

Cloud Management

INDEX

Sr.No	Name	Sign.
1.	<p>Managing Hyper-V environment with SCVMM 2012.</p> <ul style="list-style-type: none"> a) Installing and Configuring System Center 2012 R2 VMM b) Managing Hosts and Host Groups c) Connecting to Hyper-V and deploying VMs. d) Performing Live Migration using Hyper-V Manager. e) Creating a Virtual Machine and Modifying Its Properties f) Cloning a Virtual Machine g) Creating a Hyper-V Failover Cluster h) Managing a Hyper-V Failover Cluster i) Configuring and Managing Hyper-V Replica j) Moving Hyper-V Storage and Virtual Machines 	
2.	<p>Provisioning Self-Service using App-Controller.</p> <ul style="list-style-type: none"> a) Deploying a new virtual machine running Windows Server 2012 Datacenter edition to Windows Azure cloud. (Should be performed Online) b) Deploying a new virtual machine running Windows Server 2012 Datacenter edition to Hyper-V using App-Controller. c) Creating a Service Template d) Deploying a Service and Updating a Service Template 	

	<p>e)Configuring App Controller</p> <p>f)Deploying a Virtual Machine in App Controller</p>	
3.	<p>Managing Private cloud with App Controller.</p> <p>a) Deploying a new virtual machine.</p> <p>b) Adding Virtual Hard Disks and integrating it with VMs.</p>	
4.	<p>Using Data Protection Manager for Backup and Recovery.</p> <p>a) Creating a new protection group from the Protection workspace.</p> <p>b) Performing a recovery from the Recovery workspace.</p>	
5.	<p>Using Advisor for proactive Monitoring.</p> <p>a) Reviewing a critical alert for a Virtual Machine Manager server and assigning an alert.</p> <p>b) Integrating Advisor with Operations Manager.</p>	
6.	<p>Using Service Manager to Standardize.</p> <p>a) Creating a new related service request.</p> <p>b) Configuring the settings for an incident and reviewing an incident that has been closed.</p>	
7.	<p>Using Orchestrator for automation.</p> <p>a) Creating a simple virtual machine in Windows Azure using System Center Orchestrator. (Should be performed Online)</p> <p>b) Creating runbook that automates a process relating to VMware vSphere.</p>	
8.	<p>Using Configuration Manager 2012 for managing and maintaining.</p> <p>a) Setting up an alert for compliance.</p>	

	b) Connecting devices and monitoring its health. c) Managing users and user groups hierarchy.	
--	--	--

Practical No 1: Managing Hyper-V environment with SCVMM 2012.

a) Installing and Configuring System Center 2012 R2 VMM

System Center Virtual Machine Manager (SCVMM) forms part of Microsoft's System Center line of management and reporting tools, alongside previously established tools such as System Center Operations Manager and System Center Configuration Manager. SCVMM is designed for management of large numbers of Virtual Servers based on Microsoft Virtual Server and Hyper-V, and was released for enterprise customers in October 2007. A standalone version for small and medium business customers is available.

Installation of SCVMM

- **Prerequisites**

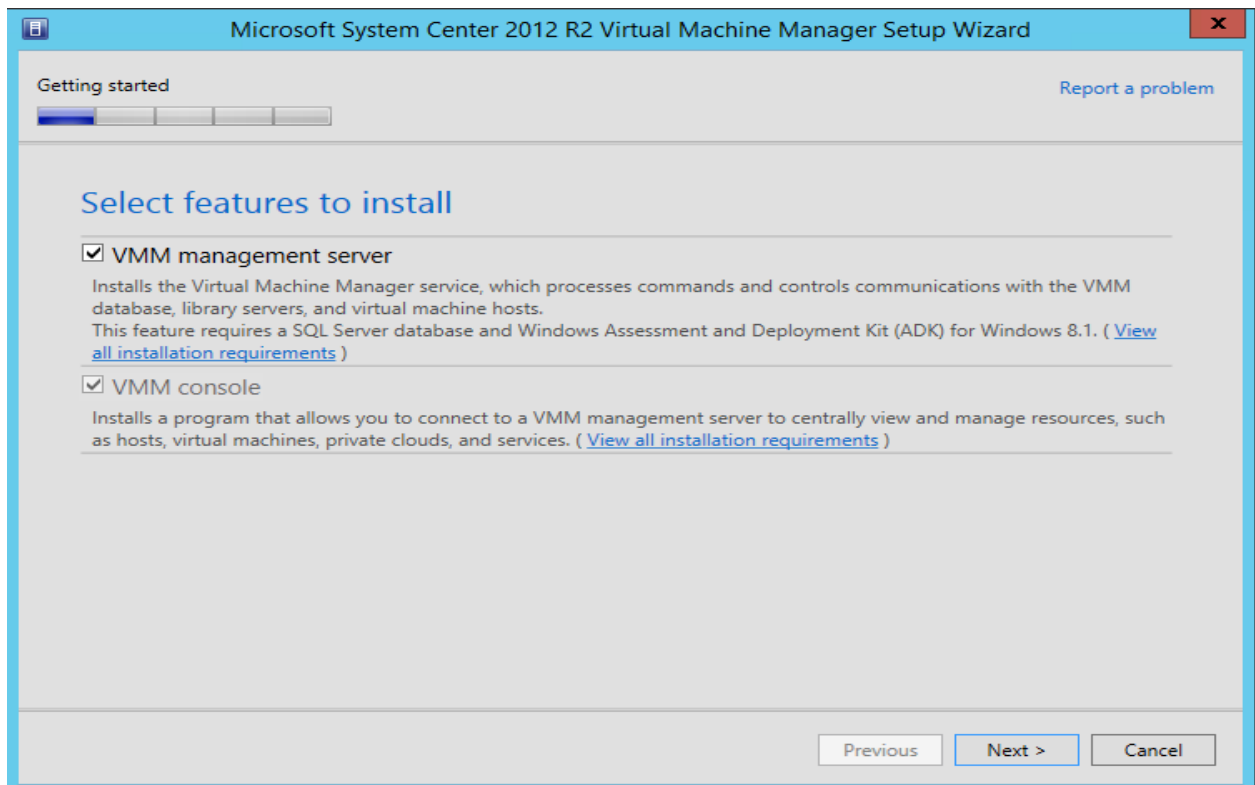
- Prepare SQL Server and select following features:

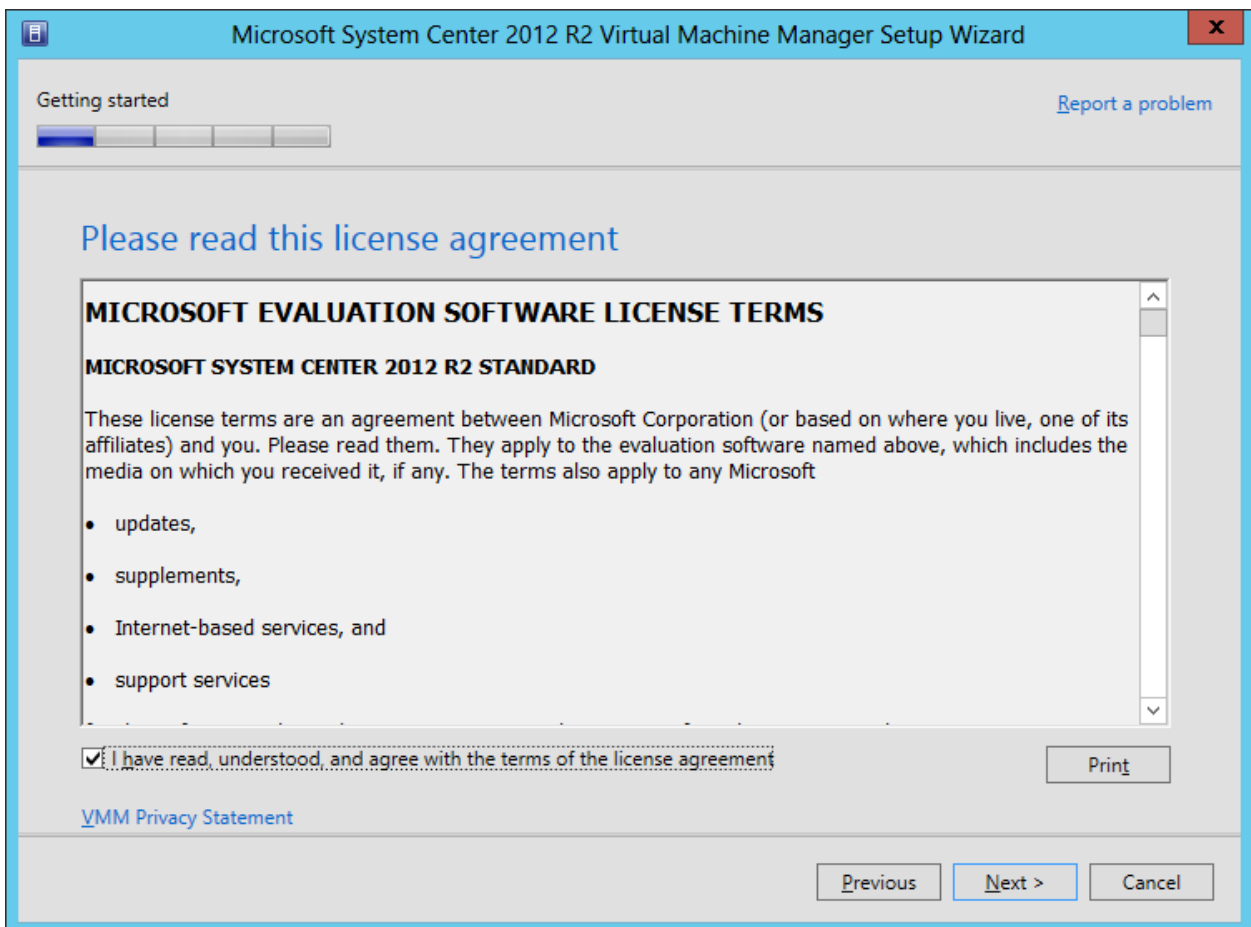
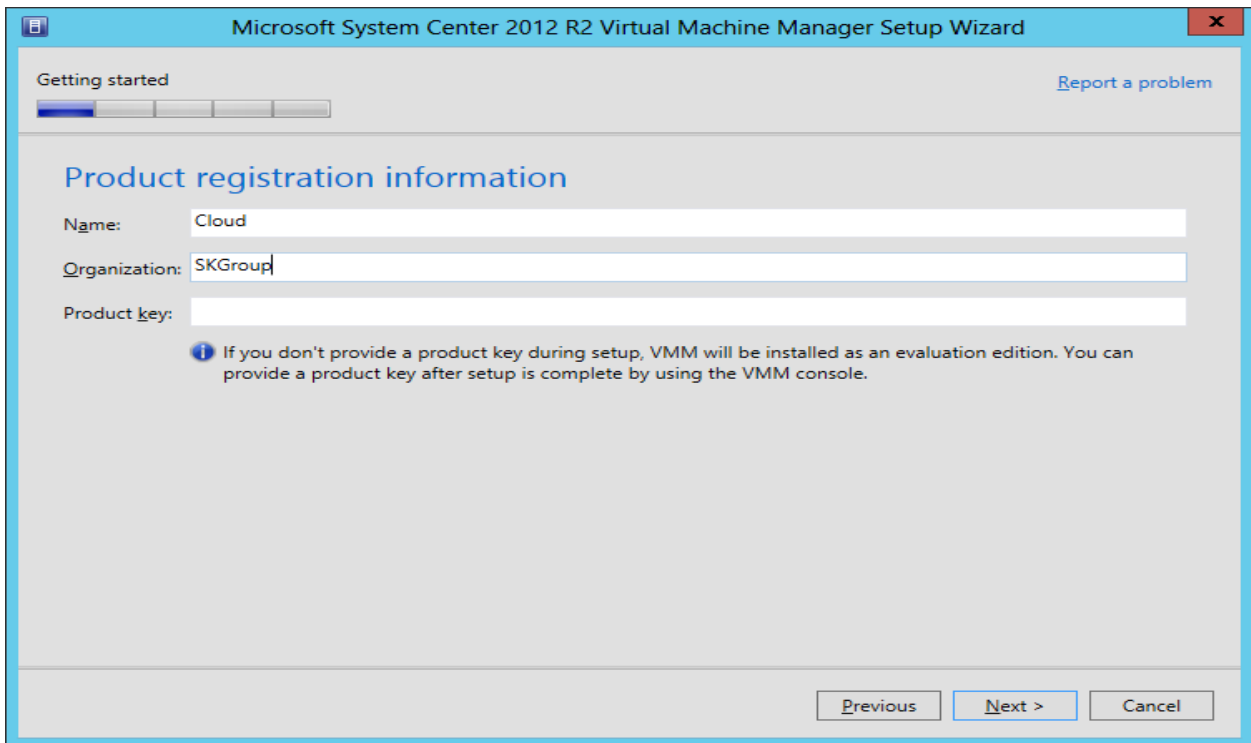
Database Engine Services

Management Tools

- Installing “Windows Assessment and Deployment Kit” (Windows ADK), Select Deployment Tools and Windows Preinstallation Environment (Windows WE)”
- Creating User “VMMService” in Service accounts in “Active Directory Computers and Users”
- Add the user in DNSAdmins
- Create login named as “VMMService” in SQL management studio
- ADSI->New->Object->container. Give value as “VMMDKM” Configure the permission. Copy the content from the “distinguished _name”

- **Installation**





Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard

Getting started [Report a problem](#)

Customer Experience Improvement Program (CEIP)

If you choose to participate:

Microsoft will

- Collect information about your software and hardware configurations.
- Collect information about how you use our software and services to identify trends and usage patterns.

Microsoft will not

- Collect your name or address.
- Ask you to take surveys; nor will you be contacted by a sales representative.
- Prompt you with additional messages that might interrupt your work.

Yes, I am willing to participate in the Customer Experience Improvement Program

No, I am not willing to participate

You can stop participating at any time by changing a setting in Customer Experience Improvement Program Settings, found in Settings workspace of the VMM console.

[More about the Customer Experience Improvement Program](#)
[Privacy Statement for the Microsoft Customer Experience Improvement Program](#)
[VMM Privacy Statement](#)

Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard

Configuration [Report a problem](#)

Database configuration

Provide information about the database that you would like to use for your VMM management server.

Server name:

Port:

Use the following credentials

User name and domain: Format: Domain\UserName

Password:

Instance name:

Select an existing database or create a new database.

New database:

Existing database:

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?](#)

Microsoft System Center 2012 R2 Virtual Machine Manager Setup Wizard

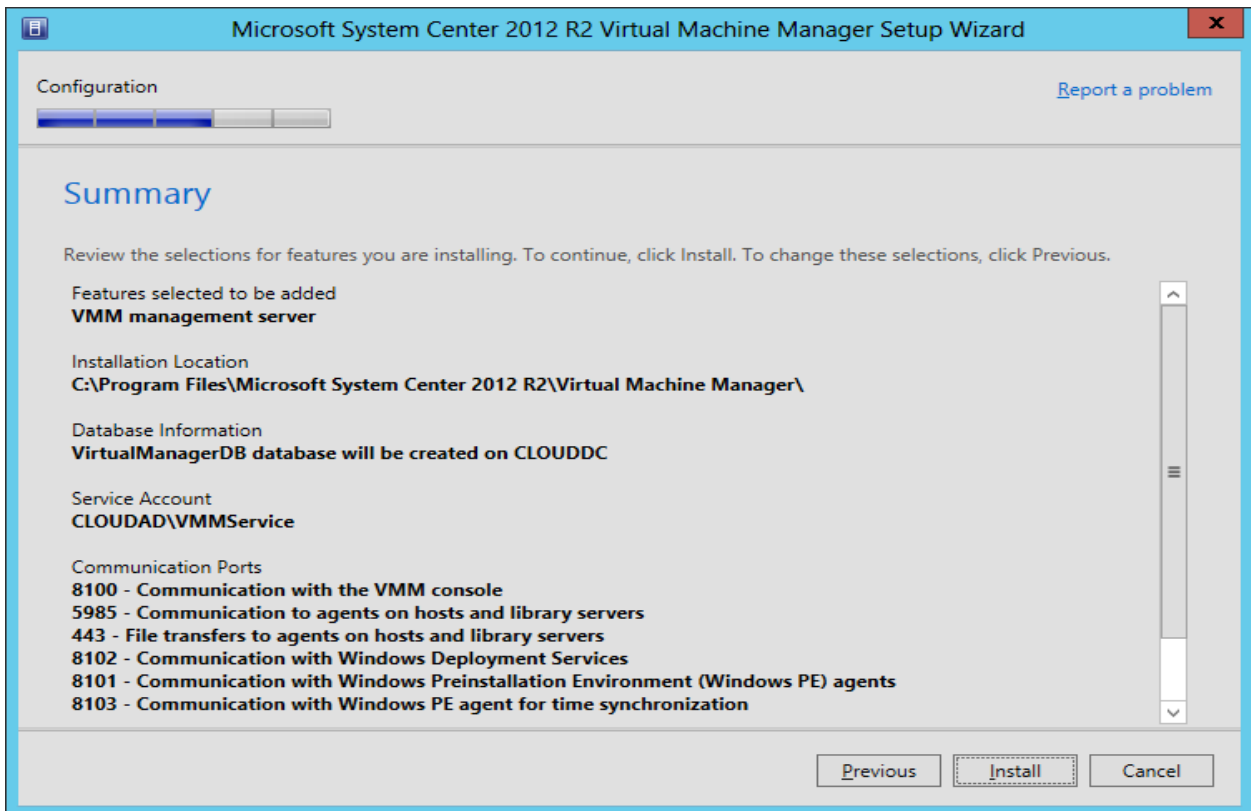
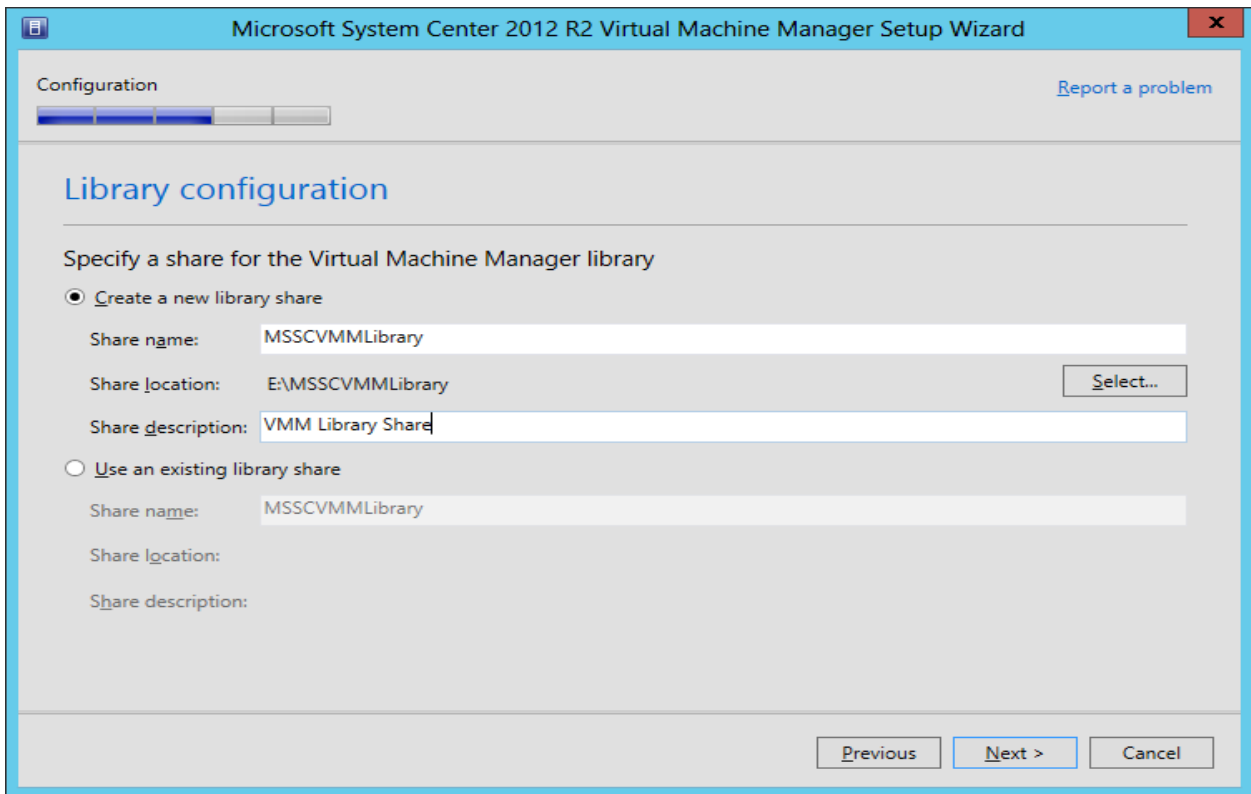
Configuration [Report a problem](#)

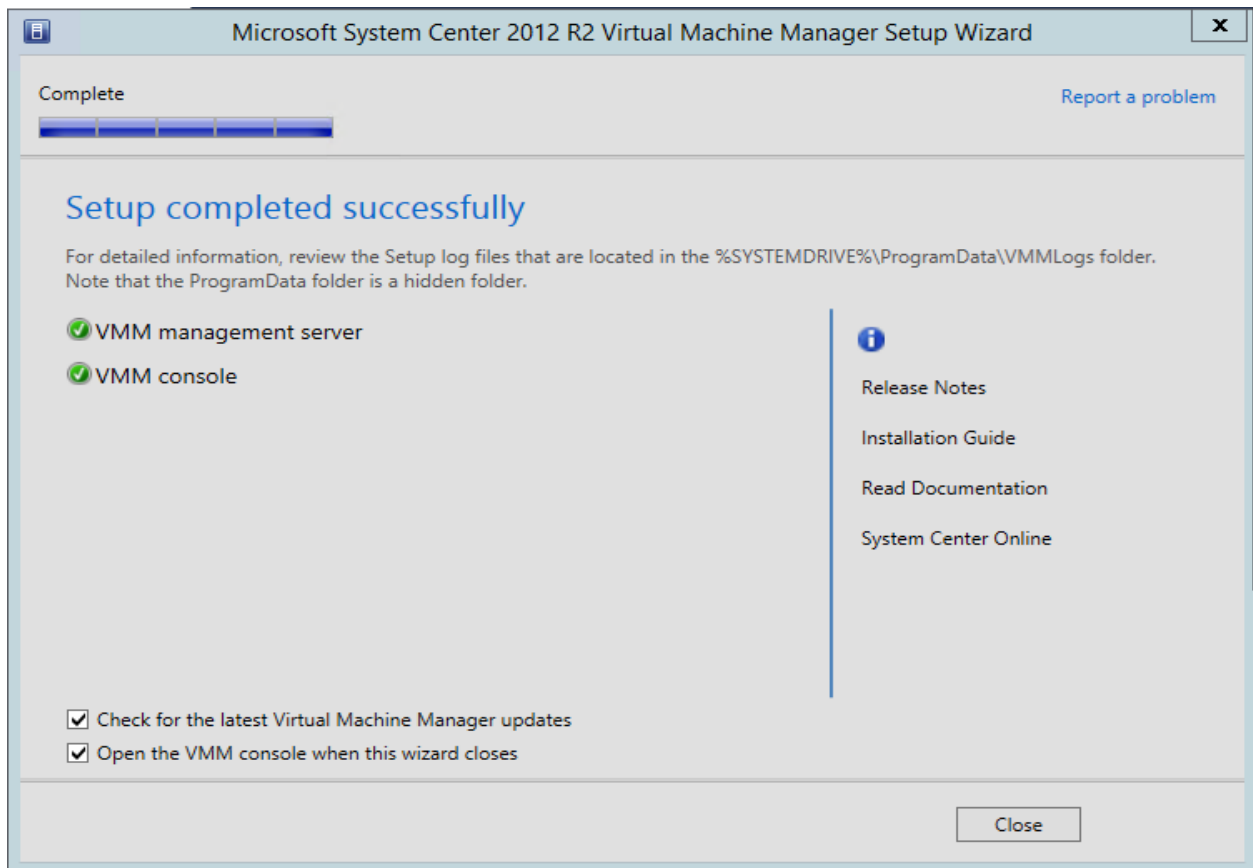
Port configuration

Management Server

Please select the ports for various VMM features.

<input type="text" value="8100"/>	Communication with the VMM console
<input type="text" value="5985"/>	Communication to agents on hosts and library servers
<input type="text" value="443"/>	File transfers to agents on hosts and library servers
<input type="text" value="8102"/>	Communication with Windows Deployment Services
<input type="text" value="8101"/>	Communication with Windows Preinstallation Environment (Windows PE) agents
<input type="text" value="8103"/>	Communication with Windows PE agent for time synchronization

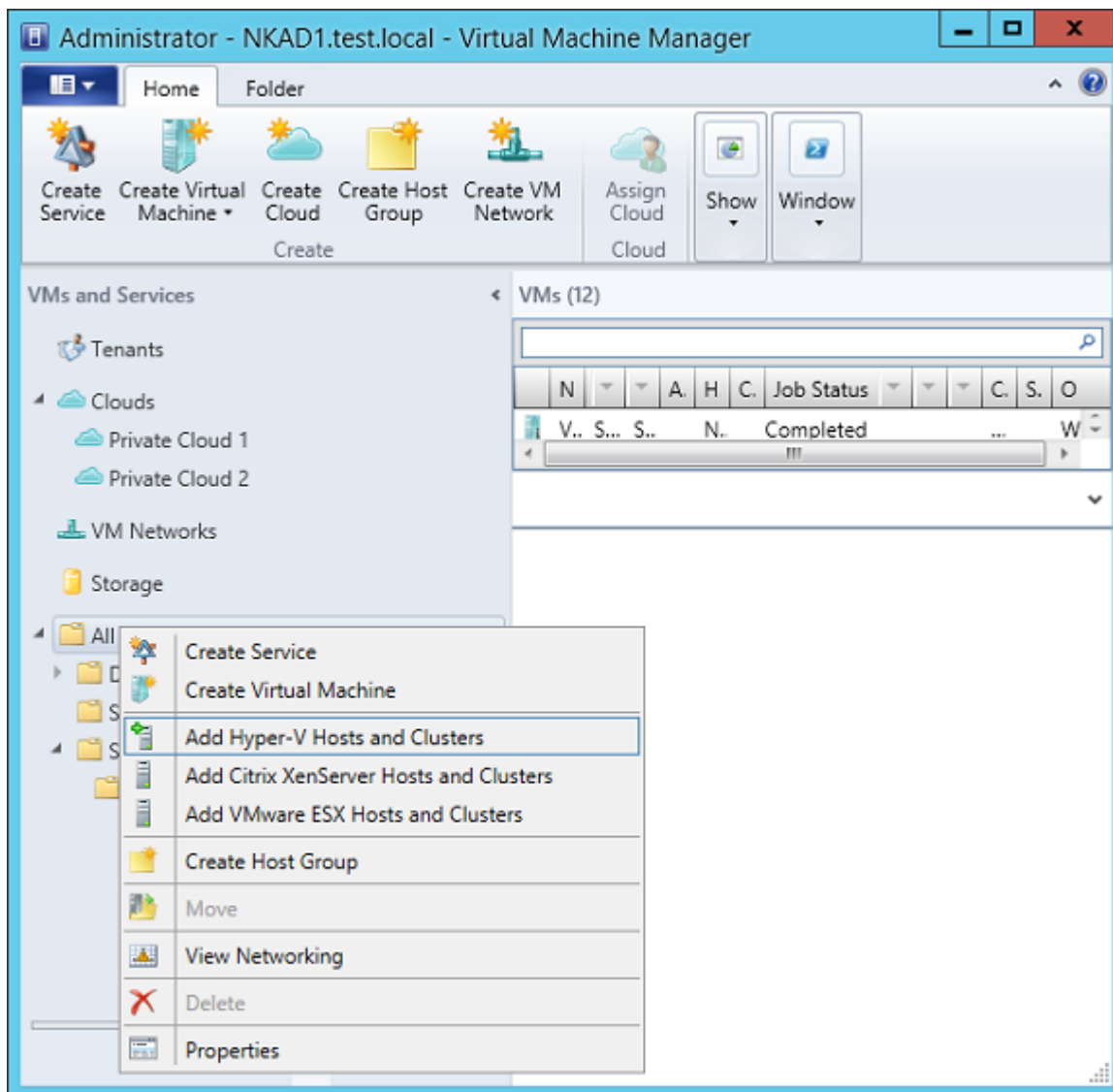




b) Managing Hosts and Host Groups

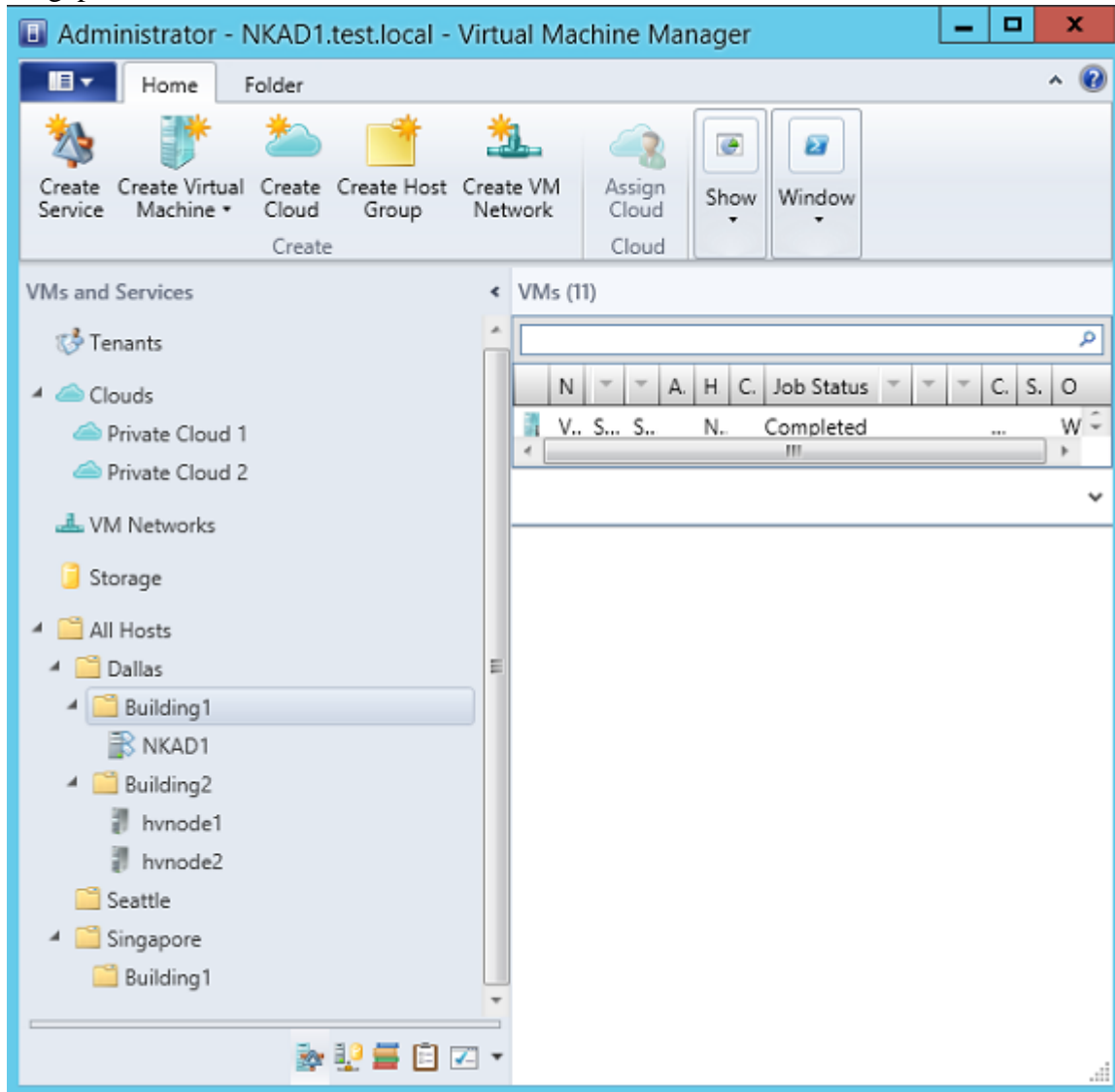
VMM Host Groups:

The first obvious question is why you would need a VMM Host Group. It is important to note that before you can manage the virtualization hosts located in datacenters, you would need to add the virtualization hosts in VMM. The Host Groups can be used to group virtualization hosts based on the physical site location.



By default, VMM provides a default Host Group called "All Hosts". "All Hosts" Host Group is the first Host Group in the VMM. You cannot rename and delete this Host Group. It is imperative to understand that a Host Group in VMM is more than just a group. As you can see in the screenshot below, I created three Host Groups in VMM called Dallas, Seattle and

Singapore.



c) Connecting to Hyper-V and deploying VMs.

So let's take a look at how you would go about adding Hyper-V hosts to Virtual Machine Manager, and then we will create some host groups. Begin the process by opening the Virtual Machine Manager console and then selecting the VMs and Services workspace. If you look at Figure A, you will notice that the All Hosts container is selected within the console tree. All Hosts is actually a host group.

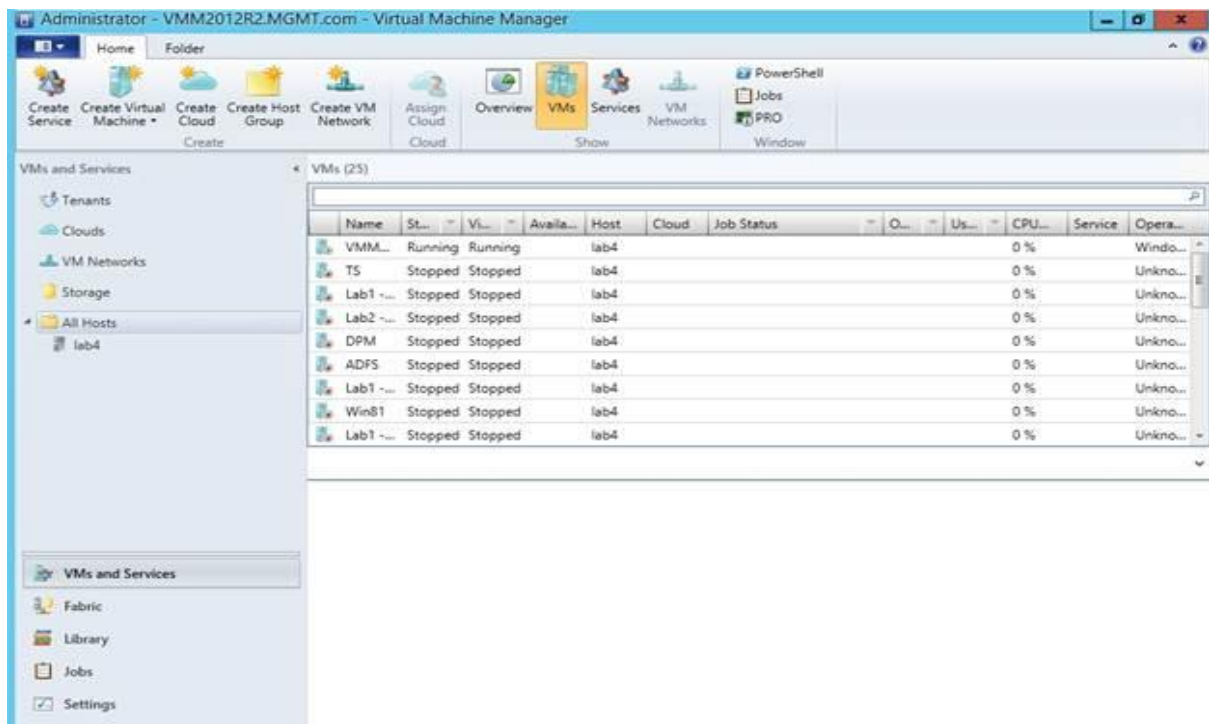


Figure A: Host servers are displayed through the VMs and Services workspace.

As you look at the figure above, you will also notice that right now a single host is listed beneath the All Hosts group. This host (Lab4) is a Hyper-V host in my lab environment. I manually added this host, but the other hosts have not yet been added.

To add a host server, right click on All Hosts. When you do, you will see a shortcut menu that provides a number of different options for adding hosts, as shown in Figure B. For instance, you can add Hyper-V hosts, Citrix hosts, and of course, VMware hosts. You will also notice that we have the option of adding host clusters. I am not going to get into host clusters in this article, because I have a separate article series on failover clustering for Hyper-V.

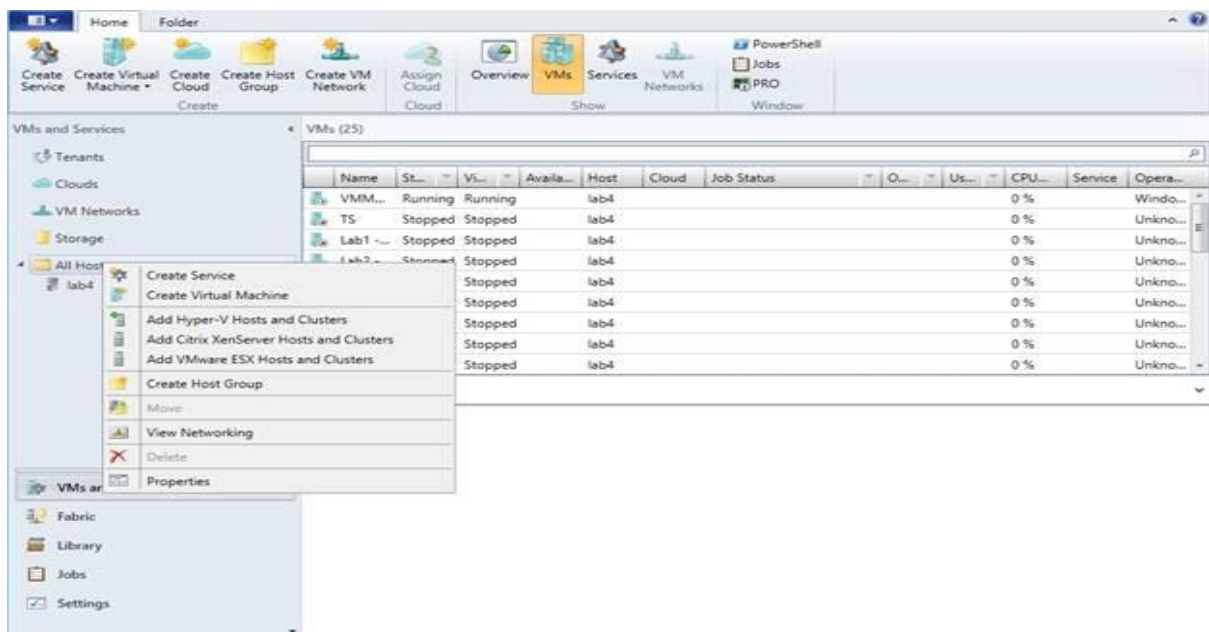


Figure B: You can add Citrix, VMware, and Hyper-V hosts.

For right now, let's go ahead and add some Hyper-V hosts. To do so, select the Add Hyper-V Hosts and Clusters option from the shortcut menu. When you do, Windows will display the Add Resource Wizard. In most cases, you will probably be adding Hyper-V hosts that reside in a trusted Active Directory domain. Therefore, when you see the wizard's first screen, choose the option to add Windows Server computers in a trusted Active Directory domain.

The next screen asks you to provide a Run As account. A Run As account is an account that has permission to perform the operation.

Click Next and you will be asked to specify the computers that you want to add. You can either enter the computer names manually, as I have done in Figure C, or you can perform an Active Directory query.

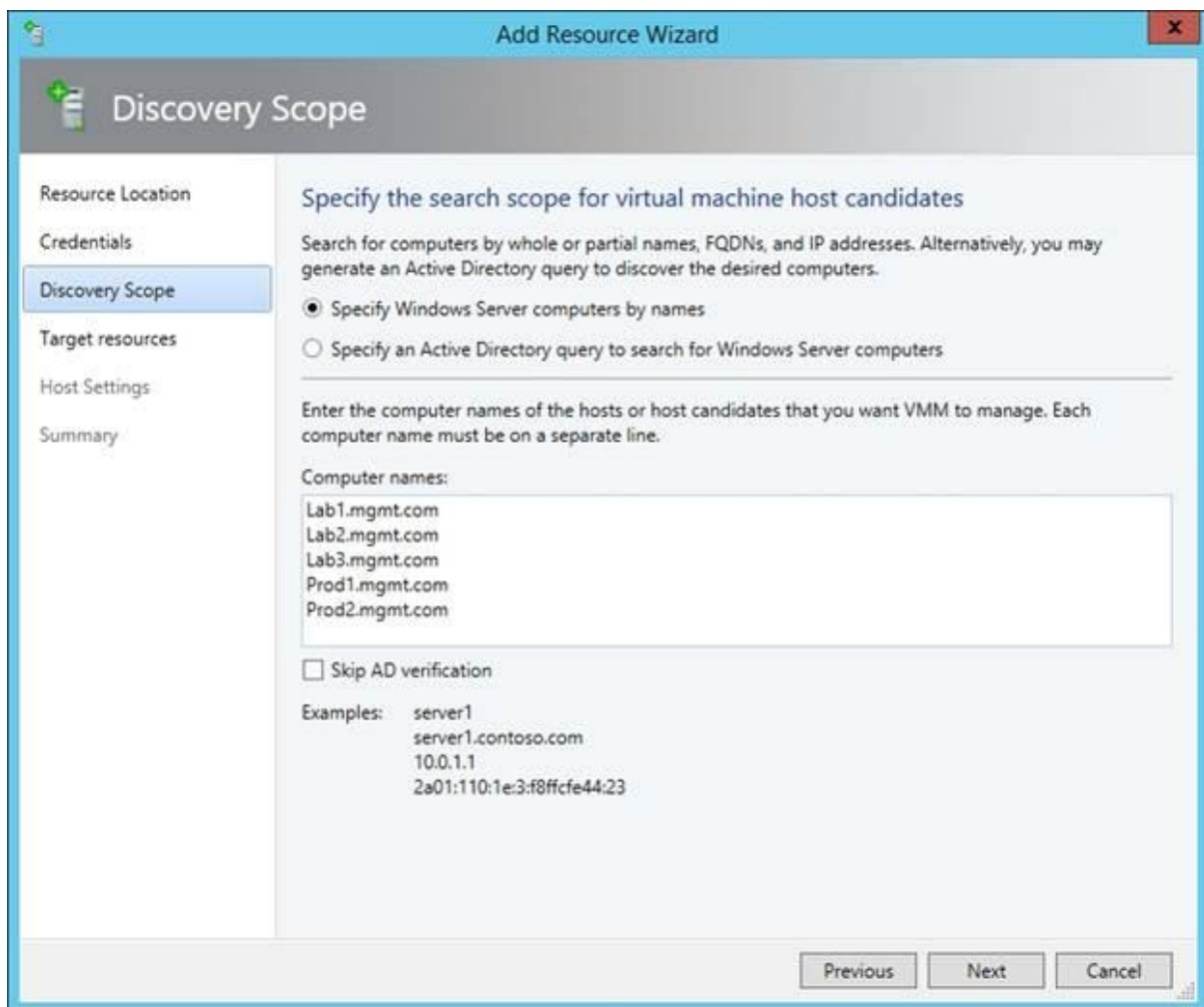


Figure C: You can manually enter the names of the hosts that you want to add.

Click Next and there will be a brief wait while Virtual Machine Manager verifies the accuracy of the information that you have entered. Once this check completes, you will see a list of the hosts that you can add to the host group. Now, simply select the check boxes that correspond to the hosts that you want to add, and click Next.

Before I move on, I want to point out that it might not always be possible to add every host. If you look at Figure D, you will notice that the servers named Lab1, Lab2, and Lab3 do not have check boxes next to them. The reason for this is because these Hyper-V hosts belong to

a cluster. You will notice that the wizard displays an object named Lab.MGMT.com. This is the cluster to which Lab1, Lab2, and Lab3 belong. I didn't tell Virtual Machine Manager that I wanted to add the cluster, but it displayed the cluster anyway because I specified the individual nodes within the cluster.

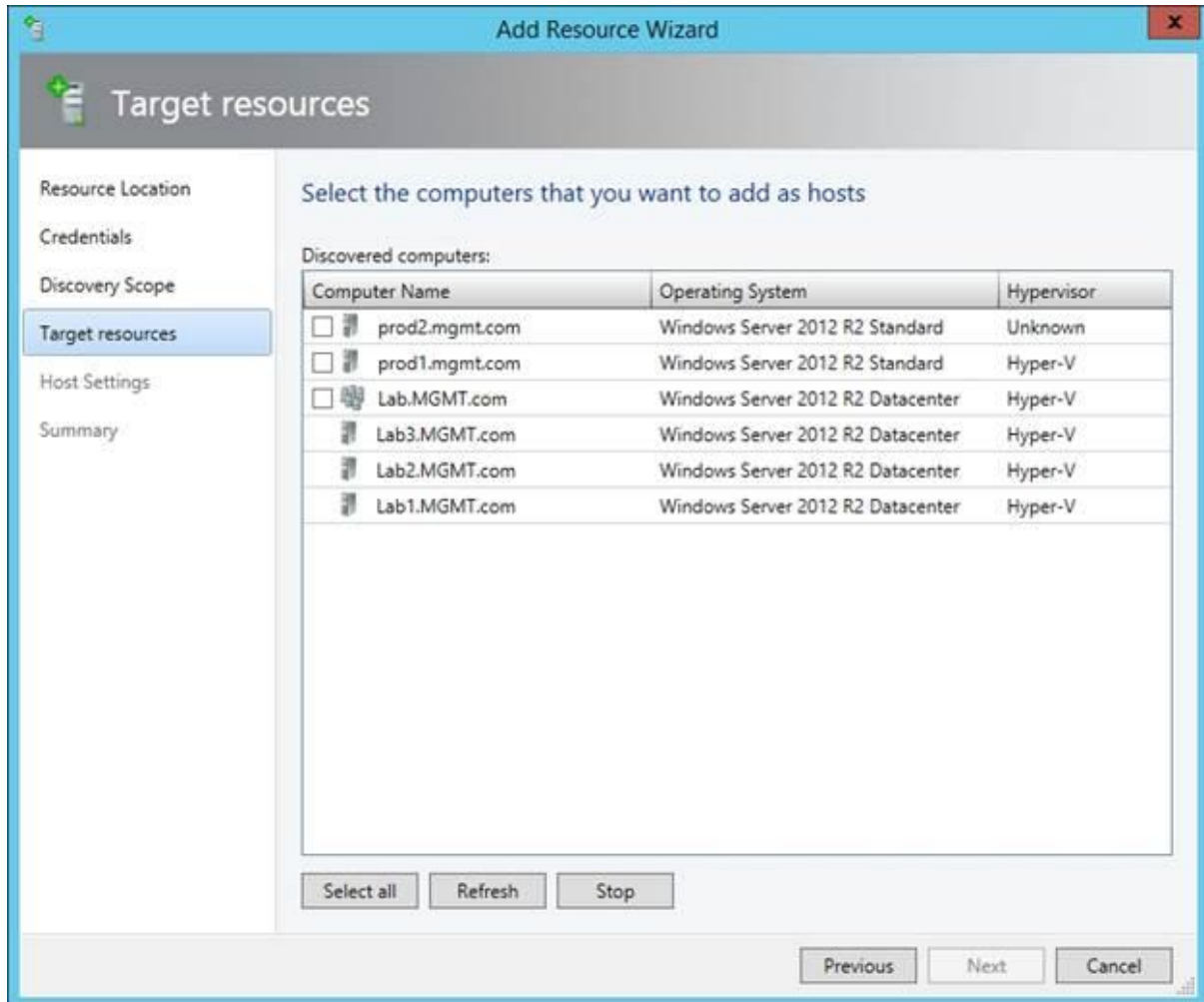


Figure D: Some hosts cannot be individually added to a host group.

With that said, select the hosts that you want to add and click Next. You will now see a screen asking you to verify your settings. Take a moment to make sure that everything is correct and click Next, followed by Finish. The hosts will be added to the host group.

Creating a Virtual Machine

The process of creating a new virtual machine works a little bit differently in Virtual Machine Manager than it does in the Hyper-V Manager. You can begin the process by either selecting a host or a host group and then clicking the Create Virtual Machine tile, located in the ribbon (be sure to choose the Create Virtual Machine option).

The next screen that you encounter asks you to choose the hardware settings for the virtual machine. You can specify the hardware manually as you do through Hyper-V Manager, but there are a couple of other options available to you, as shown in Figure F.

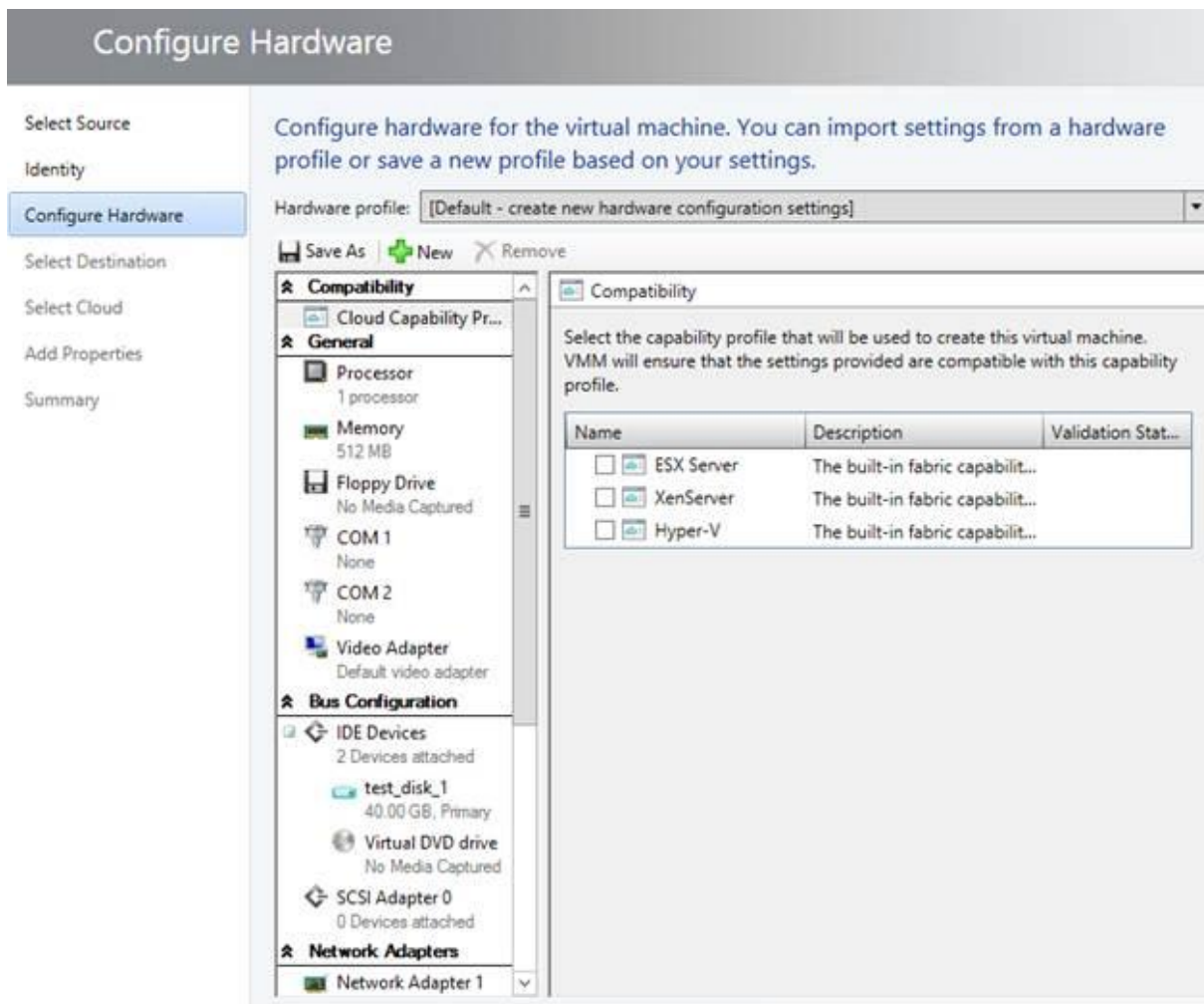


Figure F: Configure the virtual machine's hardware.

d) Performing Live Migration using Hyper-V Manager & j) Moving Hyper-V Storage and Virtual Machines

Prerequisites:

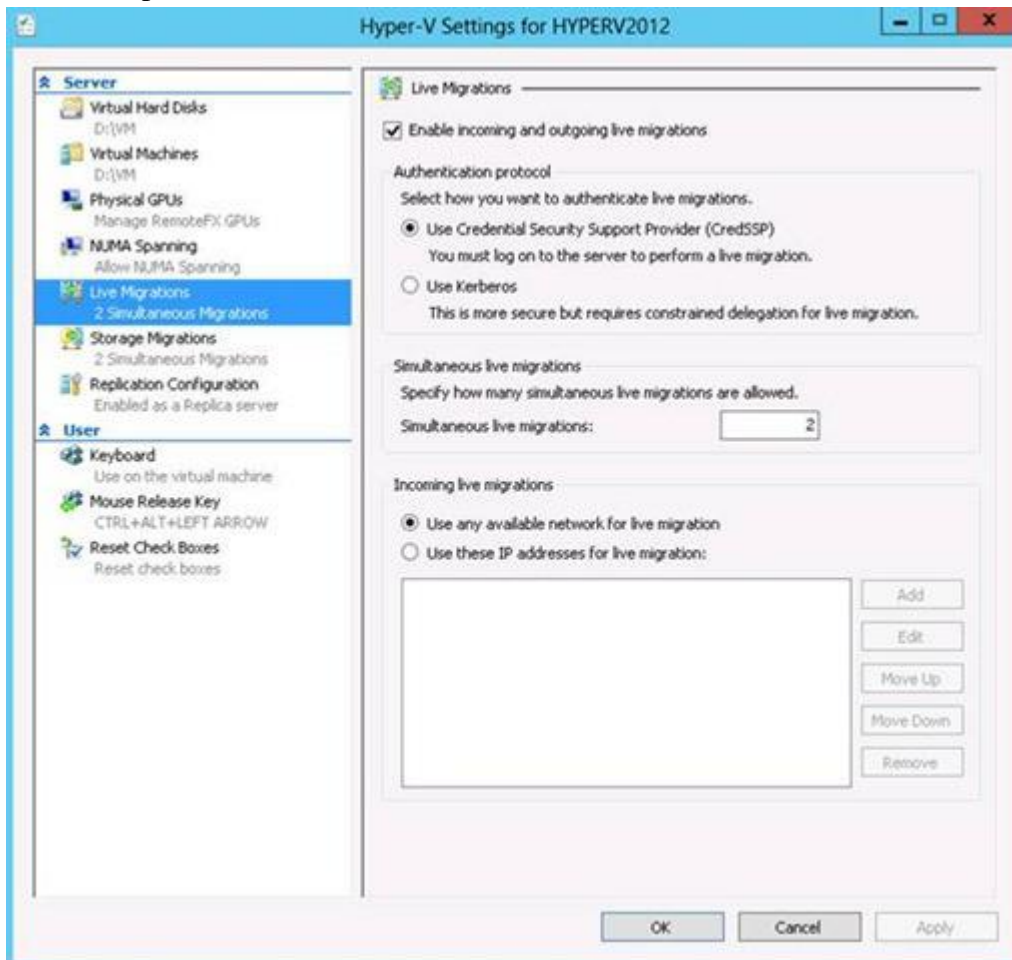
- 2 or more physical servers with the same processor manufacturer:
 - Intel or AMD CPU supporting Virtualization extensions (VT-x/AMD-V)
 - SLAT recommended for performance
- Windows Server 2012 with Hyper-V 3.0 Role installed:
 - Install Windows Server 2012 and install the Hyper-V role in server manager
- Both servers members of the same domain
 - Join both servers to the same domain
 - One or both servers may be a domain controller of a new domain if an existing domain is not available
- Both servers set up for Live Migrations

In the Hyper-V Settings in Hyper-V Manager, Live Migrations sub-menu, check the “Enable incoming and outgoing live migrations” checkbox.

