

Contents

Azure Migrate Documentation

Overview

[About Azure Migrate](#)

[What's new](#)

[Common questions](#)

[General](#)

[Azure Migrate appliance](#)

[Server Assessment tool/dependency analysis](#)

[Server Migration tool](#)

Tutorials

[Assess and migrate VMware VMs](#)

[Prepare VMware for assessment and migration](#)

[Assess VMware VMs for migration](#)

[Migrate VMware VMs](#)

[About migration options for VMware VMs](#)

[Migrate VMware VMs with agentless migration](#)

[Migrate VMware VMs with agent-based migration](#)

[Assess and migrate Hyper-V VMs](#)

[Prepare Hyper-V for assessment and migration](#)

[Assess Hyper-V VMs for migration](#)

[Migrate Hyper-V VMs](#)

[Assess and migrate physical servers](#)

[Prepare physical servers for assessment and migration](#)

[Assess physical servers](#)

[Migrate physical servers](#)

[Assess imported servers for migration](#)

[Assess imported servers for migration](#)

Concepts

[Support matrices](#)

General support
VMware assessment support
VMware migration support
Hyper-V assessment support
Hyper-V migration support
Physical server assessment support
Physical server migration support
Azure Migrate appliance requirements
Replication appliance requirements
Azure Migrate appliance architecture
Hyper-V migration architecture
VMware agent-based migration architecture
Assessments overview
Best practices for assessments
Dependency analysis overview

How-to guides

Create and manage Azure Migrate projects
Add a tool for the first time
Add assessment tools
Deploy Azure Migrate appliance
 Deploy appliance for VMware (OVA)
 Deploy appliance for Hyper-V (VHD)
 Deploy appliance for VMware/Hyper-V (script)
 Deploy appliance for physical servers
Limit discovery scope for VMware VMs
Discover applications/roles/features
Group machines for assessment
Analyze machine dependencies (agent-based)
Analyze machine dependencies (agentless)
Create an assessment
Assess a SQL Server database
Customize an assessment

[Add migration tools](#)

[Migrate VMware VMs to Azure VMs encrypted with SSE and CMK](#)

[Prepare machines for migration](#)

[Delete an Azure Migrate project](#)

[Work with previous version](#)

[Scale assessment and migration](#)

[Assess large numbers of VMware VMs](#)

[Assess large numbers of Hyper-V VMs](#)

[Assess large numbers of physical servers](#)

[Automate migration of large number of VMs](#)

[Migration examples \(Contoso series\)](#)

Troubleshoot

[Troubleshoot Azure Migrate](#)

[Troubleshoot Azure Migrate projects](#)

[Troubleshoot Azure Migrate appliance/discovery](#)

[Troubleshoot assessment/dependency visualization](#)

Resources

[Migration in the Cloud Adoption Framework](#)

[REST API](#)

[Resource Manager template](#)

[Pricing](#)

[UserVoice](#)

[Forum](#)

[Blog](#)

[Azure Migrate](#)

[Azure Roadmap](#)

About Azure Migrate

3/23/2020 • 5 minutes to read • [Edit Online](#)

This article provides a quick overview of the Azure Migrate service.

Azure Migrate provides a centralized hub to assess and migrate on-premises servers, infrastructure, applications, and data to Azure. Azure Migrate provides the following features:

- **Unified migration platform:** A single portal to start, run, and track your migration journey to Azure.
- **Range of tools:** A range of tools for assessment and migration. Tools include Azure Migrate: Server Assessment, and Azure Migrate: Server Migration. Azure Migrate integrates with other Azure services, and with other tools and independent software vendor (ISV) offerings.
- **Assessment and migration:** In the Azure Migrate hub you can assess and migrate:
 - **Servers:** Assess and migrate on-premises servers to Azure VMs.
 - **Databases:** Assess and migrate on-premises databases to Azure SQL DB, or to Azure SQL Managed Instance.
 - **Web applications:** Assess and migrate on-premises web applications to Azure App Service, using the Azure App Service Assistant.
 - **Virtual desktops:** Assess and migrate your on-premises virtual desktop infrastructure (VDI), to Windows Virtual Desktop in Azure.
 - **Data:** Migrate large amounts of data to Azure quickly and cost-effectively, using Azure Data Box products.

Integrated tools

The Azure Migrate hub includes these tools.

TOOL	ASSESS/MIGRATE	DETAILS
Azure Migrate:Server Assessment	Assess servers.	Discover and assess on-premises VMware VMs, Hyper-V VMs, and physical servers, in preparation for migration to Azure.
Azure Migrate:Server Migration	Migrate servers.	Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized machines, and public cloud VMs, to Azure.
Database Migration Assistant (DMA)	Assess on-premises SQL Server databases for migration to Azure SQL DB, Azure SQL Managed Instance, or to Azure VMs running SQL Server.	DMA helps pinpoint potential blocking issues for migration. It identifies unsupported features, new features that you can benefit from after migration, and helps you to identify the right path for database migration. Learn more .
Database Migration Service (DMS)	Migrate on-premises databases to Azure VMs running SQL, Azure SQL DB, and Azure SQL Managed Instances.	Learn more about DMS.

TOOL	ASSESS/MIGRATE	DETAILS
Movere	Assess servers.	Learn more about Movere.
Web App Migration Assistant	Assess and migrate on-premises web apps to Azure.	Use the Azure App Service Migration Assistant to assess on-premises websites for migration to the Azure App Service. Use the Assistant to migrate .NET and PHP web apps to Azure. Learn more about the Azure App Service Migration Assistant.
Azure Data Box	Offline data migration.	Use Azure Data Box products to move large amounts of data offline to Azure. Learn more .

ISV integration

Azure Migrate integrates with a number of ISV offerings.

ISV	FEATURE
Carbonite	Migrate servers
Cloudamize	Assess servers
Corent Technology	Assess and migrate servers
Device 42	Assess servers
Lakeside	Assess VDI
RackWare	Migrate servers
Turbonomic	Assess servers
UnifyCloud	Assess servers and databases

Azure Migrate Server Assessment tool

The Azure Migrate:Server Assessment tool discovers and assesses on-premises VMware VMs, Hyper-V VMs, and physical servers for migration to Azure. Here's what the tool does:

- **Azure readiness:** Assesses whether on-premises machines are ready for migration to Azure.
- **Azure sizing:** Estimates the size of Azure VMs after migration.
- **Azure cost estimation:** Estimated costs for running on-premises servers in Azure.
- **Dependency analysis:** If you use Server Assessment with [dependency analysis](#), you can effectively identify cross-server dependencies, and optimize strategies for moving inter-dependent servers to Azure.

Server Assessment uses a lightweight [Azure Migrate appliance](#) that you deploy on-premises.

- The appliance runs on a VM or physical server. You can install it easily using a downloaded template.

- The appliance discovers on-premises machines, and continually sends machine metadata and performance data to Azure Migrate.
- Appliance discovery is agentless. Nothing is installed on discovered machines.
- After the appliance discovery, you gather discovered machines into groups, and run assessments for a group.

Azure Migrate Server Migration tool

The Azure Migrate:Server Migration tool helps you to migrate on-premises VMware VMs, Hyper-V VMs, physical servers, other virtualized machines, and public cloud VMs, to Azure. You can migrate machines after assessing them, or migrate them without an assessment.

For agentless migration of VMware VMs, and migration of Hyper-V VMs, Server Migration uses an Azure Migrate appliance that you deploy on-premises. The appliance is also used if you set up server assessment, and it's described in the previous section.

Selecting assessment/migration tools

In the Azure Migrate hub, you select the tool you want to use for assessment or migration, and add it to an Azure Migrate project. If you add an ISV tool or Movere:

- To get started you obtain a license, or sign up for a free trial, in accordance with the tool instructions. Tools licensing is determined by the ISV or tool.
- In each tool, there's an option to connect to Azure Migrate. Follow the tool instructions to connect.
- You track your migration journey from within the Azure Migrate project, across all tools.

Movere

Movere is a SaaS platform that increases business intelligence by accurately presenting entire IT environments within a single day. As organizations grow, change, and digitally optimize, the solution provides enterprises with the confidence they need to have visibility and control of their environments regardless of platform, application, or geography. Movere was [acquired](#) by Microsoft and is no longer sold as a standalone offer. Movere is available through the Microsoft Solution Assessment and Cloud Economics Programs. [Learn more](#) about Movere.

We encourage you to also look at Azure Migrate, our built-in migration service. Azure Migrate provides a central hub to simplify your migration to the cloud. The hub features comprehensive support for different workloads, including physical and virtual servers, databases, and applications. End-to-end visibility makes it easy to track progress throughout discovery, assessment, and migration. With both Azure and partner ISV tools built in, Azure Migrate also has an extensive range of features, including virtual and physical server discovery, performance-based right sizing, cost planning, import-based assessments, and agentless application dependency analysis. If you're looking for expert help to get started, Microsoft has skilled [Azure Expert Managed Service Provider](#) to guide you along the journey. Check out the [Azure Migrate website](#).

Azure Migrate versions

There are two versions of the Azure Migrate service:

- **Current version:** Use this version to create Azure Migrate projects, discover on-premises machines, and orchestrate assessments and migrations. [Learn more](#) about what's new in this version.
- **Previous version:** If you used the previous version of Azure Migrate (only assessment of on-premises VMware VMs was supported), you should now use the current version. You can no longer create Azure Migrate projects using the previous version, and we recommend that you don't perform new discoveries. To access existing projects, in the Azure portal, search for and select **Azure Migrate**. On the **Azure Migrate**

dashboard, there's a notification and a link to access old Azure Migrate projects.

Next steps

- Try our tutorials to assess [VMware VMs](#), [Hyper-V VMs](#), or [physical servers](#).
- [Review frequently asked questions](#) about Azure Migrate.

What's new in Azure Migrate

3/23/2020 • 3 minutes to read • [Edit Online](#)

Azure Migrate helps you to discover, assess, and migrate on-premises servers, apps, and data to the Microsoft Azure cloud. This article summarizes new releases and features in Azure Migrate.

Update (March 2020)

A script-based installation is now available to set up the [Azure Migrate appliance](#):

- The script-based installation is an alternative to the .OVA (VMware)/VHD (Hyper-V) installation of the appliance.
- It provides a PowerShell installer script that can be used to set up the appliance for VMware/Hyper-V on an existing machine running Windows Server 2016.

Update (November 2019)

A number of new features were added to Azure Migrate:

- **Physical server assessment.** Assessment of on-premises physical servers is now supported, in addition to physical server migration that is already supported.
- **Import-based assessment.** Assessment of machines using metadata and performance data provided in a CSV file is now supported.
- **Application discovery:** Azure Migrate now supports application-level discovery of apps, roles, and features using the Azure Migrate appliance. This is currently supported for VMware VMs only, and is limited to discovery only (assessment isn't currently supported). [Learn more](#)
- **Agentless dependency visualization:** You no longer need to explicitly install agents for dependency visualization. Both agentless and agent-based are now supported.
- **Virtual Desktop:** Use ISV tools to assess and migrate on-premises virtual desktop infrastructure (VDI) to Windows Virtual Desktop in Azure.
- **Web app:** The Azure App Service Migration Assistant, used for assessing and migration web apps, is now integrated into Azure Migrate.

New assessment and migration tools were added to Azure Migrate:

- **Rackware:** Offering cloud migration.
- **Movere:** Offering assessment.

[Learn more](#) about using tools and ISV offerings for assessment and migration in Azure Migrate.

Azure Migrate current version

The current version of Azure Migrate (released in July 2019) provides a number of new features:

- **Unified migration platform:** Azure Migrate now provides a single portal to centralize, manage, and track your migration journey to Azure, with an improved deployment flow and portal experience.
- **Assessment and migration tools:** Azure Migrate provides native tools, and integrates with other Azure services, as well as with independent software vendor (ISV) tools. [Learn more](#) about ISV integration.
- **Azure Migrate assessment:** Using the Azure Migrate Server Assessment tool, you can assess VMware VMs and Hyper-V VMs for migration to Azure. You can also assess for migration using other Azure services, and ISV tools.

- **Azure Migrate migration:** Using the Azure Migrate Server Migration tool, you can migrate on-premises VMware VMs and Hyper-V VMs to Azure, as well as physical servers, other virtualized servers, and private/public cloud VMs. In addition, you can migrate to Azure using ISV tools.
- **Azure Migrate appliance:** Azure Migrate deploys a lightweight appliance for discovery and assessment of on-premises VMware VMs and Hyper-V VMs.
 - This appliance is used by Azure Migrate Server Assessment, and Azure Migrate Server Migration for agentless migration.
 - The appliance continuously discovers server metadata and performance data, for the purposes of assessment and migration.
- **VMware VM migration:** Azure Migrate Server Migration provides a couple of methods for migrating on-premises VMware VMs to Azure. An agentless migration using the Azure Migrate appliance, and an agent-based migration that uses a replication appliance, and deploys an agent on each VM you want to migrate. [Learn more](#)
- **Database assessment and migration:** From Azure Migrate, you can assess on-premises databases for migration to Azure using the Azure Database Migration Assistant. You can migrate databases using the Azure Database Migration Service.
- **Web app migration:** You can assess web apps using a public endpoint URL with the Azure App Service. For migration of internal .NET apps, you can download and run the App Service Migration Assistant.
- **Data Box:** Import large amounts offline data into Azure using Azure Data Box in Azure Migrate.

Azure Migrate previous version

If you were using the previous version of Azure Migrate (only assessment of on-premises VMware VMs was supported), you should now use the current version. In the previous version, you can no longer create new Azure Migrate projects, or perform new discoveries. You can still access existing projects. To do this in the Azure portal > All services, search for **Azure Migrate**. In the Azure Migrate notifications, there's a link to access old Azure Migrate projects.

Next steps

- [Learn more](#) about Azure Migrate pricing.
- [Review frequently asked questions](#) about Azure Migrate.
- Try out our tutorials to assess [VMware VMs](#) and [Hyper-V VMs](#).

minutes to read • [Edit Online](#)

This article answers common questions about Azure Migrate. If you have questions after you read this article, you can post them in the [Azure Migrate forum](#). You also can review these articles:

- Questions about the [Azure Migrate appliance](#)
- Questions about [discovery, assessment, and dependency visualization](#)

What is Azure Migrate?

Azure Migrate provides a central hub to track discovery, assessment, and migration of your on-premises apps and workloads and private and public cloud VMs to Azure. The hub provides Azure Migrate tools for assessment and migration and third-party ISV offerings. [Learn more](#).

What can I do with Azure Migrate?

Use Azure Migrate to discover, assess, and migrate on-premises infrastructure, applications, and data to Azure. Azure Migrate supports assessment and migration of on-premises VMware VMs, Hyper-V VMs, physical servers, other virtualized VMs, databases, web apps, and virtual desktops.

What's the difference between Azure Migrate and Azure Site Recovery?

[Azure Migrate](#) provides a centralized hub for assessment and migration to Azure.

[Azure Site Recovery](#) is a disaster recovery solution.

The Azure Migrate: Server Migration tool uses some back-end Site Recovery functionality for lift-and-shift migration of some on-premises machines.

What's the difference between Azure Migrate: Server Assessment and the MAP Toolkit?

Server Assessment provides assessment to help with migration readiness, and evaluation of workloads for migration to Azure. The [Microsoft Assessment and Planning \(MAP\) Toolkit](#) helps with other tasks, including migration planning for newer versions of Windows client and server operating systems, and software usage tracking. For these scenarios, continue to use the MAP Toolkit.

What's the difference between Server Assessment and the Site Recovery Deployment Planner?

Server Assessment is a migration planning tool. The Site Recovery Deployment Planner is a disaster recovery planning tool.

Choose your tool based on what you want to do:

- **Plan on-premises migration to Azure:** If you plan to migrate your on-premises servers to Azure, use Server Assessment for migration planning. Server Assessment assesses on-premises workloads and provides guidance and tools to help you migrate. After the migration plan is in place, you can use tools like Azure Migrate: Server Migration to migrate the machines to Azure.

- **Plan disaster recovery to Azure:** If you plan to set up disaster recovery from on-premises to Azure with Site Recovery, use the Site Recovery Deployment Planner. The Deployment Planner provides a deep, Site Recovery-specific assessment of your on-premises environment for the purpose of disaster recovery. It provides recommendations related to disaster recovery, such as replication and failover.

How does Server Migration work with Site Recovery?

- If you use Azure Migrate: Server Migration to perform an *agentless* migration of on-premises VMware VMs, migration is native to Azure Migrate and Site Recovery isn't used.
- If you use Azure Migrate: Server Migration to perform an *agent-based* migration of VMware VMs, or if you migrate Hyper-V VMs or physical servers, Azure Migrate: Server Migration uses the Azure Site Recovery replication engine.

Which geographies are supported?

- **VMware VMs:** Review the Azure Migrate [supported geographies](#) for VMware VMs.
- **Hyper-V VMs:** Review the Azure Migrate [supported geographies](#) for Hyper-V VMs.

How do I get started?

Identify the tool you need, and then add the tool to an Azure Migrate project.

To add an ISV tool or Movere:

1. Get started by obtaining a license, or sign up for a free trial, in accordance with the tool policy. Licensing for tools is in accordance with the ISV or tool licensing model.
2. In each tool, there's an option to connect to Azure Migrate. Follow the tool instructions and documentation to connect the tool with Azure Migrate.

You can track your migration journey from within the Azure Migrate project, across Azure, and in other tools.

How do I delete a project?

Learn how to [delete a project](#).

Next steps

Read the [Azure Migrate overview](#).

Azure Migrate appliance: Common questions

3/31/2020 • 5 minutes to read • [Edit Online](#)

This article answers common questions about the Azure Migrate appliance. If you have other questions, check these resources:

- [General questions](#) about Azure Migrate
- Questions about [discovery, assessment, and dependency visualization](#)
- Questions about [server migration](#)
- Get questions answered in the [Azure Migrate forum](#)

What is the Azure Migrate appliance?

The Azure Migrate appliance is a lightweight appliance that the Azure Migrate: Server Assessment tool uses to discover and assess on-premises servers. The Azure Migrate: Server Migration tool also uses the appliance for agentless migration of on-premises VMware VMs.

Here's more information about the Azure Migrate appliance:

- The appliance is deployed on-premises as a VM or physical machine.
- The appliance discovers on-premises machines and continually sends machine metadata and performance data to Azure Migrate.
- Appliance discovery is agentless. Nothing is installed on discovered machines.

[Learn more](#) about the appliance.

How does the appliance connect to Azure?

The appliance can connect over the internet or by using Azure ExpressRoute with public/Microsoft peering.

Does appliance analysis affect performance?

The Azure Migrate appliance profiles on-premises machines continuously to measure performance data. This profiling has almost no performance impact on profiled machines.

Can I harden the appliance VM?

When you use the downloaded template to create the appliance VM, you can add components (antivirus, for example) to the template if you leave in place the communication and firewall rules that are required for the Azure Migrate appliance.

What network connectivity is required?

See the following articles for information about network connectivity requirements for the Azure Migrate appliance:

- **VMware assessment:** [URL access](#) and [port access](#)
- **VMware agentless migration:** [URL access](#) and [port access](#)
- **Hyper-V assessment:** [URL access](#) and [port access](#)

What data does the appliance collect?

See the following articles for information about data that the Azure Migrate appliance collects on VMs:

- VMware VM: [Review](#) collected data. [
- Hyper-V VM: [Review](#) collected data.

How is data stored?

Data that's collected by the Azure Migrate appliance is stored in the Azure location where you created the Azure Migrate project.

Here's more information about how data is stored:

- The collected data is securely stored in CosmosDB in a Microsoft subscription. The data is deleted when you delete the Azure Migrate project. Storage is handled by Azure Migrate. You can't specifically choose a storage account for collected data.
- If you use [dependency visualization](#), the data that's collected is stored in the United States in an Azure Log Analytics workspace created in your Azure subscription. The data is deleted when you delete the Log Analytics workspace in your subscription.

How much data is uploaded during continuous profiling?

The volume of data that's sent to Azure Migrate depends on multiple parameters. As an example, an Azure Migrate project that has 10 machines (each with one disk and one NIC) sends approximately 50 MB of data per day. This value is approximate; the actual value varies depending on the number of data points for the disks and NICs. If the number of machines, disks, or NICs increases, the increase in data that's sent is nonlinear.

Is data encrypted at rest and in transit?

Yes, for both:

- Metadata is securely sent to the Azure Migrate service over the internet via HTTPS.
- Metadata is stored in an [Azure Cosmos](#) database and in [Azure Blob storage](#) in a Microsoft subscription. The metadata is encrypted at rest for storage.
- The data for dependency analysis also is encrypted in transit (by secure HTTPS). It's stored in a Log Analytics workspace in your subscription. The data is encrypted at rest for dependency analysis.

How does the appliance connect to vCenter Server?

These steps describe how the appliance connects to VMware vCenter Server:

1. The appliance connects to vCenter Server (port 443) by using the credentials you provided when you set up the appliance.
2. The appliance uses VMware PowerCLI to query vCenter Server to collect metadata about the VMs that are managed by vCenter Server.
3. The appliance collects configuration data about VMs (cores, memory, disks, NICs) and the performance history of each VM for the past month.
4. The collected metadata is sent to the Azure Migrate: Server Assessment tool (over the internet via HTTPS) for assessment.

Can the Azure Migrate appliance connect to multiple vCenter Servers?

No. There's a one-to-one mapping between an [Azure Migrate appliance](#) and vCenter Server. To discover VMs on

multiple vCenter Server instances, you must deploy multiple appliances.

Can an Azure Migrate project have multiple appliances?

A project can have multiple appliances attached to it. However, an appliance can only be associated with one project.

Can the Azure Migrate appliance/Replication appliance connect to the same vCenter?

Yes. You can add both the Azure Migrate appliance (used for assessment and agentless VMware migration), and the replication appliance (used for agent-based migration of VMware VMs) to the same vCenter server.

How many VMs or servers can I discover with an appliance?

You can discover up to 10,000 VMware VMs, up to 5,000 Hyper-V VMs, and up to 250 physical servers with a single appliance. If you have more machines in your on-premises environment, read about [scaling a Hyper-V assessment](#), [scaling a VMware assessment](#), and [scaling a physical server assessment](#).

Can I delete an appliance?

Currently, deleting an appliance from the project isn't supported.

The only way to delete the appliance is to delete the resource group that contains the Azure Migrate project that's associated with the appliance.

However, deleting the resource group also deletes other registered appliances, the discovered inventory, assessments, and all other Azure components in the resource group that are associated with the project.

Can I use the appliance with a different subscription or project?

After you use the appliance to initiate discovery, you can't reconfigure the appliance to use with a different Azure subscription, and you can't use it in a different Azure Migrate project. You also can't discover VMs on a different instance of vCenter Server. Set up a new appliance for these tasks.

Can I set up the appliance on an Azure VM?

No. Currently, this option isn't supported.

Can I discover on an ESXi host?

No. To discover VMware VMs, you must have vCenter Server.

How do I update the appliance?

By default, the appliance and its installed agents are updated automatically. The appliance checks for updates every 24 hours. Updates that fail are retried.

Only the appliance and the appliance agents are updated by these automatic updates. The operating system is not updated by Azure Migrate automatic updates. Use Windows Updates to keep the operating system up to date.

Can I check agent health?

Yes. In the portal, go the [Agent health](#) page for the Azure Migrate: Server Assessment or Azure Migrate: Server Migration tool. There, you can check the connection status between Azure and the discovery and assessment

agents on the appliance.

Next steps

Read the [Azure Migrate overview](#).

This article answers common questions about discovery, assessment, and dependency analysis in Azure Migrate. If you have other questions, check these resources:

- [General questions](#) about Azure Migrate
- Questions about the [Azure Migrate appliance](#)
- Questions about [server migration](#)
- Get questions answered in the [Azure Migrate forum](#)

How many VMs can I discover with an appliance?

You can discover up to 10,000 VMware VMs, up to 5,000 Hyper-V VMs, and up to 250 physical servers by using a single appliance. If you have more machines, read about [scaling a Hyper-V assessment](#), [scaling a VMware assessment](#), or [scaling a physical server assessment](#).

The size of my VM changed. Can I run an assessment again?

The Azure Migrate appliance continuously collects information about the on-premises environment. An assessment is a point-in-time snapshot of on-premises VMs. If you change the settings on a VM that you want to assess, use the recalculate option to update the assessment with the latest changes.

How do I discover VMs in a multitenant environment?

- **VMware:** If an environment is shared across tenants and you don't want to discover a tenant's VMs in another tenant's subscription, create VMware vCenter Server credentials that can access only the VMs you want to discover. Then, use those credentials when you start discovery in the Azure Migrate appliance.
- **Hyper-V:** Discovery uses Hyper-V host credentials. If VMs share the same Hyper-V host, there's currently no way to separate the discovery.

Do I need vCenter Server?

Yes, Azure Migrate requires vCenter Server in a VMware environment to perform discovery. Azure Migrate doesn't support discovery of ESXi hosts that aren't managed by vCenter Server.

What are the sizing options?

With as-on-premises sizing, Azure Migrate doesn't consider VM performance data for assessment. Azure Migrate assesses VM sizes based on the on-premises configuration. With performance-based sizing, sizing is based on utilization data.

For example, if an on-premises VM has four cores and 8 GB of memory at 50% CPU utilization and 50% memory utilization:

- As-on-premises sizing will recommend an Azure VM SKU that has four cores and 8 GB of memory.
- Performance-based sizing will recommend a VM SKU that has two cores and 4 GB of memory because the utilization percentage is considered.

Similarly, disk sizing depends on sizing criteria and storage type:

- If the sizing criteria is performance-based and the storage type is automatic, Azure Migrate takes the IOPS and throughput values of the disk into account when it identifies the target disk type (Standard or Premium).
- If the sizing criteria is performance-based and the storage type is Premium, Azure Migrate recommends a Premium disk SKU based on the size of the on-premises disk. The same logic is applied to disk sizing when the sizing is as-on-premises and the storage type is Standard or Premium.

Does performance history and utilization affect sizing?

Yes, performance history and utilization affect sizing in Azure Migrate.

Performance history

For performance-based sizing only, Azure Migrate collects the performance history of on-premises machines, and then uses it to recommend the VM size and disk type in Azure:

1. The appliance continuously profiles the on-premises environment to gather real-time utilization data every 20 seconds.
2. The appliance rolls up the collected 20-second samples and uses them to create a single data point every 15 minutes.
3. To create the data point, the appliance selects the peak value from all 20-second samples.
4. The appliance sends the data point to Azure.

Utilization

When you create an assessment in Azure, depending on performance duration and the performance history percentile value that is set, Azure Migrate calculates the effective utilization value, and then uses it for sizing.

For example, if you set the performance duration to one day and the percentile value to 95th percentile, Azure Migrate sorts the 15-minute sample points sent by the collector for the past day in ascending order. It picks the 95th percentile value as the effective utilization.

Using the 95th percentile value ensures that outliers are ignored. Outliers might be included if your Azure Migrate uses the 99th percentile. To pick the peak usage for the period without missing any outliers, set Azure Migrate to use the 99th percentile.

How are import-based assessments different from assessments with discovery source as appliance?

Import-based assessments are assessments created with machines that are imported into Azure Migrate using a CSV file. Only four fields are mandatory to import: Server name, cores, memory, and operating system. Here are some things to note:

- The readiness criteria is less stringent in import-based assessments on the boot type parameter. If the boot type isn't provided, it is assumed the machine has BIOS boot type and the machine is not marked as **Conditionally Ready**. In assessments with discovery source as appliance, the readiness is marked as **Conditionally Ready** if the boot type is missing. This difference in readiness calculation is because users may not have all information on the machines in the early stages of migration planning when import-based assessments are done.
- Performance-based import assessments use the utilization value provided by the user for right-sizing calculations. Since the utilization value is provided by the user, the **Performance history and Percentile utilization** options are disabled in the assessment properties. In assessments with discovery source as appliance, the chosen percentile value is picked from the performance data collected by the appliance.

What is dependency visualization?

Dependency visualization can help you assess groups of VMs to migrate with greater confidence. Dependency visualization cross-checks machine dependencies before you run an assessment. It helps ensure that nothing is left

behind, and it helps avoid unexpected outages when you migrate to Azure. Azure Migrate uses the Service Map solution in Azure Monitor to enable dependency visualization. [Learn more](#).

NOTE

Dependency visualization isn't available in Azure Government.

What's the difference between agent-based and agentless?

The differences between agentless visualization and agent-based visualization are summarized in the table.

Requirement	Agentless	Agent-based
Support	This option is currently in preview, and is only available for VMware VMs. Review supported operating systems .	In general availability (GA).
Agent	No need to install agents on machines you want to cross-check.	Agents to be installed on each on-premises machine that you want to analyze: The Microsoft Monitoring agent (MMA) , and the Dependency agent .
Prerequisites	Review the prerequisites and deployment requirements.	Review the prerequisites and deployment requirements.
Log Analytics	Not required.	Azure Migrate uses the Service Map solution in Azure Monitor logs for dependency visualization. Learn more .
How it works	Captures TCP connection data on machines enabled for dependency visualization. After discovery, it gathers data at intervals of five minutes.	Service Map agents installed on a machine gather data about TCP processes and inbound/outbound connections for each process.
Data	Source machine server name, process, application name. Destination machine server name, process, application name, and port.	Source machine server name, process, application name. Destination machine server name, process, application name, and port. Number of connections, latency, and data transfer information are gathered and available for Log Analytics queries.
Visualization	Dependency map of single server can be viewed over a duration of one hour to 30 days.	Dependency map of a single server. Map can be viewed over an hour only. Dependency map of a group of servers. Add and remove servers in a group from the map view.
Data export	Can't currently be downloaded in tabular format.	Data can be queried with Log Analytics.

Do I pay for dependency visualization?

No. Learn more about [Azure Migrate pricing](#).

What do I install for agent-based dependency visualization?

To use agent-based dependency visualization, download and install agents on each on-premises machine that you want to evaluate:

- [Microsoft Monitoring Agent \(MMA\)](#)
- [Dependency agent](#)
- If you have machines that don't have internet connectivity, download and install the Log Analytics gateway on them.

You need these agents only if you use agent-based dependency visualization.

Can I use an existing workspace?

Yes, for agent-based dependency visualization you can attach an existing workspace to the migration project and use it for dependency visualization.

Can I export the dependency visualization report?

No, the dependency visualization report in agent-based visualization can't be exported. However, Azure Migrate uses Service Map, and you can use the [Service Map REST API](#) to retrieve the dependencies in JSON format.

Can I automate agent installation?

For agent-based dependency visualization:

- Use a [script to install the Dependency agent](#).
- For MMA, [use the command line or automation](#), or use a [script](#).
- In addition to scripts, you can use deployment tools like Microsoft Endpoint Configuration Manager and [Intigua](#) to deploy the agents.

What operating systems does MMA support?

- View the list of [Windows operating systems that MMA supports](#).
- View the list of [Linux operating systems that MMA supports](#).

Can I visualize dependencies for more than one hour?

For agent-based visualization, you can visualize dependencies for up to one hour. You can go back as far as one month to a specific date in history, but the maximum duration for visualization is one hour. For example, you can use the time duration in the dependency map to view dependencies for yesterday, but you can view dependencies only for a one-hour window. However, you can use Azure Monitor logs to [query dependency data](#) for a longer duration.

For agentless visualization, you can view the dependency map of a single server from a duration of between one hour and 30 days.

Can I visualize dependencies for groups of more than 10 VMs?

You can [visualize dependencies](#) for groups that have up to 10 VMs. If you have a group that has more than 10 VMs, we recommend that you split the group into smaller groups, and then visualize the dependencies.

Next steps

Read the [Azure Migrate overview](#).

This article answers common questions about the Azure Migrate: Server Migration tool. If you have other questions, check these resources:

- [General questions](#) about Azure Migrate
- Questions about the [Azure Migrate appliance](#)
- Questions about [discovery, assessment, and dependency visualization](#)
- Get questions answered in the [Azure Migrate forum](#)

How does agentless VMware replication work?

The agentless replication method for VMware uses VMware snapshots and VMware Changed Block Tracking (CBT).

Here's the process:

1. When you start replication, an initial replication cycle is scheduled. In the initial cycle, a snapshot of the VM is taken. The snapshot is used to replicate the VMs VMDKs (disks).
2. After the initial replication cycle finishes, delta replication cycles are scheduled periodically.
 - During delta replication, a snapshot is taken, and data blocks that have changed since the previous replication cycle are replicated.
 - VMware CBT is used to determine blocks that have changed since the last cycle.
 - The frequency of the periodic replication cycles is automatically managed by Azure Migrate and depends on how many other VMs and disks are concurrently replicating from the same datastore. In ideal conditions, replication eventually converges to one cycle per hour for each VM.

When you migrate, an on-demand replication cycle is scheduled for the machine to capture any remaining data. To ensure zero data loss and application consistency, you can choose to shut down the machine during migration.

Why isn't resynchronization exposed?

During agentless migration, in every delta cycle, the difference between the current snapshot and the previously taken snapshot is written. It's always the difference between snapshots, folding data in. If a specific sector is written N times between snapshots, only the last write needs to be transferred because we are interested only in the last sync. The process is different from agent-based replication, during which we track and apply every write. In this process, every delta cycle is a resynchronization. So, no resynchronization option exposed. If the disks ever are not synchronized because of a failure, it's fixed in the next cycle.

How does churn rate affect agentless replication?

Because agentless replication folds in data, the *churn pattern* is more important than the *churn rate*. When a file is written again and again, the rate doesn't have much impact. However, a pattern in which every other sector is written causes high churn in the next cycle. Because we minimize the amount of data we transfer, we allow the data to fold as much as possible before we schedule the next cycle.

How frequently is a replication cycle scheduled?

The formula to schedule the next replication cycle is (previous cycle time / 2) or one hour, whichever is higher.

For example, if a VM takes four hours for a delta cycle, the next cycle is scheduled in two hours, and not in the next

hour. The process is different immediately after initial replication, when the first delta cycle is scheduled immediately.

How does agentless replication affect VMware servers?

Agentless replication results in some performance impact on VMware vCenter Server and VMware ESXi hosts. Because agentless replication uses snapshots, it consumes IOPS on storage, so some IOPS storage bandwidth is required. We don't recommend using agentless replication if you have constraints on storage or IOPs in your environment.

Can I do agentless migration of UEFI VMs to Azure Gen 2?

No. Use Azure Site Recovery to migrate these VMs to Gen 2 Azure VMs.

Can I pin VMs to Azure Availability Zones when I migrate?

No. Azure Availability Zones aren't supported for Azure Migrate migration.

What transport protocol does Azure Migrate use during replication?

Azure Migrate uses the Network Block Device (NBD) protocol with SSL encryption.

What is the minimum vCenter Server version required for migration?

You must have at least vCenter Server 5.5 and vSphere ESXi host version 5.5.

Can customers migrate their VMs to unmanaged disks?

No. Azure Migrate supports migration only to managed disks (Standard HDD, Premium SSD).

How many VMs can I replicate at one time by using agentless migration?

Currently, you can migrate 100 VMs per instance of vCenter Server simultaneously. Migrate in batches of 10 VMs.

How do I throttle replication in using Azure Migrate appliance for agentless VMware replication?

You can throttle using NetQosPolicy. For example:

The AppNamePrefix to use in the NetQosPolicy is "GatewayWindowsService.exe". You could create a policy on the Azure Migrate appliance to throttle replication traffic from the appliance by creating a policy such as this one:

```
New-NetQosPolicy -Name "ThrottleReplication" -AppPathNameMatchCondition "GatewayWindowsService.exe" -ThrottleRateActionBitsPerSecond 1MB
```

When do I migrate machines as physical servers?

Migrating machines by treating them as physical servers is useful in a number of scenarios:

- When you're migrating on-premises physical servers.
- If you're migrating VMs virtualized by platforms such as Xen, KVM.
- To migrate Hyper-V or VMware VMs, if for some reason you're unable to use the standard migration process for [Hyper-V](#), or [VMware](#) migration. For example if you're not running VMware vCenter, and are using ESXi hosts

only.

- To migrate VMs that are currently running in private clouds to Azure
- If you want to migrate VMs running in public clouds such as Amazon Web Services (AWS) or Google Cloud Platform (GCP), to Azure.

Do I need VMware vCenter to migrate VMware VMs?

To [migrate VMware VMs](#) using VMware agent-based or agentless migration, ESXi hosts on which VMs are located must be managed by vCenter Server. If you don't have vCenter Server, you can migrate VMware VMs by migrating them as physical servers. [Learn more](#).

Next steps

Read the [Azure Migrate overview](#).

Prepare VMware VMs for assessment and migration to Azure

4/2/2020 • 5 minutes to read • [Edit Online](#)

This article helps you to prepare for assessment and/or migration of on-premises VMware VMs to Azure using [Azure Migrate](#).

This tutorial is the first in a series that shows you how to assess and migrate VMware VMs. In this tutorial, you learn how to:

- Prepare Azure to work with Azure Migrate.
- Prepare VMware for VM assessment with the Azure Migrate:Server Assessment tool.
- Prepare VMware for VM migration with the Azure Migrate:Server Migration tool.

NOTE

Tutorials show you the simplest deployment path for a scenario. They're useful when you learn how to set up a deployment, and as a quick proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prepare Azure

You need these permissions for these tasks in Azure, before you can assess or migrate VMware VMs.

TASK	DETAILS
Create an Azure Migrate project	Your Azure account needs Contributor or Owner permissions to create a project.
Register resource providers	Azure Migrate uses a lightweight Azure Migrate appliance to discover and assess VMware VMs, and to migrate them to Azure with Azure Migrate:Server Assessment. During appliance registration, resource providers are registered with the subscription chosen in the appliance. Learn more . To register the resource providers, you need a Contributor or Owner role on the subscription.

TASK	DETAILS
Create Azure AD apps	<p>When registering the appliance, Azure Migrate creates Azure Active Directory (Azure AD) apps.</p> <ul style="list-style-type: none"> - The first app is used for communication between the agents running on the appliance, and their respective services running on Azure. - The second app is used exclusively to access KeyVault created in the user's subscription for agentless VMware VM migration. Learn more. <p>You need permissions to create Azure AD apps (available in the Application Developer role).</p>
Create a Key Vault	<p>To migrate VMware VMs using agentless migration, Azure Migrate creates a Key Vault to manage access keys to the replication storage account in your subscription.</p> <p>To create the vault, you need role assignment permissions on the resource group in which the Azure Migrate project resides.</p>

Assign permissions to create project

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Assign permissions to register the appliance

To register the appliance, you assign permissions for Azure Migrate to create the Azure AD apps during appliance registration. The permissions can be assigned using one of the following methods:

- **Grant permissions:** A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
- **Assign application developer role:** A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.

NOTE

- The apps don't have any other access permissions on the subscription other than those described above.
- You only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

Grant account permissions

If you want tenant/global admin to grant permissions, do this as follows:

1. In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User Settings**.
2. The admin should set **App registrations** to **Yes**. This is a default setting that isn't sensitive. [Learn more](#).

Assign Application Developer role

Alternatively, the tenant/global admin can assign the Application Developer role to an account. [Learn more about assigning a role.](#)

Assign permissions to create a Key Vault

To enable Azure Migrate to create a Key Vault, assign permissions as follows:

1. In the resource group in the Azure portal, select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
 - To run server assessment, **Contributor** permissions are enough.
 - To run agentless server migration, you should have **Owner** (or **Contributor** and **User Access Administrator**) permissions.
3. If you don't have the required permissions, request them from the resource group owner.

Prepare for VMware VM assessment

To prepare for VMware VM assessment, you need to:

- **Verify VMware settings.** Make sure that the vCenter Server and VMs you want to migrate meet requirements.
- **Set up an account for assessment.** Azure Migrate uses this account to access the vCenter Server, to discover VMs for assessment.
- **Verify appliance requirements.** Verify deployment requirements for the Azure Migrate appliance, before you deploy it.

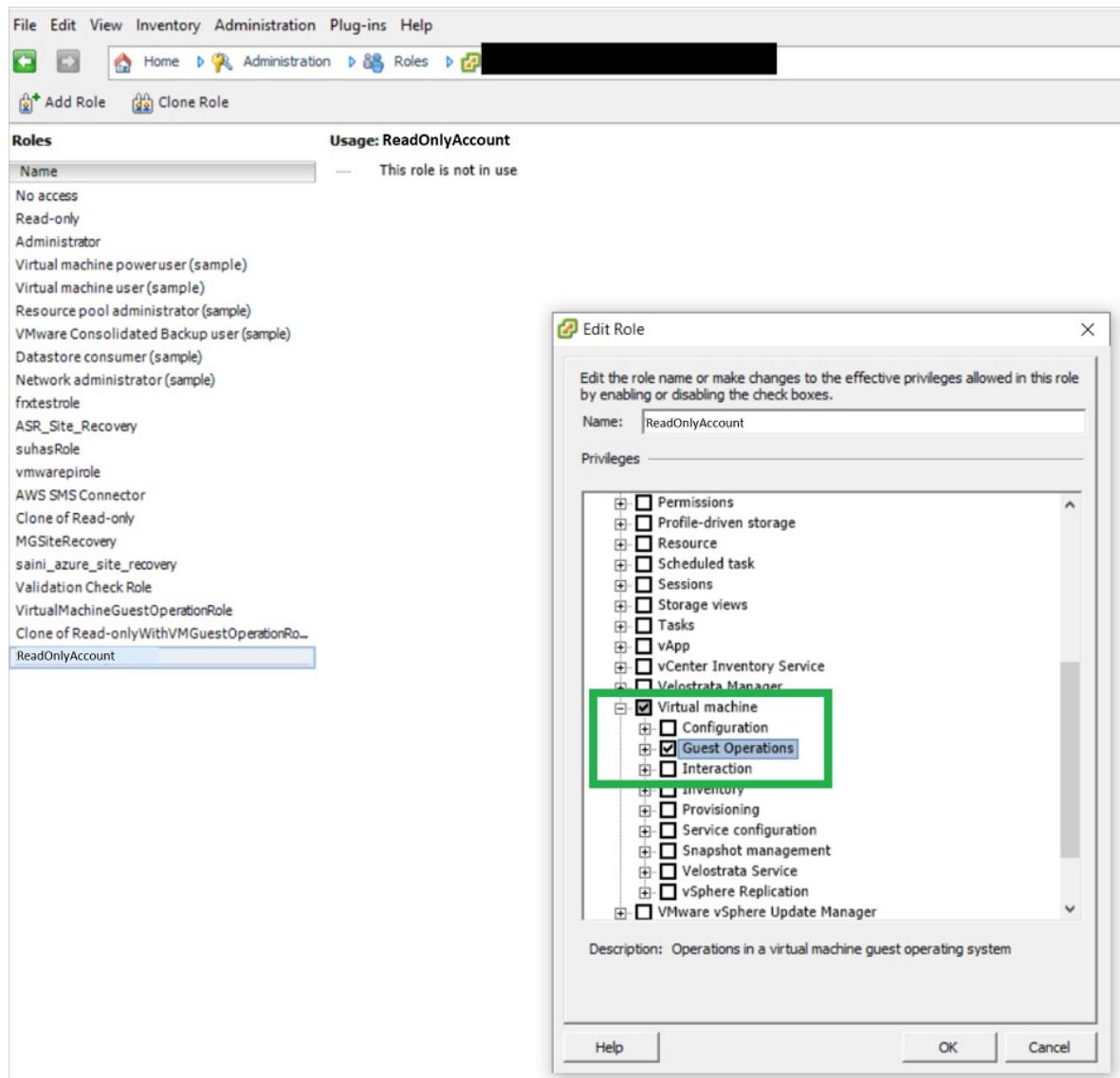
Verify VMware settings

1. [Check](#) VMware server requirements for assessment.
2. [Make sure](#) that the ports you need are open on vCenter Server.
3. On vCenter Server, make sure that your account has permissions to create a VM using an OVA file. You deploy the Azure Migrate appliance as a VMware VM, using an OVA file.

Set up an account for assessment

Azure Migrate needs to access the vCenter Server to discover VMs for assessment and agentless migration.

- If you plan to discover applications or visualize dependency in an agentless manner, create a vCenter Server account with read-only access along with privileges enabled for **Virtual machines > Guest Operations**.



- If you are not planning to do application discovery and agentless dependency visualization, set up a read-only account for the vCenter Server.

Verify appliance settings for assessment

Before setting up the Azure Migrate appliance and beginning assessment in the next tutorial, prepare for appliance deployment.

1. [Verify](#) Azure Migrate appliance requirements.
2. [Review](#) the Azure URLs that the appliance will need to access. If you're using a URL-based firewall or proxy, ensure it allows access to the required URLs.
3. [Review data](#) that the appliance collects during discovery and assessment.
4. [Note](#) port access requirements for the appliance.

Prepare for agentless VMware migration

Review the requirements for [agentless migration](#) of VMware VMs.

1. [Review](#) VMware server requirements.
2. [Review the permissions](#) that Azure Migrate needs to access the vCenter Server.
3. [Review](#) VMware VMs requirements.
4. [Review](#) the Azure Migrate appliance requirements.
5. Note the [URL access](#) and [port access](#) requirements.

Prepare for agent-based VMware migration

Review the requirements for [agent-based migration](#) of VMware VMs.

1. [Review](#) VMware server requirements.
2. [Review the permissions](#) Azure Migrate needs to access the vCenter Server.
3. [Review](#) VMware VMs requirements, including installation of the Mobility service on each VM you want to migrate.
4. Agent-based migration uses a replication appliance:
 - [Review](#) the deployment requirements for the replication appliance.
 - [Review the options](#) for installing MySQL on the appliance.
 - Review the [URL](#) and [port](#) access requirements for the replication appliance.

Next steps

In this tutorial, you:

- Set up Azure permissions.
- Prepared VMware for assessment and migration.

Continue to the second tutorial to set up an Azure Migrate project, and assess VMware VMs for migration to Azure.

[Assess VMware VMs](#)

Assess VMware VMs by using Azure Migrate Server Assessment

4/1/2020 • 10 minutes to read • [Edit Online](#)

This article shows you how to assess on-premises VMware virtual machines (VMs), using the [Azure Migrate:Server Assessment](#) tool.

This tutorial is the second in a series that demonstrates how to assess and migrate VMware VMs to Azure. In this tutorial, you learn how to:

- Set up an Azure Migrate project.
- Set up an Azure Migrate appliance that runs on-premises to assess VMs.
- Start continuous discovery of on-premises VMs. The appliance sends configuration and performance data for discovered VMs to Azure.
- Group discovered VMs, and assess the VM group.
- Review the assessment.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the how-to articles.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

- [Complete the first tutorial](#) in this series. If you don't, the instructions in this tutorial won't work.
- Here's what you should have done in the first tutorial:
 - [Prepare Azure](#) to work with Azure Migrate.
 - [Prepare VMware for assessment](#) for assessment. This includes checking VMware settings, setting up an account that Azure Migrate can use to access vCenter Server.
 - [Verify](#) what you need in order to deploy the Azure Migrate appliance for VMware assessment.

Set up an Azure Migrate project

Set up a new Azure Migrate project as follows:

1. In the Azure portal > **All services**, search for **Azure Migrate**.
2. Under **Services**, select **Azure Migrate**.
3. In **Overview**, under **Discover, assess and migrate servers**, select **Assess and migrate servers**.

4. In **Getting started**, select **Add tools**.
5. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
6. In **Project Details**, specify the project name and the geography in which you want to create the project. Asia, Europe, United Kingdom, and United States are supported.

The project geography is used only to store the metadata gathered from on-premises VMs. You can select any target region when you run a migration.

7. Select **Next**.
8. In **Select assessment tool**, select **Azure Migrate: Server Assessment > Next**.

Add a tool

Migrate project Select assessment tool [Select migration tool](#) Review + add tool(s)

Start by choosing a server discovery and assessment tool. We recommend that you discover and assess your datacenter to determine migration readiness.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
 Azure Migrate: Server Assessment	View	VMware virtual machines Hyper-V virtual machines	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Cloudamize: Cloud Assessment	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Turbonomic: Turbonomic	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 UnifyCloud: CloudRecon	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Device42: Device42	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	Learn more

Note: Visit the ISV tool's website to learn more about tool capabilities.
Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#)

Skip adding an assessment tool for now

9. In **Select migration tool**, select **Skip adding a migration tool for now > Next**.
10. In **Review + add tools**, review the settings, and select **Add tools**.
11. Wait a few minutes for the Azure Migrate project to deploy. You'll be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

Set up the Azure Migrate appliance

Azure Migrate:Server Assessment uses a lightweight Azure Migrate appliance. The appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate.

- The appliance can be set up on a VMware VM using a downloaded OVA template. Alternatively, you can set up the appliance on a VM or physical machine with a PowerShell installer script.
- This tutorial uses the OVA template. Review [this article](#) if you want to set up the appliance using a script.

After creating the appliance, you check that it can connect to Azure Migrate:Server Assessment, configure it for the first time, and register it with the Azure Migrate project.

Download the OVA template

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, select **Discover**.
2. In **Discover machines > Are your machines virtualized?**, select **Yes, with VMWare vSphere hypervisor**.
3. Select **Download** to download the OVA template file.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with 'Overview', 'Migration goals', 'Servers' (which is selected and highlighted with a red box), 'Databases', 'Data Box', 'Manage', 'Discovered items', 'Support + troubleshooting', and 'New support request'. The main area is titled 'Discover machines' and asks 'Are your machines virtualized? Yes, with VMware vSphere Hypervisor'. It provides instructions for setting up the migration appliance, including steps to download the OVA file (highlighted with a red box) and create a virtual machine. A 'Next step' section suggests refining app dependency analysis.

Verify security

Check that the OVA file is secure, before you deploy it:

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following command to generate the hash for the OVA file:

```
C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]
```

Example usage: C:\>CertUtil -HashFile C:\AzureMigrate\AzureMigrate.ova SHA256

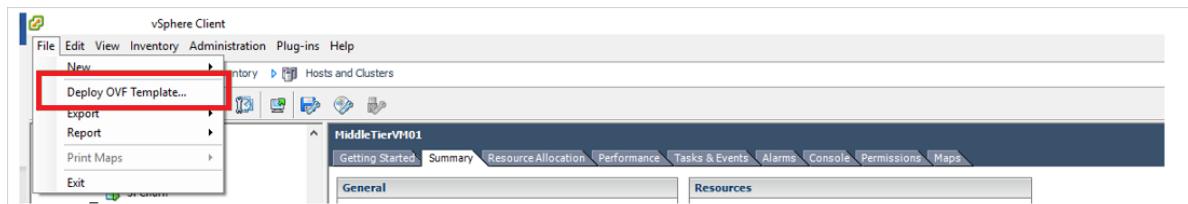
For version 2.19.07.30, the generated hash should match these values:

ALGORITHM	HASH VALUE
MD5	c06ac2a2c0f870d3b274a0b7a73b78b1
SHA256	4ce4faa3a78189a09a26bfa5b817c7acf5b555eb46999c2fad9d2ebc808540c

Create the appliance VM

Import the downloaded file, and create a VM:

1. In the vSphere Client console, select **File > Deploy OVF Template**.



2. In the Deploy OVF Template Wizard > **Source**, specify the location of the OVA file.
3. In **Name and Location**, specify a friendly name for the VM. Select the inventory object in which the VM will be hosted.
4. In **Host/Cluster**, specify the host or cluster on which the VM will run.
5. In **Storage**, specify the storage destination for the VM.
6. In **Disk Format**, specify the disk type and size.
7. In **Network Mapping**, specify the network to which the VM will connect. The network needs internet

connectivity to send metadata to Azure Migrate Server Assessment.

8. Review and confirm the settings, and then select **Finish**.

Verify appliance access to Azure

Make sure that the appliance VM can connect to [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time.

NOTE

If you set up the appliance using a [PowerShell script](#) instead of the downloaded OVA, the first two steps in this procedure aren't relevant.

1. In the vSphere Client console, right-click the VM, and then select **Open Console**.
2. Provide the language, time zone, and password for the appliance.
3. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app:
<https://appliance name or IP address: 44368>.

Alternately, you can open the app from the appliance desktop by selecting the app shortcut.

4. In the web app > **Set up prerequisites**, do the following:

- **License**: Accept the license terms, and read the third-party information.
- **Connectivity**: The app checks that the VM has internet access. If the VM uses a proxy:
 - Select **Proxy settings**, and specify the proxy address and listening port in the form `http://ProxyIPAddress` or `http://ProxyFQDN`.
 - Specify credentials if the proxy needs authentication.
 - Note that only HTTP proxy is supported.
- **Time sync**: The time on the appliance should be in sync with internet time for discovery to work properly.
- **Install updates**: The appliance ensures that the latest updates are installed.
- **Install VDDK**: The appliance checks that VMWare vSphere Virtual Disk Development Kit (VDDK) is installed. If it isn't installed, download VDDK 6.7 from VMware, and extract the downloaded zip contents to the specified location on the appliance.

Azure Migrate Server Migration uses the VDDK to replicate machines during migration to Azure.

Register the appliance with Azure Migrate

1. Select **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.

2. On the new tab, sign in by using your Azure username and password.

Sign-in with a PIN isn't supported.

3. After you successfully sign in, go back to the web app.

4. Select the subscription in which the Azure Migrate project was created, and then select the project.

5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or fewer.

6. Select **Register**.

Start continuous discovery

The appliance needs to connect to vCenter Server to discover the configuration and performance data of the VMs.

Specify vCenter Server details

1. In **Specify vCenter Server details**, specify the name (FQDN) or IP address of the vCenter Server instance. You can leave the default port or specify a custom port on which vCenter Server listens.
2. In **User name and Password**, specify the vCenter Server account credentials that the appliance will use to discover VMs on the vCenter Server instance.
 - You should have set up an account with the required permissions in the [previous tutorial](#).
 - If you want to scope discovery to specific VMware objects (vCenter Server datacenters, clusters, a folder of clusters, hosts, a folder of hosts, or individual VMs.), review the instructions in [this article](#) to restrict the account used by Azure Migrate.
3. Select **Validate connection** to make sure that the appliance can connect to vCenter Server.
4. In **Discover applications and dependencies on VMs**, optionally click **Add credentials**, and specify the operating system for which the credentials are relevant, and the credentials username and password. Then click **Add..**
 - You optionally add credentials here if you've created an account to use for the [application discovery feature](#), or the [agentless dependency analysis feature](#).
 - If you're not using these features, you can skip this setting.
 - Review the credentials needed for [app discovery](#), or for [agentless analysis](#).
5. **Save and start discovery**, to kick off VM discovery.

Discovery works as follows:

- It takes around 15 minutes for discovered VM metadata to appear in the portal.
- Discovery of installed applications, roles, and features takes some time. The duration depends on the number of VMs being discovered. For 500 VMs, it takes approximately one hour for the application inventory to appear in the Azure Migrate portal.

Verify VMs in the portal

After discovery, you can verify that the VMs appear in the Azure portal:

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers > Azure Migrate: Server Assessment**, select the icon that displays the count for **Discovered servers**.

Set up an assessment

You can create two types of assessments by using Azure Migrate Server Assessment:

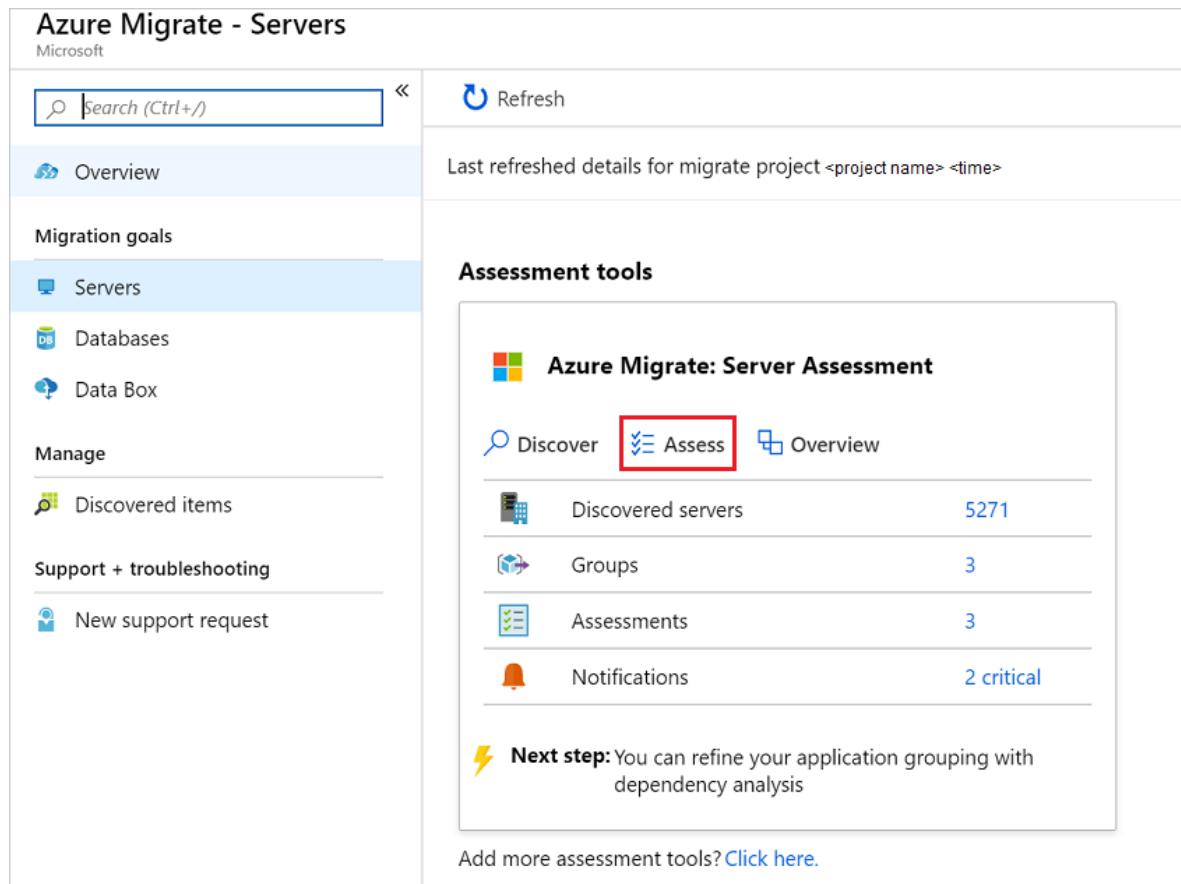
ASSESSMENT	DETAILS	DATA
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.

ASSESSMENT	DETAILS	DATA
As on-premises	Assessments based on on-premises sizing	<p>Recommended VM size: Based on the on-premises VM size.</p> <p>Recommended disk type: Based on the storage type setting that you select for the assessment.</p>

Run an assessment

Run an assessment as follows:

1. Review the [best practices](#) for creating assessments.
2. On the **Servers** tab, in the Azure Migrate: Server Assessment tile, select **Assess**.



The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with links like Overview, Migration goals (Servers selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has a search bar at the top. Below it, there's a summary message: "Last refreshed details for migrate project <project name> <time>". Under "Assessment tools", there's a box titled "Azure Migrate: Server Assessment" containing four items: Discover, Assess (which is highlighted with a red box), and Overview. Below this are statistics: 5271 Discovered servers, 3 Groups, 3 Assessments, and 2 critical Notifications. At the bottom of the box, there's a note: "Next step: You can refine your application grouping with dependency analysis". At the very bottom of the dashboard, it says "Add more assessment tools? Click here."

3. In **Assess servers**, specify a name for the assessment.
4. Select **View all**, and then review the assessment properties.

Assessment properties



You can also edit these properties later by opening the **assessment** and clicking on '**Edit properties**' command on top

TARGET PROPERTIES

Target location

North Europe

Storage type

Automatic

Reserved instances

3 years reserved

VM SIZE

Sizing criterion

Performance-based

Performance history

1 Day

Percentile utilization

95th

Save

Discard

5. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more VMs together for assessment.
6. In **Add machines to the group**, select VMs to add to the group.
7. Select **Create Assessment** to create the group and run the assessment.

Assess servers

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

* Assessment name

Enter the assessment...

Assessment properties

(Showing 3 of 13)

[View all](#)

Migration target location : North Europe

Sizing criterion : Performance-based

Reserved instances : 3 years reserved

Select or create a group

Create New Use Existing

Enter the group name

Add machines to the group

 [How to create groups using dependency visualization](#)

Select all Clear selection

Search to filter machines

< Previous

Page 1 of 586

[Next >](#)

NAME

IP ADDRESS

OPERATING SYSTEM

51H8TestVM-17

[Create assessment](#)

8. After the assessment is created, view it in **Servers > Azure Migrate: Server Assessment > Assessments**.

9. Select **Export assessment** to download it as an Excel file.

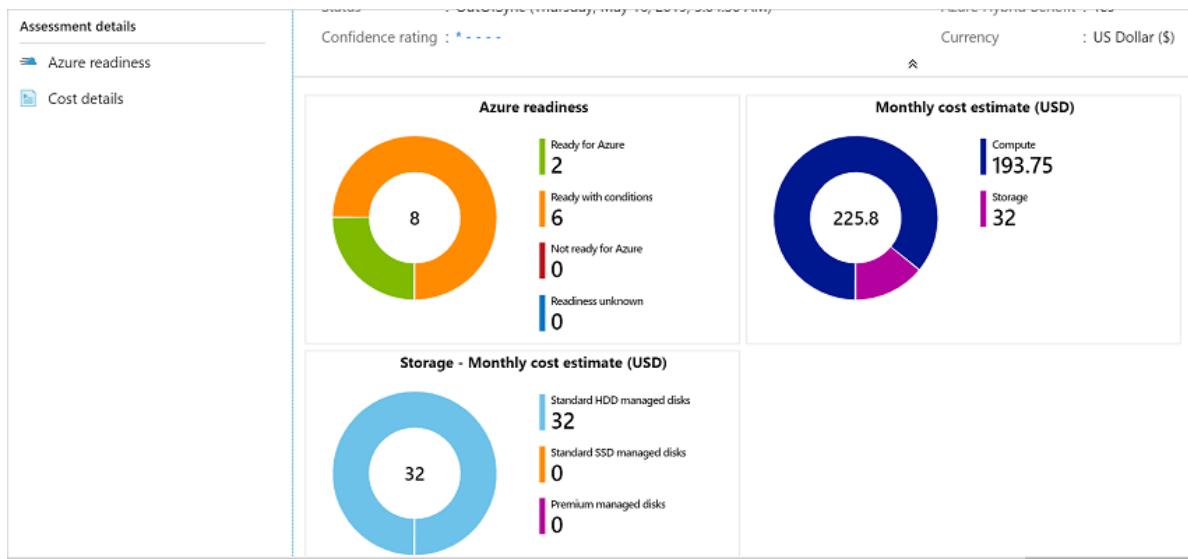
Review an assessment

An assessment describes:

- **Azure readiness:** Whether VMs are suitable for migration to Azure.
- **Monthly cost estimation:** The estimated monthly compute and storage costs for running the VMs in Azure.
- **Monthly storage cost estimation:** Estimated costs for disk storage after migration.

To view an assessment:

1. In **Migration goals > Servers**, select **Assessments** in **Azure Migrate: Server Assessment**.
2. In **Assessments**, select an assessment to open it.



Review Azure readiness

1. In **Azure readiness**, verify whether VMs are ready for migration to Azure.
2. Review the VM status:
 - **Ready for Azure**: Used when Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
 - **Ready with conditions**: Shows issues and suggested remediation.
 - **Not ready for Azure**: Shows issues and suggested remediation.
 - **Readiness unknown**: Used when Azure Migrate can't assess readiness because of data availability issues.
3. Select an **Azure readiness** status. You can view VM readiness details. You can also drill down to see VM details, including compute, storage, and network settings.

Review cost details

The assessment summary shows the estimated compute and storage cost of running VMs in Azure. Costs are aggregated for all VMs in the assessed group. You can drill down to see cost details for specific VMs.

NOTE

Cost estimates are based on the size recommendations for a machine, its disks, and its properties. Estimates are for running the on-premises VMs as IaaS VMs. Azure Migrate Server Assessment doesn't consider PaaS or SaaS costs.

The aggregated storage costs for the assessed group are split over different types of storage disks.

Review confidence rating

Azure Migrate Server Assessment assigns a confidence rating to a performance-based assessment, from 1 star (lowest) to 5 stars (highest).

NAME	GROUP	STATUS	MACHINES	LOCATION	SIZING CRITERION	CONFIDENCE RATING
<input type="button" value="Search to filter assessments"/>						
assessment_5_16_2019_17_34_29	day2	OutOfSync	0	North Europe	Performance-based	★★★★★
assessment_5_20_2019_17_42_6	Mygroup	Ready	6	North Europe	Performance-based	★★★★★
assessment_5_22_2019_22_56_13	Day2-group	OutDated	14	North Europe	Performance-based	★★★★★

The confidence rating helps you estimate the reliability of the assessment's size recommendations. The rating is based on the availability of data points needed to compute the assessment:

DATA POINT AVAILABILITY	CONFIDENCE RATING
0%-20%	1 star
21%-40%	2 stars
41%-60%	3 stars
61%-80%	4 stars
81%-100%	5 stars

[Learn about best practices for confidence ratings.](#)

Next steps

In this tutorial, you set up an Azure Migrate appliance. You also created and reviewed an assessment.

To learn how to migrate VMware VMs to Azure by using Azure Migrate Server Migration, continue to the third tutorial in the series:

[Migrate VMware VMs](#)

You can migrate VMware VMs to Azure using the Azure Migrate Server Migration tool. This tool offers a couple of options for VMware VM migration:

- Migration using agentless replication. Migrate VMs without needing to install anything on them.
- Migration with an agent for replication. Install an agent on the VM for replication.

Compare migration methods

Use these selected comparisons to help you decide which method to use. You can also review full support requirements for [agentless](#) and [agent-based](#) migration.

SETTING	AGENTLESS	AGENT-BASED
Azure permissions	You need permissions to create an Azure Migrate project, and to register Azure AD apps created when you deploy the Azure Migrate appliance.	You need Contributor permissions on the Azure subscription.
Simultaneous replication	A maximum of 100 VMs can be simultaneously replicated from a vCenter Server. If you have more than 50 VMs for migration, create multiple batches of VMs. Replicating more at a single time will impact performance.	NA
Appliance deployment	The Azure Migrate appliance is deployed on-premises.	The Azure Migrate Replication appliance is deployed on-premises.
Site Recovery compatibility	Compatible.	You can't replicate with Azure Migrate Server Migration if you've set up replication for a machine using Site Recovery.
Target disk	Managed disks	Managed disks
Disk limits	OS disk: 2 TB Data disk: 4 TB Maximum disks: 60	OS disk: 2 TB Data disk: 8 TB Maximum disks: 63
Passthrough disks	Not supported	Supported

SETTING	AGENTLESS	AGENT-BASED
UEFI boot	Not supported	The migrated VM in Azure will be automatically converted to a BIOS boot VM. The OS disk should have up to four partitions, and volumes should be formatted with NTFS.

Deployment steps comparison

After reviewing the limitations, understanding the steps involved in deploying each solution might help you decide which option to choose.

TASK	DETAILS	AGENTLESS	AGENT-BASED
Assessment	<p>Assess servers before migration. Assessment is optional. We suggest that you assess machines before you migrate them, but you don't have to.</p> <p>For assessment, Azure Migrate sets up a lightweight appliance to discover and assess VMs.</p>	If you run an agentless migration after assessment, the same Azure Migrate appliance set up for assessment is used for agentless migration.	If you run an agent-based migration after assessment, the appliance set up for assessment isn't used during agentless migration. You can leave the appliance in place, or remove it if you don't want to do further discovery and assessment.
Prepare VMware servers and VMs for migration	Configure a number of settings on VMware servers and VMs.	Required	Required
Add the Server Migration tool	Add the Azure Migrate Server Migration tool in the Azure Migrate project.	Required	Required
Deploy the Azure Migrate appliance	Set up a lightweight appliance on a VMware VM for VM discovery and assessment.	Required	Not required.
Install the Mobility service on VMs	Install the Mobility service on each VM you want to replicate	Not required	Required
Deploy the Azure Migrate Server Migration replication appliance	Set up an appliance on a VMware VM to discover VMs, and bridge between the Mobility service running on VMs and Azure Migrate Server Migration	Not required	Required
Replicate VMs. Enable VM replication.	Configure replication settings and select VMs to replicate	Required	Required

Task	Details	Agentless	Agent-based
Run a test migration	Run a test migration to make sure everything's working as expected.	Required	Required
Run a full migration	Migrate the VMs.	Required	Required

Next steps

[Migrate VMware VMs](#) with agentless migration.

Migrate VMware VMs to Azure (agentless)

3/4/2020 • 12 minutes to read • [Edit Online](#)

This article shows you how to migrate on-premises VMware VMs to Azure, using agentless migration with the Azure Migrate Server Migration tool.

[Azure Migrate](#) provides a central hub to track discovery, assessment and migration of your on-premises apps and workloads, and AWS/GCP VM instances, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

This tutorial is the third in a series that demonstrates how to assess and migrate VMware VMs to Azure using Azure Migrate Server Assessment and Migration. In this tutorial, you learn how to:

- Prepare VMs for migration.
- Add the Azure Migration Server Migration tool.
- Discover VMs you want to migrate.
- Start replicating VMs.
- Run a test migration to make sure everything's working as expected.
- Run a full VM migration.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Migration methods

You can migrate VMware VMs to Azure using the Azure Migrate Server Migration tool. This tool offers a couple of options for VMware VM migration:

- Migration using agentless replication. Migrate VMs without needing to install anything on them.
- Migration with an agent for replication. Install an agent on the VM for replication.

To decide whether you want to use agentless or agent-based migration, review these articles:

- [Learn how](#) agentless migration works, and [compare migration methods](#).
- [Read this article](#) if you want to use the agent-based method.

Prerequisites

Before you begin this tutorial, you should:

1. [Complete the first tutorial](#) in this series to set up Azure and VMware for migration. Specifically, in this tutorial you need to:
 - [Prepare Azure](#) for migration.
 - [Prepare the on-premises environment](#) for migration.
2. We recommend that you try assessing VMware VMs with Azure Migrate Server Assessment before migrating them to Azure. To set up assessment, [complete the second tutorial](#) in this series. If you don't want to assess VMs you can skip this tutorial. Although we recommend that you try out an assessment, but you don't have to run an assessment before you try a migration.

Add the Azure Migrate Server Migration tool

If you didn't follow the second tutorial to assess VMware VMs, you need to [follow these instructions](#) set up an

Azure Migrate project, and select the Azure Migrate Server Migration tool.

If you followed the second tutorial and already have an Azure Migrate project set up, add the Azure Migrate Server Migration tool as follows:

1. In the Azure Migrate project, click **Overview**.
2. In **Discover, assess, and migration servers**, click **Assess and migrate servers**.

