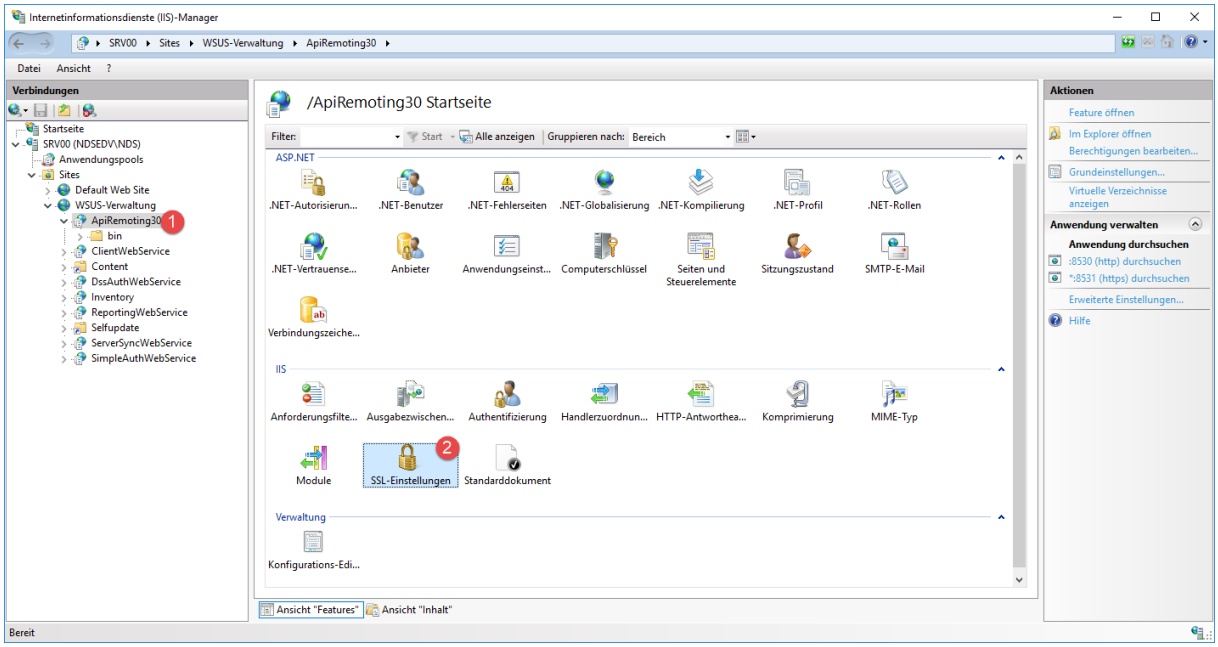


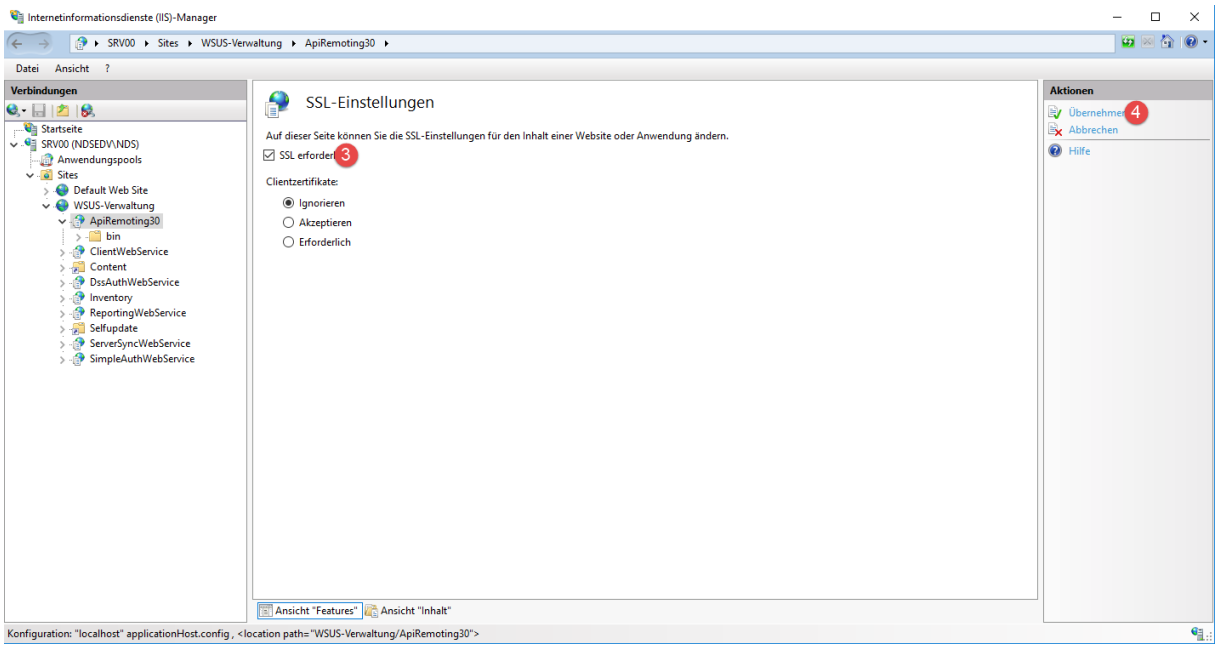
Erweiterte Sicherheit beim Anmeldeprozess

