Microsoft Forefront TMG – Installing Forefront TMG on a RODC

Abstract

In this article I will explain how to install Forefront TMG on a Read Only Domain Controller (RODC).

Let's begin

Installing Forefront TMG on a Domain Controller was not a supported scenario until Forefront TMG Service Pack 1 has been released. With Forefront TMG SP1 we are now able to install Forefront TMG on a Domain Controller with the Read Only Domain Controller role (RODC). A RODC can be used for small branch offices which require a local Domain Controller but do not want to implement a full writeable Domain Controller in the branch office for security reasons.

As a prerequisite for installing a RODC the Windows Forest Functional Level must be Windows Server 2008 or higher and you must once prepare your Active Directory environment to allow a RODC installation with the command line tool ADPREP / RODCPREP which is a Windows Server component.

Next we create a new Organizational Unit (OU) in Active Directory. This OU is used by a preparation script of Forefront TMG to create the accounts and groups (SQL groups for example) which are required for a Forefront TMG installation.

Active Directory Users and Computers		
File Action View Help		
🗢 🔿 🙋 💼 🔏 📋 🖻 🙆	- 🔽 📷 🗏 🗽 🛅 🍸 🗾 🍇	
 Active Directory Users and Computers [W2K8R? Saved Queries adomain.local Builtin Computers 	2-EN. domain.lc Name TMG-BRANCH Properties General Managed By Object Security COM+ Attribute Editor TMG-BRANCH Description: Street: City: State/province:	Type User
	Zip/Postal Code:	
	OK Cancel Apply Help	

Figure 1: New OU for Forefront TMG

We can use the DSQUERY utility to locate the Distinguished Name (DN) for the new created OU. You must note the DN of the OU to execute the script to prepare the Forefront TMG installation.

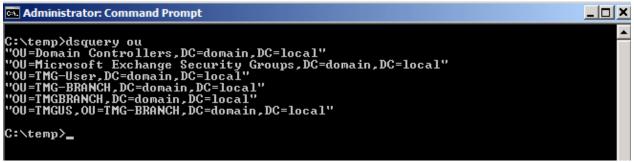


Figure 2: Execute DSQUERY to note the name of the OU

Script

The script which pre creates the Forefront TMG installation account and the SQL Server groups can be found <u>here</u>:

Copy the content of the script into a Notepad file and save it with a name you want and the .CMD extension and execute the script as shown in the following screenshot.

Attention: It is VERY important to enter the DN of the created OU with correct upperand lowercase characters. The script is case sensitive!

C:\temp>PrepareBranch.cmd RODC-TMG "OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local" The Organization Unit Tree OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local was not fou nd OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local will be created within 10 seconds *** If you do not want to create OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local *** Type Ctrl-C NOW !!! Waiting for 9 seconds, press a key to continue ... Creating OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local dsadd succeeded:OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local "OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local" dsadd succeeded:CN=SQLServer2005SQLBrowserUser\$RODC-TMG,OU=TMGUS,OU=TMG-BRANCH,D C=domain,DC=local dsadd_succeeded:CN=SQLServerMSSQLServerADHelperUser\$RODC-TMG,OU=TMGUS,OU=TMG-BRA NCH,DC=domain,DC=local NCH, DC=domain, DC=local dsadd_succeeded:CN=SQLServerMSSQLUser\$RODC-TMG\$ISARS,OU=TMGUS,OU=TMG-BRANCH,DC=d omain,DC=local dsadd_succeeded:CN=SQLServerMSSQLUser\$RODC-TMG\$MSFW,OU=TMGUS,OU=TMG-BRANCH,DC=do main,DC=local dsadd_succeeded:CN=SQLServerReportServerUser\$RODC-TMG\$MSRS10.ISARS,OU=TMGUS,OU=T MG-BRANCH,DC=domain,DC=local dsadd_succeeded:CN=SQLServerSQLAgentUser\$RODC-TMG\$ISARS,OU=TMGUS,OU=TMG-BRANCH,D asaaa sacceeaaacn-squserversquhgentuser\$RODC-IMG\$ISARS,OU=IMGUS,OU=IMG-BRANCH,D C=domain,DC=local dsadd succeeded:CN=SQLServerSQLAgentUser\$RODC-IMG\$MSFW,OU=IMGUS,OU=IMG-BRANCH,DC =domain,DC=local These groups are created: "CN=SQLServer2005SQLBrowserUser\$RODC-TMG,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=loc al" "CN=SQLServerMSSQLServerADHelperUser\$RODC-TMG,OU=TMGUS,OU=TMG-BRANCH,DC=domain,D C=local" UNN=SQLServerMSSQLL___fpope_TMCfLSoP2_ON_TMCN2_ON_TMC_PDOVCN_PC-local____ "CN=SQLServerMSSQLUser\$RODC-TMG\$ISARS,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local" "CN=SQLServerMSSQLUser\$RODC-TMG\$MSFW,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local" "CN=SQLServerReportServerUser\$RODC-TMG\$MSRS10.ISARS,OU=TMGUS,OU=TMG-BRANCH,DC=do main,DC=local" "CN=SQLServerSQLAgentUser\$RODC-TMG\$ISARS,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=loc al" "CN=SQLServerSQLAgentUser\$RODC-TMG\$MSFW,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=loca Enter User Password: Confirm user password: dsadd_succeeded:CN=RODC-TMGAdmin,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local "CN=RODC-TMGAdmin,OU=TMGUS,OU=TMG-BRANCH,DC=domain,DC=local" C:∖temp>

