How-To Library

Informatica

Connecting to Microsoft Azure Synapse SQL using an Azure private endpoint

Abstract

You can use an Azure private endpoint to securely and privately connect to your Microsoft Azure Synapse SQL account on a virtual network. This article explains how to configure an Azure private endpoint in the Azure portal.

Supported Versions

- Informatica Cloud® Data Integration Microsoft Azure Synapse SQL Connector

Table of Contents

Overview

A private endpoint is a network interface for an Azure service in your virtual network. When you create a private endpoint for your Microsoft Azure Synapse SQL account, it provides secure connectivity between clients on your virtual network and your Microsoft Azure Synapse SQL account. The private endpoint is assigned an IP address from the IP address range of your virtual network.

Before you connect to Microsoft Azure Synapse SQL using an Azure private endpoint, perform the following prerequisite tasks in Azure:

1. Create a network security group (optional).
2. Create a virtual network.
3. Add a subnet to the virtual network.
4. Create a virtual machine.
5. Create an Azure private endpoint.
6. Create a virtual network link.
7. Verify the Azure private endpoint configuration.

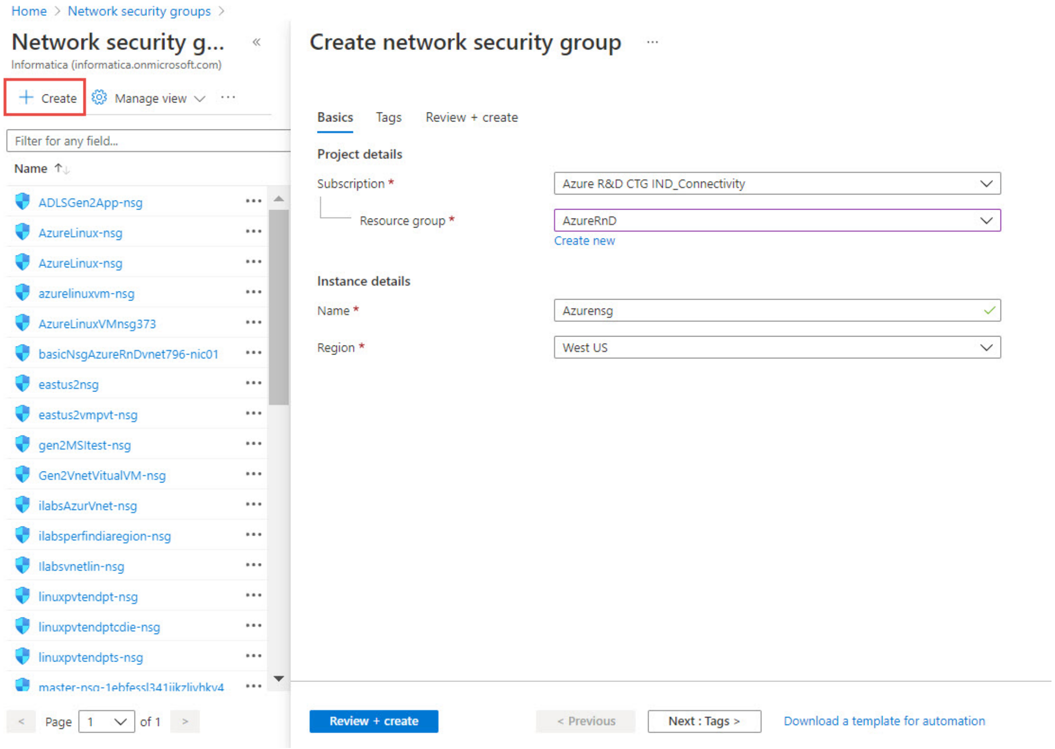
Create a network security group

Create a network security group to allow or deny access to Azure resources in an Azure Virtual Network.

A network security group consists of a set of access control rules that allow or deny access to the resources in an Azure Virtual Network. You can associate a network security group to subnets or individual network interfaces attached to virtual machines.

A network security group is not a mandatory requirement to use an Azure private endpoint.

1. Log in to the Azure portal.
2. In the search box, enter **Network security groups** , and select **Network security groups** in the search results.
3. On the **Network security groups**, click **Create**.
4. On the **Basics** tab, enter the project and instance details.