Select use CredSSP as the Authentication protocol as it is simpler to configure but requires you to be logged on to the server

Specify 1 or more Simultaneous live migrations

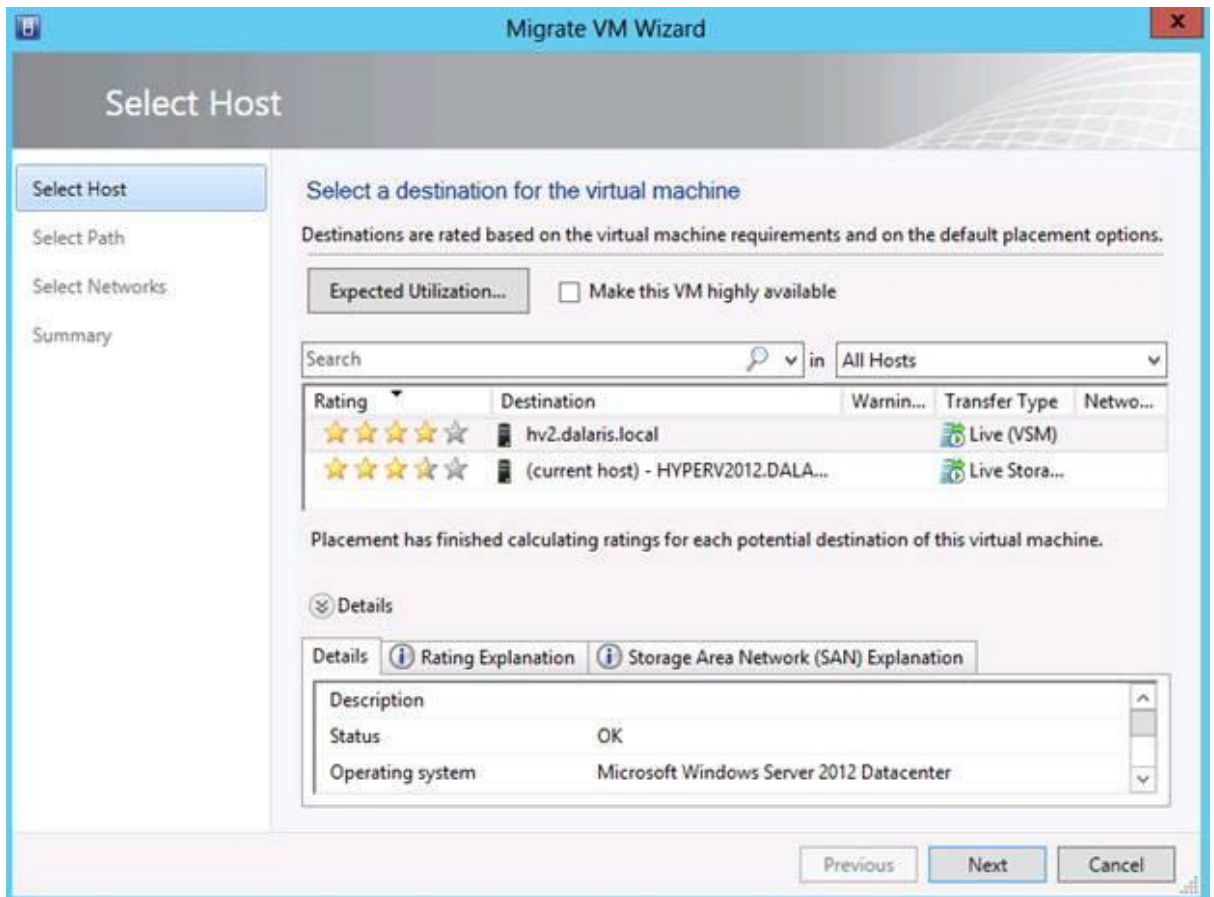
Select “Use any available network for live migration” or configure the IP range if you have multiple networks



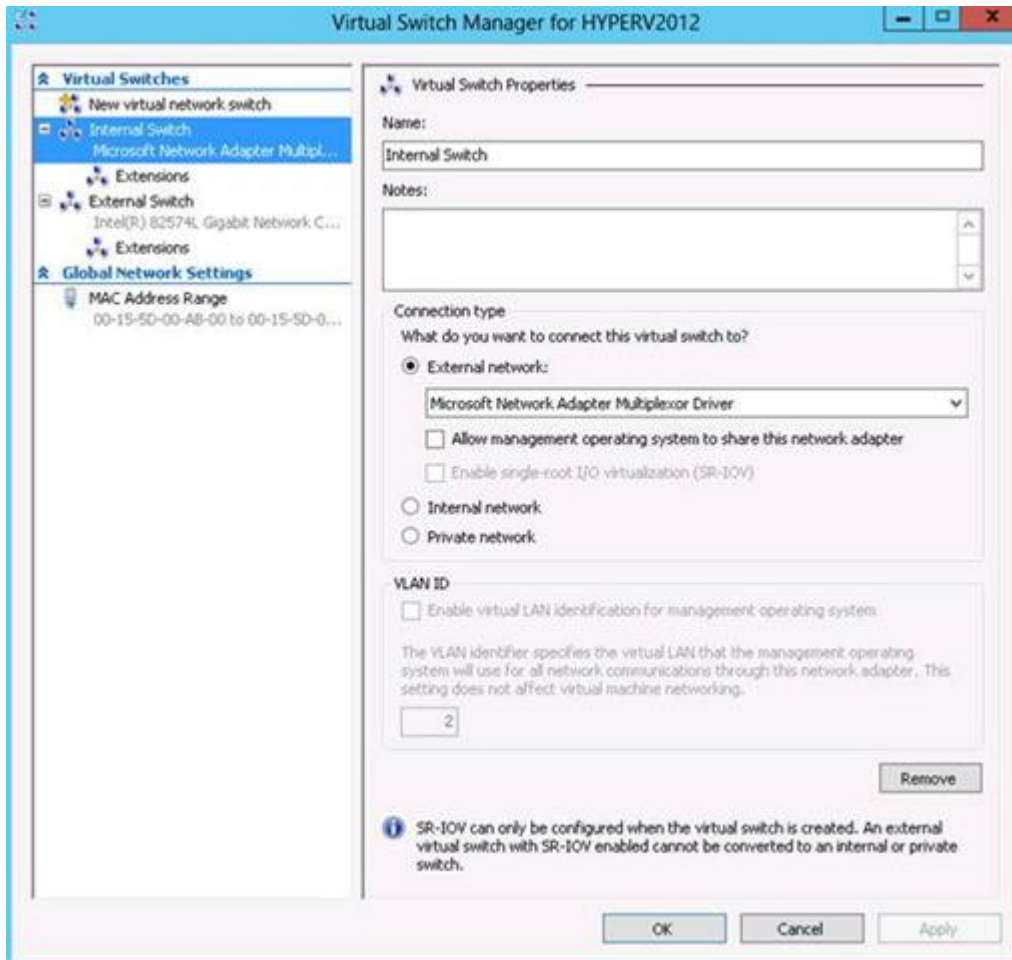
Identical network configuration

This can be tested in SCVMM under the Migrate VM Wizard

This portion of the setup is easier to configure using VMM since it gives feedback and recommendations to your current configuration:

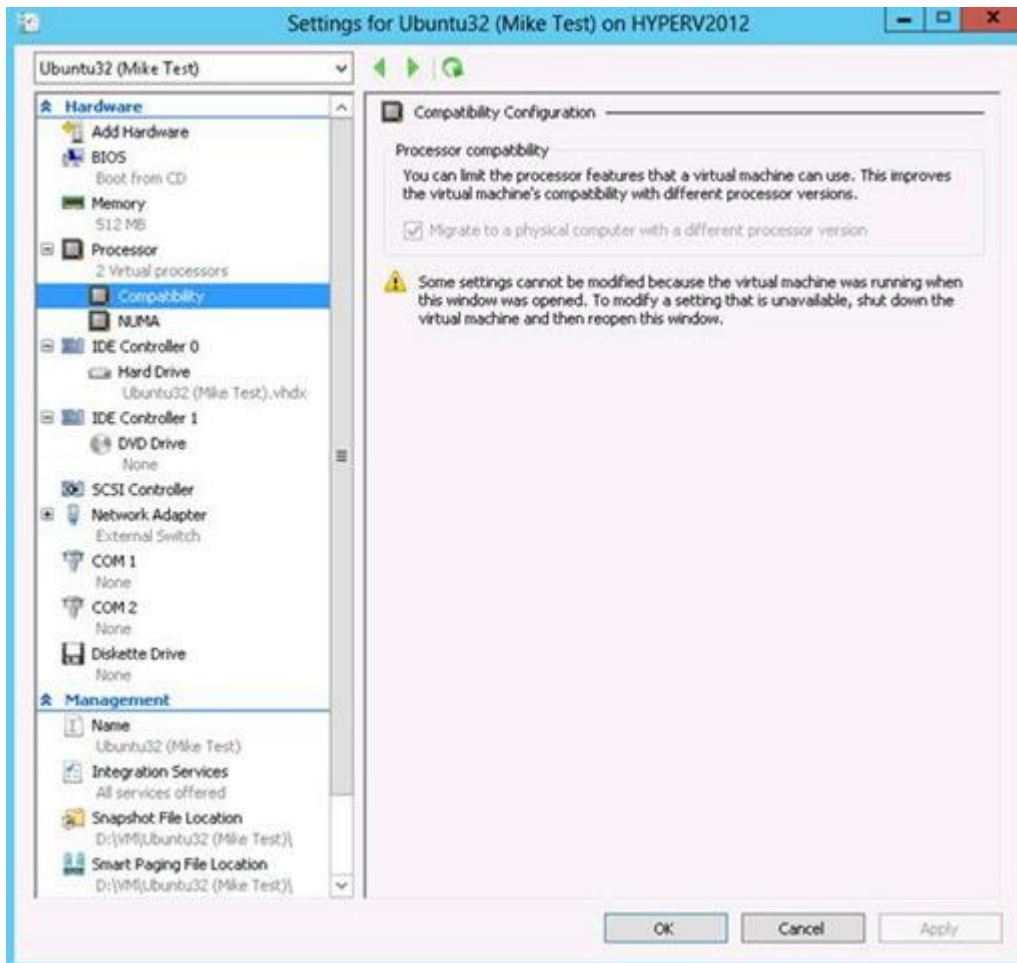


If SCVMM is unavailable, name your virtual switches the same on both physical servers:



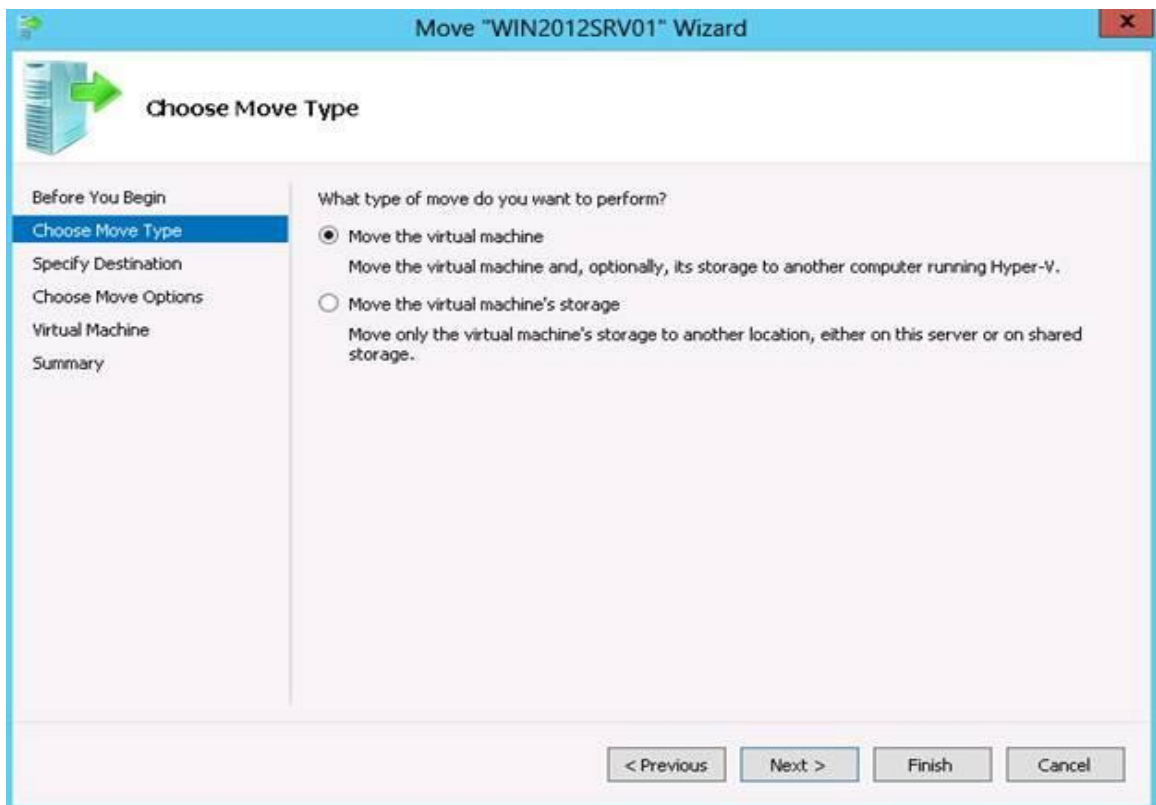
Recommended:

Same processor architecture (Workaround by setting Compatibility Configuration > “Migrate to a physical computer with a different processor version” checkbox in VM Settings under Processor > Compatibility sub-tree)

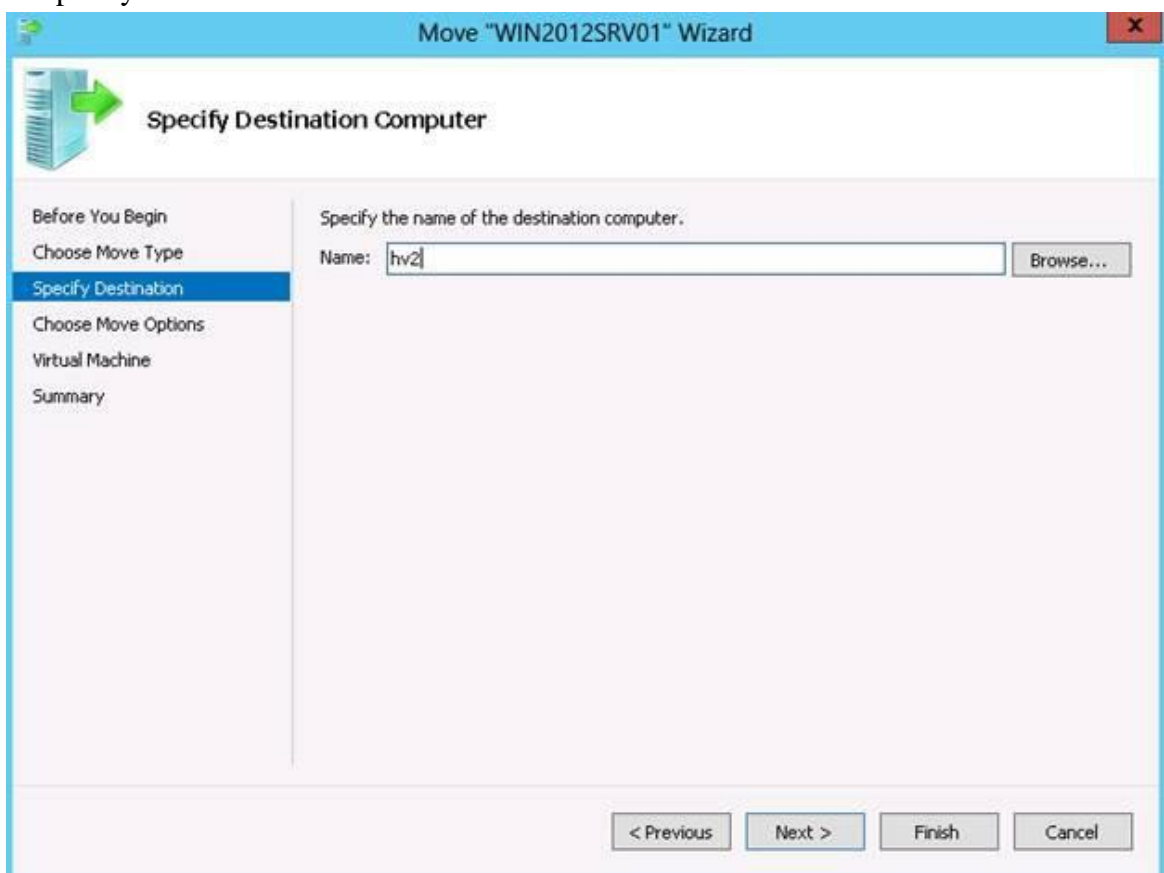


After these prerequisites are complete, the process of actually performing a live migration is simple:

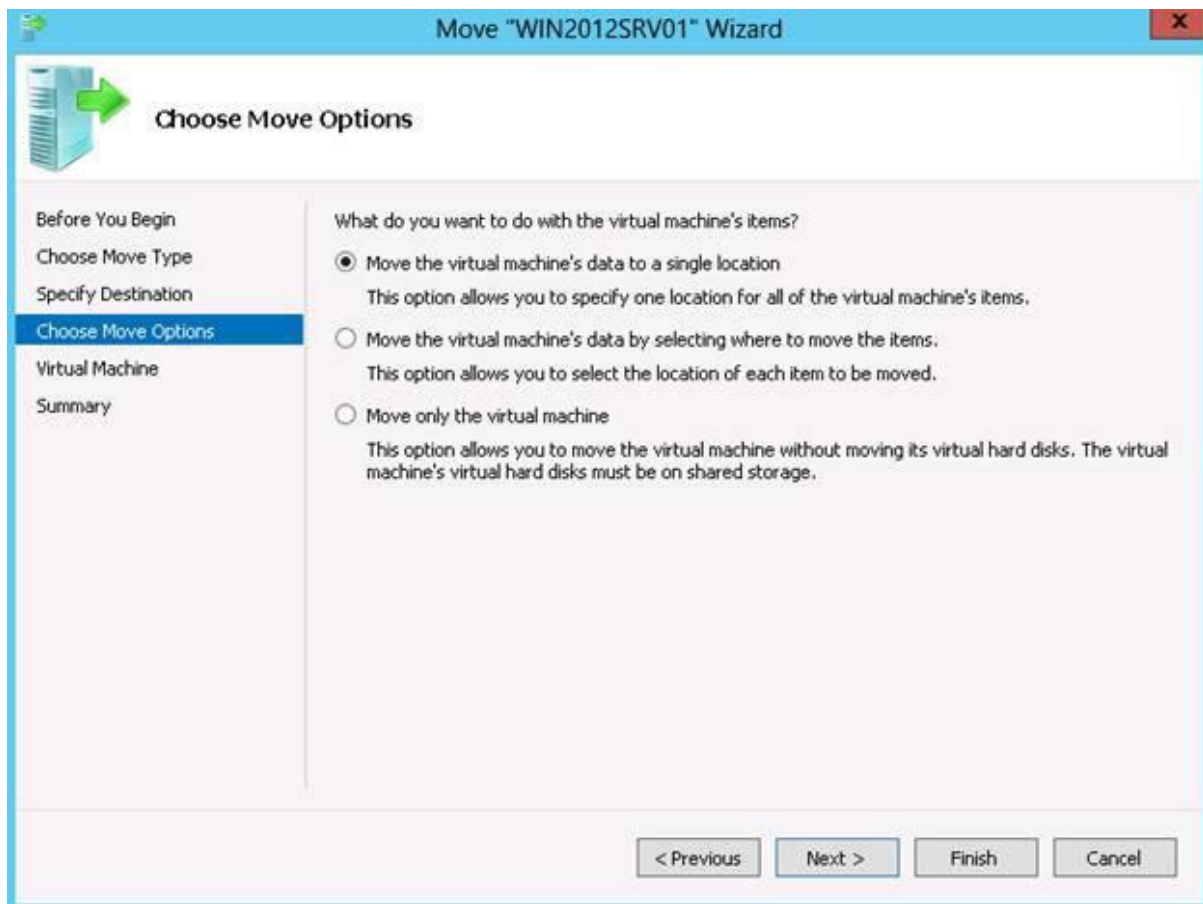
1. Right click Virtual Machine in Hyper-V manager and select Move.
2. Follow the Wizard, specifying the Move Type as “Move the virtual machine”



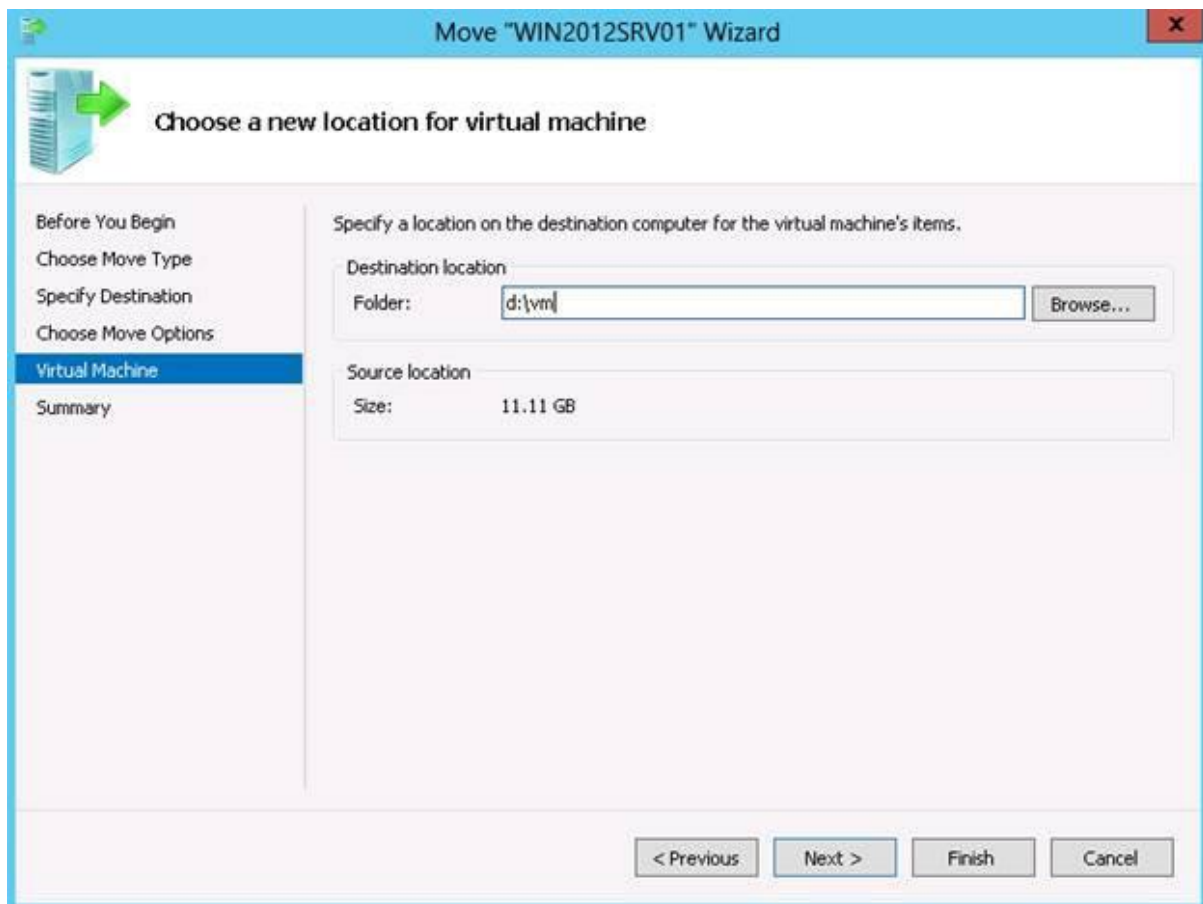
3. Specify the destination server name



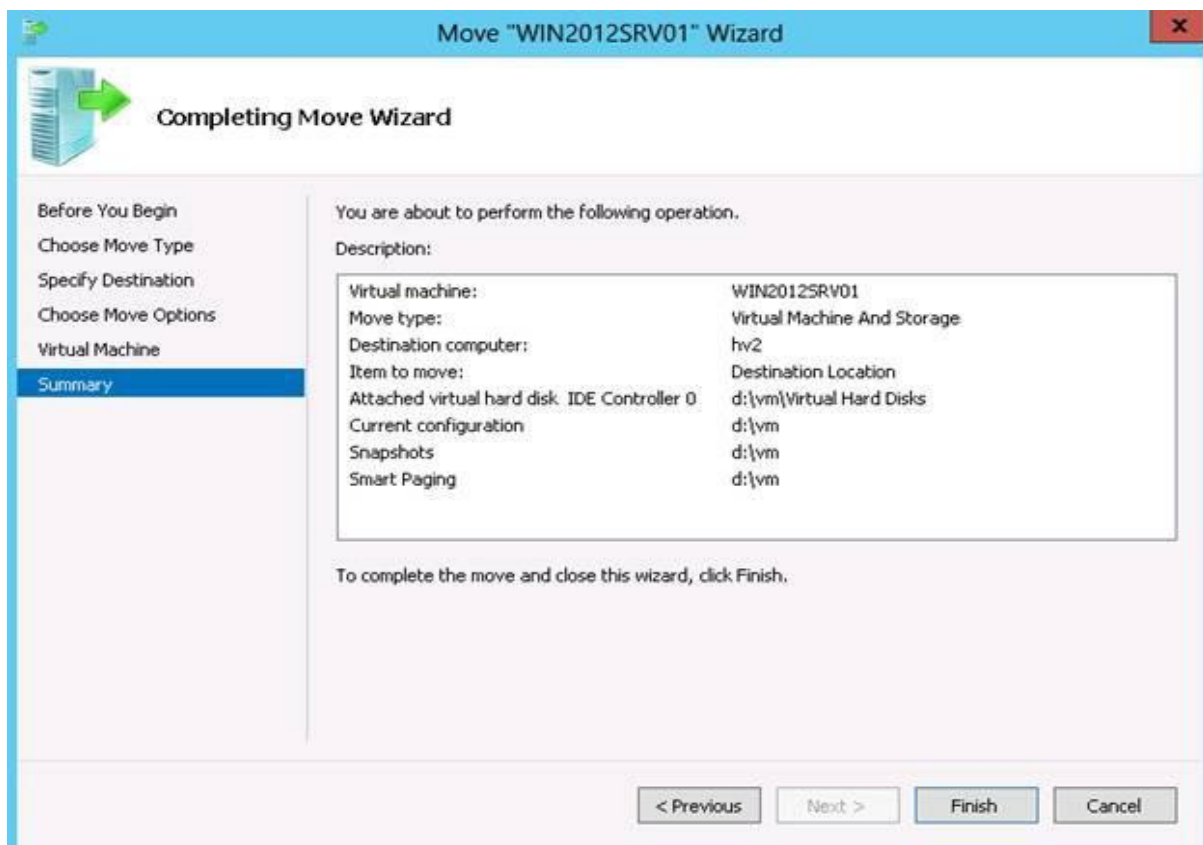
4. Select the “Move the virtual machine’s data to a single location” option



5. Specify the location on the target server to save the VM file or browse for the location using Remote File Browser



6. Review and accept the configuration by clicking Finish on the wizard



e) Creating a Virtual Machine and Modifying Its Properties

Creating Generation 2 VMs:

The Identity page of the Create Virtual Machine Wizard was modified to allow you to select which type of VM you want to create. When creating a Generation 2 VM just select “Generation 2” from the generation dropdown. This will do two major things: First, when you come to the Configure Hardware page you will notice that those hardware devices that are not support by Generation 2 VMs such as floppy drives, legacy networking and IDE controllers will not be present. Second, when selecting the destination host for the VM only Windows Server 2012 R2 hosts will be allowed.

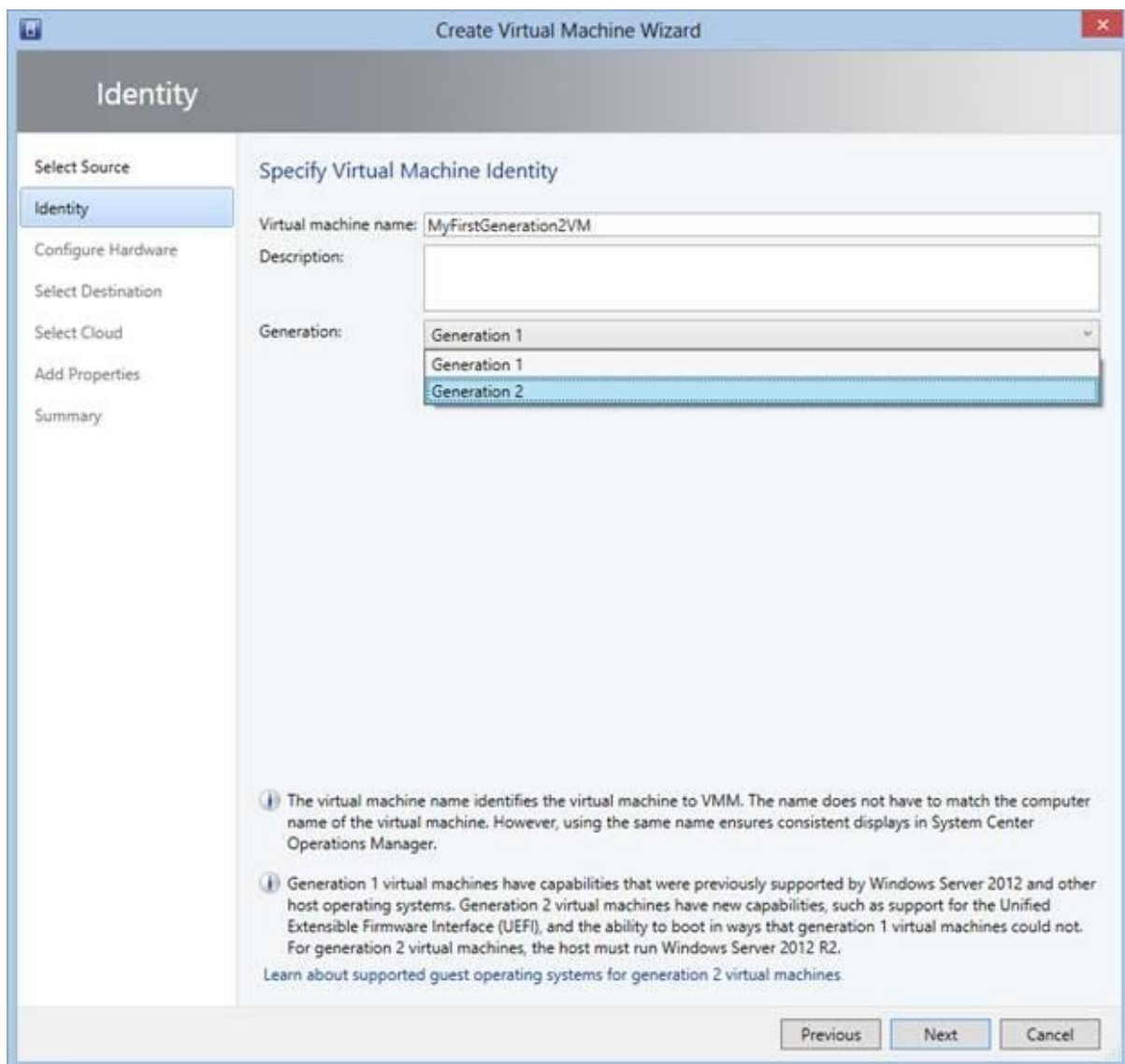


Figure 1 - Creating a Generation 2 VM

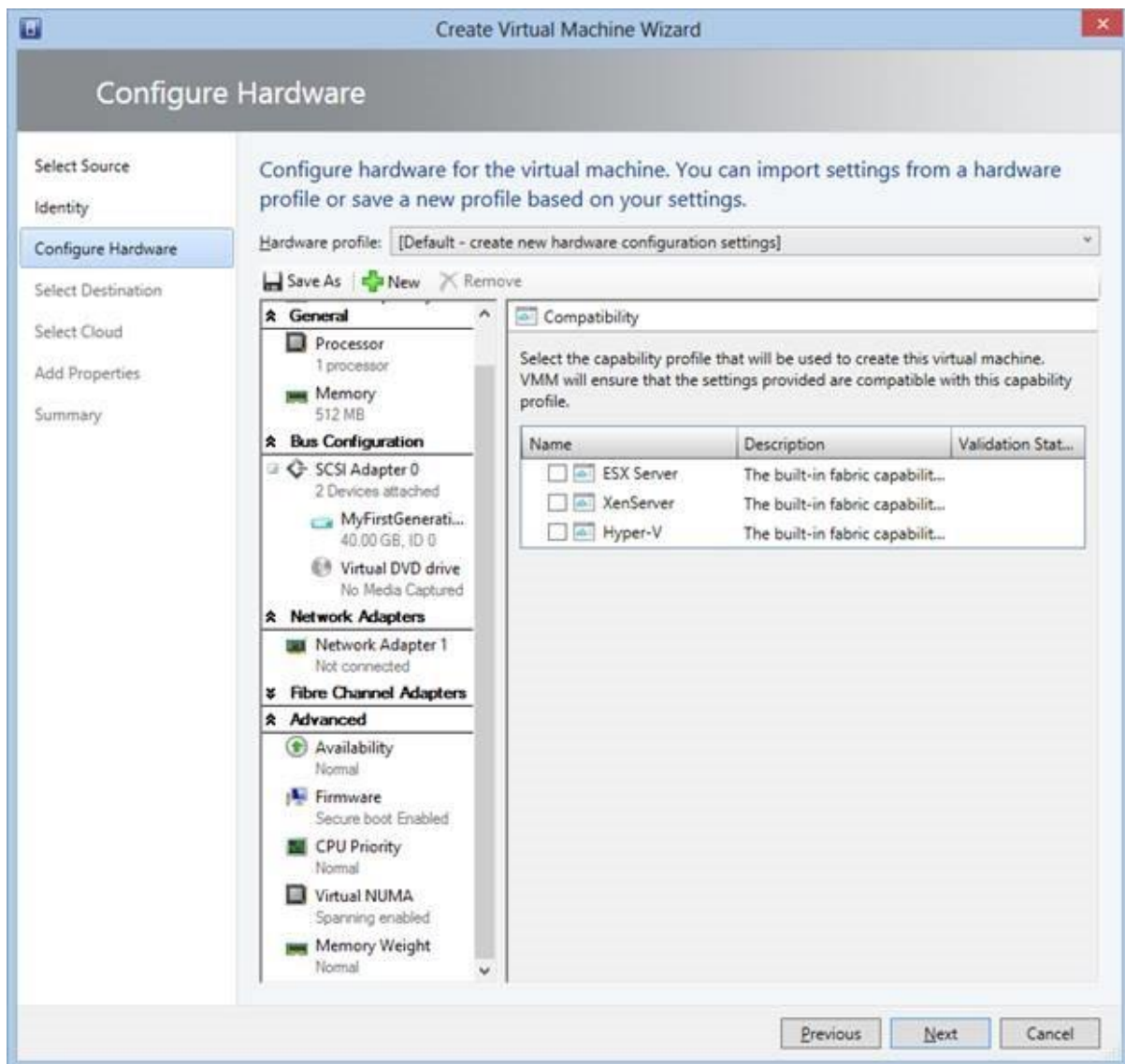


Figure 2 - Hardware for a Generation 2 VM

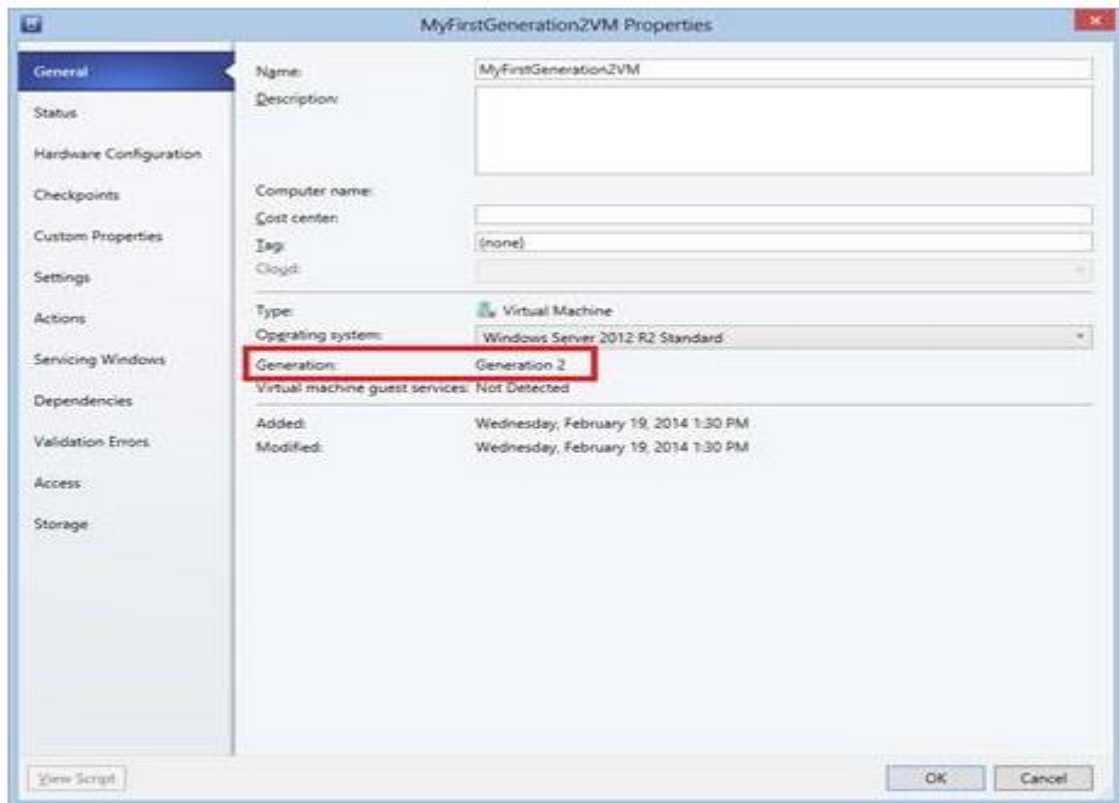


Figure 3 - Generation 2 VM Properties

f) Cloning a Virtual Machine

To initiate this action from within Hyper-v Manager on Windows 8.1 or Windows Server 2012 R2, use these steps:

Open Hyper-V Manager.

Find the running virtual machine that you want to clone.

Right-click on it and click on Export.

To initiate this process on SCVMM 2012 R2, use these steps:

Launch your Virtual Machine Manager console.

Select the virtual machine tab.

Locate the running virtual machine that you wish to clone.

Right-click on it, hover over "create" and select "clone"

Virtual Machine Tools Administrator - scvmm.armstrong.house - Virtual Machine M...

Home Folder Virtual Machine

Create Shut Down Power On Pause Power Off Reset Save State Discard Saved State Create Checkpoint Manage Checkpoints Connect or View Delete Properties

VMs (25)

Name	Status	Virtu...	Host	Job Status	CPU Ave...	Operatin...	VM Additions
Status: Running							
Borderland	Running	Running	hyper-v-2	Completed	0 %	64-bit edi...	6.3.9600.163...
Domain Controller - 2	Running	Running	hyper-v-2	Completed		64-bit edi...	6.3.9600.163...
TMG Server	Running	Ru					9600.163...
File Server	Running	Ru					9600.163...
Domain Controller - 1	Running	Ru			0 %	Windows...	6.3.9600.163...
Backup Server	Running	Ru			0 %	Windows...	6.3.9600.163...
FTP Server	Running	Ru			0 %	64-bit edi...	6.3.9600.163...
WDS	Running	Ru			0 %	Windows...	6.3.9600.163...
VPN Server	Running	Ru			0 %	64-bit edi...	6.3.9600.163...
WSUS	Running	Ru			0 %	Windows...	6.3.9600.163...
MineCraft Server	Running	Ru			2 %	64-bit edi...	6.3.9600.163...
SCVMM	Running	Ru			0 %	Windows...	6.3.9600.163...
Gateway	Running	Ru			0 %	Unknown	Detected
Status: Stopped							
File Server	Stopped	Sto			0 %	Unknown	Not Detected
Backup Server	Stopped	Sto			0 %	Unknown	Not Detected
Domain Controller - 2	Stopped	Sto			0 %	Unknown	Not Detected
MineCraft Server	Stopped	Sto			0 %	Unknown	Not Detected
Borderland	Stopped	Sto			0 %	Unknown	Not Detected
FTP Server	Stopped	Sto			0 %	Unknown	Not Detected
TMG Server	Stopped	Sto			0 %	Unknown	Not Detected
WSUS	Stopped	Sto			0 %	Unknown	Not Detected
Domain Controller - 1	Stopped	Stopped	hyper-v-2	Completed w/ Info	0 %	Unknown	Not Detected
VPN Server	Stopped	Stopped	hyper-v-1	Completed	0 %	Unknown	Not Detected
Domain Controller - 2							

Navigation Pane

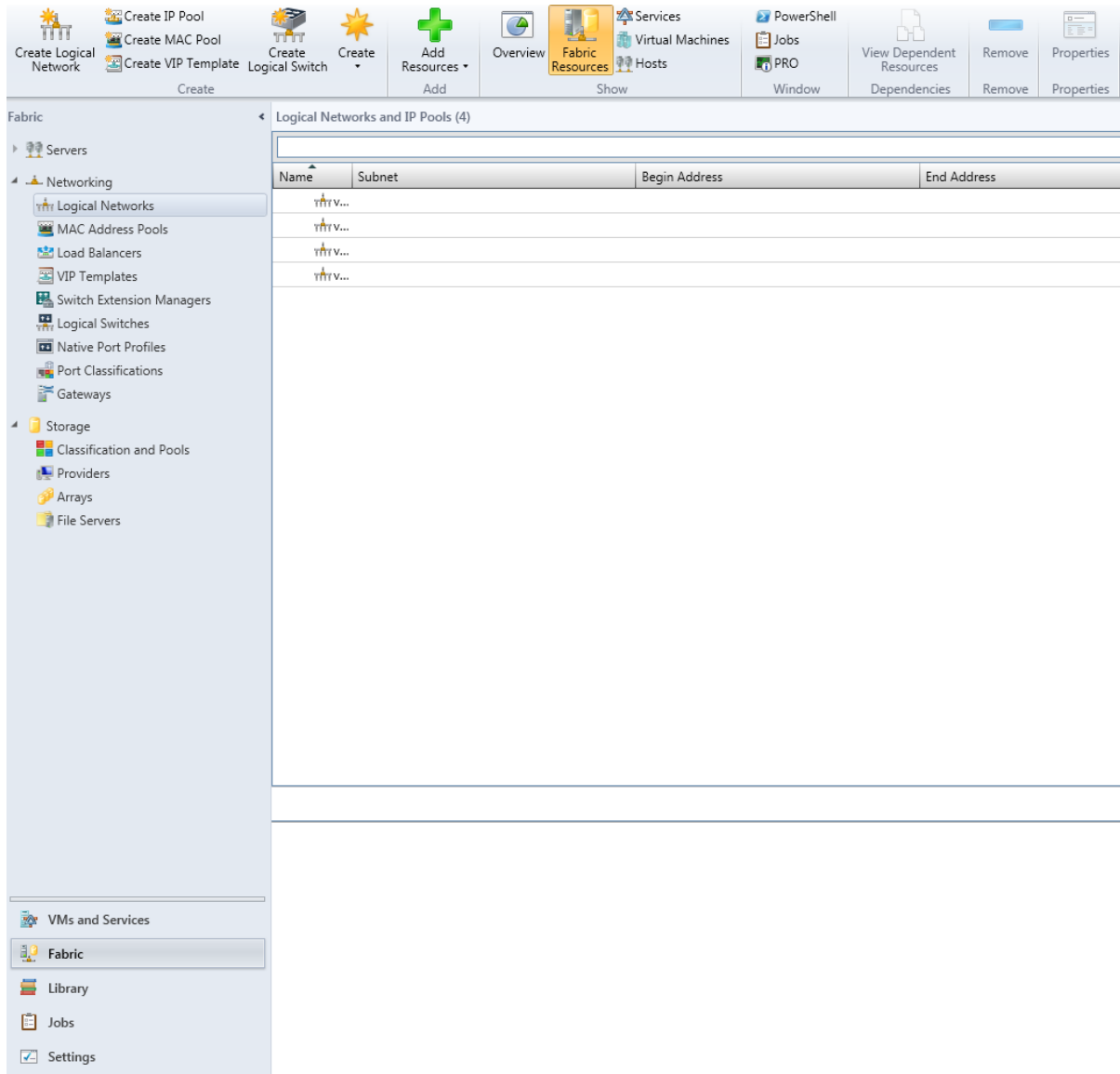
Context Menu:

- Create
- Clone
- Create VM Template
- Shut Down
- Power On
- Power Off
- Pause
- Resume
- Reset
- Save State
- Discard Saved State
- Migrate Storage
- Migrate Virtual Machine
- Store in Library
- Create Checkpoint
- Manage Checkpoints
- Refresh
- Repair
- Install Virtual Guest Services
- Connect or View
- Delete
- Properties

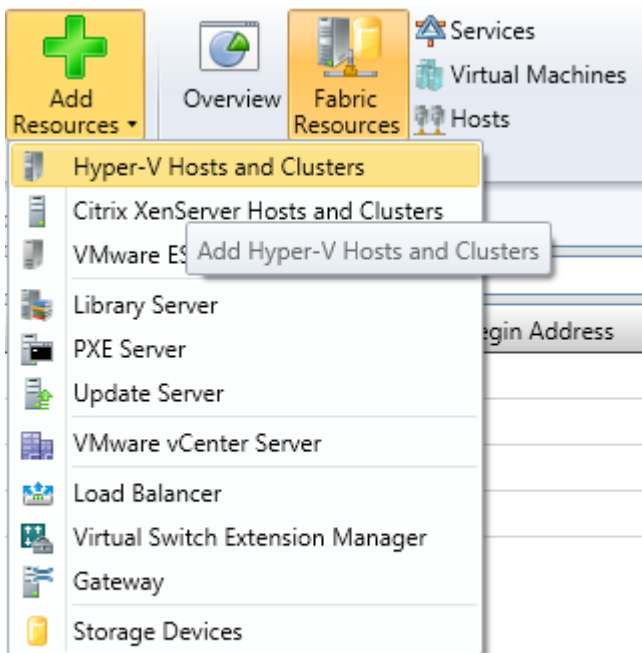
g) Creating a Hyper-V Failover Cluster & h) Managing a Hyper-V Failover Cluster

How to Add a Hyper-V Failover Cluster on Virtual Machine Manager 2012:

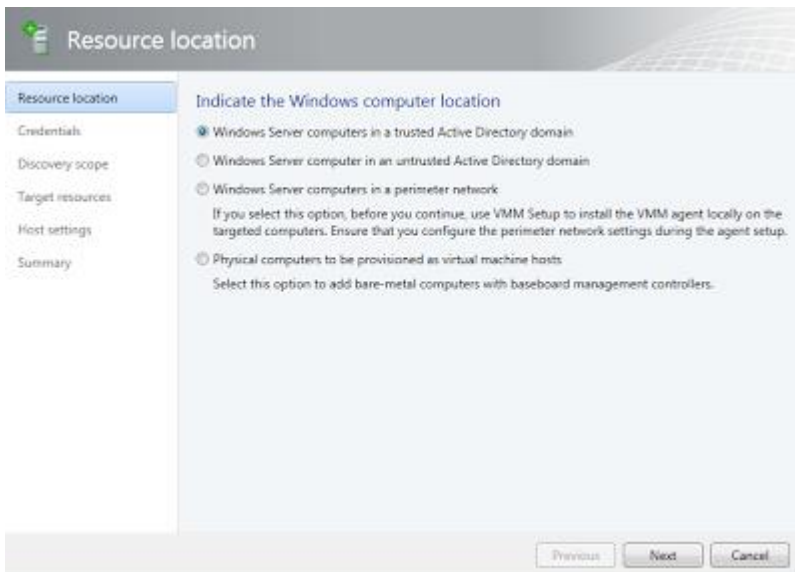
Go to Fabric and then click on Add Resources



Add Hyper-V Host and Clusters



In my Scenario I have my Hyper-V Cluster on a Trusted AD



Specify the credentials for discover the Hosts

The screenshot shows the 'Credentials' configuration window. On the left is a navigation pane with 'Credentials' selected. The main area is titled 'Specify the credentials to use for discovery'. It contains a 'Run As account' field with a 'Browse...' button, and a 'Manually enter the credentials' section with 'User name' and 'Password' fields. An example 'contoso\domainuser' is shown below the user name field. A warning icon and text at the bottom explain that the credentials must be a local administrator on the host machines.

Resource location
Credentials
Discovery scope
Target resources
Host settings
Summary

Specify the credentials to use for discovery

The Run As account or credentials will be used to discover computers and to install the Hyper-V role and the Virtual Machine Manager agent if necessary.

Use an existing Run As account
Run As account:

Manually enter the credentials
User name:
Example: contoso\domainuser
Password:

! The above provided credentials or Run As account should be a local administrator on the host machines. If a Run As account is provided, then it will be used while adding the host as well as for providing future access to the host during its lifetime. If credentials are entered manually, then they will only be used while adding the host. Once the host has been successfully added, the VMM service account will be added as local administrator on the host and used to provide any future access to it.

Specify the hosts that you want to discover

The screenshot shows the 'Discovery scope' configuration window. On the left is a navigation pane with 'Discovery scope' selected. The main area is titled 'Specify the search scope for virtual machine host candidates'. It offers two options: 'Specify Windows Server computers by names' (selected) and 'Specify an Active Directory query to search for Windows Server computers'. A text box for 'Computer names' contains 'Hyper-V_Cluster01'. There is a 'Skip AD verification' checkbox and a list of examples including 'server1', 'server1.contoso.com', '10.0.1.1', and '2a01:110-1e:3f8Rcf4423'.

Resource location
Credentials
Discovery scope
Target resources
Host settings
Summary

Specify the search scope for virtual machine host candidates

Search for computers by whole or partial names, FQDNs, and IP addresses. Alternatively, you may generate an Active Directory query to discover the desired computers.

Specify Windows Server computers by names
 Specify an Active Directory query to search for Windows Server computers

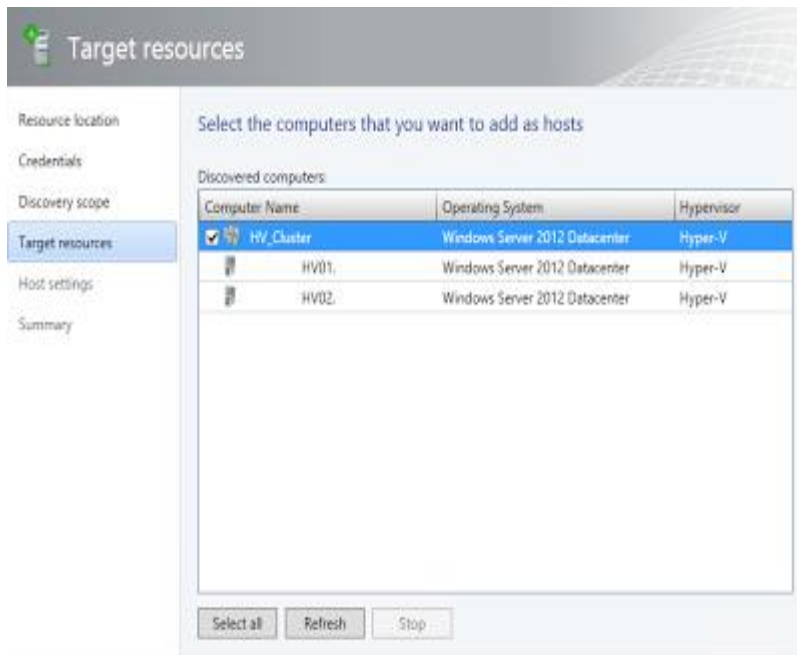
Enter the computer names of the hosts or host candidates that you want VMM to manage. Each computer name must be on a separate line.

