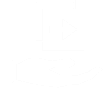
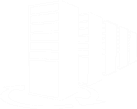
**Lab on Demand**

**-**



**Azure Site Recovery**

Hyper-V to Azure

Workshop Plus



Produced by Microsoft

2016

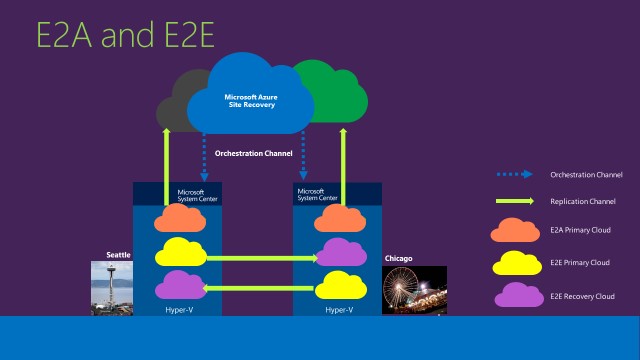
# HANDS-ON-LAB FOR BCDR WORKSHOP

As Fabric admins of a large enterprise, you have decided to enable protection for various applications of your datacenters. You are the owner of two datacenters – one each in Seattle and Chicago - and you need to configure the clouds, VMs and their underlying networks so that it represents applications in the datacenter. Since you have SLAs for different applications, you plan to protect them differently.

You are divided into two teams – Fabrikam and Contoso. Each team has their own clouds and applications. Fabrikam team is based out of Seattle. Contoso team is based out of Chicago. Help each team protect their workloads.

For Hyper-V,

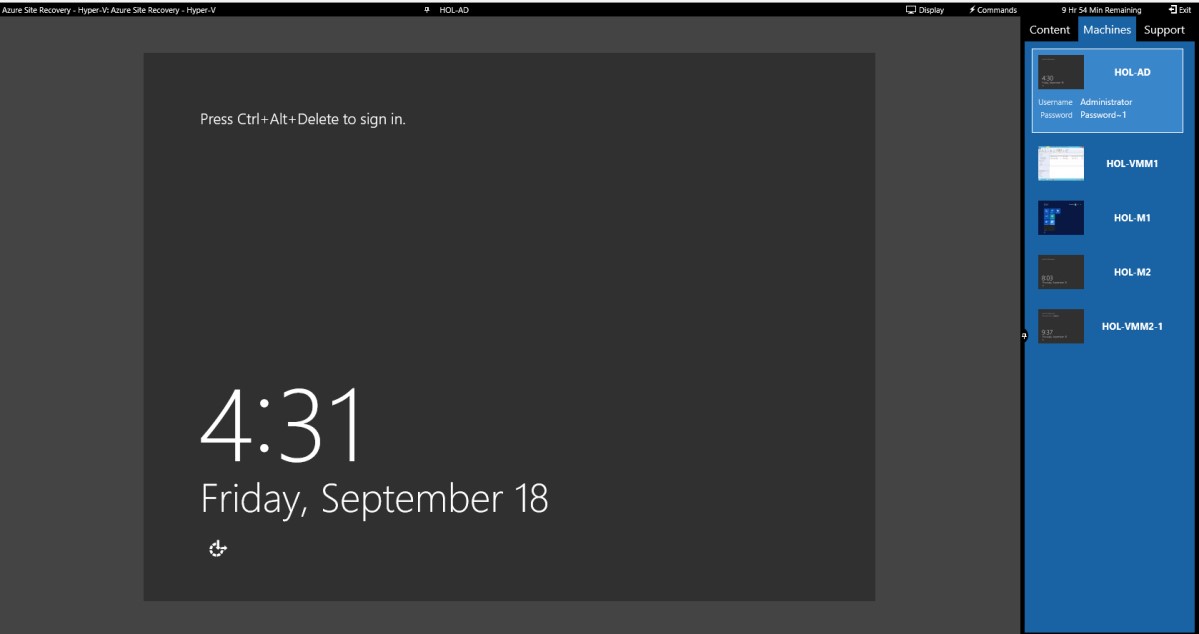
* For those that can be protected to Azure, you will use Azure (E2A)
* For those that are HBI but do not require 0 RPO, you will use your other datacenter (E2E)



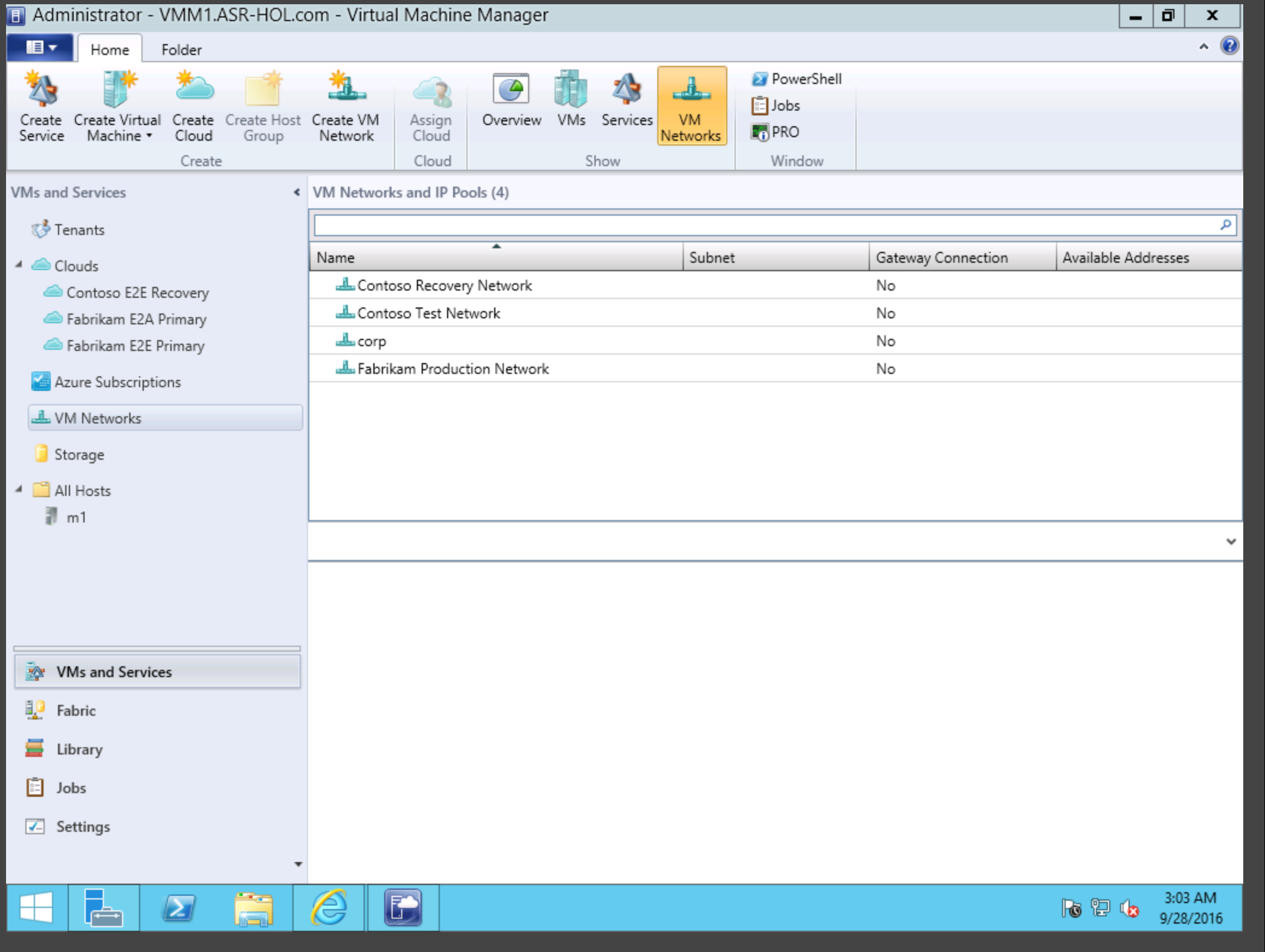
# Before you begin

* **Link to Environment & Access Credentials** – <To be Provided during the training.>
* **Azure access crentials** - <To be Provided during the training.>
* Each participant will be provided with a dedicated virtual environment, that comprises of
  + **HOL-AD (Active Directory)**
  + **HOL – VMM1 (Primary VMM Server - Seattle)** o **HOL – M1 (Hyper-V Host managed by VMM1)**
  + HOL – M2 (Hyper-V Host managed by VMM2 -– **Needed only for Hyper-V OnPrem to OnPrem DR scenario)**

o HOL – VMM2 (Secondary VMM Server Chicago – **Needed only for Hyper-V OnPrem to OnPrem DR scenario)**



**Each Lab environment has two datacenters. Following is an example topology. For this lab you need to work with only 1 Site (Seattle) using VMM1. Login into HOL-VMM1 to validate below.**



|  |  |
| --- | --- |
| **VMM1** | **Host** |
| **Seattle Site** | **M1** |

Each of you has either Seattle or Chicago as the Datacenter. The cloud naming convention is as follows:

|  |  |
| --- | --- |
| **Seattle Site** |  |
| Fabrikam E2A  Primary | Production workloads that will be protected to Azure  >>>You need to use only this cloud for this lab |
| Fabrikam E2E  Primary | Production workloads for the Fabrikam team in Seattle site – will be protected by Fabrikam E2E Recovery in the Chicago Site - |
| Contoso E2E  Recovery | Clouds to protect the Chicago site Contoso workloads |

The underlying networks are as below:

|  |  |
| --- | --- |
| **Seattle Site** |  |
| Fabrikam Production  Network | Available to Seattle Fabrikam E2E and E2A clouds  >>>Only this network will be used for this lab |
| Contoso Recovery  Network | Available to Contoso recovery cloud in Seattle |
| Contoso Test  Network | Available to Cotnoso recovery cloud in Seattle |

Apart from the above pre-created networks, you will need to create the Networks that will be required for Azure recovery – steps are given in the exercises.

## 

## Pre-work;

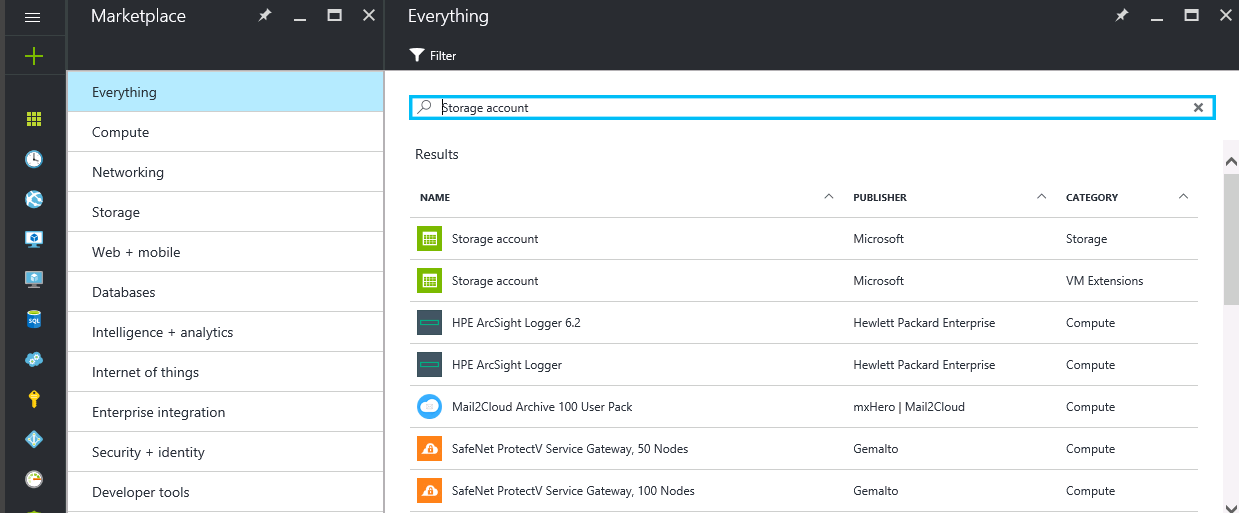
To make the setup of ASR as fluent as possible, it is important to have the prerequisites created before we jump in. Therefore, we will first create a storage account, resource group and virtual networks that the replicated VM’s will use on failover.

