

Opgave

Opgaven er hentet fra:

<http://blogs.technet.com/b/kevinholman/archive/2013/10/30/configmgr-2012-r2-quickstart-deployment-guide.aspx>

Jeg har i et testmiljø kørt med følgende RAM:

RRAS01 – 1024 - 2048

DC01 – 1024 - 2048

DB03 – 2048 – 4096

CM01 – 2048 - 4096

Workstaion01 512 – 2048

Workstation02 – 512 – 2048

Max antal CPU per maskine.

Server Names\Roles:

- DB03 SQL Database Services, Reporting Services
- CM1 Primary Site Server

Windows Server 2012 R2 will be installed as the base OS for all platforms. All servers will be a member of the AD domain.

SQL 2012 with SP1 will be the base standard for all SQL database and reporting services. <http://technet.microsoft.com/en-us/library/gg682077.aspx>

High Level Deployment Process:

1. In AD, create the following accounts and groups, according to your naming convention:
 - DOMAIN\ConfigMgrAdmins ConfigMgr Administrators security group
 - DOMAIN\ConfigMgrLocalAdmin ConfigMgr Client Push account
2. Add the domain user accounts for yourself and your team to the “ConfigMgrAdmins” group.
3. Install *Windows Server 2012 R2* to all server role servers.
4. Install Prerequisites and SQL 2012 with SP1.
5. Install the Site Server and Database Components
6. Install the Reporting components.

Prerequisites:

1. Install Windows Server 2012 R2 to **all Servers**
2. Join all servers to domain.
3. Install all available Windows Updates.
4. Add the “ConfigMgrAdmins” domain global group to the Local Administrators group on each server.
5. On CM1, Install required prerequisites for the site system roles (this covers all site system roles combined on a single server):

Open PowerShell (*as an administrator*) and run the following:

Add-WindowsFeature Web-Windows-Auth,Web-ISAPI-Ext,Web-Metabase,Web-WMI,BITS,RDC,NET-Framework-Features,Web-Asp-Net,Web-Asp-Net45,NET-HTTP-Activation,NET-Non-HTTP-Activ,Web-Static-Content,Web-Default-Doc,Web-Dir-Browsing,Web-Http-Errors,Web-Http-Redirect,Web-App-Dev,Web-Net-Ext,Web-Net-Ext45,Web-ISAPI-Filter,Web-Health,Web-Http-Logging,Web-Log-Libraries,Web-Request-Monitor,Web-HTTP-Tracing,Web-Security,Web-Filtering,Web-Performance,Web-Stat-Compression,Web-Mgmt-Console,Web-Scripting-Tools,Web-Mgmt-Compat -Restart

Note – if your machines are not internet connected, you might need to add a “–Source D:\sources\sxs” or whatever the path is to your Windows installation media. By default Windows 2012 gets .NET 3.5 from Windows Update, but this doesn't always work, and will never work for machines without an internet connection.

