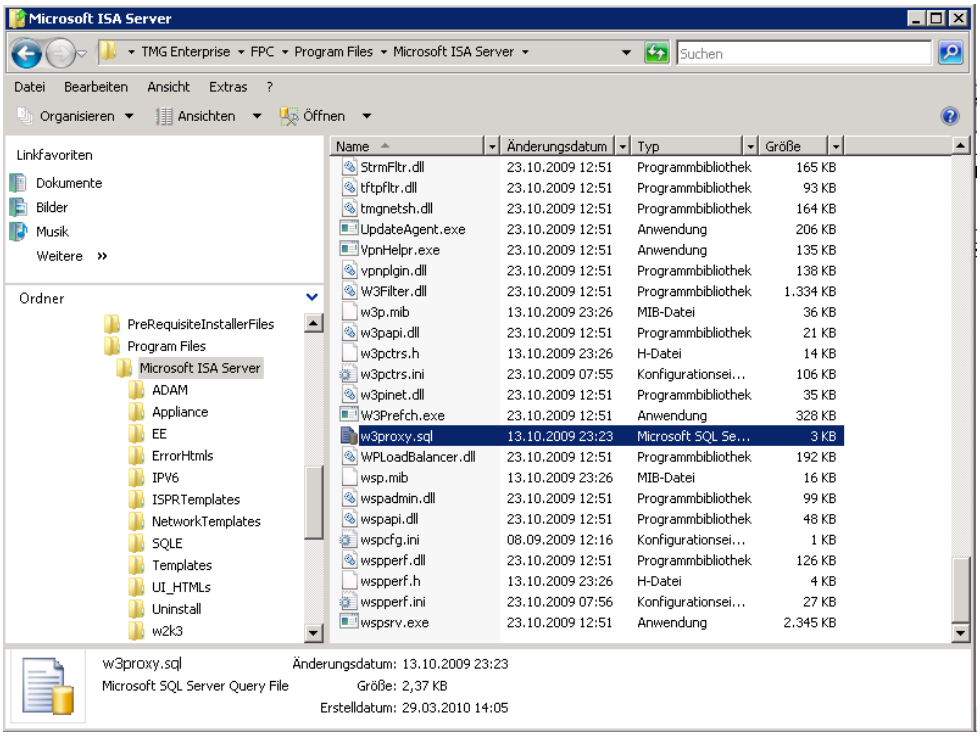
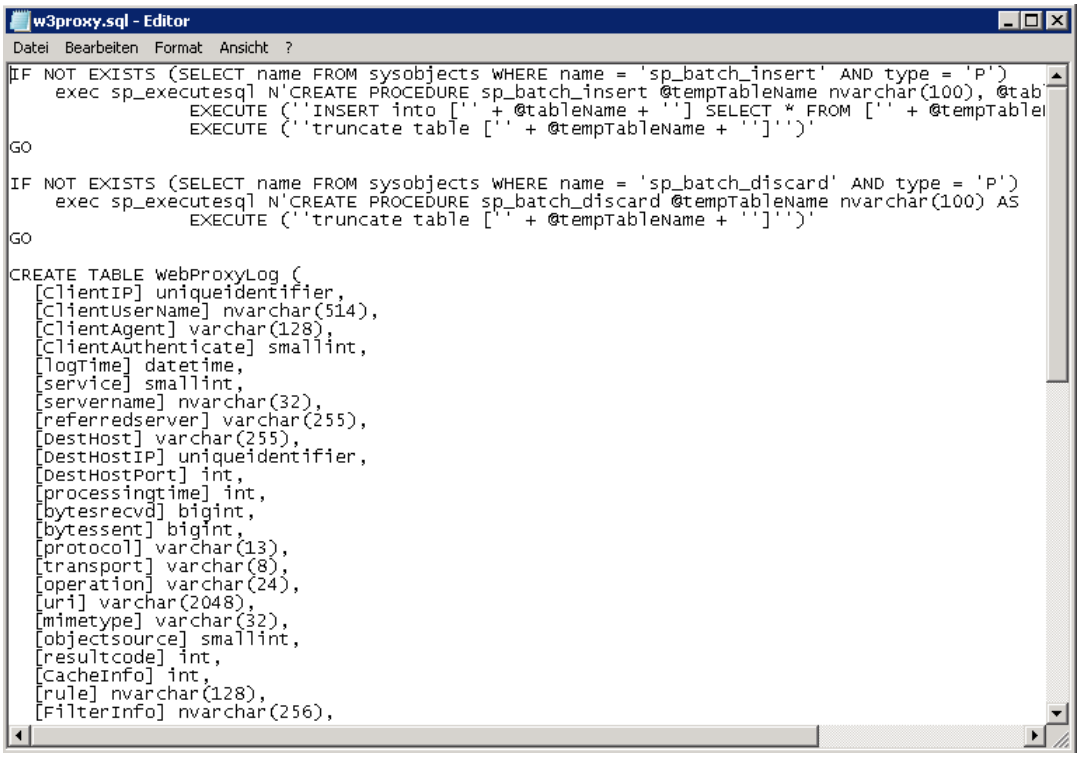
Forefront TMG - SQL Server Logging einstellen

