

Un-trusted domain monitoring with



System Center Operations Manager 2007 un-trusted domain monitoring scenario:

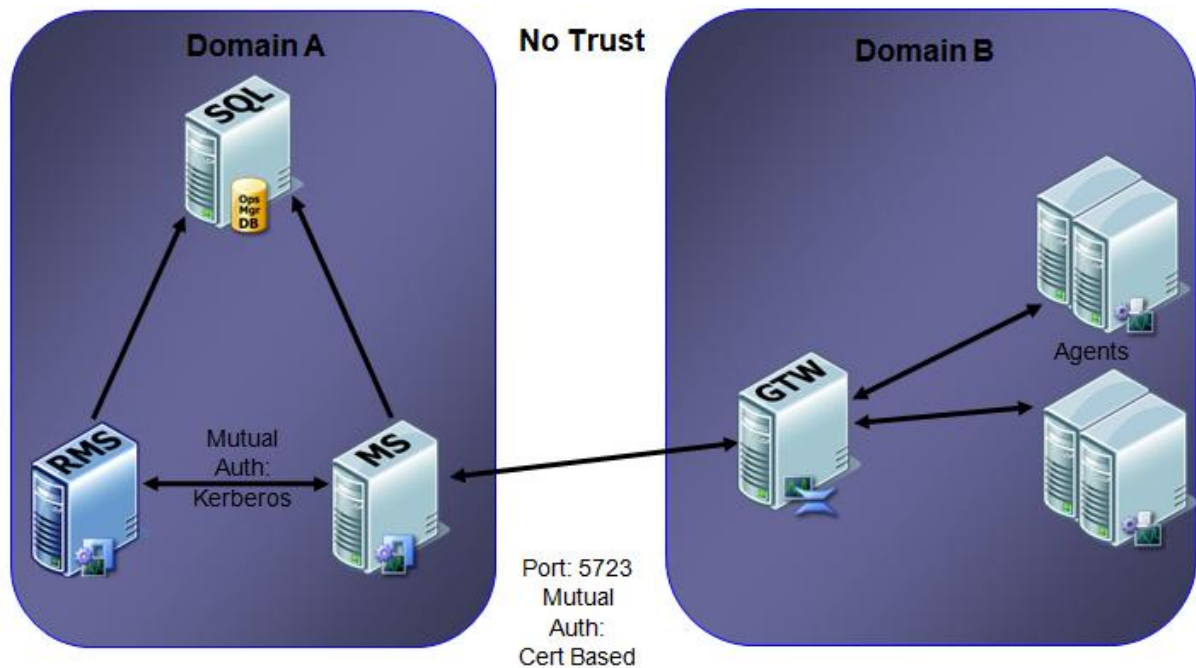
The environment where we are implementing the un-trusted domain monitoring contains the following components: Standalone Root CA and a Root Management server in a Microsoft windows 2003 domain. The un-trusted domain contains a Gateway server which is a member of the un-trusted Microsoft windows 2003 domain.

Information:

System Center Operations Manager 2007 uses mutual authentication to communication with the agents and Gateway server. First an agent or Gateway will try to communicate with Kerberos and when this is not possible, certificates will be used for the secure communication. In System Center Operations Manager 2007 mutual authentication cannot be disabled like in MOM 2005 so if you want to setup a Gateway server in an un-trusted domain the following actions must be taken:

DOCUMENT NAME: Un-trusted domain monitoring with SCOM 2007 Gateway server_v0.1
VERSION: 0.1
Author: Walter Eikenboom

Scenario:



Steps to take:

1. Importing Trusted Root certificate - all servers
2. Creating and installing Server (Client, Server) Certificates - RMS server
3. Creating and installing Server (Client, Server) Certificates – Gateway server
4. Export the Server (Client, Server) Certificate – all servers
5. Running MOMcertimport.exe on the servers - all servers
6. Running the Gateway approval tool – RMS server
7. Running the MOMGateway.msi – Gateway server

Additional steps:

1. Issue new certificates from the Standalone Root CA
2. How to remove a certificate imported with the MOMCertimport tool in System Center Operations Manager 2007.

