

Azure Bastion

Azure Bastion is a fully managed platform as a service (PaaS) from Microsoft Azure that provides secure and seamless RDP and SSH access to virtual machines (VMs) directly through the Azure Portal. It eliminates the need for exposing VMs to the public internet or setting up a separate bastion host or jump server for accessing VMs in a virtual network.

Azure Bastion is designed to enhance security by providing secure RDP and SSH connectivity over SSL/TLS, which eliminates the need for administrators to manage public IP addresses or handle inbound NAT rules. It also integrates with Azure Active Directory (AD) for identity management and multifactor authentication (MFA), adding an extra layer of security.

Some key features of Azure Bastion include:

1. **Seamless RDP/SSH Access:** Azure Bastion provides browser-based access to Azure VMs via the Azure Portal, removing the need for VPNs or public IP addresses.
2. **Secure Connectivity:** All RDP/SSH sessions are encrypted using SSL/TLS, ensuring data confidentiality and integrity.
3. **Zero Public IP Exposure:** VMs do not require public IP addresses, reducing the attack surface and eliminating the need to manage network security groups (NSGs) or firewall rules for inbound traffic.
4. **Centralized Management:** Administrators can centrally manage access policies and permissions through Azure RBAC (Role-Based Access Control) and Azure AD.
5. **Audit Trails:** Azure Bastion logs all RDP/SSH sessions, providing administrators with detailed audit trails for compliance and security monitoring purposes.

Overall, Azure Bastion simplifies and secures remote access to Azure VMs, making it an essential component for managing and maintaining Azure infrastructure.

Use cases of Azure Bastion:

Azure Bastion can be beneficial in various scenarios where secure remote access to Azure virtual machines (VMs) is required. Here are some common use cases:

1. **Secure Remote Administration:** Azure Bastion provides a secure way for administrators to remotely access VMs for maintenance, troubleshooting, and management tasks without exposing them to the public internet.
2. **Compliance Requirements:** Organizations with strict compliance requirements, such as those in the healthcare or finance sectors, can use Azure Bastion to ensure that remote access to VMs meets security standards without compromising sensitive data.
3. **Remote Development and Testing:** Developers and testers often need remote access to VMs for software development, testing, and debugging purposes. Azure Bastion provides a secure and convenient way to access these VMs from anywhere.

4. **Hybrid Cloud Scenarios:** In hybrid cloud environments where on-premises infrastructure is integrated with Azure resources, Azure Bastion can serve as a secure gateway for accessing VMs deployed in Azure from on-premises networks.
5. **Third-party Access:** When providing access to VMs for third-party vendors or contractors, Azure Bastion ensures that access is secure and auditable, reducing the risk of unauthorized access to sensitive systems.
6. **Multi-user Access:** Azure Bastion supports multi-user access with role-based access control (RBAC), allowing organizations to define granular access policies and permissions for different users or groups.
7. **Zero Trust Network Access:** As part of a zero trust security model, Azure Bastion helps enforce the principle of least privilege by providing secure, on-demand access to VMs without exposing them to the broader network.
8. **Dynamic Scalability:** Azure Bastion scales dynamically based on demand, allowing organizations to handle fluctuations in remote access requirements efficiently without the need for manual intervention or provisioning of additional infrastructure.

In this lab, we are configuring Azure Bastion to enable secure remote access to Azure virtual machines (VMs) without exposing them to the public internet. The end goal is to enhance security by eliminating the need for public IP addresses, managing inbound NAT rules, and ensuring encrypted RDP/SSH sessions for VM access. By setting up Azure Bastion, we simplify remote administration, comply with security standards, facilitate remote development and testing, and enable secure access for third parties while maintaining centralized management and audit trails.

To begin with the Lab:

1. Now from the previous lab we have our setup ready.
2. The whole idea of the Azure Bastion service is to ensure that we don't have public IP addresses assigned to machines. Now, we do have a public IP address assigned to the demo VM.
3. So, we are going to remove it. Then we will delete it from our resources.
4. For that go to the Network interface then go to IP configuration and disassociate the public IP address.

The screenshot shows the 'IP configurations' section for a virtual machine named 'demo-vm288'. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Settings, IP configurations, DNS servers, Network security group, Properties, Locks, Monitoring, Automation, and Help. Under 'IP configurations', there's a table with one row: Name 'ipconfig1' and IP Version 'IPv4'. On the right, there's a detailed view of the configuration. It shows a warning about primary IP configuration already existing. The 'Name' is set to 'ipconfig1', 'IP version' is 'IPv4', and 'Type' is 'Primary'. Under 'Private IP address settings', 'Allocation' is set to 'Dynamic'. Under 'Public IP address settings', there's a note about unchecking the 'Associate public IP address' checkbox. A red box highlights this checkbox. At the bottom, there are 'Save' and 'Cancel' buttons.

