

Exercise - Setup a secure Azure Virtual Network

5 minutes

An [Azure Virtual Network \(VNet\)](#) is similar to a traditional network but with the added benefits provided by Azure infrastructure.

VNets enable your resources, such as virtual machines (VMs) and ML workspaces, to securely communicate with each other and other networks or the internet.

A Machine Learning engineer can use them in a variety of scenarios, such as linking a VM to data stored on-premises, restricting access to a training API so that only personnel from their lab can see it, or exposing an inference endpoint to the internet.

In this exercise, we'll create a VNet and use it to secure access the workspace we created in the previous exercise. While this exercise gives an intuition about the mechanics of securing a workspace, this is not a complete solution. Refer to the documentation linked at the end of the exercise for complete instructions.

⚠ Warning

This exercise will only give a basic intuition as to the process involved in securing an ML workspace's network environment. For complete step-by-step process for a production environment, follow the link at the end of this exercise.

⚠ Warning

This exercise will block access to the affected workspace and should not be performed on a production workspace.

Prerequisites

- Basic knowledge of networking concepts.
- An Azure account and a subscription.
- A resource group Azure Machine Learning Workspace as created in the previous exercise.

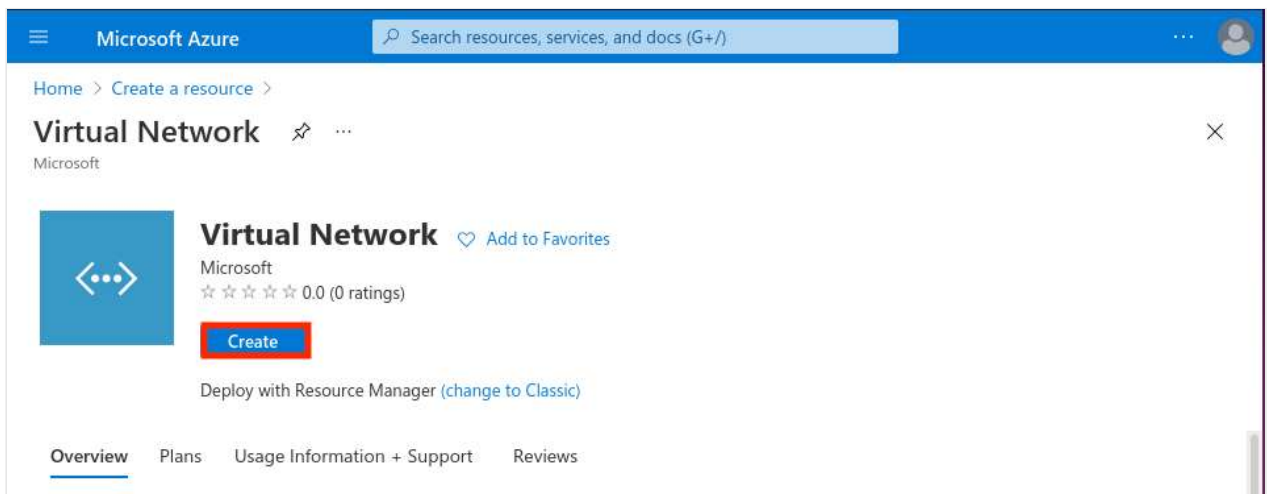
Sign in to Azure

Sign in to the [Azure portal](#) .

Create a VNet

Let's create a VNet for this exercise:

1. In the Azure portal, Select **Create a resource** in the upper left-hand corner of the portal.
2. In the search box, enter **Virtual Network**. Select **Virtual Network** in the search results.
3. In the **Virtual Network** page, select **Create**.



4. In **Create virtual network**, enter or select this information in the **Basics** tab:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Create a resource > Marketplace > Virtual Network >

Create virtual network

BasicsIP AddressesSecurityTagsReview + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

Project details

Subscription * ⓘ

Microsoft Partner Network

Resource group * ⓘ

MLResourceGroup

Create new

Instance details

Name *

MLVNet

Region *

(US) East US

Review + create


< Previous

Next : IP Addresses >

[Download a template for automation](#)

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Enter MLResourceGroup (or the name of the Resource Group you created in the previous exercise)
Instance details	
Name	Enter MLVNet .
Region	Select (US) East US .

