Active Directory Domain Services Deployment with Azure Virtual Network Subnetting

Project Overview

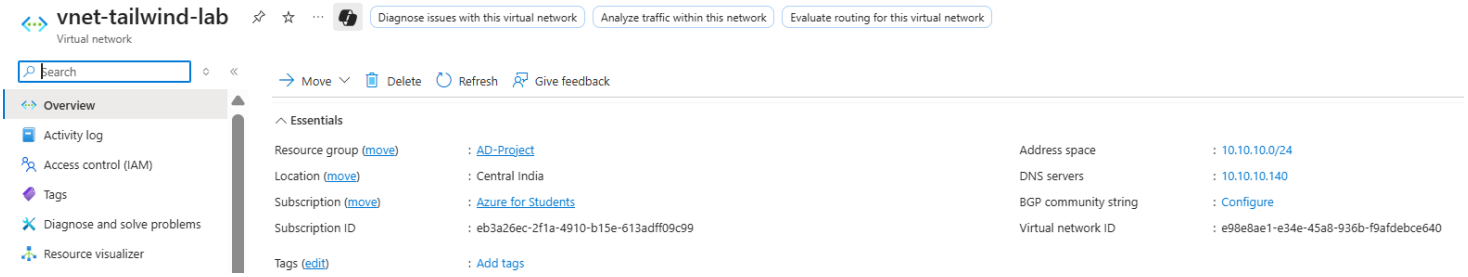
This guided project prepares you to manage Active Directory Domain Services (AD DS) by walking through:

- Creating and deploying domains
- Configuring group policy objects
- Establishing and enforcing password policies
- Maintaining overall security of Active Directory

1. Introduction to Azure Virtual Networks

Azure Virtual Networks (VNets) are the backbone for securely running Azure resources. VNets allow your resources, such as VMs and domain controllers, to communicate privately and securely.

Screenshot:



2. Creating the Virtual Network

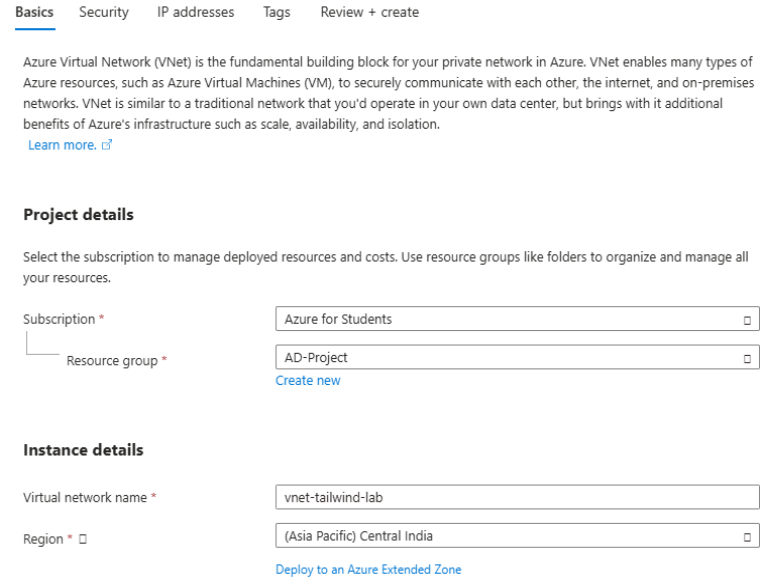
Step 1: Select Subscription and Resource Group

- Subscription: Azure for Students
- Resource group: AD-Project

Step-2: Configure Virtual Network Details

- Name: vnet-tailwind-lab
- Region: Central India

Screenshot:

