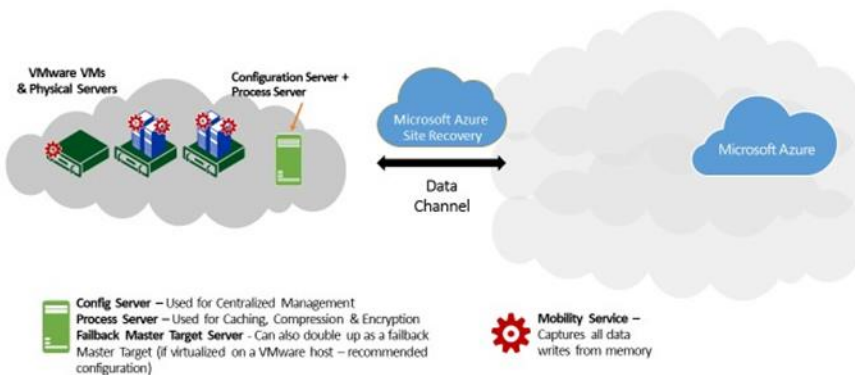


As Fabric admins of Contoso, you have decided to enable protection for various applications of your datacenters. You are the owner of a datacenter running some non-virtualized workloads (Physical machines) and a large part virtualized using the Hyper-V and VMware stacks. Since you have SLAs for different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

Key Components in VMware to Azure (Enhanced) Protection using ASR

Recover VMware and Physical Servers in Azure



Those familiar with the in-market VMware to Azure solution will be aware of the complexity involved in configuring and maintain multiple infrastructure components such as the Configuration Server on an IaaS VM, Master Target on an Azure IaaS VM and on-premises Process Server.

This process has been greatly simplified in the Enhanced VMware to Azure solution. You now only need to have a single on-premises server to get started and all the infrastructure components can run on the same server. The process of installing the various components are also greatly simplified via one single unified installer. The installer has two modes

- Configuration Server + Process Server: Install both components on the same server and get started
- Process Server: Install additional Process servers and register them with the Configuration Server as you scale

In the diagram depicted above the Green server acts as the Configuration Server + Process Server. Additionally, any Process server deployment can also double up as a Master Target server used for failback of failed over VMs running in Azure as long as

these units are deployed as virtualized servers on the ESXi host to which you are failing back.

You no longer need to run a standalone Master Target server in Azure in order to hold replicated data. Replicated data is now directly written to replica disks created on Azure blob storage by the ASR Protection service (fully PaaS). The elimination of the requirement to run any sort of Infrastructure components in the customer's Azure subscription greatly brings down the Total Cost of ownership of the solution while at the same time simplifying manageability.

The individual software components perform the following function: -

CONFIGURATION SERVER = This software component is responsible for all control plane activity and acts as the intermediary between ASR and on-premises servers. The Configuration server component communicates to ASR through the DR Provider that is installed along with this component

PROCESS SERVER = This software component receives replicated data in real-time from the machines being protected. It then performs data optimization such as caching, compression before sending the data to the ASR protection service. This component talks to the ASR Protection Service through the MARS agent which is installed along with this component

ASR-V2A (VMware & Physical to Azure) – Protect an application using a Protection Group

The objective of this lab is to familiarize you with the steps required to configure ASR DR Protection to Azure for an application that is running across multiple machines using the Protection group construct in ASR. You will end the exercise by creating a Protection group and adding virtual machines into it for replication to azure.

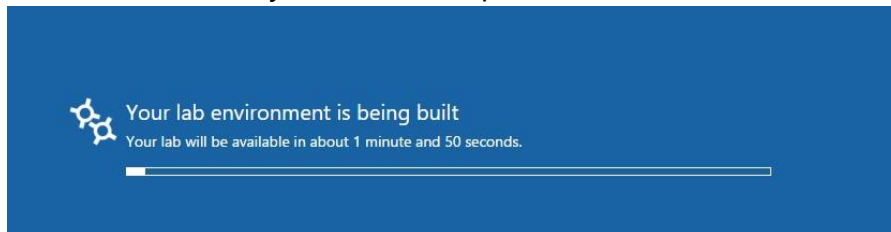
Before you begin

- 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://manage.windowsazure.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 CentOS virtual machine on it (This is the VM that you will protect and recover in Azure).
 - And a machine (ConfigurationServer) on which he will install the Configuration server and Process Server components.

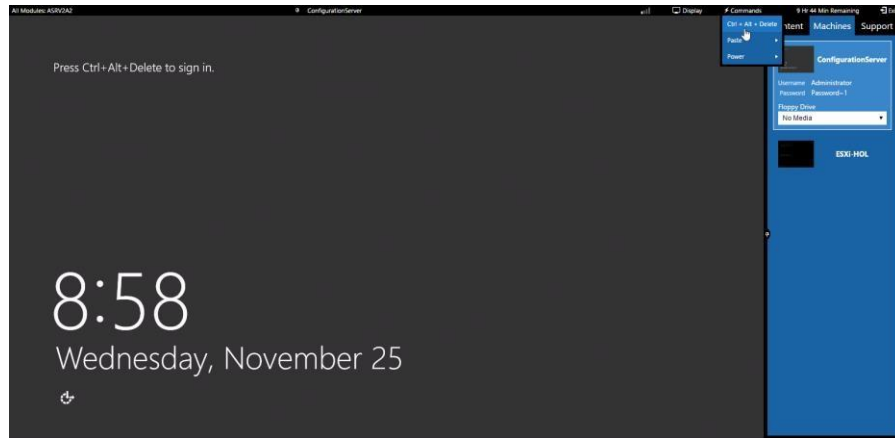
Step 1: Prepare your virtual infrastructure

- Using a web browser open the lab link provided to you. This will setup the virtual infrastructure that you will use as part of this lab



Step 2: Create a Recovery Services vault.

1. Log into the ConfigurationServer machine using the credentials provided (Administrator/Password~1). To login click the commands button and select Ctrl+Alt+Del. Enter the credentials to login