1. Importing Trusted Root certificate.

For all servers (Root Management Server and Gateway server)

1. Logon to the Root Management Server with administrative privileges and navigate to the certificate server web site with <http://standaloneCAroot.domain.com/cersrv>
2. Click on "Download a CA certificate, certificate chain or CRL"
3. Click on "Download Ca certificate chain"
4. Save the "certnew.p7b" to the "c:\\" (or some place you want)
5. Click start run "MMC" and from the file menu "Add/remove Snap-in.." select
 - a. Click "Add"
 - b. Select "Certificates"
 - c. Click "Add"
 - d. Select "Computer account"
 - e. Click "Next"
 - f. Select "local computer"
 - g. Click "Finish"
6. Click "Close" and "Ok" to access the Certificates console.
7. Navigate to the folder "Trusted Certification Authorities"
8. Right click the "Certificates" folder and select "All Tasks" and "Import"
 - a. In the wizard click "Next"
 - b. Click "Browse" and browse to the "certnew.p7b" on the "c:\\" (or some place you put it)
 - c. Click "Next"
 - d. Select "Place all certificates in the following store" and make sure the Certificate store is "Root Certification Authorities" and click "Next"
 - e. Click "Finish" to complete the import.
9. Delete the "certnew.p7b"
10. The import of the trusted Root certificate is finished

2. Creating and installing Server (Client, Server) Certificates

For the Root Management Server (RMS)

1. Logon to the Root Management Server with administrative privileges and navigate to the certificate CA server web site with <http://standaloneCAroot.domain.com/cersrv>
2. Click "Request a certificate"
3. Click "advanced certificate request"
4. Click "Create and submit a request to this CA"
5. Use the following for the certification request:
 - a. Name: **Managementserver.domain.com**
 - b. Type: Other
 - c. OID: 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2
 - d. Select: Mark key as exportable
 - e. Select: Store certificate in the local computer certificate store
 - f. Friendly name: **Managementserver.domain.com**
 - g. Click "Submit"
 - h. Close Internet explorer
6. Let the certificate be issued on the Standalone Root CA (see how to: [1. Issue new certificates from the Standalone Root CA](#)).
7. Navigate to <http://standaloneCAroot/cersrv>
8. Click "View status of a pending certificate request"
9. Click the Issued certificate
10. Install the issued certificate

3. Creating an installing Server (Client, Server) Certificates

For the Gateway server.

1. Logon to the Gateway server with administrative privileges and navigate to the certificate CA server web site with <http://standaloneCAroot.domain.com/certsrv>
2. Click "Request a certificate"
3. Click "advanced certificate request"
4. Click "Create and submit a request to this CA"
5. Use the following for the certification request:
 - a. Name: **Servname.untrusteddomain.com**
 - b. Type: Other
 - c. OID: 1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2
 - d. Select: Mark key as exportable
 - e. Select: Store certificate in the local computer certificate store
 - f. Friendly name: **Servname.untrusteddomain.com**
6. Let the certificate be issued on the Standalone Root CA (see how to: [1. Issue new certificates from the Standalone Root CA](#)).
7. Navigate to <http://standaloneCAroot.domain.com/cersrv>
8. Click "View status of a pending certificate request"
9. Click the Issued certificate
10. Install the issued certificate

4. Export the Server (Client, Server) Certificate

This must be done on the Gateway server and the Root Management Server (RMS).

1. Logon to the Server with administrative privileges
2. Click "Start => Run" "MMC" and from the file menu "Add/remove Snap-in.." select
 - a. Click "Add"
 - b. Select "Certificates"
 - c. Click "Add"
 - d. Select "Computer account"
 - e. Click "Next"
 - f. Select "local computer"
 - g. Click "Finish"
3. Click "Close" and "Ok" to access the Certificates console.
4. Navigate to the folder "Certificates (Local Computer)\personal\Certificates"
5. Select the new installed Client,Server certificate and right click "All tasks => Export"
 - a. In the new wizard click "Next"
 - b. Select "Yes, Export the private key"
 - c. Click "Next"
 - d. Select "Personal Information Exchange – PKCS #12 Certificates (PFX)"
 - e. Select "Enable Strong protection (requires IE5.0, NT4 SP4 or above)"
 - f. Click "Next"
 - g. Type a password for the certificate twice and click "Next"
 - h. Select "Browse" c:\serverFQDN.pfx"
 - i. Click "Next"
 - j. Check the export information and if correct click "Finish"
 - k. Click "OK" to finish the export

5. Running MOMcertimport.exe on the servers.

This must be done on all servers.

