

Master Thesis - Security Aspects in Virtual Networks

SITREP 18

Laurent De Wilde

Master of Science in the Applied Computer Science
Vrije Universiteit Brussel

May 11, 2015

Work done

- Wrote the final thesis document up until the work performed so far.
- Wrote a manual about setting up a private cloud as requested by Dr. Hasan Fayyad-Kazan
- Performed some additional network penetration testing.
- I set up countermeasures against some network attacks.

The following pages contain the manual about setting up a private cloud. Note that this manual is not complete yet.

Chapter 4

Installation of a private cloud

In addition to network attacks against stand-alone network computers, some attacks against private clouds will be performed. In this chapter, the installation of a cloud environment using Windows Server 2012 R2 will be covered in detail.

4.1 Installation of Microsoft System Center 2012 R2 Virtual Machine Manager

4.1.1 Installation requirements

Before installing System Center 2012 R2 VMM, some hardware - and software requirements must be met.

Processor	Dual-core of 2,8 GHz
RAM	4 GB
Hard disk space without a local VMM database	40 GB
Hard disk space with a local VMM database	150 GB

Hardware requirements (up to managing 150 hosts)

When managing more than 150 hosts, it is recommended to use a dedicated computer for MSSQL Server. That is, to store the VMM database on a dedicated computer.

Software requirements

- Microsoft .NET Framework 4.5 or higher

- Windows Deployment and installation kit for Windows 8.1
- Windows Server 2012 R2
- Microsoft SQL Server 2012 (with or without SP1 and SP2)

Other requirements

- The server where the VMM will be installed, must be a member of an Active Directory domain.
- The server name cannot exceed 15 characters

4.1.2 General installation overview

...

4.1.3 Pre-installation configuration

Prior to installing VMM, some settings will be configured such as a static IP address and joining the server to an AD domain. The complete installation has been performed on a freshly installed Windows Server 2012 R2 as VM on a Windows Server 2012 R2 running Hyper-V. Make sure you are logged in as a Domain Admin.

In order to be able to join the server to a domain, a static IP must be set. Make sure the DNS servers point to the DNS servers of the AD domain.

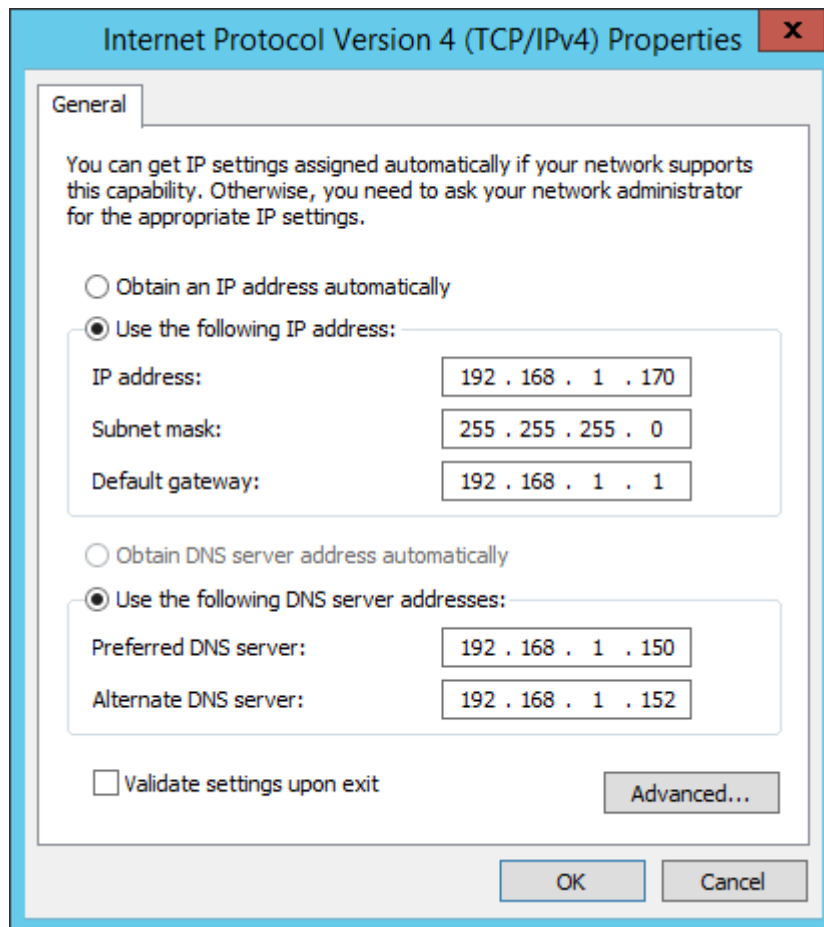


Figure 4.1: configuring static IP settings.

After this, the server can be joined to the AD domain.

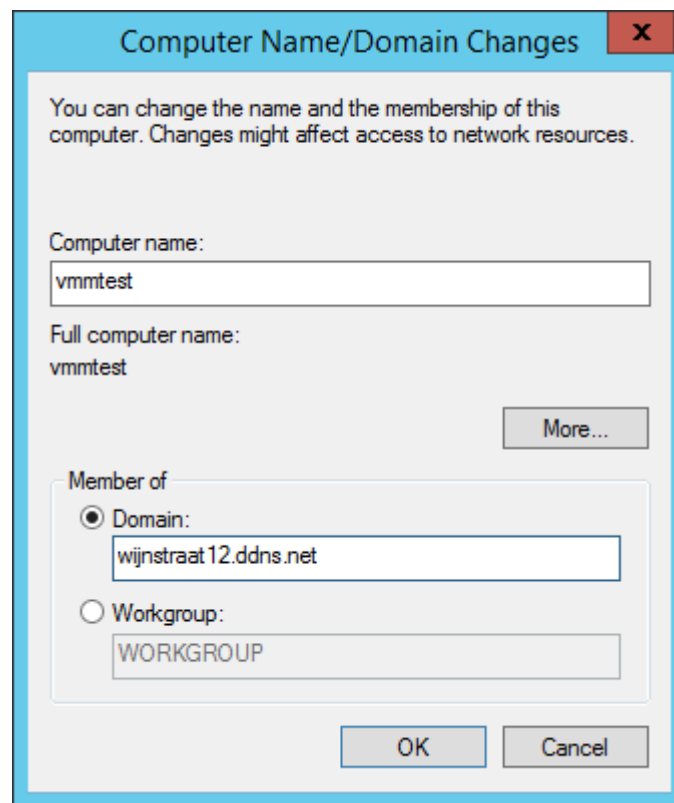


Figure 4.2: Setting an appropriate server name and joining the server to the AD domain.

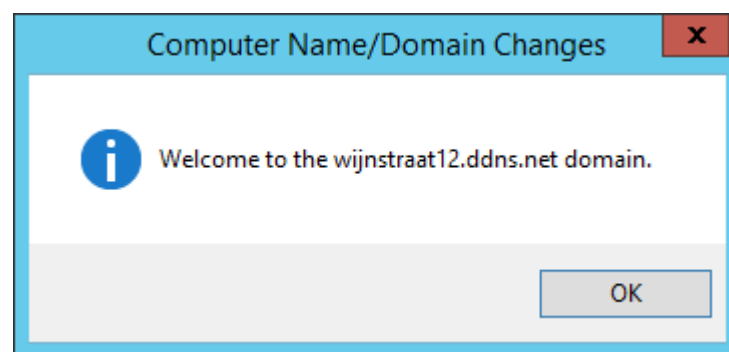


Figure 4.3: Confirmation of successfully joining the AD domain.

Next, the server has to be rebooted and the overview screen of the local server must be something as the figure below.

Computer name	vmmtest	Last installed updates	Never
Domain	wijnstraat12.ddns.net	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Domain: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Enabled	IE Enhanced Security Configuration	Off
NIC Teaming	Disabled	Time zone	(UTC+01:00) Brussels, Copenhagen, Madrid, Paris
Ethernet	192.168.1.170, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2012 R2 Datacenter	Processors	Intel(R) Core(TM) i7 CPU 930 @ 2.80GHz
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	4 GB
		Total disk space	99.66 GB

Figure 4.4: The overview screen of the local server with a proper server name set, the server being joined to the domain, the firewall and remote desktop both being enabled. Also, a static IP has been set and the IE Enhanced Security Configuration has been disabled. Now we are ready to install Microsoft SQL Server 2012 SP2.

4.1.4 Installation of MSSQL Server 2012 SP2

In this tutorial, SQL Server will be installed on the same server as the Virtual Machine Manager will be installed on. Before installing SQL Server 2012, the `netfx3` package will have to be installed, otherwise the installation process will fail. This is achieved by executing following command in PowerShell:

```
dism /online /enable-feature /featurename:netfx3 /all /source:d:\sources\sxs
```

Before executing this command, make sure that the installation media (that is, the .ISO image of WS2012R2) is inserted.

```

Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.WIJNSTRAAT12> dism /online /enable-feature /featurename:netfx3 /all /source:d:\sources\sxs

Deployment Image Servicing and Management tool
Version: 6.3.9600.17031

Image Version: 6.3.9600.17031

Enabling feature(s)
[=====100.0%=====]
The operation completed successfully.
PS C:\Users\Administrator.WIJNSTRAAT12>

```

Figure 4.5: `netfx3` has been installed successfully.

Now, the actual installation of SQL Server can begin. When mounting the SQL Server .ISO image and trying to run setup.exe, I expected some error messages. However, when first extracting the .ISO file with WinRAR and then executing setup.exe, everything went fine.

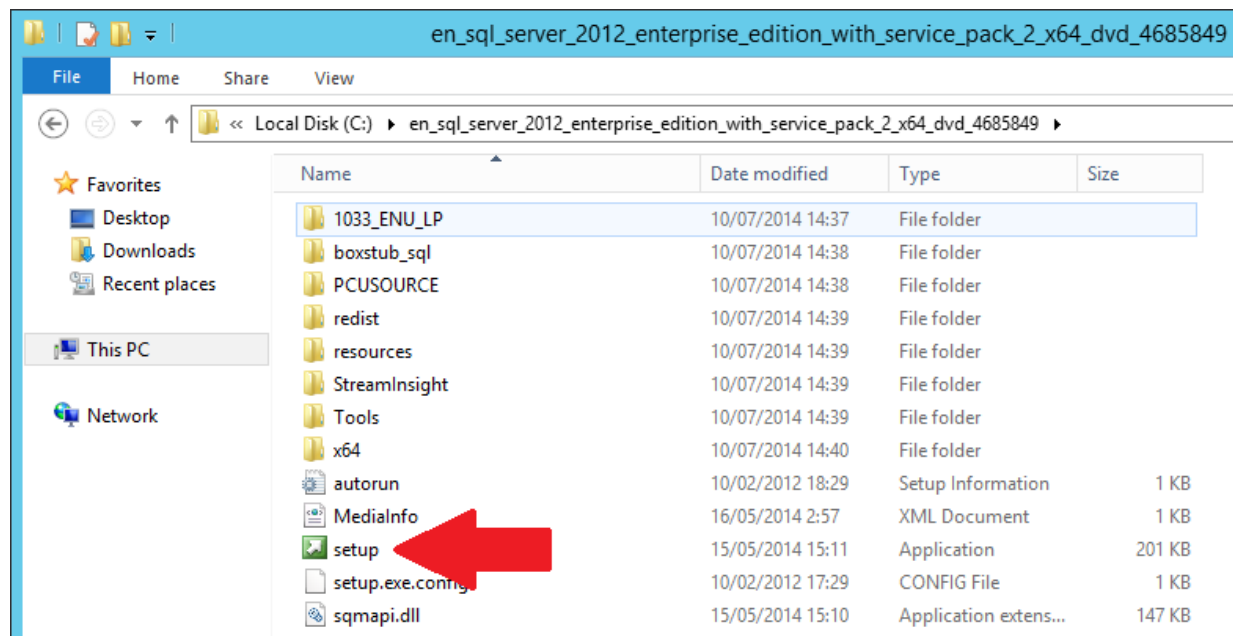


Figure 4.6: Extract the image using WinRAR and run setup.exe.

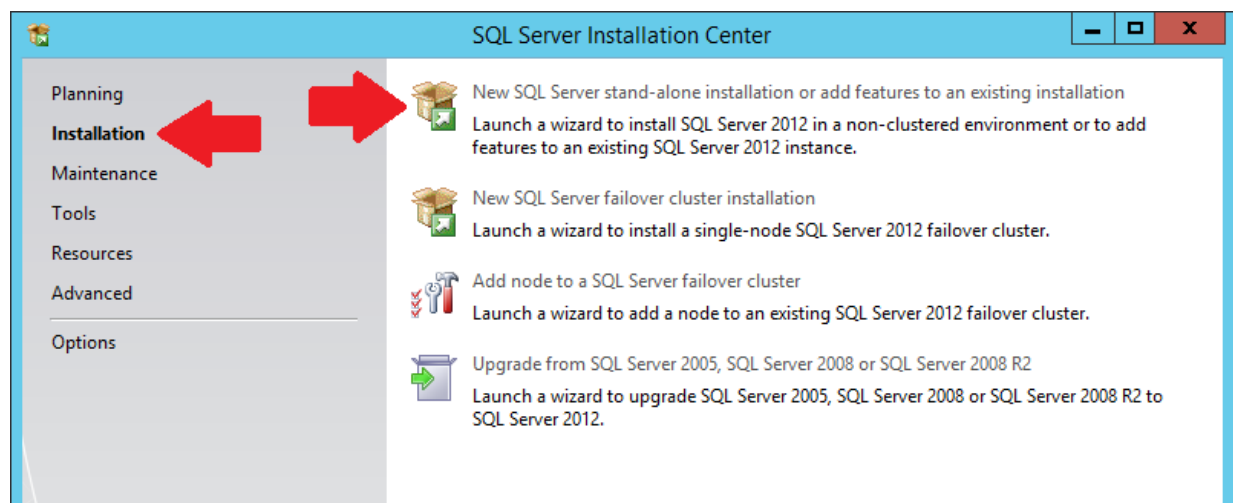


Figure 4.7: In the left pane, select “Installation” and subsequently in the right pane, select “New SQL Server stand-alone configuration”.

The installation will begin and the prerequisites will be checked. When every prerequisite is fulfilled, all marks will be green. Next, enter the product key or choose the evaluation version. After this, the license terms will have to be accepted and the installation will check for product updates.

When everything has been passed successfully, one should be seeing the following figure.

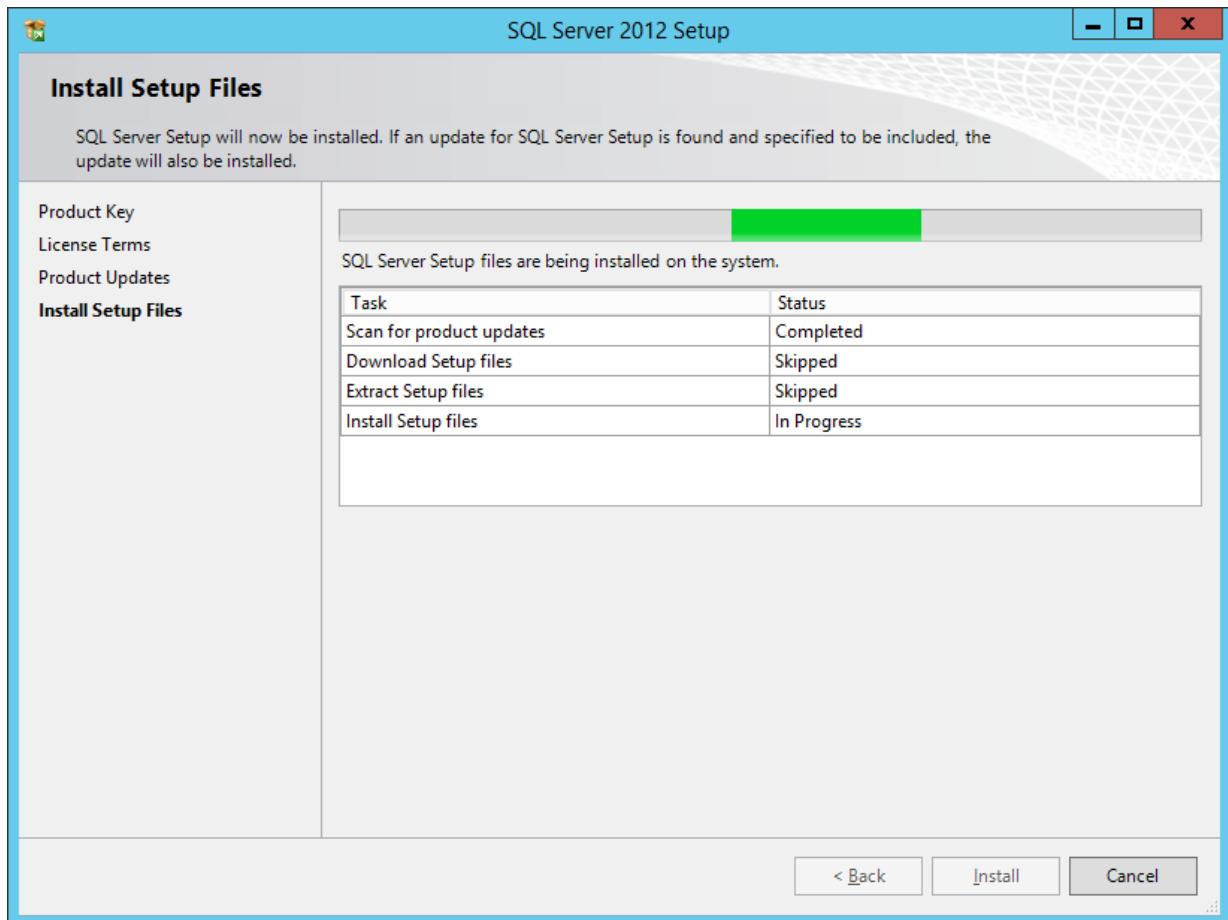


Figure 4.8: Setup files are being installed.

Some additional prerequisites are checked. When everything is passed, setup can be continued.

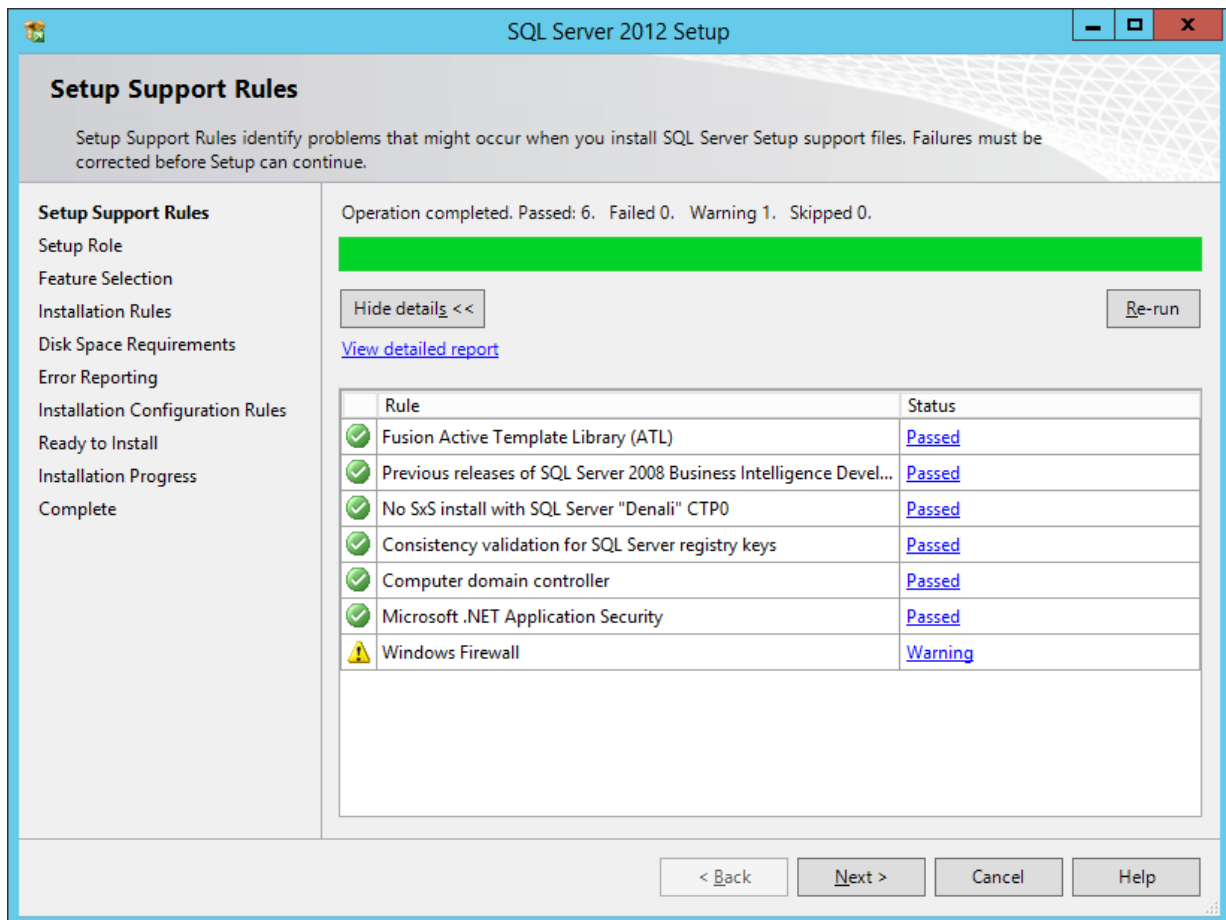


Figure 4.9: Checking additional prerequisites.