5. Select the **IP Addresses** tab, or select the **Next: IP Addresses** button at the bottom of the page.

 **Tip**

If your screen comes with the IPv4 address space and *default* subnet setup like in the image below, skip to step 9.

The screenshot shows the 'Create virtual network' page in the Microsoft Azure portal, specifically the 'IP Addresses' tab. The page has a blue header with the Microsoft Azure logo and a search bar. Below the header, there's a breadcrumb trail: Home > Create a resource > Marketplace > Virtual Network >. The main title is 'Create virtual network' with a close button (X) in the top right corner. The 'IP Addresses' tab is selected, and the 'Review + create' tab is also visible. The page content includes a description of the virtual network's address space, a text input field for the IPv4 address space (currently showing '10.1.0.0/16' and '10.1.0.0 - 10.1.255.255 (65536 addresses)'), and a checkbox to 'Add IPv6 address space'. Below this, there's a description of the subnet's address range and a table for subnets. The table has columns for 'Subnet name', 'Subnet address range', and 'NAT gateway'. A single subnet named 'default' is listed with the address range '10.1.0.0/24' and no NAT gateway. At the bottom, there's a 'Review + create' button, a '< Previous' button, a 'Next : Security >' button, and a 'Download a template for automation' link.

Microsoft Azure Search resources, services, and docs (G+/)

Home > Create a resource > Marketplace > Virtual Network >

Create virtual network

Basics **IP Addresses** Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.1.0.0/16 10.1.0.0 - 10.1.255.255 (65536 addresses)

☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

<input type="checkbox"/> Subnet name	Subnet address range	NAT gateway
<input type="checkbox"/> default	10.1.0.0/24	-

i Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more >](#)

Review + create < Previous Next : Security > [Download a template for automation](#)

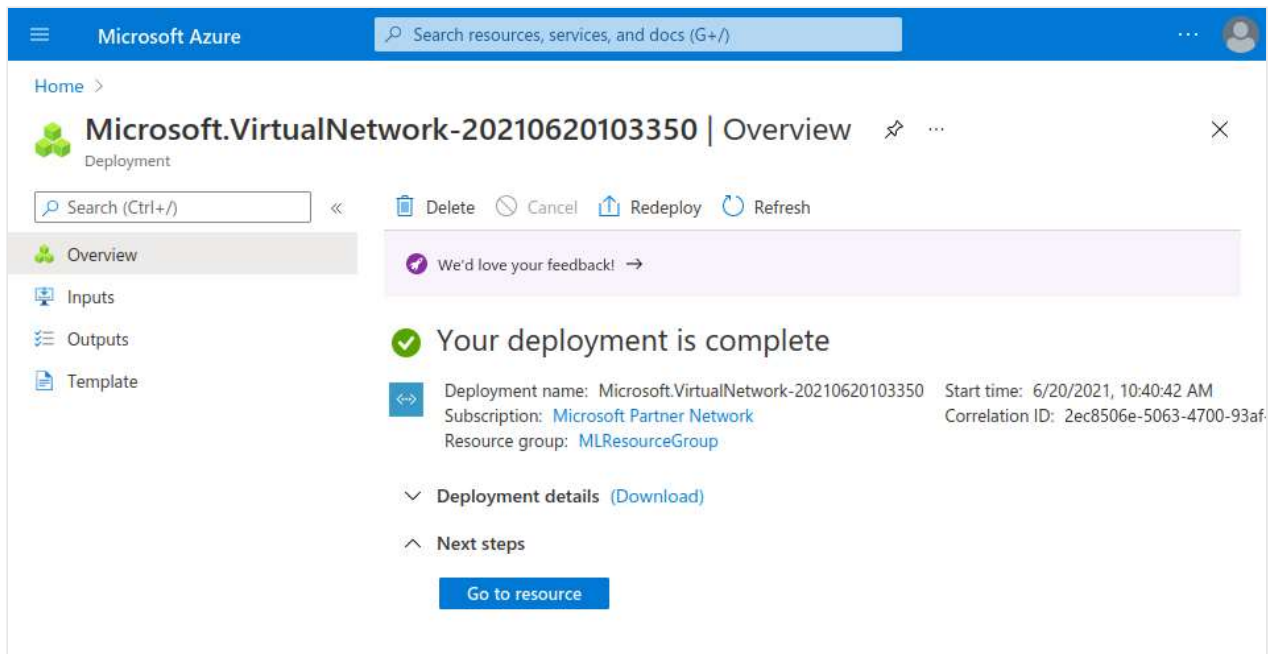
6. In **IPv4 address space**, select the existing address space and change it to **10.1.0.0/16**.

