



10TH MAGNITUDE

Azure Site Recovery Migration Guide

VMware vSphere Environments

10th Magnitude, LLC
20 North Wacker Drive #530
Chicago, IL 60606

Notice of Confidentiality

© 2018 10th Magnitude, LLC All rights reserved

THIS DOCUMENT IS 10TH MAGNITUDE PROPRIETARY AND CONFIDENTIAL INFORMATION AND IS SUBJECT TO THE TERMS OF THE 10TH MAGNITUDE NON-DISCLOSURE AGREEMENT. NEITHER THIS DOCUMENT NOR ITS CONTENTS MAY BE REVEALED OR DISCLOSED TO UNAUTHORIZED PERSONS OR SENT OUTSIDE THE AFOREMENTIONED COMPANY WITHOUT PRIOR PERMISSION FROM 10TH MAGNITUDE.

TABLE OF CONTENTS

Summary	3
Azure Site Recovery (ASR) Deployment.....	3
Deployment Considerations	3
Example Deployment Topologies	4
Prepare On-Prem and Azure Environments for ASR.....	5
Deploy a Configuration Server.....	7
Discover and Enable Replication on Source Machines	9
Discovery and Replication of Physical Machines	9
Discovery and Replication of Virtual Machines	13
Configuring the Landing Zone of Protected Items.....	16
Create A Recovery Plan.....	17
Perform Failover Testing.....	19
Prerequisites	19
Failover Testing Steps	19
Failover.....	21
Prerequisites	21
Failover Steps.....	21
Post Failover.....	23
Recommended Post Failover Configuration	23
Post Failover Cleanup.....	23

SUMMARY

This is a general high-level step-by-step guide for performing a migration to Azure from a VMware specific on-prem environment. The guide will cover how to setup migration tooling, replication of source machines, how to perform failover testing, and completing a failover.

AZURE SITE RECOVERY (ASR) DEPLOYMENT

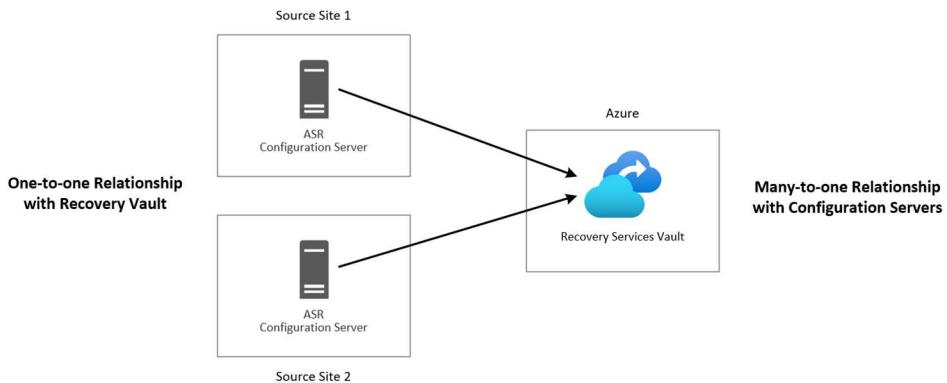
Before you start, it's a good idea to review 10th Magnitude's ASR Planning Guide and the Microsoft ASR Setup Guide to get a clear understanding of the architecture and what needs to be deployed to support the migration.

Useful reference links:

<https://docs.microsoft.com/en-us/azure/cloud-solution-provider/migration/on-premises-to-azure-csp/asr-capacity-planning>
<https://docs.microsoft.com/en-us/azure/cloud-solution-provider/migration/on-premises-to-azure-csp/asr-setup-guide>
https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vm_admin.doc/GUID-17BEDA21-43F6-41F4-8FB2-E01D275FE9B4.html

DEPLOYMENT CONSIDERATIONS

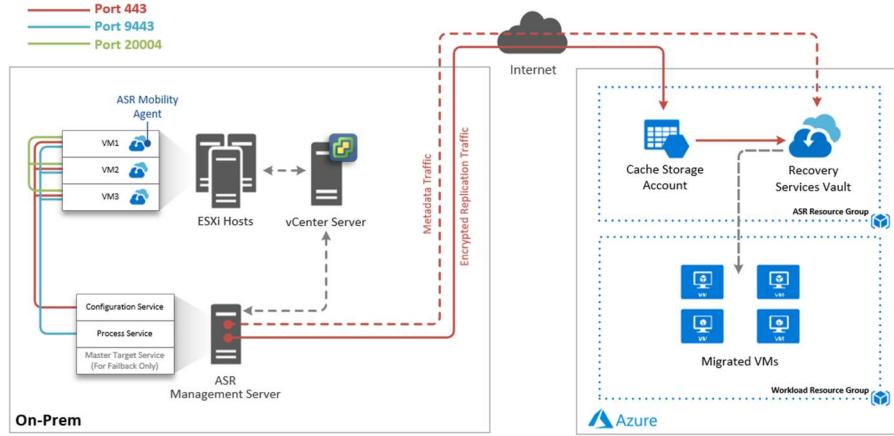
- Each ASR Configuration Server can only be registered to a single Azure Recovery Services vault (one-to-one relationship). A single Azure Recovery Vault can have multiple Configuration Servers registered to it (many-to-one relationship). When a Configuration Server is registered to a Recovery Services Vault, the vault cannot be changed.



