Rehost an on-premises Linux app to Azure VMs and Azure Database for MySQL

04/04/2019 • 16 minutes to read • Contributors

In this article

This article shows how the fictional company Contoso rehosts a two-tier Linux-based Apache/MySQL/PHP (LAMP) app, migrating it from on-premises to Azure using Azure VMs and Azure Database for MySQL.

osTicket, the service desk app used in this example, is provided as open source. If you'd like to use it for your own testing, 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:

- **Address business growth.** Contoso is growing, and as a result there's pressure on the on-premises systems and infrastructure.
- **Limit risk.** The service desk app is critical for the business. Contoso wants to move it to Azure with zero risk.
- **Extend.** Contoso doesn't want to change the app right now. It simply wants to keep the app stable.

Migration goals

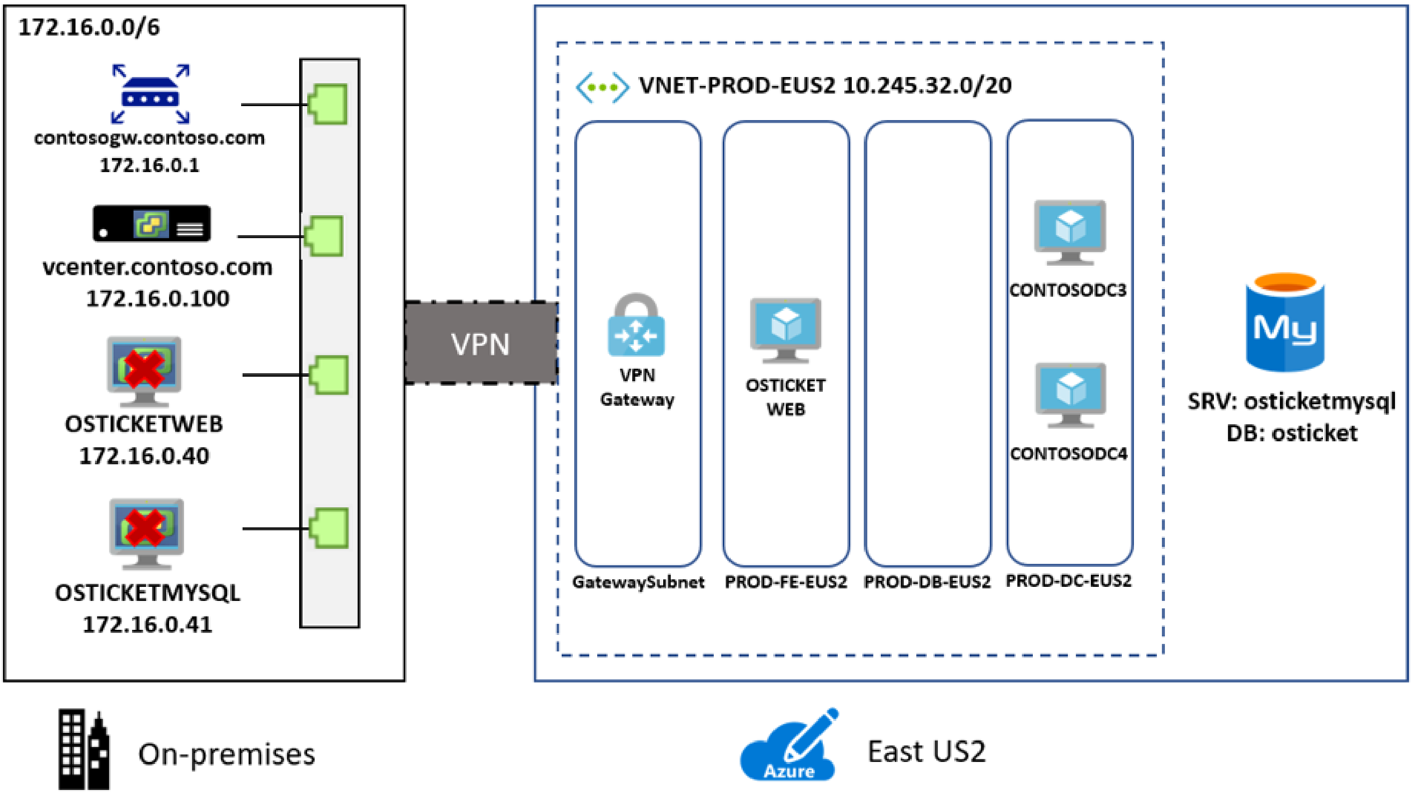
The Contoso cloud team has pinned down goals for this migration, in order to determine the best migration method:

- After migration, the app in Azure should have the same performance capabilities as it does today in their on-premises VMware environment. The app will remain as critical in the cloud as it is on-premises.
- Contoso doesn’t want to invest in this app. It's important to the business, but in its current form Contoso simply want to move it safely to the cloud.
- Having completed a couple of Windows app migrations, Contoso wants to learn how to use a Linux-based infrastructure in Azure.
- Contoso wants to minimize database admin tasks after the application is moved to the cloud.

Proposed architecture

In this scenario:

- The app is tiered across two VMs (`OSTICKETWEB` and `OSTICKETMYSQL`).
- 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`).
- The web tier app on `OSTICKETWEB` will be migrated to an Azure IaaS VM.
- The app database will be migrated to the Azure Database for MySQL PaaS service.
- Since Contoso is migrating a production workload, the resources will reside in the production resource group `ContosoRG`.
- The resources will be replicated to the primary region (East US 2), and placed in the production network (`VNET-PROD-EUS2`):
  - The web VM will reside in the front-end subnet (`PROD-FE-EUS2`).
  - The database instance will reside in the database subnet (`PROD-DB-EUS2`).
- The app database will be migrated to Azure Database for MySQL using MySQL tools.
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



Migration process

Contoso will complete the migration process as follows:

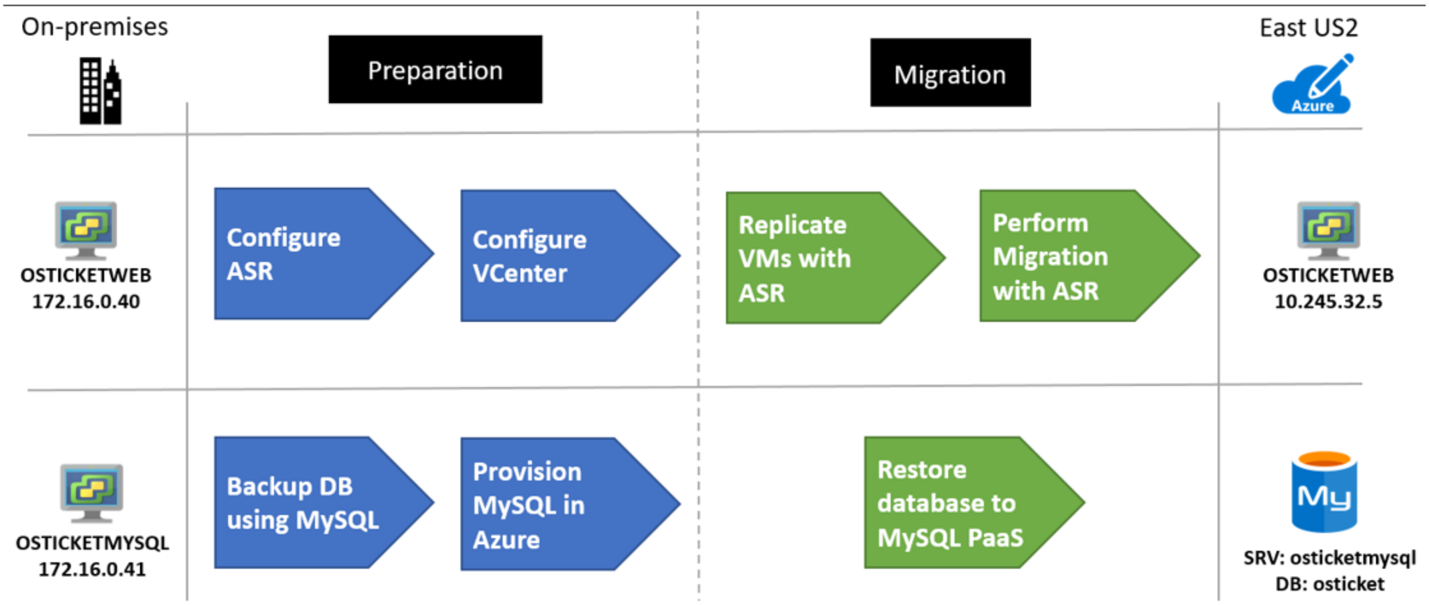
To migrate the web VM:

1. As a first step, Contoso sets up the Azure and on-premises infrastructure needed to deploy Site Recovery.
2. After preparing the Azure and on-premises components, Contoso sets up and enables replication for the web VM.
3. After replication is up-and-running, Contoso migrates the VM by failing it over to Azure.

To migrate the database:

1. Contoso provisions a MySQL instance in Azure.

2. Contoso sets up MySQL workbench, and backs up the database locally.
3. Contoso then restore the database from the local backup to Azure.



Azure services

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.
Azure Database for MySQL	The database is based on the open-source MySQL Server engine. It provides a fully managed enterprise-ready community MySQL database, as a service for app development and deployment.	

Prerequisites

Here's what Contoso needs for this scenario.

Requirements	Details
Azure subscription	Contoso created subscriptions during an earlier article. If you don't have an Azure subscription, create a free account. If you create a free account, you're the administrator of your subscription and can perform all actions. 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. If you need more granular permissions, review this article.
Azure infrastructure	Contoso set up the Azure infrastructure as described in Azure infrastructure for migration. Learn more about specific network and storage requirements for Site Recovery.

Requirements	Details
On-premises servers	The on-premises vCenter server should be running version 5.5, 6.0, or 6.5 An ESXi host running version 5.5, 6.0 or 6.5 One or more VMware VMs running on the ESXi host.
On-premises VMs	Review Linux VM requirements that are supported for migration with Site Recovery. Verify supported Linux file and storage systems. VMs must meet Azure requirements.

Scenario steps

Here's how Contoso admins will complete the migration:

✓ **Step 1: Prepare Azure for Site Recovery.** They create an Azure storage account to hold replicated data, and create 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: Provision the database.** In Azure, they provision an instance of Azure Database for MySQL.
✓ **Step 4: Replicate VMs.** They configure the Site Recovery source and target environment, set up a replication policy, and start replicating VMs to Azure storage.
✓ **Step 5: Migrate the database.** They set up migration with MySQL tools.
✓ **Step 6: Migrate the VMs with Site Recovery.** Lastly, 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

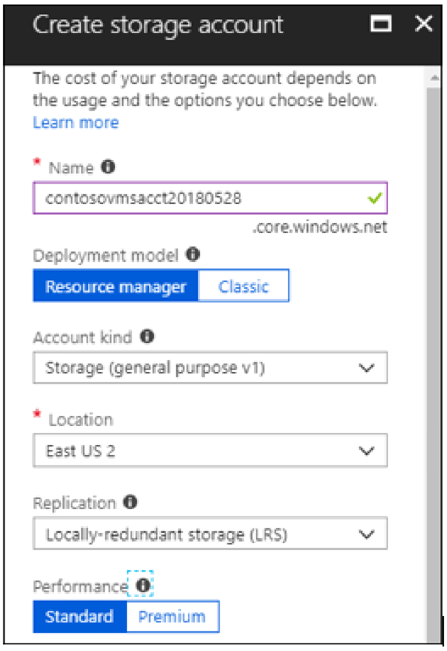
Contoso needs a couple of Azure components for Site Recovery:

- A VNet in which failed over resources are located. Contoso already created the VNet during Azure infrastructure deployment
- A new Azure storage account to hold replicated data.
- A Recovery Services vault in Azure.

The Contoso admins create a storage account and vault as follows:

1. They create a storage account (**contosovmsacc20180528**) in the East US 2 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.



Create storage account

The cost of your storage account depends on the usage and the options you choose below. Learn more

* Name

contosovmsacct20180528 ✓

.core.windows.net

Deployment model

[✓ Resource manager] Classic

Account kind

Storage (general purpose v1)

* Location

East US 2

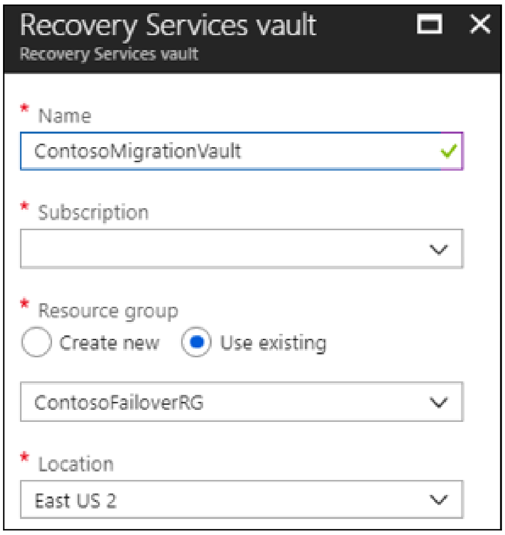
Replication

Locally-redundant storage (LRS)

Performance

[✓ Standard] Premium

2. With the network and storage account in place, they create a vault (ContosoMigrationVault), and place it in the **ContosoFailoverRG** resource group, in the primary East US 2 region.



Recovery Services vault

Recovery Services vault

* Name

ContosoMigrationVault ✓

* Subscription

* Resource group

○ Create new ● Use existing

ContosoFailoverRG

* Location

East US 2

Need more help?

Learn about setting up Azure for Site Recovery.

Step 2: Prepare on-premises VMware for Site Recovery

Contoso admins prepare the on-premises VMware infrastructure as follows:

- They create an account on the vCenter server, to automate VM discovery.
- They create an account that allows automatic installation of the Mobility service on VMware VMs that will be replicated.
- They prepare on-premises VMs, so that they can connect to Azure VMs when they're created after the migration.

Prepare an account for automatic discovery

Site Recovery needs access to VMware servers to:

- Automatically discover VMs. At least a read-only account is required.

- Orchestrate replication, failover, and failback. You need an account that can 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 then assign that role the required permissions.

Prepare an account for Mobility service installation

The Mobility service must be installed on each VM that Contoso wants to migrate.

- Site Recovery can do an automatic push installation of this component when you enable replication for the VMs.
- For automatic installation. Site Recovery needs an account with permissions to access the VM.
- Account details are input during replication setup.
- The account can be domain or local account, as long as it has installation permissions.

Prepare to connect to Azure VMs after failover

After failover to Azure, Contoso wants to be able to connect to the Azure VMs. To do this, Contoso admins need to do the following:

- To access over the internet, they enable SSH on the on-premises Linux VM before the migration. For Ubuntu this can be completed using the following command: **Sudo apt-get ssh install -y**.
- After the failover, they should check **Boot diagnostics** to view a screenshot of the VM.
- If this doesn't work, they need to verify that the VM is running, and review these troubleshooting tips.

