Microsoft

Desktop-as-a-Service (DaaS) Using Windows Virutal Desktop (WVD)

Business Continuity with Azure Site Recovery

Prepared for:
Service Provider Partners
Oct. 2019

Prepared by:
Microsoft – **O**ne **C**ommercial **P**artner (OCP)

MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Contents

1. Overview

This document is a walk-through of implementing Azure Site Recovery (ASR) within Windows Virtual Desktop (WVD) in Microsoft Azure. In this walk-through, we'll setup a 24-hour back up, with a 4-hour snapshot frequency. Additionally, we'll establish a dual-region replication policy & test fail-over.

Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Please be advised this information is provided to help understand/summarize this process and your enterprises` implementation may contain additional customizations and/or settings that ***might not*** be covered in this document.

1. Prerequisites

Azure & Windows Active Directory Prerequisites

Before getting started, **all** items listed below **must** be checked/validated to ensure the most basic requirements are in place to proceed with executing the remaining steps in this guide.

- A Windows Virtual Desktop tenant.
- An account with permissions to manage that tenant (such as RDS Contributor.)
- Session host pool VMs configured and registered with the Windows Virtual Desktop service.

General Best Practices

Since everyone's business and technical requirements vary across the board, it is always a good idea to familiarize yourselves with the standard best practices across the different Azure technologies & services.

- Please follow the guidance here to maintain a consistent naming convention across your resources, unless you are already using a naming system.
- Azure security best practices and patterns
- Azure Active Directory Hybrid Identity best practices
- Azure identity management and access control security best practices
- Azure Networking & security Best Practices
- Azure Storage security overview

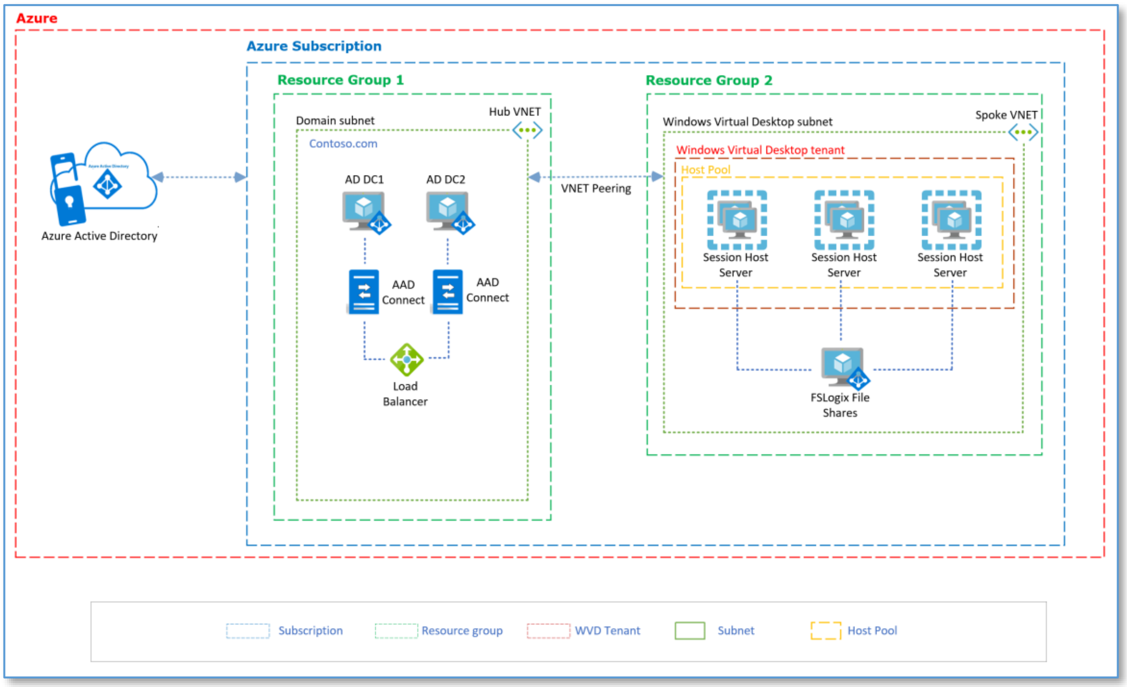
- Best practices for Azure VM security

Azure Networking

The recommendation is to design your Azure Networking using a Hub-Spoke topology. Consider the HUB like a DMZ deployed with your Virtual network Gateways and other security/edge appliances like Firewalls Etc. while the Spoke will act as the backend zone where your session hosts servers are deployed to and is peered with the HUB. This is our design for this walk-through, so you'll need this already setup before proceeding.

Azure Architectural Diagram

Below is a diagram of the Azure environment that we'll use. It shows the objects created in Azure and their relationships within the environment. In this example, the company name will be Contoso.



2. Setup Disaster Recovery for Azure WVD VMs

This section is a walkthrough of setting up ASR for your WVD deployment. We will:

- Create a Recovery Services vault
- Verify target resource settings
- Set up outbound network connectivity for VMs

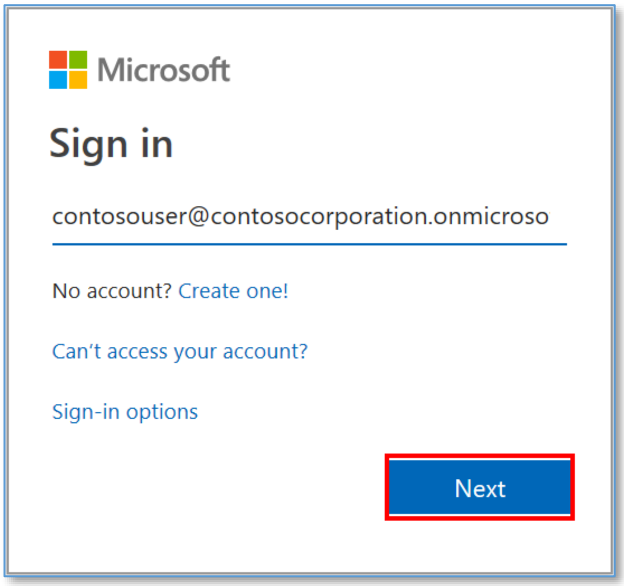
- Enable replication for a UDP file server VM

Create a Recovery Services vault

We need to create the vault in any region, *except* the source region. In that remote region, we'll create a resource group in which to create the vault. In our example below, the new resource group is named **ContosoRSVRG** and is created in the Central US region.

1. Log into your Azure subscription using the PowerShell Connect-AzAccount cmdlet:

```
Connect-AzAccount
```



Microsoft

Sign in

contosouser@contosocorporation.onmicroso

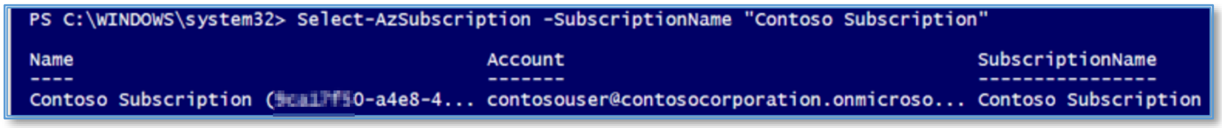
No account? Create one!

Can't access your account?

Sign-in options

2. Select the Azure subscription you want to replicate your virtual machines to. In our example, we're using the Contoso subscription for both source and target:

```
Select-AzSubscription -SubscriptionName "Contoso Subscription"
```



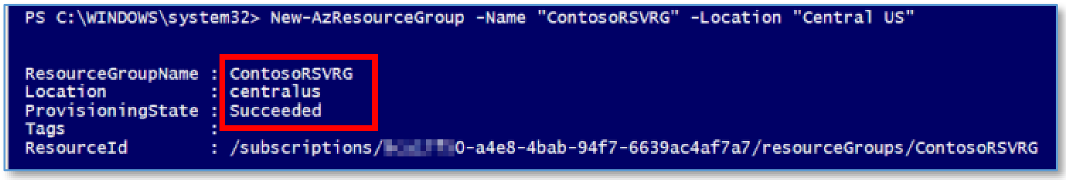
```
PS C:\WINDOWS\system32> Select-AzSubscription -SubscriptionName "Contoso Subscription"

Name                                       Account                                        SubscriptionName
----                                       -------                                        ----------------
Contoso Subscription ([redacted]0-a4e8-4... contosouser@contosocorporation.onmicroso... Contoso Subscription
```

3. Create a resource group in which to create the Recovery Services vault. We're using Central US as the target region for this walk-through, while our source region is East US:

   Make sure your subscription has enough resources to support VM sizes that match your source VMs. Site Recovery picks the same size, or the closest possible size, for the target VM.

```
New-AzResourceGroup -Name "ContosoRSVRG" -Location "Central US"
```

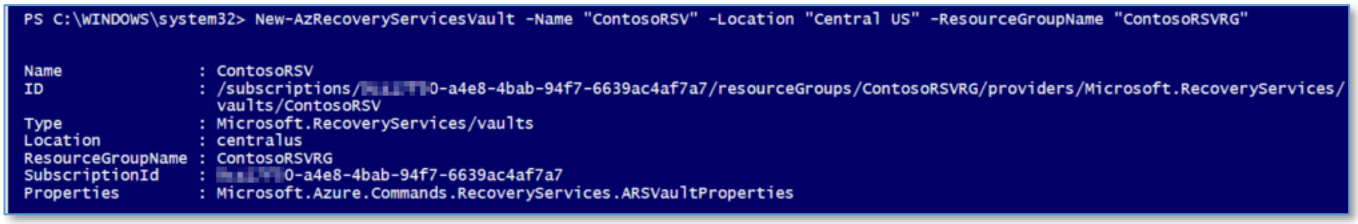


```
PS C:\WINDOWS\system32> New-AzResourceGroup -Name "ContosoRSVRG" -Location "Central US"

ResourceGroupName : ContosoRSVRG
Location          : centralus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/[redacted]0-a4e8-4bab-94f7-6639ac4af7a7/resourceGroups/ContosoRSVRG
```

4. Create a Recovery services vault. We'll call ours **ContosoRSV**:

```
New-AzRecoveryServicesVault -Name "ContosoRSV" -Location "Central US" `
-ResourceGroupName "ContosoRSVRG"
```



```
PS C:\WINDOWS\system32> New-AzRecoveryServicesVault -Name "ContosoRSV" -Location "Central US" -ResourceGroupName "ContosoRSVRG"

Name              : ContosoRSV
ID                : /subscriptions/[redacted]0-a4e8-4bab-94f7-6639ac4af7a7/resourceGroups/ContosoRSVRG/providers/Microsoft.RecoveryServices/
                    vaults/ContosoRSV
Type              : Microsoft.RecoveryServices/vaults
Location          : centralus
ResourceGroupName : ContosoRSVRG
SubscriptionId    : [redacted]0-a4e8-4bab-94f7-6639ac4af7a7
Properties        : Microsoft.Azure.Commands.RecoveryServices.ARSVaultProperties
```

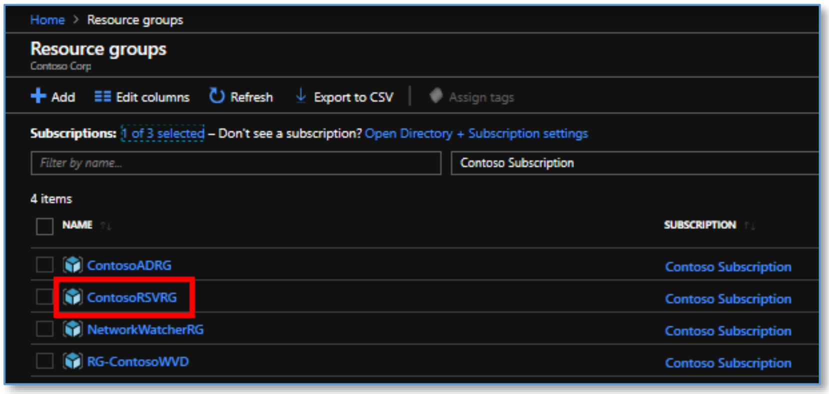
The Recovery services vault is now ready for replication configuration.

Note

Only Azure VMs running Windows operating systems and **enabled for encryption with Azure AD app** are currently supported by Azure Site Recovery.

