Tell us about your PDF experience.

Azure Bastion documentation

Learn how to use Azure Bastion to connect to a virtual machine. Configure secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over SSL. When you connect via Azure Bastion, your virtual machines do not need a public IP address.

About Azure Bastion

OVERVIEW

What is Azure Bastion?

CONCEPT

Azure Bastion FAQ

TRAINING

Introduction to Azure Bastion

VIDEO

Azure Bastion

Get started

QUICKSTART

Deploy Bastion with default settings

HOW-TO GUIDE

Deploy Bastion using manual settings

Connect to a virtual machine (Linux)

Connect to a virtual machine (Windows)

TRAINING

Connect to a VM using Azure Bastion

VIDEO

Working with Azure Bastion

Working with virtual machine sessions

CONCEPT

Connecting to VMs

VM supported features

HOW-TO GUIDE

Copy and paste

Full screen view

Upload or download files

Reference

REFERENCE

Azure PowerShell

Azure CLI

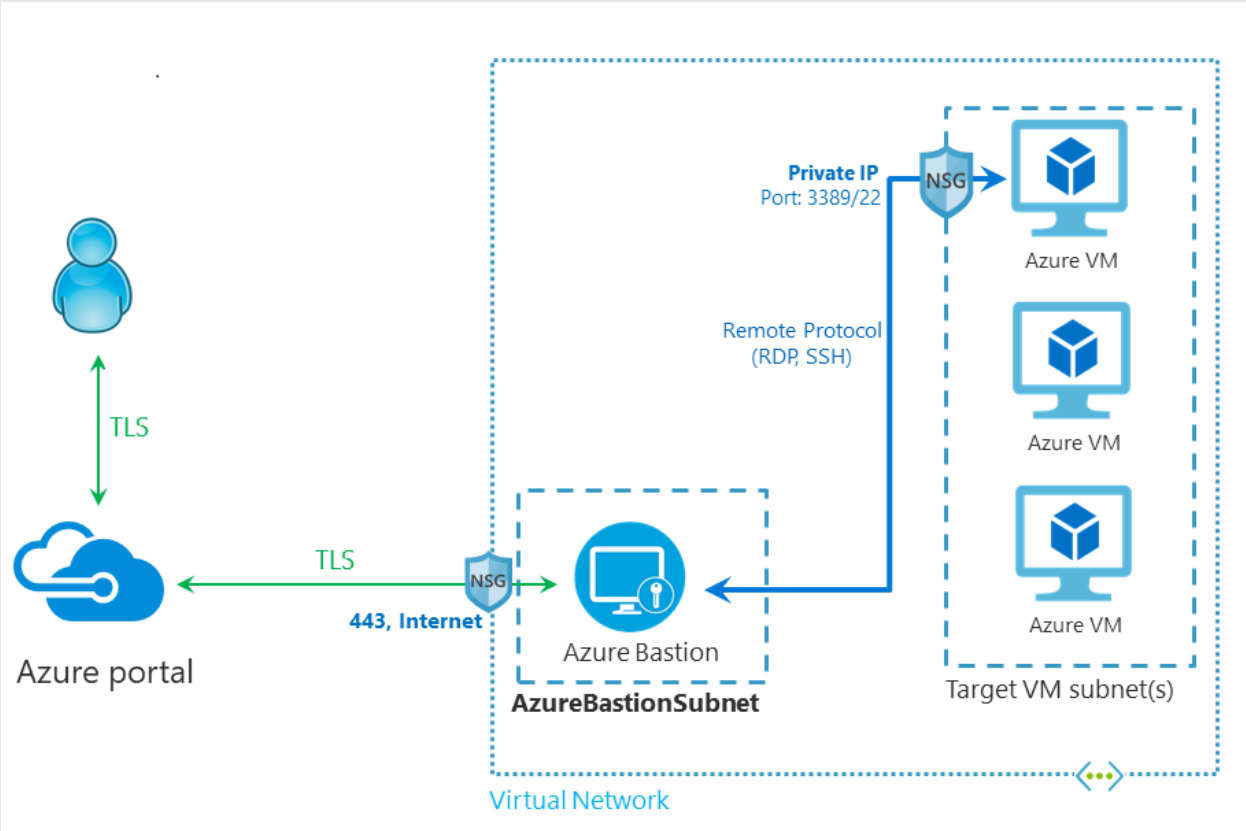
REST

What is Azure Bastion?

Article • 02/03/2023 • 5 minutes to read

Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal, or via the native SSH or RDP client already installed on your local computer. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines don't need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.



Key benefits

Benefit	Description

Benefit	Description
RDP and SSH through the Azure portal	You can get to the RDP and SSH session directly in the Azure portal using a single-click seamless experience.
Remote Session over TLS and firewall traversal for RDP/SSH	Azure Bastion uses an HTML5 based web client that is automatically streamed to your local device. Your RDP/SSH session is over TLS on port 443. This enables the traffic to traverse firewalls more securely. Bastion supports TLS 1.2 and above. Older TLS versions are not supported.
No Public IP address required on the Azure VM	Azure Bastion opens the RDP/SSH connection to your Azure VM by using the private IP address on your VM. You don't need a public IP address on your virtual machine.
No hassle of managing Network Security Groups (NSGs)	You don't need to apply any NSGs to the Azure Bastion subnet. Because Azure Bastion connects to your virtual machines over private IP, you can configure your NSGs to allow RDP/SSH from Azure Bastion only. This removes the hassle of managing NSGs each time you need to securely connect to your virtual machines. For more information about NSGs, see Network Security Groups.
No need to manage a separate bastion host on a VM	Azure Bastion is a fully managed platform PaaS service from Azure that is hardened internally to provide you secure RDP/SSH connectivity.
Protection against port scanning	Your VMs are protected against port scanning by rogue and malicious users because you don't need to expose the VMs to the internet.
Hardening in one place only	Azure Bastion sits at the perimeter of your virtual network, so you don’t need to worry about hardening each of the VMs in your virtual network.

Benefit	Description
Protection against zero-day exploits	The Azure platform protects against zero-day exploits by keeping the Azure Bastion hardened and always up to date for you.

SKUs

Azure Bastion has two available SKUs, Basic and Standard. For more information, including how to upgrade a SKU, see the Configuration settings article.

The following table shows features and corresponding SKUs.

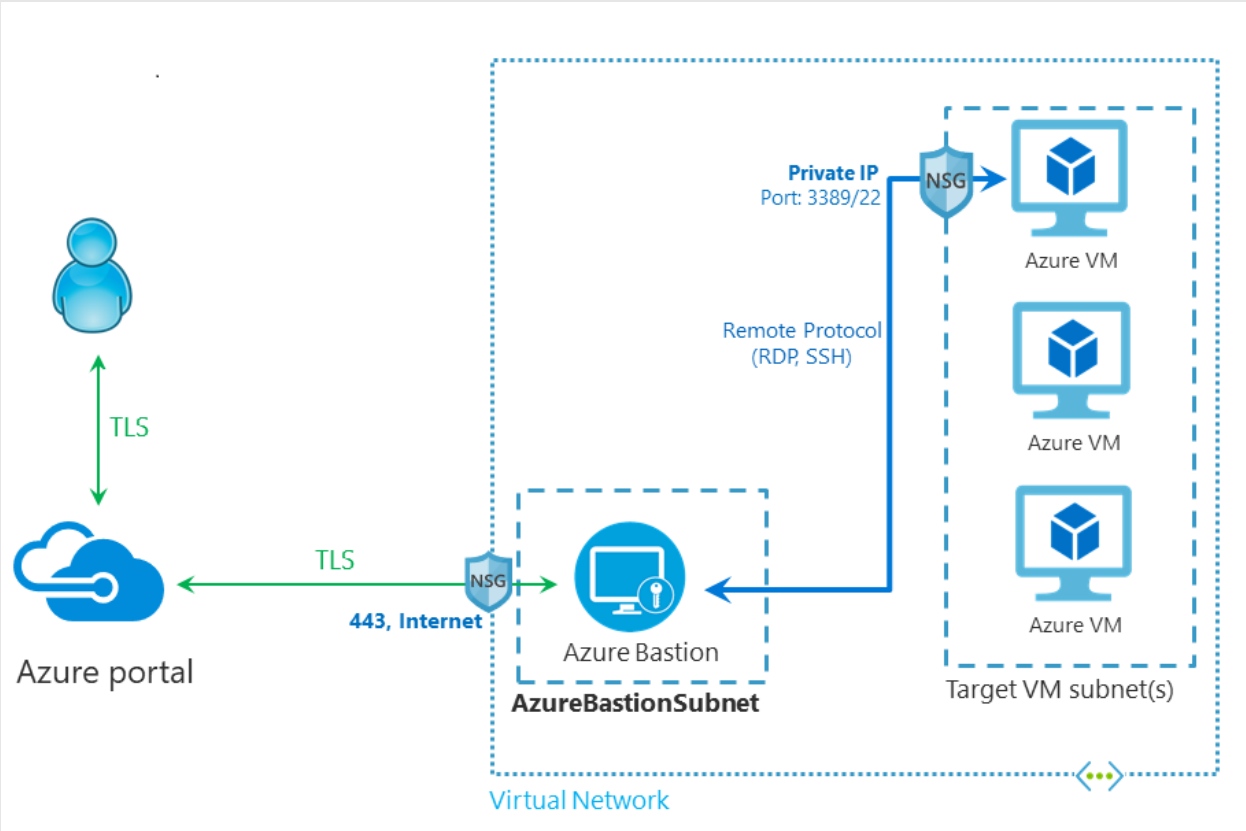
Feature	Basic SKU	Standard SKU
Connect to target VMs in peered virtual networks	Yes	Yes
Access Linux VM Private Keys in Azure Key Vault (AKV)	Yes	Yes
Connect to Linux VM using SSH	Yes	Yes
Connect to Windows VM using RDP	Yes	Yes
Kerberos authentication	Yes	Yes
VM audio output	Yes	Yes
Shareable link	No	Yes
Connect to VMs using a native client	No	Yes
Connect to VMs via IP address	No	Yes
Host scaling	No	Yes
Specify custom inbound port	No	Yes
Connect to Linux VM using RDP	No	Yes
Connect to Windows VM using SSH	No	Yes
Upload or download files	No	Yes
Disable copy/paste (web-based clients)	No	Yes

Architecture

Azure Bastion is deployed to a virtual network and supports virtual network peering. Specifically, Azure Bastion manages RDP/SSH connectivity to VMs created in the local or peered virtual networks.

RDP and SSH are some of the fundamental means through which you can connect to your workloads running in Azure. Exposing RDP/SSH ports over the Internet isn't desired and is seen as a significant threat surface. This is often due to protocol vulnerabilities. To contain this threat surface, you can deploy bastion hosts (also known as jump-servers) at the public side of your perimeter network. Bastion host servers are designed and configured to withstand attacks. Bastion servers also provide RDP and SSH connectivity to the workloads sitting behind the bastion, as well as further inside the network.

Currently, by default, new Bastion deployments don't support zone redundancies. Previously deployed bastions may or may not be zone-redundant. The exceptions are Bastion deployments in Korea Central and Southeast Asia, which do support zone redundancies.



This figure shows the architecture of an Azure Bastion deployment. In this diagram:

- The Bastion host is deployed in the virtual network that contains the AzureBastionSubnet subnet that has a minimum /26 prefix.
- The user connects to the Azure portal using any HTML5 browser.
- The user selects the virtual machine to connect to.
- With a single click, the RDP/SSH session opens in the browser.
- No public IP is required on the Azure VM.

Host scaling

Azure Bastion supports manual host scaling. You can configure the number of host **instances** (scale units) in order to manage the number of concurrent RDP/SSH connections that Azure Bastion can support. Increasing the number of host instances lets Azure Bastion manage more concurrent sessions. Decreasing the number of instances decreases the number of concurrent supported sessions. Azure Bastion supports up to 50 host instances. This feature is available for the Azure Bastion Standard SKU only.

For more information, see the Configuration settings article.

Pricing

Azure Bastion pricing is a combination of hourly pricing based on SKU and instances (scale units), plus data transfer rates. Hourly pricing starts from the moment Bastion is deployed, regardless of outbound data usage. For the latest pricing information, see the Azure Bastion pricing page.

What's new?

Subscribe to the RSS feed and view the latest Azure Bastion feature updates on the Azure Updates page.

Bastion FAQ

For frequently asked questions, see the Bastion FAQ.

Next steps

- Quickstart: Deploy Bastion using default settings.
- Tutorial: Deploy Bastion using specified settings.
- Learn module: Introduction to Azure Bastion.
- Learn about some of the other key networking capabilities of Azure.

Additional resources

Documentation

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Azure network security groups overview

Learn about network security groups. Network security groups help you filter network traffic between Azure resources.

Tutorial: Deploy Bastion using specified settings: Azure portal

Learn how to deploy Bastion using settings that you specify - Azure portal.

VNet peering and Azure Bastion architecture

Learn how VNet peering and Azure Bastion can be used together to connect to VMs.

Network security group - how it works

Learn how network security groups help you filter network traffic between Azure resources.

Quickstart: Deploy Bastion with default settings - Azure Bastion

Learn how to deploy Bastion with default settings from the Azure portal.

Deploy & configure Azure Firewall using the Azure portal

In this article, you learn how to deploy and configure Azure Firewall using the Azure portal.

Show 5 more

Training

Learning paths and modules

Introduction to Azure Bastion - Training

Describe how Azure Bastion provides secure and seamless connectivity to your VMs directly in the Azure portal. Determine whether Azure Bastion can replace your administrative jump boxes.

Quickstart: Deploy Azure Bastion with default settings

Article • 09/09/2022 • 6 minutes to read

In this quickstart, you'll learn how to deploy Azure Bastion with default settings to your virtual network using the Azure portal. After Bastion is deployed, you can connect (SSH/RDP) to virtual machines in the virtual network via Bastion using the private IP address of the VM. When you connect to a VM, it doesn't need a public IP address, client software, agent, or a special configuration. Azure Bastion is a PaaS service that's maintained for you, not a bastion host that you install on one of your VMs and maintain yourself. For more information about Azure Bastion, see What is Azure Bastion?

The following steps walk you through how to deploy Bastion from your VM resource using the Azure portal. When you deploy using default settings, the settings are based on the virtual network to which Bastion will be deployed. After deploying Bastion, you'll then connect to your VM using RDP/SSH connectivity and the VM's private IP address. If your VM has a public IP address that you don't need for anything else, you can remove it. While the steps in this quickstart help you deploy Bastion from your VM resource, you can deploy Bastion from a virtual network resource instead. The steps are similar, except you start from the virtual network resource instead of the VM resource.

Prerequisites

- **An Azure account with an active subscription**. If you don't have one, create one for free.

- **A VM in a VNet**.

  When you deploy Bastion using default values, the values are pulled from the VNet in which your VM resides. This VM doesn't become a part of the Bastion deployment itself, but you do connect to it later in the exercise.
  - If you don't already have a VM in a VNet, create one using Quickstart: Create a Windows VM, or Quickstart: Create a Linux VM.
  - If you need example values, see the Example values section.
  - If you already have a virtual network, make sure it's selected on the Networking tab when you create your VM.
  - If you don't have a virtual network, you can create one at the same time you create your VM.

- **Required VM roles:**

- Reader role on the virtual machine.
- Reader role on the NIC with private IP of the virtual machine.

- **Required VM ports inbound ports:**
  - 3389 for Windows VMs
  - 22 for Linux VMs

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Example values

You can use the following example values when creating this configuration, or you can substitute your own.

Basic VNet and VM values:

Name	Value
Virtual machine	TestVM
Resource group	TestRG1
Region	East US
Virtual network	VNet1
Address space	10.1.0.0/16
Subnets	FrontEnd: 10.1.0.0/24

Bastion values:

When you deploy from VM settings, Bastion is automatically configured with default values from the VNet

Name	Default value
AzureBastionSubnet	This subnet is created within the VNet as a /26
SKU	Basic
Name	Based on the virtual network name

Name	Default value
Public IP address name	Based on the virtual network name

Deploy Bastion

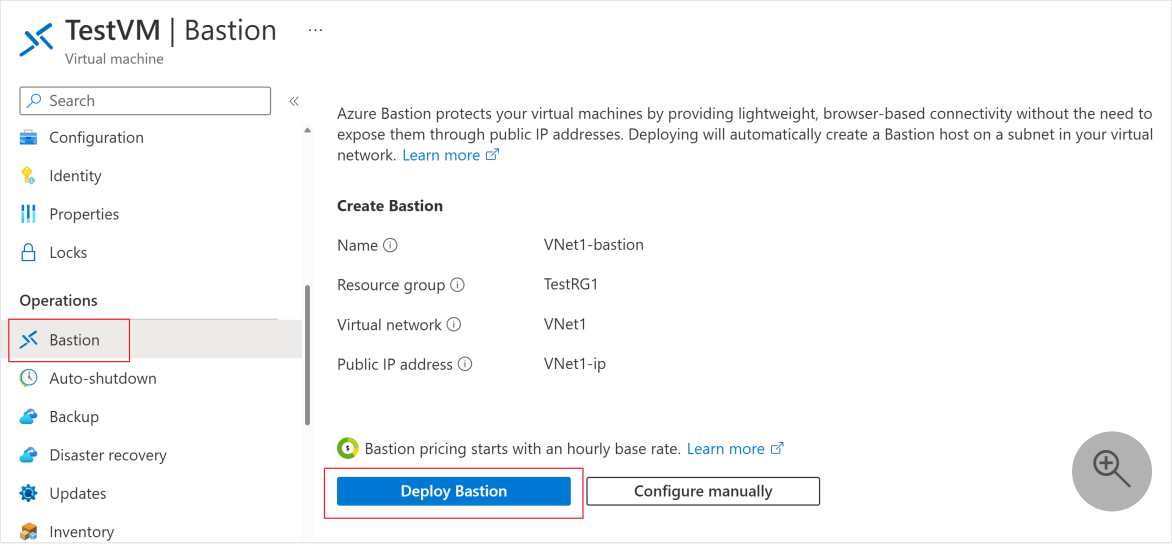
When you create Azure Bastion using default settings, the settings are configured for you. You can't modify or specify additional values for a default deployment. After deployment completes, you can always go to the bastion host **Configuration** page to select additional settings and features. For example, the default SKU is the Basic SKU. You can later upgrade to the Standard SKU to support more features. For more information, see About configuration settings.

1. Sign in to the Azure portal.

2. In the portal, go to the VM to which you want to connect. The values from the virtual network in which this VM resides will be used to create the Bastion deployment.

3. On the page for your VM, in the **Operations** section on the left menu, select **Bastion**. When the **Bastion** page opens, it checks to see if you have enough available address space to create the AzureBastionSubnet. If you don't, you'll see settings to allow you to add more address space to your VNet to meet this requirement.

4. On the **Bastion** page, you can view some of the values that will be used when creating the bastion host for your virtual network. Select **Deploy Bastion** to deploy bastion using default settings.

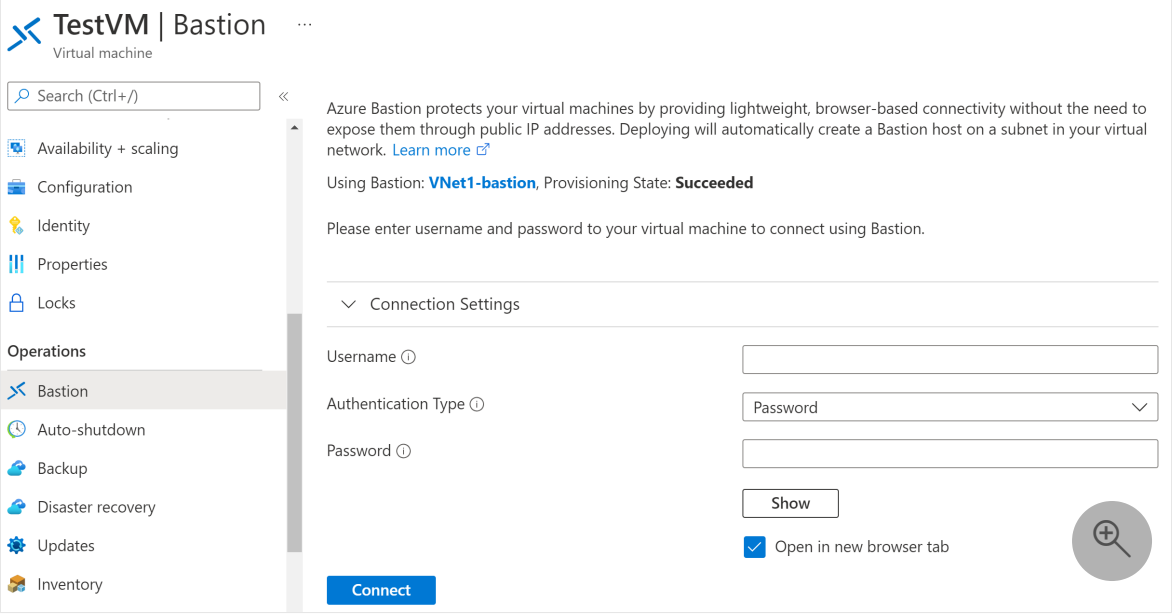


5. Bastion begins deploying. This can take around 10 minutes to complete.

Connect to a VM

When the Bastion deployment is complete, the screen changes to the **Connect** page.

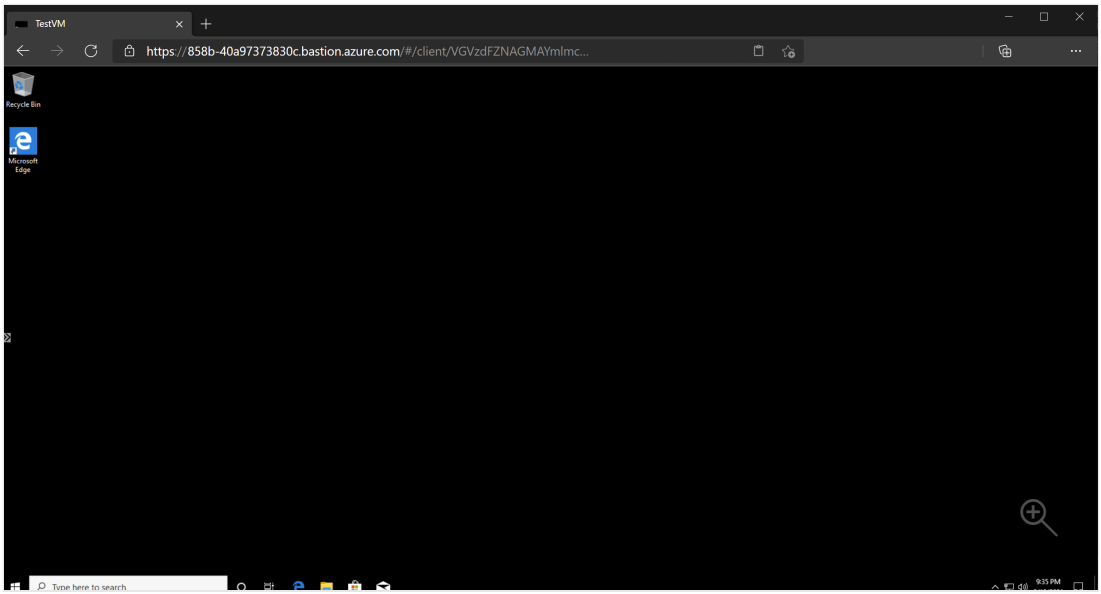
1. Type your authentication credentials. Then, select **Connect**.



2. The connection to this virtual machine via Bastion will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service. Select **Allow** when asked for permissions to the clipboard. This lets you use the remote clipboard arrows on the left of the screen.

   - When you connect, the desktop of the VM may look different than the example screenshot.

   - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

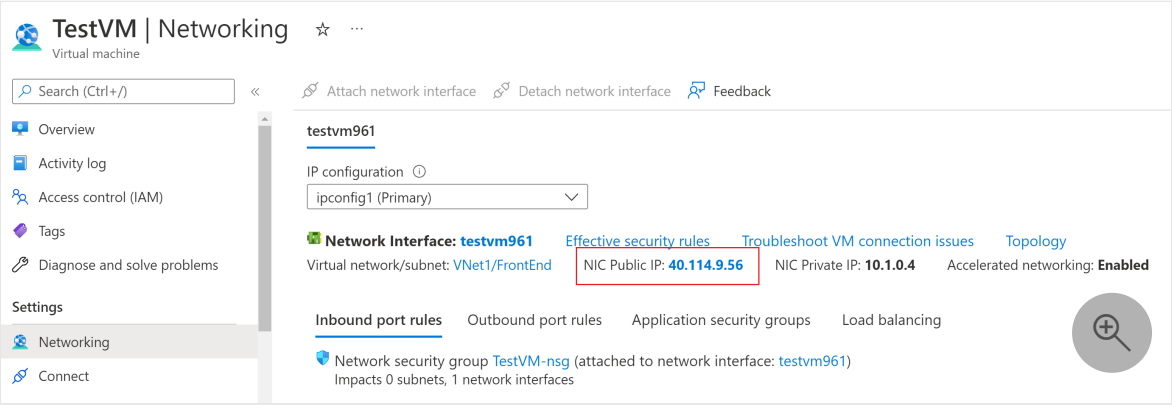
To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

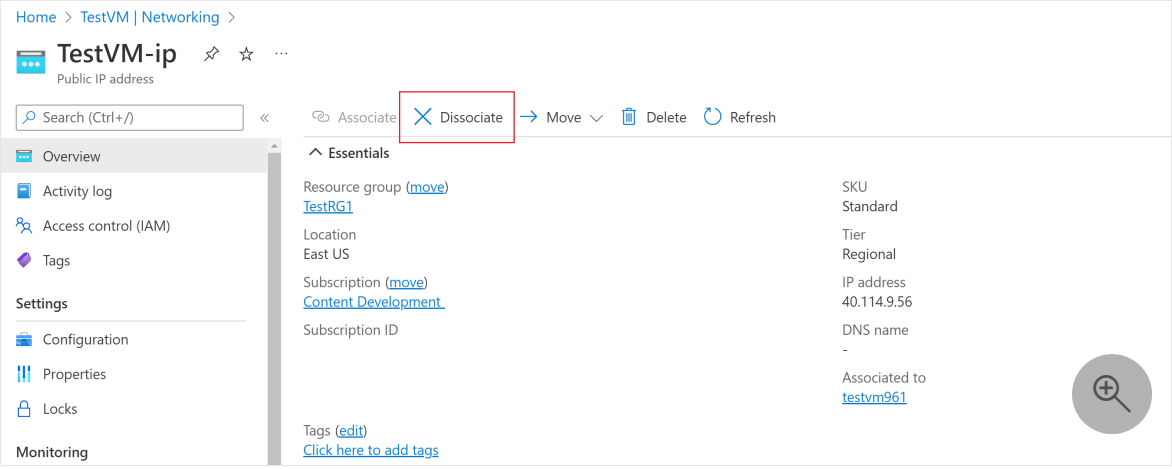
Remove VM public IP address

When you connect to a VM using Azure Bastion, you don't need a public IP address for your VM. If you aren't using the public IP address for anything else, you can dissociate it from your VM. To dissociate a public IP address from your VM, use the following steps:

1. Go to your virtual machine and select **Networking**. Click the **NIC Public IP** to open the Public IP address page.

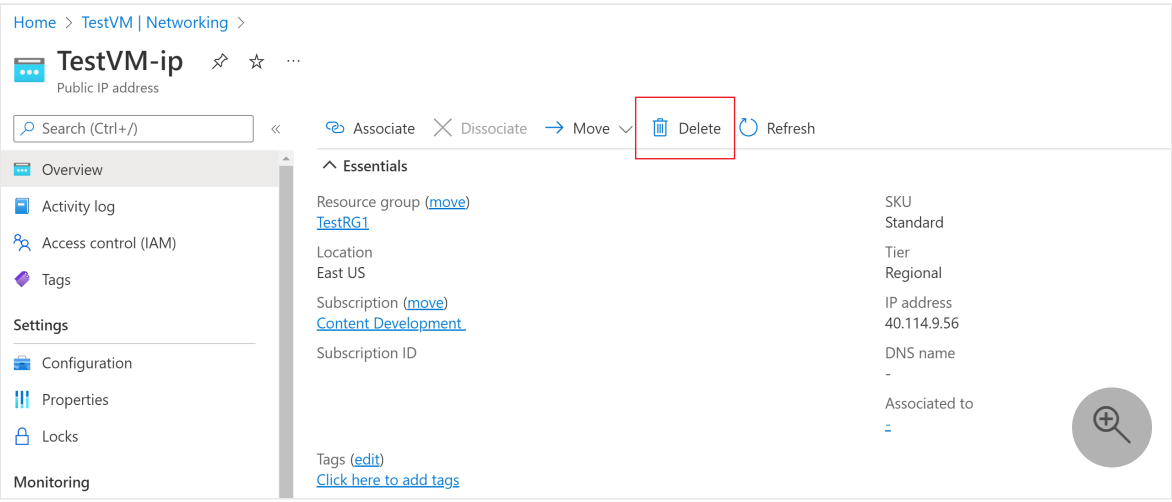


2. On the **Public IP address** page, you can see the VM network interface listed under **Associated to** on the lower right of the page. Click **Dissociate** at the top of the page.



3. Click **Yes** to dissociate the IP address from the network interface. Once the public IP address is dissociated from the VM network interface, you can see that it's no longer listed under **Associated to**.

4. After you dissociate the IP address, you can delete the public IP address resource. On the **Public IP address** page for the VM, select **Delete**.



5. Click **Yes** to delete the public IP address.

Clean up resources

When you're done using the virtual network and the virtual machines, delete the resource group and all of the resources it contains:

1. Enter the name of your resource group in the **Search** box at the top of the portal and select it from the search results.
2. Select **Delete resource group**.
3. Enter your resource group for **TYPE THE RESOURCE GROUP NAME** and select **Delete**.

Next steps

In this quickstart, you deployed Bastion to your virtual network, and then connected to a virtual machine securely via Bastion. Next, you can configure more features and work with VM connections.

VM connections

Azure Bastion configuration settings and features

Quickstart: Deploy Azure Bastion in a virtual network using an ARM template

Article • 06/30/2022 • 3 minutes to read

This quickstart describes how to use Azure Bastion template to deploy to a virtual network.

An ARM template is a JavaScript Object Notation (JSON) file that defines the infrastructure and configuration for your project. The template uses declarative syntax. In declarative syntax, you describe your intended deployment without writing the sequence of programming commands to create the deployment.

If your environment meets the prerequisites and you're familiar with using ARM templates, select the Deploy to Azure button. The template will open in the Azure portal.

Deploy to Azure

Prerequisites

- **An Azure account with an active subscription**. If you don't have one, create one for free.

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Review the template

To view the entire template used for this quickstart, see Azure Quickstart Templates: Azure Bastion as a Service.

This template by default, creates an Azure Bastion deployment with a resource group, a virtual network, network security group settings, an AzureBastionSubnet subnet, a bastion host, and a public IP address resource that's used for the bastion host.

- Microsoft.Network/bastionHosts creates the bastion host.
- Microsoft.Network/virtualNetworks creates a virtual network.

- Microsoft.Network/virtualNetworks/subnets creates the subnet.
- Microsoft Network/networkSecurityGroups controls the network security group settings.
- Microsoft.Network/publicIpAddresses specifies the public IP address value used for the bastion host.

Parameters

PARAMETER NAME	DESCRIPTION
Region	Azure region for Bastion and virtual network.
vnet-name	Name of new or existing virtual network to which Azure Bastion should be deployed.
vnet-ip-prefix	IP prefix for available addresses in virtual network address space.
vnet-new-or-existing	Specify whether to deploy new virtual network or deploy to an existing one.
bastion-subnet-ip-prefix	Bastion subnet IP prefix MUST be within the virtual network IP prefix address space.
bastion-host-name	Name of Azure Bastion resource.

> **Note**
>
> To find more templates, see **Azure Quickstart Templates**.

Deploy the template

In this section, you'll deploy Bastion using the **Deploy to Azure** button below or in the Azure portal. You don't connect and sign in to your virtual machine or deploy Bastion from your VM directly.

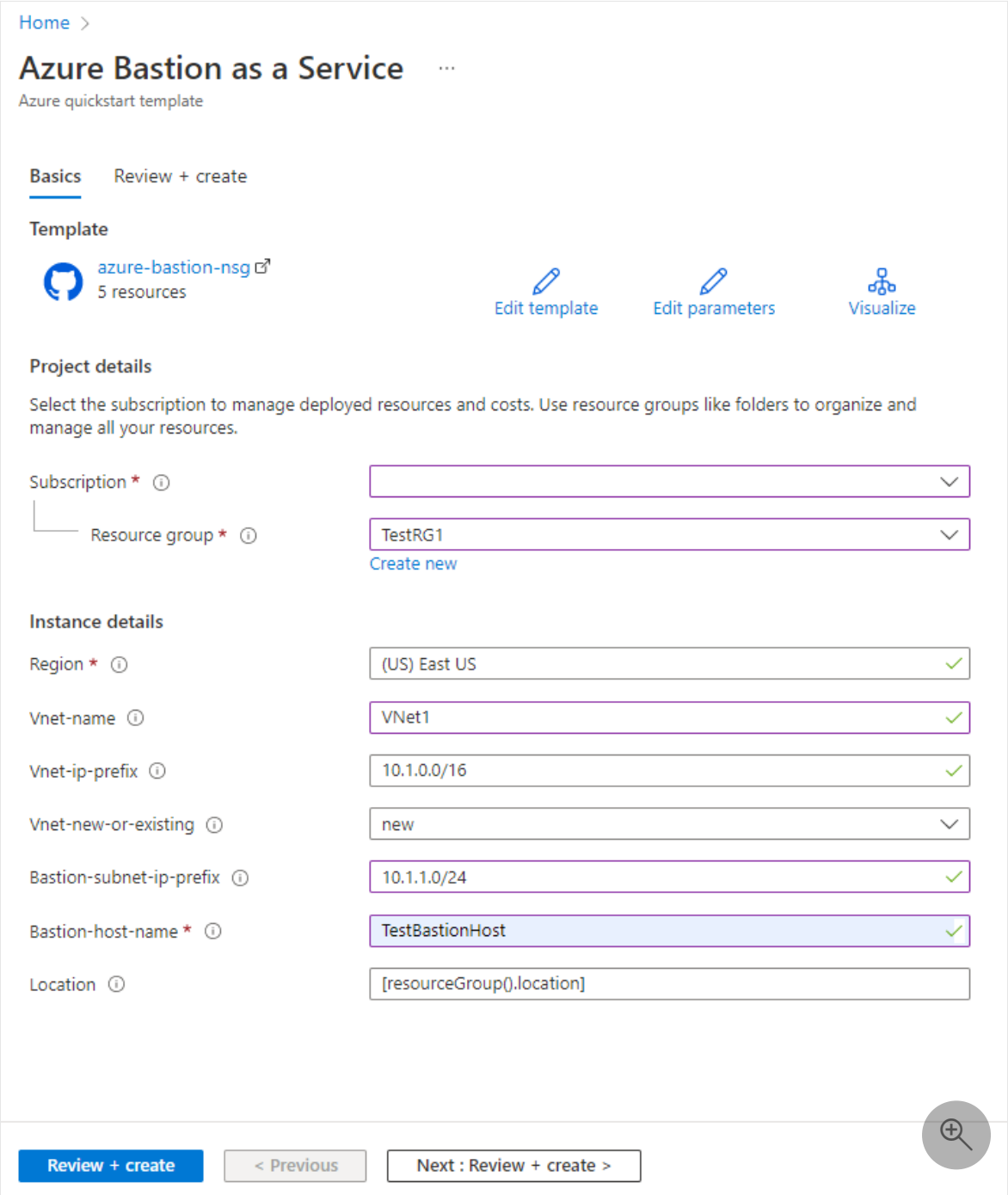
1. Sign in to the Azure portal.

2. Select the **Deploy to Azure** button below.

   Deploy to Azure

3. In the **Azure Bastion as a Service: Azure Quickstart Template**, enter or select the following information.

- If you're using the template for a test environment, you can use the example values specified.
- To view the template, click **Edit template**. On this page, you can adjust some of the values such as address space or the name of certain resources. **Save** to save your changes, or **Discard**.
- If you decide to create your bastion host in an existing VNet, make sure to fill in the values for the template as they are in your deployed environment, or the template will fail.



Setting	Example value
Subscription	Select your Azure subscription

Setting	Example value
Resource Group	Select **Create new** enter **TestRG1**, and select **OK**
Region	Enter **East US**
vnet-name	Enter **VNet1**
vnet-ip-prefix	Enter **10.1.0.0/16**
vnet-new-or-existing	Select **new**
bastion-subnet-ip-prefix	Enter **10.1.1.0/24**
bastion-host-name	Enter **TestBastionHost**

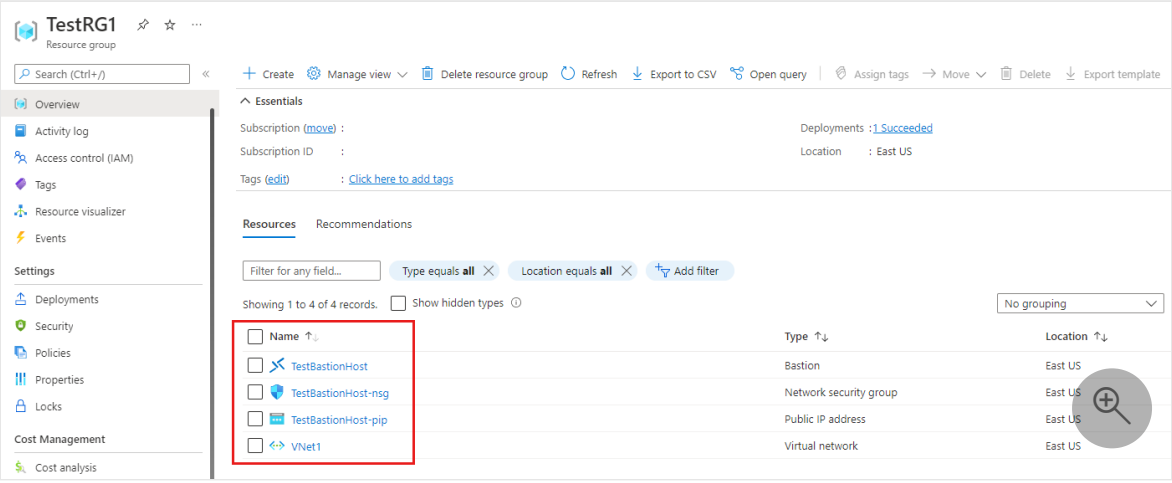
4. Select the **Review + create** tab or select the **Review + create** button. Select **Create**.

5. The deployment will complete within 10 minutes. You can view the progress on the template **Overview** page. If you close the portal, deployment will continue.

Validate the deployment

In this section, you'll validate the deployment of Azure Bastion.

1. Sign in to the Azure portal.
2. Select the **TestRG1** resource group that you created in the previous section.
3. From the Overview page of the resource group, scroll down to **Resources** in the middle pane. Validate the Bastion resource.



Clean up resources

When you're done using the virtual network and the virtual machines, delete the resource group and all of the resources it contains:

1. Enter the name of your resource group in the **Search** box at the top of the portal and select it from the search results.
2. Select **Delete resource group**.
3. Enter your resource group for **TYPE THE RESOURCE GROUP NAME** and select **Delete**.

Next steps

In this quickstart, you deployed Bastion using the Bastion ARM template, and then connected to a virtual machine securely via Bastion. Next, you can continue with the following steps if you want to copy and paste to your virtual machine.

Quickstart: Create a Windows virtual machine in the Azure portal

> Create an RDP connection to a Windows VM using Azure Bastion

Tutorial: Deploy Bastion using specified settings

Article • 09/21/2022 • 9 minutes to read

This tutorial helps you deploy Azure Bastion from the Azure portal using your own specified manual settings. When you use manual settings, you can specify configuration values such as instance counts and the SKU at the time of deployment. After Bastion is deployed, you can connect (SSH/RDP) to virtual machines in the virtual network via Bastion using the private IP address of the VM. When you connect to a VM, it doesn't need a public IP address, client software, agent, or a special configuration.

In this tutorial, you deploy Bastion using the Standard SKU tier and adjust host scaling (instance count). After the deployment is complete, you connect to your VM via private IP address. If your VM has a public IP address that you don't need for anything else, you can remove it.

Azure Bastion is a PaaS service that's maintained for you, not a bastion host that you install on one of your VMs and maintain yourself. For more information about Azure Bastion, see What is Azure Bastion?

In this tutorial, you'll learn how to:

- ✓ Deploy Bastion to your VNet.
- ✓ Connect to a virtual machine.
- ✓ Remove the public IP address from a virtual machine.

If you don’t have an Azure subscription, create a free account before you begin.

Prerequisites

- A virtual network. This will be the VNet to which you deploy Bastion.
- A virtual machine in the virtual network. This VM isn't a part of the Bastion configuration and doesn't become a bastion host. You connect to this VM later in this tutorial via Bastion. If you don't have a VM, create one using Quickstart: Create a VM.
- **Required VM roles:**
  - Reader role on the virtual machine.
  - Reader role on the NIC with private IP of the virtual machine.

- **Required inbound ports:**
  - For Windows VMs - RDP (3389)
  - For Linux VMs - SSH (22)

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Example values

You can use the following example values when creating this configuration, or you can substitute your own.

Basic VNet and VM values:

Name	Value
Virtual machine	TestVM
Resource group	TestRG1
Region	East US
Virtual network	VNet1
Address space	10.1.0.0/16
Subnets	FrontEnd: 10.1.0.0/24

Azure Bastion values:

Name	Value
Name	VNet1-bastion
+ Subnet Name	AzureBastionSubnet
AzureBastionSubnet addresses	A subnet within your VNet address space with a subnet mask /26 or larger. For example, 10.1.1.0/26.
Tier/SKU	Standard
Instance count (host scaling)	3 or greater

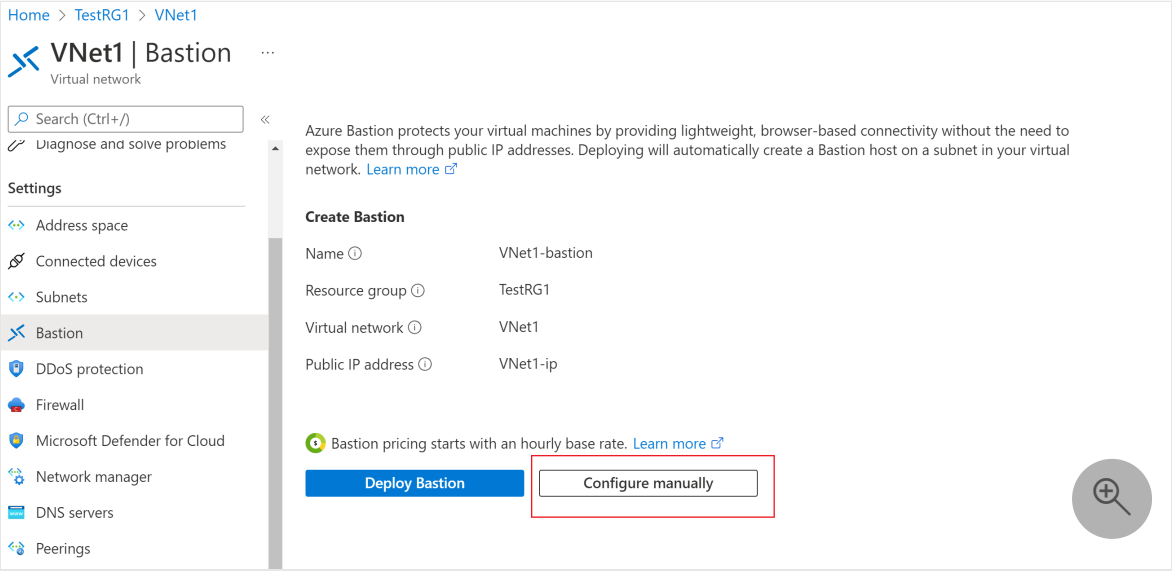
Name	Value
Public IP address	Create new
Public IP address name	VNet1-ip
Public IP address SKU	Standard
Assignment	Static

> **Important**
>
> For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

Deploy Bastion

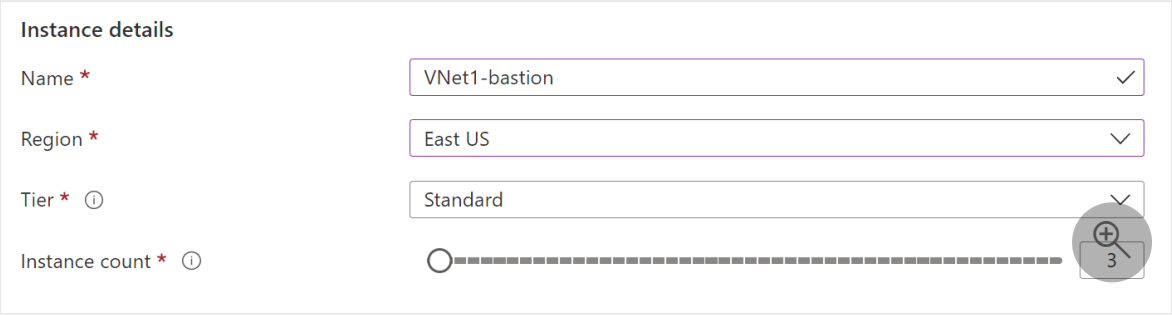
This section helps you deploy Bastion to your VNet. Once Bastion is deployed, you can connect securely to any VM in the VNet using its private IP address.

1. Sign in to the Azure portal.
2. Go to your virtual network.
3. On the page for your virtual network, in the left pane, select **Bastion** to open the **Bastion** page.
4. On the Bastion page, select **Configure manually**. This lets you configure specific additional settings when deploying Bastion to your VNet.



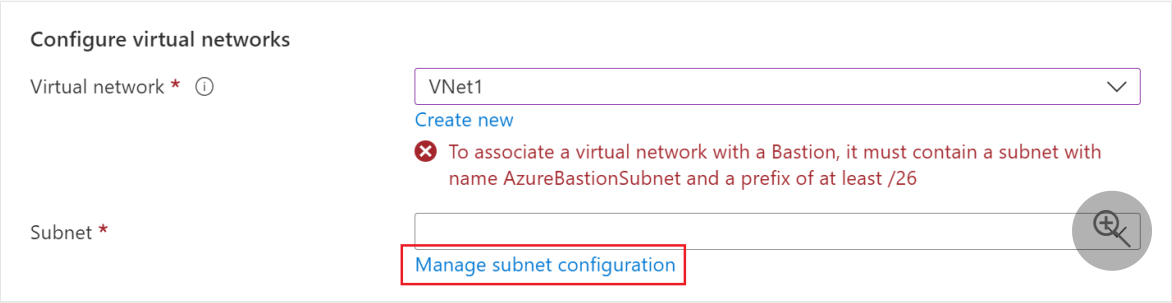
5. On the **Create a Bastion** page, configure the settings for your bastion host. Project details are populated from your virtual network values. Configure the **Instance details** values.

   - **Name**: Type the name that you want to use for your bastion resource.
   - **Region**: The Azure public region in which the resource will be created. Choose the region in which your virtual network resides.
   - **Tier:** The tier is also known as the **SKU**. For this tutorial, select **Standard**. The Standard SKU lets you configure the instance count for host scaling and other features. For more information about features that require the Standard SKU, see Configuration settings - SKU.
   - **Instance count:** This is the setting for **host scaling**. It's configured in scale unit increments. Use the slider or type a number to configure the instance count that you want. For this tutorial, you can select the instance count you'd prefer. For more information, see Host scaling and Pricing .



6. Configure the **virtual networks** settings. Select your VNet from the dropdown. If you don't see your VNet in the dropdown list, make sure you selected the correct Region in the previous settings on this page.

7. To configure the AzureBastionSubnet, select **Manage subnet configuration**.



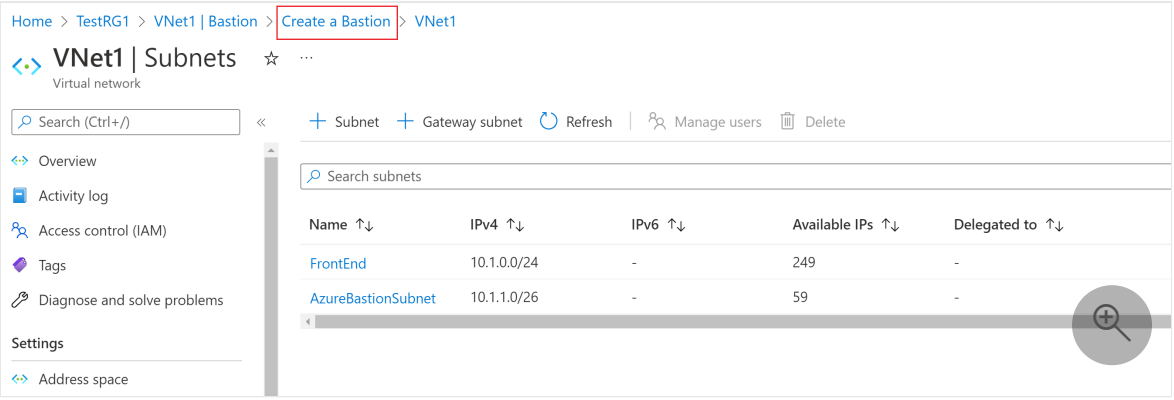
8. On the **Subnets** page, select **+Subnet** to open the **Add subnet** page.

9. On the **Add subnet page**, create the 'AzureBastionSubnet' subnet using the following values. Leave the other values as default.

   - The subnet name must be **AzureBastionSubnet**.
   - The subnet must be at least **/26 or larger** (/26, /25, /24 etc.) to accommodate features available with the Standard SKU.

   Select **Save** at the bottom of the page to save your values.

10. At the top of the **Subnets** page, select **Create a Bastion** to return to the Bastion configuration page.



11. The **Public IP address** section is where you configure the public IP address of the Bastion host resource on which RDP/SSH will be accessed (over port 443). The public IP address must be in the same region as the Bastion resource you're creating. Create a new IP address. You can leave the default naming suggestion.

12. When you finish specifying the settings, select **Review + Create**. This validates the values.

13. Once validation passes, you can deploy Bastion. Select **Create**. You'll see a message letting you know that your deployment is in process. Status will display on this page as the resources are created. It takes about 10 minutes for the Bastion resource to be created and deployed.

Connect to a VM

You can use any of the following detailed articles to connect to a VM. Some connection types require the Bastion Standard SKU.

- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

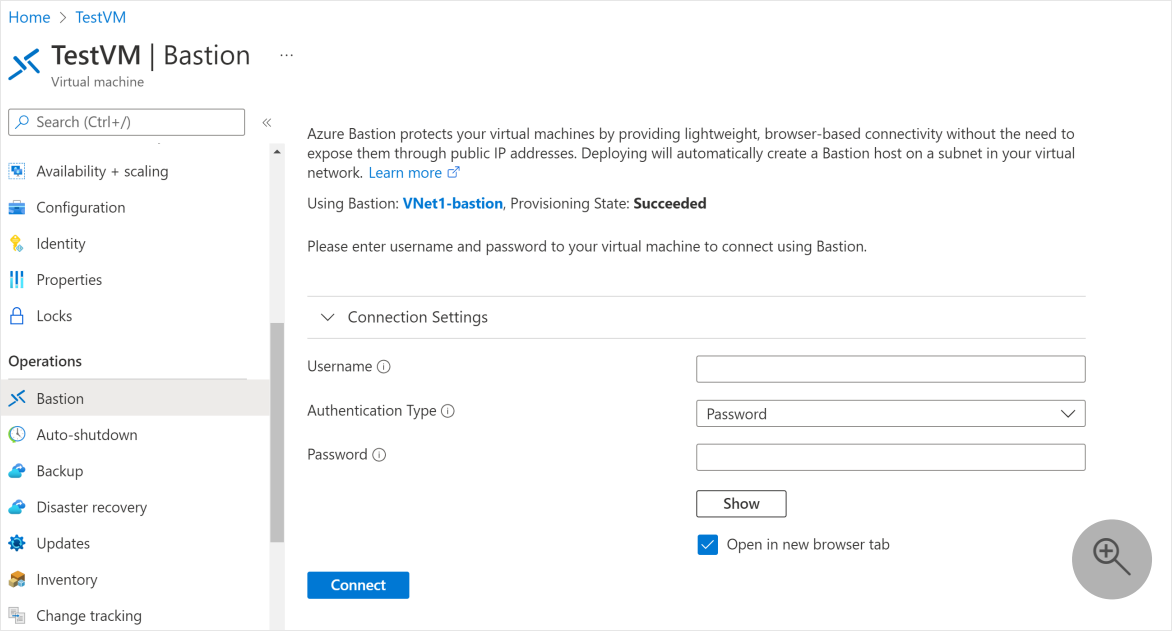
You can also use the basic Connection steps in the section below to connect to your VM.

Connection steps

1. In the Azure portal, go to the virtual machine to which you want to connect.

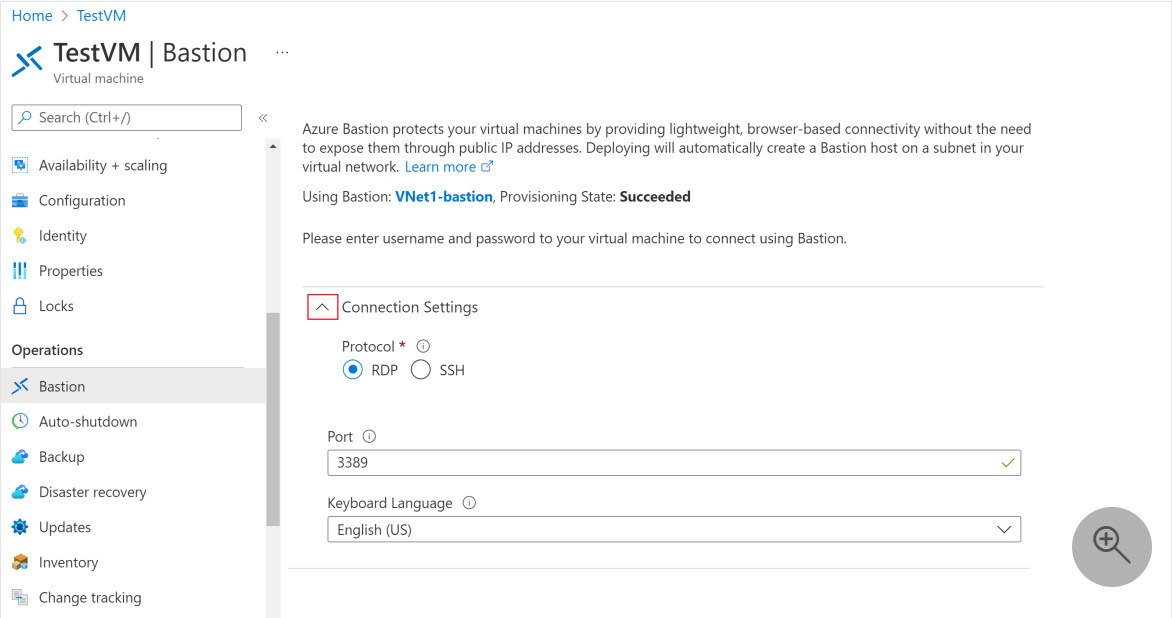
2. At the top of the page, select **Connect->Bastion** to go to the **Bastion** page. You can also go to the Bastion page using the left menu.

3. The options available on the **Bastion** page are dependant on the Bastion SKU tier. If you're using the **Basic SKU**, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22. You don't have options to change the port number or the protocol. However, you can change the keyboard language for RDP by expanding **Connection Settings**.

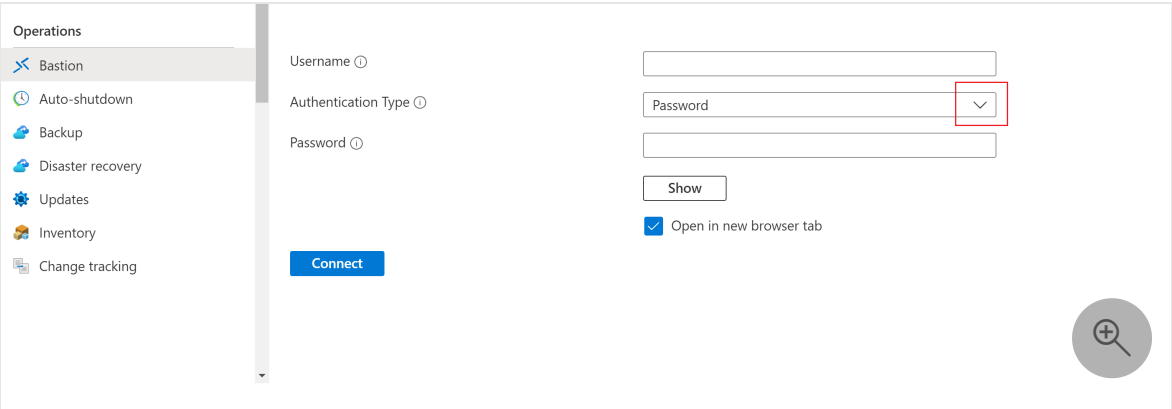


If you're using the **Standard SKU**, you have more connection protocol and port options available. Expand **Connection Settings** to see the options. Typically, unless

you have configured different settings for your VM, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22.



4. Select the **Authentication Type** from the dropdown. The protocol determines the available authentication types. Complete the required authentication values.



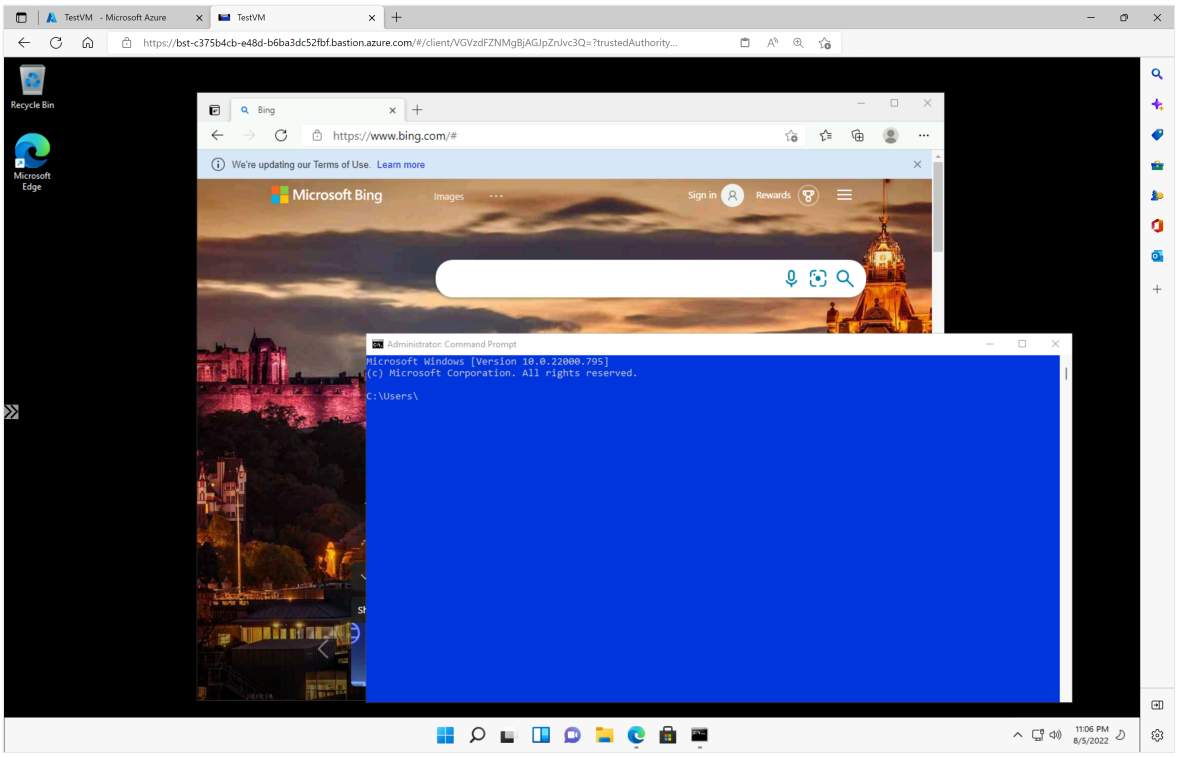
5. To open the VM session in a new browser tab, leave **Open in a new browser tab** selected.

6. Click **Connect** to connect to the VM.

7. The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

    - When you connect, the desktop of the VM will look different than the example screenshot.
    - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from

a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

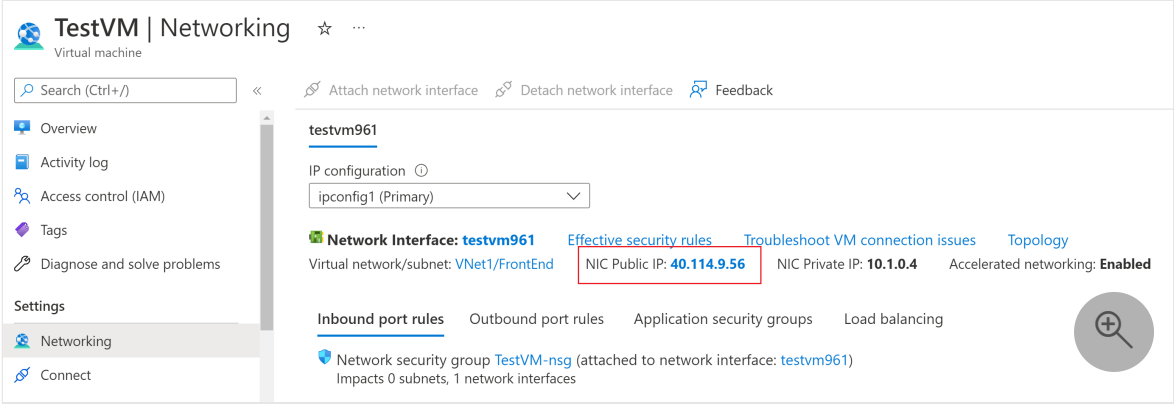
To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

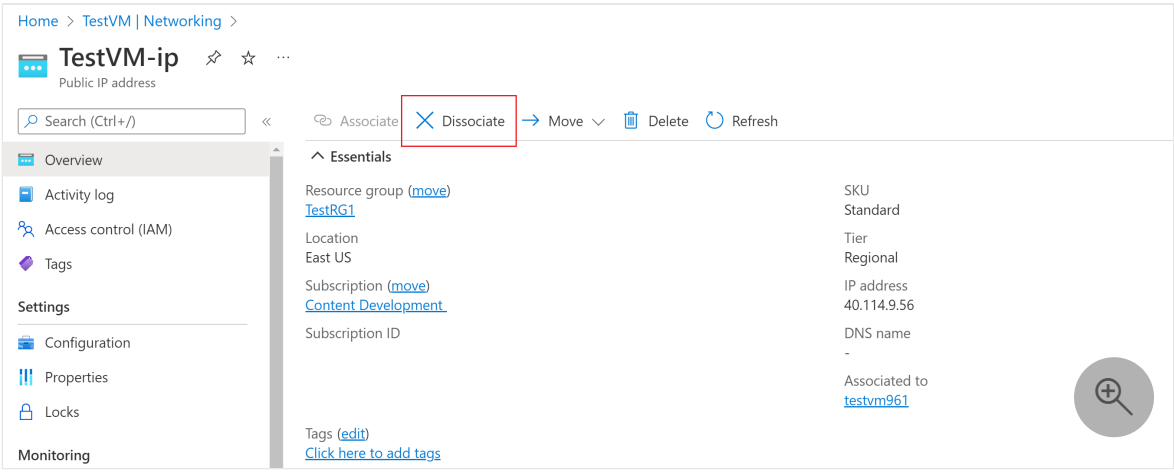
Remove VM public IP address

When you connect to a VM using Azure Bastion, you don't need a public IP address for your VM. If you aren't using the public IP address for anything else, you can dissociate it from your VM. To dissociate a public IP address from your VM, use the following steps:

1. Go to your virtual machine and select **Networking**. Click the **NIC Public IP** to open the Public IP address page.

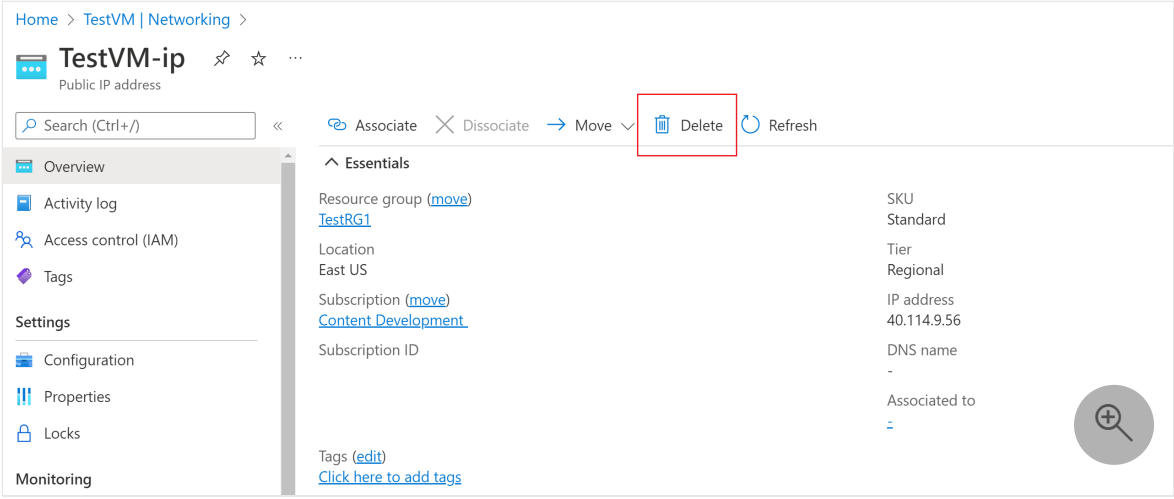


2. On the **Public IP address** page, you can see the VM network interface listed under **Associated to** on the lower right of the page. Click **Dissociate** at the top of the page.



3. Click **Yes** to dissociate the IP address from the network interface. Once the public IP address is dissociated from the VM network interface, you can see that it's no longer listed under **Associated to**.

4. After you dissociate the IP address, you can delete the public IP address resource. On the **Public IP address** page for the VM, select **Delete**.



5. Click **Yes** to delete the public IP address.

Clean up resources

If you're not going to continue to use this application, delete your resources using the following steps:

1. Enter the name of your resource group in the **Search** box at the top of the portal. When you see your resource group in the search results, select it.
2. Select **Delete resource group**.
3. Enter the name of your resource group for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

Next steps

In this tutorial, you deployed Bastion to a virtual network and connected to a VM. You then removed the public IP address from the VM. Next, learn about and configure additional Bastion features.

Bastion features and configuration settings

Bastion - VM connections and features

Tutorial: Protect your Bastion host with Azure DDoS protection

Article • 02/01/2023 • 9 minutes to read

This article helps you create an Azure Bastion host with a DDoS protected virtual network. Azure DDoS protection protects your publicly accessible bastion host from Distributed Denial of Service attacks.

> **Important**
>
> Azure DDoS Protection incurs a cost when you use the Standard SKU. Overages charges only apply if more than 100 public IPs are protected in the tenant. Ensure you delete the resources in this tutorial if you aren't using the resources in the future. For information about pricing, see **Azure DDoS Protection Pricing**. For more information about Azure DDoS protection, see **What is Azure DDoS Protection?**.

In this tutorial, you'll learn how to:

- ✓ Deploy Bastion to your VNet.
- ✓ Create a DDoS protection plan and enable DDoS protection.
- ✓ Connect to a virtual machine.
- ✓ Remove the public IP address from a virtual machine.

If you don't have an Azure subscription, create a free account before you begin.

