Tutorial: Set up lab to lab communication with advanced networking

Article • 08/29/2023

ⓘ **Important**

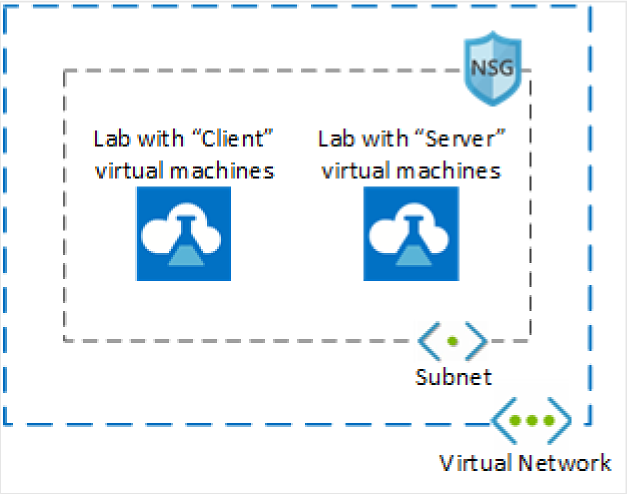
Azure Lab Services will be retired on June 28, 2027. For more information, see the retirement guide .

ⓘ **Note**

This article references features available in lab plans, which replaced lab accounts.

Azure Lab Services advanced networking enables you to control the network for labs created using lab plans. You can use advanced networking to implement various scenarios including connecting to licensing servers, using hub-spoke model for Azure Networking, or lab to lab communication. In this tutorial, you set up lab-to-lab communication for a web development class.

After you complete this tutorial, you'll have a lab with two lab virtual machines that are able to communicate with each other: a server VM and a client VM.


NSG
Lab with "Client" virtual machines
Lab with "Server" virtual machines
Subnet
Virtual Network

Learn more about the supported networking scenarios in Azure Lab Services.

In this tutorial, you learn how to:

- ✓ Create a resource group
- ✓ Create a virtual network and subnet
- ✓ Delegate subnet to Azure Lab Services

- ✓ Create a network security group
- ✓ Update the network security group inbound rules
- ✓ Associate the network security group to virtual network
- ✓ Create a lab plan using advanced networking
- ✓ Create two labs
- ✓ Enable ICMP on the templates VMs
- ✓ Publish both labs
- ✓ Test communication between lab VMs

Prerequisites

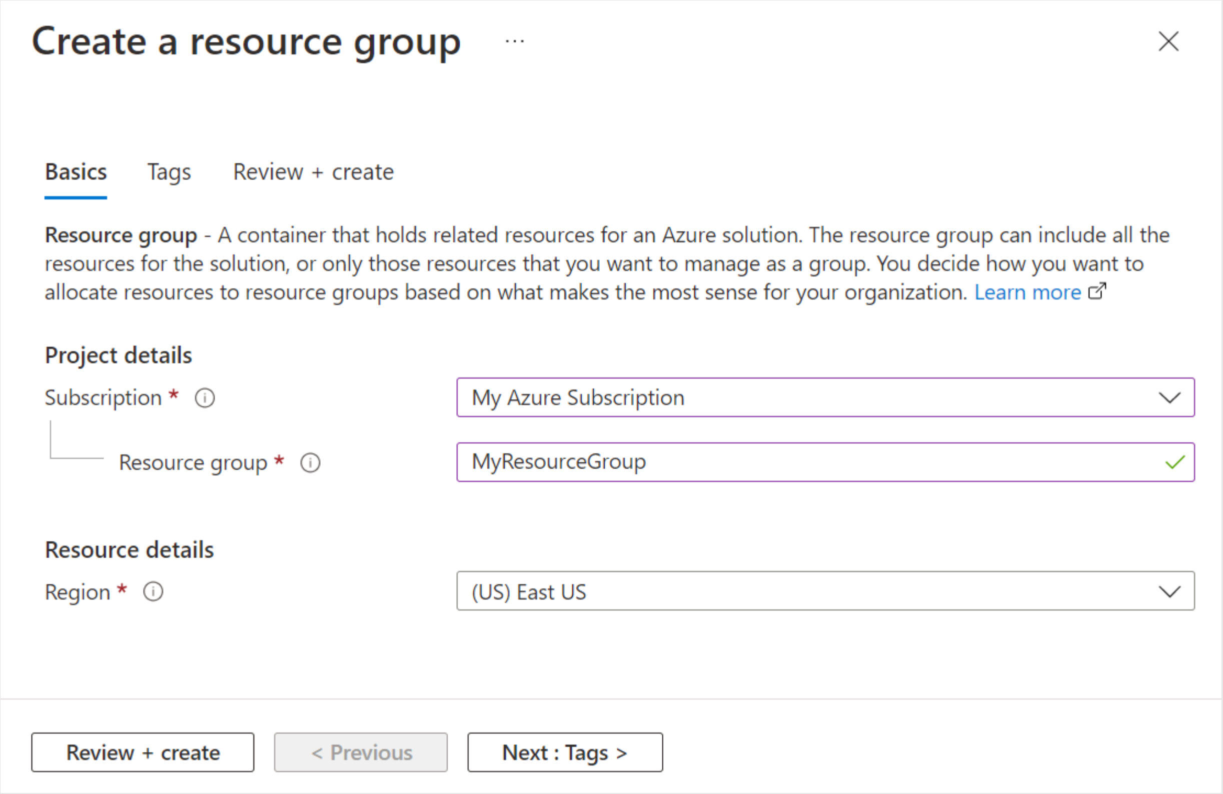
- An Azure account with an active subscription. If you don't have an Azure subscription, create a free account before you begin.
- An Azure account with permission to create and manage resources in the subscription, such as the Contributor or Owner Azure RBAC role.

Create a resource group

A resource group is a logical container into which Azure resources, such as web apps, databases, and storage accounts, are deployed and managed. For example, you can choose to delete the entire resource group in one simple step later.

The following steps show how to use the Azure portal to create a resource group. For simplicity, you create all resources for this tutorial in the same resource group.

1. Sign in to the Azure portal .
2. Select **Resource groups**.
3. Select **+ Create** from the top menu.
4. On the **Basics** tab of the **Create a resource group** page, do the following actions:
   a. For **Subscription**, choose the subscription in which you want to create your labs.
   b. For **Resource group**, type **MyResourceGroup**.
   c. For **Region**, select the region closest to you. For more information about available regions, see Azure geographies .



Create a resource group

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. Learn more

Project details

Subscription * : My Azure Subscription

Resource group * : MyResourceGroup

Resource details

Region * : (US) East US

5. Select **Review + Create**.
6. Review the summary, and select **Create**.

Create a virtual network and subnet

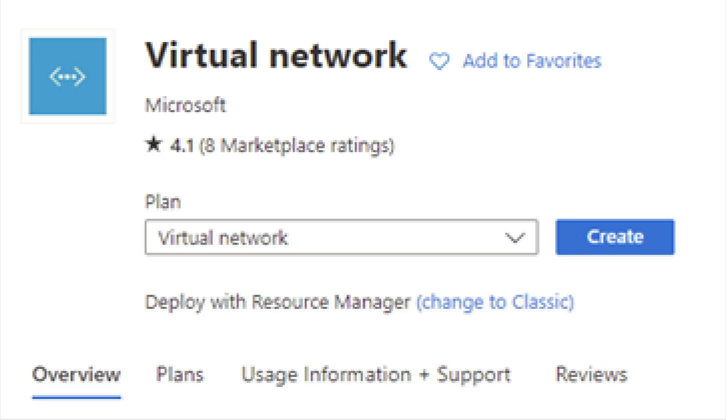
The following steps show how to use the Azure portal to create a virtual network and subnet that can be used with Azure Lab Services.

> **Important**
>
> When using Azure Lab Services with advanced networking, the virtual network, subnet, lab plan and lab must all be in the same region. For more information about which regions are supported by various products, see Azure products by region .

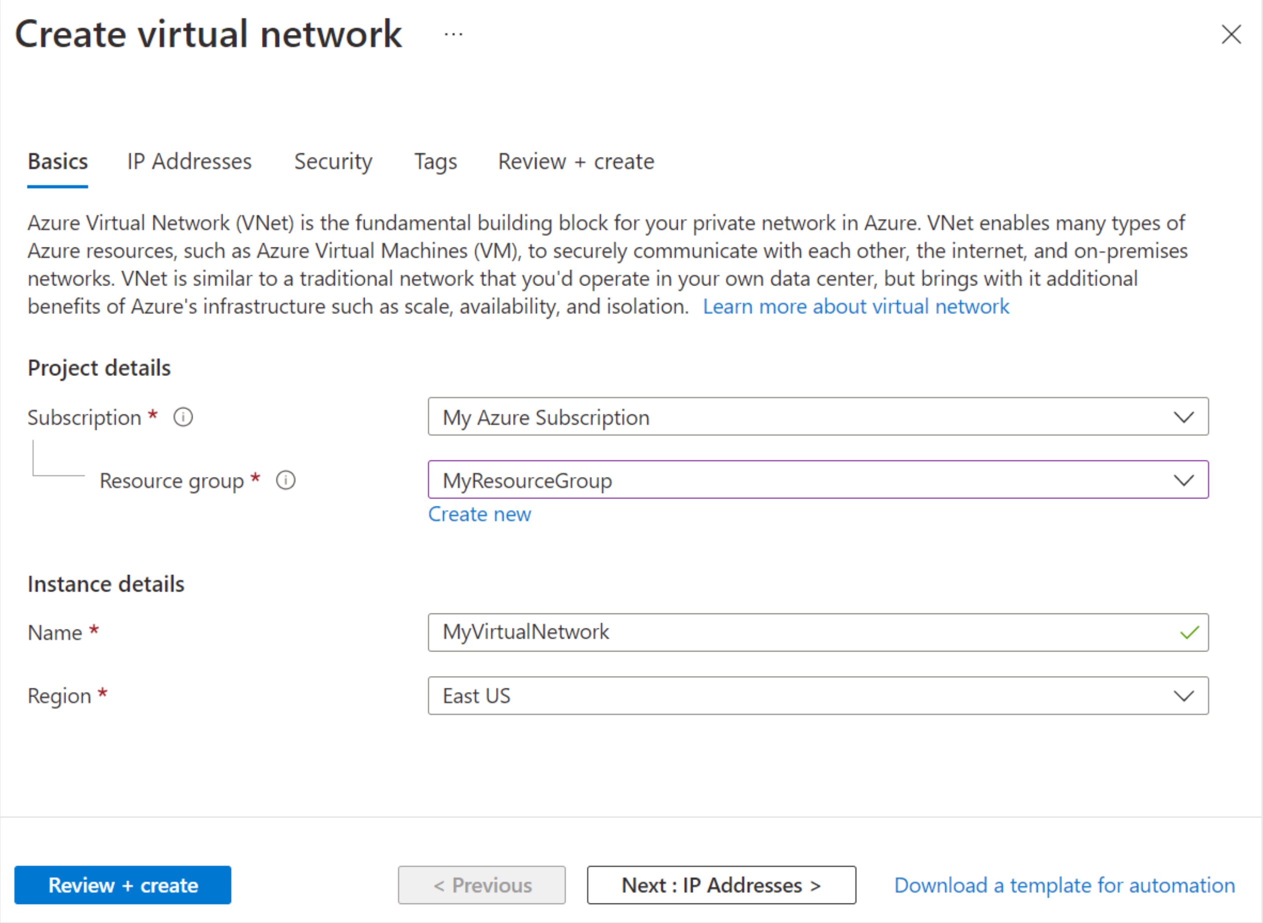
1. Open **MyResourceGroup** created previously.

