

Create an App Service	1
Enable VNet Integration for the App Service	2
Use App Service Diagnostics	2
Create Azure Virtual Network (VNet)	3
Create Peering from VNet1 to VNet2	4
Move one VM from a Vnet to another	4
Test VNet Peering	4
Create Azure Virtual Network (VNet)	5
Create an azure VPN Gateway	5
Configure Point-to-Site Configuration	8
Azure vNet-to-vNet Connections	11
Create a Private DNS Zone	12
Link the Private DNS Zone to a VNet	12
Create a DNS resolver inside the virtual network	12

Create an App Service

1. Navigate to the Azure Portal.
2. In the left-hand sidebar, click on "+ Create a resource."
3. Search for "Web App" and select it.
4. Click the "Create" button to initiate the setup.
5. Fill in the details for your App Service:
 - a. Subscription: Select the appropriate subscription.
 - b. Resource Group: Choose an existing resource group or create a new one.
 - c. Name: Provide a unique name for the App Service.
 - d. Publish: Select 'Code' or 'Docker Container' depending on your use case.
 - e. Runtime stack: Choose the appropriate runtime for your application (e.g., .NET, Node.js).
 - f. Operating System: Choose between Windows and Linux based on your application's requirements.
 - g. Region: Select the desired region.
 - h. App Service plan: Either use an existing plan or create a new one. Note: To use VNet Integration, the App Service plan should be a Premium, PremiumV2, or PremiumV3 tier.

6. Review any additional settings as needed and then click on the "Review + create" button.
7. After validation, click the "Create" button.

Enable VNet Integration for the App Service

1. Once your App Service is created, go to its overview page.
2. In the left-hand settings pane, under the "Settings" section, click on "Networking."
3. Under the "VNet Integration" section, click on "Click here to configure."
4. Click on "+ Add VNet" to start the VNet Integration setup.
5. You'll be presented with two options: "Integrate with an existing virtual network" or "Create a new VNet." If you have an existing VNet you'd like to integrate with, select that. Otherwise, you can set up a new VNet directly from here.
6. Fill in the required details:
 - a. Virtual Network: If using an existing VNet, select it from the dropdown list.
 - b. Subnet: Choose the appropriate subnet. Note: The subnet you select must have the 'Microsoft.Web/serverfarms' service endpoint enabled.
7. Click "OK" to initiate the integration.

Use App Service Diagnostics

1. Navigate to Your App Service
 - a. Go to the Azure Portal.
 - b. In the left-hand sidebar, click on "App Services" and then select your specific App Service from the list.
2. Open App Service Diagnostics
 - a. In the left-hand settings pane for your App Service, click on "Diagnose and solve problems."
3. Access the Networking Tools
 - a. Once inside the App Service Diagnostics, look for the section titled "Diagnostic Tools."
 - b. Click on "Networking Troubleshooter." This category contains diagnostics tools for checking the network-related configurations and issues of your App Service.
4. Use the Connection Issues tool to test connection to different IPs and services

Microsoft Azure

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

Home > App Services > coraxdaily | Diagnose and solve problems >

coraxdaily | Diagnostic Tools

Overview

Proactive Tools

- Auto-Heal
- Proactive CPU Monitoring
- Crash Monitoring

Diagnostic Tools

- Collect .NET Profiler Trace
- Collect Memory Dump
- Check Connection Strings
- Collect Network Trace

Search for common problems or tools

Ask Genie Refresh Feedback Get Resiliency Score report

Network/Connectivity Troubleshooter

Check your network connectivity and troubleshoot network issues

Tell us more about the problem you are experiencing:

Connection issues

- ✓ Connection between App Service worker(s) and VNet is healthy
- ✓ Dns setting is healthy
- i App Service's VNet related behaviors will be changed by following App Settings

Create Azure Virtual Network (VNet)

1. Login to the Azure Portal:
 - a. Open your web browser and navigate to the Azure Portal.
 - b. Sign in with your Azure account credentials.
2. Navigate to Virtual Networks:
 - a. In the left-hand side menu, click on "Create a resource."
 - b. In the "Search the Marketplace" box, type "Virtual Network" and select it from the dropdown.
3. Initiate VNet Creation:
 - a. Click on the "Create" button.
4. Fill in the Basic Details:
 - a. Subscription: Choose the appropriate Azure subscription.
 - b. Resource Group: Either select an existing resource group or create a new one.
 - c. Name: Provide a name for the Virtual Network. E.g., "MyVNet"
 - d. Region: Choose a region where you want the VNet to reside.
5. IP Addresses Configuration:
 - a. IPv4 Address space: Define an address range for the VNet. For this example, let's use 10.3.0.0/16.
6. Security Options:
 - a. You can leave the default options or configure DDoS protection and firewall as per your requirements.
 - b. Click on the "Review + create" button, then on the next screen, click "Create."