Danach stellen wir die einzelnen Services wie gezeigt auf SSL um. Der Ablauf ist immer derselbe 1-4.

- APIremoting30
- ClientWebService
- DSSAuthWebService
- ServerSyncWebService
- SimpleAuthWebService

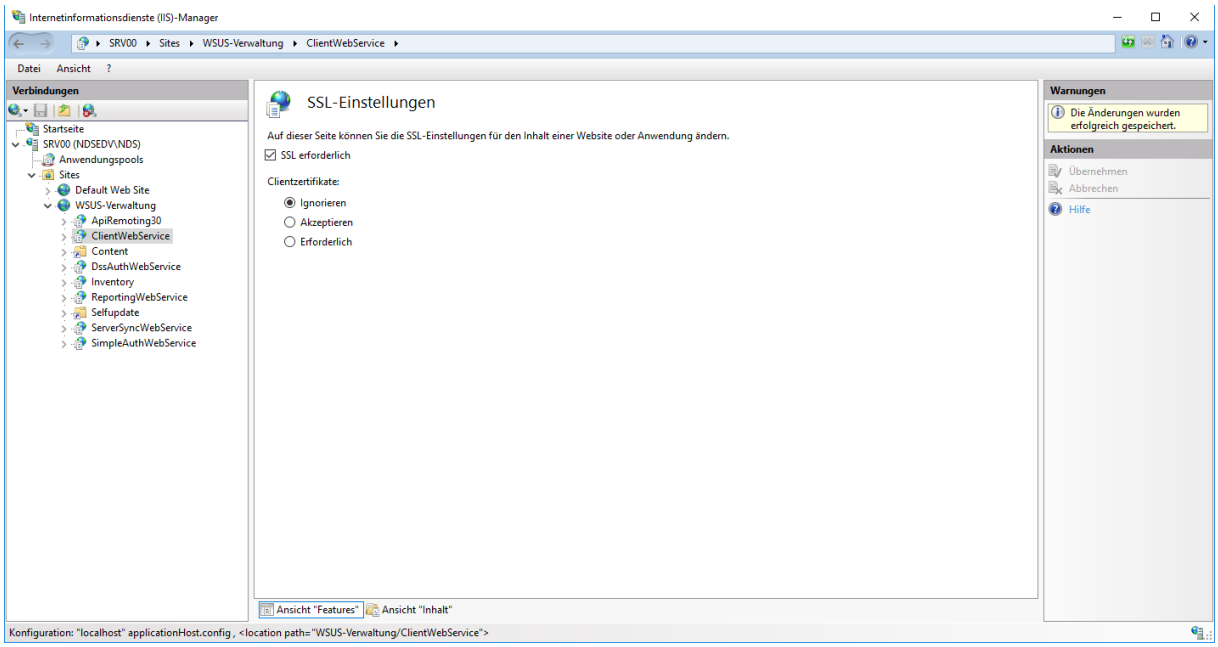
APIremoting30



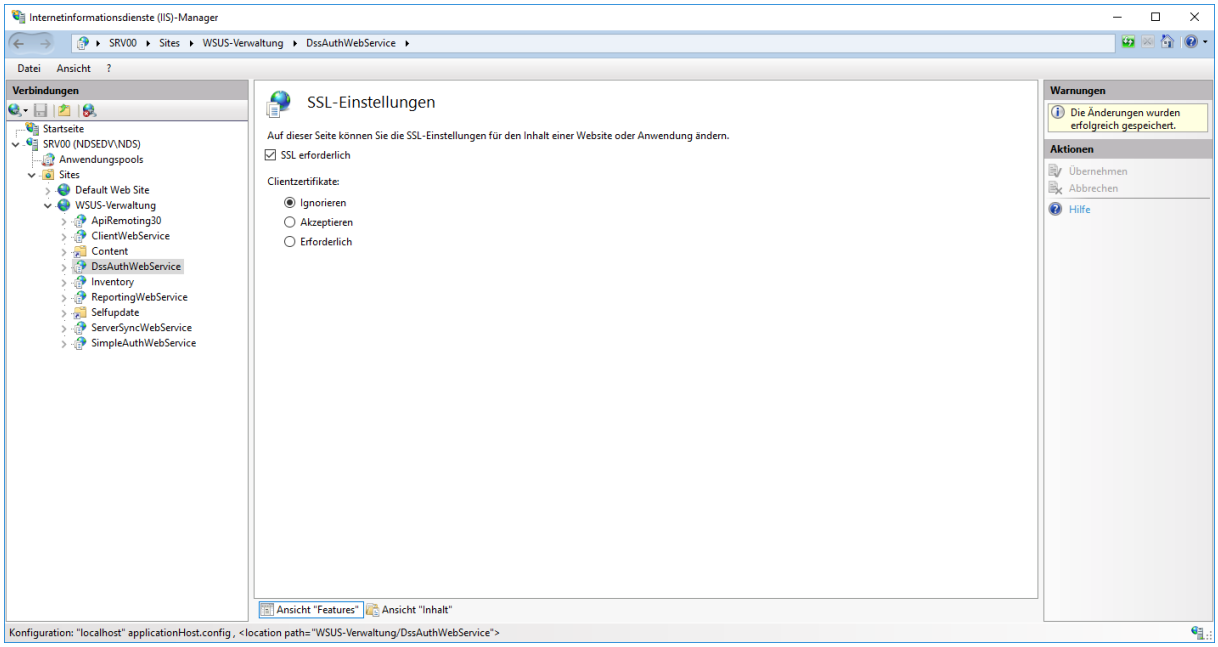


Erweiterte Sicherheit beim Anmeldeprozess

ClientWebService



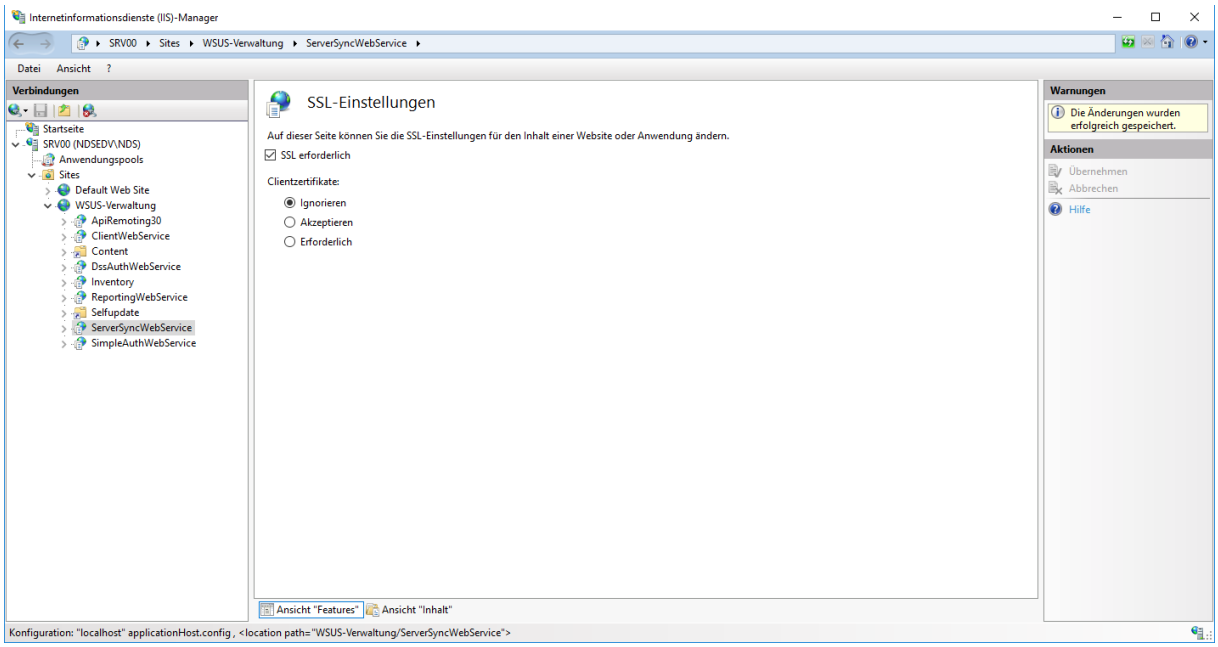
