


Rehost an on-premises app to Azure VMs

10/11/2018 • 17 minutes to read • Contributors 

In this article

[Business drivers](#)

[Migration goals](#)

[Solution design](#)

[Prerequisites](#)

[Scenario steps](#)

[Step 1: Prepare Azure for the Site Recovery service](#)

[Step 2: Prepare on-premises VMware for Site Recovery](#)

[Step 3: Replicate the on-premises VMs](#)

[Step 4: Migrate the VMs](#)

[Clean up after migration](#)

[Review the deployment](#)

[BCDR](#)

[Conclusion](#)

This article demonstrates how the fictional company Contoso rehosts a two-tier Windows .NET front-end app running on VMware VMs, by migrating the app VMs to Azure VMs.

The SmartHotel360 app used in this example is provided as open source. If you'd like to use it for your own testing purposes, you can download it from [GitHub](#).

Business drivers

The IT Leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing, and as a result there is pressure on their on-premises systems and infrastructure.
- **Limit risk.** The SmartHotel360 app is critical for the Contoso business. It wants to move the app to Azure with zero risk.
- **Extend.** Contoso doesn't want to modify the app, but does want to ensure that it's stable.

Migration goals

The Contoso cloud team has pinned down goals for this migration. These goals are used to determine the best migration method:

- After migration, the app in Azure should have the same performance capabilities as it does today in VMware. The app will remain as critical in the cloud as it is on-premises.
- Contoso doesn't want to invest in this app. It is important to the business, but in its current form Contoso simply wants to move it safely to the cloud.
- Contoso doesn't want to change the ops model for this app. Contoso do want to interact with it in the cloud in the same way that they do now.
- Contoso doesn't want to change any app functionality. Only the app location will change.

Solution design

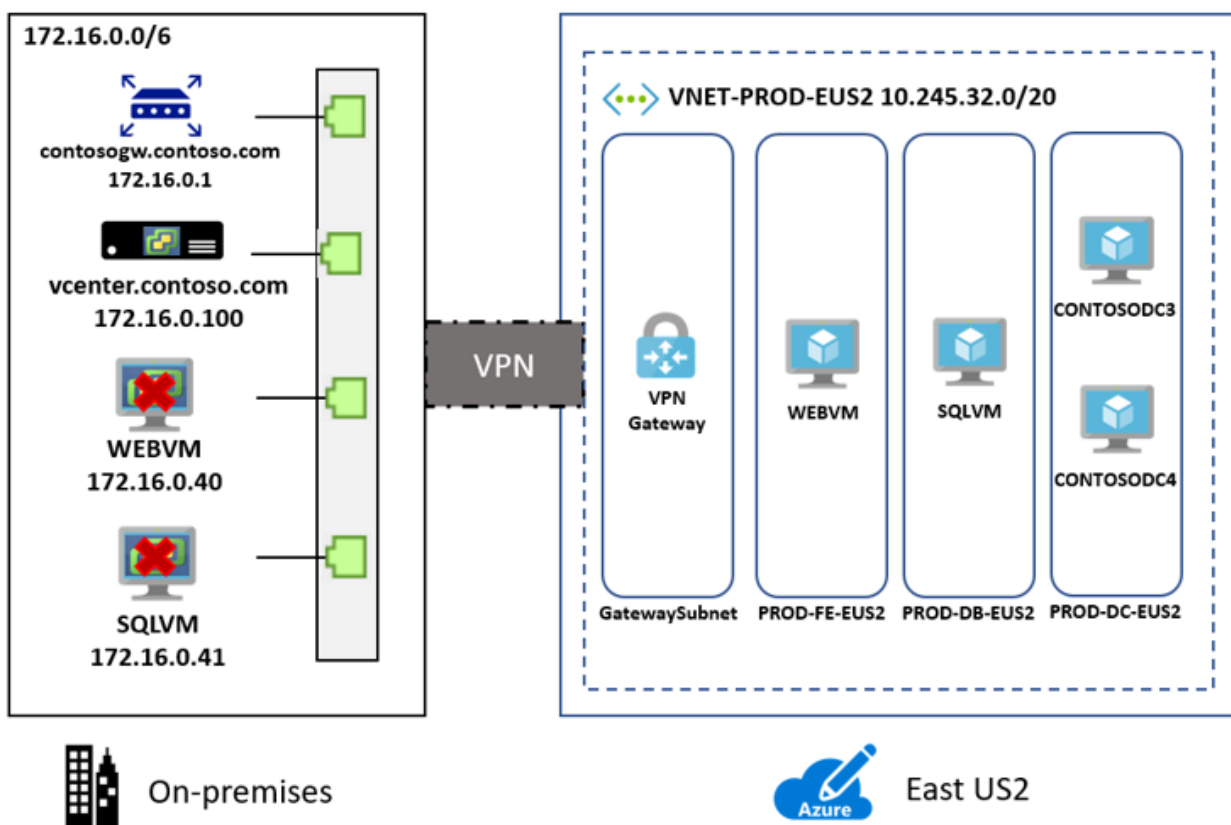
After pinning down goals and requirements, Contoso designs and review a deployment solution, and identifies the migration process, including the Azure services that Contoso will use for the migration.

Current app

- The app is tiered across two VMs (**WEBVM** and **SQLVM**).
- The VMs are located on VMware ESXi host **contosohost1.contoso.com** (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (**vcenter.contoso.com**), running on a VM.
- Contoso has an on-premises datacenter (contoso-datacenter), with an on-premises domain controller (**contosodc1**).

Proposed architecture

- Since the app is a production workload, the app VMs in Azure will reside in the production resource group ContosoRG.
- The app VMs will be migrated to the primary Azure region (East US 2) and placed in the production network (VNET-PROD-EUS2).
- The web front-end VM will reside in the front-end subnet (PROD-FE-EUS2) in the production network.
- The database VM will reside in the database subnet (PROD-DB-EUS2) in the production network.
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



Database considerations

As part of the solution design process, Contoso did a feature comparison between Azure SQL Database and SQL Server. The following considerations helped them to decide to go with SQL Server running on an Azure IaaS VM:

- Using an Azure VM running SQL Server seems to be an optimal solution if Contoso needs to customize the operating system or the database server, or if it might want to colocate and run third-party apps on the same VM.
- With Software Assurance, in future Contoso can exchange existing licenses for discounted rates on a SQL Database Managed Instance using the Azure Hybrid Benefit for SQL Server. This can save up to 30% on Managed Instance.