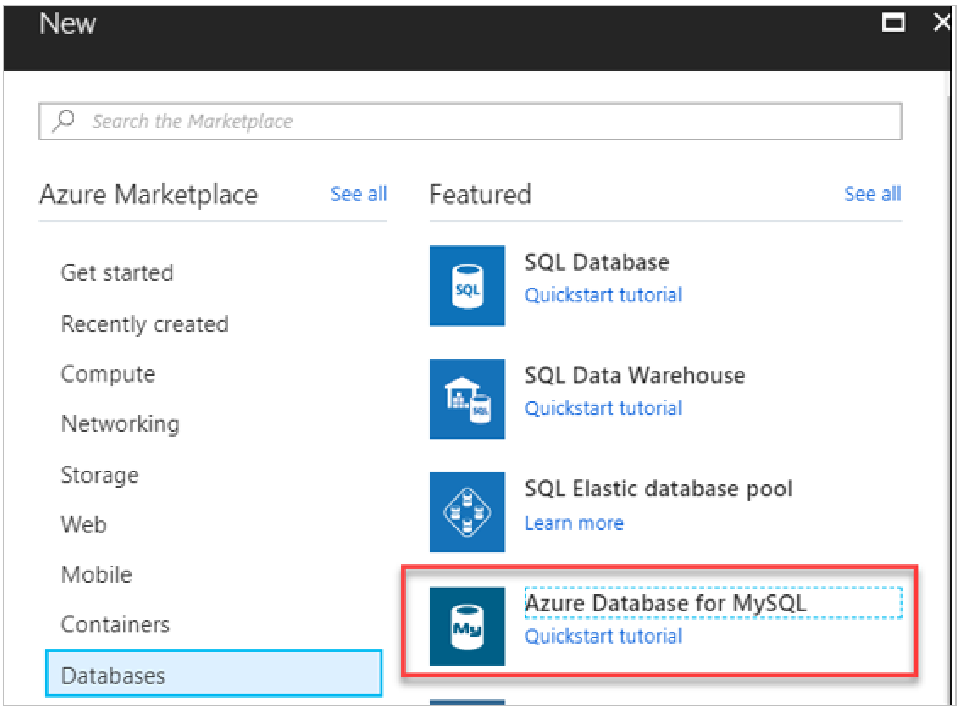
Need more help?

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

Step 3: Provision Azure Database for MySQL

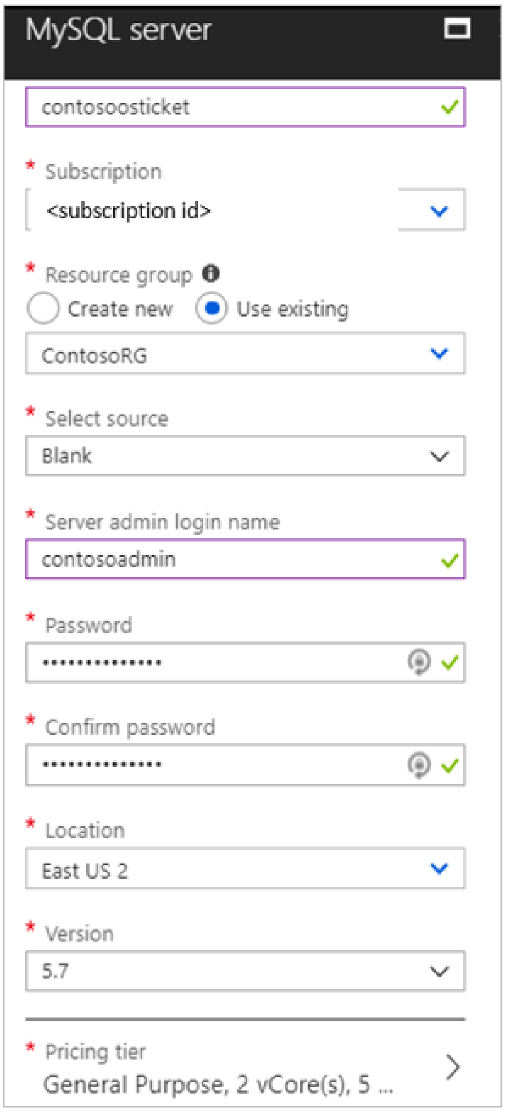
Contoso admins provision a MySQL database instance in the primary East US 2 region.

1. In the Azure portal, they create an Azure Database for MySQL resource.



2. They add the name **contosoosticket** for the Azure database. They add the database to the production resource group **ContosoRG**, and specify credentials for it.

3. The on-premises MySQL database is version 5.7, so they select this version for compatibility. They use the default sizes, which match their database requirements.



MySQL server

contosoosticket ✓

* Subscription: <subscription id>

* Resource group: ○ Create new ● Use existing

ContosoRG

* Select source: Blank

* Server admin login name: contosoadmin ✓

* Password: •••••••••••••• ✓

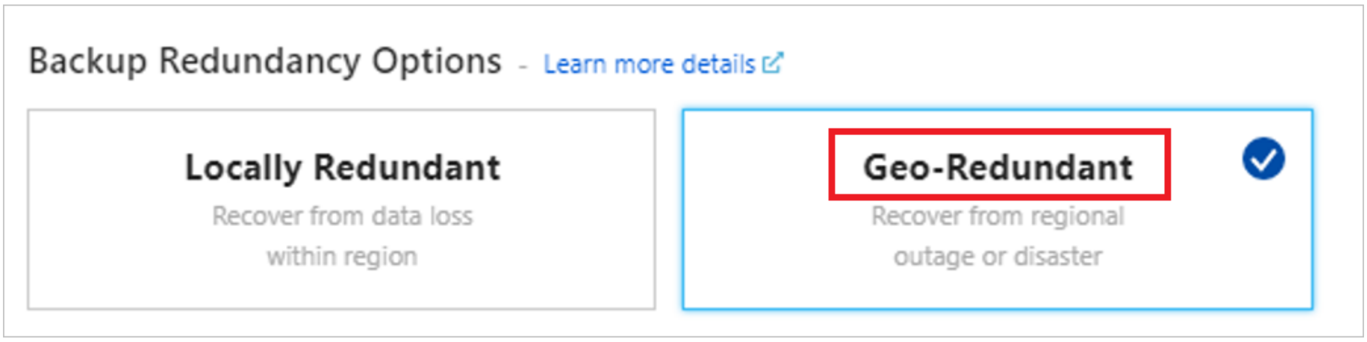
* Confirm password: •••••••••••••• ✓

* Location: East US 2

* Version: 5.7

* Pricing tier: General Purpose, 2 vCore(s), 5 ...

4. For **Backup Redundancy Options**, they select to use **Geo-Redundant**. This option allows them to restore the database in their secondary Central US region if an outage occurs. They can only configure this option when they provision the database.

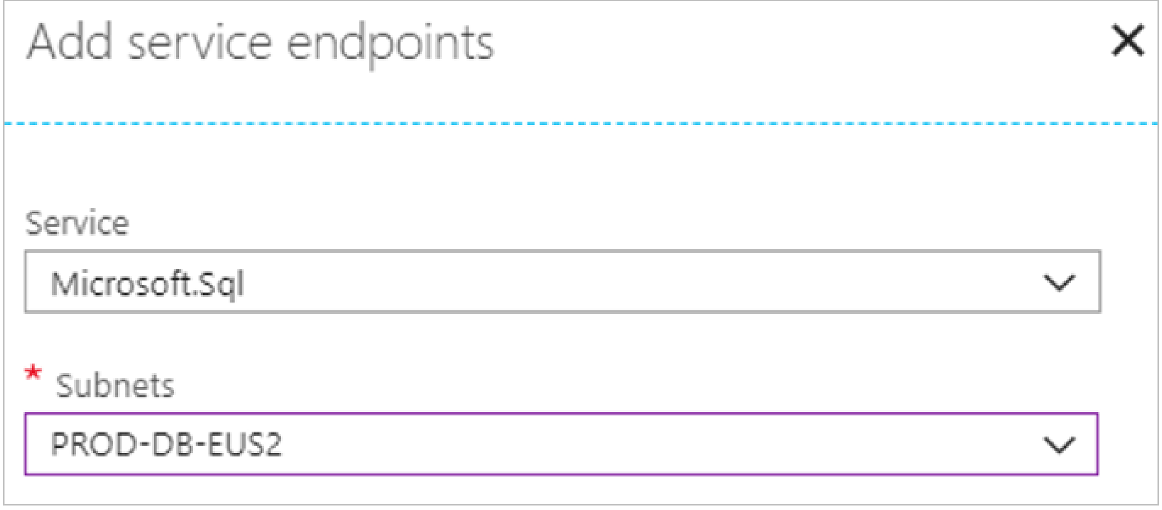


Backup Redundancy Options - Learn more details

Locally Redundant: Recover from data loss within region

Geo-Redundant ✓: Recover from regional outage or disaster

5. In the **VNET-PROD-EUS2** network > **Service endpoints**, they add a service endpoint (a database subnet) for the SQL service.



Add service endpoints

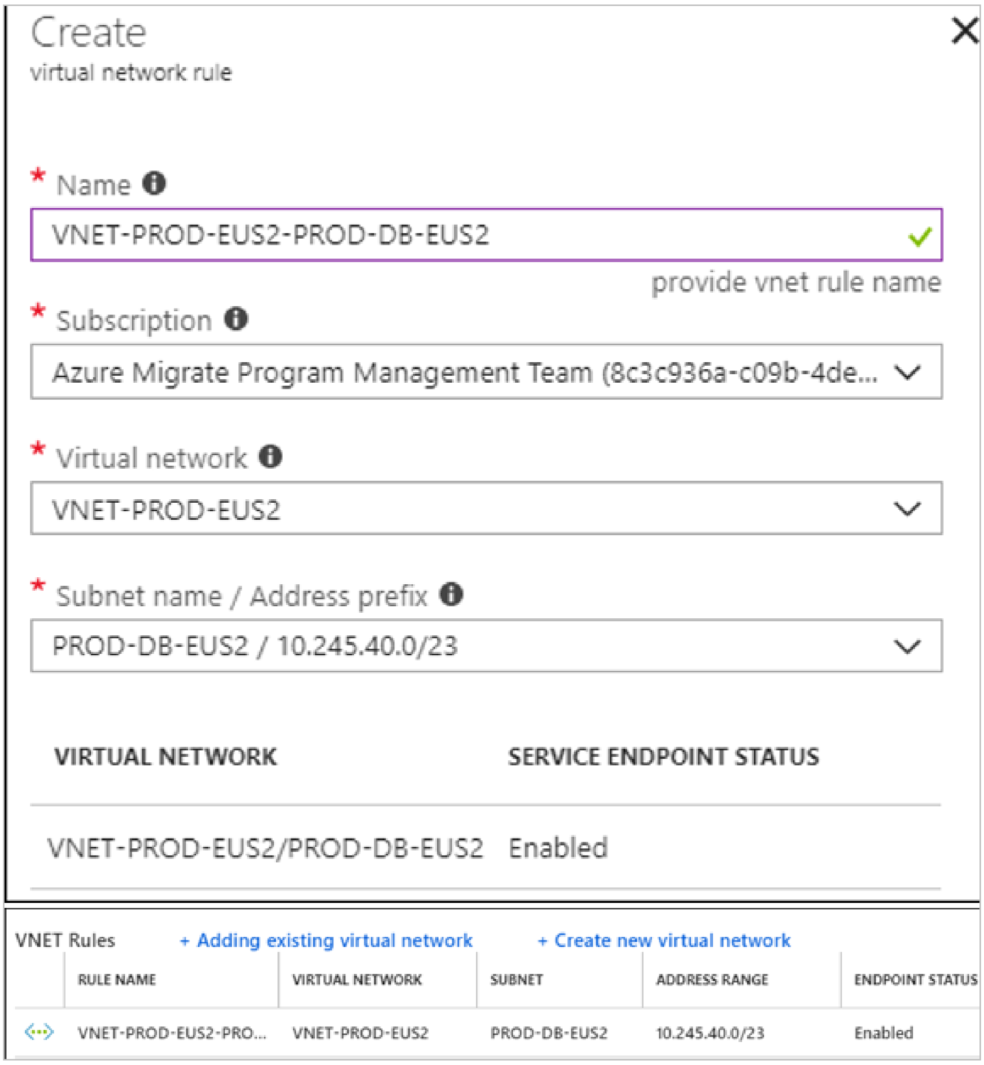
Service

Microsoft.Sql

* Subnets

PROD-DB-EUS2

6. After adding the subnet, they create a virtual network rule that allows access from the database subnet in the production network.



Create

virtual network rule

* Name

VNET-PROD-EUS2-PROD-DB-EUS2 ✓

provide vnet rule name

* Subscription

Azure Migrate Program Management Team (8c3c936a-c09b-4de...

* Virtual network

VNET-PROD-EUS2

* Subnet name / Address prefix

PROD-DB-EUS2 / 10.245.40.0/23

VIRTUAL NETWORK	SERVICE ENDPOINT STATUS
VNET-PROD-EUS2/PROD-DB-EUS2	Enabled

VNET Rules + Adding existing virtual network + Create new virtual network

	RULE NAME	VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS
<··>	VNET-PROD-EUS2-PRO...	VNET-PROD-EUS2	PROD-DB-EUS2	10.245.40.0/23	Enabled

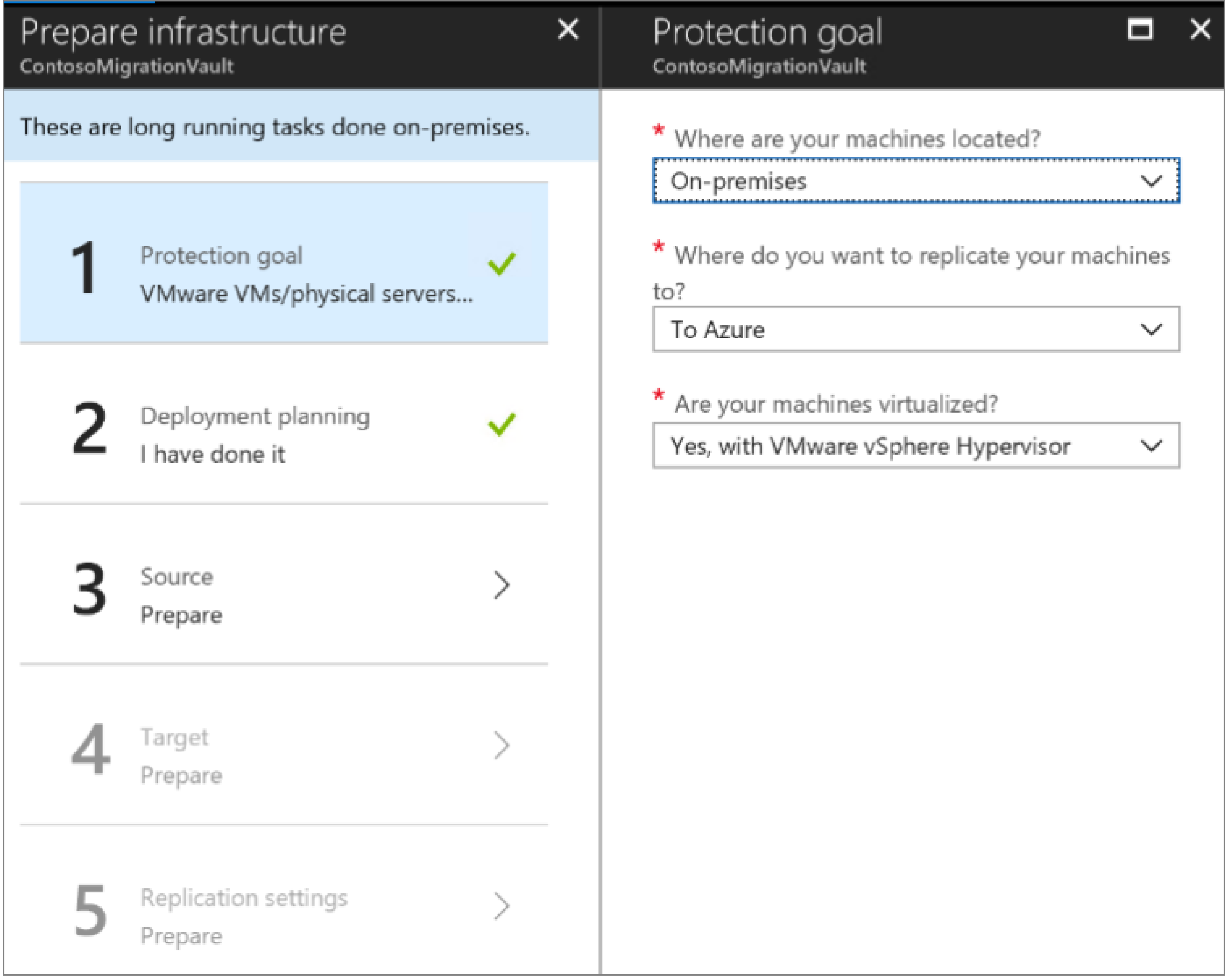
Step 4: Replicate the on-premises VMs

Before they can migrate the web VM to Azure, Contoso admins set up and enable replication.