Create Peering from VNet1 to VNet2

1. In the Azure Portal, navigate to "Virtual networks" and select VNet1 (the first VNet).
2. In the VNet1 settings pane, under the "Settings" section, click on "Peerings."
3. Click on the "+ Add" button.
4. Fill in the details for the peering:
 - a. Name: Enter a descriptive name for the peering from VNet1 to VNet2.
 - b. Peer details: Select "I know my resource ID" or "I know my resource details" and then select VNet2 as the peer VNet.
 - c. Peering mode: Typically, choose "Hub" or "Spoke" based on your architecture. For most cases, "Spoke" will suffice.
 - d. Allow virtual network access: Set to "Enabled" to allow resources in VNet1 to communicate with VNet2.
5. Click "OK" to create the peering.

Move one VM from a Vnet to another

1. Take a backup of the VM. Just in case(Optional)
2. Delete the original VM. Make sure not to delete its disks or any other resources attached to it such as public IP or NSG.
3. Create a new NIC in the target vnet as part of a new VM configuration in PowerShell.
4. Create a new VM using the VM configuration created above.

Test VNet Peering

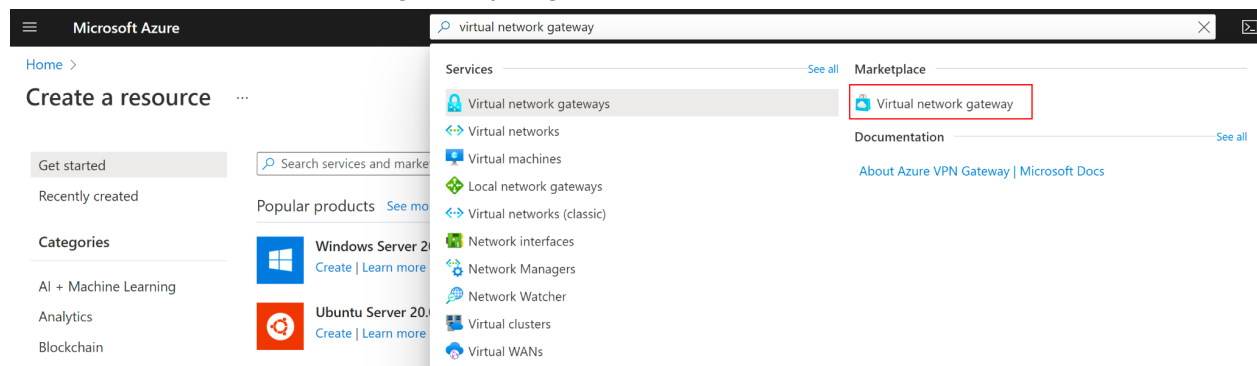
1. Deploy VMs (or use existing ones) in both VNet1 and VNet2.
2. Obtain the private IP addresses of these VMs. Let's say VM1 is in VNet1 and VM2 is in VNet2.
3. RDP or SSH into VM1.
4. From VM1, try to RDP the private IP address of VM2.
5. If the peering is set up correctly and there are no Network Security Group (NSG) rules blocking traffic, you should receive a response from VM2.
6. Play with the peering configurations
 - a. One way peering

Create Azure Virtual Network (VNet)

7. Login to the Azure Portal:
 - a. Open your web browser and navigate to the Azure Portal.
 - b. Sign in with your Azure account credentials.
8. Navigate to Virtual Networks:
 - a. In the left-hand side menu, click on "Create a resource."
 - b. In the "Search the Marketplace" box, type "Virtual Network" and select it from the dropdown.
9. Initiate VNet Creation:
 - a. Click on the "Create" button.
10. Fill in the Basic Details:
 - a. Subscription: Choose the appropriate Azure subscription.
 - b. Resource Group: Either select an existing resource group or create a new one.
 - c. Name: Provide a name for the Virtual Network. E.g., "MyVNet"
 - d. Region: Choose a region where you want the VNet to reside.
11. IP Addresses Configuration:
 - a. IPv4 Address space: Define an address range for the VNet. For this example, let's use 10.4.0.0/16.
12. Security Options:
 - a. You can leave the default options or configure DDoS protection and firewall as per your requirements.
 - b. Click on the "Review + create" button, then on the next screen, click "Create."