Solution review

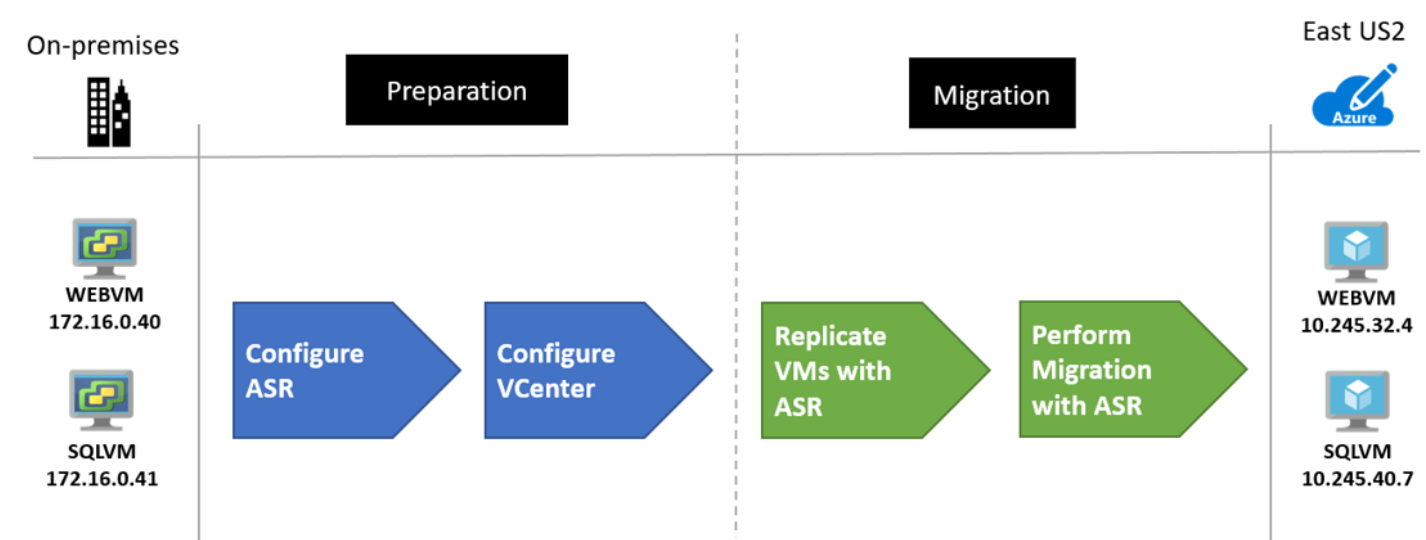
Contoso evaluates the proposed design by putting together a pros and cons list.

Consideration	Details
Pros	<p>Both the app VMs will be moved to Azure without changes, making the migration simple.</p> <p>Since Contoso is using "lift and shift" for both app VMs, no special configuration or migration tools are needed for the app database.</p> <p>Contoso can take advantage of their investment in Software Assurance, using the Azure Hybrid Benefit.</p> <p>Contoso will retain full control of the app VMs in Azure.</p>
Cons	<p>WEBVM and SQLVM are running Windows Server 2008 R2. The operating system is supported by Azure for specific roles (July 2018). Learn more.</p> <p>The web and data tiers of the app will remain a single point of failover.</p> <p>SQLVM is running on SQL Server 2008 R2 which isn't in mainstream support. However it is supported for Azure VMs (July 2018). Learn more.</p> <p>Contoso will need to continue supporting the app as Azure VMs rather than moving to a managed service such as Azure App Service and Azure SQL Database.</p>

Migration process

Contoso will migrate the app front-end and database VMs to Azure VMs with Site Recovery:

- As a first step, Contoso prepares and sets up Azure components for Site Recovery, and prepares the on-premises VMware infrastructure.
- They already have the [Azure infrastructure](#) in place, so Contoso just needs to add a couple of Azure components specifically for Site Recovery.
- With everything prepared, Contoso can start replicating the VMs.
- After replication is enabled and working, Contoso will migrate the VM by failing it over to Azure.



Azure services

Service	Description	Cost
---------	-------------	------

Service	Description	Cost
Azure Site Recovery	The service orchestrates and manages migration and disaster recovery for Azure VMs, and on-premises VMs and physical servers.	During replication to Azure, Azure Storage charges are incurred. Azure VMs are created, and incur charges, when failover occurs. Learn more about charges and pricing.

Prerequisites

Here's what Contoso needs to run this scenario.

Requirements	Details
Azure subscription	<p>Contoso created subscriptions in an earlier article in this series. If you don't have an Azure subscription, create a free account.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, review this article.</p>
Azure infrastructure	<p>Learn how Contoso set up an Azure infrastructure.</p> <p>Learn more about specific network and storage requirements for Site Recovery.</p>
On-premises servers	<p>On-premises vCenter Servers should be running version 5.5, 6.0, or 6.5</p> <p>ESXi hosts should run version 5.5, 6.0 or 6.5</p> <p>One or more VMware VMs should be running on the ESXi host.</p>
On-premises VMs	VMs must meet Azure requirements .

Scenario steps

Here's how Contoso admins will run the migration:

- ✓ **Step 1: Prepare Azure for Site Recovery.** They create an Azure storage account to hold replicated data, and a Recovery Services vault.
- ✓ **Step 2: Prepare on-premises VMware for Site Recovery.** They prepare accounts for VM discovery and agent installation, and prepare to connect to Azure VMs after failover.
- ✓ **Step 3: Replicate VMs.** They set up replication, and start replicating VMs to Azure storage.
- ✓ **Step 4: Migrate the VMs with Site Recovery.** They run a test failover to make sure everything's working, and then run a full failover to migrate the VMs to Azure.

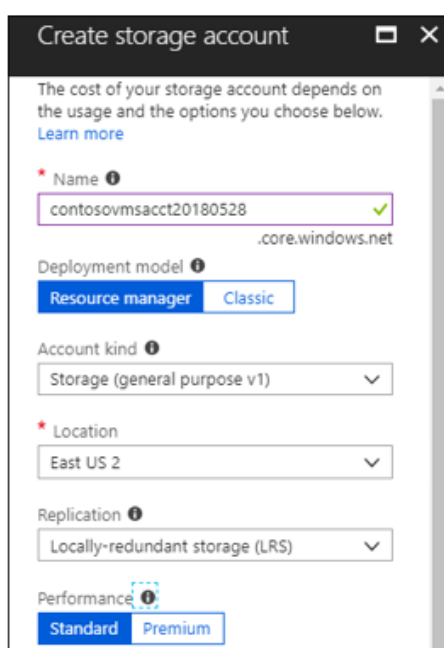
Step 1: Prepare Azure for the Site Recovery service

Here are the Azure components Contoso needs to migrate the VMs to Azure:

- A VNet in which Azure VMs will be located when they're created during failover.
- An Azure storage account to hold replicated data.
- A Recovery Services vault in Azure.

They set these up as follows:

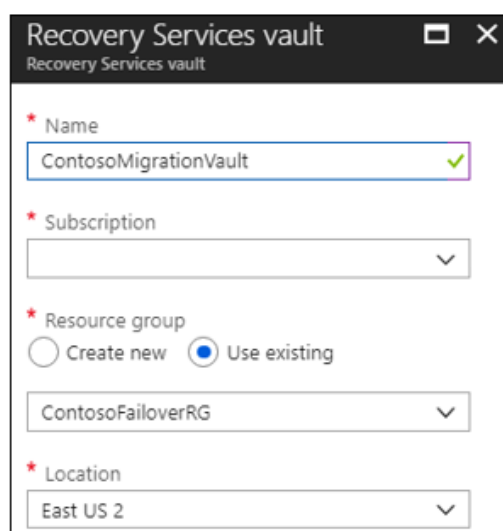
1. Set up a network-Contoso already set up a network that can be for Site Recovery when they [deployed the Azure infrastructure](#)
 - The SmartHotel360 app is a production app, and the VMs will be migrated to the Azure production network (VNET-PROD-EUS2) in the primary East US 2 region.
 - Both VMs will be placed in the ContosoRG resource group, which is used for production resources.
 - The app front-end VM (WEBVM) will migrate to the front-end subnet (PROD-FE-EUS2), in the production network.
 - The app database VM (SQLVM) will migrate to the database subnet (PROD-DB-EUS2), in the production network.
2. Set up a storage account-Contoso creates an Azure storage account (contosovmsacc20180528) in the primary region.
 - The storage account must be in the same region as the Recovery Services vault.
 - They use a general-purpose account, with standard storage, and LRS replication.



