TD SYNNEX

SITE RECOVERY ON AZURE

Step-by-Step Deployment Guide

TD SYNNEX

1. TD SYNNEX Azure Site Recovery Step by Step. 3

1.0 Things to know prior to using this Guide 3

1.1 Azure Site Recovery deployment 4

1.2 How to connect 20

1.3 Post-Deployment Tasks 47

2. Azure Notions 62

1. TD SYNNEX Site Recovery Step by Step

1.0 Things to know prior to using this Guide

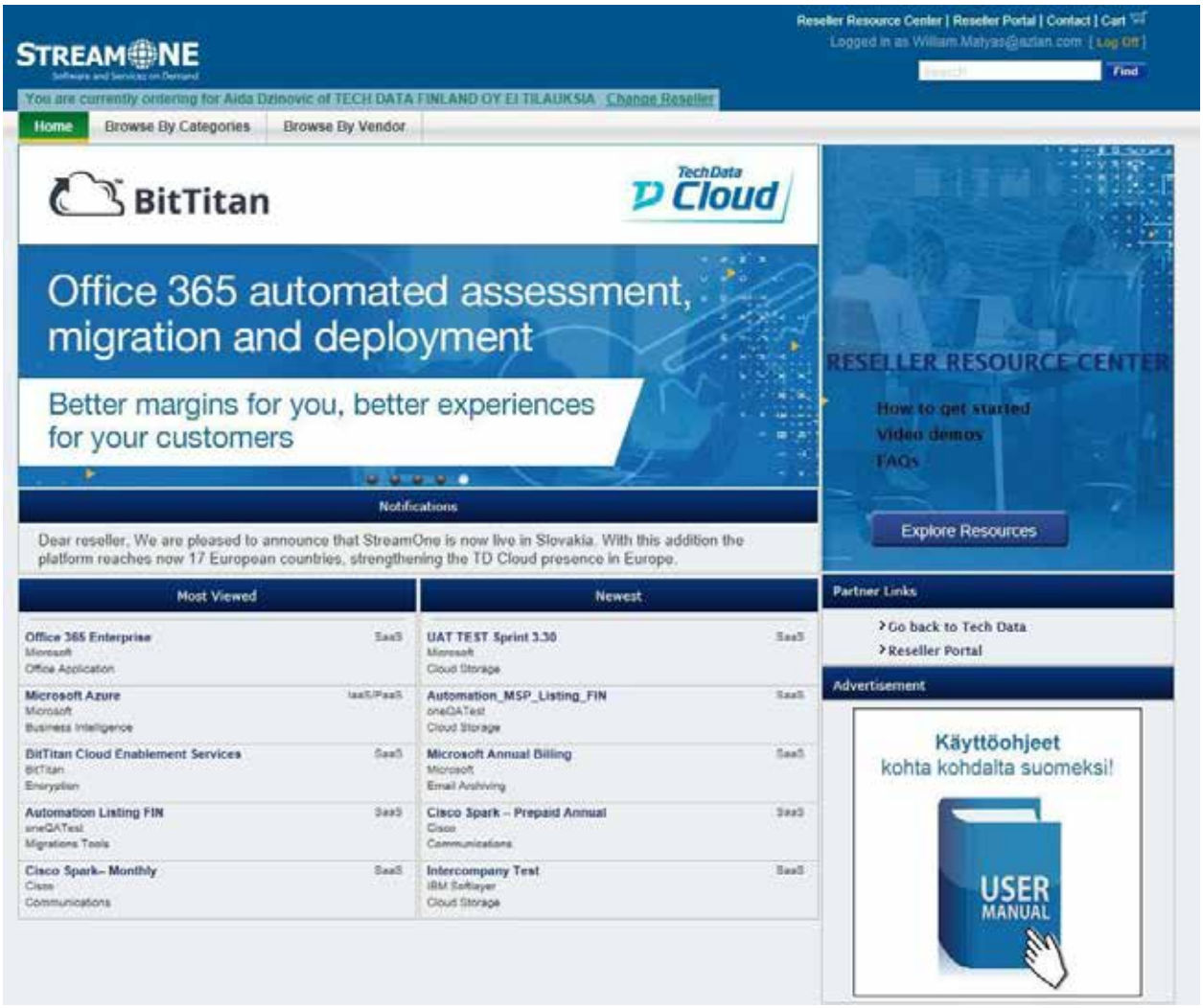
- You would need to familiarize yourself with this document prior to diving in.
- All the Screen Shots in this Guide are for reference only.
- This Guide will assist you with the deployment of the Azure Site Recovery Bundle in an Azure CSP subscription that was purchased through the StreamOnePortal. In depth training on Azure is outside of this guide.

- *Accessing the Azure Site Recovery in Azure*
  You would need to login to the Azure portal to get the IP address
  - **https://portal.azure.com**
  - You would need to login using the same user name and password as the one created in StreamOne and what was emailed to you.

- For example: **john.doe@contoso.onmicrosoft.com**
- It will give you a one-time password and you will need to change it.
  - To access the Azure Backup, you must ensure you have the **Login** and **Password** that were created during the StreamOne ordering process.
  - If you were not the person who accessed the StreamOne ordering portal to do the
  - purchasing, please get with that person and obtain the user login and password that were initially created.

1.1 Azure Backup on Azure deployment.

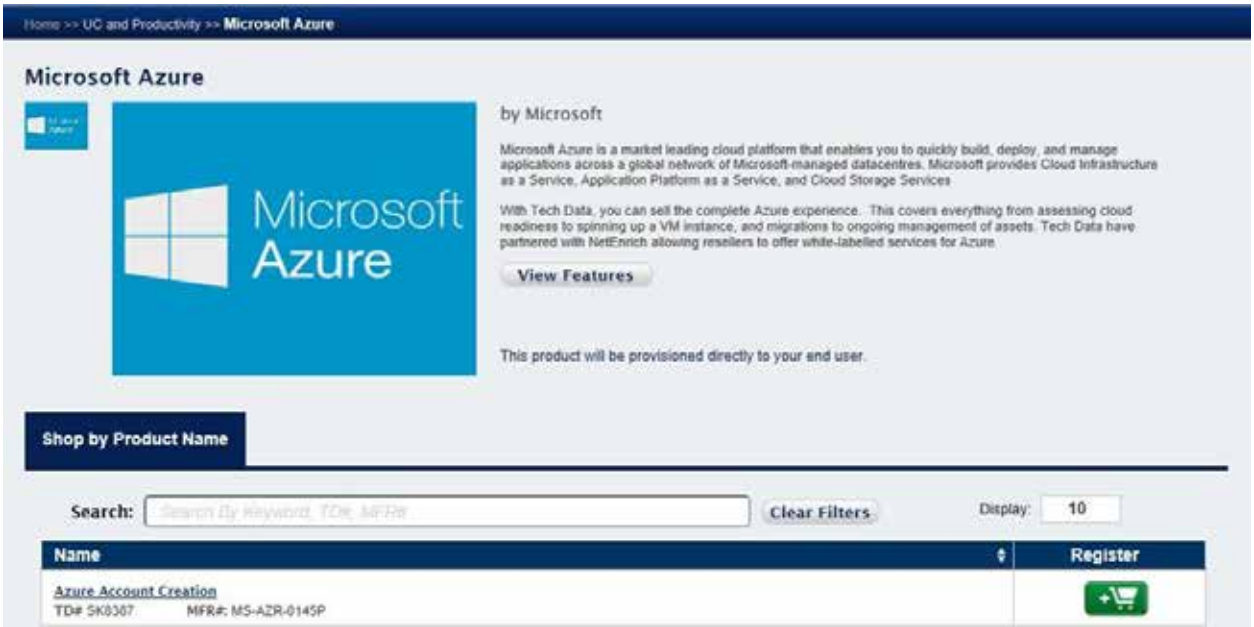
Connect to StreamOne Cloud Marketplace:



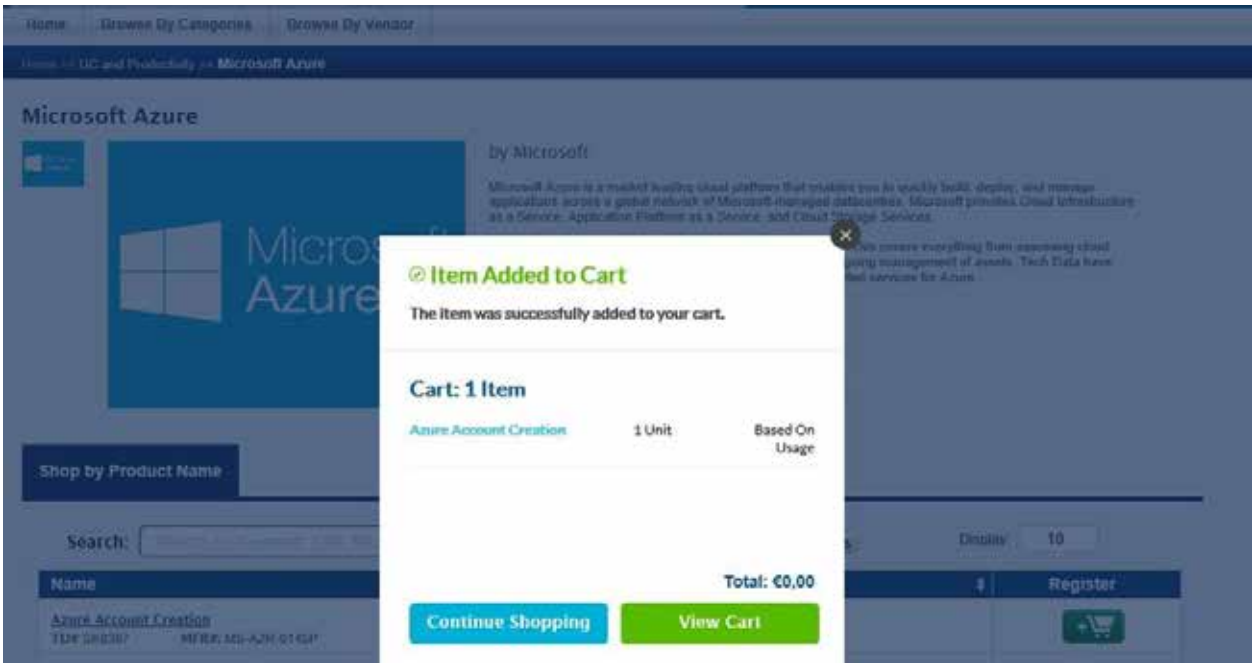
You can search for the Microsoft Azure SKU in Most Viewed, browsing by Categories or Vendor, or directly searching for it in the search field:

Click on Microsoft Azure:

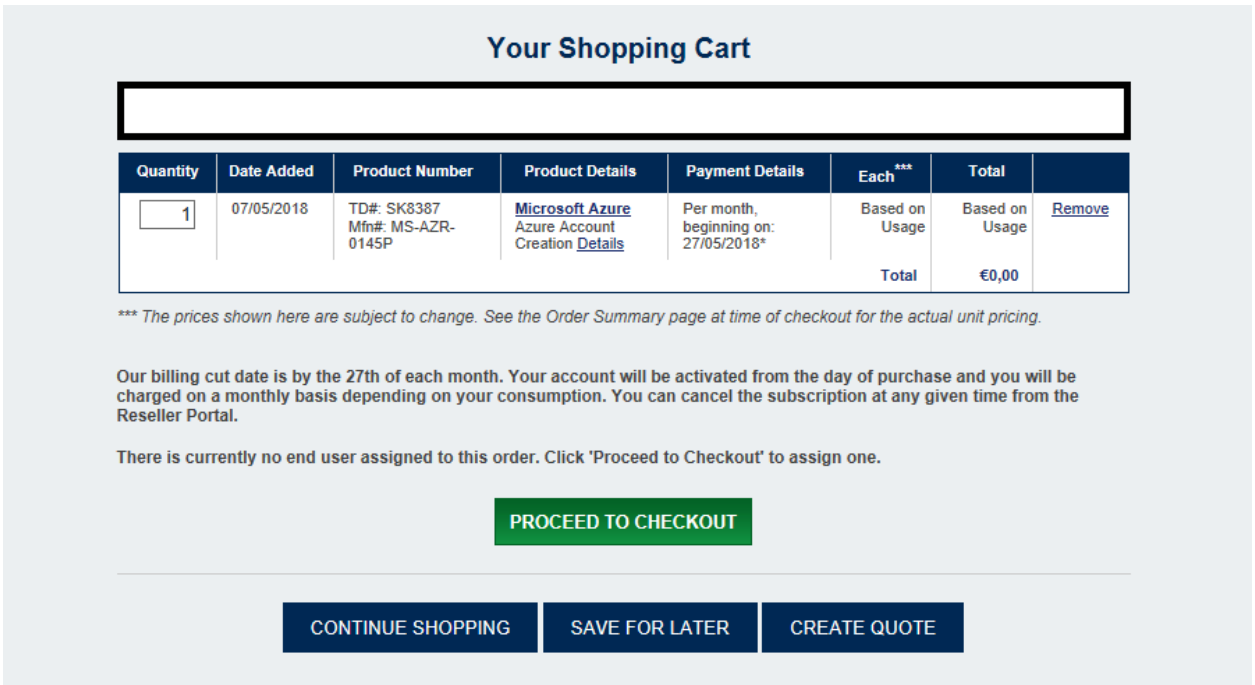
Click on "ADD TO CART" button of registration SKU:



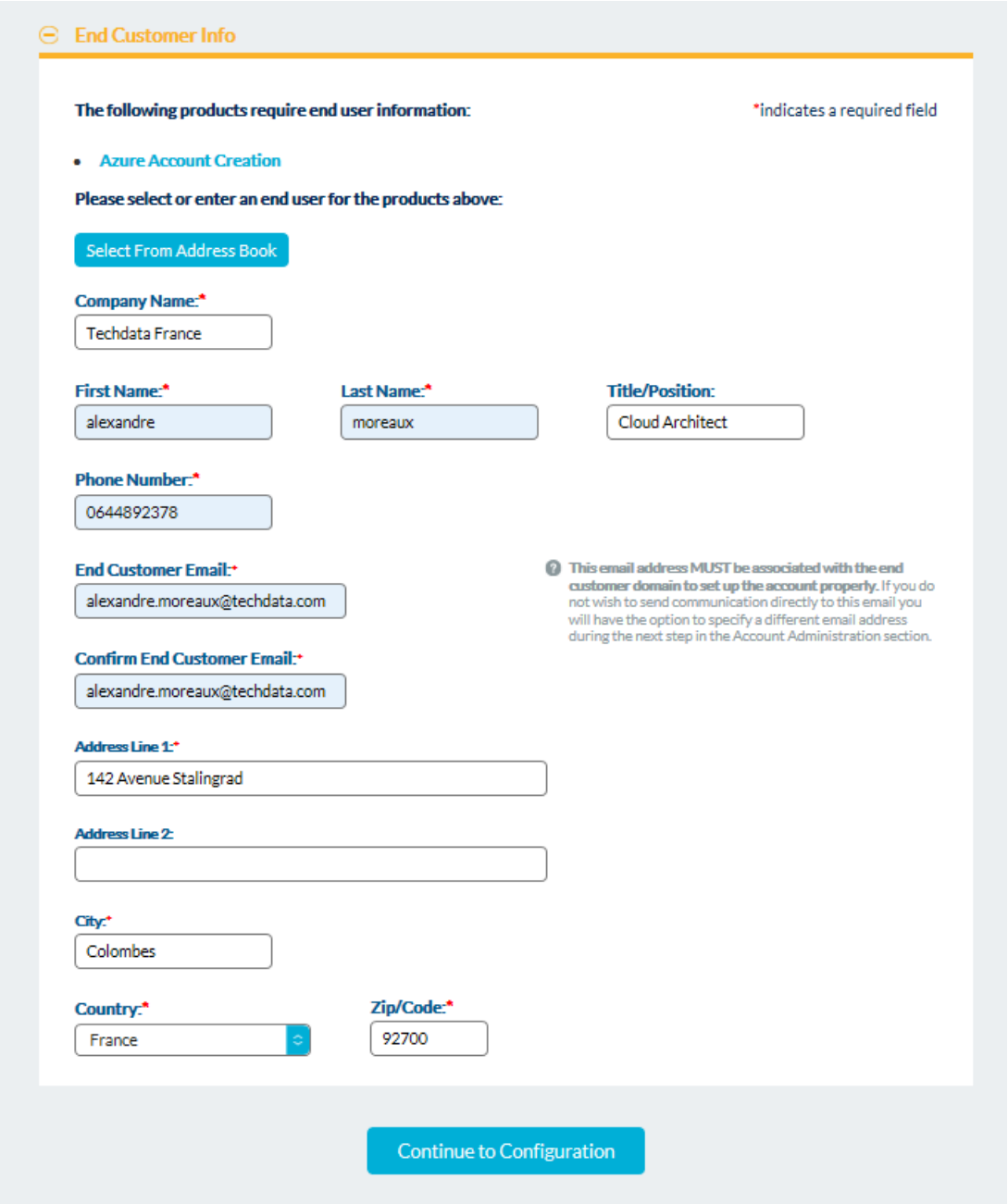
Click on "View Cart" button:



Click on 'Proceed to Checkout' button:



Fill End User information or select any end user using your email and click on "Continue to Configuration" button.

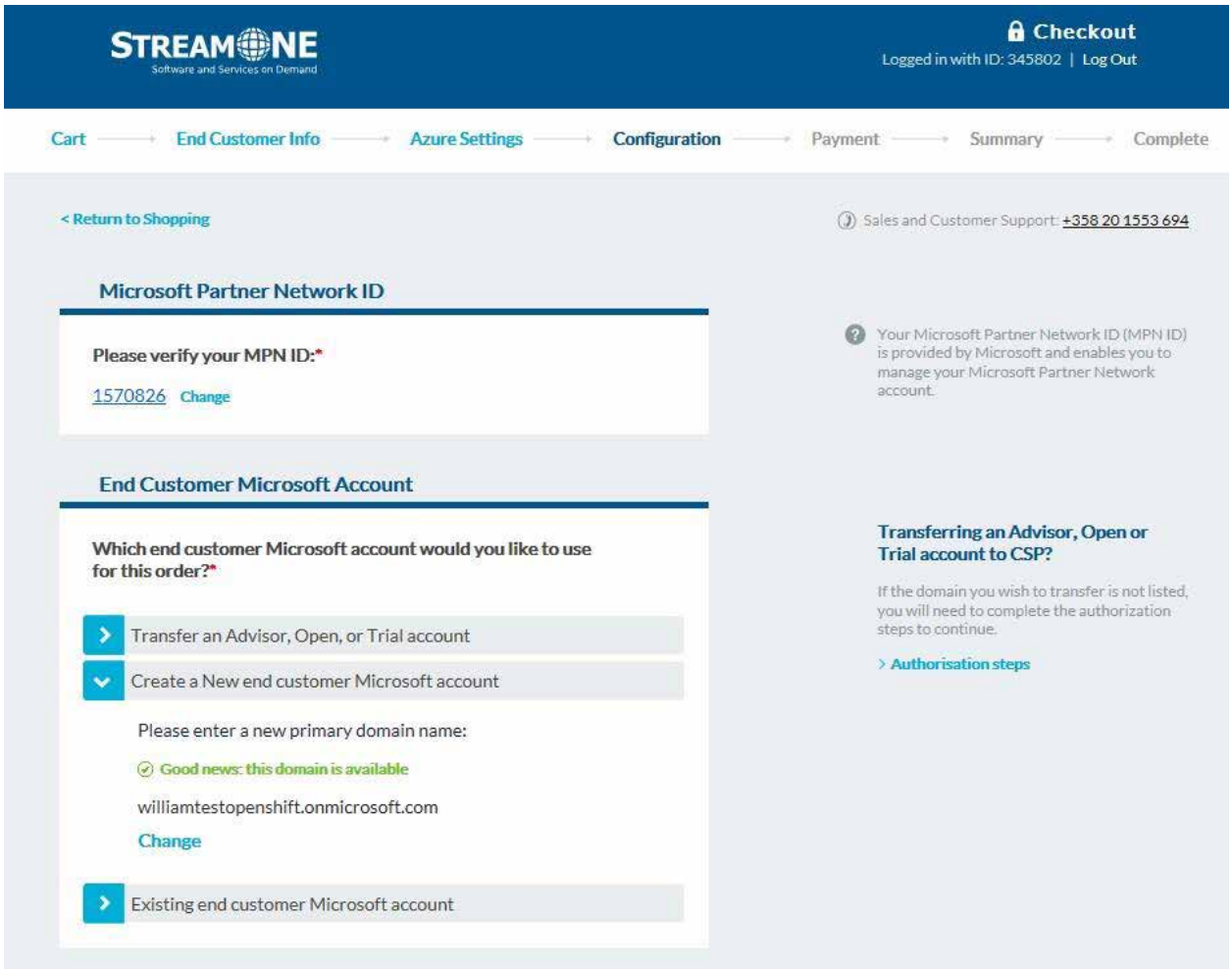


Click on "Continue Configuration" button available in Bundle Summary section.

Configuration page should be displayed.

Fill in your Microsoft Partner Network ID.

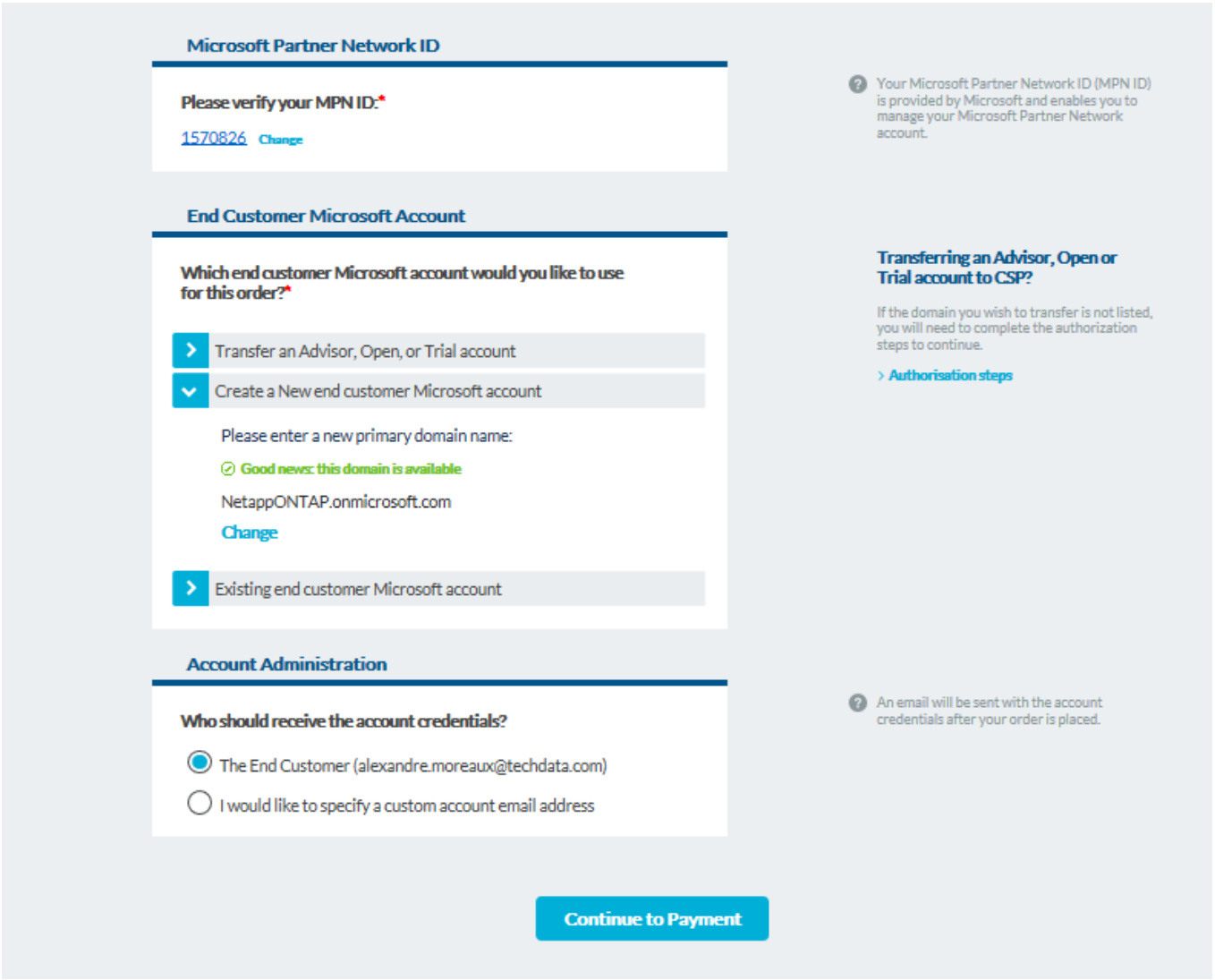
Click on Create a New end customer Microsoft account button.



Enter any unique domain name and click on Check Availability button.

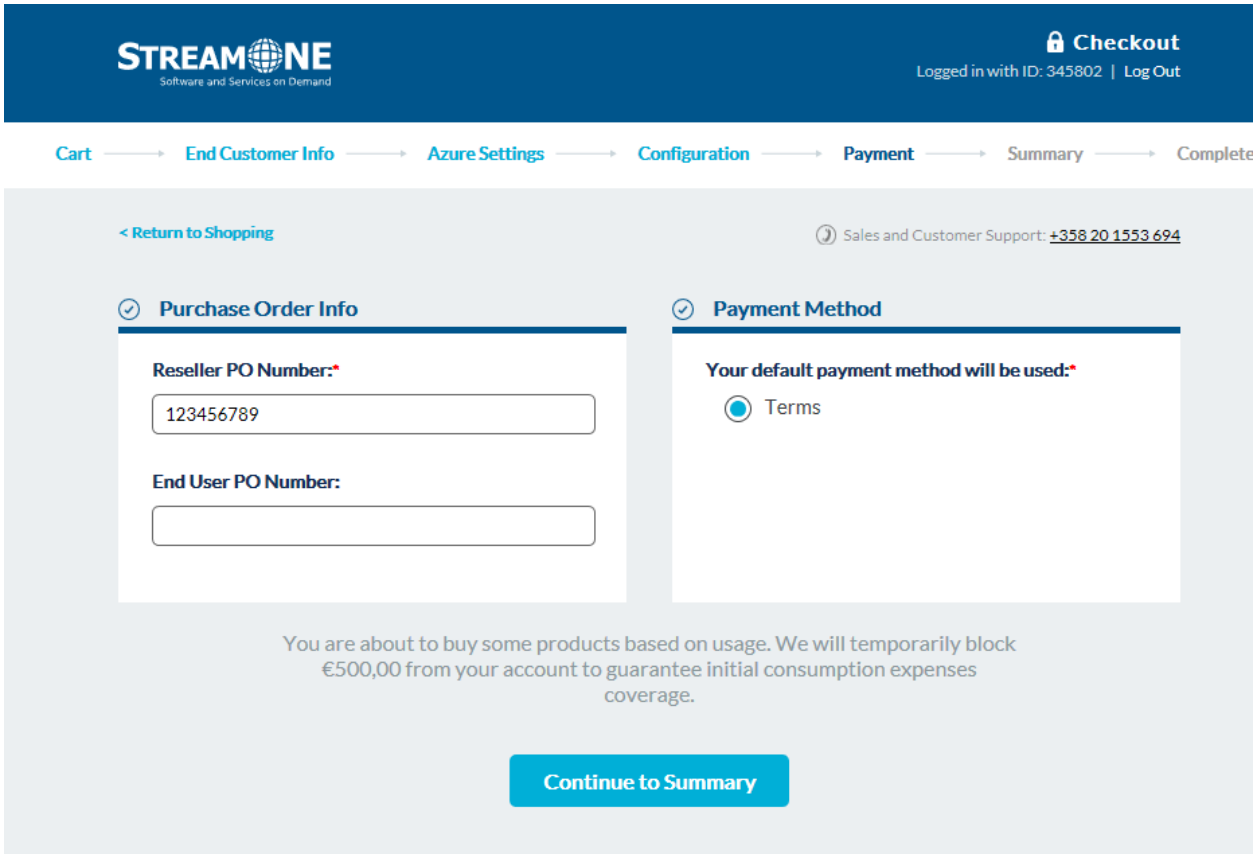
Select "The End Customer email" radio button from the "Account Administration" module.

Or select "I will administer the account" radio button from the account administration module and enter the Delegate admin email ID.



