The private preview is now available in all regions where Azure Site Recovery is currently available (except government clouds). Please refer to [Azure product availability by region](https://azure.microsoft.com/en-in/regions/services/) for more details about region availability.

Replicate Azure virtual machines to Azure using Azure Site Recovery (ASR) with the Azure portal

**Private Preview**

SCENARIO GUIDE

JANUARY 2017

|  |  |
| --- | --- |
| **X** | **Do not use “Azure to Azure DR scenario” on any production servers or data during this private preview!**  As a service in private preview, ASR does not yet offer an SLA and there is a possibility of data corruption, data loss and service interruptions as we continue to develop this service, with your feedback. To maximize the value of the feedback you provide, please use a copy of production servers and attempt to simulate your actual use cases in a lab environment, but do not use ASR on any production servers or live production data during this private preview. |

CONTENTS

[INTRODUCTION 3](#_Toc473406905)

[RELEASE NOTES 3](#_Toc473406906)

[GETTING STARTED 6](#_Toc473406907)

[Create a Recovery Services vault 6](#_Toc473406908)

[Prerequisites 7](#_Toc473406909)

[PRIVATE PREVIEW SCENARIOS 8](#_Toc473406910)

[Scenario 1 – Enable replication 8](#_Toc473406911)

[Scenario 2 – Test Failover 15](#_Toc473406912)

[Scenario 3 – Failover 18](#_Toc473406913)

[Scenario 4 – Re-protect after failover 22](#_Toc473406914)

[Scenario 5 – Failback 23](#_Toc473406915)

[Scenario 6 – Re-protect after failback 24](#_Toc473406916)

[MONITORING SITE RECOVERY OPERATIONS 24](#_Toc473406917)

[DISABLING REPLICATION 27](#_Toc473406918)

[DELETING RECOVERY SERVICES VAULT 28](#_Toc473406919)

|  |  |  |
| --- | --- | --- |
| **X** | **Do not use “Azure to Azure DR scenario” on any production servers or data during this private preview!**  As a service in private preview, ASR does not yet offer an SLA for “Azure to Azure DR scenario” and there is a possibility of data corruption, data loss and service interruptions as we continue to develop this service, with your feedback. To maximize the value of the feedback you provide, please use a copy of production servers and attempt to simulate your actual use cases in a lab environment, but do not use ASR on any production servers or live production data during this private preview. |  |

# INTRODUCTION

Intro

This is the private preview release of “DR for Azure Virtual Machines” scenario using Azure Site Recovery (ASR). In subsequent releases, we may ask you to start from scratch. There is no migration or upgrade supported between private preview releases and public preview.

You should be creating a new “Recovery services” vault for trying the private preview scenarios. And, delete the vault once you are done. **Post 31 days of its creation, the vault used for Azure VMs can be automatically deleted** by ASR at any time without any notice. Do not use this vault for any other ASR scenarios (VMware/Physical to Azure, Hyper-V to Azure or VMM to VMM scenarios). Also, do not use an existing vault which is being used for other ASR scenarios.

ASR will not charge for protecting any VM for the first 31 days. Make sure you disable replication for the VMs within 31 days. Otherwise, you can incur billing charges and the same will not be reversed. Note that any Compute, Network and Storage charges incurred for the test environment are billed to your subscription and ASR does not control it.

This document will provide you the step by step guidance to try the DR solution for Azure VMs using Azure Site Recovery.

# RELEASE NOTES

Intro

The following are the supported configurations for the current private preview release.

1. Support only for the below Windows OS versions for private preview.
   * Windows server 2012 R2
   * Windows server 2012
   * Windows server 2008 R2 SP1
2. Support only for the below Linux OS versions for private preview. We will add support for more Linux versions in the next updates.
   * Linux RHEL 6.7
   * Linux RHEL 7.2 with 3.10.0-327.el7.x86\_64 kernel version
   * Linux Cent OS 6.6
   * Oracle Linux 6.4
3. You can use up to **8 data disks** on your VMs. Do not use any more than that as it is not a tested and certified scenario. For public preview, we will support as many disks as Azure supports.
4. You can use **Classic or Resource Manager** VMs.
5. You can use **Premium or Standard storage** for your disks. You can also use OS disk on Standard Storage and data disk on Premium storage (combined storage scenario)
   * Note that you can use only ONE Target storage account per VM. So, even if it is a combined storage account scenario on source, it will end up in one storage account in Target. This is the limitation for the current private preview.
6. No [Recovery plan](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-create-recovery-plans) support for Azure VMs in private preview. For public preview, recovery plan support will be available.
7. No Multi-VM Replication group support for Azure VMs.
8. No [Storage spaces](https://technet.microsoft.com/library/hh831739.aspx) support. For public preview, storage spaces support will be available.
9. If you have Azure VM extensions configured in a specific way on the source VM, you need to reconfigure them post “Test Failover” or “Failover”. If you reconfigured the Azure VM extensions post failover, you need to reconfigure them in a similar way post “Failback (failover in reverse direction)”.
10. ASR will not charge for protecting any VM for the 1st 31 days. Make sure you disable replication for the VMs within 31 days. Otherwise, you can incur billing charges. Note that any Compute, Network and Storage charges incurred for the test environment are billed to your subscription and ASR does not control it.
11. You should be creating a new “Recovery services” vault for trying the private preview scenarios. Do not use this vault for any other ASR scenarios (VMware/Physical to Azure, Hyper-V to Azure or VMM to VMM scenarios). And, delete the vault once you are done. **Post 31 days of its creation, the vault used for Azure VMs can be automatically deleted** by ASR at any time without any notice.
12. Always use ONLY <http://aka.ms/asr-a2a-private-preview-portal> to access the Azure portal while trying private preview scenarios.

The following are the list of known issues for the current private preview release.

1. If you are using Premium storage disks, do not use “Latest point” option during “Test Failover” or “Failover”. Use only “Latest processed point” option or one of the custom recovery points. There is a known issue and will be fixed in the next update.
2. “Enable replication” can occasionally fail first time due to a known issue with root certificates on the VMs. You need to “Retry” the job and it should succeed. The issue will be fixed in the next update.

* For a VM running Windows OS, ensure the trusted root certificates are present on the machine following the guidance in the below article.

<https://technet.microsoft.com/en-in/library/dn265983.aspx>

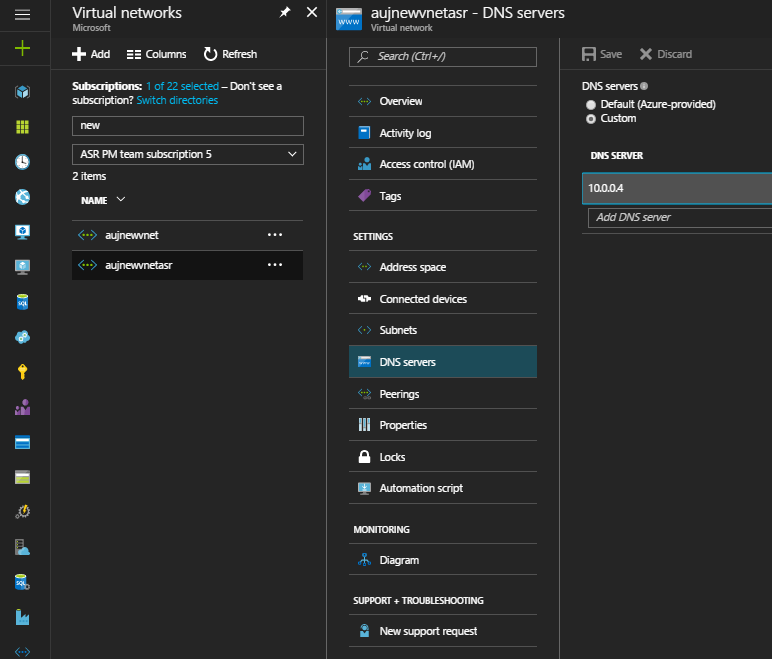
* For a VM running Linux OS, follow the guidance for trusted root certificates published by the Linux OS version distributor.

1. You cannot delete the “Recovery services vault” used for private preview from Azure portal. There is a known issue and will be fixed in the next update. As a workaround, you can either delete the entire “Resource group” or use the below PowerShell cmdlet to delete the vault. The issue will be fixed in the next update.

