



Migrate Your Virtual Machines to Microsoft Azure

Includes guidance for optional data migration

Proof of Concept guide

September 2017

Copyright Information

© 2017 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.

Some examples are for illustration only and are fictitious. No real association is intended or inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal reference purposes.

Table of Contents

Executive overview	1
Stage 1: Discover and assess environment with Azure Migrate	2
Step 1: Prepare your environment.....	3
Step 2: Discover virtual machines.....	4
Step 3: Group virtual machines	9
Step 4: Assess groups of virtual machines.....	13
Stage 2: Migrate virtual machines using Azure Site Recovery.....	20
Understand the migration process.....	20
Step 1: Set up Azure services	21
Step 2: Connect to VMware servers	26
Step 3: Set up the target environment.....	26
Step 4: Complete migration	34
Optional: Migrate a SQL Server database to Azure SQL Database	35
Stage 3: Optimize migrated workloads.....	51
Summary.....	54
Appendix 1: Discovery stage with partner Cloudamize	55
Create a Cloudamize account.....	55
Configure your VMware vCenter environment.....	56
Perform discovery and run an assessment.....	57
Review Infrastructure Assessment Summary from Cloudamize	59
Appendix 2: Discovery stage with partner Movere	63
Deploy Movere	63
Assess results	67

Executive overview

Perhaps you want to start migrating critical parts of your infrastructure to the cloud, but figuring out how can be challenging and time consuming. If your organization is like others, eighty percent of your IT resources are dedicated to keeping your datacenter running—where will you find the time and budget to perform the migration quickly?

Migrating to the cloud doesn't have to be difficult, but many organizations struggle to get started. Before they can showcase the cost benefits of moving to the cloud or determine if their workloads will lift and shift without effort, they need deep visibility into their own environment and the tight interdependencies between applications, workloads, and data. No wonder many organizations feel anxious taking the first step.

Microsoft offers an end-to-end solution to provide you with a proven framework and tools to migrate your first workload and give you a complete roadmap for discovery, migration, and continual optimization, including better insights and strategies for running your entire datacenter portfolio on Azure.

This guide provides an overview of the three-stage migration process and focuses on how to identify virtual machines, applications, and data that can easily be moved to the cloud.

1. **Discover.** Use available tools to get better visibility of applications, workloads, and data in your environment, and assess the optimal resource level to run them in Microsoft Azure. Use this information to help decide which workloads to move.
2. **Migrate.** Move selected workloads to Azure from a variety of sources including physical servers and virtualized workloads hosted on Microsoft Hyper-V or VMware environments.
3. **Optimize.** Fine tune your Azure-based workloads and maximize your ROI.

This guide walks you through an example to assess an environment using Azure Migrate or, optionally, one of two partner solutions discussed in the appendices. The Microsoft and partner discovery solutions help IT professionals assess potential Azure usage costs before they migrate workloads to Azure using the Azure Site Recovery service in the Azure portal. For purposes of this example, the workloads migrated to Azure in this guide are running on on-premises VMware virtual machines.

Stage 1: Discover and assess environment with Azure Migrate

Starting migration with a discovery process can help you assess your on-premises workloads to prepare for migration. Microsoft offers Azure Migrate to help you determine which workloads are suitable for migration and estimate costs to run them in Azure using performance-based sizing tools that consider resource usage. This service is for you if you are contemplating lift-and-shift migrations or are already in the early phases of migration assessment. (Optionally, you can use one of the Microsoft partner solutions in the Appendices of this guide.)

Azure Migrate supports these capabilities:

- Discovery of workloads.
- Appliance-based, agentless, and non-intrusive discovery of on-premises virtual machines.
- VMware vCenter Server 5.5- and 6.0-managed virtual machines.
- Assessment of discovered workloads, which includes:
 - **Azure readiness summary:** Which of your on-premises machines are suitable for Azure?
 - **Size recommendations:** What are the appropriate Microsoft Azure Virtual Machine sizes and Azure disk sizes based on the performance history of the on-premises virtual machine?
 - **Monthly costs:** The estimated cost for running the machines in Azure.

Azure Migrate bases an assessment on several values, including:

- **Target location:** By default, Azure Migrate assumes the Azure location to which you want to migrate is the location in which you create the migration project.
- **Storage redundancy:** What is the type of storage that the Azure Virtual Machines will use after migration? Currently Azure Migrate supports only [Locally redundant storage \(LRS\)](#).
- **Pricing plans:** You can specify whether you're enrolled in Software Assurance and can use the [Azure Hybrid Use Benefit](#), and whether you have any Azure offers that should be applied. You can also specify any subscription-specific discount (in a percentage) that you might be getting on top of the offer.
- **Pricing tier:** Azure Migrate takes Azure Virtual Machine tier pricing into account to meet your exact requirements. By default, the Standard tier is used.

Azure Migrate primarily supports Infrastructure-as-a-Service (IaaS)-based assessments for lift-and-shift migrations. However, during the discovery process, if database servers are found, Azure Migrate will recommend the use of Azure Database Migration Service, which is discussed in the [Migrate virtual machines using Azure Site Recovery](#) section of this guide.

First, take a moment to review the steps for using Azure Migrate.

1. Create a migration project in Azure.
2. Azure discovers information about on-premises machines using a virtual machine called the Collector Appliance. Download the appliance setup file, which is in Open Virtualization Appliance (.ova) format, and import the file into the on-premises vCenter server as a virtual machine.
3. After you've created the Collector virtual machine, connect to it and run the Collector.
4. The collector service uses VMware PowerCLI cmdlets to collect metadata about the on-premises virtual machines from the vCenter Server. Note this is an agentless discovery and you do not need to install anything on the ESXi hosts or the virtual machines for metadata collection.
5. The collector service collects information about virtual machines, including cores, memory, disks and disk sizes, and network adapters. It also collects performance data for the virtual machines, including CPU and memory use, disk IOPS, disk throughput (MBps), and network output (MBps). Collected metadata is then pushed to the Azure Migrate project and can be viewed in the Azure portal.
6. You can then create an assessment for a group of virtual machines in the Azure Migrate portal. The assessment report can be viewed in the portal, or it can be downloaded in an Excel format. The assessment report includes information about Azure readiness, sizing, and cost estimations for running the on-premises virtual machines in Azure.

Use these four steps to discover and assess your on-premises workloads for migration to Azure.

1. Prepare your environment.
2. Discover virtual machines.
3. Group virtual machines.
4. Assess the groups of virtual machines.

Step 1: Prepare your environment

Start by confirming you have met the prerequisites for using Azure Migrate.

Azure Migrate prerequisites

1. To get started with Azure Migrate, you need a Microsoft Azure account or the free trial.
2. Assess VMware Virtual machines located on vSphere ESXi hosts that are managed with a vCenter server running version 5.5 or 6.0.
3. The ESXi host or cluster on which the Collector VM (version 8.0) runs must be running version 5.0 or later.

4. To discover virtual machines, Azure Migrate needs an account with read-only administrator credentials for the vCenter server.
5. Create a vCenter virtual machine in .ova format. Download an appliance and import it to the vCenter server to create the virtual machine. The virtual machine must be able to connect to the internet to send metadata to Azure.
6. Set statistics settings for the vCenter server to statistics level 2. The default Level 1 will work, but Azure Migrate won't be able to collect data for performance-based sizing for storage.

After you complete the prerequisites, you have the option to tag your virtual machines to help accelerate assessments. Alternatively, you can group the virtual machines later, after discovery.

Tag your virtual machines in vCenter (optional)

Planning migrations is easier when you tag the virtual machines you want to migrate. Using tags, you can jumpstart the assessment, because the Collector automatically creates groups of virtual machines for you based on the tag values. However, this is an optional step and if you do not have tags in vCenter server, you can group virtual machines using the Azure Migrate service.

Use these steps to tag your virtual machines in vCenter server.

1. In the VMware vSphere Web Client, navigate to the vCenter server instance.
2. To review current tags, click **Tags**.
3. To tag a virtual machine, click **Related Objects > Virtual Machines**, and select the virtual machine.
4. In **Summary > Tags**, click **Assign**.
5. Click **New Tag**, and specify a tag name and description.
6. To create a category for the tag, select **New Category** in the drop-down list.
7. Specify a category name and description and the cardinality, and click **OK**.

Step 2: Discover virtual machines

Using Azure Migrate to discover on-premises workloads involves these steps.

1. Create a Project.
2. Download the Collector appliance.
3. Create the Collector virtual machine.
4. Run the Collector to discover virtual machines.
5. Verify discovered virtual machines in the portal.

Create a Project

Azure Migrate projects hold the metadata of your on-premises machines and enables you to assess migration suitability.

Use these steps to create a project.

1. Log on to the Azure portal and click **New**.
2. Search for Azure Migrate in the search box, and select the service **Azure Migrate** (preview) in the search results, and then click **Create**.
3. Select the Azure Migrate service from the search results.
4. Click **Create**.

Azure Migrate makes it easy to assess on-premises workloads for migrations to Azure. This Limited Preview release includes the following functionality:

Discovery

- Appliance-based, friction-less, and non-intrusive discovery of on-premises virtual machines (VMs)
- vCenter Server 5.5- and 6.0-managed VMs

Assessments

- Is the VM suitable for running in Azure?
- What would be the appropriate Azure VM size based on the performance history of the VM?
- What would be the ongoing cost of running the VM in Azure?

Get started by creating a new Project. It will hold the metadata of your on-premises machines and enable you to assess their migration suitability.

Microsoft Azure Migration projects > Project001

Discover machines + Create assessment Delete project

Essentials

Machines Assessments Groups

400 0 2

Learn more
Overview of Azure Migrate

Assessments

NAME	GROUP	STATUS	APPROVAL STATE
No assessments found			

Groups

NAME	RESOURCES	LAST SYNCED DATE
US_Soft_galleries	12	02/17/2016 13:40:00 PM
US_Softsource	12	02/17/2016 13:40:00 PM

Create

5. Specify a name for the new project.
6. Select the subscription you want the project to get associated to.
7. Create a new resource group, or select an existing one.
8. Specify an Azure location.
9. To quickly access the project from the Dashboard, select **Pin to dashboard**.

10. Click **Create**

Create Migration project

Migration project

You are on your way to assess your on-premises machines for migration to Azure. Create a project to start the process.

[Learn more](#)

* Name ?
ContosoProject10

* Subscription
Azure Migrate Test2

* Resource group ?
 Create new Use existing
AzureMigEU

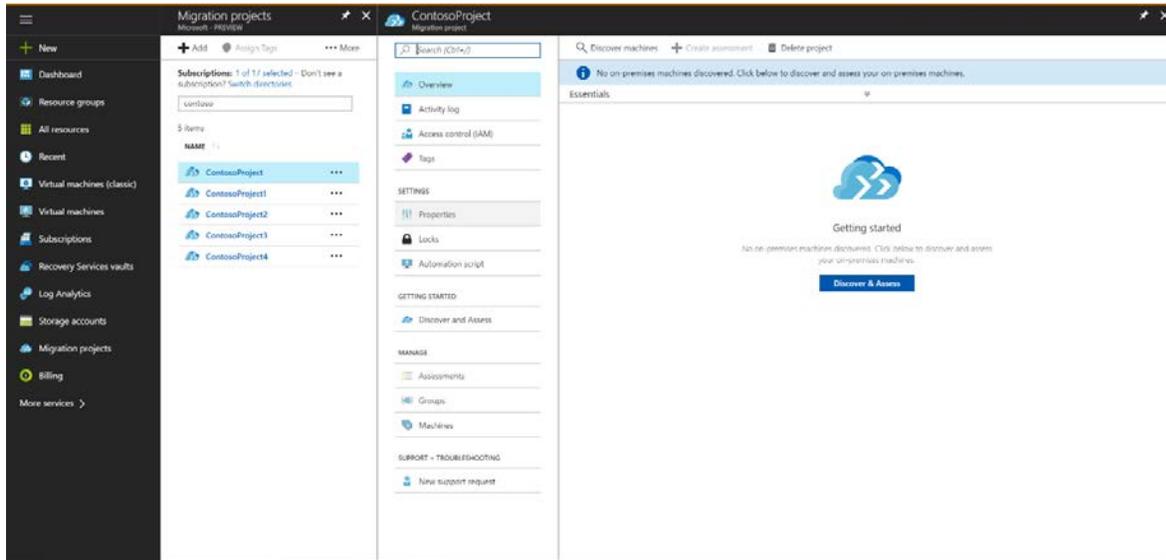
* Location ?
East US

A new Operations Management Suite (OMS) workspace will be created to enable dependency visualization feature. You will be charged for the workspace if you use the feature. [Learn more.](#)

Pin to dashboard

Create Automation options

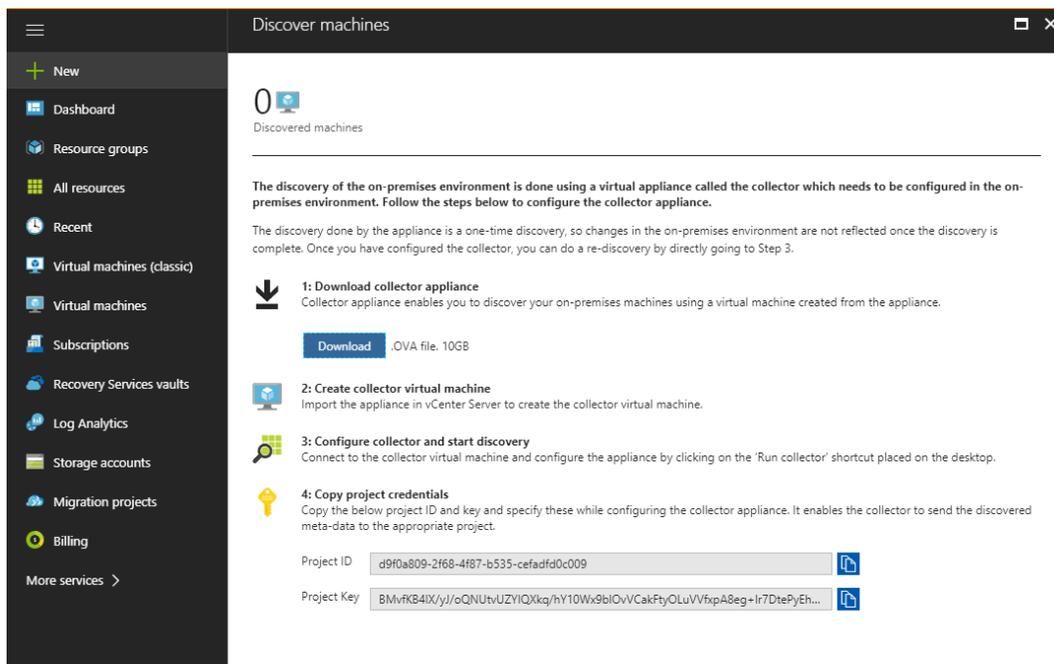
The new project appears on the Dashboard, under **All resources**, and in the Projects blade.



Download the Collector appliance

The Collector appliance is a single file in Open Virtualization Appliance (.ova) format that you download and run on an on-premises environment to discover on-premises workloads. Follow these steps to download the Collector.

1. Select the project, and click **Discover & Assess** on the Overview blade.
2. Click **Discover Machines**, and then click **Download**.
3. Copy the Project ID and project key values to use when you configure the Collector.



Create the Collector virtual machine

In the vCenter Server, import the Collector appliance as a virtual machine using the Deploy OVF Template wizard.

1. In vSphere Client console, click **File > Deploy OVF Template**.
2. In the Deploy OVF Template Wizard > **Source**, specify the location for the .ovf file.
3. In **Name** and **Location**, specify a friendly name for the Collector virtual machine, the inventory object in which the virtual machine will be hosted.
4. In **Host/Cluster**, specify the host or cluster on which the Collector virtual machine will run.
5. In **Storage**, specify the storage destination for the Collector virtual machine.
6. In **Disk Format**, specify the disk type and size.
7. In **Network Mapping**, specify the network to which the Collector virtual machine will connect. The network must be connected to the internet to send metadata to Azure.
8. Review and confirm the settings, and then click **Finish**.

Run the Collector to discover virtual machines

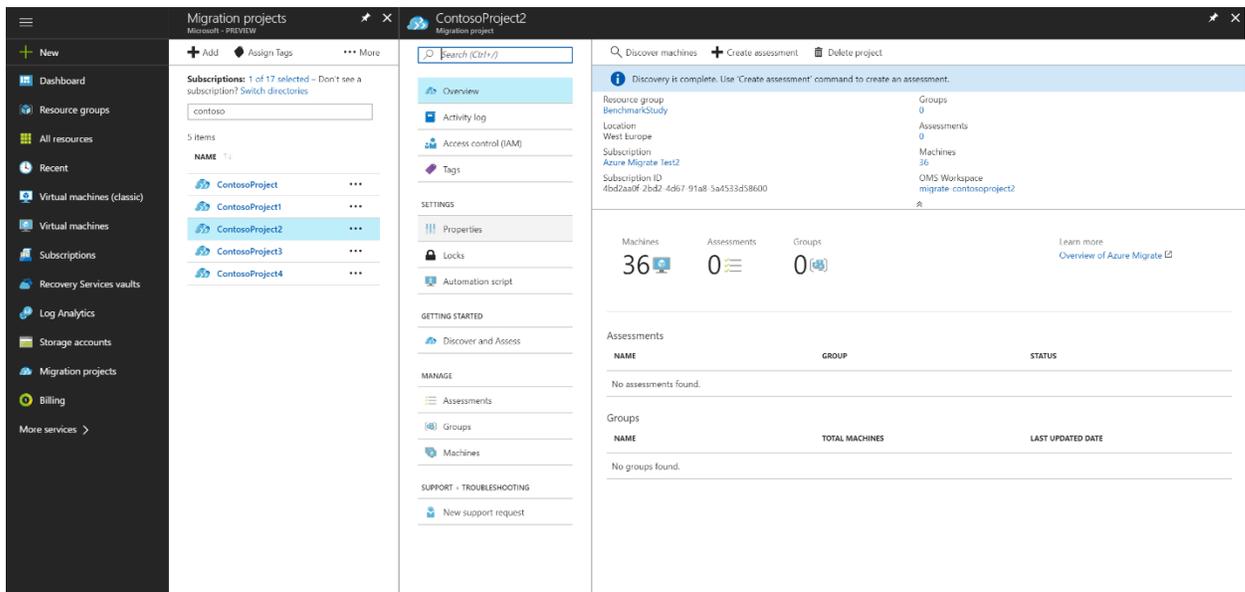
1. In the vSphere Client console, right-click the virtual machine > **Open Console**.
2. Provide the language, time zone, and password preferences for the appliance.
3. In the Azure Migrate Collector, open **Set Up Prerequisites**, and then
 - Accept the license terms, and read the third-party information.
 - The Collector checks that the virtual machine has internet access. If the virtual machine accesses the internet via a proxy, click **Proxy settings**, and specify the proxy address and listening port. Specify credentials if proxy access needs authentication.
 - The Collector checks that the Windows profiler service is running. The service is installed by default on the Collector virtual machine.
 - Select to download and install the VMware PowerCLI.
4. In **Discover Machines**, do the following:
 - Specify the name (FQDN) or IP address of the vCenter server and the read-only account the Collector will use to discover virtual machines on the vCenter server.
 - Select a scope for virtual machine discovery. The Collector can only discover virtual machines within the specified scope. Scope can be set to a specific folder, datacenter, or cluster, but it shouldn't contain more than 1000 virtual machines.
 - If you're using tagging on the vCenter server, select tag categories for virtual machine grouping. Azure Migrate automatically groups virtual machines based on tag values in the category. If you're not using tagging, you can group virtual machines in the Azure portal.

- In **Select Project**, specify the Azure Migrate project ID and key you copied from the Azure portal. If didn't copy them, open Azure in a browser from the Collector virtual machine. In the project **Overview** page, click **Discover Machines**, and copy the values.
- In **Complete Discovery**, you can monitor the discovery status, and check that metadata is collected from the virtual machines in scope. The Collector provides an approximate discovery time.

Verify discovered virtual machines in the portal

Discovery time depends on how many virtual machines you are discovering. Typically, for 100 virtual machines, it takes about an hour for discovery to finish and display the virtual machines in the Azure Migrate portal after the Collector finishes running. To check for discovered virtual machines in the portal:

- In the migration project, click **Manage > Machines**.
- Check that the virtual machines you want to discover appear in the portal.



Step 3: Group virtual machines

Enterprises typically migrate virtual machines with dependencies together at the same time to ensure their functionality after migration to Azure.

Azure Migrate allows you to categorize the virtual machines by group so you can assess all the virtual machines in a group.

- If you provided a tag category—which was an optional step while configuring the Collector—groups will be automatically created for the workloads based on the tag values.
- If a tag category is not provided while configuring the Collector, you can create groups of virtual machines in the Azure Migrate portal.

Note: Azure Migrate provides you the flexibility to group virtual machines based on any criteria you want, for example grouping by application or department.

Optional: Assess machine dependencies before adding them to a group

Use this step if you want to group your virtual machines by dependencies. If you map dependencies, you can group machines more accurately. You can either verify dependencies for specific machines before adding them to a group, or verify the dependencies of a group after creating it. If you want to verify dependencies for a specific machine before you add it to a group, do this:

1. In **Manage > Machines**, search **the Machine** for which you want to view the dependencies.
2. In **the Dependencies column** for the machine, click **Install agent**.
3. To calculate dependencies, download and install these agents on the machine:
 - Microsoft Monitoring agent
 - Dependency agent
4. Copy the workspace ID and key to use later when you install the Microsoft Monitoring agent on a machine.

Dependencies

Dependency visualization of machines requires a deeper discovery which involves installation and configuration of the below agents on the on-premises machines. You will be charged for using the dependency visualization feature. [Learn more](#)

Step 1: Download & install Microsoft Monitoring Agent (MMA)

1. Windows 64-bit
2. Linux

[Learn more about installation of MMA agent.](#)

Step 2: Download and install dependency agent

1. Windows 64-bit
2. Linux

[Learn more about installation of dependency agent.](#)

If you have machines with no internet connectivity to OMS, you need to download and install OMS gateway.