Set a protection goal

1. In the vault, under the vault name (ContosoVMVault) they set a replication goal (**Getting Started** > **Site Recovery** > **Prepare infrastructure**.

2. They specify that their machines are located on-premises, that they're VMware VMs, and that they want to replicate to Azure.



Prepare infrastructure
ContosoMigrationVault

These are long running tasks done on-premises.

1 Protection goal
VMware VMs/physical servers... ✓

2 Deployment planning
I have done it ✓

3 Source
Prepare

4 Target
Prepare

5 Replication settings
Prepare

Protection goal
ContosoMigrationVault

* Where are your machines located?
On-premises

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

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

Confirm deployment planning

To continue, they confirm that they've completed deployment planning, by selecting **Yes, I have done it**. Contoso are only migrating a single VM in this scenario, and don't need deployment planning.

Set up the source environment

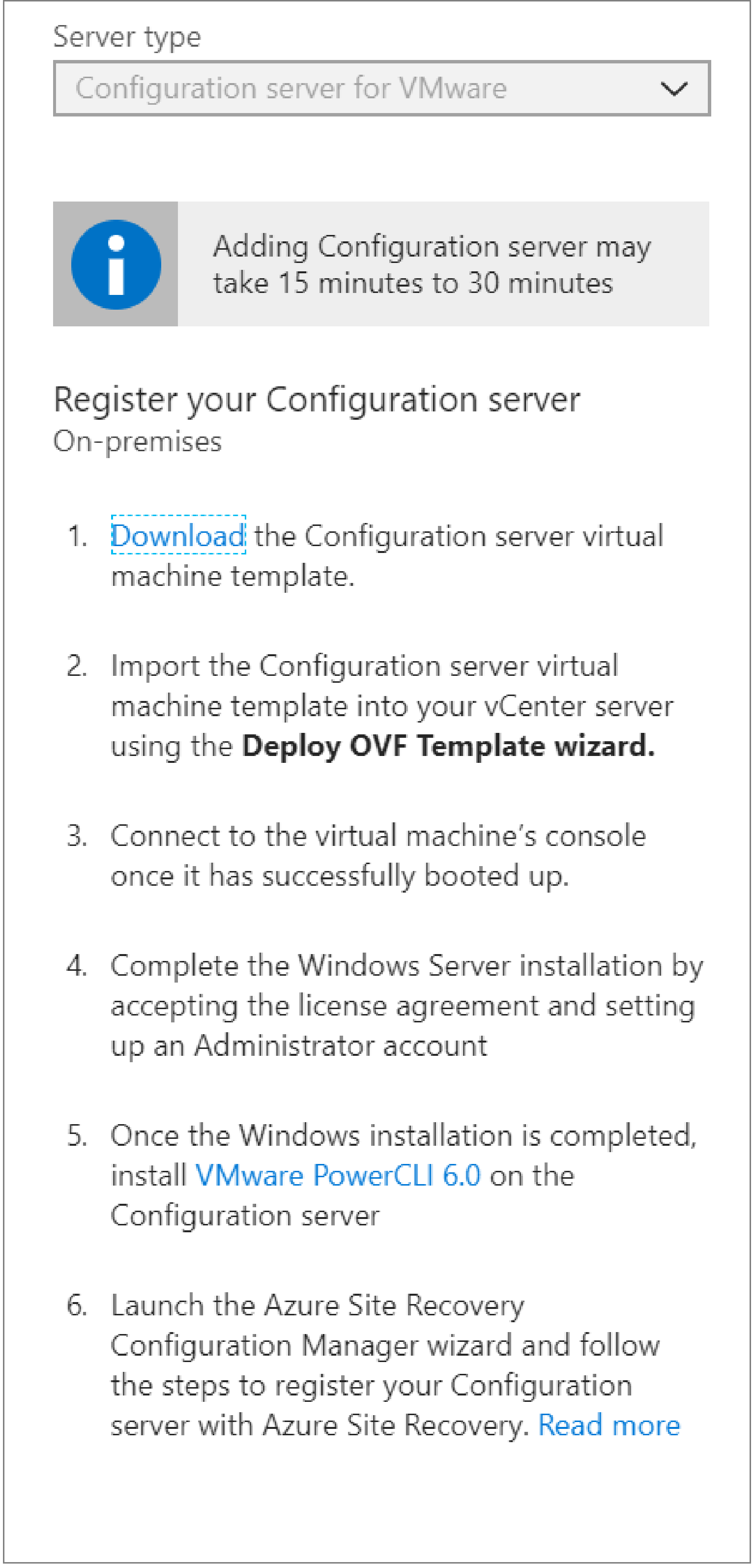
Contoso admins now configure the source environment. To do this, using an OVF template they deploy a Site Recovery configuration server as a highly available, on-premises VMware VM. After the configuration server is up and running, they register it in the vault.

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 do this as follows:

1. They download the OVF template from **Prepare Infrastructure** > **Source** > **Configuration Server**.



Server type

Configuration server for VMware

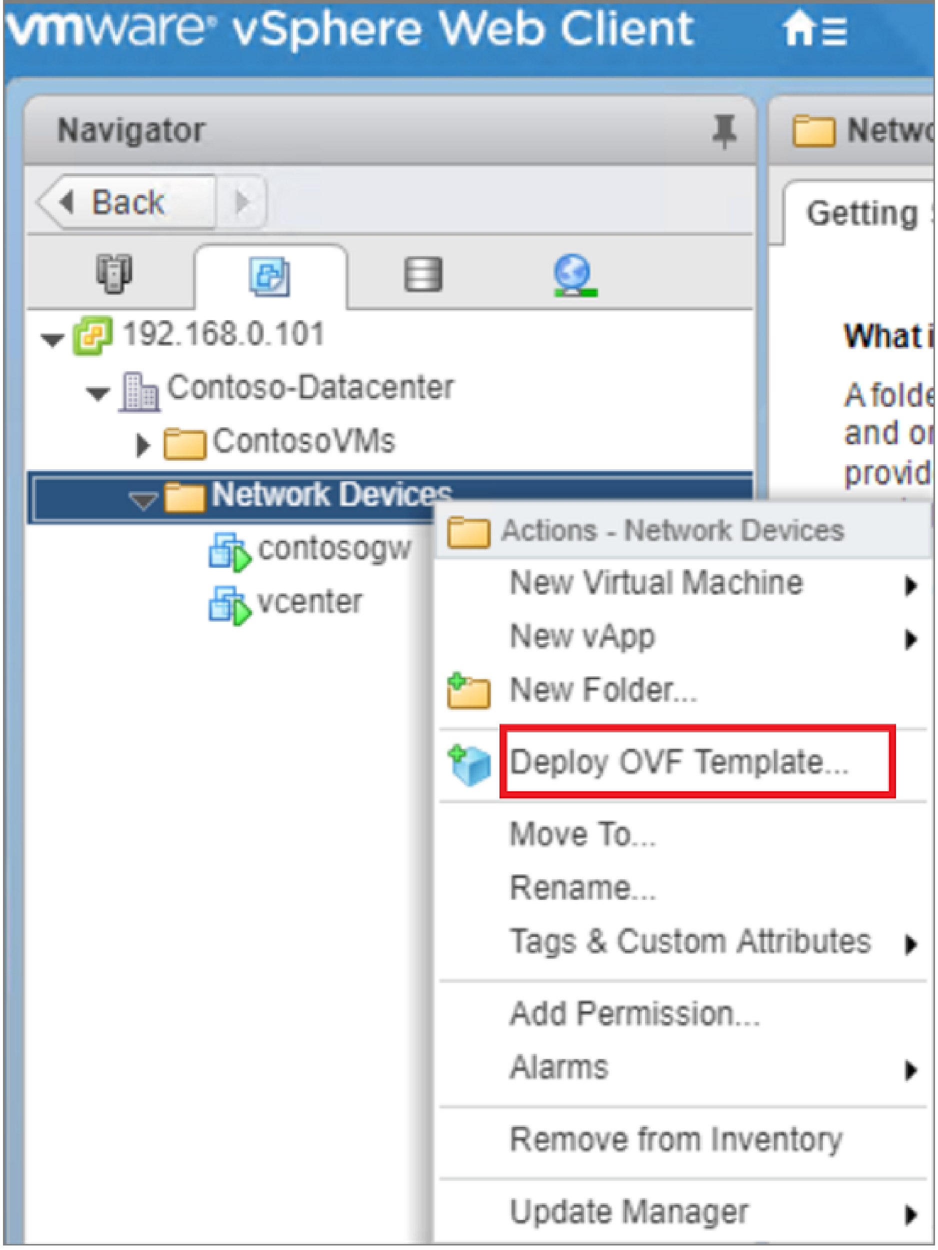
Adding Configuration server may take 15 minutes to 30 minutes

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 the VM, and deploy the VM.



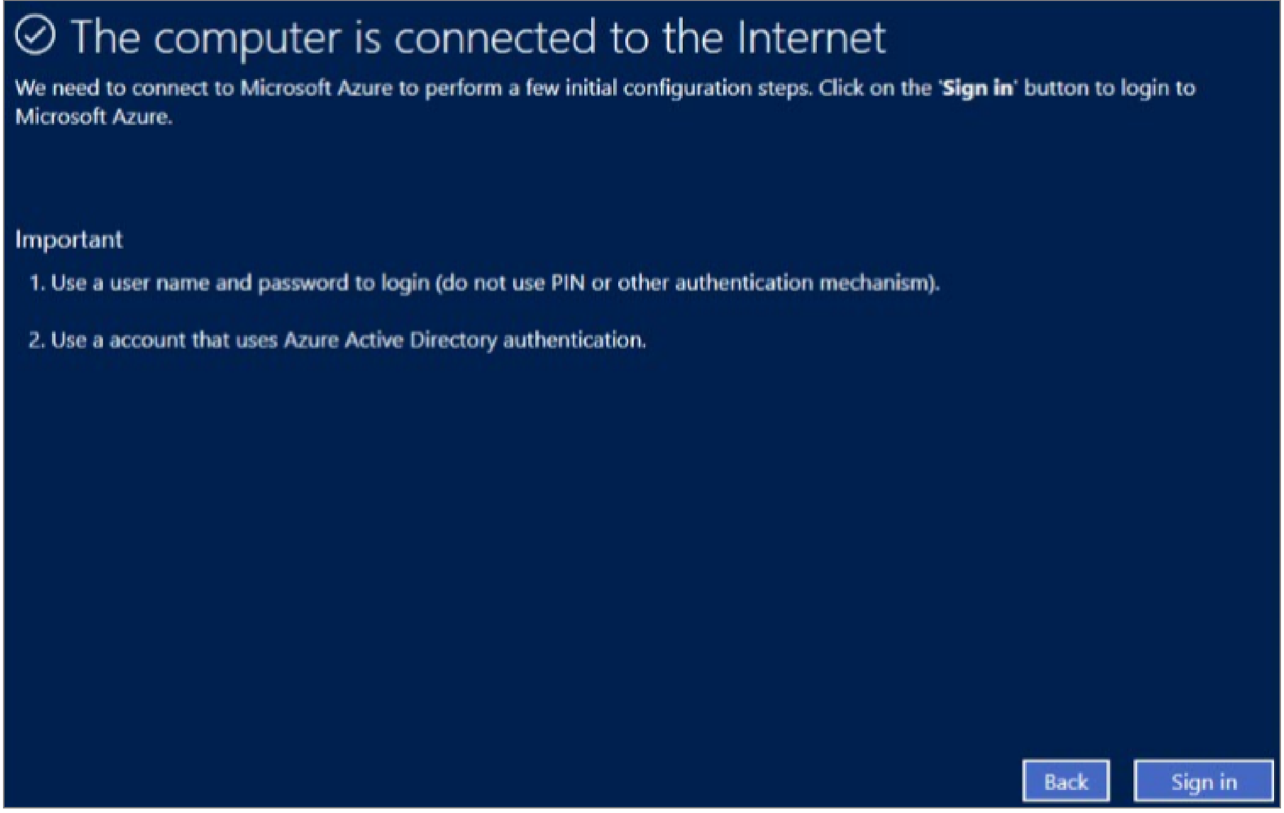
3. When they turn on the VM for the first time, it boots up into a Windows Server 2016 installation experience. They accept the license agreement, and enter an administrator password.

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 use for registering the configuration server in the vault.

6. The tool checks that the VM can connect to Azure.

7. 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.



The computer is connected to the Internet

We need to connect to Microsoft Azure to perform a few initial configuration steps. Click on the '**Sign in**' button to login to Microsoft Azure.