**Azure Storage Account and Resource Group Creation**

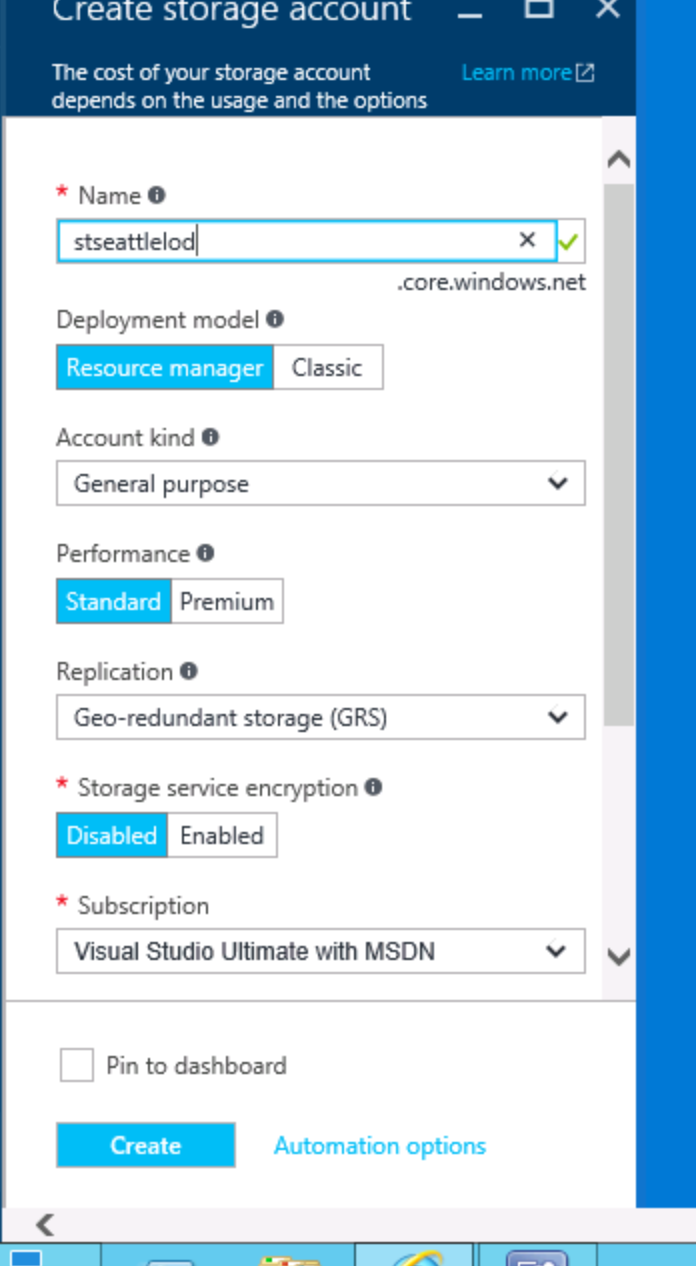
**From HOL-VMM1 Machine** - Log on to the azure portal <https://portal.azure.com/> using your Azure portal credentials.

1. **Create an Azure storage account in the same Geo as Vault (<Central US> in this case)** . To do this, click on “+” in the azure portal and type “Storage account” in the search field to find it in the market place.

Click on Storage Account then click on Create

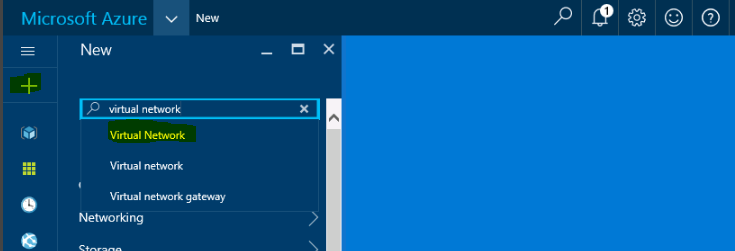


1. Name it as **stseattlelod.** If that name is not available append a random number to its end.
2. The storage account should be “**Geo-Redundant**”. This ensures that Azure Storage service copies the contents of this storage into another Azure datacenter to protect against storage outages.
3. In Resource Group, click the “Create New” radio button and call it **ASR-RG**. Make sure the location is set to “**Central US**”. Click “Create”.

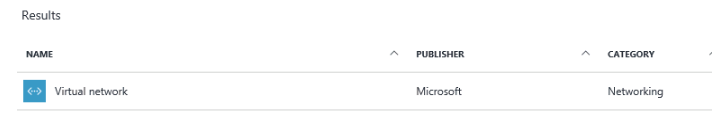


**Create Virtual Networks**

1. For Seattle site – create the following networks – use the Pod number appropriately
2. In the portal, click the “+”> type “Virtual Network”;



1. In the results field, click “Virtual Network;

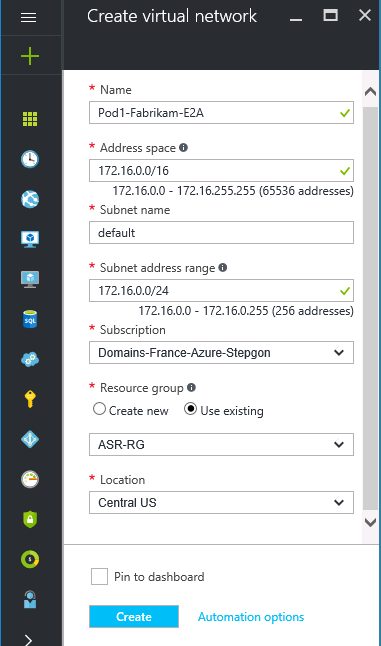


1. Then choose “Resource Manager” as deployment model and click Create.
2. Create below two networks with the properties mentioned in the table below;
3. **Pod1-Fabrikam-E2A**
4. **Pod1-Fabrikam-E2A-Test**

*Only create above two virtual networks, not the ones for Contoso.*

|  |  |  |
| --- | --- | --- |
| **P** | **od1** | **Properties** |
| Pod1-Fabrikam-E2A | Used during mapping. Use it with Fabrikam Production  Network | Address Space – 172.16.0.0  Subnet - 172.16.0.0  Location – Central US  DNS Server - None |
| Pod1-Fabrikam-E2A-Test | Used only during Test failover. | Address Space – 192.168.0.0  Subnet – 192.168.0.0  Location – Central US  DNS Server - None |
| *Pod1-Contoso-E2A* | *Used during mapping. Use it with Contoso Production*  *Network* | *Address Space – 172.16.*  *Location – Central US*  *DNS Server - None* |
| *Pod1-Contoso-E2A-Test* | *Used only during Test failover.* | *Address Space – 192.168.*  *Location – Central US*  *DNS Server - None* |

1. Use the ASR-RG Group created in the previous step(radio button “Use existing”) and location Central US, as per below example;



1. Do the same for the Pod1-Fabrikam-E2A-Test virtual network.

# ASR-E2A (Hyper-V) - Registration and Getting Started

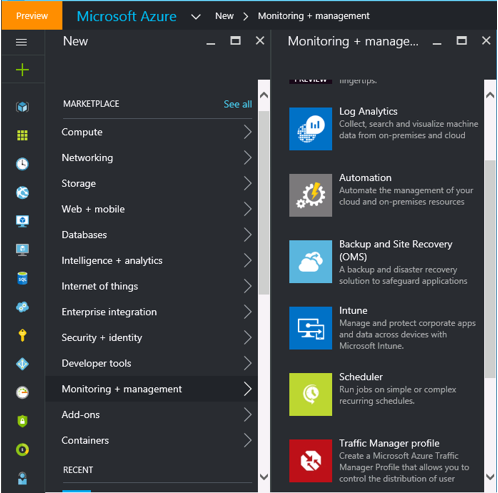
The objective of this lab is to familiarize you with the registration of Microsoft’s Disaster Recovery solution for Private Clouds. You will end the exercise by registering the VMM server to Azure Site Recovery Service.

## Objective

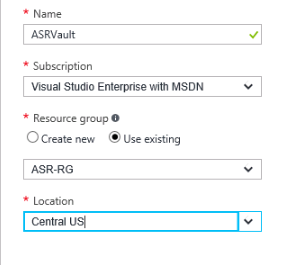
* *Identify your vault*
* *Prepare VMM server by registration*
* *Install agent on the Host machine*

## Part 1 – Create your Vault

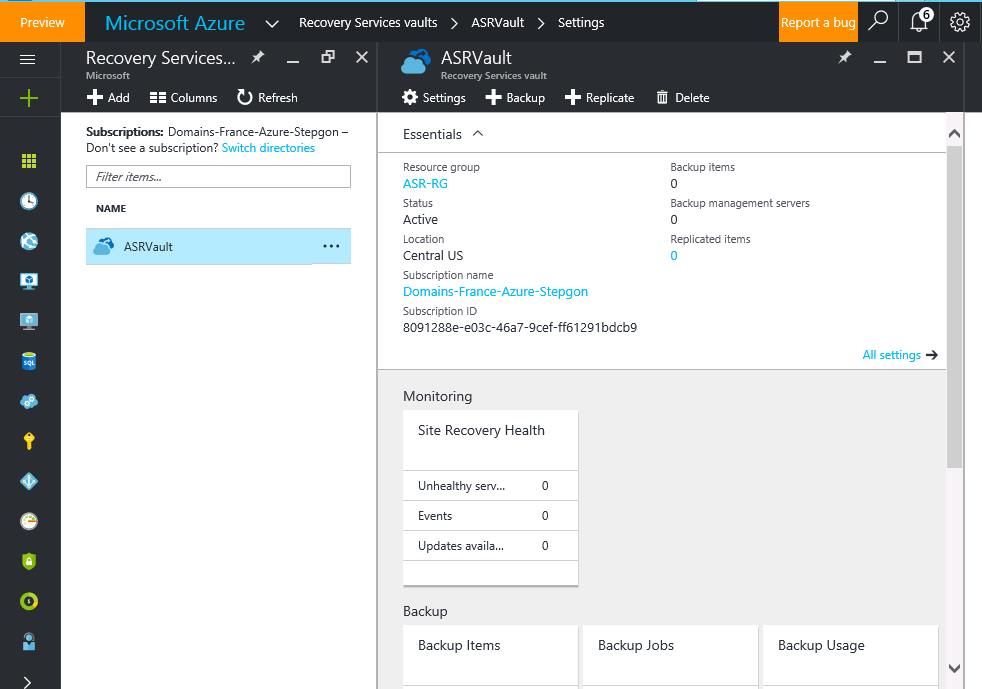
1. **From HOL-VMM1 Machine (Do open browser from this machine as we need to download a Provider on VMM Server)** - Log on to the azure portal <https://portal.azure.com/> using your Azure portal credentials.
2. Click **New** > **Monitoring + Management** > **Backup and Site Recovery (OMS)**. Alternatively, you can click **Browse** > **Recovery Services** vaults > **Add**.