Enable Replication

1. In the Azure Portal, click the new resource group you just made. Our is the **ContosoRSVRG** resource group:



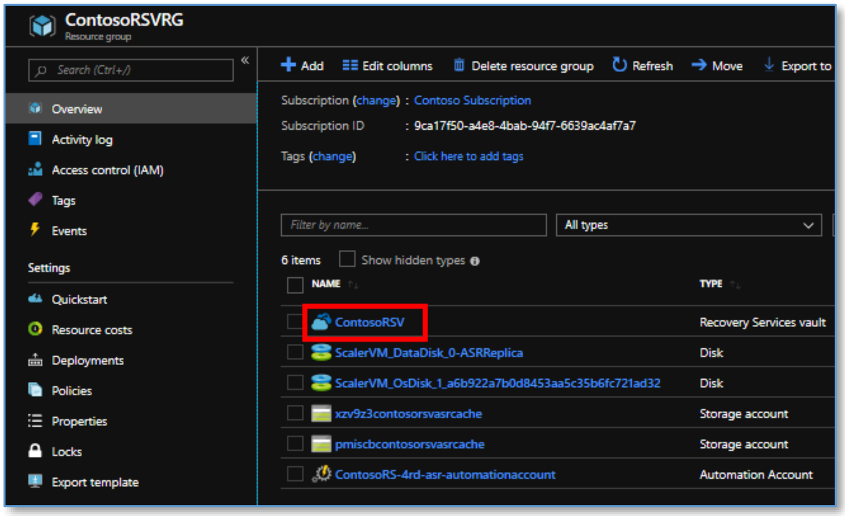
Subscriptions: 1 of 3 selected – Don't see a subscription? Open Directory + Subscription settings

Filter by name... | Contoso Subscription

4 items

NAME	SUBSCRIPTION
ContosoADRG	Contoso Subscription
ContosoRSVRG	Contoso Subscription
NetworkWatcherRG	Contoso Subscription
RG-ContosoWVD	Contoso Subscription

2. Click the Recovery Services vault name, then click **+Replicate:**



Subscription (change) : Contoso Subscription

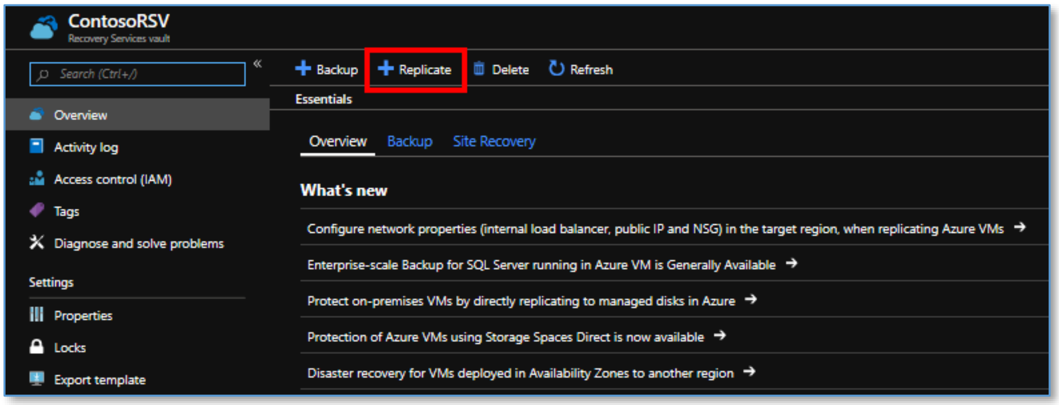
Subscription ID : 9ca17f50-a4e8-4bab-94f7-6639ac4af7a7

Tags (change) : Click here to add tags

Filter by name... | All types

6 items □ Show hidden types

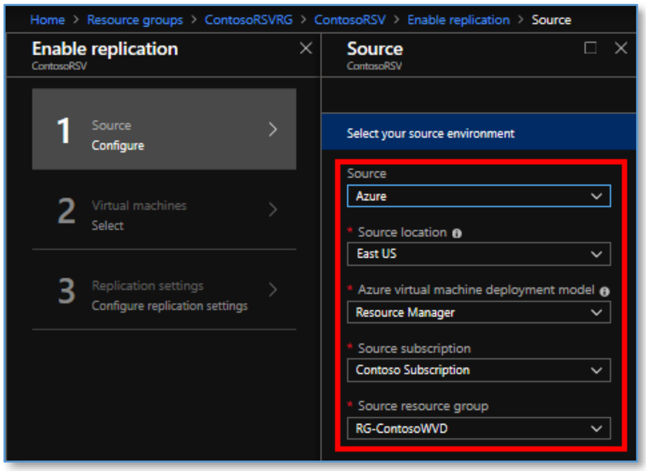
NAME	TYPE
ContosoRSV	Recovery Services vault
ScalerVM_DataDisk_0-ASRReplica	Disk
ScalerVM_OsDisk_1_a6b922a7b0d8453aa5c35b6fc721ad32	Disk
xzv9z3contosorsvasrcache	Storage account
pmiscbcontosorsvasrcache	Storage account
ContosoRS-4rd-asr-automationaccount	Automation Account



What's new

- Configure network properties (internal load balancer, public IP and NSG) in the target region, when replicating Azure VMs →
- Enterprise-scale Backup for SQL Server running in Azure VM is Generally Available →
- Protect on-premises VMs by directly replicating to managed disks in Azure →
- Protection of Azure VMs using Storage Spaces Direct is now available →
- Disaster recovery for VMs deployed in Availability Zones to another region →

- As shown below, in **Source**, select **Azure**.
- In **Source location**, select the region where the VMs are currently running.
- Select the **Source subscription** where the virtual machines are running. This can be any subscription within the same Azure Active Directory tenant where your recovery services vault exists.
- Select the **Source resource group** and click **OK** to save the settings:



Home > Resource groups > ContosoRSVRG > ContosoRSV > Enable replication > Source

Enable replication
ContosoRSV

1 Source
Configure

2 Virtual machines
Select

3 Replication settings
Configure replication settings

Source
ContosoRSV

Select your source environment

Source: Azure

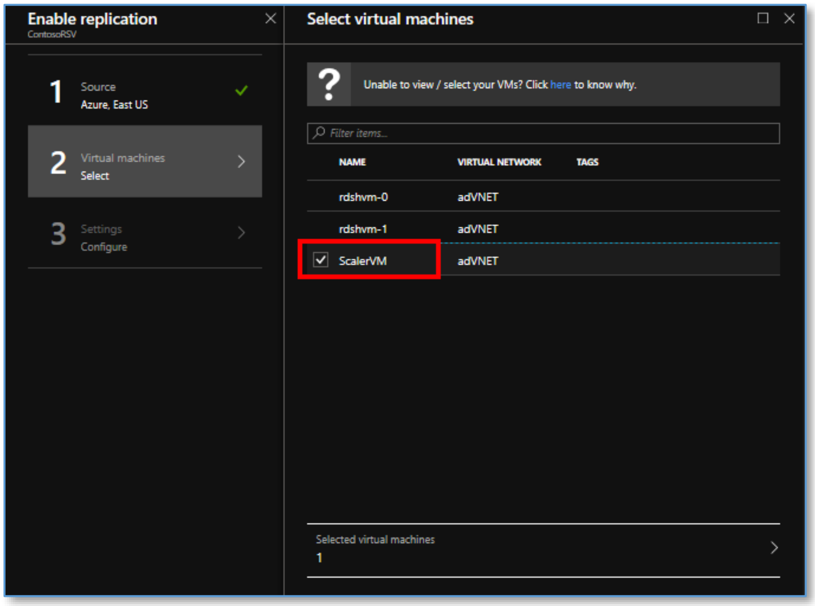
* Source location: East US

* Azure virtual machine deployment model: Resource Manager

* Source subscription: Contoso Subscription

* Source resource group: RG-ContosoWVD

3. Site Recovery retrieves a list of the VMs associated with the subscription and resource group. In **Virtual Machines**, select any of the VMs to replicate. We'll select our ScalerVM:



Enable replication
ContosoRSV

1 Source
Azure, East US ✓

2 Virtual machines
Select

3 Settings
Configure

Select virtual machines

Unable to view / select your VMs? Click here to know why.

Filter items...

	NAME	VIRTUAL NETWORK	TAGS
	rdshvm-0	adVNET	
	rdshvm-1	adVNET	
☑	ScalerVM	adVNET	

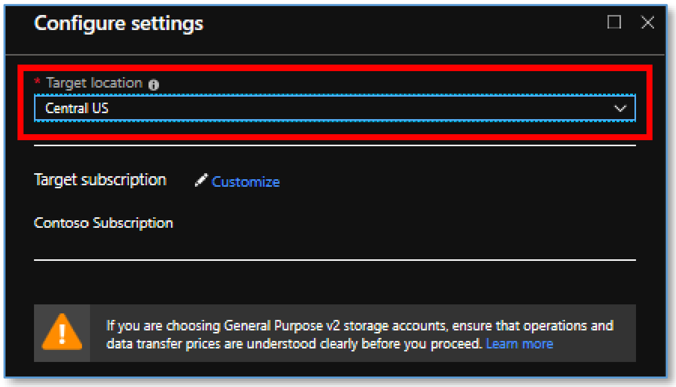
Selected virtual machines
1

4. Click **OK**.

Configure replication settings

Site Recovery creates a default settings and replication policy for the target region. You can change the settings as required.

1. Click **Settings** to view the target and replication settings. Change the **Target location** to your remote region. We're using **Central US** for this walkthrough:



Configure settings

* Target location

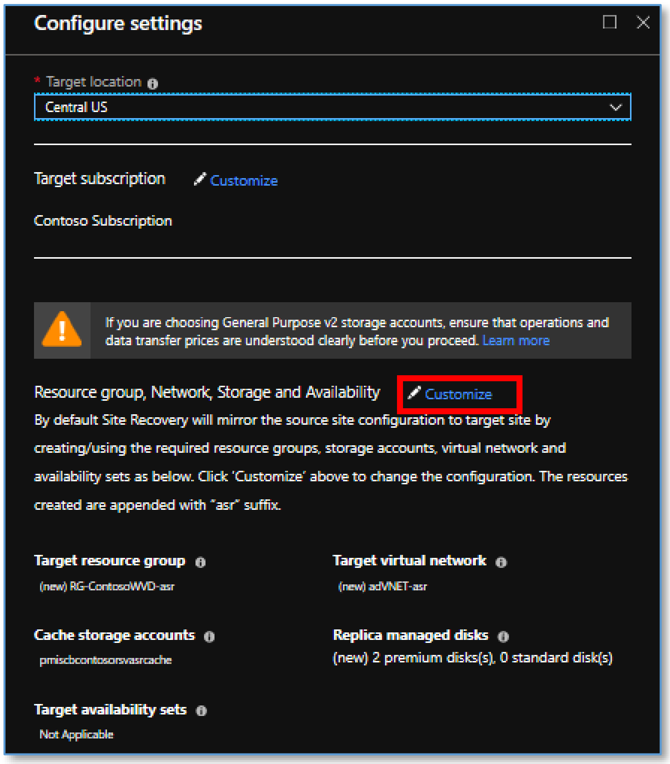
Central US

Target subscription ✎ Customize

Contoso Subscription

If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. Learn more

2. Click the **Customize** link shown below, to change the default settings:



Configure settings

* Target location

Central US

Target subscription ✎ Customize

Contoso Subscription

If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. Learn more

Resource group, Network, Storage and Availability ✎ Customize

By default Site Recovery will mirror the source site configuration to target site by creating/using the required resource groups, storage accounts, virtual network and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

Target resource group
(new) RG-ContosoWVD-asr

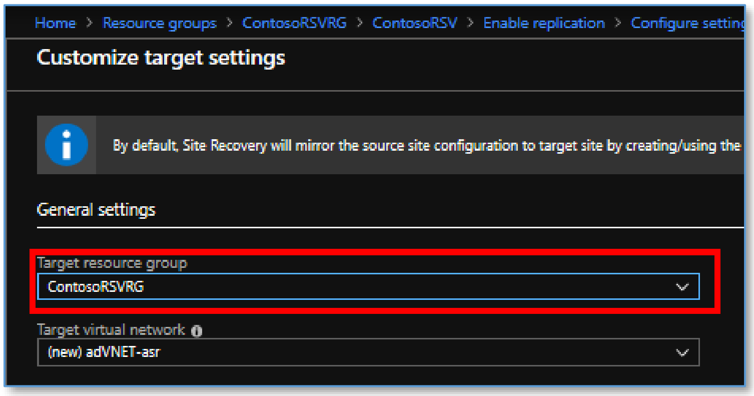
Target virtual network
(new) adVNET-asr

Cache storage accounts
pmiscbcontosorsvasrcache

Replica managed disks
(new) 2 premium disks(s), 0 standard disk(s)