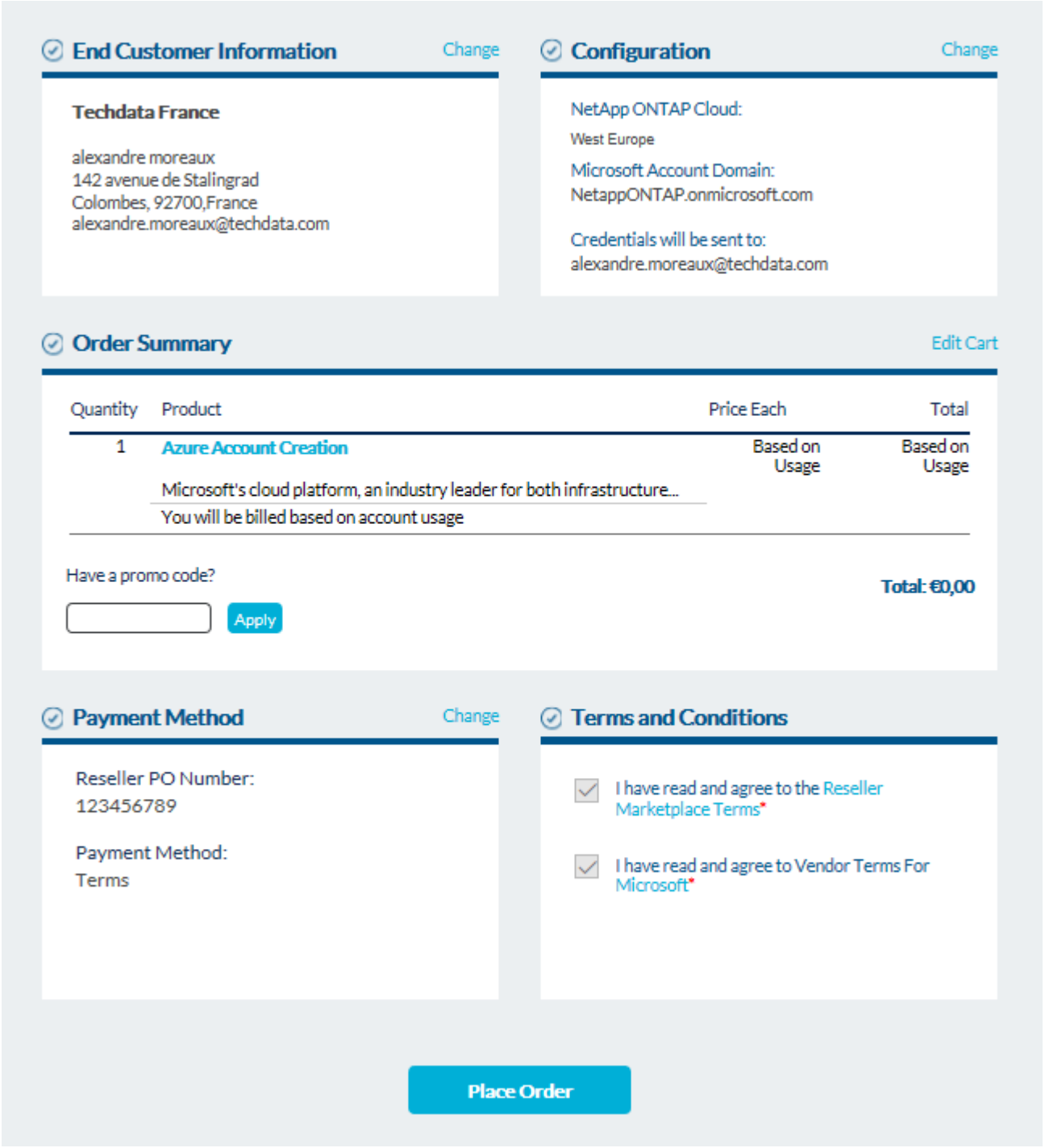
Click on "Continue to Payment" button.

Enter Reseller PO number.

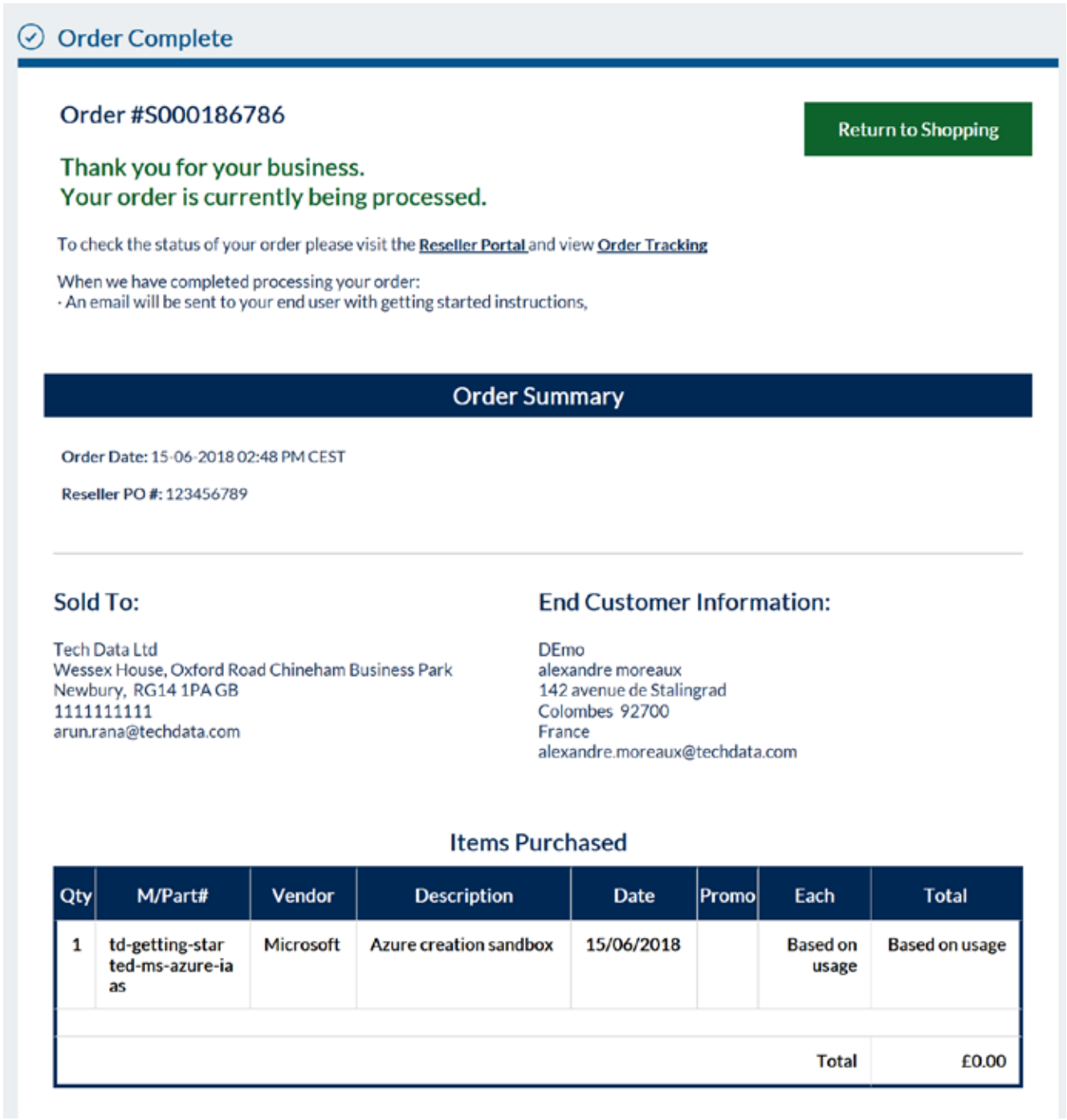


Click on "Continue to Summary" button.

Verify the information shown and click on "Place Order" button.



Your order should be complete.



Order Complete

Order #S000186786

Return to Shopping

Thank you for your business.
Your order is currently being processed.

To check the status of your order please visit the Reseller Portal and view Order Tracking

When we have completed processing your order:
· An email will be sent to your end user with getting started instructions,

Order Summary

Order Date: 15-06-2018 02:48 PM CEST

Reseller PO #: 123456789

Sold To:

Tech Data Ltd
Wessex House, Oxford Road Chineham Business Park
Newbury, RG14 1PA GB
1111111111
arun.rana@techdata.com

End Customer Information:

DEmo
alexandre moreaux
142 avenue de Stalingrad
Colombes 92700
France
alexandre.moreaux@techdata.com

Items Purchased

Qty	M/Part#	Vendor	Description	Date	Promo	Each	Total
1	td-getting-started-ms-azure-iaas	Microsoft	Azure creation sandbox	15/06/2018		Based on usage	Based on usage
						Total	£0.00

You should receive an email with your Microsoft Subscription Informations:

Dear alexandre moreaux,

Your Microsoft account has been setup.

Please continue to https://login.microsoftonline.com and login with the username and password below for your Office 365 subscriptions.
For Azure, please use https://portal.azure.com/

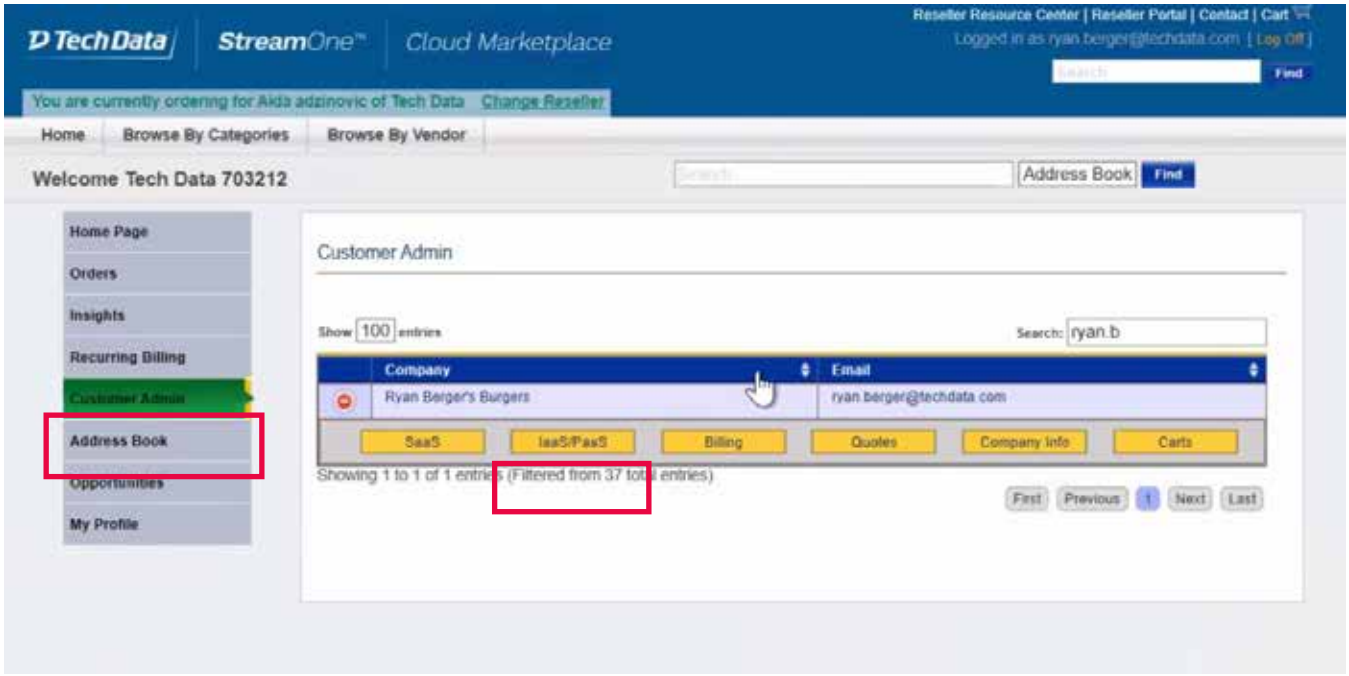
Username: admin@alexandreNETAPP2.onmicrosoft.com

Password: [X3)Nu(3

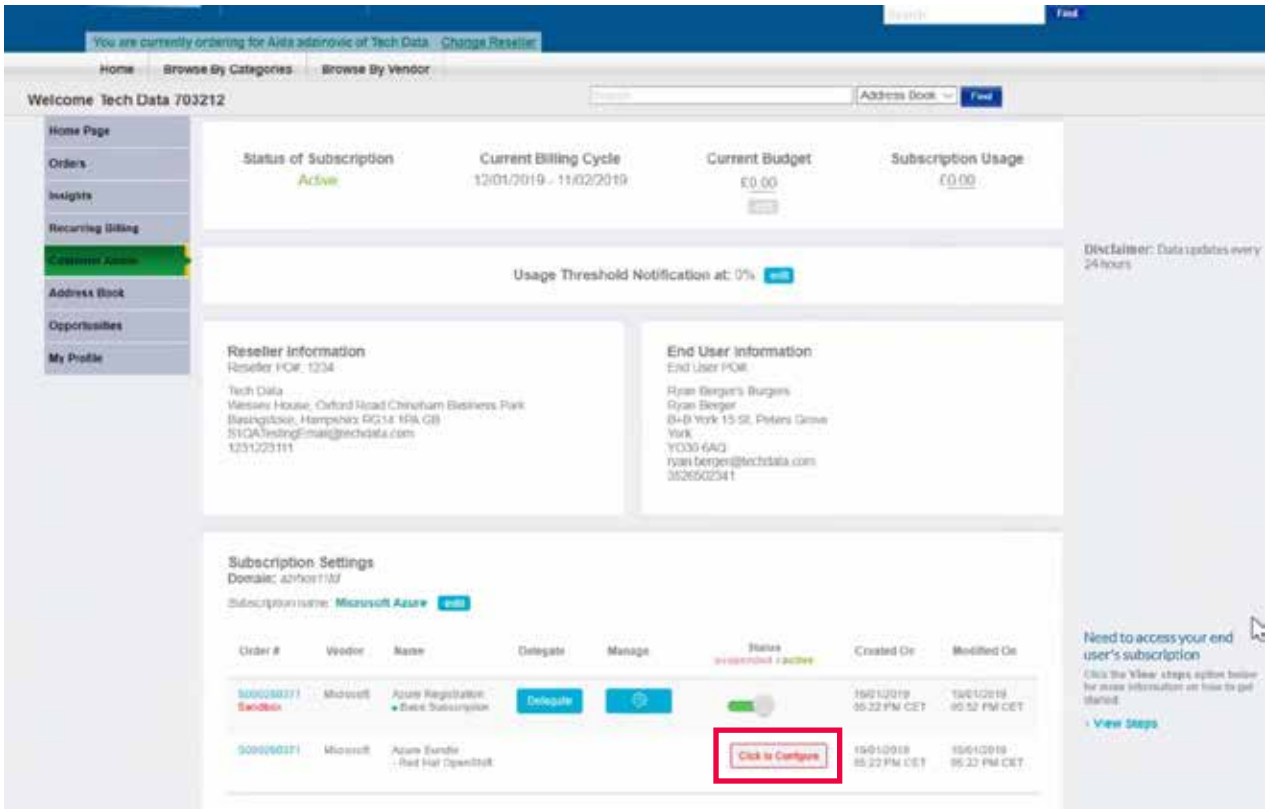
Your Subscriptions:

Name	Quantity
Azure Account Creation	1

Now click on Reseller Portal, then Customer Admin. Look for your Customer and click on IaaS/PaaS.



Then click on “Click to Configure”:



ASR post deployment with Hyper-V Source

Register your Hyper-V host(s)

On-premises

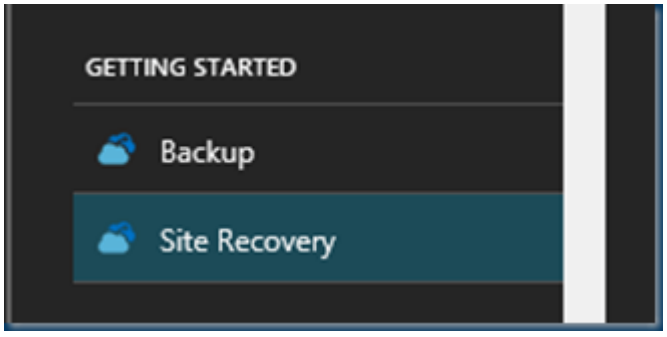
Make sure the host is running Windows Server 2012 R2 or above.

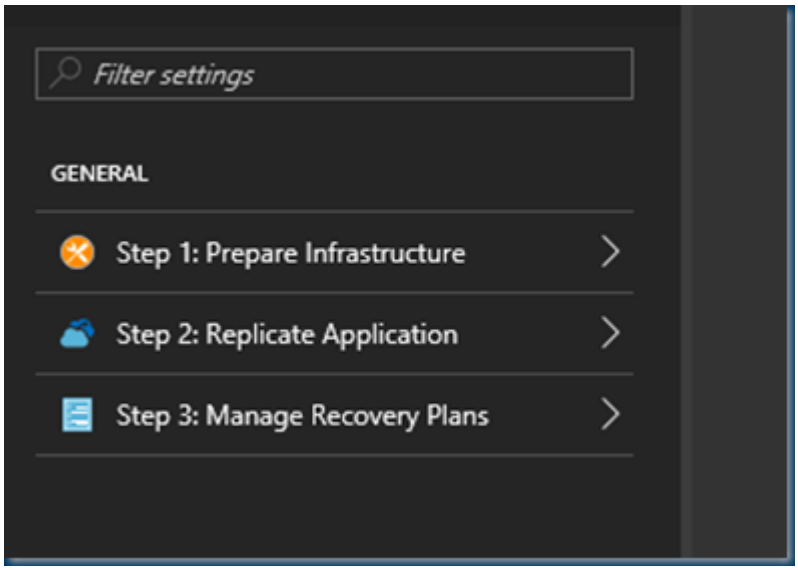
Download the Agent

The installer for the Microsoft Azure Site Recovery Provider.

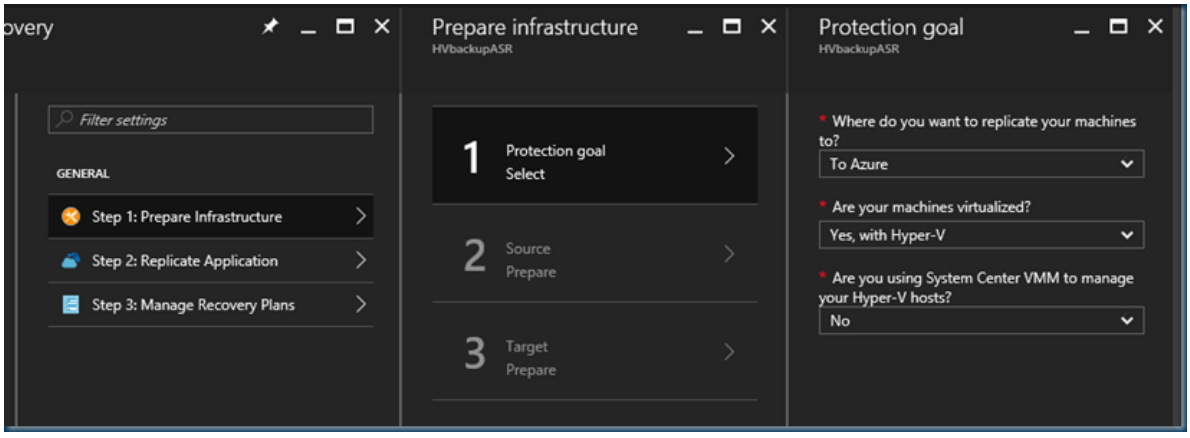
Download the vault registration key to register the host in a Hyper-V site

This download is replication agent to Azure and need to be installed on the Hyper-v Server



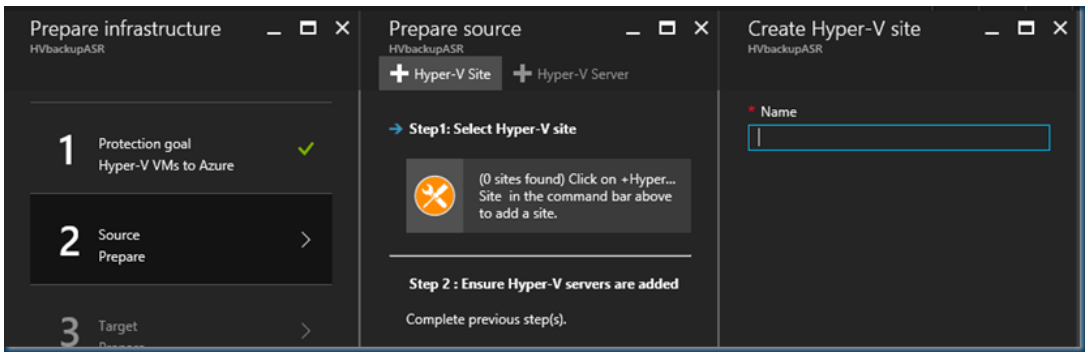


Selecting the Site Recovery and start with Step 1



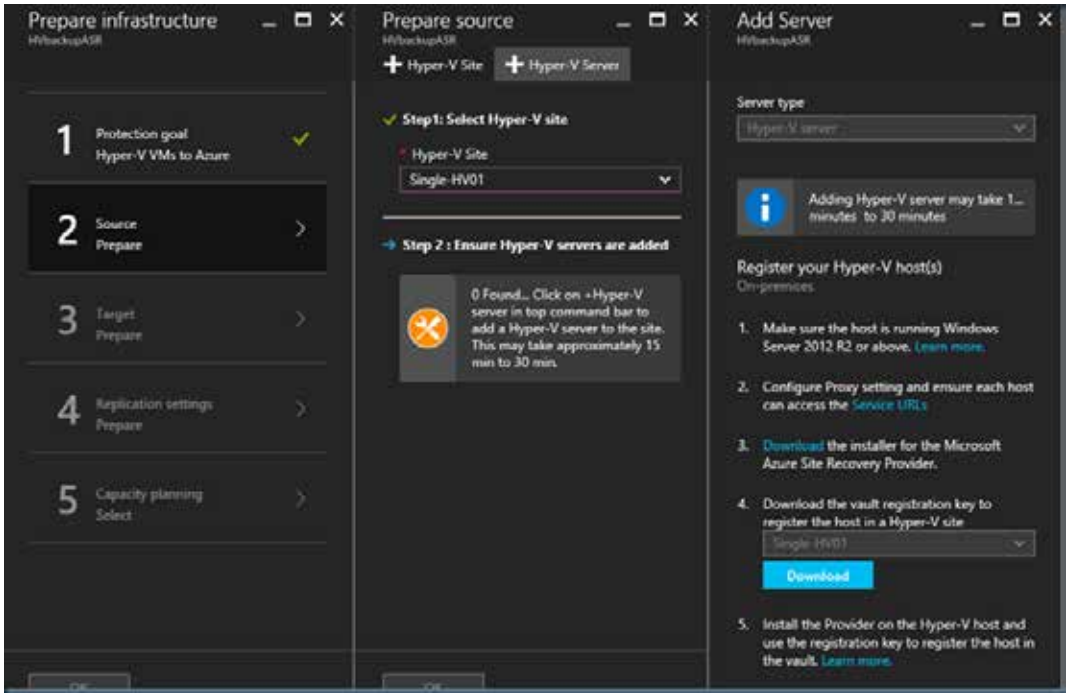
In this step We select our Protection goal select To Azure, and select Yes, with Hyper-V.

Select No to confirm you're not using VMM.

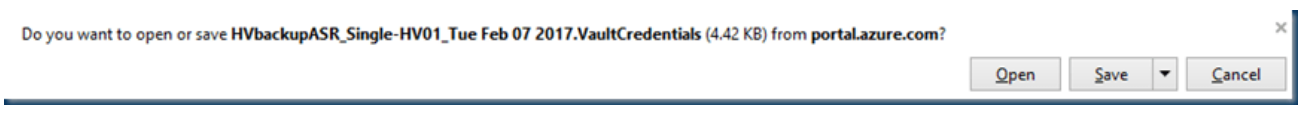


We need to create a Site of this hyper-v server.

This is a Cosmetic name and points to the Hyper-v server or servers, if this is a Test server then this should be HVtest etc.

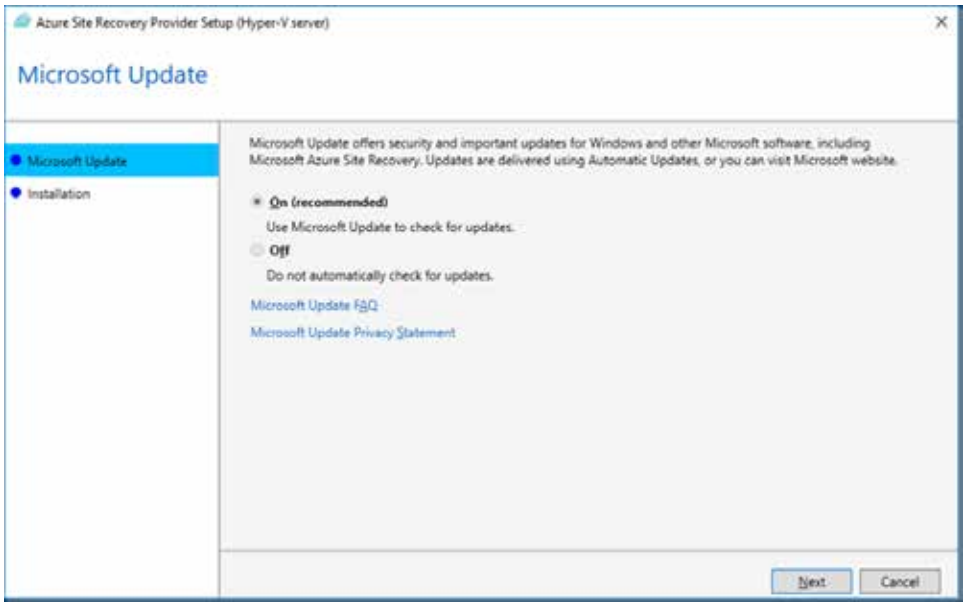


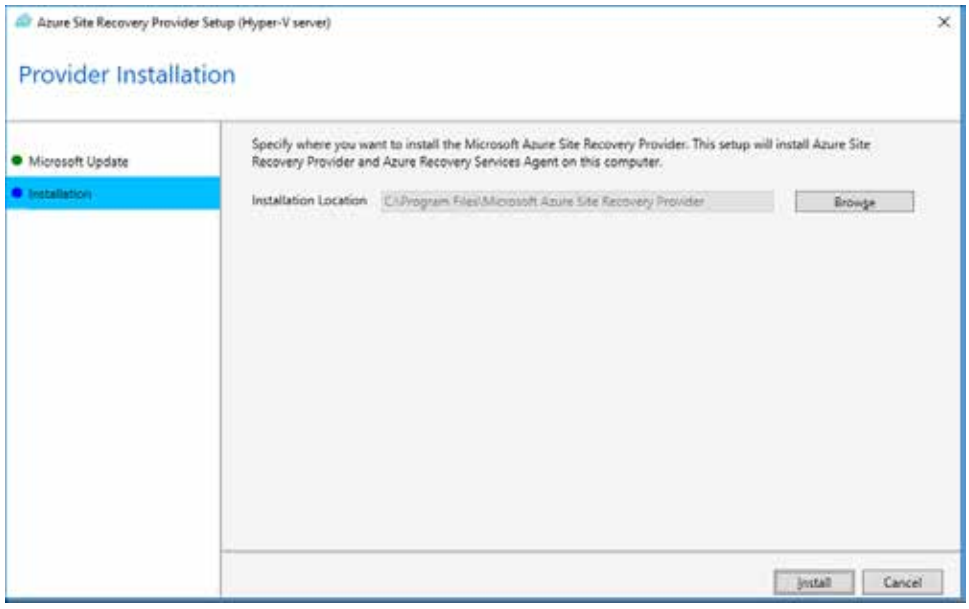
I need to install the Agent and use the vault keys to connect to Azure.
Also downloaded here



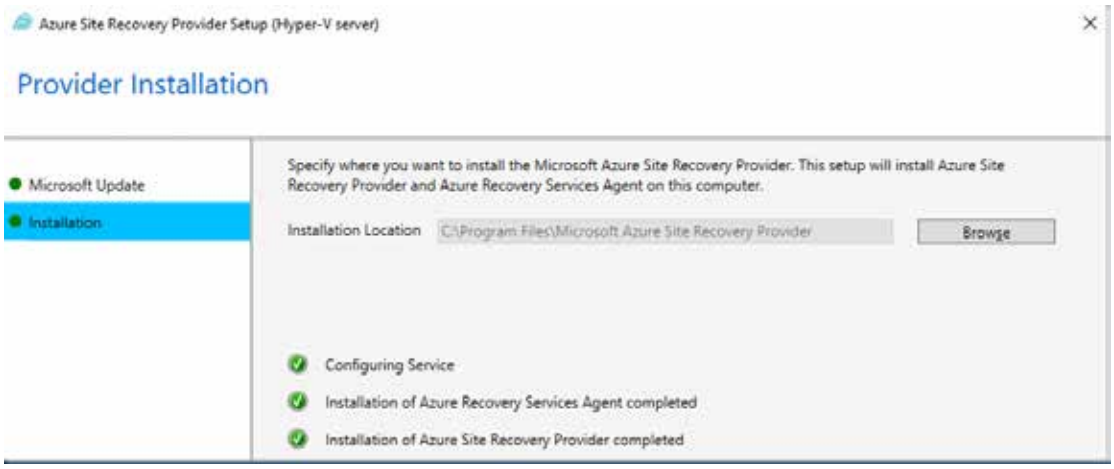
Installing the Hyper-v Agent

Use the Exe just downloaded and follow the steps.