Important

1. Use a user name and password to login (do not use PIN or other authentication mechanism).

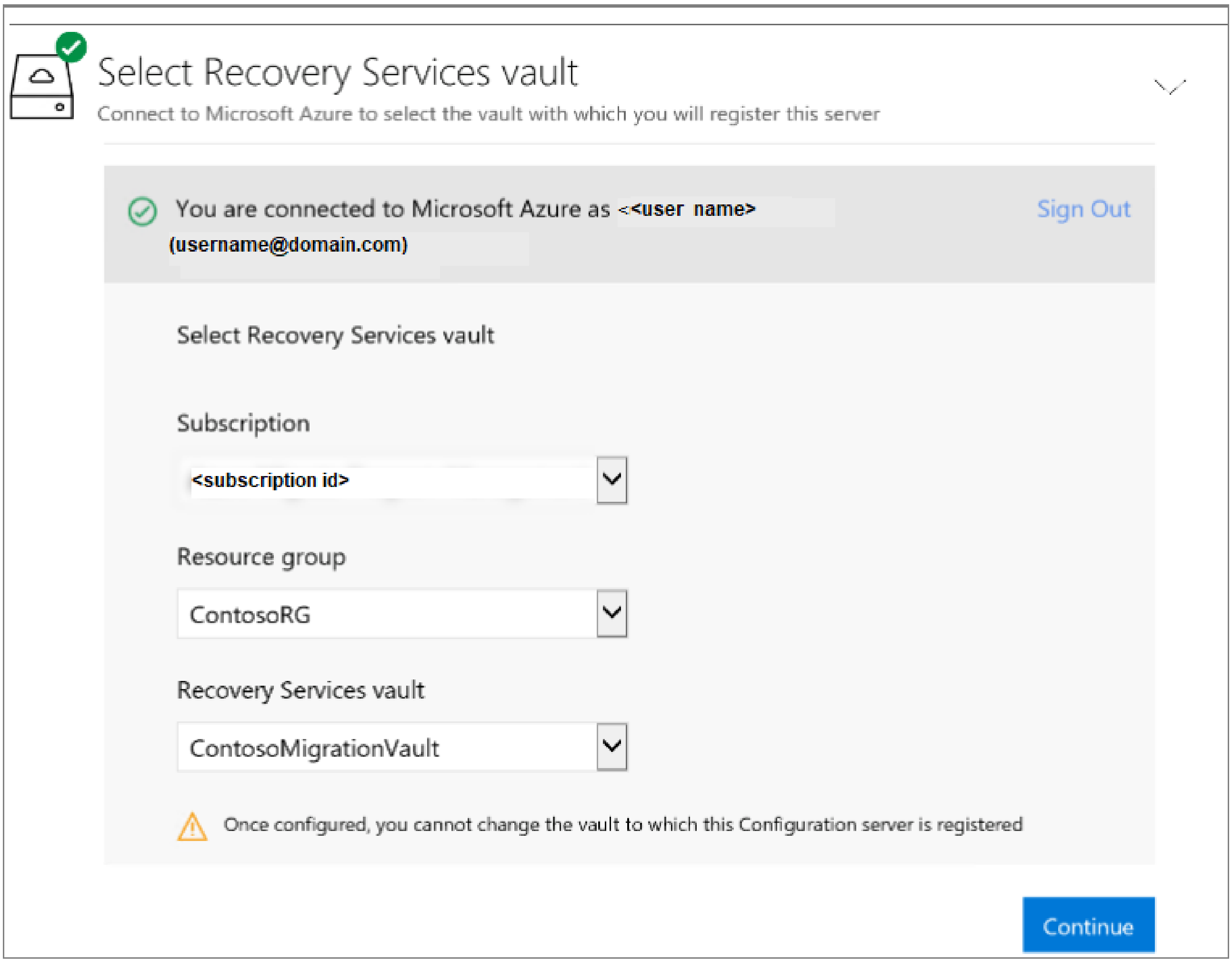
2. Use a account that uses Azure Active Directory authentication.

8. The tool performs some configuration tasks and then reboots.

9. They sign in to the machine again, and the Configuration Server Management Wizard starts automatically.

10. In the wizard, they select the NIC to receive replication traffic. This setting can't be changed after it's configured.

11. They select the subscription, resource group, and vault in which to register the configuration server.



Select Recovery Services vault

Connect to Microsoft Azure to select the vault with which you will register this server

You are connected to Microsoft Azure as <<user name> (username@domain.com)

Select Recovery Services vault

Subscription

<subscription id>

Resource group

ContosoRG

Recovery Services vault

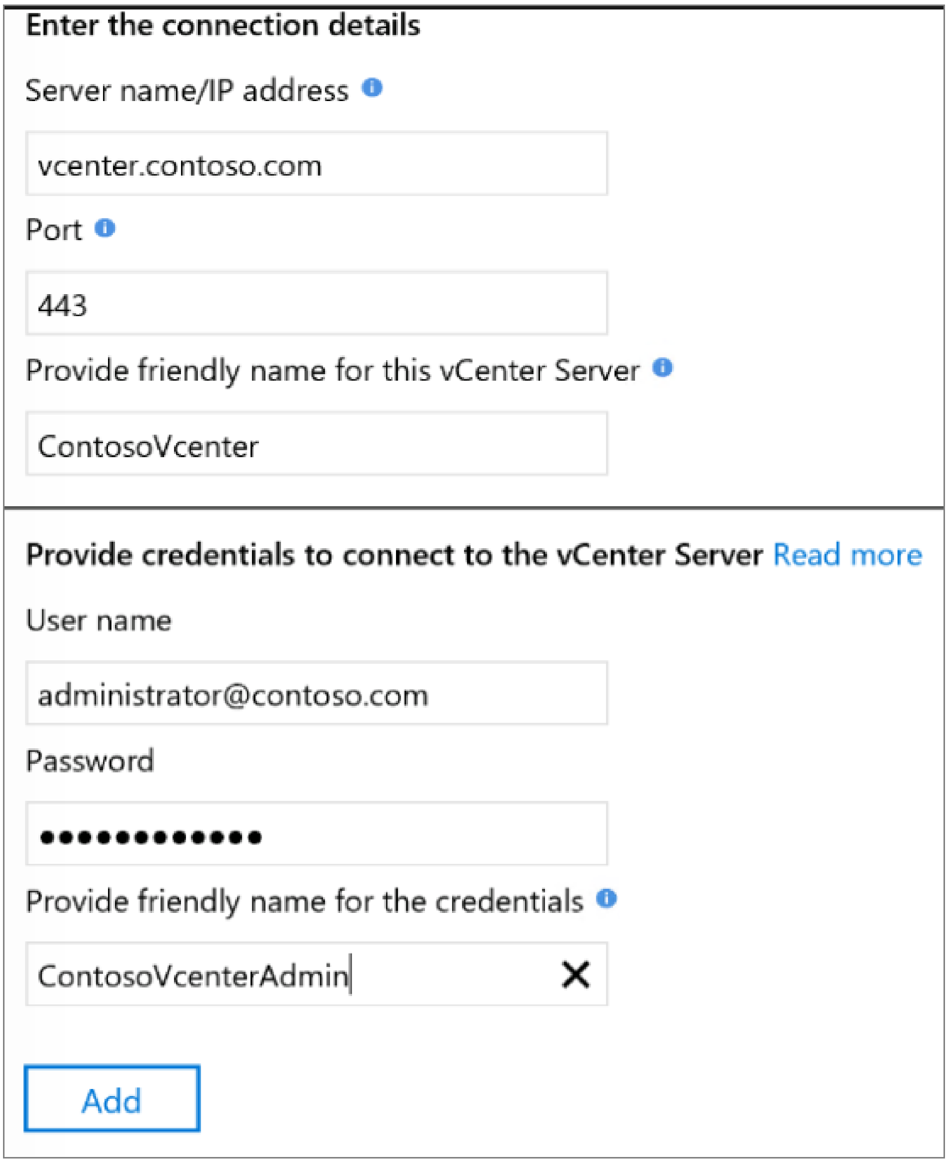
ContosoMigrationVault

Once configured, you cannot change the vault to which this Configuration server is registered

12. Now, they download and install MySQL Server, and VMware PowerCLI.

13. 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 vCenter server.

14. They input the account that they created for automatic discovery, and the credentials that Site Recovery will use to automatically install the Mobility Service.



Enter the connection details

Server name/IP address: vcenter.contoso.com

Port: 443

Provide friendly name for this vCenter Server: ContosoVcenter

Provide credentials to connect to the vCenter Server Read more

User name: administrator@contoso.com

Password: ●●●●●●●●●●●●●

Provide friendly name for the credentials: ContosoVcenterAdmin

15. After registration finishes, in the Azure portal, they check that the configuration server and VMware server are listed on the **Source** page in the vault. Discovery can take 15 minutes or more.

16. With everything in place, Site Recovery connects to VMware servers, and discovers VMs.

Set up the target

Now Contoso admins input 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.

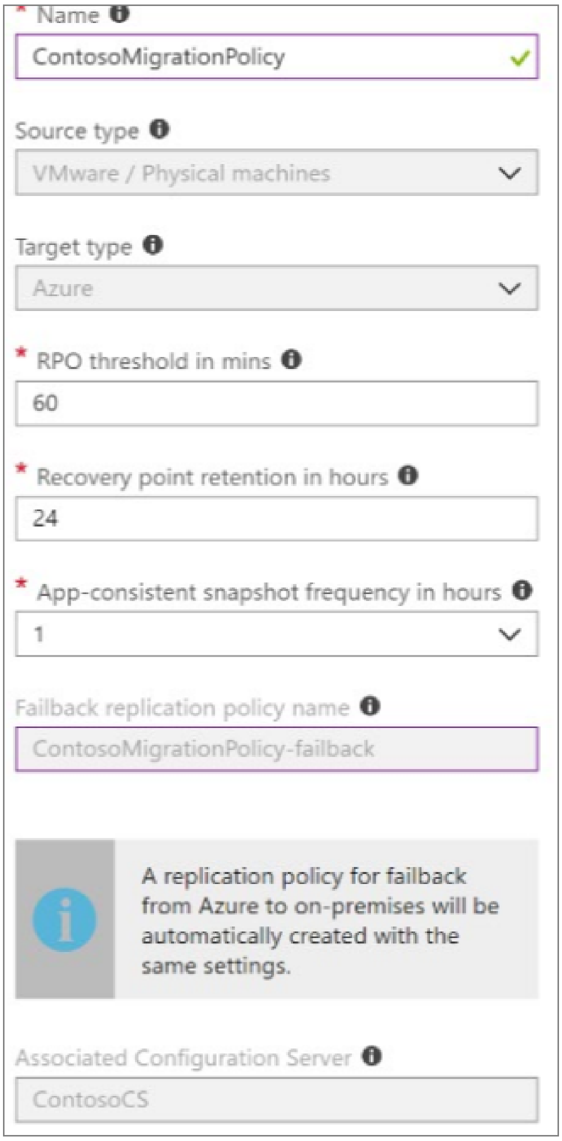
Create a replication policy

With the source and target set up, Contoso admins are ready to 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

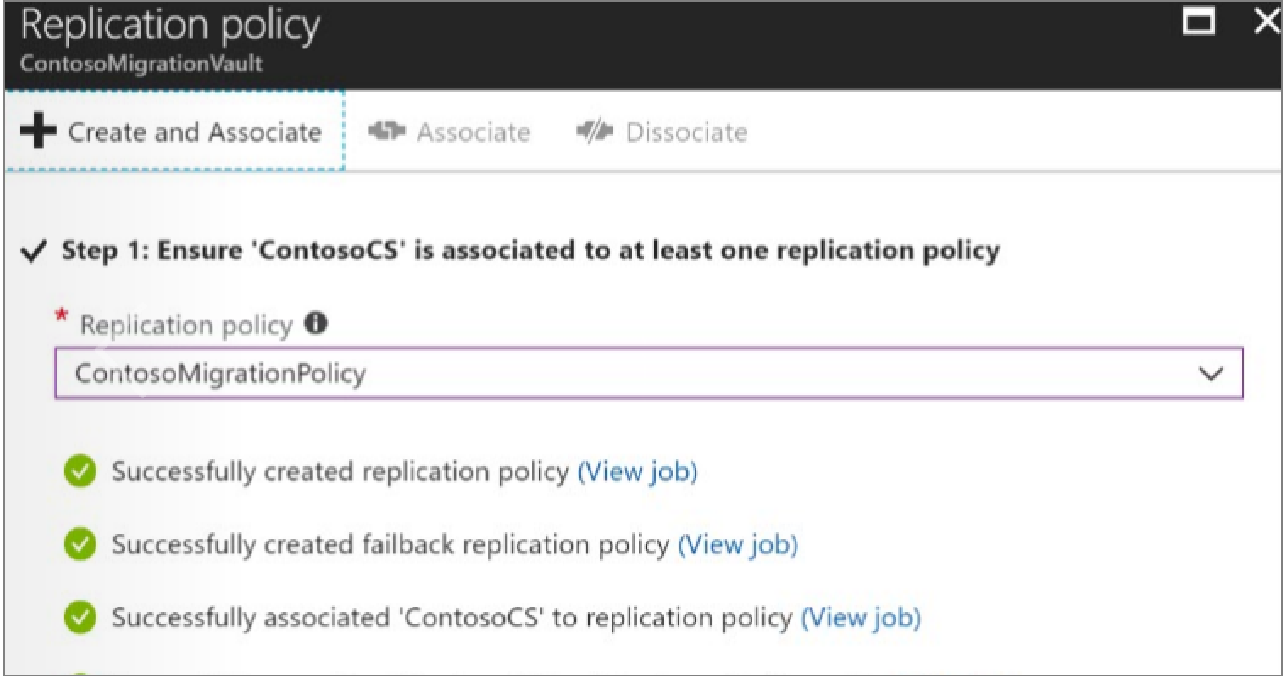
* App-consistent snapshot frequency in hours
1

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.



