# WebDAV Publishing mit Forefront TMG

Autoren: Marc Grote und Yannik Kellner

<u>Umgebung:</u> 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



# Datentraegerpartition fuer WebDAV Daten

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

# WebDAV Extension Download

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=13e97aaa-fb1b-4cf8b95f-19ae02321385&displaylang=en

# WebDAV Erweiterung installieren

**IIS Einstellungen fuer WebDAV** 

Neues virtuelles Verzeichnis anlegen

Virtuelles Ve	rzeichnis bearbeiten	? ×
Sitename: Pfad:	Default Web Site /	
Alias:		
Transfer		
Beispiel: Bild	er	
Physikalische	er Pfad:	
D:\filetransf	er	
Pass-Throug	h-Authentifizierung	
Verbinden a	ils Einstellungen testen	
	OK Abbred	hen

# Berechtigungen setzen

📙 Eigenschaften von filetransfer	×
Allgemein Freigabe Sicherheit Vorgängerversione	en Anpassen
Objektname: D:\filetransfer	
Gruppen- oder Benutzernamen:	
& ERSTELLER-BESITZER	
SYSTEM	
👗 Filetransfer (transfer@tableal)	
Administratoren (STIETLING\Administratoren)	
Klicken Sie auf "Bearbeiten", um dieB Berechtigungen zu ändern.	earbeiten
Berechtigungen für "Filetransfer" Zulassen	Verweigern
Vollzugriff	-
Ändern 🗸	
Lesen, Ausführen 🗸	
Ordnerinhalt anzeigen 🗸	
Lesen 🗸	
Schreiben 🗸	
Klicken Sie auf "Erweitert", um spezielle Berechtigungen anzuzeigen.	Erweitert
Weitere Informationen über Zugriffssteuerung und Be	rechtigungen
OK Abbrechen	Übernehmen

# WebDAV Authorisierungsregel anlegen

	Male DAM Evetally in some	A	ktionen	
-	webDAv-Erstellungsreg	lein		Erstellungsregel hinzufügen
Geben S	ie mit diesem Feature Regeln zum Autori	isieren von Benutzern fü	ir den	Bearbeiten
Zugriff a	uf Inhalt an.		×	CEntfernen
Pfad *	Benutzer	Rollen		🖒 Nach oben
	Ci di Si Gi		Lesen, -	Nach unten
Erst	ellungsregel bearbeiten		? ×	WebDAV-Einstellungen
				) Hilfe
<sup>2</sup>	ugriff zulassen für:			Onlinehilfe
	Gesamter Inhalt			
0	Bestimmter Inhalt:			
	, Beispiel: *.bas, wsvc.axd			
	ugriff auf diesen Inhalt zulassen für: —			
0	- Alle Benutzer			
0	Bestimmte Rollen oder Benutzergrupp	en:		
	, Beispiel: Admin, Guest			
	Bestimmte Benutzer:			
	transfer			
	, Beispiel: User1, User2			
E	erechtigungen			
F	Lesen			
F	Quelle			
F	Schreiben			
		OK Abbrect	nen	

#### SSL erfordern



#### SSL-Einstellungen

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

Clientzertifikate: Ignorieren

- O Akzeptieren

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\_vist a

### Webserver Zertifikat Intern

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



### Webserver Zertifikat extern

	Gültigkeit	Ausgestellt	von	Ablaufdatum	
Ender Hick States and the second	Gültig	VeriSign Cla	ss 3 S	06.08.2011	
terminal.	Gültig	VeriSign Cla	ss 3 S	12.08.2012	
	Gültig	VeriSign Cla	ss 3 5	16.02.2013	
				1	
Nur aültige Zertifikate anzeigen				-	
, , , , , , , , , , , , , , , , , , ,					
ails zur Zertifikatinstallation:					
ails zur Zertifikatinstallation:	7ertifikatsneicher	Priva	ter Schlüs	cel	
ails zur Zertifikatinstallation: rvername ) SRV	Zertifikatspeicher	Priva echner Korr	ater Schlüs ekt installie	sel	
ails zur Zertifikatinstallation: Irvername SRV	Zertifikatspeicher Korrekt installiert (lokaler R Korrekt installiert (lokaler R	Priva echner Korr echner Korr	ater Schlüs ekt installie ekt installie	sel ert ert	
ails zur Zertifikatinstallation: rvername SRV	Zertifikatspeicher Korrekt installiert (lokaler R Korrekt installiert (lokaler R	echner Korr echner Korr	ater Schlüs ekt installie ekt installie	sel ert ert	

# Forefront TMG Webserverpublishing Rule

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

<ul> <li>Anforderungen an die veröffentlichte Site weiterleiten</li> <li>Legen Sie fest, wie die Firewall Anforderungen an den veröffentlichten Server weiterleitet:</li> <li>Ursprung der Anforderungen scheint der Forefront TMG-Computer zu sein</li> <li>Ursprung der Anforderungen scheint der ursprüngliche Client zu sein</li> </ul>					
Regel testen OK Abbrechen Übernehme					
Eigenschaften von WebDAV 🔀					
Allgemein     Netzwerke     Verbindungen       Zertifikate     Authentifizierung     Formulare     SSO       Methode zur Clientauthentifizierung     Methode, mit der sich Clients bei Forefront TMG authentifizieren:					
HTTP-Authentifizierung					
☑ Standard					
Methode zur Authentifizierungsüberprüfung Forefront TMG überprüft die Clientanmeldeinformationen mithilfe von: Windows (Active Directory) LDAP (Active Directory) RADIUS RADIUS RADIUS OTP Verifizierungsserver konfigurieren					
Erweitert					