On the feature selecting screen, make sure the following features are checked:

- Database Engine Services
- Management Tools - Basic
- Management Tools - Advanced
- SQL Client connectivity SDK

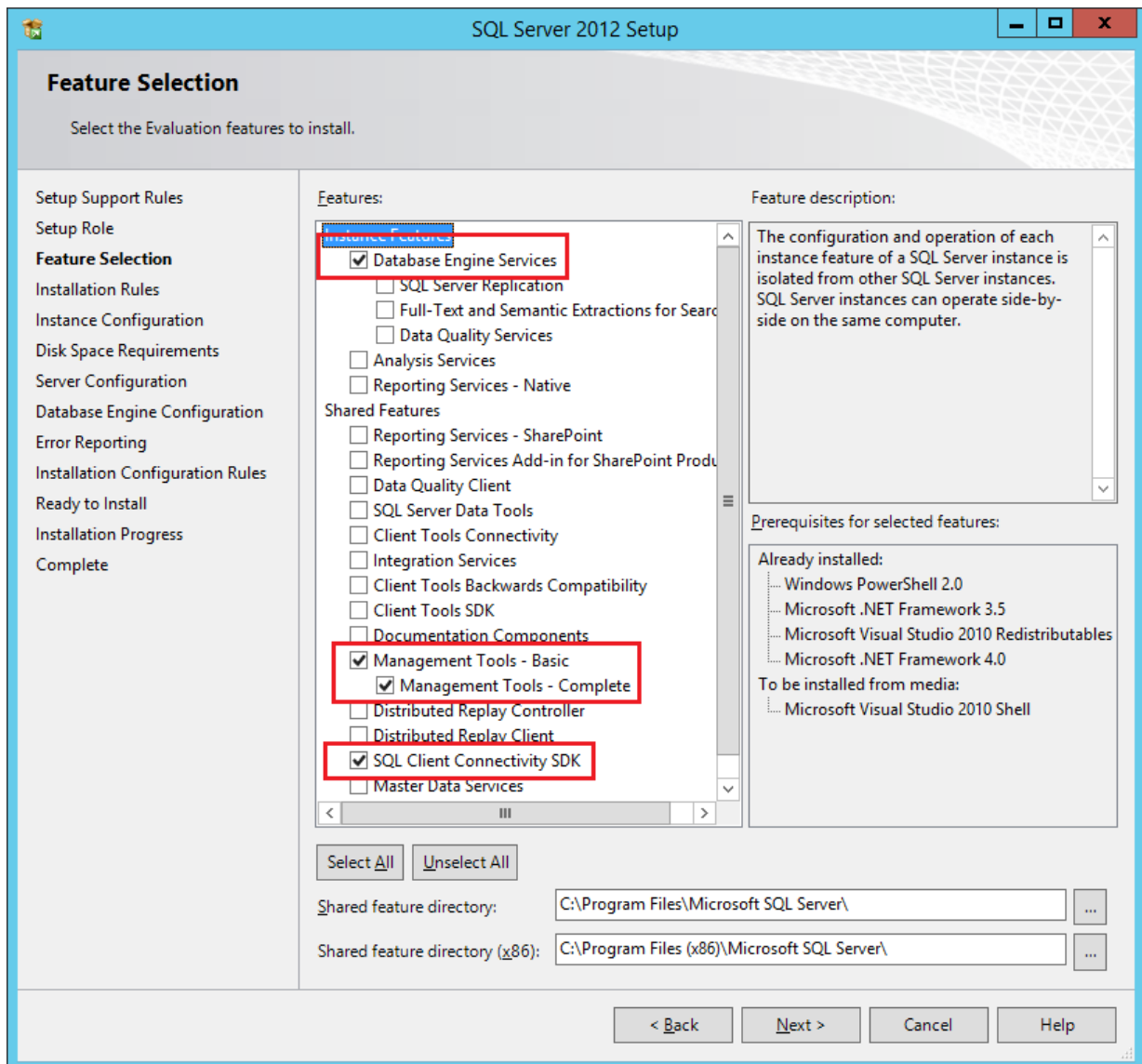


Figure 4.10: Selection of the features.

On the next screen, choose “Windows Authentication Mode” and specify the administrators. In this case, both Domain Admins as well as Local Admins have been chosen.

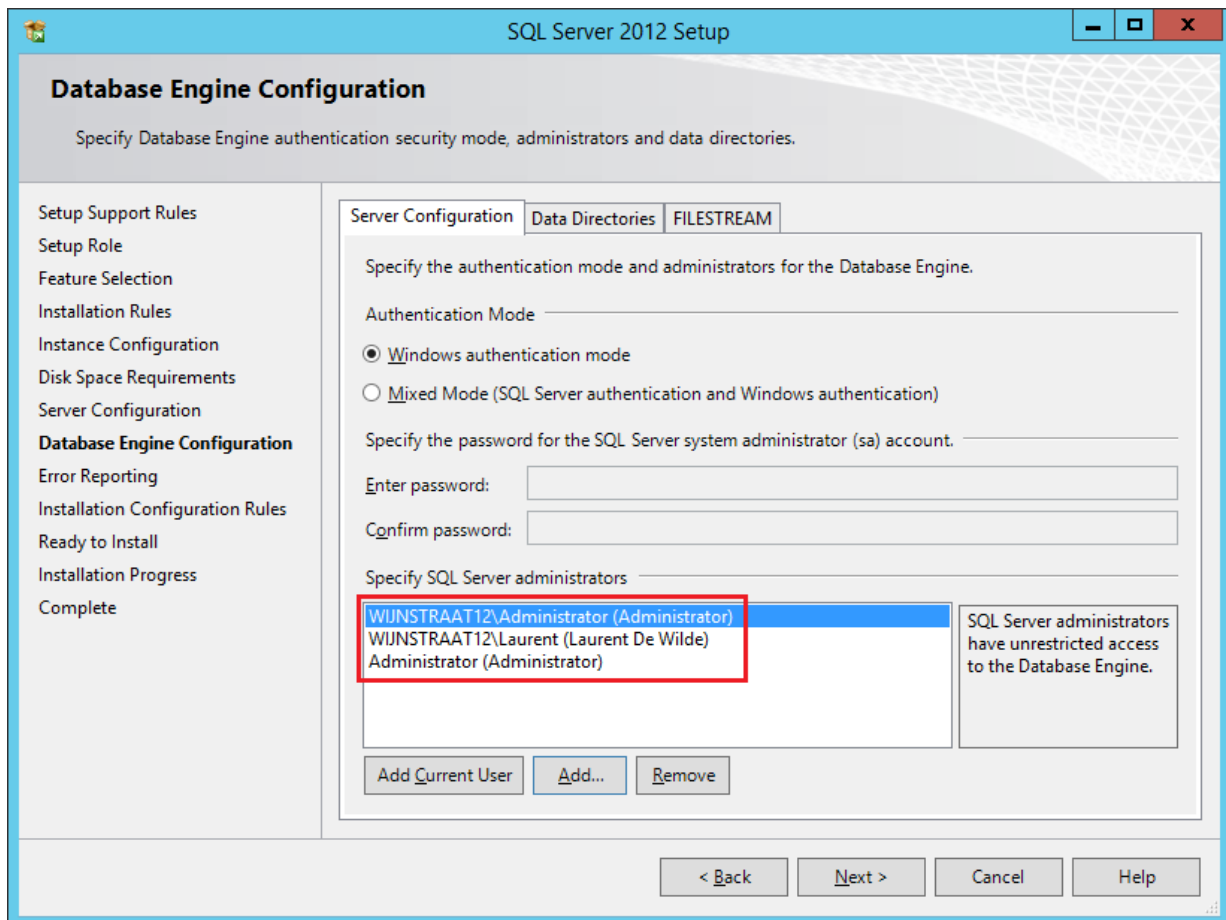


Figure 4.11: Windows Authentication Mode is chosen and the SQL administrators are added.

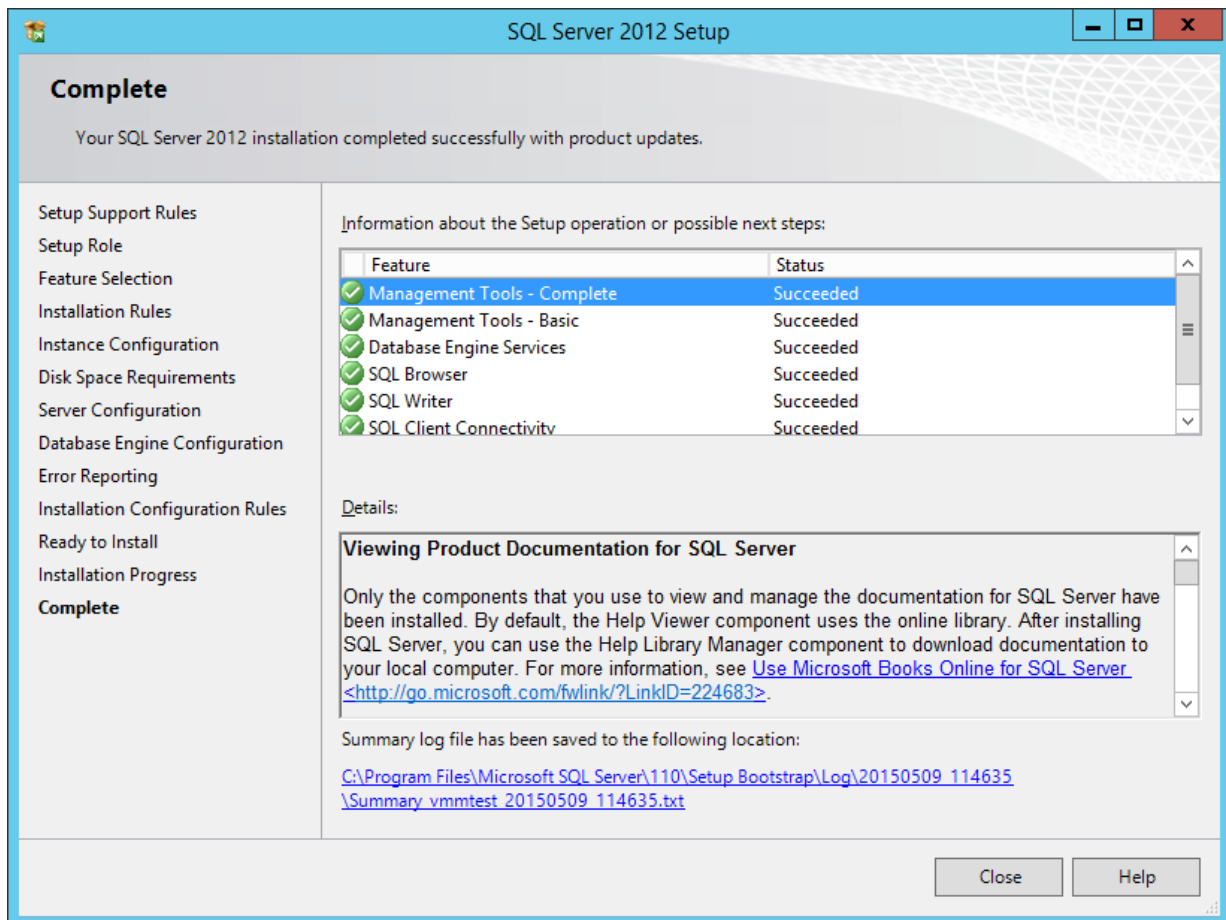


Figure 4.12: Setup has completed successfully.

4.1.5 Configuring Distributed Key Management in Active Directory

Distributed key management is used when a VMM cluster is used. The database of VMM is encrypted because it contains sensitive data. Consider the situation where two servers are used to form a clustered VMM environment. If the decryption keys are stored locally on server 1 and this particular server goes offline, there is no way to access the decryption keys anymore. This is why the keys are stored in a special container in Active Directory. This way, anytime access to the decryption keys is guaranteed.

In combination with DKM, a service account needs to be as well. This account is used to, for example, share .ISO images in the shared libraries of VMM.

Let us configure Distributed Key Management (DKM) and the service account.

To do so, a new OU named “ServiceAccounts” is made under the root domain in the “Active Directory Users and Groups” snap-in. In this newly created OU, a (domain)user “VMMService” is made. This user serves as the service account for VMM.

Make sure that the password never expires.

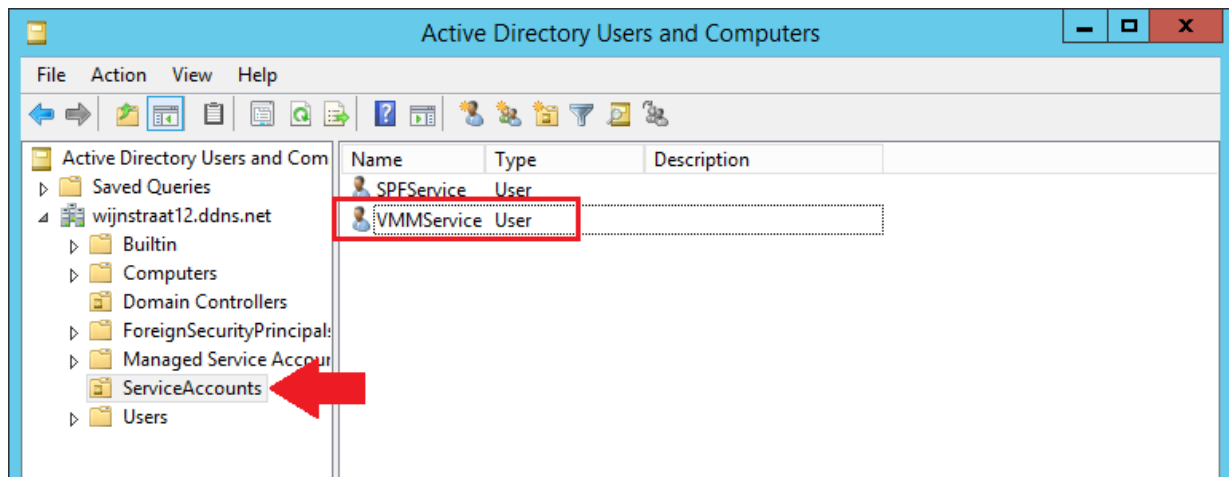


Figure 4.13: Making the service account for DKM.

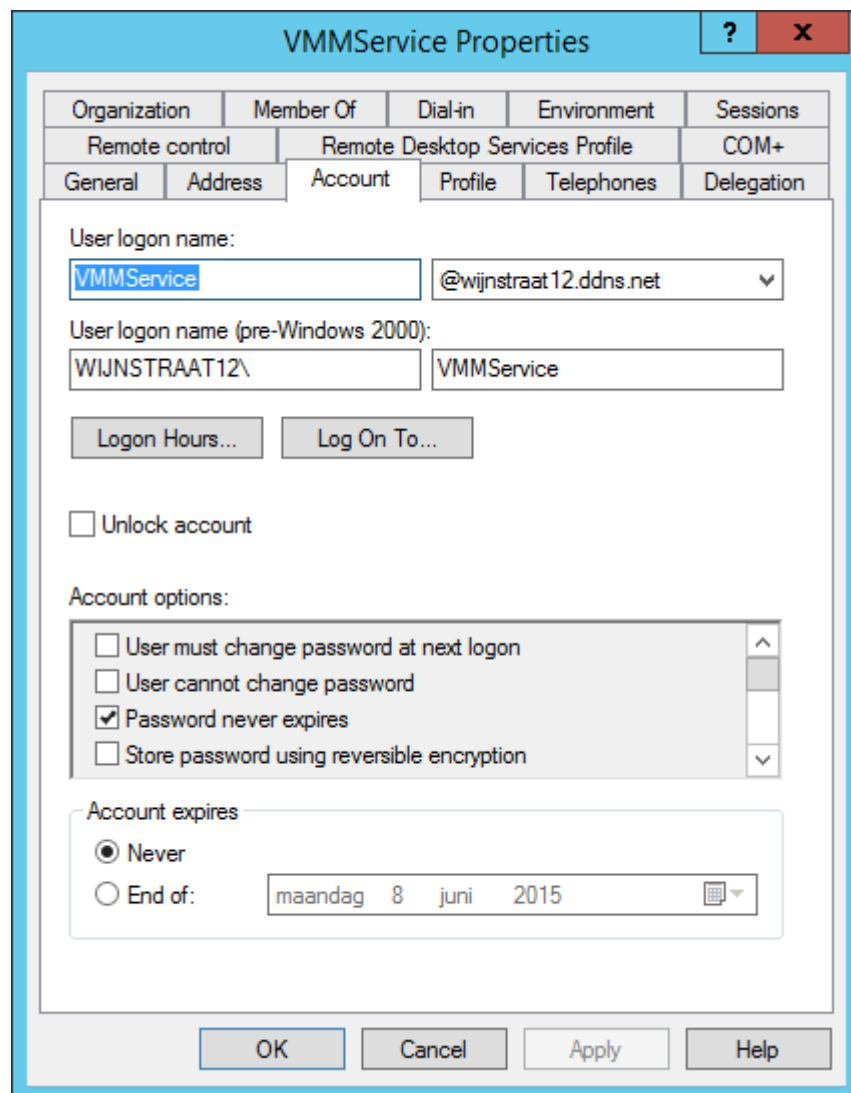


Figure 4.14: The properties of the service account.

Now, the actual container for the keys can be made in Active Directory. To do so, open “ADSI Edit” from the local server overview of the server manager: **Server Manager** → **Local Server** → **Tools** → **ADSI Edit**.

Accept the default naming context (click **OK**) and expand the **Default naming context** node. Right click on the root OU and choose **New** → **Object**.

Select **container** and name it for example “**VMMDKM**”. Click **Finish**.

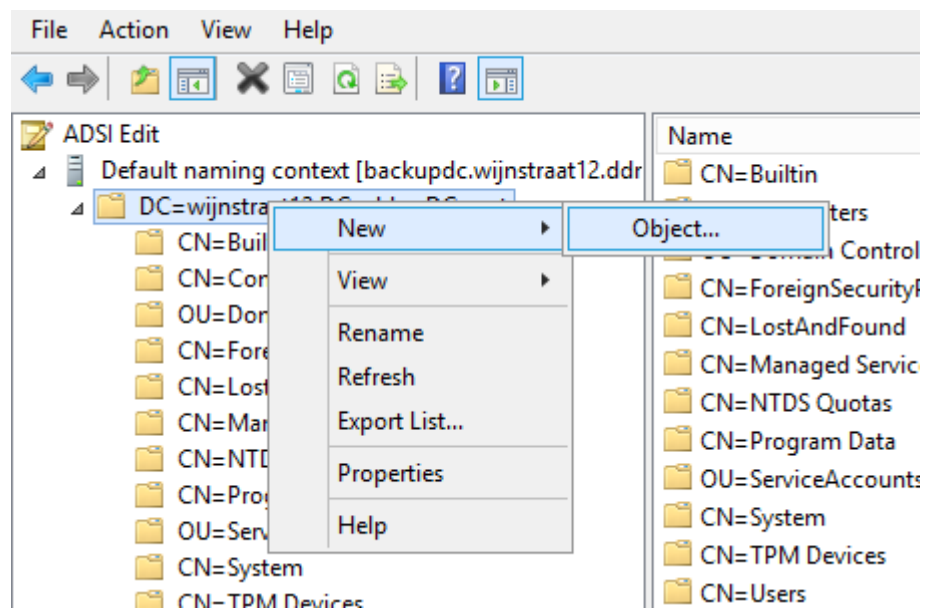


Figure 4.15: Create a new Object.

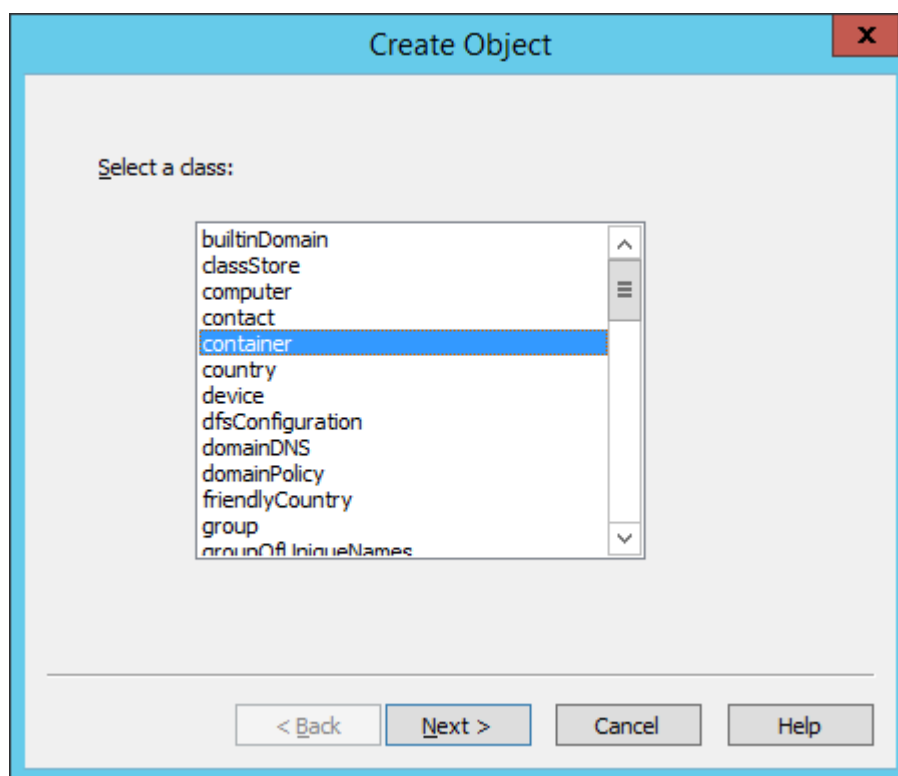
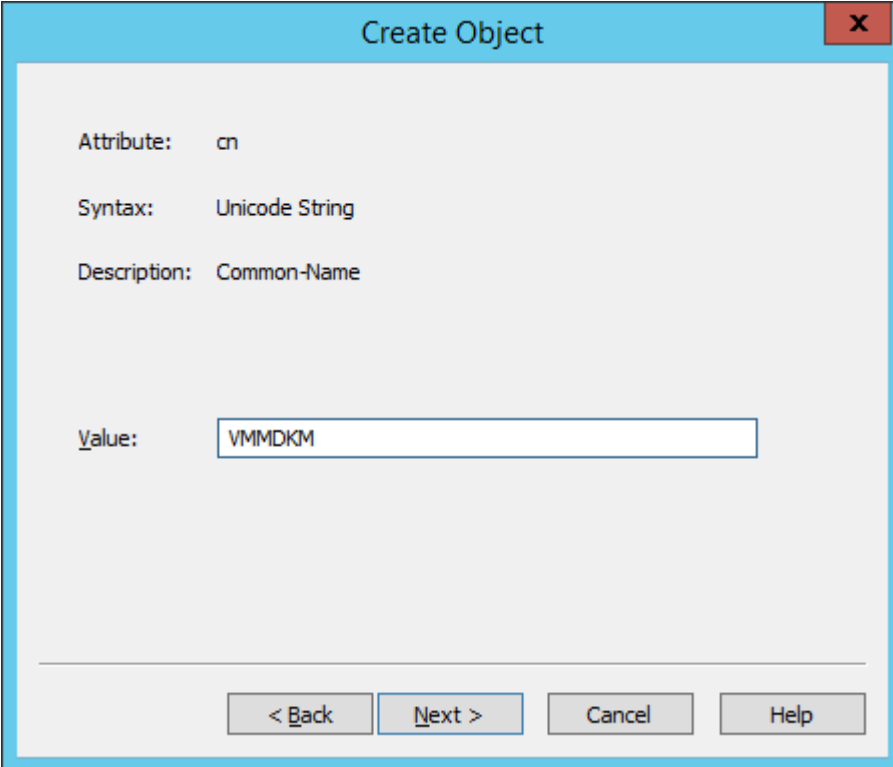


Figure 4.16: Creation of the container.