2. Select + **Create** in the upper left corner of the Azure portal and search for "virtual network".

3. Select the **Virtual network** tile and then select **Create**.


Virtual network
Add to Favorites
Microsoft
★ 4.1 (8 Marketplace ratings)
Plan
Virtual network
Create
Deploy with Resource Manager (change to Classic)
Overview
Plans
Usage Information + Support
Reviews

4. On the **Basics** tab of the **Create virtual network**, do the following actions:
   a. For **Subscription**, choose the same subscription as the resource group.
   b. For **Resource group**, choose **MyResourceGroup**.
   c. For **Name**, enter **MyVirtualNetwork**.
   d. For **Region**, choose region that is also supported by Azure Lab Services. For more information about supported regions, see Azure Lab Services by region .
   e. Select **Next: IP Addresses**.


Create virtual network

Basics | IP Addresses | Security | Tags | Review + 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 * : My Azure Subscription

Resource group * : MyResourceGroup

Create new

Instance details

Name * : MyVirtualNetwork

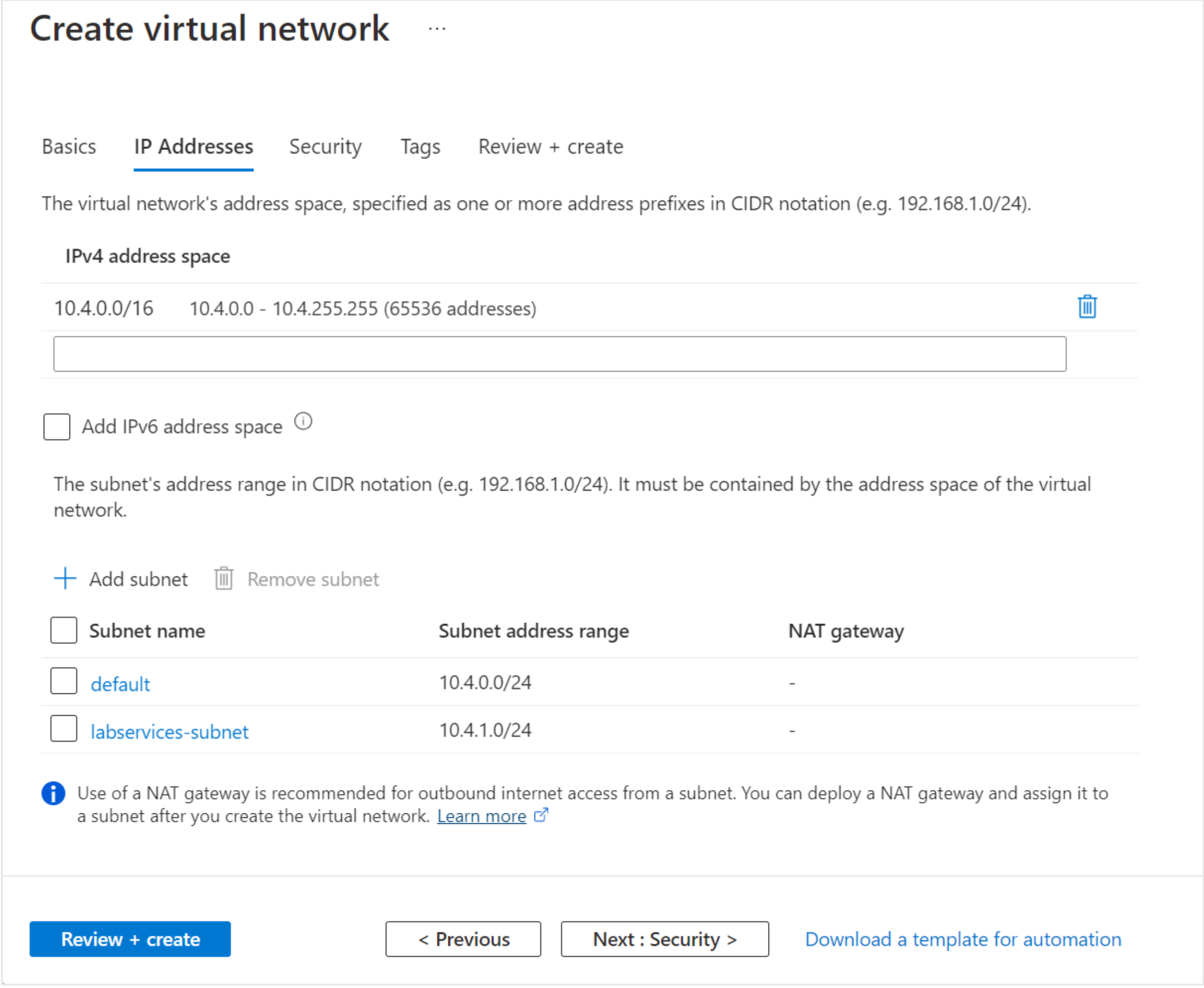
Region * : East US

5. On the **IP Addresses** tab, create a subnet that is used by the labs.
   a. Select + **Add subnet**
   b. For **Subnet name**, enter **labservices-subnet**.

   c. For **Subnet address range**, enter range in CIDR notation. For example, 10.0.1.0/24 has enough IP addresses for 251 lab VMs. (Azure reserves five IP addresses for every subnet.) To create a subnet with more available IP addresses for VMs, use a different CIDR prefix length. For example, 10.0.0.0/20 would have room for over 4000 IP addresses for lab VMs. For more information about adding subnets, see Add a subnet.

   d. Select **OK**.

6. Select **Review + Create**.



Create virtual network

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	
10.4.0.0/16	10.4.0.0 - 10.4.255.255 (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.

□ Subnet name	Subnet address range	NAT gateway
□ default	10.4.0.0/24	-
□ labservices-subnet	10.4.1.0/24	-

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

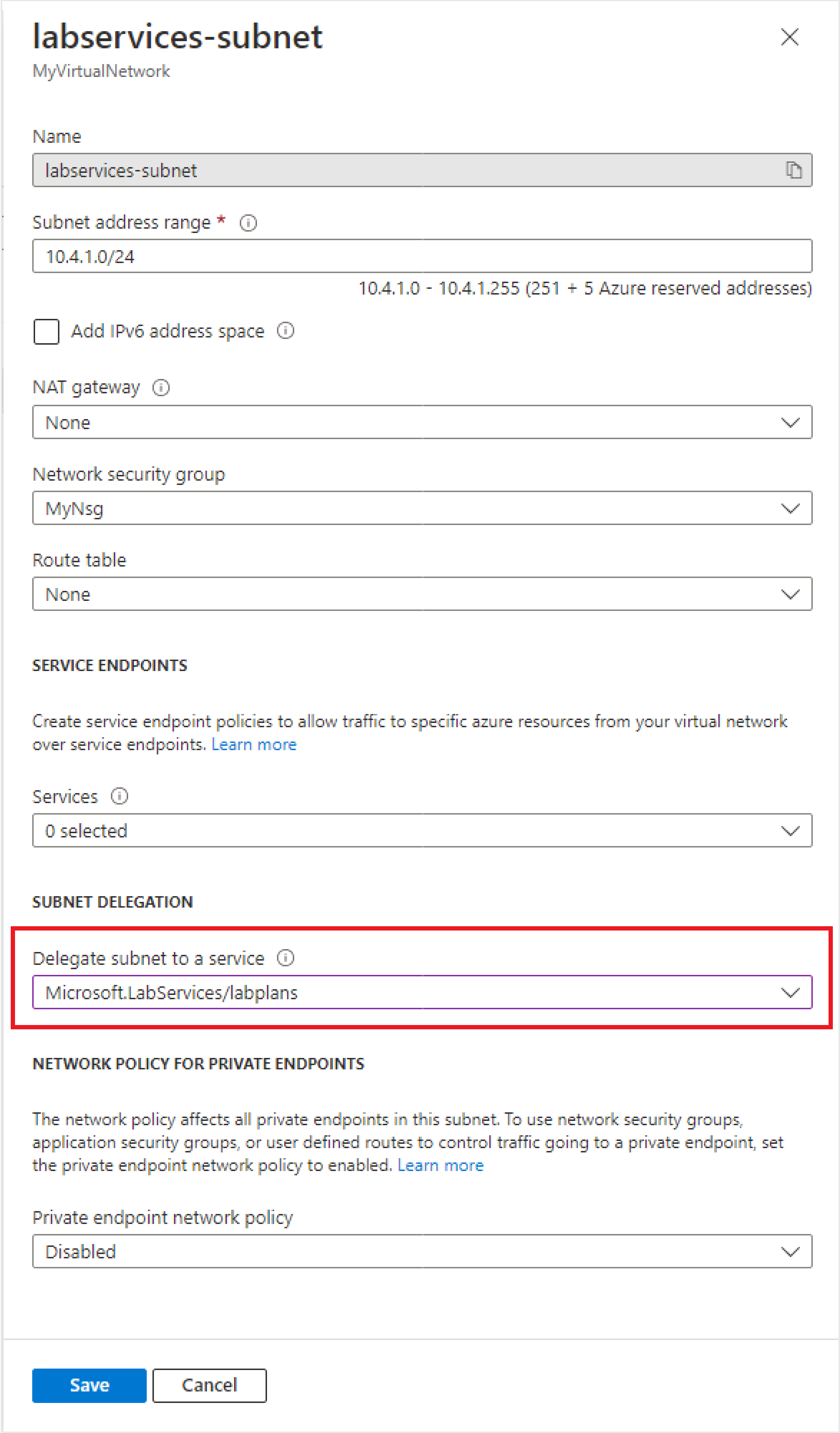
7. Once validation passes, select **Create**.

Delegate subnet to Azure Lab Services

Next, you configure the subnet to be used with Azure Lab Services. To use a subnet with Azure Lab Services, the subnet must be delegated to the service.

1. Open the **MyVirtualNetwork** resource.
2. Select the **Subnets** item on the left menu.
3. Select **labservices-subnet** subnet.