The screenshot shows the 'Create storage account' form in the Azure portal. The form includes the following fields and options:

- Name:** contosovmsacct20180528 (with a green checkmark and a note '.core.windows.net')
- Deployment model:** Resource manager (selected) and Classic
- Account kind:** Storage (general purpose v1)
- Location:** East US 2
- Replication:** Locally-redundant storage (LRS)
- Performance:** Standard (selected) and Premium

3. Create a vault-With the network and storage account in place, Contoso now creates a Recovery Services vault (ContosoMigrationVault), and places it in the ContosoFailoverRG resource group in the primary East US 2 region.



The screenshot shows the 'Recovery Services vault' form in the Azure portal. The form includes the following fields and options:

- Name:** ContosoMigrationVault (with a green checkmark)
- Subscription:** (empty dropdown)
- Resource group:** Create new (radio button) and Use existing (radio button, selected). Below this is a dropdown menu showing 'ContosoFailoverRG'.
- Location:** East US 2

Need more help?

Step 2: Prepare on-premises VMware for Site Recovery

Here's what Contoso prepares on-premises:

- An account on the vCenter server or vSphere ESXi host, to automate VM discovery.
- An account that allows automatic installation of the Mobility service on the VMware VMs.
- On-premises VM settings, so that Contoso can connect to the replicated Azure VMs after failover.

Prepare an account for automatic discovery

Site Recovery needs access to VMware servers to:

- Automatically discover VMs.
- Orchestrate replication, failover, and failback for VMs.
- At least a read-only account is required. The account should be able to run operations such as creating and removing disks, and turning on VMs.

Contoso admins set up the account as follows:

1. They create a role at the vCenter level.
2. They assign that role the required permissions.

Prepare an account for Mobility service installation

The Mobility service must be installed on each VM.

- Site Recovery can do an automatic push installation of the Mobility service when VM replication is enabled.
- An account is required, so that Site Recovery can access the VMs for the push installation. You specify this account when you set up replication.
- The account can be domain or local, with permissions to install on the VMs.

Prepare to connect to Azure VMs after failover

After failover, Contoso wants to connect to the Azure VMs. To do this, Contoso admins do the following before migration:

1. For access over the internet they:
 - Enable RDP on the on-premises VM before failover.
 - Ensure that TCP and UDP rules are added for the **Public** profile.
 - Check that RDP is allowed in **Windows Firewall > Allowed Apps** for all profiles.
2. For access over site-to-site VPN, they:
 - Enable RDP on the on-premises machine.
 - Allow RDP in the **Windows Firewall -> Allowed apps and features**, for **Domain and Private** networks.
 - Set the operating system's SAN policy on the on-premises VM to **OnlineAll**.

In addition, when they run a failover they need to check the following:

- There should be no Windows updates pending on the VM when triggering a failover. If there are, they won't be able to log into the VM until the update completes.
- After failover, they can check **Boot diagnostics** to view a screenshot of the VM. If this doesn't work, they should verify that the VM is running, and review these [troubleshooting tips](#).

Need more help?

- [Learn about](#) creating and assigning a role for automatic discovery.
- [Learn about](#) creating an account for push installation of the Mobility service.

Step 3: Replicate the on-premises VMs

Before Contoso admins can run a migration to Azure, they need to set up and enable replication.

Set a replication goal

1. In the vault, under the vault name (ContosoVMVault) they select a replication goal (**Getting Started** > **Site Recovery** > **Prepare infrastructure**).
2. They specify that their machines are located on-premises, running on VMware, and replicating to Azure.

The screenshot shows two side-by-side configuration windows for 'ContosoMigrationVault'.

Prepare infrastructure window:

- Header: Prepare infrastructure, ContosoMigrationVault
- Message: These are long running tasks done on-premises.
- Progress list:
 - 1 Protection goal VMware VMs/physical servers... (Completed with green checkmark)
 - 2 Deployment planning I have done it (Completed with green checkmark)
 - 3 Source Prepare (Next step, indicated by a right arrow)
 - 4 Target Prepare (Next step, indicated by a right arrow)
 - 5 Replication settings Prepare (Next step, indicated by a right arrow)

Protection goal window:

- Header: Protection goal, ContosoMigrationVault
- Form fields:
 - * Where are your machines located? (Dropdown menu: On-premises)
 - * Where do you want to replicate your machines to? (Dropdown menu: To Azure)
 - * Are your machines virtualized? (Dropdown menu: Yes, with VMware vSphere Hypervisor)

Confirm deployment planning

To continue, they confirm that they have completed deployment planning, by selecting **Yes, I have done it**. In this scenario, Contoso are only migrating two VMs, and don't need deployment planning.

Set up the source environment

Contoso admins need to configure the source environment. To do this, they download an OVF template and use it to deploy the Site Recovery configuration server as a highly available, on-premises VMware VM. After the configuration server is up and running, they register it in the vault.

The configuration server runs several components:


- The configuration server component that coordinates communications between on-premises and Azure and manages data replication.
- The process server that acts as a replication gateway. It receives replication data; optimizes it with caching, compression, and encryption; and sends it to Azure storage.
- The process server also installs Mobility Service on VMs you want to replicate and performs automatic discovery of on-premises VMware VMs.

Contoso admins perform these steps as follows:

1. In the vault, they download the OVF template from **Prepare Infrastructure > Source > Configuration Server**.

Server type

Configuration server for VMware



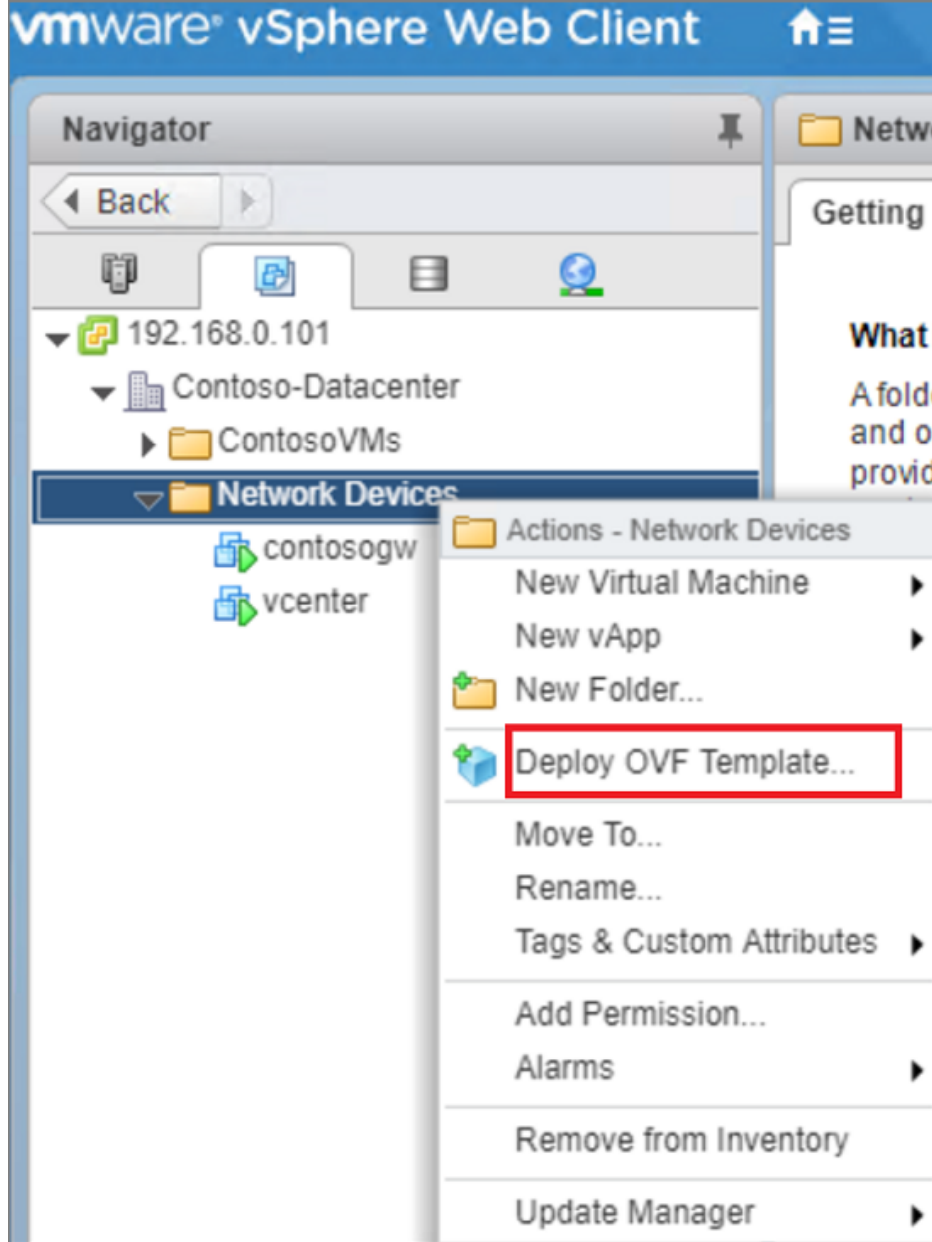
Adding Configuration server may take 15 minutes to 30 minutes

Register your Configuration server

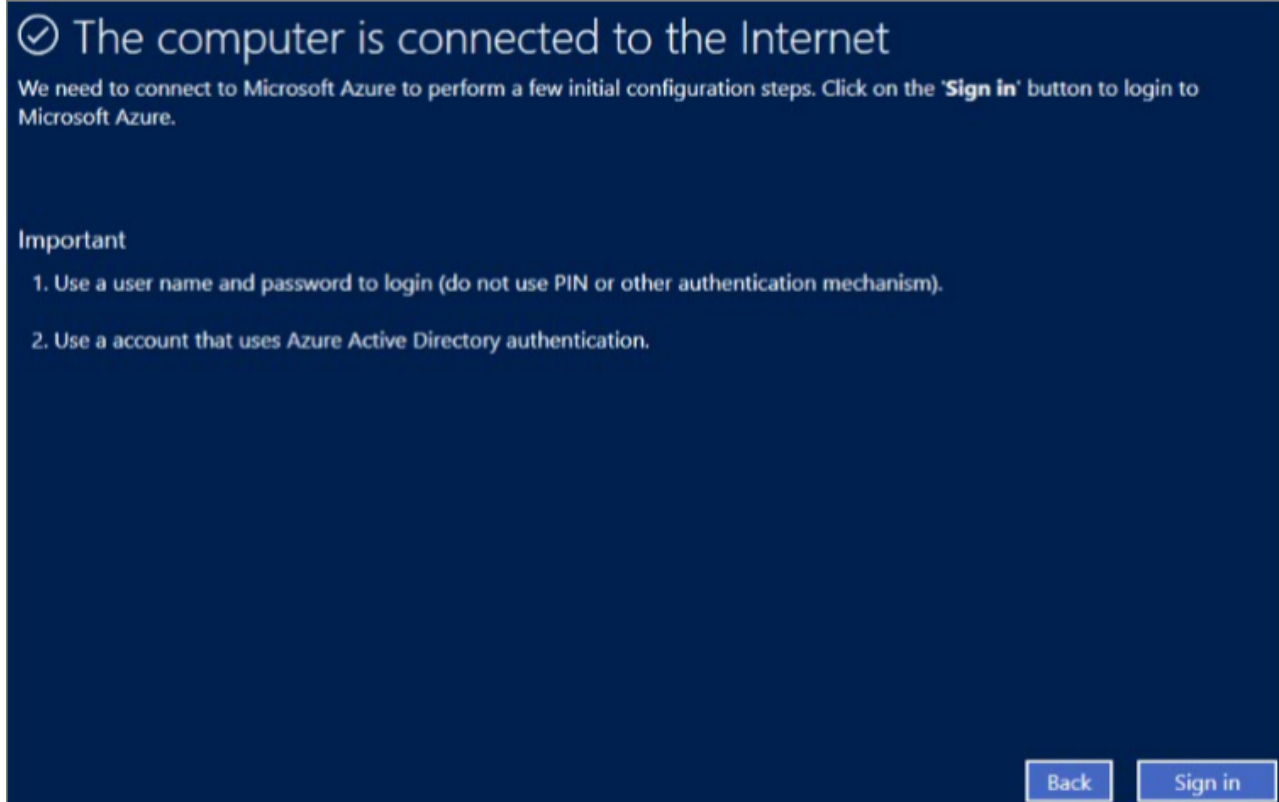
On-premises

1. [Download](#) the Configuration server virtual machine template.
2. Import the Configuration server virtual machine template into your vCenter server using the **Deploy OVF Template wizard**.
3. Connect to the virtual machine's console once it has successfully booted up.
4. Complete the Windows Server installation by accepting the license agreement and setting up an Administrator account
5. Once the Windows installation is completed, install [VMware PowerCLI 6.0](#) on the Configuration server
6. Launch the Azure Site Recovery Configuration Manager wizard and follow the steps to register your Configuration server with Azure Site Recovery. [Read more](#)