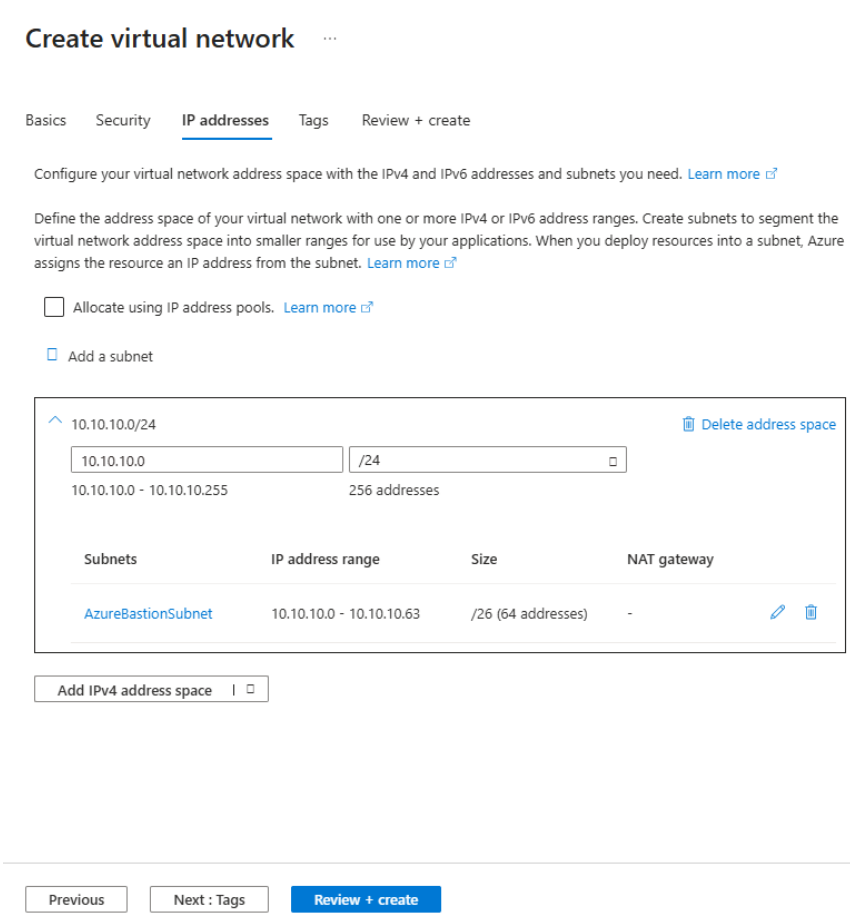


3. Subnetting the Virtual Network

Defining Address Space

- IPv4 address space: `10.10.10.0/24`
- Division into subnets, e.g., Azure Bastion and Servers

Screenshot:



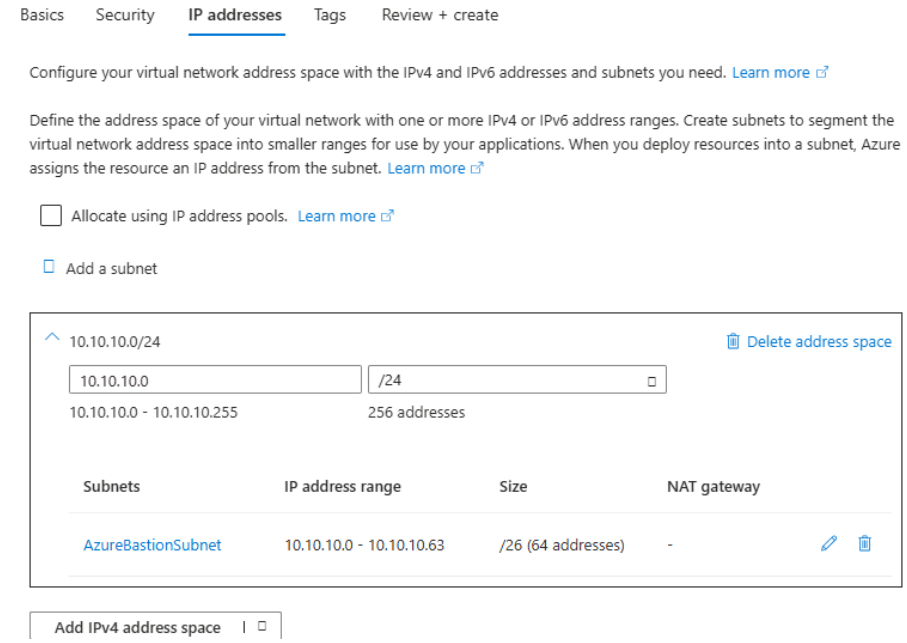
Azure Bastion Subnet:

- Name: AzureBastionSubnet
- Address range: `10.10.10.0/26` (64 addresses)

