

© 2016 Microsoft Corporation. All rights reserved.

Microsoft Proprietary and Confidential Information

This training package content is proprietary and confidential, and is intended only for users described in the training materials. Some elements of this document are subject to change. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

This content and information is provided to you under a Non-Disclosure Agreement and cannot be distributed. Copying or disclosing all or any portion of the content and/or information included in this package is strictly prohibited. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in, or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft and the Microsoft products and services listed are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Participant Guide

WorkShopPlus

Azure Site Recovery

Module 4 Lab: VMware Azure Portal

Table of Contents

[Lab VMWare ASR Scenario 3](#_Toc463465331)

[Overview 3](#_Toc463465332)

[Exercise 1: Initial Configuration of Process/Configuration Server 5](#_Toc463465333)

[Exercise 2: Create your Azure Site Recovery vault in your subscription 8](#_Toc463465334)

[Exercise 3: Getting started with your Azure Site Recovery vault 10](#_Toc463465335)

[Exercise 4: Configure Configuration Server Accounts 14](#_Toc463465336)

[Exercise 5: Identify your Recovery Services Vault 18](#_Toc463465337)

[Exercise 6: Add vCenter Server/ESXi Host 20](#_Toc463465338)

[Exercise 7: Create a Protection Group 23](#_Toc463465339)

[Exercise 8: Enable Protection on a VMware VM 26](#_Toc463465340)

[Exercise 9: Create a Recovery Plan 30](#_Toc463465341)

[Exercise 10: Recover a VM in Azure 32](#_Toc463465342)

## Lab VMWare ASR Scenario

|  |  |
| --- | --- |
|  |  |
|  | The time to complete this module, including exercises, is 240 minutes. |
|  | The key takeaways from this lab are:   * Infrastructure requirements for VMWare to Azure VM protection * How to create a Protection group to protect your VM and how to enable protection for your VMware virtual machines. * How to failover virtual machines from VMware to Azure using Recovery Plans |
|  |  |

### Overview

#### As Fabric admins of Contoso, you have decided to enable protection for various applications of your datacenters. You are the owner of a datacenter running some non-virtualized workloads (Physical machines) and a large part virtualized using the Hyper-V and VMware stacks. Since you have SLAs for different applications, you plan to protect them differently.

#### Key Components in VMWare to Azure Protection Using Azure Site Recovery

**PROCESS/CONFIGURATION SERVER**: The management server setup as an on premises physical or virtual machine that acts as command and control for all operations. This is the first server that will be deployed by a customer to try out VMware and Physical DR to Azure scenarios. This server needs to be “registered” with the ASR Vault. All management actions originate or flow through this server.

**MASTER TARGET SERVER:** The server which stores and writes all the replicated data. This server is deployed in the customer’s azure subscription. This server is “registered” to an Azure Vault as well.

#### Prerequisites

* Internet access
* Azure Subscription and an Operations Management Suite subscription already setup and configured

#### Before you begin

* Ensure you have received the credentials to an Azure subscription (Azure Pass) to use for this Lab. Validate that you are able to log in to the Azure management portal (<https://portal.azure.com> ) using the credentials provided to you.
* Each participant will be provided with a dedicated virtual environment, that comprises of one VMware ESXi host with 1 virtual machine on it that is a source server for you to protect. Each participant also has a machine (ConfigurationServer) that will become your Process/Configuration Server and also provide access the vSphere client to access the VMware virtual machine.

#### Virtual machine technology

This lab is completed using virtual machines. To log on to the virtual machines, press CTRL+ALT+END and enter your logon credentials. Alternatively, you can use the Commands menu in the Learn On Demand Systems (LODS) console.

#### Computers in these labs

This lab uses computers as described in the following table.

|  |  |  |
| --- | --- | --- |
| Computer | Role | Configuration |
| ESXi-HOL | VMware ESXi Hypervisor | Virtual Machine Host |
| ConfigurationServer | Windows Server 2012 R2 | Machine to install on-premises ASR components and access Azure from. |

* All user accounts in this lab use the password **Password~1 (NOTE this is the tilde character not a hyphen)**

### Exercise 1: Initial Configuration of Process/Configuration Server

|  |  |
| --- | --- |
|  | The time to complete this exercise is 10 minutes. |
|  | The key takeaways from this exercise are:   * None |
|  |  |

#### Setup the Process/Configuration Server

1. Ensure that the ESXi-HOL host has been fully configured. You can verify this by connecting to ESXi-HOL and then verifying that you can see “Download tools to manage this host from”:

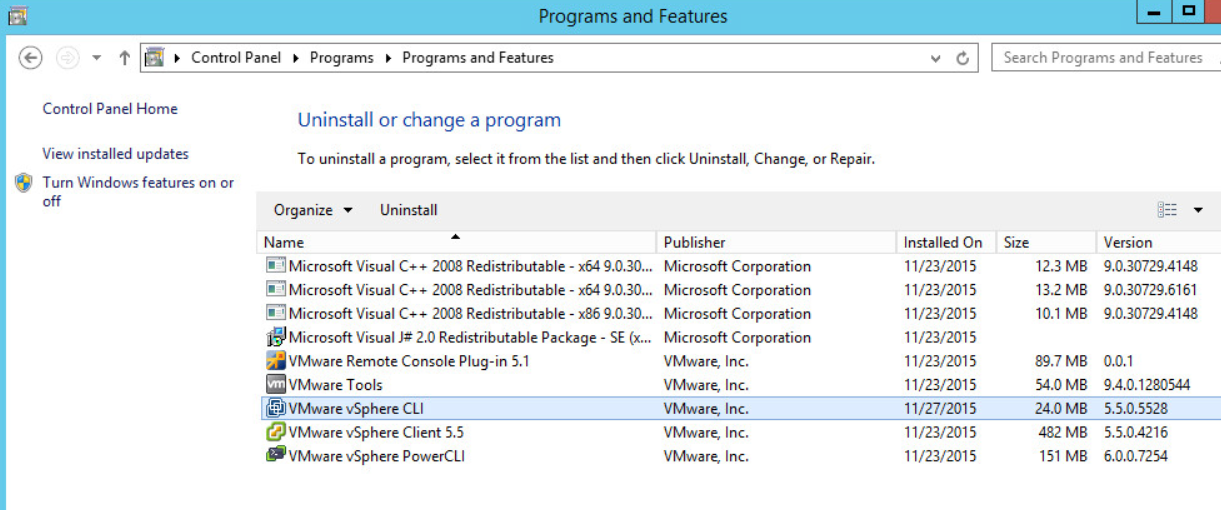


The *ASR Unified Installer* software must first be installed on the *Configuration Server* VM. We will do this by downloading that software from Azure. But there are some pre-requisites that must be addressed first.

Please confirm by checking the Programs and Features object from the Windows Control Panel that the following items are installed.

VMware vSphere CLI version 5.5  
VMware vSphere Client 5.5  
VMware vSphere PowerCLI 6.0

By resizing the *Programs and Features* window the *Version* column will become visible, allowing you to verify the version.



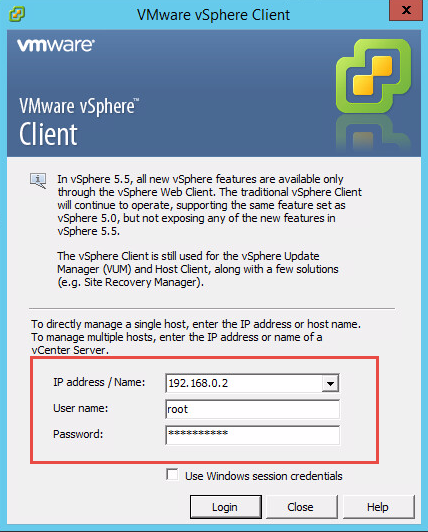
If these items are not correctly installed, you can find the installation files in the Downloads folder for the logged on user. If you have questions on how to install them, please ask your instructor.