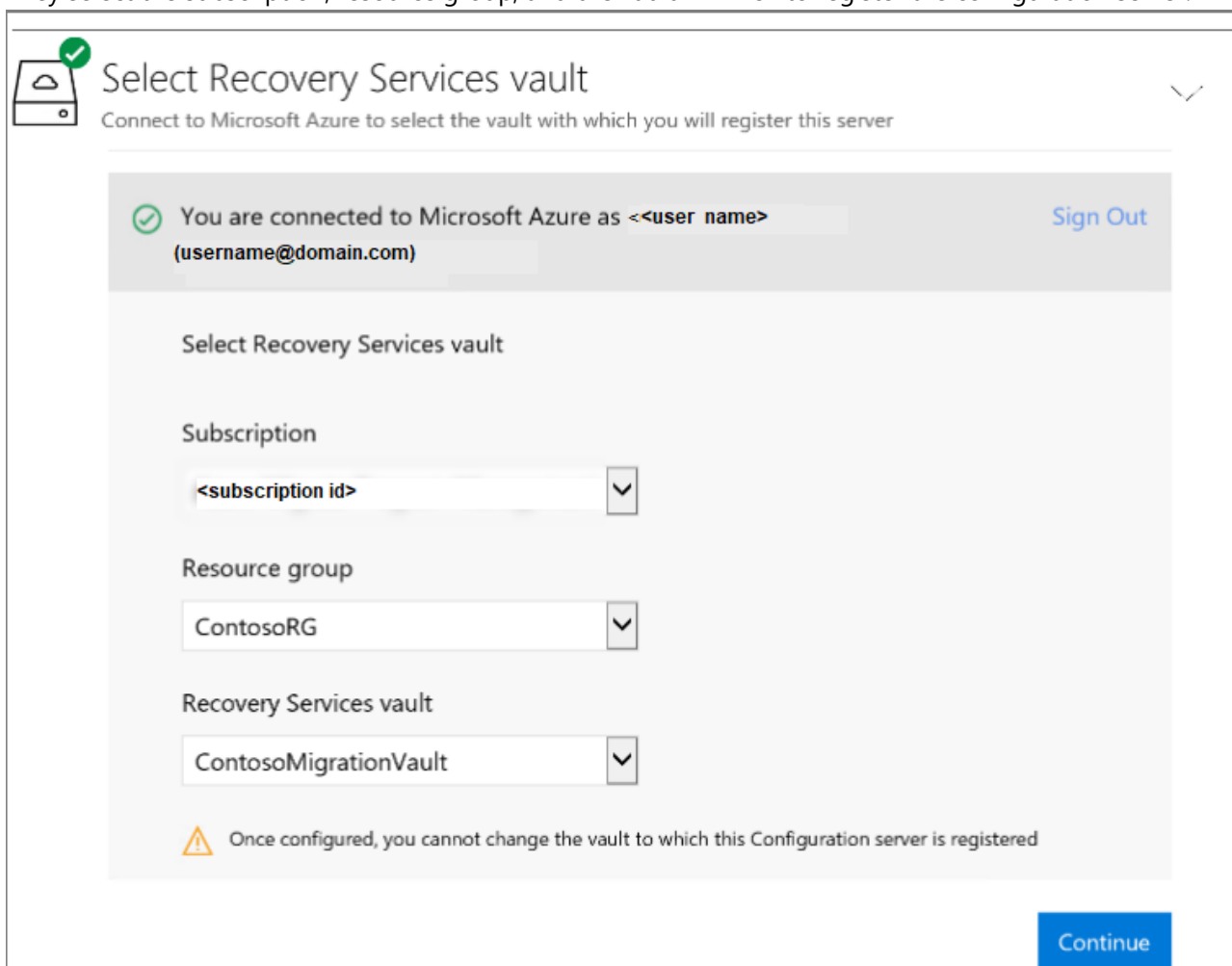
2. They import the template into VMware to create and deploy the VM.



3. When they turn on the VM for the first time, it boots up into a Windows Server 2016 installation experience. They accept the license agreement, and enter an administrator password.
4. After the installation finishes, they sign in to the VM as the administrator. At first sign-in, the Azure Site Recovery Configuration Tool runs by default.
5. In the tool, they specify a name to register the configuration server in the vault.
6. The tool checks that the VM can connect to Azure. After the connection is established, they sign in to the Azure subscription. The credentials must have access to the vault in which they'll register the configuration server.



7. The tool performs some configuration tasks and then reboots.
8. They sign in to the machine again, and the Configuration Server Management Wizard starts automatically.
9. In the wizard, they select the NIC to receive replication traffic. This setting can't be changed after it's configured.
10. They select the subscription, resource group, and the vault in which to register the configuration server.



11. They download and install MySQL Server, and VMware PowerCLI.

12. After validation, they specify the FQDN or IP address of the vCenter server or vSphere host. They leave the default port, and specify a friendly name for the server in Azure.
13. They specify the account that they created for automatic discovery, and the credentials that are used to automatically install the Mobility Service. For Windows machines, the account needs local administrator privileges on the VMs.

Enter the connection details

Server name/IP address ⓘ

Port ⓘ

Provide friendly name for this vCenter Server ⓘ

Provide credentials to connect to the vCenter Server [Read more](#)

User name

Password

Provide friendly name for the credentials ⓘ

 ✕

Add

14. After registration finishes, in the Azure portal, they double check that the configuration server and VMware server are listed on the **Source** page in the vault. Discovery can take 15 minutes or more.
15. Site Recovery then connects to VMware servers using the specified settings, and discovers VMs.

Set up the target

Now Contoso admins specify the target replication settings.

1. In **Prepare infrastructure > Target**, they select the target settings.
2. Site Recovery checks that there's an Azure storage account and network in the specified target location.

Create a replication policy

Now Contoso admins can create a replication policy.

1. In **Prepare infrastructure > Replication Settings > Replication Policy > Create and Associate**, they create a policy **ContosoMigrationPolicy**.
2. They use the default settings:

- **RPO threshold:** Default of 60 minutes. This value defines how often recovery points are created. An alert is generated if continuous replication exceeds this limit.
- **Recovery point retention:** Default of 24 hours. This value specifies how long the retention window is for each recovery point. Replicated VMs can be recovered to any point in a window.
- **App-consistent snapshot frequency:** Default of one hour. This value specifies the frequency at which application-consistent snapshots are created.

* Name ⓘ
 ContosoMigrationPolicy ✓

Source type ⓘ
 VMware / Physical machines ▼


Target type ⓘ
 Azure ▼

* RPO threshold in mins ⓘ
 60

* Recovery point retention in hours ⓘ
 24

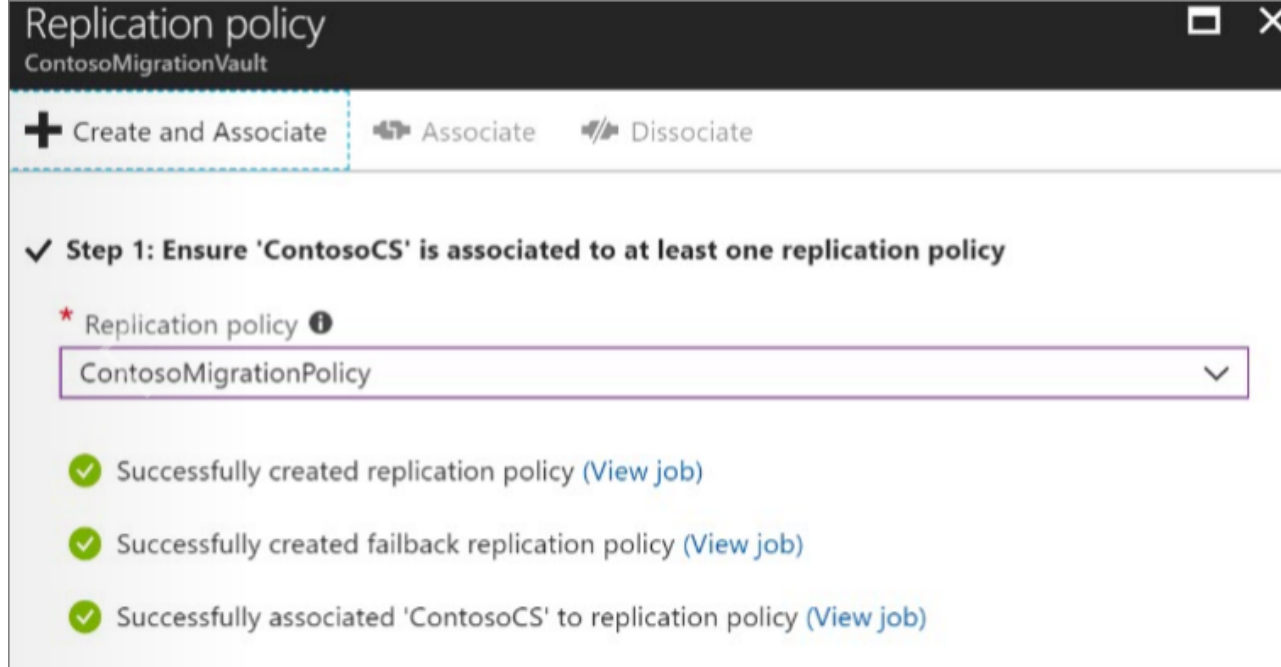
* App-consistent snapshot frequency in hours ⓘ
 1 ▼

