
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.

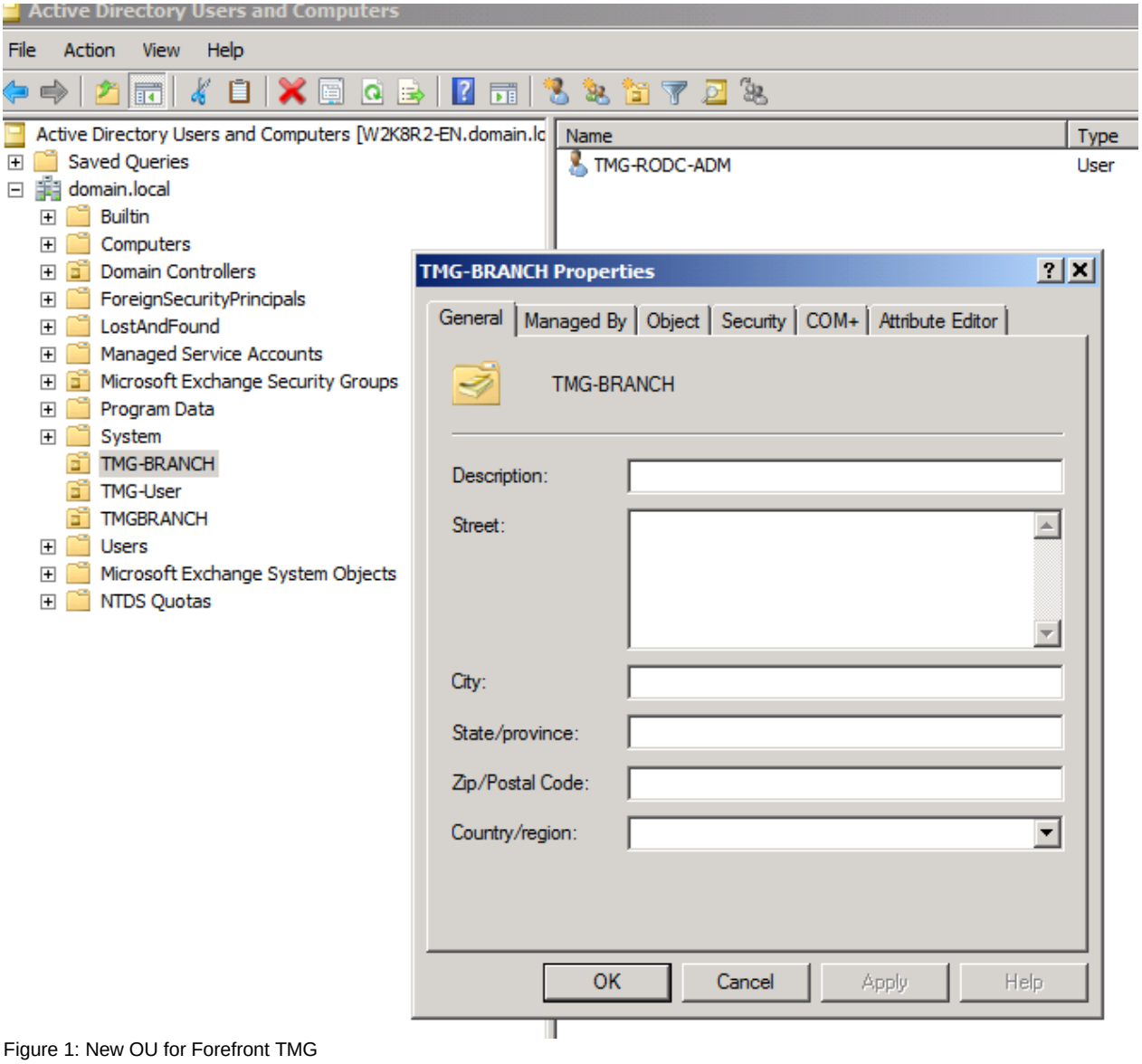

Figure 1: New OU for Forefront TMG

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.