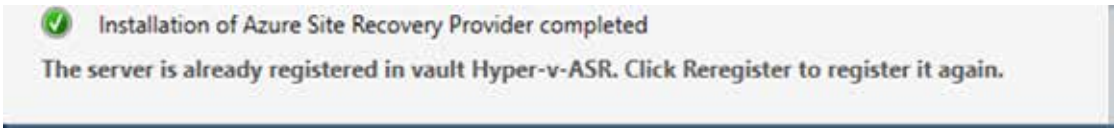




Use a location be careful if not installing on the C drive and not replication the other drive there can be miscommunication in the VM. Better leave this default.



But in case You already played with this or want different naming and started all over the may be an issue " the server is already registered"

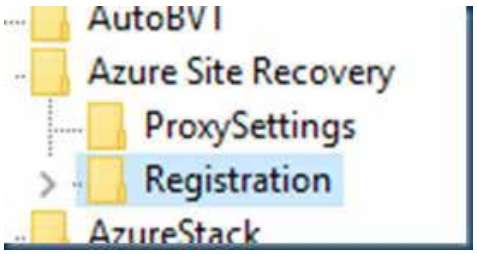


To fix this error and enable the ASR Provider and agent setup to complete successfully, follow these steps:

Go to the Register

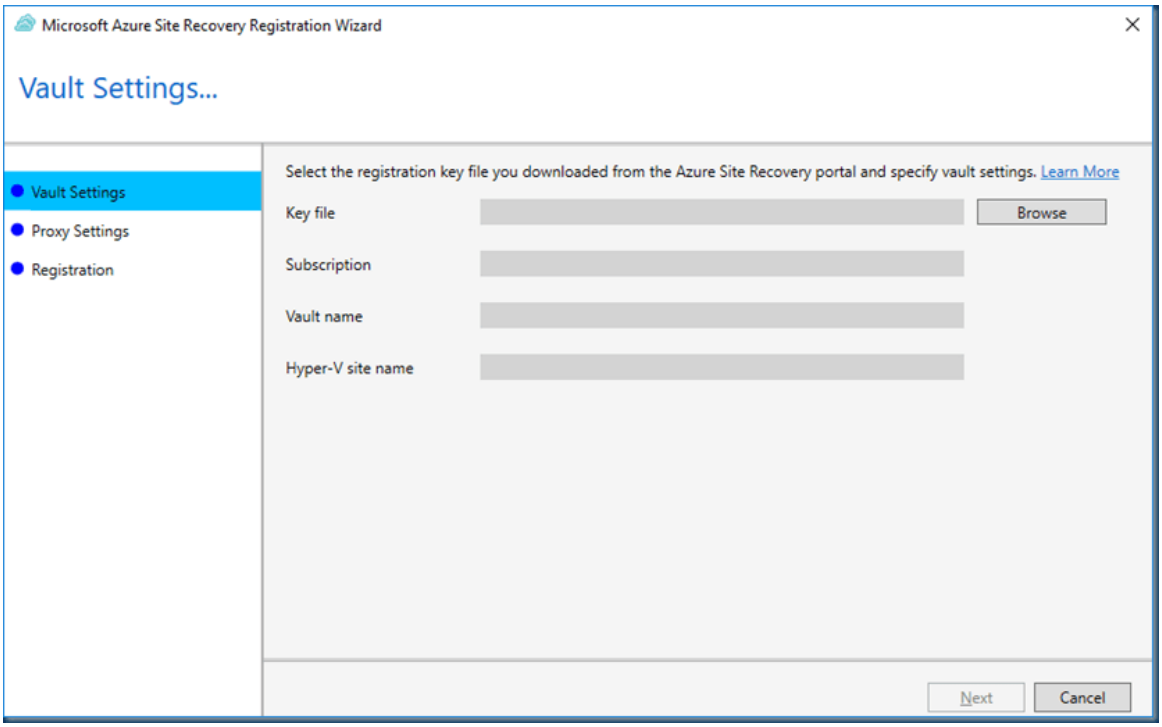
Make a backup of the following registry key:

HKEY_LOCAL_MACHINESOFTWAREMicrosoftAzure Site Recovery

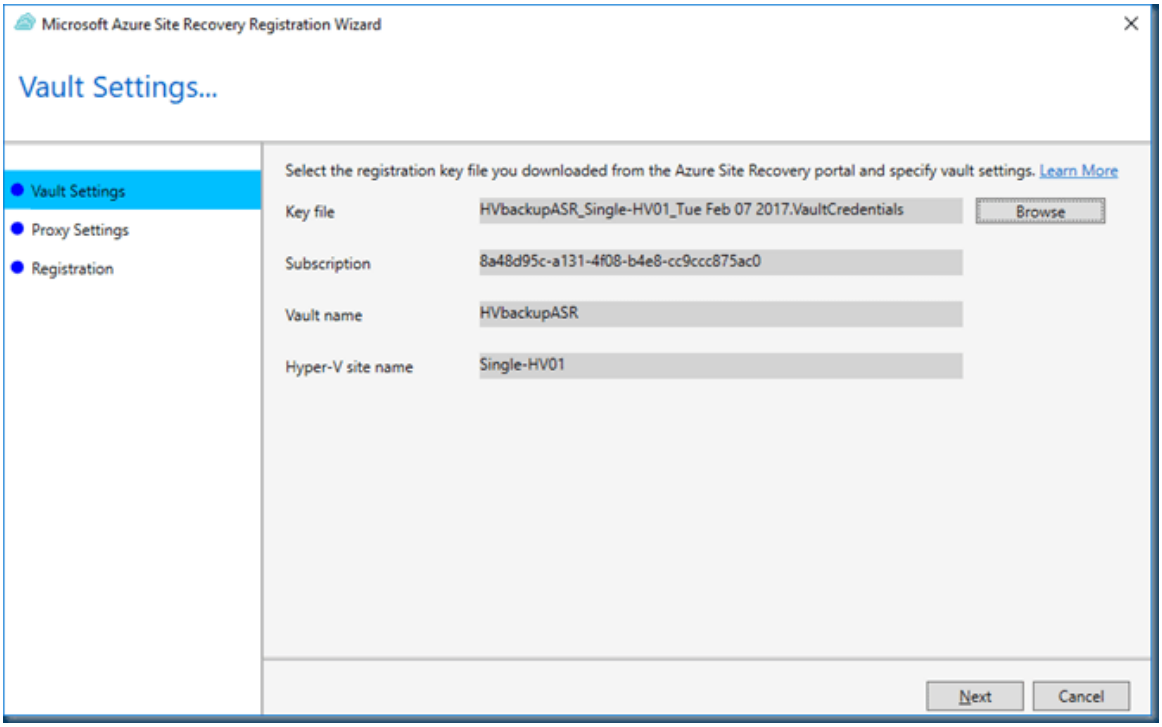


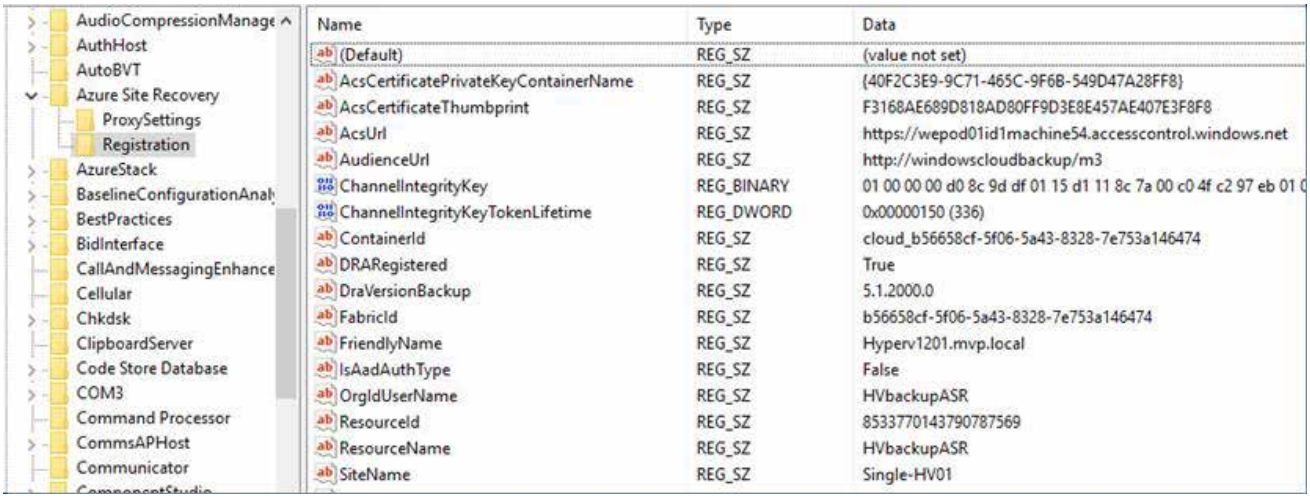
Delete the registry key that you backed up in step 2.

Restart the Provider and agent setup.

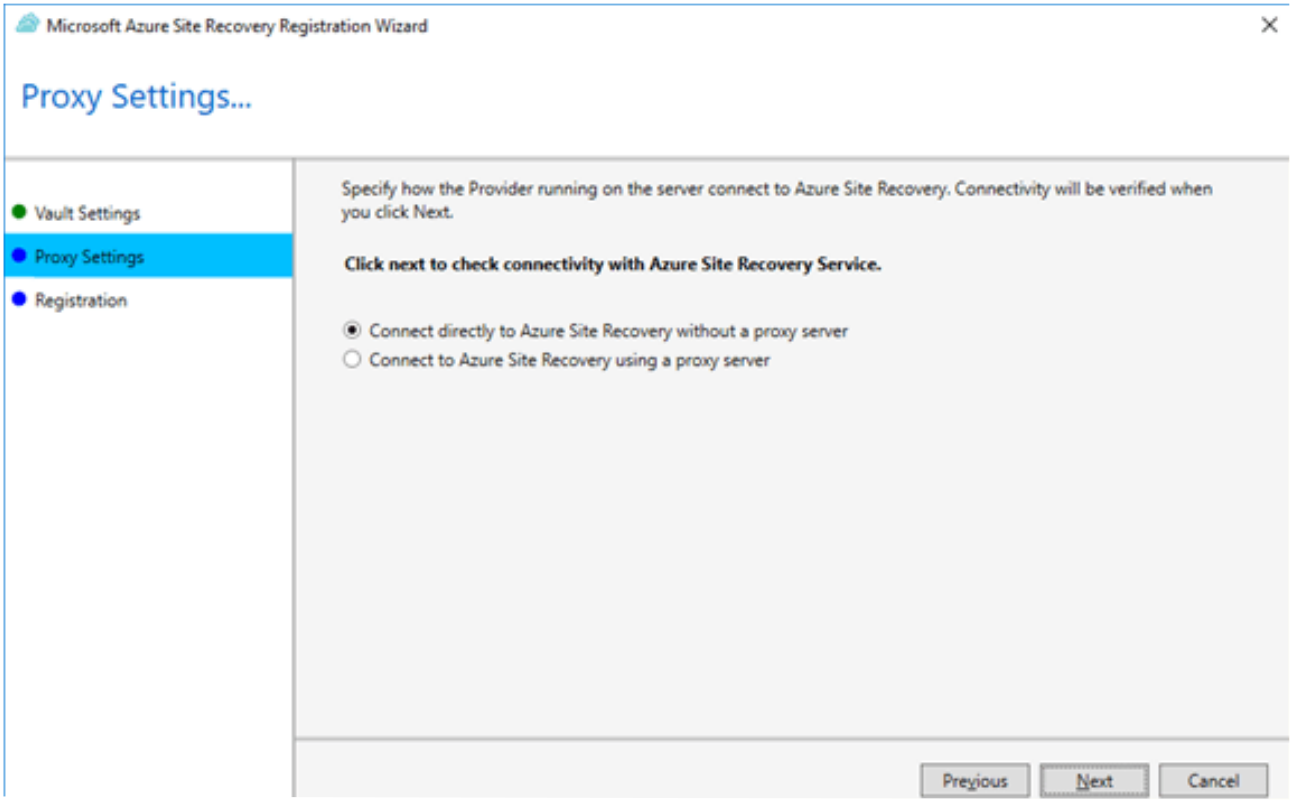


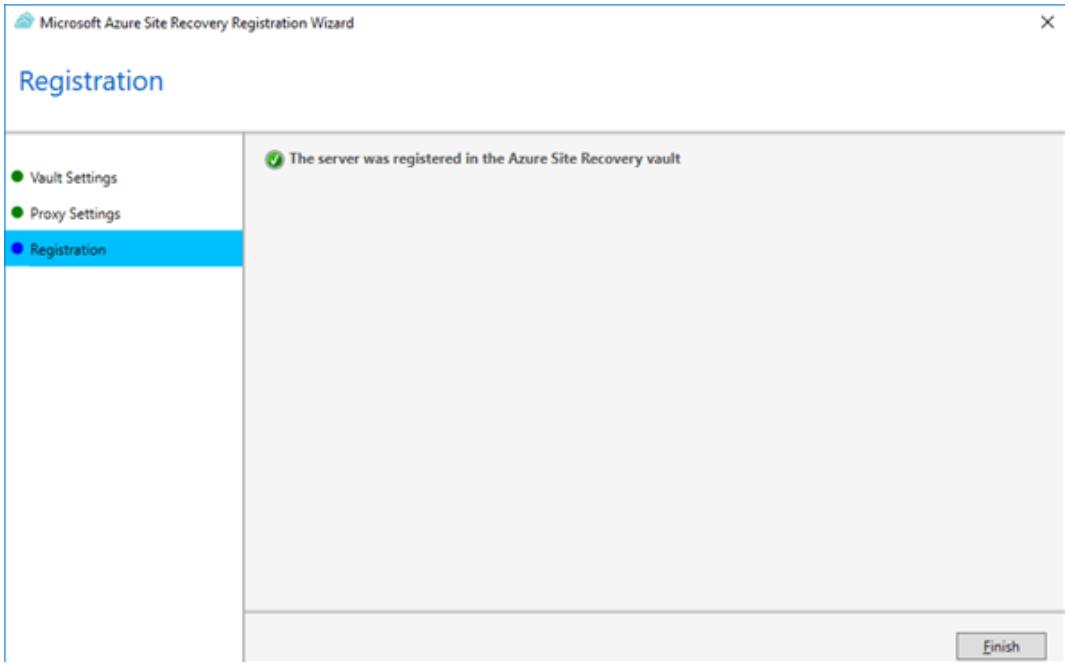
Use the downloaded Keys and import them.



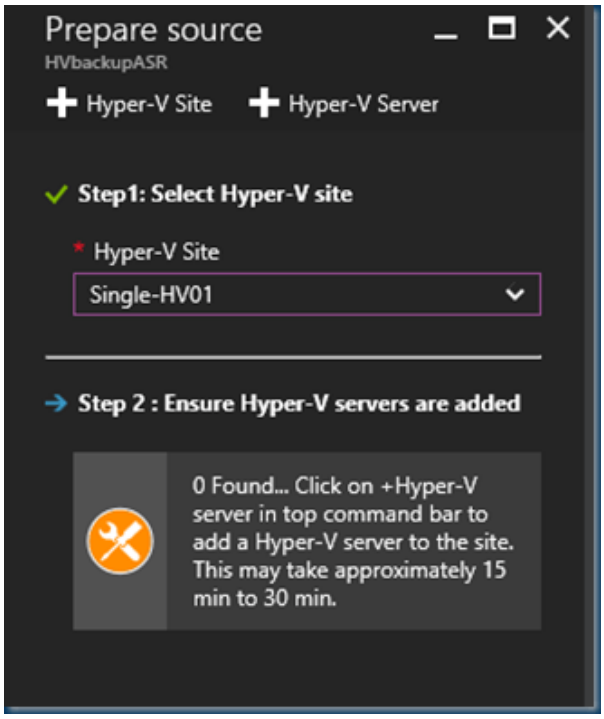


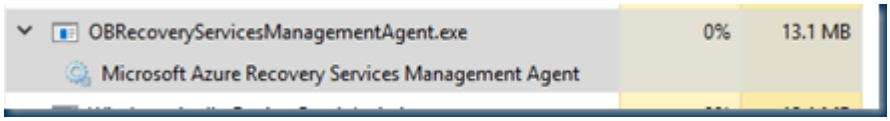
Checking the Register you can see that the key is valid and all the info is there.



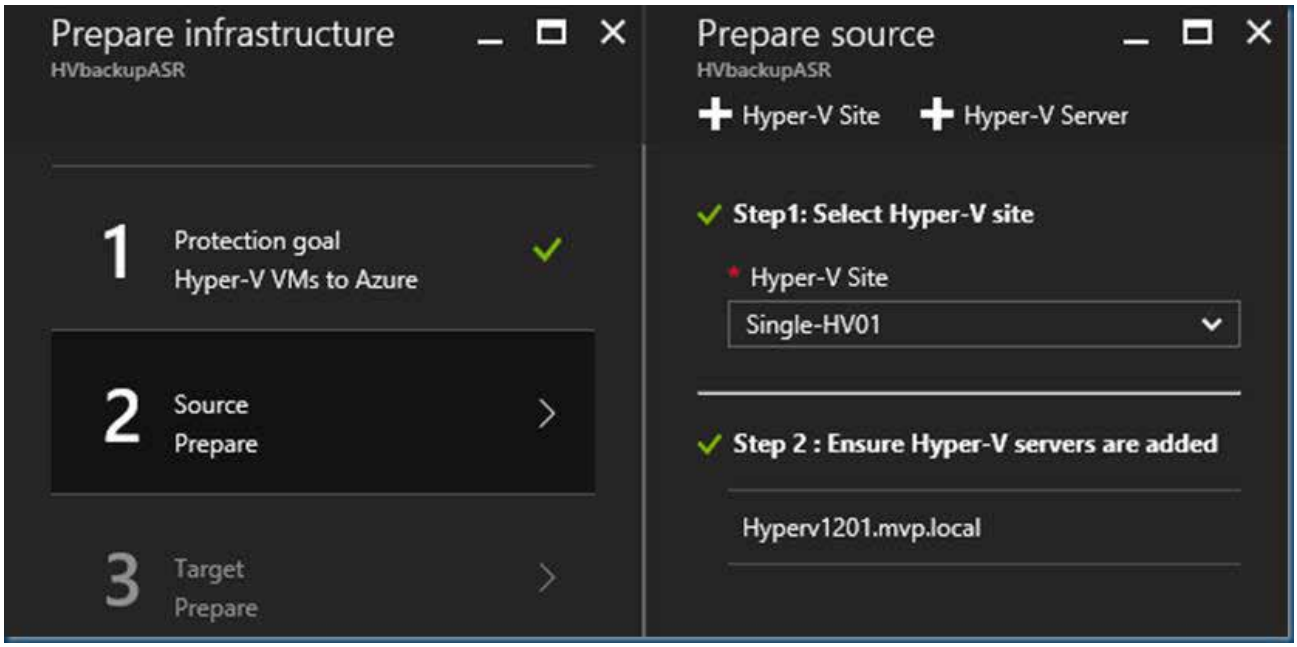


And the installation is done. It can take some time to add the server to Azure maybe several hops back and forth to the menu

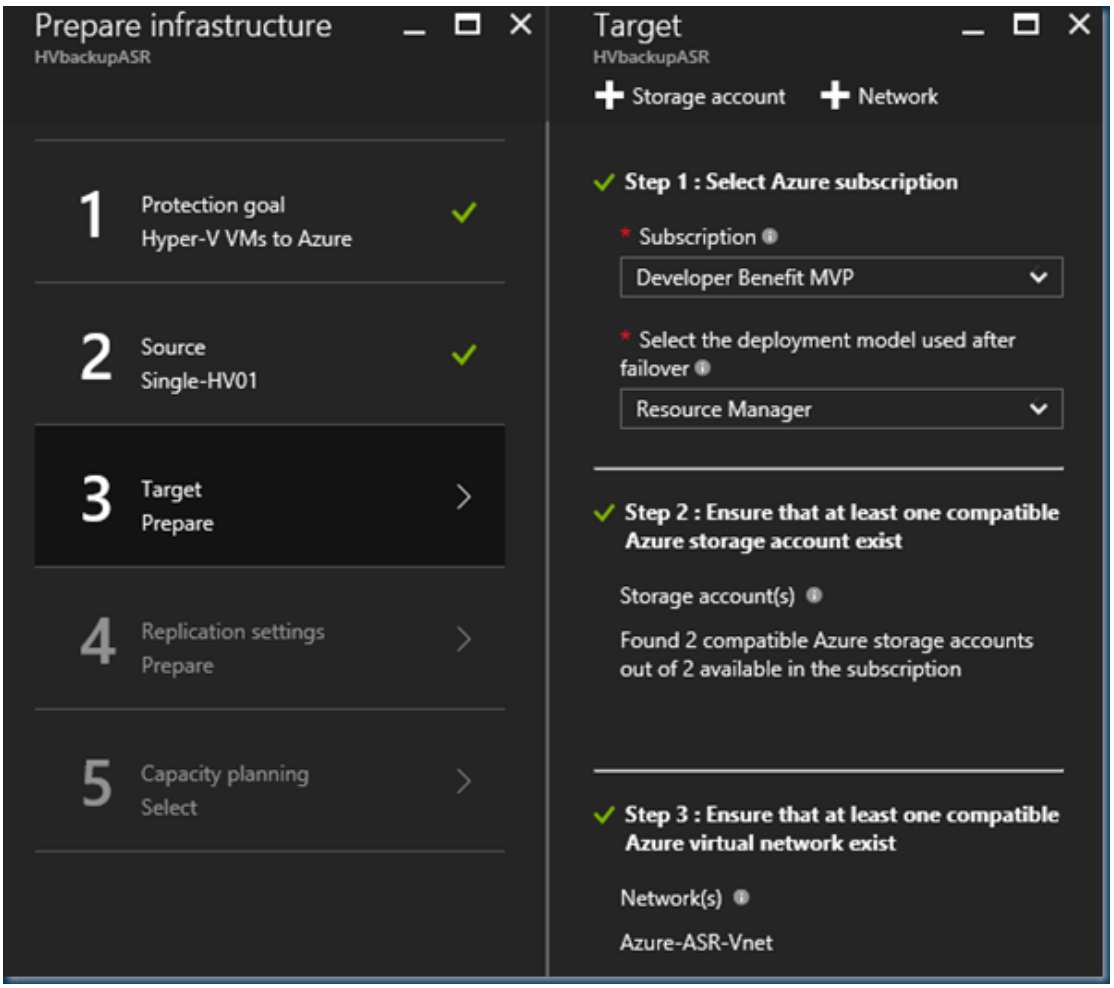




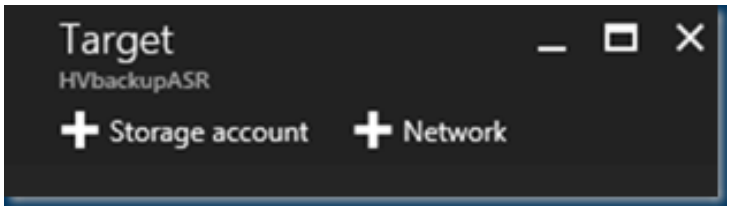
You can see the process running in the Task manager.



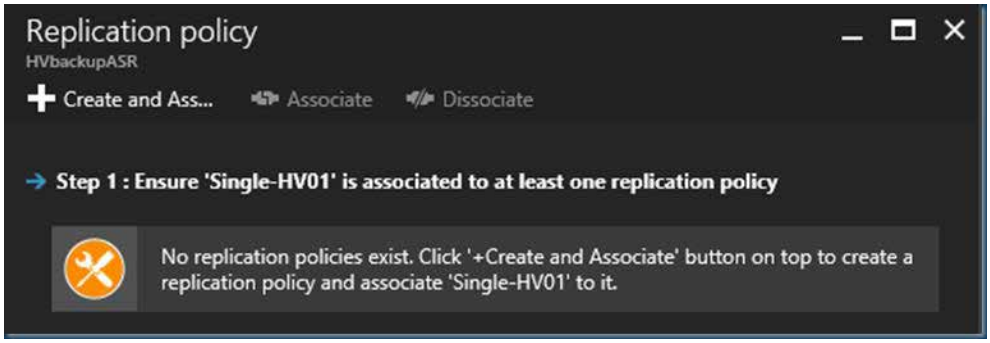
Jumping back and to the step 2 you can see the Hyper-v server is added to the Vault.



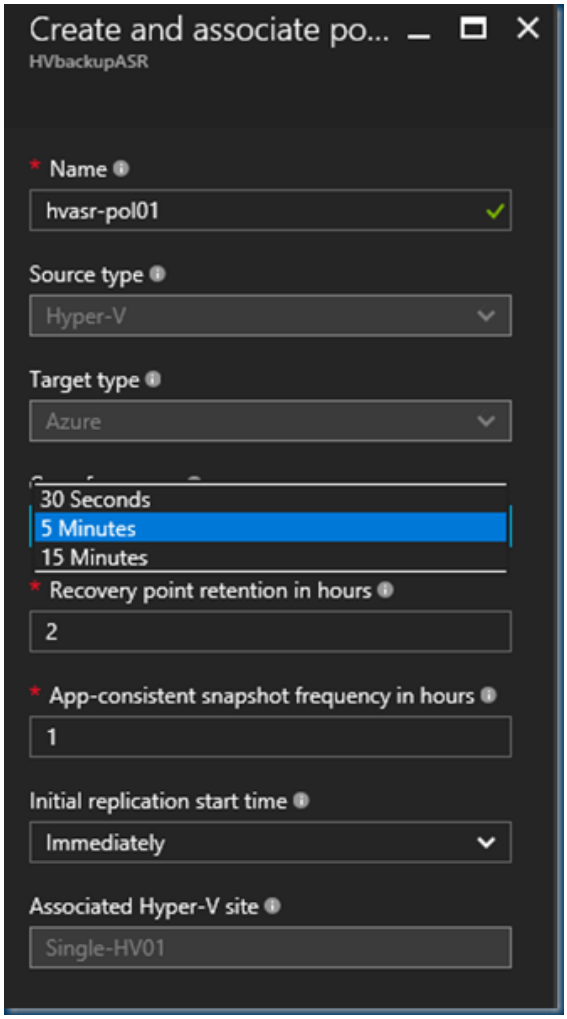
Added a storage account and a network. If this is not the storage account or network you want no worry you can change this before the replication starts.



Check this if you want a new account or different network.



Next step would be creating a replication policy.



In Create and associate policy specify a policy name.

In Copy frequency specify how often you want to replicate delta data after the initial replication (every 30 seconds, 5 or 15 minutes).

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.

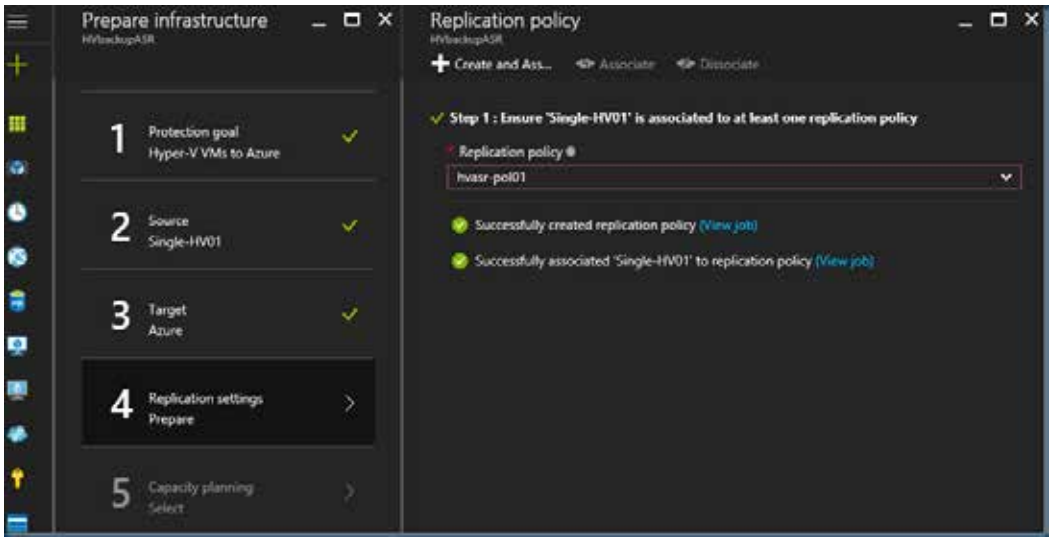
In App-consistent snapshot frequency specify how frequently (1-12 hours) recovery points containing application-consistent snapshots will be created.

Hyper-V uses two types of snapshots — a standard snapshot that provides an incremental snapshot of the entire virtual machine, and an application-consistent snapshot that takes a point-in-time snapshot of the application data inside the virtual machine.