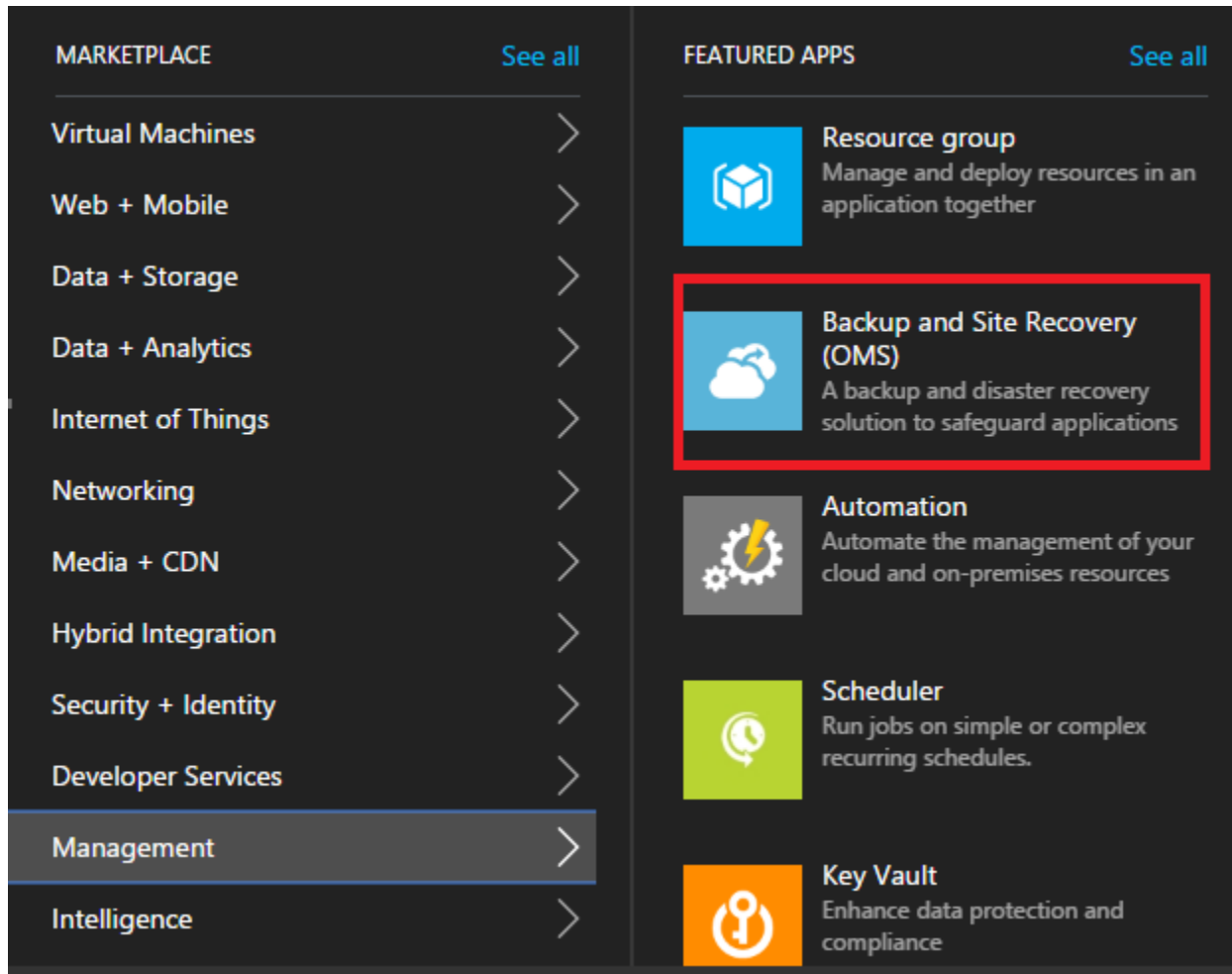


2. Once logged in, open Internet Explorer by clicking on the Internet Explorer icon pinned to the taskbar. On the browser open <https://portal.azure.com> and login using the Azure account provided to you for this lab.
3. On the Azure portal first create an Azure storage account which you'll use to protect servers to. Select **New -> Data + Storage -> Storage account**. Enter a name for your storage account. Specify the deployment model to be used: Resource Manager or Classic. Resource Manager is the recommended deployment model. Select the type of storage account: General purpose or Blob storage. General purpose is the default. If General purpose was selected, then specify the performance tier: Standard or Premium.

For the storage account (for eg: **holstore1**), select Central-US as the location and GRS as the Storage replication type. Select the subscription in which you want to create the new storage account. Specify a new resource group

4. (optional) Create an Azure virtual network that you want to failover your protected virtual machine to. Select **NEW > Networking > Virtual network**, then click **Resource Manager** from the Select a deployment model list, and then click **Create**. Specify a name for the network (for eg: **holnetwork**), choose an address space, select Central US as the location. Optionally you can create a second network to connect to for Test failover.
5. Create a Recovery Services vault. Click **New > Management > Backup and Site Recovery (OMS)**. Alternatively, you can click **Browse > Recovery**

Services vaults > **Add**. Pick a name for your vault (for eg: **HOL**) and select Central US as the location.



Recovery Services vault
Recovery Services vault - PREVIEW

* Name
ContosoVault ✓

* Subscription
ASR Canary Test Subscription 1 >

* Create a new resource group
ContosoRG ✓
[Select existing](#)

* Location
East US >

☒ Pin to dashboard

Create

6. In the Recovery Services vaults blade select your vault and click Settings. In Getting Started click **Site Recovery** > > **Step 1: Prepare Infrastructure** > **Protection goal**.
7. In **Protection goal** select **To Azure**, and select **Yes, with VMware vSphere Hypervisor**. Then click **OK**.

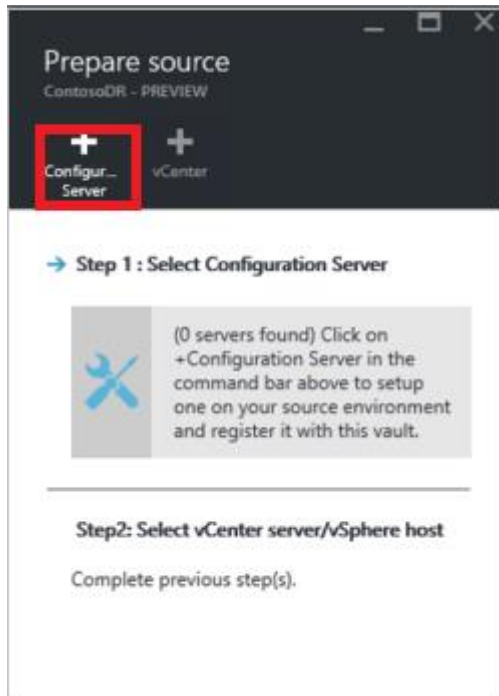
* Where do you want to replicate your machines to?
To Azure ▼

* Are your machines virtualized?
Yes, with VMware vSphere Hypervisor ▼

Step 3: Set up the source environment

Set up the configuration server and register it in the Recovery Services vault.

1. Click **Step 1: Prepare Infrastructure > Source**. In **Prepare source** click **+Configuration server** to add one.




2. In the **Add Server** blade check that **Configuration Server** appears in **Server type**.
3. Download the Site Recovery Unified Setup installation file.
4. Download the vault registration key.

Add Server

ContosoDR - PREVIEW

Server type

Configuration Server

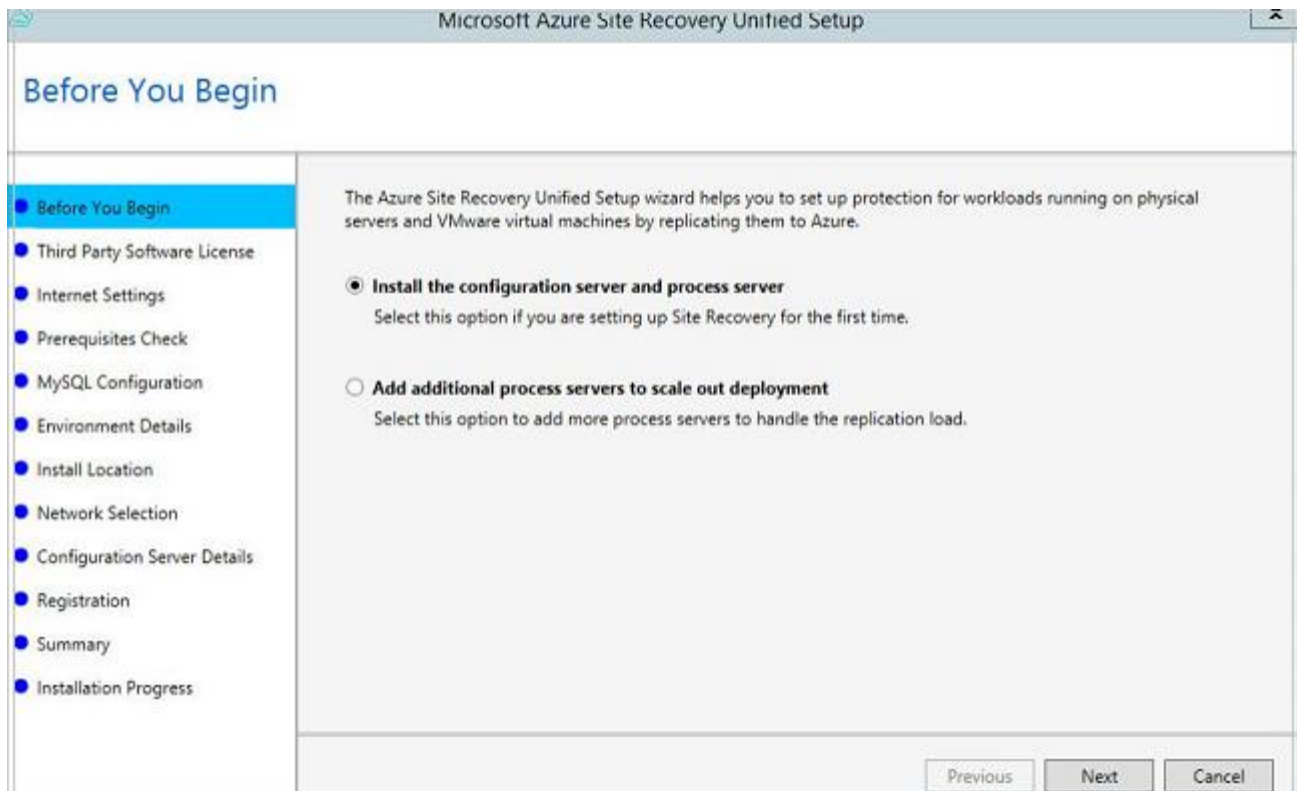
 Adding Configuration Server may take 15 minutes to 30 minutes