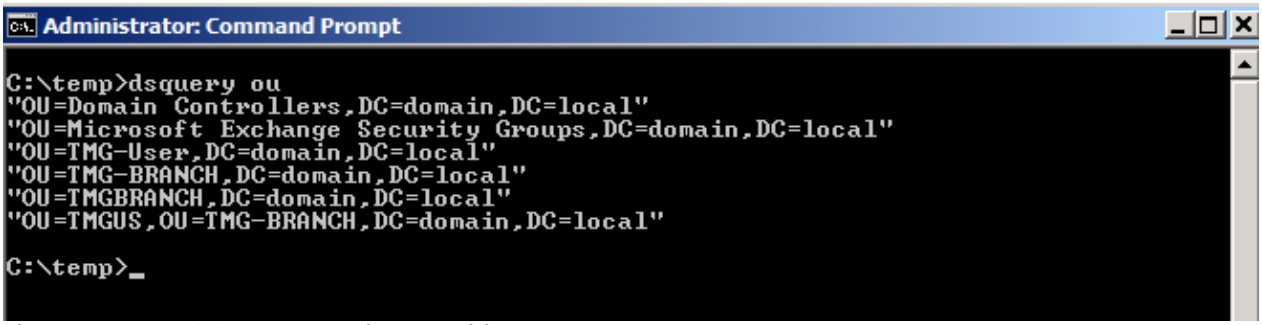

Figure 2: Execute DSQUERY to note the name of the OU

Script

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

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 upper- and 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
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
C=domain,DC=local
dsadd succeeded:CN=SQLServerSQLAgentUser$RODC-TMG$MSFW,OU=TMGUS,OU=TMG-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"
"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
l"

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 sucessfully you will see the new created users and groups in the Active Directory Users and Computers SnapIn.

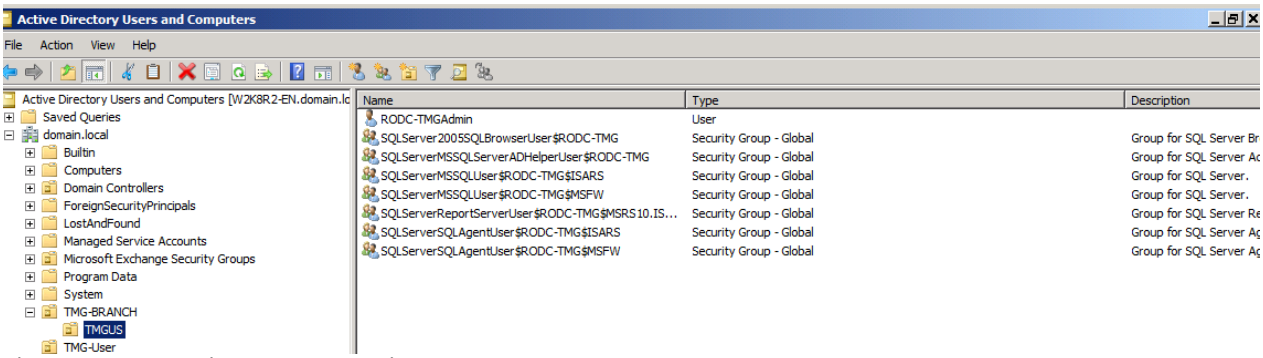

Figure 4: New created user accounts and user groups

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.