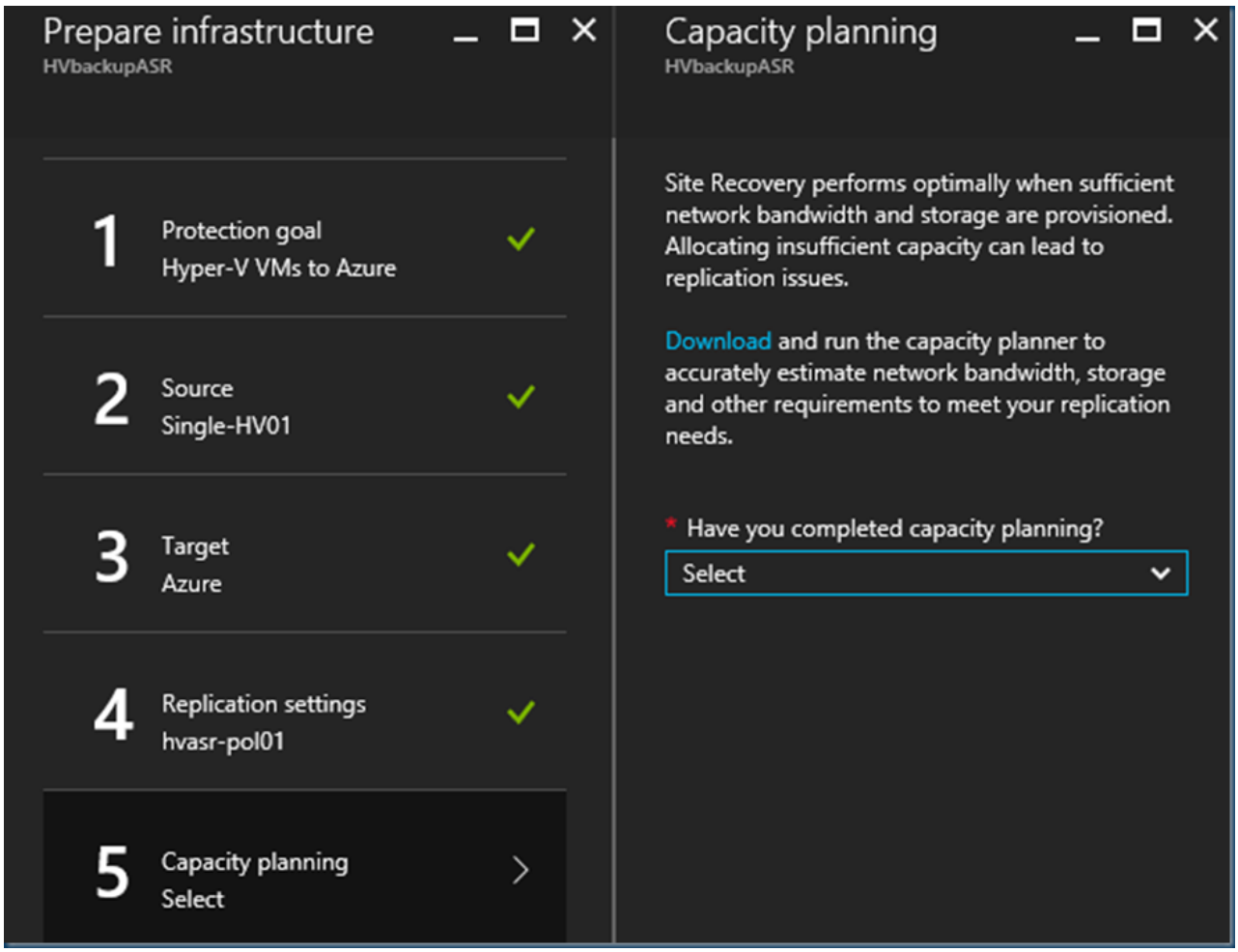
Application-consistent snapshots use Volume Shadow Copy Service (VSS) to ensure that applications are in a consistent state when the snapshot is taken. Note that if you enable application-consistent snapshots, it will affect the performance of applications running on source virtual machines.

Ensure that the value you set is less than the number of additional recovery points you configure.

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 o utside your busy hours.



As you can see the policy's are applied but you can create multiple but you can use only one at each site.



Allocating insufficient capacity can lead to replication issues. Site Recovery provides a capacity planner to help you allocate the right resources for your source environment, the site recovery components, networking and storage.

You can run the planner in quick mode for estimations based on an average number of VMs, disks, and storage, or in detailed mode in which you'll input figures at the workload level.

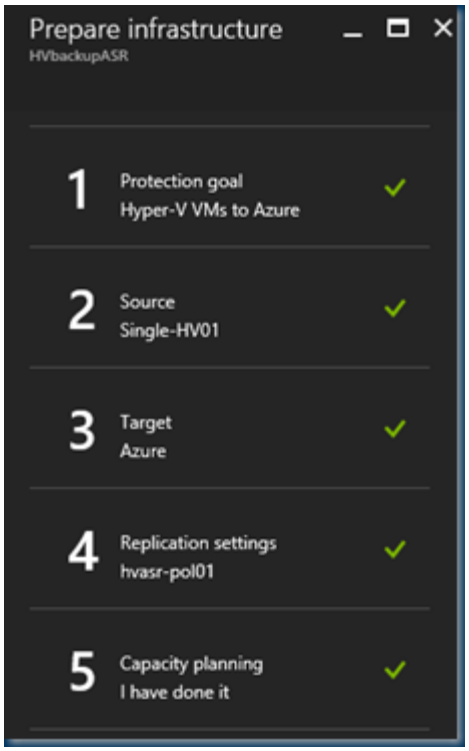
Get the Azure Site Recovery Capacity planner here: Download

Capacity Planner

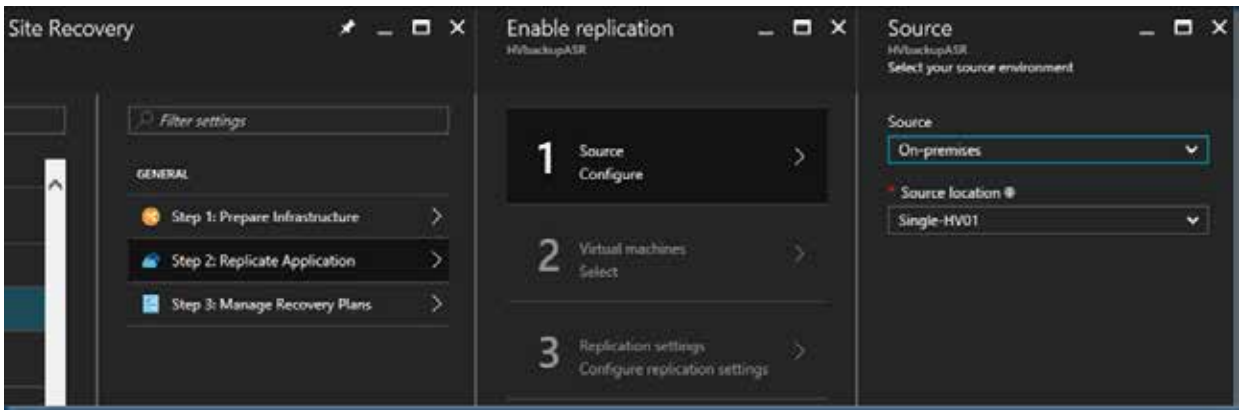
INPUTS			OUTPUT		
Infra Inputs source	Manual	Reset to Defaults	Network Bandwidth requirements		
Select your scenario	Hyper-V to Azure		Bandwidth required for delta replication (in Megabits/sec)	200 Mbps	
Total number of virtual machines	100		Bandwidth required for initial replication (In Megabits/sec)	180 Mbps	Adjust B18,B19 to suit available bandwidth
Average number of VHDs per virtual machine	2		Bandwidth refers to dedicated bandwidth for replication.		
Average size of VHD (in GBs)	300		Azure requirements		
Average utilization per disk (%)	70%		Storage required (in GBs)	43400	
Total data to be replicated (in GBs)	42000		Total IOPS on standard storage accounts	3186	
Churn Inputs			Number of standard storage accounts required	5	
Average daily data change rate (%)	5%		Number of Blob disks required	200	
Amount of data changed per day (in GBs)	2100		Number of premium storage accounts required	0	
Compression	0%		Total IOPS on premium storage accounts	0	
Amount of data Xfered per day (in GBs)	2100				
Retention Inputs			Other Infra requirements		
Number of recovery points	16		Number of Configuration Servers required	NA	
Initial Replication Inputs			Number of additional Process Servers required	NA	
Number of hours in which initial replication for the batch of virtual machines should complete	16		100% additional storage on the Source	60000	
Number of virtual machines per initial replication batch	3				

A quick overview of the Azure Site Recovery Capacity planner

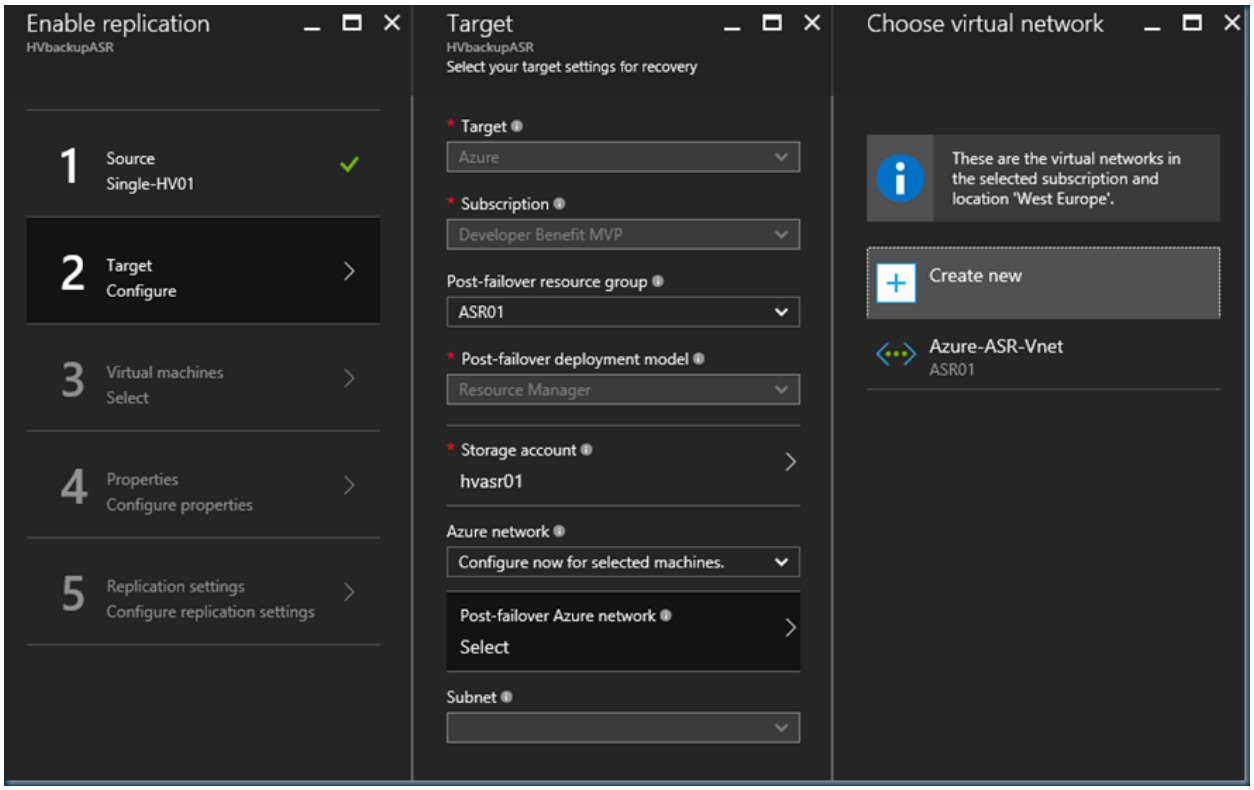
If you skip this or thinking this will be fine I'll show you later what can happen.



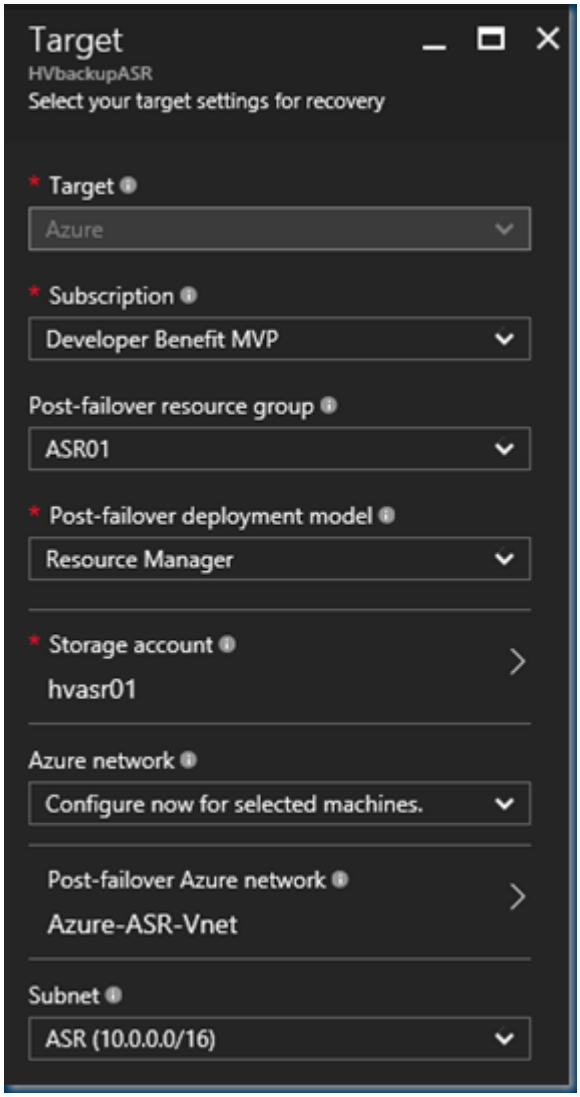
Now that all steps are completed in the ASR infrastructure we can start



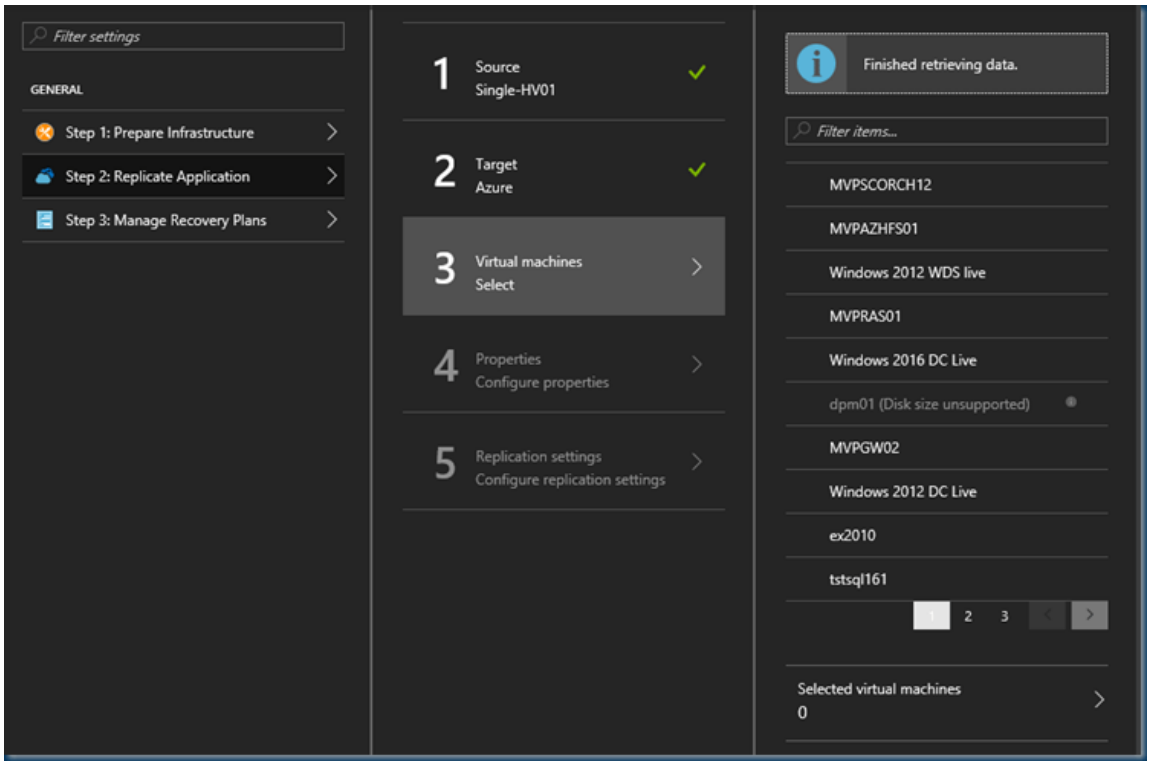
The replication can't be Throttled only for backup operations you can Enable internet bandwidth usage throttling.

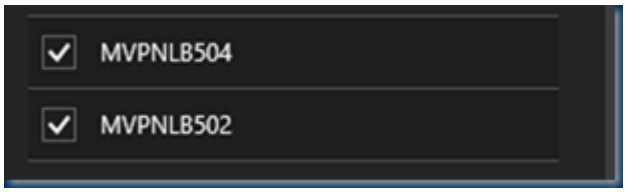


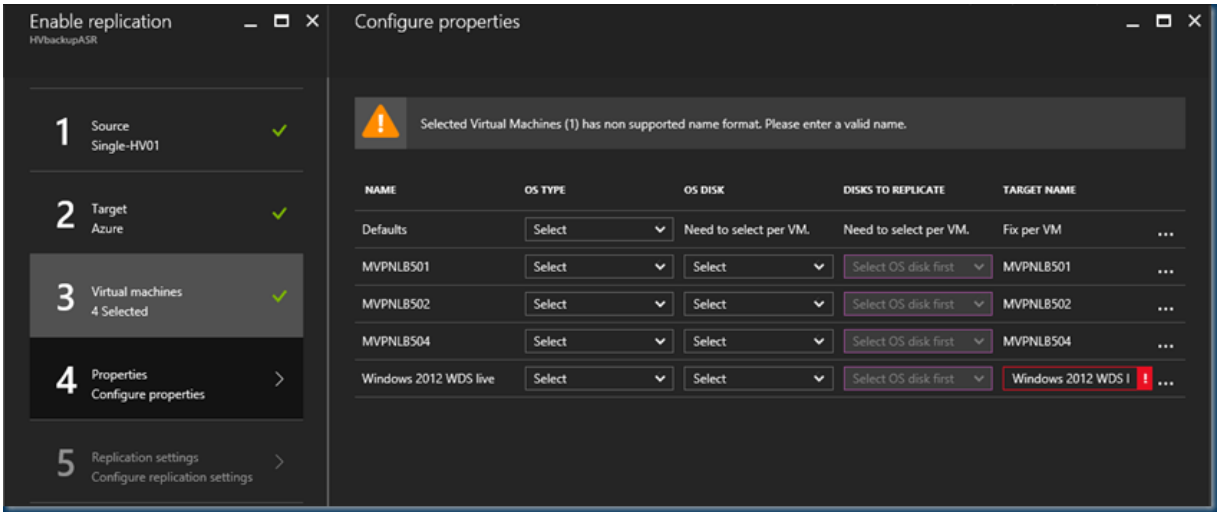
Selecting the Right networks for the replicated VM's and subnets and the correct Storage account.



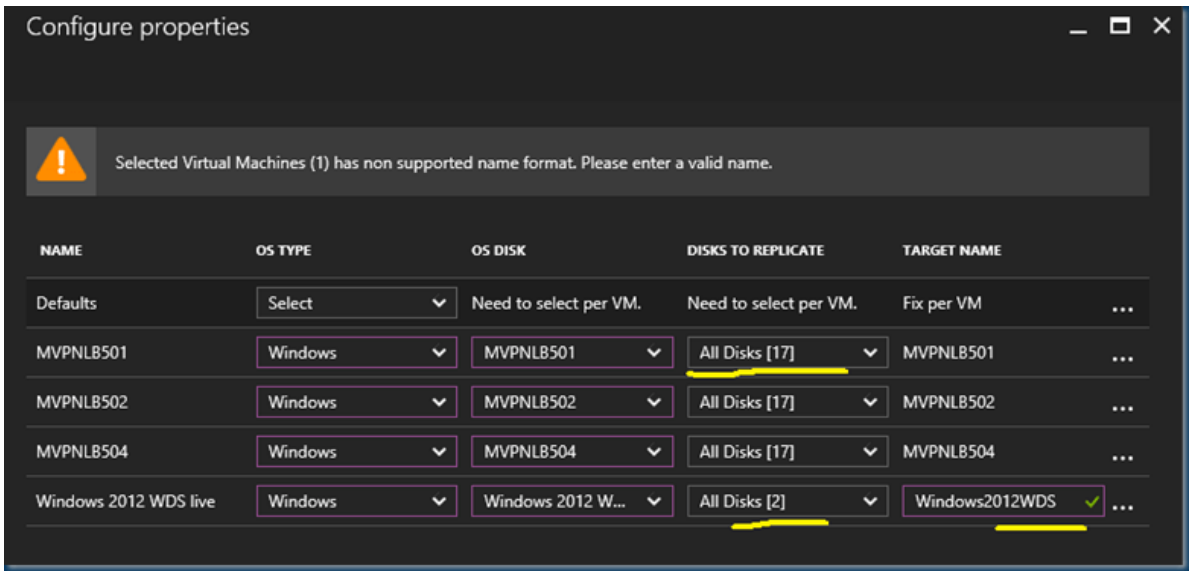
Next is selecting what VM's I need to replicate. If there is no VM list then there is something wrong with your connection.


Filter settings
GENERAL
Step 1: Prepare Infrastructure
Step 2: Replicate Application
Step 3: Manage Recovery Plans
1 Source
Single-HV01
2 Target
Azure
3 Virtual machines
Select
4 Properties
Configure properties
5 Replication settings
Configure replication settings
Finished retrieving data.
Filter items...
MVPSCORCH12
MVPAZHFS01
Windows 2012 WDS live
MVPRAS01
Windows 2016 DC Live
dpm01 (Disk size unsupported)
MVPGW02
Windows 2012 DC Live
ex2010
tstsql161
1 2 3
Selected virtual machines
0

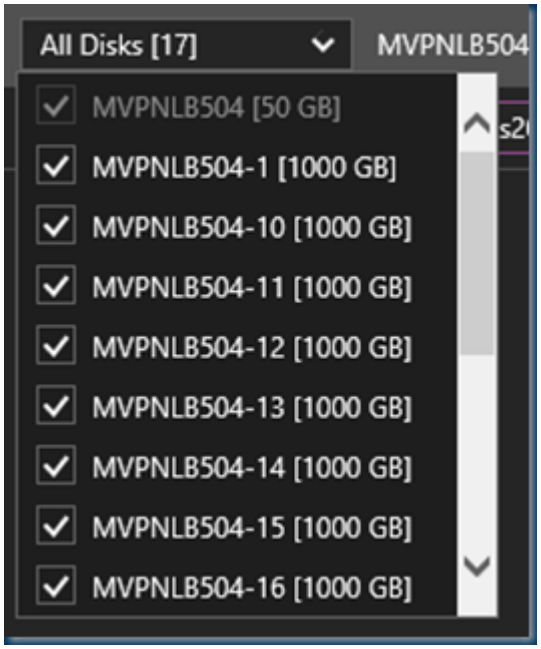

MVPNLB504
MVPNLB502


Enable replication
HVbackupASR
1 Source
Single-HV01
2 Target
Azure
3 Virtual machines
4 Selected
4 Properties
Configure properties
5 Replication settings
Configure replication settings
Configure properties
Selected Virtual Machines (1) has non supported name format. Please enter a valid name.
NAME
OS TYPE
OS DISK
DISKS TO REPLICATE
TARGET NAME
Defaults
Select
Need to select per VM.
Need to select per VM.
Fix per VM
MVPNLB501
MVPNLB502
MVPNLB504
Windows 2012 WDS live
Select OS disk first
Windows 2012 WDS l

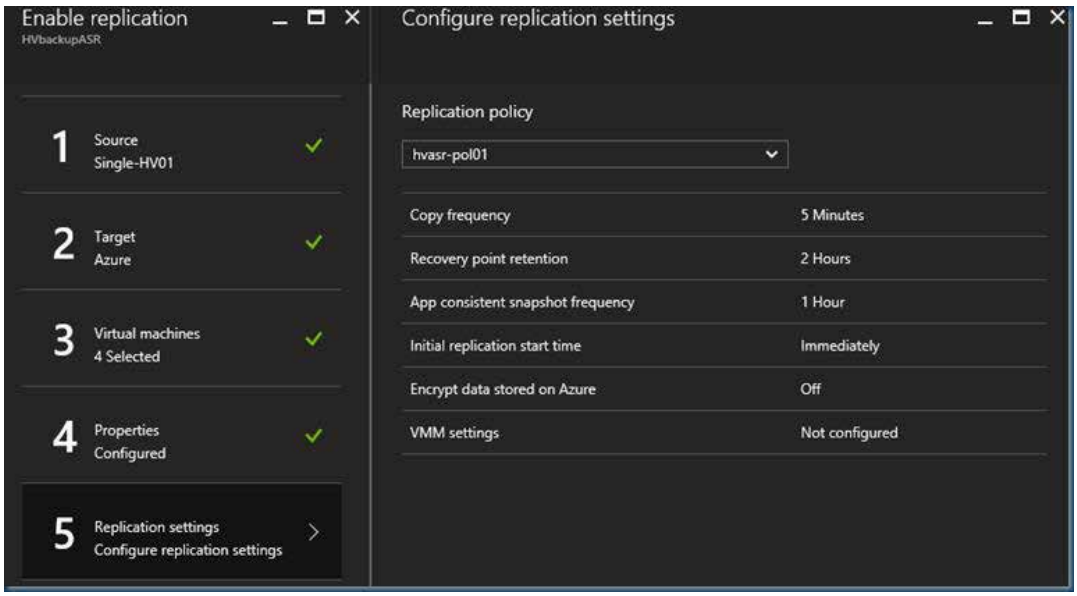
Selecting a few VM's you can see even the names can be changed to the right Azure style or if there a characters in the name that are not supported.

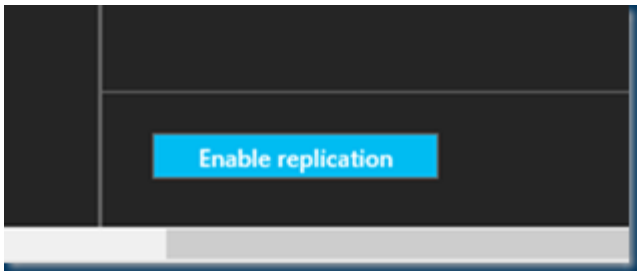


you can select what disk you want and what to skip.