Computer names:

Skip AD verification

Examples: server1
server1.contoso.com
10.0.1.1
2a01:110-1e:3f8Rcf4423

Now select the Hosts or Cluster



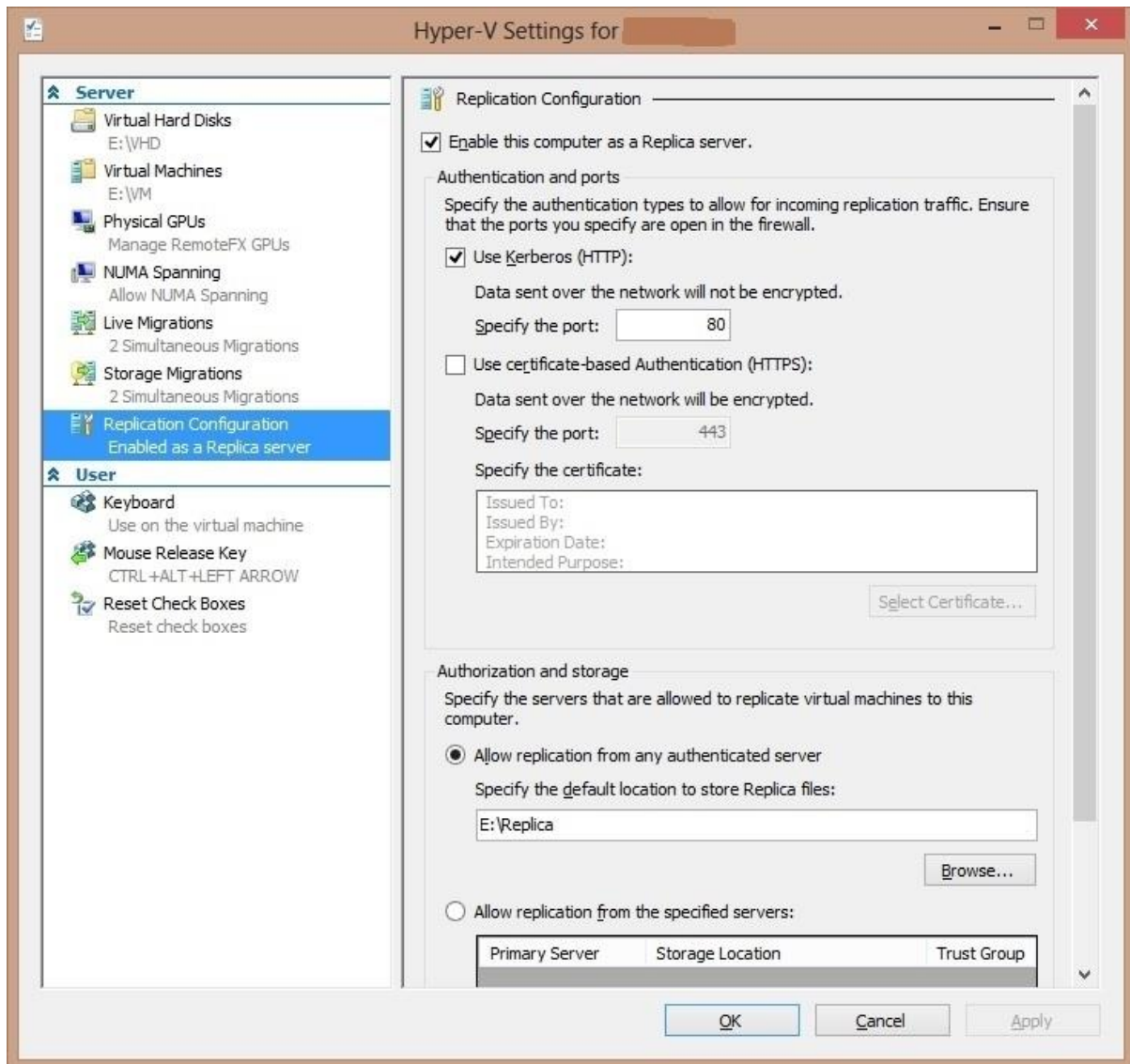
Cluster Added.

i) Configuring and Managing Hyper-V Replica

VM replication with Hyper-v is a built-in feature that can assist with business continuity and disaster recovery in the event of a failure. Server 2012 R2 and Hyper-v Server 2012 R2 allow for a third replica server, but R2 is not available as of the creation of this how-to.

This how-to assumes that you have a primary Hyper-v server already in production, and a host which you plan to use as your replica server online with Server 2012 and the Hyper-v role installed.

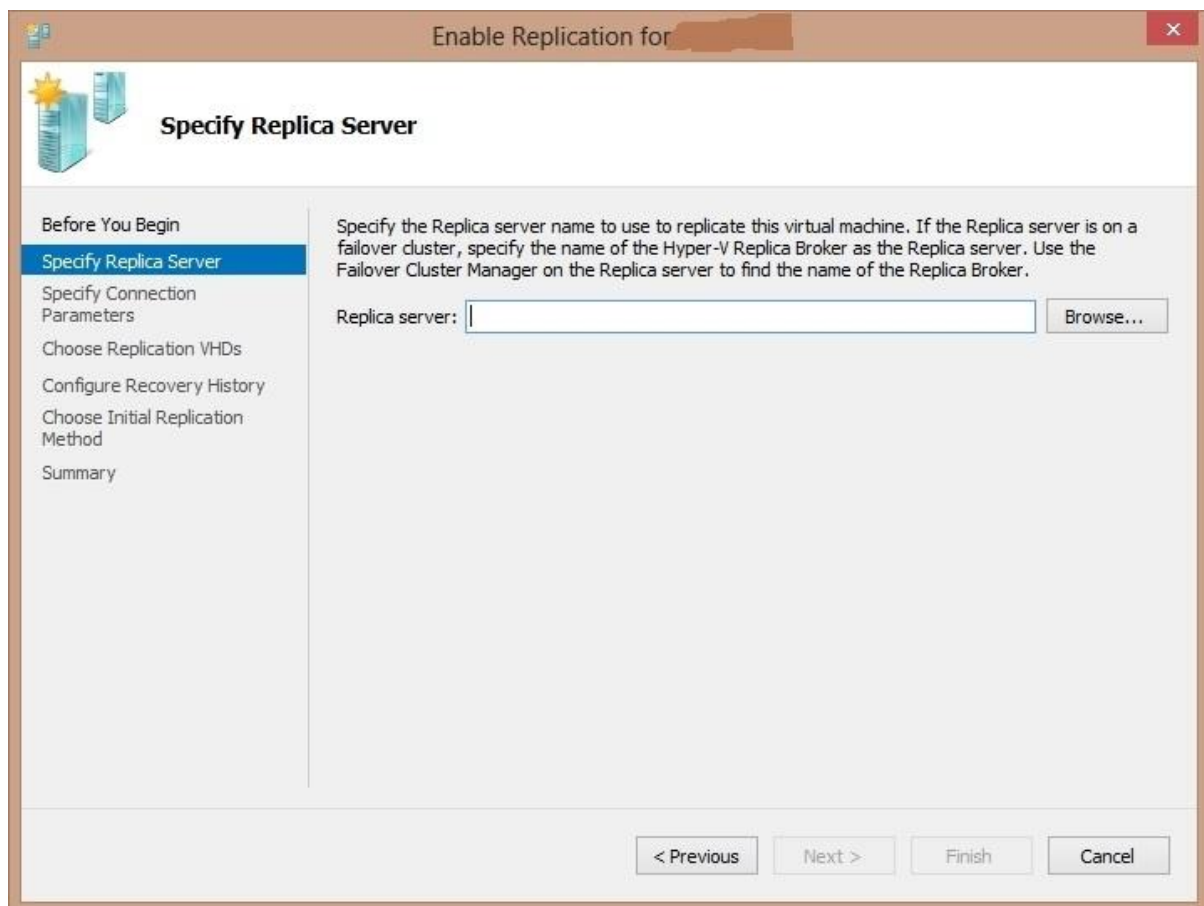
Step 1: Configure Your Secondary Hyper-v Host as a Replica Server



- Open Hyper-v Manager.
- Right click "Hyper-v Manager" in the left pane, and select "add server". Enter the computer name of the server you plan to use for your replica server and click "ok". The replica host will appear in the left pane.
- Right click on your replica host in the left pane, and select "Hyper-v Settings...".
- The Hyper-v Settings window will appear. Select "Replication Configuration" on the left side of the window.
- Check the "Enable this computer as a replica server" box.
- The "Use Kerberos (HTTP)" checkbox will be checked by default. With this setting selected, replica traffic is sent using HTTP. Hyper-v also allows you to configure the replica traffic to be sent as HTTPS traffic using certificate based authentication, but in this how-to, we will utilize HTTP.

- At the bottom of the "Replica Configuration" options, you have the option to allow replication from any authenticated server, or configure the replica server to only allow replication from specific servers. By default, "Allow replication from any authenticated server" is selected. Select the appropriate option (for this how-to, we will be using the default "Allow replication from any authenticated server" option).
- At the bottom of the "Replication Configuration" window, select the default location to store replica files. This is going to be where the VM's and VHD or VHDX files are stored on your replica server.
- Once all options in the replica configuration have been configured, click "OK" on the Hyper-v Settings window.

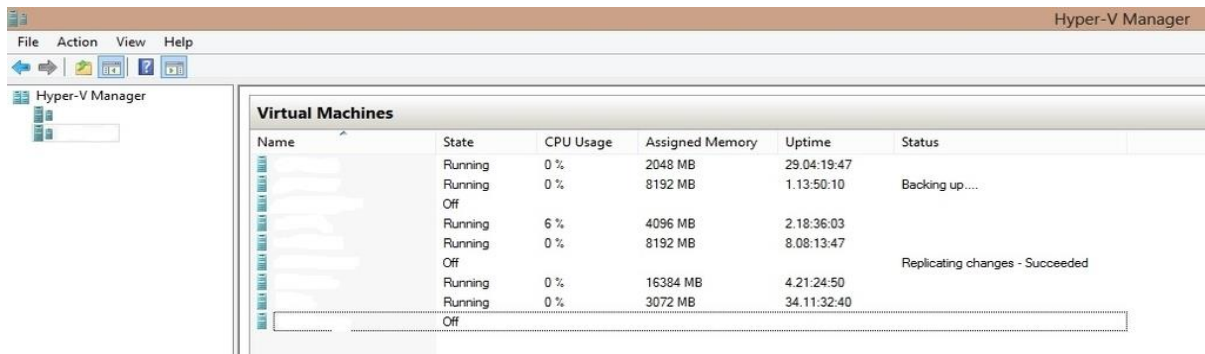
Step 2: Configure Replication of the Virtual Machines on the Primary Hyper-v Host



- Open Hyper-v Manager.
- Right click "Hyper-v Manager" in the left pane, and select "add server". Enter the computer name of your primary Hyper-v host and click "ok". The primary host will appear in the left pane.
- Select the primary host in the left pane. Your virtual machines will appear in the right pane.

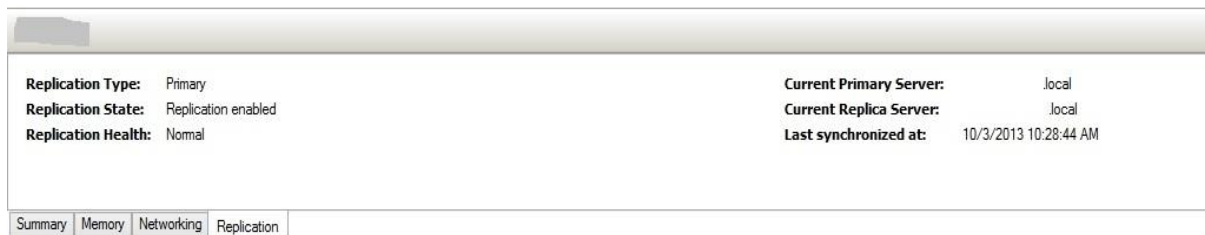
- Right click on a VM that you would like to replicate to your secondary server, and select "Enable Replication".
- The "Enable Replication" wizard will appear. Click "Next" on the "Before you Begin" section.
- The next section of the "Enable Replication" wizard asks for your replica server. Enter the name of your replica server, and click "Next". This section also allows you to browse for the server if you need to.
- The "Specify Connection Parameters" section of the wizard will appear. The replica server, replica server port, and authentication type will be grayed out because you configured these options on your replica previously. The checkbox for "Compress the data that is transmitted over the network" is checked by default, you can uncheck if you wish. Compressing the replica traffic uses additional system resources because the Hyper-v host has to compress the replica data before transmitting, and the Hyper-v replica host has to uncompress the data after it is received. Of course, compressing the replica traffic will decrease bandwidth usage. Click "Next".
- The "Choose Replicaion VHDs" section of the replication wizard will appear. By default, the VHD or VHDX file for the virtual machine that you are configuring replication for is selected. Unless there are any additional VHDs that you need to replicate (like if you have a separate VHD for a dedicated paging file), select "Next".
- The "Configure Recovery History" section of the replication wizard will appear. You have the option to only keep the latest recovery point on the replica server, or maintain additional recovery points. By default, the option for "only the latest recovery point" is selected. If you would like to keep additional recovery points (snapshots) on the replica server, chose "additional recovery points", and select the options that you require. Click "next".
- The "Choose Initial Replication Method" section of the wizard will appear. You can choose to send the initial copy of the network, or send the initial copy using external media. Be aware that sending the initial replica between sites or over a slow connection can take quite a long time. You can also select the option to use an existing virtual machine on the replica server as the initial copy, which you can use if you have restored a copy of the VM to the replica server. The restored VM will be used as the initial copy. For this how-to, we are going to select the default option, "Send initial copy over the network". At the bottom of this section of the wizard, select whether you would like to start replication immediately, or start at a specific time. Select "next" to continue.
- The "Completing the Enable Replication Wizard" section will appear. This page provides a summary of the options that you selected in the previous sections of the wizard. Click "Finish" to start the initial replication.

Step 3: Monitor Initial Replication:



- After you have started the initial replication, you can monitor the replication status in Hyper-v Manager.
- Select your Hyper-v Host in the left pane, and your VM's will appear in the right pane. Within the "status" section of the VM on the right, it should state "Sending Initial Replica" and provide a completion percentage for the VM that you just configured replication.
- If you select your replica host from the right pane, the status for the VM will be listed as "receiving initial replica" and it should provide the same percentage that your Hyper-v host displays.

Step 4: Monitor Ongoing Replication:



- After the initial replica has completed, you can monitor the ongoing replication health from Hyper-v Manager.
- From Hyper-v Manager, select your Hyper-v Host from the left pane. Your VM's will appear in the right pane.
- Select the VM from which you configured replication.
- At the bottom of the Hyper-v Manager window, select the "Replication" tab.
- If replication is occurring successfully, your replication health will be listed as "Normal". The replication tab will also display the last synchronization.
- Hyper-v replication can also be monitored by Microsoft System Center Operations Manager 2012.

Sign: _____

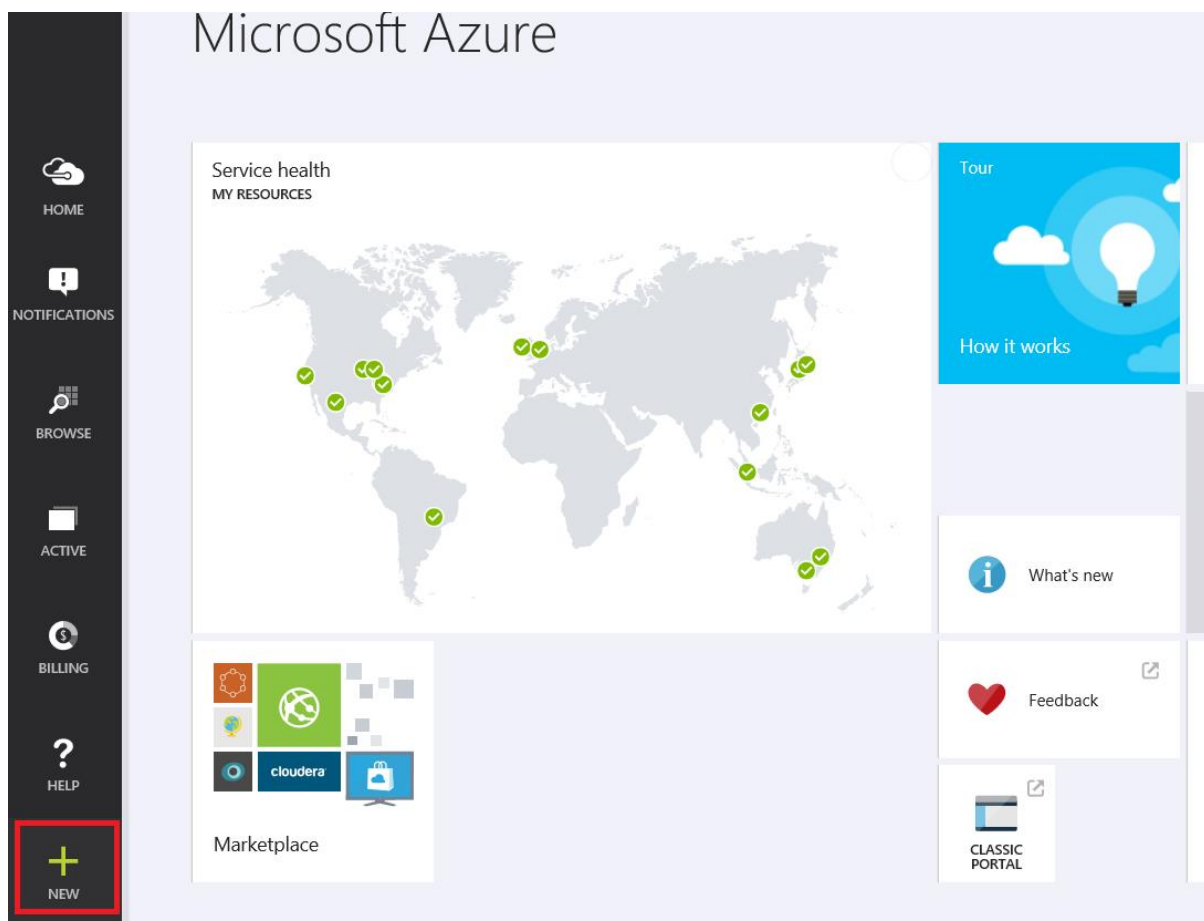
Practical No 2: Provisioning Self-Service using App-Controller.

a) Deploying a new virtual machine running Windows Server 2012 Data center edition to Windows Azure cloud. (Should be performed Online)

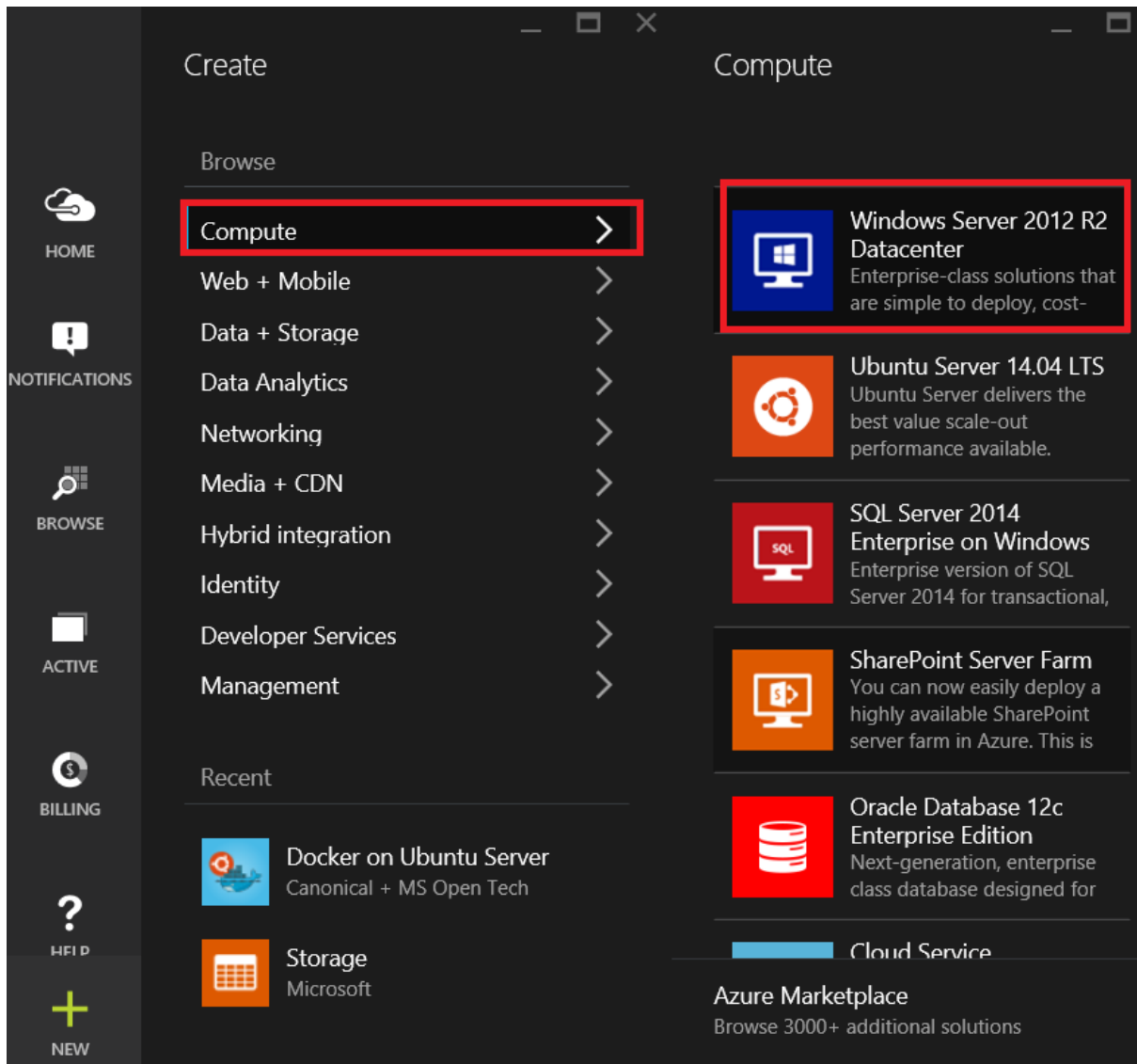
How to create the virtual machine:

This section shows you how to use the Preview portal to create a VM, using Windows Server 2012 R2 Datacenter as an example. You can use Azure's default settings for most of the configuration and create the VM in just a few minutes.

1. Sign in to the Preview portal.
2. On the Hub menu, click New.



3. In the New blade, click Compute, and then click Windows Server 2012 R2 Datacenter.




4. On the Create VM blade, fill in the Host Name you want for the VM, the administrative User Name, and a strong Password.

Create VM

WINDOWS SERVER 2012 R2 DATACENTER

Host Name

azurevm 


User Name

azureuser  


Password

●●●●●●●● 

PRICING TIER

Basic A1 

OPTIONAL CONFIGURATION

Network, storage, diagnostics 

RESOURCE GROUP

Group-5 

SUBSCRIPTION

Internal Consumption 

LOCATION

Central US 

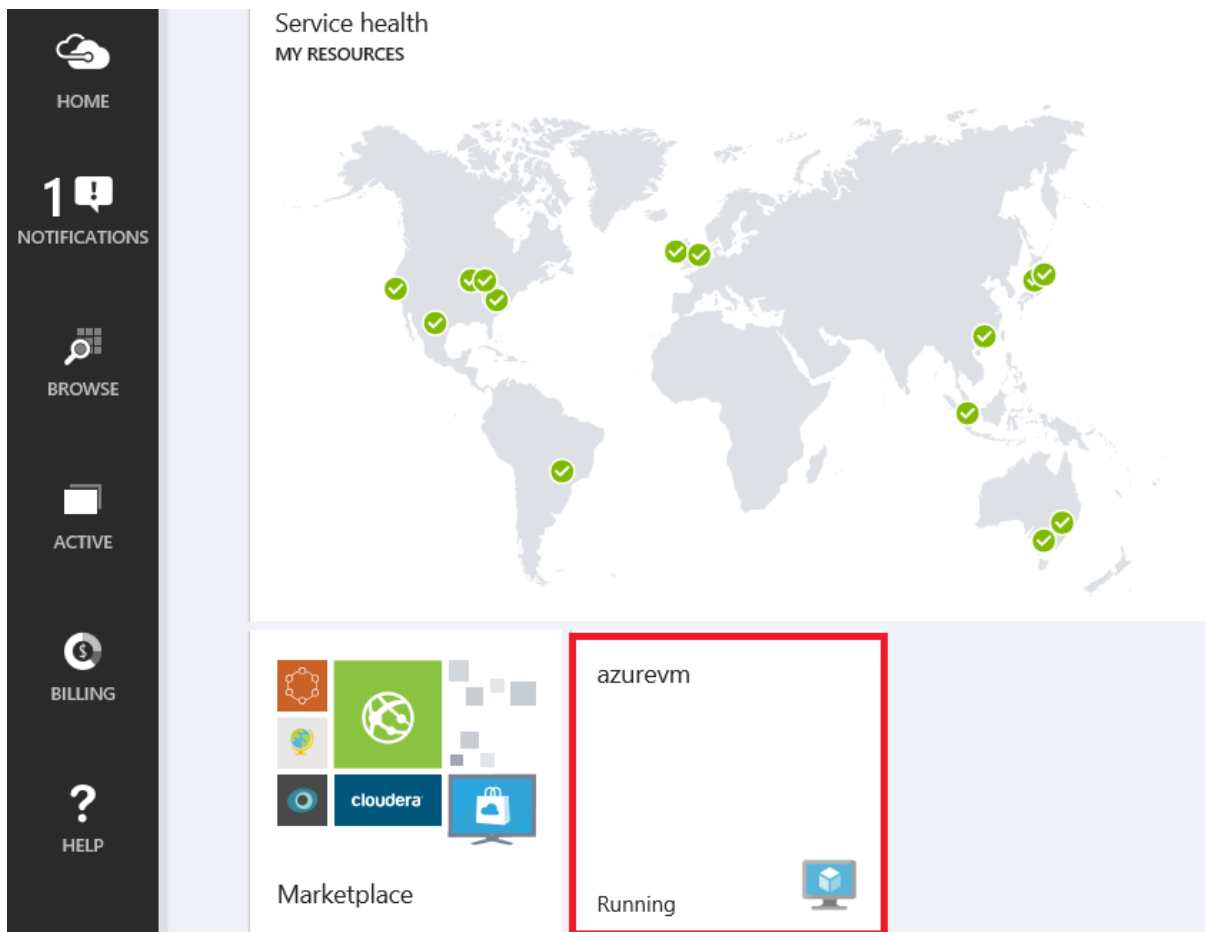
Pin to Startboard

Create

5. Review the default settings, such as the Pricing Tier and Optional Configuration. These choices affect the size of VM as well as networking options such as domain membership. For example, to try out Premium Storage on a virtual machine, you'll need to pick a region and size that supports it. For your first virtual machine, the defaults are usually fine.

6. When you're done reviewing or updating the settings, click Create.

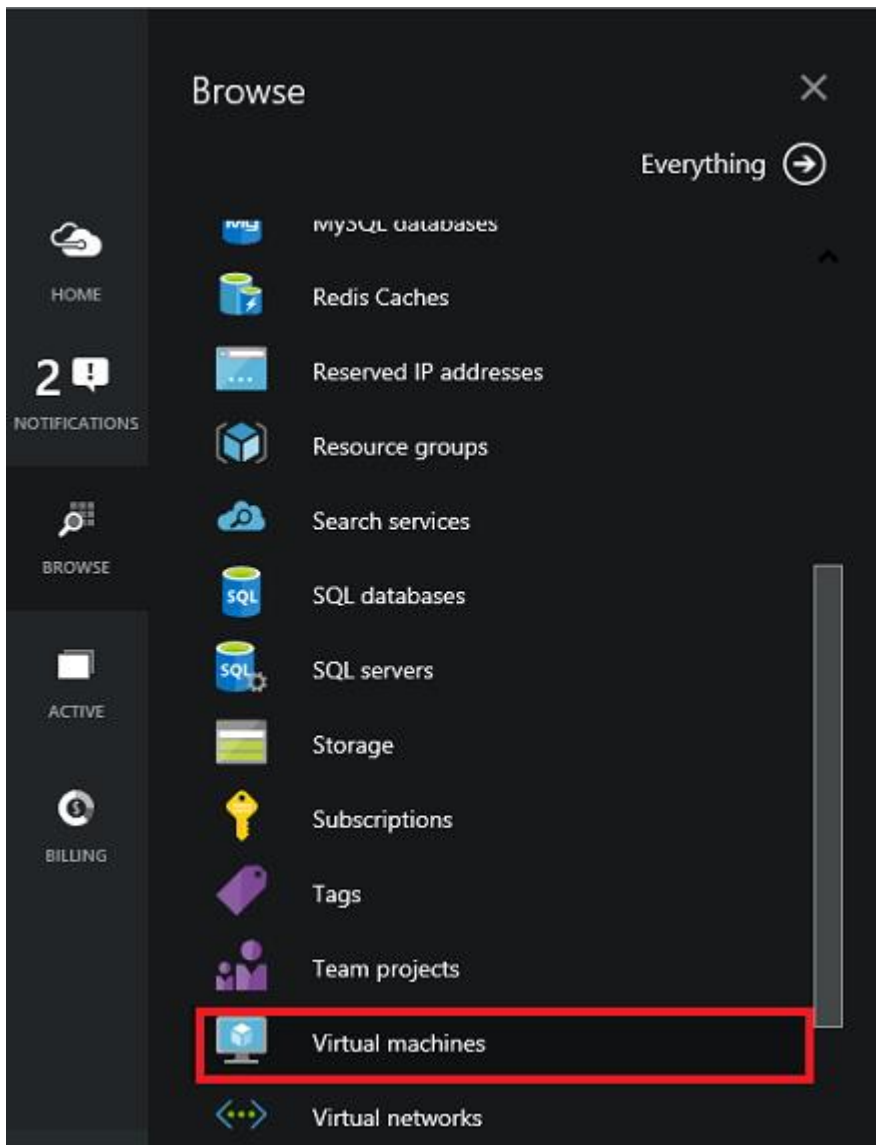
7. While Azure creates the VM, you can keep track of the progress in Notifications, in the Hub menu. After Azure creates the VM, you'll see it on your Startboard.



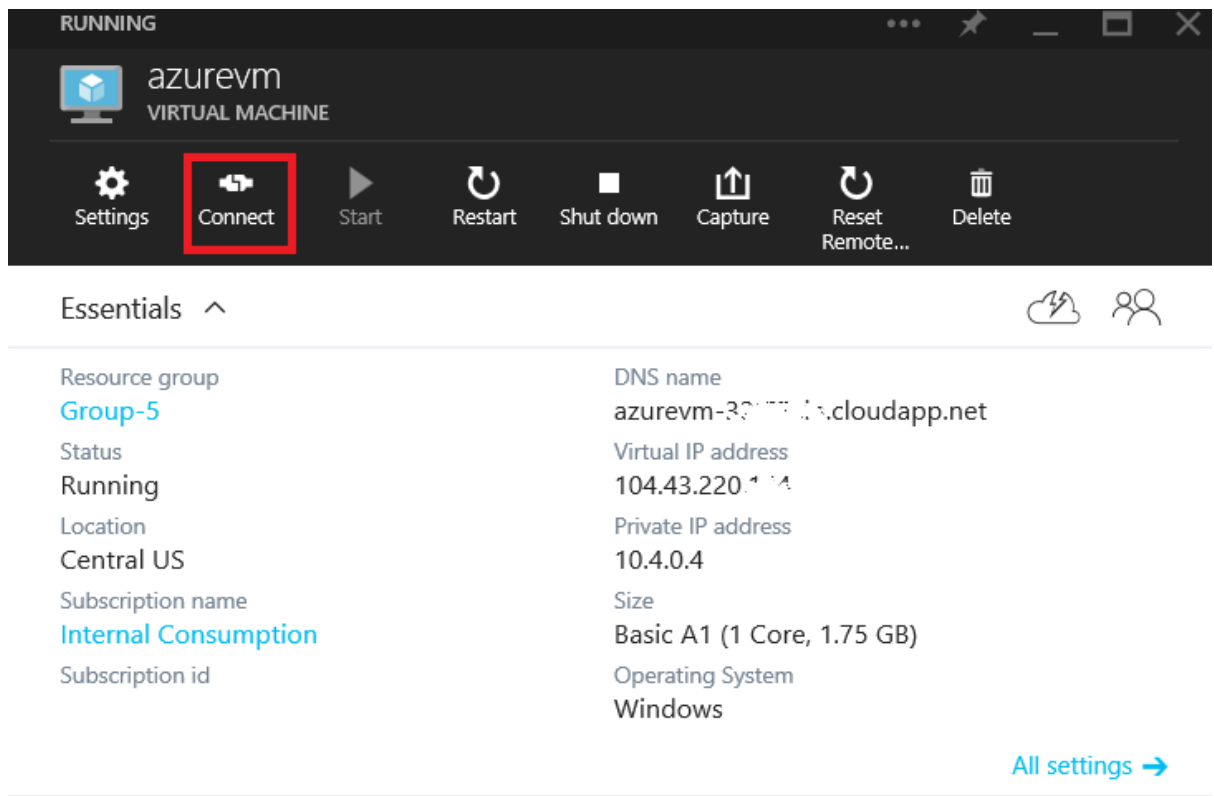
How to log on to the virtual machine after you create it:

This section shows you how to log on to the VM so you can manage its settings and the applications that you'll run on it.

1. If you haven't already done so, sign in to the Preview portal.
2. Click your VM on the Startboard. If you need to find it, click Browse and then click Virtual machines. Then select your VM from the list.



3. On the VM blade, click **Connect** at the top.



4. Click Open to use the Remote Desktop Protocol file that was automatically created for the virtual machine.
 5. Click Connect to proceed with the connection process.
 6. Type the user name and password of the administrative account on the virtual machine, and then click OK.
 7. Click Yes to verify the identity of the virtual machine.
- You can now work with the virtual machine just as you would with any other server.

b) Deploying a new virtual machine running Windows Server 2012 Data center edition to Hyper-V using App-Controller & f) Deploying a Virtual Machine in App Controller

Log on to the App Controller website, which takes the form <https://<App Controller Server>>. Next, choose the Settings navigation node and the Connections child navigation node. Choose the Connect, SCVMM action, as shown in Figure 1.

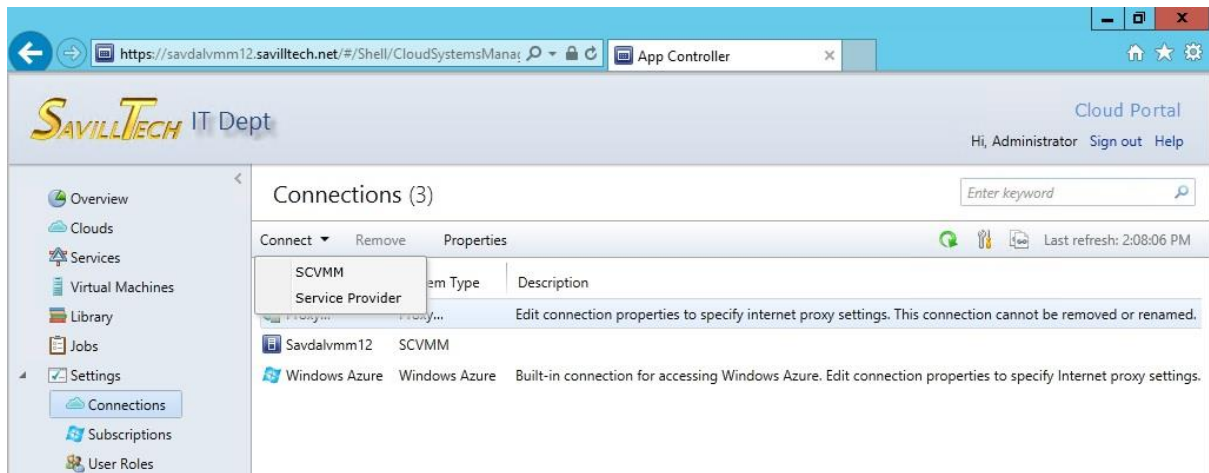
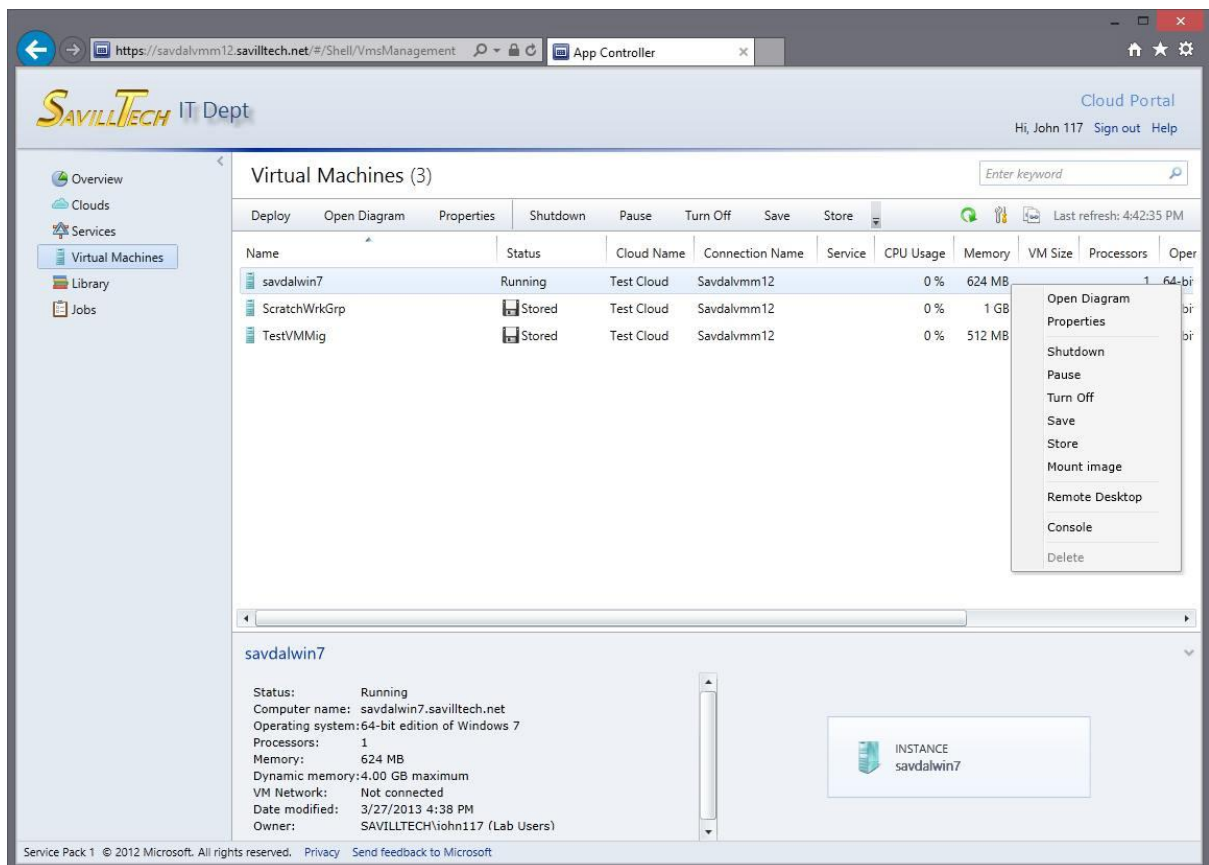


Figure 1: Connecting App Controller to VMM

Once you are connected to VMM you will have access to all the Virtual machine and can also deploy new Virtual machines.



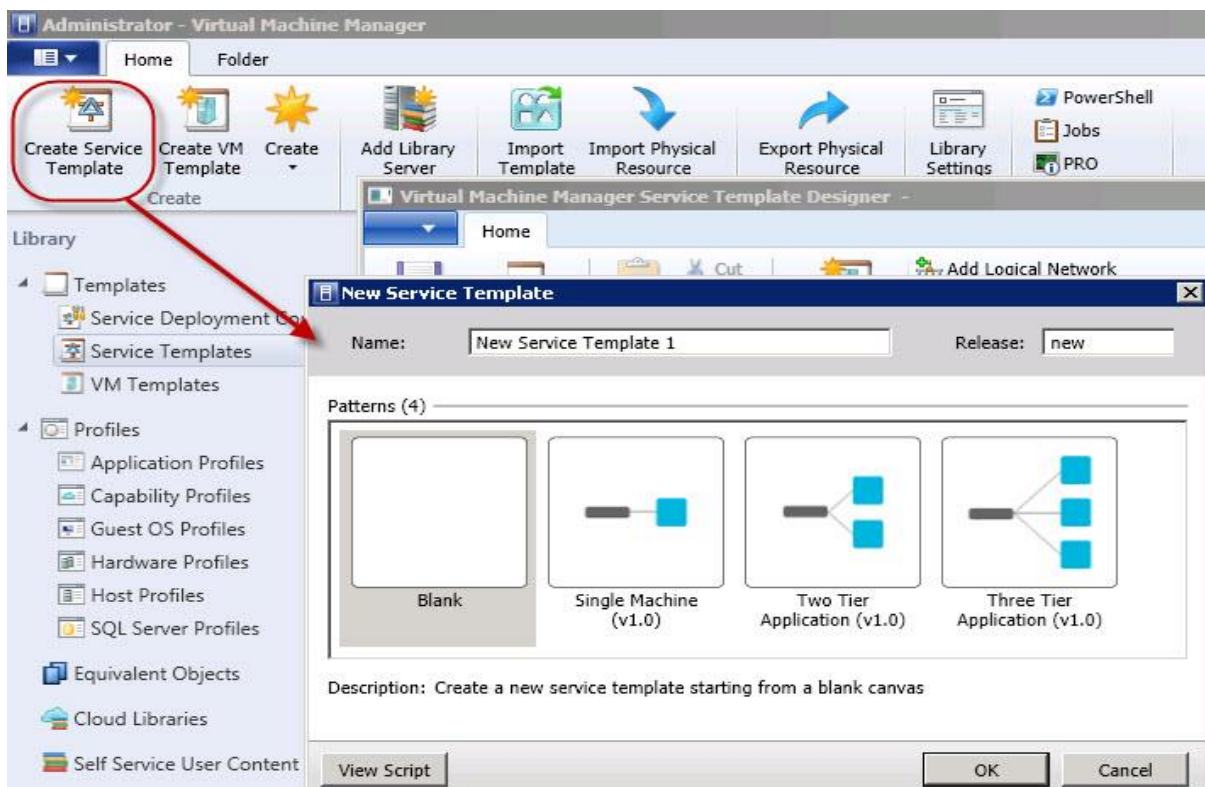
c) Creating a Service Template & d) Deploying a Service and Updating a Service Template

Create a service template in VMM

Follow these steps in System Center 2012 VMM to create a service template. A prerequisite is that you have defined VM Templates for each VM application role that you want to add to the service template. Also you need to have created a private cloud in VMM with resources available to match those required by the VM Templates. These prerequisites will allow VMM to match application VMs to fabric resources that will support them.

1. Navigate to the Library space and click the Create Service Template button in the ribbon.
2. Select one of the predefined service templates and press OK. (See **Figure B**.)
3. Observe your list of VM templates on the left side of the designer (see Figure A, VM Templates tab).
4. Drag VM templates into the designer canvas to add VMs to that tier. Alternatively, drag a VM template onto a tier to replace the default settings for that tier.
5. Add hardware load balancers and logical networks to the designer canvas. Use the connector button in the ribbon to connect network interfaces.
6. Press the Save and Validate button in the ribbon when done, then exit the designer.

Figure B:

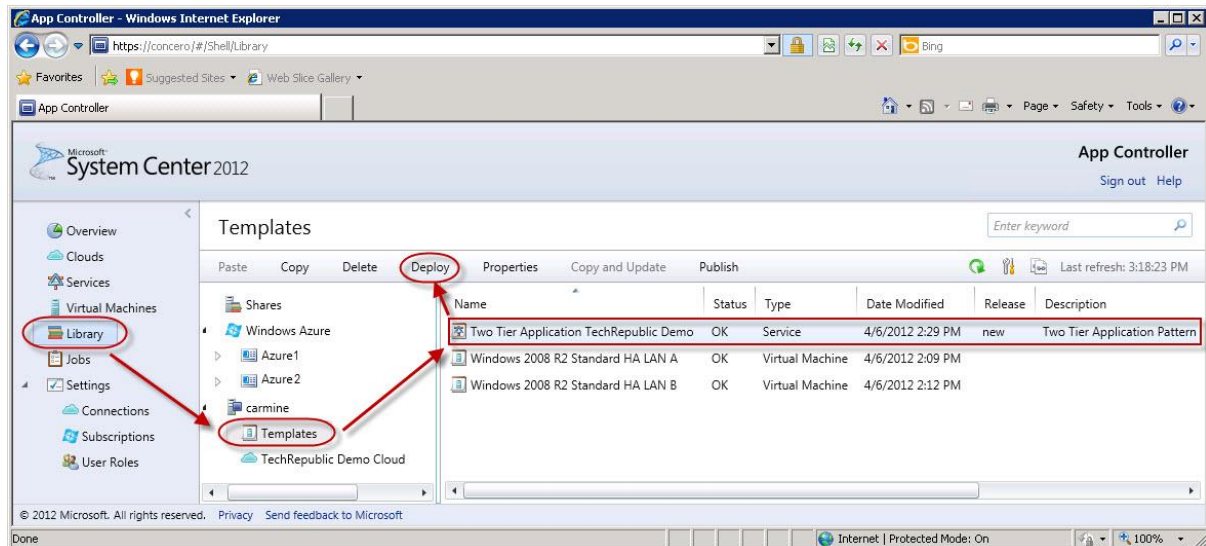


Creating a service template in the VMM Library space.

Use a service template in App Controller:

App Controller should be connected to our on-premise VMM server for access to our private cloud resources, as well as connecting to Azure for management of our public cloud subscriptions. Now that we have defined a service template, we can use App Controller to actually launch the application deployment to our private cloud.

Figure C:

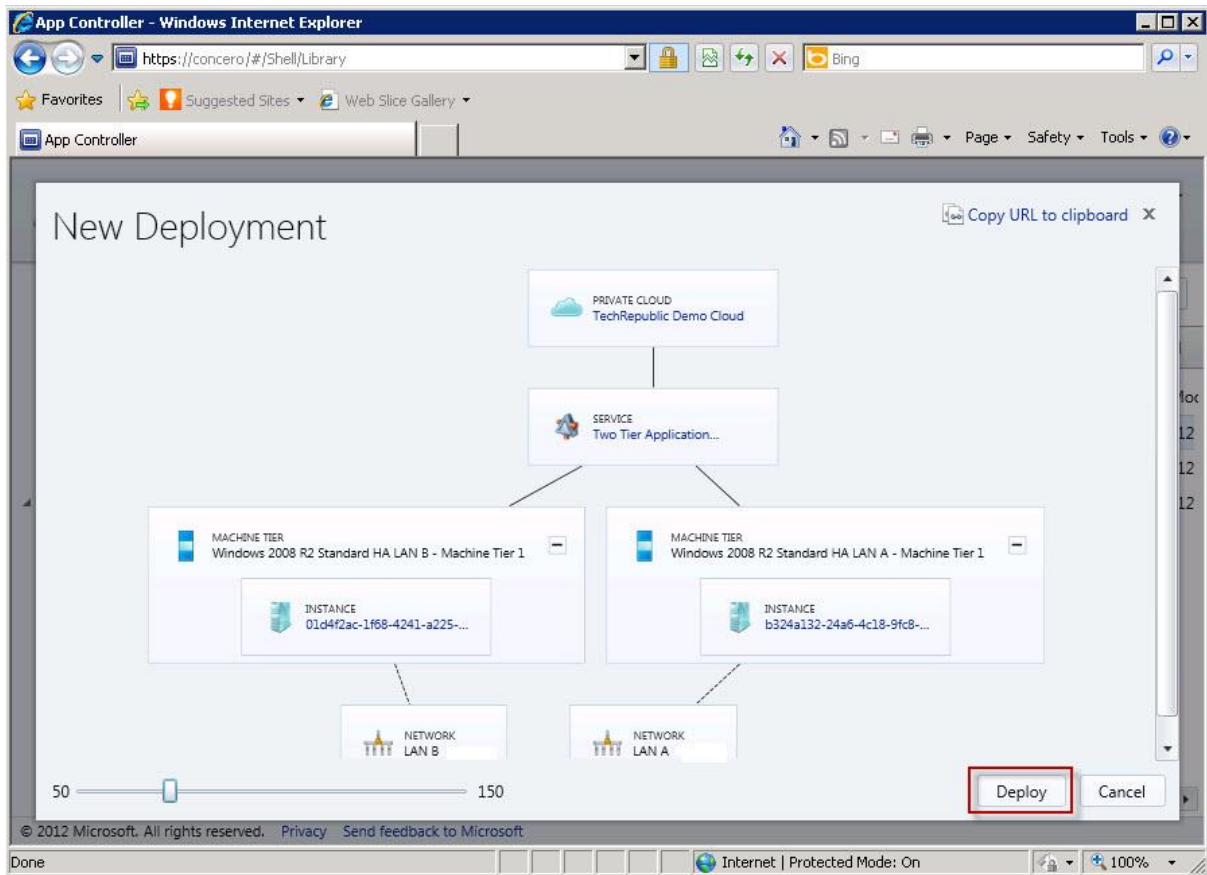


App Controller: Self-service deployment of an application using a service template.

Figure C from the App Controller web portal lists the same Two Tier Application template seen in the VMM template designer in **Figure A**. Here are the steps to deploy the application with App Controller:

1. From the App Controller Library space, select Templates, then select the template of the application you want to deploy, and click on Deploy in the templates menu.
2. You will be presented with a screen to select which private cloud to deploy the application to, then a graphical representation of the application you are about to deploy as seen in **Figure D**.
3. Click the Deploy button and VMM will start to execute your instructions and deploy the application to the fabric.

Figure D:

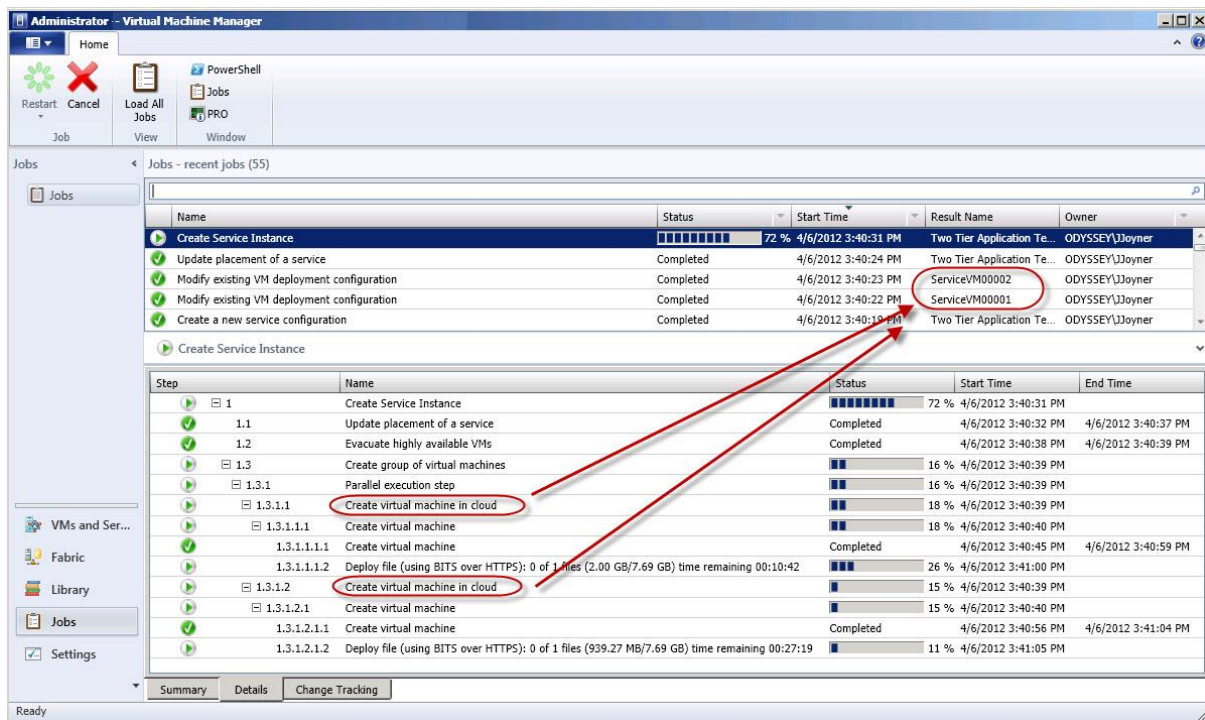


App Controller: Graphical depiction of the application you are about to deploy.

Figure E below shows the progress of VMM as the jobs are executing. These are the jobs to deploy the application to the private cloud selected by the user with App Controller.

- Two VMs (ServiceVM00001 and ServiceVM00002) have been automatically named and placed (one VM each) in two host clusters in the private cloud.
- In the design of this application, the network of the host cluster matches the network fault domain the VM is assigned to.
- The fact that both the VM Templates and the host clusters in the private cloud have "LAN A" and "LAN B" associations permits VMM to intelligently distribute the VMs to host clusters that preserve the isolation between the fault domains.

