System-Center-Team Microsoft

02-16-2019 01:

Monitoring OpsMgr workgroup clients - Part 1: Installing and configuring the Root CA

First published on TECHNET on May 18, 2015
~ Irfan Rabbani | Senior Support Escalation Engineer

This article is the first in a series of posts on how to monitor System Center 2012 R2 Operations Manager clients that are not members of your Active Directory domain. The series will be broken out into three parts:

Part 1: Installing the Microsoft Certificate Authority Server for Operations Manager certificate based authentication

Part 2: Installing certificates and final configuration

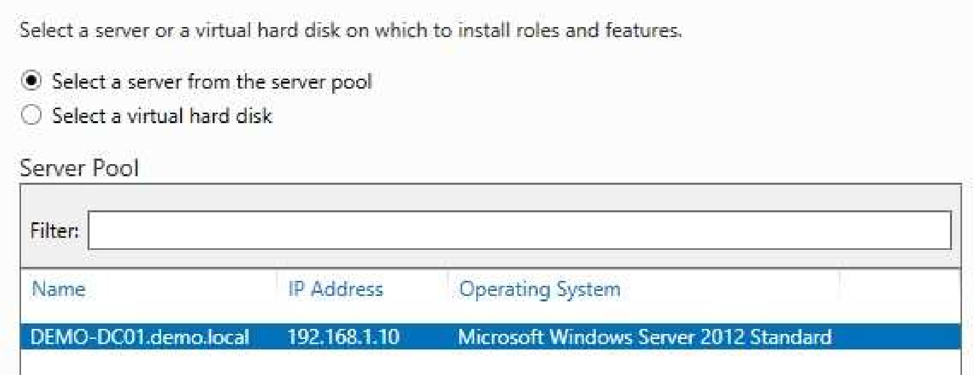
Part 3: Installing and configuring a gateway

To begin part 1, we first need to look at how clients outside the domain will authenticate to our Operations Manager infrastructure. System Center Operations Manager 2007 & System Center 2012 Operations Manager use 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. If you happen to have agents that lie outside of your domain, such as in a DMZ, you'll need to use certificates for agent to server communication.

If you already have an Enterprise Root CA then you may not need to install a new one, however be sure to check out the second part below where we configure the certificate template and make it available to clients.

Step 1: Install the Active Directory Certification Authority Role

1. Open *Server Manager* , then click **Add Roles and Features** . Click **Next** , then click **Active Directory Certificate Services** . Click **Next** two times to get to the screen below. Here you will select the server where you want to install the role. Once selected, click Next.



Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

Filter:

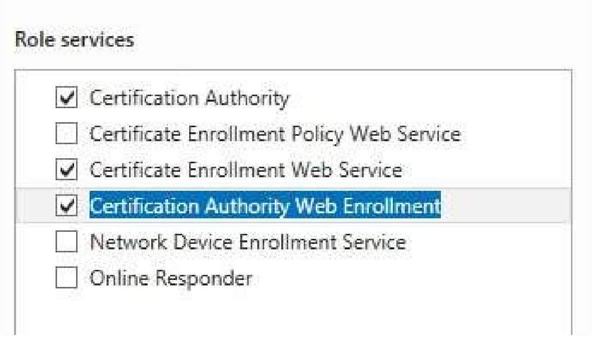
Name	IP Address	Operating System
DEMO-DC01.demo.local	192.168.1.10	Microsoft Windows Server 2012 Standard

2. On the *Select Role Services* page, click **Active Directory Certification Authority** . Click **Next** three times.

3. Choose the following Features:

- Certificate Authority
- Certificate Enrollment Web Service
- Certificate Authority Web Enrollment

Click **Next** three times.



Role services

☑ Certification Authority
□ Certificate Enrollment Policy Web Service
☑ Certificate Enrollment Web Service
☑ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

4. On the last page, check settings and choose Install.

After the installation finishes, restart the computer.

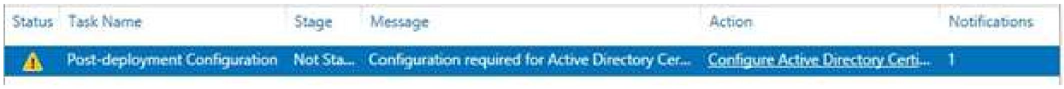
Step 2: Configure the Root CA

Once the Active Directory Certification Authority role is installed, we need to configure it.