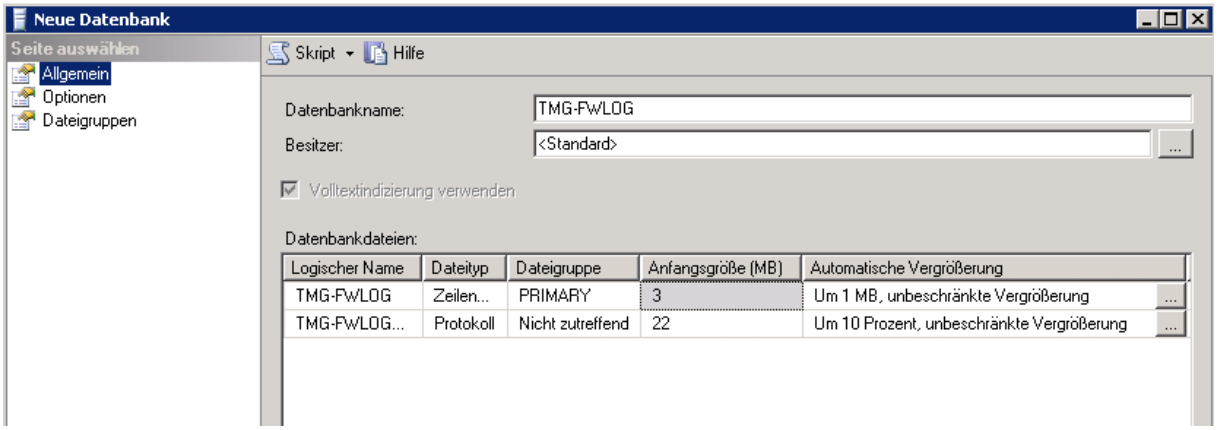
Skripte lokalisieren



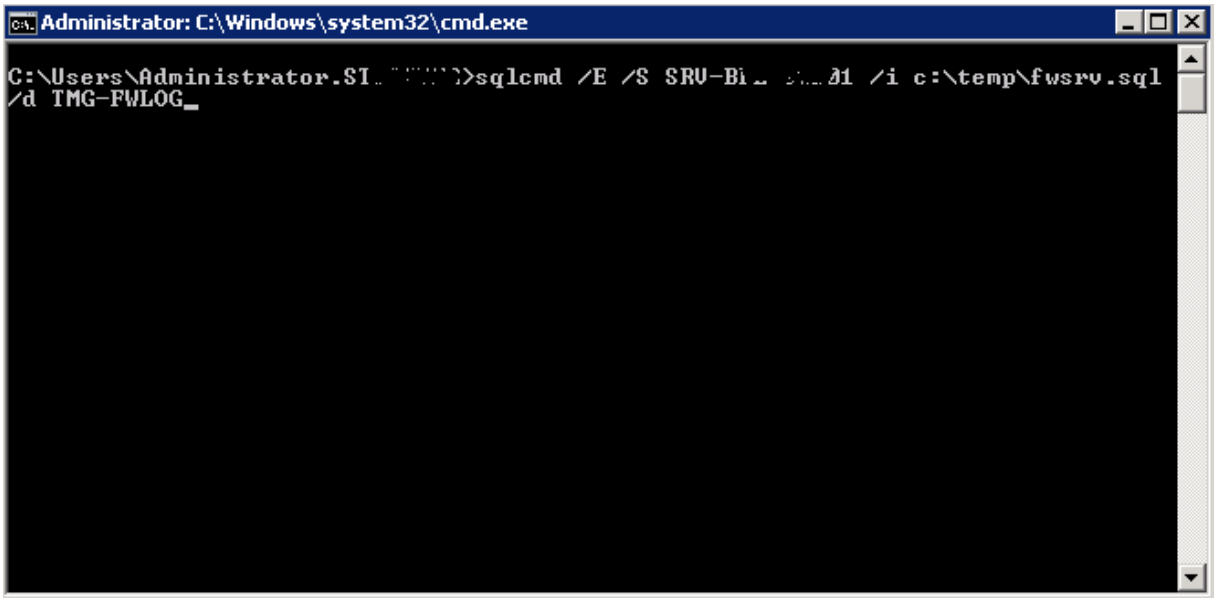
Inhalt



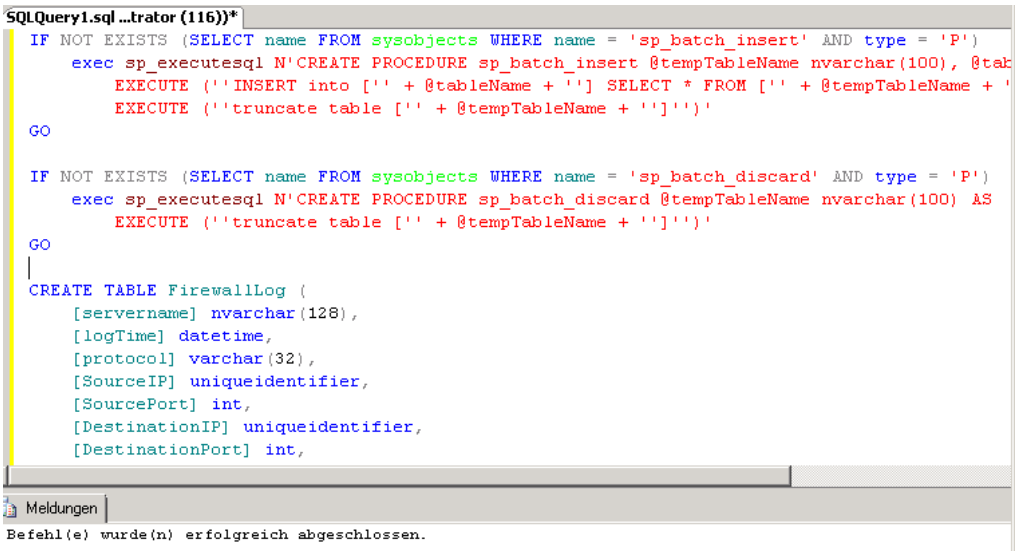
Neue DB fuer Webproxy Log und Firewall Log im Cluster anlegen