Register your Configuration Server

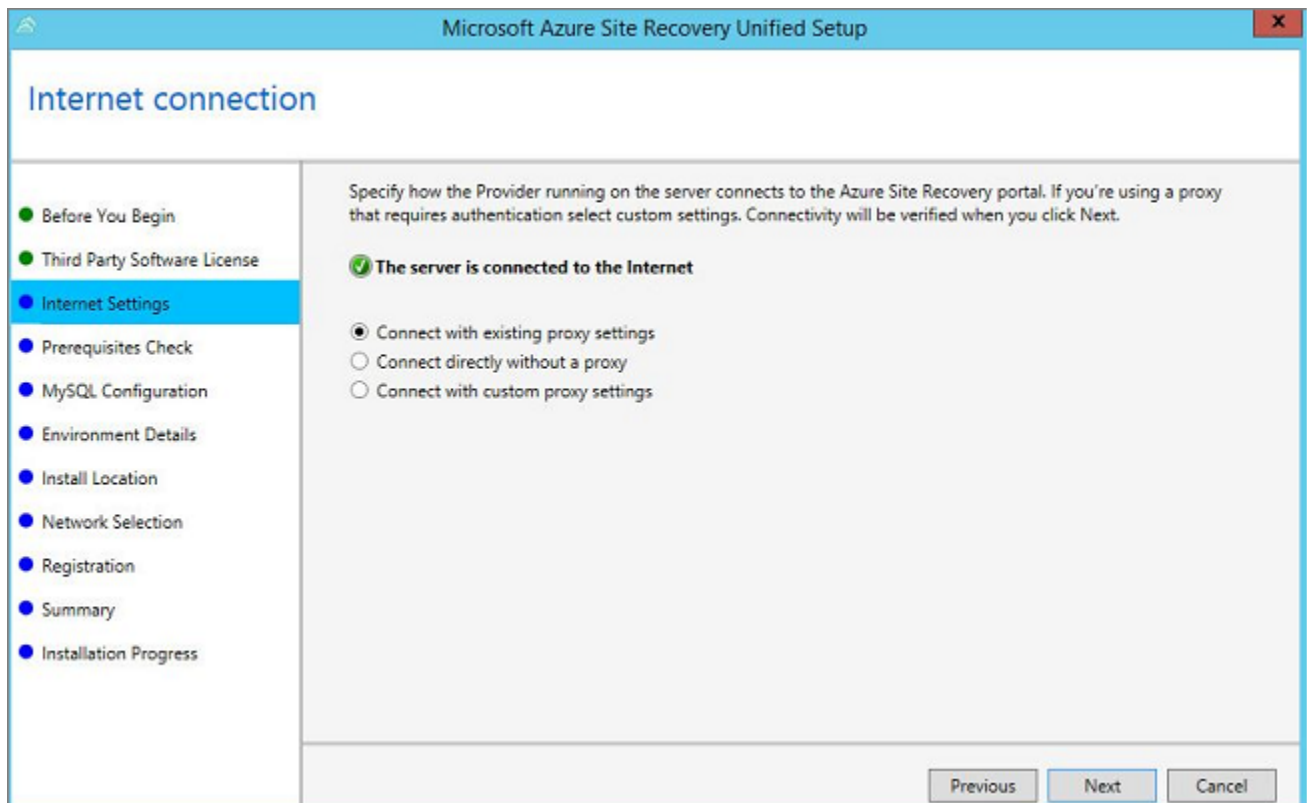
On-premises

1. Make sure server on which you plan to set up the Configuration Server is running Windows Server 2012 R2 virtual machine
2. Configure Proxy so that server can access the [Service URLs](#)
3. [Download](#) the Microsoft Azure Site Recovery Unified Setup
4. Download the vault registration key
[Download](#)
5. Run the installer to set up the Configuration Server and Process Server and use the vault registration key to register it with the vault. [Learn more.](#)
6. Run cspconfigtool.exe to create one or more management accounts on the configuration server.
7. If you're protecting VMware VMs make sure the management accounts have administrator permissions on the vCenter server/vSphere host; Server/ESXi host from which you'll replicate virtual machines. [Learn more.](#)
8. If you're protecting physical servers make sure the management accounts have administrator permissions on the physical server.