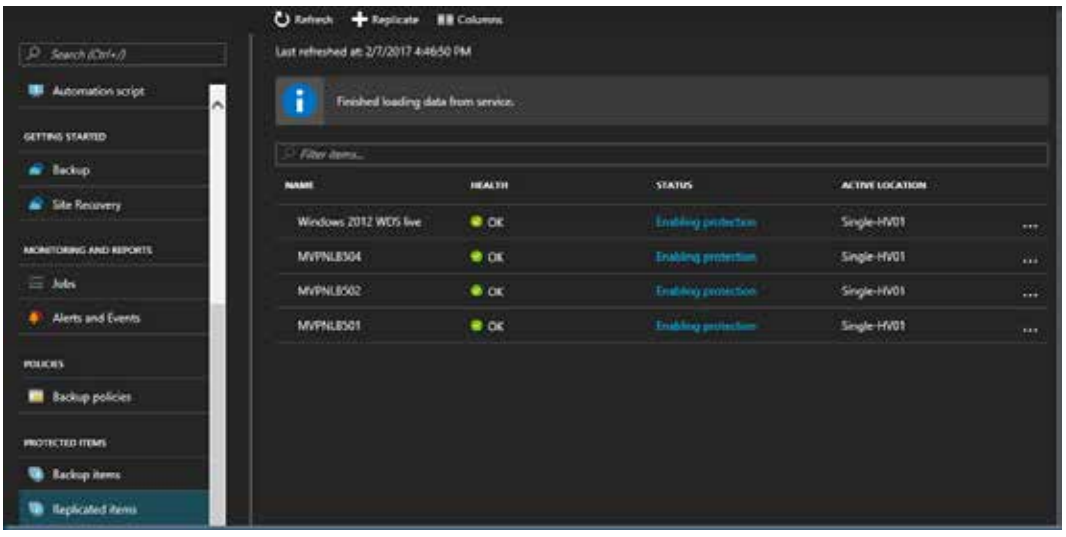


After these final steps we are ready to replicate

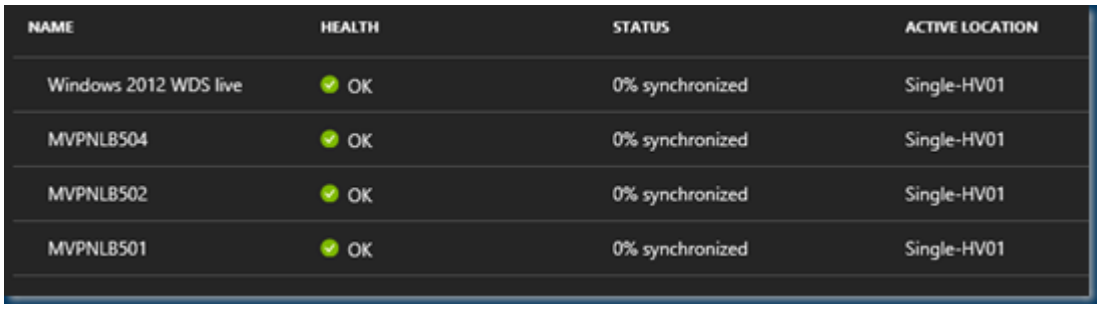




In a quick overview we can start the replication

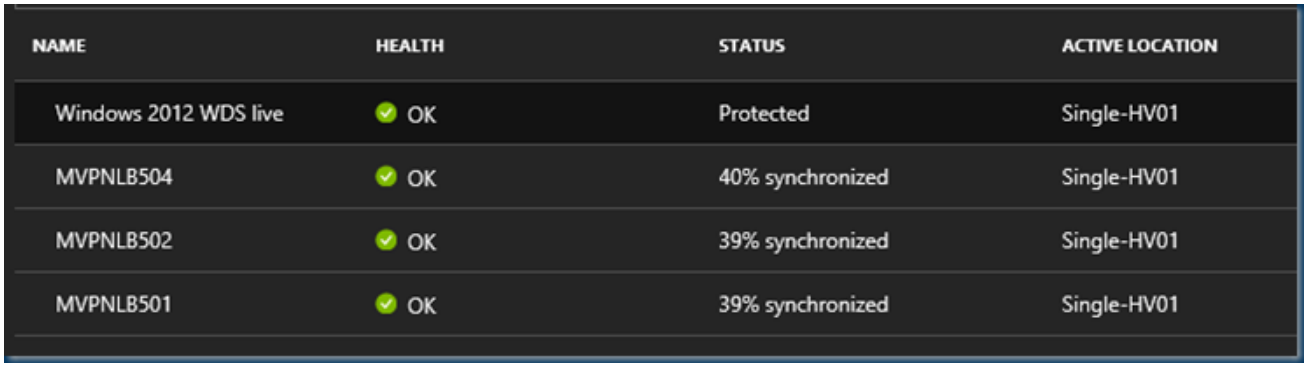


The replication is started and as you can see here comes the ASR Capacity planner.

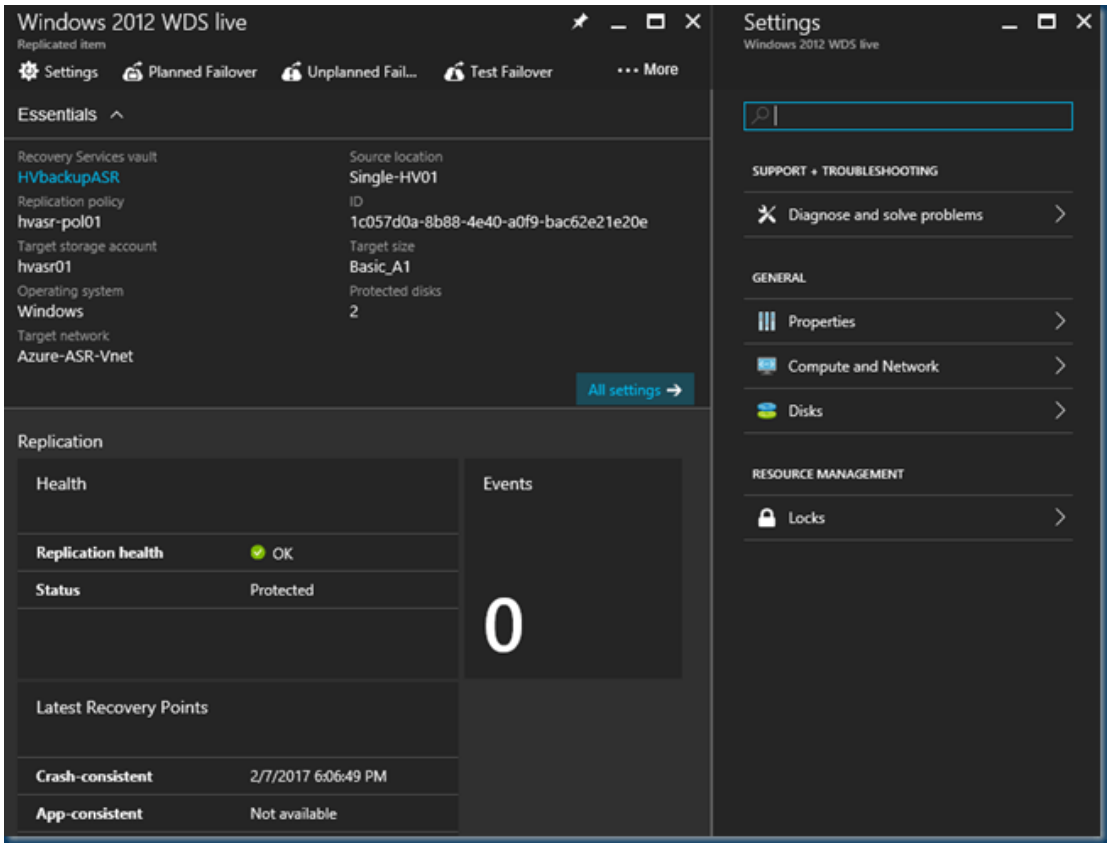


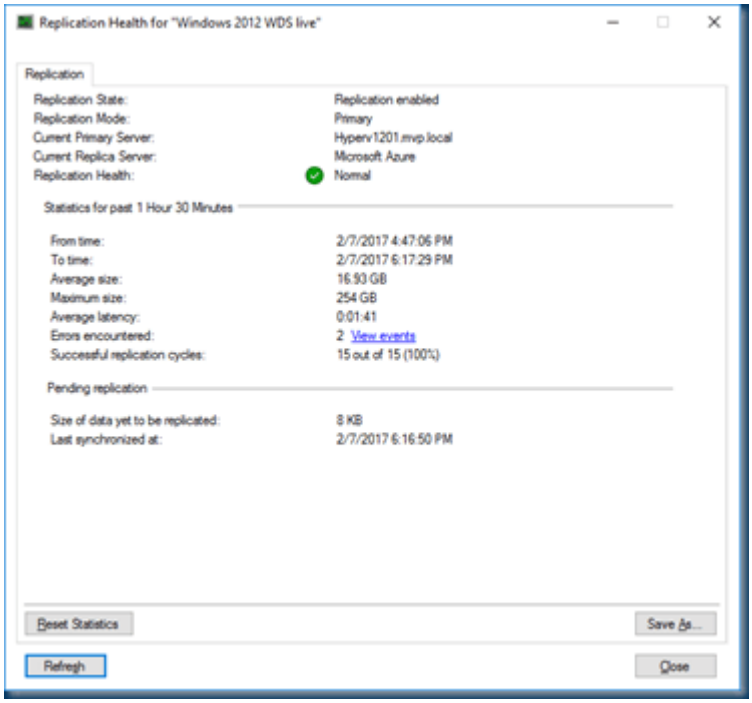
NAME	HEALTH	STATUS	ACTIVE LOCATION
Windows 2012 WDS live	OK	0% synchronized	Single-HV01
MVPNLB504	OK	0% synchronized	Single-HV01
MVPNLB502	OK	0% synchronized	Single-HV01
MVPNLB501	OK	0% synchronized	Single-HV01

Checking the Hyper-v server you can see the progress there or in Azure

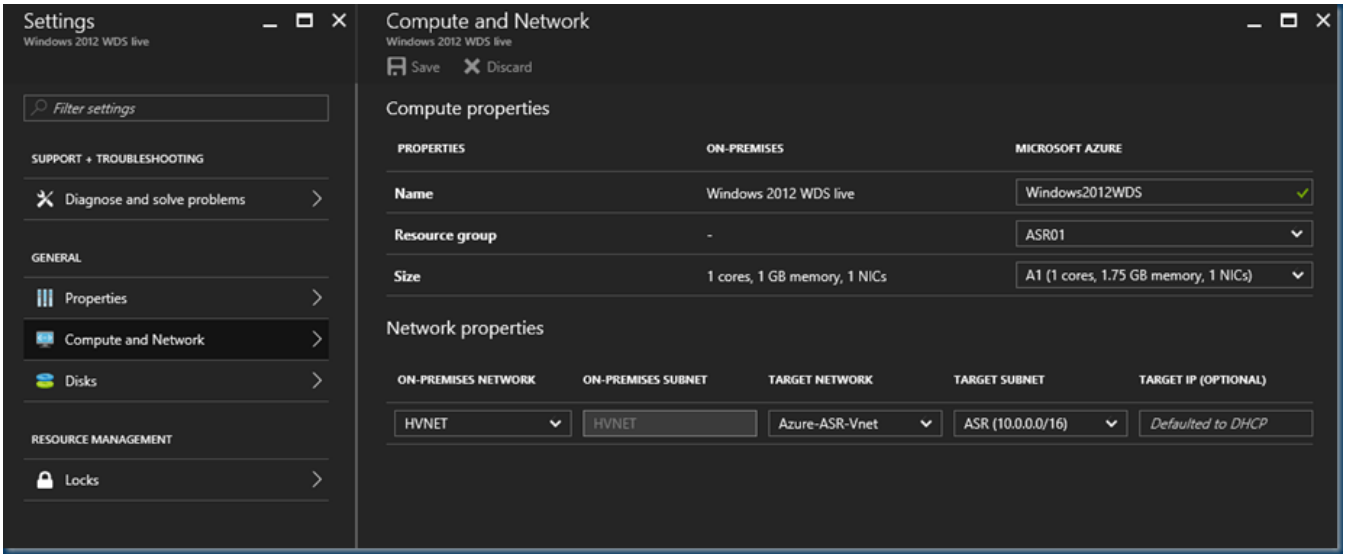


NAME	HEALTH	STATUS	ACTIVE LOCATION
Windows 2012 WDS live	OK	Protected	Single-HV01
MVPNLB504	OK	40% synchronized	Single-HV01
MVPNLB502	OK	39% synchronized	Single-HV01
MVPNLB501	OK	39% synchronized	Single-HV01

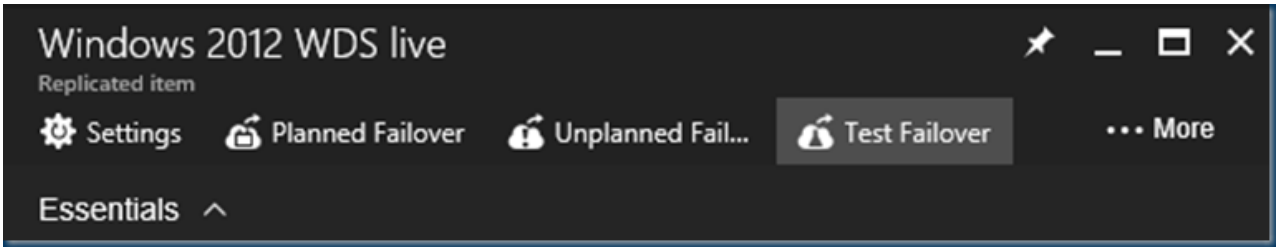

Windows 2012 WDS live
Replicated item
Settings
Planned Failover
Unplanned Fail...
Test Failover
More
Essentials
Recovery Services vault
HVbackupASR
Source location
Single-HV01
Replication policy
hvasr-pol01
ID
1c057d0a-8b88-4e40-a0f9-bac62e21e20e
Target storage account
hvasr01
Target size
Basic_A1
Operating system
Windows
Protected disks
2
Target network
Azure-ASR-Vnet
All settings
Replication
Health
Replication health
OK
Status
Protected
Events
0
Latest Recovery Points
Crash-consistent
2/7/2017 6:06:49 PM
App-consistent
Not available
Settings
Windows 2012 WDS live
SUPPORT + TROUBLESHOOTING
Diagnose and solve problems
GENERAL
Properties
Compute and Network
Disks
RESOURCE MANAGEMENT
Locks


Replication Health for "Windows 2012 WDS live"
Replication
Replication State:
Replication enabled
Replication Mode:
Primary
Current Primary Server:
Hyperv1201.mvp.local
Current Replica Server:
Microsoft Azure
Replication Health:
Normal
Statistics for past 1 Hour 30 Minutes
From time:
2/7/2017 4:47:06 PM
To time:
2/7/2017 6:17:29 PM
Average size:
16.93 GB
Maximum size:
254 GB
Average latency:
0:01:41
Errors encountered:
2 View events
Successful replication cycles:
15 out of 15 (100%)
Pending replication
Size of data yet to be replicated:
8 KB
Last synchronized at:
2/7/2017 6:16:50 PM
Reset Statistics
Save As...
Refresh
Close

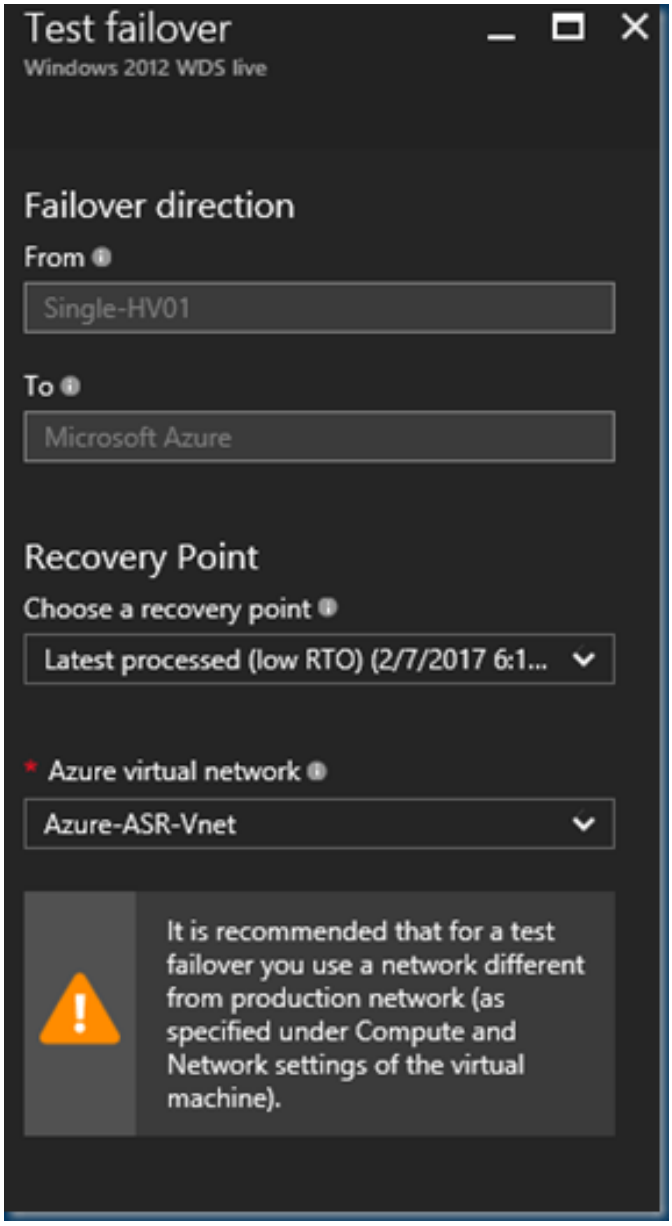
But As ASR is using ASR you can also drill down on the replica options.



When the replica is done you can change the Azure VM in any way change the network, VM size the VM can be better than on prem.

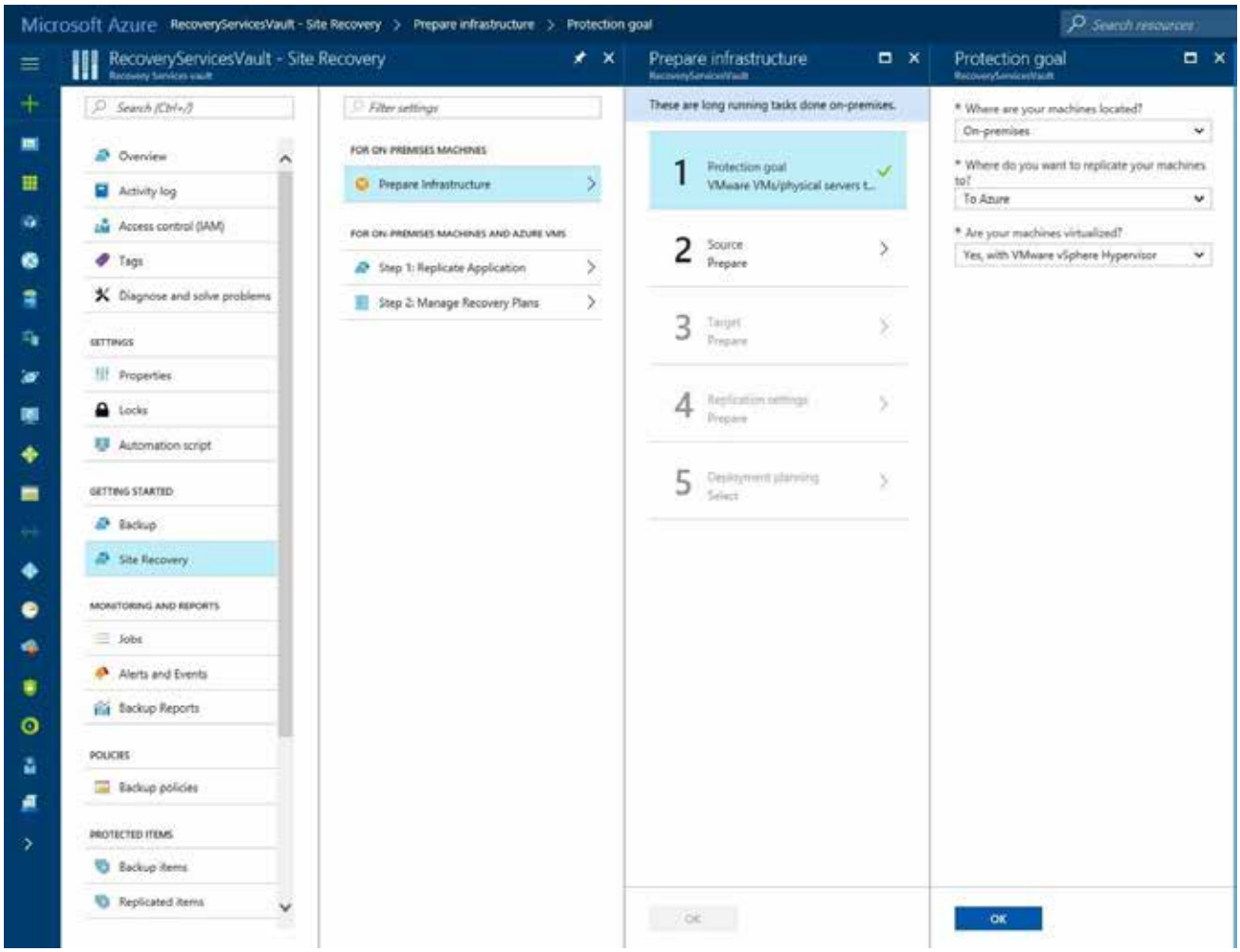


As ASR stands for recovery you can do a test failover or planned. As you are not using VMM the Azure portal is the Orchestrator for the Failover.



Testing the VM is easy a you can run the VM Side by Side and you can change all the settings. A great option to get started with Azure.

ASR post deployment with VMware Source

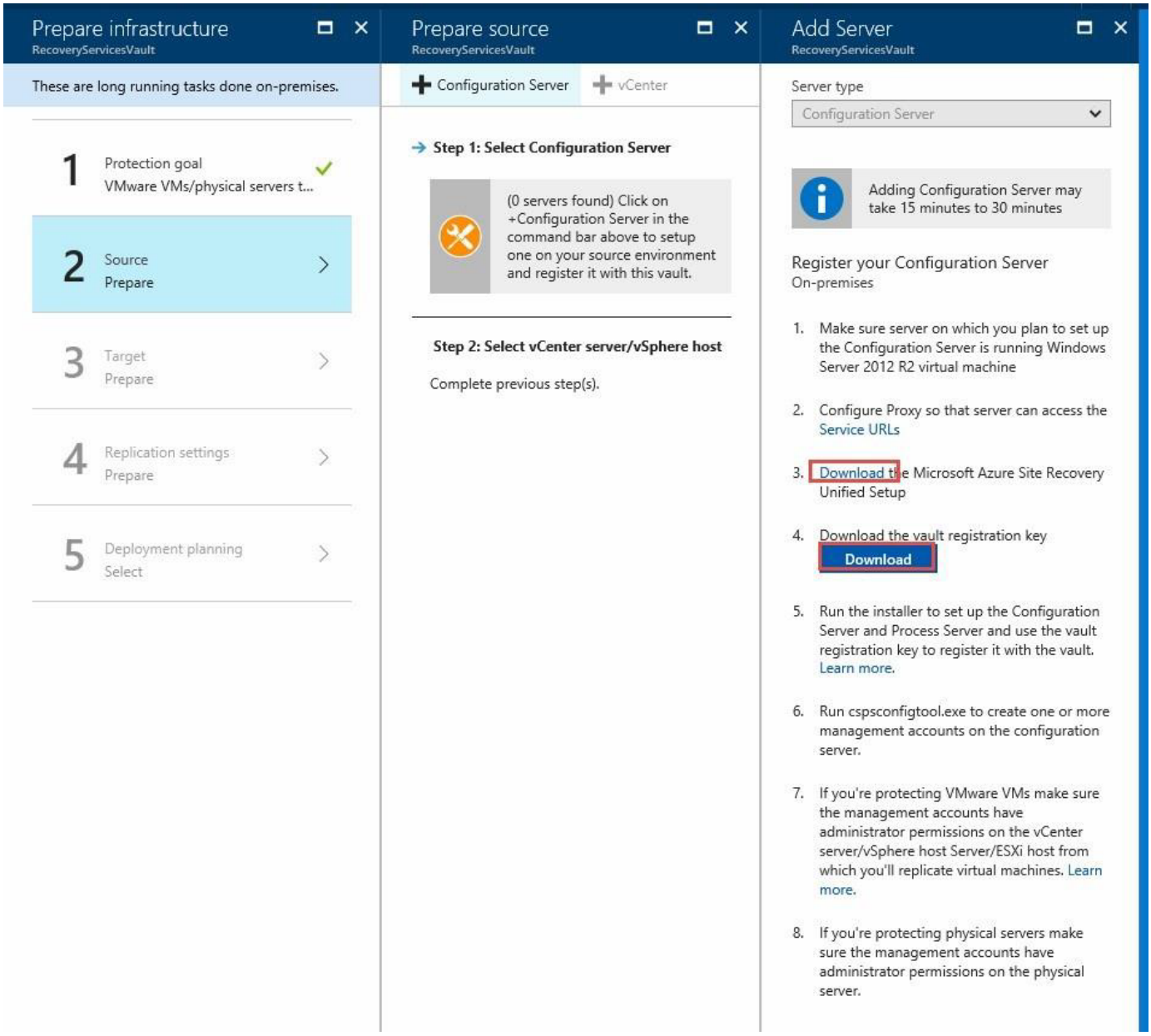


Next, we will prepare the source.

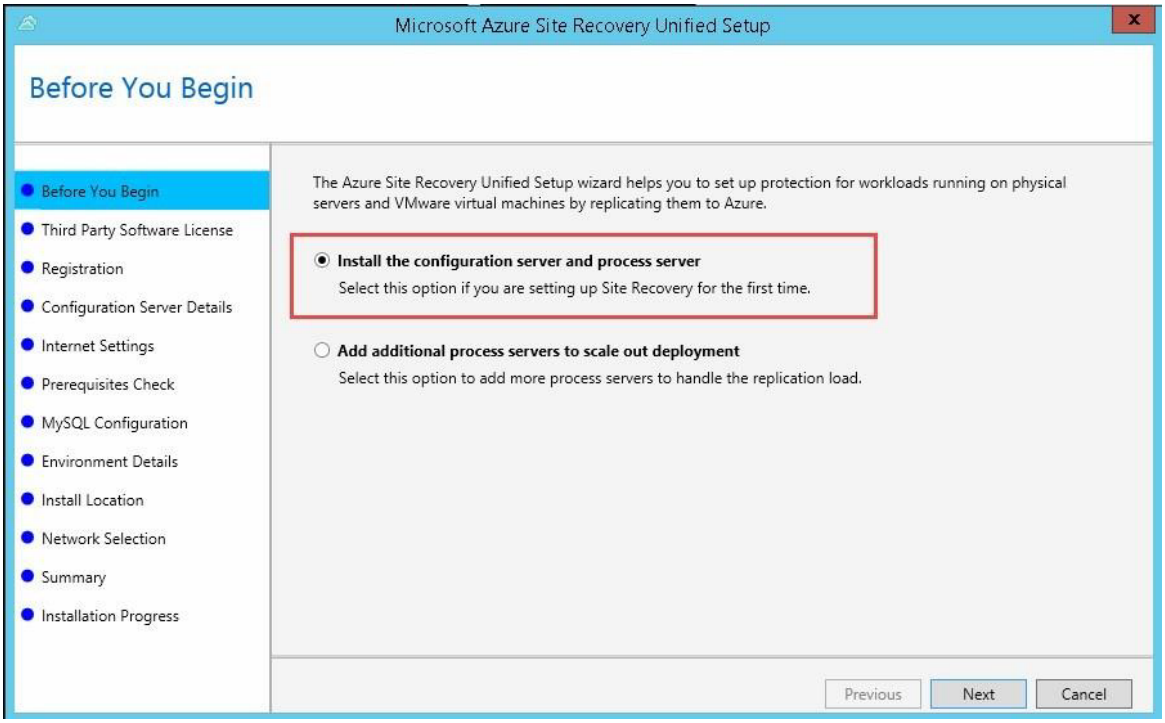
We will use the Configuration Server.

This must be installed on Server 2012 R2 on-prem, and will act as a processor to continuously back up VMs to ASR.

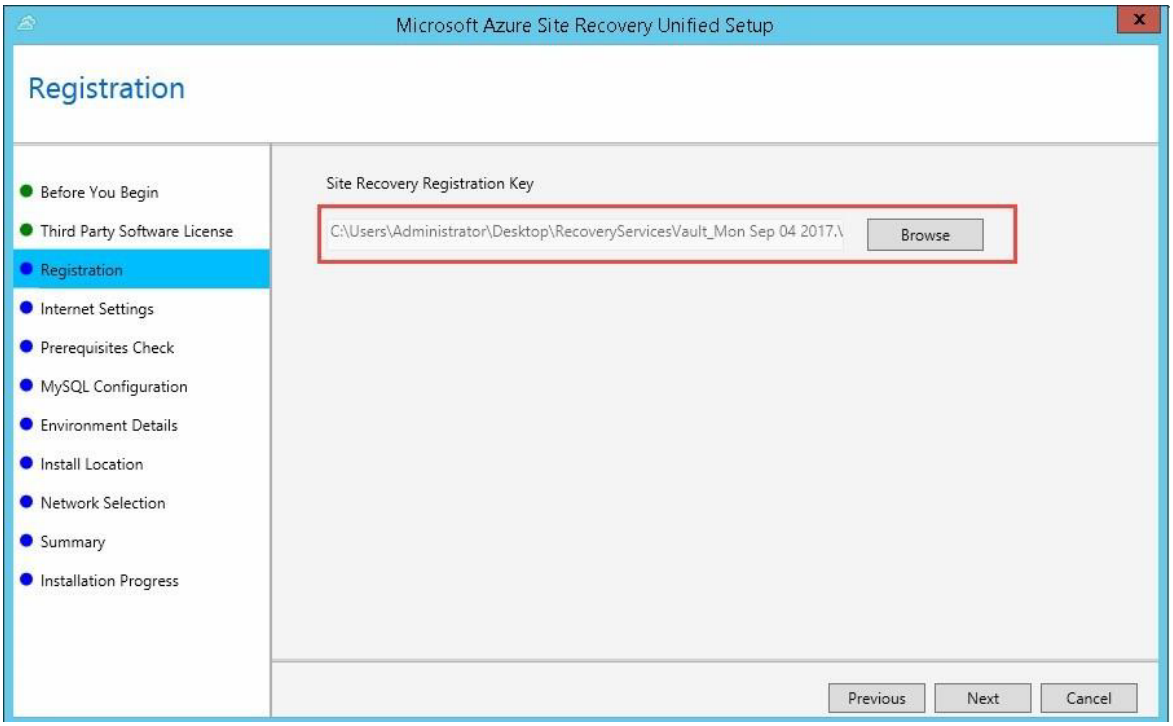
Download the setup and vault credentials in step 3 and 4.