Figure E:



Watching the progress of deploying the two-tier application in the VMM console.

e) Configuring App Controller

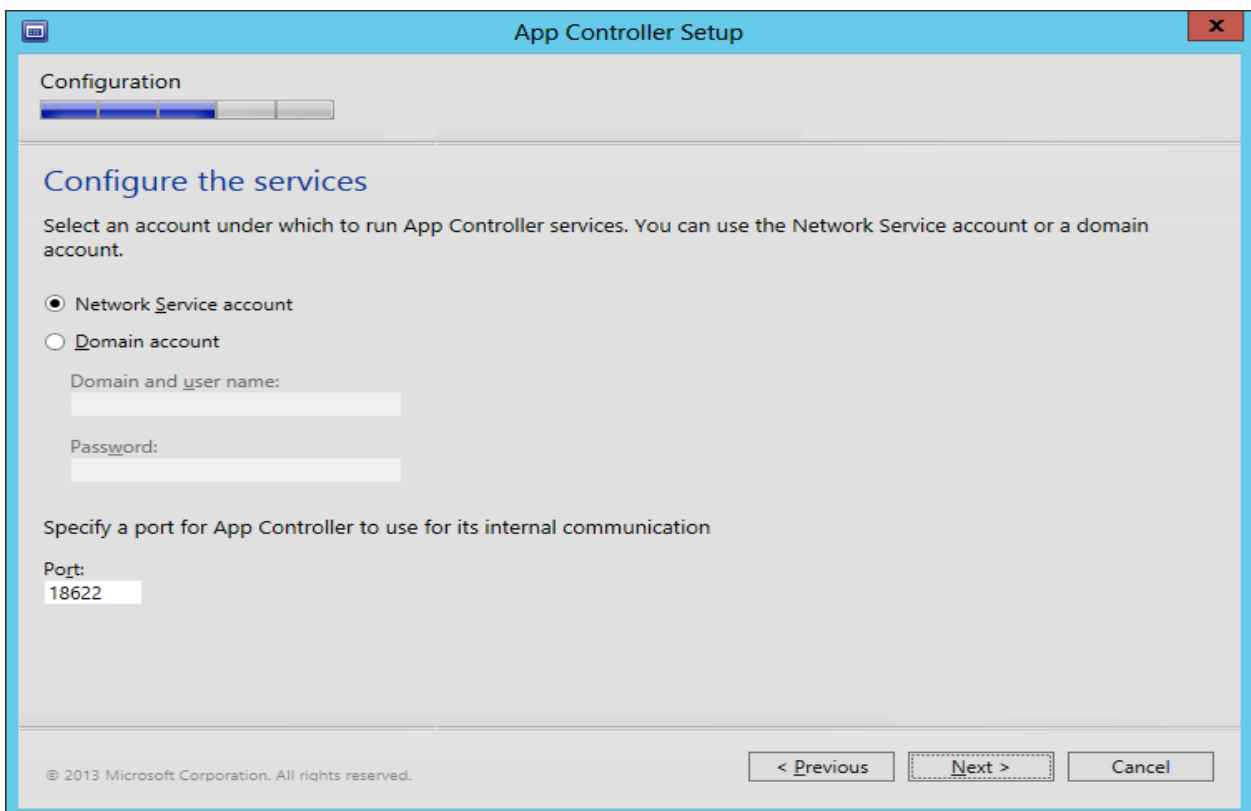
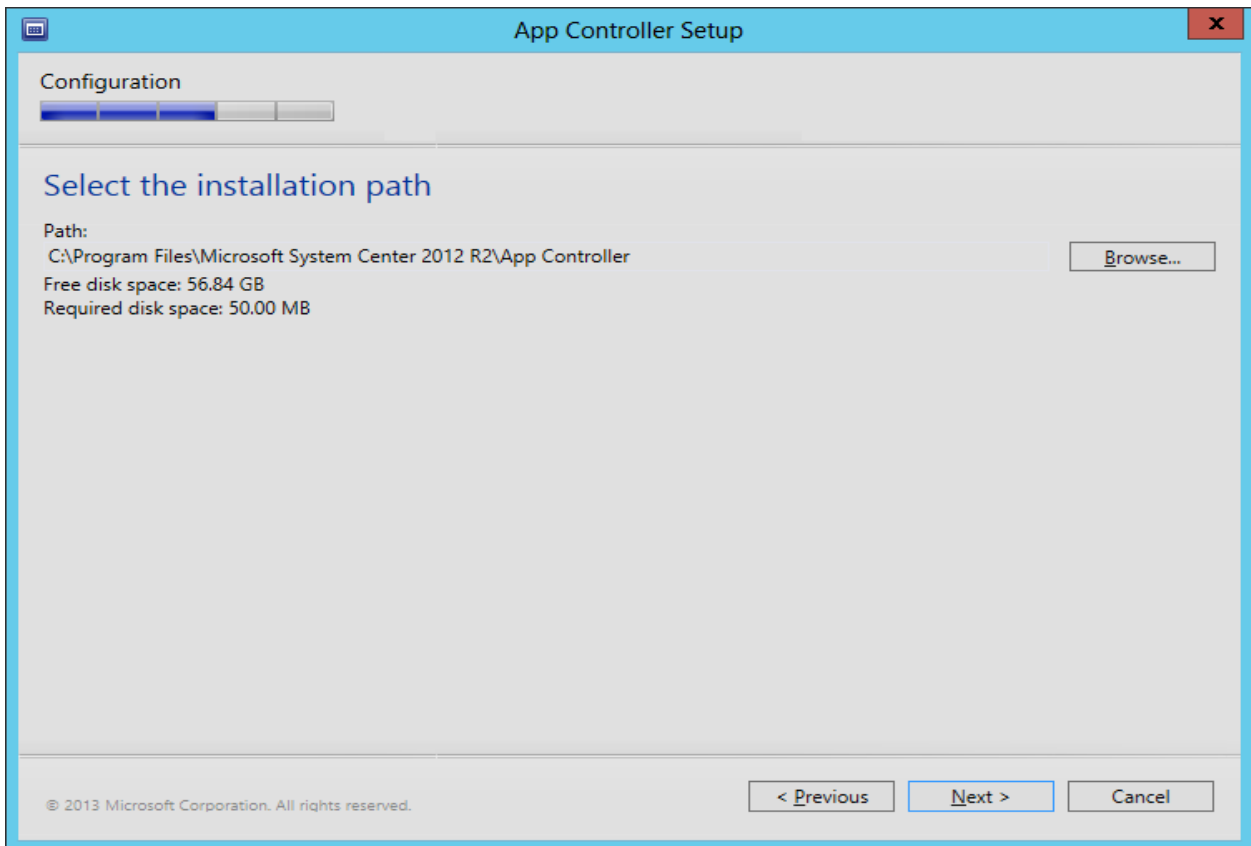
App Controller provides a self-service cloud experience for deploying and managing virtual machines (VMs) and services in cloud environments. The self-service experience provided by App Controller through a web browser is consistent across all types of clouds, including private, public, and hosted clouds. This capability makes App Controller the ideal platform for implementing the hybrid computing model.

Installation of App Controller

- **Prerequisites**
 - Installing VMM Console
 - Creating Self-Signed Certificate in IIS

- Installation





App Controller Setup

Configuration

Configure the website

Specify the binding settings you want to use for the App Controller website.

Type: **HTTPS** IP address: **All unassigned** Port: **446**

Generate self-signed certificate

Use existing certificate:

CLOUDDC.CLOUDAD.com

© 2013 Microsoft Corporation. All rights reserved.

App Controller Setup

Configuration

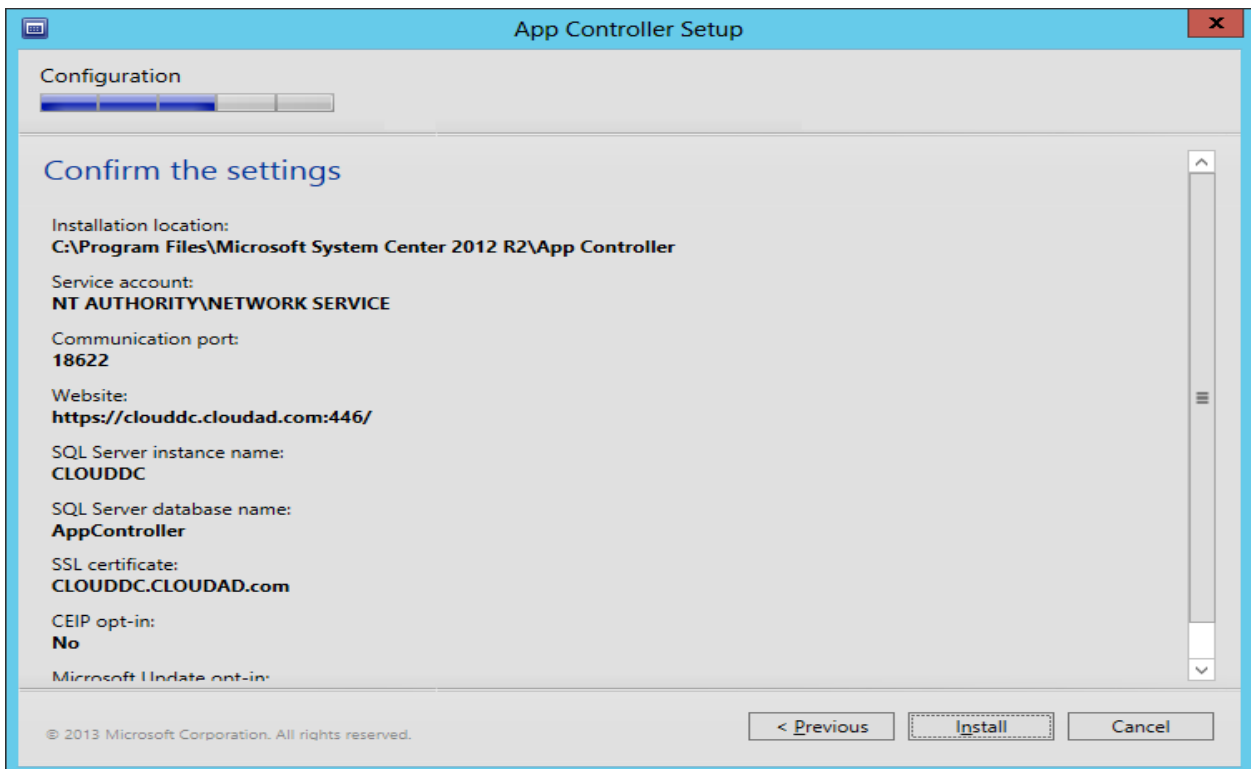
Configure the SQL Server database

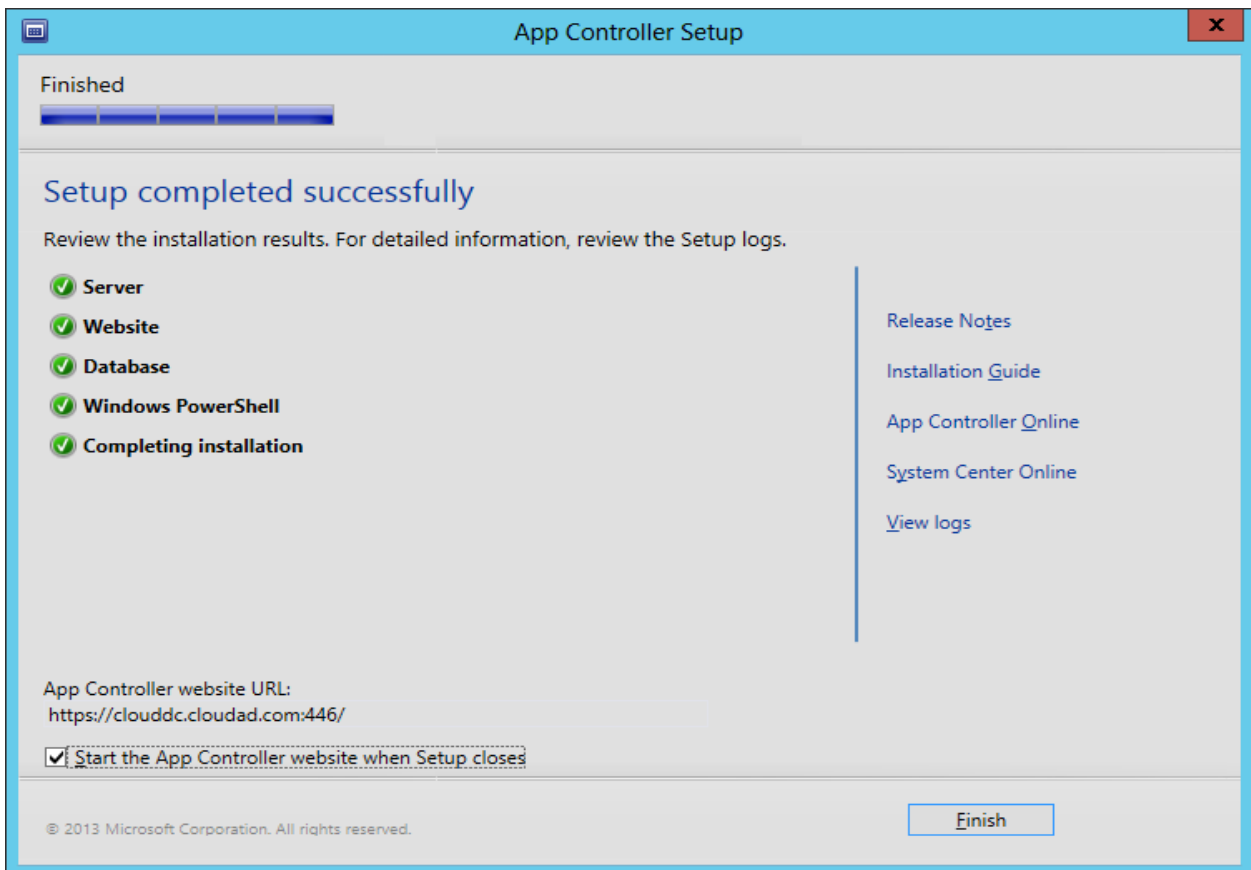
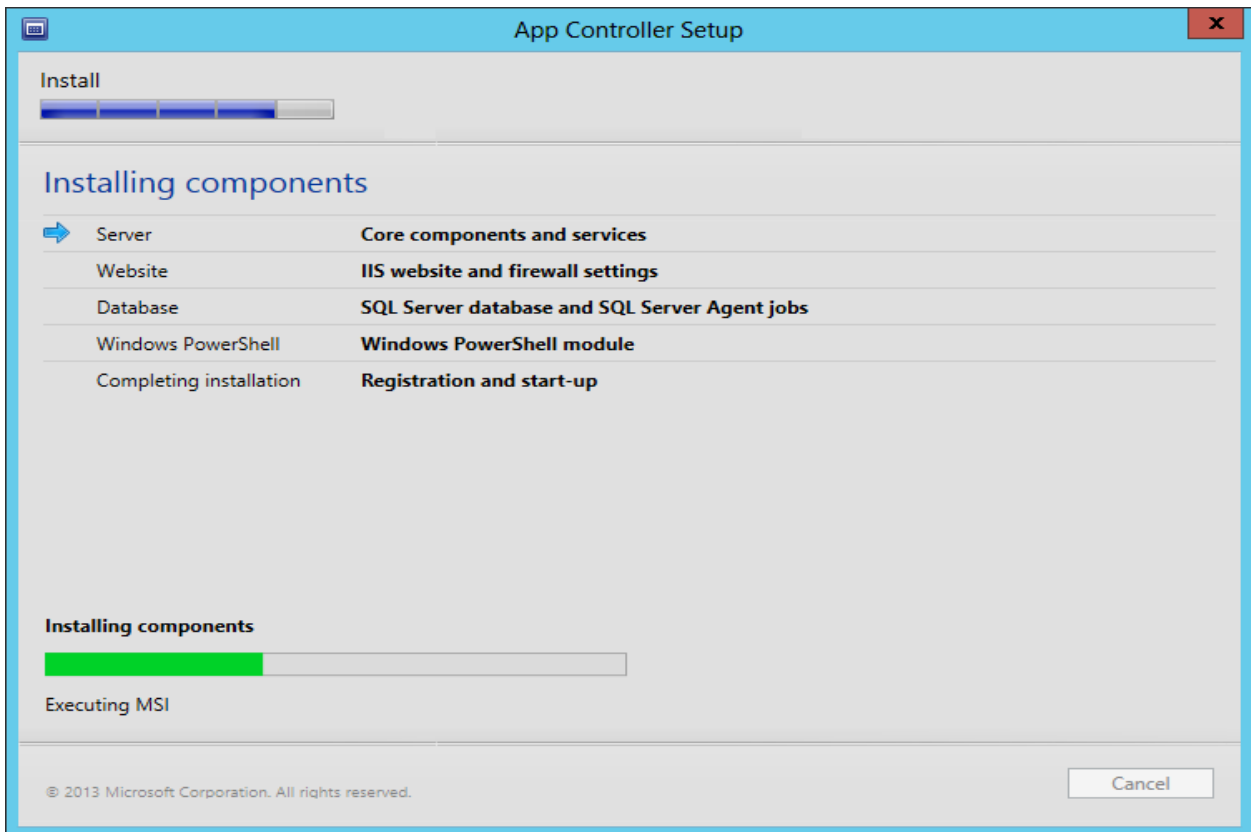
Server name: **CLOUDDC** Port:

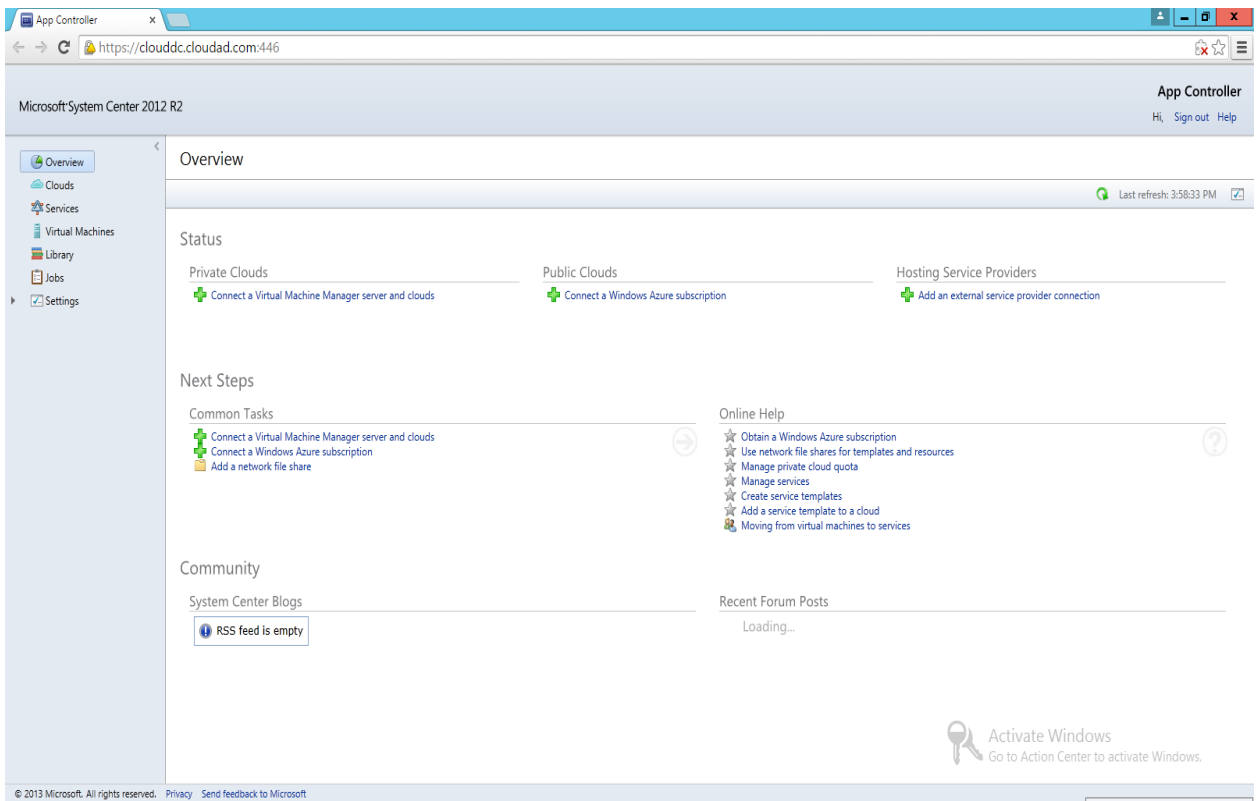
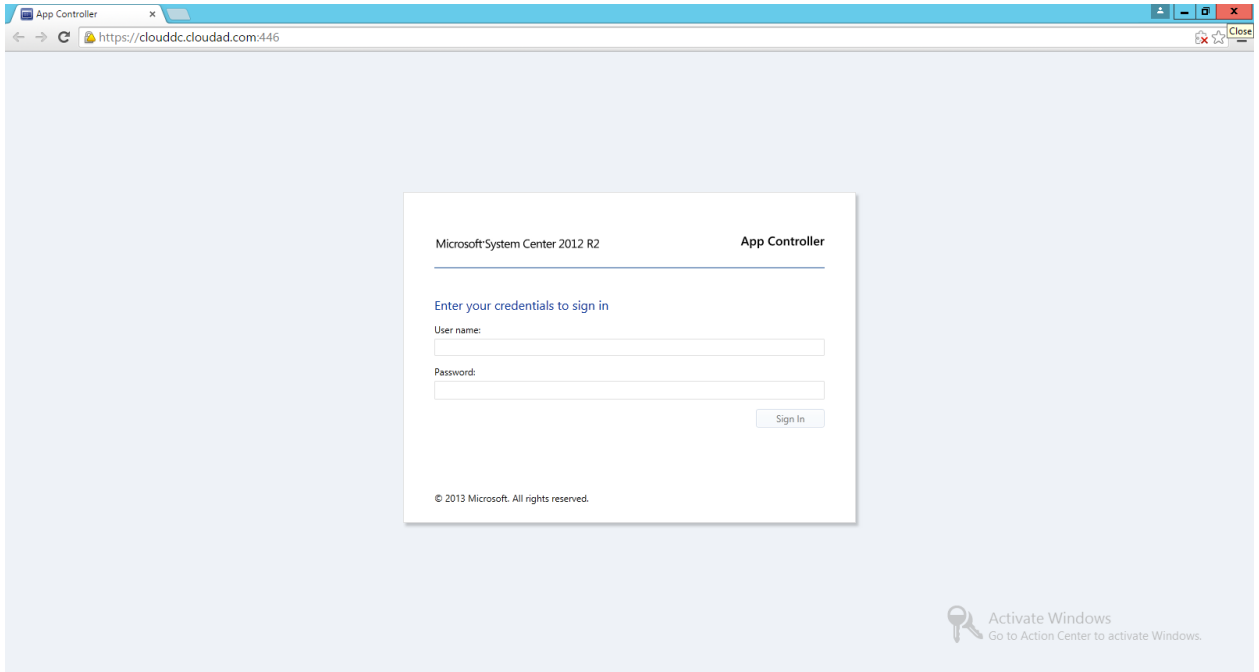
Instance name: **MSSQLSERVER**

Database name: **AppController**

© 2013 Microsoft Corporation. All rights reserved.







Sign: _____

Practical No 3: Managing Private cloud with App Controller.

a) Deploying a new virtual machine.

To deploy a new application workload to an existing private cloud using System Center 2012 R2 App Controller, complete the following steps:

1. Click the Clouds page and then right-click the private cloud to which the new application workload should be deployed and select the Deploy option shown in Figure 2-14.

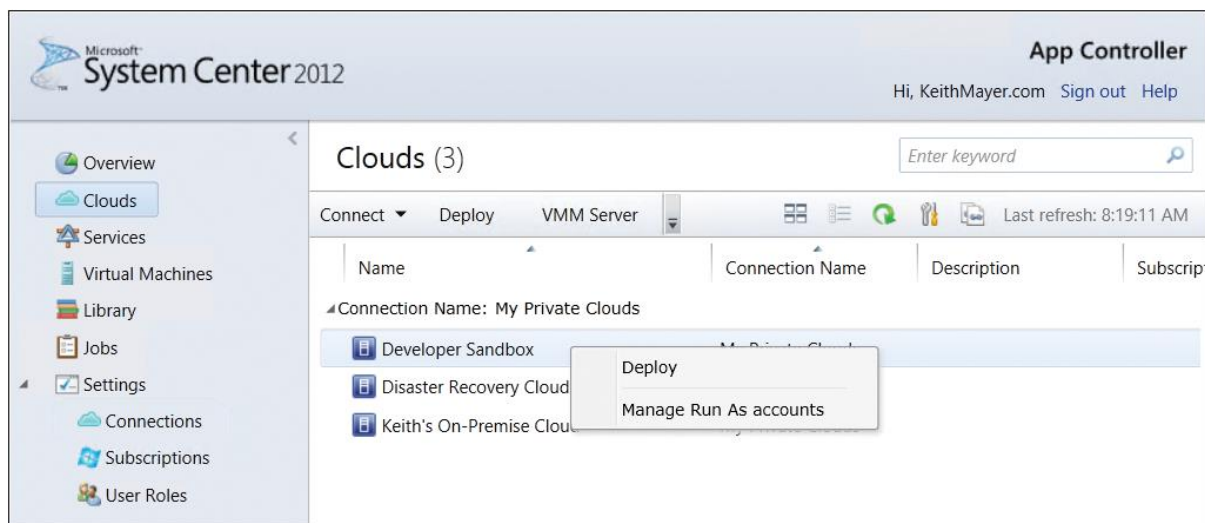


FIGURE 2-14 A new workload can be deployed to a private cloud.

2. From the right-click menu, select Deploy to launch the New Deployment dialog box, as shown in Figure 2-15.

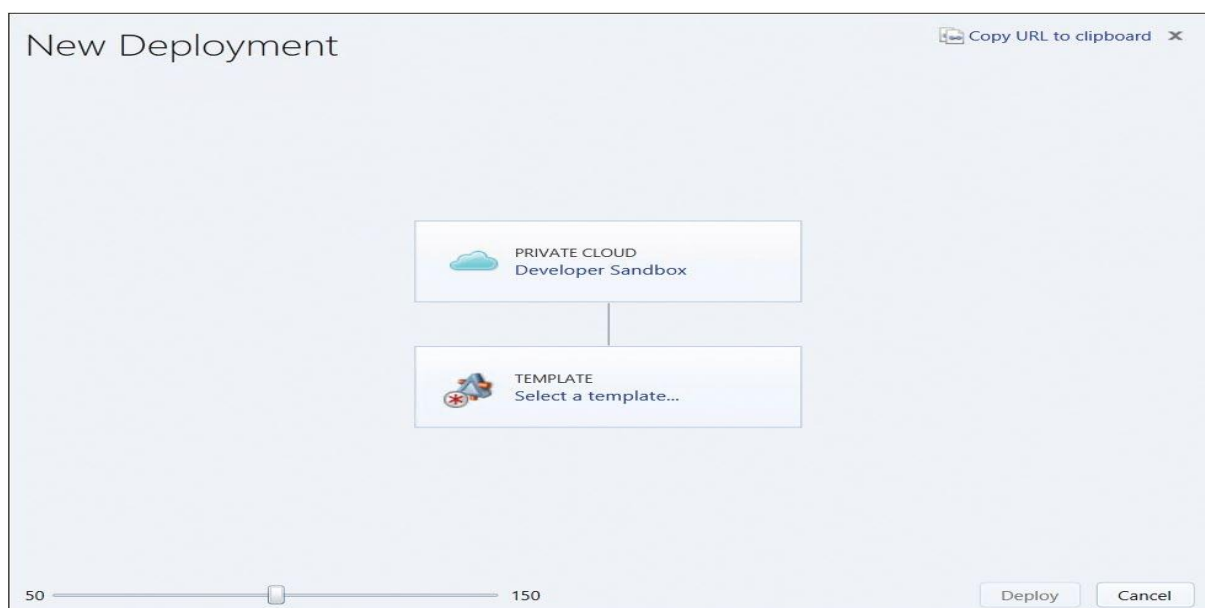


FIGURE 2-15 Use the New Deployment dialog box to select a template.

3. On the New Deployment dialog box, click Select A Template and select the appropriate VM Template or Service Template previously defined in System Center 2012 R2 VMM (see Figure 2-16). VM Templates are used to specify a template configuration for a single VM being deployed to a private cloud, whereas Service Templates can include a template configuration for more complex multi-tier applications that can involve multiple virtual machines, applications, virtual networks, and load balancers as part of a single template.

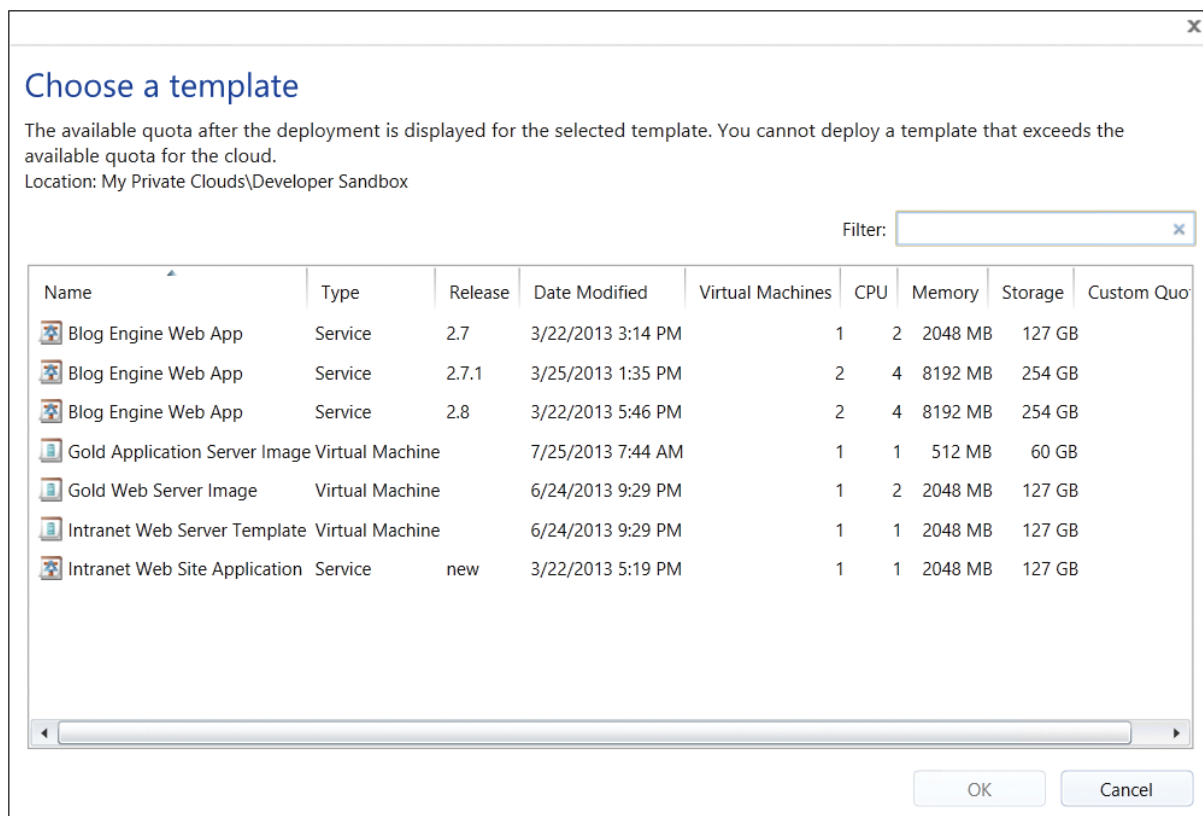


FIGURE 2-16 You can select a template from the Choose A Template dialog box.

4. After selecting the desired template for deploying a new workload, click OK. This will return to the prior New Deployment dialog box where you'll be presented with options to configure the settings for this new deployment, as shown in Figure 2-17.

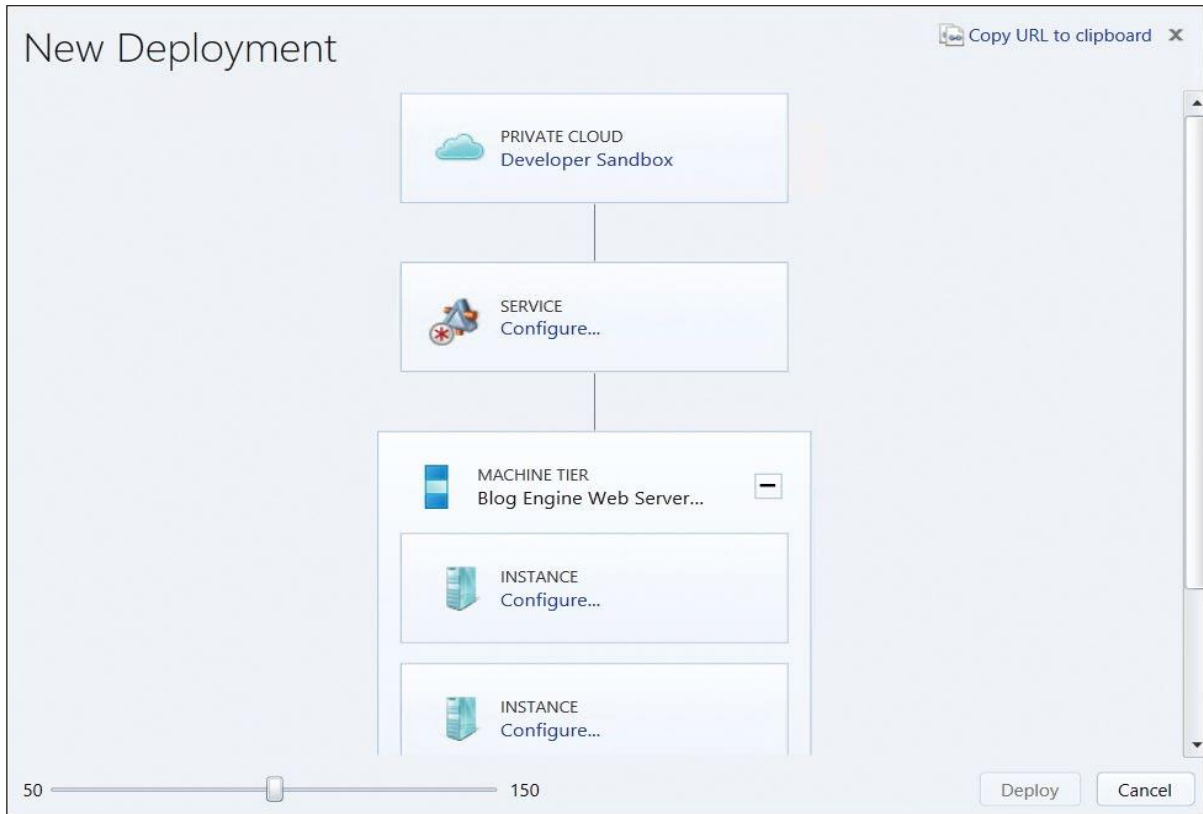


FIGURE 2-17 Use the Configure Settings from the New Deployment dialog box to configure the deployment.

5. On the New Deployment dialog box, click Configure in the SERVICE box to configure the general configuration properties for this new application workload. This will display the Properties page for the new service, or application workload, being deployed to the selected private cloud (see Figure 2-18).

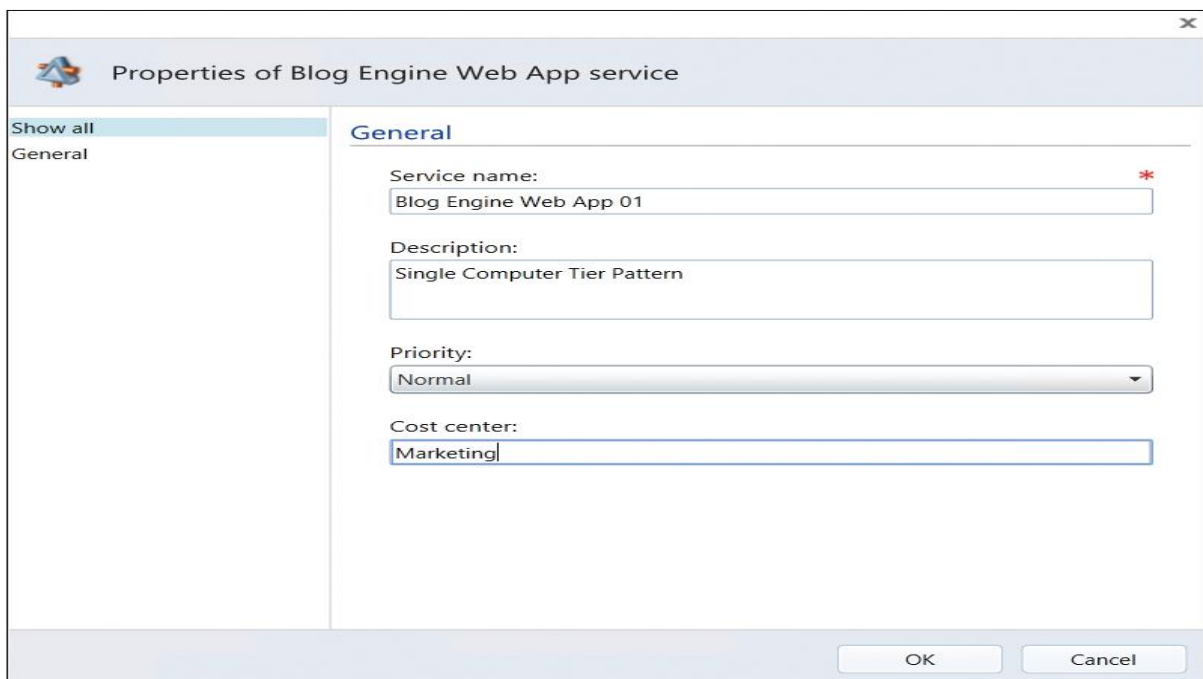


FIGURE 2-18 Configure the properties of the new service.

6. In the Properties page, enter a Service name for the new service being deployed, and optionally assign a Description, Priority, and Cost Center. Click OK to save this configuration information for the Service and return to the New Deployment dialog box, as displayed in Figure 2-19.

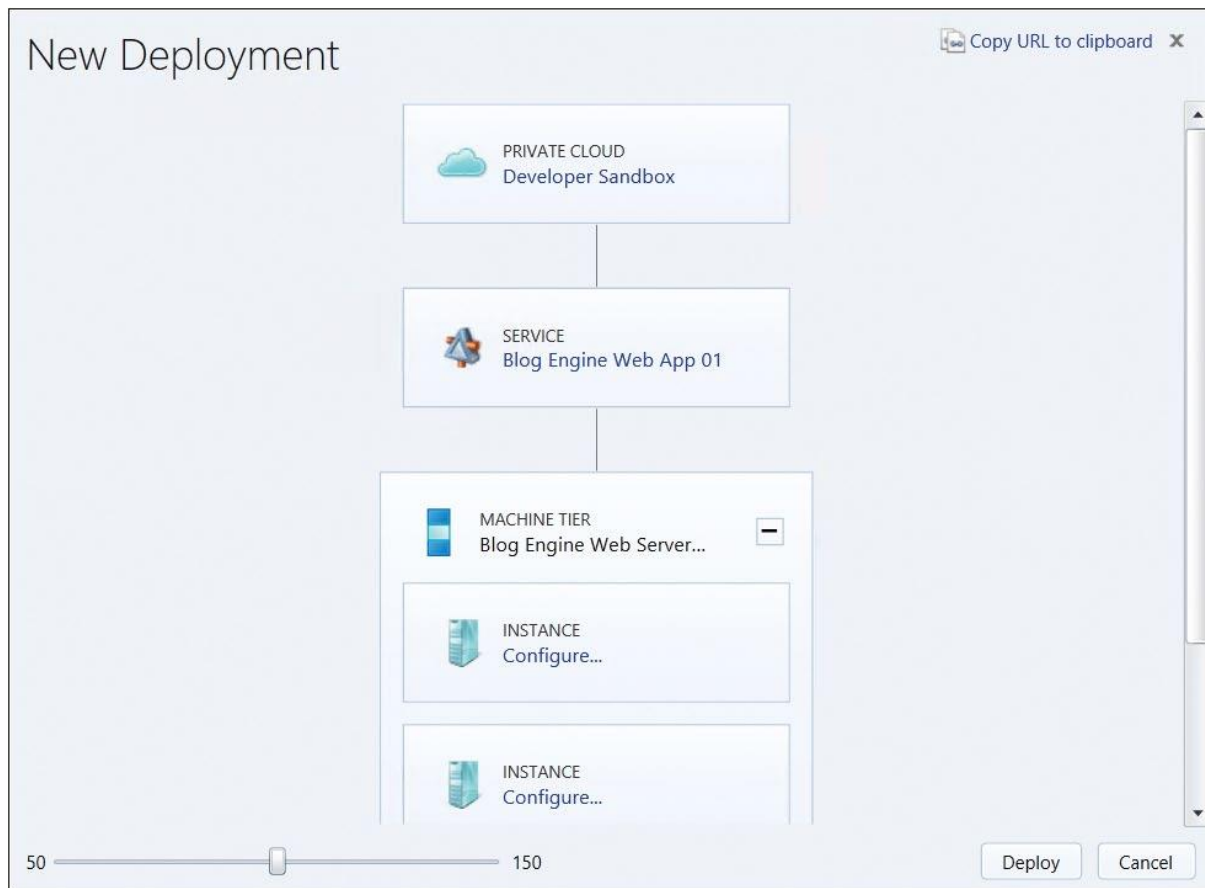


FIGURE 2-19 A summary of the new deployment showing the configured service.

7. Similarly, to configure each VM in each Machine Tier of the service being deployed, click each Configure in the INSTANCE box in the New Deployment dialog box to enter virtual machine configuration settings, if required by the template being used for deployment (see Figure 2-20).

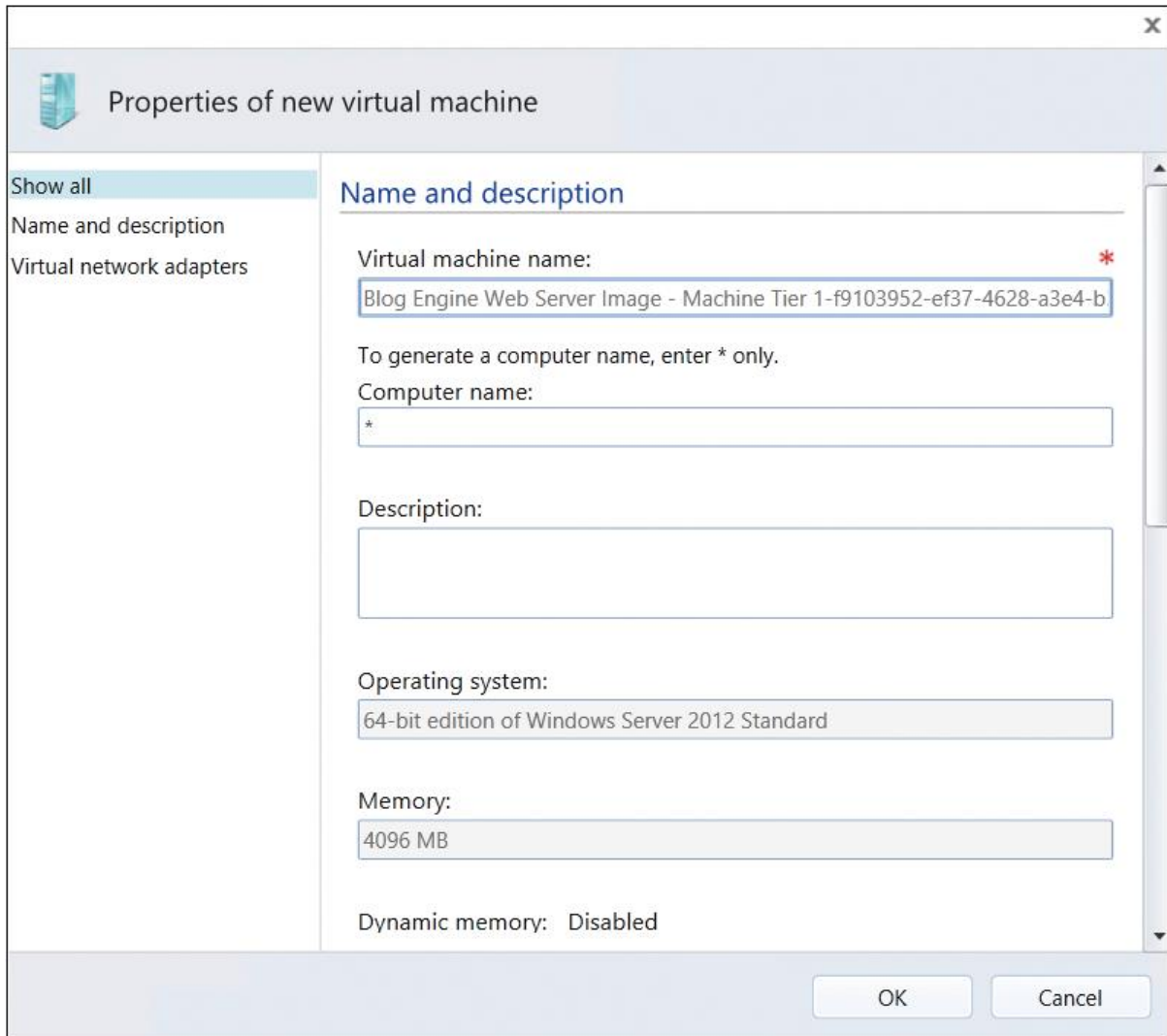


FIGURE 2-20 You can set the name and description in the Properties Of New Virtual Machine page.

8. For the Service Template that is being used in this example, all VM properties have been completed automatically by the template, so there's no additional configuration information needed. Click OK to return to the prior New Deployment page.

9. To deploy the new application workload to the selected private cloud, click Deploy.

Depending on the complexity of the Service Template or VM Template being deployed to a private cloud, the deployment process can require several minutes to complete. While the deployment is being processed, the Jobs page on the App Controller portal can be used to confirm the status of in-progress jobs. When all jobs associated with the new deployment are displayed with a Completed status, the new application workload will have been successfully deployed, as shown in Figure 2-21.

After the successful deployment of the application workload to the selected private cloud, the Services and Virtual Machines pages in the App Controller portal can be used to confirm workload status and manage the deployed workloads, as shown in Figure 2-22 and Figure 2-23.

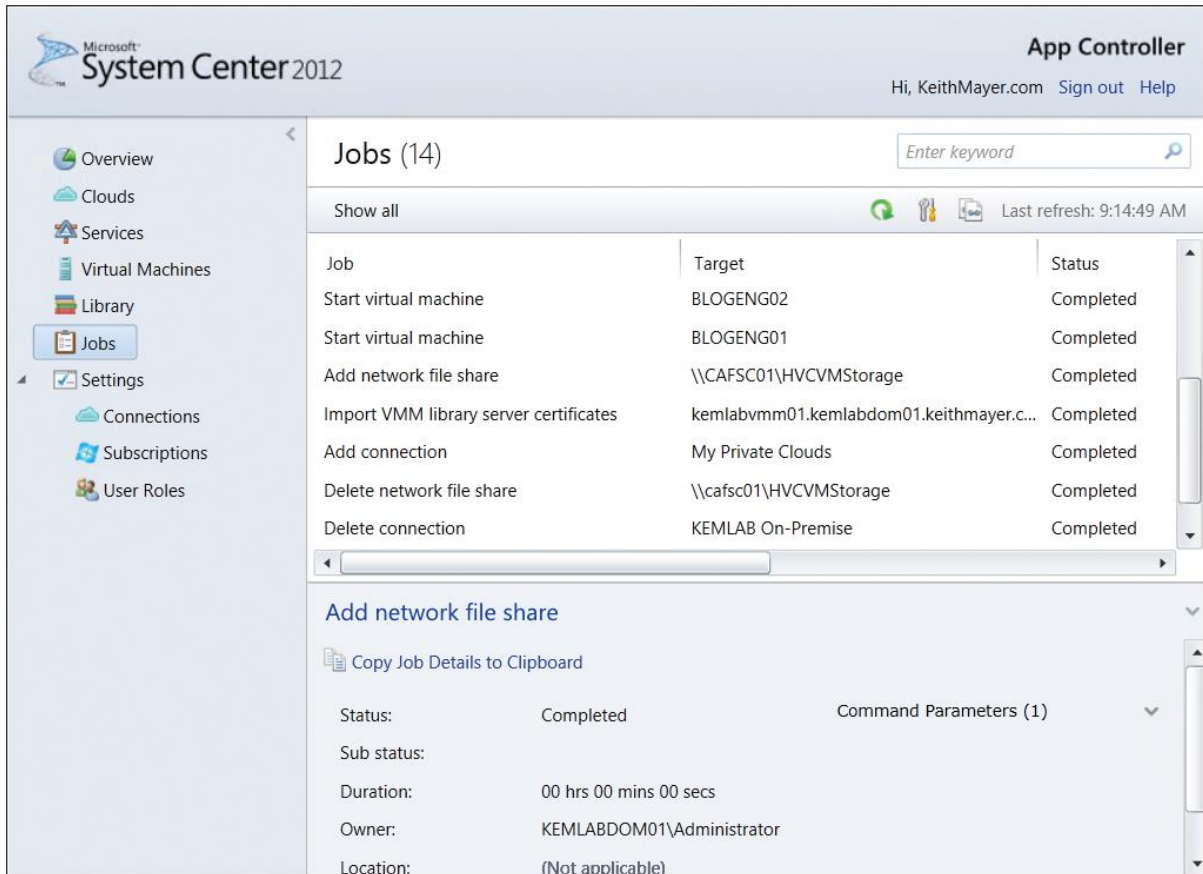


FIGURE 2-21 The App Controller Portal allows you to view the Jobs page.

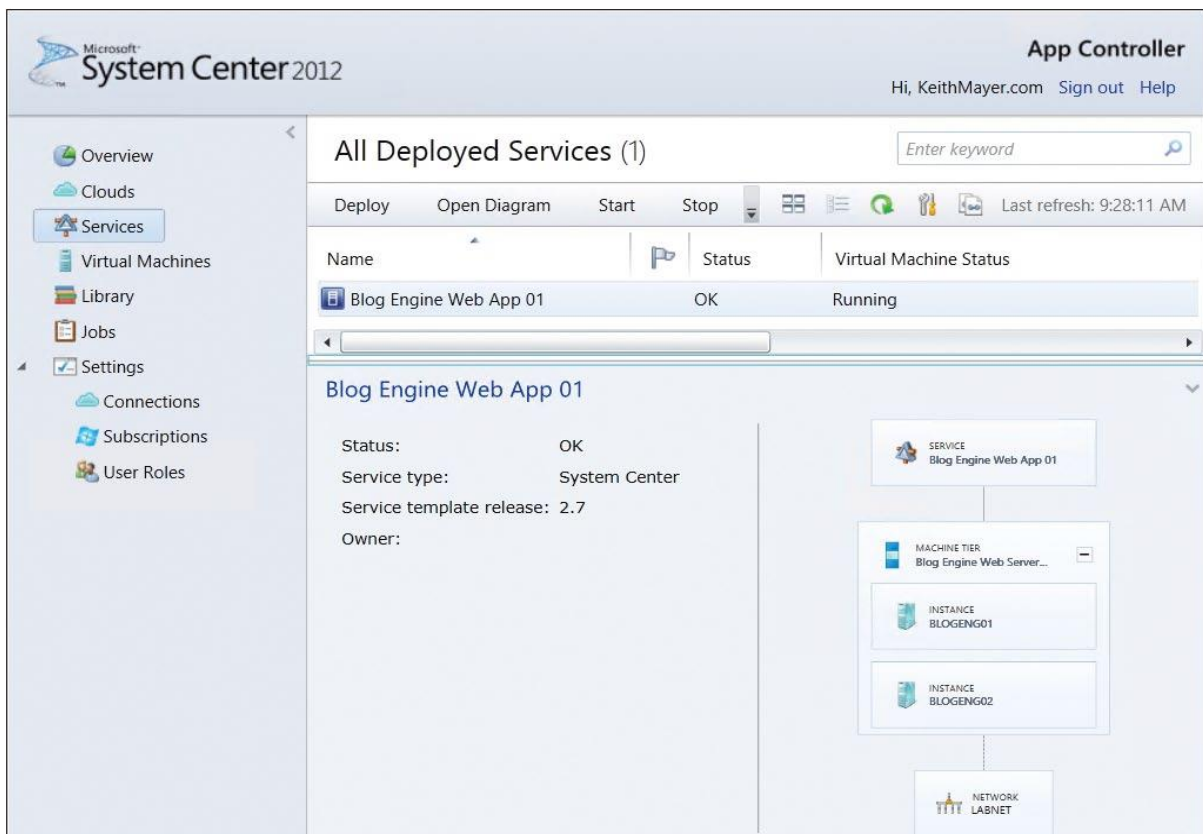


FIGURE 2-22 You can view all Deployed Services in a private cloud.

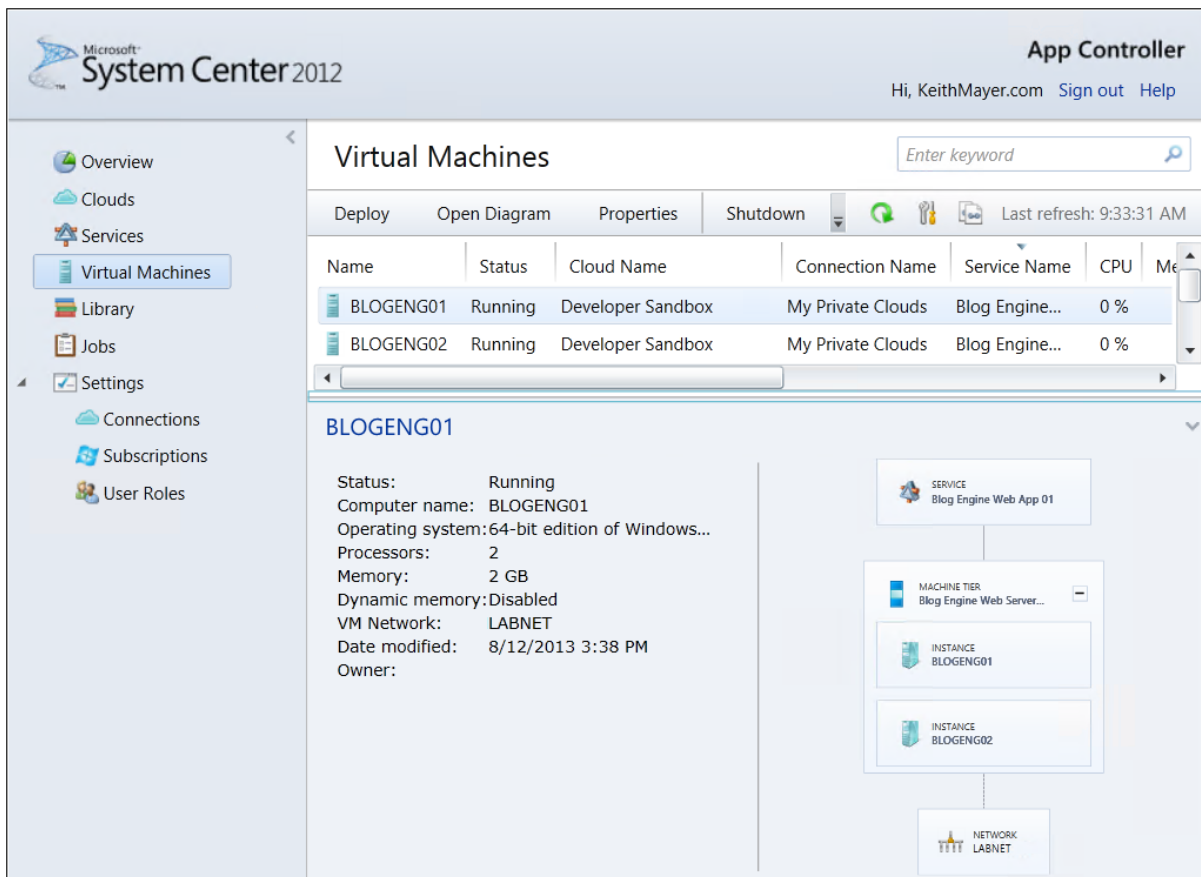


FIGURE 2-23 You can view the deployed Virtual Machine instances in a private cloud.