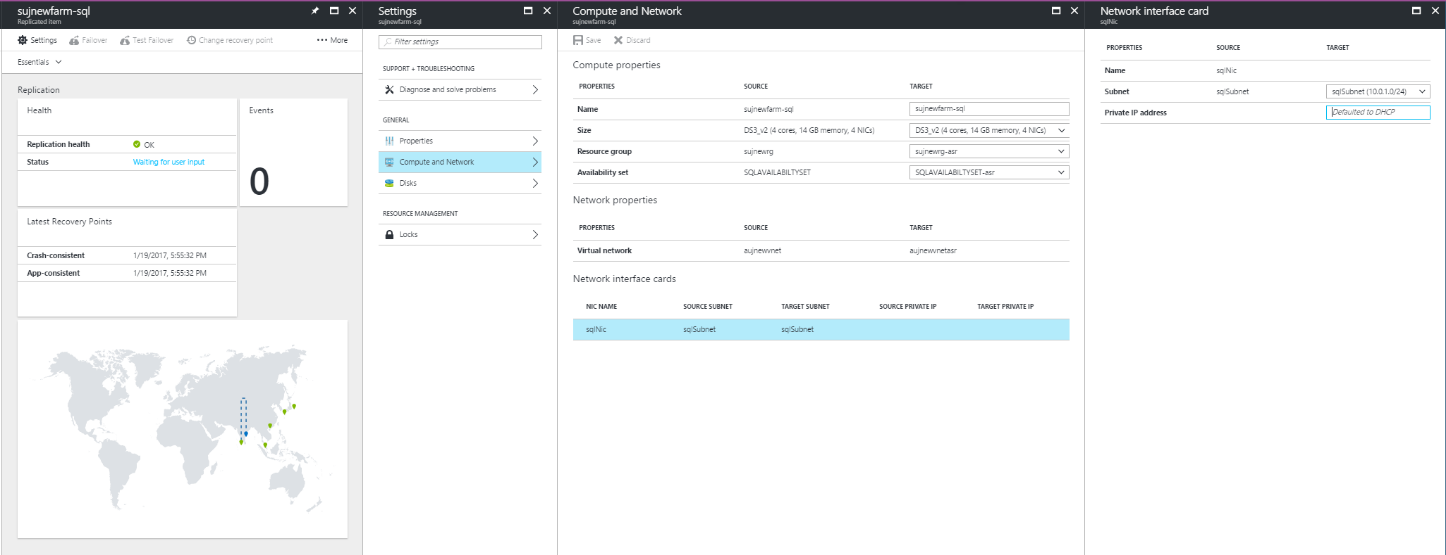
<https://docs.microsoft.com/en-us/powershell/resourcemanager/azurerm.recoveryservices/v2.2.0/remove-azurermrecoveryservicesvault>

Use the above command with utmost caution only on vaults which are sure to be deleted. If you delete any vault by mistake, you will lose all the data. And, there is no way to reverse it.

1. If your source Azure virtual network has DNS set to “custom”, the same will not be set if the “target virtual network” is created as part of Enable replication flow in ASR. You need to manually set the DNS server to custom and set the correct DNS server IP addresses (refer to the screenshot below). This is a known issue and will be fixed in the next update.



1. If the source VM has a static IP set on the NIC ([static IP documentation](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-reserved-private-ip)), the default setting of the corresponding replicated item in ASR will not be static IP. It is set to Dynamic IP. As a workaround, you can set the static IP explicitly in replicated item settings in portal (refer to the screenshot below). This issue will be fixed in the further updates.



# GETTING STARTED

Intro

|  |  |
| --- | --- |
| **!** | Always use ONLY <http://aka.ms/asr-a2a-private-preview-portal> to access the Azure portal while trying private preview scenarios. |

### Create a Recovery Services vault

1. Sign in to the Azure portal
2. Click **New** > **Management** > **Backup and Site Recovery (OMS)**. Alternately, you can click **Browse** > **Recovery Services** vaults > **Add**.

|  |  |  |
| --- | --- | --- |
| **i** |  | Make sure you create “Recovery services vault” in the same subscription where the Azure virtual machines are running. You cannot replicate VMs running in one subscription to another subscription. |

|  |  |  |
| --- | --- | --- |
| **i** |  | It is recommended that you create “Recovery services vault” in the location where you want to replicate your machines to i.e. the target Azure location. You cannot have your vault in source location as in the event of region wide disruption, your vault will also not available. |

1. In **Name** specify a friendly name to identify the vault. If you have more than one subscription, select the subscription in which the source VMs are running.
2. Create a new resource group or select an existing one, and specify an Azure location. You can select any location other than your source location where VMs are currently running.
3. If you want to quickly access the vault from the Dashboard click Pin to dashboard and then click **Create vault**.

The new vault will appear on the **Dashboard** > **All resources**, and on the **Browse > Recovery Services vaults** list.

### Prerequisites

1. If you are using [Network Security Groups (NSG)](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg) rules to control access to control outbound internet connectivity on the Azure VMs, ensure that you whitelist the below Azure data center IP ranges made available in this [link](https://www.microsoft.com/en-in/download/details.aspx?id=41653).
   * Source region IP ranges where your Azure VMs are running
   * Target region IP ranges where your VMs need to be replicated to
   * A specific list of IP ranges in ‘West US’ as the ‘Site recovery extension’ is hosted and available in ‘West US’ for the private preview. This requirement will not be there for public preview as the extension will be made available in all regions. Please send an email to ‘sujay.talasila@microsoft.com’ to get the specific list of IPs in ‘West US’ that need to be whitelisted.

You can use the below script for reference to automatically whitelist the IPs for a specific region. Note that this is a sample utility tool for reference and there will be no support from product group on the same.



1. If you are using any firewall proxy to control outbound internet connectivity, ensure you whitelist all the required Azure Site recovery service URLs listed below(or) the IP ranges mentioned in the previous point.
   * \*.blob.core.windows.net
     + The above URL is required so that data can be written to the storage account form the VM.
   * \*.hypervrecoverymanager.windowsazure.com
     + The above URL is required so that the Site recovery service communication can happen from the VM.
   * 169.254.169.254
     + The above URL is used for metadata service fetching on Azure VMs. Refer to [this article](https://azure.microsoft.com/en-us/blog/what-just-happened-to-my-vm-in-vm-metadata-service/) for more details.
   * login.microsoftonline.com
     + The above URL is used for authorization and authentication to the Site recovery service URLs.
2. If you are having an “[Express Route](https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction)” connection between your on-premises datacenter and Azure region and have a need for your application to talk to the on-premises machines, ensure that you have at least “[Site-to-Site](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal)” connection between your target Azure region and on-premises datacenter. If a lot of traffic is expected to flow between your target DR Azure region and on-premises datacenter, then you should have another Express Route connection between target Azure region and on-premises datacenter.
3. If you are using [Forced Tunneling](https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm) between Azure virtual network and your on-premises datacenter, ensure that the replication traffic is not forced to on-premises by creating the correct routing rules in your forced tunnel configuration.
4. For AD and DNS, it is recommended to use native AD replication. You can refer to “Site to Azure” section in [Protect Active Directory and DNS with Azure Site Recovery](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-active-directory) for guidance. For “Azure to Azure”, best practices are like “Site to Azure”. A first-class guidance document for AD and DNS for “Azure to Azure” will be published soon.
5. If you are using SQL Always ON clustering on primary site, it is recommended to use SQL Always ON for DR too. You can refer to [Protect SQL Server with SQL Server disaster recovery and Azure Site Recovery](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-sql) for guidance. A first-class guidance document for protecting SQL server for “Azure to Azure” will be published soon.

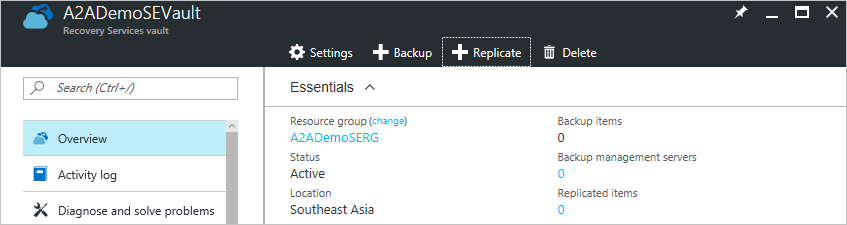
# PRIVATE PREVIEW SCENARIOS

Intro

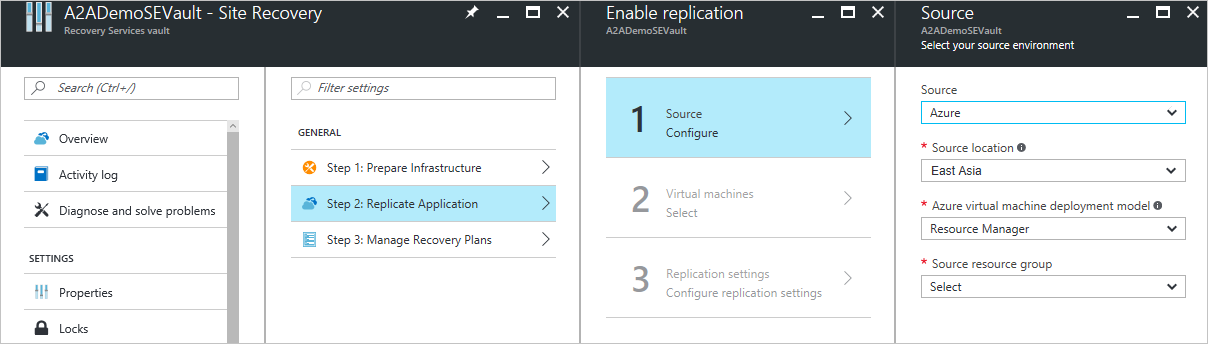
## Scenario 1 – Enable replication

For this article, the VMs are in the ‘East Asia’ Azure location and will be replicated to the ‘South East Asia’ location. The steps are as follows:

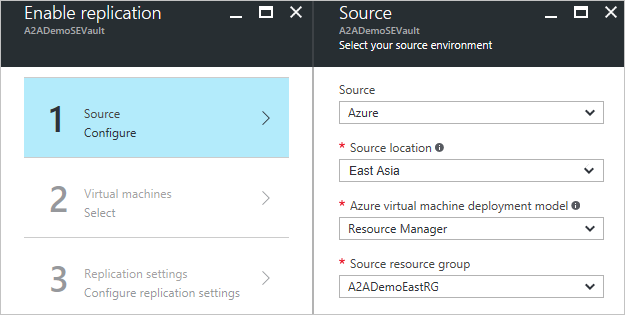
1. Open the vault and click **+Replicate** at the top of the vault.