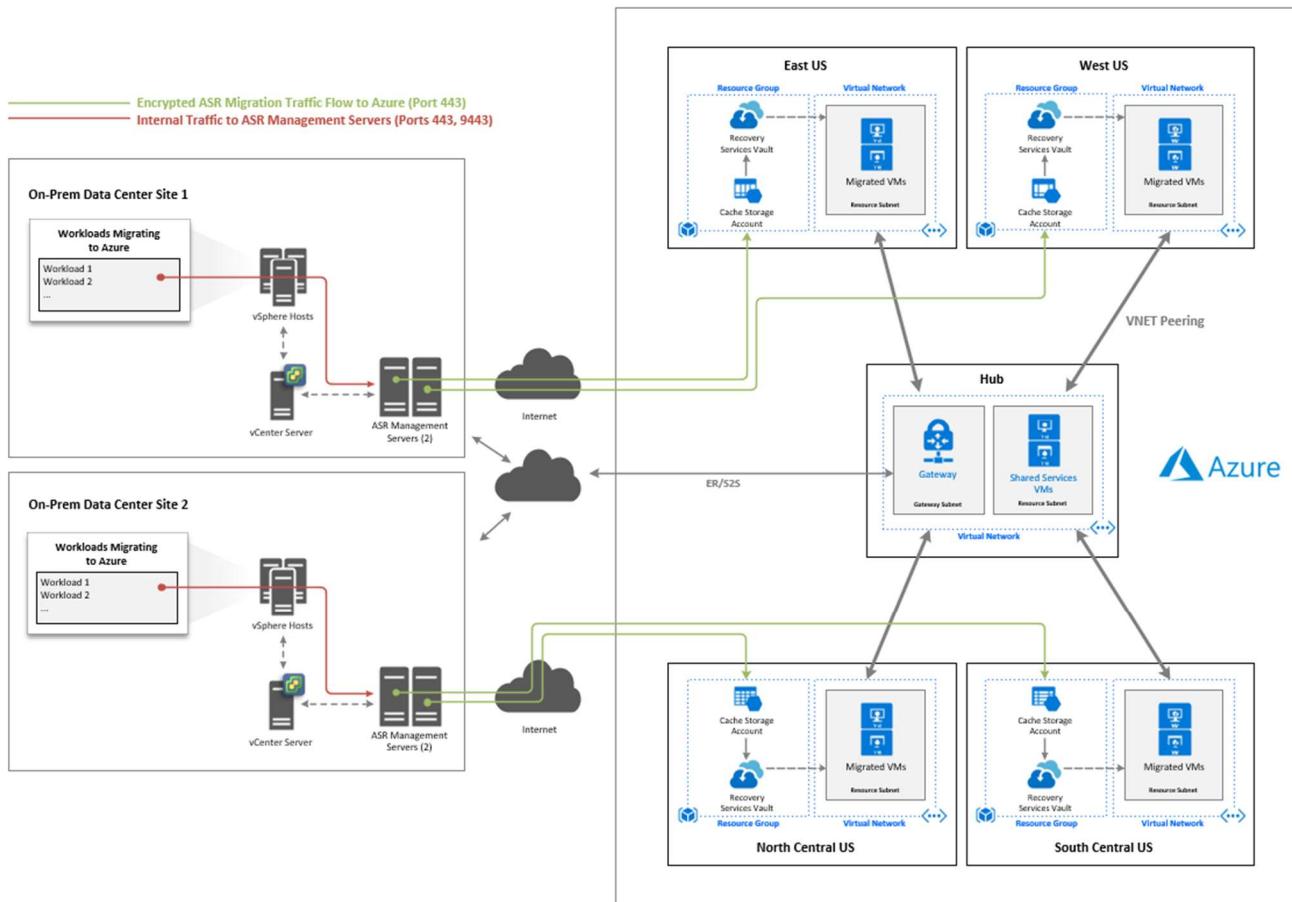
- If multiple geographically diverse source locations will be in scope, a Configuration Server should be deployed in each source location.
- If multiple target Azure regions will be in scope for migration, a Recovery Services Vault and cache Storage Account must be created in each target Azure region. A Configuration Server will need to be deployed and registered to each target region's Recovery Services Vault. You will need multiple Configuration Servers in a single source location to migrate to multiple Azure regions from the source. Please see the example diagrams in the next section.

EXAMPLE DEPLOYMENT TOPOLOGIES

Single Source, Single Azure Target Region



Multiple Source Locations, Multiple Azure Target Regions



1. Create an ASR service account in the on-prem environment to connect to vCenter or the ESXi host(s) for automatic discovery. Ideally this account should be an Active Directory account.
 - a. The ASR service account will need local administrator permissions on the source servers that will be migrated and will be used to push install the ASR Mobility Service agent.
 - b. The ASR service account will need read only access granted on the vCenter or ESXi host(s) to gather inventory and virtual machine metadata.
2. Create a Resource Group in each target subscription for the ASR components
3. Create a Storage Account to be used for caching and logging in each target subscription and region
 - a. From the Azure Portal, select Create a Resource and search for Storage Account, then click Create
 - i. Select the Resource Group created in the previous step
 - ii. Name the Storage Account
 - iii. Select the target Azure region as the location
 - iv. Select Standard performance
 - v. Select StorageV2 for kind
 - vi. Select LRS for replication
 - vii. Select Hot as the access tier
 - viii. Leave other options as default
 - ix. Click Review + create

Create storage account

[Basics](#) [Networking](#) [Advanced](#) [Tags](#) [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below.
[Learn more about Azure storage accounts](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	Visual Studio Enterprise – MPN
Resource group *	scus-vs-asrpoc-rg Create new

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name *	scusvsarcachestorage01
Location *	(US) South Central US
Performance	<input checked="" type="radio"/> Standard <input type="radio"/> Premium
Account kind	StorageV2 (general purpose v2)
Replication	Locally-redundant storage (LRS)
Access tier (default)	<input type="radio"/> Cool <input checked="" type="radio"/> Hot

4. Create a Recovery Services Vault in the target region(s)
 - a. From the Azure Portal, select Create a Resource and search for Backup and Site Recovery, then click create.
 - i. Name the Vault
 - ii. Select the Resource Group created in step 2
 - iii. Select the correct target region
 - iv. Click Review + create

Create Recovery Services vault

Preview

Basics * Tags Review + create

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription *	Visual Studio Enterprise – MPN
Resource group *	scus-vs-asrpoc-rg Create new

Instance Details

Vault name *	scus-vs-asr-rsv
Region *	(US) South Central US

5. You should now have a Recovery Services Vault and Storage Account provisioned in your ASR Resource Group. Repeat for any other target regions in scope.

Showing 1 to 2 of 2 records. Show hidden types

<input type="checkbox"/> Name ↑↓	Type ↑↓	Location ↑↓
<input type="checkbox"/> scus-vs-asr-rsv	Recovery Services vault	South Central US
<input type="checkbox"/> scusvsasrcachestorage01	Storage account	South Central US

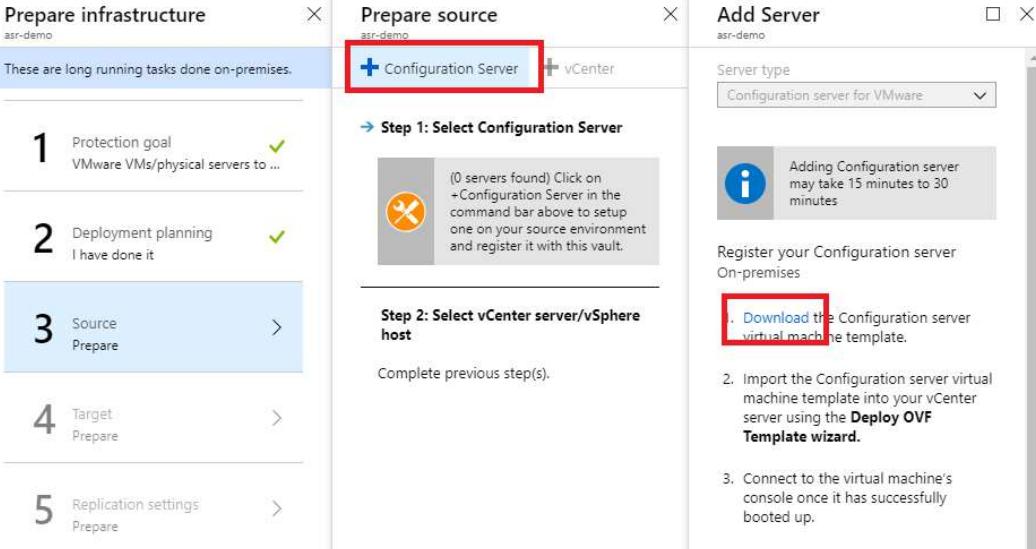
DEPLOY A CONFIGURATION SERVER

Use the following steps to deploy an ASR Configuration Server and register it to Azure Site Recovery.