#### Confirm the presence of the VMware VM to be protected

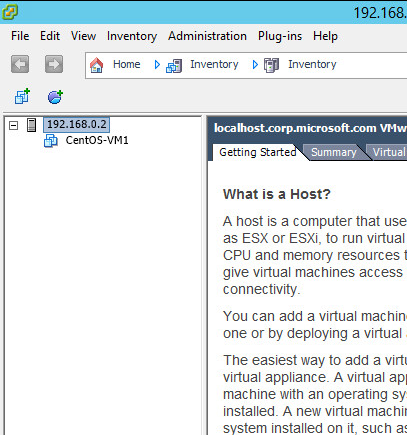
1. The machine we are planning to protect in this lab is a VM on your ESXi host.
2. Log on to the ConfigurationServer machine and open the VMware vSphere Console on the desktop
3. Use the following credentials to log into vSphere:

**Username:** root

**Password:** Password~1



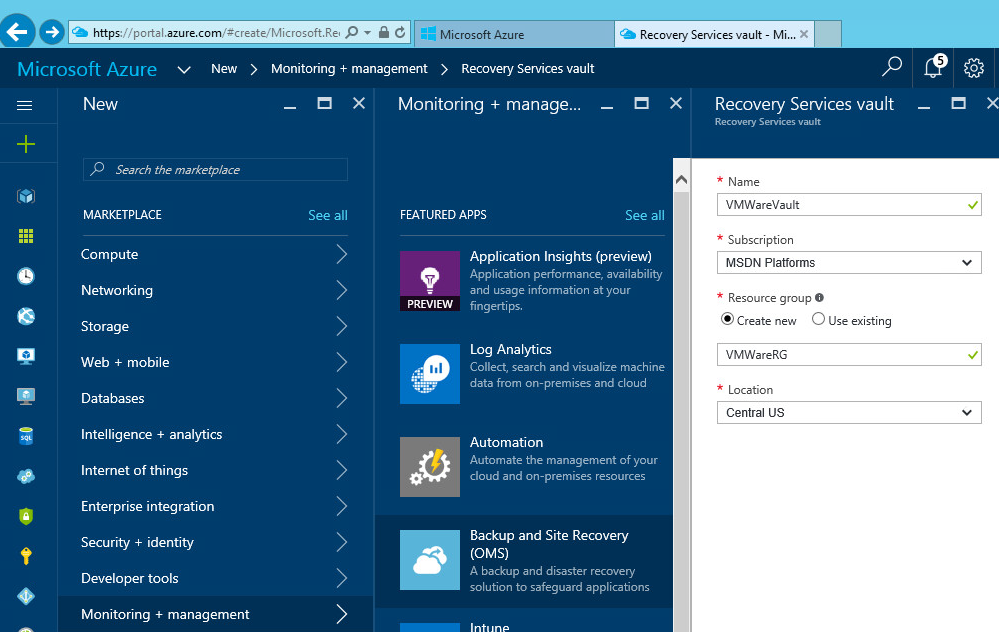
1. In the vSphere client, **expand** the 192.168.0.2 tree (on the left-hand side of the console) and make sure that you can see CentOS-VM1.

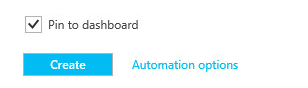


### Exercise 2: Create your Azure Site Recovery vault in your subscription

|  |  |
| --- | --- |
|  | The time to complete this exercise is 10 minutes. |
|  | The key takeaways from this exercise are:   * How to create a Site Recovery Vault |

#### Create your Vault

1. Log onto *ConfigurationServer*.
2. From *ConfigurationServer*, log on to the Microsoft Azure portal [http://portal.azure.com/](http://portal.windowsazure.com/) using your Azure portal credentials.
3. Click *New* *> Monitoring + Management > Backup and Site Recovery (OMS)*
4. Create a new vault in named *VMwareVault* and create a resource group called *VMWareRG* in the Central US location.



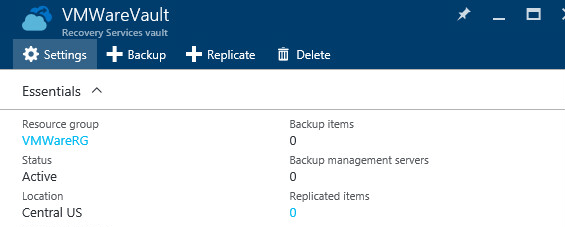
1. For easier navigation, check the *Pin to dashboard* option as this will allow you to navigate to your vault from the landing page.   
   Click **Create** to create the vault based on the specified settings.

### Exercise 3: Getting started with your Azure Site Recovery vault

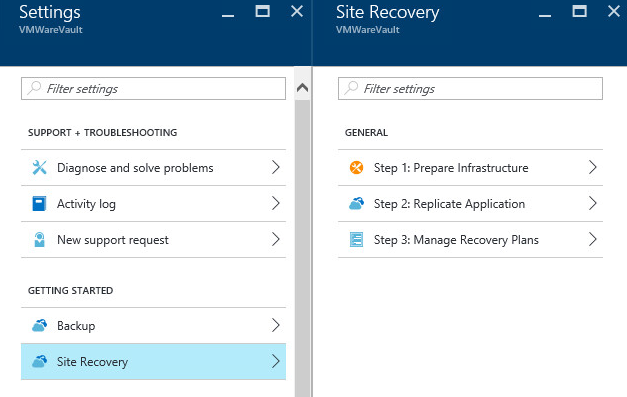
After the vault has been created, you can use the *Getting Started* experience to configure your vault for it’s intended purpose.

#### Setting the Protection Goal

1. Bring up the vault that was created in the previous exercise and click *Settings*



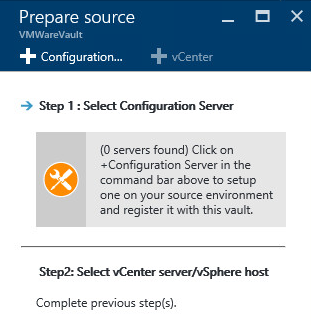
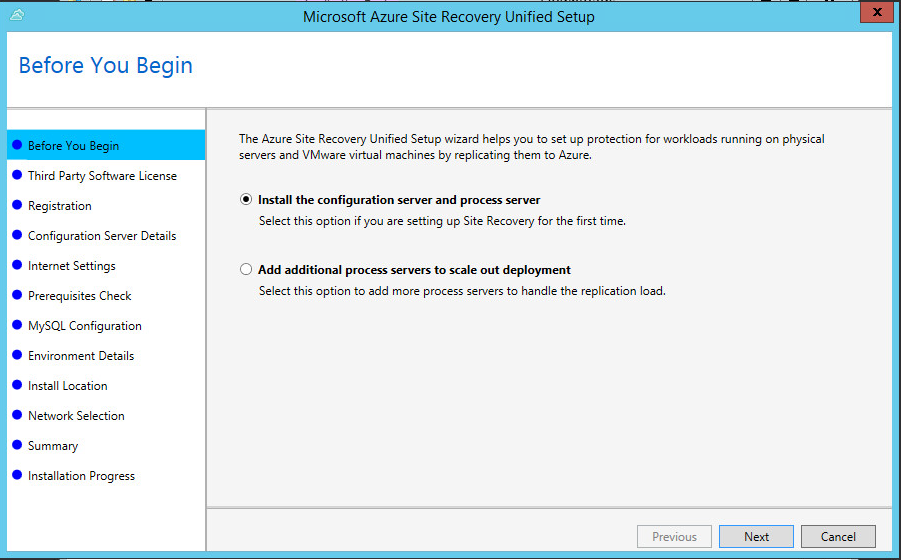
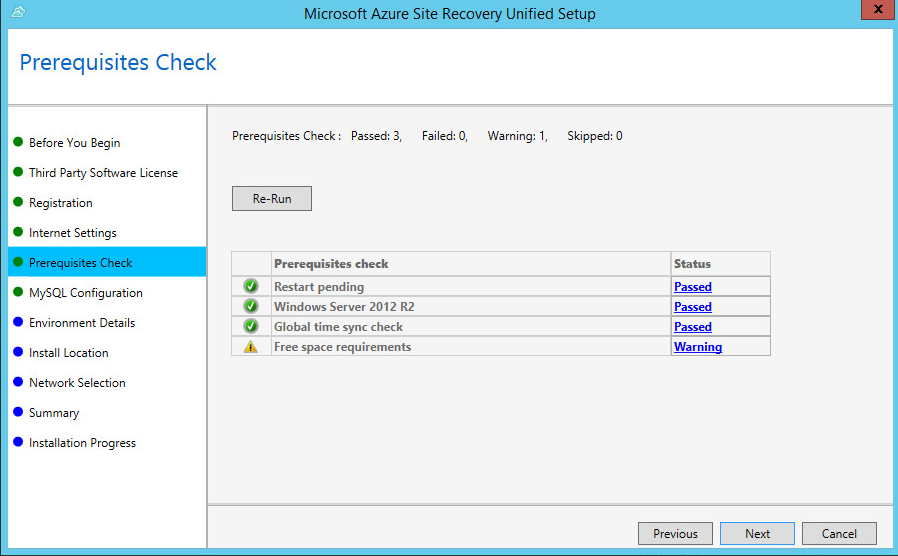
1. The settings pane lists several steps, select *Step 1: Prepare Infrastructure*

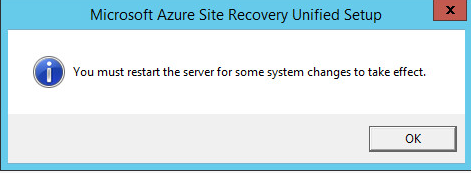


1. As the protection goal, select *‘To Azure’* and *‘Yes, with VMWare vSphere Hypervisor’* and click ‘*OK’*.  
   This will complete the step ‘Protection Goal’ and open up the next step, ‘Source’.