4. Under the **Subnet delegation** section, select **Microsoft.LabServices/labplans** for the **Delegate subnet to a service** setting.
5. Select **Save**.



labservices-subnet

MyVirtualNetwork

Name

labservices-subnet

Subnet address range *

10.4.1.0/24

10.4.1.0 - 10.4.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway

None

Network security group

MyNsg

Route table

None

SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more

Services

0 selected

SUBNET DELEGATION

Delegate subnet to a service

Microsoft.LabServices/labplans

NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. Learn more

Private endpoint network policy

Disabled

Create a network security group

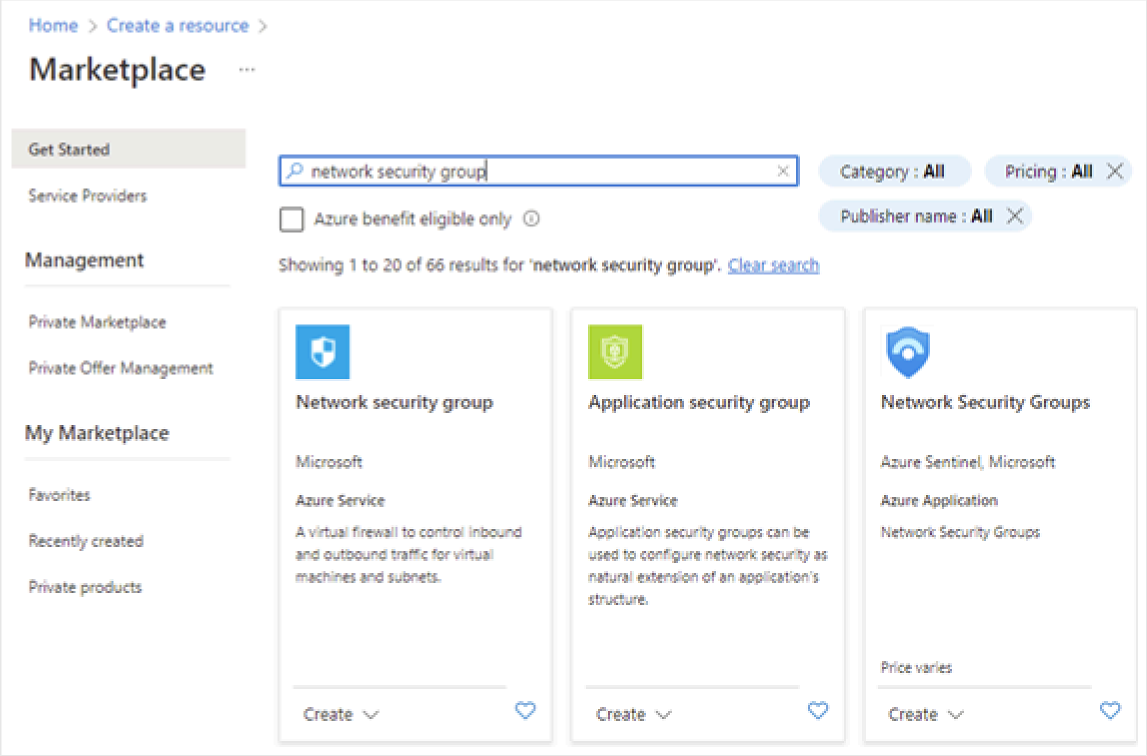
You can use an NSG to control traffic to one or more virtual machines (VMs), role instances, network adapters (NICs), or subnets in your virtual network. An NSG contains access control rules that allow or deny traffic based on traffic direction, protocol, source address and port, and destination address and port. The rules of an NSG can be changed at any time, and changes are applied to all associated instances.

For more information about NSGs, visit what is an NSG.

An NSG is required when using advanced networking in Azure Lab Services.

To create an NSG, complete the following steps:

1. Select **+ Create a Resource** in the upper left corner of the Azure portal and search for "network security group".



network security group

Category : All | Pricing : All | Publisher name : All

□ Azure benefit eligible only

Showing 1 to 20 of 66 results for 'network security group'. Clear search

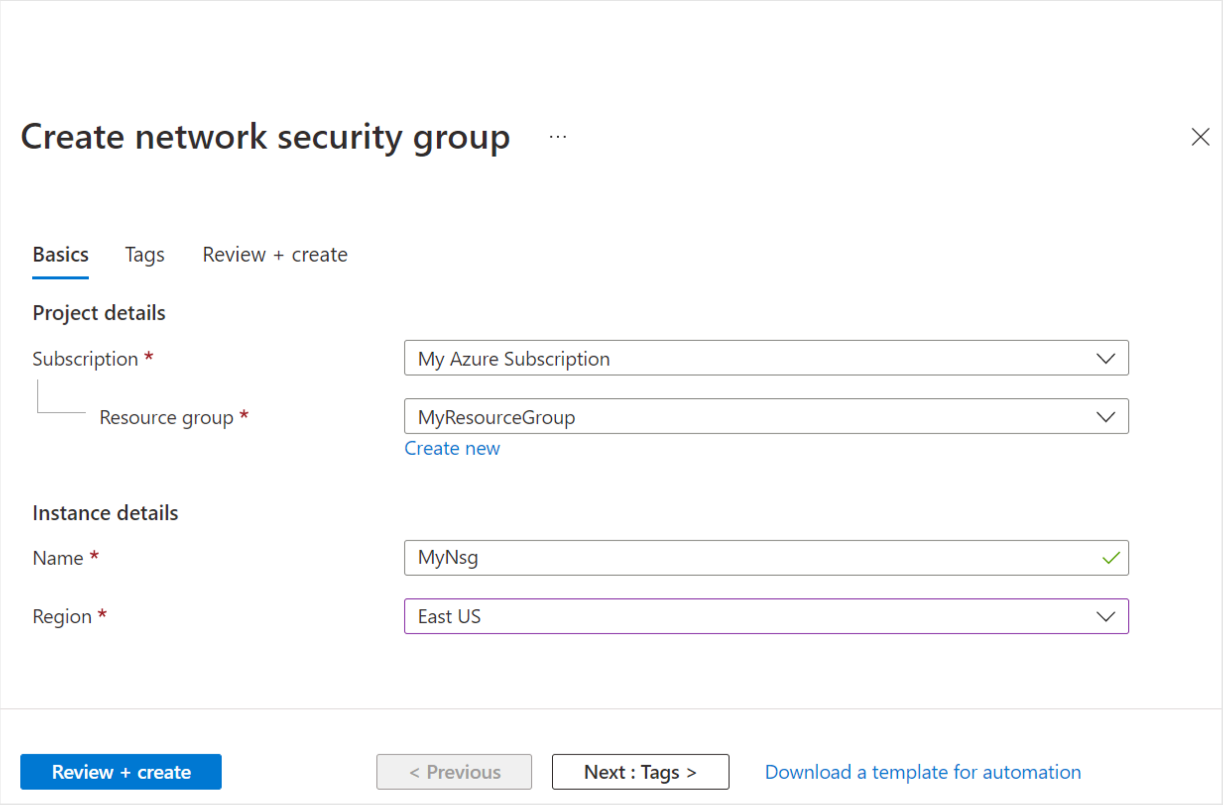
Network security group
Microsoft
Azure Service
A virtual firewall to control inbound and outbound traffic for virtual machines and subnets.

Application security group
Microsoft
Azure Service
Application security groups can be used to configure network security as natural extension of an application's structure.

Network Security Groups
Azure Sentinel, Microsoft
Azure Application
Network Security Groups
Price varies

2. Select the **Network security group** tile and then select **Create**.
3. On the **Basics** tab, of the **Create network security group**, do the following actions:
   a. For **Subscription**, choose the same subscription as used previously.
   b. For **Resource group**, choose **MyResourceGroup**.
   c. For the **Name**, enter **MyNsg**.
   d. For **Region**, choose same region as **MyVirtualNetwork** that was created previously.

e. Select **Review + Create**.



Create network security group

Project details

Subscription * My Azure Subscription

Resource group * MyResourceGroup

Instance details

Name * MyNsg

Region * East US

4. When validation passes, select **Create**.

Update the network security group inbound rules

To ensure that lab users can use remote desktop to connect to the lab VMs, you need to create a security rule to allow this type of traffic. When you use Linux, you need to adapt the rule for SSH.

To create a rule that allows both RDP and SSH traffic for the subnet you created previously:

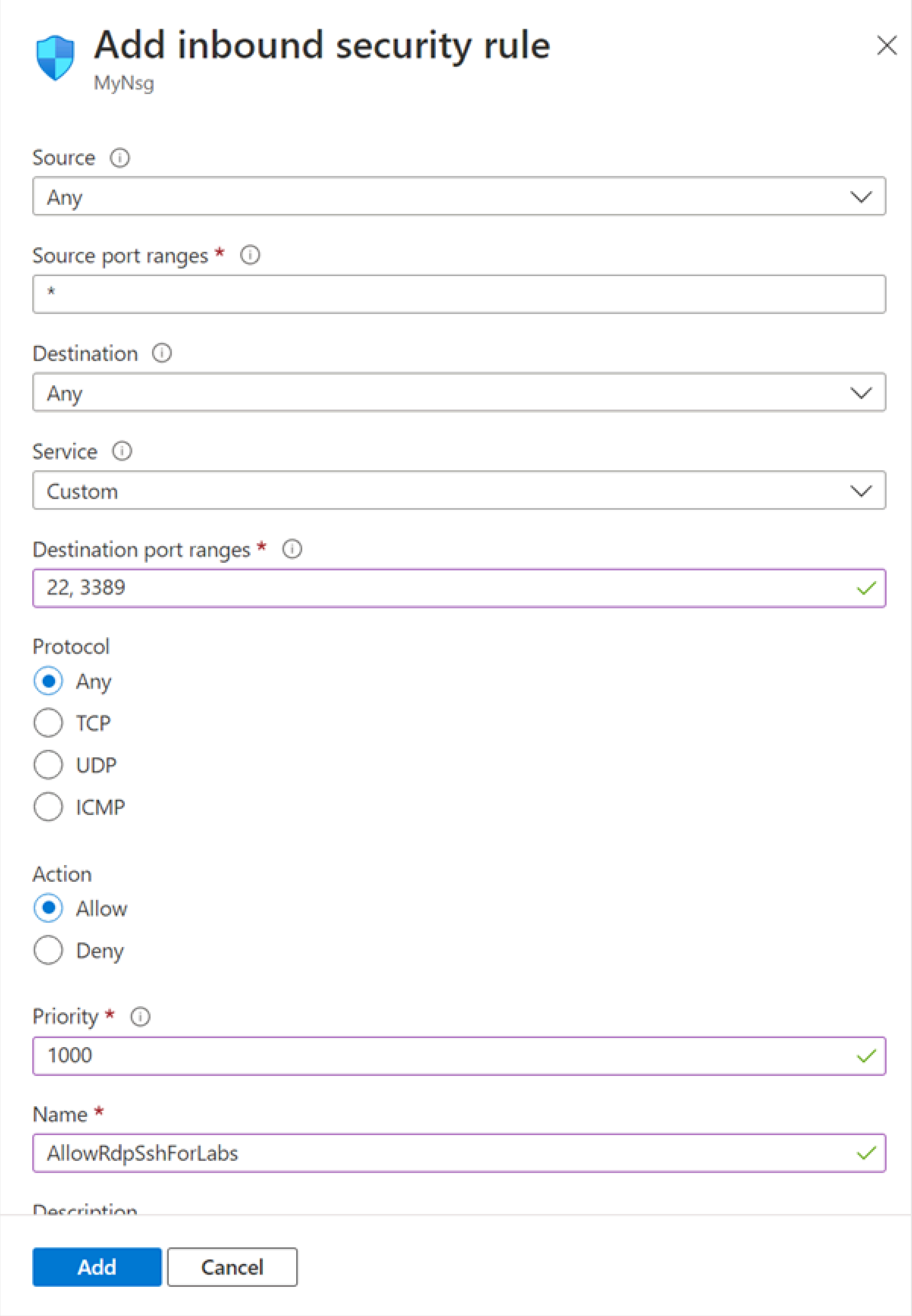
1. Open **MyNsg**.
2. Select **Inbound security rules** on the left menu.
3. Select **+ Add** from the top menu bar. Fill in the details for adding the inbound security rule as follows:
   a. For **Source**, select **Any**.
   b. For **Source port ranges**, select *.
   c. For **Destination**, select **IP Addresses**.
   d. For **Destination IP addresses/CIDR ranges**, select subnet range from **labservices-subnet** created previously.
   e. For **Service**, select **Custom**.
   f. For **Destination port ranges**, enter **22, 3389**. Port 22 is for Secure Shell protocol (SSH). Port 3389 is for Remote Desktop Protocol (RDP).
   g. For **Protocol**, select **Any**.

h. For **Action**, select **Allow**.

i. For **Priority**, select **1000**. Priority must be higher than other **Deny** rules for RDP and/or SSH.

j. For **Name**, enter **AllowRdpSshForLabs**.

k. Select **Add**.