A screenshot of a Windows dialog box titled "Create Object". The dialog has a light blue header bar with the title and a red close button. The main area is light gray and contains four labels with corresponding values: "Attribute:" with "cn", "Syntax:" with "Unicode String", "Description:" with "Common-Name", and "Value:" with a text box containing "VMMDKM". At the bottom, there are four buttons: "< Back", "Next >", "Cancel", and "Help".

Attribute:	cn
Syntax:	Unicode String
Description:	Common-Name
Value:	VMMDKM

< Back Next > Cancel Help

Figure 4.17: Creation of the container.

Next, some permissions for the VMMDKM container must be set. To do so, right click on the newly created container and select **Properties**. On the **Security** tab, click advanced. Click **Edit**.

Make sure the principal is "VMMService". and change **Applies to:** to "This object and all descendant objects".

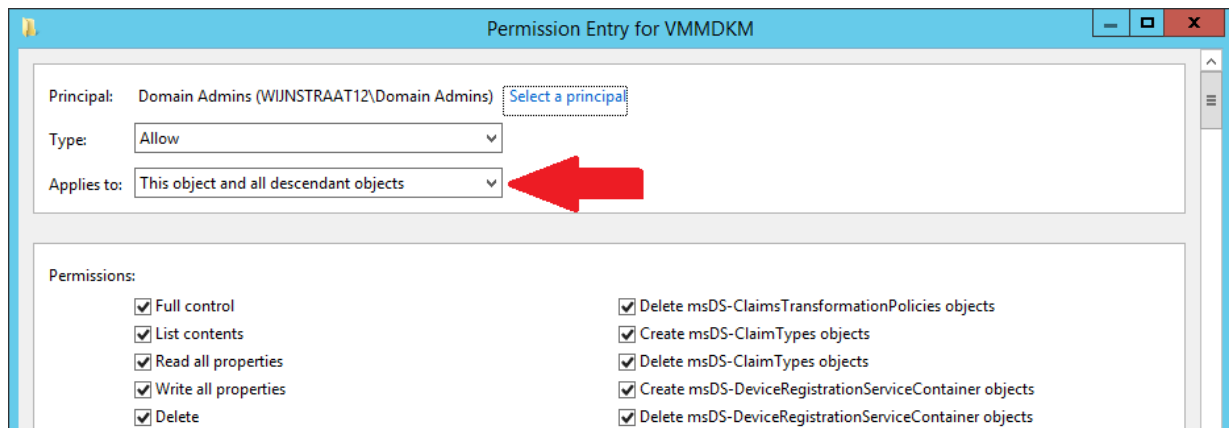


Figure 4.18: Configuration of the permissions for VMMDKM.

After this, the VMMSvc account needs to be added to the **local** administrators group. To do so, open computer management and select **Local Users and Groups** → **Groups**. Right click on the **Administrators** group and choose **Properties** and add the “VMM-Service” account to the group. Click **OK**.

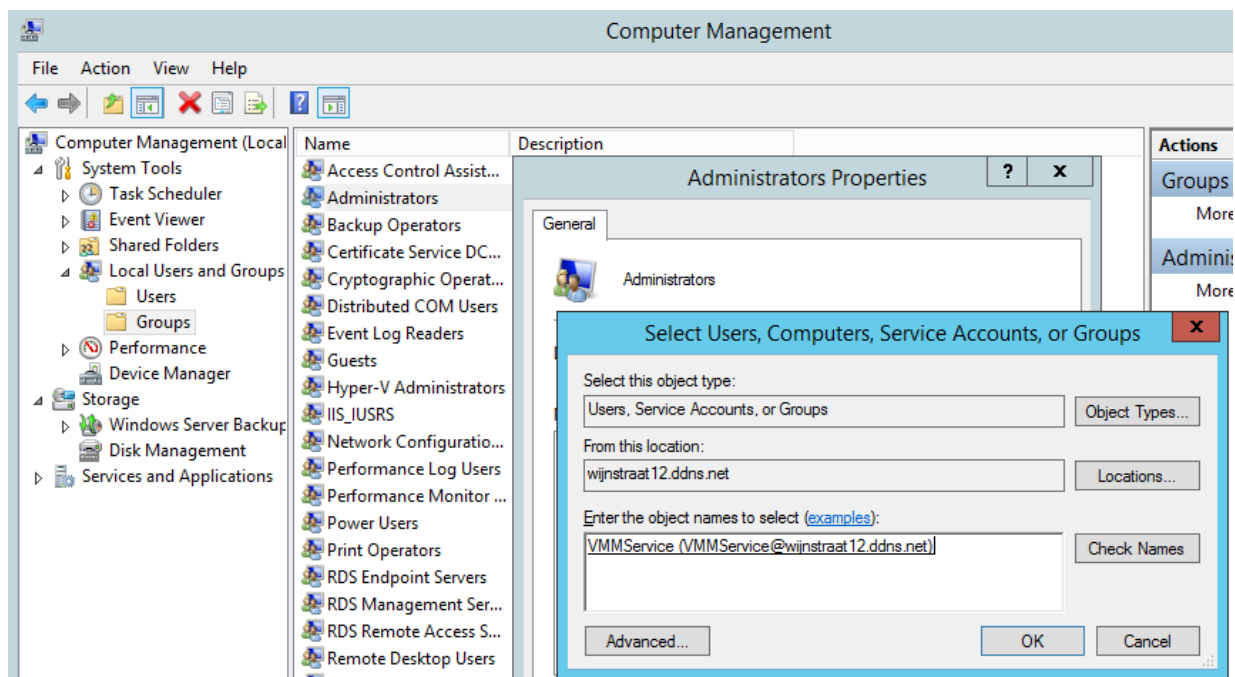


Figure 4.19: Adding the VMMSvc account to the local administrators group.

4.1.6 Post configuration of MSSQL Server

The VMMSerivce account has to be given database access. Therefore, open “SQL Server Management Studio”, login using Windows Authentication and expand the **Security** folder. Right click on **Logins** and create a new login. This login account is the VMMSerivce account.

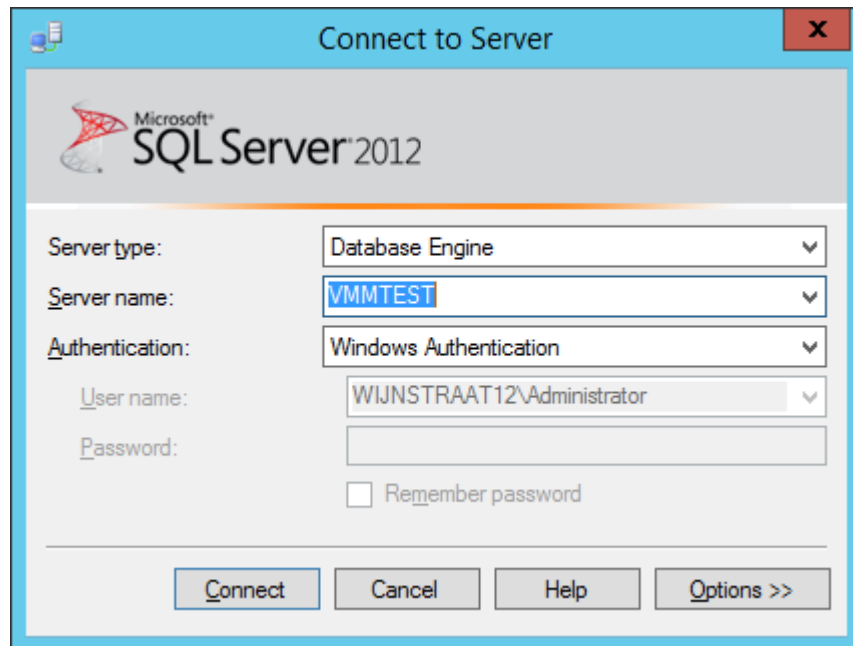


Figure 4.20: Login into SQL Server Management Studio using Windows Authentication.

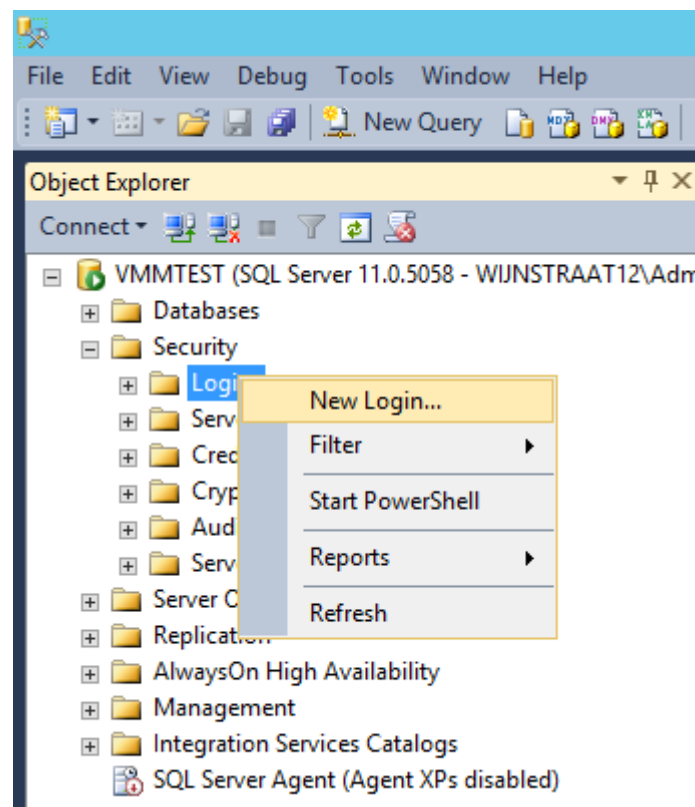


Figure 4.21: Creation of a new login.

On the **Server** role page of this new login, make sure to check the “dbcreator”, “process admin”, “public” and “security admin” roles. After this is completed, exit Management Studio.

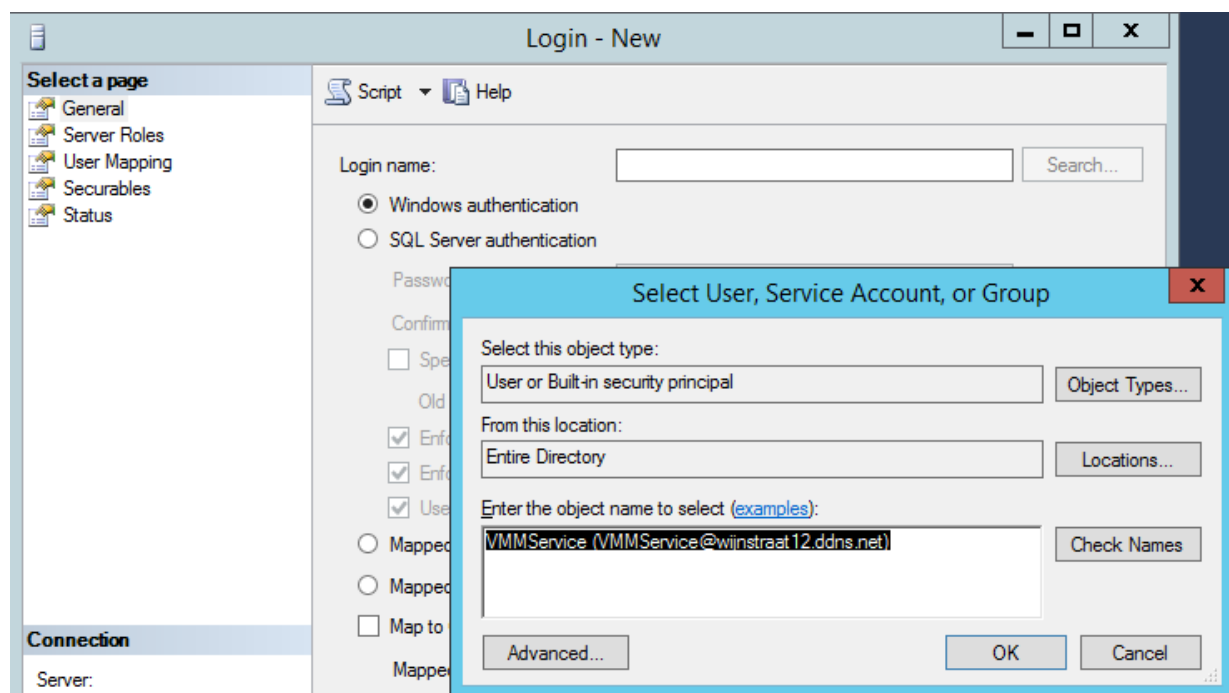


Figure 4.22: Selecting the VMMService account.

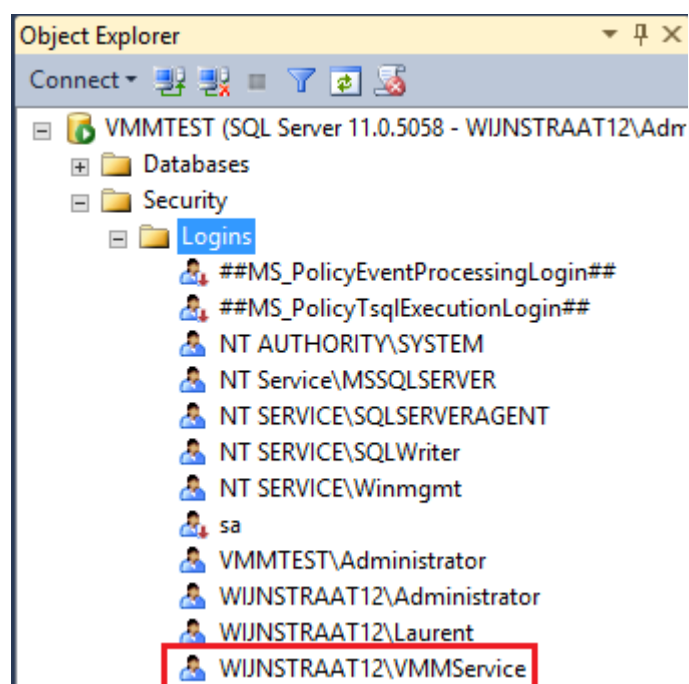


Figure 4.23: Confirmation.

4.1.7 Installation of VMM

There is one prerequisite that is not fulfilled yet: the installation of the Windows Assessment and Deployment Kit. Since Windows Server 2012 R2 is used, Windows ADK for Windows 8.1 must be installed. The Windows ADK can be downloaded from the Microsoft website: <https://www.microsoft.com/en-us/download/details.aspx?id=39982>

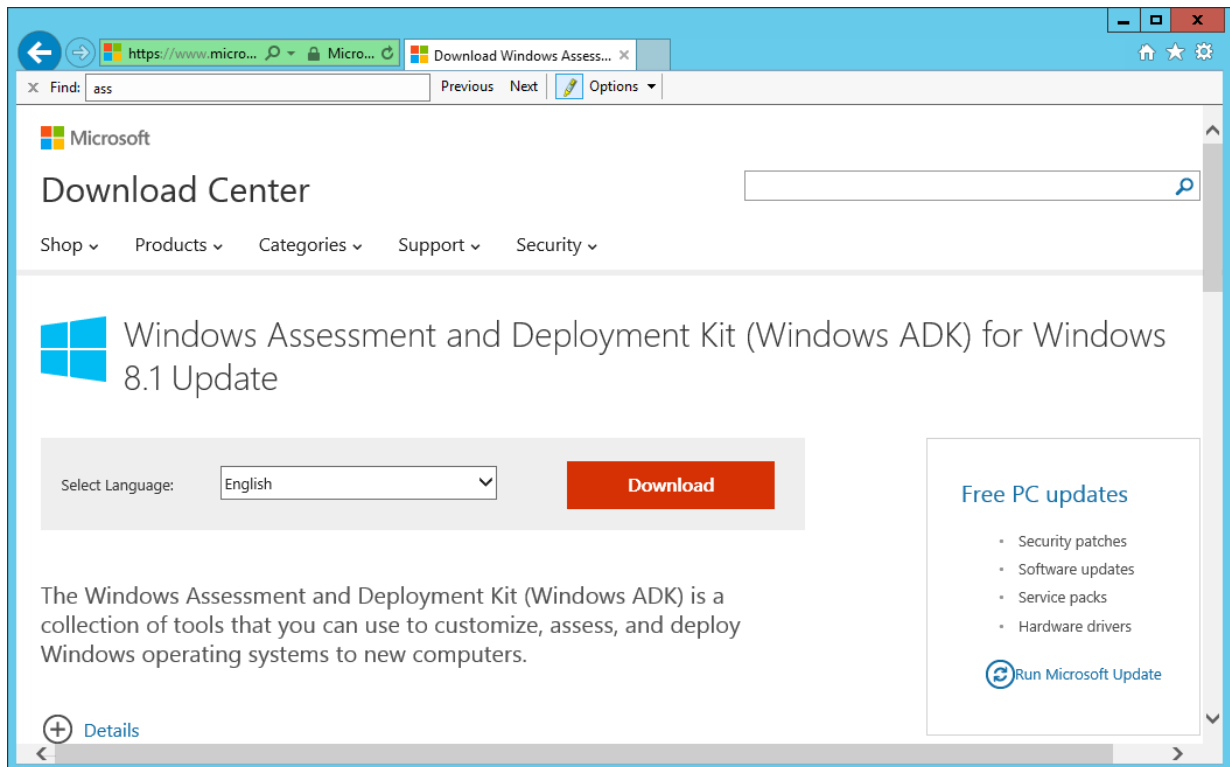


Figure 4.24: Download the Windows ADK for Windows 8.1.

Since we are installing VMM on the computer we are currently logged into, choose the option “Install the Windows Assessment and Deployment Kit for Windows 8.1 to this computer”.

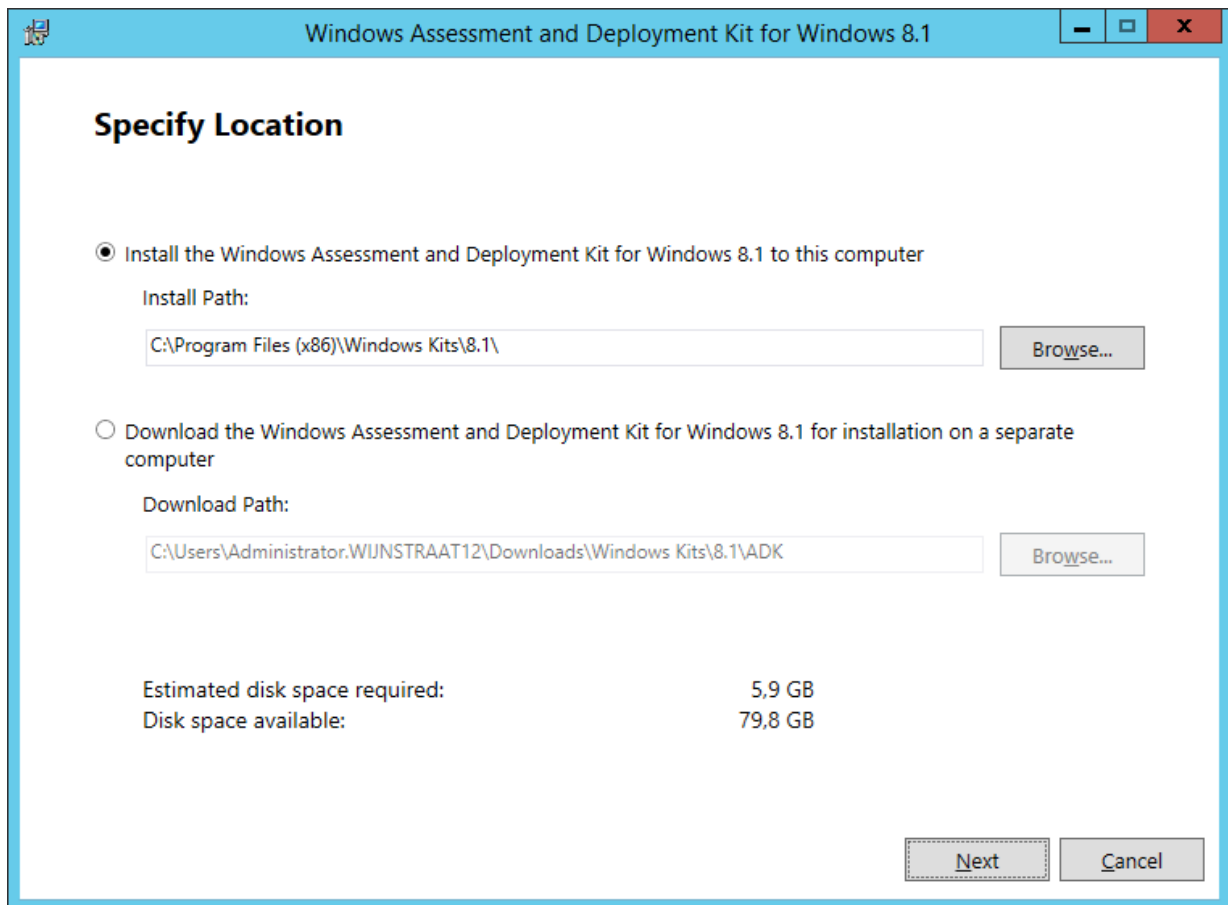


Figure 4.25: Install the ADK on the current compute, since VMM will also be installed on this local computer.

Choose whether or not you want to participate with the Customer Experience Improvement Program and accept the License Agreement.

On the “Select features screen”, make sure you only select “Deployment Tools” and “Windows Preinstallation Environment”.