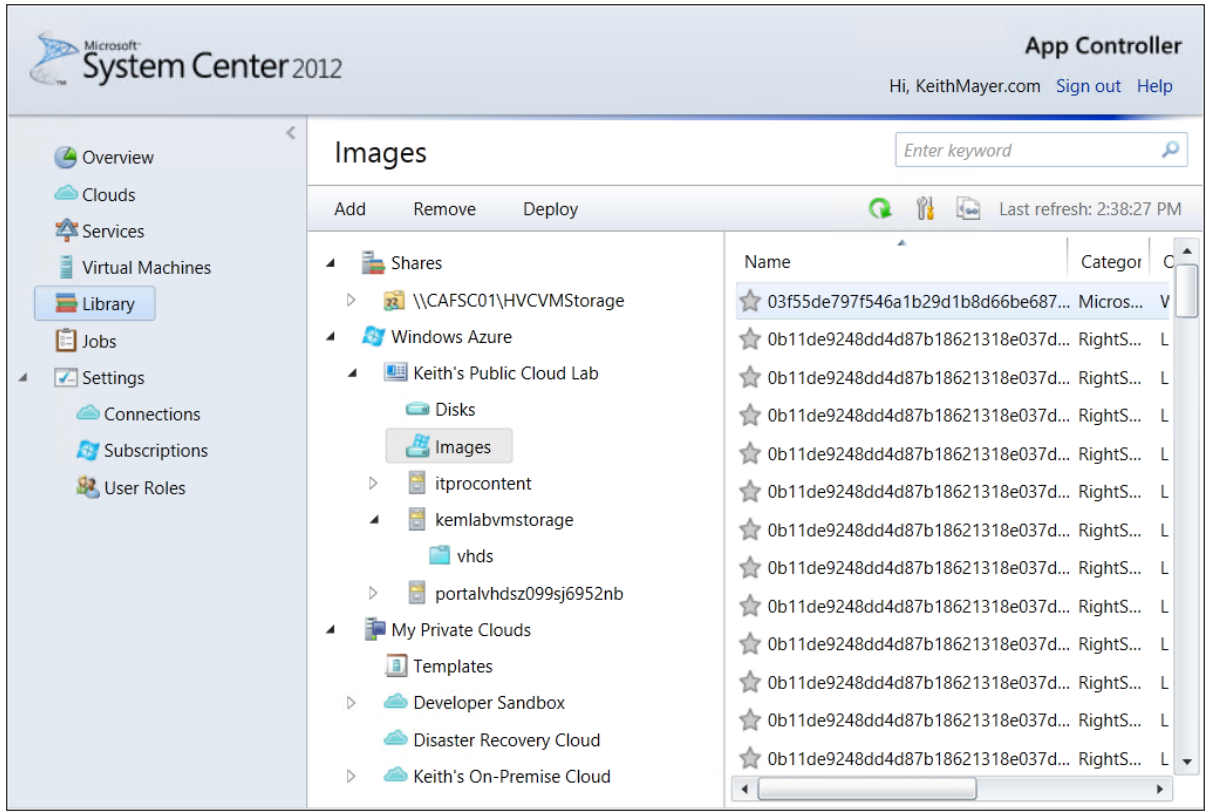
b) Adding Virtual Hard Disks and integrating it with VMs.

To upload a virtual hard disk or image to Windows Azure

1. On the **Library** page, expand the **Windows Azure** node.
2. Expand the Windows Azure subscription to the Windows Azure storage account in which the destination container is located.
3. Do one of the following:
 - To upload a virtual hard disk, select the **Disks** folder and click **Add** in the taskbar.
 - To upload an image, right-click the **Images** folder and click **Add** in the taskbar.
4. Specify the file share, VMMLibrary, or Windows Azure storage container from which you want to retrieve the source disk or image.
5. Do one of the following:
 - For a virtual hard disk, specify the operating system that is installed on the disk. If no operating system installed, select **None**.

- For a disk image, specify the operating system that is installed on the image.

6. Click **OK**.



You can manage disks and images from the Library page.

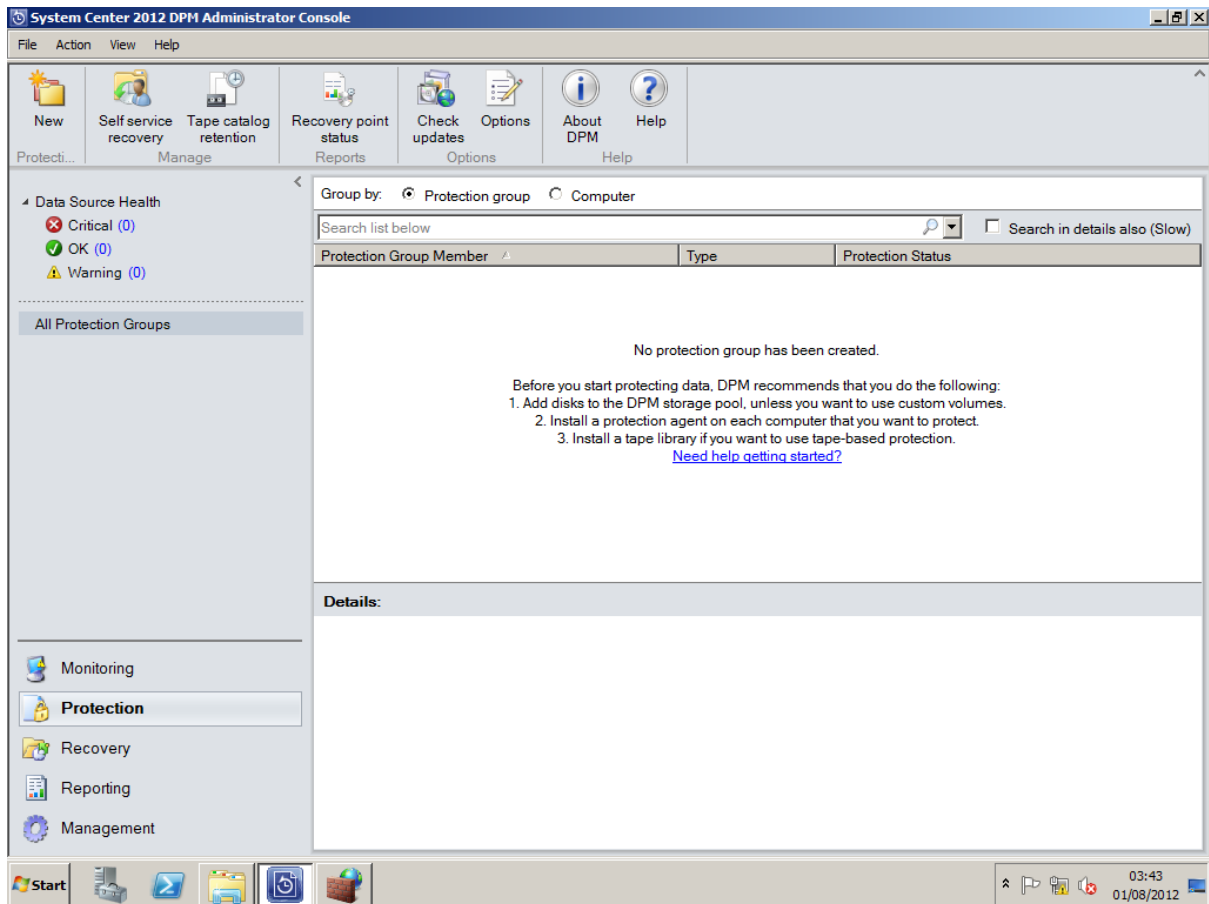
Sign: _____

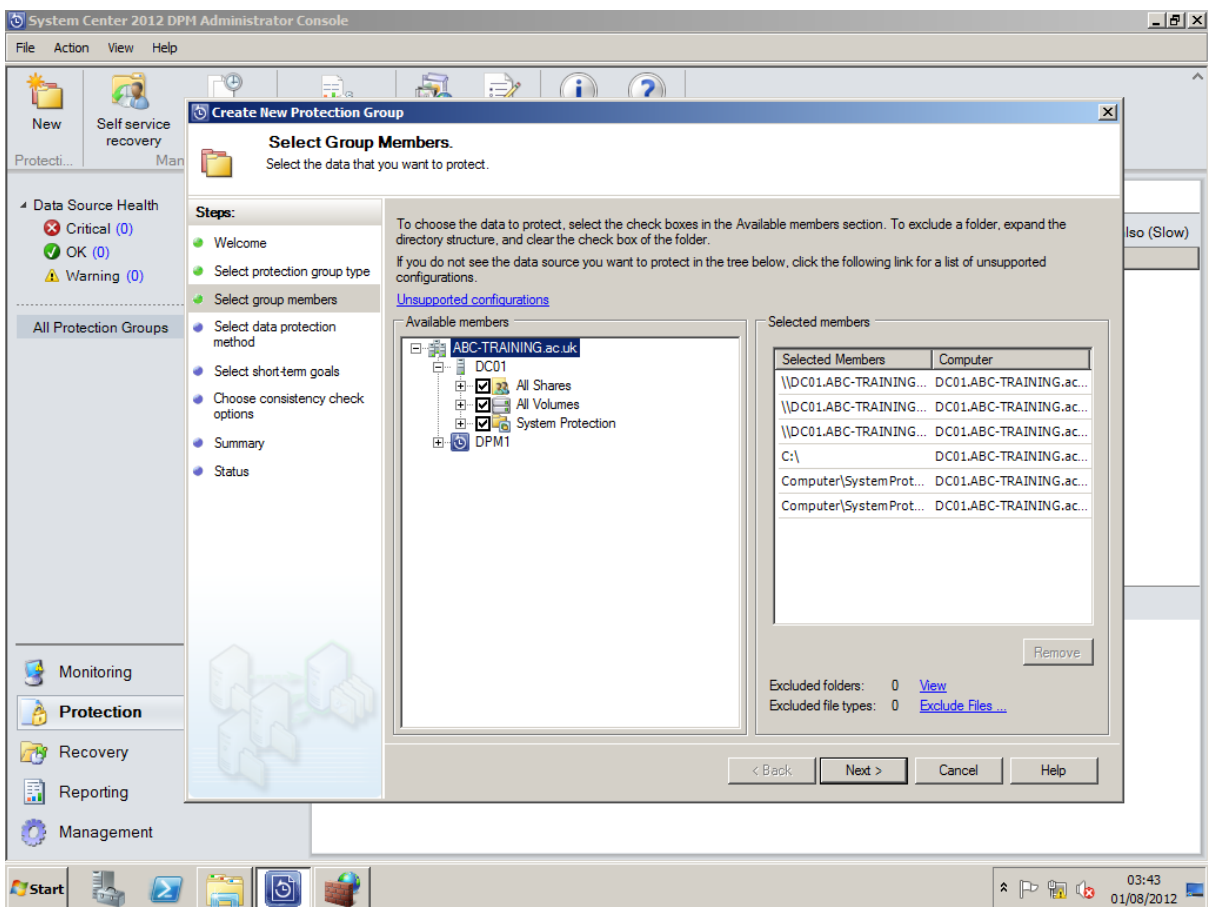
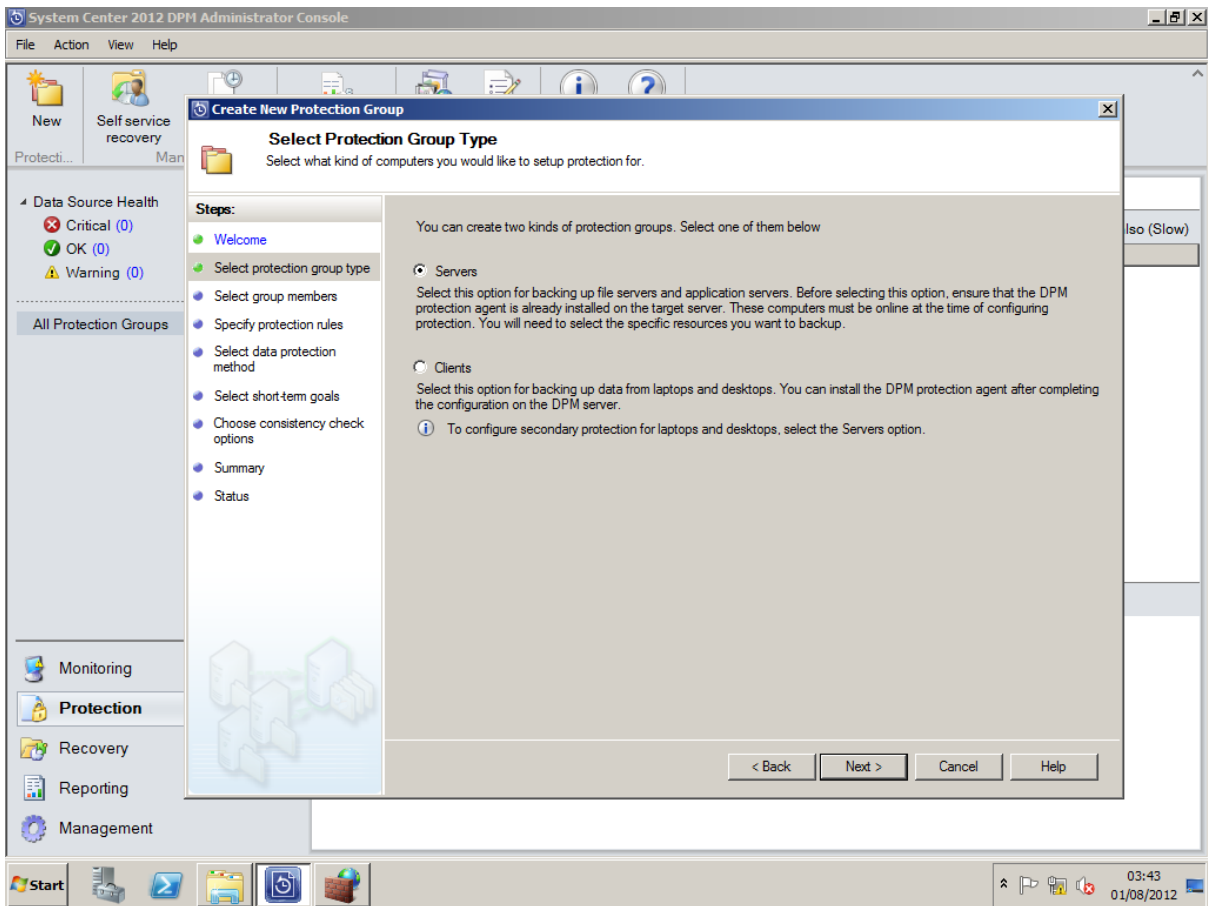
Practical No 4: Using Data Protection Manager for Backup and Recovery.

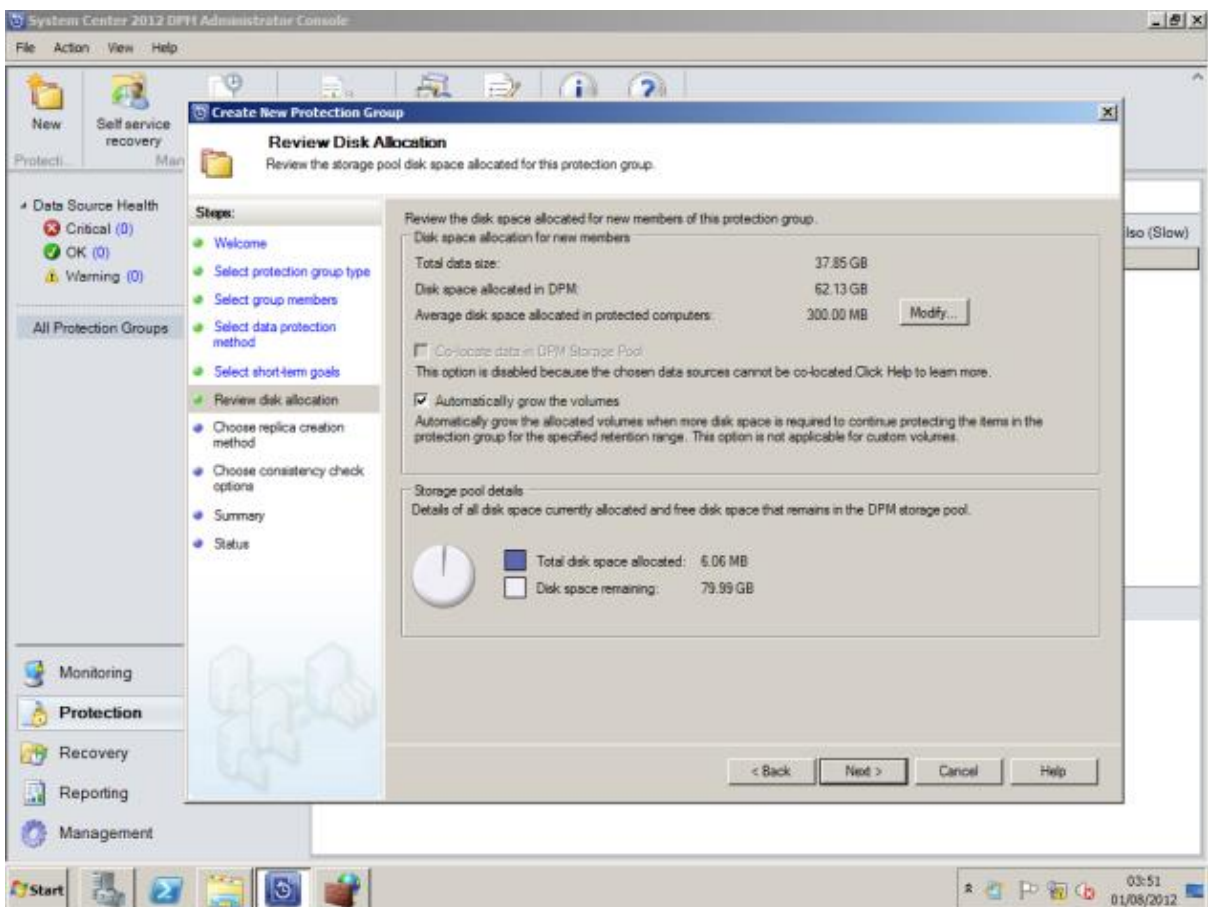
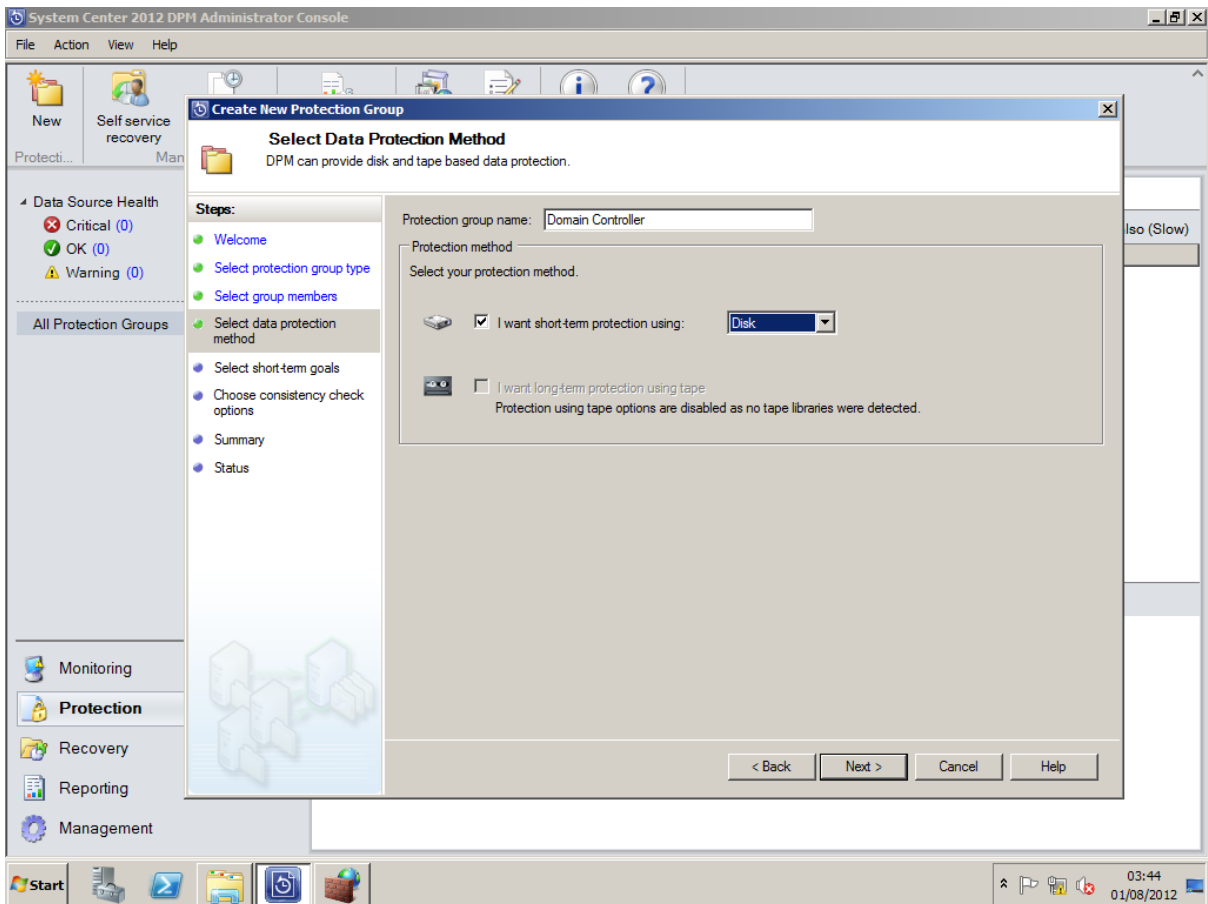
a) Creating a new protection group from the Protection workspace.

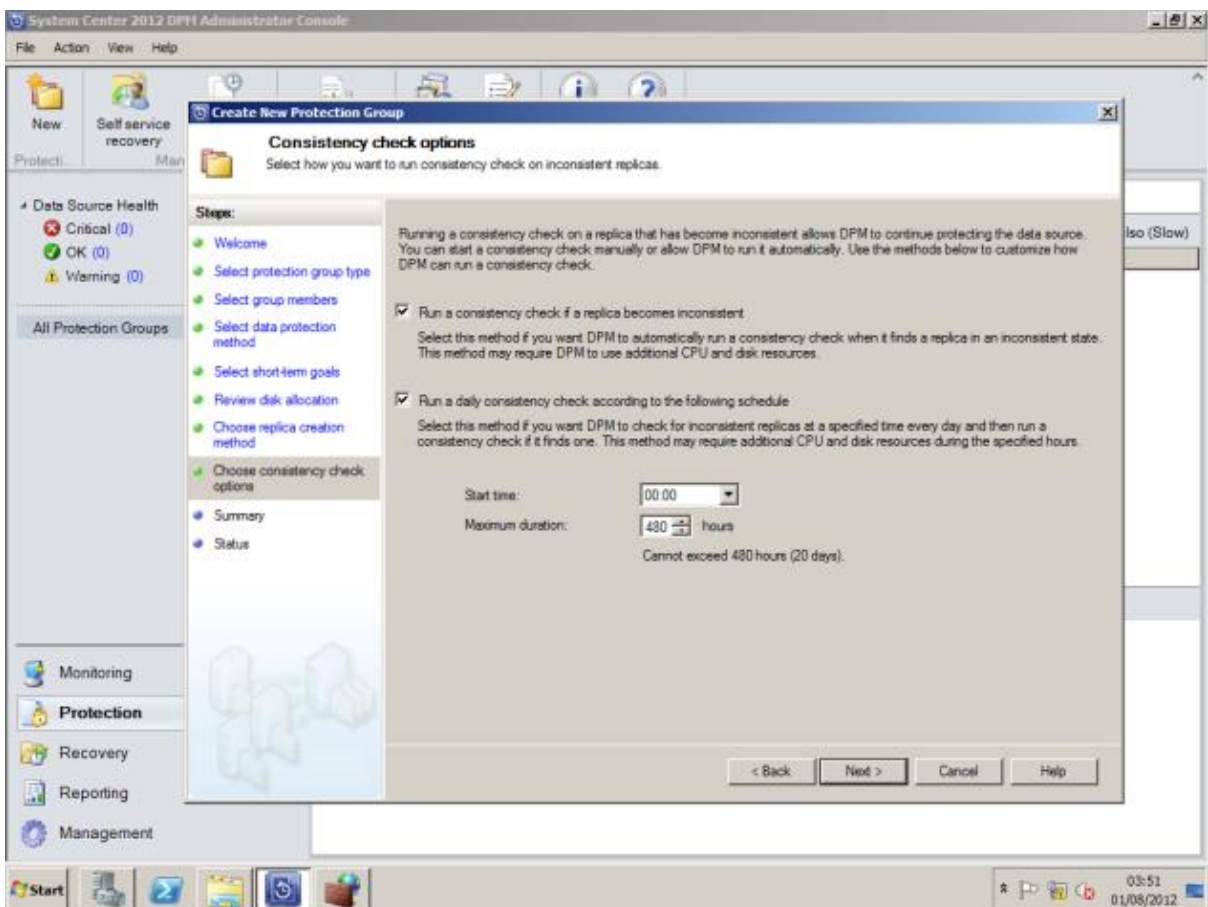
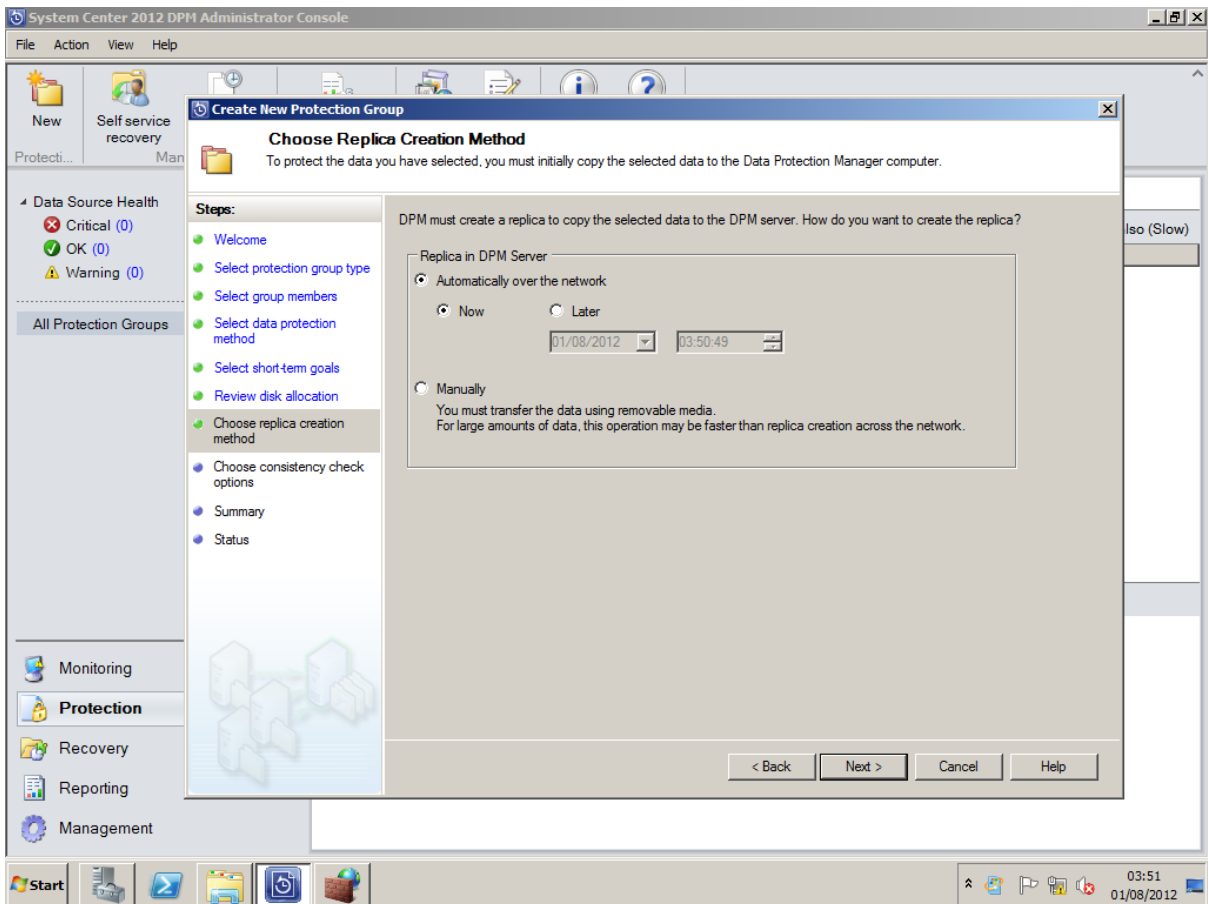
Create Protection Groups

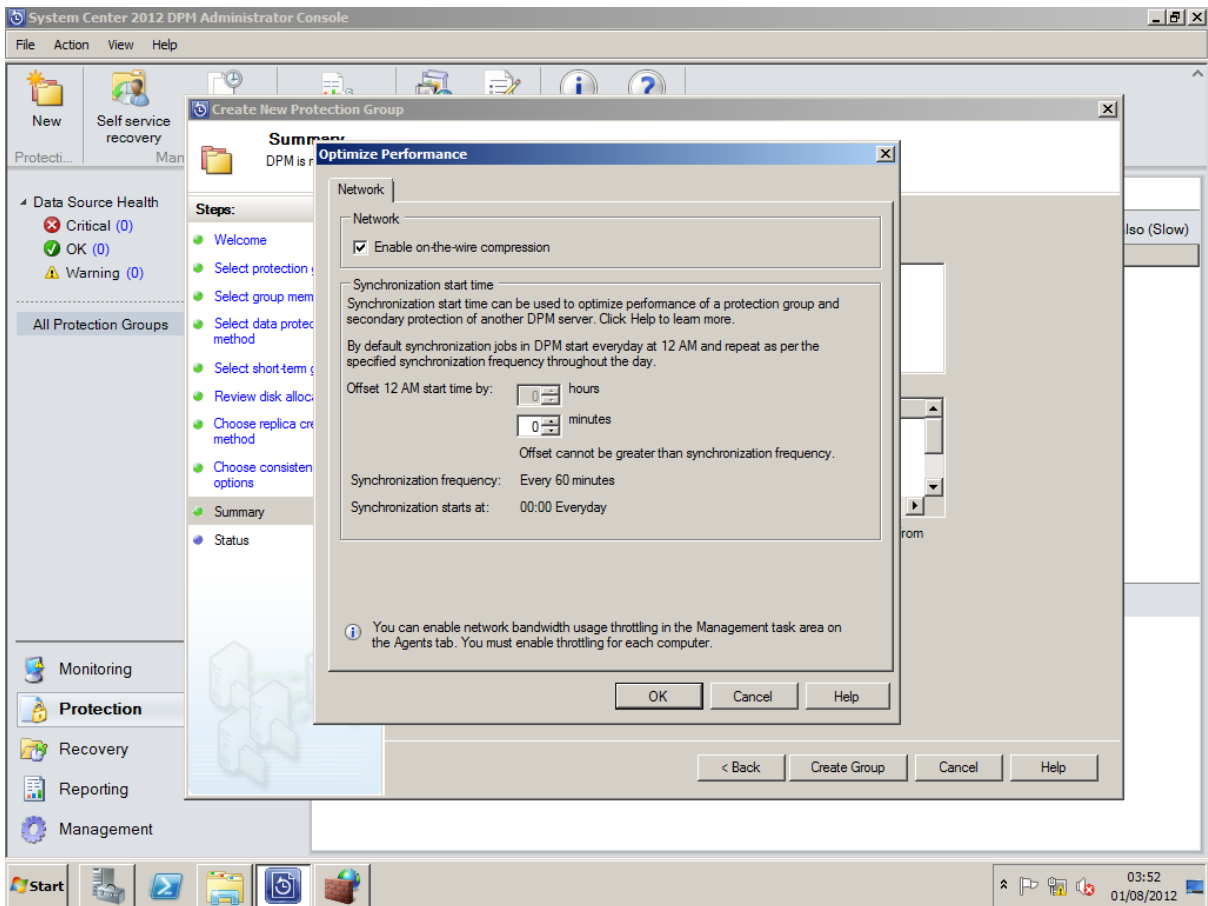
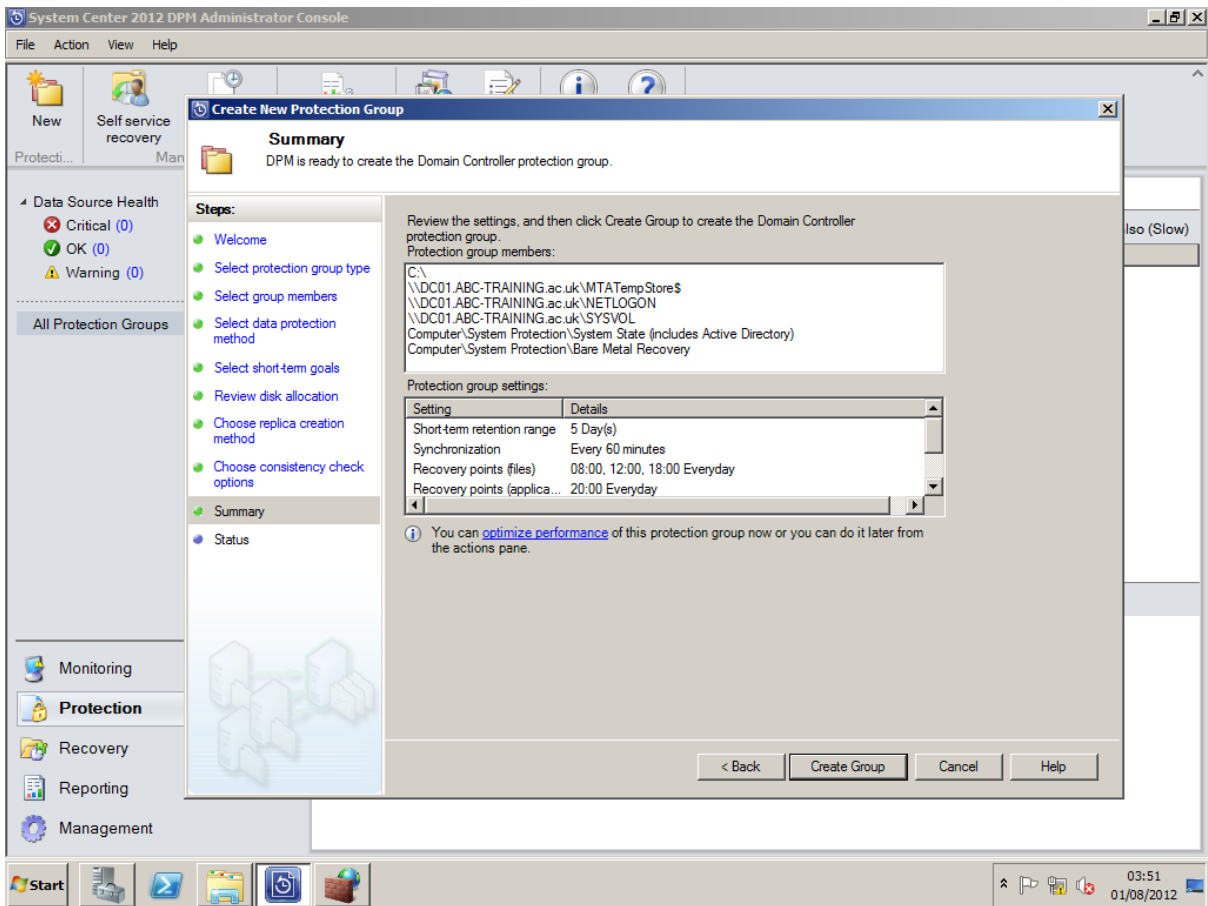
Protection Groups are groups of servers that are configured to backup at certain times. This allows you to segregate server types and backup systems in various groups.

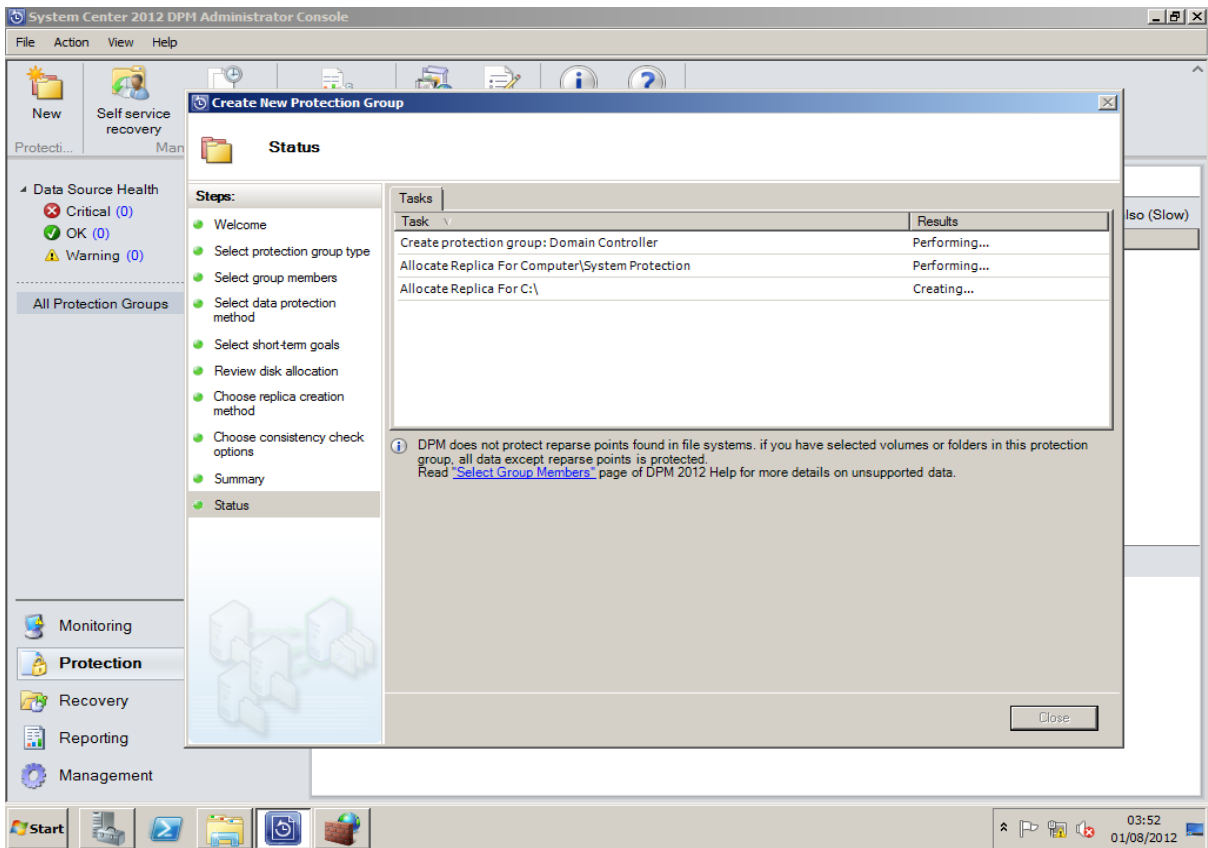




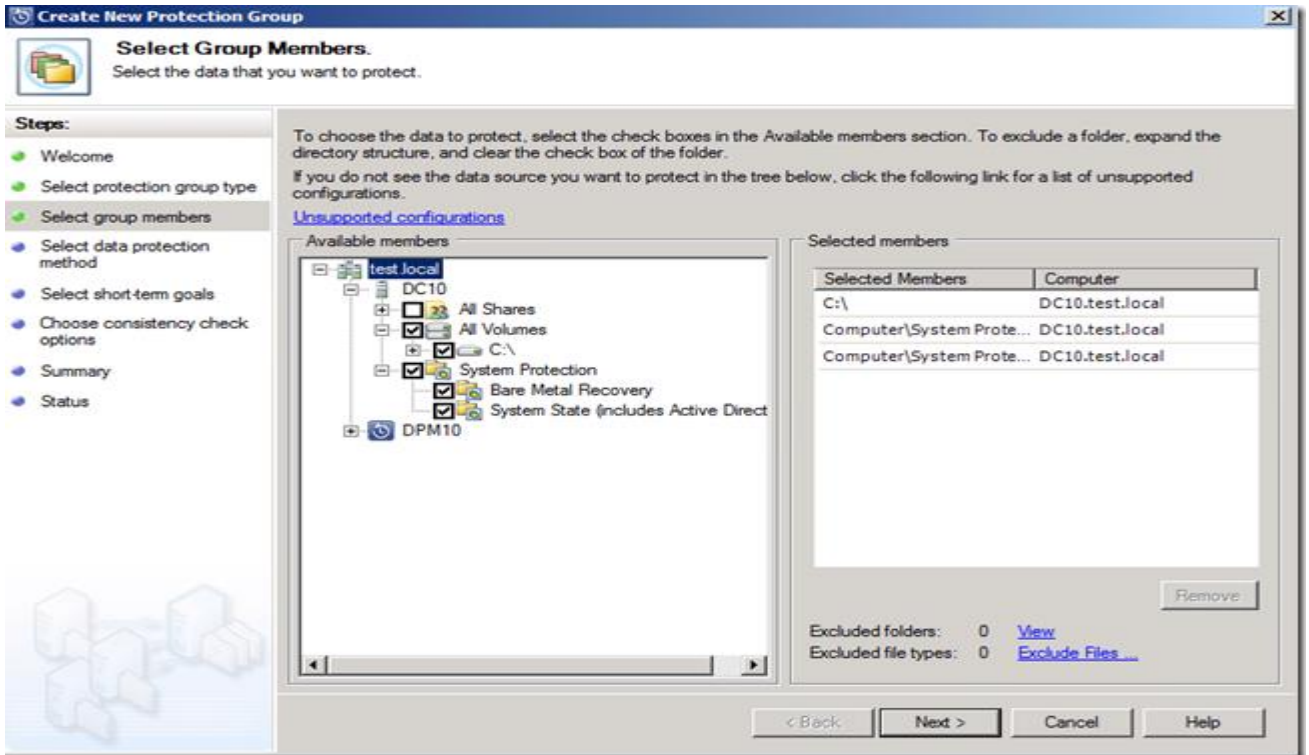




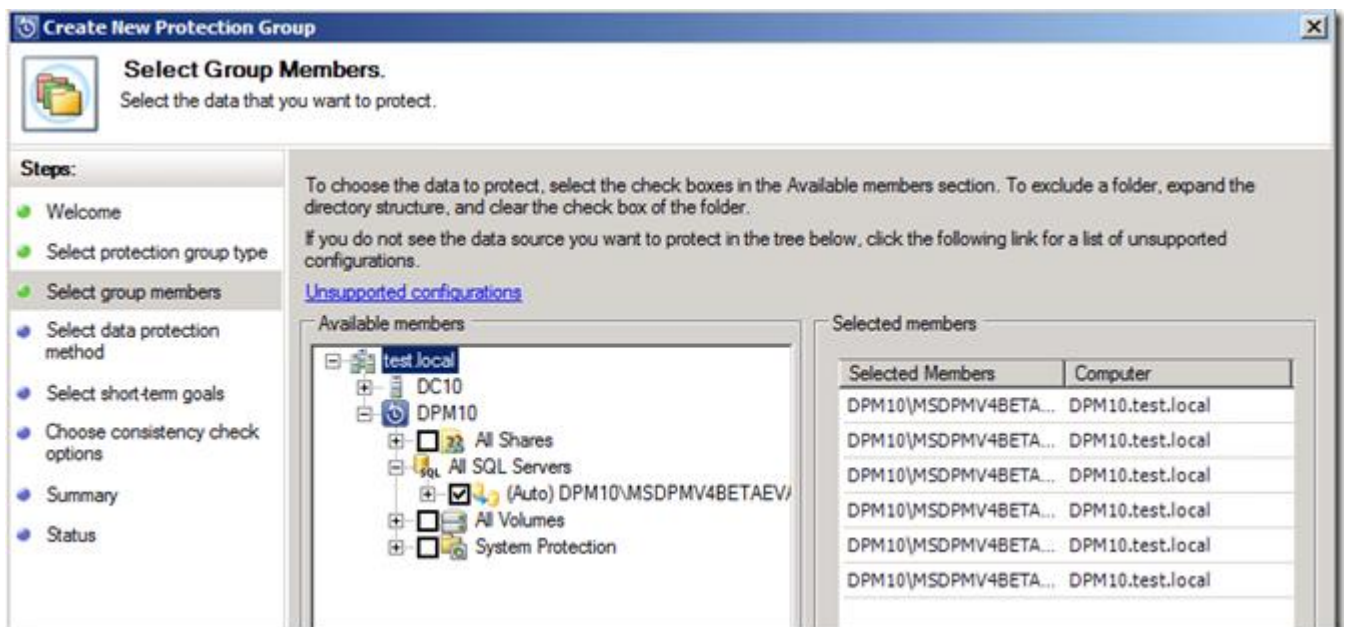




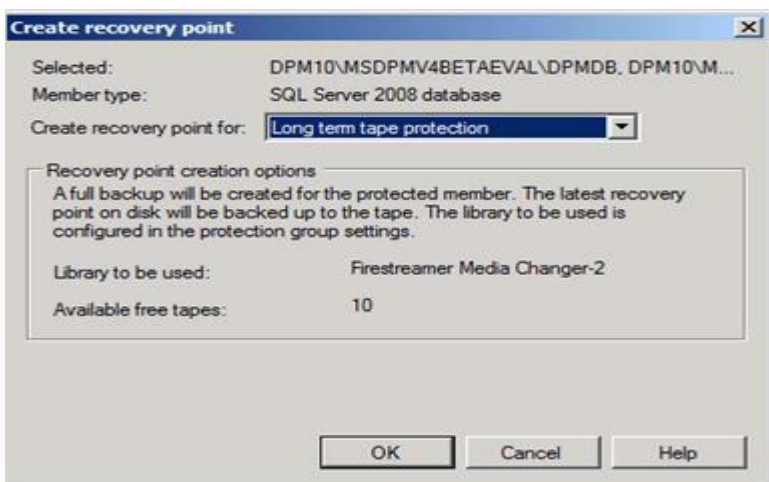
b) Performing a recovery from the Recovery workspace.



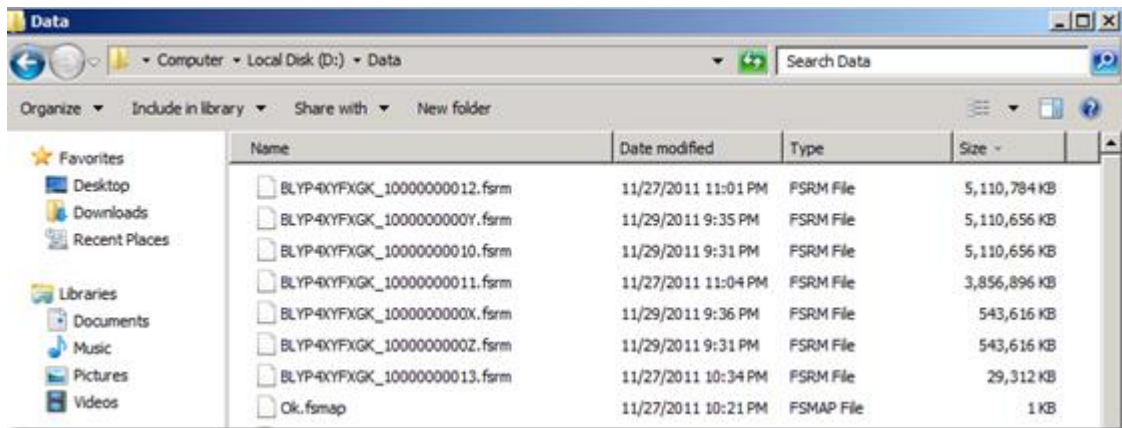
On the test.local domain we need a complete backup of the Domain Controller



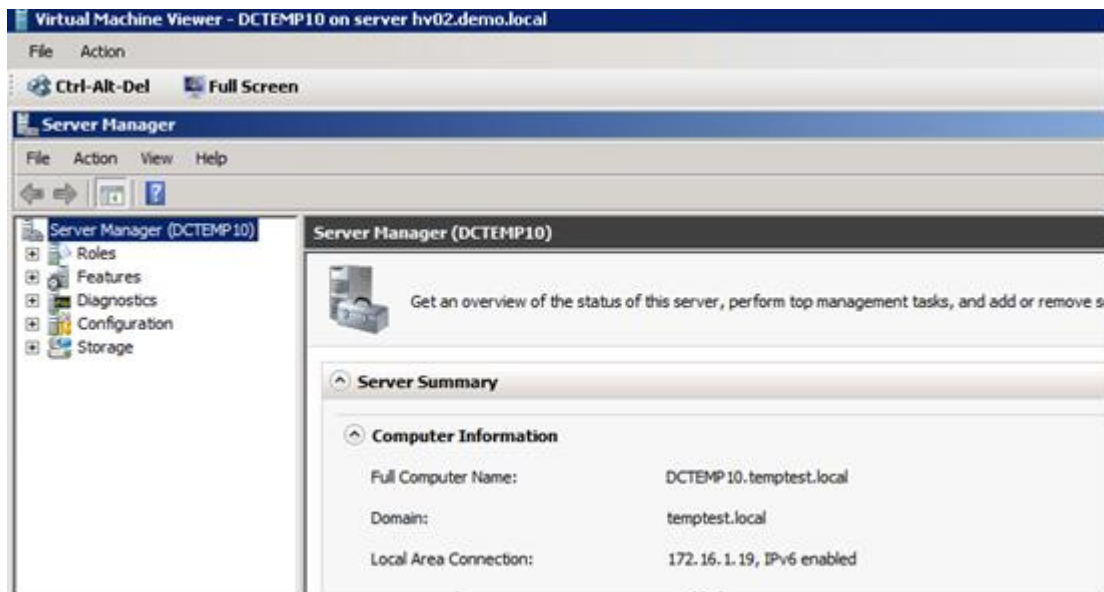
And we will need the configuration database for Data Protection Manager



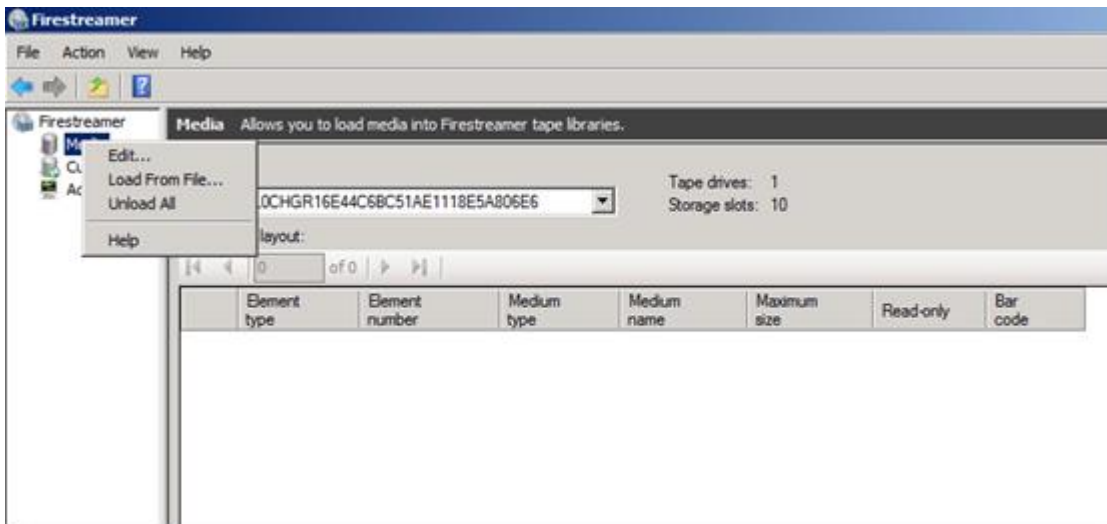
After creating the Protection Groups create a manual recovery point to tape , both for the domain controller and the Data Protection Manager configuration database



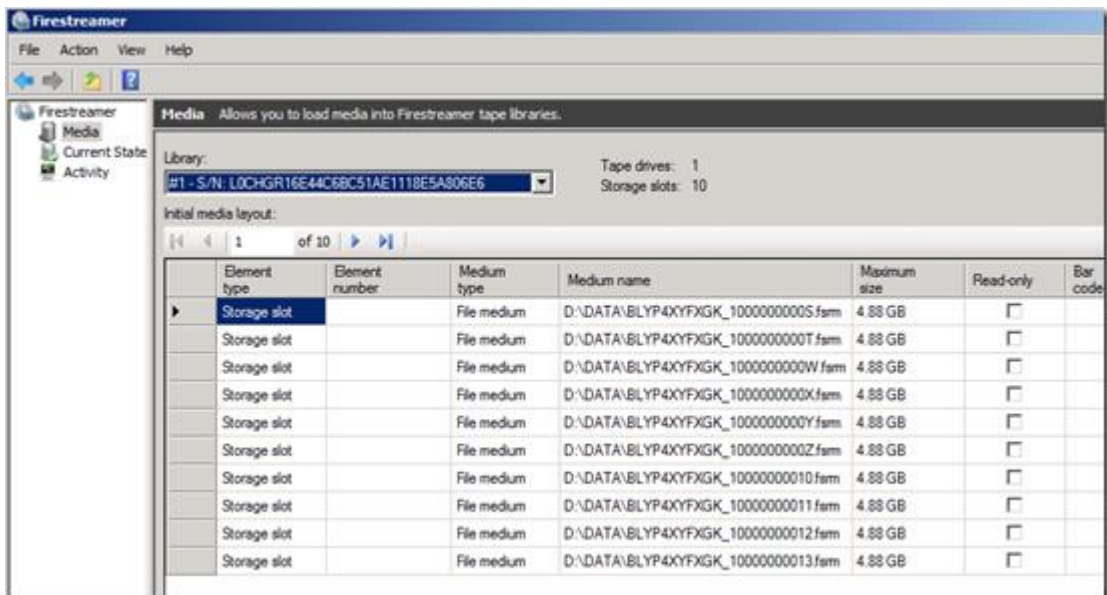
For testing I am using Cristalink brilliant Virtual Tape Library for Data Protection Manager <http://www.cristalink.com/fs/> , so here the backup is located on 3 virtual tapes.