Skripte auf dem SQL Cluster ausfuehren



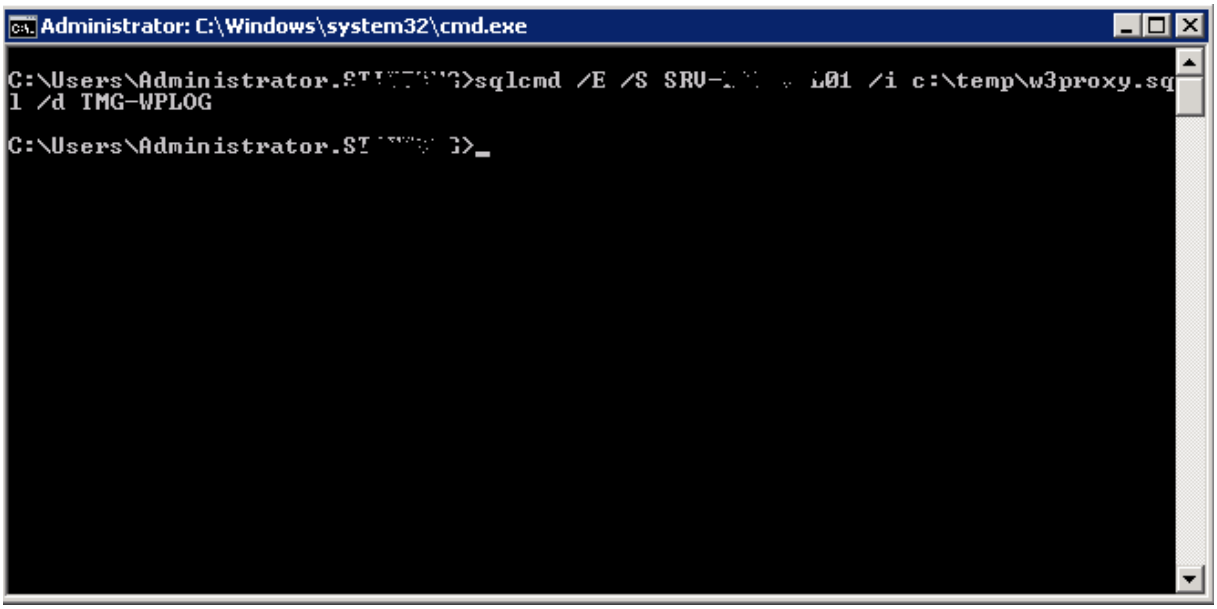
Oder per Management Studio



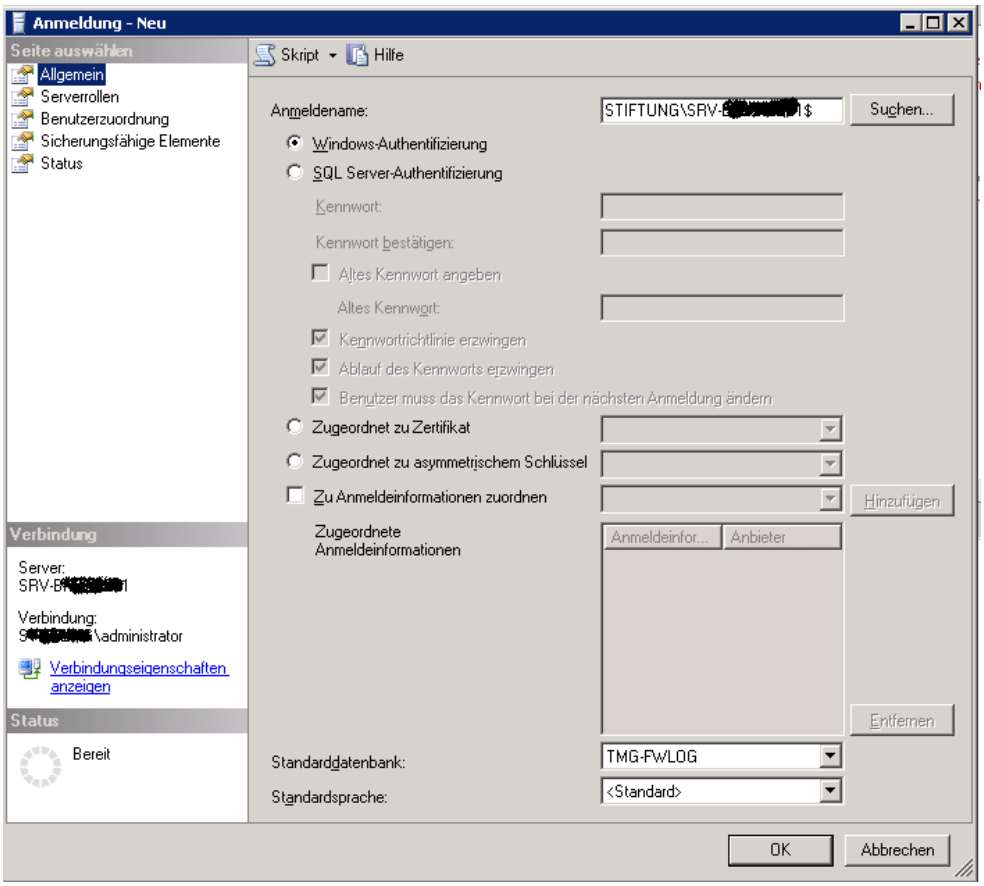
Das gleiche auch nochmal fuer das Webproxy Logging