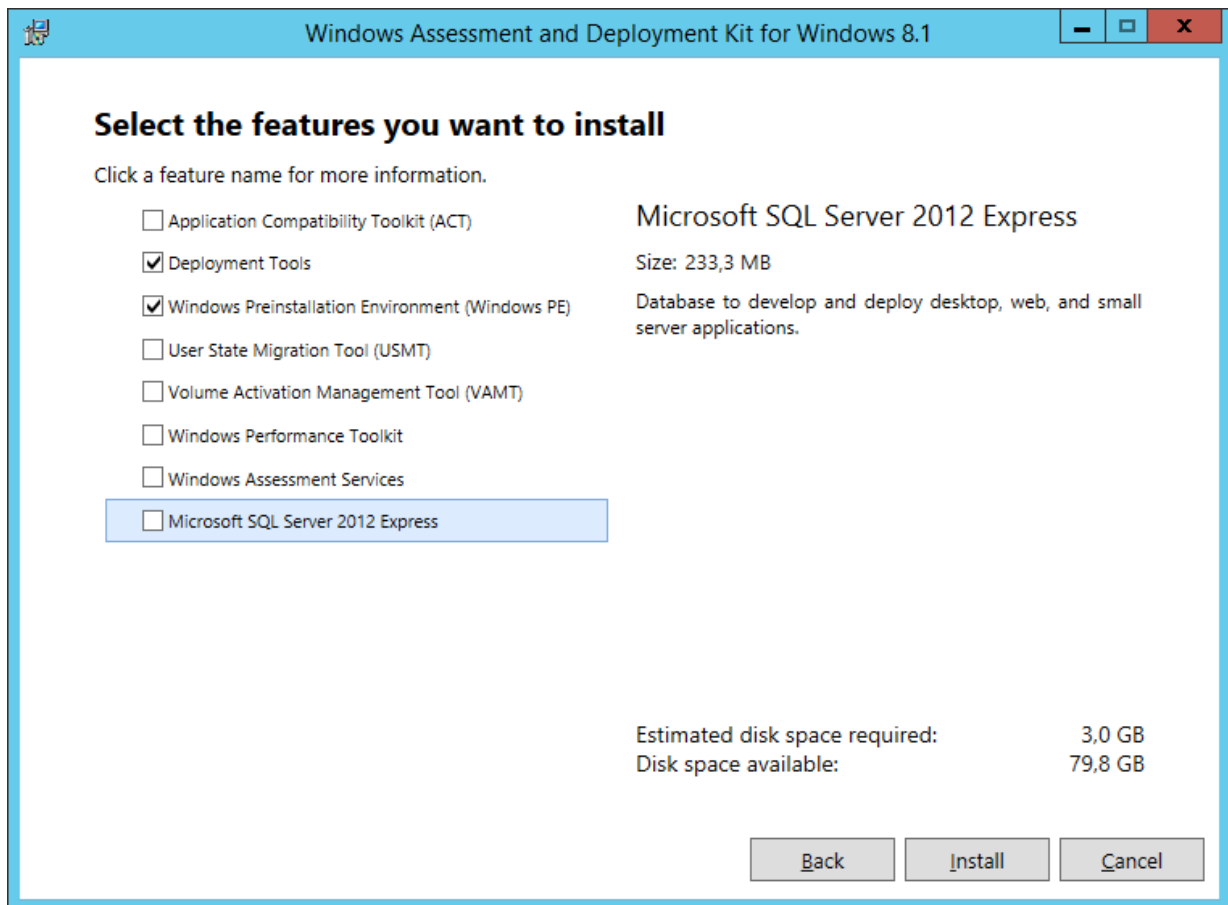


Figure 4.26: Install only the Deployment Tools and Windows PE.

Now the actual installation of SCVMM can be started. To do so, double click on the .msi file that has been downloaded from the Microsoft site. After extracting the files, open the folder and double click on `setup.exe`. The main screen of SCVMM is shown.

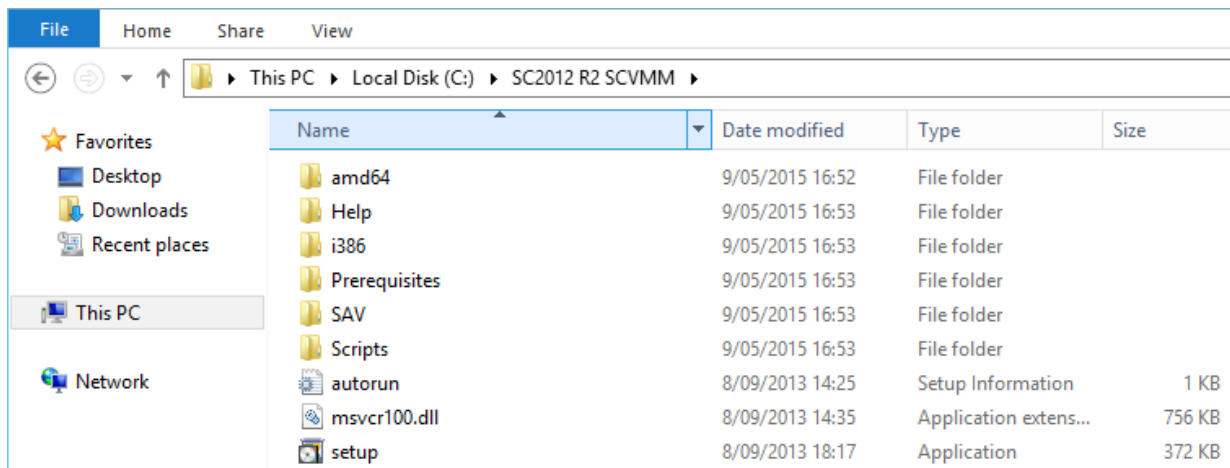


Figure 4.27: Extract the files and double click on `setup.exe`.

Since we want to install VMM, choose for `Install`.



Figure 4.28: The main screen of Virtual Machine Manager 2012 R2 is shown.

Select **VMM management server**, the **VMM console** is automatically selected as well. The console is the Graphical User Interface of Virtual Machine Manager that allows one to connect to the VMM management server.

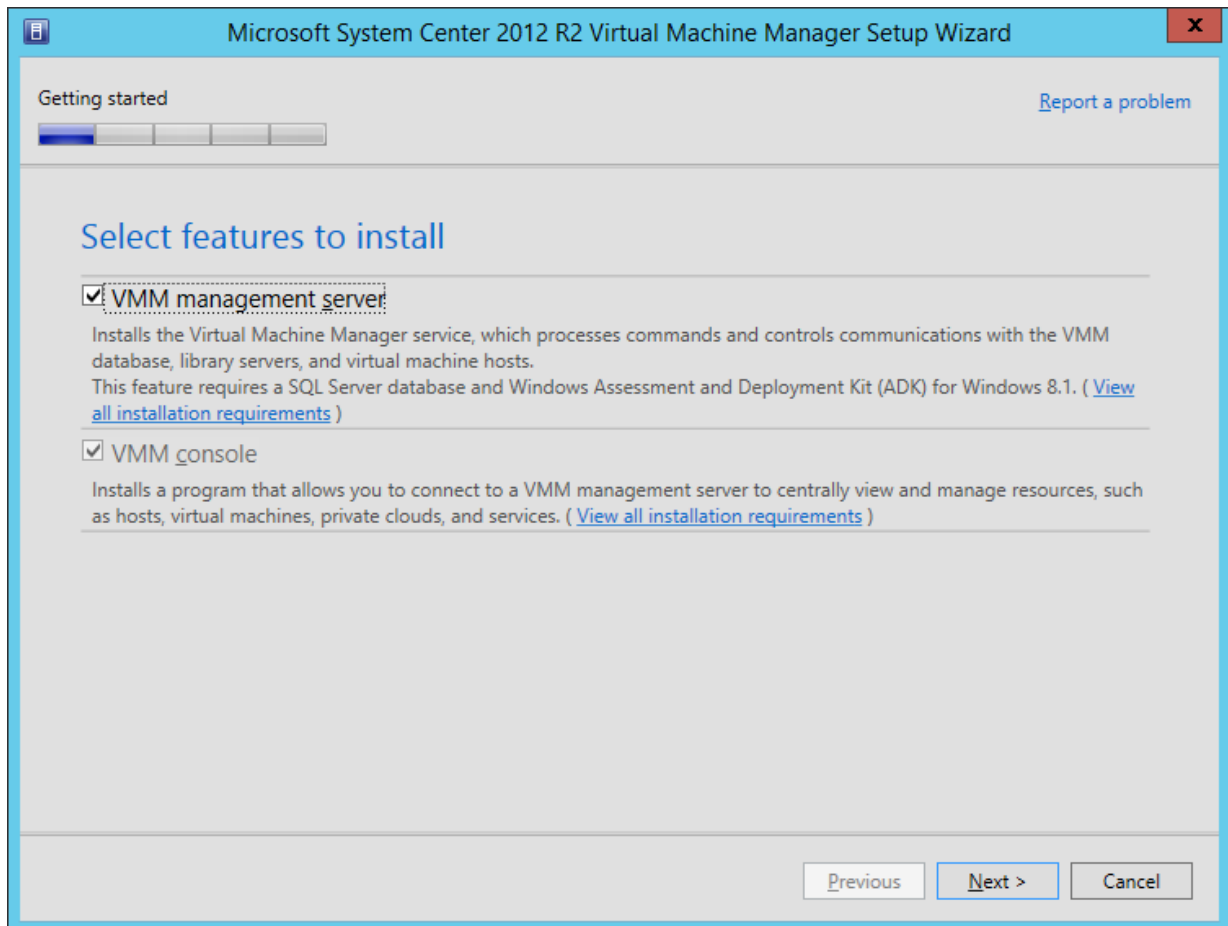


Figure 4.29: Select the VMM management server.

Next, the installation location has to be chosen.

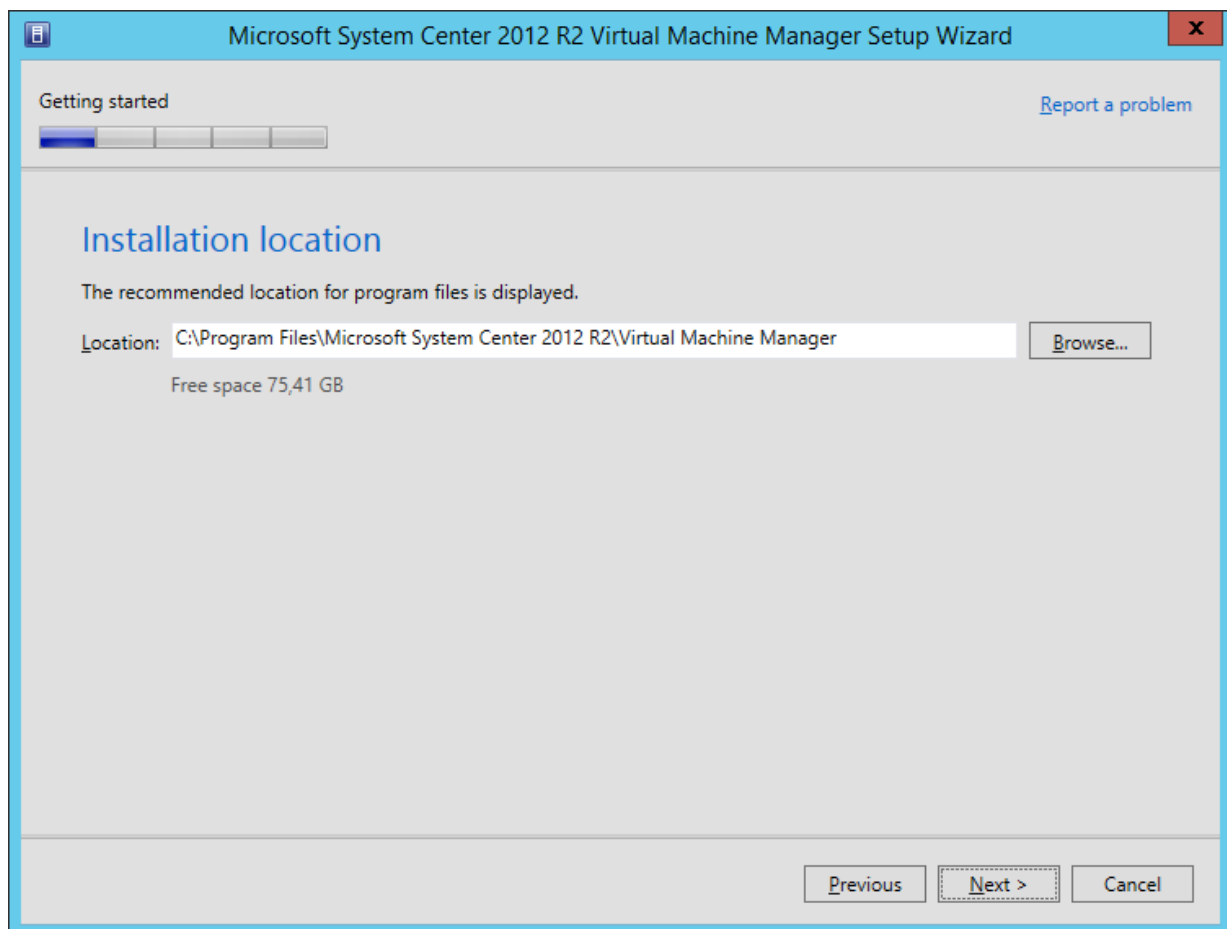


Figure 4.30: Choose the installation location.

On the next screen, the information regarding the database connection and configuration has to be provided. On the **Server name** field, “VMMTEST” or “localhost” are both valid names. Leave the **Port** field empty. The default port is used.

We want to login using the VMMService account. This is why we created the login in the previous section. Enter its name and password. Make sure to also provide the NETBIOS domain name of the account in capital letters, followed by a backslash (\) before the account name. An example could be: WIJNSTRAAT12\VMMService.

Specify the **Instance name** (“MSSQLSERVER” by default) and select **New database**.

The screenshot shows the 'Database configuration' step of the Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard. The window has a blue title bar and a 'Report a problem' link in the top right. A progress bar at the top indicates the current step. The main content area is titled 'Database configuration' and contains the following fields and options:

- Server name:** A text box containing 'VMMTEST' and a 'Browse' button.
- Port:** An empty text box.
- ☒ **Use the following credentials**
- User name and domain:** A text box containing 'WIJNSTRAAT12\VMMService'.
- Password:** A text box with masked characters (dots).
- Instance name:** A dropdown menu showing 'MSSQLSERVER'.
- Select an existing database or create a new database.**
- ☒ **New database:** A text box containing 'VirtualManagerDB'.
- ☐ **Existing database:** An empty dropdown menu.

At the bottom right, there are three buttons: 'Previous', 'Next >', and 'Cancel'.

Figure 4.31: Configuration of the database.

Now, Distributed Key Management has to be configured. Another reason why a service account has been configured in the Active Directory. Note that DKM is optional, but if we want to configure a high availability VMM cluster in the future, the prerequisite work is already performed.

Provide the same VMMSERVICE account as used in the previous step(s). Don't forget to also specify the NETBIOS domain name.

Check **Store my keys in Active Directory** and specify the DN (Distinguished Name) of the VMMDKM container created earlier.

Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard

Configuration

[Report a problem](#)

Configure service account and distributed key management

Virtual Machine Manager Service Account

Select the account to be used by the VMM service. Highly available VMM installations require the use of a domain account.
[Which type of account should I use?](#)

☐ Local System account
☒ Domain account

User name and domain: Password:

Distributed Key Management

Select whether to store encryption keys in Active Directory instead of on the local machine. Highly available VMM installations require the keys be stored in Active Directory.

☒ Store my keys in Active Directory

Provide the location in Active Directory. For example, CN=DKM,DC=contoso,DC=com.

[How do I configure distributed key management?](#)

Figure 4.32: .

In the shared library, all your shared files such as .ISO images will be stored. Therefore, it might be a good idea to specify another destination of with more space than the default location. In this example, the default location is used.

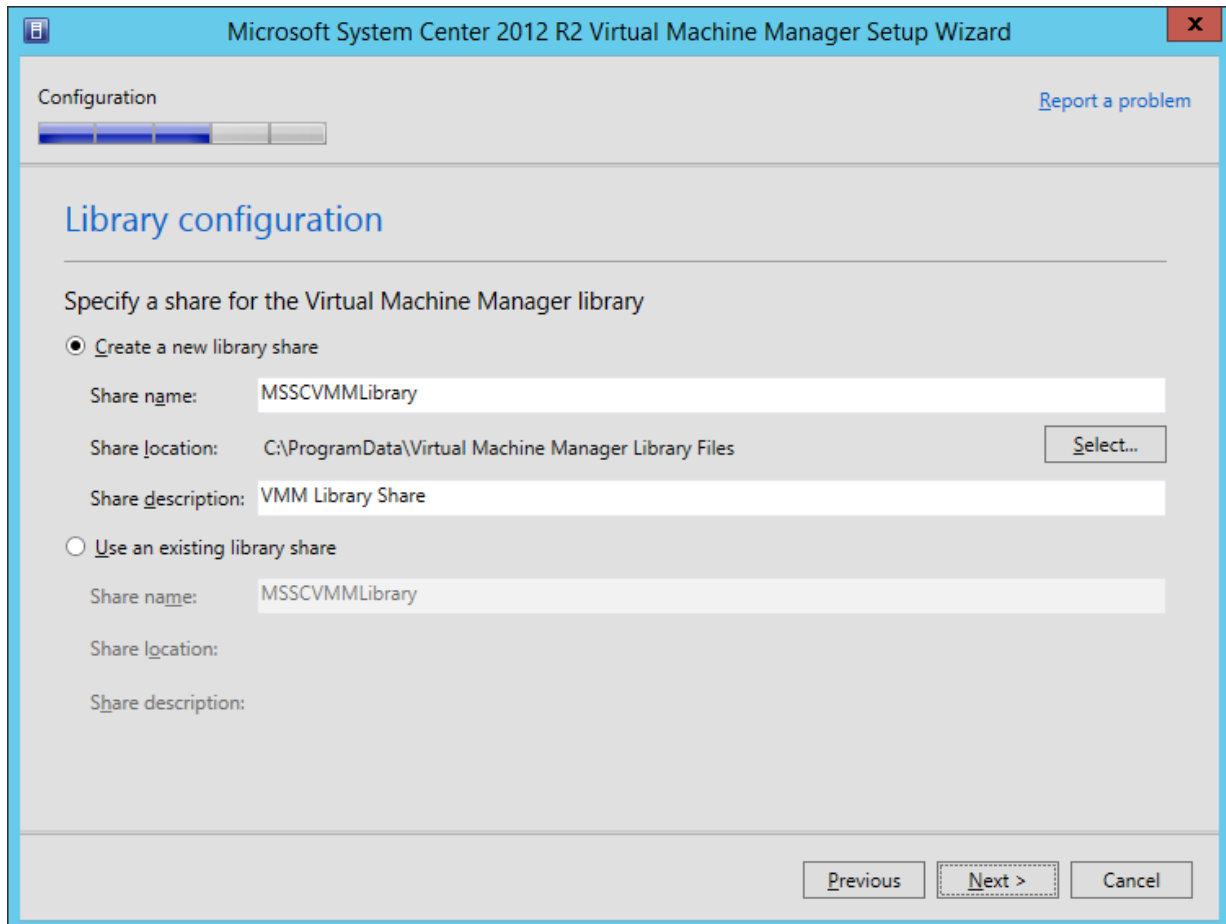


Figure 4.33: Specify the location of the shared libraries.

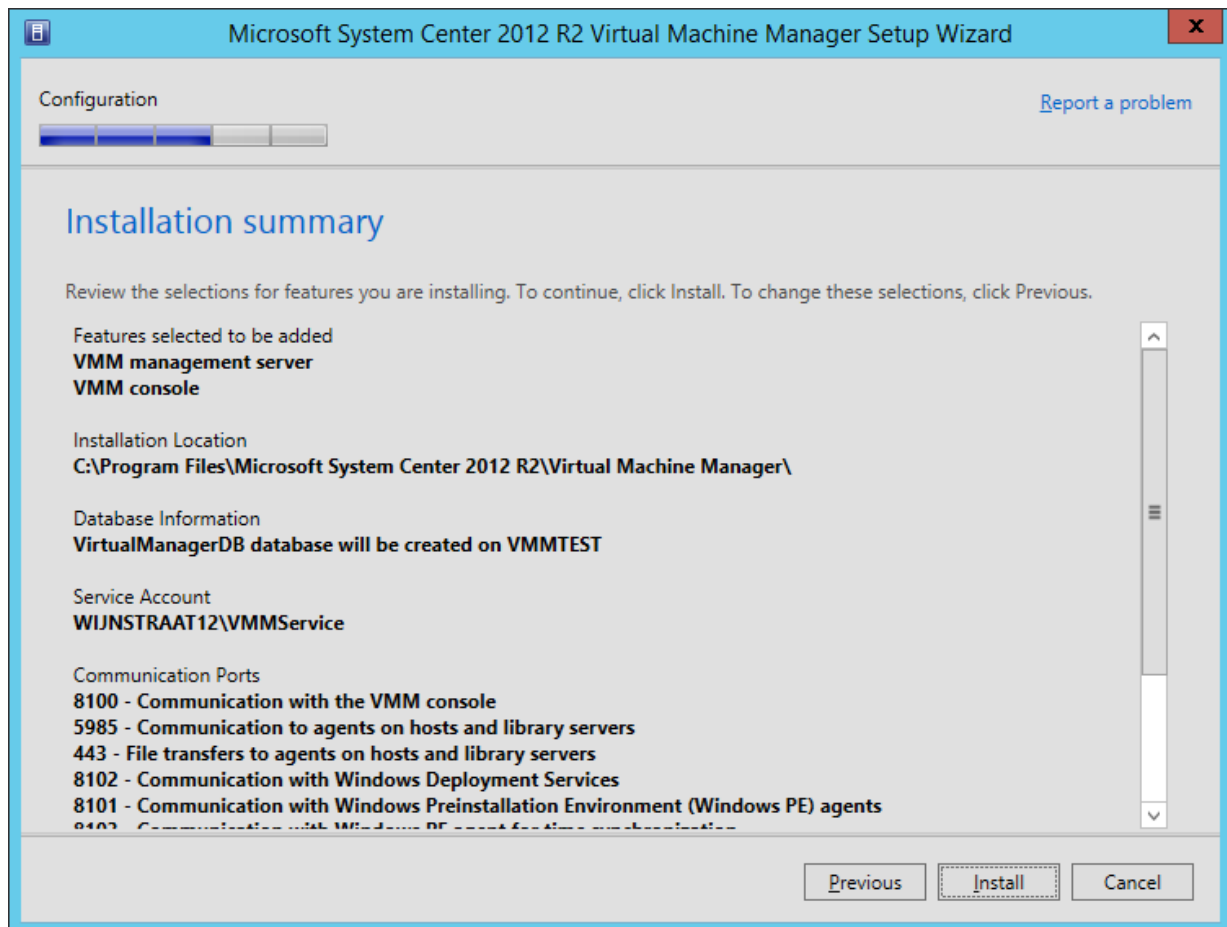


Figure 4.34: Overview of the configuration settings. Click Install.