Prerequisites

- A virtual network. This will be the VNet to which you deploy Bastion.
- A virtual machine in the virtual network. This VM isn't a part of the Bastion configuration and doesn't become a bastion host. You connect to this VM later in this tutorial via Bastion. If you don't have a VM, create one using Quickstart: Create a VM.
- **Required VM roles:**
  - Reader role on the virtual machine.
  - Reader role on the NIC with private IP of the virtual machine.
- **Required inbound ports:**

- For Windows VMs - RDP (3389)
- For Linux VMs - SSH (22)

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Example values

You can use the following example values when creating this configuration, or you can substitute your own.

Basic VNet and VM values:

Name	Value
Virtual machine	TestVM
Resource group	TestRG1
Region	East US
Virtual network	VNet1
Address space	10.1.0.0/16
Subnets	FrontEnd: 10.1.0.0/24

Azure Bastion values:

Name	Value
Name	VNet1-bastion
+ Subnet Name	AzureBastionSubnet
AzureBastionSubnet addresses	A subnet within your VNet address space with a subnet mask /26 or larger. For example, 10.1.1.0/26.
Tier/SKU	Standard
Instance count (host scaling)	3 or greater

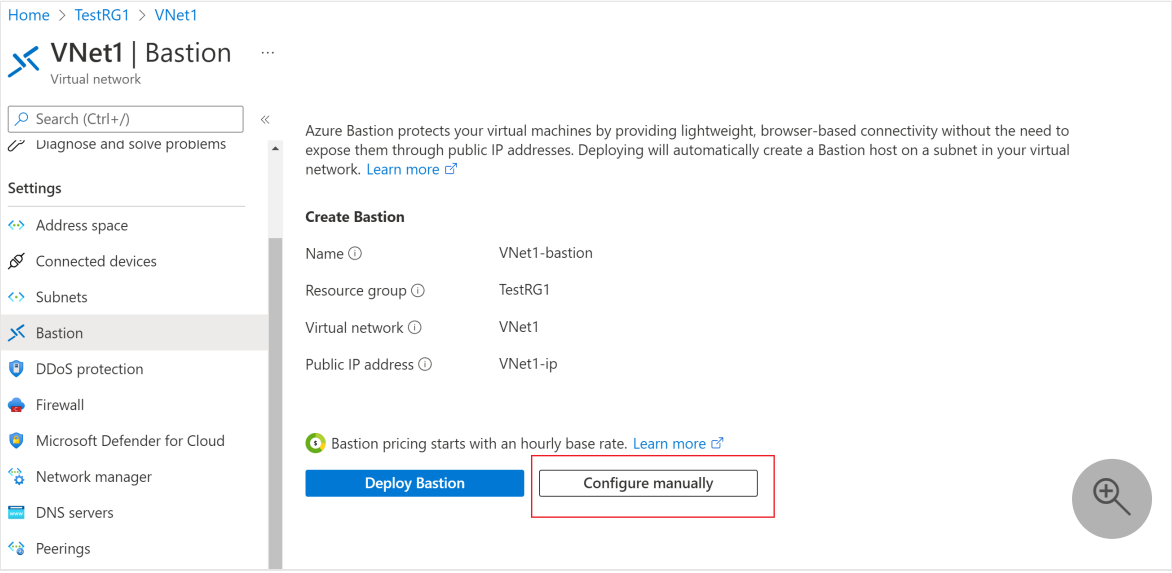
Name	Value
Public IP address	Create new
Public IP address name	VNet1-ip
Public IP address SKU	Standard
Assignment	Static

> **Important**
>
> For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

Deploy Bastion

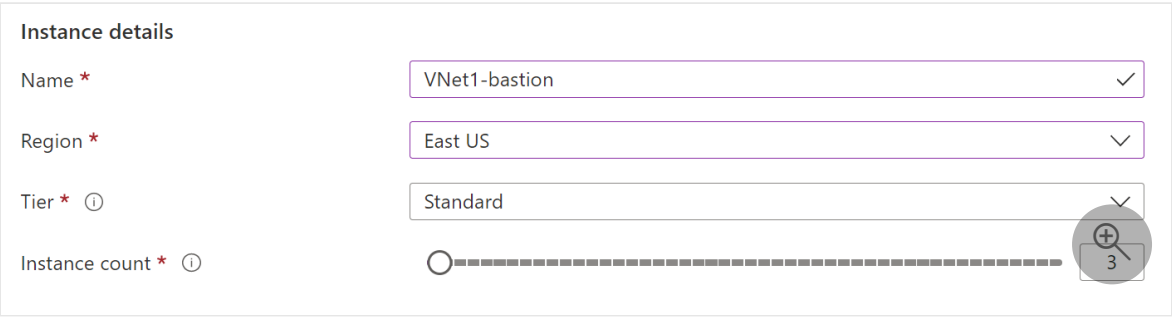
This section helps you deploy Bastion to your VNet. Once Bastion is deployed, you can connect securely to any VM in the VNet using its private IP address.

1. Sign in to the Azure portal.
2. Go to your virtual network.
3. On the page for your virtual network, in the left pane, select **Bastion** to open the **Bastion** page.
4. On the Bastion page, select **Configure manually**. This lets you configure specific additional settings when deploying Bastion to your VNet.



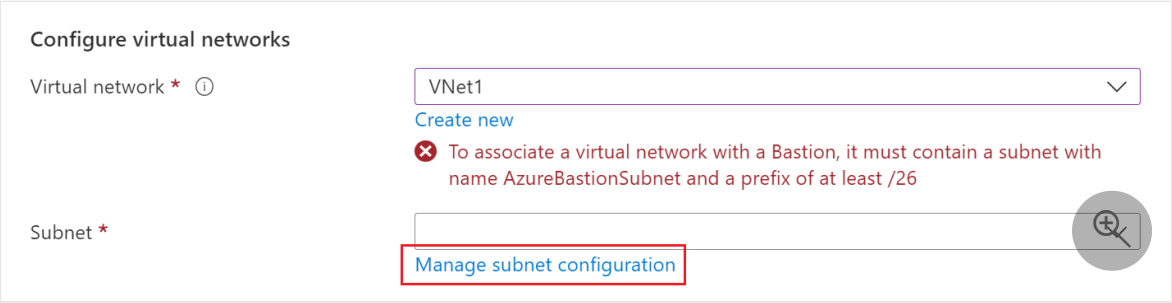
5. On the **Create a Bastion** page, configure the settings for your bastion host. Project details are populated from your virtual network values. Configure the **Instance details** values.

   - **Name**: Type the name that you want to use for your bastion resource.
   - **Region**: The Azure public region in which the resource will be created. Choose the region in which your virtual network resides.
   - **Tier:** The tier is also known as the **SKU**. For this tutorial, select **Standard**. The Standard SKU lets you configure the instance count for host scaling and other features. For more information about features that require the Standard SKU, see Configuration settings - SKU.
   - **Instance count:** This is the setting for **host scaling**. It's configured in scale unit increments. Use the slider or type a number to configure the instance count that you want. For this tutorial, you can select the instance count you'd prefer. For more information, see Host scaling and Pricing .



6. Configure the **virtual networks** settings. Select your VNet from the dropdown. If you don't see your VNet in the dropdown list, make sure you selected the correct Region in the previous settings on this page.

7. To configure the AzureBastionSubnet, select **Manage subnet configuration**.



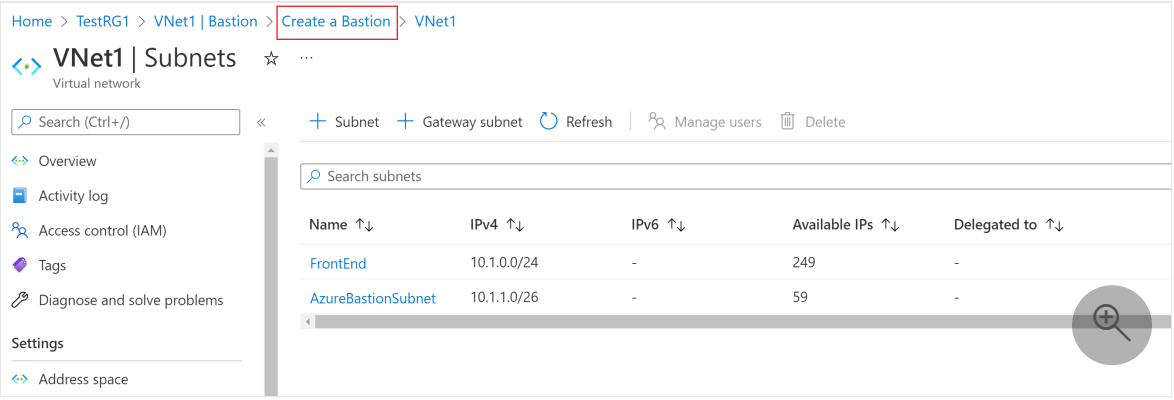
8. On the **Subnets** page, select **+Subnet** to open the **Add subnet** page.

9. On the **Add subnet page**, create the 'AzureBastionSubnet' subnet using the following values. Leave the other values as default.

   - The subnet name must be **AzureBastionSubnet**.
   - The subnet must be at least **/26 or larger** (/26, /25, /24 etc.) to accommodate features available with the Standard SKU.

   Select **Save** at the bottom of the page to save your values.

10. At the top of the **Subnets** page, select **Create a Bastion** to return to the Bastion configuration page.



11. The **Public IP address** section is where you configure the public IP address of the Bastion host resource on which RDP/SSH will be accessed (over port 443). The public IP address must be in the same region as the Bastion resource you're creating. Create a new IP address. You can leave the default naming suggestion.

12. When you finish specifying the settings, select **Review + Create**. This validates the values.

13. Once validation passes, you can deploy Bastion. Select **Create**. You'll see a message letting you know that your deployment is in process. Status will display on this page as the resources are created. It takes about 10 minutes for the Bastion resource to be created and deployed.

Enable Azure DDoS protection

This section helps you create an Azure DDoS protection and enable the service on the virtual network.

1. In the search box in the portal, enter **DDoS protection**. Select **DDoS protection plans** in the search results.
2. Select **+ Create**.
3. In the **Basics** tab of **Create a DDoS protection plan**, enter or select the following information:

Setting	Value
Project details	
Subscription	Select your subscription.
Resource group	Select your resource group.
Name	Enter a name for the DDoS protection plan.
Region	Select the region.

4. Select **Review + create**.
5. Select **Create**.
6. In the search box in the portal, enter **Virtual network**. Select **Virtual networks** in the search results.
7. Select your virtual network.
8. In **Settings**, select **DDoS protection**.
9. Select **Enable**.
10. Select the pull-down box in **DDoS protection plan**. Select the protection plan you created in the previous steps.
11. Select **Save**.

Connect to a VM

You can use any of the following detailed articles to connect to a VM. Some connection types require the Bastion Standard SKU.

- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

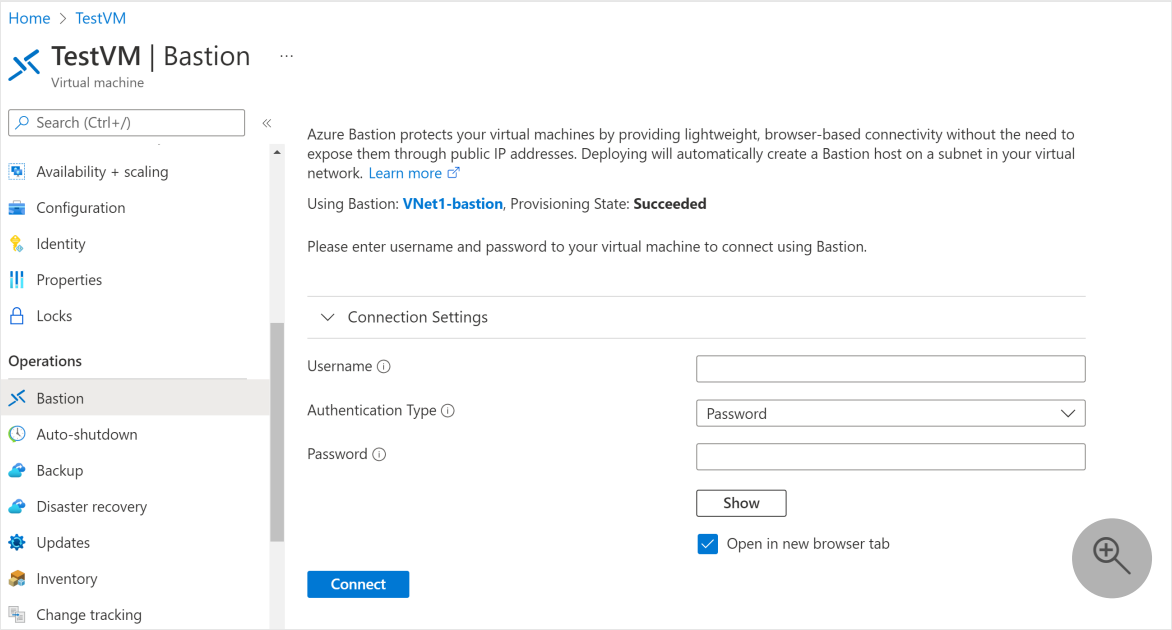
You can also use the basic Connection steps in the section below to connect to your VM.

Connection steps

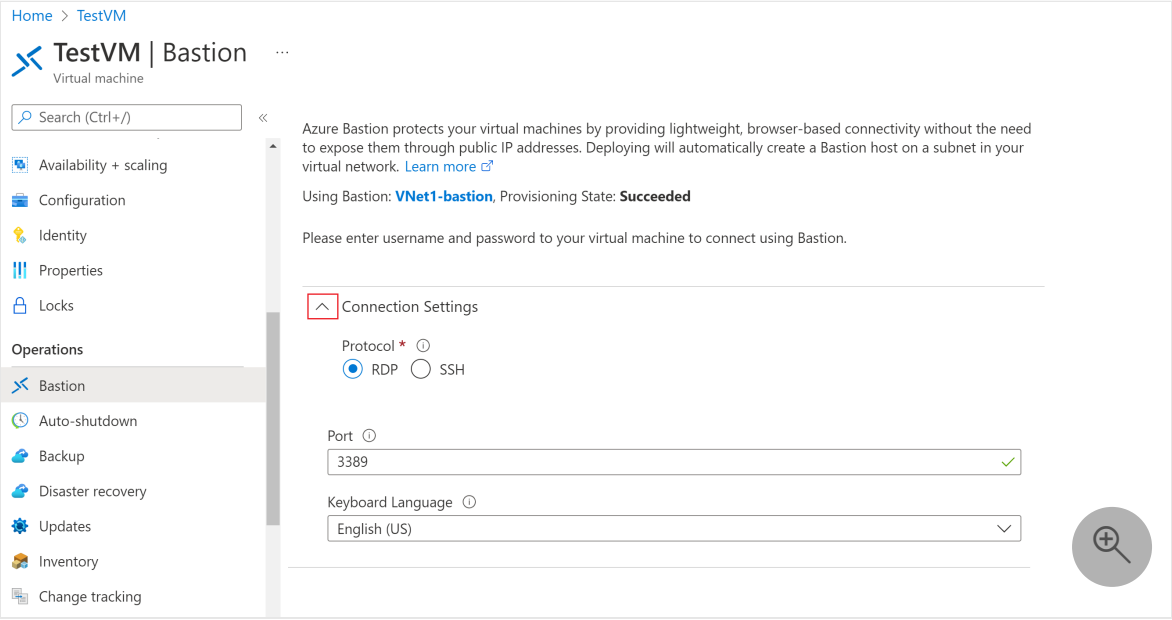
1. In the Azure portal, go to the virtual machine to which you want to connect.

2. At the top of the page, select **Connect->Bastion** to go to the **Bastion** page. You can also go to the Bastion page using the left menu.

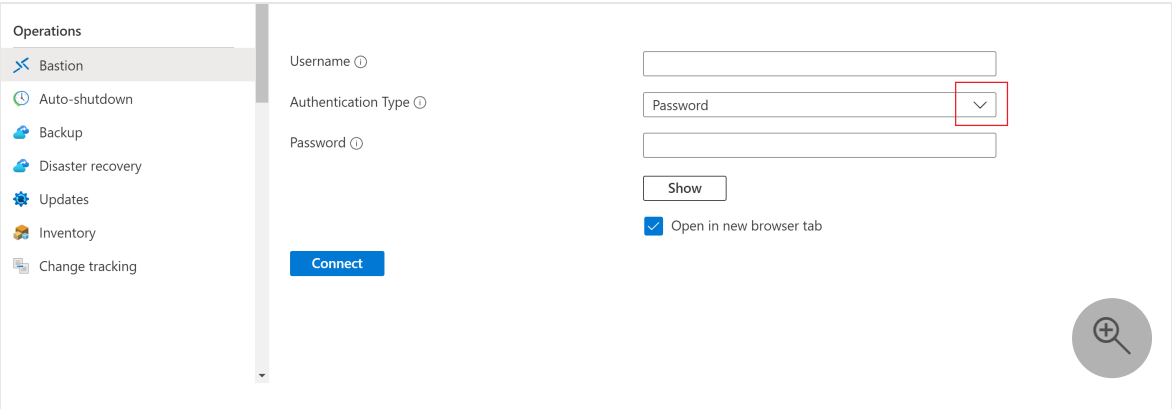
3. The options available on the **Bastion** page are dependant on the Bastion SKU tier. If you're using the **Basic SKU**, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22. You don't have options to change the port number or the protocol. However, you can change the keyboard language for RDP by expanding **Connection Settings**.



If you're using the **Standard SKU**, you have more connection protocol and port options available. Expand **Connection Settings** to see the options. Typically, unless you have configured different settings for your VM, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22.



4. Select the **Authentication Type** from the dropdown. The protocol determines the available authentication types. Complete the required authentication values.

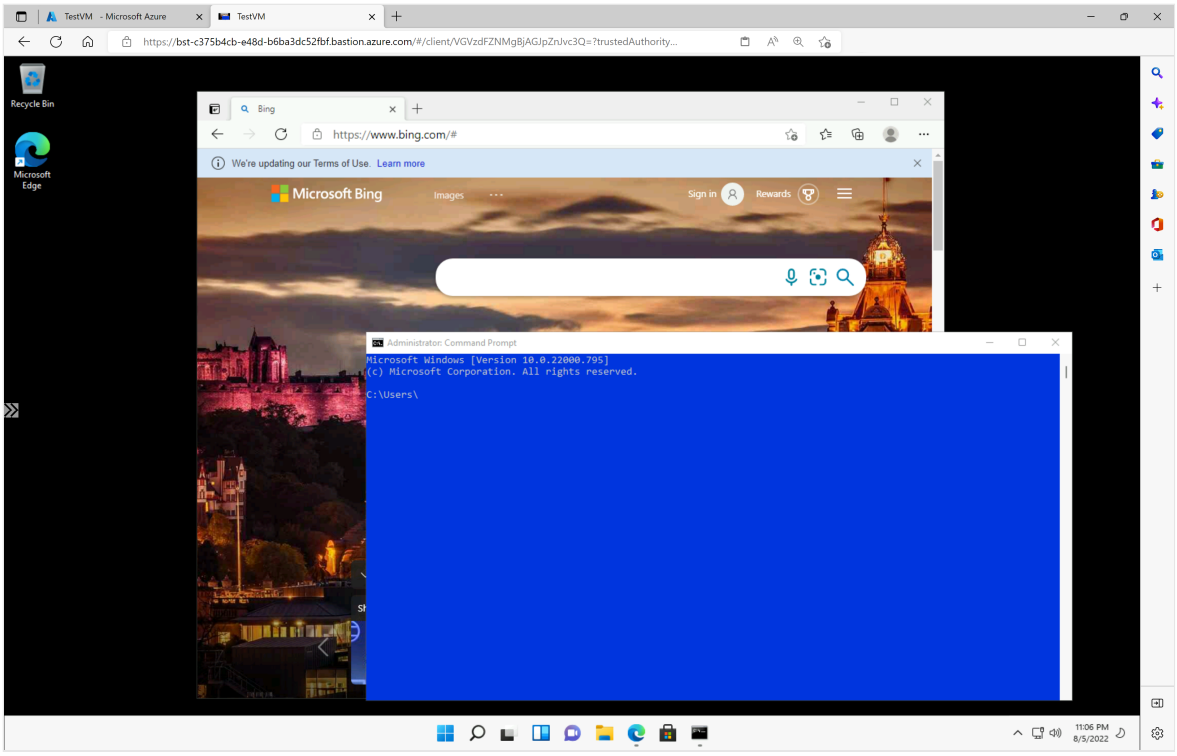


5. To open the VM session in a new browser tab, leave **Open in a new browser tab** selected.

6. Click **Connect** to connect to the VM.

7. The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

    - When you connect, the desktop of the VM will look different than the example screenshot.
    - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

To enable remote audio output on a Windows VM:

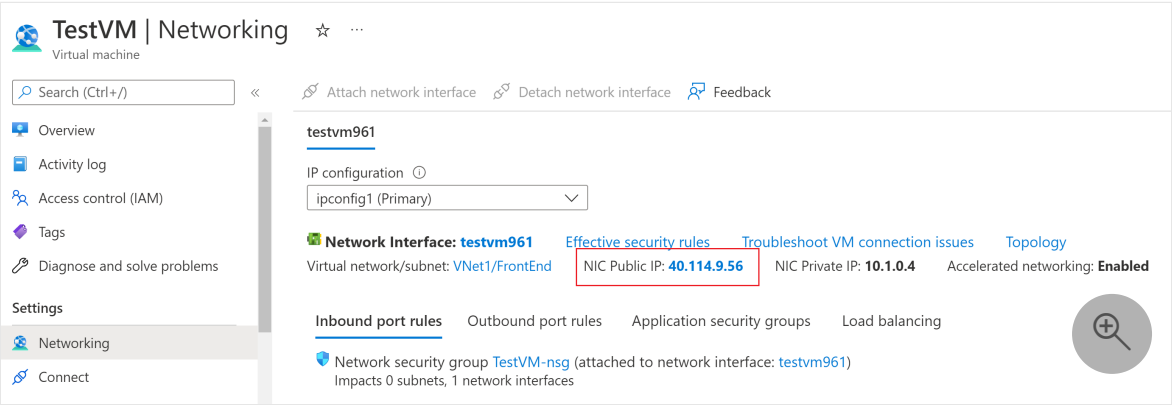
1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

Remove VM public IP address

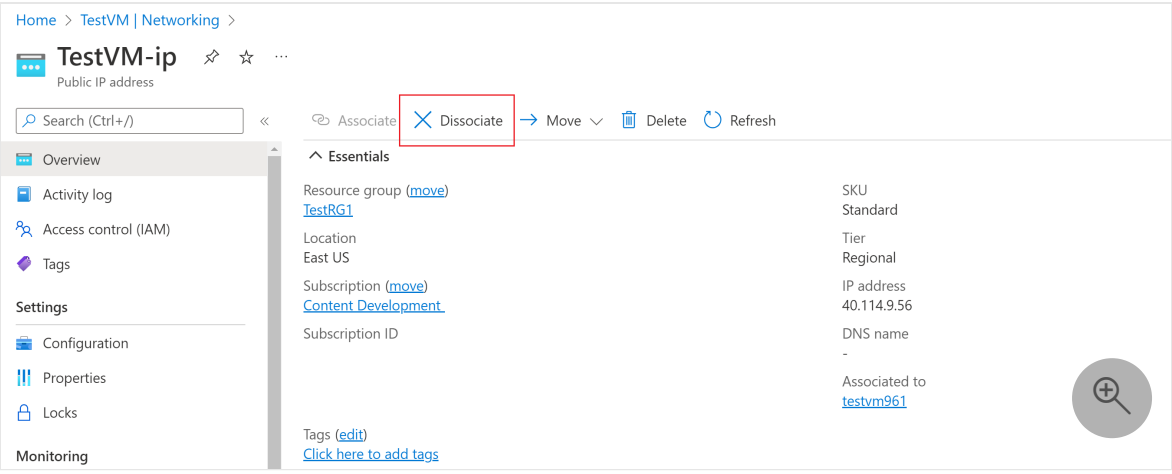
When you connect to a VM using Azure Bastion, you don't need a public IP address for your VM. If you aren't using the public IP address for anything else, you can dissociate it

from your VM. To dissociate a public IP address from your VM, use the following steps:

1. Go to your virtual machine and select **Networking**. Click the **NIC Public IP** to open the Public IP address page.

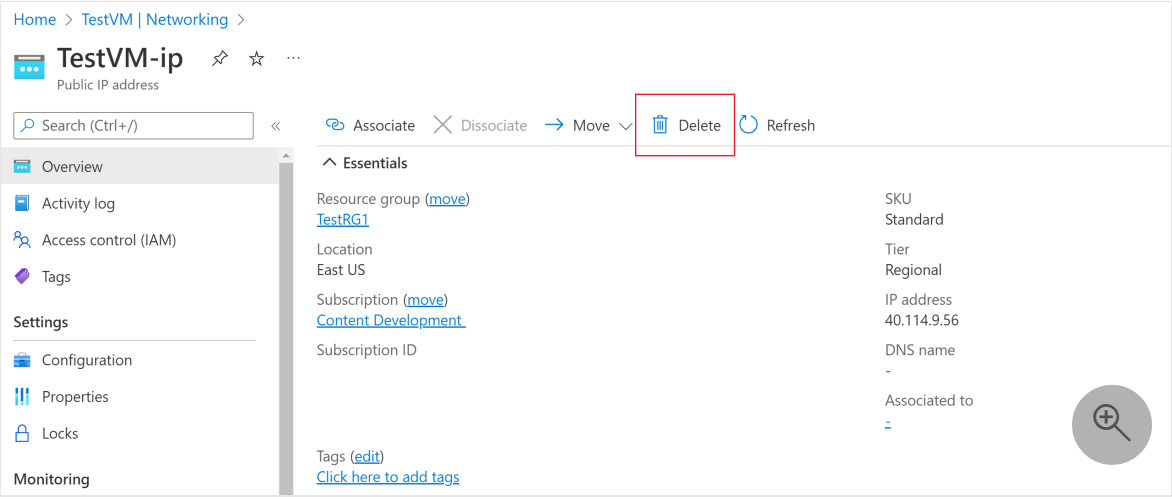


2. On the **Public IP address** page, you can see the VM network interface listed under **Associated to** on the lower right of the page. Click **Dissociate** at the top of the page.



3. Click **Yes** to dissociate the IP address from the network interface. Once the public IP address is dissociated from the VM network interface, you can see that it's no longer listed under **Associated to**.

4. After you dissociate the IP address, you can delete the public IP address resource. On the **Public IP address** page for the VM, select **Delete**.



5. Click **Yes** to delete the public IP address.

Clean up resources

If you're not going to continue to use this application, delete your resources using the following steps:

1. Enter the name of your resource group in the **Search** box at the top of the portal. When you see your resource group in the search results, select it.
2. Select **Delete resource group**.
3. Enter the name of your resource group for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

Next steps

In this tutorial, you deployed Bastion to a virtual network and connected to a VM. You then removed the public IP address from the VM. Next, learn about and configure additional Bastion features.

Bastion features and configuration settings

Bastion - VM connections and features

Additional resources

Enable remote work by using Azure networking services

Article • 02/28/2023 • 6 minutes to read

This article describes the options that are available to organizations to set up remote access for their users or to supplement their existing solutions with additional capacity during periods of peak utilization.

Network architects are faced with the following challenges:

- Address an increase in network utilization.
- Provide reliable and secure connectivity to more employees of their company and customers.
- Provide connectivity to remote locations across the globe.

Not all networks (for example, private WAN and corporate core networks) experience congestion from peak loads of remote workers. The bottlenecks are commonly reported only in home broadband networks and in VPN gateways of on-premises networks of corporations.

Network planners can help ease bottlenecks and alleviate network congestion by keeping in mind that different traffic types need different network treatment priorities. Some traffic requires smart load redirection or redistribution.

For example, real-time telemedicine traffic of doctor/patient interaction has a high importance and is sensitive to delay or jitter. Replication of traffic between storage solutions is not delay sensitive. Telemedicine traffic must be routed via the most optimal network path with a high quality of service, whereas it's acceptable to use a suboptimal route for traffic between storage solutions.

Elasticity and high availability in the Microsoft network

Azure is designed to withstand sudden changes in resource utilization and to keep systems running during periods of peak utilization.

Microsoft maintains and operates one of the world's largest networks. The Microsoft network has been designed for high availability to withstand various types of failures, from failure of a single network element to failure of an entire region.

The Microsoft network is also designed to handle various types of network traffic. This traffic can include delay-sensitive multimedia traffic for Skype and Teams, content delivery networks, real-time big data analysis, Azure Storage, Bing, and Xbox. To provide optimal performance, the Microsoft network attracts all the traffic that's destined to (or wanting to transit through) its resources as close as possible to the origin of the traffic.

> **Note**
>
> Using the Azure networking features described in this article takes advantage of the traffic attraction behavior of the Microsoft global network to provide a better networking experience for customers. The traffic attraction behavior of the Microsoft network helps offload traffic as soon as possible from the first-mile and last-mile networks that might experience congestion during periods of peak utilization.

Enable employees to work remotely

Azure VPN Gateway supports both point-to-site (P2S) and site-to-site (S2S) VPN connections. By using Azure VPN Gateway, you can scale your employees' connections to securely access both your Azure-deployed resources and your on-premises resources. For more information, see Remote work using Azure VPN Gateway point-to-site.

If you're using Secure Socket Tunneling Protocol (SSTP), the number of concurrent connections is limited to 128. To get a higher number of connections, we suggest transitioning to OpenVPN or IKEv2. For more information, see Transition to OpenVPN protocol or IKEv2 from SSTP.

To access your resources deployed in Azure, remote developers can use Azure Bastion instead of a VPN connection. That solution can provide secure shell access (RDP or SSH) without requiring public IP addresses on the VMs that are being accessed. For more information, see Enable remote work by using Azure Bastion.

You can use Azure Virtual WAN to:

- Aggregate large-scale VPN connections.
- Support any-to-any connections between resources in different on-premises global locations and in different regional hub-and-spoke virtual networks.
- Optimize utilization of multiple home broadband networks.

For more information, see Azure Virtual WAN and supporting remote work.

Another way to support a remote workforce is to deploy a virtual desktop infrastructure (VDI) hosted in your Azure virtual network, secured with Azure Firewall. For example, Azure Virtual Desktop is a desktop and app virtualization service that runs in Azure. With Virtual Desktop, you can set up a scalable and flexible environment in your Azure subscription without the need to run any additional gateway servers. You're responsible only for the Virtual Desktop virtual machines in your virtual network. For more information, see Azure Firewall remote work support.

Azure also has a rich set of ecosystem partners. Their network virtual appliances (NVAs) on Azure can also help scale VPN connectivity. For more information, see NVA considerations for remote work.

Extend employee connections to access globally distributed resources

The following Azure solutions can help enable employees to access your globally distributed resources. Your resources could be in any of the Azure regions, in on-premises networks, or even in other public or private clouds.

- **Azure virtual network peering**: If you deploy your resources in more than one Azure region or if you aggregate the connectivity of remotely working employees by using multiple virtual networks, you can establish connectivity between the virtual networks by using virtual network peering. For more information, see Virtual network peering.

- **Azure VPN-based solution**: For your remote employees connected to Azure via P2S or S2S VPN, you can enable access to on-premises networks by configuring S2S VPN between your on-premises networks and Azure VPN Gateway. For more information, see Create a site-to-site connection.

- **Azure ExpressRoute**: By using ExpressRoute private peering, you can enable private connectivity between your Azure deployments and on-premises infrastructure or your infrastructure in a colocation facility. ExpressRoute, via Microsoft peering, also permits accessing public endpoints in Microsoft from your on-premises network.

  ExpressRoute connections don't go over the public internet. They offer secure connectivity, reliability, and higher throughput, with lower and more consistent latencies than typical connections over the internet. For more information, see ExpressRoute overview.

Using an existing network provider that's already part of the ExpressRoute partner ecosystem can help reduce the time to get large-bandwidth connections to Microsoft. By using ExpressRoute Direct, you can directly connect your on-premises network to the Microsoft backbone. ExpressRoute Direct offers two line-rate options: dual 10 Gbps or 100 Gbps.

- **Azure Virtual WAN**: Azure Virtual WAN allows seamless interoperability between your VPN connections and ExpressRoute circuits. As mentioned earlier, Azure Virtual WAN also supports any-to-any connections between resources in different on-premises global locations and in different regional hub-and-spoke virtual networks.

Scale customer connectivity to front-end resources

During times when more people go online, many corporate websites experience increased customer traffic. Azure Application Gateway can help manage this increased front-end workload. For more information, see Application Gateway high-traffic support.

Microsoft support for multicloud traffic

For your deployments in other public clouds, Microsoft can provide global connectivity. Azure Virtual WAN, VPN Gateway, or ExpressRoute can help in this regard. To extend connectivity from Azure to other clouds, you can configure S2S VPN between the two clouds. You can also establish connectivity from Azure to other public clouds by using ExpressRoute.

Oracle Cloud is part of the ExpressRoute partner ecosystem. You can set up a direct interconnection between Azure and Oracle Cloud Infrastructure.

Most service providers that are part of the ExpressRoute partner ecosystem also offer private connectivity to other public clouds. By using these service providers, you can establish private connectivity between your deployments in Azure and other clouds via ExpressRoute.

Next steps

The following articles discuss how you can use Azure networking features to scale users to work remotely:

Article	Description
Remote work using Azure VPN Gateway point-to-site	Review available options to set up remote access for users or to supplement their existing solutions with additional capacity for your organization.
Azure Virtual WAN and supporting remote work	Use Azure Virtual WAN to address the remote connectivity needs of your organization.
Application Gateway high-traffic support	Use Azure Application Gateway with web application firewall (WAF) for a scalable and secure way to manage traffic to your web applications.
Working remotely: NVA considerations for remote work	Review guidance about using NVAs in Azure to provide remote access solutions.
Transition to OpenVPN protocol or IKEv2 from SSTP	Overcome the limit of 128 concurrent connections for SSTP by transitioning to OpenVPN protocol or IKEv2.
Enable remote work by using Azure Bastion	Provide RDP/SSH connectivity to virtual machines within the Azure virtual network, directly in the Azure portal, without the use of a public IP address.
Using Azure ExpressRoute to create hybrid connectivity to support remote users	Use ExpressRoute for hybrid connectivity to enable users in your organization to work remotely.
Azure Firewall remote work support	Help protect your Azure virtual network resources by using Azure Firewall.

Additional resources

🕮 Documentation

Tutorial: Deploy and configure Azure Firewall and policy in a hybrid network using the Azure portal

In this tutorial, you learn how to deploy and configure Azure Firewall and policy using the Azure portal.

Azure Firewall forced tunneling

You can configure forced tunneling to route Internet-bound traffic to an additional firewall or network virtual appliance for further processing.

Upgrade an Azure Virtual WAN from Basic to Standard - Azure portal

You can upgrade your virtual WAN type for greater functionality.

Scale SNAT ports with Azure NAT Gateway

You can integrate Azure Firewall with NAT Gateway to increase SNAT ports.

Tutorial: Secure your virtual hub using Azure Firewall Manager

In this tutorial, you learn how to secure your virtual hub with Azure Firewall Manager using the Azure portal.

Site-to-Site VPN connections over ExpressRoute private peering - Azure VPN Gateway

Learn how to configure site-to-site VPN connections over ExpressRoute private peering in order to encrypt traffic.

Show 3 more

Training

Learning path

Architect network infrastructure in Azure learning path - Learn

Learn how to architect a secure, flexible, network infrastructure in Azure and connect on-premises networks to your Azure resources.

Certification

Microsoft Certified: Azure Network Engineer Associate - Learn

This certification will be available in July 2021. Candidates for the Azure Network Engineer Associate certification should have subject matter expertise in planning, implementing, and maintaining Azure networking solutions, including hybrid networking, connectivity, routing, security, and private acces…

Enable remote work by using Azure Bastion

Article • 02/28/2023 • 2 minutes to read

Azure Bastion supports remote work scenarios by allowing users with internet connectivity to access Azure virtual machines. In particular, it enables IT administrators to manage their applications running on Azure at any time and from anywhere around the globe.

Securely access virtual machines

Azure Bastion provides RDP/SSH connectivity to virtual machines within an Azure virtual network, directly in the Azure portal, without the use of a public IP address. For more information about the Azure Bastion architecture and key features, check out What is Azure Bastion?.

Azure Bastion is deployed per virtual network. Companies can configure and manage one Azure Bastion to quickly support remote user access to virtual machines within an Azure virtual network. For guidance on how to create and manage Azure Bastion, see Create an Azure Bastion host.

Next steps

- Configure Azure Bastion by using the Azure portal, PowerShell, or the Azure CLI.
- Read the Azure Bastion FAQ.

Additional resources

Documentation

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Azure security baseline for Azure Bastion

The Azure Bastion security baseline provides procedural guidance and resources for implementing

the security recommendations specified in the Azure Security Benchmark.

Add scale units for host scaling: Azure portal - Azure Bastion

Learn how to add additional instances (scale units) to Azure Bastion.

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Show 2 more

Training

Module

Connect to virtual machines through the Azure portal by using Azure Bastion - Learn

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Certification

Microsoft Certified: Azure Administrator Associate - Learn

Azure administrators implement, manage, and monitor an organization's Microsoft Azure environment.

Azure Bastion FAQ

Article • 02/15/2023 • 10 minutes to read

Bastion FAQs

Which browsers are supported?

The browser must support HTML 5. Use the Microsoft Edge browser or Google Chrome on Windows. For Apple Mac, use Google Chrome browser. Microsoft Edge Chromium is also supported on both Windows and Mac, respectively.

How does pricing work?

Azure Bastion pricing is a combination of hourly pricing based on SKU and instances (scale units), plus data transfer rates. Hourly pricing starts from the moment Bastion is deployed, regardless of outbound data usage. For the latest pricing information, see the Azure Bastion pricing page.

Is IPv6 supported?

At this time, IPv6 isn't supported. Azure Bastion supports IPv4 only. This means that you can only assign an IPv4 public IP address to your Bastion resource, and that you can use your Bastion to connect to IPv4 target VMs. You can also use your Bastion to connect to dual-stack target VMs, but you'll only be able to send and receive IPv4 traffic via Azure Bastion.

Where does Azure Bastion store customer data?

Azure Bastion doesn't move or store customer data out of the region it's deployed in.

Does Azure Bastion support Virtual WAN?

Yes, you can use Azure Bastion for Virtual WAN deployments. However, deploying Azure Bastion within a Virtual WAN hub isn't supported. You can deploy Azure Bastion in a spoke VNet and use the IP-based connection feature to connect to virtual machines deployed across a different VNet via the Virtual WAN hub. If the Azure Virtual WAN hub will be integrated with Azure Firewall as a Secured Virtual Hub, default 0.0.0.0/0 route must not be overwritten.

Can I use Azure Bastion with Azure Private DNS Zones?

Azure Bastion needs to be able to communicate with certain internal endpoints to successfully connect to target resources. Therefore, you *can* use Azure Bastion with Azure Private DNS Zones as long as the zone name you select doesn't overlap with the naming of these internal endpoints. Before you deploy your Azure Bastion resource, make sure that the host virtual network isn't linked to a private DNS zone with the following exact names:

- management.azure.com
- blob.core.windows.net
- core.windows.net
- vaultcore.windows.net
- vault.azure.net
- azure.com

You may use a private DNS zone ending with one of the names listed above (ex: privatelink.blob.core.windows.net).

Azure Bastion isn't supported with Azure Private DNS Zones in national clouds.

Does Azure Bastion support Private Link?

No, Azure Bastion doesn't currently support private link.

Can I have an Azure Bastion subnet of size /27 or smaller (/28, /29, etc.)?

For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work. However, we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of host scaling in the future.

Can I deploy multiple Azure resources in my Azure Bastion subnet?

No. The Azure Bastion subnet (*AzureBastionSubnet*) is reserved only for the deployment of your Azure Bastion resource.

Is user-defined routing (UDR) supported on an Azure Bastion subnet?

No. UDR isn't supported on an Azure Bastion subnet.

For scenarios that include both Azure Bastion and Azure Firewall/Network Virtual Appliance (NVA) in the same virtual network, you don't need to force traffic from an Azure Bastion subnet to Azure Firewall because the communication between Azure Bastion and your VMs is private. For more information, see Accessing VMs behind Azure Firewall with Bastion.

Can I upgrade from a Basic SKU to a Standard SKU?

Yes. For steps, see Upgrade a SKU. For more information about SKUs, see the Configuration settings article.

Can I downgrade from a Standard SKU to a Basic SKU?

No. Downgrading from a Standard SKU to a Basic SKU isn't supported. For more information about SKUs, see the Configuration settings article.

Does Bastion support connectivity to Azure Virtual Desktop?

No, Bastion connectivity to Azure Virtual Desktop isn't supported.

Why do I get "Your session has expired" error message before the Bastion session starts?

A session should be initiated only from the Azure portal. Sign in to the Azure portal and begin your session again. If you go to the URL directly from another browser session or tab, this error is expected. It helps ensure that your session is more secure and that the session can be accessed only through the Azure portal.

How do I handle deployment failures?

Review any error messages and raise a support request in the Azure portal as needed. Deployment failures may result from Azure subscription limits, quotas, and constraints. Specifically, customers may encounter a limit on the number of public IP addresses allowed per subscription that causes the Azure Bastion deployment to fail.

How do I incorporate Azure Bastion in my Disaster Recovery plan?

Azure Bastion is deployed within VNets or peered VNets, and is associated to an Azure region. You're responsible for deploying Azure Bastion to a Disaster Recovery (DR) site VNet. In the event of an Azure region failure, perform a failover operation for your VMs to the DR region. Then, use the Azure Bastion host that's deployed in the DR region to connect to the VMs that are now deployed there.

Does Bastion support zone redundancies?

Currently, by default, new Bastion deployments don't support zone redundancies. Previously deployed bastions may or may not be zone-redundant. The exceptions are Bastion deployments in Korea Central and Southeast Asia, which do support zone redundancies.

Does Bastion support Azure AD guest accounts?

Yes, Azure AD guest accounts can be granted access to Bastion and can connect to virtual machines. However, Azure AD guest users can't connect to Azure VMs via Azure AD authentication. Non-guest users are supported via Azure AD authentication. For more information about Azure AD authentication for Azure VMs (for non-guest users), see Log in to a Windows virtual machine in Azure by using Azure AD.

VM features and connection FAQs

Are any roles required to access a virtual machine?

In order to make a connection, the following roles are required:

- Reader role on the virtual machine.
- Reader role on the NIC with private IP of the virtual machine.
- Reader role on the Azure Bastion resource.
- Reader Role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network).

Do I need a public IP on my virtual machine to connect via Azure Bastion?

No. When you connect to a VM using Azure Bastion, you don't need a public IP on the Azure virtual machine that you're connecting to. The Bastion service will open the RDP/SSH session/connection to your virtual machine over the private IP of your virtual machine, within your virtual network.

Do I need an RDP or SSH client?

No. You can access your virtual machine from the Azure portal using your browser. For available connections and methods, see About VM connections and features.

Can I connect to my VM using a native client?

Yes. You can connect to a VM from your local computer using a native client. See Connect to a VM using a native client.

Do I need an agent running in the Azure virtual machine?

No. You don't need to install an agent or any software on your browser or your Azure virtual machine. The Bastion service is agentless and doesn't require any additional software for RDP/SSH.

What features are supported for VM sessions?

See About VM connections and features for supported features.

Is remote audio available for VMs?

Yes. See About VM connections and features.

Does Azure Bastion support file transfer?

Azure Bastion offers support for file transfer between your target VM and local computer using Bastion and a native RDP or SSH client. At this time, you can’t upload or download files using PowerShell or via the Azure portal. For more information, see Upload and download files using the native client.

Does Bastion hardening work with AADJ VM extension-joined VMs?

This feature doesn't work with AADJ VM extension-joined machines using Azure AD users. For more information, see Log in to a Windows virtual machine in Azure by using Azure AD.

Does Azure Bastion require an RDS CAL for administrative purposes on Azure-hosted VMs?

No, access to Windows Server VMs by Azure Bastion doesn't require an RDS CAL when used solely for administrative purposes.

Which keyboard layouts are supported during the Bastion remote session?

Azure Bastion currently supports the following keyboard layouts inside the VM:

- en-us-qwerty
- en-gb-qwerty
- de-ch-qwertz
- de-de-qwertz
- fr-be-azerty
- fr-fr-azerty
- fr-ch-qwertz
- hu-hu-qwertz
- it-it-qwerty
- ja-jp-qwerty
- pt-br-qwerty
- es-es-qwerty
- es-latam-qwerty
- sv-se-qwerty
- tr-tr-qwerty

To establish the correct key mappings for your target language, you must set the keyboard layout on your local computer to your target language *and* the keyboard layout inside the target VM to your target language. Both keyboards must be set to your target language to establish the correct key mappings inside the target VM.

To set your target language as your keyboard layout on a Windows workstation, navigate to Settings > Time & Language > Language & Region. Under "Preferred languages," select "Add a language" and add your target language. You'll then be able to see your keyboard layouts on your toolbar. To set English (United States) as your

keyboard layout, select "ENG" on your toolbar or click Windows + Spacebar to open keyboard layouts.

Is there a keyboard solution to toggle focus between a VM and browser?

Users can use "Ctrl+Shift+Alt" to effectively switch focus between the VM and the browser.

What is the maximum screen resolution supported via Bastion?

Currently, 1920x1080 (1080p) is the maximum supported resolution.

Does Azure Bastion support timezone configuration or timezone redirection for target VMs?

Azure Bastion currently doesn't support timezone redirection and isn't timezone configurable. Timezone settings for a VM can be manually updated after successfully connecting to the Guest OS.

Will an existing session disconnect during maintenance on the Bastion host?

Yes, existing sessions on the target Bastion resource will disconnect during maintenance on the Bastion resource.

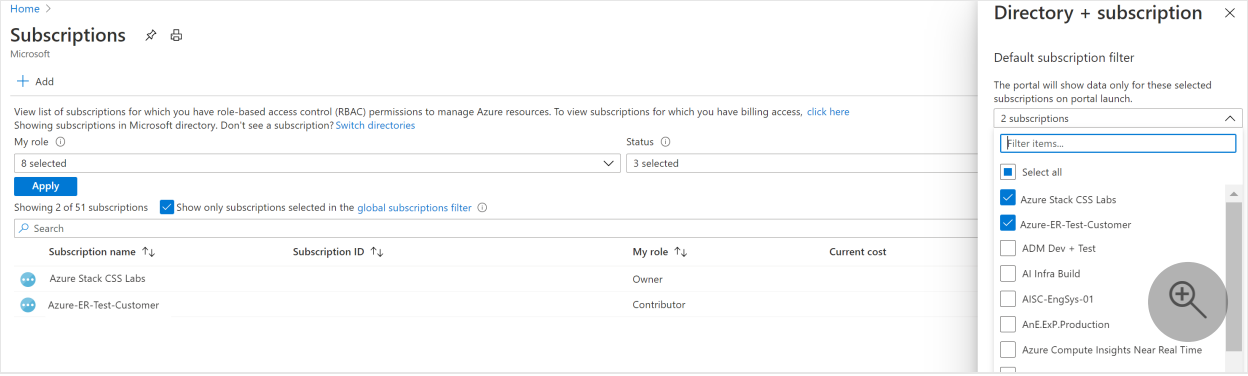
VNet peering FAQs

Can I still deploy multiple Bastion hosts across peered virtual networks?

Yes. By default, a user sees the Bastion host that is deployed in the same virtual network in which VM resides. However, in the **Connect** menu, a user can see multiple Bastion hosts detected across peered networks. They can select the Bastion host that they prefer to use to connect to the VM deployed in the virtual network.

If my peered VNets are deployed in different subscriptions, will connectivity via Bastion work?

Yes, connectivity via Bastion will continue to work for peered VNets across different subscription for a single Tenant. Subscriptions across two different Tenants aren't supported. To see Bastion in the **Connect** drop down menu, the user must select the subs they have access to in **Subscription** > **global subscription**.



I have access to the peered VNet, but I can't see the VM deployed there.

Make sure the user has **read** access to both the VM, and the peered VNet. Additionally, check under IAM that the user has **read** access to following resources:

- Reader role on the virtual machine.
- Reader role on the NIC with private IP of the virtual machine.
- Reader role on the Azure Bastion resource.
- Reader Role on the virtual network (Not needed if there isn't a peered virtual network).

Permissions	Description	Permission type
Microsoft.Network/bastionHosts/read	Gets a Bastion Host	Action
Microsoft.Network/virtualNetworks/BastionHosts/action	Gets Bastion Host references in a virtual network.	Action
Microsoft.Network/virtualNetworks/bastionHosts/default/action	Gets Bastion Host references in a virtual network.	Action

Permissions	Description	Permission type
Microsoft.Network/networkInterfaces/read	Gets a network interface definition.	Action
Microsoft.Network/networkInterfaces/ipconfigurations/read	Gets a network interface IP configuration definition.	Action
Microsoft.Network/virtualNetworks/read	Get the virtual network definition	Action
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Gets references to all the virtual machines in a virtual network subnet	Action
Microsoft.Network/virtualNetworks/virtualMachines/read	Gets references to all the virtual machines in a virtual network	Action

My privatelink.azure.com cannot resolve to management.privatelinke.azure.com

This may be due to the Private DNS zone for privatelink.azure.com linked to the Bastion virtual network causing management.azure.com CNAMEs to resolve to management.privatelink.azure.com behind the scenes. Create a CNAME record in their privatelink.azure.com zone for management.privatelink.azure.com to arm-frontdoor-prod.trafficmanager.net to enable successful DNS resolution.

Next steps

For more information, see What is Azure Bastion.

Additional resources

Documentation

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Create a shareable link for Azure Bastion

Learn how to create a shareable link to let a user connect to a target resource via Bastion without using the Azure portal.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

Working remotely using Bastion: Azure Bastion

Learn how to use Azure Bastion to enable working remotely due to the COVID-19 pandemic.

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Add scale units for host scaling: Azure portal - Azure Bastion

Learn how to add additional instances (scale units) to Azure Bastion.

VNet peering and Azure Bastion architecture

Learn how VNet peering and Azure Bastion can be used together to connect to VMs.

Show 5 more

Training

Learning paths and modules

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

About Bastion configuration settings

Article • 12/13/2022 • 5 minutes to read

The sections in this article discuss the resources and settings for Azure Bastion.

SKUs

A SKU is also known as a Tier. Azure Bastion supports two SKU types: Basic and Standard. The SKU is configured in the Azure portal during the workflow when you configure Bastion. You can upgrade a Basic SKU to a Standard SKU.

- The **Basic SKU** provides base functionality, enabling Azure Bastion to manage RDP/SSH connectivity to virtual machines (VMs) without exposing public IP addresses on the target application VMs.
- The **Standard SKU** enables premium features.

The following table shows the availability of features per corresponding SKU.

Feature	Basic SKU	Standard SKU
Connect to target VMs in peered virtual networks	Yes	Yes
Access Linux VM Private Keys in Azure Key Vault (AKV)	Yes	Yes
Connect to Linux VM using SSH	Yes	Yes
Connect to Windows VM using RDP	Yes	Yes
Kerberos authentication	Yes	Yes
VM audio output	Yes	Yes
Shareable link	No	Yes
Connect to VMs using a native client	No	Yes
Connect to VMs via IP address	No	Yes
Host scaling	No	Yes
Specify custom inbound port	No	Yes
Connect to Linux VM using RDP	No	Yes
Connect to Windows VM using SSH	No	Yes
Upload or download files	No	Yes

Feature	Basic SKU	Standard SKU
Disable copy/paste (web-based clients)	No	Yes

Specify SKU

Currently, you must use the Azure portal if you want to specify the Standard SKU. If you use the Azure CLI or Azure PowerShell to configure Bastion, the SKU can't be specified and defaults to the Basic SKU.

Method	SKU Value	Links
Azure portal	Tier - Basic or Standard	Tutorial
Azure portal	Tier - Basic	Quickstart
Azure PowerShell	Basic	How-to
Azure CLI	Basic	How-to

Upgrade a SKU

Azure Bastion supports upgrading from a Basic to a Standard SKU.

> **Note**
>
> Downgrading from a Standard SKU to a Basic SKU is not supported. To downgrade, you must delete and recreate Azure Bastion.

You can configure this setting using the following method:

Method	Value	Links
Azure portal	Tier	How-to

Azure Bastion subnet

> **Important**
>
> For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and

will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

Azure Bastion requires a dedicated subnet: **AzureBastionSubnet**. You must create this subnet in the same virtual network that you want to deploy Azure Bastion to. The subnet must have the following configuration:

- Subnet name must be *AzureBastionSubnet*.
- Subnet size must be /26 or larger (/25, /24 etc.).
- For host scaling, a /26 or larger subnet is recommended. Using a smaller subnet space limits the number of scale units. For more information, see the Host scaling section of this article.
- The subnet must be in the same VNet and resource group as the bastion host.
- The subnet cannot contain additional resources.

You can configure this setting using the following methods:

Method	Value	Links
Azure portal	Subnet	Quickstart Tutorial
Azure PowerShell	-subnetName	cmdlet
Azure CLI	--subnet-name	command

Public IP address

Azure Bastion requires a Public IP address. The Public IP must have the following configuration:

- The Public IP address SKU must be **Standard**.
- The Public IP address assignment/allocation method must be **Static**.
- The Public IP address name is the resource name by which you want to refer to this public IP address.
- You can choose to use a public IP address that you already created, as long as it meets the criteria required by Azure Bastion and is not already in use.

You can configure this setting using the following methods:

Method	Value	Links	Requires Standard SKU

Method	Value	Links	Requires Standard SKU
Azure portal	Public IP address	Azure portal	Yes
Azure PowerShell	-PublicIpAddress	cmdlet	Yes
Azure CLI	--public-ip create	command	Yes

Instances and host scaling

An instance is an optimized Azure VM that is created when you configure Azure Bastion. It's fully managed by Azure and runs all of the processes needed for Azure Bastion. An instance is also referred to as a scale unit. You connect to client VMs via an Azure Bastion instance. When you configure Azure Bastion using the Basic SKU, two instances are created. If you use the Standard SKU, you can specify the number of instances. This is called **host scaling**.

Each instance can support 20 concurrent RDP connections and 40 concurrent SSH connections for medium workloads (see Azure subscription limits and quotas for more information). The number of connections per instances depends on what actions you are taking when connected to the client VM. For example, if you are doing something data intensive, it creates a larger load for the instance to process. Once the concurrent sessions are exceeded, an additional scale unit (instance) is required.

Instances are created in the AzureBastionSubnet. To allow for host scaling, the AzureBastionSubnet should be /26 or larger. Using a smaller subnet limits the number of instances you can create. For more information about the AzureBastionSubnet, see the subnets section in this article.

You can configure this setting using the following methods:

Method	Value	Links	Requires Standard SKU
Azure portal	Instance count	How-to	Yes
Azure PowerShell	ScaleUnit	How-to	Yes

Custom ports

You can specify the port that you want to use to connect to your VMs. By default, the inbound ports used to connect are 3389 for RDP and 22 for SSH. If you configure a custom port value, specify that value when you connect to the VM.

Custom port values are supported for the Standard SKU only.

Shareable link (Preview)

The Bastion **Shareable Link** feature lets users connect to a target resource using Azure Bastion without accessing the Azure portal.

When a user without Azure credentials clicks a shareable link, a webpage will open that prompts the user to sign in to the target resource via RDP or SSH. Users authenticate using username and password or private key, depending on what you have configured in the Azure portal for that target resource. Users can connect to the same resources that you can currently connect to with Azure Bastion: VMs or virtual machine scale set.

Method	Value	Links	Requires Standard SKU
Azure portal	Shareable Link	Configure	Yes

Next steps

For frequently asked questions, see the Azure Bastion FAQ.

About VM connections and features

Article • 04/19/2022 • 2 minutes to read

The sections in this article show you various features and settings that are available when you connect to a VM using Azure Bastion.

Connect to a VM

You can use a variety of different methods to connect to a target VM. Some connection types require Bastion to be configured with the Standard SKU. Use the following articles to connect.

- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

Copy and paste

You can copy and paste text between your local device and the remote session. Only text copy/paste is supported. By default, this feature is enabled. If you want to disable this feature for web-based clients, you can change the setting on the configuration page for your bastion host. To disable, your bastion host must be configured with the Standard SKU tier.

For steps and more information, see Copy and paste - Windows VMs.

Full screen view

You can change to full screen view and back using your browser. For steps and more information, see Change to full screen view.

Upload or download files

Azure Bastion offers support for file transfer between your target VM and local computer using Bastion and a native RDP or native SSH client. It may also be possible to use certain third-party clients and tools to upload and download files.

For steps and more information, see Upload or download files to a VM using a native client.

Remote audio

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

FAQ

For FAQs, see Bastion FAQ - VM connections and features.

Next steps

Quickstart: Deploy Azure Bastion with default settings

VNet peering and Azure Bastion

Article • 02/08/2023 • 2 minutes to read

Azure Bastion and VNet peering can be used together. When VNet peering is configured, you don't have to deploy Azure Bastion in each peered VNet. This means if you have an Azure Bastion host configured in one virtual network (VNet), it can be used to connect to VMs deployed in a peered VNet without deploying an additional bastion host. For more information about VNet peering, see About virtual network peering.

Azure Bastion works with the following types of peering:

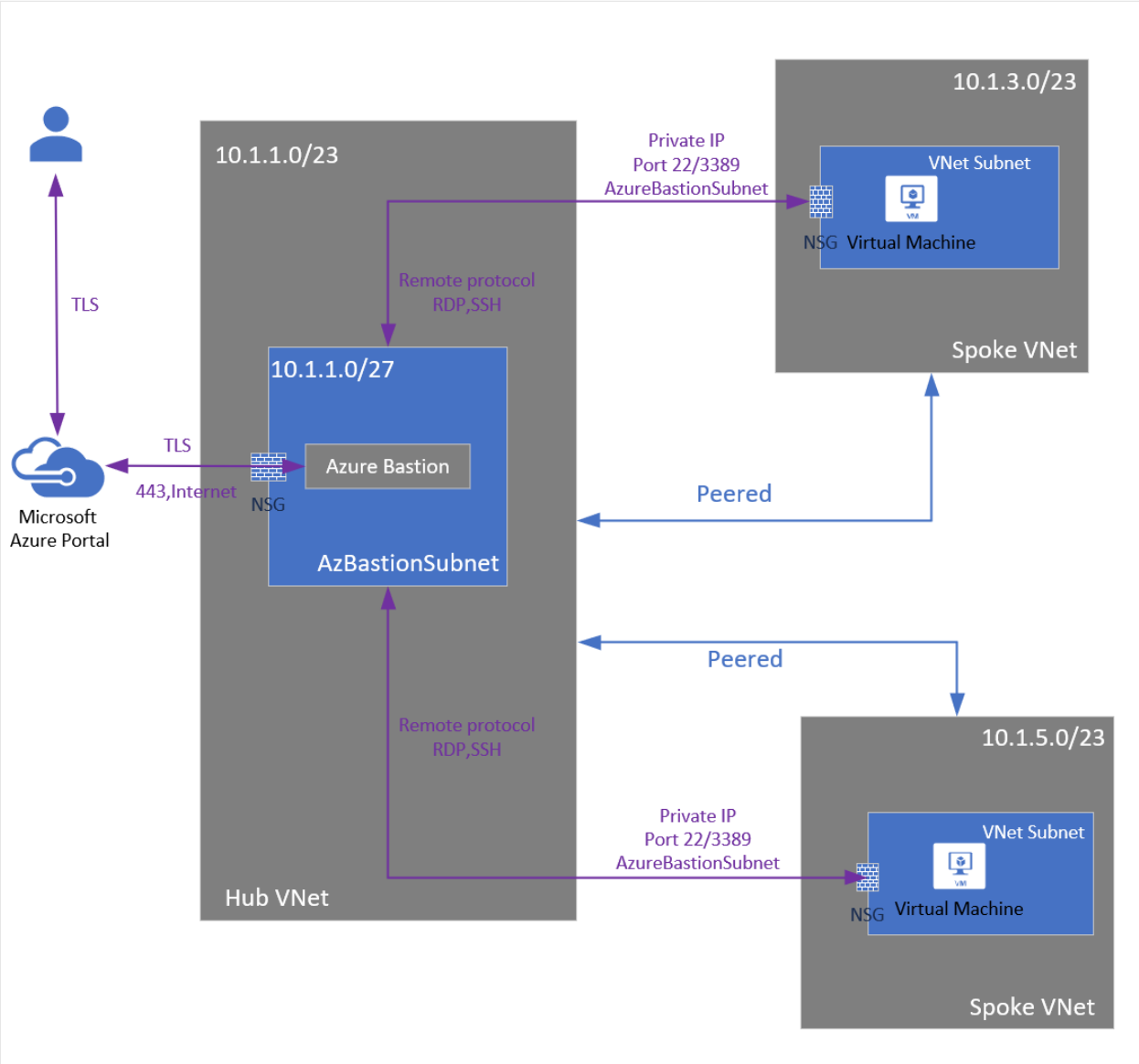
- **Virtual network peering:** Connect virtual networks within the same Azure region.
- **Global virtual network peering:** Connecting virtual networks across Azure regions.

> **Note**
>
> Deploying Azure Bastion **within** a Virtual WAN hub is not supported. You can deploy Azure Bastion in a spoke VNet and use the **IP-based connection** feature to connect to virtual machines deployed across a different VNet via the Virtual WAN hub.

Architecture

When VNet peering is configured, Azure Bastion can be deployed in hub-and-spoke or full-mesh topologies. Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine.

Once you provision the Azure Bastion service in your virtual network, the RDP/SSH experience is available to all your VMs in the same VNet and peered VNets. This means you can consolidate Bastion deployment to single VNet and still reach VMs deployed in a peered VNet, centralizing the overall deployment.



The diagram shows the architecture of an Azure Bastion deployment in a hub-and-spoke model. In the diagram, you can see the following configuration:

- The bastion host is deployed in the centralized hub virtual network.
- Centralized Network Security Group (NSG) is deployed.
- A public IP is not required on the Azure VM.

Deployment overview

1. Verify that you have configured VNets, and virtual machines within the VNets.
2. Configure VNet peering.
3. Configure Bastion in one of the VNets.
4. Verify permissions.
5. Connect to a VM via Azure Bastion. In order to connect via Azure Bastion, you must have the correct permissions for the subscription you are signed into.

To verify permissions

Verify the following permissions when working with this architecture:

- Ensure you have **read** access to both the target VM and the peered VNet.
- Check your permissions in **YourSubscription | IAM** and verify that you have read access to the following resources:
  - Reader role on the virtual machine.
  - Reader role on the NIC with private IP of the virtual machine.
  - Reader role on the Azure Bastion resource.
  - Reader role on the virtual network (for peered virtual networks).

Bastion VNet peering FAQ

For frequently asked questions, see the Bastion VNet peering FAQ.

Next steps

Read the Bastion FAQ.

Additional resources

🕮 Documentation

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

Tutorial: Deploy Bastion using specified settings: Azure portal

Learn how to deploy Bastion using settings that you specify - Azure portal.

Quickstart: Deploy Bastion with default settings - Azure Bastion

Learn how to deploy Bastion with default settings from the Azure portal.

Deploy & configure Azure Firewall using the Azure portal

In this article, you learn how to deploy and configure Azure Firewall using the Azure portal.

Move Azure network security group (NSG) to another Azure region using the Azure portal

Use Azure Resource Manager template to move Azure network security group from one Azure region to another using the Azure portal.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

What is auto registration feature in Azure DNS private zones?

Overview of auto registration feature in Azure DNS private zones.

Show 5 more

Training

Learning paths and modules

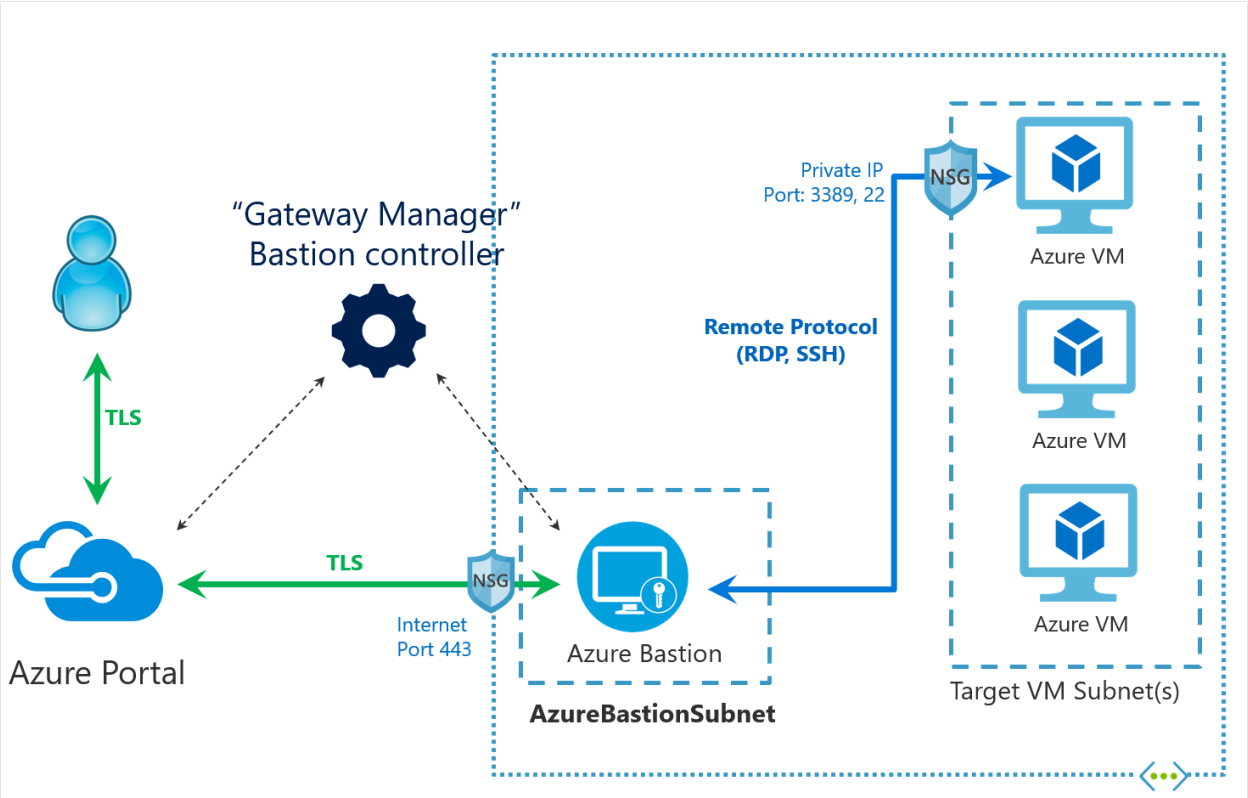
Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Working with NSG access and Azure Bastion

Article • 02/08/2023 • 3 minutes to read

When working with Azure Bastion, you can use network security groups (NSGs). For more information, see Security Groups.



In this diagram:

- The Bastion host is deployed to the virtual network.
- The user connects to the Azure portal using any HTML5 browser.
- The user navigates to the Azure virtual machine to RDP/SSH.
- Connect Integration - Single-click RDP/SSH session inside the browser
- No public IP is required on the Azure VM.

Network security groups

This section shows you the network traffic between the user and Azure Bastion, and through to target VMs in your virtual network:

> ⓘ **Important**

If you choose to use an NSG with your Azure Bastion resource, you **must** create all of the following ingress and egress traffic rules. Omitting any of the following rules in your NSG will block your Azure Bastion resource from receiving necessary updates in the future and therefore open up your resource to future security vulnerabilities.

AzureBastionSubnet

Azure Bastion is deployed specifically to ***AzureBastionSubnet***.