Add inbound security rule

MyNsg

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 22, 3389

Protocol

● Any

○ TCP

○ UDP

○ ICMP

Action

● Allow

○ Deny

Priority *: 1000

Name *: AllowRdpSshForLabs

Description

4. Wait for the rule to be created.

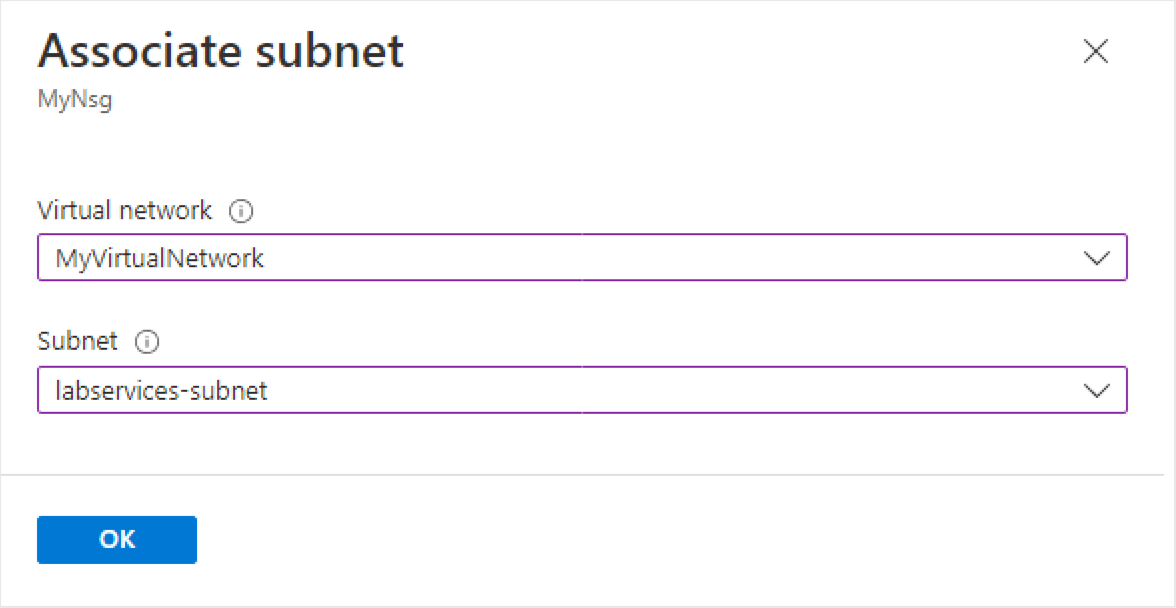
5. Select **Refresh** on the menu bar. The new rule now shows in the list of rules.

Associate network security group to virtual network

You now have an NSG with an inbound security rule to allow lab VMs to connect to the virtual network.

To associate the NSG with the virtual network you created earlier:

1. Open **MyVirtualNetwork**.
2. Select **Subnets** on the left menu.
3. Select **+ Associate** from the top menu bar.
4. On the **Associate subnet** page, do the following actions:
   a. For **Virtual network**, select **MyVirtualNetwork**.
   b. For **Subnet**, select **labservices-subnet**.
   c. Select **OK**.



Associate subnet

MyNsg

Virtual network: MyVirtualNetwork

Subnet: labservices-subnet

⚠ **Warning**

Connecting the network security group to the subnet is a **required step**. Lab users are not able to connect to their lab VMs if there is no network security group associated with the subnet.

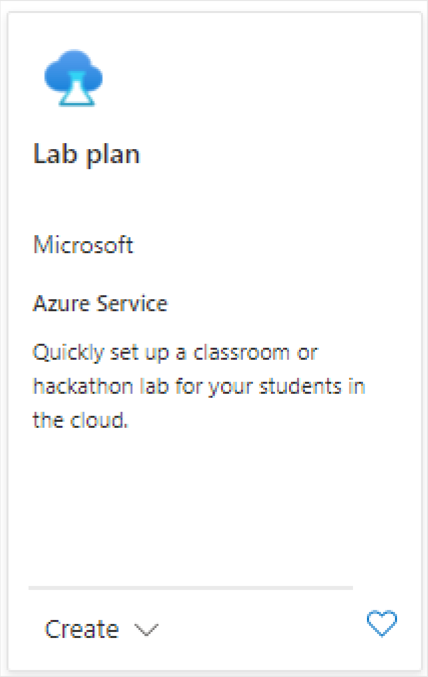
Create a lab plan using advanced networking

Now that the virtual network is created and configured, you can create the lab plan:

1. Select **Create a resource** in the upper left-hand corner of the Azure portal.

2. Search for **lab plan**.

3. On the **Lab plan** tile, select the **Create** dropdown and choose **Lab plan**.



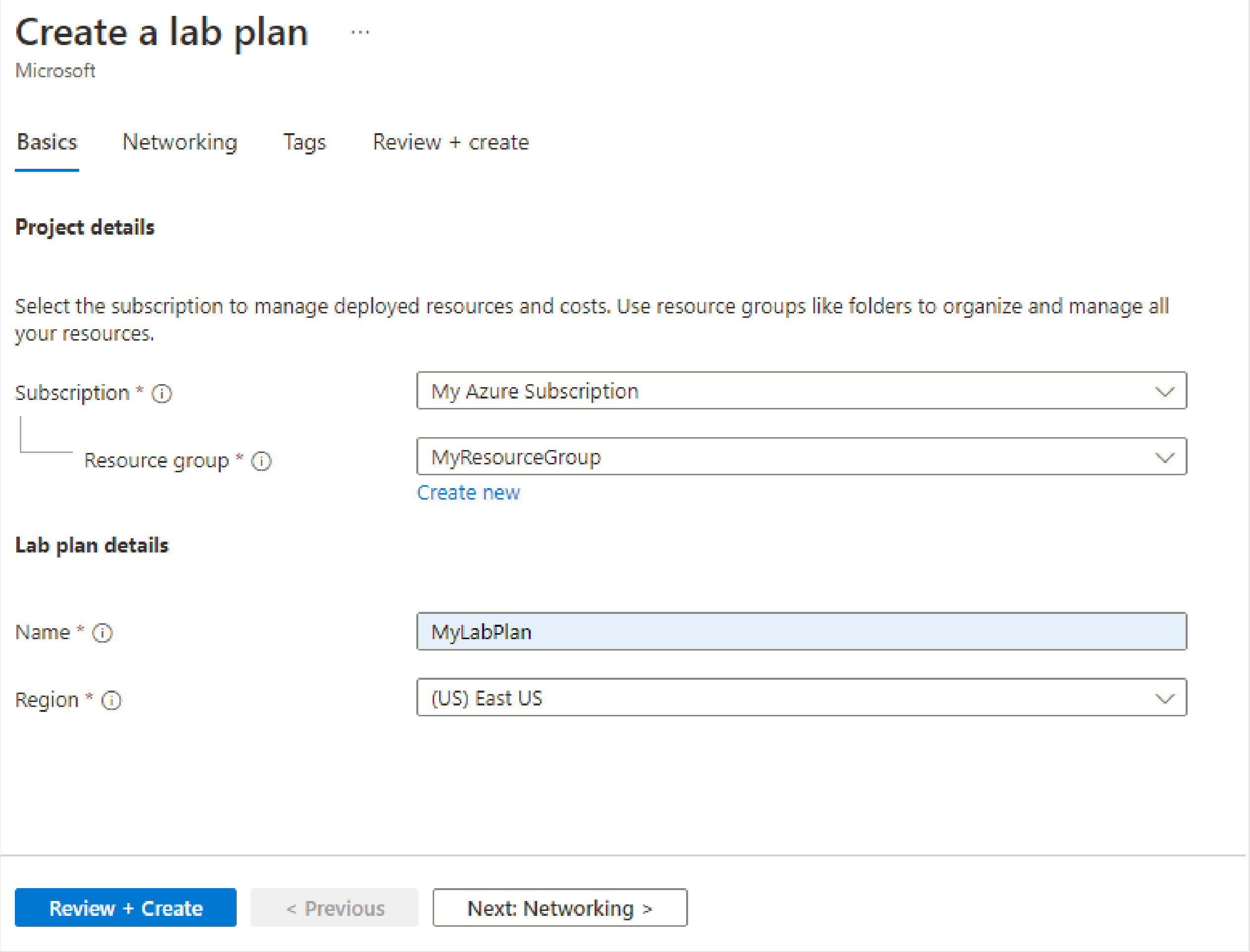
Lab plan

Microsoft

Azure Service

Quickly set up a classroom or hackathon lab for your students in the cloud.

4. On the **Basics** tab of the **Create a lab plan** page, do the following actions:
   a. For **Azure subscription**, select the subscription used earlier.
   b. For **Resource group**, select an existing resource group or select **Create new**, and enter a name for the new resource group.
   c. For **Name**, enter a lab plan name. For more information about naming restrictions, see Microsoft.LabServices resource name rules.
   d. For **Region**, select a location/region in which you want to create the lab plan.