1. Create a new vault in **Central US region** and name it **ASRVault** in the existing Resource Group named **ASR-RG**

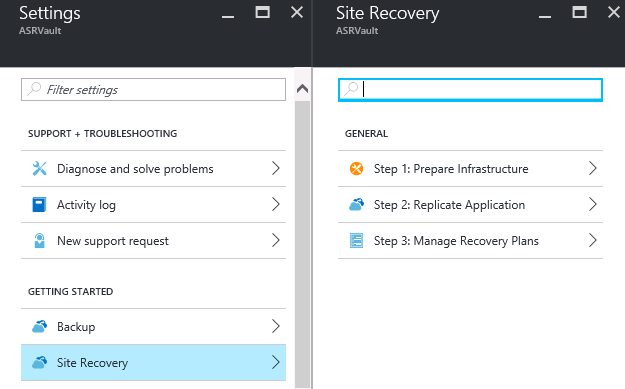


1. In the **Recovery Services vaults** blade select your vault and click **Settings**.

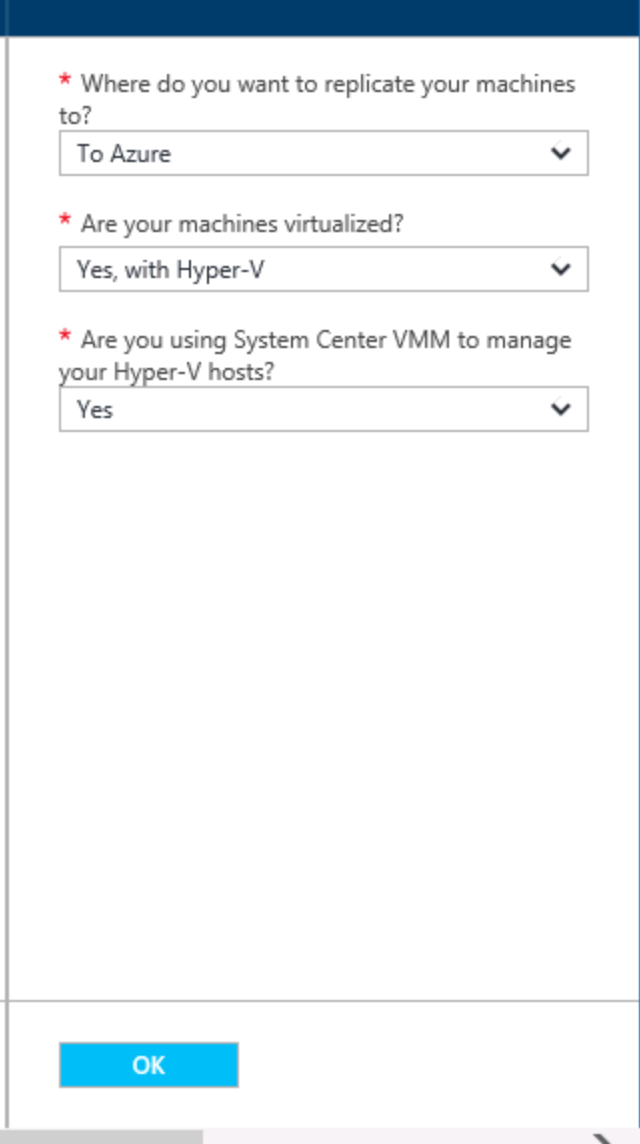




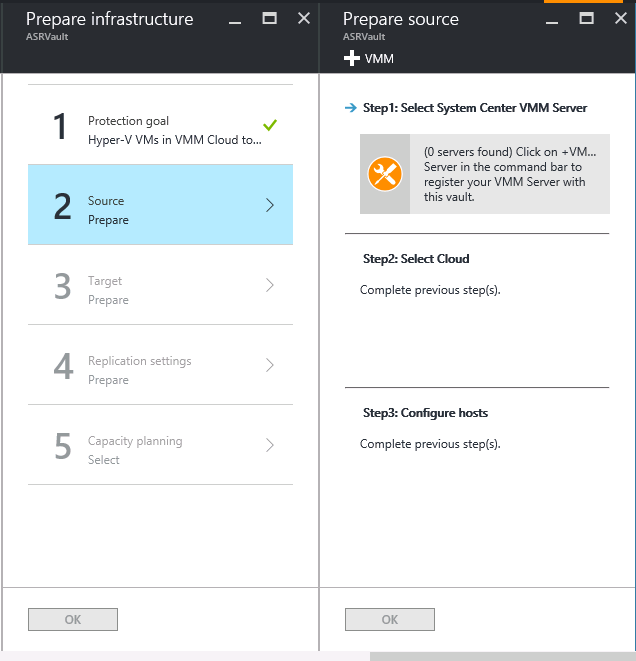
1. In **Getting Started** click **Site Recovery** > **Step 1: Prepare Infrastructure** > **Protection goal**.



1. In **Protection goal** select **To Azure**, and select **Yes, with Hyper-V**. Select **Yes** to confirm you're using VMM to manage Hyper-V hosts and the recovery site. Then click **OK**.

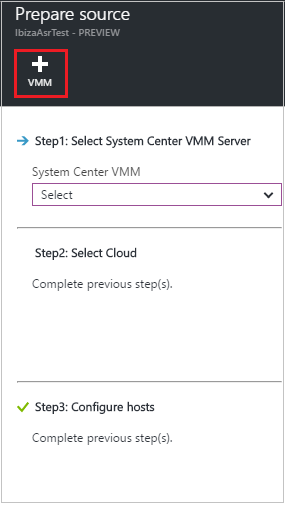


**Part 2 – Prepare VMM server by registration**





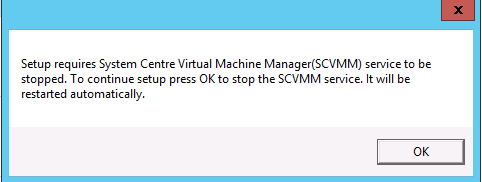
1. In **Prepare source** click **+ VMM** to add a VMM server.



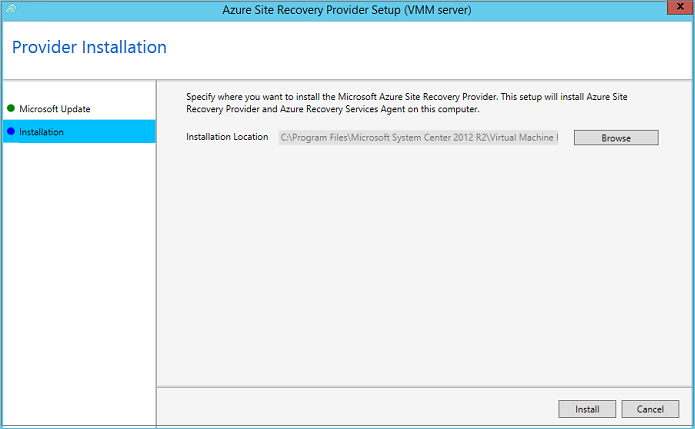
1. Download on your VMM server the Azure Site Recovery Provider (**MASR**) installation file and the registration key by clicking on the corresponding links



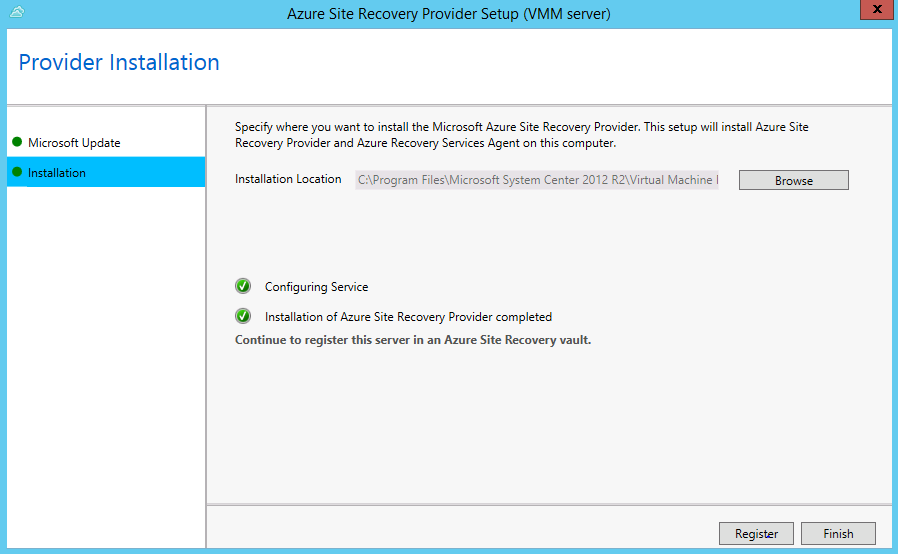
1. Run the Azure Site Recovery Provider on the VMM Server inside the VM.
2. Run the Provider setup file.
3. Click OK on the warning to stop VMM



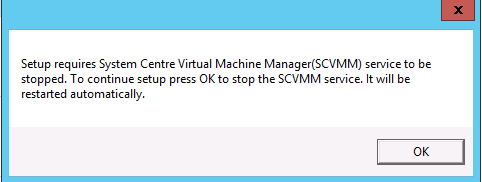
1. In **Microsoft Update** you can opt in for updates so that Provider updates are installed in accordance with your Microsoft Update policy.
2. In **Installation** accept or modify the default Provider installation location and click **Install**.



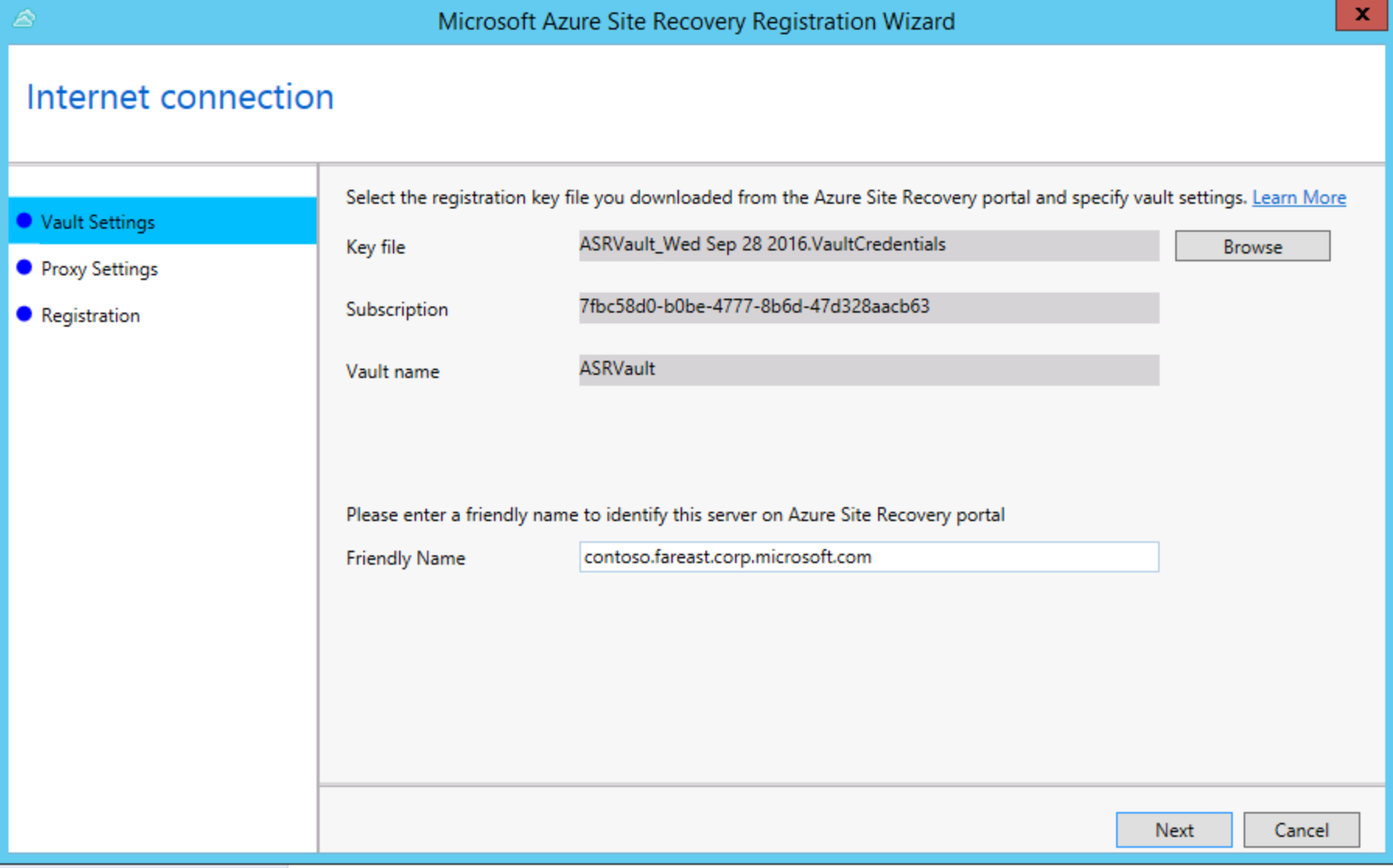
1. When installation finishes click **Register** to register the VMM server in the vault.