ADLSGen2App-nsg
AzureLinux-nsg
AzureLinux-nsg
azurelinuxvm-nsg
AzureLinuxVMnsg373
basicNsgAzureRnDvnet796-nic01
eastus2nsg
eastus2vmpvt-nsg
gen2MSItest-nsg
Gen2VnetVitualVM-nsg
ilabsAzurVnet-nsg
ilabsperfindiaregion-nsg
Ilabsvnetlin-nsg
linuxpvtendpt-nsg
linuxpvtendptcdie-nsg
linuxpvtendpts-nsg
master-nsg-1ebfesl341jikzlivhkv4

Project details

Subscription * Azure R&D CTG IND_Connectivity

Resource group * AzureRnD

Instance details

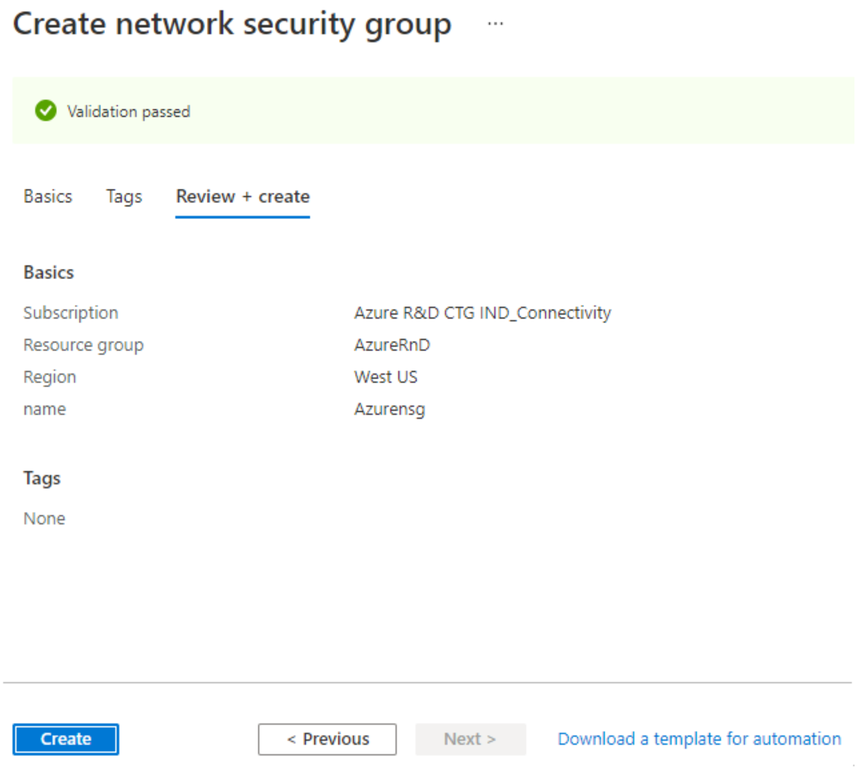
Name * Azurensg

Region * West US

   a. In the **Subscription** field, select your subscription for which you want to create the virtual network.
   b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.
   c. In the **Name** field, enter a name for the network security group.
   d. In the **Region** field, select the region.

      Note: Ensure that the network security group, the virtual network, and all the Azure resources are in the same region.

5. Click **Review + Create**, verify the configurations, and click **Create**.


Create network security group

Validation passed

Basics

Subscription Azure R&D CTG IND_Connectivity
Resource group AzureRnD
Region West US
name Azurensg