- **Ingress Traffic:**
  - **Ingress Traffic from public internet:** The Azure Bastion will create a public IP that needs port 443 enabled on the public IP for ingress traffic. Port 3389/22 are NOT required to be opened on the AzureBastionSubnet. Note that the source can be either the Internet or a set of public IP addresses that you specify.
  - **Ingress Traffic from Azure Bastion control plane:** For control plane connectivity, enable port 443 inbound from **GatewayManager** service tag. This enables the control plane, that is, Gateway Manager to be able to talk to Azure Bastion.
  - **Ingress Traffic from Azure Bastion data plane:** For data plane communication between the underlying components of Azure Bastion, enable ports 8080, 5701 inbound from the **VirtualNetwork** service tag to the **VirtualNetwork** service tag. This enables the components of Azure Bastion to talk to each other.
  - **Ingress Traffic from Azure Load Balancer:** For health probes, enable port 443 inbound from the **AzureLoadBalancer** service tag. This enables Azure Load Balancer to detect connectivity

Priority	Name	Port	Protocol	Source	Destination	Action
120	AllowHttpsInbound	443	TCP	Internet	Any	Allow
130	AllowGatewayManagerInbound	443	TCP	GatewayManager	Any	Allow
140	AllowAzureLoadBalancerInbound	443	TCP	AzureLoadBalancer	Any	Allow
150	AllowBastionHostCommunication	8080,5701	Any	VirtualNetwork	VirtualNetwork	Allow

- **Egress Traffic:**
  - **Egress Traffic to target VMs:** Azure Bastion will reach the target VMs over private IP. The NSGs need to allow egress traffic to other target VM subnets for port 3389 and 22. If you are using the custom port feature as part of Standard SKU, the NSGs will instead need to allow egress traffic to other target VM subnets for the custom value(s) you have opened on your target VMs.
  - **Egress Traffic to Azure Bastion data plane:** For data plane communication between the underlying components of Azure Bastion, enable ports 8080, 5701 outbound from the **VirtualNetwork** service tag to the **VirtualNetwork** service tag. This enables the components of Azure Bastion to talk to each other.

- **Egress Traffic to other public endpoints in Azure:** Azure Bastion needs to be able to connect to various public endpoints within Azure (for example, for storing diagnostics logs and metering logs). For this reason, Azure Bastion needs outbound to 443 to **AzureCloud** service tag.
- **Egress Traffic to Internet:** Azure Bastion needs to be able to communicate with the Internet for session and certificate validation. For this reason, we recommend enabling port 80 outbound to the **Internet.**

Priority	Name	Port	Protocol	Source	Destination	Action
100	AllowSshRdpOutbound	22,3389	Any	Any	VirtualNetwork	Allow
110	AllowAzureCloudOutbound	443	TCP	Any	AzureCloud	Allow
120	AllowBastionCommunication	8080,5701	Any	VirtualNetwork	VirtualNetwork	Allow
130	AllowGetSessionInformation	80	Any	Any	Internet	Allow

Target VM Subnet

This is the subnet that contains the target virtual machine that you want to RDP/SSH to.

- **Ingress Traffic from Azure Bastion:** Azure Bastion will reach to the target VM over private IP. RDP/SSH ports (ports 3389/22 respectively, or custom port values if you are using the custom port feature as a part of Standard SKU) need to be opened on the target VM side over private IP. As a best practice, you can add the Azure Bastion Subnet IP address range in this rule to allow only Bastion to be able to open these ports on the target VMs in your target VM subnet.

Next steps

For more information about Azure Bastion, see the FAQ.

Additional resources

Documentation

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Create a shareable link for Azure Bastion

Learn how to create a shareable link to let a user connect to a target resource via Bastion without using the Azure portal.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

Configure Bastion for Kerberos authentication: Azure portal - Azure Bastion

Learn how to configure Bastion to use Kerberos authentication via the Azure portal.

Add scale units for host scaling: Azure portal - Azure Bastion

Learn how to add additional instances (scale units) to Azure Bastion.

Update the address space for a peered virtual network - Azure portal

Learn how to add, modify or delete the address ranges for a peered virtual network without downtime.

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Show 5 more

Training

Learning paths and modules

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Azure security baseline for Azure Bastion

Article • 11/14/2022 • 16 minutes to read

This security baseline applies guidance from the Azure Security Benchmark version 2.0 to Azure Bastion. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the **security controls** defined by the Azure Security Benchmark and the related guidance applicable to Azure Bastion.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud dashboard.

When a section has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance to the Azure Security Benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

> **Note**
>
> **Controls** not applicable to Azure Bastion, and those for which the global guidance is recommended verbatim, have been excluded. To see how Azure Bastion completely maps to the Azure Security Benchmark, see the **full Azure Bastion security baseline mapping file**.

Network Security

For more information, see the Azure Security Benchmark: Network Security.

NS-1: Implement security for internal traffic

Guidance: When you deploy Azure Bastion resources you must create or use an existing virtual network. Ensure that all Azure virtual networks follow an enterprise segmentation principle that aligns to the business risks. Any system that could incur higher risk for the organization should be isolated within its own virtual network and sufficiently secured with a network security group (NSG).

Azure Bastion service requires following ports need to be open for service to function properly:

- Ingress Traffic:
  - Ingress Traffic from public internet: The Azure Bastion will create a public IP that needs port 443 enabled on the public IP for ingress traffic. Port 3389/22 are NOT required to be opened on the AzureBastionSubnet.
  - Ingress Traffic from Azure Bastion control plane: For control plane connectivity, enable port 443 inbound from GatewayManager service tag. This enables the control plane, that is, Gateway Manager to be able to communicate with Azure Bastion.
- Egress Traffic:
  - Egress Traffic to target virtual machines (VMs): Azure Bastion will reach the target VMs over private IP. The NSGs need to allow egress traffic to other target VM subnets for port 3389 and 22.
  - Egress Traffic to other public endpoints in Azure: Azure Bastion needs to be able to connect to various public endpoints within Azure (for example, for storing diagnostics logs and metering logs). For this reason, Azure Bastion needs outbound to 443 to AzureCloud service tag.

Connectivity to Gateway Manager and Azure service tag is protected (locked down) by Azure certificates. External entities, including the consumers of those resources, can't communicate on these endpoints.

- How to create a network security group with security rules
- You can learn more about Bastion NSG requirement here

Responsibility: Customer

Microsoft Defender for Cloud monitoring: The Azure Security Benchmark is the default policy initiative for Microsoft Defender for Cloud and is the foundation for Microsoft Defender for Cloud's recommendations. The Azure Policy definitions related to this control are enabled automatically by Microsoft Defender for Cloud. Alerts related to this control may require an Microsoft Defender plan for the related services.

Azure Policy built-in definitions - Microsoft.Network:

Name (Azure portal)	Description	Effect(s)	Version (GitHub)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
All Internet traffic should be routed via your deployed Azure Firewall	Microsoft Defender for Cloud has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview
Subnets should be associated with a Network Security Group	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0

NS-2: Connect private networks together

Guidance: Azure Bastion supports deploying into a peered network to centralize your Bastion deployment and enable cross-network connectivity.

- Azure Bastion and virtual network peering

Responsibility: Customer

NS-7: Secure Domain Name Service (DNS)

Guidance: Not applicable; Azure Bastion does not expose its underlying DNS configurations, these settings are maintained by Microsoft.

Responsibility: Microsoft

Identity Management

For more information, see the Azure Security Benchmark: Identity Management.

IM-1: Standardize Azure Active Directory as the central identity and authentication system

Guidance: Azure Bastion is integrated with Azure Active Directory (Azure AD) which is Azure's default identity and access management service. Users can access the Azure

portal using Azure AD authentication to manage Azure Bastion service (create, update, and delete Bastion resources).

Connecting to virtual machines using Azure Bastion relies on either an SSH key or username/password, and currently does not support the use of Azure AD credentials.

You can store your SSH keys as Azure Key Vault secrets and use these secrets to connect to your virtual machines using Azure Bastion. You can control user access to these secrets by assigning Key Vault access policies either on individual users or Azure AD groups. Your users will need the following permissions to use this method to connect to a virtual machine:

- **Get** access to the secrets stored in the chosen Azure Key Vault
- **List** access to the secrets stored in the chosen Azure Key Vault

In addition to an SSH key or username/password, when connecting to virtual machines using Azure Bastion your user will need the following role assignments:

- Reader role on the target virtual machine
- Reader role on the NIC with the private IP of the target virtual machine
- Reader role on the Azure Bastion resource
- Reader Role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network)

For more information, see the following references:

- Connect to a Linux virtual machine using Azure Bastion
- Connect to a Windows virtual machine using Azure Bastion
- Azure built-in roles

Responsibility: Customer

IM-3: Use Azure AD single sign-on (SSO) for application access

Guidance: Azure Bastion doesn't support SSO for authentication when authenticating to virtual machine resources, only SSH or username/password are supported. However, Azure Bastion uses Azure Active Directory (Azure AD) to provide identity and access management for the overall service. Users can authenticate to Azure AD to access and manage their Azure Bastion resources, and experience seamless single-sign on with their own synced enterprise identities via Azure AD Connect.

- Understand Application SSO with Azure AD
- Azure AD connect
- Connect to a Linux virtual machine using Azure Bastion
- Connect to a Windows virtual machine using Azure Bastion

Responsibility: Customer

Privileged Access

For more information, see the Azure Security Benchmark: Privileged Access.

PA-3: Review and reconcile user access regularly

Guidance: Azure Bastion uses Azure Active Directory (Azure AD) accounts and Azure RBAC to manage its resources. Review user accounts and access assignment regularly to ensure the accounts and their access are valid. You can use Azure AD access reviews to review group memberships, access to enterprise applications, and role assignments. Azure AD reporting can provide logs to help discover stale accounts. You can also use Azure AD Privileged Identity Management to create access review report workflow to facilitate the review process.

In addition, Azure Privileged Identity Management can also be configured to alert when an excessive number of administrator accounts are created, and to identify administrator accounts that are stale or improperly configured.

- Create an access review of Azure resource roles in Privileged Identity Management (PIM)
- Removing access to a delegation
- How to use Azure AD identity and access reviews

Responsibility: Customer

PA-6: Use privileged access workstations

Guidance: Secured, isolated workstations are critically important for the security of sensitive roles like administrators, developers, and critical service operators. Depending on your requirements, you can use highly secured user workstations for performing administrative management tasks with your Azure Bastion resources in production

environments. Use Azure Active Directory (Azure AD), Microsoft Defender Advanced Threat Protection (ATP), and/or Microsoft Intune to deploy a secure and managed user workstation for administrative tasks. The secured workstations can be centrally managed to enforce secured configuration, including strong authentication, software and hardware baselines, and restricted logical and network access.

- Understand privileged access workstations
- Deploy a privileged access workstation

Responsibility: Customer

PA-7: Follow just enough administration (least privilege principle)

Guidance: Azure Bastion is integrated with Azure role-based access control (RBAC) to manage its resources. Azure RBAC allows you to manage Azure resource access through role assignments. You can assign these built-in roles to users, groups, service principals and managed identities. There are pre-defined built-in roles for certain resources, and these roles can be inventoried or queried through tools such as Azure CLI, Azure PowerShell or the Azure portal. The privileges you assign to resources through the Azure RBAC should be always limited to what is required by the roles. This complements the just in time (JIT) approach of Azure Active Directory (Azure AD) Privileged Identity Management (PIM) and should be reviewed periodically. Use built-in roles to allocate permission and only create custom roles when required.

When connecting to virtual machines using Azure Bastion your user will need the following role assignments:

- Reader role on the target virtual machine
- Reader role on the NIC with the private IP of the target virtual machine
- Reader role on the Azure Bastion resource

For more information, see the following references:

- Connect to a Linux virtual machine using Azure Bastion
- Connect to a Windows virtual machine using Azure Bastion
- Azure built-in roles

Responsibility: Customer

Data Protection

For more information, see the Azure Security Benchmark: Data Protection.

DP-4: Encrypt sensitive information in transit

Guidance: Azure Bastion uses TLS for data in transit between user and virtual machine.

- Azure Bastion key features

Responsibility: Microsoft

Asset Management

For more information, see the Azure Security Benchmark: Asset Management.

AM-1: Ensure security team has visibility into risks for assets

Guidance: Ensure security teams are granted Security Reader permissions in your Azure tenant and subscriptions so they can monitor for security risks using Microsoft Defender for Cloud.

Depending on how security team responsibilities are structured, monitoring for security risks could be the responsibility of a central security team or a local team. That said, security insights and risks must always be aggregated centrally within an organization.

Security Reader permissions can be applied broadly to an entire tenant (Root Management Group) or scoped to management groups or specific subscriptions.

Note: Additional permissions might be required to get visibility into workloads and services.

- Overview of Security Reader Role
- Overview of Azure Management Groups

Responsibility: Customer

AM-2: Ensure security team has access to asset inventory and metadata

Guidance: Apply tags to your Azure Bastion resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair. For example, you can apply the name "Environment" and the value "Production" to all the resources in production. Ensure that security teams have access to a continuously updated inventory of assets on Azure. They can use Azure Resource Graph to query and discover all resources in your subscriptions, including Azure services, applications, and network resources.

- How to create queries with Azure Resource Graph Explorer
- Microsoft Defender for Cloud asset inventory management
- For more information about tagging assets, see the resource naming and tagging decision guide

Responsibility: Customer

AM-3: Use only approved Azure services

Guidance: Use Azure Policy to audit and restrict which services users can provision in your environment, this includes being able to allow or deny deployments of Azure Bastion resources. Use Azure Resource Graph to query for and discover resources within their subscriptions. You can also use Azure Monitor to create rules to trigger alerts when a non-approved service is detected.

- How to configure and manage Azure Policy
- How to deny a specific resource type with Azure Policy
- How to create queries with Azure Resource Graph Explorer

Responsibility: Customer

Logging and Threat Detection

For more information, see the Azure Security Benchmark: Logging and Threat Detection.

LT-2: Enable threat detection for Azure identity and access management

Guidance: Azure Bastion integrates with Azure Active Directory (Azure AD) and the service is accessed over the Azure portal. By default management actions to the service (such as create, update, and delete) are captured via the Azure Activity Log. Users

should also enable Azure Bastion resource logs, such as session BastionAuditLogs to track bastion sessions.

Azure AD provides the following user logs that can be viewed in Azure AD reporting or integrated with Azure Monitor, Microsoft Sentinel or other SIEM/monitoring tools for more sophisticated monitoring and analytics use cases:

- Sign-ins – The sign-ins report provides information about the usage of managed applications and user sign-in activities.
- Audit logs - Provides traceability through logs for all changes done by various features within Azure AD. Examples of audit logs include changes made to any resources within Azure AD like adding or removing users, apps, groups, roles and policies.
- Risky sign-ins - A risky sign-in is an indicator for a sign-in attempt that might have been performed by someone who is not the legitimate owner of a user account.
- Users flagged for risk - A risky user is an indicator for a user account that might have been compromised.

Microsoft Defender for Cloud can also alert on certain suspicious activities such as an excessive number of failed authentication attempts, and deprecated accounts in the subscription. In addition to the basic security hygiene monitoring, Microsoft Defender for Cloud's Threat Protection module can also collect more in-depth security alerts from individual Azure compute resources (such as virtual machines, containers, app service), data resources (such as SQL DB and storage), and Azure service layers. This capability allows you to see account anomalies inside the individual resources.

- Azure Bastion resource logs
- Audit activity reports in Azure AD
- Enable Azure Identity Protection
- Threat protection in Microsoft Defender for Cloud

Responsibility: Customer

LT-3: Enable logging for Azure network activities

Guidance: Enable Azure Bastion resource logs, use these diagnostics logs to view which users connected to which workloads, at what time, from where, and other such relevant logging information. Users can configure these logs to be sent to a storage account for long-term retention and auditing.

Enable and collect network security group (NSG) resource logs and NSG flow logs on the network security groups that are applied to the virtual networks you have your Azure Bastion resource deployed. These logs can then be used for analyzing network security and to support incident investigations, threat hunting, and security alert generation. You can send the flow logs to an Azure Monitor Log Analytics workspace and then use Traffic Analytics to provide insights.

- Enable and work with Azure Bastion logs
- How to enable network security group flow logs
- Azure Firewall logs and metrics
- How to enable and use Traffic Analytics
- Monitoring with Network Watcher

Responsibility: Customer

Microsoft Defender for Cloud monitoring: The Azure Security Benchmark is the default policy initiative for Microsoft Defender for Cloud and is the foundation for Microsoft Defender for Cloud's recommendations. The Azure Policy definitions related to this control are enabled automatically by Microsoft Defender for Cloud. Alerts related to this control may require an Microsoft Defender plan for the related services.

Azure Policy built-in definitions - Microsoft.Network:

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Network Watcher should be enabled	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	3.0.0

LT-4: Enable logging for Azure resources

Guidance: Activity logs, which are automatically available, contain all write operations (PUT, POST, DELETE) for your Azure Bastion resources except read operations (GET).

Activity logs can be used to find an error when troubleshooting or to monitor how a user in your organization modified a resource.

- How to collect platform logs and metrics with Azure Monitor
- Understand logging and different log types in Azure
- Enable Azure resource logs for Azure Bastion

Responsibility: Customer

LT-5: Centralize security log management and analysis

Guidance: Centralize logging storage and analysis to enable correlation. For each log source, ensure you have assigned a data owner, access guidance, storage location, what tools are used to process and access the data, and data retention requirements.

Ensure you are integrating Azure activity logs into your central logging. Ingest logs via Azure Monitor to aggregate security data generated by endpoint devices, network resources, and other security systems. In Azure Monitor, use Log Analytics workspaces to query and perform analytics, and use Azure Storage accounts for long term and archival storage.

In addition, enable and onboard data to Microsoft Sentinel or a third-party SIEM.

Many organizations choose to use Microsoft Sentinel for “hot” data that is used frequently and Azure Storage for “cold” data that is used less frequently.

- How to collect platform logs and metrics with Azure Monitor
- How to onboard Microsoft Sentinel

Responsibility: Customer

LT-6: Configure log storage retention

Guidance: Ensure that any storage accounts or Log Analytics workspaces used for storing Azure Bastion logs has the log retention period set according to your organization's compliance regulations.

In Azure Monitor, you can set your Log Analytics workspace retention period according to your organization's compliance regulations.

- How to configure Log Analytics Workspace Retention Period

- Storing resource logs in an Azure Storage Account
- Enable and work with Azure Bastions logs

Responsibility: Customer

LT-7: Use approved time synchronization sources

Guidance: Azure Bastion does not support configuring your own time synchronization sources. The Azure Bastion service relies on Microsoft time synchronization sources, and these are not exposed to customers for configuration.

Responsibility: Microsoft

Posture and Vulnerability Management

For more information, see the Azure Security Benchmark: Posture and Vulnerability Management.

PV-1: Establish secure configurations for Azure services

Guidance: Define and implement standard security configurations for Azure Bastion with Azure Policy. Use Azure Policy aliases in the "Microsoft.Network" namespace to create custom policies to audit or enforce the network configuration of your Azure Bastion. Customers can also establish secure configurations by leveraging Azure Blueprints or ARM templates to deploy Bastion resources securely and consistently.

- How to view available Azure Policy Aliases
- How to configure and manage Azure Policy
- Learn about ARM templates
- Overview about Azure Blueprints

Responsibility: Customer

PV-2: Sustain secure configurations for Azure services

Guidance: Define and implement standard security configurations for Azure Bastion with Azure Policy. Use Azure Policy aliases in the "Microsoft.Network" namespace to create custom policies to audit or enforce the network configuration of your Bastion resources.

- How to view available Azure Policy Aliases
- How to configure and manage Azure Policy

Responsibility: Customer

PV-6: Perform software vulnerability assessments

Guidance: Microsoft performs vulnerability management on the underlying systems that support Azure Bastion.

Responsibility: Microsoft

PV-7: Rapidly and automatically remediate software vulnerabilities

Guidance: Microsoft performs vulnerability management and software update on the underlying systems that support Azure Bastion.

Responsibility: Microsoft

PV-8: Conduct regular attack simulation

Guidance: As required, conduct penetration testing or red team activities on your Azure resources and ensure remediation of all critical security findings.

Follow the Microsoft Cloud Penetration Testing Rules of Engagement to ensure your penetration tests are not in violation of Microsoft policies. Use Microsoft's strategy and execution of Red Teaming and live site penetration testing against Microsoft-managed cloud infrastructure, services, and applications.

- Penetration testing in Azure
- Penetration Testing Rules of Engagement
- Microsoft Cloud Red Teaming

Responsibility: Shared

Endpoint Security

For more information, see the Azure Security Benchmark: Endpoint Security.

ES-1: Use Endpoint Detection and Response (EDR)

Guidance: Azure Bastion is a fully managed PaaS offering and Microsoft is responsible for handling endpoint protection.

Responsibility: Microsoft

ES-2: Use centrally managed modern anti-malware software

Guidance: Azure Bastion is a fully managed PaaS offering and Microsoft is responsible for installing and managing anti-malware protection.

Responsibility: Microsoft

ES-3: Ensure anti-malware software and signatures are updated

Guidance: Azure Bastion is a fully managed PaaS offering and Microsoft is responsible for installing, managing, and updating anti-malware signature.

Responsibility: Microsoft

Next steps

- See the Azure Security Benchmark V2 overview
- Learn more about Azure security baselines

Tutorial: Deploy Bastion using specified settings

Article • 09/21/2022 • 9 minutes to read

This tutorial helps you deploy Azure Bastion from the Azure portal using your own specified manual settings. When you use manual settings, you can specify configuration values such as instance counts and the SKU at the time of deployment. After Bastion is deployed, you can connect (SSH/RDP) to virtual machines in the virtual network via Bastion using the private IP address of the VM. When you connect to a VM, it doesn't need a public IP address, client software, agent, or a special configuration.

In this tutorial, you deploy Bastion using the Standard SKU tier and adjust host scaling (instance count). After the deployment is complete, you connect to your VM via private IP address. If your VM has a public IP address that you don't need for anything else, you can remove it.

Azure Bastion is a PaaS service that's maintained for you, not a bastion host that you install on one of your VMs and maintain yourself. For more information about Azure Bastion, see What is Azure Bastion?

In this tutorial, you'll learn how to:

- ✓ Deploy Bastion to your VNet.
- ✓ Connect to a virtual machine.
- ✓ Remove the public IP address from a virtual machine.

If you don’t have an Azure subscription, create a free account before you begin.

Prerequisites

- A virtual network. This will be the VNet to which you deploy Bastion.
- A virtual machine in the virtual network. This VM isn't a part of the Bastion configuration and doesn't become a bastion host. You connect to this VM later in this tutorial via Bastion. If you don't have a VM, create one using Quickstart: Create a VM.
- **Required VM roles:**
  - Reader role on the virtual machine.
  - Reader role on the NIC with private IP of the virtual machine.

- **Required inbound ports:**
  - For Windows VMs - RDP (3389)
  - For Linux VMs - SSH (22)

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Example values

You can use the following example values when creating this configuration, or you can substitute your own.

Basic VNet and VM values:

Name	Value
Virtual machine	TestVM
Resource group	TestRG1
Region	East US
Virtual network	VNet1
Address space	10.1.0.0/16
Subnets	FrontEnd: 10.1.0.0/24

Azure Bastion values:

Name	Value
Name	VNet1-bastion
+ Subnet Name	AzureBastionSubnet
AzureBastionSubnet addresses	A subnet within your VNet address space with a subnet mask /26 or larger. For example, 10.1.1.0/26.
Tier/SKU	Standard
Instance count (host scaling)	3 or greater

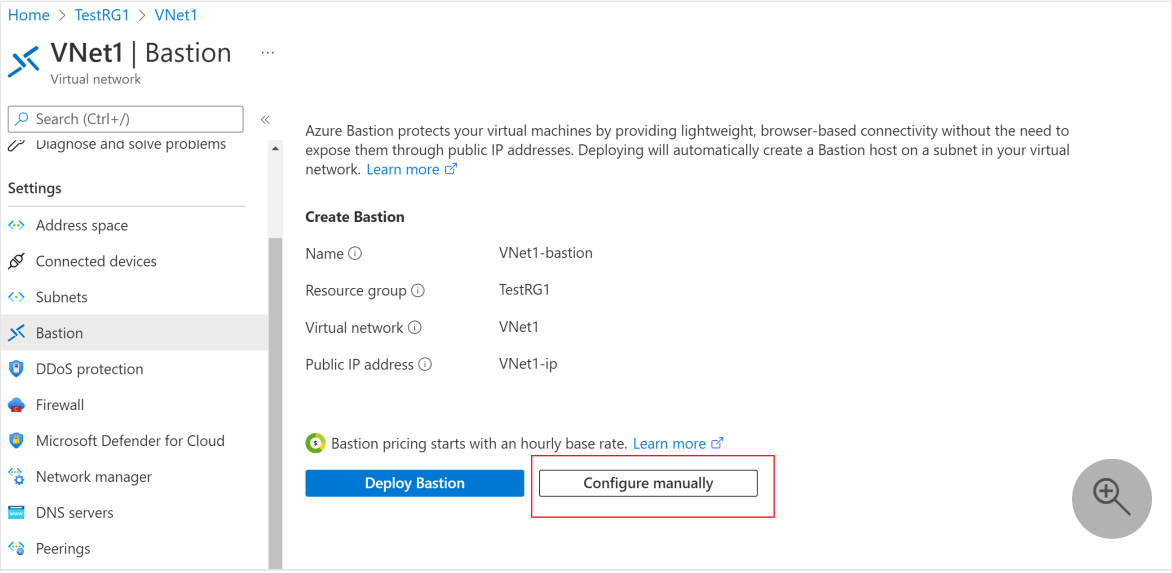
Name	Value
Public IP address	Create new
Public IP address name	VNet1-ip
Public IP address SKU	Standard
Assignment	Static

> **Important**
>
> For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

Deploy Bastion

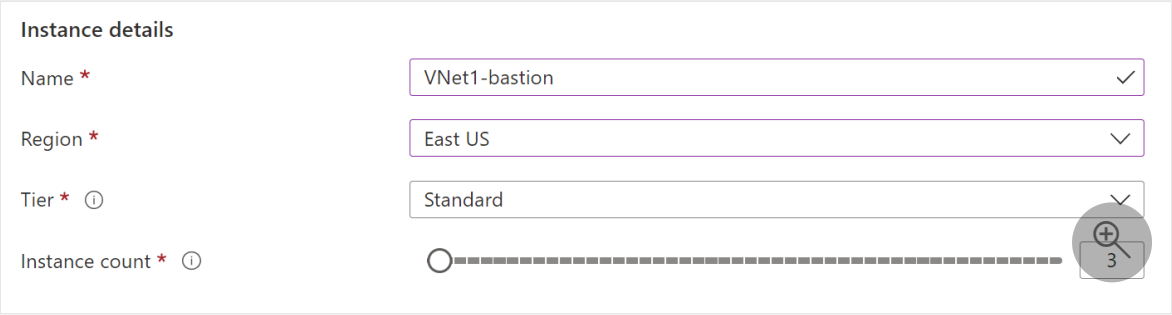
This section helps you deploy Bastion to your VNet. Once Bastion is deployed, you can connect securely to any VM in the VNet using its private IP address.

1. Sign in to the Azure portal.
2. Go to your virtual network.
3. On the page for your virtual network, in the left pane, select **Bastion** to open the **Bastion** page.
4. On the Bastion page, select **Configure manually**. This lets you configure specific additional settings when deploying Bastion to your VNet.



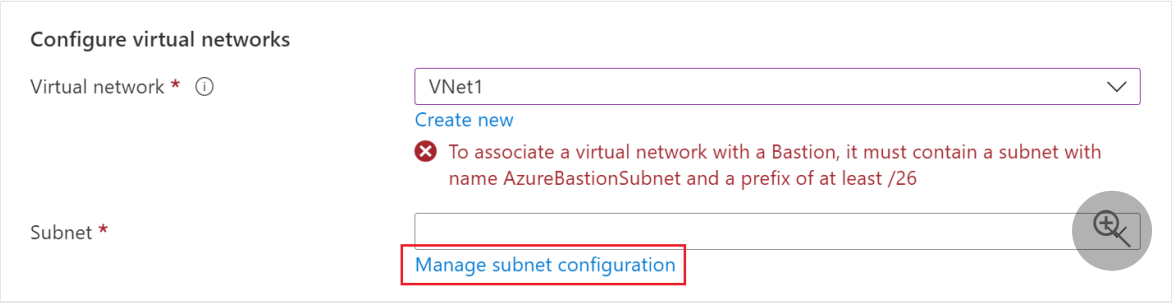
5. On the **Create a Bastion** page, configure the settings for your bastion host. Project details are populated from your virtual network values. Configure the **Instance details** values.

   - **Name**: Type the name that you want to use for your bastion resource.
   - **Region**: The Azure public region in which the resource will be created. Choose the region in which your virtual network resides.
   - **Tier:** The tier is also known as the **SKU**. For this tutorial, select **Standard**. The Standard SKU lets you configure the instance count for host scaling and other features. For more information about features that require the Standard SKU, see Configuration settings - SKU.
   - **Instance count:** This is the setting for **host scaling**. It's configured in scale unit increments. Use the slider or type a number to configure the instance count that you want. For this tutorial, you can select the instance count you'd prefer. For more information, see Host scaling and Pricing .



6. Configure the **virtual networks** settings. Select your VNet from the dropdown. If you don't see your VNet in the dropdown list, make sure you selected the correct Region in the previous settings on this page.

7. To configure the AzureBastionSubnet, select **Manage subnet configuration**.



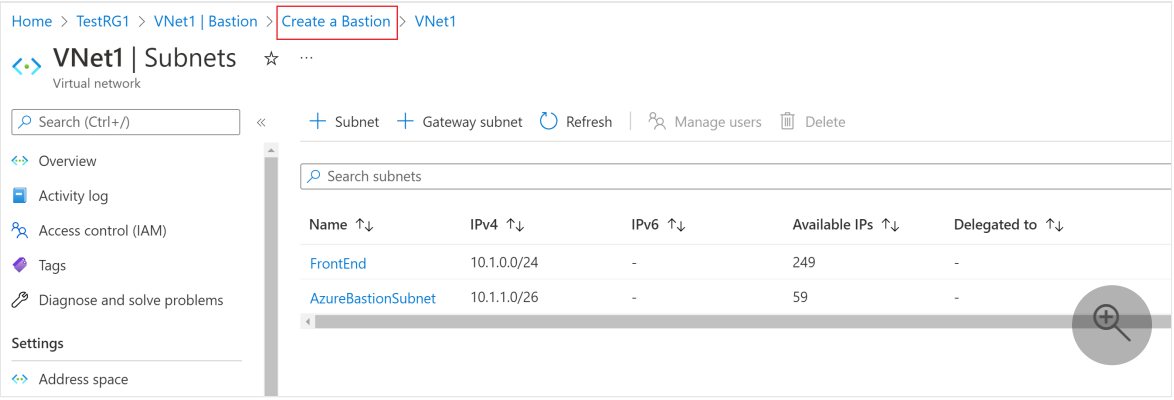
8. On the **Subnets** page, select **+Subnet** to open the **Add subnet** page.

9. On the **Add subnet page**, create the 'AzureBastionSubnet' subnet using the following values. Leave the other values as default.

   - The subnet name must be **AzureBastionSubnet**.
   - The subnet must be at least **/26 or larger** (/26, /25, /24 etc.) to accommodate features available with the Standard SKU.

   Select **Save** at the bottom of the page to save your values.

10. At the top of the **Subnets** page, select **Create a Bastion** to return to the Bastion configuration page.



11. The **Public IP address** section is where you configure the public IP address of the Bastion host resource on which RDP/SSH will be accessed (over port 443). The public IP address must be in the same region as the Bastion resource you're creating. Create a new IP address. You can leave the default naming suggestion.

12. When you finish specifying the settings, select **Review + Create**. This validates the values.

13. Once validation passes, you can deploy Bastion. Select **Create**. You'll see a message letting you know that your deployment is in process. Status will display on this page as the resources are created. It takes about 10 minutes for the Bastion resource to be created and deployed.

Connect to a VM

You can use any of the following detailed articles to connect to a VM. Some connection types require the Bastion Standard SKU.

- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

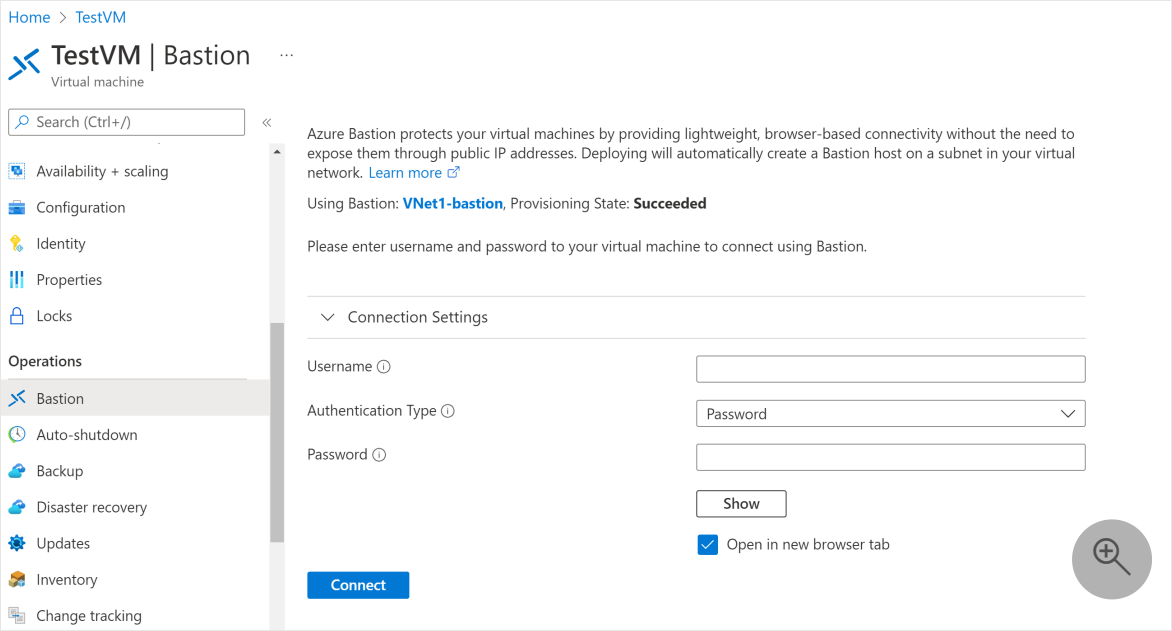
You can also use the basic Connection steps in the section below to connect to your VM.

Connection steps

1. In the Azure portal, go to the virtual machine to which you want to connect.

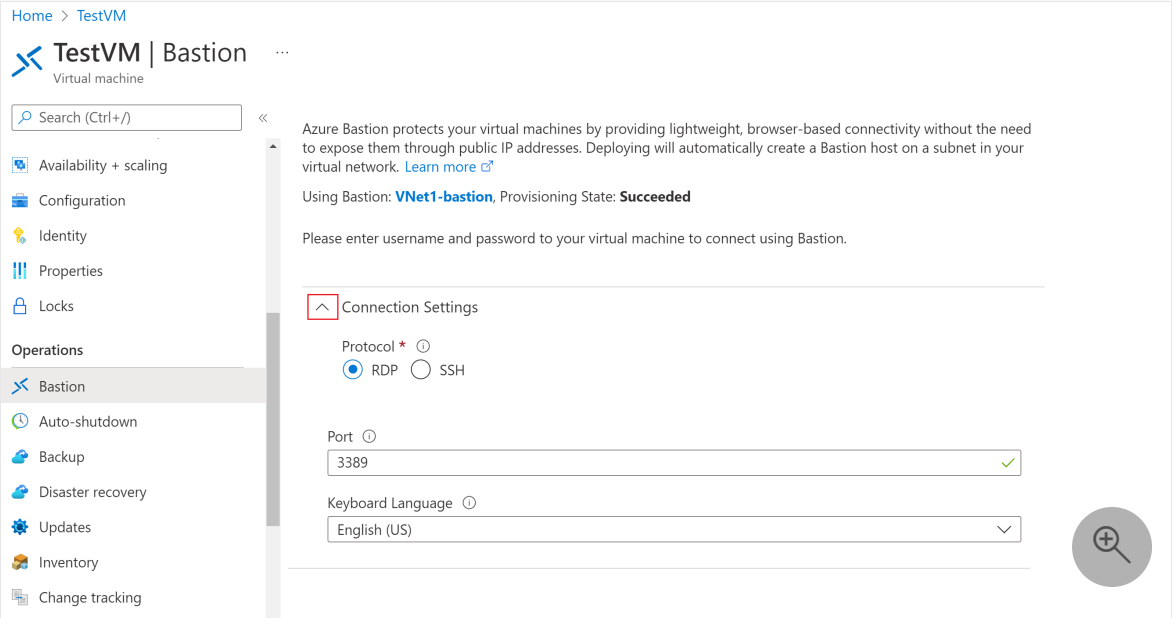
2. At the top of the page, select **Connect->Bastion** to go to the **Bastion** page. You can also go to the Bastion page using the left menu.

3. The options available on the **Bastion** page are dependant on the Bastion SKU tier. If you're using the **Basic SKU**, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22. You don't have options to change the port number or the protocol. However, you can change the keyboard language for RDP by expanding **Connection Settings**.

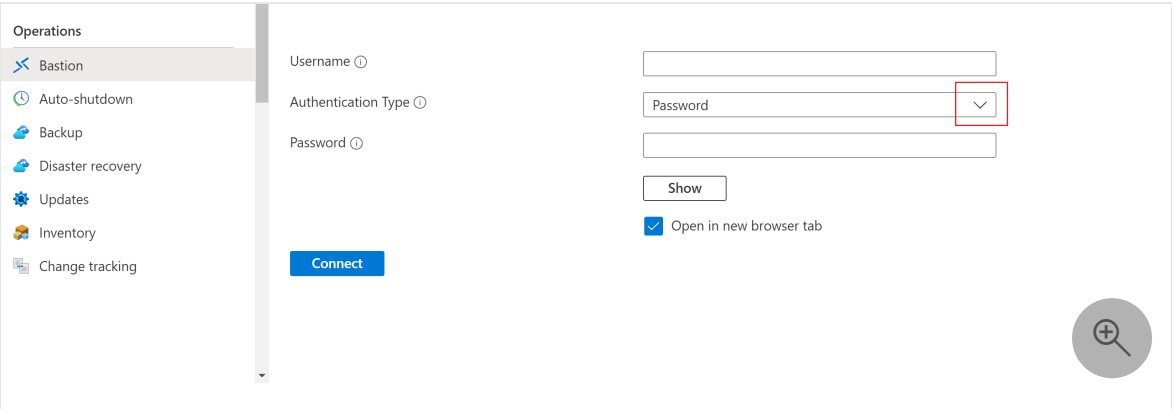


If you're using the **Standard SKU**, you have more connection protocol and port options available. Expand **Connection Settings** to see the options. Typically, unless

you have configured different settings for your VM, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22.



4. Select the **Authentication Type** from the dropdown. The protocol determines the available authentication types. Complete the required authentication values.



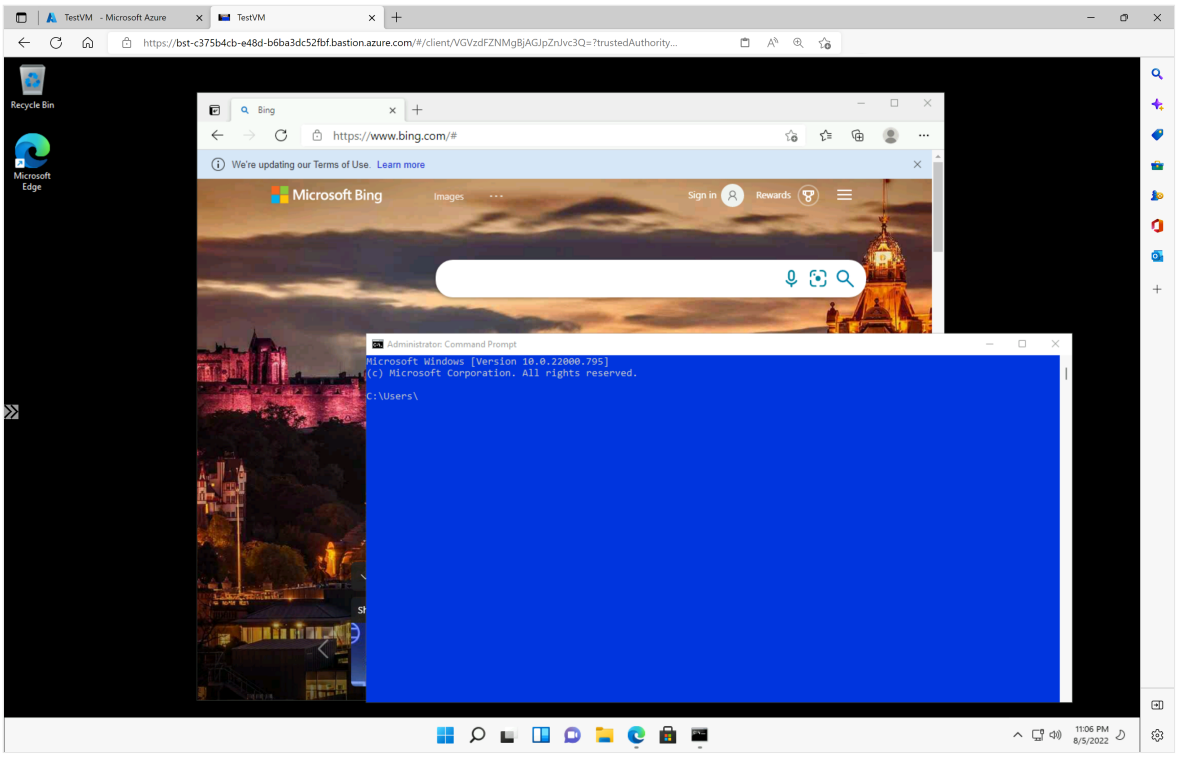
5. To open the VM session in a new browser tab, leave **Open in a new browser tab** selected.

6. Click **Connect** to connect to the VM.

7. The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

    - When you connect, the desktop of the VM will look different than the example screenshot.
    - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from

a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

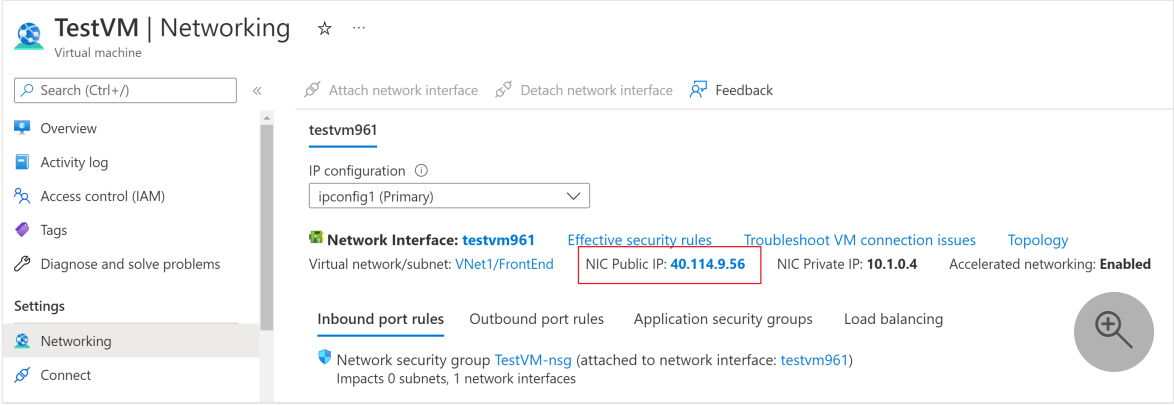
To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

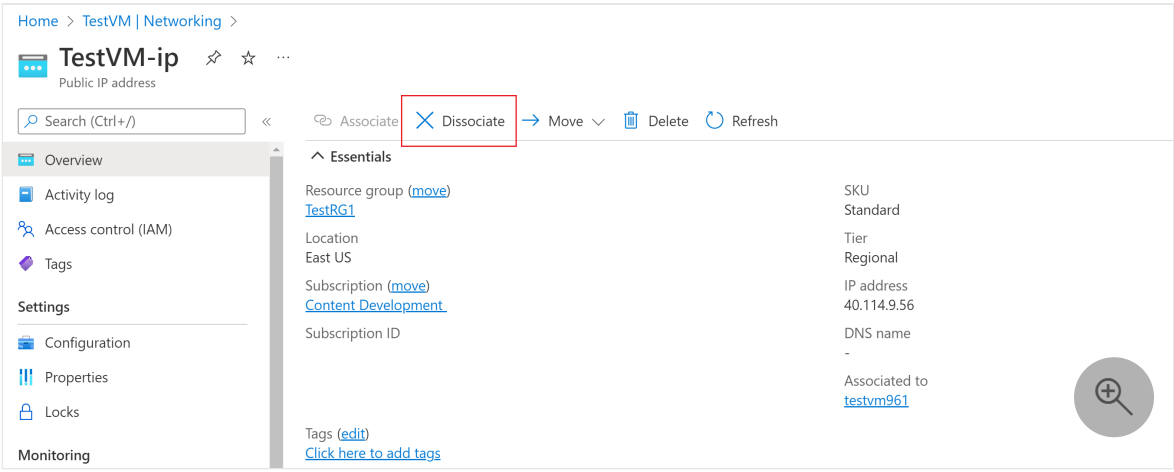
Remove VM public IP address

When you connect to a VM using Azure Bastion, you don't need a public IP address for your VM. If you aren't using the public IP address for anything else, you can dissociate it from your VM. To dissociate a public IP address from your VM, use the following steps:

1. Go to your virtual machine and select **Networking**. Click the **NIC Public IP** to open the Public IP address page.

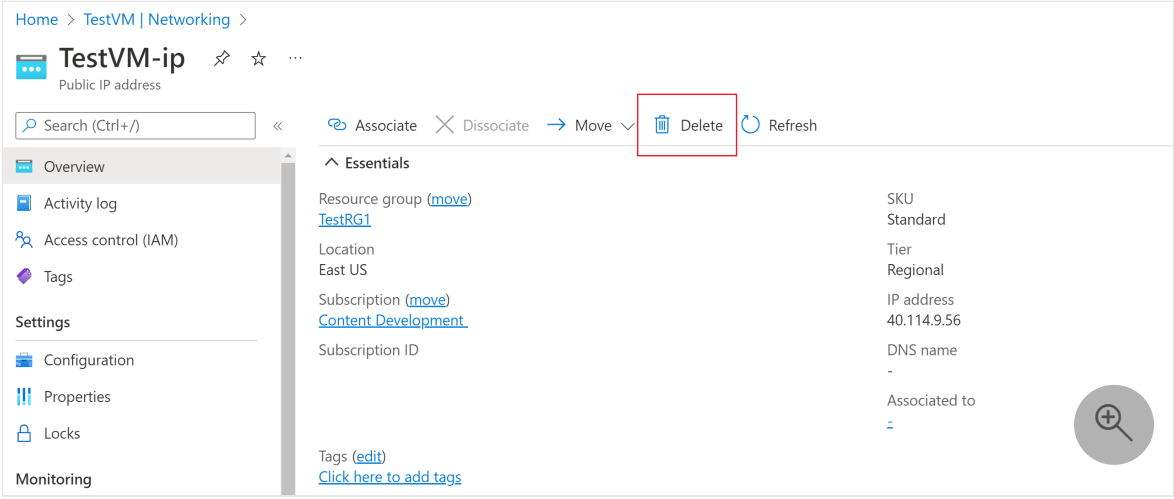


2. On the **Public IP address** page, you can see the VM network interface listed under **Associated to** on the lower right of the page. Click **Dissociate** at the top of the page.



3. Click **Yes** to dissociate the IP address from the network interface. Once the public IP address is dissociated from the VM network interface, you can see that it's no longer listed under **Associated to**.

4. After you dissociate the IP address, you can delete the public IP address resource. On the **Public IP address** page for the VM, select **Delete**.



5. Click **Yes** to delete the public IP address.

Clean up resources

If you're not going to continue to use this application, delete your resources using the following steps:

1. Enter the name of your resource group in the **Search** box at the top of the portal. When you see your resource group in the search results, select it.
2. Select **Delete resource group**.
3. Enter the name of your resource group for **TYPE THE RESOURCE GROUP NAME:** and select **Delete**.

Next steps

In this tutorial, you deployed Bastion to a virtual network and connected to a VM. You then removed the public IP address from the VM. Next, learn about and configure additional Bastion features.

Bastion features and configuration settings

Bastion - VM connections and features

Deploy Bastion using Azure PowerShell

Article • 03/08/2023 • 8 minutes to read

This article shows you how to deploy Azure Bastion with the Standard SKU using PowerShell. Azure Bastion is a PaaS service that's maintained for you, not a bastion host that you install on your VM and maintain yourself. An Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine. For more information about Azure Bastion, see What is Azure Bastion?

Once you deploy Bastion to your virtual network, you can connect to your VMs via private IP address. This seamless RDP/SSH experience is available to all the VMs in the same virtual network. If your VM has a public IP address that you don't need for anything else, you can remove it.

You can also deploy Bastion by using the following other methods:

- Azure portal
- Azure CLI
- Quickstart - deploy with default settings

If you don't have an Azure subscription, create a free account before you begin.

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Prerequisites

The following prerequisites are required.

Azure PowerShell

This article uses PowerShell cmdlets. To run the cmdlets, you can use Azure Cloud Shell. Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open Cloud Shell, just select **Try it** from the upper-right corner of a code block. You can also open Cloud Shell on a separate browser tab by going to

https://shell.azure.com/powershell. Select **Copy** to copy the blocks of code, paste them into Cloud Shell, and select the Enter key to run them.

You can also install and run the Azure PowerShell cmdlets locally on your computer. PowerShell cmdlets are updated frequently. If you have not installed the latest version, the values specified in the instructions may fail. To find the versions of Azure PowerShell installed on your computer, use the `Get-Module -ListAvailable Az` cmdlet. To install or update, see Install the Azure PowerShell module.

Example values

You can use the following example values when creating this configuration, or you can substitute your own.

Basic VNet and VM values:

Name	Value
Virtual machine	TestVM
Resource group	TestRG1
Region	East US
Virtual network	VNet1
Address space	10.1.0.0/16
Subnets	FrontEnd: 10.1.0.0/24

Azure Bastion values:

Name	Value
Name	VNet1-bastion
Subnet Name	FrontEnd
Subnet Name	AzureBastionSubnet
AzureBastionSubnet addresses	A subnet within your VNet address space with a subnet mask /26 or larger. For example, 10.1.1.0/26.
Tier/SKU	Standard
Public IP address	Create new

Name	Value
Public IP address name	VNet1-ip
Public IP address SKU	Standard
Assignment	Static

Deploy Bastion

This section helps you create a virtual network, subnets, and deploy Azure Bastion using Azure PowerShell.

1. Create an Azure resource group with New-AzResourceGroup. A resource group is a logical container into which Azure resources are deployed and managed. If you're running PowerShell locally, open your PowerShell console with elevated privileges and connect to Azure using the `Connect-AzAccount` command.

   Azure PowerShell

   ```
   New-AzResourceGroup -Name TestRG1 -Location EastUS
   ```

2. Create a virtual network.

   Azure PowerShell

   ```
   $virtualNetwork = New-AzVirtualNetwork `
   -ResourceGroupName TestRG1 `
   -Location EastUS `
   -Name VNet1 `
   -AddressPrefix 10.1.0.0/16
   ```

3. Set the configuration for the virtual network.

   Azure PowerShell

   ```
   $virtualNetwork | Set-AzVirtualNetwork
   ```

4. Configure and set a subnet for your virtual network. This will be the subnet to which you'll deploy a VM. The variable used for *-VirtualNetwork* was set in the previous steps.

   Azure PowerShell

```
$subnetConfig = Add-AzVirtualNetworkSubnetConfig `
-Name 'FrontEnd' `
-AddressPrefix 10.1.0.0/24 `
-VirtualNetwork $virtualNetwork
```

Azure PowerShell

```
$virtualNetwork | Set-AzVirtualNetwork
```

5. Configure and set the Azure Bastion subnet for your virtual network. This subnet is reserved exclusively for Azure Bastion resources. You must create the Azure Bastion subnet using the name value **AzureBastionSubnet**. This value lets Azure know which subnet to deploy the Bastion resources to. The example below also helps you add an Azure Bastion subnet to an existing VNet.

> **Important**
>
> For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

- The smallest subnet AzureBastionSubnet size you can create is /26. We recommend that you create a /26 or larger size to accommodate host scaling.
  - For more information about scaling, see Configuration settings - Host scaling.
  - For more information about settings, see Configuration settings - AzureBastionSubnet.
- Create the **AzureBastionSubnet** without any route tables or delegations.
- If you use Network Security Groups on the **AzureBastionSubnet**, refer to the Work with NSGs article.

Declare the variable.

Azure PowerShell

```
$virtualNetwork = Get-AzVirtualNetwork -Name "VNet1" `
-ResourceGroupName "TestRG1"
```

Add the configuration.

Azure PowerShell

```
Add-AzVirtualNetworkSubnetConfig -Name "AzureBastionSubnet" `
-VirtualNetwork $virtualNetwork -AddressPrefix "10.1.1.0/26" `
```

Set the configuration.

Azure PowerShell

```
$virtualNetwork | Set-AzVirtualNetwork
```

6. Create a public IP address for Azure Bastion. The public IP is the public IP address the Bastion resource on which RDP/SSH will be accessed (over port 443). The public IP address must be in the same region as the Bastion resource you're creating.

Azure PowerShell

```
$publicip = New-AzPublicIpAddress -ResourceGroupName "TestRG1" -name
"VNet1-ip" -location "EastUS" -AllocationMethod Static -Sku Standard
```

7. Create a new Azure Bastion resource in the AzureBastionSubnet using the New-AzBastion command. The following example uses the **Standard SKU**. The Standard SKU lets you configure more Bastion features and connect to VMs using more connection types. For more information, see Bastion SKUs. If you want to deploy using the Basic SKU, change the -Sku value to "Basic".

Azure PowerShell

```
New-AzBastion -ResourceGroupName "TestRG1" -Name "VNet1-bastion" `
-PublicIpAddressRgName "TestRG1" -PublicIpAddressName "VNet1-ip" `
-VirtualNetworkRgName "TestRG1" -VirtualNetworkName "VNet1" `
-Sku "Standard"
```

8. It takes about 10 minutes for the Bastion resources to deploy. You can create a VM in the next section while Bastion deploys to your virtual network.

Create a VM

You can create a VM using the Quickstart: Create a VM using PowerShell or Quickstart: Create a VM using the portal articles. Be sure you deploy the VM to the virtual network

to which you deployed Bastion. The VM you create in this section isn't a part of the Bastion configuration and doesn't become a bastion host. You connect to this VM later in this tutorial via Bastion.

The following required roles for your resources.

- Required VM roles:
  - Reader role on the virtual machine.
  - Reader role on the NIC with private IP of the virtual machine.

- Required inbound ports:
  - For Windows VMS - RDP (3389)
  - For Linux VMs - SSH (22)

Connect to a VM

You can use the Connection steps in the section below to connect to your VM. You can also use any of the following articles to connect to a VM. Some connection types require the Bastion Standard SKU.

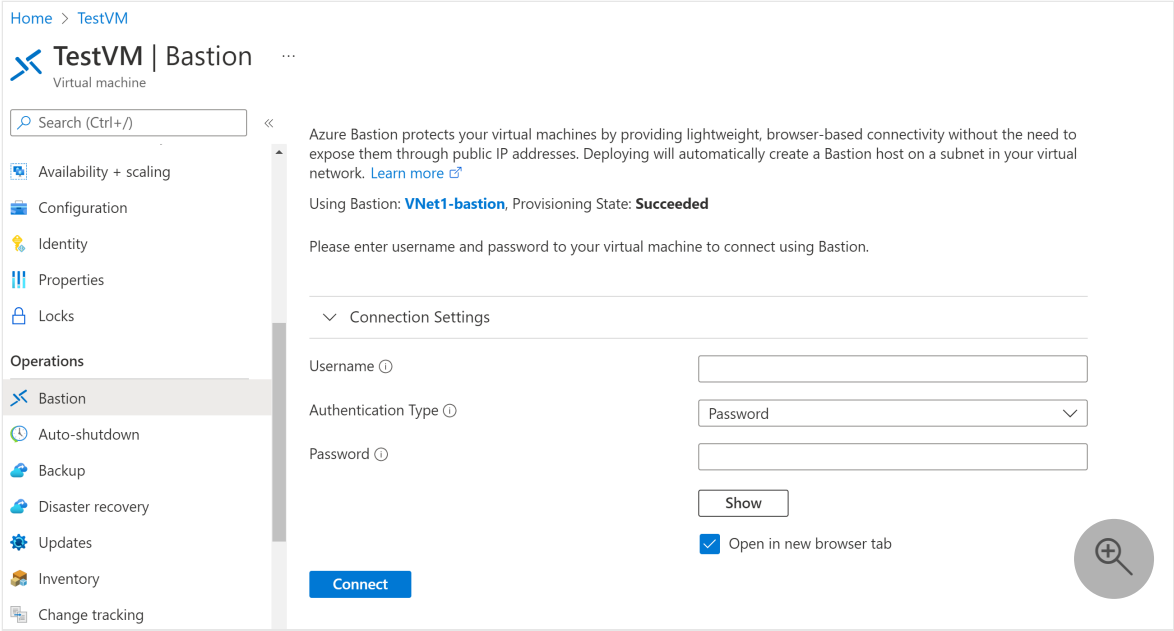
- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

Connection steps

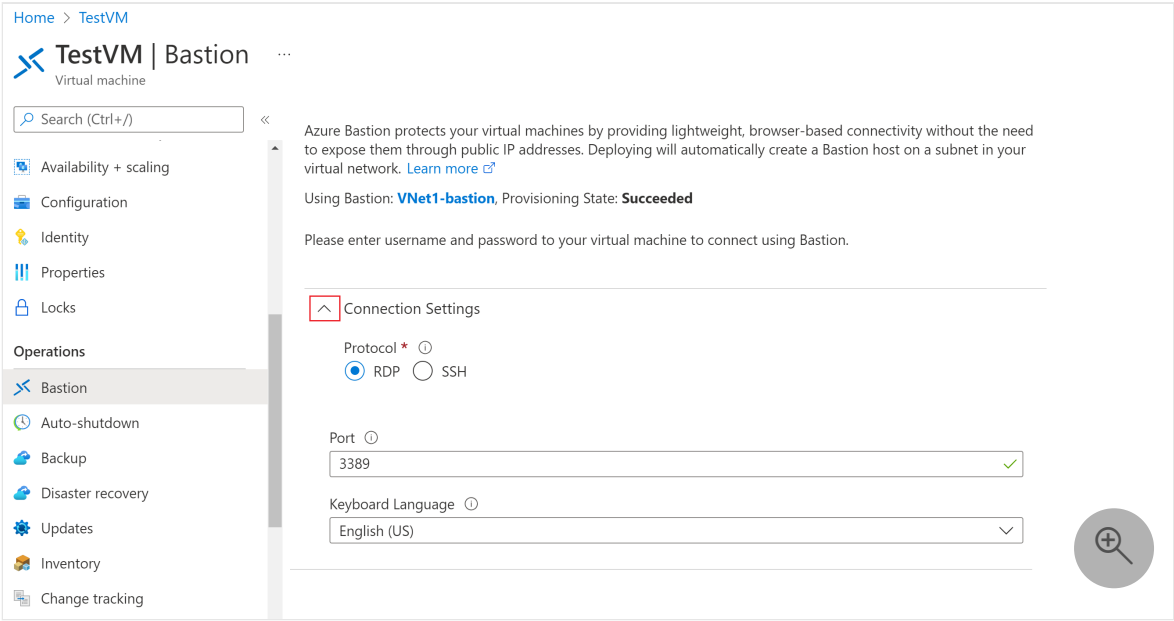
1. In the Azure portal, go to the virtual machine to which you want to connect.

2. At the top of the page, select **Connect->Bastion** to go to the **Bastion** page. You can also go to the Bastion page using the left menu.

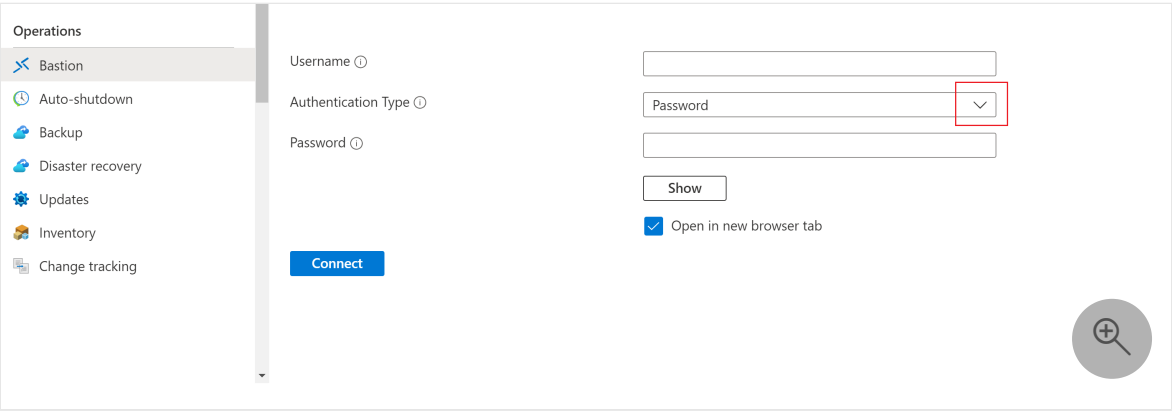
3. The options available on the **Bastion** page are dependant on the Bastion SKU tier. If you're using the **Basic SKU**, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22. You don't have options to change the port number or the protocol. However, you can change the keyboard language for RDP by expanding **Connection Settings**.



If you're using the **Standard SKU**, you have more connection protocol and port options available. Expand **Connection Settings** to see the options. Typically, unless you have configured different settings for your VM, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22.



4. Select the **Authentication Type** from the dropdown. The protocol determines the available authentication types. Complete the required authentication values.

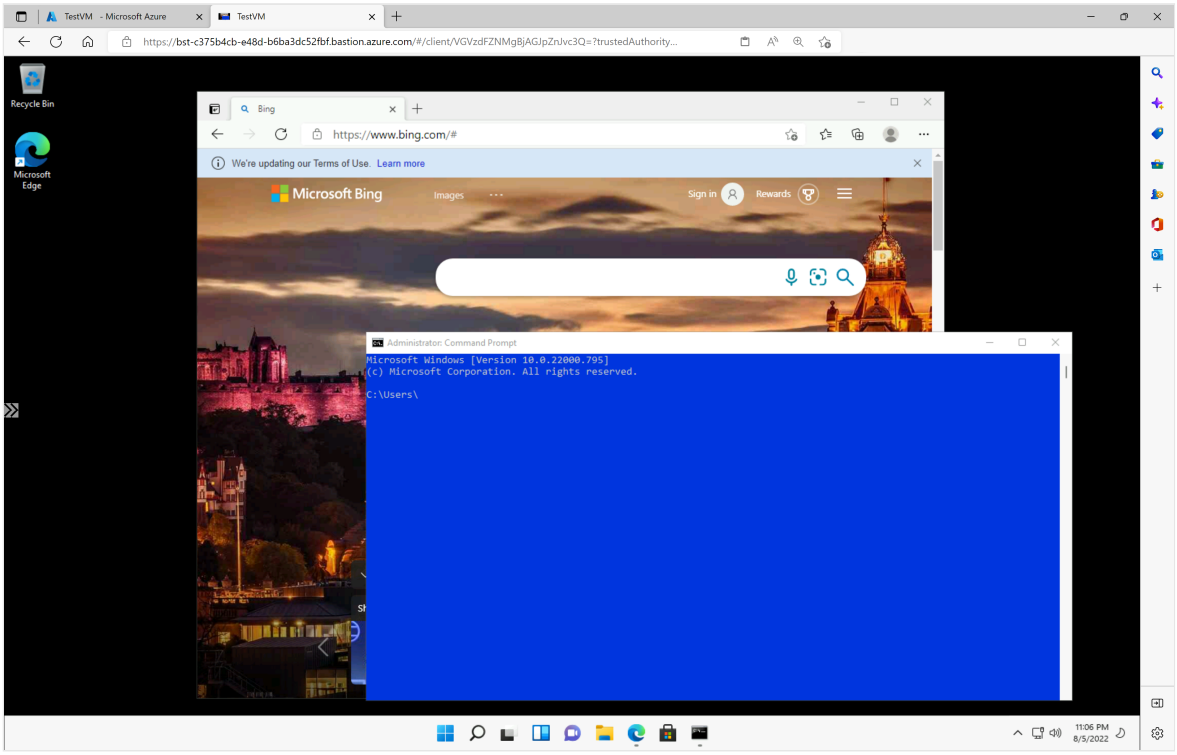


5. To open the VM session in a new browser tab, leave **Open in a new browser tab** selected.

6. Click **Connect** to connect to the VM.

7. The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

    - When you connect, the desktop of the VM will look different than the example screenshot.
    - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

Remove VM public IP address

Azure Bastion doesn't use the public IP address to connect to the client VM. If you don't need the public IP address for your VM, you can disassociate the public IP address. See Dissociate a public IP address from an Azure VM.

Next steps

- To use Network Security Groups with the Azure Bastion subnet, see Work with NSGs.
- To understand VNet peering, see VNet peering and Azure Bastion.

Additional resources

Documentation

Azure PowerShell samples for virtual network

Learn about Azure PowerShell samples for managing virtual networks, including a sample for creating a virtual network for multi-tier applications.

Quickstart: Create a virtual network - Azure PowerShell - Azure Virtual Network

In this quickstart, you create a virtual network using the Azure portal. A virtual network lets Azure resources communicate with each other and with the internet.

Create, change, or delete an Azure network interface

Learn what a network interface is and how to create, change settings for, and delete one.

Quickstart to diagnose a VM network traffic filter problem - Azure CLI - Azure Network Watcher

Learn how to use Azure CLI to diagnose a virtual machine network traffic filter problem using the IP flow verify capability of Azure Network Watcher.

Create and manage Windows VMs in Azure that use multiple NICs - Azure Virtual Machines

Learn how to create and manage a Windows VM that has multiple NICs attached to it by using Azure PowerShell or Resource Manager templates.

Upgrade a SKU - Azure Bastion

Learn how to change Tiers from the Basic to the Standard SKU.

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Quickstart: Create a public IP - PowerShell - Azure Virtual Network

In this quickstart, learn how to create a public IP using Azure PowerShell

Show 5 more

Training

Module

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Deploy Bastion using Azure CLI

Article • 03/15/2022 • 6 minutes to read

This article shows you how to deploy Azure Bastion using CLI. Azure Bastion is a PaaS service that's maintained for you, not a bastion host that you install on your VM and maintain yourself. An Azure Bastion deployment is per virtual network, not per subscription/account or virtual machine. For more information about Azure Bastion, see What is Azure Bastion?

Once you deploy Bastion to your virtual network, you can connect to your VMs via private IP address. This seamless RDP/SSH experience is available to all the VMs in the same virtual network. If your VM has a public IP address that you don't need for anything else, you can remove it.

You can also deploy Bastion by using the following other methods:

- Azure portal
- Azure PowerShell
- Quickstart - deploy with default settings

Prerequisites

Azure subscription

Verify that you have an Azure subscription. If you don't already have an Azure subscription, you can activate your MSDN subscriber benefits or sign up for a free account.

Azure CLI

This article uses the Azure CLI. To run commands, you can use Azure Cloud Shell. The Azure Cloud Shell is a free interactive shell that you can use to run the steps in this article. It has common Azure tools preinstalled and configured to use with your account.

To open the Cloud Shell, just select **Try it** from the upper right corner of a code block. You can also launch Cloud Shell in a separate browser tab by going to https://shell.azure.com and toggle the dropdown in the left corner to reflect Bash or PowerShell. Select **Copy** to copy the blocks of code, paste it into the Cloud Shell, and press enter to run it.

> **Note**
>
> The use of Azure Bastion with Azure Private DNS Zones is not supported at this time. Before you begin, please make sure that the virtual network where you plan to deploy your Bastion resource is not linked to a private DNS zone.

Deploy Bastion

This section helps you deploy Azure Bastion using Azure CLI.

> **Note**
>
> As shown in the examples, use the `--location` parameter with `--resource-group` for every command to ensure that the resources are deployed together.

1. Create a virtual network and an Azure Bastion subnet. You must create the Azure Bastion subnet using the name value **AzureBastionSubnet**. This value lets Azure know which subnet to deploy the Bastion resources to. This is different than a VPN gateway subnet.