#### Setting up the source environment

As part of setting up the source environment, a Configuration Server is needed. In this lab environment, the machine that is currently being worked on will function as the Configuration Server.

1. In the ‘Prepare Source’ tab, click the ‘+Configuration Server’ option.  
     
   
2. The ‘Register your Configuration Server’ pane opens. Download the Unified Setup files that are being offered in step 3.
3. Click the ‘Download’ button listed in step 4 to download the registration key. A key will be generated. This file will have a .VaultCredentials extension. When the option is provided, use Save to store the file on the machine.
4. Run the Unified Setup (MicrosoftAzureSiteRecoveryUnifiedSetup.exe) to install the Configuration Server.
5. When the setup has launched, select the *‘Install the configuration server and process server’* option.This will be the default selection. Click *Next*.  
     
   
6. The *‘I Accept the third party license agreement’* will have to be checked to be able to download the MySQL setup files and to be able to continue with the setup.
7. Use the *Browse* button to locate the Site Recovery Registration key that was downloaded in step c. Click ‘*Next’*.
8. The Internet connection settings can be left to default setting, click ‘*Next’*.
9. A Prerequisites check will be done, which will flag a warning for the ‘Free space requirements’. In this lab setup, this is to be expected. Click ‘*Next’*.  
   
10. On the ‘MySQL Configuration’ screen, create credentials that meet the criteria listed and click ‘*Next*’
11. Select ‘Yes’ on the ‘Environment Details’ screen to indicate this setup will be used with VMWare virtual machines.  
    After selecting ‘Yes’, a check will be done to verify if vSphere PowerCLI 6.0 is present on the machine. In this lab environment that prerequisite is already met and this will be indicated by a green checkbox. Click ‘Next’.
12. The ‘Install Location’ will flag the lack of 600GB of free space. For this lab the warning can be ignored. Click ‘*Next*’
13. On the ‘Network Selection’ screen, leave the default setting and click ‘Next’.
14. From the ‘Installation Progress’ page, review the data and click Install and wait for the products to complete
15. A message will be presented indicating the machine needs to be rebooted. However,  
    **do not reboot the machine at this time**.



1. A Configuration Server Passphrase will be presented in a popup window. Click ‘Yes’ to copy it to the clipboard.
2. To ensure that you will not lose that Passphrase, click the Start button and open Notepad. Paste the Passphrase from the clipboard to Notepad, and save the file

### Exercise 4: Configure Configuration Server Accounts

|  |  |
| --- | --- |
|  | The time to complete this exercise is 15 minutes. |
|  | The key takeaways from this exercise are:   * Configuring the Configuration Server Accounts which will be used by ASR to communicate with your VMware and virtual machine infrastructure. |
|  |  |

As part of Exercise 2, you have already created a Recovery service vault named VMwareVault in your Azure subscription.

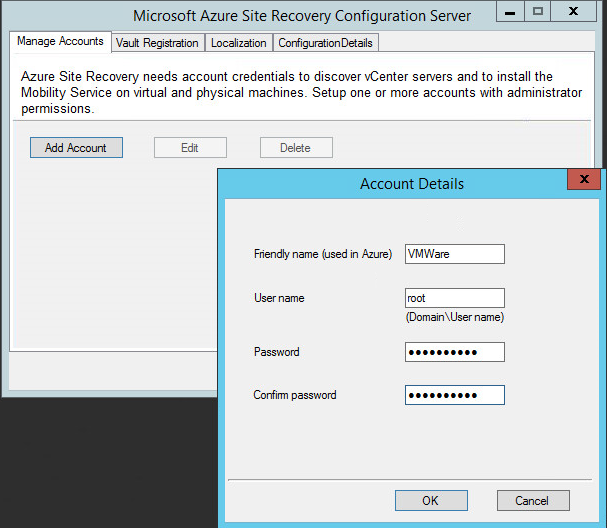
#### Adding the VMWare account

The next step is to define an account on the VMware server that will be able to connect to and process the replication of the VMs on the server.

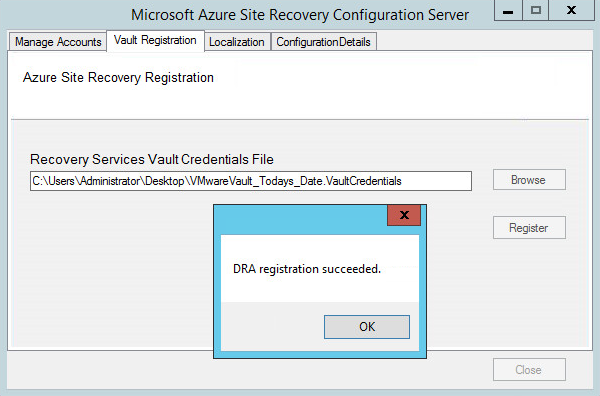
For this purpose, we are going to use the *root* account on the VMware server. In an enterprise scenario you would likely create a specific service account for this purpose.

1. Click the Add Account button on the Manage Accounts tab and enter the following data:

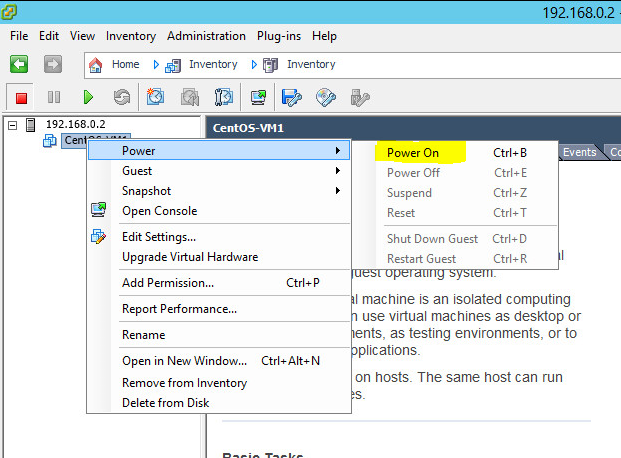
|  |  |  |
| --- | --- | --- |
| **Friendly Name** | **User Name** | **Password** |
| VMware | root | Password~1 |



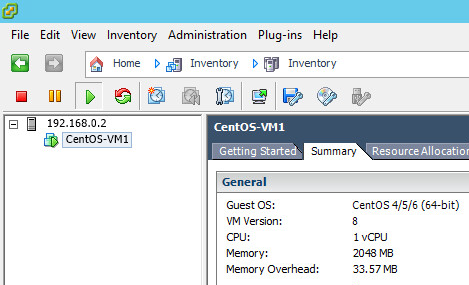
1. Next, **click** on the *Vault Registration Tab*, **Browse** to the desktop and **select** the Vault Registration Key that you downloaded earlier. Click **‘***Register’*.   
   Be patient as the registration process might take a minute or two.
2. When the dialog “DRA registration succeeded.” appears, **click** OK. The account will be displayed, click *Close* to exit the application:



1. This completes the installation of the local Process/Configuration server. The last remaining step is to reboot this server.
2. Click the Start button and then use the Power button in the top right corner to Restart the computer
3. Once the computer restarts, log back in to the server using the lab server credentials.
4. Use the desktop shortcut for the vSphere client to launch it. Log in using the username *root* and the password of *Password~1*. You may see an Evaluation notice. Click OK, this is expected.
5. Click on the plus sign next to the IP address (the VMWare host) in the left hand pane to expand the options underneath.
6. Right-click on the CentOS-VM1 system and choose *Power* and then *Power On* in the sub menu.