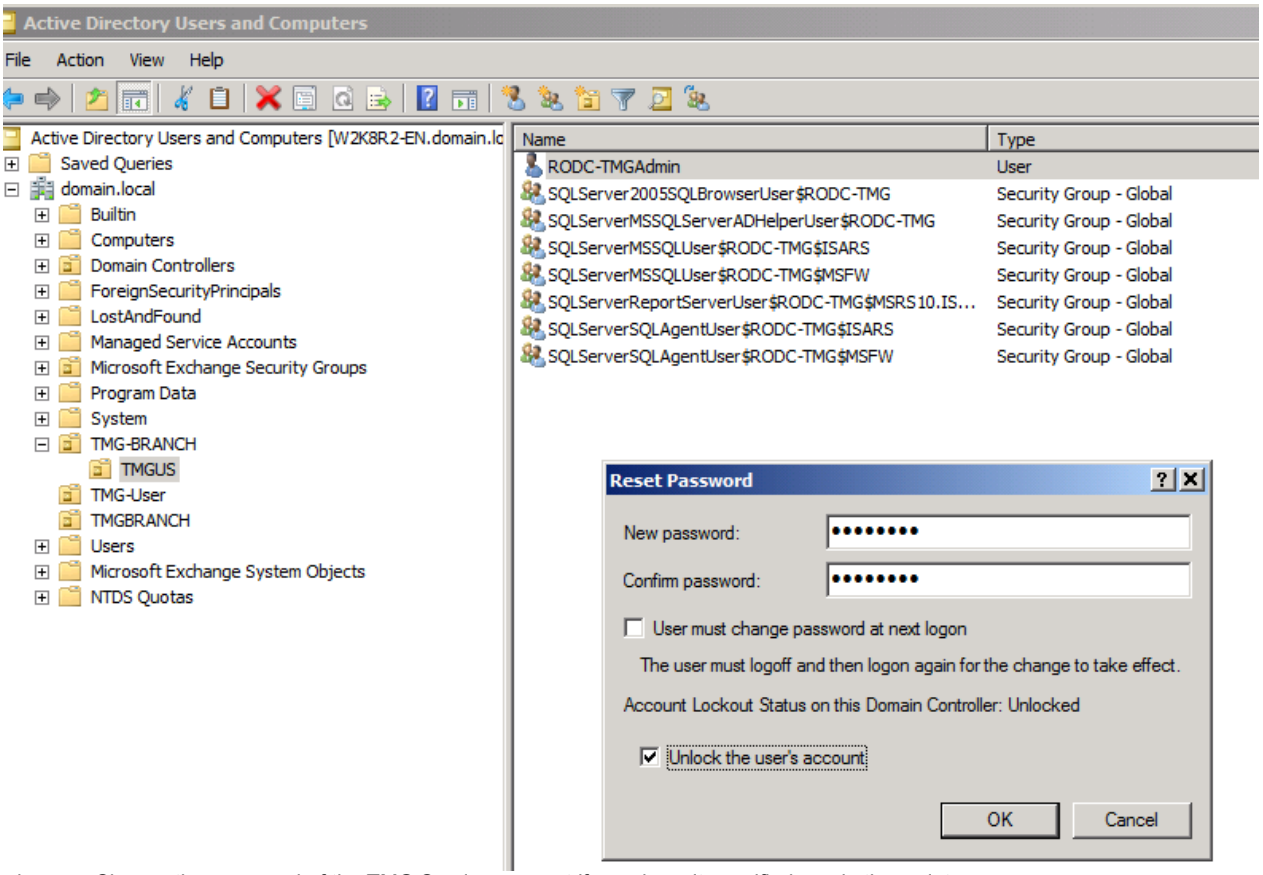

Figure 5: Change the password of the TMG Service account if you doesn't specified one in the script

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.

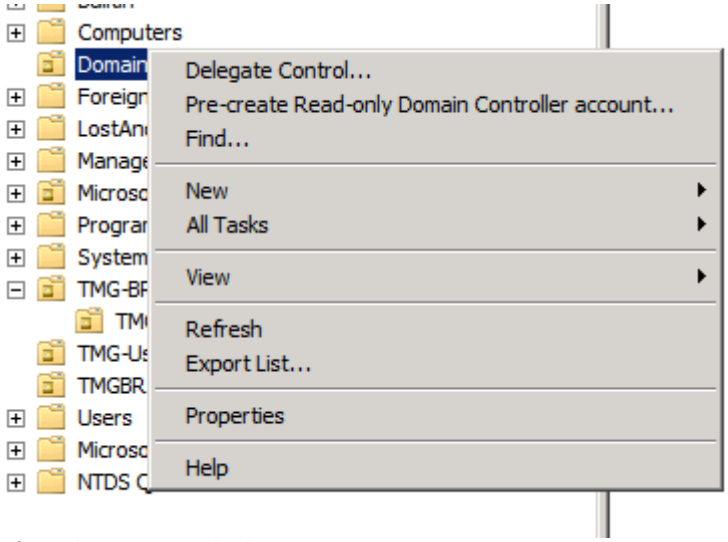

Figure 6: Precreate RODC account

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.