After installing these roles/features, you might have to register ASP.NET with IIS. The simplest way is to open an elevated command prompt:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319>aspnet_regiis.exe –r
```

6. On CM1 – Install the Deployment Tools, Windows PE, and the User State Migration tool from the Windows 8.1 ADK: <http://www.microsoft.com/en-us/download/details.aspx?id=39982>
7. On CM1 – add the WSUS feature from Server Manager.
8. Install **SQL 2012 with SPI** to **the DB server role**

- Setup is fairly straightforward. This document will not go into details and best practices for SQL configuration. Consult your DBA team to ensure your SQL deployment is configured for best practices according to your corporate standards.
- Run setup, choose Installation > New Installation...
- When prompted for feature selection, install **ALL** of the following:
 - Database Engine Services
 - Full-Text and Semantic Extractions for Search (required for OpsMgr is doing a shared SQL deployment)
 - Reporting Services - Native
- Optionally – consider adding the following to ease administration:

- Management Tools – Basic and Complete (for running queries and configuring SQL services)
- On the Instance configuration, choose a default instance, or a named instance. Default instances are fine for testing and labs. Production clustered instances of SQL will generally be a named instance. For the purposes of the POC, choose default instance to keep things simple.
- On the Server configuration screen, set SQL Server Agent to Automatic. You can accept the defaults for the service accounts, but I recommend using a Domain account for the service account. Input the DOMAIN\sqlsvc account and password for Agent, Engine, and Reporting.
- On the Collation Tab – you can use the default which is **SQL_Latin1_General_CP1_CI_AS** or choose another supported collation.
- On the Account provisioning tab – add your personal domain user account or a group you already have set up for SQL admins. Alternatively, you can use the ConfigMgrAdmins global group here. This will grant more rights than is required to all ConfigMgrAdmin accounts, but is fine for testing purposes of the POC.
- On the Data Directories tab – set your drive letters correctly for your SQL databases, logs, TempDB, and backup.
- On the Reporting Services Configuration – choose to **Install and Configure**. This will install and configure SRS to be active on this server, and use the default DBEngine present to house the reporting server databases. This is the simplest configuration. If you install Reporting Services on a stand-alone (no DBEngine) server, you will need to configure this manually.
- Setup will complete.
- You will need to disable Windows Firewall on the SQL server, or make the necessary modifications to the firewall to allow all SQL traffic. See <http://msdn.microsoft.com/en-us/library/ms175043.aspx>

9. On the SQL server – add the Computer Account in the domain to the local administrators group of the SQL database server (DOMAIN\CM1\$)

10. In Active Directory – extend the schema, create the System Management container, and assign permissions: http://technet.microsoft.com/en-us/library/gg712264.aspx#BKMK_PrePAD

Step by step deployment guide:

1. Install the Primary Site Server role on **CM1**.

- Log on using **your personal domain user account** that is a member of the **ConfigMgrAdmins** group.
- Run **Splash.hta**
- Click **Install**
- Read the “Before You Begin” Info and click **Next**.
- On the Available Setup Options, choose to install a **primary site**, but to **NOT** check the box for typical options. We are going to configure each step for our site and use a remote SQL database server.
- Choose Eval or input your **license key** and click Next.
- **Accept** the Eula and click Next.
- **Accept** the additional license agreements and click Next.
- Provide a path to the prereq file downloads. If you have not downloaded these recently then create a new folder for these, locally or on a remote path.
- Choose your language(s) and click **Next**, on the server and client screens.
- Input a site code for your primary site. Input a description. Choose a path. Make sure you are also installing the console. Click **Next**.

- Choose to install a primary site as a stand alone site. We can add a CAS later in ConfigMgr 2012 SP1 and later.
- Input the SQL server name, instance, click **Next**.
- Accept the default for the SMS provider. **Next**.
- Choose to configure the communication method on each site system role, and **to not use** HTTPS (don't check box.) **Next**.
- Choose **HTTP** for the MP and DP – we can change this to HTTPS with certs down the road. Next.
- Choose to enable CEIP or not. **Next**.
- Choose **next** to run prereq checker. Resolve any issues. Click **Begin Install**.
- Install Completes. Click **Close**.

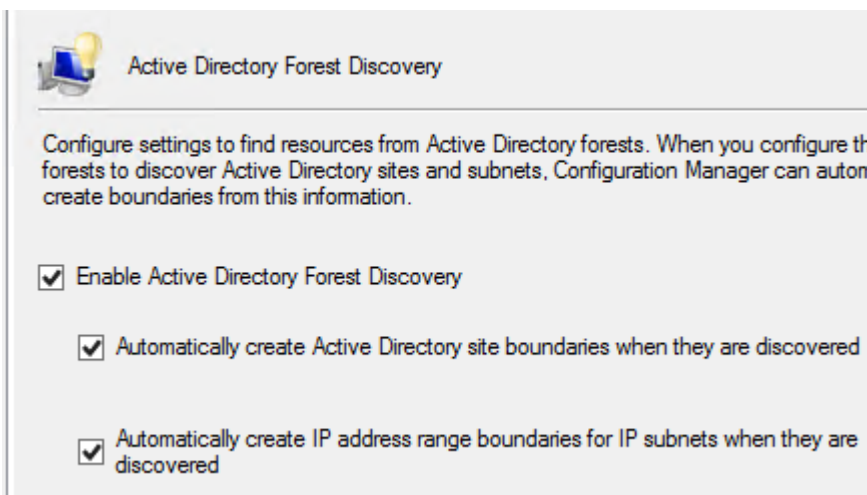
Post Deployment Configuration:

1. Add Site System Roles:

- <http://technet.microsoft.com/en-us/library/hh272770.aspx>
- Application Catalog roles
- Asset Intelligence
- Endpoint protection
- Fallback status
- Software update

2. Enable discoveries

- <http://technet.microsoft.com/en-us/library/hh427340.aspx>
- Enable AD Forest Discovery



This will bring in the AD site and IP boundaries.

- Enable AD Group discovery to bring in Security groups and group membership for computers. Create a scope that makes sense only for groups you need to discover.
- Enable AD system discoveries to bring in systems.
- Enable User discovery

3. Configure Boundaries and Boundary Groups

- Create a boundary group and add your site boundaries and site servers to it, for site assignment.

4. Configure Client Device Settings

- Administration > Client Settings > Create Custom Client Device Settings
- Check:
 - Client Policy
 - Computer Agent
 - Software Updates
- Configure Client policy polling as appropriate (longer for production, faster for labs)
- Configure “Set Website” for Application Catalog on Computer Agent settings and customize any additional settings.
- Set a schedule for software update scans for 1 day.
- Deploy your new client device systems to All Systems (for a lab)

5. Install Clients: <http://technet.microsoft.com/en-us/library/gg712298.aspx>

- Assign a client Push account to Administration > Site Configuration > Sites > Client Installation Settings
- Install clients to a collection

6. Verify Hardware and software inventory for clients

7. Enable Endpoint protection

- Client Settings – create a new client device setting. Enable endpoint protection.
- Configure Client device settings to turn on Endpoint protection and deploy endpoints.
- Deploy new client policy to All Desktop and Server Clients Collection, or a custom collection
- Create automatic deployment rule for definition updates using Definition template.

Continue on with additional steps from TechNet, such as software deployment, software updates, OSD, etc.