

WebDAV Publishing mit Forefront TMG

Autoren: Marc Grote und Yannik Kellner

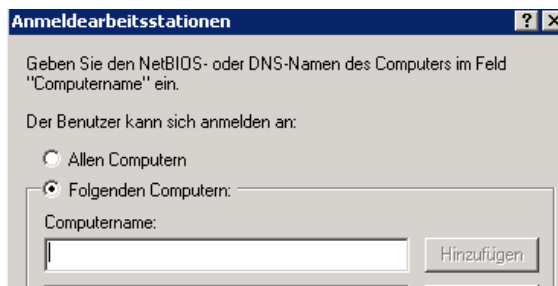
Umgebung:

Forefront TMG Server

IIS 7.0 Server mit WebDAV Extension

Benutzeraccount fuer WebDAV Zugriff

Komplexes Kennwort, Anmeldung nur am IIS Server erlauben, Kennwort laeuft nicht ab



Datenträgerpartition fuer WebDAV Daten

Eigene Festplattenpartition fuer die Daten auf welche per WebDAV zugegriffen werden soll oder mit Diskquotas arbeiten um einen Festplatteneueberlauf zu verhindern

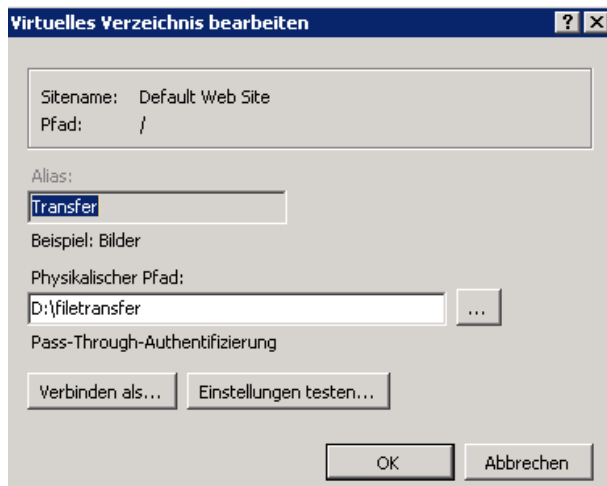
WebDAV Extension Download

<http://www.microsoft.com/downloads/en/details.aspx?FamilyID=13e97aaa-fb1b-4cf8-b95f-19ae02321385&displaylang=en>

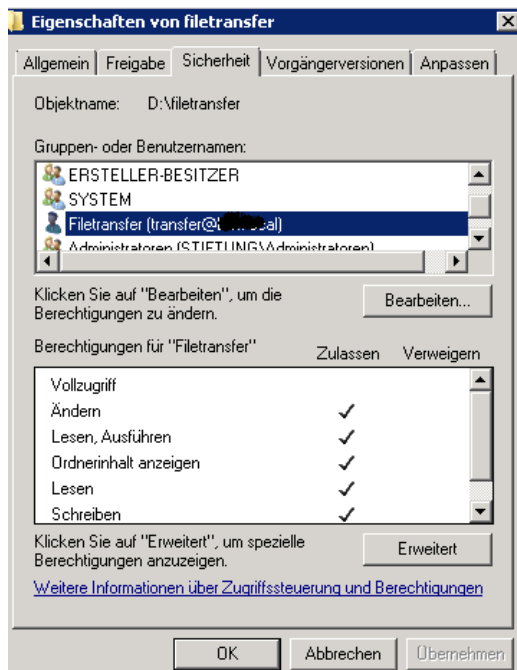
WebDAV Erweiterung installieren

IIS Einstellungen fuer WebDAV

Neues virtuelles Verzeichnis anlegen



Berechtigungen setzen



WebDAV Autorisierungsregel anlegen

WebDAV-Erstellungsregeln

Geben Sie mit diesem Feature Regeln zum Autorisieren von Benutzern für den Zugriff auf Inhalt an.

Pfad	Benutzer	Rollen	Zugriff
*	transfer		Lesen; S

Erstellungsregel bearbeiten

Zugriff zulassen für:

- Gesamter Inhalt
- Bestimmter Inhalt:

Beispiel: *.bas, wsvc.axd

Zugriff auf diesen Inhalt zulassen für:

- Alle Benutzer
- Bestimmte Rollen oder Benutzergruppen:

Beispiel: Admin, Guest
- Bestimmte Benutzer:

Beispiel: User1, User2

Berechtigungen

- Lesen
- Quelle
- Schreiben

OK Abbrechen

Aktionen

- Erstellungsregel hinzufügen...
- Bearbeiten...
- Entfernen...
- Nach oben
- Nach unten
- WebDAV-Einstellungen...
- Hilfe
- Onlinehilfe

SSL erfordern

SSL-Einstellungen

Auf dieser Seite können Sie die SSL-Einstellungen für den Inhalt einer Website oder Anwendung ändern.