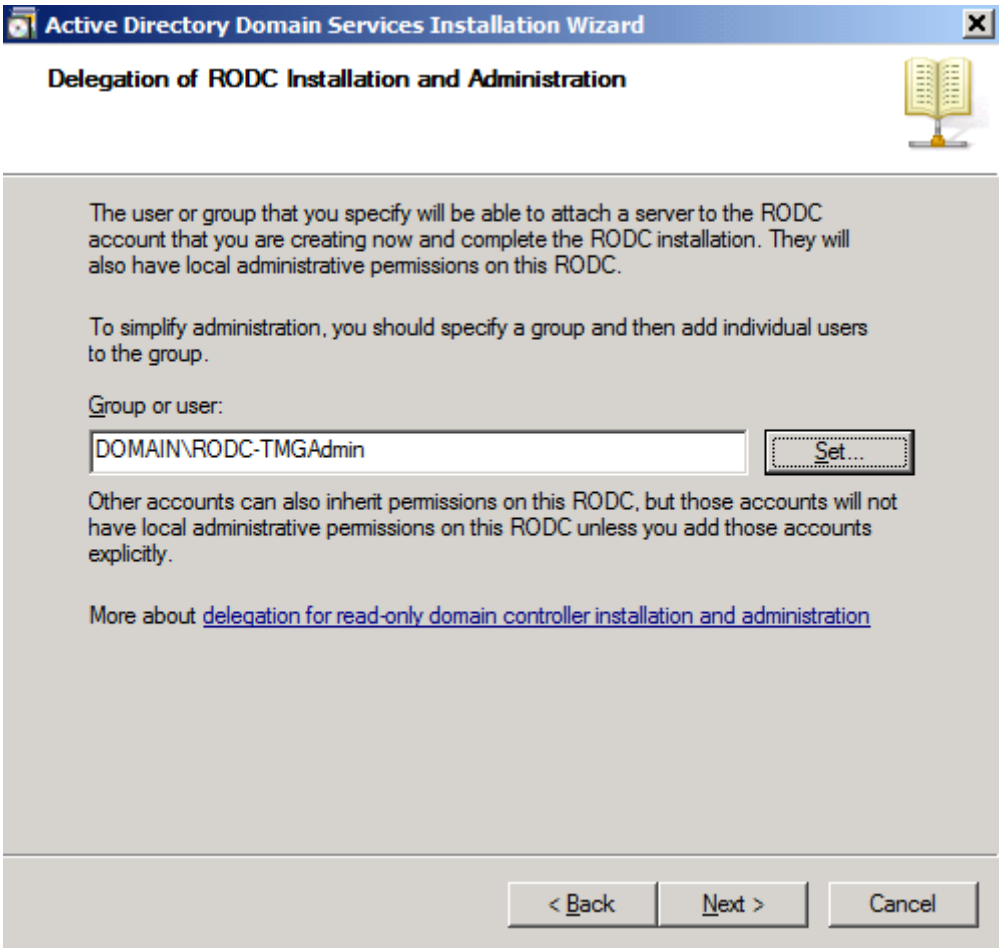

Figure 7: RODC Account from the TMG script

The RODC computer account has been created in Active Diretcory.