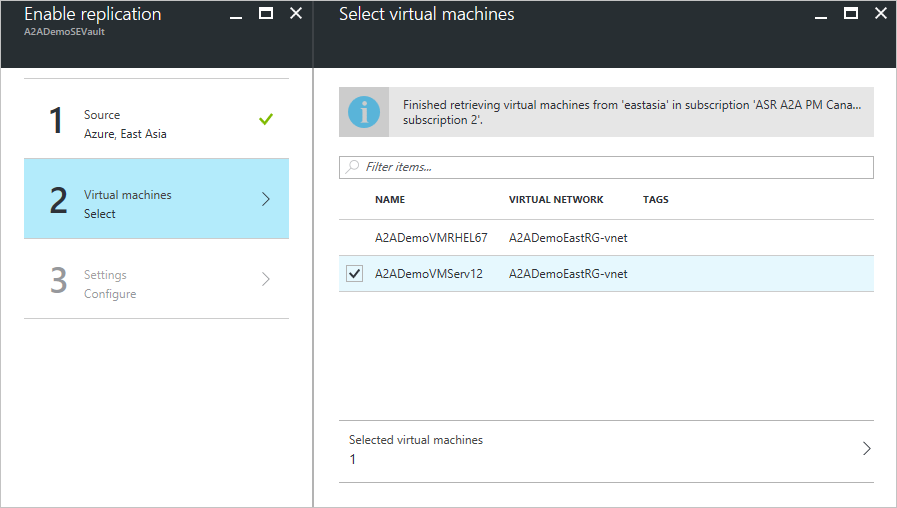
1. Alternately, you can also go to the vault **Settings** and under **Settings > Getting Started**, click **Site Recovery > Step 2: Replicate application > Source**. Since the replication is from Azure to Azure, there is no need to prepare any infrastructure under Step 1 of this settings blade.



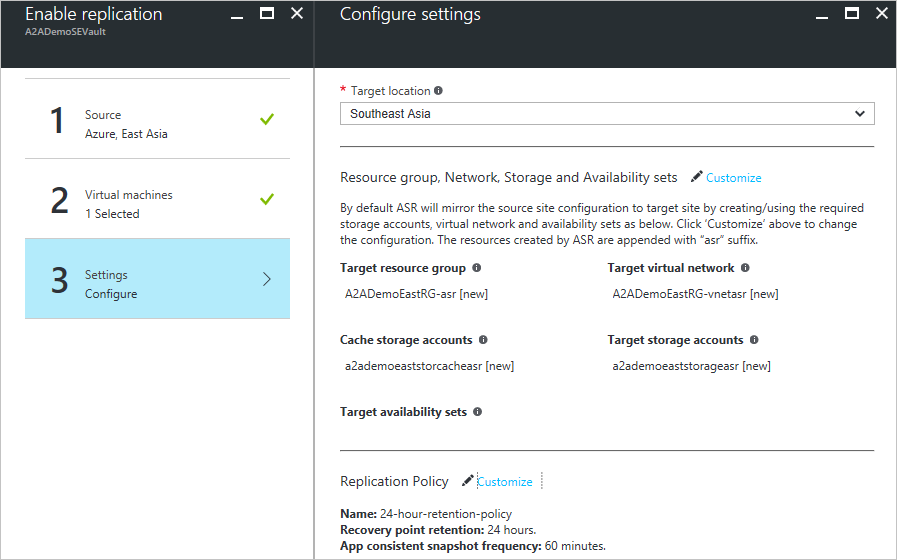
1. Select ‘Azure’ as the source and ‘East Asia’ as the source location (default options). Choose between ‘Resource Manager’ and ‘Classic’ for the deployment model and based on this selection, choose the appropriate resource group or cloud service. Then click **OK**.



1. In **Virtual Machines** > **Select virtual machines**, click and select each machine you want to replicate. You can only select machines for which replication can be enabled. Then click **OK**.

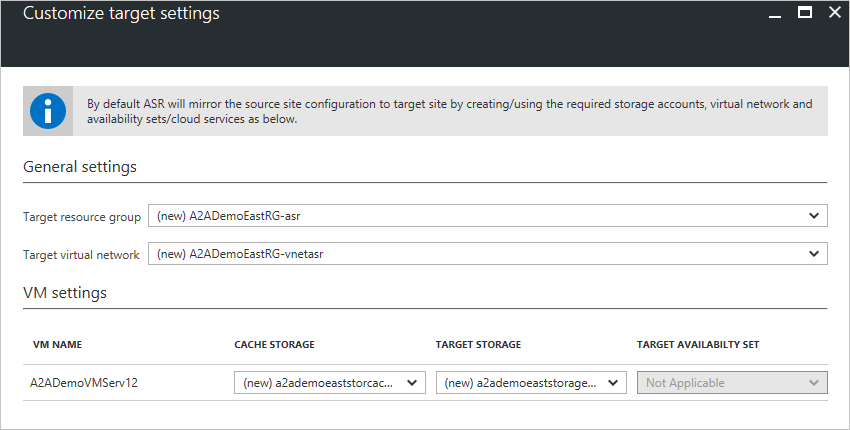


1. In **Settings** > **Configure settings,** ensure that the target location is the same as the location of the recovery vault. For this article, the target location is ‘South East Asia’.

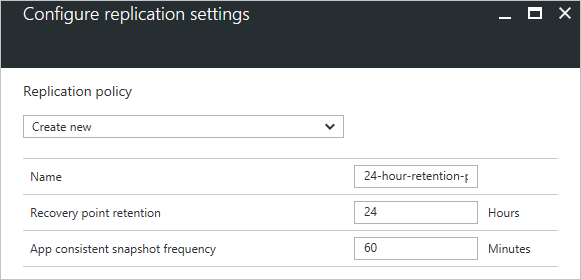


|  |  |  |  |
| --- | --- | --- | --- |
| **i** |  | By default, ASR will mirror the source site configuration to `target site by creating/using the required storage accounts, virtual network and availability sets identified from the source. If any resource is not already available, ASR will create them. The resources created by ASR are appended with ‘asr’ suffix. New resources to be provisioned are indicated by a ‘[new]’ suffix. Click **Customize** to change the configuration. |  |

1. You can click on ‘Customize’ to change the default resource group, network, storage and availability sets.



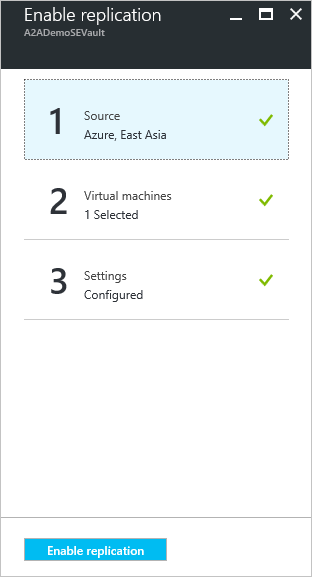
1. The first time you replicate a VM, ASR will create a new replication policy with default settings of ‘24 hours’ for recovery point retention and ’60 minutes’ for app consistent snapshot frequency. Click **Customize** to change this configuration or create new policies.