1. Start the setup from Azure
 - a. In the Azure portal, open the target Recovery Service vault
 - b. In the Site Recovery section, click Getting Started

The screenshot shows the Azure portal interface for a Recovery Services vault named 'asr-demo'. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Properties, Locks, Export template, Getting started (Backup and Site Recovery), Protected items (Backup items and Replicated items), and Manage (Backup policies). The main content area has tabs for Overview, Backup, and Site Recovery, with Overview selected. Under 'What's new', there are several bullet points about enterprise-scale backup for SQL Server, protecting on-premises VMs, protection of Azure VMs using Storage Spaces Direct, disaster recovery for VMs in Availability Zones, and instant recovery of Azure VMs. Below this is a 'Backup' section with links for Getting started, Backup dashboard, Backup items, Backup policies, and Learn more. To its right is a 'Site Recovery' section with links for Getting started (which is highlighted with a red box), Site Recovery dashboard, Replicated items, Manage Recovery Plans, and Learn more.

- c. Click Prepare Infrastructure
- d. Protection Goal
 - i. Where are your machines located, select On-premises
 - ii. Where do you want to replicate your machines, select To Azure
 - iii. Are your machines virtualized, select Yes, with VMware vSphere Hypervisor
 - iv. Click OK.
- e. Deployment Planning
 - i. Select Yes, I have done it
 - ii. Click OK.

- f. Source
- Click + Configuration Server
 - Download to download the OVF template. Since this is a large file (20GB+), you should download directly into the source environment if possible.
- 
2. Deploy the OVF template into the VMware environment.
- Log into vCenter server
 - Right-click any inventory object that is a valid parent object of a virtual machine, such as a data center, folder, cluster, resource pool, or host, and select Deploy OVF Template. The Deploy OVF Template wizard opens.
 - On the Select an OVF template page, specify the location of the source OVF or OVA template and click Next.
 - On the Select a name and folder page, enter a unique name for the virtual machine or vAPP, select a deployment location, and click Next.
 - On the Select a compute resource page, select a resource where to run the deployed VM template, and click Next.
 - On the Review details page, verify the OVF or OVA template details and click Next.
 - On the Select storage page, define where and how to store the files for the deployed OVF or OVA template. Make sure to select a datastore large enough to accommodate the virtual machine or vApp and all associated virtual disk files.
 - Select the disk format for the virtual machine virtual disks. Use the default values from the template here.
 - Select a VM Storage Policy. This option is available only if storage policies are enabled on the destination resource.
 - (Optional) Enable the Show datastores from Storage DRS clusters check box to choose individual datastores from Storage DRS clusters for the initial placement of the virtual machine. Select a datastore to store the deployed OVF or OVA template.
 - On the Select networks page, select a source network and map it to a destination network. Click Next.
 - On the Ready to complete page, review the page and click Finish.
3. After the template is deployed, boot the VM and connect to the VMs console to complete the Windows Server installation.
4. Finish setting up the server to desired specifications – join to the domain, run Windows Update, etc. It is important to keep this server up-to-date or the services may stop.

5. Launch the ASR Configuration Manager wizard from the link on the desktop. Run through the wizard and fill in the required information to register the server with the Recovery Services Vault. It can take 15-30 minutes for the Configuration Server to show up in the vault.
6. Go back to the Recovery Services Vault unified setup in Step 1 and go through the wizard again. On Source step, verify you see the configuration server listed and select it, then select whether you are connecting to vCenter or vSphere hosts. If your Configuration Server isn't listed, go back to the Recovery Vault landing page, click Site Recovery Infrastructure, Configuration Servers, click the ellipsis (...), and then select Refresh Server.
7. On the Target step, select the correct subscription, use Resource Manager, and select the virtual networks.
8. On the Replication Settings step, create a replication policy and click OK, then click OK again.

DISCOVER AND ENABLE REPLICATION ON SOURCE MACHINES

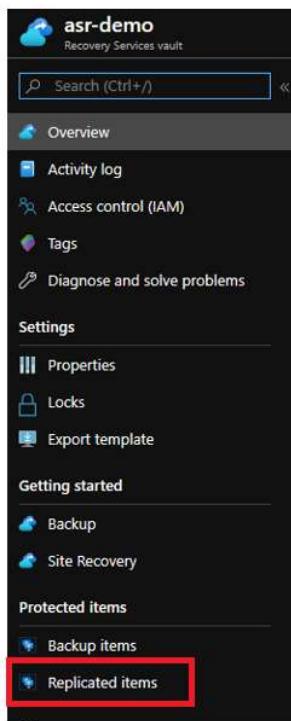
Once you have configured your Recovery Services Vault, you will be able to discover machines in your on-premises environment and enable replication to Azure. Depending on whether the source machines are physical or virtualized, use the appropriate following steps. If you have a combination of physical and virtualized machines, use the appropriate steps for the type of machine to be replicated.

Useful Reference Links:

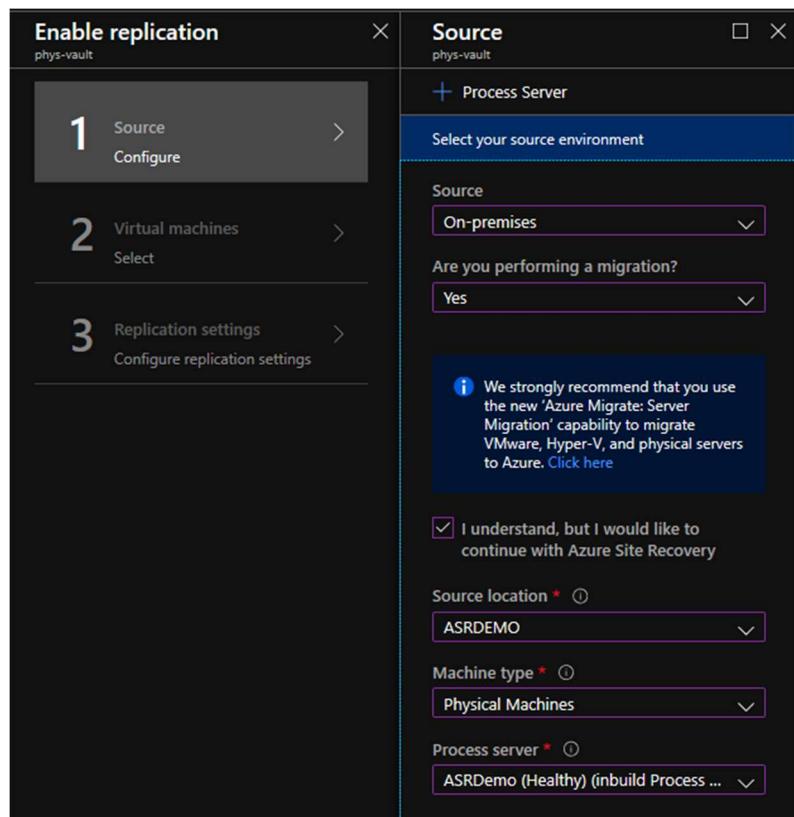
<https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-enable-replication>

DISCOVERY AND REPLICATION OF PHYSICAL MACHINES

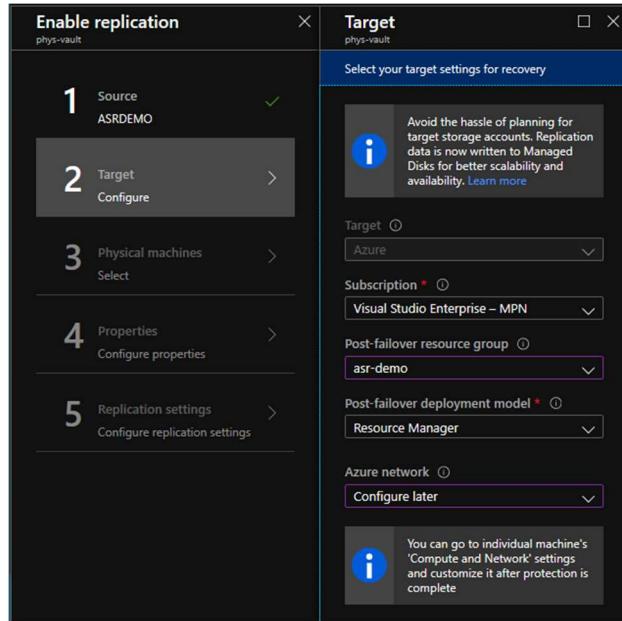
1. In the Azure Portal, navigate to the Recovery Services Vault you created in the previous section.
2. Select *Replicated Items* under the *Protected Items* section to view all protected items in the vault.