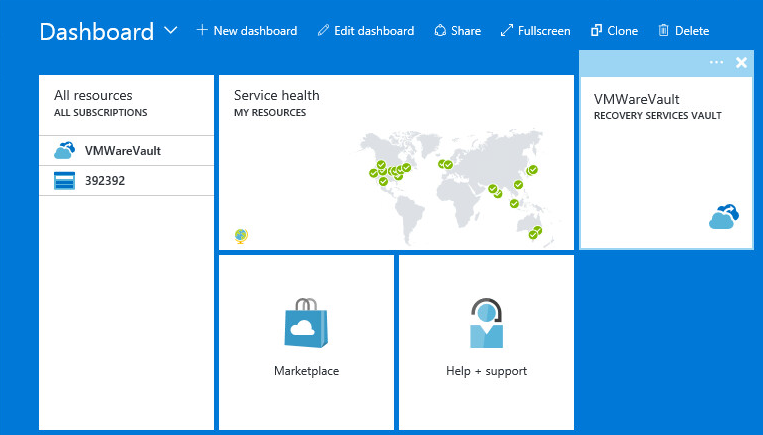
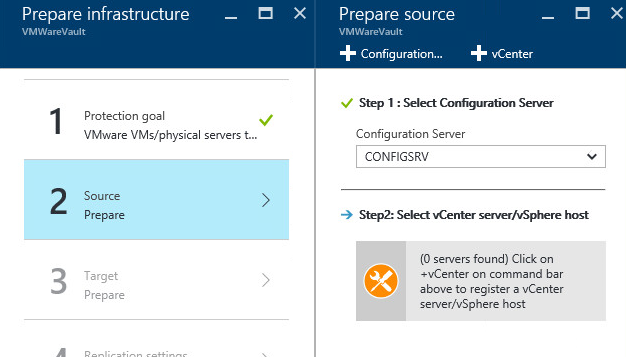
1. Switch to the Summary Tab. You will see a yellow box that is a warning message that requires input from you before the machine will power on properly. The default option is set to *I Copied It*. Leave this option selected and click the *OK* button.
2. The graphic beside the server name should now be a green, right facing triangle indicating the VM is running.



### Exercise 5: Add vCenter Server/ESXi Host

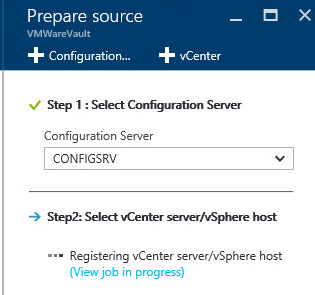
|  |  |
| --- | --- |
|  | The time to complete this exercise is 15 minutes. |
|  | The key takeaways from this exercise are:   * How to add a ESXi host to your Azure Vault. |
|  |  |

#### Add the vCenter Server

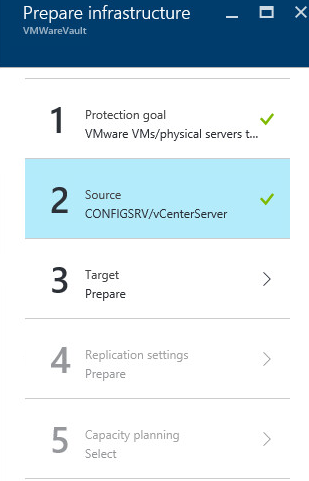
1. From *ConfigurationServer*, log on to the Microsoft Azure portal [http://portal.azure.com/](http://portal.windowsazure.com/) using your Azure portal credentials.
2. Locate your vault and select it. If it was created and ‘pinned’ to the dashboard it will be clearly presented after logging in.  
     
   
3. In the vault, go back to the *Getting Started* experience and go to *Step 2:Source.* At this point, a Configuration Server will be listed. Use the *+Vcenter* to add a VMWare vCenter server.  
     
   
4. In the *Add vCenter* pane, use the following details and click *OK*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **IP Address** | **Port** | **Friendly Name** | **Process Server** | **Account** |
| 192.168.0.2 | 443 | <Your Choice> | Select from list | VMware |

1. A job will be started to add the vCenter server. Wait for this job to complete. The progress of the job can be monitored by clicking the *View job in progress* link



The active job will be presented and will show as *In Progress*. Typically this job will run for several minutes before it will be listed as *Successful.*  
After is is listed as successful, return to the *Getting Started* experience, *Step 2:Source* and click ‘*OK’* to complete the step of adding a vCenter server. This will complete *Step 2:Source* as can be seen by the checkbox.

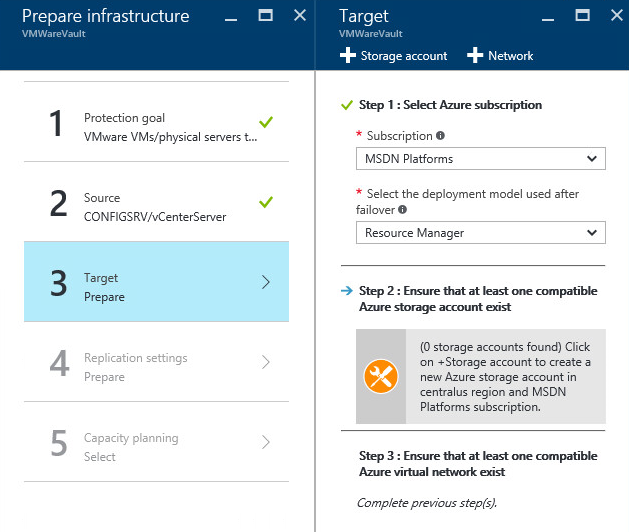


Exercise 6: Setting up the target environment

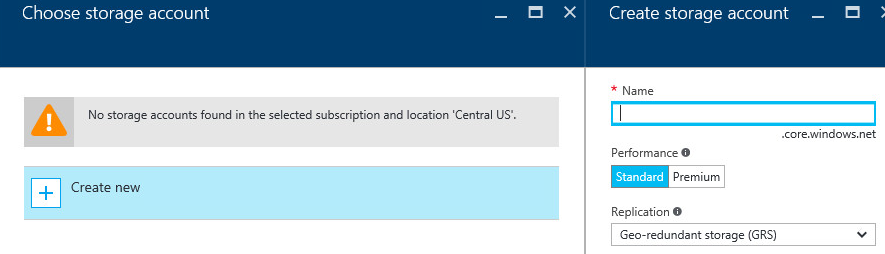
|  |  |
| --- | --- |
|  | The time to complete this exercise is 15 minutes. |
|  | The key takeaways from this exercise are:   * Defining the target environment |
|  |  |

Adding a storage account

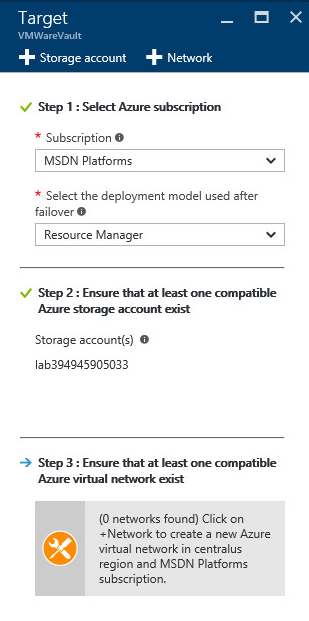
1. In the *Getting Started* Experience, go to *Step 3:Target* and click ‘+Storage Account’

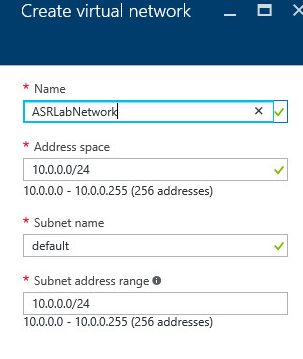


1. Pick a name of your choice for the Storage Account name. Leave the rest of the choices as default and then click ‘*OK’*



Adding an Azure Network

1. After the ‘adding a storage account’ job completes, the screen will return to the wizard. It will list the newly created storage account but will indicate it is still missing the network.   
   Click *+Network* to add an Azure Network  
     
   
2. On the *Create virtual Network* tab, create a new network. For these exercises, there is no need for a specific network configuration.