Figure 3: Forefront TMG account preparation script

After the script has been executed successfully you will see the new created users and groups in the Active Directory Users and Computers SnapIn.

Active Directory Users and Computers			_ _ 7 ×
File Action View Help			
늘 🔿 🙍 🚛 🤞 🗋 🕌 🖉 🖬 🍐	🖞 💐 🛅 🍸 💆 🖗		
Active Directory Users and Computers [W2K8R2-EN.domain.ld		Туре	Description
	SRODC-TMGAdmin	User	
⊡ 🙀 domain.local	SQLServer2005SQLBrowserUser\$RODC-TMG	Security Group - Global	Group for SQL Server Br
🗄 🧰 Builtin	& SQLServerMSSQLServerADHelperUser\$RODC-TMG	Security Group - Global	Group for SQL Server Ac
Computers	& SQLServerMSSQLUser\$RODC-TMG\$ISARS	Security Group - Global	Group for SQL Server.
	용 SQLServerMSSQLUser\$RODC-TMG\$MSFW SQLServerReportServerUser\$RODC-TMG\$MSRS10.IS SQLServerSQLAgentUser\$RODC-TMG\$ISARS	Security Group - Global	Group for SQL Server.
		Security Group - Global	Group for SQL Server Re
Costand-ound Managed Service Accounts		Security Group - Global	Group for SQL Server Ag
Microsoft Exchange Security Groups	& SQLServerSQLAgentUser\$RODC-TMG\$MSFW	Security Group - Global	Group for SQL Server Ac
🗉 📔 Program Data			
🗉 🧮 System			
E 💼 TMG-BRANCH			
TMGUS			
🖬 TMG-User			

Figure 4: New created user accounts and user groups

If you forgot to specify the password of the Forefront TMG service account until the script execution, a disabled user account will be created. You have to set a password for the account and the account must be enabled.

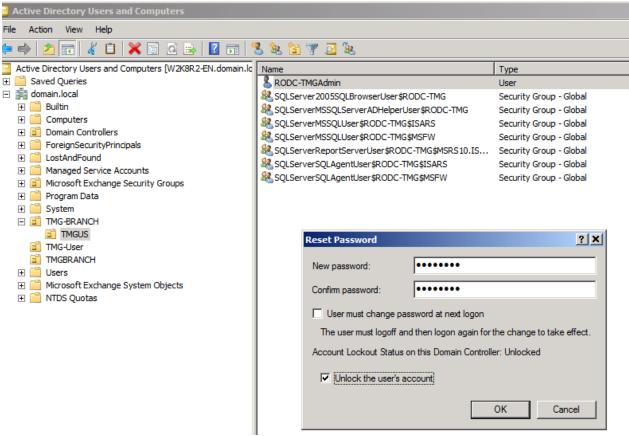


Figure 5: Change the password of the TMG Service account if you doesn't specified one in the script

Now it is time to precreate the RODC computer account before you install the RODC. Start Active Directory users and Computers, locate the Domain Controllers OU and pre-create the account.

ci 🔛 contan	
🛨 🚞 Computer	s
道 Domain	Delegate Control
🕀 🚞 Foreign	Pre-create Read-only Domain Controller account
🛨 🚞 LostAnı	Find
🛨 🚞 Manage —	
🛨 💼 Microsc	New 🕨
🛨 🚞 Prograr	All Tasks
🛨 🚞 System 🗌	
🖃 💼 TMG-BF	View •
🖬 TM	Refresh
💼 TMG-U:	Export List
🧾 TMGBR -	Export list
🛨 🧮 Users	Properties
🛨 📔 Microsc 🗌	
🕀 📔 NTDS 🤇	Help

Figure 6: Precreate RODC account

Specify the name of the RODC and the Active Directory site where the RODC will be installed.