   > **Important**
   >
   > For Azure Bastion resources deployed on or after November 2, 2021, the minimum AzureBastionSubnet size is /26 or larger (/25, /24, etc.). All Azure Bastion resources deployed in subnets of size /27 prior to this date are unaffected by this change and will continue to work, but we highly recommend increasing the size of any existing AzureBastionSubnet to /26 in case you choose to take advantage of **host scaling** in the future.

   - The smallest subnet AzureBastionSubnet size you can create is /26. We recommend that you create a /26 or larger size to accommodate host scaling.
     - For more information about scaling, see Configuration settings - Host scaling.
     - For more information about settings, see Configuration settings - AzureBastionSubnet.
   - Create the **AzureBastionSubnet** without any route tables or delegations.
   - If you use Network Security Groups on the **AzureBastionSubnet**, refer to the Work with NSGs article.

Azure CLI

```
az network vnet create --resource-group MyResourceGroup --name MyVnet --address-prefix 10.0.0.0/16 --subnet-name AzureBastionSubnet --subnet-prefix 10.0.0.0/24 --location northeurope
```

2. Create a public IP address for Azure Bastion. The public IP is the public IP address the Bastion resource on which RDP/SSH will be accessed (over port 443). The public IP address must be in the same region as the Bastion resource you're creating.

   The following example uses the **Standard SKU**. The Standard SKU lets you configure more Bastion features and connect to VMs using more connection types. For more information, see Bastion SKUs.

   Azure CLI

   ```
   az network public-ip create --resource-group MyResourceGroup --name MyIp --sku Standard --location northeurope
   ```

3. Create a new Azure Bastion resource in the AzureBastionSubnet of your virtual network. It takes about 10 minutes for the Bastion resource to create and deploy.

   Azure CLI

   ```
   az network bastion create --name MyBastion --public-ip-address MyIp --resource-group MyResourceGroup --vnet-name MyVnet --location northeurope
   ```

Connect to a VM

You can use the Connection steps in the section below to connect to your VM. You can also use any of the following articles to connect to a VM. Some connection types require the Bastion Standard SKU.

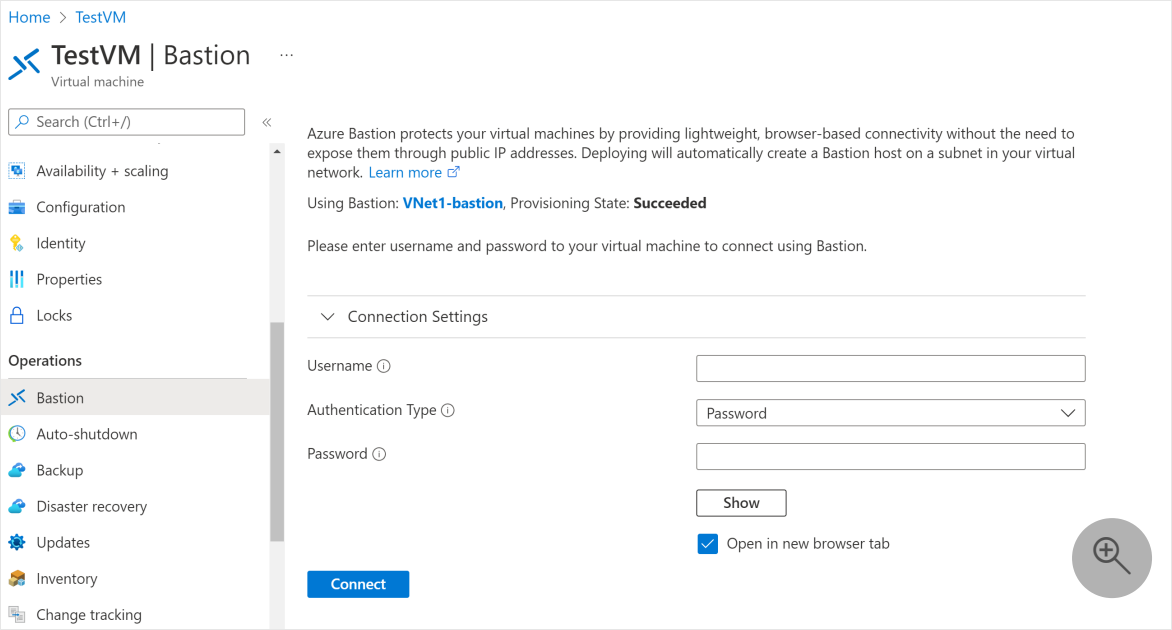
- Windows - RDP
- Windows - SSH
- Linux - SSH
- Linux - RDP
- Connect from a local computer using a native client
- Connect to a scale set

Connection steps

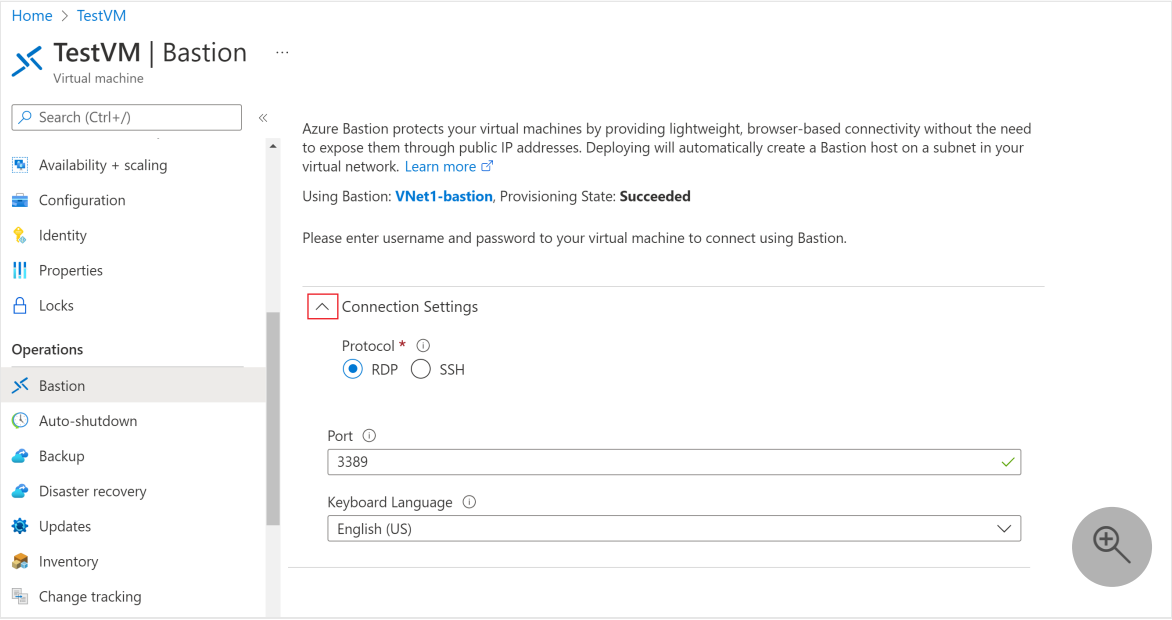
1. In the Azure portal, go to the virtual machine to which you want to connect.

2. At the top of the page, select **Connect->Bastion** to go to the **Bastion** page. You can also go to the Bastion page using the left menu.

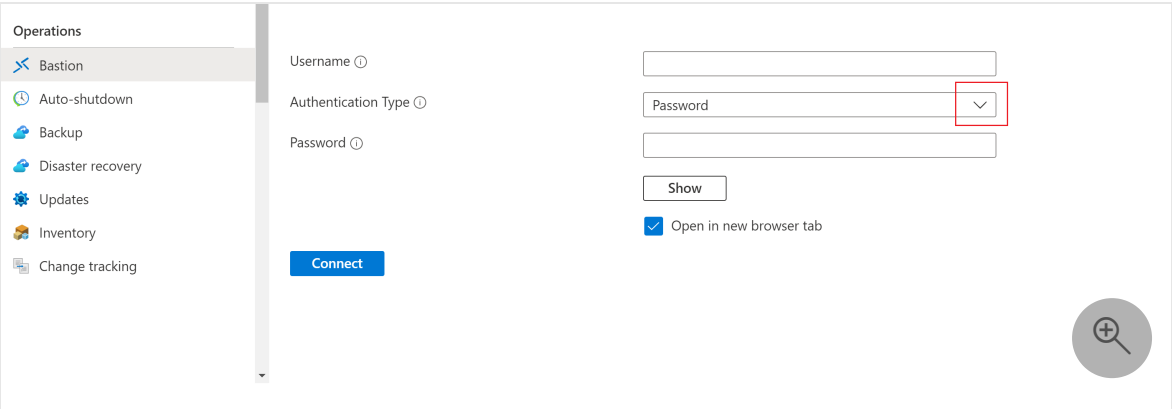
3. The options available on the **Bastion** page are dependant on the Bastion SKU tier. If you're using the **Basic SKU**, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22. You don't have options to change the port number or the protocol. However, you can change the keyboard language for RDP by expanding **Connection Settings**.



If you're using the **Standard SKU**, you have more connection protocol and port options available. Expand **Connection Settings** to see the options. Typically, unless you have configured different settings for your VM, you connect to a Windows computer using RDP and port 3389, and to a Linux computer using SSH and port 22.



4. Select the **Authentication Type** from the dropdown. The protocol determines the available authentication types. Complete the required authentication values.

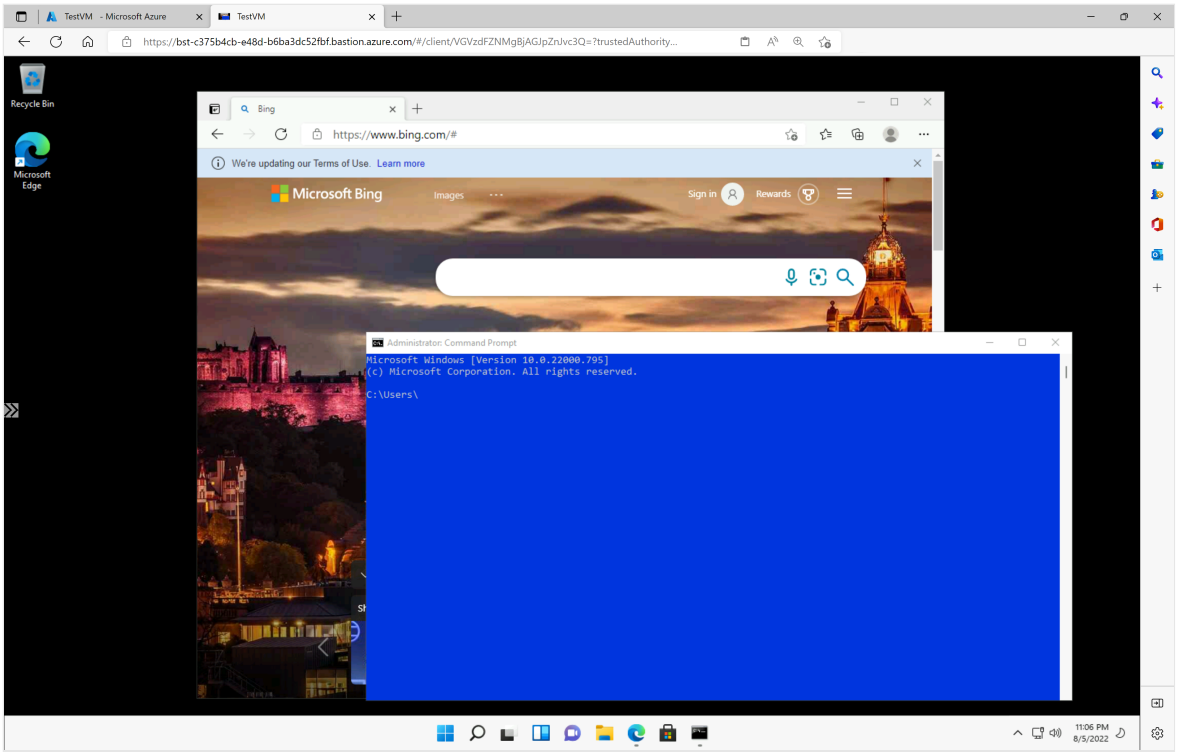


5. To open the VM session in a new browser tab, leave **Open in a new browser tab** selected.

6. Click **Connect** to connect to the VM.

7. The connection to this virtual machine, via Bastion, will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

    - When you connect, the desktop of the VM will look different than the example screenshot.
    - Using keyboard shortcut keys while connected to a VM may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.



To enable audio output

You can enable remote audio output for your VM. Some VMs automatically enable this setting, others require you to enable audio settings manually. The settings are changed on the VM itself. Your Bastion deployment doesn't need any special configuration settings to enable remote audio output.

> **Note**
>
> Audio output takes up bandwidth on your internet connection.

To enable remote audio output on a Windows VM:

1. After you're connected to the VM, on the right-hand bottom corner of the toolbar, you'll see an audio button.
2. Right-click the audio button and select "Sounds".
3. A pop-up appears asking if you would like to enable the Windows Audio Service. Select "Yes". You can configure more audio options in Sound preferences.
4. To verify sound output, hover your mouse over the audio button on the toolbar.

Remove VM public IP address

Azure Bastion doesn't use the public IP address to connect to the client VM. If you don't need the public IP address for your VM, you can disassociate the public IP address. See

Dissociate a public IP address from an Azure VM.

Next steps

- To use Network Security Groups with the Azure Bastion subnet, see Work with NSGs.
- To understand VNet peering, see VNet peering and Azure Bastion.

Upgrade a SKU

Article • 08/03/2022 • 2 minutes to read

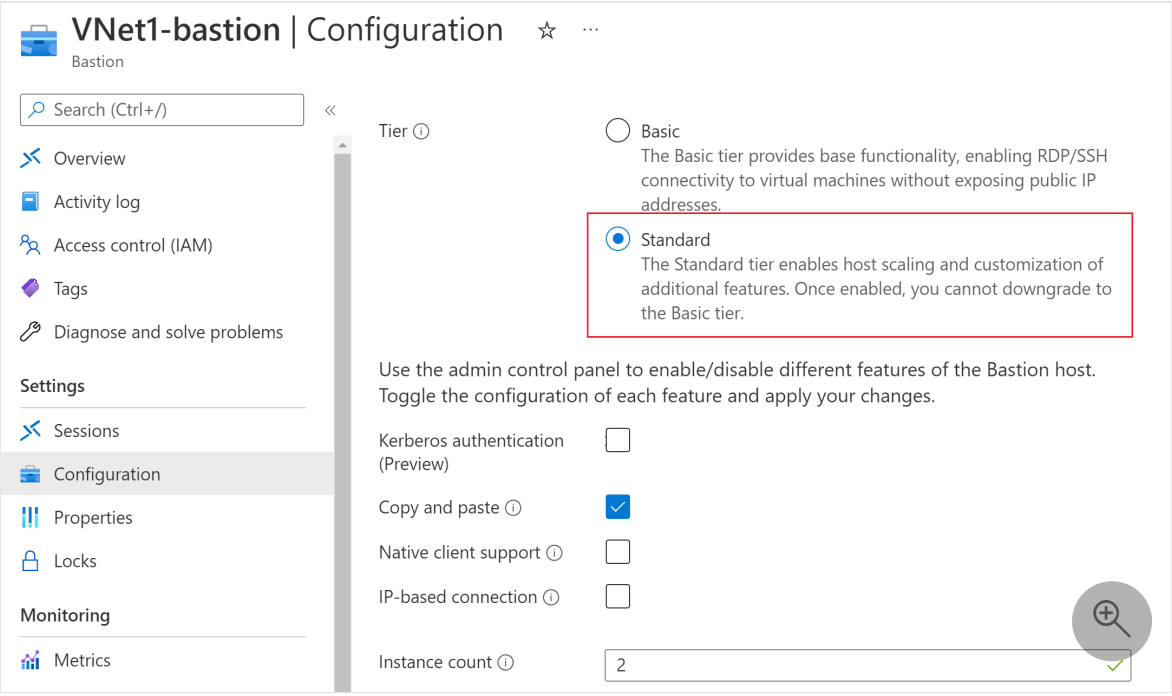
This article helps you upgrade from the Basic Tier (SKU) to Standard. Once you upgrade, you can't revert back to the Basic SKU without deleting and reconfiguring Bastion. Currently, this setting can be configured in the Azure portal only. For more information about features and SKUs, see Configuration settings.

Configuration steps

1. Sign in to the Azure portal.

2. In the Azure portal, go to your Bastion host.

3. On the **Configuration** page, for **Tier**, select **Standard**.



4. You can add features at the same time you upgrade the SKU. You don't need to upgrade the SKU and then go back to add the features as a separate step.

5. Click **Apply** to apply changes. The bastion host will update. This takes about 10 minutes to complete.

Next steps

- See Configuration settings for more configuration information.
- Read the Bastion FAQ.

Configure host scaling using the Azure portal

Article • 08/03/2022 • 2 minutes to read

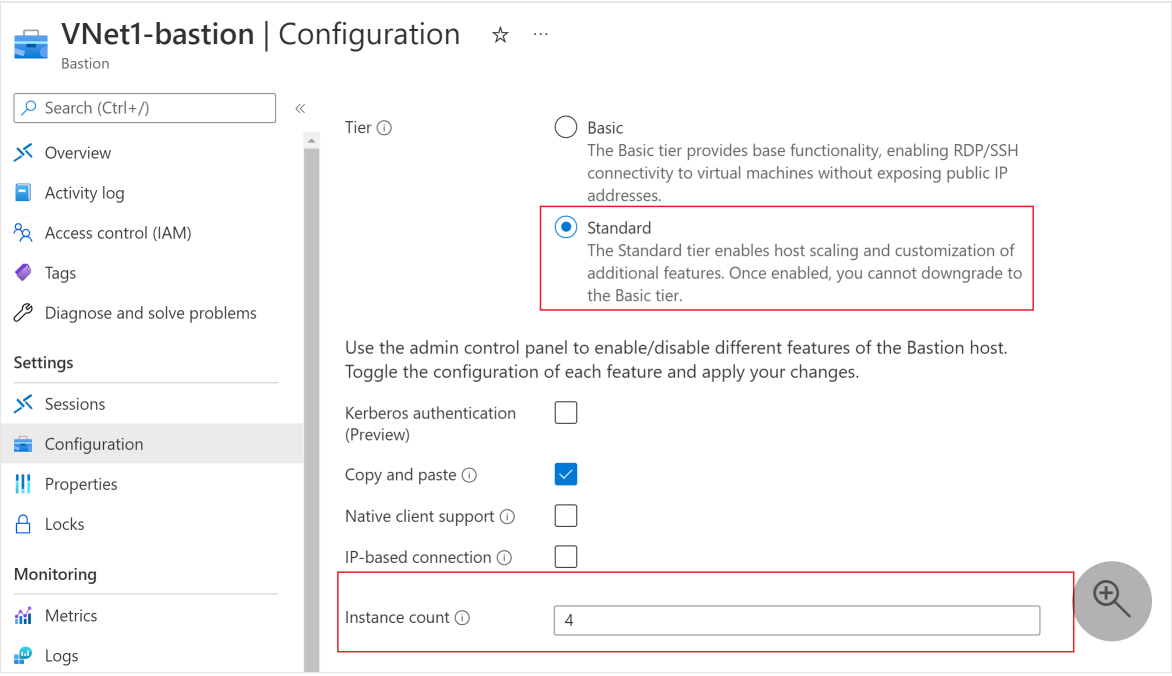
This article helps you add additional scale units (instances) to Azure Bastion to accommodate additional concurrent client connections using the Azure portal. For more information about host scaling, see Configuration settings.

Configuration steps

1. Sign in to the Azure portal.

2. In the Azure portal, go to your Bastion host.

3. Host scaling instance count requires Standard tier. On the **Configuration** page, for **Tier**, verify the tier is **Standard**. If the tier is Basic, select **Standard**. To configure scaling, adjust the instance count. Each instance is a scale unit.



4. Click **Apply** to apply changes.

> **Note**
>
> Any changes to the host scale units will disrupt active bastion connections.

Next steps

For more information about configuration settings, see Azure Bastion configuration settings.

Configure host scaling using Azure PowerShell

Article • 11/30/2021 • 2 minutes to read

This article helps you add additional scale units (instances) to Azure Bastion to accommodate additional concurrent client connections using PowerShell. For more information about host scaling, see Configuration settings.

Configuration steps

1. Get the target Bastion resource. Use the example below, modifying the values as needed.

   Azure PowerShell

   ```
   $bastion = Get-AzBastion -Name bastion -ResourceGroupName bastion-rg
   ```

2. Set the target scale unit, also known as "instance count". In the following example, we set the scale units to 5.

   Azure PowerShell

   ```
   $bastion.ScaleUnit = 5
   Set-AzBastion -InputObject $bastion
   ```

3. Confirm "Y" to overwrite the resource. After the resource is overwritten, the specified value is shown in the output for "Scale Units".

   > **Note**
   >
   > Any changes to the host scale units will disrupt active bastion connections.

Next steps

For more information about configuration settings, see Azure Bastion configuration settings.

Create a shareable link for Bastion - preview

Article • 03/08/2023 • 4 minutes to read

The Bastion **Shareable Link** feature lets users connect to a target resource (virtual machine or virtual machine scale set) using Azure Bastion without accessing the Azure portal. This article helps you use the Shareable Link feature to create a shareable link for an existing Azure Bastion deployment.

When a user without Azure credentials clicks a shareable link, a webpage opens that prompts the user to sign in to the target resource via RDP or SSH. Users authenticate using username and password or private key, depending on what you have configured for the target resource. The shareable link does not contain any credentials - the admin must provide sign-in credentials to the user.

By default, users in your org will have only read access to shared links. If a user has read access, they'll only be able to use and view shared links, but can't create or delete a shareable link. For more information, see the Permissions section of this article.

Considerations

- Shareable Links isn't currently supported for peered VNets that aren't in the same subscription.
- Shareable Links isn't currently supported for peered VNEts across tenants.
- Shareable Links isn't currently supported for peered VNets that aren't in the same region.
- Shareable Links isn't supported for national clouds during preview.
- The Standard SKU is required for this feature.

Prerequisites

- Azure Bastion is deployed to your VNet. See Tutorial - Deploy Bastion using manual settings for steps.

- Bastion must be configured to use the **Standard** SKU for this feature. You can update the SKU from Basic to Standard when you configure the shareable links feature.

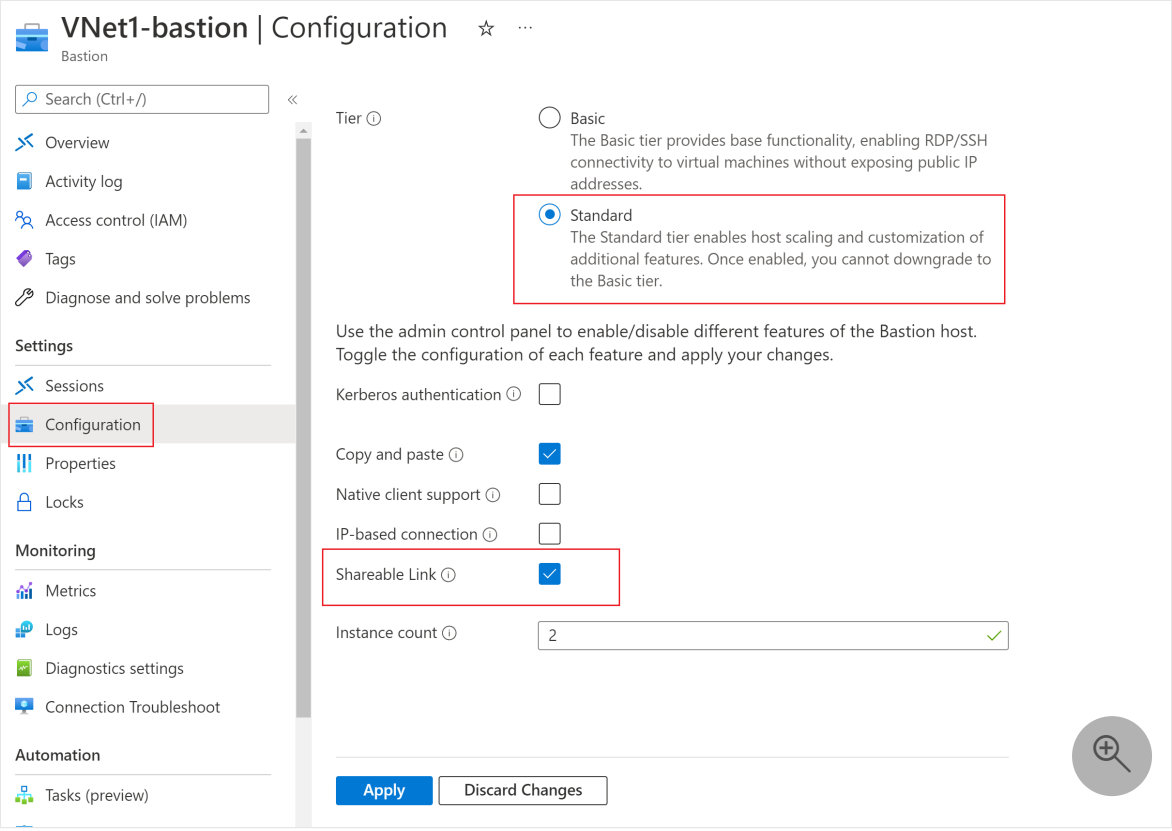
- The VNet contains the VM resource to which you want to create a shareable link.

Enable Shareable Link feature

Before you can create a shareable link to a VM, you must first enable the feature.

1. In the Azure portal, go to your bastion resource.

2. On your **Bastion** page, in the left pane, click **Configuration**.



3. On the **Configuration** page, for **Tier**, select **Standard** if it isn't already selected. This feature requires the **Standard SKU**.

4. Select **Shareable Link** from the listed features to enable the Shareable Link feature.

5. Verify that you've selected the settings that you want, then click **Apply**.

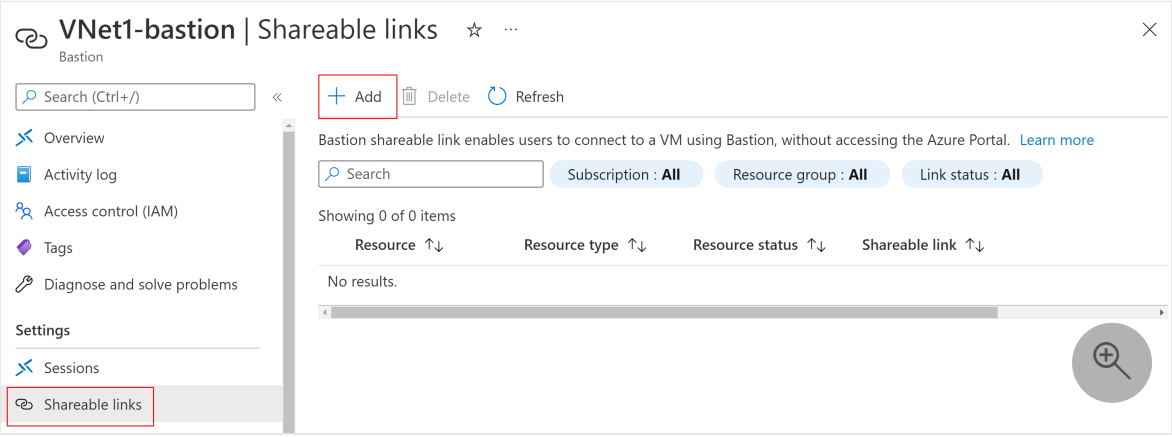
6. Bastion will immediately begin updating the settings for your bastion host. Updates will take about 10 minutes.

Create shareable links

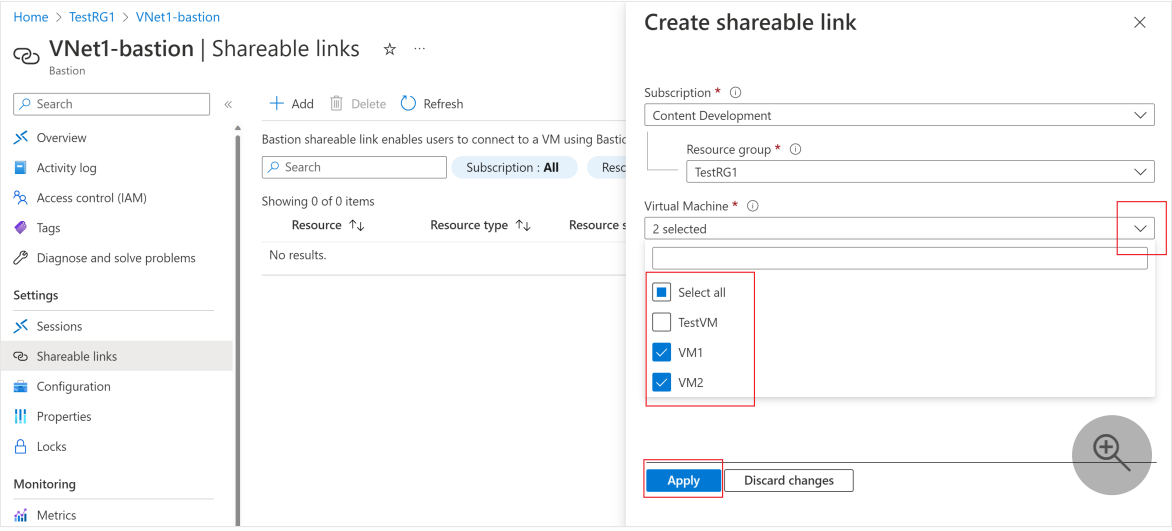
In this section, you specify each resource for which you want to create a shareable link

1. In the Azure portal, go to your bastion resource.

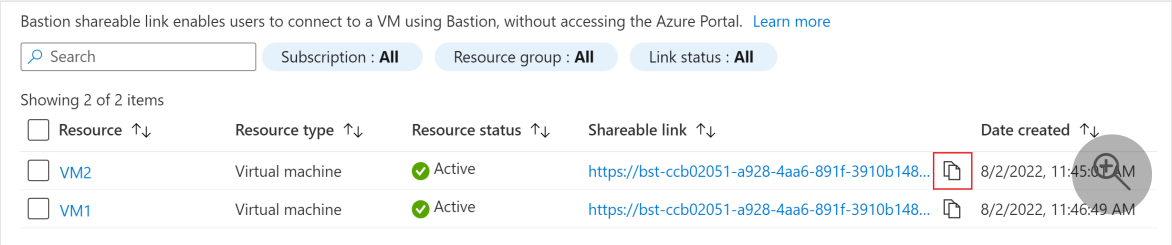
2. On your bastion page, in the left pane, click **Shareable links**. Click + **Add** to open the **Create shareable link** page.



3. On the **Create shareable link** page, select the resources for which you want to create a shareable link. You can select specific resources, or you can select all. A separate shareable link will be created for each selected resource. Click **Apply** to create links.



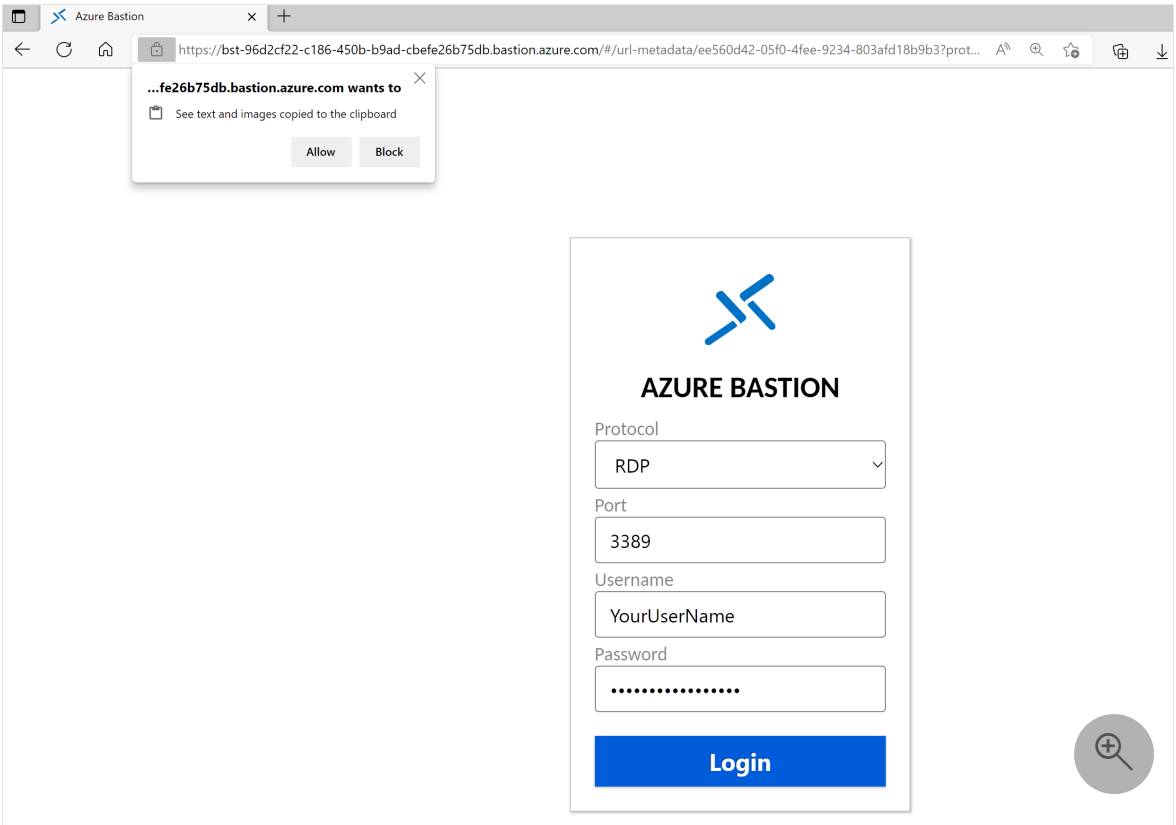
4. Once the links are created, you can view them on the **Shareable links** page. The following example shows links for multiple resources. You can see that each resource has a separate link and the link status is **Active**. To share a link, copy it, then send it to the user. The link doesn't contain authentication credentials.



Connect to a VM

1. After receiving the link, the user opens the link in their browser.

2. In the left corner, the user can select whether to see text and images copied to the clipboard. The user inputs the required information, then clicks **Login** to connect. A shared link doesn't contain authentication credentials. The admin must provide sign-in credentials to the user. Custom port and protocols are supported.

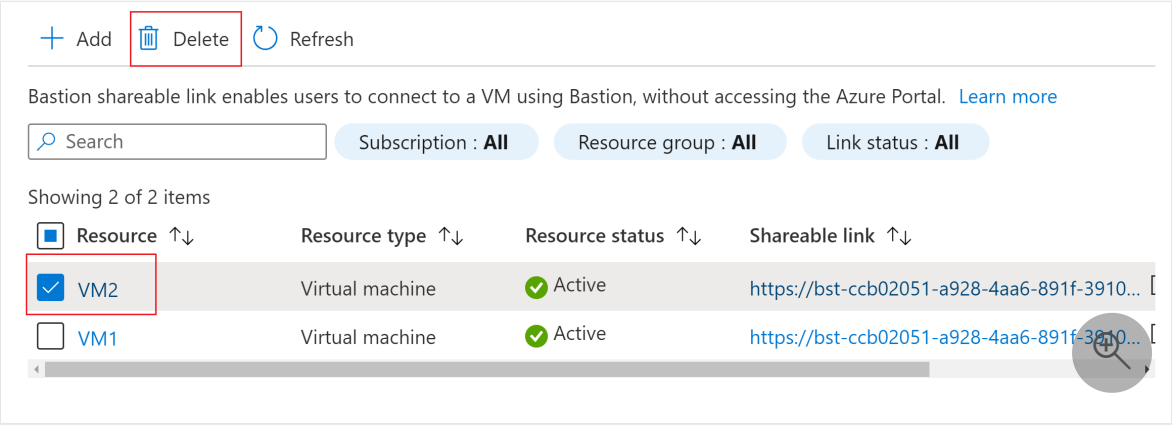


> **Note**
>
> If a link is no longer able to be opened, this means that someone in your organization has deleted that resource. While you'll still be able to see the shared links in your list, it will no longer connect to the target resource and will lead to a connection error. You can delete the shared link in your list, or keep it for auditing purposes.

Delete a shareable link

1. In the Azure portal, go to your **Bastion resource -> Shareable Links**.

2. On the **Shareable Links** page, select the resource link that you want to delete, then click **Delete**.



Permissions

Permissions to the Shareable Link feature are configured using Access control (IAM). By default, users in your org will have only read access to shared links. If a user has read access, they'll only be able to use and view shared links, but can't create or delete a shared link.

To give someone permissions to create or delete a shared link, use the following steps:

1. In the Azure portal, go to the Bastion host.
2. Go to the **Access control (IAM)** page.
3. In the Microsoft.Network/bastionHosts section, configure the following permissions:

   - Other: Creates shareable urls for the VMs under a bastion and returns the URLs.
   - Other: Deletes shareable urls for the provided VMs under a bastion.
   - Other: Deletes shareable urls for the provided tokens under a bastion.

   These correspond to the following PowerShell cmdlets:

   - Microsoft.Network/bastionHosts/createShareableLinks/action
   - Microsoft.Network/bastionHosts/deleteShareableLinks/action
   - Microsoft.Network/bastionHosts/deleteShareableLinksByToken/action
   - Microsoft.Network/bastionHosts/getShareableLinks/action - If this isn't enabled, the user won't be able to see a shareable link.

Next steps

- For additional features, see Bastion features and configuration settings.
- For more information about Azure Bastion, see What is Azure Bastion?

Additional resources

Documentation

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

How to block network traffic with Azure Virtual Network Manager (Preview) - Azure portal

Learn how to block network traffic using security rules in Azure Virtual Network Manager with the Azure portal.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

Connect to a VM - specified private IP address: Azure portal - Azure Bastion

Learn how to connect to your virtual machines using a specified private IP address via Azure Bastion.

Configure Bastion for Kerberos authentication: Azure portal - Azure Bastion

Learn how to configure Bastion to use Kerberos authentication via the Azure portal.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Show 5 more

How to configure Bastion for Kerberos authentication using the Azure portal (Preview)

Article • 02/01/2023 • 6 minutes to read

This article shows you how to configure Azure Bastion to use Kerberos authentication. Kerberos authentication can be used with both the Basic and the Standard Bastion SKUs. For more information about Kerberos authentication, see the Kerberos authentication overview. For more information about Azure Bastion, see What is Azure Bastion?

Considerations

- During Preview, the Kerberos setting for Azure Bastion can be configured in the Azure portal only.
- VMs migrated from on-premises to Azure are not currently supported for Kerberos.
- Cross-realm authentication is not currently supported for Kerberos.
- Changes to DNS server are not currently supported for Kerberos. After making any changes to DNS server, you will need to delete and re-create the Bastion resource.

Prerequisites

- An Azure account with an active subscription. If you don't have one, create one for free. To be able to connect to a VM through your browser using Bastion, you must be able to sign in to the Azure portal.

- An Azure virtual network. For steps to create a VNet, see Quickstart: Create a virtual network.

Update VNet DNS servers

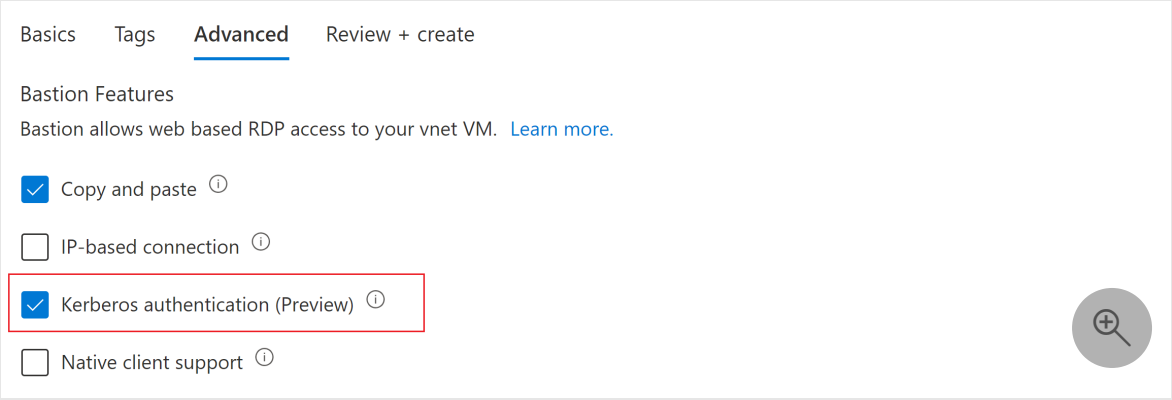
In this section, the following steps help you update your virtual network to specify custom DNS settings.

1. Sign in to the Azure portal.
2. Go to the virtual network for which you want to deploy the Bastion resources.
3. Go to the **DNS servers** page for your VNet and select **Custom**. Add the IP address of your Azure-hosted domain controller and **Save**.

Deploy Bastion

1. Begin configuring your bastion deployment using the steps in Tutorial: Deploy Bastion using manual configuration settings. Configure the settings on the **Basics** tab. Then, at the top of the page, click **Advanced** to go to the Advanced tab.

2. On the **Advanced** tab, select **Kerberos**.



3. At the bottom of the page, select **Review + create**, then **Create** to deploy Bastion to your virtual network.

4. Once the deployment completes, you can use it to sign in to any reachable Windows VMs joined to the custom DNS you specified in the earlier steps.

To modify an existing Bastion deployment

In this section, the following steps help you modify your virtual network and existing Bastion deployment for Kerberos authentication.

1. Update the DNS settings for your virtual network.
2. Go to the portal page for your Bastion deployment and select **Configuration**.
3. On the Configuration page, select **Kerberos authentication**, then select **Apply**.
4. Bastion will update with the new configuration settings.

To verify Bastion is using Kerberos

> **Note**
>
> You must use the User Principal Name (UPN) to sign in using Kerberos.

Once you have enabled Kerberos on your Bastion resource, you can verify that it's actually using Kerberos for authentication to the target domain-joined VM.

1. Sign into the target VM (either via Bastion or not). Search for "Edit Group Policy" from the taskbar and open the **Local Group Policy Editor**.
2. Select **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
3. Find the policy **Networking security: Restrict NTLM: Incoming NTLM Traffic** and set it to **Deny all domain accounts**. Because Bastion uses NTLM for authentication when Kerberos is disabled, this setting ensures that NTLM-based authentication is unsuccessful for future sign-in attempts on the VM.
4. End the VM session.
5. Connect to the target VM again using Bastion. Sign-in should succeed, indicating that Bastion used Kerberos (and not NTLM) for authentication.

Quickstart: Setup Bastion with Kerberos - Resource Manager template

Review the template

```
{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "location": {
      "defaultValue": "[resourceGroup().location]",
      "type": "string"
    },
    "defaultNsgName": {
      "type": "string",
      "defaultValue": "Default-nsg"
    },
    "VnetName": {
      "type": "string",
      "defaultValue": "myVnet"
    },
    "ClientVMName": {
      "defaultValue": "Client-vm",
      "type": "string"
    },
    "ServerVMName": {
      "defaultValue": "Server-vm",
      "type": "string"
    },
    "vmsize": {
      "defaultValue": "Standard_DS1_v2",
      "type": "string",
```

```
      "metadata": {
        "description": "VM SKU to deploy"
      }
    },
    "ServerVMUsername": {
      "type": "string",
      "defaultValue": "serveruser",
      "metadata": {
        "description": "Admin username on all VMs."
      }
    },
    "ServerVMPassword": {
      "type": "securestring",
      "metadata": {
        "description": "Admin password on all VMs."
      }
    },
    "SafeModeAdministratorPassword": {
      "type": "securestring",
      "metadata": {
        "description": "See https://learn.microsoft.com/en-
us/powershell/module/addsdeployment/install-addsdomaincontroller?
view=windowsserver2022-ps#-safemodeadministratorpassword"
      }
    },
    "ClientVMUsername": {
      "type": "string",
      "defaultValue": "clientuser",
      "metadata": {
        "description": "username on ClientVM."
      }
    },
    "ClientVMPassword": {
      "type": "securestring",
      "metadata": {
        "description": "password on ClientVM."
      }
    },
    "ServerVmImage": {
      "type": "object",
      "defaultValue": {
        "offer": "WindowsServer",
        "publisher": "MicrosoftWindowsServer",
        "sku": "2019-Datacenter",
        "version": "latest"
      }
    },
    "ClientVmImage": {
      "type": "object",
      "defaultValue": {
        "offer": "Windows",
        "publisher": "microsoftvisualstudio",
        "sku": "Windows-10-N-x64",
        "version": "latest"
      }
```

```
    },
    "publicIPAllocationMethod": {
      "type": "string",
      "defaultValue": "Static"
    },
    "BastionName": {
      "defaultValue": "Bastion",
      "type": "string"
    },
    "BastionPublicIPName": {
        "defaultValue": "Bastion-ip",
        "type": "string"
    }
  },
  "variables": {
    "DefaultSubnetId": "
[concat(resourceId('Microsoft.Network/virtualNetworks',
parameters('VnetName')), '/subnets/default')]",
    "ClientVMSubnetId": "
[concat(resourceId('Microsoft.Network/virtualNetworks',
parameters('VnetName')), '/subnets/clientvm-subnet')]",
    "DNSServerIpAddress": "10.16.0.4",
    "ClientVMPrivateIpAddress": "10.16.1.4"
  },
  "resources": [
    {
      "apiVersion": "2020-03-01",
      "name": "[parameters('VnetName')]",
      "type": "Microsoft.Network/virtualNetworks",
      "location": "[parameters('location')]",
      "properties": {
        "dhcpOptions": {
          "dnsServers": [ "[variables('DNSServerIpAddress')]" ]
        },
        "subnets": [
          {
            "name": "default",
            "properties": {
              "addressPrefix": "10.16.0.0/24"
            }
          },
          {
            "name": "clientvm-subnet",
            "properties": {
              "addressPrefix": "10.16.1.0/24"
            }
          },
          {
            "name": "AzureBastionSubnet",
            "properties": {
              "addressPrefix": "10.16.2.0/24"
            }
          }
        ],
        "addressSpace": {
```

```
          "addressPrefixes": [
            "10.16.0.0/16"
          ]
        }
      }
    },
    {
      "type": "Microsoft.Network/networkInterfaces",
      "apiVersion": "2018-10-01",
      "name": "[concat(parameters('ServerVMName'), 'Nic')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/',
parameters('VnetName'))]"
      ],
      "properties": {
        "ipConfigurations": [
          {
            "name": "[concat(parameters('ServerVMName'), 'NicIpConfig')]",
            "properties": {
              "privateIPAllocationMethod": "Static",
              "privateIPAddress": "[variables('DNSServerIpAddress')]",
              "subnet": {
                "id": "[variables('DefaultSubnetId')]"
              }
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Compute/virtualMachines",
      "apiVersion": "2020-06-01",
      "name": "[parameters('ServerVMName')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "[concat('Microsoft.Network/networkInterfaces/',
parameters('ServerVMName'), 'Nic')]"
      ],
      "properties": {
        "hardwareProfile": {
          "vmSize": "[parameters('vmSize')]"
        },
        "osProfile": {
          "AdminUsername": "[parameters('ServerVMUsername')]",
          "AdminPassword": "[parameters('ServerVMPassword')]",
          "computerName": "[parameters('ServerVMName')]"
        },
        "storageProfile": {
          "imageReference": "[parameters('ServerVmImage')]",
          "osDisk": {
            "createOption": "FromImage",
            "managedDisk": {
              "storageAccountType": "Standard_LRS"
            }
```

```
          }
        },
        "networkProfile": {
          "networkInterfaces": [
            {
              "id": "[ResourceId('Microsoft.Network/networkInterfaces/',
concat(parameters('ServerVMName'), 'Nic'))]"
            }
          ]
        }
      }
    },
    {
      "type": "Microsoft.Compute/virtualMachines/extensions",
      "apiVersion": "2021-04-01",
      "name": "[concat(parameters('ServerVMName'),'/',
'PromoteToDomainController')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "
[concat('Microsoft.Compute/virtualMachines/',parameters('ServerVMName'))]"
      ],
      "properties": {
        "publisher": "Microsoft.Compute",
        "type": "CustomScriptExtension",
        "typeHandlerVersion": "1.7",
        "autoUpgradeMinorVersion": true,
        "settings": {
          "commandToExecute": "[concat('powershell.exe -Command \"Install-
windowsfeature AD-domain-services; Import-Module
ADDSDeployment;$Secure_String_Pwd = ConvertTo-SecureString
',parameters('SafeModeAdministratorPassword'),' -AsPlainText -Force;
Install-ADDSForest -DomainName \"bastionkrb.test\" -
SafeModeAdministratorPassword $Secure_String_Pwd -Force:$true')]"
          }
      }
    },
    {
      "type": "Microsoft.Network/networkInterfaces",
      "apiVersion": "2018-10-01",
      "name": "[concat(parameters('ClientVMName'), 'Nic')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "[concat('Microsoft.Network/virtualNetworks/',
parameters('VnetName'))]",
        "[concat('Microsoft.Compute/virtualMachines/',
parameters('ServerVMName'))]"
      ],
      "properties": {
        "ipConfigurations": [
          {
            "name": "[concat(parameters('ClientVMName'), 'NicIpConfig')]",
            "properties": {
              "privateIPAllocationMethod": "Static",
              "privateIPAddress": "[variables('ClientVMPrivateIpAddress')]",
```

```
              "subnet": {
                "id": "[variables('ClientVMSubnetId')]"
              }
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Compute/virtualMachines",
      "apiVersion": "2020-06-01",
      "name": "[parameters('ClientVMName')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "[concat('Microsoft.Network/networkInterfaces/',
parameters('ClientVMName'), 'Nic')]"
      ],
      "properties": {
        "hardwareProfile": {
          "vmSize": "[parameters('vmSize')]"
        },
        "osProfile": {
          "AdminUsername": "[parameters('ClientVMUsername')]",
          "AdminPassword": "[parameters('ClientVMPassword')]",
          "computerName": "[parameters('ClientVMName')]"
        },
        "storageProfile": {
          "imageReference": "[parameters('ClientVmImage')]",
          "osDisk": {
            "createOption": "FromImage",
            "managedDisk": {
              "storageAccountType": "Standard_LRS"
            }
          }
        },
        "networkProfile": {
          "networkInterfaces": [
            {
              "id": "[ResourceId('Microsoft.Network/networkInterfaces/',
concat(parameters('ClientVMName'), 'Nic'))]"
            }
          ]
        }
      }
    },
    {
      "type": "Microsoft.Compute/virtualMachines/extensions",
      "apiVersion": "2021-04-01",
      "name": "[concat(parameters('ClientVMName'),'/', 'DomainJoin')]",
      "location": "[parameters('location')]",
      "dependsOn": [
        "
[concat('Microsoft.Compute/virtualMachines/',parameters('ClientVMName'))]",
        "[concat('Microsoft.Compute/virtualMachines/',
parameters('ServerVMName'),'/extensions/', 'PromoteToDomainController')]",
```

```
        "[concat('Microsoft.Network/bastionHosts/',
parameters('BastionName'))]"
      ],
      "properties": {
        "publisher": "Microsoft.Compute",
        "type": "CustomScriptExtension",
        "typeHandlerVersion": "1.7",
        "autoUpgradeMinorVersion": true,
        "settings": {
          "commandToExecute": "[concat('powershell.exe -Command Set-
ItemProperty -Path HKLM:\\SYSTEM\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\
-Name RestrictReceivingNTLMTraffic -Value 1; $Pass= ConvertTo-SecureString -
String ',parameters('ServerVMPassword'),' -AsPlainText -Force; $Credential =
New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList
\"AD\\serveruser\", $Pass; do { try { $joined = add-computer -computername
Client-vm -domainname bastionkrb.test –credential $Credential -passthru -
restart –force; } catch {}} while ($joined.HasSucceeded -ne $true)')]"
          }
      }
    },
    {
      "apiVersion": "2020-11-01",
      "type": "Microsoft.Network/publicIPAddresses",
      "name": "[parameters('BastionPublicIPName')]",
      "location": "[resourceGroup().location]",
      "sku": {
        "name": "Standard"
      },
      "properties": {
        "publicIPAllocationMethod": "Static"
      },
      "tags": {}
    },
    {
        "type": "Microsoft.Network/bastionHosts",
        "apiVersion": "2020-11-01",
        "name": "[parameters('BastionName')]",
        "location": "[resourceGroup().location]",
        "dependsOn": [
            "[concat('Microsoft.Network/virtualNetworks/',
parameters('VnetName'))]",
            "[concat('Microsoft.Network/publicIpAddresses/',
parameters('BastionPublicIPName'))]"
        ],
        "sku": {
            "name": "Standard"
        },
        "properties": {
            "enableKerberos": "true",
            "ipConfigurations": [
                {
                    "name": "IpConf",
                    "properties": {
                        "privateIPAllocationMethod": "Dynamic",
                        "publicIPAddress": {
```

```
                                "id": "
[resourceId('Microsoft.Network/publicIpAddresses',
parameters('BastionPublicIPName'))]"
                            },
                            "subnet": {
                                "id": "
[concat(resourceId('Microsoft.Network/virtualNetworks',
parameters('VnetName')), '/subnets/AzureBastionSubnet')]"
                            }
                        }
                    }
                ]
            }
        }
    ]
}
```

The following resources have been defined in the template:

- Deploys the following Azure resources:
  - Microsoft.Network/virtualNetworks: create an Azure virtual network.
  - Microsoft.Network/bastionHosts: create a Standard SKU Bastion with a public IP and Kerberos feature enabled
  - Create a Windows 10 ClientVM and a Windows Server 2019 ServerVM
- Have the DNS Server of the VNET point to the private IP address of the ServerVM (domain controller).
- Runs a Custom Script Extension on the ServerVM to promote it to a domain controller with domain name: `bastionkrb.test`.
- Runs a Custom Script Extension on the ClientVM to have it:
  - **Restrict NTLM: Incoming NTLM traffic** = Deny all domain accounts (this is to ensure Kerberos is used for authentication).
  - Domain-join the `bastionkrb.test` domain.

Deploy the template

To setup Kerberos, deploy the ARM template above by running the following PS cmd:

```
New-AzResourceGroupDeployment -ResourceGroupName <your-rg-name> -
TemplateFile "<path-to-template>\KerberosDeployment.json"`
```

Review deployed resources

Now, login to ClientVM using Bastion with Kerberos authentication:

- credentials: username = `serveruser@bastionkrb.test` and password = `<password-entered-during-deployment>`.

Next steps

For more information about Azure Bastion, see What is Azure Bastion?

Additional resources

Documentation

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

Create a shareable link for Azure Bastion

Learn how to create a shareable link to let a user connect to a target resource via Bastion without using the Azure portal.

Troubleshoot Azure Bastion

Learn how to troubleshoot Azure Bastion.

Connect to a VM - specified private IP address: Azure portal - Azure Bastion

Learn how to connect to your virtual machines using a specified private IP address via Azure Bastion.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

Connect to a VM using a native client and Azure Bastion - Azure Bastion

Learn how to connect to a VM from a Windows computer by using Bastion and a native client.

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Show 5 more

Training

Learning paths and modules

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Create an RDP connection to a Windows VM using Azure Bastion

Article • 10/18/2022 • 2 minutes to read

This article shows you how to securely and seamlessly create an RDP connection to your Windows VMs located in an Azure virtual network directly through the Azure portal. When you use Azure Bastion, your VMs don't require a client, agent, or additional software. You can also connect to a Windows VM using SSH. For information, see Create an SSH connection to a Windows VM.

Azure Bastion provides secure connectivity to all of the VMs in the virtual network in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. For more information, see What is Azure Bastion?

Prerequisites

Before you begin, verify that you've met the following criteria:

- A VNet with the Bastion host already installed.
  - Make sure that you have set up an Azure Bastion host for the virtual network in which the VM is located. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in the virtual network.
  - To set up an Azure Bastion host, see Create a bastion host. If you plan to configure custom port values, be sure to select the Standard SKU when configuring Bastion.
- A Windows virtual machine in the virtual network.

Required roles

- Reader role on the virtual machine.
- Reader role on the NIC with private IP of the virtual machine.
- Reader role on the Azure Bastion resource.
- Reader role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network).

Ports

To connect to the Windows VM, you must have the following ports open on your Windows VM:

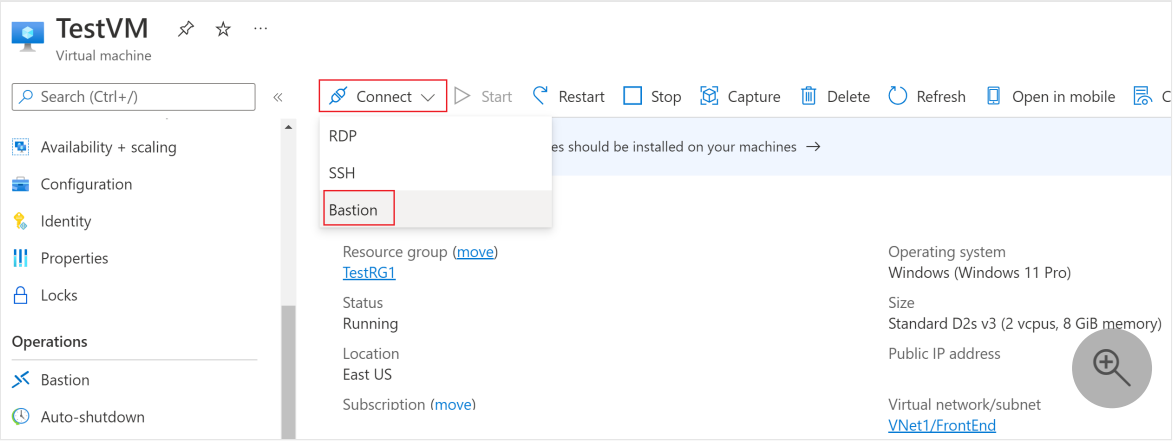
- Inbound port: RDP (3389) ***or***
- Inbound port: Custom value (you'll then need to specify this custom port when you connect to the VM via Azure Bastion)

> **Note**
>
> If you want to specify a custom port value, Azure Bastion must be configured using the Standard SKU. The Basic SKU does not allow you to specify custom ports.

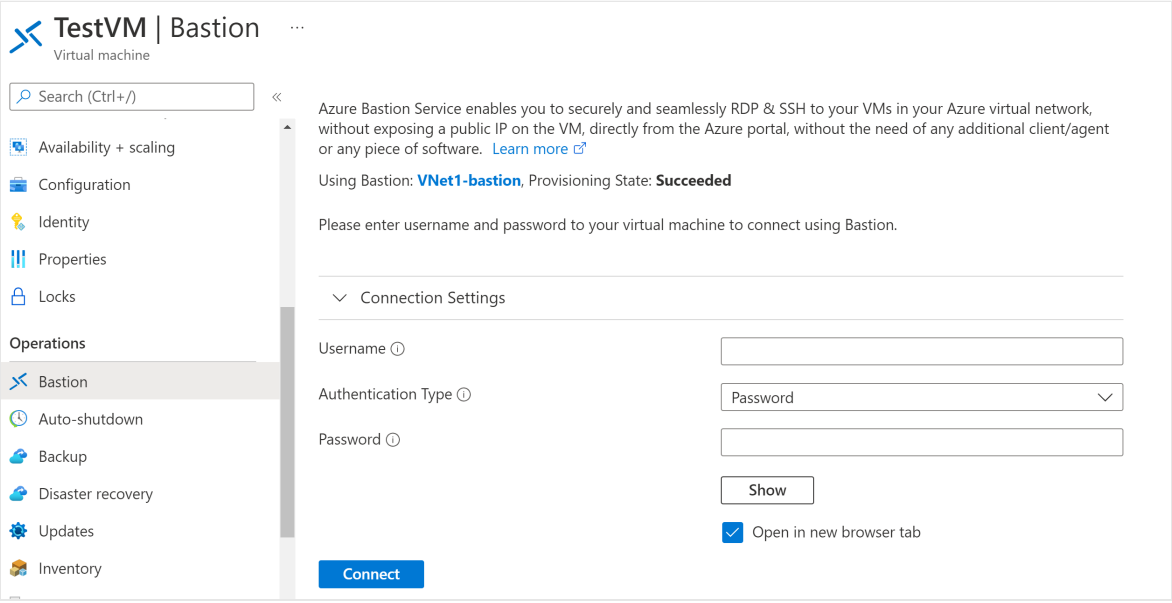
See the Azure Bastion FAQ for additional requirements.

Connect

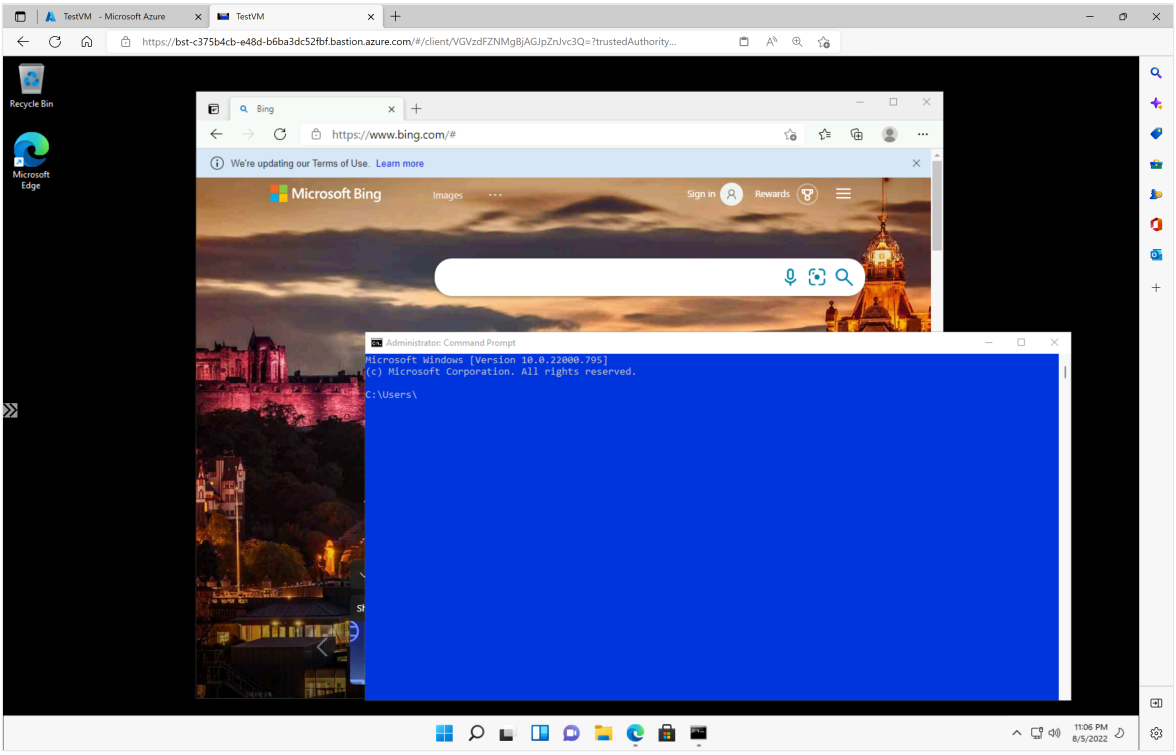
1. In the Azure portal, go to the virtual machine that you want to connect to. On the **Overview** page, select **Connect**, then select **Bastion** from the dropdown to open the Bastion page. You can also select **Bastion** from the left pane.



2. On the **Bastion** page, enter the required authentication credentials, then click **Connect**. If you configured your bastion host using the Standard SKU, you'll see additional credential options on this page. If your VM is domain-joined, you must use the following format: **username@domain.com**.



3. When you click **Connect**,the RDP connection to this virtual machine via Bastion will open in your browser (over HTML5) using port 443 and the Bastion service. The following example shows a connection to a Windows 11 virtual machine in a new browser tab. The page you see depends on the VM you're connecting to.



When working with the VM, using keyboard shortcut keys may not result in the same behavior as shortcut keys on a local computer. For example, when connected to a Windows VM from a Windows client, CTRL+ALT+END is the keyboard shortcut for CTRL+ALT+Delete on a local computer. To do this from a Mac while connected to a Windows VM, the keyboard shortcut is Fn+CTRL+ALT+Backspace.

Next steps

Read the Bastion FAQ for additional connection information.

Create an SSH connection to a Windows VM using Azure Bastion

Article • 10/19/2022 • 6 minutes to read

This article shows you how to securely and seamlessly create an SSH connection to your Windows VMs located in an Azure virtual network directly through the Azure portal. When you use Azure Bastion, your VMs don't require a client, agent, or additional software. You can also connect to a Windows VM using RDP. For information, see Create an RDP connection to a Windows VM.

Azure Bastion provides secure connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. For more information, see the What is Azure Bastion?.

> **Note**
>
> If you want to create an SSH connection to a Windows VM, Azure Bastion must be configured using the Standard SKU.

When connecting to a Windows virtual machine using SSH, you can use both username/password and SSH keys for authentication.

The SSH private key must be in a format that begins with `"-----BEGIN RSA PRIVATE KEY-----"` and ends with `"-----END RSA PRIVATE KEY-----"`.

Prerequisites

Make sure that you have set up an Azure Bastion host for the virtual network in which the VM resides. For more information, see Create an Azure Bastion host. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in this virtual network.

To SSH to a Windows virtual machine, you must also ensure that:

- Your Windows virtual machine is running Windows Server 2019 or later.
- You have OpenSSH Server installed and running on your Windows virtual machine. To learn how to do this, see Install OpenSSH.
- Azure Bastion has been configured to use the Standard SKU.

Required roles

In order to make a connection, the following roles are required:

- Reader role on the virtual machine
- Reader role on the NIC with private IP of the virtual machine
- Reader role on the Azure Bastion resource
- Reader role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network).

Ports

In order to connect to the Windows VM via SSH, you must have the following ports open on your VM:

- Inbound port: SSH (22) *or*
- Inbound port: Custom value (you will then need to specify this custom port when you connect to the VM via Azure Bastion)

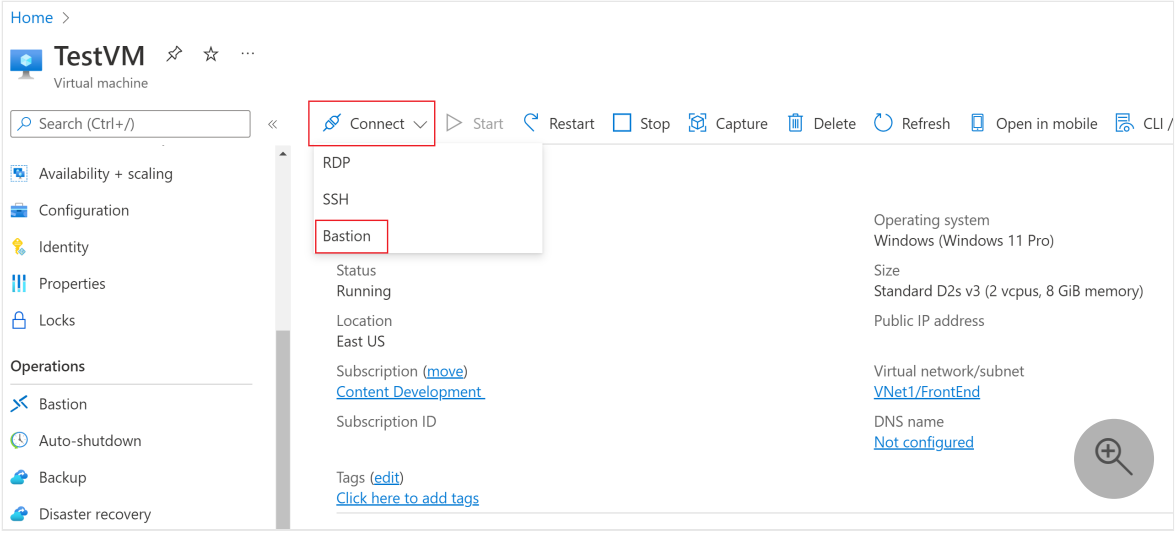
See the Azure Bastion FAQ for additional requirements.

