

## DMZ Server monitoring with



### **System Center Operations Manager 2007 DMZ server monitoring scenario:**

The environments where this guide will be helpful can contain the following components:

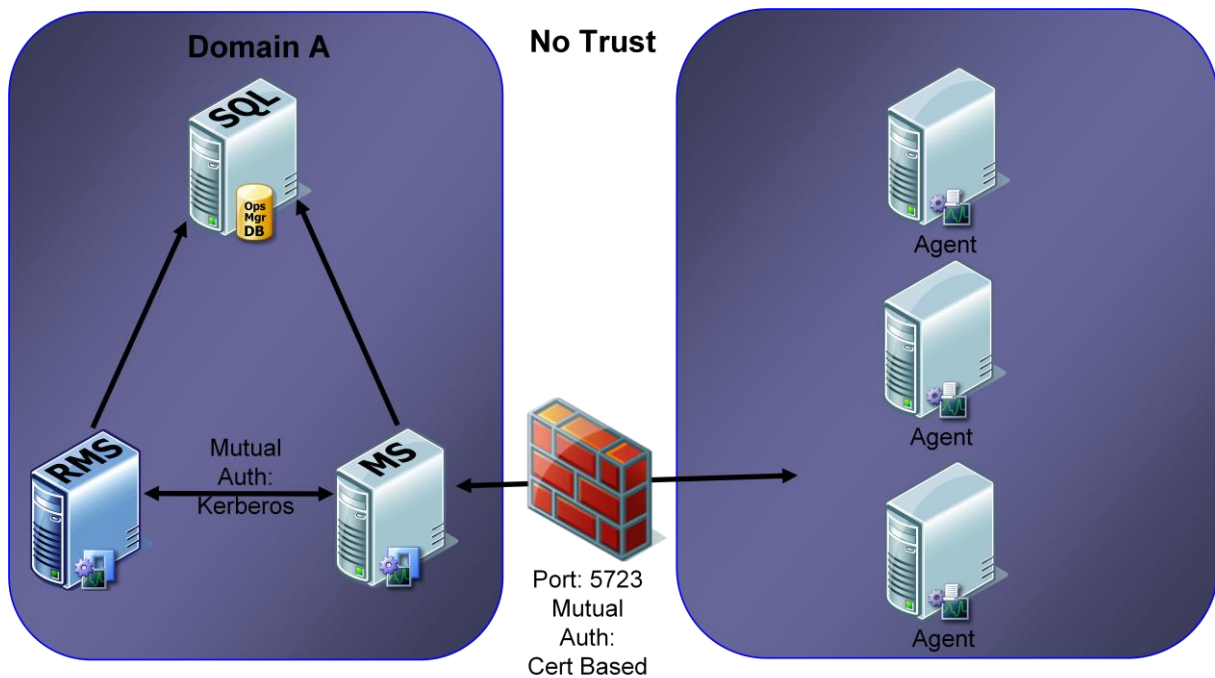
- Standalone Root CA and a Root Management both running Windows 2003 Server in a Microsoft Windows 2003 domain. The DMZ server is a Microsoft Windows 2003 workgroup server.
- Enterprise Root CA and a Root Management server both running Windows server 2008 Enterprise edition. The DMZ server is a Microsoft Windows Server 2008 workgroup server. Hot fixes (<http://weblogwally.spaces.live.com/blog/cns!A913F865098E0556!419.entry>) for server 2008 must be installed on all 2008 servers!

#### **Information:**

System Center Operations Manager 2007 uses mutual authentication to communication with the agents. First the agent 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 monitor a DMZ server or Workgroup server the following actions must be taken.

**DOCUMENT NAME:** DMZ Server Monitoring with System Center Operations Manager 2007  
**VERSION:** 0.3  
**Author:** Walter Eikenboom  
**Published:** <http://weblogwally.spaces.live.com>

**Scenario:**



**Steps to take:**

1. Importing Trusted Root certificate - all servers
2. Creating and installing Server (Client, Server) Certificates - OpsMgr servers
  1. For Windows 2003 Standalone Root CA
  2. For Windows Server 2008 Enterprise Root CA
3. Creating and installing Server (Client, Server) Certificates – Workgroup and/or DMZ servers
  1. For Windows 2003 Standalone Root CA
  2. For Windows Server 2008 Enterprise Root CA
4. Export the Server (Client, Server) Certificate
  1. For Windows 2003 Standalone Root CA
  2. For Windows Server 2008 Enterprise Root CA
5. Allow manual agent installation.
6. Manual OpsMgr 2007 agent installation
7. Running MOMcertimport on the servers - all servers
8. Approve agent
9. Create Run As Account
10. Change default Action Account Run As profile