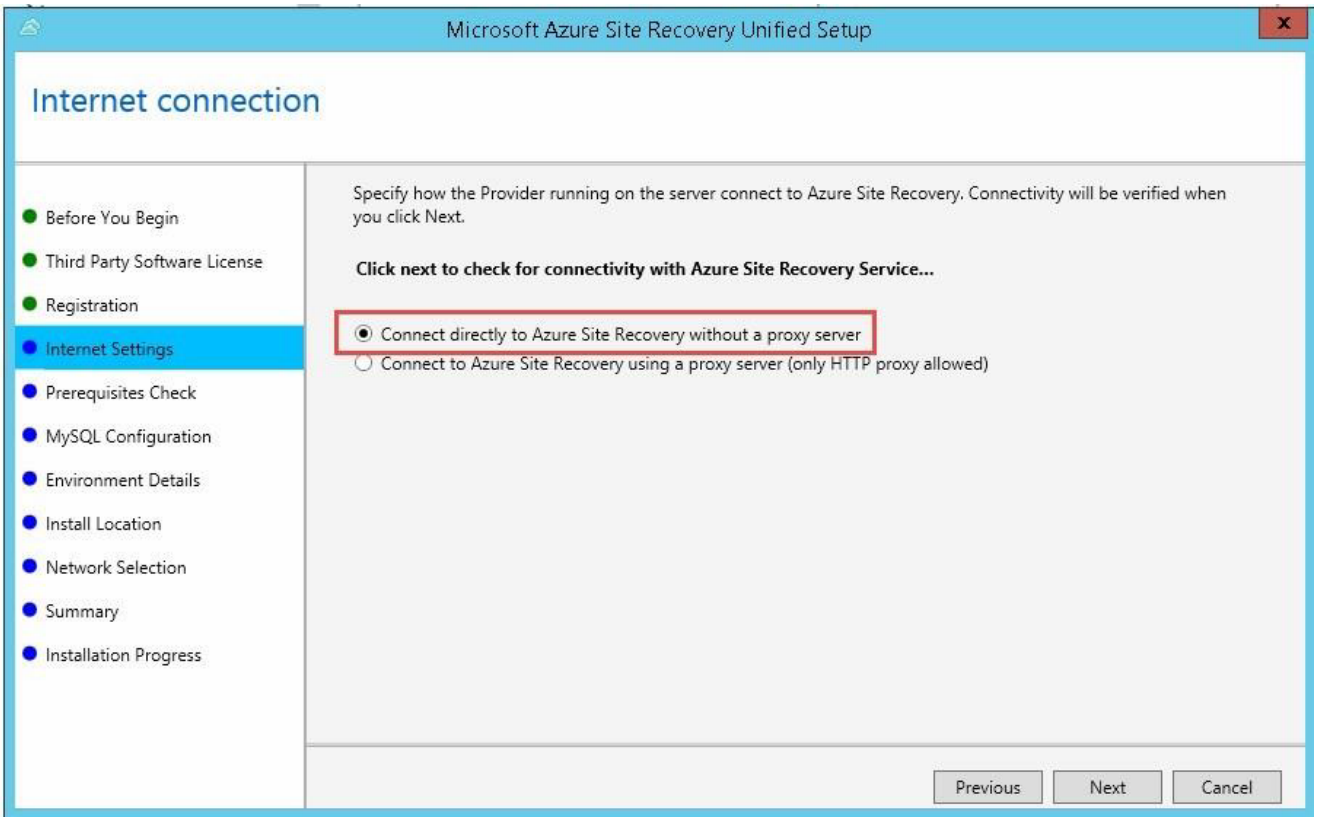
Run the Configuration Server setup and choose to install the Configuration Server and process server.



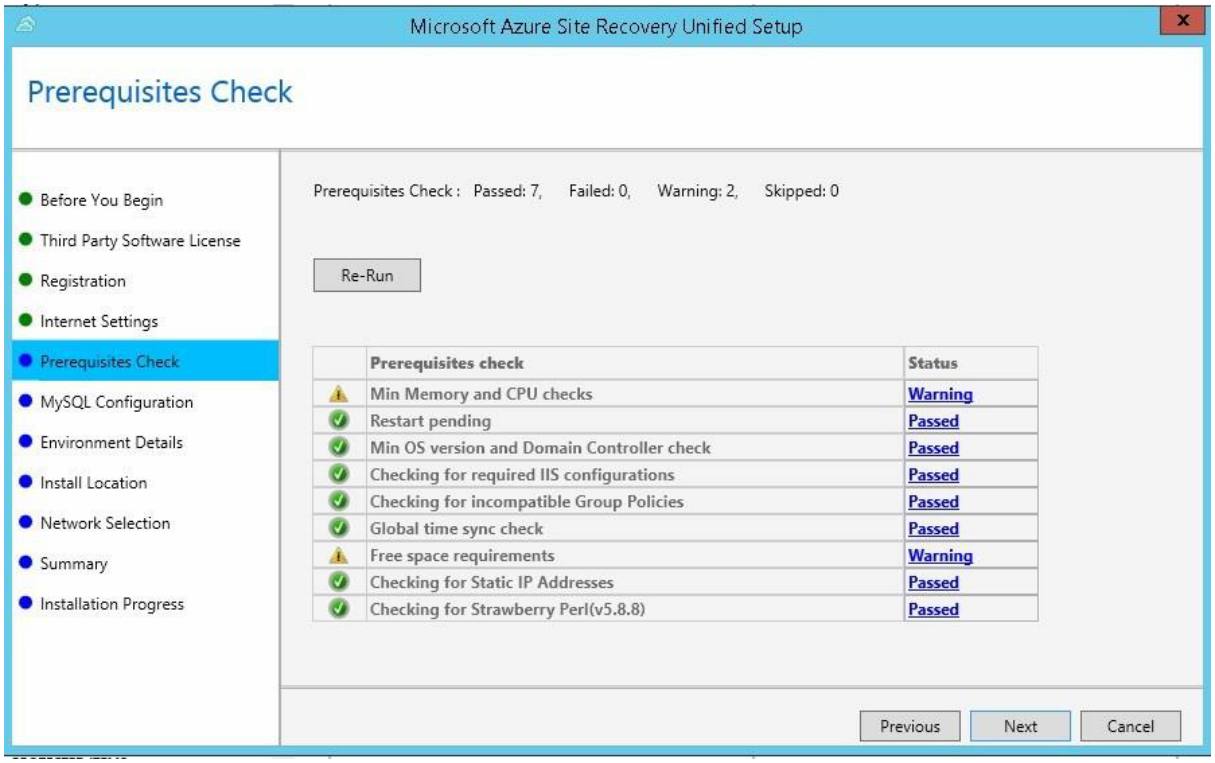
Enter the path to the vault credentials you downloaded on the next step.



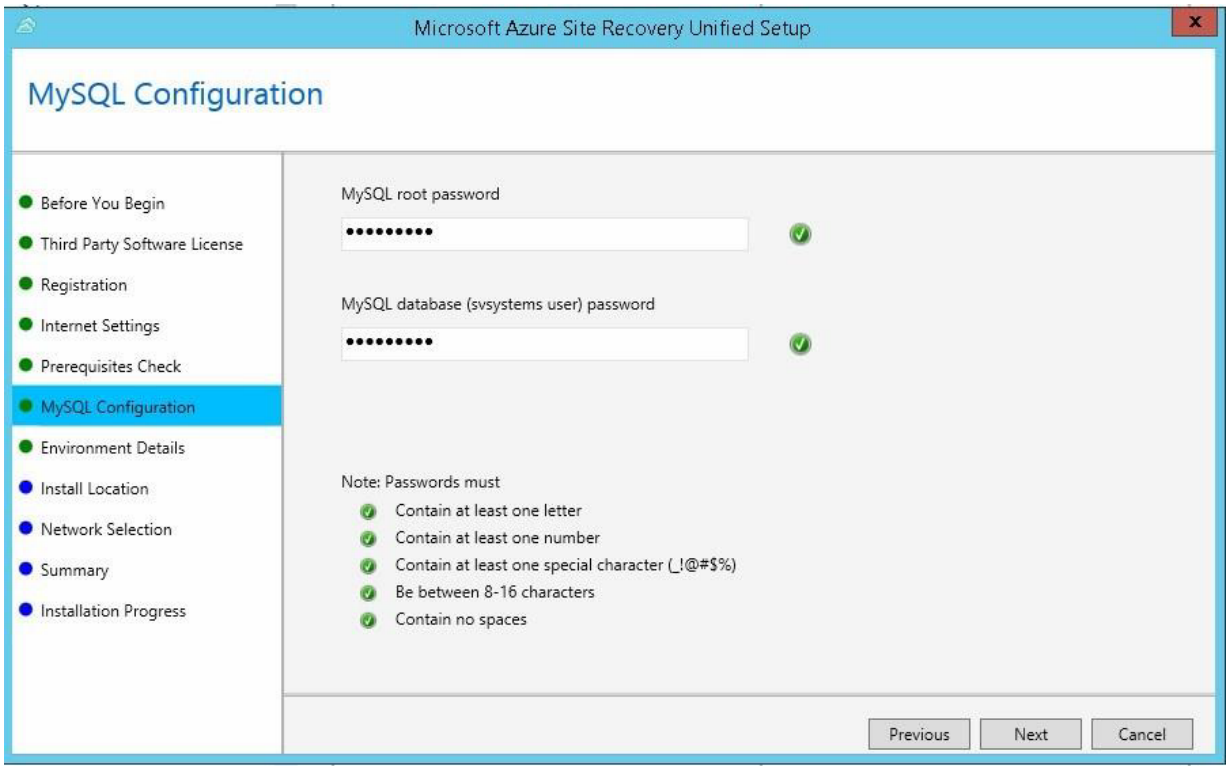
Configure a proxy server if you server does not have a direct connection to the Internet. ASR works directly over the Internet or proxy and does not require a VPN connection to Azure.



Check that you pass all prerequisites and continue.

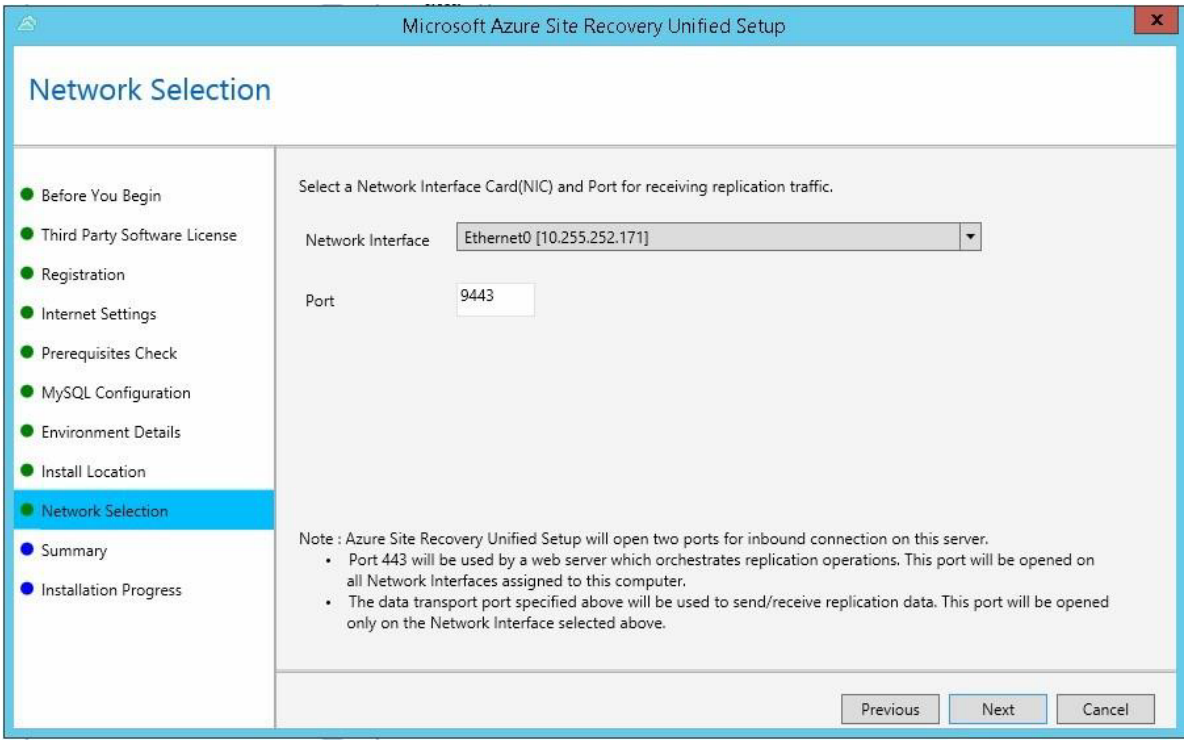


Choose a MySQL password and continue the wizard.

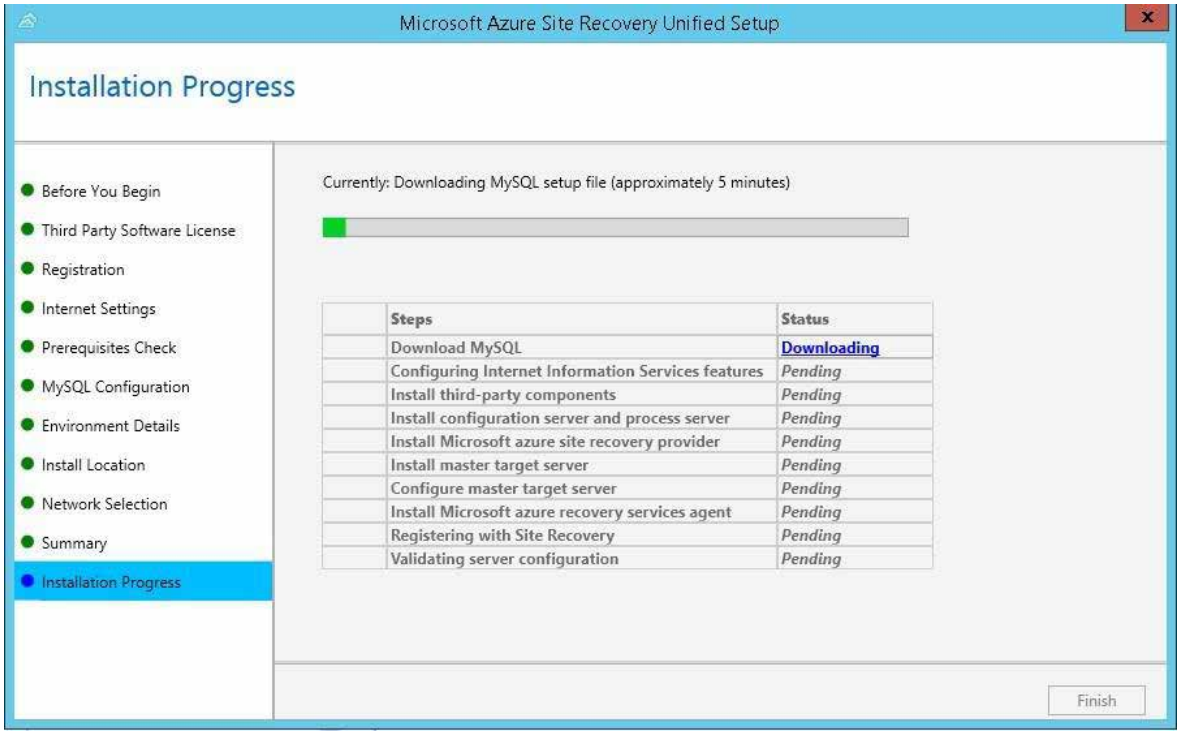


Choose yes when asked to protect VMware virtual machines. This may require you to install VMware tools and the vSphere PowerCLI if they are not already present on the Configuration Server.

Choose an install location for the ASR Configuration Server and choose the network interface used for replication traffic on the Configuration Server.

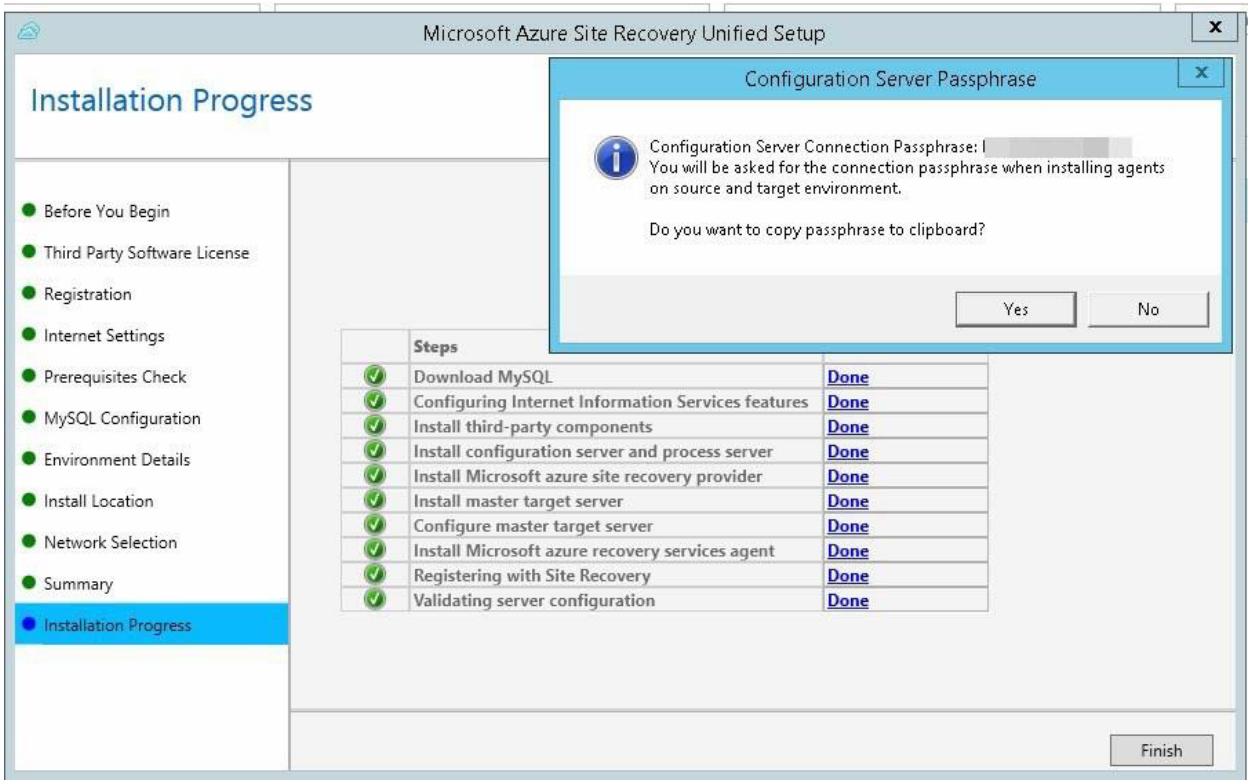


Allow setup to complete. It should take 15 minutes or so.



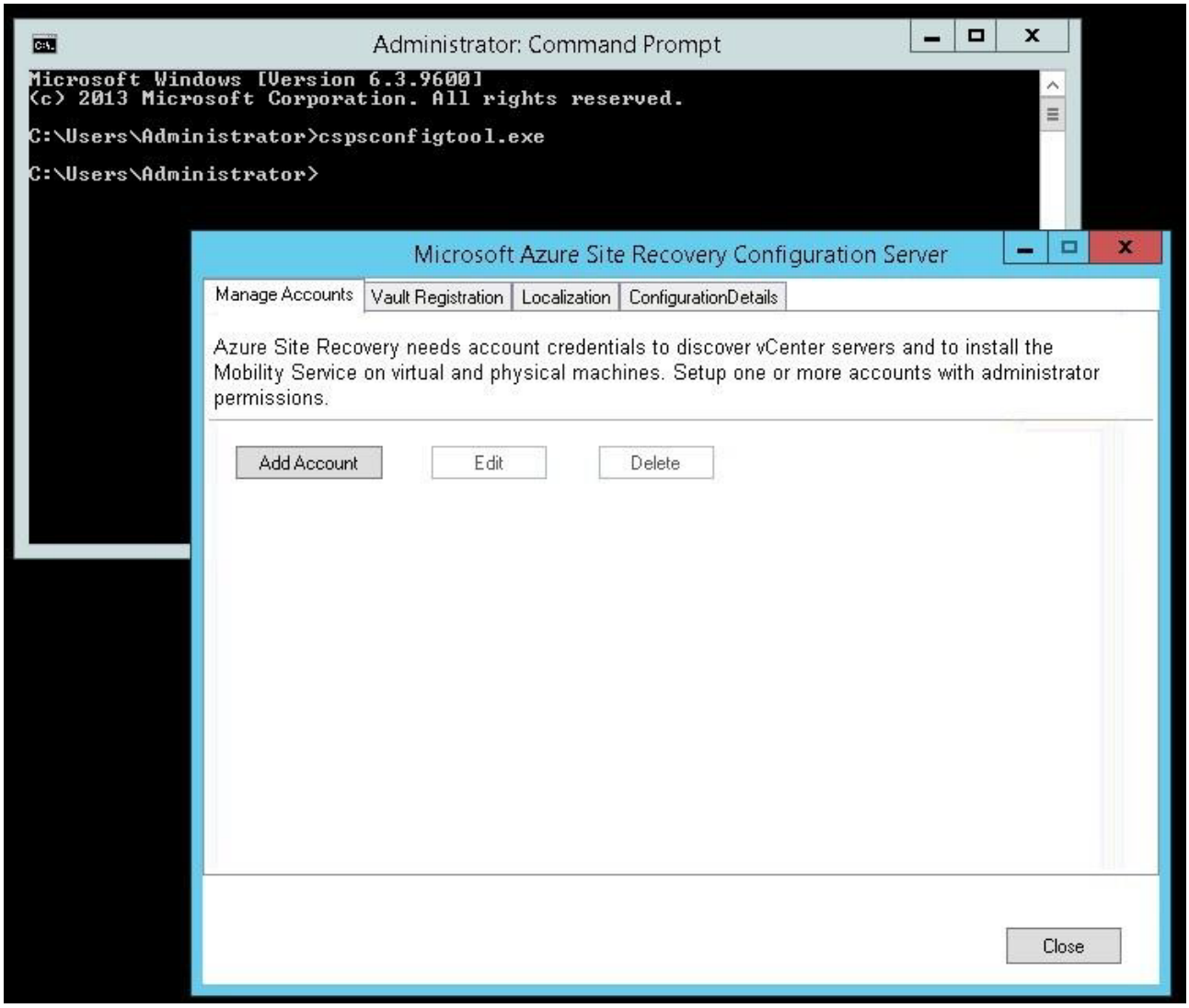
Save the passphrase generated at the end of the installation.

This will be used as an approval mechanism when ASR agents are deployed. You can also regenerate the passphrase later if desired.



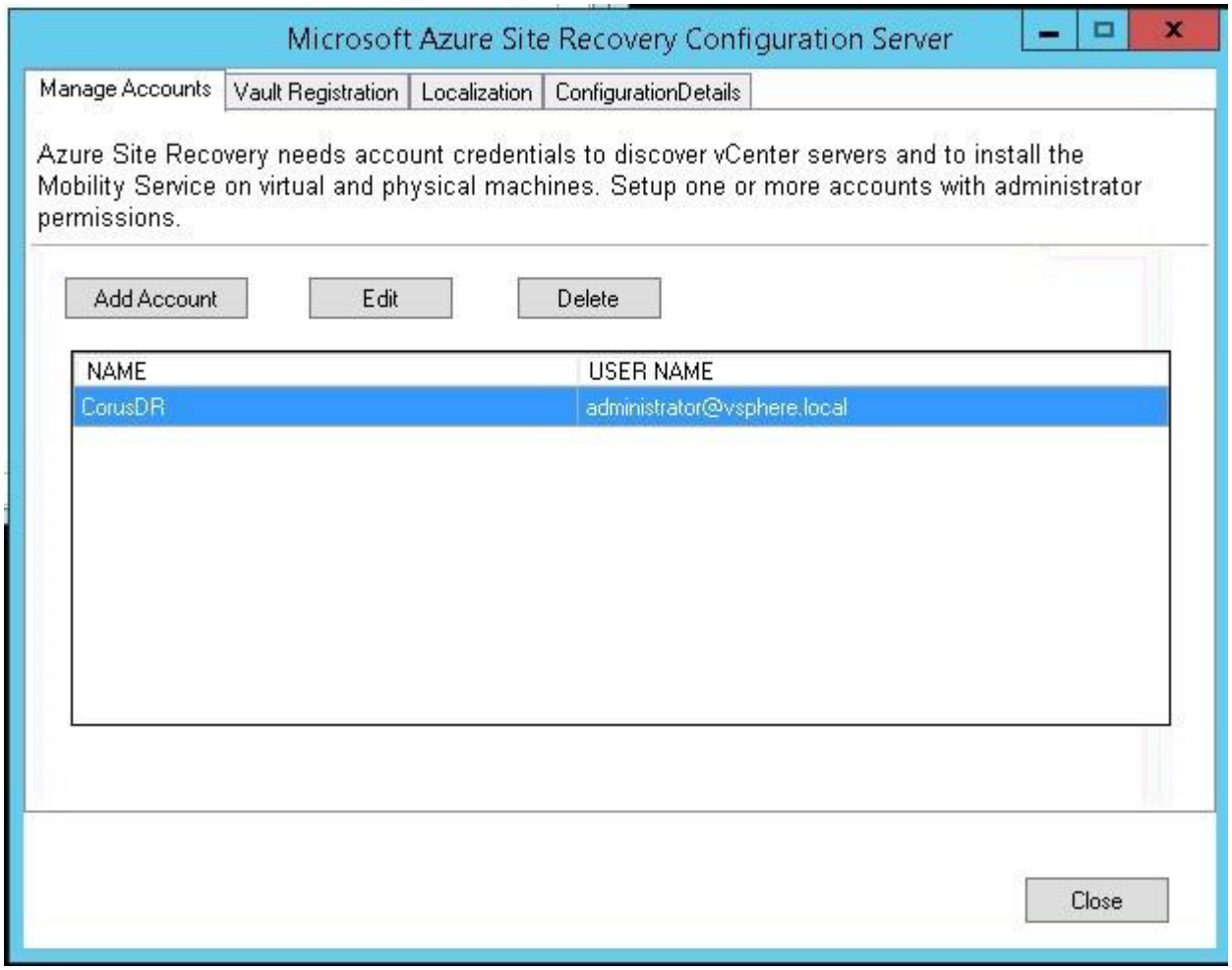
When the installation is complete, you will be prompted to reboot the server – do that before continuing.

After reboot, launch the ASR Configuration tool from Start Menu or just type in “cspsconfigtool.exe” from command prompt.



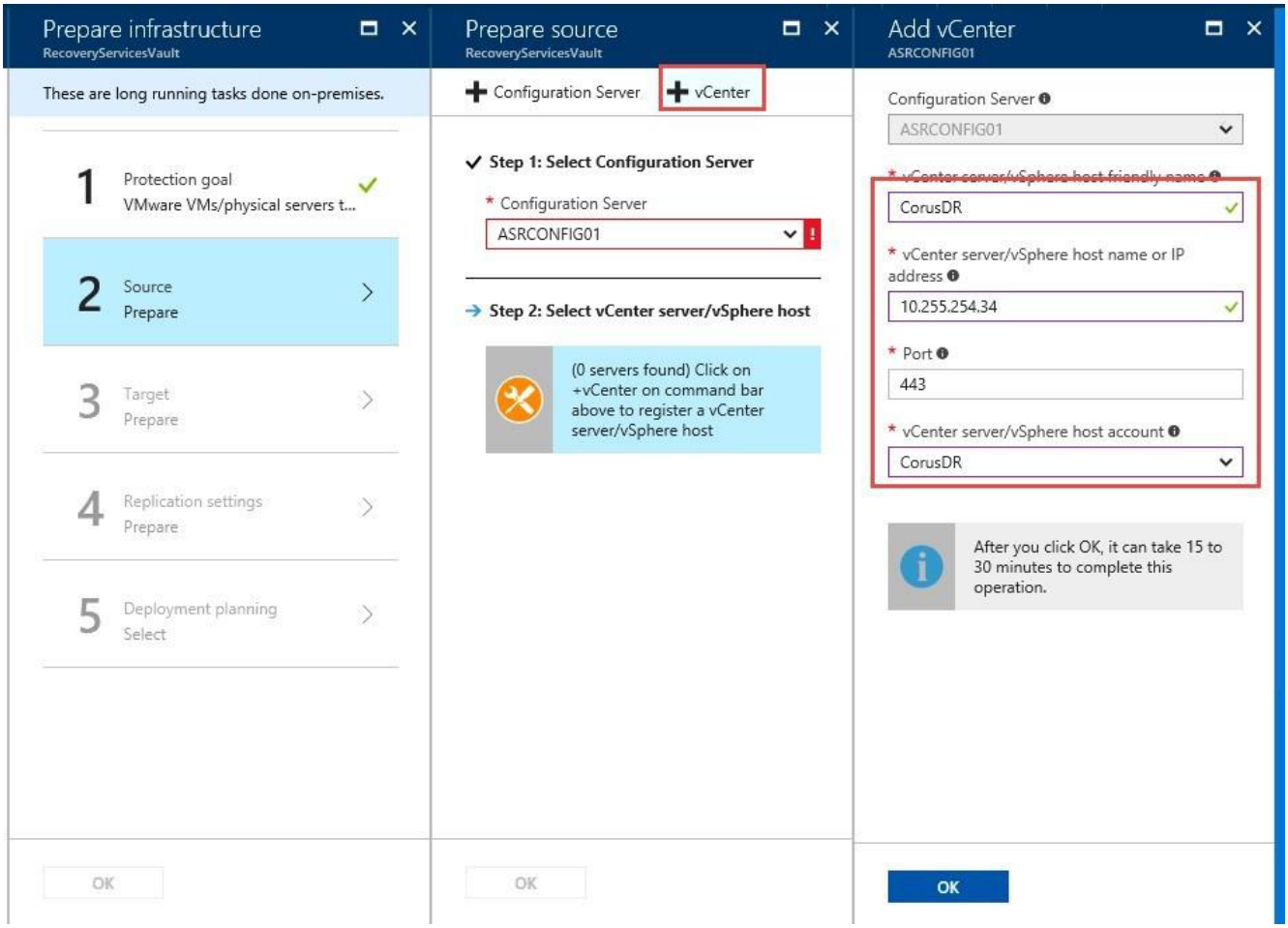
Add an account that has administrative permissions to the VMs you want to migrate from VMware.