The screenshot shows the Azure Migrate Overview page. On the left, there's a sidebar with links like 'Overview', 'Migration goals', 'Manage', and 'Support + troubleshooting'. The main area has a heading 'Migrate your on-premises datacenter to Azure' and a sub-section 'Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or find an expert to help with your migration. Learn more'. Below this are three cards: 'Assess and migrate web apps to Azure', 'Discover, assess and migrate databases', and 'Discover, assess and migrate servers'. The 'Discover, assess and migrate servers' card is highlighted with a red box around its title and 'Assess and migrate servers' button. A magnifying glass icon is shown above the rocket ship icon in the server migration card.

3. In **Migration tools**, select **Click here to add a migration tool when you are ready to migrate**.

The screenshot shows the 'Assessment tools' page under the 'Azure Migrate' project. It features two main sections: 'Azure Migrate: Server Assessment' and 'Cloudamize'. The 'Azure Migrate: Server Assessment' section includes a 'Quick start' guide with steps 1: Discover and 2: Assess. The 'Cloudamize' section includes a 'Quick start' guide with steps 1: Register and 2: Connect. At the bottom, there's a note 'Add more assessment tools? Click here.' and a 'Migration tools' section with a note 'You do not have any migration tools yet. Click here to add a migration tool when you are ready to migrate.' A red box highlights the 'Click here' link in the migration tools section.

4. In the tools list, select **Azure Migrate: Server Migration > Add tool**

The screenshot shows the 'Tools' list page under the 'Azure Migrate' project. It lists various migration tools with their details. The 'Azure Migrate: Server Migration' tool is selected and highlighted with a red box. The table columns include TOOL, PRICING, SUPPORTED WORKLOADS, FEATURES, and LEARN MORE. The 'Azure Migrate: Server Migration' row shows it supports VMware virtual machines, Hyper-V virtual machines, Physical machines, and Migration from other public clouds. It also supports Windows and Linux, Agentless and agent-based migration, Cutover in seconds, and Minimal application downtime. A 'View' link is provided for more details.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
Azure Migrate: Server Migration	View	VMware virtual machines Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless and agent-based migration Cutover in seconds Minimal application downtime	Learn more

Set up the Azure Migrate appliance

Azure Migrate Server Migration runs a lightweight VMware VM appliance. The appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate Server Migration. The same appliance is also

used by the Azure Migrate Server Assessment tool.

If you followed the second tutorial to assess VMware VMs, you already set up the appliance during that tutorial. If you didn't follow that tutorial, you need to set up the appliance now. To do this, you:

- Download an OVA template file, and import it to vCenter Server.
- Create the appliance, and check that it can connect to Azure Migrate Server Assessment.
- Configure the appliance for the first time, and register it with the Azure Migrate project.

Follow the instructions in [this article](#) to set up the appliance.

Prepare VMs for migration

Azure Migrate requires some VM changes to ensure that VMs can be migrated to Azure.

- For some operating systems, Azure Migrate makes these changes automatically. [Learn more](#)
- If you're migrating a VM that doesn't have one of these operating systems, follow the instructions to prepare the VM.
- It's important to make these changes before you begin migration. If you migrate the VM before you make the change, the VM might not boot up in Azure.
- Configuration changes you make on on-premises VMs are replicated to Azure after replication for the VM is enabled. To ensure that changes are replicated, make sure that the recovery point you migrate to is later than the time at which the configuration changes were made on-premises.

Prepare Windows Server VMs

ACTION	DETAILS	INSTRUCTIONS
Ensure that Windows volumes in Azure VM use the same drive letter assignments as the on-premises VM.	Configure the SAN policy as Online All.	<ol style="list-style-type: none">1. Sign in to the VM with an admin account, and open a command window.2. Type <code>diskpart</code> to run the Diskpart utility.3. Type <code>SAN POLICY=OnlineAll</code>4. Type <code>Exit</code> to leave Diskpart, and close the command prompt.
Enable Azure serial access console for the Azure VM	This helps with troubleshooting. You don't need to reboot the VM. The Azure VM will boot using the disk image, and this is equivalent to a reboot for the new VM.	Follow these instructions to enable.
Install Hyper-V Guest Integration	If you're migrating machines running Windows Server 2003, install Hyper-V Guest Integration Services on the VM operating system.	Learn more .
Remote Desktop	Enable Remote Desktop on the VM, and check that the Windows Firewall isn't blocking Remote Desktop access on any network profiles.	Learn more .

Prepare Linux VMs

ACTION	DETAILS

ACTION	DETAILS
Install Hyper-V Linux Integration Services	Most new versions of Linux distributions have this included by default.
Rebuild the Linux init image to contain the necessary Hyper-V drivers	This ensures that the VM will boot in Azure, and is only required on some distributions.
Enable Azure serial console logging	This helps with troubleshooting. You don't need to reboot the VM. The Azure VM will boot using the disk image, and this is equivalent to a reboot for the new VM. Follow these instructions to enable.
Update device map file	Update the device map file that has the device name to volume associations, to use persistent device identifiers
Update fstab entries	Update entries to use persistent volume identifiers.
Remove udev rule	Remove any udev rules that reserves interface names based on mac address etc.
Update network interfaces	Update network interfaces to receive IP address based on DHCP.
Enable ssh	Ensure ssh is enabled and the sshd service is set to start automatically on reboot. Ensure that incoming ssh connection requests are not blocked by the OS firewall or scriptable rules.

[Follow this article](#) that discusses these steps for running a Linux VM on Azure, and include instructions for some of the popular Linux distributions.

Replicate VMs

With discovery completed, you can begin replication of VMware VMs to Azure.

NOTE

You can replicate up to 10 machines together. If you need to replicate more, then replicate them simultaneously in batches of 10. For agentless migration you can run up to 100 simultaneous replications.

1. In the Azure Migrate project > **Servers**, **Azure Migrate: Server Migration**, click **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with links like Overview, Migration goals, Servers (which is selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has a header "Azure Migrate - Servers" and "Microsoft". It includes a search bar, a refresh button, and a note about the last refresh at 7/8/2019, 11:08:58 AM. Below this is the "Assessment tools" section, which contains a box titled "Azure Migrate: Server Assessment" with tabs for Discover, Assess, and Overview. Under "Discover", it shows 442 Discovered servers, 2 Groups, 2 Assessments, and 0 Notifications. A yellow lightning bolt icon with the text "Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis" is present. At the bottom of the assessment box, there's a link "Add more assessment tools? Click here." To the right of the assessment box is the "Migration tools" section, which contains a box titled "Azure Migrate: Server Migration" with tabs for Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. Under "Discover", it shows 442 Discovered servers.

2. In Replicate, > Source settings > Are your machines virtualized?, select Yes, with VMware vSphere.
3. In On-premises appliance, select the name of the Azure Migrate appliance that you set up > OK.

The screenshot shows the "Replicate" configuration page. At the top, there's a title "Replicate" and a navigation bar with tabs: Source settings (which is selected and underlined), Virtual machines, Target settings, Compute, Disks, and Review + Start replication. Below the tabs, a note says "The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure." There are two required fields with dropdown menus:

- * Are your machines virtualized?
- * On-premises appliance

- This step presumes that you have already set up an appliance when you completed the tutorial.
 - If you haven't set up an appliance, then follow the instructions in [this article](#).
4. In Virtual machines, select the machines you want to replicate.
 - If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in Import migration settings from an

Azure Migrate assessment?, select the Yes option.

- If you didn't run an assessment, or you don't want to use the assessment settings, select the No options.
- If you selected to use the assessment, select the VM group, and assessment name.

Select the virtual machines to be migrated.

* Import migration settings from an assessment? i

Select

Yes, apply migration settings from a Azure Migrate assessment

No, I'll specify the migration settings manually

5. In **Virtual machines**, search for VMs as needed, and check each VM you want to migrate. Then click **Next: Target settings**.

Select the virtual machines to be migrated.

* Import migration settings from an assessment? i

No, I'll specify the migration settings manually

* Virtual machines i

Search to filter machines

< Previous Page 1 Next >

NAME	IP ADDRESS	OPERATING SYSTEM	BOOT TYPE
<input checked="" type="checkbox"/> ContosoVMwareMigr...	2404:f801:4800:25:c95f:5fd3:7347:4f91,1...	Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoCSASR	2404:f801:4800:25:29f9:2ebd:1ee0:eeb4,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-FrontTier3		Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoWeb1	2404:f801:4800:25:9091:9912:5f46:9108,...	Microsoft Windows Server 2008 (32-bit)	bios
<input checked="" type="checkbox"/> Contoso-Configuratio...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-AzureMigrat...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb3	10.150.13.218,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoAppSrv2	2404:f801:4800:25:5de5:e919:3448:be33,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb2	10.150.13.201,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios

Selected items : 9

6. In **Target settings**, select the subscription, and target region to which you'll migrate, and specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.

7. In **Azure Hybrid Benefit**:

- Select **No** if you don't want to apply Azure Hybrid Benefit. Then click **Next**.
- Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

Replicate

Source settings Virtual machines **Target settings** Compute Disks Review + Start replication

Select target properties for migration. Migrated machines will be created with the specified properties.

* Region (US) East US

* Subscription Azure Migrate Program Management Team

* Resource group ContosoDemoRG

* Virtual Network ContosoDemoNW

* Subnet default

Azure Hybrid Benefit

Apply Azure Hybrid Benefit and save up to 49% vs. pay-as-you-go virtual machine costs with an eligible Windows Server license.

* Already have an eligible Windows Server License? **No**

8. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).

- **VM size:** If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in [Azure VM size](#).
- **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
- **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

Replicate

Source settings Virtual machines Target settings **Compute** Disks Review + Start replication

Select the Azure VM size and OS disk for the machines that are being migrated. Additionally, select an Availability Set if the migrated machine should be part of one. The OS disk is the disk that contains the operating system.

NAME	AZURE VM NAME	SOURCE VM SIZE	AZURE VM SIZE
ContosoVMwareMigration2	ContosoVMwareMigration2	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoCSASR	ContosoCSASR	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-FrontTier3	Contoso-FrontTier3	8 Cores, 16384 MB RAM	Automatically select matching configuration
ContosoWeb1	ContosoWeb1	2 Cores, 2048 MB RAM	Automatically select matching configuration
Contoso-ConfigurationServer	Contoso-ConfigurationServer	8 Cores, 16384 MB RAM	Automatically select matching configuration
Contoso-AzureMigrateAppliance	Contoso2	4 Cores, 8192 MB RAM	Automatically select matching configuration
ContosoWeb3	ContosoWeb3	2 Cores, 2048 MB RAM	Automatically select matching configuration
ContosoAppSrv2	ContosoAppSrv2	2 Cores, 4096 MB RAM	Automatically select matching configuration
ContosoWeb2	ContosoWeb2	2 Cores, 2048 MB RAM	Automatically select matching configuration

9. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then click **Next**.

- You can exclude disks from replication.
- If you exclude disks, won't be present on the Azure VM after migration.

Replicate		
Source settings	Virtual machines	Target settings
Compute	Disks	Review + Start replication
Select the managed disk type to use for the disks of the migrated machine. Optionally, you may also choose to exclude certain disks from replication by unselecting those disks from the list of disks to replicate.		
NAME	DISKS TO REPLICATE	DISK SIZE GB
ContosoVMwareMigration2	All selected scsi0:0	80 80
ContosoCSASR	All selected scsi0:0	80 80
Contoso-FrontTier3	All selected scsi0:0	80 80
ContosoWeb1	All selected scsi0:0	40 40

10. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

NOTE

You can update replication settings any time before replication starts, in **Manage > Replicating machines**. Settings can't be changed after replication starts.

Provisioning for the first time

If this is the first VM you're replicating in the Azure Migrate project, Azure Migrate Server Migration automatically provisions these resources in same resource group as the project.

- **Service bus:** Azure Migrate Server Migration uses the service bus to send replication orchestration messages to the appliance.
- **Gateway storage account:** Server Migration uses the gateway storage account to store state information about the VMs being replicated.
- **Log storage account:** The Azure Migrate appliance uploads replication logs for VMs to a log storage account. Azure Migrate applies the replication information to the replica managed disks.
- **Key vault:** The Azure Migrate appliance uses the key vault to manage connection strings for the service bus, and access keys for the storage accounts used in replication. You should have set up the permissions that the key vault needs to access the storage account when you prepared. [Review these permissions](#).

Track and monitor

- When you click **Replicate** a Start Replication job begins.
- When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.
- During initial replication, a VM snapshot is created. Disk data from the snapshot is replicated to replica managed disks in Azure.
- After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to the replica disks in Azure.

You can track job status in the portal notifications.

You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.

Migration tools

Azure Migrate: Server Migration

+ Discover Replicate Migrate Overview

Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

⚡ **Next step:** You can start migrating the replicating servers to Azure

Run a test migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

- Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating.
- Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production VNet in your Azure subscription).
- You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

Do a test migration as follows:

1. In Migration goals > Servers > Azure Migrate: Server Migration, click Test migrated servers.

Migration tools

Azure Migrate: Server Migration

Discover Replicate Migrate Overview

Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

⚡ **Next step:** You can start migrating the replicating servers to Azure

2. Right-click the VM to test, and click **Test migrate**.

The screenshot shows the Azure Migrate: Server Migration - Replicating machines dashboard. On the left, there's a navigation menu with options like Overview, Getting started, Migrate servers to Azure, Manage, Replicating machines, Jobs, Events, Settings, and Properties. The 'Replicating machines' option is selected. The main area displays a table with columns: NAME, STATUS, HEALTH, MIGRATION PHASE, LAST SYNC, and TEST MIGRATION STATUS. One row is shown for 'Contoso-Win2K8R2SP1' with the status 'Delta sync', health 'Healthy', migration phase 'Test migration pending', last sync '2/17/2019, 12:00:43 AM', and test migration status 'Never performed'. A context menu is open for this row, with items: Pin to dashboard, Test migrate (highlighted with a red box), Clean up test migration, Migrate, and Error Details.

3. In **Test Migration**, select the Azure VNet in which the Azure VM will be located after the migration. We recommend you use a non-production VNet.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

This screenshot is similar to the one above, but the context menu for the 'Contoso-Win2K8R2SP1' row now includes an additional item: 'Clean up test migration' (highlighted with a red box). The other items in the menu are 'Pin to dashboard', 'Test migrate', 'Migrate', and 'Error Details'.

Migrate VMs

After you've verified that the test migration works as expected, you can migrate the on-premises machines.

1. In the Azure Migrate project > Servers > Azure Migrate: Server Migration, click **Replicating servers**.

The screenshot shows the Azure Migrate: Server Migration - Replicating servers dashboard. At the top, there's a title 'Migration tools' and a section for 'Azure Migrate: Server Migration' with links for Discover, Replicate, Migrate, and Overview. Below this, there's a summary table with four rows: 'Discovered servers' (1), 'Replicating servers' (1, highlighted with a red box), 'Test migrated servers' (0), and 'Migrated servers' (0). A note at the bottom says: 'Next step: You can start migrating the replicating servers to Azure'.

2. In **Replicating machines**, right-click the VM > **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**.
 - By default Azure Migrate shuts down the on-premises VM, and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This ensures no data loss.
 - If you don't want to shut down the VM, select **No**
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

Complete the migration

1. After the migration is done, right-click the VM > **Stop Replication**. This stops replication for the on-premises machine, and cleans up replication state information for the VM.
2. Install the Azure VM [Windows](#) or [Linux](#) agent on the migrated machines.
3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

Post-migration best practices

- For increased resilience:
 - Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](#).
 - Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery. [Learn more](#).
- For increased security:
 - Lock down and limit inbound traffic access with [Azure Security Center - Just in time administration](#).
 - Restrict network traffic to management endpoints with [Network Security Groups](#).
 - Deploy [Azure Disk Encryption](#) to help secure disks, and keep data safe from theft and unauthorized access.
 - Read more about [securing IaaS resources](#), and visit the [Azure Security Center](#).
- For monitoring and management:
- Consider deploying [Azure Cost Management](#) to monitor resource usage and spending.

Next steps

Investigate the [cloud migration journey](#) in the Azure Cloud Adoption Framework.

Migrate VMware VMs to Azure (agent-based)

3/10/2020 • 19 minutes to read • [Edit Online](#)

This article shows you how to migrate on-premises VMware VMs to Azure, using agent-based migration with the Azure Migrate Server Migration tool.

[Azure Migrate](#) provides a central hub to track discovery, assessment and migration of your on-premises apps and workloads, and AWS/GCP VM instances, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

In this tutorial, you learn how to:

- Set up the source environment, and deploy an Azure Migrate replication appliance for agent-based migration.
- Set up the target environment for migration.
- Set up a replication policy.
- Enable replication.
- Run a test migration to make sure everything's working as expected.
- Run a full migration to Azure.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-tos for VMware assessment and migration.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Before you begin

We recommend that you try out VMware VM assessment with Azure Migrate Server Assessment, before you migrate VMs to Azure. Set up an assessment as follows:

1. Follow the tutorial to [prepare Azure and VMware](#) for assessment.
2. Then, follow [this tutorial](#) to set up an Azure Migrate appliance for assessment, and discover and assess VMs.

Although we recommend that you try out an assessment, you don't have to run an assessment before you migrate VMs.

Migration methods

You can migrate VMware VMs to Azure using the Azure Migrate Server Migration tool. This tool offers a couple of options for VMware VM migration:

- Agentless replication. Migrate VMs without needing to install anything on them.
- Agent-based migration. or replication. Install an agent (the Mobility services agent) on the VM for replication.

To decide whether you want to use agentless or agent-based migration, review these articles:

- [Learn about](#) the VMware migration options.
- [Compare migration methods](#).
- [Follow this article](#) to try out agentless migration.

Prerequisites

Before you begin this tutorial, you should:

1. [Review](#) the VMware migration architecture.
2. Make sure that your Azure account is assigned the Virtual Machine Contributor role, so that you have permissions to:
 - Create a VM in the selected resource group.
 - Create a VM in the selected virtual network.
 - Write to an Azure managed disk.
3. [Set up an Azure network](#). On-premises machines are replicated to Azure managed disks. When you fail over to Azure for migration, Azure VMs are created from these managed disks, and joined to an Azure network you specify when you set up migration.

Prepare Azure

If you have already run an assessment with Azure Migrate Server Assessment, you can skip the instructions in this section since you've already completed these steps.

If you haven't run an assessment, you need to set up Azure permissions before you can migrate with Azure Migrate Server Migration.

- **Create a project:** Your Azure account needs permissions to create an Azure Migrate project.
- **Register the Azure Migrate replication appliance:** The replication appliance creates and registers an Azure Active Directory app in your Azure account. You need to delegate permissions for this.
- **Create Key Vault:** To migrate VMware VMs using Azure Migrate Server Migration, Azure Migrate creates a Key Vault in the resource group, to manage access keys to the replication storage account in your subscription. To create the vault, you need role assignment permissions on the resource group in which the Azure Migrate project resides.

Assign permissions to create project

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Assign permissions to register the replication appliance

For agent-based migration, delegate permissions for Azure Migrate Server Migration to create and register an Azure AD app in your account. You can assign permissions using one of the following methods:

- A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
- A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.

It's worth noting that:

- The apps don't have any other access permissions on the subscription other than those described above.
- You only need these permissions when you register a new replication appliance. You can remove the permissions after the replication appliance is set up.

Grant account permissions

The tenant/global admin can grant permissions as follows

1. In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User**

Settings.

2. The admin should set App registrations to Yes.

The screenshot shows the 'User settings' page in the Microsoft Azure Active Directory. The 'User settings' tab is active. In the 'App registrations' section, there is a button labeled 'Users can register applications' with two options: 'Yes' and 'No'. The 'Yes' button is highlighted with a red box. Other sections visible include 'Administration portal', 'LinkedIn account connections' (with a note about connecting work or school accounts), 'External users', and 'Access panel'.

NOTE

This is a default setting that isn't sensitive. [Learn more.](#)

Assign Application Developer role

The tenant/global admin can assign the Application Developer role to an account. [Learn more.](#)

Assign permissions to create Key Vault

Assign role assignment permissions on the resource group in which the Azure Migrate project resides, as follows:

1. In the resource group in the Azure portal, select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions. You need **Owner** (or **Contributor** and **User Access Administrator**) permissions.
3. If you don't have the required permissions, request them from the resource group owner.

Prepare on-premises VMware

Prepare an account for automatic discovery

Azure Migrate Server Migration needs access to VMware servers to:

- Automatically discover VMs. At least a read-only account is required.
- Orchestrate replication, failover, and fallback. You need an account that can run operations such as creating and removing disks, and powering on VMs.

Create the account as follows:

1. To use a dedicated account, create a role at the vCenter level. Give the role a name such as

Azure_Site_Recovery.

2. Assign the role the permissions summarized in the table below.
3. Create a user on the vCenter server or vSphere host. Assign the role to the user.

VMware account permissions

TASK	ROLE/PERMISSIONS	DETAILS
VM discovery	<p>At least a read-only user</p> <p>Data Center object -> Propagate to Child Object, role=Read-only</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p>
Full replication, failover, fallback	<p>Create a role (Azure_Site_Recovery) with the required permissions, and then assign the role to a VMware user or group</p> <p>Data Center object -> Propagate to Child Object, role=Azure_Site_Recovery</p> <p>Datastore -> Allocate space, browse datastore, low-level file operations, remove file, update virtual machine files</p> <p>Network -> Network assign</p> <p>Resource -> Assign VM to resource pool, migrate powered off VM, migrate powered on VM</p> <p>Tasks -> Create task, update task</p> <p>Virtual machine -> Configuration</p> <p>Virtual machine -> Interact -> answer question, device connection, configure CD media, configure floppy media, power off, power on, VMware tools install</p> <p>Virtual machine -> Inventory -> Create, register, unregister</p> <p>Virtual machine -> Provisioning -> Allow virtual machine download, allow virtual machine files upload</p> <p>Virtual machine -> Snapshots -> Remove snapshots</p>	<p>User assigned at datacenter level, and has access to all the objects in the datacenter.</p> <p>To restrict access, assign the No access role with the Propagate to child object, to the child objects (vSphere hosts, datastores, VMs and networks).</p>

Prepare an account for Mobility service installation

The Mobility service must be installed on machines you want to replicate.

- The Azure Migrate replication appliance can do a push installation of this service when you enable replication for a machine, or you can install it manually, or using installation tools.
- In this tutorial, we're going to install the Mobility service with the push installation.

- For push installation, you need to prepare an account that Azure Migrate Server Migration can use to access the VM. This account is used only for the push installation, if you don't install the Mobility service manually.

Prepare the account as follows:

- Prepare a domain or local account with permissions to install on the VM.
- For Windows VMs, if you're not using a domain account, disable Remote User Access control on the local machine by adding the DWORD entry **LocalAccountTokenFilterPolicy**, with a value of 0 in the registry, under **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
- For Linux VMs, prepare a root account on the source Linux server.

Check VMware requirements

Make sure VMware servers and VMs comply with requirements for migration to Azure.

NOTE

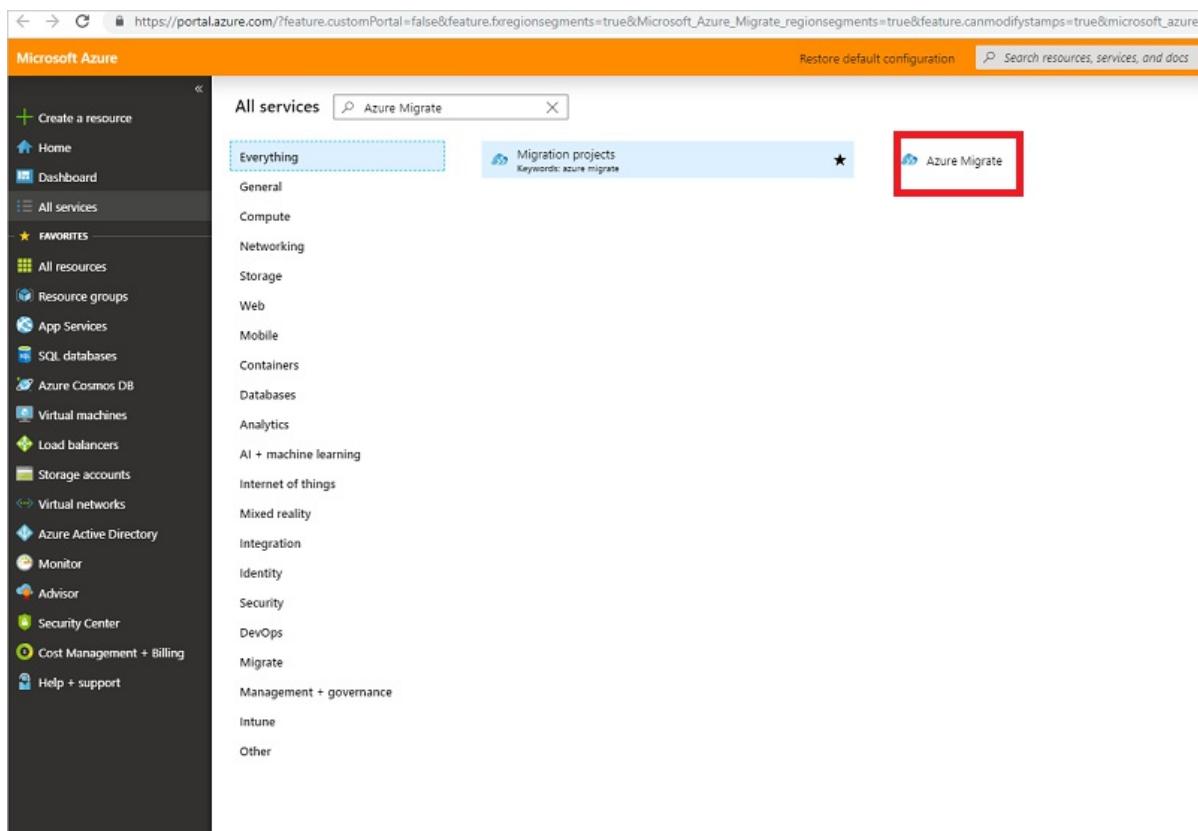
Agent-based migration with Azure Migrate Server Migration is based on features of the Azure Site Recovery service. Some requirements might link to Site Recovery documentation.

- [Verify](#) VMware server requirements.
- [Verify](#) VM support requirements for migration.
- Verify VM settings. On-premises VMs you replicate to Azure must comply with [Azure VM requirements](#).

Add the Azure Migrate Server Migration tool

If you didn't follow the tutorial to assess VMware VMs, set up an Azure Migrate project, and then add the Azure Migrate Server Migration tool:

- In the Azure portal > **All services**, search for **Azure Migrate**.
- Under **Services**, select **Azure Migrate**.



3. In Overview, click **Assess and migrate servers**.
4. Under Discover, assess and migrate servers, click **Assess and migrate servers**.

The screenshot shows the Azure Migrate service interface. On the left, there's a sidebar with options like Overview, Migration goals, Manage, and Support + troubleshooting. The main area has a heading "Migrate your on-premises datacenter to Azure" and two sections: "Discover, assess and migrate servers" and "Discover, assess and migrate databases". The "Discover, assess and migrate servers" section is highlighted with a red box around its title and "Assess and migrate servers" button. To the right, there are sections for "Assess and migrate web apps to Azure" and "Migrate on-premises data to Azure".

5. In Discover, assess and migrate servers, click **Add tools**.
6. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
7. In **Project Details**, specify the project name, and geography in which you want to create the project, and click **Next**

The screenshot shows the "Add a tool" page for a "Migrate project". At the top, there are tabs for "Migrate project", "Select assessment tool" (which is selected), "Select migration tool", and "Review + add tool(s)". Below these tabs, it says "A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project." There are dropdown menus for "Subscription" (set to "<subscription name>") and "Resource group" (set to "ContosoCorporation").

PROJECT DETAILS
Specify the name of the migrate project and the preferred geography.

Fields for "Migrate project" (set to "Contoso-Project") and "Geography" (set to "centraluseuap") are shown. At the bottom is a "Next" button.

You can create an Azure Migrate project in any of these geographies.

GEOGRAPHY	REGION
Asia	Southeast Asia
Europe	North Europe or West Europe

GEOGRAPHY	REGION
United States	East US or West Central US

The geography specified for the project is only used to store the metadata gathered from on-premises VMs. You can select any target region for the actual migration.

8. In **Select assessment tool**, select **Skip adding an assessment tool for now** > **Next**.
9. In **Select migration tool**, select **Azure Migrate: Server Migration** > **Next**.
10. In **Review + add tools**, review the settings and click **Add tools**
11. After adding the tool, it appears in the Azure Migrate project > **Servers** > **Migration tools**.

Set up the replication appliance

The first step of migration is to set up the replication appliance. The replication appliance is a single, highly available, on-premises VMware VM that hosts these components:

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

To set up the replication appliance, you download a prepared Open Virtualization Application (OVA) template. You import the template into VMware, and create the replication appliance VM.

Download the replication appliance template

Download the template as follows:

1. In the Azure Migrate project click **Servers** under **Migration Goals**.
2. In **Azure Migrate - Servers > Azure Migrate: Server Migration**, click **Discover**.

 Azure Migrate - Servers
Microsoft

Search (Ctrl+ /) « Refresh Last refreshed at: 6/20/2019, 8:28:41 PM (Click on "Refresh" to update the data.)

Overview Migration goals Servers Databases Data Box

Manage Discovered items

Support + troubleshooting New support request

Assessment tools

 Azure Migrate: Server Assessment

Discover Assess Overview

Quick start

1: Discover
Click 'Discover' to start discovering your on-premises machines.

2: Assess
Once your on-premises machines are discovered, click "Assess" to create assessments.

Add more assessment tools? [Click here.](#)

Migration tools

 Azure Migrate: Server Migration

Discover Replicate Migrate Overview

Quick start

1: Discover
Click 'Discover' to start discovering your on-premises machines.

2: Replicate
Once your on-premises machines are discovered, click "Replicate" to start replicating the discovered machines.

3: Migrate
Once your machines have replicated, click "Migrate" to migrate your machines.

Add more migration tools? [Click here.](#)

3. In Discover machines > Are your machines virtualized?, click Yes, with VMWare vSphere hypervisor.
4. In How do you want to migrate?, select Using agent-based replication.
5. In Target region, select the Azure region to which you want to migrate the machines.
6. Select Confirm that the target region for migration is region-name.
7. Click Create resources. This creates an Azure Site Recovery vault in the background.
 - You can't change the target region for this project after clicking this button.
 - All subsequent migrations are to this region.

Discover machines

Are your machines virtualized?  Yes, with VMware vSphere Hypervisor

How do you want to replicate?  Using agent-based replication Help me choose

Target region  (US) West US

 The target region for migration, once confirmed, cannot be changed for the project. After confirmation, the Server Migration tool (in this project) will allow replication and migration only to the selected target region.

Confirm that the target region for migration is "(US) West US"



8. In Do you want to install a new replication appliance?, select **Install a replication appliance**.
9. Click **Download**, to download the replication appliance. This downloads an OVF template that you use to create a new VMware VM that runs the appliance.

Do you want to install a new replication appliance or scale-out existing setup?

Install a replication appliance Help me choose

The replication appliance (Configuration Server) is a virtual appliance that is deployed on-premises. The replication appliance coordinates and manages replication for the servers that are being migrated. Follow the steps outlined below to set up and configure the replication appliance.

 **1. Download and deploy replication appliance**
Download the replication appliance virtual machine template and import it into your vCenter server using the Deploy OVF Template wizard.

Download .OVF file, 12GB

10. Note the name of the resource group and the Recovery Services vault. You need these during appliance deployment.

Import the template in VMware

After downloading the OVF template, you import it into VMware to create the replication application on a VMware VM running Windows Server 2016.

1. Sign in to the VMware vCenter server or vSphere ESXi host with the VMWare vSphere Client.
2. On the File menu, select **Deploy OVF Template** to start the **Deploy OVF Template Wizard**.
3. In **Select source**, enter the location of the downloaded OVF.
4. In **Review details**, select **Next**.
5. In **Select name and folder** and **Select configuration**, accept the default settings.
6. In **Select storage > Select virtual disk format**, for best performance select **Thick Provision Eager Zeroed**.
7. On the rest of the wizard pages, accept the default settings.
8. In **Ready to complete**, to set up the VM with the default settings, select **Power on after deployment > Finish**.

TIP

If you want to add an additional NIC, clear **Power on after deployment > Finish**. By default, the template contains a single NIC. You can add additional NICs after deployment.

Kick off replication appliance setup

1. From the VMWare vSphere Client console, turn on the VM.
2. The VM boots up into a Windows Server 2016 installation experience. Accept the license agreement, and enter an administrator password.
3. After the installation finishes, sign in to the VM as the administrator, using the admin password.
4. The first time you sign in, the replication appliance setup tool (Azure Site Recovery Configuration Tool) starts within a few seconds.
5. Enter a name to use for registering the appliance with Azure Migrate Server Migration. Then click **Next**.
6. The tool checks that the VM can connect to Azure. After the connection is established, select **Sign in** to sign in to your Azure subscription.
7. Wait for the tool to finish registering an Azure AD app to identify the appliance. The appliance reboots.
8. Sign in to the machine again. In a few seconds, the Configuration Server Management Wizard starts automatically.

Register the replication appliance

Finish setting up and registering the replication appliance.

1. In the Configuration Server Management Wizard, select **Setup connectivity**.
2. Select the NIC (by default there's only one NIC) that the replication appliance uses for VM discovery, and to do a push installation of the Mobility service on source machines.
3. Select the NIC that the replication appliance uses for connectivity with Azure. Then select **Save**. You cannot change this setting after it's configured.
4. If the appliance is located behind a proxy server, you need to specify proxy settings.
 - Specify the proxy name as **http://ip-address**, or **http://FQDN**. HTTPS proxy servers aren't supported.
5. When prompted for the subscription, resource groups, and vault details, add the details that you noted when you downloaded the appliance template.
6. In **Install third-party software**, accept the license agreement. Select **Download and Install** to install MySQL Server.
7. Select **Install VMware PowerCLI**. Make sure all browser windows are closed before you do this. Then select **Continue**.
8. In **Validate appliance configuration**, prerequisites are verified before you continue.
9. In **Configure vCenter Server/vSphere ESXi server**, enter the FQDN or IP address of the vCenter server, or vSphere host, where the VMs you want to replicate are located. Enter the port on which the server is listening. Enter a friendly name to be used for the VMware server in the vault.
10. Enter the credentials for the account you [created](#) for VMware discovery. Select **Add > Continue**.
11. In **Configure virtual machine credentials**, enter the credentials you [created](#) for push installation of the Mobility service, when you enable replication for VMs.
 - For Windows machines, the account needs local administrator privileges on the machines you want to replicate.
 - For Linux, provide details for the root account.
12. Select **Finalize configuration** to complete registration.

After the replication appliance is registered, Azure Migrate Server Assessment connects to VMware servers using the specified settings, and discovers VMs. You can view discovered VMs in **Manage > Discovered items**, in the

Other tab.

Replicate VMs

Now, select VMs for migration.

NOTE

You can replicate up to 10 machines together. If you need to replicate more, then replicate them simultaneously in batches of 10.

1. In the Azure Migrate project > Servers, Azure Migrate: Server Migration, click Replicate.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with options like Overview, Migration goals (Servers selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has two sections: 'Assessment tools' and 'Migration tools'. The 'Assessment tools' section contains a box for 'Azure Migrate: Server Assessment' with tabs for Discover, Assess, and Overview. It shows statistics: 442 Discovered servers, 2 Groups, 2 Assessments, and 0 Notifications. A note says: 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. Below this is a link to 'Add more assessment tools? Click here.'. The 'Migration tools' section contains a box for 'Azure Migrate: Server Migration' with tabs for Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. It shows 442 Discovered servers.

2. In Replicate, > Source settings > Are your machines virtualized?, select Yes, with VMware vSphere.
3. In On-premises appliance, select the name of the Azure Migrate appliance that you set up.
4. In vCenter server, specify the name of the vCenter server managing the VMs, or the vSphere server on which the VMs are hosted.
5. In Process Server, select the name of the replication appliance.
6. In Guest credentials, specify the VM admin account that will be used for push installation of the Mobility

service. Then click **Next: Virtual machines**.

The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.

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

* On-premises appliance ?
WIN-DVHS6VQ9TRQ (Replication Appliance)

* vCenter server/vSphere host ?
vCenter1

* Process Server ?
WIN-DVHS6VQ9TRQ

* Guest credentials ?
VM-admin-account

7. In **Virtual Machines**, select the machines that you want to replicate.

- If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.
- If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** options.
- If you selected to use the assessment, select the VM group, and assessment name.

8. Check each VM you want to migrate. Then click **Next: Target settings**.

9. In **Target settings**, select the subscription, and target region to which you'll migrate, and specify the resource group in which the Azure VMs will reside after migration.

10. In **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.

11. In **Azure Hybrid Benefit**:

- Select **No** if you don't want to apply Azure Hybrid Benefit. Then click **Next**.
- Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

12. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).

- **VM size:** If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in [Azure VM size](#).
- **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
- **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

13. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium managed disks) in Azure. Then click **Next**.

- You can exclude disks from replication.
- If you exclude disks, won't be present on the Azure VM after migration.

14. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

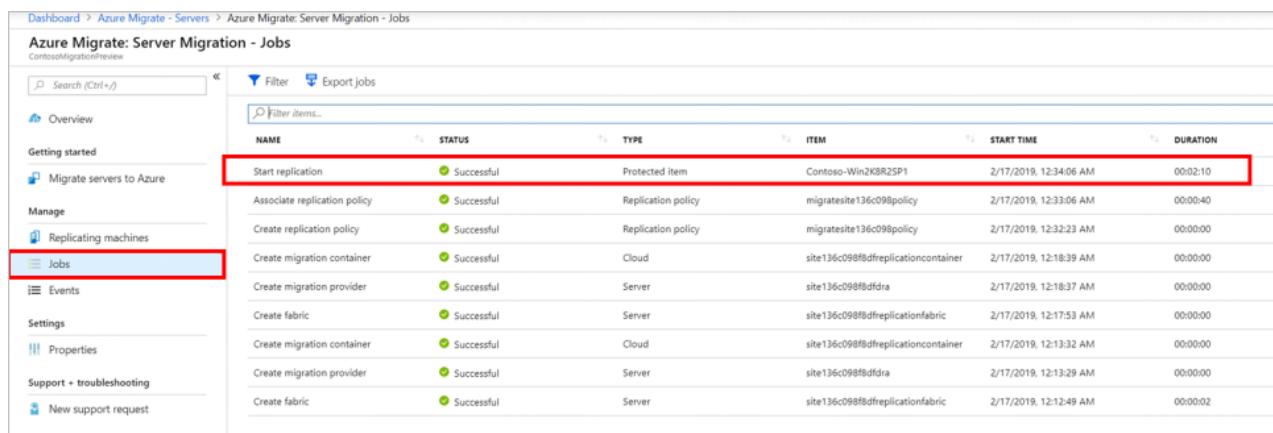
NOTE

You can update replication settings any time before replication starts, **Manage > Replicating machines**. Settings can't be changed after replication starts.

Track and monitor

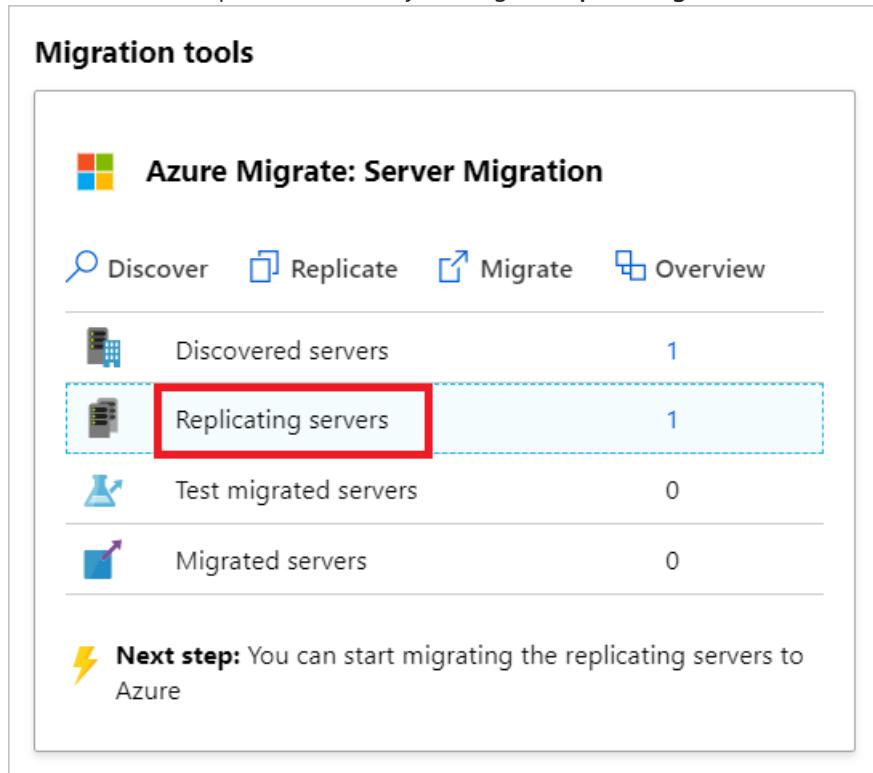
- When you click **Replicate** a Start Replication job begins.
- When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.
- After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to the replica disks in Azure.

You can track job status in the portal notifications.



NAME	STATUS	TYPE	ITEM	START TIME	DURATION
Start replication	Successful	Protected item	Contoso-Win2K8R2SP1	2/17/2019, 12:34:06 AM	00:02:10
Associate replication policy	Successful	Replication policy	migratesite136c098policy	2/17/2019, 12:33:06 AM	00:00:40
Create replication policy	Successful	Replication policy	migratesite136c098policy	2/17/2019, 12:32:23 AM	00:00:00
Create migration container	Successful	Cloud	site136c098ffddreplicationcontainer	2/17/2019, 12:18:39 AM	00:00:00
Create migration provider	Successful	Server	site136c098ffdfdra	2/17/2019, 12:18:37 AM	00:00:00
Create fabric	Successful	Server	site136c098ffddreplicationfabric	2/17/2019, 12:17:53 AM	00:00:00
Create migration container	Successful	Cloud	site136c098ffddreplicationcontainer	2/17/2019, 12:13:32 AM	00:00:00
Create migration provider	Successful	Server	site136c098ffdfdra	2/17/2019, 12:13:29 AM	00:00:00
Create fabric	Successful	Server	site136c098ffddreplicationfabric	2/17/2019, 12:12:49 AM	00:00:02

You can monitor replication status by clicking on **Replicating servers** in Azure Migrate: Server Migration.



Migration tools

Azure Migrate: Server Migration

Discover Replicate Migrate Overview

	Discovered servers	1
	Replicating servers	1
	Test migrated servers	0
	Migrated servers	0

Next step: You can start migrating the replicating servers to Azure

Run a test migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

- Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating.
- Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production VNet in your Azure subscription).
- You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

Do a test migration as follows:

1. In **Migration goals > Servers > Azure Migrate: Server Migration**, click **Test migrated servers**.

The screenshot shows the 'Azure Migrate: Server Migration' dashboard. At the top, there are four navigation tabs: 'Discover', 'Replicate', 'Migrate' (which is selected), and 'Overview'. Below the tabs, there are four categories with counts: 'Discovered servers' (442), 'Replicating servers' (6), 'Test migrated servers' (1, highlighted with a red box), and 'Migrated servers' (1). A note at the bottom says: 'Next step: You can start migrating the replicating servers to Azure'.

2. Right-click the VM to test, and click **Test migrate**.

The screenshot shows the 'Azure Migrate: Server Migration - Replicating machines' interface. On the left is a sidebar with options like 'Overview', 'Getting started', 'Migrate servers to Azure', 'Manage', 'Replicating machines' (selected), 'Jobs', 'Events', 'Settings', and 'Properties'. The main area shows a table with one row for 'Contoso-Win2K8R2SP1'. The columns are NAME, STATUS, HEALTH, MIGRATION PHASE, LAST SYNC, and TEST MIGRATION STATUS. The 'TEST MIGRATION STATUS' column has three options: 'Pin to dashboard', 'Test migrate' (highlighted with a red box), and 'Clean up test migration'. A note at the top right says: 'Last refreshed at: 2/17/2019, 12:56:13 AM'.

3. In **Test Migration**, select the Azure VNet in which the Azure VM will be located after the migration. We recommend you use a non-production VNet.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

Name	Status	Health	Migration Phase	Last Sync	Test Migration Status
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	2/17/2019, 12:00:43 AM

Migrate VMs

After you've verified that the test migration works as expected, you can migrate the on-premises machines.

1. In the Azure Migrate project > Servers > Azure Migrate: Server Migration, click Replicating servers.

Migration tools

Azure Migrate: Server Migration

Discover Replicate Migrate Overview

Discovered servers	1
Replicating servers	1
Test migrated servers	0
Migrated servers	0

Next step: You can start migrating the replicating servers to Azure

2. In Replicating machines, right-click the VM > Migrate.
3. In Migrate > Shut down virtual machines and perform a planned migration with no data loss, select Yes > OK.
 - By default Azure Migrate shuts down the on-premises VM to ensure minimum data loss.
 - If you don't want to shut down the VM, select No
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the Virtual Machines page.

Complete the migration

1. After the migration is done, right-click the VM > Stop migration. This does the following:
 - Stops replication for the on-premises machine.
 - Removes the machine from the Replicating servers count in Azure Migrate: Server Migration.
 - Cleans up replication state information for the VM.
2. Install the Azure VM [Windows](#) or [Linux](#) agent on the migrated machines.

3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

Post-migration best practices

- On-premises
 - Move app traffic over to the app running on the migrated Azure VM instance.
 - Remove the on-premises VMs from your local VM inventory.
 - Remove the on-premises VMs from local backups.
 - Update any internal documentation to show the new location and IP address of the Azure VMs.
- Tweak Azure VM settings after migration:
 - The [Azure VM agent](#) manages VM interaction with the Azure Fabric Controller. It's required for some Azure services, such as Azure Backup, Site Recovery, and Azure Security. When migrating VMs with agent-based migration, the Mobility Service installer installs Azure VM agent on Windows machines. On Linux VMs, we recommend that you install the agent after migration.
 - Manually uninstall the Mobility service from the Azure VM after migration.
 - Manually uninstall VMware tools after migration.
- In Azure:
 - Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
 - Perform final application and migration acceptance testing on the migrated application now running in Azure.
- Business continuity/disaster recovery
 - Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](#).
 - Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery. [Learn more](#).
- For increased security:
 - Lock down and limit inbound traffic access with [Azure Security Center - Just in time administration](#).
 - Restrict network traffic to management endpoints with [Network Security Groups](#).
 - Deploy [Azure Disk Encryption](#) to help secure disks, and keep data safe from theft and unauthorized access.
 - Read more about [securing IaaS resources](#), and visit the [Azure Security Center](#).
- For monitoring and management:
 - Consider deploying [Azure Cost Management](#) to monitor resource usage and spending.

Next steps

Investigate the [cloud migration journey](#) in the Azure Cloud Adoption Framework.

This article describes how to prepare for assessment of on-premises Hyper-V VMs with Azure Migrate:Server Assessment([migrate-services-overview.md#azure-migrate-server-assessment-tool](#)), and migration of Hyper-V VMs with [Azure Migrate:Server Migration](#).

This tutorial is the first in a series that shows you how to assess and migrate Hyper-V VMs to Azure. In this tutorial, you learn how to:

- Prepare Azure. Set up permissions for your Azure account and resources to work with Azure Migrate.
- Prepare on-premises Hyper-V hosts and VMs for server assessment. You can prepare using a configuration script, or manually.
- Prepare for deployment of the Azure Migrate appliance. The appliance is used to discover and assess on-premises VMs.
- Prepare on-premises Hyper-V hosts and VMs for server migration.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-tos for Hyper-V assessment and migration.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prepare Azure

Azure permissions

You need set up permissions for Azure Migrate deployment.

TASK	DETAILS
Create an Azure Migrate project	Your Azure account needs Contributor or Owner permissions to create a project.
Register resource providers	Azure Migrate uses a lightweight Azure Migrate appliance to discover and assess Hyper-V VMs with Azure Migrate Server Assessment. During appliance registration, resource providers are registered with the subscription chosen in the appliance. Learn more . To register the resource providers, you need a Contributor or Owner role on the subscription.

TASK	DETAILS
Create Azure AD app	<p>When registering the appliance, Azure Migrate creates an Azure Active Directory (Azure AD) app that's used for communication between the agents running on the appliance with their respective services running on Azure. Learn more.</p> <p>You need permissions to create Azure AD apps (available in the Application Developer role).</p>

Assign permissions to create project

Check you have permissions to create an Azure Migrate project.

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Assign permissions to register the appliance

You can assign permissions for Azure Migrate to create the Azure AD app during appliance registration, using one of the following methods:

- A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
- A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.

NOTE

- The app does not have any other access permissions on the subscription other than those described above.
- You only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

Grant account permissions

The tenant/global admin can grant permissions as follows:

1. In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User Settings**.
2. The admin should set **App registrations** to **Yes**.

The screenshot shows the 'User settings' page in the Microsoft Azure Active Directory. The left sidebar has sections for 'All users', 'Deleted users', 'Password reset', 'User settings' (which is selected), 'Activity' (with 'Sign-ins' and 'Audit logs'), and 'Troubleshooting + Support' (with 'Troubleshoot' and 'New support request'). The main content area includes sections for 'Enterprise applications' (with a link to 'Manage how end users launch and view their applications'), 'App registrations' (with a note 'Users can register applications' and a 'Yes' button highlighted with a red box), 'Administration portal' (with a note 'Restrict access to Azure AD administration portal' and 'Yes' and 'No' buttons), 'LinkedIn account connections' (with a note 'Allow users to connect work or school account with LinkedIn' and 'Yes', 'Selected', and 'No' buttons), 'External users' (with a link to 'Manage external collaboration settings'), and 'Access panel' (with a link to 'Manage settings for access panel preview features').

NOTE

This is a default setting that isn't sensitive. [Learn more.](#)

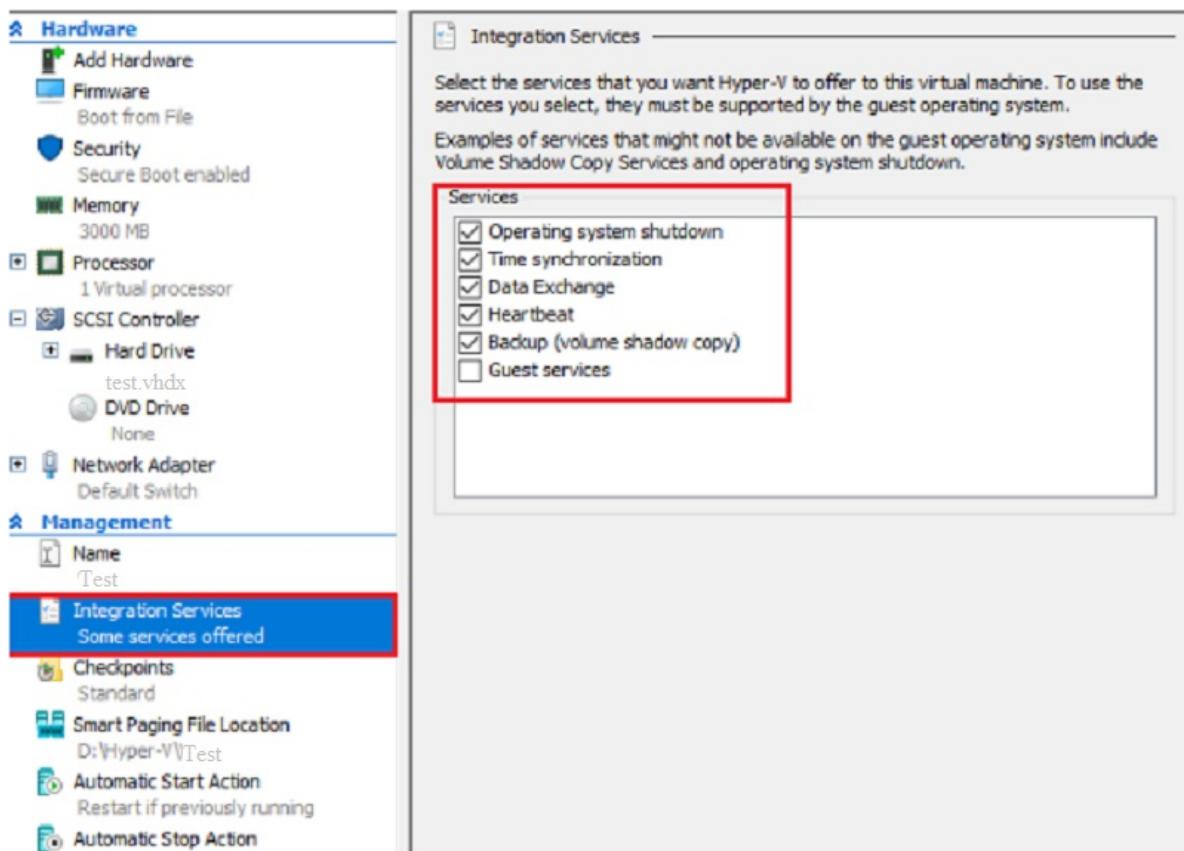
Assign Application Developer role

The tenant/global admin can assign the Application Developer role to an account. [Learn more.](#)

Prepare Hyper-V for assessment

You can prepare Hyper-V for VM assessment manually, or using a configuration script. Preparation steps are as follows:

- Verify Hyper-V host settings, and make sure that the [required ports](#) are open on Hyper-V hosts.
- Set up PowerShell remoting on each host, so that the Azure Migrate appliance can run PowerShell commands on the host, over a WinRM connection.
- Delegate credentials if VM disks are located on remote SMB shares.
- Set up an account that the appliance will use to discover VMs on Hyper-V hosts.
- Set up Hyper-V Integration Services on each VM you want to discover and assess. The default settings when you enable Integration Services are sufficient for Azure Migrate.



Prepare with a script

The script does the following:

- Checks that you're running the script on a supported PowerShell version.
- Verifies that you (the user running the script) have administrative privileges on the Hyper-V host.
- Allows you to create a local user account (not administrator) that the Azure Migrate service uses to communicate with the Hyper-V host. This user account is added to these groups on the host:
 - Remote Management Users
 - Hyper-V Administrators
 - Performance Monitor Users
- Checks that the host is running a supported version of Hyper-V, and the Hyper-V role.
- Enables the WinRM service, and opens ports 5985 (HTTP) and 5986 (HTTPS) on the host (needed for metadata collection).
- Enables PowerShell remoting on the host.
- Checks that the Hyper-V Integration Services is enabled on all VMs managed by the host.
- Enables CredSSP on the host if needed.

Run the script as follows:

1. Make sure you have PowerShell version 4.0 or later installed on the Hyper-V host.
2. Download the script from the [Microsoft Download Center](#). The script is cryptographically signed by Microsoft.
3. Validate the script integrity using either MD5, or SHA256 hash files. Hashtag values are below. Run this command to generate the hash for the script:

```
C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]
```

Example usage:

```
C:\>CertUtil -HashFile C:\Users\Administrators\Desktop\ MicrosoftAzureMigrate-Hyper-V.ps1  
SHA256
```

- After validating the script integrity, run the script on each Hyper-V host with this PowerShell command:

```
PS C:\Users\Administrators\Desktop> MicrosoftAzureMigrate-Hyper-V.ps1
```

Hashtag values

Hash values are:

HASH	VALUE
MD5	0ef418f31915d01f896ac42a80dc414e
SHA256	0ad60e7299925eff4d1ae9f1c7db485dc9316ef45b0964148a 3c07c80761ade2

Prepare manually

Follow the procedures in this section to prepare Hyper-V manually, instead of using the script.

Verify PowerShell version

Make sure you have PowerShell version 4.0 or later installed on the Hyper-V host.

Set up an account for VM discovery

Azure Migrate needs permissions to discover on-premises VMs.

- Set up a domain or local user account with administrator permissions on the Hyper-V hosts/cluster.
 - You need a single account for all hosts and clusters that you want to include in the discovery.
 - The account can be a local or domain account. We recommend it has Administrator permissions on the Hyper-V hosts or clusters.
 - Alternatively, if you don't want to assign Administrator permissions, the following permissions are needed:
 - Remote Management Users
 - Hyper-V Administrators
 - Performance Monitor Users

Verify Hyper-V host settings

- Verify [Hyper-V host requirements](#) for server assessment.
- Make sure the [required ports](#) are open on Hyper-V hosts.

Enable PowerShell remoting on hosts

Set up PowerShell remoting on each host, as follows:

- On each host, open a PowerShell console as admin.
- Run this command:

```
Enable-PSRemoting -force
```

Enable Integration Services on VMs

Integration Services should be enabled on each VM so that Azure Migrate can capture operating system information on the VM.

On VMs that you want to discover and assess, enable [Hyper-V Integration Services](#) on each VM.

Enable CredSSP on hosts

If the host has VMs with disks located on SMB shares, complete this step on the host.

- You can run this command remotely on all Hyper-V hosts.
- If you add new host nodes on a cluster they are automatically added for discovery, but you need to manually enable CredSSP on the new nodes if needed.

Enable as follows:

1. Identify Hyper-V hosts running Hyper-V VMs with disks on SMB shares.
2. Run the following command on each identified Hyper-V host:

```
Enable-WSManCredSSP -Role Server -Force
```

When you set up the appliance, you finish setting up CredSSP by [enabling it on the appliance](#). This is described in the next tutorial in this series.

Prepare for appliance deployment

Before setting up the Azure Migrate appliance and beginning assessment in the next tutorial, prepare for appliance deployment.

1. [Verify](#) appliance requirements.
2. [Review](#) the Azure URLs that the appliance will need to access.
3. Review the data that the appliance will collect during discovery and assessment.
4. [Note](#) port access requirements for the appliance.

Prepare for Hyper-V migration

1. [Review](#) Hyper-V host requirements for migration, and the Azure URLs to which Hyper-V hosts and clusters need access for VM migration.
2. [Review](#) the requirements for Hyper-V VMs that you want to migrate to Azure.

Next steps

In this tutorial, you:

- Set up Azure account permissions.
- Prepared Hyper-V hosts and VMs for assessment and migration.
- Prepared for deployment of the Azure Migrate appliance.

Continue to the next tutorial to create an Azure Migrate project, deploy the appliance, and discover and assess Hyper-V VMs for migration to Azure.

[Assess Hyper-V VMs](#)

This article shows you how to assess on-premises Hyper-V VMs, using the [Azure Migrate:Server Assessment](#) tool.

This tutorial is the second in a series that demonstrates how to assess and migrate Hyper-V VMs to Azure. In this tutorial, you learn how to:

- Set up an Azure Migrate project.
- Set up and register an Azure Migrate appliance.
- Start continuous discovery of on-premises VMs.
- Group discovered VMs, and assess the group.
- Review the assessment.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-to articles.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

- [Complete](#) the first tutorial in this series. If you don't, the instructions in this tutorial won't work.
- Here's what you should have done in the first tutorial:
 - [Prepare Azure](#) to work with Azure Migrate.
 - [Prepare Hyper-V](#) hosts and VMs assessment.
 - [Verify](#) what you need in order to deploy the Azure Migrate appliance for Hyper-V assessment.

Set up an Azure Migrate project

1. In the Azure portal > All services, search for **Azure Migrate**.
2. In the search results, select **Azure Migrate**.
3. In **Overview**, under **Discover, assess and migrate servers**, click **Assess and migrate servers**.

The screenshot shows the Azure Migrate portal interface. On the left, there's a navigation sidebar with links like Overview, Migration goals, Manage, Support + troubleshooting, and New support request. The main area has a heading 'Migrate your on-premises datacenter to Azure' and sub-sections for 'Assess and migrate web apps to Azure' and 'Migrate on-premises data to Azure'. The 'Assess and migrate servers' section is highlighted with a red box. It contains two cards: 'Discover, assess and migrate servers' and 'Discover, assess and migrate databases'. Both cards feature icons of servers and databases being assessed by a rocket ship, and a 'Get started' button.

4. In **Getting started**, click **Add tools**.
5. In the **Migrate project** tab, select your Azure subscription, and create a resource group if you don't have one.
6. In **Project Details**, specify the project name, and the region in which you want to create the project. [Review](#) the regions in which you can create Azure Migrate project.
 - The project region is used only to store the metadata gathered from on-premises VMs.
 - You can select a different Azure target region when you migrate the VMs. All Azure regions are supported for migration target.

Add a tool

[Migrate project](#) [Select assessment tool](#) [Select migration tool](#) [Review + add tool\(s\)](#)

A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.

* Subscription [?](#) [▼](#)

 └─ * Resource group [?](#) [▼](#)
 [Create new](#)

PROJECT DETAILS

Specify the name of the migrate project and the preferred geography.

* Migrate project [?](#) [✓](#)

* Region [▼](#)

7. Click **Next**.
8. In **Select assessment tool**, select **Azure Migrate: Server Assessment** > **Next**.

Add a tool

Migrate project Select assessment tool Select migration tool Review + add tool(s)

Start by choosing a server discovery and assessment tool. We recommend that you discover and assess your datacenter to determine migration readiness.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
 Azure Migrate: Server Assessment	View	VMware virtual machines Hyper-V virtual machines	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Cloudamize: Cloud Assessment	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Turbonomic: Turbonomic	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 UnifyCloud: CloudRecon	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Device42: Device42	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	Learn more

Note: Visit the ISV tool's website to learn more about tool capabilities.
 Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#)

Skip adding an assessment tool for now

9. In **Select migration tool**, select **Skip adding a migration tool for now > Next**.
10. In **Review + add tools**, review the settings, and click **Add tools**.
11. Wait a few minutes for the Azure Migrate project to deploy. You'll be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

Set up the Azure Migrate appliance

Azure Migrate:server Assessment uses a lightweight Azure Migrate appliance. The appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate.

- The appliance can be set up on a Hyper-V VM using a downloaded Hyper-V VHD. Alternatively, you can set up the appliance on a VM or physical machine with a PowerShell installer script.
- This tutorial uses the VHD. Review [this article](#) if you want to set up the appliance using a script.

After creating the appliance, you check that it can connect to Azure Migrate:Server Assessment, configure it for the first time, and register it with the Azure Migrate project.

Download the VHD

Download the zipped VHD template for the appliance.

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines > Are your machines virtualized?**, click **Yes, with Hyper-V**.
3. Click **Download** to download the VHD file.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with options like Overview, Migration goals, Servers (which is selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area is titled 'Discover machines' and asks 'Are your machines virtualized? Yes, with Hyper-V'. It provides instructions for deploying the migration appliance, downloading the VHD file, creating a virtual machine, configuring the appliance, and starting discovery. A 'Next step' section suggests refining app dependency analysis. A 'Wait for the appliance to be connected, discovery to be completed, performance data to be collected.' message is also present.

Verify security

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.

2. Run the following PowerShell command to generate the hash for the ZIP file

- `C:\>Get-FileHash -Path <file_location> -Algorithm [Hashing Algorithm]`
- Example usage: `C:\>Get-FileHash -Path ./AzureMigrateAppliance_v1.19.06.27.zip -Algorithm SHA256`

3. For appliance version 2.19.07.30, the generated hash should match these settings.

ALGORITHM	HASH VALUE
MD5	29a7531f32bcf69f32d964fa5ae950bc
SHA256	37b3f27bc44f475872e355f04fc8f38606c84534c117d1609f2d12444569b31

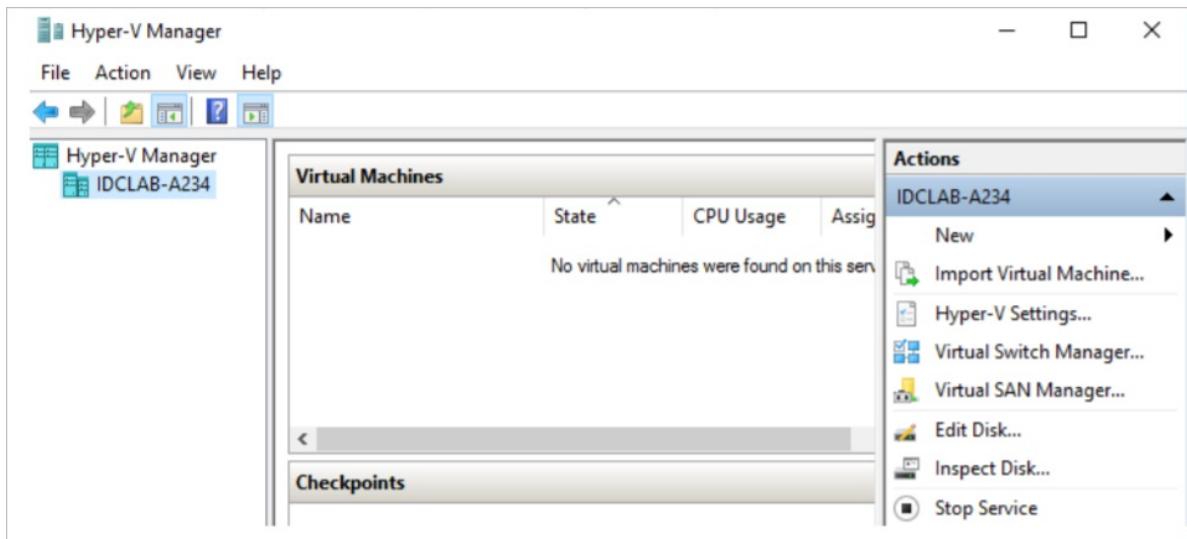
Create the appliance VM

Import the downloaded file, and create the VM.

1. After downloading the zipped VHD file to the Hyper-V host on which the appliance VM will be placed, extract the zipped file.

- In the extracted location, the file unzips into a folder called **AzureMigrateAppliance_VersionNumber**.
- This folder contains a subfolder, also called **AzureMigrateAppliance_VersionNumber**.
- This subfolder contains three further subfolders - **Snapshots**, **Virtual Hard Disks**, and **Virtual Machines**.

2. Open Hyper-V Manager. In Actions, click **Import Virtual Machine**.



3. In the Import Virtual Machine Wizard > **Before you begin**, click **Next**.
4. In **Locate Folder**, select the **Virtual Machines** folder. Then click **Next**.
5. In **Select Virtual Machine**, click **Next**.
6. In **Choose Import Type**, click **Copy the virtual machine (create a new unique ID)**. Then click **Next**.
7. In **Choose Destination**, leave the default setting. Click **Next**.
8. In **Storage Folders**, leave the default setting. Click **Next**.
9. In **Choose Network**, specify the virtual switch that the VM will use. The switch needs internet connectivity to send data to Azure. [Learn](#) about creating a virtual switch.
10. In **Summary**, review the settings. Then click **Finish**.
11. In Hyper-V Manager > **Virtual Machines**, start the VM.

Verify appliance access to Azure

Make sure that the appliance VM can connect to [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time.

NOTE

If you set up the appliance using a [PowerShell script](#) instead of the downloaded VHD, the first two steps in this procedure aren't relevant.

1. In Hyper-V Manager > **Virtual Machines**, right-click the VM > **Connect**.
2. Provide the language, time zone, and password for the appliance.
3. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app:
<https://appliance name or IP address: 44368>.
Alternately, you can open the app from the appliance desktop by clicking the app shortcut.
4. In the web app > **Set up prerequisites**, do the following:
 - **License**: Accept the license terms, and read the third-party information.
 - **Connectivity**: The app checks that the VM has internet access. If the VM uses a proxy:
 - Click **Proxy settings**, and specify the proxy address and listening port, in the form

<http://ProxyIPAddress> or <http://ProxyFQDN>.

- Specify credentials if the proxy needs authentication.
- Only HTTP proxy is supported.
- **Time sync:** Time is verified. The time on the appliance should be in sync with internet time for VM discovery to work properly.
- **Install updates:** Azure Migrate Server Assessment checks that the appliance has the latest updates installed.

Register the appliance with Azure Migrate

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
 - Sign in with your username and password.
 - Sign-in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

Delegate credentials for SMB VHDS

If you're running VHDS on SMBs, you must enable delegation of credentials from the appliance to the Hyper-V hosts. This requires the following:

- You enable each host to act as a delegate for the appliance. If you followed the tutorials in order, you did this in the previous tutorial, when you prepared Hyper-V for assessment and migration. You should have either set up CredSSP for the hosts [manually](#), or by [running a script](#) that does this.
- Enable CredSSP delegation so that the Azure Migrate appliance can act as the client, delegating credentials to a host.

Enable on the appliance as follows:

Option 1

On the appliance VM, run this command. HyperVHost1/HyperVHost2 are example host names.

```
Enable-WSManCredSSP -Role Client -DelegateComputer HyperVHost1.contoso.com HyperVHost2.contoso.com -Force
```

Example:

```
Enable-WSManCredSSP -Role Client -DelegateComputer HyperVHost1.contoso.com HyperVHost2.contoso.com -Force
```

Option 2

Alternatively, do this in the Local Group Policy Editor on the appliance:

1. In **Local Computer Policy > Computer Configuration**, click **Administrative Templates > System > Credentials Delegation**.
2. Double-click **Allow delegating fresh credentials**, and select **Enabled**.
3. In **Options**, click **Show**, and add each Hyper-V host you want to discover to the list, with **wsman/** as a prefix.
4. Then, in **Credentials Delegation**, double-click **Allow delegating fresh credentials with NTLM-only server authentication**. Again, add each Hyper-V host you want to discover to the list, with **wsman/** as a prefix.

Start continuous discovery

Connect from the appliance to Hyper-V hosts or clusters, and start VM discovery.

1. In **User name and Password**, specify the account credentials that the appliance will use to discover VMs. Specify a friendly name for the credentials, and click **Save details**.
2. Click **Add host**, and specify Hyper-V host/cluster details.
3. Click **Validate**. After validation, the number of VMs that can be discovered on each host/cluster is shown.
 - If validation fails for a host, review the error by hovering over the icon in the **Status** column. Fix issues, and validate again.
 - To remove hosts or clusters, select > **Delete**.
 - You can't remove a specific host from a cluster. You can only remove the entire cluster.
 - You can add a cluster, even if there are issues with specific hosts in the cluster.
4. After validation, click **Save and start discovery** to start the discovery process.

This starts discovery. It takes around 1.5 minutes per host for metadata of discovered servers to appear in the Azure portal.

Verify VMs in the portal

After discovery finishes, you can verify that the VMs appear in the portal.

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers > Azure Migrate: Server Assessment** page, click the icon that displays the count for **Discovered servers**.

Set up an assessment

There are two types of assessments you can run using Azure Migrate Server Assessment.

ASSESSMENT	DETAILS	DATA
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.
As on-premises	Assessments based on on-premises sizing.	Recommended VM size: Based on the on-premises VM size Recommended disk type: Based on the storage type setting you select for the assessment.

Run an assessment

Run an assessment as follows:

1. Review the [best practices](#) for creating assessments.
2. In **Servers > Azure Migrate: Server Assessment**, click **Assess**.