Supported configurations

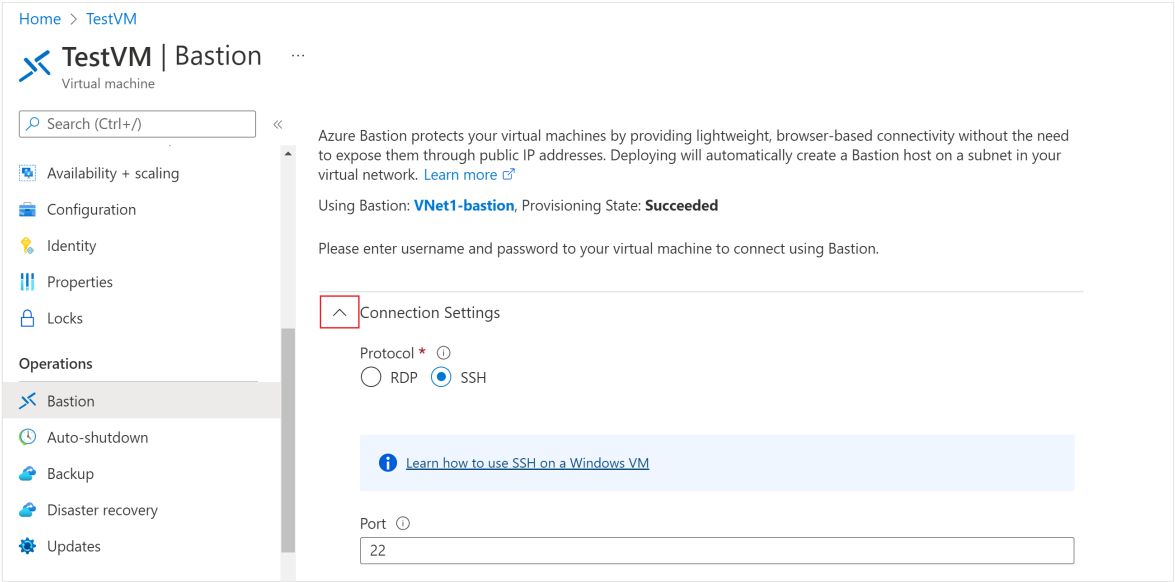
Currently, Azure Bastion only supports connecting to Windows VMs via SSH using **OpenSSH**.

Bastion connection page

1. In the Azure portal, go to the virtual machine that you want to connect to. On the **Overview** page, select **Connect**, then select **Bastion** from the dropdown to open the Bastion connection page. You can also select **Bastion** from the left pane.



2. On the **Bastion** connection page, click the **Connection Settings** arrow to expand all the available settings. If you are using a Bastion **Standard** SKU, you have more available settings than a Basic SKU.

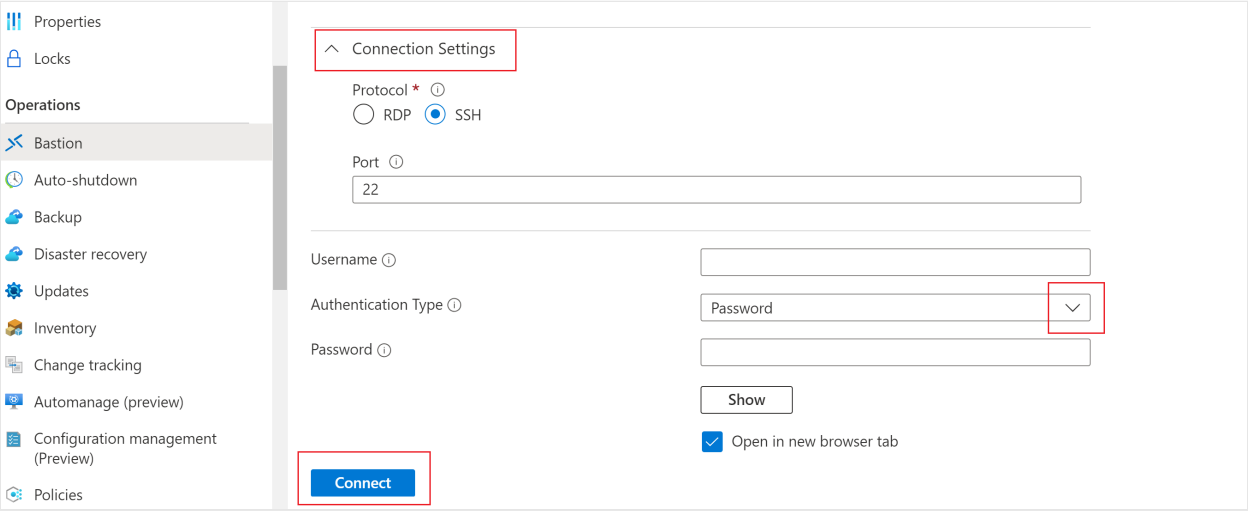


3. Authenticate and connect using one of the methods in the following sections.

- Username and password
- Private key from local file
- Password - Azure Key Vault
- Private key - Azure Key Vault

Username and password

Use the following steps to authenticate using username and password.



1. To authenticate using a username and password, configure the following settings:

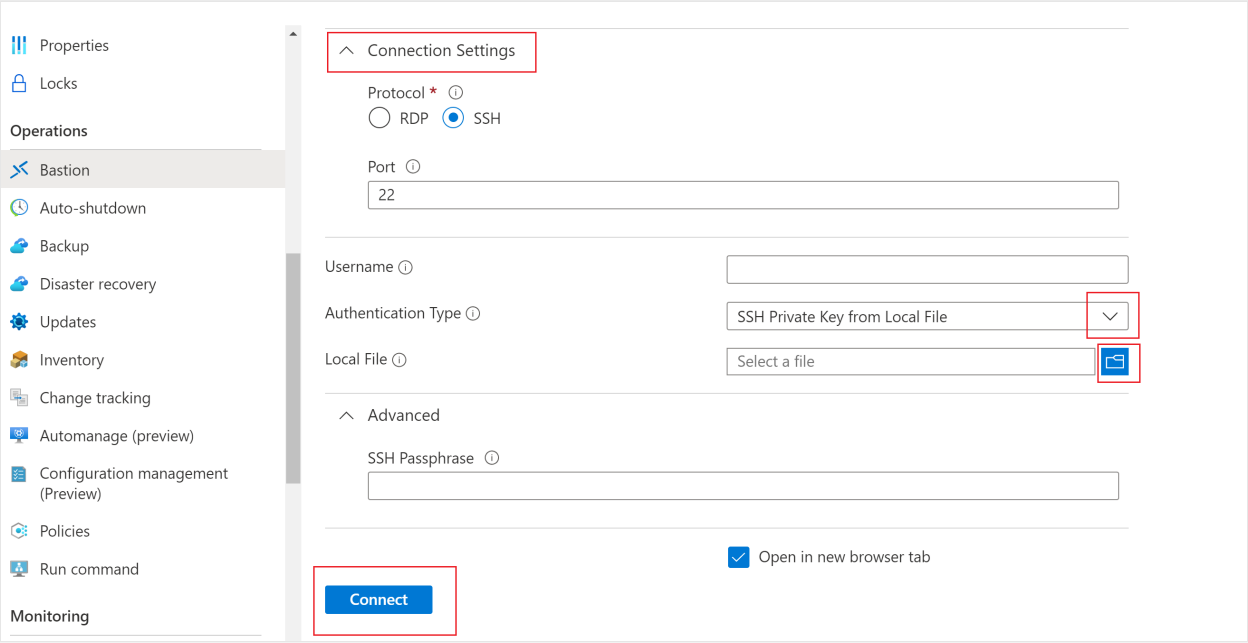
    - **Protocol**: Select SSH.
    - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
    - **Authentication type**: Select **Password** from the dropdown.
    - **Username**: Enter the username.
    - **Password**: Enter the **Password**.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Private key from local file

Use the following steps to authenticate using an SSH private key from a local file.



1. To authenticate using a private key from a local file, configure the following settings:

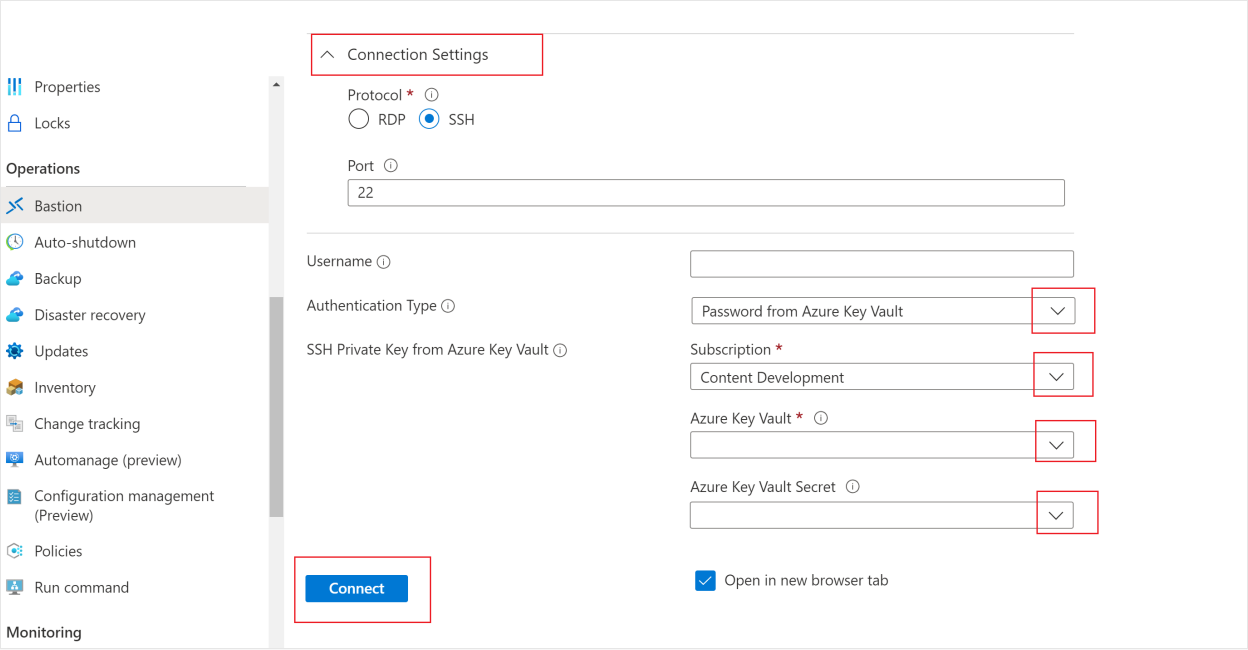
    - **Protocol**: Select SSH.
    - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
    - **Authentication type**: Select **SSH Private Key from Local File** from the dropdown.
    - **Local File**: Select the local file.
    - **SSH Passphrase**: Enter the SSH passphrase if necessary.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Password - Azure Key Vault

Use the following steps to authenticate using a password from Azure Key Vault.



1. To authenticate using a password from Azure Key Vault, configure the following settings:

    - **Protocol**: Select SSH.

    - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.

    - **Authentication type**: Select **Password from Azure Key Vault** from the dropdown.

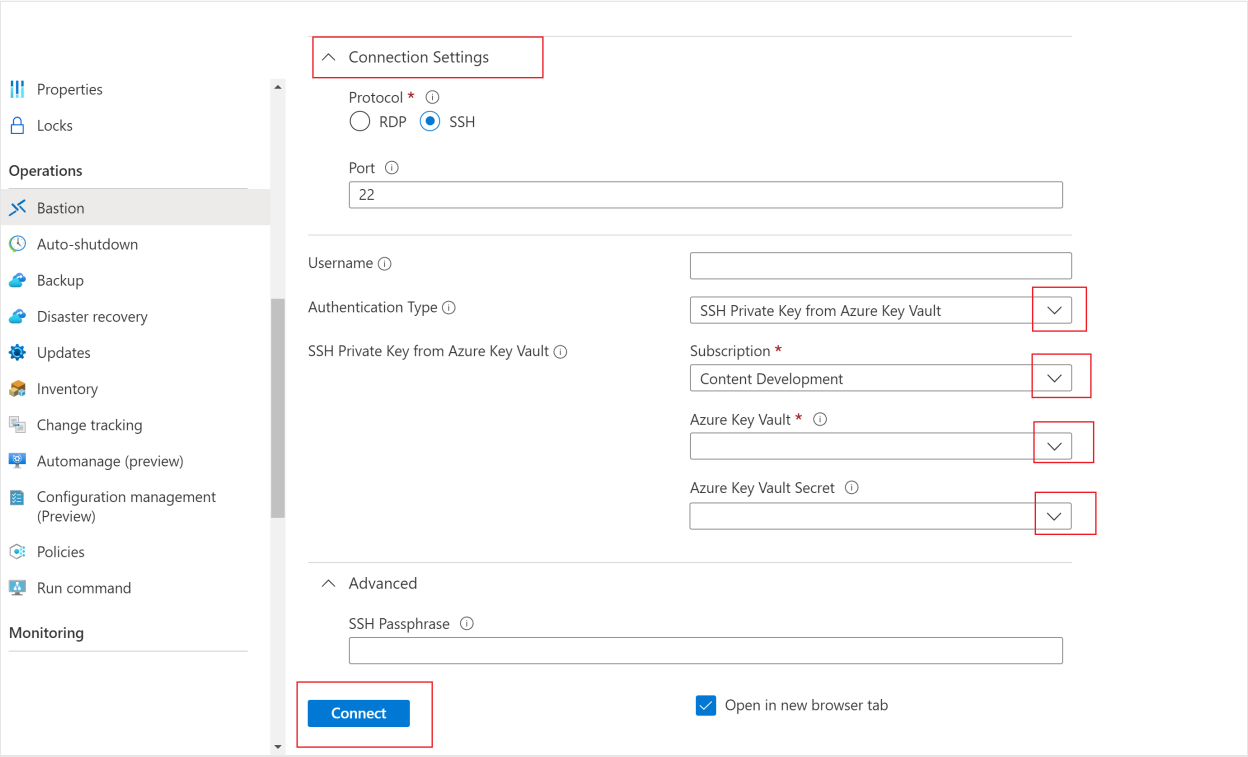
- **Username**: Enter the username.
- **Subscription**: Select the subscription.
- **Azure Key Vault**: Select the Key Vault.
- **Azure Key Vault Secret**: Select the Key Vault secret containing the value of your SSH private key.
  - If you didn't set up an Azure Key Vault resource, see Create a key vault and store your SSH private key as the value of a new Key Vault secret.
  - Make sure you have **List** and **Get** access to the secrets stored in the Key Vault resource. To assign and modify access policies for your Key Vault resource, see Assign a Key Vault access policy.

    > **Note**
    >
    > Please store your SSH private key as a secret in Azure Key Vault using the **PowerShell** or **Azure CLI** experience. Storing your private key via the Azure Key Vault portal experience will interfere with the formatting and result in unsuccessful login. If you did store your private key as a secret using the portal experience and no longer have access to the original private key file, see **Update SSH key** to update access to your target VM with a new SSH key pair.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.
3. Click **Connect** to connect to the VM.

Private key - Azure Key Vault

Use the following steps to authenticate using a private key stored in Azure Key Vault.



1. To authenticate using a private key stored in Azure Key Vault, configure the following settings:

    - **Protocol**: Select SSH.
    - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
    - **Authentication type**: Select **SSH Private Key from Azure Key Vault** from the dropdown.
    - **Username**: Enter the username.
    - **Subscription**: Select the subscription.
    - **Azure Key Vault**: Select the Key Vault.
        - If you didn't set up an Azure Key Vault resource, see Create a key vault and store your SSH private key as the value of a new Key Vault secret.
        - Make sure you have **List** and **Get** access to the secrets stored in the Key Vault resource. To assign and modify access policies for your Key Vault resource, see Assign a Key Vault access policy.

    > **Note**
    >
    > Please store your SSH private key as a secret in Azure Key Vault using the **PowerShell** or **Azure CLI** experience. Storing your private key via

> the Azure Key Vault portal experience will interfere with the formatting and result in unsuccessful login. If you did store your private key as a secret using the portal experience and no longer have access to the original private key file, see **Update SSH key** to update access to your target VM with a new SSH key pair.

- **Azure Key Vault Secret**: Select the Key Vault secret containing the value of your SSH private key.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Next steps

For more information about Azure Bastion, see the Bastion FAQ.

Create an RDP connection to a Linux VM using Azure Bastion

Article • 10/19/2022 • 2 minutes to read

This article shows you how to securely and seamlessly create an RDP connection to your Linux VMs located in an Azure virtual network directly through the Azure portal. When you use Azure Bastion, your VMs don't require a client, agent, or additional software. You can also connect to a Linux VM using SSH.

Azure Bastion provides secure connectivity to all of the VMs in the virtual network in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. For more information, see What is Azure Bastion?

Prerequisites

Before you begin, verify that you've met the following criteria:

- Make sure that you have set up an Azure Bastion host for the virtual network in which the VM resides. For more information, see Create an Azure Bastion host. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in this virtual network.
- To use RDP with a Linux virtual machine, you must also ensure that you have xrdp installed and configured on the Linux VM. To learn how to do this, see Use xrdp with Linux.
- Bastion must be configured with the Standard SKU.
- You must use username/password authentication.

Required roles

In order to make a connection, the following roles are required:

- Reader role on the virtual machine
- Reader role on the NIC with private IP of the virtual machine
- Reader role on the Azure Bastion resource
- Reader role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network).

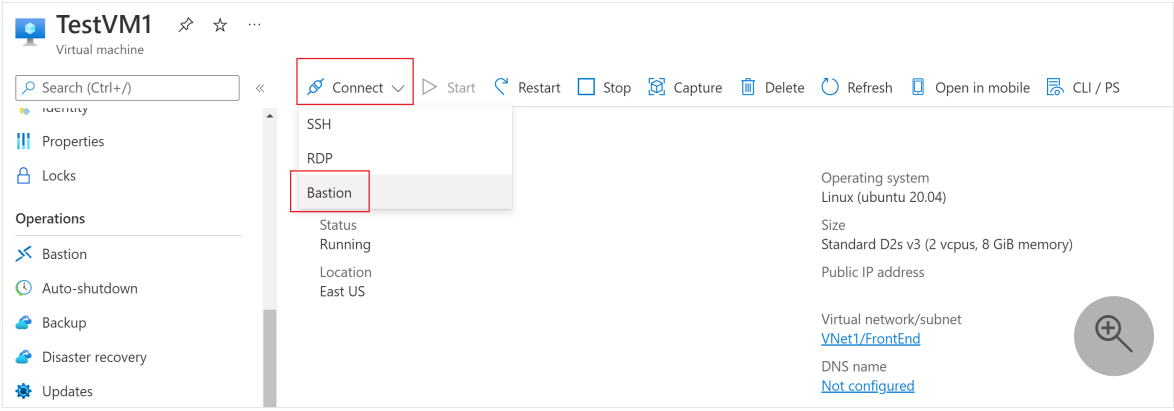
Ports

To connect to the Linux VM via RDP, you must have the following ports open on your VM:

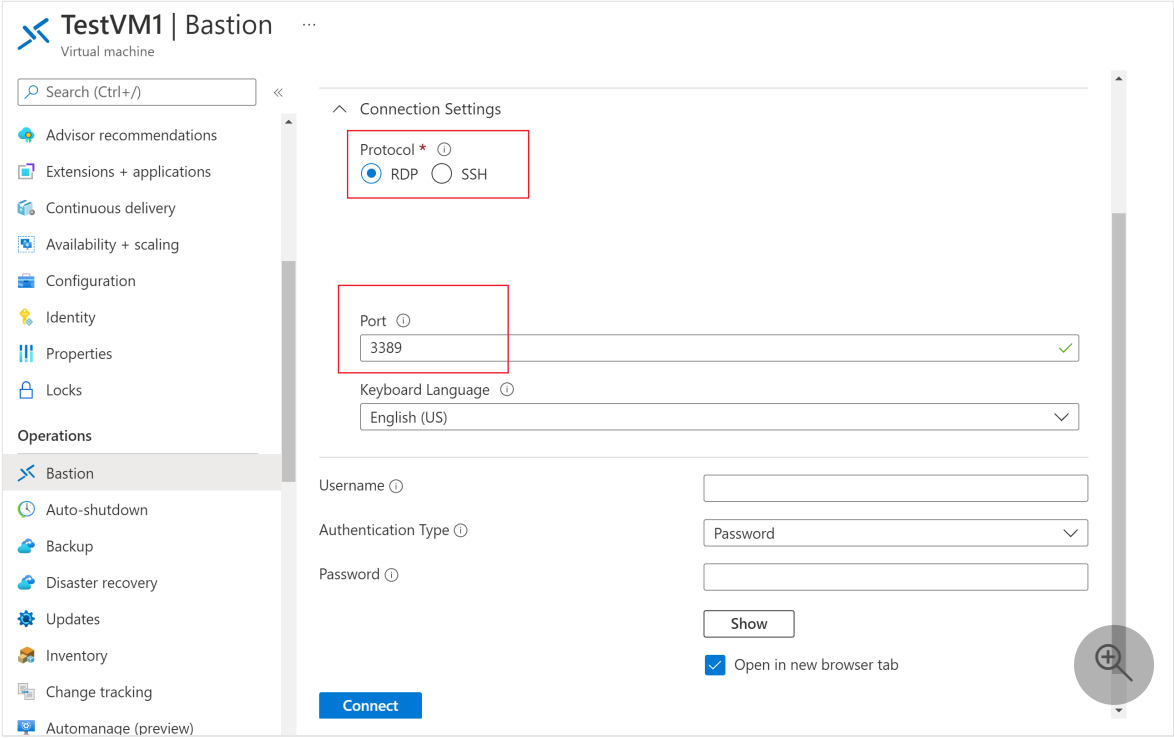
- Inbound port: RDP (3389) *or*
- Inbound port: Custom value (you'll then need to specify this custom port when you connect to the VM via Azure Bastion)

Connect

1. In the Azure portal, go to the virtual machine that you want to connect to. On the **Overview** page, select **Connect**, then select **Bastion** from the dropdown to open the Bastion page. You can also select **Bastion** from the left pane.



2. On the **Bastion** page, expand the **Connection Settings** section and select **RDP**. If you plan to use an inbound port different from the standard RDP port (3389), enter the **Port**.



3. Enter the **Username** and **Password**, and then select **Connect** to connect to the VM. The RDP connection to this virtual machine via Bastion will open directly in the browser (over HTML5) using port 443 and the Bastion service.

Next steps

Read the Bastion FAQ for more information.

Create an SSH connection to a Linux VM using Azure Bastion

Article • 10/21/2022 • 5 minutes to read

This article shows you how to securely and seamlessly create an SSH connection to your Linux VMs located in an Azure virtual network directly through the Azure portal. When you use Azure Bastion, your VMs don't require a client, agent, or additional software. You can also connect to a Linux VM using RDP. For information, see Create an RDP connection to a Linux VM.

Azure Bastion provides secure connectivity to all of the VMs in the virtual network in which it's provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH. For more information, see the What is Azure Bastion? overview article.

When connecting to a Linux virtual machine using SSH, you can use both username/password and SSH keys for authentication.

The SSH private key must be in a format that begins with `"-----BEGIN RSA PRIVATE KEY-----"` and ends with `"-----END RSA PRIVATE KEY-----"`.

Prerequisites

Make sure that you have set up an Azure Bastion host for the virtual network in which the VM resides. For more information, see Create an Azure Bastion host. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM in this virtual network.

Required roles

In order to make a connection, the following roles are required:

- Reader role on the virtual machine
- Reader role on the NIC with private IP of the virtual machine
- Reader role on the Azure Bastion resource
- Reader role on the virtual network of the target virtual machine (if the Bastion deployment is in a peered virtual network)

Ports

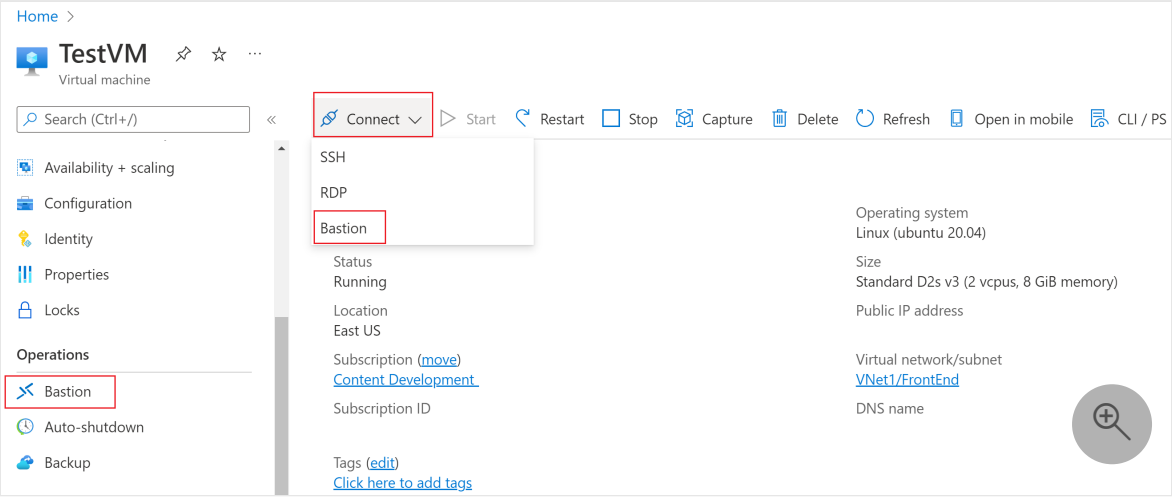
In order to connect to the Linux VM via SSH, you must have the following ports open on your VM:

- Inbound port: SSH (22) ***or***
- Inbound port: Custom value (you'll then need to specify this custom port when you connect to the VM via Azure Bastion)

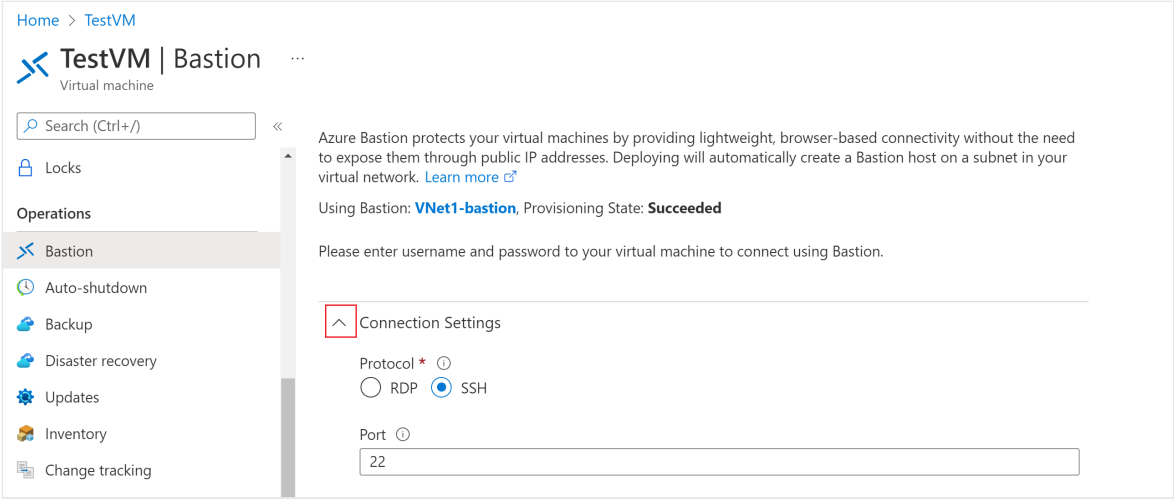
> **Note**
>
> If you want to specify a custom port value, Azure Bastion must be configured using the Standard SKU. The Basic SKU does not allow you to specify custom ports.

Bastion connection page

1. In the Azure portal, go to the virtual machine that you want to connect to. On the **Overview** page, select **Connect**, then select **Bastion** from the dropdown to open the Bastion connection page. You can also select **Bastion** from the left pane.



2. On the **Bastion** connection page, click the **Connection Settings** arrow to expand all the available settings. If you are using a Bastion **Standard** SKU, you have more available settings than a Basic SKU.

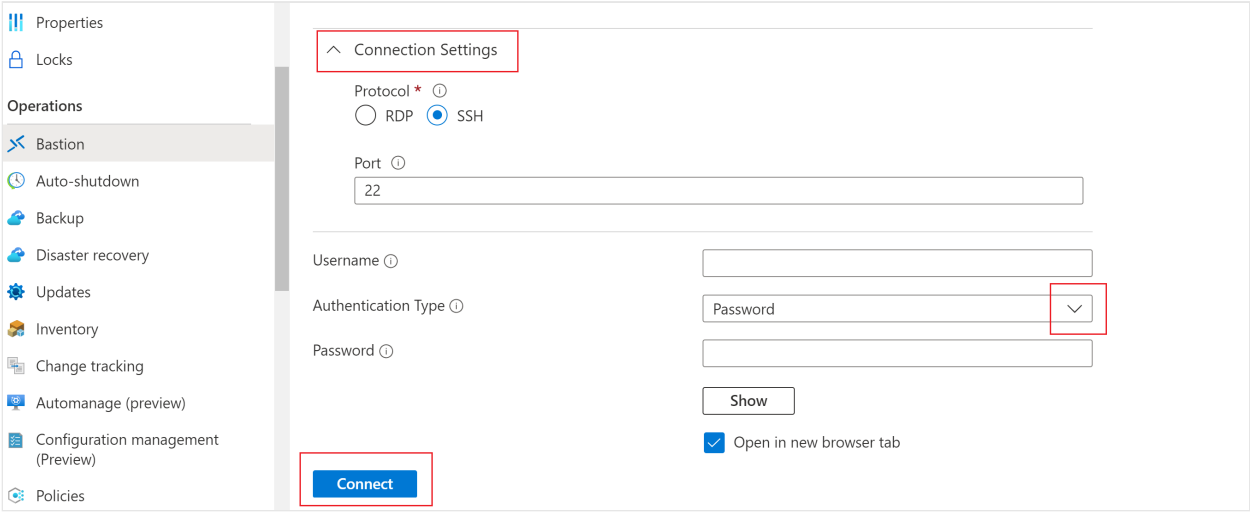


3. Authenticate and connect using one of the methods in the following sections.

- Username and password
- Private key from local file
- Password - Azure Key Vault
- Private key - Azure Key Vault

Username and password

Use the following steps to authenticate using username and password.



1. To authenticate using a username and password, configure the following settings:

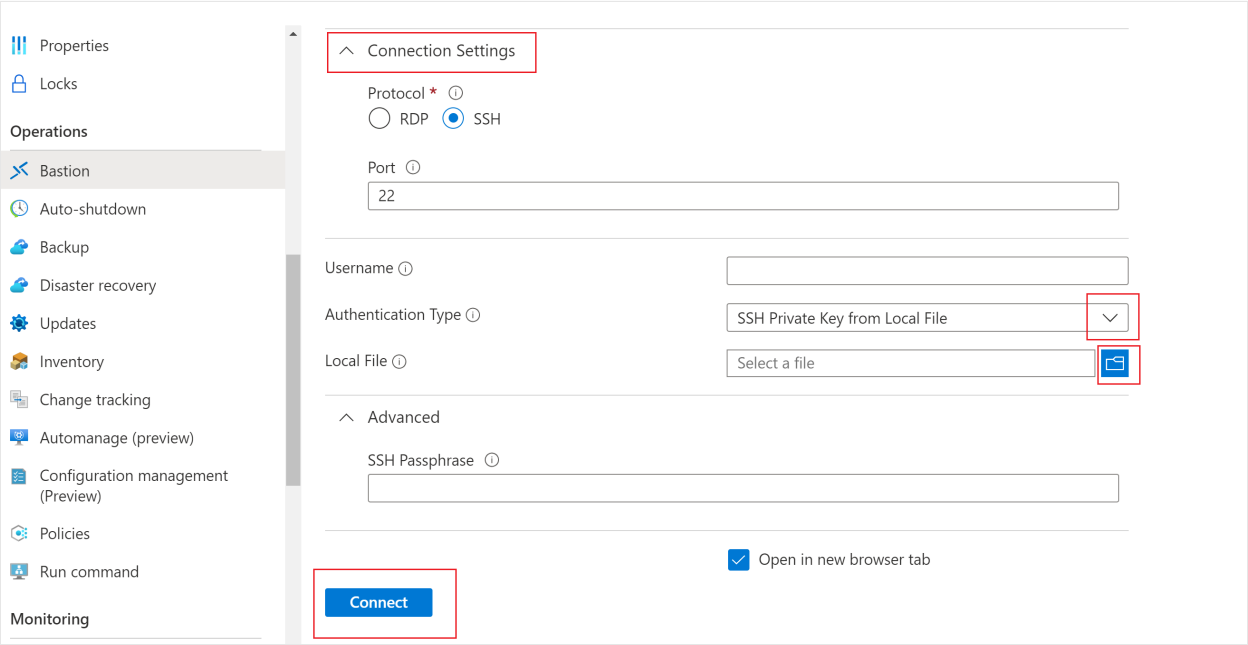
- **Protocol**: Select SSH.
- **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
- **Authentication type**: Select **Password** from the dropdown.
- **Username**: Enter the username.
- **Password**: Enter the **Password**.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Private key from local file

Use the following steps to authenticate using an SSH private key from a local file.



1. To authenticate using a private key from a local file, configure the following settings:

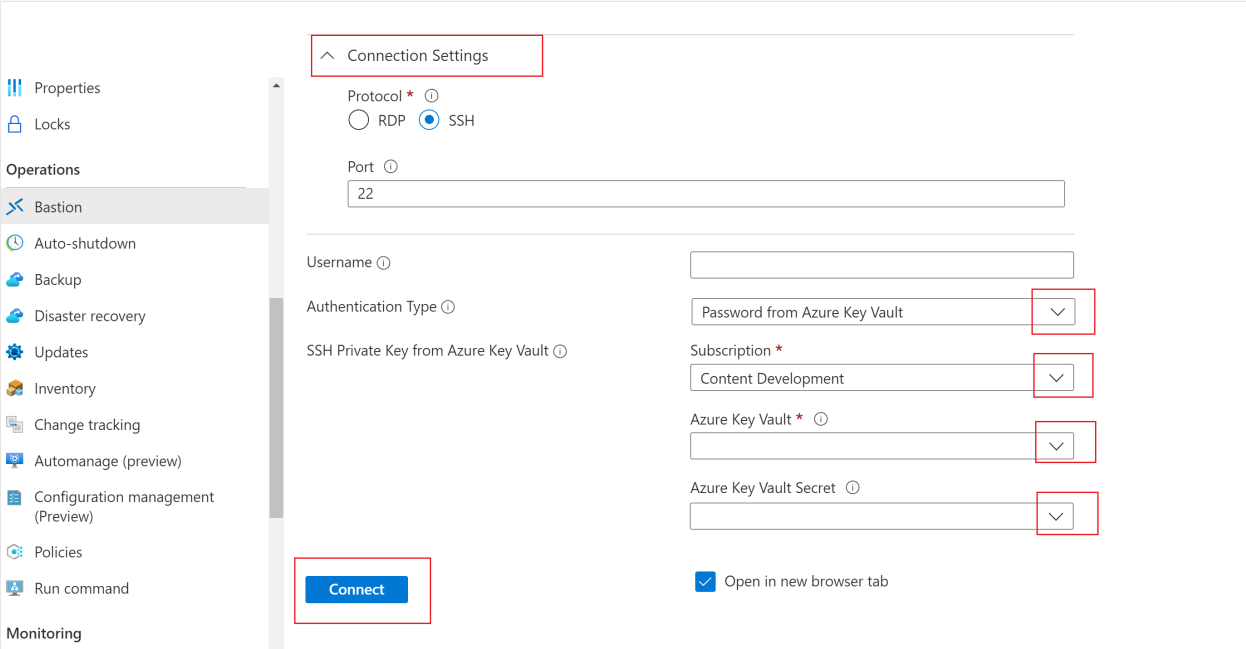
   - **Protocol**: Select SSH.
   - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
   - **Authentication type**: Select **SSH Private Key from Local File** from the dropdown.
   - **Local File**: Select the local file.
   - **SSH Passphrase**: Enter the SSH passphrase if necessary.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Password - Azure Key Vault

Use the following steps to authenticate using a password from Azure Key Vault.



1. To authenticate using a password from Azure Key Vault, configure the following settings:

   - **Protocol**: Select SSH.
   - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.
   - **Authentication type**: Select **Password from Azure Key Vault** from the dropdown.
   - **Username**: Enter the username.
   - **Subscription**: Select the subscription.
   - **Azure Key Vault**: Select the Key Vault.
   - **Azure Key Vault Secret**: Select the Key Vault secret containing the value of your SSH private key.
     - If you didn't set up an Azure Key Vault resource, see Create a key vault and store your SSH private key as the value of a new Key Vault secret.
     - Make sure you have **List** and **Get** access to the secrets stored in the Key Vault resource. To assign and modify access policies for your Key Vault resource, see Assign a Key Vault access policy.

> **Note**

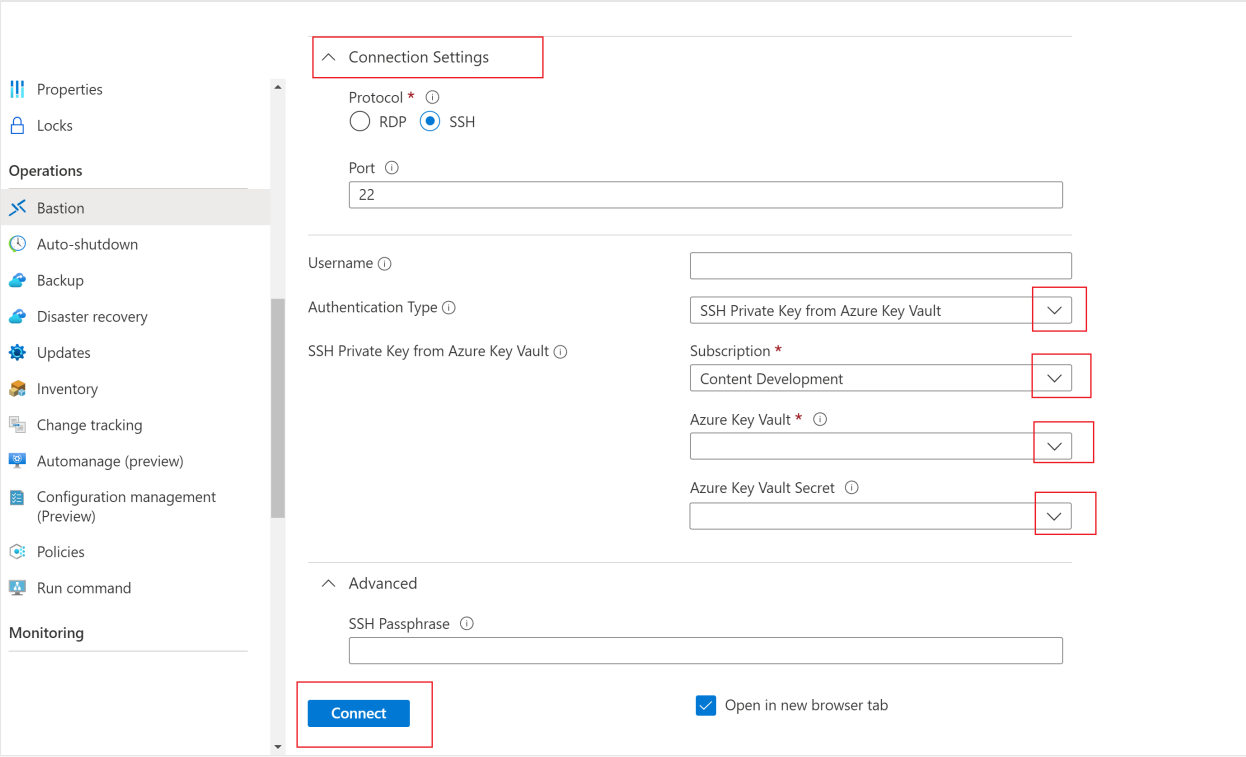
> Please store your SSH private key as a secret in Azure Key Vault using the **PowerShell** or **Azure CLI** experience. Storing your private key via the Azure Key Vault portal experience will interfere with the formatting and result in unsuccessful login. If you did store your private key as a secret using the portal experience and no longer have access to the original private key file, see **Update SSH key** to update access to your target VM with a new SSH key pair.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.

3. Click **Connect** to connect to the VM.

Private key - Azure Key Vault

Use the following steps to authenticate using a private key stored in Azure Key Vault.



1. To authenticate using a private key stored in Azure Key Vault, configure the following settings:

   - **Protocol**: Select SSH.

   - **Port**: Input the port number. Custom port connections are available for the Standard SKU only.

   - **Authentication type**: Select **SSH Private Key from Azure Key Vault** from the dropdown.

- **Username**: Enter the username.
- **Subscription**: Select the subscription.
- **Azure Key Vault**: Select the Key Vault.
  - If you didn't set up an Azure Key Vault resource, see Create a key vault and store your SSH private key as the value of a new Key Vault secret.
  - Make sure you have **List** and **Get** access to the secrets stored in the Key Vault resource. To assign and modify access policies for your Key Vault resource, see Assign a Key Vault access policy.

    > **Note**
    >
    > Please store your SSH private key as a secret in Azure Key Vault using the **PowerShell** or **Azure CLI** experience. Storing your private key via the Azure Key Vault portal experience will interfere with the formatting and result in unsuccessful login. If you did store your private key as a secret using the portal experience and no longer have access to the original private key file, see **Update SSH key** to update access to your target VM with a new SSH key pair.

- **Azure Key Vault Secret**: Select the Key Vault secret containing the value of your SSH private key.

2. To work with the VM in a new browser tab, select **Open in new browser tab**.
3. Click **Connect** to connect to the VM.

Next steps

For more information about Azure Bastion, see the Bastion FAQ.

Connect to a VM using a native client

Article • 03/09/2023 • 8 minutes to read

This article helps you configure your Bastion deployment, and then connect to a VM in the VNet using the native client (SSH or RDP) on your local computer. The native client feature lets you connect to your target VMs via Bastion using Azure CLI, and expands your sign-in options to include local SSH key pair and Azure Active Directory (Azure AD). Additionally with this feature, you can now also upload or download files, depending on the connection type and client.

Your capabilities on the VM when connecting via native client are dependent on what is enabled on the native client. Controlling access to features such as file transfer via Bastion isn't supported.

> **Note**
>
> This configuration requires the Standard SKU tier for Azure Bastion.

After you deploy this feature, there are two different sets of connection instructions.

- Connect to a VM from the native client on a Windows local computer. This lets you do the following:
  - Connect using SSH or RDP.
  - Upload and download files over RDP.
  - If you want to connect using SSH and need to upload files to your target VM, use the **az network bastion tunnel** command instead.
- Connect to a VM using the **az network bastion tunnel** command. This lets you do the following:
  - Use native clients on *non*-Windows local computers (example: a Linux PC).
  - Use the native client of your choice. (This includes the Windows native client.)
  - Connect using SSH or RDP. (Note that bastion tunnel does not relay web servers or hosts.)
  - Set up concurrent VM sessions with Bastion.
  - Upload files to your target VM from your local computer. File download from the target VM to the local client is currently not supported for this command.

Limitations

- Signing in using an SSH private key stored in Azure Key Vault isn't supported with this feature. Before signing in to your Linux VM using an SSH key pair, download

your private key to a file on your local machine.
- This feature isn't supported on Cloud Shell.

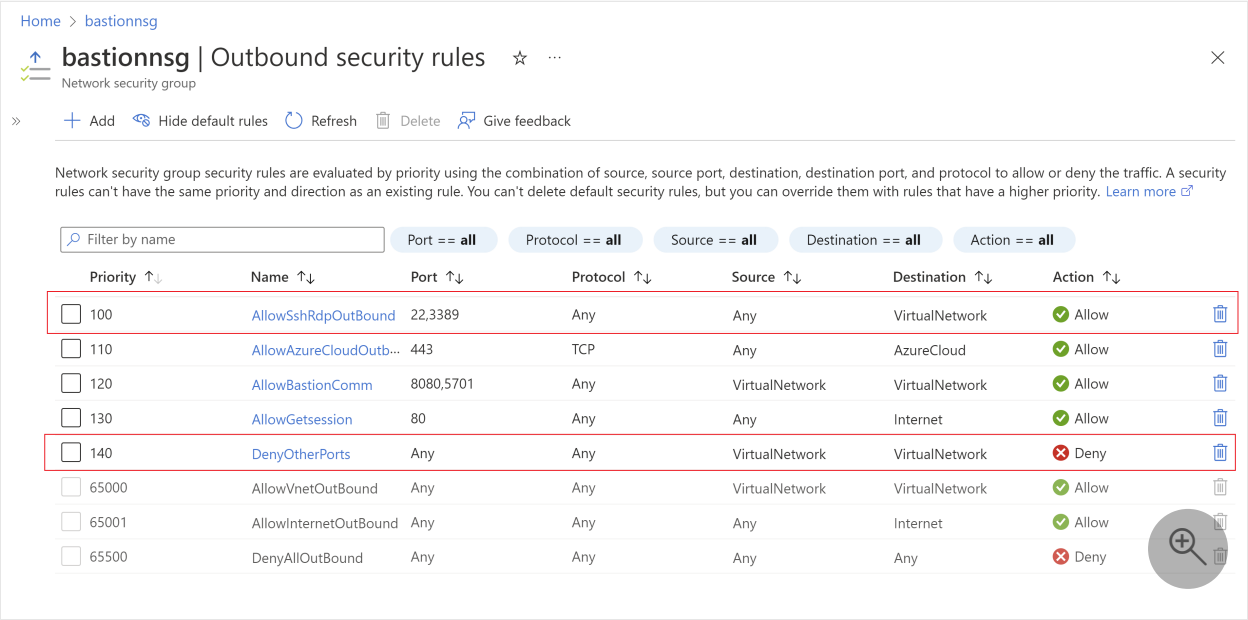
Prerequisites

Before you begin, verify that you have the following prerequisites:

- The latest version of the CLI commands (version 2.32 or later) is installed. For information about installing the CLI commands, see Install the Azure CLI and Get Started with Azure CLI.
- An Azure virtual network.
- A virtual machine in the virtual network.
- The VM's Resource ID. The Resource ID can be easily located in the Azure portal. Go to the Overview page for your VM and select the *JSON View* link to open the Resource JSON. Copy the Resource ID at the top of the page to your clipboard to use later when connecting to your VM.
- If you plan to sign in to your virtual machine using your Azure AD credentials, make sure your virtual machine is set up using one of the following methods:
  - Enable Azure AD sign-in for a Windows VM or Linux VM.
  - Configure your Windows VM to be Azure AD-joined.
  - Configure your Windows VM to be hybrid Azure AD-joined.

Secure your native client connection

If you want to further secure your native client connection, you can limit port access by only providing access to port 22/3389. To restrict port access, you must deploy the following NSG rules on your AzureBastionSubnet to allow access to select ports and deny access from any other ports.



Configure the native client support feature

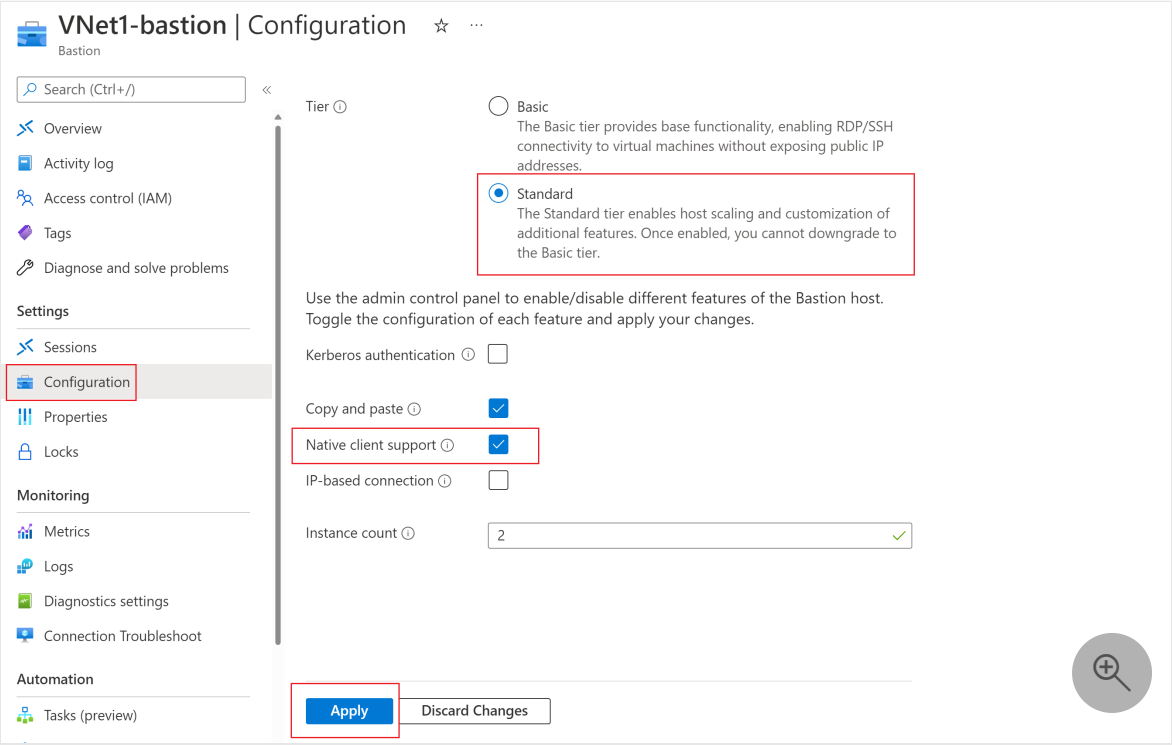
You can configure this feature by either modifying an existing Bastion deployment, or you can deploy Bastion with the feature configuration already specified.

To modify an existing Bastion deployment

If you've already deployed Bastion to your VNet, modify the following configuration settings:

1. Navigate to the **Configuration** page for your Bastion resource. Verify that the SKU Tier is **Standard**. If it isn't, select **Standard**.

2. Select the box for **Native Client Support**, then apply your changes.

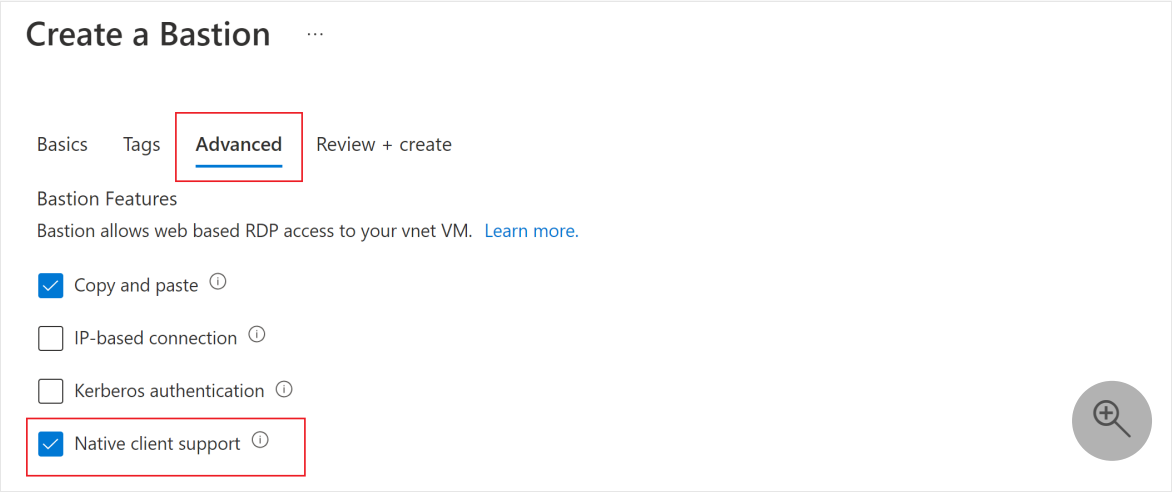


To deploy Bastion with the native client feature

If you haven't already deployed Bastion to your VNet, you can deploy with the native client feature specified by deploying Bastion using manual settings. For steps, see Tutorial - Deploy Bastion with manual settings. When you deploy Bastion, specify the following settings:

1. On the **Basics** tab, for **Instance Details -> Tier** select **Standard**. Native client support requires the Standard SKU.

2. Before you create the bastion host, go to the **Advanced** tab and check the box for **Native Client Support**, along with the checkboxes for any other additional features that you want to deploy.



3. Click **Review + create** to validate, then click **Create** to deploy your Bastion host.

Verify roles and ports

Verify that the following roles and ports are configured in order to connect to the VM.

Required roles

- Reader role on the virtual machine.
- Reader role on the NIC with private IP of the virtual machine.
- Reader role on the Azure Bastion resource.
- Virtual Machine Administrator Login or Virtual Machine User Login role, if you're using the Azure AD sign-in method. You only need to do this if you're enabling Azure AD login using the processes outlined in one of these articles:
  - Azure Windows VMs and Azure AD
  - Azure Linux VMs and Azure AD

Ports

To connect to a Linux VM using native client support, you must have the following ports open on your Linux VM:

- Inbound port: SSH (22) *or*
- Inbound port: Custom value (you'll then need to specify this custom port when you connect to the VM via Azure Bastion)

To connect to a Windows VM using native client support, you must have the following ports open on your Windows VM:

- Inbound port: RDP (3389) *or*
- Inbound port: Custom value (you'll then need to specify this custom port when you connect to the VM via Azure Bastion)

To learn about how to best configure NSGs with Azure Bastion, see Working with NSG access and Azure Bastion.

Connect to VM - Windows native client

This section helps you connect to your virtual machine from the native client on a local Windows computer. If you want to upload and download files after connecting, you must use an RDP connection. For more information about file transfers, see Upload or download files.

Use the example that corresponds to the type of target VM to which you want to connect.

- Windows VM
- Linux VM

Connect to a Windows VM

1. Sign in to your Azure account. If you have more than one subscription, select the subscription containing your Bastion resource.

   Azure CLI

   ```
   az login
   az account list
   az account set --subscription "<subscription ID>"
   ```

2. Sign in to your target Windows VM using one of the following example options. If you want to specify a custom port value, you should also include the field **--resource-port** in the sign-in command.

   RDP:

   To connect via RDP, use the following command. You'll then be prompted to input your credentials. You can use either a local username and password, or your Azure AD credentials. For more information, see Azure Windows VMs and Azure AD.

   Azure CLI

```
az network bastion rdp --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId>"
```

> ⓘ **Important**
>
> Remote connection to VMs that are joined to Azure AD is allowed only from Windows 10 or later PCs that are Azure AD registered (starting with Windows 10 20H1), Azure AD joined, or hybrid Azure AD joined to the *same* directory as the VM.

SSH:

The extension can be installed by running, `az extension add --name ssh`. To sign in using an SSH key pair, use the following example.

Azure CLI

```
az network bastion ssh --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId>" --auth-type "ssh-
key" --username "<Username>" --ssh-key "<Filepath>"
```

1. Once you sign in to your target VM, the native client on your computer will open up with your VM session; **MSTSC** for RDP sessions, and **SSH CLI extension (az ssh)** for SSH sessions.

Connect to a Linux VM

1. Sign in to your Azure account. If you have more than one subscription, select the subscription containing your Bastion resource.

   Azure CLI

   ```
   az login
   az account list
   az account set --subscription "<subscription ID>"
   ```

2. Sign in to your target Linux VM using one of the following example options. If you want to specify a custom port value, you should also include the field **--resource-port** in the sign-in command.

   Azure AD:

If you're signing in to an Azure AD login-enabled VM, use the following command. For more information, see Azure Linux VMs and Azure AD.

Azure CLI

```
az network bastion ssh --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId or
VMSSInstanceResourceId>" --auth-type  "AAD"
```

SSH:

The extension can be installed by running, `az extension add --name ssh`. To sign in using an SSH key pair, use the following example.

Azure CLI

```
az network bastion ssh --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId or
VMSSInstanceResourceId>" --auth-type "ssh-key" --username "<Username>"
--ssh-key "<Filepath>"
```

Username/password:

If you're signing in using a local username and password, use the following command. You'll then be prompted for the password for the target VM.

Azure CLI

```
az network bastion ssh --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId or
VMSSInstanceResourceId>" --auth-type "password" --username "<Username>"
```

3. Once you sign in to your target VM, the native client on your computer will open up with your VM session; **MSTSC** for RDP sessions, and **SSH CLI extension (az ssh)** for SSH sessions.

Connect to VM - other native clients

This section helps you connect to your virtual machine from native clients on *non-*Windows local computers (example: a Linux PC) using the **az network bastion tunnel** command. You can also connect using this method from a Windows computer. This is helpful when you require an SSH connection and want to upload files to your VM. Note that bastion tunnel supports RDP/SSH connection but does not relay web servers or hosts.

This connection supports file upload from the local computer to the target VM. For more information, see Upload files.

1. Sign in to your Azure account. If you have more than one subscription, select the subscription containing your Bastion resource.

   Azure CLI

   ```
   az login
   az account list
   az account set --subscription "<subscription ID>"
   ```

2. Open the tunnel to your target VM using the following command.

   Azure CLI

   ```
   az network bastion tunnel --name "<BastionName>" --resource-group "
   <ResourceGroupName>" --target-resource-id "<VMResourceId or
   VMSSInstanceResourceId>" --resource-port "<TargetVMPort>" --port "
   <LocalMachinePort>"
   ```

3. Connect to your target VM using SSH or RDP, the native client of your choice, and the local machine port you specified in Step 2.

   For example, you can use the following command if you have the OpenSSH client installed on your local computer:

   Azure CLI

   ```
   ssh <username>@127.0.0.1 -p <LocalMachinePort>
   ```

Next steps

Upload or download files

Additional resources

🕮 Documentation

Troubleshoot Azure Bastion

Learn how to troubleshoot Azure Bastion.

Connect to a VM - specified private IP address: Azure portal - Azure Bastion

Learn how to connect to your virtual machines using a specified private IP address via Azure Bastion.

Connect to a Windows VM using RDP - Azure Bastion

Learn how to use Azure Bastion to connect to Windows VM using RDP.

What is IP address 168.63.129.16?

Learn about IP address 168.63.129.16, specifically that it's used to facilitate a communication channel to Azure platform resources.

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Create a shareable link for Azure Bastion

Learn how to create a shareable link to let a user connect to a target resource via Bastion without using the Azure portal.

Upload or download files using a native client connection - Azure Bastion

Learn how to upload or download files using Azure Bastion and a native client when connected to a VM using Azure Bastion.

Tutorial: Deploy Bastion using specified settings: Azure portal

Learn how to deploy Bastion using settings that you specify - Azure portal.

Show 5 more

Training

Module

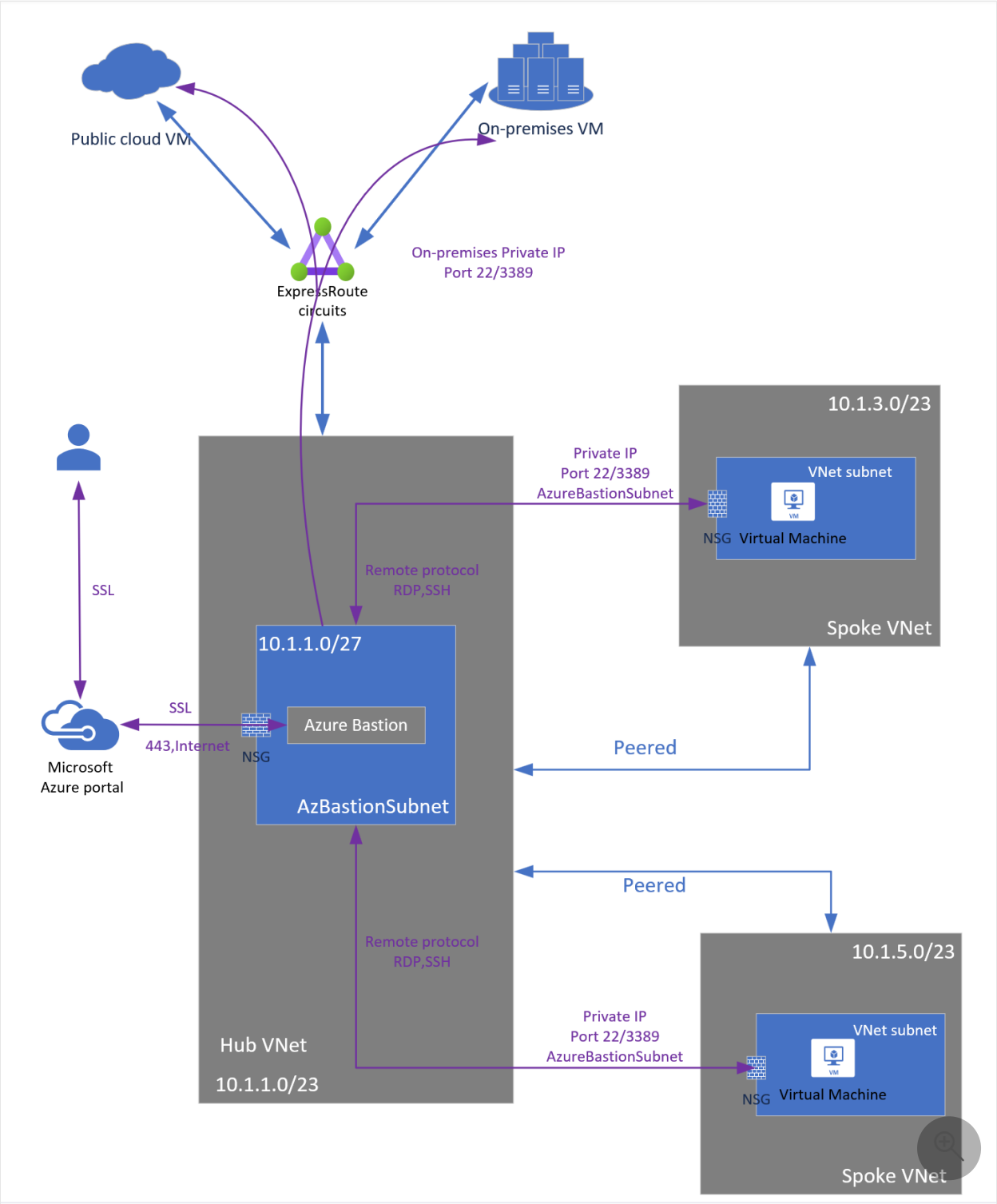
Introduction to Azure Bastion - Training

Describe how Azure Bastion provides secure and seamless connectivity to your VMs directly in the Azure portal. Determine whether Azure Bastion can replace your administrative jump boxes.

Connect to a VM via specified private IP address through the portal

Article • 02/08/2023 • 2 minutes to read

IP-based connection lets you connect to your on-premises, non-Azure, and Azure virtual machines via Azure Bastion over ExpressRoute or a VPN site-to-site connection using a specified private IP address. The steps in this article show you how to configure your Bastion deployment, and then connect to an on-premises resource using IP-based connection. For more information about Azure Bastion, see the Overview.



> **Note**
>
> This configuration requires the Standard SKU tier for Azure Bastion. To upgrade, see Upgrade a SKU.

Limitations

IP-based connection won't work with force tunneling over VPN, or when a default route is advertised over an ExpressRoute circuit. Azure Bastion requires access to the Internet and force tunneling, or the default route advertisement will result in traffic blackholing.

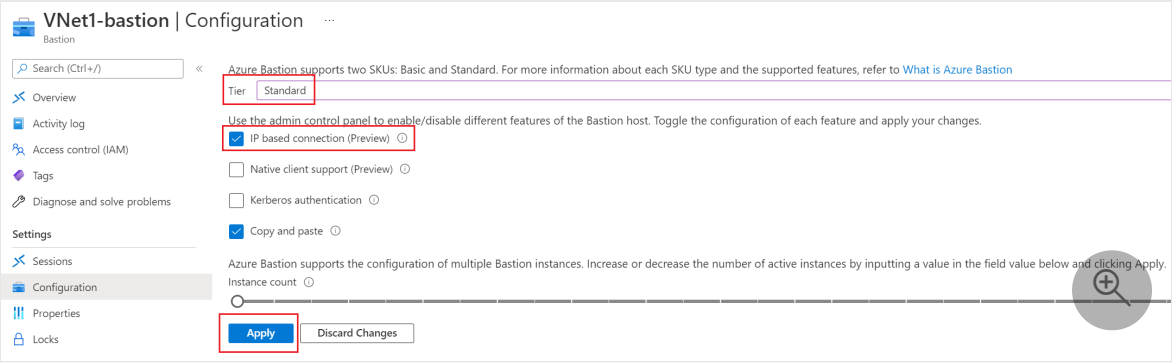
Prerequisites

Before you begin these steps, verify that you have the following environment set up:

- A VNet with Bastion already deployed.
  - Make sure that you have deployed Bastion to the virtual network. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to any VM deployed in any of the virtual networks that is reachable from Bastion.
  - To deploy Bastion, see Quickstart: Deploy Bastion with default settings.
- A virtual machine in any reachable virtual network. This is the virtual machine to which you'll connect.

Configure Bastion

1. Sign in to the Azure portal.
2. In the Azure portal, go to your Bastion deployment.
3. IP based connection requires the Standard SKU tier. On the **Configuration** page, for **Tier**, verify the tier is set to the **Standard** SKU. If the tier is set to the Basic SKU, select **Standard** from the dropdown.
4. To enable **IP based connection**, select **IP based connection**.

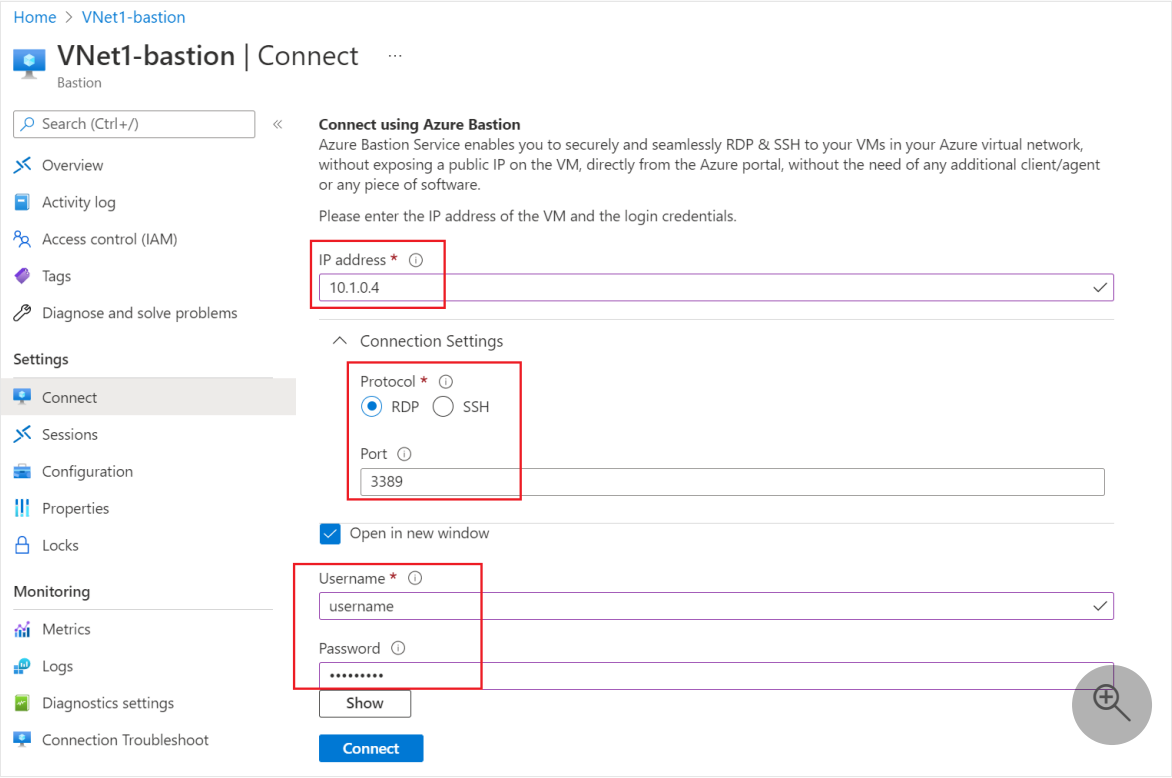


5. Select **Apply** to apply the changes. It takes a few minutes for the Bastion configuration to complete.

Connect to VM

1. To connect to a VM using a specified private IP address, you make the connection from Bastion to the VM, not directly from the VM page. On your Bastion page, select **Connect** to open the Connect page.