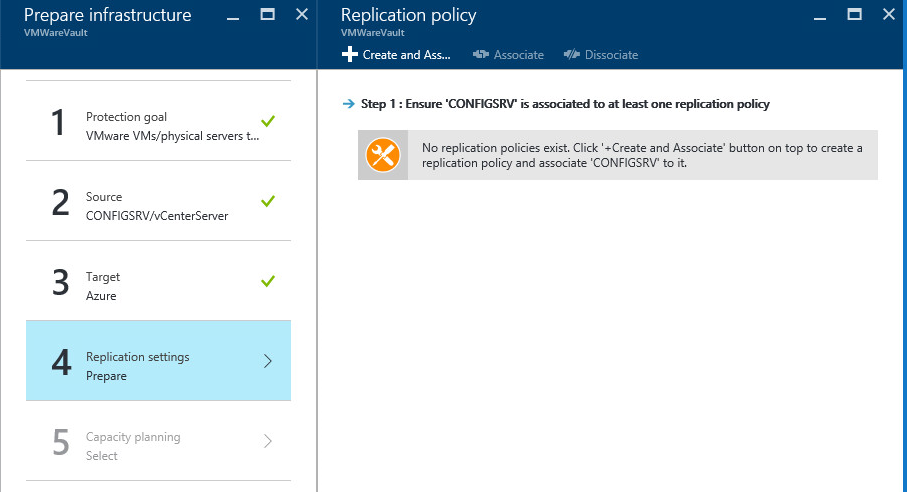


Exercise 7: Setting up replication

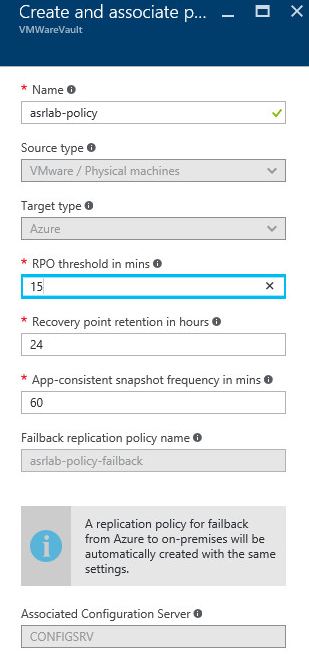
|  |  |
| --- | --- |
|  | The time to complete this exercise is 60 minutes. |
|  | The key takeaways from this exercise are:   * How to enable protection on VMware VMs to Azure. |
|  |  |

Creating a replication policy

1. Go back to the *Getting Started* experience. Steps 1,2 and 3 will be marked completed as indicated by the checkbox.   
   Select Step *4:Replication Settings.* Click *+Create and Associate policy* located on the top of the Replication Policy pane



1. On the *Create and Associate Policy* pane, provide a name for the policy, define the RPO Threshold for alerting purposes, the Recovery point retention and the App-consistent snapshot frequency.



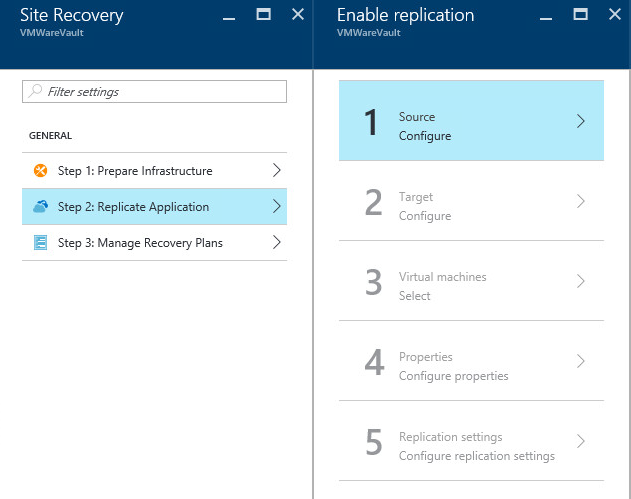
A failback policy will automatically be created, the name will be the same as the name provided for the policy that was just created, but with *-failback* added to the end.

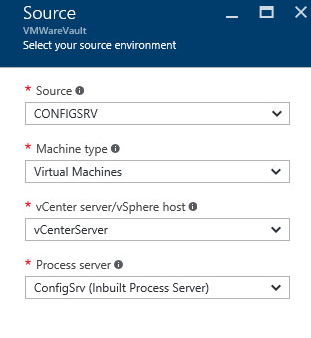
Click ‘*OK’*

Capacity Planning

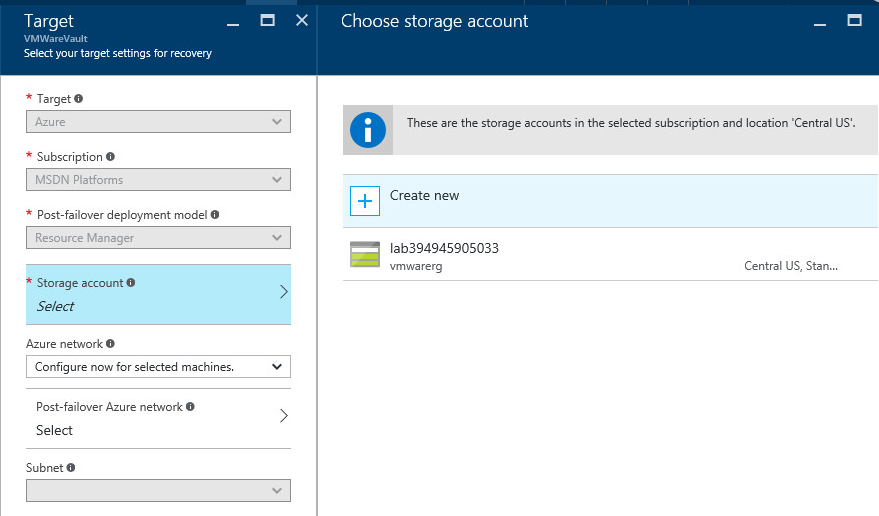
1. After the policy has been created, all the infrastructure components needed have been defined. An important part of an Azure Site Recovery setup is capacity planning. As part of the *Getting Started* experience, a link is provided to the Capacity Planner tool. This tool will allow you to estimate network bandwidth,storage and other requirements.   
   For this lab, the capacity planner will not be used. Select *‘yes,I have done it’* and click *OK.*
2. The pane will be closed and the *Prepare Infrastructure* pane will now list all five steps with a checkmark. Click *OK*.

Replicating applications

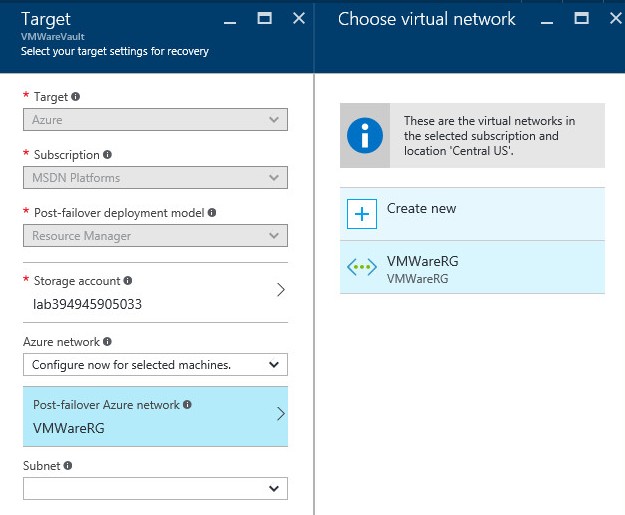
1. In the VMWare Vault pane, select Step 2:Replicate Application  
     