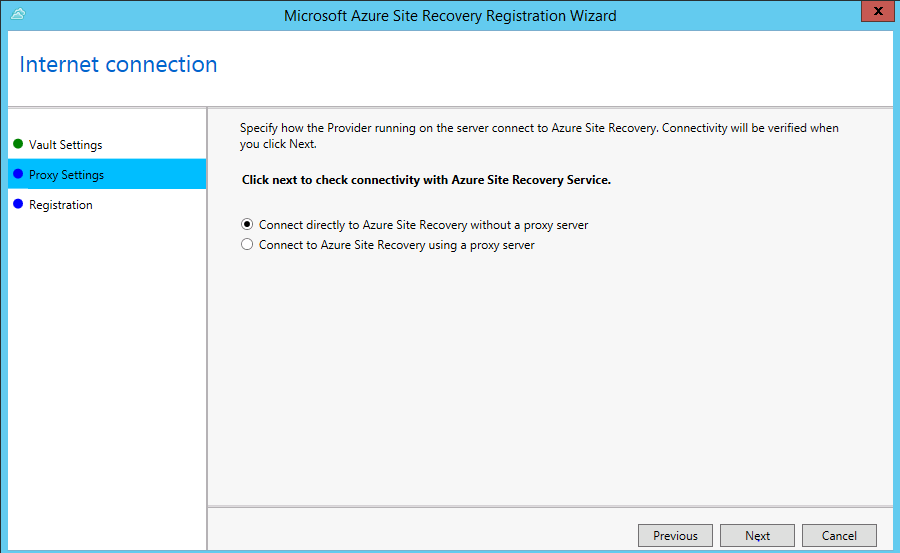
1. Click OK on the warning to stop VMM



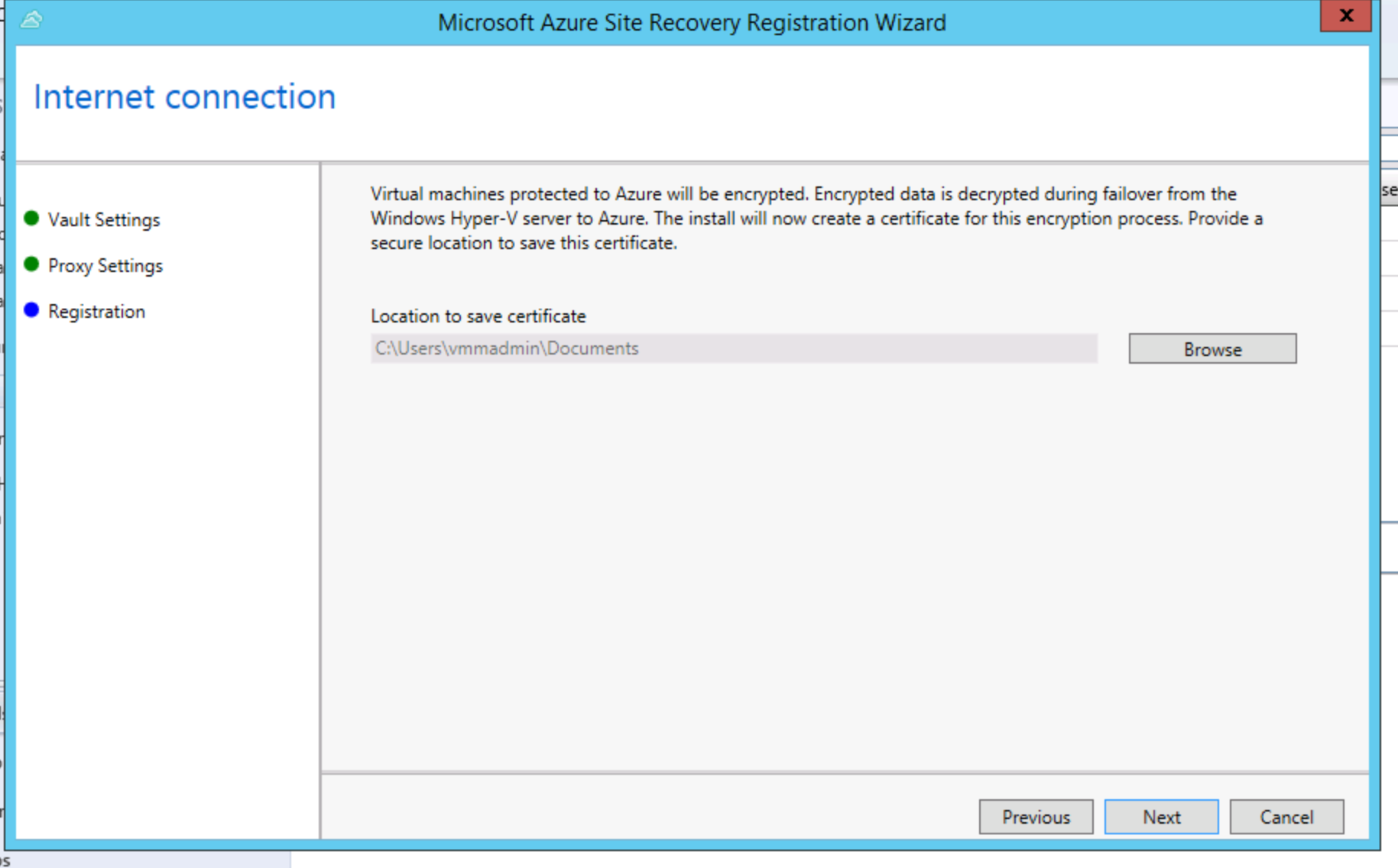
1. In **Vault Settings** page, click **Browse** to select the vault key file. Specify the Azure Site Recovery subscription and the vault name.



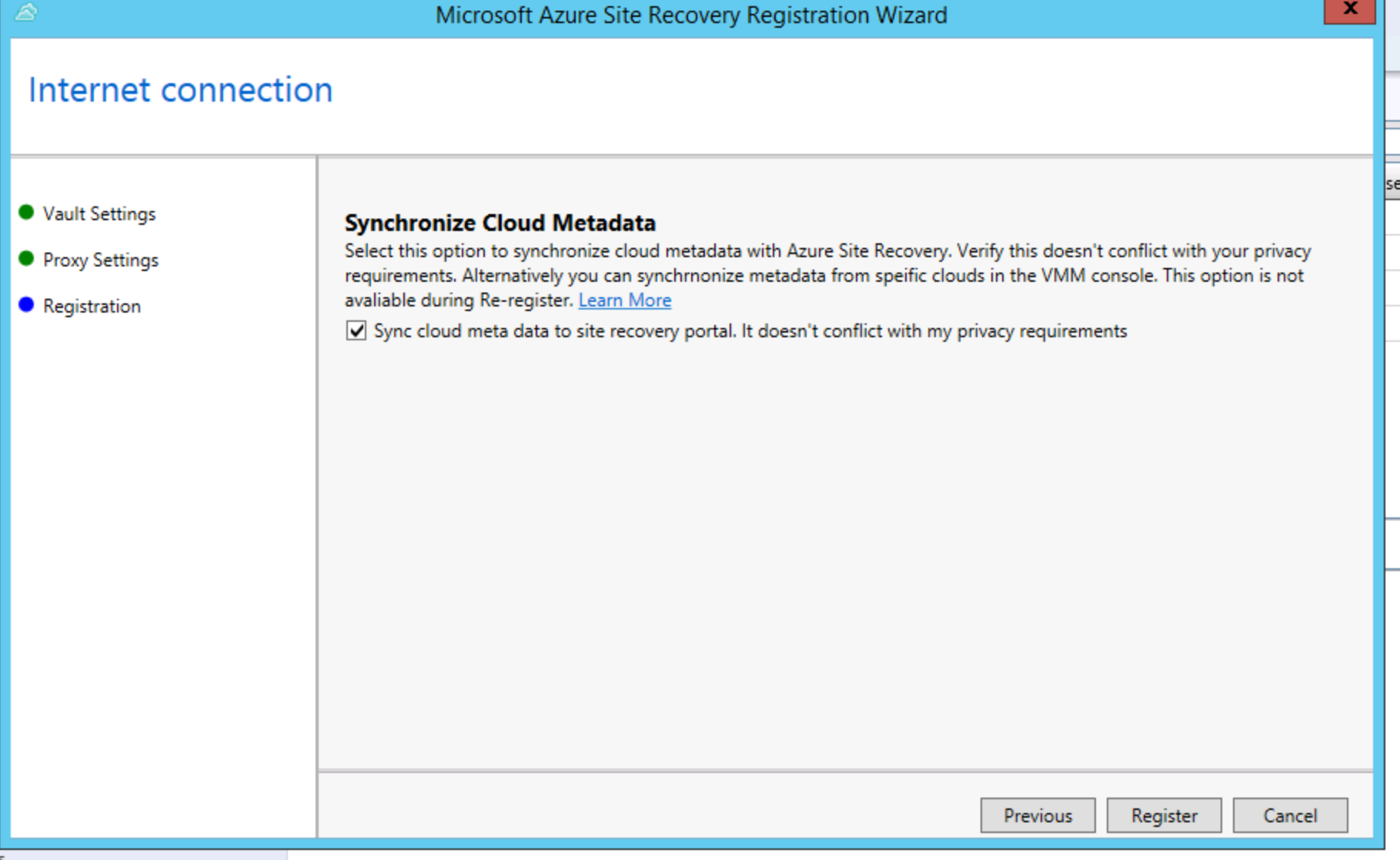
1. In **Proxy settings** specify how the Provider running on the VMM server will connect to Site Recovery over the internet.