DSSAuthWebService



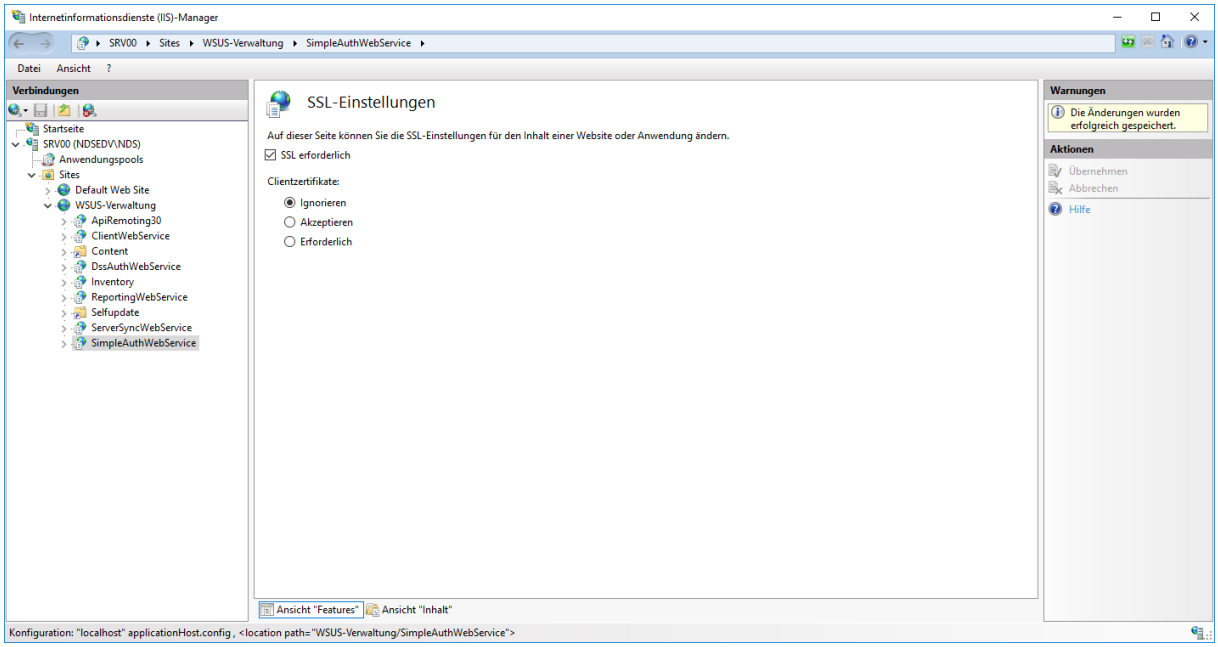
Erstellt von Jörn Walter **01.07.2019**

Erweiterte Sicherheit beim Anmeldeprozess

ServerSyncWebService



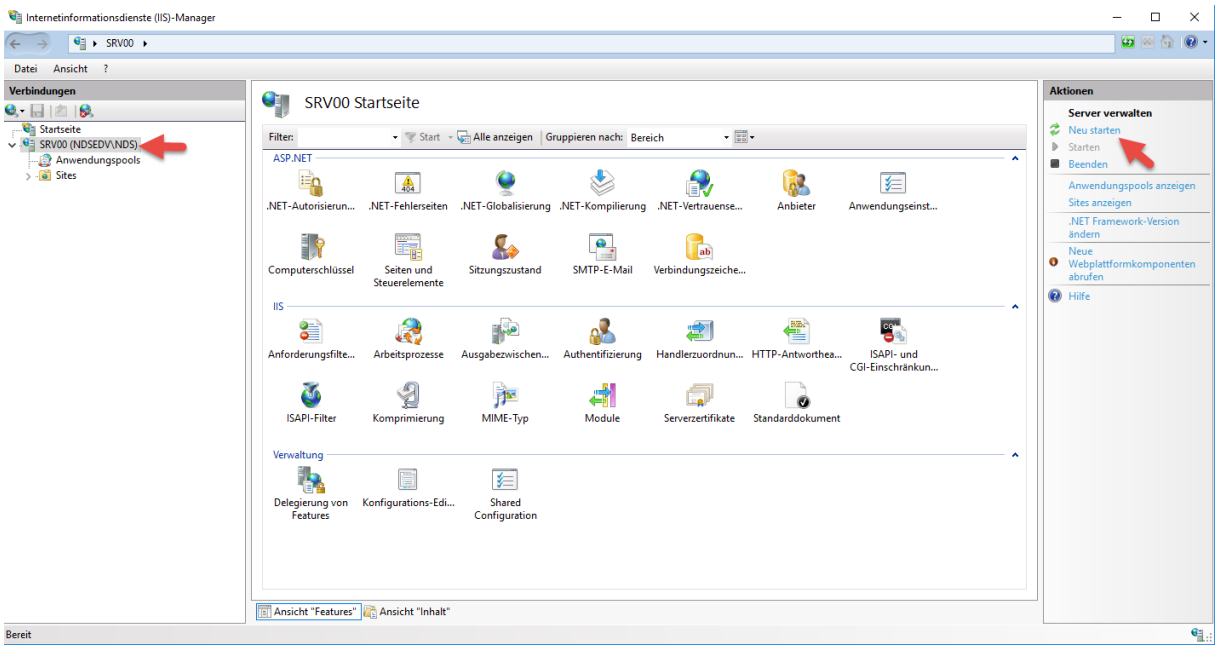