DB anlegen

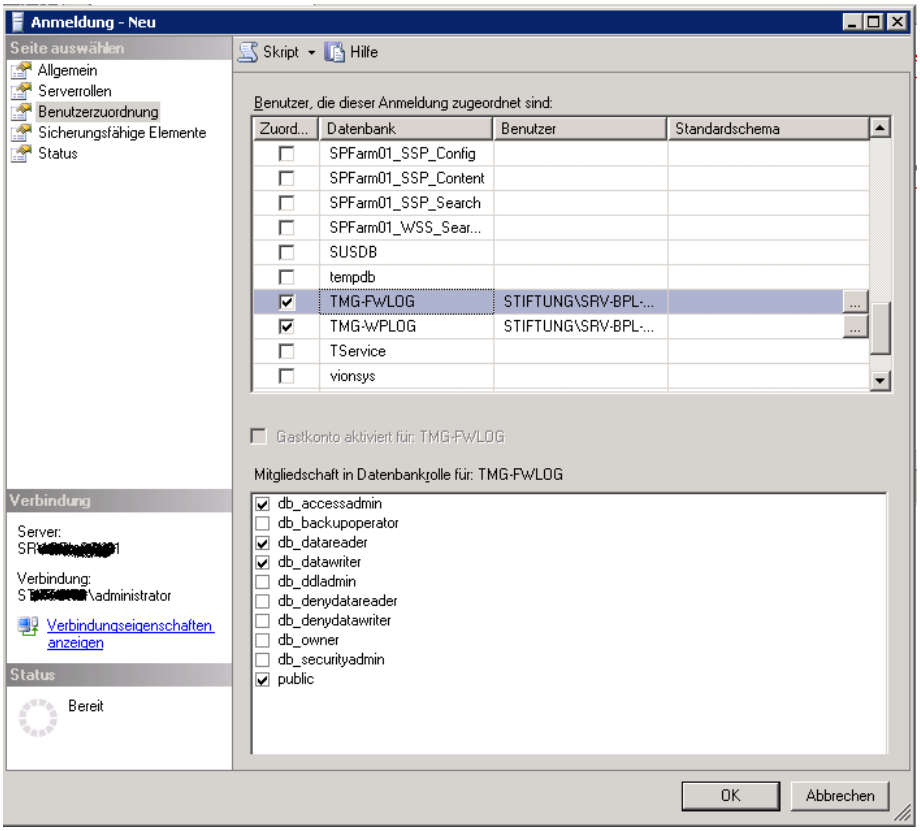
DB mit Tabellen fuellen



Neues SQL Login mit Windows Authentifizierung fuer die TMG Cluster Nodes anlegen

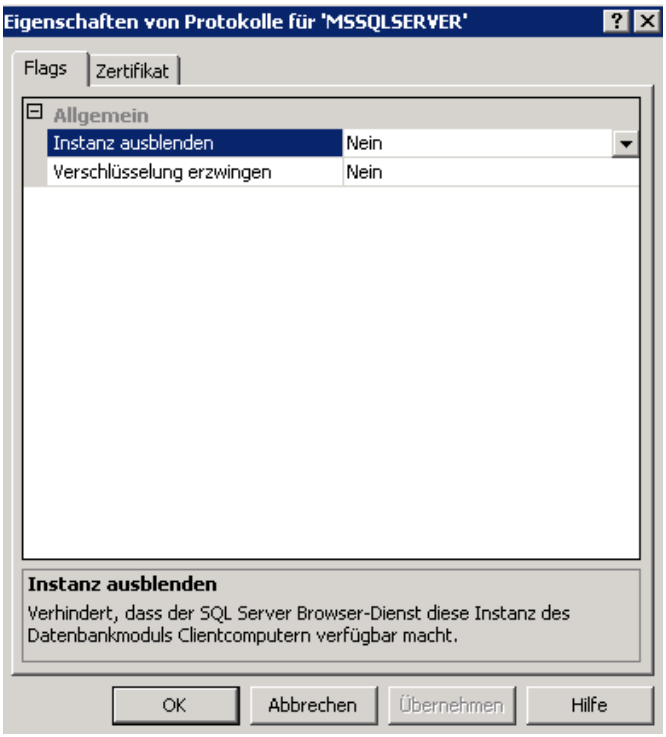


Benoetigte Rechte

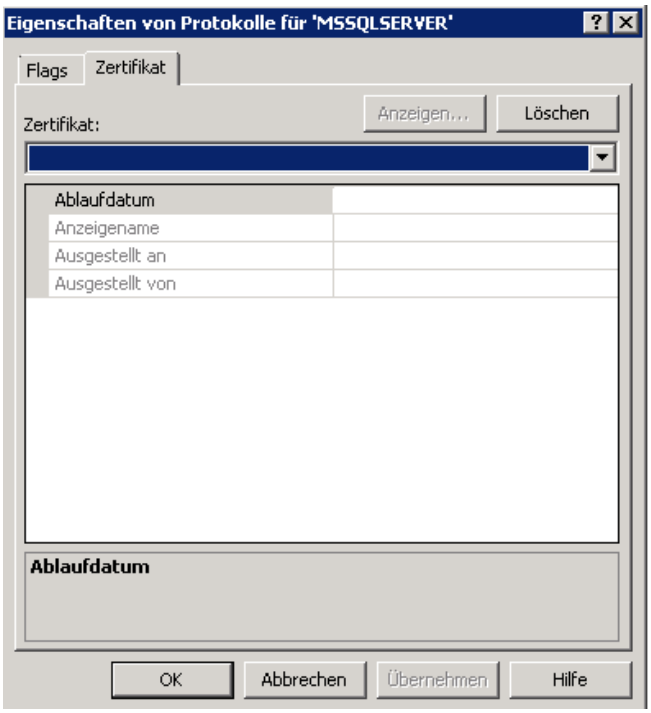


Verschluesselung auf dem SQL Server aktivieren

TMG verwendet standardmaessig eine HTTPS Verschluesselung zum SQL Server. Damit die Verschluesselung funktioniert, benoetigt der SQL Server ein Zertifikat einer RootCA, welcher TMG und SQL vertrauen und die Verschluesselung muss aktiviert werden. Achtung bei Force Encryption, wenn noch andere DB im Cluster liegen (was ja eigentlich der Fall sein sollte ☺.