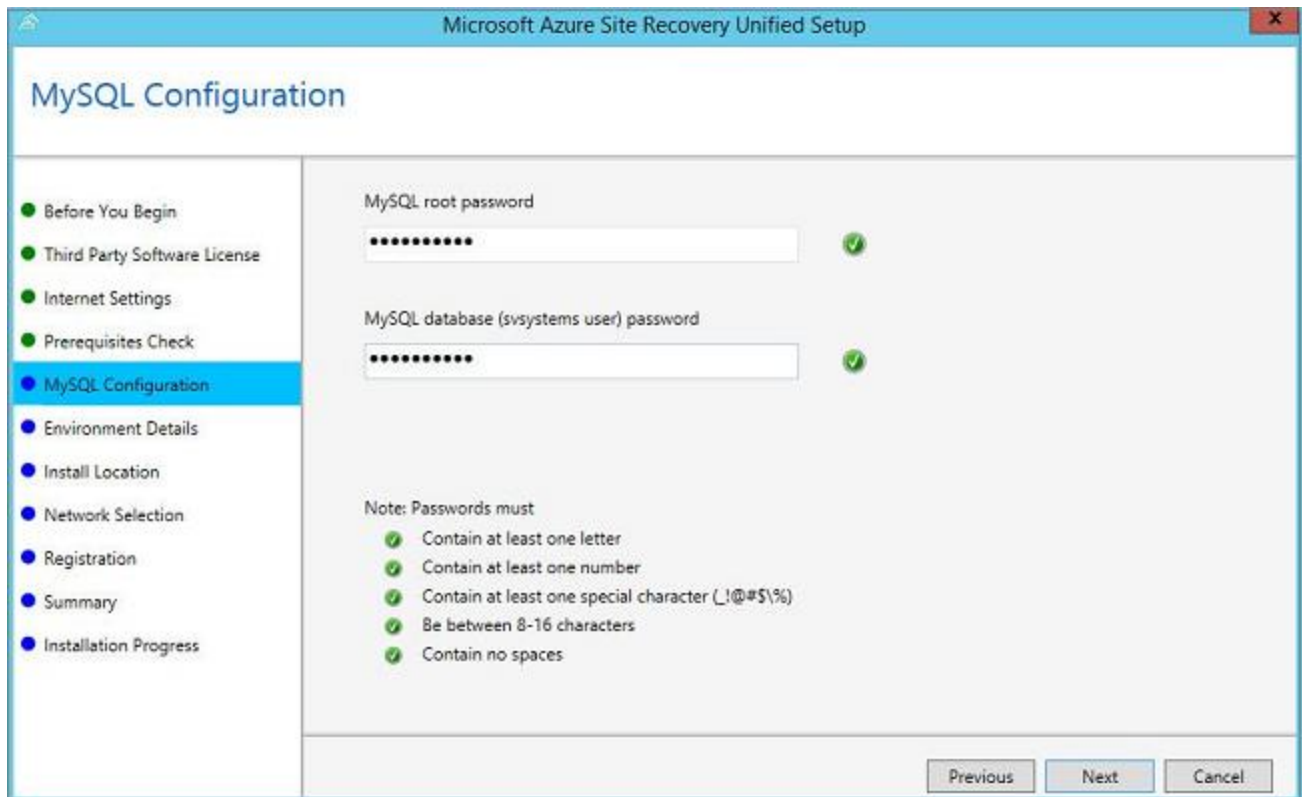
5. On the machine - **'Configuration Server'**, run Unified Setup to install the configuration server, the process server, and the master target server.
6. In **Before you begin** select **Install the configuration server and process server.**



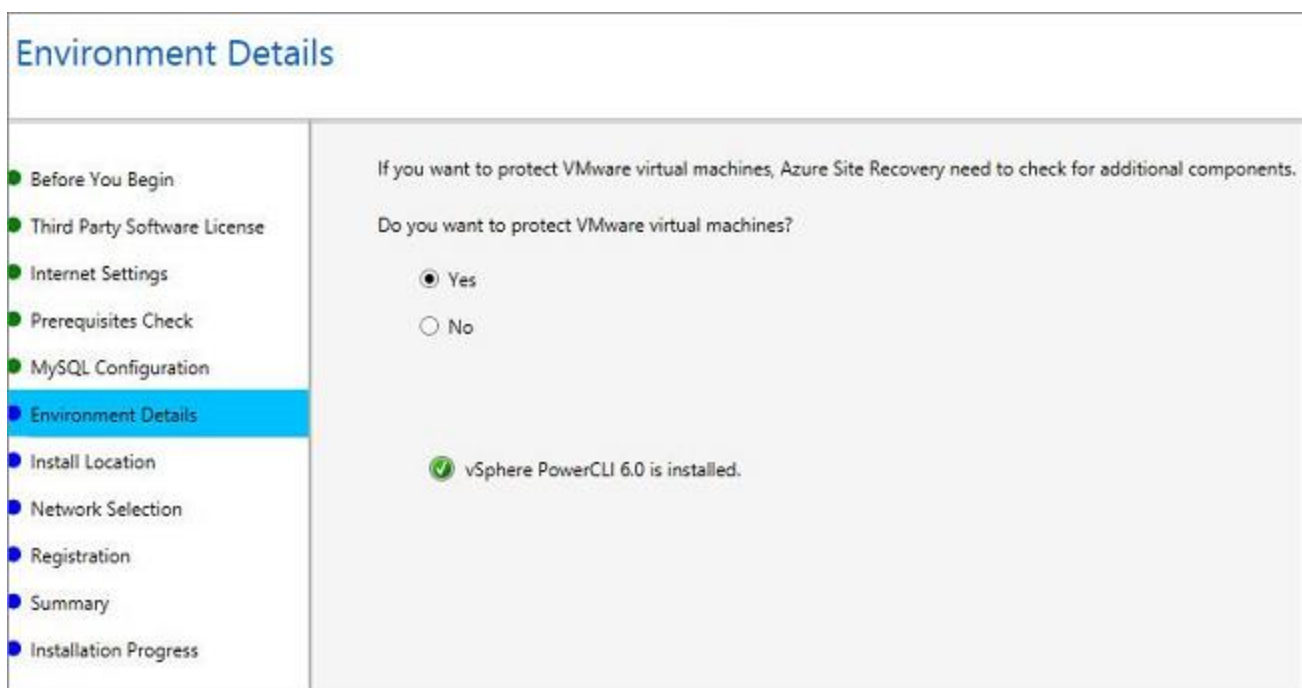
7. In **Third-Party Software License** click **I Accept** to download and install MySQL.
8. In **Internet Settings** specify how the Provider running on the configuration server will connect to Azure Site Recovery over the internet.
 - If you want to connect with the proxy that's currently set up on the machine, select **Connect with existing proxy settings**.
 - If you want the Provider to connect directly select **Connect directly without a proxy**.
 - If the existing proxy requires authentication, or you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**.



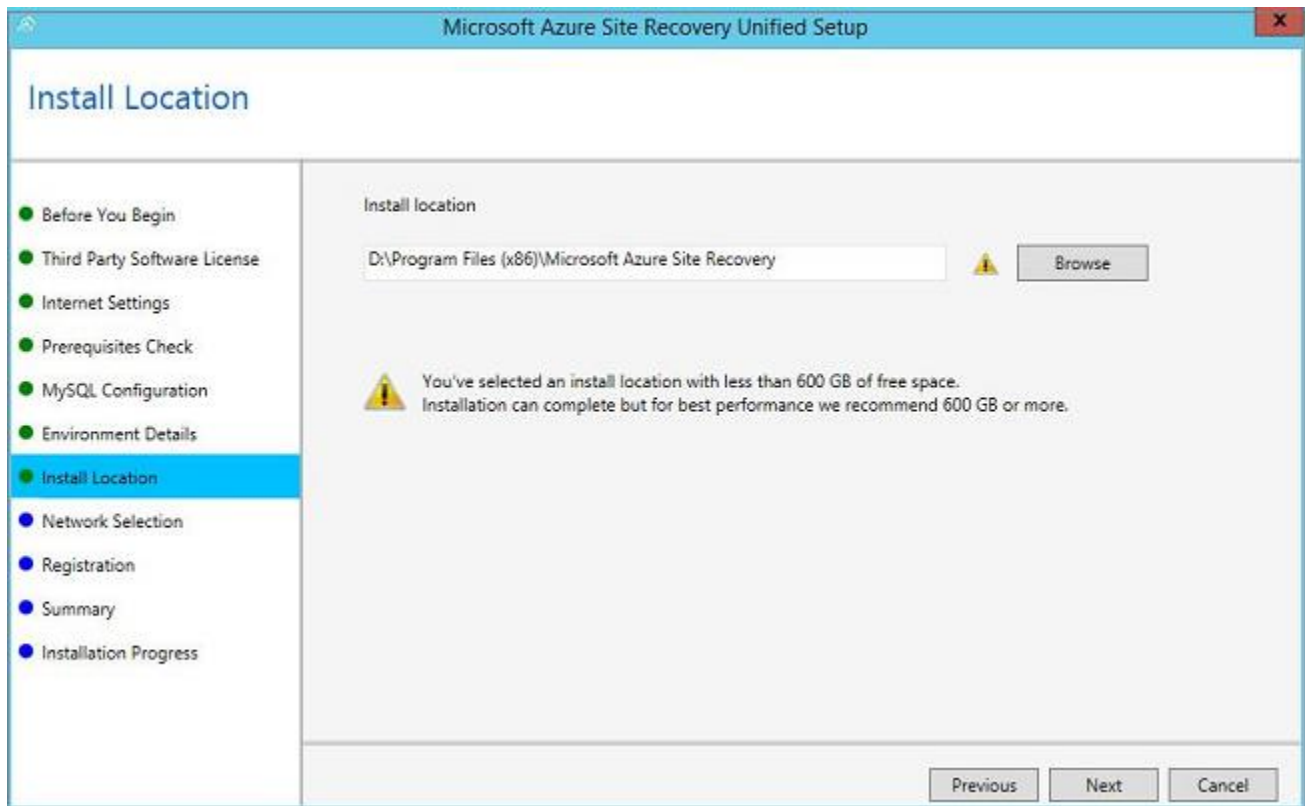
9. In **Prerequisites Check**, setup runs a check to make sure that installation can run. If a warning appears about the **Global time sync check** verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.
10. In **MySQL Configuration** create credentials for logging onto the MySQL server instance that will be installed.