   
2. On the Source pane, use the dropdown box to select a Process Server, only one will be listed. Click OK.

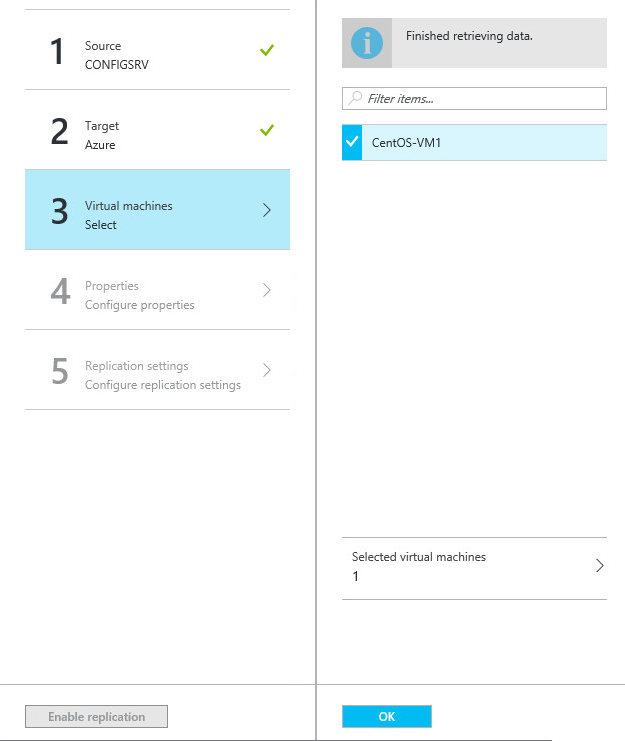


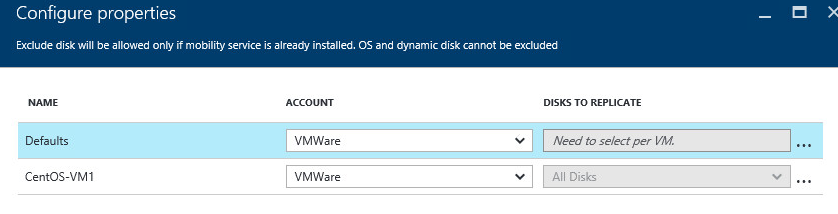
1. The Source pane will be closed. Select Step 2:Target. Use the *Select* option for the Storage Account to select the previously created Storage Account.



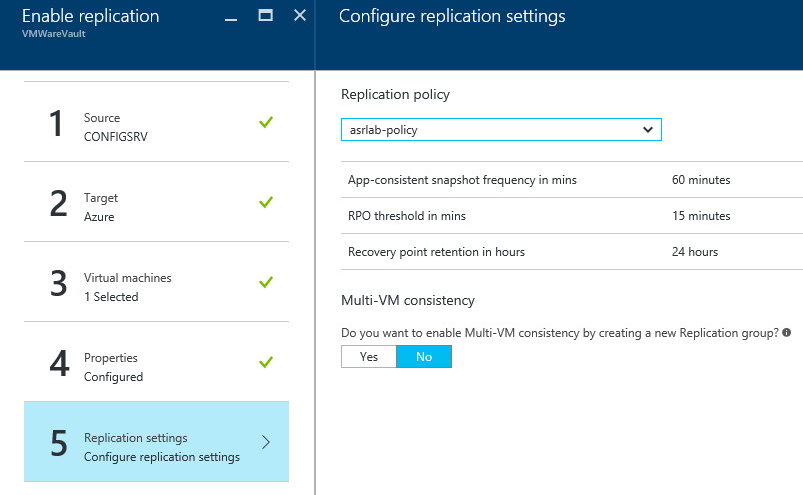
1. Do the same for the network, use the option *Configure now for selected machines*. Select the previously created network and a subnet and click *OK*.



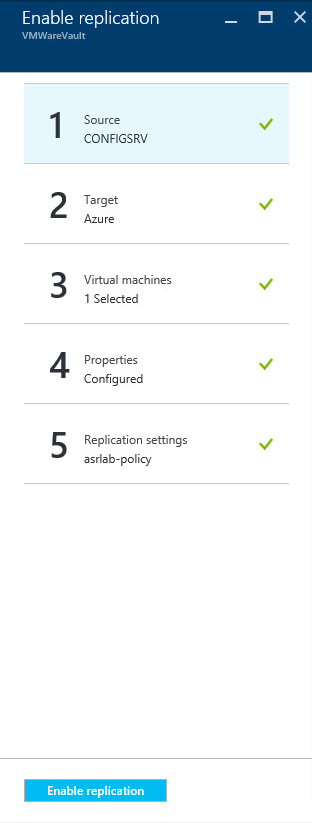
1. The Target Pane will be closed and a checkmark will appear in the Enable Replication pane, next to Step 2:Target.  
   Select Step 3:Virtual Machines. A virtual machine *CentOS-VM1* will be shown. This is the virtual machine that was manually started using the vSphere Client in a previous step. Since VMWare vCenter has been added to the setup, automatic discovery of virtual machines is possible.   
   Select the virtual machine. A checkbox will be displayed next to the virtual machine. Click *OK*.   
     
     
   
2. On the Configure Properties page, the settings can be left as displayed. In this lab the credentials for the VMWare vCenter server and the CentOS-VM1 virtual machine are identical. Therefore we can use the same account. In most environments this will not be the case.



1. The *Configure Replication Settings* pane will allow you to select a Replication Policy. In this case, only one exists. Click *OK*.



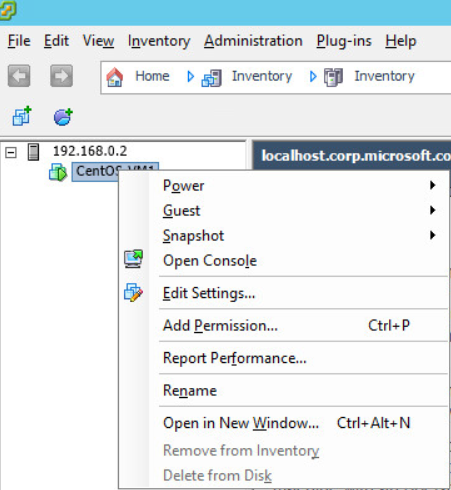
1. The Enable Replication pane will now list all steps as being completed. Click *Enable Replication* at the bottom of the page.



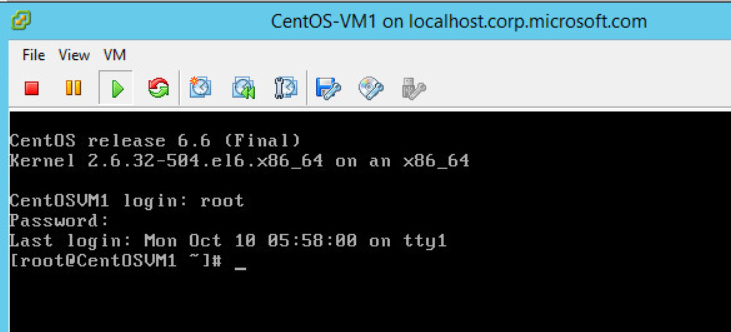
1. A job ‘*Enabling protection’* will start. This job will push the Mobility Service to the selected virtual machine(s) and do the initial data transfer to the Recovery Vault.



**Note: in case the ‘Enabling Protection’ job fails, continue with the steps below. If the ‘Enabling Protection’ job was successful continue with step J.**If the job fails, connect to the console of the CentOS-VM1 virtual machine.  
Do this by starting vCenter if it is not already running, right-clicking the virtual machine and selecting ‘Open Console’.



Click the console window to activate control. Be aware that at this point, all keyboard input is directed towards the Linux virtual machine and not the Remote Desktop session.   
Also note the comment in the bottom of the console window: *To release cursor, press CTRL + ALT.*

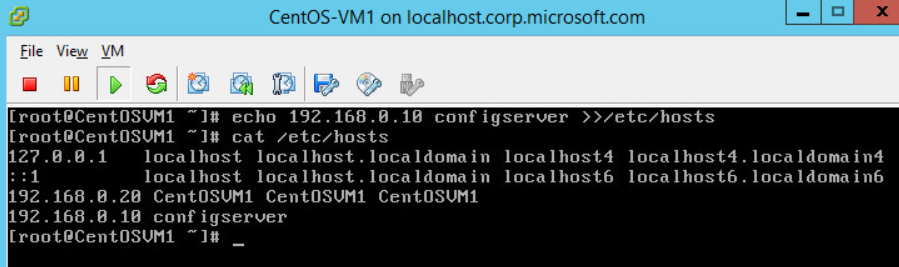


In the console windows, type the following:

*echo 192.168.0.10 configserver >>/etc/hosts*

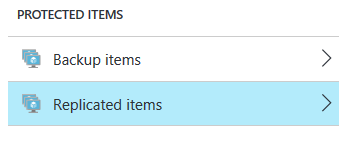
*cat /etc/hosts*

The output should look like the window below. The first command above will have added a ‘*hosts*’ entry for the ConfigServer VM.