- After that you have to go to the Virtual Network of Demo VM and create an empty subnet for Bastion service. Also, you need to select Azure Bastion for Subnet Purpose.

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more ↗](#)

The screenshot shows the 'Subnet' configuration page. Under 'Subnet purpose', 'Azure Bastion' is selected. The 'Name' is 'AzureBastionSubnet'. Under 'IPv4', 'Include an IPv4 address space' is checked. The 'IPv4 address range' is '10.0.0.0/16'. The 'Starting address' is '10.0.1.0' and the 'Size' is '/26 (64 addresses)'. The 'Subnet address range' is '10.0.1.0 - 10.0.1.63'.

- Now you need to go to Demo VM and from overview click on Connect and choose to connect via Bastion.

The screenshot shows the 'Overview' page for a virtual machine named 'demo-VM'. On the left, there's a sidebar with options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Connect. Under 'Connect', there are two options: 'Connect' and 'Connect via Bastion'. The 'Connect via Bastion' option is highlighted with a red box. On the right, there's a summary of the VM's status: Status: Running, Location: North Europe, Subscription (move): Azure Pass - Sponsorship, and Subscription ID: 3541d15a-44aa-4f6e-a120-1b7a6d5925bf.

7. After that you have to choose dedicated Deployment Options and then click on Configure Manually.

↖ Dedicated Deployment Options

Create Bastion

Name ⓘ demo-VN-bastion

Resource group ⓘ new-grp

Virtual network ⓘ demo-VN

Public IP address ⓘ demo-VN-ip

 Bastion pricing starts with an hourly base rate. [Learn more ↗](#)

Deploy Bastion

Configure manually

8. Now you need to give it a name and then for tier choose basic.

Basics Advanced Tags Review + create

Bastion allows web based RDP access to your vnet VM. [Learn more ↗](#)

Project details

Subscription *

Azure Pass - Sponsorship

Resource group *

new-grp



[Create new](#)

Instance details

Name *

demo-bastion



Region *

North Europe



Availability zone ⓘ

None



Tier * ⓘ

Basic



Instance count ⓘ

2

9. After that you need to choose the virtual network and it will automatically pick up the subnet. Now it will be going to create a new IP address it will be for Bastion.

Configure virtual networks

Virtual network * ⓘ

[Create new](#)

Subnet *

[Manage subnet configuration](#)

Configure IP Address

IP Address ⓘ Public IP address Private IP address

Public IP address

Public IP address * ⓘ Create new Use existing

Public IP address name *

Public IP address SKU Standard

Assignment Dynamic Static

Availability zone None

10. After that just move to the review page and create your bastion. This will take some time to deploy.
11. Now once your resource is deployed go to all resources and go to Demo VM and connect via Bastion.
12. Below you can see that you just need to write the username and password and click on connect.

demo-VM | Bastion

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Connect

Bastion

Windows Admin Center

Networking

Network settings

Load balancing

Application security groups

Network manager

Settings

to expose them through public IP addresses. Deploying will automatically create a Bastion host on a subnet in your virtual network. [Learn more](#)

Using Bastion: demo-bastion

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language ⓘ English (US)