11. In **Environment Details**, select whether you're going to replicate VMware VMs. If you are then setup checks that PowerCLI 6.0 is installed.



12. In **Install Location** select where you want to install the binaries and store the cache. You can select a drive that has at least 5 GB of storage available but we recommend a cache drive with at least 600 GB of free space.



13. In **Network Selection** specify the listener (network adapter and SSL port) on which the configuration server will send and receive replication data.

Microsoft Azure Site Recovery Unified Setup

Network Selection

Select a Network Interface Card(NIC) and Port for receiving replication traffic.

Network Interface: Ethernet [10.150.3.143]

Port: 9443

Note : Azure Site Recovery Unified Setup will open two ports for inbound connection on this server.

- Port 443 will be used by a web server which orchestrates replication operations
- The data transport port specified above will be used to send/receive replication data

Previous Next Cancel

14. In **Registration** browse and select the registration key you downloaded from the vault.

Microsoft Azure Site Recovery Unified Setup

Registration

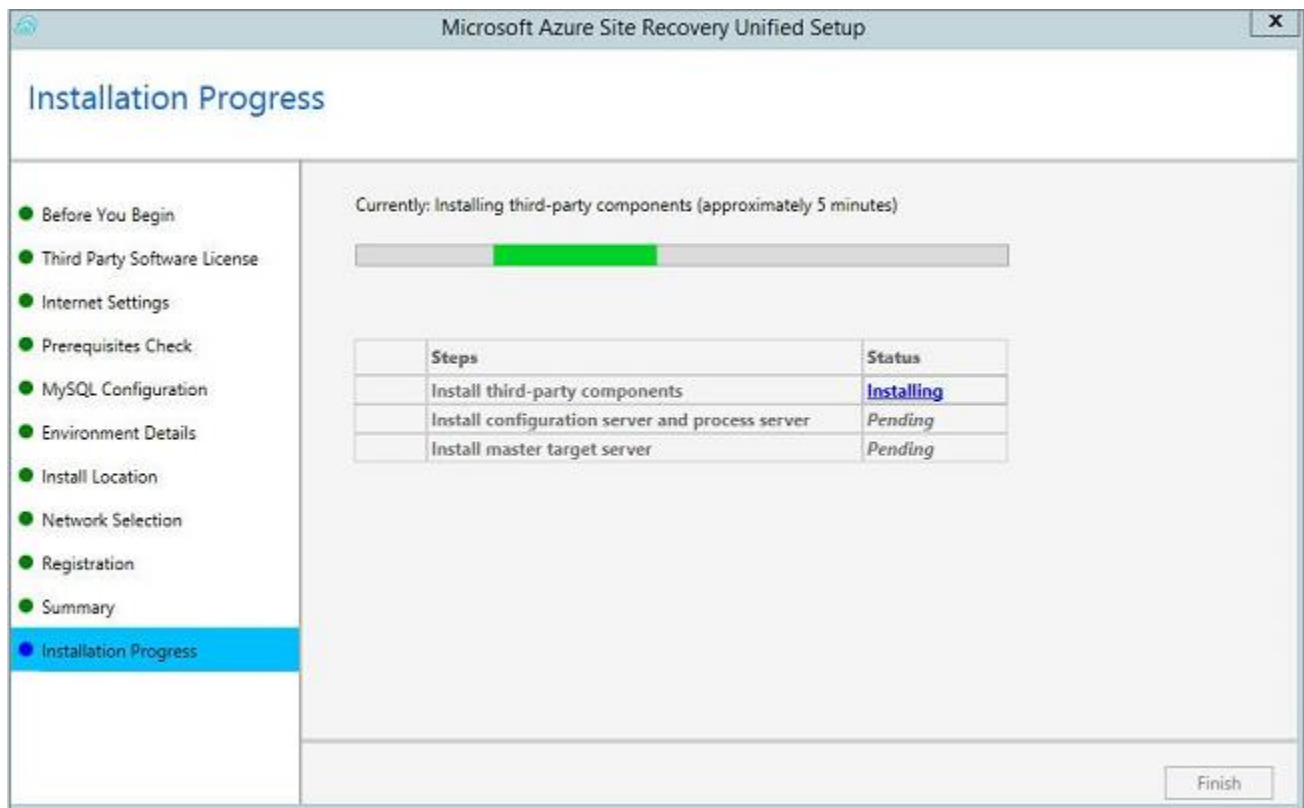
Site Recovery Registration Key

C:\Users\anoopkv\Desktop\MyValut.VaultCredentials

Browse

Previous Next Cancel

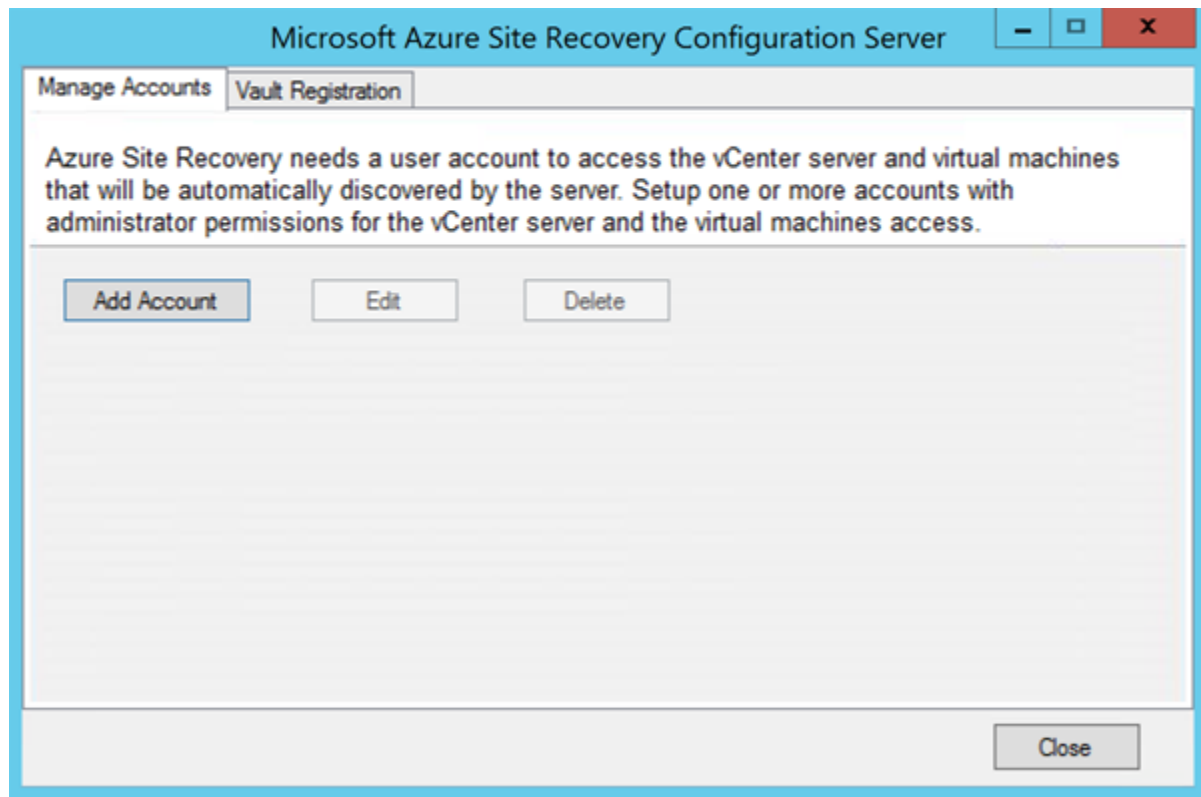
15. In **Summary** review the information and click **Install**. When installation finishes a passphrase is generated. You'll need it when you enable replication so copy it and keep it in a secure location.