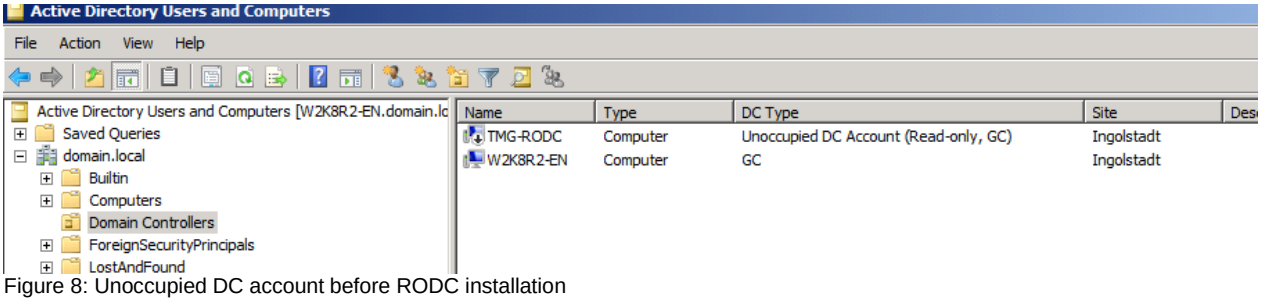

Figure 8: Unoccupied DC account before RODC installation

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.