Authentication Type ⓘ VM Password

Username

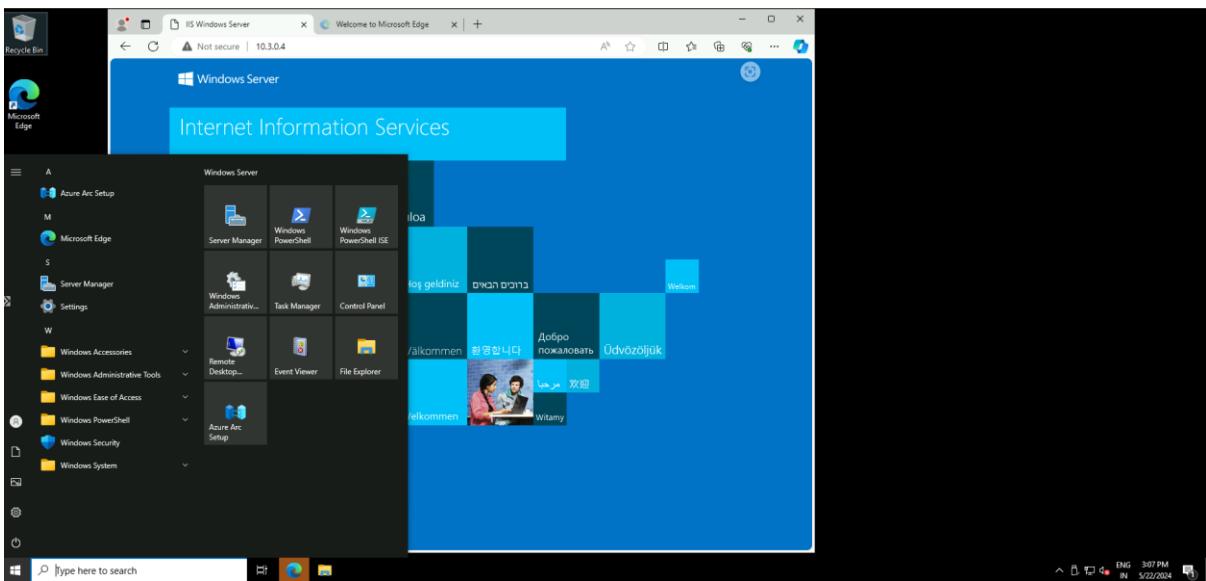
VM Password ⓘ

Show

Open in new browser tab

Connect

13. In your browser in the new tab you can see that you have connected with your VM.



14. Now you should go to Test VM and try to connect via bastion in it too.

A screenshot of the Azure portal's "Virtual machines" section. The top navigation bar includes "Create", "Switch to classic", "Reservations", "Manage view", "Refresh", "Export to CSV", "Open query", "Assign tags", and "Start". Below the navigation is a search bar and several filter buttons: "Subscription equals all", "Type equals all", "Resource group equals all", "Location equals all", and a "Add filter" button. A message "Showing 1 to 2 of 2 records." is displayed. The main table lists two virtual machines: "demo-VM" and "test-VM".

Name	Type	Subscription	Resource group	Location	Status
demo-VM	Virtual machine	Azure Pass - Sponsors...	NEW-GRP	North Europe	Running
test-VM	Virtual machine	Azure Pass - Sponsors...	new-grp	North Europe	Running

15. Below you can see that you have the option to connect.

test-VM | Bastion ⋮

Virtual machine

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Connect
 - Connect
 - Bastion**
- Windows Admin Center
- Networking
- Settings
- Availability + scale
- Security
- Backup + disaster recovery
- Operations
- Monitoring

Using Bastion: **demo-bastion**

Provisioning State: **Succeeded**

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language: English (US)

Authentication Type: VM Password

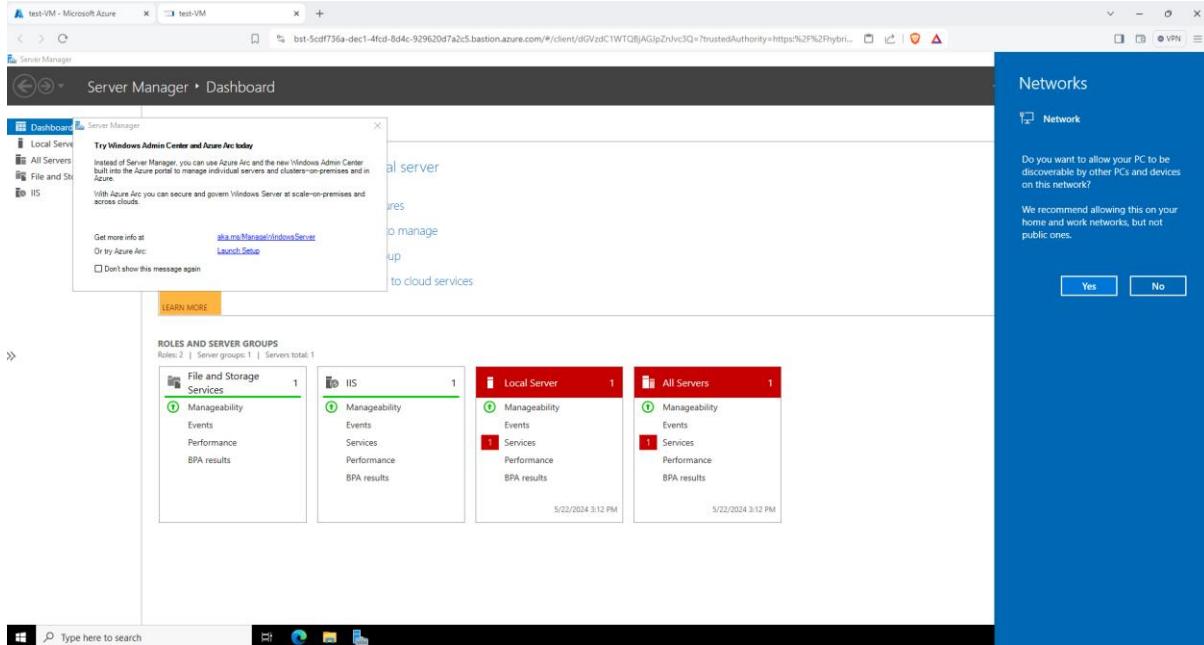
Username: testuser

VM Password: Show

Open in new browser tab

Connect

16. And here you can see that you have connected successfully.



17. When you have a virtual network peering between virtual networks you can use the same Azure Bastion host to even connect to virtual machines that are in the remote network.