Azure Migrate - Servers

Microsoft

Search (Ctrl+ /) « Refresh

Last refreshed details for migrate project <project name> <time>

Assessment tools

Azure Migrate: Server Assessment

- Discover
- Assess** (highlighted with a red box)
- Overview

Discovered servers	5271
Groups	3
Assessments	3
Notifications	2 critical

Next step: You can refine your application grouping with dependency analysis

Add more assessment tools? [Click here.](#)

3. In **Assess Servers**, specify a name for the assessment.
4. Click **View all** to review the assessment properties.

Assessment properties

You can also edit these properties later by opening the **assessment** and clicking on 'Edit properties' command on top

TARGET DETAILS

Target location: West US 2	Storage type: Premium managed disks	Reserved instances: 3 years reserved
----------------------------	-------------------------------------	--------------------------------------

SIZING

Sizing criterion: As on-premises	Performance history: Not applicable	Percentile utilization: Not applicable
VM series: 6 selected	Comfort factor: 1	

PRICING

Offer: Pay-As-You-Go	Currency: US Dollar (\$)	Discount (%): 0	VM uptime: 31 Day(s) per month	Hour(s) per day: 24
----------------------	--------------------------	-----------------	--------------------------------	---------------------

Azure Hybrid Benefit
Apply Azure Hybrid Benefit and save up to 49% vs. pay-as-you-go costs with an eligible Windows Server license.

* Already have a Windows Server license? Yes No

[Review Azure hybrid benefit compliance](#)

5. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more VMs together for assessment.
6. In **Add machines to the group**, select VMs to add to the group.
7. Click **Create Assessment** to create the group, and run the assessment.

Create assessment

ContosoCorporationProject

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

Assessment properties (Showing 3 of 13) [View all](#)

Migration target location	: West US 2
Sizing criterion	: As on-premises
Reserved instances	: 3 years reserved

Select or create a group

Create New Use Existing

VMware-Group1 ✓

Add machines to the group

[Select all](#) [Clear selection](#)

[Search to filter machines](#)

NAME	IP ADDR
<input checked="" type="checkbox"/> Data Tier 01	2404:f8
<input checked="" type="checkbox"/> Middle tier 01	2404:f8
VMware vCenter Server Appliance	10.150.
<input checked="" type="checkbox"/> Middle Tier 02	2404:f8
<input checked="" type="checkbox"/> Data Tier 02	2404:f8
Azure Migrate Collector Appliance	2404:f8
<input checked="" type="checkbox"/> Web Tier 02	2404:f8
<input checked="" type="checkbox"/> Web Tier 01	2404:f8

8. After the assessment is created, view it in **Servers > Azure Migrate: Server Assessment**.

9. Click **Export assessment**, to download it as an Excel file.

Review an assessment

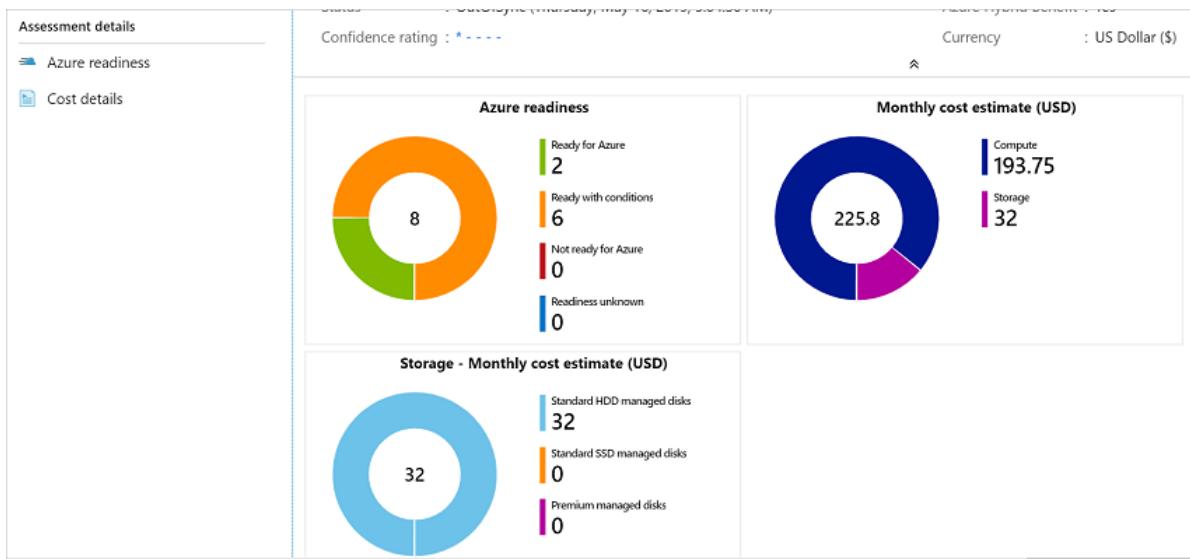
An assessment describes:

- **Azure readiness:** Whether VMs are suitable for migration to Azure.
- **Monthly cost estimation:** The estimated monthly compute and storage costs for running the VMs in Azure.
- **Monthly storage cost estimation:** Estimated costs for disk storage after migration.

View an assessment

1. In **Migration goals > Servers > Azure Migrate: Server Assessment**, click **Assessments**.

2. In **Assessments**, click on an assessment to open it.



Review Azure readiness

1. In **Azure readiness**, verify whether VMs are ready for migration to Azure.
2. Review the VM status:
 - **Ready for Azure**: Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
 - **Ready with conditions**: Shows issues and suggested remediation.
 - **Not ready for Azure**: Shows issues and suggested remediation.
 - **Readiness unknown**: Used when Azure Migrate can't assess readiness, due to data availability issues.
3. Click on an **Azure readiness** status. You can view VM readiness details, and drill down to see VM details, including compute, storage, and network settings.

Review cost details

This view shows the estimated compute and storage cost of running VMs in Azure.

1. Review the monthly compute and storage costs. Costs are aggregated for all VMs in the assessed group.
 - Cost estimates are based on the size recommendations for a machine, and its disks and properties.
 - Estimated monthly costs for compute and storage are shown.
 - The cost estimation is for running the on-premises VMs as IaaS VMs. Azure Migrate Server Assessment doesn't consider PaaS or SaaS costs.
2. You can review monthly storage cost estimates. This view shows aggregated storage costs for the assessed group, split over different types of storage disks.
3. You can drill down to see details for specific VMs.

Review confidence rating

When you run performance-based assessments, a confidence rating is assigned to the assessment.

Assess servers	Columns						
Search to filter assessments							
NAME	GROUP	STATUS	MACHINES	LOCATION	SIZING CRITERION	CONFIDENCE RATING	
assessment_5_16_2019_17_34_29	day2	OutOfSync	0	North Europe	Performance-based	★★★★★	
assessment_5_20_2019_17_42_6	Mygroup	Ready	6	North Europe	Performance-based	★★★★★	
assessment_5_22_2019_22_56_18	Day2-group	OutDated	14	North Europe	Performance-based	★★★★★	

- A rating from 1-star (lowest) to 5-star (highest) is awarded.
- The confidence rating helps you estimate the reliability of the size recommendations provided by the assessment.
- The confidence rating is based on the availability of data points needed to compute the assessment.

Confidence ratings for an assessment are as follows.

DATA POINT AVAILABILITY	CONFIDENCE RATING
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

[Learn more](#) about best practices for confidence ratings.

Next steps

In this tutorial, you:

- Set up an Azure Migrate appliance
- Created and reviewed an assessment

Continue to the third tutorial in the series, to learn how to migrate Hyper-V VMs to Azure with Azure Migrate Server Migration.

[Migrate Hyper-V VMs](#)

This article shows you how to migrate on-premises Hyper-V VMs to Azure, using agentless migration with the Azure Migrate: Server Migration tool.

Azure Migrate provides a central hub to track discovery, assessment, and migration of your on-premises apps and workloads, and private/public cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

This tutorial is the third in a series that demonstrates how to assess and migrate Hyper-V to Azure using Azure Migrate Server Assessment and Migration. In this tutorial, you learn how to:

- Prepare Azure and your on-premises Hyper-V environment
- Set up the source environment, and deploy a replication appliance.
- Set up the target environment.
- Enable replication.
- Run a test migration to make sure everything's working as expected.
- Run a full migration to Azure.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

Before you begin this tutorial, you should:

1. [Review](#) the Hyper-V migration architecture.
2. [Complete the first tutorial](#) in this series to set up Azure and Hyper-V for migration. In the first tutorial, you:
 - [Prepare Azure](#) for migration.
 - [Prepare the on-premises environment](#) for migration.
3. We recommend that you try assessing Hyper-V VMs, using Azure Migrate: Server Assessment, before migrating them to Azure. To do this, [complete the second tutorial](#) in this series. Although we recommend that you try out an assessment, you don't have to run an assessment before you migrate VMs.
4. Make sure that your Azure account is assigned the Virtual Machine Contributor role, so that you have permissions to:
 - Create a VM in the selected resource group.
 - Create a VM in the selected virtual network.
 - Write to an Azure managed disk.
5. [Set up an Azure network](#). When you migrate to Azure, the created Azure VMs are joined to an Azure network you specify when you set up migration.

Add the Azure Migrate Server Migration tool

If you didn't follow the second tutorial to assess Hyper-V VMs, you need to [follow these instructions](#) to set up an Azure Migrate project, and add the Azure Migrate Server Assessment tool to the project.

If you followed the second tutorial and already have an Azure Migrate project, add the Azure Migrate: Server Migration tool as follows:

1. In the Azure Migrate project, click **Overview**.
2. In **Discover, assess, and migration servers**, click **Assess and migrate servers**.
3. In **Migration tools**, select **Click here to add a migration tool when you are ready to migrate**.

The screenshot shows the Azure Migrate interface. In the 'Assessment tools' section, there are two cards: 'Azure Migrate: Server Assessment' and 'Cloudamize'. The 'Azure Migrate: Server Assessment' card has a 'Quick start' section with steps 1: Discover and 2: Assess. The 'Cloudamize' card has a 'Quick start' section with steps 1: Register and 2: Connect. Below these cards is a link 'Add more assessment tools? Click here.' In the 'Migration tools' section, there is a message 'You do not have any migration tools yet' followed by a link 'Click here to add a migration tool when you are ready to migrate'.

4. In the tools list, select **Azure Migrate: Server Migration > Add tool**

The screenshot shows the 'Azure Migrate' tools list. It displays a table with columns: TOOL, PRICING, SUPPORTED WORKLOADS, FEATURES, and LEARN MORE. The 'Azure Migrate: Server Migration' tool is listed with the following details:

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
Azure Migrate: Server Migration	View	VMware virtual machines Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless and agent-based migration Cutover in seconds Minimal application downtime	Learn more

Set up the Azure Migrate appliance

Azure Migrate Server Migration runs a software agent on Hyper-V Hosts or cluster nodes to orchestrate and replicate data to Azure Migrate and doesn't require a dedicated appliance for migration.

- The Azure Migrate : Server Assessment appliance performs VM discovery and sends VM metadata and performance data to Azure Migrate Server Migration.
- Migration orchestration and data replication is handled by Microsoft Azure Site Recovery provider and Microsoft Azure Recovery Service agent.

To set up the appliance:

- If you followed the second tutorial to assess Hyper-V VMs, you already set up the appliance during that tutorial, and don't need to do it again.
- If you didn't follow that tutorial, you need to set up the appliance now. To do this, you:
 - Download a compressed Hyper-V VHD from the Azure portal.
 - Create the appliance, and check that it can connect to Azure Migrate Server Assessment.
 - Configure the appliance for the first time, and register it with the Azure Migrate project.

Follow the detailed instructions in [this article](#) to set up the appliance.

Prepare Hyper-V hosts

1. In the Azure Migrate project > **Servers**, in **Azure Migrate: Server Migration**, click **Discover**.
2. In **Discover machines** > **Are your machines virtualized?**, select **Yes, with Hyper-V**.
3. In **Target region**, select the Azure region to which you want to migrate the machines.
4. Select **Confirm that the target region for migration is region-name**.
5. Click **Create resources**. This creates an Azure Site Recovery vault in the background.
 - If you've already set up migration with Azure Migrate Server Migration, this option won't appear since resources were set up previously.
 - You can't change the target region for this project after clicking this button.
 - All subsequent migrations are to this region.
6. In **Prepare Hyper-V host servers**, download the Hyper-V Replication provider, and the registration key file.
 - The registration key is needed to register the Hyper-V host with Azure Migrate Server Migration.
 - The key is valid for five days after you generate it.

Discover machines

Are your machines virtualized? ⓘ
Yes, with Hyper-V

Target region ⓘ
(US) Central US

Prepare for replication by downloading and installing the replication provider software on your Hyper-V hosts. Follow the steps below to setup and configure Hyper-V host servers.

1. Prepare Hyper-V host servers.
 [Download](#) the Hyper-V replication provider(AzureSiteRecoveryProvider.exe) software installer. Use the installer to install the replication provider on the Hyper-V servers.
 Download the registration key file and use it to register the Hyper-V host to this Azure Migrate project.
[Download](#)

7. Copy the provider setup file and registration key file to each Hyper-V host (or cluster node) running VMs you want to replicate.
8. Run the provider setup file on each host, as described in the next procedure.
9. After installing the provider on hosts, in **Discover machines**, click **Finalize registration**.

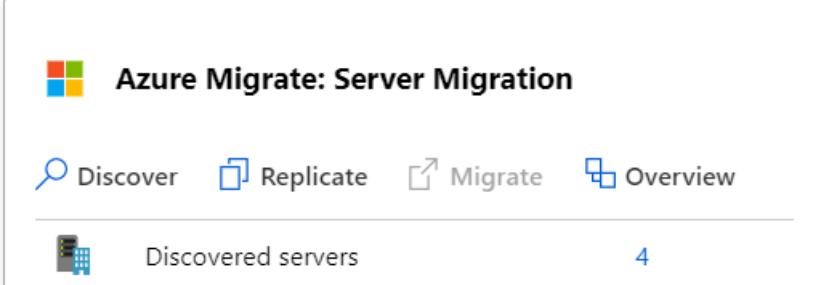
2. Finalize registration.
 Prepare for replication by finalizing registration for the Hyper-V hosts.

 Registered Hyper-V hosts	1 (Connected)
--	----------------------

[Finalize registration](#)

It can take up to 15 minutes after finalizing registration until discovered VMs appear in Azure Migrate Server Migration. As VMs are discovered, the **Discovered servers** count rises.

Migration tools



The screenshot shows the Azure Migrate: Server Migration interface. At the top, there's a navigation bar with four tabs: 'Discover' (selected), 'Replicate', 'Migrate', and 'Overview'. Below the tabs, there's a section titled 'Discovered servers' which displays a count of 4.

Register Hyper-V hosts

Install the downloaded setup file (AzureSiteRecoveryProvider.exe) on each relevant Hyper-V host.

1. Run the provider setup file on each host or cluster node.
2. In the Provider Setup wizard > **Microsoft Update**, opt in to use Microsoft Update to check for Provider updates.
3. In **Installation**, accept the default installation location for the Provider and agent, and select **Install**.
4. After installation, in the Registration Wizard > **Vault Settings**, select **Browse**, and in **Key File**, select the vault key file that you downloaded.
5. In **Proxy Settings**, specify how the provider running on the host connects to the internet.
 - If the appliance is located behind a proxy server, you need to specify proxy settings.
 - Specify the proxy name as **http://ip-address**, or **http://FQDN**. HTTPS proxy servers aren't supported.
6. Make sure that the provider can reach the [required URLs](#).
7. In **Registration**, after the host is registered, click **Finish**.

Replicate Hyper-V VMs

With discovery completed, you can begin replication of Hyper-V VMs to Azure.

NOTE

You can replicate up to 10 machines together. If you need to replicate more, then replicate them simultaneously in batches of 10.

1. In the Azure Migrate project > **Servers**, **Azure Migrate: Server Migration**, click **Replicate**.
2. In **Replicate**, > **Source settings** > **Are your machines virtualized?**, select **Yes**, with **Hyper-V**. Then click **Next: Virtual machines**.
3. In **Virtual machines**, select the machines you want to replicate.
 - If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.
 - If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** options.
 - If you selected to use the assessment, select the VM group, and assessment name.

Replicate

Source settings **Virtual machines** Target settings Compute Disks Review + Start replication

Select the virtual machines to be migrated.

* Import migration settings from an assessment? ?

Select

Yes, apply migration settings from a Azure Migrate assessment

No, I'll specify the migration settings manually

4. In **Virtual machines**, search for VMs as needed, and check each VM you want to migrate. Then, click **Next: Target settings**.

Source settings **Virtual machines** Target settings Compute Disks Review + Start replication

Select the virtual machines to be migrated.

* Import migration settings from an assessment? ?

No, I'll specify the migration settings manually

* Virtual machines ?

Search to filter machines < Previous Page 1 Next >

NAME	IP ADDRESS	OPERATING SYSTEM	BOOT TYPE
<input checked="" type="checkbox"/> ContosoVMwareMigr...	2404:f801:4800:25:c95f:5fd3:7347:4f91,1...	Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoCSASR	2404:f801:4800:25:29f9:2ebd:1ee0:eeb4,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-FrontTier3		Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoWeb1	2404:f801:4800:25:9091:9912:5f46:9108,...	Microsoft Windows Server 2008 (32-bit)	bios
<input checked="" type="checkbox"/> Contoso-Configuratio...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-AzureMigrat...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb3	10.150.13.218,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoAppSrv2	2404:f801:4800:25:5de5:e919:3448:be33,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb2	10.150.13.201,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios

Selected items : 9

5. In **Target settings**, select the target region to which you'll migrate, the subscription, and the resource group in which the Azure VMs will reside after migration.
6. In **Replication Storage Account**, select the Azure Storage account in which replicated data will be stored in Azure.
7. **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.
8. In **Azure Hybrid Benefit**:
 - Select **No** if you don't want to apply Azure Hybrid Benefit. Then, click **Next**.
 - Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

Replicate

Source settings Virtual machines **Target settings** Compute Disks Review + Start replication

Select target properties for migration. Migrated machines will be created with the specified properties.

Region ⓘ	Central US
Subscription * ⓘ	<subscription id>
Resource group * ⓘ	ContosoHyperV
* Replication Storage Account ⓘ	contosodemorgdiag (Standard)
Virtual Network * ⓘ	ContosoDemoRG-vnet
Subnet * ⓘ	default

Azure Hybrid Benefit

Apply Azure Hybrid Benefit and save up to 49% vs. pay-as-you-go virtual machine costs with an eligible Windows Server license.

Already have an eligible Windows Server License? * ⓘ

Yes No

9. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).

- **VM size:** If you're using assessment recommendations, the VM size dropdown will contain the recommended size. Otherwise Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in [Azure VM size](#).
- **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
- **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

Source settings Virtual machines Target settings **Compute** Disks Review + Start replication

Select the Azure VM size and OS disk for the machines that are being migrated. Additionally, select an Availability Set if the migrated machine should be part of one.

NAME	AZURE VM NAME	SOURCE VM SIZE
ContosoVMwareMigration2	ContosoVMwareMigration2	8 Cores, 16384 MB RAM
ContosoCSASR	ContosoCSASR	2 Cores, 2048 MB RAM
Contoso-FrontTier3	Contoso-FrontTier3	8 Cores, 16384 MB RAM
ContosoWeb1	ContosoWeb1	2 Cores, 2048 MB RAM
Contoso-ConfigurationServer	Contoso-ConfigurationServer	8 Cores, 16384 MB RAM
Contoso-AzureMigrateAppliance	Contoso2	4 Cores, 8192 MB RAM
ContosoWeb3	ContosoWeb3	2 Cores, 2048 MB RAM
ContosoAppSrv2	ContosoAppSrv2	2 Cores, 4096 MB RAM
ContosoWeb2	ContosoWeb2	2 Cores, 2048 MB RAM

10. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then click **Next**.

- You can exclude disks from replication.
- If you exclude disks, won't be present on the Azure VM after migration.

Replicate	
Source settings Virtual machines Target settings Compute Disks Review + Start replication	
Select the managed disk type to use for the disks of the migrated machine. Optionally, you may also choose to exclude certain disks from replication by unselecting them.	
NAME	DISKS TO REPLICATE
ContosoVMwareMigration2	<input checked="" type="checkbox"/> All selected scsi0:0
ContosoCSASR	<input checked="" type="checkbox"/> All selected scsi0:0
Contoso-FrontTier3	<input checked="" type="checkbox"/> All selected scsi0:0
ContosoWeb1	<input checked="" type="checkbox"/> All selected scsi0:0

11. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

NOTE

You can update replication settings any time before replication starts, in **Manage > Replicating machines**. Settings can't be changed after replication starts.

Provisioning for the first time

If this is the first VM you're replicating in the Azure Migrate project, Azure Migrate: Server Migration automatically provisions these resources in same resource group as the project.

- **Service bus:** Azure Migrate: Server Migration uses the Service Bus to send replication orchestration messages to the appliance.
- **Gateway storage account:** Azure Migrate: Server Migration uses the gateway storage account to store state information about the VMs being replicated.
- **Log storage account:** The Azure Migrate appliance uploads replication logs for VMs to a log storage account. Azure Migrate applies the replication information to the replica-managed disks.
- **Key vault:** The Azure Migrate appliance uses the key vault to manage connection strings for the service bus, and access keys for the storage accounts used in replication. You should have set up the permissions that the key vault needs to access the storage account when you [prepared Azure](#) for Hyper-V VM assessment and migration.

Track and monitor

- When you click **Replicate** a Start Replication job begins.
- When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.
- After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to Azure.

You can track job status in the portal notifications.

You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.

Migration tools

Azure Migrate: Server Migration

+ Discover Replicate Migrate Overview

Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

⚡ **Next step:** You can start migrating the replicating servers to Azure

Run a test migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

- Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating.
- Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production Azure VNet in your Azure subscription).
- You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

Do a test migration as follows:

1. In Migration goals > Servers > Azure Migrate: Server Migration, click Test migrated servers.

Azure Migrate: Server Migration

Discover Replicate Migrate Overview

Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

⚡ **Next step:** You can start migrating the replicating servers to Azure

2. Right-click the VM to test, and click **Test migrate**.

Dashboard > Azure Migrate - Servers > Azure Migrate: Server Migration - Replicating machines

Azure Migrate: Server Migration - Replicating machines

ContosoMigrationReview

Search (Ctrl+ /) Refresh Columns

Last refreshed at: 2/17/2019, 12:56:13 AM

i Finished loading data from service.

Filter items...

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00 AM

3. In **Test Migration**, select the Azure virtual network in which the Azure VM will be located after the migration. We recommend you use a non-production virtual network.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.

Refresh Columns

Last refreshed at: 2/17/2019, 1:02:40 AM

i Finished loading data from service.

Filter items...

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM

Migrate VMs

After you've verified that the test migration works as expected, you can migrate the on-premises machines.

1. In the Azure Migrate project > **Servers** > **Azure Migrate: Server Migration**, click **Replicating servers**.

Migration tools

The screenshot shows the Azure Migrate: Server Migration interface. At the top, there are four navigation tabs: Discover, Replicate, Migrate, and Overview. Below the tabs, there is a summary table with four rows:

Category	Status
Discovered servers	1
Replicating servers	1
Test migrated servers	0

A red box highlights the "Replicating servers" row. At the bottom of the interface, there is a note: **Next step:** You can start migrating the replicating servers to Azure.

2. In **Replicating machines**, right-click the VM > **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**.
 - By default Azure Migrate shuts down the on-premises VM, and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This ensures no data loss.
 - If you don't want to shut down the VM, select **No**
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

Complete the migration

1. After the migration is done, right-click the VM > **Stop migration**. This does the following:
 - Stops replication for the on-premises machine.
 - Removes the machine from the **Replicating servers** count in Azure Migrate: Server Migration.
 - Cleans up replication state information for the VM.
2. Install the Azure VM [Windows](#) or [Linux](#) agent on the migrated machines.
3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

Post-migration best practices

- For increased resilience:
 - Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](#).
 - Keep workloads running and continuously available by replicating Azure VMs to a secondary region

with Site Recovery. [Learn more](#).

- For increased security:
 - Lock down and limit inbound traffic access with [Azure Security Center - Just in time administration](#).
 - Restrict network traffic to management endpoints with [Network Security Groups](#).
 - Deploy [Azure Disk Encryption](#) to help secure disks, and keep data safe from theft and unauthorized access.
 - Read more about [securing IaaS resources](#), and visit the [Azure Security Center](#).
- For monitoring and management:
- Consider deploying [Azure Cost Management](#) to monitor resource usage and spending.

Next steps

Investigate the [cloud migration journey](#) in the Azure Cloud Adoption Framework.

This article describes how to prepare for assessment of on-premises physical servers with [Azure Migrate](#).

[Azure Migrate](#) provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

This tutorial is the first in a series that shows you how to assess physical servers with Azure Migrate. In this tutorial, you learn how to:

- Prepare Azure. Set up permissions for your Azure account and resources to work with Azure Migrate.
- Prepare on-premises physical servers for server assessment.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-tos for physical servers assessment.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prepare Azure

Azure permissions

You need set up permissions for Azure Migrate deployment.

TASK	DETAILS
Create an Azure Migrate project	Your Azure account needs Contributor or Owner permissions to create a project.
Register resource providers	Azure Migrate uses a lightweight Azure Migrate appliance to discover and assess Hyper-V VMs with Azure Migrate Server Assessment. During appliance registration, resource providers are registered with the subscription chosen in the appliance. Learn more . To register the resource providers, you need a Contributor or Owner role on the subscription.
Create Azure AD app	When registering the appliance, Azure Migrate creates an Azure Active Directory (Azure AD) app that's used for communication between the agents running on the appliance with their respective services running on Azure. Learn more . You need permissions to create Azure AD apps (available in the Application Developer) role.

Assign permissions to create project

Check you have permissions to create an Azure Migrate project.

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Assign permissions to register the appliance

You can assign permissions for Azure Migrate to create the Azure AD app during appliance registration, using one of the following methods:

- A tenant/global admin can grant permissions to users in the tenant, to create and register Azure AD apps.
- A tenant/global admin can assign the Application Developer role (that has the permissions) to the account.

NOTE

- The app does not have any other access permissions on the subscription other than those described above.
- You only need these permissions when you register a new appliance. You can remove the permissions after the appliance is set up.

Grant account permissions

The tenant/global admin can grant permissions as follows:

1. In Azure AD, the tenant/global admin should navigate to **Azure Active Directory > Users > User Settings**.
2. The admin should set **App registrations** to **Yes**.

The screenshot shows the 'User settings' page in the Azure Active Directory. The left sidebar includes 'All users', 'Deleted users', 'Password reset', and 'User settings' (which is selected). Under 'Activity', there are 'Sign-ins' and 'Audit logs'. Under 'Troubleshooting + Support', there are 'Troubleshoot' and 'New support request'. The main content area shows the 'Enterprise applications' section with a link to 'Manage how end users launch and view their applications'. Below it is the 'App registrations' section, which contains a note: 'Users can register applications' with 'Yes' and 'No' buttons, where 'Yes' is highlighted with a red box. Further down are sections for 'Administration portal' (with 'Restrict access to Azure AD administration portal' and 'Yes'/'No' buttons), 'LinkedIn account connections' (with 'Allow users to connect work or school account with LinkedIn' and 'Yes', 'Selected', and 'No' buttons), 'External users' (with 'Manage external collaboration settings'), and 'Access panel' (with 'Manage settings for access panel preview features').

NOTE

This is a default setting that isn't sensitive. [Learn more](#).

Assign Application Developer role

The tenant/global admin can assign the Application Developer role to an account. [Learn more](#).

Prepare for physical server assessment

To prepare for physical server assessment, you need to verify the physical server settings and verify settings for appliance deployment:

Verify physical server settings

1. Verify [physical server requirements](#) for server assessment.
2. Make sure the [required ports](#) are open on physical servers.

Verify appliance settings

Before setting up the Azure Migrate appliance and beginning assessment in the next tutorial, prepare for appliance deployment.

1. [Verify](#) appliance requirements for physical servers.
2. [Review](#) the Azure URLs that the appliance will need to access.
3. [Review](#) that that the appliance will collect during discovery and assessment.
4. [Note](#) port access requirements physical server assessment.

Set up an account for physical server discovery

Azure Migrate needs permissions to discover on-premises servers.

- **Windows:** Set up a local user account on all the Windows servers that you want to include in the discovery. The user account needs to be added to the following groups: - Remote Management Users - Performance Monitor Users - Performance Log users
- **Linux:** You need a root account on the Linux servers that you want to discover.

Prepare for physical server migration

Review the requirements for migration of physical servers.

- [Review](#) physical server requirements for migration.
- Azure Migrate: Server Migration uses a replication server for physical server migration:
 - [Review](#) the deployment requirements for the replication appliance, and the [options](#) for installing MySQL on the appliance.
 - Review the [URL](#) and [port] (migrate-replication-appliance.md#port-access) access requirements for the replication appliance.

Next steps

In this tutorial, you:

- Set up Azure account permissions.
- Prepared physical servers for assessment.

Continue to the next tutorial to create an Azure Migrate project, and assess physical servers for migration to Azure

[**Assess physical servers**](#)

This article shows you how to assess on-premises physical servers, using the Azure Migrate: Server Assessment tool.

Azure Migrate provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

This tutorial is the second in a series that demonstrates how to assess and migrate physical servers to Azure. In this tutorial, you learn how to:

- Set up an Azure Migrate project.
- Set up an Azure Migrate appliance that runs on-premises to assess physical servers.
- Start continuous discovery of on-premises physical servers. The appliance sends configuration and performance data for discovered servers to Azure.
- Group discovered servers, and assess the server group.
- Review the assessment.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-to articles.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

- [Complete](#) the first tutorial in this series. If you don't, the instructions in this tutorial won't work.
- Here's what you should have done in the first tutorial:
 - [Set up Azure permissions](#) for Azure Migrate.
 - [Prepare physical servers](#) for assessment. Appliance requirements should be verified. You should also have an account set up for physical server discovery. Required ports should be available, and you should be aware of the URLs needed for access to Azure.

Set up an Azure Migrate project

Set up a new Azure Migrate project as follows.

1. In the Azure portal > **All services**, search for **Azure Migrate**.
2. Under **Services**, select **Azure Migrate**.
3. In **Overview**, under **Discover, assess and migrate servers**, click **Assess and migrate servers**.

4. In **Getting started**, click **Add tools**.
5. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
6. In **Project Details**, specify the project name, and the geography in which you want to create the project. Asia, Europe, UK and the United States are supported.
 - The project geography is used only to store the metadata gathered from on-premises servers.
 - You can select any target region when you run a migration.

7. Click **Next**.
8. In **Select assessment tool**, select **Azure Migrate: Server Assessment > Next**.

Add a tool

Migrate project Select assessment tool **Select migration tool** Review + add tool(s)

Start by choosing a server discovery and assessment tool. We recommend that you discover and assess your datacenter to determine migration readiness.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
 Azure Migrate: Server Assessment	View	VMware virtual machines Hyper-V virtual machines	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Cloudamize: Cloud Assessment	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Turbonomic: Turbonomic	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 UnifyCloud: CloudRecon	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 D42 Device42: Device42	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	Learn more

Note: Visit the ISV tool's website to learn more about tool capabilities.
Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#)

Skip adding an assessment tool for now

9. In **Select migration tool**, select **Skip adding a migration tool for now** > **Next**.
10. In **Review + add tools**, review the settings, and click **Add tools**.
11. Wait a few minutes for the Azure Migrate project to deploy. You'll be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

Set up the appliance

Azure Migrate: Server Assessment runs a lightweight appliance.

- This appliance performs physical server discovery and sends server metadata and performance data to Azure Migrate Server Assessment.
- To set up the appliance you:
 - Download a zipped file with Azure Migrate installer script from the Azure portal.
 - Extract the contents from the zipped file. Launch the PowerShell console with administrative privileges.
 - Execute the PowerShell script to launch the appliance web application.
 - Configure the appliance for the first time, and register it with the Azure Migrate project.
- You can set up multiple appliances for a single Azure Migrate project. Across all appliances, you can discover any number of physical servers. A maximum of 250 servers can be discovered per appliance.

Download the installer script

Download the zipped file for the appliance.

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines > Are your machines virtualized?**, click **Not virtualized/Other**.
3. Click **Download** to download the zipped file.

Home > Azure Migrate - Servers > Discover machines

Discover machines

[Discover using appliance](#) Import using CSV

Are your machines virtualized? Not virtualized / Other

To discover your on-premises environment, you will need to deploy the Azure Migrate appliance. Follow the steps below to setup and configure the appliance. Once set up, this appliance remains connected to Azure Migrate, and performs continuous discovery of your on-premises environment.

The discovery requires access credentials to the physical servers you want to discover. The discovery will also collect performance counters that can be used for performance-based assessments.

 **1: Download Azure Migrate appliance**
The Azure Migrate appliance enables you to discover your on-premises machines. Use this PowerShell script to set up the appliance. Download the zipped folder to proceed.

[Download](#) .zip file. 50MB

 **Run the script to set up the appliance**
Before you start, ensure these [prerequisites](#) are met. Run the script to deploy the appliance configuration manager either on a virtual machine or a physical server.

 **3: Configure the appliance and and start discovery from web browser**
Access the appliance configuration UI from your browser by going to the IP address of the machine (in your network). Complete the process to initiate the discovery.

 **Wait for the appliance to be connected, discovery to be completed, performance data to be collected.**
About 15 minutes after you start discovery, the migration overview dashboard will show the machines discovered. You can then proceed with assessments or migrations.

Verify security

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following command to generate the hash for the zipped file

- `C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]`
- Example usage: `C:\>CertUtil -HashFile C:\Users\administrator\Desktop\AzureMigrateInstaller.zip SHA256`

3. For the latest appliance version, the generated hash should match these settings.

ALGORITHM	HASH VALUE
MD5	1e92ede3e87c03bd148e56a708cdd33f
SHA256	a3fa78edc8ff8aff9ab5ae66be1b64e66de7b9f475b6542beef1 14b20bfdac3c

Run the Azure Migrate installer script

The installer script does the following:

- Installs agents and a web application for physical server discovery and assessment.
- Install Windows roles, including Windows Activation Service, IIS, and PowerShell ISE.
- Download and installs an IIS rewritable module. [Learn more](#).
- Updates a registry key (HKLM) with persistent setting details for Azure Migrate.
- Creates the following files under the path:
 - **Config Files:** %ProgramData%\Microsoft Azure\Config
 - **Log Files:** %ProgramData%\Microsoft Azure\Logs

Run the script as follows:

1. Extract the zipped file to a folder on the server that will host the appliance.
2. Launch PowerShell on the above server with administrative (elevated) privilege.
3. Change the PowerShell directory to the folder where the contents have been extracted from the downloaded zipped file.
4. Run the script named **AzureMigrateInstaller.ps1** by running the following command:

```
PS C:\Users\administrator\Desktop\AzureMigrateInstaller> AzureMigrateInstaller.ps1
```

The script will launch the appliance web application when it finishes successfully.

In case of any issues, you can access the script logs at C:\ProgramData\Microsoft Azure\Logs\AzureMigrateScenarioInstaller_.Timestamp.log for troubleshooting.

NOTE

Please do not execute the Azure Migrate installer script on an existing Azure Migrate appliance.

Verify appliance access to Azure

Make sure that the appliance can connect to [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time.

1. Open a browser on any machine that can connect to the appliance, and open the URL of the appliance web app: **https://appliance name or IP address: 44368**.

Alternately, you can open the app from the desktop by clicking the app shortcut.

2. In the web app > **Set up prerequisites**, do the following:

- **License**: Accept the license terms, and read the third-party information.
- **Connectivity**: The app checks that the server has internet access. If the server uses a proxy:
 - Click **Proxy settings**, and specify the proxy address and listening port, in the form http://ProxyIPAddress or http://ProxyFQDN.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
- **Time sync**: Time is verified. The time on the appliance should be in sync with internet time for server discovery to work properly.
- **Install updates**: Azure Migrate Server Assessment checks that the appliance has the latest updates installed.

Register the appliance with Azure Migrate

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
 - Sign in with your username and password.
 - Sign-in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

Start continuous discovery

Now, connect from the appliance to the physical servers to be discovered, and start the discovery.

1. Click **Add Credentials** to specify the account credentials that the appliance will use to discover servers.
2. Specify the **Operating System**, friendly name for the credentials, **Username** and **Password** and click **Add**. You can add one set of credentials each for Windows and Linux servers.
3. Click **Add server**, and specify server details- FQDN/IP address and friendly name of credentials (one entry per row) to connect to the server.
4. Click **Validate**. After validation, the list of servers that can be discovered is shown.
 - If validation fails for a server, review the error by hovering over the icon in the **Status** column. Fix issues, and validate again.
 - To remove a server, select > **Delete**.
5. After validation, click **Save and start discovery** to start the discovery process.

This starts discovery. It takes around 1.5 minutes per server for metadata of discovered server to appear in the Azure portal.

Verify servers in the portal

After discovery, you can verify that the servers appear in the Azure portal.

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers > Azure Migrate: Server Assessment** page, click the icon that displays the count for **Discovered servers**.

Set up an assessment

There are two types of assessments you can create using Azure Migrate: Server Assessment.

ASSESSMENT	DETAILS	DATA
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.
As on-premises	Assessments based on on-premises sizing.	Recommended VM size: Based on the on-premises server size Recommended disk type: Based on the storage type setting you select for the assessment.

Run an assessment

Run an assessment as follows:

1. Review the [best practices](#) for creating assessments.
2. In the **Servers** tab, in **Azure Migrate: Server Assessment** tile, click **Assess**.

Azure Migrate - Servers

Microsoft

Search (Ctrl+ /)

Overview

Migration goals

Servers

Databases

Data Box

Manage

Discovered items

Support + troubleshooting

New support request

Last refreshed details for migrate project <project name> <time>

Assessment tools

Azure Migrate: Server Assessment

Discover Assess Overview

	Discovered servers	5271
	Groups	3
	Assessments	3
	Notifications	2 critical

Next step: You can refine your application grouping with dependency analysis

Add more assessment tools? [Click here.](#)

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with links like Overview, Migration goals, Servers, Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The Servers link is currently selected. On the right, under 'Assessment tools', there's a section titled 'Azure Migrate: Server Assessment'. It has three tabs: Discover, Assess (which is highlighted with a red box), and Overview. Below the tabs is a table with four rows: Discovered servers (5271), Groups (3), Assessments (3), and Notifications (2 critical). At the bottom of this section, there's a tooltip: 'Next step: You can refine your application grouping with dependency analysis'. At the very bottom of the dashboard, there's a link 'Add more assessment tools? Click here.'

3. In **Assess servers**, specify a name for the assessment.
4. Click **View all** to review the assessment properties.

Assessment properties



You can also edit these properties later by opening the **assessment** and clicking on '**Edit properties**' command on top

TARGET PROPERTIES

Target location

North Europe

Storage type

Automatic

Reserved instances

3 years reserved

VM SIZE

Sizing criterion

Performance-based

Performance history

1 Day

Percentile utilization

95th

Save

Discard

5. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more servers together for assessment.
6. In **Add machines to the group**, select servers to add to the group.
7. Click **Create Assessment** to create the group, and run the assessment.

Home > Azure Migrate - Servers > Assess servers

Assess servers

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

Discovery source: Machines discovered from Azure Migrate appliance

Assessment name: *

Enter the assessment name

Assessment properties (Showing 3 of 13) [View all](#)

Migration target location	: Southeast Asia
Sizing criterion	: Performance-based
Reserved instances	: 3 years reserved

Select or create a group

Create New Use Existing

Enter the group name

Add machines to the group

Appliance name: 2 selected

Select all Clear selection Search to filter machines

Name	IP address
FTA-W2K12STD-01	2404:f801:4800:25:19f5:f3bf:ccfe:85ab,10.150.14.14
el39-SL11Sp3-1	10.150.10.190,2404:f801:4800:25:250:56ff:feb7:8683
a404-r1w12r2-1	2404:f801:4800:25:48b:6eac:cc2fc00,10.150.14.224
MicrosoftAzureMigration	2404:f801:4800:25:698e:17d1:39c0:15a2,10.150.13.165
a922_rhel5u10-3	10.150.88.174,2404:f801:4800:a:250:56ff:feb7:9b3a,2404:f801:4800:20:250:56...
MAMApp	2404:f801:4800:25:35e0:4d4c:1a09:b08f,10.150.13.73

Create assessment

8. After the assessment is created, view it in **Servers > Azure Migrate: Server Assessment > Assessments**.
9. Click **Export assessment**, to download it as an Excel file.

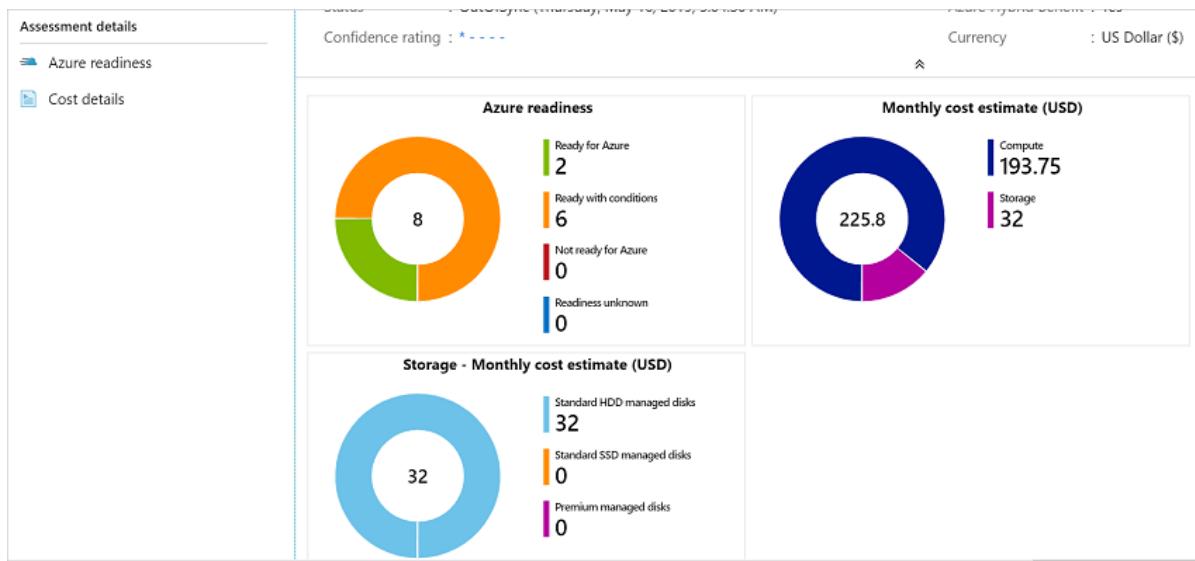
Review an assessment

An assessment describes:

- **Azure readiness:** Whether servers are suitable for migration to Azure.
- **Monthly cost estimation:** The estimated monthly compute and storage costs for running the servers in Azure.
- **Monthly storage cost estimation:** Estimated costs for disk storage after migration.

View an assessment

1. In **Migration goals > Servers**, click **Assessments** in **Azure Migrate: Server Assessment**.
2. In **Assessments**, click on an assessment to open it.



Review Azure readiness

1. In **Azure readiness**, verify whether the servers are ready for migration to Azure.
2. Review the status:
 - **Ready for Azure:** Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
 - **Ready with conditions:** Shows issues and suggested remediation.
 - **Not ready for Azure:** Shows issues and suggested remediation.
 - **Readiness unknown:** Used when Azure Migrate can't assess readiness, due to data availability issues.
3. Click on an **Azure readiness** status. You can view server readiness details, and drill down to see server details, including compute, storage, and network settings.

Review cost details

This view shows the estimated compute and storage cost of running VMs in Azure.

1. Review the monthly compute and storage costs. Costs are aggregated for all servers in the assessed group.
 - Cost estimates are based on the size recommendations for a machine, and its disks and properties.
 - Estimated monthly costs for compute and storage are shown.
 - The cost estimation is for running the on-premises servers as IaaS VMs. Azure Migrate Server Assessment doesn't consider PaaS or SaaS costs.
2. You can review monthly storage cost estimates. This view shows aggregated storage costs for the assessed group, split over different types of storage disks.
3. You can drill down to see details for specific servers.

Review confidence rating

When you run performance-based assessments, a confidence rating is assigned to the assessment.

Assess servers	Columns						
Search to filter assessments							
NAME	GROUP	STATUS	MACHINES	LOCATION	SIZING CRITERION	CONFIDENCE RATING	
assessment_5_16_2019_17_34_29	day2	OutOfSync	0	North Europe	Performance-based	★★★★★	
assessment_5_20_2019_17_42_6	Mygroup	Ready	6	North Europe	Performance-based	★★★★★	
assessment_5_22_2019_22_56_13	Day2-group	OutDated	14	North Europe	Performance-based	★★★★★	

- A rating from 1-star (lowest) to 5-star (highest) is awarded.
- The confidence rating helps you estimate the reliability of the size recommendations provided by the assessment.
- The confidence rating is based on the availability of data points needed to compute the assessment.

Confidence ratings for an assessment are as follows.

DATA POINT AVAILABILITY	CONFIDENCE RATING
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

[Learn more](#) about best practices for confidence ratings.

Next steps

In this tutorial, you:

- Set up an Azure Migrate appliance
- Created and reviewed an assessment

Continue to the third tutorial in the series, to learn how to migrate physical servers to Azure with Azure Migrate: Server Migration.

[Migrate physical servers](#)

This article shows you how to migrate machines as physical servers to Azure, using the Azure Migrate:Server Migration tool. Migrating machines by treating them as physical servers is useful in a number of scenarios:

- Migrate on-premises physical servers.
- Migrate VMs virtualized by platforms such as Xen, KVM.
- Migrate Hyper-V or VMware VMs, if for some reason you're unable to use the standard migration process for [Hyper-V](#), or [VMware](#) migration.
- Migrate VMs running in private clouds.
- Migrate VMs running in public clouds such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).

[Azure Migrate](#) provides a central hub to track discovery, assessment and migration of your on-premises apps and workloads, and cloud VM instances, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

In this tutorial, you learn how to:

- Prepare Azure for migration with the Azure Migrate Server Migration tool.
- Check requirements for machines you want to migrate, and prepare a machine for the Azure Migrate replication appliance that's used to discover and migrate machines to Azure.
- Add the Azure Migrate Server Migration tool in the Azure Migrate hub.
- Set up the replication appliance.
- Install the Mobility service on machines you want to migrate.
- Enable replication.
- Run a test migration to make sure everything's working as expected.
- Run a full migration to Azure.

NOTE

Tutorials show you the simplest deployment path for a scenario so that you can quickly set up a proof-of-concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-tos for Azure Migrate.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

Before you begin this tutorial, you should:

1. [Review](#) the migration architecture.
2. Make sure that your Azure account is assigned the Virtual Machine Contributor role, so that you have permissions to:
 - Create a VM in the selected resource group.
 - Create a VM in the selected virtual network.
 - Write to an Azure managed disk.
3. [Set up an Azure network](#). When you replicate to Azure, Azure VMs are created, and joined to an Azure

network you specify when you set up migration.

Prepare Azure

Set up Azure permissions before you can migrate with Azure Migrate Server Migration.

- **Create a project:** Your Azure account needs permissions to create an Azure Migrate project.

Assign permissions to create project

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and click it to view permissions.
3. You should have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Prepare for migration

Check machine requirements for migration

Make sure machines comply with requirements for migration to Azure.

NOTE

Agent-based migration with Azure Migrate Server Migration, has the same replication architecture as the agent based disaster recovery feature of the Azure Site Recovery service, and some of the components used share the same code base. Some requirements might link to Site Recovery documentation.

1. [Verify](#) physical server requirements.
2. Verify VM settings. On-premises machines that you replicate to Azure must comply with [Azure VM requirements](#).

Prepare a machine for the replication appliance

Azure Migrate Server Migration uses a replication appliance to replicate machines to Azure. The replication appliance runs the following components.

- **Configuration server:** The configuration server coordinates communications between on-premises and Azure, and manages data replication.
- **Process server:** The process server acts as a replication gateway. It receives replication data; optimizes it with caching, compression, and encryption, and sends it to a cache storage account in Azure.

Before you start, you need to prepare a Windows Server 2016 machine to host the replication appliance. The machine should comply with [these requirements](#). The appliance shouldn't be installed on a source machine you want to protect.

Add the Azure Migrate Server Migration tool

Set up an Azure Migrate project, and then add the Azure Migrate Server Migration tool to it.

1. In the Azure portal > **All services**, search for **Azure Migrate**.
2. Under **Services**, select **Azure Migrate**.
3. In **Overview**, click **Assess and migrate servers**.
4. Under **Discover, assess and migrate servers**, click **Assess and migrate servers**.

The screenshot shows the Azure Migrate service interface. On the left, there's a sidebar with navigation links like Overview, Migration goals (Servers, Databases, Data Box), Manage (Discovered items), Support + troubleshooting, and New support request. The main area has a title "Migrate your on-premises datacenter to Azure" with a subtitle "Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or find an expert to help with your migration. Learn more". Below this are three sections: "Discover, assess and migrate servers" (with a red box around it), "Discover, assess and migrate databases", and "Assess and migrate web apps to Azure". Each section has a brief description and a "Assess and migrate [category]" button.

5. In **Discover, assess and migrate servers**, click **Add tools**.
6. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
7. In **Project Details**, specify the project name, and geography in which you want to create the project, and click **Next**

The screenshot shows the "Add a tool" page. At the top, there are tabs: "Migrate project" (selected), "Select assessment tool" (highlighted in blue), "Select migration tool", and "Review + add tool(s)". Below the tabs, there's a note about a migrate project and how to select a subscription and resource group. The "Subscription" field is set to "<subscription-name>" and the "Resource group" field is set to "ContosoCorporation" with a "Create new" link. Under "PROJECT DETAILS", there are fields for "Migrate project" (set to "Contoso-project") and "Region" (set to "(Asia Pacific) Southeast Asia").

You can create an Azure Migrate project in any of these geographies.

GEOGRAPHY	REGION
Asia	Southeast Asia
Europe	North Europe or West Europe
United States	East US or West Central US

The geography specified for the project is only used to store the metadata gathered from on-premises VMs. You can select any target region for the actual migration.

8. In **Select assessment tool**, select **Skip adding an assessment tool for now > Next**.
9. In **Select migration tool**, select **Azure Migrate: Server Migration > Next**.
10. In **Review + add tools**, review the settings, and click **Add tools**

11. After adding the tool, it appears in the Azure Migrate project > Servers > Migration tools.

Set up the replication appliance

The first step of migration is to set up the replication appliance. You download the installer file for the appliance, and run it on the [machine you prepared](#). After installing the appliance, you register it with Azure Migrate Server Migration.

Download the replication appliance installer

1. In the Azure Migrate project > Servers, in Azure Migrate: Server Migration, click Discover.

The screenshot shows the Azure Migrate - Servers interface. On the left, there's a navigation sidebar with options like Overview, Migration goals (Servers selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area is divided into two sections: **Assessment tools** and **Migration tools**.

Assessment tools: Contains the "Azure Migrate: Server Assessment" section. It includes a "Discover" button (which is highlighted with a red box), an "Assess" button, and an "Overview" button. Below these are "Quick start" steps: "1: Discover" (Click 'Discover' to start discovering your on-premises machines) and "2: Assess" (Once your on-premises machines are discovered, click "Assess" to create assessments). At the bottom, there's a link "Add more assessment tools? [Click here.](#)"

Migration tools: Contains the "Azure Migrate: Server Migration" section. It includes "Discover", "Replicate", "Migrate", and "Overview" buttons. Below these are "Quick start" steps: "1: Discover" (Click 'Discover' to start discovering your on-premises machines), "2: Replicate" (Once your on-premises machines are discovered, click "Replicate" to start replicating the discovered machines), and "3: Migrate" (Once your machines have replicated, click "Migrate" to migrate your machines). At the bottom, there's a link "Add more migration tools? [Click here.](#)"

2. In Discover machines > Are your machines virtualized?, click Not virtualized/Other.
3. In Target region, select the Azure region to which you want to migrate the machines.

4. Select **Confirm** that the target region for migration is region-name.
5. Click **Create resources**. This creates an Azure Site Recovery vault in the background.
 - If you've already set up migration with Azure Migrate Server Migration, the target option can't be configured, since resources were set up previously.
 - You can't change the target region for this project after clicking this button.
 - All subsequent migrations are to this region.
6. In **Do you want to install a new replication appliance?**, select **Install a replication appliance**.
7. In **Download and install the replication appliance software**, download the appliance installer, and the registration key. You need to the key in order to register the appliance. The key is valid for five days after it's downloaded.

Discover machines

Are your machines virtualized? [?](#)
Not virtualized / Other

Target region [?](#)
(US) Central US

Do you want to install a new replication appliance or scale-out existing setup?
Install a replication appliance [Help me choose](#)

The replication appliance (Configuration Server) is a virtual appliance that is deployed on-premises. The replication appliance coordinates and manages replication for the servers that are being migrated. Follow the steps outlined below to set up and configure the replication appliance

1. Download and install the replication appliance software.
Create a new Windows Server 2016 machine by following the [Configuration Server sizing guidelines](#).
[Download](#) the replication appliance software installer and use it to complete installation of the replication appliance software on the newly created Windows Server 2016 machine.

2. Configure the replication appliance and register it to the Azure Migrate project
Download the registration key file and use it to register the replication appliance to this project. The replication appliance installer will ask for a registration key.
[Download](#)

8. Copy the appliance setup file and key file to the Windows Server 2016 machine you created for the appliance.
9. Run the replication appliance setup file, as described in the next procedure. After installation completes, the Appliance configuration wizard will be launched automatically (You can also launch the wizard manually by using the cspconfigtool shortcut that is created on the desktop of the appliance). Use the Manage Accounts tab of the wizard to add account details to use for push installation of the Mobility service. In this tutorial we'll be manually installing the Mobility Service on machines to be replicated, so create a dummy account in this step and proceed.
10. After the appliance has restarted after setup, in **Discover machines**, select the new appliance in **Select Configuration Server**, and click **Finalize registration**. Finalize registration performs a couple of final tasks to prepare the replication appliance.

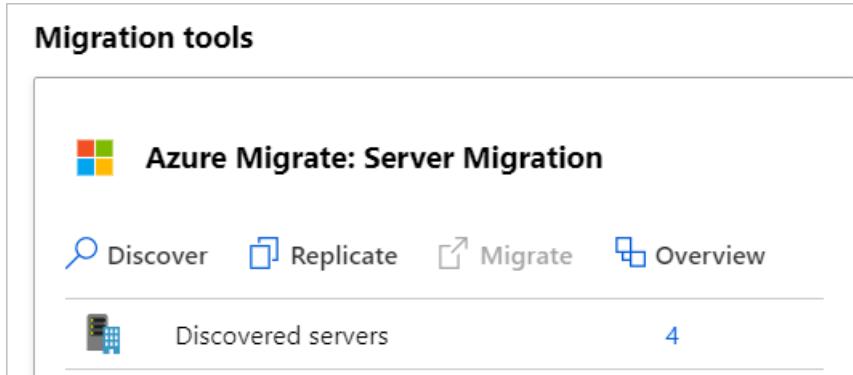
3. Finalize registration
Prepare for replication by finalizing registration for the replication appliance (Configuration Server). Select the replication appliance from the drop down to finalize registration for it.

* Select Configuration Server
WIN-DVHS6VQ9TRQ 

 Registration finalized

It may take some time after finalizing registration until discovered machines appear in Azure Migrate Server

Migration. As VMs are discovered, the **Discovered servers** count rises.



The screenshot shows the Azure Migrate: Server Migration interface. At the top, there's a navigation bar with four tabs: 'Discover' (selected), 'Replicate', 'Migrate', and 'Overview'. Below the tabs, there's a summary card with the text 'Discovered servers' and the number '4'.

Install the Mobility service

On machines you want to migrate, you need to install the Mobility service agent. The agent installers are available on the replication appliance. You find the right installer, and install the agent on each machine you want to migrate. Do this as follows:

1. Sign in to the replication appliance.
2. Navigate to `%ProgramData%\ASR\home\svsystems\pushinstallsvc\repository`.
3. Find the installer for the machine operating system and version. Review [supported operating systems](#).
4. Copy the installer file to the machine you want to migrate.
5. Make sure that you have the passphrase that was generated when you deployed the appliance.
 - Store the file in a temporary text file on the machine.
 - You can obtain the passphrase on the replication appliance. From the command line, run `C:\ProgramData\ASR\home\svsystems\bin\genpassphrase.exe -v` to view the current passphrase.
 - Don't regenerate the passphrase. This will break connectivity and you will have to reregister the replication appliance.

Install on Windows

1. Extract the contents of installer file to a local folder (for example C:\Temp) on the machine, as follows:

```
ren Microsoft-ASR_UA*Windows*release.exe MobilityServiceInstaller.exe  
MobilityServiceInstaller.exe /q /x:C:\Temp\Extracted  
cd C:\Temp\Extracted
```

2. Run the Mobility Service Installer:

```
UnifiedAgent.exe /Role "MS" /Silent
```

3. Register the agent with the replication appliance:

```
cd C:\Program Files (x86)\Microsoft Azure Site Recovery\agent  
UnifiedAgentConfigurator.exe /CSEndPoint <replication appliance IP address> /PassphraseFilePath  
<Passphrase File Path>
```

Install on Linux

1. Extract the contents of the installer tarball to a local folder (for example /tmp/MobSvlnstaller) on the machine, as follows:

```
mkdir /tmp/MobSvcInstaller  
tar -C /tmp/MobSvcInstaller -xvf <Installer tarball>  
cd /tmp/MobSvcInstaller
```

2. Run the installer script:

```
sudo ./install -r MS -q
```

3. Register the agent with the replication appliance:

```
/usr/local/ASR/Vx/bin/UnifiedAgentConfigurator.sh -i <replication appliance IP address> -P <Passphrase  
File Path>
```

Replicate machines

Now, select machines for migration.

NOTE

You can replicate up to 10 machines together. If you need to replicate more, then replicate them simultaneously in batches of 10.

1. In the Azure Migrate project > **Servers**, **Azure Migrate: Server Migration**, click **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with links for Overview, Migration goals (Servers selected), Databases, Data Box, Manage (Discoverd items), Support + troubleshooting (New support request), and a search bar. The main content area has two sections: 'Assessment tools' and 'Migration tools'. The 'Assessment tools' section contains a summary of discovered servers (442), groups (2), assessments (2), and notifications (0). It also includes a 'Next step' callout: 'Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. Below this is a link to 'Add more assessment tools? Click here.' The 'Migration tools' section contains a summary of discovered servers (442) and includes tabs for Discover, Replicate (highlighted with a red box), Migrate, and Overview.

Assessment tools

Azure Migrate: Server Assessment

Discover Assess Overview

	Discovered servers	442
	Groups	2
	Assessments	2
	Notifications	0

Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis

Add more assessment tools? [Click here.](#)

Migration tools

Azure Migrate: Server Migration

Discover **Replicate** Migrate Overview

	Discovered servers	442
--	--------------------	-----

2. In Replicate, > Source settings > Are your machines virtualized?, select Not virtualized/Other.
3. In On-premises appliance, select the name of the Azure Migrate appliance that you set up.
4. In Process Server, select the name of the replication appliance.
5. In Guest credentials, you specify a dummy account that will be used for installing the Mobility service manually (push install is not supported in Physical). Then click Next: Virtual machines.

Replicate

Source settings Virtual machines Target settings Compute Disks Review + Start replication

The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.

* Are your machines virtualized? [?](#)

* On-premises appliance [?](#)

* Process Server [?](#)

* Guest credentials [?](#)

6. In **Virtual Machines**, in **Import migration settings from an assessment?**, leave the default setting **No, I'll specify the migration settings manually**.

7. Check each VM you want to migrate. Then click **Next: Target settings**.

Source settings **Virtual machines** Target settings Compute Disks Review + Start replication

Select machines to replicate (Learn how to [discover non-virtualized/other machines](#) for server migration.)

* Import migration settings from an assessment? [?](#)

* Virtual machines [?](#)

NAME	IP ADDRESS	OPERATING SYSTEM	BOOT TYPE
<input checked="" type="checkbox"/> ContosoVMwareMigr...	2404:f801:4800:25:c95f:5fd3:7347:4f91,1...	Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoCSASR	2404:f801:4800:25:29f9:2ebd:1ee0:eeb4,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-FrontTier3		Microsoft Windows Server Threshold (64...)	bios
<input checked="" type="checkbox"/> ContosoWeb1	2404:f801:4800:25:9091:9912:5f46:9108,...	Microsoft Windows Server 2008 (32-bit)	bios
<input checked="" type="checkbox"/> Contoso-Configuratio...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> Contoso-AzureMigrat...		Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb3	10.150.13.218,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoAppSrv2	2404:f801:4800:25:5de5:e919:3448:be33,...	Microsoft Windows Server 2012 (64-bit)	bios
<input checked="" type="checkbox"/> ContosoWeb2	10.150.13.201,2404:f801:4800:25:250:56f...	CentOS 4/5/6/7 (64-bit)	bios

Selected items : 9

8. In **Target settings**, select the subscription, and target region to which you'll migrate, and specify the resource group in which the Azure VMs will reside after migration.

9. In **Virtual Network**, select the Azure VNet/subnet to which the Azure VMs will be joined after migration.

10. In **Azure Hybrid Benefit**:

- Select **No** if you don't want to apply Azure Hybrid Benefit. Then click **Next**.
- Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or

Windows Server subscriptions, and you want to apply the benefit to the machines you're migrating. Then click **Next**.

11. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).

- VM size:** By default, Azure Migrate Server Migration picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in [Azure VM size](#).
- OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
- Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.

NAME	AZURE VM NAME	SOURCE VM SIZE
ContosoVMwareMigration2	ContosoVMwareMigration2	8 Cores, 16384 MB RAM
ContosoCSASR	ContosoCSASR	2 Cores, 2048 MB RAM
Contoso-FrontTier3	Contoso-FrontTier3	8 Cores, 16384 MB RAM
ContosoWeb1	ContosoWeb1	2 Cores, 2048 MB RAM
Contoso-ConfigurationServer	Contoso-ConfigurationServer	8 Cores, 16384 MB RAM
Contoso-AzureMigrateAppliance	Contoso2	4 Cores, 8192 MB RAM
ContosoWeb3	ContosoWeb3	2 Cores, 2048 MB RAM
ContosoAppSrv2	ContosoAppSrv2	2 Cores, 4096 MB RAM
ContosoWeb2	ContosoWeb2	2 Cores, 2048 MB RAM

12. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium managed disks) in Azure. Then click **Next**.

- You can exclude disks from replication.
- If you exclude disks, won't be present on the Azure VM after migration.

Replicate	
Source settings	Virtual machines
Target settings	Compute
Disks	
Select the managed disk type to use for the disks of the migrated machine. Optionally, you may also choose to exclude certain disks from replication by unselecting them.	
NAME	DISKS TO REPLICATE
ContosoVMwareMigration2	All selected scsi0:0
ContosoCSASR	All selected scsi0:0
Contoso-FrontTier3	All selected scsi0:0
ContosoWeb1	All selected scsi0:0

13. In **Review and start replication**, review the settings, and click **Replicate** to start the initial replication for the servers.

NOTE

You can update replication settings any time before replication starts, **Manage > Replicating machines**. Settings can't be changed after replication starts.

Track and monitor

- When you click **Replicate** a Start Replication job begins.
- When the Start Replication job finishes successfully, the machines begin their initial replication to Azure.
- After initial replication finishes, delta replication begins. Incremental changes to on-premises disks are periodically replicated to the replica disks in Azure.

You can track job status in the portal notifications.

You can monitor replication status by clicking on **Replicating servers** in **Azure Migrate: Server Migration**.

Migration tools

Azure Migrate: Server Migration

+ Discover Replicate Migrate **Overview**

Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

Next step: You can start migrating the replicating servers to Azure

Run a test migration

When delta replication begins, you can run a test migration for the VMs, before running a full migration to Azure. We highly recommend that you do this at least once for each machine, before you migrate it.

- Running a test migration checks that migration will work as expected, without impacting the on-premises machines, which remain operational, and continue replicating.
- Test migration simulates the migration by creating an Azure VM using replicated data (usually migrating to a non-production VNet in your Azure subscription).
- You can use the replicated test Azure VM to validate the migration, perform app testing, and address any issues before full migration.

Do a test migration as follows:

1. In Migration goals > Servers > Azure Migrate: Server Migration, click **Test migrated servers**.

The screenshot shows the 'Migration tools' interface for Azure Migrate: Server Migration. At the top, there's a navigation bar with 'Discover', 'Replicate', 'Migrate', and 'Overview'. Below that is a summary table with four rows:

Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

A yellow lightning bolt icon with the text 'Next step: You can start migrating the replicating servers to Azure' is displayed below the table.

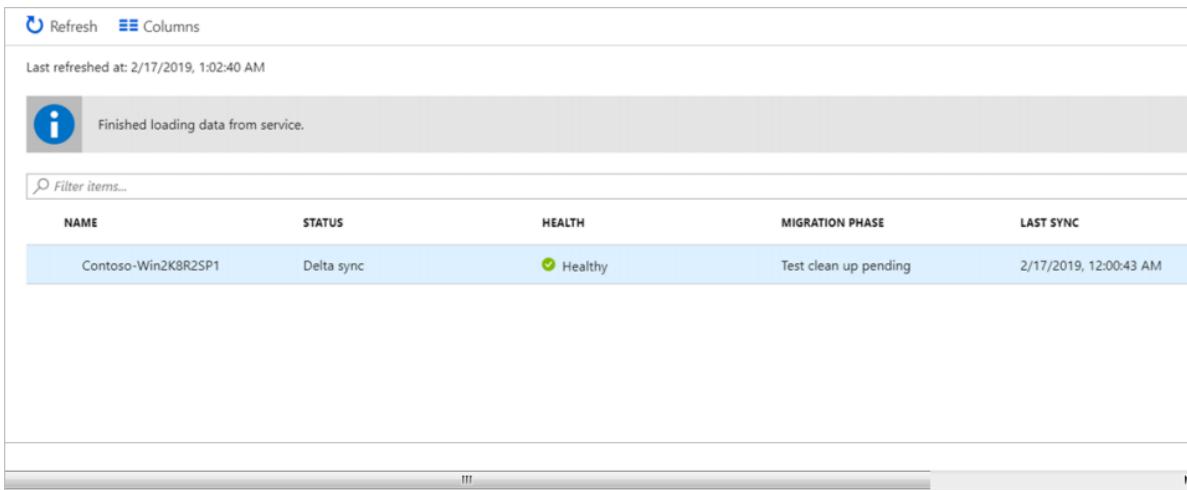
2. Right-click the VM to test, and click **Test migrate**.

The screenshot shows the 'Azure Migrate - Servers' blade. On the left, there's a sidebar with 'Overview', 'Getting started', 'Migrate servers to Azure', 'Manage', 'Replicating machines' (which is selected), 'Jobs', 'Events', 'Settings', and 'Properties'. The main area shows a message 'Finished loading data from service.' and a table of replicating machines:

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:4

3. In **Test Migration**, select the Azure VNet in which the Azure VM will be located after the migration. We recommend you use a non-production VNet.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.

- After the test is done, right-click the Azure VM in **Replicating machines**, and click **Clean up test migration**.



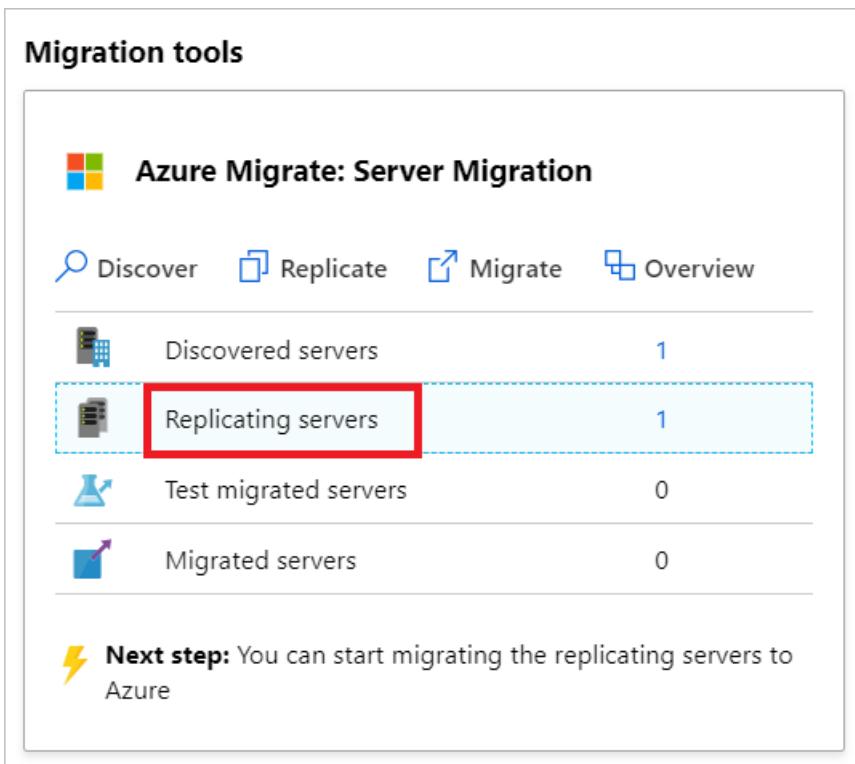
The screenshot shows a table titled 'Replicating machines' with the following columns: NAME, STATUS, HEALTH, MIGRATION PHASE, and LAST SYNC. There is one item listed:

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM

Migrate VMs

After you've verified that the test migration works as expected, you can migrate the on-premises machines.

- In the Azure Migrate project > **Servers** > **Azure Migrate: Server Migration**, click **Replicating servers**.



The screenshot shows the 'Migration tools' blade with the following sections:

- Azure Migrate: Server Migration** icon
- Discover**, **Replicate**, **Migrate**, **Overview** buttons
- Discovered servers**: 1
- Replicating servers**: 1 (This item is highlighted with a red box and a dashed blue border.)
- Test migrated servers**: 0
- Migrated servers**: 0
- Next step:** You can start migrating the replicating servers to Azure

- In **Replicating machines**, right-click the VM > **Migrate**.
- In **Migrate** > **Shut down virtual machines** and perform a planned migration with no data loss, select **Yes** > **OK**.
 - If you don't want to shut down the VM, select **No**

Note: For Physical Server Migration, the recommendation is to bring the application down as part of the migration window (don't let the applications accept any connections) and then initiate the migration (The server needs to be kept running, so remaining changes can be synchronized) before the migration is completed.
- A migration job starts for the VM. Track the job in Azure notifications.