[Learn more](#)

Step 3: Configure MMA agent

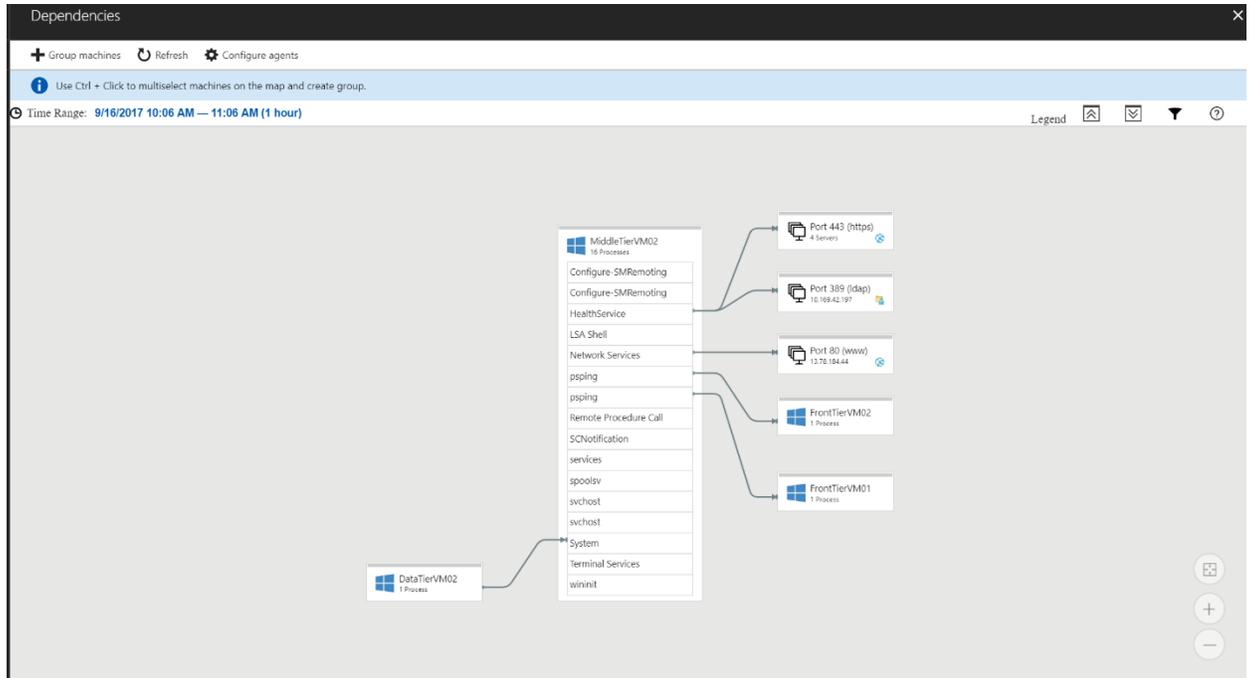
Configure MMA agent with the workspace by specifying the below workspace ID and key.

[Learn more](#)

Workspace ID:

Workspace key:

- After you install the agents on the machine, return to the portal and click **Machines**. This time the **Dependencies column** for the machine should contain the text **View dependencies**. Click **View dependencies**.



- By default, the dependency time range is an hour. Click the time range to shorten it, specify start and end dates, or change the duration. Press **Ctrl + Click** to select multiple machines on the map, and then click **Group machines**.
- In **Group machines**, specify a group name. Verify the machines you added have the dependency agents installed and have been discovered by Azure Migrate. Machines must be discovered to assess them. We recommend that you install the dependency agents to complete dependency mapping.
- Click **OK** to save the group settings. Alternatively, you can add machines to an existing group.

Create a Group

You can create groups of virtual machines from the Machines blade or from the Groups blade, using a similar process.

Create a group from the Machines blade

- Navigate to the Dashboard of a project and click the Machines tile.
- Click **Group Machines**.
- Specify a name for the group in the **Name** box, and then select the machines that you want to add to the group.

4. Click **Create**.

The screenshot shows the 'Create group' dialog in Azure. The dialog is titled 'Create group' and has a subtitle 'Groups'. It contains the following elements:

- A description: 'A group is a collection of machines that you would like to assess and migrate together. Assessments are created on groups to help you determine Azure readiness of your on-premises machines.'
- A section for '1. Group name' with a text input field containing 'contosofacilities' and a green checkmark.
- A section for '2. Add machines to the group' with a search input field containing 'tier'.
- A table of virtual machines with columns 'NAME', 'IP ADDRESS', and 'OPERATING SYSTEM'. All 8 machines are checked.
- A 'Selected machines' section showing '8' machines.
- A checkbox for 'Create a new assessment automatically for this group.' which is unchecked.
- A blue 'Create' button at the bottom.

NAME	IP ADDRESS	OPERATING SYSTEM
<input checked="" type="checkbox"/> DataTierVM03		Microsoft Windows Server ...
<input checked="" type="checkbox"/> DataTierVM01	2404:f801:4800:25:a84a:c0d...	Microsoft Windows Server ...
<input checked="" type="checkbox"/> MiddleTierVM01	2404:f801:4800:25:f168:7c8...	Microsoft Windows Server ...
<input checked="" type="checkbox"/> MiddleTierVM02	2404:f801:4800:25:d72:4b7...	Microsoft Windows Server ...
<input checked="" type="checkbox"/> DataTierVM02	2404:f801:4800:25:583a:41...	Microsoft Windows Server ...
<input checked="" type="checkbox"/> MiddleTierVM03	10.150.10.119,2404:f801:48...	CentOS 4/5/6/7 (64-bit)
<input checked="" type="checkbox"/> FrontTierVM01	2404:f801:4800:25:a070:37...	Microsoft Windows Server ...
<input checked="" type="checkbox"/> FrontTierVM02	2404:f801:4800:25:c987:923...	Microsoft Windows Server ...

After the group is successfully created, you can add/remove machines to/from this group and refine the group membership.

Add/Remove machines to/from an existing group

1. Navigate to the dashboard of a project and click the Groups tile.

2. Select the Group you want to add/remove machines to/from.
3. Click **Add Machines** or **Remove Machines**.
4. Select the machines that you want to add/remove to/from the group.
5. Click **Add** or **Remove**.

Step 4: Assess groups of virtual machines

Azure Migrate allows you to assess a group to analyze the Azure suitability of the machines in the group, conduct performance-based right-sizing for Azure, and estimate the cost for running the virtual machines in Azure.

Note: Discovery of your on-premises workloads and creation of groups is a prerequisite for assessment. Prior to assessment, you can refine the membership of a group by adding or removing machines to/from the group.

Create an assessment

Follow these steps to generate an assessment for the group.

1. Select the project you want under **Project**.
2. On the project dashboard, click **Groups**.
3. Create a new group or select an existing group to assess under **Group**.

- Click **Create Assessment** to create a new assessment for the group.

An assessment helps you determine Azure readiness of your on-premises machines. It is created on a group of machines that you assess and migrate together.

1. Select or create a group

Create New Use Existing

contosopayroll ✓

2. Add machines to the group

tier

	NAME	IP ADDRESS	OPERATING SYSTEM
<input checked="" type="checkbox"/>	DataTierVM03		Microsoft Windows Server ...
<input checked="" type="checkbox"/>	DataTierVM01	2404:f801:4800:25:a84a:c0d...	Microsoft Windows Server ...
<input checked="" type="checkbox"/>	MiddleTierVM02	2404:f801:4800:25:d72:4b7...	Microsoft Windows Server ...
<input checked="" type="checkbox"/>	MiddleTierVM01	2404:f801:4800:25:f168:7c8...	Microsoft Windows Server ...
<input checked="" type="checkbox"/>	DataTierVM02	2404:f801:4800:25:583a:41...	Microsoft Windows Server ...
<input checked="" type="checkbox"/>	MiddleTierVM03	10.150.10.119,2404:f801:48...	CentOS 4/5/6/7 (64-bit)
<input checked="" type="checkbox"/>	FrontTierVM02	2404:f801:4800:25:c987:92...	Microsoft Windows Server ...
<input checked="" type="checkbox"/>	FrontTierVM01	2404:f801:4800:25:a070:37...	Microsoft Windows Server ...

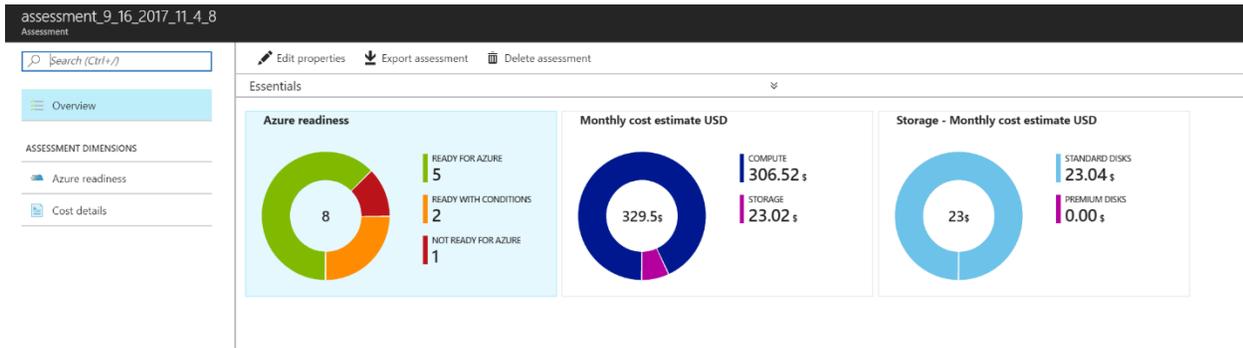
Create assessment

The assessment includes these details.

- Summary of the number of machines suitable for Azure which is referred to as Azure Readiness.
- Monthly estimate of the cost for running the machines in Azure after migration.
- Storage monthly cost estimate.

Once you have created an assessment, you can view it later using the **View Assessments** command on the Group blade or by using Representational State Transfer (REST) API. For more information about using the REST API, review the [Azure REST Reference document](#).

This is a sample assessment result where you can view graphics for Azure readiness, monthly cost estimates for computing, and a monthly cost estimates for storage.



Customize an assessment

When you use the **Create Assessment** command, Azure Migrate assumes smart defaults for the properties of the group (for example, target location, storage redundancy, and so on) and creates the assessment based on these properties. However, you can customize these using the **Edit Properties** command on the Assessment blade.

Property	Description	Default
Target location	The Azure location to which you want to migrate	Location where you created the migration project
Storage redundancy	The storage that the Azure Virtual Machines will use after migration.	Only Locally redundant storage (LRS) is currently available
Comfort factor	Factors considered such as seasonal usage, short performance history, likely increase in future usage. For example, a 10-core virtual machine with 20% utilization will result in a 2-core virtual machine. However, if the virtual machine has a comfort factor of 2.0, the resulting recommendation would be for a 4-core virtual machine.	Setting is 1.3
Performance history	Duration of performance history evaluated.	One month
Percentile utilization	Percentage of performance history evaluated.	95%
Pricing tier	Virtual machines are evaluated on a tier system.	Standard tier

Property	Description	Default
Offer	Azure offers that apply.	Pay-as-you-go
Currency	Billing currency	US Dollars
Discount (%)	Any subscription-specific discount you are receiving on top of the offer.	0%
Azure Hybrid Benefit for Windows Server	If set to Yes , non-Windows Azure prices are considered for Windows virtual machines.	Yes

Assessment calculation

Azure Migrate performs three checks on virtual machines in this order:

1. Azure Suitability Analysis
2. Performance-based sizing
3. Monthly cost estimate

A machine is assessed in each subsequent stage only if it passes the previous stage. For example, if a machine fails the Azure suitability check, it is marked unsuitable for Azure and right-sizing and cost estimation is not completed for the machine.

Azure Suitability Analysis

Azure has certain limits and constraints that might prevent some virtual machines from qualifying for Azure hosting. For example, if a virtual machine has a disk size more than 1024 GB, it cannot be hosted on Azure. For more information, [review Azure virtual machine limits](#). Azure Migrate checks for the following conditions. Each virtual machine must meet all criteria to be marked as suitable for Azure.

- Storage
 - Allocated size of each disk (including OS disk) is ≤ 1024 GB
 - Number of disks attached to the machine is ≤ 65 ii.
- Networking: Number of NICs attached to the machine is ≤ 32
- Compute
 - Boot type is BIOS (and not UEFI)
 - Number of cores in the machine is less than or equal to the maximum number (32) of cores supported by any Azure Virtual Machine.

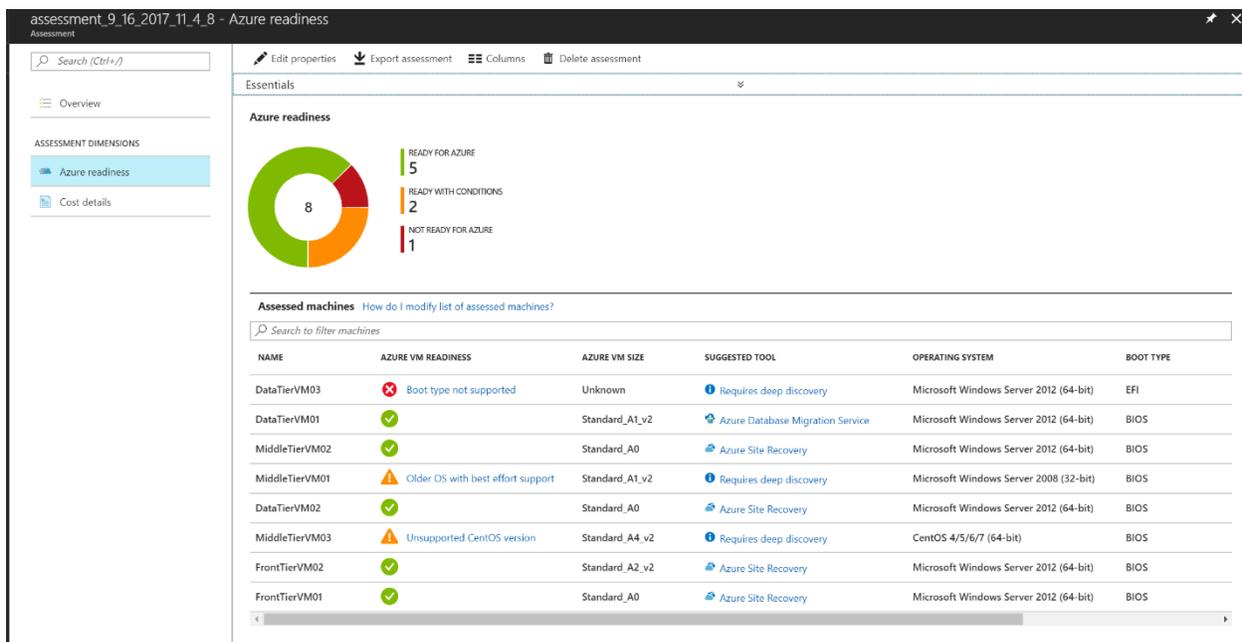
Note: Using the performance history of the machine, AM considers the utilized cores of the machine for the comparison rather than considering all the allocated cores. If any comfort factor is specified in the assessment settings, the number of utilized cores is multiplied with the comfort factor to come up with the effective number of cores. If there is no performance history available for the machine, AM falls back to the allocated number of cores for all the checks.

- Memory size of the machine is less than or equal to the maximum memory (448 GB) supported by any Azure Virtual Machine.

Note: Using the performance history of the machine, AM considers the utilized memory of the machine for the comparison rather than considering the allocated memory. If any comfort factor is specified in the assessment settings, the utilized memory is multiplied with the comfort factor to come up with the effective memory size. If there is no performance history available for the machine, AM falls back to the allocated memory for all the checks.

- Operating System in the machine is supported by Azure. Review the [list of software directly supported by Azure](#).

This is a sample suitability assessment.



Performance-based sizing

After a machine is marked as suitable for Azure, AM tries to map it to a virtual machine size in Azure. Azure Migrate considers the following criteria to match the machine to an Azure Virtual Machine.

- **Storage check** Azure Migrate tries to map every disk attached to the machine to a disk in Azure:
 - Only managed disks are currently supported.
 - Azure Migrate looks at the I/O per second (IOPS) throughput (MBps) of each disk attached to the machine, and multiplies it with the comfort factor.
 - If Azure Migrate can't find a disk with the required IOPS and throughput, it marks the machine as unsuitable for Azure.

- From the suitable set of disks, Azure Migrate selects the ones that support the storage redundancy method and location, specified in the assessment settings. If there are multiple eligible disks, Azure Migrate selects the one with the lowest cost.
- **Network check** Azure Migrate aggregates the data transmitted per second (MBps) from the machine (network out), across all the network adapters attached to it:
 - Azure Migrate applies the comfort factor to the aggregated number and uses the result to find an Azure Virtual Machine that can support it.
 - When finding the virtual machine, Azure Migrate also checks that it can support the required number of network adapters.
 - Note that Azure Migrate takes the network settings from the virtual machine and assumes it to be network outside the datacenter.
 - If no network utilization data is available, only the network adapter count is considered for virtual machine sizing.
- **Compute check** After storage and network requirements are calculated, Azure Migrate considers compute requirements:
 - If the performance data is available for the virtual machine, Azure Migrate looks at the utilized cores and memory, and applies the comfort factor. Based on that number, it tries to find a suitable virtual machine size in Azure.
 - If no suitable size is found, the machine is marked as unsuitable for Azure.
 - If a suitable size is found, Azure Migrate applies the storage and networking requirements it calculated. It then applies location and pricing tier settings, for the final virtual machine size recommendation.

Monthly Cost Estimation

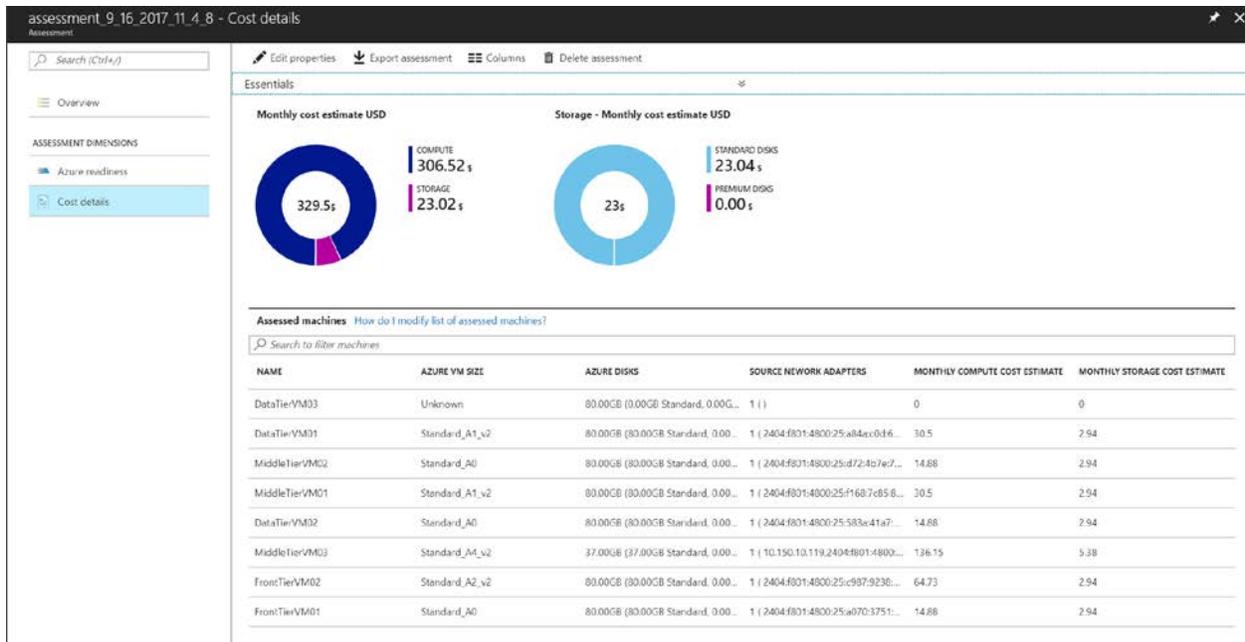
Once Azure Migrate delivers the size recommendation, it calculates the compute, storage, and networking costs that may be incurred after the virtual machines are migrated to Azure. You can adjust the currency in the assessment settings.

- **Compute:** For each machine, using the recommended size, Azure Migrate calls the Billing API to calculate the monthly cost that will be incurred in Azure. The cost calculation considers the machine operating system (Windows or non-Windows), software assurance, offer, location, and currency specified in the assessment settings, and then aggregates the cost across all machines to come up with the total monthly compute cost.
- **Storage:** The monthly storage cost of a machine is calculated by aggregating the monthly cost of all the disks attached to the machine. Azure Migrate then aggregates the storage cost across all machines to come up with the total monthly storage cost.

Note: that the calculation of the cost of a disk does not currently consider the offer specified in the assessment settings.

- **Networking:** The monthly networking cost of a machine is calculated by aggregating the monthly cost of all the network adapters attached to the machine.

Note: Azure Migrate considers all the data transferred out of the network adapter as out of the datacenter and calculates the cost per network adapter. Once the networking cost per machine is calculated, AM then aggregates the cost across all the machines to come up with the total monthly networking cost.



Once you have assessed your environment and selected the workloads you want to move to Azure, you are ready to migrate. The next section describes the components and processes used to migrate selected VMware virtual machines to Azure.

Stage 2: Migrate virtual machines using Azure Site Recovery

Now that you have assessed your environment and selected the workloads you want to move to Azure, you are ready to migrate. This section describes the components and processes used to migrate on-premises VMware virtual machines to Azure using the Microsoft Azure Site Recovery service. Microsoft offers the Azure Site Recovery service as a [free trial for the first 31 days](#).

Understand the migration process

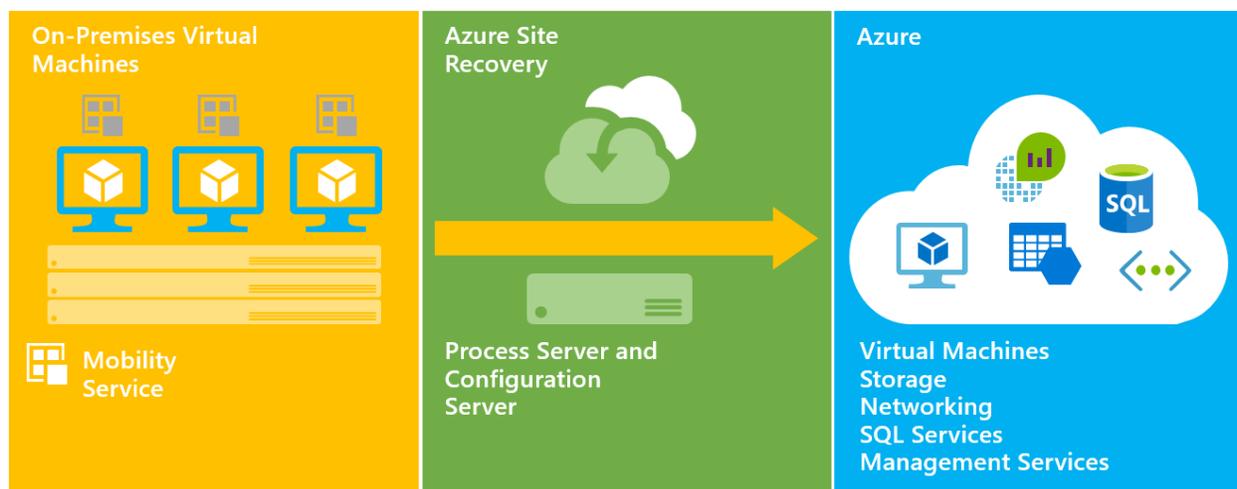
Before undertaking the migration process, take some time to understand the overall environment by walking through some basic information. For more details, review the article [Replicate VMware virtual machines to Azure with Site Recovery](#).

Before you start deployment, review the architecture and make sure you understand all the components you need to deploy.

Next, make sure you understand the prerequisites and limitations for a Microsoft Azure account, Azure networks, and storage accounts. You also need:

- On-premises Site Recovery components
- On-premises VMware prerequisites
- Mobility service component installed on the virtual machine you want to replicate.

The components for migration are illustrated in the following image.



With an understanding of the architecture, components, and process for replication, the next step is to install and configure all the on-premises and Azure components.

These are the general steps to migrate:

1. Set up Azure services.
2. Connect to VMware servers.
3. Set up the target environment.
4. Complete migration.

Step 1: Set up Azure services

When migrating VMware virtual machines to Azure, there are nuances with networking and IP addresses. Before migration, review the [guidance to plan networking for VMware to Azure replication](#).