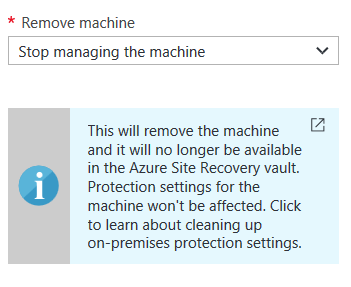


Release keyboard control of the console by pressing CTRL + ALT and close the window.

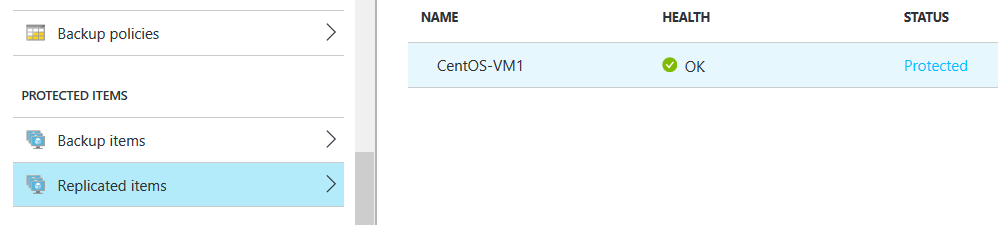
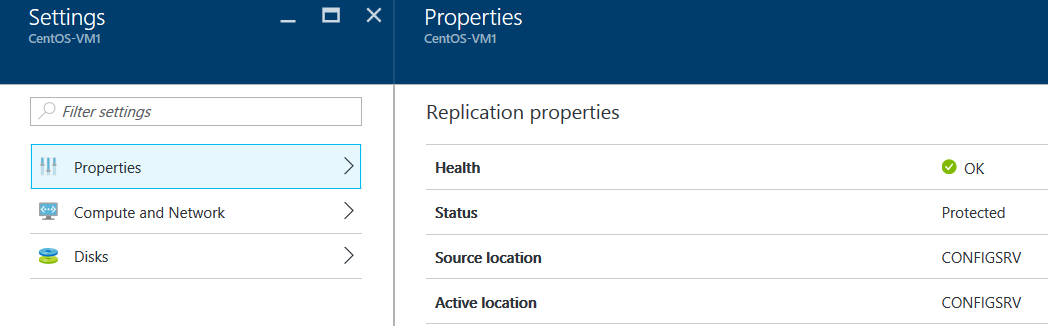
Even though the job was unsuccessful, the CentOS-VM1 virtual machine will already have been added to the Recovery Vault. To be able to complete the steps in this lab as documented, the virtual machine will need to be cleaned up.   
To do this, go to the settings of the Recovery Vault and selected *‘Replicated Items’*



The CentOS-VM1 will be shown. Select it and choose ‘Delete’. Choose ‘*Stop managing the virtual machine*’ and click *‘OK’*



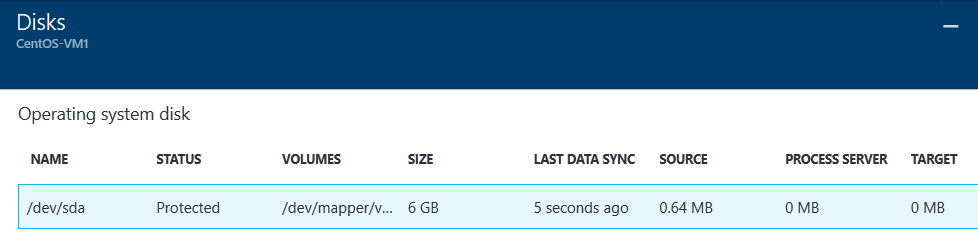
After these steps have been executed go back to step E to setup the protection again.   
Note that the checkboxes in the 1.Source and 2.Target steps will have disappeared but the configuration is still present. Select both of the steps and click ‘OK’ on both of them to confirm your selections.

1. Navigate to the Settings of the Recovery Vault and bring up the protected virtual machine under *Replicated Items*.  
     
     
     
   Select *CentOS-VM1* by clicking on the name. Two new blades will be displayed to the right of the selection screen. One blade will have the same name as virtual machine and the second one will be called ‘*Settings*’.  
     
   Select ‘*Properties’* of the virtual machine  
     
   

This will show statistics and configuration details for the selected virtual machine.

Select the ‘*Compute and Network’* option to bring up how the protected virtual machine will show up in Azure. The settings here reflect the Azure VM Name, VM Size and network properties.   
It is possible to change the values presented in this screen.  
  
There are several reasons why one might want to change the suggested VM Size:

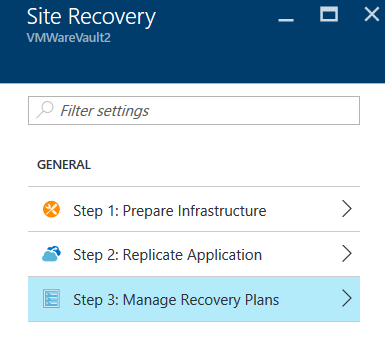
* to keep costs down when running these machine in Azure
* because the Source is oversized, for instance a physical machine with multiple physical CPUs and multiple cores
* As part of the failover plan, one might have chosen to not protect all on-premise machines but to give the ones that are enough resources.

Select the ‘*Disks’* option to bring up the disks that are part of the protected virtual machine. Since the virtual machine in this lab only has a single disk it will only list an *Operating System* *disk* and not a *Data disk*.  
  


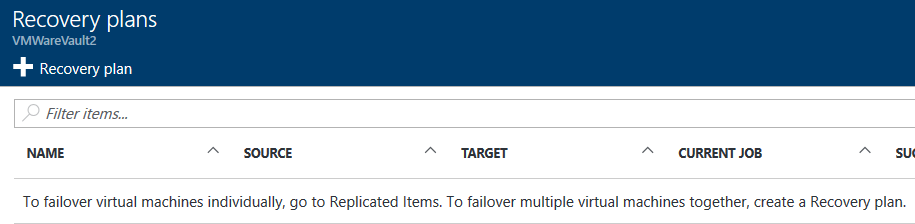
Exercise 6: Testing the deployment

Failovers can be done for each virtual machine individually or using a Recovery Plan for multiple virtual machines. Even though in this lab only one virtual machine is used, a Recovery Plan will be used.

1. Close any blades that are still open for the protected virtual machine.   
   Go to the *Getting Started* experience for the Recovery Vault and select ‘Step 3:Manage Recovery Plans’.

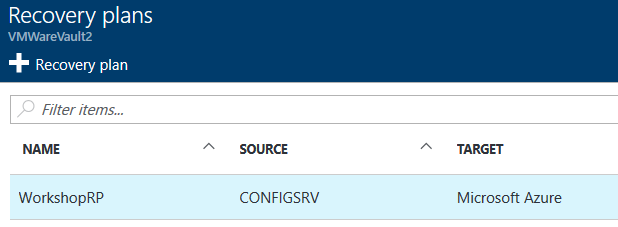


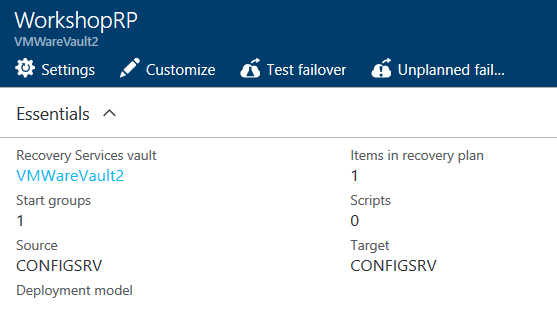
1. Click the ‘*+Recovery Plan’* option at the top of the screen



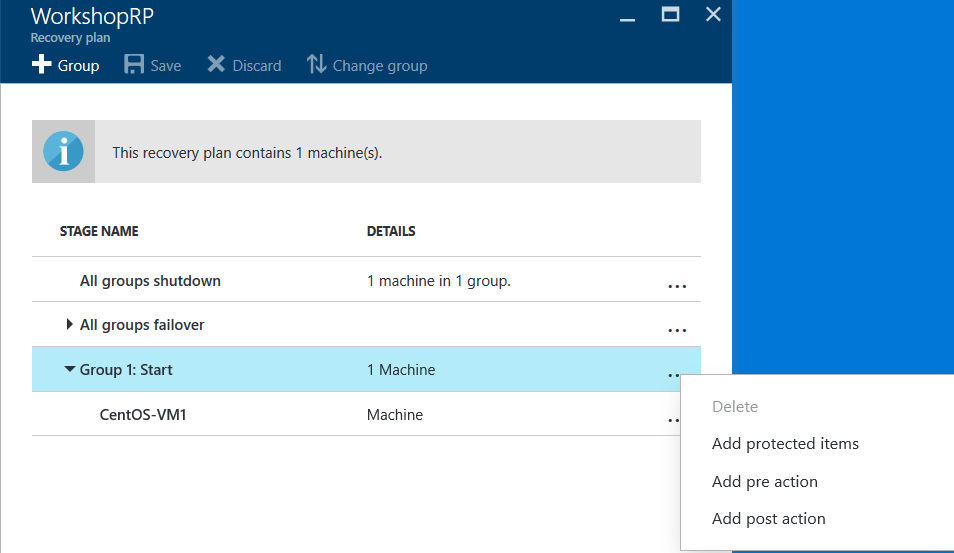
1. Define a name for the Recovery plan, choose *‘Microsoft Azure’* as the target and choose the CentOS-VM1 as the item.