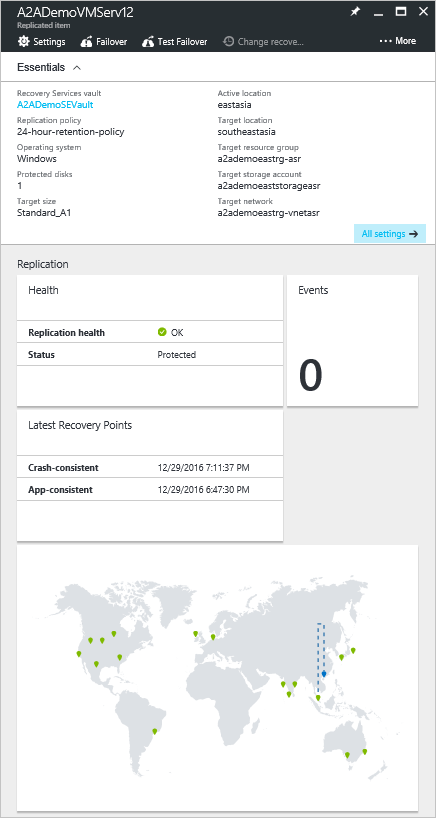
1. Click **Create target resources**. As the name indicates, this will provision the required target resources for the selected VMs to be replicated. This step will take about a minute to complete.

|  |  |
| --- | --- |
| **!** | Do not close the blade when the required target resources are being provisioned. It should take about a minute to complete. If you close the blade or refresh the browser, you need to start the ‘Enable replication’ step again. |

1. Click **Enable replication** once the above steps are complete.

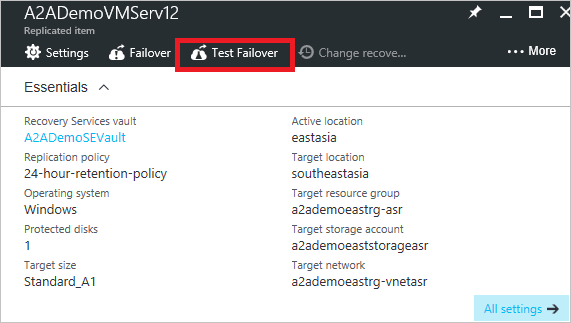


1. This will trigger the VM replication and you can track progress of the **Enable Protection** job in **Settings** > **Jobs** > **Site Recovery Jobs**.
2. Depending on the size of the disks, it can take a few hours before the initial data synchronization is complete.
3. From **Settings** > **Replicated Items** you can view the status of the protected VM and the initial replication progress.
4. Clicking on the VM name launches the VM overview blade where you can see various settings related to the replicated VM.

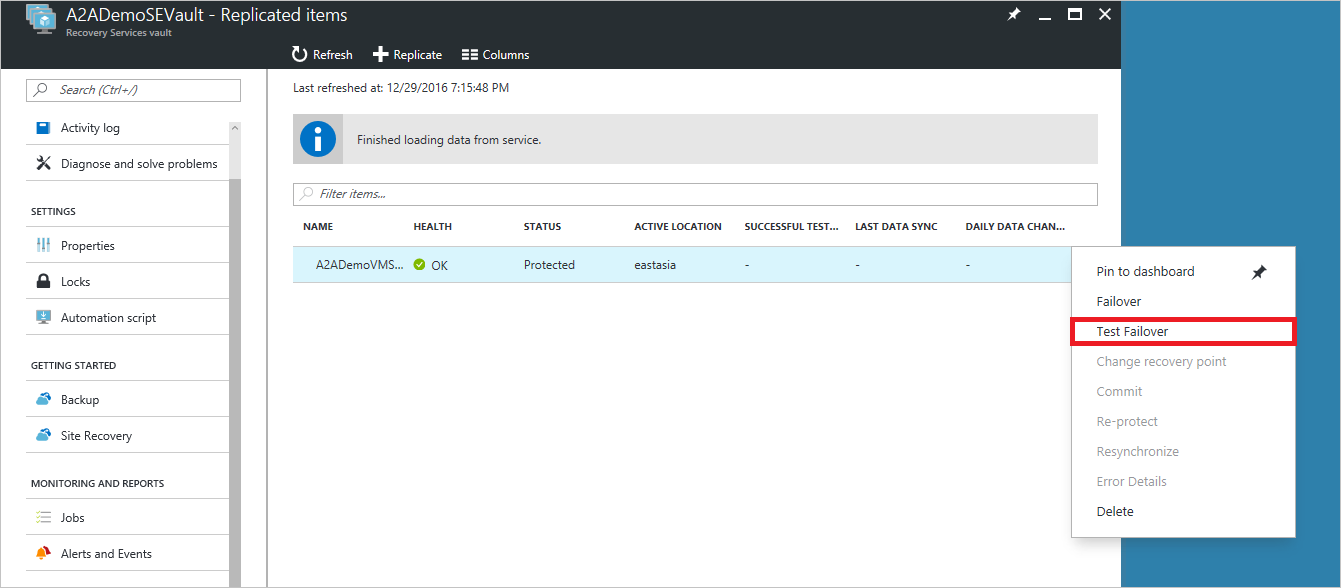


## Scenario 2 – Test Failover

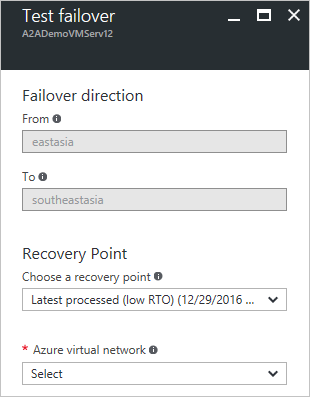
1. To fail over a single machine, in **Settings** > **Replicated Items**, click the **VM** > **Test Failover** icon from the top bar of the VM overview.



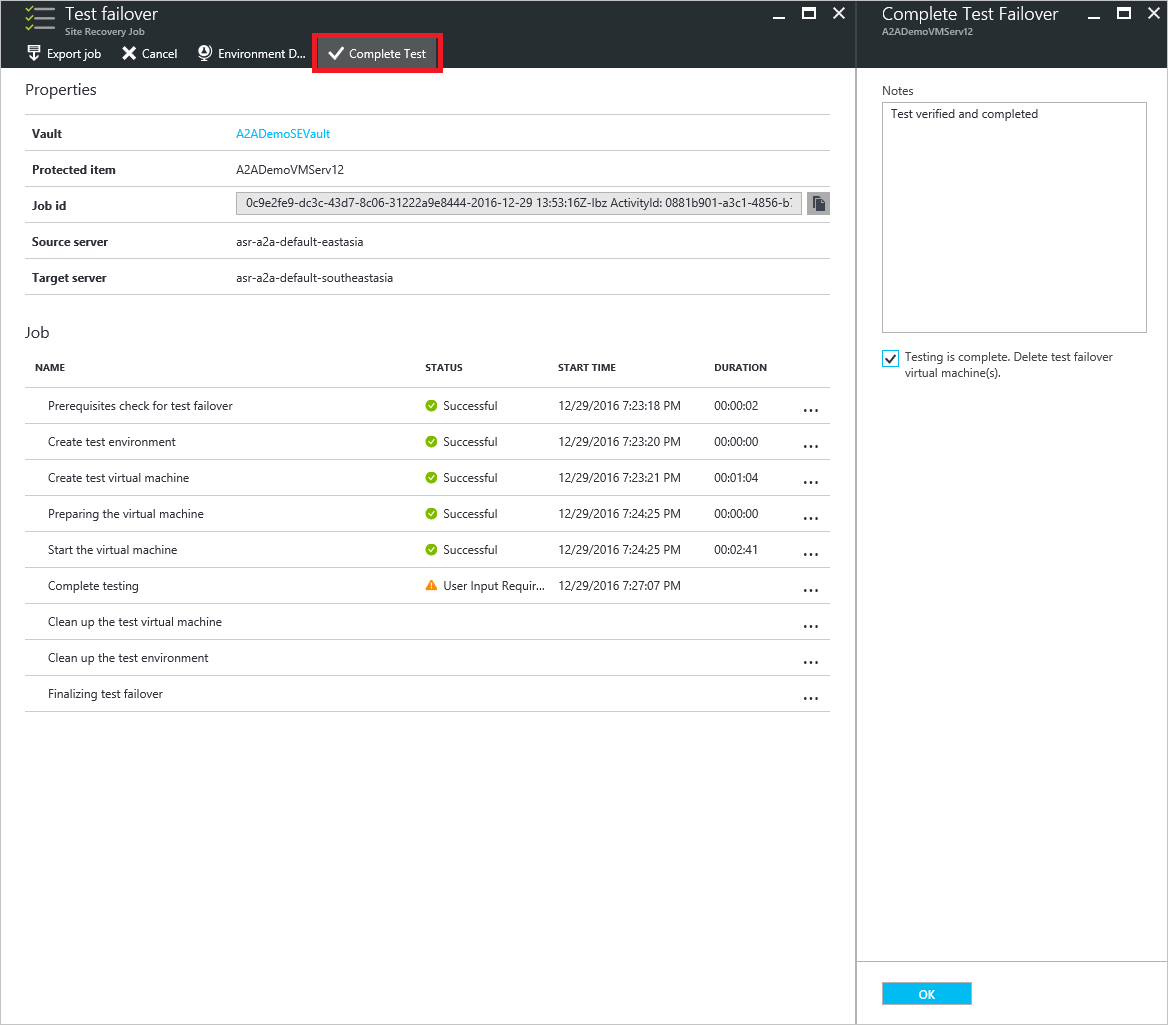
1. Alternately, you can also right click the VM/select context menu of the VM and click **Test Failover.**

****

1. In **Test Failover** (direction from ‘eastasia’ to ‘southeastasia’), select the recovery point and Azure network to which Azure VMs will be connected after failover occurs. It is suggested to use a non-production test network for the test failover.