Set up an Azure network

You will need an internal Azure network to allow the Azure Virtual Machines and other resources to communicate after the migration.

- Set up an Azure network following the guidance in the article, [Create a virtual network with multiple subnets](#). Azure Virtual Machines are placed in this network when they're created after failover.
 - Site Recovery in the Azure portal can use networks set up in [Resource Manager](#), or in classic mode.
 - The network should be in the same region as the Recovery Services vault.
- Learn about [virtual network pricing](#).
- Learn more about [Azure Virtual Machine connectivity](#) after failover.

Set up an Azure storage account

Azure Site Recovery replicates on-premises machines to Azure storage. Azure Virtual Machines are created from the storage after failover occurs.

Follow the [guidance to set up an Azure storage account](#) for replicated data, and keep these points in mind:

- Site Recovery in the Azure portal can use storage accounts set up in Resource Manager, or in classic mode.
- The storage account can be standard or [premium](#). Use the results from the discovery stage—using Azure Migrate or a partner solution--to determine which account type is best for your environment.
- If you set up a premium account, you will also need an additional standard account for log data.
- Prepare VMware account permissions in advance. Azure Site Recovery requires access to VMware for the process server to automatically discover virtual machines. Because you

only want to migrate VMware virtual machines to Azure without ever failing them back, you can use a VMware account with a read-only role.

Create a Recovery Services vault

1. Sign in to the [Azure portal](#) > **Recovery Services**.
2. Click **New** > **Monitoring & Management** > **Backup and Site Recovery**.
3. In **Name**, specify a friendly name to identify the vault. If you have more than one subscription, select one of them.
4. [Create a resource group](#), or select an existing one. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery Pricing Details](#).
5. If you want to quickly access the vault from the dashboard, click **Pin to dashboard**, and then click **Create**.

The new vault will appear on **Dashboard** > **All resources** and on the main **Recovery Services vaults** blade.

Select a protection goal

In this task, select what you want to replicate, and where you want to replicate to.

1. Click **Recovery Services vaults** > vault.
2. In the Resource Menu, click **Site Recovery** > **Prepare Infrastructure** > **Protection goal**.
3. In Protection goal, select **To Azure** > **Yes, with VMware vSphere Hypervisor**.

Set up the source environment

In this task, set up the configuration server, register it in the vault, and discover virtual machines.

1. Click **Site Recovery** > **Step 1: Prepare Infrastructure** > **Source**.
2. If you don't have a configuration server, click **Configuration server**.
3. In **Add Server**, check that **Configuration Server** appears in **Server type**.
4. Download the Site Recovery Unified Setup installation file.
5. Download the vault registration key. You need this when you run Unified Setup. The key is valid for five days after you generate it.

Register the configuration server in the vault

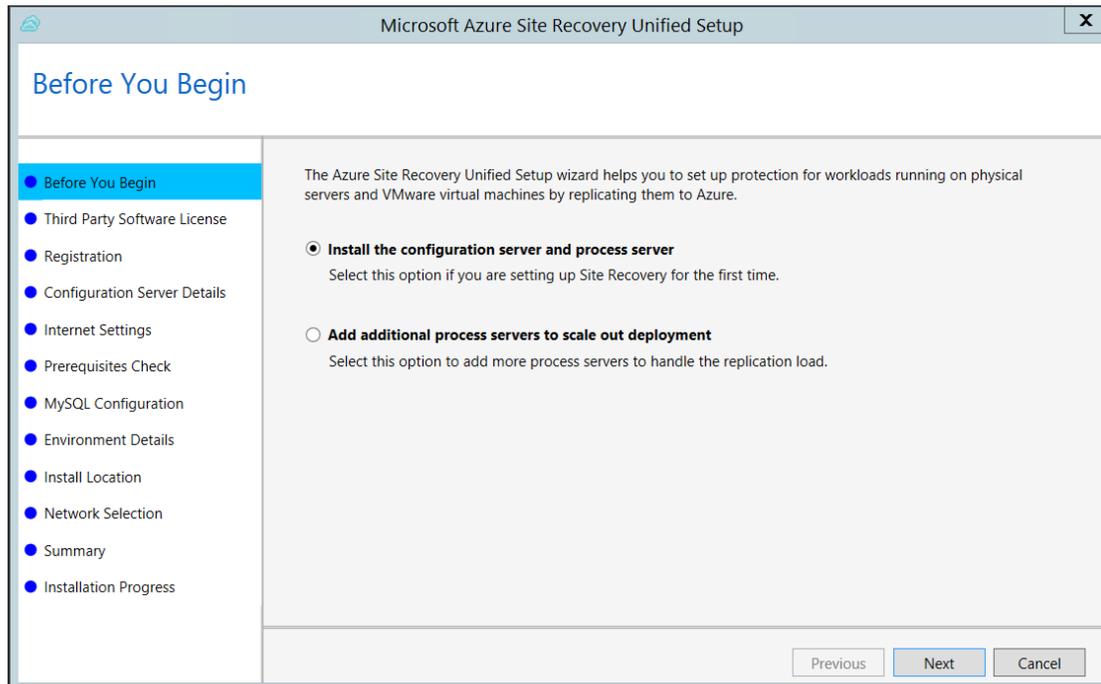
The next task requires you to run Unified Setup to install the configuration server, the process server, and the master target server. First however, do these three steps.

1. On the configuration server virtual machine, make sure that the system clock is synchronized with a [Time Server](#). It should match. If it's 15 minutes in front or behind, setup might fail.

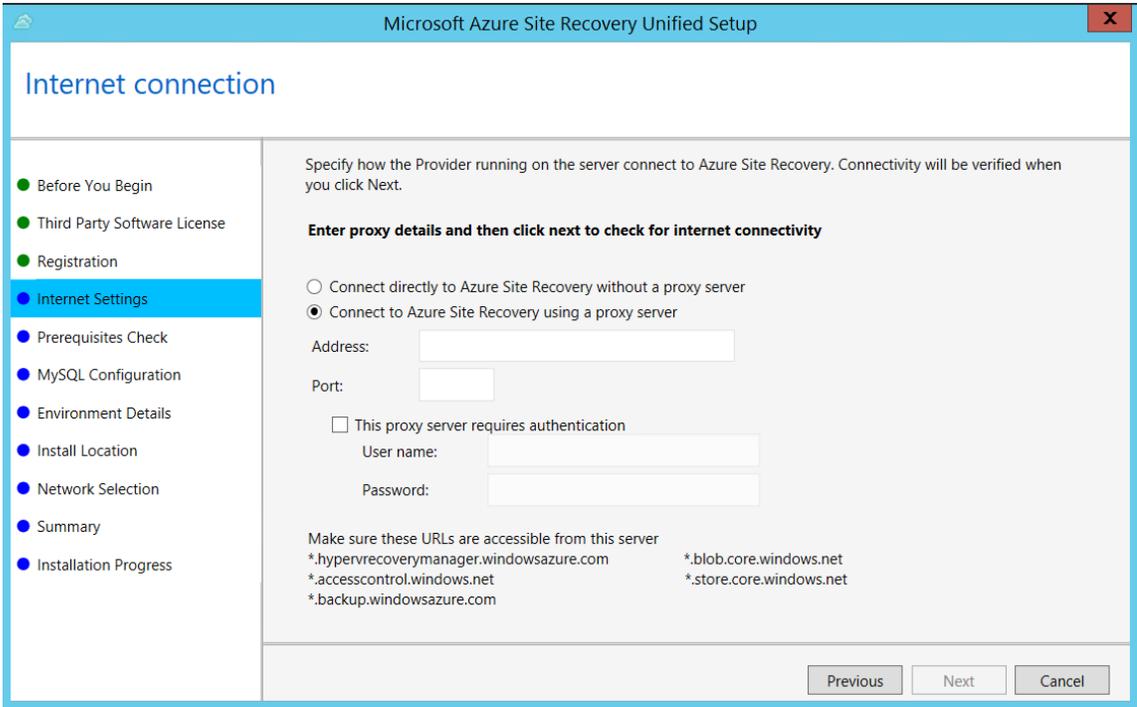
2. Run setup as a Local Administrator on the configuration server virtual machine.
3. Make sure TLS 1.0 is enabled on the virtual machine.

Now you are ready to run Setup.

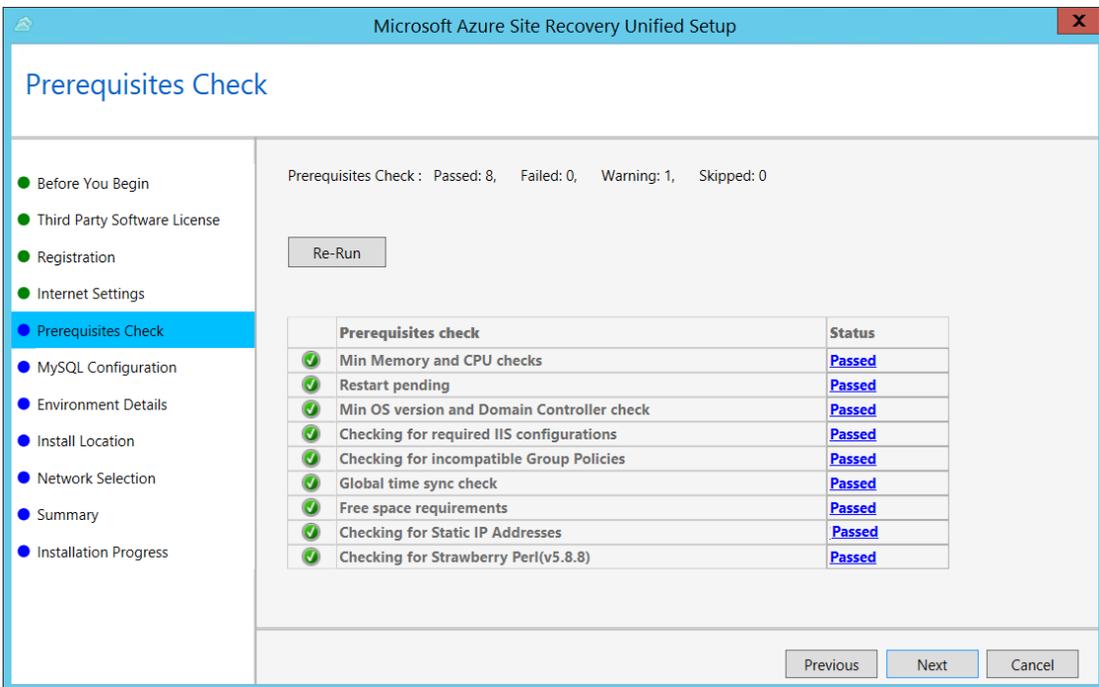
1. Run the Unified Setup installation file.
2. In **Before You Begin**, select **Install the configuration server and process server**.



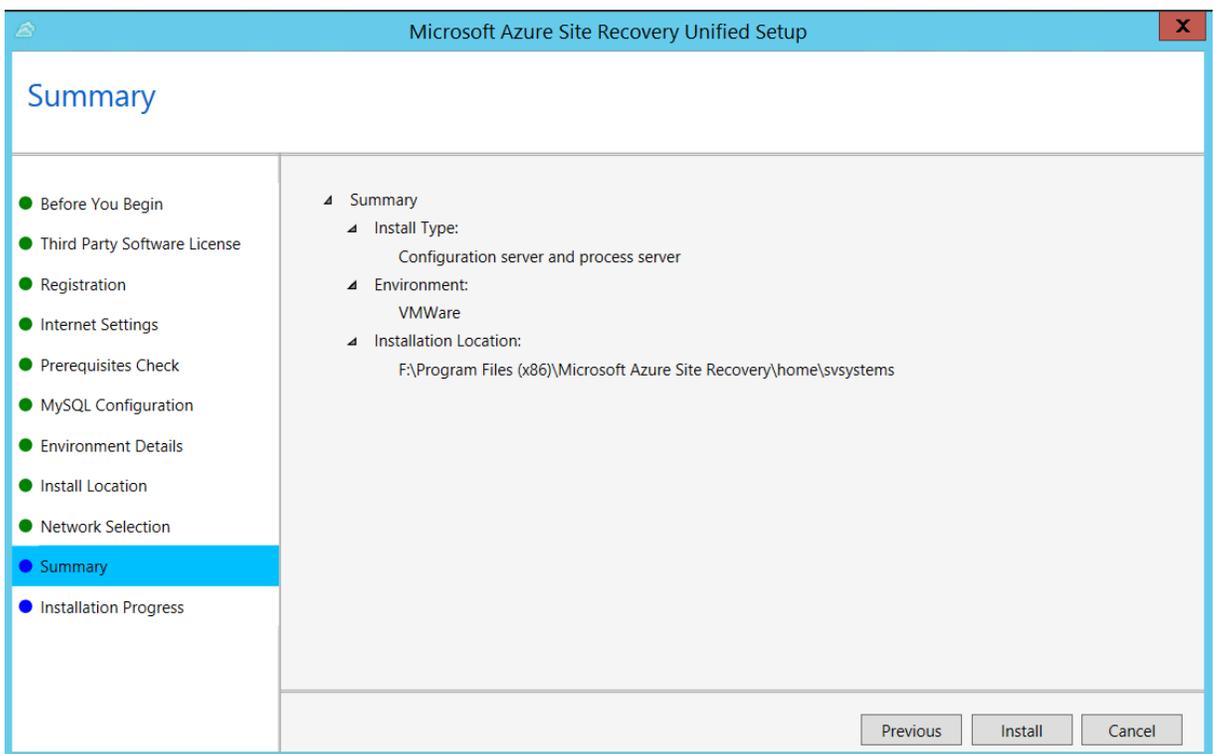
3. From the **Third-Party Software License** screen, click **I Accept** to download and install MySQL.
4. From the **Registration** screen, select the registration key you downloaded from the vault, and then click **Next**.
5. From the **Internet Settings** screen, specify how the Provider running on the configuration server connects to Azure Site Recovery over the Internet.
 - a. If you want to connect with the proxy that's currently set up on the machine, select **Connect to Azure Site Recovery using a proxy server**.
 - b. If you want the Provider to connect directly, select **Connect directly to Azure Site Recovery without a proxy server**.
 - c. If the existing proxy requires authentication, or if you want to use a custom proxy for the Provider connection, select **Connect with custom proxy settings**.
 - o If you use a custom proxy, you need to specify the address, port, and credentials.



- From the **Prerequisites Check** screen, run a check to make sure that installation can run. If a warning appears about the **Global time sync check**, verify that the time on the system clock (**Date and Time** settings) is the same as the time zone.



7. In the **MySQL Configuration** screen, create credentials for logging on to the MySQL server instance that is installed.
8. From the **Environment Details** screen, select whether to replicate VMware virtual machines. If you will, Setup checks that PowerCLI 6.0 is installed.
9. From the **Install Location** screen, select where you want to install the binaries and store the cache. The drive you select must have at least 5 GB of disk space available, but we recommend a cache drive with at least 600 GB of available space.
10. From the **Network Selection** screen, specify the listener (network adapter and SSL port) on which the configuration server sends and receives replication data. Port 9443 is the default port used for sending and receiving replication traffic, but you can modify this port number to suit your environment's requirements. In addition to the port 9443, we also open port 443, which is used by a web server to orchestrate replication operations. Do not use port 443 for sending or receiving replication traffic.
11. In the **Summary** screen, review the information and click **Install**. When installation finishes, a passphrase is generated. You will need this when you enable replication, so copy it and keep it in a secure location.



After registration finishes, the server is displayed on the **Settings > Servers** in the vault.

Note: The configuration server can also be installed from the command line.

Step 2: Connect to VMware servers

To allow Azure Site Recovery to discover virtual machines running in your on-premises environment, you need to connect your VMware vCenter Server or vSphere ESXi hosts with Site Recovery. Note the following before you start:

- If you add the vCenter server or vSphere hosts to Site Recovery with an account without administrator privileges on the server, the account needs these privileges enabled:
 - Datacenter, Datastore, Folder, Host, Network, Resource, Virtual machine, vSphere Distributed Switch.
 - The vCenter server needs Storage views permissions.
- When you add VMware servers to Site Recovery, it can take 15 minutes or longer for them to appear in the portal.

Step 3: Set up the target environment

Before you set up the target environment, make sure you have an Azure storage account and a virtual network set up.

1. Click **Prepare infrastructure > Target**, and select the Azure subscription you want to use.
2. Specify whether your target deployment model is Resource Manager-based, or classic.
3. Site Recovery verifies that you have one or more compatible Azure storage accounts and networks.

The screenshot shows a 'Target' configuration window for VMware. At the top, there are two expandable sections: '+ Storage account' and '+ Network'. Below these, the configuration is organized into three steps, each with a checkmark indicating completion:

- Step 1: Select Azure subscription**
 - * Subscription: Azure in Open
 - * Select the deployment model used after failover: Resource Manager
- Step 2: Ensure that at least one compatible Azure storage account exist**
 - Storage account(s): Found vmwarewebserver (Standard) storage account.
- Step 3: Ensure that at least one compatible Azure virtual network exist**
 - Network(s): MigrationNetwork

An 'OK' button is located at the bottom of the window.

Create replication policy

You need a replication policy to automate the replication to Azure.

1. To create a new replication policy, click **Site Recovery infrastructure > Replication Policies > Replication Policy**.
2. Under **RPO threshold**, specify the RPO limit. This value specifies how often data recovery points are created. An alert is generated if continuous replication exceeds this limit.
3. Under **Recovery point retention**, specify (in hours) how long the retention window is for each recovery point. Replicated virtual machines can be recovered to any point in a window. Up to 24 hours retention is supported for machines replicated to premium storage, and 72 hours for standard storage.
4. Under **App-consistent snapshot frequency**, specify how often (in minutes) recovery points containing application-consistent snapshots will be created.
5. Click **OK** to create the policy.
6. When you create a new policy it's automatically associated with the configuration server. By default, a matching policy is automatically created for failback. For example, if the replication policy is **rep-policy** then the failback policy will be **rep-policy-failback**. The failback policy isn't used until you initiate a failback from Azure.

Create replication policy
VMware

* Name ⓘ
VMware-Migration-Policy x

Source type ⓘ
VMware / Physical machines v

Target type ⓘ
Azure v

* RPO threshold in mins ⓘ
15

* Recovery point retention in hours ⓘ
24

* App-consistent snapshot frequency in mins ⓘ
60

Failback replication policy name ⓘ
Enter policy name

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

OK

Prepare for push installation of the Mobility service

The Mobility service must be installed on all virtual machines you want to replicate. There are several ways to install the service, including manual installation, push installation from the Site Recovery process server, and installation using methods such as System Center Configuration Manager. Here you can review [prerequisites and installation methods for the Mobility Service](#).

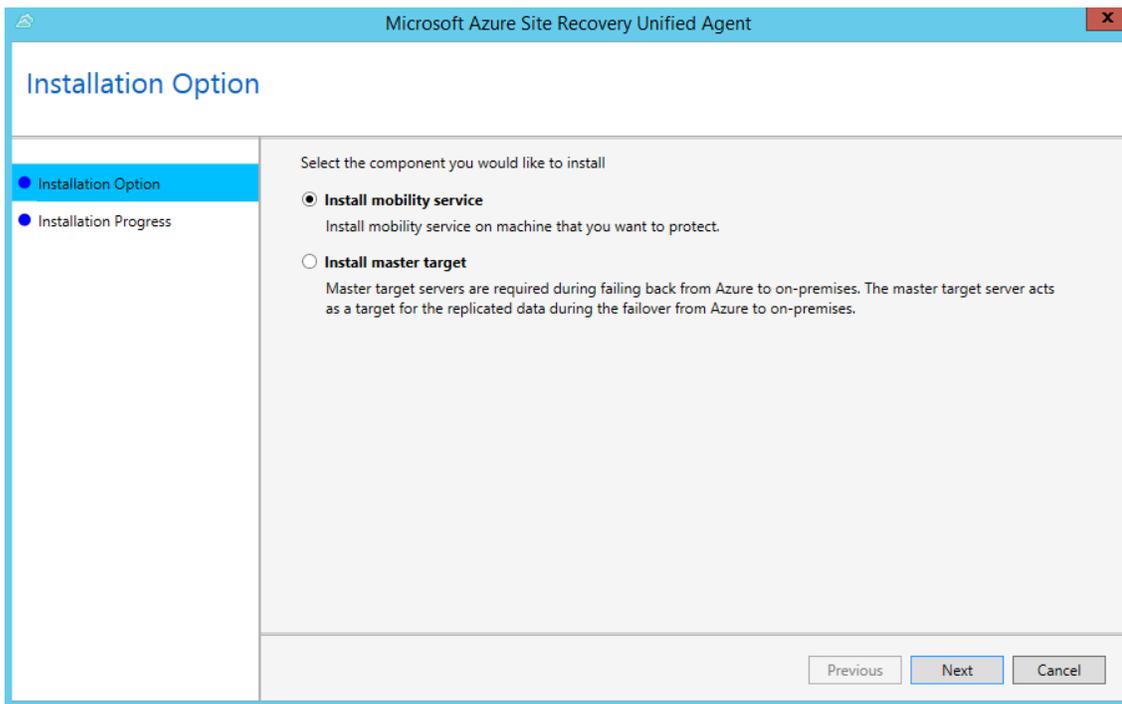
If you want to use push installation from the Azure Site Recovery process server, you need to prepare an account that Azure Site Recovery can use to access the virtual machine. The following describes the options:

- You can use a domain or local account

- For Windows, if you're not using a domain account, you need to disable Remote User Access control on the local machine. To do this, in the registry under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**, add the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 1.
- If you want to add the registry entry for Windows from a CLI, type: `REG ADD HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v LocalAccountTokenFilterPolicy /t REG_DWORD /d 1.`
- For Linux, the account should be root on the source Linux server.

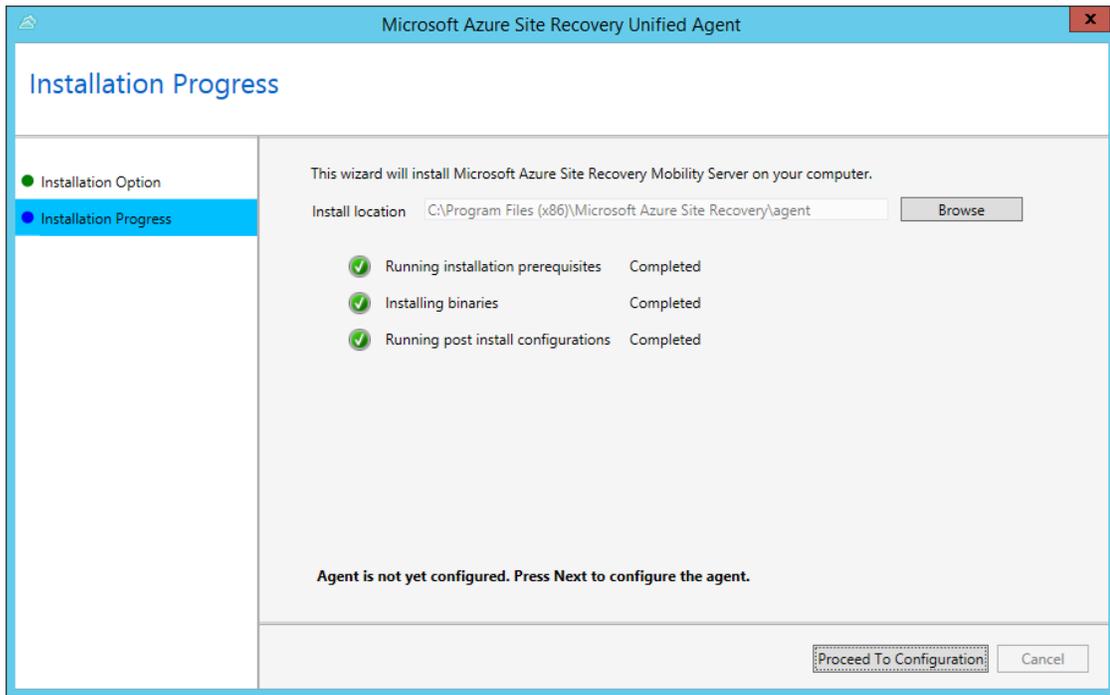
Install Mobility Service manually by using the GUI

1. Copy the installer executable to the virtual machine that is being migrated to Azure, and then open the installer.
2. On the **Installation Option** pane, select **Install Mobility Service**.