16. After registration finishes the server is displayed in the **Settings** > **Servers** blade in the vault.

Add the VMware account used for automatic discovery

1. Open **CSPSConfigtool.exe**. It's available as a shortcut on the desktop and located in the [INSTALL LOCATION]\home\svsystems\bin folder.
2. Click **Manage Accounts** > **Add Account**.



- In **Account Details** add the account that will be used for automatic discovery. We will now add two accounts to the configuration server. One called '**VMwareServer**' which will be used to discover VMs running on your ESXi host and one called '**Linux**' that will be used to enable protection on your source VM
 - VMwareServer username:root password:Password~1
 - Linux username:root password:Password~1

Account Details

Friendly name (used in Azure)

User name
(Domain\User name)

Password

Confirm password

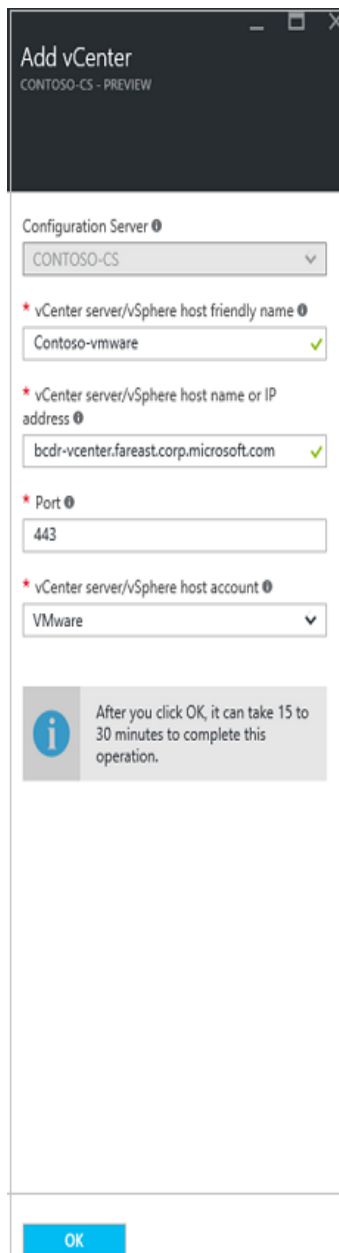
OK Cancel

Step 4: Connect to vSphere hosts and vCenter servers

1. Go to the Site Recovery vault - **HOL** you created in your Internet Explorer.
2. Click **Prepare infrastructure** > **Source**. In **Prepare source** select the configuration server, and click **+vCenter** to add a vSphere host or vCenter server.
3. In **Add vCenter** Provide the details of your ESXi host as follows
 - IP address: 192.168.0.2
 - Port : 443
 - Friendly name: Pick any name of your choice

- Process Server: Select your Process server from the dropdown box. This is the same as your Configuration Server (ConfigurationServer)
- Account: VMwareServer (This is the account you added in the previous step)

NOTE: It may take some time (5-10 minutes) for the accounts to show up in the portal dropdown. If you don't see any accounts listed on the portal cancel the operation and retry after sometime. Alternatively, you can refresh your configuration server from the server's page and retry



The screenshot shows a window titled "Add vCenter" with a subtitle "CONTOSO-CS - PREVIEW". The window contains several input fields and a confirmation button. The "Configuration Server" is set to "CONTOSO-CS". The "vCenter server/vSphere host friendly name" is "Contoso-vmware". The "vCenter server/vSphere host name or IP address" is "bcdr-vcenter.fareast.corp.microsoft.com". The "Port" is "443". The "vCenter server/vSphere host account" is "VMware". A message box at the bottom states: "After you click OK, it can take 15 to 30 minutes to complete this operation." An "OK" button is at the bottom right.

Add vCenter
CONTOSO-CS - PREVIEW


Configuration Server ⓘ
CONTOSO-CS ▼

* vCenter server/vSphere host friendly name ⓘ
Contoso-vmware ✓

* vCenter server/vSphere host name or IP address ⓘ
bcdr-vcenter.fareast.corp.microsoft.com ✓

* Port ⓘ
443

* vCenter server/vSphere host account ⓘ
VMware ▼

 After you click OK, it can take 15 to 30 minutes to complete this operation.

OK

Step 5: Set up the target environment

Verify you have a storage account for replication, and an Azure network to which Azure VMs will connect after failover.

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.

Target
ContosoDR - PREVIEW

+ Storage account + Network

✓ **Step 1 : Select Azure subscription**

* Subscription ⓘ
ASR Canary Test Subscription 3 ▼

* Select the deployment model used after failover ⓘ
Resource Manager ▼

✓ **Step 2 : Ensure that at least one compatible Azure storage account exist**

Storage account(s) ⓘ
Found 30 compatible Azure storage accounts out of 50 available in the subscription

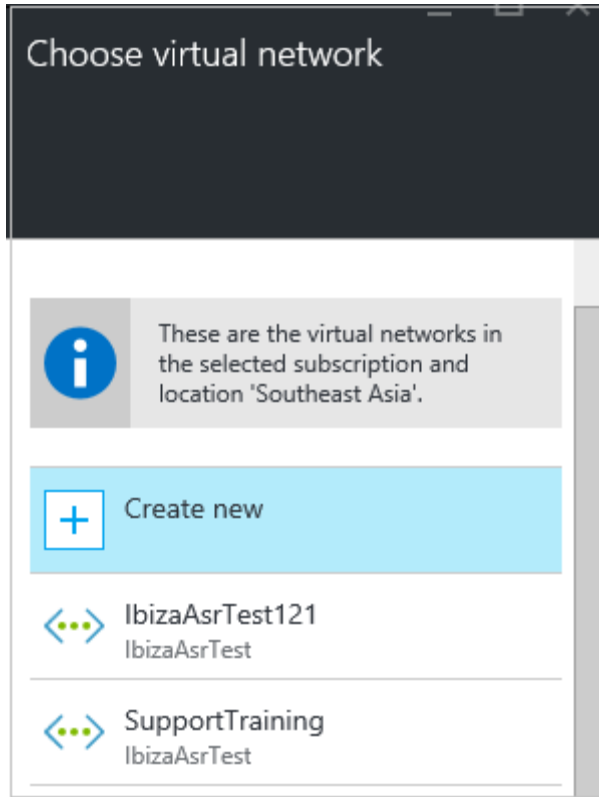
✓ **Step 3 : Ensure that at least one compatible Azure virtual network exist**

Network(s) ⓘ
Found 4 compatible Azure virtual networks out of 6 available in the subscription

OK

Site Recovery checks that you have one or more compatible Azure storage accounts and networks.