**Additional steps:**

1. Issue new certificates from the Standalone Root CA
2. Add SCOM Gateway Client Server certificate template to web enrolment Certificate templates

## 1. Importing Trusted Root certificate.

On all servers (RMS, Management server and all Workgroup servers)

1. Logon to the Server(s) with administrative privileges and navigate to the certificate server web site with <http://standaloneCAroot.domain.com/cersrv> for the stand alone root CA or <https://enterpriseCAroot.domain.com/certsrv> for the Enterprise root CA.
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 Root 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

On the Root Management Server (RMS) and management server (MS)

### 2.1 For Windows 2003 Standalone Root CA

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

2.2 For Windows Server 2008 Enterprise Root CA

1. Logon to the Root Management Server with administrative privileges and navigate to the certificate CA server web site with <https://enterpriseCAroot.domain.com/cersrv>
2. Click "Continue to this website(not recommended)"
3. Logon with the required permission.
4. In the top bar accept and install the Certificate enrolment ActiveX plugin.
5. "Request a certificate"
6. Click "advanced certificate request"
7. Click "Create and submit a request to this CA"
8. Use the following for the certification request:
  - a. Certificate Template: SCOM Gateway Client Server Template
  - b. Name: **Managementserver.domain.com**
  - c. Select: Mark key as exportable
  - d. Friendly name: **Managementserver.domain.com**
  - e. Click "Submit"
  - f. Accept the Web Access Confirmation
  - g. Click "Install this Certificate"
  - h. Accept the Web Access Confirmation
  - i. Close Internet explorer
9. 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"
  - h. Click "Add"
  - i. Select "Certificates"
  - j. Select "My user account"
  - k. Click "Finish"
10. Click "Ok" to access the Certificates console.
11. Navigate to "Certificates - Current User" "Personal" "Certificates" store.
12. Right click the **Managementserver.domain.com** certificate select "All Tasks" and "Export"
  - a. In the wizard click "Next"
  - b. Select "Yes, export the private key"
  - c. Leave everything default and click "Next"
  - d. Give in a password two times and click "Next"
  - e. Select a location and filename to export the certificate to (C:\Managementserver.domain.com).
  - f. Click "Next" and click "Finish to export the certificate.
13. Navigate to the "Certificates – local computer" "Personal" store.
14. Right click the "Personal" folder and select "All Tasks" and "Import"
  - a. In the wizard click "Next"
  - b. Click "Browse" and change file extension to "\*. \* All files"
  - c. Browse to the "Managementserver.domain.com.pfx" on the "c:\\" (or where you exported the certificate to)
  - d. Click "Next"
  - e. Enter the Password defined under 12.d and click "Next"
  - f. Leave default and click "Next"
  - g. Click "Finish" to complete the import.
15. **Don't** delete the exported "Managementserver.domain.com.pfx" you will need it again.

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

On the workgroup and/or DMZ server.

3.1 For Windows 2003 Standalone Root CA

1. Logon to the DMZ/Workgroup 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: **Servername**
  - 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: **Servername**
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

### 3.2 For Windows Server 2008 Enterprise Root CA

1. Logon to the DMZ/Workgroup server with administrative privileges and navigate to the certificate CA server web site with <https://enterpriseCAroot.domain.com/cersrv>
2. Click "Continue to this website(not recommended)"
3. Logon with the required permission.
4. "Request a certificate"
5. Click "advanced certificate request"
6. Click "Create and submit a request to this CA"
7. In the top bar accept and install the Certificate enrolment ActiveX plugin.
8. Use the following for the certification request:
  - a. Certificate Template: SCOM Gateway Client Server Template
  - b. Name: **Servername**
  - c. Select: Mark key as exportable
  - d. Friendly name: **Servername**
  - e. Click "Submit"
  - f. Accept the Web Access Confirmation
  - g. Click "Install this Certificate"
  - h. Accept the Web Access Confirmation
  - i. Close Internet explorer
9. 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"
  - h. Click "Add"
  - i. Select "Certificates"
  - j. Select "My user account"
  - k. Click "Finish"
10. Click "Ok" to access the Certificates console.
11. Navigate to "Certificates - Current User" "Personal" "Certificates" store.
12. Right click the **Servername** certificate select "All Tasks" and "Export"
  - a. In the wizard click "Next"
  - b. Select "Yes, export the private key"
  - c. Leave everything default and click "Next"

- d. Give in a password two times and click "Next"
  - e. Select a location and filename to export the certificate to (C:\Servername.untrusteddomain.com).
  - f. Click "Next" and click "Finish" to export the certificate.
13. Navigate to the "Certificates – local computer" "Personal" store.
14. Right click the "Personal" folder and select "All Tasks" and "Import"
- a. In the wizard click "Next"
  - b. Click "Browse" and change file extension to "\*. \* All files"
  - c. Browse to the "**Servername.pfx**" on the "c:\" (or where you exported the certificate to)
  - d. Click "Next"
  - e. Enter the Password defined under 12.d and click "Next"
  - f. Leave default and click "Next"
  - g. Click "Finish" to complete the import.
15. **Don't** delete the exported "**Servername.pfx**" you will need it again.