SimpleAuthWebService



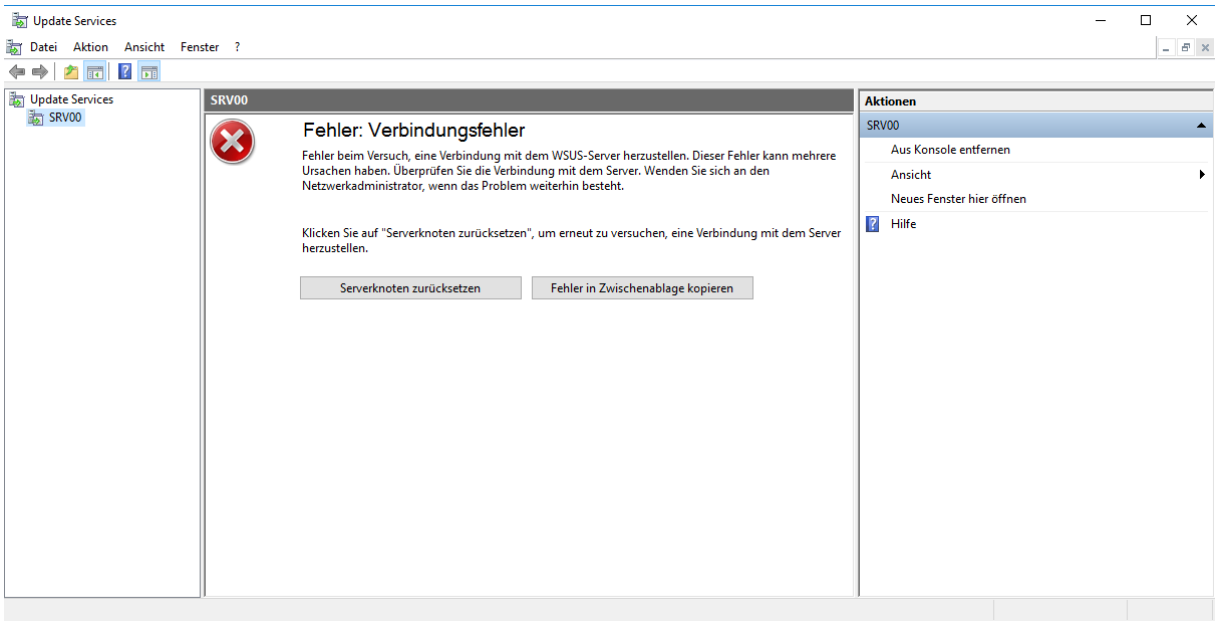
Erstellt von Jörn Walter **01.07.2019**

Erweiterte Sicherheit beim Anmeldeprozess

Jetzt starten wir den IIS einmal durch.