Create a lab plan

Microsoft

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : My Azure Subscription

Resource group * : MyResourceGroup

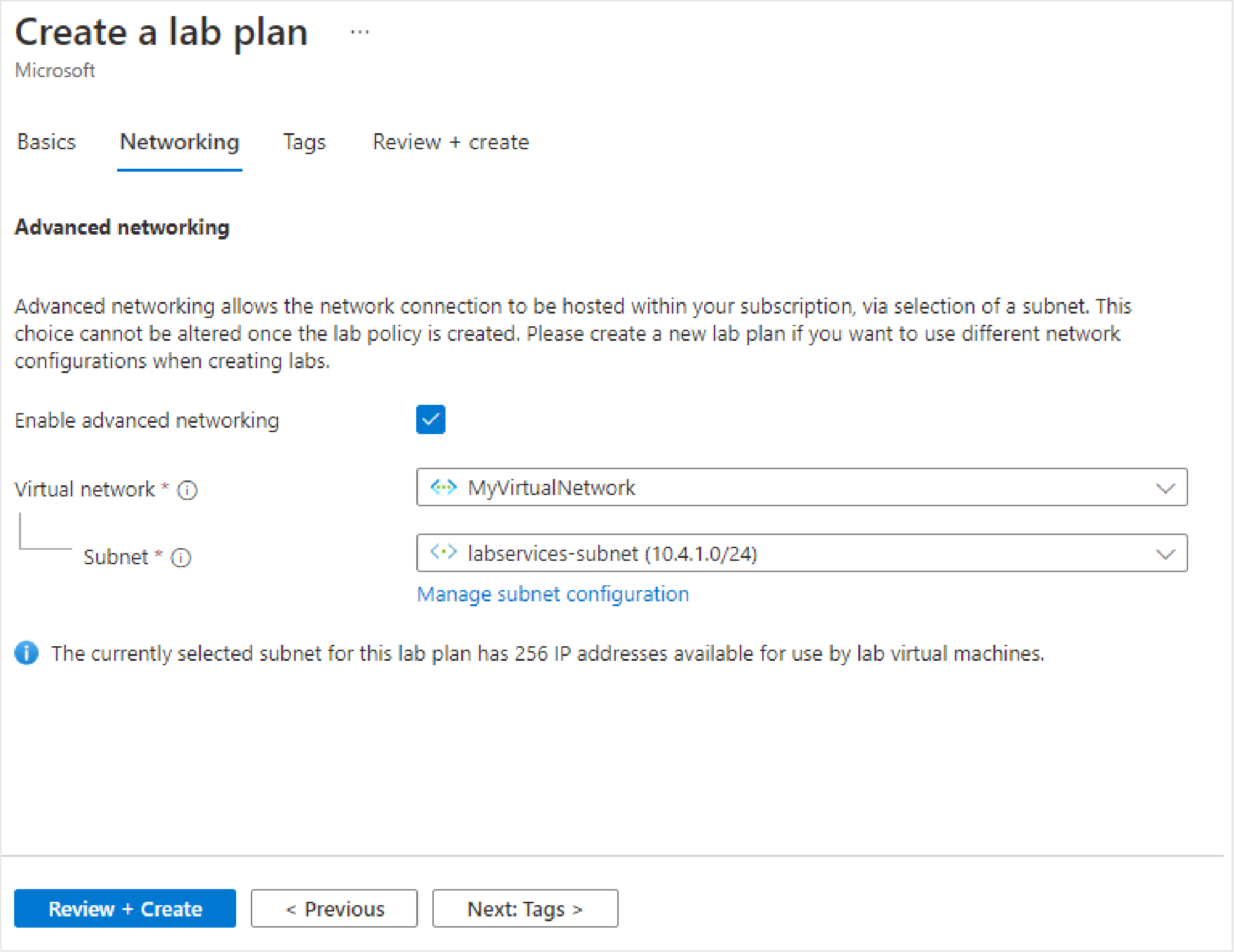
Lab plan details

Name * : MyLabPlan

Region * : (US) East US

5. Select **Next: Networking**.

6. On the **Networking** tab, do the following actions:
   a. Check **Enable advanced networking**.
   b. For **Virtual network**, choose **MyVirtualNetwork**.
   c. For **Subnet**, choose **labservices-subnet**.
   d. Select **Review + Create**.



Advanced networking

Advanced networking allows the network connection to be hosted within your subscription, via selection of a subnet. This choice cannot be altered once the lab policy is created. Please create a new lab plan if you want to use different network configurations when creating labs.

Enable advanced networking ☑

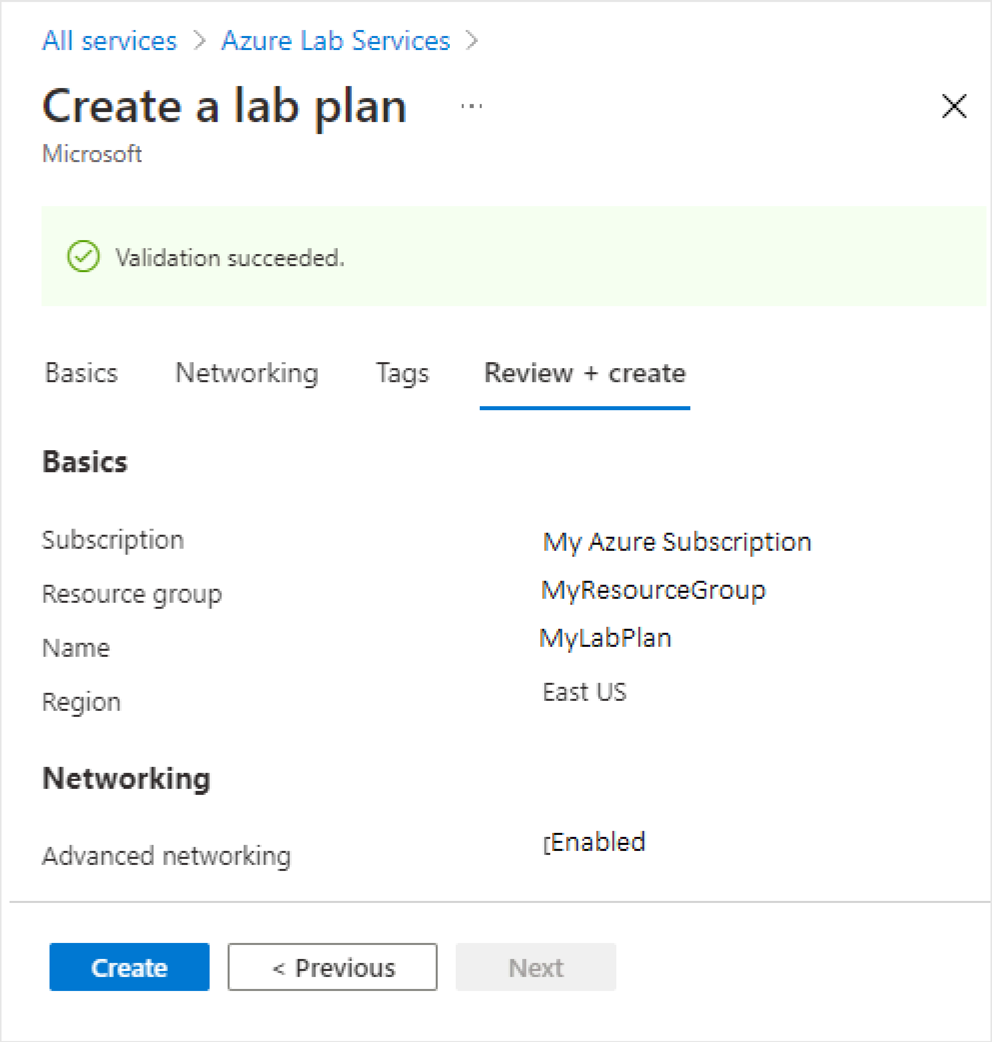
Virtual network * ⓘ MyVirtualNetwork

Subnet * ⓘ labservices-subnet (10.4.1.0/24)

Manage subnet configuration

ⓘ The currently selected subnet for this lab plan has 256 IP addresses available for use by lab virtual machines.

7. When the validation succeeds, select **Create**.



Create a lab plan

Microsoft

Validation succeeded.

Basics

Subscription: My Azure Subscription

Resource group: MyResourceGroup

Name: MyLabPlan

Region: East US

Networking

Advanced networking: [Enabled

ⓘ **Note**

Advanced networking can only be enabled when lab plans are created. Advanced networking can't be added later.

Create two labs

Next, create two labs that use advanced networking. These labs use the **labservices-subnet** that's associated with Azure Lab Services. Any lab VMs created using **MyLabPlan** can communicate with each other. Communication can be restricted by using NSGs, firewalls, and more.

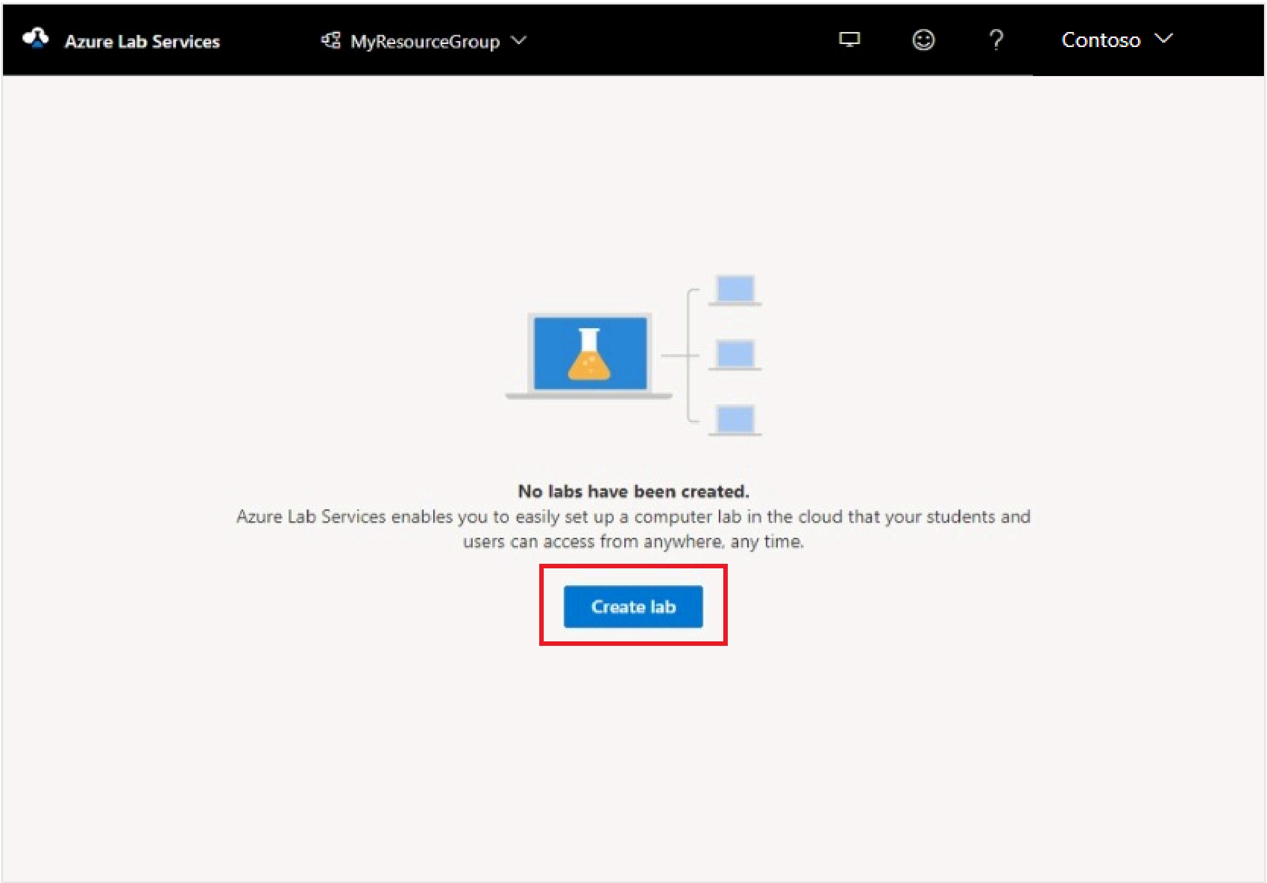
Perform the following steps to create both labs. Repeat these steps the server VM and the client VM.

1. Navigate to the Azure Lab Services website: https://labs.azure.com .

2. Select **Sign in** and enter your credentials. Azure Lab Services supports organizational accounts and Microsoft accounts.