Once complete, close the configuration tool.

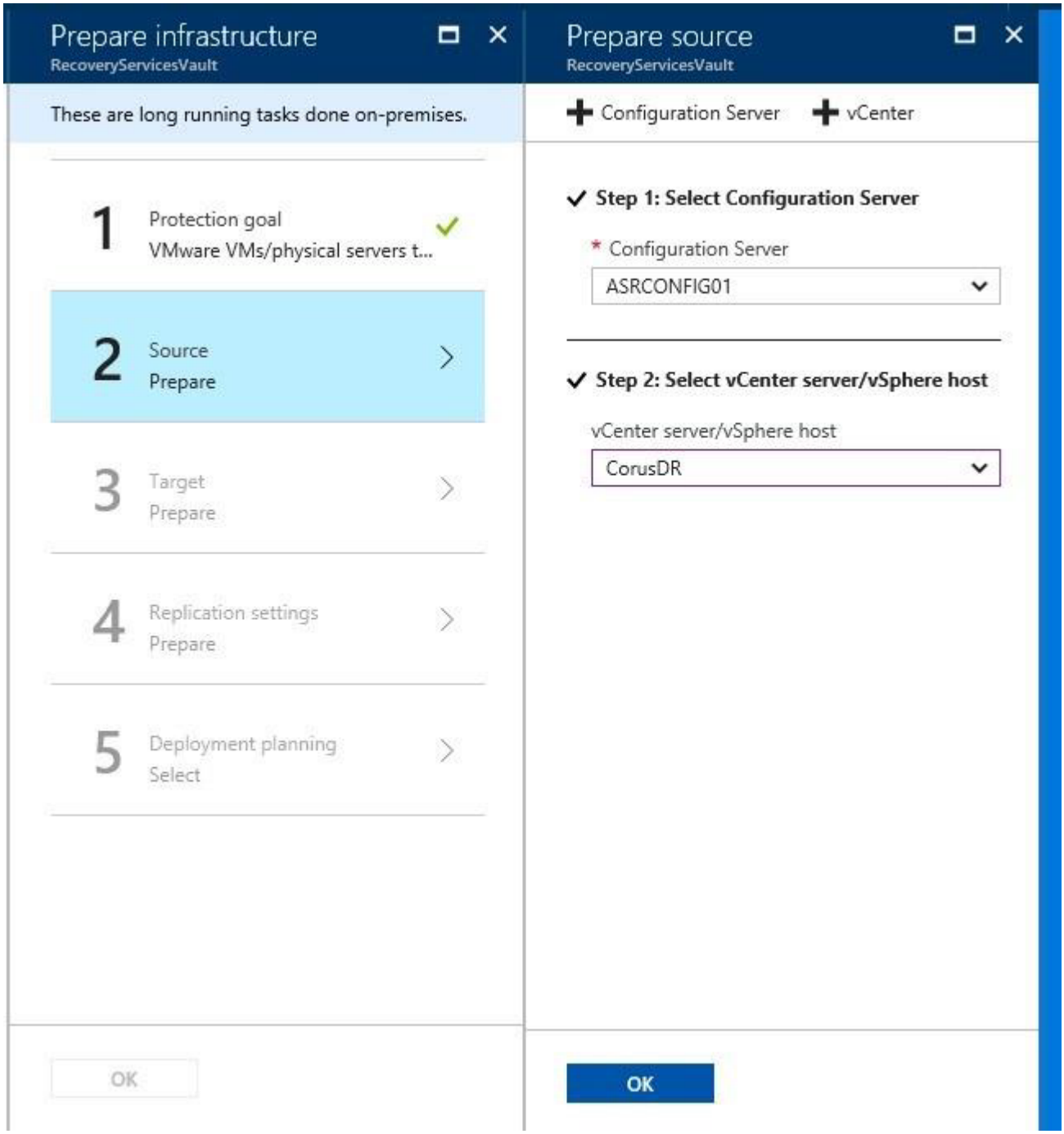


Go back to the Azure portal and go to Step 2 (Prepare).

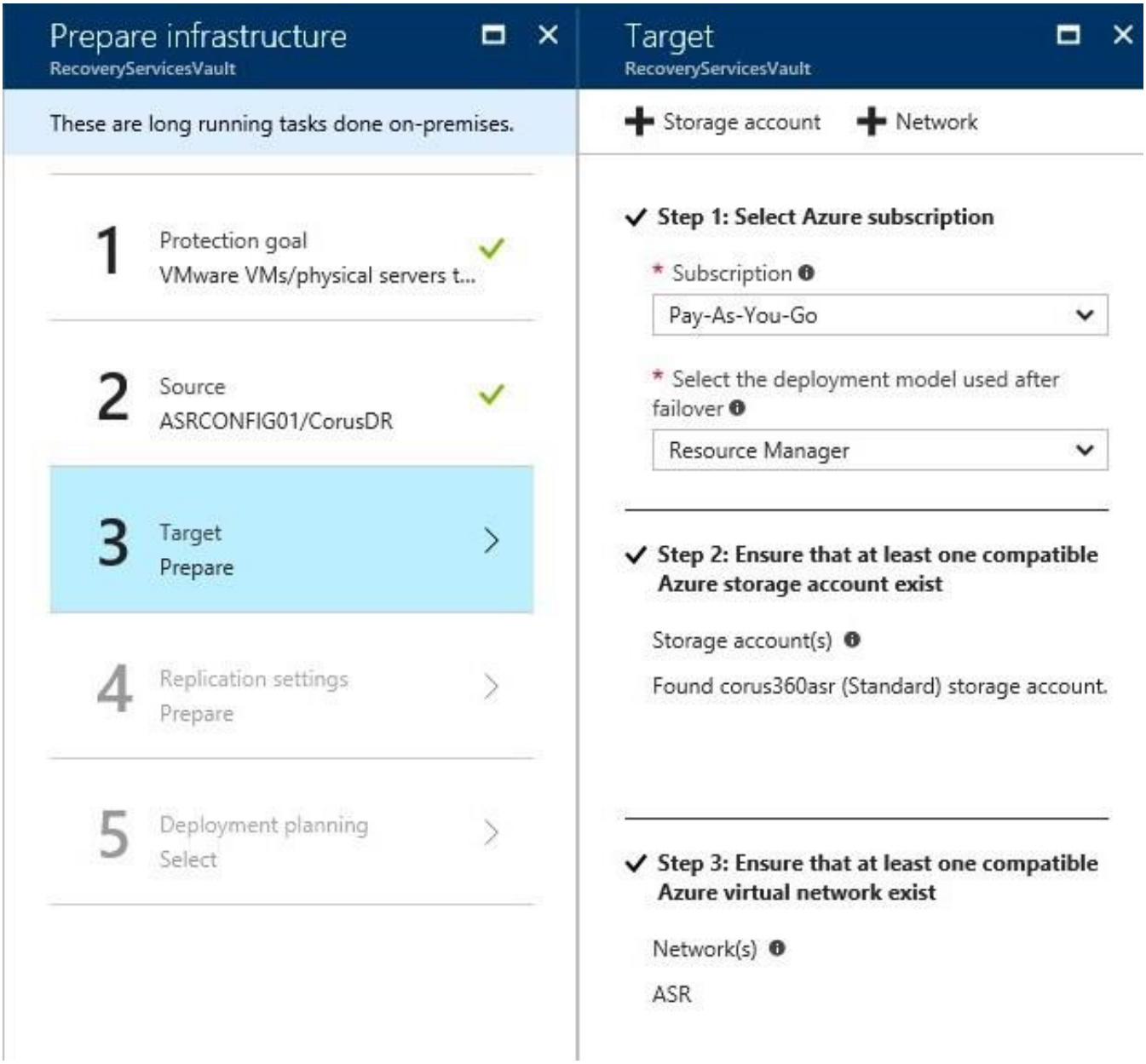
Your Configuration Server and VMware account should show in the Azure portal after 15 minutes from being added on the local server. Click “+vCenter” and enter the local IP/hostname of the VMware host server in your datacenter. This configures the connection from Azure.



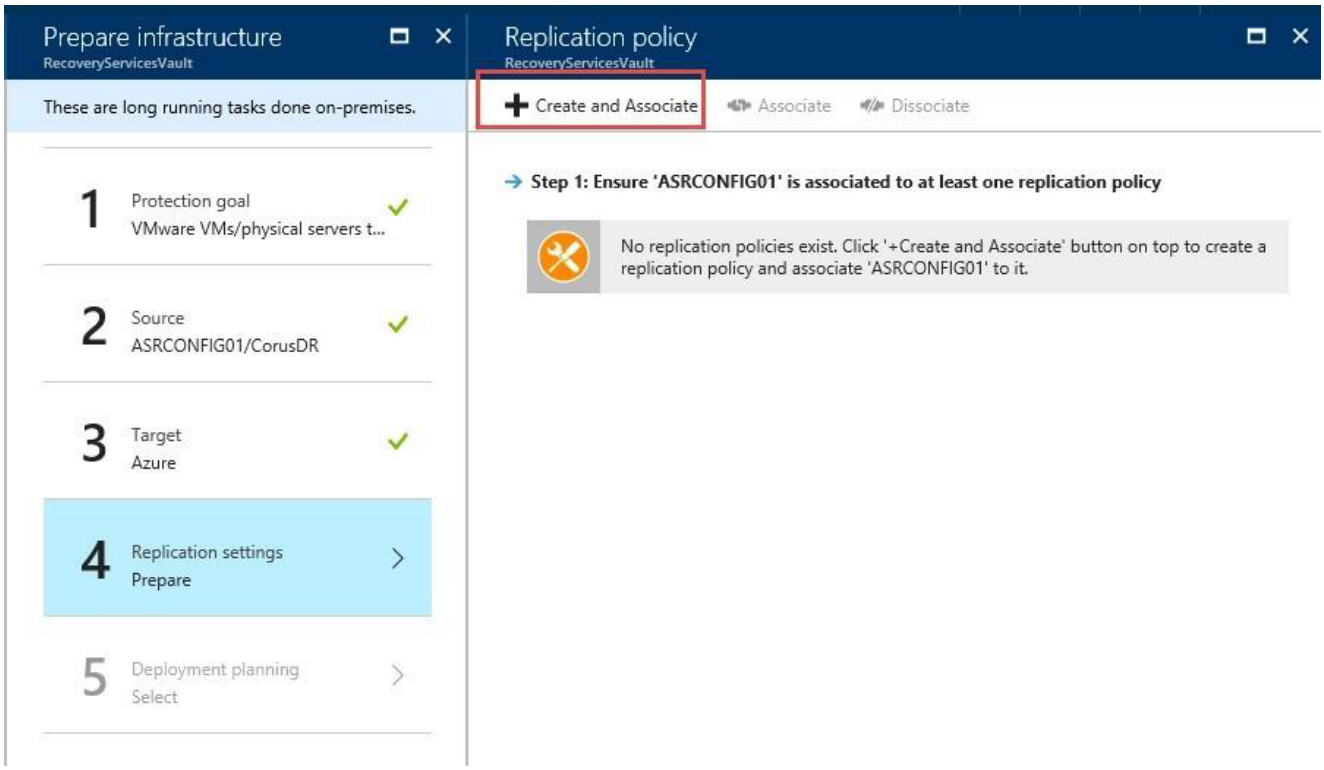
Once the VMware host server is added, you should be able to complete step 2.



On step 3, enter the resource group and subscription that you'd like to use for ASR.



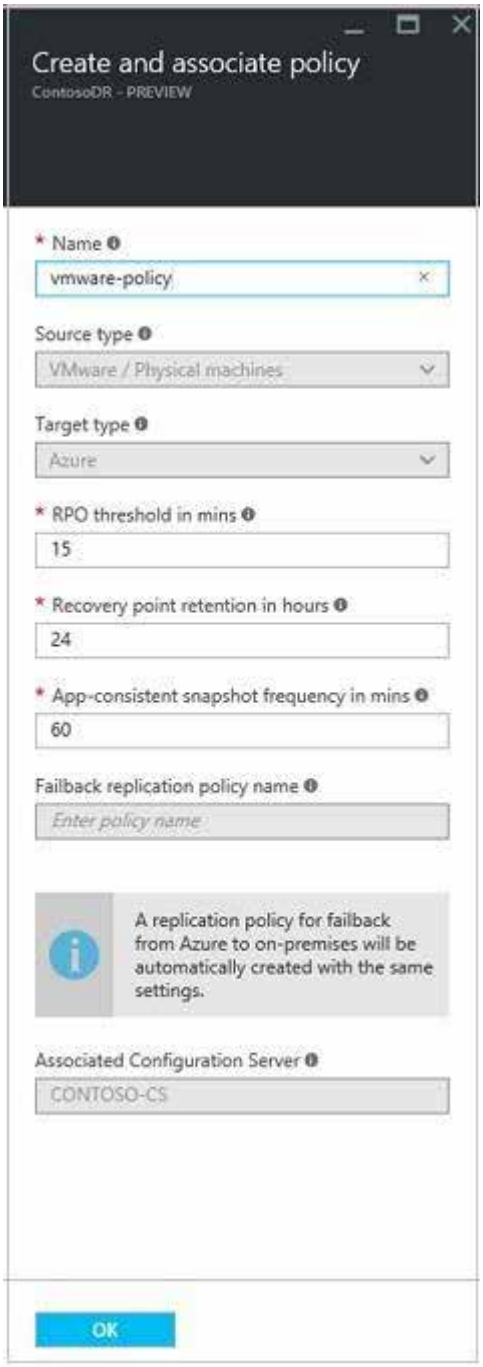
On step 4, click Create and Associate.



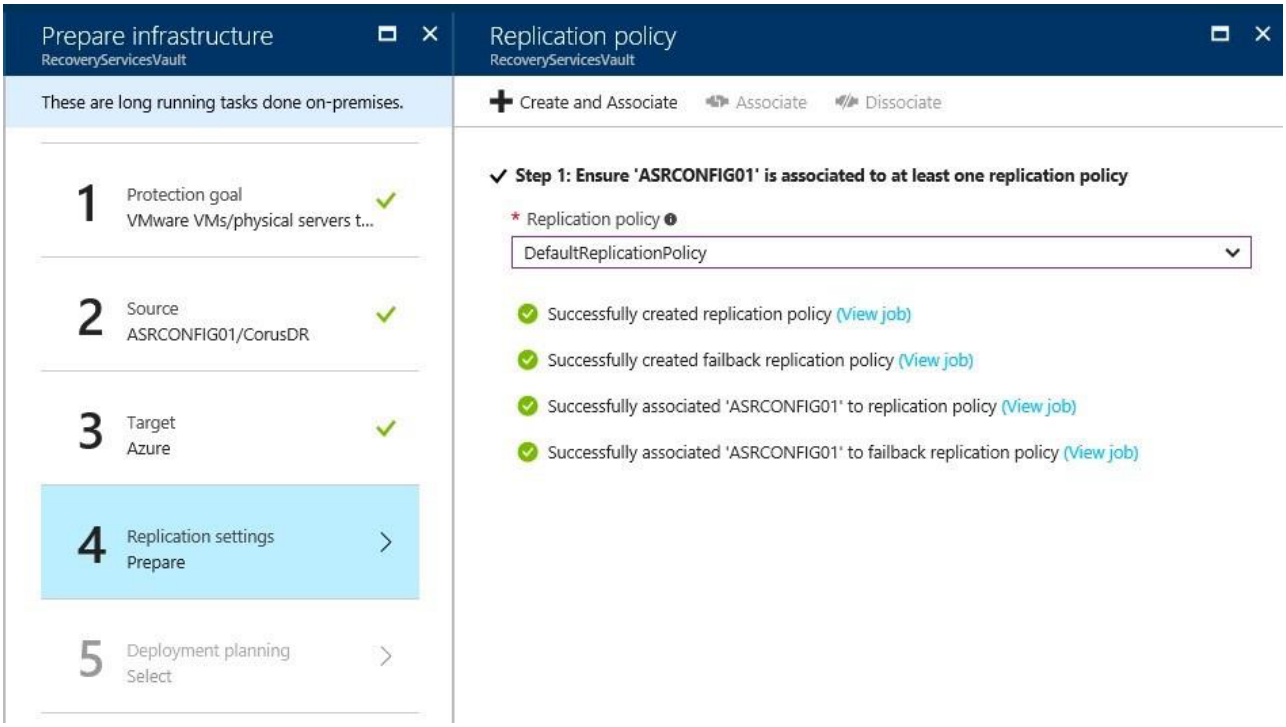
You will now create a backup policy.

The RPO threshold controls how often data recovery points are created. The Recovery Point Retention controls how long data recovery points are stored

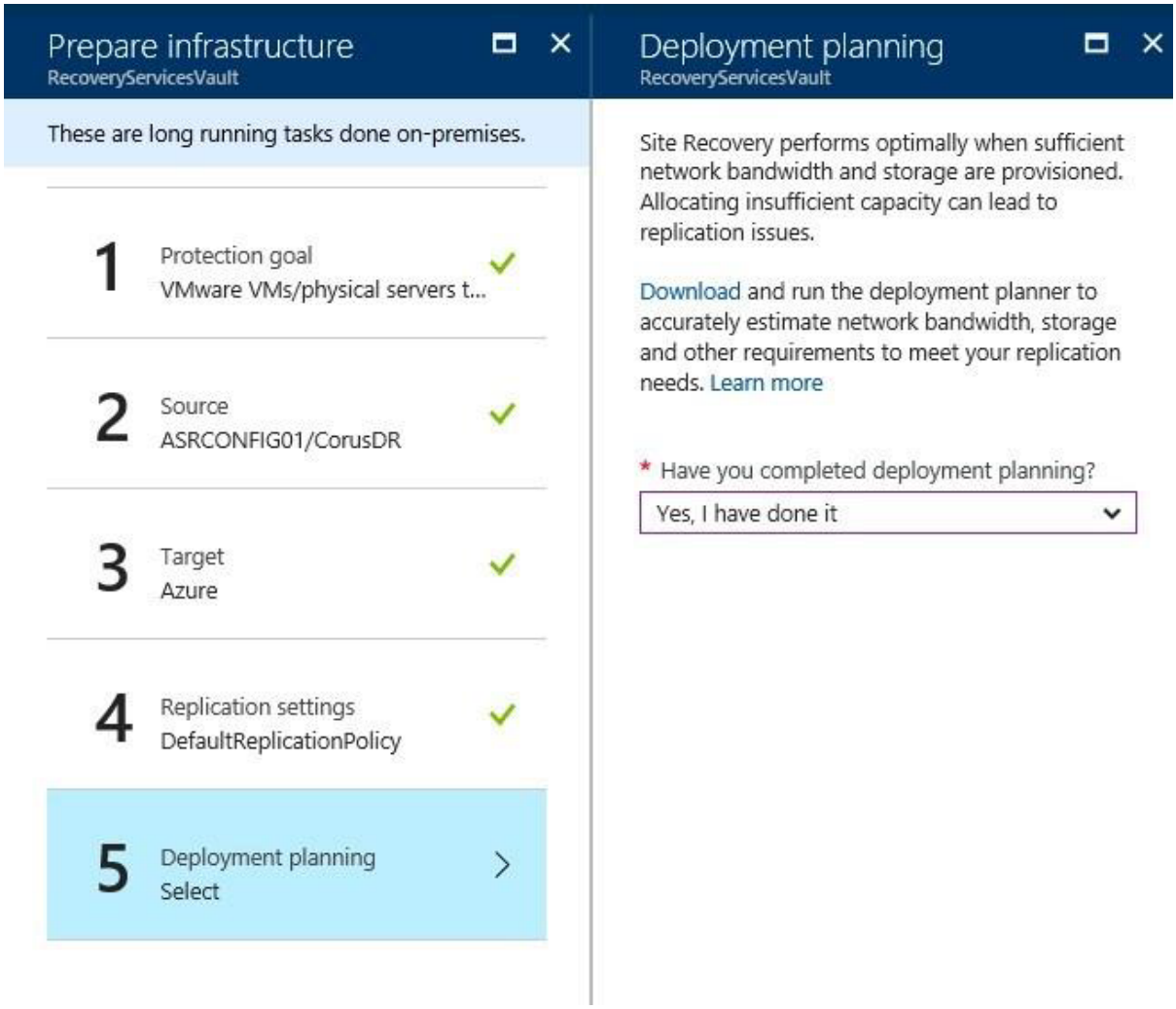
(your limit is 24 hours if you used premium storage for your blob, or 72 hours if you used standard storage). The default values work fine if you're not sure what to use, and new policies can be created and applied later.



Your replication policy should now be created and associated, and you can continue to Step 5.



Step 5 is a friendly reminder to plan for your network bandwidth and storage. In short, you should balance the frequency of backup snapshots with the storage and bandwidth requirements of your environment. If snapshot jobs take longer to run, you may want to reduce their frequency so they don't overlap.

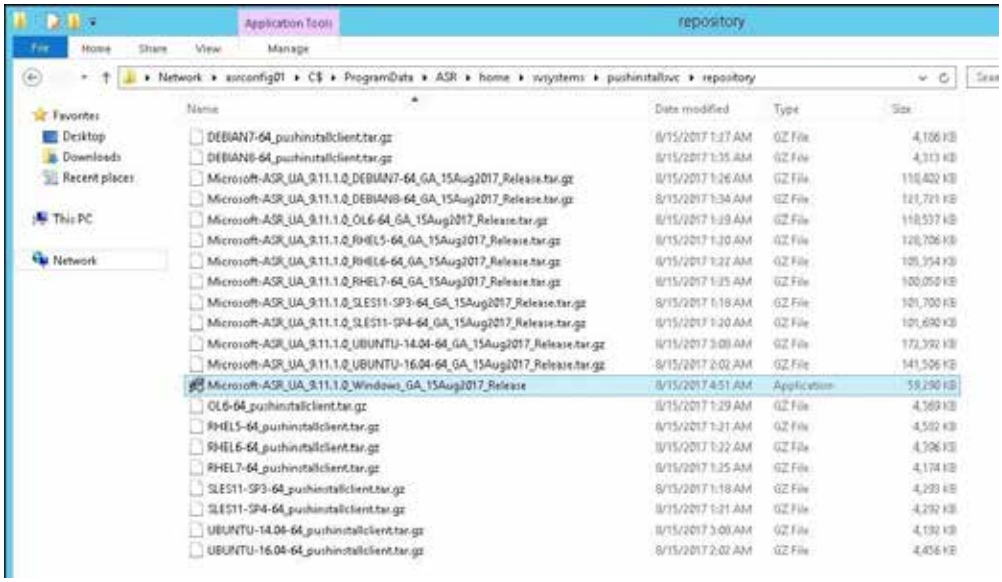


The ASR agent is also referred to as the Mobility Service, which can be deployed several ways. In this guide, we will install it manually using the GUI on our target server which will be restored to ASR.

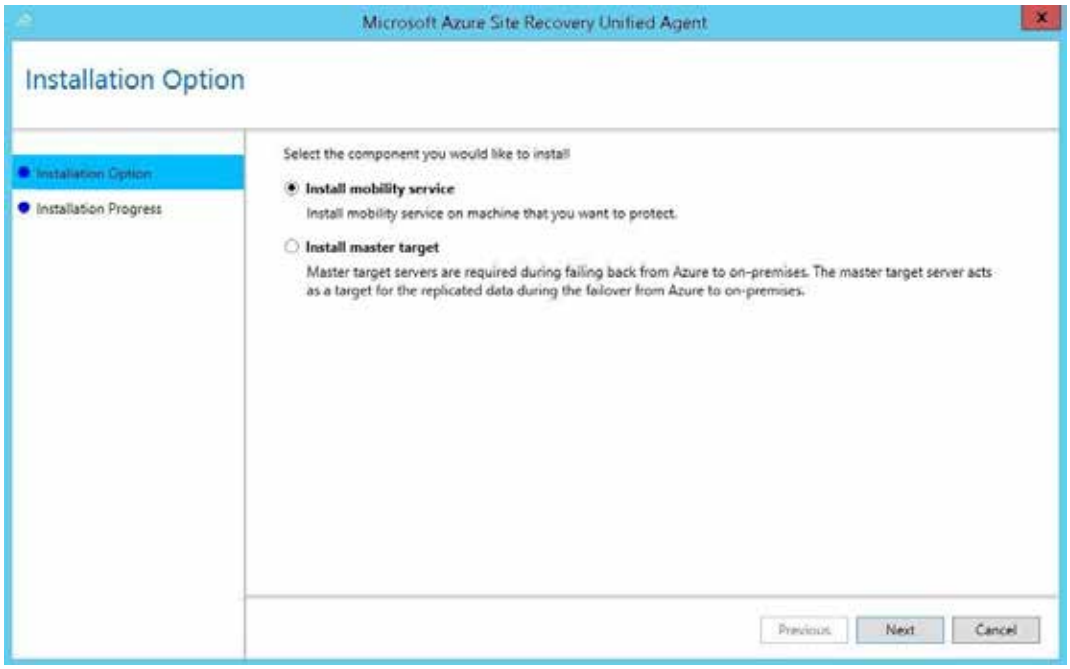
For all of the ways to install the ASR agent, check **https://docs.microsoft.com/en-us/azure/site-recovery/vmware-walkthrough-install-mobility**

On the Configuration Server, the installation files for the ASR Agent/Mobility Service are located under:

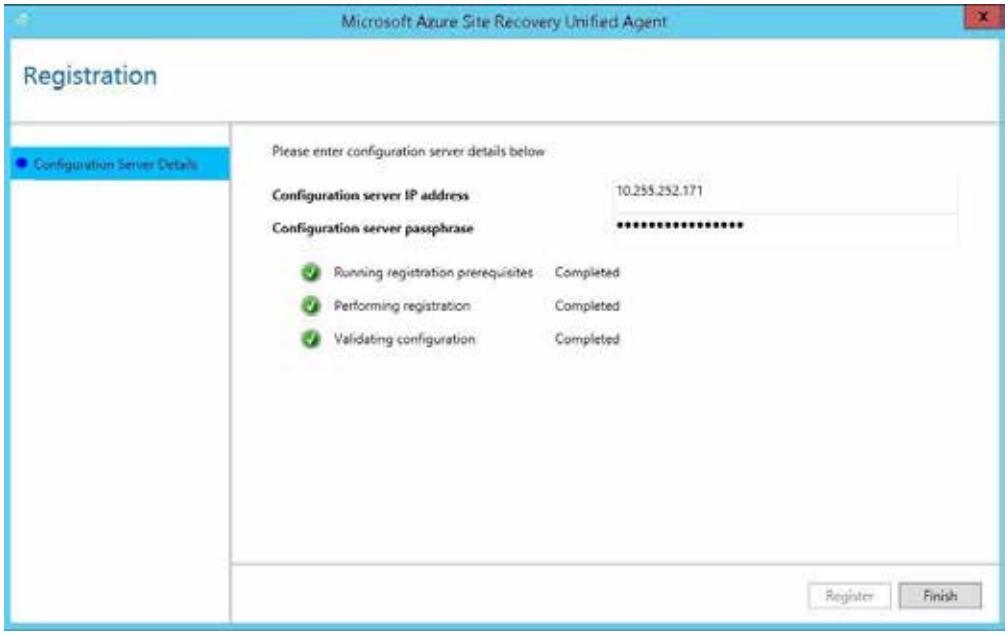
C:\ProgramData\ASR\home\svsystems\pushinstallsvc\repository
Copy them to the target server and run the binary that matches the OS of the target system.