Target availability sets
Not Applicable

3. Change the **Target resource group** to the resource group in the target region that holds Azure VMs after failover. This is the resource group we created earlier, where we located the Recovery Services vault. We're using **ContosoRSVRG** in this walkthrough:



Home > Resource groups > ContosoRSVRG > ContosoRSV > Enable replication > Configure setting

Customize target settings

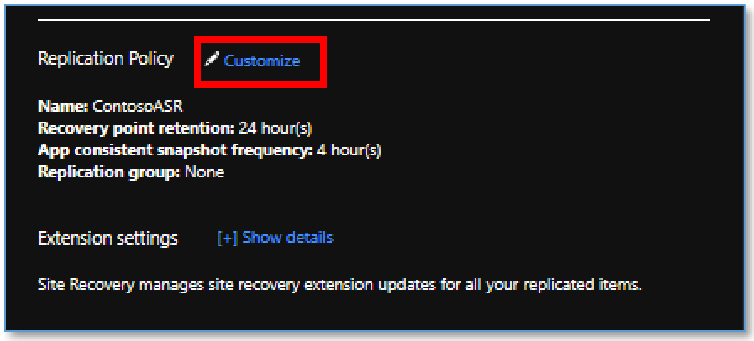
By default, Site Recovery will mirror the source site configuration to target site by creating/using the

General settings

Target resource group: ContosoRSVRG

Target virtual network: (new) adVNET-asr

4. To customize replication policy settings, click **Customize** next to **Replication policy**:



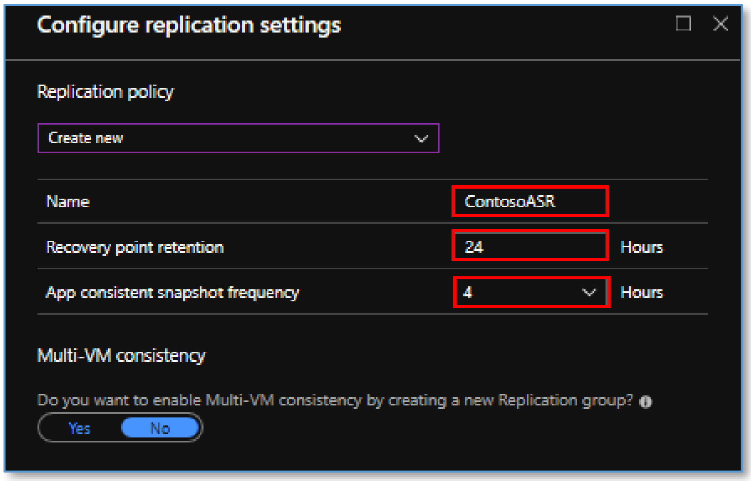
Replication Policy

Name: ContosoASR
Recovery point retention: 24 hour(s)
App consistent snapshot frequency: 4 hour(s)
Replication group: None

Extension settings [+] Show details

Site Recovery manages site recovery extension updates for all your replicated items.

- **Name** = Replication Policy name. We're using **ContosoASR**
- **Recovery point retention** & **snapshot frequency,** we left at their defaults.



Configure replication settings

Replication policy: Create new

Name: ContosoASR

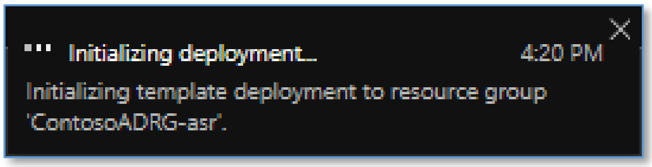
Recovery point retention: 24 Hours

App consistent snapshot frequency: 4 Hours

Multi-VM consistency

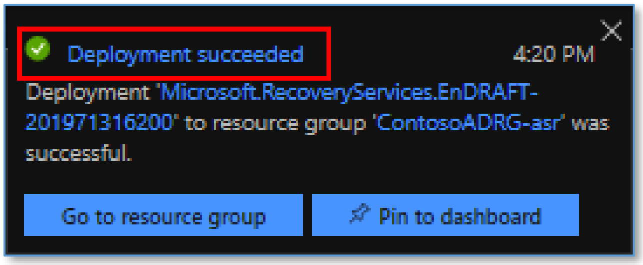
Do you want to enable Multi-VM consistency by creating a new Replication group? Yes [✓ No]

5. Click **OK** & **Create target resources** buttons, & Azure deploys any new resources required:



Initializing deployment... 4:20 PM

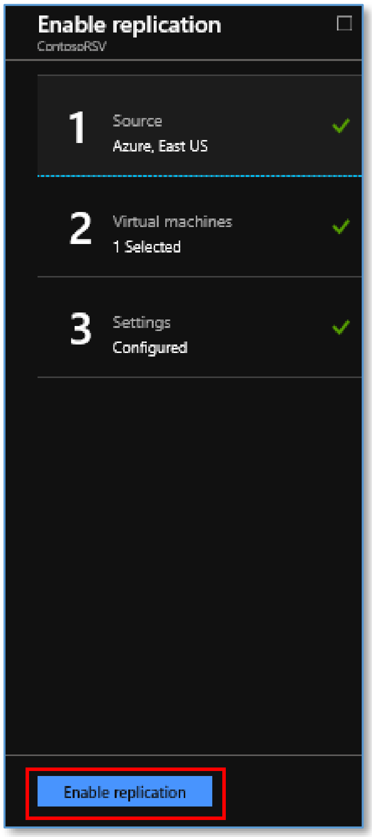
Initializing template deployment to resource group 'ContosoADRG-asr'.



Deployment succeeded 4:20 PM

Deployment 'Microsoft.RecoveryServices.EnDRAFT-201971316200' to resource group 'ContosoADRG-asr' was successful.

6. Finally, click the **Enable Replication** button to begin replication.



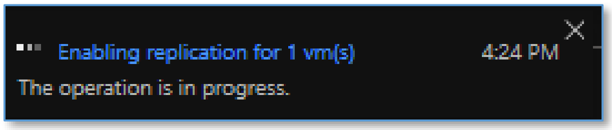
Enable replication

ContosoRSV

1 Source: Azure, East US ✓

2 Virtual machines: 1 Selected ✓

3 Settings: Configured ✓

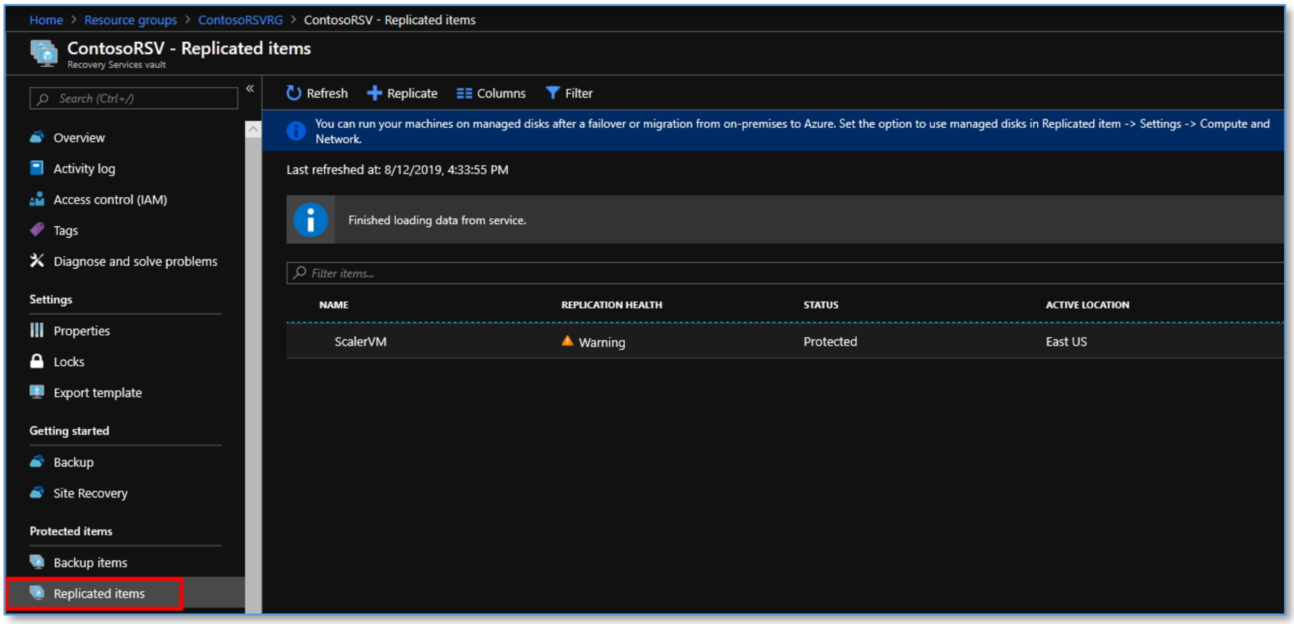


Enabling replication for 1 vm(s) 4:24 PM

The operation is in progress.

Track replication status

1. In **Protected items**, click **Replicated items** to see the list of backed-up VMs:



ContosoRSV - Replicated items
Recovery Services vault

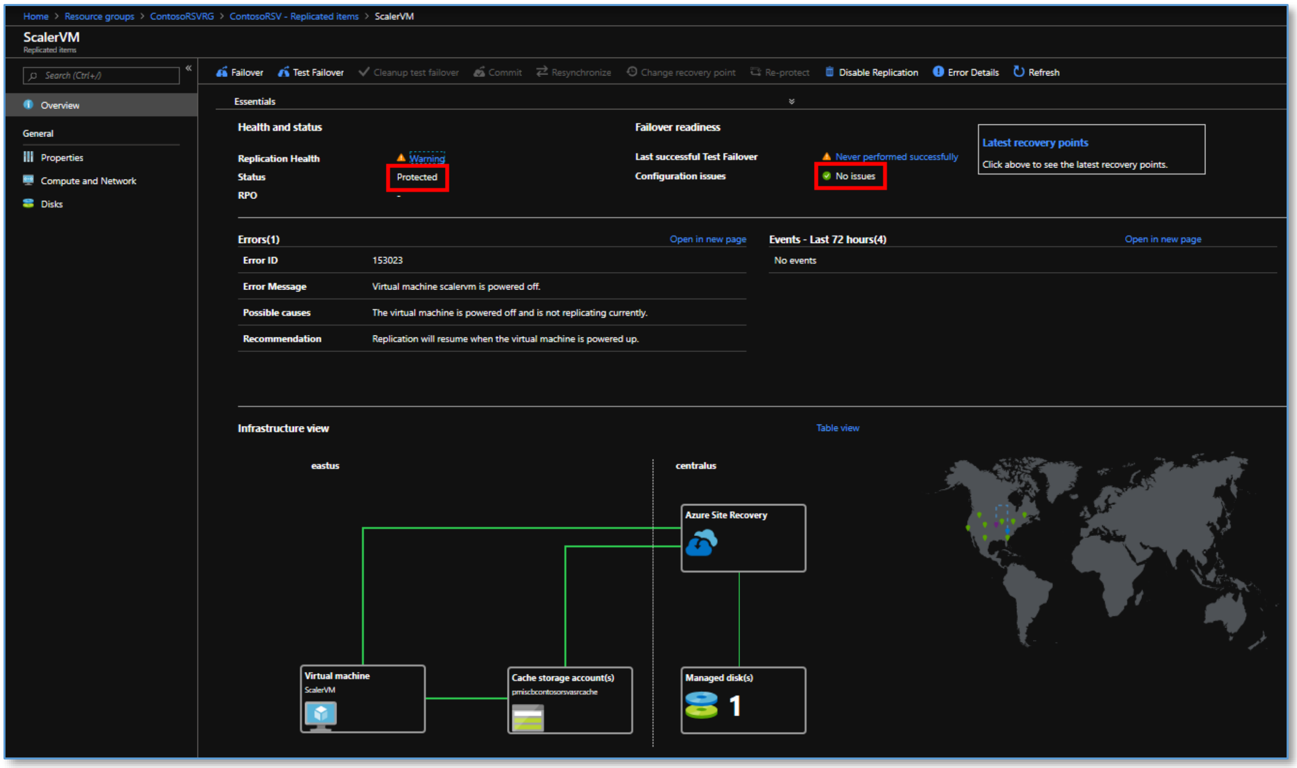
You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 8/12/2019, 4:33:55 PM

Finished loading data from service.

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
ScalerVM	⚠ Warning	Protected	East US

2. Click on of the VMs in the list to see current replication status:



ScalerVM
Replicated items

Essentials

Health and status

Replication Health	⚠ Warning
Status	Protected
RPO	-

Failover readiness

Last successful Test Failover	⚠ Never performed successfully
Configuration issues	✓ No issues

Latest recovery points
Click above to see the latest recovery points.

Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

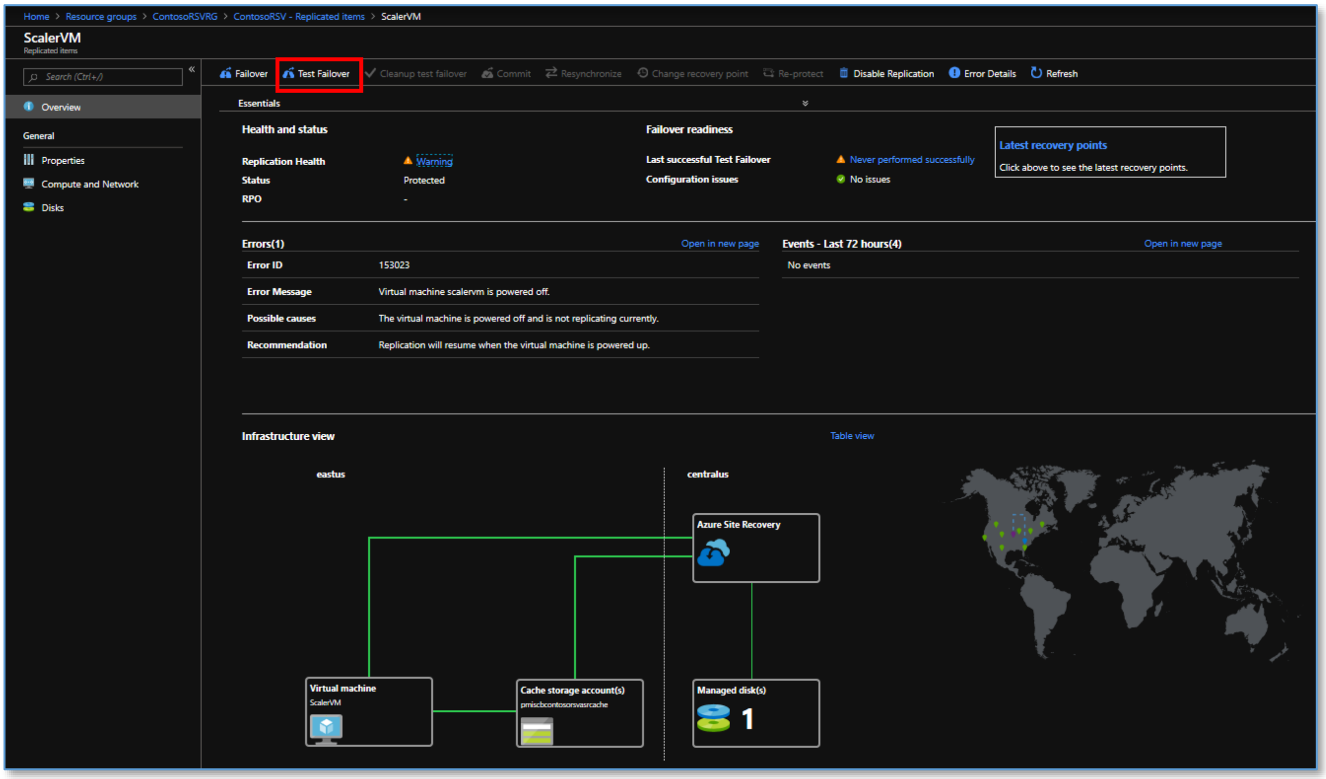
Events - Last 72 hours(4)

No events

3. Run a Disaster Recovery Drill

This section shows you how to run a disaster recovery drill for an Azure VM, from one Azure region to another, with a test failover. A drill validates your replication strategy without data loss or downtime and doesn't affect your production environment.

1. In **Protected items**, click **Replicated items,** then click on a VM we'll fail over *from*. We're using our **ScalerVM** for the walkthrough:



Health and status

Replication Health: Warning
Status: Protected
RPO: -

Failover readiness

Last successful Test Failover: Never performed successfully
Configuration issues: No issues

Latest recovery points
Click above to see the latest recovery points.

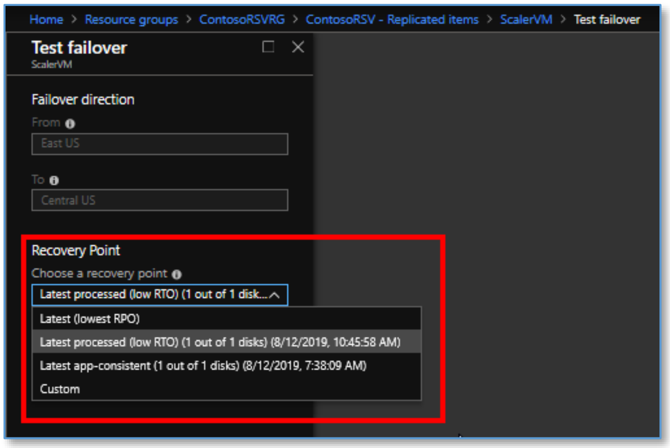
Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

Events - Last 72 hours(4)

No events

2. In **Test Failover**, Select a recovery point to use for the failover. We're selecting **Latest processed** fails the VM over to the latest successful recovery point:


Home > Resource groups > ContosoRSVRG > ContosoRSV - Replicated items > ScalerVM > Test failover
Test failover
ScalerVM
Failover direction
Recovery Point

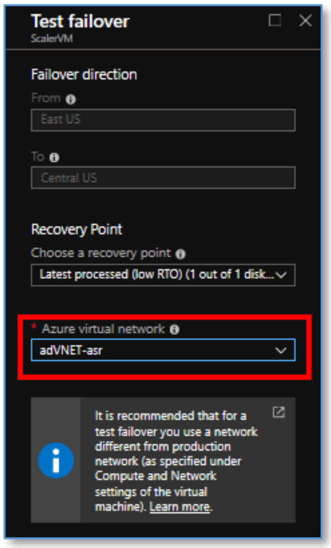
From: East US

To: Central US

Choose a recovery point: Latest processed (low RTO) (1 out of 1 disk...

- Latest (lowest RPO)
- Latest processed (low RTO) (1 out of 1 disks) (8/12/2019, 10:45:58 AM)
- Latest app-consistent (1 out of 1 disks) (8/12/2019, 7:38:09 AM)
- Custom

3. Select the target Azure virtual network to which Azure VMs in the secondary region will be connected, after the failover occurs:



Failover direction

From: East US

To: Central US

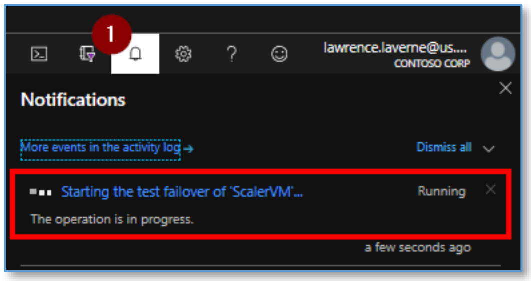
Recovery Point

Choose a recovery point: Latest processed (low RTO) (1 out of 1 disk...

* Azure virtual network: adVNET-asr

It is recommended that for a test failover you use a network different from production network (as specified under Compute and Network settings of the virtual machine). Learn more.

4. To start the failover, click **OK**. To track progress, click the notifications icon:

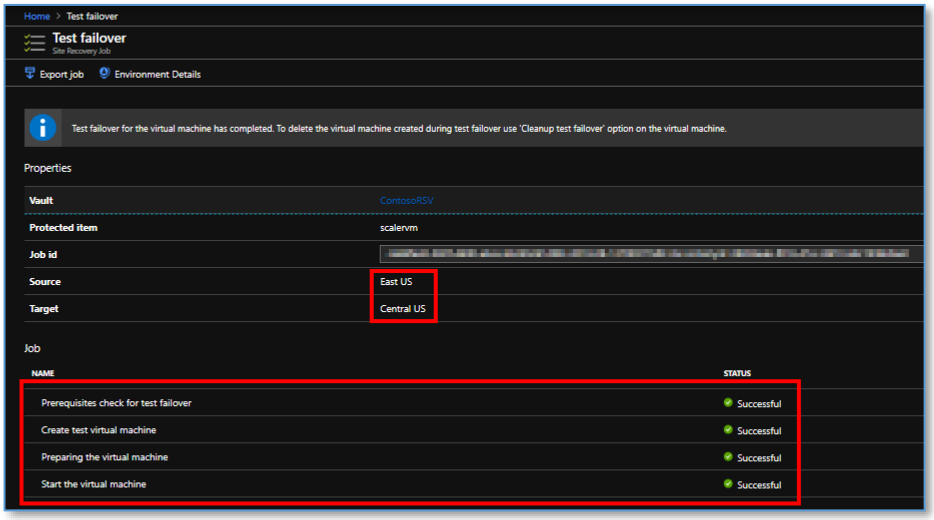


Starting the test failover of 'ScalerVM'... Running

The operation is in progress.

a few seconds ago

5. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Click it to see the fail-over progression:



Test failover for the virtual machine has completed. To delete the virtual machine created during test failover use 'Cleanup test failover' option on the virtual machine.

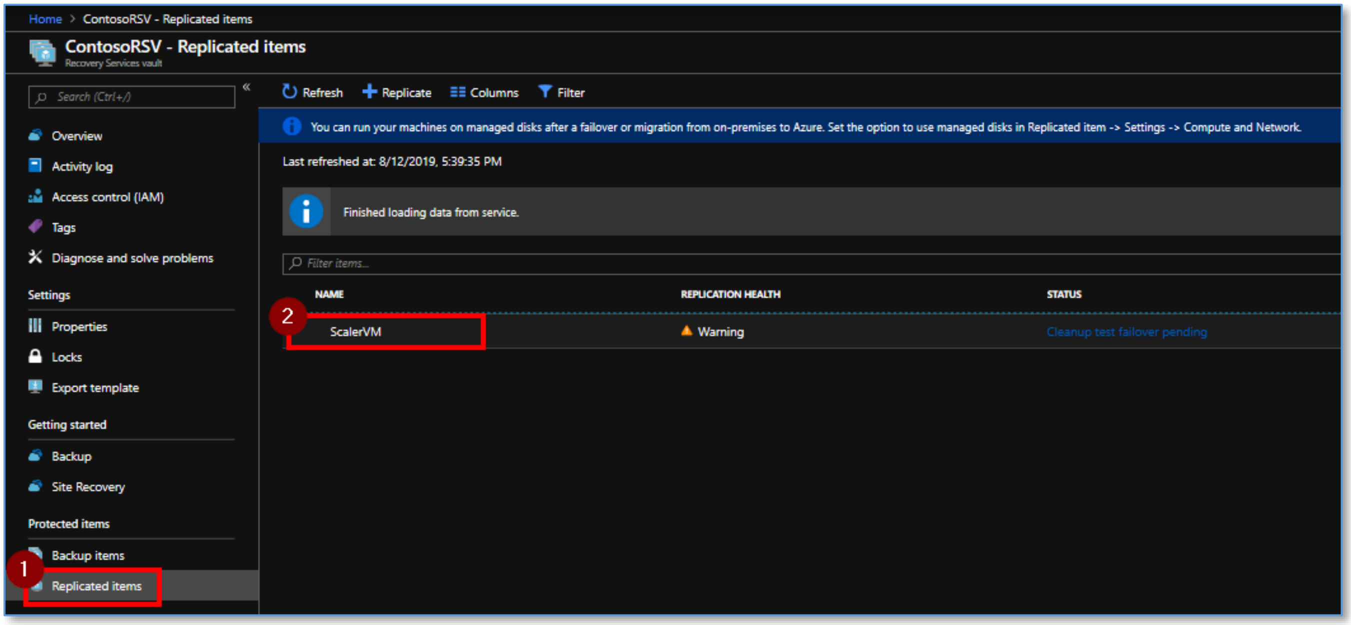
Properties

Vault	ContosoRSV
Protected item	scalervm
Job id	[redacted]
Source	East US
Target	Central US

Job

NAME	STATUS
Prerequisites check for test failover	✓ Successful
Create test virtual machine	✓ Successful
Preparing the virtual machine	✓ Successful
Start the virtual machine	✓ Successful

6. To delete the VM(s) that were created during the test failover, click on the replicated VM:



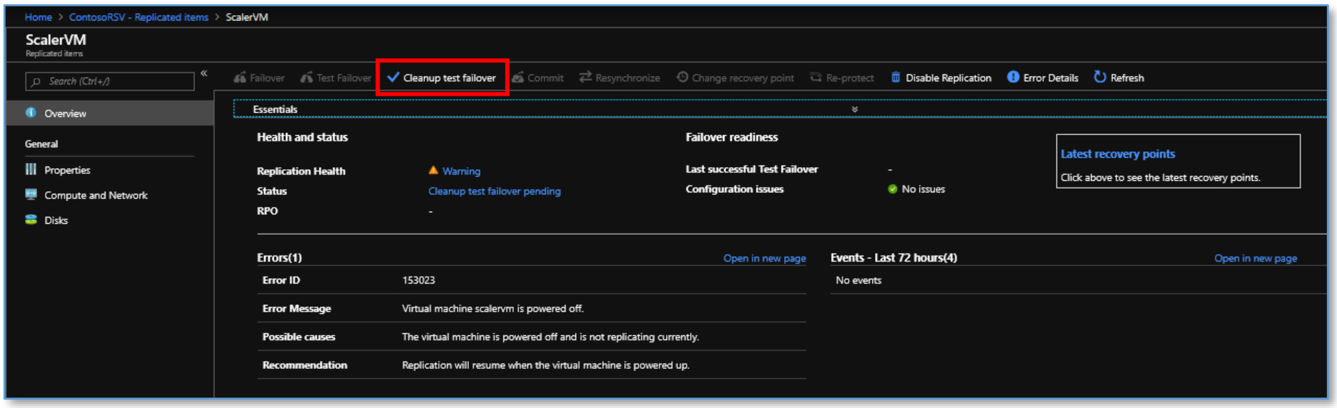
You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 8/12/2019, 5:39:35 PM

Finished loading data from service.