Failback replication policy name ⓘ
 ContosoMigrationPolicy-failback

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

Associated Configuration Server ⓘ
 ContosoCS

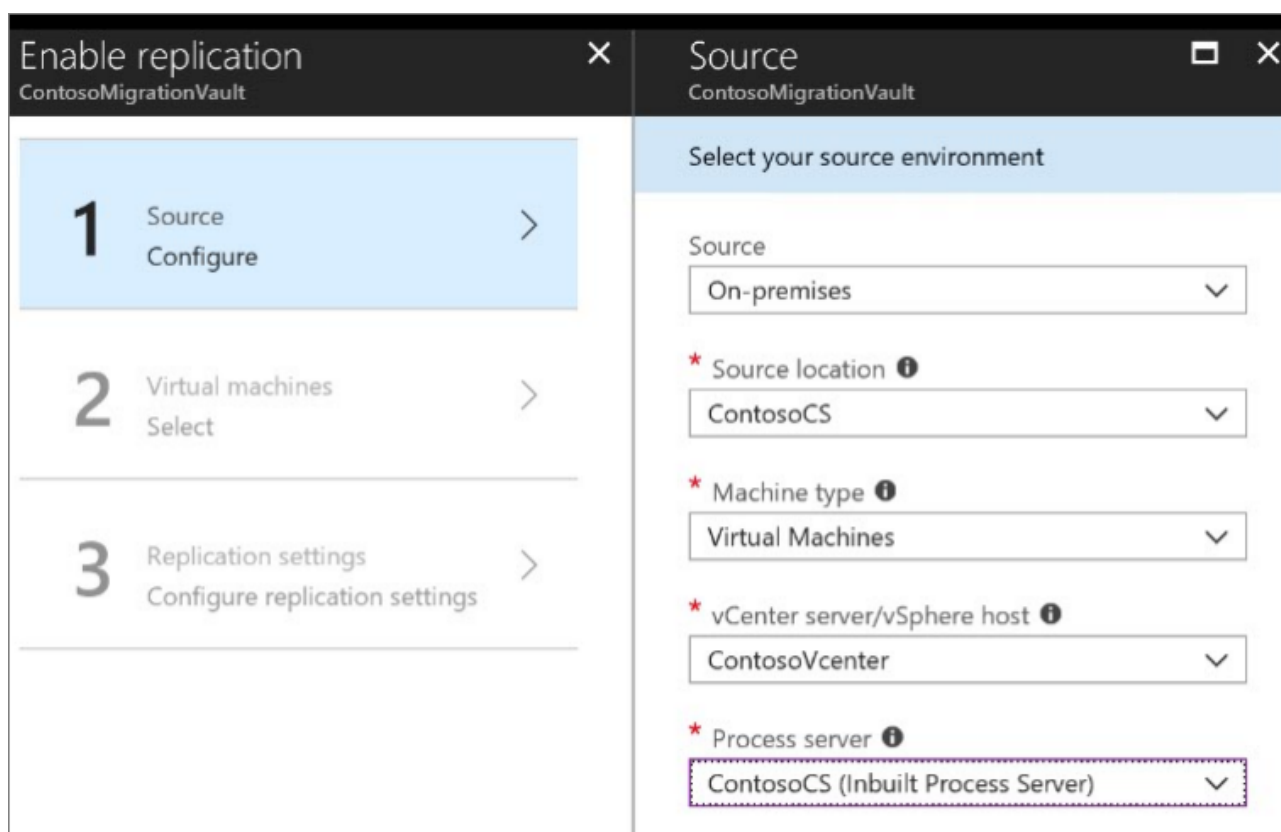
3. The policy is automatically associated with the configuration server.



Enable replication for WEBVM

With everything in place, Contoso admins can now enable replication for the VMs. They start with WebVM.

1. In **Replicate application** > **Source** > **+Replicate** they select the source settings.
2. They indicate that they want to enable VMs, select the vCenter server, and the configuration server.



3. They select the target settings, including the resource group and Azure network, and the storage account.

Target
ContosoMigrationVault

Select your target settings for recovery

* Target ⓘ
Azure

* Subscription ⓘ
<subscription id>

Post-failover resource group ⓘ
ContosoRG

* Post-failover deployment model ⓘ
Resource Manager

* Storage account ⓘ
contosovmsacct20180528

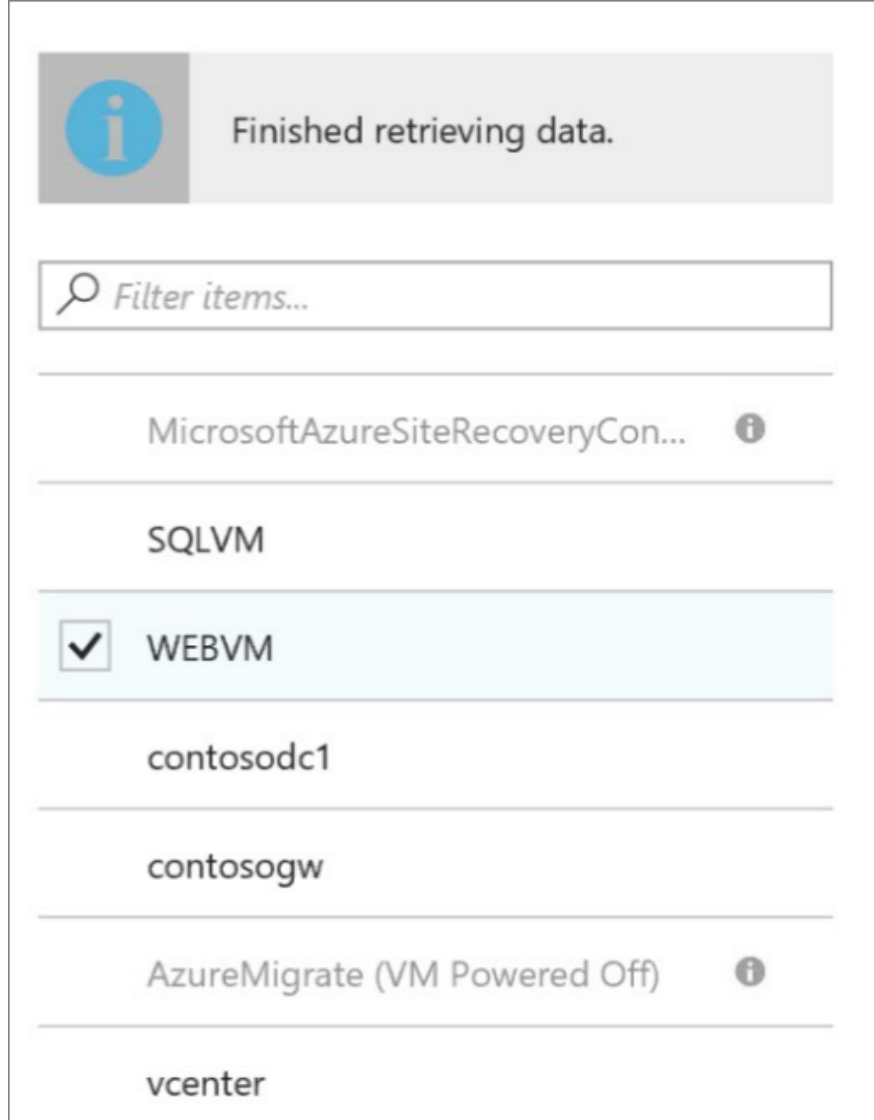
Azure network ⓘ
Configure now for selected machines.