SSL erforderlich

Clientzertifikate:

- Ignorieren
- Akzeptieren
- Erforderlich

Achtung: Evtl. Problem beruecksichtigen – Stichwort IE Zonenmodell

<http://www.it-training-grote.de/download/IIS-Auth.pdf>

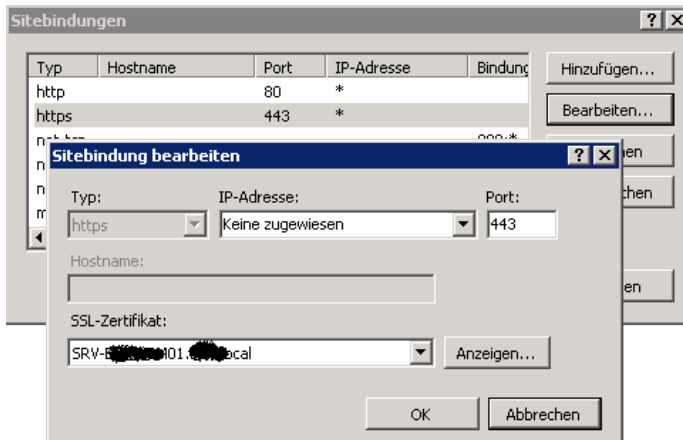
Achtung:

Basic Authentication ueber HTTPS fuer WebDAV und Windows Vista / 7

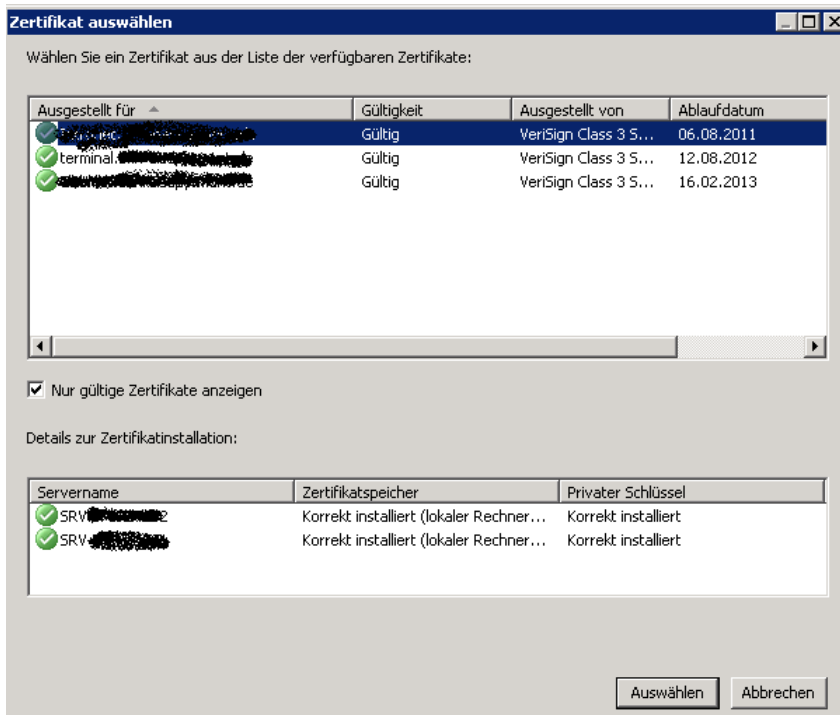
http://www.webdavsystem.com/server/documentation/authentication/basic_auth_vista

Webserver Zertifikat Intern

Ausgestellt auf den CN, welcher auch in der TMG Veroeffentlichungsregel verwendet wird