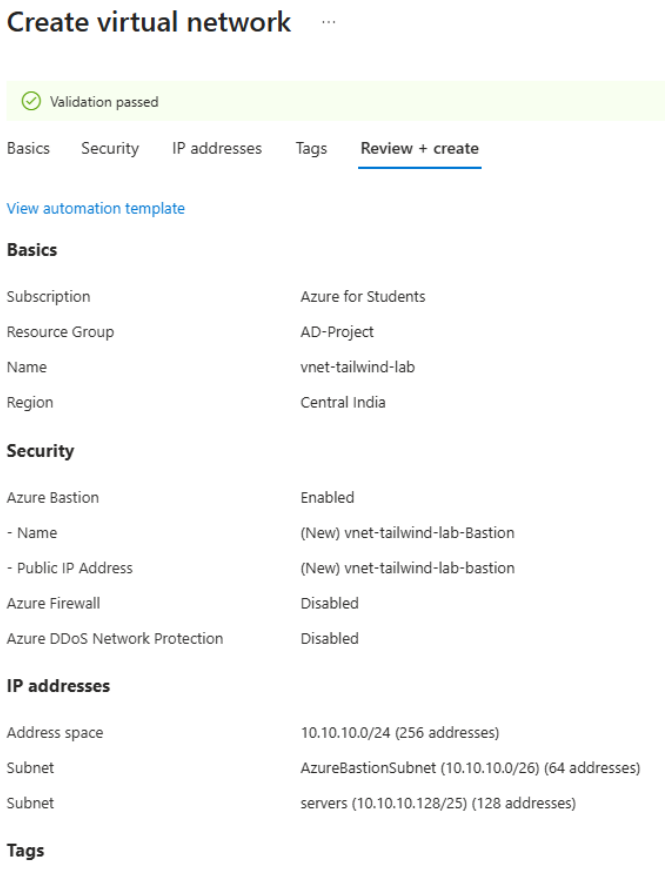
Servers Subnet:

- Name: servers
- Address range: `10.10.10.128/25` (128 addresses)

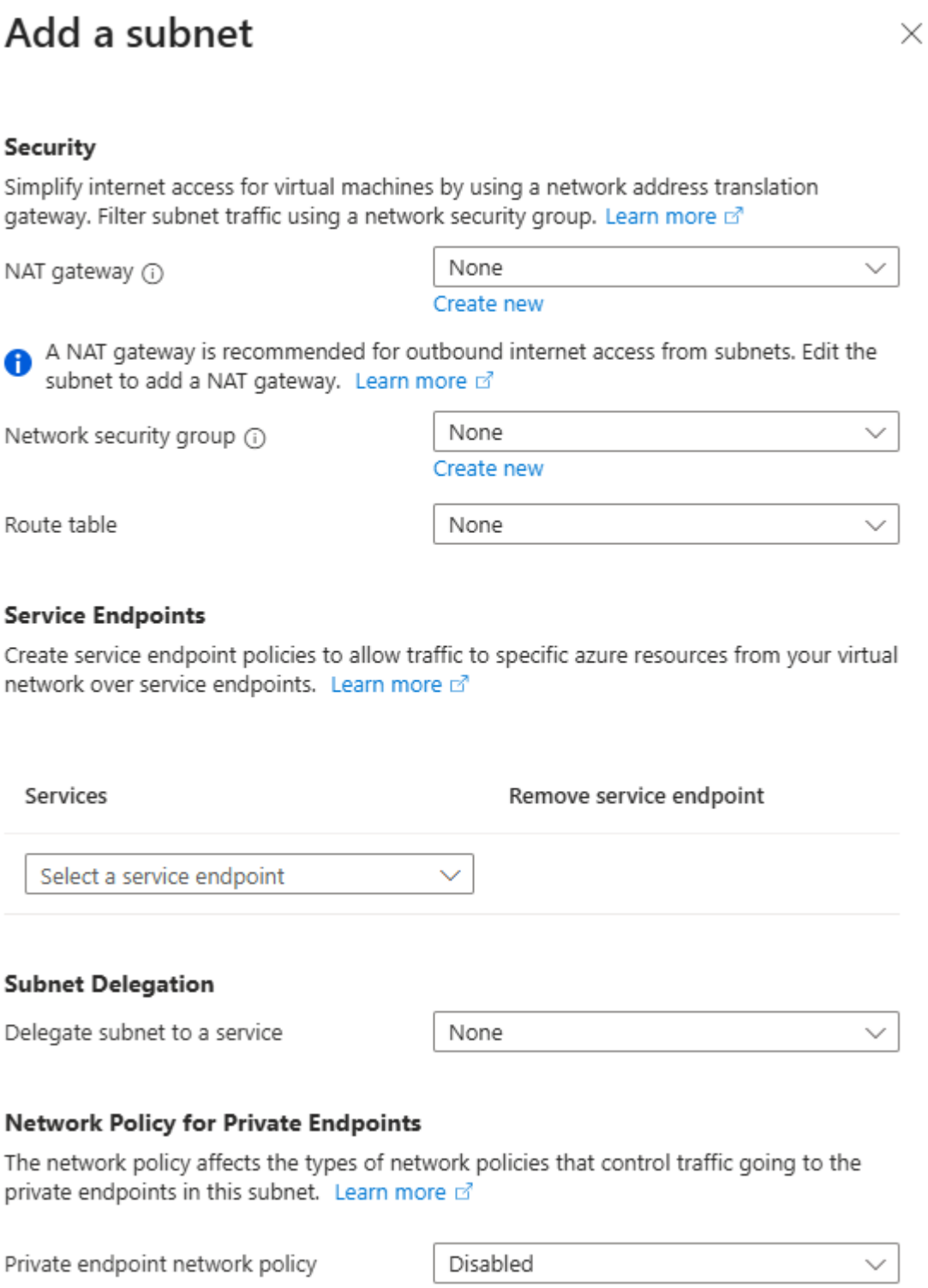
Screenshot:



