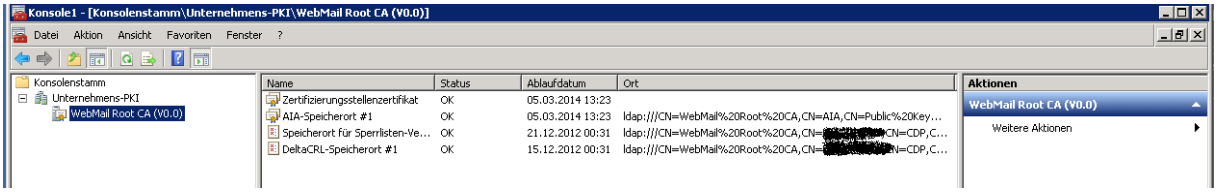
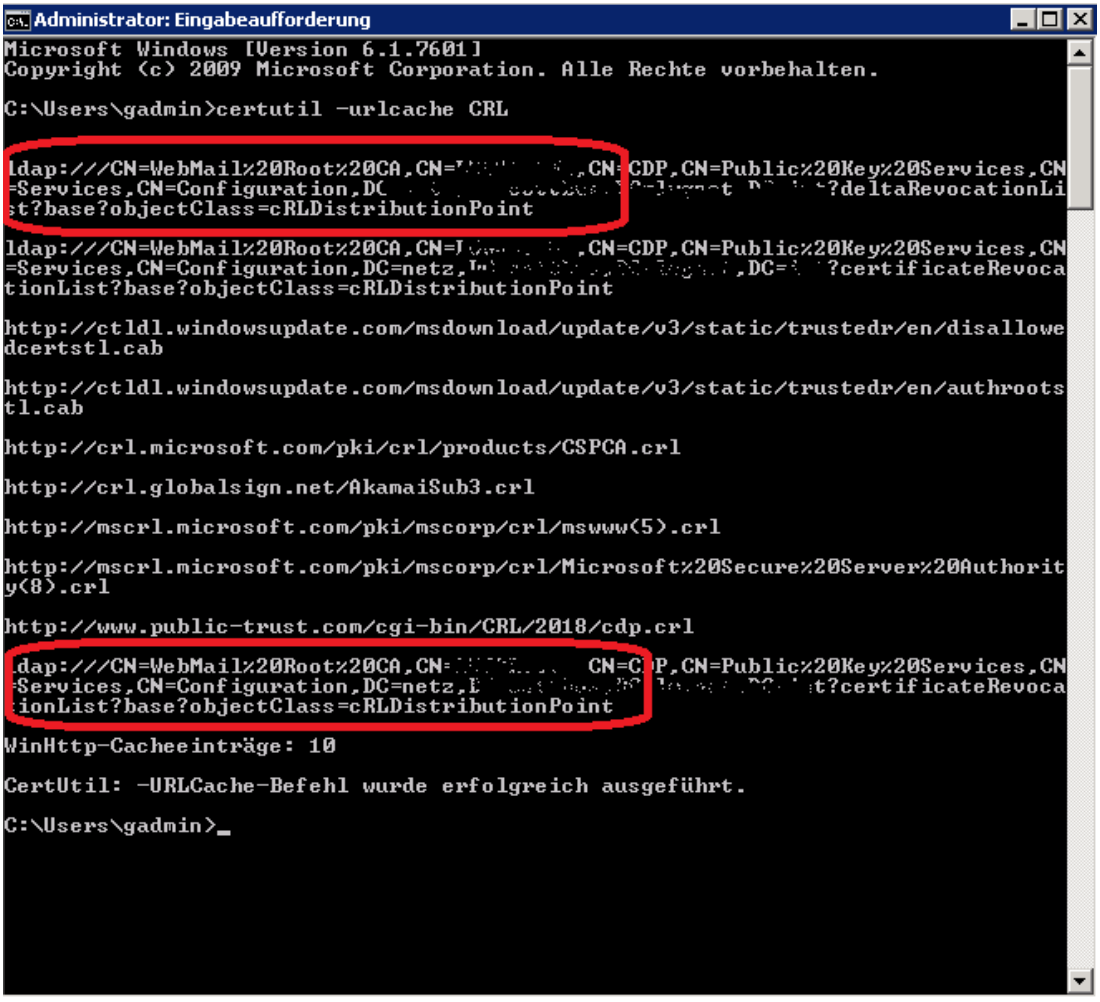
Windows Server 2008 R2 CA Migration – Exchange 2010 CRL

Nach der Migration der CA von einem Windows Server 2008 R2 auf einen anderen Server konnte auf dem Exchange Server 2010 kein neues Exchange Zertifikat angefordert werden. Die Meldung war dass der Zertifikatsperrstatus nicht geprueft werden konnte.