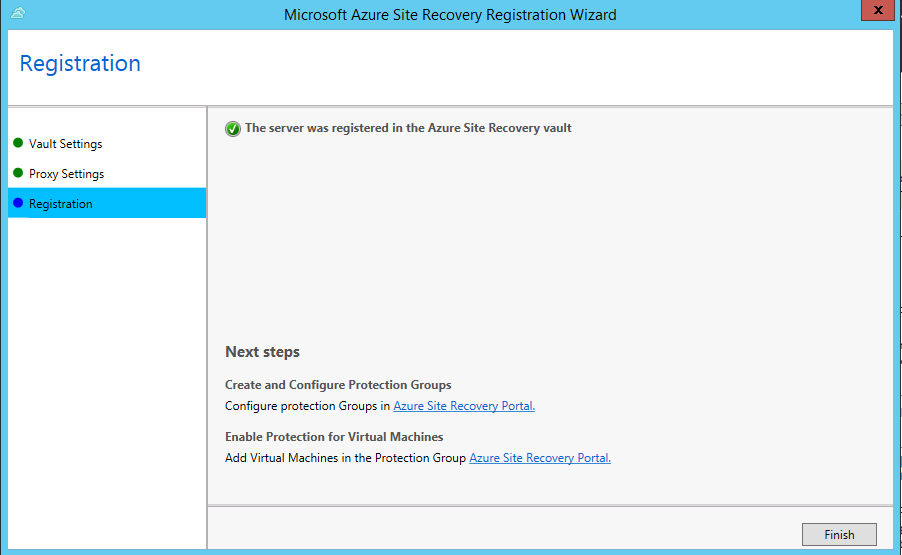


1. Accept or modify the location of an SSL certificate that’s automatically generated for data encryption. Click on **Next**

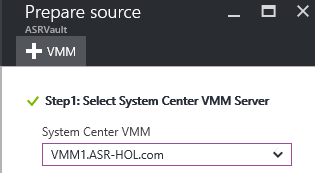


1. Enable **Sync cloud metadata** if you want to synchronize metadata for all clouds on the VMM server with the vault. If you don't want to synchronize all clouds, you can leave this setting unchecked and synchronize each cloud individually in the cloud properties in the VMM console. Click **Register** to complete the process.





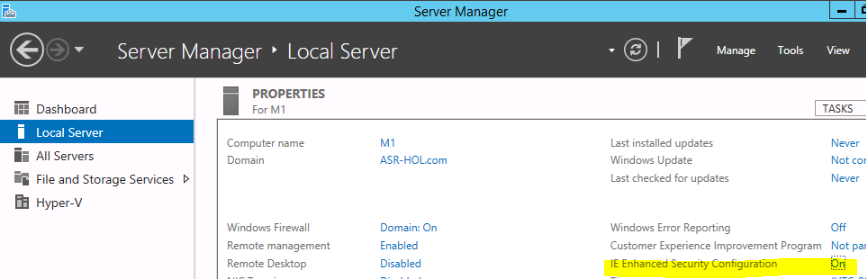
Go to the Azure management portal and check the VMM Server shows up and has a heartbeat with a green tick against connected.



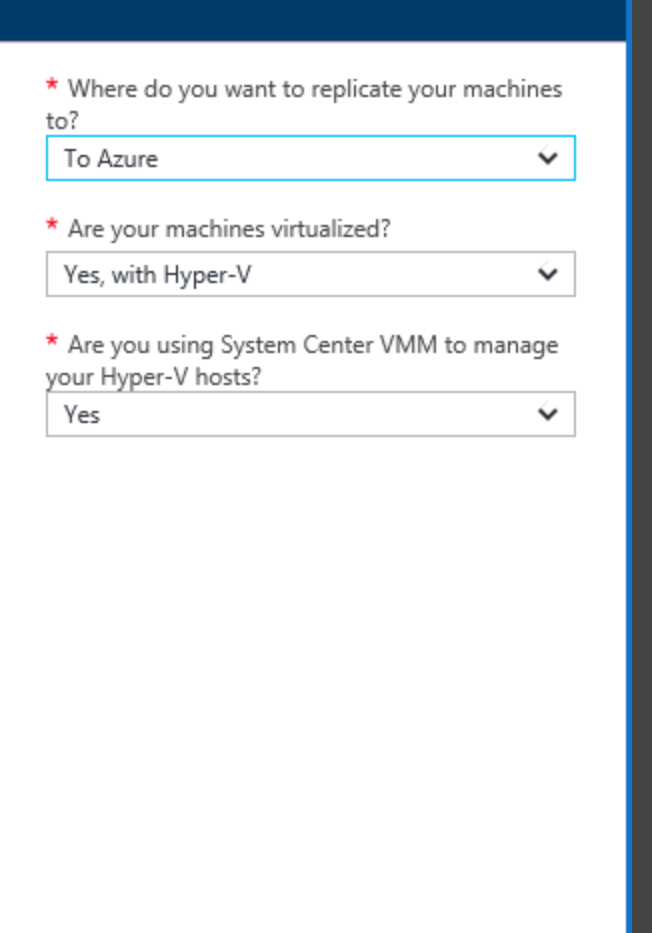
## Part 3 – Prepare Host machines

**Next you need to download the Agent and install it on your Hyper-V Hosts**

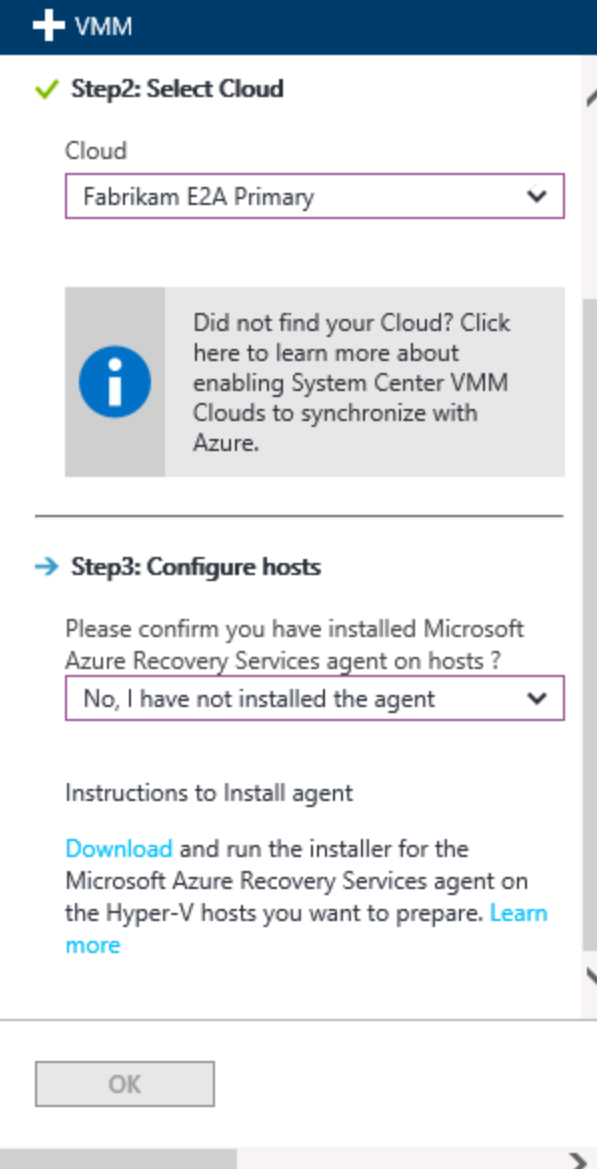
1. **Login into the host machine – HOL-M1.**
2. Disable IE Enhanced Security through Server Manager > Local Server;



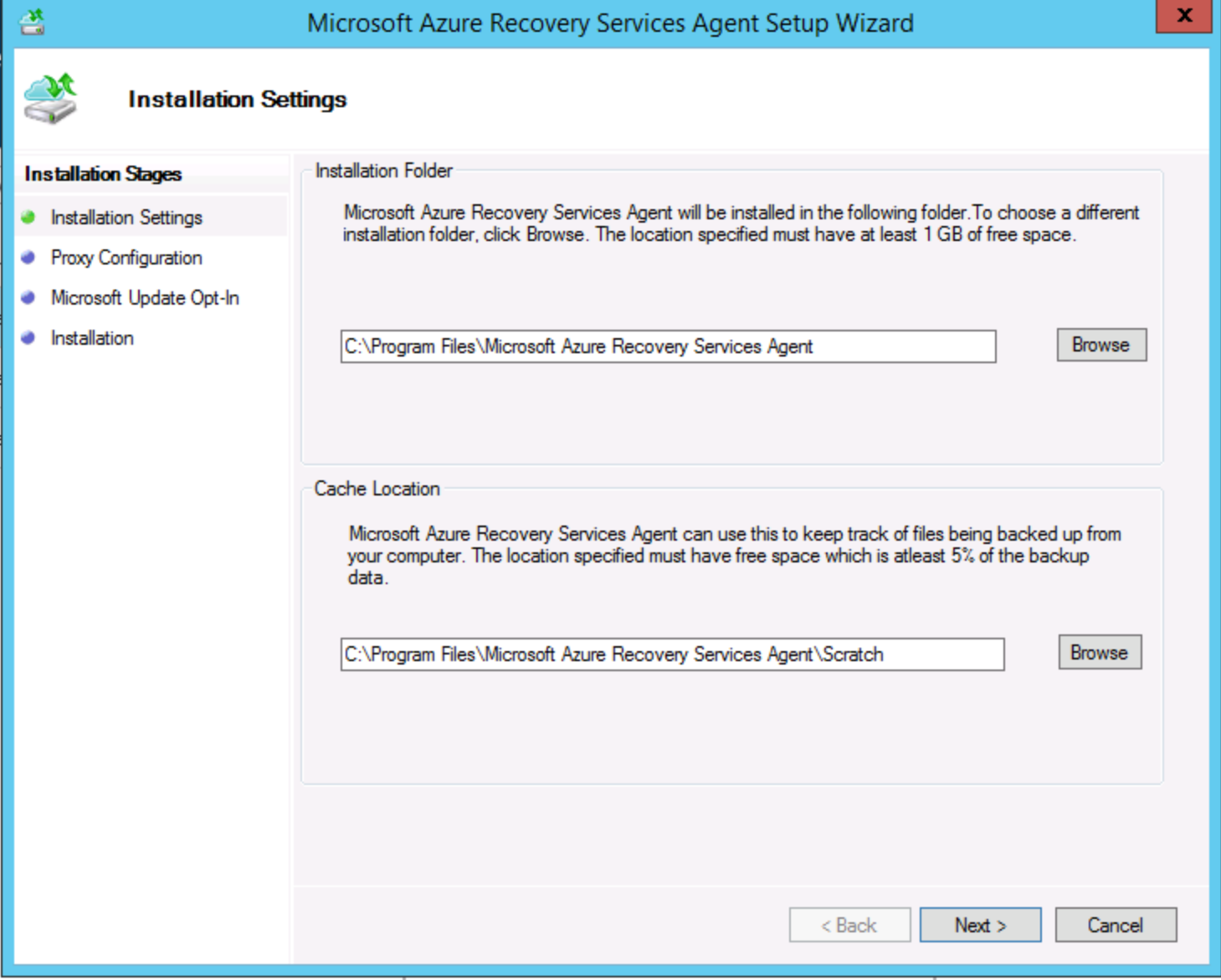
1. Log on to the azure portal <https://portal.azure.com/> using your Azure portal credentials.
2. In the **Recovery Services vaults** blade select your vault and click **Settings**.
3. In **Getting Started** click **Site Recovery** > **Step 1: Prepare Infrastructure** > **Protection goal**.
4. In **Protection goal** select **To Azure**, and select **Yes, with Hyper-V**. Select **Yes** to confirm you're using VMM to manage Hyper-V hosts and the recovery site. Then click **OK**.