3. Select the Azure network – **holnetwork** that you created earlier.



Step 6: Set up replication settings

1. To create a new replication policy click **Prepare infrastructure > Replication Settings > +Create and Associate**.
2. In **Create and associate policy** specify a policy name – ***vmware-policy***
3. In **RPO threshold**: specify the RPO limit. Alerts will be generated when continuous replication exceeds this limit.
4. In **Recovery point retention**, specify in hours how long the retention window will be for each recovery point.
5. In **App-consistent snapshot frequency**, specify how often (in minutes) recovery points containing application-consistent snapshots will be created.

6. When you create a replication policy, by default a matching policy is automatically created for failback. For example, if the replication policy is **rep-policy** then the failback policy will be **rep-policy-failback**. This policy isn't used until you initiate a failback.
7. Click **OK** to create the policy.

Create and associate policy
ContosoDR - PREVIEW

* Name ⓘ
vmware-policy x

Source type ⓘ
VMware / Physical machines v


Target type ⓘ
Azure v

* RPO threshold in mins ⓘ
15

* Recovery point retention in hours ⓘ
24

* App-consistent snapshot frequency in mins ⓘ
60

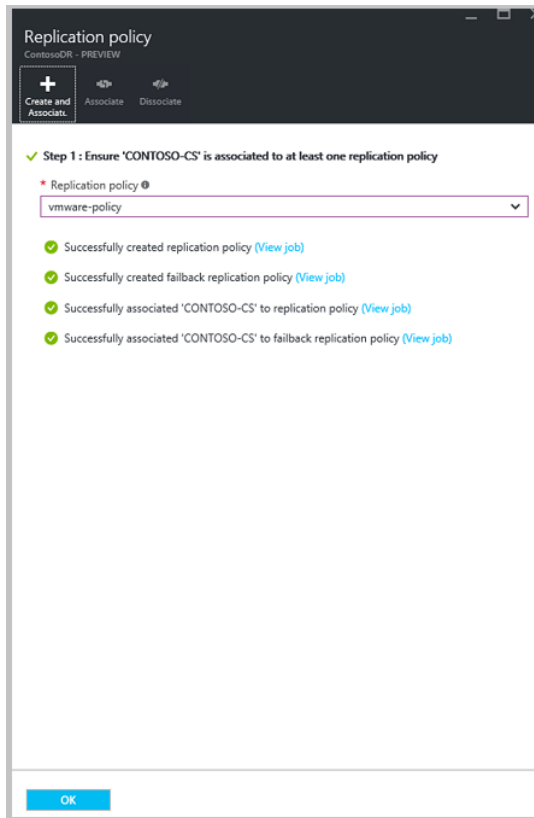
Failback replication policy name ⓘ
Enter policy name

 A replication policy for failback from Azure to on-premises will be automatically created with the same settings.

Associated Configuration Server ⓘ
CONTOSO-CS

OK

8. When you create a new policy it's automatically associated with the configuration server. Click **OK**.



Step 6: Replicate applications

Install the Mobility service: The first step in enabling protection for virtual machines and physical servers is to install the Mobility service. You can do this in a couple of ways:

For this lab scenario, we will do a process server push based installation. When you enable replication on a machine, push and install the Mobility service component from the process server. Note that push installation won't occur if machines are already running an up-to date version of the component.

An account needs to be present on the VM you want to protect that can be used by the process server to access the machine – As mentioned earlier, in this lab scenario, it will be 'Linux'

Note:

1. Click **Step 2: Replicate application > Source**.
2. In the **Source** blade > **Source** select the configuration server.

3. In **Machine type** select **Virtual Machines** or **Physical Machines**.
4. In **vCenter/vSphere Hypervisor** select the ESXI host – **ESXi – HOL**.
5. Select the process server – **ConfigurationServer** Then click **OK**.

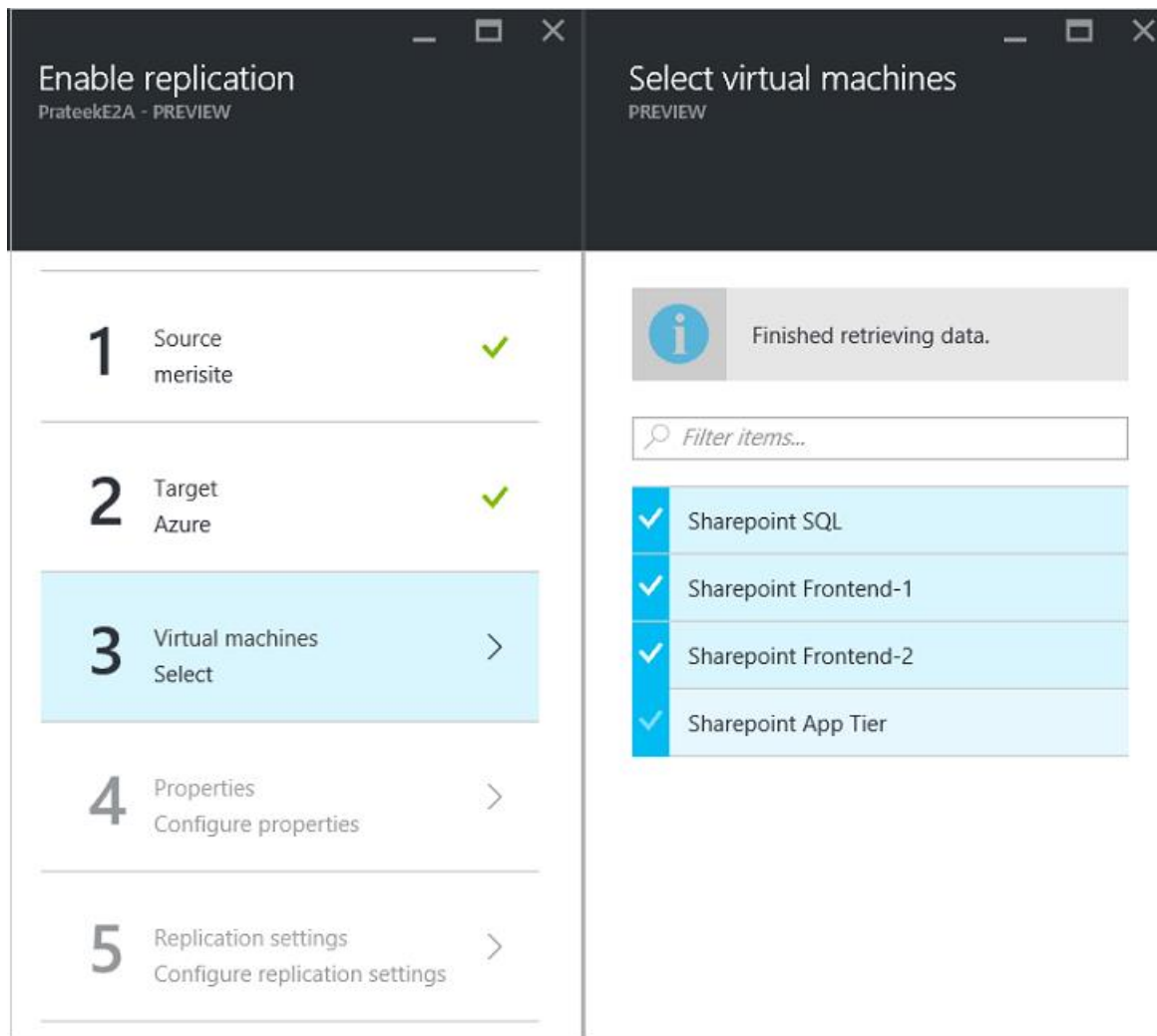
The screenshot displays the 'Enable replication' wizard interface. The left sidebar shows a sequence of five steps: 1. Source (CONTOSO-CS), 2. Target (Configure), 3. Virtual machines (Select), 4. Properties (Configure properties), and 5. Replication settings (Configure replication settings). The first step, 'Source', is highlighted in light blue. The main panel on the right, titled 'Source', contains the instruction 'Select your source environment' and four dropdown menus, each preceded by a red asterisk and a help icon: 'Source' (set to CONTOSO-CS), 'Machine type' (set to Virtual Machines), 'vCenter server/vSphere host' (set to Contoso-vmware), and 'Process server' (set to contoso-cs (Inbuilt Process Server)). At the bottom of the wizard, there is a grey 'Enable replication' button on the left and a blue 'OK' button on the right.