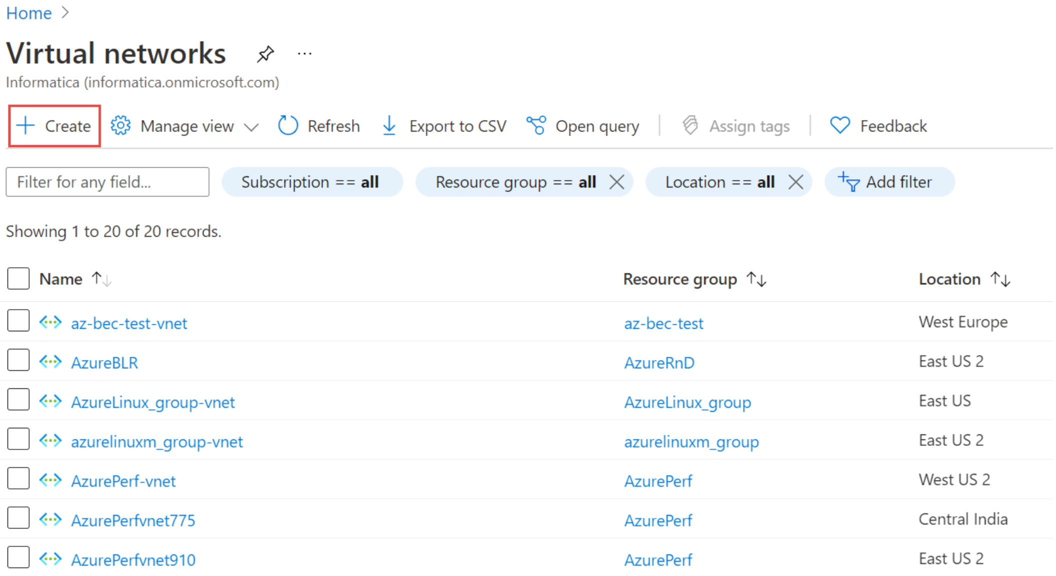
Tags

None

Create a virtual network

Create an Azure Virtual Network to allow Azure resources, such as Azure Virtual Machines, to securely communicate with each other, the internet, and on-premises networks.

1. In the search box, enter **Virtual networks**, and select **Virtual networks** in the search results.
2. On the **Virtual networks** page, click **Create**.



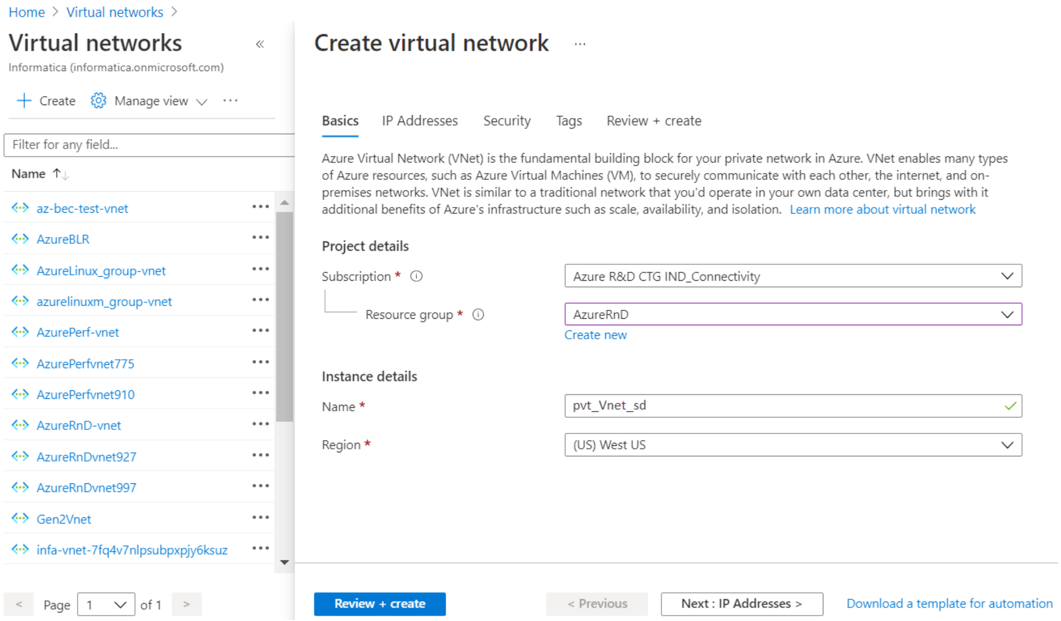
Virtual networks

Informatica (informatica.onmicrosoft.com)

Showing 1 to 20 of 20 records.