1. Open *Server Manager* and click **AD CS**

2. On the *Configuration Required for AD Certificate Services* page, choose **More** .

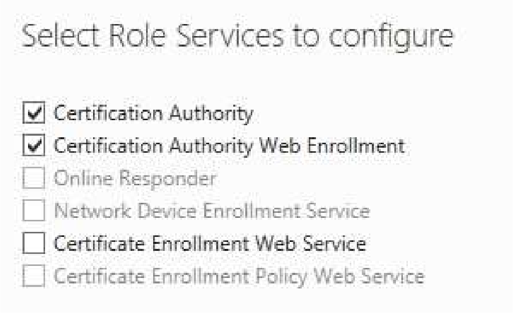
3. Choose *Configure Active Directory Certificate Service* on the destination server:



Status	Task Name	Stage	Message	Action	Notifications
⚠	Post-deployment Configuration	Not Sta...	Configuration required for Active Directory Cer...	Configure Active Directory Certi...	1

4. Check the credentials and click **Next**

5. Select **Certificate Authority** and **Certification Authority Web Enrollment** and click **Next** (we will cover the web enrollment later).



Select Role Services to configure

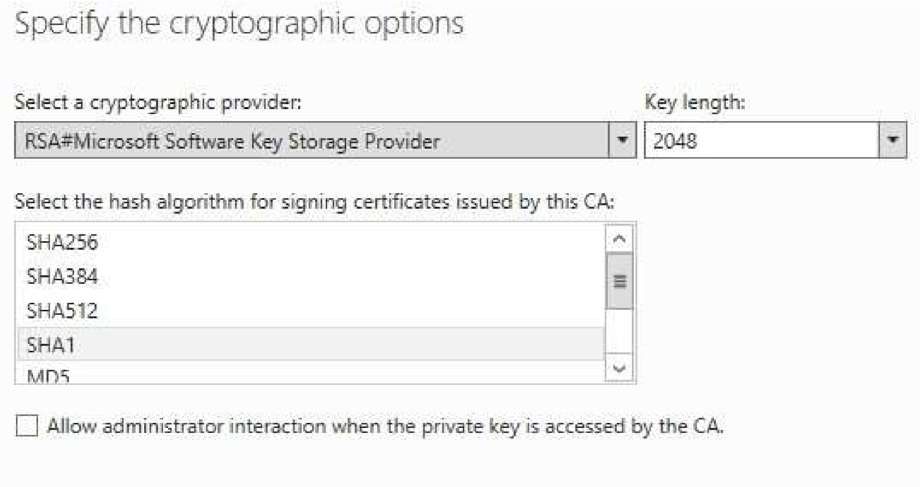
☑ Certification Authority
☑ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