4.2 Installation of Windows Azure Pack

Windows Azure Pack (formerly known as Windows Azure Services for Windows Server [Vredevoort, 2013]), is a collection of Windows Azure technologies that allows one to build its own private cloud and runs on top of SC Virtual Machine Manager 2012 R2 which, in his turn, runs on top of Windows Server 2012 R2. It basically brings Windows Azure to one's own datacenter [Maurer, 2014b,a].

Prior to installing Windows Azure Pack, the Service Profider Foundation (SPF) needs to be installed. It offers Infrastructure as a Service (IaaS) and is installed on top of VMM. So basically, the layered infrastructure is like this: Windows Server 2012 R2 → Virtual Machine Manager 2012 R2 → Service Provider Foundation → Windows Azure Pack.

Windows Aure Pack is installed on a dedicated machine called `windowsazure`. Windows

Aure Pack (or WAP for short) requires Microsoft SQL Server 2012 or higher. The SQL Server installed on the VMM virtual machine can be used, or a new, local, instance can be created.

4.2.1 Prerequisites

The installation of Windows Service Provider Foundation requires some additional steps to be performed prior to its installation. The following requirements must be met:

- Operating System: Windows Server 2012 or higher with PowerShell 3.0.
- System Center Virtual Machine Manager console SP1 or higher.
- Web Server IIS Server role with Scripts and Tools, Basic Security, Windows Authentication and ASP.NET 4.5.
- .NET Framework 4.5 or higher + HTTP Activation.
- Management OData IIS Extension.
- WCF Data Services 5.0 for OData V3.
- ASP.NET MVC 4

The installation of all the prerequisites will be covered in this manual. As previously said, WAP is installed on a dedicated VM with a fresh install of Windows Server 2012 R2. The server is given a static IP address and is made member of the same AD domain that the VMM server is running in. That is, `wijnstraat12.ddns.net`.

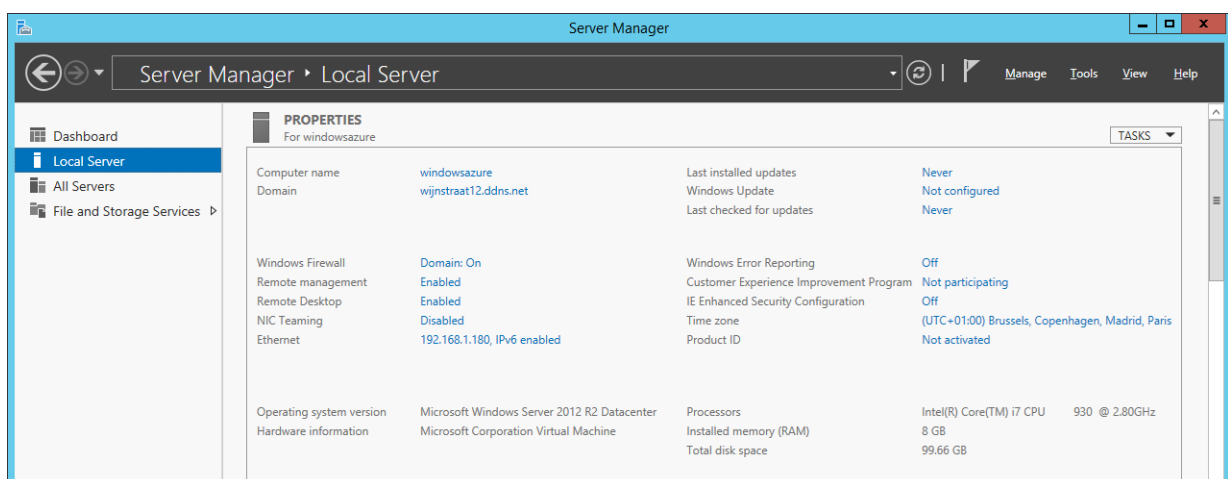


Figure 4.35: Overview screen of the local server showing the begin situation.

When choosing an installation of a new instance of SQL Server, make sure to select **Mixed Mode** as authentication mode. When reusing the existant instance of SQL Server, additional configuration will have to be performed in order to be able to install the WAP.

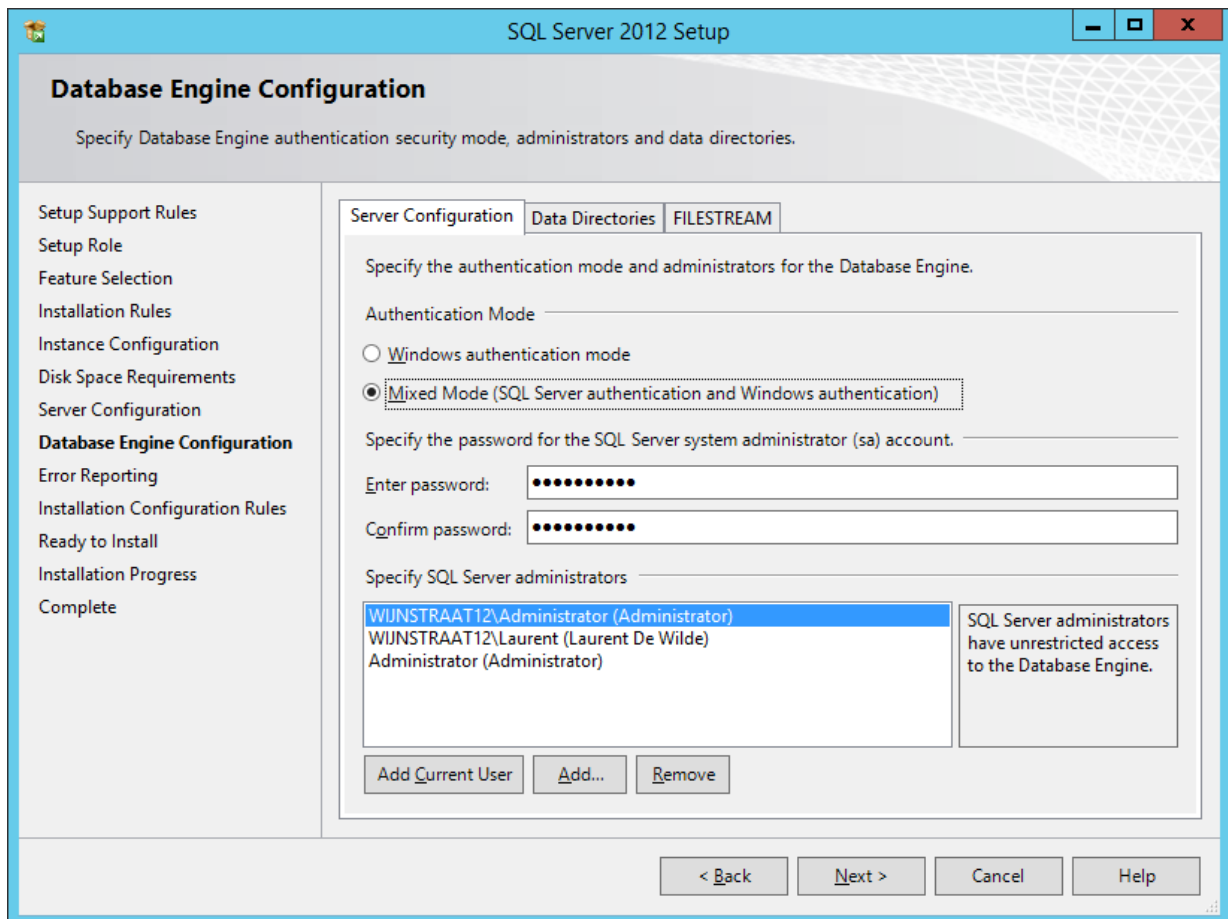


Figure 4.36: Authentication Mode: Mixed Mode.

Now the server is ready to install the prerequisites. The installation of the VMM console is the first requirement and can be installed from the VMM installation media. Extract the files of the .msi file and launch `setup.exe`. Choose **Install** and check **VMM console**. Click **Install** on the confirmation screen.

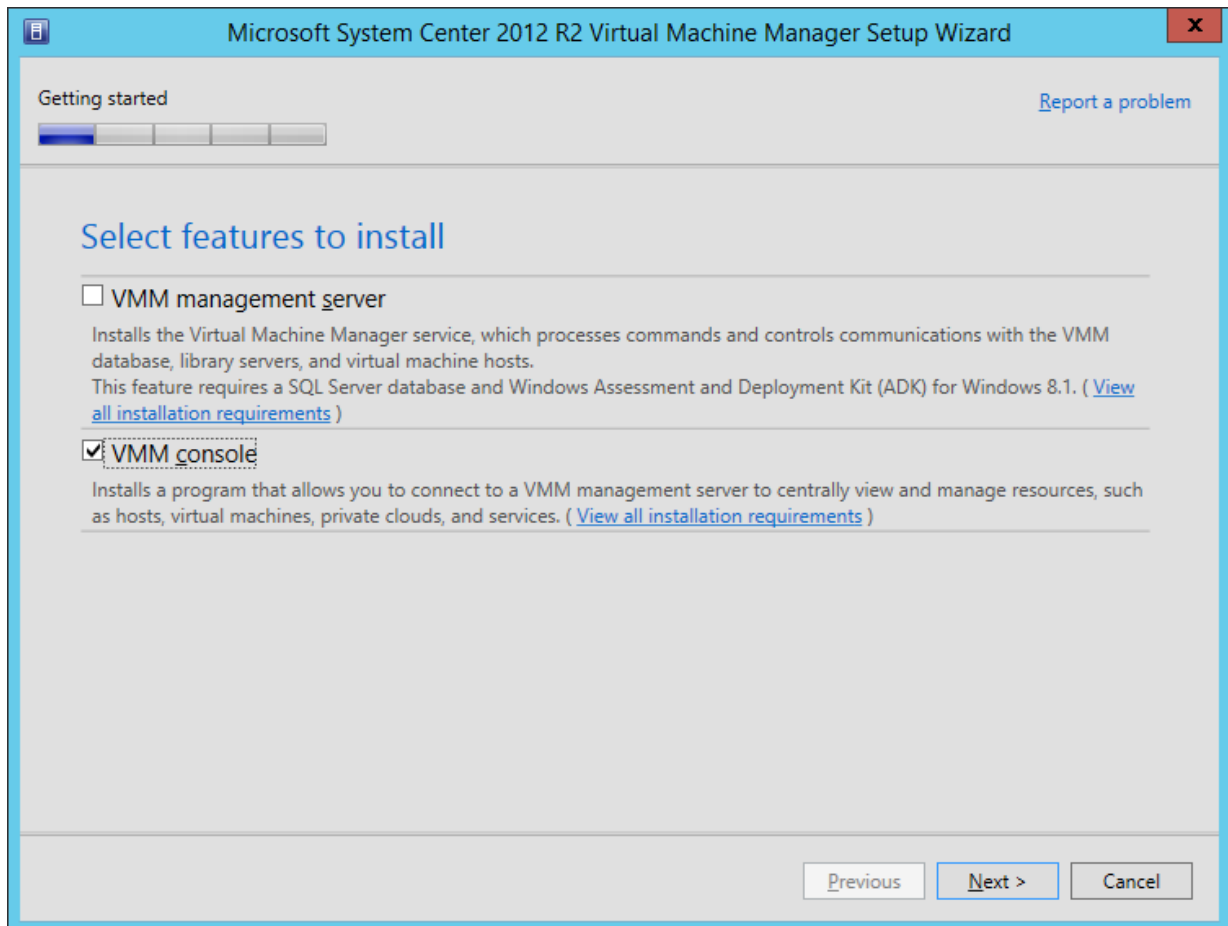


Figure 4.37: Install only the VMM console.

Next step is the installation of the Web Server (IIS). Therefore, open Add roles and services from the Server Manager and check Web Server (IIS). Click Next.

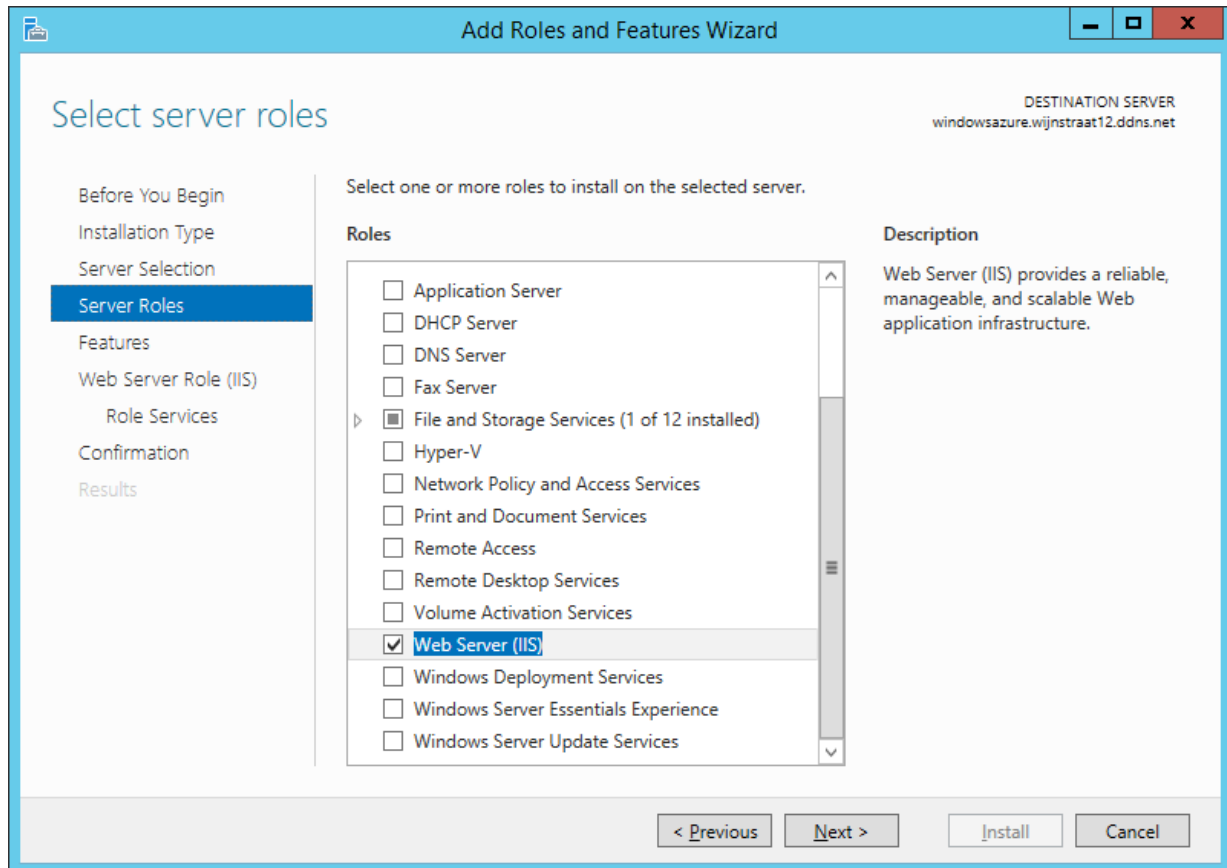


Figure 4.38: Select the Web Server (IIS) Server Role.

On the Features screen, select the following features:

- .NET Framework 4.5 Features → WCF Services → HTTP Activation
- Management OData IIS Extension and its associated features.

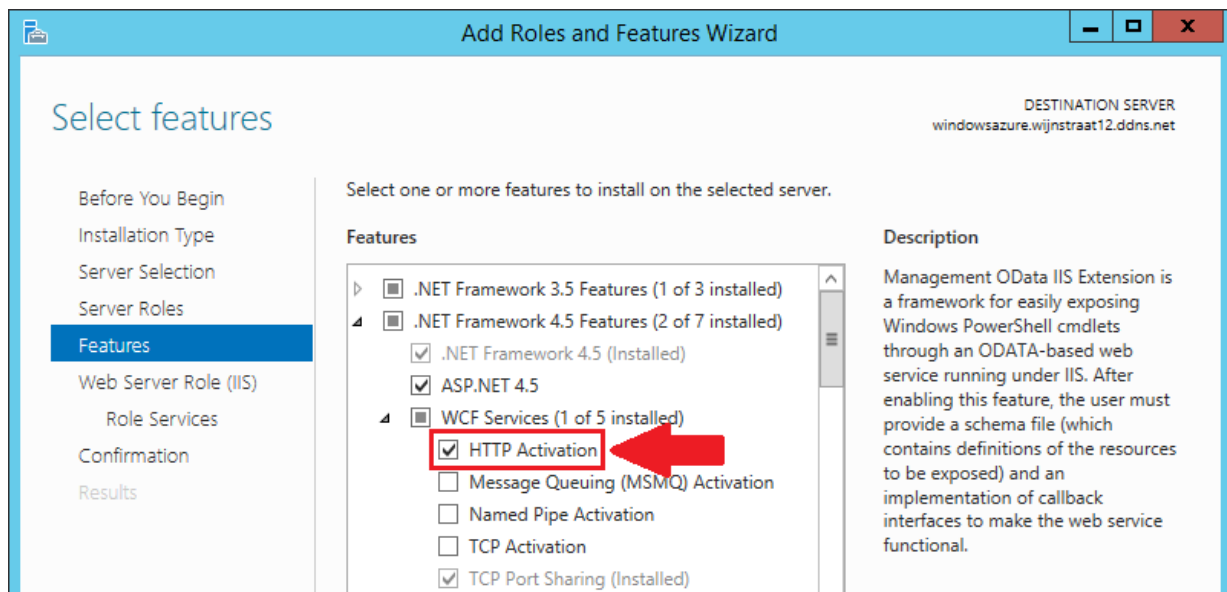


Figure 4.39: Select HTTP Activation.

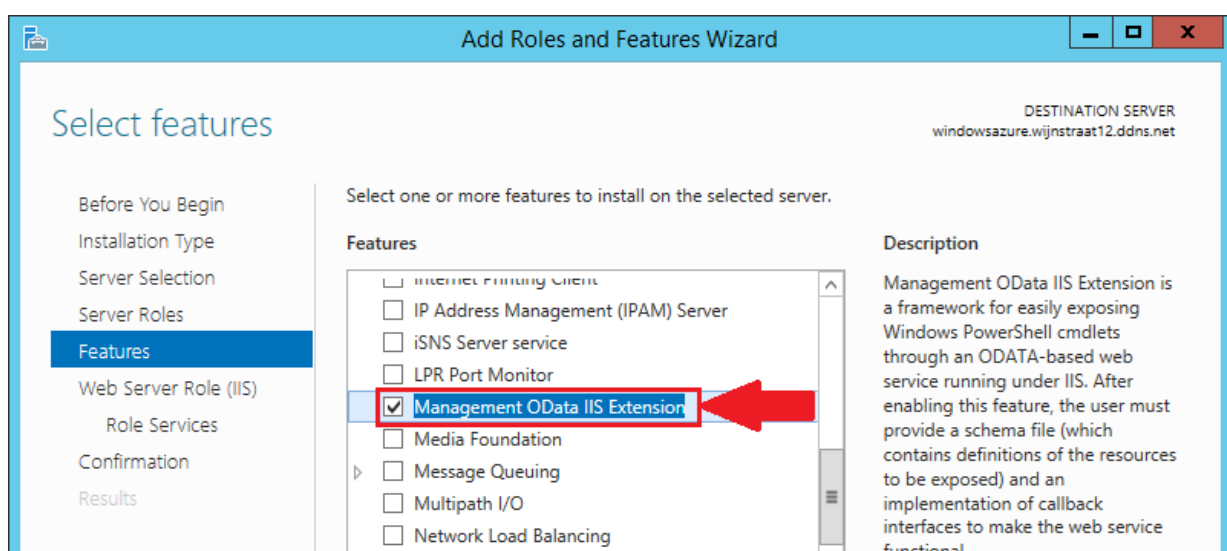


Figure 4.40: Select Management OData IIS Extension.

On the Web Server Role (IIS) – Role Services screen, select following role services:

- IIS Management → Scripts and Tools
- Security → Basic Authentication
- Security → Windows Authentication
- Application Development → .NET 4.5

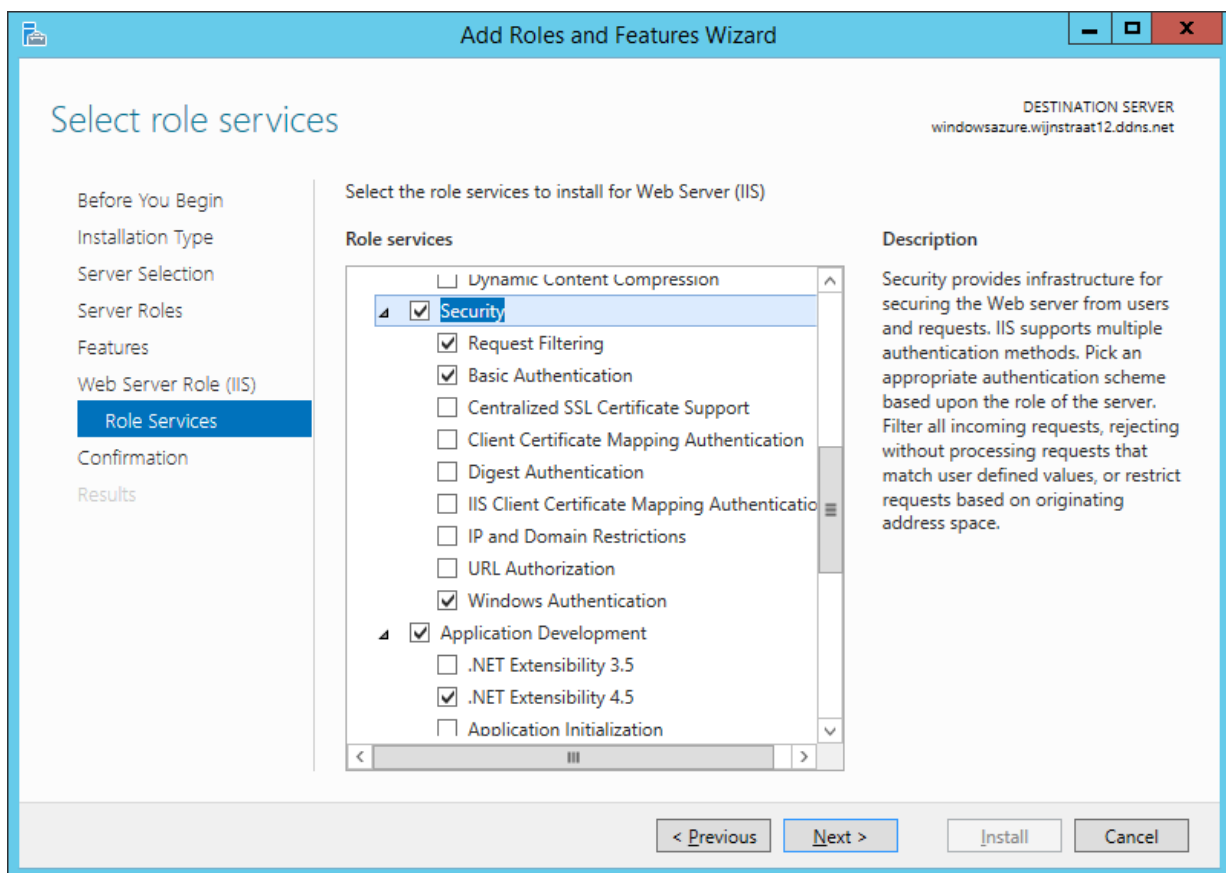


Figure 4.41: .