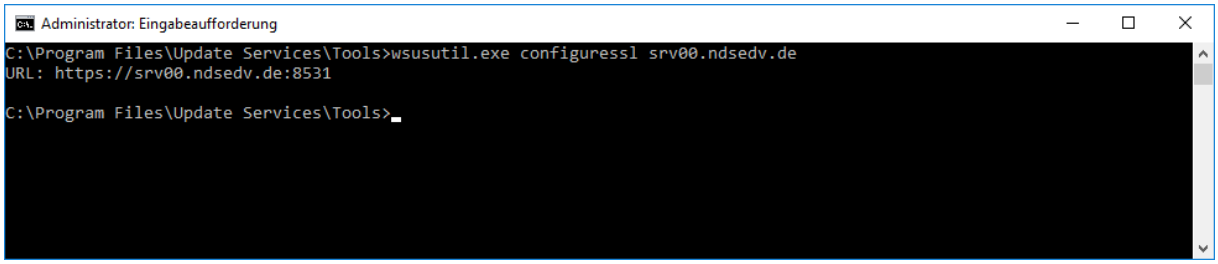


Würde man jetzt versuchen die WSUS-Konsole zu öffnen, würde ein Verbindungsfehler angezeigt werden. Die Konsole muss auch noch auf SSL umgestellt werden



Dazu öffne wir die CMD mit administrativen Rechten und setzen folgenden Befehl ab:

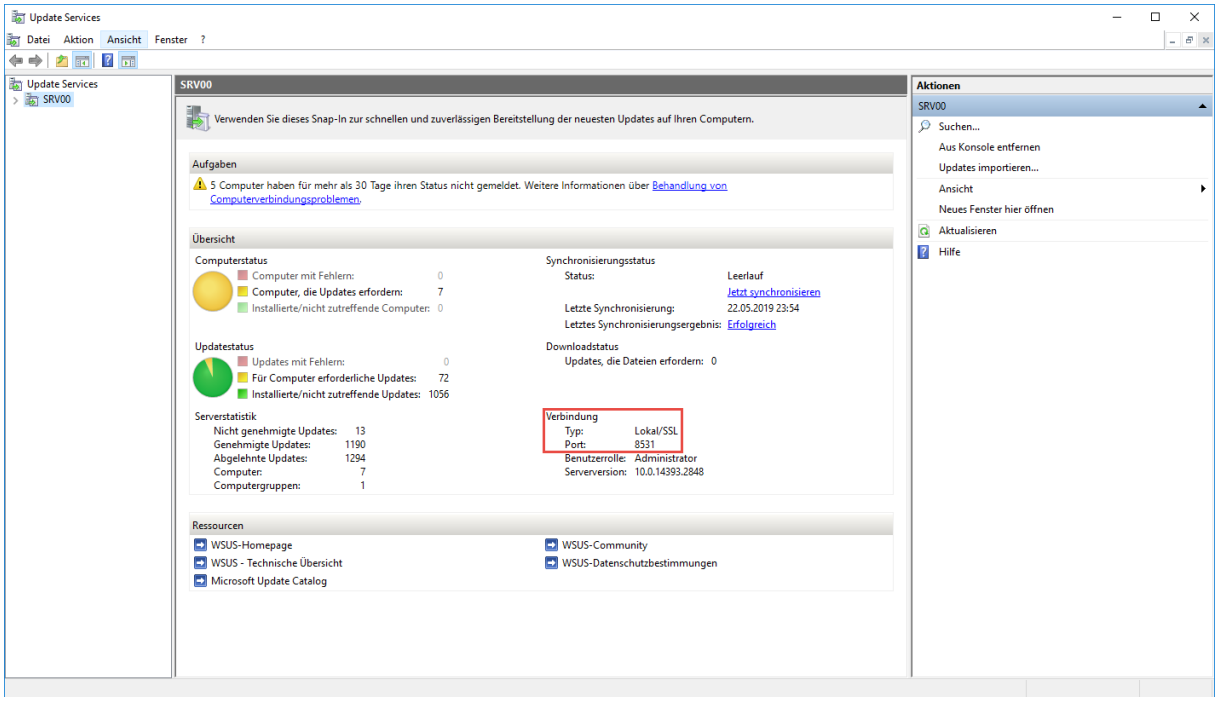
wsusutil.exe configuressl srv00.ndsedv.de