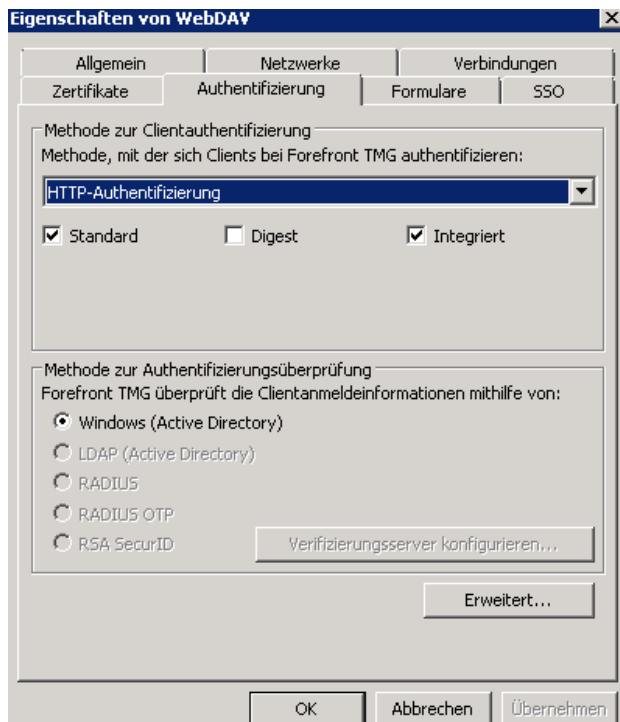
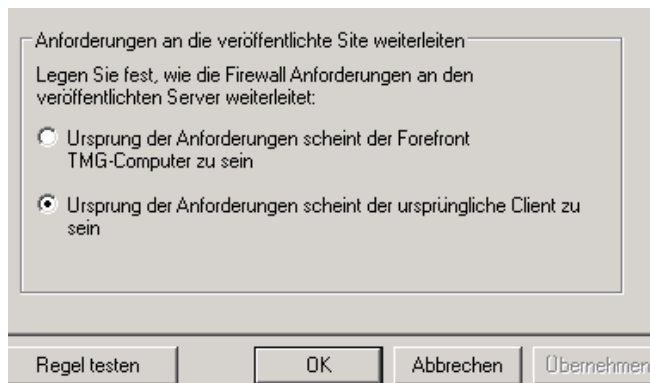


Webserver Zertifikat extern

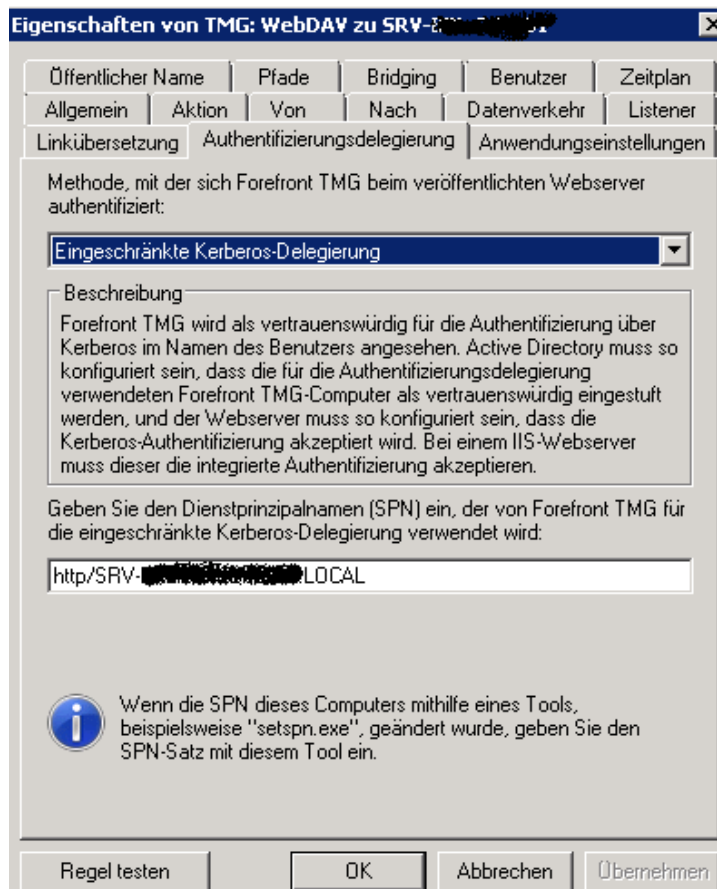


Forefront TMG Webserverpublishing Rule

Es wird eine normale sichere Webserververoeffentlichungsregel erstellt, daher hier nur die wichtigsten Schritte:



KDC einstellen

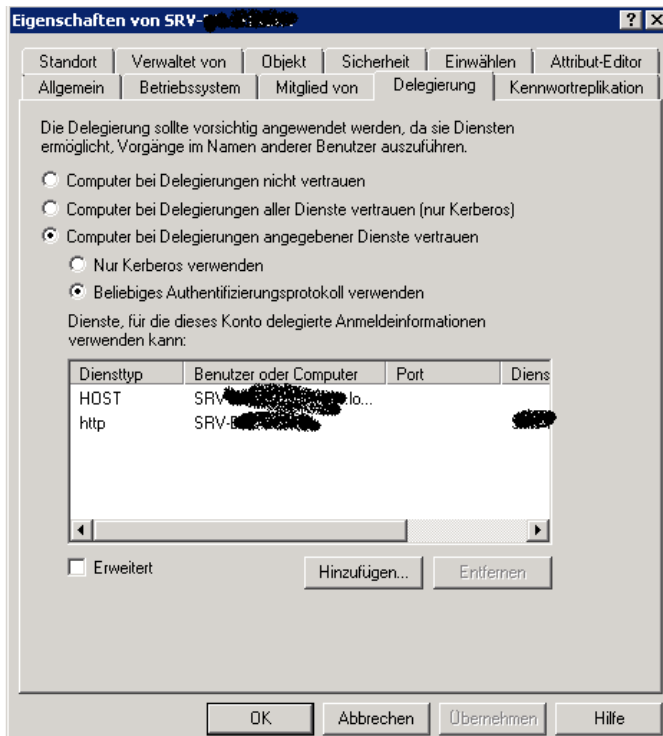


Der SPN muss mit SETSPN registriert werden und in ADUC fuer den TMG Server die Berechtigungen delegiert werden

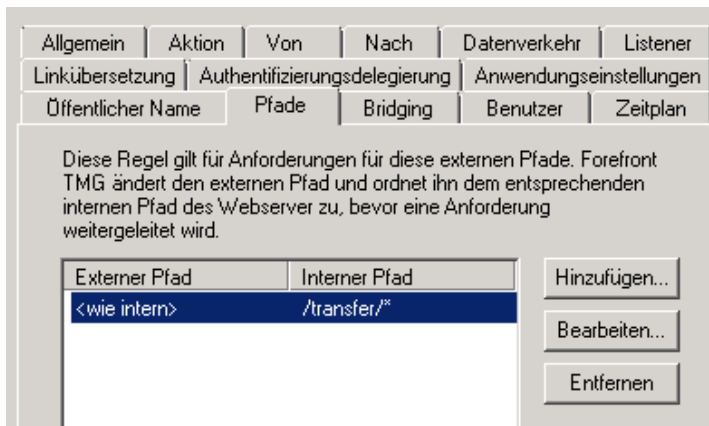
```
Administrator: Eingabeaufforderung
Hinweis: Diese Parameter können mit der Option "-S" verwendet werden,
um anzugeben, vor dem Hinzufügen des SPN eine Duplikatprüfung
ausgeführt werden soll.
Hinweis: -T kann mehrfach angegeben werden.

Beispiele:
setspn -R daserver1
  Registriert werden SPN "HOST/daserver1" und "HOST/<DNS von daserver1>"
setspn -A http/daserver daserver1
  Registriert wird SPN "http/daserver" für Computer "daserver1"
setspn -D http/daserver daserver1
  Gelöscht wird SPN "http/daserver" für Computer "daserver1"
setspn -F -S http/daserver daserver1
  Registriert wird SPN "http/daserver" für Computer "daserver1"
  ,falls kein derartiger SPN in der Gesamtstruktur vorhanden ist
setspn -U -A http/daserver dauser
  Registriert wird SPN "http/daserver" für das Benutzerkonto "dauser"
setspn -T * -T foo -X
  Gemeldet werden alle doppelten SPN-Registrierungen in dieser Domäne sowie
  foo setspn -T foo -F -Q */daserver
  Gefunden werden alle SPNs im Format */daserver die in der Gesamtstruktur von
  foo registriert sind.

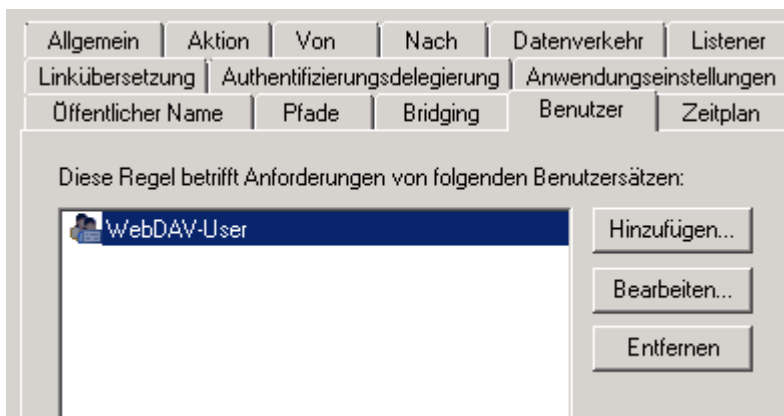
C:\Users\administrator.STIFTUNG>setspn -A NAME-IN-TMG-REGEL TMG-NETBIOSNAME_
```



Pfade beschraenken auf das WebDAV Verzeichnis



Benutzer im TMG auf die WebDAV Benutzer (Windows User oder –Gruppen) beschraenken



Clientzugriff auf die WebDAV Freigabe

Clientzugriff entweder per WebDAV Redirector von Windows Client oder extra WebDAV Client.



Aktuelles Problem zur Zeit: Ordner und Dateien koennen erstellt und geloesch, aber nicht umbenannt werden. Da arbeiten wir noch dran.