Replication policy
ContosoMigrationVault

✓ Step 1: Ensure 'ContosoCS' is associated to at least one replication policy

* Replication policy: ContosoMigrationPolicy

✓ Successfully created replication policy (View job)

✓ Successfully created failback replication policy (View job)

✓ Successfully associated 'ContosoCS' to replication policy (View job)

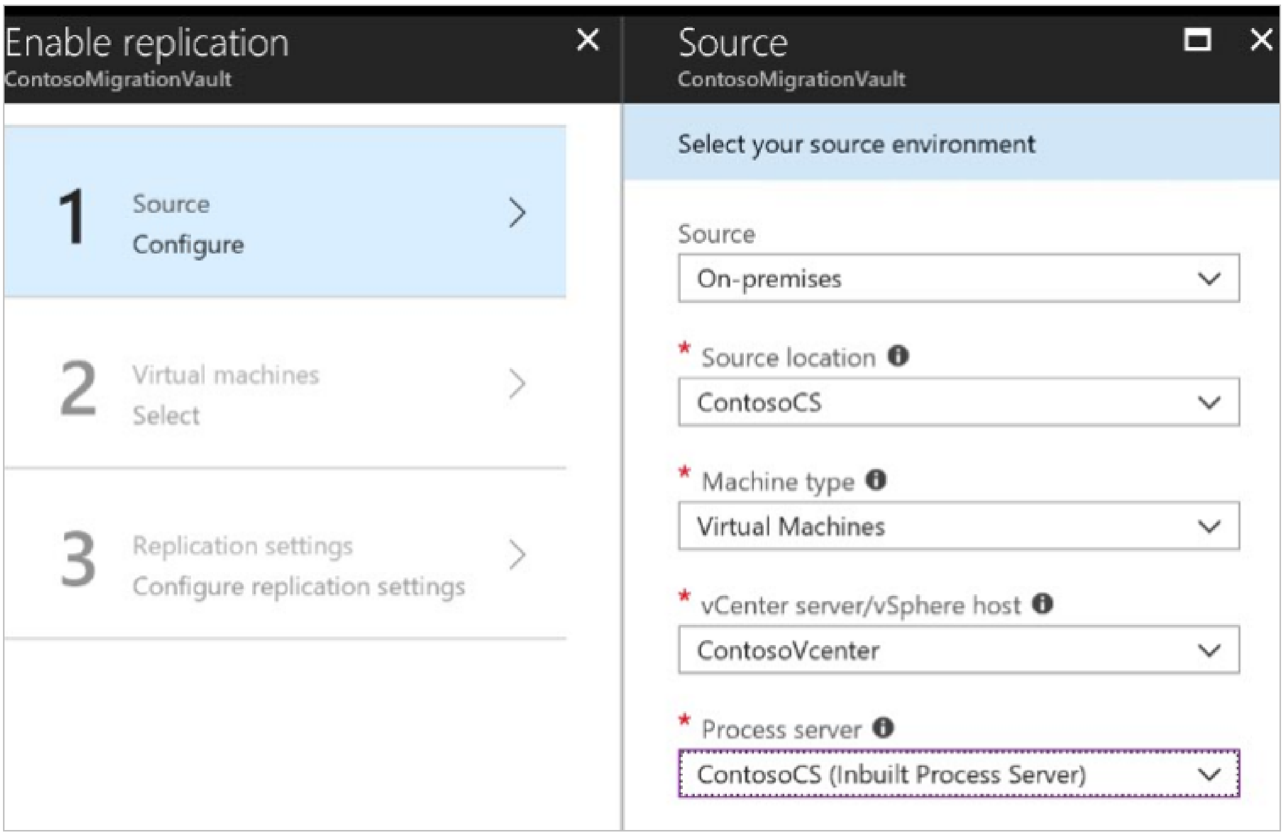
Need more help?

- 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.
- Learn more about the Azure Guest agent for Linux.

Enable replication for the Web VM

Now Contoso admins can start replicating the **OSTICKETWEB** VM.

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



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

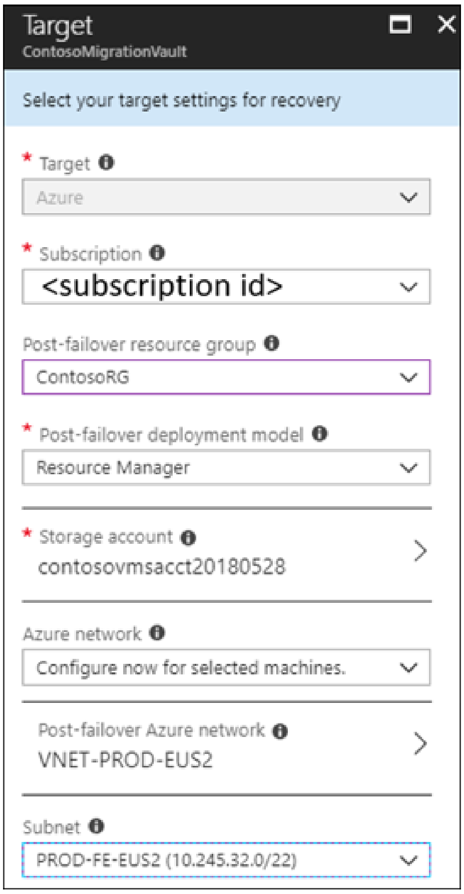
* Source location: ContosoCS

* Machine type: Virtual Machines

* vCenter server/vSphere host: ContosoVcenter

* Process server: ContosoCS (Inbuilt Process Server)

3. Now they specify the target settings. These include the resource group and network in which the Azure VM will be located after failover, and the storage account in which replicated data will be stored.



Target
ContosoMigrationVault

Select your target settings for recovery

* Target: Azure

* Subscription: <subscription id>

Post-failover resource group: ContosoRG

* Post-failover deployment model: Resource Manager

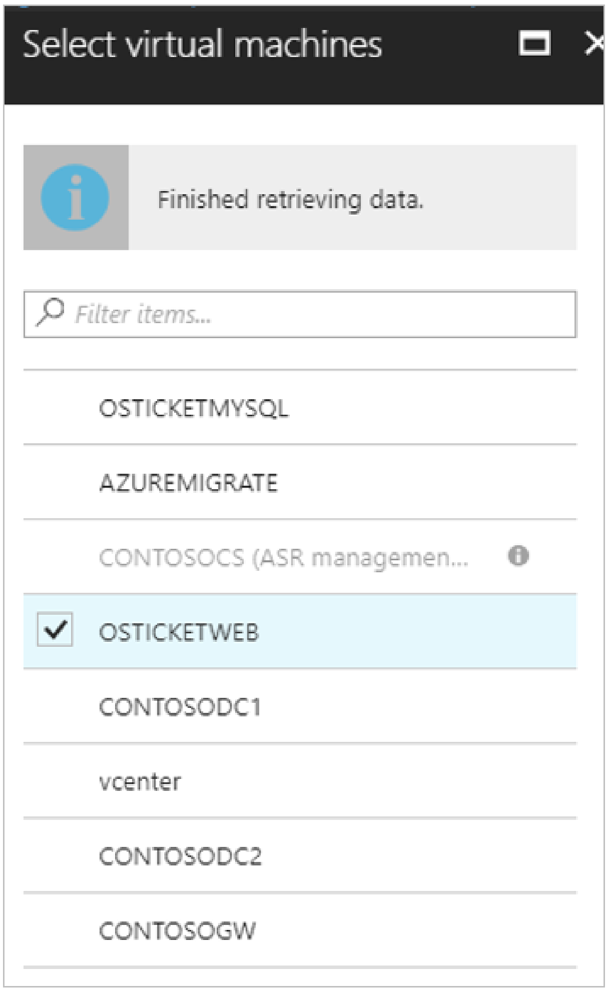
* Storage account: contosovmsacct20180528

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 **OSTICKETWEB** for replication.



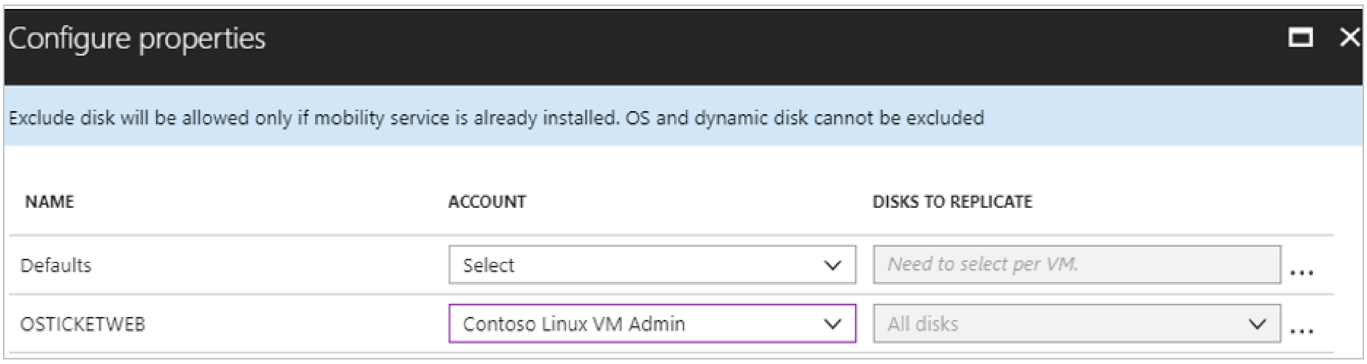
Select virtual machines

Finished retrieving data.

Filter items...

- OSTICKETMYSQL
- AZUREMIGRATE
- CONTOSOCS (ASR managemen...
- ☑ OSTICKETWEB
- CONTOSODC1
- vcenter
- CONTOSODC2
- CONTOSOGW

5. In the VM properties, they select the account that should be used to automatically install the Mobility Service on the VM.



Configure properties

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

NAME	ACCOUNT	DISKS TO REPLICATE
Defaults	Select	Need to select per VM.
OSTICKETWEB	Contoso Linux VM Admin	All disks

6. in **Replication settings** > **Configure replication settings**, they check that the correct replication policy is applied, and select **Enable Replication**. The Mobility service will be automatically installed.

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

Need more help?

You can read a full walkthrough of all these steps in Enable replication.

Step 5: Migrate the database

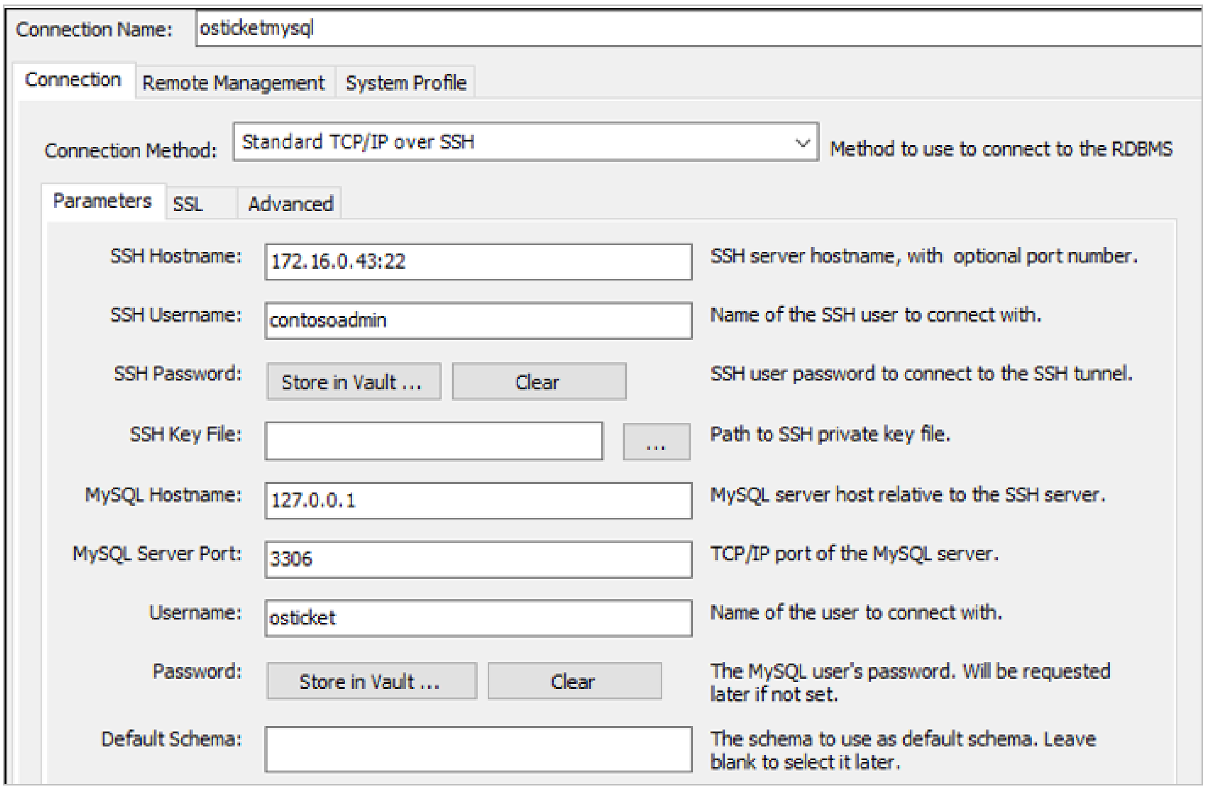
Contoso admins migrate the database using backup and restore, with MySQL tools. They install MySQL Workbench, back up the database from OSTICKETMYSQL, and then restore it to Azure Database for MySQL Server.

Install MySQL Workbench

1. They check the prerequisites and downloads MySQL Workbench.

2. They install MySQL Workbench for Windows in accordance with the installation instructions.

3. In MySQL Workbench, they create a MySQL connection to OSTICKETMYSQL.



Connection Name: osticketmysql

Connection Method: Standard TCP/IP over SSH — Method to use to connect to the RDBMS

SSH Hostname: 172.16.0.43:22 — SSH server hostname, with optional port number.

SSH Username: contosoadmin — Name of the SSH user to connect with.

SSH Password: — SSH user password to connect to the SSH tunnel.

SSH Key File: — Path to SSH private key file.

MySQL Hostname: 127.0.0.1 — MySQL server host relative to the SSH server.

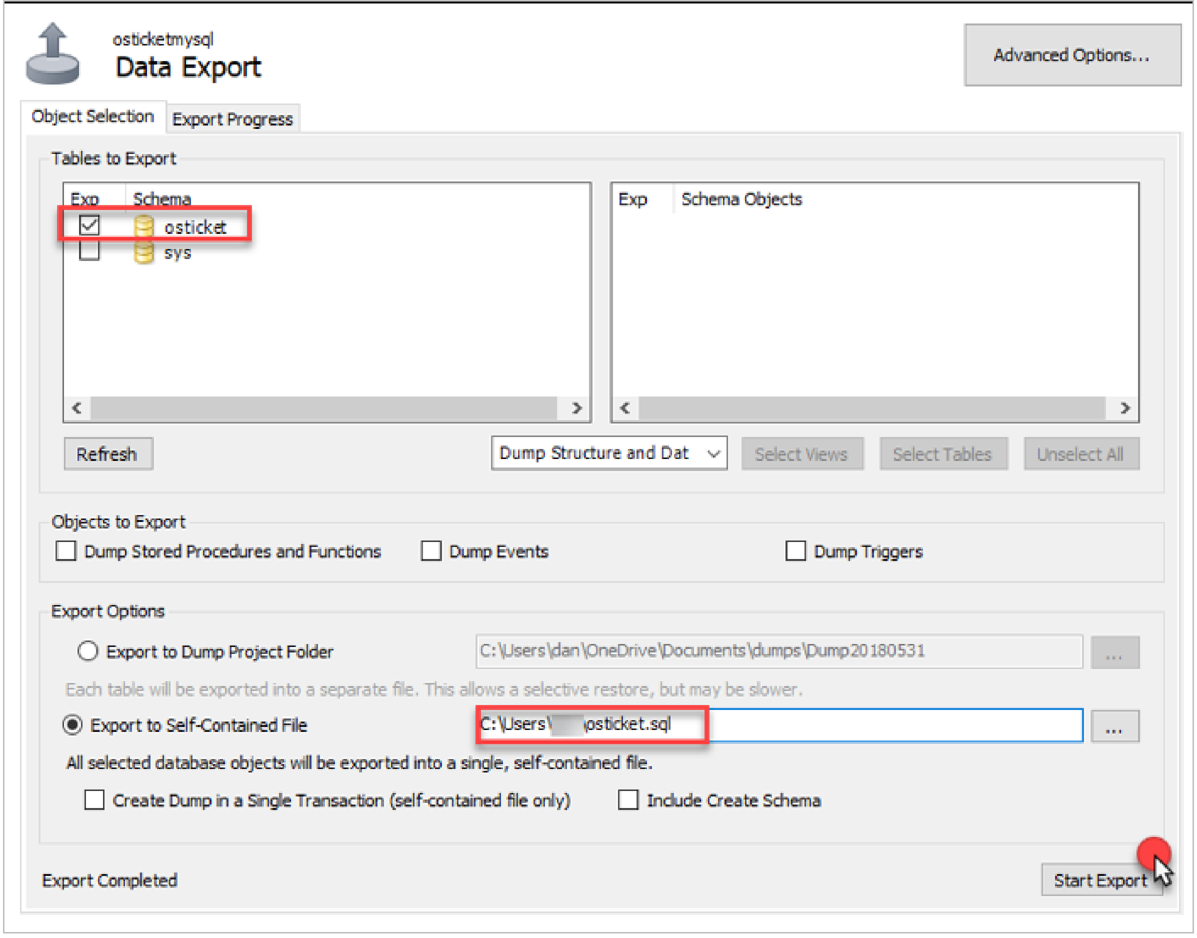
MySQL Server Port: 3306 — TCP/IP port of the MySQL server.