## 4. Export the Server (Client, Server) Certificate

This must be done on all Workgroup/DMZ servers, root management server(RMS) and management server(MS).

### 4.1 For Windows 2003 Standalone Root CA

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

### 4.2 For Windows Server 2008 Enterprise Root CA

No actions required

## 5. Allow manual agent installation.

Before the first manual agent installation, the global setting must be changed from **reject** to "Review new manual agent installation in pending management view" in the operations console of OpsMgr 2007.

1. Open a Operations Console with OpsMgr administrative privileges
2. Navigate to "Administration => Settings => Server"
3. In the right pane click "Security"

4. On the "General" tab select "Review new manual agent installation in pending management view"
5. and Click "OK" to finish

## 6. Manual OpsMgr 2007 agent installation

On the workgroup and/or DMZ servers.

1. Logon to the Server with administrative privileges
2. On the Operations Manager 2007 installation media, double-click the SetupOM.exe file.
3. On the Start page, select Install Operations Manager 2007 Agent.
4. On the Welcome page, click "Next".
5. On the Destination Folder page leave the installation folder set to the default click "Next".
6. On the Management Group Configuration page leave the Specify Management Group information check box selected, and then click "Next".
7. On the Management Group Configuration page, do the following:
  - a. Type the Management Group Name
  - b. Type the Management Server name.
  - c. Leave the default 5273.
  - d. Click Next.
8. When the Agent Action Account page displays leave it set to the default of Local System and then click Next.
9. On the Ready to Install page, review the settings and then click Install to display the Installing Systems Center Operations Manager Agent page.
10. When the Completing the Systems Center Operations Manager Agent Setup Wizard page displays, click Finish.

## 7. Running MOMcertimport.exe on the servers.

This must be done on all servers

1. On the start menu Click "Start" and "Run"
2. Type "cmd"
3. Navigate to > cd "program files\System Center Operations Manager 2007\Supportools\i386"
4. Type >MOMcertimport.exe "c:\servername.domain.com.pfx" or "c:\servername.pfx"
5. Type the asked password for the certificate import and press "Enter".
6. The certificate is now imported in OpsMgr 2007.
7. Restart the "OpsMgr Health Service" on the server.

## 8. Approve agent

In the System Center Operations Manager Console.

After every manual agent installation the new agent must be approved in the operations Console of OpsMgr 2007.

1. Open the Operations console as an OpsMgr Admin member.
2. Navigate to "Administration => Pending Management"
3. Right-click "Approve"
4. Click "Approve"

To check if the agent is successfully approved look in the "Agent Managed" folder for the approved agent to see if the agent is there.

## 9. Create Run As Account

In the System Center Operations Manager Console.

1. Open a Operations Console with OpsMgr administrative privileges
2. Navigate to "Administration => Security => Run As Account"
3. Right-click "Run As Account" and select create run as account
4. In the Create Run As Account Wizard click "Next".
5. Select "Action account" in the Run As Account type list
6. Type a display name in the Display Name text box
7. Click Next
8. On the Account page, type:
  - a. Servername\username
  - b. password
  - c. The domain should be greyed out (Local machine account).
9. Click Create to finish

## 10. Change default Action Account Run As profile

In the System Center Operations Manager Console.

1. Open a Operations Console with OpsMgr administrative privileges
2. Navigate to "Administration => Security => Run As Profiles"
3. In the right pane double click the "Default Action Account"
4. Click on the "Run As Account" tab
5. Select "Run As Account: "dropdown menu and select the workgroup server local account
6. Click "OK" and click "OK"

In the operations console the monitored servers will show up with OS and health discovery so the rules are running and OpsMgr is monitoring the server.

## 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. Add SCOM Gateway Client Server certificate template to web enrolment.

1. Logon to the Enterprise Root CA
2. Open the Certification authority in "Administrative Tools"
3. Navigate to the Certificate Templates folder.
4. Right click the Certificate Templates folder
5. Click "New"=>"Certificate Template to issue"
6. Select the "SCOM Gateway Client Server Certificate" and click OK
7. The "SCOM Gateway Client Server Template" will now be available in the "Certificate templates" folder and will be available when requesting a certificate by using the web enrolment page.

## Thanks to

Stefan Stranger (former MOM MVP) for reviewing the v0.1 DMZ Server monitoring guide.