Some additional software needs to be installed being WCF Data Services 5.0 for OData V3 and ASP.NET MVC 4.

The WCF Data Services 5.0 for OData V3 can be downloaded from this location: <https://www.microsoft.com/en-us/download/details.aspx?id=29306>. The installation is straightforward and will not be covered. Just execute the installer, accept the License Agreement and click Install.

ASP.NET MVC 4 can be download from the following location: <https://www.microsoft.com/en-us/download/details.aspx?id=30683>. The installation is roughly the same as the WCF Data Services.

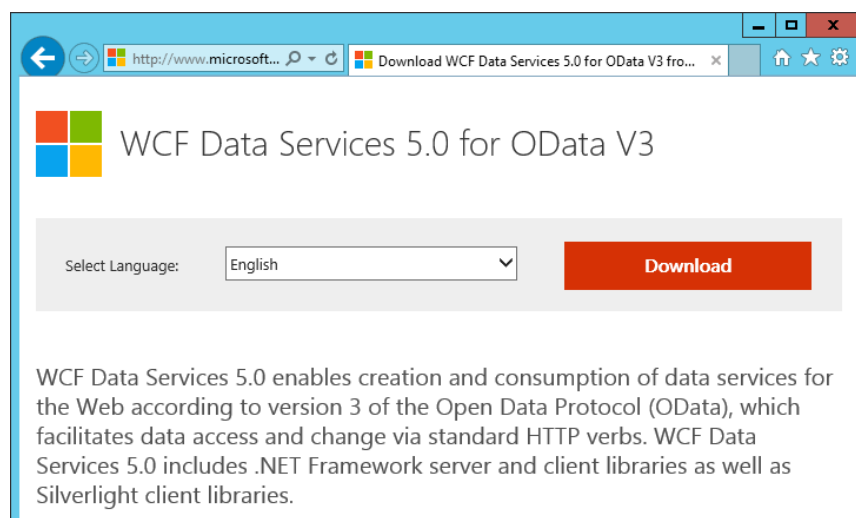


Figure 4.42: Download and install WCF Data Services for OData V3.



Figure 4.43: Download and install ASP.NET MVC 4.

Also for the Service Provider Foundation, a service accounts needs to be made. Therefore, add a domain user in the Active Directory called **SPFService**. Make sure the password never expires.

Four additional domain groups need to be made for setting permissions on the directories created by the installer. Those four groups are: **SPFAdmins**, **SPFProvider**, **SPFUsage** and **SPFVMM**.

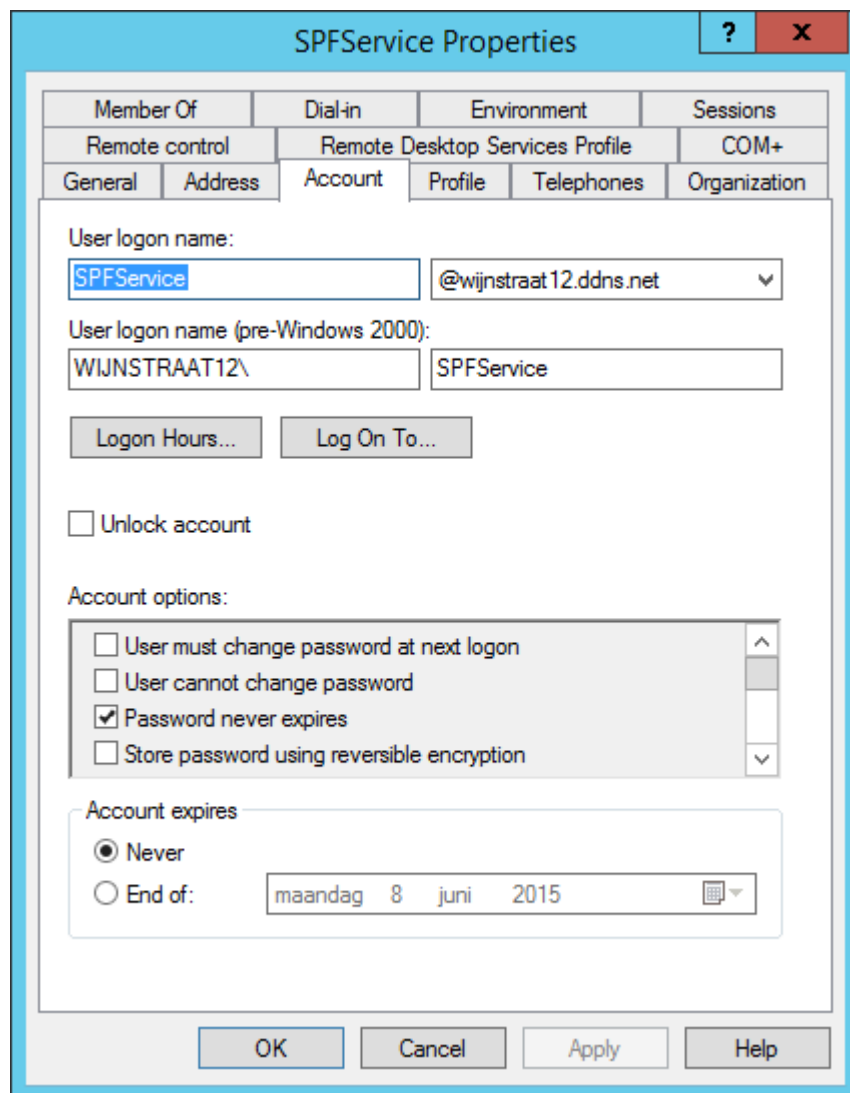


Figure 4.44: The properties of the domain account SPFService.

SPFAdmins	Security Group - Global
SPFProvider	Security Group - Global
SPFUsage	Security Group - Global
SPFVMM	Security Group - Global

Figure 4.45: The four global security groups have been made.

Communications to and from the webserver should be secured / encrypted by SSL, which requires certificates. Two types of certificates exist: self-signed certificates and certificates issued by a standalone certification authority.

In our case, the Windows Azure Pack will be installed on the same domain as the Service Provider Foundation and thus we are not required to use a public certificate issued by a standalone certification authority. So self-signed certificates will be used.

Installing such a certificate is done by using IIS Manager. Open it and select the webserver in the **Connections** pane. Next, click **Server Certificates** in the main window. On the **Actions** pane, click **Create Self-Signed Certificate**.

Specify the common name. Keep in mind that the common name must match the URL that is used when connecting to the Service Provider Foundation.

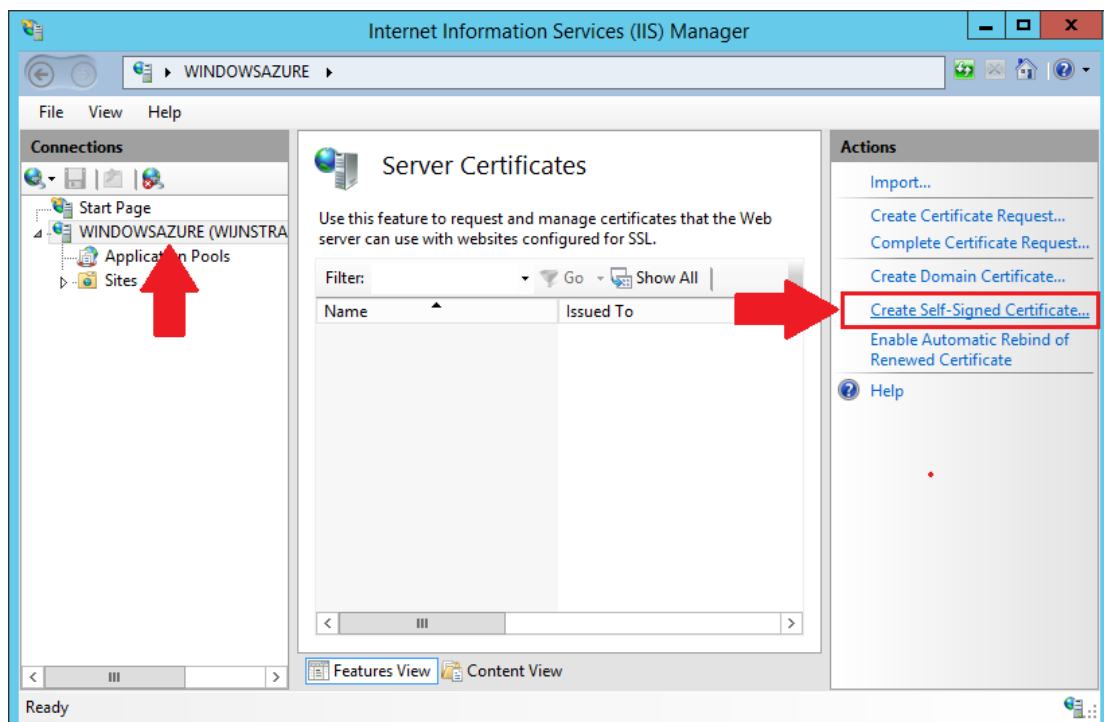


Figure 4.46: Create a self-signed certificate.

Now the installation of Service Provider Foundation can be started. The SPF can be found as a standalone installation on the System Center Orchestrator installation media. Extract the files of System Center Orchestrator, double click on `setup.exe` and select Service Provider Foundation.

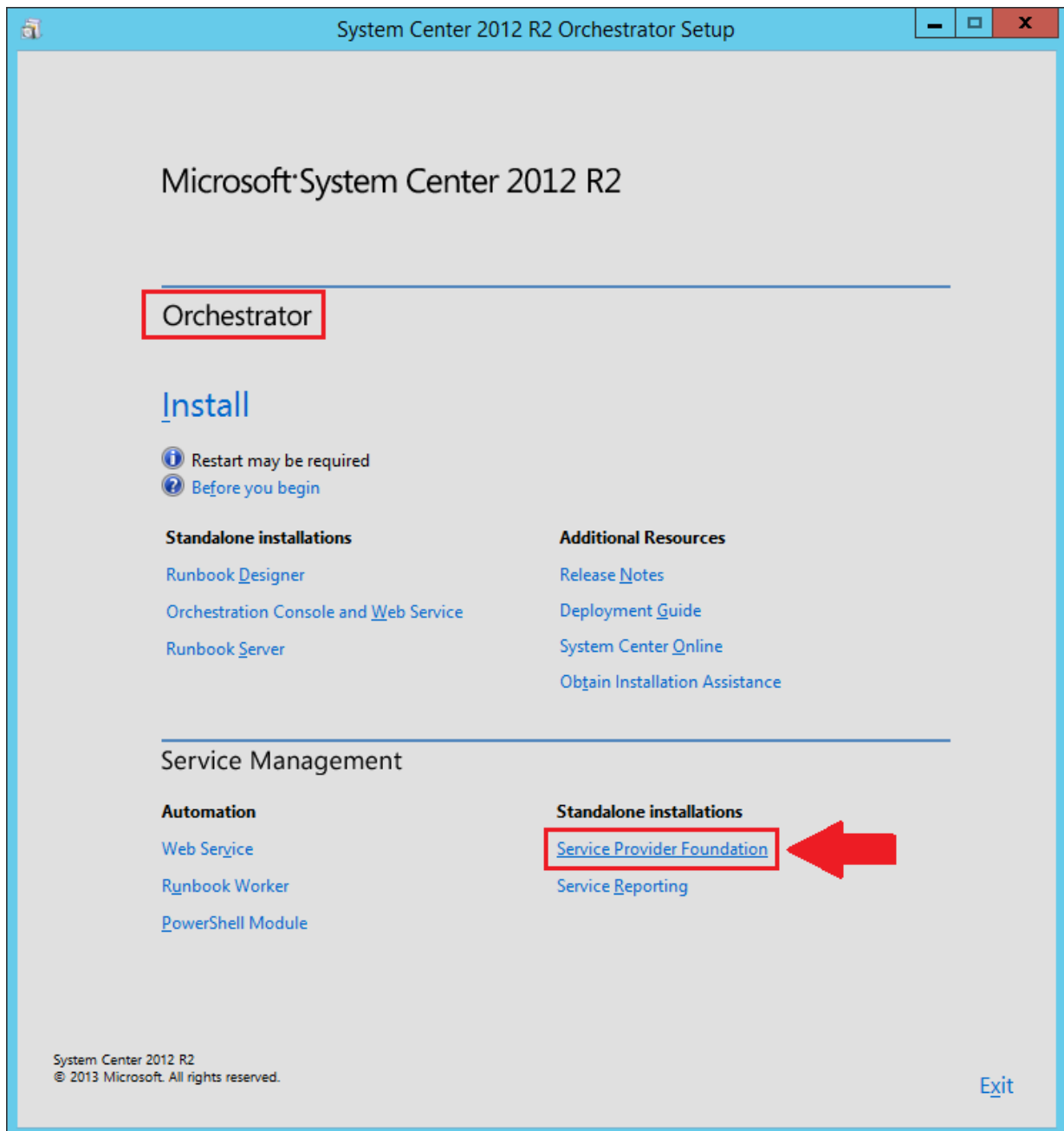


Figure 4.47: SPF can be found on the SC Orchestrator installation media.

The installer will check if all the prerequisites have been met.

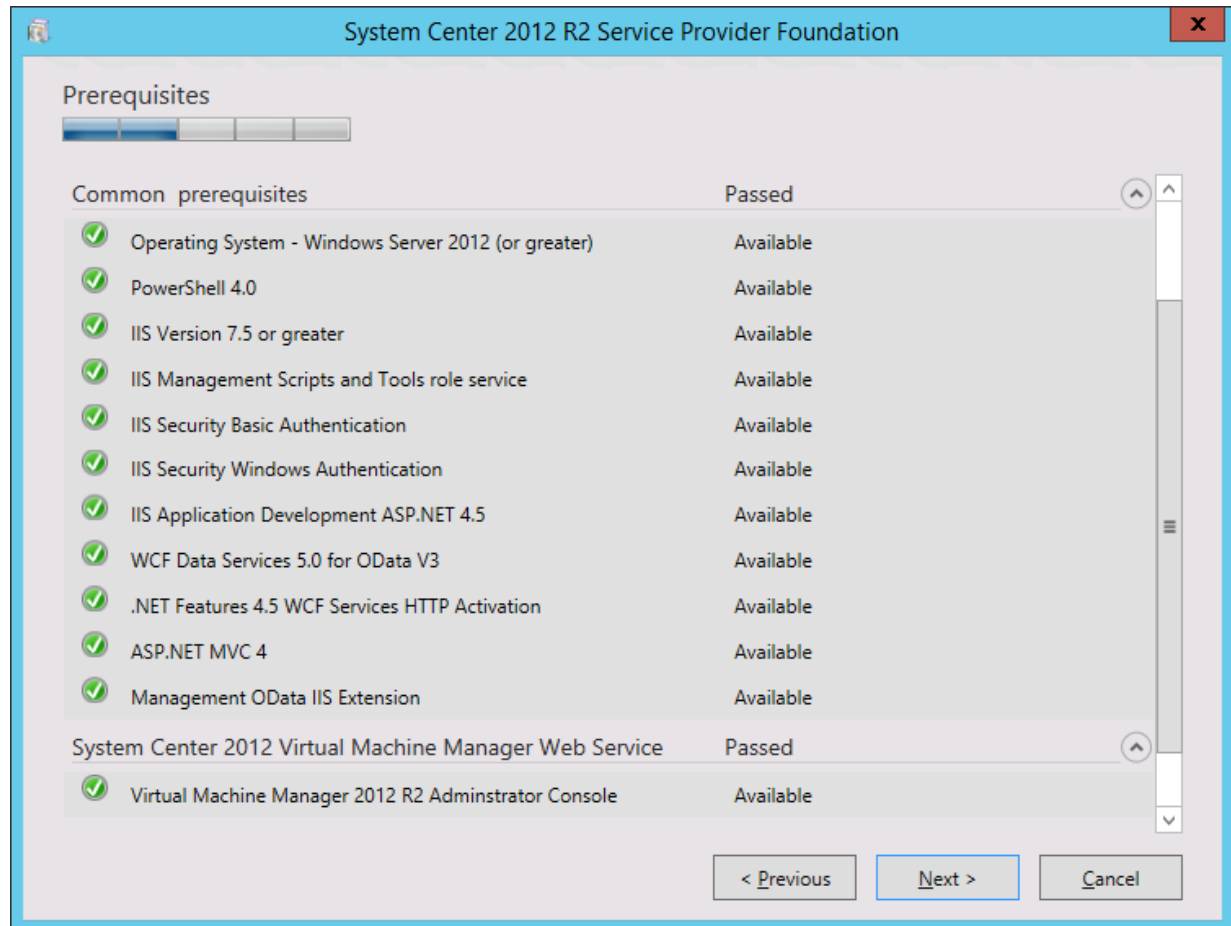


Figure 4.48: The prerequisites are checked. When everything is installed, setup can be continued.

Next, the database server location where the SPF database will be created, has to be configured. Either use the newly created, local SQL instance or use the SQL Server created earlier when setting up the VMM. In both cases, make sure the firewall allows both incoming and outgoing traffic on port 1433.

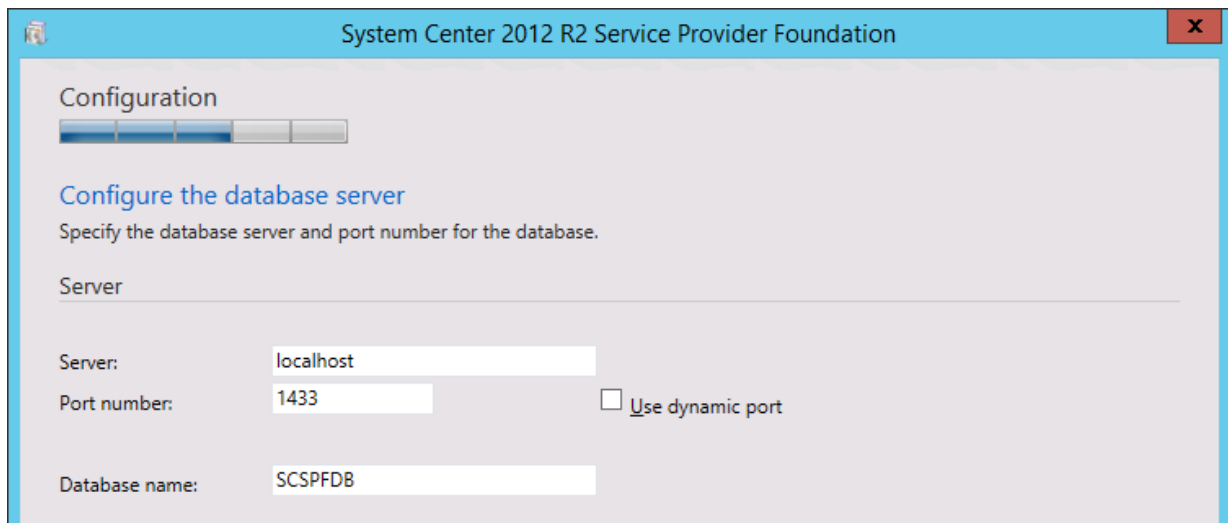


Figure 4.49: Configuration of the database. A newly created instance can be used, as well as the instance created earlier when setting up the VMM virtual machine.

Then the certificate for the web service has to be selected. Since we already created a certificate, select **Use existing certificate:** and select the correct certificate.

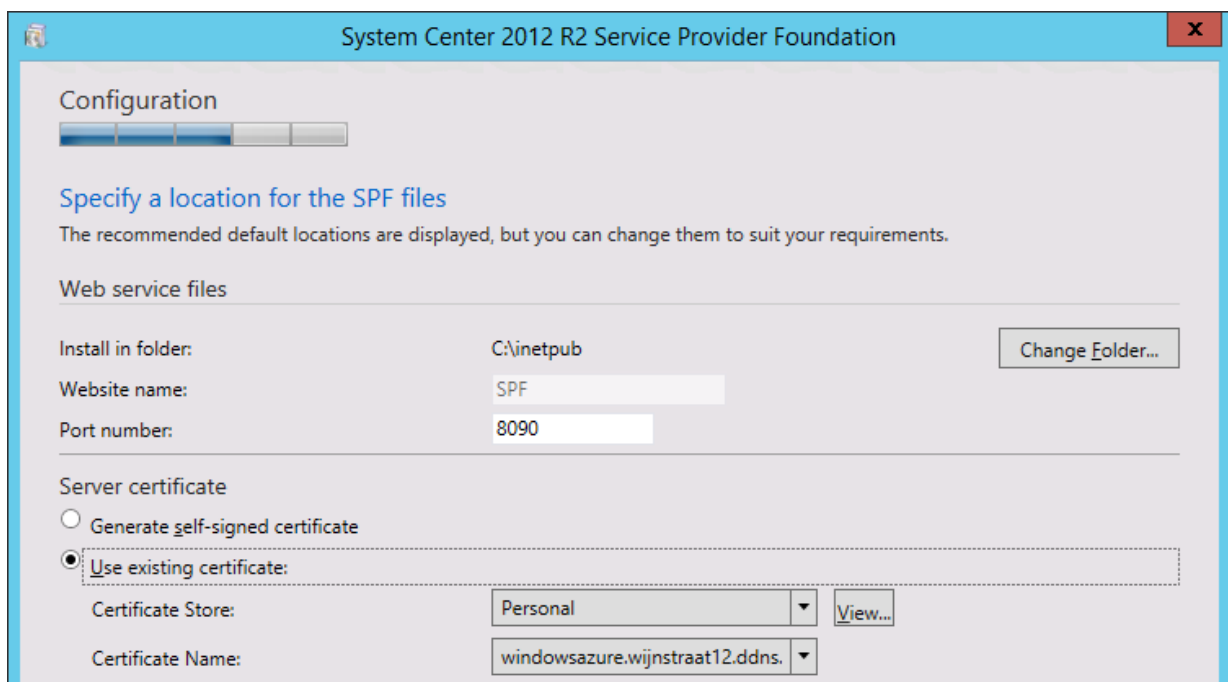


Figure 4.50: Certificate selection. Choose the self-singed certificate created earlier.