Post-failover Azure network ⓘ
VNET-PROD-EUS2

Subnet ⓘ
PROD-FE-EUS2 (10.245.32.0/22)

4. They select **WebVM** for replication, check the replication policy, and enable replication.

- At this stage they only select WEBVM because VNet and subnet must be selected, and the app VMs will be placed in different subnets.
- Site Recovery automatically installs the Mobility service on the VM when replication is enabled.



5. They track replication progress in **Jobs**. After the **Finalize Protection** job runs, the machine is ready for failover.

6. In **Essentials** in the Azure portal, they can see the structure for the VMs replicating to Azure.

Enable replication for SQLVM

Now Contoso admins can start replicating the SQLVM machine, using the same process as above.

1. They select source settings.

Enable replication

ContosoMigrationVault

1

Source
Configure

>

2

Virtual machines
Select

>

3

Replication settings
Configure replication settings

>

Source

ContosoMigrationVault

Select your source environment

Source

On-premises

* Source location ⓘ

ContosoCS

* Machine type ⓘ

Virtual Machines

* vCenter server/vSphere host ⓘ

ContosoVcenter

* Process server ⓘ

ContosoCS (Inbuilt Process Server)

2. They then specify the target settings.

Target

ContosoMigrationVault

Select your target settings for recovery

* Target ⓘ

Azure

* Subscription ⓘ

Azure Migrate Program Management Team

Post-failover resource group ⓘ

ContosoRG

* Post-failover deployment model ⓘ

Resource Manager

* Storage account ⓘ

contosovmsacct20180528

Azure network ⓘ

Configure now for selected machines.

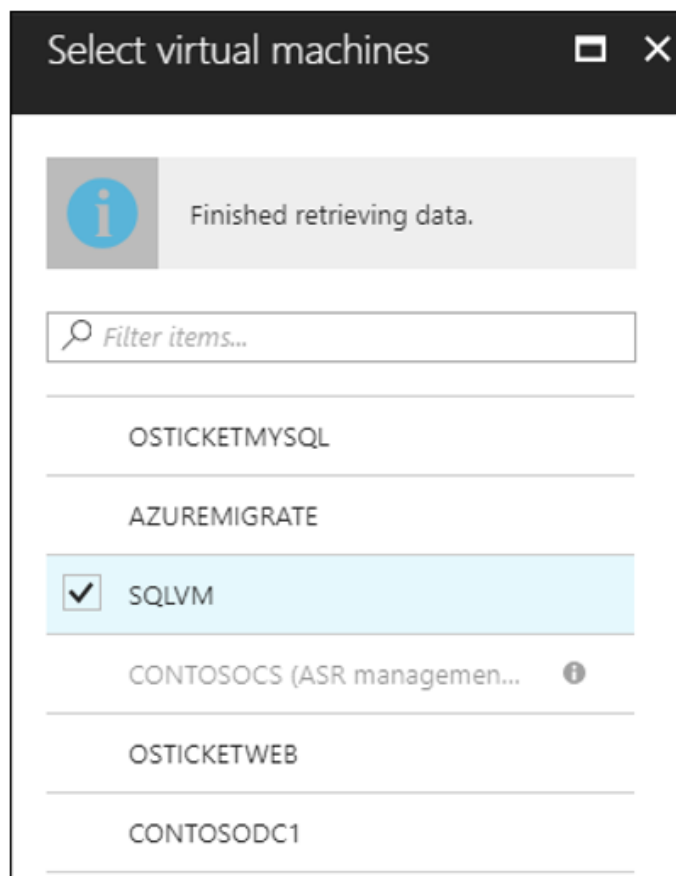
Post-failover Azure network ⓘ

VNET-PROD-EUS2

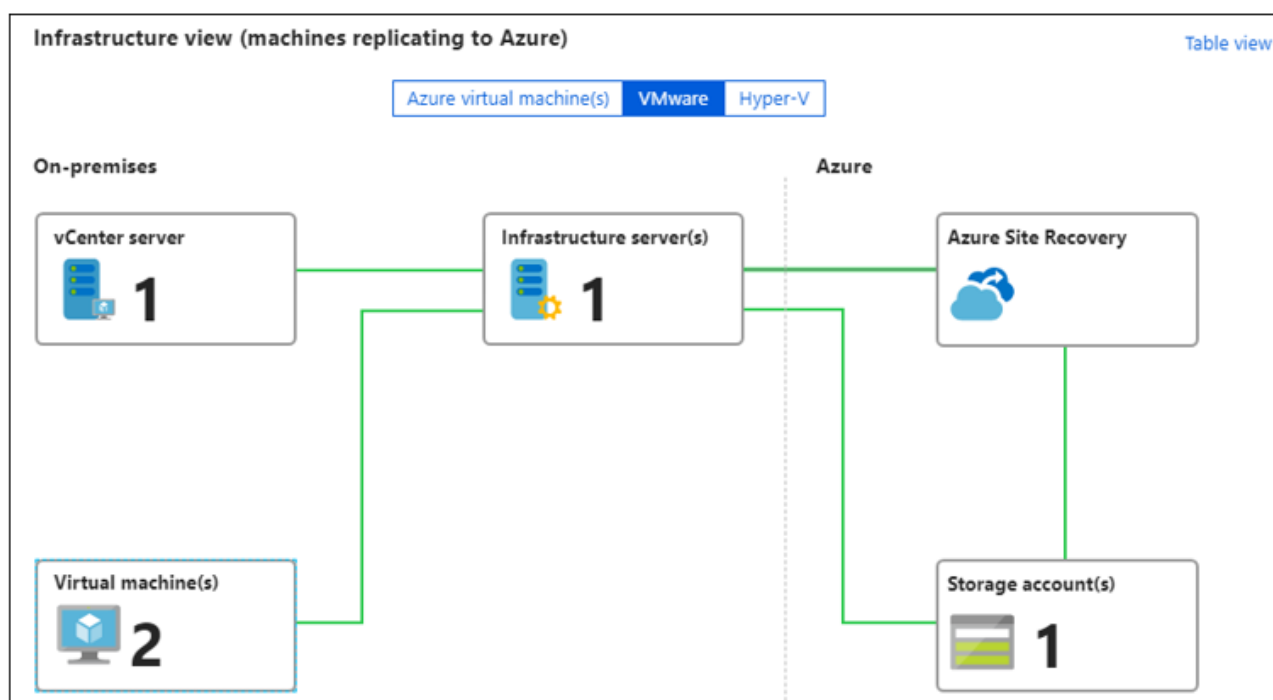
Subnet ⓘ

PROD-DB-EUS2 (10.245.40.0/23)

3. They select SQLVM for replication.



4. They apply the same replication policy that was used for WEBVM, and enable replication.



Need more help?