5. After the job finishes, you can view and manage the VM from the [Virtual Machines](#) page.

Complete the migration

1. After the migration is done, right-click the VM > **Stop migration**. This does the following:
 - Stops replication for the on-premises machine.
 - Removes the machine from the **Replicating servers** count in Azure Migrate: Server Migration.
 - Cleans up replication state information for the machine.
2. Install the Azure VM [Windows](#) or [Linux](#) agent on the migrated machines.
3. Perform any post-migration app tweaks, such as updating database connection strings, and web server configurations.
4. Perform final application and migration acceptance testing on the migrated application now running in Azure.
5. Cut over traffic to the migrated Azure VM instance.
6. Remove the on-premises VMs from your local VM inventory.
7. Remove the on-premises VMs from local backups.
8. Update any internal documentation to show the new location and IP address of the Azure VMs.

Post-migration best practices

- For increased resilience:
 - Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](#).
 - Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery. [Learn more](#).
- For increased security:
 - Lock down and limit inbound traffic access with [Azure Security Center - Just in time administration](#).
 - Restrict network traffic to management endpoints with [Network Security Groups](#).
 - Deploy [Azure Disk Encryption](#) to help secure disks, and keep data safe from theft and unauthorized access.
 - Read more about [securing IaaS resources](#), and visit the [Azure Security Center](#).
- For monitoring and management:
 - Consider deploying [Azure Cost Management](#) to monitor resource usage and spending.

Next steps

Investigate the [cloud migration journey](#) in the Azure Cloud Adoption Framework.

Assess servers by using imported data

4/10/2020 • 10 minutes to read • [Edit Online](#)

This article explains how to assess on-premises servers with the [Azure Migrate: Server Assessment](#) tool, by importing server metadata in comma-separated values (CSV) format. This assessment method doesn't require you to set up the Azure Migrate appliance to create an assessment. It's useful if:

- You want to create a quick, initial assessment before you deploy the appliance.
- You can't deploy the Azure Migrate appliance in your organization.
- You can't share credentials that allow access to on-premises servers.
- Security constraints prevent you from gathering and sending data collected by the appliance to Azure. You can control the data you share in an imported file. Also, much of the data (for example, providing IP addresses) is optional.

Before you start

Be aware of these points:

- You can add up to a maximum of 20,000 servers in a single CSV file.
- You can add up to 20,000 servers in an Azure Migrate project by using CSV.
- You can upload server information to Server Assessment multiple times by using CSV.
- Gathering application information is useful in evaluating your on-premises environment for migration. However, Server Assessment doesn't currently perform application-level assessment or take applications into account when creating an assessment.

In this tutorial, you learn how to:

- Set up an Azure Migrate project.
- Fill in a CSV file with server information.
- Import the file to add server information into Server Assessment.
- Create and review an assessment.

NOTE

Tutorials show you the simplest deployment path for a scenario, so that you can quickly set up a proof of concept. Tutorials use default options where possible, and don't show all possible settings and paths. For detailed instructions, review the How-to guides.

If you don't have an Azure subscription, create a [free account](#) before you begin.

Set Azure permissions for Azure Migrate

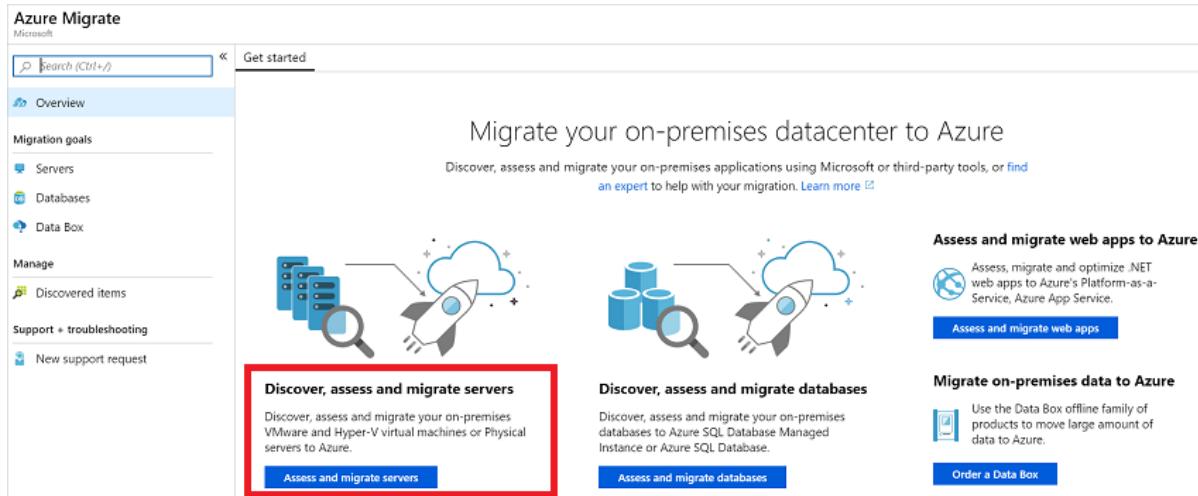
Your Azure account needs permissions to create an Azure Migrate project.

1. In the Azure portal, open the subscription, and select **Access control (IAM)**.
2. In **Check access**, find the relevant account, and then select it to view permissions.
3. Make sure you have **Contributor** or **Owner** permissions.
 - If you just created a free Azure account, you're the owner of your subscription.
 - If you're not the subscription owner, work with the owner to assign the role.

Set up an Azure Migrate project

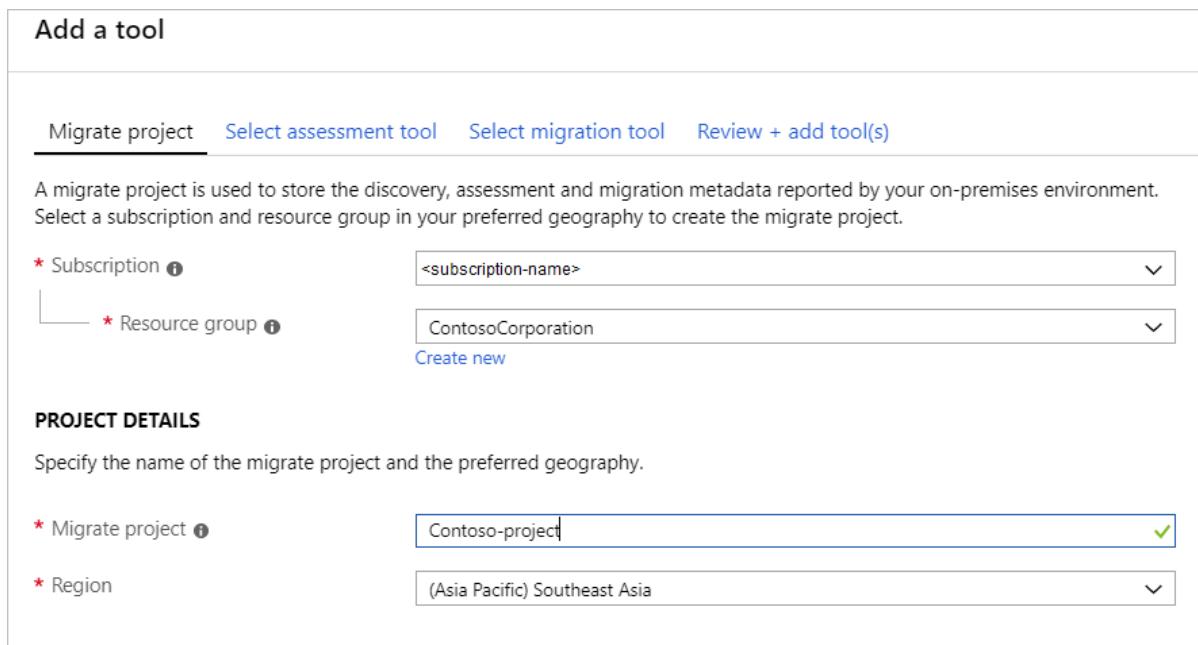
To set up a new Azure Migrate project:

1. In the Azure portal, in All services, search for Azure Migrate.
2. Under Services, select Azure Migrate.
3. In Overview, under Discover, assess and migrate servers, select Assess and migrate servers.



The screenshot shows the Azure Migrate service in the Azure portal. The left sidebar includes 'Overview', 'Migration goals' (Servers, Databases, Data Box), 'Manage' (Discovered items, Support + troubleshooting, New support request), and a search bar. The main area has a heading 'Migrate your on-premises datacenter to Azure' with a sub-instruction: 'Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or find an expert to help with your migration. Learn more'. It features three cards: 'Discover, assess and migrate servers' (with a red box around it and a blue 'Assess and migrate servers' button), 'Discover, assess and migrate databases', and 'Assess and migrate web apps to Azure' (with a blue 'Assess and migrate web apps' button). A fourth card, 'Migrate on-premises data to Azure' (with a blue 'Order a Data Box' button), is partially visible on the right.

4. In Getting started, select Add tool(s).
5. In Migrate project, select your Azure subscription, and create a resource group if you don't have one.
6. In PROJECT DETAILS, specify the project name and the geography in which you want to create the project.
For more information:
 - Review [supported geographies](#). The project geography is used only to store the metadata gathered from on-premises VMs.
 - You can select any target region when you run a migration.



The screenshot shows the 'Add a tool' step in the Azure Migrate setup wizard. At the top, there are tabs: 'Migrate project' (selected), 'Select assessment tool' (blue), 'Select migration tool', and 'Review + add tool(s)'. Below, it says: 'A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.' There are two dropdowns: 'Subscription' (set to 'ContosoCorporation') and 'Resource group' (set to 'ContosoCorporation'). Under 'PROJECT DETAILS', it says: 'Specify the name of the migrate project and the preferred geography.' There are two input fields: 'Migrate project' (set to 'Contoso-project') and 'Region' (set to '(Asia Pacific) Southeast Asia').

7. Select Next.
8. In Select assessment tool, select Azure Migrate: Server Assessment > Next.

Add a tool

Migrate project Select assessment tool Select migration tool Review + add tool(s)

Start by choosing a server discovery and assessment tool. We recommend that you discover and assess your datacenter to determine migration readiness.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
 Azure Migrate: Server Assessment	View	VMware virtual machines Hyper-V virtual machines	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Cloudamize: Cloud Assessment	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Corent Tech: SurPaaS MaaS	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Turbonomic: Turbonomic	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 UnifyCloud: CloudRecon	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	Learn more
 Device42: Device42	View	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	Learn more

Note: Visit the ISV tool's website to learn more about tool capabilities.
 Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#)

Skip adding an assessment tool for now

9. In **Select migration tool**, select **Skip adding a migration tool for now > Next**.
10. In **Review + add tools**, review the settings, and then select **Add tools**.
11. Wait a few minutes for the Azure Migrate project to deploy. You'll then be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

Prepare the CSV

Download the CSV template and add server information to it.

Download the template

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, select **Discover**.
2. In **Discover machines**, select **Import using CSV**.
3. Select **Download** to download the CSV template. Alternatively, you can [download it directly](#).

Home > Azure Migrate - Servers > Discover machines

Discover machines

[Discover using appliance](#) [Import using CSV](#)

Import your on-premises server inventory using a CSV file. You can use the imported inventory to create a quick assessment for migration to Azure.

(i) Use CSV import to get a quick assessment on cost and compatibility. For accurate assessments, use appliance-based discovery and profiling.

Steps to import using CSV.

- 1. Download CSV template.**
Download the template to import your on-premises server inventory. Learn more about the template here.
[Download](#) .CSV file
- 2. Add server inventory data in the CSV file.**
Populate the CSV template with your server inventory data.
Note: Fields marked with '*' in the header are mandatory to import the servers.
- 3. Import the CSV file.**
The file will be reviewed for errors and the servers will be added to the Azure Migrate project.
Note: Remediation guidance on failures will be added to the same file in additional columns titled 'Machine validation status' and 'Machine errors'.
Upload the CSV file (i)
 Select a file [Import](#)

Add server information

Gather server data and add it to the CSV file.

- To gather data, you can export it from tools you use for on-premises server management, such as VMware vSphere or your configuration-management database (CMDB).
- To review sample data, download our [example file](#).

The following table summarizes the file fields to fill in:

FIELD NAME	MANDATORY	DETAILS
Server name	Yes	We recommend specifying the fully qualified domain name (FQDN).
IP address	No	Server address.
Cores	Yes	Number of processor cores allocated to the server.
Memory	Yes	Total RAM, in MB, allocated to the server.
OS name	Yes	Server operating system. Operating system names that match or contain the names in this list are recognized by the assessment.
OS version	No	Server operating system version.
Number of disks	No	Not needed if individual disk details are provided.

FIELD NAME	MANDATORY	DETAILS
Disk 1 size	No	Maximum size of disk, in GB. You can add details for more disks by adding columns in the template. You can add up to eight disks.
Disk 1 read ops	No	Disk read operations per second.
Disk 1 write ops	No	Disk write operations per second.
Disk 1 read throughput	No	Data read from the disk per second, in MB per second.
Disk 1 write throughput	No	Data written to disk per second, in MB per second.
CPU utilization percentage	No	Percentage of CPU used.
Memory utilization percentage	No	Percentage of RAM used.
Total disks read ops	No	Disk-read operations per second.
Total disks write ops	No	Disk-write operations per second.
Total disks read throughput	No	Data read from the disk, in MB per second.
Total disks write throughput	No	Data written to disk, in MB per second.
Network In throughput	No	Data received by the server, in MB per second.
Network Out throughput	No	Data transmitted by the server, in MB per second.
Firmware type	No	Server firmware. Values can be "BIOS" or "UEFI".
No	Server MAC address.	

Add operating systems

Assessment recognizes specific operating system names. Any name you specify must exactly match one of the strings in the [supported names list](#).

Add multiple disks

The template provides default fields for the first disk. You can add similar columns for up to eight disks.

For example, to specify all fields for a second disk, add these columns:

- Disk 2 size
- Disk 2 read ops
- Disk 2 write ops
- Disk 2 read throughput

- Disk 2 write throughput

Import the server information

After adding information to the CSV template, import the servers into Server Assessment.

1. In Azure Migrate, in **Discover machines**, go to the completed template.
2. Select **Import**.
3. The import status is shown.
 - If warnings appear in the status, you can either fix them or continue without addressing them.
 - To improve assessment accuracy, improve the server information as suggested in warnings.
 - To view and fix warnings, select **Download warning details .CSV**. This operation downloads the CSV with warnings included. Review the warnings and fix issues as needed.
 - If errors appear in the status so that the import status is **Failed**, you must fix those errors before you can continue with the import:
 - a. Download the CSV, which now includes error details.
 - b. Review and address the errors as necessary.
 - c. Upload the modified file again.
4. When the import status is **Completed**, the server information has been imported.

Update server information

You can update the information for a server by importing the data for the server again with the same **Server name**. You can't modify the **Server name** field. Deleting servers is currently not supported.

Verify servers in the portal

To verify that the servers appear in the Azure portal after discovery:

1. Open the Azure Migrate dashboard.
2. On the **Azure Migrate - Servers > Azure Migrate: Server Assessment** page, select the icon that displays the count for **Discovered servers**.
3. Select the **Import based** tab.

Set up and run an assessment

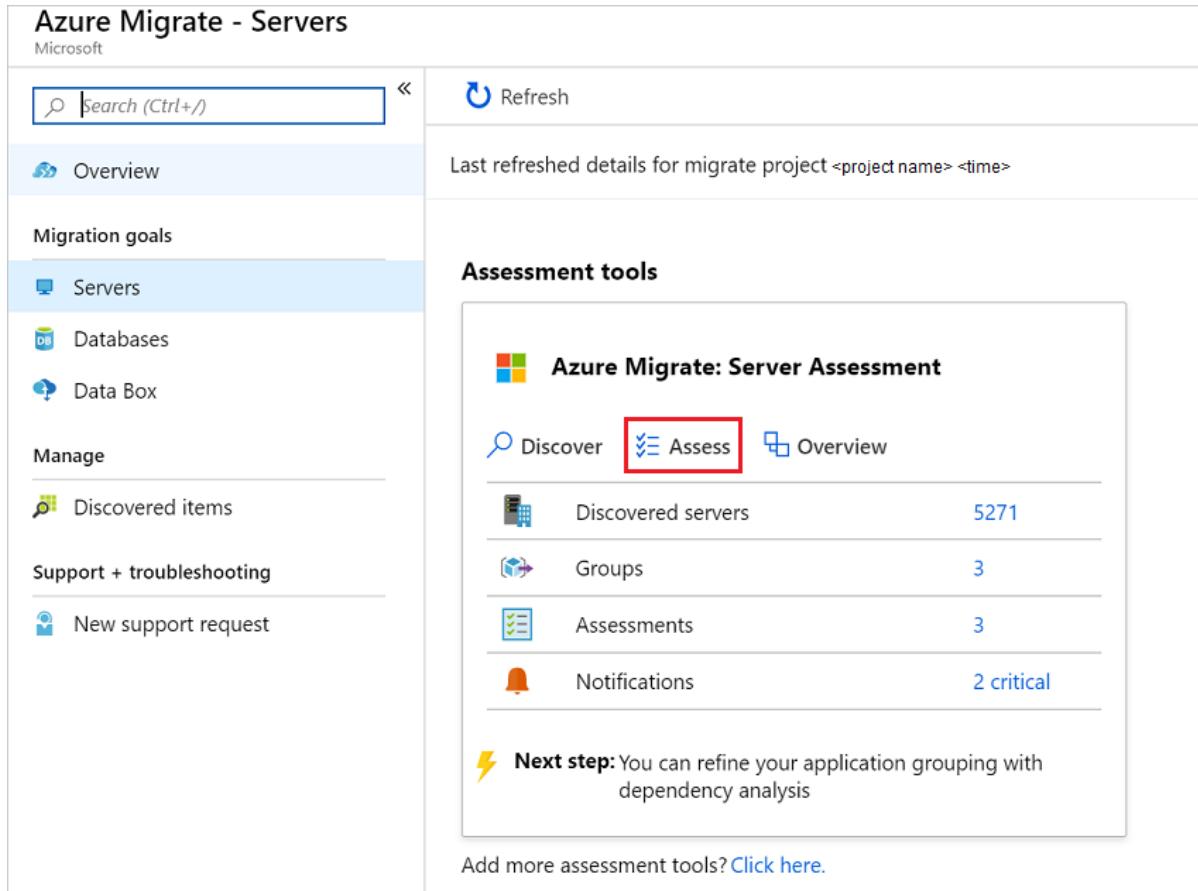
You can create two types of assessments by using Server Assessment.

ASSESSMENT TYPE	DETAILS	DATA
Performance-based	Assessments based on performance-data values specified.	<p>Recommended VM size: Based on CPU and memory usage data.</p> <p>Recommended disk type (standard or premium managed disk): Based on the input/output per second (IOPS) and throughput of the on-premises disks.</p>

ASSESSMENT TYPE	DETAILS	DATA
As on-premises	Assessments based on on-premises sizing.	<p>Recommended VM size: Based on the server size specified.</p> <p>Recommended disk type: Based on the storage-type setting you select for the assessment.</p>

To run an assessment:

1. Review the [best practices](#) for creating assessments.
2. In the Servers tab, in the Azure Migrate: Server Assessment tile, select Assess.



The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with navigation links: Overview, Migration goals, Servers (which is selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area is titled "Assessment tools". It features a card for "Azure Migrate: Server Assessment" with three tabs: Discover (blue), Assess (red, highlighted with a red box), and Overview (blue). Below the tabs, there are four metrics: Discovered servers (5271), Groups (3), Assessments (3), and Notifications (2 critical). A callout box says: "Next step: You can refine your application grouping with dependency analysis". At the bottom of the card, it says "Add more assessment tools? Click here.".

3. In **Assess servers**, specify a name for the assessment.
4. In **Discovery source**, select **Machines added via import to Azure Migrate**.
5. Select **View all** to review the assessment properties.

Assessment properties



You can also edit these properties later by opening the **assessment** and clicking on '**Edit properties**' command on top

TARGET PROPERTIES

Target location

North Europe

Storage type

Automatic

Reserved instances

3 years reserved

VM SIZE

Sizing criterion

Performance-based

Performance history

1 Day

Percentile utilization

95th

Save

Discard

6. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more VMs together for assessment.
7. In **Add machines to the group**, select servers to add to the group.
8. Select **Create assessment** to create the group, and then run the assessment.

Home > Azure Migrate - Servers > Assess servers

Assess servers

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

Discovery source: Machines discovered from Azure Migrate appliance

Assessment name *: Enter the assessment name

Assessment properties (Showing 3 of 13) [View all](#)

Migration target location	: Southeast Asia
Sizing criterion	: Performance-based
Reserved instances	: 3 years reserved

Select or create a group

Create New Use Existing

Enter the group name

Add machines to the group

Appliance name: 2 selected

Select all Clear selection Search to filter machines

Name	IP address
FTA-W2K12STD-01	2404:f801:4800:25:19f5:f3bf:ccfe:85ab,10.150.14.14
el39-SL11Sp3-1	10.150.10.190,2404:f801:4800:25:250:56ff:feb7:8683
a404-r1w12r2-1	2404:f801:4800:25:48b:6eac:cc2f:c00,10.150.14.224
MicrosoftAzureMigration	2404:f801:4800:25:698e:17d1:39c0:15a2,10.150.13.165
a922_rhel5u10-3	10.150.88.174,2404:f801:4800:a:250:56ff:feb7:9b3a,2404:f801:4800:20:250:56...
MAMApp	2404:f801:4800:25:35e0:4d4c:1a09:b08f,10.150.13.73

[Create assessment](#)

9. After the assessment is created, view it in **Servers > Azure Migrate: Server Assessment > Assessments**.

10. Select **Export assessment** to download it as a Microsoft Excel file.

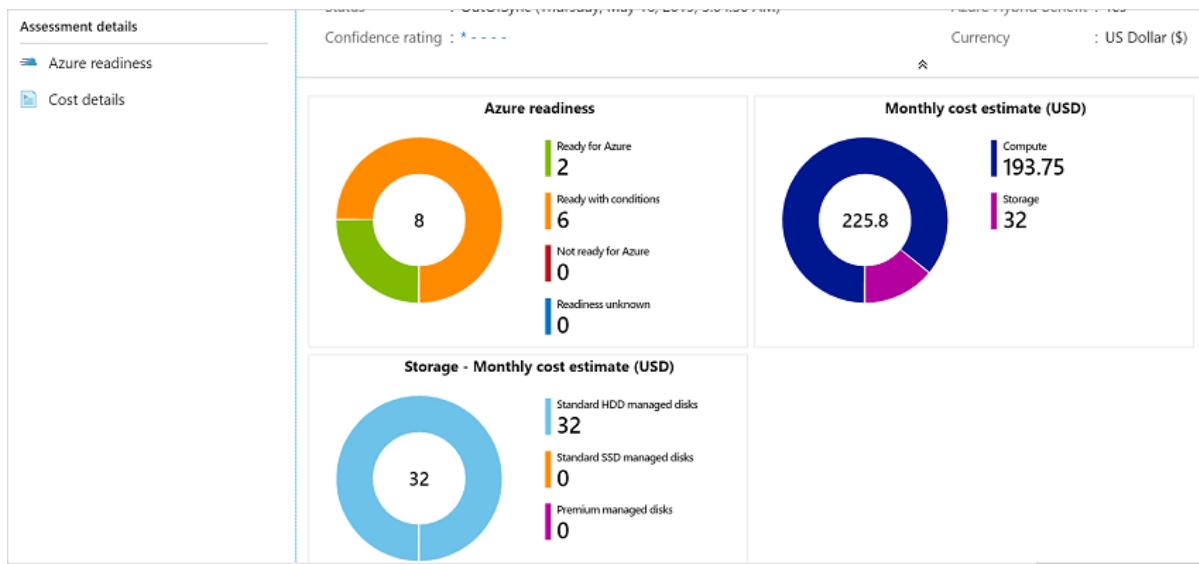
Review an assessment

An assessment describes:

- **Azure readiness:** Whether servers are suitable for migration to Azure.
- **Monthly cost estimation:** Estimated monthly compute and storage costs for running the servers in Azure.
- **Monthly storage cost estimation:** Estimated costs for disk storage after migration.

View an assessment

1. In **Migration goals > Servers**, select **Assessments** in **Azure Migrate: Server Assessment**.
2. In **Assessments**, select an assessment to open it.



Review Azure readiness

- In **Azure readiness**, determine whether the servers are ready for migration to Azure.
- Review the status:
 - Ready for Azure:** Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
 - Ready with conditions:** Shows problems and suggested remediation.
 - Not ready for Azure:** Shows problems and suggested remediation.
 - Readiness unknown:** Azure Migrate can't assess readiness, due to data-availability issues.
- Select an **Azure readiness** status. You can view server-readiness details and drill down to see server details, including compute, storage, and network settings.

Review cost details

This view shows the estimated compute and storage cost of running VMs in Azure. You can:

- Review the monthly compute and storage costs. Costs are aggregated for all servers in the assessed group.
 - Cost estimates are based on the size recommendations for a machine, and its disks and properties.
 - Estimated monthly costs for compute and storage are shown.
 - The cost estimate is for running the on-premises servers as infrastructure-as-a-service (IaaS) VMs. Server Assessment doesn't consider platform-as-a-service (PaaS) or software-as-a-service (SaaS) costs.
- Review monthly storage-cost estimates. This view shows aggregated storage costs for the assessed group, split among different types of storage disks.
- Drill down to see details for specific VMs.

NOTE

Confidence ratings are not assigned to assessments of servers imported into Server Assessment by using CSV.

Supported operating system names

A - H

Apple Mac OS X 10

Asianux 3

Asianux 4

Asianux 5

CentOS

CentOS 4/5

CoreOS Linux

Debian GNU/Linux 4

Debian GNU/Linux 5

Debian GNU/Linux 6

Debian GNU/Linux 7

Debian GNU/Linux 8

FreeBSD

I - R

IBM OS/2

MS-DOS

Novell NetWare 5

Novell NetWare 6

Oracle Linux

Oracle Linux 4/5

Oracle Solaris 10

Oracle Solaris 11

Red Hat Enterprise Linux 2

Red Hat Enterprise Linux 3

Red Hat Enterprise Linux 4

Red Hat Enterprise Linux 5

Red Hat Enterprise Linux 6

Red Hat Enterprise Linux 7

Red Hat Fedora

S - T

SCO OpenServer 5

SCO OpenServer 6

SCO UnixWare 7

Serenity Systems eComStation 1

Serenity Systems eComStation 2

Sun Microsystems Solaris 8

Sun Microsystems Solaris 9

SUSE Linux Enterprise 10

SUSE Linux Enterprise 11

SUSE Linux Enterprise 12

SUSE Linux Enterprise 8/9

SUSE Linux Enterprise 11

SUSE openSUSE

U - Z

Ubuntu Linux

VMware ESXi 4

VMware ESXi 5

VMware ESXi 6

Windows 10

Windows 2000

Windows 3

Windows 7

Windows 8

Windows 95

Windows 98

Windows NT

Windows Server (R) 2008

Windows Server 2003

Windows Server 2008

Windows Server 2008 R2

Windows Server 2012

Windows Server 2012 R2

Windows Server 2016

Windows Server 2019

Windows Server Threshold

Windows Vista

Windows Web Server 2008 R2

Windows XP Professional

Next steps

In this tutorial, you:

- Imported servers into Azure Migrate: Server Assessment by using CSV.
- Created and reviewed an assessment.

Now, [deploy an appliance](#) for more accurate assessments, and gather servers together into groups for deeper assessment by using [dependency analysis](#).

Azure Migrate support matrix

3/23/2020 • 5 minutes to read • [Edit Online](#)

You can use the [Azure Migrate service](#) to assess and migrate machines to the Microsoft Azure cloud. This article summarizes general support settings and limitations for Azure Migrate scenarios and deployments.

Supported assessment/migration scenarios

The table summarizes supported discovery, assessment, and migration scenarios.

DEPLOYMENT	DETAILS
App-specific discovery	You can discover apps, roles, and features running on VMware VMs. Currently this feature is limited to discovery only. Assessment is currently at the machine level. We don't yet offer app, role, or feature-specific assessment.
On-premises assessment	Assess on-premises workloads and data running on VMware VMs, Hyper-V VMs, and physical servers. Assess using Azure Migrate Server Assessment and Microsoft Data Migration Assistant (DMA), as well as other tools and ISV offerings.
On-premises migration to Azure	Migrate workloads and data running on physical servers, VMware VMs, Hyper-V VMs, physical servers, and cloud-based VMS to Azure. Migrate using Azure Migrate Server Assessment and Azure Database Migration Service (DMS), and well as other tools and ISV offerings.

Supported tools

Specific tool support is summarized in the table.

TOOL	ASSESS	MIGRATE
Azure Migrate Server Assessment	Assess VMware VMs , Hyper-V VMs , and physical servers .	Not available (NA)
Azure Migrate Server Migration	NA	Migrate VMware VMs , Hyper-V VMs , and physical servers .
Carbonite	NA	Migrate VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.
Cloudamize	Assess VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.	NA
Corent Technology	Assess and migrate VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.	Migrate VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.
Device 42	Assess VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.	NA

TOOL	ASSESS	MIGRATE
DMA	Assess on-premises SQL Server databases.	NA
DMS	NA	Migrate SQL Server, Oracle, MySQL, PostgreSQL, MongoDB.
Lakeside	Assess virtual desktop infrastructure (VDI)	NA
Movere	Assess VMWare VMs, Hyper-V VMs, Xen VMs, physical machines, workstations (including VDI), public cloud workloads	NA
RackWare	NA	Migrate VMWare VMs, Hyper-V VMs, Xen VMs, KVM VMs, physical machines, public cloud workloads
Turbonomic	Assess VMware VMs, Hyper-V VMs, physical servers, public cloud workloads.	NA
UnifyCloud	Assess VMware VMs, Hyper-V VMs, physical servers, public cloud workloads, and SQL Server databases.	NA
Webapp Migration Assistant	Assess web apps	Migrate web apps.

Azure Migrate projects

SUPPORT	DETAILS
Subscription	You can have multiple Azure Migrate projects in a subscription.
Azure permissions	You need Contributor or Owner permissions in the subscription to create an Azure Migrate project.
VMware VMs	Assess up to 35,000 VMware VMs in a single project.
Hyper-V VMs	Assess up to 35,000 Hyper-V VMs in a single project.

A project can include both VMware VMs and Hyper-V VMs, up to the assessment limits.

Azure permissions

For Azure Migrate to work with Azure you need these permissions before you start assessing and migrating machines.

TASK	PERMISSIONS	DETAILS
Create an Azure Migrate project	Your Azure account needs permissions to create a project.	Set up for VMware , Hyper-V , or physical servers .

Task	Permissions	Details
Register the Azure Migrate appliance	<p>Azure Migrate uses a lightweight Azure Migrate appliance to assess machines with Azure Migrate Server Assessment, and to run agentless migration of VMware VMs with Azure Migrate Server Migration. This appliance discovers machines, and sends metadata and performance data to Azure Migrate.</p> <p>During registration, register providers (Microsoft.OffAzure, Microsoft.Migrate and Microsoft.KeyVault) are registered with the subscription chosen in the appliance, so that the subscription works with the resource provider. To register, you need Contributor or Owner access on the subscription.</p> <p>VMware-During onboarding, Azure Migrate creates two Azure Active Directory (Azure AD) apps. The first app communicates between the appliance agents and the Azure Migrate service. The app doesn't have permissions to make Azure resource management calls or have RBAC access for resources. The second app accesses an Azure Key Vault created in the user subscription for agentless VMware migration only. In agentless migration, Azure Migrate creates a Key Vault to manage access keys to the replication storage account in your subscription. It has RBAC access on the Azure Key Vault (in the customer tenant) when discovery is initiated from the appliance.</p> <p>Hyper-V-During onboarding, Azure Migrate creates one Azure AD app. The app communicates between the appliance agents and the Azure Migrate service. The app doesn't have permissions to make Azure resource management calls or have RBAC access for resources.</p>	Set up for VMware , Hyper-V , or physical servers .
Create a key vault for VMware agentless migration	To migrate VMware VMs with agentless Azure Migrate Server Migration, Azure Migrate creates a Key Vault to manage access keys to the replication storage account in your subscription. To create the vault, you set permissions (Owner, or Contributor and User Access Administrator) on the resource group in which the Azure Migrate project resides.	Set up permissions.

Supported geographies

You can create an Azure Migrate project in a number of geographies. Although you can only create projects in these

geographies, you can assess or migrate machines for other target locations. The project geography is only used to store the discovered metadata.

GEOGRAPHY	METADATA STORAGE LOCATION
Azure Government	US Gov Virginia
Asia Pacific	East Asia or Southeast Asia
Australia	Australia East or Australia Southeast
Brazil	Brazil South
Canada	Canada Central or Canada East
Europe	North Europe or West Europe
France	France Central
India	Central India or South India
Japan	Japan East or Japan West
Korea	Korea Central or Korea South
United Kingdom	UK South or UK West
United States	Central US or West US 2

NOTE

Support for Azure Government is currently only available for the [older version](#) of Azure Migrate.

VMware assessment and migration

[Review the Azure Migrate Server Assessment and Server Migration support matrix for VMware VMs.](#)

Hyper-V assessment and migration

[Review the Azure Migrate Server Assessment and Server Migration support matrix for Hyper-V VMs.](#)

Azure Migrate versions

There are two versions of the Azure Migrate service:

- **Current version:** Using this version you can create new Azure Migrate projects, discover on-premises assesses, and orchestrate assessments and migrations. [Learn more](#).
- **Previous version:** For customer using the previous version of Azure Migrate (only assessment of on-premises VMware VMs was supported), you should now use the current version. In the previous version, you can't create new Azure Migrate projects or perform new discoveries.

Next steps

- [Assess VMware VMs](#) for migration.
- [Assess Hyper-V VMs](#) for migration.

Support matrix for VMware assessment

3/30/2020 • 7 minutes to read • [Edit Online](#)

This article summarizes prerequisites and support requirements when you assess VMware VMs for migration to Azure, using the Azure Migrate:Server Assessment](migrate-services-overview.md#azure-migrate-server-assessment-tool) tool. If you want to migrate VMware VMs to Azure, review the [migration support matrix](#).

To assess VMware VMs, you create an Azure Migrate project, and then add the Server Assessment tool to the project. After the tool is added, you deploy the [Azure Migrate appliance](#). The appliance continuously discovers on-premises machines, and sends machine metadata and performance data to Azure. After discovery is complete, you gather discovered machines into groups, and run an assessment for a group.

Limitations

SUPPORT	DETAILS
Project limits	You can create multiple projects in an Azure subscription. You can discover and assess up to 35,000 VMware VMs in a single project . A project can also include physical servers, and Hyper-V VMs, up to the assessment limits for each.
Discovery	The Azure Migrate appliance can discover up to 10,000 VMware VMs on a vCenter Server.
Assessment	You can add up to 35,000 machines in a single group. You can assess up to 35,000 VMs in a single assessment.

[Learn more](#) about assessments.

Application discovery

In addition to discovering machines, Server Assessment can discover apps, role, and features running on machines. Discovering your app inventory allows you to identify and plan a migration path tailored for your on-premises workloads.

SUPPORT	DETAILS
Supported machines	App discovery is currently supported for VMware VMs only.
Discovery	App discovery is agentless. It uses machine guest credentials, and remotely accesses machines using WMI and SSH calls.
VM support	App-discovery is supported for all Windows and Linux versions.
vCenter credentials	App discovery needs a vCenter Server account with read-only access, and privileges enabled for Virtual Machines > Guest Operations.

SUPPORT	DETAILS
VM credentials	App discovery currently supports the use of one credential for all Windows servers, and one credential for all Linux servers.
	You create a guest user account for Windows VMs, and a regular/normal user account (non-sudo access) for all Linux VMs.
VMware tools	VMware tools must be installed and running on VMs you want to discover. The VMware tools version must be later than 10.2.0.
PowerShell	VMs must have PowerShell version 2.0 or later installed.
Port access	On ESXi hosts running VMs you want to discover, the Azure Migrate appliance must be able to connect to TCP port 443.
Limits	For app-discovery, you can discover up to 10000 VMs on each Azure Migrate appliance.

VMware requirements

VMWARE	DETAILS
VMware VMs	Assessment is supported for all Windows and Linux operating systems.
vCenter Server	Machines you want to discovery and assess must be managed by vCenter Server version 5.5, 6.0, 6.5, or 6.7.
Permissions (assessment)	vCenter Server read-only account.
Permissions (app-discovery)	vCenter Server account with read-only access, and privileges enabled for Virtual machines > Guest Operations .
Permissions (dependency visualization)	Center Server account with read-only access, and privileges enabled for Virtual machines > Guest Operations .

Azure Migrate appliance requirements

Azure Migrate uses the [Azure Migrate appliance](#) for discovery and assessment. You can deploy the appliance as a VMWare VM using an OVA template, imported into vCenter Server, or using a [PowerShell script](#).

- Learn about [appliance requirements](#) for VMware.
- Learn about [URLs](#) the appliance needs to access.

Port access

DEVICE	CONNECTION

DEVICE	CONNECTION
Appliance	<p>Inbound connections on TCP port 3389 to allow remote desktop connections to the appliance.</p> <p>Inbound connections on port 44368 to remotely access the appliance management app using the URL: <code>https://<appliance-ip-or-name>:44368</code></p> <p>Outbound connections on port 443 (HTTPS), to send discovery and performance metadata to Azure Migrate.</p>
vCenter server	<p>Inbound connections on TCP port 443 to allow the appliance to collect configuration and performance metadata for assessments.</p> <p>The appliance connects to vCenter on port 443 by default. If the vCenter server listens on a different port, you can modify the port when you set up discovery.</p>
ESXi hosts (app discovery/agentless dependency analysis)	If you want to do app discovery or agentless dependency analysis , then the appliance connects to ESXi hosts on TCP port 443, to discover applications, to and run agentless dependency visualization on VMs.

Agentless dependency analysis requirements

[Dependency analysis](#) helps you to identify dependencies between on-premises machines that you want to assess and migrate to Azure. The table summarizes the requirements for setting up agentless dependency analysis.

REQUIREMENT	DETAILS
Before deployment	<p>You should have an Azure Migrate project in place, with the Server Assessment tool added to the project.</p> <p>You deploy dependency visualization after setting up an Azure Migrate appliance to discover your on-premises VMWare machines.</p> <p>Learn how to create a project for the first time. Learn how to add an assessment tool to an existing project. Learn how to set up the Azure Migrate appliance for assessment of VMware VMs.</p>
VM support	Currently supported for VMware VMs only.
Windows VMs	Windows Server 2016 Windows Server 2012 R2 Windows Server 2012 Windows Server 2008 R2 (64-bit).
Windows account	For dependency analysis, the Azure Migrate appliance needs a local or a domain Administrator account to access Windows VMs.

Requirement	Details
Linux VMs	Red Hat Enterprise Linux 7, 6, 5 Ubuntu Linux 14.04, 16.04 Debian 7, 8 Oracle Linux 6, 7 CentOS 5, 6, 7.
Linux account	For dependency analysis, on Linux machines the Azure Migrate appliance needs a user account with Root privilege. Alternately, the user account needs these permissions on /bin/netstat and /bin/ls files: CAP_DAC_READ_SEARCH and CAP_SYS_PTRACE.
Required agents	No agent required on machines you want to analyze.
VMware Tools	VMware Tools (later than 10.2) must be installed and running on each VM you want to analyze.
vCenter Server credentials	Dependency visualization needs a vCenter Server account with read-only access, and privileges enabled for Virtual Machines > Guest Operations.
PowerShell	VMs must have PowerShell version 2.0 or above installed.
Port access	On ESXi hosts running VMs you want to analyze, the Azure Migrate appliance must be able to connect to TCP port 443.

Agent-based dependency analysis requirements

Dependency analysis helps you to identify dependencies between on-premises machines that you want to assess and migrate to Azure. The table summarizes the requirements for setting up agent-based dependency analysis.

Requirement	Details
Before deployment	You should have an Azure Migrate project in place, with the Azure Migrate: Server Assessment tool added to the project. You deploy dependency visualization after setting up an Azure Migrate appliance to discover your on-premises machines Learn how to create a project for the first time. Learn how to add an assessment tool to an existing project. Learn how to set up the Azure Migrate appliance for assessment of Hyper-V , VMware , or physical servers.
Azure Government	Dependency visualization isn't available in Azure Government.

Requirement	Details
Log Analytics	<p>Azure Migrate uses the Service Map solution in Azure Monitor logs for dependency visualization.</p> <p>You associate a new or existing Log Analytics workspace with an Azure Migrate project. The workspace for an Azure Migrate project can't be modified after it's added.</p> <p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>The workspace must reside in the East US, Southeast Asia, or West Europe regions. Workspaces in other regions can't be associated with a project.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>In Log Analytics, the workspace associated with Azure Migrate is tagged with the Migration Project key, and the project name.</p>
Required agents	<p>On each machine you want to analyze, install the following agents:</p> <p>The Microsoft Monitoring agent (MMA). The Dependency agent.</p> <p>If on-premises machines aren't connected to the internet, you need to download and install Log Analytics gateway on them.</p> <p>Learn more about installing the Dependency agent and MMA.</p>
Log Analytics workspace	<p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>Azure Migrate supports workspaces residing in the East US, Southeast Asia, and West Europe regions.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>The workspace for an Azure Migrate project can't be modified after it's added.</p>

Requirement	Details
Costs	<p>The Service Map solution doesn't incur any charges for the first 180 days (from the day that you associate the Log Analytics workspace with the Azure Migrate project)/</p> <p>After 180 days, standard Log Analytics charges will apply.</p> <p>Using any solution other than Service Map in the associated Log Analytics workspace will incur standard charges for Log Analytics.</p> <p>When the Azure Migrate project is deleted, the workspace is not deleted along with it. After deleting the project, Service Map usage isn't free, and each node will be charged as per the paid tier of Log Analytics workspace/</p> <p>If you have projects that you created before Azure Migrate general availability (GA- 28 February 2018), you might have incurred additional Service Map charges. To ensure payment after 180 days only, we recommend that you create a new project, since existing workspaces before GA are still chargeable.</p>
Management	<p>When you register agents to the workspace, you use the ID and key provided by the Azure Migrate project.</p> <p>You can use the Log Analytics workspace outside Azure Migrate.</p> <p>If you delete the associated Azure Migrate project, the workspace isn't deleted automatically. Delete it manually.</p> <p>Don't delete the workspace created by Azure Migrate, unless you delete the Azure Migrate project. If you do, the dependency visualization functionality will not work as expected.</p>
Internet connectivity	<p>If machines aren't connected to the internet, you need to install the Log Analytics gateway on them.</p>

Next steps

- [Review](#) best practices for creating assessments.
- [Prepare for VMware](#) assessment.

Support matrix for VMware migration

3/5/2020 • 7 minutes to read • [Edit Online](#)

This article summarizes support settings and limitations for migrating VMware VMs with [Azure Migrate: Server Migration](#). If you're looking for information about assessing VMware VMs for migration to Azure, review the [assessment support matrix](#).

Migration options

You can migrate VMware VMs in a couple of ways:

- With agentless migration: Migrate VMs without needing to install anything on them. You deploy the [Azure Migrate appliance](#) for agentless migration.
- With agent-based migration: Install an agent on the VM for replication. For agent-based migration, you need to deploy a [replication appliance](#).

Review [this article](#) to figure out which method you want to use.

Migration limitations

- You can select up to 10 VMs at once for replication. If you want to migrate more machines, then replicate in groups of 10.
- For VMware agentless migration, you can run up to 100 replications simultaneously.

Agentless-VMware servers

VMWARE	DETAILS
VMware vCenter Server	Version 5.5, 6.0, 6.5, or 6.7.
VMware vSphere ESXI host	Version 5.5, 6.0, 6.5, or 6.7.

VMWARE	DETAILS
vCenter Server permissions	<p>Agentless migration uses the Migrate Appliance. The appliance needs these permissions:</p> <ul style="list-style-type: none"> - Datastore.Browse: Allow browsing of VM log files to troubleshoot snapshot creation and deletion. - Datastore.LowLevelFileOperations: Allow read/write/delete/rename operations in the datastore browser, to troubleshoot snapshot creation and deletion. - VirtualMachine.Configuration.DiskChangeTracking: Allow enable or disable change tracking of VM disks, to pull changed blocks of data between snapshots. - VirtualMachine.Configuration.DiskLease: Allow disk lease operations for a VM, to read the disk using the VMware vSphere Virtual Disk Development Kit (VDDK). - VirtualMachine.Provisioning.AllowDiskAccess: (specifically for vSphere 6.0 and above) Allow opening a disk on a VM for random read access on the disk using the VDDK. - VirtualMachine.Provisioning.AllowReadOnlyDiskAccess: Allow opening a disk on a VM, to read the disk using the VDDK. - VirtualMachine.Provisioning.AllowDiskRandomAccess: Allow opening a disk on a VM, to read the disk using the VDDK. - VirtualMachine.Provisioning.AllowVirtualMachineDownload: Allows read operations on files associated with a VM, to download the logs and troubleshoot if failure occurs. - VirtualMachine.SnapshotManagement.*: Allow creation and management of VM snapshots for replication. - Virtual Machine.Interaction.Power Off: Allow the VM to be powered off during migration to Azure.

Agentless-VMware VMs

SUPPORT	DETAILS
Supported operating systems	Windows and Linux operating systems that are supported by Azure can be migrated using agentless migration.

SUPPORT	DETAILS
Required changes for Azure	<p>Some VMs might require changes so that they can run in Azure. Azure Migrate makes these changes automatically for the following operating systems:</p> <ul style="list-style-type: none"> - Red Hat Enterprise Linux 6.5+, 7.0+ - CentOS 6.5+, 7.0+ - SUSE Linux Enterprise Server 12 SP1+ - Ubuntu 14.04LTS, 16.04LTS, 18.04LTS - Debian 7, 8 <p>For other operating systems, you need to make adjustments manually before migration. The relevant articles contain instructions about how to do this.</p>
Linux boot	If /boot is on a dedicated partition, it should reside on the OS disk, and not be spread across multiple disks. If /boot is part of the root (/) partition, then the "/" partition should be on the OS disk, and not span other disks.
UEFI boot	VMs with UEFI boot aren't supported for migration.
Disk size	2 TB OS disk; 4 TB for data disks.
Disk limits	Up to 60 disks per VM.
Encrypted disks/volumes	VMs with encrypted disks/volumes aren't supported for migration.
Shared disk cluster	Not supported.
Independent disks	Not supported.
RDM/passthrough disks	If VMs have RDM or passthrough disks, these disks won't be replicated to Azure.
NFS	NFS volumes mounted as volumes on the VMs won't be replicated.
iSCSI targets	VMs with iSCSI targets aren't supported for agentless migration.
Multipath IO	Not supported.
Storage vMotion	Not supported. Replication won't work if a VM uses storage vMotion.
Teamed NICs	Not supported.
IPv6	Not supported.
Target disk	VMs can only be migrated to managed disks (standard HDD, premium SSD) in Azure.
Simultaneous replication	100 VMs per vCenter Server. If you have more, migrate them in batches of 100.

Agentless-Azure Migrate appliance

Agentless migration uses the Azure Migrate appliance, deployed on a VMware VM.

- Learn about [appliance requirements](#) for VMware.
- Learn about [URLs](#) the appliance needs to access.

Agentless-ports

DEVICE	CONNECTION
Appliance	Outbound connections on port 443 to upload replicated data to Azure, and to communicate with Azure Migrate services orchestrating replication and migration.
vCenter server	Inbound connections on port 443 to allow the appliance to orchestrate replication - create snapshots, copy data, release snapshots
vSphere/ESXI host	Inbound on TCP port 902 for the appliance to replicate data from snapshots.

Agent-based-VMware servers

This table summarizes assessment support and limitations for VMware virtualization servers.

VMWARE REQUIREMENTS	DETAILS
VMware vCenter Server	Version 5.5, 6.0, 6.5, or 6.7.
VMware vSphere ESXI host	Version 5.5, 6.0, 6.5, or 6.7.
vCenter Server permissions	A read-only account for vCenter Server.

Agent-based-VMware VMs

The table summarizes VMware VM support for VMware VMs you want to migrate using agent-based migration.

SUPPORT	DETAILS
Machine workload	Azure Migrate supports migration of any workload (say Active Directory, SQL server, etc.) running on a supported machine.
Operating systems	For the latest information, review the operating system support for Site Recovery. Azure Migrate provides identical VM operating system support.
Linux file system/guest storage	For the latest information, review the Linux file system support for Site Recovery. Azure Migrate has identical Linux file system support.
Network/Storage	For the latest information, review the network and storage prerequisites for Site Recovery. Azure Migrate provides identical network/storage requirements.

SUPPORT	DETAILS
Azure requirements	For the latest information, review the Azure network, storage, and compute requirements for Site Recovery. Azure Migrate has identical requirements for VMware migration.
Mobility service	The Mobility service agent must be installed on each VM you want to migrate.
UEFI boot	The migrated VM in Azure will be automatically converted to a BIOS boot VM. The OS disk should have up to four partitions, and volumes should be formatted with NTFS.
Target disk	VMs can only be migrated to managed disks (standard HDD, premium SSD) in Azure.
Disk size	2 TB OS disk; 8 TB for data disks.
Disk limits	Up to 63 disks per VM.
Encrypted disks/volumes	VMs with encrypted disks/volumes aren't supported for migration.
Shared disk cluster	Not supported.
Independent disks	Supported.
Passthrough disks	Supported.
NFS	NFS volumes mounted as volumes on the VMs won't be replicated.
iSCSI targets	VMs with iSCSI targets aren't supported for agentless migration.
Multipath IO	Not supported.
Storage vMotion	Supported
Teamed NICs	Not supported.
IPv6	Not supported.

Agent-based-replication appliance

When you set up the replication appliance using the OVA template provided in the Azure Migrate hub, the appliance runs Windows Server 2016 and complies with the support requirements. If you set up the replication appliance manually on a physical server, then make sure that it complies with the requirements.

- Learn about [replication appliance requirements](#) for VMware.
- MySQL must be installed on the appliance. Learn about [installation options](#).
- Learn about [URLs](#) and [ports](#) the replication appliance needs to access.

Agent-based-ports

DEVICE	CONNECTION
VMs	<p>The Mobility service running on VMs communicates with the on-premises replication appliance (configuration server) on port HTTPS 443 inbound, for replication management.</p> <p>VMs send replication data to the process server (running on the configuration server machine) on port HTTPS 9443 inbound. This port can be modified.</p>
Replication appliance	The replication appliance orchestrates replication with Azure over port HTTPS 443 outbound.
Process server	<p>The process server receives replication data, optimizes, and encrypts it, and sends it to Azure storage over port 443 outbound.</p> <p>By default the process server runs on the replication appliance.</p>

Azure VM requirements

All on-premises VMs replicated to Azure must meet the Azure VM requirements summarized in this table. When Site Recovery runs a prerequisites check for replication, the check will fail if some of the requirements aren't met.

COMPONENT	REQUIREMENTS	DETAILS
Guest operating system	Verifies supported VMware VM operating systems for migration. You can migrate any workload running on a supported operating system.	Check fails if unsupported.
Guest operating system architecture	64-bit.	Check fails if unsupported.
Operating system disk size	Up to 2,048 GB.	Check fails if unsupported.
Operating system disk count	1	Check fails if unsupported.
Data disk count	64 or less.	Check fails if unsupported.
Data disk size	Up to 4,095 GB	Check fails if unsupported.
Network adapters	Multiple adapters are supported.	
Shared VHD	Not supported.	Check fails if unsupported.
FC disk	Not supported.	Check fails if unsupported.
BitLocker	Not supported.	BitLocker must be disabled before you enable replication for a machine.

Component	Requirements	Details
VM name	<p>From 1 to 63 characters. Restricted to letters, numbers, and hyphens.</p> <p>The machine name must start and end with a letter or number.</p>	Update the value in the machine properties in Site Recovery.
Connect after migration-Windows	<p>To connect to Azure VMs running Windows after migration:</p> <ul style="list-style-type: none"> - Before migration enables RDP on the on-premises VM. Make sure that TCP, and UDP rules are added for the Public profile, and that RDP is allowed in Windows Firewall > Allowed Apps, for all profiles. <p>For site-to-site VPN access, enable RDP and allow RDP in Windows Firewall - > Allowed apps and features for Domain and Private networks. In addition, check that the operating system's SAN policy is set to OnlineAll.</p> <p>Learn more.</p>	
Connect after migration-Linux	<p>To connect to Azure VMs after migration using SSH:</p> <p>Before migration, on the on-premises machine, check that the Secure Shell service is set to Start, and that firewall rules allow an SSH connection.</p> <p>After failover, on the Azure VM, allow incoming connections to the SSH port for the network security group rules on the failed over VM, and for the Azure subnet to which it's connected. In addition, add a public IP address for the VM.</p>	

Next steps

Select a VMware migration option.

Support matrix for Hyper-V assessment

3/30/2020 • 5 minutes to read • [Edit Online](#)

This article summarizes prerequisites and support requirements when you assess Hyper-V VMs for migration to Azure, using the [Azure Migrate:Server Assessment](#) tool. If you want to migrate Hyper-V VMs to Azure, review the [migration support matrix](#).

To set up Hyper-V VM assessment, you create an Azure Migrate project, and add the Server Assessment tool to the project. After the tool is added, you deploy the [Azure Migrate appliance](#). The appliance continuously discovers on-premises machines, and sends machine metadata and performance data to Azure. After discovery is complete, you gather discovered machines into groups, and run an assessment for a group.

Limitations

SUPPORT	DETAILS
Assessment limits	You can discover and assess up to 35,000 Hyper-V VMs in a single Azure Migrate project .
Project limits	You can create multiple projects in an Azure subscription. In addition to Hyper-V VMs, a project can include VMware VMs and physical servers, up to the assessment limits for each.
Discovery	The Azure Migrate appliance can discover up to 5000 Hyper-V VMs. The appliance can connect to up to 300 Hyper-V hosts.
Assessment	You can add up to 35,000 machines in a single group. You can assess up to 35,000 VMs in a single assessment for a group.

[Learn more](#) about assessments.

Hyper-V host requirements

SUPPORT	DETAILS
Hyper-V host	The Hyper-V host can be standalone, or deployed in a cluster. The Hyper-V host can run Windows Server 2019, Windows Server 2016, or Windows Server 2012 R2. You can't assess VMs located on Hyper-V hosts running Windows Server 2012.
Permissions	You need Administrator permissions on the Hyper-V host. If you don't want to assign Administrator permissions, create a local or domain user account, and add the user account to these groups- Remote Management Users, Hyper-V Administrators, and Performance Monitor Users.

SUPPORT	DETAILS
PowerShell remoting	PowerShell remoting must be enabled on each Hyper-V host.
Hyper-V Replica	If you use Hyper-V Replica (or you have multiple VMs with the same VM identifiers), and you discover both the original and replicated VMs using Azure Migrate, the assessment generated by Azure Migrate might not be accurate.

Hyper-V VM requirements

SUPPORT	DETAILS
Operating system	All Windows and Linux operating systems.
Integration Services	Hyper-V Integration Services must be running on VMs that you assess, in order to capture operating system information.

Azure Migrate appliance requirements

Azure Migrate uses the [Azure Migrate appliance](#) for discovery and assessment. You can deploy the appliance using a compressed Hyper-V VHD that you download from the portal, or using a [PowerShell script](#).

- Learn about [appliance requirements](#) for Hyper-V.
- Learn about [URLs](#) the appliance needs to access.

Port access

The following table summarizes port requirements for assessment.

DEVICE	CONNECTION
Appliance	<p>Inbound connections on TCP port 3389 to allow remote desktop connections to the appliance.</p> <p>Inbound connections on port 44368 to remotely access the appliance management app using the URL: <code>https://<appliance-ip-or-name>:44368</code></p> <p>Outbound connections on ports 443 (HTTPS), to send discovery and performance metadata to Azure Migrate.</p>
Hyper-V host/cluster	Inbound connections on WinRM ports 5985 (HTTP) and 5986 (HTTPS), to pull metadata and performance data for Hyper-V VMs using a Common Information Model (CIM) session.

Agent-based dependency analysis requirements

[Dependency analysis](#) helps you to identify dependencies between on-premises machines that you want to assess and migrate to Azure. The table summarizes the requirements for setting up agent-based dependency analysis. Hyper-V currently only supports agent-based dependency visualization.

Requirement	Details
Before deployment	<p>You should have an Azure Migrate project in place, with the Server Assessment tool added to the project.</p> <p>You deploy dependency visualization after setting up an Azure Migrate appliance to discover your on-premises machines</p> <p>Learn how to create a project for the first time. Learn how to add an assessment tool to an existing project. Learn how to set up the Azure Migrate appliance for assessment of Hyper-V VMs.</p>
Azure Government	<p>Dependency visualization isn't available in Azure Government.</p>
Log Analytics	<p>Azure Migrate uses the Service Map solution in Azure Monitor logs for dependency visualization.</p> <p>You associate a new or existing Log Analytics workspace with an Azure Migrate project. The workspace for an Azure Migrate project can't be modified after it's added.</p> <p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>The workspace must reside in the East US, Southeast Asia, or West Europe regions. Workspaces in other regions can't be associated with a project.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>In Log Analytics, the workspace associated with Azure Migrate is tagged with the Migration Project key, and the project name.</p>
Required agents	<p>On each machine you want to analyze, install the following agents:</p> <p>The Microsoft Monitoring agent (MMA). The Dependency agent.</p> <p>If on-premises machines aren't connected to the internet, you need to download and install Log Analytics gateway on them.</p> <p>Learn more about installing the Dependency agent and MMA.</p>
Log Analytics workspace	<p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>Azure Migrate supports workspaces residing in the East US, Southeast Asia, and West Europe regions.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>The workspace for an Azure Migrate project can't be modified after it's added.</p>

Requirement	Details
Costs	<p>The Service Map solution doesn't incur any charges for the first 180 days (from the day that you associate the Log Analytics workspace with the Azure Migrate project)/</p> <p>After 180 days, standard Log Analytics charges will apply.</p> <p>Using any solution other than Service Map in the associated Log Analytics workspace will incur standard charges for Log Analytics.</p> <p>When the Azure Migrate project is deleted, the workspace is not deleted along with it. After deleting the project, Service Map usage isn't free, and each node will be charged as per the paid tier of Log Analytics workspace/</p> <p>If you have projects that you created before Azure Migrate general availability (GA- 28 February 2018), you might have incurred additional Service Map charges. To ensure payment after 180 days only, we recommend that you create a new project, since existing workspaces before GA are still chargeable.</p>
Management	<p>When you register agents to the workspace, you use the ID and key provided by the Azure Migrate project.</p> <p>You can use the Log Analytics workspace outside Azure Migrate.</p> <p>If you delete the associated Azure Migrate project, the workspace isn't deleted automatically. Delete it manually.</p> <p>Don't delete the workspace created by Azure Migrate, unless you delete the Azure Migrate project. If you do, the dependency visualization functionality will not work as expected.</p>
Internet connectivity	<p>If machines aren't connected to the internet, you need to install the Log Analytics gateway on them.</p>

Next steps

[Prepare for Hyper-V VM assessment](#)

This article summarizes support settings and limitations for migrating Hyper-V VMs with [Azure Migrate: Server Migration](#). If you're looking for information about assessing Hyper-V VMs for migration to Azure, review the [assessment support matrix](#).

Migration limitations

You can select up to 10 VMs at once for replication. If you want to migrate more machines, replicate in groups of 10.

Hyper-V hosts

SUPPORT	DETAILS
Deployment	The Hyper-V host can be standalone or deployed in a cluster. Azure Migrate replication software (Hyper-V Replication provider) needs to be installed on the Hyper-V hosts.
Permissions	You need administrator permissions on the Hyper-V host.
Host operating system	Windows Server 2019, Windows Server 2016, or Windows Server 2012 R2.
URL access	The replication provider software on the Hyper-V hosts will need access to these URLs: <ul style="list-style-type: none">- login.microsoftonline.com: Access control and identity management using Active Directory.- *.backup.windowsazure.com: Replication data transfer and coordination. Migrate service URLs.- *.blob.core.windows.net: Upload data to storage accounts.- dc.services.visualstudio.com: Upload app logs used for internal monitoring.- time.windows.com: Verifies time synchronization between system and global time.
Port access	Outbound connections on HTTPS port 443 to send VM replication data.

Hyper-V VMs

SUPPORT	DETAILS
Operating system	All Windows and Linux operating systems that are supported by Azure.

SUPPORT	DETAILS
Required changes for Azure	Some VMs might require changes so that they can run in Azure. You need to make adjustments manually before migration. The relevant articles contain instructions about how to do this.
Linux boot	If /boot is on a dedicated partition, it should reside on the OS disk, and not be spread across multiple disks. If /boot is part of the root (/) partition, then the '/' partition should be on the OS disk, and not span other disks.
UEFI boot	The migrated VM in Azure will be automatically converted to a BIOS boot VM. The VM should be running Windows Server 2012 and later only. The OS disk should have up to five partitions or fewer and the size of OS disk should be less than 300 GB.
Disk size	2 TB for the OS disk, 4 TB for data disks.
Disk number	A maximum of 16 disks per VM.
Encrypted disks/volumes	Not supported for migration.
RDM/passthrough disks	Not supported for migration.
Shared disk	VMs using shared disks aren't supported for migration.
NFS	NFS volumes mounted as volumes on the VMs won't be replicated.
iSCSI	VMs with iSCSI targets aren't supported for migration.
Target disk	You can migrate to Azure VMs with managed disks only.
IPv6	Not supported.
NIC teaming	Not supported.
Azure Site Recovery	You can't replicate using Azure Migrate Server Migration if the VM is enabled for replication with Azure Site Recovery.
Ports	Outbound connections on HTTPS port 443 to send VM replication data.

Azure VM requirements

All on-premises VMs replicated to Azure must meet the Azure VM requirements summarized in this table.

COMPONENT	REQUIREMENTS	DETAILS
Operating system disk size	Up to 2,048 GB.	Check fails if unsupported.

Component	Requirements	Details
Operating system disk count	1	Check fails if unsupported.
Data disk count	16 or less.	Check fails if unsupported.
Data disk size	Up to 4,095 GB	Check fails if unsupported.
Network adapters	Multiple adapters are supported.	
Shared VHD	Not supported.	Check fails if unsupported.
FC disk	Not supported.	Check fails if unsupported.
BitLocker	Not supported.	BitLocker must be disabled before you enable replication for a machine.
VM name	<p>From 1 to 63 characters. Restricted to letters, numbers, and hyphens.</p> <p>The machine name must start and end with a letter or number.</p>	Update the value in the machine properties in Site Recovery.
Connect after migration-Windows	<p>To connect to Azure VMs running Windows after migration:</p> <ul style="list-style-type: none"> - Before migration enables RDP on the on-premises VM. Make sure that TCP, and UDP rules are added for the Public profile, and that RDP is allowed in Windows Firewall > Allowed Apps, for all profiles. <p>For site-to-site VPN access, enable RDP and allow RDP in Windows Firewall -> Allowed apps and features for Domain and Private networks. In addition, check that the operating system's SAN policy is set to OnlineAll. Learn more.</p>	
Connect after migration-Linux	<p>To connect to Azure VMs after migration using SSH:</p> <p>Before migration, on the on-premises machine, check that the Secure Shell service is set to Start, and that firewall rules allow an SSH connection.</p> <p>After failover, on the Azure VM, allow incoming connections to the SSH port for the network security group rules on the failed over VM, and for the Azure subnet to which it's connected. In addition, add a public IP address for the VM.</p>	

Next steps

[Migrate Hyper-V VMs](#) for migration.

Support matrix for physical server assessment

3/30/2020 • 5 minutes to read • [Edit Online](#)

This article summarizes prerequisites and support requirements when you assess physical servers for migration to Azure, using the [Azure Migrate:Server Assessment](#) tool. If you want to migrate physical servers to Azure, review the [migration support matrix](#).

To assess physical servers, you create an Azure Migrate project, and add the Server Assessment tool to the project. After the tool is added, you deploy the [Azure Migrate appliance](#). The appliance continuously discovers on-premises machines, and sends machine metadata and performance data to Azure. After discovery is complete, you gather discovered machines into groups, and run an assessment for a group.

Limitations

SUPPORT	DETAILS
Assessment limits	You can discover and assess up to 35,000 physical servers in a single Azure Migrate project .
Project limits	You can create multiple projects in an Azure subscription. In addition to physical servers, a project can include VMware VMs and Hyper-V VMs, up to the assessment limits for each.
Discovery	The Azure Migrate appliance can discover up to 250 physical servers.
Assessment	You can add up to 35,000 machines in a single group. You can assess up to 35,000 machines in a single assessment.

[Learn more](#) about assessments.

Physical server requirements

SUPPORT	DETAILS
Physical server deployment	The physical server can be standalone, or deployed in a cluster.
Permissions	Windows: You need a local or domain user account on all the Windows servers you want to discover. The user account should be added to these groups: Remote Desktop Users, Performance Monitor Users, and Performance Log users. Linux: You need a root account on the Linux servers that you want to discover.
Operating system	All Windows and Linux operating systems that are supported by Azure, except for Windows Server 2003, and SUSE Linux.

Azure Migrate appliance requirements

Azure Migrate uses the [Azure Migrate appliance](#) for discovery and assessment. The appliance for physical servers can run on a VM or a physical machine. You set the appliance up using a PowerShell script that you download from the Azure portal.

- Learn about [appliance requirements](#) for physical servers.
- Learn about [URLs](#) the appliance needs to access.

Port access

The following table summarizes port requirements for assessment.

DEVICE	CONNECTION
Appliance	<p>Inbound connections on TCP port 3389, to allow remote desktop connections to the appliance.</p> <p>Inbound connections on port 44368, to remotely access the appliance management app using the URL: <code>https://<appliance-ip-or-name>:44368</code></p> <p>Outbound connections on ports 443 (HTTPS), to send discovery and performance metadata to Azure Migrate.</p>
Physical servers	<p>Windows: Inbound connections on WinRM ports 5985 (HTTP) and 5986 (HTTPS), to pull configuration and performance metadata from Windows servers.</p> <p>Linux: Inbound connections on port 22 (UDP), to pull configuration and performance metadata from Linux servers.</p>

Agent-based dependency analysis requirements

[Dependency analysis](#) helps you to identify dependencies between on-premises machines that you want to assess and migrate to Azure. The table summarizes the requirements for setting up agent-based dependency analysis. Currently only agent-based dependency analysis is supported for physical servers.

REQUIREMENT	DETAILS
Before deployment	<p>You should have an Azure Migrate project in place, with the Server Assessment tool added to the project.</p> <p>You deploy dependency visualization after setting up an Azure Migrate appliance to discover your on-premises machines</p> <p>Learn how to create a project for the first time. Learn how to add an assessment tool to an existing project. Learn how to set up the Azure Migrate appliance for assessment of Hyper-V, VMware, or physical servers.</p>
Azure Government	Dependency visualization isn't available in Azure Government.

Requirement	Details
Log Analytics	<p>Azure Migrate uses the Service Map solution in Azure Monitor logs for dependency visualization.</p> <p>You associate a new or existing Log Analytics workspace with an Azure Migrate project. The workspace for an Azure Migrate project can't be modified after it's added.</p> <p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>The workspace must reside in the East US, Southeast Asia, or West Europe regions. Workspaces in other regions can't be associated with a project.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>In Log Analytics, the workspace associated with Azure Migrate is tagged with the Migration Project key, and the project name.</p>
Required agents	<p>On each machine you want to analyze, install the following agents:</p> <p>The Microsoft Monitoring agent (MMA). The Dependency agent.</p> <p>If on-premises machines aren't connected to the internet, you need to download and install Log Analytics gateway on them.</p> <p>Learn more about installing the Dependency agent and MMA.</p>
Log Analytics workspace	<p>The workspace must be in the same subscription as the Azure Migrate project.</p> <p>Azure Migrate supports workspaces residing in the East US, Southeast Asia, and West Europe regions.</p> <p>The workspace must be in a region in which Service Map is supported.</p> <p>The workspace for an Azure Migrate project can't be modified after it's added.</p>

Requirement	Details
Costs	<p>The Service Map solution doesn't incur any charges for the first 180 days (from the day that you associate the Log Analytics workspace with the Azure Migrate project)/</p> <p>After 180 days, standard Log Analytics charges will apply.</p> <p>Using any solution other than Service Map in the associated Log Analytics workspace will incur standard charges for Log Analytics.</p> <p>When the Azure Migrate project is deleted, the workspace is not deleted along with it. After deleting the project, Service Map usage isn't free, and each node will be charged as per the paid tier of Log Analytics workspace/</p> <p>If you have projects that you created before Azure Migrate general availability (GA- 28 February 2018), you might have incurred additional Service Map charges. To ensure payment after 180 days only, we recommend that you create a new project, since existing workspaces before GA are still chargeable.</p>
Management	<p>When you register agents to the workspace, you use the ID and key provided by the Azure Migrate project.</p> <p>You can use the Log Analytics workspace outside Azure Migrate.</p> <p>If you delete the associated Azure Migrate project, the workspace isn't deleted automatically. Delete it manually.</p> <p>Don't delete the workspace created by Azure Migrate, unless you delete the Azure Migrate project. If you do, the dependency visualization functionality will not work as expected.</p>
Internet connectivity	<p>If machines aren't connected to the internet, you need to install the Log Analytics gateway on them.</p>

Next steps

[Prepare for physical server assessment](#).

Support matrix for physical server migration

4/1/2020 • 4 minutes to read • [Edit Online](#)

This article summarizes support settings and limitations for migrating physical servers with [Azure Migrate: Server Migration](#). If you're looking for information about assessing physical servers for migration to Azure, review the [assessment support matrix](#).

Overview

You can migrate on-premises machines as physical servers, using agent-based replication. Using this tool, you can migrate a wide range of machines to Azure:

- On-premises physical servers.
- VMs virtualized by platforms such as Xen, KVM.
- Hyper-V VMs or VMware VMs if for some reason you don't want to use the standard [Hyper-V](#) or [VMware](#) flows.
- VMs running in private clouds.
- VMs running in public clouds such as Amazon Web Services (AWS) or Google Cloud Platform (GCP).

Migration limitations

You can select up to 10 machines at once for replication. If you want to migrate more machines, then replicate in groups of 10.

Physical server requirements

The table summarizes support for physical servers you want to migrate using agent-based migration.

SUPPORT	DETAILS
Machine workload	Azure Migrate supports migration of any workload (say Active Directory, SQL server, etc.) running on a supported machine.
Operating systems	For the latest information, review the operating system support for Site Recovery. Azure Migrate provides identical operating system support.
Linux file system/guest storage	For the latest information, review the Linux file system support for Site Recovery. Azure Migrate provides identical Linux file system support.
Network/Storage	For the latest information, review the network and storage prerequisites for Site Recovery. Azure Migrate provides identical network/storage requirements.
Azure requirements	For the latest information, review the Azure network , storage , and compute requirements for Site Recovery. Azure Migrate has identical requirements for physical server migration.
Mobility service	The Mobility service agent must be installed on each machine you want to migrate.