NAME	REPLICATION HEALTH	STATUS
ScalerVM	⚠ Warning	Cleanup test failover pending

7. Then click on **Cleanup test failover**:



Health and status

Replication Health: ⚠ Warning
Status: Cleanup test failover pending
RPO: -

Failover readiness

Last successful Test Failover: -
Configuration issues: ● No issues

Latest recovery points
Click above to see the latest recovery points.

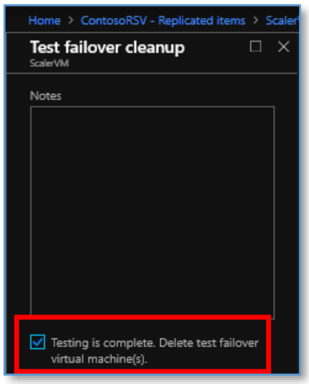
Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

Events - Last 72 hours(4)

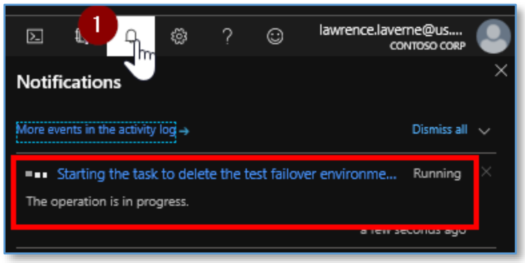
No events

8. Check the **Testing is complete…** box, and click **OK**:



☑ Testing is complete. Delete test failover virtual machine(s).

9. Verify that the deletion is in progress by clicking the Notification icon:



Starting the task to delete the test failover environme... Running

The operation is in progress.

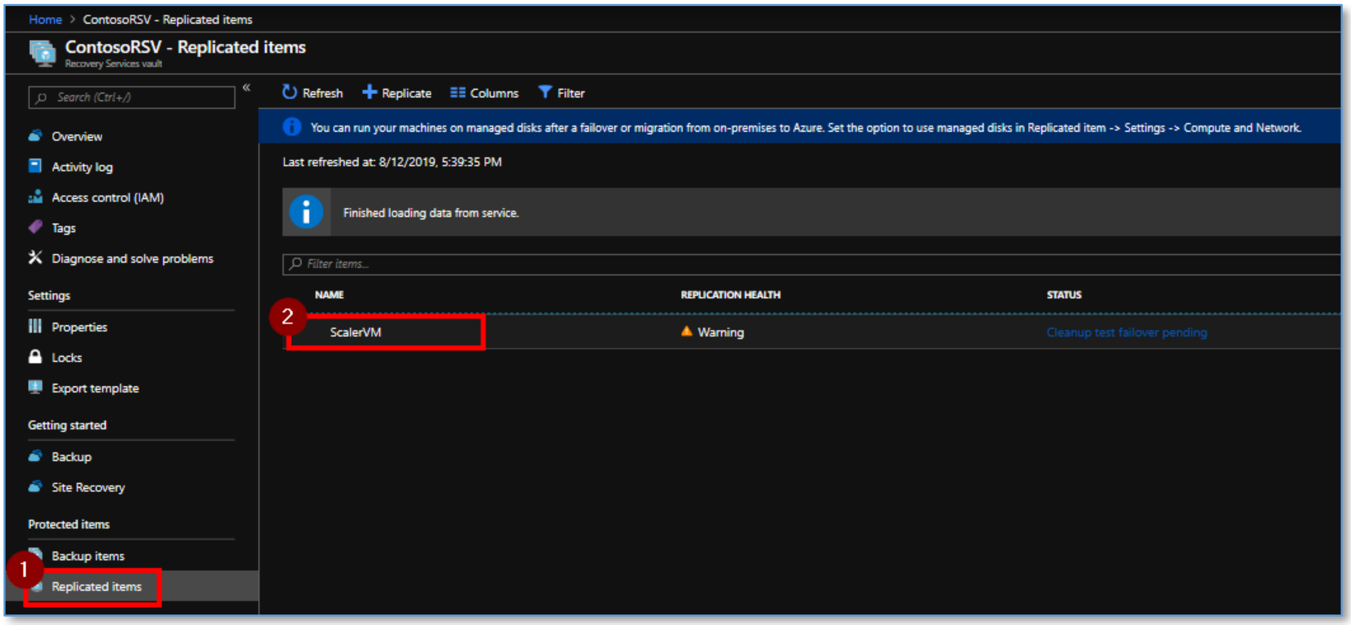
a few seconds ago

4. Fail-over and re-protect Azure VMs between Regions

This section describes how to fail over an Azure virtual machine (VM) to a secondary Azure region with the Azure Site Recovery service. After you've failed over, you'll re-protect the VM so that it replicates to the primary region.

Run a failover to the secondary region

1. In **Replicated items**, select the VM that you want to fail over & click **Failover**:

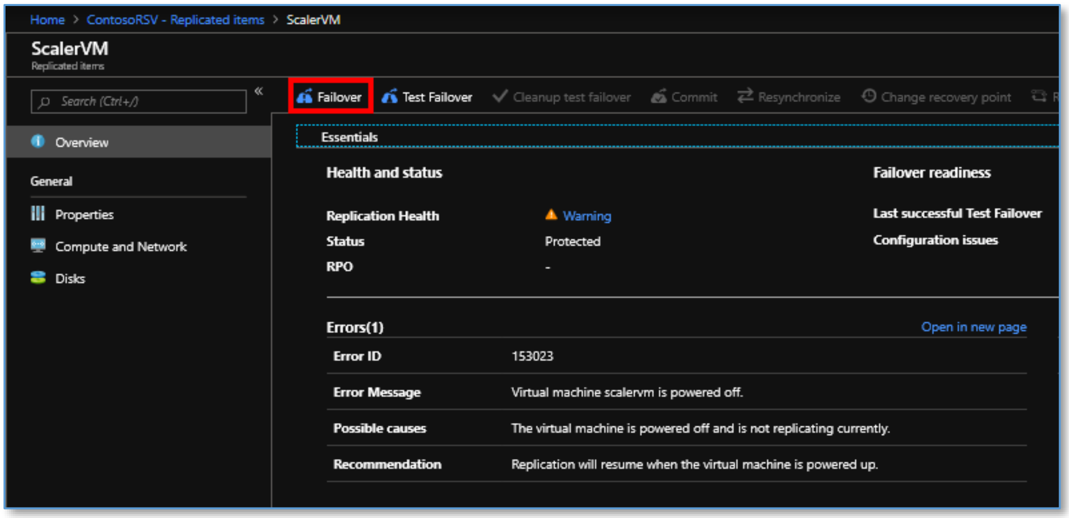


You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 8/12/2019, 5:39:35 PM

Finished loading data from service.

NAME	REPLICATION HEALTH	STATUS
ScalerVM	⚠ Warning	Cleanup test failover pending



Health and status

Replication Health: Warning
Status: Protected
RPO: -

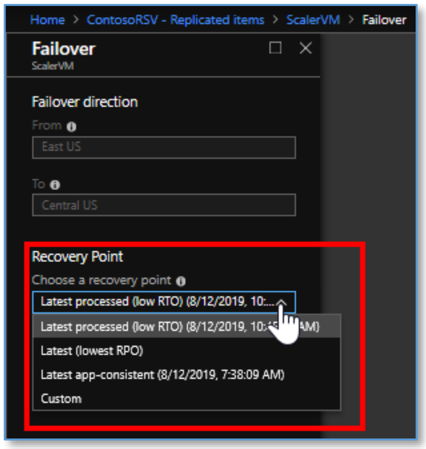
Failover readiness

Last successful Test Failover
Configuration issues

Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

2. In **Failover**, select a **Recovery Point** to fail over to. We're selecting **Latest processed**:


Home > ContosoRSV - Replicated items > ScalerVM > Failover
Failover
ScalerVM

Failover direction

From: East US

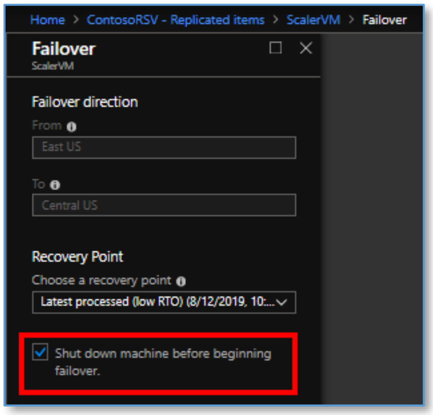
To: Central US

Recovery Point

Choose a recovery point: Latest processed (low RTO) (8/12/2019, 10:...

Latest processed (low RTO) (8/12/2019, 10:... AM)
Latest (lowest RPO)
Latest app-consistent (8/12/2019, 7:38:09 AM)
Custom

3. Select **Shut down machine before beginning failover** if you want Site Recovery to attempt to do a shutdown of source VMs before triggering the failover. Failover continues even if shutdown fails. Site Recovery does not clean up the source after failover:



Failover direction

From: East US

To: Central US

Recovery Point

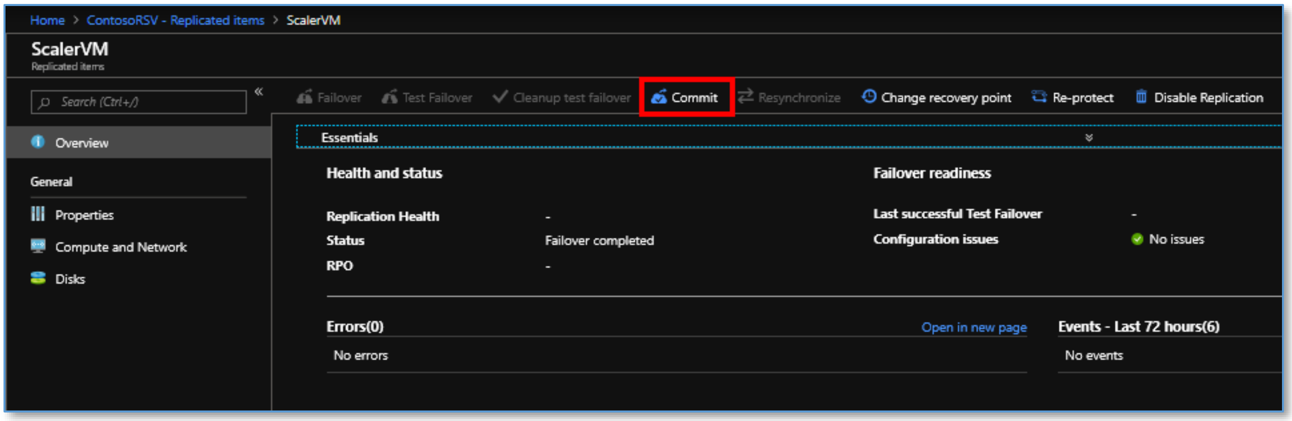
Choose a recovery point: Latest processed (low RTO) (8/12/2019, 10:...

☑ Shut down machine before beginning failover.

4. Click **OK**, and follow the failover progress on the **Jobs** page.

5. After the failover, you can validate the virtual machine by logging in to it. If you want to use another recovery point for the virtual machine, then you can use the **Change recovery point** option.