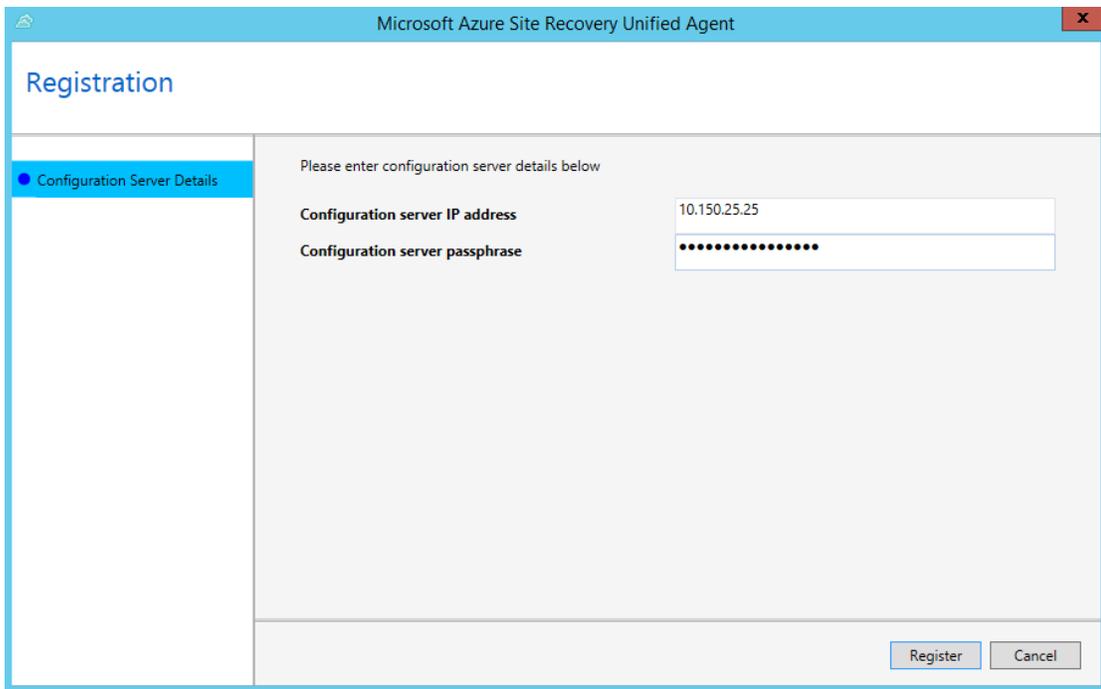


3. Select the install location and click **Install** to begin the installation procedure.

4. You can use **Installation Progress** page to monitor the installer's progress.



5. Once installation is complete, click the **Proceed to Configuration** button to register the Mobility Service with your Configuration server.



6. Click on the **Register** button to complete the registration.

Read about [other methods to install the Mobility Service](#).

Configure replication

After you have installed and configured both the Process Server and the Mobility Service agents, continue configuring replication in Azure.

1. In the Azure portal, navigate to **Site Recovery** > **Step1: Replicate Application** > **Enable Replication**, and then click **Step 1: Source Configure** > **Source**.
2. In **Source**, select **On-Premises**.
3. In **Source location**, select your Configuration Server.
4. In **Machine type**, select **Virtual Machines**.
5. In **vCenter/vSphere Hypervisor**, select the vCenter server that manages the vSphere host, or select the host.
6. Select the process server or the configuration server if you haven't created any additional process servers, and then click **OK**.

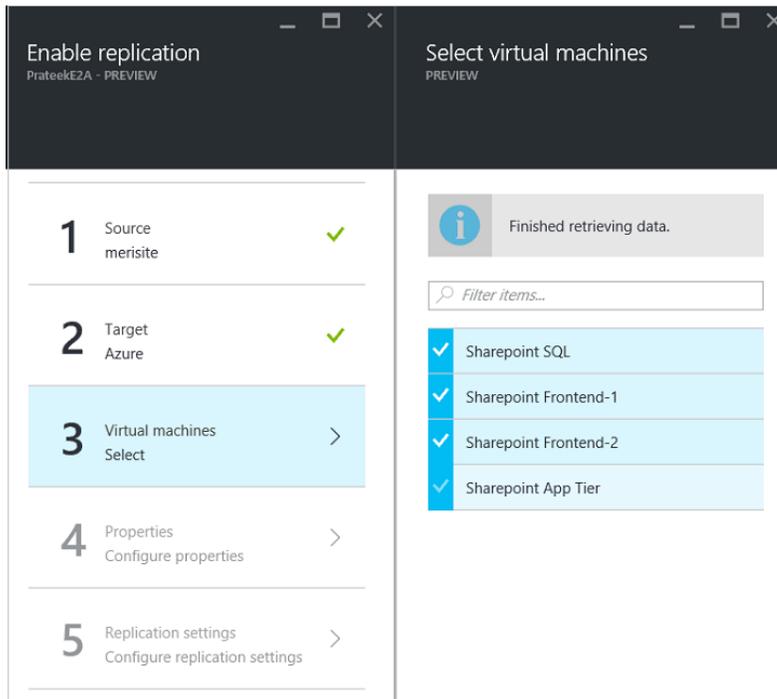
The screenshot displays two side-by-side windows from the Azure portal. The left window, titled 'Enable replication', shows a progress bar with three steps: '1 Source Configure', '2 Virtual machines Select', and '3 Replication settings Configure replication settings'. The 'Source Configure' step is highlighted in blue. Below the progress bar is an 'Enable replication' button. The right window, titled 'Source', is titled 'Select your source environment' and contains five dropdown menus: 'Source' (set to 'On-premises'), '* Source location' (set to 'WIN-I87O1JB9J2G'), '* Machine type' (set to 'Virtual Machines'), '* vCenter server/vSphere host' (set to 'vCenter1'), and '* Process server' (set to 'WIN-I87O1JB9J2G (Inbuilt Process Server)'). Below these dropdowns is an 'OK' button.

7. In **Target**, select the subscription and the resource group in which you want to create the migrated virtual machines. Choose the deployment model for the migrated virtual machines that you want to use in Azure (classic or resource manager).
8. Select the Azure storage account you want to use for replicating data. If you don't want to use an account you've already set up, you can create a new one.
9. Select the Azure network and subnet to which Azure Virtual Machines will connect when they're created after migration. Select **Configure now for selected machines** to apply the network setting to all machines you select for protection, or select **Configure later** to select the Azure network per virtual machine.

Note If you don't want to use an existing network, you can create one.

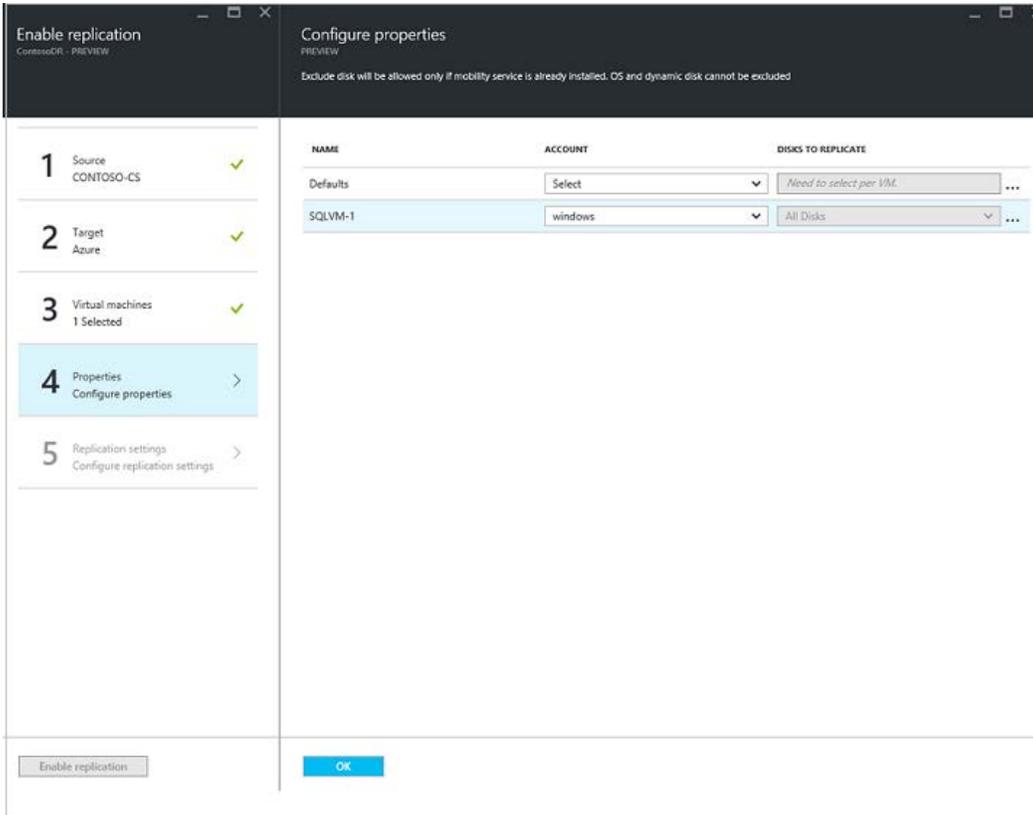
The screenshot shows two side-by-side windows from the VMware interface. The left window, titled 'Enable replication', contains a progress list with five steps: 1. Source (WIN-I87O1JB9J2G) with a green checkmark; 2. Target (Configure) which is highlighted in blue and has a right-pointing arrow; 3. Virtual machines (Select) with a right-pointing arrow; 4. Properties (Configure properties) with a right-pointing arrow; and 5. Replication settings (Configure replication settings) with a right-pointing arrow. At the bottom of this window is a greyed-out 'Enable replication' button. The right window, titled 'Target', is for configuring recovery settings. It includes a header 'Select your target settings for recovery' and several dropdown menus: 'Target' (set to Azure), 'Subscription' (set to Azure in Open), 'Post-failover resource group' (set to Migration), 'Post-failover deployment model' (set to Resource Manager), 'Storage account' (set to vmwarewebserver), 'Azure network' (set to 'Configure now for selected machines.'), 'Post-failover Azure network' (set to MigrationNetwork), and 'Subnet' (set to default (10.0.0.0/24)). At the bottom of this window is a blue 'OK' button.

10. Point to **Virtual Machines** > **Select**, select each enabled machine you want to replicate, and then click **OK**.



11. In **Properties** > **Configure properties**, select the process server account that will automatically install the Mobility service on the machine.

- By default, all disks are replicated. Click **All Disks** and clear any disks you don't want to replicate, and then click **OK**. You can set additional virtual machine disk properties later if needed.

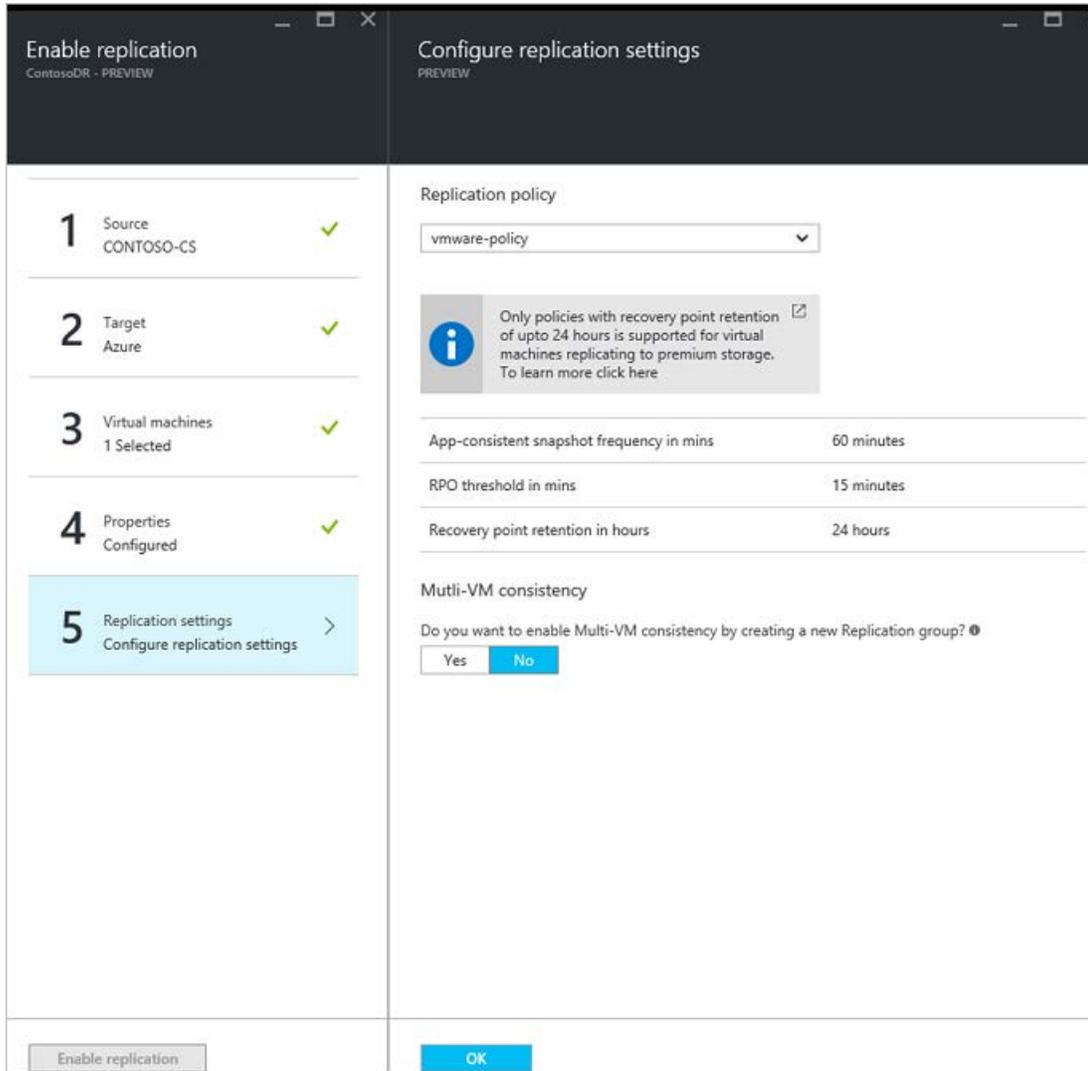


- In **Replication settings > Configure replication settings**, verify that the correct replication policy is selected. If you modify a policy, changes will be applied to the replicating machine and to new machines.
- Enable **Multi-VM consistency** if you want to gather machines into a replication group, specify a name for the group, and then click **OK**.

Important

Machines in replication groups replicate together, and have shared crash-consistent and app-consistent recovery points when they fail over.

We recommend that you gather virtual machines and physical servers together so that they mirror your workloads. Enabling multi-VM consistency can impact workload performance and should only be used if machines are running the same workload and you need consistency.



15. Click **Enable Replication**. You can track progress of the **Enable Protection** job in **Settings > Jobs > Site Recovery Jobs**. After the **Finalize Protection** job runs the machine is ready for failover.

Step 4: Complete migration

Because migration is different than failover, it is important to configure Site Recovery for a migration.

For migration, you don't need to commit a failover or delete machines. Instead, select the **Complete Migration** option for each machine you want to migrate.

1. In **Replicated Items**, right-click the virtual machine, and then click **Complete Migration**.
2. Click **OK** to complete the migration.

You can track progress in the virtual machine properties by monitoring the Complete Migration job in Site Recovery jobs. The Complete Migration action completes the migration process, removes replication for the machine, and stops Site Recovery billing for the machine.

At this point, your virtual machine has been migrated to Azure and you can begin using the IP addresses you set up in Networking. If you must migrate a database, the next section outlines migrating SQL Server databases using Migration Data Assistant and Azure Database Migration Service. Otherwise, the migration process continues with [Stage 3: Optimize](#) later in this guide.

Optional: Migrate a SQL Server database to Azure SQL Database

In some cases, the SQL Server database can be migrated directly with the virtual machine. The migration process is less complex if you migrate the database to the SQL Server service in Azure. Microsoft Data Migration Assistant (DMA) and the Azure Database Migration Service (DMS) streamline the process by creating a migration workflow that helps move database schemas, data and users, server roles, and SQL and Windows logins.

- Microsoft Data Migration Assistant enables discovery and assessment of current data environment, identifies compatibility issues, and recommends performance and reliability improvements.
- Azure Database Migration Service partners with DMA to migrate existing on-premises SQL Server, Oracle, and MySQL databases to Azure SQL Database, Azure SQL Database Managed Instance or SQL Server on Azure virtual machines.

This guide outlines how to use DMA and DMS to discover, assess, and migrate a SQL Server, Oracle, or MySQL database to Azure. The processes for assessing and migrating SQL Server to Azure can help organizations increase database performance through the selection of high-performance CPUs, increased memory size, or improved disk type through Premium Storage.

Moving a SQL Server database to Microsoft Azure SQL Database with Data Migration Assistant is a three-part process:

1. Prepare a database in a SQL Server for migration to Azure SQL Database using the [Data Migration Assistant](#) (DMA).
2. Export the database to a BACPAC file.
3. Import the BACPAC file into an Azure SQL Database.

Using Microsoft Data Migration Assistant

Step 1: Prepare for migration

Complete these prerequisites:

- Install the newest version of Microsoft [SQL Server Management Studio](#) (SSMS). Installing SSMS also installs the newest version of SQLPackage, a command-line utility that can be used to automate a range of database development tasks.
- Download and Install the Microsoft [Data Migration Assistant](#) (DMA).
- Identify and have access to a database to migrate.

Note: If there is a need to fix compatibility issues, use [SQL Server Data Tools](#).

Follow these steps to use [Data Migration Assistant](#) to assess the readiness of your database for migration to Azure SQL Database:

1. Open the Microsoft Data Migration Assistant. You can run DMA on any computer with connectivity to the SQL Server instance containing the database that you plan to migrate; you do not need to install it on the computer hosting the SQL Server instance.
2. In the left-hand menu, click **New** to create an **Assessment** project. Fill in the form with a **Project name** (all other values should be left at their default values), and then click **Create**.
3. On the **Options** page, click **Next**.
4. On the **Select sources** page, enter the name of SQL Server instance containing the server you plan to migrate. Change the other values on this page if necessary, and then click **Connect**.
5. In the **Add sources** portion of the **Select sources** page, select the checkboxes for the databases to be tested for compatibility, and then click **Add**.
6. Click **Start Assessment**.
7. When the assessment completes, look for the checkmark in the green circle to see if the database is sufficiently compatible to migrate.
8. Review the results the **SQL Server feature parity** results. Specifically review the information about unsupported and partially supported features, and the recommended actions.
9. Review the **Compatibility issues** by clicking that option in the upper left. Specifically review the information about migration blockers, behavior changes, and deprecated features for each compatibility level. For the AdventureWorks2008R2 database, review the changes to Full-Text Search since SQL Server 2008, and the changes to SERVERPROPERTY('LCID') since SQL Server 2000. For details about these changes, links for more information are provided. Many search options and settings for Full-Text Search have changed.

Important

After you migrate your database to Azure SQL Database, you can choose to operate the database at its current compatibility level (level 100 for the AdventureWorks2008R2 database) or at a higher level. For more information on the implications and options for operating a database at a specific

compatibility level, see [ALTER DATABASE Compatibility Level](#). See also [ALTER DATABASE SCOPED CONFIGURATION](#) for information about additional database-level settings related to compatibility levels.

10. Optionally, click Export report to save the report as a JSON file.
11. Close the Data Migration Assistant.

Step 2: Export to BACPAC file

To make the database portable for import into Azure, you need to create a BACPAC file. A BACPAC file is a .zip file with an extension of BACPAC containing the metadata and data from a SQL Server database. A BACPAC file can be stored in Azure blob storage or in local storage for archiving or for migration, for example from SQL Server to Azure SQL Database. For an export to be transactional and consistent, you must ensure that no write activity is occurring during the export.

Follow these steps to use the SQLPackage command-line utility to export the AdventureWorks2008R2 database to local storage.

1. Open a Windows command prompt and change your directory to a folder in which you have the **130** version of SQLPackage, such as **C:\Program Files (x86)\Microsoft SQL Server\130\DAC\bin**.
2. Execute the following SQLPackage command at the command prompt to export the **AdventureWorks2008R2** database from **localhost** to **AdventureWorks2008R2.bacpac**. Change any of these values as appropriate to your environment.

```
SQLPackageCopy
```

```
sqlpackage.exe /Action:Export /ssn:localhost /sdn:AdventureWorks2008R2 /tf:AdventureWorks2008R2.bacpac
```

Once the execution is complete the generated BACPAC file is stored in the directory where the sqlpackage executable is located. In this example, **C:\Program Files (x86)\Microsoft SQL Server\130\DAC\bin**.