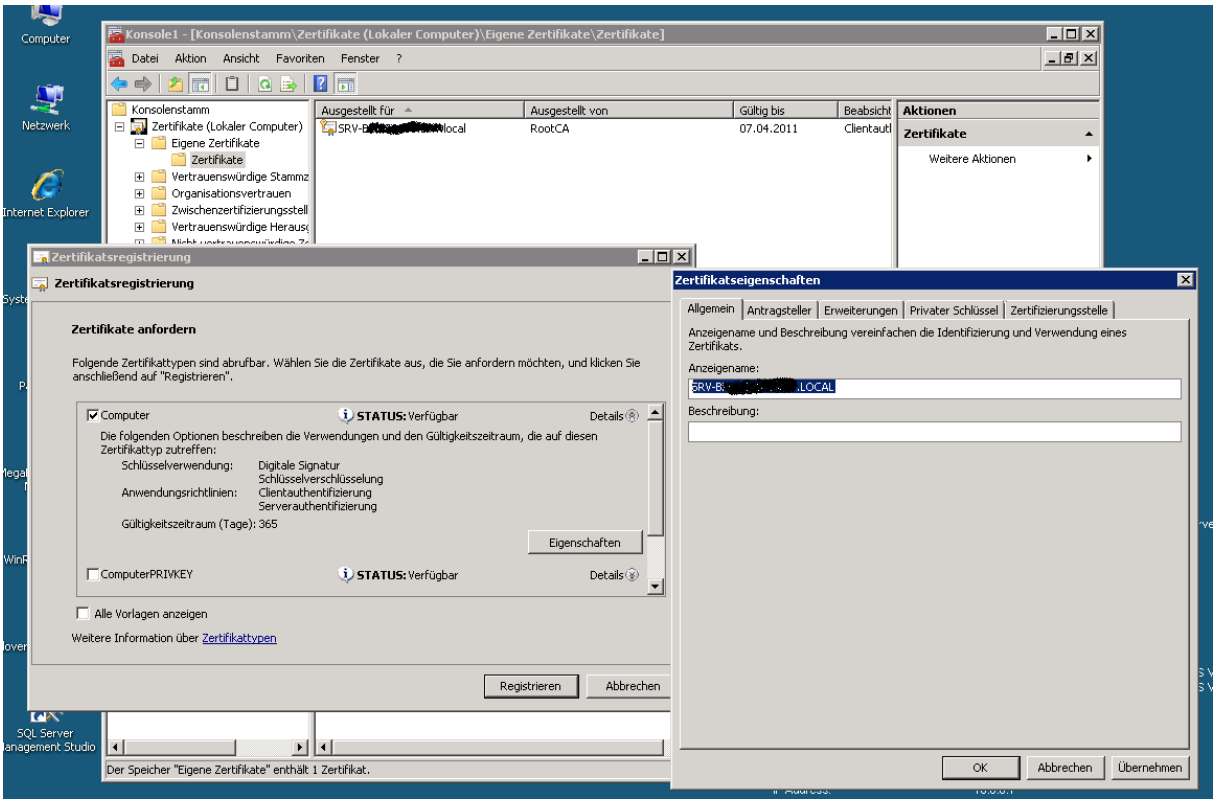
Kein Zertifikat vorhanden



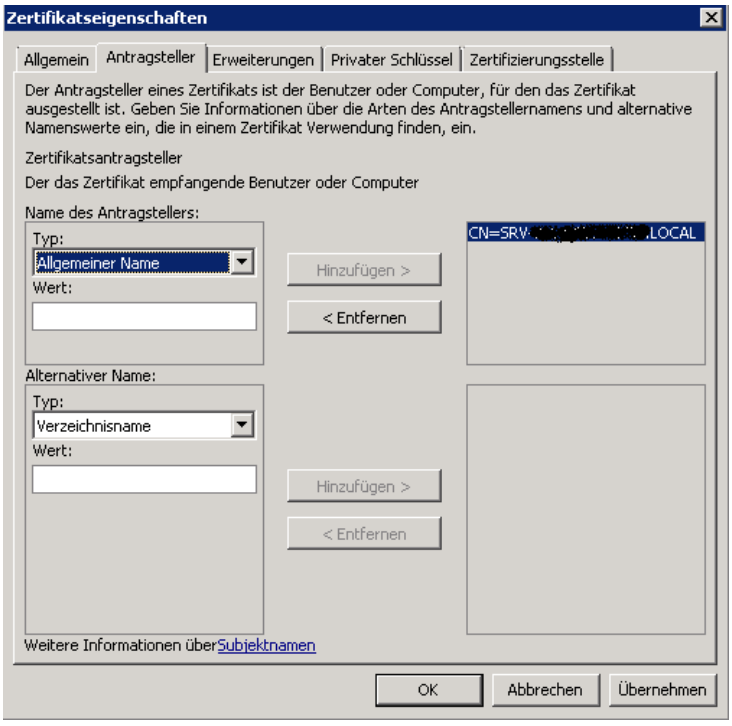
Verschluesselung auf einem Cluster
Wenn Sie die Verschlüsselung für einen Failovercluster verwenden möchten, müssen Sie das Serverzertifikat mit dem vollqualifizierten DNS-Namen der über den Failovercluster verfügenden Instanz auf allen Knoten im Failovercluster installieren. Wenn beispielsweise ein Cluster mit den beiden Knoten **test1.*your company*.com** und **test2.*your company*.com** sowie eine über einen Failovercluster verfügende Instanz von SQL Server mit dem Namen **fcisql** vorliegt, müssen Sie für **fcisql.*your company*.com** ein Zertifikat abrufen und auf beiden Knoten installieren.