Name	Resource group	Location
az-bec-test-vnet	az-bec-test	West Europe
AzureBLR	AzureRnD	East US 2
AzureLinux_group-vnet	AzureLinux_group	East US
azurelinuxm_group-vnet	azurelinuxm_group	East US 2
AzurePerf-vnet	AzurePerf	West US 2
AzurePerfvnet775	AzurePerf	Central India
AzurePerfvnet910	AzurePerf	East US 2

3. On the **Basics** tab, enter the project and instance details.



Home > Virtual networks >

Virtual networks

Informatica (informatica.onmicrosoft.com)

+ Create | Manage view | ···

Filter for any field...

Name ↑↓

- az-bec-test-vnet
- AzureBLR
- AzureLinux_group-vnet
- azurelinuxm_group-vnet
- AzurePerf-vnet
- AzurePerfvnet775
- AzurePerfvnet910
- AzureRnD-vnet
- AzureRnDvnet927
- AzureRnDvnet997
- Gen2Vnet
- infa-vnet-7fq4v7nlpsubpxpjy6ksuz

< Page 1 of 1 >

Create virtual network ···

Basics | IP Addresses | Security | Tags | Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. Learn more about virtual network

Project details

Subscription * : Azure R&D CTG IND_Connectivity

Resource group * : AzureRnD

Create new

Instance details

Name * : pvt_Vnet_sd ✓

Region * : (US) West US

Review + create | < Previous | Next : IP Addresses > | Download a template for automation

a. In the **Subscription** field, select your subscription for which you want to create the virtual network.

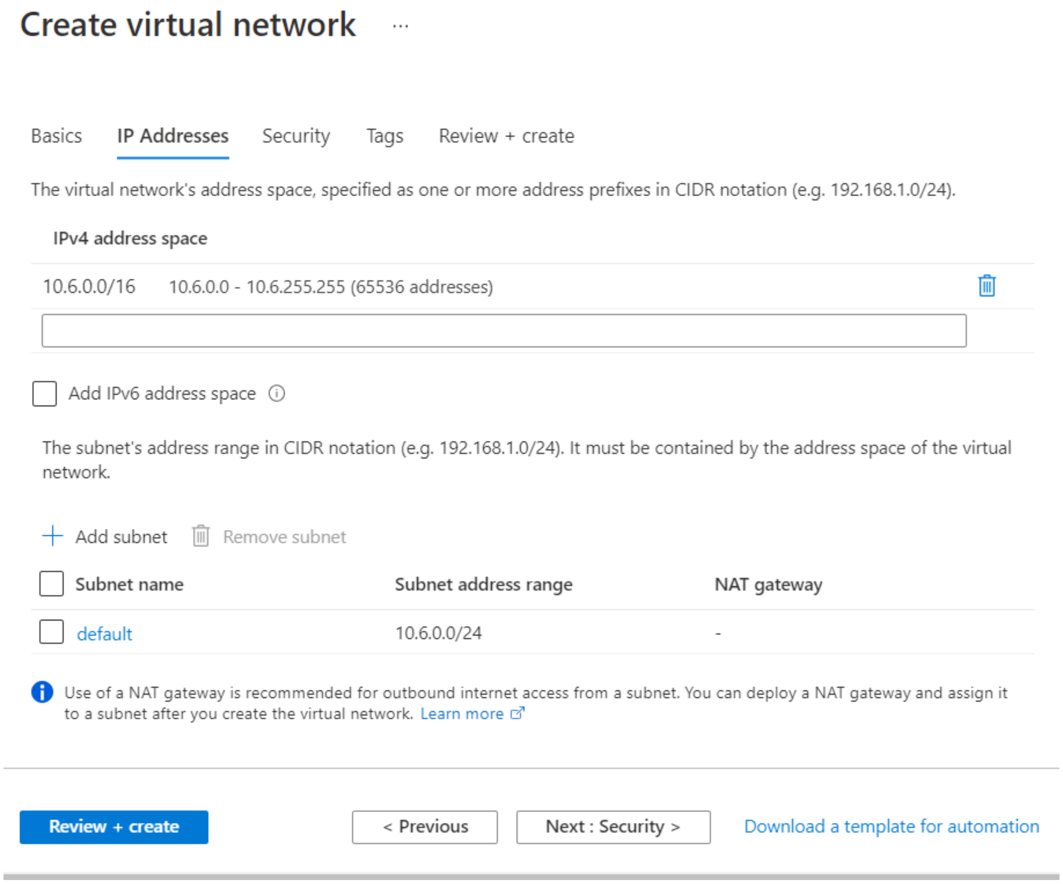
b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

c. In the **Name** field, enter a name for the virtual network.

d. In the **Region** field, select the region.