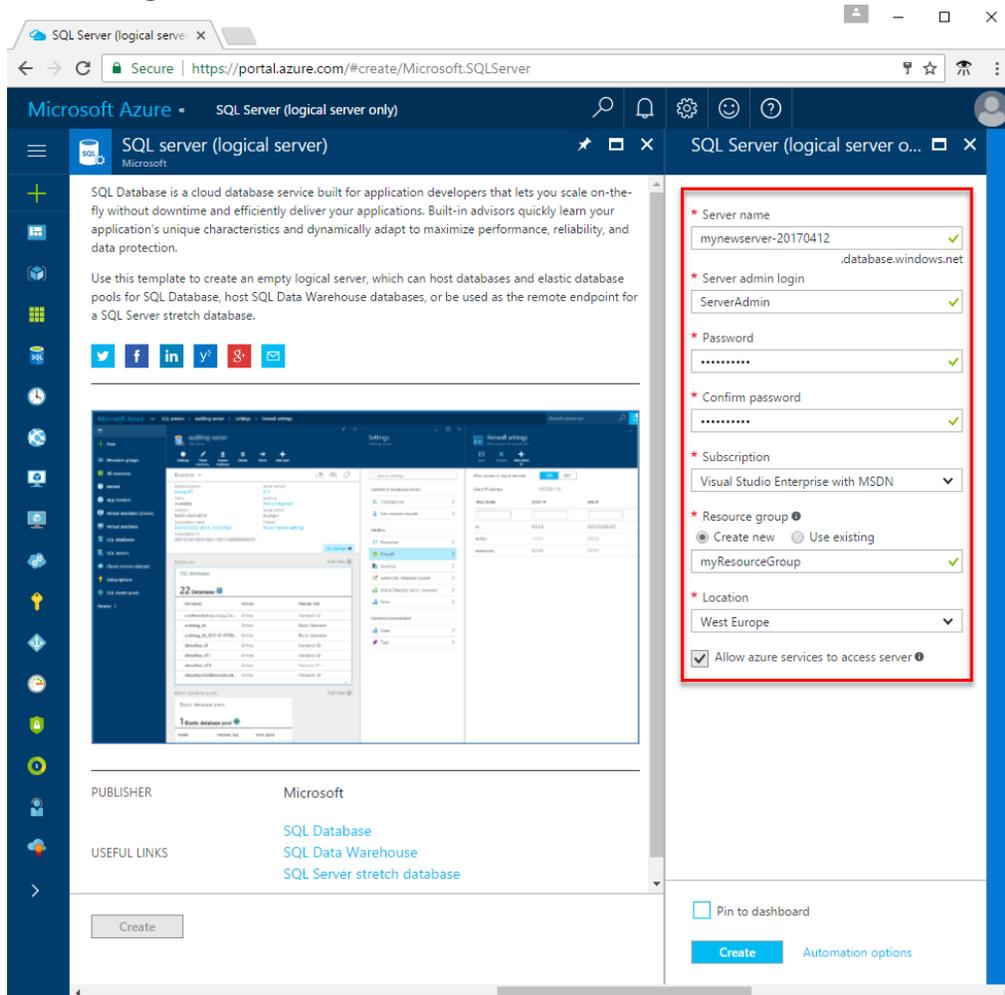
3. Log in to the [Azure portal](#).

Note: Logging on from the computer from which you are running the SQLPackage command-line utility eases the creation of the firewall rule in step 5.

4. Create a SQL Server logical server

A **SQL Server logical server** acts as a central administrative point for multiple databases. Follow these steps to create a SQL server logical server to contain the migrated Adventure Works OLTP SQL Server database.

- Click the **New** button found on the upper left-hand corner of the Azure portal.
- Type **sql server** in the search window on the **New** page, and select **SQL server (logical server)** from the filtered list.
- Click **Create**, and enter the properties for the new SQL Server (logical server).
- Complete the SQL server (logical server) form with the values from the red box in this image.



- Click **Create** to provision the logical server. Provisioning takes a few minutes.

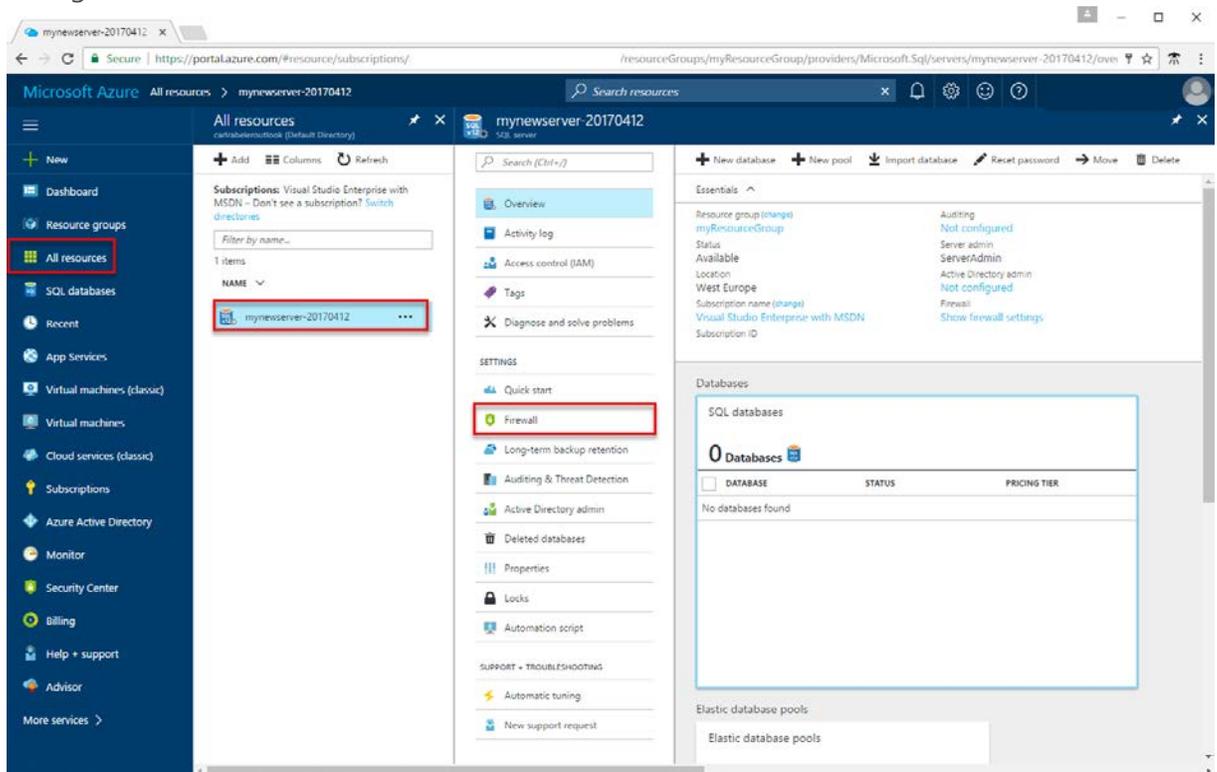
Important

Remember your server name, server admin login name, and password. You need these values later in this tutorial.

Step 3: Create a server-level firewall rule

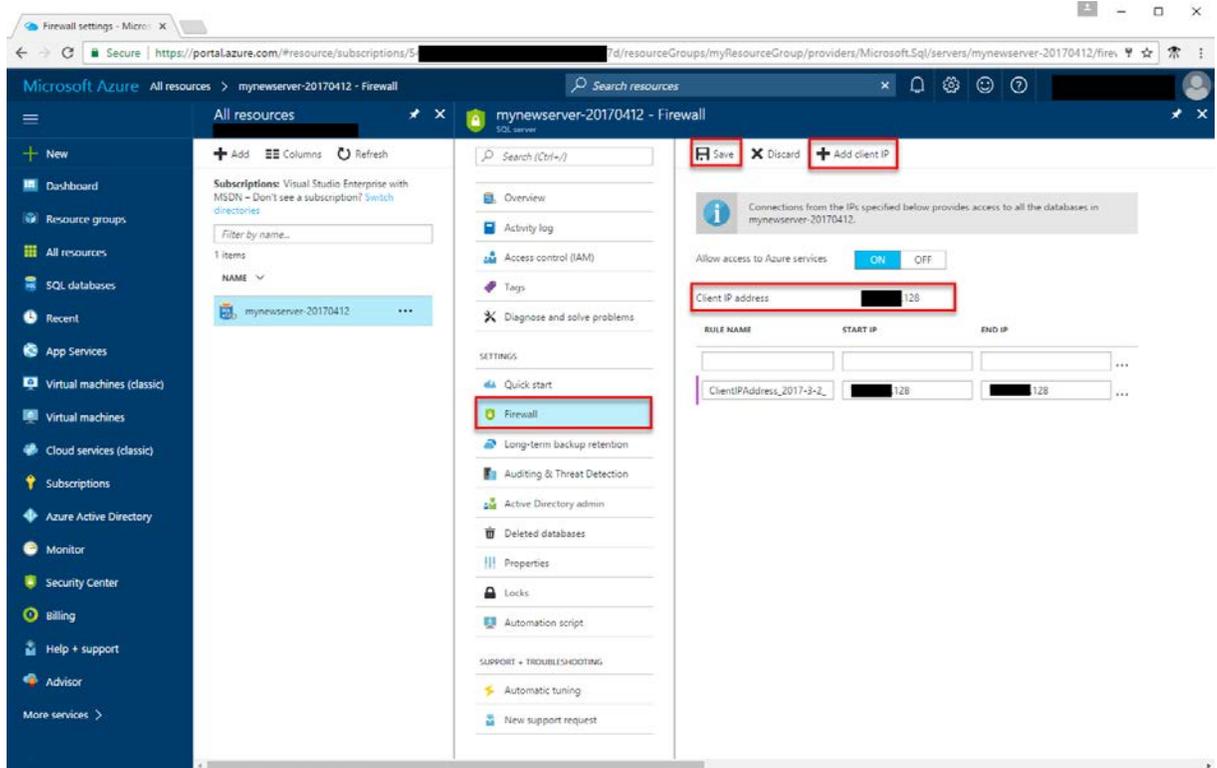
The SQL Database service creates a firewall at the server-level that prevents external applications and tools from connecting to the server or any databases on the server unless a firewall rule is created to open the firewall for specific IP addresses. Follow these steps to create a SQL Database server-level firewall rule for the IP address of the computer from which you are running the SQLPackage command-line utility. This allows SQLPackage to connect to the SQL Database logical server through the Azure SQL Database firewall.

1. Click **All resources** from the left-hand menu, and click the new server on the **All resources** page. The overview page for the server opens and provides options for further configuration.



2. Click **Firewall** in the left-hand menu under **Settings** on the overview page.

3. Click **Add client IP** on the toolbar to add the IP address of the computer you are currently using, and then click **Save**. This creates a server-level firewall rule for this IP address.



4. Click **OK**.

You can now use the server admin account you created to connect to all databases on this server using Microsoft SQL Server Management Studio or another tool of your choice.

Note: SQL Database communicates over port 1433. If you are trying to connect from within a corporate network, outbound traffic over port 1433 may not be allowed by your network's firewall. If so, you cannot connect to your Azure SQL Database server unless your IT department opens port 1433.

Step 3: Import a BACPAC file to Azure SQL Database

At this point, you should use the BACPAC file you created earlier. The newest versions of the SQLPackage command-line utility provides support for creating an Azure SQL database at a specified [service tier and performance level](#). For best performance during the import process, select a high service tier and performance level, and then scale down after import if the service tier and performance level is higher than you need.

The SQLPackage command-line utility is the preferred method to import your BACPAC database to Azure SQL Database for most production environments. For more information, see [Migrating from SQL Server to Azure SQL Database using BACPAC Files](#).

Execute the following SQLPackage command at the command prompt to import your database from local storage to the SQL server logical server that you previously created to a new database, a service tier of **Premium**, and a Service Objective of **P6**. Replace the values in angle brackets with appropriate values for your SQL server logical server and specify a name for the new database (also replace the angle brackets). You can also choose to change the values for database edition and service object give as appropriate to your environment. For this tutorial, the migrated database is called **myMigratedDatabase**.

Copy

```
SqlPackage.exe /a:import /tcs:"Data
Source=<your_server_name>.database.windows.net;Initial
Catalog=<your_new_database_name>;User
Id=<change_to_your_admin_user_account>;Password=<change_to_your_passwor
d>" /sf:AdventureWorks2008R2.bacpac /p:DatabaseEdition=Premium
/p:DatabaseServiceObjective=P6
```

Important

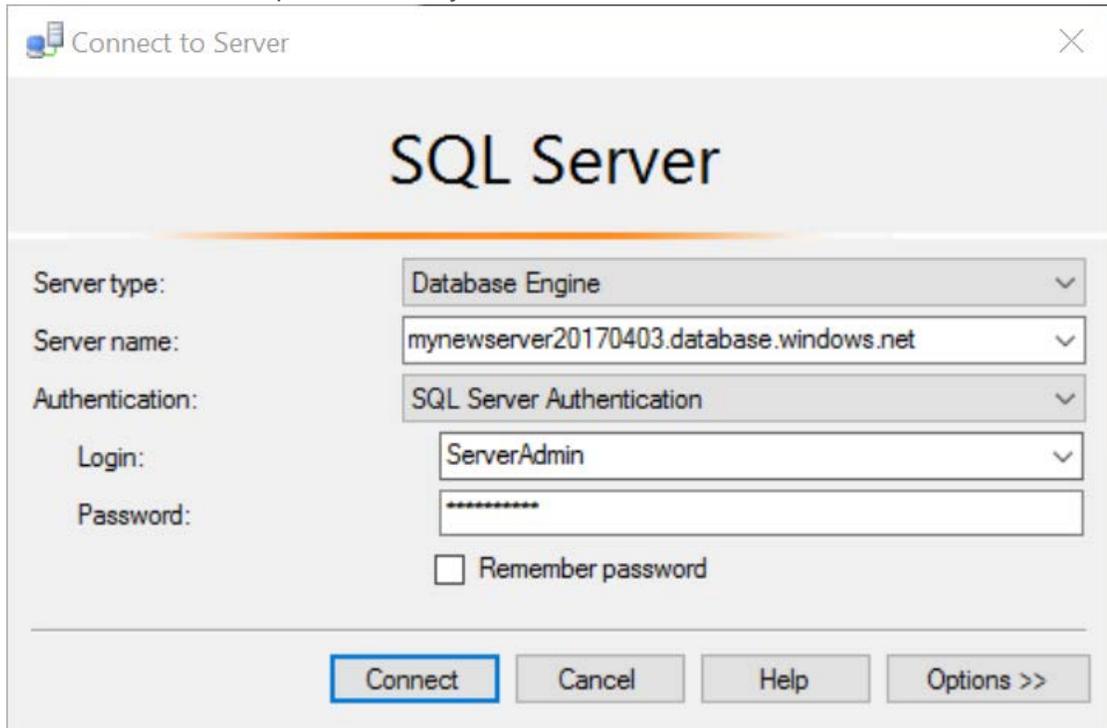
A SQL server logical server listens on port 1433. If you are attempting to connect to a SQL server logical server from within a corporate firewall, this port must be open in the corporate firewall for you to successfully connect.

Connect using SQL Server Management Studio (SSMS)

Use SQL Server Management Studio to establish a connection to your Azure SQL Database server and the newly migrated database called **myMigratedDatabase** in this tutorial. If you are running SSMS on a different computer from which you ran SQLPackage, create a firewall rule for this computer using the steps in the previous procedure.

1. Open SQL Server Management Studio.
2. In the **Connect to Server** dialog box, enter this information.
 - **Server type:** Specify Database engine
 - **Server name:** Enter your fully qualified server name, such as **mynewserver20170403.database.windows.net**
 - **Authentication:** Specify SQL Server Authentication

- **Login:** Enter your server admin account
- **Password:** Enter the password for your server admin account



3. Click **Connect**.
4. In **Object Explorer**, expand **Databases**, and then expand **myMigratedDatabase** to view the objects in the sample database.

Change database properties

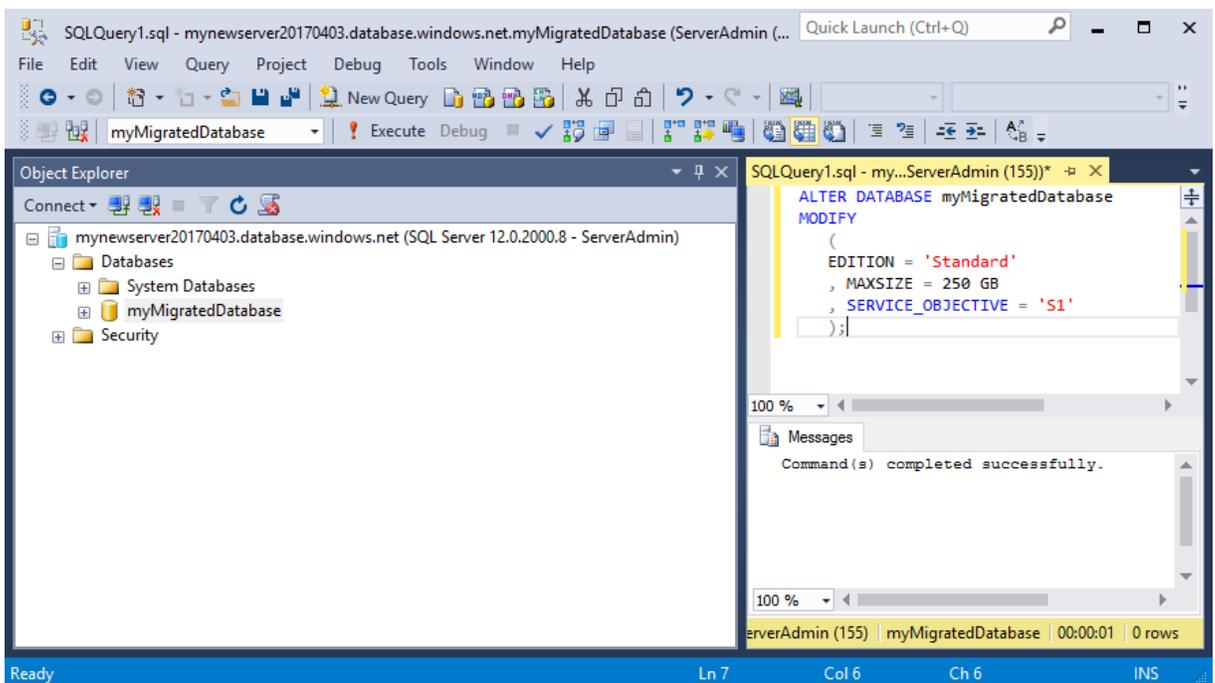
You can change the service tier, performance level, and compatibility level using SQL Server Management Studio. During the import phase, we recommend that you import to a higher performance tier database for best performance, but one that you may scale down after the import completes to save money until you are ready to actively use the imported database.

Changing the compatibility level may yield better performance and access to the newest capabilities of the Azure SQL Database service. When you migrate an older database, its database compatibility level is maintained at the lowest supported level compatible with the database being imported. For more information, see [Improved query performance with compatibility Level 130 in Azure SQL Database](#).

1. In **Object Explorer**, right-click **myMigratedDatabase** and click **New Query**. A query window opens connected to your database.
2. Execute the following command to set the service tier to Standard and the performance level to **S1**.

Copy

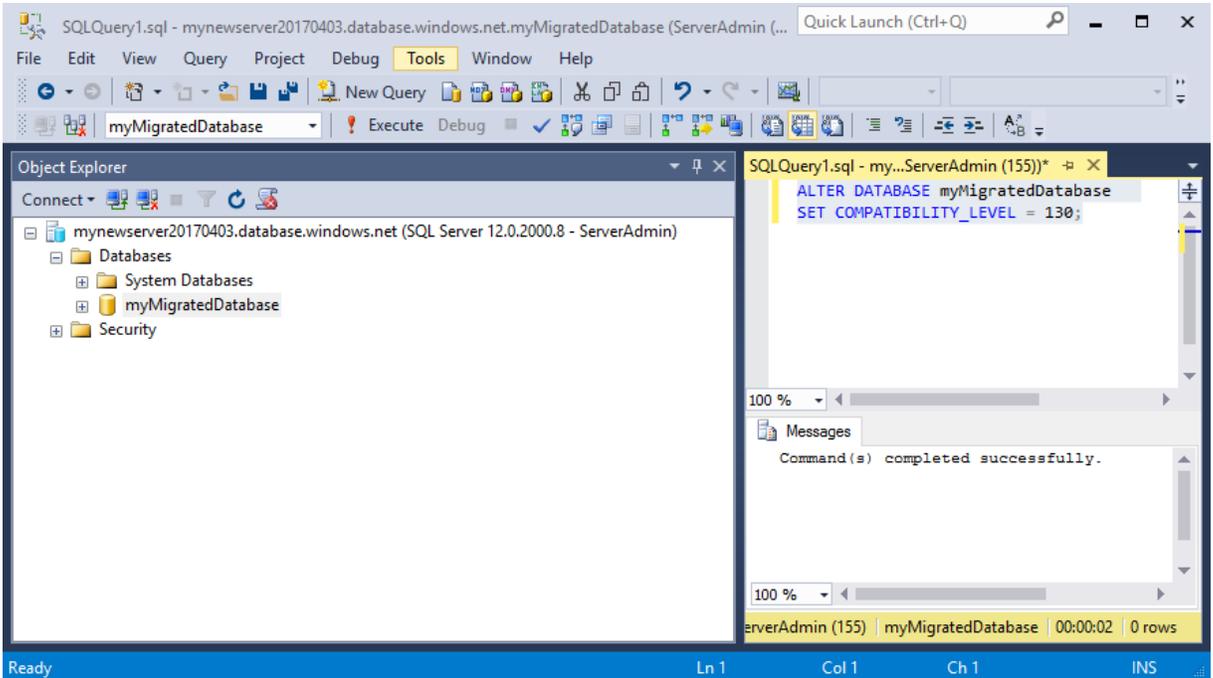
```
ALTER DATABASE myMigratedDatabase
MODIFY
(
    EDITION = 'Standard'
    , MAXSIZE = 250 GB
    , SERVICE_OBJECTIVE = 'S1'
);
```



3. Execute the following command to change the database compatibility level to 130.

Copy

```
ALTER DATABASE myMigratedDatabase
SET COMPATIBILITY_LEVEL = 130;
```



At this point you should have full control of the migrated database.

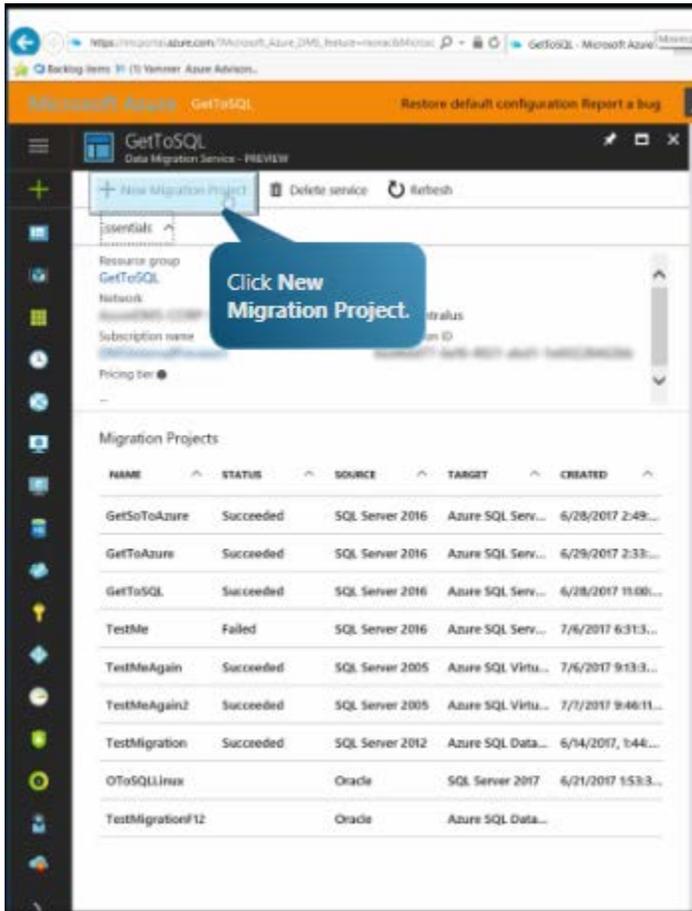
Using Azure Database Migration Service

Azure Database Migration Service (ADMS), now in limited preview, can help you migrate existing on-premises SQL Server, Oracle, and MySQL databases to Azure SQL Database, Azure SQL Database Managed Instance, or SQL Server on an Azure Virtual Machine.