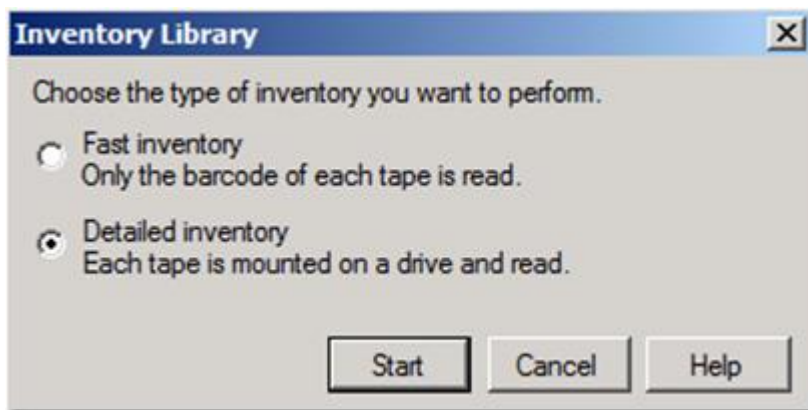
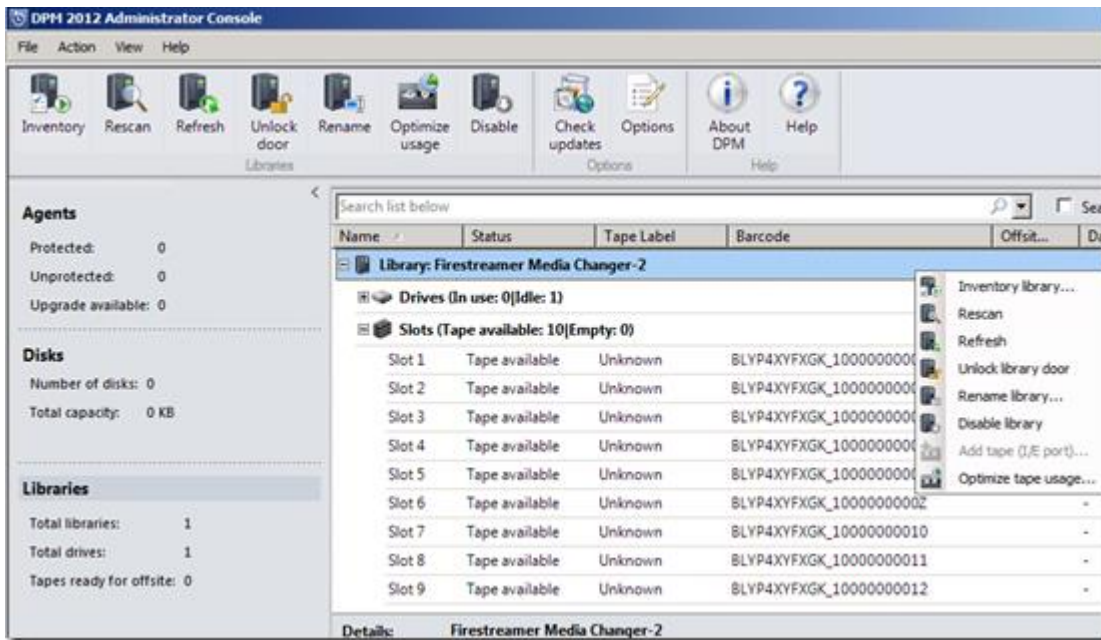
We need a new domain to restore to until we can get the original production environment up and running so here we created a new domain and is adding a Data Protection Manager Server to the same domain.



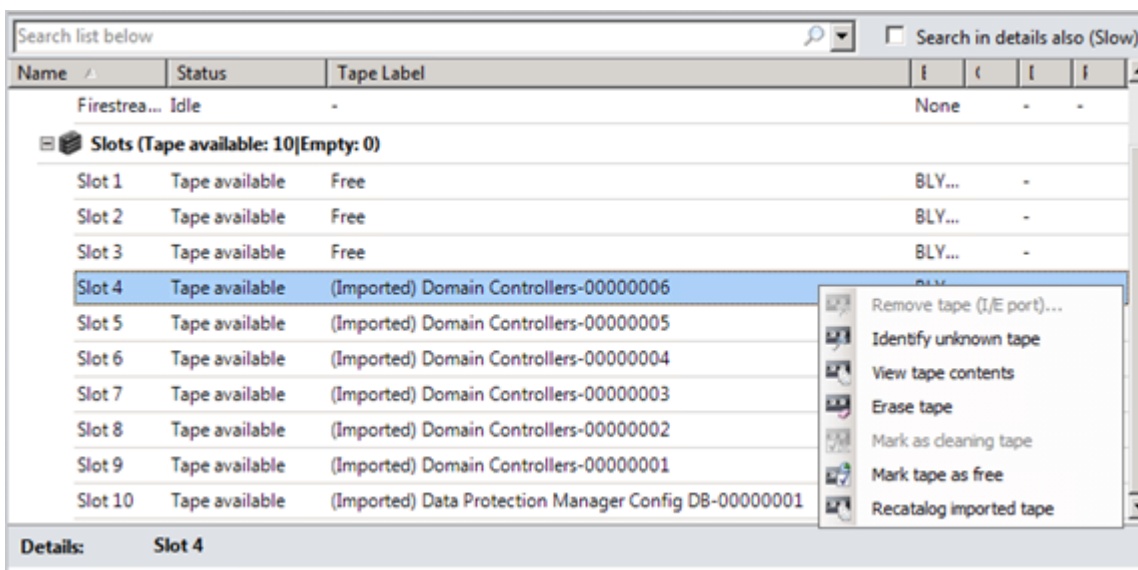
To simulate adding tapes from the library we use FileStreams Import feature Load From File



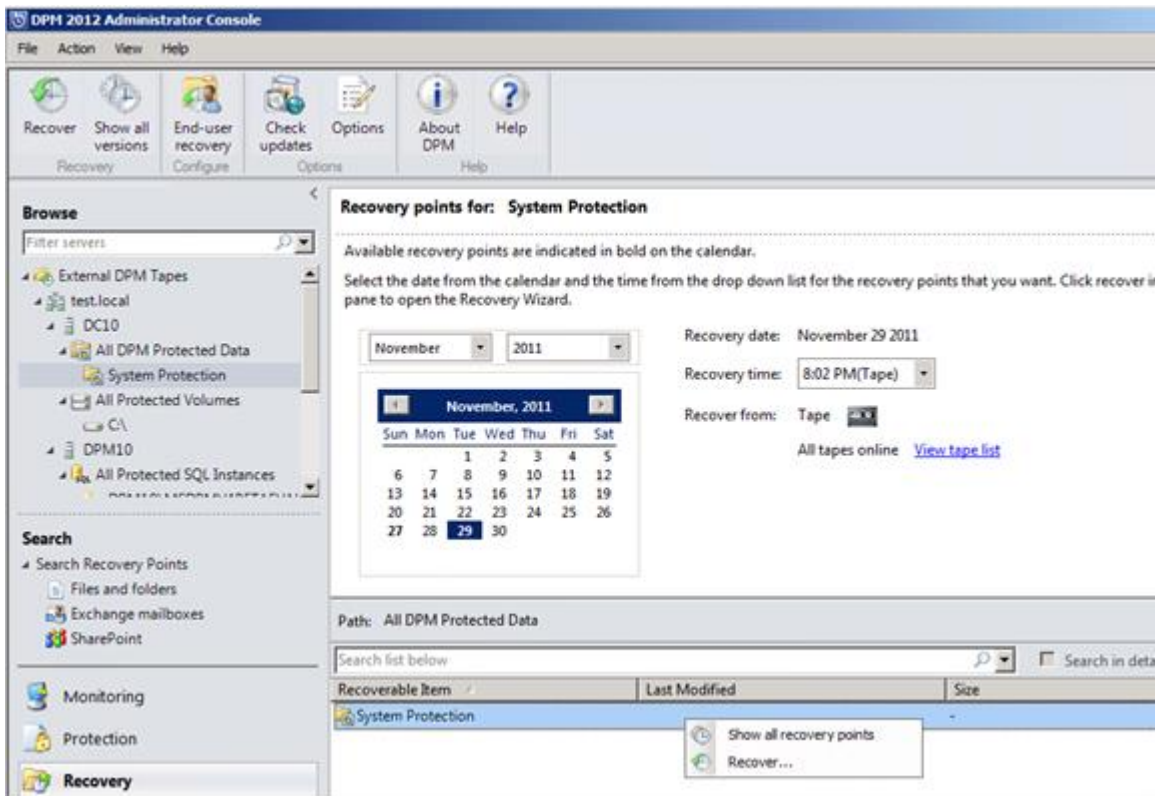
And then we can see the same tapes as we had before the wipe of the Domain Controller and Data Protection Manager Server



We then need to start a detailed inventory so we can see what's on the tapes



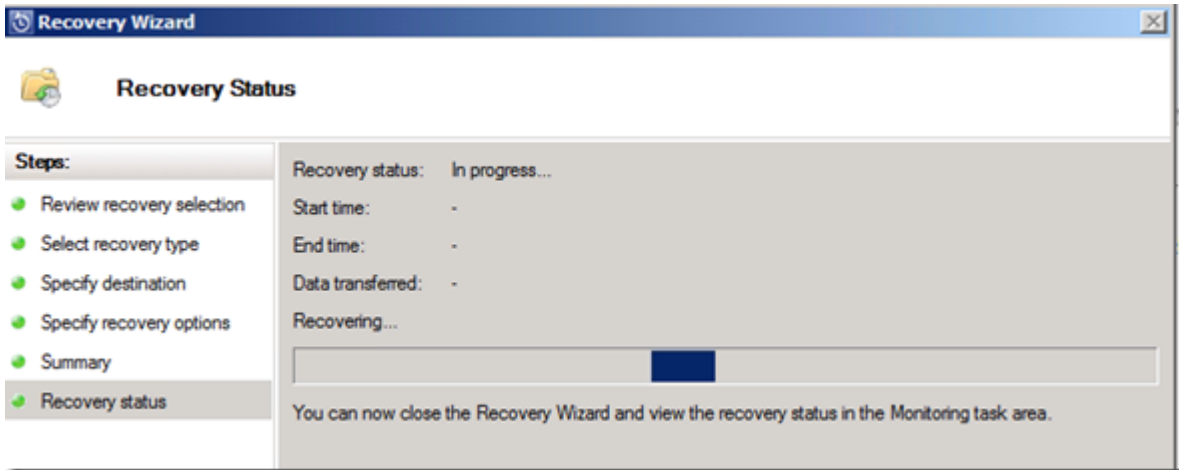
After the detailed inventory have completed we need to Recatalog Imported Tape to add the content of the tapes to the Data Protection Managers configuration database



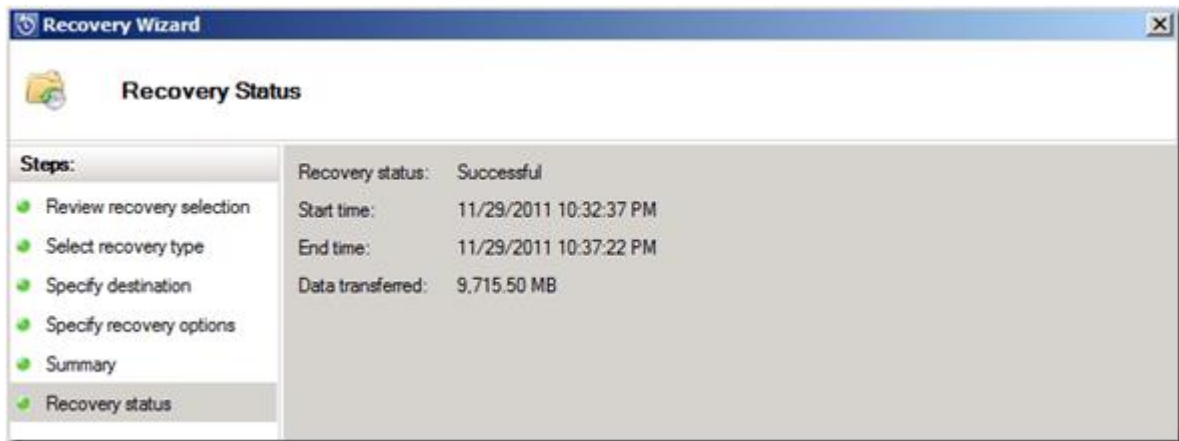
We then need to recover the System Protection from the tapes we did a recatalog on



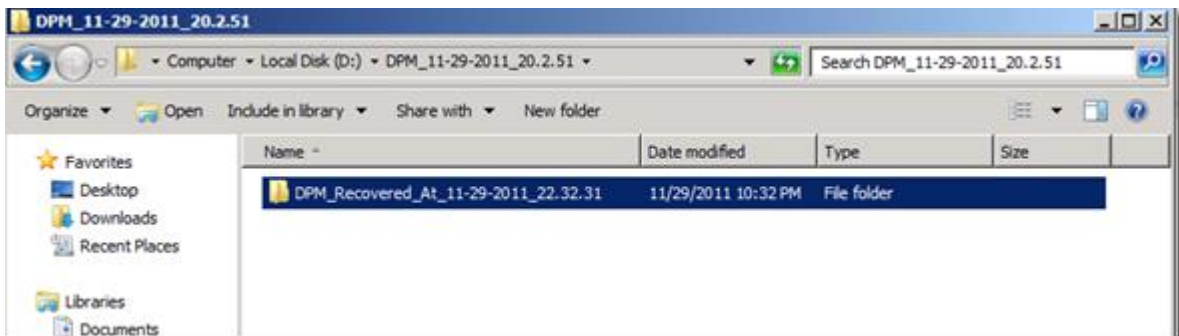
Only restore option for systemprotection is a network folder



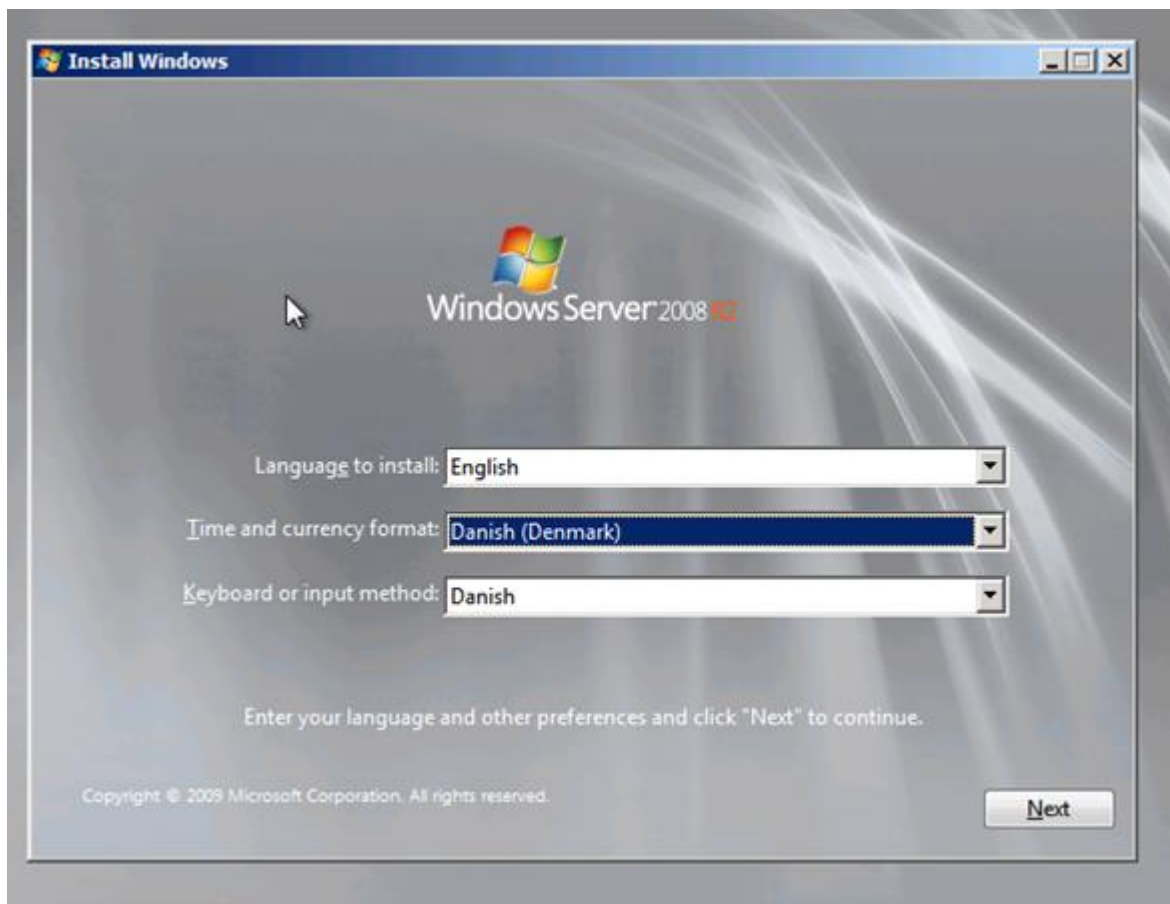
And its time to start the restore



Data Protection Manager == Success



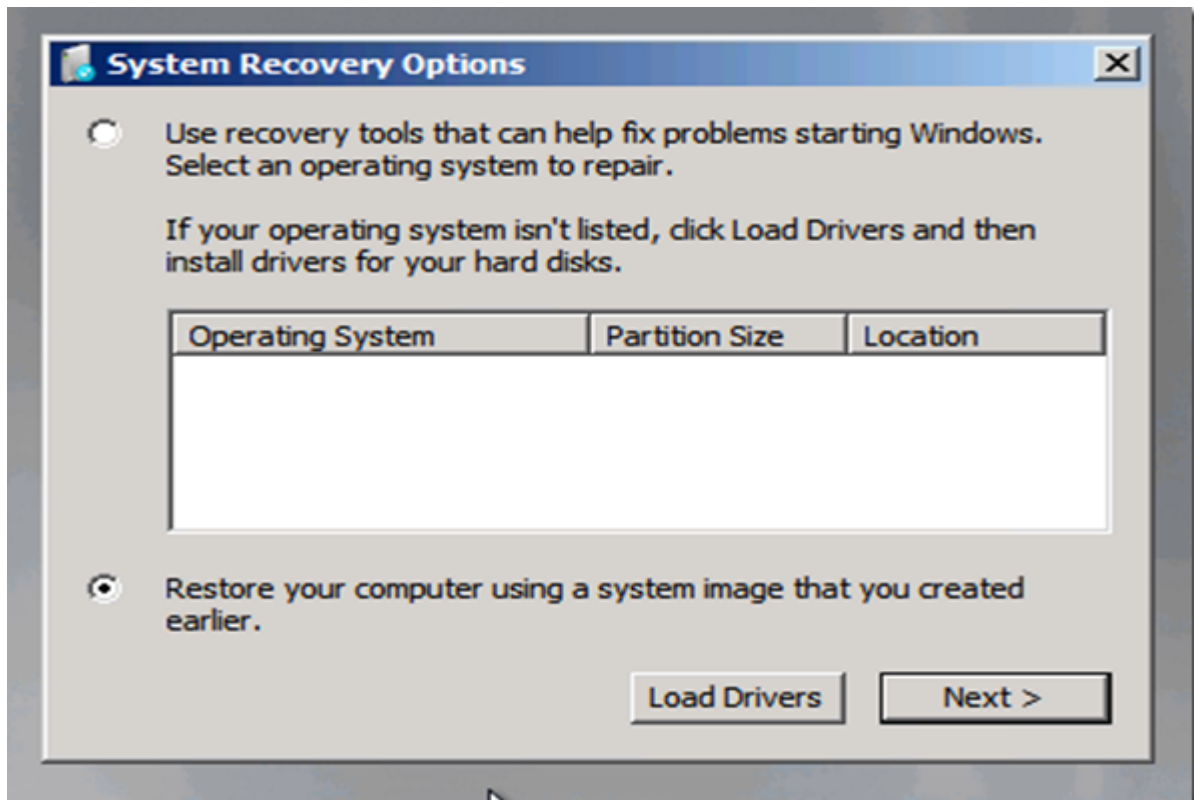
We then need to share the folder out so we can access it from the Windows 2008 R2 installation media



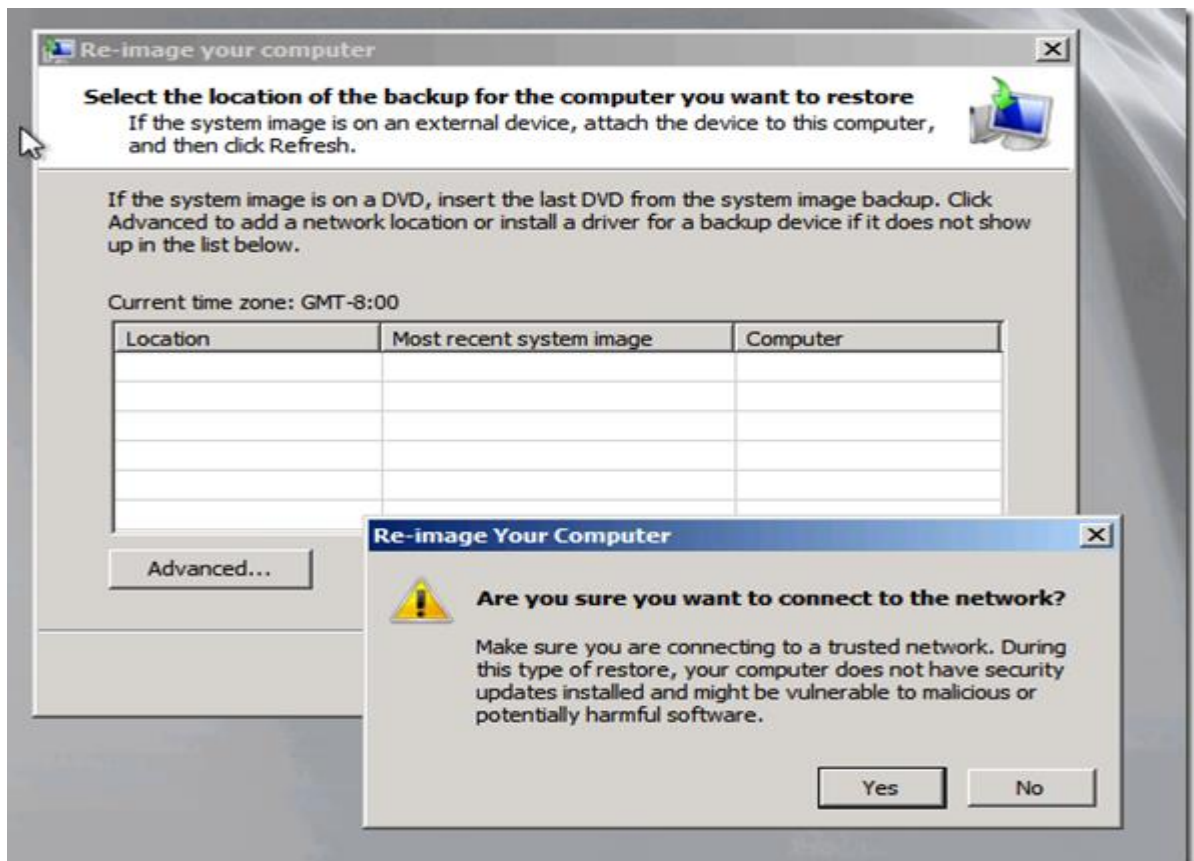
to Restore from the recovered data we need to start the Windows 2008 R2 installer , DHCP needs to be enabled for networking support



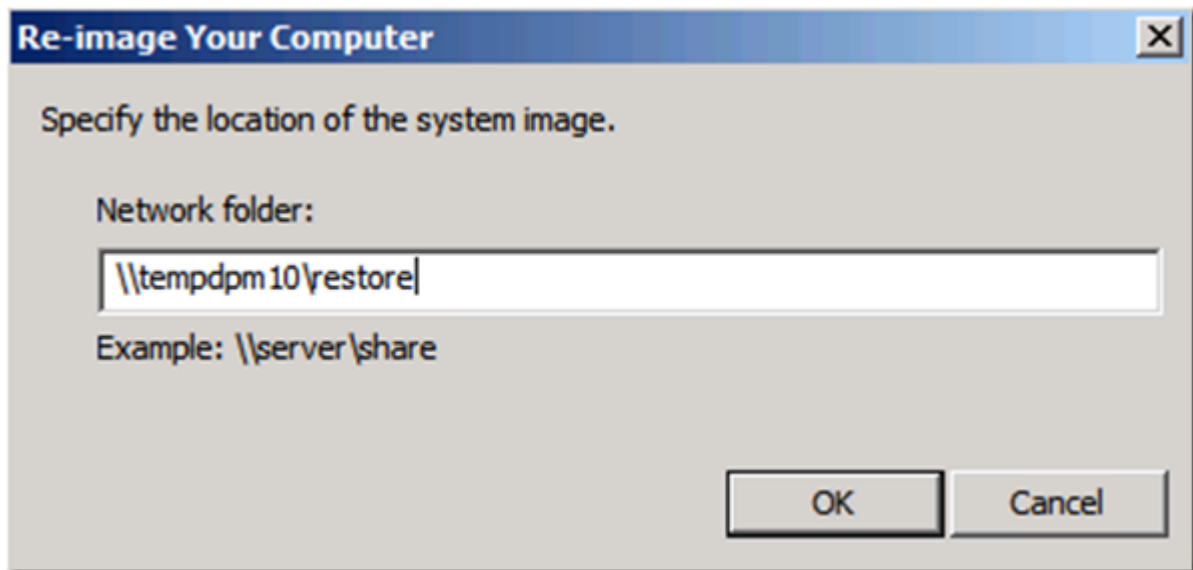
Select a repair



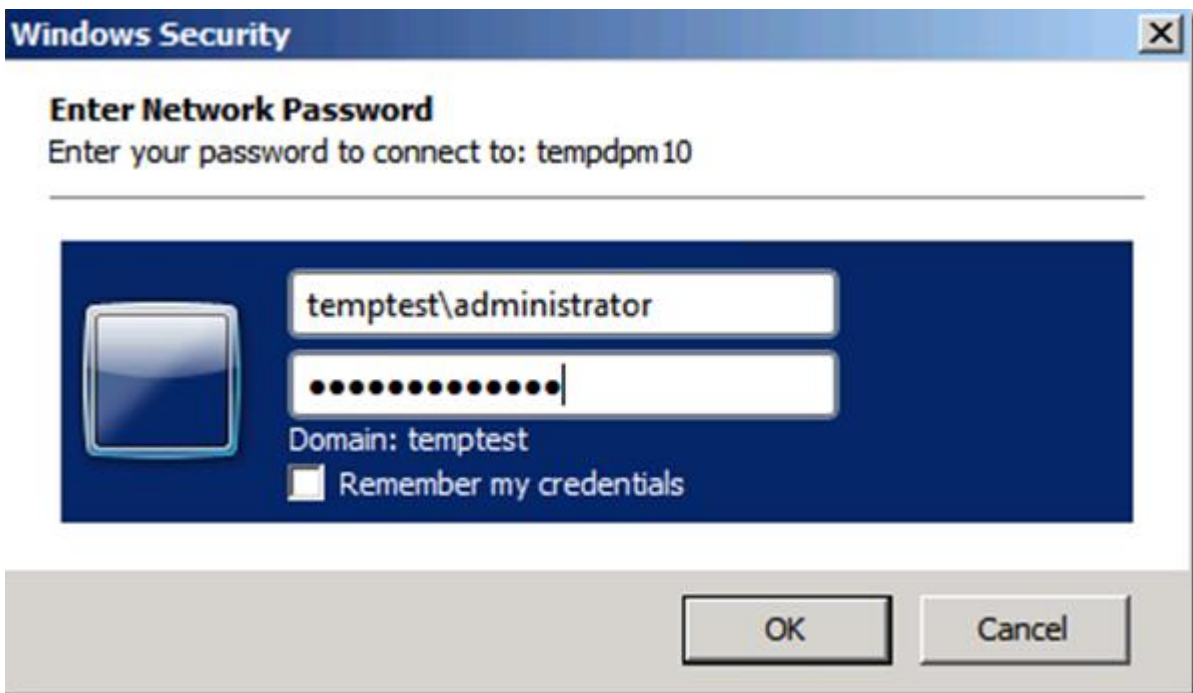
As there are no local images to restore from select next



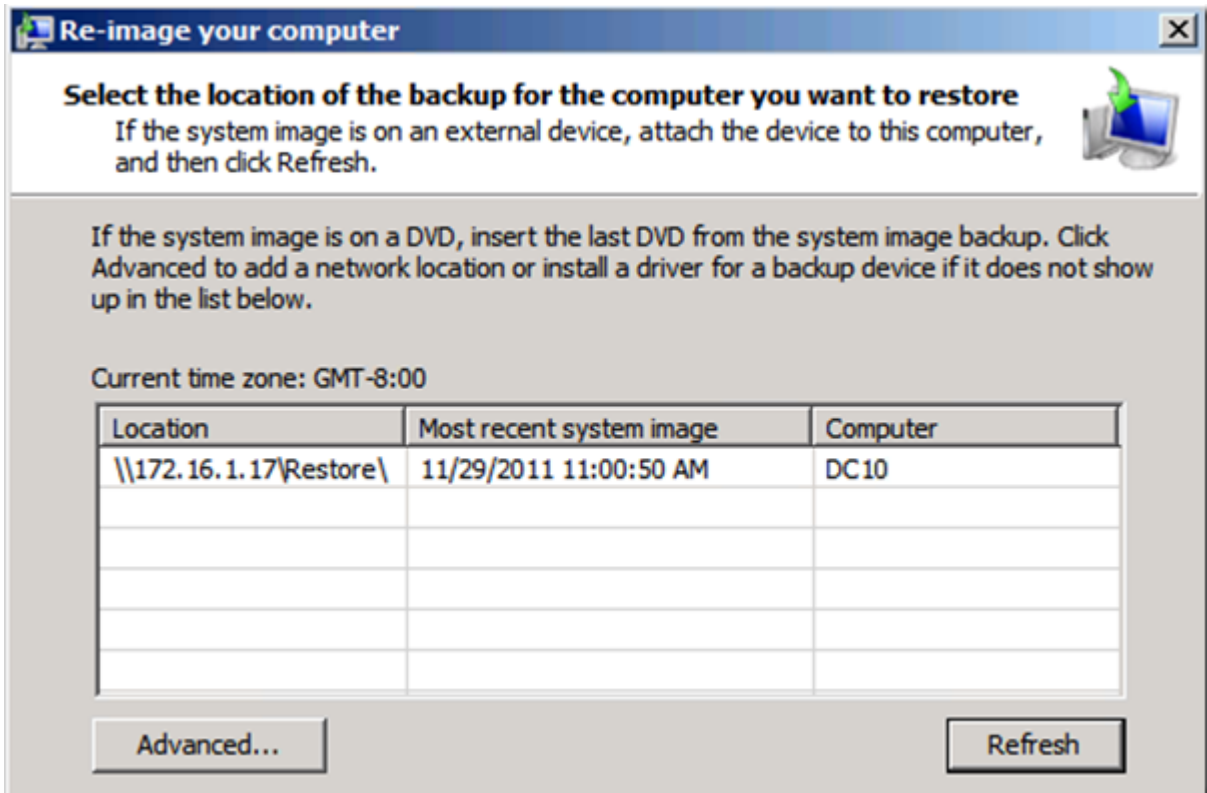
And start networking



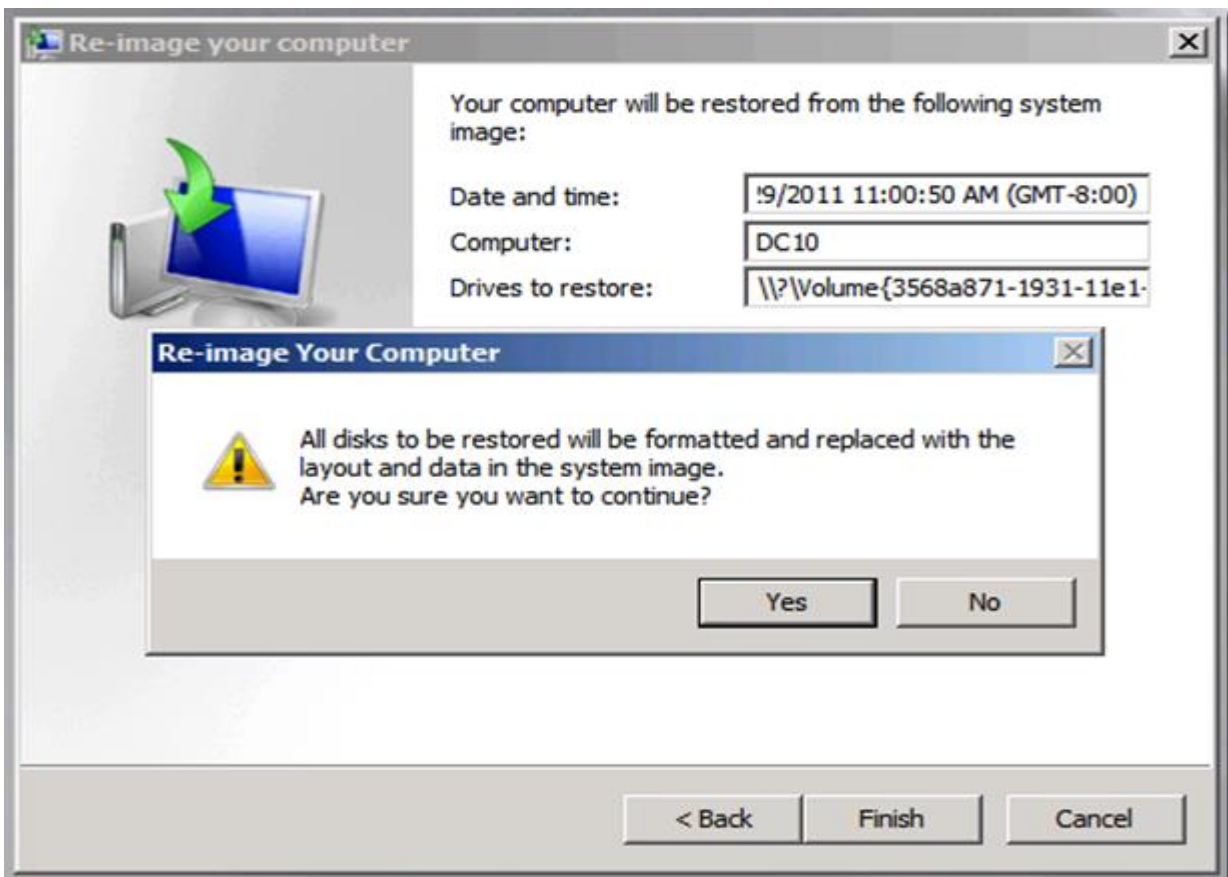
Connect to the DPM Server



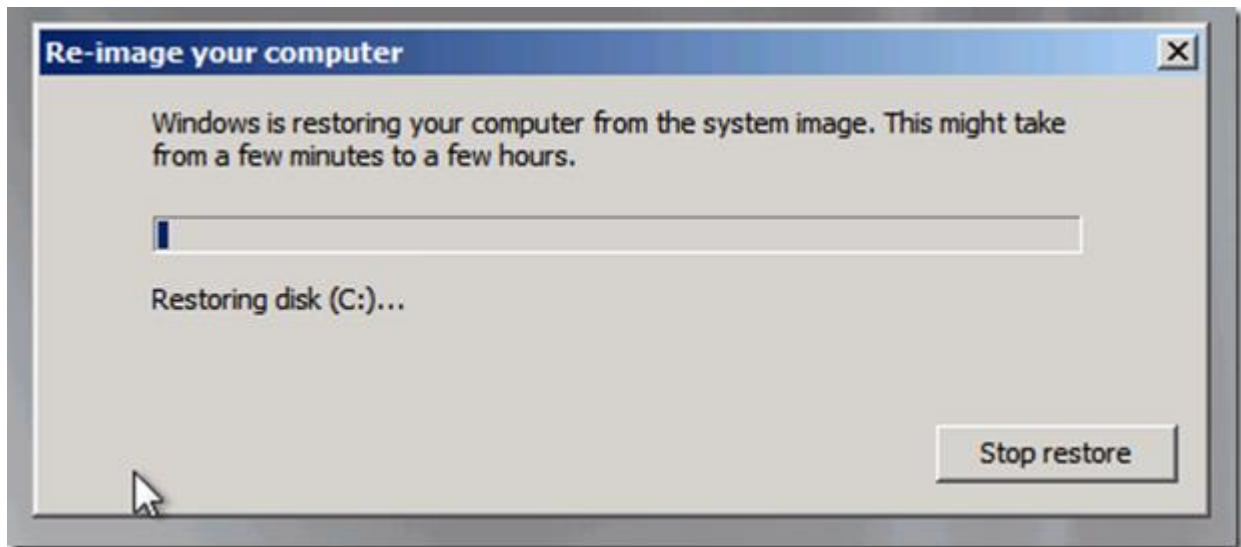
With Credentials from the new temporary domain



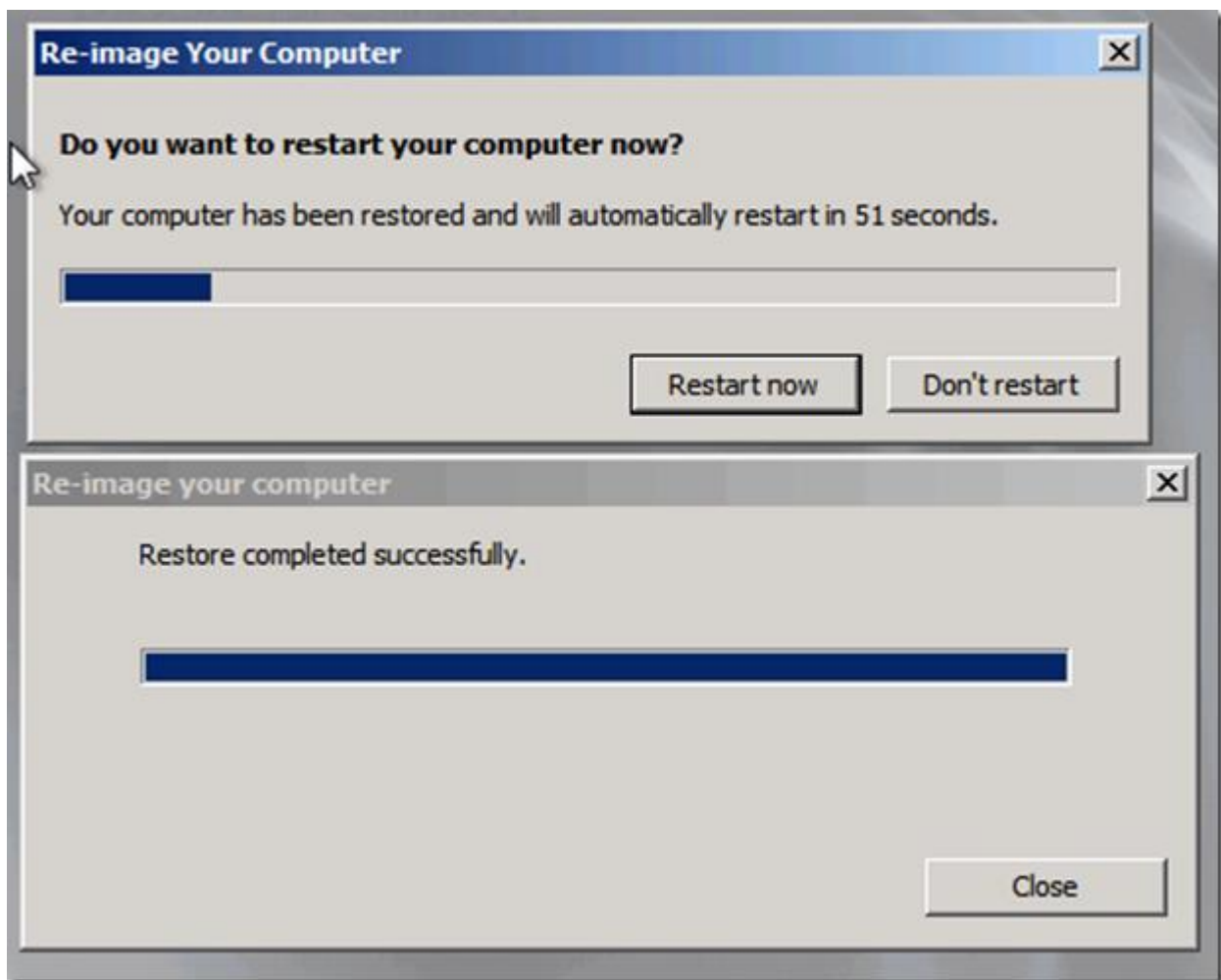
Select the Image to restore



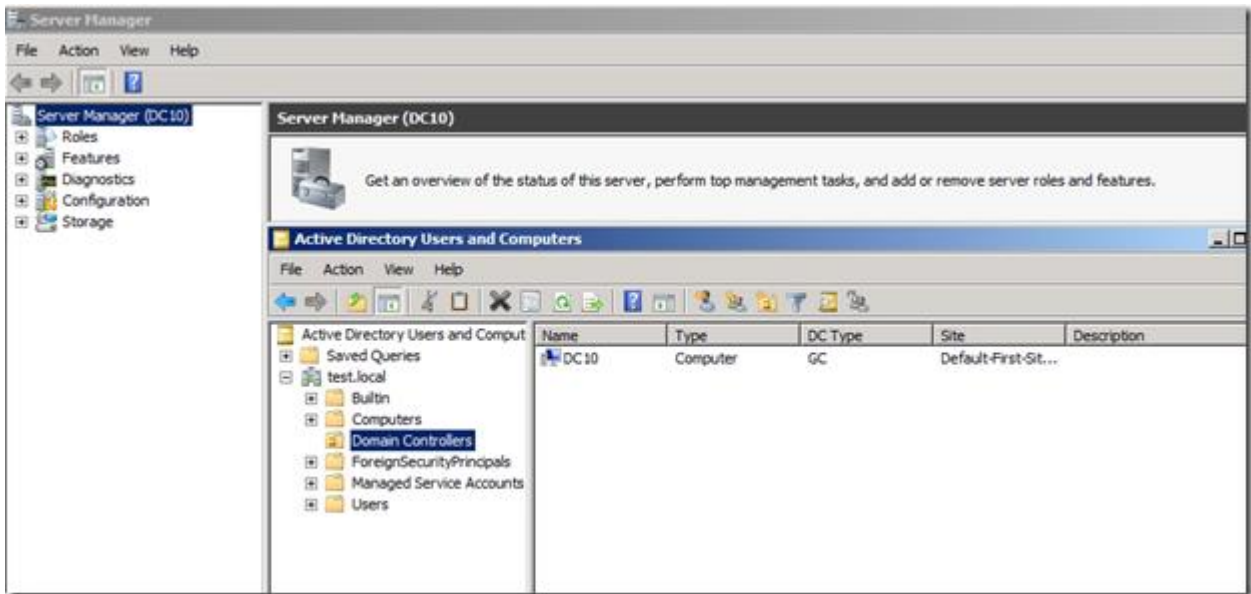
Start the ReImage



And Wait 😊



For about 12 minutes on my test setup



And after a reboot and setting fixed ip address the domain is up and running , and we now have a working domain so we can start to restore the Data Protection Manager server and then start restore all remaining workloads.

Sign: _____

Practical No 5: Using Advisor for proactive Monitoring.

a) Reviewing a critical alert for a Virtual Machine Manager server and assigning an alert.

The screenshot shows the System Center Advisor Alerts interface. The top navigation bar includes 'Welcome, Paul', 'Expert IT Solutions', 'Help', 'Feedback', and 'Sign out'. The main area displays a list of alerts under the heading 'Alerts' with a total of 84 items. The alerts are categorized into 'Error (6 items)' and 'Warning (78 items)'. The selected alert is 'Windows operating system missing update KB976700 to prevent performance problems with SQL Server'. The alert description states: 'You are missing Windows Update KB976700. This update addresses a known issue that leads to poor performance for applications like SQL Server that performs large I/O operations frequently. When this issue occurs, you will see unexplained high CPU usage in privileged mode. This issue occurs only in Windows 7 and Windows Server 2008 R2 operating systems. Apply the Windows kernel update from KB976700 or any Windows hotfix that includes this fix. See the Knowledge Base article for more information on how to address this issue.' The 'Information detected relating to this issue' table shows the following data:

Property Name/ Description	Value
Current NTOSKRNL.EXE file version	6.1.7600.16385
Required NTOSKRNL.EXE file version	6.1.7600.20700
Current NTKRNLP.AXE file version	6.1.7600.16385
Required NTKRNLP.AXE file version	6.1.7600.20700

The Alerts view informs you of severity, time and server name to expedite troubleshooting.

The screenshot shows the System Center Advisor Account settings page. The top navigation bar includes 'Welcome, Paul', 'Expert IT Solutions', 'Help', 'Feedback', and 'Sign out'. The main area is titled 'Account' and contains sections for 'Company Information' and 'User Information'. The 'Company Information' section includes fields for 'Company ID' and 'Company name' (Expert IT Solutions). The 'User Information' section includes fields for 'Windows Live ID', 'First name' (Paul), and 'Last name' (Schnackenburg). There is a checkbox for 'Receive email notifications of new System Center Advisor Alerts' which is checked. The 'Manage User Accounts' section includes a 'Manage Users...' button. The 'Close Company Account' section includes a 'Close Company Account...' button.

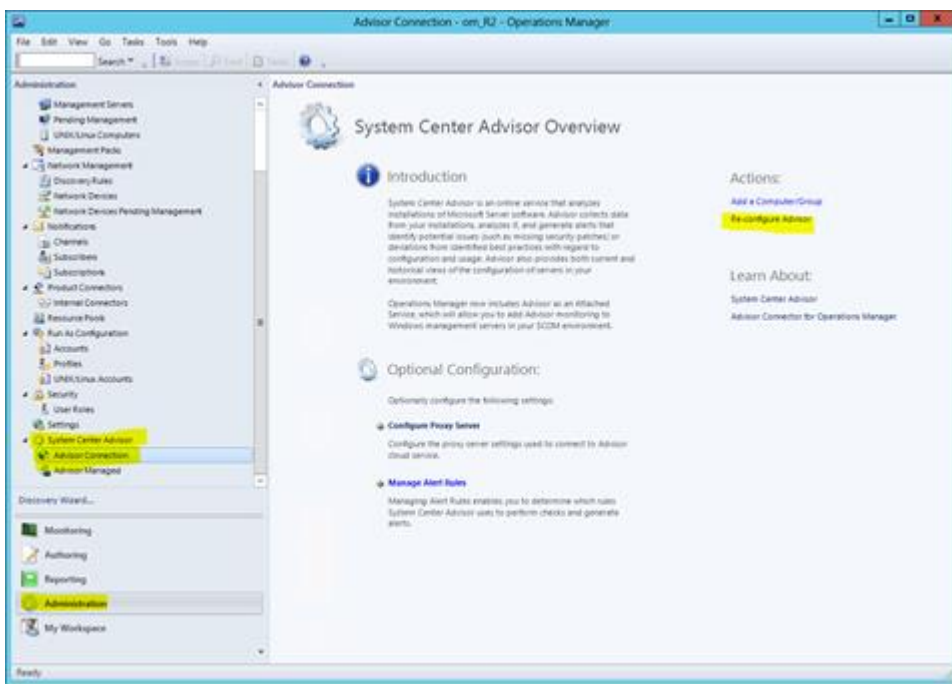
Setting up user accounts and configuring SCA e-mail alerts

b) Integrating Advisor with Operations Manager.

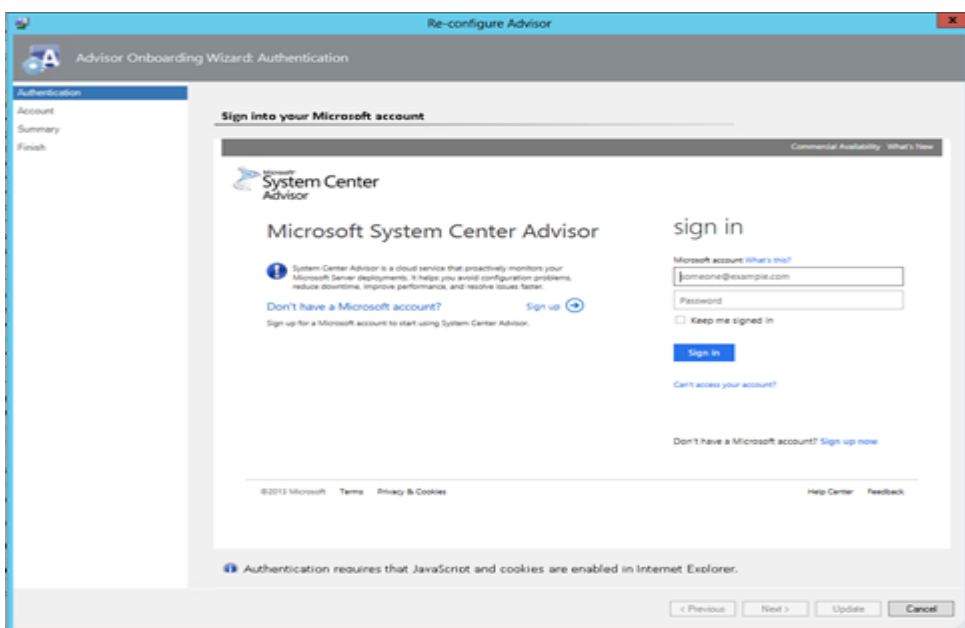
1.) Install SCOM 2012 R2, in my case I am using the SCOM 2012 R2 preview version. I am not showing how to setup SCOM 2012 R2 because this is not the focus of this post.

2.) Sign up for a Microsoft account aka Windows Live ID

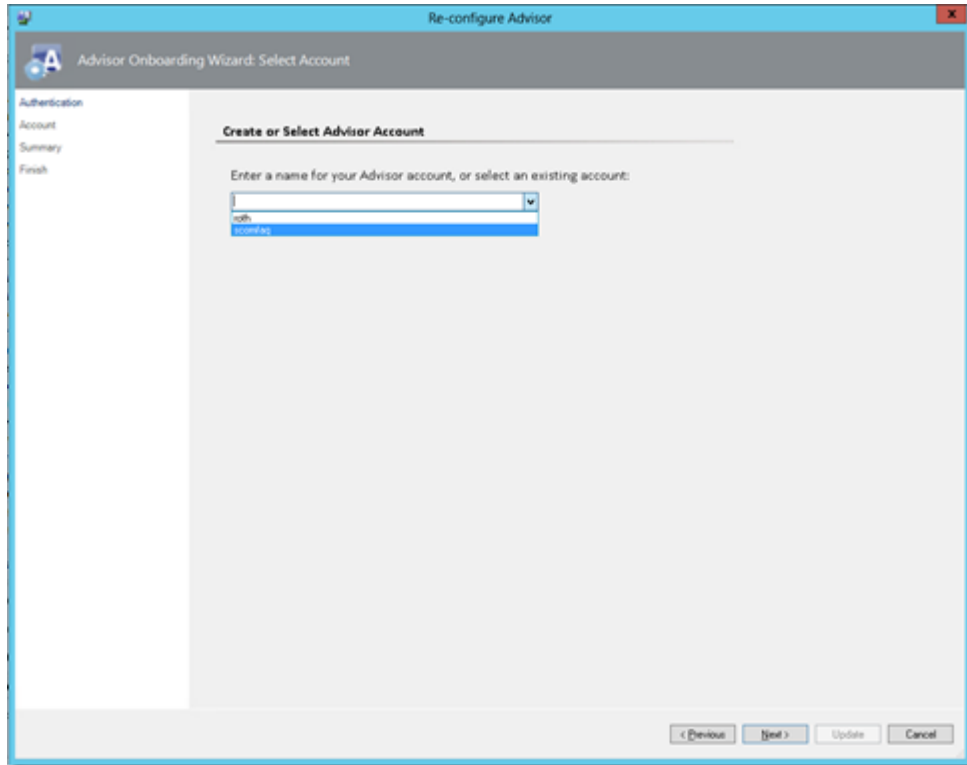
3.) Go to Administration/System Center Advisor/Advisor Connection and choose Register Advisor. Because I have already setup SCA there is only a Re-configure Advisor link on the screenshot...