Screenshot:



Screenshot:

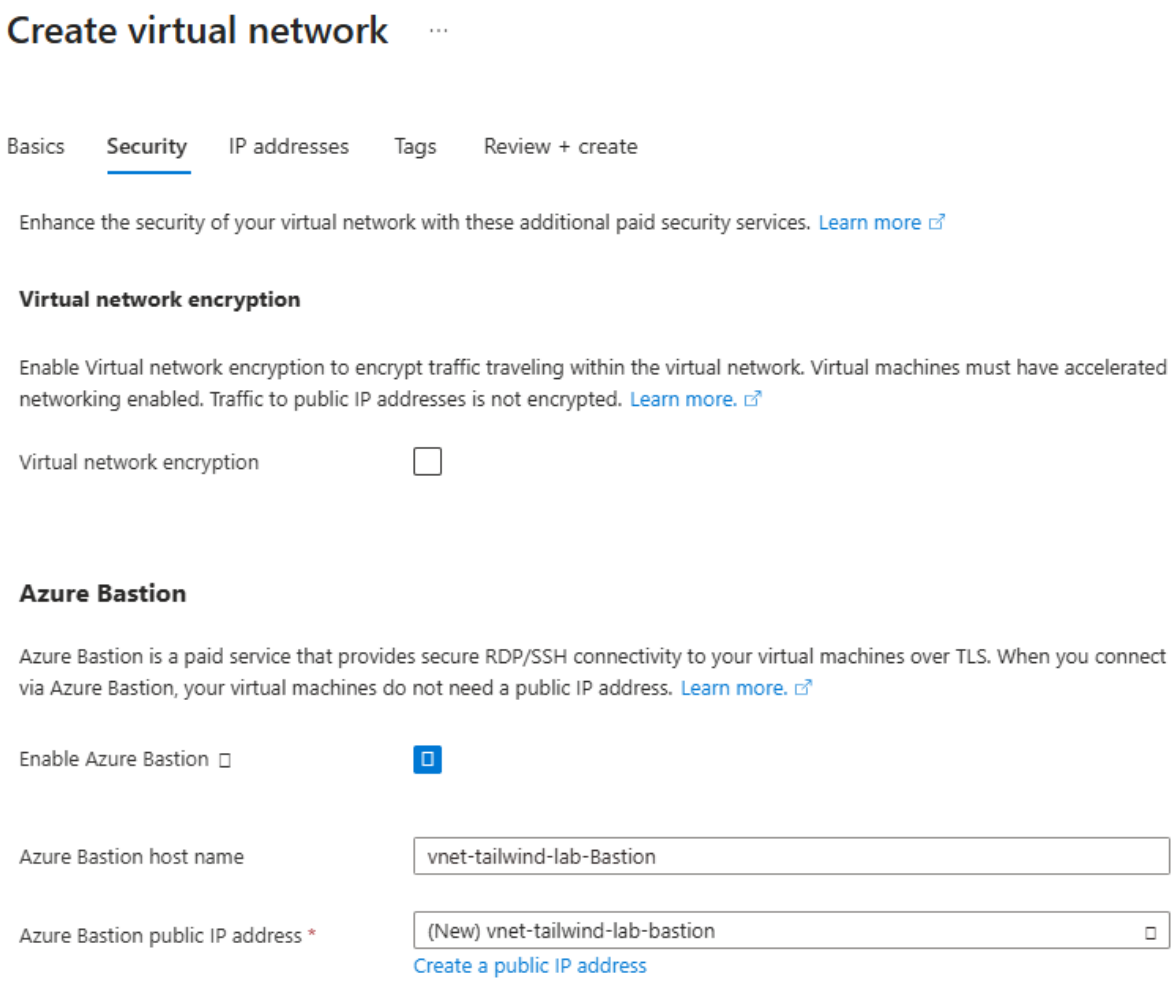

Add a subnet
Security
Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more
NAT gateway
None
Create new
A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. Learn more
Network security group
None
Create new
Route table
None
Service Endpoints
Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. Learn more
Services
Remove service endpoint