   Note: Ensure that the virtual network and all the Azure resources are in the same region.

4. Click **Next: IP Addresses**.
   The IP Addresses tab shows the IP address space of the virtual network and the address range of the subnet.



The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space	
10.6.0.0/16	10.6.0.0 - 10.6.255.255 (65536 addresses)

□ Add IPv6 address space

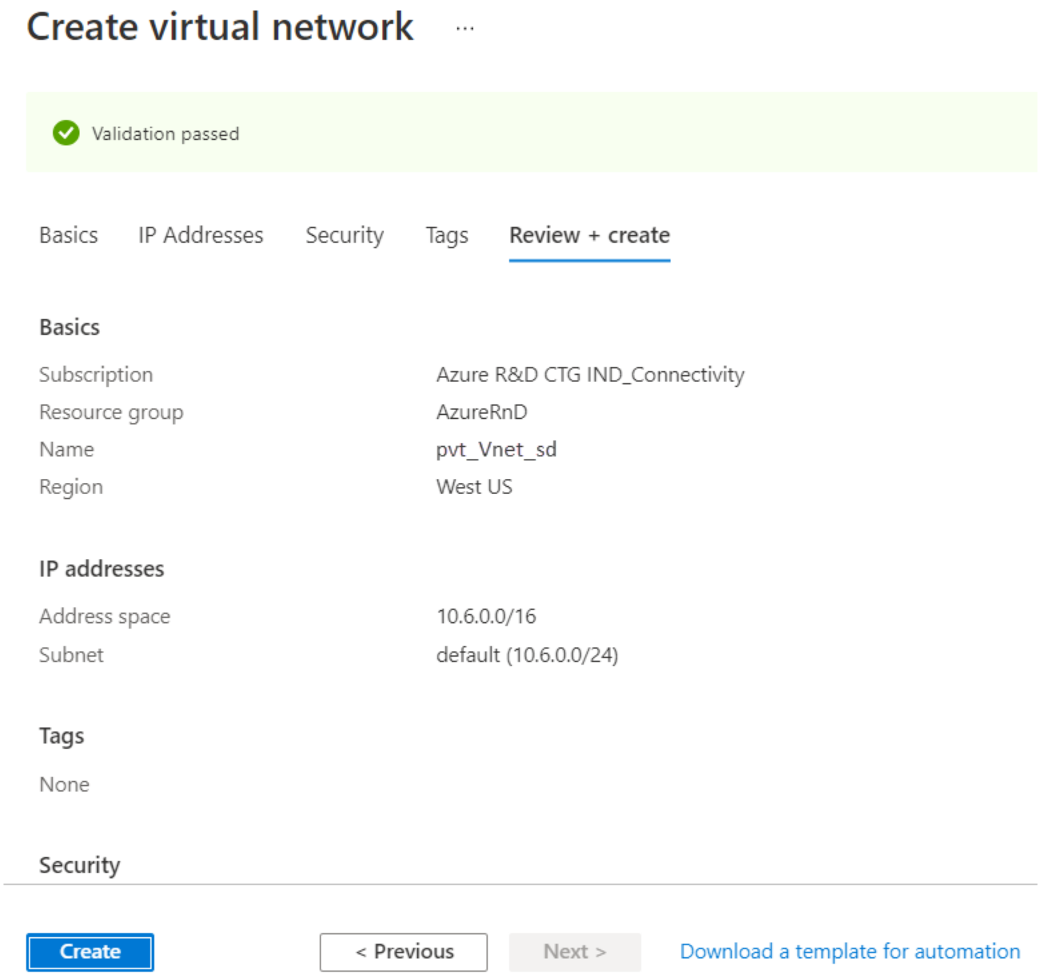
The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

□ Subnet name	Subnet address range	NAT gateway
□ default	10.6.0.0/24	-

Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. Learn more

You can use the default subnet or add a new subnet. The subnet address range must be contained by the address space of the virtual network.