Anschließend können Sie das Kontrollkästchen **ForceEncryption** im Eigenschaftenfeld **Protokolle für <Server>** der **SQL Server-Netzwerkkonfiguration** aktivieren, um den Failovercluster für die Verschlüsselung zu konfigurieren.

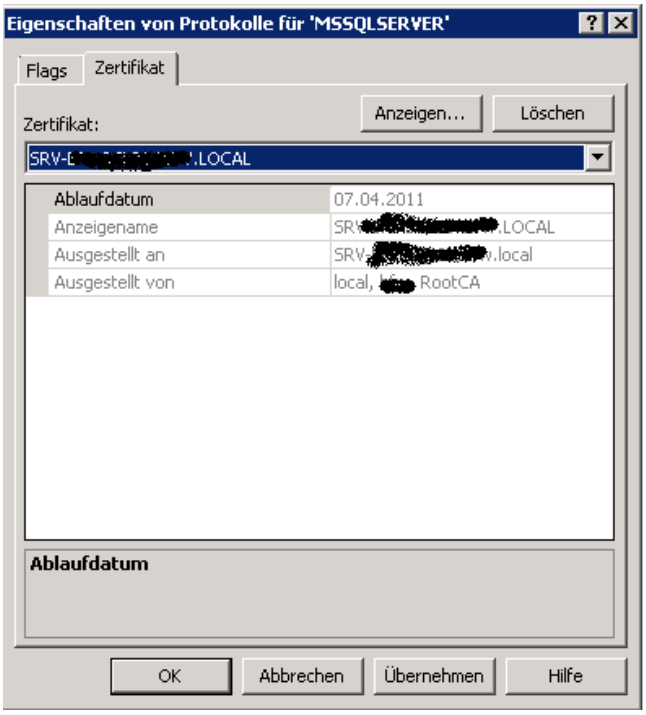
Zertifikat anfordern (lokaler Computer) – auf **ALLEN** SQL Cluster Knoten



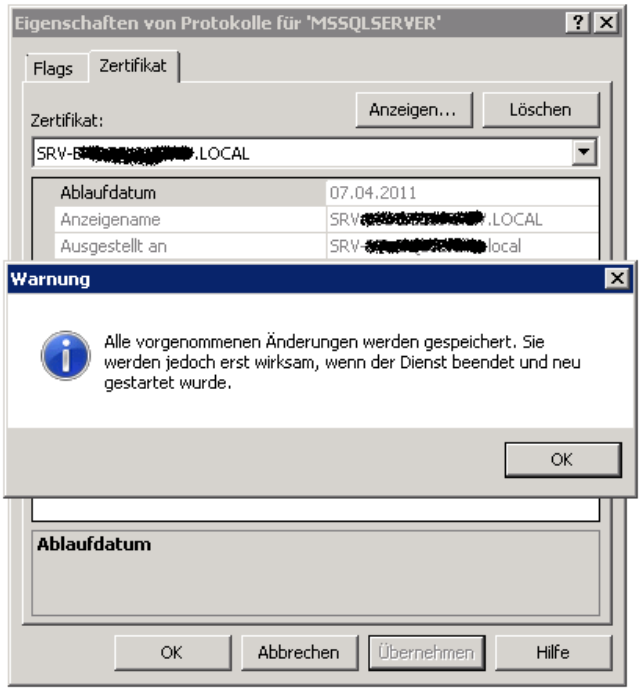
CN angeben



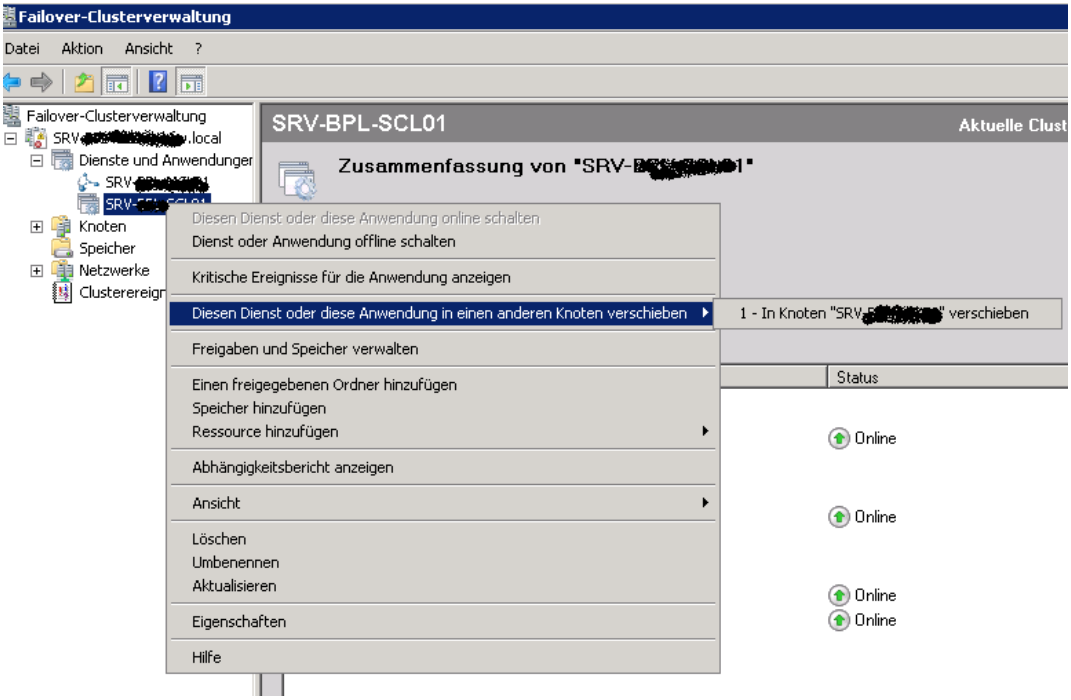
Jetzt kann auch das Zertifikat ausgewaehlt werden



