**Move Azure VMs to another region**

There are various scenarios in which you'd want to move your existing Azure IaaS virtual machines (VMs) from one region to another. For example, you want to improve reliability and availability of your existing VMs, to improve manageability, or to move for governance reasons.

* Verify prerequisites for the move
* Prepare the source VMs and the target region
* Copy the data and enable replication
* Test the configuration and perform the move
* Delete the resources in the source region

## Prerequisites

* Make sure that the Azure VMs are in the Azure region from which you want to move.
* Verify that your choice of [source region - target region combination is supported](https://docs.microsoft.com/azure/site-recovery/azure-to-azure-support-matrix#region-support), and make an informed decision about the target region.
* Make sure that you understand the [scenario architecture and components](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-architecture).
* Review the [support limitations and requirements](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-support-matrix).
* Verify account permissions. If you created your free Azure account, you're the administrator of your subscription. If you're not the subscription administrator, work with the administrator to assign the permissions that you need. To enable replication for a VM and essentially copy data by using Azure Site Recovery, you must have:
  + Permissions to create a VM in Azure resources. The Virtual Machine Contributor built-in role has these permissions, which include:
  + Permission to create a VM in the selected resource group
  + Permission to create a VM in the selected virtual network
  + Permission to write to the selected storage account
  + Permissions to manage Azure Site Recovery operations. The Site Recovery Contributor role has all the permissions that are required to manage Site Recovery operations in a Recovery Services vault.
* Make sure that all the latest root certificates are on the Azure VMs that you want to move. If the latest root certificates aren't on the VM, security constraints will prevent the data copy to the target region.
* For Windows VMs, install all the latest Windows updates on the VM, so that all the trusted root certificates are on the machine. In a disconnected environment, follow the standard Windows Update and certificate update processes for your organization.
* For Linux VMs, follow the guidance provided by your Linux distributor to get the latest trusted root certificates and certificate revocation list on the VM.
* Make sure that you're not using an authentication proxy to control network connectivity for VMs that you want to move.
* If the VM that you're trying to move doesn't have access to the internet, or it's using a firewall proxy to control outbound access, [check the requirements](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-enable-replication#set-up-outbound-network-connectivity-for-vms).
* Identify the source networking layout and all the resources that you're currently using. This includes but isn't limited to load balancers, network security groups (NSGs), and public IPs.
* Verify that your Azure subscription allows you to create VMs in the target region that's used for disaster recovery. Contact support to enable the required quota.
* Make sure that your subscription has enough resources to support VMs with sizes that match your source VMs. If you're using Site Recovery to copy data to the target, Site Recovery chooses the same size or the closest possible size for the target VM.
* Make sure that you create a target resource for every component that's identified in the source networking layout. This step is important to ensure that your VMs have all the functionality and features in the target region that you had in the source region.
* To create the most commonly used network resources that are relevant for you based on the source VM configuration, see the following documentation:
  + [Network security groups](https://docs.microsoft.com/azure/virtual-network/manage-network-security-group)
  + [Load balancers](https://docs.microsoft.com/azure/load-balancer)
  + [Public IP](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-public-ip-address)
  + For any other networking components, see the [networking documentation](https://docs.microsoft.com/azure/#pivot=products&panel=network).

## Prepare

The following steps shows how to prepare the virtual machine for the move using Azure Site Recovery as a solution.

### Create the vault in any region, except the source region

1. Sign in to the [Azure portal](https://portal.azure.com/) > **Recovery Services**.
2. Select **Create a resource** > **Management Tools** > **Backup and Site Recovery**.
3. In **Name**, specify the friendly name **ContosoVMVault**. If you have more than one subscription, select the appropriate one.
4. Create the resource group **ContosoRG**.
5. Specify an Azure region. To check supported regions, see geographic availability in [Azure Site Recovery pricing details](https://azure.microsoft.com/pricing/details/site-recovery/).
6. In **Recovery Services vaults**, select **Overview** > **ContosoVMVault** > **+Replicate**.
7. In **Source**, select **Azure**.
8. In **Source location**, select the source Azure region where your VMs are currently running.
9. Select the Resource Manager deployment model. Then select the **Source subscription** and **Source resource group**.
10. Select **OK** to save the settings.

### Enable replication for Azure VMs and start copying the data

Site Recovery retrieves a list of the VMs that are associated with the subscription and resource group.

1. In the next step, select the VM that you want to move, then select **OK**.
2. In **Settings**, select **Disaster recovery**.
3. In **Configure disaster recovery** > **Target region**, select the target region to which you'll replicate.
4. For this tutorial, accept the other default settings.
5. Select **Enable replication**. This step starts a job to enable replication for the VM.

## Move

The following steps shows how to perform the move to the target region.

1. Go to the vault. In **Settings** > **Replicated items**, select the VM, and then select **Failover**.
2. In **Failover**, select **Latest**.
3. Select **Shut down machine before beginning failover**. Site Recovery attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails. You can follow the failover progress on the **Jobs** page.
4. After the job is finished, check that the VM appears in the target Azure region as expected.

## Discard

In case you checked the moved VM and need to make changed to point of failover or want to go back to a previous point, in the **Replicated items**, right-select the VM > **Change recovery point**. This step provides you the option to specify a different recovery point and failover to that one.

## Commit

Once you have checked the moved VM and are ready to commit the change, in the **Replicated items**, right-select the VM > **Commit**. This step finishes the move process to the target region. Wait until the commit job finishes.

## Clean up

The following steps will guide you through how to clean up the source region as well as related resources that were used for the move.

For all resources that were used for the move:

* Go to the VM. Select **Disable Replication**. This step stops the process from copying the data for the VM

If you have no plans to reuse any of the source resources, complete these additional steps:

1. Delete all the relevant network resources in the source region that you identified in [prerequisites](https://docs.microsoft.com/en-us/azure/site-recovery/azure-to-azure-tutorial-migrate#prerequisites).
2. Delete the corresponding storage account in the source region.