Username: osticket — Name of the user to connect with.

Password: — The MySQL user's password. Will be requested later if not set.

Default Schema: — The schema to use as default schema. Leave blank to select it later.

4. They export the database as **osticket**, to a local self-contained file.



osticketmysql

Data Export

Advanced Options...

Object Selection | Export Progress

Tables to Export

Exp	Schema
☑	osticket
□	sys

Exp	Schema Objects

Refresh | Dump Structure and Dat | Select Views | Select Tables | Unselect All

Objects to Export

□ Dump Stored Procedures and Functions □ Dump Events □ Dump Triggers

Export Options

○ Export to Dump Project Folder C:\Users\dan\OneDrive\Documents\dumps\Dump20180531

Each table will be exported into a separate file. This allows a selective restore, but may be slower.

● Export to Self-Contained File C:\Users\[redacted]\osticket.sql

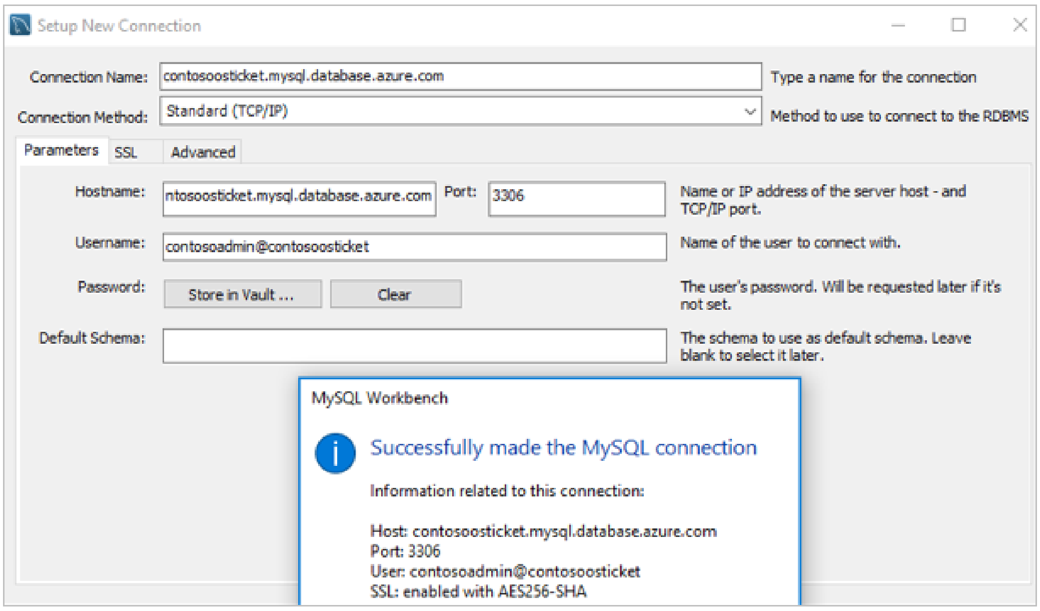
All selected database objects will be exported into a single, self-contained file.

□ Create Dump in a Single Transaction (self-contained file only) □ Include Create Schema

Export Completed

Start Export

5. After the database has been backed up locally, they create a connection to the Azure Database for MySQL instance.



Setup New Connection

Connection Name: contosoosticket.mysql.database.azure.com Type a name for the connection

Connection Method: Standard (TCP/IP) Method to use to connect to the RDBMS

Parameters | SSL | Advanced

Hostname: ntosoosticket.mysql.database.azure.com Port: 3306 Name or IP address of the server host - and TCP/IP port.

Username: contosoadmin@contosoosticket Name of the user to connect with.

Password: Store in Vault ... Clear The user's password. Will be requested later if it's not set.

Default Schema: The schema to use as default schema. Leave blank to select it later.

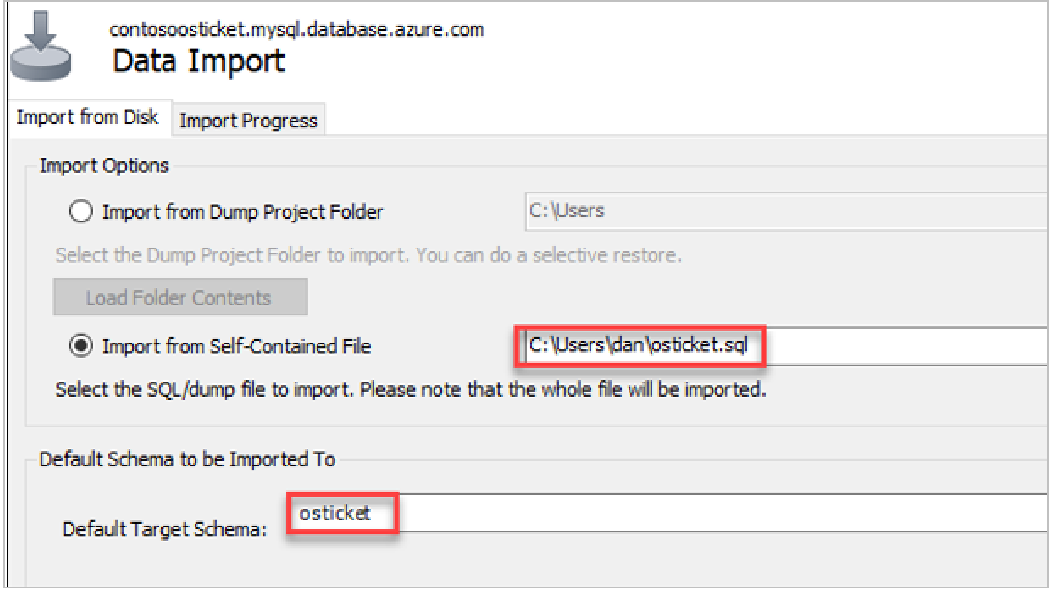
MySQL Workbench

Successfully made the MySQL connection

Information related to this connection:

Host: contosoosticket.mysql.database.azure.com
Port: 3306
User: contosoadmin@contosoosticket
SSL: enabled with AES256-SHA

6. Now, they can import (restore) the database in the Azure Database for MySQL instance, from the self-contained file. A new schema (osticket) is created for the instance.



contosoosticket.mysql.database.azure.com

Data Import

Import Options

○ Import from Dump Project Folder C:\Users

Select the Dump Project Folder to import. You can do a selective restore.

● Import from Self-Contained File C:\Users\dan\osticket.sql

Select the SQL/dump file to import. Please note that the whole file will be imported.

Default Schema to be Imported To

Default Target Schema: osticket

Step 6: Migrate the VMs with Site Recovery

Finally, Contoso admins run a quick test failover, and then migrate the VM.

Run a test failover

Running a test failover helps verify that everything's working as expected, before the migration.

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.

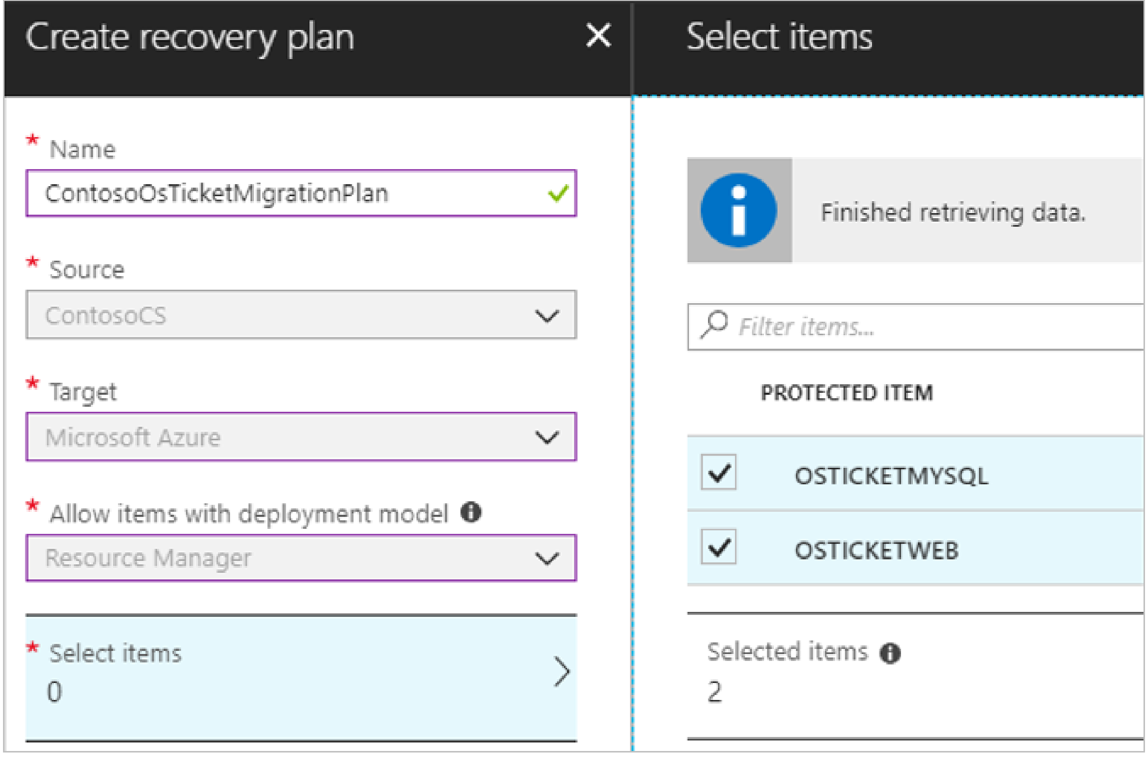
4. After the failover finishes, the replica Azure VM appears in the Azure portal. They check that the VM is the appropriate size, that it's connected to the right network, and that it's running.

5. After verifying, they clean up the failover, and record and save any observations.

Migrate the VM

To migrate the VM, Contoso admins creates a recovery plan that includes the VM, and fail over the plan to Azure.

1. They create a plan, and add **OSTICKETWEB** to it.


Create recovery plan

* Name
ContosoOsTicketMigrationPlan

* Source
ContosoCS

* Target
Microsoft Azure

* Allow items with deployment model
Resource Manager

* Select items
0

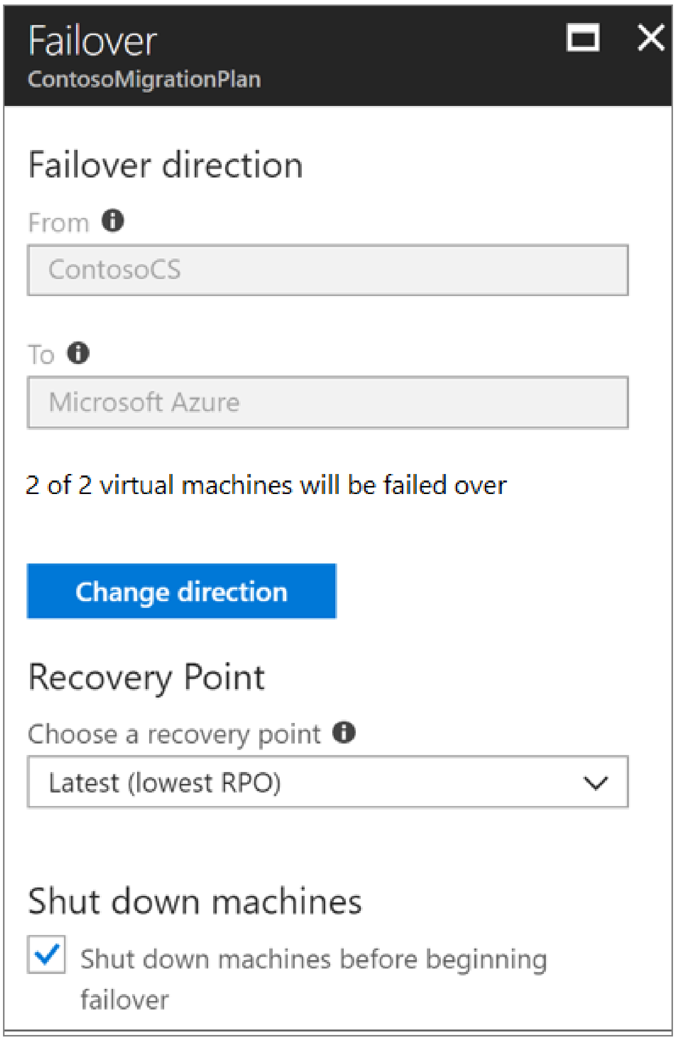
Select items

Finished retrieving data.

PROTECTED ITEM
☑ OSTICKETMYSQL
☑ OSTICKETWEB

Selected items
2

2. They run a failover on the plan. They select the latest recovery point, and specify 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

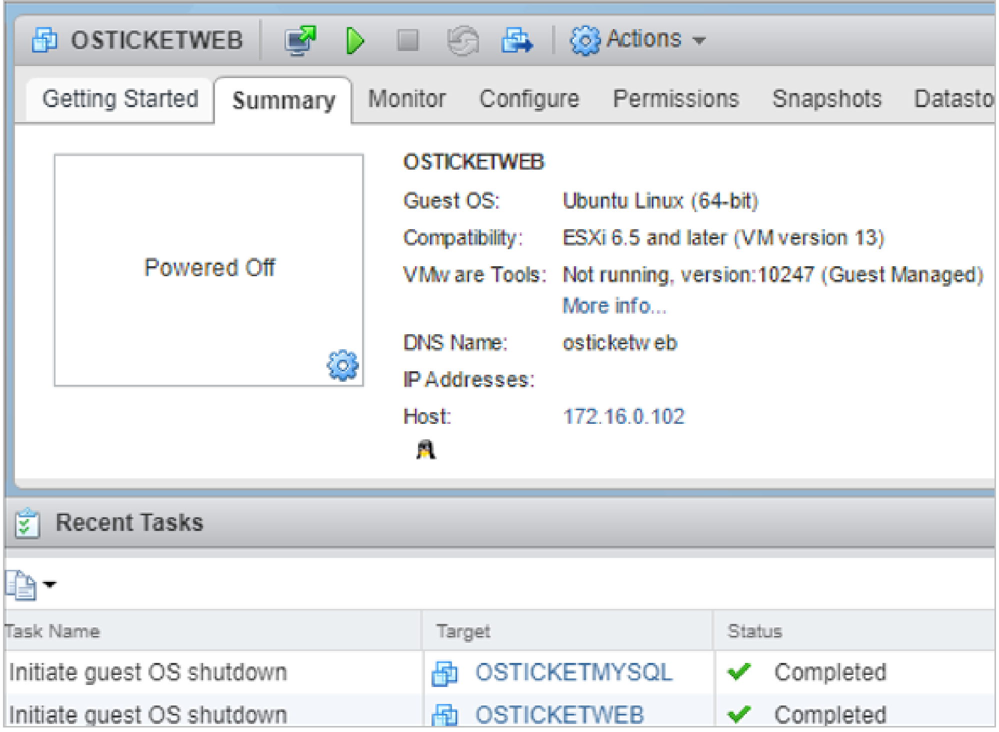
Recovery Point

Choose a recovery point
Latest (lowest RPO)

Shut down machines

☑ Shut down machines before beginning failover

3. During the failover, vCenter Server issues commands to stop the two VMs running on the ESXi host.



OSTICKETWEB

Guest OS: Ubuntu Linux (64-bit)

Compatibility: ESXi 6.5 and later (VM version 13)

VMware Tools: Not running, version:10247 (Guest Managed)
More info...