Now, the configuration of the virtual directories of IIS, permissions and App Pool Identities have to be configured. In the next four steps, the four domain groups created earlier need to be specified in each step. The service account **SPFService** is used in all steps.

The screenshot shows the 'System Center 2012 R2 Service Provider Foundation' configuration window. The title bar is blue with the text 'System Center 2012 R2 Service Provider Foundation' and a close button. The main content area is light gray. At the top, there's a 'Configuration' section with a progress bar. Below it, the title 'Configure the Admin web service' is in blue. The instructions say: 'Configure the Internet Information Services (IIS) settings for the System Center Administrator web service.' The 'Virtual directory:' field is 'Admin'. The 'Domain security groups or users:' field is 'WIJNSTRAAT12\SPFAdmins', with a note 'For example: CONTOSO\JohnDoe; CONTOSO\TestGroup'. The 'Application pool' section is expanded, showing 'Application pool name:' as 'Admin'. Under 'Application pool credentials:', the 'Service Account' radio button is selected. The 'User name:' field is 'WIJNSTRAAT12\SPFService', with a note 'For example: CONTOSO\JohnDoe'. The 'Password:' field is masked with dots. At the bottom, there are three buttons: '< Previous', 'Next >', and 'Cancel'.

Figure 4.51: Configuration of the **Admin** virtual directory of IIS. Choose the **SPFAdmin** and the **SPFService** service account, both created earlier in the pre-setup process.

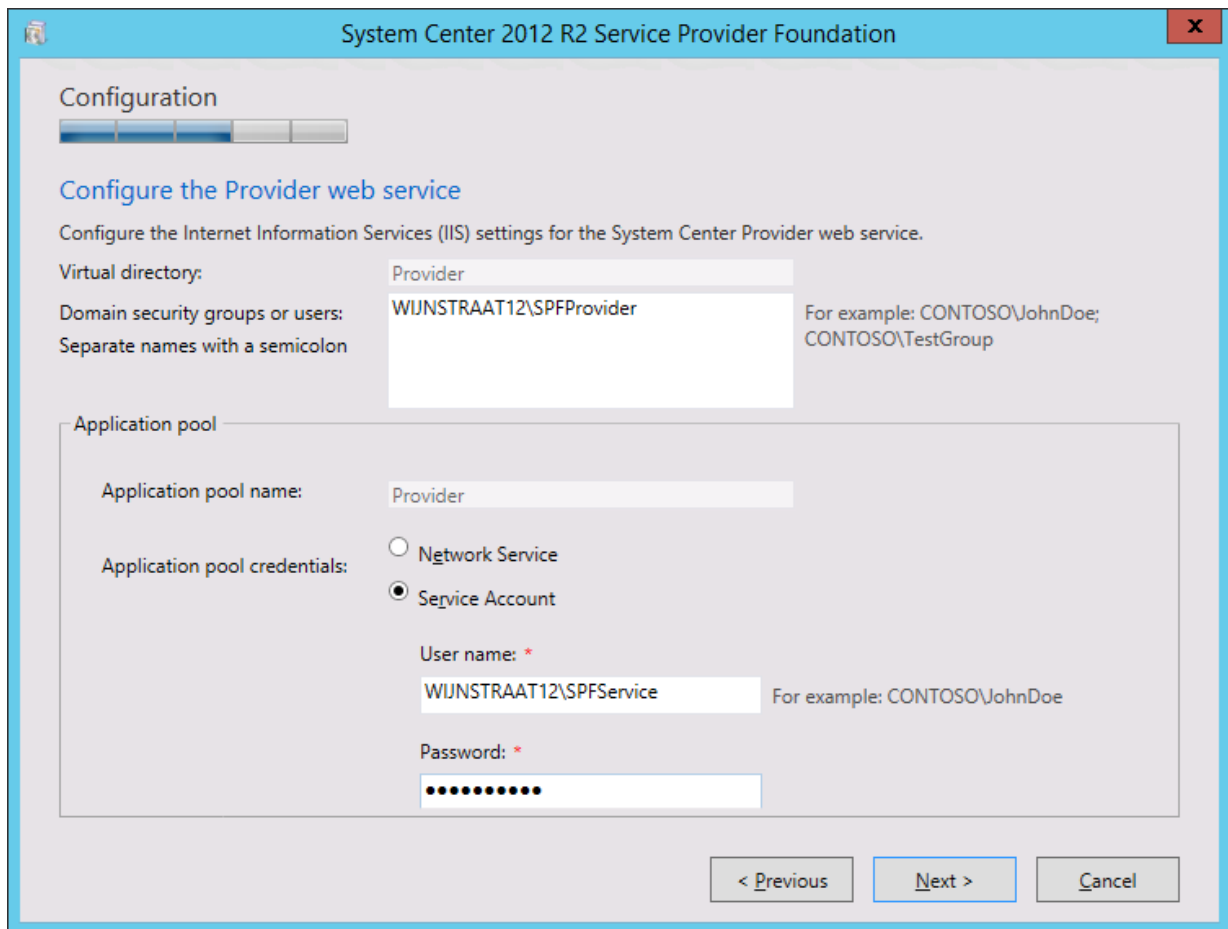


Figure 4.52: Configuration of the Provider virtual directory of IIS. Choose the SPFProvider and the SPFService service account, both created earlier in the pre-setup process.

Then the VMM web service and the Usage web service have to be specified. Use SPFVMM and SPFUsage respectively for this purposes. The service account remains the same: SPFService.

4.2.2 Post Installation of Service Provider Foundation

In order to use Windows Azure Pack correctly, some additional configuration must be performed. The SPFSERVICE account must be given additional permissions. It needs to be added as a member of the following **local** groups:

- SPF_Admin
- SPF_Provider
- SPF_Usage
- SPF_VMM

Double click on either one of them, click **Add...** and search for the SPFSERVICE account. Click **OK**. Repeat this process for the other groups.

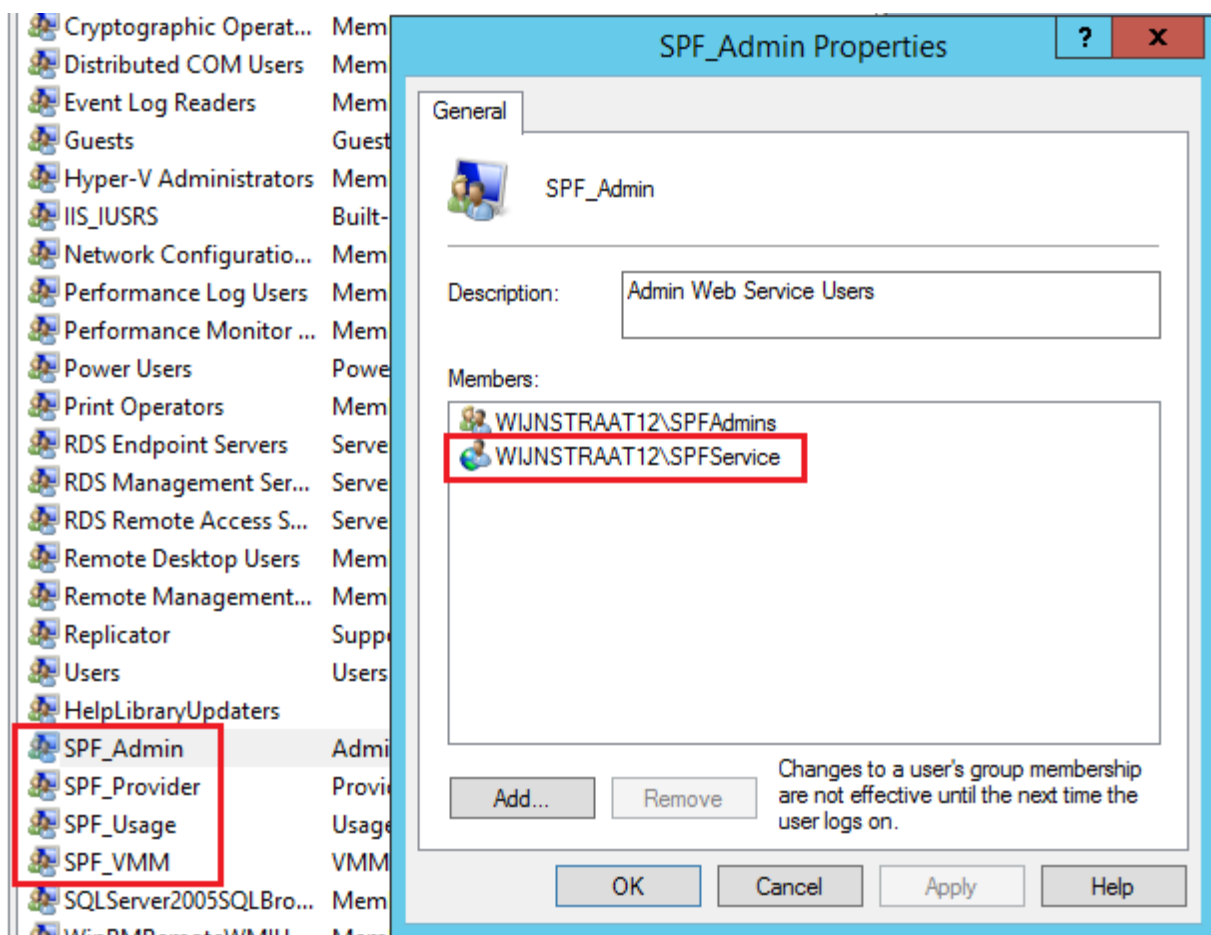


Figure 4.53: Add the SPFSERVICE account to the local groups created by the Service Provider Foundation installation.

The SPFSservice account also needs to be added to the Administrator user role in VMM. To do so, open VMM (either the console installed on this VM or on the VMM virtual machine itself). Click on **Settings** in the bottom-left corner and click on **Security** → **User Roles**. Double click on the **Administrator** user role and on the **Members** tab, click **Add...** to add the SPFSservice account to the user role.

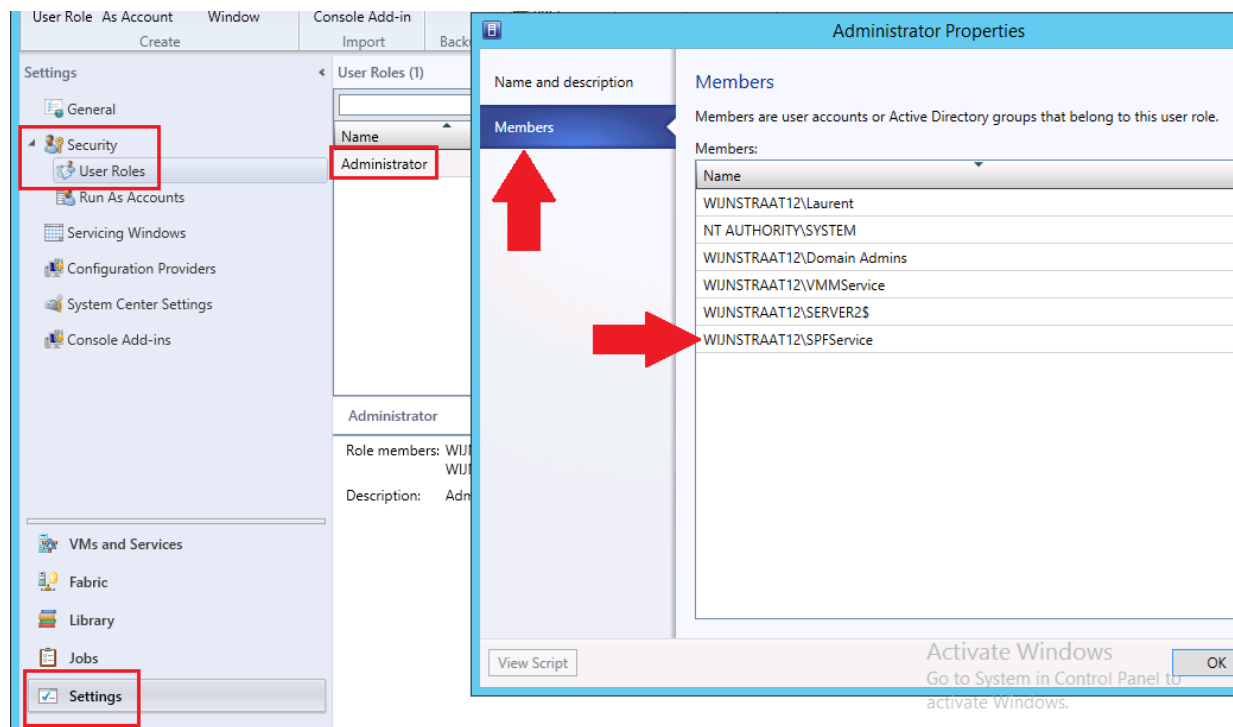


Figure 4.54: The SPFSservice account needs administrative permissions in Virtual Machine Manager.

The SPFService account needs permissions in the SQL Server as well. To set those permissions, open SQL Server Management Studio and navigate to **Security** → **Logins** and double click on **WIJNSTRAAT12\SPFService**. Select the **Server Roles** tab and check **sysadmin**.

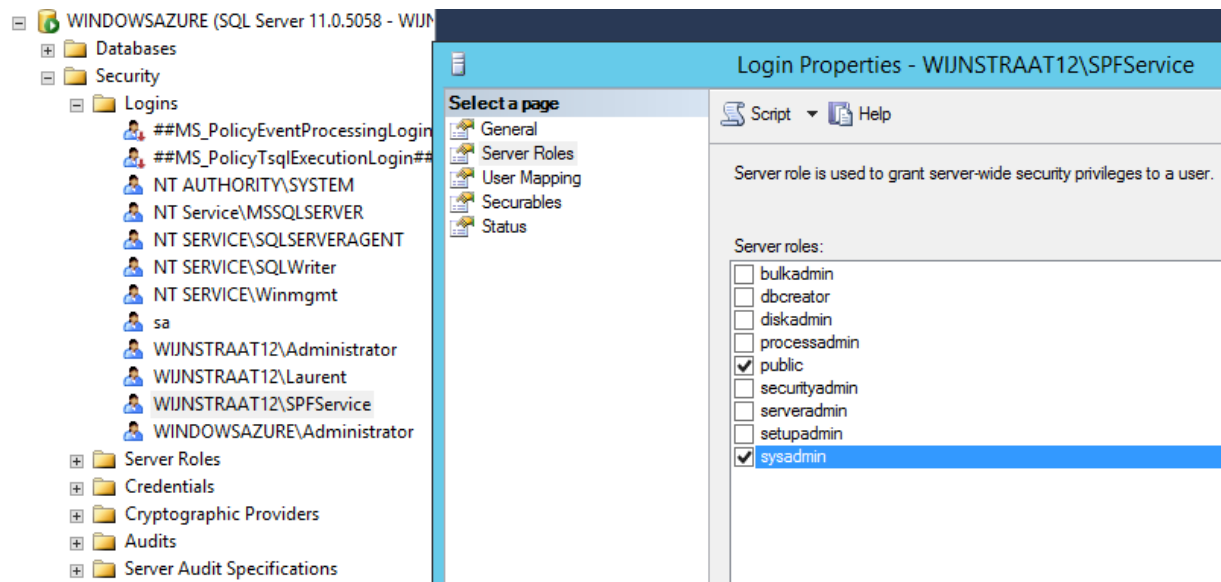


Figure 4.55: Adding administrative permissions to the SPFService account.

To verify the correct Application Pool settings of the web service, make sure that the identity of the Application Pools **Admin**, **Provider**, **Usage** and **VMM** is set to **WIJNSTRAAT12\SPFService**. To do so, open IIS Manager and select the **WINDOWS Azure** web server. In the **Actions** pane on the right, click on **View Application Pools**.

Name	Status	.NET CLR V...	Managed Pipel...	Identity
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolIdentity
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolIdentity
Admin	Started	v4.0	Integrated	WIJNSTRAAT12\SPFService
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolIdentity
Provider	Started	v4.0	Integrated	WIJNSTRAAT12\SPFService
Usage	Started	v4.0	Integrated	WIJNSTRAAT12\SPFService
VMM	Started	v4.0	Integrated	WIJNSTRAAT12\SPFService

Figure 4.56: Verifying the correct settings of the Application Pools.

To register the Service Provider Foundation in Windows Azure Pack, a **local** account has to be made on the same computer on where WAP will be installed. In our case, this is the current virtual machine we are working on.

Therefore, create a **local** user account named **SPF_REG** and make it a member of the following groups:

- SPF_Admin
- SPF_Provider
- SPF_VMM
- SPF_Usage

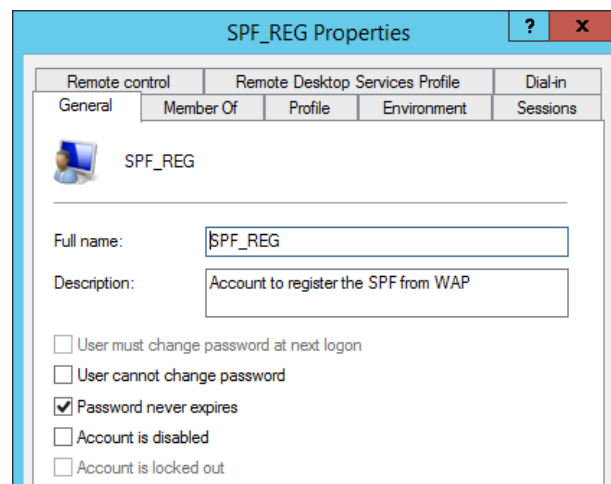


Figure 4.57: Creation of the local SPF_REG account.

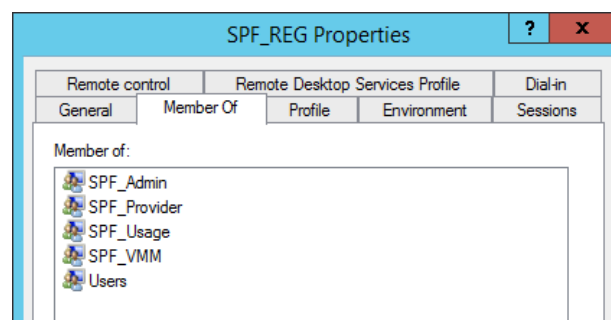


Figure 4.58: The account has been added to the four local groups created by the SPF installer.

4.2.3 Installation of the Windows Azure Pack

Two possibilities exist to install WAP: single server installation or distributed installation. The single server installation has been chosen, so this manual will focus on the installation of all the components of WAP on one server.

To install the Windows Azure Pack on a single server, download and run the Web Platform Installer 5.0, which can be downloaded from the Microsoft website: <http://www.microsoft.com/web/downloads/platform.aspx>.

On the Products tab, on the left pane select Windows Azure and add Windows Azure Pack: Portal and API Express with all its dependencies. Click Next.

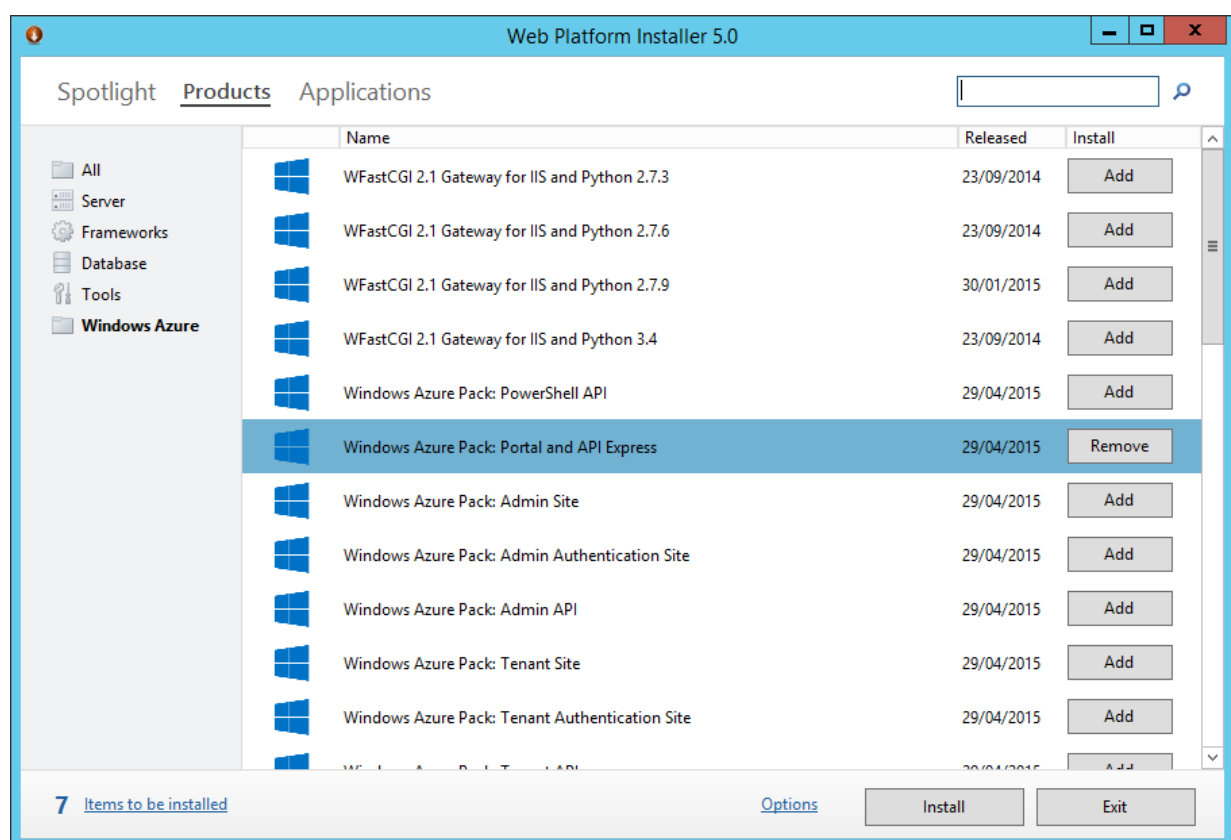


Figure 4.59: Selection of the WAP Portal and API Express.