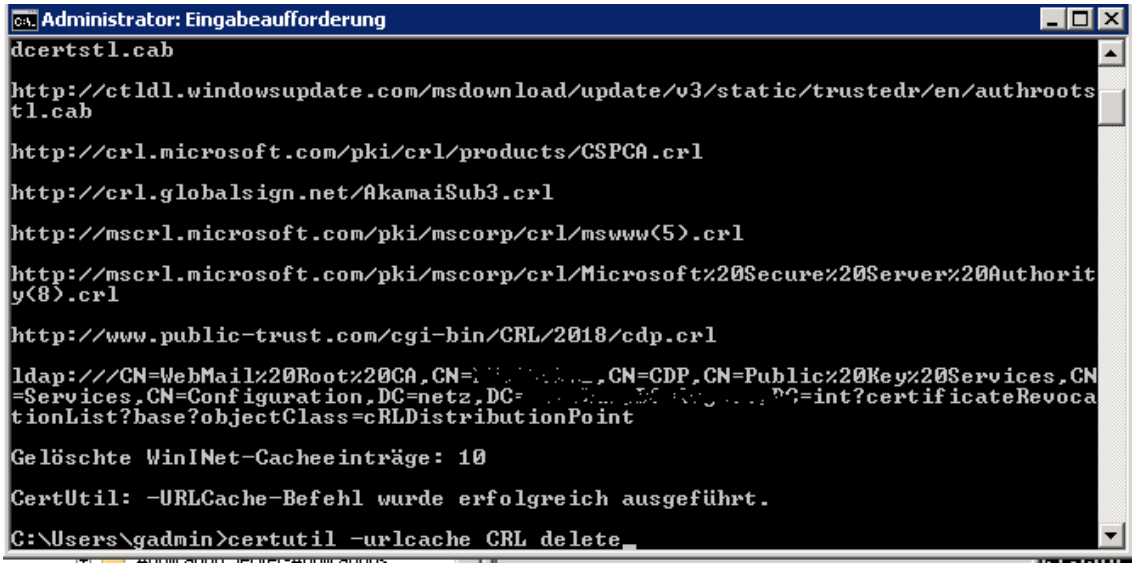
Auf dem neuen CA-Server meldete das PKI Health Utility keine Fehlermeldung



Auf dem Exchange Server konnte man sehen dass der Server noch eine alte CRL zu dem alten PKI-Server aufgebaut hat, obwohl die Base- und Delta CRL neu veroeffentlicht wurde und auf dem Exchange Server veroeffentlicht wurde. Wie man im Screenshot sehen kann, werden zwei CRL (des alten PKI Server und des neuen PKI Server angezeigt)



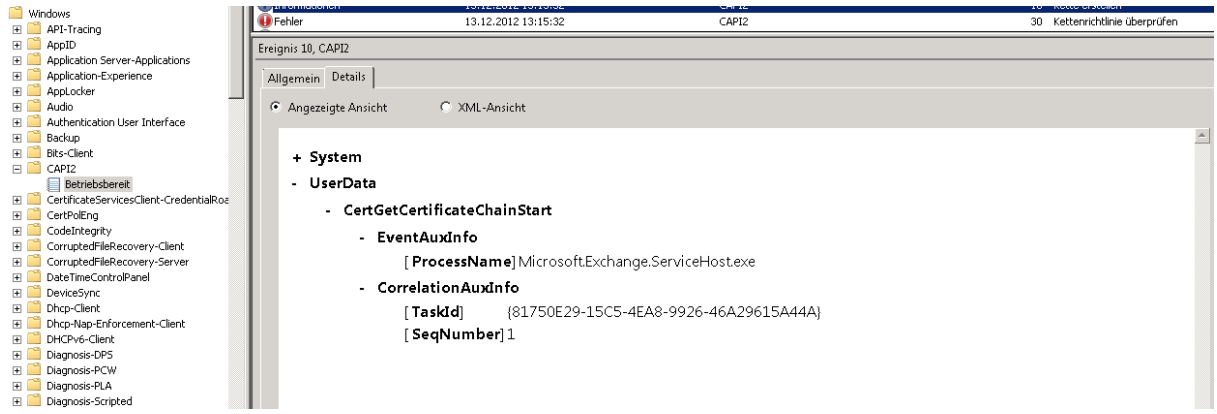
Mit dem Befehl *Certutil –Urlcache CRL delete* wurde der CRL Cache geloescht



Danach war der CRL Cache auch geleert.

Die Exchange Konsole meldete aber weiterhin dass die CRL-Pruefung nicht erfolgreich ist.

Daraufhin habe ich das CAPI-Logging auf dem Exchange Server aktiviert und festgestellt das der Microsoft Exchange Service Host noch versucht auf alte CRL-Informationen zuzugreifen und den Certificate Chain nicht pruefen kann, bzw. noch gegen den alten CDP auf dem alten PKI-Server prueft.



Die einfache Loesung war den Microsoft Exchange-Diensthost Service durchzustarten und danach konnte das neue Zertifikat auch gegen den CDP geprueft werden