5. Click **Review + Create**, verify the configurations, and click **Create**.



Create virtual network

Validation passed

Basics

Subscription	Azure R&D CTG IND_Connectivity
Resource group	AzureRnD
Name	pvt_Vnet_sd
Region	West US

IP addresses

Address space	10.6.0.0/16
Subnet	default (10.6.0.0/24)

Tags

None

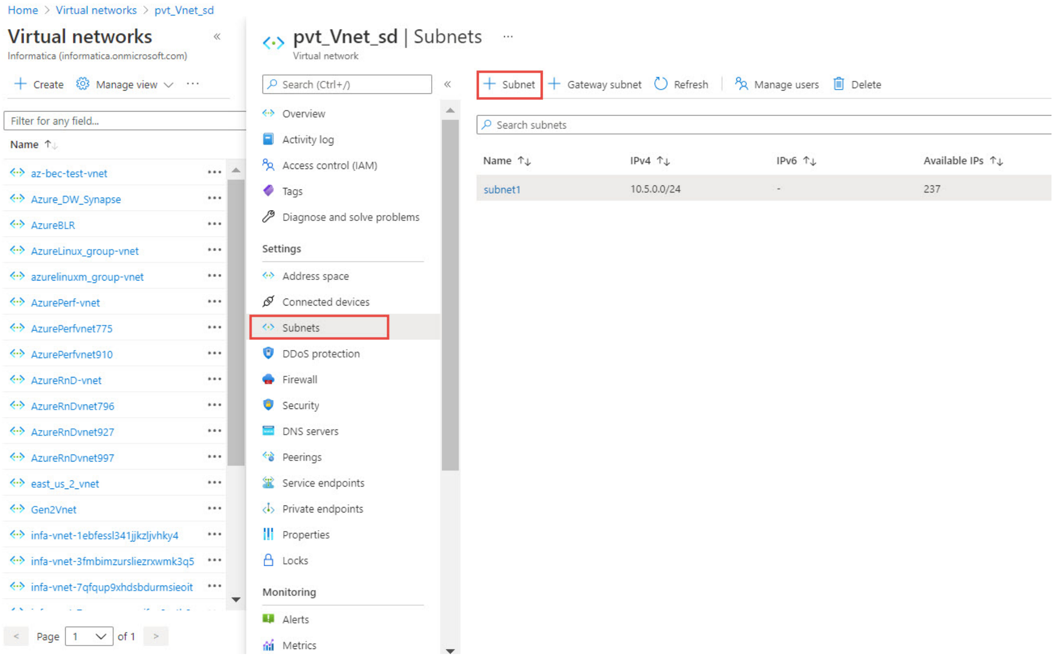
Security

Add a subnet to the virtual network

Add a subnet to the virtual network to deploy the Azure resources.

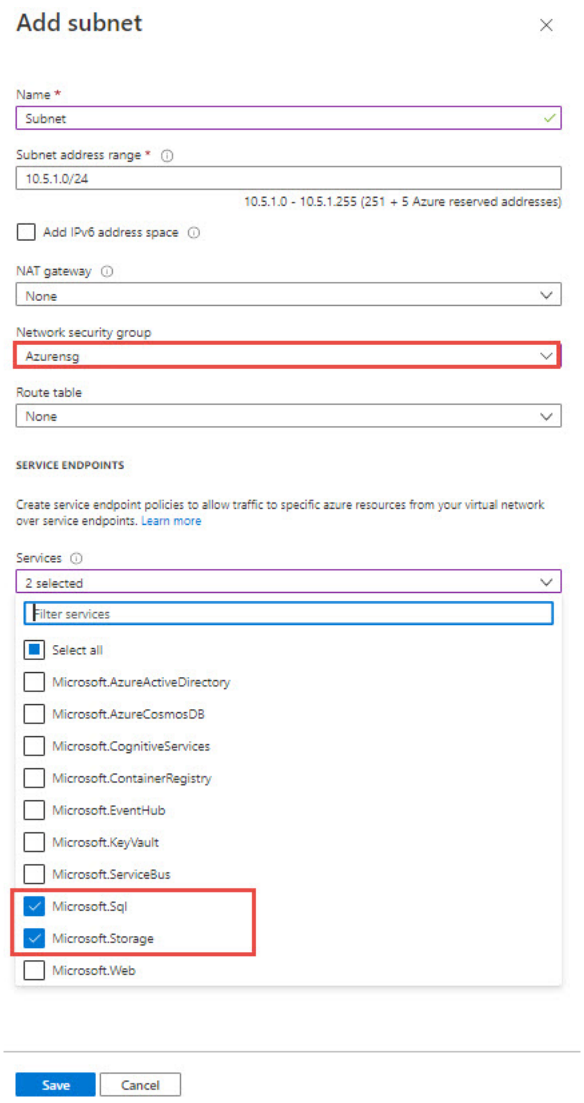
A subnet is a range of IP addresses in the virtual network. You can segment the virtual network into one or more subnetworks and allocate a portion of the virtual network's address space to each subnet. You can then deploy Azure resources in a specific subnet.