- You can read a full walkthrough of all these steps in [Set up disaster recovery for on-premises VMware VMs](#).
- Detailed instructions are available to help you [set up the source environment](#), [deploy the configuration server](#), and [configure replication settings](#).
- You can learn more about [enabling replication](#).

Step 4: Migrate the VMs

Contoso admins run a quick test failover, and then a full failover to migrate the VMs.

Run a test failover

A test failover helps to ensure that everything's working as expected.

1. They run a test failover to the latest available point in time (**Latest processed**).
2. They select **Shut down machine before beginning failover**, so that Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails.
3. Test failover runs:
 - A prerequisites check runs to make sure all of the conditions required for migration are in place.
 - Failover processes the data, so that an Azure VM can be created. If select the latest recovery point, a recovery point is created from the data.
 - An Azure VM is created using the data processed in the previous step.
4. After the failover finishes, the replica Azure VM appears in the Azure portal. They check that the VM is the appropriate size, connected to the right network, and is running.
5. After verifying the test failover, they clean up the failover, and record and save any observations.

Create and customize a recovery plan

After verifying that the test failover worked as expected, Contoso admins create a recovery plan for migration.

- A recovery plan specifies the order in which failover occurs, and indicates how Azure VMs will be brought online in Azure.
- Since the app is two-tier, they customize the recovery plan so that the data VM (SQLVM) starts before the front-end (WEBVM).

1. In **Recovery Plans (Site Recovery)** > **+Recovery Plan**, they create a plan and add the VMs to it.

PROTECTED ITEM	TYPE
<input checked="" type="checkbox"/> SQLVM	Machine
<input checked="" type="checkbox"/> WEBVM	Machine

2. After creating the plan, they customize it (**Recovery Plans** > **SmartHotelMigrationPlan** > **Customize**).
3. They remove WEBVM from **Group 1: Start**. This ensures that the first start action affects SQLVM only.
4. In **+Group** > **Add protected items**, they add WEBVM to Group 2: Start. The VMs need to be in two different groups.

Migrate the VMs

Now Contoso admins run a full failover to complete the migration.

1. They select the recovery plan > **Failover**.

2. They select to fail over to the latest recovery point, and that Site Recovery should try to shut down the on-premises VM before triggering the failover. They can follow the failover progress on the **Jobs** page.

Failover

ContosoMigrationPlan

Failover direction

From ⓘ

ContosoCS

To ⓘ

Microsoft Azure

2 of 2 virtual machines will be failed over

Change direction

Recovery Point

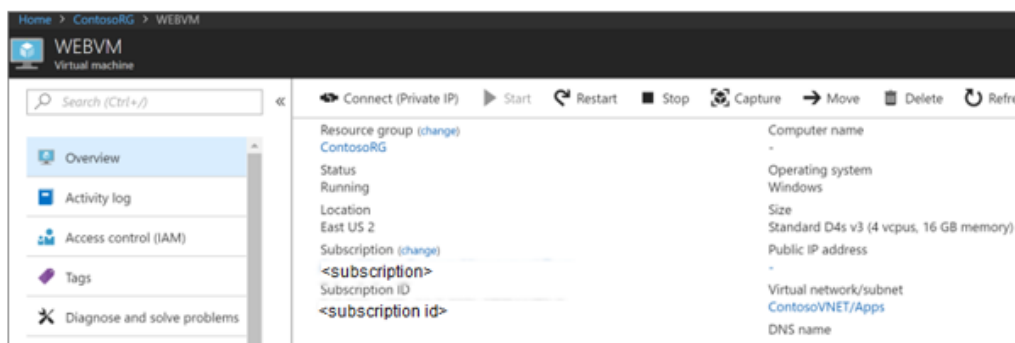
Choose a recovery point ⓘ

Latest (lowest RPO) ▾

Shut down machines


☒ Shut down machines before beginning failover

3. After the failover, they verify that the Azure VM appears as expected in the Azure portal.



4. After verification, they complete the migration for each VM. This stops replication for the VM, and stops Site Recovery billing for it.

NAME	...	STATUS	ACTIVE LOCATION
SQLVM	-	Failover completed	Microsoft Azure
WEBVM	-	Failover completed	Microsoft Azure

Pin to dashboard 

Failover

Test Failover

Cleanup test failover

Change recovery point

Commit

Complete Migration

Re-protect

Resynchronize

Error Details

Disable Replication

Need more help?

- [Learn about](#) running a test failover.
- [Learn](#) how to create a recovery plan.
- [Learn about](#) failing over to Azure.

Clean up after migration

With migration complete, the SmartHotel360 app tiers are now running on Azure VMs.

Now, Contoso needs to complete these cleanup steps:

- Remove the WEBVM machine from the vCenter inventory.
- Remove the SQLVM machine from the vCenter inventory.
- Remove WEBVM and SQLVM from local backup jobs.
- Update internal documentation to show the new location, and IP addresses for the VMs.
- Review any resources that interact with the VMs, and update any relevant settings or documentation to reflect the new configuration.

Review the deployment

With the app now running, Contoso now needs to fully operationalize and secure it in Azure.

Security

The Contoso security team reviews the Azure VMs, to determine any security issues.

- To control access, the team reviews the network security groups (NSGs) for the VMs. NSGs are used to ensure that only traffic allowed to the app can reach it.
- The team also consider securing the data on the disk using Azure Disk Encryption and Key Vault.

[Read more](#) about security practices for VMs.

BCDR

For business continuity and disaster recovery (BCDR), Contoso takes the following actions:

- Keep data safe: Contoso backs up the data on the VMs using the Azure Backup service. [Learn more.](#)
- Keep apps up and running: Contoso replicates the app VMs in Azure to a secondary region using Site Recovery. [Learn more.](#)

Licensing and cost optimization

1. Contoso has existing licensing for their VMs, and will take advantage of the Azure Hybrid Benefit. Contoso will convert the existing Azure VMs, to take advantage of this pricing.
2. Contoso will enable Azure Cost Management licensed by Cloudyn, a Microsoft subsidiary. It's a multicloud cost management solution that helps to use and manage Azure and other cloud resources. [Learn more](#) about Azure Cost Management.

Conclusion

In this article, Contoso rehosted the SmartHotel360 app in Azure by migrating the app VMs to Azure VMs using the Site Recovery service.