ОК

Abbrechen Übernehmen

# KDC einstellen

Eigenschaften von TMG: WebDAV zu SRV-800 COMPANY					
Öffentlicher Name Pfade Bridging Benutzer Zeitplan Allgemein Aktion Von Nach Datenverkehr Listener Linkübersetzung Authentifizierungsdelegierung Anwendungseinstellungen					
Methode, mit der sich Forefront TMG beim veröffentlichten Webserver authentifiziert:					
Eingeschränkte Kerberos-Delegierung					
Beschreibung Forefront TMG wird als vertrauenswürdig für die Authentifizierung über Kerberos im Namen des Benutzers angesehen. Active Directory muss so konfiguriert sein, dass die für die Authentifizierungsdelegierung verwendeten Forefront TMG-Computer als vertrauenswürdig eingestuft werden, und der Webserver muss so konfiguriert sein, dass die Kerberos-Authentifizierung akzeptiert wird. Bei einem IIS-Webserver muss dieser die integrierte Authentifizierung akzeptieren. Geben Sie den Dienstorinzipalnamen (SPN) ein, der von Forefront TMG für					
http/SRV- <b>Wenn die SPN dieses Computers mithilfe eines Tools,</b> beispielsweise "setspn.exe", geändert wurde, geben Sie den SPN-Satz mit diesem Tool ein.					
Regel testen         OK         Abbrechen         Obernehmen					

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 -I * -I too -X Gemeldet werden alle doppelten SPN-Registrierungen in dieser Domäne sowi foo setspn -I foo -F -Q */daserver Gefunden werden alle SPNs im Format */daserver die in der Gesamtstruktur foo registriert sind.	Le Von
C:\Users\administrator.STIFTUNG>setspn -A NAME-IN-TMG-REGEL TMG-NETBIOSNAME	

Eigenschaften von SR <sup>1</sup>							
Standort Verwalte Allgemein Betrieb	t von Objekt Sicherheit Einwählen Attribut-Editor system Mitglied von Delegierung Kennwortreplikation						
Die Delegierung sollte vorsichtig angewendet werden, da sie Diensten ermöglicht, Vorgänge im Namen anderer Benutzer auszuführen.							
C Computer bei Dele	gierungen nicht vertrauen						
Computer bei Dele	gierungen aller Dienste vertrauen (nur Kerberos)						
Computer bei Dele	gierungen angegebener Dienste vertrauen						
C Nur Kerberos	verwenden						
Beliebiges Aut	hentifizierungsprotokoll verwenden						
Dienste, für die die verwenden kann:	ses Konto delegierte Anmeldeinformationen						
Diensttyp	Benutzer oder Computer Port Diens						
HOST	SRV III III III						
http							
•							
Erweitert	Erweitert Hinzufügen Entfernen						
	OK Abbrechen Übernehmen Hilfe						

Pfade beschraenken auf das WebDAV Verzeichnis

All	lgemein	Aktion	Von	Nach	Dater	nverkehr	Listener
Lin	kübersetz	ung 🛛 Au	thentifizierun	igsdelegieru	ng Anw	endungse	einstellungen
Ŭ	ffentlicher	Name	Pfade	de Bridging Bei		nutzer	Zeitplan
Diese Regel gilt für Anforderungen für diese externen Pfade. Forefront TMG ändert den externen Pfad und ordnet ihn dem entsprechenden internen Pfad des Webserver zu, bevor eine Anforderung weitergeleitet wird.							orefront enden
	Externer Pfad Interner Pfad					Hinz	utugen
Bearbeite						rbeiten	
						En	tfernen

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

Allgemein Aktion	Von	Nach	Datenve	rkehr	Listene	er
Linkübersetzung Aut	nentifizierung	gsdelegierung	Anwen	dungse	einstellung	en
Öffentlicher Name   Pfade   Bridgi		Bridging	Benutzer		Zeitplan	
Diese Regel betrifft A	nforderunge	n von folgend	len Benutz	zersätze Hinzu	en: Ifügen	
				Bear	beiten	
				Ent	fernen	

# Clientzugriff auf die WebDAV Freigabe

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

🍓 Ne	tzlaufwerk v	erbinden	×
$\bigcirc$	🍕 Netzlaul	fwerk verbinden	
	Welcher Nel	tzwerkordner soll zugeordnet werden?	
	Bestimmer hergestellt	n Sie den Laufwerkbuchstaben für die Verbindung und den Ordner, mit dem die Verbindung werden soll:	
	Laufwerk:	Z:	
	<u>O</u> rdner:	https://webdav.meine-domain.de/transfer	
		Beispiel: \\Server\Freigabe	
		厂 Verbindung bei <u>A</u> nmeldung wiederherstellen	
		Verbindung mit anderen Anmeldeinformationen herstellen	
		Verbindung mit einer Website herstellen, auf der Sie Dokumente und Bilder speichern können	
		Eertig stellen Abbrechen	

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