6. Once you are satisfied validating the failed over virtual machine, you can **Commit** the failover. Committing deletes all the recovery points available with the service. You won't be able to change the recovery point afterward.



Health and status

Replication Health -
Status Failover completed
RPO -

Failover readiness

Last successful Test Failover -
Configuration issues ✓ No issues

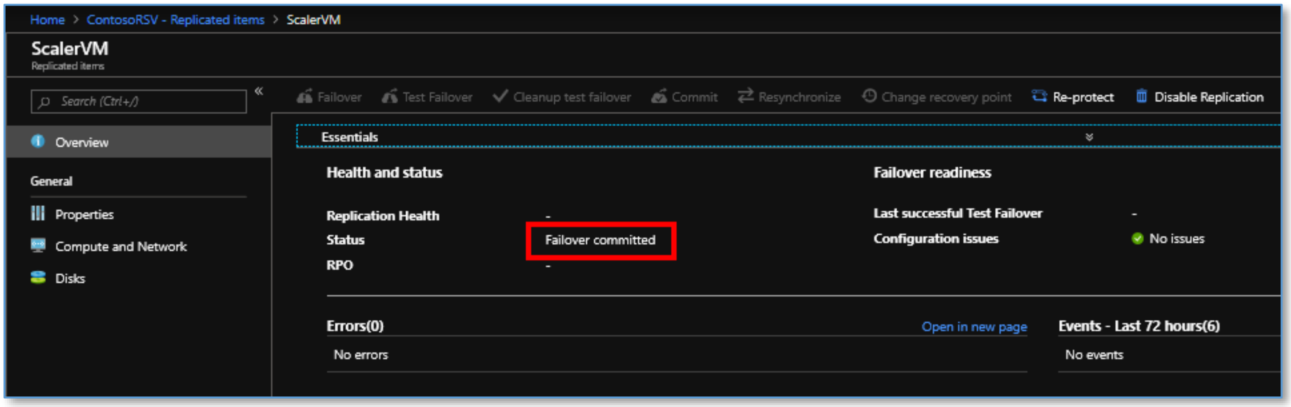
Errors(0)
No errors

Events - Last 72 hours(6)
No events

Re-protect the Secondary VM

After failover of the VM, you need to re-protect it so that it replicates back to the primary region.

1. Make sure that the VM is in the **Failover committed** state:



Health and status

Replication Health -
Status Failover committed
RPO -

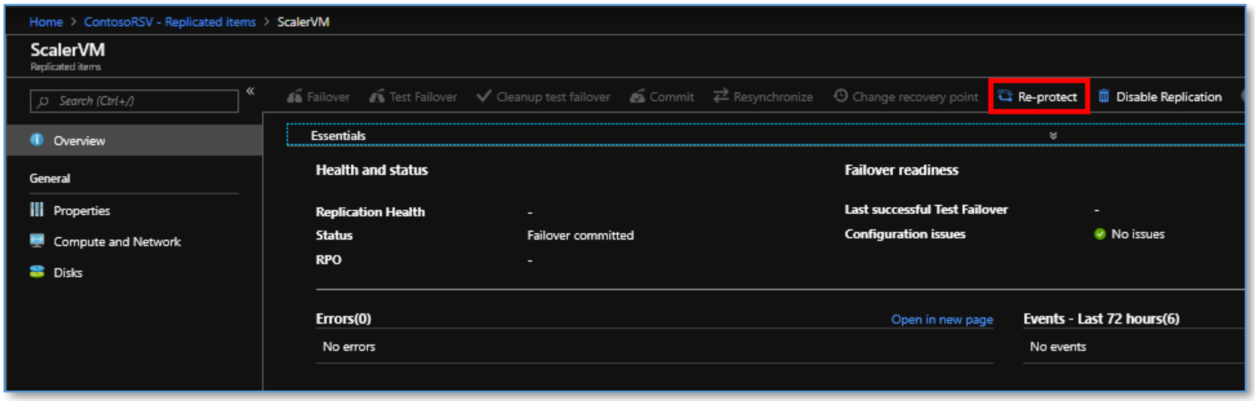
Failover readiness

Last successful Test Failover -
Configuration issues ✓ No issues

Errors(0)
No errors

Events - Last 72 hours(6)
No events

2. Click **Re-Protect**.



Health and status

Replication Health -
Status Failover committed
RPO -

Failover readiness

Last successful Test Failover -
Configuration issues No issues

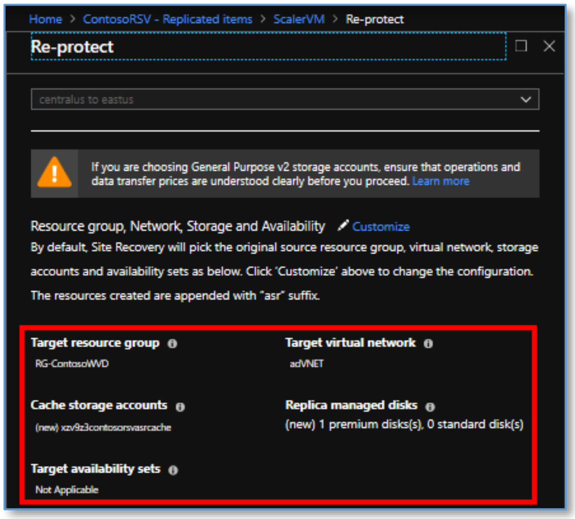
Errors(0)

No errors

Events - Last 72 hours(6)

No events

1. The direction of protection, secondary to primary region, is already selected. Review the **Resource group, Network, Storage, and Availability sets** information. Any resources marked as new are created as part of the re-protect operation.


Home > ContosoRSV - Replicated items > ScalerVM > Re-protect
Re-protect
Customize

centralus to eastus

If you are choosing General Purpose v2 storage accounts, ensure that operations and data transfer prices are understood clearly before you proceed. Learn more

Resource group, Network, Storage and Availability

By default, Site Recovery will pick the original source resource group, virtual network, storage accounts and availability sets as below. Click 'Customize' above to change the configuration. The resources created are appended with "asr" suffix.

Target resource group
RG-ContosoWVD

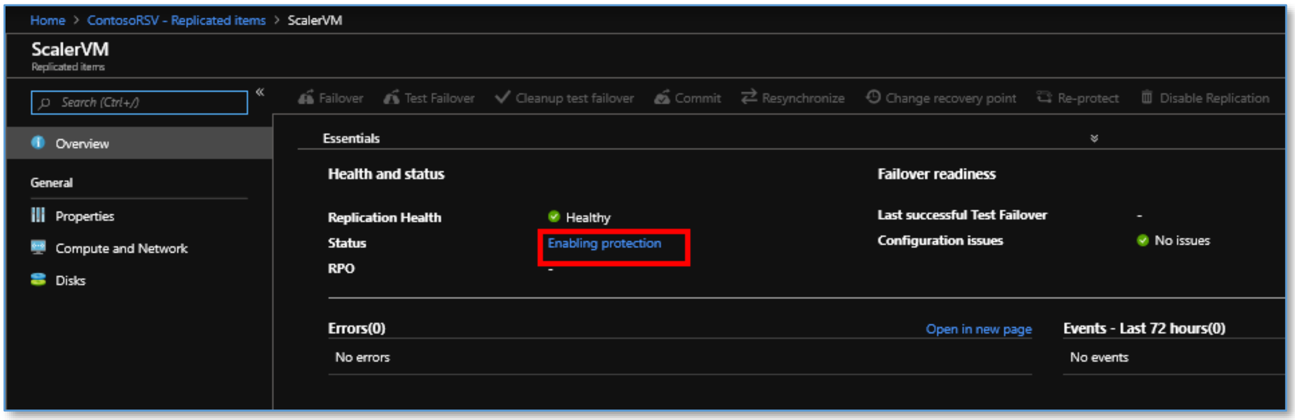
Target virtual network
adVNET

Cache storage accounts
(new) xzv9z3contosorsvasrcache

Replica managed disks
(new) 1 premium disks(s), 0 standard disk(s)

Target availability sets
Not Applicable

2. Click **OK** to trigger a re-protect job:



Health and status

Replication Health Healthy
Status Enabling protection
RPO -

Failover readiness

Last successful Test Failover -
Configuration issues No issues

Errors(0)

No errors

Events - Last 72 hours(0)

No events

Integrating a failed-over WVD VM into a secondary host pool

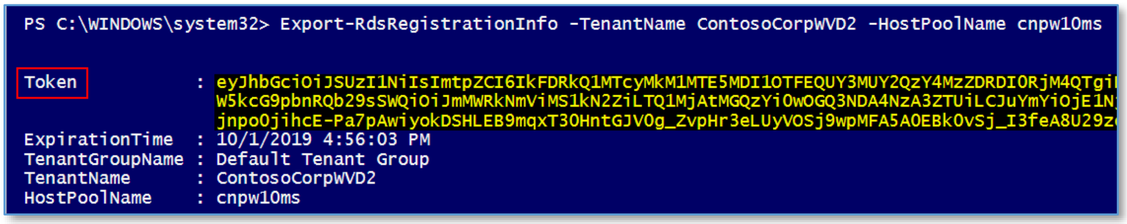
When you are failing-over a WVD VM from one host pool to another, the VM must be re-tokenized. Re-tokenizing means to add a registration token of the target host pool to the VM.

1. Set the registration token for the target host pool. Our example uses the parameters below:

```
New-RdsRegistrationInfo -TenantName ContosoCorpWVD2 `
-HostPoolName cnpw10ms -ExpirationHours 48
```

2. Get the Registration **Token** of the target host pool:

```
Export-RdsRegistrationInfo -TenantName ContosoCorpWVD2 `
-HostPoolName cnpw10ms
```

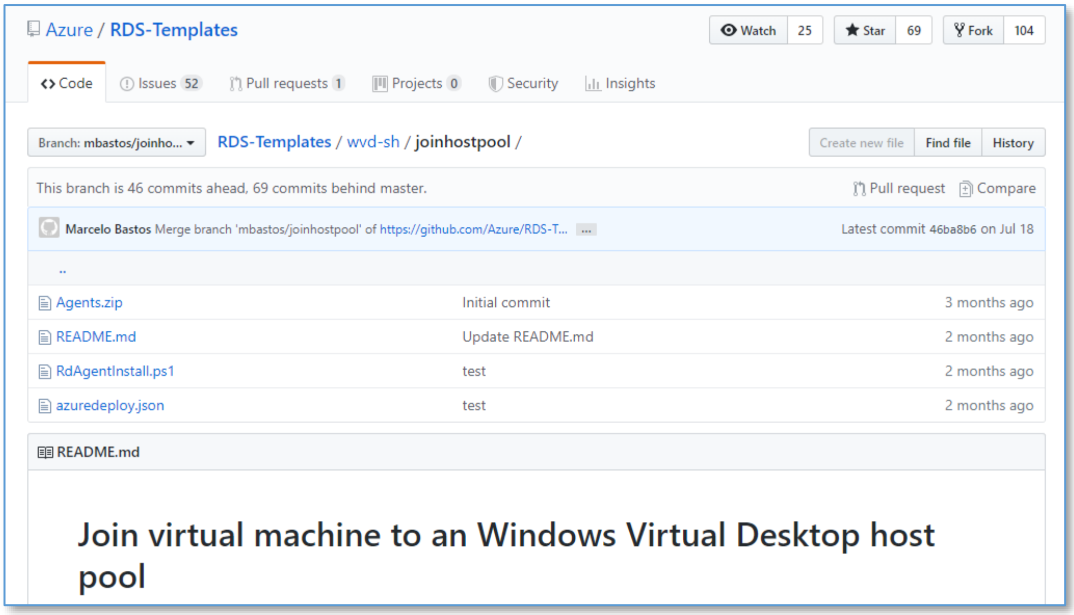


```
PS C:\WINDOWS\system32> Export-RdsRegistrationInfo -TenantName ContosoCorpWVD2 -HostPoolName cnpw10ms

Token          : eyJhbGciOiJSUzI1NiIsImtpZCI6IkFDRkQ1MTcyMkM1MTE5MDI1OTFEQUY3MUY2QzY4MzZDRDI0RjM4QTgi
                 W5kcG9pbnRQb29sSWQiOiJmMWRkNmViMS1kN2ZiLTQ1MjAtMGQzYi0wOGQ3NDA4NzA3ZTUiLCJuYmYiOjE1N
                 jnpoOjihcE-Pa7pAwiyokDSHLEB9mqxT3OHntGJV0g_ZvpHr3eLUyVOSj9wpMFA5A0EBk0vSj_I3feA8U29z
ExpirationTime : 10/1/2019 4:56:03 PM
TenantGroupName : Default Tenant Group
TenantName     : ContosoCorpWVD2
HostPoolName   : cnpw10ms
```

Copy the highlighted text to Notepad, we'll need it below.