Select a service endpoint
Subnet Delegation
Delegate subnet to a service
None
Network Policy for Private Endpoints
The network policy affects the types of network policies that control traffic going to the private endpoints in this subnet. Learn more
Private endpoint network policy
Disabled

Azure Bastion provides secure RDP/SSH connectivity without exposing VMs to public IPs.

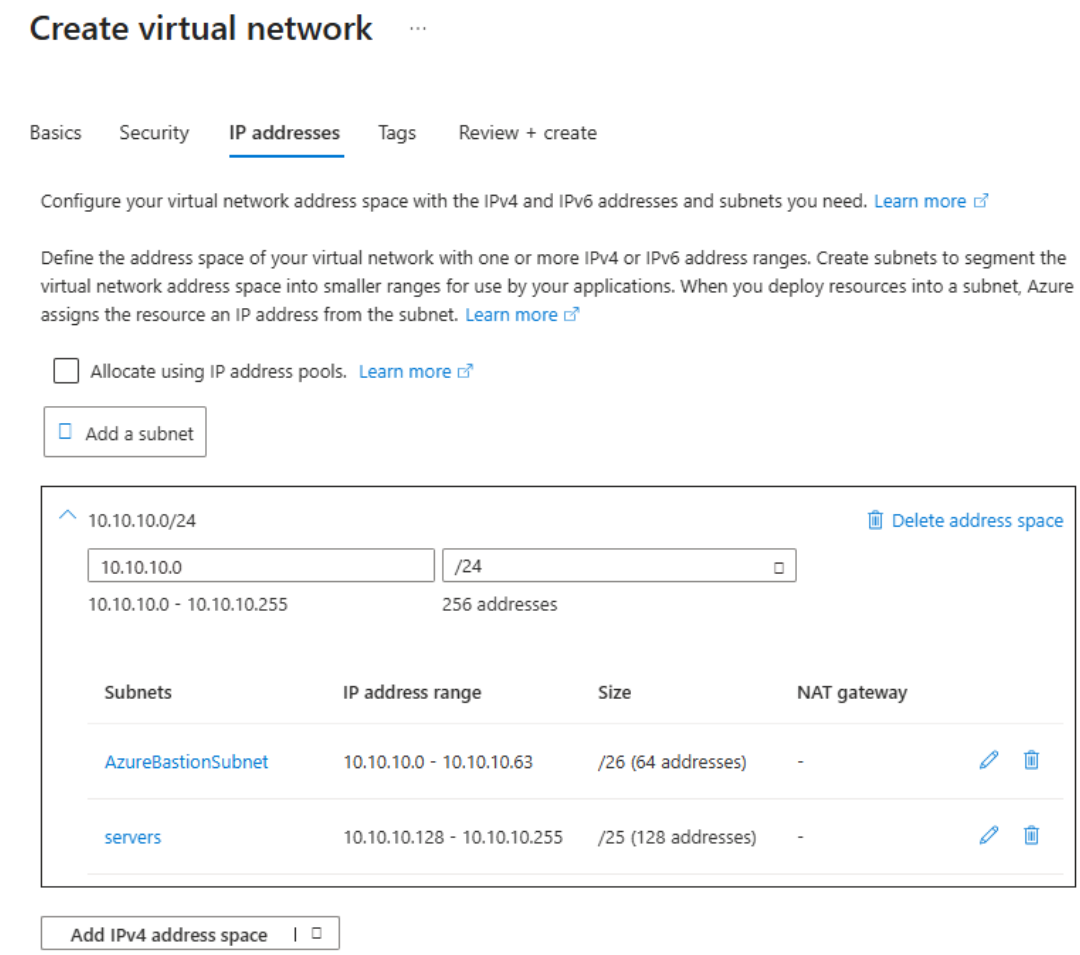
Enabling Bastion:

- Hostname: vnet-tailwind-lab-Bastion
- Public IP: (New) vnet-tailwind-lab-bastion

Screenshot:

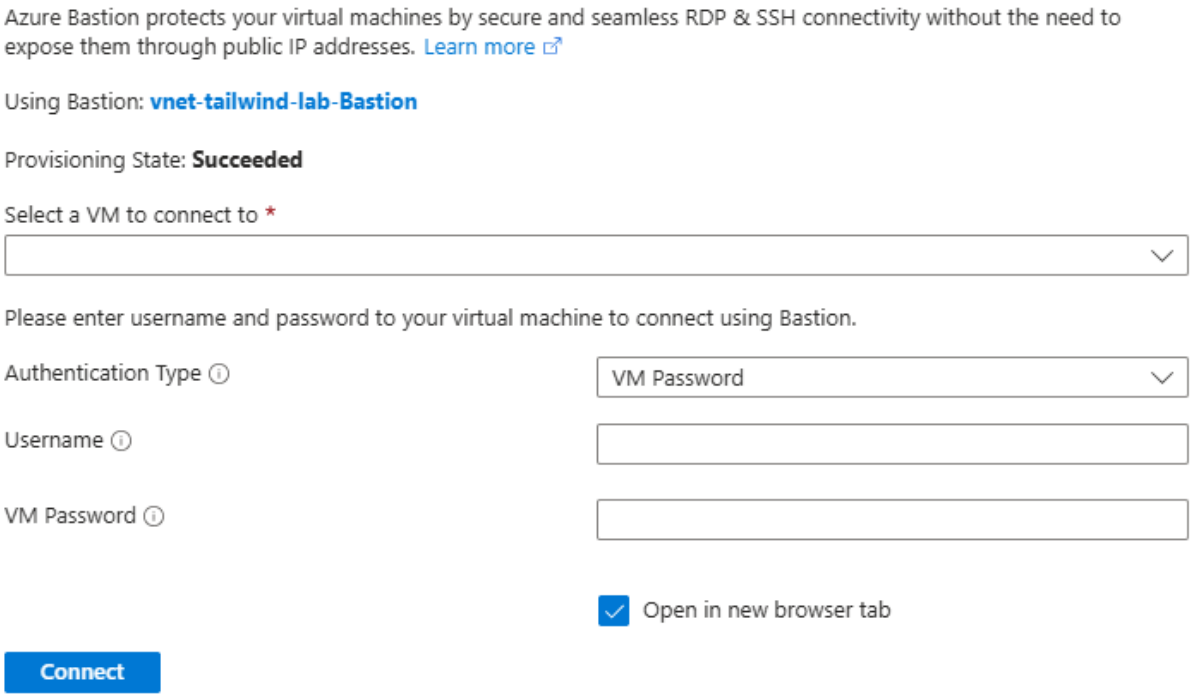


Screenshot:



Validate configuration before deployment. Review network name, group, region, address space, subnets, and Bastion.

Screenshot:



A summary overview pane after deployment shows address range, DNS, region, and resource group.

Screenshot:

Optional security, routing, and endpoint settings for each subnet.