Create an azure VPN Gateway

1. In Search resources, services, and docs (G+/) type virtual network gateway. Locate Virtual network gateway in the Marketplace search results and select it to open the Create virtual network gateway page.



2. On the Basics tab, fill in the values for Project details and Instance details.
 - a. Subscription: Select the subscription you want to use from the dropdown.

- b. Resource Group: This setting is autofilled when you select your virtual network on this page.
- c. Name: Name your gateway. Naming your gateway not the same as naming a gateway subnet. It's the name of the gateway object you're creating.
- d. Region: Select the region in which you want to create this resource. The region for the gateway must be the same as the virtual network.
- e. Gateway type: Select VPN. VPN gateways use the virtual network gateway type VPN.
- f. SKU: Select the gateway SKU that supports the features you want to use from the dropdown. See Gateway SKUs. In the portal, the SKUs available in the dropdown depend on the VPN type you select. The Basic SKU can only be configured using Azure CLI or PowerShell. You can't configure the Basic SKU in the Azure portal.
- g. Generation: Select the generation you want to use. We recommend using a Generation2 SKU. For more information, see Gateway SKUs.
- h. Virtual network: From the dropdown, select the virtual network to which you want to add this gateway. If you can't see the VNet for which you want to create a gateway, make sure you selected the correct subscription and region in the previous settings.
- i. Gateway subnet address range: This field only appears if your VNet doesn't have a gateway subnet. It's best to specify /27 or larger (/26,/25 etc.). This allows enough IP addresses for future changes, such as adding an ExpressRoute gateway. If you already have a gateway subnet, you can view GatewaySubnet details by navigating to your virtual network. Select Subnets to view the range. If you want to change the range, you can delete and recreate the GatewaySubnet.

Create virtual network gateway ...

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more](#) ↗

Project details

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

Subscription * Content Development ▼

Resource group ⓘ TestRG1 (derived from virtual network's resource group)

Instance details

Name * VNet1GW ✓

Region * East US ▼

Gateway type * ⓘ ☒ VPN ☐ ExpressRoute

SKU * ⓘ VpnGw2 ▼

Generation ⓘ Generation2 ▼

Virtual network * ⓘ VNet1 ▼

[Create virtual network](#)


ⓘ Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range * ⓘ 10.1.255.0/27 ✓


10.1.255.0 - 10.1.255.31 (32 addresses)


3. Specify in the values for Public IP address. These settings specify the public IP address object that gets associated with the
4. VPN gateway. The public IP address is assigned to this object when the VPN gateway is created. The only time the primary public IP address changes is when the gateway is deleted and re-created. It doesn't change across resizing, resetting, or other internal maintenance/upgrades of your VPN gateway.
 - a. Public IP address type: For this exercise, if you have the option to choose the address type, select Standard.
 - b. Public IP address: Leave Create new selected.
 - c. Public IP address name: In the text box, type a name for your public IP address instance.
 - d. Public IP address SKU: Setting is autoselected.

- e. Assignment: The assignment is typically autoselected and can be either Dynamic or Static.
- f. Enable active-active mode: Select Disabled. Only enable this setting if you're creating an active-active gateway configuration.
- g. Configure BGP: Select Disabled, unless your configuration specifically requires this setting. If you do require this setting, the default ASN is 65515, although this value can be changed.