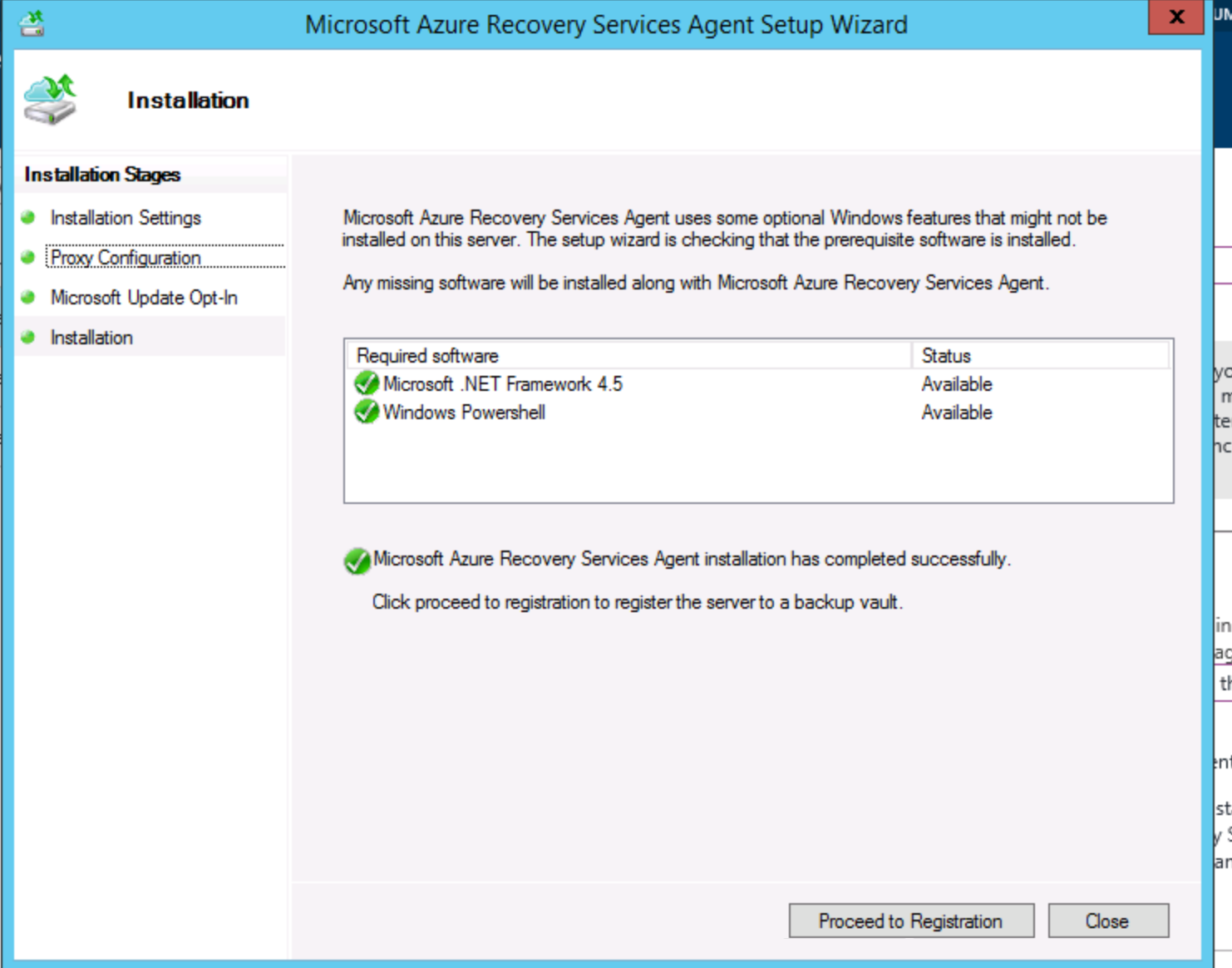
1. In **Prepare source** select the VMM server and the cloud “Fabrikam E2A Primary”. Then, on step 3, select “No, I have not installed the agent”.



1. Download the installation file for the **Microsoft Azure Recovery Services agent** on the host machine M1 (Step-3). Note this is a different installer than the installer downloaded on the VMM machine.

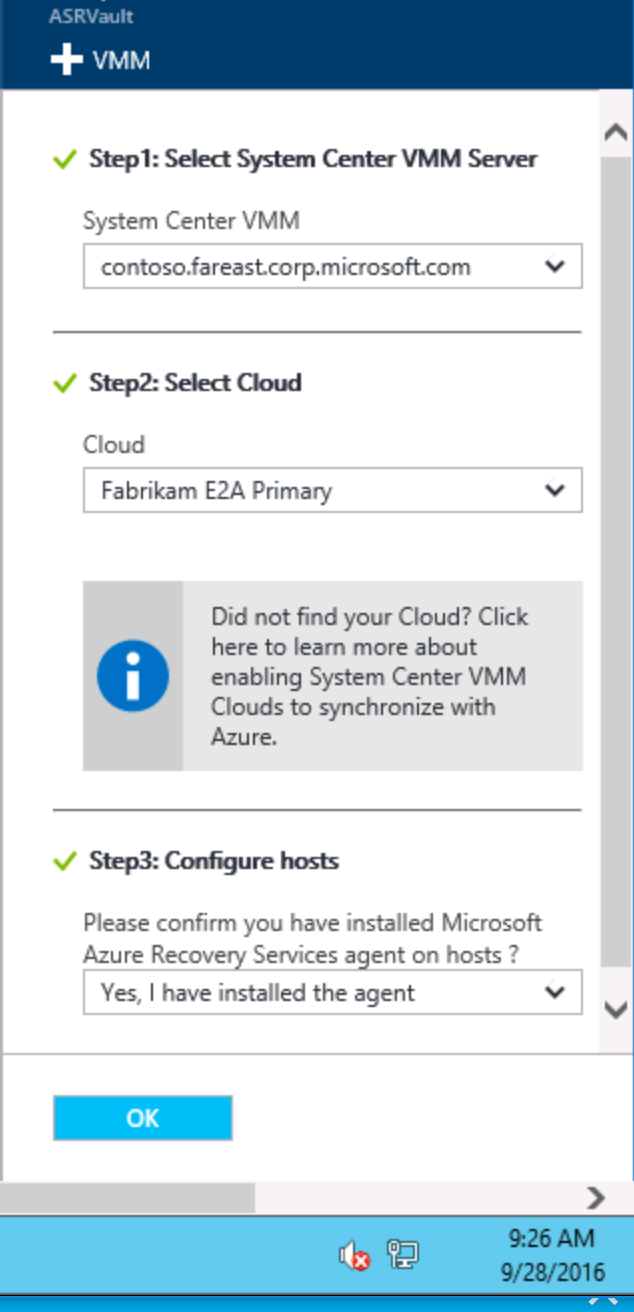


1. Install the agent on the host machine. This agent is the combined agent that sends data from the host to Azure – both for backup and DR purposes. Keep the defaults throughout the steps. **Do not “proceed to registration” after the setup completed – you can close the setup dialog.**



Go back in your **Recovery Services vault** **Settings**.

In **Step 3: Configure Hosts** > Select **“Yes, I have installed the agent”** and click **OK**



# ASR-E2A (Hyper-V) – Cloud Configure, Enable DR and Network Mapping

## Introduction

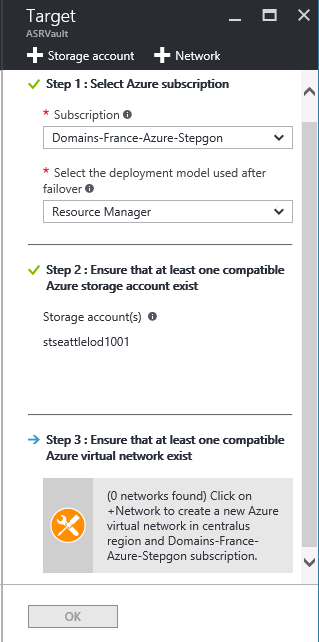
The objective of this lab is to familiarize you with the mapping of Compute, Storage and Network from on-premises to Azure. In this exercise, you are expected to enable protection capability for the clouds.

### Objective

* *Set up the target environment*
* *Set up replication settings*
* *Enable Protection for Virtual Machines*
* *Map Networks*

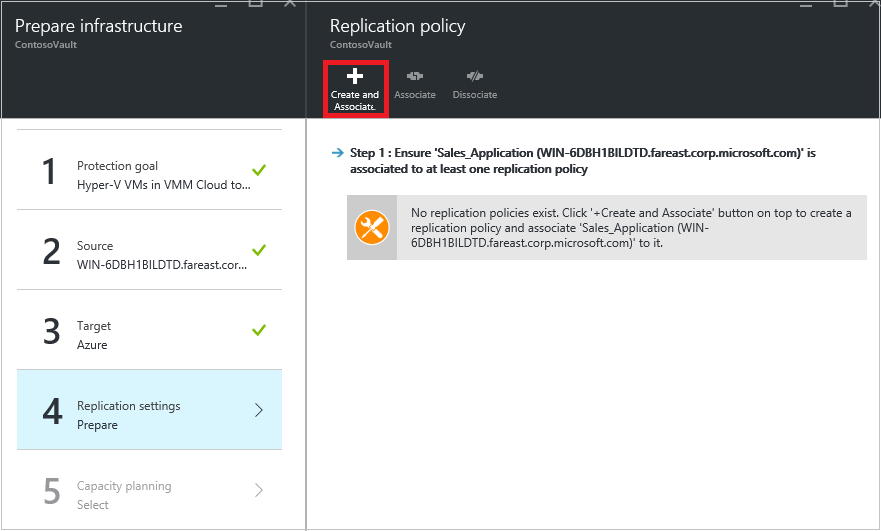
### Part 1 – Set up the target environment

1. Click **Prepare infrastructure** > **Target** and select the Azure subscription you want to use.
2. Specify the deployment model you want to use for VMs after failover > Resource Manager.
3. Site Recovery checks that you have one or more compatible Azure storage accounts and networks. If you have multiple, click on the “+ Storage Account” or “+ Network” and make sure that the ones created for this lab are in there; for storage account, it is stseattlelodxx and the networks should be called “Pod1-Fabrikam-E2A” and “Pod1-Fabrikam-E2A-Test”.

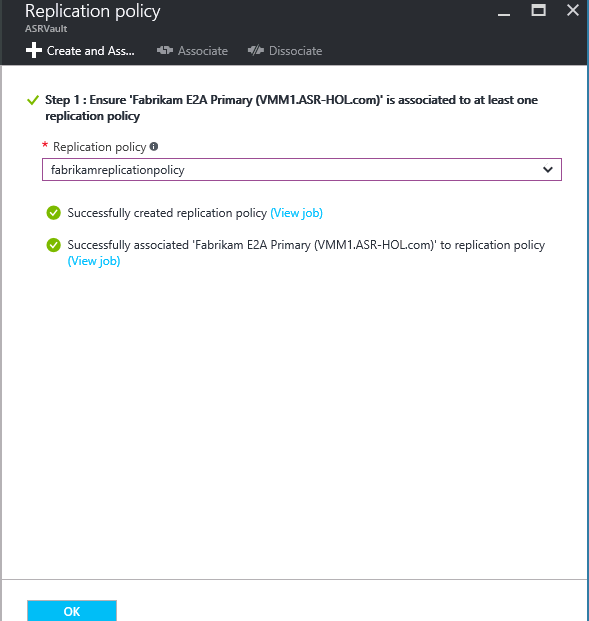


### Part 2 – Set up replication settings

1. To create a new replication policy in the ASRVault, click Settings>Site Recovery>**Prepare infrastructure** > **Replication Settings** >**+Create and associate**.



1. In **Create and associate policy** specify a policy name (fabrikamreplication policy for example)
2. In **Copy frequency** specify how often you want to replicate delta data after the initial replication (every 30 seconds, 5 or 15 minutes).
3. In **Recovery point retention**, specify in hours how long the retention window will be for each recovery point. Protected machines can be recovered to any point within a window.
4. In **App-consistent snapshot frequency** specify how frequently (1-12 hours) recovery points containing application-consistent snapshots will be created
5. In **Initial replication start time** specify when to start the initial replication. The replication occurs over your internet bandwidth so you might want to schedule it outside your busy hours.
6. In **Encrypt data stored on Azure** specify whether to encrypt at rest data in Azure storage. Then click **OK**.



