

Mehrfach ausgestellte Zertifikate fuer die Remote Desktop Session Host Authentifizierung

Bei vielen Servern bei einem meiner Kunden ist mir aufgefallen, dass im Zertifikatspeicher des Computers sehr viele Zertifikate basierend auf der Vorlage RDP Session Host Authentication vorhanden sind

Konsolenstamm	Ausgestellt für	Ausgestellt von	Ablaufdatum	Beabsichtigte Zwecke	Anzeigename	Status	Zertifikatvo
Zertifikate (Lokaler Computer)							
Eigene Zertifikate							
Zertifikate							
Vertrauenswürdige Stammz...							
Organisationsvertrauen							
Zwischenzertifizierungsstell							
Vertrauenswürdige Herausst...							
Nicht vertrauenswürdige Ze...							
Drittanbieter-Stammzertifizi							
Vertrauenswürdige Persone...							
Remote Desktop							
Zertifikatregistrierungsinfo							
Smartcard vertrauenswürdigi							
SMS							
Vertrauenswürdige Geräte							
	301	301	02.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	27.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	12.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	08.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	31.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	08.08.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	24.06.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	25.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	04.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	17.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	02.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	05.05.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	10.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	21.02.2013	Clientauthentifizieru...	<Keine>	inco	
	301	301	16.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	05.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	02.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	16.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	21.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	30.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	21.08.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	28.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	25.05.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	16.04.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	15.04.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	14.04.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	06.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	14.05.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	13.08.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	24.07.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	14.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	18.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	24.02.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	28.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	09.08.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	21.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	31.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	15.08.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	24.04.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	27.06.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	29.01.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	13.03.2013	RDP Session Host Au...	<Keine>	Remot	
	301	301	07.02.2013	RDP Session Host Au...	<Keine>	Remot	

In der Ereignisanzeige

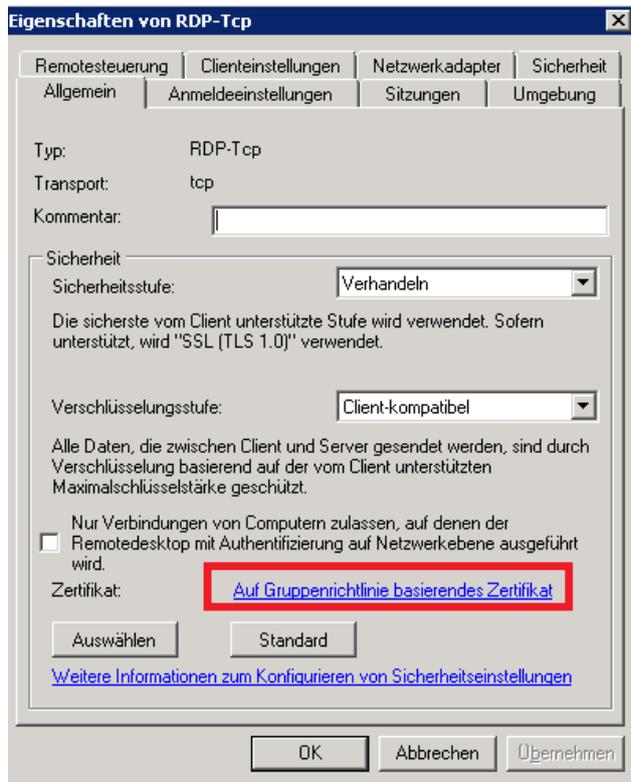
System	Anzahl von Ereignissen: 8.470			
Gefiltert: Protokoll: System; Quelle: ; Ereignis-ID: 1063 Anzahl der Ereignisse: 232				
Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	23.08.2012 01:24:32	TerminalServices-Remo...	1063	Keine
Informationen	22.08.2012 13:24:24	TerminalServices-Remo...	1063	Keine
Informationen	22.08.2012 13:07:47	TerminalServices-Remo...	1063	Keine
Informationen	22.08.2012 01:07:40	TerminalServices-Remo...	1063	Keine
Informationen	21.08.2012 13:07:28	TerminalServices-Remo...	1063	Keine
Informationen	21.08.2012 01:52:41	TerminalServices-Remo...	1063	Keine
Informationen	20.08.2012 13:52:28	TerminalServices-Remo...	1063	Keine
Informationen	20.08.2012 13:11:47	TerminalServices-Remo...	1063	Keine
Informationen	20.08.2012 01:11:40	TerminalServices-Remo...	1063	Keine
Informationen	19.08.2012 13:11:29	TerminalServices-Remo...	1063	Keine
Informationen	19.08.2012 03:48:40	TerminalServices-Remo...	1063	Keine
Informationen	18.08.2012 15:48:33	TerminalServices-Remo...	1063	Keine