3. On the top page, select +Replicate
4. In the *Enable replication* blade:
 - a. Configure the *Source*
 - i. Are you performing a migration? – Yes
 - ii. Check the box – I understand, but I would like to continue with Azure Site Recovery
 - iii. Select the *Source location* – the source location is the Configuration Server name that you designated
 - iv. Select *Machine Type* – in this case we will be discovering a physical machine
 - v. Select *Process Server* – This will be the same as your Configuration Server, unless a scale-out process server has been added



- b. Configure Target
 - i. Target will be preselected as *Azure*
 - ii. Select the *Subscription* where you want to create the virtual machine during failover
 - iii. Select the *Resource Group* where you want to create the virtual machine during failover
 - iv. Select the *Deployment Model* – it is recommended you select *Resource Manager*
 - v. You have the option to configure the *Azure Network* in this step, or, in a later step



c. Select Physical Machines

- i. Click +Physical Machine
- ii. In the *Add physical machines* blade, enter the *Name*, *IP Address* and *OS Type* of the machine you are going to discover – you can add multiple machines at one time
- iii. Select *OK* to begin the discovery job

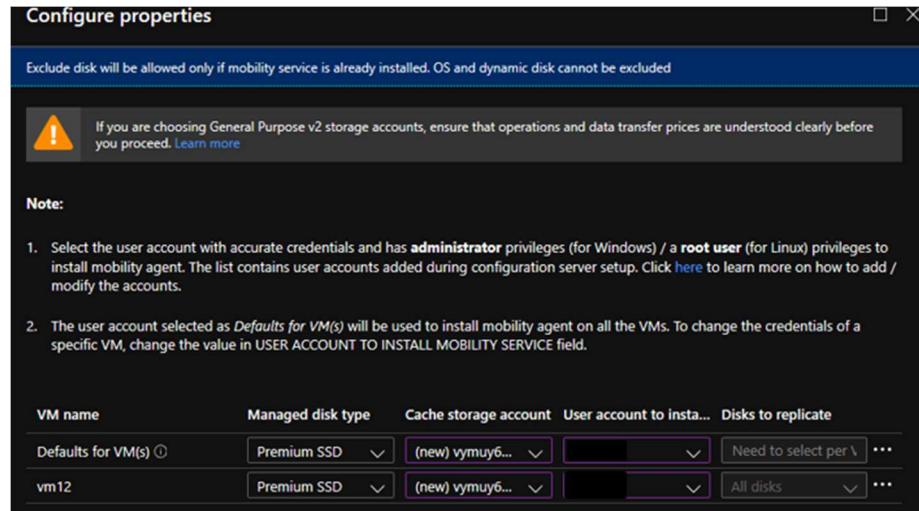
Add physical machines		
Name	IP address	OS type
vm12	172.18.55.150	Windows
<input type="text" value="Enter name"/>	<input type="text" value="Enter IP address"/>	Select

- iv. Once the discovery job has finished, you will be able to see the discovered machine in the previous *Select physical machines* blade.

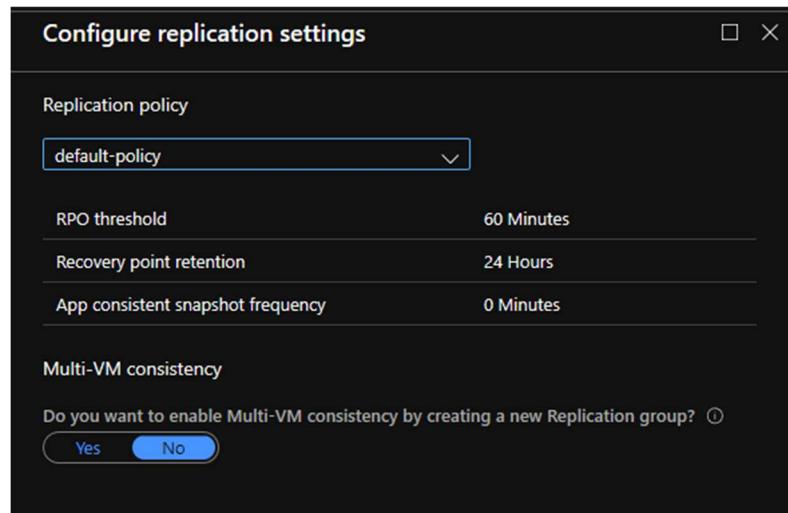
Select physical machines		
+ Physical machine		
Finished loading data from service		
Name	IP address	OS type
<input checked="" type="checkbox"/> vm12	172.18.55.150	WINDOW
<		>

- v. Select the newly discovered machine and click *OK*

- d. Configure the Properties of each discovered machine
 - i. Select the *Managed Disk Type* desired performance
 - ii. Select the *Cache Storage Account* that your replica disks will be written to – select the storage account that was created during the preparation setup section.
 - iii. Select the user account that was created preparation setup section to push install the Mobility Agent



- e. Configure replication settings
 - i. Select the *Replication Policy* you created in the previous section

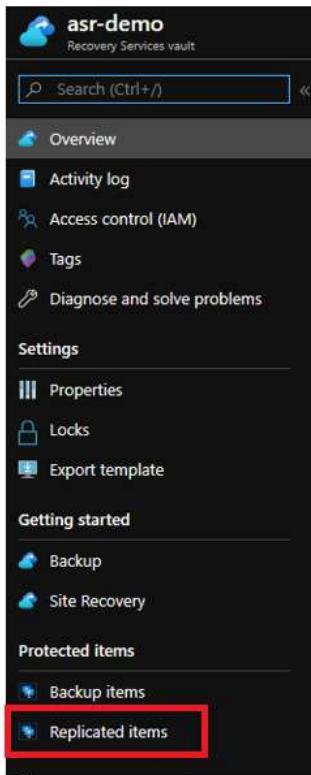


- f. Once these selections have been made, click *Enable Replication* and the job will begin