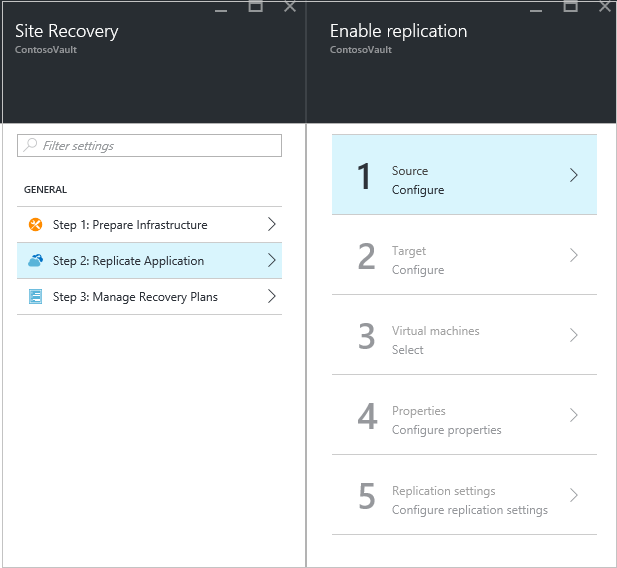
1. When you create a new policy it's automatically associated with the VMM cloud. Click **OK**. You can associate additional VMM Clouds (and the VMs in them) with this replication policy in **Settings** > **Replication** > policy name > **Associate VMM Cloud**.
2. Once done, in step 5: Capacity Planning, chose “Yes, I have done it” and click ok. Click ok again to go back to the Site Recovery blade.

### Part 3 – Enable protection for VMs

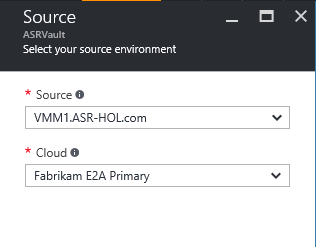
The fabric admin has enabled DR capability at the Cloud/infrastructure level and communicated the same to the App admins of the respective data centers. Now they want the App Admins to start enabling their VMs for Protection.

Now as App admins you need to enable recovery capability for your respective application.

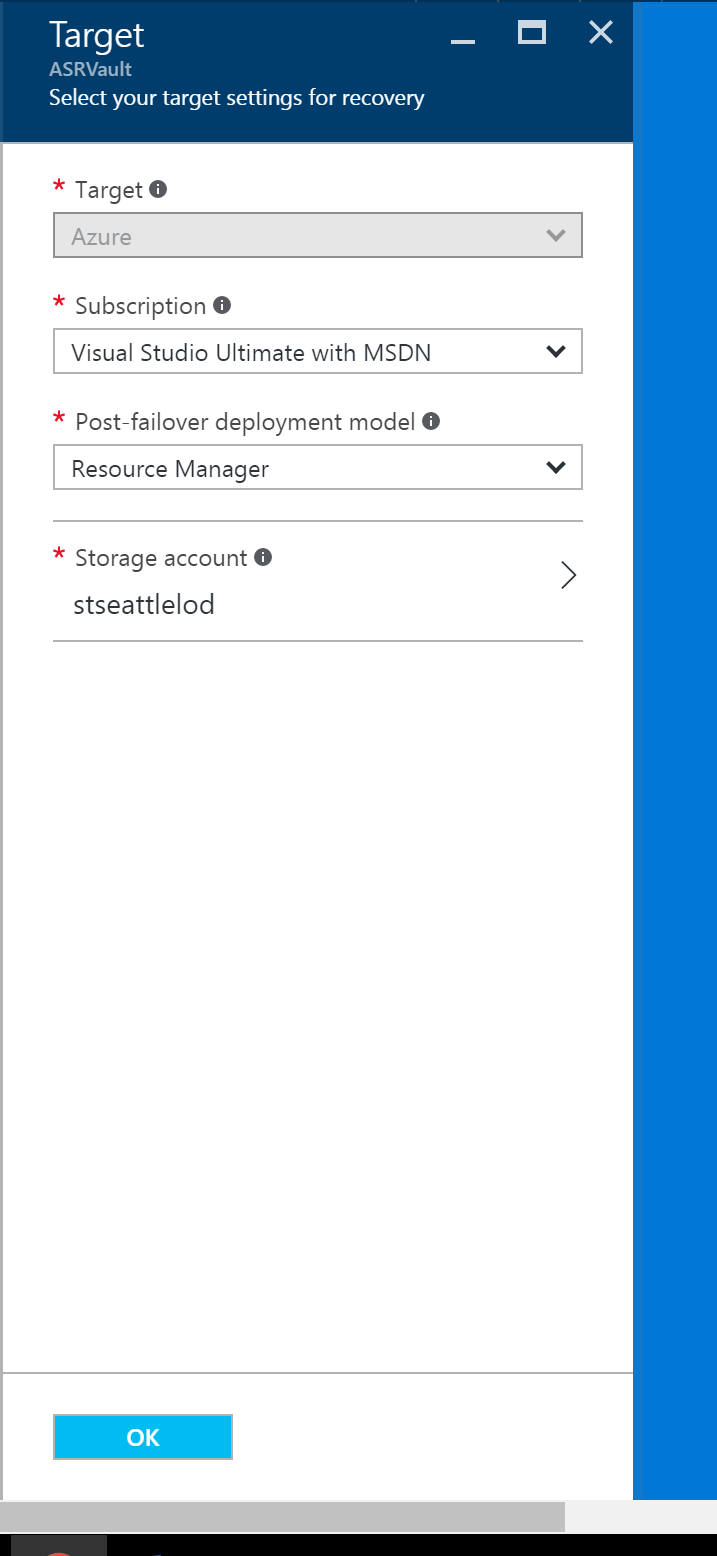
1. Click **Step 2: Replicate application** > **Source**. After you've enabled replication for the first time you'll click **+Replicate** in the vault to enable replication for additional machines.



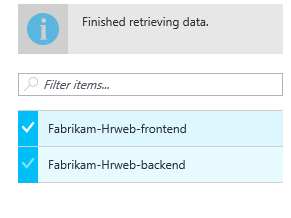
1. In the **Source** blade > select the VMM server and the cloud in which the Hyper-V hosts are located for eg: ***Fabrikam E2A Primary.*** Then click **OK**.



1. In **Target** select the subscription, post-failover deployment model, and the storage account you're using for replicated data.

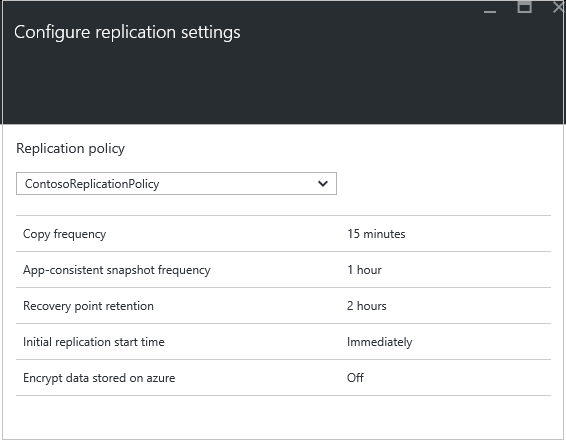


1. Select the storage account you want to use.
2. In **Virtual Machines** > **Select virtual machines: *Fabrikam-Hrweb-frontend***  and ***Fabrikam-Hrweb-backend***. Then click **OK**.

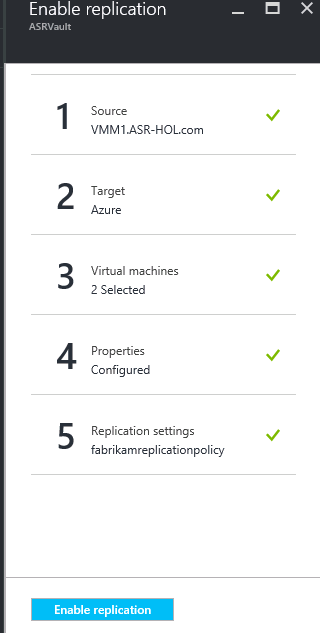


6. In **Properties** > **Configure properties**, select the operating system for the selected VMs, and the OS disk. Select the OS as Windows then click **OK**. You can set additional properties later.

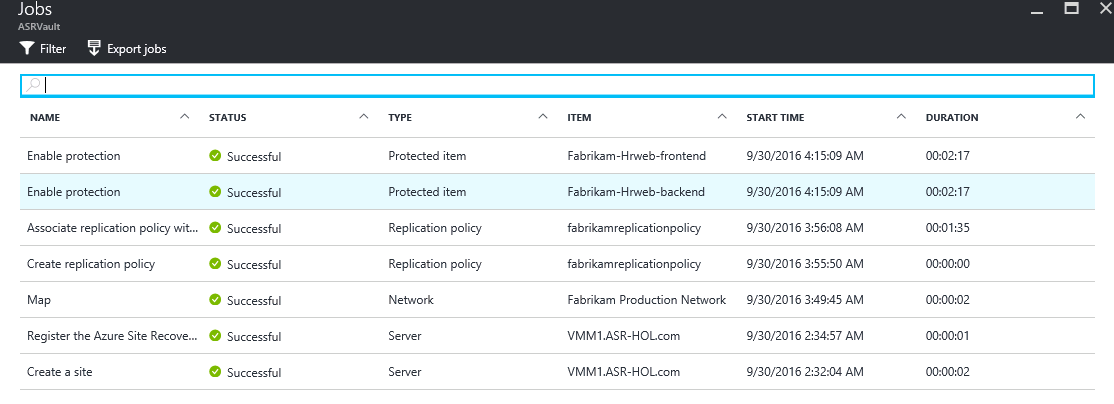
7. In **Replication settings** > **Configure replication settings**, select the replication policy you want to apply for the protected VMs. Then click **OK**. You can modify the replication policy in **Settings** > **Replication policies** > policy name > **Edit Settings**. Changes you apply will be used for machines that are already replicating, and new machines.



Click on Enable Replication button



You can track progress of the **Enable Protection** job in **Settings** > **Jobs** > **Site Recovery jobs**. After the **Finalize Protection** job runs the machine is ready for failover.

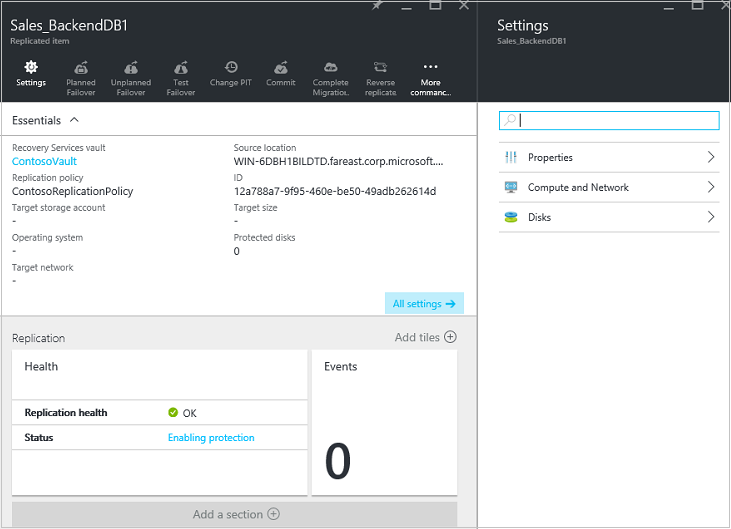


Please note the initial replication could take several minutes to complete.