1. 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 name > **Settings** > **Jobs** > **Site Recovery jobs**.
2. When the failover reaches the **Complete testing** status, do the following:
   1. View the replica virtual machine in the Azure portal. Verify that the virtual machine starts successfully.
   2. If you’re set up to access virtual machines from your on-premises network, you can initiate a Remote Desktop connection to the virtual machine.
   3. Click **Complete test** to finish it.
   4. Use the **Notes**, to record and save any observations associated with the test failover.
   5. Click **Testing is complete. Delete test failover virtual machine(s)**, to automatically clean up the test environment. After this is done the test failover will show a Complete status.
   6. At this stage any elements or VMs created automatically by Site Recovery during the test failover are deleted. Any additional elements you've created for test failover aren't deleted.



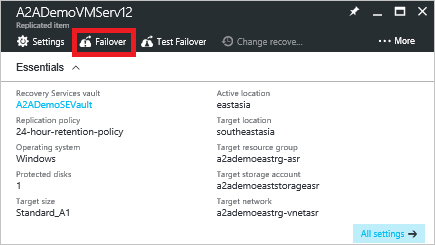
1. After the failover completes, you should also be able to see the replica Azure machine appear in the **Azure portal > Virtual Machines**. You should make sure that the VM is the appropriate size, that it's connected to the appropriate network, and that it's running.
2. To RDP into the machine [add a public IP](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-monitoring-and-troubleshooting#adding-a-public-ip-on-a-resource-manager-virtual-machine) on the VM’s NIC and click ‘Connect’ on the VM overview blade.



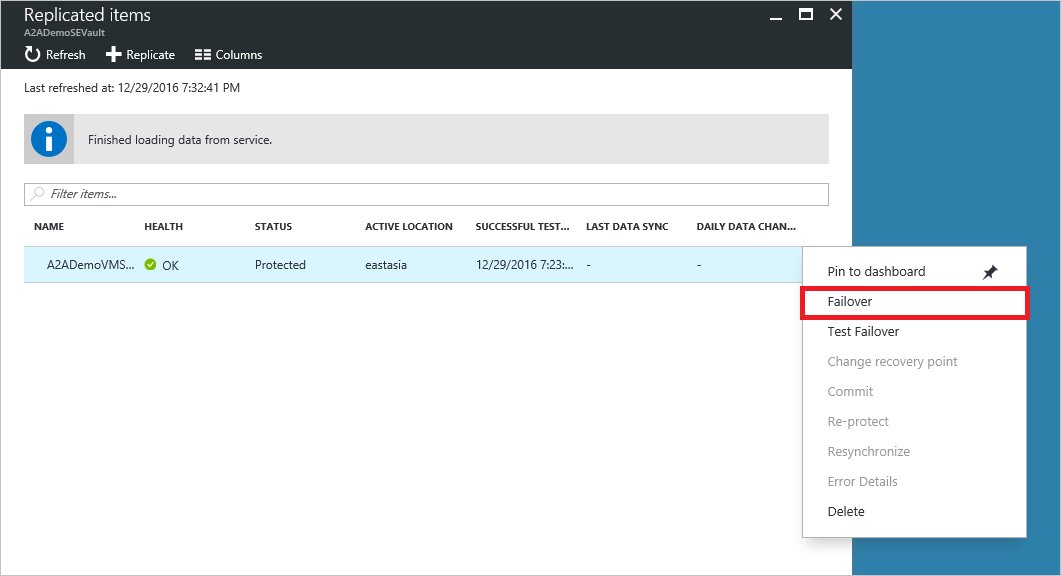
## Scenario 3 – Failover

The unplanned failover option initiates the actual failover of the VM from the original Azure location to the failover location. It is strongly suggested to run a test failover before performing an unplanned failover since many of the changes under an unplanned failover are not reversible. ASR will also display a warning if an unplanned failover is attempted without a prior test failover 60 days before the unplanned failover.

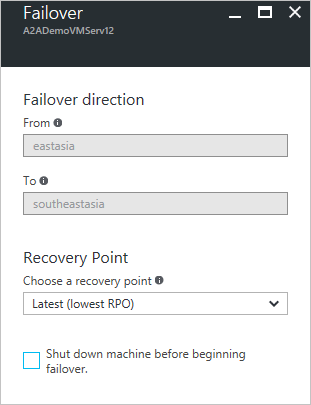
1. To fail over a single machine, in **Settings** > **Replicated Items**, click the **VM** > **Failover** icon from the top bar of the VM overview.



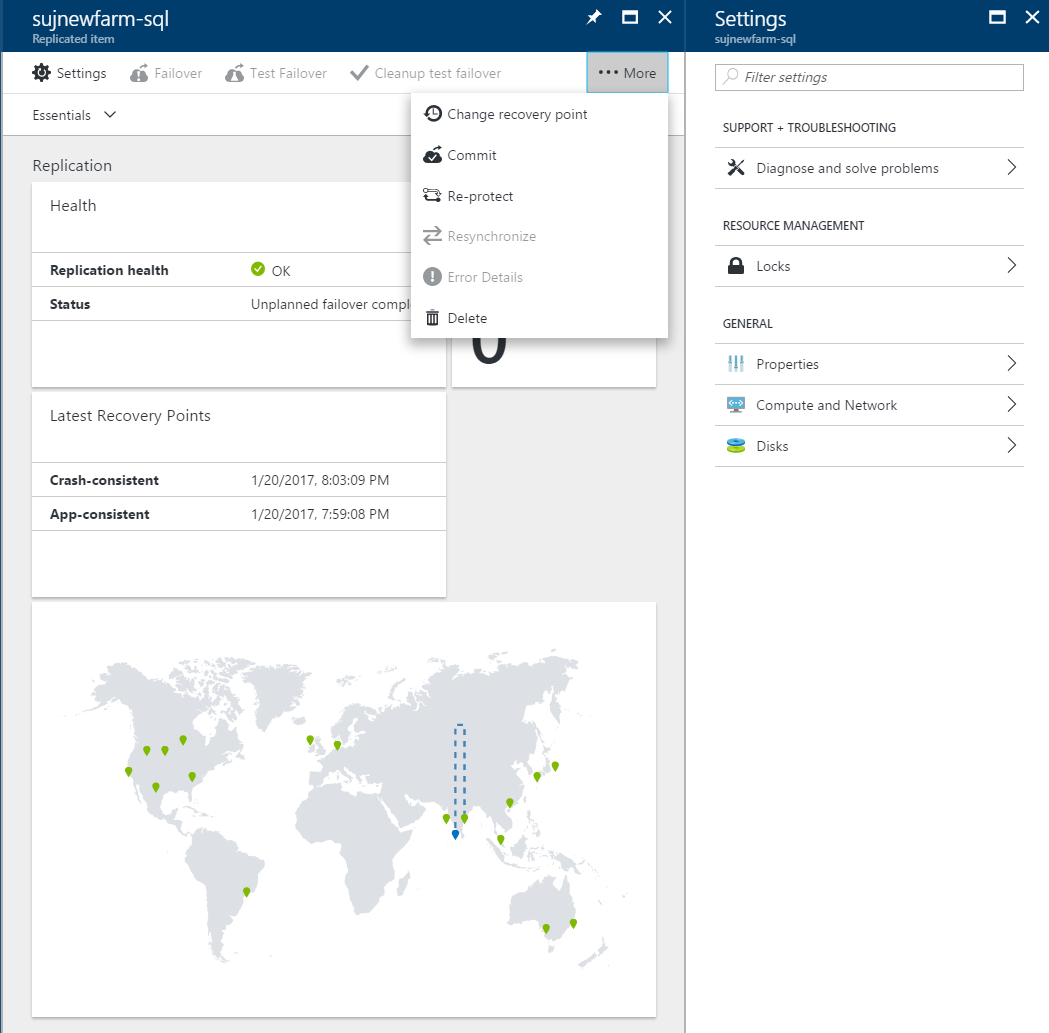
Alternately, you can also right click the VM/select context menu of the VM and click **Failover.**