SUPPORT	DETAILS
UEFI boot	The migrated machine in Azure will be automatically converted to a BIOS boot Azure VM. Only server running Windows Server 2012 and later supported. The OS disk should have up to four partitions, and volumes should be formatted with NTFS.
Target disk	Machines can only be migrated to managed disks (standard HDD, premium SSD) in Azure.
Disk size	2 TB OS disk; 8 TB for data disks.
Disk limits	Up to 63 disks per machine.
Encrypted disks/volumes	Machines with encrypted disks/volumes aren't supported for migration.
Shared disk cluster	Not supported.
Independent disks	Supported.
Passthrough disks	Supported.
NFS	NFS volumes mounted as volumes on the machines won't be replicated.
iSCSI targets	Machines with iSCSI targets aren't supported for agentless migration.
Multipath IO	Not supported.
Storage vMotion	Supported
Teamed NICs	Not supported.
IPv6	Not supported.

Replication appliance requirements

If you set up the replication appliance manually on a physical server, then make sure that it complies with the requirements summarized in the table. When you set up the Azure Migrate replication appliance as an VMware VM using the OVA template provided in the Azure Migrate hub, the appliance is set up with Windows Server 2016, and complies with the support requirements.

- Learn about [replication appliance requirements](#).
- MySQL must be installed on the appliance. Learn about [installation options](#).
- Learn about [URLs](#) the replication appliance needs to access.

Azure VM requirements

All on-premises VMs replicated to Azure must meet the Azure VM requirements summarized in this table. When Site Recovery runs a prerequisites check for replication, the check will fail if some of the requirements aren't met.

Component	Requirements	Details
Guest operating system	Verifies supported operating systems. You can migrate any workload running on a supported operating system.	Check fails if unsupported.
Guest operating system architecture	64-bit.	Check fails if unsupported.
Operating system disk size	Up to 2,048 GB.	Check fails if unsupported.
Operating system disk count	1	Check fails if unsupported.
Data disk count	64 or less.	Check fails if unsupported.
Data disk size	Up to 4,095 GB	Check fails if unsupported.
Network adapters	Multiple adapters are supported.	
Shared VHD	Not supported.	Check fails if unsupported.
FC disk	Not supported.	Check fails if unsupported.
BitLocker	Not supported.	BitLocker must be disabled before you enable replication for a machine.
VM name	<p>From 1 to 63 characters. Restricted to letters, numbers, and hyphens.</p> <p>The machine name must start and end with a letter or number.</p>	Update the value in the machine properties in Site Recovery.
Connect after migration-Windows	<p>To connect to Azure VMs running Windows after migration:</p> <ul style="list-style-type: none"> - Before migration enables RDP on the on-premises VM. Make sure that TCP, and UDP rules are added for the Public profile, and that RDP is allowed in Windows Firewall > Allowed Apps, for all profiles. <p>For site-to-site VPN access, enable RDP and allow RDP in Windows Firewall - > Allowed apps and features for Domain and Private networks. In addition, check that the operating system's SAN policy is set to OnlineAll. Learn more.</p>	

COMPONENT	REQUIREMENTS	DETAILS
Connect after migration-Linux	<p>To connect to Azure VMs after migration using SSH:</p> <p>Before migration, on the on-premises machine, check that the Secure Shell service is set to Start, and that firewall rules allow an SSH connection.</p> <p>After failover, on the Azure VM, allow incoming connections to the SSH port for the network security group rules on the failed over VM, and for the Azure subnet to which it's connected. In addition, add a public IP address for the VM.</p>	

Next steps

[Migrate physical servers.](#)

Azure Migrate appliance

3/31/2020 • 11 minutes to read • [Edit Online](#)

This article summarizes the prerequisites and support requirements for the Azure Migrate appliance.

Deployment scenarios

The Azure Migrate appliance is used in the following scenarios.

SCENARIO	TOOL	USED FOR
VMware VM assessment	Azure Migrate:Server Assessment	Discover VMware VMs Discover machine apps and dependencies Collect machine metadata and performance metadata for assessments.
VMware VM agentless migration	Azure Migrate:Server Migration	Discover VMware VMs Replicate VMware VMs with agentless migration.
Hyper-V VM assessment	Azure Migrate:Server Assessment	Discover Hyper-V VMs Collect machine metadata and performance metadata for assessments.
Physical machine assessment	Azure Migrate:Server Assessment	Discover physical servers (or VMs you treat as physical servers). Collect machine metadata and performance metadata for assessments.

Appliance - VMware

The following table summarizes the Azure Migrate appliance requirements for VMware.

REQUIREMENT	VMWARE

Requirement	VMware
Appliance components	<p>The appliance has the following components:</p> <ul style="list-style-type: none"> - Management app: This is a web app for user input during appliance deployment. Used when assessing machines for migration to Azure. - Discovery agent: The agent gathers machine configuration data. Used when assessing machines for migration to Azure. - Assessment agent: The agent collects performance data. Used when assessing machines for migration to Azure. - Auto update service: Updates appliance components (runs every 24 hours). - DRA agent: Orchestrates VM replication, and coordinates communication between replicated machines and Azure. Used only when replicating VMware VMs to Azure using agentless migration. - Gateway: Sends replicated data to Azure. Used only when replicating VMware VMs to Azure using agentless migration.
Supported deployment	<p>Deploy as VMware VM using OVA template.</p> <p>Deploy as a VMware VM or physical machine using PowerShell installation script.</p>
Project support	<p>An appliance can be associated with a single project. Any number of appliances can be associated with a single project.</p>
Discovery limits	<p>An appliance can discover up to 10,000 VMware VMs on a vCenter Server.</p> <p>An appliance can connect to a single vCenter Server.</p>
OVA template	<p>Download from portal or from https://aka.ms/migrate/appliance/vmware.</p> <p>Download size is 11.2 GB.</p> <p>The downloaded appliance template comes with a Windows Server 2016 evaluation license, which is valid for 180 days. If the evaluation period is close to expiry, we recommend that you download and deploy a new appliance, or that you activate the operating system license of the appliance VM.</p>
PowerShell script	<p>Script download.</p>

Requirement	VMware
Software/hardware	<p>The appliance should run on machine with Windows Server 2016, 32-GB RAM, 8 vCPUs, around 80 GB of disk storage, and an external virtual switch.</p> <p>The appliance requires internet access, either directly or through a proxy.</p> <p>If you run the appliance on a VMware VM, you need enough resources on the vCenter Server to allocate a VM that meets the requirements.</p> <p>If you run the appliance on a physical machine, make sure that it's running Windows Server 2016, and meets hardware requirements.</p>
VMware requirements	<p>If you deploy the appliance as a VMware VM, it must be deployed on an ESXi host running version 5.5 or later.</p> <p>vCenter Server running 5.5, 6.0, 6.5, or 6.7.</p>
VDDK (agentless migration)	If you deploy the appliance as a VMware VM, and you're running an agentless migration, the VMware vSphere VDDK must be installed on the appliance VM.
Hash value-OVA	Verify the OVA template hash values.
Hash value-PowerShell script	Verify the PowerShell script hash values.

Appliance - Hyper-V

Requirement	Hyper-V
Appliance components	<p>The appliance has the following components:</p> <ul style="list-style-type: none"> - Management app: This is a web app for user input during appliance deployment. Used when assessing machines for migration to Azure. - Discovery agent: The agent gathers machine configuration data. Used when assessing machines for migration to Azure. - Assessment agent: The agent collects performance data. Used when assessing machines for migration to Azure. - Auto update service: Updates appliance components (runs every 24 hours).
Supported deployment	<p>Deploy as Hyper-V VM using a VHD template.</p> <p>Deploy as a Hyper-V VM or physical machine using a PowerShell installation script.</p>
Project support	An appliance can be associated with a single project. Any number of appliances can be associated with a single project.
Discovery limits	An appliance can discover up to 5000 Hyper-V VMs. An appliance can connect to up to 300 Hyper-V hosts.

REQUIREMENT	HYPER-V
VHD template	Zipped folder including VHD. Download from portal or from https://aka.ms/migrate/appliance/hyperv . Download size is 10 GB. The downloaded appliance template comes with a Windows Server 2016 evaluation license, which is valid for 180 days. If the evaluation period is close to expiry, we recommend that you download and deploy a new appliance, or that you activate the operating system license of the appliance VM.
PowerShell script	Script download .
Software/hardware*	The appliance should run on machine with Windows Server 2016, 32-GB RAM, 8 vCPUs, around 80 GB of disk storage, and an external virtual switch. The appliance needs a static or dynamic IP address, and requires internet access, either directly or through a proxy. If you run the appliance as a Hyper-V VM, you need enough resources on the Hyper-V host to allocate 16-GB RAM, 8 vCPUs, around 80 GB of storage space, and an external switch for the appliance VM. If you run the appliance on a physical machine, make sure that it's running Windows Server 2016, and meets hardware requirements.
Hyper-V requirements	If you deploy the appliance with the VHD template, the appliance VM provided by Azure Migrate is Hyper-V VM version 5.0. The Hyper-V host must be running Windows Server 2012 R2 or later.
Hash value-VHD	Verify the VHD template hash values.
Hash value-PowerShell script	Verify the PowerShell script hash values.

Appliance - Physical

REQUIREMENT	PHYSICAL
-------------	----------

Requirement	Physical
Appliance components	<p>The appliance has the following components:</p> <ul style="list-style-type: none"> - Management app: This is a web app for user input during appliance deployment. Used when assessing machines for migration to Azure. - Discovery agent: The agent gathers machine configuration data. Used when assessing machines for migration to Azure. - Assessment agent: The agent collects performance data. Used when assessing machines for migration to Azure. - Auto update service: Updates appliance components (runs every 24 hours).
Supported deployment	Deploy as a dedicated physical machine, or a VM, using a PowerShell installation script.
Project support	An appliance can be associated with a single project. Any number of appliances can be associated with a single project.
Discovery limits	An appliance can discover up to 250 physical servers.
PowerShell script	<p>Download the script (AzureMigrateInstaller.ps1) in a zipped folder from the portal. Learn more. Alternatively, download directly.</p> <p>Download size is 59.7 MB.</p>
Software/hardware	<p>The appliance should run on machine with Windows Server 2016, 32-GB RAM, 8 vCPUs, around 80 GB of disk storage, and an external virtual switch.</p> <p>The appliance needs a static or dynamic IP address, and requires internet access, either directly or through a proxy.</p> <p>If you run the appliance on a physical machine, make sure that it's running Windows Server 2016, and meets hardware requirements.</p>
Hash value	Verify the PowerShell script hash values.

URL access

The Azure Migrate appliance needs connectivity to the internet.

- When you deploy the appliance, Azure Migrate does a connectivity check to the URLs summarized in the table below.
- If you're using a URL-based proxy to connect to the internet, you need to allow access to these URLs, making sure that the proxy resolves any CNAME records received while looking up the URLs.

URL	Details
*.portal.azure.com	Navigate to the Azure portal.

URL	DETAILS
*.windows.net *.msftauth.net *.msauth.net *.microsoft.com *.live.com	Sign in to your Azure subscription.
*.microsoftonline.com *.microsoftonline-p.com	Create Azure Active Directory (AD) apps for the appliance to communicate with Azure Migrate.
management.azure.com	Create Azure AD apps for the appliance to communicate with the Azure Migrate service.
dc.services.visualstudio.com	Upload app logs used for internal monitoring.
*.vault.azure.net	Manage secrets in the Azure Key Vault.
aka.ms/*	Allow access to aka links. Used for Azure Migrate appliance updates.
download.microsoft.com/download	Allow downloads from Microsoft download.
*.servicebus.windows.net	Communication between the appliance and the Azure Migrate service.
*.discoverysrv.windowsazure.com *.migration.windowsazure.com	Connect to Azure Migrate service URLs.
*.hypervrecoverymanager.windowsazure.com	Used for VMware agentless migration Connect to Azure Migrate service URLs.
*.blob.core.windows.net	Used for VMware agentless migration Upload data to storage for migration.

Collected data - VMware

The appliance collects metadata, performance data, and dependency analysis data (if agentless [dependency analysis](#) is used).

Metadata

Metadata discovered by the Azure Migrate appliance helps you to figure out whether machines and apps are ready for migration to Azure, right-size machines and apps, plans costs, and analyze application dependencies. Microsoft doesn't use this data in any license compliance audit.

Here's the full list of VMware VM metadata that the appliance collects and sends to Azure.

DATA	COUNTER
Machine details	
VM ID	vm.Config.InstanceUuid

DATA	COUNTER
VM name	vm.Config.Name
vCenter Server ID	VMwareClient.Instance.Uuid
VM description	vm.Summary.Config.Annotation
License product name	vm.Client.ServiceContent.About.LicenseProductName
Operating system type	vm.SummaryConfig.GuestFullName
Boot type	vm.Config.Firmware
Number of cores	vm.Config.Hardware.NumCPU
Memory (MB)	vm.Config.Hardware.MemoryMB
Number of disks	vm.Config.Hardware.Device.ToList().FindAll(x => is VirtualDisk).count
Disk size list	vm.Config.Hardware.Device.ToList().FindAll(x => is VirtualDisk)
Network adapters list	vm.Config.Hardware.Device.ToList().FindAll(x => is VirtualEthernet).count
CPU utilization	cpu.usage.average
Memory utilization	mem.usage.average
Per disk details	
Disk key value	disk.Key
Diskunit number	disk.UnitNumber
Disk controller key value	disk.ControllerKey.Value
Gigabytes provisioned	virtualDisk.DeviceInfo.Summary
Disk name	Value generated using disk.UnitNumber, disk.Key, disk.ControllerKey.VAlue
Read operations per second	virtualDisk.numberReadAveraged.average
Write operations per second	virtualDisk.numberWriteAveraged.average
Read throughput (MB per second)	virtualDisk.read.average
Write throughput (MB per second)	virtualDisk.write.average
Per NIC details	

DATA	COUNTER
Network adapter name	nic.Key
MAC address	((VirtualEthernetCard)nic).MacAddress
IPv4 addresses	vm.Guest.Net
IPv6 addresses	vm.Guest.Net
Read throughput (MB per second)	net.received.average
Write throughput (MB per second)	net.transmitted.average
Inventory path details	
Name	container.GetType().Name
Type of child object	container.ChildType
Reference details	container.MoRef
Parent details	Container.Parent
Folder details per VM	((Folder)container).ChildEntity.Type
Datacenter details per VM	((Datacenter)container).VmFolder
Datacenter details per host folder	((Datacenter)container).HostFolder
Cluster details per host	((ClusterComputeResource)container).Host
Host details per VM	((HostSystem)container).VM

Performance data

Here's the VMware VM performance data that the appliance collects and sends to Azure.

DATA	COUNTER	ASSESSMENT IMPACT
CPU utilization	cpu.usage.average	Recommended VM size/cost
Memory utilization	mem.usage.average	Recommended VM size/cost
Disk read throughput (MB per second)	virtualDisk.read.average	Calculation for disk size, storage cost, VM size
Disk writes throughput (MB per second)	virtualDisk.write.average	Calculation for disk size, storage cost, VM size
Disk read operations per second	virtualDisk.numberReadAveraged.average	Calculation for disk size, storage cost, VM size

DATA	COUNTER	ASSESSMENT IMPACT
Disk writes operations per second	virtualDisk.numberWriteAveraged.average	Calculation for disk size, storage cost, VM size
NIC read throughput (MB per second)	net.received.average	Calculation for VM size
NIC writes throughput (MB per second)	net.transmitted.average	Calculation for VM size

App dependencies metadata

Agentless dependency analysis collects connection and process data.

Connection data

Here's the connection data that the appliance collects from each VM enabled for agentless dependency analysis. This data is sent to Azure.

DATA	COMMAND USED
Local port	netstat
Local IP address	netstat
Remote port	netstat
Remote IP address	netstat
TCP connection state	netstat
Process ID	netstat
No. of active connections	netstat

Process data

Here's the process data that the appliance collects from each VM enabled for agentless dependency analysis. This data is sent to Azure.

DATA	WMI CLASS	WMI CLASS PROPERTY
Process name	Win32_Process	ExecutablePath
Process arguments	Win32_Process	CommandLine
Application name	Win32_Process	VersionInfo.ProductName parameter of ExecutablePath property

Linux VM data

Here's the connection and process data that the appliance collects from each Linux VM enabled for agentless dependency analysis. This data is sent to Azure.

DATA	COMMAND USED
Local port	netstat

DATA	COMMAND USED
Local IP address	netstat
Remote port	netstat
Remote IP address	netstat
TCP connection state	netstat
No. of active connections	netstat
Process ID	netstat
Process name	ps
Process arguments	ps
Application name	dpkg or rpm

Collected data - Hyper-V

The appliance collects metadata, performance data, and dependency analysis data (if agentless [dependency analysis](#) is used).

Metadata

Metadata discovered by the Azure Migrate appliance helps you to figure out whether machines and apps are ready for migration to Azure, right-size machines and apps, plans costs, and analyze application dependencies. Microsoft doesn't use this data in any license compliance audit.

Here's the full list of Hyper-V VM metadata that the appliance collects and sends to Azure.

*DATA	WMI CLASS	WMI CLASS PROPERTY
Machine details		
Serial number of BIOS _MsVm_BIOSElement	BIOSSerialNumber	
VM type (Gen 1 or 2)	Msvm_VirtualSystemSettingData	VirtualSystemSubType
VM display name	Msvm_VirtualSystemSettingData	ElementName
VM version	Msvm_ProcessorSettingData	VirtualQuantity
Memory (bytes)	Msvm_MemorySettingData	VirtualQuantity
Maximum memory that can be consumed by VM	Msvm_MemorySettingData	Limit
Dynamic memory enabled	Msvm_MemorySettingData	DynamicMemoryEnabled

*DATA	WMI CLASS	WMI CLASS PROPERTY
Operating system name/version/FQDN	Msvm_KvpExchangeComponent	GuestIntrinsicExchangeItems Name Data
VM power status	Msvm_ComputerSystem	EnabledState
Per disk details		
Disk identifier	Msvm_VirtualHardDiskSettingData	VirtualDiskId
Virtual hard disk type	Msvm_VirtualHardDiskSettingData	Type
Virtual hard disk size	Msvm_VirtualHardDiskSettingData	MaxInternalSize
Virtual hard disk parent	Msvm_VirtualHardDiskSettingData	ParentPath
Per NIC details		
IP addresses (synthetic NICs)	Msvm_GuestNetworkAdapterConfiguration	IPAddresses
DHCP enabled (synthetic NICs)	Msvm_GuestNetworkAdapterConfiguration	DHCPEnabled
NIC ID (synthetic NICs)	Msvm_SyntheticEthernetPortSettingData	InstanceId
NIC MAC address (synthetic NICs)	Msvm_SyntheticEthernetPortSettingData	Address
NIC ID (legacy NICs)	MsvmEmulatedEthernetPortSettingData	InstanceId
NIC MAC ID (legacy NICs)	MsvmEmulatedEthernetPortSettingData	Address

Performance data

Here's the Hyper VM performance data that the appliance collects and sends to Azure.

PERFORMANCE COUNTER CLASS	COUNTER	ASSESSMENT IMPACT
Hyper-V Hypervisor Virtual Processor	% Guest Run Time	Recommended VM size/cost
Hyper-V Dynamic Memory VM	Current Pressure (%) Guest Visible Physical Memory (MB)	Recommended VM size/cost
Hyper-V Virtual Storage Device	Read Bytes/Second	Calculation for disk size, storage cost, VM size
Hyper-V Virtual Storage Device	Write Bytes/Second	Calculation for disk size, storage cost, VM size
Hyper-V Virtual Network Adapter	Bytes Received/Second	Calculation for VM size

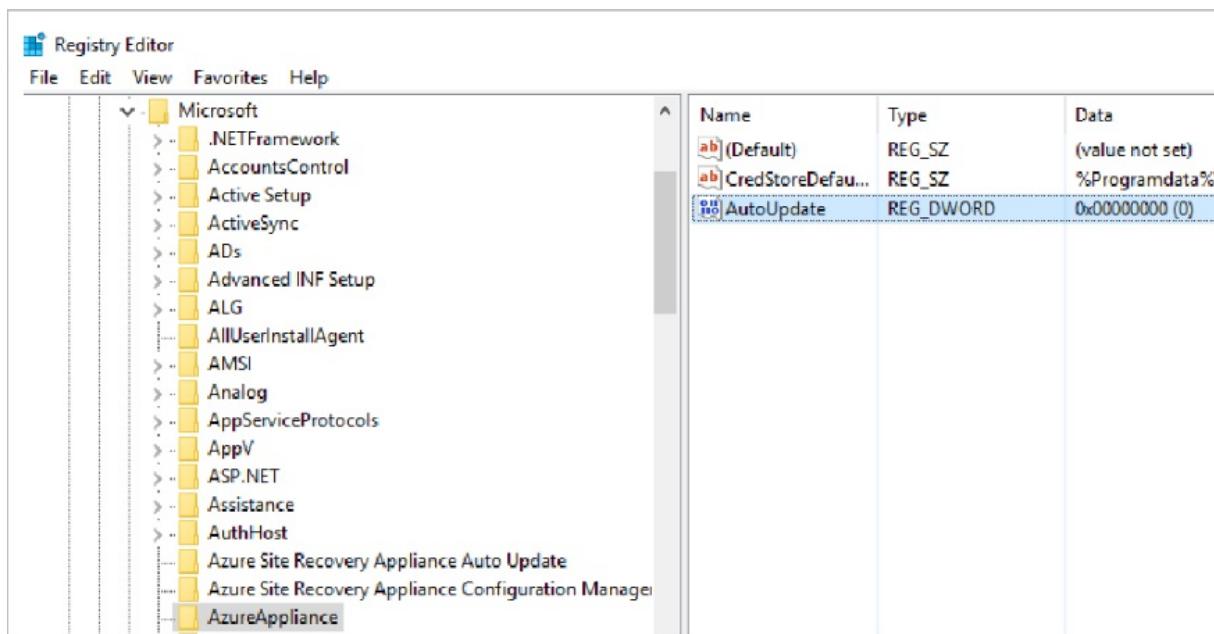
PERFORMANCE COUNTER CLASS	COUNTER	ASSESSMENT IMPACT
Hyper-V Virtual Network Adapter	Bytes Sent/Second	Calculation for VM size

- CPU utilization is the sum of all usage, for all virtual processors attached to a VM.
- Memory utilization is (Current Pressure * Guest Visible Physical Memory) / 100.
- Disk and network utilization values are collected from the listed Hyper-V performance counters.

Appliance upgrades

The appliance is upgraded as the Azure Migrate agents running on the appliance are updated. This happens automatically because auto-update is enabled on the appliance by default. You can change this default setting to update the agents manually.

- **Turn off auto-update:** You turn off auto-update in the registry by setting HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AzureAppliance "AutoUpdate" key to 0 (DWORD). If you decide to use manual updates, it's important to update all agents on the appliance at the same time, using the **Update** button for each outdated agent on the appliance.
- **Update manually:** For manual updates, make sure that you update all the agents on the appliance, using the **Update** button for each outdated agent on the appliance. You can switch the update setting back to automatic updates at any time.



Next steps

- [Learn how](#) to set up the appliance for VMware.
- [Learn how](#) to set up the appliance for Hyper-V.
- [Learn how](#) to set up the appliance for physical servers.

This article describes the replication appliance used by [Azure Migrate: Server Migration](#) tool when migrating VMware VMs, physical machines, and private/public cloud VMs to Azure, using agent-based migration.

Overview

The replication appliance is deployed when you set up agent-based migration of VMware VMs or physical servers. It's deployed as a single on-premises machine, either as a VMware VM or a physical server. It runs:

- **Replication appliance:** The replication appliance coordinates communications, and manages data replication, for on-premises VMware VMs and physical servers replicating to Azure.
- **Process server:** The process server, which is installed by default on the replication appliance, and does the following:
 - **Replication gateway:** It acts as a replication gateway. It receives replication data from machines enabled for replication. It optimizes replication data with caching, compression, and encryption, and sends it to Azure.
 - **Agent installer:** Performs a push installation of the Mobility Service. This service must be installed and running on each on-premises machine that you want to replicate for migration.

Appliance deployment

USED FOR	DETAILS
VMware VM agent-based migration	You download OVA template from the Azure Migrate hub, and import to vCenter Server to create the appliance VM.
Physical machine agent-based migration	If you don't have a VMware infrastructure, or if you can't create a VMware VM using an OVA template, you download a software installer from the Azure Migrate hub, and run it to set up the appliance machine.

Appliance requirements

When you set up the replication appliance using the OVA template provided in the Azure Migrate hub, the appliance runs Windows Server 2016 and complies with the support requirements. If you set up the replication appliance manually on a physical server, then make sure that it complies with the requirements.

COMPONENT	REQUIREMENT
VMware VM appliance	
PowerCLI	PowerCLI version 6.0 should be installed if the replication appliance is running on a VMware VM.
NIC type	VMXNET3 (if the appliance is a VMware VM)
Hardware settings	

COMPONENT	REQUIREMENT
CPU cores	8
RAM	16 GB
Number of disks	Three: The OS disk, process server cache disk, and retention drive.
Free disk space (cache)	600 GB
Free disk space (retention disk)	600 GB
Software settings	
Operating system	Windows Server 2016 or Windows Server 2012 R2
License	<p>The appliance comes with a Windows Server 2016 evaluation license, which is valid for 180 days.</p> <p>If the evaluation period is close to expiry, we recommend that you download and deploy a new appliance, or that you activate the operating system license of the appliance VM.</p>
Operating system locale	English (en-us)
TLS	TLS 1.2 should be enabled.
.NET Framework	.NET Framework 4.6 or later should be installed on the machine (with strong cryptography enabled).
MySQL	<p>MySQL should be installed on the appliance.</p> <p>MySQL should be installed. You can install manually, or Site Recovery can install it during appliance deployment.</p>
Other apps	Don't run other apps on the replication appliance.
Windows Server roles	<p>Don't enable these roles:</p> <ul style="list-style-type: none"> - Active Directory Domain Services - Internet Information Services - Hyper-V
Group policies	<p>Don't enable these group policies:</p> <ul style="list-style-type: none"> - Prevent access to the command prompt. - Prevent access to registry editing tools. - Trust logic for file attachments. - Turn on Script Execution. <p>Learn more</p>
IIS	<ul style="list-style-type: none"> - No pre-existing default website - No pre-existing website/application listening on port 443 - Enable anonymous authentication - Enable FastCGI setting
Network settings	

COMPONENT	REQUIREMENT
IP address type	Static
Ports	443 (Control channel orchestration) 9443 (Data transport)
NIC type	VMXNET3

MySQL installation

MySQL must be installed on the replication appliance machine. It can be installed using one of these methods.

METHOD	DETAILS
Download and install manually	Download MySQL application & place it in the folder C:\Temp\ASRSetup, then install manually. When you set up the appliance MySQL will show as already installed.
Without online download	Place the MySQL installer application in the folder C:\Temp\ASRSetup. When you install the appliance and click to download and install MySQL, setup will use the installer you added.
Download and install in Azure Migrate	When you install the appliance and are prompted for MySQL, select Download and install .

URL access

The replication appliance needs access to these URLs.

URL	DETAILS
*.backup.windowsazure.com	Used for replicated data transfer and coordination
*.store.core.windows.net	Used for replicated data transfer and coordination
*.blob.core.windows.net	Used to access storage account that stores replicated data
*.hypervrecoverymanager.windowsazure.com	Used for replication management operations and coordination
https://management.azure.com	Used for replication management operations and coordination
*.services.visualstudio.com	Used for telemetry purposes (It is optional)
time.nist.gov	Used to check time synchronization between system and global time.
time.windows.com	Used to check time synchronization between system and global time.

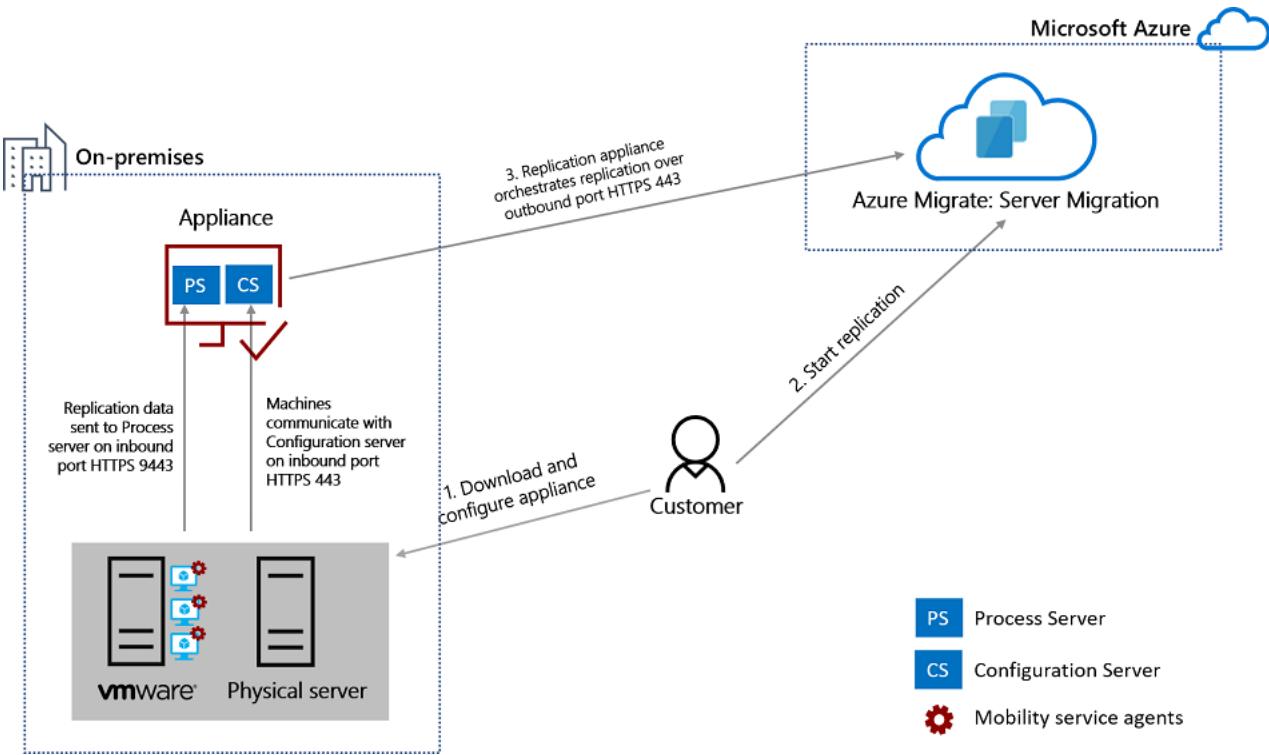
URL	DETAILS
https://login.microsoftonline.com https://secure.aadcdn.microsoftonline-p.com https://login.live.com https://graph.windows.net https://login.windows.net https://www.live.com https://www.microsoft.com	OVF setup needs access to these URLs. They are used for access control and identity management by Azure Active Directory
https://dev.mysql.com/get/Downloads/MySQLInstaller/mysql-installer-community-5.7.20.0.msi	To complete MySQL download

Port access

DEVICE	CONNECTION
VMs	<p>The Mobility service running on VMs communicates with the on-premises replication appliance (configuration server) on port HTTPS 443 inbound, for replication management.</p> <p>VMs send replication data to the process server (running on the configuration server machine) on port HTTPS 9443 inbound. This port can be modified.</p>
Replication appliance	The replication appliance orchestrates replication with Azure over port HTTPS 443 outbound.
Process server	<p>The process server receives replication data, optimizes, and encrypts it, and sends it to Azure storage over port 443 outbound.</p> <p>By default the process server runs on the replication appliance.</p>

Replication process

- When you enable replication for a VM, initial replication to Azure storage begins, using the specified replication policy.
- Traffic replicates to Azure storage public endpoints over the internet. Replicating traffic over a site-to-site virtual private network (VPN) from an on-premises site to Azure isn't supported.
- After initial replication finishes, delta replication begins. Tracked changes for a machine are logged.
- Communication happens as follows:
 - VMs communicate with the replication appliance on port HTTPS 443 inbound, for replication management.
 - The replication appliance orchestrates replication with Azure over port HTTPS 443 outbound.
 - VMs send replication data to the process server (running on the replication appliance) on port HTTPS 9443 inbound. This port can be modified.
 - The process server receives replication data, optimizes and encrypts it, and sends it to Azure storage over port 443 outbound.
- The replication data logs first land in a cache storage account in Azure. These logs are processed and the data is stored in an Azure managed disk.



Appliance upgrades

The appliance is upgraded manually from the Azure Migrate hub. We recommend that you always run the latest version.

1. In Azure Migrate > Servers > Azure Migrate: Server Assessment, Infrastructure servers, click **Configuration servers**.
2. In **Configuration servers**, a link appears in **Agent Version** when a new version of the replication appliance is available.
3. Download the installer to the replication appliance machine, and install the upgrade. The installer detects the version current running on the appliance.

Next steps

- [Learn how](#) to set up the replication appliance for agent-based VMware VM migration.
- [Learn how](#) to set up the replication appliance for physical servers.

Azure Migrate appliance architecture

3/30/2020 • 4 minutes to read • [Edit Online](#)

This article describes the Azure Migrate appliance architecture and processes. The Azure Migrate appliance is a lightweight appliance that's deployed on premises, to discover VMs and physical servers for migration to Azure.

Deployment scenarios

The Azure Migrate appliance is used in the following scenarios.

SCENARIO	TOOL	USED FOR
VMware VM assessment	Azure Migrate:Server Assessment	Discover VMware VMs. Discover machine apps and dependencies. Collect machine metadata and performance metadata and send to Azure.
VMware VM migration (agentless)	Azure Migrate:Server Migration	Discover VMware VMs Replicate VMware VMs with agentless migration .
Hyper-V VM assessment	Azure Migrate:Server Assessment	Discover Hyper-V VMs. Collect machine metadata and performance metadata and send to Azure.
Physical machine	Azure Migrate:Server Assessment	Discover physical servers. Collect machine metadata and performance metadata and send to Azure.

Appliance components

The appliance has a number of components.

- **Management app:** This is a web app for user input during appliance deployment. Used when assessing machines for migration to Azure.
- **Discovery agent:** The agent gathers machine configuration data. Used when assessing machines for migration to Azure.
- **Assessment agent:** The agent collects performance data. Used when assessing machines for migration to Azure.
- **DRA agent:** Orchestrates VM replication, and coordinates communication between replicated machines and Azure. Used only when replicating VMware VMs to Azure using agentless migration.
- **Gateway:** Sends replicated data to Azure. Used only when replicating VMware VMs to Azure using agentless migration.

- **Auto update service:** Updates appliance components (runs every 24 hours).

Appliance deployment

- The Azure Migrate appliance can be set up using a template for [Hyper-V](#) or [VMware](#) or using a PowerShell script installer for [VMware/Hyper-V](#), and for [physical servers](#).
- Appliance support requirements and deployment prerequisites are summarized in the [appliance support matrix](#).

Appliance registration

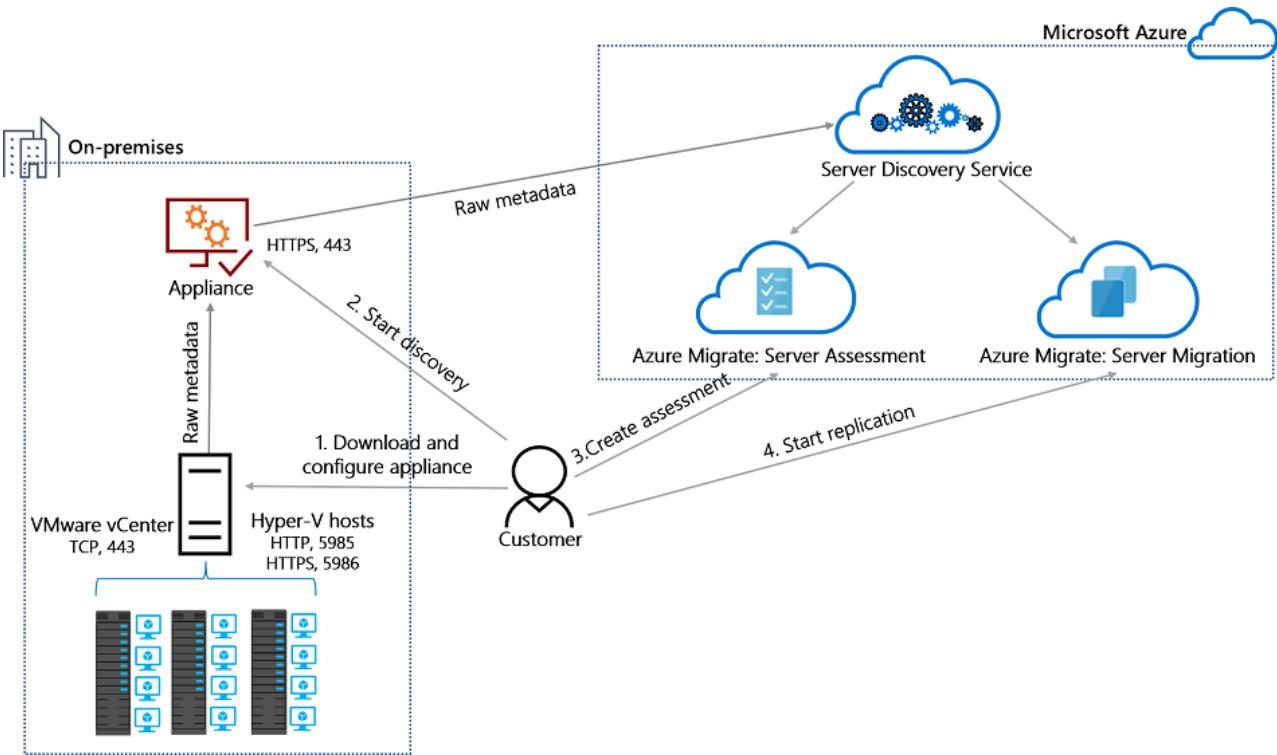
During appliance setup, you register the appliance with Azure Migrate, and the actions summarized in the table occur.

ACTION	DETAILS	PERMISSIONS
Register source providers	<p>These resources providers are registered in the subscription you choose during appliance setup: Microsoft.OffAzure, Microsoft.Migrate and Microsoft.KeyVault.</p> <p>Registering a resource provider configures your subscription to work with the resource provider.</p>	To register the resource providers, you need a Contributor or Owner role on the subscription.
Create Azure AD app-communication	<p>Azure Migrate creates an Azure Active Directory (Azure AD) app for communication (authentication and authorization) between the agents running on the appliance, and their respective services running on Azure.</p> <p>This app does not have privileges to make Azure Resource Manager calls, or RBAC access on any resource.</p>	You need these permissions for Azure Migrate to create the app.
Create Azure AD apps-Key vault	<p>This app is created only for agentless migration of VMware VMs to Azure.</p> <p>It's used exclusively to access the key vault created in the user's subscription for agentless migration.</p> <p>It has RBAC access on the Azure key vault (created in customer's tenant), when discovery is initiated from the appliance.</p>	You need these permissions for Azure Migrate to create the app.

Collected data

Data collected by the client for all deployment scenarios is summarized in the [appliance support matrix](#).

Discovery and collection process



The appliance communicates with vCenter Servers and Hyper-V hosts/cluster using the following process.

1. Start discovery:

- When you start the discovery on the Hyper-V appliance, it communicates with the Hyper-V hosts on WinRM ports 5985 (HTTP) and 5986 (HTTPS).
- When you start discovery on the VMware appliance, it communicates with the vCenter server on TCP port 443 by default. If the vCenter server listens on a different port, you can configure it in the appliance web app.

2. Gather metadata and performance data:

- The appliance uses a Common Information Model (CIM) session to gather Hyper-V VM data from the Hyper-V host on ports 5985 and 5986.
- The appliance communicates with port 443 by default, to gather VMware VM data from the vCenter Server.

3. Send data:

The appliance sends the collected data to Azure Migrate Server Assessment and Azure Migrate Server Migration over SSL port 443. The appliance can connect to Azure over the internet, or you can use ExpressRoute with public/Microsoft peering.

- For performance data, the appliance collects real-time utilization data.
 - Performance data is collected every 20 seconds for VMware, and every 30 seconds for Hyper-V, for each performance metric.
 - The collected data is rolled up to create a single data point for 10 minutes.
 - The peak utilization value is selected from all of the 20/30-second data points, and sent to Azure for assessment calculation.
 - Based on the percentile value specified in the assessment properties (50th/90th/95th/99th), the ten-minute points are sorted in ascending order, and the appropriate percentile value is used to compute the assessment
- For Server Migration, the appliance starts collecting VM data, and replicates it to Azure.

4. Assess and migrate:

You can now create assessments from the metadata collected by the appliance using Azure Migrate Server Assessment. In addition, you can also start migrating VMware VMs using Azure Migrate Server Migration to orchestrate agentless VM replication.

Appliance upgrades

The appliance is upgraded as the Azure Migrate agents running on the appliance are updated. This happens automatically because auto-update is enabled on the appliance by default. You can change this default setting to update the agents manually.

You turn off auto-update in the registry by setting the
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\AzureAppliance "AutoUpdate" key to 0 (DWORD).

Next steps

[Review](#) the appliance support matrix.

This article provides an overview of the architecture and processes used when you migrate Hyper-V VMs with the Azure Migrate Server Migration tool.

Azure Migrate provides a central hub to track discovery, assessment, and migration of your on-premises apps and workloads, and private/public cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

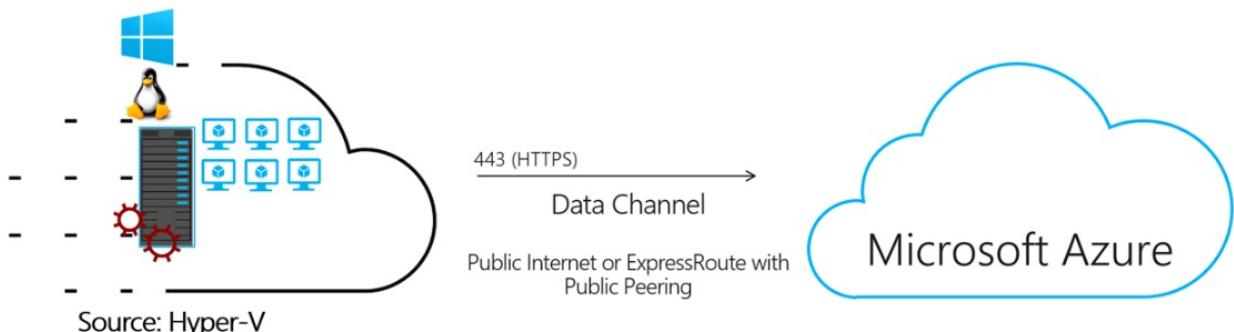
Agentless migration

The Azure Migrate Server Migration tool provides agentless replication for on-premises Hyper-V VMs, using a migration workflow that's optimized for Hyper-V. You install a software agent only on Hyper-V hosts or cluster nodes. Nothing needs to be installed on Hyper-V VMs.

Server Migration and Azure Site Recovery

Azure Migrate Server Migration is a tool for migrating on-premises workloads, and cloud-based VMs, to Azure. Site Recovery is a disaster recovery tool. The tools share some common technology components used for data replication, but serve different purposes.

Architectural components



COMPONENT	DEPLOYMENT
Replication provider	The Microsoft Azure Site Recovery provider is installed on Hyper-V hosts, and registered with Azure Migration Server Migration. The provider orchestrates replication for Hyper-V VMs.

COMPONENT	DEPLOYMENT
Recovery Services agent	<p>The Microsoft Azure Recovery Service agent handles data replication. It works with the provider to replicate data from Hyper-V VMs to Azure.</p> <p>The replicated data is uploaded to a storage account in your Azure subscription. The Server Migration tool processes the replicated data, and applies it to replica disks in the subscription. The replica disks are used to create the Azure VMs when you migrate.</p>

- Components are installed by a single setup file, downloaded from Azure Migrate Server Migration in the portal.
- The provider and appliance use outbound HTTPS port 443 connections to communicate with Azure Migrate Server Migration.
- Communications from the provider and agent are secure and encrypted.

Replication process

1. When you enable replication for a Hyper-V VM, initial replication begins.
2. A Hyper-V VM snapshot is taken.
3. VHDs on the VM are replicated one-by-one, until they're all copied to Azure. Initial replication time depends on the VM size, and network bandwidth.
4. Disk changes that occur during initial replication are tracked using Hyper-V Replica, and stored in log files (hrl files).
 - Log files are in the same folder as the disks.
 - Each disk has an associated hrl file that's sent to secondary storage.
 - The snapshot and log files consume disk resources while initial replication is in progress.
5. After initial replication finishes, the VM snapshot is deleted, and delta replication begins.
6. Incremental disk changes are tracked in hrl files. Replication logs are periodically uploaded to an Azure storage account by the Recovery Services agent.

Performance and scaling

Replication performance for Hyper-V is influenced by factors that include VM size, the data change rate (churn) of the VMs, available space on the Hyper-V host for log file storage, upload bandwidth for replication data, and target storage in Azure.

- If you're replicating multiple machines at the same time, use the [Azure Site Recovery Deployment Planner](#) for Hyper-V, to help optimize replication.
- Plan your Hyper-V replication, and distribute replication over Azure storage accounts, in accordance with capacity.

Control upload throughput

You can limit the amount of bandwidth used to upload data to Azure on each Hyper-V host. Be careful. If you set the values too low it will adversely impact replication, and delay migration.

1. Sign in to the Hyper-V host or cluster node.
2. Run C:\Program Files\Microsoft Azure Recovery Services Agent\bin\wabadmin.msc, to open the Windows Azure Backup MMC snap-in.
3. In the snap-in, select **Change Properties**.
4. In **Throttling**, select **Enable internet bandwidth usage throttling for backup operations**. Set the limits for work and non-work hours. Valid ranges are from 512 Kbps to 1,023 Mbps.

Influence upload efficiency

If you have spare bandwidth for replication, and want to increase uploads, you can increase the number of threads allocated for the upload task, as follows:

1. Open the registry with Regedit.
2. Navigate to key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication\UploadThreadsPerVM
3. Increase the value for the number of threads used for data upload for each replicating VM. The default value is 4 and the max value is 32.

Next steps

Try out [Hyper-V migration](#) using Azure Migrate Server Migration.

This article provides an overview of the architecture and processes used for agent-based replication of VMware VMs with the [Azure Migrate: Server Migration](#) tool.

Using Azure Migrate: Server Migration, you can replicate VMware VMs with a couple of options:

- Migrate VMs using agent-based replication, as described in this article.
- Migrate VMware VMs using agentless replication. This migrates VMs without needing to install anything on them.

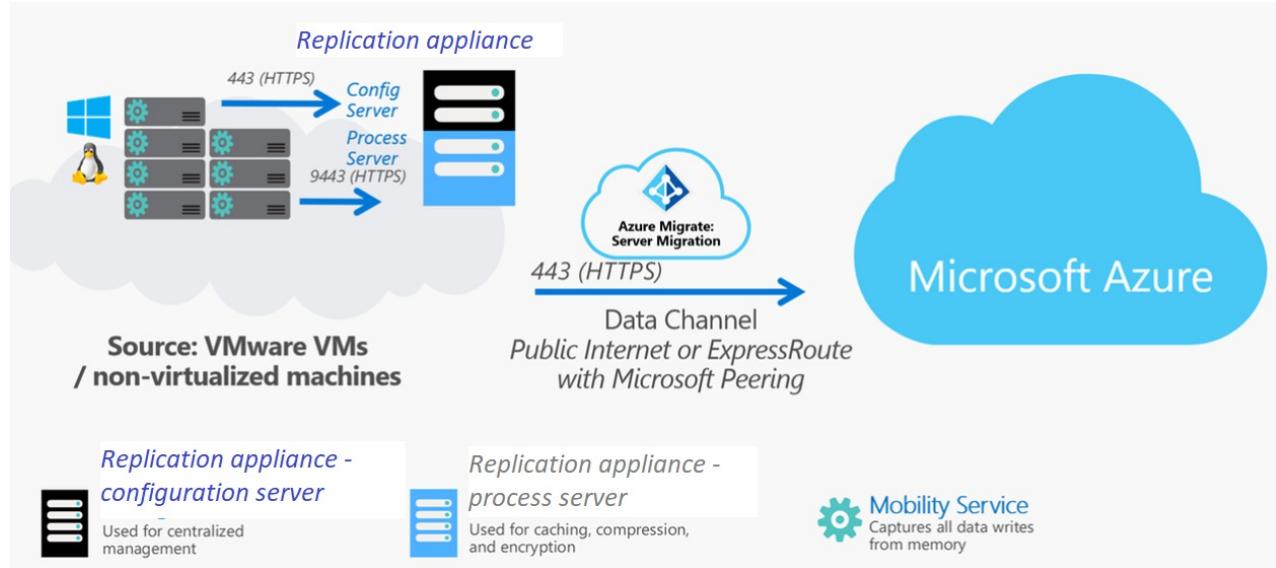
Learn more about [selecting and comparing](#) migration methods for VMware VMs.

Agent-based migration

Agent-based migration is used to migrate on-premises VMware VMs and physical servers to Azure. It can also be used to migrate other on-premises virtualized servers, as well as private and public cloud VMs, including AWS instances, and GCP VMs. Agent-based migration in Azure Migrate uses some backend functionality from the [Azure Site Recovery](#) service.

Architectural components

The diagram illustrates the components involved in agent-based migration.



The table summarizes the components used for agent-based migration.

COMPONENT	DETAILS	INSTALLATION
-----------	---------	--------------

COMPONENT	DETAILS	INSTALLATION
Replication appliance	<p>The replication appliance (configuration server/process server) is an on-premises machine that acts as a bridge between the on-premises environment, and Server Migration. The appliance discovers the on-premises machine inventory, so that Server Migration can orchestrate replication and migration. The appliance has two components:</p> <p>Configuration server: Connects to Server Migration and coordinates replication.</p> <p>Process server: Handles data replication. The process server receives machine data, compresses and encrypts it, and sends to Azure. In Azure, Server Migration writes the data to managed disks.</p>	By default the process server is installed together with the configuration server on the replication appliance.
Mobility service	<p>The Mobility service is an agent installed on each machine you want to replicate and migrate. It sends replication data from the machine to the process server.</p>	Installation files for different versions of the Mobility service are located on the replication appliance. You download and install the agent you need, in accordance with the operating system and version of the machine you want to replicate.

Mobility service installation

You can deploy the Mobility Service using the following methods:

- **Push installation:** The Mobility service is installed by the process server when you enable protection for a machine.
- **Install manually:** You can install the Mobility service manually on each machine through UI or command prompt.

The Mobility service communicates with the replication appliance and replicated machines. If you have antivirus software running on the replication appliance, process servers, or machines being replicated, the following folders should be excluded from scanning:

- C:\Program Files\Microsoft Azure Recovery Services Agent
- C:\ProgramData\ASR
- C:\ProgramData\ASRLogs
- C:\ProgramData\ASRSetupLogs
- C:\ProgramData\LogUploadServiceLogs
- C:\ProgramData\Microsoft Azure Site Recovery
- C:\Program Files (x86)\Microsoft Azure Site Recovery
- C:\ProgramData\ASR\agent (on Windows machines with the Mobility service installed)

Replication process

1. When you enable replication for a machine, initial replication to Azure begins.
2. During initial replication, the Mobility service reads data from the machine disks, and sends it to the process server.

3. This data is used to seed a copy of the disk in your Azure subscription.
4. After initial replication finishes, replication of delta changes to Azure begins. Replication is block-level, and near-continuous.
5. The Mobility service intercepts writes to disk memory, by integrating with the storage subsystem of the operating system. This method avoids disk I/O operations on the replicating machine, for incremental replication.
6. Tracked changes for a machine are sent to the process server on inbound port HTTPS 9443. This port can be modified. The process server compresses and encrypts it, and sends it to Azure.

Ports

DEVICE	CONNECTION
Replicating machines	<p>The Mobility service running on VMs communicates with the on-premises replication appliance on port HTTPS 443 inbound, for replication management.</p> <p>Machines send replication data to the process server on port HTTPS 9443 inbound. This port can be modified.</p>
Replication appliance	The replication appliance orchestrates replication with Azure over port HTTPS 443 outbound.
Process server	The process server receives replication data, optimizes and encrypts it, and sends it to Azure storage over port 443 outbound.

Performance and scaling

By default, you deploy a single replication appliance that runs both the configuration server and the process server. If you're only replicating a few machines, this deployment is sufficient. However, if you're replicating and migrating hundreds of machines, a single process server might not be able to handle all the replication traffic. In this case, you can deploy additional, scale-out process servers.

Plan VMware deployment

If you're replicating VMware VMs, you can use the [Site Recovery Deployment Planner for VMware](#), to help determine performance requirements, including the daily data change rate, and the process servers you need.

Replication appliance capacity

Use the values in this table to figure out whether you need an additional process server in your deployment.

- If your daily change rate (churn rate) is over 2 TB, deploy an additional process server.
- If you're replicating more than 200 machines, deploy an additional replication appliance.

CPU	MEMORY	FREE SPACE-DATA CACHING	CHURN RATE	REPLICATION LIMITS
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz)	16 GB	300 GB	500 GB or less	< 100 machines
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz)	18 GB	600 GB	501 GB to 1 TB	100-150 machines.

CPU	MEMORY	FREE SPACE-DATA CACHING	CHURN RATE	REPLICATION LIMITS
16 vCPUs (2 sockets * 8 cores @ 2.5 GHz)	32 G1	1 TB	1 TB to 2 TB	151-200 machines.

Sizing scale-out process servers

If you need to deploy a scale-out process server, use this table to figure out server sizing.

PROCESS SERVER	FREE SPACE FOR DATA CACHING	CHURN RATE	REPLICATION LIMITS
4 vCPUs (2 sockets * 2 cores @ 2.5 GHz), 8-GB memory	300 GB	250 GB or less	Up to 85 machines
8 vCPUs (2 sockets * 4 cores @ 2.5 GHz), 12-GB memory	600 GB	251 GB to 1 TB	86-150 machines.
12 vCPUs (2 sockets * 6 cores @ 2.5 GHz), 24-GB memory	1 TB	1-2 TB	151-225 machines.

Throttle upload bandwidth.

VMware traffic that replicates to Azure goes through a specific process server. You can limit upload throughput by throttling bandwidth on the machines that are running as process servers. You can influence bandwidth using this registry key:

- The HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Azure Backup\Replication\UploadThreadsPerVM registry value specifies the number of threads that are used for data transfer (initial or delta replication) of a disk. A higher value increases the network bandwidth that's used for replication. The default value is four. The maximum value is 32. Monitor traffic to optimize the value.
- In addition, you can throttle bandwidth on the process server machine as follows:
 - On the process server machine, open the Azure Backup MMC snap-in. There's a shortcut on the desktop or in the folder C:\Program Files\Microsoft Azure Recovery Services Agent\bin.
 - In the snap-in, select **Change Properties**.
 - In **Throttling**, select **Enable internet bandwidth usage throttling for backup operations**. Set the limits for work and non-work hours. Valid ranges are from 512 Kbps to 1,023 Mbps.

Next steps

Try out [agent-based migration](#) for [VMware](#) or [physical servers](#).

Assessments in Azure Migrate:Server Assessment

3/23/2020 • 17 minutes to read • [Edit Online](#)

This article provides an overview of assessments in the [Azure Migrate:Server Assessment](#) tool. The Server Assessment tool can assess on-premises VMware VMs, Hyper-V VMs, and physical servers, for migration to Azure.

What's an assessment?

An assessment with the Server Assessment tool measures the readiness, and estimates the impact, of migrating on-premises servers to Azure.

Types of assessments

Assessments you create with Server Assessment are a point-in-time snapshot of data. Server Assessment provides two types of assessments.

ASSESSMENT TYPE	DETAILS	DATA
Performance-based	Assessments that make recommendations based on collected performance data	VM size recommendation is based on CPU and memory utilization data. Disk type recommendation (standard HDD/SSD or premium-managed disks) is based on the IOPS and throughput of the on-premises disks.
As-is on-premises	Assessments that don't use performance data to make recommendations.	VM size recommendation is based on the on-premises VM size The recommended disk type is based on the selected storage type for the assessment.

How do I run an assessment?

There are a couple of ways to run an assessment:

- Assess machines using server metadata collected by a lightweight Azure Migrate appliance. The appliance discovers on-premises machines, and sends machine metadata/performance data to Azure Migrate.
- Assess machines using server metadata that's imported in a comma-separated values (CSV) format.

How do I assess with the appliance?

If you're deploying an Azure Migrate appliance to discover on-premises servers, you do the following:

1. You set up Azure and your on-premises environment to work with Server Assessment.
2. For your first assessment, you create an Azure project, and add the Server Assessment tool to it.
3. You deploy a lightweight Azure Migrate appliance. The appliance continuously discovers on-premises machines, and sends machine metadata and performance data to Azure Migrate. The appliance is deployed as a VM or a physical machine. There's no need to install anything on machines that you want to assess.
4. After the appliance begins machine discovery, you can gather machines you want to assess into a group, and

run an assessment for the group.

You can follow our tutorials for [VMware](#), [Hyper-V](#), or [physical servers](#) to try out these steps.

How do I assess with imported data?

If you're assessing servers using a CSV file, you don't need an appliance. Instead, you do the following:

1. You set up Azure to work with Server Assessment.
2. For your first assessment, you create an Azure project, and add the Server Assessment tool to it.
3. You download a CSV template, and add server data to it.
4. You import the template into Server Assessment.
5. You discover servers added with the import, gather them into a group, and run an assessment for the group.

What data does the appliance collect?

If you're using the Azure Migrate appliance for assessment, learn about the metadata and performance data that's collected for [VMware](#) and [Hyper-V](#).

How does the appliance calculate performance data?

If you use the appliance for discovery, performance data for compute settings is collected as follows:

1. The appliance collects a real-time sample point:
 - **VMware VMs:** The appliance collects a real-time sample point at every 20-second interval.
 - **Hyper-V VMs:** The real-time sample point is collected at every 30-second interval.
 - **Physical servers:** The real-time sample point is collected at every five-minute interval.
2. The appliance rolls up the sample points (20 seconds, 30 seconds, five minutes) to create a single data point every 10 minutes. To create the single point, the appliance selects the peak value from all the samples, and then sends it to Azure.
3. Server Assessment stores all the 10-minute sample points for the last month.
4. When you create an assessment, Server Assessment identifies the appropriate data point to use for right-sizing, based on the percentile values for *Performance history* and *Percentile utilization*.
 - For example, if the performance history is set to one week, and the percentile utilization is the 95th percentile, Server Assessment sorts the 10-minute sample points for the last week in ascending order, and picks the 95th percentile value for right-sizing.
 - The 95th percentile value makes sure that you ignore any outliers, which might be included if you pick the 99th percentile.
 - If you want to pick the peak usage for the period and don't want to miss any outliers, you should select the 99th percentile for percentile utilization.
5. This value is multiplied by the comfort factor to get the effective performance utilization data for each metric (CPU utilization, memory utilization, disk IOPS (read and write), disk throughput (read and write), and network throughput (in and out) that the appliance collects.

How are assessments calculated?

Assessments in Server Assessment are calculated using metadata/performance data for the on-premises machines. If you deploy the Azure Migrate appliance, then assessment using the data collected by the appliance. If you run an assessment for machines imported using a .CSV file, you provide the metadata for the calculation. Calculations occur in three stages:

- Calculate Azure readiness:** Assess whether machines are suitable for migration to Azure.
- Calculate sizing recommendations:** Estimate compute, storage, and network sizing.
- Calculate monthly costs:** Calculate the estimated monthly compute and storage costs for running the machines in Azure after migration.

Calculations are in order, and a machine server moves along to a later stage only if it passes the previous one. For example, if a server fails the Azure readiness, it's marked as unsuitable for Azure, and sizing and costing is not done for that server.

What's in an assessment?

Here's what included in an assessment in Server Assessment.

PROPERTY	DETAILS
Target location	The location to which you want to migrate. Server Assessment currently supports these target Azure regions: Australia East, Australia Southeast, Brazil South, Canada Central, Canada East, Central India, Central US, China East, China North, East Asia, East US, East US2, Germany Central, Germany Northeast, Japan East, Japan West, Korea Central, Korea South, North Central US, North Europe, South Central US, Southeast Asia, South India, UK South, UK West, US Gov Arizona, US Gov Texas, US Gov Virginia, West Central US, West Europe, West India, West US, and West US2.
<i>Target storage disk (as-is sizing)*</i>	The type of disks to use for storage in Azure. Specify the target storage disk as premium managed, standard SSD managed, or standard HDD managed.
Target storage disk (performance based sizing)	Specify the type of target storage disk as automatic, premium managed, standard HDD managed, or standard SSD managed. Automatic: The disk recommendation is based on the performance data of the disks (the input/output operations per second (IOPS) and throughput). Premium/standard: The assessment recommends a disk SKU within the storage type selected. If you want to achieve a single instance VM SLA of 99.9%, considering using premium managed disks. This ensures that all disks in the assessment are recommended as premium-managed disks. Azure Migrate only supports managed disks for migration assessment.
Reserved Instances (RIs)	Specify Reserved Instances in Azure, so that cost estimations in the assessment take RI discounts into account. RIs are currently supported only for Pay-As-You-Go offers in Azure Migrate.

PROPERTY	DETAILS
Sizing criteria	Used to right-size the VM in Azure. Use as-is sizing, or performance-based sizing.
Performance history	Used with performance-based sizing. Specify the duration used when evaluating performance data.
Percentile utilization	Used with performance-based sizing. Specifies the percentile value of the performance sample to be used for right-sizing.
VM series	Specify the Azure VM series that you want to consider for right-sizing. For example, if you don't have a production environment that needs A-series VMs in Azure, you can exclude A-series from the list or series.
Comfort factor	Buffer used during assessment. Applied on top of machine utilization data for VMs (CPU, memory, disk, and network). It accounts for issues such as seasonal usage, short performance history, and likely increases in future usage. For example, a 10-core VM with 20% utilization normally results in a two-core VM. With a comfort factor of 2.0x, the result is a four-core VM instead.
Offer	Displays the Azure offer in which you're enrolled. Server Assessment estimates the cost accordingly.
Currency	Billing currency for your account.
Discount (%)	Lists any subscription-specific discounts you receive on top of the Azure offer. The default setting is 0%.
VM uptime	If Azure VMs won't run 24 hours a day, 7 days a week, you can specify the duration (days per month and hours per day) they will run. Cost estimates are handled accordingly. The default value is 31 days per month and 24 hours per day.
Azure Hybrid Benefit	Specifies whether you have software assurance and are eligible for Azure Hybrid Benefit . If set to Yes (the default setting), non-Windows Azure prices are considered for Windows VMs.

Review the [best practices](#) for creating assessment with Server Assessment.

Calculate readiness

Not all machines are suitable to run in Azure. Server Assessment assesses each on-premises machine, and assigns it a readiness category.

- **Ready for Azure:** The machine can be migrated as-is to Azure without any changes. It will start in Azure with full Azure support.
- **Conditionally ready for Azure:** The machine might start in Azure, but might not have full Azure support. For example, a machine that's running an older version of Windows Server isn't supported in Azure. You must be careful before you migrate these machines to Azure. Follow the remediation guidance suggested in the

assessment to fix the readiness issues.

- **Not ready for Azure:** The machine won't start in Azure. For example, if an on-premises machine disk is more than 64-TBs, it can't be hosted in Azure. Follow the remediation guidance to fix the issue before migration.
- **Readiness unknown:** Azure Migrate couldn't determine the readiness of a machine, because of insufficient metadata.

To calculate readiness, Server Assessment reviews the machine properties and operating system settings summarized in the following tables.

Machine properties

Server Assessment reviews the following properties of the on-premises VM to determine whether it can run on Azure.

PROPERTY	DETAILS	AZURE READINESS STATUS
Boot type	Azure supports VMs with a boot type of BIOS, not UEFI.	Conditionally ready if the boot type is UEFI.
Cores	<p>The number of cores in the machines must be equal to or less than the maximum number of cores (128) supported for an Azure VM.</p> <p>If performance history is available, Azure Migrate considers the utilized cores for comparison. If a comfort factor is specified in the assessment settings, the number of utilized cores is multiplied by the comfort factor.</p> <p>If there's no performance history, Azure Migrate uses the allocated cores without applying the comfort factor.</p>	Ready if less than or equal to limits.
Memory	<p>The machine memory size must be equal to or less than the maximum memory (3892 gigabytes [GB] on Azure M series Standard_M128m²) allowed for an Azure VM. Learn more.</p> <p>If performance history is available, Azure Migrate considers the utilized memory for comparison. If a comfort factor is specified, the utilized memory is multiplied by the comfort factor.</p> <p>If there's no history, the allocated memory is used without applying the comfort factor.</p>	Ready if within limits.

PROPERTY	DETAILS	AZURE READINESS STATUS
Storage disk	<p>Allocated size of a disk must be 32 TB or less. Although Azure supports 64-TB disks with Ultra SSD disks, Azure Migrate: Server Assessment currently checks for 32 TB as the disk size limits as it does not support Ultra SSD yet.</p> <p>The number of disks attached to the machine must be 65 or fewer, including the OS disk.</p>	Ready if within limits.
Networking	A machine must have 32 or fewer network interfaces (NICs) attached to it.	Ready if within limits.

Guest operating system

Along with VM properties, Server Assessment looks at the guest operating system of the machines to determine whether it can run on Azure.

NOTE

For VMware VMs, Server Assessment uses the operating system specified for the VM in vCenter Server to handle the guest OS analysis. For Linux VMs running on VMware, it currently does not identify the exact kernel version of the guest OS.

The following logic is used by Server Assessment to identify Azure readiness based on the operating system.

OPERATING SYSTEM	DETAILS	AZURE READINESS STATUS
Windows Server 2016 & all SPs	Azure provides full support.	Ready for Azure
Windows Server 2012 R2 & all SPs	Azure provides full support.	Ready for Azure
Windows Server 2012 & all SPs	Azure provides full support.	Ready for Azure
Windows Server 2008 R2 with all SPs	Azure provides full support.	Ready for Azure
Windows Server 2008 (32-bit and 64-bit)	Azure provides full support.	Ready for Azure
Windows Server 2003, 2003 R2	These operating systems have passed their end-of-support date and need a Custom Support Agreement (CSA) for support in Azure.	Conditionally ready for Azure. Consider upgrading the OS before migrating to Azure.
Windows 2000, 98, 95, NT, 3.1, MS-DOS	These operating systems have passed their end-of-support date. The machine might start in Azure, but Azure provides no OS support.	Conditionally ready for Azure. We recommend that you upgrade the OS before migrating to Azure.
Windows Client 7, 8 and 10	Azure provides support with Visual Studio subscription only .	Conditionally ready for Azure
Windows 10 Pro Desktop	Azure provides support with Multitenant Hosting Rights .	Conditionally ready for Azure

OPERATING SYSTEM	DETAILS	AZURE READINESS STATUS
Windows Vista, XP Professional	These operating systems have passed their end-of-support date. The machine might start in Azure, but Azure provides no OS support.	Conditionally ready for Azure. We recommend that you upgrade the OS before migrating to Azure.
Linux	Azure endorses these Linux operating systems . Other Linux operating systems might start in Azure, but we recommend that you upgrade the OS to an endorsed version before migrating to Azure.	Ready for Azure if the version is endorsed. Conditionally ready if the version is not endorsed.
Other operating systems For example, Oracle Solaris, Apple macOS etc., FreeBSD, etc.	Azure doesn't endorse these operating systems. The machine might start in Azure, but Azure provides no OS support.	Conditionally ready for Azure. We recommend that you install a supported OS before migrating to Azure.
OS specified as Other in vCenter Server	Azure Migrate cannot identify the OS in this case.	Unknown readiness. Ensure that the OS running inside the VM is supported in Azure.
32-bit operating systems	The machine might start in Azure, but Azure might not provide full support.	Conditionally ready for Azure. Consider upgrading the OS of the machine from 32-bit OS to 64-bit OS before migrating to Azure.

Calculating sizing

After the machine is marked as ready for Azure, Server Assessment makes sizing recommendations to identify the Azure VM and disk SKU. Sizing calculations depend upon whether you're using as-is on-premises sizing, or performance-based sizing.

Calculate sizing (as-is on-premises)

If you use as-is on-premises sizing, Server Assessment doesn't consider the performance history of the VMs and disks.

- **Compute sizing:** It allocates an Azure VM SKU based on the size allocated on-premises.
- **Storage/disk sizing:** Server Assessment looks at the storage type specified in assessment properties (standard HDD/SSD/premium), and recommends the disk type accordingly. The default storage type is premium disks.
- **Network sizing:** Server Assessment considers the network adapter on the on-premises machine.

Calculate sizing (performance-based)

If you use performance-basing sizing, Server Assessment making sizing recommendations as follows:

- Server Assessment considers the performance history of the machine to identify the VM size and disk type in Azure.
- If servers have been imported using a CSV file, the values you specify are used. This method is especially helpful if you've over-allocated the on-premises machine, utilization is actually low, and you want to right-size the VM in Azure to save costs.
- If you don't want to use the performance data, reset the sizing criteria to as-is on-premises, as described in the previous section.

Calculate storage sizing

For storage sizing, Azure Migrate tries to map every disk attached to the machine to a disk in Azure, and works as follows:

1. Server Assessment adds the read and write IOPS of a disk to get the total IOPS required. Similarly, it adds the read and write throughput values to get the total throughput of each disk.
2. If you've specified storage type as Automatic, based on the effective IOPS and throughput values, Server Assessment determines whether the disk should be mapped to a standard HDD, standard SSD, or a premium disk in Azure. If the storage type is set to Standard HDD/SSD/Premium, Server Assessment tries to find a disk SKU within the storage type selected (Standard HDD/SSD/Premium disks).
3. Disks are selected as follows:
 - If Server Assessment can't find a disk with the required IOPS and throughput, it marks the machine as unsuitable for Azure.
 - If Server Assessment finds a set of suitable disks, it selects the disks that support the location specified in the assessment settings.
 - If there are multiple eligible disks, Server Assessment selects the disk with the lowest cost.
 - If performance data for any disk is unavailable, the configuration data of the disk (disk size) is used to find a standard SSD disk in Azure.

Calculate network sizing

Server Assessment tries to find an Azure VM that can support the number of network adapters attached to the on-premises machine and the performance required by these network adapters.

- To get the effective network performance of the on-premises VM, Server Assessment aggregates the data transmitted per second (Mbps) out of the machine (network out), across all network adapters, and applies the comfort factor. It uses this number to find an Azure VM that can support the required network performance.
- Along with network performance, Server Assessment also considers whether the Azure VM can support the required the number of network adapters.
- If no network performance data is available, Server Assessment considers only the network adapter count for VM sizing.