6. Choose **Enterprise Root CA** , click **Next.**

7. On the *CA Type* section choose **Root CA** and click **Next.**

8. Choose **Create a new private key** and click **Next.**

9. Specify the Certificate Server Cryptographic options (we left them with the default values) and click **Next.**



Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

10. Fill in the Common name for this CA. I suggest you use a logical name (we used Enterprise-CA). Click **Next.**

11. Choose the *Validity Period* and choose **Next** two times (we left it default).

12. Check the *Confirmation* page and choose **Configure.**

13. For "Do you want to configure additional Role Services" choose **Yes.**

14. Choose **Next** and now choose the **Certificate Enrollment Web Service.**

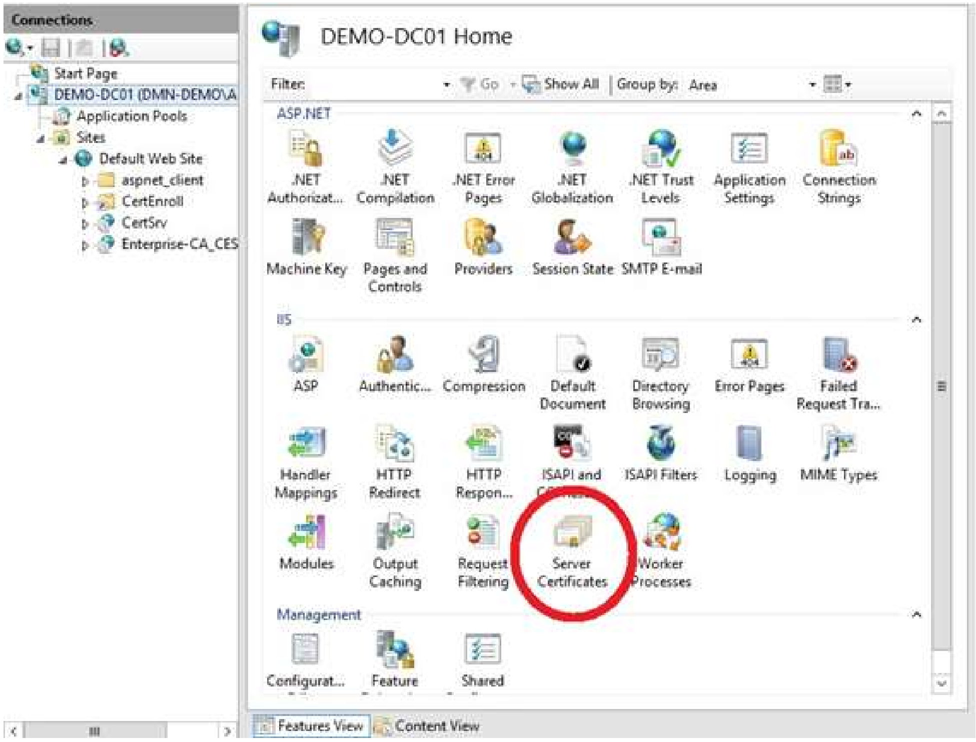
15. Click **Next** three times and on the *Specify the Service account* section, choose the service user that is a member of the IIS_IUSRS group (this group is in the Active Directory) and choose **Next.**

16. Select the **Enterprise CA** and click **Next.**

17. Check the *Confirmatio* n page and choose **Configure.**

At this point we are done installing the Enterprise Root CA. Now we are going to make the certificate site secure because it's necessary for web enrolment.

18. Click on **Server Certificates** , **Create self-signed certificate.**



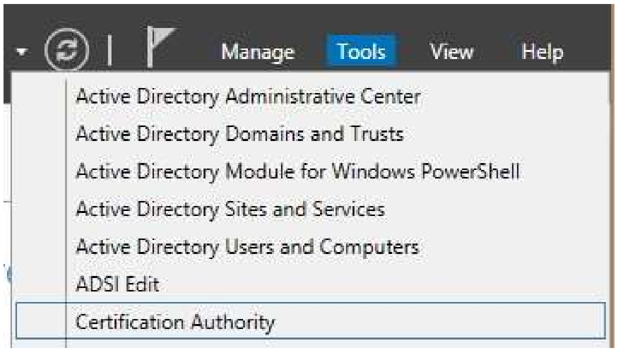
19. Give it a friendly name (in our case we used **CA1-Dc1**) and click **OK.**

Step 3: Create the Operations Manager Certificate Template

This section explains how to make an OpsMgr 2012 R2 certificate template in Windows Server 2012.

NOTE *In my Lab I installed the Root CA on the Domain Controller.*

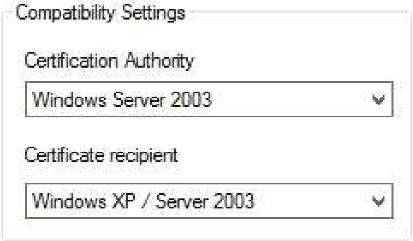
1. Open Server Manager, click **Tools** and click **Certificate Authority.**


Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Certification Authority

2. Select the Enterprise CA, right-click **Certificate Templates** , then right-click **Manage** .

3. Right-click on **IPSec (Offline request)** and select **Duplicate Template.**

4. Leave the default to Windows Server 2003 and Windows XP/ Server 2003. This way we are always backwards compatible.



Compatibility Settings

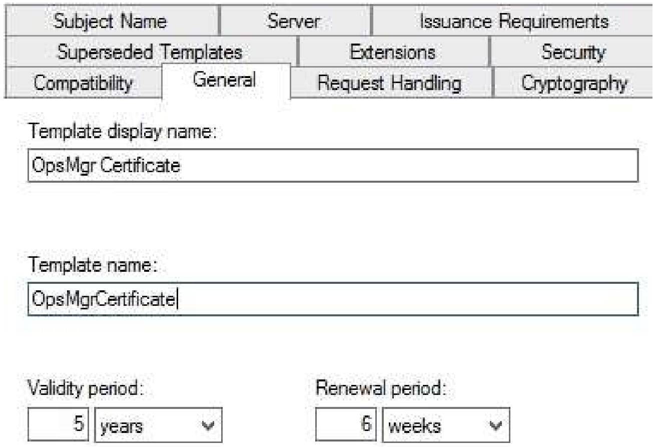
Certification Authority

Windows Server 2003

Certificate recipient

Windows XP / Server 2003

5. Go to the **General** tab and type a logical **Template Display name** and **Template Name** (we used OpsMgr Certificate and OpsMgrCertificate) and we changed the validity period to 5 years.



Template display name:

OpsMgr Certificate

Template name:

OpsMgrCertificate

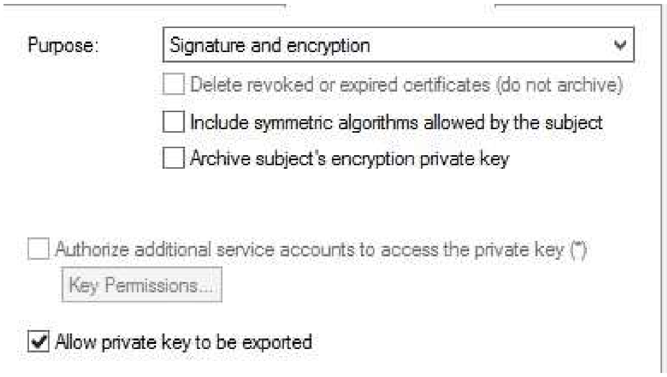
Validity period:

5 years

Renewal period:

6 weeks

6. Go to the *Request Handling* tab and check the option to allow the private key to be exported.



Purpose: Signature and encryption

□ Delete revoked or expired certificates (do not archive)

□ Include symmetric algorithms allowed by the subject

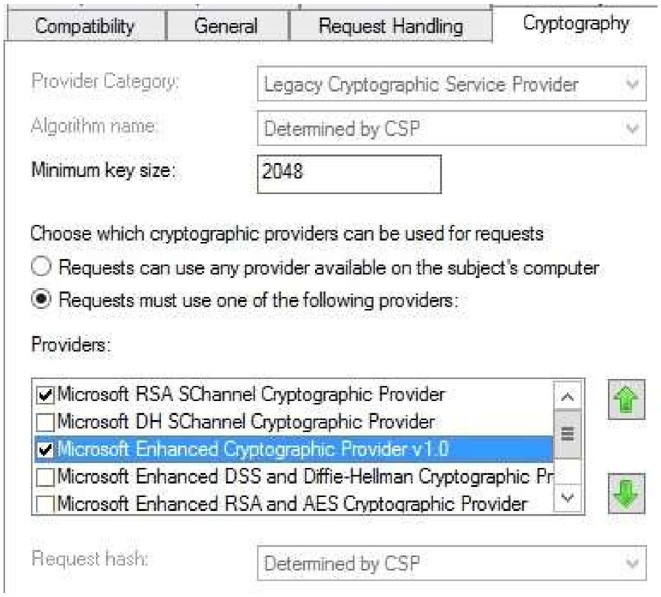
□ Archive subject's encryption private key

□ Authorize additional service accounts to access the private key (*)

Key Permissions...

☑ Allow private key to be exported

7. Go to **Cryptography** and choose the **minimum key size** - we selected **2048** . This is sufficient and takes less CPU time to process. Also check the **Microsoft Enhanced Cryptographic Provider v1.0** button.