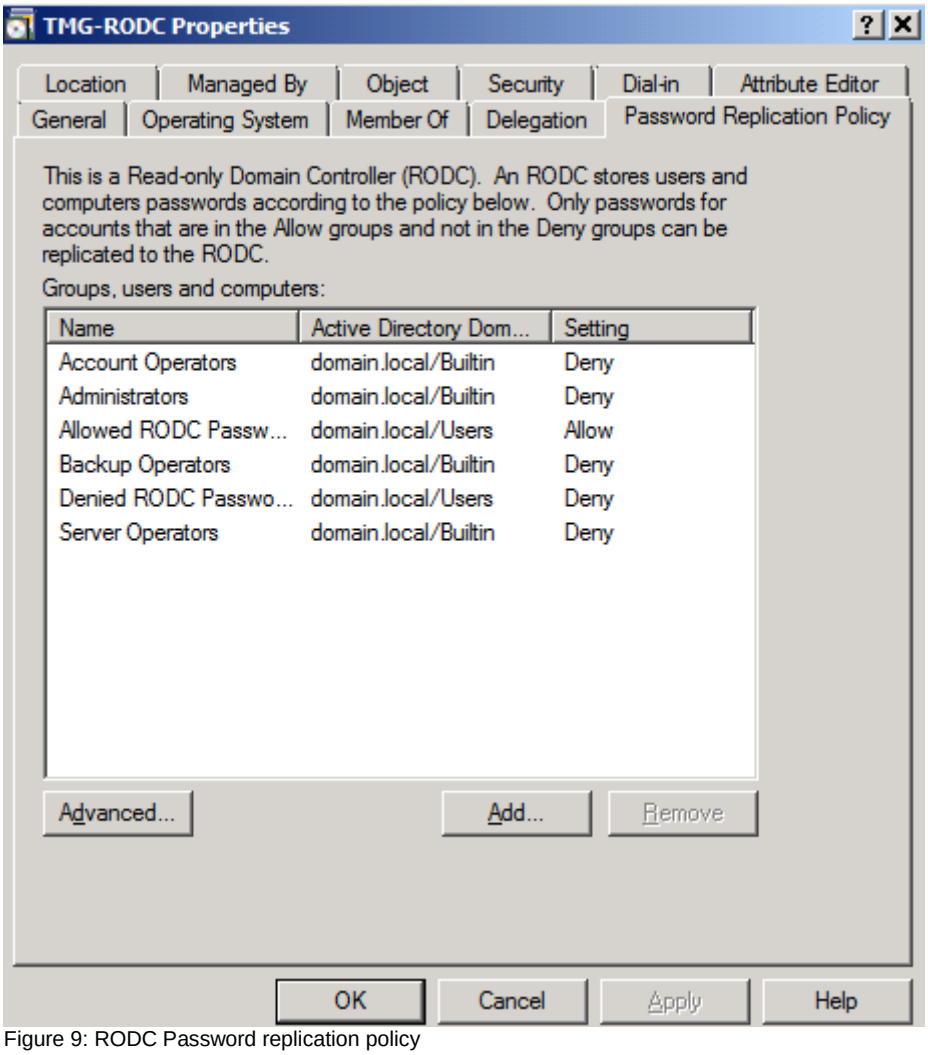

Figure 9: RODC Password replication policy

Allow passwords to replicate to the RODC

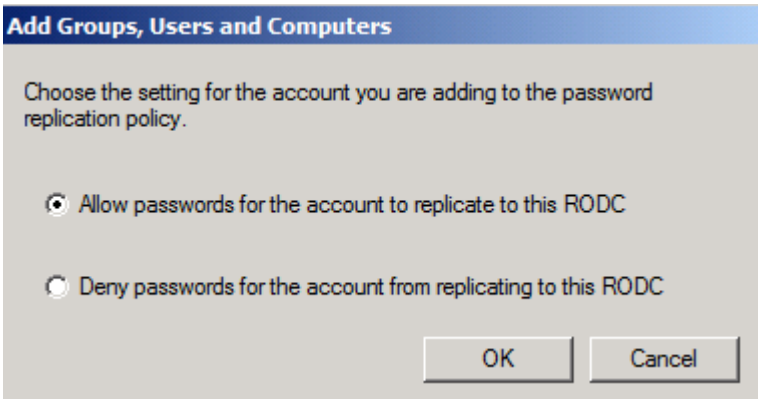

Figure 10: Allow password replication to the RODC for the TMG accounts

Select all accounts and groups created earlier by the script.