Calculate compute sizing

After it calculates storage and network requirements, Server Assessment considers CPU and memory requirements to find a suitable VM size in Azure.

- Azure Migrate looks at the effective utilized cores and memory to find a suitable VM 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 calculations. It then applies location and pricing tier settings for the final VM size recommendation.
- If there are multiple eligible Azure VM sizes, the one with the lowest cost is recommended.

Confidence ratings (performance-based)

Each performance-based assessment in Azure Migrate is associated with a confidence rating that ranges from one (lowest) to five stars (highest). The confidence rating helps you estimate the reliability of the size recommendations provided by Azure Migrate.

- The confidence rating is assigned to an assessment based on the availability of data points needed to compute the assessment.
- For performance-based sizing, Server Assessment needs:
 - The utilization data for CPU and VM memory.
 - The disk IOPS and throughput data for every disk attached to the VM.
 - The network I/O to handle performance-based sizing for each network adapter attached to a VM.
 - If any of these utilization numbers aren't available, the size recommendations might not be reliable.

NOTE

Confidence ratings aren't assigned for servers assessed using an imported .CSV file. Ratings also aren't applicable for as-is on-premises assessment.

Ratings

Depending on the percentage of data points available, the confidence rating for the assessment goes as follows.

AVAILABILITY OF DATA POINTS	CONFIDENCE RATING
0-20%	1 star
21-40%	2 stars
41-60%	3 stars
61-80%	4 stars
81-100%	5 stars

Low confidence ratings

Here are a few reasons why an assessment could get a low confidence rating:

- You didn't profile your environment for the duration for which you are creating the assessment. For example, if you create the assessment with performance duration set to one day, you must wait for at least a day after you start discovery for all the data points to get collected.
- Some VMs were shut down during the period for which the assessment was calculated. If any VMs are turned off for some duration, Server Assessment can't collect the performance data for that period.
- Some VMs were created during the period for which the assessment was calculated. For example, if you created an assessment for the performance history of the last month, but some VMs were created in the environment only a week ago, the performance history of the new VMs won't exist for the complete duration.

NOTE

If the confidence rating of any assessment is less than five stars, we recommend that you wait at least a day for the appliance to profile the environment, and then recalculate the assessment. If you don't, performance-based sizing might not be reliable. In that case, we recommend that you switch the assessment to on-premises sizing.

Calculate monthly costs

After sizing recommendations are complete, Azure Migrate calculates compute and storage costs for after migration.

- **Compute cost:** Using the recommended Azure VM size, Azure Migrate uses the Billing API to calculate the monthly cost for the VM.
 - The calculation takes the operating system, software assurance, reserved instances, VM uptime, location, and currency settings into account.
 - It aggregates the cost across all machines to calculate the total monthly compute cost.
- **Storage cost:** The monthly storage cost for a machine is calculated by aggregating the monthly cost of all disks attached to the machine, as follows:
 - Server Assessment calculates the total monthly storage costs by aggregating the storage costs of all

machines.

- Currently, the calculation doesn't consider offers specified in the assessment settings.

Costs are displayed in the currency specified in the assessment settings.

Next steps

[Review](#) best practices for creating assessments.

- Learn about running assessments for [VMware VMs](#), [Hyper-V VMs](#), and [physical servers](#).
- Learn about assessing servers [imported with a CSV file](#).
- Learn about setting up [dependency visualization](#).

Azure Migrate provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

This article summarizes best practices when creating assessments using the Azure Migrate Server Assessment tool.

About assessments

Assessments you create with Azure Migrate Server Assessment are a point-in-time snapshot of data. There are two types of assessments in Azure Migrate.

ASSESSMENT TYPE	DETAILS	DATA
Performance-based	Assessments that make recommendations based on collected performance data	VM size recommendation is based on CPU and memory utilization data. Disk type recommendation (standard HDD/SSD or premium-managed disks) is based on the IOPS and throughput of the on-premises disks.
As-is on-premises	Assessments that don't use performance data to make recommendations.	VM size recommendation is based on the on-premises VM size The recommended disk type is based on what you select in the storage type setting for the assessment.

Example

As an example, if you have an on-premises VM with four cores at 20% utilization, and memory of 8 GB with 10% utilization, the assessments will be as follows:

- **Performance-based assessment:**
 - Identifies effective cores and memory based on core ($4 \times 0.20 = 0.8$), and memory ($8 \text{ GB} \times 0.10 = 0.8$) utilization.
 - Applies the comfort factor specified in assessment properties (let's say 1.3x) to get the values to be used for sizing.
 - Recommends the nearest VM size in Azure that can support ~1.04 cores (0.8×1.3) and ~1.04 GB (0.8×1.3) memory.
- **As-is (as on-premises) assessment:**
 - Recommends a VM with four cores; 8 GB of memory.

Best practices for creating assessments

The Azure Migrate appliance continuously profiles your on-premises environment, and sends metadata and performance data to Azure. Follow these best practices for assessments of servers discovered using an appliance:

- **Create as-is assessments:** You can create as-is assessments immediately once your machines show up in the Azure Migrate portal.
- **Create performance-based assessment:** After setting up discovery, we recommend that you wait at least a day before running a performance-based assessment:
 - Collecting performance data takes time. Waiting at least a day ensures that there are enough performance data points before you run the assessment.
 - When you're running performance-based assessments, make sure you profile your environment for the assessment duration. For example, if you create an assessment with a performance duration set to one week, you need to wait for at least a week after you start discovery, for all the data points to be collected. If you don't, the assessment won't get a five-star rating.
- **Recalculate assessments:** Since assessments are point-in-time snapshots, they aren't automatically updated with the latest data. To update an assessment with the latest data, you need to recalculate it.

Follow these best practices for assessments of servers imported into Azure Migrate via .CSV file:

- **Create as-is assessments:** You can create as-is assessments immediately once your machines show up in the Azure Migrate portal.
- **Create performance-based assessment:** This helps to get a better cost estimate, especially if you have overprovisioned server capacity on-premises. However, the accuracy of the performance-based assessment depends on the performance data specified by you for the servers.
- **Recalculate assessments:** Since assessments are point-in-time snapshots, they aren't automatically updated with the latest data. To update an assessment with the latest imported data, you need to recalculate it.

Best practices for confidence ratings

When you run performance-based assessments, a confidence rating from 1-star (lowest) to 5-star (highest) is awarded to the assessment. To use confidence ratings effectively:

- Azure Migrate Server Assessment needs the utilization data for VM CPU/Memory.
- For each disk attached to the on-premises VM, it needs the read/write IOPS/throughput data.
- For each network adapter attached to the VM, it needs the network in/out data.

Depending on the percentage of data points available for the selected duration, the confidence rating for an assessment is provided as summarized in the following table.

DATA POINT AVAILABILITY	CONFIDENCE RATING
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

Common assessment issues

Here's how to address some common environment issues that affect assessments.

Out-of-sync assessments

If you add or remove machines from a group after you create an assessment, the assessment you created will be

marked **out-of-sync**. Run the assessment again (**Recalculate**) to reflect the group changes.

Outdated assessments

If there are on-premises changes to VMs that are in a group that's been assessed, the assessment is marked **outdated**. To reflect the changes, run the assessment again.

Low confidence rating

An assessment might not have all the data points for a number of reasons:

- You did not profile your environment for the duration for which you are creating the assessment. For example, if you are creating a *performance-based assessment* with performance duration set to one week, you need to wait for at least a week after you start the discovery for all the data points to get collected. You can always click on **Recalculate** to see the latest applicable confidence rating. Confidence rating is applicable only when you create a *performance-based assessment*.
- Few VMs were shut down during the period for which the assessment is calculated. If some VMs were powered off for some duration, Server Assessment will not be able to collect the performance data for that period.
- Few VMs were created after discovery in Server Assessment had started. For example, if you are creating an assessment for the performance history of last one month, but few VMs were created in the environment only a week ago. In this case, the performance data for the new VMs will not be available for the entire duration and the confidence rating would be low.

Next steps

- [Learn](#) how assessments are calculated.
- [Learn](#) how to customize an assessment.

This article describes dependency analysis in Azure Migrate:Server Assessment.

Overview

Dependency analysis helps you to identify dependencies between on-premises machines that you want to assess and migrate to Azure.

- In Azure Migrate:Server Assessment, you gather machines into a group, and then assess the group. Dependency analysis helps you to group machines more accurately, with high confidence for assessment.
- Dependency analysis enables you to identify machines that must be migrated together. You can identify whether machines are in use, or if they can be decommissioned instead of migrated.
- Analyzing dependencies helps ensure that nothing is left behind, and avoid surprise outages during migration.
- Analysis is especially useful if you're not sure whether machines are part of an app deployment that you want to migrate to Azure.
- [Review](#) common questions about dependency analysis.

There are two options for deploying dependency analysis

- **Agent-based:** Agent-based dependency analysis requires agents to be installed on each on-premises machine that you want to analyze.
- **Agentless:** With agentless analysis, you don't need to install agents on machines you want to cross-check. This option is currently in preview, and is only available for VMware VMs.

NOTE

Dependency analysis isn't available in Azure Government.

Agentless analysis

Agentless dependency analysis works by capturing TCP connection data from machines for which it's enabled. No agents are installed on machines you want to analyze.

Collected data

After dependency discovery starts, the appliance polls data from machines every five minutes to gather data. This data is collected from guest VMs via vCenter Server, using vSphere APIs. The gathered data is processed on the Azure Migrate appliance, to deduce identity information, and is sent to Azure Migrate every six hours.

Polling gathers this data from machines:

- Name of processes that have active connections.
- Name of application that run processes that have active connections.
- Destination port on the active connections.

Agent-based analysis

For agent-based analysis, Server Assessment uses the [Service Map solution](#) in Azure Monitor to enable

dependency visualization and analysis. The [Microsoft Monitoring Agent/Log Analytics agent](#) and the [Dependency agent](#), must be installed on each machine you want to analyze.

Collected data

For agent-based visualization, the following data is collected:

- Source machine server name, process, application name.
- Destination machine server name, process, application name, and port.
- Number of connections, latency, and data transfer information are gathered and available for Log Analytics queries.

Compare agentless and agent-based

The differences between agentless visualization and agent-based visualization are summarized in the table.

Requirement	Agentless	Agent-based
Support	This option is currently in preview, and is only available for VMware VMs. Review supported operating systems.	In general availability (GA).
Agent	No need to install agents on machines you want to cross-check.	Agents to be installed on each on-premises machine that you want to analyze: The Microsoft Monitoring agent (MMA) , and the Dependency agent .
Log Analytics	Not required.	Azure Migrate uses the Service Map solution in Azure Monitor logs for dependency analysis.
How it works	Captures TCP connection data on machines enabled for dependency visualization. After discovery, it gathers data at intervals of five minutes.	Service Map agents installed on a machine gather data about TCP processes and inbound/outbound connections for each process.
Data	Source machine server name, process, application name. Destination machine server name, process, application name, and port.	Source machine server name, process, application name. Destination machine server name, process, application name, and port. Number of connections, latency, and data transfer information are gathered and available for Log Analytics queries.
Visualization	Dependency map of single server can be viewed over a duration of one hour to 30 days.	Dependency map of a single server. Map can be viewed over an hour only. Dependency map of a group of servers. Add and remove servers in a group from the map view.
Data export	Can't currently be downloaded in tabular format.	Data can be queried with Log Analytics.

Next steps

- Review the requirements for setting up agent-based analysis for [VMware VMs](#), [physical servers](#), and [Hyper-V VMs](#).
- [Review](#) the requirements for agentless analysis of VMware VMs.
- [Set up](#) agent-based dependency visualization
- [Try out](#) agentless dependency visualization for VMware VMs.
- Review [common questions](#) about dependency visualization.

minutes to read • [Edit Online](#)

This article describes how to create, manage, and delete Azure Migrate projects.

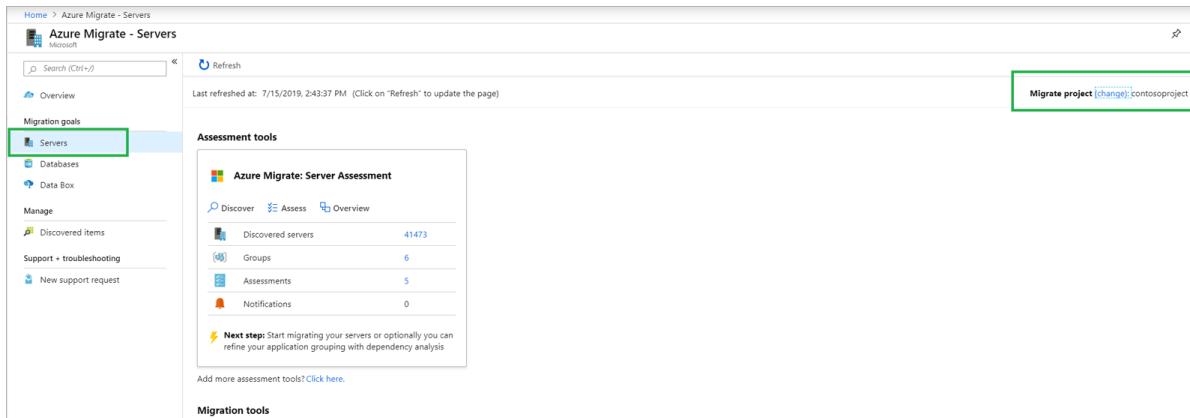
Create a project for the first time

The first time you set up Azure Migrate, you create a project and add an assessment or migration tool. [Follow these instructions](#) to set up for the first time.

Create additional projects

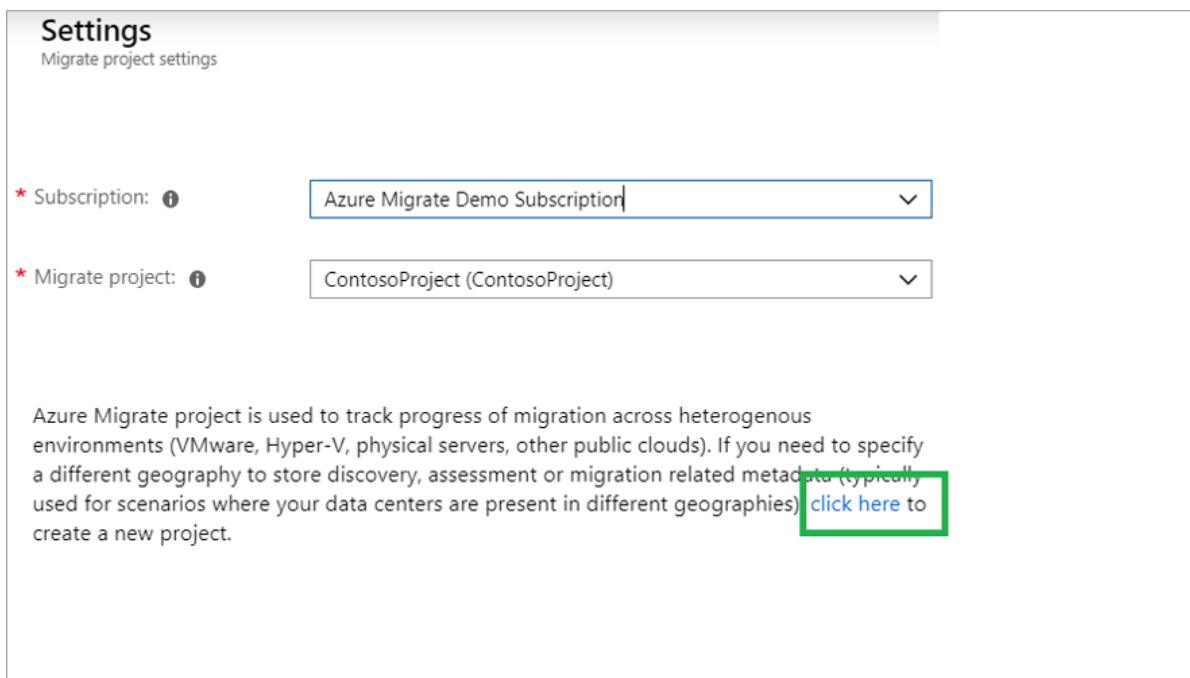
If you already have an Azure Migrate project and you want to create an additional project, do the following:

1. In the [Azure portal](#), search for **Azure Migrate**.
2. On the Azure Migrate dashboard > **Servers**, select **change** in the upper-right corner.



The screenshot shows the Azure Migrate - Servers dashboard. The left sidebar has a 'Migration goals' section with 'Servers' selected, indicated by a green box. The main area is titled 'Assessment tools' and contains a sub-section 'Azure Migrate: Server Assessment' with tabs for 'Discover', 'Assess', and 'Overview'. Below these are four metrics: 'Discovered servers' (41473), 'Groups' (6), 'Assessments' (5), and 'Notifications' (0). A note at the bottom says 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. At the bottom of the page, there's a link 'Add more assessment tools? Click here.' and a 'Migration tools' section.

3. To create a new project, select [click here](#).



The screenshot shows the 'Settings' page for creating a new project. It has a header 'Settings' and 'Migrate project settings'. There are two dropdown menus: one for 'Subscription' (selected: 'Azure Migrate Demo Subscription') and one for 'Migrate project' (selected: 'ContosoProject (ContosoProject)'). Below these, a note states: 'Azure Migrate project is used to track progress of migration across heterogenous environments (VMware, Hyper-V, physical servers, other public clouds). If you need to specify a different geography to store discovery, assessment or migration related metadata (typically used for scenarios where your data centers are present in different geographies) [click here](#) to create a new project.' A green box highlights the 'click here' link.

Find a project

Find a project as follows:

1. In the [Azure portal](#), search for **Azure Migrate**.
2. In the Azure Migrate dashboard > **Servers**, select **change** in the upper-right corner.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation menu with 'Servers' highlighted. The main area has a title 'Azure Migrate: Server Assessment' with tabs for 'Discover', 'Assess', and 'Overview'. Under 'Discover', it shows 41473 discovered servers, 6 groups, 5 assessments, and 0 notifications. A note says 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. At the bottom right, there's a button labeled 'Migrate project [change]: contosoproject'.

3. Select the appropriate subscription and Azure Migrate project.

If you created the project in the [previous version](#) of Azure Migrate, find it as follows:

1. In the [Azure portal](#), search for **Azure Migrate**.
2. In the Azure Migrate dashboard, if you've created a project in the previous version, a banner referencing older projects appears. Select the banner.

The screenshot shows the Azure Migrate dashboard with a prominent banner at the top: 'Azure Migrate is now a hub for all your migration needs and tools. Get started by clicking on "Assess and Migrate servers". If you had previously performed discovery and assessments with the classic Azure Migrate experience, click here to access your older projects.' Below the banner, there are sections for 'Discover, assess and migrate servers', 'Assess and migrate databases', and 'Assess and migrate web apps to Azure'. Each section has a 'Assess and migrate' button.

3. Review the list of old projects.

Delete a project

Delete as follows:

1. Open the Azure resource group in which the project was created.
2. In the resource group page, select **Show hidden types**.
3. Select the migrate project you want to delete, and its associated resources.
 - The resource type is **Microsoft.Migrate/migrateprojects**.
 - If the resource group is exclusively used by the Azure Migrate project, you can delete the entire resource group.

Note that:

- When you delete, both the project and the metadata about discovered machines are deleted.
- If you're using the older version of Azure Migrate, open the Azure resource group in which the project was created. Select the migrate project you want to delete (the resource type is **Migration project**).

- If you're using dependency analysis with an Azure Log Analytics workspace:
 - If you've attached a Log Analytics workspace to the Server Assessment tool, the workspace isn't automatically deleted. The same Log Analytics workspace can be used for multiple scenarios.
 - If you want to delete the Log Analytics workspace, do that manually.

Delete a workspace manually

1. Browse to the Log Analytics workspace attached to the project.

- If you haven't deleted the Azure Migrate project, you can find the link to the workspace in **Essentials > Server Assessment**.

Home > Azure Migrate - Servers > Azure Migrate: Server Assessment

Azure Migrate: Server Assessment

ContosoProject

Search (Ctrl+ /)

Assess servers Replicate

Overview

Manage

- Assessments
- Groups
- Agent health
- Notifications

Resource group
ContosoProject

Location
West Europe

Subscription
Azure Migrate Demo Subscription

Subscription ID [REDACTED]

Groups	6
Assessments	5
Machines	41480

OMS Workspace
Requires configuration

- If you've already deleted the Azure Migrate project, select **Resource Groups** in the left pane of the Azure portal and find the workspace.

2. [Follow the instructions](#) to delete the workspace.

Next steps

Add [assessment](#) or [migration](#) tools to Azure Migrate projects.

This article describes how to add an assessment or migration tool to an [Azure Migrate](#) project for the first time. Azure Migrate provides a central hub to track discovery, assessment and migration of your on-premises apps and workloads, and private/public cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as other tools and independent software vendor (ISV) [offerings](#).

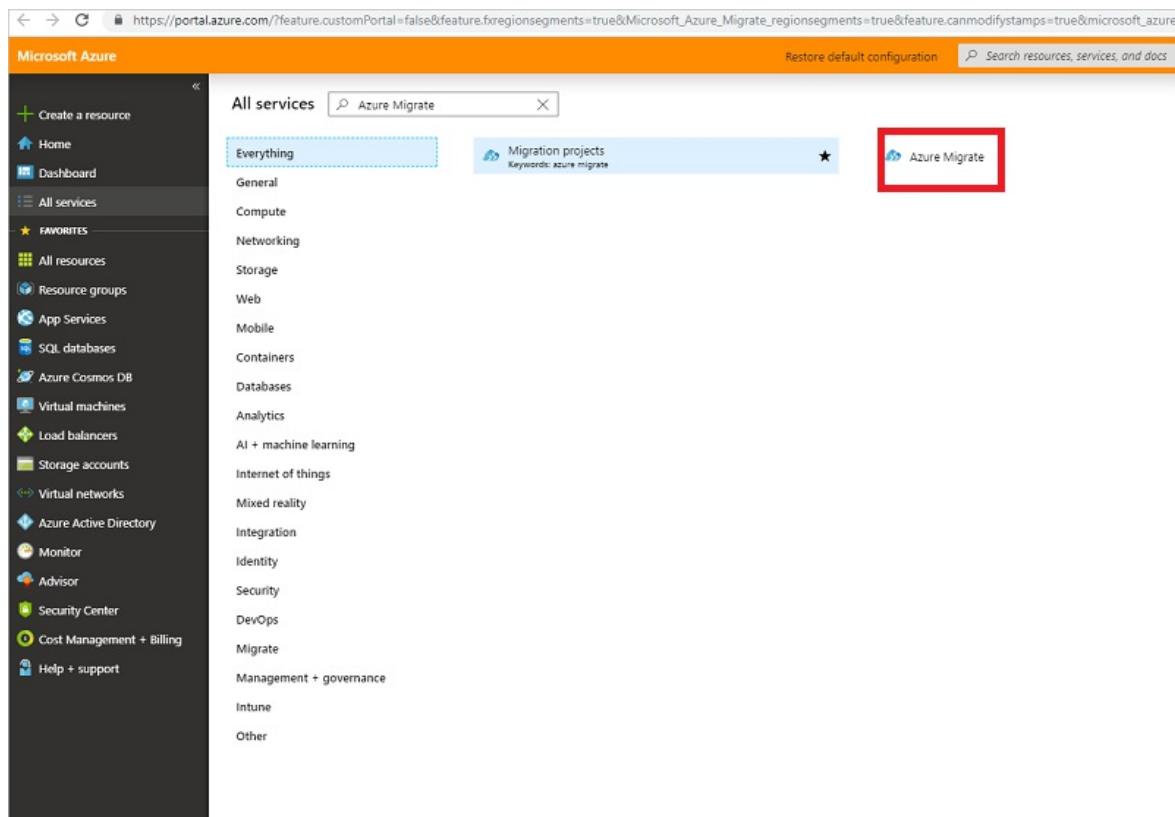
Create a project and add a tool

Set up a new Azure Migrate project in an Azure subscription, and add a tool.

- An Azure Migrate project is used to store discovery, assessment, and migration metadata collected from the environment you're assessing or migrating.
- In a project you can track discovered assets, and orchestrate assessment and migration.

1. In the Azure portal > **All services**, search for **Azure Migrate**.

2. Under **Services**, select **Azure Migrate**.



3. In **Overview**, click **Assess and migrate servers**.

4. Under **Discover, assess and migrate servers**, click **Assess and migrate servers**.

Azure Migrate

Microsoft

Get started

Search (Ctrl+ /)

Overview

Migration goals

- Servers
- Databases
- Data Box

Manage

- Discovered items

Support + troubleshooting

New support request

Migrate your on-premises datacenter to Azure

Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or [find an expert](#) to help with your migration. [Learn more](#)

Assess and migrate web apps to Azure

Assess, migrate and optimize .NET web apps to Azure's Platform-as-a-Service, Azure App Service.

[Assess and migrate web apps](#)

Discover, assess and migrate servers

Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.

[Assess and migrate servers](#)

Discover, assess and migrate databases

Discover, assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

[Assess and migrate databases](#)

Migrate on-premises data to Azure

Use the Data Box offline family of products to move large amount of data to Azure.

[Order a Data Box](#)

5. In **Discover, assess and migrate servers**, click **Add tools**.
6. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
7. In **Project Details**, specify the project name, and geography in which you want to create the project.

Add a tool

[Migrate project](#) [Select assessment tool](#) [Select migration tool](#) [Review + add tool\(s\)](#)

A migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.

* Subscription ?	<input type="text" value="<subscription-name>"/>
└─ * Resource group ?	<input type="text" value="ContosoCorporation"/> Create new

PROJECT DETAILS

Specify the name of the migrate project and the preferred geography.

* Migrate project ?	<input type="text" value="Contoso-project"/> ✓
* Region	<input type="text" value="(Asia Pacific) Southeast Asia"/> ▼

You can create an Azure Migrate project in any of these geographies.

GEOGRAPHY	STORAGE LOCATION REGION
Asia	Southeast Asia or East Asia
Europe	North Europe or West Europe
Japan	Japan East or Japan West
United Kingdom	UK South or UK West
United States	Central US or West US 2
Canada	Canada Central
India	India Central or India South

GEOGRAPHY	STORAGE LOCATION REGION
Australia	Australia SouthEast

The geography specified for the project is only used to store the metadata gathered from on-premises VMs. You can select any target region for the actual migration.

If you want to specify a specific region within a geography for deploying the migrate project and its associated resources (Policy restrictions in your subscription may allow deploying of Azure resources only to a specific Azure region), you can use the below API to create a migrate project. Specify the Subscription ID, Resource group name, Migrate project name along with location(any of the Azure regions mentioned in the table where Azure Migrate is deployed.)

```
PUT
/subscriptions/<subid>/resourceGroups/<rg>/providers/Microsoft.Migrate/MigrateProjects/<mymigrateprojectname>?
api-version=2018-09-01-preview "<location: 'centralus', properties: {}>"
```

- Click **Next**, and add an assessment or migration tool.

NOTE

When you create a project you need to add at least one assessment or migration tool.

- In **Select assessment tool**, add an assessment tool. If you don't need an assessment tool, select **Skip adding an assessment tool for now > Next**.
- In **Select migration tool**, add a migration tool as required. If you don't need a migration tool right now, select **Skip adding a migration tool for now > Next**.
- In **Review + add tools**, review the settings and click **Add tools**.

After creating the project you can select additional tools for assessment and migration of servers and workloads, databases, and web apps.

Create additional projects

In some circumstances, you might need to create additional Azure Migrate projects. For example if you have datacenters in different geographies, or you need to store metadata in a different geography. Create an additional project as follows:

- In the current Azure Migrate project, click **Servers or Databases**.
- In the top right-hand corner, click **Change** next to the current project name.
- In **Settings**, select **Click here to create a new project**.
- Create a new project and add a new tool as described in the previous procedure.

Next steps

Learn how to add additional [assessment](#) and [migration](#) tools.

Add assessment tools

11/19/2019 • 2 minutes to read • [Edit Online](#)

This article describes how to add assessment tools in [Azure Migrate](#).

Azure Migrate provides a hub of tools for assessment and migration to Azure. It includes Azure Migrate tools, as well as other tools and independent software vendor (ISV) offerings.

If you want to add an assessment tool and you don't yet have an Azure Migrate project, follow this [article](#).

Select a tool

If you choose a non-Azure Migrate tool for assessment, start by obtaining a license, or signing up for a free trial, in accordance with the tool policy. Tools have an option to connect to Azure Migrate. Follow the instructions and documentation, to connect the tool to Azure Migrate. [Learn more](#) about tools.

Select an assessment scenario

1. In the Azure Migrate project, click [Overview](#).
2. Select the assessment scenario you want to use:
 - To discover and assess machines and workloads for migration to Azure, select [Assess and migrate servers](#).
 - To assess on-premises SQL machines, select [Assess and migrate databases](#).
 - To assess on-premises web apps, select [Assess and migrate web apps](#).

Migrate your on-premises datacenter to Azure

Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or [find an expert](#) to help with your migration. [Learn more](#)



Discover, assess and migrate servers

Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.

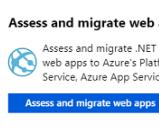
[Assess and migrate servers](#)



Assess and migrate databases

Assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

[Assess and migrate databases](#)



Assess and migrate web apps to Azure

Assess and migrate .NET and PHP web apps to Azure's Platform-as-a-Service, Azure App Service.

[Assess and migrate web apps](#)



Migrate on-premises data to Azure

Use the Data Box offline family of products to move large amount of data to Azure.

[Order a Data Box](#)

Select a server assessment tool

1. Click [Assess and Migrate Servers](#).
2. In **Azure Migrate - Servers**, if you haven't added an assessment tool, under **Assessment tools**, select [Click here to add an assessment tool](#). If you've already added assessment tools, in **Add more assessment tools**, select [Change](#).

NOTE

If you need to navigate to a different project, in **Azure Migrate - Servers**, next to **See details for a different migrate project**, click [Click here](#).

3. In **Azure Migrate**, select the assessment tool you want to use.

- If you use Azure Migrate Server Assessment, you can set up, run, and view assessments directly in the Azure Migrate project.
- If you use a different assessment tool, navigate to the link provided for their site, and run the assessment in accordance with the instructions they provide.

Select a database assessment tool

1. Click **Assess and migrate databases**
2. In **Databases**, click **Add tools**.
3. In Add a tool > **Select assessment tool**, select the tool you want to use to assess your database.

Select a web app assessment tool

1. Click **Assess and migrate web apps**.
2. Follow the link to the Migration tool for the Azure App Service. Use the migration tool to:
 - **Assess apps online**: You can assess apps with a public URL online, using the Azure App Service Migration Assistant.
 - **.NET/PHP**: For internal .NET and PHP apps, you can download and run the Migration Assistant.

Next steps

Try out an assess using Azure Migrate Server Assessment for [VMware VMs](#), [Hyper-V](#), or [physical servers](#)

Set up an appliance for VMware VMs

3/26/2020 • 5 minutes to read • [Edit Online](#)

This article describes how to set up the Azure Migrate appliance for assessment with the [Azure Migrate:Server Assessment](#) tool, and for agentless migration using the [Azure Migrate:Server Migration](#) tool.

The [Azure Migrate appliance](#) is a lightweight appliance used by Azure Migrate:Server Assessment and Server Migration to discover on-premises VMware VMs, send VM metadata/performance data to Azure, and for replication of VMware VMs during agentless migration.

You can set up the Azure Migrate appliance for VMware VM assessment using an OVA template that you download, or using a PowerShell installation script. This article describes how to set up the appliance using the OVA template. If you want to set up the appliance using the script, follow the instructions in [this article](#).

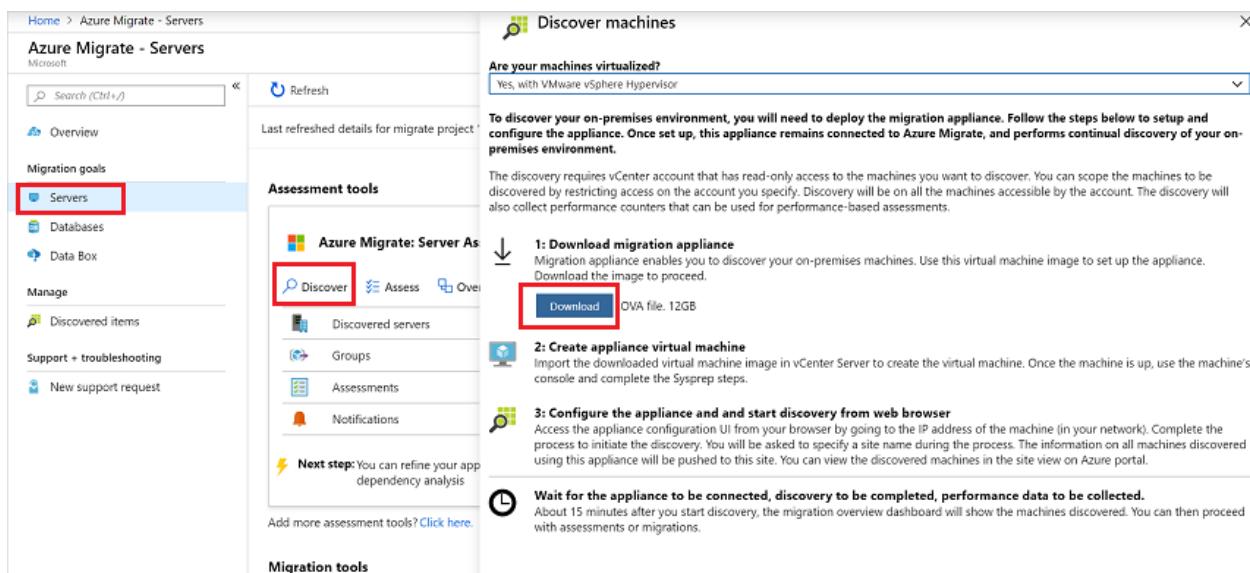
Appliance deployment (OVA)

To set up the appliance using an OVA template you:

- Download an OVA template file, and import it to vCenter Server.
- Create the appliance, and check that it can connect to Azure Migrate Server Assessment.
- Configure the appliance for the first time, and register it with the Azure Migrate project.

Download the OVA template

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines > Are your machines virtualized?**, click **Yes, with VMWare vSphere hypervisor**.
3. Click **Download** to download the .OVA template file.



The screenshot shows the Azure Migrate - Servers interface. On the left, there's a navigation sidebar with 'Overview', 'Migration goals' (where 'Servers' is selected and highlighted with a red box), 'Databases', 'Data Box', 'Manage' (with 'Discovered items'), 'Support + troubleshooting', and 'New support request'. The main area has a title 'Discover machines' and a question 'Are your machines virtualized?'. A dropdown menu shows 'Yes, with VMWare vSphere Hypervisor'. Below this, there's a section titled 'Azure Migrate: Server As' with 'Discover' (highlighted with a red box), 'Assess', and 'Overview' buttons. Under 'Discover', there are links for 'Discovered servers', 'Groups', 'Assessments', and 'Notifications'. A note says 'Next step: You can refine your app dependency analysis'. At the bottom of the main area, there's a 'Migration tools' section. To the right, a large panel provides steps for setting up the appliance: 1. Download migration appliance (button highlighted with a red box), 2. Create appliance virtual machine, 3. Configure the appliance and start discovery from web browser, and 4. Wait for the appliance to be connected, discovery to be completed, performance data to be collected. It also mentions that about 15 minutes after starting discovery, the migration overview dashboard will show discovered machines.

Verify security

Check that the OVA file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following command, to generate the hash for the OVA:

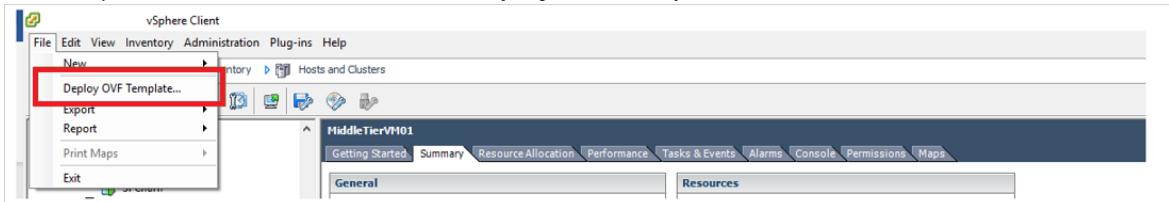
• `C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]`

- Example usage: `C:\>CertUtil -HashFile C:\AzureMigrate\AzureMigrate.ova SHA256`
3. For the latest appliance version, the generated hash should match these [settings](#).

Create the appliance VM

Import the downloaded file, and create a VM.

1. In the vSphere Client console, click **File > Deploy OVF Template**.



2. In the Deploy OVF Template Wizard > **Source**, specify the location of the OVA file.
3. In **Name and Location**, specify a friendly name for the VM. Select the inventory object in which the VM will be hosted.
4. In **Host/Cluster**, specify the host or cluster on which the VM will run.
5. In **Storage**, specify the storage destination for the VM.
6. In **Disk Format**, specify the disk type and size.
7. In **Network Mapping**, specify the network to which the VM will connect. The network needs internet connectivity, to send metadata to Azure Migrate Server Assessment.
8. Review and confirm the settings, then click **Finish**.

Verify appliance access to Azure

Make sure that the appliance VM can connect to [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time. If you deploy the appliance using a script instead of an OVA template, the first two steps in the procedure aren't applicable.

1. In the vSphere Client console, right-click the VM > **Open Console**.
2. Provide the language, time zone, and password for the appliance.
3. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app:
`https://appliance name or IP address: 44368`.

Alternately, you can open the app from the appliance desktop by clicking the app shortcut.

4. In the web app > **Set up prerequisites**, do the following:
 - **License**: Accept the license terms, and read the third-party information.
 - **Connectivity**: The app checks that the VM has internet access. If the VM uses a proxy:
 - Click **Proxy settings**, and specify the proxy address and listening port, in the form `http://ProxyIPAddress` or `http://ProxyFQDN`.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
 - **Time sync**: Time is verified. The time on the appliance should be in sync with internet time for discovery to work properly.
 - **Install updates**: Azure Migrate checks that the latest appliance updates are installed.

- **Install VDDK:** Azure Migrate checks that the VMWare vSphere Virtual Disk Development Kit (VDDK) is installed.
 - Azure Migrates uses the VDDK to replicate machines during migration to Azure.
 - Download VDDK 6.7 from VMware, and extract the downloaded zip contents to the specified location on the appliance.

Register the appliance with Azure Migrate

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
 - Sign in with your username and password.
 - Sign in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

Start continuous discovery by providing vCenter Server and VM credential

The appliance needs to connect to vCenter Server to discover the configuration and performance data of the VMs.

Specify vCenter Server details

1. In **Specify vCenter Server details**, specify the name (FQDN) or IP address of the vCenter Server. You can leave the default port, or specify a custom port on which your vCenter Server listens.
2. In **User name** and **Password**, specify the read-only account credentials that the appliance will use to discover VMs on the vCenter server. You can scope the discovery by limiting access to the vCenter account. [Learn more](#).
3. Click **Validate connection** to make sure that the appliance can connect to vCenter Server.

Specify VM credentials

For discovery of applications, roles and features and visualizing dependencies of the VMs, you can provide a VM credential that has access to the VMware VMs. You can add one credential for Windows VMs and one credential for Linux VMs. [Learn more](#) about the access privileges needed.

NOTE

This input is optional and is needed to enable application discovery and agentless dependency visualization.

1. In **Discover applications and dependencies on VMs**, click **Add credentials**.
2. Select the **Operating System**.
3. Provide a friendly name for the credential.
4. In **Username** and **Password**, specify an account that has at least guest access on the VMs.
5. Click **Add**.

Once you have specified the vCenter Server and VM credentials (optional), click **Save and start discovery** to start discovery of the on-premises environment.

It takes around 15 minutes for metadata of discovered VMs to appear in the portal. Discovery of installed applications, roles, and features takes some time, the duration depends on the number of VMs being discovered.

For 500 VMs, it takes approximately 1 hour for the application inventory to appear in the Azure Migrate portal.

Next steps

Review the tutorials for [VMware assessment](#) and [agentless migration](#).

This article describes how to set up the Azure Migrate appliance for assessment of Hyper-V VMs with the [Azure Migrate:Server Assessment](#) tool.

The [Azure Migrate appliance](#) is a lightweight appliance used by Azure Migrate:Server Assessment/Migration to discover on-premises Hyper-V VMs, and send VM metadata/performance data to Azure.

You can set up the Azure Migrate appliance for Hyper-V VM assessment using a VHD template that you download, or using a PowerShell installation script. This article describes how to set up the appliance using the VHD template. If you want to set up the appliance using the script, follow the instructions in [this article](#).

Appliance deployment (VHD)

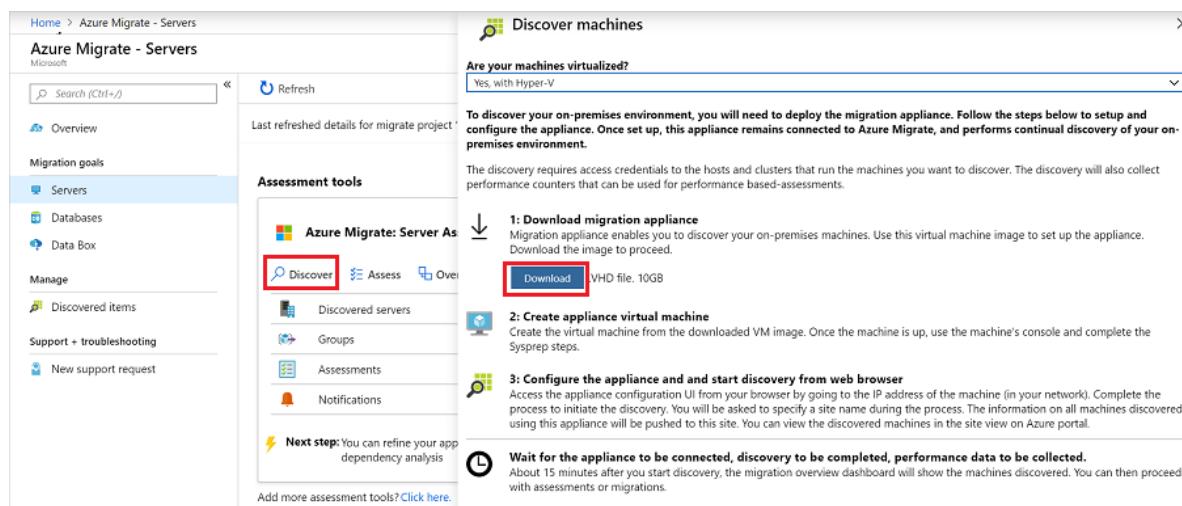
To set up the appliance using a VHD template:

- Download a compressed Hyper-V VHD from the Azure portal.
- Create the appliance, and check that it can connect to Azure Migrate Server Assessment.
- Configure the appliance for the first time, and register it with the Azure Migrate project.

Download the VHD

Download the zipped VHD template for the appliance.

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines > Are your machines virtualized?**, click **Yes, with Hyper-V**.
3. Click **Download** to download the VHD file.



Verify security

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following command to generate the hash for the VHD

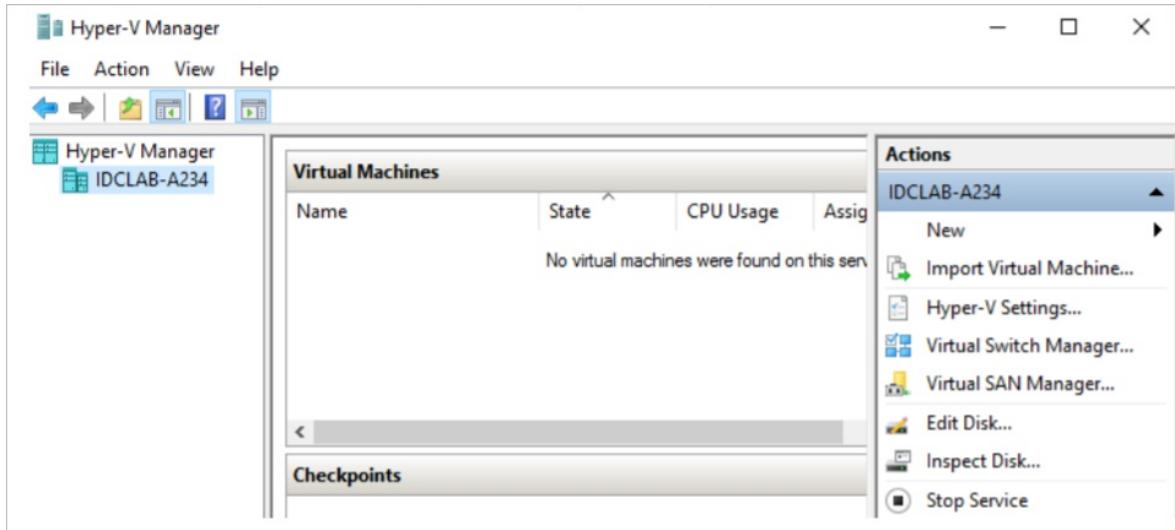
- `C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]`
- Example usage: `C:\>CertUtil -HashFile C:\AzureMigrate\AzureMigrate.vhd SHA256`

3. For appliance version 2.19.11.12, the generated hash should match these [settings](#).

Create the appliance VM

Import the downloaded file, and create the VM.

1. Extract the zipped VHD file to a folder on the Hyper-V host that will host the appliance VM. Three folders are extracted.
2. Open Hyper-V Manager. In Actions, click Import Virtual Machine.



3. In the Import Virtual Machine Wizard > **Before you begin**, click **Next**.
4. In **Locate Folder**, specify the folder containing the extracted VHD. Then click **Next**.
5. In **Select Virtual Machine**, click **Next**.
6. In **Choose Import Type**, click **Copy the virtual machine (create a new unique ID)**. Then click **Next**.
7. In **Choose Destination**, leave the default setting. Click **Next**.
8. In **Storage Folders**, leave the default setting. Click **Next**.
9. In **Choose Network**, specify the virtual switch that the VM will use. The switch needs internet connectivity to send data to Azure.
10. In **Summary**, review the settings. Then click **Finish**.
11. In Hyper-V Manager > **Virtual Machines**, start the VM.

Verify appliance access to Azure

Make sure that the appliance VM can connect to [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time. If you deploy the appliance using a script instead of a VHD, the first two steps in the procedure aren't applicable.

1. In Hyper-V Manager > **Virtual Machines**, right-click the VM > **Connect**.
2. Provide the language, time zone, and password for the appliance.
3. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app:
<https://appliance name or IP address: 44368>.

Alternately, you can open the app from the appliance desktop by clicking the app shortcut.

4. In the web app > **Set up prerequisites**, do the following:

- **License:** Accept the license terms, and read the third-party information.
- **Connectivity:** The app checks that the VM has internet access. If the VM uses a proxy:
 - Click **Proxy settings**, and specify the proxy address and listening port, in the form `http://ProxyIPAddress` or `http://ProxyFQDN`.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
- **Time sync:** Time is verified. The time on the appliance should be in sync with internet time for VM discovery to work properly.
- **Install updates:** Azure Migrate Server Assessment checks that the appliance has the latest updates installed.

Register the appliance with Azure Migrate

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
 - Sign in with your username and password.
 - Sign-in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

Delegate credentials for SMB VHDS

If you're running VHDS on SMBs, you must enable delegation of credentials from the appliance to the Hyper-V hosts. To do this from the appliance:

1. On the appliance VM, run this command. HyperVHost1/HyperVHost2 are example host names.

```
Enable-WSManCredSSP -Role Client -DelegateComputer HyperVHost1.contoso.com HyperVHost2.contoso.com -Force
```

2. Alternatively, do this in the Local Group Policy Editor on the appliance:

- In **Local Computer Policy** > **Computer Configuration**, click **Administrative Templates** > **System** > **Credentials Delegation**.
- Double-click **Allow delegating fresh credentials**, and select **Enabled**.
- In **Options**, click **Show**, and add each Hyper-V host you want to discover to the list, with `wsman/` as a prefix.
- In **Credentials Delegation**, double-click **Allow delegating fresh credentials with NTLM-only server authentication**. Again, add each Hyper-V host you want to discover to the list, with `wsman/` as a prefix.

Start continuous discovery

Connect from the appliance to Hyper-V hosts or clusters, and start VM discovery.

1. In **User name** and **Password**, specify the account credentials that the appliance will use to discover VMs. Specify a friendly name for the credentials, and click **Save details**.
2. Click **Add host**, and specify Hyper-V host/cluster details.

3. Click **Validate**. After validation, the number of VMs that can be discovered on each host/cluster is shown.

- If validation fails for a host, review the error by hovering over the icon in the **Status** column. Fix issues, and validate again.
- To remove hosts or clusters, select > **Delete**.
- You can't remove a specific host from a cluster. You can only remove the entire cluster.
- You can add a cluster, even if there are issues with specific hosts in the cluster.

4. After validation, click **Save and start discovery** to start the discovery process.

This starts discovery. It takes around 15 minutes for metadata of discovered VMs to appear in the Azure portal.

Verify VMs in the portal

After discovery finishes, you can verify that the VMs appear in the portal.

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers > Azure Migrate: Server Assessment** page, click the icon that displays the count for **Discovered servers**.

Next steps

Try out [Hyper-V assessment](#) with Azure Migrate Server Assessment.

This article describes how to set up the [Azure Migrate appliance](#) using a PowerShell installer script.

The script provides:

- An alternative to setting up the appliance using an OVA template, for assessment and agentless migration of VMware VMs.
- An alternative to setting up the appliance using a VHD template, for assessment and migration of Hyper-V VMs.
- For assessment of physical servers (or VMs that you want to migrate as physical servers), the script is the only method for setting up the appliance.

Prerequisites

The script sets up the Azure Migrate appliance on an existing physical machine or VM.

- The machine that will act as the appliance must be running Windows Server 2016, with 32 GB of memory, eight vCPUs, around 80 GB of disk storage, and an external virtual switch. It requires a static or dynamic IP address, and access to the internet.
- Before you deploy the appliance, review detailed appliance requirements for [VMware VMs](#), [Hyper-V VMs](#), and [physical servers](#).
- Don't run the script on an existing Azure Migrate appliance.

Download the script

1. Locate the machine/VM that will act as the Azure Migrate appliance.

2. On the machine, do the following:

- To use the appliance with VMware VMs or Hyper-V VMs, [download](#) the zipped folder containing the installer script and the MSIs.
- To use the appliance with physical servers, download the script from the Azure Migrate portal, as described in this [tutorial](#).

Verify file security

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.

2. Run the following command to generate the hash for the zipped file

- `C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]`
- Example usage:
`C:\>CertUtil -HashFile C:\Users\administrator\Desktop\AzureMigrateInstaller.zip SHA256`

3. Verify that the generated hash values match these settings (for the latest appliance version):

ALGORITHM	HASH VALUE
MD5	1e92ede3e87c03bd148e56a708cd33f

ALGORITHM	HASH VALUE
SHA256	a3fa78edc8ff8aff9ab5ae66be1b64e66de7b9f475b6542beef114b20bfdac3c

Run the script

Here's what the script does:

- Installs agents and a web application.
- Installs Windows roles, including Windows Activation Service, IIS, and PowerShell ISE.
- Downloads and installs an IIS rewritable module. [Learn more](#).
- Updates a registry key (HKLM), with persistent settings for Azure Migrate.
- Creates log and configuration files as follows:
 - **Config Files:** %ProgramData%\Microsoft Azure\Config
 - **Log Files:** %ProgramData%\Microsoft Azure\Logs

To run the script:

1. Extract the zipped file to a folder on the machine that will host the appliance.
2. Launch PowerShell on the machine, with administrator (elevated) privileges.
3. Change the PowerShell directory to the folder containing the contents extracted from the downloaded zipped file.
4. Run the script **AzureMigrateInstaller.ps1** as follows:

- For VMware:

```
PS C:\Users\administrator\Desktop\AzureMigrateInstaller> AzureMigrateInstaller.ps1 -scenario
VMware
```

- For Hyper-V:

```
PS C:\Users\administrator\Desktop\AzureMigrateInstaller> AzureMigrateInstaller.ps1 -scenario
HyperV
```

- For physical servers:

```
PS C:\Users\administrator\Desktop\AzureMigrateInstaller> AzureMigrateInstaller.ps1
```

5. After the script runs successfully, it launches the appliance web application so that you can set up the appliance. If you encounter any issues, you can view the script logs at C:\ProgramData\Microsoft Azure\Logs\AzureMigrateScenarioInstaller_.Timestamp.log.

Next steps

After you've set up the appliance using the script, follow these instructions:

- Set up the appliance for [VMware](#).
- Set up the appliance for [Hyper-V](#).
- Set up the appliance for [physical servers](#).

This article describes how to set up the Azure Migrate appliance if you're assessing physical servers with the Azure Migrate: Server Assessment tool.

The Azure Migrate appliance is a lightweight appliance, used by Azure Migrate Server Assessment to do the following:

- Discover on-premises servers.
- Send metadata and performance data for discovered servers to Azure Migrate Server Assessment.

[Learn more](#) about the Azure Migrate appliance.

Appliance deployment steps

To set up the appliance you:

- Download a zipped file with Azure Migrate installer script from the Azure portal.
- Extract the contents from the zipped file. Launch the PowerShell console with administrative privileges.
- Execute the PowerShell script to launch the appliance web application.
- Configure the appliance for the first time, and register it with the Azure Migrate project.

Download the installer script

Download the zipped file for the appliance.

1. In **Migration Goals > Servers > Azure Migrate: Server Assessment**, click **Discover**.
2. In **Discover machines > Are your machines virtualized?**, click **Not virtualized/Other**.
3. Click **Download** to download the zipped file.

Home > Azure Migrate - Servers > Discover machines

Discover machines

[Discover using appliance](#) Import using CSV

Are your machines virtualized?

Not virtualized / Other

To discover your on-premises environment, you will need to deploy the Azure Migrate appliance. Follow the steps below to setup and configure the appliance. Once set up, this appliance remains connected to Azure Migrate, and performs continuous discovery of your on-premises environment.

The discovery requires access credentials to the physical servers you want to discover. The discovery will also collect performance counters that can be used for performance-based assessments.

1: Download Azure Migrate appliance
The Azure Migrate appliance enables you to discover your on-premises machines. Use this PowerShell script to set up the appliance. Download the zipped folder to proceed.

[Download](#) .zip file. 50MB

Run the script to set up the appliance
Before you start, ensure these [prerequisites](#) are met. Run the script to deploy the appliance configuration manager either on a virtual machine or a physical server.

3: Configure the appliance and and start discovery from web browser
Access the appliance configuration UI from your browser by going to the IP address of the machine (in your network). Complete the process to initiate the discovery.

Wait for the appliance to be connected, discovery to be completed, performance data to be collected.
About 15 minutes after you start discovery, the migration overview dashboard will show the machines discovered. You can then proceed with assessments or migrations.

Verify security

Check that the zipped file is secure, before you deploy it.

1. On the machine to which you downloaded the file, open an administrator command window.
2. Run the following command to generate the hash for the VHD
 - `C:\>CertUtil -HashFile <file_location> [Hashing Algorithm]`
 - Example usage: `C:\>CertUtil -HashFile C:\AzureMigrate\AzureMigrate.ova SHA256`
3. For the latest appliance version, the generated hash should match these [settings](#).

Run the Azure Migrate installer script

The installer script does the following:

- Installs agents and a web application for physical server discovery and assessment.
- Install Windows roles, including Windows Activation Service, IIS, and PowerShell ISE.
- Download and installs an IIS rewritable module. [Learn more](#).
- Updates a registry key (HKLM) with persistent setting details for Azure Migrate.
- Creates the following files under the path:
 - **Config Files:** %Programdata%\Microsoft Azure\Config
 - **Log Files:** %Programdata%\Microsoft Azure\Logs

Run the script as follows:

1. Extract the zipped file to a folder on the server that will host the appliance.
2. Launch PowerShell on the above server with administrative (elevated) privilege.
3. Change the PowerShell directory to the folder where the contents have been extracted from the downloaded zipped file.
4. Run the script named **AzureMigrateInstaller.ps1** by running the following command:

```
PS C:\Users\administrator\Desktop\AzureMigrateInstaller> AzureMigrateInstaller.ps1
```

The script will launch the appliance web application when it finishes successfully.

In case of any issues, you can access the script logs at C:\ProgramData\Microsoft Azure\Logs\AzureMigrateScenarioInstaller_ Timestamp.log for troubleshooting.

NOTE

Please do not execute the Azure Migrate installer script on an existing Azure Migrate appliance.

Verify appliance access to Azure

Make sure that the appliance VM can connect to the required [Azure URLs](#).

Configure the appliance

Set up the appliance for the first time.

1. Open a browser on any machine that can connect to the VM, and open the URL of the appliance web app:
https://appliance name or IP address: 44368.

Alternately, you can open the app from the desktop by clicking the app shortcut.

2. In the web app > **Set up prerequisites**, do the following:

- **License**: Accept the license terms, and read the third-party information.
- **Connectivity**: The app checks that the VM has internet access. If the VM uses a proxy:
 - Click **Proxy settings**, and specify the proxy address and listening port, in the form http://ProxyIPAddress or http://ProxyFQDN.
 - Specify credentials if the proxy needs authentication.
 - Only HTTP proxy is supported.
- **Time sync**: Time is verified. The time on the appliance should be in sync with internet time for VM discovery to work properly.
- **Install updates**: Azure Migrate Server Assessment checks that the appliance has the latest updates installed.

Register the appliance with Azure Migrate

1. Click **Log In**. If it doesn't appear, make sure you've disabled the pop-up blocker in the browser.
2. On the new tab, sign in using your Azure credentials.
 - Sign in with your username and password.
 - Sign-in with a PIN isn't supported.
3. After successfully signing in, go back to the web app.
4. Select the subscription in which the Azure Migrate project was created. Then select the project.
5. Specify a name for the appliance. The name should be alphanumeric with 14 characters or less.
6. Click **Register**.

Start continuous discovery

Connect from the appliance to physical servers, and start the discovery.

1. Click **Add Credentials** to specify the account credentials that the appliance will use to discover servers.
2. Specify the **Operating System**, friendly name for the credentials, **Username** and **Password** and click **Add**.

You can add one set of credentials each for Windows and Linux servers.

3. Click **Add server**, and specify server details- FQDN/IP address and friendly name of credentials (one entry per row) to connect to the server.
4. Click **Validate**. After validation, the list of servers that can be discovered is shown.
 - If validation fails for a server, review the error by hovering over the icon in the **Status** column. Fix issues, and validate again.
 - To remove a server, select > **Delete**.
5. After validation, click **Save and start discovery** to start the discovery process.

This starts discovery. It takes around 15 minutes for metadata of discovered VMs to appear in the Azure portal.

Verify servers in the portal

After discovery finishes, you can verify that the servers appear in the portal.

1. Open the Azure Migrate dashboard.
2. In **Azure Migrate - Servers > Azure Migrate: Server Assessment** page, click the icon that displays the count for **Discovered servers**.

Next steps

Try out [assessment of physical servers](#) with Azure Migrate Server Assessment.

Set discovery scope for VMware VMs

3/26/2020 • 3 minutes to read • [Edit Online](#)

This article describes how to limit the scope of discovery for VMware VMs that are discovered by the [Azure Migrate appliance](#).

The Azure Migrate appliance discovers on-premises VMware VMs when you:

- Use the [Azure Migrate:Server Assessment](#) tool to assess VMware VMs for migration to Azure.
- Use the [Azure Migrate:Server Migration](#) tool for [agentless migration](#) of VMware VMs to Azure.

Set discovery scope

After you set up the Azure Migrate appliance for VMware VMs assessment or migration, the appliance starts discovering VMs, and sending VM metadata to Azure. Before you connect the appliance to vCenter Server for discovery, you can set the discovery scope to limit discovery to vCenter Server datacenters, clusters, a folder of clusters, hosts, a folder of hosts, or individual VMs.

To set the scope, you assign permissions on the account that Azure Migrate is using to access the vCenter Server.

Create a vCenter user account

If you haven't already set up a vCenter user account that the Azure Migrate appliance uses to discover, assess, and migrate VMware VMs, do that first.

1. Log in to vSphere Web Client as the vCenter Server administrator.
2. Select **Administration > SSO users and Groups**, and click the **Users** tab.
3. Select the **New User** icon.
4. Fill in the new user information > **OK**.

The account permissions depend on what you're deploying.

FEATURE	ACCOUNT PERMISSIONS
Assess	The account needs read-only access.
Discover apps/roles/features	The account needs read-only access, with privileges enabled for Virtual machines > Guest Operations.
Analyze dependencies (agentless)	The account needs read-only access, with privileges enabled for Virtual machines > Guest Operations.
Migrate (agentless)	You need a role that's assigned the right permissions. To create a role, log in to vSphere Web Client as the vCenter Server administrator. Select the vCenter Server instance > Create role . Specify a role name, for example <i>Azure_Migrate</i> , and assign the required permissions to the role.

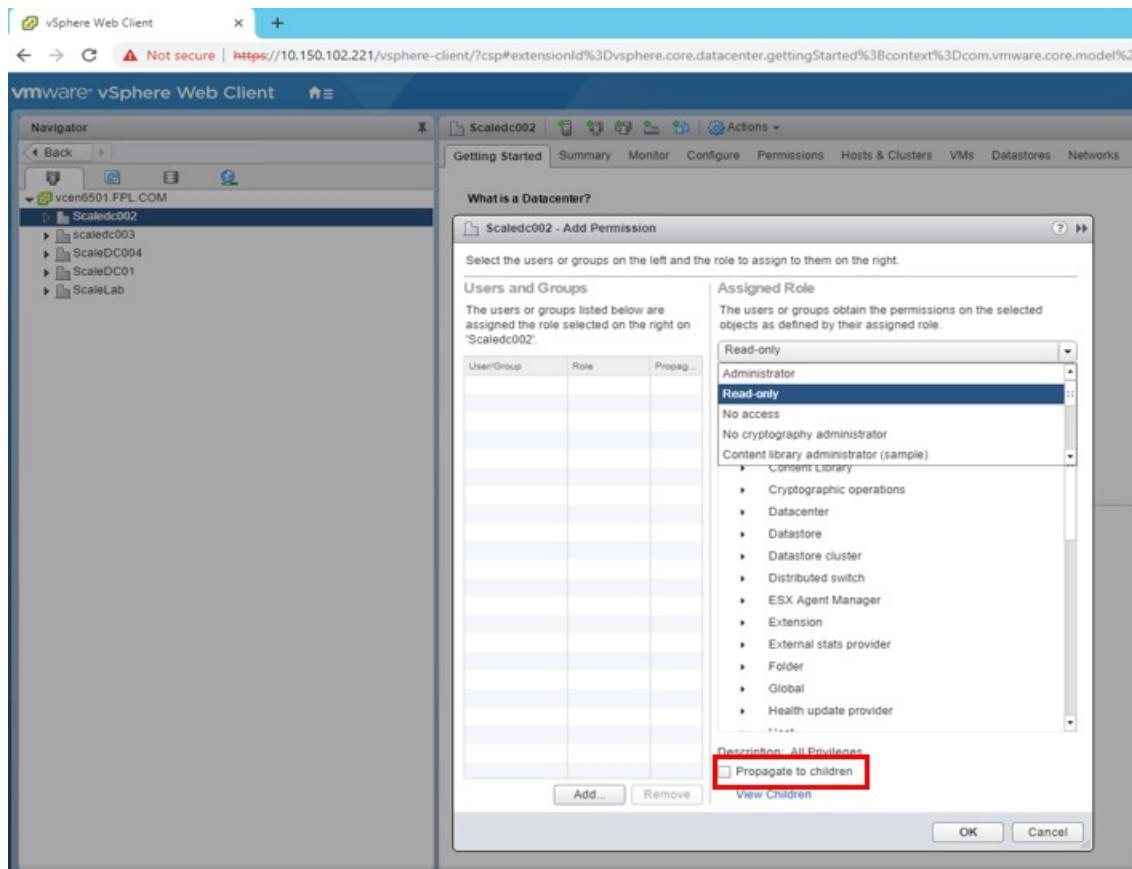
Assign permissions on vCenter objects

You can assign permissions on inventory objects using one of two methods:

- Assign a role with the required permissions, to the account you're using, for all parent objects that host VMs you want to discover/migrate.
- Alternatively, you can assign the role and user account at the datacenter level, and propagate them to the child objects. Then give the account a **No access** role, for every object that you don't want to discover/migrate. We don't recommend this approach since it's cumbersome, and might expose access controls, because every new child object is automatically granted access inherited from the parent.

To assign a role to the account you're using for all relevant objects, do the following:

- **For assessment:** For VM assessment, apply the **Read-only** role to the vCenter user account for all parent objects hosting VMs you want to discover. Parent objects included: host, folder of hosts, cluster, and folder of clusters in the hierarchy, up to the datacenter. Propagate these permissions to child objects in the hierarchy.



- **For agentless migration:** For agentless migration, apply a user-defined role with **required permissions** to the user account, for all parent objects hosting VMs you want to discover. You can name the role *Azure_Migrate*.

Scope support

Currently, the Server Assessment tool can't discover VMs if the vCenter account has access granted at the vCenter VM folder level. Folders of hosts and clusters are supported.

If you want to scope your discovery by VM folders, complete the next procedure to ensure that the vCenter account has read-only access assigned at a VM level.

1. Assign read-only permissions on all VMs in the VM folders you want to scope for discovery.
2. Grant read-only access to all the parent objects that host VMs.
 - All parent objects (host, folder of hosts, cluster, folder of clusters) in the hierarchy up to the datacenter are included.
 - You don't need to propagate the permissions to all child objects.
3. Use the credentials for discovery by selecting the datacenter as **Collection Scope**. The role-based access control setup ensures that the corresponding vCenter user account has access to only tenant-specific VMs.

Next steps

[Set up the appliance](#) and [start continuous discovery](#).

Discover machine apps, roles, and features

3/17/2020 • 2 minutes to read • [Edit Online](#)

This article describes how to discover applications, roles, and features on on-premises servers, using Azure Migrate: Server Assessment.

Discovering the inventory of apps, and roles/features running on your on-premises machines helps you to identify and plan a migration path to Azure that's tailored for your workloads.

NOTE

App discovery is currently in preview for VMware VMs only, and is limited to discovery only. We don't yet offer app-based assessment. Machine-based assessment for on-premises VMware VMs, Hyper-V VMs, and physical servers.

App discovery using Azure Migrate: Server Assessment is agentless. Nothing is installed on machines and VMs. Server Assessment uses the Azure Migrate appliance to perform discovery along with machine guest credentials. The appliance remotely accesses the VMware machines using VMware APIs.

Before you start

1. Make sure you've [created](#) an Azure Migrate project.
2. Make sure you've [added](#) the Azure Migrate: Server Assessment tool to a project.
3. Check the [VMware requirements](#) for discovering and assessing VMware VMs with the Azure Migrate appliance.
4. Check the [requirements](#) for deploying the Azure Migrate appliance.
5. [Verify support and requirements](#) for application discovery.

Prepare for app discovery

1. [Prepare for appliance deployment](#). Preparation includes verifying appliance settings, and setting up an account that the appliance will use to access vCenter Server.
2. Make sure you have a user account (one each for Windows and Linux servers) with administrator permissions for machines on which you want to discover apps, roles, and features.
3. [Deploy the Azure Migrate appliance](#) to start discovery. To deploy the appliance, you download and import an OVA template into VMware to create the appliance as a VMware VM. You configure the appliance and then register it with Azure Migrate.
4. As you deploy the appliance, to start continuous discovery you specify the following:
 - The name of the vCenter Server to which you want to connect.
 - Credentials that you created for the appliance to connect to vCenter Server.
 - The account credentials you created for the appliance to connect to Windows/Linux VMs.

After the appliance is deployed and you've provided credentials, the appliance starts continuous discovery of VM metadata and performance data, along with and discovery of apps, features, and roles. The duration of app discovery depends on how many VMs you have. It typically takes an hour for app-discovery of 500 VMs.

Review and export the inventory

After discovery ends, if you provided credentials for app discovery, you can review and export the app inventory in the Azure portal.

1. In **Azure Migrate - Servers > Azure Migrate: Server Assessment**, click the displayed count to open the **Discovered servers** page.

NOTE

At this stage you can also optionally set up dependency mapping for discovered machines, so that you can visualize dependencies across machines you want to assess. [Learn more](#).

2. In **Applications discovered**, click the displayed count.
3. In **Application inventory**, you can review the discovered apps, roles, and features.
4. To export the inventory, in **Discovered Servers**, click **Export app inventory**.

The app inventory is exported and downloaded in Excel format. The **Application Inventory** sheet displays all the apps discovered across all the machines.

Next steps

- [Create an assessment](#) for lift and shift migration of the discovered servers.
- Assess a SQL Server databases using [Azure Migrate: Database Assessment](#).

This article describes how to create groups of machines for assessment with Azure Migrate: Server Assessment.

Azure Migrate helps you to migrate to Azure. Azure Migrate provides a centralized hub to track discovery, assessment, and migration of on-premises infrastructure, applications, and data to Azure. The hub provides Azure tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

Grouping machines

You gather machines into groups to assess whether they're suitable for migration to Azure, and to get Azure sizing and cost estimations for them. There are a couple of ways to create groups:

- If you know the machines that need be migrated together, you can manually create the group in Azure Migrate.
- If you are not sure about the machines that need to be grouped together, you can use the dependency visualization functionality in Azure Migrate to create groups.

NOTE

The dependency visualization functionality is not available in Azure Government.

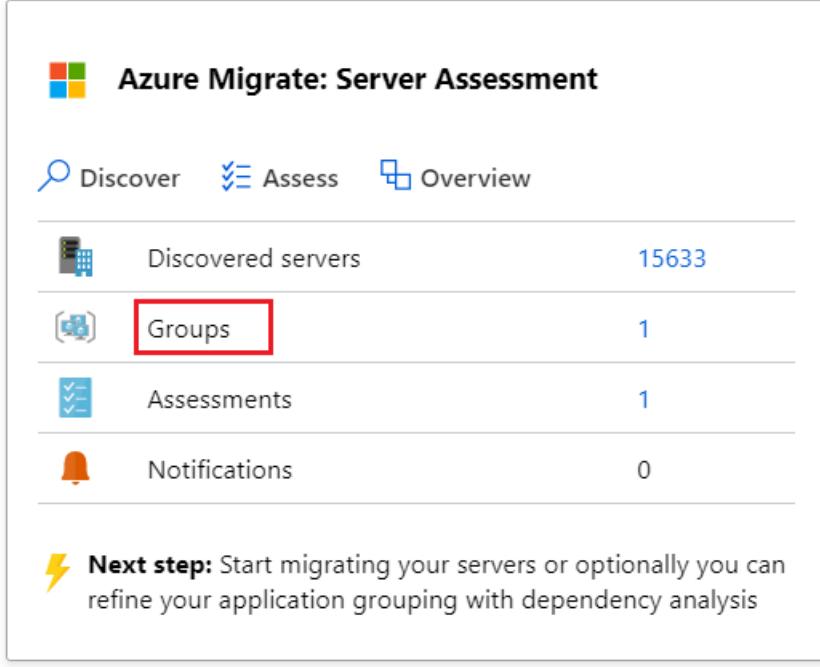
Create a group manually

You can create a group at the same time that you [create an assessment](#).