7. Select **+ Add subnet**, then enter **default** for **Subnet name** and **10.1.0.0/24** for **Subnet address range**.

8. Select **Add**.

9. Select the **Review + create** tab or select the **Review + create** button.

10. Select **Create** and wait a few moments for the deployment to finish:



❗ Important

For simplicity, we are creating a single subnet for our Virtual Network. A subnet is a range of IP addresses in the VNet. We could split a VNet into multiple subnets for organization and security, for example, a *training* subnet that only Data Scientists could use, and an *inference* subnet that is publicly available.

Testing workspace access

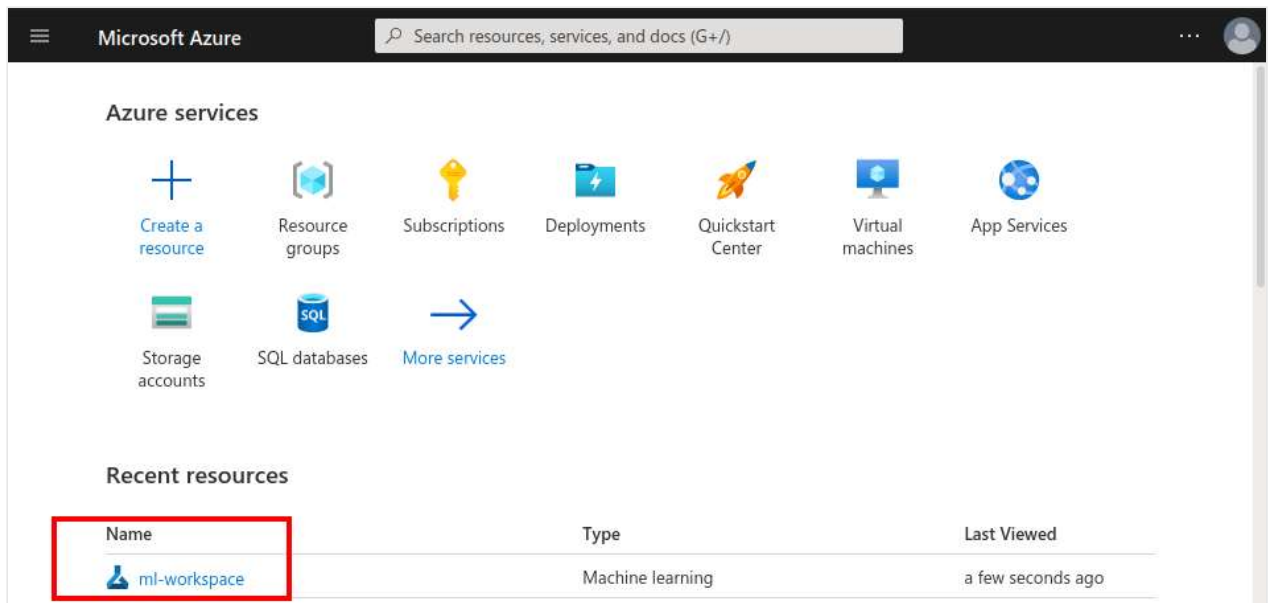
We just added a VNet to our resource group, but is it restricting access to our **ml-workspace**?

We can test that using [Azure Machine Learning Studio](#) to access the contents of the workspace.

