**Tutorial: Connect to a storage account using an Azure Private Endpoint**

* 09/25/2020
* 5 minutes to read
  + [](https://github.com/asudbring)
  + [](https://github.com/DCtheGeek)

Azure Private endpoint is the fundamental building block for Private Link in Azure. It enables Azure resources, like virtual machines (VMs), to communicate with Private Link resources privately.

In this tutorial, you learn how to:

* Create a virtual network and bastion host.
* Create a virtual machine.
* Create storage account with a private endpoint.
* Test connectivity to storage account private endpoint.

If you don't have an Azure subscription, create a [free account](https://azure.microsoft.com/free/?WT.mc_id=A261C142F) before you begin.

**Prerequisites**

* An Azure subscription

**Sign in to Azure**

Sign in to the [Azure portal](https://portal.azure.com/).

**Create a virtual network and bastion host**

In this section, you'll create a virtual network, subnet, and bastion host.

The bastion host will be used to connect securely to the virtual machine for testing the private endpoint.

1. On the upper-left side of the screen, select **Create a resource > Networking > Virtual network** or search for **Virtual network** in the search box.
2. In **Create virtual network**, enter or select this information in the **Basics** tab:

| **TABLE 1** | |
| --- | --- |
| **Setting** | **Value** |
| **Project Details** |  |
| Subscription | Select your Azure subscription |
| Resource Group | Select **myResourceGroup** |
| **Instance details** |  |
| Name | Enter **myVNet** |
| Region | Select **East US** |

1. Select the **IP Addresses** tab or select the **Next: IP Addresses** button at the bottom of the page.
2. In the **IP Addresses** tab, enter this information:

| **TABLE 2** | |
| --- | --- |
| **Setting** | **Value** |
| IPv4 address space | Enter **10.1.0.0/16** |

1. Under **Subnet name**, select the word **default**.
2. In **Edit subnet**, enter this information:

| **TABLE 3** | |
| --- | --- |
| **Setting** | **Value** |
| Subnet name | Enter **mySubnet** |
| Subnet address range | Enter **10.1.0.0/24** |

1. Select **Save**.
2. Select the **Security** tab.
3. Under **BastionHost**, select **Enable**. Enter this information:

| **TABLE 4** | |
| --- | --- |
| **Setting** | **Value** |
| Bastion name | Enter **myBastionHost** |
| AzureBastionSubnet address space | Enter **10.1.1.0/24** |
| Public IP Address | Select **Create new**. For **Name**, enter **myBastionIP**. Select **OK**. |

1. Select the **Review + create** tab or select the **Review + create** button.
2. Select **Create**.

**Create a virtual machine**

In this section, you'll create a virtual machine that will be used to test the private endpoint.

1. On the upper-left side of the portal, select **Create a resource** > **Compute** > **Virtual machine** or search for **Virtual machine** in the search box.
2. In **Create a virtual machine**, type or select the values in the **Basics** tab:

| **TABLE 5** | |
| --- | --- |
| **Setting** | **Value** |
| **Project Details** |  |
| Subscription | Select your Azure subscription |
| Resource Group | Select **myResourceGroup** |
| **Instance details** |  |
| Virtual machine name | Enter **myVM** |
| Region | Select **East US** |
| Availability Options | Select **No infrastructure redundancy required** |
| Image | Select **Windows Server 2019 Datacenter - Gen1** |
| Azure Spot instance | Select **No** |
| Size | Choose VM size or take default setting |
| **Administrator account** |  |
| Username | Enter a username |
| Password | Enter a password |
| Confirm password | Reenter password |

1. Select the **Networking** tab, or select **Next: Disks**, then **Next: Networking**.
2. In the Networking tab, select or enter:

| **TABLE 6** | |
| --- | --- |
| **Setting** | **Value** |
| **Network interface** |  |
| Virtual network | **myVNet** |
| Subnet | **mySubnet** |
| Public IP | Select **None**. |
| NIC network security group | **Basic** |
| Public inbound ports | Select **None**. |

1. Select **Review + create**.
2. Review the settings, and then select **Create**.

**Note**

Azure provides an ephemeral IP for Azure Virtual Machines which aren't assigned a public IP address, or are in the backend pool of an internal Basic Azure Load Balancer. The ephemeral IP mechanism provides an outbound IP address that isn't configurable.

The ephemeral IP is disabled when a public IP address is assigned to the virtual machine or the virtual machine is placed in the backend pool of a Standard Load Balancer with or without outbound rules. If a [**Azure Virtual Network NAT**](https://docs.microsoft.com/en-us/azure/virtual-network/nat-overview) gateway resource is assigned to the subnet of the virtual machine, the ephemeral IP is disabled.