3. Browse to [this ARM Template]() and click **Deploy to Azure** button:



RDS-Templates / wvd-sh / joinhostpool /

This branch is 46 commits ahead, 69 commits behind master.

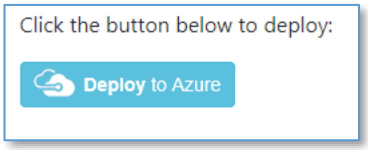
Marcelo Bastos Merge branch 'mbastos/joinhostpool' of https://github.com/Azure/RDS-T... … Latest commit 46ba8b6 on Jul 18

..

Agents.zip	Initial commit	3 months ago
README.md	Update README.md	2 months ago
RdAgentInstall.ps1	test	2 months ago
azuredeploy.json	test	2 months ago

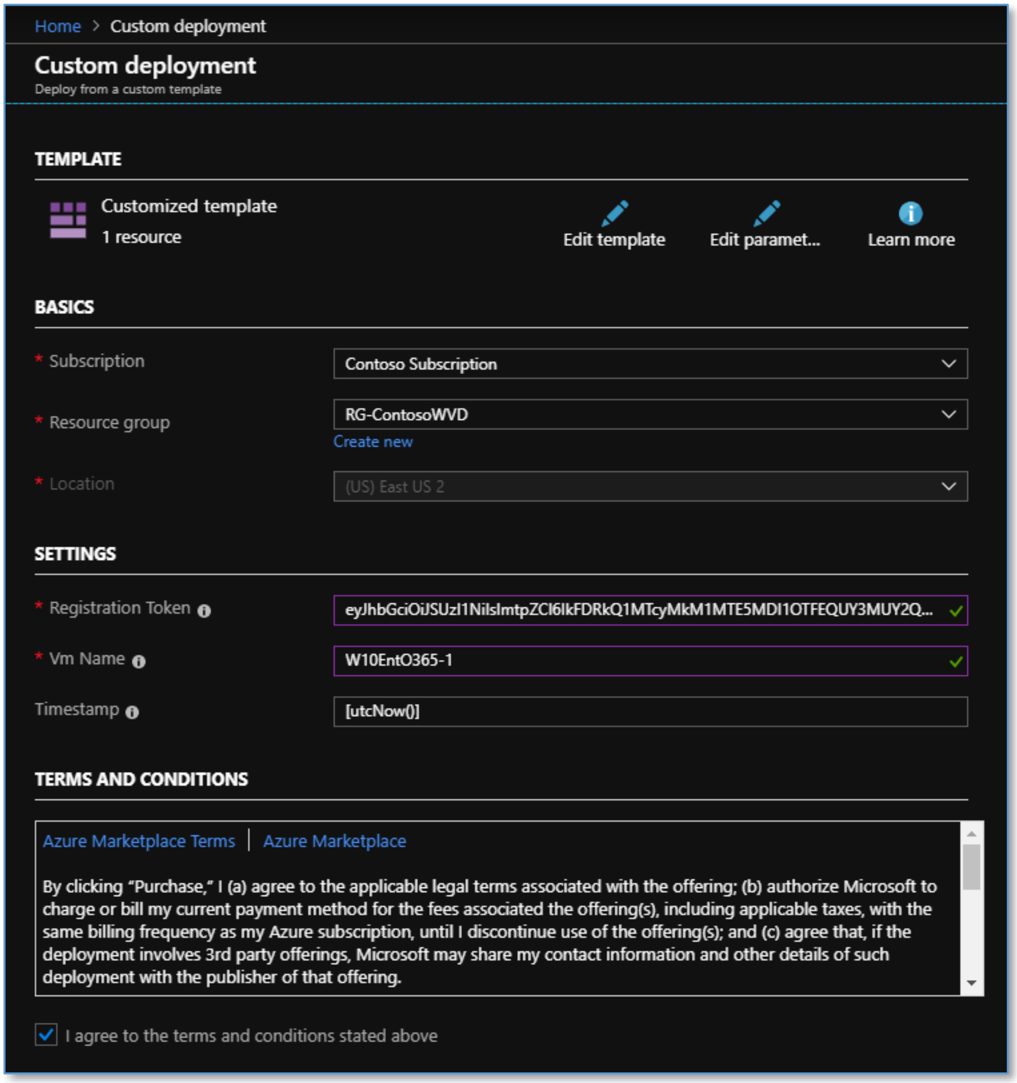
README.md

Join virtual machine to an Windows Virtual Desktop host pool



Click the button below to deploy:

4. Complete the parameters as shown below:



Home > Custom deployment

Custom deployment

Deploy from a custom template

TEMPLATE

Customized template

1 resource

BASICS

* Subscription	Contoso Subscription
* Resource group	RG-ContosoWVD Create new
* Location	(US) East US 2

SETTINGS

* Registration Token	eyJhbGciOiJSUzI1NiIsImtpZCI6IkFDRkQ1MTcyMkM1MTE5MDI1OTFEQUY3MUY2Q... ✓
* Vm Name	W10EntO365-1 ✓
Timestamp	[utcNow()]

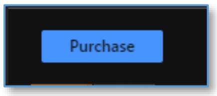
TERMS AND CONDITIONS

Azure Marketplace Terms | Azure Marketplace

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with the publisher of that offering.

☑ I agree to the terms and conditions stated above

5. Click the Purchase button:



The RDS client is deployed and the registration completes.

Fail back an Azure VM between Azure regions

In this section we will fail back a single Azure VM to its primary region. Following the steps below, we will:

- Fail back the VM in the secondary region.

- Re-protect the primary VM back to the secondary region.

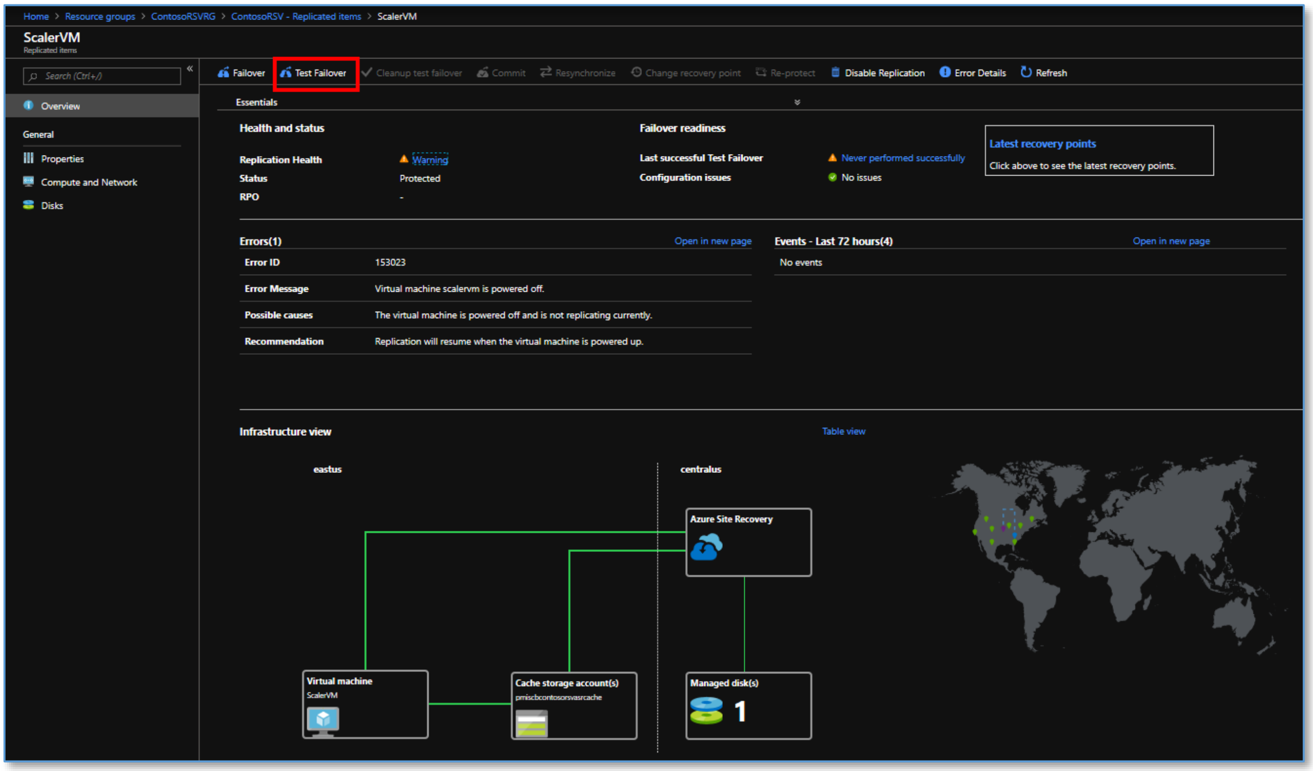
Before starting:

- Make sure that the status of the VM is **Failover committed**.
- Verify that you're able to create and access new resources in the primary region.
- Make sure that re-protection is enabled.

Fail back to the primary region

After VMs are re-protected, you can fail back to the primary region as needed.

1. In the vault, select **Replicated items**, and then select the VM that was re-protected:
2. Click **Test failover** to perform a test failover back to the primary region.



Health and status

Replication Health: Warning
Status: Protected
RPO: -

Failover readiness

Last successful Test Failover: Never performed successfully
Configuration issues: No issues

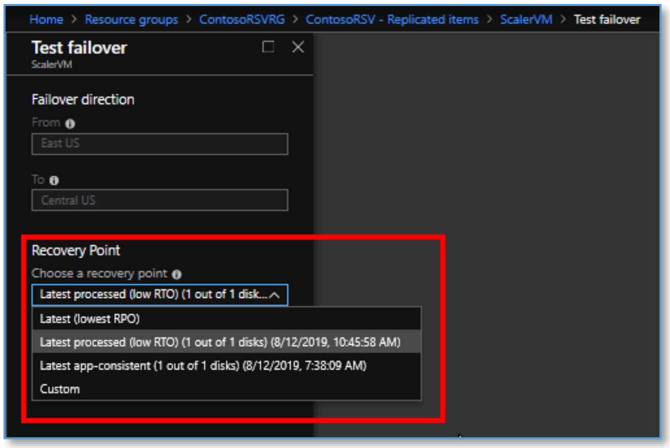
Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

Events - Last 72 hours(4)

No events

1. In **Test Failover**, Select a recovery point to use for the failover. We're selecting **Latest processed** fails the VM over to the latest successful recovery point:


Home > Resource groups > ContosoRSVRG > ContosoRSV - Replicated items > ScalerVM > Test failover

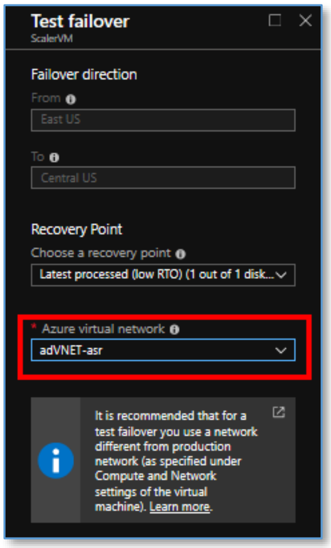
Test failover
ScalerVM

Failover direction
From: East US
To: Central US

Recovery Point
Choose a recovery point: Latest processed (low RTO) (1 out of 1 disk...

- Latest (lowest RPO)
- Latest processed (low RTO) (1 out of 1 disks) (8/12/2019, 10:45:58 AM)
- Latest app-consistent (1 out of 1 disks) (8/12/2019, 7:38:09 AM)
- Custom

2. Select the target Azure virtual network to which Azure VMs in the secondary region will be connected, after the failover occurs:


Test failover
ScalerVM

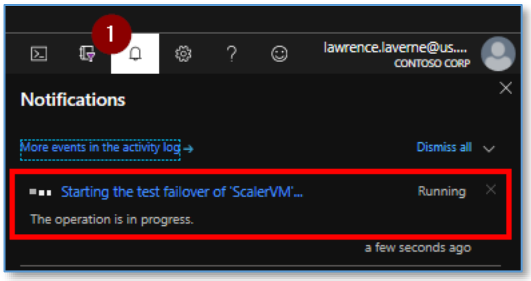
Failover direction
From: East US
To: Central US

Recovery Point
Choose a recovery point: Latest processed (low RTO) (1 out of 1 disk...