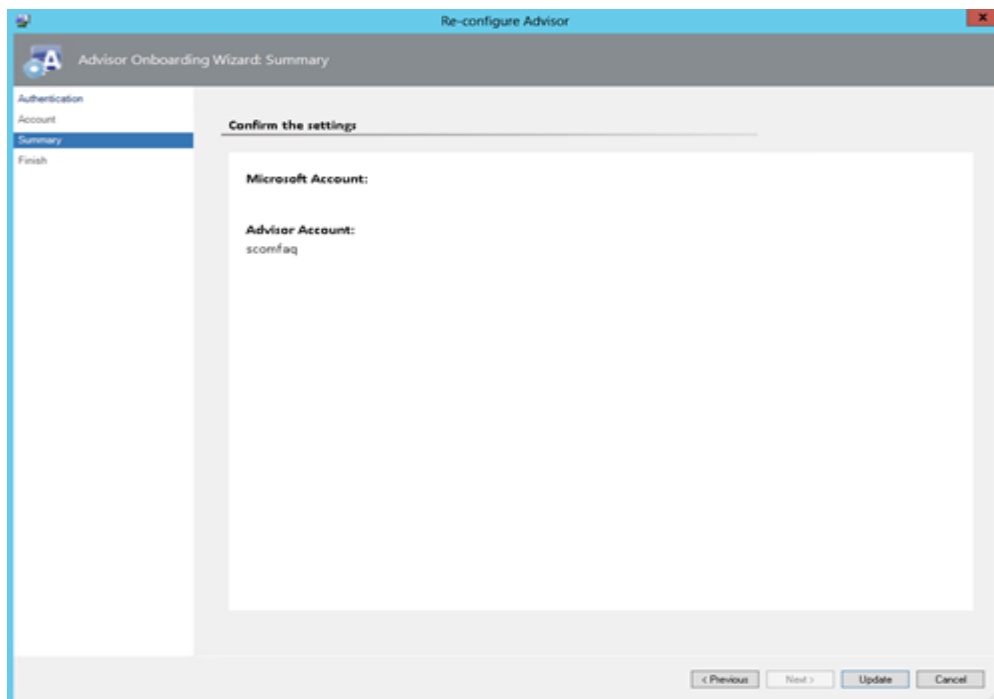
A wizard will open and you need your previously created Microsoft account...



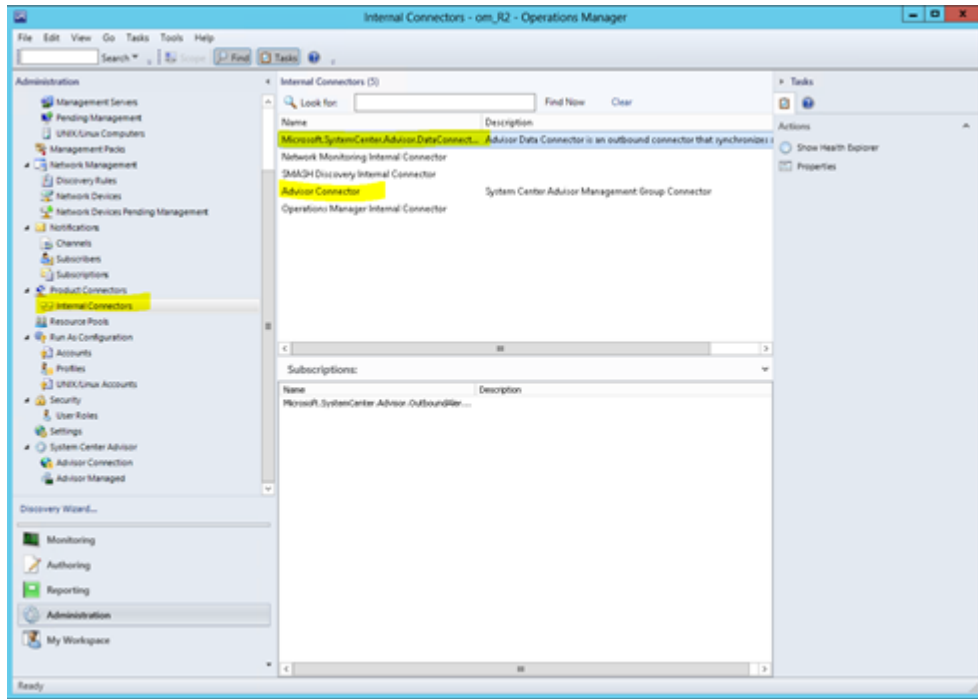
Enter a new Advisor Account by typing an account name. I have accounts created before therefore I will select scomfaq. You can create as many Advisor accounts as you want. These accounts will be used to separate the data if you login into the System Center Advisor portal. There you will be prompted or you can select via dropdown to choose from which account to want to see the data....



If you click Update in my case or Done if you run this wizard for the first time, your setup is finished. YES, that's it, the Advisor setup is finished! So easy...

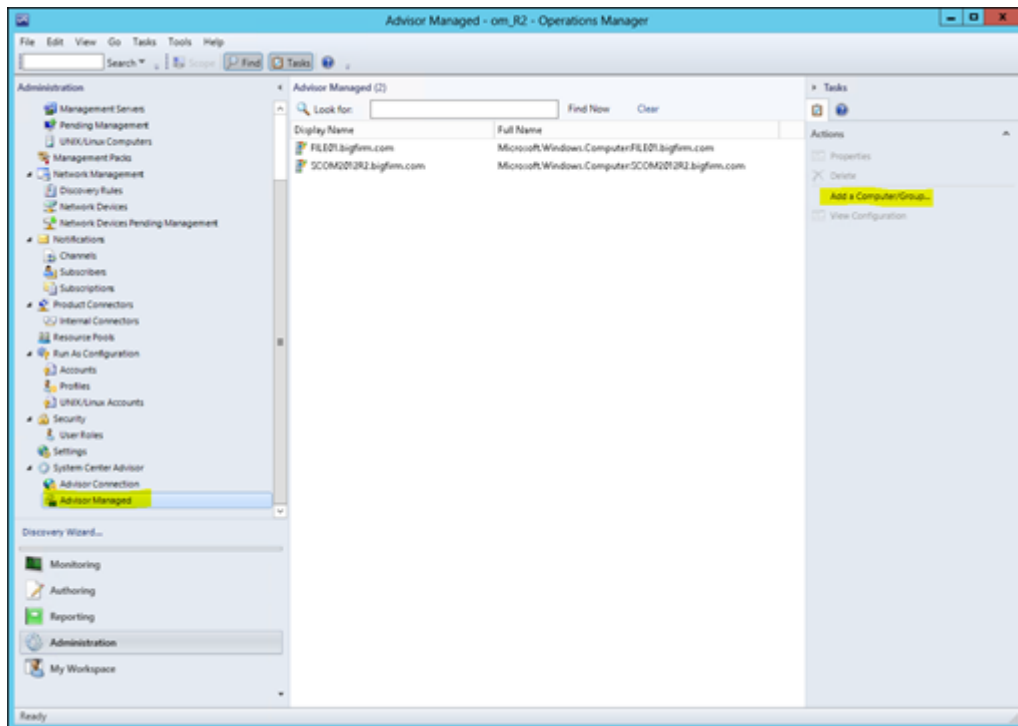


If you go to Administration/Internal Connectors you will see 2 new connectors have been added...

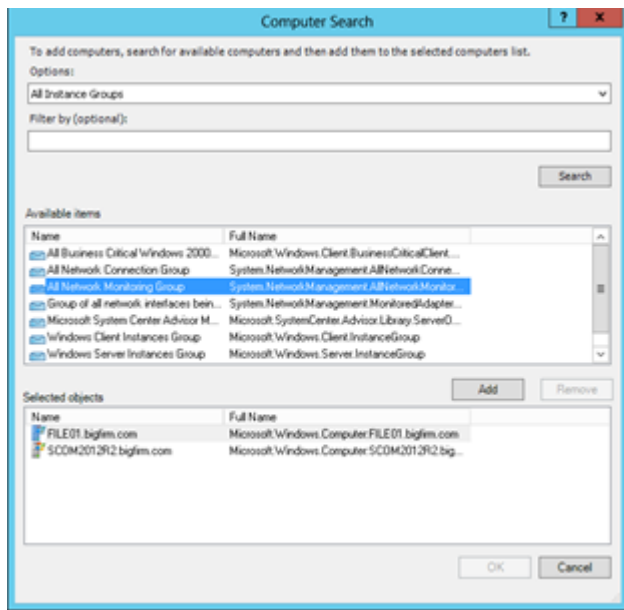


Configuration

As a next step we need to tell Advisor which computers to monitor. Therefore we go to Administration/Advisor Managed/Add a Computer Group...

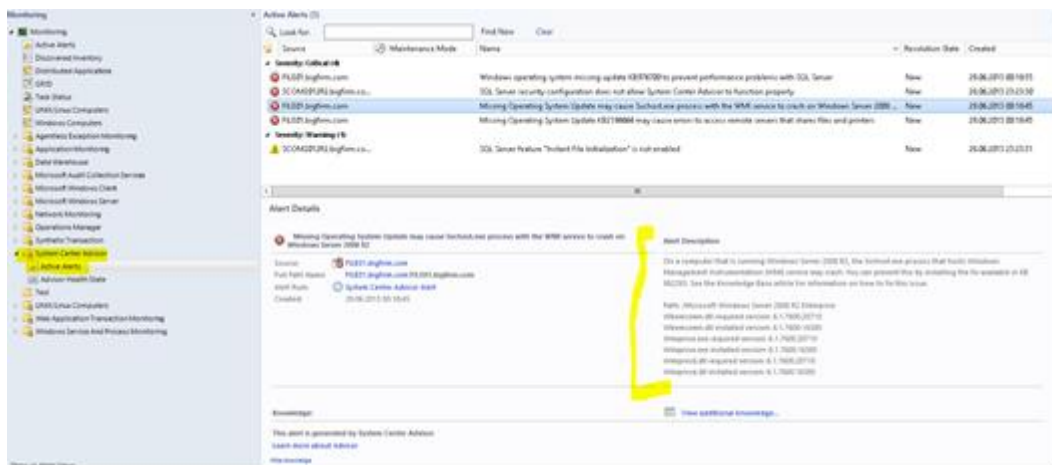


You can add computers and groups, this means you can create a dynamic group and add this group to Advisor and Advisor will automatically analyze all objects in this group...



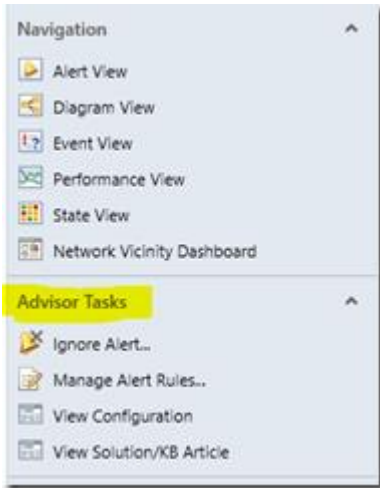
SCOM Views

After a few hours the first alerts are flying into your management group. Go to Monitoring/System Center Advisor and you will find a bunch of alerts. Look close at the alert description how detailed the information appears...

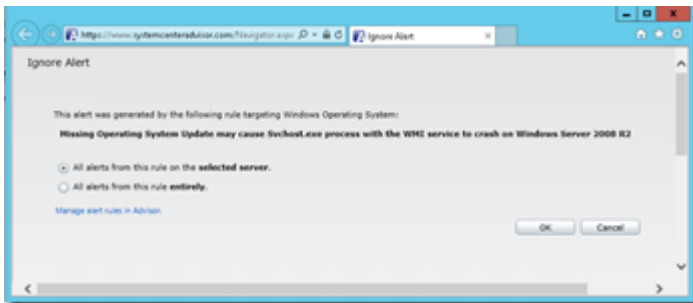


On the right hand side you will find 4 tasks...

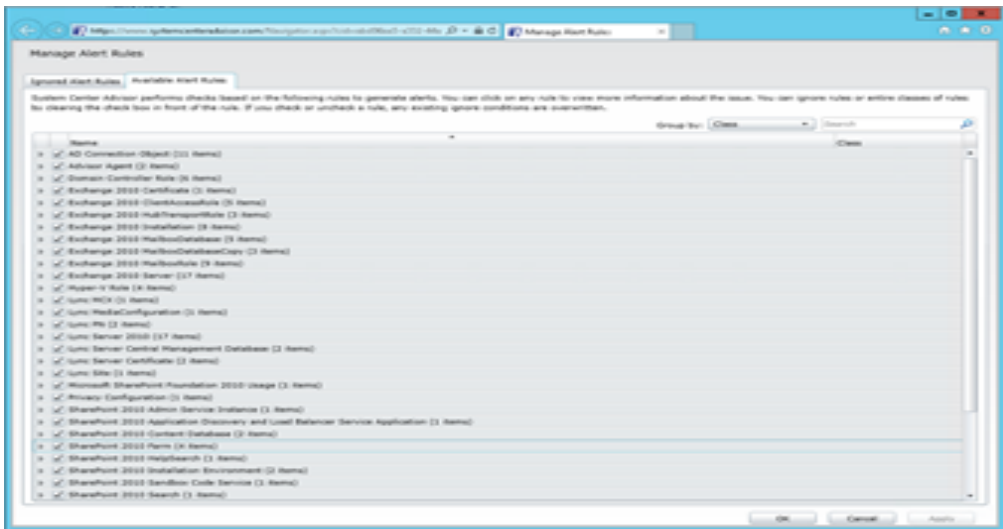
- Ignore Alert...
- Manage Alert Rules...
- View Configuration
- View Solution/KB Article



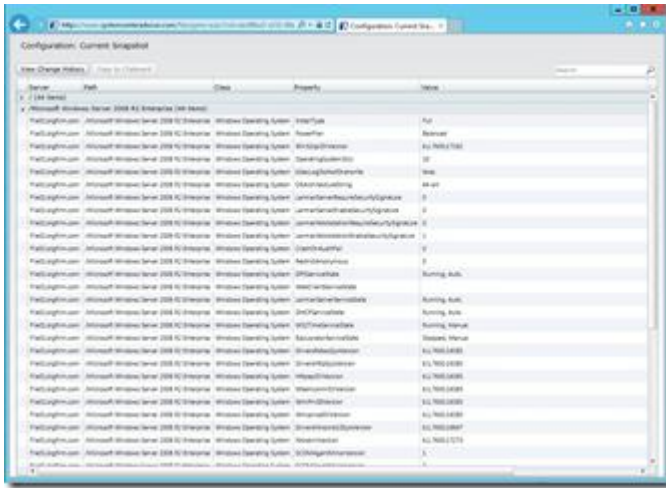
Ignore Alert will allow you to disable the rule...



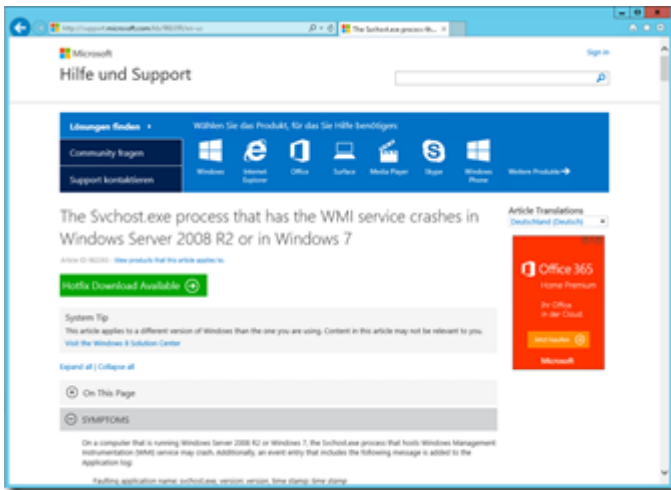
Manage Alert Rules, will show you all the rules available...



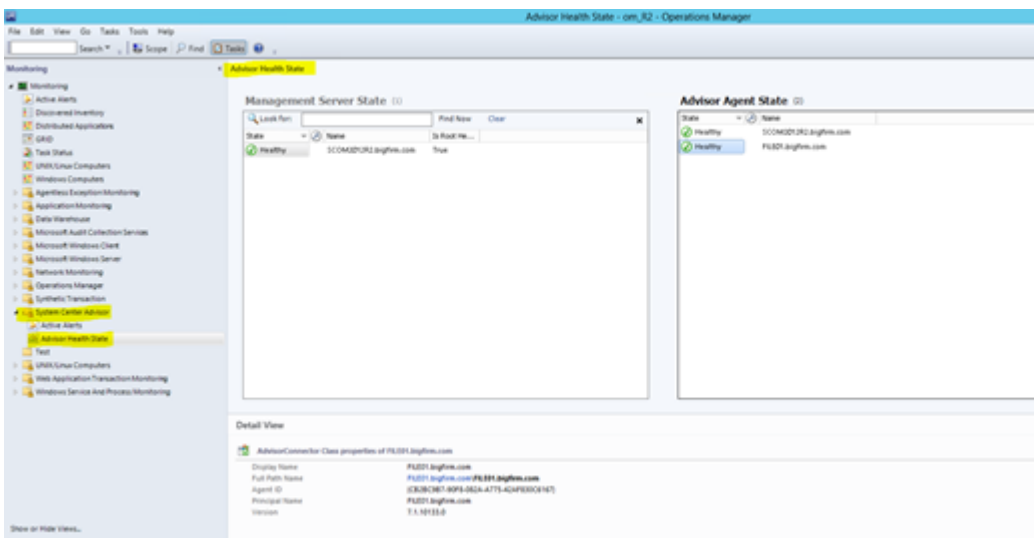
View Configuration will show you all the detailed properties collected from the system where the alert occurred...



View Solution/KB Article shows you the solution to this problem...

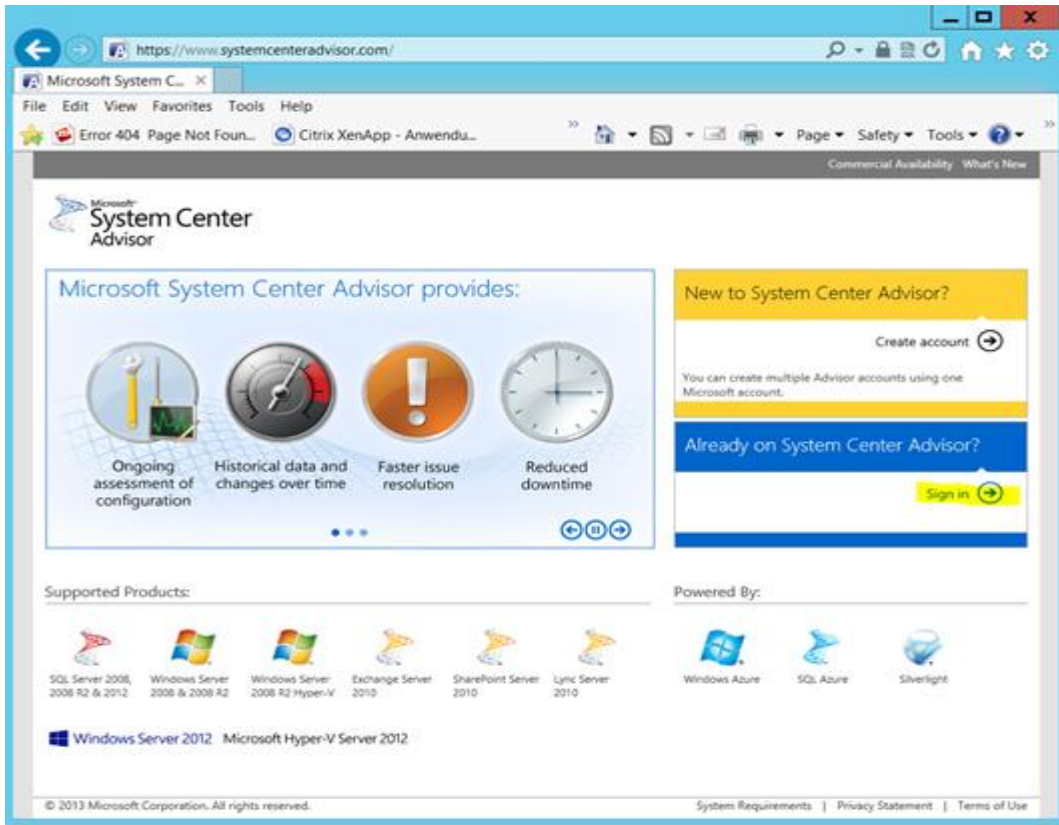


If you navigate to Advisor Health State dashboard you will have an overview if the management server is connected correctly to System Center Advisor and if all the Advisor agents are in a healthy state...

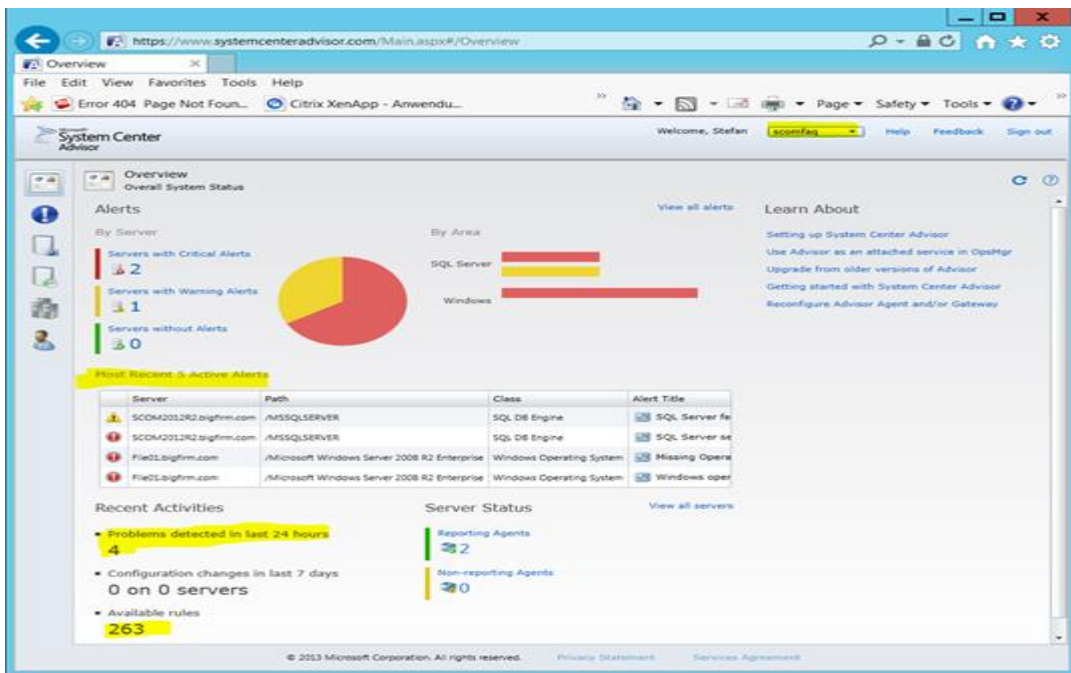


Advisor Portal

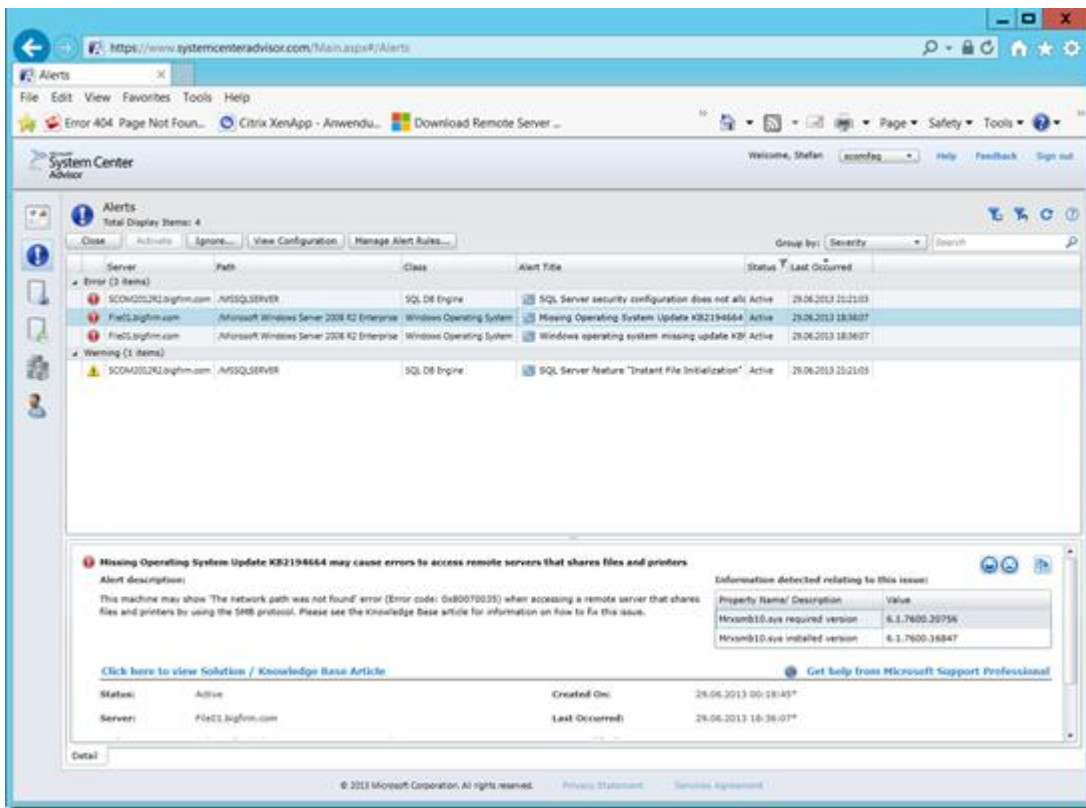
If you would like to check your data online navigate to <http://www.systemcenteradvisor.com> and login with your Microsoft account...



You will get a nice dashboard with your most important information...



Or detailed alert information as you have seen in your SCOM console...



You also can change the rules, account information or add and remove Advisor agents.

Sign: _____

Practical No 6: Using Service Manager to Standardize.

a) Creating a new related service request.

Configuring General Settings

The Request Offering wizard experience begins on the “General” page, pictured in Figure 1.

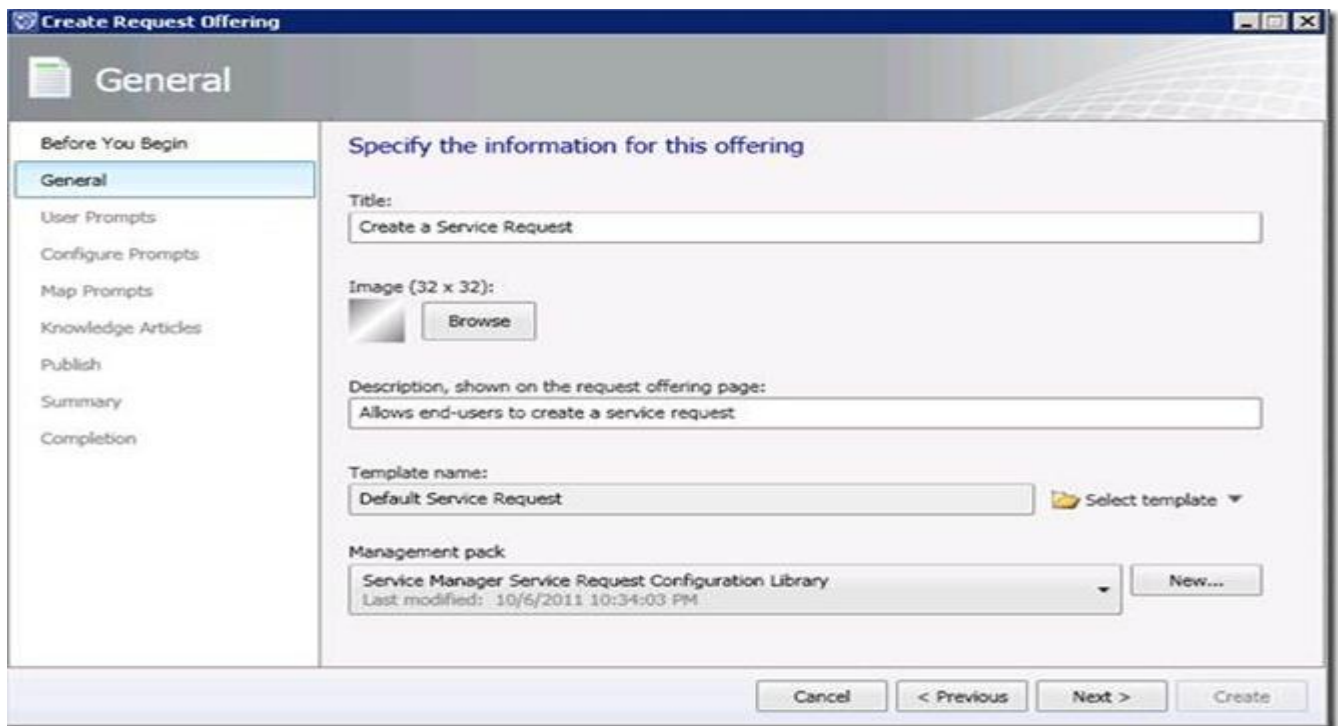


Figure 1: General Page

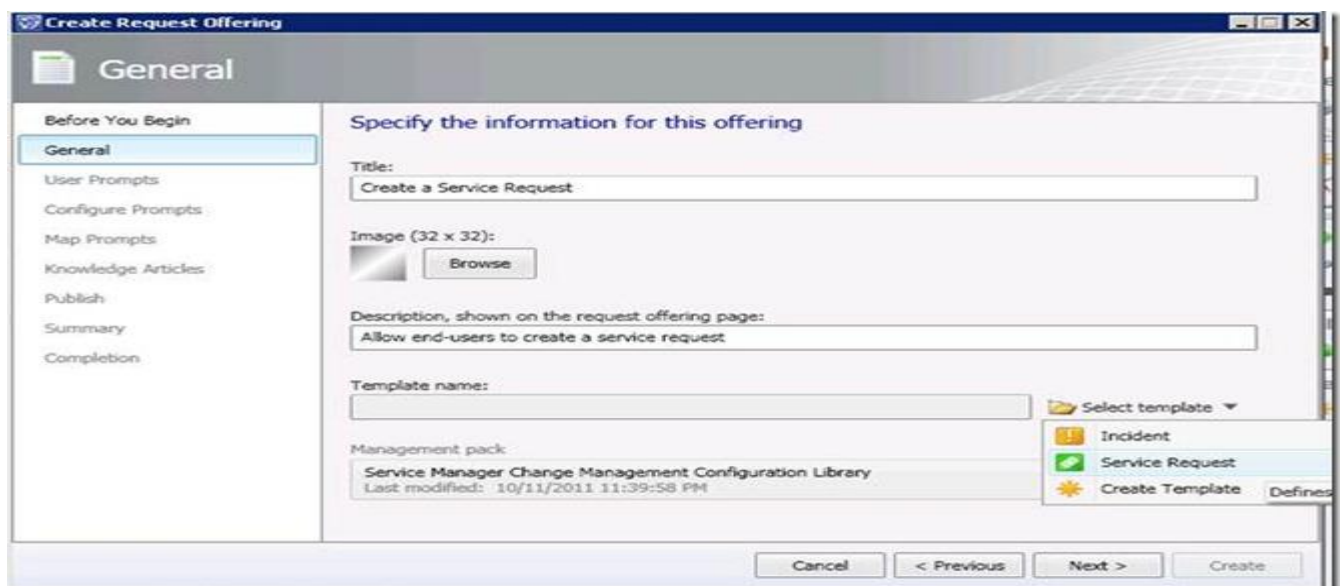


Figure 2: General Page, Select template drop down active

Creating User Prompts

On the “User Prompts” page of the RO wizard, a request author configures the set of prompts that will be displayed to the end user. Each user prompt typically represents (1) a *question* that the service provider will ask the user in order to take action on his or her request or (2) *read-only information* that the service provider will supply to the user to so that he or she can better answer a question.

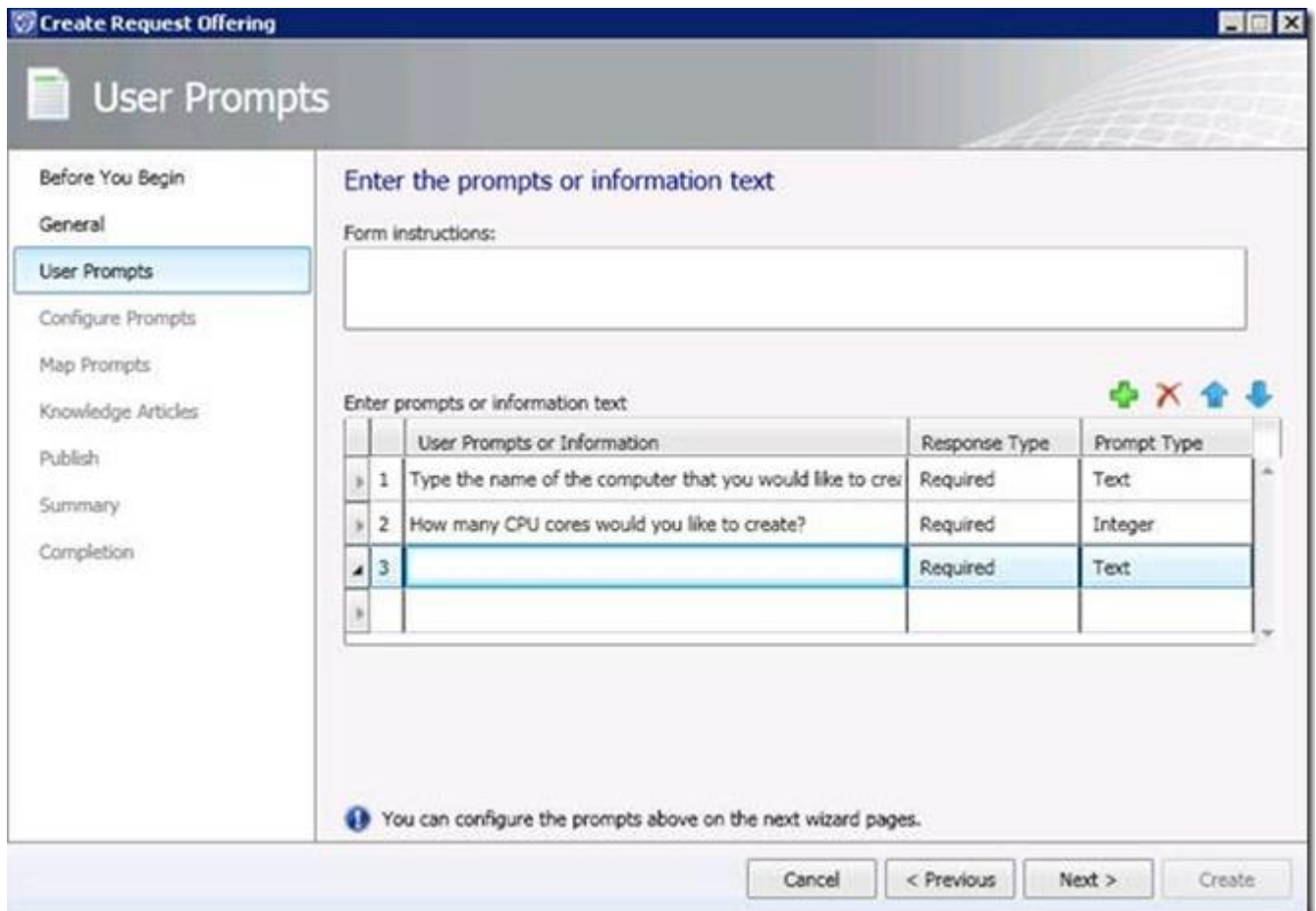


Figure 3: User Prompts Page

Configuring User Prompts

Once the Request Offering author has selected the type of control to display to the user, he or she can configure the parameters of that control on the next wizard page: “Configure Prompts.” This is the page on which the interactive behavior of each prompt control is defined.

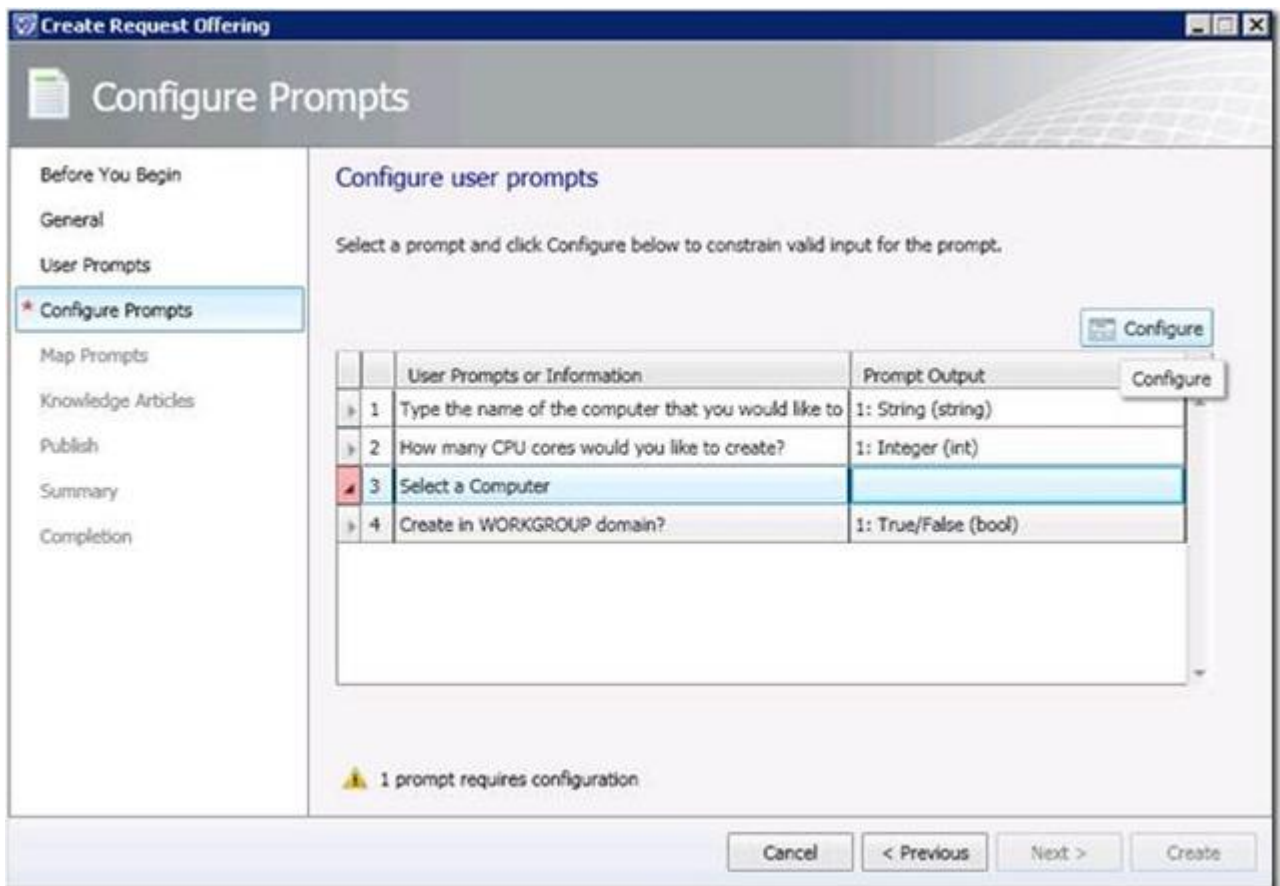


Figure 4: Configure Prompts Page

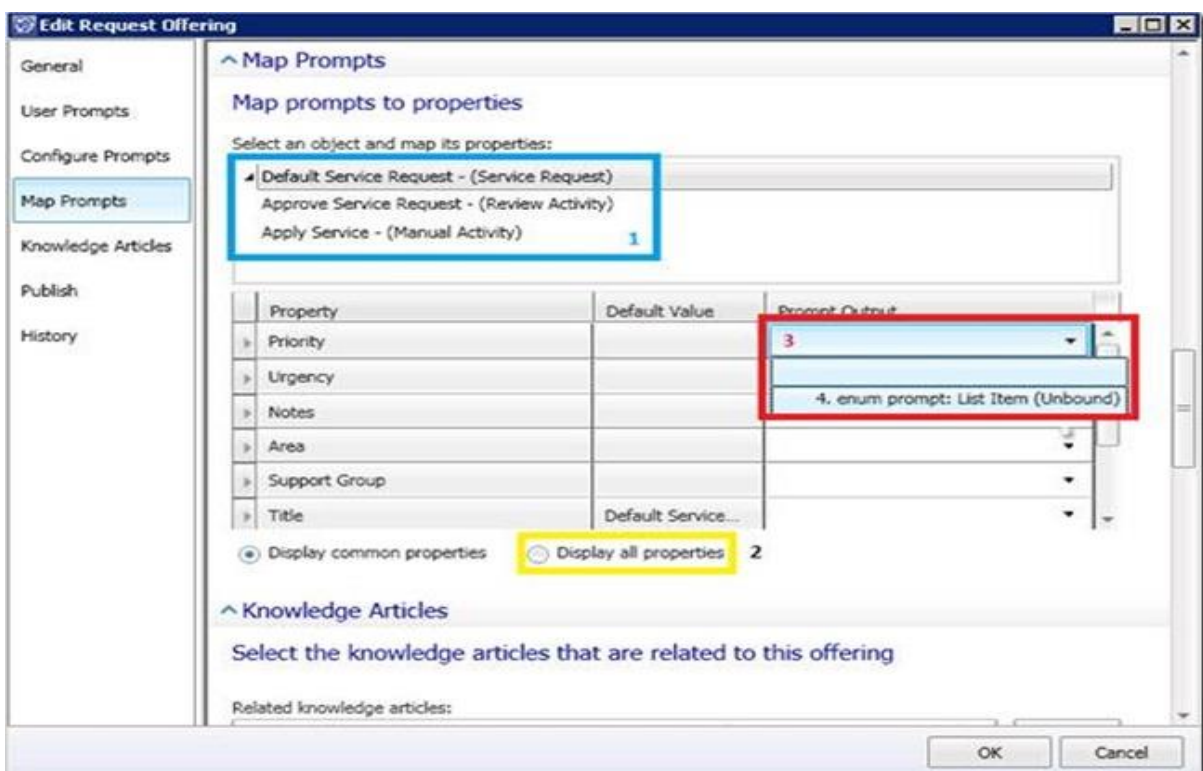


Figure 5: Map Prompts Page

Knowledge Article

Links to relevant knowledge articles can be established on the “Knowledge Article” page. These articles are associated with the request offering when it is displayed on the web portal.

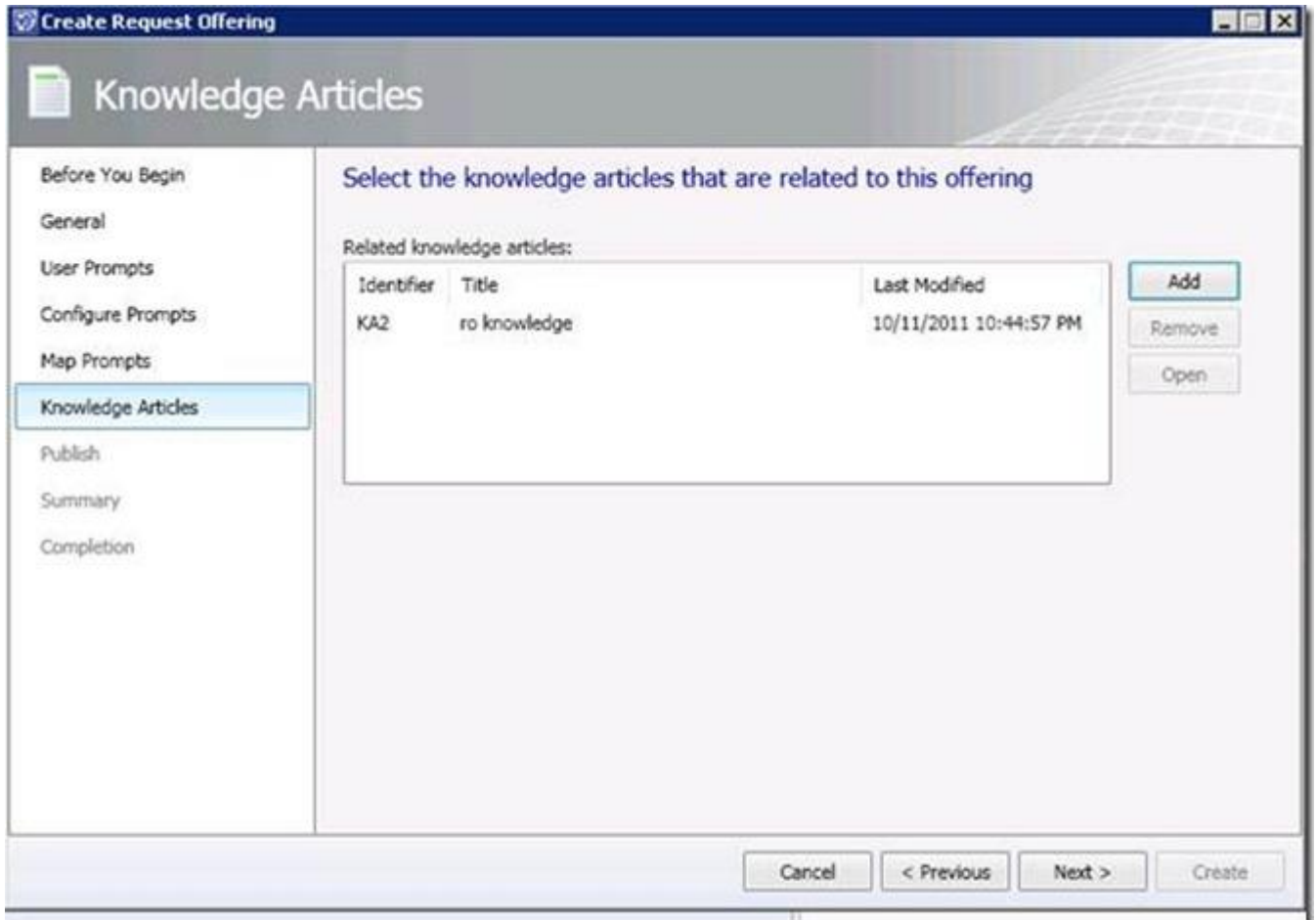


Figure 6: Knowledge Articles Page

Publish

Completing the “Publish” page ends the Request Offering wizard experience. On this page, request authors can designate an owner for the request offering and set the request offering status as either “Draft” or “Publish.” Only published request offerings are visible in the self-service portal. A request offering created in “Draft” status mode can later be promoted to “Publish” status.

Figure 7: Publish Page

If the status of the request offering is set to “Publish,” validation runs before the wizard completes to alert the user to any configuration errors in the request offering. Two common configuration errors include:

1. Failing to map a Required user prompt to at least one property on the Map Prompts page
2. Failing to specify a target relationship for a Required Query Results prompt when that prompt’s outputs are *not* transmitted through token criteria to a subsequent Query Results prompt. Checking either of the two relationship checkboxes on the Options page of the Query Results configuration form bypasses this error.

b) Configuring the settings for an incident and reviewing an incident that has been closed.

To create the alert connector, perform the following steps:

1. In the Administration workspace of the Server Manager console, click Connectors.

2. On the Tasks pane, click Create Connector, and then click Operations Manager Alert Connector.
3. On the General page of the Operations Manager Alert Connector Wizard, provide a name for the alert connector.
4. On the Server Details page, shown in Figure 1-8, specify the name of the Operations Manager server and a Run As account that has permission to connect to Operations Manager. Ensure that you use the Test Connection button to verify that the account works and has appropriate permissions.

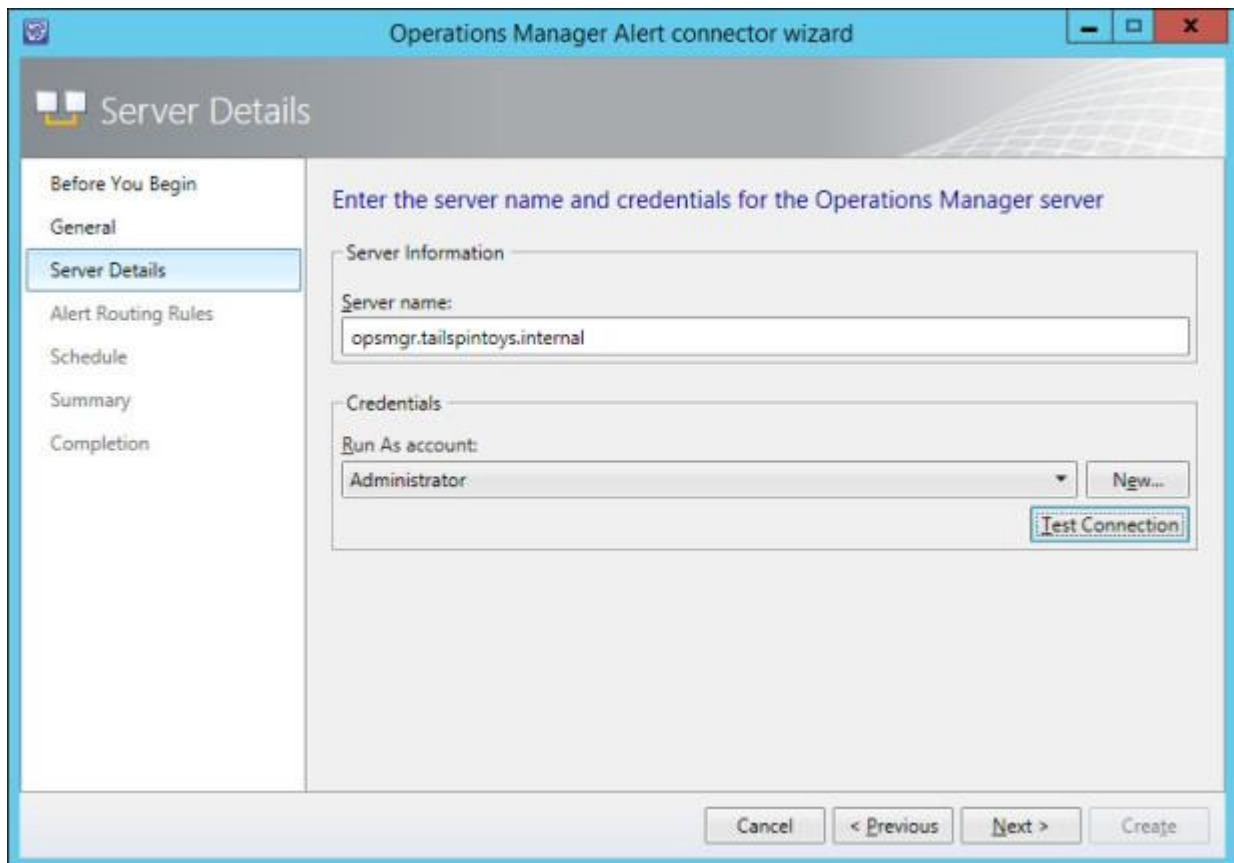


FIGURE 1-8 Alert connector configuration

5. On the Alert Routing Rules page, click Add to add an alert routing rule. An alert routing rule allows you to specify which Service Manager incident template will be used to create an incident based on an Operations Manager alert.
6. In the Add Alert Routing Rule dialog box, shown in Figure 1-9, provide the following information:
 - **Rule Name** The name of the alert routing rule.
 - **Template** The Service Manager incident template that will be used when creating the Service Manager incident.
 - **Criteria Type** Here you can select the conditions that trigger the alert routing rule. You can choose between the alert being generated by a specific Operations Manager management pack, being generated by a specific computer or security group, a custom field, or an Operations Manager monitoring class.

- **Select Alert Severity And Priority** Allows you to specify the alert priorities and severities that will trigger the alert routing rule.

Add Alert Routing Rule

Rule Name
Network Alerts

Template
Networking Issue Incident Template

Select Criteria Type

Operations Manager Management Pack containing the Rule or Monitor raising the alert

Management Pack Name Equals Network Management - Core

Computer for which the alert was raised

Computer is a member of group

Custom Field

Operations Manager class for which the alert was raised

Monitoring class name

Select alert severity and priority

Priority | High

Severity | Critical

OK Cancel

FIGURE 1-9 Alert routing rule

7. As Figure 1-10 shows, alerts that don't match any of your configured rules will automatically be created as incidents using the Operations Manager Incident Template.

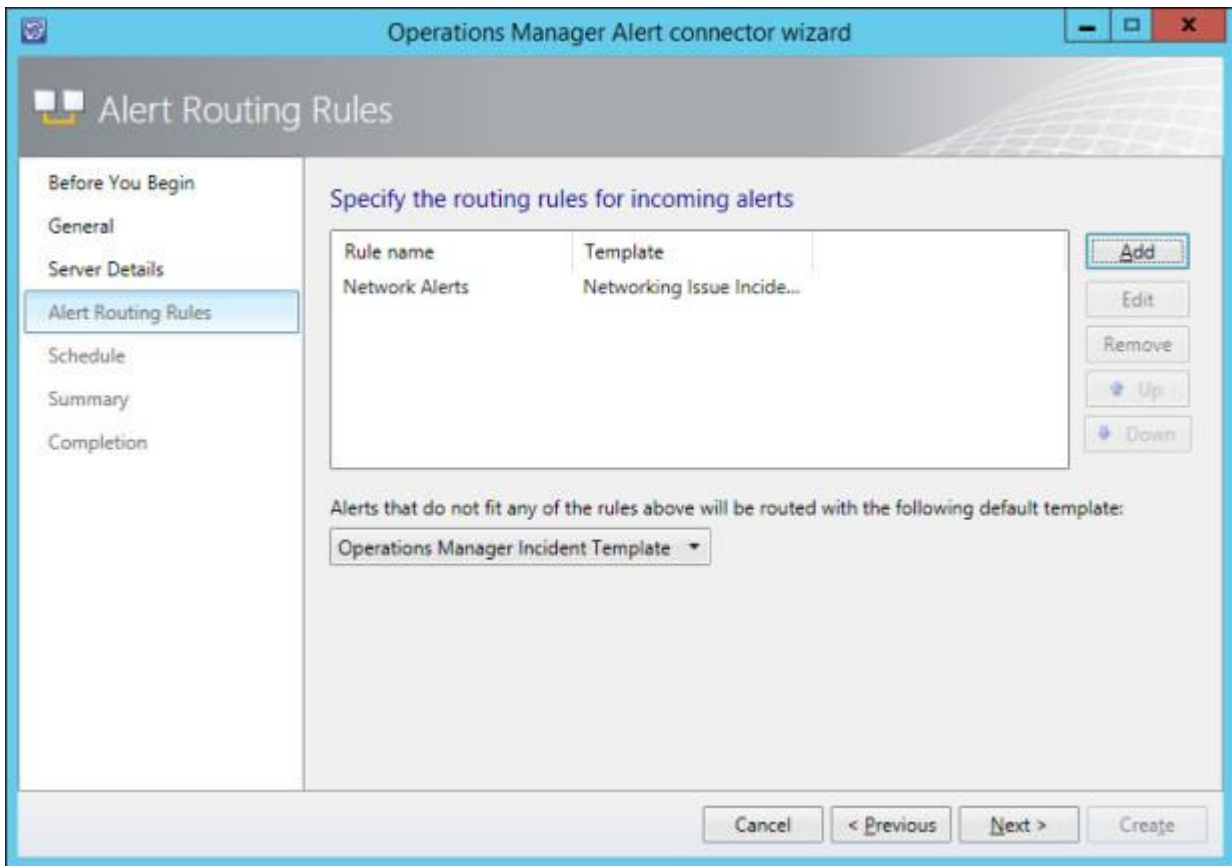


FIGURE 1-10 Routing rules

8. On the Schedule page, select the frequency at which Service Manager will query the Operations Manager server for alerts. You can also configure the connector so that alerts within Operations Manager will be closed when the incident that relates to the alert is resolved or closed in Service Manager. You can also configure Service Manager to automatically mark incidents as Resolved if the incident that triggered the alert in Operations Manager is closed. Figure 1-11 shows these settings.