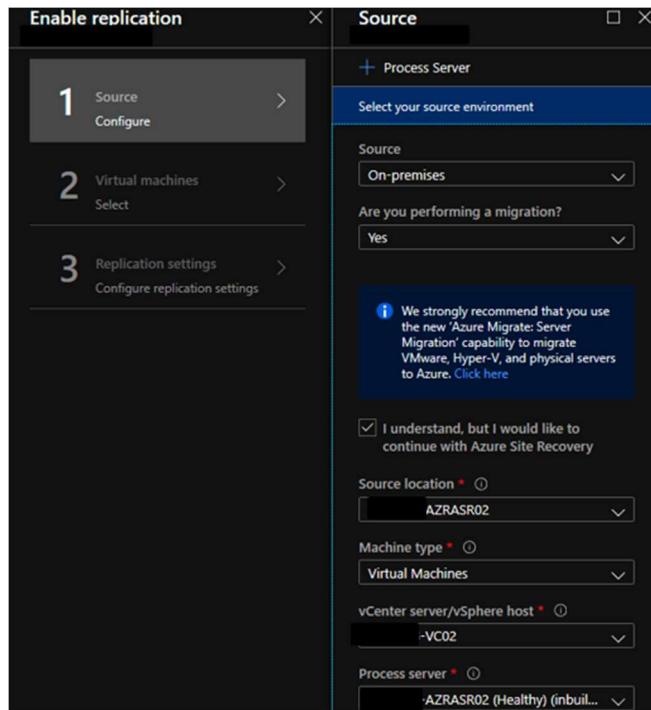
Note: Initial synchronization time depends on size of the source machine, network bandwidth, and churn rate on the on-premises machine.

DISCOVERY AND REPLICATION OF VIRTUAL MACHINES

1. In the Azure Portal, navigate to the Recovery Services Vault you created in the previous section.
2. Select *Replicated Items* under the *Protected Items* section to view all protected items in the vault.

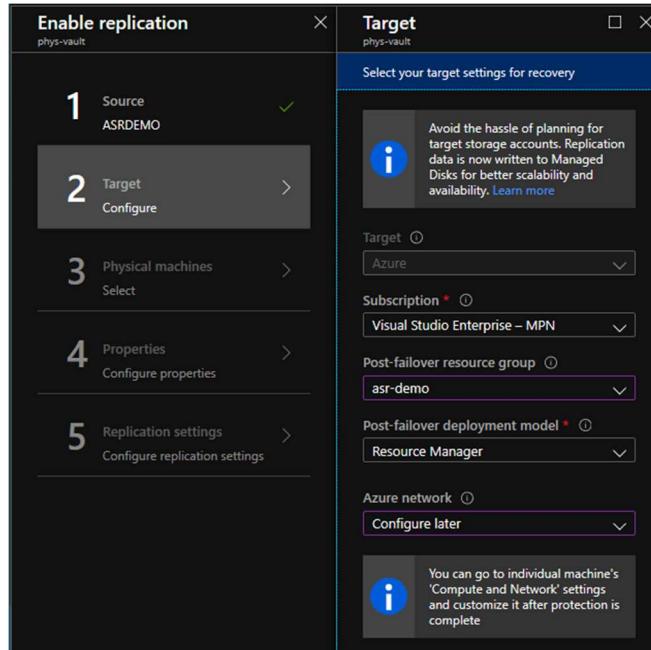


3. On the top page, select *+Replicate*
4. In the *Enable Replication* blade
 - a. Configure the Source
 - i. The source location will be *On-Premises*
 - ii. *Are you performing a migration? – Yes*
 - iii. Check the box – *I understand, but I would like to continue with Azure Site Recovery*
 - iv. Select the *Source location* – the source location is the Configuration Server name that you designated
 - v. Select *Machine Type* – in this case we will be discovering a virtual machine
 - vi. *vCenter server/vSphere Host* – select the VMWare environment where you registered your configuration server
 - vii. Select *Process Server* – This will be the same as your Configuration Server, unless a scale-out process server has been added



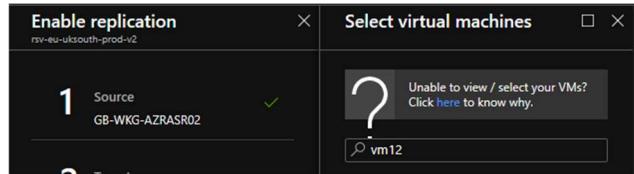
b. Configure Target

- i. Target will be preselected as *Azure*
- ii. Select the *Subscription* where you want to create the virtual machine during failover
- iii. Select the *Resource Group* where you want to create the virtual machine during failover
- iv. Select the *Deployment Model* – it is recommended you select *Resource Manager*
- v. You have the option to configure the *Azure Network* in this step, or, in a later step



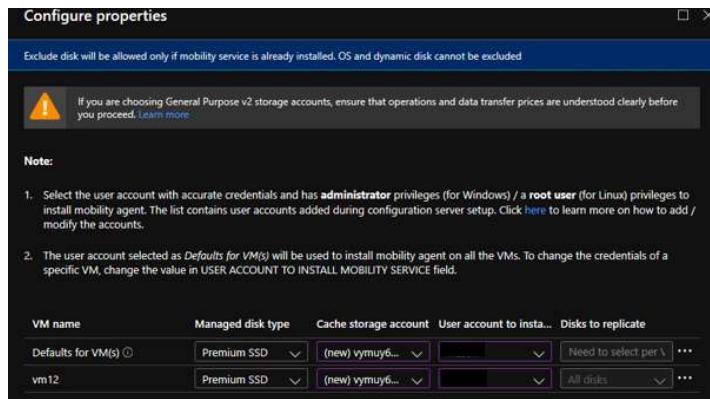
c. Select *Virtual Machines*

- i. The virtual machines that are in your VMWare environment will be automatically discovered.
Select the machines you would like to protect with this Recovery Services Vault
- ii. You can provide a name in the *Filter Items* box to search for virtual machines
- iii. Up to 10 machines can be selected to begin replication at one time.



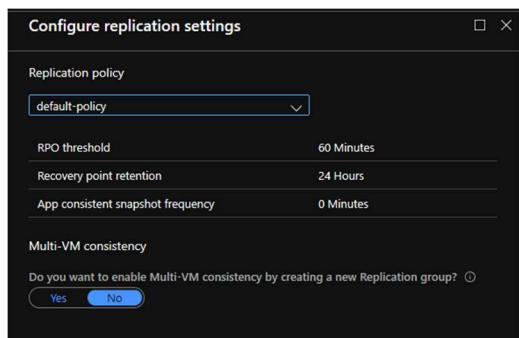
d. Configure the Properties of each discovered machine

- i. Select the *Managed Disk Type*
- ii. Select the *Cache Storage Account* that your replica disks will be written to – select the storage account created in the preparation section.
- iii. Select the user account created in the preparation section to push install the Mobility Agent



e. Configure replication settings

- i. Select the *Replication Policy* you created in the previous section



- f. Once these selections have been made, click *Enable Replication* and the job will begin

Note: Initial synchronization time depends on size of the source machine, network bandwidth, and churn rate on the on-premises machine.