* Azure virtual network: adVNET-asr

It is recommended that for a test failover you use a network different from production network (as specified under Compute and Network settings of the virtual machine). Learn more.

3. To start the failover, click **OK**. To track progress, click the notifications icon:



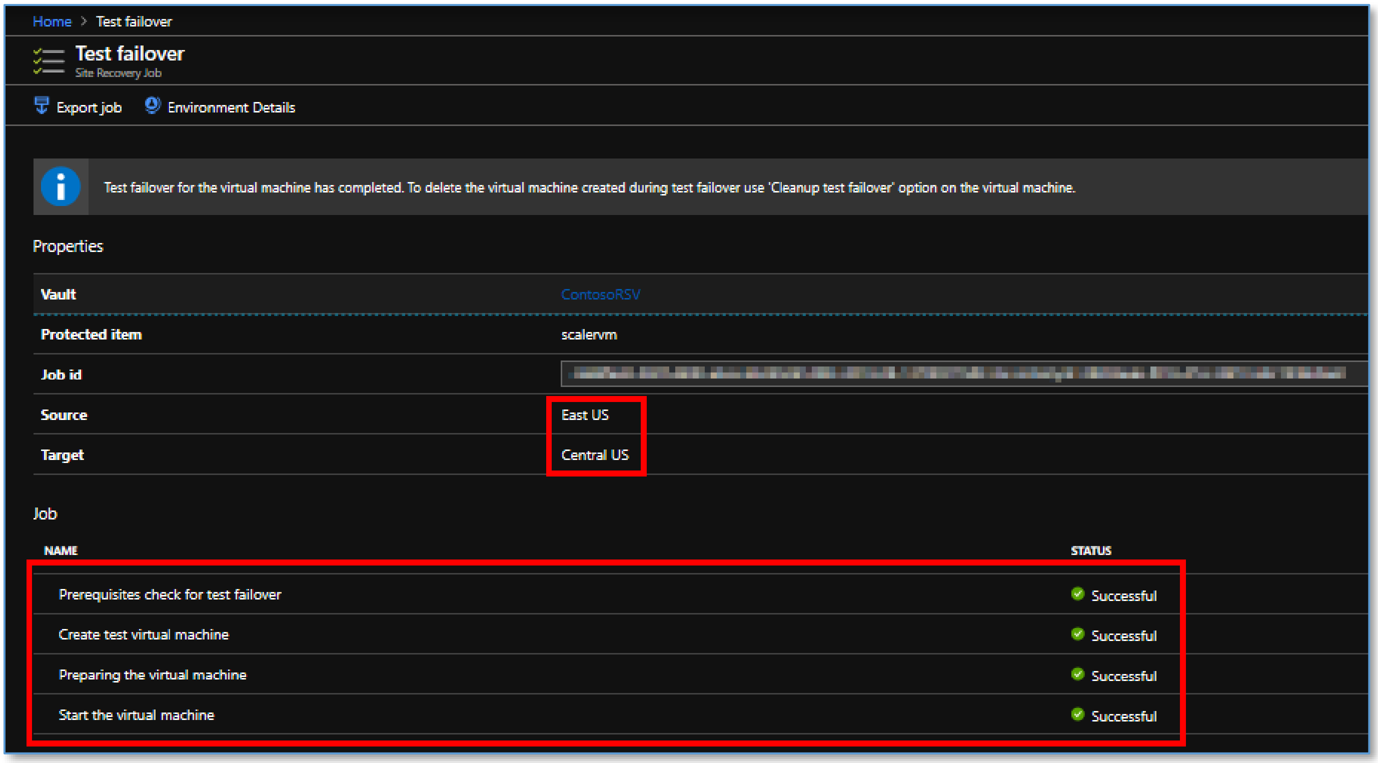
Notifications

More events in the activity log →

Dismiss all

Starting the test failover of 'ScalerVM'... Running
The operation is in progress.
a few seconds ago

4. After the failover finishes, the replica Azure VM appears in the Azure portal > **Virtual Machines**. Click it to see the fail-over progression:



Test failover for the virtual machine has completed. To delete the virtual machine created during test failover use 'Cleanup test failover' option on the virtual machine.

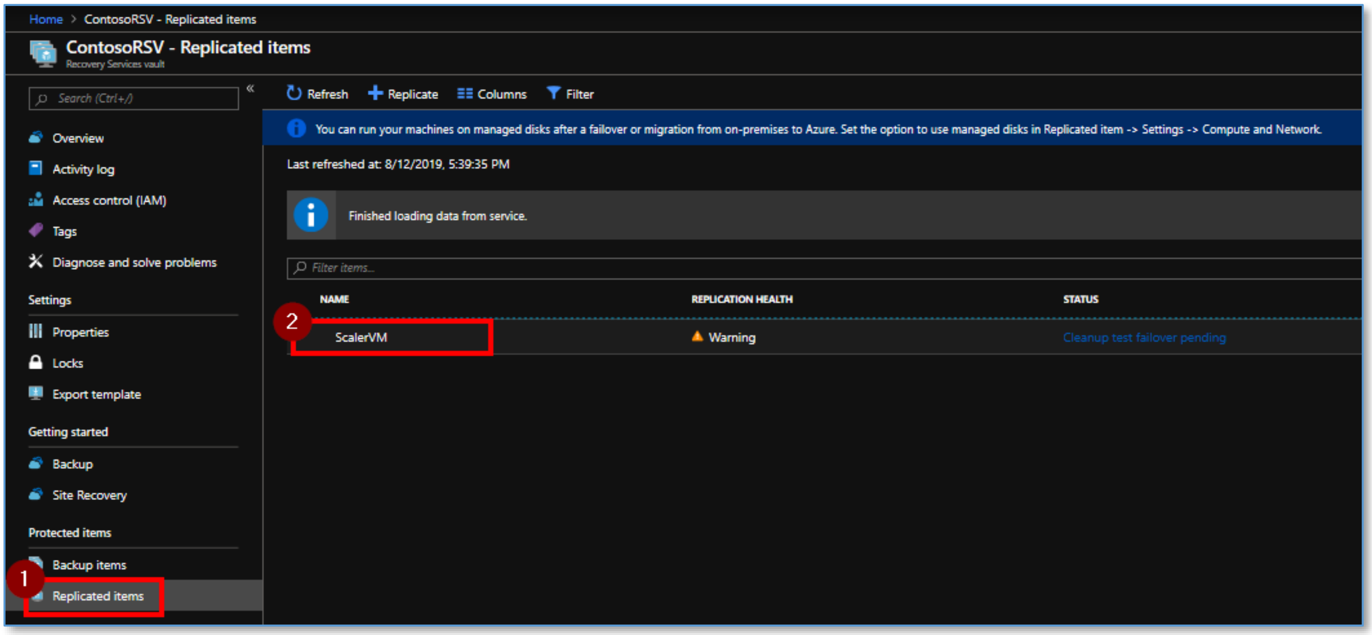
Properties

Vault	ContosoRSV
Protected item	scalervm
Job id	[redacted]
Source	East US
Target	Central US

Job

NAME	STATUS
Prerequisites check for test failover	✓ Successful
Create test virtual machine	✓ Successful
Preparing the virtual machine	✓ Successful
Start the virtual machine	✓ Successful

5. To delete the VM(s) that were created during the test failover, click on the replicated VM:



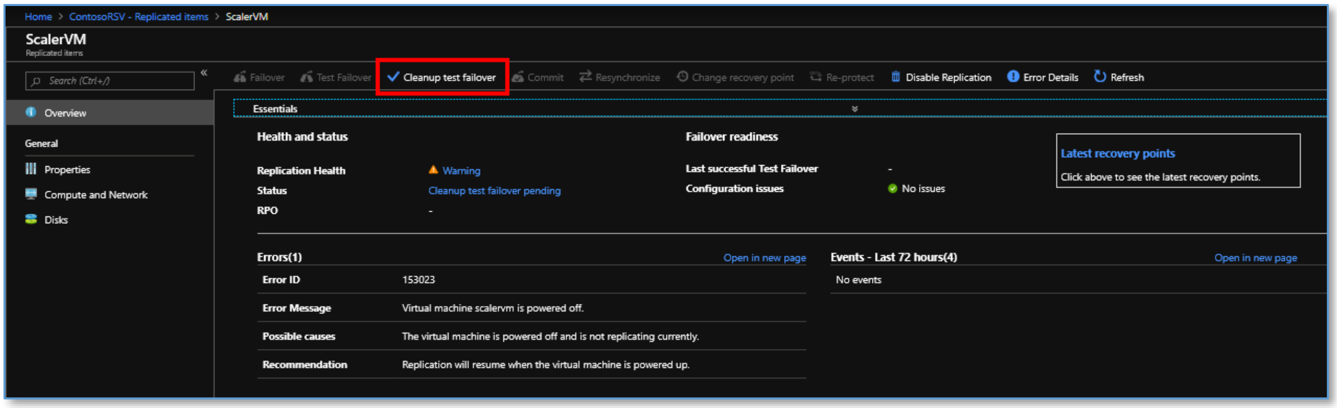
You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the option to use managed disks in Replicated item -> Settings -> Compute and Network.

Last refreshed at: 8/12/2019, 5:39:35 PM

Finished loading data from service.

NAME	REPLICATION HEALTH	STATUS
ScalerVM	⚠ Warning	Cleanup test failover pending

6. Then click on **Cleanup test failover**:



Health and status

Replication Health: Warning
Status: Cleanup test failover pending
RPO: -

Failover readiness

Last successful Test Failover: -
Configuration issues: No issues

Latest recovery points
Click above to see the latest recovery points.

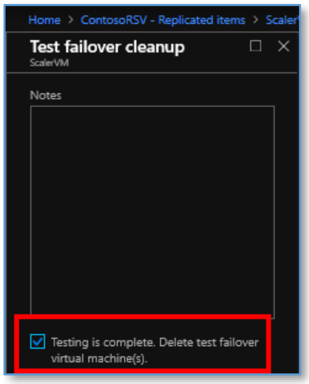
Errors(1)

Error ID	153023
Error Message	Virtual machine scalervm is powered off.
Possible causes	The virtual machine is powered off and is not replicating currently.
Recommendation	Replication will resume when the virtual machine is powered up.

Events - Last 72 hours(4)

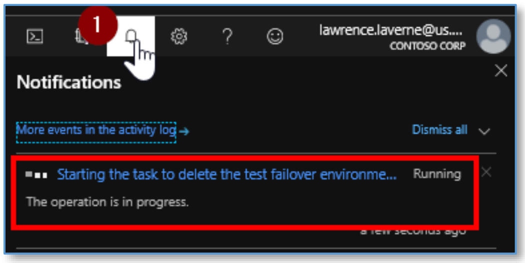
No events

7. Check the **Testing is complete...** box, and click **OK**:



☑ Testing is complete. Delete test failover virtual machine(s).

8. Verify that the deletion is in progress by clicking the Notification icon:



Starting the task to delete the test failover environme... Running
The operation is in progress.
a few seconds ago

Note

The disaster recovery VMs will remain in the shutdown/deallocated state. This is by design because Site Recovery saves the VM information, which might be useful for failover from the primary to the secondary region later. *You aren't charged for the deallocated VMs, so they should be kept as they are.*

5. Support

Opening tickets

In case of an issue for Windows Virtual Desktop go to the Azure Portal and open a technical ticket based on your existing support plan at https://azure.microsoft.com/en-us/support/create-ticket/

Look for Service under **COMPUTE** and select **Windows Virtual Desktop-Preview**. You will find options to create tickets for the WVD service itself and for Office:

For Office issues you can file tickets during public preview in the Azure Portal when using Office in context of Windows Virtual Desktop.

Information you should provide for failed connection or management interactions when using the service:

- Use the diagnostics service to retrieve the **Activity ID** for failed connections or management interactions.
- Provide the approximate timeframe the issue happened

NOTE: This workflow will change post general availability.

Other resources you can leverage

Windows Virtual Desktop contains a number of knowledge articles as well as trouble shooting guides. Pay attention to the updated diagnostics chapter that provides Error scenarios you can mitigate: https://docs.microsoft.com/azure/virtual-desktop/overview

Exchange on our community forum on issues important to you for Windows Virtual Desktop: https://techcommunity.microsoft.com/t5/Windows-Virtual-Desktop/bd-p/WindowsVirtualDesktop

When setting up your environment you will be using other Azure Services. You can watch the health dashboard here to verify health state on any Azure service you are consuming: https://azure.microsoft.com/en-us/status/