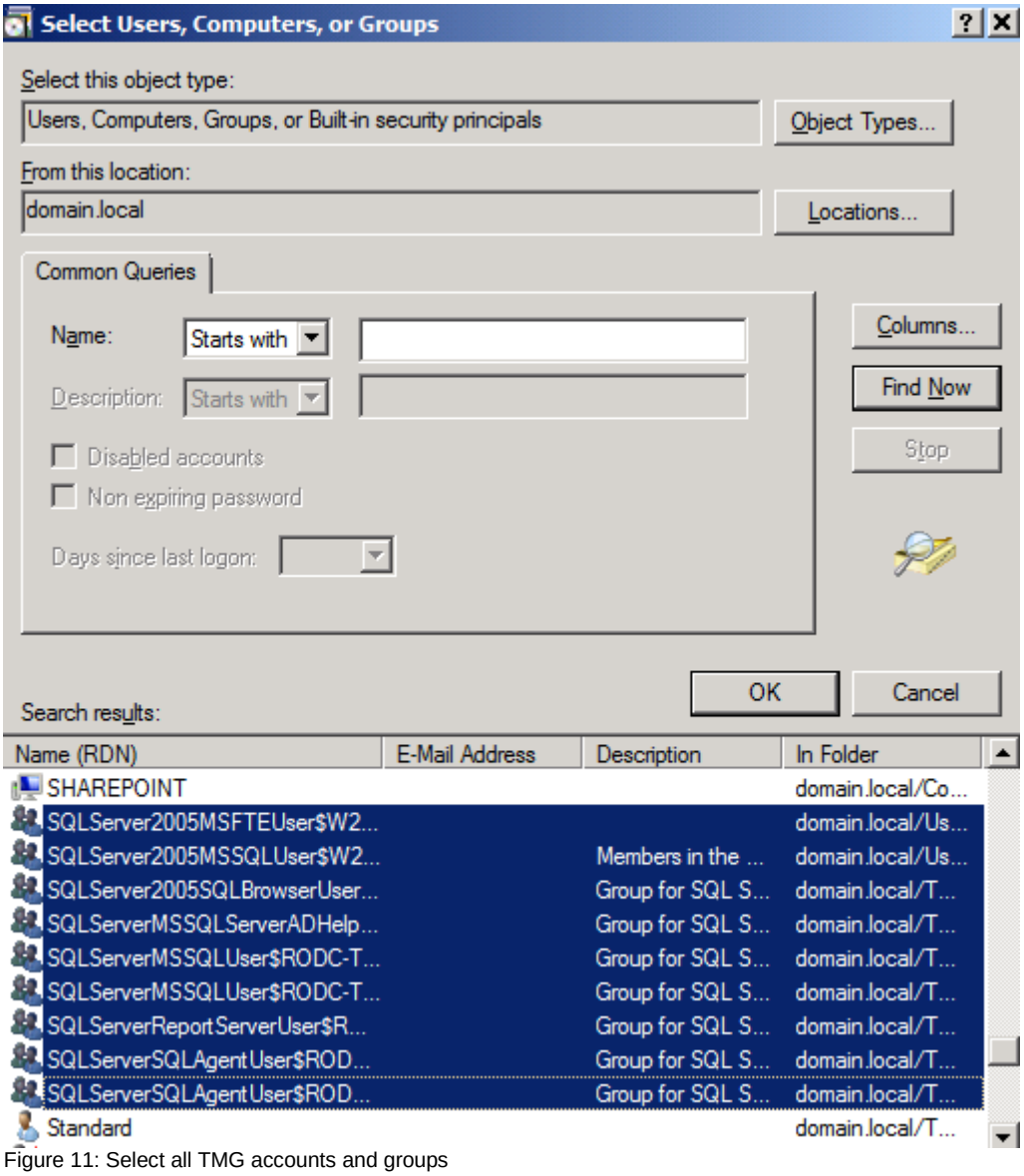

Figure 11: Select all TMG accounts and groups

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.