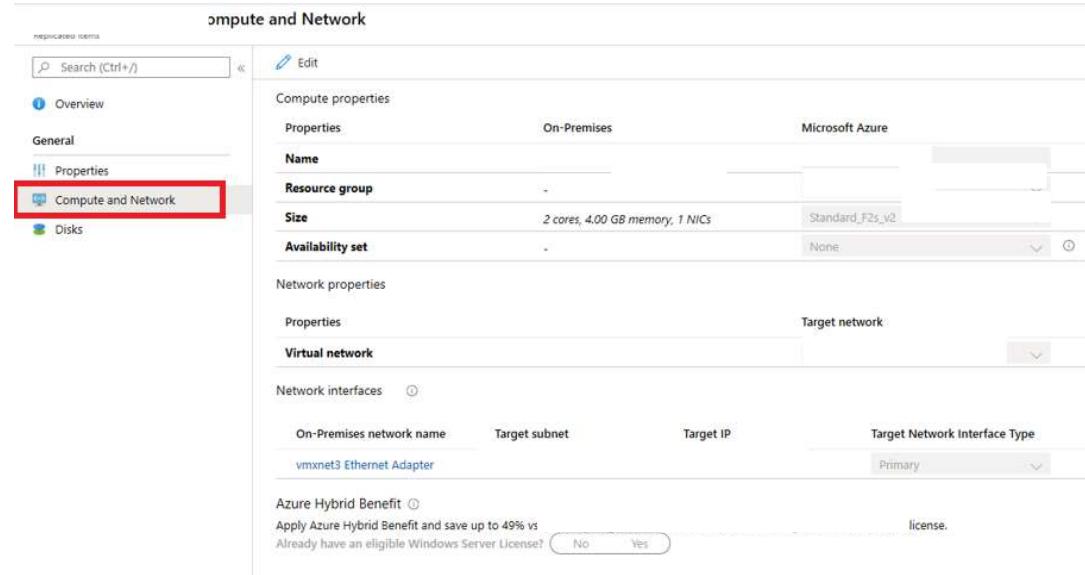
CONFIGURING THE LANDING ZONE OF PROTECTED ITEMS

- Once items have synchronized, click the protected item you want to configure under *Replicated Items*

- Select the *Compute and Network* tab to view and change VM properties such as:

- Target Name
- Target Resource Group
- Target Size
- Availability Sets
- Configure Managed disks (Use of managed disks is recommended)
- Target Network, Subnet and [Static or Dynamic] IP Address
- Hybrid Use Benefit

Note: You will only be able to select resources in the subscription that you chose as your target when enabling replication. You will only be able to select Availability Sets that have been created previously in the target Resource Group.



- Click *Save* to keep any changes you have made.

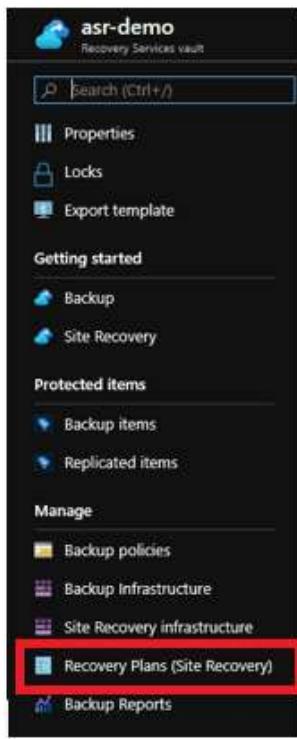
CREATE A RECOVERY PLAN

If failing over multiple VMs or there is a need to orchestrate boot order or add scripts, you should create a Recovery Plan. Recovery Plans enable you to group together protected items in your Recovery Services Vault. You can leverage a recovery plan to conduct failover testing, failover, boot machines in a specific sequence, or add automation runbooks to script actions during failover.

Useful Reference Links:

<https://docs.microsoft.com/en-us/azure/site-recovery/recovery-plan-overview>

1. Navigate to your Recovery Services Vault and select *Recovery Plans (Site Recovery)* in the left pane under *Manage*



2. On top of the page, select *+Recovery Plan* – it is required to have at least one protected item in your recovery services vault to create a recovery plan.
3. In the *Create recovery plan* blade
 - a. Give the recovery plan a *Name* that briefly describes the workload or group of servers that will be failed over
 - b. Select *Source* – this will be the configuration server you registered to the Recovery Services Vault
 - c. Select *Target* – Microsoft Azure will be your target
 - d. *Allow items with deployment model* – Select *Resource Manager*
 - e. Click *select items* – you will be able to select items currently protected by the configuration server (*Source*) that you registered with recovery services vault.

Create recovery plan

Up to 100 protected instances can be added to recovery plan. [Learn more.](#)

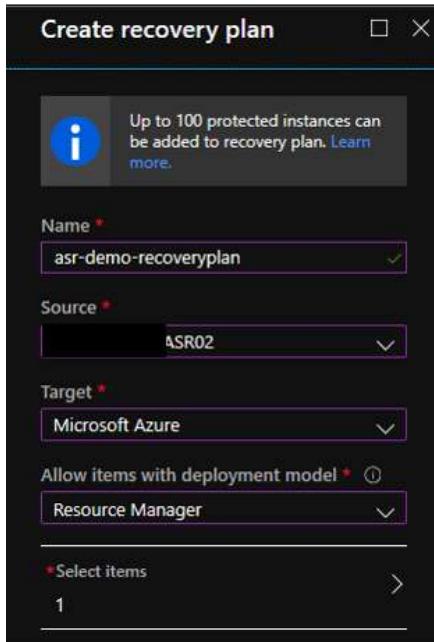
Name * asr-demo-recoveryplan

Source * ASR02

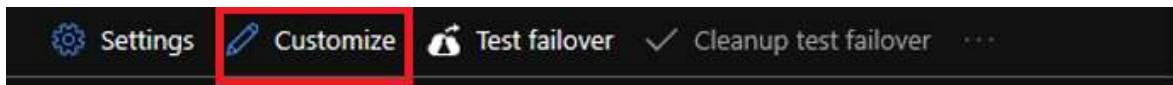
Target * Microsoft Azure

Allow items with deployment model * Resource Manager

*Select items > 1

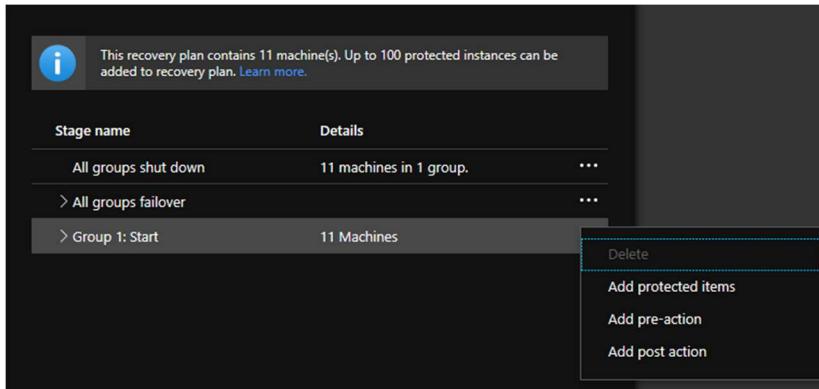


- f. When the job finishes you will be able to select the recovery plan and click *Customize* to add or remove machines; add pre or post actions such as automation runbooks or manual actions; add groups to recovery plan. Up to 100 protected items can be added to a single recovery plan.



This recovery plan contains 11 machine(s). Up to 100 protected instances can be added to recovery plan. [Learn more.](#)

Stage name	Details	...
All groups shut down	11 machines in 1 group.	...
> All groups failover		...
> Group 1: Start	11 Machines	<ul style="list-style-type: none">DeleteAdd protected itemsAdd pre-actionAdd post action



PERFORM FAILOVER TESTING

Failover testing is recommended before attempting a failover to ensure that the machine(s) will boot and function properly in Azure. This testing will help uncover any issues that may require troubleshooting and provide the ability to actively troubleshoot and document resolution without affecting the production environment.