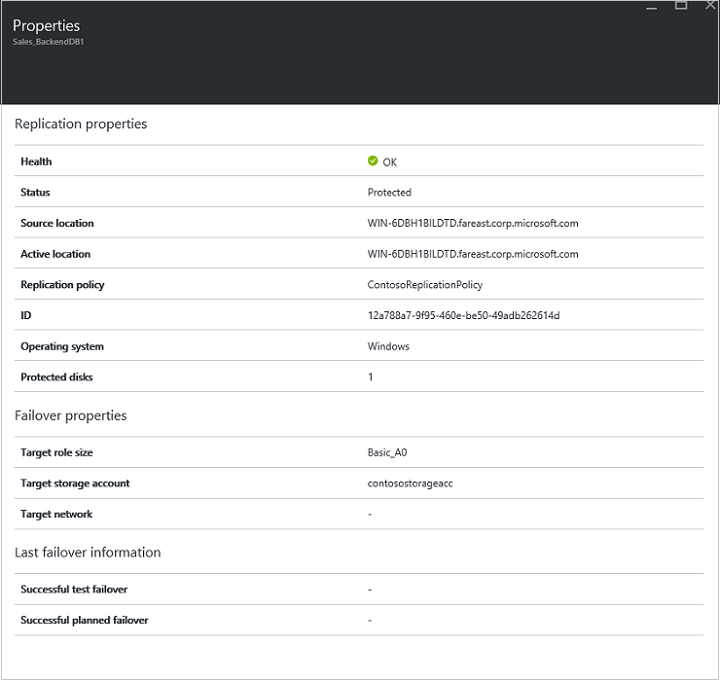
### Part 4 – VM Properties

Based on the characteristics of the VMs that are enabled for protection, the service chooses an IaaS size. You can choose a different size – either for costing reasons or for performance reasons.

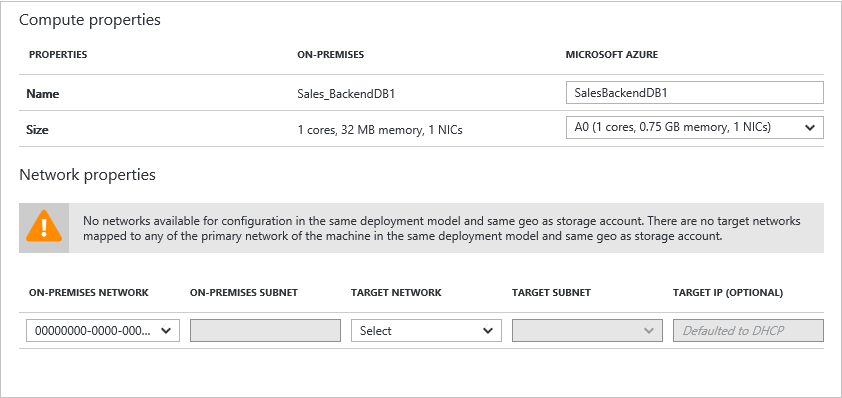
1. Click **Settings** > **Protected Items** > **Replicated Items** > and select the machine to see its details.



1. In **Properties** you can view replication and failover information for the VM.



1. In **Compute and Network** > **Compute properties** you can specify the Azure VM name and target size. You can also view and modify information about the target network, subnet, and IP address that will be assigned to the Azure VM.

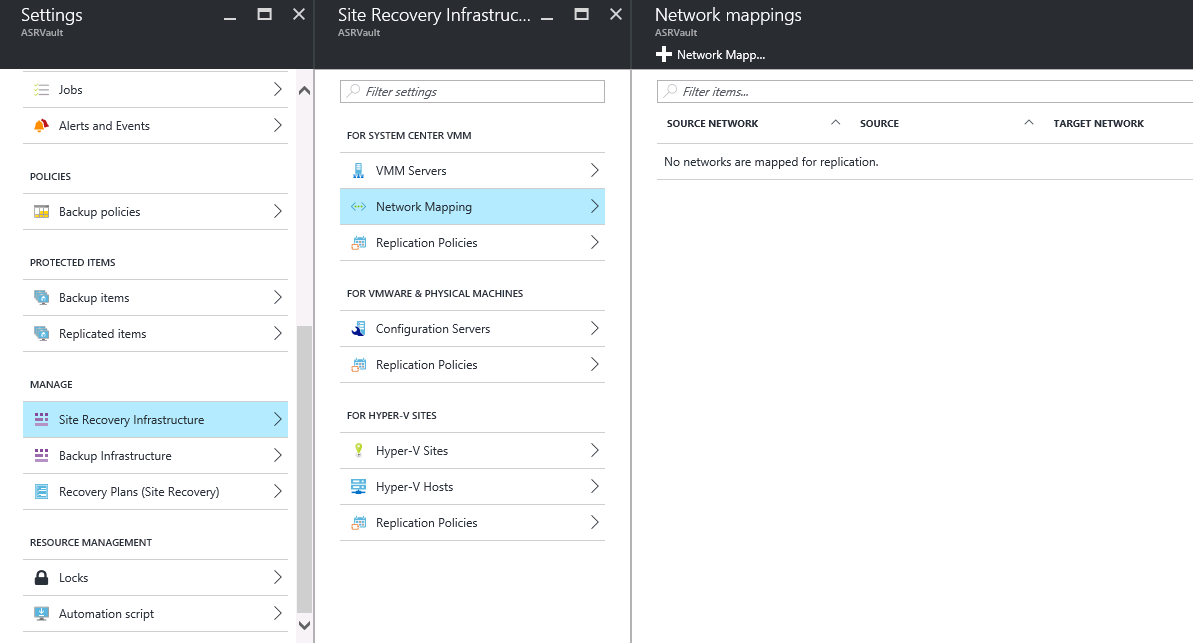


1. In **Disks** you can see the operating system and data disks on the VM that will be replicated.

### Part 5 – Configure Network Mapping

Now, you need to map the networks from VMM to Azure so that the VMs that are failed over to Azure are automatically connected to the corresponding network.

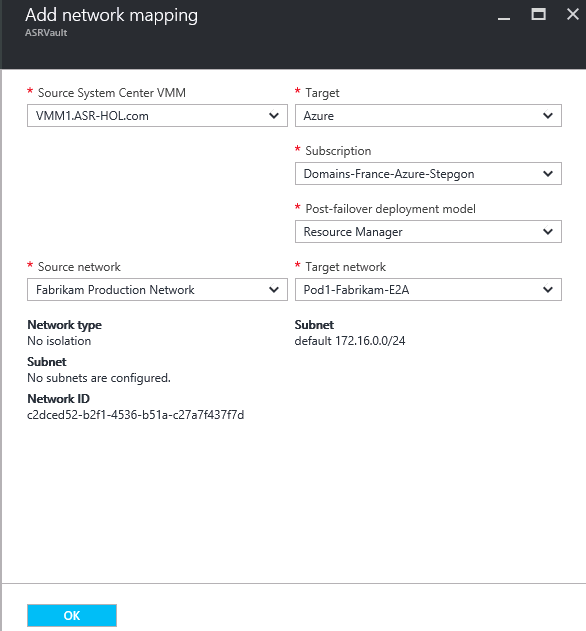
1. In **Settings** > **Site Recovery Infrastructure** > **Network mapping** > **Network Mappings**



1. click the **+Network Mapping** icon.



1. On the **Add network mapping** select the source VMM server, and **Azure** as the target.
2. Verify the subscription and the deployment model (Resource Manager) after failover.
3. In **Source network**, select the source on-premises VM network you want to map from the list associated with the VMM server > Fabrikam Production Network.
4. In **Target network** select the Azure network in which replica Azure VMs will be located when they're spun up. Then click **OK**.



# ASR-E2A (Hyper-V): Recover your applications in case of Disaster/Maintenance

The DR infrastructure is doing the necessary replication and both Fabric Admin (in Azure Portal) and App admins (In VMM console) can monitor the health of their recovery capability and check whether everything is running smooth.

As part of regular DR Drill, the App team wants to check their DR readiness. For this they have asked the Fabric admin to help them with the Test Failover. A Test Azure Network is created in Azure and has been communicated to the App team. The Fabric Admin will initiate a test failover and then when it completed will ask the App team to confirm the application is working.

So as part of this exercise Fabric Admins have to recover the applications as part of a Test failover keeping the on-premises workload unaffected.

## Objective

* *Create a Recovery plan*
* *Customize the plan to model dependencies*
* *Test failover the application*

## Part 1- create a recovery plan

On the portal, author a recovery plan for your application. A recovery plan allows you to automate the complete failover process through orchestration of VM failovers, scripts and manual actions.

1. Go to your vault, go to “Manage” and then select *Recovery Plans(Site Recovery)* in the portal. Click “+ Recovery Plan” to build a new recovery plan.
2. Provide name as **p*od1hrweb-fabrikam (for Chicago give the name pod1hrwebcontoso)***
3. Select the **Seattle VMM** and select **Azure** as Target Location.
4. Select the VMs you protected – ***Fabrikam-Hrweb-frontend and FabrikamHrweb-backend***.
5. Wait for some time to so that Recovery Plan gets created.

In this application **Fabrikam-Hrweb-frontend** has a dependency on **Fabrikam-Hrweb-backend** and needs backend vitual machine to come up first for proper functioning. Customize the recovery plan to change the order in which the VMs needs to be failed over

1. Right click on the recovery plan and select *Customize* on the recovery plan.
2. Create a new Group by selecting the operation *+Group*
3. As front end server needs to be failed over last; move **Fabrikam-Hrweb-frontend** to Group2. Click “Save”.
4. Add post action after **group 1 : start**
   1. To add a post action, right click the group and select “**Add post action**”.Now select the tab *Manual Action* and provide a description about the manual operation. For the sake of this exercise, add dummy instructions like “*Wait for some time for services to start*”.

[**Below step for script is not available for current HOL setup. Basically this shows how you can enable running of scripts using Azure Automation as part of ASR recovery plans.]**

1. Add a script after the **group 2 : start – Bonus exercise**
   1. To add a post action, right click the group and select “**Add post action**”.Now select the tab “Script” and launch the Script dialog.
   2. Give the name for the script as “**Enable HTTP Endpoint**”
   3. Select the Azure Automation Account “**HOL-Scripts**” iv. Select the Azure Runbook Script “**OpenPort80**”

v. Don’t add a script for VMM direction

2. Click on “Save” to save your customization. The recovery plan for your application ready for failover.

## Part 2 – Do a Test recovery (*this will not work as the machines are nested on Hyper-V*)

1. Now to failover your application, select the recovery plan you createdfrom the list *Recovery Plans*  and click Test Failover.
2. Select the appropriate test Azure network for your Pod and VMM site. For example, for pod1 Seattle for the Fabrikam team select the network **Pod1-Fabrikam-E2A-Test.**
3. Check *Jobs* to view the progress of the failover task.
4. As you have a Manual Task as part of recovery plan, execution of the recovery plan will pause at this point for you to validate the necessary state. When you hit this manual action, acknowledge that you have completed the manual action – then the recovery plan will continue to execute.
5. You can see the progress of the Azure Automation script.
6. The recovery plan will stop when test failover has completed and waiting for a manual action.

Check the cloud service and you will see a new cloud service with the name with a prefix of the recovery plan. Click on the Cloud Services tab on the left navigation pane to check.

Once you have confirmed that the virtual machine is created in Azure you can clean up the environment.

1. Complete test failover of the recovery plan by going to the job page and completing it. 8. Ensure that the test failover job completes and all the VMs created and now removed.

# Lab Summary

In this lab you have performed the initial cloud configuration for your protection, enabled protection for your virtual machines and failed the same over using recovery plans.

Thank you for completing this lab, your feedback on the lab and your experiences with it is very important to us.