For the delegated RODC installation and Administration account specify the account created be the script earlier.

🗟 Active Directory Domain Services Installation Wizard 🛛 🔀
Delegation of RODC Installation and Administration
The user or group that you specify will be able to attach a server to the RODC account that you are creating now and complete the RODC installation. They will also have local administrative permissions on this RODC.
To simplify administration, you should specify a group and then add individual users to the group.
Group or user:
DOMAIN\RODC-TMGAdmin Set
Other accounts can also inherit permissions on this RODC, but those accounts will not have local administrative permissions on this RODC unless you add those accounts explicitly.
More about delegation for read-only domain controller installation and administration
< <u>B</u> ack <u>N</u> ext > Cancel

Figure 7: RODC Account from the TMG script

The RODC computer account has been created in Active Diretcory.

Active Directory Users and Computers					
File Action View Help					
🗢 🔿 🖄 📷 🗎 🛱 🧟 🗟 🚺 🖬 🐍 🗞 1	🖥 🔻 🗾 🐍				
Active Directory Users and Computers [W2K8R2-EN.domain.lc	Name	Туре	DC Type	Site	Des
🕀 🚞 Saved Queries	TMG-RODC	Computer	Unoccupied DC Account (Read-only, GC)	Ingolstadt	
🖃 🚔 domain.local	W2K8R2-EN	Computer	GC	Ingolstadt	
🕀 🚞 Builtin					
🗄 🚞 Computers					
Domain Controllers					
🕀 🧰 ForeignSecurityPrincipals					

Figure 8: Unoccupied DC account before RODC installation

Navigate to the properties of the RODC account to the Password Replication Policy tab and click ADD to add additional users / groups you want to replicate to the RODC.

TMG-RODC Properties Location Managed By General Operating System This is a Read-only Domain computers passwords accoor accounts that are in the All replicated to the RODC. Groups, users and computer	n Member Of Delega Controller (RODC). An RC rding to the policy below. ow groups and not in the D	tion Password Rep DDC stores users and Only passwords for	22
Name	Active Directory Dom	Setting	
Account Operators	domain.local/Builtin	Deny	
Administrators	domain.local/Builtin	Deny	
Allowed RODC Passw	domain.local/Users	Allow	
Backup Operators	domain.local/Builtin	Deny	
Denied RODC Passwo	domain.local/Users	Deny	
Server Operators	domain.local/Builtin	Deny	
Advanced	<u>A</u> dd	<u>R</u> emove]
gure 9: RODC Password repl	OK Cancel	Apply	Help

Figure 9: RODC Password replication policy

Allow passwords to replicate to the RODC

Add Groups, Users and Computers
Choose the setting for the account you are adding to the password replication policy.
 Allow passwords for the account to replicate to this RODC
O Deny passwords for the account from replicating to this RODC
OK Cancel

Figure 10: Allow password replication to the RODC for the TMG accounts

Select all accounts and groups created earlier by the script.

Select Users, Computers, or G	roups		?
Select this object type:			
Users, Computers, Groups, or Built-in	security principals		Object Types
From this location:			
domain.local			Locations
Common Queries			
Name: Starts with			<u>C</u> olumns
			Find Now
Description: Starts with			Tind tow
Disabled accounts			Stop
Non expiring password			
	-		e-
Days since last logon:	-		P
	-		9 7
	2		<i>9</i>
Days since last logon:	7		DK Cancel
Days since last logon:	-		
Days since last logon:	E-Mail Address	Description	In Folder
Days since last logon:			In Folder
Days since last logon:		Description	In Folder domain.local/Co domain.local/Us
Days since last logon:		Description Members in the	In Folder domain local/Co domain local/Us domain local/Us
Days since last logon: Search results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServer2005SQLBrowserUser		Description Members in the Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/Us
Days since last logon: earch results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2. SQLServer2005MSSQLUser\$W2. SQLServer2005SQLBrowserUser. SQLServerMSSQLServerADHelp.		Description Members in the Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T
Days since last logon: earch results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServer2005SQLBrowserUser SQLServerMSSQLServerADHelp SQLServerMSSQLUser\$RODC-T		Description Members in the Group for SQL S. Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T domain.local/T
Days since last logon: Search results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServerMSSQLServerADHelp SQLServerMSSQLUser\$RODC-T SQLServerMSSQLUser\$RODC-T		Description Members in the Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T domain.local/T domain.local/T
Days since last logon: Search results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServer2005SQLBrowserUser SQLServerMSSQLServerADHelp SQLServerMSSQLUser\$RODC-T SQLServerMSSQLUser\$RODC-T SQLServerReportServerUser\$R		Description Members in the Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T domain.local/T domain.local/T domain.local/T
Days since last logon: Search results: ame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServer2005SQLBrowserUser SQLServerMSSQLUser\$RODC-T SQLServerMSSQLUser\$RODC-T SQLServerReportServerUser\$R SQLServerReportServerUser\$R SQLServerSQLAgentUser\$ROD		Description Members in the Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T domain.local/T domain.local/T domain.local/T
Days since last logon: Search results: Jame (RDN) SHAREPOINT SQLServer2005MSFTEUser\$W2 SQLServer2005MSSQLUser\$W2 SQLServerMSSQLServerADHelp SQLServerMSSQLUser\$RODC-T SQLServerMSSQLUser\$RODC-T		Description Members in the Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S. Group for SQL S.	In Folder domain.local/Co domain.local/Us domain.local/Us domain.local/T domain.local/T domain.local/T domain.local/T domain.local/T domain.local/T