ADMS is designed to simplify the complex workflows you can encounter when migrating various database types to databases in Azure.

Before performing a migration, an assessment report is used to pinpoint issues that must be addressed prior to the migration. After you resolve the issues, you can perform the migration. To perform a database migration using Azure Database Migration Service, complete these steps:

1. In the Azure portal, select **Data Migration Service**, and then click **New Migration Project**.



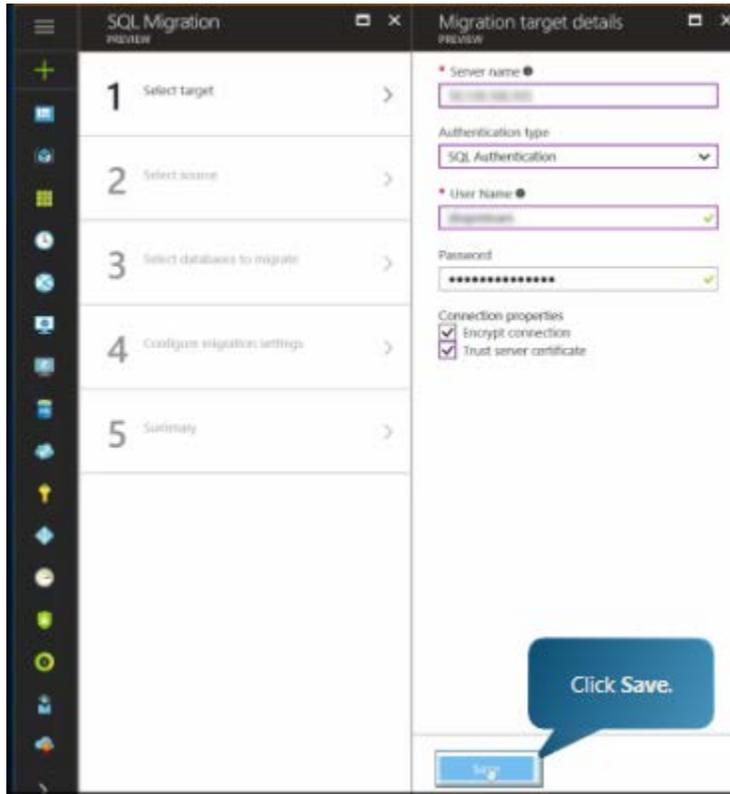
2. In **New Migration Project**, enter a unique project name, server source type and a target server type.

3. Click **Start**.

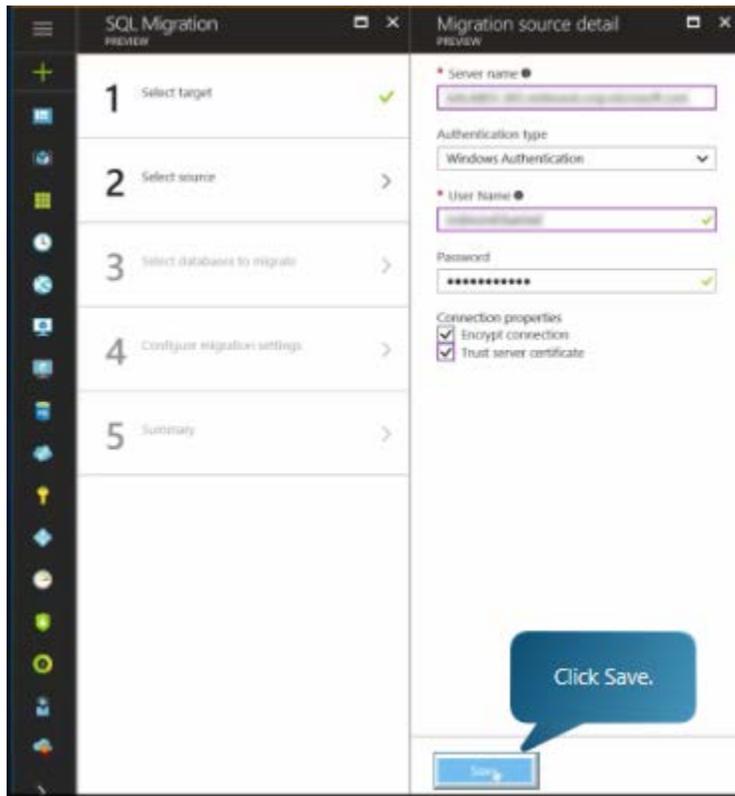
The screenshot shows the GetToSQL Data Migration Service interface. The main window displays a list of migration projects with columns for NAME, STATUS, SOURCE, TARGET, and CREATED. A 'New migration project' dialog box is open on the right, showing a 'Start' button at the bottom. A blue callout bubble with the text 'Click Start.' points to the 'Start' button.

NAME	STATUS	SOURCE	TARGET	CREATED
GetSoToAzure	Succeeded	SQL Server 2016	Azure SQL Serv...	6/28/2017 2:48...
GetToAzure	Succeeded	SQL Server 2016	Azure SQL Serv...	6/29/2017 2:33...
GetToSQL	Succeeded	SQL Server 2016	Azure SQL Serv...	6/28/2017 11:00...
TestMe	Failed	SQL Server 2016	Azure SQL Serv...	7/6/2017 6:31:3...
TestMeAgain	Succeeded	SQL Server 2005	Azure SQL Virtu...	7/6/2017 9:13:3...
TestMeAgain2	Succeeded	SQL Server 2005	Azure SQL Virtu...	7/7/2017 9:46:11...
TestMigration	Succeeded	SQL Server 2012	Azure SQL Data...	6/14/2017, 1:44...
OToSQLLinux		Oracle	SQL Server 2017	6/21/2017 1:53:3...
TestMigration12		Oracle	Azure SQL Data...	

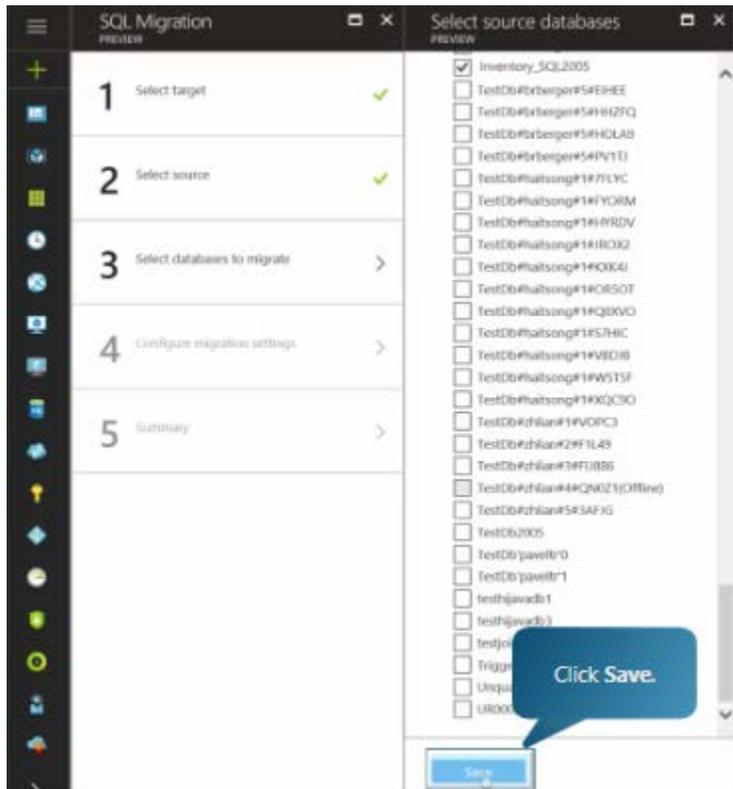
4. Provide all options under **Migration target details**, and then click **Save**.



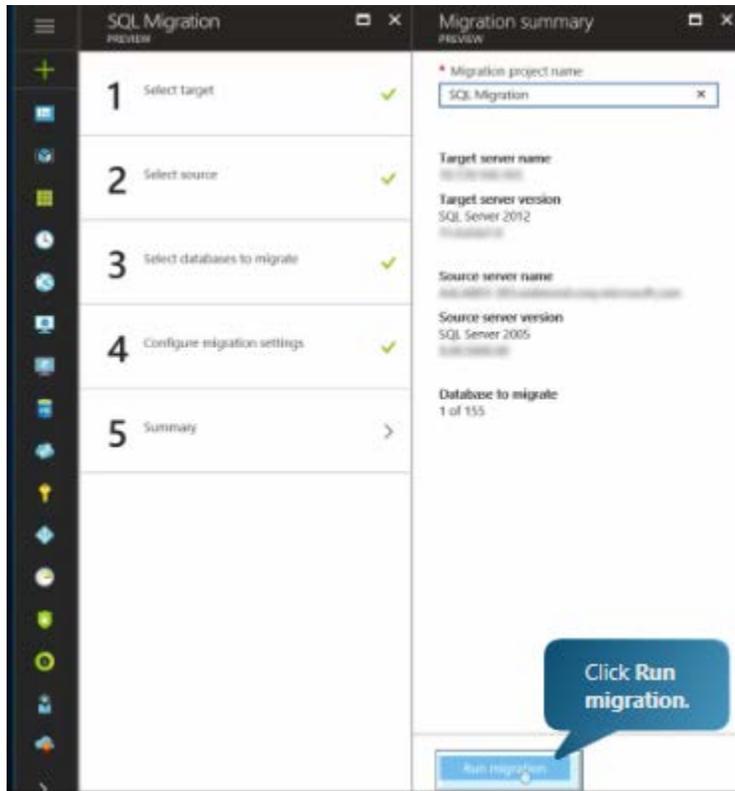
5. Provide all options under **Migration source detail**, and then click **Save**.



- In the **Select source** databases list, select each source database you want to migrate, and then click **Save**.



- Review the details summary, and then click **Run Migration** to start the migration. The amount of time the migration will run depends on a variety of factors including size and complexity of the database, source disk speed, and network speed.



- Once the migration is finished, a **Completed** status will be displayed in the SQL Migration dashboard.



Stage 3: Optimize migrated workloads

For many organizations, migrating workloads to the cloud gives them more resources and tools to optimize their computing environment and gain operational efficiencies compared to operating on-premises. Microsoft provides a range of technologies to assist with workload optimization, including cost optimization.

Using the broad range of management capabilities available with Microsoft Azure services, you can optimize and secure almost every operational aspect of your computing environment in Azure, including the virtual machines you have migrated from your on-premises environment. For example, you can use Azure Cost Management to track daily costs and make right-sizing decisions. You can use Azure Log Analytics to analyze Azure data to determine how much CPU or memory a virtual machine is using, and then automate processes to alleviate a CPU or memory bottleneck. If you anticipate extremely erratic or bursting traffic into a virtual machine, you can automate Virtual Machine Scale Sets to create more virtual machines to handle the increased traffic. Conversely, you can reduce the number of virtual machines as the traffic decreases to minimize the cost of the overall environment for that application.

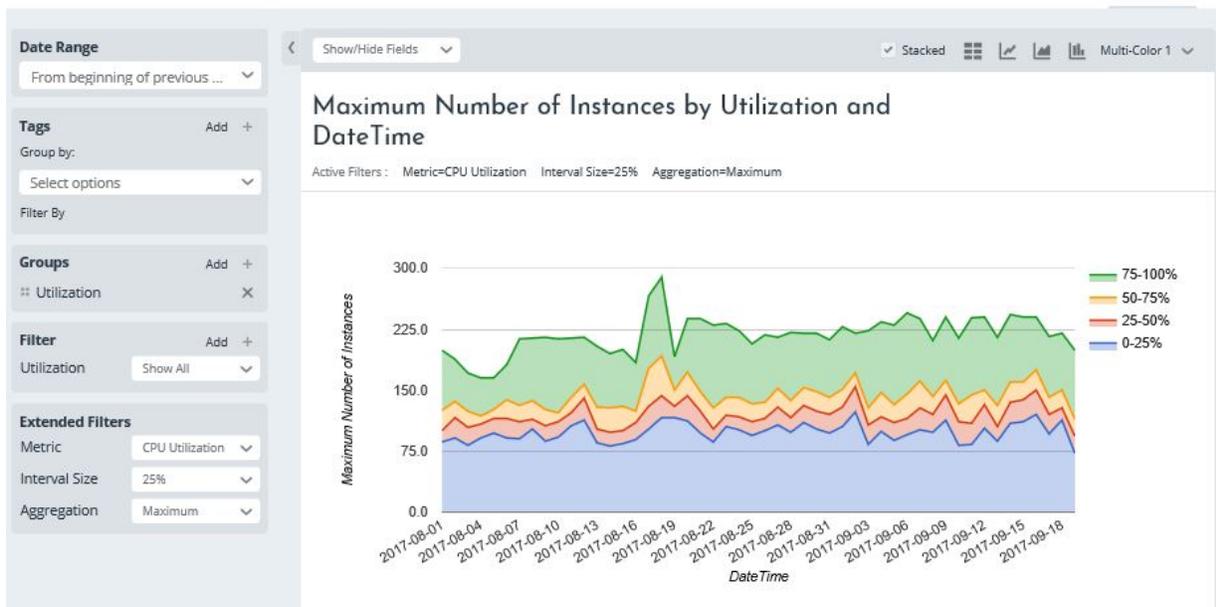
Azure Cost Management with Cloudyn: Cloudyn is a cloud service owned by Microsoft available free to Enterprise Agreement customers. It is tightly integrated with Azure operations and will appeal to both business managers and IT because it provides detailed visibility into the resource costs of running systems on Azure. Through its reporting interface, organizations can monitor costs split across websites, virtual machines, storage, applications, databases, and networks.

Cloudyn helps ensure migrated virtual machines continue to deliver targeted resource utilization and best cost by recommending changes. Track costs against budget using spending reports that help identify which virtual machine types are consuming budget and support decisions on how to modify the Azure environment to maximize ROI. Cloudyn benefits include:

- Visibility into resource costs
- Visibility into application and departmental costs
- Budgeting
- Cost optimization with right-sizing guidance

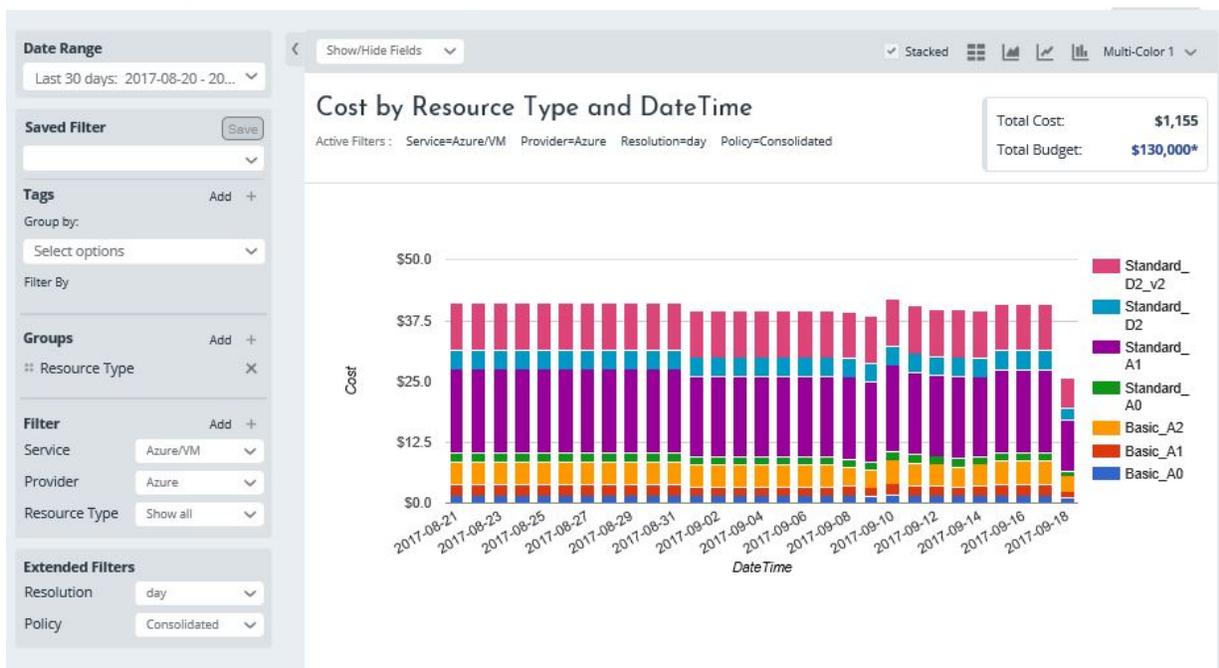
This Cloudyn VM Efficiency report shows actual usage of virtual machines over time in Azure.

VM Efficiency



A VM Daily Cost Tracking report shows spend on a daily basis across all virtual machine types and sizes.

VM Daily Cost Tracking



The Sizing Opportunities report includes projected cost savings, current instance type, and recommended instance type to simplify virtual-machine sizing decisions.

Sizing Opportunities ⓘ

Details	Potential Annual Savings	Instances to modify	Instance Type	Recommended Type	Scope
+	\$701	2	Standard_A1	Standard_A0	Instance Size Switch
+	\$675	1	Basic_A2	Basic_A1	Instance Size Switch
+	\$613	1	Standard_A1	Standard_A0	Instance Size Switch
+	\$350	1	Standard_A1	Standard_A0	Instance Size Switch
+	\$350	1	Standard_A1	Standard_A0	Instance Size Switch
+	\$350	1	Standard_A1	Standard_A0	Instance Size Switch
+	\$350	1	Standard_A1	Standard_A0	Instance Size Switch
+	\$193	1	Basic_A1	Basic_A0	Instance Size Switch
+	\$79	1	Basic_A1	Basic_A0	Instance Size Switch

Azure offers a number of integrated management and security services.

Azure Security Center (ASC): Use ASC to prevent, detect, and respond to threats with increased visibility and control over the security of your Azure resources. ASC provides a comprehensive view into an organization’s IT security posture with built-in search queries for issues requiring attention.

Azure Log Analytics: The Log Analytics service can automate operations while strengthening your security and compliance position, as well as protect your data and workloads with Backup and Site Recovery services. Log Analytics also integrates with your existing Microsoft System Center investments to provide a consolidated view of performance, event, and alert and configuration data. Use it to help manage and protect your entire IT infrastructure footprint, including on-premises datacenters. The service helps you collect, correlate, search, and act on log data. It offers real-time operational insight using an integrated search, custom dashboards, and Microsoft-developed solutions for data analytics in the Solution Gallery.

Azure Automation: Azure Automation helps you orchestrate and automate complex and repetitive operations. With the introduction of the hybrid runbook worker, Azure services extend these capabilities from the cloud to your on-premises datacenter. You can automate manual and repeated tasks using both runbooks developed directly in the PowerShell ISE or the graphical authoring interface. It also provides a way for you to automate the manual, long running, error-prone, and frequently repeated administrative tasks common to datacenter or cloud

environments. You can implement administrative processes as runbooks that can perform multiple tasks with no human intervention. When it makes sense, you can schedule runbooks to automate tasks at recurring intervals.

Azure Backup and Disaster Recovery: Backup and Disaster Recovery, powered by Azure Site Recovery and Azure Backup, help you protect and extend your datacenter to more easily implement backup and disaster recovery strategies. The replication capabilities of Azure Site Recovery help protect critical applications and migrate applications to Azure. Azure Backup is a scalable solution that protects your application data and retains it for years without any capital investment and with minimal operating costs.

Summary

As organizations move on-premises virtual machines to Azure, a best practice is to move workloads through three stages: discover, migrate, and optimize. Microsoft and its partners offer tools to help increase the efficiency and reduce the complexity of those stages.

For the discovery stage, several partners provide options to using Azure Migrate. These alternatives include the Cloudamize and Movere solutions referenced in the appendices of this guide. Like Azure Migrate, the partner solutions also discover virtual machines and workloads in your environment and recommend virtual machine instances in Azure to inform decisions about reducing size and cost.

For the migration stage, organizations can use Azure Site Recovery, as well as Microsoft Data Migration Assistant and Azure Database Migration Services, to simplify and automate the migration of on-premises virtual machines and databases to Azure. These services minimize disruption to business operations.

To optimize the Azure virtual machine environment after migration, you can use Azure management and security services to refine virtual machine efficiencies using operational data analytics and improved governance. Azure Automation also helps keep your environment secure and backed up and can even provide site recovery in case of an outage.

These products and features are all designed to help ease the overall migration process to Azure of a wide and growing range of applications and data, so organizations can more quickly and easily benefit from Microsoft cloud computing.

Appendix 1: Discovery stage with partner Cloudamize

There are multiple ways you can discover and assess your environment for migration. This appendix covers the discovery and assessment process with Microsoft partner Cloudamize.

Cloudamize, a cloud computing analytics platform, analyzes data and recommends options to speed up and simplify your environment for migration to the cloud. The actual assessment takes several hours, with the entire process lasting no more than a few weeks depending on the size and complexity of the computing environment.

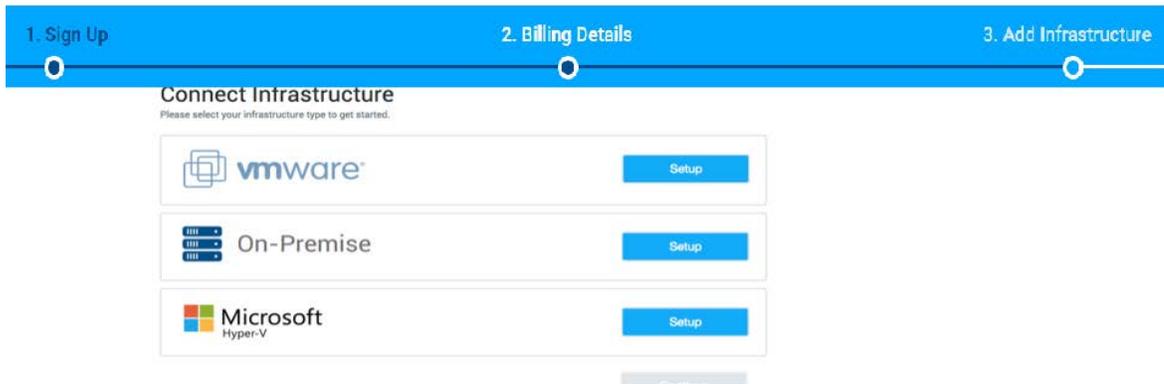
Cloudamize findings also can help you determine which virtual machines to migrate to Azure. For example, a virtual machine with a CPU bottleneck, high memory utilization, or constrained storage might be a candidate for migration. Azure enables you to rapidly configure more of what you need without buying and configuring additional hardware.

Get started by preparing for the Cloudamize assessment. Create a Cloudamize account, and install the vCenter Proxy and virtual machine agents as outlined in these steps. Later, you will run the assessment and Cloudamize will analyze the data and provide an interactive dashboard and customized, downloadable reports outlining virtual machine instance sizes, costs, and storage alternatives.

Create a Cloudamize account

1. To create your Cloudamize account, you will need an Access Code or a credit card to purchase a plan. Navigate to the Pre-Cloud application and click Register.
2. Create a Cloudamize login, provide the requested information and an Access Code, if you have one, accept the Terms of Service, and then click Sign Up.
3. If you did not enter an Access Code, select a plan to purchase and your billing information.