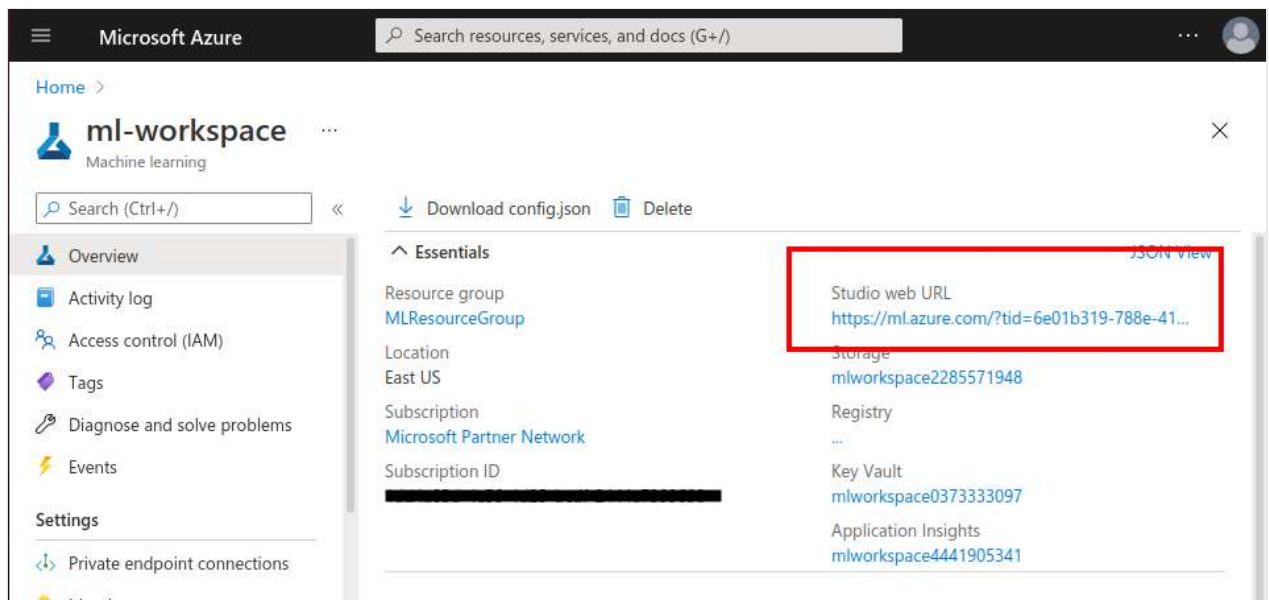
💡 Tip

The Azure Machine Learning Workspace is a web portal with high-level tools for model training, deployment, and asset management.

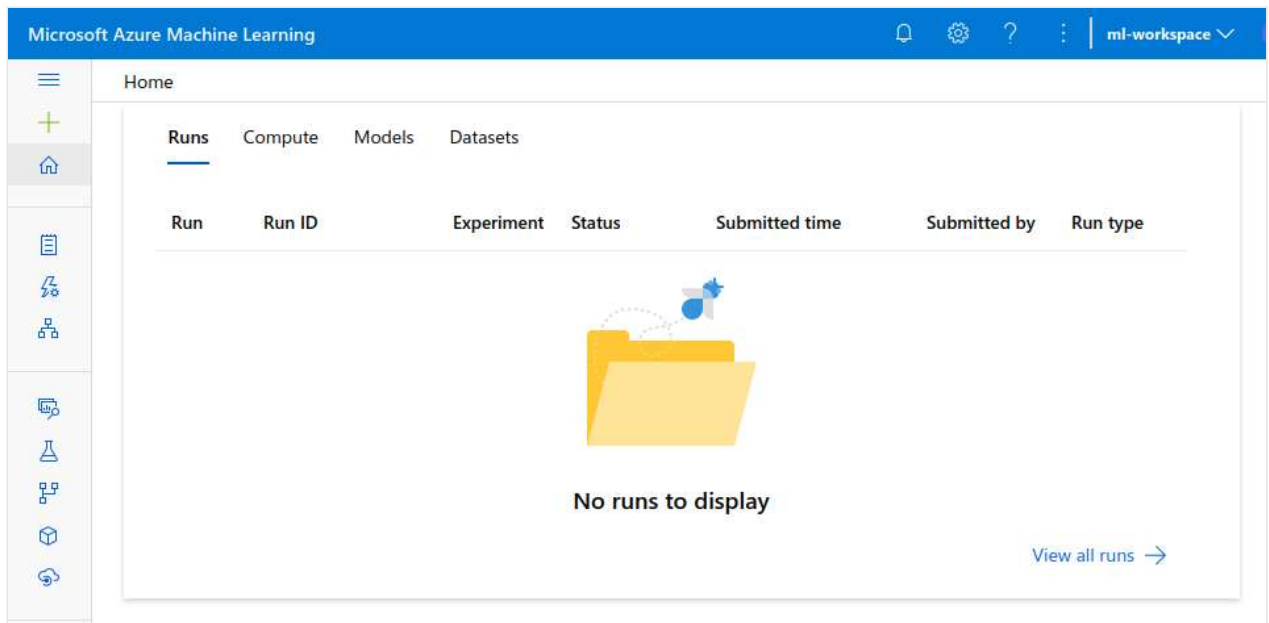
1. Select **Home** to go back to the home page
2. Select the **ml-workspace** in the list of recent resources:



3. Select the **Studio web URL** for your workspace:



4. Azure Machine Learning Studio should open in a new tab or window. Scroll down until you can see the tabs below (Runs, Compute, Models, and Datasets):



Each tab above represents a "folder" that stores the resources you and your team would use in Machine Learning.

Although you probably don't have any objects there yet, like in the image above, there should be no warnings or error messages, meaning that there's no network access restrictions on those resources yet.

Secure network access to the ML Workspace

So far we've created two independent resources:

- An ML workspace (**ml-workspace**)
- A VNet (**MLVNet**)

We now have to connect these two so that the workspace network traffic has to go through our VNet. In other words, we want our workspace available **only** to resources that are connected to the **MLVNet** virtual network.

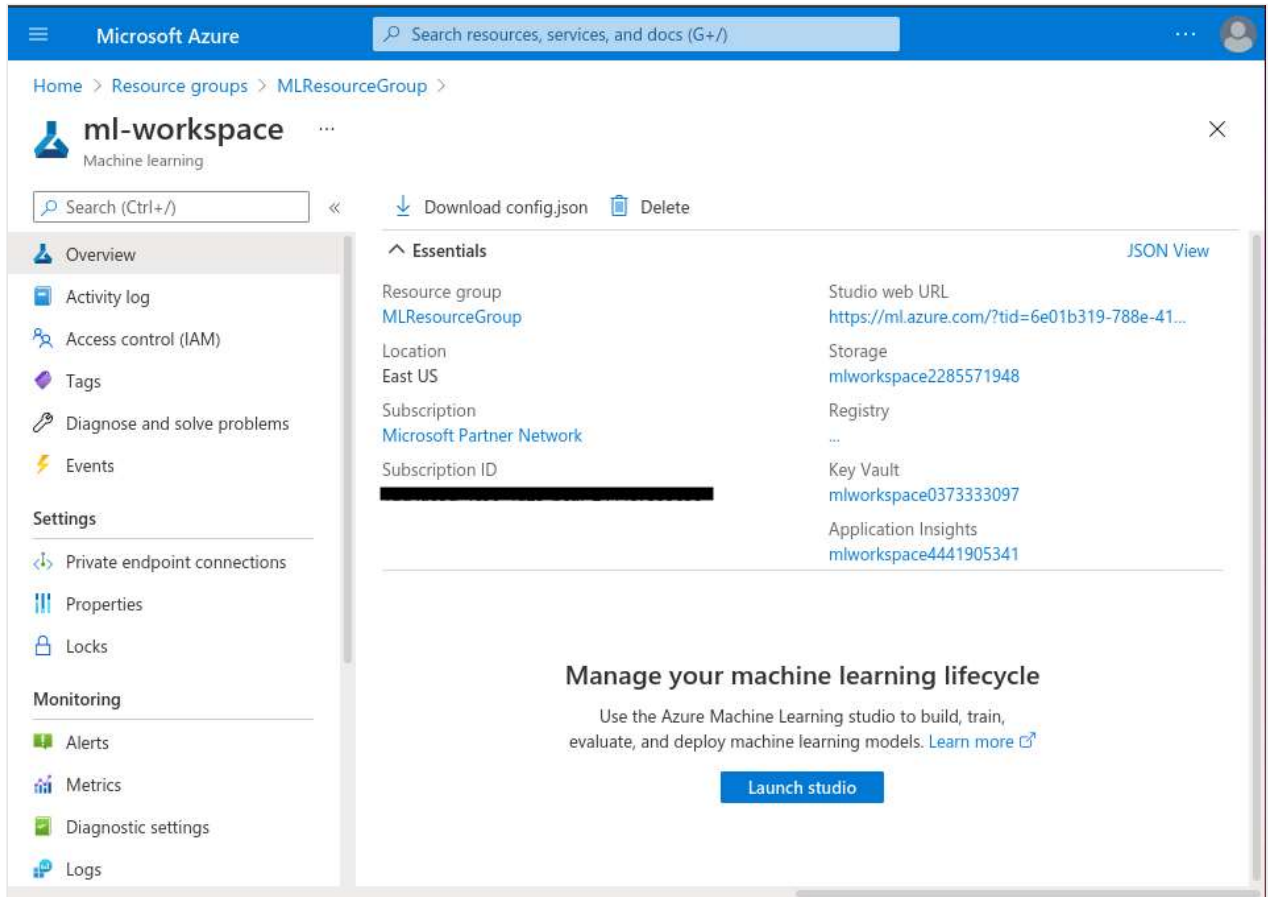
To accomplish that, we need to define a [Private Endpoint](#) for the *ml-workspace* resource.