Erweiterte Sicherheit beim Anmeldeprozess

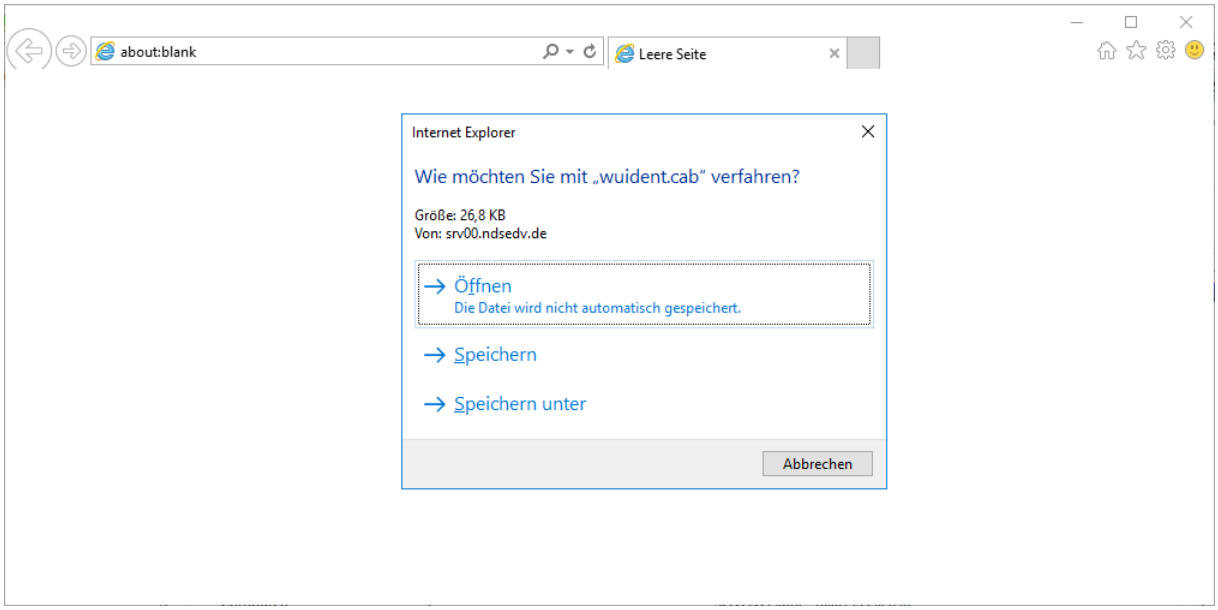
Die Konsole lässt sich nun wieder öffnen und die Kommunikation ist auf SSL umgestellt.

Sollte sich die Konsole nicht öffnen lassen, einfach den IIS noch einmal durchstarten und die Bindung des Zertifikats kontrollieren.



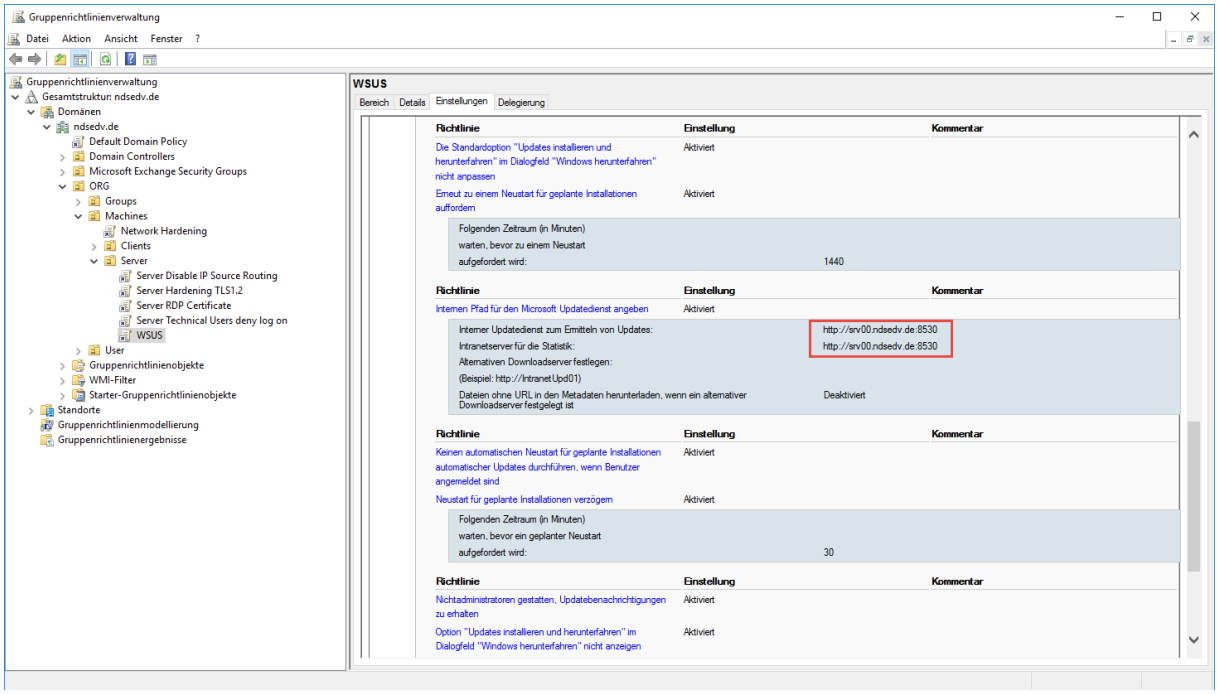
Jetzt prüfen wir ob die Client-Verbindung steht.