4. Choose the system in your infrastructure and click Setup. In this example, we've selected VMware.



Configure your VMware vCenter environment

Next, configure VMware vCenter and install the virtual machine agents to work with Cloudamize. Follow these steps to ensure the vCenter environment is communicating with the Cloudamize SaaS application to perform the discovery and assessment.

Note: The vCenter agent/proxy reports on hardware statistics. If you want information, including dependencies, about applications running on each virtual machine, install Cloudamize agents on each virtual machine in the vCenter environment.

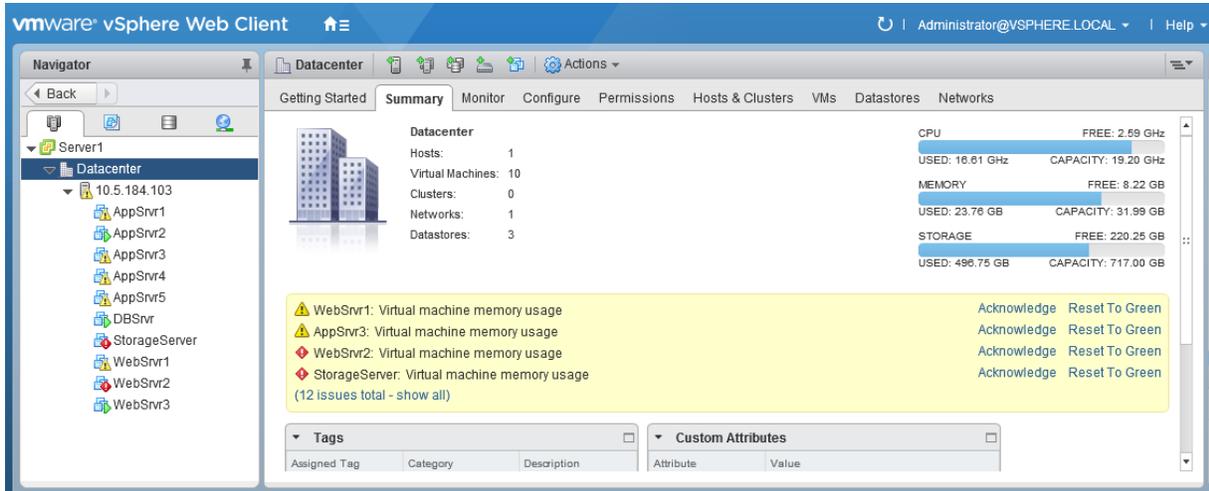
These are the major steps for setting up the vCenter environment:

1. Create read-only credentials on the vCenter host server and within vCenter to allow access to vCenter, and then configure the Cloudamize SaaS solution with the vCenter IP address and login credentials to collect system level data on any virtual machines running on the vCenter.
2. Open TCP port 443 outbound to the Cloudamize vCenter data Collector at IP address 184.73.183.154.

Note: The Cloudamize Proxy also allows for using Port 80 to send data to their SaaS solution.

3. Install Cloudamize proxy either on vCenter or on any other internet-facing virtual machine. Because the Cloudamize proxy is unique for each vCenter, if you have multiple vCenters you will need to install multiple proxies on unique machines using the [Cloudamize Proxy Setup Instructions](#).
4. Cloudamize can also collect application inter-connectivity data from the virtual machines by installing the Cloudamize Windows/Linux agent on the virtual machines you want to monitor. Review the [Cloudamize instructions to install Cloudamize agents](#).

This example shows the 10 virtual machines running on VMware ESXi and managed by vCenter Server. Cloudamize will run an assessment to discover these virtual machines.



Note: Numerous errors display in the example environment because the system is running out of compute and memory resources, which makes it an excellent candidate to move to Azure.

Perform discovery and run an assessment

After installing the vCenter proxy and the virtual machine agents, they begin sending data to the Cloudamize SaaS solution. You can view initial findings in the Cloudamize portal, including the virtual machine names and whether the agent is installed, the operating system type, and the node name. The following image shows how Cloudamize represents the VMware environment.

Total Nodes Monitored: 10 Total Agents Installed: 10 Purchased Nodes: 10

Instance Settings Asset Settings Stop All Agents

Nodes Monitored: 10 Agents Installed: 10

View Infrastructure: Server1 All

Move Selected Nodes to: Default Submit Download Excel

#	Node Name	Node ID	Data Center	Resource Pool	Asset	Assessment Scope	Reason	Agent Status
<input type="checkbox"/>	AppSrv1	VaQdHCK0_64505-vm-87.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	AppSrv2	VaQdHCK0_64505-vm-90.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	AppSrv3	VaQdHCK0_64505-vm-88.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	AppSrv4	VaQdHCK0_64505-vm-57.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	AppSrv5	VaQdHCK0_64505-vm-53.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	DBSrvr	VaQdHCK0_64505-vm-84.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	StorageServer	VaQdHCK0_64505-vm-86.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	WebSrv1	VaQdHCK0_64505-vm-48.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	WebSrv2	VaQdHCK0_64505-vm-49.64505	Datacenter	Resources	Default	Included	N/A	Started
<input type="checkbox"/>	WebSrv3	VaQdHCK0_64505-vm-89.64505	Datacenter	Resources	Default	Included	N/A	Started

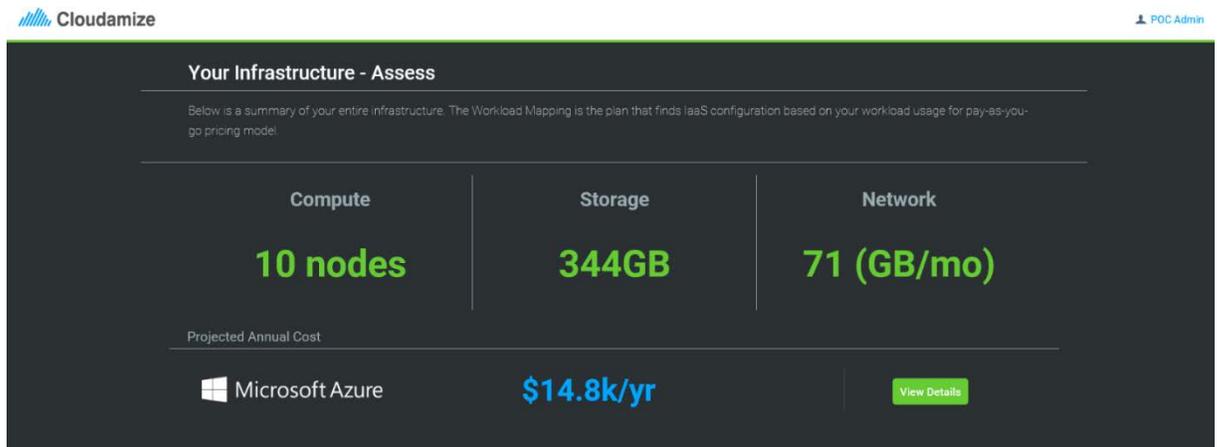
After you verify that all virtual machines in your environment are displayed, you are ready to run an assessment.

1. In the portal under **Inventory Settings**, click each node you want to include in the assessment and click **Start Assessment** in the upper right-hand corner of the portal.

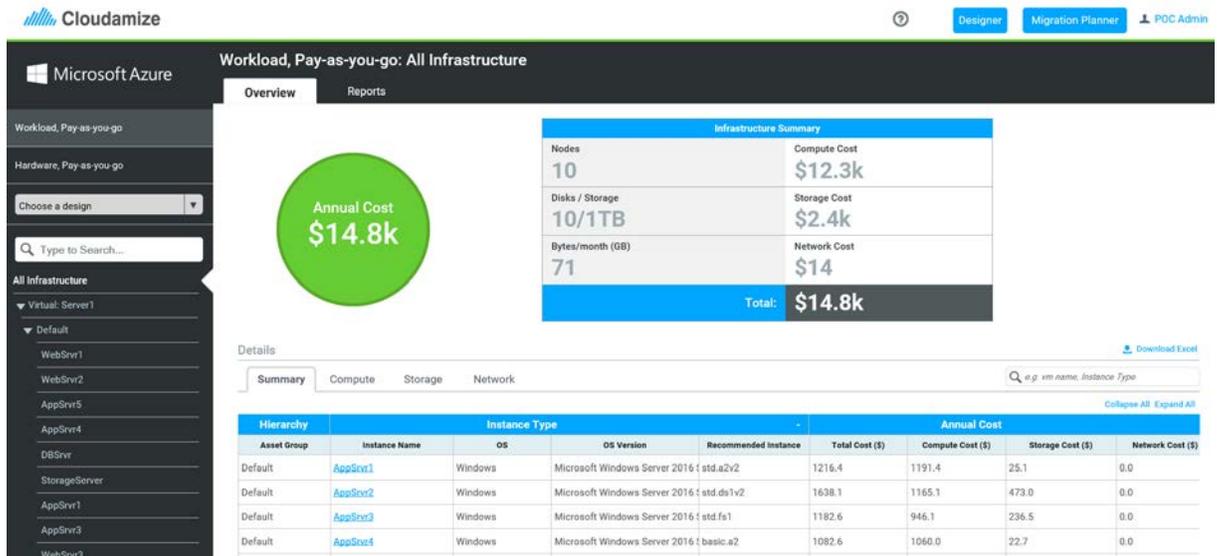
- Follow the prompts to set the duration of the assessment. The system will provide a completion date for the assessment.

Note The assessment does not display in real time. Check with Clouddamize to better understand the nuances of running an assessment in relation to the amount of time it takes.

- After the assessment is complete, you can find the results on the main dashboard. Review the Compute, Storage, and Network areas to identify a Projected Annual Cost. This image illustrates the assessment results for the 10-node environment in the example.

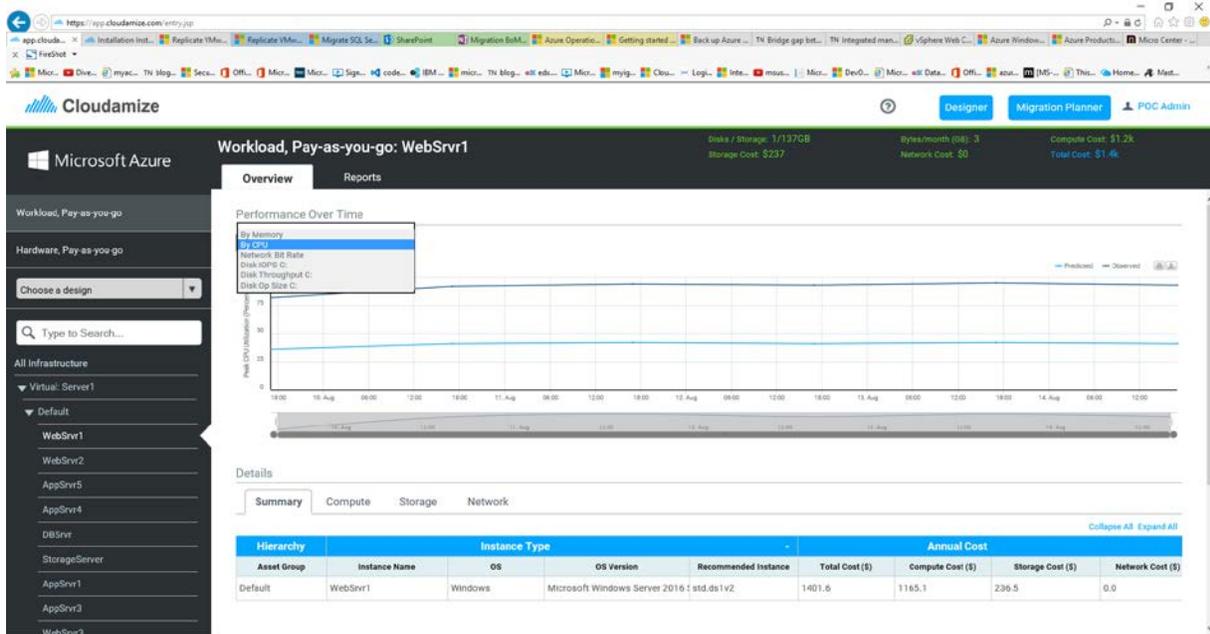


To find out more, click **View Details**. The following image shows the details of the assessment for the example.



The assessment includes listings of recommended instance sizes in Azure. You can find more data by viewing the Compute, Storage, and Network tabs. You can also drill down into the usage data in each server by clicking the instance name in the grid or selecting the server in the left

Navigation blade. The following image shows more details for a single server, including CPU usage over time, and Memory, Network, and Disk usage statistics.



In addition to interactive summaries and individual server details, Cloudamize prepares reports on various aspects of its assessment findings, including an Infrastructure Assessment Summary that is described in the next section.

Review Infrastructure Assessment Summary from Cloudamize

Cloudamize evaluates your current infrastructure based on data your systems have generated during the assessment period, and estimates of your costs and potential savings from moving to Azure.

Example workload result. This is the Cloudamize assessment of example environment for 10 virtual machines.

Total Nodes	10
Total Disk	10
Total Bytes/month (GB)	71
Hardware, Pay-as-you-go	\$5.6k
Workload, Pay-as-you-go	\$14.8k

Cloudamize analyzes the workload and projects performance for an Azure environment. The Cloudamize platform maps workloads to Azure based on these major factors:

- Hardware mapping
- Workload mapping
- Azure pricing plans

Hardware mapping: Cloudamize creates a like-to-like mapping of the system configurations to an equivalent Azure instance and storage size and estimates Total Cost of Ownership (TCO) based on this configuration. This mapping is based on system hardware specifications (For example, number of CPUs, CPU speed, and assigned memory, disk size, and so on) and does not take actual workload or usage into account.

Workload mapping: Cloudamize maps system configurations and actual workload and usage characteristics to an Azure environment. The system maps instance sizes, storage, and network demand and estimates TCO based on the suggested configuration.

Cloudamize uses these parameters when constructing an optimal plan: peak CPU usage, disk occupancy, peak disk usage, peak network usage, unused compute or storage resources, and disk IOPS and usage patterns.

Pricing plans: Cloudamize maps usage to Azure Pay-As-You-Go pricing plans, which are hourly rates that require no up-front spending, and then recommends pricing plans to maximize savings based on usage patterns of each virtual machine.

Total Cost of Ownership overview

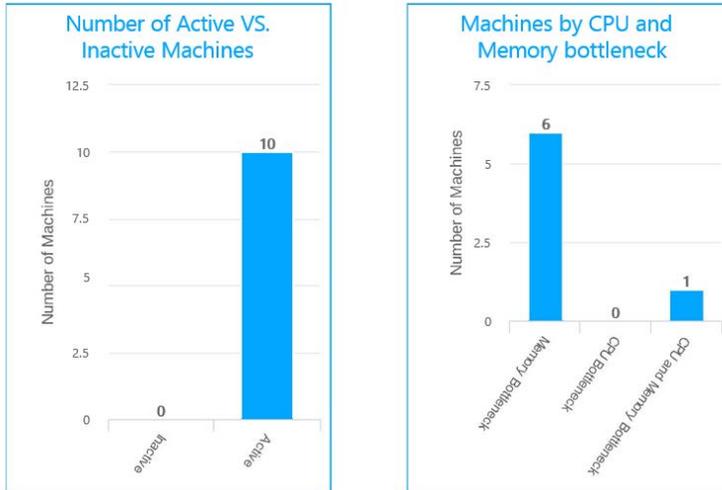
The Cloudamize assessment determines optimal mapping to Azure Pay-As-You-Go pricing plans using three categories of workload optimization: Compute, Storage, and Network.

Example workload result. The pricing results for the compute, storage, and network categories can help determine which virtual machines to migrate to Azure.

	Compute	Storage	Network	Total
Hardware, Pay-as-you-go	\$5.4k	\$92	\$14	\$5.6k
Workload, Pay-as-you-go	\$12.3k	\$2.4k	\$14	\$14.8k

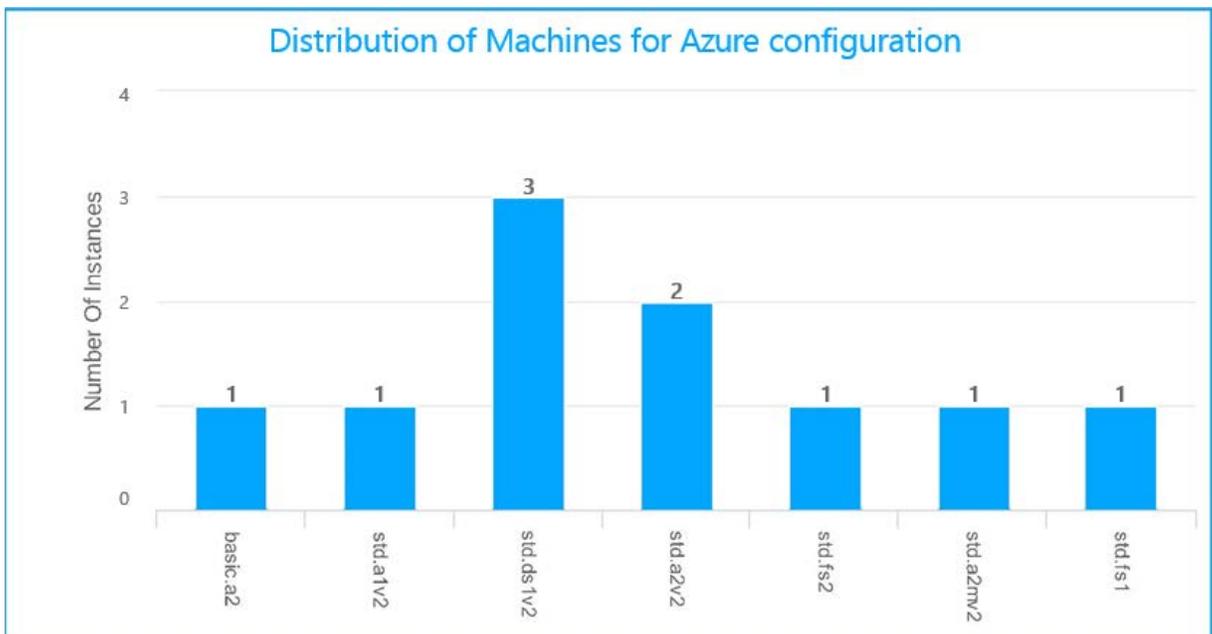
WORKLOAD OPTIMIZATION: COMPUTE Cloudamize provides charts to identify usage and performance bottlenecks.

Example workload result. Cloudamize evaluated workload on the virtual machines and found that all 10 were active, with no virtual machines turned off for the duration of the analysis. The following charts identified no virtual machines with CPU bottlenecks, six with memory bottlenecks, and one with both CPU and memory bottlenecks.



PROJECTED INSTANCE SIZES Cloudamize can also recommend Azure instance sizes that correspond to your on-premises usage. If a virtual machine is constrained in some way, one option is to review the projected instances and increase size for CPU, memory, or storage to facilitate anticipated growth or increase performance of the application.

Example workload result. Cloudamize has recommended instance sizes for the post-migration Azure environment in the following image.



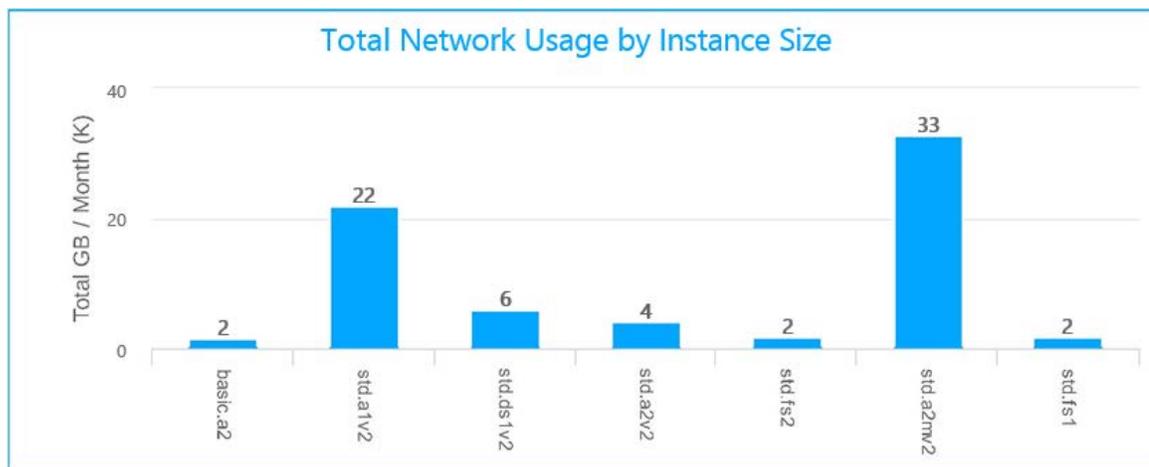
WORKLOAD OPTIMIZATION: STORAGE Cloudamize also estimates the amount of storage that would be required for the workloads.

Example workload result. Cloudamize has estimated that Azure storage costs will be \$2,423 and confirmed 10 of the 10 example disks were in use with no unused storage.

Metric	Value	Cost
Observed Disk Capacity (GB)	288	
Observed Disk Occupancy (GB)	177	
Observed IOPS/Sec	639	
Predicted Cloud Capacity (GB)	1474	\$2358
Total IOPS Cost	639	\$65
Total Cost		\$2423

WORKLOAD OPTIMIZATION: NETWORK Cloudamize measures network usage and calculates network usage costs based on the activity during the assessment and applies the network usage to each instance size to assist with decision-making.

Example workload result. Based on current network usage, Cloudamize estimated network usage at 71 GB/month and projects Azure costs of \$14 per year. This chart shows projected total network usage by instance type.



After you discuss the Cloudamize assessment results with your team, you can determine the most likely virtual machines to migrate to Azure. In [Stage 2](#) in this guide, we provide steps to

migrate virtual machines in your environment using Azure Site Recovery. Azure Site Recovery automates the replication of virtual machines based on policies that you set and control.

Appendix 2: Discovery stage with partner Movere

There are multiple ways you can discover and assess your environment for migration. This appendix describes the discovery and assessment process with Microsoft partner Movere.

Movere is a SaaS solution, residing in Azure, that uses the latest technology and security standards. Movere is designed as a research platform for users to find exactly what they are looking for without having to continually export, integrate, and analyze data outside of the system that gathered it. Once set up, Movere automatically collects and integrates data from multiple disparate sources, so organizations can focus on results rather than on preparing data for analysis.

Movere has three key components.

1. Movere Console, which is the data collection engine.
2. Movere Website, a presentation layer including tabular data and visualizations.
3. Multi User Interface for user administration, including role setting and permissions.

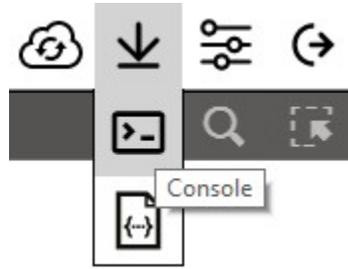
Deploy Movere

You can begin to use Movere to deploy, configure, and collect data within 15 minutes. Many customers use the approach that follows to see how much of their environment can be inventoried with no preparation. Other customers adopt a step-by-step approach that might include capturing Active Directory data, capturing hypervisor data, moving on to IT asset management data, and then scanning individual devices. Here are the basic steps if you want to run a quick discovery and assessment:

1. Register on the Movere website at <https://www.movere.io/> and then log in to the Movere website, and download a copy of the Movere Console.