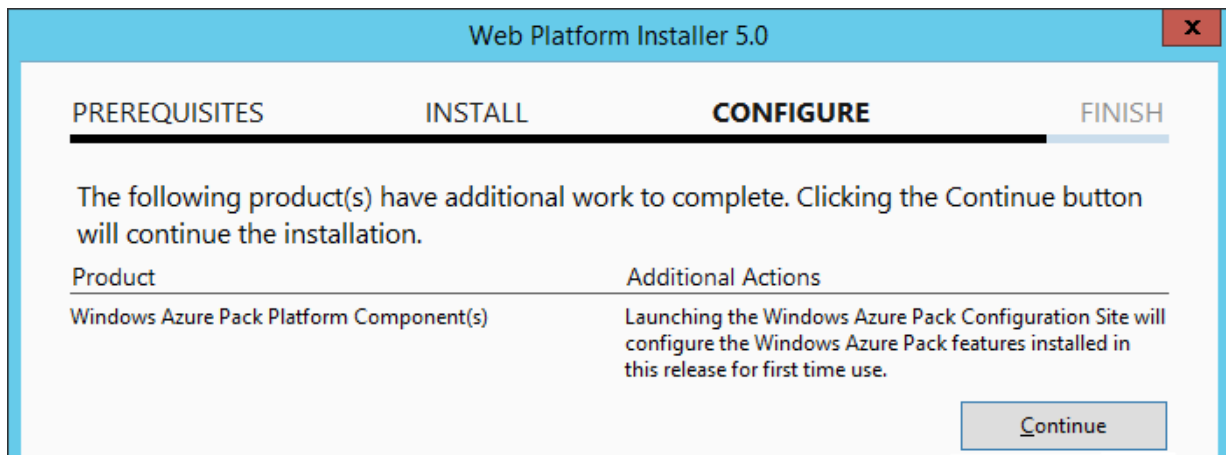


Figure 4.60: Click Next.

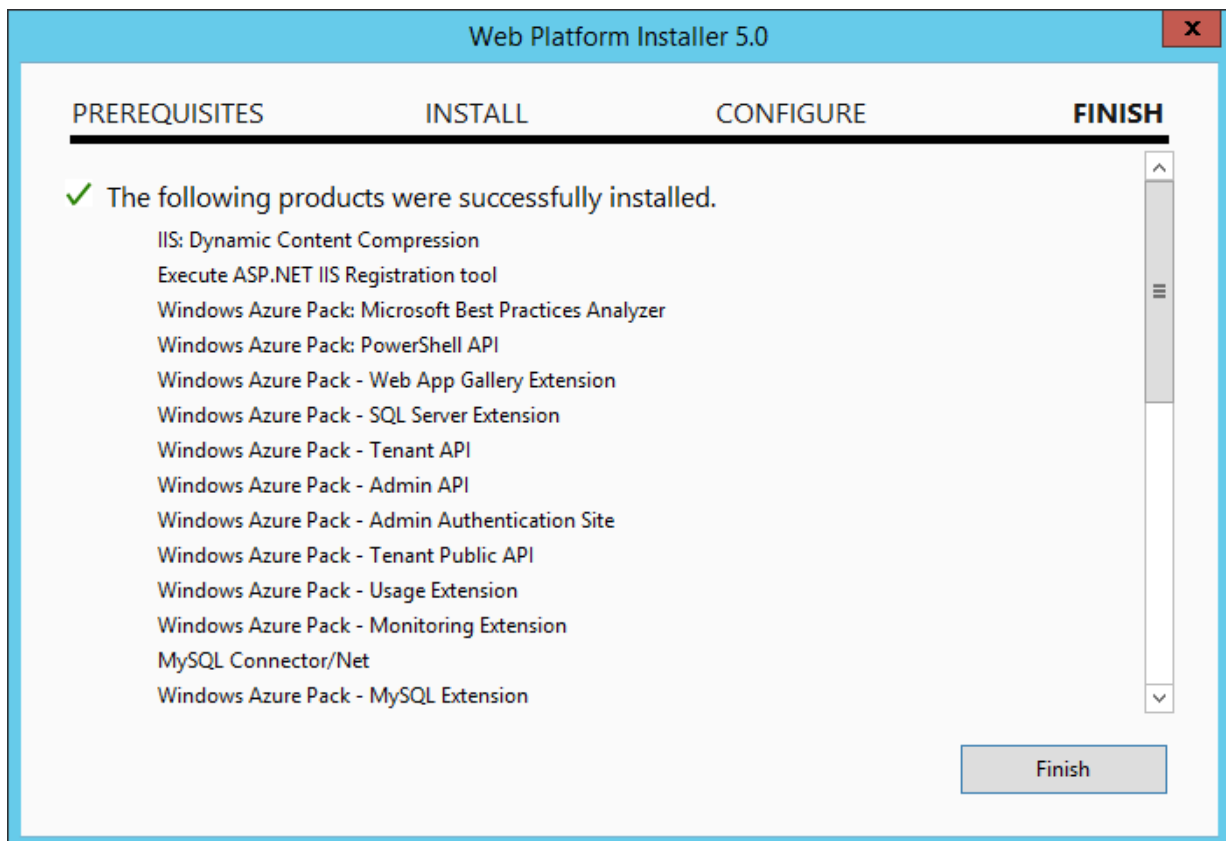


Figure 4.61: The installation has completed successfully. Click Finish.

After the installation has finished, go to <https://localhost:30101> from where the setup will be continued.

The first step is configuring the database connection which WAP will use. Fill in the appropriate server name, for example `localhost` or the name of the virtual machine that runs VMM and thus also runs an instance of SQL Server.

Choose **SQL Server Authentication** and let the database server admin name be `sa`. Fill in the password.

Then, choose a catchphrase. The use of a catchphrase requires SQL Authentication. When using an existing SQL Server instance using Windows Authentication (for example, the one configured on the VMM), setting up a catchphrase will not work. The security authentication mode needs to be changed to SQL Server and Windows Authentication mode. A guide to do so, can be found here: <https://technet.microsoft.com/en-us/library/ms188670.aspx>.

When a local instance has been created and Mixed Authentication Mode has been selected during installation, further configuration is not required.

Windows Azure Pack

WINDOWS AZURE PACK SETUP

Database Server Setup

Database Server

Please specify the SQL Server that you would like to use for the Windows Azure Pack databases. Please use the same SQL Server instance for configuring the Windows Azure Pack Admin, Tenant and Tenant Public APIs, Admin Site and Tenant Site.

SERVER NAME

AUTHENTICATION TYPE

SQL Server Authentication

DATABASE SERVER ADMIN USERNAME

DATABASE SERVER ADMIN PASSWORD

Configuration Store

Please provide a passphrase below that will be used to store and retrieve secrets from the configuration store. The same passphrase needs to be used in all machines on this deployment. Note that if the configuration store does not exist yet, the passphrase is always valid.

PASSPHRASE

CONFIRM PASSPHRASE

2 3

Figure 4.62: Configuration of the database access for use with WAP.

Choose whether or not you want to participate to the Customer Experience Improvement Program and go to the final page (3).

The **Features Setup** page shows which features will be configured. When clicking on the checkmark at the right bottom of the page, the configuration will start. When everything is configured successfully, green checkmarks will appear in before the configuration role as illustrated in the figure below.

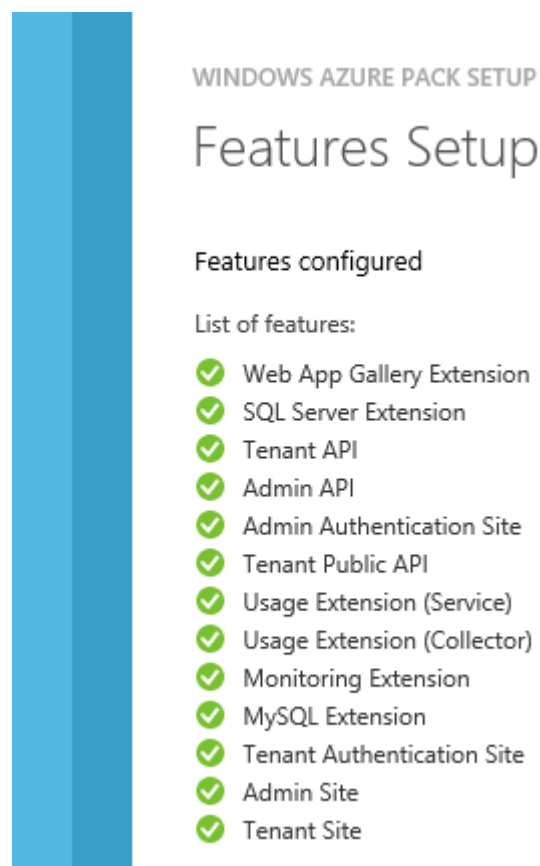


Figure 4.63: Setup has completed successfully.

The installation and configuration of WAP has been completed successfully! Now we have to login into WAP and configure a cloud.

Therefore, go to <https://localhost:30091> and log in using the **local** administrator account. To force Windows using the the local account, use a “.\” before the account name. An example would be: `.\Administrator`.

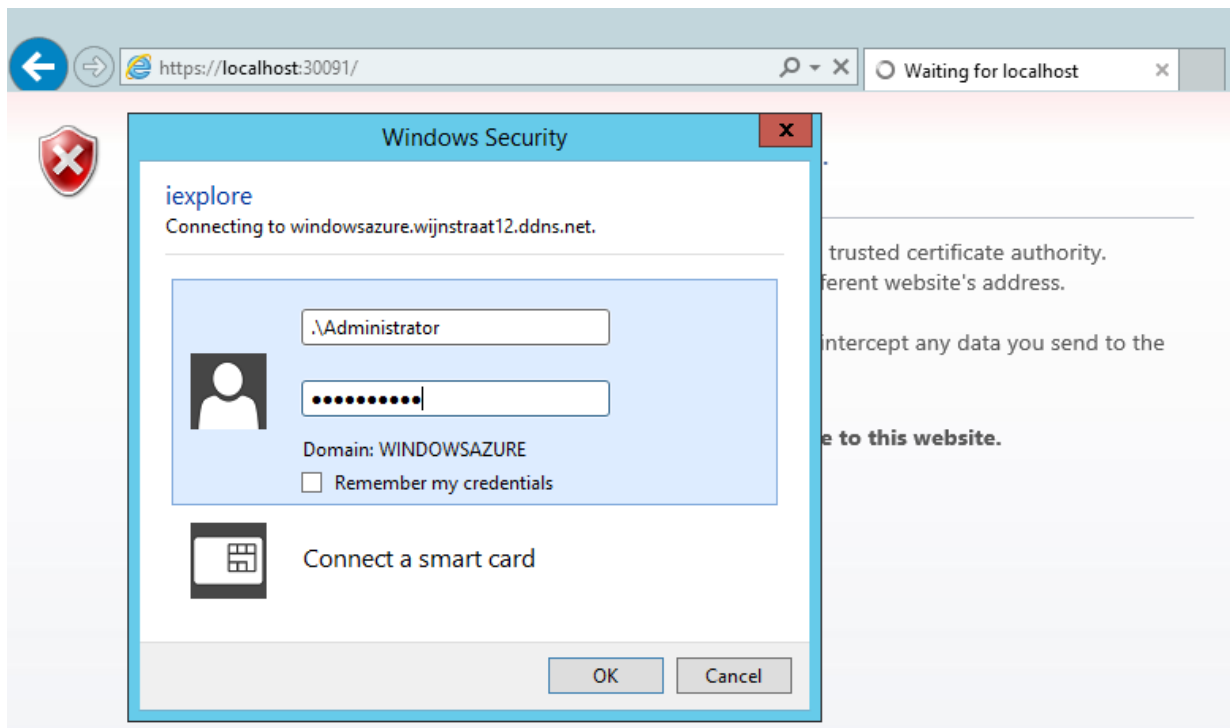


Figure 4.64: Login using the local administrator account.

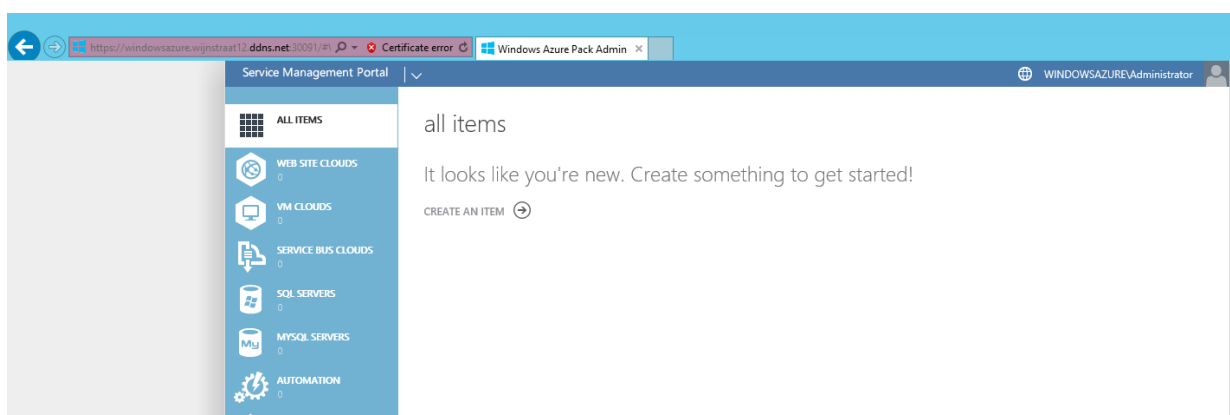


Figure 4.65: The main screen of WAP.

Now, the configuration of a VM cloud can be started. Select **VM Clouds** in the left pane. First, the Service Provider Foundation Endpoint must be registered using the local account **SPF_REG** created earlier.

However, in the past I received error messages saying that the registration of the SPF Endpoint could not be completed. The solution is as follows: reset the password of the **SPF_REG** account using the **Local Users and Groups** snap-in. Right click on the **SPF_REG** account and choose **Set password...**

After that, the IIS Web Server needs to be reset. To do so, open PowerShell and execute following command: `iisreset.exe`.



Figure 4.66: Before setting up a VM cloud, the SPF Endpoint needs to be registered.

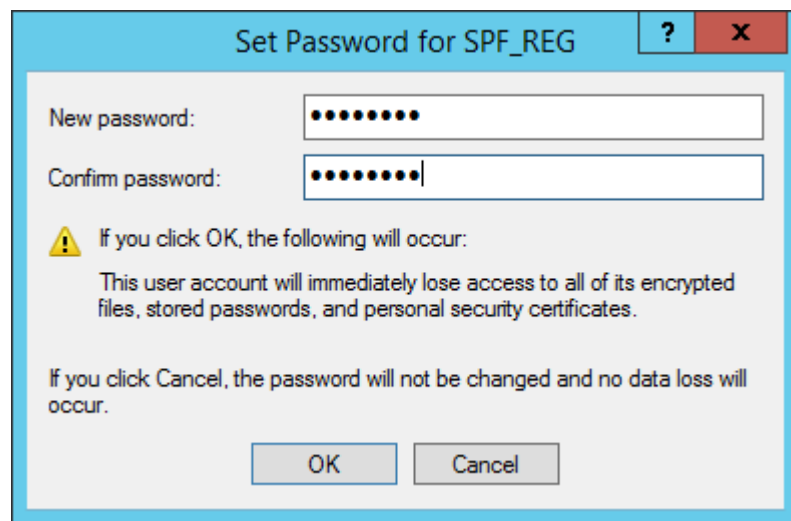


Figure 4.67: In case of failure, reset the password for the SPF_REG account.

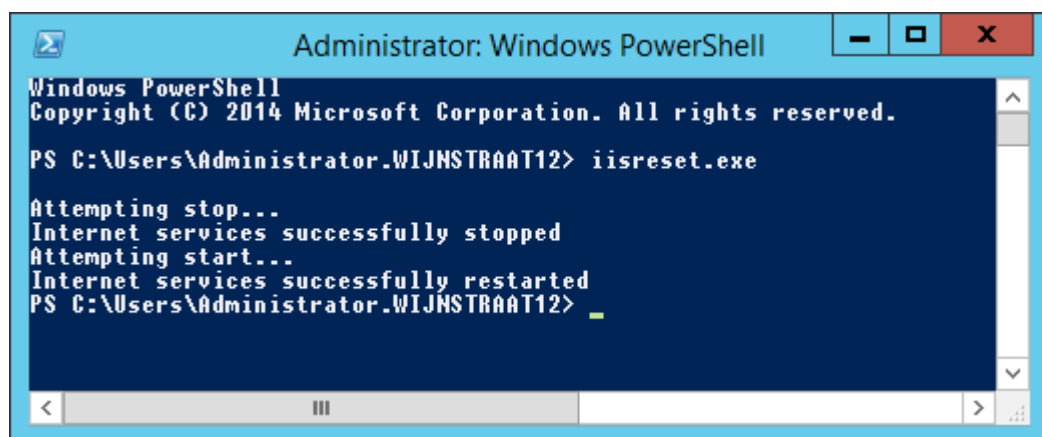


Figure 4.68: Restart the Web Server ...

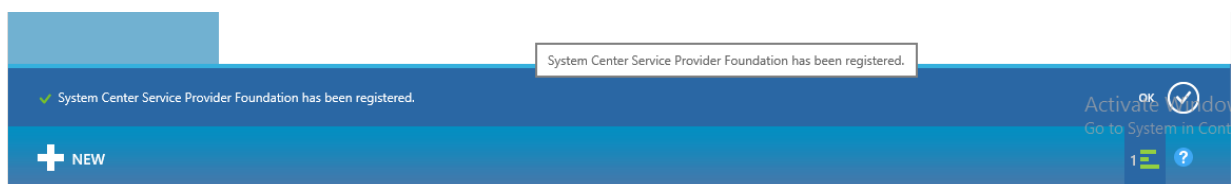


Figure 4.69: ...and everything should work fine now.

To manage a VM cloud, we must first connect to the VMM server. The existing cloud in VMM will be displayed in the VM Clouds.

Therefore, fill in the Virtual Machine Manager server FQDN: `vmmtest.wijnstraat12.ddns.net`.

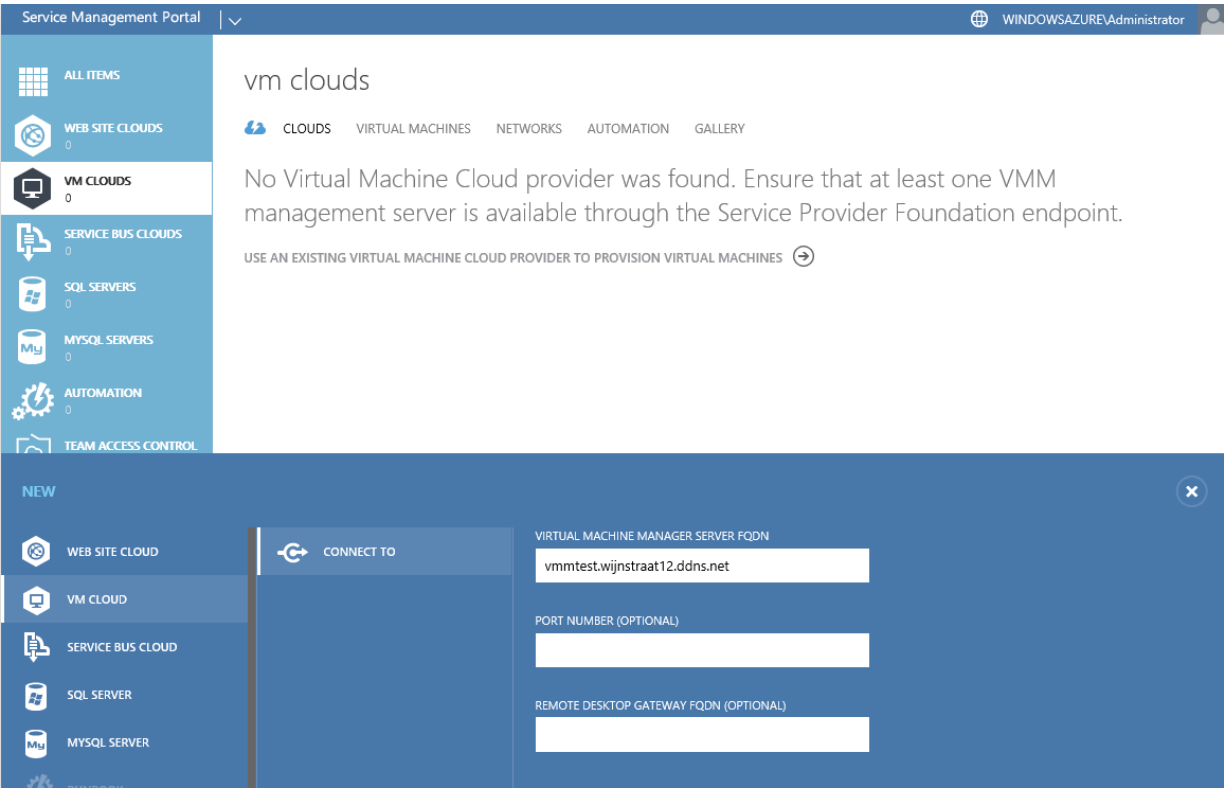


Figure 4.70: Connect to the VMM server.

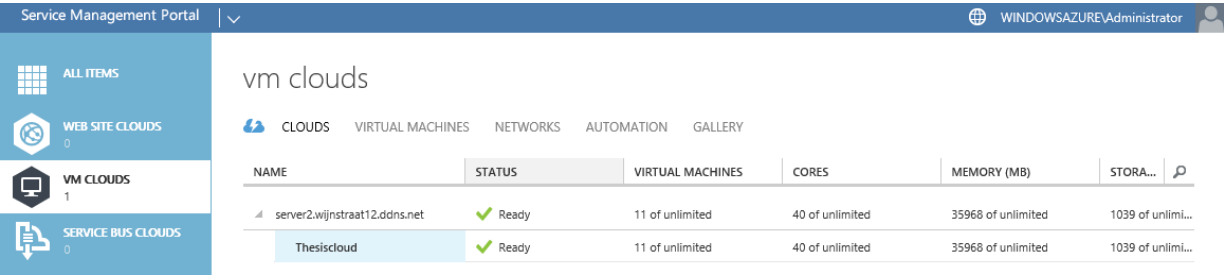


Figure 4.71: The cloud is now visible in VM clouds.

Planning

Problems

Issues

Assistance