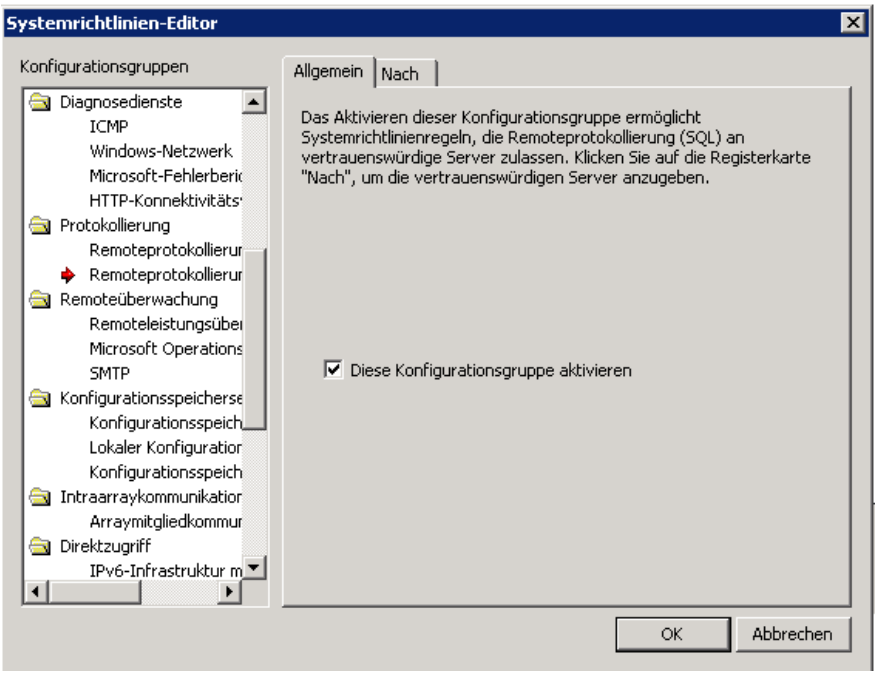
Auch auf dem zweiten SQL Node aktivieren



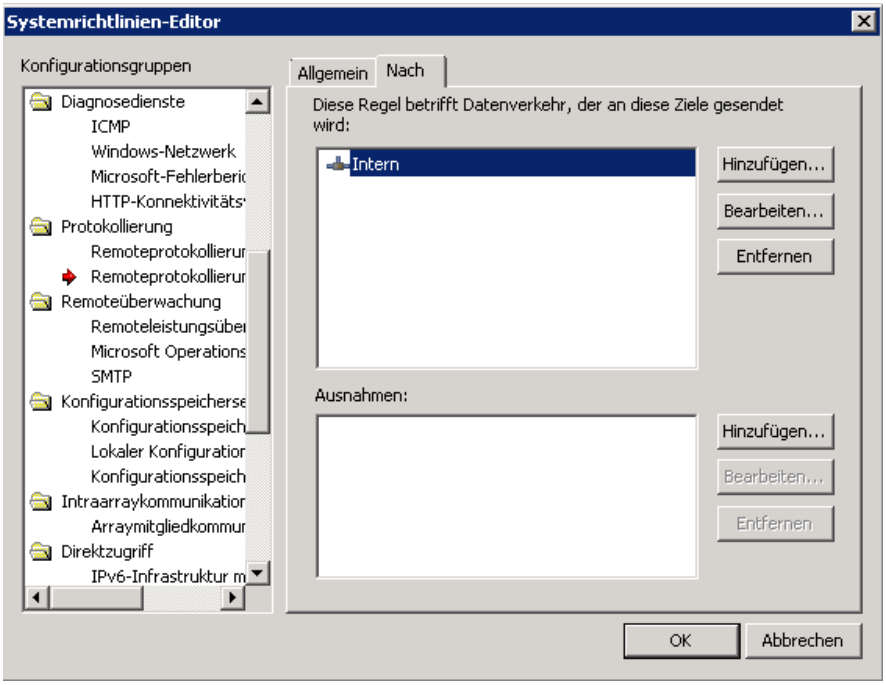
Also einmal einen SQL Cluster Schwenk durchfuehren und die SQL Dienste neu starten



TMG System Policy konfigurieren, das Remote SQL Logging erlaubt ist

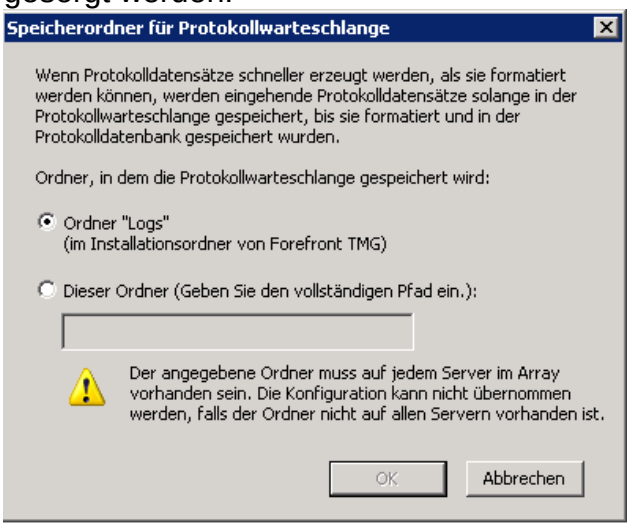


INTERN anpassen auf die SQL Nodes und Cluster



Large Logging Queue (LLQ)