3. Select **MyResourceGroup** from the dropdown on the menu bar.

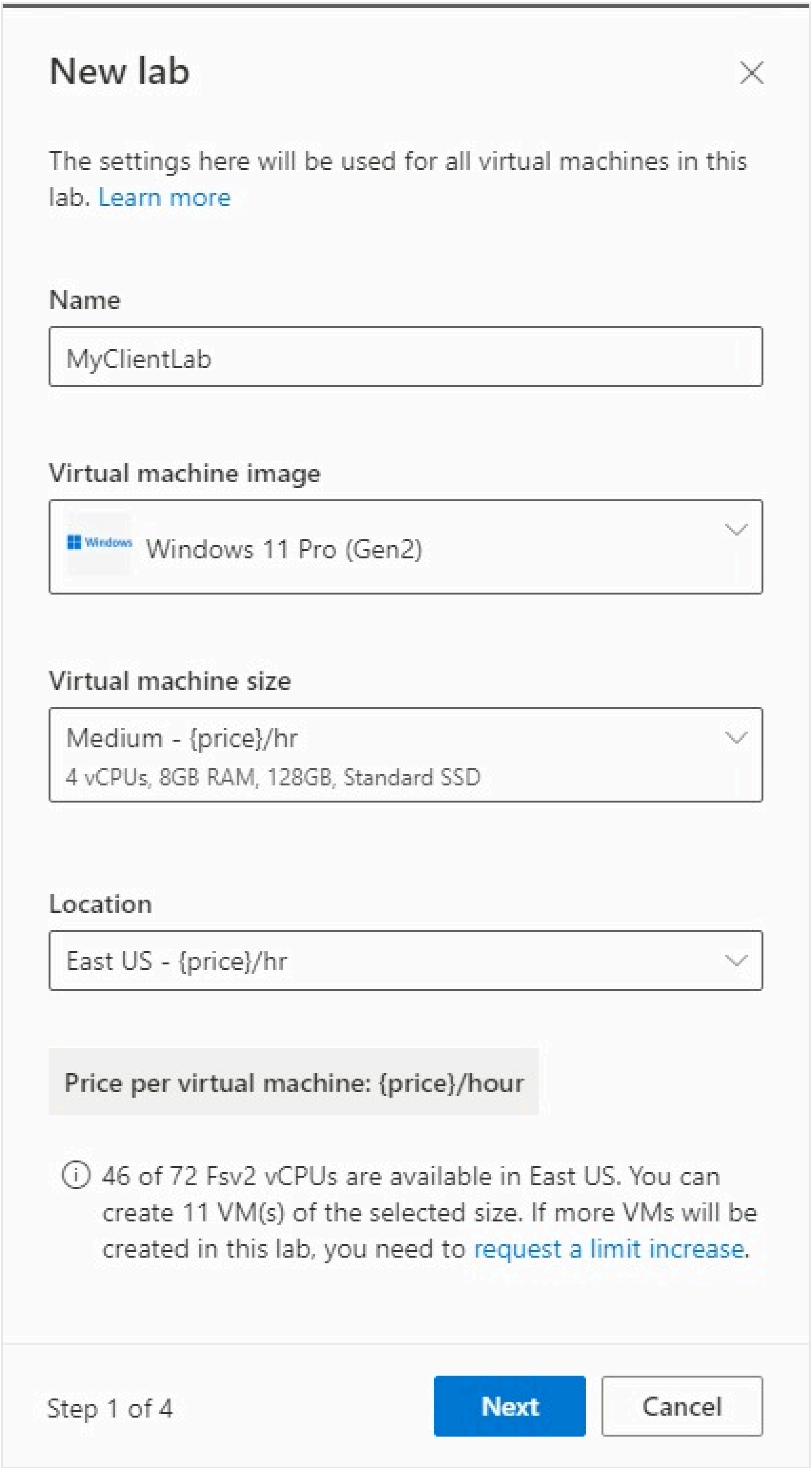
4. Select **New lab**.



No labs have been created.

Azure Lab Services enables you to easily set up a computer lab in the cloud that your students and users can access from anywhere, any time.

5. In the **New Lab** window, do the following actions:
   a. Specify a **name**. The name should be easily identifiable. Use **MyServerLab** for the lab with the server VMs and **MyClientLab** for the lab with the client VMs. For more information about naming restrictions, see Microsoft.LabServices resource name rules.
   b. Choose a **virtual machine image**. For this tutorial, use **Windows 11 Pro**, but you can choose another available image if you want. For more information about enabling virtual machine images, see Specify Marketplace images available to lab creators.
   c. For **size**, select **Medium**.
   d. **Region** only has one region. When a lab uses advanced networking, the lab must be in the same region as the associated subnet.
   e. Select **Next**.



New lab

The settings here will be used for all virtual machines in this lab. Learn more

Name

MyClientLab

Virtual machine image

Windows 11 Pro (Gen2)

Virtual machine size

Medium - {price}/hr
4 vCPUs, 8GB RAM, 128GB, Standard SSD

Location

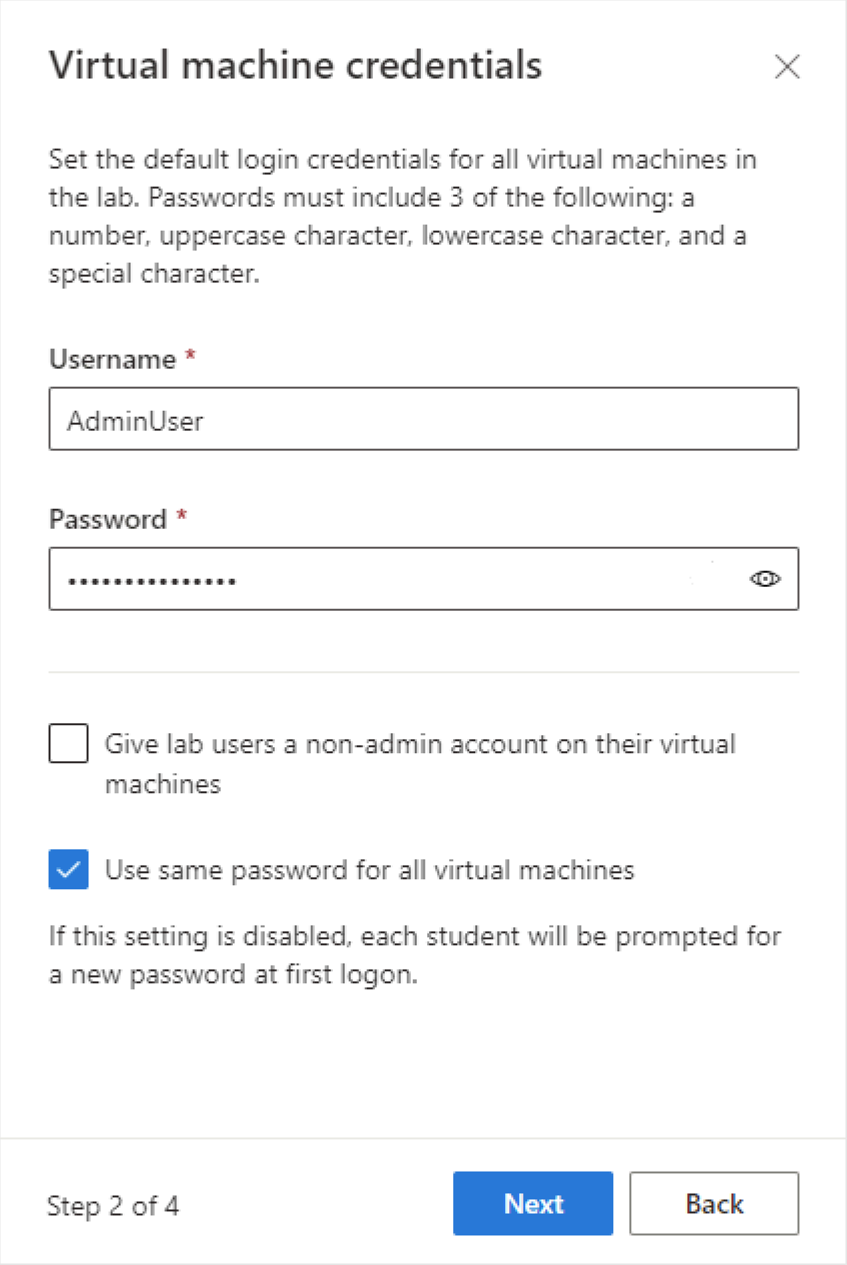
East US - {price}/hr

Price per virtual machine: {price}/hour

46 of 72 Fsv2 vCPUs are available in East US. You can create 11 VM(s) of the selected size. If more VMs will be created in this lab, you need to request a limit increase.

Step 1 of 4

6. On the **Virtual machine credentials** page, specify default administrator credentials for all VMs in the lab. Specify the **name** and **password** for the administrator. By default all the lab VMs have the same password as the one specified here. Select **Next**.



Virtual machine credentials

Set the default login credentials for all virtual machines in the lab. Passwords must include 3 of the following: a number, uppercase character, lowercase character, and a special character.

Username *

AdminUser

Password *

•••••••••••••••

□ Give lab users a non-admin account on their virtual machines

☑ Use same password for all virtual machines

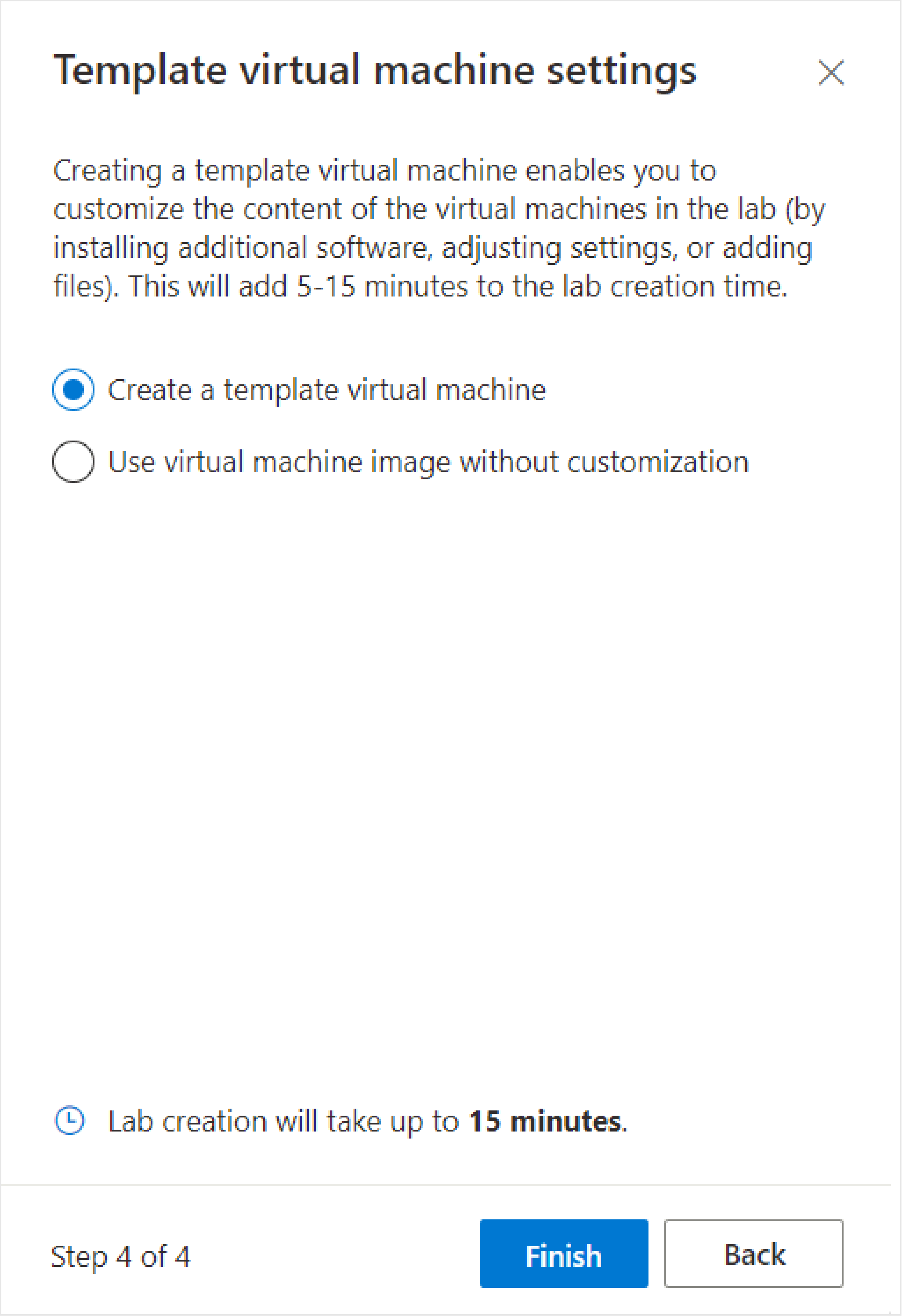
If this setting is disabled, each student will be prompted for a new password at first logon.