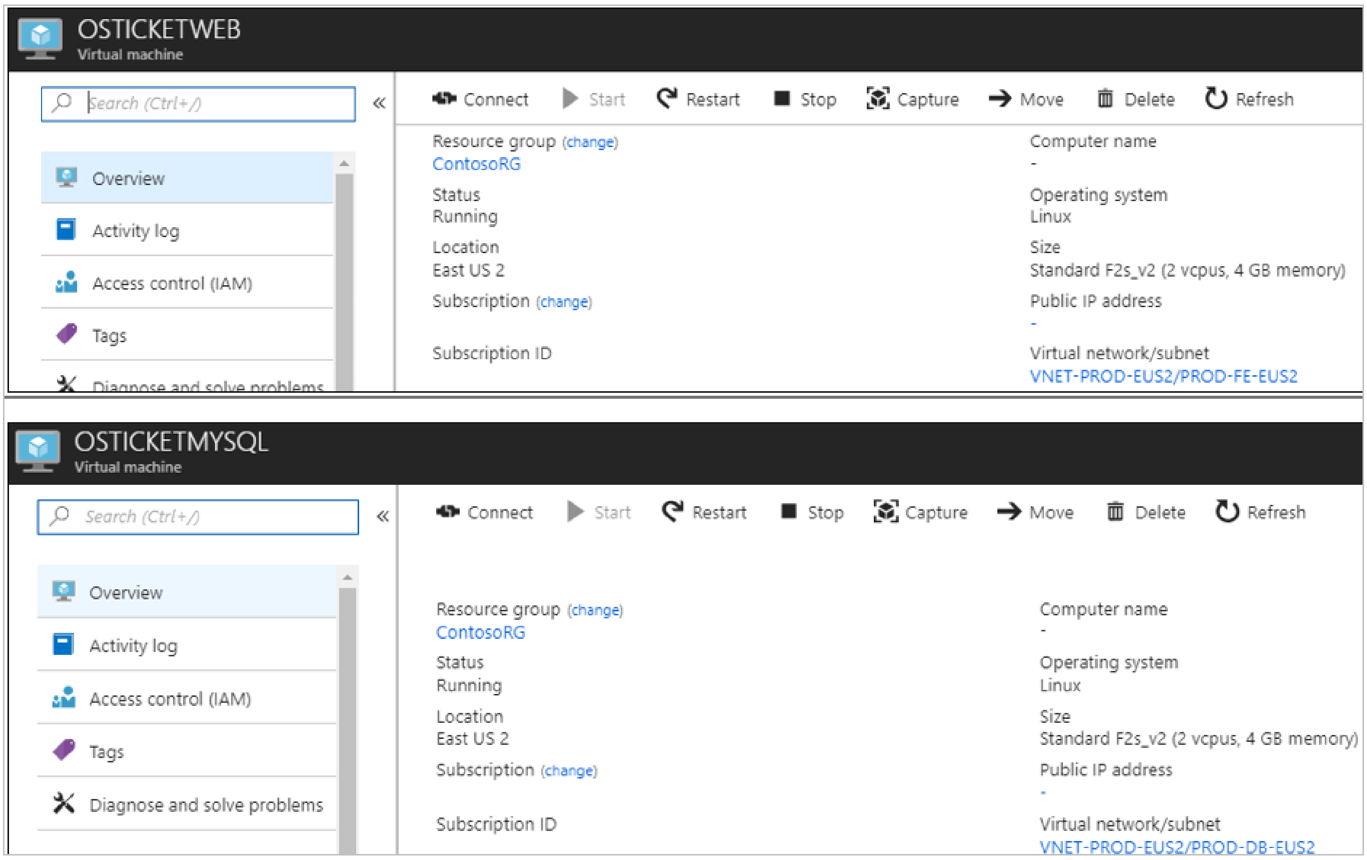
DNS Name: osticketweb

IP Addresses:

Host: 172.16.0.102

Task Name	Target	Status
Initiate guest OS shutdown	OSTICKETMYSQL	✓ Completed
Initiate guest OS shutdown	OSTICKETWEB	✓ Completed

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



Resource group (change)
ContosoRG

Status
Running

Location
East US 2

Subscription (change)

Subscription ID

Computer name
-

Operating system
Linux

Size
Standard F2s_v2 (2 vcpus, 4 GB memory)

Public IP address
-

Virtual network/subnet
VNET-PROD-EUS2/PROD-FE-EUS2

Resource group (change)
ContosoRG

Status
Running

Location
East US 2

Subscription (change)

Subscription ID

Computer name
-

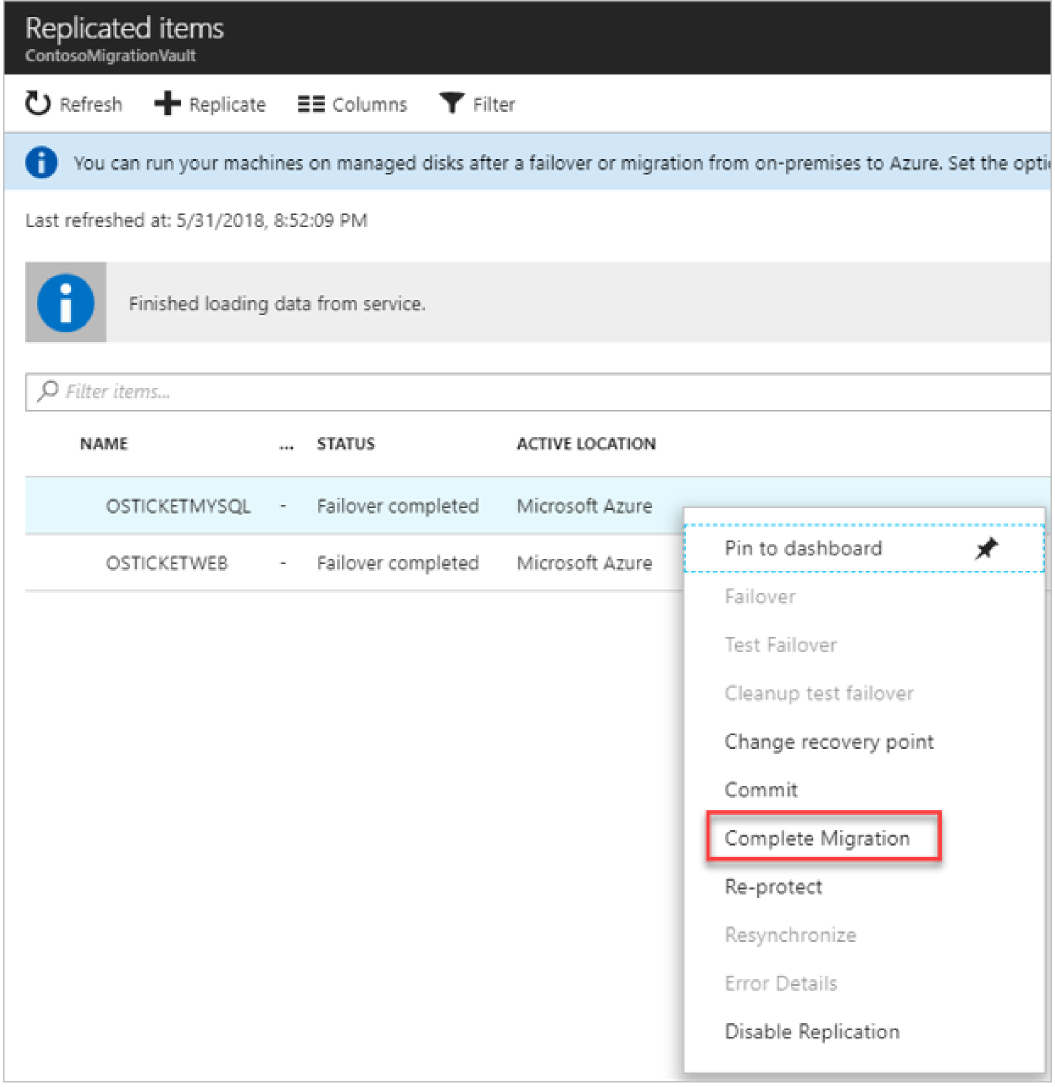
Operating system
Linux

Size
Standard F2s_v2 (2 vcpus, 4 GB memory)

Public IP address
-

Virtual network/subnet
VNET-PROD-EUS2/PROD-DB-EUS2

5. After checking the VM, they complete the migration. This stops replication for the VM, and stops Site Recovery billing for the VM.



You can run your machines on managed disks after a failover or migration from on-premises to Azure. Set the opti

Last refreshed at: 5/31/2018, 8:52:09 PM

Finished loading data from service.

NAME	...	STATUS	ACTIVE LOCATION
OSTICKETMYSQL	-	Failover completed	Microsoft Azure
OSTICKETWEB	-	Failover completed	Microsoft Azure

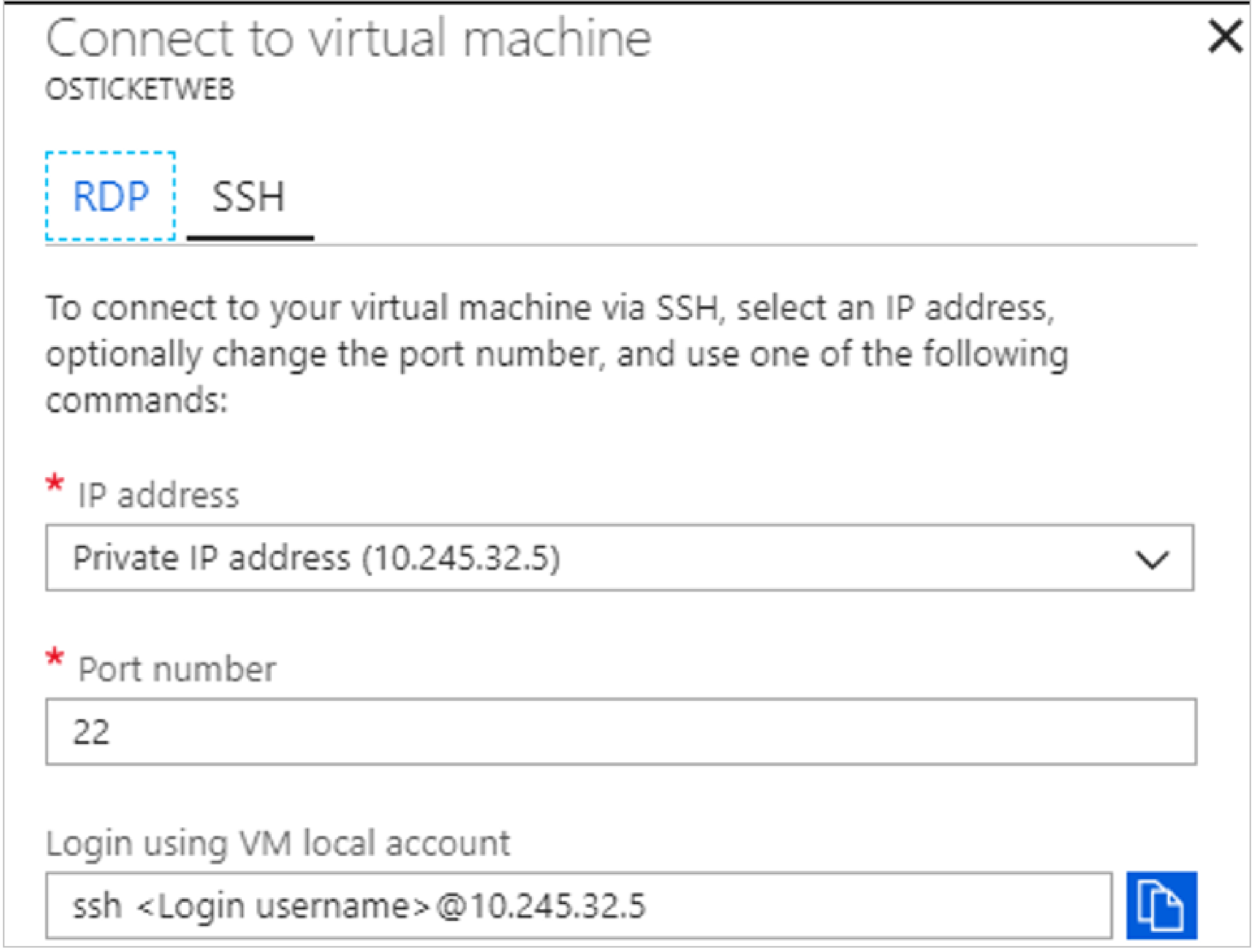
Need more help?

- Learn about running a test failover.
- Learn how to create a recovery plan.
- Learn about failing over to Azure.

Connect the VM to the database

As the final step in the migration process, Contoso admins update the connection string of the app to point to the Azure Database for MySQL.

1. They make an SSH connection to the OSTICKETWEB VM using Putty or another SSH client. The VM is private so they connect using the private IP address.