2. On the Bastion **Connect** page, for **IP address**, enter the private IP address of the target VM.



3. Adjust your connection settings to the desired **Protocol** and **Port**.

4. Enter your credentials in **Username** and **Password**.

5. Select **Connect** to connect to your virtual machine.

Next steps

Read the Bastion FAQ for additional information.

Additional resources

Documentation

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

Connect to a VM using a native client and Azure Bastion - Azure Bastion

Learn how to connect to a VM from a Windows computer by using Bastion and a native client.

About VM connections and features - Azure Bastion

Learn about VM connections and features when connecting using Azure Bastion.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Configure Bastion for Kerberos authentication: Azure portal - Azure Bastion

Learn how to configure Bastion to use Kerberos authentication via the Azure portal.

Connect to a Windows VM using RDP - Azure Bastion

Learn how to use Azure Bastion to connect to Windows VM using RDP.

Configure IP addresses for an Azure network interface

Learn how to add, change, and remove private and public IP addresses for a network interface.

Show 5 more

Training

Learning paths and modules

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

Connect to a virtual machine scale set using Azure Bastion

Article • 05/24/2022 • 2 minutes to read

This article shows you how to securely and seamlessly connect to your virtual machine scale set instance in an Azure virtual network directly from the Azure portal using Azure Bastion. When you use Azure Bastion, VMs don't require a client, agent, or additional software. For more information about Azure Bastion, see the Overview. For more information about virtual machine scale sets, see What are virtual machine scale sets?

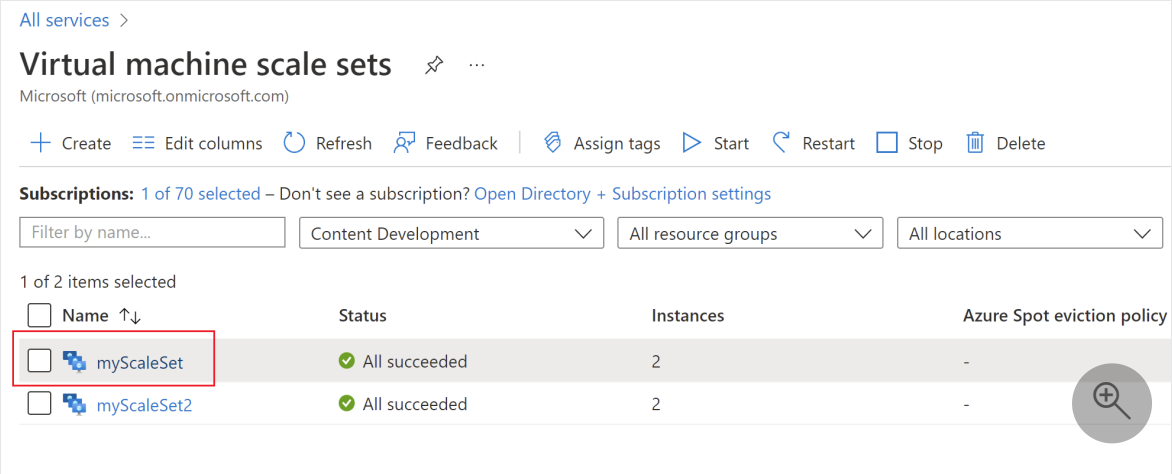
Prerequisites

Make sure that you have set up an Azure Bastion host for the virtual network in which the virtual machine scale set resides. For more information, see Create an Azure Bastion host. Once the Bastion service is provisioned and deployed in your virtual network, you can use it to connect to a virtual machine scale set instance in this virtual network.

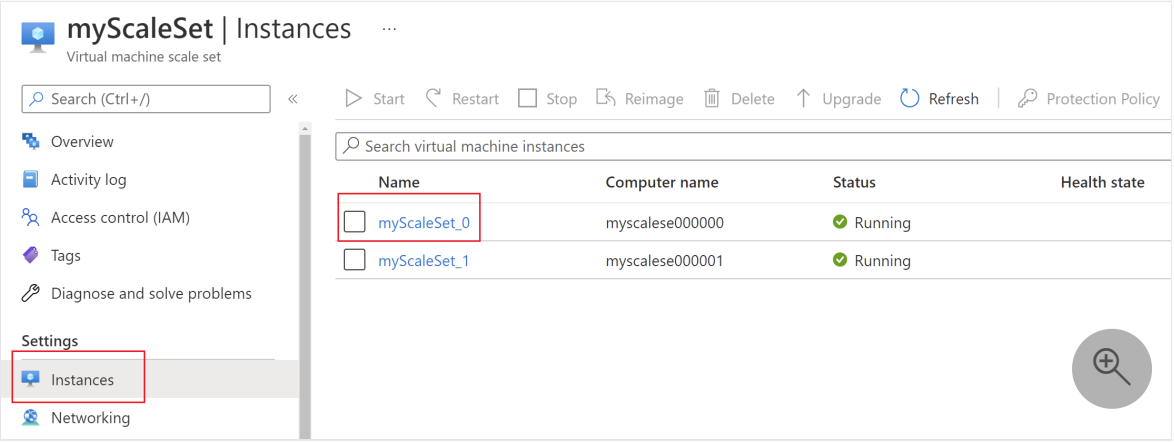
Connect

This section shows you the basic steps to connect to your virtual machine scale set.

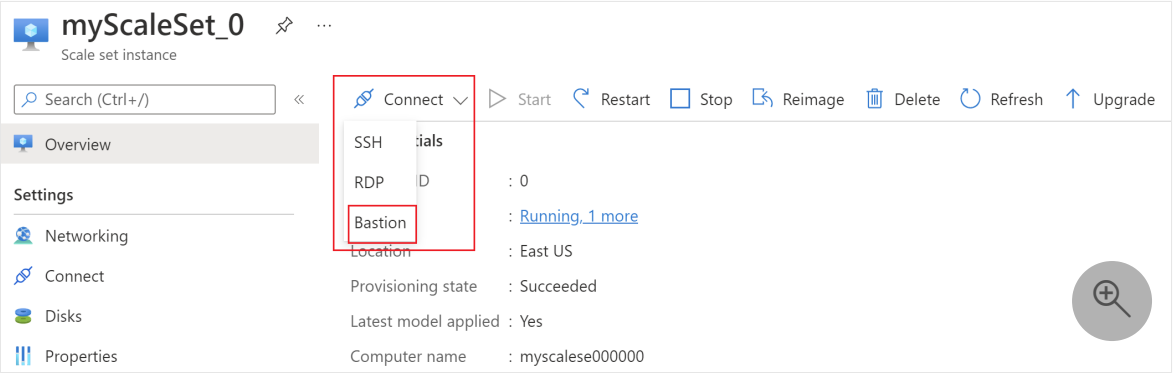
1. Open the Azure portal. Go to the virtual machine scale set that you want to connect to.



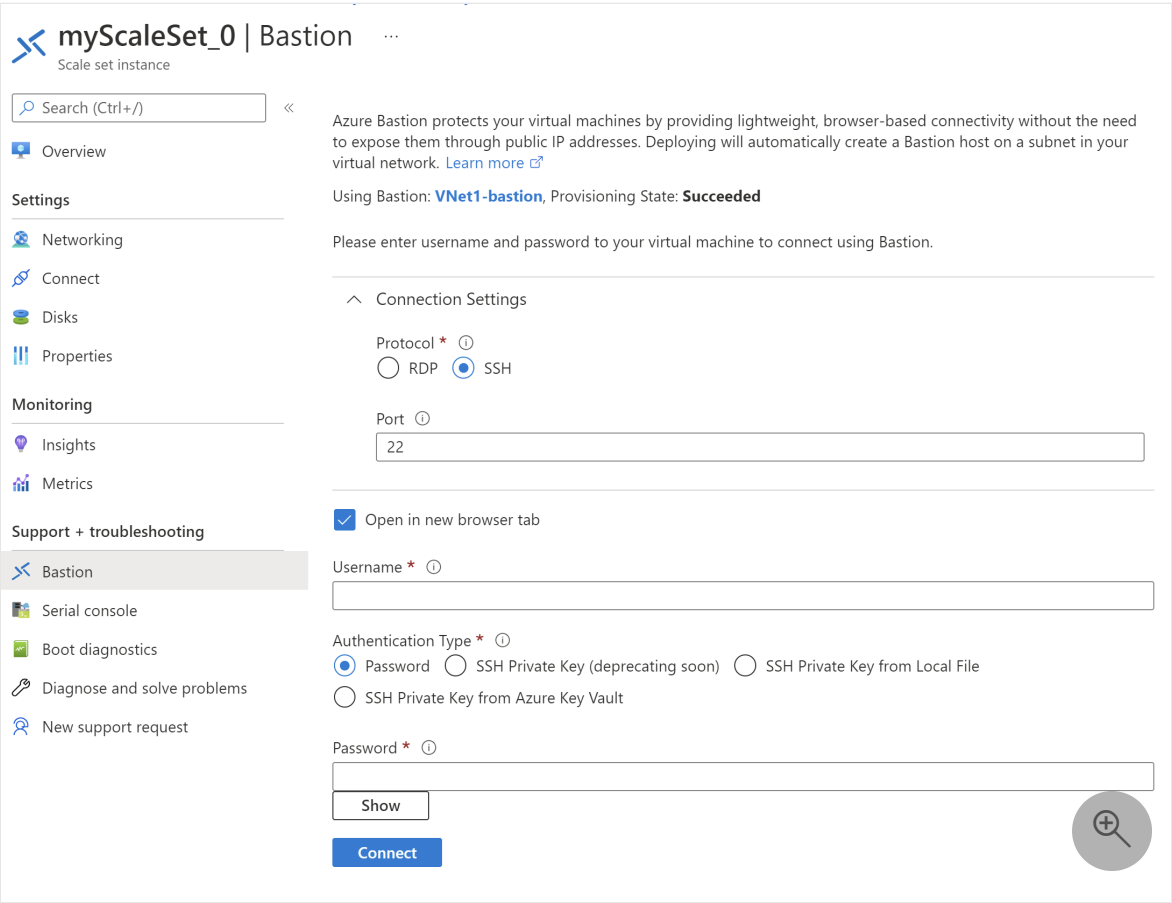
2. Go to the virtual machine scale set instance that you want to connect to.



3. Select **Connect** at the top of the page, then choose **Bastion** from the dropdown.



4. On the **Bastion** page, fill in the required settings. The settings you can select depend on the virtual machine to which you're connecting, and the Bastion SKU tier that you're using. The Standard SKU gives you more connection options than the Basic SKU. For more information about settings, see Bastion configuration settings.



5. After filling in the values on the Bastion page, select **Connect** to connect to the instance.

Next steps

Read the Bastion FAQ.

Enable browser connection to DevTest Labs VMs with Azure Bastion

Article • 12/20/2022 • 4 minutes to read

Azure DevTest Labs integrates with Azure Bastion to allow connecting to lab virtual machines (VMs) through a browser. As a lab owner, you can enable browser access to all your lab VMs through Azure Bastion.

Azure Bastion provides secure and seamless remote desktop protocol (RDP) and secure shell (SSH) connectivity over transport layer security (TLS), directly from the Azure portal. You don't need any other client, agent, or software to connect to your lab VMs through your browser. Your VMs don't need public IP addresses.

This article covers two different ways to enable Azure Bastion browser connectivity to DevTest Labs VMs:

- You can create a new Azure Bastion-enabled virtual network for your lab and its VMs.
- You can deploy Azure Bastion in your existing lab virtual network.

Prerequisites

- Have or create a lab in DevTest Labs.
- To use Azure Bastion browser access, lab users must have **Reader** role on the Azure Bastion host and on the lab virtual network that has Azure Bastion configured.

Option 1: Connect a lab to an Azure Bastion-enabled virtual network

First, create a new virtual network with an Azure Bastion subnet and another subnet in it. An Azure Bastion subnet doesn't allow creating non-Azure Bastion resources in it, so you need the other subnet for creating lab VMs.

1. In the Azure portal, search for and select **virtual networks**.

2. Select **+ Create** at the top of the **Virtual networks** page.

3. On the **Create virtual network** screen, enter a **Name** for the new virtual network, and select the same **Subscription**, **Resource group**, and **Region** as your lab.

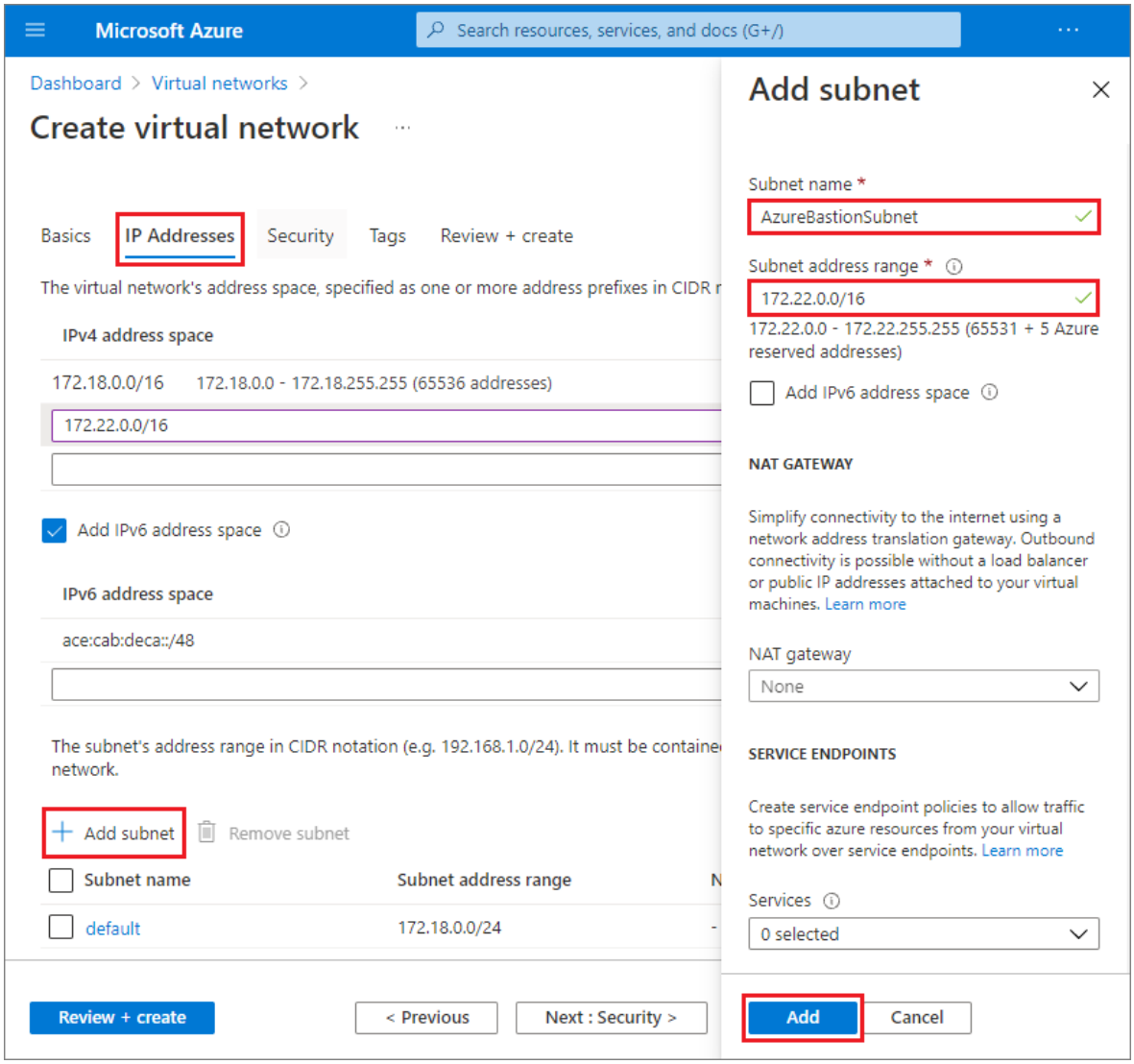
4. Select **Next: IP Addresses**.

5. On the **IP Addresses** tab, there's already one subnet, **default**. Select **Add subnet**.

6. On the **Add subnet** pane, enter *AzureBastionSubnet* under **Name**.

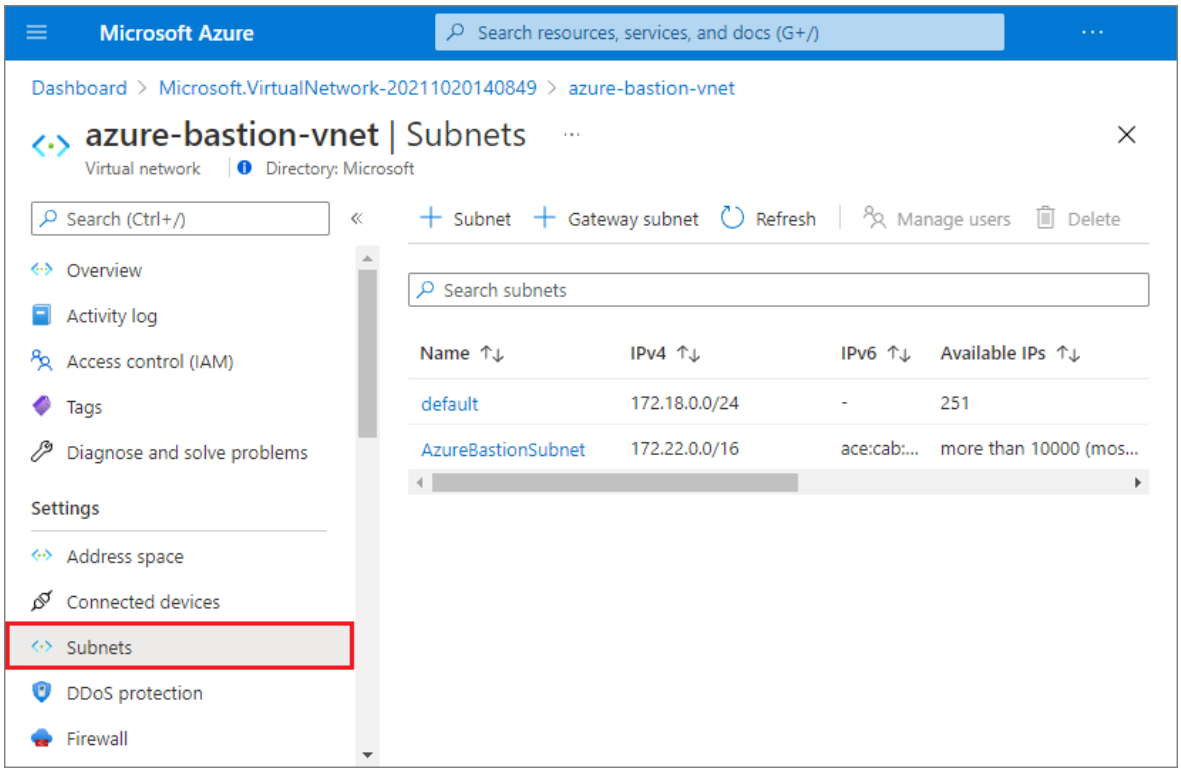
7. Under **Subnet address range**, enter an address range that's within the virtual network's address space but doesn't overlap with the default subnet. If necessary, you can add new address spaces in the blank fields on the **Create virtual network** page.

8. Select **Add**.



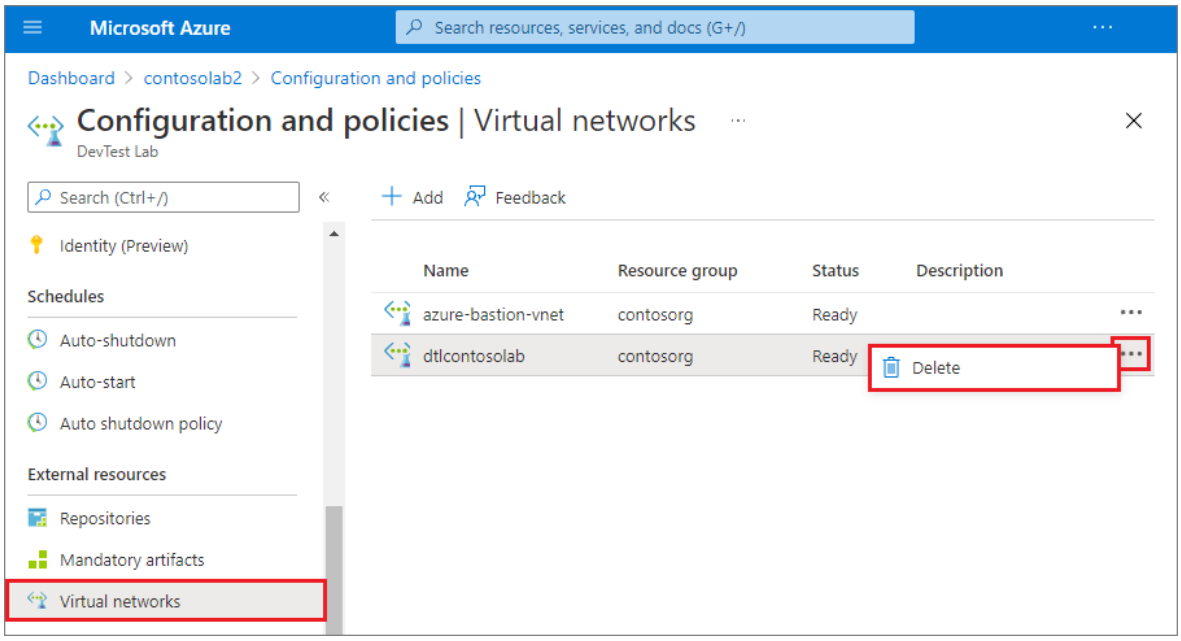
9. Select **Review + create**, and when validation passes, select **Create**.

10. Once the new virtual network is created, go to its page, select **Subnets** in the left navigation, and confirm that there are two subnets, **default** and **AzureBastionSubnet**.



Next, connect your lab to the new virtual network:

1. From your lab **Overview** page, select **Configuration and policies** in the left navigation.
2. On the **Configuration and policies** page, in the left navigation under **External resources**, select **Virtual networks**.
3. On the **Configuration and policies | Virtual networks** page, select **Add**.
4. On the **Virtual network** page, select **Select virtual network**.
5. On the **Choose virtual network** page, select the Azure Bastion-enabled virtual network you just created.
6. On the **Virtual network** page, select **Save**.
7. On the **Configuration and policies | Virtual networks** page, remove any previous virtual network from the lab. Select **...** next to that virtual network, select **Delete**, and then select **Yes**.



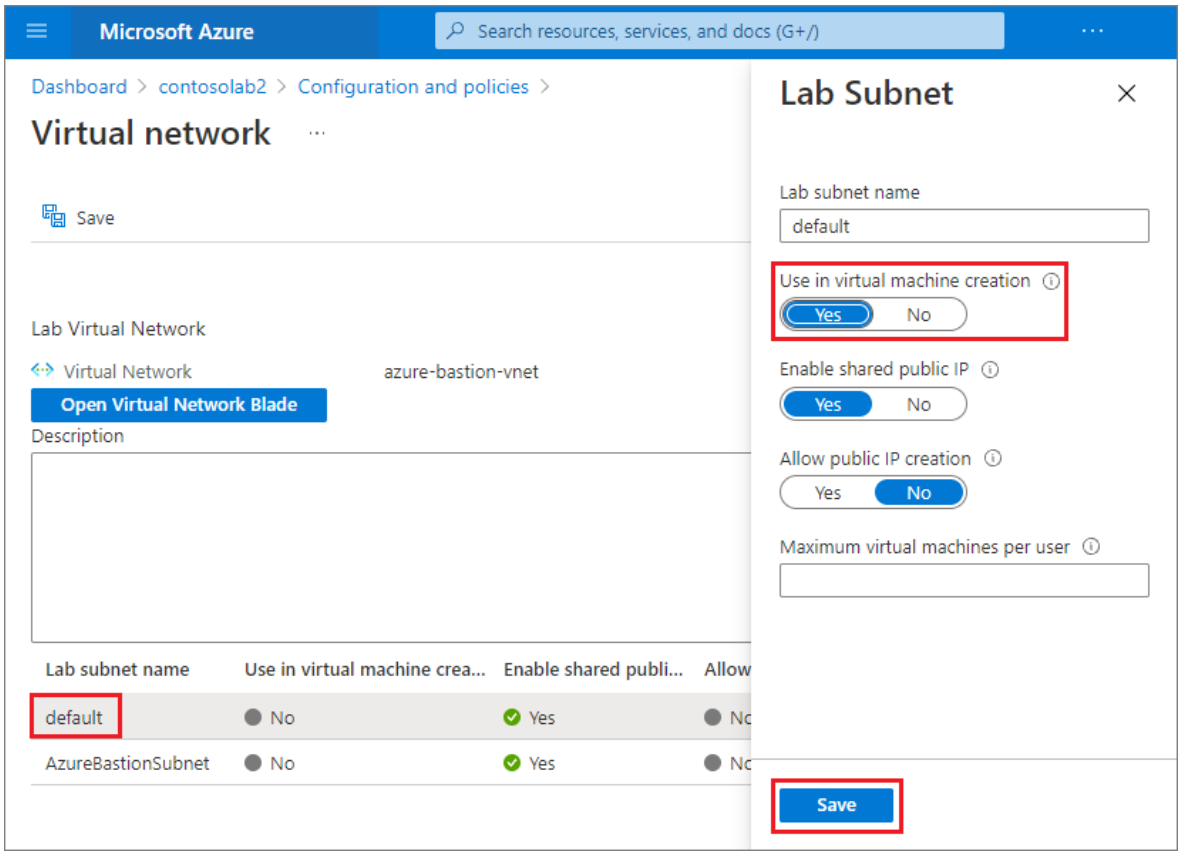
Enable VM creation in the non-Azure Bastion subnet:

1. On the **Configuration and policies | Virtual networks** page, select the Azure Bastion-enabled virtual network.

2. On the **Virtual network** page, make sure that both the **AzureBastionSubnet** subnet and the **default** subnet appear. If you don't see both subnets, close and reopen the page.

3. Select the **default** subnet.

4. On the **Lab Subnet** pane, under **Use in virtual machine creation**, select **Yes**, and then select **Save**. You can now create VMs in the default subnet of your lab virtual network.



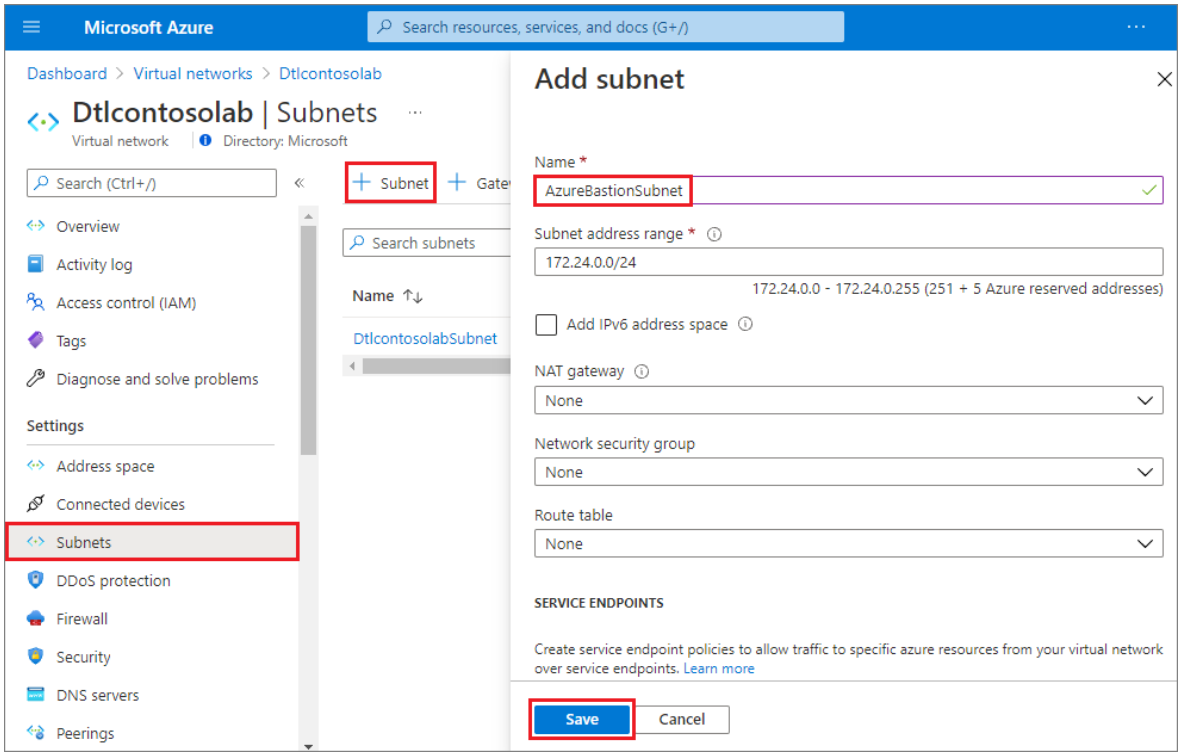
Option 2: Deploy Azure Bastion in a lab's existing virtual network

First, create a new Azure Bastion subnet in your lab's existing virtual network:

1. In the Azure portal, search for and select **Virtual networks**.
2. On the **Virtual networks** page, select your lab's existing virtual network from the list.
3. On the virtual network page, select **Subnets**.
4. On the **Subnets** page, select **+ Subnet** on the top menu.
5. On the **Add Subnet screen**, enter *AzureBastionSubnet* under **Name**.
6. Under **Subnet address range**, enter an address range that's within the virtual network's address space, but doesn't overlap with the existing lab subnet.

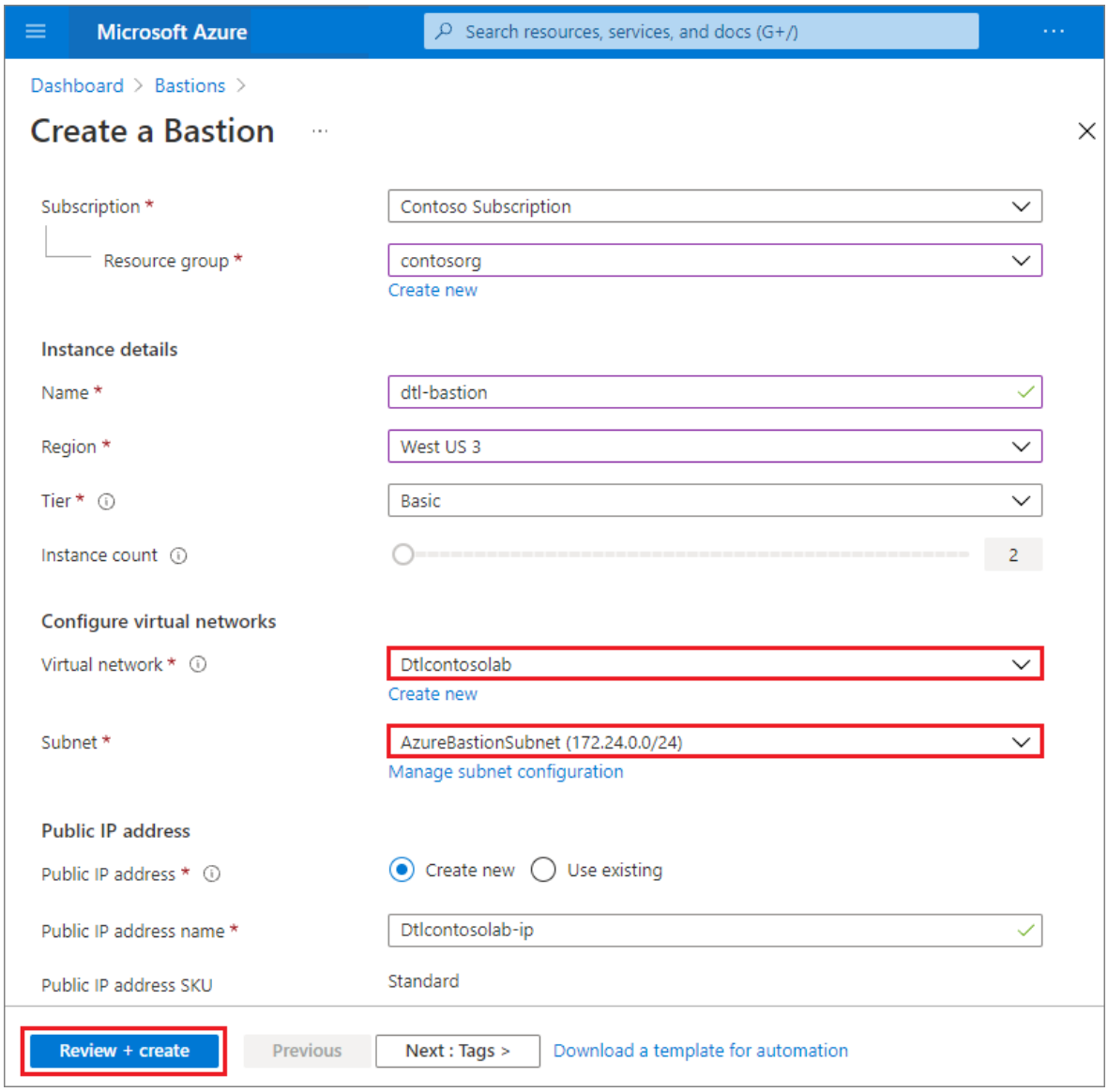
> **Tip**
>
> You might have to cancel out of this dialog, select **Address space** in the virtual network's left navigation, and create a new address space for the subnet.

7. Select **Save**.



Next, deploy the Azure Bastion host in the new Azure Bastion subnet:

1. In the Azure portal, search for and select **Bastions**.
2. On the **Bastions** page, select **+ Create** at the top.
3. On the **Create a Bastion** page, enter a **Name**, and select the same **Subscription**, **Resource group**, and **Region** as your lab.
4. Under **Virtual networks**, select your lab's virtual network from the dropdown list, and make sure **AzureBastionSubnet** is selected under **Subnet**.
5. Select **Review + create**, and when validation passes, select **Create**.



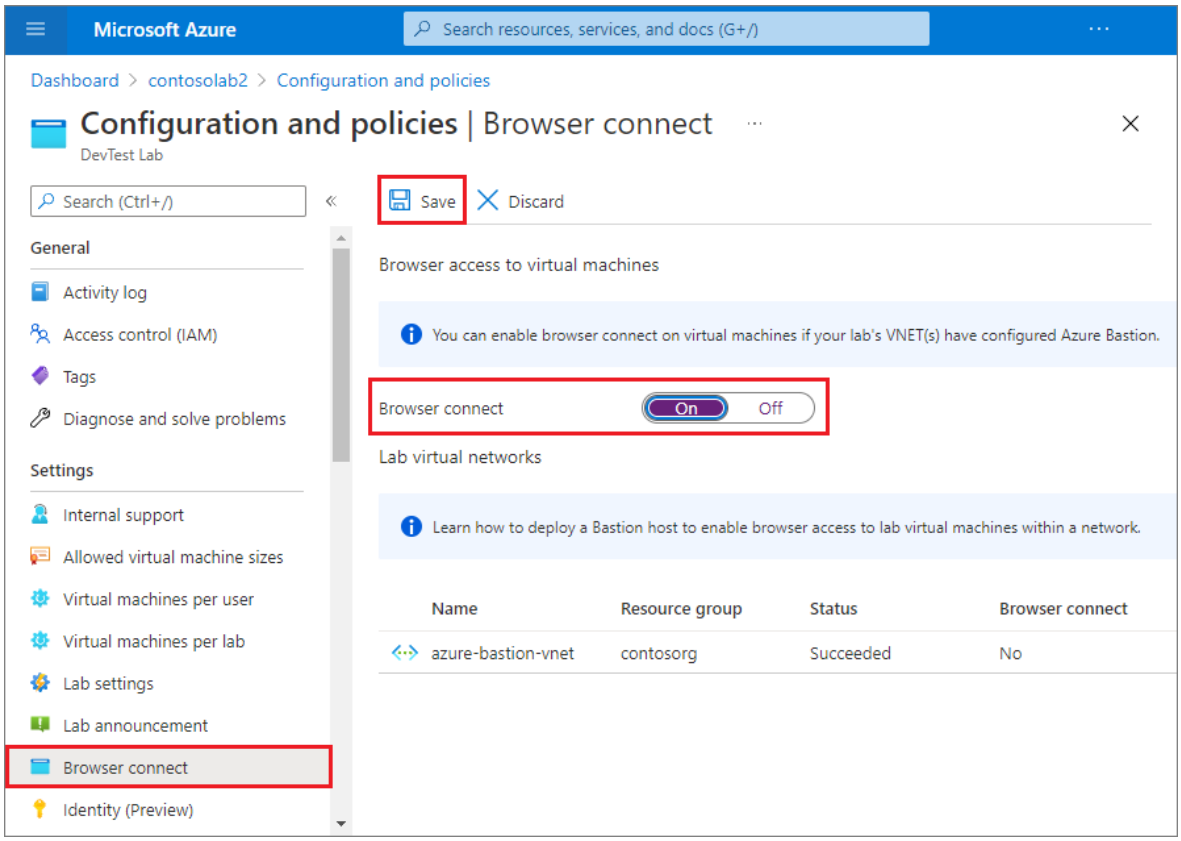
Connect to lab VMs through Azure Bastion

Once you deploy Azure Bastion in your lab virtual network, enable browser connections for the lab:

1. On the lab **Overview** page, select **Configuration and policies**, and then under **Settings**, select **Browser connect**.

2. On the **Browser connect** page, select **On**.

3. Select **Save** at the top of the page.



To connect to a lab VM through Azure Bastion:

1. On the lab **Overview** page, from **My virtual machines**, select a lab VM.
2. At the top of the VM's page, select **Browser connect**.
3. In the **Browser connect** pane, enter your VM's username and password, and select **Connect**.

Next steps

- What is Azure Bastion?
- Add a VM to your lab

Copy and paste to a Windows virtual machine: Azure Bastion

Article • 09/21/2022 • 2 minutes to read

This article helps you copy and paste text to and from virtual machines when using Azure Bastion.

Prerequisites

Before you proceed, make sure you have the following items.

- A VNet with Azure Bastion deployed.
- A Windows VM deployed to your VNet.

Configure the bastion host

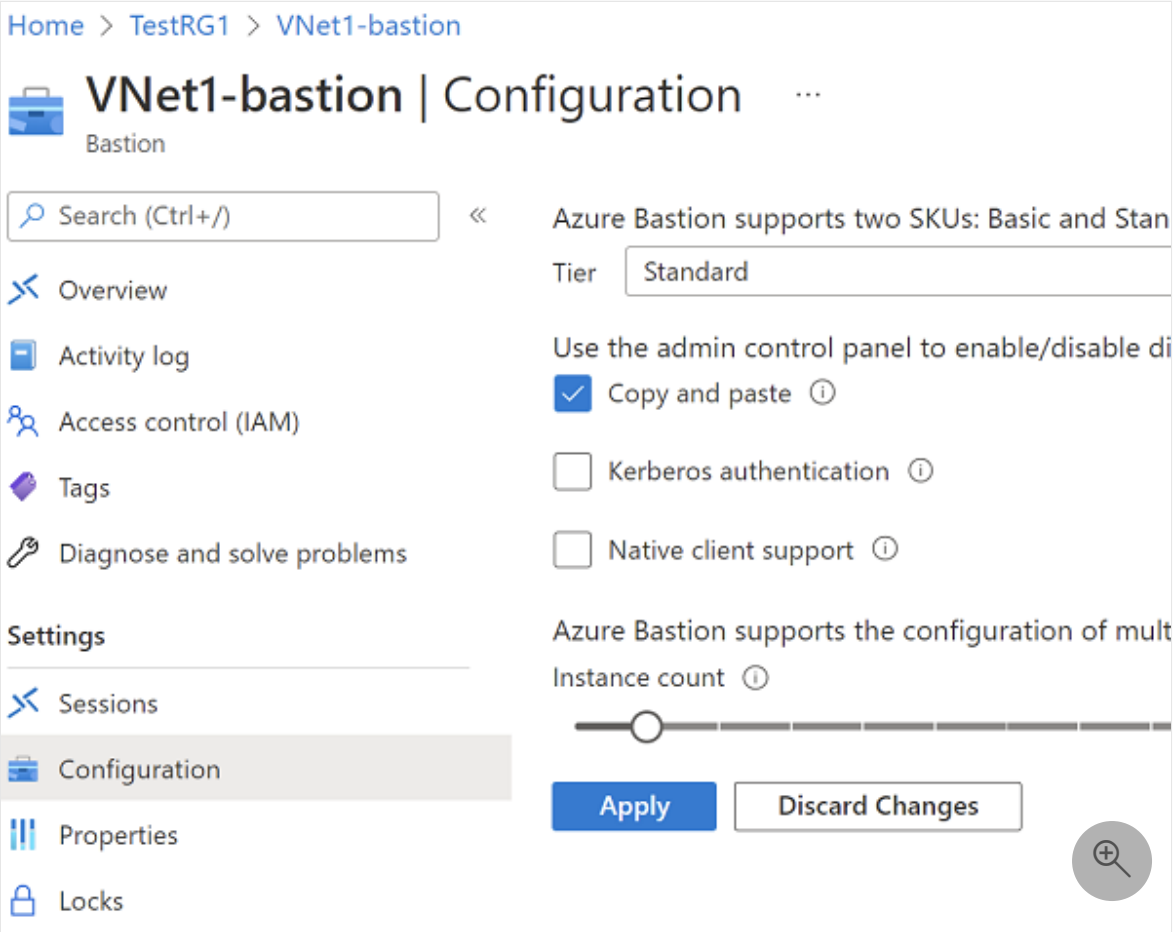
By default, Azure Bastion is automatically enabled to allow copy and paste for all sessions connected through the bastion resource. You don't need to configure anything additional. This applies to both the Basic and the Standard SKU tier. If you want to disable this feature, you can disable it for web-based clients on the configuration page of your Bastion resource.

1. To view or change your configuration, in the portal, go to your Bastion resource.

2. Go to the **Configuration** page.

    - To enable, select the **Copy and paste** checkbox if it isn't already selected.
    - To disable, clear the checkbox. Disable is only available with the Standard SKU. You can upgrade the SKU if necessary.

3. **Apply** changes. The bastion host will update.



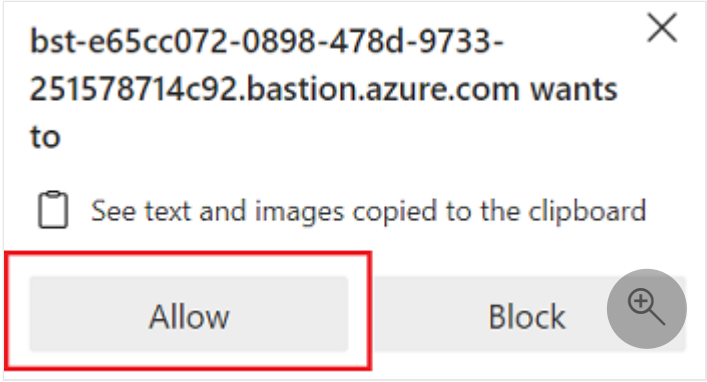
Copy and paste

For browsers that support the advanced Clipboard API access, you can copy and paste text between your local device and the remote session in the same way you copy and paste between applications on your local device. For other browsers, you can use the Bastion clipboard access tool palette.

> **Note**
>
> Only text copy/paste is currently supported.

Advanced Clipboard API browsers

1. Connect to your VM.
2. For direct copy and paste, your browser may prompt you for clipboard access when the Bastion session is being initialized. **Allow** the web page to access the clipboard.



3. You can now use keyboard shortcuts as usual to copy and paste. If you're working from a Mac, the keyboard shortcut to paste is **SHIFT-CTRL-V**.

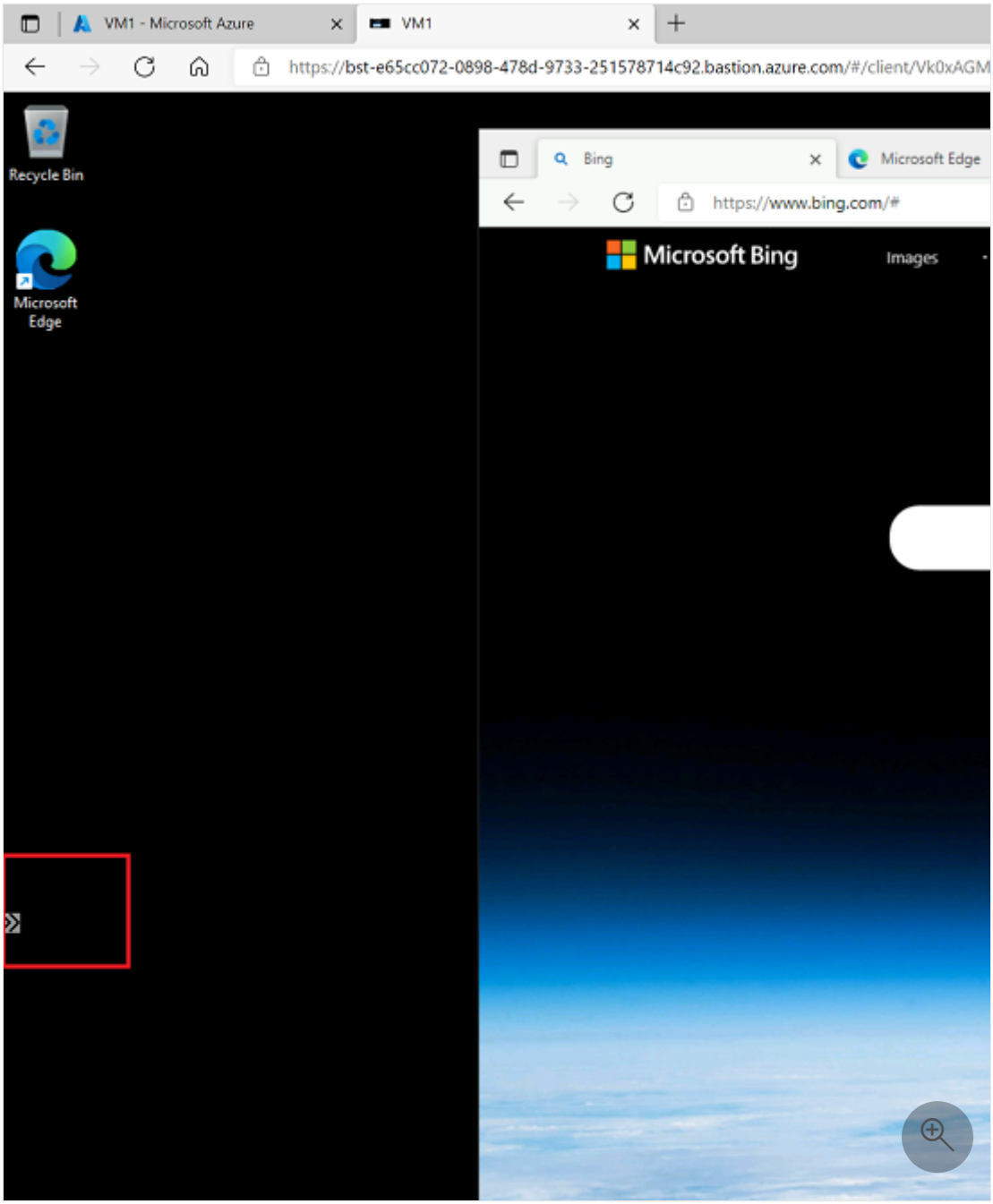
Non-advanced Clipboard API browsers

To copy text from your local computer to a VM, use the following steps.

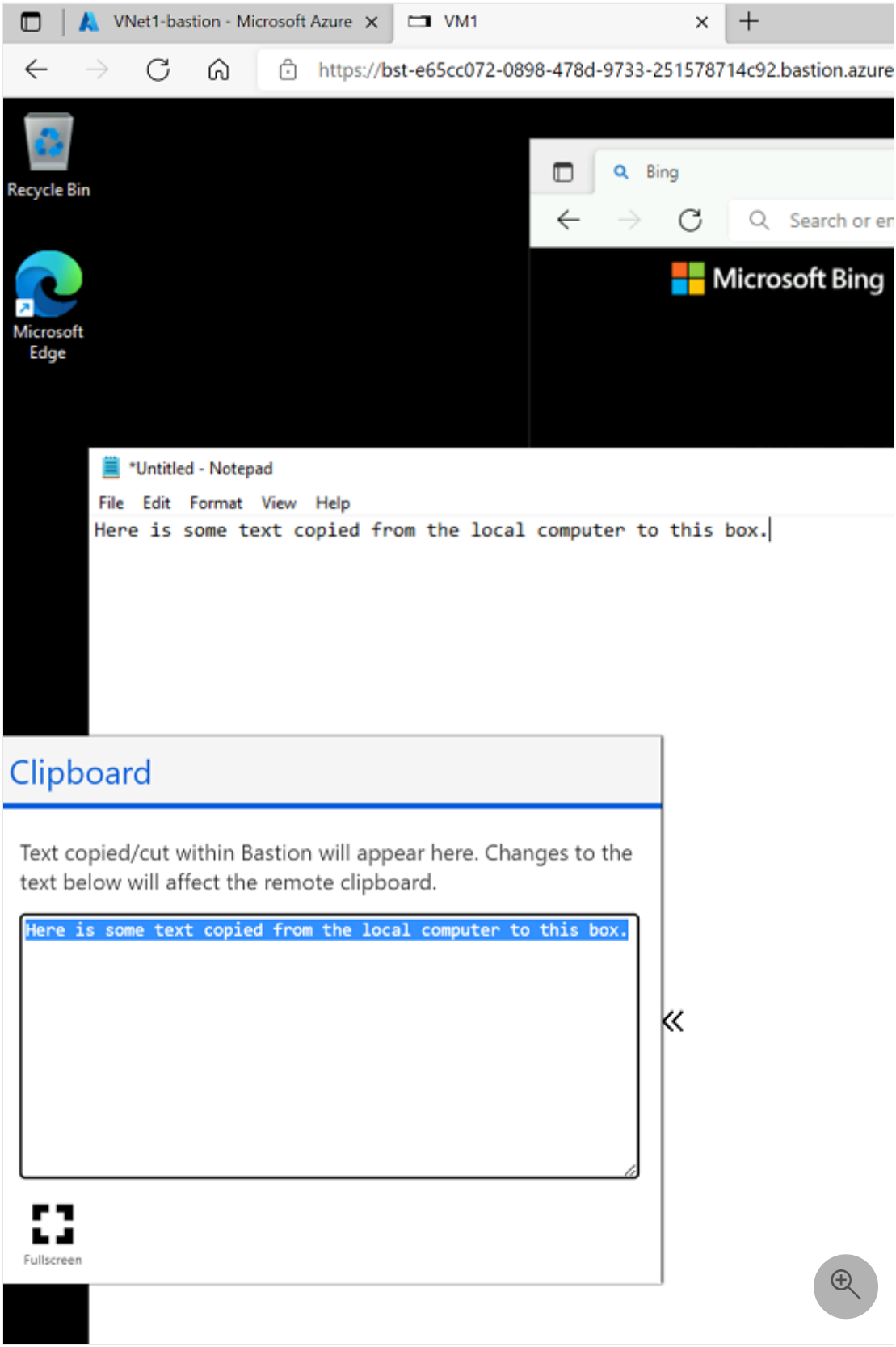
1. Connect to your VM.

2. Copy the text/content from the local device into your local clipboard.

3. On the VM, launch the Bastion clipboard access tool palette by selecting the two arrows. The arrows are located on the left center of the session.



4. Copy the text from your local computer. Typically, the copied text automatically shows on the Bastion clipboard access tool palette. If doesn't show up on the tool palette, then paste the text in the text area on the tool palette. Once the text is in the text area, you can paste it to the remote session. In this example, we copied text to the Bastion clipboard tool palette, then pasted it to the VM Notepad app.



5. If you want to copy the text from the VM to your local computer, copy the text to the clipboard access tool. Once your text is in the text area on the palette, paste it to your local computer.

Next steps

For more VM features, see About VM connections and features.

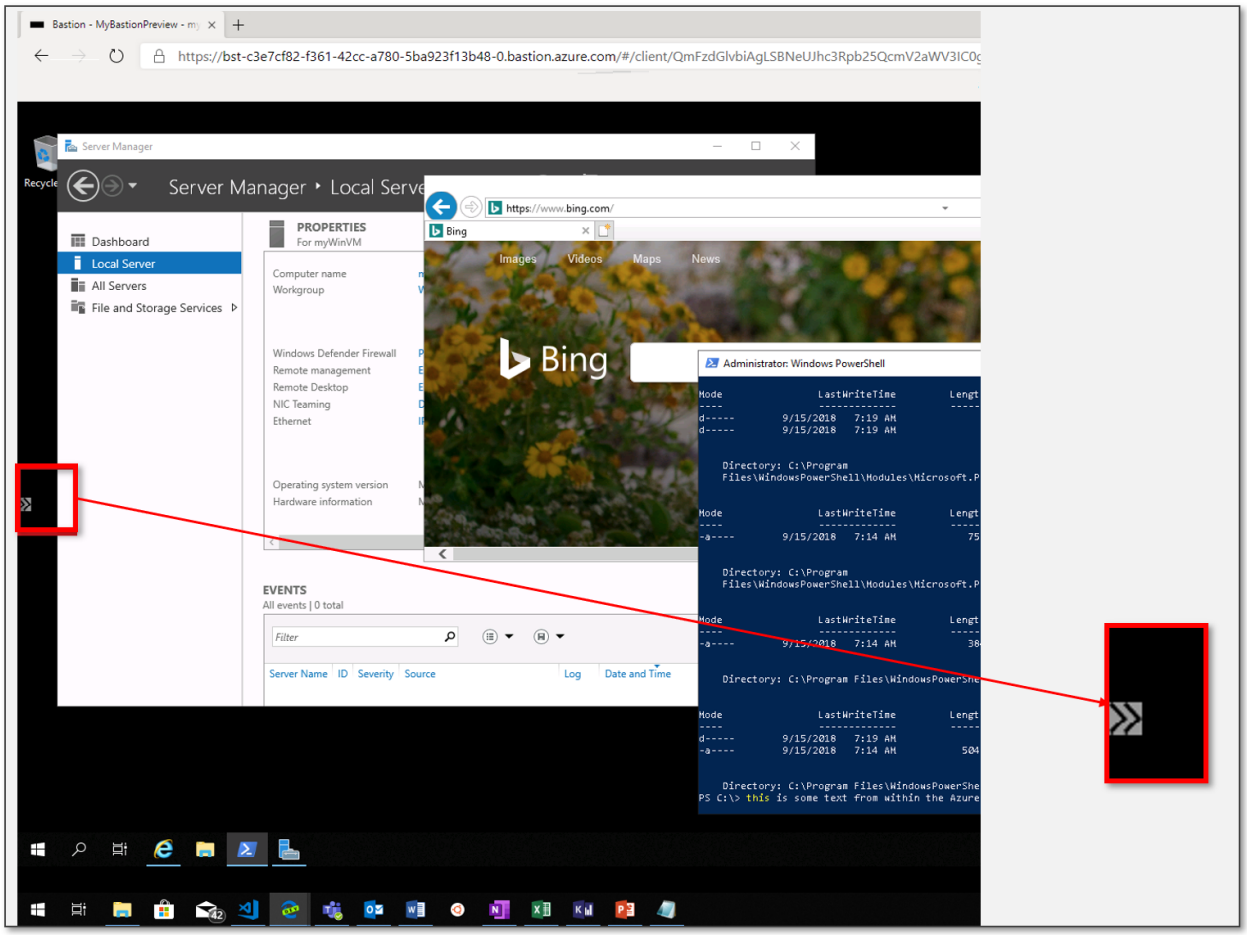
Change to full screen view for a VM session

Article • 02/08/2023 • 2 minutes to read

This article helps you change the virtual machine view to full screen and back in your browser when connected to a VM using Azure Bastion.

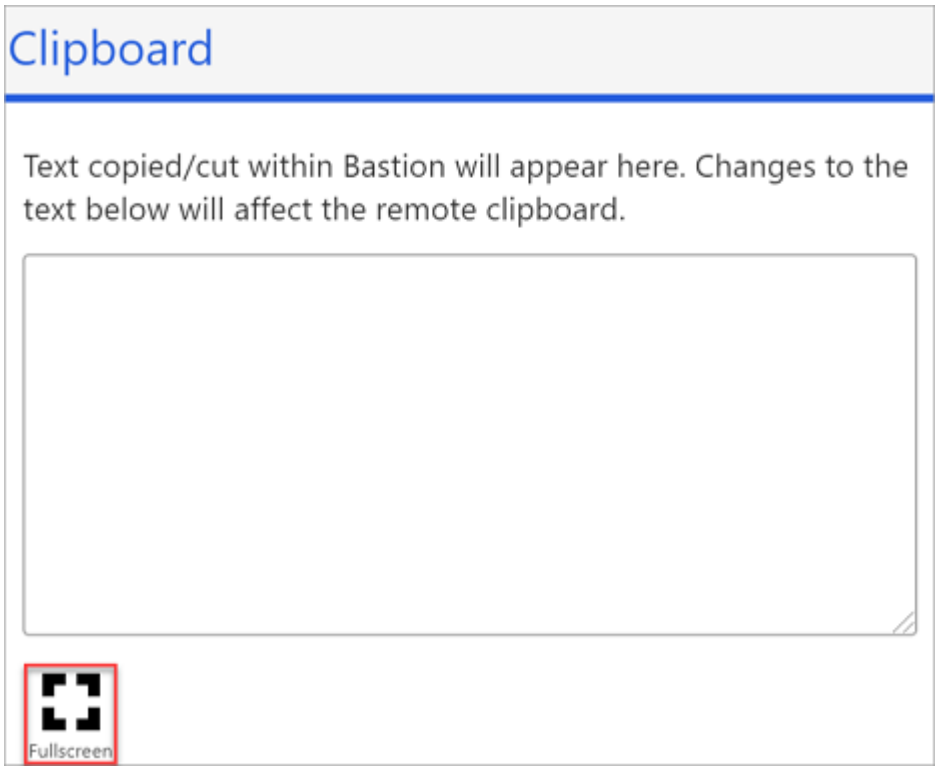
Launch the clipboard tool

During the remote session, launch the Bastion clipboard access tool palette by selecting the two arrows that located on the left center of the session.



Select full screen

Select the **Fullscreen** button to switch the session to a full screen experience. Once you switch, the session will reinitialize to full screen.



Next steps

For more VM features, see About VM connections and features.

Additional resources

Documentation

Connect to a VM using a native client and Azure Bastion - Azure Bastion

Learn how to connect to a VM from a Windows computer by using Bastion and a native client.

Copy and paste to and from a Windows virtual machine: Azure - Azure Bastion

Learn how copy and paste to and from a Windows VM using Bastion.

Upload or download files using a native client connection - Azure Bastion

Learn how to upload or download files using Azure Bastion and a native client when connected to a VM using Azure Bastion.

Connect to a Windows VM using RDP - Azure Bastion

Learn how to use Azure Bastion to connect to Windows VM using RDP.

Troubleshoot Azure Bastion

Learn how to troubleshoot Azure Bastion.

Connect to a VM - specified private IP address: Azure portal - Azure Bastion

Learn how to connect to your virtual machines using a specified private IP address via Azure Bastion.

Associate a public IP address to a virtual machine

Learn how to associate a public IP address to a virtual machine (VM) by using the Azure portal, Azure CLI or Azure PowerShell.

Cannot remote desktop to Azure Virtual Machines because of static IP - Virtual Machines

Learn how to troubleshoot RDP problem that is caused by static IP in Microsoft Azure.

Show 5 more

File upload and download to a VM using a native client

Article • 02/08/2023 • 3 minutes to read

Azure Bastion offers support for file transfer between your target VM and local computer using Bastion and a native RDP or native SSH client. To learn more about native client support, refer to Connect to a VM using the native client. While it may be possible to use third-party clients and tools to upload or download files, this article focuses on working with supported native clients.

- File transfers are supported using the native client only. You can't upload or download files using PowerShell or via the Azure portal.
- To both upload and download files, you must use the Windows native client and RDP.
- You can upload files to a VM using the native client of your choice and either RDP or SSH.
- This feature requires the Standard SKU. The Basic SKU doesn't support using the native client.

Prerequisites

- Install Azure CLI (version 2.32 or later) to run the commands in this article. For information about installing the CLI commands, see Install the Azure CLI and Get Started with Azure CLI.
- Get the Resource ID for the VM to which you want to connect. The Resource ID can be easily located in the Azure portal. Go to the Overview page for your VM and select the *JSON View* link to open the Resource JSON. Copy the Resource ID at the top of the page to your clipboard to use later when connecting to your VM.

Upload and download files - RDP

The steps in this section apply when connecting to a target VM from a Windows local computer using the native Windows client and RDP. The **az network bastion rdp** command uses the native client MSTSC. Once connected to the target VM, you can upload and download files using **right-click**, then **Copy** and **Paste**. To learn more about this command and how to connect, see Connect to a VM using a native client.

> ⓘ **Note**

File transfer over SSH is not supported using this method. Instead, use the **az network bastion tunnel command** to upload files over SSH.

1. Sign in to your Azure account. If you have more than one subscription, select the subscription containing your Bastion resource.

   Azure CLI

   ```
   az login
   az account list
   az account set --subscription "<subscription ID>"
   ```

2. Sign in to your target VM via RDP using the following command. You can use either a local username and password, or your Azure AD credentials. To learn more about how to use Azure AD to sign in to your Azure Windows VMs, see Azure Windows VMs and Azure AD.

   Azure CLI

   ```
   az network bastion rdp --name "<BastionName>" --resource-group "
   <BastionResourceGroupName>" --target-resource-id "<VMResourceId>"
   ```

3. Once you sign in to your target VM, the native client on your computer will open up with your VM session. You can now transfer files between your VM and local machine using right-click, then **Copy** and **Paste**.

Upload files - SSH and RDP

The steps in this section apply to native clients other than Windows, as well as Windows native clients that want to connect over SSH to upload files. This section helps you upload files from your local computer to your target VM over SSH or RDP using the **az network bastion tunnel** command. To learn more about the tunnel command and how to connect, see Connect to a VM using a native client.

> **Note**
>
> This command can be used to upload files from your local computer to the target VM. File download is not supported.

1. Sign in to your Azure account. If you have more than one subscription, select the subscription containing your Bastion resource.

Azure CLI

```
az login
az account list
az account set --subscription "<subscription ID>"
```

2. Open the tunnel to your target VM using the following command:

Azure CLI

```
az network bastion tunnel --name "<BastionName>" --resource-group "
<ResourceGroupName>" --target-resource-id "<VMResourceId>" --resource-
port "<TargetVMPort>" --port "<LocalMachinePort>"
```

3. Open a second command prompt to connect to your target VM through the tunnel. In this second command prompt window, you can upload files from your local machine to your target VM using the following command:

Azure CLI

```
scp -P <LocalMachinePort>  <local machine file path>
<username>@127.0.0.1:<target VM file path>
```

4. Connect to your target VM using SSH or RDP, the native client of your choice, and the local machine port you specified in Step 3.

   For example, you can use the following command if you have the OpenSSH client installed on your local computer:

Azure CLI

```
ssh <username>@127.0.0.1 -p <LocalMachinePort>
```

Next steps

For more VM features, see About VM connections and features.

Additional resources

🕮 Documentation

Connect to a VM using a native client and Azure Bastion - Azure Bastion

Learn how to connect to a VM from a Windows computer by using Bastion and a native client.

Connect to a Windows VM using SSH - Azure Bastion

Learn how to use Azure Bastion to connect to Windows VM using SSH.

Connect to a Linux VM using SSH - Azure Bastion

Learn how to use Azure Bastion to connect to Linux VM using SSH.

Associate a public IP address to a virtual machine

Learn how to associate a public IP address to a virtual machine (VM) by using the Azure portal, Azure CLI or Azure PowerShell.

DNS Name resolution options for Linux VMs - Azure Virtual Machines

Name Resolution scenarios for Linux virtual machines in Azure IaaS, including provided DNS services, hybrid external DNS and Bring Your Own DNS server.

Copy and paste to and from a Windows virtual machine: Azure - Azure Bastion

Learn how copy and paste to and from a Windows VM using Bastion.

Connect to a Linux VM using RDP - Azure Bastion

Learn how to use Azure Bastion to connect to Linux VM using RDP.

Troubleshoot SSH connection issues to an Azure VM - Virtual Machines

How to troubleshoot issues such as 'SSH connection failed' or 'SSH connection refused' for an Azure VM running Linux.

Show 5 more

How to configure monitoring and metrics for Azure Bastion using Azure Monitor

Article • 03/03/2022 • 2 minutes to read

This article helps you work with monitoring and metrics for Azure Bastion using Azure Monitor.

> **Note**
>
> Using **Classic Metrics** is not recommended.

About metrics

Azure Bastion has various metrics that are available. The following table shows the category and dimensions for each available metric.

Metric	Category	Dimension(s)
Bastion communication status**	Availability	N/A
Total memory	Availability	Instance
Used CPU	Traffic	Instance
Used memory	Traffic	Instance
Session count	Performance	Instance

** Bastion communication status is only applicable for bastion hosts deployed after November 2020.

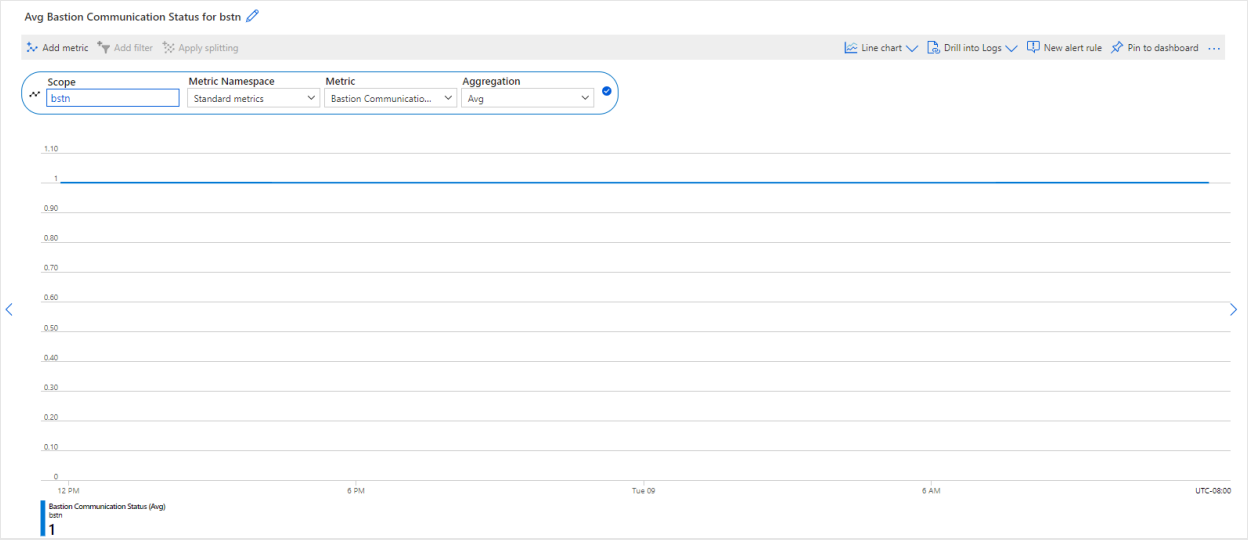
Availability metrics

Bastion communication status

You can view the communication status of Azure Bastion, aggregated across all instances comprising the bastion host.