Note: Never share your copy of Movere with anybody outside of your organization. The file you receive contains confidential information, including a customer ID and other configuration details unique to your organization that Movere uses to identify the data you upload to the cloud.

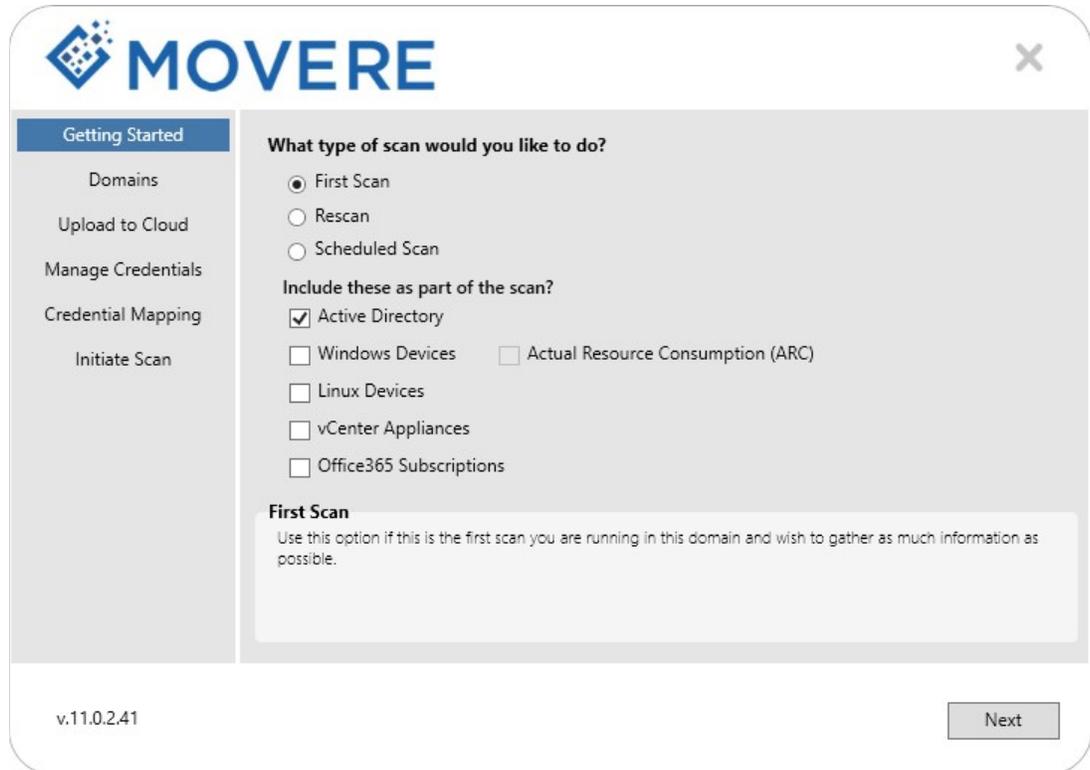
2. Click Console button to download the Movere Console Movere.zip from the Movere website.



3. Copy the zip file you download to a Windows device that meets the minimum system requirements.
4. Extract the zip file into a folder on a local drive, creating a path such as C:\Movere; do not use a UNC path.
5. Double-click Movere.Console.WPF.exe file.
6. After you read and agree to the Privacy and Subscription agreements, check the **Windows Devices** check box on the **Getting Started** tab.
7. On the **Upload to Cloud** tab, enter the same username and password used to access the Movere website.

Note: This will place a security token file called token.txt valid for 90 days on the device where you are running the Movere Console.

8. On the **Manage Credentials** tab, enter at least one set of credentials with local administrative rights to the Windows devices you are attempting to scan. From the **Credential Mapping** tab, assign the credentials to be used for the domain you are targeting.
9. From the **Getting Started** tab, in the section called **What type of scan would you like to do?** check the type of scan you want.
 - a. Select **First Scan** if this is the first scan you are running in the chosen domain.
 - b. Select **Rescan** under one of these scenarios:
 - i. Your initial scan is limited to an Active Directory extraction only,
 - ii. You are targeting devices not captured during a previous scan; or
 - iii. You are targeting devices previously inventoried to update your inventory data or to reflect changes made to your environment.
 - c. Select **Scheduled Scan** if you want Movere to perform scans on a regular basis without user intervention. You can schedule scans by day, time and interval, such as daily, weekly, or monthly.

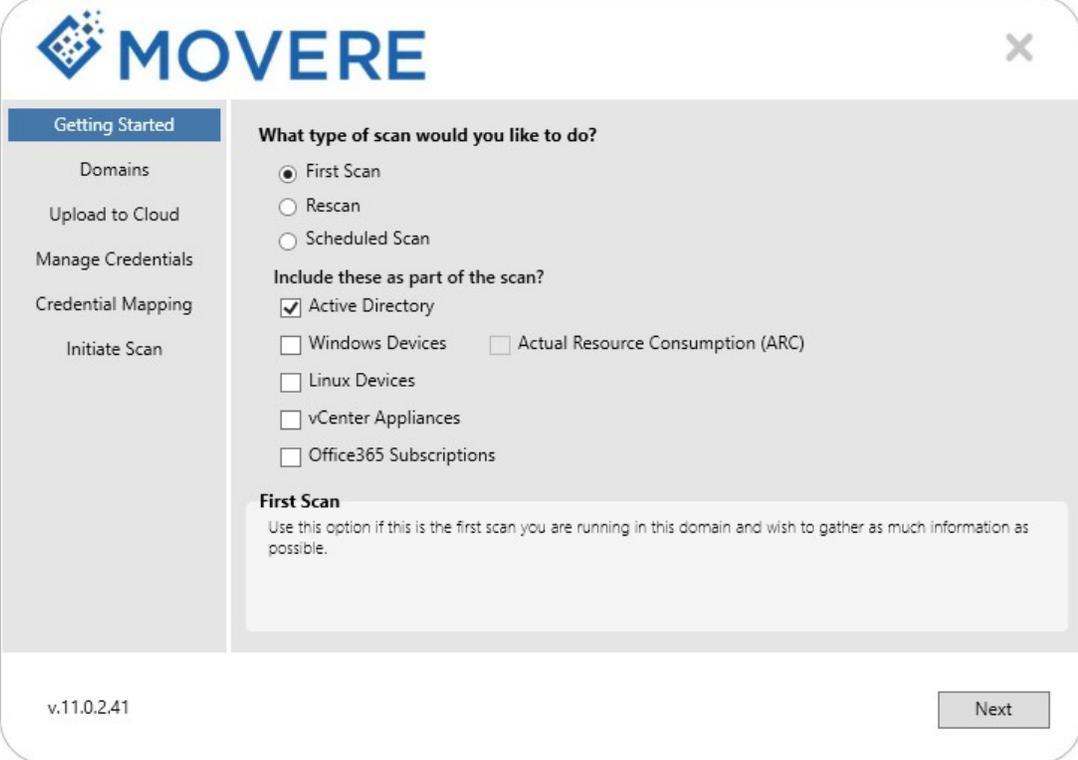


10. From the **Getting Started** tab, under **Include these as part of scan**, choose options based on your needs.
 - a. Select Active Directory to gather objects from the Active Directory domain(s) selected on the **Domains** tab, including computers, users and trusts. This data forms the foundation of the inventory process.
 - b. Select **Windows devices** if you want Movere to scan each Windows device based upon the selected device criteria (servers and/or workstations), within each domain.

IMPORTANT: If the targeted domain(s) contain Windows device objects no longer in use, Movere recommends not checking this option and using the first scan to extract Active Directory data only. Movere will process the Active Directory data it collects to identify the active Windows devices within each domain. Using the Rescan option, Movere will target only the Windows devices identified as active, i.e. not disabled, not a cluster account, having a last login timestamp and/or password reset within the past 31 days. This approach will reduce the overall scanning time by minimizing the number of attempts made to connect to devices that no longer exist.

- c. Select VMware vCenter Server Appliance if you want to scan your vCenter environment. Because the VMware vCenter Server Appliance (VCSA) is a SUSE Linux Enterprise based appliance is not built on Windows, it will not be

inventoried during the Windows scanning process and you will need to be request a scan separately. To initiate a VCSA scan from the 'Getting Started' menu by selecting 'First Scan' then checking the 'vCenter Appliances' option. Once you have selected this option, click **Next**.



MOVERE

Getting Started

- Domains
- Upload to Cloud
- Manage Credentials
- Credential Mapping
- Initiate Scan

What type of scan would you like to do?

First Scan
 Rescan
 Scheduled Scan

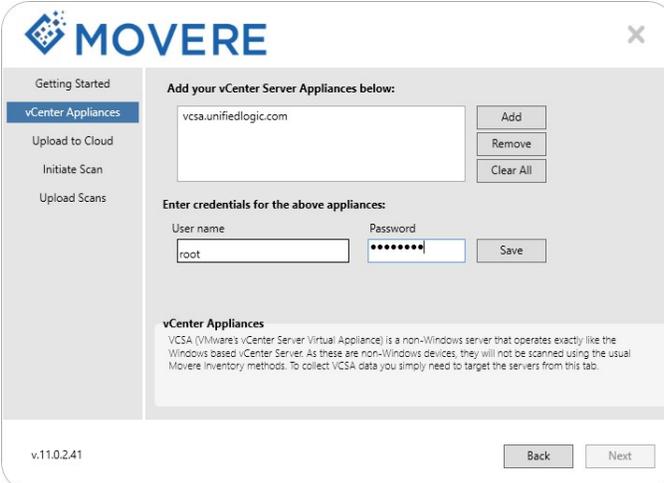
Include these as part of the scan?

Active Directory
 Windows Devices Actual Resource Consumption (ARC)
 Linux Devices
 vCenter Appliances
 Office365 Subscriptions

First Scan
Use this option if this is the first scan you are running in this domain and wish to gather as much information as possible.

v.11.0.2.41 Next

- i. On the **vCenter Appliances** tab, click **Add** and enter the appliance NetBIOS, Fully Qualified Name, or IP address. You will then need to enter the username and password that has access to the appliance. When you enter credentials specific to VCSA and select **Save**, you will see **vCenter credentials added** at the bottom of the **vCenter Appliances** tab. Repeat this step for each VCSA in your environment.



MOVERE

Getting Started

- vCenter Appliances**
- Upload to Cloud
- Initiate Scan
- Upload Scans

Add your vCenter Server Appliances below:

vcsa.unifiedlogic.com Add
Remove
Clear All

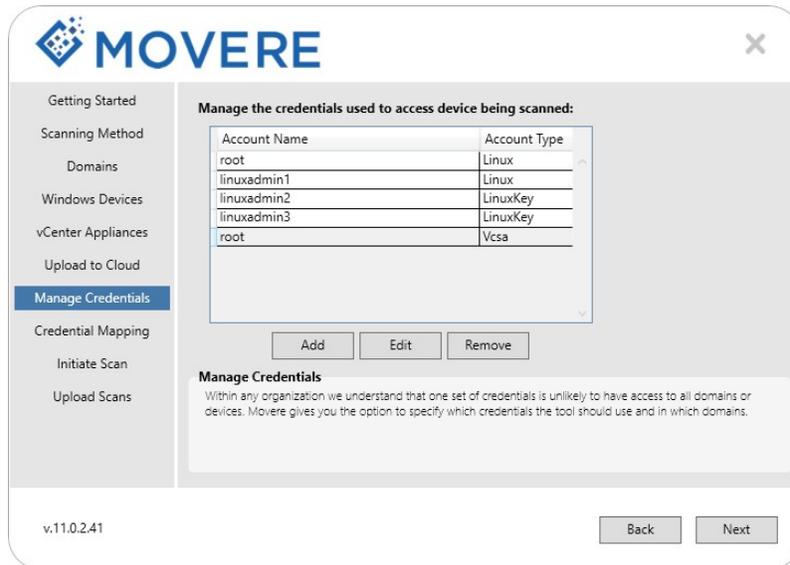
Enter credentials for the above appliances:

User name: root Password: •••••••• Save

vCenter Appliances
VCSA (VMware's vCenter Server Virtual Appliance) is a non-Windows server that operates exactly like the Windows based vCenter Server. As these are non-Windows devices, they will not be scanned using the usual Movere inventory methods. To collect VCSA data you simply need to target the servers from this tab.

v.11.0.2.41 Back Next

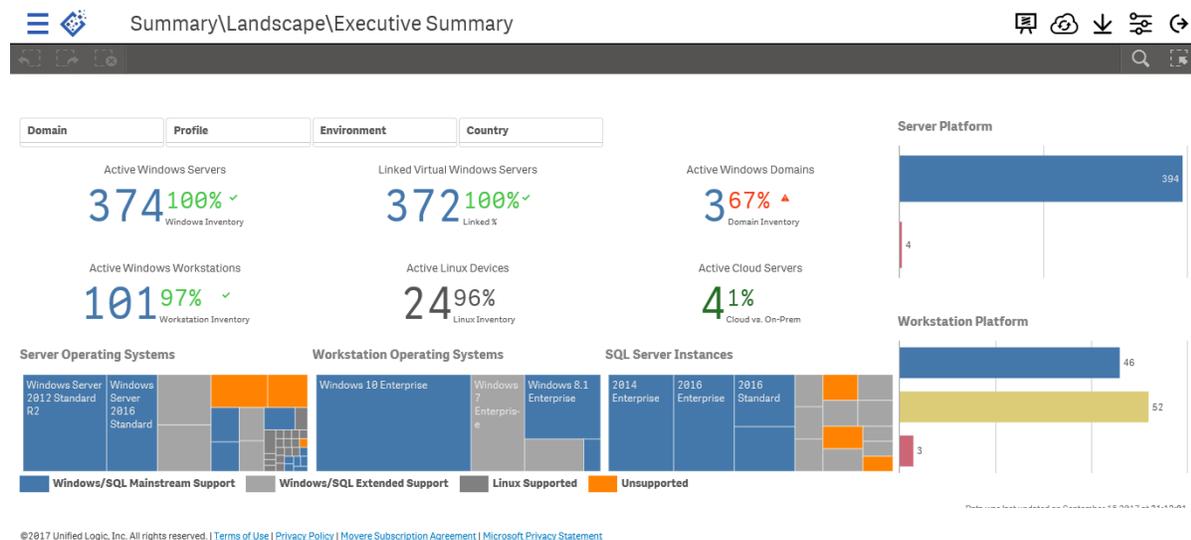
Note: You can update or delete credentials, including for your vCenter appliance, in the Manage Credentials tab.



- ii. After you have identified your vCenter Appliance(s) and provided the appropriate credentials to access them, you are ready to scan your VCSA infrastructure. To initiate a scan, click the **Initiate Scan** tab and select **Scan**.

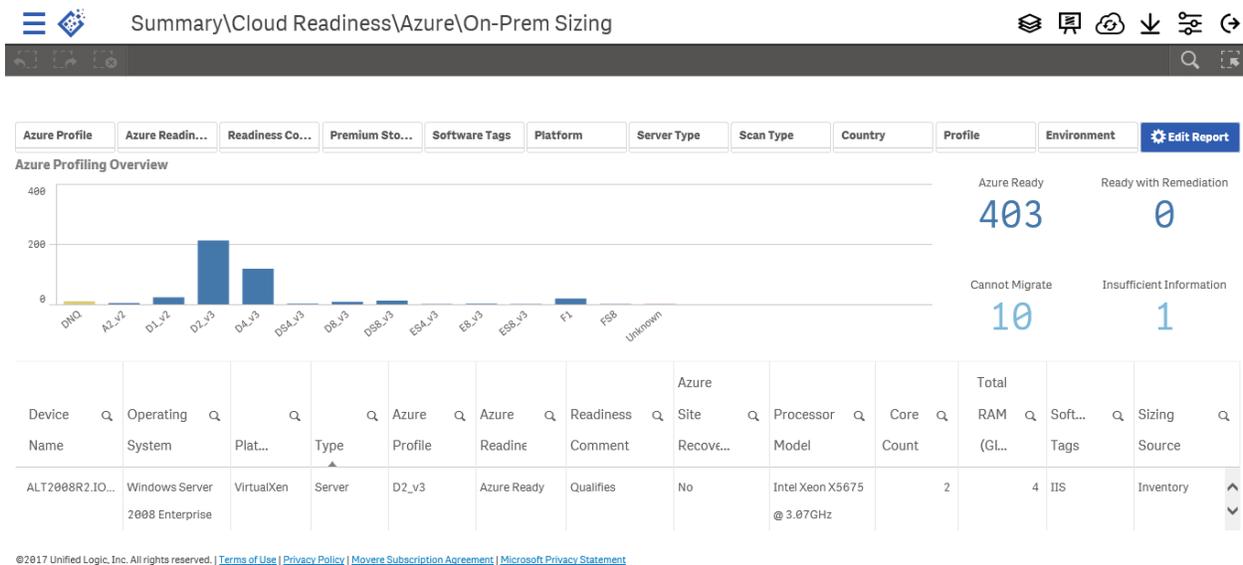
Assess results

After your scan data is uploaded to the Movere cloud service, typically within minutes, you can use the dashboard to analyze the results in premade or custom. This image illustrates scan findings as displayed in the [Summary](#).



Workload sizing

To view the number and types of servers physically ready to run on Azure, you can find that report from the main dashboard in **Summary\CloudReadiness\Azure\On-Prem Sizing** as shown in this image. Movere offers a significant array of detail and multiple drill-down sections including mapping to Azure instance sizes, processor models and core count, RAM amounts, and geographic details.



Azure cost estimates

Movere provides estimated costs for running the on-premises virtual machines in Azure in **Summary\Cloud Readiness\Azure\On-Prem VM Pricing** as in this image. Organizations can also estimate costs by Azure region.

Summary\Cloud Readiness\Azure\On-Prem VM Pricing

Azure Region Selector	Azure Estimated Price Per Profile (Compute)									
	OS Type	Environment	Profile	Azure Profile	Device Count	Hours	*Azure Rate Per Hour	*Cost Per Month		
Australia East	SLES	Test	DD	D1_v2	3	177.14	\$0.170	\$99.143		
Australia Southeast	Linux	Test	DD	F1	1	177.14	\$0.002	\$10.963		
Brazil South	Windows	Test	DD	D2_v3	56	177.14	-	-		
Canada Central	Linux	Test	DD	D2_v3	2	177.14	-	-		
Canada East	Windows	-	Movere - Demo - Servers - Virtual	F88	1	744.00	\$0.056	\$644.384		
Central India	Windows	-	-	A2_v2	2	744.00	\$0.136	\$202.368		
Central US	Windows	-	Movere - Demo - Servers - Virtual	A2_v2	1	744.00	\$0.136	\$101.184		
East Asia	Windows	-	Movere - Demo - Servers - Virtual	D1_v2	20	744.00	\$0.133	\$1,079.040		
East US	Windows	-	Movere - Demo - Servers - Virtual	F1	18	744.00	\$0.108	\$1,446.336		
East US 2	Linux	-	Service	A2_v2	1	744.00	\$0.091	\$67.784		
Germany Central	Windows	-	Movere - Demo - Servers - Virtual	D2_v3	139	744.00	-	-		
Germany Northeast	Windows	-	Movere - Demo - Servers - Virtual	D4_v3	95	744.00	-	-		
Japan East	Windows	-	Movere - Demo - Servers - Virtual	D58_v3	17	744.00	-	-		
Japan West	Windows	-	Movere - Demo - Servers - Virtual	-	-	-	-	-		
Korea Central	Windows	-	Movere - Demo - Servers - Virtual	-	-	-	-	-		
Korea South	Windows	-	Movere - Demo - Servers - Virtual	-	-	-	-	-		
North Central US	Windows	-	Movere - Demo - Servers - Virtual	-	-	-	-	-		
North Europe	Linux	-	Service	A2_v2	1	744.00	\$0.091	\$67.784		
South Central US	Windows	-	Movere - Demo - Servers - Virtual	D2_v3	139	744.00	-	-		
South India	Windows	-	Movere - Demo - Servers - Virtual	D4_v3	95	744.00	-	-		
Southeast Asia	Windows	-	Movere - Demo - Servers - Virtual	D4_v3	95	744.00	-	-		
UK South	Windows	-	Movere - Demo - Servers - Virtual	D58_v3	17	744.00	-	-		
UK West	Windows	-	Movere - Demo - Servers - Virtual	D58_v3	17	744.00	-	-		
West Central US	Windows	-	Movere - Demo - Servers - Virtual	D58_v3	17	744.00	-	-		
West Europe	Windows	-	Movere - Demo - Servers - Virtual	D58_v3	17	744.00	-	-		
Totals					403			\$4,942.262		

*Note: Default Azure Region is West US

Movere also provides storage cost estimates based on the data scans in **Summary\Cloud Readiness\Azure\On-Prem Storage Pricing** as shown in this image.

Summary\Cloud Readiness\Azure\On-Prem Storage Pricing

Azure Region Selector	Azure Estimated Price Per Profile (Storage)									
	Environment	Profile	Azure Profile	Unit Count	Metric	*Rate	*Cost Per Month			
Australia East	Test	DD	S4	11	Disk	\$0.770	\$8.470			
Australia Southeast	Test	DD	S6	52	Disk	\$1.510	\$78.520			
Brazil South	-	JUMP	S4	1	Disk	\$0.770	\$0.770			
Canada Central	-	JUMP	S6	11	Disk	\$1.510	\$16.610			
Canada East	-	JUMP	S10	1	Disk	\$2.950	\$2.950			
Central India	-	JUMP	S15	8	Disk	\$5.670	\$45.360			
Central US	-	JUMP	S70	1	Disk	\$10.800	\$10.800			
East Asia	-	JUMP	P20	1	Disk	\$73.220	\$73.220			
East US	-	JUMP	S4	27	Disk	\$0.770	\$20.790			
East US 2	-	JUMP	P10	1	Disk	\$73.220	\$73.220			
Germany Central	-	JUMP	S4	187	Disk	\$0.770	\$143.990			
Germany Northeast	-	JUMP	S6	164	Disk	\$1.510	\$247.640			
Japan East	-	JUMP	S10	8	Disk	\$2.950	\$23.600			
Japan West	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
Korea Central	-	JUMP	S4	27	Disk	\$0.770	\$20.790			
Korea South	-	JUMP	P10	1	Disk	\$73.220	\$73.220			
North Central US	-	JUMP	S4	187	Disk	\$0.770	\$143.990			
North Europe	-	JUMP	S6	164	Disk	\$1.510	\$247.640			
South Central US	-	JUMP	S10	8	Disk	\$2.950	\$23.600			
South India	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
Southeast Asia	-	JUMP	S10	8	Disk	\$2.950	\$23.600			
UK South	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
UK West	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
West Central US	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
West Europe	-	JUMP	P4	1	Disk	\$5.200	\$5.200			
Totals				417			\$992.100			

*Note: Default Azure Region is West US and Prices reflect Managed Disks

Movere is one option you can use to discover and assess your environment. Built-in reports and analytics can help organizations determine which virtual machines are best suited to move to Azure and provide estimates of the associated operating costs in Azure. After you discuss the

assessment results with your team, you can determine the best virtual machines to migrate to Azure.

In [Stage 2](#) in this guide, we provide steps to migrate virtual machines in your environment using Azure Site Recovery. Azure Site Recovery automates the replication of virtual machines based on policies that you set and control.