****

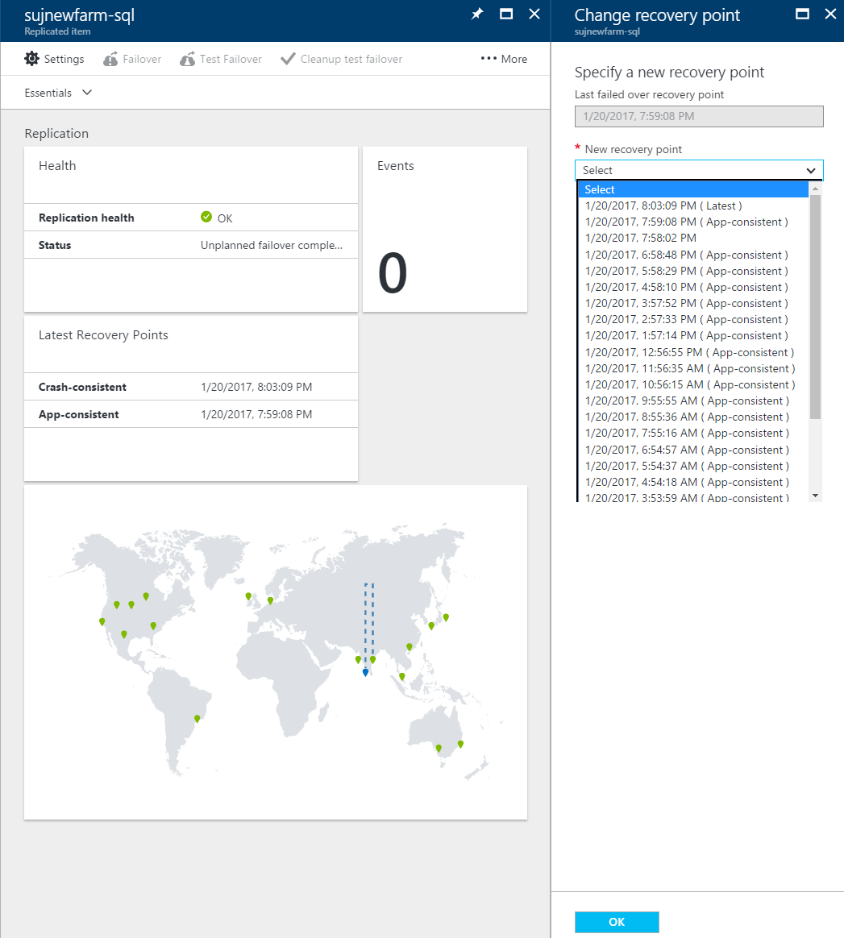
1. In **Failover** (direction from ‘eastasia’ to ‘southeastasia’), select the required recovery point.



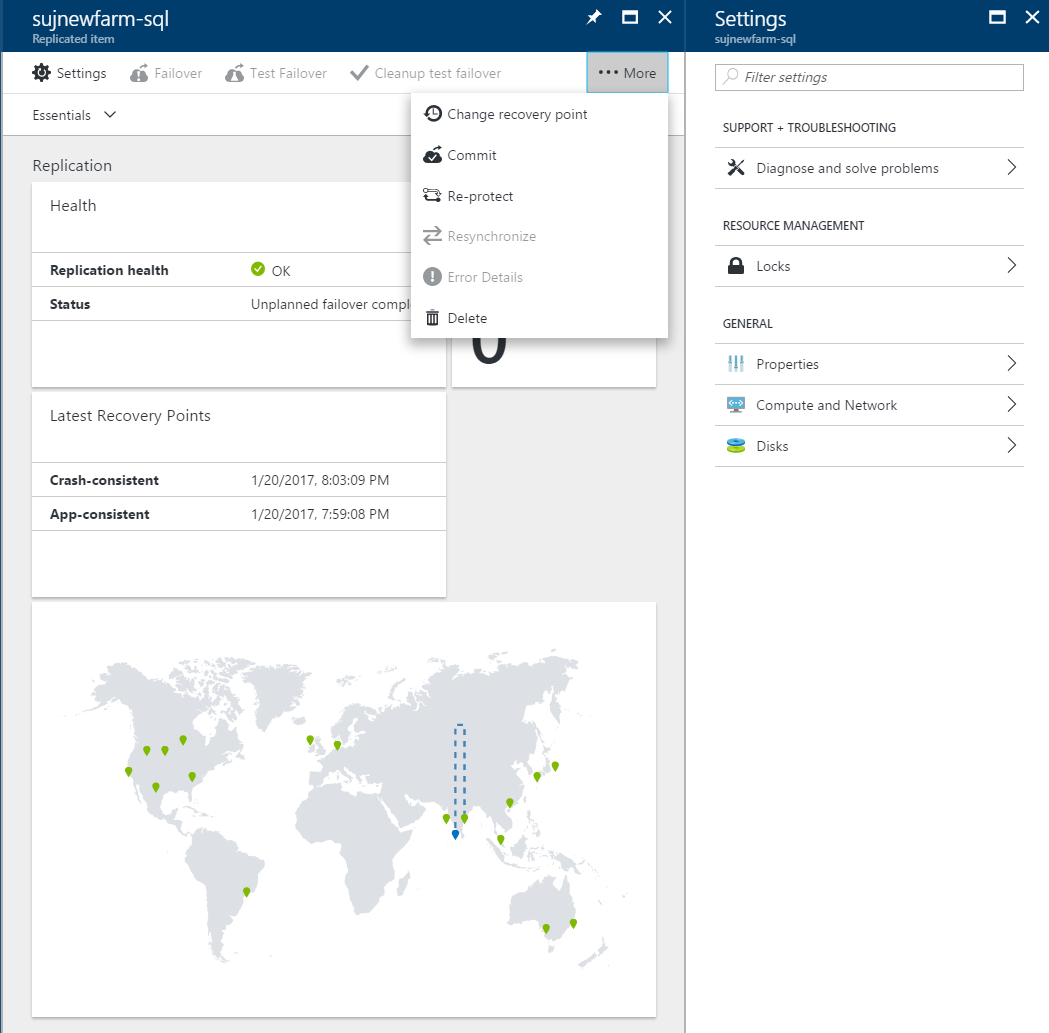
1. Select **Shut down machine before beginning failover** to specify that Site Recovery should try to shut down the protected virtual machines and synchronize the data so that the latest version of the data will be failed over.
2. Click **OK** to begin the failover. You can track progress by clicking on the VM to open its properties, or on the **Unplanned Failover** job in vault name > **Settings** > **Jobs** > **Site Recovery jobs**.
3. After the failover, the virtual machines are in a commit pending state. You can change the recovery point based on you need before committing the failover.
4. To change recovery point, click on “Change recovery point”.



1. You can select any recovery point available and click OK. The VM will be recovered to that point.



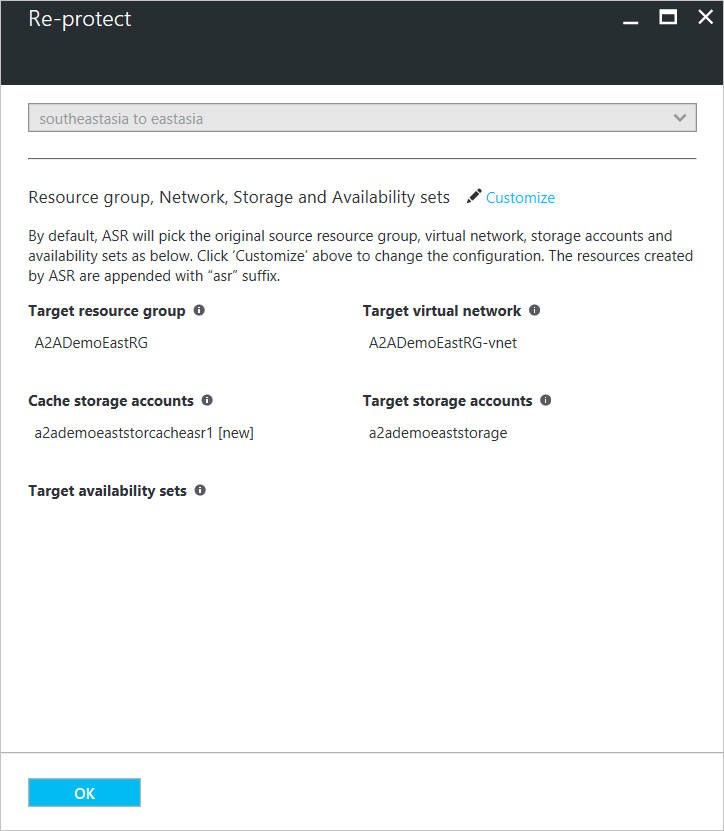
1. Click **Commit** to confirm the current failover point. Committing a failover is a non-reversible operation so ensure that the failed-over VM boots and meets your failover requirements. If it does not, then you can change the recovery point to any other available recovery point. Post a commit, all previous recovery points are removed.



## Scenario 4 – Re-protect after failover

After failover is complete the virtual machines start up and are running at the secondary location. However, they aren’t protected or replicating. When the primary site is available again with the same underlying infrastructure, you must reverse replicate the VM. This ensures that all the data is replicated back to the primary site, and that the virtual machine is ready for failover again.