6. In **Target** select the vault subscription, and in **Post-failover deployment model** select the model - resource management that you want to use in Azure after failover.
7. Select the Azure storage account you'll use for replicating data - **holstore1**

8. Select the Azure network and subnet to which Azure VMs will connect when they're spun up after failover – **holnetwork**. Select **Configure now for selected machines** to apply the network setting to all machines you select for protection.

The image shows two side-by-side windows from the 'ContosoDR - PREVIEW' application. The left window, titled 'Enable replication', contains a vertical list of five steps: 1. Source (CONTOSO-CS, marked with a green check), 2. Target (Configure, highlighted in light blue), 3. Virtual machines (Select), 4. Properties (Configure properties), and 5. Replication settings (Configure replication settings). At the bottom is an 'Enable replication' button. The right window, titled 'Target', prompts the user to 'Select your target settings for recovery'. It contains several dropdown menus: 'Target' (set to 'Azure'), 'Subscription' (set to 'ASR Canary Test Subscription 3'), 'Post-failover deployment model' (set to 'Resource Manager'), 'Storage account' (set to 'contosodrppremium'), and 'Storage account for replication logs' (set to 'contosodrstd'). Below these are three more dropdowns: 'Azure network' (set to 'Configure now for selected machines.'), 'Post-failover Azure network' (set to 'InMageS2SVPNSEA'), and 'Subnet' (set to 'GateWaySubnet (10.0.1.0/24)'). An 'OK' button is at the bottom right.

9. In **Virtual Machines** > **Select virtual machines** click and select the machine you want to replicate – **CentOS VM** Then click **OK**.



10. In **Properties** > **Configure properties**, select the account that will be used by the process server to automatically install the Mobility service on the machine- **Linux**. By default, all disks are replicated. Click **All Disks** and clear any disks you don't want to replicate. Then click **OK**.

Enable replication

CommsDn - PREVIEW

1 Source

CONTOSO-CS

✓

2 Target

Azure

✓

3 Virtual machines

1 Selected

✓

4 Properties

Configure properties

>

5 Replication settings

Configure replication settings

>

Enable replication

Configure properties

PREVIEW

Exclude disk will be allowed only if mobility service is already installed. OS and dynamic disk cannot be excluded

NAME	ACCOUNT	DISKS TO REPLICATE
Defaults	Select	Need to select per VM. ...
SQLVM-1	windows	All Disks ...

OK

11. In **Replication settings** > **Configure replication settings** verify that the correct replication policy is selected *vmware-policy*

Enable replication

ContosoDR - PREVIEW

Configure replication settings

PREVIEW

1

Source

CONTOSO-CS

✓

2

Target

Azure

✓

3

Virtual machines

1 Selected

✓

4

Properties

Configured

✓

5

Replication settings

Configure replication settings

>

Replication policy

vmware-policy

i

Only policies with recovery point retention of upto 24 hours is supported for virtual machines replicating to premium storage. To learn more click here

App-consistent snapshot frequency in mins

60 minutes

RPO threshold in mins

15 minutes

Recovery point retention in hours

24 hours

Multi-VM consistency

Do you want to enable Multi-VM consistency by creating a new Replication group?

Yes

No

Enable replication

OK

12. Click **Enable Replication**. 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.

Enable replication

ContosoDR - PREVIEW

Source

ContosoDR - PREVIEW

Select your source environment

1 Source
CONTOSO-CS

2 Target
Configure

3 Virtual machines
Select

4 Properties
Configure properties

5 Replication settings
Configure replication settings

* Source ⓘ
CONTOSO-CS

* Machine type ⓘ
Virtual Machines

* vCenter server/vSphere host ⓘ
Contoso-vmware

* Process server ⓘ
contoso-cs (Inbuilt Process Server)

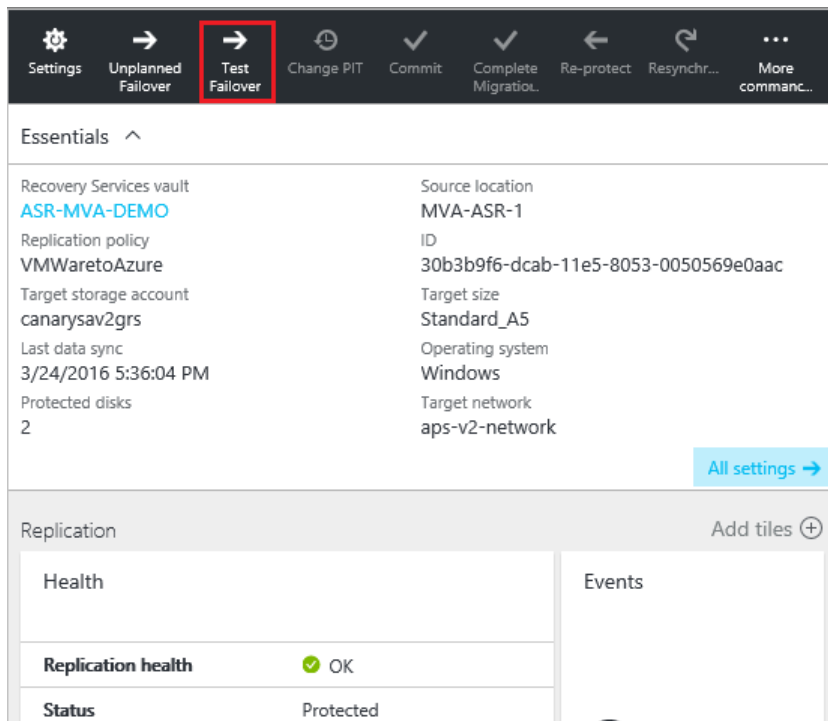
Enable replication

OK

Step 7: Test the deployment

In order to test the deployment, you can run a test failover for a single virtual machine or a recovery plan that contains one or more virtual machines.

To fail over a single machine, in **Settings** > **Replicated Items**, click the VM – **Centos-VM** > **+Test Failover** icon.



1. In **Test Failover** select the Azure network – **holnetwork**.
2. Click **OK** to begin the failover. You can track progress by clicking on the VM to open its properties, or on the **Test Failover** job in vault > **Settings** > **Jobs** > **Site Recovery jobs**.
3. When the failover reaches the **Complete testing** status, do the following:
 - a. View the replica virtual machine in the Azure portal. Verify that the virtual machine starts successfully.
 - b. Click **Complete test** to finish it.