Step 2 of 4

> **Important**
>
> Make a note of user name and password. They won't be shown again.

7. On the **Lab policies** page, leave the default selections and select **Next**.

8. On the **Template virtual machine settings** window, leave the selection on **Create a template virtual machine**. Select **Finish**.



Template virtual machine settings

Creating a template virtual machine enables you to customize the content of the virtual machines in the lab (by installing additional software, adjusting settings, or adding files). This will add 5-15 minutes to the lab creation time.

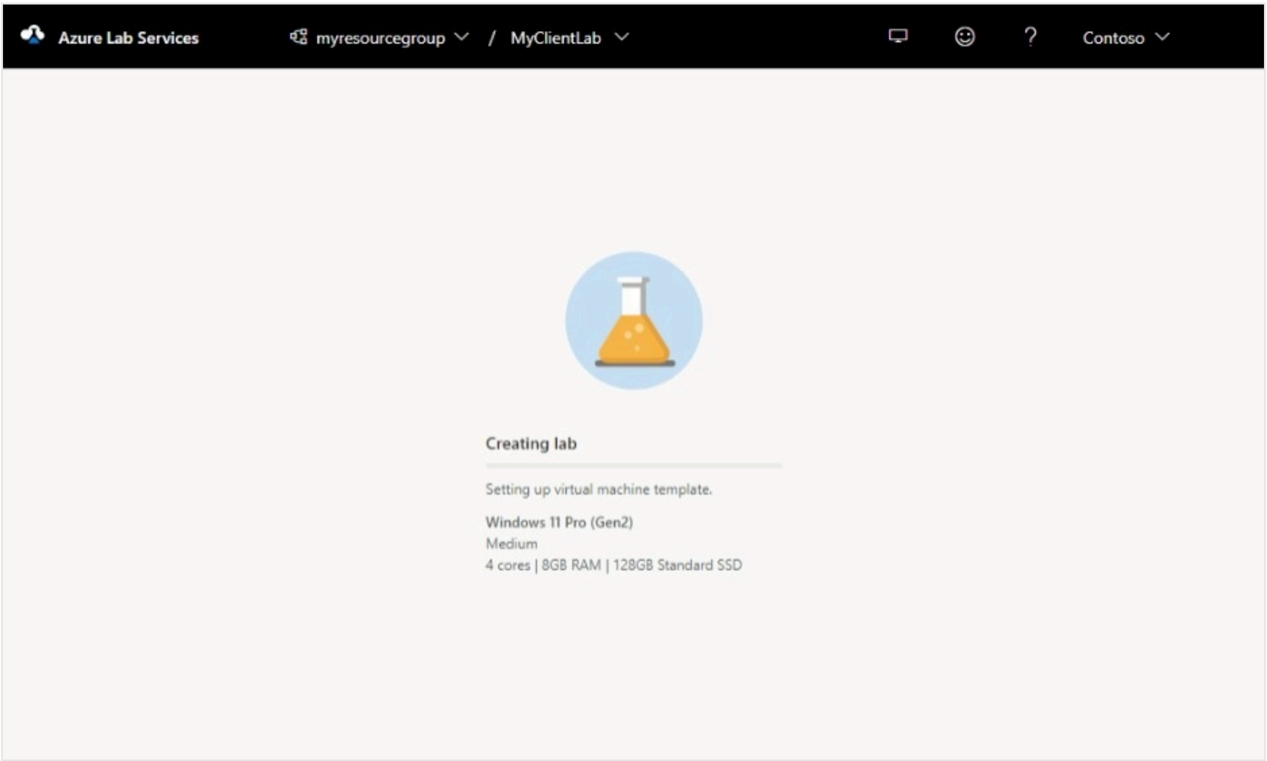
● Create a template virtual machine

○ Use virtual machine image without customization

Lab creation will take up to **15 minutes**.

Step 4 of 4

9. You should see the following screen that shows the status of the template VM creation.



Creating lab

Setting up virtual machine template.

Windows 11 Pro (Gen2)
Medium
4 cores | 8GB RAM | 128GB Standard SSD

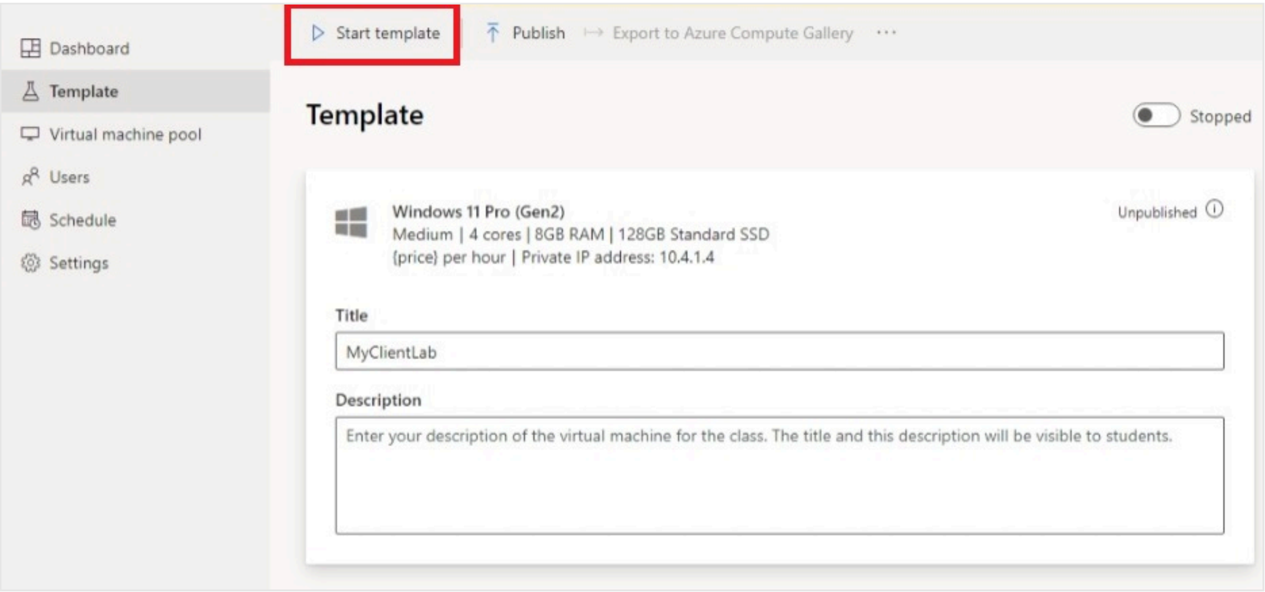
10. Wait for the template VM to be created.

Enable ICMP on the lab templates

Once the labs are created, enable ICMP (ping) for testing communication between the lab VMs. First, enable ICMP on the template VMs for both labs. Enabling ICMP on the template VM also enables it on the lab VMs. Once the labs are published, the lab VMs are able to ping each other.

To enable ICMP, complete the following steps for each template VM in each lab.

1. On the **Template** page for the lab, start and connect to the template VM.
   a. Select **Start template**.



Template

Windows 11 Pro (Gen2)
Medium | 4 cores | 8GB RAM | 128GB Standard SSD
(price) per hour | Private IP address: 10.4.1.4

Title

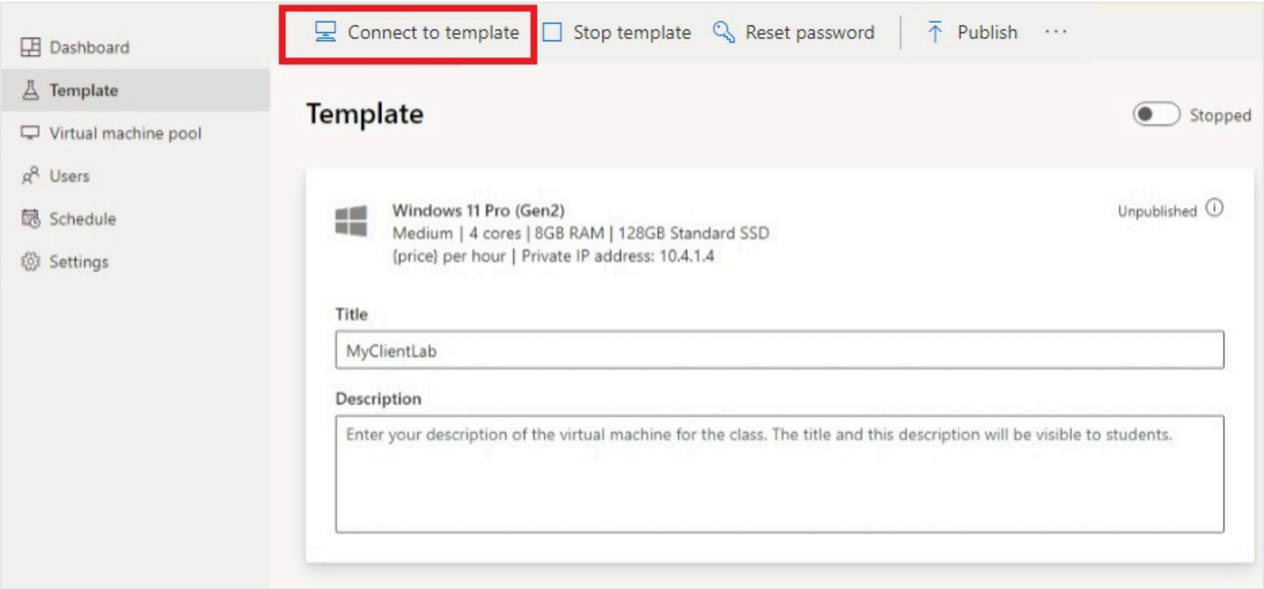
MyClientLab

Description

Enter your description of the virtual machine for the class. The title and this description will be visible to students.

> ⓘ **Note**
>
> Template VMs incur **cost** when running, so ensure that the template VM is shutdown when you don’t need it to be running.

a. Once the template is started, select **Connect to template**.



Windows 11 Pro (Gen2)
Medium | 4 cores | 8GB RAM | 128GB Standard SSD
{price} per hour | Private IP address: 10.4.1.4

Title: MyClientLab

Description: Enter your description of the virtual machine for the class. The title and this description will be visible to students.