If you want to create a group manually outside of creating an assessment, do the following:

1. In the Azure Migrate project > **Overview**, click **Assess and migrate servers**. In **Azure Migrate: Server Assessment**, click **Groups**
 - If you haven't yet added the Azure Migrate: Server Assessment tool, click to add it. [Learn more](#).
 - If you haven't yet created an Azure Migrate project, [learn more](#).

Assessment tools



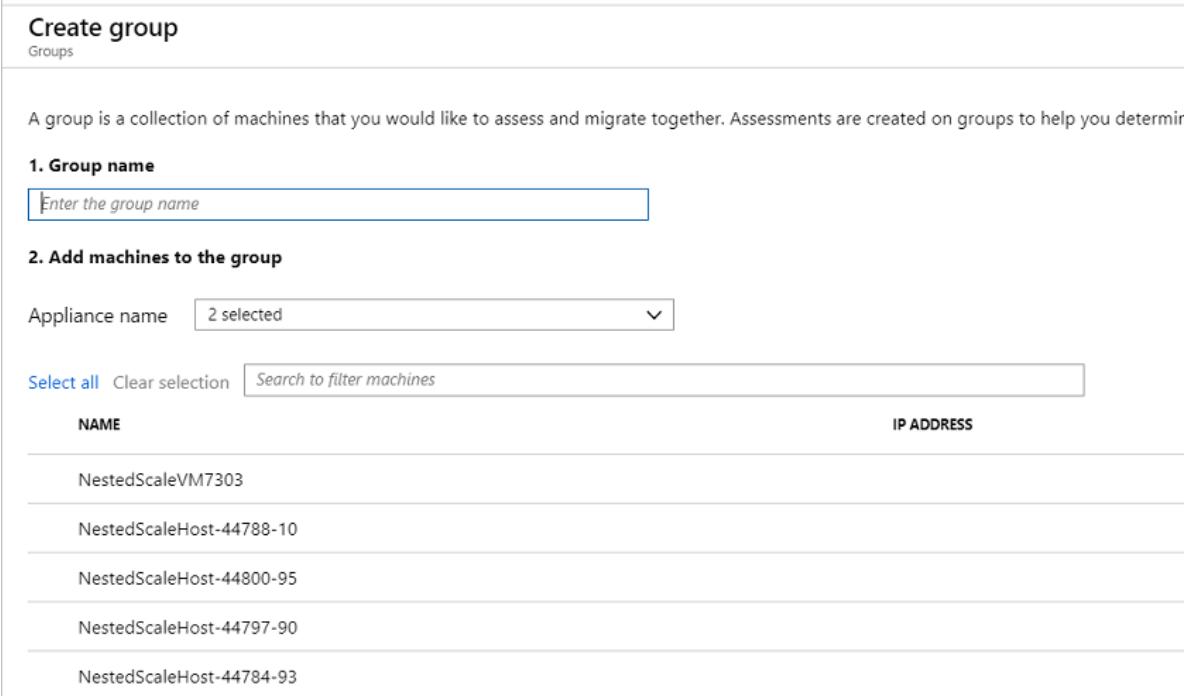
The screenshot shows the Azure Migrate: Server Assessment interface. At the top, there's a navigation bar with 'Discover', 'Assess', and 'Overview' buttons. Below this is a summary table with four rows:

	Discovered servers	15633
	Groups	1
	Assessments	1
	Notifications	0

A yellow lightning bolt icon with the text 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis' is displayed below the table.

At the bottom left, there's a link 'Add more assessment tools? [Click here.](#)'

2. Click the **Group** icon.
3. In **Create group**, specify a group name, and in **Appliance name**, select the Azure Migrate appliance you're using for machine discovery.
4. From the machine list, select the machines you want to add to the group > **Create**.



The screenshot shows the 'Create group' dialog box. It has a header 'Create group' and a sub-header 'Groups'. The main area contains the following steps:

1. **Group name**: A text input field with placeholder text 'Enter the group name'.
2. **Add machines to the group**: A dropdown menu labeled 'Appliance name' with '2 selected' and a '▼' button. Below it is a search bar with 'Select all' and 'Clear selection' buttons, and a 'Search to filter machines' input field.

NAME	IP ADDRESS
NestedScaleVM7303	
NestedScaleHost-44788-10	
NestedScaleHost-44800-95	
NestedScaleHost-44797-90	
NestedScaleHost-44784-93	

You can now use this group when you [create an assessment](#).

Refine a group with dependency mapping

Dependency mapping helps you to visualize dependencies across machines. You typically use dependency mapping when you want to assess machine groups with higher levels of confidence.

- It helps you to cross-check machine dependencies, before you run an assessment.
- It also helps to effectively plan your migration to Azure, by ensuring that nothing is left behind, and thus avoiding surprise outages during migration.
- You can discover interdependent systems that need to migrate together, and identify whether a running system is still serving users, or is a candidate for decommissioning instead of migration.

If you've already [set up dependency mapping](#), and want to refine an existing group, do the following:

1. In the Servers tab, in **Azure Migrate: Server Assessment** tile, click **Groups**.

2. Click the group you want to refine.

- If you haven't yet set up dependency mapping, the **Dependencies** column will show a **Requires installation** status. For each VM for which you want to visualize dependencies, click **Requires installation**. Install a couple of agents on each VM, before you can map the machine dependencies. [Learn more](#).

NAME	MEMBER OF	DEPENDENCIES	CORES
NestedScaleVM7303	groupa	Requires installation	1
NestedScaleHost-44788-10	groupa	Requires installation	1
NestedScaleHost-44800-95	groupa	Requires installation	1

- If you've already set up dependency mapping, on the group page, click **View dependencies** to open the group dependency map.

3. After clicking **View dependencies**, the group dependency map shows the following:

- Inbound (clients) and outbound (servers) TCP connections to and from all machines in the group that have the dependency agents installed.
- Dependent machines that don't have the dependency agents installed are grouped by port numbers.
- Dependent machines with dependency agents installed are shown as separate boxes.
- Processes running inside the machine. Expand each machine box to view the processes.
- Machine properties (including FQDN, operating system, MAC address). Click on each machine box to view the details.

4. To view dependencies in a time interval of your choice, modify the time range (an hour by default) by specifying start and end dates, or the duration.

NOTE

Time range can be up to an hour. If you need a longer range, use [Azure Monitor to query dependent data](#) for a longer period.

5. After you've identified the dependencies you would like to add to or remove from the group, you can modify the group. Use Ctrl+Click to add or remove machines from the group.

- You can only add machines that have been discovered.
- Adding and removing machines invalidates past assessments for a group.
- You can optionally create a new assessment when you modify the group.

Next steps

Learn how to set up and use [dependency mapping](#) to create high confidence groups.

Set up dependency visualization

3/17/2020 • 7 minutes to read • [Edit Online](#)

This article describes how to set up agent-based dependency analysis in Azure Migrate:Server Assessment.

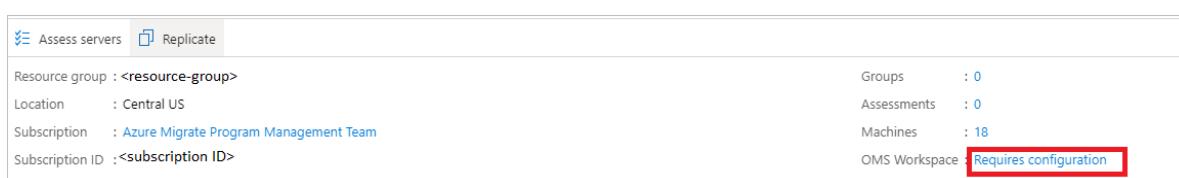
[Dependency analysis](#) helps you to identify and understand dependencies across machines you want to assess and migrate to Azure.

Before you start

- [Learn about](#) agent-based dependency analysis.
- Review the prerequisites and support requirements for setting up agent-based dependency visualization for [VMware VMs](#), [physical servers](#), and [Hyper-V VMs](#).
- Make sure you've [created](#) an Azure Migrate project.
- If you've already created a project, make sure you've [added](#) the Azure Migrate:Server Assessment tool.
- Make sure you've set up an [Azure Migrate appliance](#) to discover your on-premises machines. Learn how to set up an appliance for [VMware](#), [Hyper-V](#), or [physical servers](#). The appliance discovers on-premises machines, and sends metadata, performance data to Azure Migrate:Server Assessment.
- To use dependency visualization, you associate a [Log Analytics workspace](#) with an Azure Migrate project:
 - You can attach a workspace only after setting up the Azure Migrate appliance, and discovering machines in the Azure Migrate project.
 - Make sure you have a workspace in the subscription that contains the Azure Migrate project.
 - The workspace must reside in the East US, Southeast Asia, or West Europe regions. Workspaces in other regions can't be associated with a project.
 - The workspace must be in a region in which [Service Map is supported](#).
 - You can associate a new or existing Log Analytics workspace with an Azure Migrate project.
 - You attach the workspace the first time that you set up dependency visualization for a machine. The workspace for an Azure Migrate project can't be modified after it's added.
 - In Log Analytics, the workspace associated with Azure Migrate is tagged with the Migration Project key, and the project name.

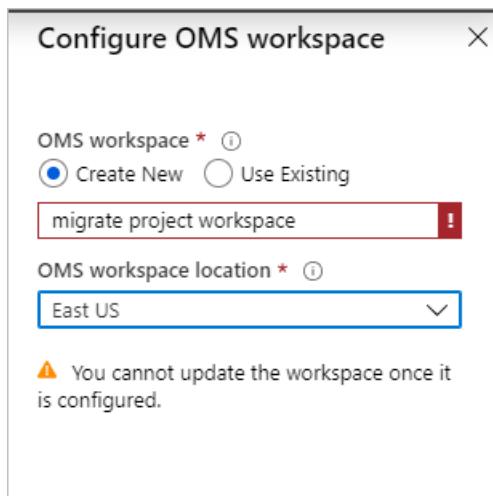
Associate a workspace

1. After you've discovered machines for assessment, in **Servers > Azure Migrate: Server Assessment**, click **Overview**.
2. In **Azure Migrate: Server Assessment**, click **Essentials**.
3. In **OMS Workspace**, click **Requires configuration**.



4. In **Configure OMS workspace**, specify whether you want to create a new workspace, or use an existing one.
 - You can select an existing workspace from all the workspaces in the migrate project subscription.
 - You need Reader access to the workspace to associate it.

5. If you create a new workspace, select a location for it.



Download and install the VM agents

On each machine you want to analyze, install the agents.

NOTE

For machines monitored by System Center Operations Manager 2012 R2 or later, you don't need to install the MMA agent. Service Map integrates with Operations Manager. [Follow](#) integration guidance.

1. In **Azure Migrate: Server Assessment**, click **Discovered servers**.
2. For each machine you want to analyze with dependency visualization, in the **Dependencies** column, click **Requires agent installation**.
3. In the **Dependencies** page, download the MMA and Dependency agent for Windows or Linux.
4. Under **Configure MMA agent**, copy the workspace ID and key. You need these when you install the MMA agent.

Dependencies
migratoproject6880project

Dependency visualization of machines requires a deeper discovery which involves installation and configuration of the below agents on the on-premises machines. [Learn more](#)

Configured OMS workspace: [migrate-contosodemo-180413100901](#)

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:
 [Copy](#)

Workspace key:
 [Copy](#)

Once the installation of the agents is done, it may take up to 15 minutes to reflect in the Azure Migrate portal.

Install the MMA

Install the MMA on each Windows or Linux machine you want to analyze.

Install MMA on a Windows machine

To install the agent on a Windows machine:

1. Double-click the downloaded agent.
2. On the **Welcome** page, click **Next**. On the **License Terms** page, click **I Agree** to accept the license.
3. In **Destination Folder**, keep or modify the default installation folder > **Next**.
4. In **Agent Setup Options**, select **Azure Log Analytics** > **Next**.
5. Click **Add** to add a new Log Analytics workspace. Paste in the workspace ID and key that you copied from the portal. Click **Next**.

You can install the agent from the command line or using an automated method such as Configuration Manager or [Intigua](#).

- [Learn more](#) about using these methods to install the MMA agent.
- The MMA agent can also be installed using this [script](#).
- [Learn more](#) about the Windows operating systems supported by MMA.

Install MMA on a Linux machine

To install the MMA on a Linux machine:

1. Transfer the appropriate bundle (x86 or x64) to your Linux computer using scp/sftp.
2. Install the bundle by using the --install argument.

```
sudo sh ./omsagent-<version>.universal.x64.sh --install -w <workspace id> -s <workspace key>
```

[Learn more](#) about the list of Linux operating systems support by MMA.

Install the Dependency agent

1. To install the Dependency agent on a Windows machine, double-click the setup file and follow the wizard.
2. To install the Dependency agent on a Linux machine, install as root using the following command:

```
sh InstallDependencyAgent-Linux64.bin
```

- [Learn more](#) about how you can use scripts to install the Dependency agent.
- [Learn more](#) about the operating systems supported by the Dependency agent.

Create a group using dependency visualization

Now create a group for assessment.

NOTE

Groups for which you want to visualize dependencies shouldn't contain more than 10 machines. If you have more than 10 machines, split them into smaller groups.

1. In **Azure Migrate: Server Assessment**, click **Discovered servers**.
2. In the **Dependencies** column, click **View dependencies** for each machine you want to review.
3. On the dependency map, you can see the following:

- Inbound (clients) and outbound (servers) TCP connections, to and from the machine.
 - Dependent machines that don't have the dependency agents installed are grouped by port numbers.
 - Dependent machines with dependency agents installed are shown as separate boxes.
 - Processes running inside the machine. Expand each machine box to view the processes.
 - Machine properties (including FQDN, operating system, MAC address). Click on each machine box to view the details.
4. You can look at dependencies for different time durations by clicking on the time duration in the time range label.
 - By default the range is an hour.
 - You can modify the time range, or specify start and end dates, and duration.
 - Time range can be up to an hour. If you need a longer range, use Azure Monitor to query dependent data for a longer period.
 5. After you've identified the dependent machines that you want to group together, use Ctrl+Click to select multiple machines on the map, and click **Group machines**.
 6. Specify a group name.
 7. Verify that the dependent machines are discovered by Azure Migrate.
 - If a dependent machine isn't discovered by Azure Migrate: Server Assessment, you can't add it to the group.
 - To add a machine, run discovery again, and verify that the machine is discovered.
 8. If you want to create an assessment for this group, select the checkbox to create a new assessment for the group.
 9. Click **OK** to save the group.

After creating the group, we recommend that you install agents on all the machines in the group, and then visualize dependencies for the entire group.

Query dependency data in Azure Monitor

You can query dependency data captured by Service Map in the Log Analytics workspace associated with the Azure Migrate project. Log Analytics is used to write and run Azure Monitor log queries.

- [Learn how to search for Service Map data in Log Analytics](#).
- [Get an overview of writing log queries in Log Analytics](#).

Run a query for dependency data as follows:

1. After you install the agents, go to the portal and click **Overview**.
2. In **Azure Migrate: Server Assessment**, click **Overview**. Click the down arrow to expand **Essentials**.
3. In **OMS Workspace**, click the workspace name.
4. On the Log Analytics workspace page > **General**, click **Logs**.
5. Write your query, and click **Run**.

Sample queries

Here are a few sample queries that you can use to extract dependency data.

- You can modify the queries to extract your preferred data points.
- [Review a complete list of dependency data records](#).
- [Review additional sample queries](#).

Sample: Review inbound connections

Review inbound connections for a set of VMs.

- The records in the table for connection metrics (VMConnection) don't represent individual physical network connections.
- Multiple physical network connections are grouped into a logical connection.
- [Learn more](#) about how physical network connection data is aggregated in VMConnection.

```
// the machines of interest
let ips=materialize(ServiceMapComputer_CL
| summarize ips=makeset(todynamic(Ipv4Addresses_s)) by MonitoredMachine=ResourceName_s
| mvexpand ips to typeof(string));
let StartDateTime = datetime(2019-03-25T00:00:00Z);
let EndDateTime = datetime(2019-03-30T01:00:00Z);
VMConnection
| where Direction == 'inbound'
| where TimeGenerated > StartDateTime and TimeGenerated < EndDateTime
| join kind=inner (ips) on $left.DestinationIp == $right.ips
| summarize sum(LinksEstablished) by Computer, Direction, SourceIp, DestinationIp, DestinationPort
```

Sample: Summarize sent and received data

This sample summarizes the volume of data sent and received on inbound connections between a set of machines.

```
// the machines of interest
let ips=materialize(ServiceMapComputer_CL
| summarize ips=makeset(todynamic(Ipv4Addresses_s)) by MonitoredMachine=ResourceName_s
| mvexpand ips to typeof(string));
let StartDateTime = datetime(2019-03-25T00:00:00Z);
let EndDateTime = datetime(2019-03-30T01:00:00Z);
VMConnection
| where Direction == 'inbound'
| where TimeGenerated > StartDateTime and TimeGenerated < EndDateTime
| join kind=inner (ips) on $left.DestinationIp == $right.ips
| summarize sum(BytesSent), sum(BytesReceived) by Computer, Direction, SourceIp, DestinationIp,
DestinationPort
```

Next steps

[Create an assessment](#) for a group.

This article describes how to set up agentless dependency analysis in Azure Migrate:Server Assessment. [Dependency analysis](#) helps you to identify and understand dependencies across machines you want to assess and migrate to Azure.

IMPORTANT

Agentless dependency visualization is currently in preview for VMware VMs only, discovered with the Azure Migrate:Server Assessment tool. Features might be limited or incomplete. This preview is covered by customer support and can be used for production workloads. For more information, see [Supplemental Terms of Use for Microsoft Azure Previews](#).

Before you start

- [Learn about](#) agentless dependency analysis.
- [Review](#) the prerequisites and support requirements for setting up agentless dependency visualization for VMware VMs
- Make sure you've [created](#) an Azure Migrate project.
- If you've already created a project, make sure you've [added](#) the Azure Migrate:Server Assessment tool.
- Make sure you've set up an [Azure Migrate appliance](#) to discover your on-premises machines. Learn how to set up an appliance for [VMware](#) VMs. The appliance discovers on-premises machines, and sends metadata and performance data to Azure Migrate:Server Assessment.

Current limitations

- Right now you can't add or remove a server from a group, in the dependency analysis view.
- A dependency map for a group of servers isn't currently available.
- Currently, the dependency data can't be downloaded in tabular format.

Create a user account for discovery

Set up a user account so that Server Assessment can access the VM for discovery. [Learn about account requirements](#).

Add the user account to the appliance

Add the user account to the appliance.

1. Open the appliance management app.
2. Navigate to the **Provide vCenter details** panel.
3. In **Discover application and dependencies on VMs**, click **Add credentials**
4. Choose the **Operating system**, provide a friendly name for the account, and the **User name/Password**
5. Click **Save**.
6. Click **Save and start discovery**.

Password
••••••••

Update Credential Successfully connected to vCenter Server

What metadata is discovered and what is it used for? [Learn more](#)

Discover applications and dependencies on VMs

Provide VM credentials for discovery of applications and for dependency analysis on the machines. [Learn more](#) about permissions.

The credentials will be saved on the appliance in an encrypted format. The discovery of applications and dependencies is done remotely without the installation of any agent or script on VMs.

Add credentials

Skip addition of VM credentials. You will not be able to discover applications and dependencies.
Added credentials

OS Type	Friendly Name	Action
Linux	linuxcreds	Edit
Windows	windowscreds	Edit

Start dependency discovery

Choose the machines on which you want to enable dependency discovery.

1. In Azure Migrate: Server Assessment, click **Discovered servers**.
2. Click the **Dependency analysis** icon.
3. Click **Add servers**.
4. In the **Add servers** page, choose the appliance that's discovering the relevant machines.
5. From the machine list, select the machines.
6. Click **Add servers**.

Home > Azure Migrate - Servers > Discovered servers

Discovered servers

ContosoMigration

Create group Create assessment Replicate Export application inventory Dependency analysis (Preview) Refresh

Agentless dependency analysis is now available in preview. Click here to request access.

Add servers Remove servers

Azure Migrate appliance Import based (Preview)

Appliance name VMware1 (VMware)

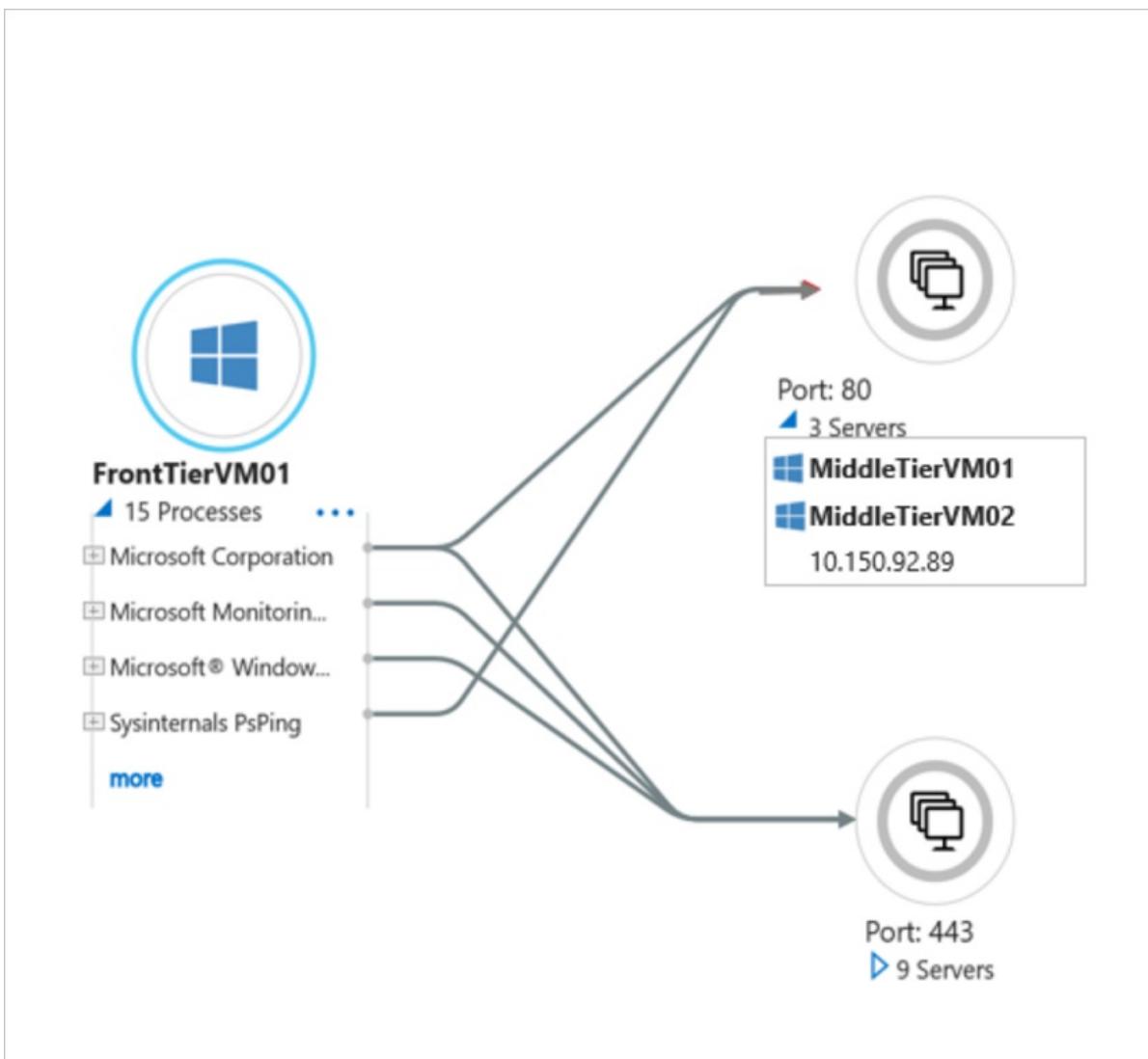
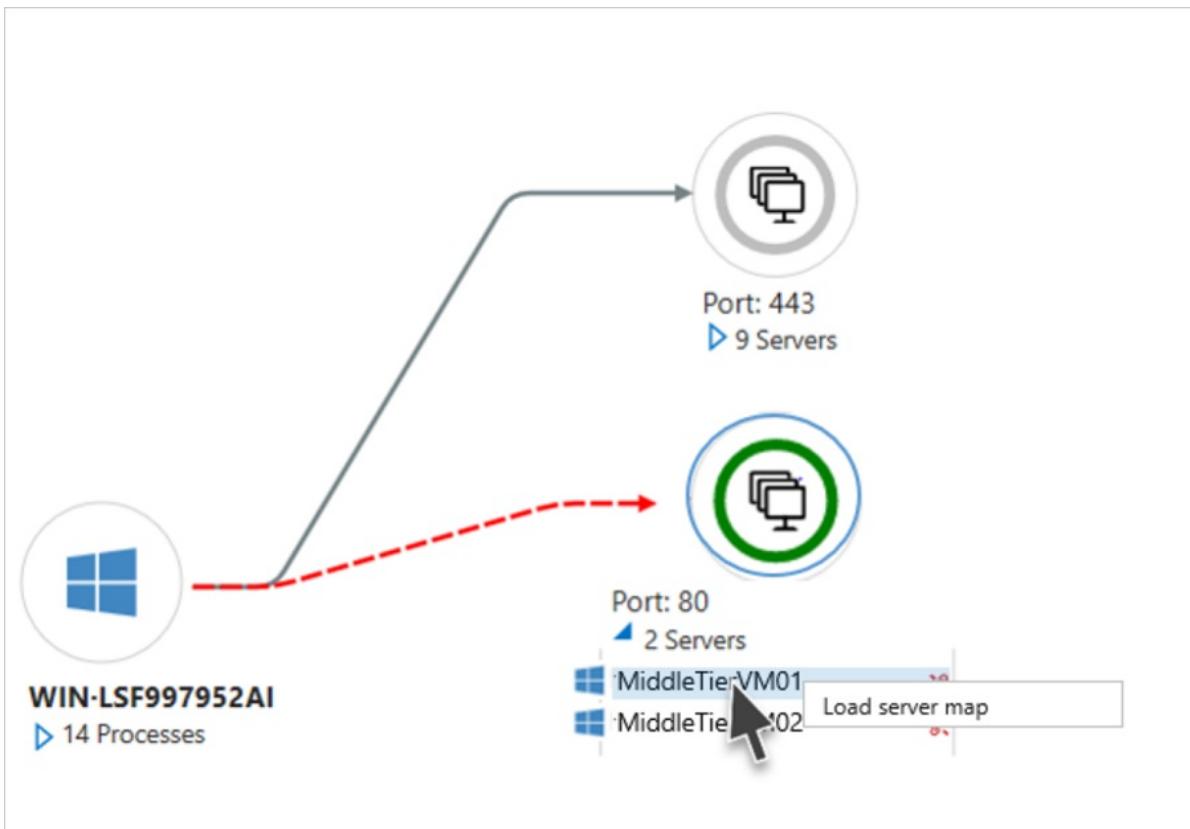
Search to filter rows

Name	IP address	Applications Discovered	Dependencies (Agentless)	Cores
V2A-Win2K16STD	-	⚠️ 11 Applications	Not enabled	4
GA Demo5	-	⚠️ 3 Applications	Not enabled	8
FW12DCCRM-01	-	⚠️ 13 Applications	Not enabled	2
FW12R2DCFS-45	-	⚠️ 13 Applications	Not enabled	2
PayrollWeb04	10.150.10.189,2404:f801:4...	1 Applications	View dependencies	4
Contoso-DataTier3	-	⚠️ Not available	Not enabled	8

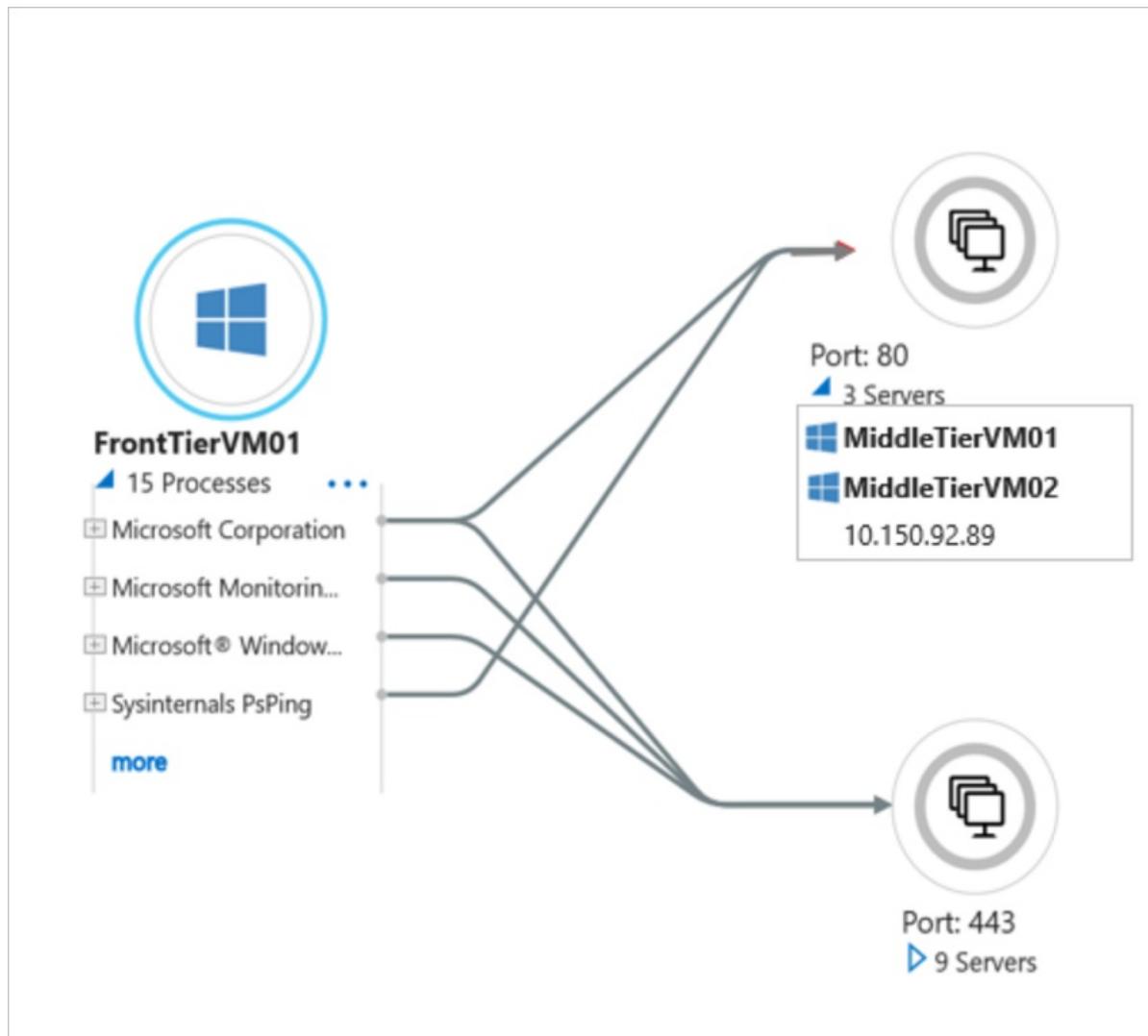
You can visualize dependencies around six hours after starting dependency discovery.

Visualize dependencies

1. In **Azure Migrate: Server Assessment**, click **Discovered servers**.
2. Search for the machine you want to view.
3. In the **Dependencies** column, click **View dependencies**
4. Change the time period for which you want to view the map using the **Time duration** dropdown.
5. Expand the **Client** group to list the machines with a dependency on the selected machine.
6. Expand the **Port** group to list the machines that have a dependency from the selected machine.
7. To navigate to the map view of any of the dependent machines, click on the machine name > **Load server map**



8. Expand the selected machine to view process-level details for each dependency.



NOTE

Process information for a dependency is not always available. If it's not available, the dependency is depicted with the process marked as "Unknown process".

Stop dependency discovery

Choose the machines on which you want to stop dependency discovery.

1. In Azure Migrate: Server Assessment, click **Discovered servers**.
2. Click the **Dependency analysis** icon.
3. Click **Remove servers**.
4. In the **Remove servers** page, choose the appliance that is discovering the VMs on which you look to stop dependency discovery.
5. From the machine list, select the machines.
6. Click **Remove servers**.

Next steps

[Group the machines](#) for assessment.

minutes to read • [Edit Online](#)

This article describes how to create an assessment for on-premises VMware VMs or Hyper-V VMs with Azure Migrate: Server Assessment.

Azure Migrate helps you to migrate to Azure. Azure Migrate provides a centralized hub to track discovery, assessment, and migration of on-premises infrastructure, applications, and data to Azure. The hub provides Azure tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

Before you start

- Make sure you've [created](#) an Azure Migrate project.
- If you've already created a project, make sure you've [added](#) the Azure Migrate: Server Assessment tool.
- To create an assessment, you need to set up an Azure Migrate appliance for [VMware](#) or [Hyper-V](#). The appliance discovers on-premises machines, and sends metadata and performance data to Azure Migrate: Server Assessment. [Learn more](#).

Assessment overview

There are two types of assessments you can create using Azure Migrate: Server Assessment.

ASSESSMENT	DETAILS	DATA
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.
As on-premises	Assessments based on on-premises sizing.	Recommended VM size: Based on the on-premises VM size Recommended disk type: Based on the storage type setting you select for the assessment.

[Learn more](#) about assessments.

Run an assessment

Run an assessment as follows:

1. Review the [best practices](#) for creating assessments.
2. In the Servers tab, in **Azure Migrate: Server Assessment** tile, click **Assess**.

Azure Migrate - Servers

Microsoft

Search (Ctrl+ /) «

Refresh

Last refreshed details for migrate project <project name> <time>

Overview

Migration goals

Servers

Databases

Data Box

Manage

Discovered items

Support + troubleshooting

New support request

Assessment tools

Azure Migrate: Server Assessment

Discover Assess Overview

	Discovered servers	5271
	Groups	3
	Assessments	3
	Notifications	2 critical

Next step: You can refine your application grouping with dependency analysis

Add more assessment tools? [Click here.](#)

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with links like Overview, Migration goals, and Manage. The main area is titled 'Assessment tools' and contains a section for 'Azure Migrate: Server Assessment'. It has tabs for Discover, Assess (which is highlighted with a red box), and Overview. Below the tabs is a table with four rows: Discovered servers (5271), Groups (3), Assessments (3), and Notifications (2 critical). At the bottom, there's a note about refining application grouping with dependency analysis and a link to add more tools.

3. In **Assess servers**, specify a name for the assessment.
4. Click **View all** to review the assessment properties.

Assessment properties



You can also edit these properties later by opening the **assessment** and clicking on '**Edit properties**' command on top

TARGET PROPERTIES

Target location i

North Europe v

Storage type i

Automatic v

Reserved instances i

3 years reserved v

VM SIZE

Sizing criterion i

Performance-based v

Performance history i

1 Day v

Percentile utilization i

95th v

Save

Discard

5. In **Select or create a group**, select **Create New**, and specify a group name. A group gathers one or more VMs together for assessment.
6. In **Add machines to the group**, select VMs to add to the group.
7. Click **Create Assessment** to create the group, and run the assessment.

Assess servers

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

* Assessment name

Enter the assessment...

Assessment properties

(Showing 3 of 13)

[View all](#)

Migration target location : North Europe

Sizing criterion : Performance-based

Reserved instances : 3 years reserved

Select or create a group

Create New Use Existing

Enter the group name

Add machines to the group

 [How to create groups using dependency visualization](#)

[Select all](#) [Clear selection](#)

Search to filter machines

< Previous

Page 1 of 586

[Next >](#)

NAME	IP ADDRESS	OPERATING SYSTEM
51H8TestVM-17		

[Create assessment](#)

8. After the assessment is created, view it in **Servers > Azure Migrate: Server Assessment > Assessments**.

9. Click **Export assessment**, to download it as an Excel file.

Review an assessment

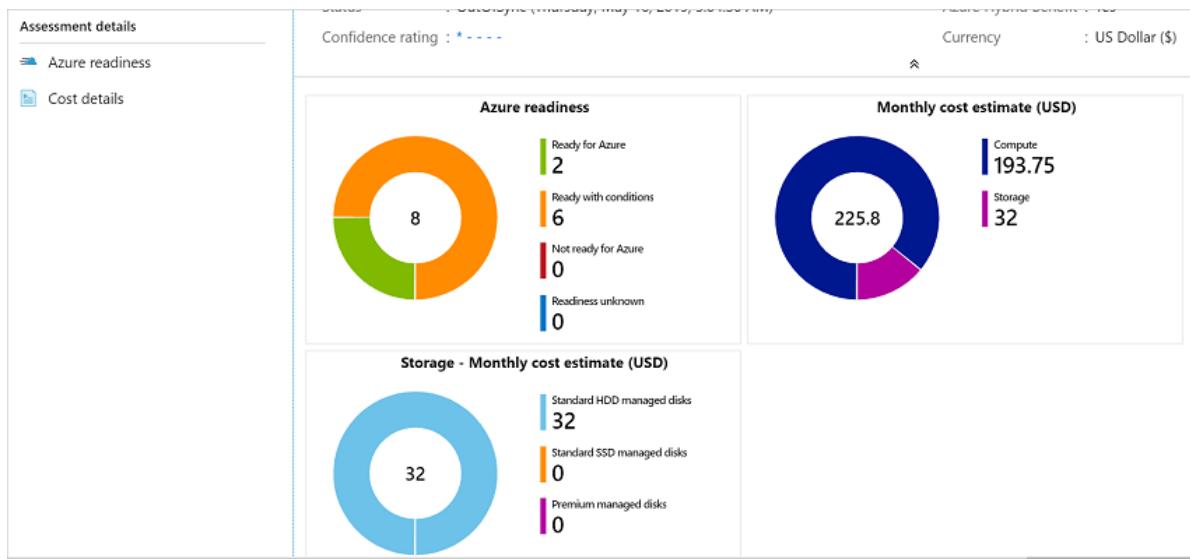
An assessment describes:

- **Azure readiness:** Whether VMs are suitable for migration to Azure.
- **Monthly cost estimation:** The estimated monthly compute and storage costs for running the VMs in Azure.
- **Monthly storage cost estimation:** Estimated costs for disk storage after migration.

View an assessment

1. In **Migration goals > Servers**, click **Assessments** in **Azure Migrate: Server Assessment**.

2. In **Assessments**, click on an assessment to open it.



Review Azure readiness

1. In **Azure readiness**, verify whether VMs are ready for migration to Azure.
2. Review the VM status:
 - **Ready for Azure**: Azure Migrate recommends a VM size and cost estimates for VMs in the assessment.
 - **Ready with conditions**: Shows issues and suggested remediation.
 - **Not ready for Azure**: Shows issues and suggested remediation.
 - **Readiness unknown**: Used when Azure Migrate can't assess readiness, due to data availability issues.
3. Click on an **Azure readiness** status. You can view VM readiness details, and drill down to see VM details, including compute, storage, and network settings.

Review cost details

This view shows the estimated compute and storage cost of running VMs in Azure.

1. Review the monthly compute and storage costs. Costs are aggregated for all VMs in the assessed group.
 - Cost estimates are based on the size recommendations for a machine, and its disks and properties.
 - Estimated monthly costs for compute and storage are shown.
 - The cost estimation is for running the on-premises VMs as IaaS VMs. Azure Migrate Server Assessment doesn't consider PaaS or SaaS costs.
2. You can review monthly storage cost estimates. This view shows aggregated storage costs for the assessed group, split over different types of storage disks.
3. You can drill down to see details for specific VMs.

Review confidence rating

When you run performance-based assessments, a confidence rating is assigned to the assessment.

Assess servers		Columns						
Name	Group	Status	Machines	Location	Sizing Criterion	Confidence Rating		
assessment_5_16_2019_17_34_29	day2	OutOfSync	0	North Europe	Performance-based	★★★★★		
assessment_5_20_2019_17_42_6	Mygroup	Ready	6	North Europe	Performance-based	★★★★★		
assessment_5_22_2019_22_56_13	Day2-group	OutDated	14	North Europe	Performance-based	★★★★★		

- A rating from 1-star (lowest) to 5-star (highest) is awarded.
- The confidence rating helps you estimate the reliability of the size recommendations provided by the assessment.
- The confidence rating is based on the availability of data points needed to compute the assessment.

Confidence ratings for an assessment are as follows.

DATA POINT AVAILABILITY	CONFIDENCE RATING
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

Next steps

- Learn how to use [dependency mapping](#) to create high confidence groups.
- [Learn more](#) about how assessments are calculated.

minutes to read • [Edit Online](#)

This article describes how to customize assessments created by Azure Migrate Server Assessment.

Azure Migrate provides a central hub to track discovery, assessment, and migration of your on-premises apps and workloads, and private/public cloud VMs, to Azure. The hub provides Azure Migrate tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings.

You can use the Azure Migrate Server Assessment tool to create assessments for on-premises VMware VMs and Hyper-V VMs, in preparation for migration to Azure.

About assessments

There are two types of assessments you can run using Azure Migrate Server Assessment.

ASSESSMENT	DETAILS	DATA
Performance-based	Assessments based on collected performance data	Recommended VM size: Based on CPU and memory utilization data. Recommended disk type (standard or premium managed disk): Based on the IOPS and throughput of the on-premises disks.
As on-premises	Assessments based on on-premises sizing.	Recommended VM size: Based on the on-premises VM size Recommended disk type: Based on the storage type setting you select for the assessment.

How is an assessment done?

An assessment done in Azure Migrate Server Assessment has three stages. Assessment starts with a suitability analysis, followed by sizing, and lastly, a monthly cost estimation. A machine only moves along to a later stage if it passes the previous one. For example, if a machine fails the Azure suitability check, it's marked as unsuitable for Azure, and sizing and costing won't be done. [Learn more](#).

What's in an assessment?

PROPERTY	DETAILS

PROPERTY	DETAILS
Target location	<p>The Azure location to which you want to migrate. Server Assessment currently supports these target regions: Australia East, Australia Southeast, Brazil South, Canada Central, Canada East, Central India, Central US, China East, China North, East Asia, East US, East US2, Germany Central, Germany Northeast, Japan East, Japan West, Korea Central, Korea South, North Central US, North Europe, South Central US, Southeast Asia, South India, UK South, UK West, US Gov Arizona, US Gov Texas, US Gov Virginia, West Central US, West Europe, West India, West US, and West US2.</p>
Storage type	<p>You can use this property to specify the type of disks you want to move to, in Azure.</p> <p>For as-on premises sizing, you can specify the target storage type either as Premium-managed disks, Standard SSD-managed disks or Standard HDD-managed disks. For performance-based sizing, you can specify the target disk type either as Automatic, Premium-managed disks, Standard HDD-managed disks, or Standard SSD-managed disks.</p> <p>When you specify the storage type as automatic, the disk recommendation is done based on the performance data of the disks (IOPS and throughput). If you specify the storage type as premium/standard, the assessment will recommend a disk SKU within the storage type selected. If you want to achieve a single instance VM SLA of 99.9%, you may want to specify the storage type as Premium-managed disks. This ensures that all disks in the assessment are recommended as Premium-managed disks. Azure</p>
Reserved Instances (RI)	<p>This property helps you specify if you have Reserved Instances in Azure, cost estimations in the assessment are then done taking into RI discounts. Reserved instances are currently only supported for Pay-As-You-Go offer in Azure Migrate.</p>
Sizing criterion	<p>The criterion to be used to right-size VMs for Azure. You can either do <i>performance-based</i> sizing or size the VMs <i>as on-premises</i>, without considering the performance history.</p>
Performance history	<p>The duration to consider for evaluating the performance data of machines. This property is only applicable when sizing criterion is <i>performance-based</i>.</p>
Percentile utilization	<p>The percentile value of the performance sample set to be considered for right-sizing. This property is only applicable when sizing is <i>performance-based</i>.</p>
VM series	<p>You can specify the VM series that you would like to consider for right-sizing. For example, if you have a production environment that you do not plan to migrate to A-series VMs in Azure, you can exclude A-series from the list or series and the right-sizing is done only in the selected series.</p>

PROPERTY	DETAILS
Comfort factor	Azure Migrate Server Assessment considers a buffer (comfort factor) during assessment. This buffer is applied on top of machine utilization data for VMs (CPU, memory, disk, and network). The comfort factor accounts for issues such as seasonal usage, short performance history, and likely increases in future usage. For example, a 10-core VM with 20% utilization normally results in a 2-core VM. However, with a comfort factor of 2.0x, the result is a 4-core VM instead.
Offer	The Azure offer you're enrolled to. Azure Migrate estimates the cost accordingly.
Currency	Billing currency.
Discount (%)	Any subscription-specific discount you receive on top of the Azure offer. The default setting is 0%.
VM uptime	If your VMs are not going to be running 24x7 in Azure, you can specify the duration (number of days per month and number of hours per day) for which they would be running and the cost estimations would be done accordingly. The default value is 31 days per month and 24 hours per day.
Azure Hybrid Benefit	Specify whether you have software assurance and are eligible for Azure Hybrid Benefit . If set to Yes, non-Windows Azure prices are considered for Windows VMs. Default is Yes.

Edit assessment properties

To edit assessment properties after creating an assessment, do the following:

1. In the Azure Migrate project, click **Servers**.
2. In **Azure Migrate: Server Assessment**, click the assessments count.
3. In **Assessment**, click the relevant assessment > **Edit properties**.
4. Customize the assessment properties in accordance with the table above.
5. Click **Save** to update the assessment.

You can also edit assessment properties when you're creating an assessment.

Next steps

[Learn more](#) about how assessments are calculated.

minutes to read • [Edit Online](#)

This article describes how to add migration tools in [Azure Migrate](#).

Azure Migrate provides a hub of tools for assessment and migration to Azure. It includes native tools, tools provided by other Azure services, and third-party independent software vendor (ISV) offerings.

If you want to add a migration tool and haven't yet set up an Azure Migrate project, follow this [article](#).

Selecting an ISV tool

If you choose an [ISV tool](#) for migration, you can start by obtaining a license, or signing up for a free trial, in accordance with the ISV policy. In each tool, there's an option to connect to Azure Migrate. Deploy the tool, and follow the tool instructions and documentation to connect the tool workspace with Azure Migrate.

Select a migration scenario

1. In the Azure Migrate project, click **Overview**.
2. Select the migration scenario you want to use:
 - To migrate machines and workloads to Azure, select **Assess and migrate servers**.
 - To migrate on-premises SQL machines, select **Assess and migrate databases**.
 - To migrate on-premises web apps, select **Assess and migrate web apps**.
 - To migrate large amounts of on-premises data to Azure in offline mode, select **Order a Data Box**.

Migrate your on-premises datacenter to Azure

Discover, assess and migrate your on-premises applications using Microsoft or third-party tools, or [find an expert](#) to help with your migration. [Learn more](#)



Discover, assess and migrate servers

Discover, assess and migrate your on-premises VMware and Hyper-V virtual machines or Physical servers to Azure.

[Assess and migrate servers](#)



Assess and migrate databases

Assess and migrate your on-premises databases to Azure SQL Database Managed Instance or Azure SQL Database.

[Assess and migrate databases](#)



Assess and migrate web apps to Azure

Assess and migrate .NET and PHP web apps to Azure's Platform-as-a-Service, Azure App Service.

[Assess and migrate web apps](#)



Migrate on-premises data to Azure

Use the Data Box offline family of products to move large amount of data to Azure.

[Order a Data Box](#)

Select a server migration tool

1. Click **Assess and Migrate Servers**.
2. In **Azure Migrate - Servers**, if you haven't added migration tools yet, under **Migration tools**, select **Click here to add a migration tool**. If you've already added migration tools, in **Add more migration tools**, select **Change**.

NOTE

If you need to navigate to a different project, in **Azure Migrate - Servers**, next to **See details for a different migrate project**, click **Click here**.

3. In **Azure Migrate**, select the migration tool you want to use.

- If you use Azure Migrate Server Migration, you can set up and run migrations directly in the Azure Migrate project.
- If you use a third-party assessment tool, navigate to the link provided for the ISV, and run the migration in accordance with the instructions they provide.

Select a database migration tool

1. Click **Assess and migrate databases**
2. In **Databases**, click **Add tools**.
3. In Add a tool > **Select migration tool**, select the tool you want to use to migrate your database.

Select a web app migration tool

1. Click **Assess and migrate web apps**.
2. Follow the link to the Migration tool for the Azure App Service. Use the migration tool to:
 - **Assess apps online**: You can assess and migrate apps with a public URL online, using the Azure App Service Migration Assistant.
 - **.NET/PHP**: For internal .NET and PHP apps, you can download and run the Migration Assistant.

Order an Azure Data Box

To migrate large amounts of data to Azure, you can order an Azure Data Box for offline data transfer.

1. Click **Order a Data Box**.
2. In **Select your Azure Data Box**, specify your subscription.
3. The transfer will be an import to Azure. Specify the data source, and the Azure region destination for the data.

Next steps

Try out a migration using Azure Migrate Server Migration for [Hyper-V](#) or [VMware](#) VMs.

Migrate VMware VMs to Azure VMs enabled with server-side encryption and customer-managed keys

3/12/2020 • 8 minutes to read • [Edit Online](#)

This article describes how to migrate VMware VMs to Azure virtual machines with disks encrypted using server-side encryption(SSE) with customer-managed keys(CMK), using Azure Migrate Server Migration (agentless replication).

The Azure Migrate Server Migration portal experience lets you [migrate VMware VMs to Azure with agentless replication](#). The portal experience currently doesn't offer the ability to turn on SSE with CMK for your replicated disks in Azure. The ability to turn on SSE with CMK for the replicated disks is currently available only through REST API. In this article, you'll see how to create and deploy an [Azure Resource Manager template](#) to replicate a VMware VM and configure the replicated disks in Azure to use SSE with CMK.

The examples in this article use [Azure PowerShell](#) to perform the tasks needed to create and deploy the Resource Manager template.

[Learn more](#) about server-side encryption (SSE) with customer managed keys(CMK) for managed disks.

Prerequisites

- [Review the tutorial](#) on migration of VMware VMs to Azure with agentless replication to understand tool requirements.
- [Follow these instructions](#) to create an Azure Migrate project and add the **Azure Migrate: Server Migration** tool to the project.
- [Follow these instructions](#) to set up the Azure Migrate appliance for VMware in your on-premises environment and complete discovery.

Prepare for replication

Once VM discovery is complete, the Discovered Servers line on the Server Migration tile will show a count of VMware VMs discovered by the appliance.

Before you can start replicating VMs, the replication infrastructure needs to be prepared.

1. Create a Service Bus instance in the target region. The Service Bus is used by the on-premises Azure Migrate appliance to communicate with the Server Migration service to coordinate replication and migration.
2. Create a storage account for transfer of operation logs from replication.
3. Create a storage account that the Azure Migrate appliance uploads replication data to.
4. Create a Key Vault and configure the Key Vault to manage shared access signature tokens for blob access on the storage accounts created in step 3 and 4.
5. Generate a shared access signature token for the service bus created in step 1 and create a secret for the token in the Key Vault created in the previous step.
6. Create a Key Vault access policy to give the on-premises Azure Migrate appliance (using the appliance AAD app) and the Server Migration Service access to the Key Vault.
7. Create a replication policy and configure the Server Migration service with details of the replication infrastructure created in the previous step.

The replication infrastructure must be created in the target Azure region for the migration and in the target Azure subscription that the VMs are being migrated to.

The Server Migration portal experience simplifies preparation of the replication infrastructure by automatically doing this for you when you replicate a VM for the first time in a project. In this article, we'll assume that you've already replicated one or more VMs using the portal experience and that the replication infrastructure is already created. We'll look at how to discover details of the existing replication infrastructure and how to use these details as inputs to the Resource Manager template that will be used to set up replication with CMK.

Identifying replication infrastructure components

1. On the Azure portal, go the resource groups page and select the resource group in which the Azure Migrate project was created.
2. Select **Deployments** from the left menu and search for a deployment name beginning with the string "*Microsoft.MigrateV2.VMwareV2EnableMigrate*". You'll see a list of Resource Manager templates created by the portal experience to set up replication for VMs in this project. We'll download one such template and use that as the base to prepare the template for replication with CMK.
3. To download the template, select any deployment matching the string pattern in the previous step > select **Template** from the left menu > Click **Download** from the top menu. Save the template.json file locally. You'll edit this template file in the last step.

Create a Disk Encryption Set

A disk encryption set object maps Managed Disks to a Key Vault that contains the CMK to use for SSE. To replicate VMs with CMK, you'll create a disk encryption set and pass it as an input to the replication operation.

Follow the example [here](#) to create a disk encryption set using Azure PowerShell. Ensure that the disk encryption set is created in the target subscription that VMs are being migrated to, and in the target Azure region for the migration.

```
$Location = "southcentralus"                                #Target Azure region for migration
$TargetResourceGroupName = "ContosoMigrationTarget"
$keyVaultName = "ContosoCMKKV"
$keyName = "ContosoCMKKey"
$keyDestination = "Software"
$diskEncryptionSetName = "ContosoCMKDES"

$keyVault = New-AzKeyVault -Name $keyVaultName -ResourceGroupName $TargetResourceGroupName -Location $Location
-EnableSoftDelete -EnablePurgeProtection

$key = Add-AzKeyVaultKey -VaultName $keyVaultName -Name $keyName -Destination $keyDestination

$desConfig = New-AzDiskEncryptionSetConfig -Location $Location -SourceVaultId $keyVault.ResourceId -KeyUrl
$key.Key.Kid -IdentityType SystemAssigned

$des = New-AzDiskEncryptionSet -Name $diskEncryptionSetName -ResourceGroupName $TargetResourceGroupName -
InputObject $desConfig

Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ObjectId $des.Identity.PrincipalId -PermissionsToKeys
wrapkey,unwrapkey,get

New-AzRoleAssignment -ResourceName $keyVaultName -ResourceGroupName $TargetResourceGroupName -ResourceType
"Microsoft.KeyVault/vaults" -ObjectId $des.Identity.PrincipalId -RoleDefinitionName "Reader"
```

Get details of the VMware VM to migrate

In this step, you'll use Azure PowerShell to get the details of the VM that needs to be migrated. These details will be used to construct the Resource Manager template for replication. Specifically, the two properties of interest are:

- The machine Resource ID for the discovered VMs.
- The list of disks for the VM and their disk identifiers.

```

$ProjectResourceGroup = "ContosoVMwareCMK"      #Resource group that the Azure Migrate Project is created in
$ProjectName = "ContosoVMwareCMK"                #Name of the Azure Migrate Project

$solution = Get-AzResource -ResourceGroupName $ProjectResourceGroup -ResourceType
Microsoft.Migrate/MigrateProjects/solutions -ExpandProperties -ResourceName $ProjectName | where Name -eq
"Servers-Discovery-ServerDis
covery"

# Displays one entry for each appliance in the project mapping the appliance to the VMware sites discovered
through the appliance.
$solution.Properties.details.extendedDetails.applianceNameToSiteIdMapV2 | ConvertFrom-Json | select
ApplianceName, SiteId

```

```

ApplianceName SiteId
----- -----
VMwareAppliance /subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliance8basite

```

Copy the value of the SiteId string corresponding to the Azure Migrate appliance that the VM is discovered through. In the example shown above, the SiteId is *"/subscriptions/509099b2-9d2c-4636-b43e-bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliance8basite"*

```

#Replace value with SiteId from the previous step
$SiteId = "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliance8basite"
$SiteName = Get-AzResource -ResourceId $SiteId -ExpandProperties | Select-Object -ExpandProperty Name
$DiscoveredMachines = Get-AzResource -ResourceGroupName $ProjectResourceGroup -ResourceType
Microsoft.OffAzure/VMwareSites/machines -ExpandProperties -ResourceName $SiteName

#Get machine details
PS /home/bharathram> $MachineName = "FPL-W19-09"      #Replace string with VMware VM name of the machine to
migrate
PS /home/bharathram> $machine = $DiscoveredMachines | where {$_._Properties.displayName -eq $MachineName}
PS /home/bharathram> $machine.count    #Validate that only 1 VM was found matching this name.

```

Copy the ResourceId, name and disk uuid values for the machine to be migrated.

```

PS > $machine.Name
10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_50098f99-f949-22ca-642b-724ec6595210
PS > $machine.ResourceId
/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliance8basite/ma
chines/10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_50098f99-f949-22ca-642b-724ec6595210

PS > $machine.Properties.disks | select uuid, label, name, maxSizeInBytes

          uuid           label       name   maxSizeInBytes
          ----           ----       ----   -----
6000C291-5106-2aac-7a74-4f33c3ddb78c Hard disk 1 scsi0:0    42949672960
6000C293-39a1-bd70-7b24-735f0eeb79c4 Hard disk 2 scsi0:1    53687091200
6000C29e-cbee-4d79-39c7-d00dd0208aa9 Hard disk 3 scsi0:2    53687091200

```

Create Resource Manager template for replication

- Open the Resource Manager template file that you downloaded in the **Identifying replication infrastructure**

components step in an editor of your choice.

- Remove all resource definitions from the template except for resources that are of type `"Microsoft.RecoveryServices/vaults replicationFabrics replicationProtectionContainers replicationMigrationItems"`
- If there are multiple resource definitions of the above type, remove all but one. Remove any `dependsOn` property definitions from the resource definition.
- At the end of this step, you should have a file that looks like the example below and has the same set of properties.

```
{  
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "type":  
                "Microsoft.RecoveryServices/vaults replicationFabrics replicationProtectionContainers replicationMigrationItems",  
            "apiVersion": "2018-01-10",  
            "name":  
                "ContosoMigration7371rsvault/VMware104e4replicationfabric/VMware104e4replicationcontainer/10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_500937f3-805e-9414-11b1-f22923456e08",  
            "properties": {  
                "policyId": "/Subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.RecoveryServices/vaults/ContosoMigration7371rs vault/replicationPolicies/migrateVMware104e4sitepolicy",  
                "providerSpecificDetails": {  
                    "instanceType": "VMwareCbt",  
                    "vmwareMachineId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.OffAzure/VMwareSites/VMware104e4site/machines/10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_500937f3-805e-9414-11b1-f22923456e08",  
                    "targetResourceGroupId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/PayrollRG",  
                    "targetNetworkId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/PayrollRG/providers/Microsoft.Network/virtualNetworks/PayrollNW",  
                    "targetSubnetName": "PayrollSubnet",  
                    "licenseType": "NoLicenseType",  
                    "disksToInclude": [  
                        {  
                            "diskId": "6000C295-dafe-a0eb-906e-d47cb5b05a1d",  
                            "isOSDisk": "true",  
                            "logStorageAccountId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.Storage/storageAccounts/migratelsa1432469187",  
                            "logStorageAccountSasSecretName": "migratelsa1432469187-cacheSas",  
                            "diskType": "Standard_LRS"  
                        }  
                    ],  
                    "dataMoverRunAsAccountId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.OffAzure/VMwareSites/VMware104e4site/runasaccounts/b090bef3-b733-5e34-bc8f-eb6f2701432a",  
                    "snapshotRunAsAccountId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.OffAzure/VMwareSites/VMware104e4site/runasaccounts/b090bef3-b733-5e34-bc8f-eb6f2701432a",  
                    "targetBootDiagnosticsStorageAccountId": "/subscriptions/6785ea1f-ac40-4244-a9ce-94b12fd832ca/resourceGroups/ContosoMigration/providers/Microsoft.Storage/storageAccounts/migratelsa1432469187",  
                    "targetVmName": "PayrollWeb04"  
                }  
            }  
        ]  
    }  
}
```

- Edit the `name` property in the resource definition. Replace the string that follows the last "/" in the name property with the value of `$machine.Name` (from the previous step).
- Change the value of the `properties.providerSpecificDetails.vmwareMachineId` property with value of

`$machine.ResourceId` from the previous step).

- Set the values for **targetResourceGroupId**, **targetNetworkId**, **targetSubnetName** to the target resource group ID, target virtual network resource ID, and target subnet name respectively.
- Set the value of **licenseType** to "WindowsServer" to apply Azure Hybrid Benefit for this VM. If this VM is not eligible for Azure Hybrid Benefit, set the value of **licenseType** to **NoLicenseType**.
- Change the value of the **targetVmName** property to the desired Azure virtual machine name for the migrated VM.
- Optionally add a property named **targetVmSize** below the **targetVmName** property. Set the value of the **targetVmSize** property to the desired Azure virtual machine size for the migrated VM.
- The **disksToInclude** property is a list of disk inputs for replication with each list item representing one on-premises disk. Create as many list items as the number of disks on the on-premises VM. Replace the **diskId** property in the list item to the uuid of the disks identified in the previous step. Set the **isOSDisk** value to "true" for the OS disk of the VM and "false" for all other disks. Leave the **logStorageAccountId** and the **logStorageAccountSasSecretName** properties unchanged. Set the **diskType** value to the Azure Managed Disk type (*Standard_LRS*, *Premium_LRS*, *StandardSSD_LRS*) to use for the disk. For the disks that need to be encrypted with CMK, add a property named **diskEncryptionSetId** and set the value to the resource ID of the disk encryption set created(`$des.Id`) in the *Create a Disk Encryption Set* step
- Save the edited template file. For the example above, the edited template file looks as follows:

```
{  
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",  
    "contentVersion": "1.0.0.0",  
    "resources": [  
        {  
            "type":  
                "Microsoft.RecoveryServices/vaults/replicationFabrics/replicationProtectionContainers/replicationMigrationItems",  
            "apiVersion": "2018-01-10",  
            "name":  
                "ContosoVMwareCMK00ddrsvault/VMwareAppliance8bare replicationfabric/VMwareAppliance8bare replicationcontainer/10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_50098f99-f949-22ca-642b-724ec6595210",  
            "properties": {  
                "policyId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.RecoveryServices/vaults/ContosoVMwareCMK00ddrs  
vault/replicationPolicies/migrateVMwareAppliance8basitepolicy",  
                "providerSpecificDetails": {  
                    "instanceType": "VMwareCbt",  
                    "vmwareMachineId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OfferAzure/VMwareSites/VMwareAppliance8basite/ma  
chines/10-150-8-52-b090bef3-b733-5e34-bc8f-eb6f2701432a_50098f99-f949-22ca-642b-724ec6595210",  
                    "targetResourceGroupId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/ContosoMigrationTarget",  
                    "targetNetworkId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/cmkRTTest/providers/Microsoft.Network/virtualNetworks/cmkvm1_vnet",  
                    "targetSubnetName": "cmkvm1_subnet",  
                    "licenseType": "NoLicenseType",  
                    "disksToInclude": [  
                        {  
                            "diskId": "6000C291-5106-2aac-7a74-4f33c3ddb78c",  
                            "isOSDisk": "true",  
                            "logStorageAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.Storage/storageAccounts/migratelsa1671875959",  
                            "logStorageAccountSasSecretName": "migratelsa1671875959-cacheSas",  
                            "diskEncryptionSetId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/CONTOSOMIGRATIONTARGET/providers/Microsoft.Compute/diskEncryptionSets/ContosoCMKDES  
",  
                            "diskType": "Standard_LRS"  
                        },  
                        {  
                            "diskId": "6000C293-39a1-bd70-7b24-735f0eeb79c4",  
                            "isOSDisk": "false",  
                            "logStorageAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/ContosoCMKDESDR/providers/Microsoft.Storage/storageAccounts/migratelsa1671875959",  
                            "logStorageAccountSasSecretName": "migratelsa1671875959-dataSas",  
                            "diskEncryptionSetId": "/subscriptions/509099b2-9d2c-4636-b43e-  
bd5cafb6be69/resourceGroups/CONTOSOMIGRATIONTARGET/providers/Microsoft.Compute/diskEncryptionSets/ContosoCMKDES  
",  
                            "diskType": "Standard_LRS"  
                        }  
                    ]  
                }  
            }  
        }  
    ]  
}
```

```

    "logStorageAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.Storage/storageAccounts/migratelsa1671875959",
        "logStorageAccountSasSecretName": "migratelsa1671875959-cacheSas",
        "diskEncryptionSetId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/CONTOSOMIGRATIONTARGET/providers/Microsoft.Compute/diskEncryptionSets/ContosoCMKDES
",
            "diskType": "Standard_LRS"
        },
        {
            "diskId": "6000C29e-cbee-4d79-39c7-d00dd0208aa9",
            "isOSDisk": "false",
            "logStorageAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.Storage/storageAccounts/migratelsa1671875959",
                "logStorageAccountSasSecretName": "migratelsa1671875959-cacheSas",
                "diskEncryptionSetId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/CONTOSOMIGRATIONTARGET/providers/Microsoft.Compute/diskEncryptionSets/ContosoCMKDES
",
                    "diskType": "Standard_LRS"
                }
            ],
            "dataMoverRunAsAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliancea8basite/ru
nasaccounts/b090bef3-b733-5e34-bc8f-eb6f2701432a",
                "snapshotRunAsAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.OffAzure/VMwareSites/VMwareAppliancea8basite/ru
nasaccounts/b090bef3-b733-5e34-bc8f-eb6f2701432a",
                    "targetBootDiagnosticsStorageAccountId": "/subscriptions/509099b2-9d2c-4636-b43e-
bd5cafb6be69/resourceGroups/ContosoVMwareCMK/providers/Microsoft.Storage/storageAccounts/migratelsa1671875959",
                        "performAutoResync": "true",
                        "targetVmName": "FPL-W19-09"
                    }
                }
            ]
        }
    }
}

```

Set up replication

You can now deploy the edited Resource Manager template to the project resource group to set up replication for the VM. Learn how to [deploy resource with Azure Resource Manager templates and Azure PowerShell](#)

```

New-AzResourceGroupDeployment -ResourceGroupName $ProjectResourceGroup -TemplateFile
"C:\Users\Administrator\Downloads\template.json"

```

```

DeploymentName      : template
ResourceGroupName   : ContosoVMwareCMK
ProvisioningState   : Succeeded
Timestamp          : 3/11/2020 8:52:00 PM
Mode               : Incremental
TemplateLink       :
Parameters         :
Outputs             :
DeploymentLogLevel :

```

Next steps

[Monitor replication](#) status through the portal experience and perform Test migrations and migration.

Prepare on-premises machines for migration to Azure

3/8/2020 • 6 minutes to read • [Edit Online](#)

This article describes how to prepare on-premises machines before you start migrating them to Azure by using [Azure Migrate: Server Migration](#).

In this article, you:

- Verify migration limitations.
- Check operating system requirements and support limitations.
- Review URL and port access for machines you want to migrate.
- Review changes you might need to make before you begin migration.
- Configure settings so drive letters are preserved after migration.
- Prepare machines so you can connect to the Azure VMs after migration.

Verify migration limitations

- You can assess up to 35,000 VMware VMs/Hyper-V VMs in a single Azure Migrate project by using Azure Migrate Server Migration. A project can combine VMware VMs and Hyper-V VMs, up to the limits for each.
- You can select up to 10 VMs at a time for migration. If you need to replicate more, replicate in groups of 10.
- For VMware agentless migration, you can run up to 100 replications simultaneously.

Verify operating system requirements

- Verify that your [Windows operating systems](#) are supported in Azure.
- Verify that your [Linux distributions](#) are supported in Azure.

See what's supported

For VMware VMs, Server Migration supports [agentless or agent-based migration](#).

- **VMware VMs:** Verify [migration requirements and support](#) for VMware VMs.
- **Hyper-V VMs:** Verify [migration requirements and support](#) for Hyper-V VMs.
- **Physical machines:** Verify [migration requirements and support](#) for on-premises physical machines and other virtualized servers.

Review URL and port access

Machines might need internet access during migration.

- **Azure Migrate appliance:** Review [URLs](#) and [ports](#) the Azure Migrate appliance needs to access during agentless migration.
- **VMware VM agent-based migration:** Review [URLs](#) and [ports](#) the replication appliance uses during VMware VM agent-based migration.
- **Hyper-V hosts:** Review [URLs and ports](#) the Hyper-V hosts need to access during migration.
- **Physical servers:** Review [URLs](#) and [ports](#) the replication appliance uses during physical server migration.

Verify required changes before migrating

Some VMs might require changes so they can run in Azure. Azure Migrate makes these changes automatically for VMs that are running these operating systems:

- Red Hat Enterprise Linux 7.0+, 6.5+
- CentOS 7.0+, 6.5+
- SUSE Linux Enterprise Server 12 SP1+
- Ubuntu 18.04LTS, 16.04LTS, 14.04LTS
- Debian 8, 7

For other operating systems, you must manually prepare machines before migration.

Prepare Windows machines

If you're migrating a Windows machine, make the following changes before migration. If you migrate the VM before you make the changes, the VM might not boot up in Azure.

1. [Enable Azure Serial Console](#) for the Azure VM. Enabling the console helps you troubleshoot. You don't need to reboot the VM. The Azure VM will boot by using the disk image. The disk image boot is equivalent to a reboot for the new VM.
2. If you're migrating machines that are running Windows Server 2003, install Hyper-V Guest Integration Services on the VM operating system. [Learn more](#).

Prepare Linux machines

1. Install Hyper-V Linux Integration Services. Most new versions of Linux distributions include Hyper-V Linux Integration Services by default.
2. Rebuild the Linux init image so it contains the necessary Hyper-V drivers. Rebuilding the init image ensures that the VM will boot in Azure (required only on some distributions).
3. [Enable Azure Serial Console logging](#). Enabling console logging helps you troubleshoot. You don't need to reboot the VM. The Azure VM will boot by using the disk image. The disk image boot is equivalent to a reboot for the new VM.
4. Update the device map file with the device name-to-volume associations, so you use persistent device identifiers.
5. Update entries in the fstab file to use persistent volume identifiers.
6. Remove any udev rules that reserve interface names based on MAC address, and so on.
7. Update network interfaces to receive an IP address from DHCP.

Learn more about the [steps to run a Linux VM on Azure](#), and get instructions for some of the popular Linux distributions.

Preserve drive letters after migration

When you migrate an on-premises machine to Microsoft Azure, the drive letters of additional data disks might change from their original values.

By default, Azure VMs are assigned drive D to use as temporary storage. This drive assignment causes all other attached storage drive assignments to increment by one letter. For example, if your on-premises installation uses a data disk that is assigned to drive D for application installations, the assignment for this drive increments to drive E after you migrate the VM to Azure. To prevent this automatic assignment, and to ensure that Azure assigns the next free drive letter to its temporary volume, set the storage area network (SAN) policy to **OnlineAll**:

1. On the on-premises machine (not the host server), open an elevated command prompt.
2. Enter **diskpart**.
3. Enter **SAN**. If the drive letter of the guest operating system isn't maintained, **Offline All** or **Offline Shared** is

- returned.
4. At the DISKPART prompt, enter SAN Policy=OnlineAll. This setting ensures that disks are brought online, and it ensures that you can read and write to both disks.
 5. During the test migration, you can verify that the drive letters are preserved.