Public IP Address Type  ☐ Basic ☒ Standard


Public IP address


Public IP address *  ☒ Create new ☐ Use existing

Public IP address name * 

Public IP address SKU Standard

Assignment ☐ Dynamic ☒ Static

Enable active-active mode *  ☐ Enabled ☒ Disabled

Configure BGP *  ☐ Enabled ☒ Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

[Review + create](#)

[Previous](#)

[Next : Tags >](#)

[Download a template for automation](#)

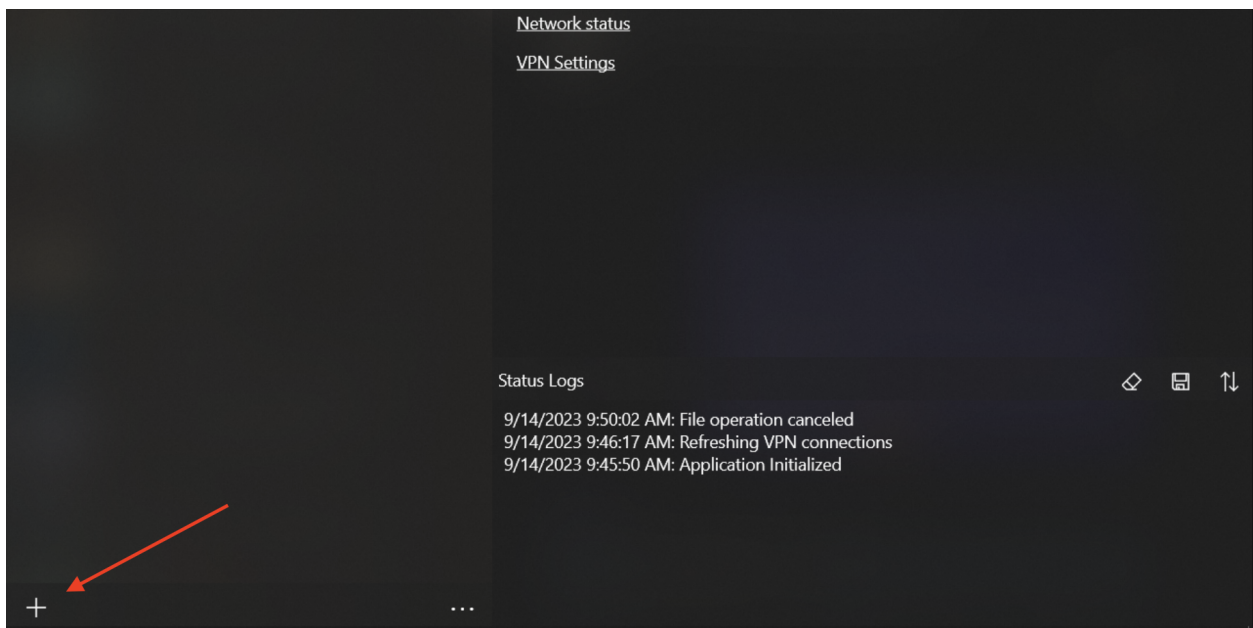
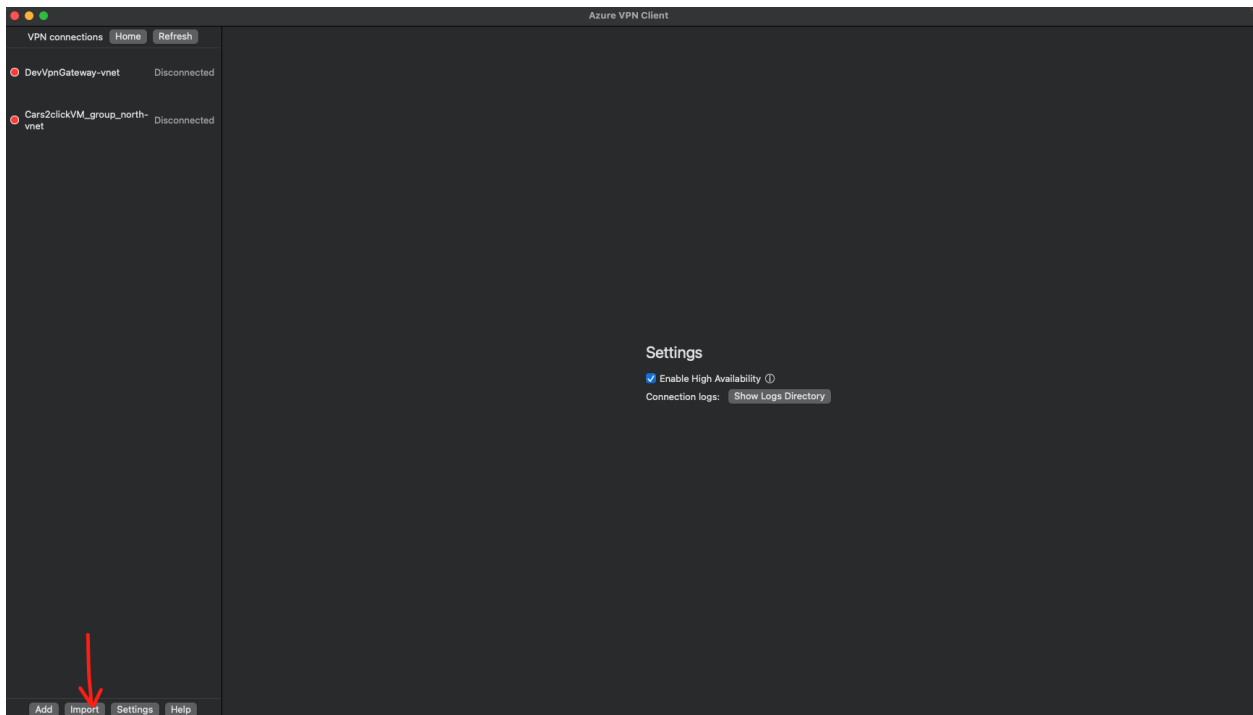
5. Select Review + create to run validation.
6. Once validation passes, select Create to deploy the VPN gateway.