When you're logged in to the template VM, modify the firewall rules on the VM to allow ICMP. Because you're using Windows 11, you can use PowerShell and the Enable-NetFirewallRule cmdlet. To open a PowerShell window:

1. Select the Start button.
2. Type "PowerShell"
3. Select the **Windows PowerShell** app.

Run the following code:

PowerShell

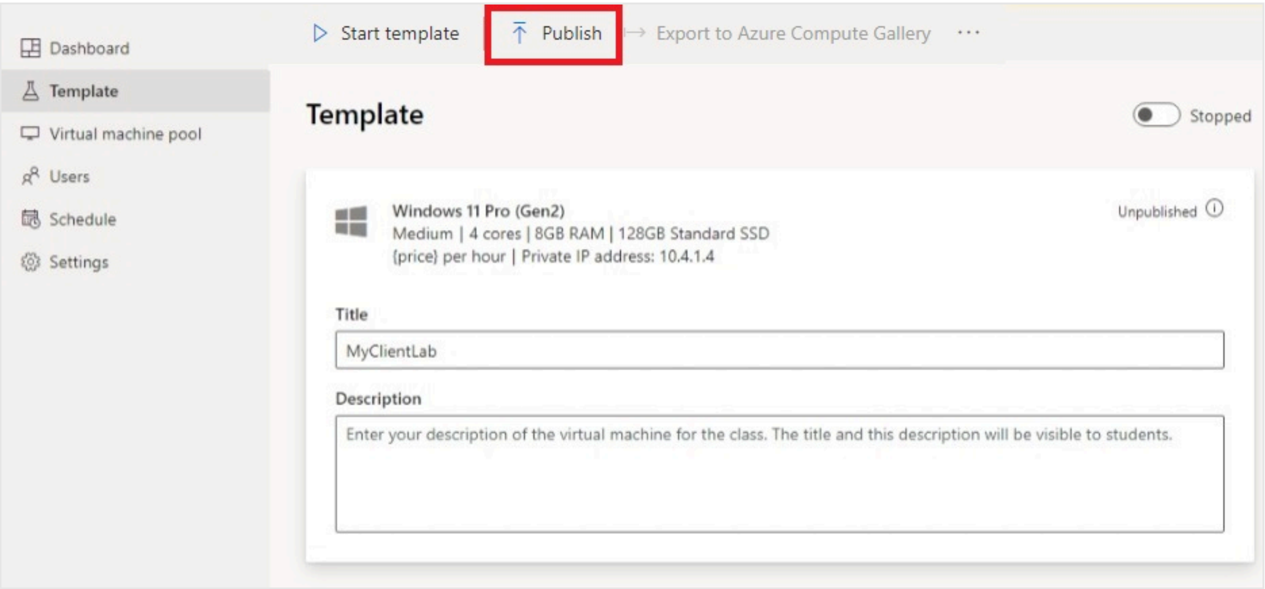
```powershell
Enable-NetFirewallRule -Name CoreNet-Diag-ICMP4-EchoRequest-In
Enable-NetFirewallRule -Name CoreNet-Diag-ICMP4-EchoRequest-Out
```

On the **Template** page for the lab, select **Stop** to stop the template VM.

Publish both labs

In this step, you publish the lab. When you publish the template VM, Azure Lab Services creates VMs in the lab by using the template. All virtual machines have the same configuration as the template.

1. On the **Template** page, select **Publish**.



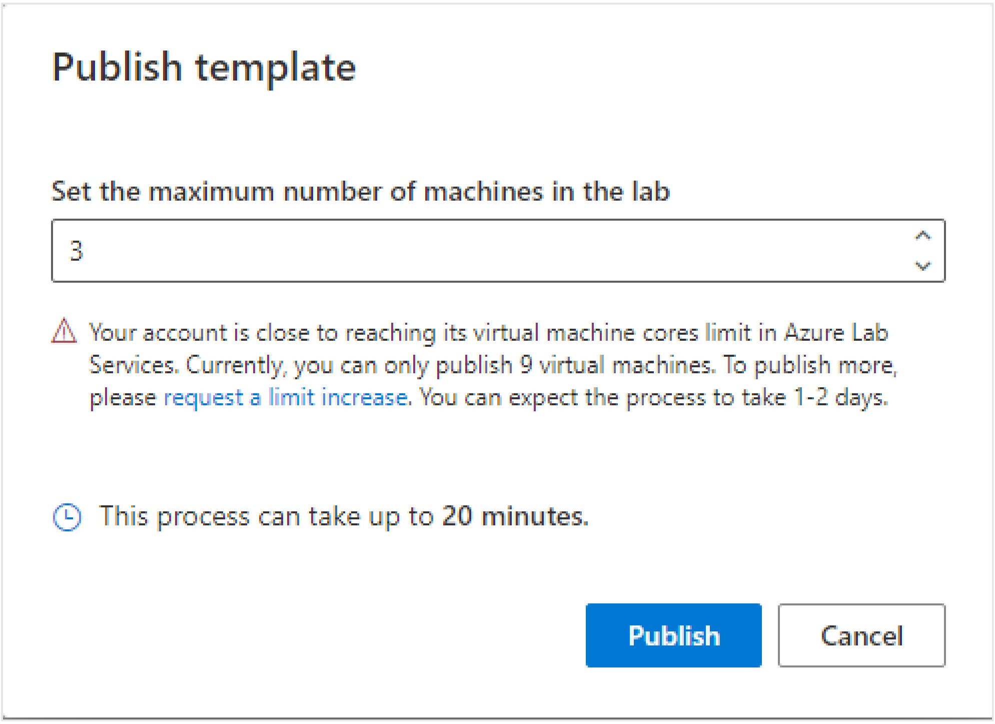
Template

Windows 11 Pro (Gen2)
Medium | 4 cores | 8GB RAM | 128GB Standard SSD
{price} per hour | Private IP address: 10.4.1.4

Title: MyClientLab

Description: Enter your description of the virtual machine for the class. The title and this description will be visible to students.

2. Enter the number of machines that are needed for the lab, then select **Publish**.



Publish template

Set the maximum number of machines in the lab: 3

⚠ Your account is close to reaching its virtual machine cores limit in Azure Lab Services. Currently, you can only publish 9 virtual machines. To publish more, please request a limit increase. You can expect the process to take 1-2 days.

This process can take up to **20 minutes.**

> ⚠ **Warning**
>
> Publishing is an irreversible action! It can't be undone.

3. You see the **status of publishing** the template page. Wait until the publishing is complete.

Test communication between lab VMs

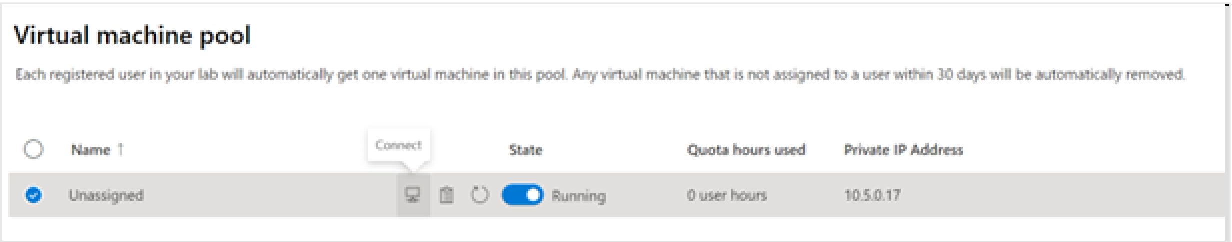
In this section, confirm that the two lab virtual machines in different labs are able to communicate with each other.

First, start and connect to a lab VM from each lab. Complete the following steps for each lab.

1. Open the lab in the Azure Lab Services website .
2. Select **Virtual machine pool** on the left menu.
3. Select a single VM listed in the virtual machine pool.
4. Take note of the **Private IP Address** for the VM. You need the private IP addresses of both the server lab and client lab VMs later.
5. Select the **State** slider to change the state from **Stopped** to **Starting**.

   > ⓘ **Note**
   >
   > When an lab educator starts a lab VM, quota for the lab user isn't affected. Quota for a user specifies the number of lab hours available to a lab user outside of the scheduled class time. For more information on quotas, see **Set quotas for users**.

6. Once the **State** is **Running**, select the connect icon for the running VM. Open the download RDP file to connect to the VM. For more information about connection experiences on different operating systems, see Connect to a lab VM.

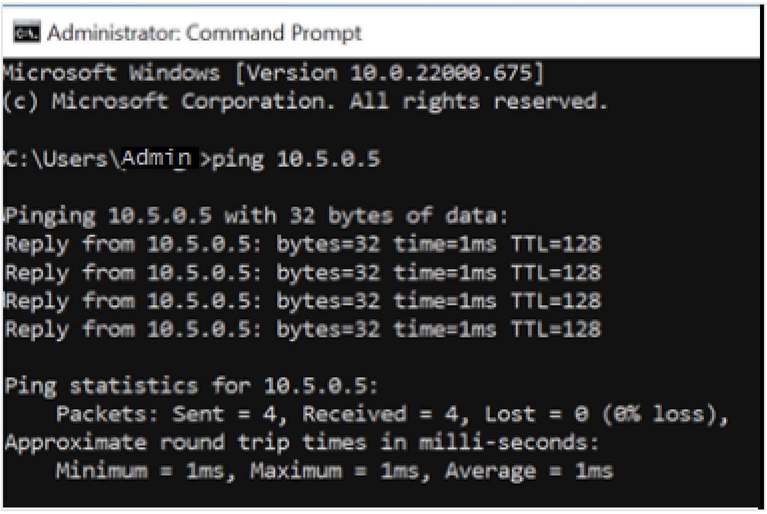


Virtual machine pool

Each registered user in your lab will automatically get one virtual machine in this pool. Any virtual machine that is not assigned to a user within 30 days will be automatically removed.

○	Name ↑	Connect	State	Quota hours used	Private IP Address
●	Unassigned		Running	0 user hours	10.5.0.17

Now, use the ping utility to test cross-lab communication. From the lab VM in the server lab, open a command prompt. Use `ping {ip-address}`. The `{ip-address}` is the **Private IP Address** of the client VM, that you noted previously. This test can also be done from the lab VM from the client lab to the lab VM in the server lab.



```
Microsoft Windows [Version 10.0.22000.675]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Admin >ping 10.5.0.5

Pinging 10.5.0.5 with 32 bytes of data:
Reply from 10.5.0.5: bytes=32 time=1ms TTL=128
Reply from 10.5.0.5: bytes=32 time=1ms TTL=128
Reply from 10.5.0.5: bytes=32 time=1ms TTL=128
Reply from 10.5.0.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.5.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

When done, navigate to the **Virtual machine pool** page for each lab, select the lab VM and select the **State** slider to stop the lab VM.

Clean up resources

If you're not going to continue to use this application, delete the virtual network, network security group, lab plan and labs with the following steps:

1. In the Azure portal, select the resource group you want to delete.
2. Select **Delete resource group**.
3. To confirm the deletion, type the name of the resource group

Troubleshooting

Lab creation fails with `You are not authorized to access this resource`

When you create a new lab plan, it might take a few minutes for the permissions to propagate to the lab level. You can assign the Lab Creator role at the resource group level to prevent this behavior:

1. In the Azure portal, go to the resource group that contains the lab plan.
2. Select **Access control (IAM)** from the left navigation.
3. Select **Add** > **Add role assignment**.
4. Assign the **Lab Creator** role to the user account.

Next steps

Add lab users to the labs