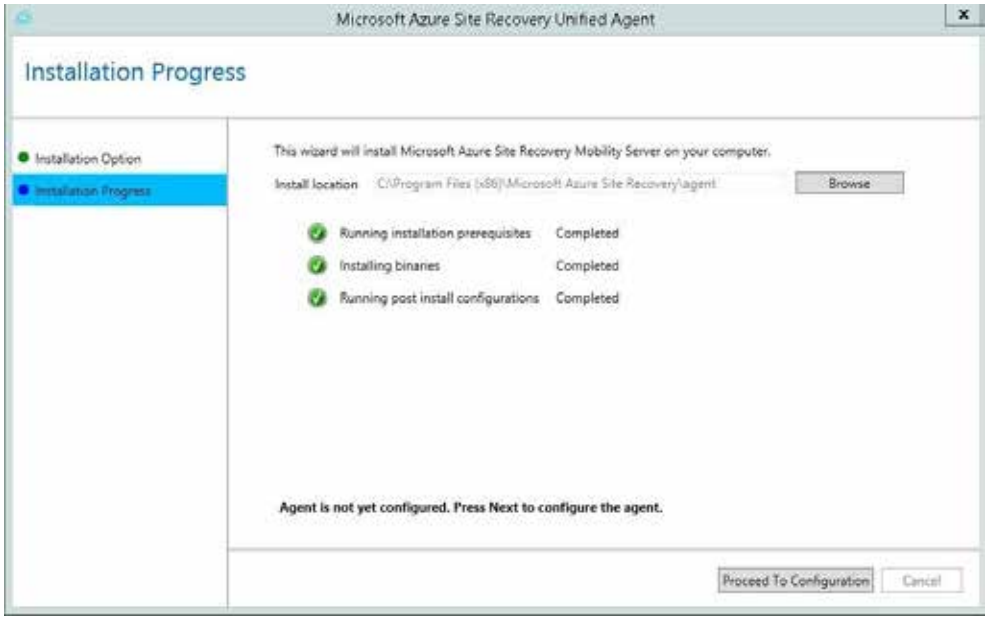
Launch the setup and choose Install Mobility Service.



Enter the IP address for your Configuration Server and enter the passphrase that was generated at the end of the Configuration Server setup process.

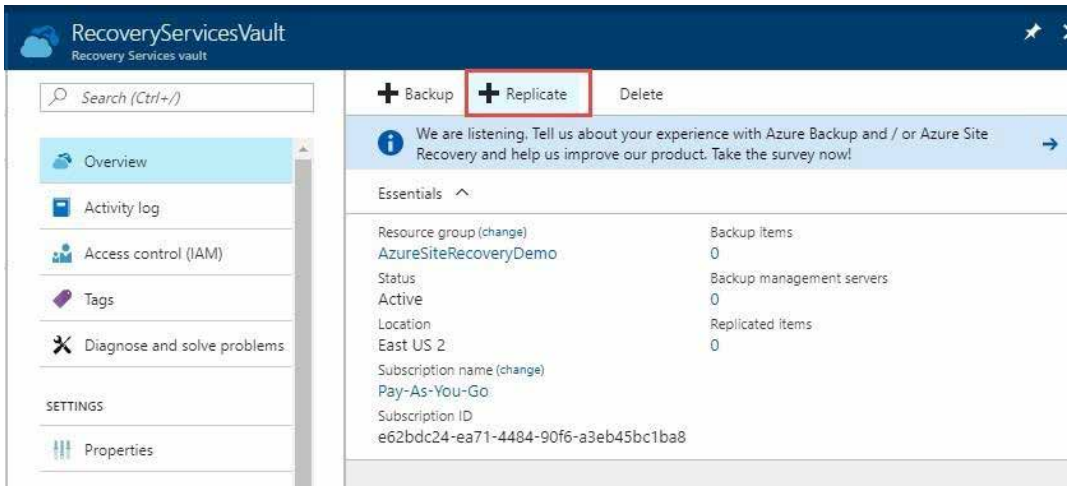


Give the agent an installation path and Proceed to Configuration, which will complete the setup process.

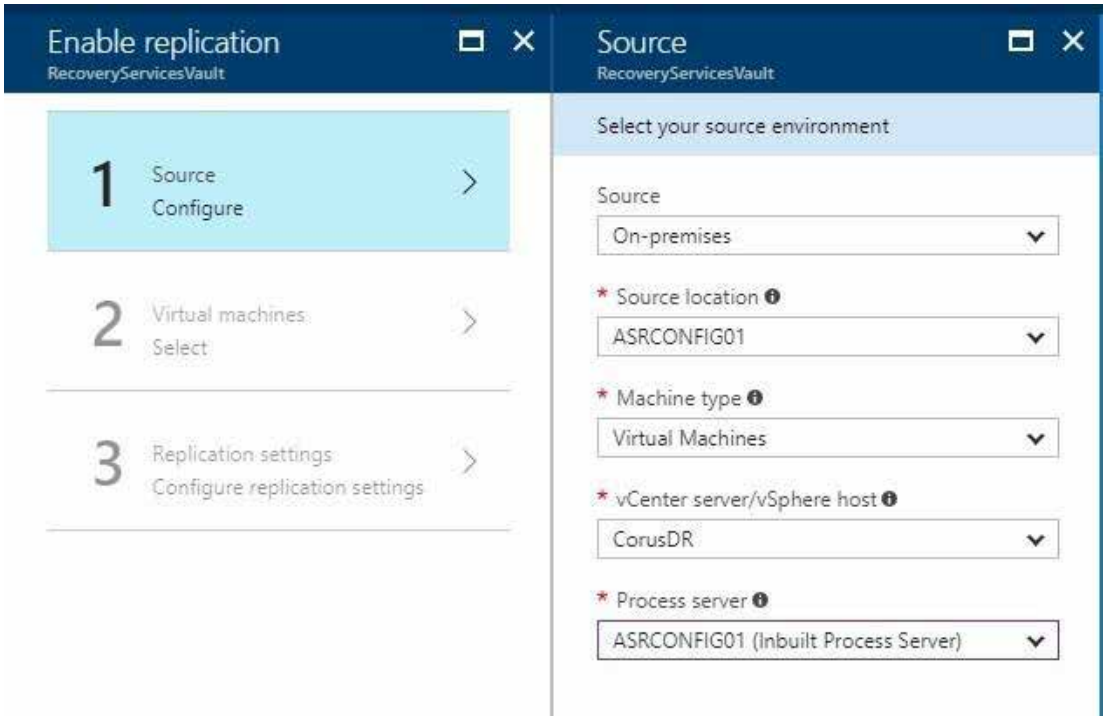


The agent will check into the Configuration Server and be available in the Azure portal.

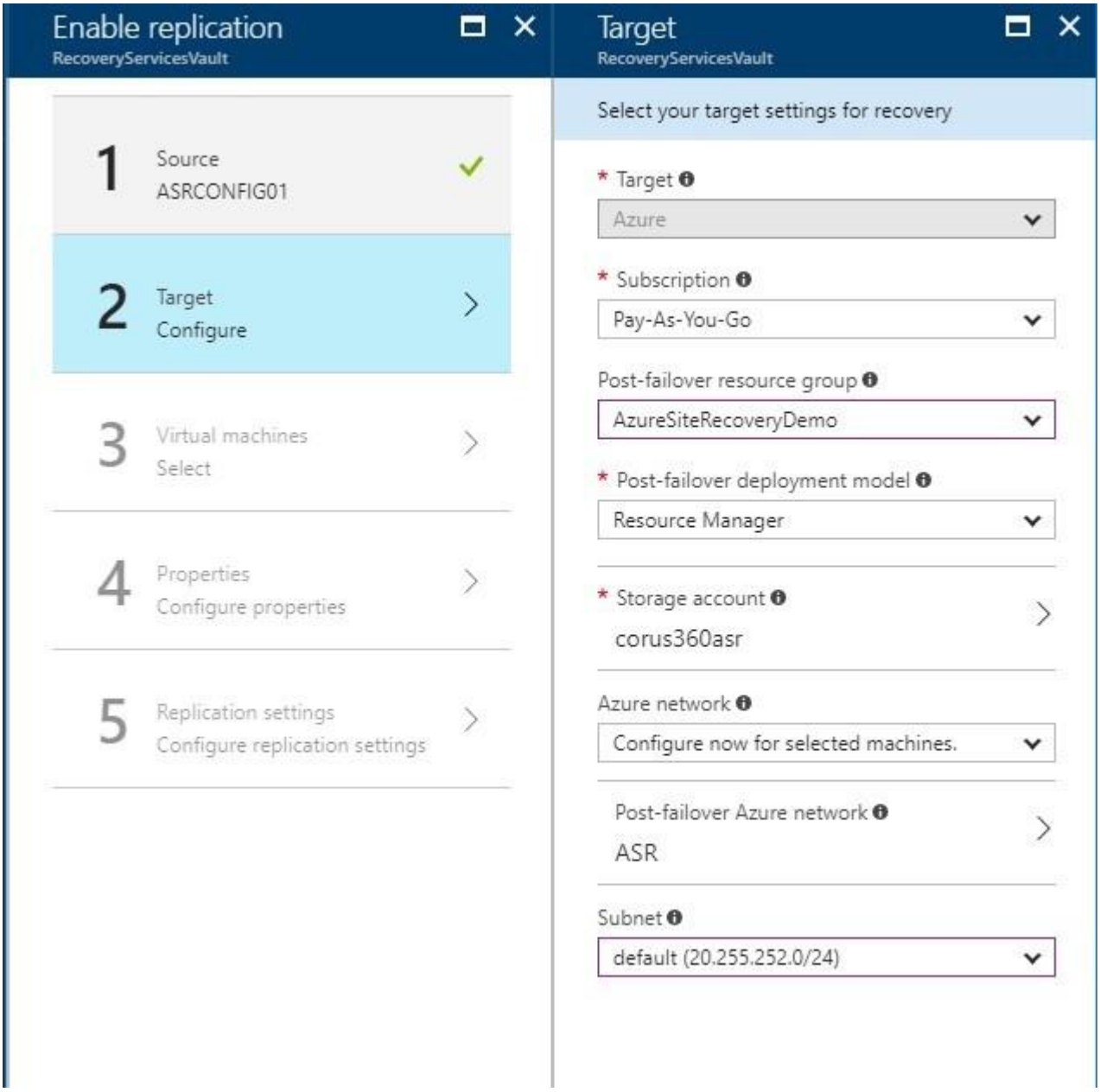
Go back to your Recovery Services Vault in Azure and choose Replicate in the top menu.



Choose your source settings which use the Configuration Server and the VMware host account.

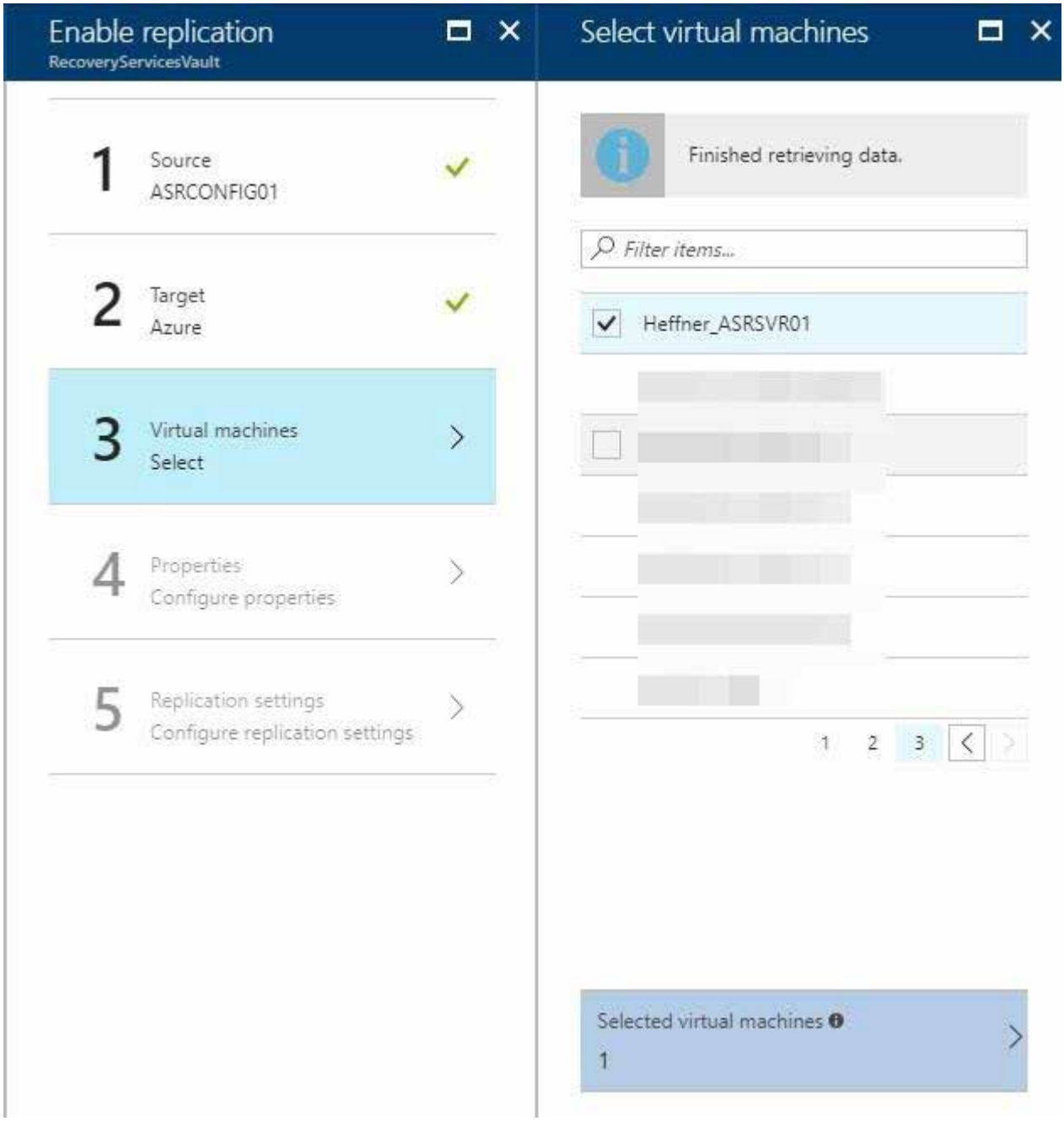


In Step 2, configure your recovery target. These settings control where a restored VM will reside once it has been failed over to Azure.



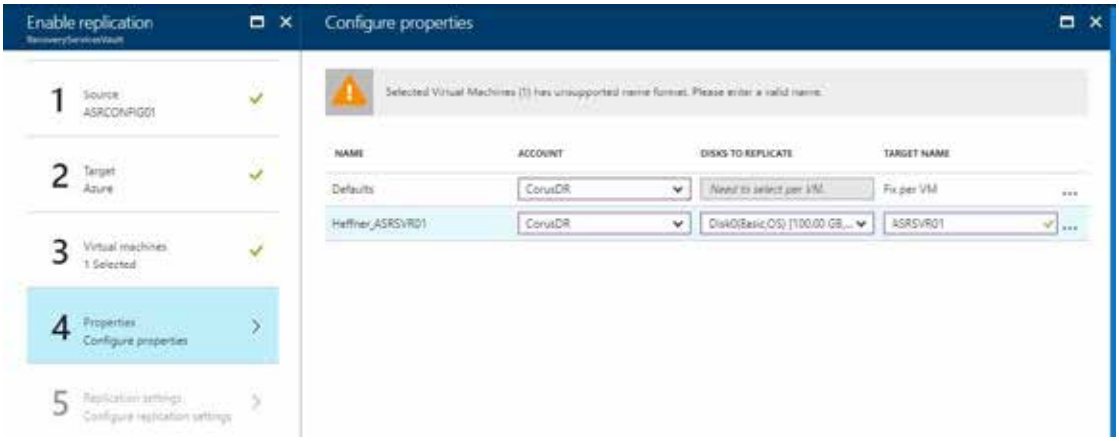
In Step 3, check the box next to the VMs that you want to be able to restore to Azure Site Recovery.

These will need the ASR agent installed if you have not done so already. In this guide, we will use just one target server.



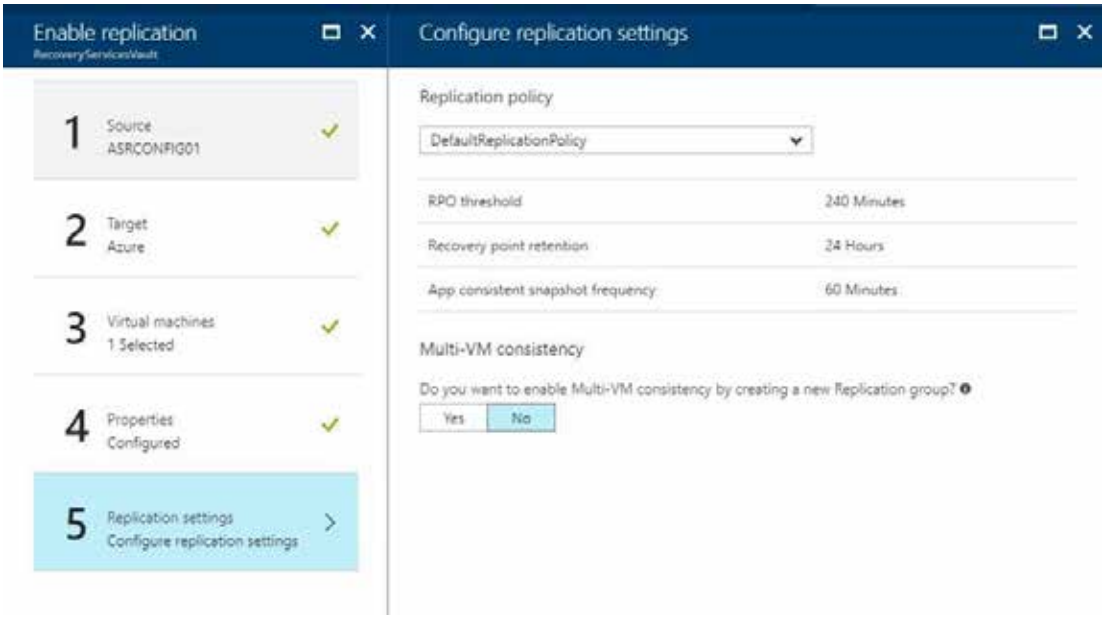
In Step 4, configure the VM settings for the restored VM in Azure.

These are properties like the size of the VM, managed disks, etc. These settings can be modified later if you're not sure what to use yet.

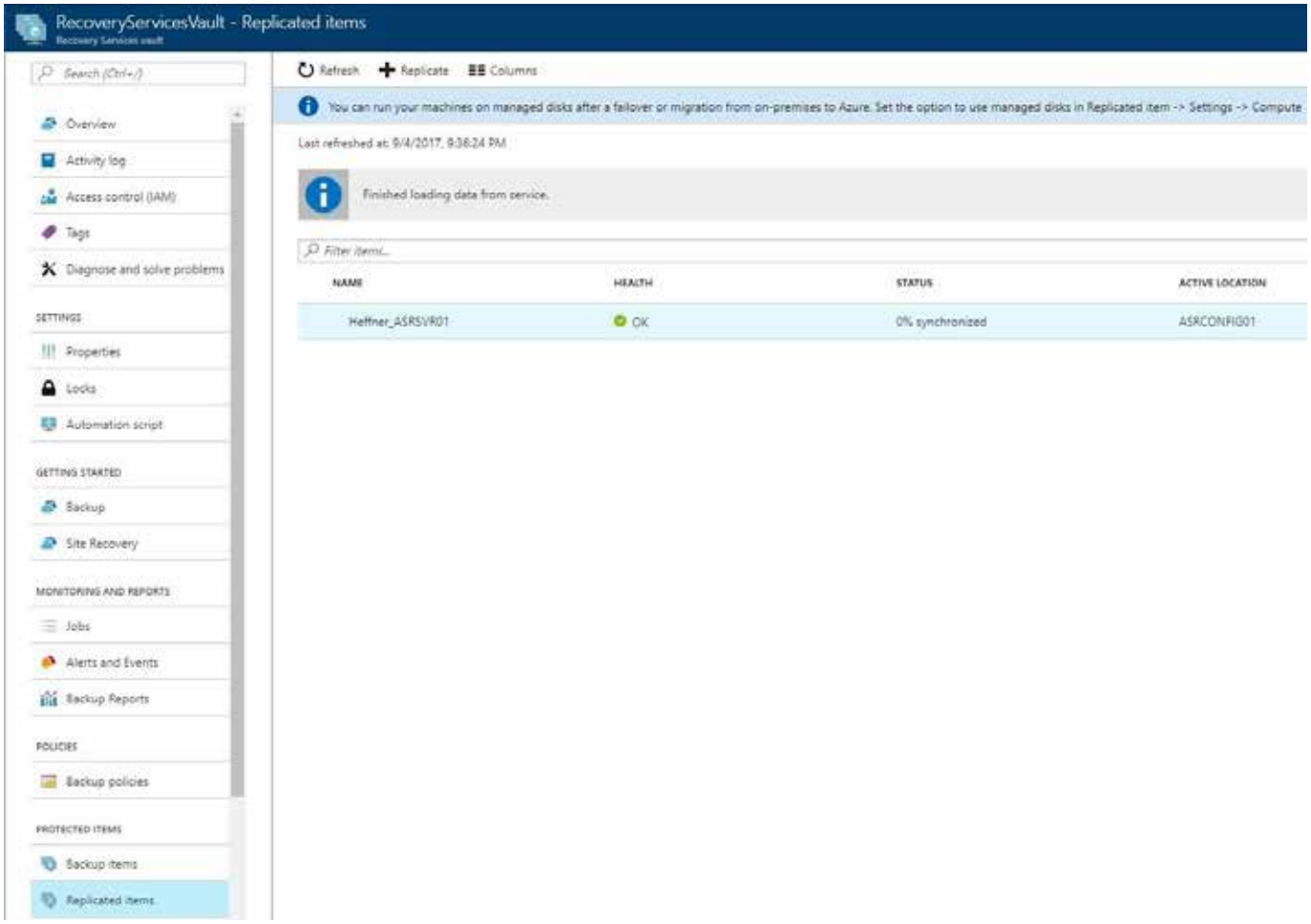


On step 5, you can choose the Replication Policy that you'd like to use, which we created in a previous step.

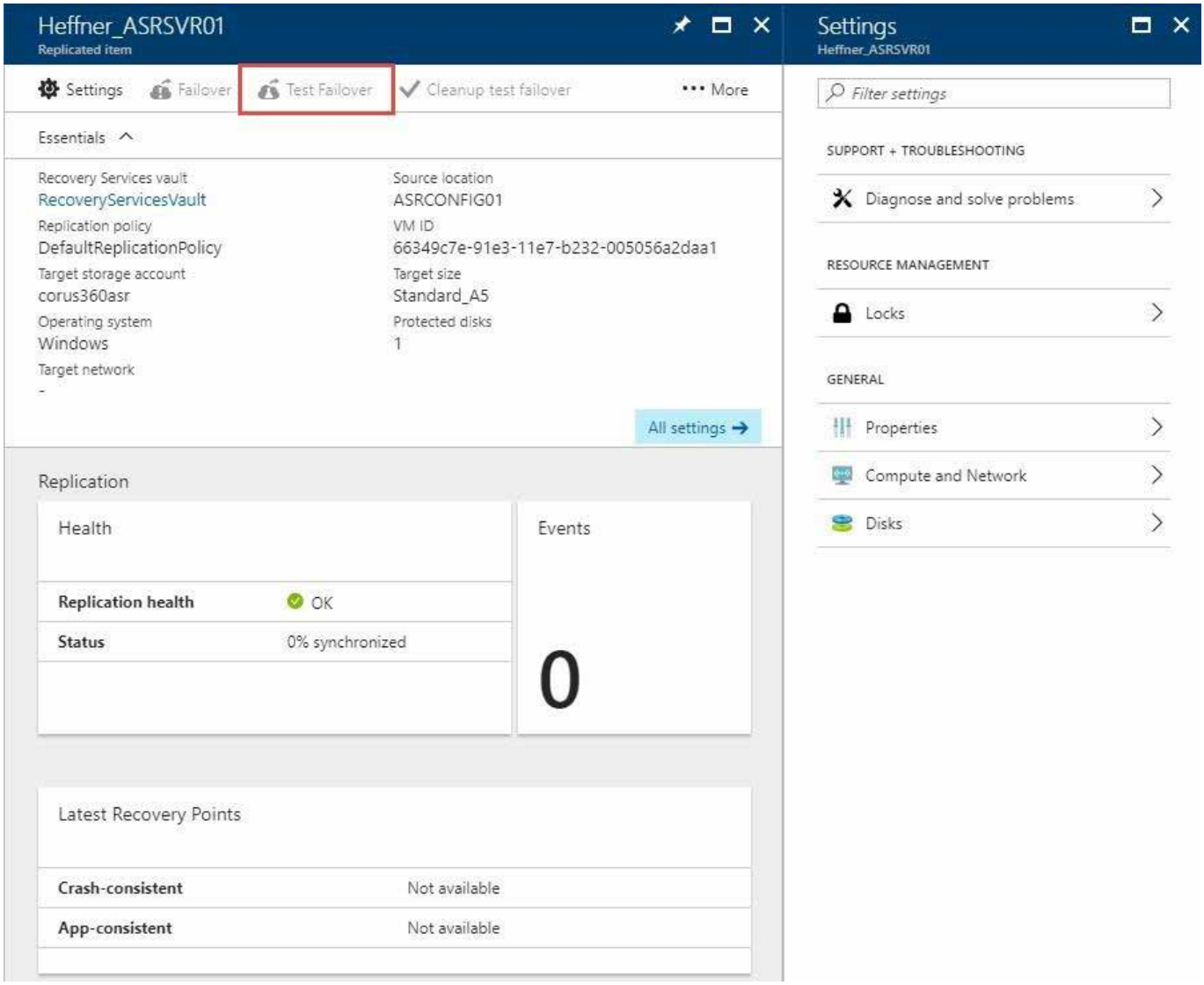
Enable Multi-VM consistency if you are backing up multiple VMs that share the same workloads.



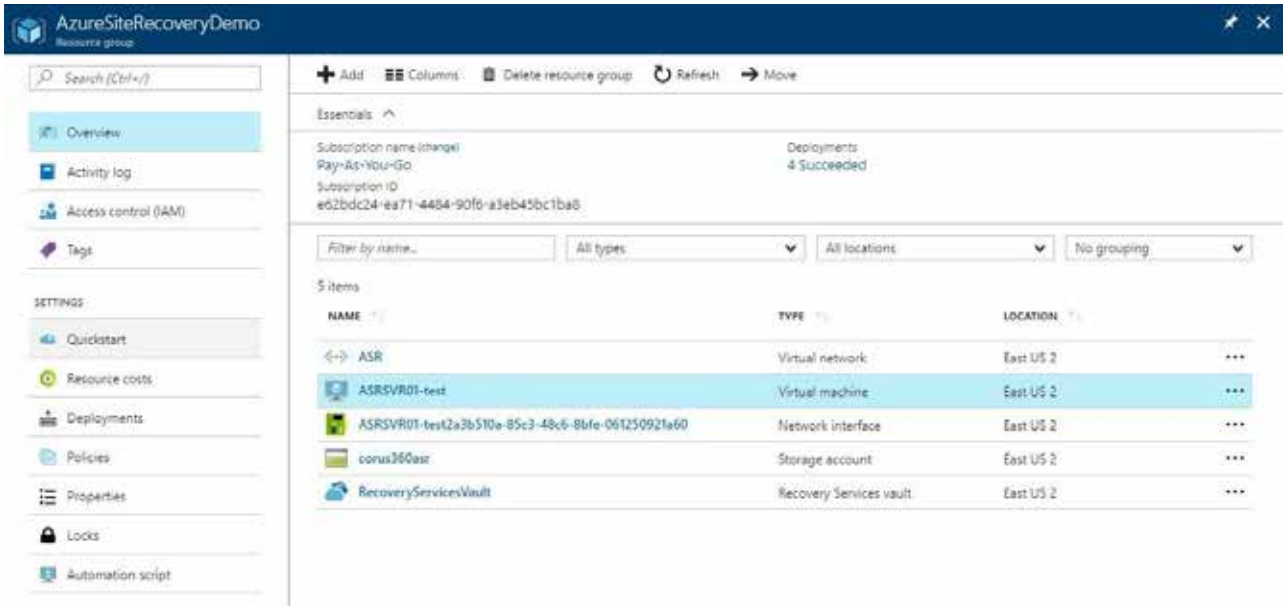
Now that replication has been configured, you can see every VM being protected under Replication Items under the Recovery Services Vault. Each item will have a synchronization status.



If you click one of the replicated items, you can view/change the properties set during initial configuration, but you can also choose to Test Failover, which will spin up an instance of the protected VM in Azure within minutes. Choosing Failover will perform a real production failover.



Once the failover completes, you should see the replicated VM running in your Resource Group. Using the test failover method will leave the original VM intact and append the name of the Azure VM with a “-test”.



From here, you can utilize your Disaster Recovery site in Azure Site Recovery or use ASR as a migration tool to easily move your systems up to Azure.