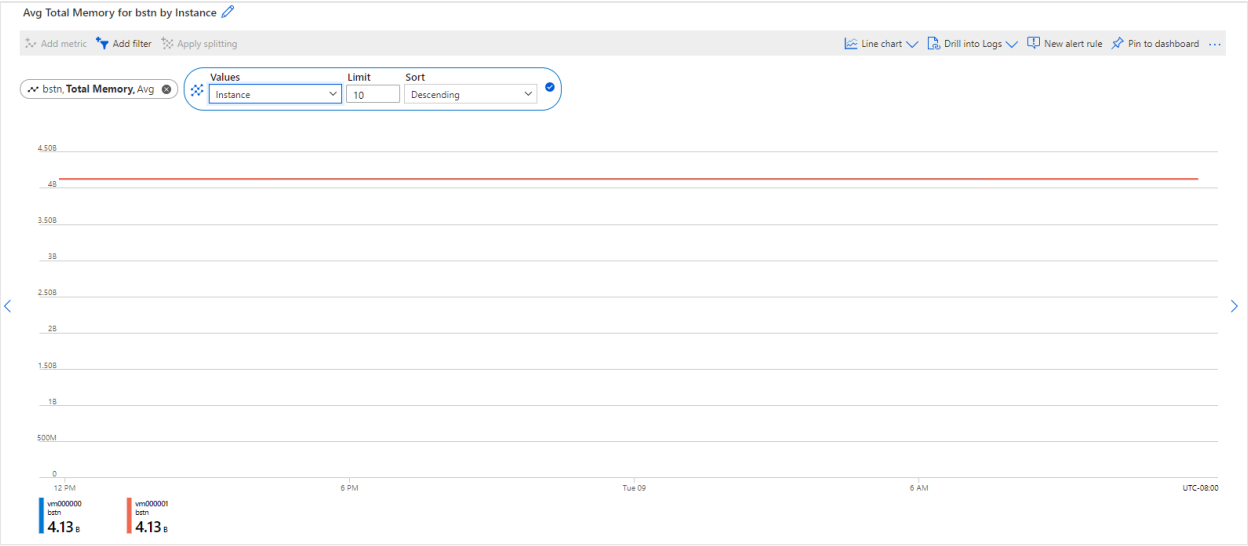
- A value of **1** indicates that the bastion is available.

- A value of **0** indicates that the bastion service is unavailable.



Total memory

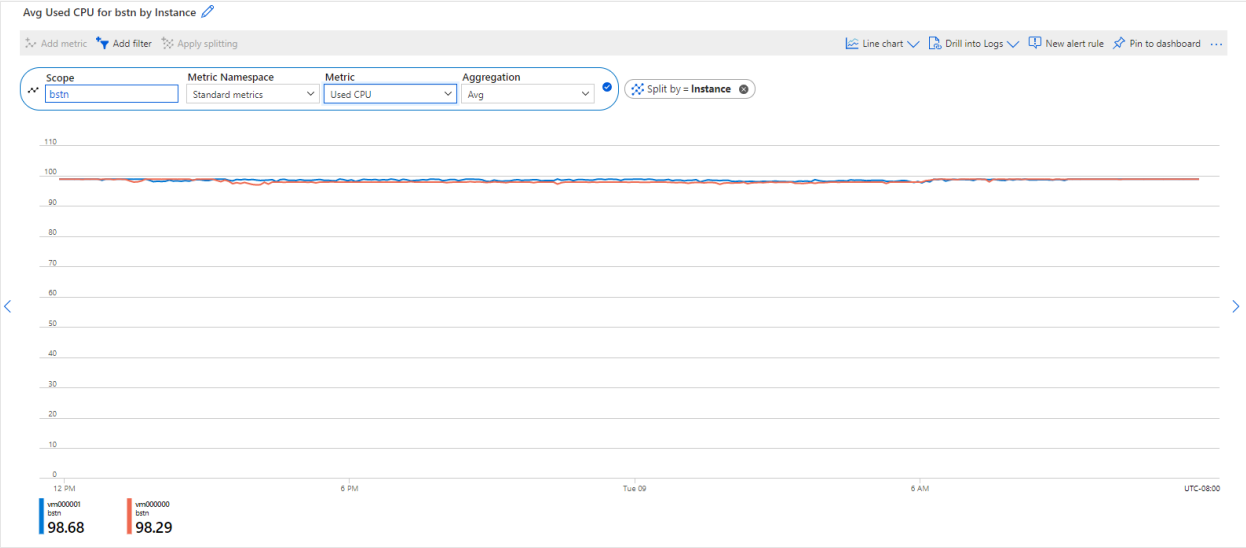
You can view the total memory of Azure Bastion, split across each bastion instance.



Traffic metrics

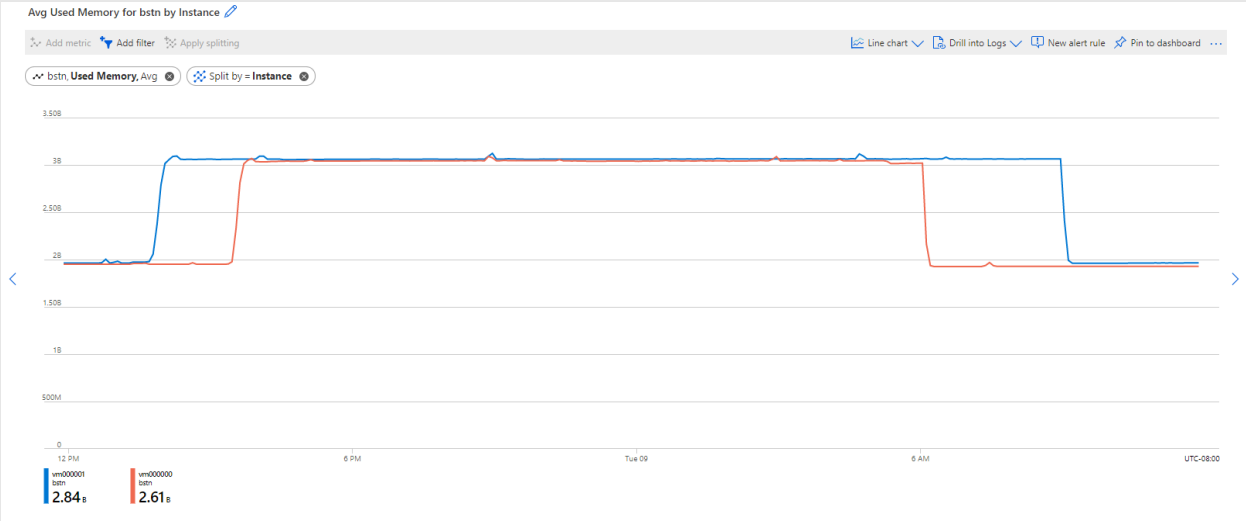
Used CPU

You can view the CPU utilization of Azure Bastion, split across each bastion instance. Monitoring this metric will help gauge the availability and capacity of the instances that comprise Azure Bastion



Used memory

You can view memory utilization across each bastion instance, split across each bastion instance. Monitoring this metric will help gauge the availability and capacity of the instances that comprise Azure Bastion.



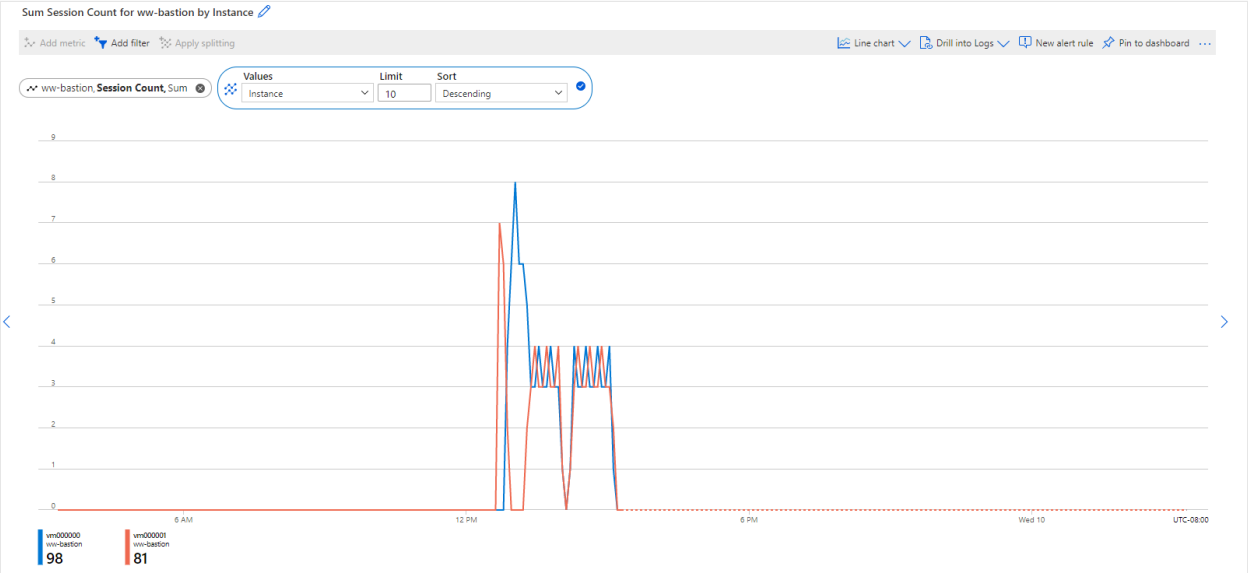
Performance metrics

Session count

You can view the count of active sessions per bastion instance, aggregated across each session type (RDP and SSH). Each Azure Bastion can support a range of active RDP and SSH sessions. Monitoring this metric will help you to understand if you need to adjust the number of instances running the bastion service. For more information about the session count Azure Bastion can support, refer to the Azure Bastion FAQ.

The recommended values for this metric's configuration are:

- **Aggregation:** Avg
- **Granularity:** 5 or 15 minutes
- Splitting by instances is recommended to get a more accurate count



How to view metrics

1. To view metrics, go to your bastion host.

2. From the **Monitoring** list, select **Metrics**.

3. Select the parameters. If no metrics are set, click **Add metric**, and then select the parameters.

    - **Scope:** By default, the scope is set to the bastion host.
    - **Metric Namespace:** Standard Metrics.
    - **Metric:** Select the metric that you want to view.

4. Once a metric is selected, the default aggregation will be applied. Optionally, you can apply splitting, which will show the metric with different dimensions.

Next steps

Read the Bastion FAQ.

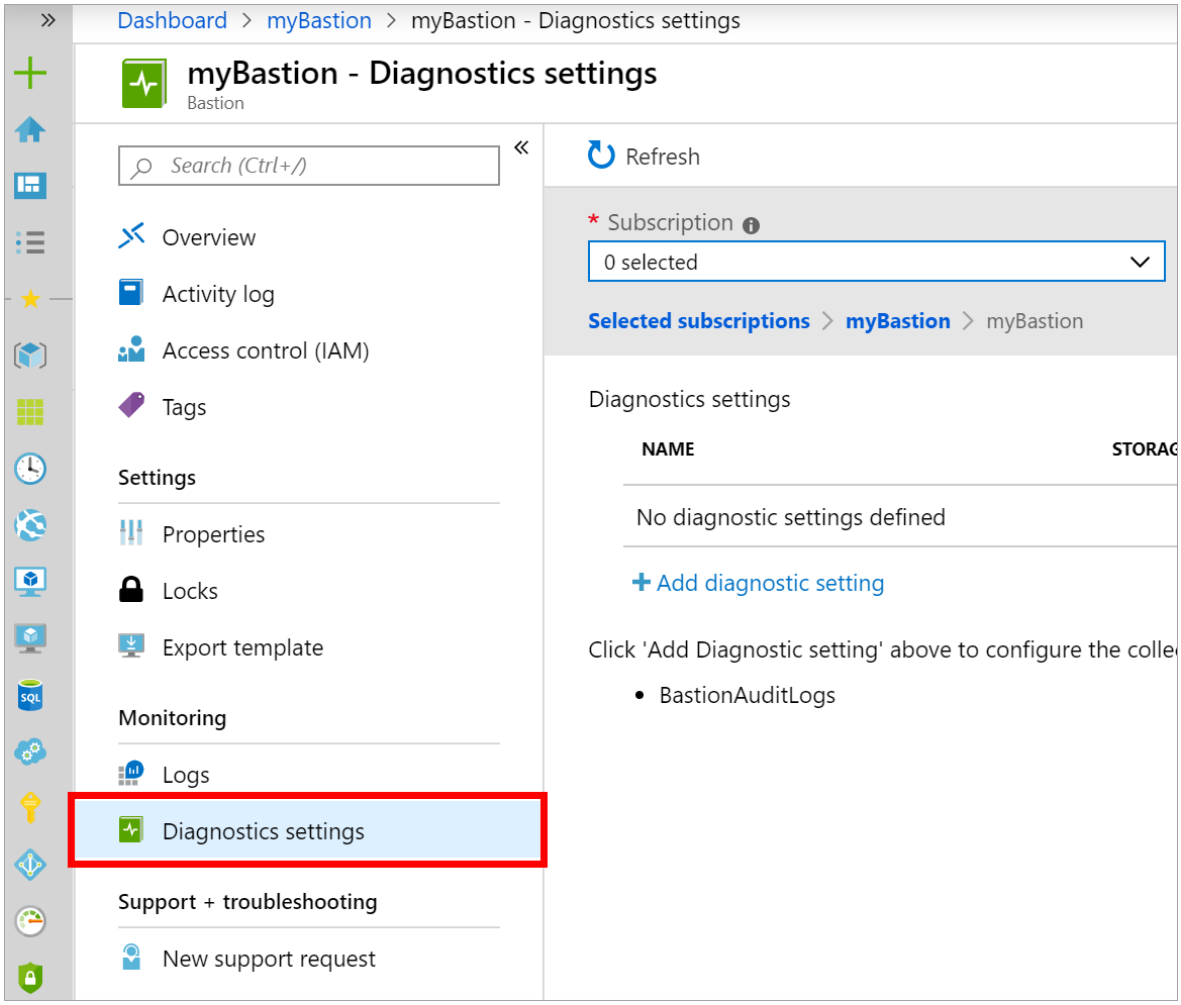
Enable and work with Bastion resource logs

Article • 02/08/2023 • 2 minutes to read

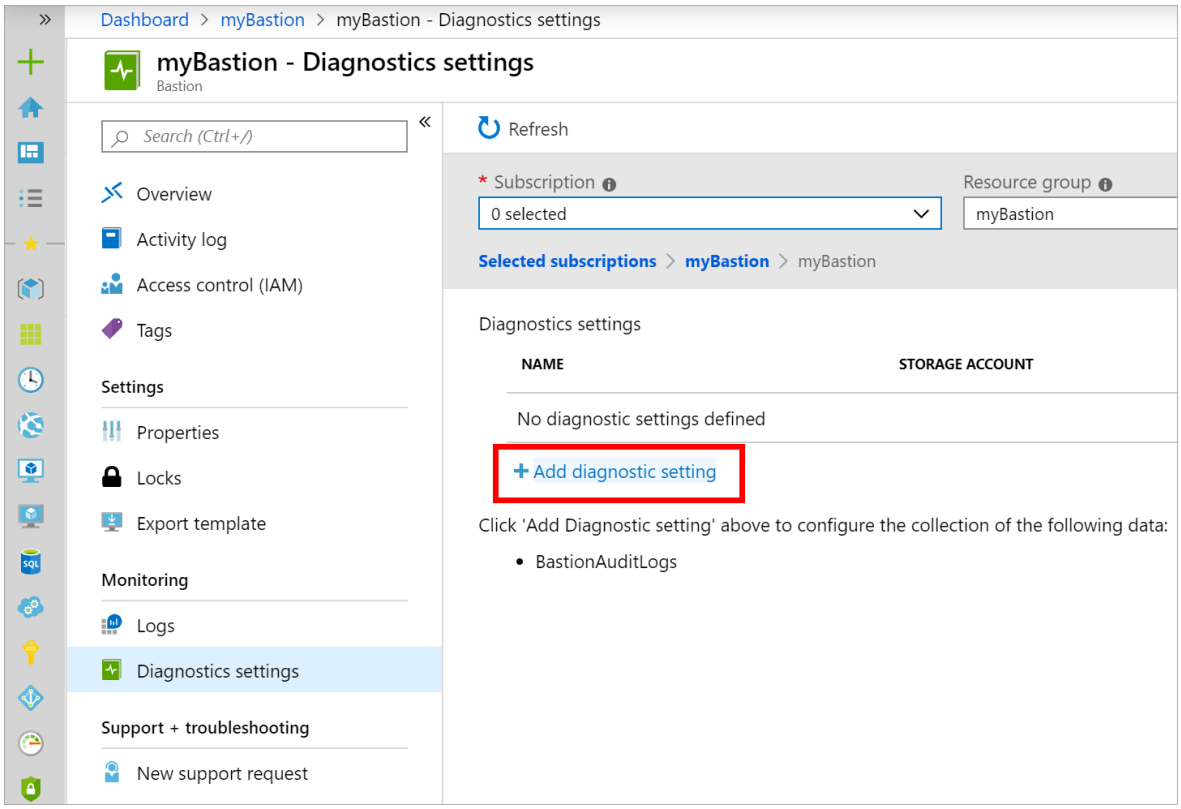
As users connect to workloads using Azure Bastion, Bastion can log diagnostics of the remote sessions. You can then use the diagnostics to view which users connected to which workloads, at what time, from where, and other such relevant logging information. In order to use the diagnostics, you must enable diagnostics logs on Azure Bastion. This article helps you enable diagnostics logs, and then view the logs.

Enable the resource log

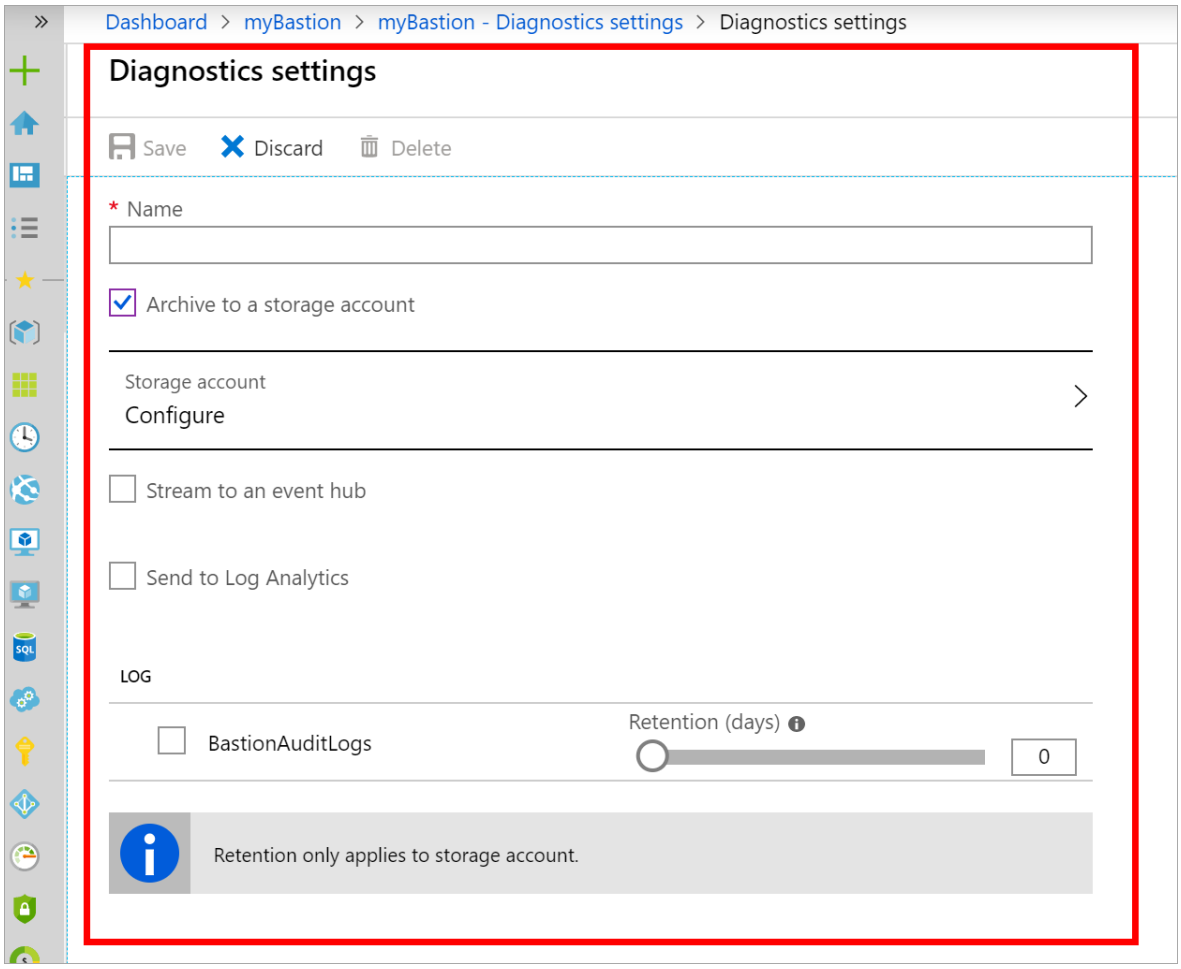
1. In the Azure portal, go to your Azure Bastion resource and select **Diagnostics settings** from the Azure Bastion page.



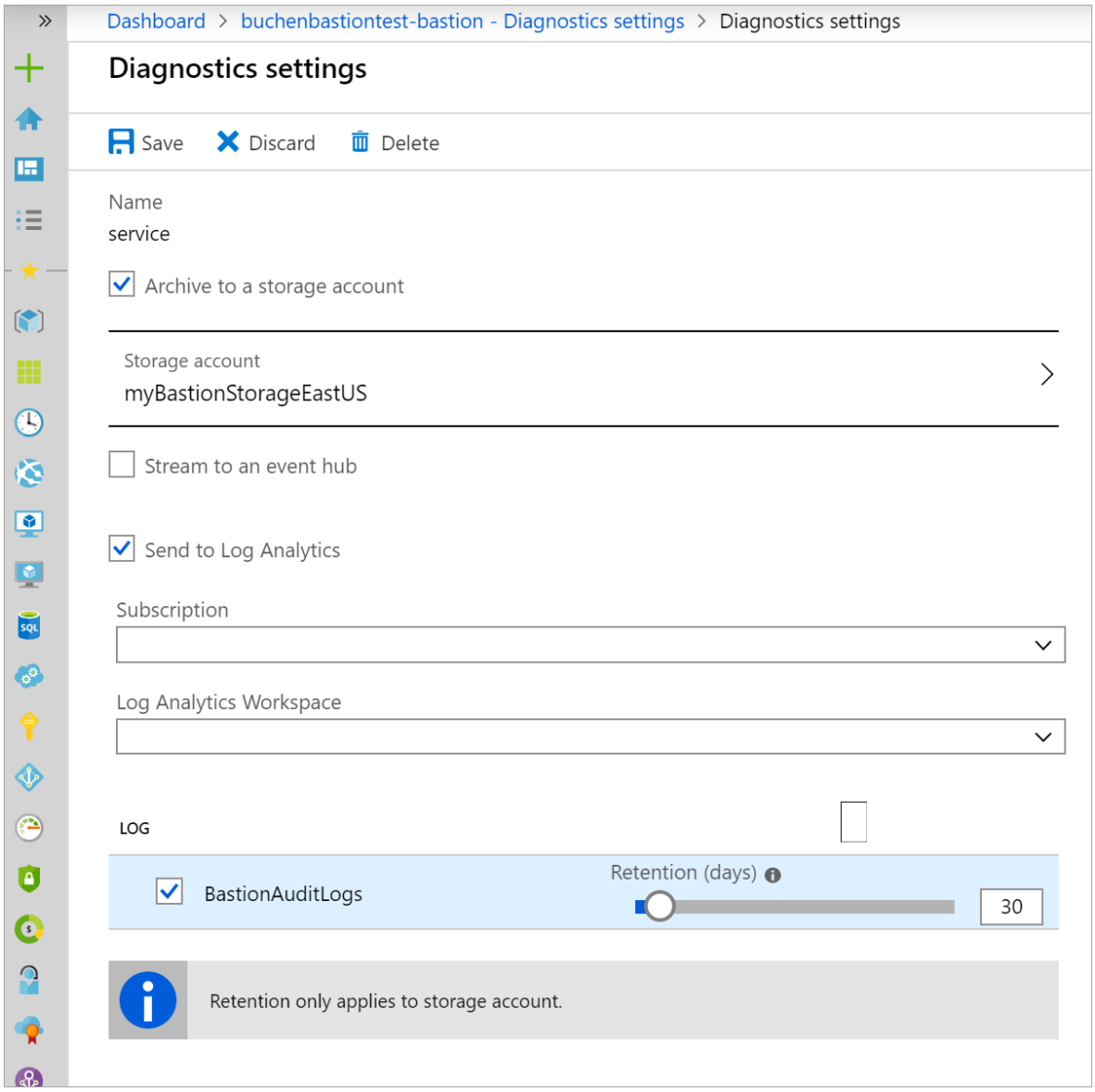
2. Select **Diagnostics settings**, then select **+Add diagnostic setting** to add a destination for the logs.



3. On the **Diagnostics settings** page, select the type of storage account to be used for storing diagnostics logs.



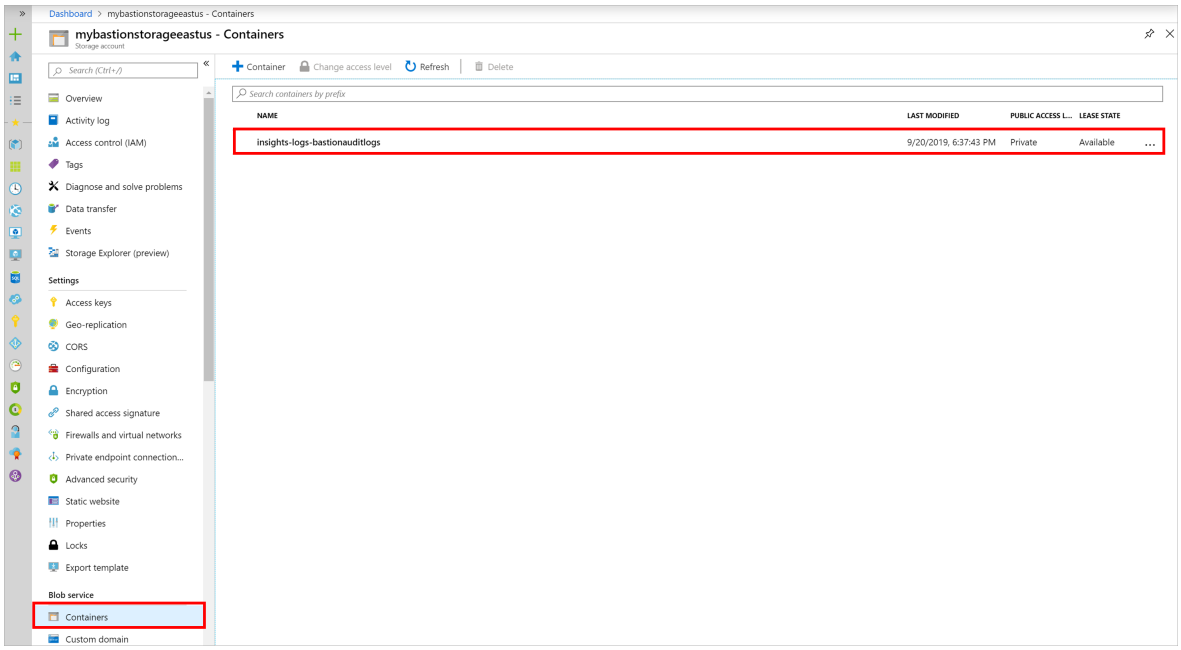
4. When you complete the settings, it will look similar to this example:



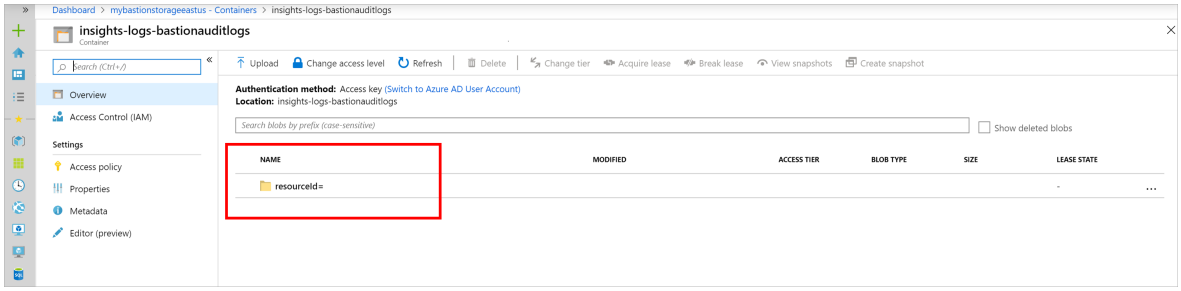
View diagnostics log

To access your diagnostics logs, you can directly use the storage account that you specified while enabling the diagnostics settings.

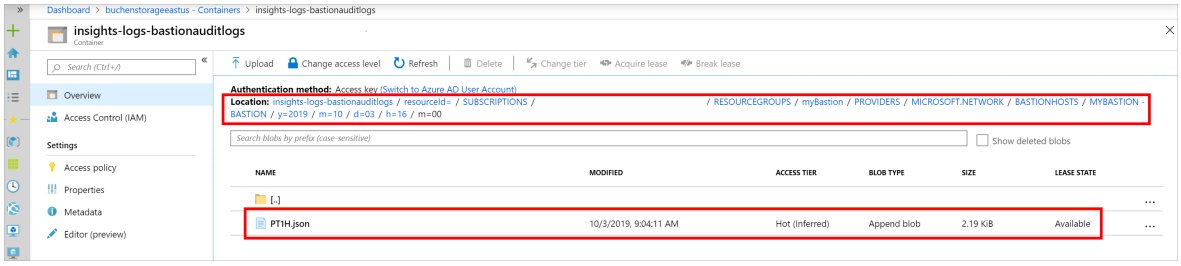
1. Navigate to your storage account resource, then to **Containers**. You see the **insights-logs-bastionauditlogs** blob created in your storage account blob container.



2. As you go inside the container, you see various folders in your blob. These folders indicate the resource hierarchy for your Azure Bastion resource.



3. Navigate to the full hierarchy of your Azure Bastion resource whose diagnostics logs you wish to access/view. The 'y=', 'm=', 'd=', 'h=' and 'm=' indicate the year, month, day, hour, and minute respectively for the resource logs.



4. Locate the json file created by Azure Bastion that contains the diagnostics log data for the time-period navigated to.

5. Download the json file from your storage blob container. An example entry of successful login from the json file is shown below for reference:

JSON

```
{
"time":"2019-10-03T16:03:34.776Z",
```

```
"resourceId":"/SUBSCRIPTIONS/<subscripionID>/RESOURCEGROUPS/MYBASTION/P
ROVIDERS/MICROSOFT.NETWORK/BASTIONHOSTS/MYBASTION-BASTION",
"operationName":"Microsoft.Network/BastionHost/connect",
"category":"BastionAuditLogs",
"level":"Informational",
"location":"eastus",
"properties":{
   "userName":"<username>",
   "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90
Safari/537.36",
   "clientIpAddress":"131.107.159.86",
   "clientPort":24039,
   "protocol":"ssh",

"targetResourceId":"/SUBSCRIPTIONS/<subscripionID>/RESOURCEGROUPS/MYBAS
TION/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/LINUX-KEY",
   "subscriptionId":"<subscripionID>",
   "message":"Successfully Connected.",
   "resourceType":"VM",
   "targetVMIPAddress":"172.16.1.5",
   "userEmail":"<userAzureAccountEmailAddress>",
   "tunnelId":"<tunnelID>"
},
"FluentdIngestTimestamp":"2019-10-03T16:03:34.0000000Z",
"Region":"eastus",
"CustomerSubscriptionId":"<subscripionID>"
}
```


Below is an example entry of unsuccessful login (e.g. due to incorrect username/password) from the json file:

JSON


```
{
"time":"2019-10-03T16:03:34.776Z",
"resourceId":"/SUBSCRIPTIONS/<subscripionID>/RESOURCEGROUPS/MYBASTION/P
ROVIDERS/MICROSOFT.NETWORK/BASTIONHOSTS/MYBASTION-BASTION",
"operationName":"Microsoft.Network/BastionHost/connect",
"category":"BastionAuditLogs",
"level":"Informational",
"location":"eastus",
"properties":{
   "userName":"<username>",
   "userAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.90
Safari/537.36",
   "clientIpAddress":"131.107.159.86",
   "clientPort":24039,
   "protocol":"ssh",

"targetResourceId":"/SUBSCRIPTIONS/<subscripionID>/RESOURCEGROUPS/MYBAS
TION/PROVIDERS/MICROSOFT.COMPUTE/VIRTUALMACHINES/LINUX-KEY",
```

```
    "subscriptionId":"<subscripionID>",
    "message":"Login Failed",
    "resourceType":"VM",
    "targetVMIPAddress":"172.16.1.5",
    "userEmail":"<userAzureAccountEmailAddress>",
    "tunnelId":"<tunnelID>"
  },
  "FluentdIngestTimestamp":"2019-10-03T16:03:34.0000000Z",
  "Region":"eastus",
  "CustomerSubscriptionId":"<subscripionID>"
  }
```


Next steps

Read the Bastion FAQ.

Additional resources

Documentation

Azure Bastion session monitoring and management

Learn how to select an ongoing session and force-disconnect or delete it.

Use Azure Firewall to protect Azure Virtual Desktop

Learn how to use Azure Firewall to protect Azure Virtual Desktop deployments

Configure monitoring and metrics using Azure Monitor - Azure Bastion

Learn about Azure Bastion monitoring and metrics using Azure Monitor.

Networking for Azure Virtual Desktop - Cloud Adoption Framework

Use the Cloud Adoption Framework for Azure to identify networking capabilities that your landing zone needs to support Azure Virtual Desktop workloads.

Azure Bastion FAQ

Learn about frequently asked questions for Azure Bastion.

About Azure Bastion configuration settings

Learn about the available configuration settings for Azure Bastion.

Working with VMs and NSGs in Azure Bastion

Learn about using network security groups with Azure Bastion.

Create a shareable link for Azure Bastion

Learn how to create a shareable link to let a user connect to a target resource via Bastion without using the Azure portal.

Show 5 more

Training

Learning paths and modules

Connect to virtual machines through the Azure portal by using Azure Bastion - Training

Learn how to deploy Azure Bastion to securely connect to Azure virtual machines directly within the Azure portal.

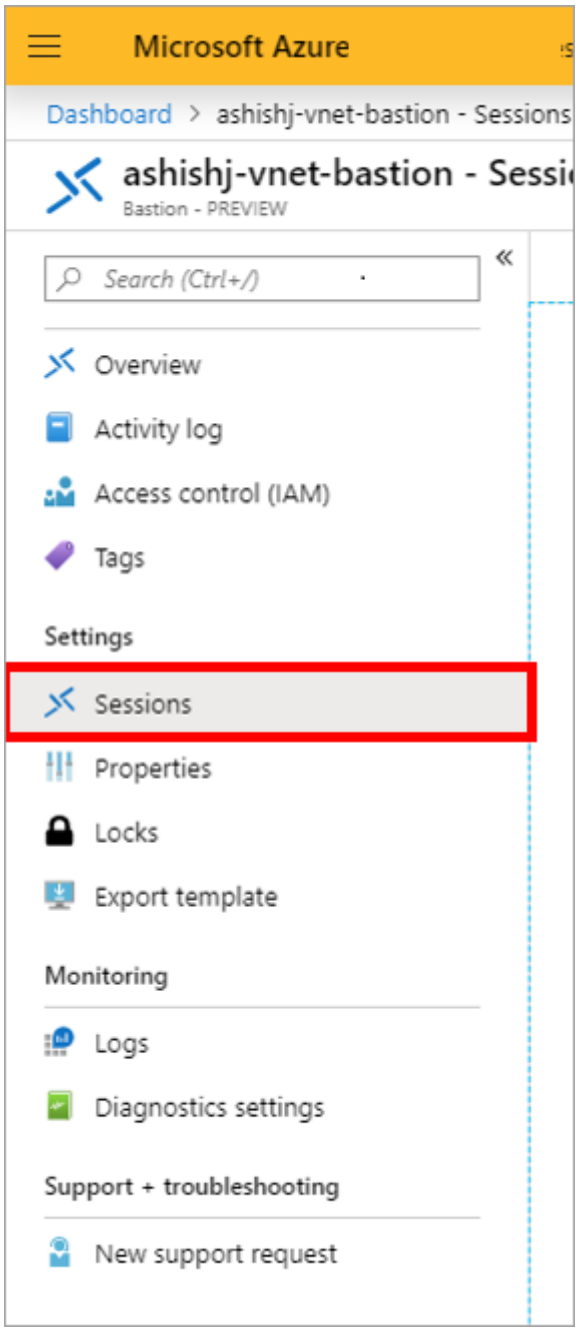
Session monitoring and management for Azure Bastion

Article • 03/03/2022 • 2 minutes to read

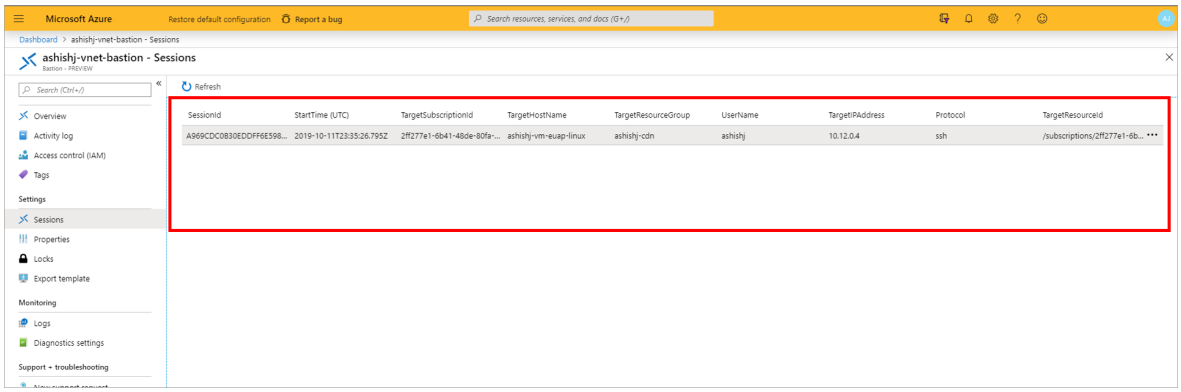
Once the Bastion service is provisioned and deployed in your virtual network, you can use it to seamlessly connect to any VM in this virtual network. As users connect to workloads, Azure Bastion can be used to monitor the remote sessions and take quick management actions. Azure Bastion session monitoring lets you view which users are connected to which VMs. It shows the IP that the user connected from, how long they have been connected, and when they connected. The session management experience lets you select an ongoing session and force-disconnect or delete a session in order to disconnect the user from the ongoing session.

Monitor remote sessions

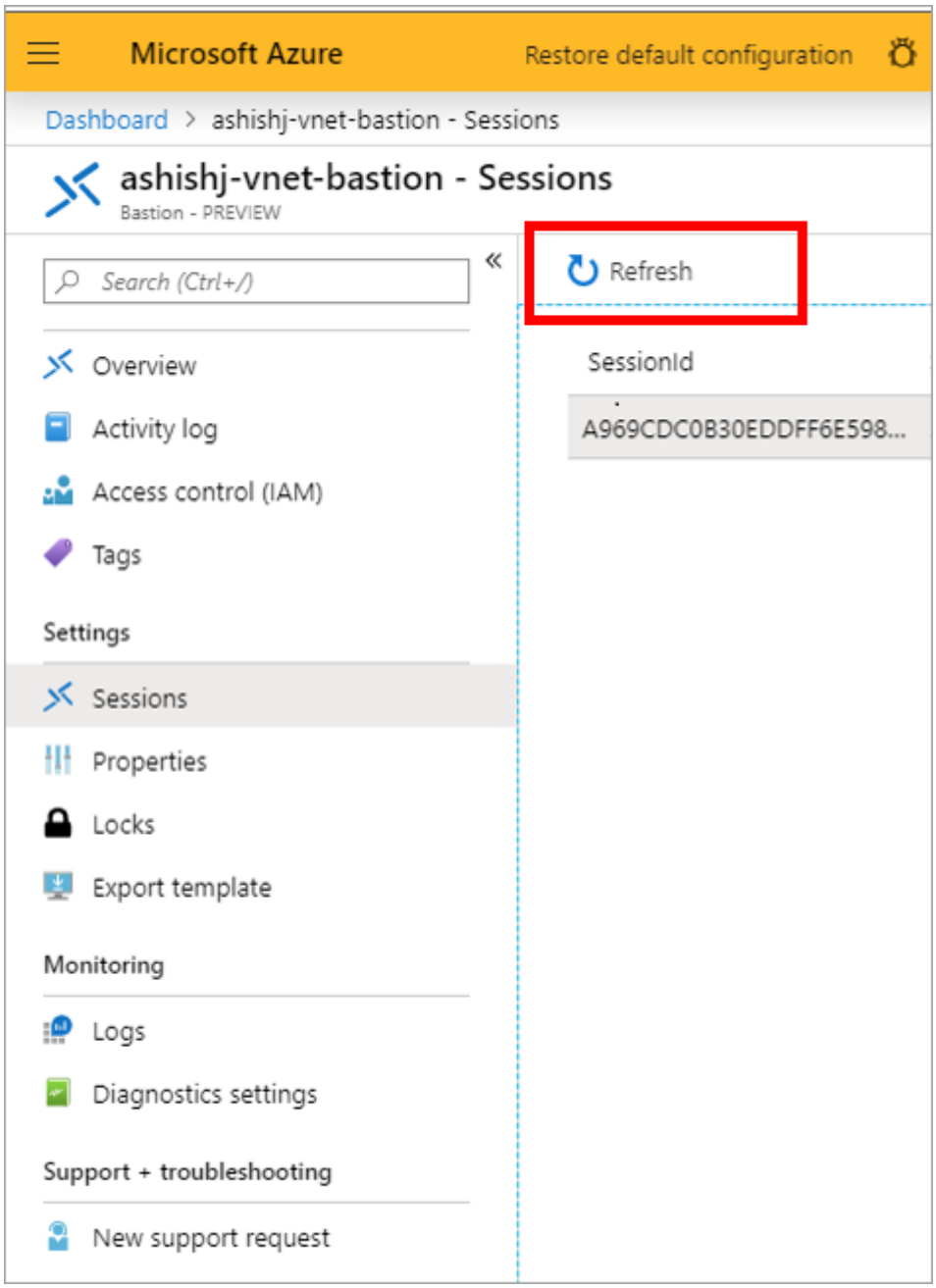
1. In the Azure portal, go to your Azure Bastion resource and select **Sessions** from the Azure Bastion page.



2. On the **Sessions** page, you can see the ongoing remote sessions on the right side.



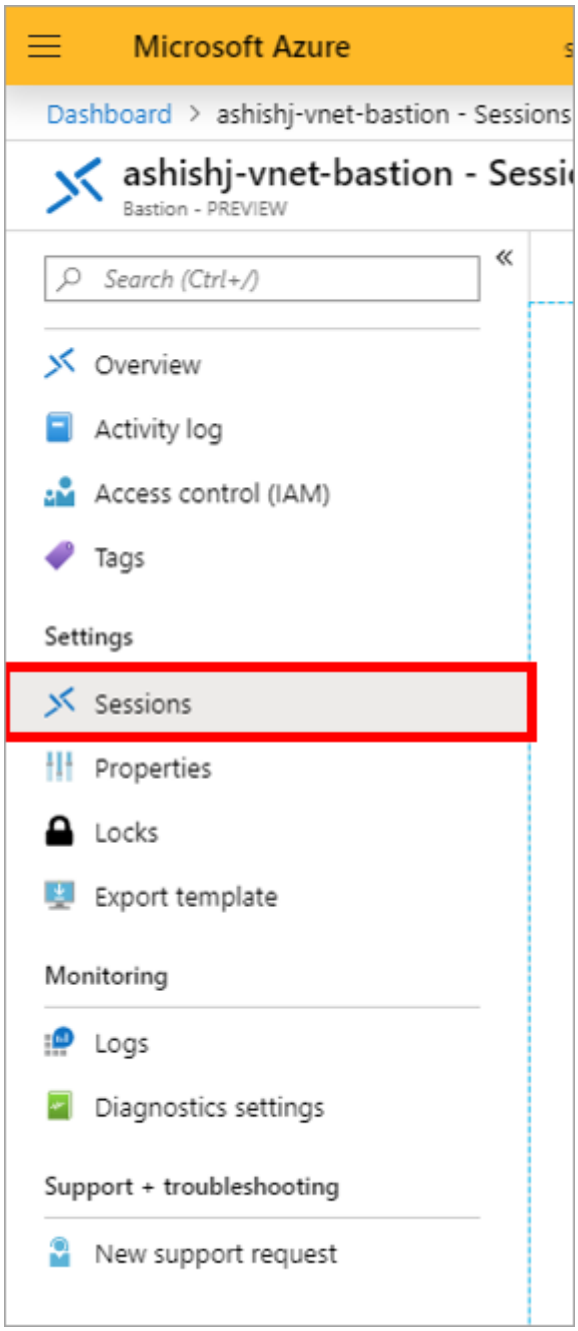
3. Select **Refresh** to see the updated list of remote sessions. When you select Refresh, Azure Bastion will fetch the latest monitoring information and refresh it in the portal.



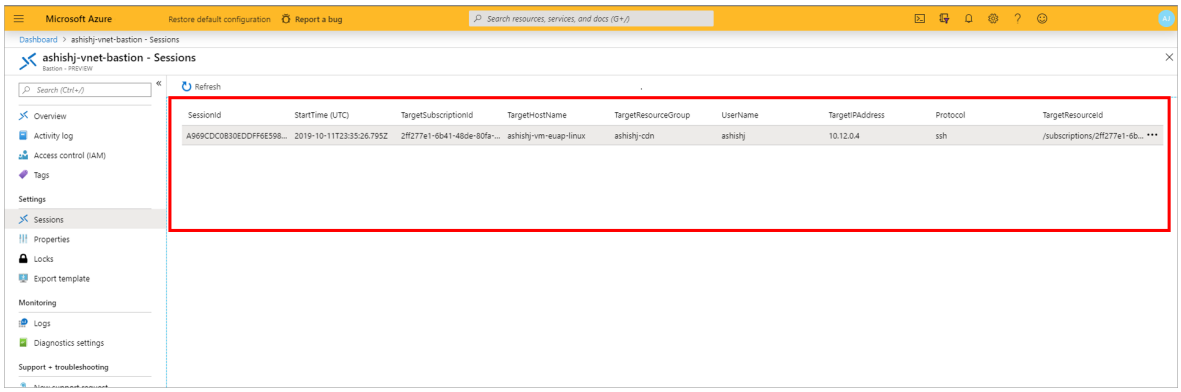
Delete or force-disconnect an ongoing remote session

You can select a set of session(s) and force-disconnect them. The following steps show you how to delete remote sessions:

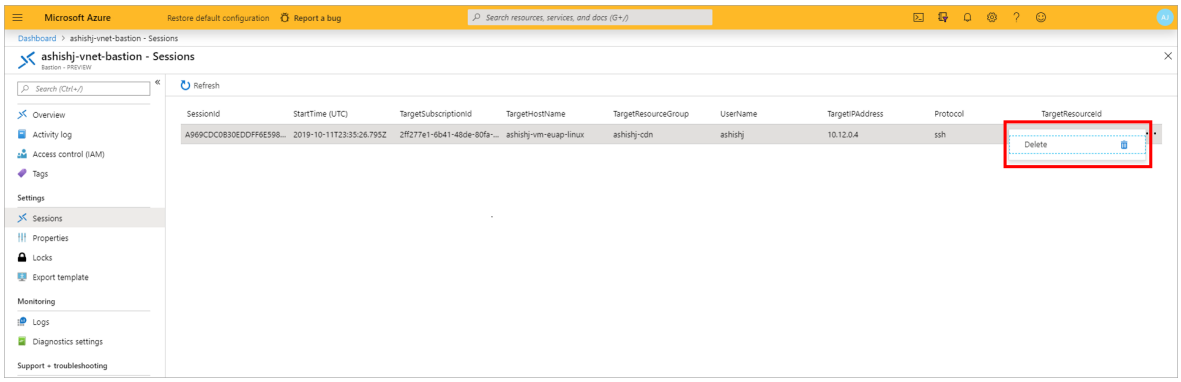
1. Navigate to your Azure Bastion resource and select **Sessions** from the Azure Bastion page.



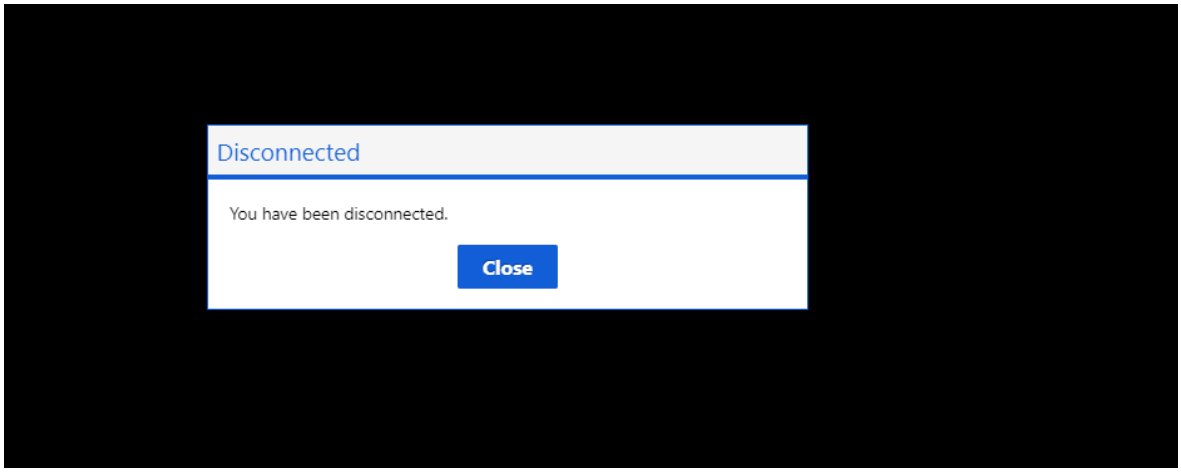
2. After you select Sessions, you see a list of remote sessions.



3. Select a specific remote session, then select the three ellipses on the right-side end of the session row, and then select **Delete**.



4. When you select Delete, the remote session will be disconnected and the user will be shown a "You have been disconnected" message in the remote session.



Next steps

Read the Bastion FAQ.

Troubleshoot Azure Bastion

Article • 09/15/2021 • 3 minutes to read

This article shows you how to troubleshoot Azure Bastion.

Unable to create an NSG on AzureBastionSubnet

Q: When I try to create an NSG on the Azure Bastion subnet, I get the following error: '*Network security group <NSG name> does not have necessary rules for Azure Bastion Subnet AzureBastionSubnet*".

A: If you create and apply an NSG to *AzureBastionSubnet*, make sure you have added the required rules to the NSG. For a list of required rules, see Working with NSG access and Azure Bastion. If you do not add these rules, the NSG creation/update will fail.

An example of the NSG rules is available for reference in the quickstart template. For more information, see NSG guidance for Azure Bastion.

Unable to use my SSH key with Azure Bastion

Q: When I try to browse my SSH key file, I get the following error: '*SSH Private key must start with -----BEGIN RSA PRIVATE KEY----- and ends with -----END RSA PRIVATE KEY-----*'.

A: Azure Bastion supports only RSA SSH keys, at this point in time. Make sure that you browse a key file that is RSA private key for SSH, with public key provisioned on the target VM.

As an example, you can use the following command to create a new RSA SSH key:

ssh-keygen -t rsa -b 4096 -C "email@domain.com"

Output:

```
ashishj@dreamcatcher:~$ ssh-keygen -t rsa -b 4096 -C "email@domain.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ashishj/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ashishj/.ssh/id_rsa.
```

```
Your public key has been saved in /home/ashishj/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:c+SBciKXnwceaNQ8Ms8C4h46BsNosYx+9d+AUxdazuE email@domain.com
The key's randomart image is:
+---[RSA 4096]----+
|      .o         |
| .. ..oo+. +     |
|=.o...B==.O o    |
|==o  =.*oO E     |
|++ .. ..S =      |
|oo..   + =       |
|...     o o      |
|         . .     |
|                 |
+----[SHA256]-----+
```

Unable to sign in to my Windows domain-joined virtual machine

Q: I am unable to connect to my Windows virtual machine that is domain-joined.

A: Azure Bastion supports domain-joined VM sign-in for username-password based domain sign-in only. When specifying the domain credentials in the Azure portal, use the UPN (username@domain) format instead of *domain\username* format to sign in. This is supported for domain-joined or hybrid-joined (both domain-joined as well as Azure AD-joined) virtual machines. It is not supported for Azure AD-joined-only virtual machines.

Unable to connect to virtual machine

Q: I am unable to connect to my virtual machine (and I'm not experiencing the problems above).

A: You can troubleshoot your connectivity issues by navigating to the **Connection Troubleshoot** tab (in the **Monitoring** section) of your Azure Bastion resource in the Azure portal. Network Watcher Connection Troubleshoot provides the capability to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IPv4 address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Check". Learn more.

File transfer issues

Q: Is file transfer supported with Azure Bastion?

A: File transfer is not supported at this time. We are working on adding support.

Black screen in the Azure portal

Q: When I try to connect using Azure Bastion, I can't connect to the target VM and I get a black screen in the Azure portal.

A: This happens when there is either a network connectivity issue between your web browser and Azure Bastion (your client Internet firewall may be blocking WebSockets traffic or similar), or between the Azure Bastion and your target VM. Most cases include an NSG applied either to AzureBastionSubnet, or on your target VM subnet that is blocking the RDP/SSH traffic in your virtual network. Allow WebSockets traffic on your client internet firewall, and check the NSGs on your target VM subnet.

Next steps

For more information, see the Bastion FAQ.

Az.Network

Reference

In this article

Application Gateway
DNS
ExpressRoute
Load Balancer
Network Watcher
Networking
Route
Virtual Network
VPN

This topic displays help topics for the Azure Network Cmdlets.

Application Gateway

Add-AzApplicationGatewayAuthenticationCertificate	Adds an authentication certificate to an application gateway.
Add-AzApplicationGatewayBackendAddressPool	Adds a back-end address pool to an application gateway.
Add-AzApplicationGatewayBackendHttpSetting	Adds back-end HTTP settings to an application gateway.
Add-AzApplicationGatewayBackendSetting	Adds back-end TCP\TLS settings to an application gateway.
Add-AzApplicationGatewayCustomError	Adds a custom error to an application gateway.
Add-AzApplicationGatewayFrontendIPConfig	Adds a front-end IP configuration to an application gateway.
Add-AzApplicationGatewayFrontendPort	Adds a front-end port to an application gateway.
Add-AzApplicationGatewayHttpListener	Adds an HTTP listener to an application gateway.
Add-AzApplicationGatewayHttpListenerCustomError	Adds a custom error to a http listener of an application gateway.
Add-AzApplicationGatewayIPConfiguration	Adds an IP configuration to an application gateway.
Add-AzApplicationGatewayListener	Adds an listener to an application gateway.
Add-AzApplicationGatewayPrivateLinkConfiguration	Adds a private link configuration to an application gateway.
Add-AzApplicationGatewayProbeConfig	Adds a health probe to an Application Gateway.
Add-AzApplicationGatewayRedirectConfiguration	Adds a redirect configuration to an Application Gateway.

Add-AzApplicationGatewayRequestRoutingRule	Adds a request routing rule to an application gateway.
Add-AzApplicationGatewayRewriteRuleSet	Adds a rewrite rule set to an application gateway.
Add-AzApplicationGatewayRoutingRule	Adds a routing rule to an application gateway.
Add-AzApplicationGatewaySslCertificate	Adds an SSL certificate to an application gateway.
Add-AzApplicationGatewaySslProfile	Adds SSL profile to an application gateway.
Add-AzApplicationGatewayTrustedClientCertificate	Adds a trusted client CA certificate chain to an application gateway.
Add-AzApplicationGatewayTrustedRootCertificate	Adds a trusted root certificate to an application gateway.
Add-AzApplicationGatewayUrlPathMapConfig	Adds an array of URL path mappings to a backend server pool.
Get-AzApplicationGateway	Gets an application gateway.
Get-AzApplicationGatewayAuthenticationCertificate	Gets an authentication certificate for an application gateway.
Get-AzApplicationGatewayAutoscaleConfiguration	Gets the Autoscale Configuration of the Application Gateway.
Get-AzApplicationGatewayAvailableServerVariableAndHeader	Get the supported server variables and available request and response headers.
Get-AzApplicationGatewayAvailableSslOption	Gets all available ssl options for ssl policy for Application Gateway.
Get-AzApplicationGatewayAvailableWafRuleSet	Gets all available web application firewall rule sets.
Get-AzApplicationGatewayBackendAddressPool	Gets a back-end address pool for an application gateway.
Get-AzApplicationGatewayBackendHealth	Gets application gateway backend health.
Get-AzApplicationGatewayBackendHttpSetting	Gets the back-end HTTP settings of an application gateway.
Get-AzApplicationGatewayBackendSetting	Gets the back-end TCP\TLS settings of an application gateway.
Get-AzApplicationGatewayClientAuthConfiguration	Gets the client authentication configuration of a SSL profile object.
Get-AzApplicationGatewayConnectionDraining	Gets the connection draining configuration of a back-end HTTP settings object.
Get-AzApplicationGatewayCustomError	Gets custom error(s) from an application gateway.
Get-AzApplicationGatewayFirewallPolicy	Gets an application gateway firewall policy.
Get-AzApplicationGatewayFrontendIPConfig	Gets the front-end IP configuration of an application gateway.
Get-AzApplicationGatewayFrontendPort	Gets the front-end port of an application gateway.

Get-AzApplicationGatewayHttpListener	Gets the HTTP listener of an application gateway.
Get-AzApplicationGatewayHttpListenerCustomError	Gets custom error(s) from a http listener of an application gateway.
Get-AzApplicationGatewayIdentity	Get identity assigned to the application gateway.
Get-AzApplicationGatewayIPConfiguration	Gets the IP configuration of an application gateway.
Get-AzApplicationGatewayListener	Gets the TCP\TLS listener of an application gateway.
Get-AzApplicationGatewayPrivateLinkConfiguration	Gets the private link configuration of an application gateway.
Get-AzApplicationGatewayProbeConfig	Gets an existing health probe configuration from an Application Gateway.
Get-AzApplicationGatewayRedirectConfiguration	Gets an existing redirect configuration from an Application Gateway.
Get-AzApplicationGatewayRequestRoutingRule	Gets the request routing rule of an application gateway.
Get-AzApplicationGatewayRewriteRuleSet	Gets the rewrite rule set of an application gateway.
Get-AzApplicationGatewayRoutingRule	Gets the routing rule of an application gateway.
Get-AzApplicationGatewaySku	Gets the SKU of an application gateway.
Get-AzApplicationGatewaySslCertificate	Gets an SSL certificate for an application gateway.
Get-AzApplicationGatewaySslPolicy	Gets the SSL policy of an application gateway.
Get-AzApplicationGatewaySslPredefinedPolicy	Gets Predefined SSL Policies provided by Application Gateway.
Get-AzApplicationGatewaySslProfile	Gets the SSL profile of an application gateway.
Get-AzApplicationGatewaySslProfilePolicy	Gets the SSL policy of an application gateway SSL profile.
Get-AzApplicationGatewayTrustedClientCertificate	Gets the trusted client CA certificate chain with a specific name from the Application Gateway.
Get-AzApplicationGatewayTrustedRootCertificate	Gets the Trusted Root Certificate with a specific name from the Application Gateway.
Get-AzApplicationGatewayUrlPathMapConfig	Gets an array of URL path mappings to a backend server pool.
Get-AzApplicationGatewayWafDynamicManifest	Gets the web application firewall manifest and all the supported rule sets.
Get-AzApplicationGatewayWebApplicationFirewallConfiguration	Gets the WAF configuration of an application gateway.
New-AzApplicationGateway	Creates an application gateway.
New-AzApplicationGatewayAuthenticationCertificate	Creates an authentication certificate for an application gateway.

New-AzApplicationGatewayAutoscaleConfiguration	Creates a Autoscale Configuration for the Application Gateway.
New-AzApplicationGatewayBackendAddressPool	Creates a back-end address pool for an application gateway.
New-AzApplicationGatewayBackendHttpSetting	Creates back-end HTTP setting for an application gateway.
New-AzApplicationGatewayBackendSetting	Creates back-end TCP\TLS setting for an application gateway.
New-AzApplicationGatewayClientAuthConfiguration	Creates a new client authentication configuration for SSL profile.
New-AzApplicationGatewayConnectionDraining	Creates a new connection draining configuration for back-end HTTP settings.
New-AzApplicationGatewayCustomError	Creates a custom error with http status code and custom error page url
New-AzApplicationGatewayFirewallCondition	Creates a match condition for custom rule
New-AzApplicationGatewayFirewallCustomRule	Creates a new custom rule for the application gateway firewall policy.
New-AzApplicationGatewayFirewallDisabledRuleGroupConfig	Creates a new disabled rule group configuration.
New-AzApplicationGatewayFirewallExclusionConfig	Creates a new exclusion rule list for application gateway waf
New-AzApplicationGatewayFirewallMatchVariable	Creates a match variable for firewall condition.
New-AzApplicationGatewayFirewallPolicy	Creates a application gateway firewall policy.
New-AzApplicationGatewayFirewallPolicyExclusion	Creates an exclusion on the Firewall Policy
New-AzApplicationGatewayFirewallPolicyExclusionManagedRule	Creates an exclusionManagedRule entry for ExclusionManagedRuleGroup entry.
New-AzApplicationGatewayFirewallPolicyExclusionManagedRuleGroup	Creates ExclusionManagedRuleGroup entry in ExclusionManagedRuleSets for the firewall policy exclusion.
New-AzApplicationGatewayFirewallPolicyExclusionManagedRuleSet	Creates an ExclusionManagedRuleSet for the firewallPolicy exclusion
New-AzApplicationGatewayFirewallPolicyManagedRule	Create ManagedRules for the firewall policy.
New-AzApplicationGatewayFirewallPolicyManagedRuleGroupOverride	Creates RuleGroupOverride entry in ManagedRuleSets for the firewall policy.
New-AzApplicationGatewayFirewallPolicyManagedRuleOverride	Creates a managedRuleOverride entry for RuleGroupOverrideGroup entry.
New-AzApplicationGatewayFirewallPolicyManagedRuleSet	Creates a ManagedRuleSet for the firewallPolicy
New-AzApplicationGatewayFirewallPolicySetting	Creates a policy setting for the firewall policy
New-AzApplicationGatewayFrontendIPConfig	Creates a front-end IP configuration for an application gateway.
New-AzApplicationGatewayFrontendPort	Creates a front-end port for an application

	gateway.
New-AzApplicationGatewayHttpListener	Creates an HTTP listener for an application gateway.
New-AzApplicationGatewayIdentity	Creates an identity object for an application gateway. This will hold reference to the user assigned identity.
New-AzApplicationGatewayIPConfiguration	Creates an IP configuration for an application gateway.
New-AzApplicationGatewayListener	Creates an TCP\TLS listener for an application gateway.
New-AzApplicationGatewayPathRuleConfig	Creates an application gateway path rule.
New-AzApplicationGatewayPrivateLinkConfiguration	Creates a private link configuration for an application gateway
New-AzApplicationGatewayPrivateLinkIpConfiguration	Creates an Ip Configuration to be associated with PrivateLink Configuration
New-AzApplicationGatewayProbeConfig	Creates a health probe.
New-AzApplicationGatewayProbeHealthResponseMatch	Creates a health probe response match used by Health Probe for an application gateway.
New-AzApplicationGatewayRedirectConfiguration	Creates a redirect configuration for an application gateway.
New-AzApplicationGatewayRequestRoutingRule	Creates a request routing rule for an application gateway.
New-AzApplicationGatewayRewriteRule	Creates a rewrite rule for an application gateway.
New-AzApplicationGatewayRewriteRuleActionSet	Creates a rewrite rule action set for an application gateway.
New-AzApplicationGatewayRewriteRuleCondition	Adds a condition to the RewriteRule for an application gateway.
New-AzApplicationGatewayRewriteRuleHeaderConfiguration	Creates a rewrite rule header configuration for an application gateway.
New-AzApplicationGatewayRewriteRuleSet	Creates a rewrite rule set for an application gateway.
New-AzApplicationGatewayRewriteRuleUrlConfiguration	Creates a rewrite rule url configuration for an application gateway.
New-AzApplicationGatewayRoutingRule	Creates a routing rule for an application gateway.
New-AzApplicationGatewaySku	Creates a SKU for an application gateway.
New-AzApplicationGatewaySslCertificate	Creates an SSL certificate for an Azure application gateway.
New-AzApplicationGatewaySslPolicy	Creates an SSL policy for an application gateway.
New-AzApplicationGatewaySslProfile	Creates SSL profile for an application gateway.
New-AzApplicationGatewayTrustedClientCertificate	Creates a trusted client CA certificate chain for an

	application gateway.
New-AzApplicationGatewayTrustedRootCertificate	Creates a Trusted Root Certificate for an application gateway.
New-AzApplicationGatewayUrlPathMapConfig	Creates an array of URL path mappings to a backend server pool.
New-AzApplicationGatewayWebApplicationFirewallConfiguration	Creates a WAF configuration for an application gateway.
Remove-AzApplicationGateway	Removes an application gateway.
Remove-AzApplicationGatewayAuthenticationCertificate	Removes an authentication certificate from an application gateway.
Remove-AzApplicationGatewayAutoscaleConfiguration	Removes Autoscale Configuration from an application gateway.
Remove-AzApplicationGatewayBackendAddressPool	Removes a back-end address pool from an application gateway.
Remove-AzApplicationGatewayBackendHttpSetting	Removes back-end HTTP settings from an application gateway.
Remove-AzApplicationGatewayBackendSetting	Removes back-end TCP\TLS settings from an application gateway.
Remove-AzApplicationGatewayClientAuthConfiguration	Removes the client authentication configuration of a SSL profile object.
Remove-AzApplicationGatewayConnectionDraining	Removes the connection draining configuration of a back-end HTTP settings object.
Remove-AzApplicationGatewayCustomError	Removes a custom error from an application gateway.
Remove-AzApplicationGatewayFirewallPolicy	Removes an application gateway firewall policy.
Remove-AzApplicationGatewayFrontendIPConfig	Removes a front-end IP configuration from an application gateway.
Remove-AzApplicationGatewayFrontendPort	Removes a front-end port from an application gateway.
Remove-AzApplicationGatewayHttpListener	Removes an HTTP listener from an application gateway.
Remove-AzApplicationGatewayHttpListenerCustomError	Removes a custom error from a http listener of an application gateway.
Remove-AzApplicationGatewayIdentity	Removes a identity from an application gateway.
Remove-AzApplicationGatewayIPConfiguration	Removes an IP configuration from an application gateway.
Remove-AzApplicationGatewayListener	Removes a TCP\TLS listener from an application gateway.
Remove-AzApplicationGatewayPrivateLinkConfiguration	Removes a privateLink configuration from an application gateway.

Remove-AzApplicationGatewayProbeConfig	Removes a health probe from an existing application gateway.
Remove-AzApplicationGatewayRedirectConfiguration	Removes a redirect configuration from an existing Application Gateway.
Remove-AzApplicationGatewayRequestRoutingRule	Removes a request routing rule from an application gateway.
Remove-AzApplicationGatewayRewriteRuleSet	Removes a rewrite rule set from an application gateway.
Remove-AzApplicationGatewayRoutingRule	Removes a routing rule from an application gateway.
Remove-AzApplicationGatewaySslCertificate	Removes an SSL certificate from an Azure application gateway.
Remove-AzApplicationGatewaySslPolicy	Removes an SSL policy from an Azure application gateway.
Remove-AzApplicationGatewaySslProfile	Removes the ssl profile from an application gateway.
Remove-AzApplicationGatewaySslProfilePolicy	Removes an SSL policy from an Azure application gateway SSL profile.
Remove-AzApplicationGatewayTrustedClientCertificate	Removes the trusted client CA certificate chain object from an application gateway.
Remove-AzApplicationGatewayTrustedRootCertificate	Removes a Trusted Root Certificate from an application gateway.
Remove-AzApplicationGatewayUrlPathMapConfig	Removes URL path mappings to a backend server pool.
Set-AzApplicationGateway	Updates an application gateway.
Set-AzApplicationGatewayAuthenticationCertificate	Updates an authentication certificate for an application gateway.
Set-AzApplicationGatewayAutoscaleConfiguration	Updates Autoscale Configuration of an application gateway.
Set-AzApplicationGatewayBackendAddressPool	Updates a back-end address pool for an application gateway.
Set-AzApplicationGatewayBackendHttpSetting	Updates back-end HTTP settings for an application gateway.
Set-AzApplicationGatewayBackendSetting	Updates back-end TCP\TLS settings for an application gateway.
Set-AzApplicationGatewayClientAuthConfiguration	Modifies the client auth configuration of a ssl profile object.
Set-AzApplicationGatewayConnectionDraining	Modifies the connection draining configuration of a back-end HTTP settings object.
Set-AzApplicationGatewayCustomError	Updates a custom error in an application gateway.
Set-AzApplicationGatewayFirewallPolicy	Updates an application gateway firewall policy.