Configure Point-to-Site Configuration

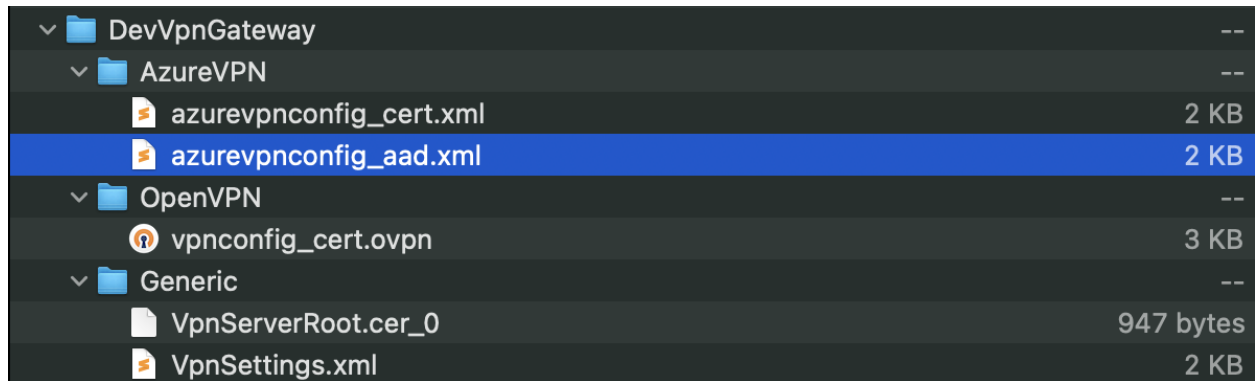
1. Once the VNet Gateway is deployed, go to its settings.
2. Under the Settings section, select Point-to-site configuration.
3. Click Configure now.
4. Specify the address pool that VPN clients receive when connecting. Ensure that this doesn't overlap with the address spaces you're using in your VNet. 172.16.201.0/24
5. Choose the Tunnel type: OpenVPN(SSL)
6. For authentication type, you can choose Azure certificate Azure Active Directory
7. Setup:
 - a. Tenant: <https://login.microsoftonline.com/TenantID>
 - b. Audience: 41b23e61-6c1e-4545-b367-cd054e0ed4b4
 - c. Issuer: <https://sts.windows.net/TenantID/>
8. Save
9. Download VPN client

Setup Azure VPN Client

1. Download Azure VPN Client from <https://apps.microsoft.com/store/detail/azure-vpn-client/9NP355QT2SQB?hl=en-us&gl=us> and install it
2. Open Azure VPN client, and click on the plus sign/import on the bottom left



3. Click on import and navigate to the unzip files, go to Azure VPN folder, and select "azurevpnconfig_aad.xml"



▼	DevVpnGateway	--
▼	AzureVPN	--
	azurevpnconfig_cert.xml	2 KB
	azurevpnconfig_aad.xml	2 KB
▼	OpenVPN	--
	vpnconfig_cert.ovpn	3 KB
▼	Generic	--
	VpnServerRoot.cer_0	947 bytes
	VpnSettings.xml	2 KB