For more information on outbound connections in Azure, see [**Using Source Network Address Translation (SNAT) for outbound connections**](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections).

**Create storage account with a private endpoint**

In this section, you'll create a storage account and configure the private endpoint.

1. In the left-hand menu, select **Create a resource** > **Storage** > **Storage account**, or search for **Storage account** in the search box.
2. In the **Basics** tab of **Create storage account** enter or select the following information:

| **TABLE 7** | |
| --- | --- |
| **Setting** | **Value** |
| **Project Details** |  |
| Subscription | Select your Azure subscription |
| Resource Group | Select **myResourceGroup** |
| **Instance details** |  |
| Storage account name | Enter **mystorageaccount**. If the name is unavailable, enter a unique name. |
| Location | Select **East US** |
| Performance | Leave the default **Standard** |
| Account kind | Leave the default **Storage (general purpose v2)** |
| Replication | Leave the default **Read-access geo-redundant storage (RA-GRS)** |

1. Select the **Networking** tab or select the **Next: Networking** button.
2. In the **Networking** tab, under **Connectivity method** select **Private endpoint**.
3. In **Private endpoint**, select **+ Add**.
4. In **Create private endpoint** enter or select the following information:

| **TABLE 8** | |
| --- | --- |
| **Setting** | **Value** |
| Subscription | Select your Azure subscription |
| Resource Group | Select **myResourceGroup** |
| Location | Select **East US** |
| Name | Enter **myPrivateEndpoint** |
| Storage subresource | Leave the default **blob** |
| **Networking** |  |
| Virtual network | Select **myVNet** |
| Subnet | Select **mySubnet** |
| **Private DNS integration** |  |
| Integrate with private DNS zone | Leave the default **Yes** |
| Private DNS Zone | Leave the default (New) privatelink.blob.core.windows.net |

1. Select **OK**.
2. Select **Review + create**.
3. Select **Create**.
4. Select **Resource groups** in the left-hand navigation pane.
5. Select **myResourceGroup**.
6. Select the storage account you created in the previous steps.
7. In the **Settings** section of the storage account, select **Access keys**.
8. Select copy on the **Connection string** for **key1**.

**Test connectivity to private endpoint**

In this section, you'll use the virtual machine you created in the previous step to connect to the storage account across the private endpoint.

1. Select **Resource groups** in the left-hand navigation pane.
2. Select **myResourceGroup**.
3. Select **myVM**.
4. On the overview page for **myVM**, select **Connect** then **Bastion**.
5. Select the blue **Use Bastion** button.
6. Enter the username and password that you entered during the virtual machine creation.
7. Open Windows PowerShell on the server after you connect.
8. Enter nslookup <storage-account-name>.blob.core.windows.net. Replace **<storage-account-name>** with the name of the storage account you created in the previous steps. You'll receive a message similar to what is displayed below:

PowerShellCopy

Server: UnKnown

Address: 168.63.129.16

Non-authoritative answer:

Name: mystorageaccount8675.privatelink.blob.core.windows.net

Address: 10.1.0.5

Aliases: mystorageaccount8675.blob.core.windows.net

A private IP address of **10.1.0.5** is returned for the storage account name. This address is in the subnet of the virtual network you created previously.

1. Install [Microsoft Azure Storage Explorer](https://docs.microsoft.com/en-us/azure/vs-azure-tools-storage-manage-with-storage-explorer?tabs=windows&toc=/azure/storage/blobs/toc.json) on the virtual machine.
2. Select **Finish** after the **Microsoft Azure Storage Explorer** is installed. Leave the box checked to open the application.
3. In the **Connect to Azure Storage** screen, select **Use a connection string**.
4. Select **Next**.
5. Enter your storage account name from the previous steps in **Display name**.
6. In the box under **Connection String**, paste the connection string from the storage account you copied in the previous steps.
7. Select **Next**.
8. Verify the settings are correct in **Connection Summary**.
9. Select **Connect**.
10. Close the connection to **myVM**.

**Clean up resources**

If you're not going to continue to use this application, delete the virtual network, virtual machine, and storage account with the following steps:

1. From the left-hand menu, select **Resource groups**.
2. Select **myResourceGroup**.
3. Select **Delete resource group**.
4. Enter **myResourceGroup** in **TYPE THE RESOURCE GROUP NAME**.
5. Select **Delete**.