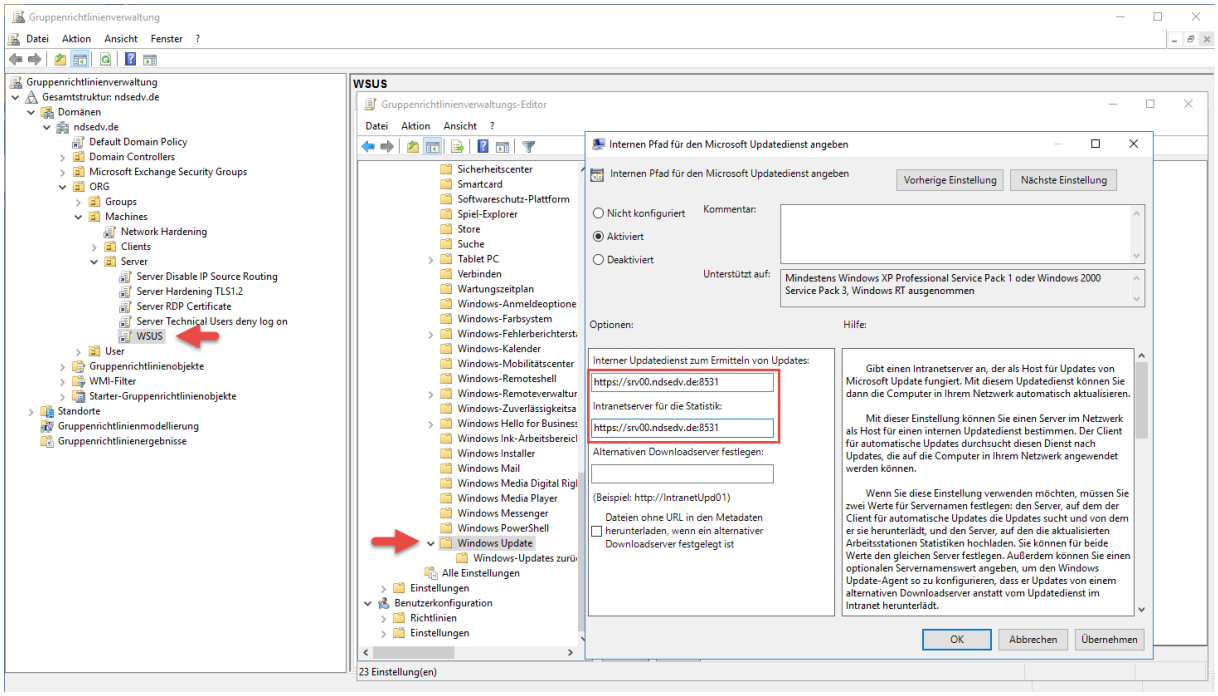
https://srv00.ndsedv.de:8531/selfupdate/wuident.cab



Erweiterte Sicherheit beim Anmeldeprozess

Um das Ganze schlussendlich fertig zu stellen, passen wir noch die Gruppenrichtlinie an, um die ganzen Clients und Server über die Umstellung zu informieren.





Erweiterte Sicherheit beim Anmeldeprozess

Nach einem gpudpate sollte die neue Verbindung in der Registry an dieser Stelle gefunden werden.