Compatibility | General | Request Handling | Cryptography

Provider Category: Legacy Cryptographic Service Provider

Algorithm name: Determined by CSP

Minimum key size: 2048

Choose which cryptographic providers can be used for requests

○ Requests can use any provider available on the subject's computer

● Requests must use one of the following providers:

Providers:

☑ Microsoft RSA SChannel Cryptographic Provider

□ Microsoft DH SChannel Cryptographic Provider

☑ Microsoft Enhanced Cryptographic Provider v1.0

□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Pr

□ Microsoft Enhanced RSA and AES Cryptographic Provider

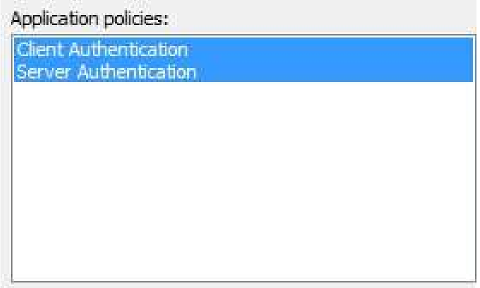
Request hash: Determined by CSP

8. Go to the tab titled **Extensions** . Select the option **Applications Policies** and click **Edit** . Remove **IP security IKE intermediate** and add the following policies:

- Client Authentication

- Server Authentication

Click **OK** .

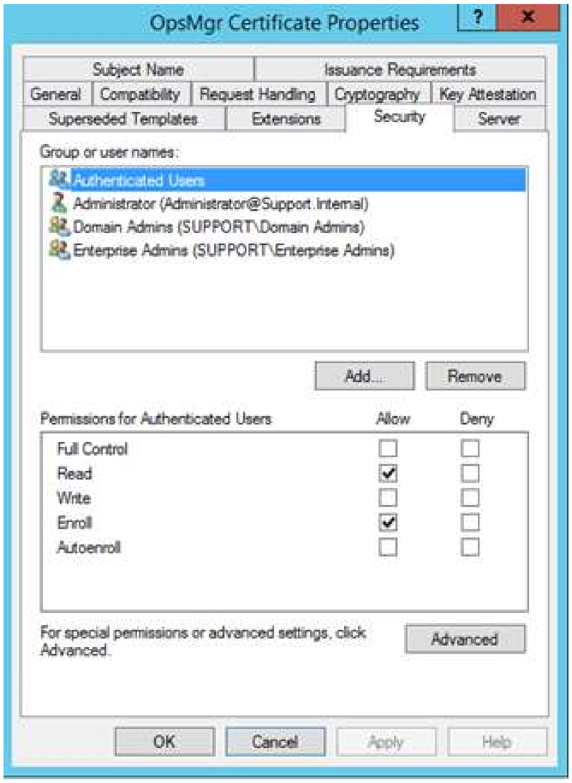


Application policies:

Client Authentication

Server Authentication

9. Go to the tab titled **Security** . **Authenticated Users** need to have **Read & Enroll** access. Click **Apply** and **OK** . The template is now created.



Group or user names:

- Authenticated Users
- Administrator (Administrator@Support.Internal)
- Domain Admins (SUPPORT\Domain Admins)
- Enterprise Admins (SUPPORT\Enterprise Admins)

Permissions for Authenticated Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	□	□

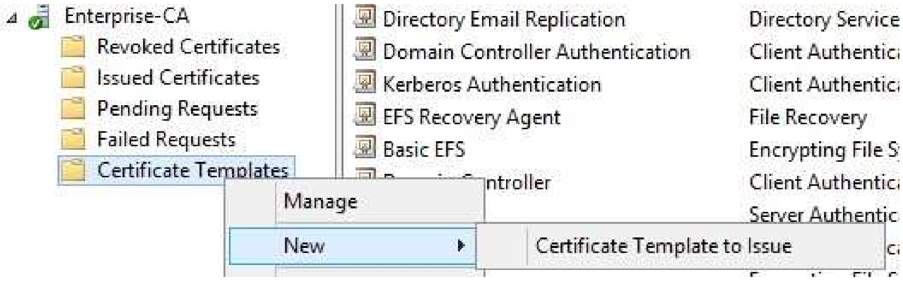
For special permissions or advanced settings, click Advanced.