In **Settings** > **Replicated Items**, right click the VM and click **Re-protect** to begin reverse replication. As before during the initial replication process, you can modify the resource group, network, storage and availability sets for the VM to be replicated. Click **Customize** to make the modifications.



Once the re-protect operation completes and the VM is again under protection, you can click on the VM summary under **Settings** > **Replicated Items** and verify the direction of the replication (‘southeastasia’ to ‘eastasia’).

## Scenario 5 – Failback

After failover and reprotection of the VM, the machine is now is ready to be failed back to the original site. This involves performing an unplanned failover in the opposite direction to that done before (i.e. ‘southeastaisa’ to ‘eastasia’)

The process is similar to that of the initial failover, the difference being the direction of the failover compared to the original. The process is as follows:

1. Perform a test failover in the required failback direction. This involves:
   1. Right click VM name from **Settings** > **Replicated Items** and click **Test Failover**.
   2. Select the recovery point and network.
   3. Verify the VM for consistency and click **Complete test** when the option becomes available.
   4. Complete the test and remove test artifacts.
2. Perform an unplanned failover in the required direction (‘eastasia’ to ‘southeastasia’) by:
   1. Clicking **Settings** > **Replicated Items,** right-click VM name and click **Failover.**
   2. Choose the recovery point and click **OK.**
   3. Post failover, either **Commit** or **Change recovery point** for the VM to finalize the failover.
3. Like the post-failover state, the failed back VM is neither protected nor replicating.
   1. Protect the VM by right-clicking the VM name from **Settings** > **Replicated Items** and click **Re-protect** to begin reverse replication.
   2. This will now protect the VM from its original site by replicating to the failover site.
   3. Modify the resource group, network, storage and availability set as desired and click **OK.**

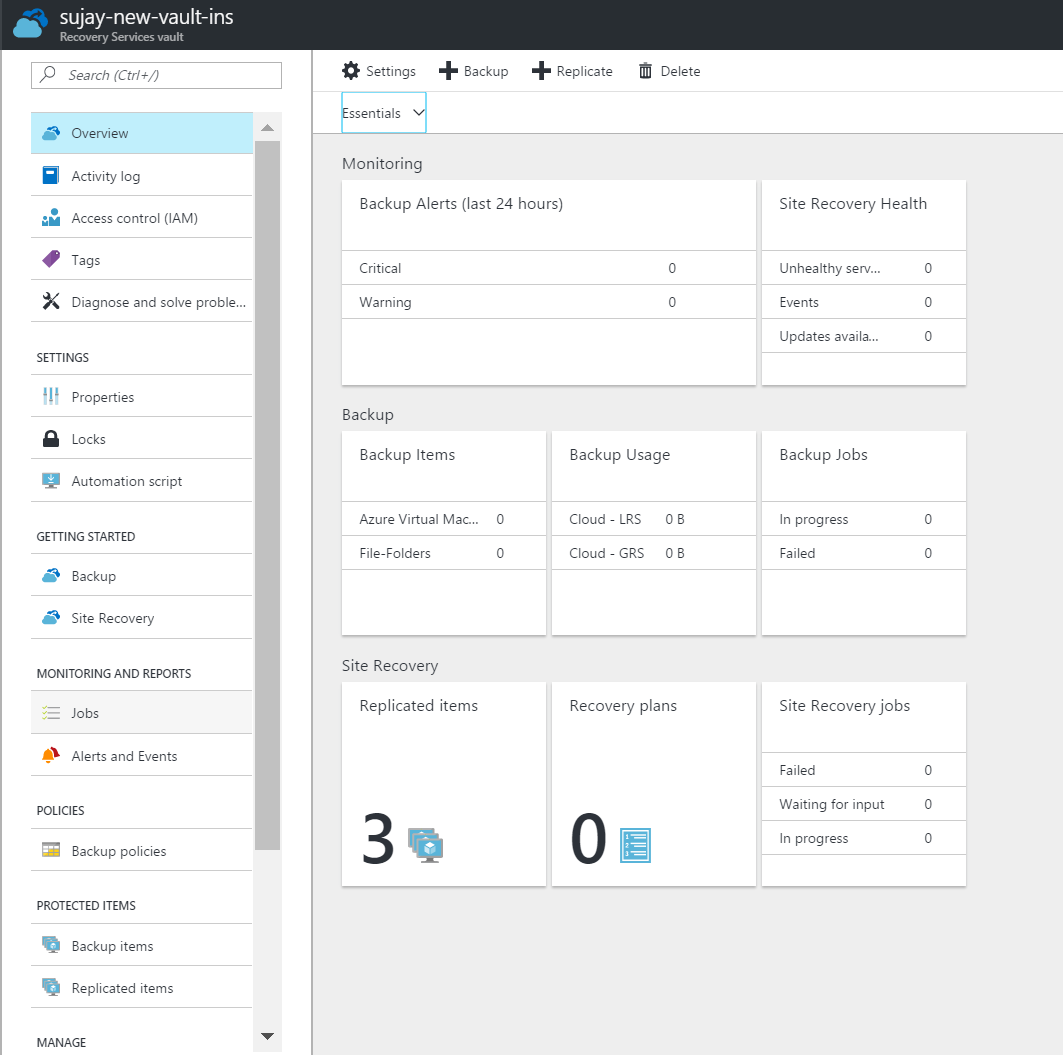
Post the above steps, the VM will now be protected at its original location ‘East Asia’ with replication to ‘South East Asia’.

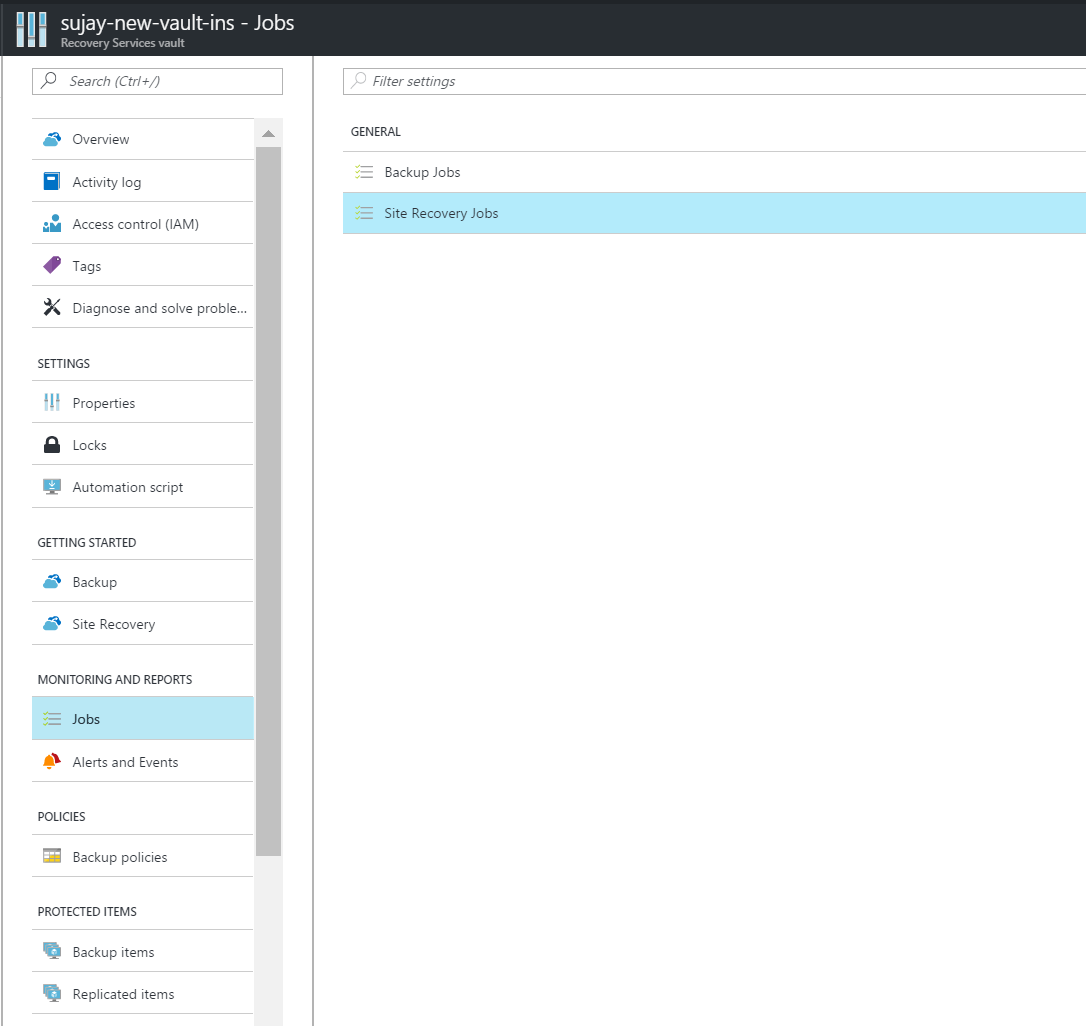
## Scenario 6 – Re-protect after failback