Connect to virtual machine

OSTICKETWEB

To connect to your virtual machine via SSH, select an IP address, optionally change the port number, and use one of the following commands:

* IP address

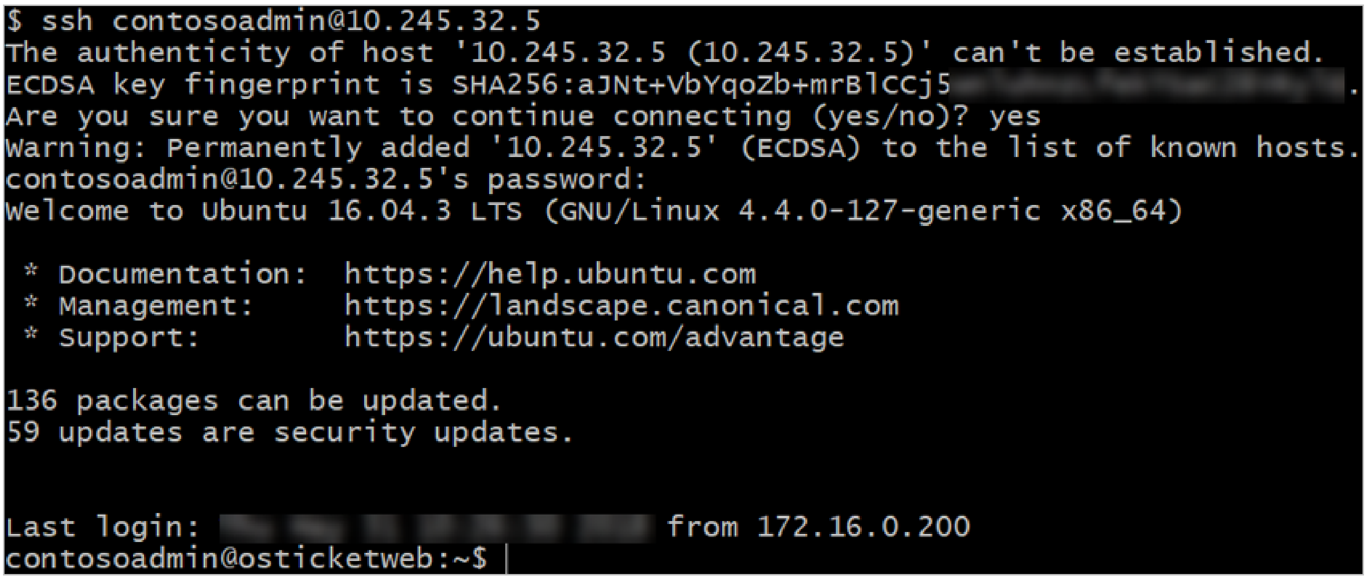
Private IP address (10.245.32.5)

* Port number

22

Login using VM local account

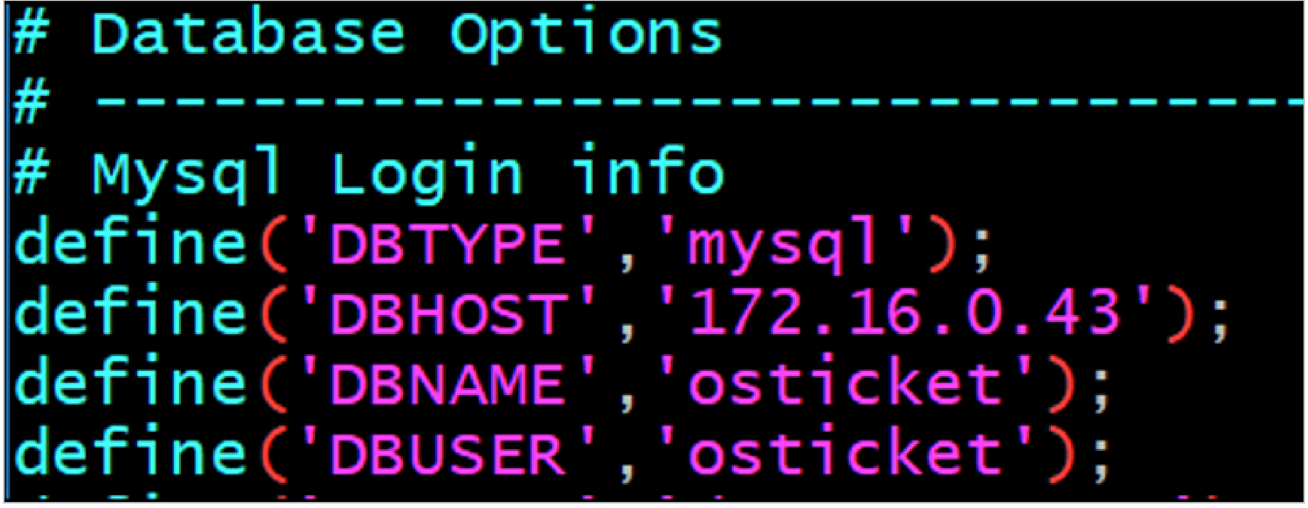
ssh <Login username>@10.245.32.5



```
$ ssh contosoadmin@10.245.32.5
The authenticity of host '10.245.32.5 (10.245.32.5)' can't be established.
ECDSA key fingerprint is SHA256:aJNt+VbYqoZb+mrBlCCj5[redacted].
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.245.32.5' (ECDSA) to the list of known hosts.
contosoadmin@10.245.32.5's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-127-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

136 packages can be updated.
59 updates are security updates.


Last login: [redacted] from 172.16.0.200
contosoadmin@osticketweb:~$ |
```

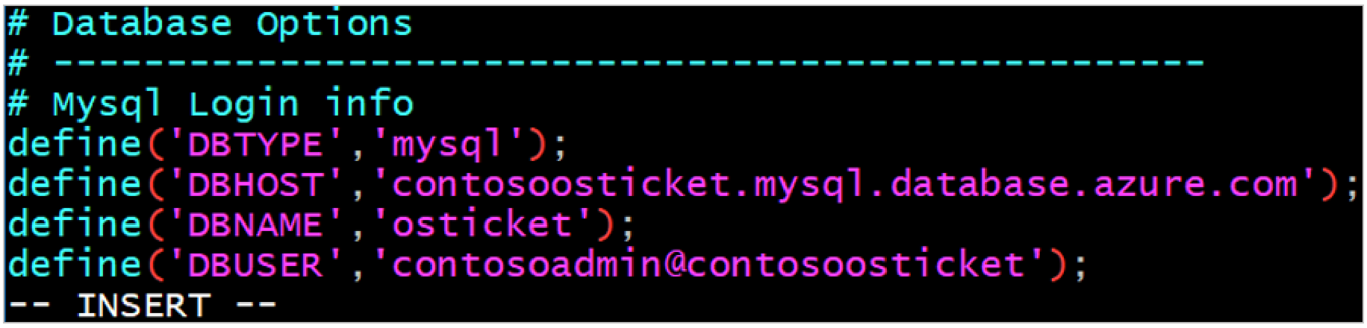
2. They update settings so that the **OSTICKETWEB** VM can communicate with the **OSTICKETMYSQL** database. Currently the configuration is hardcoded with the on-premises IP address 172.16.0.43.

   Before the update:

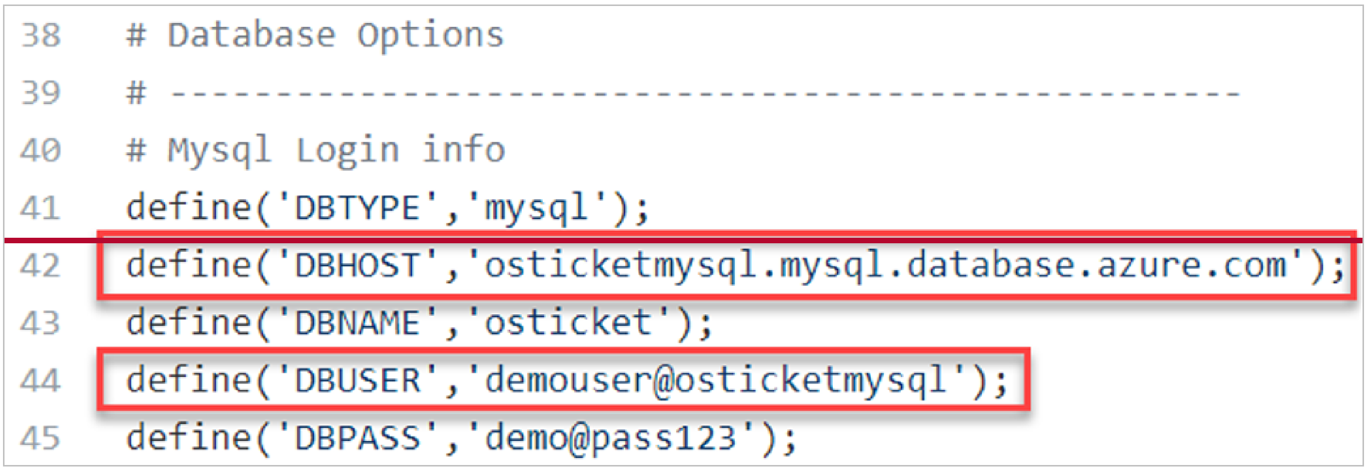


```
# Database Options
# ------------------------------
# Mysql Login info
define('DBTYPE','mysql');
define('DBHOST','172.16.0.43');
define('DBNAME','osticket');
define('DBUSER','osticket');
```

After the update:

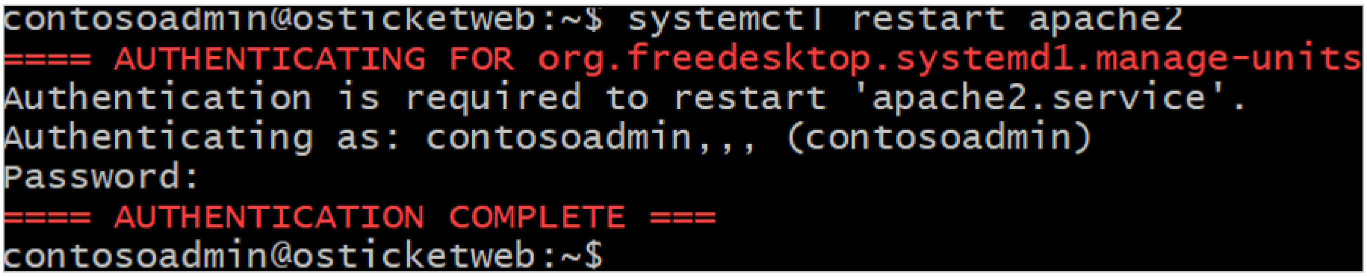


```
# Database Options
# ----------------------------------------------
# Mysql Login info
define('DBTYPE','mysql');
define('DBHOST','contosoosticket.mysql.database.azure.com');
define('DBNAME','osticket');
define('DBUSER','contosoadmin@contosoosticket');
-- INSERT --
```



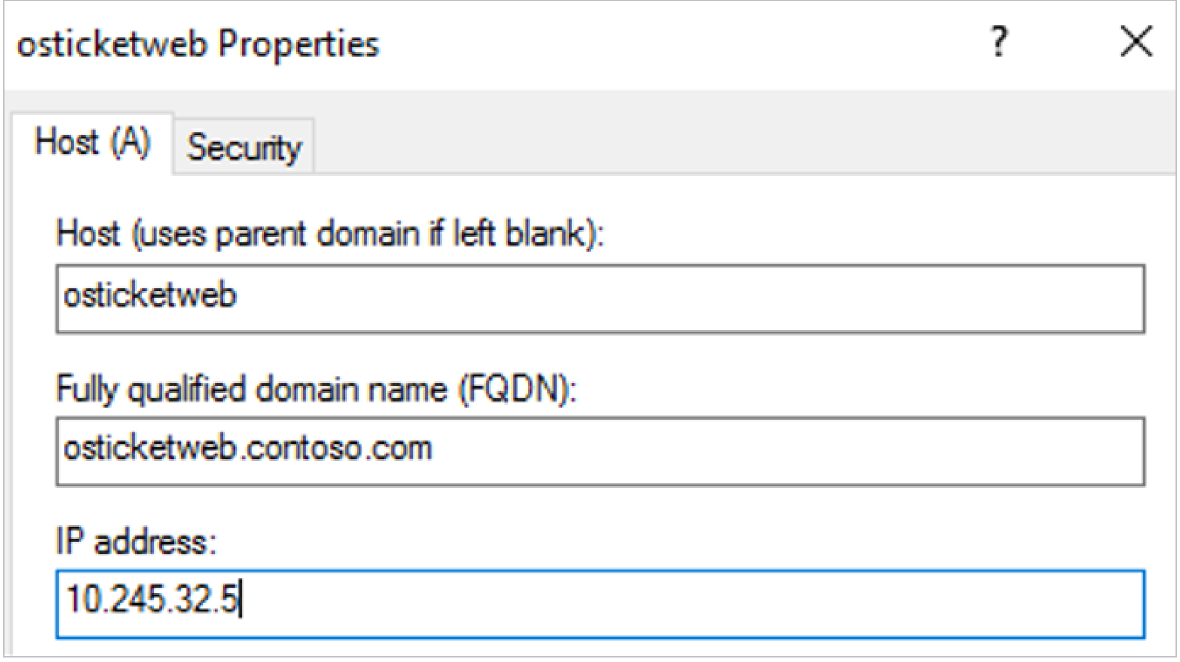
```
# Database Options
# ---------------------------------------------------
# Mysql Login info
define('DBTYPE','mysql');
define('DBHOST','osticketmysql.mysql.database.azure.com');
define('DBNAME','osticket');
define('DBUSER','demouser@osticketmysql');
define('DBPASS','demo@pass123');
```

3. They restart the service with **systemctl restart apache2**.



```
contosoadmin@osticketweb:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units
Authentication is required to restart 'apache2.service'.
Authenticating as: contosoadmin,,, (contosoadmin)
Password:
==== AUTHENTICATION COMPLETE ===
contosoadmin@osticketweb:~$
```

4. Finally, they update the DNS records for **OSTICKETWEB**, on one of the Contoso domain controllers.



Host (uses parent domain if left blank):
osticketweb

Fully qualified domain name (FQDN):
osticketweb.contoso.com

IP address:
10.245.32.5

Clean up after migration

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

Now, Contoso needs to do the following:

- Remove the VMware VMs from the vCenter inventory.
- Remove the on-premises VMs from local backup jobs.
- Update internal documentation show new locations and IP addresses.
- Review any resources that interact with the on-premises VMs, and update any relevant settings or documentation to reflect the new configuration.
- Contoso used the Azure Migrate service with dependency mapping to assess the **OSTICKETWEB** VM for migration. They should now remove the agents (Microsoft Monitoring Agent/Dependency Agent) they installed for this purpose, from the VM.

Review the deployment

With the app now running, Contoso need to fully operationalize and secure their new infrastructure.

Security

The Contoso security team review the VM and database to determine any security issues.

- They review the network security groups (NSGs) for the VM, to control access. NSGs are used to ensure that only traffic allowed to the application can pass.
- They consider securing the data on the VM disks using Disk encryption and Azure Key Vault.
- Communication between the VM and database instance isn't configured for SSL. They will need to do this to ensure that database traffic can't be hacked.

Read more about security practices for VMs.

BCDR

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

- **Keep data safe.** Contoso backs up the data on the app VM using the Azure Backup service. Learn more. They don't need to configure backup for the database. Azure Database for MySQL automatically creates and stores

server backups. They selected to use geo-redundancy for the database, so it's resilient and production-ready.
- **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

- After deploying resources, Contoso assigns Azure tags, in accordance with decisions they made during the Azure infrastructure deployment.
- There are no licensing issues for the Contoso Ubuntu servers.
- Contoso will enable Azure Cost Management licensed by Cloudyn, a Microsoft subsidiary. It's a multicloud cost management solution that helps you to use and manage Azure and other cloud resources. Learn more about Azure Cost Management.