10. Click **Apply** and **OK,** the template is now created.

Step 4: Make the Template Available

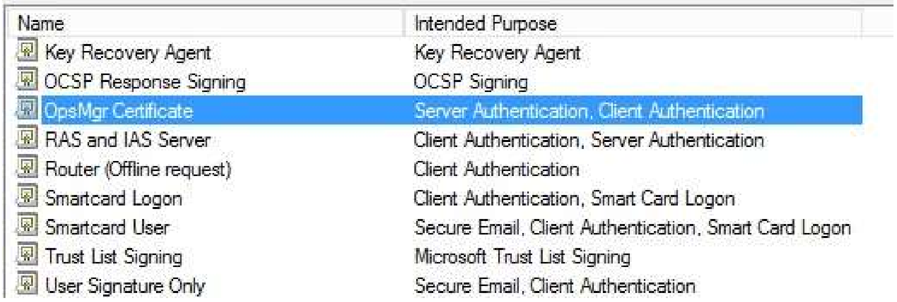
Now that we have the template created, it's time to make it available.

1. Open *Server Manager* , click **Tools** , click **Certificate Authority** , right-click **Certificate Templates** , **New** , **Certificate Template** .



Directory Email Replication	Directory Service
Domain Controller Authentication	Client Authentic
Kerberos Authentication	Client Authentic
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File S
D...ntroller	Client Authentic
	Server Authentic

2. Choose **OpsMgr Certificate** and click **OK** :



Name	Intended Purpose
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
OpsMgr Certificate	Server Authentication, Client Authentication
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication

After these steps the OpsMgr Certificate template is displayed in the certificate templates.

Additional Information

Authentication and Data Encryption for Windows Computers: https://technet.microsoft.com/en-us/library/hh212810.aspx

How to Obtain a Certificate Using Windows Server 2008 Enterprise CA in Ops Manager 2007 **:** http://technet.microsoft.com/en-us/library/dd362553.aspx

How to Obtain a Certificate Using Windows Server 2008 Stand-Alone CA in Ops Manager 2007: http://technet.microsoft.com/en-us/library/dd362655.aspx

How to Obtain a Certificate Using Windows Server 2003 Enterprise CA in Ops Manager 2007: http://technet.microsoft.com/en-us/library/bb735413.aspx

How to Obtain a Certificate Using Windows Server 2003 Stand-Alone CA in Ops Manager 2007: http://technet.microsoft.com/en-us/library/bb735417.aspx

That should take care of getting our Enterprise Root CA installed and configured. In our next installment we'll talk about installing our certificates and completing final configuration in Operations Manager.

Irfan Rabbani | Senior Support Escalation Engineer | Microsoft GBS Management and Security Division

Get the latest System Center news on Facebook and Twitter :

System Center All Up: http://blogs.technet.com/b/systemcenter/

Configuration Manager Support Team blog: http://blogs.technet.com/configurationmgr/
Data Protection Manager Team blog: http://blogs.technet.com/dpm/
Orchestrator Support Team blog: http://blogs.technet.com/b/orchestrator/

Operations Manager Team blog: http://blogs.technet.com/momteam/
Service Manager Team blog: http://blogs.technet.com/b/servicemanager
Virtual Machine Manager Team blog: http://blogs.technet.com/scvmm

Microsoft Intune: http://blogs.technet.com/b/microsoftintune/
WSUS Support Team blog: http://blogs.technet.com/sus/
The RMS blog: http://blogs.technet.com/b/rms/
App-V Team blog: http://blogs.technet.com/appv/
MED-V Team blog: http://blogs.technet.com/medv/
Server App-V Team blog: http://blogs.technet.com/b/serverappv
The Surface Team blog: http://blogs.technet.com/b/surface/
The Application Proxy blog: http://blogs.technet.com/b/applicationproxyblog/

The Forefront Endpoint Protection blog : http://blogs.technet.com/b/clientsecurity/
The Forefront Identity Manager blog : http://blogs.msdn.com/b/ms-identity-support/
The Forefront TMG blog: http://blogs.technet.com/b/isablog/
The Forefront UAG blog: http://blogs.technet.com/b/edgeaccessblog/

OpsMgr 2012 R2

👍 0 Likes

Share