Useful Reference Links:

<https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-test-failover-to-azure>

PREREQUISITES

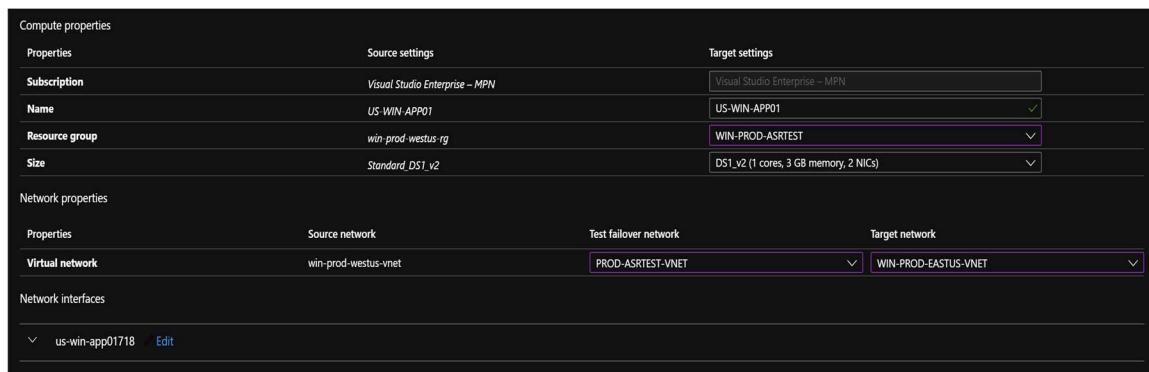
- A VNET or subnet that is isolated from the production network and designated for failover testing. During a failover test, ASR will create and power on the replicated VMs, but will not shut down the on-premises machines. The Azure VMs must be isolated during testing to avoid unintended communication to production resources, Active Directory or DNS conflicts, etc.
- Preferably a jump box with connectivity to the isolated test network to test and troubleshoot machines during failover testing.
- Virtual machines must be fully synchronized with the Azure Site Recovery vault to perform a failover test.

FAILOVER TESTING STEPS

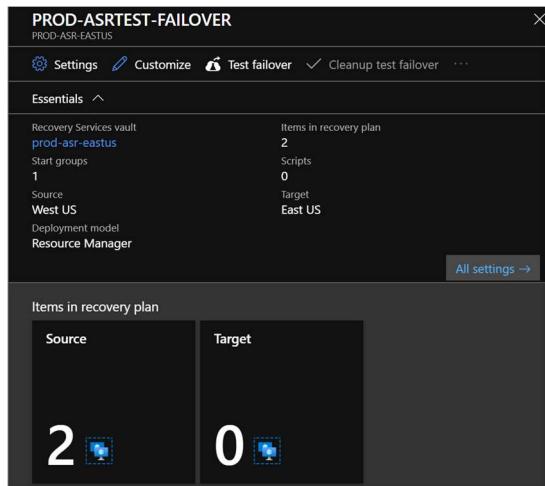
1. Determine that the VM(s) is in an appropriate failover state. In this example healthy, if the VM(s) have a warning or critical note under replication health ensure the error will not cause a failure in the failover.

Name	Replication Health	Status
US-WIN-APP01	Healthy	Protected
US-WIN-APP02	Healthy	Protected

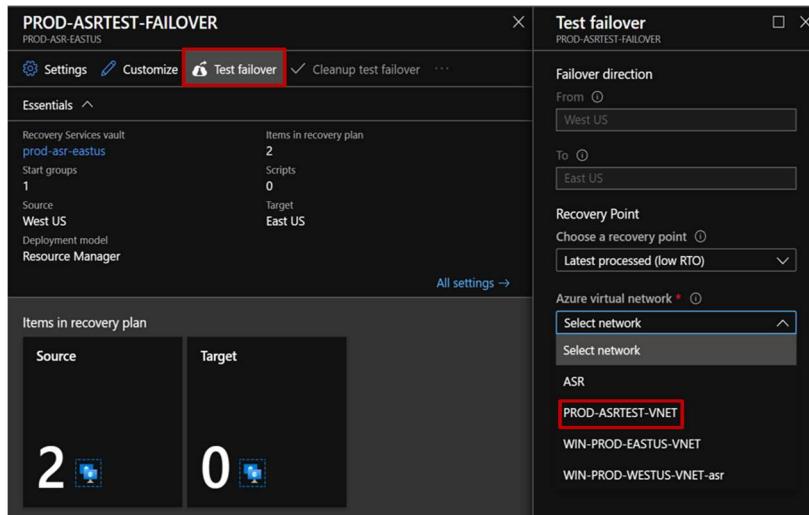
2. Adjust the machine to Failover into the appropriate resources. It is highly recommended that you use a non-production isolated testing network to perform failover testing.



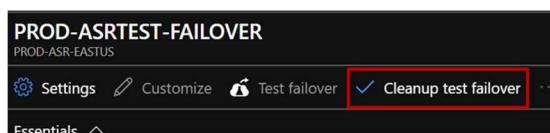
- If failing over multiple VMs, it is recommended to create a failover plan. Failover plans will simplify the failover process and allow grouping and automation scripts in the failover process to perform post failover configurations that may be required. Detailed steps of how to create a failover plan can be found in a previous section.



- Perform a Failover Test by opening the Recovery Services Vault, selecting replicated items (or failover plans) and selecting Test Failover. Ensure the isolated testing network is selected for the Azure virtual network.



- Once failover testing is completed, cleaning up the test environment is accomplished by navigating back to the VM in the Azure Site Recovery vault or navigating to the recovery plan and selecting Clean up test failover. This will delete all testing resources created during the test failover.



FAILOVER

Perform live failover after a successful test failover is performed and successful troubleshooting determined the VM(s) will work in Azure. A live failover is recommended to migrate the machines to Azure. It is recommended that all stakeholders and any personnel required to have a successful failover such as, networking team, security team and/or the application owner(s) are available to perform necessary tasks.

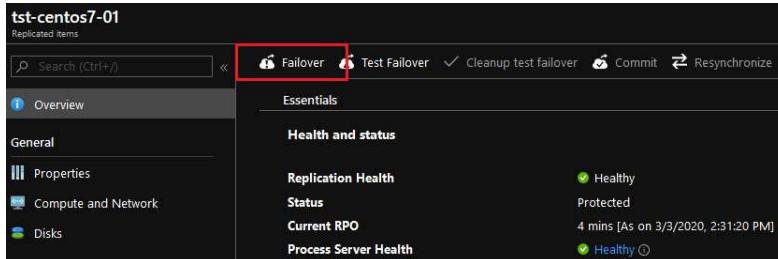
PREREQUISITES

- A successful failover test has been completed. This is not required to initiate a failover, but is highly recommended.
- The replicated items are fully synchronized with an acceptable RPO.
- The failover has been communicated to all affected parties and an appropriate downtime window has been established.
- A clear failover plan with all steps from all parties involved has been created and reviewed.
- Create Recovery Plans if failing over multiple VMs or there is a need to orchestrate boot order or add scripts.