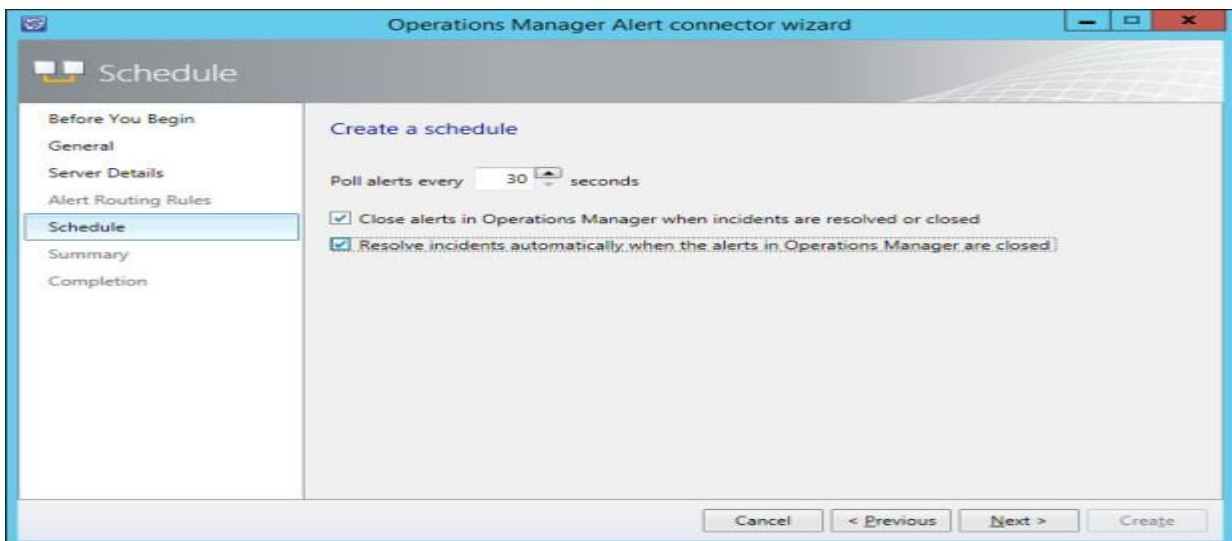


FIGURE 1-11 Schedule settings

9. On the Summary page, review the connector setup, and then create the connector.

Once the connector is created, you can modify the alert routing rules by editing the properties of the connector as shown in Figure 1-12.

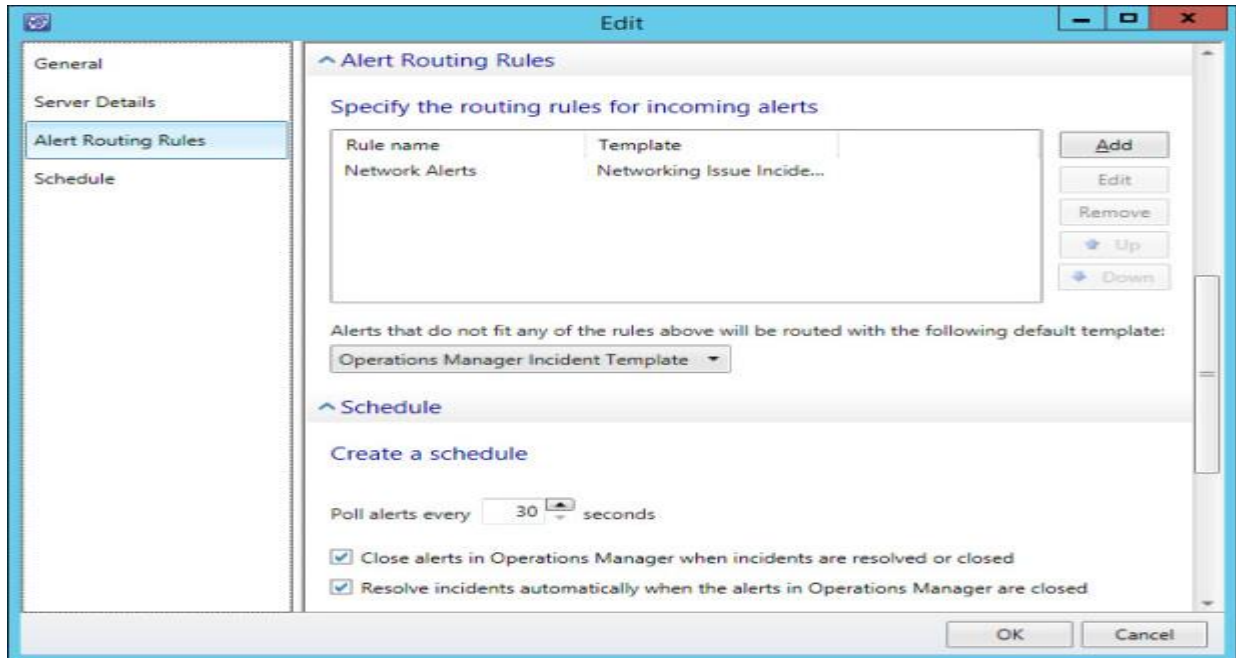


FIGURE 1-12 Connector properties

Sign: _____

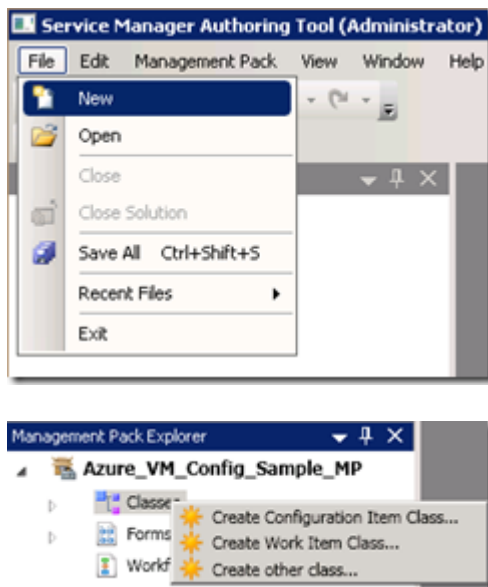
Practical No 7: Using Orchestrator for automation.

a) Creating a simple virtual machine in Windows Azure using System Center Orchestrator. (Should be performed Online)

Step 1. Create a new configuration item class in Service Manager

So for the Windows Azure VM configuration to come out of Service Manager we will need to create a new configuration item class which you can do with the **System Center Service Manager Authoring Tool** which can be downloaded here:<http://www.microsoft.com/en-us/download/details.aspx?id=36214>

Start the Authoring Tool, click “File” and then “New” and let’s create a new management pack and a new configuration item class:



Since I wanted an unique identifier (not a GUID) which I could refer to, I decided to create an “Azure VM Config ID” which I made my key property. I initially wanted to use my Azure VM ConfigName as an unique name (sounds logical doesn’t it?), but quickly found out that if you delete that configuration, you can’t re-use that same name, because it is still in the database with the status of “pending delete”. So first delete the famous “Property_4” default key property:

Key	Name	Data type	Value constraints
	About Configuration Item	Relationship	Configuration Item
	Affects Customers	Relationship	User
	Asset Status	List	Asset Status
	Collection has configuration item	Relationship	Configuration Item
	Config Item References Location	Relationship	Location
	Contains Configuration Item	Relationship	Configuration Item
	Display Name	String	
	DisplayName (Internal)	String	
	Has File Attachment	Relationship	File Attachment
	Id (Internal)	GUID	
	Is Related to Configuration Item	Relationship	Configuration Item
	LastModified (Internal)	Date Time	
	LastModifiedBy (Internal)	String	
	Notes	Rich Text	
	Object Status	List	Object Status
	Owned By User	Relationship	User
	Served By User	Relationship	User
	Timestamp (Internal)	Date Time	
	Property_4	String	

If you want your new key property to be filled in and incremented automatically then set these two fields:

Azure VM Config ID (Property)	
General	
Data Type	String
Description	
Internal Name	AzureVMConfigID
Name	Azure VM Config ID
Others	
Auto Increment	True ←
Case Sensitive	False
Default Value	{0} ←
Key	True
Maximum Length	256
Maximum Value	2147483647
Minimum Length	0
Minimum Value	-2147483648
Required	False

This will automatically increment your ID *without* prompting the user for a value when the configuration form is being filled in.

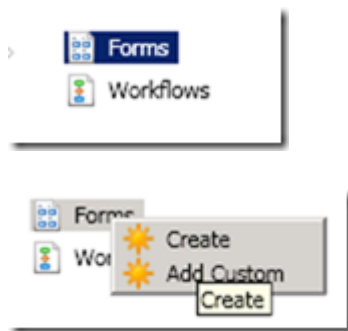
The next step is to think about which fields you need and would like to have. Your logical starting point I think is to look at the “*AzureDeploymentDemo.txt*” text file and get those fields in there which I’ve done to start with:

Key	Name	Data type	Value constraints
	Azure VM Config ID	String	
	Azure VM Config Name	String	
	Blob VH Name	String	
	Service Description	String	
	Service DNS Prefix	String	
	Service Label	String	
	Service Location Affinity	List	Azure VM Config -
	Service Location Dr Affinity Group	List	Azure VM Config -
	Storage Account Description	String	
	Storage Account Label	String	
	Storage Account Location Affinity	List	Azure VM Config -
	Storage Account Location Dr Affinity Group	List	Azure VM Config -
	Storage Account Name	String	
	Storage Container Name	String	
	VM Computer Name	String	
	VM Deployment Label	String	
	VM Deployment Name	String	
	VM Deployment Slot	List	Azure VM Config -
	VM Endpoint Local Port	List	Azure VM Config -
	VM Endpoint Name	String	
	VM Endpoint Protocol	List	Azure VM Config -
	VM Endpoint Public Port	List	Azure VM Config -
	VM Image Type	List	Azure VM Config -
	VM Instance Name	String	
	VM Instance Size	List	Azure VM Config -
	VM Operating System Type	List	Azure VM Config -

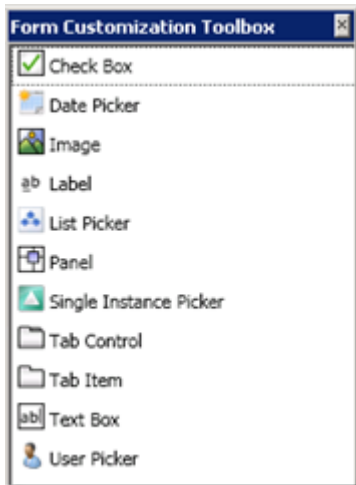
Since my initial objective was to “just deploy a Windows Azure VM” I initially used only those fields to just do that, you can pretty much create your own property if you see a need for it. My recommendation to you is to really overthink the property you are adding. Is it a configuration property or for example a connection string, which probably should be stored in another place.

Step 2. Create a custom form

Now that you have added all the custom properties to your new configuration item class, you can go all fancy with creating a custom form. You can add text labels, dropdown boxes, a logo, different font types and colors, etc.:



Use the “Form Customization Toolbox” to create the form you would like, just start drop and dragging:



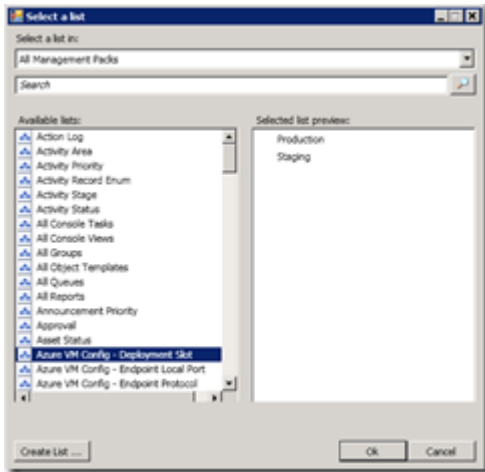
And you will end up with something like this:

Notice that I'm using dropdown boxes for fields that are common or fields that you don't want your users to become "creative" with like VM sizes or the source image you would like them to use. To achieve that you change the property to a "list data type" property:

VM Deployment Slot	List	Azure VM Config - Deployment Slot
VM Endpoint Local Port	List	Azure VM Config - Endpoint Local Port
VM Endpoint Name	String	
VM Endpoint Protocol	List	Azure VM Config - Endpoint Protocol
VM Endpoint Public Port	List	Azure VM Config - Endpoint Public Port
VM Image Type	List	Azure VM Config - Image Type

VM Deployment Slot (Property)	
General	
Date Type	List
Description	
Internal Name	VMDeploymentSlot
Name	VM Deployment Slot
Others	
Auto Increment	False
Case Sensitive	False
Default Value	
Key	False
Maximum Length	256
Maximum Value	2147483647
Minimum Length	0
Minimum Value	-2147483648
Required	False
Value Constraints	
List type	Azure VM Config - Deployment Slot
List type internal name	AzureVMConfigDeploymentSlotList

And then create a custom list:



If you would like to put entries/values in the list you can edit your new management pack with a XML editor or you can add those values later in the Service Manager console. Here's a snippet view from Visual Studio:

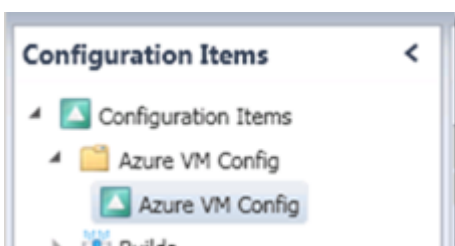


If you are not comfortable with XML editing then import your new management pack into Service Manager, add values to your new list, export your management pack and open the modified management pack in the authoring console.

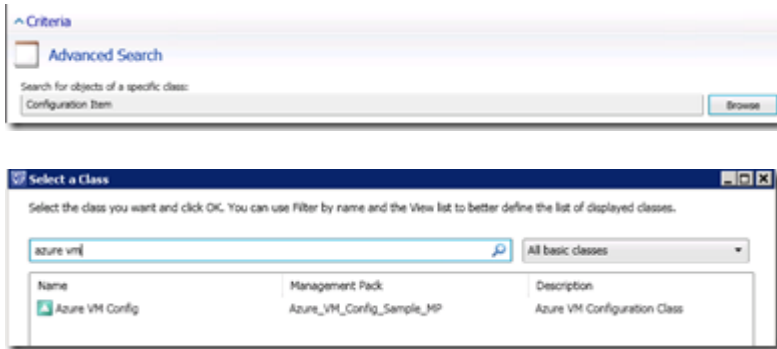
Note: This would be a good time to start saving different versions of your management pack in case something goes wrong and you need to revert back 😊

Step 3. Create a Service Manager console view

Now that you have created your custom configuration class, a custom form, your lists and added those to dropdown boxes onto your form, it is time to finally import your new management pack into Service Manager. After importing your MP you can create a new folder & view to expose your new class and form:

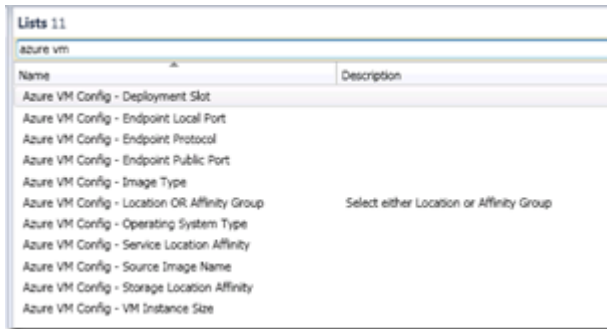


If you create your new view, you need to browse for your new configuration item class:

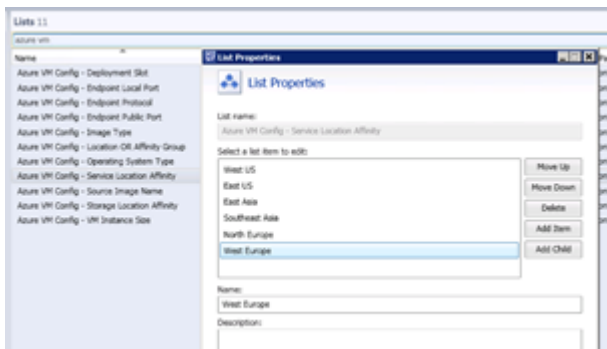


Then add all the the columns you wish to display.

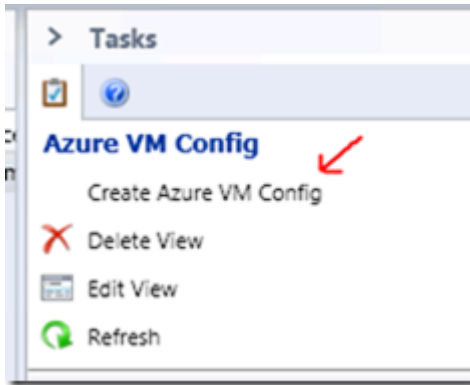
Before you create your first Windows Azure VM configuration, make sure that all the lists are populated. Go under “Library” and then “Lists” and search for you custom class:



Verify that you have entries:



Now go back to “Configuration Items” node and create your first Windows Azure VM configuration:



VM Config Name:
Gold

Service
Service Label: xwservice01 Service Description: my demo Location OR Affinity Group: Location
Service DNS Prefix: xwservice01 Service Location Affinity: West Europe

Storage
Storage Account Name: xwstorageaccount Storage Account Description: my demo Storage Location OR Affinity Group: Location
Storage Account Label: xwservicestorage Storage Container Name: xwservicestorage Storage Account Location Affinity: West Europe

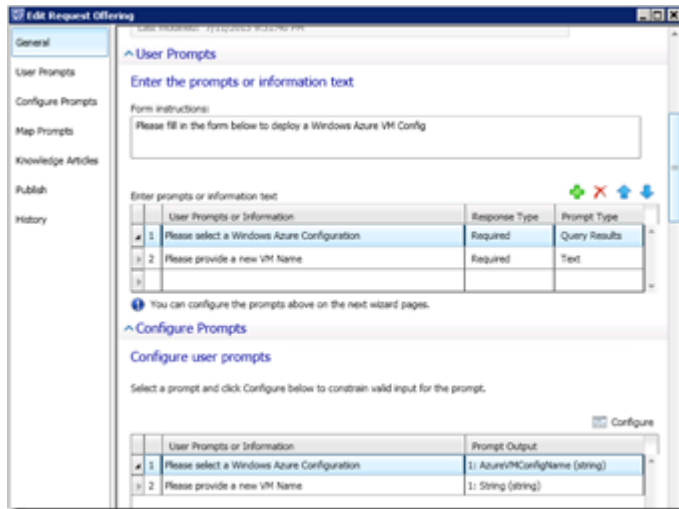
VM
VM Deployment Name: xwdeployment VM Deployment Label: xwdeployment Image Type: PlatformImage
VM Deployment Slot: Production Operating System Type: Windows
VM Computer Name: xwdemovm VM Instance Name: xwdemovm Blob VHD Name: xwdemovm.vhd
VM Instance Size: ExtraSmall VM Source Image: a699494372c04f50bc8f2bb1289d6106_Windows-Server-2012-R2-Preview-201306.01-en-us-127GB.vhd

Endpoint
VM Endpoint Name: xwendpoint VM EndPoint Protocol: TCP
VM Endpoint Local Port: 3389 VM Endpoint Public Port: 3389

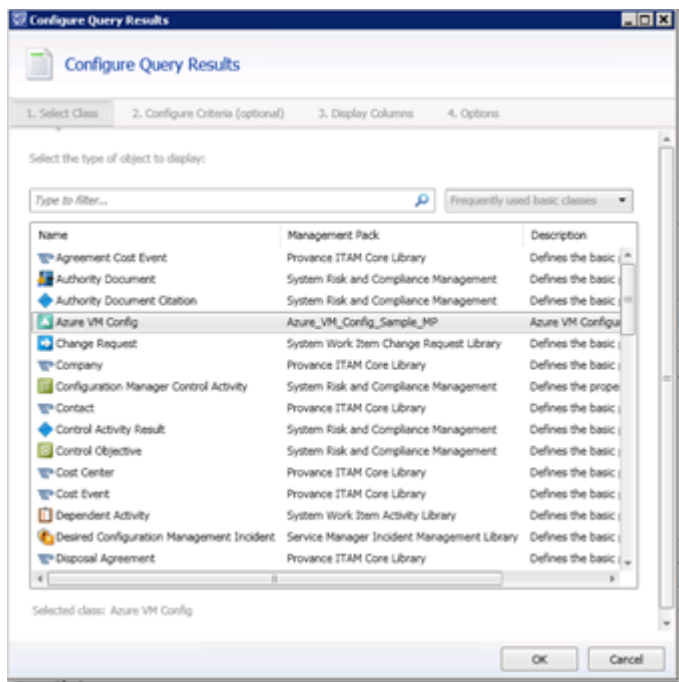
Step 4. Create a Service and a Request Offering for the self-service portal

Now that we have a Windows Azure VM configuration stored into the CMDB the next step is to make a Request and a Service Offering. Since there are a bunch of blog posts out there on how to do that, I won't dive into it right here, but one thing to consider is to determine which values you would like to be "overwritten". You could go ahead and deploy this configuration as is or you could decide which fields you would allow to be set through self-service. To keep it simple and to test drive what I've created, I decided to just allow the self-service user to

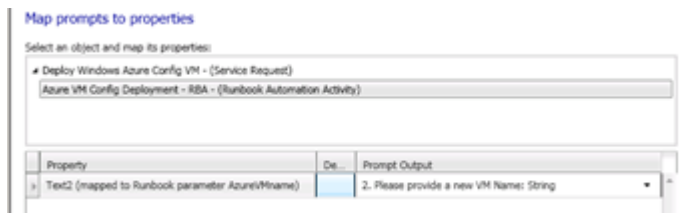
select a Windows Azure configuration and to provide only the Virtual Machine Name. Your Request Offering would then look like this:



Configure your query:



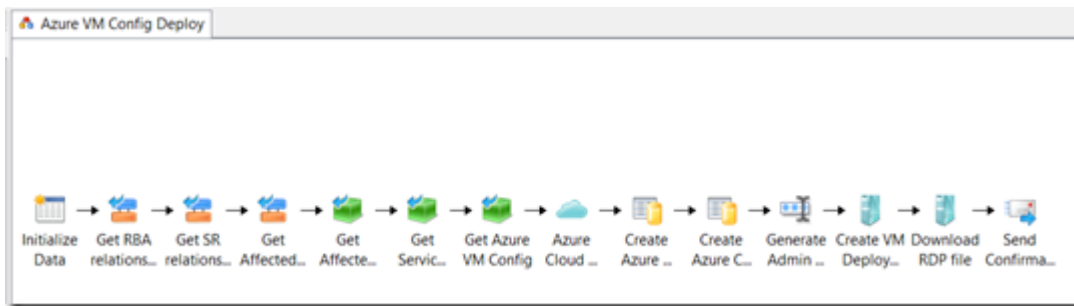
Map your prompt to the "Runbook Automation Activity":



You might wonder why only map the VM Name and not the selected Azure VM Configuration? Well remember the golden rule when you retrieve Service Manager data from Orchestrator. If your data is in the Service Manager CMDB, you don't have to map that and don't put it into the "Initialize Data" activity as a parameter, just use Orchestrator to retrieve that CMDB relationship, that is the beauty of a correlated CMDB. In addition you cannot map a multi-value instance to a string.

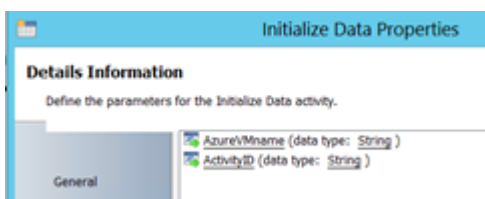
Step 5. Create an Orchestrator runbook, which will be called from Service Manager

Now the Service Manager side is ready, you can leverage Charles Joy's comprehensive Windows Azure runbooks in a number of ways. You can create a "master" runbook to retrieve the Service Manager relationships and invoke several other runbooks from there. To quickly test drive what has been created and to "just deploy a Windows Azure VM" you could also create a simple runbook which looks like this:

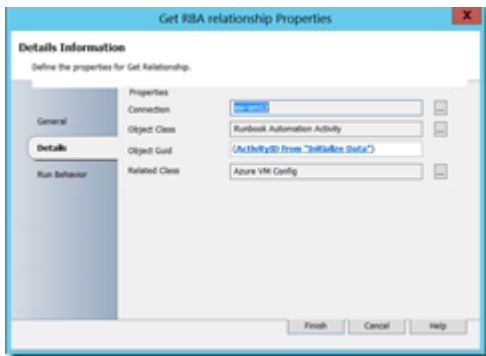


Don't get intimidated because of the number of activities. If you watch closely you see that the first 6 activities – after the "Initialize Data" activity – are all about retrieving the Service Manager CMDB relationships. You actually only need 4 Windows Azure activities to deploy a VM, including the creation of a Cloud service and storage. The rest of those are all meant to impress whoever you would like to impress and demonstrate the flexibility and power of System Center.

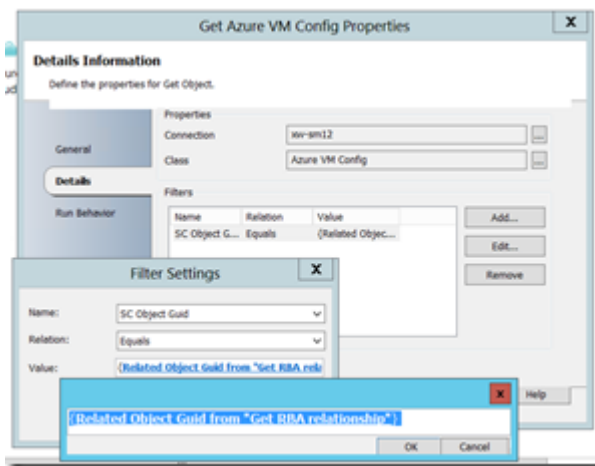
The Initialize Data activity only contains, besides an identifier, the AzureVMname in my simple test scenario:



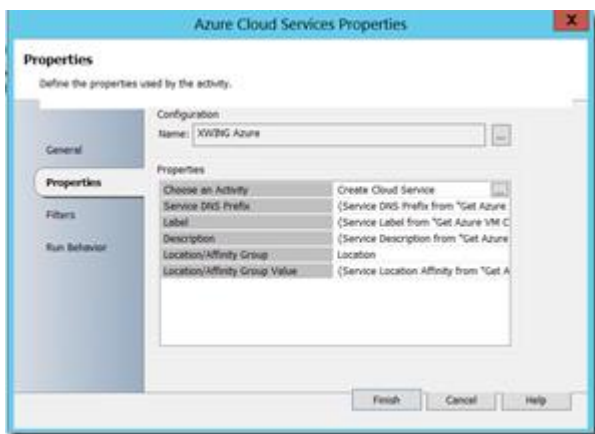
I'm using the standard Windows Azure Orchestrator activities which you need to populate with fields coming from the Service Manager CMDB. To do that you just retrieve the relationship one time where the "related class" is your new configuration item class:



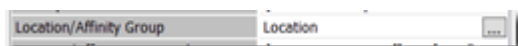
Set your filter settings as follow and you're done:



Now configure all the activities so that all fields come from the data bus "Get Object" activity (called "Get Azure VM Config" in my example)

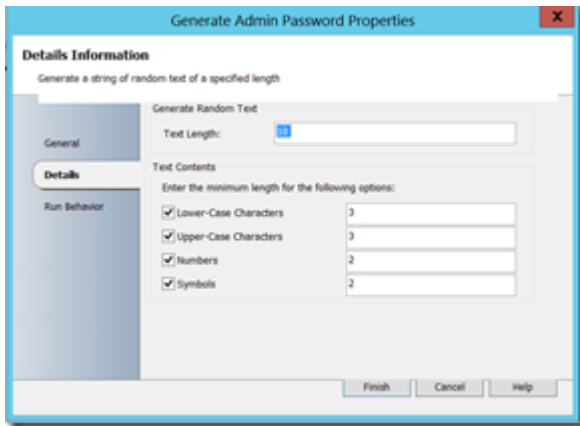


You will notice that some fields cannot use a data bus value like this one:



Since I'm anticipating for Windows Azure PowerShell usage, I decided to keep those fields in the config, although you can't use them in the standard Windows Azure activities.

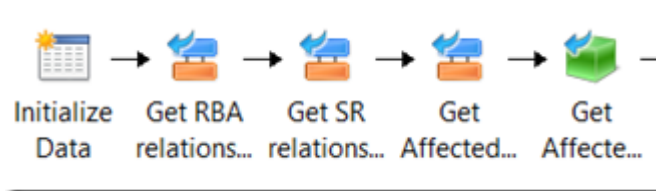
Because I don't like to store passwords in a configuration - which I think is a bad practice - I've added a "Generate Admin Password" activity so that you can decide how complex your password needs to be:



The downside is that if you don't have proper notification or registration in place, you will end up with a deployed VM which you cannot RDP into because of the automated password generation, but hey, good security has its price

To have notification in place which not only sends confirmation to the requesting user - in Service Manager terminology called the "affected user" - but also sends the generated password, I've added a "Send Email" activity. In here you can add data bus values like AzureVMname and password.

For the email to be sent to the "affected user" - so the user who has requested the VM - you need to use some get relationship activities to get that user (Get SR relationship, Get Affected User Relationship, Get Affected User):



If you want to create a really fancy HTML email with nice formatting and colors, just create your email in Word and save as HTML. Then cut and paste the HTML code in the message area of the "send email" activity and pick your fields where you want Orchestrator data bus values to appear, like in the example below.

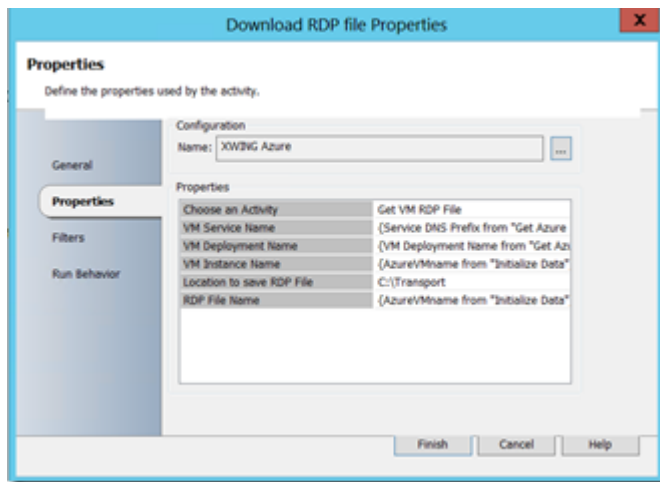
Snippet from the send email activity (using HTML for fancy formatting):

```

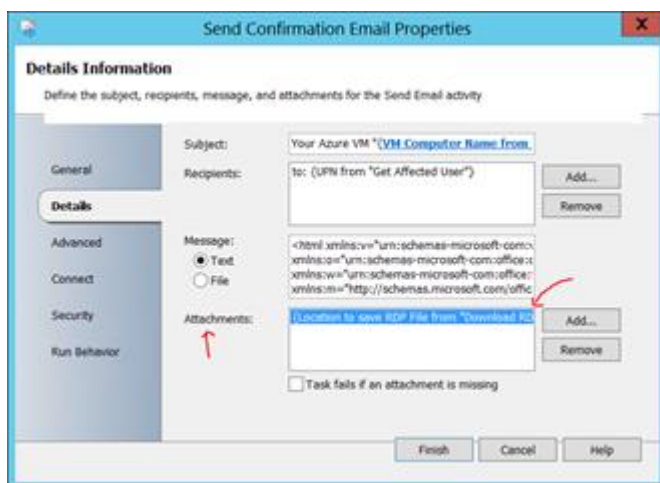
<p class=MsoListParagraph-l1 style="margin-left: 0.5in">Virtual <span style="font-size: 10pt"></span></p>
<p class=MsoListParagraph-l1 style="margin-left: 0.5in"><span style="font-size: 10pt"></span></p>
<p class=MsoListParagraph-l1 style="margin-left: 0.5in">Administrator <span style="font-size: 10pt"></span></p>

```

Let's do one more fancy thing and that is to add the RDP file as an attachment to the email so that your user just has to open the RDP file to connect to the new Windows Azure VM, isn't it cool that we have a standard Windows Azure cascading activity for that?:



Add it to the email and we're done:



Step 6. Deploy a Windows Azure VM through the self-service portal

Now that we're all set up, it's time to test drive!

Let's start with the Service Manager self-service portal (assuming that you have at least 1 Azure VM Config entry):

Deploy Windows Azure Config VM

Please fill in the form below to deploy a Windows Azure VM Config

Please select a Windows Azure Configuration

Search for instances

Azure VM Config Name
<input checked="" type="checkbox"/> Gold

↓

1 object selected (out of 1). 28

Please provide a new VM Name

You can have your users look at the “Gold” configuration by clicking on it:

28

Details

Property	Type	Value
Azure VM Config (27 items)		
Service Location Affinity	enum	West Europe
Service Description	string	my demo
Service Label	string	xwservice01
Service DNS Prefix	string	xwservice01
Storage Account Name	string	xwstorageaccount
Storage Account Description	string	my demo
Storage Account Label	string	xwservicestorage
Storage Container Name	string	xwservicestorage
VM Computer Name	string	xwdemovm
VM Instance Name	string	xwdemovm
Blob VHD Name	string	xwdemovm.vhd
VM Endpoint Name	string	xwendpoint
VM Source Image Name	enum	a699494373c04fc0bc8f2bb1389d6106__Windows-Server-2012-R2-Preview-201306.01-en-us-127GB.vhd
VM Deployment Name	string	xwdeployment
VM Endpoint Protocol	enum	TCP
VM Endpoint Public Port	enum	3389
VM Endpoint Local Port	enum	3389

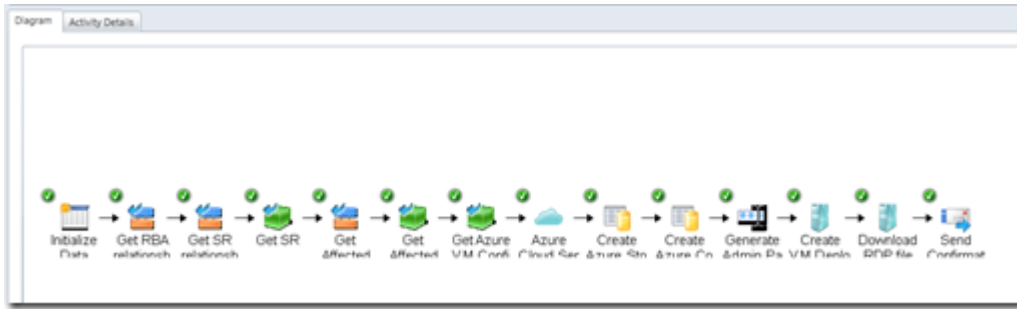
Let's submit the Service Request:

All Open Service Requests 1

Filter

ID	Title	Owner	Status	Priority
SR1654	Deploy Windows Azure Config VM		In Progress	Medium

Orchestrator runbook has successfully run:



Checking the Windows Azure portal, looks good:

NAME	TYPE	STATUS	SUBSCRIPTION	LOCATION
xwingstorage2	Storage Account	✓ Online	Windows Azure MSDN ...	West Europe
xinstorageaccount	Storage Account	✓ Online	Windows Azure MSDN ...	West Europe
TianderVM01	Virtual machine	✓ Running	Windows Azure MSDN ...	West Europe
xservice01	Cloud service	✓ Running	Windows Azure MSDN ...	West Europe
xwing	Web Site	✓ Running	Windows Azure MSDN ...	West Europe

Got a nice email confirmation (*notice the attachment, it's the RDP file*):

From: SM12_Workflow
 To: Admin Dude
 Cc:
 Subject: Your Azure VM "TianderVM01" has been created

Message TianderVM01.rdp (328 B)

Dear Admin Dude,

We have successfully created a new Azure Virtual Machine with the following details:

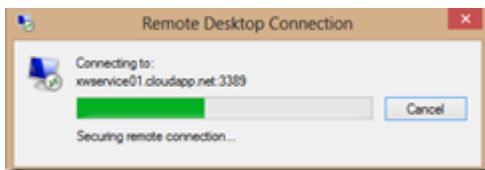
Virtual Machine Name: TianderVM01
Administrator password: \$R3iB3yb'K

Please use the attached RDP file to connect to your new VM.

To enter a new Service Request, please use this link:
[Service Manager Self-Service Portal](#)

Kind regards,
Global IT Helpdesk

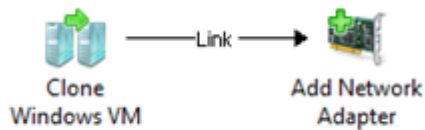
Open the RDP file:



Logged on to our new Windows Azure VM!:



b) Creating runbook that automates a process relating to VMware vSphere.



A whole new set of tools for vSphere has been released for Orchestrator 2012 R2. Over 30 Activities to build out incredible automation Runbooks.

System Center 2012 R2 Integration Pack for VMware vSphere
<http://www.microsoft.com/en-us/download/details.aspx?id=40874>

Feature Summary

The Integration Pack includes the following activities:

- Add Network Adapter
- Add VM Disk
- Clone Linux VM
- Clone Windows VM
- Create VM
- Customize VM
- Delete VM
- Get Cluster Properties
- Get Datastore Capacity
- Get Hosts
- Get Resource Pool Runtime Info
- Get Resource Pools
- Get VM List
- Get VM Properties
- Get VM Status
- Migrate VM
- Move VM
- Reconfigure VM
- Reset VM
- Revert VM Snapshot
- Set Guest Info Variables
- Set VM CD/DVD to ISO Image
- Set VM Networks
- Start VM
- Stop VM
- Suspend VM
- Take VM Snapshot
- Maintenance Mode
- Get Host Properties
- Get Host Datastores

Configuration Screen

Add Configuration

Name:

Type: ...

Properties

Server	<input type="text"/>
User	<input type="text"/>
Password	<input type="text"/>
SSL	True
Port	<input type="text"/>
Webservice Timeout	<input type="text"/>

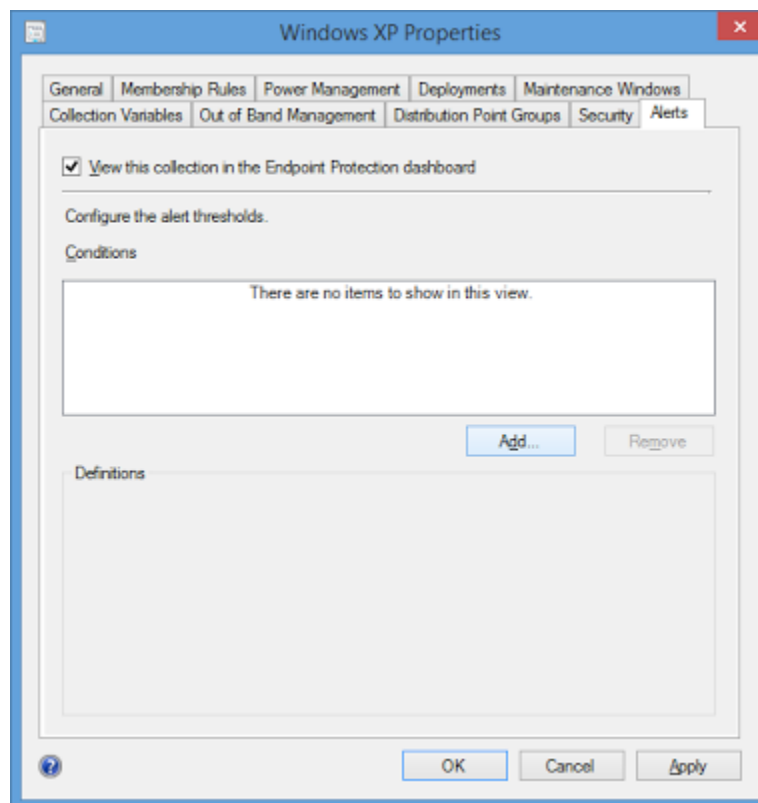
Sign: _____

Practical No 8: Using Configuration Manager 2012 for managing and maintaining.

a) Setting up an alert for compliance.

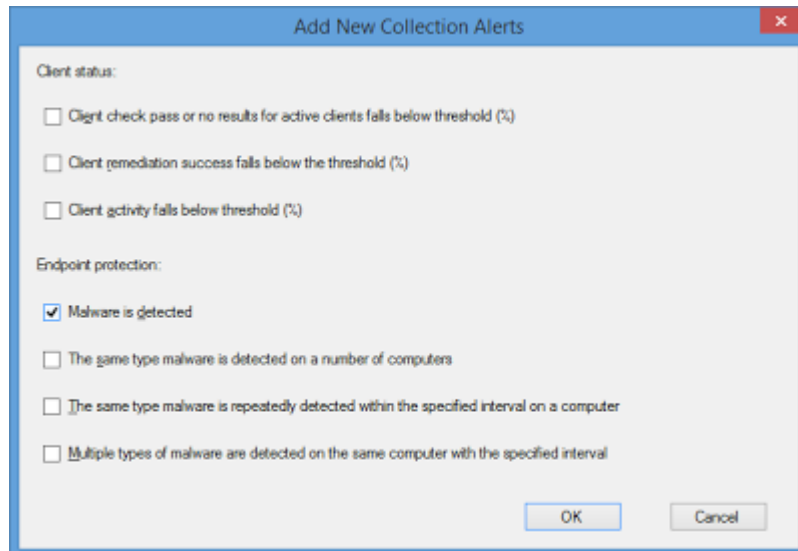
Load up your SCCM console. Once loaded go to 'Assets and Compliance' and go to 'Device Collections'. Select a collection you want to set an alert on and right click it then select 'Properties'.

Along the top of the window select 'Alerts'. Tick the 'View this collection...' tick box and then select 'Add'.



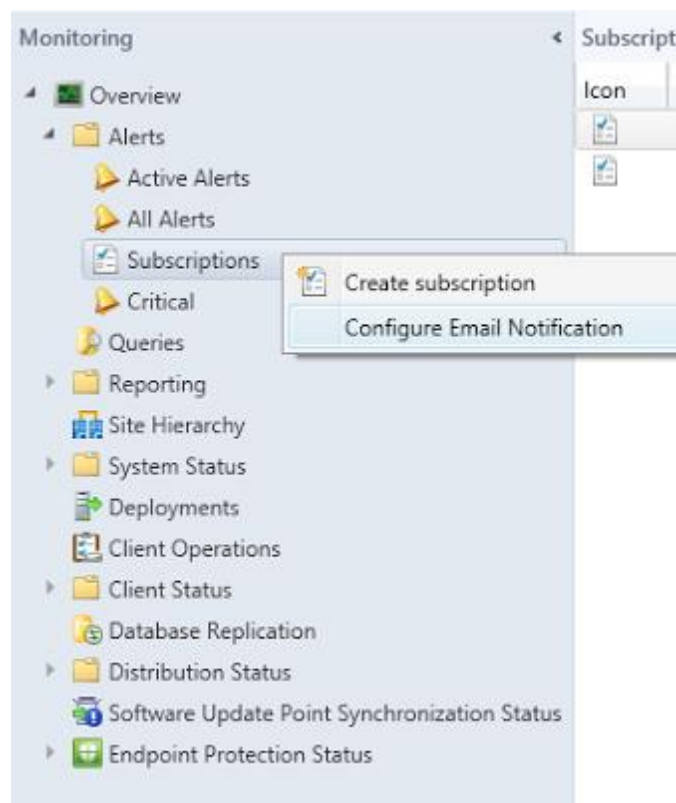
Alerts

On the next screen you will see lots of boxes. Here you can pick and choose what you would like SCCM to alert you about. As we are only doing a malware detection alert only that box will be checked.



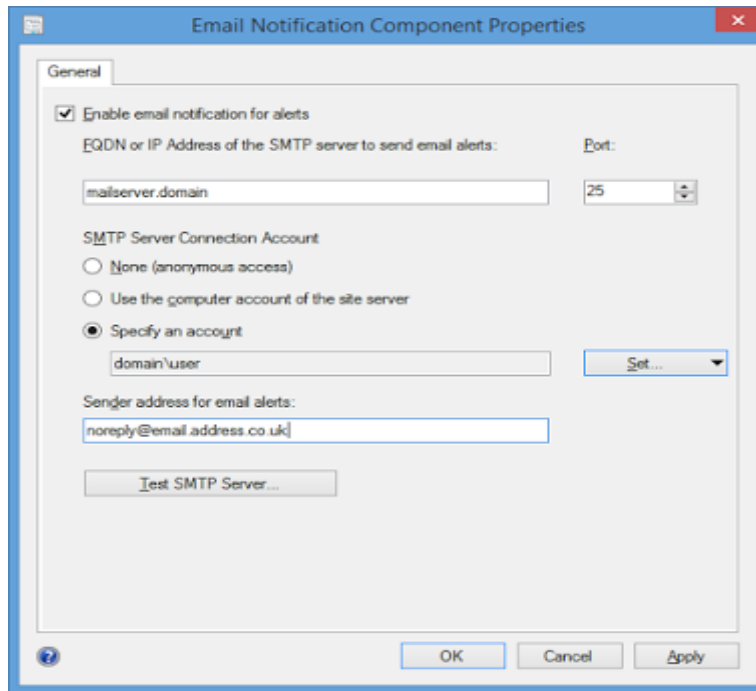
Alert Choices

Once selected make your way back to the main SCCM window. Next go to 'Monitoring' on the left hand side then expand 'Alerts'. In here find 'Subscriptions', right click it and select 'Configure Email Notification'.



Configure Email

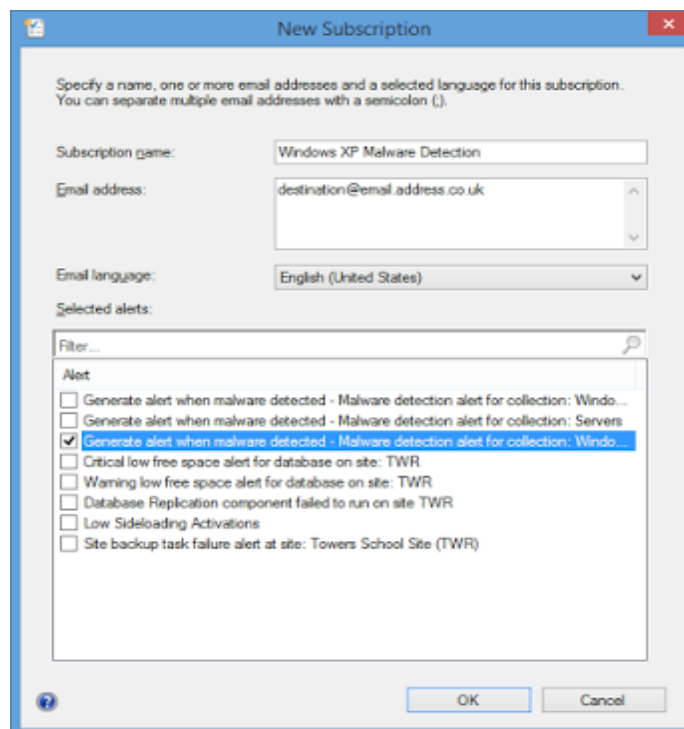
On the next window tick 'Enable email notifications for alerts'. In the field below put in the FQDN of your mail server. You will then want to select 'Specify an account' and use an account that has access to connect to the mail server. Lastly set an email address the alerts will be sent from.



Email Notification Settings

Once done run a test and if that's successful click 'OK'.

Next go back to 'Subscriptions', right click it and this time select 'Create Subscription'. On the next window you will need to give the subscription a name and set an email address that SCCM will send the alerts to. At the bottom of the window you will see some tick boxes. These are default ones already created as well as any you have created. Find the one created earlier and tick it then when all done click "OK".

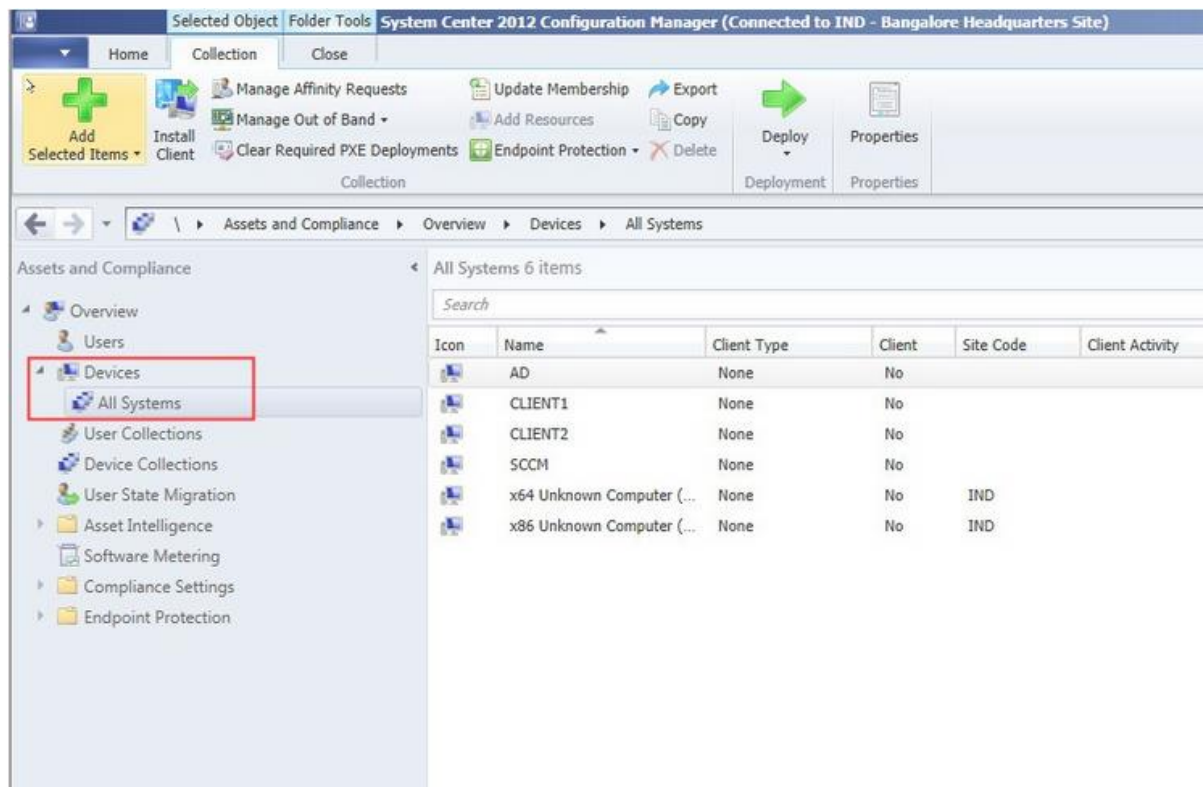


Subscription Settings

And that's all there is to it. If it's all successful you should now start receiving emails with information about any malware detected on your system as well as alerts in Endpoint Monitoring on the SCCM console.

b) Connecting devices and monitoring its health.

- Run the full discovery for the Active directory users, system and groups, wait for few minutes while the discovery cycle is complete.
- Click on Assets and compliance, click on Devices and click on All Systems.



c) Managing users and user groups hierarchy.

- Run the full discovery for the Active directory users, system and groups, wait for few minutes while the discovery cycle is complete.
- Click on All Users and Users Groups

System Center 2012 Configuration Manager (Connected to IND - Bangalore Headquarters Site)

Home | Collection | Close

Add Selected Items | Manage Affinity Requests | Update Membership | Add Resources | Export | Copy | Delete | Deploy | Properties

Assets and Compliance > Overview > Users > All Users and User Groups

Assets and Compliance < All Users and User Groups 22 items

Search

Icon	Name	Domain	Resource Type
	PRAJWAL\Administrator (Administrat...	PRAJWAL	User
	PRAJWAL\Allowed RODC Password...	PRAJWAL	User Group
	PRAJWAL\Cert Publishers	PRAJWAL	User Group
	PRAJWAL\Denied RODC Password R...	PRAJWAL	User Group
	PRAJWAL\DHCP Administrators	PRAJWAL	User Group
	PRAJWAL\DHCP Users	PRAJWAL	User Group
	PRAJWAL\DnsAdmins	PRAJWAL	User Group
	PRAJWAL\DnsUpdateProxy	PRAJWAL	User Group
	PRAJWAL\Domain Admins	PRAJWAL	User Group
	PRAJWAL\Domain Computers	PRAJWAL	User Group
	PRAJWAL\Domain Controllers	PRAJWAL	User Group
	PRAJWAL\Domain Guests	PRAJWAL	User Group
	PRAJWAL\Domain Users	PRAJWAL	User Group
	PRAJWAL\Enterprise Admins	PRAJWAL	User Group

Sign: _____