1. Copy the MOMcertimport.exe from the installation source "\SupportTools\i386" to a local directory.
2. On the start menu click "Start" and "Run"
3. Type "cmd"
4. Navigate to > cd "local directory"
5. Type >MOMcertimport.exe "c:\servername.domain.com.pfx" or "c:\servername.pfx"
6. Type the asked password for the certificate import and press "Enter".
7. The certificate is now imported in OpsMgr 2007.
8. Restart the "OpsMgr Health Service" on the server.

6. Running Gateway approval tool on the RMS servers.

On the Root Management Server (RMS).

1. Logon to the Server with administrative privileges.
2. Copy the Microsoft.EnterpriseManagement.GatewayApprovalTool.exe file from the installation source SupportTools into the installation folder for Operations Manager "Program Files\System Center Operations Manager 2007".
3. On the start menu click "Start" and "Run"
4. Type "cmd"
5. Navigate to > cd "program files\System Center Operations Manager 2007"
11. Type > Microsoft.EnterpriseManagement.GatewayApprovalTool /ManagementServerName=**Managementserver.domain.com**
6. /GatewayName=**Servername.untrusteddomain.com**
7. Press ENTER.

7. Running MOMGateway.msi on the Gateway server.

Before installing the Gateway server there must be a Gateway Action Account in the un-trusted domain. The account needs to have agent installation rights in the un-trusted domain to work fully functional from the Root Management Server into the un-trusted domain.

On the Gateway server.

1. Logon to the Server with administrative privileges.
2. On the Operations Manager 2007 installation media, open the \gateway\i386 folder, and then double-click the MOMGateway.msi file.
3. On the Welcome page, click "Next".
4. On the Destination Folder page leave the installation folder set to the default click "Next".
5. On the Management Group Configuration page, do the following:
 - a. Type the Management Group Name
 - b. Type the Management Server name.
 - c. Leave the management server port default: 5273.
 - d. Click Next.
6. When the Gateway Action Account page displays enter the Gateway Action Account name and password and click Next.
7. On the Ready to Install page, review the installation settings, and then click Install.
8. On the Completing the System Center Operations Manager Gateway Setup wizard page, click Finish.

After the installing the Gateway server, the Gateway Action Account is automatically placed in the "Run as accounts" under Action Account and placed in the "Run as Profiles" Default Action Account for the Gateway server.

In the operations console the monitored server will show up with OS and health discovery so the rules are running and OpsMgr is monitoring the server. Take a look in Device management, Management servers there should be Gateway server be present.

Additional steps

1. Issue new certificates from the Standalone Root CA

1. Logon to the Standalone Root CA
2. Open the Certification authority in "Administrative Tools"
3. Navigate to "Pending requests"
4. Right click the new certificate and select "all tasks" and "Issue"
5. Repeat this for all new requested certificates (RMS, MS and workgroup servers)

2. How to remove a certificate imported with the MOMCertimport tool in System Center Operations Manager 2007.

1. Logon to the Server with administrative privileges.
2. On the start menu click "Start" and "Run"
3. Type "regedit"
4. On the Registry editor expand "HKEY_LOCAL_MACHINE => SOFTWARE => Microsoft => Microsoft Operation Manager => 3.0 => Machine Settings".
5. Right-click "**ChannelCertificateSerialNumber**" and click modify.
6. In the **Edit Binary Value** dialog box, select the binary data, and click **Delete**

Thanks to

Stefan Stranger (MOM MVP) for reviewing the un-trusted domain server monitoring guide.