Ereignis 1063, TerminalServices-RemoteConnectionManager

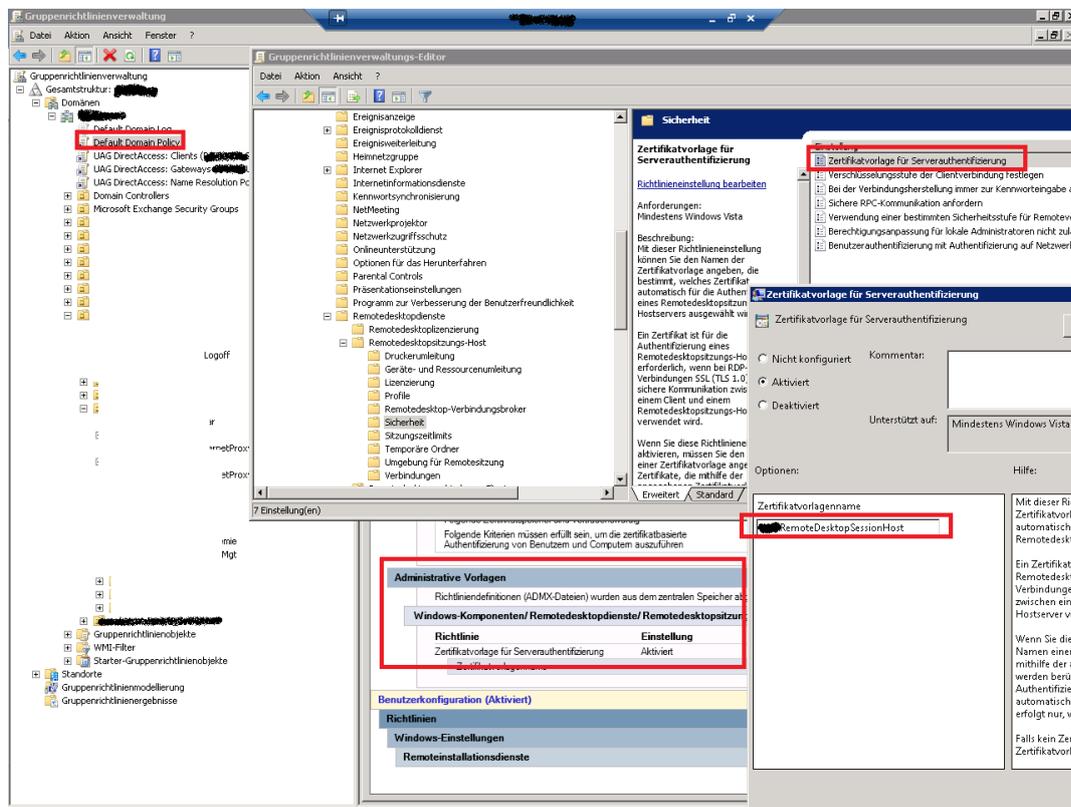
Allgemein Details

Es wurde ein neues vorlagenbasierten Zertifikat installiert, das vom Terminalserver für die Authentifizierung und Verschlüsselung mithilfe von Transport Layer Security (TLS) 1.0\Secure Sockets Layer (SSL) verwendet werden soll. Der Name dieses Zertifikats ist [REDACTED]. Der SHA1-Hashwert dieses Zertifikats wird in den Ereignisdaten bereitgestellt.

In den Eigenschaften der RDP-TCP Verbindung fuer die Remote Desktop Host Konfiguration steht:



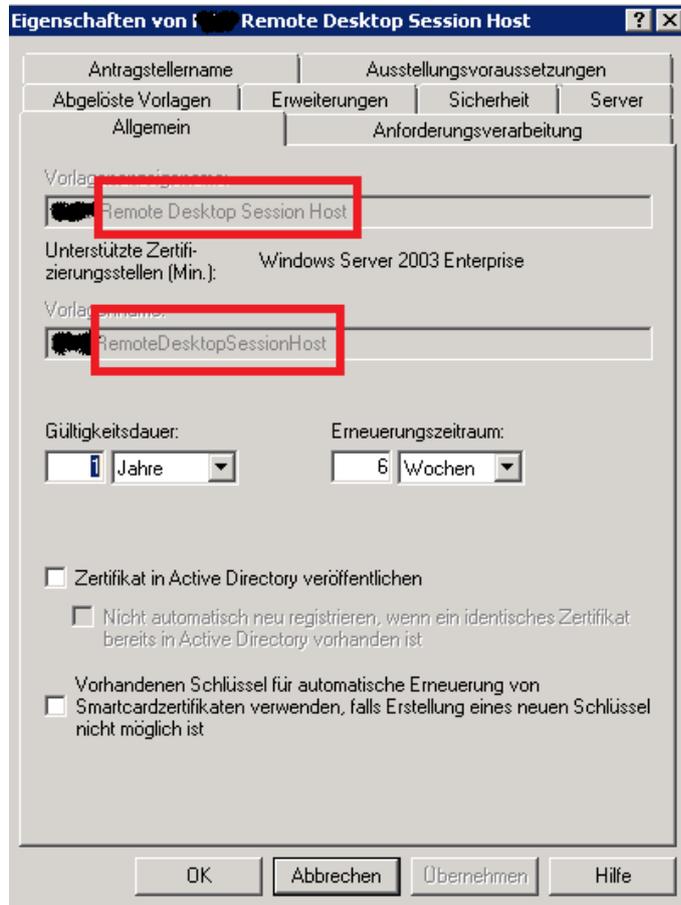
Ursache ist meinen Forschungen nach die folgende Gruppenrichtlinieneinstellung in der Default Domain Policy:



Nach langem Suchen bin ich hier fuendig geworden:

<http://support.microsoft.com/kb/2531138/en-us>

Der Anzeigename und der Name der Zertifikatvorlage sind unterschiedlich und/oder die Einstellungen in der Gruppenrichtlinie entsprechen nicht dem Namen der Zertifikatvorlage.

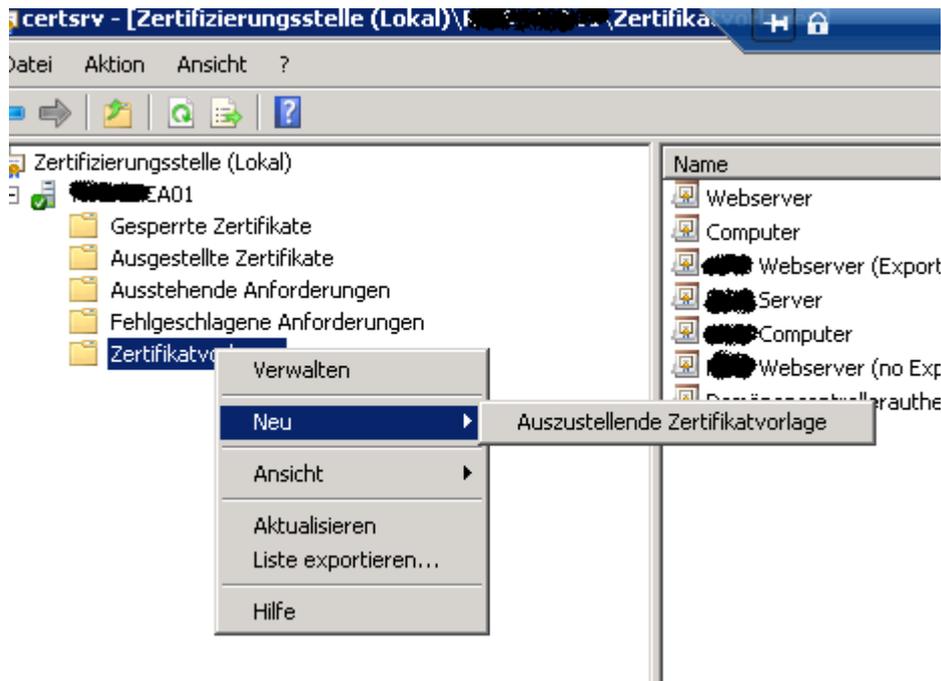


Loesung:

Namen aendern:



Vorlage neu ausstellen zur Verwendung fuer die CA



In der Gruppenrichtlinie sicherstellen dass der Name der Zertifikatvorlage mit dem Namen der Zertifikatvorlage in der Gruppenrichtlinie uebereinstimmt.