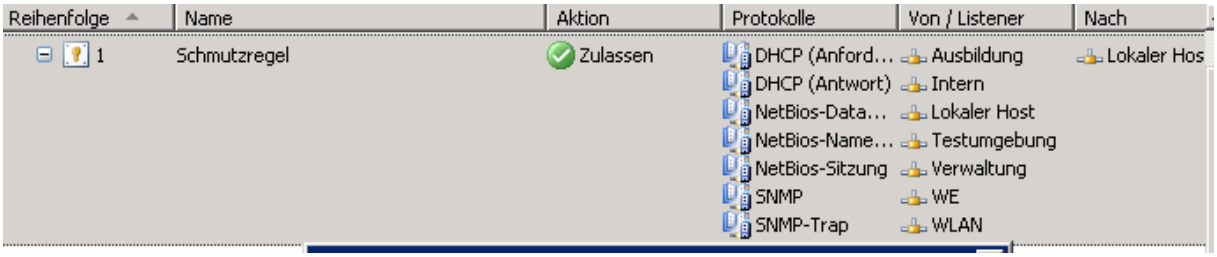
Wenn TMG nicht in den Remote SQL Server loggen kann, werden die Logs lokal zwischengespeichert. Hier sollte fuer ausreichend Plattenplatz auf den TMG Servern gesorgt werden.



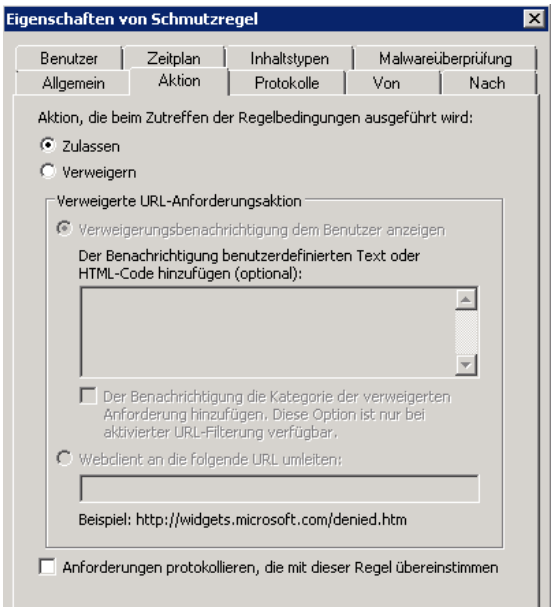
Damit wird verhindert das der TMG in den Firewall Lockdown Modus geht

Weitere Informationen zum TMG Firewall Lockdown Modus
http://www.isaserver.org/tutorials/Explaining-Microsoft-Forefront-TMG-Firewall-Lockdown-Mode.html

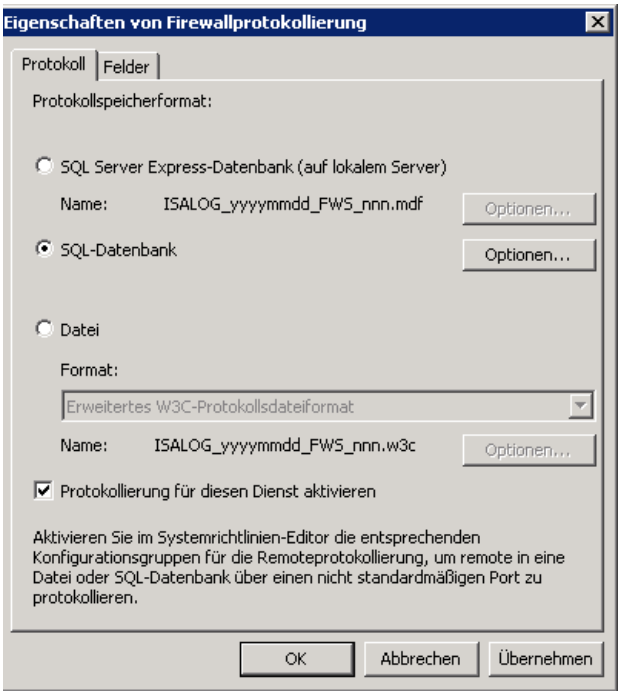
Da TMG sehr viel loggt, kann es Sinn machen, sogenannte Schmutzregeln zu konfigurieren, fuer die nicht notwendiger Traffic (DHCP/NETBIOS etc.) nicht gelogged wird. Damit schont man die Terrabytes auf dem SQL im SAN ☺



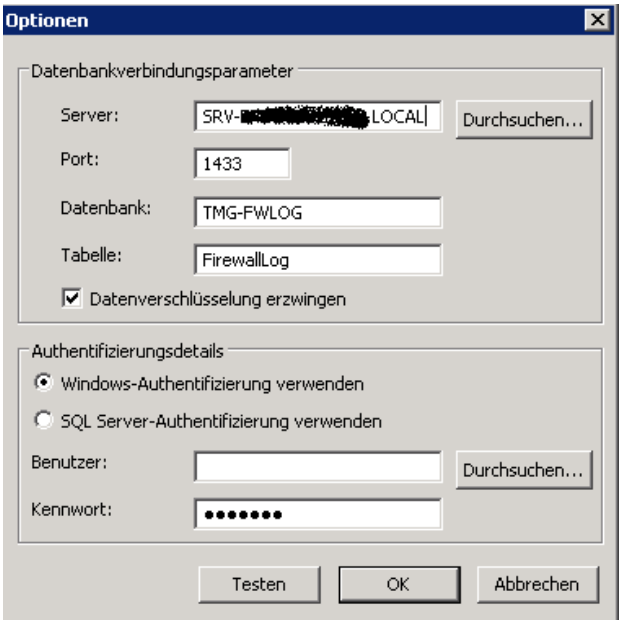
Nicht protokollieren



SQL Logging einschalten



Verbindungsparameter angeben



Testen