💡 Tip

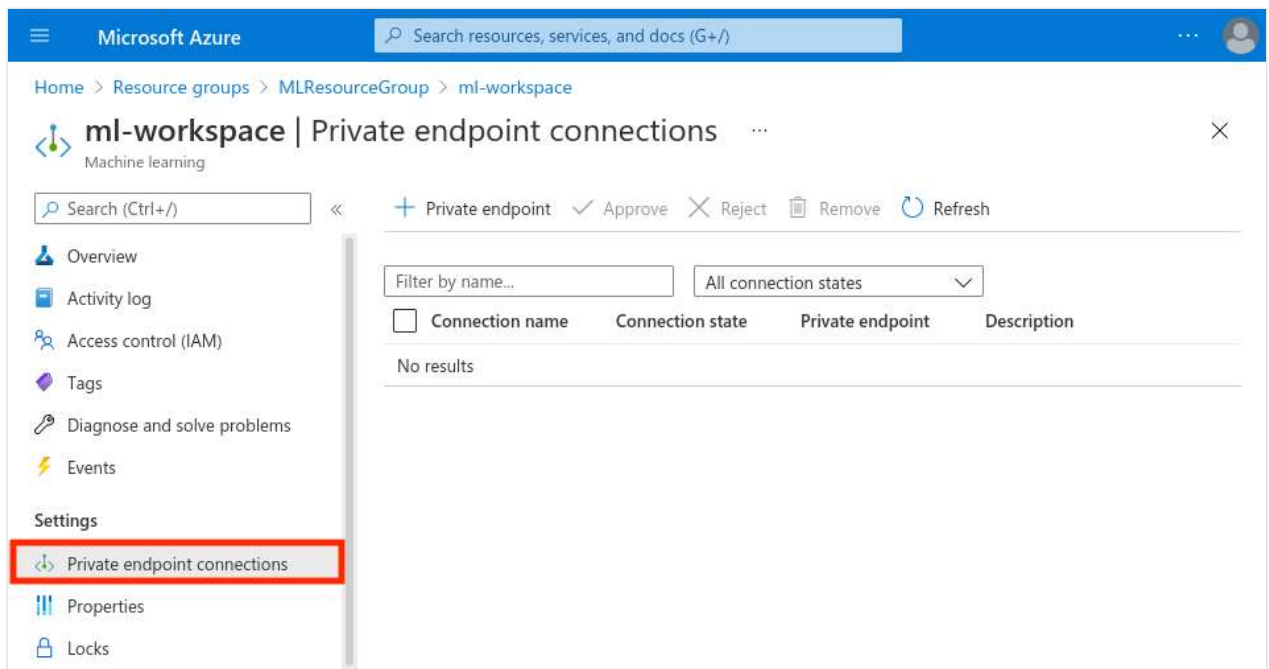
A Private Endpoint is a network interface that uses a private IP Address from your VNet to create secure and private connections to a resource.