Figure 11: Select all TMG accounts and groups

RODC Installation

After all prerequisted has been finished you are now able to install the Read Only Domain Controller (RODC). Start DCPROMO on the new Windows Server 2008 R2 machine and follow the instructions of the wizard. Because we precreated the RODC account in Active Directory we will get the infomational message that the account already exists which we accept whit clicking the OK checkbox.

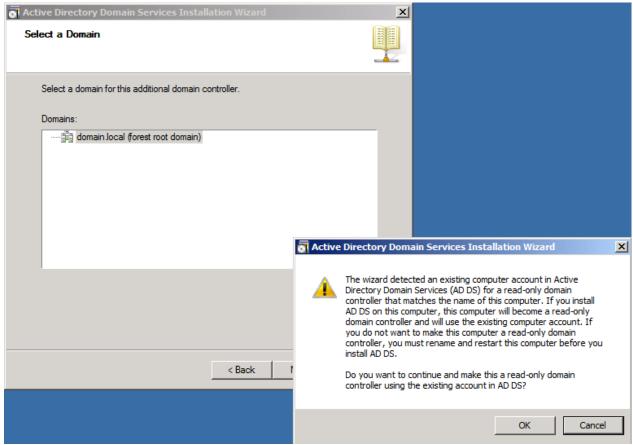


Figure 12: RODC installation

Forefront TMG Installation

After a successful RODC installation we start with installing Forefront TMG on the Server. The setup process is almost the same as a Forefront TMG installation on a Windows member server.

First we need to install the Forefront TMG preqrequisites. This must be done with a command line tool called Servermanagercmd which is the command line part of the UI tool Servermanager which is used since Windows Server 2008 to install roles and features on a Windows Server 2008 machine.

C:\Users\administrator.DOMAIN>ServerManagerCmd.exe
Servermanagercmd.exe is deprecated, and is not guaranteed to be supported in fut ure releases of Windows. We recommend that you use the Windows PowerShell cmdlet s that are available for Server Manager.
Start Installation
Skipping [.NET Framework 3.5.1 Features] .NET Framework 3.5.1 because it is alre ady installed on this computer.
<u> </u>

Figure 13: Installing Forefront TMG prerequistes

TMG SP1 Slipstream Installation

Because the RTM version of Forefront TMG doesn't support the installation on a RODC you must create a Slipstream installation of Forefront TMG RTM with Forefront TMG SP1. Copy the content of the Forefront TMG DVD and the .MSP file of Forefront TMG to a local directory on the Server and execute the following command from the command line.

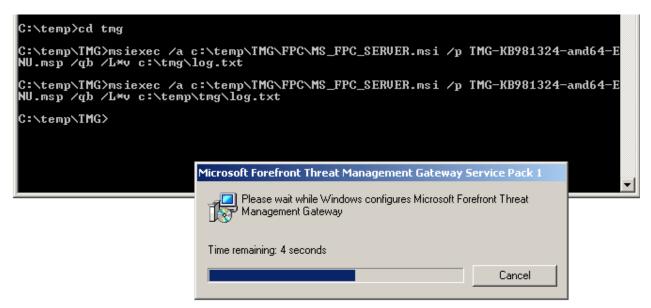


Figure 14: Forefront TMG SP1 Slipstream installation

After the Forefront TMG SP1 slipstream installation was successfully we can start installing Forefront TMG on the RODC. The installation process is now the same as every Forefront TMG installation.

Conclusion

In this article I tried to show you how to install Forefront TMG on a Read Only Domain Controller (RODC). I personally never had to install a TMG Server on a RODC but as you have been seen in this article it is possible without problems when you are good prepared.

Related links

Installing Forefront TMG on a RODC http://technet.microsoft.com/en-us/library/ff808305.aspx