4. All the fields required for the connection should be auto filled on the right side of the screen.

Azure VPN Client

DevVpnGateway-vnet

VPN Server

azuregateway-7c060069-b054-409a-9c04-8906702dc ⓘ

Server Validation

Certificate Information

DigiCert Global Root CA ⓘ

Server Secret

..... ⓘ

Client Authentication

Authentication Type

Azure Active Directory ⓘ

Tenant

https://login.microsoftonline.com/754b003a-1dfd-46c5-l ⓘ

Audience

41b23e61-6c1e-4545-b367-cd054e0ed4b4 ⓘ

Issuer

https://sts.windows.net/754b003a-1dfd-46c5-8fe3-f983 ⓘ

Clear Saved Account ⓘ

Save Cancel

5. Click on Save
6. Click on the Connect button, and use your local AD account for authentication
7. Test the connection

Azure vNet-to-vNet Connections

<https://doc.primekey.com/ejbca-cloud/ejbca-cloud-azure/azure-va-configuration-and-administration-guide/azure-vnet-to-vnet-connections>

Create a Private DNS Zone

1. Login to the Azure Portal:
 - a. Navigate to <https://portal.azure.com> and sign in with your Azure account.
2. Go to the 'Private DNS zones' Service:
 - a. In the left-hand menu, click on "Create a resource".
 - b. In the search box, type "Private DNS zones" and select it.
 - c. Click on the + Add button to create a new private DNS zone.
3. Fill in the Basics:
 - a. Select your Subscription and Resource Group (or create a new resource group).
 - b. Enter a name for the private DNS zone (e.g., myprivatezone.local).
 - c. Select the desired region (usually the same region as your VNet).
4. Review and Create:
 - a. Review the settings.
 - b. Click on Review + create, then click Create.

Link the Private DNS Zone to a VNet

1. Navigate to the Created Private DNS Zone:
 - a. From the Azure portal dashboard, go to Resource groups.
 - b. Select your resource group and click on the private DNS zone you just created.
2. Link to VNet:
 - a. In the DNS zone's left menu, under the Settings section, click on Virtual network links.
 - b. Click on the + Add button to create a new link.
3. Configure the Link:
 - a. Provide a name for the link.
 - b. Choose your Subscription (if it's not already selected).
 - c. For the Virtual Network, select the desired VNet from the dropdown list.
 - d. Set Registration to 'Yes' if you want the DNS records of the VMs in the VNet to be automatically registered in this DNS zone. Otherwise, set it to 'No'.
 - e. Click OK to create the link.

Create a DNS resolver inside the virtual network

1. Open the Azure portal and search for DNS Private Resolvers.
2. Select DNS Private Resolvers, select Create, and then on the Basics tab for Create a DNS Private Resolver enter the following:
 - a. Subscription: Choose the subscription name you're using.

- b. Resource group: Choose the name of the resource group that you created.
- c. Name: Enter a name for your DNS resolver (ex: mydnsresolver).
- d. Region: Choose the region you used for the virtual network.
- e. Virtual Network: Select the virtual network that you created.
- f. Don't create the DNS resolver yet.

Home > DNS Private Resolvers >

Create a DNS Private Resolver ...

Basics Inbound Endpoints Outbound Endpoints Ruleset Tags Review + Create

Azure DNS private resolver bridges on-premises DNS namespaces with private DNS zones hosted on Azure DNS without the burden of deploying VM-based custom DNS servers. You can resolve DNS queries from on-premises networks and do conditional forwarding to on-premises DNS zones. [Learn more](#)

Project details

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

Subscription ⓘ *

Resource group ⓘ * [Create new](#)

Instance details

Private resolver is a regional service. Only virtual networks and rulesets in the same region can use this private resolver.

Name *

Region *

ⓘ DNS private resolver and rulesets are currently not supported in westus2 region(s).

ⓘ DNS Private Resolver and Virtual Network must exist in same location, hence the region selected here will affect the available virtual networks for selection.

Virtual Network

Select a virtual network for your private resolver and endpoints. [Learn more](#)

Virtual Network ⓘ *

3. Select the Inbound Endpoints tab, select Add an endpoint, and then enter a name next to Endpoint name (ex: myinboundendpoint).
4. Next to Subnet, select the inbound endpoint subnet you created (ex: snet-inbound, 10.0.0.0/28) and then select Save.