Create a Private Endpoint

1. Go to "Home", select **Resource Groups**, select the **MLResourceGroup** resource group, and then select your **ml_workspace** workspace:



2. In the left-hand menu, select **Private endpoint connections**:



3. Select **Private Endpoint** and fill the form with the following values:

Microsoft Azure

Search resources, services, and docs (G+)

...

Home > Resource groups > MLResourceGroup > ml-workspace >

Create a private endpoint ...

X

1 Basics2 Resource3 Configuration4 Tags5 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * ⓘ

Microsoft Partner Network

Resource group * ⓘ

MLResourceGroup

Create new

Instance details

Name *

MLPrivateEndpoint

Region *

(US) East US

< Previous

Next : Resource >

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Enter MLResourceGroup (or the name of the Resource Group you created in the previous exercise)
Instance details	
Name	Enter MLPrivateEndpoint .
Region	Select (US) East US .

4. Select the **Next: Resource >** button.
5. In the **Resource** tab, use the values below

Home > Resource groups > MLResourceGroup > ml-workspace >

Create a private endpoint

✓ Basics 2 Resource 3 Configuration 4 Tags 5 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Connection method ① ☒ Connect to an Azure resource in my directory. ☐ Connect to an Azure resource by resource ID or alias.

Subscription * ①

Resource type * ①

⚠ A Machine Learning Workspace can only have one private endpoint connection; all resources with an existing connection are excluded from the dropdown.

Resource * ①

Target sub-resource * ①

< Previous Next : Configuration >

Setting	Value
Project details	
Subscription	Select your subscription.
Resource type	Enter Microsoft.MachineLearningService/workspaces
Instance details	
Resource *	Select ml-workspace .
Target subresource	Select amlworkspace .

6. Select the **Next: Configuration >** button.

Leave the suggested defaults:

Microsoft Azure

Search resources, services, and docs (G+ /)

...

Home > ml-workspace >

Create a private endpoint ...

✕

✓ Basics

✓ Resource

3 Configuration

4 Tags

5 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ⓘ

MLVNet

Subnet * ⓘ

default (10.1.0.0/24)

ⓘ If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone

☒ Yes ☐ No

Configuration name

Subscription

Private DNS zone

Review + create

< Previous

Next : Tags >

Setting	Value
Virtual Network *	MLVNet
Subnet *	default (10.1.0.0/24)
Integrate with private DNS zone	Yes

7. Select **Review + Create** to validate the deployment, then select **Create** to deploy the endpoint (this can take a few moments):

Microsoft Azure

Search resources, services, and docs (G+)

Home > ml-workspace >

Create a private endpoint

✓ Basics ✓ Resource **3 Configuration** ④ Tags ⑤ Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network * ① MLVNet

Subnet * ① default (10.10.0/24)

i If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone ☒ Yes ☐ No

Configuration name	Subscription	Private DNS zone
--------------------	--------------	------------------

[Review + create](#) [< Previous](#) [Next : Tags >](#)

Testing the network configuration

We can make sure our workspace is inside the VNet now by testing if we still have access to its resources:

1. Reload the Azure Machine Learning Studio window (or [open the Studio](#) again):

2. As the warning shows, access to those resources is now blocked. That happens because your workspace is now inside the VNet, and it's configured to block all requests that don't originate from within the *default* subnet we created (remember we're trying to access it from the **outside** of the network perimeter).

Secured but inaccessible

You've just secured the network access to your ML workspace.

Notice that in the same way you can't access it, neither can any other resources in your organization that aren't part of the subnet.

Opening things up so that resources can connect requires some strategic planning!

We recommend reading our [how to secure a workspace using a vnet](#) guide for more in-depth reference.

Summary

In this unit you've covered the following topics:

- What a Virtual Network is and some of its uses
- Creating an Azure Virtual Network
- Creating subnets in a Virtual Network
- How to use Private Endpoints to secure network access to your Machine Learning workspaces
- Accessing a workspace using Azure Machine Learning Studio and check if resources are blocked

Next unit: Knowledge check

[Continue >](#)

How are we doing? ☆ ☆ ☆ ☆ ☆