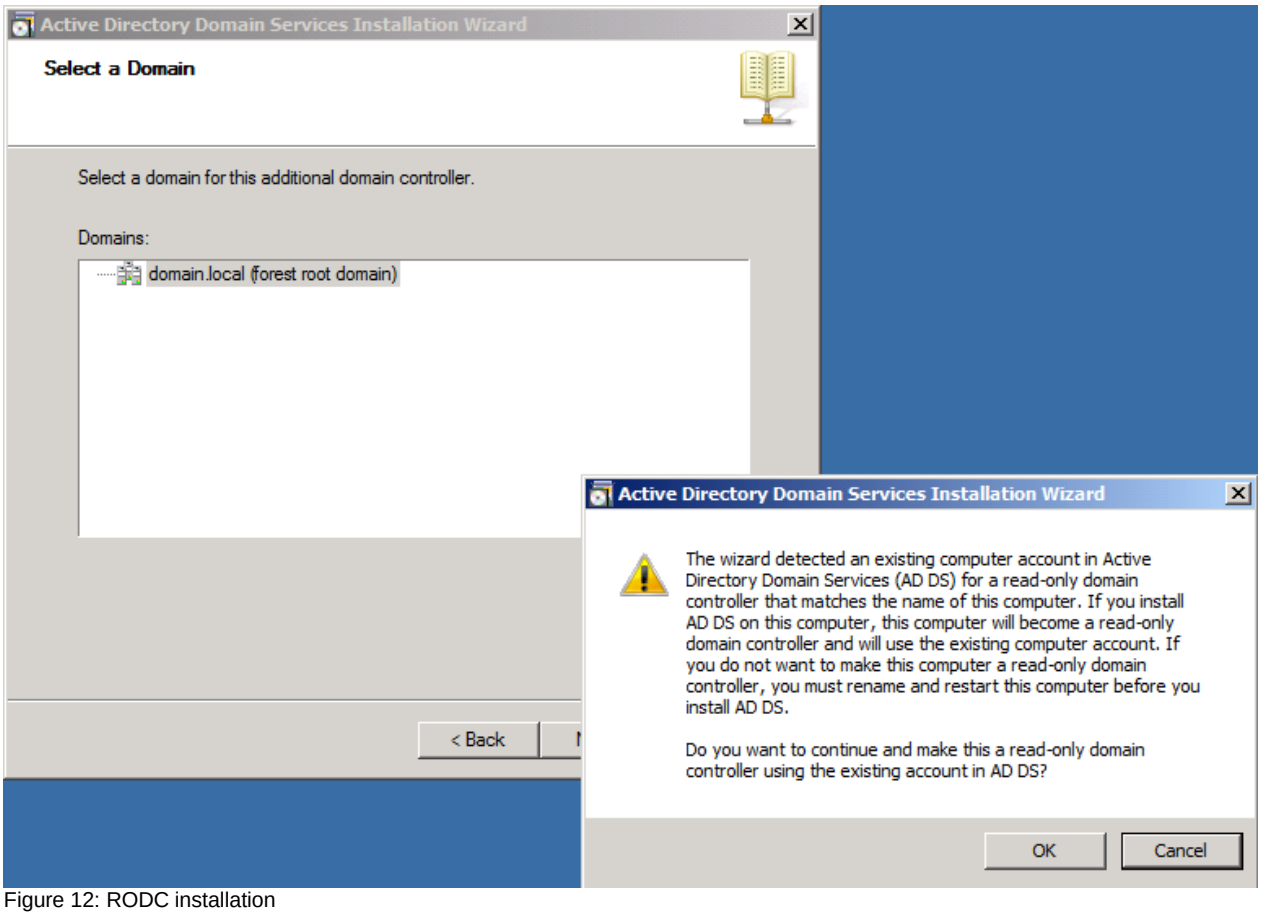

Figure 12: RODC installation

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 -inputpath D:\FPC\PreRequisit
eInstallerFiles\WinRolesInstallSA_Win7.xml -logPath C:\TEMP\TMG-Prerequisites.lo
g

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.

<079/100>
```

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.

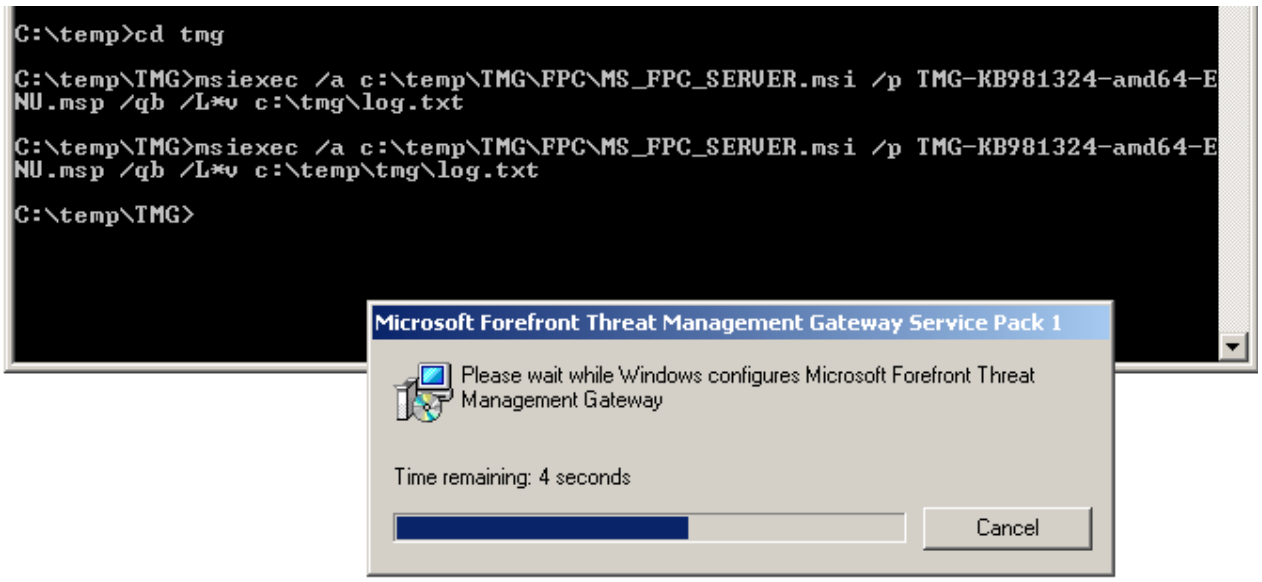

Figure 14: Forefront TMG SP1 Slipstream installation

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