Set-AzApplicationGatewayFrontendIPConfig	Modifies a front-end IP address configuration.
Set-AzApplicationGatewayFrontendPort	Modifies a front-end port for an application gateway.
Set-AzApplicationGatewayHttpListener	Modifies an HTTP listener for an application gateway.
Set-AzApplicationGatewayHttpListenerCustomError	Updates a custom error in a http listener of an application gateway.
Set-AzApplicationGatewayIdentity	Updates a identity assigned to the application gateway.
Set-AzApplicationGatewayIPConfiguration	Modifies an IP configuration for an application gateway.
Set-AzApplicationGatewayListener	Modifies a TCP\TLS listener for an application gateway.
Set-AzApplicationGatewayPrivateLinkConfiguration	Modifies an PrivateLink Configuration for an application gateway.
Set-AzApplicationGatewayProbeConfig	Sets the health probe configuration on an existing Application Gateway.
Set-AzApplicationGatewayRedirectConfiguration	Sets the redirect configuration on an existing Application Gateway.
Set-AzApplicationGatewayRequestRoutingRule	Modifies a request routing rule for an application gateway.
Set-AzApplicationGatewayRewriteRuleSet	Modifies a rewrite rule set for an application gateway.
Set-AzApplicationGatewayRoutingRule	Modifies a routing rule for an application gateway.
Set-AzApplicationGatewaySku	Modifies the SKU of an application gateway.
Set-AzApplicationGatewaySslCertificate	Updates an SSL certificate for an application gateway.
Set-AzApplicationGatewaySslPolicy	Modifies the SSL policy of an application gateway.
Set-AzApplicationGatewaySslProfile	Updates ssl profile for an application gateway.
Set-AzApplicationGatewaySslProfilePolicy	Modifies the SSL policy of an application gateway SSL profile.
Set-AzApplicationGatewayTrustedClientCertificate	Modifies the trusted client CA certificate chain of an application gateway.
Set-AzApplicationGatewayTrustedRootCertificate	Updates a Trusted Root Certificate of an application gateway.
Set-AzApplicationGatewayUrlPathMapConfig	Sets configuration for an array of URL path mappings to a backend server pool.
Set-AzApplicationGatewayWebApplicationFirewallConfiguration	Modifies the WAF configuration of an application gateway.
Start-AzApplicationGateway	Starts an application gateway.

Stop-AzApplicationGateway	Stops an application gateway

DNS

Get-AzPrivateDnsZoneGroup	Gets private DNS zone group
New-AzFirewallPolicyDnsSetting	Creates a new DNS Setting for Azure Firewall Policy
New-AzPrivateDnsZoneConfig	Creates DNS zone configuration of the private dns zone group.
New-AzPrivateDnsZoneGroup	Creates a private DNS zone group in the specified private endpoint.
Remove-AzPrivateDnsZoneGroup	Removes a DNS zone group.
Set-AzPrivateDnsZoneGroup	Updates DNS zone group
Test-AzDnsAvailability	Checks whether a domain name in the cloudapp.azure.com zone is available for use.

ExpressRoute

Add-AzExpressRouteCircuitAuthorization	Adds an ExpressRoute circuit authorization.
Add-AzExpressRouteCircuitConnectionConfig	Adds a circuit connection configuration to Private Peering of an Express Route Circuit.
Add-AzExpressRouteCircuitPeeringConfig	Adds a peering configuration to an ExpressRoute circuit.
Add-AzExpressRouteCrossConnectionPeering	Adds a peering configuration to an ExpressRoute cross connection.
Add-AzExpressRoutePortAuthorization	Adds an ExpressRoutePort authorization.
Get-AzExpressRouteCircuit	Gets an Azure ExpressRoute circuit from Azure.
Get-AzExpressRouteCircuitARPTable	Gets the ARP table from an ExpressRoute circuit.
Get-AzExpressRouteCircuitAuthorization	Gets information about ExpressRoute circuit authorizations.
Get-AzExpressRouteCircuitConnectionConfig	Gets an ExpressRoute circuit connection configuration associated with Private Peering of ExpressRouteCircuit.
Get-AzExpressRouteCircuitPeeringConfig	Gets an ExpressRoute circuit peering configuration.
Get-AzExpressRouteCircuitRouteTable	Gets a route table from an ExpressRoute circuit.
Get-AzExpressRouteCircuitRouteTableSummary	Gets a route table summary of an ExpressRoute circuit.
Get-AzExpressRouteCircuitStat	Gets usage statistics of an ExpressRoute circuit.
Get-AzExpressRouteConnection	Gets a ExpressRoute connection by name or lists all ExpressRoute connections connected to a ExpressRouteGateway.
Get-AzExpressRouteCrossConnection	Gets an Azure ExpressRoute cross connection from Azure.
Get-AzExpressRouteCrossConnectionArpTable	Gets the ARP table from an ExpressRoute cross connection.

Get-AzExpressRouteCrossConnectionPeering	Gets an ExpressRoute cross connection peering configuration.
Get-AzExpressRouteCrossConnectionRouteTable	Gets a route table from an ExpressRoute cross connection.
Get-AzExpressRouteCrossConnectionRouteTableSummary	Gets a route table summary of an ExpressRoute cross connection.
Get-AzExpressRouteGateway	Gets a ExpressRouteGateway resource using ResourceGroupName and GatewayName OR lists all gateways by ResourceGroupName or SubscriptionId.
Get-AzExpressRoutePort	Gets an Azure ExpressRoutePort resource.
Get-AzExpressRoutePortAuthorization	Gets information about ExpressRoutePort authorizations.
Get-AzExpressRoutePortIdentity	Get identity assigned to an ExpressRoutePort.
Get-AzExpressRoutePortLinkConfig	Gets an ExpressRoutePort link configuration.
Get-AzExpressRoutePortsLocation	Gets the locations at which ExpressRoutePort resources are available.
Get-AzExpressRouteServiceProvider	Gets a list ExpressRoute service providers and their attributes.
Move-AzExpressRouteCircuit	Moves an ExpressRoute circuit from the classic deployment model to the Resource Manager deployment model.
New-AzExpressRouteCircuit	Creates an Azure express route circuit.
New-AzExpressRouteCircuitAuthorization	Creates an ExpressRoute circuit authorization.
New-AzExpressRouteCircuitPeeringConfig	Creates a new peering configuration to be added to an ExpressRoute circuit.
New-AzExpressRouteConnection	Creates an ExpressRoute connection that connects an ExpressRoute gateway to an on premise ExpressRoute circuit
New-AzExpressRouteGateway	Creates a Scalable ExpressRoute Gateway.
New-AzExpressRoutePort	Creates an Azure ExpressRoutePort.
New-AzExpressRoutePortIdentity	Creates an Azure ExpressRoutePortIdentity.
New-AzExpressRoutePortLOA	Download letter of authorization document for an express route port.
Remove-AzExpressRouteCircuit	Removes an ExpressRoute circuit.
Remove-AzExpressRouteCircuitAuthorization	Removes an existing ExpressRoute configuration authorization.
Remove-AzExpressRouteCircuitConnectionConfig	Removes an ExpressRoute circuit connection configuration.
Remove-AzExpressRouteCircuitPeeringConfig	Removes an ExpressRoute circuit peering configuration.
Remove-AzExpressRouteConnection	Removes a ExpressRouteConnection.
Remove-AzExpressRouteCrossConnectionPeering	Removes an ExpressRoute cross connection peering configuration.
Remove-AzExpressRouteGateway	The Remove-AzExpressRouteGateway cmdlet removes an Azure ExpressRoute gateway. This is a gateway specific to Azure Virtual WAN's software defined connectivity.

Remove-AzExpressRoutePort	Removes an ExpressRoutePort.
Remove-AzExpressRoutePortAuthorization	Removes an existing ExpressRoutePort authorization.
Remove-AzExpressRoutePortIdentity	Removes a identity from an ExpressRoutePort.
Set-AzExpressRouteCircuit	Modifies an ExpressRoute circuit.
Set-AzExpressRouteCircuitConnectionConfig	Updates a circuit connection configuration created in Private Peerings for an Express Route Circuit.
Set-AzExpressRouteCircuitPeeringConfig	Saves a modified ExpressRoute peering configuration.
Set-AzExpressRouteConnection	Updates an express route connection created between an express route gateway and on-premise express route circuit peering.
Set-AzExpressRouteCrossConnection	Modifies an ExpressRoute cross connection.
Set-AzExpressRouteGateway	Updates a Scalable ExpressRoute Gateway.
Set-AzExpressRoutePort	Modifies an ExpressRoutePort.
Set-AzExpressRoutePortIdentity	Updates a identity assigned to an ExpressRoutePort.

Load Balancer

Add-AzLoadBalancerBackendAddressPoolConfig	Adds a backend address pool configuration to a load balancer.
Add-AzLoadBalancerFrontendIpConfig	Adds a front-end IP configuration to a load balancer.
Add-AzLoadBalancerInboundNatPoolConfig	Adds an inbound NAT pool to a load balancer.
Add-AzLoadBalancerInboundNatRuleConfig	Adds an inbound NAT rule configuration to a load balancer.
Add-AzLoadBalancerOutboundRuleConfig	Adds an outbound rule configuration to a load balancer.
Add-AzLoadBalancerProbeConfig	Adds a probe configuration to a load balancer.
Add-AzLoadBalancerRuleConfig	Adds a rule configuration to a load balancer.
Get-AzLoadBalancer	Gets a load balancer.
Get-AzLoadBalancerBackendAddressInboundNatRulePortMapping	Get-AzLoadBalancerBackendAddressInboundNatRulePortMapping retrieves inbound nat rule port mapping list for one backend address.
Get-AzLoadBalancerBackendAddressPool	Get-AzLoadBalancerBackendAddressPool retrieves one or more backend address pools associated with a load balancer.
Get-AzLoadBalancerBackendAddressPoolConfig	Gets a backend address pool configuration for a load balancer.
Get-AzLoadBalancerFrontendIpConfig	Gets a front-end IP configuration in a load balancer.
Get-AzLoadBalancerInboundNatPoolConfig	Gets one or more inbound NAT pool configurations from a load balancer.
Get-AzLoadBalancerInboundNatRuleConfig	Gets an inbound NAT rule configuration for a load balancer.

Get-AzLoadBalancerOutboundRuleConfig	Gets an outbound rule configuration in a load balancer.
Get-AzLoadBalancerProbeConfig	Gets a probe configuration for a load balancer.
Get-AzLoadBalancerRuleConfig	Gets the rule configuration for a load balancer.
New-AzLoadBalancer	Creates a load balancer.
New-AzLoadBalancerBackendAddressConfig	Returns a load balancer backend address config.
New-AzLoadBalancerBackendAddressPool	Creates a backend address pool on a loadbalancer.
New-AzLoadBalancerBackendAddressPoolConfig	Creates a backend address pool configuration for a load balancer.
New-AzLoadBalancerBackendAddressPoolTunnelInterfaceConfig	Creates a tunnel interface in a backend address pool of a load balancer.
New-AzLoadBalancerFrontendIpConfig	Creates a front-end IP configuration for a load balancer.
New-AzLoadBalancerInboundNatPoolConfig	Creates an inbound NAT pool configuration for a load balancer.
New-AzLoadBalancerInboundNatRuleConfig	Creates an inbound NAT rule configuration for a load balancer.
New-AzLoadBalancerOutboundRuleConfig	Creates an outbound rule configuration for a load balancer.
New-AzLoadBalancerProbeConfig	Creates a probe configuration for a load balancer.
New-AzLoadBalancerRuleConfig	Creates a rule configuration for a load balancer.
Remove-AzLoadBalancer	Removes a load balancer.
Remove-AzLoadBalancerBackendAddressPool	Removes a backend pool from a load balancer
Remove-AzLoadBalancerBackendAddressPoolConfig	Removes a backend address pool configuration from a load balancer.
Remove-AzLoadBalancerFrontendIpConfig	Removes a front-end IP configuration from a load balancer.
Remove-AzLoadBalancerInboundNatPoolConfig	Removes an inbound NAT pool configuration from a load balancer.
Remove-AzLoadBalancerInboundNatRuleConfig	Removes an inbound NAT rule configuration from a load balancer.
Remove-AzLoadBalancerOutboundRuleConfig	Removes an outbound rule configuration from a load balancer.
Remove-AzLoadBalancerProbeConfig	Removes a probe configuration from a load balancer.
Remove-AzLoadBalancerRuleConfig	Removes a rule configuration for a load balancer.
Set-AzLoadBalancer	Updates a load balancer.
Set-AzLoadBalancerBackendAddressPool	Updates the backend pool on a loadbalancer
Set-AzLoadBalancerFrontendIpConfig	Updates a front-end IP configuration for a load balancer.
Set-AzLoadBalancerInboundNatPoolConfig	Sets an inbound NAT pool configuration for a load balancer.
Set-AzLoadBalancerInboundNatRuleConfig	Sets an inbound NAT rule configuration for a load balancer.

Set-AzLoadBalancerOutboundRuleConfig	Sets an outbound rule configuration for a load balancer.
Set-AzLoadBalancerProbeConfig	Updates a probe configuration for a load balancer.
Set-AzLoadBalancerRuleConfig	Updates a rule configuration for a load balancer.

Network Watcher

Get-AzNetworkWatcher	Gets the properties of a Network Watcher
Get-AzNetworkWatcherConnectionMonitor	Returns connection monitor with specified name or the list of connection monitors
Get-AzNetworkWatcherConnectionMonitorReport	Query a snapshot of the most recent connection states.
Get-AzNetworkWatcherFlowLog	Gets a flow log resource or a list of flow log resources in the specified subscription and region.
Get-AzNetworkWatcherFlowLogStatus	Gets the status of flow logging on a resource.
Get-AzNetworkWatcherNextHop	Gets the next hop from a VM.
Get-AzNetworkWatcherPacketCapture	Gets information and properties and status of a packet capture resource.
Get-AzNetworkWatcherReachabilityProvidersList	Lists all available internet service providers for a specified Azure region.
Get-AzNetworkWatcherReachabilityReport	Gets the relative latency score for internet service providers from a specified location to Azure regions.
Get-AzNetworkWatcherSecurityGroupView	View the configured and effective network security group rules applied on a VM.
Get-AzNetworkWatcherTopology	Gets a network level view of resources and their relationships in a resource group.
Get-AzNetworkWatcherTroubleshootingResult	Gets the troubleshooting result from the previously run or currently running troubleshooting operation.
Invoke-AzNetworkWatcherNetworkConfigurationDiagnostic	Invoke network configuration diagnostic session for specified network profiles on target resource.
New-AzNetworkWatcher	Creates a new Network Watcher resource.
New-AzNetworkWatcherConnectionMonitor	Creates a connection monitor resource.
New-AzNetworkWatcherConnectionMonitorEndpointObject	Creates connection monitor endpoint.
New-AzNetworkWatcherConnectionMonitorEndpointScopeItemObject	Creates a connection monitor endpoint scope item.
New-AzNetworkWatcherConnectionMonitorObject	Create a connection monitor V2 object.

New-AzNetworkWatcherConnectionMonitorOutputObject	Create connection monitor output destination object.
New-AzNetworkWatcherConnectionMonitorProtocolConfigurationObject	Create protocol configuration used to perform test evaluation over TCP, HTTP or ICMP.
New-AzNetworkWatcherConnectionMonitorTestConfigurationObject	Create a connection monitor test configuration.
New-AzNetworkWatcherConnectionMonitorTestGroupObject	Create a connection monitor test group.
New-AzNetworkWatcherFlowLog	Create or update a flow log resource for the specified network security group.
New-AzNetworkWatcherNetworkConfigurationDiagnosticProfile	Creates a new network configuration diagnostic profile object. This object is used to restrict the network configuration during a diagnostic session using the specified criteria.
New-AzNetworkWatcherPacketCapture	Creates a new packet capture resource and starts a packet capture session on a VM.
New-AzNetworkWatcherPacketCaptureV2	V2 Version of Packet Capture Cmdlet which creates a new packet capture resource and starts a packet capture session on a VM, VMSS or few instances of VMSS.
New-AzNetworkWatcherProtocolConfiguration	Creates a new protocol configuration object.
Remove-AzNetworkWatcher	Removes a Network Watcher.
Remove-AzNetworkWatcherConnectionMonitor	Remove connection monitor.
Remove-AzNetworkWatcherFlowLog	Deletes the specified flow log resource.
Remove-AzNetworkWatcherPacketCapture	Removes a packet capture resource.
Set-AzNetworkWatcherConfigFlowLog	Configures flow logging for a target resource.
Set-AzNetworkWatcherConnectionMonitor	Updates connection monitor resource.
Set-AzNetworkWatcherFlowLog	Updates flow log resource.
Start-AzNetworkWatcherConnectionMonitor	Start a connection monitor
Start-AzNetworkWatcherResourceTroubleshooting	Starts troubleshooting on a Networking resource in Azure.
Stop-AzNetworkWatcherConnectionMonitor	Stop a connection monitor
Stop-AzNetworkWatcherPacketCapture	Stops a running packet capture session
Test-AzNetworkWatcherConnectivity	Returns connectivity information for a specified source VM and a destination.
Test-AzNetworkWatcherIPFlow	Returns whether the packet is allowed or denied to or from a particular destination.

Networking

Add-AzDelegation	Adds a delegation to a subnet.
Add-AzNetworkInterfaceIpConfig	Adds a network interface IP configuration to a network interface.
Add-AzNetworkInterfaceTapConfig	Creates a TapConfiguration resource associated to a NetworkInterface. This will reference to an existing VirtualNetworkTap resource.
Add-AzNetworkSecurityRuleConfig	Adds a network security rule configuration to a network security group.
Add-AzRoutingPolicy	Add a Routing Policy to the Routing Intent object.
Add-AzServiceEndpointPolicyDefinition	Adds a service endpoint policy definition to a specified policy.
Approve-AzPrivateEndpointConnection	Approves a private endpoint connection.
Deny-AzPrivateEndpointConnection	denies a private endpoint connection.
Deploy-AzNetworkManagerCommit	Deploys a network manager commit.
Get-AzApplicationSecurityGroup	Gets an application security group.
Get-AzAutoApprovedPrivateLinkService	Gets an array of private link service id that can be linked to a private end point with auto approved.
Get-AzAvailablePrivateEndpointType	Return available private end point types in the location.
Get-AzAvailableServiceAlias	Get available service aliases in the region.
Get-AzAvailableServiceDelegation	Get available service delegations in the region.
Get-AzBastion	Gets a Bastion resource or Bastion resources.
Get-AzBgpServiceCommunity	Provides a list of all services / regions, BGP communities, and associated prefixes.
Get-AzCustomIpPrefix	Gets a CustomIpPrefix resource
Get-AzDdosProtectionPlan	Gets a DDoS protection plan.
Get-AzDelegation	Get a delegation (or all of the delegations) on a given subnet.
Get-AzEffectiveNetworkSecurityGroup	Gets the effective network security group of a network interface.
Get-AzFirewall	Gets a Azure Firewall.
Get-AzFirewallFqdnTag	Gets the available Azure Firewall Fqdn Tags.
Get-AzFirewallLearnedIpPrefix	Gets firewall auto learned ip prefixes.
Get-AzFirewallPolicy	Gets a Azure Firewall Policy
Get-AzFirewallPolicyRuleCollectionGroup	Gets a Azure Firewall Policy Rule Collection Group
Get-AzIpAllocation	Gets a Azure IpAllocation.
Get-AzIpGroup	Get an Azure IpGroup
Get-AzLocalNetworkGateway	Gets a Local Network Gateway

Get-AzNatGateway	Gets a Nat Gateway resource in a resource group by name or NatGateway Id or all Nat Gateway resources in a resource group.
Get-AzNetworkInterface	Gets a network interface.
Get-AzNetworkInterfaceIpConfig	Gets a network interface IP configuration for a network interface.
Get-AzNetworkInterfaceTapConfig	Gets a Tap configuration resource.
Get-AzNetworkManager	Gets a network manager in a resource group.
Get-AzNetworkManagerActiveConnectivityConfiguration	Lists NetworkManager Active Connectivity Configurations in network manager.
Get-AzNetworkManagerActiveSecurityAdminRule	Lists NetworkManager Active Security Admin Rules in network manager.
Get-AzNetworkManagerConnectivityConfiguration	Gets a connectivity configuration in a network manager.
Get-AzNetworkManagerDeploymentStatus	Lists Deployment Status in a network manager.
Get-AzNetworkManagerEffectiveConnectivityConfiguration	Lists NetworkManager Effective Connectivity Configurations applied on a virtual networks.
Get-AzNetworkManagerEffectiveSecurityAdminRule	Lists NetworkManager Effective Security Admin Rules applied on a virtual networks.
Get-AzNetworkManagerGroup	Gets network group(s) in a network manager.
Get-AzNetworkManagerManagementGroupConnection	Gets a network manager management group connection.
Get-AzNetworkManagerScopeConnection	Gets a scope connection in a network manager.
Get-AzNetworkManagerSecurityAdminConfiguration	Gets a network security admin configuration in a network manager.
Get-AzNetworkManagerSecurityAdminRule	Gets a security admin rule in a network manager.
Get-AzNetworkManagerSecurityAdminRuleCollection	Gets a security admin rule collection in a network manager.
Get-AzNetworkManagerStaticMember	Gets network manager static members.
Get-AzNetworkManagerSubscriptionConnection	Gets a network manager subscription connection.
Get-AzNetworkProfile	Gets an existing network profile top level resource
Get-AzNetworkSecurityGroup	Gets a network security group.
Get-AzNetworkSecurityRuleConfig	Get a network security rule configuration for a network security group.
Get-AzNetworkServiceTag	Gets the list of service tag information resources.
Get-AzNetworkUsage	Lists network usages for a subscription
Get-AzNetworkVirtualAppliance	Get or List Network Virtual Appliances.
Get-AzNetworkVirtualApplianceSku	Get or List available Network Virtual Appliance Skus in the inventory.

Get-AzPrivateEndpoint	Get a private endpoint
Get-AzPrivateEndpointConnection	Gets a private endpoint connection resource.
Get-AzPrivateLinkResource	Gets a private link resource.
Get-AzPrivateLinkService	Gets private link service
Get-AzPublicIpAddress	Gets a public IP address.
Get-AzPublicIpPrefix	Gets a public IP prefix
Get-AzRoutingIntent	Retrieves a routing intent resource associated with a VirtualHub.
Get-AzRoutingPolicy	Retrieves a routing policy of a routing intent resource associated with a VirtualHub.
Get-AzSecurityPartnerProvider	Get an Azure SecurityPartnerProvider
Get-AzServiceEndpointPolicy	Gets a service endpoint policy.
Get-AzServiceEndpointPolicyDefinition	Gets a service endpoint policy definition.
Get-AzVirtualApplianceSite	Get or List sites connected to Network Virtual Appliance resource(s).
Get-AzVirtualHub	Gets an Azure VirtualHub by Name and ResourceGroupName or lists all Virtual Hubs by ResourceGroupName/Subscription.
Get-AzVirtualHubBgpConnection	The Get-AzVirtualHubBgpConnection cmdlet gets a Virtual WAN Hub BGP Connection in a Virtual WAN Hub or lists all Virtual WAN Hub BGP Connections in a Virtual WAN Hub.
Get-AzVirtualHubVnetConnection	Gets a Virtual Network Connection in a virtual hub or lists all virtual network connections in a virtual hub.
Get-AzVirtualWan	Gets a Virtual WAN or all Virtual WANs in a resource group or subscription.
New-AzApplicationSecurityGroup	Creates an application security group.
New-AzBastion	Creates a bastion resource.
New-AzContainerNicConfig	Creates a new container network interface configuration object.
New-AzContainerNicConfigIpConfig	Creates a container nic configuration ip configuration object.
New-AzCustomIpPrefix	Creates a CustomIpPrefix resource
New-AzDdosProtectionPlan	Creates a DDoS protection plan.
New-AzDelegation	Creates a service delegation.
New-AzFirewall	Creates a new Firewall in a resource group.
New-AzFirewallApplicationRule	Creates a Firewall Application Rule.
New-AzFirewallApplicationRuleCollection	Creates a collection of Firewall application rules.
New-AzFirewallHubIpAddress	Ip addresses assoicated to the firewall on virtual hub

New-AzFirewallHubPublicIpAddress	Public Ip assoicated to the firewall on virtual hub
New-AzFirewallNatRule	Creates a Firewall NAT Rule.
New-AzFirewallNatRuleCollection	Creates a collection of Firewall NAT rules.
New-AzFirewallNetworkRule	Creates a Firewall Network Rule.
New-AzFirewallNetworkRuleCollection	Creates a Azure Firewall Network Collection of Network rules.
New-AzFirewallPolicy	Creates a new Azure Firewall Policy
New-AzFirewallPolicyApplicationRule	Create a new Azure Firewall Policy Application Rule
New-AzFirewallPolicyExplicitProxy	Creates a new Explicit Proxy
New-AzFirewallPolicyFilterRuleCollection	Create a new Azure Firewall Policy Filter Rule Collection
New-AzFirewallPolicyIntrusionDetection	Creates a new Azure Firewall Policy Intrusion Detection to associate with Firewall Policy
New-AzFirewallPolicyIntrusionDetectionBypassTraffic	Creates a new Azure Firewall Policy Intrusion Detection Bypass Traffic Setting
New-AzFirewallPolicyIntrusionDetectionSignatureOverride	Creates a new Azure Firewall Policy Intrusion Detection Signature Override
New-AzFirewallPolicyNatRule	Create a new Azure Firewall Policy NAT Rule
New-AzFirewallPolicyNatRuleCollection	Create a new Azure Firewall Policy Nat Rule Collection
New-AzFirewallPolicyNetworkRule	Create a new Azure Firewall Policy Network Rule
New-AzFirewallPolicyRuleCollectionGroup	Create a new Azure Firewall Policy Rule Collection Group
New-AzFirewallPolicySnat	Creates SNAT configuration of PrivateRange and AutoLearnPrivateRanges for the firewall policy
New-AzFirewallPolicySqlSetting	Creates a new SQL Setting for Azure Firewall Policy
New-AzFirewallPolicyThreatIntelWhitelist	Create a new threat intelligence whitelist for Azure Firewall Policy
New-AzFirewallPublicIpAddress	This is the placeholder for the Ip Address that can be used for multi pip on azure firewall.
New-AzFirewallThreatIntelWhitelist	Create a new threat intelligence whitelist for Azure Firewall
New-AzIpAllocation	Creates an Azure IpAllocation.
New-AzIpConfigurationBgpPeeringAddressObject	creates a new IpconfigurationBgpPeeringAddressObject
New-AzIpGroup	Creates an Azure IpGroup.
New-AzIpsecPolicy	Creates an IPSec Policy.
New-AzIpsecTrafficSelectorPolicy	Creates a traffic selector policy.
New-AzLocalNetworkGateway	Creates a Local Network Gateway
New-AzNatGateway	Create new Nat Gateway resource with properties Public Ip Address/Public Ip Prefix, IdleTimeoutInMinutes and Sku.

New-AzNetworkInterface	Creates a network interface.
New-AzNetworkInterfaceIpConfig	Creates a network interface IP configuration.
New-AzNetworkManager	Creates a network manager.
New-AzNetworkManagerAddressPrefixItem	Creates a network manager address prefix item.
New-AzNetworkManagerConnectivityConfiguration	Creates a network manager connectivity configuration.
New-AzNetworkManagerConnectivityGroupItem	Creates a connectivity group item.
New-AzNetworkManagerGroup	Creates a network manager group.
New-AzNetworkManagerHub	Creates a network manager hub.
New-AzNetworkManagerManagementGroupConnection	Creates a network manager management group connection.
New-AzNetworkManagerScope	Creates a network manager scope.
New-AzNetworkManagerScopeConnection	Creates a scope connection.
New-AzNetworkManagerSecurityAdminConfiguration	Creates a security admin configuration.
New-AzNetworkManagerSecurityAdminRule	Creates a security admin rule.
New-AzNetworkManagerSecurityAdminRuleCollection	Creates a security admin rule collection.
New-AzNetworkManagerSecurityGroupItem	Creates a security group item.
New-AzNetworkManagerStaticMember	Creates a network manager static member.
New-AzNetworkManagerSubscriptionConnection	Creates a network manager subscription connection.
New-AzNetworkProfile	Creates a new network profile.
New-AzNetworkSecurityGroup	Creates a network security group.
New-AzNetworkSecurityRuleConfig	Creates a network security rule configuration.
New-AzNetworkVirtualAppliance	Create a Network Virtual Appliance resource.
New-AzO365PolicyProperty	Create an office 365 traffic breakout policy object.
New-AzOffice365PolicyProperty	Define a new Office 365 traffic breakout policy to be used with a Virtual Appliance site.
New-AzPacketCaptureFilterConfig	Creates a new packet capture filter object.
New-AzPacketCaptureScopeConfig	Creates a new packet capture scope object.
New-AzPrivateEndpoint	Creates a private endpoint.
New-AzPrivateEndpointIpConfiguration	Creates an IpConfiguration object for private endpoint.
New-AzPrivateLinkService	Creates a private link service
New-AzPrivateLinkServiceConnection	Creates a private link service connection configuration.
New-AzPrivateLinkServiceIpConfig	Create a private link service ip configuration.
New-AzPublicIpAddress	Creates a public IP address.

New-AzPublicIpPrefix	Creates a Public IP Prefix
New-AzPublicIpTag	Creates an IP Tag.
New-AzRadiusServer	Creates an external radius server configuration
New-AzRoutingConfiguration	Creates a RoutingConfiguration object.
New-AzRoutingIntent	Creates a routing intent resource associated with a VirtualHub.
New-AzRoutingPolicy	Returns an in-memory routing policy object.
New-AzSecurityPartnerProvider	Creates an Azure SecurityPartnerProvider.
New-AzServiceEndpointPolicy	Creates a service endpoint policy.
New-AzServiceEndpointPolicyDefinition	Creates a service endpoint policy definition.
New-AzVirtualApplianceSite	Create a site connected to a Network Virtual Appliance.
New-AzVirtualApplianceSkuProperty	Define a Network Virtual Appliance sku for the resource.
New-AzVirtualHub	Creates an Azure VirtualHub resource.
New-AzVirtualHubBgpConnection	The New-AzVirtualHubBgpConnection cmdlet creates a HubBgpConnection resource that peers the Azure Virtual WAN Hub Router with a BGP-enabled peer in a virtual network connected to the Virtual WAN Hub.
New-AzVirtualHubVnetConnection	The New-AzVirtualHubVnetConnection cmdlet creates a HubVirtualNetworkConnection resource that peers a Virtual Network to the Azure Virtual Hub.
New-AzVirtualWan	Creates an Azure Virtual WAN.
Remove-AzApplicationSecurityGroup	Removes an application security group.
Remove-AzBastion	Removes a bastion resource.
Remove-AzCustomIpPrefix	Removes a CustomIpPrefix
Remove-AzDdosProtectionPlan	Removes a DDoS protection plan.
Remove-AzDelegation	Removes a service delegation from the provided subnet.
Remove-AzFirewall	Remove a Firewall.
Remove-AzFirewallPolicy	Removes an Azure Firewall Policy
Remove-AzFirewallPolicyRuleCollectionGroup	Removes a Azure Firewall Policy Rule Collection Group in a Azure firewall policy
Remove-AzIpAllocation	Deletes an Azure IpAllocation.
Remove-AzIpGroup	Deletes an Azure IpGroup.
Remove-AzLocalNetworkGateway	Deletes a Local Network Gateway
Remove-AzNatGateway	Remove Nat Gateway resource.
Remove-AzNetworkInterface	Removes a network interface.

Remove-AzNetworkInterfaceIpConfig	Removes a network interface IP configuration from a network interface.
Remove-AzNetworkInterfaceTapConfig	Removes a tap configuration from given network interface
Remove-AzNetworkManager	Removes a network manager.
Remove-AzNetworkManagerConnectivityConfiguration	Removes a connectivity configuration.
Remove-AzNetworkManagerGroup	Removes a network Group.
Remove-AzNetworkManagerManagementGroupConnection	Removes a network manager management group connection.
Remove-AzNetworkManagerScopeConnection	Removes a network manager scope connection.
Remove-AzNetworkManagerSecurityAdminConfiguration	Removes a security admin configuration.
Remove-AzNetworkManagerSecurityAdminRule	Removes a security admin rule.
Remove-AzNetworkManagerSecurityAdminRuleCollection	Removes a security admin rule collection.
Remove-AzNetworkManagerStaticMember	Removes a network manager static member.
Remove-AzNetworkManagerSubscriptionConnection	Remove a network manager subscription connection.
Remove-AzNetworkProfile	Removes a network profile.
Remove-AzNetworkSecurityGroup	Removes a network security group.
Remove-AzNetworkSecurityRuleConfig	Removes a network security rule from a network security group.
Remove-AzNetworkVirtualAppliance	Remove a Network Virtual Appliance resource.
Remove-AzPrivateEndpoint	Removes a private endpoint.
Remove-AzPrivateEndpointConnection	Removes a private endpoint connection.
Remove-AzPrivateLinkService	Removes a private link service
Remove-AzPublicIpAddress	Removes a public IP address.
Remove-AzPublicIpPrefix	Removes a public IP prefix
Remove-AzRoutingIntent	Delete a routing intent resource associated with a VirtualHub.
Remove-AzRoutingPolicy	Removes the specified routing policy from a routing intent resource associated with a VirtualHub.
Remove-AzSecurityPartnerProvider	Deletes an Azure SecurityPartnerProvider.
Remove-AzServiceEndpointPolicy	Removes a service endpoint policy.
Remove-AzServiceEndpointPolicyDefinition	Removes a service endpoint policy definition.
Remove-AzVirtualApplianceSite	Remove a virtual appliance site from a Network Virtual Appliance resource.

Remove-AzVirtualHub	Removes an Azure VirtualHub resource.
Remove-AzVirtualHubBgpConnection	The Remove-AzVirtualHubBgpConnection cmdlet removes a HubBgpConnection resource that peers the Azure Virtual WAN Hub Router with a BGP-enabled peer in a virtual network connected to the Virtual WAN Hub.
Remove-AzVirtualHubVnetConnection	The Remove-AzVirtualHubVnetConnection cmdlet removes an Azure Virtual Network Connection which peers a remote VNET to the hub VNET.
Remove-AzVirtualWan	Removes an Azure Virtual WAN.
Set-AzBastion	Updates the Bastion Resource.
Set-AzFirewall	Saves a modified Firewall.
Set-AzFirewallPolicy	Saves a modified azure firewall policy
Set-AzFirewallPolicyRuleCollectionGroup	saves a modified azure firewall policy rule collection group
Set-AzIpAllocation	Saves a modified IpAllocation.
Set-AzIpGroup	Saves a modified Firewall.
Set-AzLocalNetworkGateway	Modifies a local network gateway.
Set-AzNatGateway	Update Nat Gateway Resource with Public Ip Address, Public Ip Prefix and IdleTimeoutInMinutes.
Set-AzNetworkInterface	Updates a network interface.
Set-AzNetworkInterfaceIpConfig	Updates an IP configuration for a network interface.
Set-AzNetworkInterfaceTapConfig	Updates a tap configuration for a network interface.
Set-AzNetworkManager	Updates a network manager..
Set-AzNetworkManagerConnectivityConfiguration	Updates a connectivity configuration.
Set-AzNetworkManagerGroup	Updates a network manager group.
Set-AzNetworkManagerManagementGroupConnection	Update a network manger management group connection
Set-AzNetworkManagerScopeConnection	Update a network manager scope connection.
Set-AzNetworkManagerSecurityAdminConfiguration	Updates a network manager security admin configuration.
Set-AzNetworkManagerSecurityAdminRule	Updates a network manager security admin rule.
Set-AzNetworkManagerSecurityAdminRuleCollection	Updates a network manager security admin rule collection.
Set-AzNetworkManagerSubscriptionConnection	Update a network manger subscription connection.
Set-AzNetworkProfile	Updates a network profile.
Set-AzNetworkSecurityGroup	Updates a network security group.
Set-AzNetworkSecurityRuleConfig	Updates a network security rule configuration for a network security group.
Set-AzPrivateEndpoint	Updates a private endpoint.

Set-AzPrivateEndpointConnection	Updates a private endpoint connection state on private link service.
Set-AzPrivateLinkService	Updates a private link service.
Set-AzPublicIpAddress	Updates a public IP address.
Set-AzPublicIpPrefix	Sets the Tags for an existing PublicIpPrefix
Set-AzRoutingIntent	Updates a routing intent resource associated with a VirtualHub.
Set-AzRoutingPolicy	Updates the destinations or nexthop for the specified Routing Policy of a Routing Intent object.
Set-AzSecurityPartnerProvider	Saves a modified Azure SecurityPartnerProvider.
Set-AzServiceEndpointPolicy	Updates a service endpoint policy.
Set-AzServiceEndpointPolicyDefinition	Updates a service endpoint policy definition.
Set-AzVirtualHub	Modifies a Virtual Hub to add a Virtual HUb Route Table to it.
Start-AzVirtualnetworkGatewayPacketCapture	Starts Packet Capture Operation on a Virtual Network Gateway.
Test-AzPrivateIPAddressAvailability	Test availability of a private IP address in a virtual network.
Test-AzPrivateLinkServiceVisibility	The **Test-AzPrivateLinkServiceVisibility** checks whether a private link service is visible for current use.
Update-AzCustomIpPrefix	Updates a CustomIpPrefix
Update-AzNetworkVirtualAppliance	Update or Change a Network Virtual Appliance resource.
Update-AzVirtualApplianceSite	Change or Modify a Virtual Appliance site connected to a Network Virtual Appliance resource.
Update-AzVirtualHub	Updates a virtual hub.
Update-AzVirtualHubBgpConnection	The Update-AzVirtualHubBgpConnection cmdlet updates an existing HubBgpConnection resource (Virtual WAN Hub BGP Connection).
Update-AzVirtualHubVnetConnection	Updates an existing HubVirtualNetworkConnection.
Update-AzVirtualWan	Updates an Azure Virtual WAN.

Route

Add-AzRouteConfig	Adds a route to a route table.
Add-AzRouteFilterRuleConfig	Adds a route filter rule to a route filter.
Add-AzRouteServerPeer	Add a peer to an Azure RouteServer
Add-AzVirtualHubRoute	Creates a VirtualHubRoute object which can be passed as parameter to the Add-AzVirtualHubRouteTable command.
Add-AzVirtualHubRouteTable	Creates a Virtual Hub Route Table resource which is a child of VirtualHub.

Add-AzVirtualRouterPeer	Add a Peer to an Azure VirtualRouter
Get-AzEffectiveRouteTable	Gets the effective route table of a network interface.
Get-AzRouteConfig	Gets routes from a route table.
Get-AzRouteFilter	Gets a route filter.
Get-AzRouteFilterRuleConfig	Gets a route filter rule in a route filter.
Get-AzRouteServer	Get an Azure RouteServer
Get-AzRouteServerPeer	Gets a RouteServer peer in an Azure RouteServer
Get-AzRouteServerPeerAdvertisedRoute	List routes being advertised by specific route server peer
Get-AzRouteServerPeerLearnedRoute	List routes learned by a specific route server peer
Get-AzRouteTable	Gets route tables.
Get-AzVHubRouteTable	Retrieves a hub route table resource associated with a VirtualHub.
Get-AzVirtualHubRouteTable	Gets a Virtual Hub Route Table in a virtual hub or lists all route tables in a virtual hub. The cmdlet Get-AzVHubRouteTable is replacing this cmdlet.
Get-AzVirtualRouter	Get an Azure VirtualRouter
Get-AzVirtualRouterPeer	Gets a VirtualRouter peer in an Azure VirtualRouter
Get-AzVirtualRouterPeerAdvertisedRoute	List routes being advertised by specific virtual router peer
Get-AzVirtualRouterPeerLearnedRoute	List routes learned by a specific virtual router peer
New-AzRouteConfig	Creates a route for a route table.
New-AzRouteFilter	Creates a route filter.
New-AzRouteFilterRuleConfig	Creates a route filter rule for a route filter.
New-AzRouteServer	Creates an Azure RouteServer.
New-AzRouteTable	Creates a route table.
New-AzStaticRoute	Creates a StaticRoute object which can then be added to a RoutingConfiguration object.
New-AzVHubRoute	Creates a VHubRoute object which can be passed as parameter to the New-AzVHubRouteTable command.
New-AzVHubRouteTable	Creates a hub route table resource associated with a VirtualHub.
New-AzVirtualHubRoute	Creates an Azure Virtual Hub Route object.
New-AzVirtualHubRouteTable	Creates an Azure Virtual Hub Route Table object.
New-AzVirtualRouter	Creates an Azure VirtualRouter.
Remove-AzRouteConfig	Removes a route from a route table.
Remove-AzRouteFilter	Removes a route filter.

Remove-AzRouteFilterRuleConfig	Removes a route filter rule from a route filter.
Remove-AzRouteServer	Deletes an Azure RouteServer.
Remove-AzRouteServerPeer	Removes a Peer from an Azure RouteServer
Remove-AzRouteTable	Removes a route table.
Remove-AzVHubRouteTable	Delete a hub route table resource associated with a VirtualHub.
Remove-AzVirtualHubRouteTable	Delete a virtual hub route table resource associated with a virtual hub.
Remove-AzVirtualRouter	Deletes an Azure VirtualRouter.
Remove-AzVirtualRouterPeer	Removes a Peer from an Azure VirtualRouter
Reset-AzHubRouter	Resets the RoutingState of a VirtualHub resource.
Set-AzRouteConfig	Updates a route configuration for a route table.
Set-AzRouteFilter	Updates a route filter.
Set-AzRouteFilterRuleConfig	Modifies the route filter rule of a route filter.
Set-AzRouteTable	Updates a route table.
Update-AzRouteServer	Update an Azure RouteServer.
Update-AzRouteServerPeer	Update a Peer in an Azure RouteServer
Update-AzVHubRouteTable	Delete a hub route table resource associated with a VirtualHub.
Update-AzVirtualRouter	Updates a Virtual Router.
Update-AzVirtualRouterPeer	Update a Peer in an Azure VirtualRouter

Virtual Network

Add-AzVirtualNetworkGatewayIpConfig	Adds an IP configuration to a virtual network gateway.
Add-AzVirtualNetworkPeering	Creates a peering between two virtual networks.
Add-AzVirtualNetworkSubnetConfig	Adds a subnet configuration to a virtual network.
Disconnect-AzVirtualNetworkGatewayVpnConnection	Disconnect given connected vpn client connections with a given virtual network gateway.
Get-AzVirtualNetwork	Gets a virtual network in a resource group.
Get-AzVirtualNetworkAvailableEndpointService	Lists available endpoint services for location.
Get-AzVirtualNetworkGateway	Gets a Virtual Network Gateway
Get-AzVirtualNetworkGatewayAdvertisedRoute	Lists routes being advertised by an Azure virtual network gateway
Get-AzVirtualNetworkGatewayBGPPeerStatus	Lists an Azure virtual network gateway's BGP peers
Get-AzVirtualNetworkGatewayConnection	Gets a Virtual Network Gateway Connection
Get-AzVirtualNetworkGatewayConnectionIkeSa	Get IKE Security Associations of a Virtual Network

	Gateway Connection
Get-AzVirtualNetworkGatewayConnectionSharedKey	Displays the shared key used for the connection.
Get-AzVirtualNetworkGatewayConnectionVpnDeviceConfigScript	This commandlet takes the connection resource, VPN device brand, model, firmware version, and return the corresponding configuration script that customers can apply directly on their on-premises VPN devices. The script will follow the syntax of the selected device, and fill in the necessary parameters such as Azure gateway public IP addresses, virtual network address prefixes, VPN tunnel pre-shared key, etc. so customers can simply copy-paste to their VPN device configurations.
Get-AzVirtualNetworkGatewayLearnedRoute	Lists routes learned by an Azure virtual network gateway
Get-AzVirtualNetworkGatewayNatRule	Gets a Virtual Network Gateway NatRule.
Get-AzVirtualNetworkGatewaySupportedVpnDevice	This commandlet returns a list of supported VPN device brands, models, and firmware versions.
Get-AzVirtualNetworkGatewayVpnClientConnectionHealth	Get the list of vpn client connection health of an Azure virtual network gateway for per vpn client connection
Get-AzVirtualNetworkPeering	Gets the virtual network peering.
Get-AzVirtualNetworkSubnetConfig	Gets a subnet in a virtual network.
Get-AzVirtualNetworkTap	Gets a virtual network tap
Get-AzVirtualNetworkUsageList	Gets virtual network current usage.
New-AzVirtualNetwork	Creates a virtual network.
New-AzVirtualNetworkGateway	Creates a Virtual Network Gateway
New-AzVirtualNetworkGatewayConnection	Creates the Site-to-Site VPN connection between the virtual network gateway and the on-prem VPN device.
New-AzVirtualNetworkGatewayIpConfig	Creates an IP Configuration for a Virtual Network Gateway
New-AzVirtualNetworkGatewayNatRule	Creates the virtual network gateway natRule object.
New-AzVirtualNetworkGatewayPolicyGroup	Create a Virtual Network Gateway Policy Group
New-AzVirtualNetworkGatewayPolicyGroupmember	Create a Virtual Network Gateway Policy Group Member
New-AzVirtualNetworkSubnetConfig	Creates a virtual network subnet configuration.
New-AzVirtualNetworkTap	Creates a VirtualNetworkTap resource.
Remove-AzVirtualNetwork	Removes a virtual network.
Remove-AzVirtualNetworkGateway	Deletes a Virtual Network Gateway
Remove-AzVirtualNetworkGatewayConnection	Deletes a Virtual Network Gateway Connection
Remove-AzVirtualNetworkGatewayDefaultSite	Removes the default site from a virtual network gateway.

Remove-AzVirtualNetworkGatewayIpConfig	Removes an IP Configuration from a Virtual Network Gateway
Remove-AzVirtualNetworkGatewayNatRule	Removes or Delete a Virtual Network Gateway NatRule.
Remove-AzVirtualNetworkPeering	Removes a virtual network peering.
Remove-AzVirtualNetworkSubnetConfig	Removes a subnet configuration from a virtual network.
Remove-AzVirtualNetworkTap	Removes a virtual network tap.
Reset-AzVirtualNetworkGateway	Resets the Virtual Network Gateway
Reset-AzVirtualNetworkGatewayConnection	Reset a Virtual Network Gateway Connection
Reset-AzVirtualNetworkGatewayConnectionSharedKey	Resets the shared key of the virtual network gateway connection.
Resize-AzVirtualNetworkGateway	Resizes an existing virtual network gateway.
Set-AzVirtualNetwork	Updates a virtual network.
Set-AzVirtualNetworkGateway	Updates a virtual network gateway.
Set-AzVirtualNetworkGatewayConnection	Configures a virtual network gateway connection.
Set-AzVirtualNetworkGatewayConnectionSharedKey	Configures the shared key of the virtual network gateway connection.
Set-AzVirtualNetworkGatewayDefaultSite	Sets the default site for a virtual network gateway.
Set-AzVirtualNetworkPeering	Configures a virtual network peering.
Set-AzVirtualNetworkSubnetConfig	Updates a subnet configuration for a virtual network.
Set-AzVirtualNetworkTap	Updates a virtual network tap.
Start-AzVirtualNetworkGatewayConnectionPacketCapture	Starts Packet Capture Operation on a Virtual Network Gateway Connection.
Stop-AzVirtualNetworkGatewayConnectionPacketCapture	Stops Packet Capture Operation on a Virtual Network Gateway connection
Stop-AzVirtualNetworkGatewayPacketCapture	Stops Packet Capture Operation on a Virtual Network Gateway.
Sync-AzVirtualNetworkPeering	Command to sync the address space on the peering link if the remote virtual network has a new address space.
Update-AzVirtualNetworkGatewayNatRule	Updates a Virtual Network Gateway NatRule.

VPN

Add-AzVpnClientRevokedCertificate	Adds a VPN client-revocation certificate.
Add-AzVpnClientRootCertificate	Adds a VPN client root certificate.
Disconnect-AzP2SVpnGatewayVpnConnection	Disconnect given connected vpn client connections with a given p2s vpn gateway

Get-AzP2sVpnGateway	Gets an existing P2SVpnGateway under VirtualHub.
Get-AzP2sVpnGatewayConnectionHealth	Gets the current aggregared point to site connections health information from P2SVpnGateway.
Get-AzP2sVpnGatewayDetailedConnectionHealth	Gets the detailed information of current point to site connections from P2SVpnGateway.
Get-AzP2sVpnGatewayVpnProfile	Generates and returns a SAS url for customer to download Vpn profile for point to site client setup to have point to site connectivity to P2SVpnGateway.
Get-AzVirtualWanVpnConfiguration	Gets the Vpn configuration for a subset of VpnSites connected to this WAN via VpnConnections. Uploads the generated Vpn configuration to a storage blob specified by the customer.
Get-AzVirtualWanVpnServerConfiguration	Gets the list of all VpnServerConfigurations that are associated with this VirtualWan.
Get-AzVirtualWanVpnServerConfigurationVpnProfile	Generates and downloads Vpn profile at VirtualWan-VpnServerConfiguration level for Point to site client setup.
Get-AzVpnClientConfiguration	Allows users to easily download the Vpn Profile package that was generated using the New-AzVpnClientConfiguration commandlet.
Get-AzVpnClientIpsecParameter	Gets the vpn Ipsec parameters set on Virtual Network Gateway for Point to site connections.
Get-AzVpnClientPackage	Gets information about a VPN client package.
Get-AzVpnClientRevokedCertificate	Gets information about VPN client-revocation certificates.
Get-AzVpnClientRootCertificate	Gets information about VPN root certificates.
Get-AzVpnConnection	Gets a vpn connection by name or lists all vpn connections connected to a VpnGateway. **Note** This Powershell command is for customers using Virtual WAN Site-to-site VPN Gateway only.
Get-AzVpnGateway	Gets a VpnGateway resource using ResourceGroupName and GatewayName OR lists all gateways by ResourceGroupName or SubscriptionId.
Get-AzVpnGatewayNatRule	Gets a NAT rule associated with VpnGateway.
Get-AzVpnServerConfiguration	Gets an existing VpnServerConfiguration for point to site connectivity.
Get-AzVpnServerConfigurationPolicyGroup	Create a new P2SVpnGateway under VirtualHub for point to site connectivity.
Get-AzVpnSite	Gets an Azure VpnSite resource by name OR lists all VpnSites in a ResourceGroup or SubscriptionId. This is an RM representation of customer branches that are uploaded to Azure for S2S connectivity with a Cortex virtual hub.
Get-AzVpnSiteLinkConnectionIkeSa	Get IKE Security Associations of VPN Site Link Connections

New-AzP2sVpnGateway	Create a new P2SVpnGateway under VirtualHub for point to site connectivity.
New-AzVpnClientConfiguration	This command allows the users to create the Vpn profile package based on pre-configured vpn settings on the VPN gateway, in addition to some additional settings that users may need to configure, for e.g. some root certificates.
New-AzVpnClientConnectionConfiguration	Create Virtual Network Gateway Connection configuration
New-AzVpnClientIpsecParameter	This command allows the users to create the Vpn ipsec parameters object specifying one or all values such as IpsecEncryption,IpsecIntegrity,IkeEncryption,IkeIntegrity,DhGroup,PfsGroup to set on the existing VPN gateway.
New-AzVpnClientIpsecPolicy	This command allows the users to create the Vpn ipsec policy object specifying one or all values such as IpsecEncryption,IpsecIntegrity,IkeEncryption,IkeIntegrity,DhGroup,PfsGroup to set on the VPN gateway. This command let output object is used to set vpn ipsec policy for both new / existing gateway.
New-AzVpnClientRevokedCertificate	Creates a new VPN client-revocation certificate.
New-AzVpnClientRootCertificate	Creates a new VPN client root certificate.
New-AzVpnConnection	Creates a IPSec connection that connects a VpnGateway to a remote customer branch represented in RM as a VpnSite.
New-AzVpnGateway	Creates a Scalable VPN Gateway.
New-AzVpnGatewayNatRule	Creates a NAT rule on a VpnGateway which can be associated with VpnSiteLinkConnection.
New-AzVpnServerConfiguration	Create a new VpnServerConfiguration for point to site connectivity.
New-AzVpnServerConfigurationPolicyGroup	Create a new P2SVpnGateway under VirtualHub for point to site connectivity.
New-AzVpnSite	Creates a new Azure VpnSite resource. This is an RM representation of customer branches that are uploaded to Azure for S2S connectivity with a Cortex virtual hub.
New-AzVpnSiteLink	Creates an Azure VpnSiteLink object.
New-AzVpnSiteLinkConnection	Creates an Azure VpnSiteLinkConnection object.
Remove-AzP2sVpnGateway	Removes an existing P2SVpnGateway.
Remove-AzVpnClientIpsecParameter	Removes Vpn custom ipsec policy set on Virtual Network Gateway resource.
Remove-AzVpnClientRevokedCertificate	Removes a VPN client-revocation certificate.
Remove-AzVpnClientRootCertificate	Removes an existing VPN client root certificate.
Remove-AzVpnConnection	Removes a VpnConnection.
Remove-AzVpnGateway	The Remove-AzVpnGateway cmdlet removes an Azure VPN gateway. This is a gateway specific to Azure Virtual WAN's software defined connectivity.
Remove-AzVpnGatewayNatRule	Removes a NAT rule associated with VpnGateway.

Remove-AzVpnServerConfiguration	Removes an existing VpnServerConfiguration.
Remove-AzVpnServerConfigurationPolicyGroup	Create a new P2SVpnGateway under VirtualHub for point to site connectivity.
Remove-AzVpnSite	Removes an Azure VpnSite resource.
Reset-AzP2sVpnGateway	Resets the scalable P2S VPN gateway.
Reset-AzVpnGateway	Resets the scalable VPN gateway.
Reset-AzVpnSiteLinkConnection	Reset a VPN Site Link Connection
Set-AzVpnClientIpsecParameter	Sets the vpn ipsec parameters for existing virtual network gateway.
Start-AzVpnConnectionPacketCapture	Starts Packet Capture Operation on a Vpn Connection.
Start-AzVpnGatewayPacketCapture	Starts Packet Capture Operation on a Vpn Gateway.
Stop-AzVpnConnectionPacketCapture	Stops Packet Capture Operation on a Vpn connection
Stop-AzVpnGatewayPacketCapture	Stops Packet Capture Operation on a Vpn Gateway.
Update-AzP2sVpnGateway	Update an existing P2SVpnGateway under VirtualHub for point to site connectivity.
Update-AzVpnConnection	Updates a VPN connection.
Update-AzVpnGateway	Updates a scalable VPN gateway.
Update-AzVpnGatewayNatRule	Updates a NAT rule associated with VpnGateway.
Update-AzVpnServerConfiguration	Updates an existing VpnServerConfiguration.
Update-AzVpnServerConfigurationPolicyGroup	Create a new P2SVpnGateway under VirtualHub for point to site connectivity.
Update-AzVpnSite	Updates a VPN site.

Bastion Hosts

Reference

Service: Virtual Networks

API Version: 2022-09-01

In this article

Operations

Operations

Create Or Update	Creates or updates the specified Bastion Host.
Delete	Deletes the specified Bastion Host.
Get	Gets the specified Bastion Host.
List	Lists all Bastion Hosts in a subscription.
List By Resource Group	Lists all Bastion Hosts in a resource group.
Update Tags	Updates Tags for BastionHost resource

az network bastion

Reference

> **Note**
>
> This reference is part of the **bastion** extension for the Azure CLI (version 2.43.0 or higher). The extension will automatically install the first time you run an **az network bastion** command. **Learn more** about extensions.

Manage Azure Bastion host machines.

In this article

Commands
az network bastion create
az network bastion delete
az network bastion list
az network bastion rdp
az network bastion show
az network bastion ssh
az network bastion tunnel
az network bastion update
az network bastion wait

Commands

az network bastion create	Create a Azure Bastion host machine.
az network bastion delete	Delete a Azure Bastion host machine.
az network bastion list	List all Azure Bastion host machines.
az network bastion rdp	RDP to target Virtual Machine using Tunneling from Azure Bastion.
az network bastion show	Show a Azure Bastion host machine.
az network bastion ssh	SSH to a virtual machine using Tunneling from Azure Bastion.
az network bastion tunnel	Open a tunnel through Azure Bastion to a target virtual machine.
az network bastion update	Update a Azure Bastion host machine.

az network bastion wait	Place the CLI in a waiting state until a condition is met.

az network bastion create

Create a Azure Bastion host machine.

Azure CLI

```
az network bastion create --name
                          --public-ip-address
                          --resource-group
                          --vnet-name
                          [--disable-copy-paste {0, 1, f, false, n, no, t,
true, y, yes}]
                          [--enable-ip-connect {0, 1, f, false, n, no, t,
true, y, yes}]
                          [--enable-tunneling {0, 1, f, false, n, no, t,
true, y, yes}]
                          [--location]
                          [--no-wait {0, 1, f, false, n, no, t, true, y,
yes}]
                          [--scale-units]
                          [--sku {Basic, Standard}]
                          [--tags]
```

Examples

Create a Azure Bastion host machine.

Azure CLI

```
az network bastion create --location westus2 --name MyBastionHost --public-
ip-address MyPublicIpAddress --resource-group MyResourceGroup --vnet-name
MyVnet
```

Required Parameters

`--name -n`

Name of the bastion host.

`--public-ip-address`

Name or ID of Azure Public IP. The SKU of the public IP must be Standard.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--vnet-name`

Name of the virtual network. It must have a subnet called AzureBastionSubnet.

Optional Parameters

`--disable-copy-paste`

Disable copy and paste for all sessions on this Azure Bastion resource.
accepted values: 0, 1, f, false, n, no, t, true, y, yes
default value: False

`--enable-ip-connect`

Enable IP-based Connections on this Azure Bastion resource.
accepted values: 0, 1, f, false, n, no, t, true, y, yes
default value: False

`--enable-tunneling`

Enable Native Client Support on this Azure Bastion resource.
accepted values: 0, 1, f, false, n, no, t, true, y, yes
default value: False

`--location -l`

Location. Values from: `az account list-locations`. You can configure the default location using `az configure --defaults location=<location>`.

`--no-wait`

Do not wait for the long-running operation to finish.
accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--scale-units`

Scale units for the Bastion Host resource with the range of [2, 50].

`--sku`

SKU of this Bastion Host.

accepted values: Basic, Standard

default value: Standard

`--tags`

Space-separated tags: key[=value] [key[=value] ...]. Support shorthand-syntax, json-file and yaml-file. Try `??` to show more.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion delete

Delete a Azure Bastion host machine.

Azure CLI

```
az network bastion delete [--ids]
                          [--name]
                          [--no-wait {0, 1, f, false, n, no, t, true, y,
yes}]
                          [--resource-group]
                          [--subscription]
```

Examples

Delete a Azure Bastion host machine.

Azure CLI

```
az network bastion delete --name MyBastionHost --resource-group
MyResourceGroup
```

Optional Parameters

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--no-wait`

Do not wait for the long-running operation to finish.

accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion list

List all Azure Bastion host machines.

Azure CLI

```
az network bastion list [--resource-group]
```

Examples

List all Azure Bastion host machines.

Azure CLI

```
az network bastion list -g MyResourceGroup
```

Optional Parameters

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion rdp

RDP to target Virtual Machine using Tunneling from Azure Bastion.

Azure CLI

```
az network bastion rdp [--configure]
                       [--disable-gateway {false, true}]
                       [--enable-mfa {false, true}]
                       [--ids]
                       [--name]
                       [--resource-group]
                       [--resource-port]
                       [--subscription]
                       [--target-ip-address]
                       [--target-resource-id]
```

Examples

RDP to virtual machine using Azure Bastion.

Azure CLI

```
az network bastion rdp --name MyBastionHost --resource-group MyResourceGroup
--target-resource-id vmResourceId
```

RDP to machine using reachable IP address.

Azure CLI

```
az network bastion rdp --name MyBastionHost --resource-group MyResourceGroup
--target-ip-address 10.0.0.1
```

Optional Parameters

`--configure`

Flag to configure RDP session.

default value: False

`--disable-gateway`

Flag to disable access through RD gateway.

accepted values: false, true

default value: False

`--enable-mfa`

Enable RDS auth for MFA if supported by the target machine.

accepted values: false, true

default value: False

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--resource-port`

Resource port of the target VM to which the bastion will connect.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--target-ip-address`

IP address of target Virtual Machine.

`--target-resource-id`

ResourceId of the target Virtual Machine.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion show

Show a Azure Bastion host machine.

Azure CLI

```
az network bastion show [--ids]
                        [--name]
                        [--resource-group]
                        [--subscription]
```

Examples

Show a Azure Bastion host machine.

Azure CLI

```
az network bastion show --name MyBastionHost --resource-group
MyResourceGroup
```

Optional Parameters

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion ssh

SSH to a virtual machine using Tunneling from Azure Bastion.

Azure CLI

```
az network bastion ssh --auth-type
                       [--ids]
                       [--name]
                       [--resource-group]
                       [--resource-port]
                       [--ssh-key]
                       [--subscription]
                       [--target-ip-address]
                       [--target-resource-id]
                       [--username]
```

Examples

SSH to virtual machine using Azure Bastion using password.

Azure CLI

```
az network bastion ssh --name MyBastionHost --resource-group MyResourceGroup
--target-resource-id vmResourceId --auth-type password --username xyz
```

SSH to virtual machine using Azure Bastion using ssh key file.

Azure CLI

```
az network bastion ssh --name MyBastionHost --resource-group MyResourceGroup
--target-resource-id vmResourceId --auth-type ssh-key --username xyz --ssh-
key C:/filepath/sshkey.pem
```

SSH to virtual machine using Azure Bastion using AAD.

Azure CLI

```
az network bastion ssh --name MyBastionHost --resource-group MyResourceGroup
--target-resource-id vmResourceId --auth-type AAD
```

SSH to virtual machine using Azure Bastion using AAD.

Azure CLI

```
az network bastion ssh --name MyBastionHost --resource-group MyResourceGroup
--target-resource-id vmResourceId --auth-type AAD
```

Required Parameters

`--auth-type`

Auth type to use for SSH connections.

Optional Parameters

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--resource-port`

Resource port of the target VM to which the bastion will connect.

`--ssh-key`

SSH key file location for SSH connections.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--target-ip-address`

IP address of target Virtual Machine.

`--target-resource-id`

ResourceId of the target Virtual Machine.

`--username`

User name for SSH connections.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion tunnel

Open a tunnel through Azure Bastion to a target virtual machine.

Azure CLI

```
az network bastion tunnel --port
                          --resource-port
                          [--ids]
                          [--name]
                          [--resource-group]
                          [--subscription]
                          [--target-ip-address]
                          [--target-resource-id]
                          [--timeout]
```

Examples

Open a tunnel through Azure Bastion to a target virtual machine using resourceId.

Azure CLI

```
az network bastion tunnel --name MyBastionHost --resource-group
MyResourceGroup --target-resource-id vmResourceId --resource-port 22 --port
50022
```

Open a tunnel through Azure Bastion to a target virtual machine using its IP address.

Azure CLI

```
az network bastion tunnel --name MyBastionHost --resource-group
MyResourceGroup --target-ip-address 10.0.0.1 --resource-port 22 --port 50022
```

Required Parameters

`--port`

Local port to use for the tunneling.

`--resource-port`

Resource port of the target VM to which the bastion will connect.

Optional Parameters

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--target-ip-address`

IP address of target Virtual Machine.

`--target-resource-id`

ResourceId of the target Virtual Machine.

`--timeout`

Timeout for connection to bastion host tunnel.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion update

Update a Azure Bastion host machine.

Azure CLI

```
az network bastion update [--add]
                          [--disable-copy-paste {0, 1, f, false, n, no, t, true, y, yes}]
                          [--enable-ip-connect {0, 1, f, false, n, no, t, true, y, yes}]
                          [--enable-tunneling {0, 1, f, false, n, no, t, true, y, yes}]
                          [--force-string {0, 1, f, false, n, no, t, true, y, yes}]
                          [--ids]
                          [--name]
                          [--no-wait {0, 1, f, false, n, no, t, true, y, yes}]
                          [--remove]
                          [--resource-group]
                          [--scale-units]
                          [--set]
                          [--sku {Basic, Standard}]
                          [--subscription]
```

Examples

Update a Azure Bastion host machine to enable native client support.

Azure CLI

```
az network bastion update --name MyBastionHost --resource-group
MyResourceGroup --enable-tunneling
```

Optional Parameters

`--add`

Add an object to a list of objects by specifying a path and key value pairs. Example: --add property.listProperty <key=value, string or JSON string>.

`--disable-copy-paste`

Disable copy and paste for all sessions on this Azure Bastion resource.

accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--enable-ip-connect`

Enable IP-based Connections on this Azure Bastion resource.

accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--enable-tunneling`

Enable Native Client Support on this Azure Bastion resource.

accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--force-string`

When using 'set' or 'add', preserve string literals instead of attempting to convert to JSON.

accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--name -n`

Name of the bastion host.

`--no-wait`

Do not wait for the long-running operation to finish.
accepted values: 0, 1, f, false, n, no, t, true, y, yes

`--remove`

Remove a property or an element from a list. Example: --remove property.list OR --remove propertyToRemove.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--scale-units`

Scale units for the Bastion Host resource with the range of [2, 50].

`--set`

Update an object by specifying a property path and value to set. Example: --set property1.property2=.

`--sku`

SKU of this Bastion Host.
accepted values: Basic, Standard

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.

az network bastion wait

Place the CLI in a waiting state until a condition is met.

Azure CLI

```
az network bastion wait [--created]
                        [--custom]
                        [--deleted]
                        [--exists]
                        [--ids]
                        [--interval]
                        [--name]
                        [--resource-group]
                        [--subscription]
```

```
                                [--timeout]
                                [--updated]
```

Optional Parameters

`--created`

Wait until created with 'provisioningState' at 'Succeeded'.

default value: False

`--custom`

Wait until the condition satisfies a custom JMESPath query. E.g. provisioningState!='InProgress', instanceView.statuses[?code=='PowerState/running'].

`--deleted`

Wait until deleted.

default value: False

`--exists`

Wait until the resource exists.

default value: False

`--ids`

One or more resource IDs (space-delimited). It should be a complete resource ID containing all information of 'Resource Id' arguments. You should provide either --ids or other 'Resource Id' arguments.

`--interval`

Polling interval in seconds.

default value: 30

`--name -n`

Name of the bastion host.

`--resource-group -g`

Name of resource group. You can configure the default group using `az configure --defaults group=<name>`.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--timeout`

Maximum wait in seconds.
default value: 3600

`--updated`

Wait until updated with provisioningState at 'Succeeded'.
default value: False

Global Parameters

`--debug`

Increase logging verbosity to show all debug logs.

`--help -h`

Show this help message and exit.

`--only-show-errors`

Only show errors, suppressing warnings.

`--output -o`

Output format.

`--query`

JMESPath query string. See http://jmespath.org/ for more information and examples.

`--subscription`

Name or ID of subscription. You can configure the default subscription using `az account set -s NAME_OR_ID`.

`--verbose`

Increase logging verbosity. Use --debug for full debug logs.