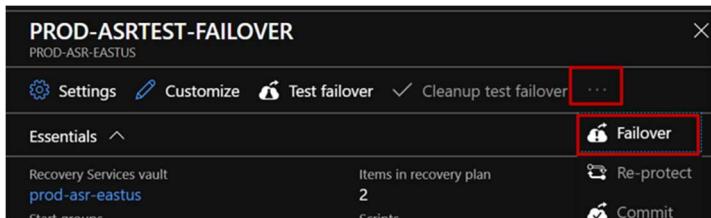
FAILOVER STEPS

1. Ensure all necessary personnel are available to field required failover tasks and to provide troubleshooting as required.
2. Navigate to the Azure Site Recovery vault in which the failover will be initiated. Select the replicated item, or navigate to the Recovery Plans.
3. Initiate the failover by selecting Failover. If using a recovery plan, select the ellipses then Failover.

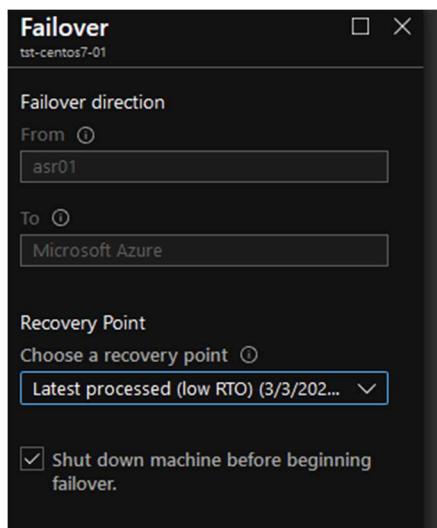
Failing over single machines:



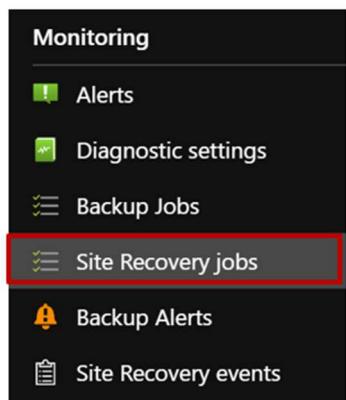
Failing over with a Recovery Plan:



- Select the latest processed recovery point.



- You can monitor the failover job by navigating back to the Recovery Services Vault and selecting Site Recovery Jobs.



- Select the migration job to monitor detailed progress.

Job	Name	Status	Start time	Duration
	Prerequisites check for the recovery plan	Successful	3/1/2020, 6:52:07 PM	00:00:13
	All groups shutdown (1)	Successful	3/1/2020, 6:52:21 PM	00:02:09
	Shutdown: Group 1 (2)	Successful	3/1/2020, 6:52:21 PM	00:02:09
	Recovery plan failover	In progress	3/1/2020, 6:52:21 PM	00:00:00
	us-win-app01	In progress	3/1/2020, 6:54:30 PM	00:00:00
	us-win-app02	In progress	3/1/2020, 6:54:30 PM	00:00:00
	Group 1: Start (2)			
	us-win-app01			00:00:00
	us-win-app02			00:00:00
	Finalizing the recovery plan			

POST FAILOVER

Following a failover, steps should be taken to configure operations on the migrated VMs to ready them for production. When the VMs have been tested and the migration has been declared a success, the replicated items need to be cleaned up so they are removed from the Recovery Services Vault.

RECOMMENDED POST FAILOVER CONFIGURATION

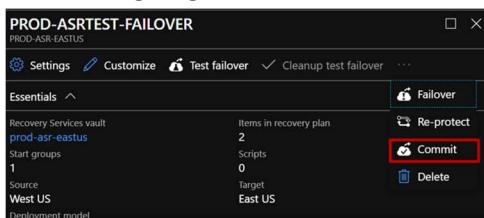
- Connect the VMs to a Log Analytics Workspace
- Enable backups
- Verify boot diagnostics are configured and using a shared storage account
- Enable extended diagnostics if desired
- Add to a patching schedule
- Verify monitoring, change tracking, enable EMS, or any other desired platform features
- Optimize the OS for Azure – move pagefile to Azure temp disk, reconfigure boot settings, etc. Guidance can be found here - <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image>

Note: The Azure VM agent is not supported on 32-bit operating systems. Certain platform features such as backups, VM extensions, run command, and any other features requiring the Azure VM agent will not be available.

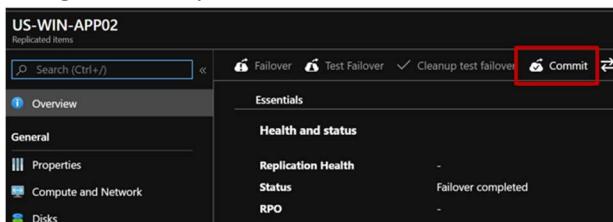
POST FAILOVER CLEANUP

1. Once the migration is successfully finished post migration cleanup can be performed. This includes committing the VM(s) recovery point to complete the migration. Navigate to the VM in the Azure Site Recovery vault or the failover plan. Then select commit.

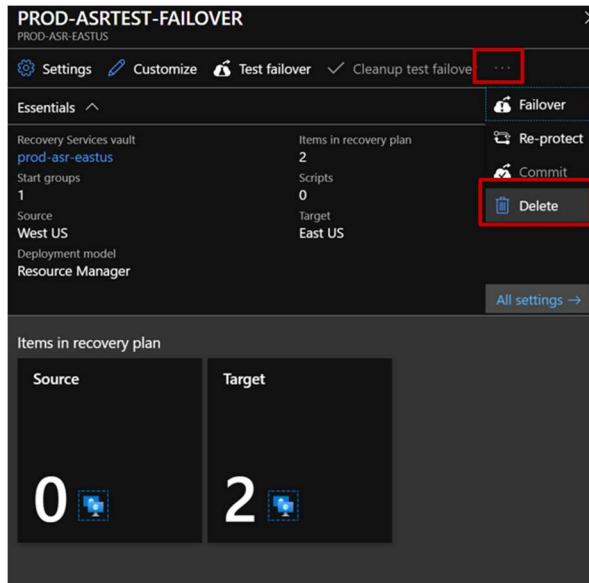
Committing single machines:



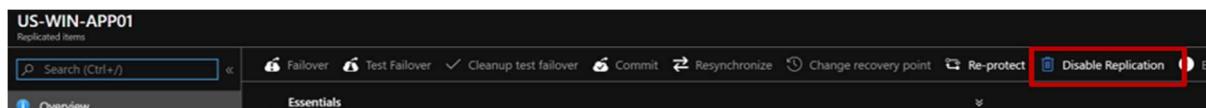
Using a failover plan:



- If using a recovery plan, you can then remove the recovery plan. Navigate to the recovery plan, select the ellipses then select Delete.



- You can now remove the replicated items from the vault. Navigate to the Recovery Services Vault, click Replicated items, select the replicated server item you'd like to remove, then select Disable Replication.



- Select disable replication and remove.



- We recommended that following a migration, whether successful or not, that a meeting is facilitated between all teams involved to discuss successes and misses during the migration. This will allow for continual improvements in the migrations process and execution, as well as help document known or newly discovered issues and prevent future problems.