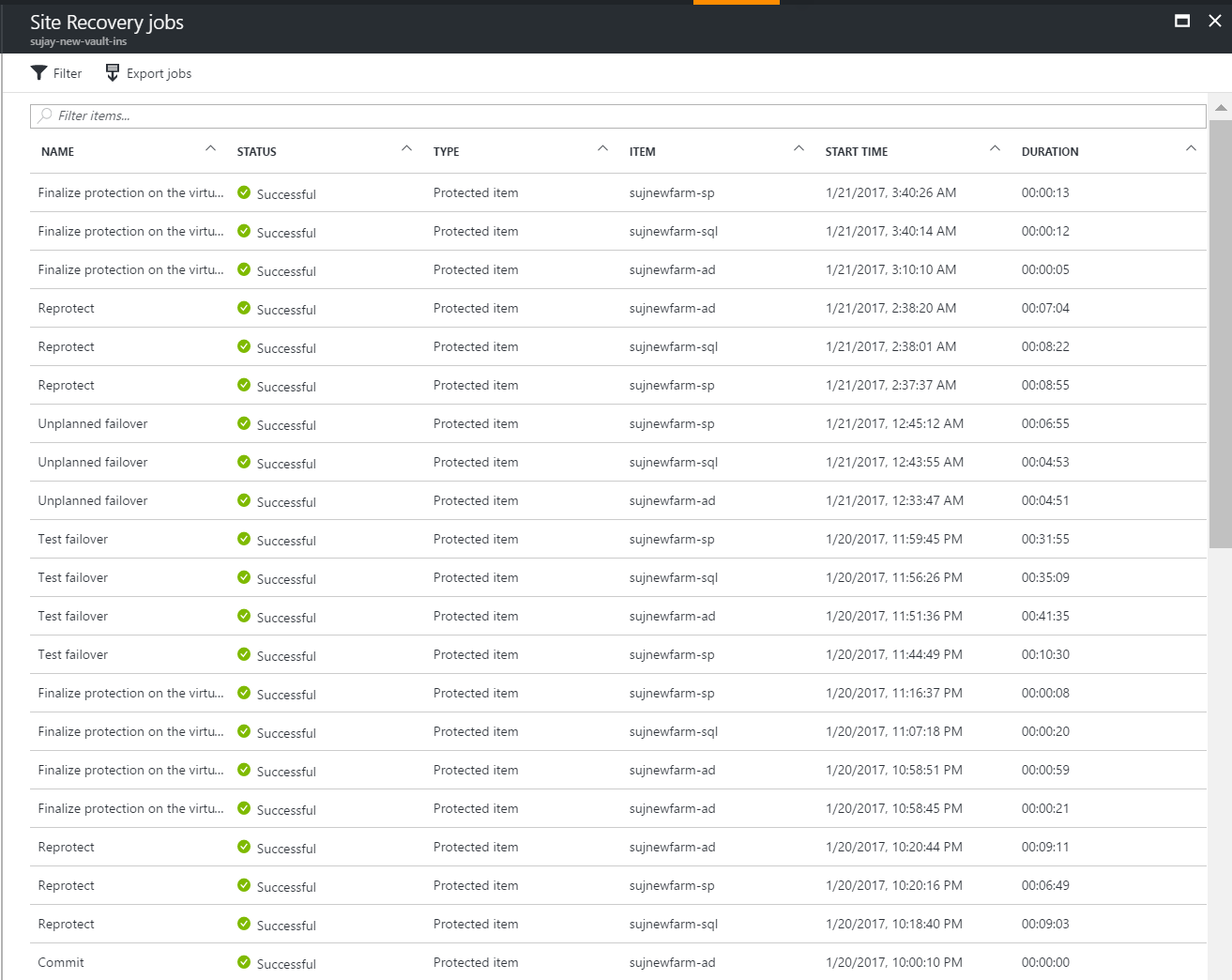
After failback (failover from target site to source site) is complete the virtual machines start up and are running at the secondary location. However, they aren’t protected or replicating. You need to enable replication to the target site following the same steps listed in “[Scenario 4](#_Scenario_4_–)”.

# MONITORING SITE RECOVERY OPERATIONS

For any ASR operation, you can track the progress and get details by going to **Jobs** > **Site Recovery Jobs** in the left menu of recovery services vault dashboard. You can refer to the screenshots below.

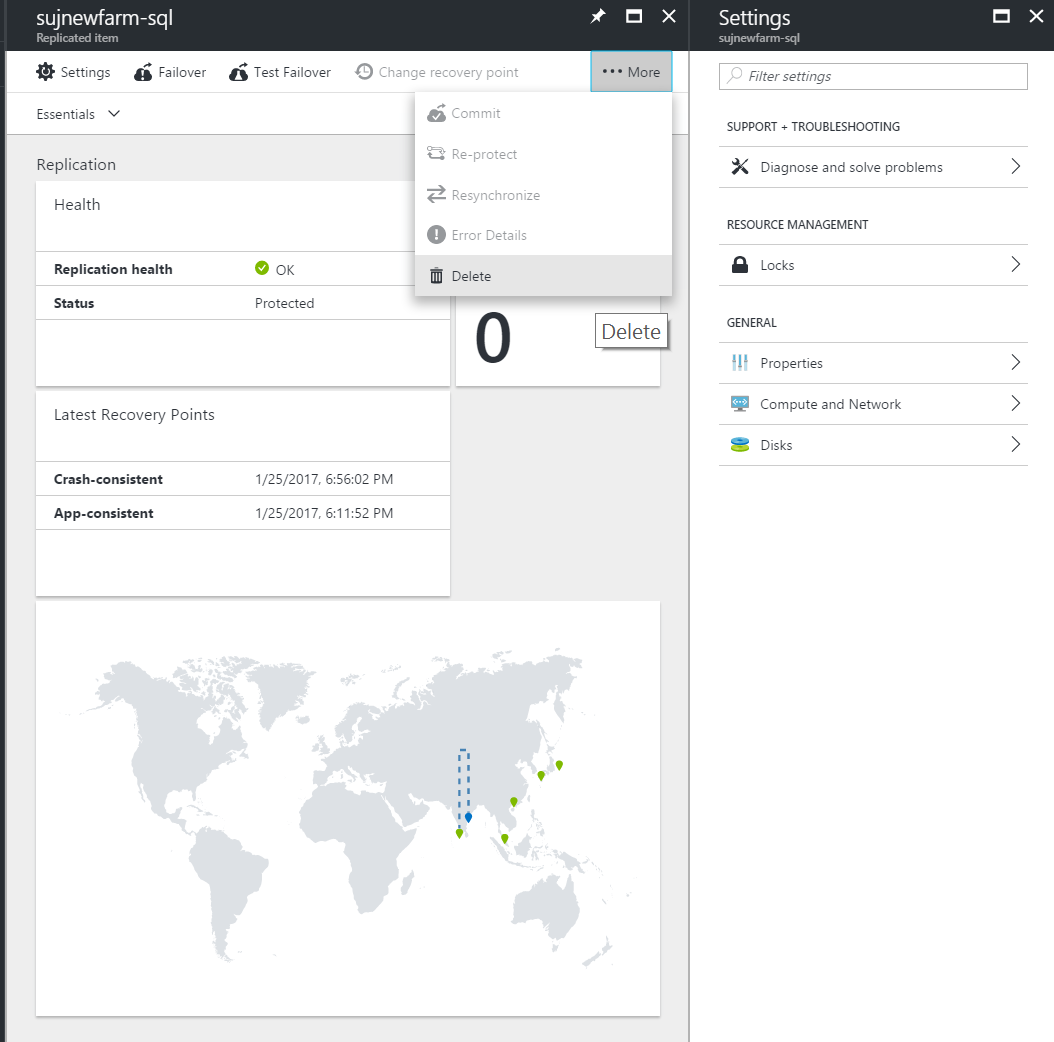






# DISABLING REPLICATION

1. To remove site recovery protection, click on **Protected Items** > **Replicated** in the left menu of recovery services vault dashboard.
2. Click on the specific replicated item to open the dashboard view.
3. Click on Delete from the menu to disable replication.



# DELETING RECOVERY SERVICES VAULT

You cannot delete the “Recovery services vault” used for private preview from Azure portal. There is a known issue and will be fixed in the next update. As a workaround, you can either delete the entire “Resource group” or use the below PowerShell cmdlet to delete the vault. The issue will be fixed in the next update.

<https://docs.microsoft.com/en-us/powershell/resourcemanager/azurerm.recoveryservices/v2.2.0/remove-azurermrecoveryservicesvault>

Use the above command with utmost caution only on vaults which are sure to be deleted. If you delete any vault by mistake, you will lose all the data. And, there is no way to reverse it.