Check Azure VM requirements

On-premises machines that you replicate to Azure must comply with Azure VM requirements for the operating system and architecture, the disks, network settings, and VM naming. Verify the requirements for [VMware VMs and physical servers](#), and [Hyper-V VMs](#) before migrating.

Prepare to connect after migration

Azure VMs are created during migration to Azure. After migration, you must be able to connect to the new Azure VMs. Multiple steps are required to connect successfully.

Prepare to connect to Azure Windows VMs

On on-premises Windows machines:

1. Configure Windows settings. Settings include removing any static persistent routes or WinHTTP proxy.
2. Make sure [required services](#) are running.
3. Enable remote desktop (RDP) to allow remote connections to the on-premises machine. Learn how to [use PowerShell to enable RDP](#).
4. To access an Azure VM over the internet after migration, in Windows Firewall on the on-premises machine, allow TCP and UDP in the Public profile, and set RDP as an allowed app for all profiles.
5. If you want to access an Azure VM over a site-to-site VPN after migration, in Windows Firewall on the on-premises machine, allow RDP for the Domain and Private profiles. Learn how to [allow RDP traffic](#).
6. Make sure there are no Windows updates pending on the on-premises VM when you migrate. If there are, updates might start installing on the Azure VM after migration, and you won't be able to sign into the VM until updates finish.

Prepare to connect with Linux Azure VMs

On on-premises Linux machines:

1. Check that the Secure Shell service is set to start automatically on system boot.
2. Check that firewall rules allow an SSH connection.

Configure Azure VMs after migration

After migration, complete these steps on the Azure VMs that are created:

1. To connect to the VM over the internet, assign a public IP address to the VM. You must use a different public IP address for the Azure VM than you used for your on-premises machine. [Learn more](#).
2. Check that network security group (NSG) rules on the VM allow incoming connections to the RDP or SSH port.
3. Check [boot diagnostics](#) to view the VM.

NOTE

The Azure Bastion service offers private RDP and SSH access to Azure VMs. [Learn more](#) about this service.

Next steps

Decide which method you want to use to [migrate VMware VMs](#) to Azure, or begin migrating [Hyper-V VMs](#) or [physical servers or virtualized or cloud VMs](#).

This article describes how to delete an [Azure Migrate](#) project.

Before you start

Before you delete a project:

- When you delete a project, the project, and discovered machine metadata are deleted.
- If you've attached a Log Analytics workspace to the Server Assessment tool for dependency analysis, decide whether you want to delete the workspace.
 - The workspace isn't automatically deleted. Delete it manually.
 - Verify what a workspace is used for before you delete it. The same Log Analytics workspace can be used for multiple scenarios.
 - Before you delete the project, you can find a link to the workspace in **Azure Migrate - Servers > Azure Migrate - Server Assessment**, under **OMS Workspace**.
 - To delete a workspace after deleting a project, find the workspace in the relevant resource group, and follow [these instructions](#).

Delete a project

1. In the Azure portal, open the resource group in which the project was created.
2. In the resource group page, select **Show hidden types**.
3. Select the project and the associated resources that you want to delete.
 - The resource type for Azure Migrate projects is **Microsoft.Migrate/migrateprojects**.
 - In the next section, review the resources created for discovery, assessment, and migration in an Azure Migrate project.
 - If the resource group only contains the Azure Migrate project, you can delete the entire resource group.
 - If you want to delete a project from the previous version of Azure Migrate, the steps are the same. The resource type for these projects is **Migration project**.

Created resources

These tables summarize the resources created for discovery, assessment, and migration in an Azure Migrate project.

NOTE

Delete the key vault with caution because it might contain security keys.

VMware/physical server

RESOURCE	TYPE
"ApplianceName"kv	Key vault
"ApplianceName"site	Microsoft.OFFAZURE/VMwareSites

RESOURCE	TYPE
"ProjectName"	Microsoft.Migrate/migrateprojects
"ProjectName"project	Microsoft.Migrate/assessmentProjects
"ProjectName"rvault	Recovery Services vault
"ProjectName"-MigrateVault-*	Recovery Services vault
migrateappligwsa*	Storage account
migrateapplilsa*	Storage account
migrateapplicsa*	Storage account
migrateapplikv*	Key vault
migrateapplisbns16041	Service Bus Namespace

Hyper-V VM

RESOURCE	TYPE
"ProjectName"	Microsoft.Migrate/migrateprojects
"ProjectName"project	Microsoft.Migrate/assessmentProjects
HyperV*kv	Key vault
HyperV*Site	Microsoft.OffAzure/HyperVSites
"ProjectName"-MigrateVault-*	Recovery Services vault

Next steps

Learn how to add additional [assessment](#) and [migration](#) tools.

Work with the previous version of Azure Migrate

2/28/2020 • 16 minutes to read • [Edit Online](#)

This article provides information about working with the previous version of Azure Migrate.

There are two versions of the Azure Migrate service:

- **Current version:** Use this version to create Azure Migrate projects, discover on-premises machines, and orchestrate assessments and migrations. [Learn more](#) about what's new in this version.
- **Previous version:** If you're using the previous version of Azure Migrate (only assessment of on-premises VMware VMs was supported), you should now use the current version. If you still need to use Azure Migrate projects created in the previous version, this is what you can and can't do:
 - You can no longer create migration projects.
 - We recommend that you don't perform new discoveries.
 - You can still access existing projects.
 - You can still run assessments.

Upgrade between versions

You can't upgrade projects or components in the previous version to the new version. You need to [create a new Azure Migrate project](#), and add assessment and migration tools to it.

Find projects from previous version

Find projects from the previous version as follows:

1. In the Azure portal > **All services**, search for and select **Azure Migrate**.
2. On the Azure Migrate dashboard, there's a notification and a link to access old Azure Migrate projects.
3. Click the link to open v1 projects.

Create an assessment

After VMs are discovered in the portal, you group them and create assessments.

- You can immediately create on-premises assessments immediately after VMs are discovered in the portal.
- For performance-based assessments, we recommend you wait at least a day before creating a performance-based assessment, to get reliable size recommendations.

Create an assessment as follows:

1. In the project **Overview** page, click **+Create assessment**.
2. Click **View all** to review the assessment properties.
3. Create the group, and specify a group name.
4. Select the machines that you want to add to the group.
5. Click **Create Assessment**, to create the group and the assessment.
6. After the assessment is created, view it in **Overview > Dashboard**.
7. Click **Export assessment**, to download it as an Excel file.

If you would like to update an existing assessment with the latest performance data, you can use the **Recalculate** command on the assessment to update it.

Review an assessment

An assessment has three stages:

- An assessment starts with a suitability analysis to figure out whether machines are compatible in Azure.
- Sizing estimations.
- Monthly cost estimation.

A machine only moves along to a later stage if it passes the previous one. For example, if a machine fails the suitability check, it's marked as unsuitable for Azure, and sizing and costing isn't done.

Review Azure readiness

The Azure readiness view in the assessment shows the readiness status of each VM.

READINESS	STATE	DETAILS
Ready for Azure	No compatibility issues. The machine can be migrated as-is to Azure, and it will boot in Azure with full Azure support.	For VMs that are ready, Azure Migrate recommends a VM size in Azure.
Conditionally ready for Azure	The machine might boot in Azure, but might not have full Azure support. For example, a machine with an older version of Windows Server that isn't supported in Azure.	Azure Migrate explains the readiness issues, and provides remediation steps.
Not ready for Azure	The VM won't boot in Azure. For example, if a VM has a disk that's more than 4 TB, it can't be hosted on Azure.	Azure Migrate explains the readiness issues, and provides remediation steps.
Readiness unknown	Azure Migrate can't identify Azure readiness, usually because data isn't available.	

Azure VM properties

Readiness takes into account a number of VM properties, to identify whether the VM can run in Azure.

PROPERTY	DETAILS	READINESS
Boot type	BIOS supported. UEFI not supported.	Conditionally ready if boot type is UEFI.
Cores	<p>Machines core <= the maximum number of cores (128) supported for an Azure VM.</p> <p>If performance history is available, Azure Migrate considers the utilized cores.</p> <p>If a comfort factor is specified in the assessment settings, the number of utilized cores is multiplied by the comfort factor.</p> <p>If there's no performance history, Azure Migrate uses the allocated cores, without applying the comfort factor.</p>	Ready if less than or equal to limits.

PROPERTY	DETAILS	READINESS
Memory	<p>The machine memory size <= the maximum memory (3892 GB on Azure M series Standard_M128m²) for an Azure VM. Learn more.</p> <p>If performance history is available, Azure Migrate considers the utilized memory.</p> <p>If a comfort factor is specified, the utilized memory is multiplied by the comfort factor.</p> <p>If there's no history the allocated memory is used, without applying the comfort factor.</p>	Ready if within limits.
Storage disk	<p>Allocated size of a disk must be 4 TB (4096 GB) or less.</p> <p>The number of disks attached to the machine must be 65 or less, including the OS disk.</p>	Ready if within limits.
Networking	A machine must have 32 or less NICs attached to it.	Ready if within limits.

Guest operating system

Along with VM properties, Azure Migrate also looks at the guest OS of the on-premises VM to identify if the VM can run in Azure.

- Azure Migrate considers the OS specified in vCenter Server.
- Since the discovery done by Azure Migrate is appliance-based, it does not have a way to verify if the OS running inside the VM is same as the one specified in vCenter Server.

The following logic is used.

OPERATING SYSTEM	DETAILS	READINESS
Windows Server 2016 and all SPs	Azure provides full support.	Ready for Azure
Windows Server 2012 R2 and all SPs	Azure provides full support.	Ready for Azure
Windows Server 2012 and all SPs	Azure provides full support.	Ready for Azure
Windows Server 2008 R2 and all SPs	Azure provides full support.	Ready for Azure
Windows Server 2008 (32-bit and 64-bit)	Azure provides full support.	Ready for Azure
Windows Server 2003, 2003 R2	Out-of-support and need a Custom Support Agreement (CSA) for support in Azure.	Conditionally ready for Azure, consider upgrading the OS before migrating to Azure.

OPERATING SYSTEM	DETAILS	READINESS
Windows 2000, 98, 95, NT, 3.1, MS-DOS	Out-of-support. The machine might boot in Azure, but no OS support is provided by Azure.	Conditionally ready for Azure, it is recommended to upgrade the OS before migrating to Azure.
Windows Client 7, 8 and 10	Azure provides support with Visual Studio subscription only .	Conditionally ready for Azure
Windows 10 Pro Desktop	Azure provides support with Multitenant Hosting Rights .	Conditionally ready for Azure
Windows Vista, XP Professional	Out-of-support. The machine might boot in Azure, but no OS support is provided by Azure.	Conditionally ready for Azure, it is recommended to upgrade the OS before migrating to Azure.
Linux	Azure endorses these Linux operating systems . Other Linux operating systems might boot in Azure, but we recommend upgrading the OS to an endorsed version, before migrating to Azure.	Ready for Azure if the version is endorsed. Conditionally ready if the version is not endorsed.
Other operating systems For example, Oracle Solaris, Apple Mac OS etc., FreeBSD, etc.	Azure doesn't endorse these operating systems. The machine may boot in Azure, but no OS support is provided by Azure.	Conditionally ready for Azure, it is recommended to install a supported OS before migrating to Azure.
OS specified as Other in vCenter Server	Azure Migrate cannot identify the OS in this case.	Unknown readiness. Ensure that the OS running inside the VM is supported in Azure.
32-bit operating systems	The machine may boot in Azure, but Azure may not provide full support.	Conditionally ready for Azure, consider upgrading the OS of the machine from 32-bit OS to 64-bit OS before migrating to Azure.

Review sizing

The Azure Migrate size recommendation depends on the sizing criterion specified in the assessment properties.

- If sizing is performance-based, the size recommendation considers the performance history of the VMs (CPU and memory) and disks (IOPS and throughput).
- If the sizing criterion is 'as on-premises', the size recommendation in Azure is based on the size of the VM on-premises. Disk sizing is based on the Storage type specified in the assessment properties (default is premium disks). Azure Migrate doesn't consider the performance data for the VM and disks.

Review cost estimates

Cost estimates show the total compute and storage cost of running the VMs in Azure, along with the details for each machine.

- Cost estimates are calculated using the size recommendation for a VM machine, and its disks, and the assessment properties.
- Estimated monthly costs for compute and storage are aggregated for all VMs in the group.
- The cost estimation is for running the on-premises VM as Azure Infrastructure as a service (IaaS) VMs. Azure Migrate doesn't consider Platform as a service (PaaS), or Software as a service (SaaS) costs.

Review confidence rating (performance-based assessment)

Each performance-based assessment is associated with a confidence rating.

- A confidence rating ranges from one-star to five-star (one-star being the lowest and five-star the highest).
- The confidence rating is assigned to an assessment, based on the availability of data points needed to compute the assessment.
- The confidence rating of an assessment helps you estimate the reliability of the size recommendations provided by Azure Migrate.
- Confidence rating isn't available for "as-is" on-premises assessments.

For performance-based sizing, Azure Migrate needs the following:

- Utilization data for CPU.
- VM memory data.
- For every disk attached to the VM, it needs the disk IOPS and throughput data.
- For each network adapter attached to a VM, Azure Migrate needs the network input/output.
- If any of the above aren't available, size recommendations (and thus confidence ratings) might not be reliable.

Depending on the percentage of data points available, the possible confidence ratings are summarized in the table.

AVAILABILITY OF DATA POINTS	CONFIDENCE RATING
0%-20%	1 Star
21%-40%	2 Star
41%-60%	3 Star
61%-80%	4 Star
81%-100%	5 Star

Assessment issues affecting confidence ratings

An assessment might not have all the data points available due to a number of reasons:

- You didn't profile your environment for the duration of the assessment. For example, if you create the assessment with performance duration set to one day, you must wait for at least a day after you start the discovery, or all the data points to be collected.
- Some VMs were shut down during the period for which the assessment was calculated. If any VMs were powered off for part of the duration, Azure Migrate can't collect performance data for that period.
- Some VMs were created in between during the assessment calculation period. For example, if you create an assessment using the last month's performance history, but create a number of VMs in the environment a week ago, the performance history of the new VMs won't be for the entire duration.

NOTE

If the confidence rating of any assessment is below five-stars, wait for at least a day for the appliance to profile the environment, and then recalculate the assessment. If you don't performance-based sizing might not be reliable. If you don't want to recalculate, we recommended switching to as on-premises sizing, by changing the assessment properties.

Create groups using dependency visualization

In addition to creating groups manually, you can create groups using dependency visualization.

- You typically use this method when you want to assess groups with higher levels of confidence by cross-

checking machine dependencies, before you run an assessment.

- Dependency visualization can help you effectively plan your migration to Azure. It helps you ensure that nothing is left behind, and that surprise outages do not occur when you are migrating to Azure.
- You can discover all interdependent systems that need to migrate together and identify whether a running system is still serving users or is a candidate for decommissioning instead of migration.
- Azure Migrate uses the Service Map solution in Azure Monitor to enable dependency visualization.

NOTE

Dependency visualization is not available in Azure Government.

To set up dependency visualization, you associate a Log Analytics workspace with an Azure Migrate project, install agents on machines for which you want to visualize dependencies, and then create groups using dependency information.

Associate a Log Analytics workspace

To use dependency visualization, you associate a Log Analytics workspace with a migration project. You can only create or attach a workspace in the same subscription where the migration project is created.

- To attach a Log Analytics workspace to a project, in [Overview](#), > [Essentials](#), click **Requires configuration**.
- You can create a new workspace, or attach an existing one:
 - To create a new workspace, specify a name. The workspace is created in a region in the same [Azure geography](#) as the migration project.
 - When you attach an existing workspace, you can pick from all the available workspaces in the same subscription as the migration project. Only those workspaces are listed which were created in a [supported Service Map region](#). To attach a workspace, ensure that you have 'Reader' access to the workspace.

NOTE

You can't change the workspace associated with a migration project.

Download and install VM agents

After you configure a workspace, you download and install agents on each on-premises machine that you want to evaluate. In addition, if you have machines with no internet connectivity, you need to download and install [Log Analytics gateway](#) on them.

- In [Overview](#), click **Manage** > **Machines**, and select the required machine.
- In the **Dependencies** column, click **Install agents**.
- On the **Dependencies** page, download and install the Microsoft Monitoring Agent (MMA), and the Dependency agent on each VM you want to assess.
- Copy the workspace ID and key. You need these when you install the MMA on the on-premises machine.

NOTE

To automate the installation of agents you can use a deployment tool such as Configuration Manager or a partner tool such as [Intigua](#), that provides an agent deployment solution for Azure Migrate.

Install the MMA agent on a Windows machine

To install the agent on a Windows machine:

- Double-click the downloaded agent.

2. On the **Welcome** page, click **Next**. On the **License Terms** page, click **I Agree** to accept the license.
3. In **Destination Folder**, keep or modify the default installation folder > **Next**.
4. In **Agent Setup Options**, select **Azure Log Analytics** > **Next**.
5. Click **Add** to add a new Log Analytics workspace. Paste in the workspace ID and key that you copied from the portal. Click **Next**.

You can install the agent from the command line or using an automated method such as Configuration Manager. [Learn more](#) about using these methods to install the MMA agent.

Install the MMA agent on a Linux machine

To install the agent on a Linux machine:

1. Transfer the appropriate bundle (x86 or x64) to your Linux computer using scp/sftp.
2. Install the bundle by using the --install argument.

```
sudo sh ./omsagent-<version>.universal.x64.sh --install -w <workspace id> -s <workspace key>
```

[Learn more](#) about the list of Linux operating systems support by MMA.

Install the MMA agent on a machine monitored by Operations Manager

For machines monitored by System Center Operations Manager 2012 R2 or later, there is no need to install the MMA agent. Service Map integrates with the Operations Manager MMA to gather the necessary dependency data. [Learn more](#). The Dependency agent does need to be installed.

Install the Dependency agent

1. To install the Dependency agent on a Windows machine, double-click the setup file and follow the wizard.
2. To install the Dependency agent on a Linux machine, install as root using the following command:

```
sh InstallDependencyAgent-Linux64.bin
```

- Learn more about the [Dependency agent support](#) for the Windows and Linux operating systems.
- [Learn more](#) about how you can use scripts to install the Dependency agent.

NOTE

The Azure Monitor for VMs article referenced to provide an overview of the system prerequisites and methods to deploy the Dependency agent are also applicable to the Service Map solution.

Create a group with dependency mapping

1. After you install the agents, go to the portal and click **Manage** > **Machines**.
2. Search for the machine where you installed the agents.
3. The **Dependencies** column for the machine should now show as **View Dependencies**. Click the column to view the dependencies of the machine.
4. The dependency map for the machine shows the following details:
 - Inbound (Clients) and outbound (Servers) TCP connections to/from the machine
 - The dependent machines that do not have the MMA and dependency agent installed are grouped by port numbers.
 - The dependent machines that have the MMA and the dependency agent installed are shown as separate boxes.
 - Processes running inside the machine, you can expand each machine box to view the processes
 - Machine properties, including the FQDN, operating System, MAC address are shown. You can click on

each machine box to view details.

5. You can view dependencies for different time durations by clicking on the time duration in the time range label. By default the range is an hour. You can modify the time range, or specify start and end dates, and duration.

NOTE

A time range of up to an hour is supported. Use Azure Monitor logs to [query dependency data](#) over a longer duration.

6. After you've identified dependent machines that you want to group together, use Ctrl+Click to select multiple machines on the map, and click **Group machines**.
7. Specify a group name. Verify that the dependent machines are discovered by Azure Migrate.

NOTE

If a dependent machine is not discovered by Azure Migrate, you can't add it to the group. To add such machines to the group, you need to run the discovery process again with the right scope in vCenter Server and ensure that the machine is discovered by Azure Migrate.

8. If you want to create an assessment for this group, select the checkbox to create a new assessment for the group.
9. Click **OK** to save the group.

Once the group is created, it is recommended to install agents on all the machines of the group and refine the group by visualizing the dependency of the entire group.

Query dependency data from Azure Monitor logs

Dependency data captured by Service Map is available for querying in the Log Analytics workspace associated with your Azure Migrate project. [Learn more](#) about the Service Map data tables to query in Azure Monitor logs.

To run the Kusto queries:

1. After you install the agents, go to the portal and click **Overview**.
2. In **Overview**, go to **Essentials** section of the project and click on workspace name provided next to **OMS Workspace**.
3. On the Log Analytics workspace page, click **General > Logs**.
4. Write your query to gather dependency data using Azure Monitor logs. Find sample queries in the next section.
5. Run your query by clicking on **Run**.

[Learn more](#) about how to write Kusto queries.

Sample Azure Monitor logs queries

Following are sample queries you can use to extract dependency data. You can modify the queries to extract your preferred data points. An exhaustive list of the fields in dependency data records is available [here](#). Find more sample queries [here](#).

Summarize inbound connections on a set of machines

The records in the table for connection metrics, VMConnection, do not represent individual physical network connections. Multiple physical network connections are grouped into a logical connection. [Learn more](#) about how physical network connection data is aggregated into a single logical record in VMConnection.

```
// the machines of interest
let ips=materialize(ServiceMapComputer_CL
| summarize ips=makeset(todynamic(Ipv4Addresses_s)) by MonitoredMachine=ResourceName_s
| mvexpand ips to typeof(string));
let StartDateTime = datetime(2019-03-25T00:00:00Z);
let EndDateTime = datetime(2019-03-30T01:00:00Z);
VMConnection
| where Direction == 'inbound'
| where TimeGenerated > StartDateTime and TimeGenerated < EndDateTime
| join kind=inner (ips) on $left.DestinationIp == $right.ips
| summarize sum(LinksEstablished) by Computer, Direction, SourceIp, DestinationIp, DestinationPort
```

Summarize volume of data sent and received on inbound connections between a set of machines

```
// the machines of interest
let ips=materialize(ServiceMapComputer_CL
| summarize ips=makeset(todynamic(Ipv4Addresses_s)) by MonitoredMachine=ResourceName_s
| mvexpand ips to typeof(string));
let StartDateTime = datetime(2019-03-25T00:00:00Z);
let EndDateTime = datetime(2019-03-30T01:00:00Z);
VMConnection
| where Direction == 'inbound'
| where TimeGenerated > StartDateTime and TimeGenerated < EndDateTime
| join kind=inner (ips) on $left.DestinationIp == $right.ips
| summarize sum(BytesSent), sum(BytesReceived) by Computer, Direction, SourceIp, DestinationIp, DestinationPort
```

Next steps

[Learn about](#) the latest version of Azure Migrate.

Assess large numbers of VMware VMs for migration to Azure

3/26/2020 • 4 minutes to read • [Edit Online](#)

This article describes how to assess large numbers (1000–35,000) of on-premises VMware VMs for migration to Azure, using the Azure Migrate Server Assessment tool.

Azure Migrate provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

In this article, you learn how to:

- Plan for assessment at scale.
- Configure Azure permissions, and prepare VMware for assessment.
- Create an Azure Migrate project, and create an assessment.
- Review the assessment as you plan for migration.

NOTE

If you want to try out a proof-of-concept to assess a couple of VMs before assessing at scale, follow our [tutorial series](#)

Plan for assessment

When planning for assessment of large number of VMware VMs, there are a couple of things to think about:

- **Plan Azure Migrate projects:** Figure out how to deploy Azure Migrate projects. For example, if your data centers are in different geographies, or you need to store discovery, assessment or migration-related metadata in a different geography, you might need multiple projects.
- **Plan appliances:** Azure Migrate uses an on-premises Azure Migrate appliance, deployed as a VMware VM, to continually discover VMs. The appliance monitors environment changes such as adding VMs, disks, or network adapters. It also sends metadata and performance data about them to Azure. You need to figure out how many appliances you need to deploy.
- **Plan accounts for discovery:** The Azure Migrate appliance uses an account with access to vCenter Server in order to discover VMs for assessment and migration. If you're discovering more than 10,000 VMs, set up multiple accounts.

Planning limits

Use the limits summarized in this table for planning.

PLANNING	LIMITS
Azure Migrate projects	Assess up to 35,000 VMs in a project.

PLANNING	LIMITS
Azure Migrate appliance	An appliance can discover up to 10,000 VMs on a vCenter Server. An appliance can only connect to a single vCenter Server. An appliance can only be associated with a single Azure Migrate project. Any number of appliances can be associated with a single Azure Migrate project.
Group	You can add up to 35,000 VMs in a single group.
Azure Migrate assessment	You can assess up to 35,000 VMs in a single assessment.

With these limits in mind, here are some example deployments:

VCENTER SERVER	VMS ON SERVER	RECOMMENDATION	ACTION
One	< 10,000	One Azure Migrate project. One appliance. One vCenter account for discovery.	Set up appliance, connect to vCenter Server with an account.
One	> 10,000	One Azure Migrate project. Multiple appliances. Multiple vCenter accounts.	Set up appliance for every 10,000 VMs. Set up vCenter accounts, and divide inventory to limit access for an account to less than 10,000 VMs. Connect each appliance to vCenter server with an account. You can analyze dependencies across machines that are discovered with different appliances.
Multiple	< 10,000	One Azure Migrate project. Multiple appliances. One vCenter account for discovery.	Set up appliances, connect to vCenter Server with an account. You can analyze dependencies across machines that are discovered with different appliances.

VCENTER SERVER	VMS ON SERVER	RECOMMENDATION	ACTION
Multiple	> 10,000	One Azure Migrate project. Multiple appliances. Multiple vCenter accounts.	If vCenter Server discovery < 10,000 VMs, set up an appliance for each vCenter Server. If vCenter Server discovery > 10,000 VMs, set up an appliance for every 10,000 VMs. Set up vCenter accounts, and divide inventory to limit access for an account to less than 10,000 VMs. Connect each appliance to vCenter server with an account. You can analyze dependencies across machines that are discovered with different appliances.

Plan discovery in a multi-tenant environment

If you're planning for a multi-tenant environment, you can scope the discovery on the vCenter Server.

- You can set the appliance discovery scope to a vCenter Server datacenters, clusters or folder of clusters, hosts or folder of hosts, or individual VMs.
- If your environment is shared across tenants and you want to discover each tenant separately, you can scope access to the vCenter account that the appliance uses for discovery.
 - You may want to scope by VM folders if the tenants share hosts. Azure Migrate can't discover VMs if the vCenter account has access granted at the vCenter VM folder level. If you are looking to scope your discovery by VM folders, you can do so by ensuring the vCenter account has read-only access assigned at a VM level. [Learn more](#).

Prepare for assessment

Prepare Azure and VMware for server assessment.

1. Verify [VMware support requirements and limitations](#).
2. Set up permissions for your Azure account to interact with Azure Migrate.
3. Prepare VMware for assessment.

Follow the instructions in [this tutorial](#) to configure these settings.

Create a project

In accordance with your planning requirements, do the following:

1. Create an Azure Migrate projects.
2. Add the Azure Migrate Server Assessment tool to the projects.

[Learn more](#)

Create and review an assessment

1. Create assessments for VMware VMs.
2. Review the assessments in preparation for migration planning.

Follow the instructions in [this tutorial](#) to configure these settings.

Next steps

In this article, you:

- Planned to scale Azure Migrate assessments for VMware VMs
- Prepared Azure and VMware for assessment
- Created an Azure Migrate project and ran assessments
- Reviewed assessments in preparation for migration.

Now, [learn how](#) assessments are calculated, and how to [modify assessments](#).

This article describes how to assess large numbers of on-premises Hyper-V VMs for migration to Azure, using the Azure Migrate Server Assessment tool.

Azure Migrate provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

In this article, you learn how to:

- Plan for assessment at scale.
- Configure Azure permissions, and prepare Hyper-V for assessment.
- Create an Azure Migrate project, and create an assessment.
- Review the assessment as you plan for migration.

NOTE

If you want to try out a proof-of-concept to assess a couple of VMs before assessing at scale, follow our [tutorial series](#)

Plan for assessment

When planning for assessment of large number of Hyper-V VMs, there are a couple of things to think about:

- **Plan Azure Migrate projects:** Figure out how to deploy Azure Migrate projects. For example, if your data centers are in different geographies, or you need to store discovery, assessment or migration-related metadata in a different geography, you might need multiple projects.
- **Plan appliances:** Azure Migrate uses an on-premises Azure Migrate appliance, deployed as a Hyper-V VM, to continually discover VMs for assessment and migration. The appliance monitors environment changes such as adding VMs, disks, or network adapters. It also sends metadata and performance data about them to Azure. You need to figure out how many appliances to deploy.

Planning limits

Use the limits summarized in this table for planning.

PLANNING	LIMITS
Azure Migrate projects	Assess up to 35,000 VMs in a project.
Azure Migrate appliance	An appliance can discover up to 5000 VMs. An appliance can connect to up to 300 Hyper-V hosts. An appliance can only be associated with a single Azure Migrate project. Any number of appliances can be associated with a single Azure Migrate project.
Group	You can add up to 35,000 VMs in a single group.

PLANNING	LIMITS
Azure Migrate assessment	You can assess up to 35,000 VMs in a single assessment.

Other planning considerations

- To start discovery from the appliance, you have to select each Hyper-V host.
- If you're running a multi-tenant environment, you can't currently discover only VMs that belong to a specific tenant.

Prepare for assessment

Prepare Azure and Hyper-V for server assessment.

1. Verify [Hyper-V support requirements and limitations](#).
2. Set up permissions for your Azure account to interact with Azure Migrate
3. Prepare Hyper-V hosts and VMs

Follow the instructions in [this tutorial](#) to configure these settings.

Create a project

In accordance with your planning requirements, do the following:

1. Create an Azure Migrate projects.
2. Add the Azure Migrate Server Assessment tool to the projects.

[Learn more](#)

Create and review an assessment

1. Create assessments for Hyper-V VMs.
2. Review the assessments in preparation for migration planning.

[Learn more](#) about creating and reviewing assessments.

Next steps

In this article, you:

- Planned to scale Azure Migrate assessments for Hyper-V VMs
- Prepared Azure and Hyper-V for assessment
- Created an Azure Migrate project and ran assessments
- Reviewed assessments in preparation for migration.

Now, [learn how](#) assessments are calculated, and how to [modify assessments](#)

This article describes how to assess large numbers of on-premises physical servers for migration to Azure, using the Azure Migrate Server Assessment tool.

[Azure Migrate](#) provides a hub of tools that help you to discover, assess, and migrate apps, infrastructure, and workloads to Microsoft Azure. The hub includes Azure Migrate tools, and third-party independent software vendor (ISV) offerings.

In this article, you learn how to:

- Plan for assessment at scale.
- Configure Azure permissions, and prepare physical servers for assessment.
- Create an Azure Migrate project, and create an assessment.
- Review the assessment as you plan for migration.

NOTE

If you want to try out a proof-of-concept to assess a couple of servers before assessing at scale, follow our [tutorial series](#).

Plan for assessment

When planning for assessment of large number of physical servers, there are a couple of things to think about:

- **Plan Azure Migrate projects:** Figure out how to deploy Azure Migrate projects. For example, if your data centers are in different geographies, or you need to store discovery, assessment or migration-related metadata in a different geography, you might need multiple projects.
- **Plan appliances:** Azure Migrate uses an on-premises Azure Migrate appliance, deployed on a Windows machine, to continually discover servers for assessment and migration. The appliance monitors environment changes such as adding VMs, disks, or network adapters. It also sends metadata and performance data about them to Azure. You need to figure out how many appliances to deploy.

Planning limits

Use the limits summarized in this table for planning.

PLANNING	LIMITS
Azure Migrate projects	Assess up to 35,000 servers in a project.
Azure Migrate appliance	An appliance can discover up to 250 servers. An appliance can only be associated with a single Azure Migrate project. Any number of appliances can be associated with a single Azure Migrate project.
Group	You can add up to 35,000 servers in a single group.
Azure Migrate assessment	You can assess up to 35,000 servers in a single assessment.

Other planning considerations

- To start discovery from the appliance, you have to select each physical server.

Prepare for assessment

Prepare Azure and physical servers for server assessment.

1. Verify [physical server support requirements and limitations](#).
2. Set up permissions for your Azure account to interact with Azure Migrate.
3. Prepare the physical servers.

Follow the instructions in [this tutorial](#) to configure these settings.

Create a project

In accordance with your planning requirements, do the following:

1. Create an Azure Migrate project.
2. Add the Azure Migrate Server Assessment tool to the projects.

[Learn more](#)

Create and review an assessment

1. Create assessments for physical servers.
2. Review the assessments in preparation for migration planning.

[Learn more](#) about creating and reviewing assessments.

Next steps

In this article, you:

- Planned to scale Azure Migrate assessments for physical servers.
- Prepared Azure and physical servers for assessment.
- Created an Azure Migrate project and ran assessments.
- Reviewed assessments in preparation for migration.

Now, [learn how](#) assessments are calculated, and how to [modify assessments](#).

This article helps you understand how to use scripts to migrate large number of virtual machines (VMs). To scale migration, you use [Azure Site Recovery](#).

Site Recovery scripts are available for your download at [Azure PowerShell Samples](#) repo on GitHub. The scripts can be used to migrate VMWare, AWS, GCP VMs, and physical servers to managed disks in Azure. You can also use these scripts to migrate Hyper-V VMs if you migrate the VMs as physical servers. The scripts that leverage Azure Site Recovery PowerShell are documented [here](#).

Current limitations

- Support specifying the static IP address only for the primary NIC of the target VM
- The scripts do not take Azure Hybrid Benefit related inputs, you need to manually update the properties of the replicated VM in the portal

How does it work?

Prerequisites

Before you get started, you need to do the following steps:

- Ensure that the Site Recovery vault is created in your Azure subscription
- Ensure that the Configuration Server and Process Server are installed in the source environment and the vault is able to discover the environment
- Ensure that a Replication Policy is created and associated with the Configuration Server
- Ensure that you have added the VM admin account to the config server (that will be used to replicate the on-premises VMs)
- Ensure that the target artifacts in Azure are created
 - Target Resource Group
 - Target Storage Account (and its Resource Group) - Create a premium storage account if you plan to migrate to premium-managed disks
 - Cache Storage Account (and its Resource Group) - Create a standard storage account in the same region as the vault
 - Target Virtual Network for failover (and its Resource Group)
 - Target Subnet
 - Target Virtual Network for Test failover (and its Resource Group)
 - Availability Set (if needed)
 - Target Network Security Group and its Resource Group
- Ensure that you have decided on the properties of the target VM
 - Target VM name
 - Target VM size in Azure (can be decided using Azure Migrate assessment)
 - Private IP Address of the primary NIC in the VM
- Download the scripts from [Azure PowerShell Samples](#) repo on GitHub

CSV Input file

Once you have all the pre-requisites completed, you need to create a CSV file, which has data for each source machine that you want to migrate. The input CSV must have a header line with the input details and a row with

details for each machine that needs to be migrated. All the scripts are designed to work on the same CSV file. A sample CSV template is available in the scripts folder for your reference.

Script execution

Once the CSV is ready, you can execute the following steps to perform migration of the on-premises VMs:

STEP #	SCRIPT NAME	DESCRIPTION
1	asr_startmigration.ps1	Enable replication for all the VMs listed in the csv, the script creates a CSV output with the job details for each VM
2	asr_replicationstatus.ps1	Check the status of replication, the script creates a csv with the status for each VM
3	asr_updateproperties.ps1	Once the VMs are replicated/protected, use this script to update the target properties of the VM (Compute and Network properties)
4	asr_propertiescheck.ps1	Verify if the properties are appropriately updated
5	asr_testmigration.ps1	Start the test failover of the VMs listed in the csv, the script creates a CSV output with the job details for each VM
6	asr_cleanuptestmigration.ps1	Once you manually validate the VMs that were test failed-over, you can use this script to clean up the test failover VMs
7	asr_migration.ps1	Perform an unplanned failover for the VMs listed in the csv, the script creates a CSV output with the job details for each VM. The script does not shut down the on premises VMs before triggering the failover, for application consistency, it is recommended that you manually shut down the VMs before executing the script.
8	asr_completemigration.ps1	Perform the commit operation on the VMs and delete the Azure Site Recovery entities
9	asr_postmigration.ps1	If you plan to assign network security groups to the NICs post-failover, you can use this script to do that. It assigns an NSG to any one NIC in the target VM.

How to migrate to managed disks?

The script, by default, migrates the VMs to managed disks in Azure. If the target storage account provided is a premium storage account, premium-managed disks are created post migration. The cache storage account can still be a standard account. If the target storage account is a standard storage account, standard disks are created post

migration.

Next steps

[Learn more](#) about migrating servers to Azure using Azure Site Recovery

We have a series of articles that demonstrates how the fictitious organization Contoso migrates on-premises infrastructure to the [Microsoft Azure](#) cloud.

The series includes information and scenarios that illustrate how to set up a migration of infrastructure, and run different types of migrations. Scenarios grow in complexity as they progress. The articles show how the Contoso company completes its migration mission, but pointers for general reading and specific instructions are provided throughout.

Migration articles

The articles in the series are summarized in the table below.

- Each migration scenario is driven by slightly different business goals that determine the migration strategy.
- For each deployment scenario, we provide information about business drivers and goals, a proposed architecture, steps to perform the migration, and recommendation for cleanup and next steps after migration is complete.

ARTICLE	DETAILS
Article 1: Overview	Overview of the article series, Contoso's migration strategy, and the sample apps that are used in the series.
Article 2: Deploy Azure infrastructure	Contoso prepares its on-premises infrastructure and its Azure infrastructure for migration. The same infrastructure is used for all migration articles in the series.
Article 3: Assess on-premises resources for migration to Azure	Contoso runs an assessment of its on-premises SmartHotel360 app running on VMware. Contoso assesses app VMs using the Azure Migrate service, and the app SQL Server database using Data Migration Assistant.
Article 4: Rehost an app on an Azure VM and SQL Database Managed Instance	Contoso runs a lift-and-shift migration to Azure for its on-premises SmartHotel360 app. Contoso migrates the app front-end VM using Azure Site Recovery . Contoso migrates the app database to an Azure SQL Database Managed Instance using the Azure Database Migration Service .
Article 5: Rehost an app on Azure VMs	Contoso migrates its SmartHotel360 app VMs to Azure VMs by using the Site Recovery service.
Article 6: Rehost an app on Azure VMs and in a SQL Server AlwaysOn availability group	Contoso migrates the SmartHotel360 app. Contoso uses Site Recovery to migrate the app VMs. It uses the Database Migration Service to migrate the app database to a SQL Server cluster that's protected by an AlwaysOn availability group.
Article 7: Rehost a Linux app on Azure VMs	Contoso completes a lift-and-shift migration of its Linux osTicket app to Azure VMs, using the Site Recovery service.

ARTICLE	DETAILS
Article 8: Rehost a Linux app on Azure VMs and Azure Database for MySQL	Contoso migrates its Linux osTicket app to Azure VMs by using Site Recovery. It migrates the app database to Azure Database for MySQL by using MySQL Workbench.
Article 9: Refactor an app in an Azure web app and Azure SQL Database	Contoso migrates its SmartHotel360 app to an Azure web app and migrates the app database to an Azure SQL Server instance with the Database Migration Assistant.
Article 10: Refactor a Linux app in an Azure web app and Azure Database for MySQL	Contoso migrates its Linux osTicket app to an Azure web app on multiple Azure regions using Azure Traffic Manager, integrated with GitHub for continuous delivery. Contoso migrates the app database to an Azure Database for MySQL instance.
Article 11: Refactor Team Foundation Server on Azure DevOps Services	Contoso migrates its on-premises Team Foundation Server deployment to Azure DevOps Services in Azure.
Article 12: Rearchitect an app in Azure containers and Azure SQL Database	Contoso migrates its SmartHotel app to Azure. Then, it rearchitects the app web tier as a Windows container running in Azure Service Fabric, and the database with Azure SQL Database.
Article 13: Rebuild an app in Azure	Contoso rebuilds its SmartHotel app by using a range of Azure capabilities and services, including Azure App Service, Azure Kubernetes Service (AKS), Azure Functions, Azure Cognitive Services, and Azure Cosmos DB.
Article 14: Scale a migration to Azure	After trying out migration combinations, Contoso prepares to scale to a full migration to Azure.

Next steps

- [Learn about](#) cloud migration.
- Learn about migrations strategies for other scenarios (source/target pairs) in the [Database Migration Guide](#).

minutes to read • [Edit Online](#)

Azure Migrate provides a hub of tools for assessment and migration, as well as third-party independent software vendor (ISV) offerings. This article helps you troubleshoot issues with Azure Migrate, Azure Migrate Server Assessment, and Azure Migrate Server Migration.

How do I create or find a project?

Review the [Azure Migrate project troubleshooting guide](#).

I can't get the appliance working

Review [answers to common issues](#) with appliance deployment.

Machines aren't discovered

Review common discovery issues.

App-discovery isn't working

Discovery of apps, roles, and features running on on-premises machines is currently only supported for VMware VMs. [Review common errors](#) for app-discovery.

Assessment isn't working

Review common assessment issues and errors.

This article helps you troubleshoot issues when creating and managing [Azure Migrate](#) projects.

How to add new project?

You can have multiple Azure Migrate projects in a subscription. [Learn how](#) to create a project for the first time, or [add additional](#) projects.

What Azure permissions are needed?

You need Contributor or Owner permissions in the subscription to create an Azure Migrate project.

Can't find a project

Finding an existing Azure Migrate project depends upon whether you're using the current or old version of Azure Migrate. [Follow](#).

Can't find a geography

You can create an Azure Migrate project in [supported geographies](#). Note that the project geography is used to store discovered machine metadata. You can assess or migrate machines in other locations too.

What are VM limits?

You can assess up to 35,000 VMware VMs or up to 35,000 Hyper-V VMs in a single project. A project can include both VMware VMs and Hyper-V VMs, up to the assessment limits.

Can I upgrade old project?

Projects from the previous version of Azure Migrate can't be updated. You need to [create a new project](#), and add tools to it.

Can't create a project

If you try to create a project and encounter a deployment error:

- Try to create the project again in case it's a transient error. In [Deployments](#), click on [Re-deploy](#) to try again.
- Check you have Contributor or Owner permissions in the subscription.
- If you're deploying in a newly added geography, wait a short time and try again.
- If you receive the error, "Requests must contain user identity headers", this might indicate that you don't have access to the Azure Active Directory (Azure AD) tenant of the organization. In this case:
 - When you're added to an Azure AD tenant for the first time, you receive an email invitation to join the tenant.
 - Accept the invitation to be added to the tenant.
 - If you can't see the email, contact a user with access to the tenant, and ask them to [resend the invitation](#) to you.
 - After receiving the invitation email, open it and select the link to accept the invitation. Then, sign out of the Azure portal and sign in again. (refreshing the browser won't work.) You can then start creating the

migration project.

How do I delete a project

Follow these instructions to delete a project. Note that when you delete a project, both the project and the metadata about discovered machines in the project are deleted.

Added tools don't show

Make sure you have the right project selected. In the Azure Migrate hub > **Servers** or in **Databases**, click on **Change** next to **Migrate project (Change)** in the top-right corner of the screen. Choose the correct subscription and project name > **OK**. The page should refresh with the added tools of the selected project.

Next steps

Add [assessment](#) or [migration](#) tools to Azure Migrate projects.

This article helps you troubleshoot issues when deploying the [Azure Migrate](#) appliance, and using the appliance to discover on-premises machines.

What's supported?

[Review](#) the appliance support requirements.

"Invalid OVF manifest entry"

If you receive the error "The provided manifest file is invalid: Invalid OVF manifest entry", do the following:

1. Verify that the Azure Migrate appliance OVA file is downloaded correctly by checking its hash value. [Learn more](#). If the hash value doesn't match, download the OVA file again and retry the deployment.
2. If deployment still fails, and you're using the VMware vSphere client to deploy the OVF file, try deploying it through the vSphere web client. If deployment still fails, try using a different web browser.
3. If you're using the vSphere web client and trying to deploy it on vCenter Server 6.5 or 6.7, try to deploy the OVA directly on the ESXi host:
 - Connect to the ESXi host directly (instead of vCenter Server) with the web client (`https://<host IP Address>/ui`).
 - In **Home > Inventory**, select **File > Deploy OVF template**. Browse to the OVA and complete the deployment.
4. If the deployment still fails, contact Azure Migrate support.

Can't connect to the internet

This can happen if the appliance machine is behind a proxy.

- Make sure you provide the authorization credentials if the proxy needs them.
- If you're using a URL-based firewall proxy to control outbound connectivity, add [these URLs](#) to an allow list.
- If you're using an intercepting proxy to connect to the internet, import the proxy certificate onto the appliance VM using [these steps](#).

Date/time synchronization error

An error about date and time synchronization (802) indicates that the server clock might be out of synchronization with the current time by more than five minutes. Change the clock time on the collector VM to match the current time:

1. Open an admin command prompt on the VM.
2. To check the time zone, run `w32tm /tz`.
3. To synchronize the time, run `w32tm /resync`.

"UnableToConnectToServer"

If you get this connection error, you might be unable to connect to vCenter Server `Servername.com:9443`. The error details indicate that there's no endpoint listening at `https://*servername*.com:9443/sdk` that can accept the message.

- Check whether you're running the latest version of the appliance. If you're not, upgrade the appliance to the [latest version](#).
- If the issue still occurs in the latest version, the appliance might be unable to resolve the specified vCenter Server name, or the specified port might be wrong. By default, if the port is not specified, the collector will try to connect to port number 443.
 1. Ping *Servername.com* from the appliance.
 2. If step 1 fails, try to connect to the vCenter server using the IP address.
 3. Identify the correct port number to connect to vCenter Server.
 4. Verify that vCenter Server is up and running.

Error 60052/60039: Appliance might not be registered

- Error 60052, "The appliance might not be registered successfully to the Azure Migrate project" occurs if the Azure account used to register the appliance has insufficient permissions.
 - Make sure that the Azure user account used to register the appliance has at least Contributor permissions on the subscription.
 - [Learn more](#) about required Azure roles and permissions.
- Error 60039, "The appliance might not be registered successfully to the Azure Migrate project" can occur if registration fails because the Azure Migrate project used to register the appliance can't be found.
 - In the Azure portal and check whether the project exists in the resource group.
 - If the project doesn't exist, create a new Azure Migrate project in your resource group and register the appliance again. [Learn how to](#) create a new project.

Error 60030/60031: Key Vault management operation failed

If you receive the error 60030 or 60031, "An Azure Key Vault management operation failed", do the following:

- Make sure the Azure user account used to register the appliance has at least Contributor permissions on the subscription.
- Make sure the account has access to the key vault specified in the error message, and then retry the operation.
- If the issue persists, contact Microsoft support.
- [Learn more](#) about the required Azure roles and permissions.

Error 60028: Discovery couldn't be initiated

Error 60028: "Discovery couldn't be initiated because of an error. The operation failed for the specified list of hosts or clusters" indicates that discovery couldn't be started on the hosts listed in the error because of a problem in accessing or retrieving VM information. The rest of the hosts were successfully added.

- Add the hosts listed in the error again, using the **Add host** option.
- If there's a validation error, review the remediation guidance to fix the errors, and then try the **Save and start discovery** option again.

Error 60025: Azure AD operation failed

Error 60025: "An Azure AD operation failed. The error occurred while creating or updating the Azure AD application" occurs when the Azure user account used to initiate the discovery is different from the account used to register the appliance. Do one of the following:

- Ensure that the user account initiating the discovery is same as the one used to register the appliance.
- Provide Azure Active Directory application access permissions to the user account for which the discovery

- operation is failing.
- Delete the resource group previously created for the Azure Migrate project. Create another resource group to start again.
 - [Learn more](#) about Azure Active Directory application permissions.

Error 50004: Can't connect to host or cluster

Error 50004: "Can't connect to a host or cluster because the server name can't be resolved. WinRM error code: 0x803381B9" might occur if the Azure DNS service for the appliance can't resolve the cluster or host name you provided.

- If you see this error on the cluster, cluster FQDN.
- You might also see this error for hosts in a cluster. This indicates that the appliance can connect to the cluster, but the cluster returns host names that aren't FQDNs. To resolve this error, update the hosts file on the appliance by adding a mapping of the IP address and host names:
 1. Open Notepad as an admin.
 2. Open the C:\Windows\System32\Drivers\etc\hosts file.
 3. Add the IP address and host name in a row. Repeat for each host or cluster where you see this error.
 4. Save and close the hosts file.
 5. Check whether the appliance can connect to the hosts, using the appliance management app. After 30 minutes, you should see the latest information for these hosts in the Azure portal.

Discovered VMs not in portal

If discovery state is "Discovery in progress", but don't yet see the VMs in the portal, wait a few minutes:

- It takes around 15 minutes for a VMware VM .
- It takes around two minutes for each added host for Hyper-V VM discovery.

If you wait and the state doesn't change, select **Refresh** on the **Servers** tab. This should show the count of the discovered servers in Azure Migrate: Server Assessment and Azure Migrate: Server Migration.

If this doesn't work and you're discovering VMware servers:

- Verify that the vCenter account you specified has permissions set correctly, with access to at least one VM.
- Azure Migrate can't discover VMware VMs if the vCenter account has access granted at vCenter VM folder level. [Learn more](#) about scoping discovery.

VM data not in portal

If discovered VMs don't appear in the portal or if the VM data is outdated, wait a few minutes. It takes up to 30 minutes for changes in discovered VM configuration data to appear in the portal. It may take a few hours for changes in application data to appear. If there's no data after this time, try refreshing, as follows

1. In **Servers > Azure Migrate Server Assessment**, select **Overview**.
2. Under **Manage**, select **Agent Health**.
3. Select **Refresh agent**.
4. Wait for the refresh operation to complete. You should now see up-to-date information.

Deleted VMs appear in portal

If you delete VMs and they still appear in the portal, wait 30 minutes. If they still appear, refresh as described above.

Common app discovery errors

Azure Migrate supports discovery of applications, roles, and features, using Azure Migrate: Server Assessment. App discovery is currently supported for VMware only. [Learn more](#) about the requirements and steps for setting up app discovery.

Typical app discovery errors are summarized in the table.

ERROR	CAUSE	ACTION
10000: "Unable to discover the applications installed on the server".	This might occur if the machine operating system isn't Windows or Linux.	Only use app discovery for Windows/Linux.
10001: "Unable to retrieve the applications installed the server".	Internal error - some missing files in appliance.	Contact Microsoft Support.
10002: "Unable to retrieve the applications installed the server".	The discovery agent on the appliance might not be working properly.	If the issue doesn't resolve itself within 24 hours, contact support.
10003 "Unable to retrieve the applications installed the server".	The discovery agent on the appliance might not be working properly.	If the issue doesn't resolve itself within 24 hours, contact support.
10004: "Unable to discover installed applications for <Windows/Linux> machines."	Credentials to access <Windows/Linux> machines weren't provided in the appliance.	Add a credential to the appliance that has access to the <Windows/Linux> machines.
10005: "Unable to access the on-premises server".	The access credentials might be wrong.	Update the appliance credentials make sure you can access the relevant machine with them.
10006: "Unable to access the on-premises server".	This might occur if the machine operating system isn't Windows or Linux.	Only use app discovery for Windows/Linux.
10007: "Unable to process the metadata retrieved"	This internal error occurred while trying to deserialize JSON	Contact Microsoft Support for a resolution
9000/9001/9002: "Unable to discover the applications installed on the server".	VMware tools might not be installed or is corrupted.	Install/reinstall VMware tools on the relevant machine, and check it's running.
9003: Unable to discover the applications installed on the server".	This might occur if the machine operating system isn't Windows or Linux.	Only use app discovery for Windows/Linux.
9004: "Unable to discover the applications installed on the server".	This might happen if the VM is powered off.	For discovery, make sure the VM is on.
9005: "Unable to discover the applications installed on the VM.	This might occur if the machine operating system isn't Windows or Linux.	Only use app discovery for Windows/Linux.
9006/9007: "Unable to retrieve the applications installed the server".	The discovery agent on the appliance might not be working properly.	If the issue doesn't resolve itself within 24 hours, contact support.

ERROR	CAUSE	ACTION
9008: "Unable to retrieve the applications installed the server".	Might be an internal error.	If the issue doesn't resolve itself within 24 hours, contact support.
9009: "Unable to retrieve the applications installed the server".	Can occur if the Windows User Account Control (UAC) settings on the server are restrictive, and prevent discovery of installed applications.	Search for 'User Account Control' settings on the server, and configure the UAC setting on the server to one of the lower two levels.
9010: "Unable to retrieve the applications installed the server".	Might be an internal error.	If the issue doesn't resolve itself within 24 hours, contact support.
9011: "File to download from guest is not found on the guest VM"	The issue can occur due to an internal error.	The issue should automatically get resolved in 24 hours. If the issue still persists, please contact Microsoft Support.
9012: "Result file contents are empty."	The issue can occur due to an internal error.	The issue should automatically get resolved in 24 hours. If the issue still persists, please contact Microsoft Support.
9013: "A new temporary profile is created for every login to the VMware VM"	A new temporary profile is created for every login into the VM	Ensure the user name provided in the guest VM credentials is in UPN format.
9015: "Unable to connect to VMware VMs due to insufficient privileges on vCenter"	Guest Operations role is not enabled on the vCenter user account	Ensure Guest Operations role is enabled on the vCenter user account.
9016: "Unable to connect to VMware VMs as the guest operations agent is out of data"	VMware tools is not properly installed or is not up to date.	Ensure the VMware tools is properly installed and up to date.
9017: "File with discovered metadata is not found on the VM."	The issue can occur due to an internal error.	Contact Microsoft Support for a resolution.
9018: "PowerShell is not installed in the Guest VMs."	PowerShell is not available in the guest VM.	Install PowerShell in the guest VM.
9019: "Unable to discover due to guest VM operation failures"	VMware guest operation failed on the VM.	Ensure that the VM credentials are valid and user name provided in the guest VM credentials is in UPN format.
9020: "File creation permission is denied."	The role associated to the user or the group policy is restricting the user to create the file in the folder	Check if the guest user provided has create permission for the file in the folder. See Notifications in Server Assessment for the name of the folder.
9021: "File create permission is denied in folder System Temp Path."	VMware tool version on the VM is unsupported	Upgrade your VMware tool version above 10.2.0.
9022: "Get WMI object access is denied."	The role associated to the user or the group policy is restricting the user to access WMI object.	Please contact Microsoft Support.

ERROR	CAUSE	ACTION
9023: "SystemRoot environment variable value is empty."	Not known	Please contact Microsoft Support.
9024: "TEMP environment variable value is empty."	Not known	Please contact Microsoft Support.
9025: "PowerShell is corrupt in the Guest VMs."	Not known	Reinstall PowerShell in the guest VM and check if PowerShell can be run on the guest VM.
8084: "Unable to discover applications due to VMware error."	The Azure Migrate appliance uses VMware APIs to discover applications. This issue can happen if an exception is thrown by vCenter Server while trying to discover applications. The fault message from VMware is displayed in the error message shown in portal.	Search for the message in the VMware documentation , and follow the steps to fix. If you can't fix, contact Microsoft support.

Next steps

Set up an appliance for [VMware](#), [Hyper-V](#), or [physical servers](#).

Troubleshoot assessment/dependency visualization

3/23/2020 • 10 minutes to read • [Edit Online](#)

This article helps you troubleshoot issues with assessment and dependency visualization with [Azure Migrate: Server Assessment](#).

Assessment readiness issues

Fix assessment readiness issues as follows:

ISSUE	FIX
Unsupported boot type	Azure doesn't support VMs with an EFI boot type. We recommend that you convert the boot type to BIOS before you run a migration. You can use Azure Migrate Server Migration to handle the migration of such VMs. It will convert the boot type of the VM to BIOS during the migration.
Conditionally supported Windows operating system	The operating system has passed its end-of-support date, and needs a Custom Support Agreement (CSA) for support in Azure . Consider upgrading before you migrate to Azure.
Unsupported Windows operating system	Azure supports only selected Windows OS versions . Consider upgrading the machine before you migrate to Azure.
Conditionally endorsed Linux OS	Azure endorses only selected Linux OS versions . Consider upgrading the machine before you migrate to Azure.
Unendorsed Linux OS	The machine might start in Azure, but Azure provides no operating system support. Consider upgrading to an endorsed Linux version before you migrate to Azure.
Unknown operating system	The operating system of the VM was specified as "Other" in vCenter Server. This behavior blocks Azure Migrate from verifying the Azure readiness of the VM. Make sure that the operating system is supported by Azure before you migrate the machine.
Unsupported bit version	VMs with a 32-bit operating systems might boot in Azure, but we recommended that you upgrade to 64-bit before you migrate to Azure.
Requires a Microsoft Visual Studio subscription	The machine is running a Windows client operating system, which is supported only through a Visual Studio subscription.
VM not found for the required storage performance	The storage performance (input/output operations per second [IOPS] and throughput) required for the machine exceeds Azure VM support. Reduce storage requirements for the machine before migration.

ISSUE	FIX
VM not found for the required network performance	The network performance (in/out) required for the machine exceeds Azure VM support. Reduce the networking requirements for the machine.
VM not found in the specified location	Use a different target location before migration.
One or more unsuitable disks	<p>One or more disks attached to the VM don't meet Azure requirements.^A</p> <p>Azure Migrate: Server Assessment currently doesn't support Ultra SSD disks, and assesses the disks based on the disk limits for premium managed disks (32 TB).</p> <p>For each disk attached to the VM, make sure that the size of the disk is < 64 TB (supported by Ultra SSD disks).</p> <p>If it isn't, reduce the disk size before you migrate to Azure, or use multiple disks in Azure and stripe them together to get higher storage limits. Make sure that the performance (IOPS and throughput) needed by each disk is supported by Azure managed virtual machine disks.</p>
One or more unsuitable network adapters.	Remove unused network adapters from the machine before migration.
Disk count exceeds limit	Remove unused disks from the machine before migration.
Disk size exceeds limit	<p>Azure Migrate: Server Assessment currently doesn't support Ultra SSD disks, and assesses the disks based on premium disk limits (32 TB).</p> <p>However, Azure supports disks with up to 64-TB size (supported by Ultra SSD disks). Shrink disks to less than 64 TB before migration, or use multiple disks in Azure and stripe them together to get higher storage limits.</p>
Disk unavailable in the specified location	Make sure the disk is in your target location before you migrate.
Disk unavailable for the specified redundancy	The disk should use the redundancy storage type defined in the assessment settings (LRS by default).
Could not determine disk suitability because of an internal error	Try creating a new assessment for the group.
VM with required cores and memory not found	Azure couldn't find a suitable VM type. Reduce the memory and number of cores of the on-premises machine before you migrate.
Could not determine VM suitability because of an internal error	Try creating a new assessment for the group.
Could not determine suitability for one or more disks because of an internal error	Try creating a new assessment for the group.

ISSUE	FIX
Could not determine suitability for one or more network adapters because of an internal error	Try creating a new assessment for the group.

Linux VMs are "conditionally ready"

Server Assessment marks Linux VMs as "Conditionally ready" due to a known gap in Server Assessment.

- The gap prevents it from detecting the minor version of the Linux OS installed on the on-premises VMs.
- For example, for RHEL 6.10, currently Server Assessment detects only RHEL 6 as the OS version.
- Because Azure endorses only specific versions of Linux, the Linux VMs are currently marked as conditionally ready in Server Assessment.
- You can determine whether the Linux OS running on the on-premises VM is endorsed in Azure by reviewing [Azure Linux support](#).
- After you've verified the endorsed distribution, you can ignore this warning.

Azure SKUs bigger than on-premises

Azure Migrate Server Assessment might recommend Azure VM SKUs with more cores and memory than current on-premises allocation based on the type of assessment:

- The VM SKU recommendation depends on the assessment properties.
- This is affected by the type of assessment you perform in Server Assessment: *Performance-based*, or *As on-premises*.
- For performance-based assessments, Server Assessment considers the utilization data of the on-premises VMs (CPU, memory, disk, and network utilization) to determine the right target VM SKU for your on-premises VMs. It also adds a comfort factor when determining effective utilization.
- For on-premises sizing, performance data is not considered, and the target SKU is recommended based on on-premises allocation.

To show how this can affect recommendations, let's take an example:

We have an on-premises VM with four cores and eight GB of memory, with 50% CPU utilization and 50% memory utilization, and a specified comfort factor of 1.3.

- If the assessment is *As on-premises*, an Azure VM SKU with four cores and 8 GB of memory is recommended.
- If the assessment is performance-based, based on effective CPU and memory utilization ($50\% \text{ of } 4 \text{ cores} * 1.3 = 2.6$ cores and $50\% \text{ of } 8\text{-GB memory} * 1.3 = 5.3\text{-GB memory}$), the cheapest VM SKU of four cores (nearest supported core count) and eight GB of memory (nearest supported memory size) is recommended.
- [Learn more](#) about assessment sizing.

Azure disk SKUs bigger than on-premises

Azure Migrate Server Assessment might recommend a bigger disk based on the type of assessment.

- Disk sizing in Server Assessment depends on two assessment properties: sizing criteria and storage type.
- If the sizing criteria is **Performance-based**, and the storage type is set to **Automatic**, the IOPS, and throughput values of the disk are considered when identifying the target disk type (Standard HDD, Standard SSD, or Premium). A disk SKU from the disk type is then recommended, and the recommendation considers the size requirements of the on-premises disk.
- If the sizing criteria is **Performance-based**, and the storage type is **Premium**, a premium disk SKU in Azure is recommended based on the IOPS, throughput, and size requirements of the on-premises disk. The same logic is

used to perform disk sizing when the sizing criteria is **As on-premises** and the storage type is **Standard HDD, Standard SSD, or Premium**.

As an example, if you have an on-premises disk with 32 GB of memory, but the aggregated read and write IOPS for the disk is 800 IOPS, Server Assessment recommends a premium disk (because of the higher IOPS requirements), and then recommends a disk SKU that can support the required IOPS and size. The nearest match in this example would be P15 (256 GB, 1100 IOPS). Even though the size required by the on-premises disk was 32 GB, Server Assessment recommends a larger disk because of the high IOPS requirement of the on-premises disk.

Utilized core/memory percentage missing

Server Assessment reports "PercentageOfCoresUtilizedMissing" or "PercentageOfMemoryUtilizedMissing" when the Azure Migrate appliance can't collect performance data for the relevant on-premises VMs.

- This can occur if the VMs are turned off during the assessment duration. The appliance can't collect performance data for a VM when it's turned off.
- If only the memory counters are missing and you're trying to assess Hyper-V VMs, check whether you have dynamic memory enabled on these VMs. There's a known issue for Hyper-V VMs only, in which an Azure Migrate appliance can't collect memory utilization data for VMs that don't have dynamic memory enabled.
- If any of the performance counters are missing, Azure Migrate Server Assessment falls back to the allocated cores and memory, and it recommends a corresponding VM size.
- If all of the performance counters are missing, ensure the port access requirements for assessment are met. Learn more about the port access requirements for [VMware](#), [Hyper-V](#) and [physical](#) server assessment.

Is the operating system license included?

Azure Migrate Server Assessment currently considers the operating system license cost only for Windows machines. License costs for Linux machines aren't currently considered.

How does performance-based sizing work?

Server Assessment continuously collects performance data of on-premises machines and uses it to recommend the VM SKU and disk SKU in Azure. [Learn how](#) performance-based data is collected.

Dependency visualization in Azure Government

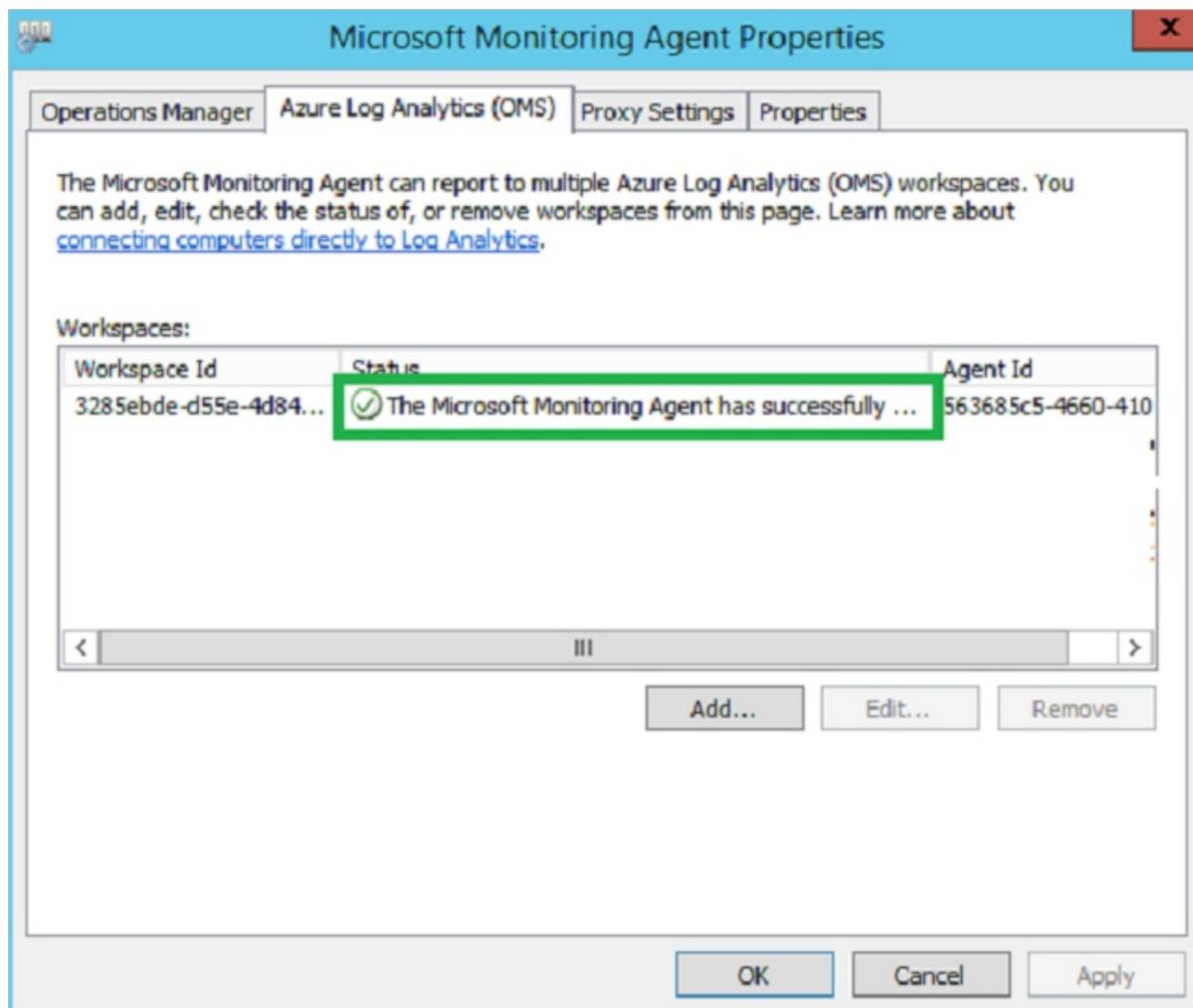
Azure Migrate depends on Service Map for the dependency visualization functionality. Because Service Map is currently unavailable in Azure Government, this functionality is not available in Azure Government.

Dependencies don't show after agent install

After you've installed the dependency visualization agents on on-premises VMs, Azure Migrate typically takes 15-30 minutes to display the dependencies in the portal. If you've waited for more than 30 minutes, make sure that the Microsoft Monitoring Agent (MMA) can connect to the Log Analytics workspace.

For Windows VMs:

1. In the Control Panel, start MMA.
2. In the **Microsoft Monitoring Agent properties > Azure Log Analytics (OMS)**, make sure that the **Status** for the workspace is green.
3. If the status isn't green, try removing the workspace and adding it again to MMA.



For Linux VMs, make sure that the installation commands for MMA and the dependency agent succeeded.

Supported operating systems

- **MMS agent:** Review the supported [Windows](#), and [Linux](#) operating systems.
- **Dependency agent:** the supported [Windows](#) and [Linux](#) operating systems.

Visualize dependencies for > hour

Although Azure Migrate allows you to go back to a particular date in the last month, the maximum duration for which you can visualize the dependencies is one hour.

For example, you can use the time duration functionality in the dependency map to view dependencies for yesterday, but you can view them for a one-hour period only.

However, you can use Azure Monitor logs to [query the dependency data](#) over a longer duration.

Visualized dependencies for > 10 machines

In Azure Migrate Server Assessment, you can [visualize dependencies for groups](#) with up to 10 VMs. For larger groups, we recommend that you split the VMs into smaller groups to visualize dependencies.

Machines show "Install agent"

After migrating machines with dependency visualization enabled to Azure, machines might show "Install agent" action instead of "View dependencies" due to the following behavior:

- After migration to Azure, on-premises machines are turned off and equivalent VMs are spun up in Azure. These

machines acquire a different MAC address.

- Machines might also have a different IP address, based on whether you've retained the on-premises IP address or not.
- If both MAC and IP addresses are different from on-premises, Azure Migrate doesn't associate the on-premises machines with any Service Map dependency data. In this case, it will show the option to install the agent rather than to view dependencies.
- After a test migration to Azure, on-premises machines remain turned on as expected. Equivalent machines spun up in Azure acquire different MAC address and might acquire different IP addresses. Unless you block outgoing Azure Monitor log traffic from these machines, Azure Migrate won't associate the on-premises machines with any Service Map dependency data, and thus will show the option to install agents, rather than to view dependencies.

Capture network traffic

Collect network traffic logs as follows:

1. Sign in to the [Azure portal](#).
2. Press F12 to start Developer Tools. If needed, clear the **Clear entries on navigation** setting.
3. Select the **Network** tab, and start capturing network traffic:
 - In Chrome, select **Preserve log**. The recording should start automatically. A red circle indicates that traffic is being captured. If the red circle doesn't appear, select the black circle to start.
 - In Microsoft Edge and Internet Explorer, recording should start automatically. If it doesn't, select the green play button.
4. Try to reproduce the error.
5. After you've encountered the error while recording, stop recording, and save a copy of the recorded activity:
 - In Chrome, right-click and select **Save as HAR with content**. This action compresses and exports the logs as a .har file.
 - In Microsoft Edge or Internet Explorer, select the **Export captured traffic** option. This action compresses and exports the log.
6. Select the **Console** tab to check for any warnings or errors. To save the console log:
 - In Chrome, right-click anywhere in the console log. Select **Save as**, to export, and zip the log.
 - In Microsoft Edge or Internet Explorer, right-click the errors and select **Copy all**.
7. Close Developer Tools.

Next steps

[Create](#) or [customize](#) an assessment.