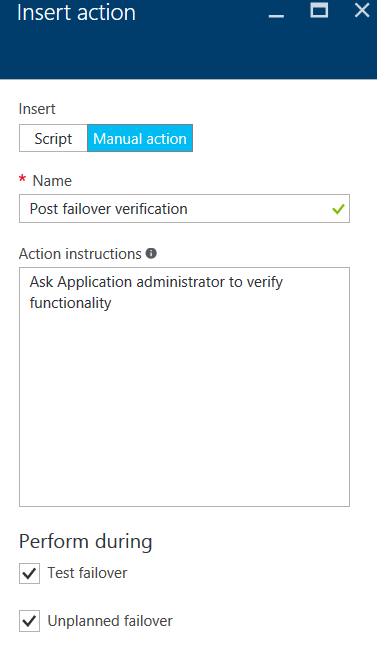
1. Click OK in both the *‘Select items’* blade and the ‘*Create Recovery Plan’* blade. This will bring up the Recovery Plan window and display the Recovery Plan that was just created.  
     
   
2. Select the Recovery Plan and select *‘Customize’*



1. A Recovery Plan can contain more than just the order in which virtual machines are failed over. Pre- or Post-actions containing Azure Automation jobs or manual steps can be included as well.   
   Choose ‘*Add Post Action’*.



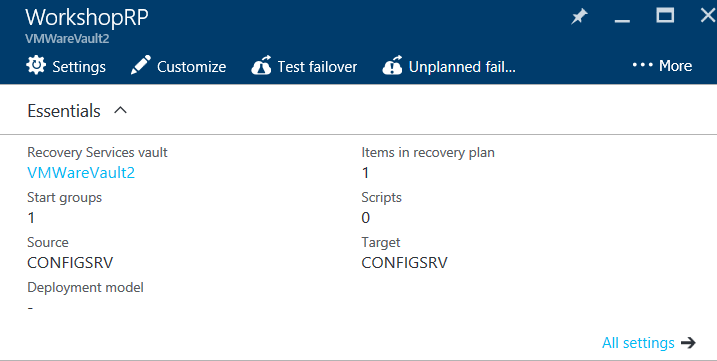
1. Switch to the *Manual Action* tab and define a name and instructions. Click ‘*OK’* to complete this step.



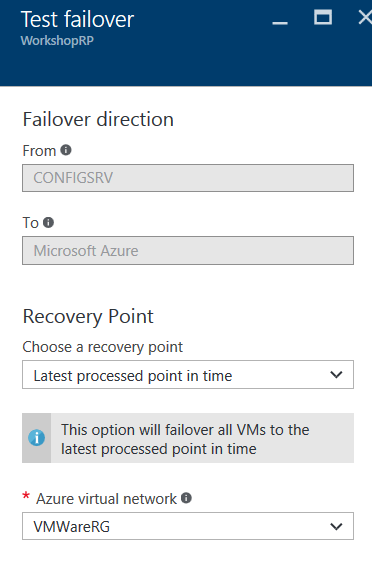
1. A warning will be presented to indicate the current version of the Recovery Plan has not been saved yet. Click ‘*Save’*.



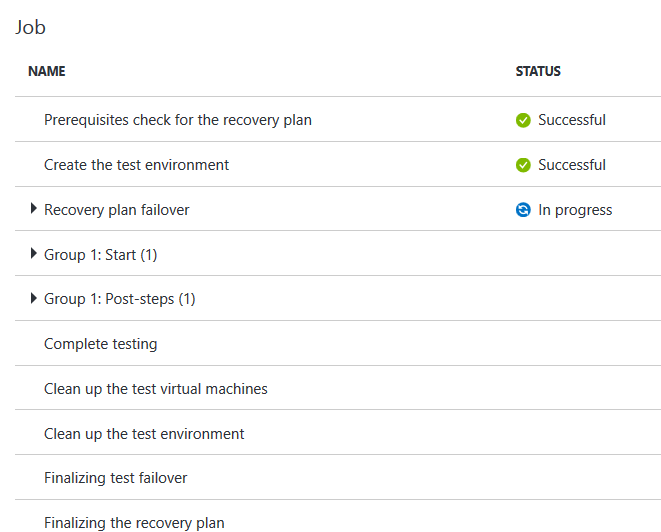
1. Close the pane and click ‘*Test Failover’*



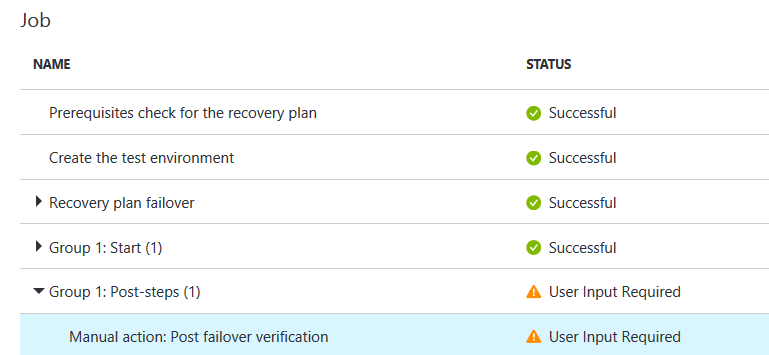
1. Accept the options presented for the Test failover and click ‘OK’



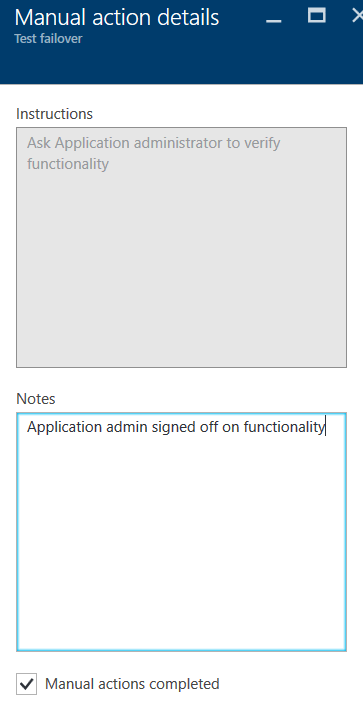
1. A Test failover job will start, clicking this job will bring up more details of the progress of the job, including the steps in the Recovery Plan.



1. Since we added an additional Post-step after failover of the virtual machine, the job will halt at that point and require user input.



Select this step. A new blade will be opened allowing you to put in a comment. This comment will be visible in the job details afterwards allowing you to track specific details.   
Place a checkmark in the ‘*Manual actions completed’* checkbox and click ‘*OK*’.



1. The Recovery Plan failover job will continue. Since the post-action that was added was the last step of the Recovery Plan, the job will halt again almost immediately.  
   In this case, the job will wait for confirmation of the Test Failover.   
     
   A Test Failover will be marked as completed automatically after 14 days. One can use this time to verify if everything failed over as expected. Be aware however that the failed over instances will consume resources and therefore will be charged.   
   It is therefore recommended to mark the test as being completed as soon as everything has been verified. Mark completion of the test by clicking *‘Complete Test’* in the top of the screen. This will take care of removing all failed over instances and these will therefore no longer consume resources.



Add comments if needed to the Test Failover job, check the box for *‘The test failover is complete’* and click OK.

