**Migrate on-premises machines to Azure**

Migrate on-premises VMs and physical servers to Azure. You learn how to:

* Set up the source and 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 one-time failover to Azure

**Before you start**

Note that devices exported by paravirtualized drivers aren't supported.

**Prepare Azure and on-premises**

* Prepare Azure as described in [this article](https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-prepare-azure). Although this article describes preparation steps for disaster recovery, the steps are also valid for migration.
* Prepare on-premises [VMware](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-tutorial-prepare-on-premises) or [Hyper-V](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-prepare-on-premises-tutorial) servers. If you're migrating physical machines, you don't need to prepare anything. Just verify the [support matrix](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-physical-azure-support-matrix).

**Select a protection goal**

Select what you want to replicate, and where you want to replicate to.

* Click **Recovery Services vaults** > vault.
* In the Resource Menu, click **Site Recovery** > **Prepare Infrastructure** > **Protection goal**.
* In **Protection goal**, select what you want to migrate.
* **VMware**: Select **To Azure** > **Yes, with VMWare vSphere Hypervisor**.
* **Physical machine**: Select **To Azure** > **Not virtualized/Other**.
* **Hyper-V**: Select **To Azure** > **Yes, with Hyper-V**. If Hyper-V VMs are managed by VMM, select **Yes**.

**Set up the source environment**

|  |  |
| --- | --- |
| **Scenario** | **Details** |
| VMware | Set up the [source environment](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-set-up-source), and set up the [configuration server](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-deploy-configuration-server). |
| Physical machine | [Set up](https://docs.microsoft.com/en-us/azure/site-recovery/physical-azure-set-up-source) the source environment and configuration server. |
| Hyper-V | Set up the [source environment](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial)  Set up the [source environment](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-azure-tutorial) for Hyper-V deployed with System Center VMM. |

**Set up the target environment**

Select and verify target resources.

* Click **Prepare infrastructure** > **Target**, and select the Azure subscription you want to use.
* Specify the Resource Manager deployment model.
* Site Recovery checks the Azure resources.
* If you're migrating VMware VMs or physical servers, Site Recovery verifies you have an Azure network in which the Azure VMs will be located when they're created after failover.
* If you're migrating Hyper-V VMs, Site Recovery verifies you have a compatible Azure storage account and network.
* If you're migrating Hyper-V VMs managed by System Center VMM, set up [network mapping](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-azure-tutorial).

**Set up a replication policy**

|  |  |
| --- | --- |
| **Scenario** | **Details** |
| VMware | Set up a [replication policy](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-set-up-replication) for VMware VMs. |
| Physical machine | Set up a [replication policy](https://docs.microsoft.com/en-us/azure/site-recovery/physical-azure-disaster-recovery) for physical machines. |
| Hyper-V | Set up a [replication policy](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial)  Set up a [replication policy](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-azure-tutorial) for Hyper-V deployed with System Center VMM. |

**Enable replication**

|  |  |
| --- | --- |
| **Scenario** | **Details** |
| VMware | [Enable replication](https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-enable-replication) for VMware VMs. |
| Physical machine | [Enable replication](https://docs.microsoft.com/en-us/azure/site-recovery/physical-azure-disaster-recovery) for physical machines. |
| Hyper-V | [Enable replication](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-tutorial)  [Enable replication](https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-vmm-azure-tutorial) for Hyper-V deployed with System Center VMM. |

**Run a test migration**

Run a [test failover](https://docs.microsoft.com/en-us/azure/site-recovery/tutorial-dr-drill-azure) to Azure, to make sure everything's working as expected.

**Migrate to Azure**

Run a failover for the machines you want to migrate.

* In **Settings** > **Replicated items** click the machine > **Failover**.
* In **Failover** select a **Recovery Point** to fail over to. Select the latest recovery point.
* The encryption key setting isn't relevant for this scenario.
* Select **Shut down machine before beginning failover**. Site Recovery will attempt to shutdown virtual machines before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
* Check that the Azure VM appears in Azure as expected.
* In **Replicated items**, right-click the VM > **Complete Migration**. This does the following:
* Finishes the migration process, stops replication for the on-premises VM, and stops Site Recovery billing for the VM.
* This step cleans up the replication data. It doesn't delete the migrated VMs.



**After migration**

After machines are migrated to Azure, there are a number of steps you should complete.

Some steps can be automated as part of the migration process using the in-built automation scripts capability in [recovery plans](https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-runbook-automation)

**Post-migration steps 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.
* The [Azure VM agent](https://docs.microsoft.com/azure/virtual-machines/extensions/agent-windows) manages VM interaction with the Azure Fabric Controller. It's required for some Azure services, such as Azure Backup, Site Recovery, and Azure Security.
* If you're migrating VMware machines and physical servers, the Mobility Service installer installs available Azure VM agent on Windows machines. On Linux VMs, we recommend that you install the agent after failover.
* If you’re migrating Azure VMs to a secondary region, the Azure VM agent must be provisioned on the VM before the migration.
* If you’re migrating Hyper-V VMs to Azure, install the Azure VM agent on the Azure VM after the migration.
* Manually remove any Site Recovery provider/agent from the VM. If you migrate VMware VMs or physical servers, uninstall the Mobility service from the VM.
* For increased resilience:
* Keep data secure by backing up Azure VMs using the Azure Backup service. [Learn more](https://docs.microsoft.com/azure/backup/quick-backup-vm-portal).
* Keep workloads running and continuously available by replicating Azure VMs to a secondary region with Site Recovery. [Learn more](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-quickstart).
* For increased security:
* Lock down and limit inbound traffic access with Azure Security Center [Just in time administration](https://docs.microsoft.com/azure/security-center/security-center-just-in-time)
* Restrict network traffic to management endpoints with [Network Security Groups](https://docs.microsoft.com/azure/virtual-network/security-overview).
* Deploy [Azure Disk Encryption](https://docs.microsoft.com/azure/security/azure-security-disk-encryption-overview) to help secure disks, and keep data safe from theft and unauthorized access.
* Read more about [securing IaaS resources](https://azure.microsoft.com/services/virtual-machines/secure-well-managed-iaas/), and visit the [Azure Security Center](https://azure.microsoft.com/services/security-center/).
* For monitoring and management:
* Consider deploying [Azure Cost Management](https://docs.microsoft.com/azure/cost-management/overview) to monitor resource usage and spending.

**Post-migration steps 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