1. Go to the virtual network that you created.
2. Under **Settings**, click **Subnets**.



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓
subnet1	10.5.0.0/24	-	237

3. Click **Subnet**.
   The **Add subnet** page appears.



Add subnet

Name *
Subnet

Subnet address range *
10.5.1.0/24
10.5.1.0 - 10.5.1.255 (251 + 5 Azure reserved addresses)

□ Add IPv6 address space

NAT gateway
None

Network security group
Azurensg

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
2 selected

Filter services

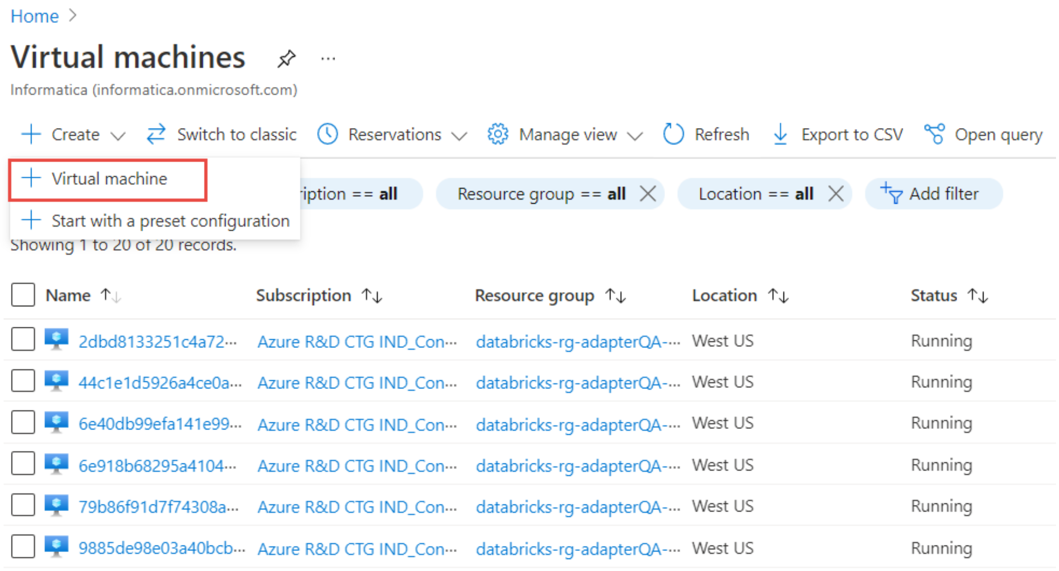
- ■ Select all
- □ Microsoft.AzureActiveDirectory
- □ Microsoft.AzureCosmosDB
- □ Microsoft.CognitiveServices
- □ Microsoft.ContainerRegistry
- □ Microsoft.EventHub
- □ Microsoft.KeyVault
- □ Microsoft.ServiceBus
- ☑ Microsoft.Sql
- ☑ Microsoft.Storage
- □ Microsoft.Web

4. In the **Name** field, enter a name for the subnet.
5. In the **Subnet address range** field, you can specify an address range as per your requirement or use the default subnet address range .
   The subnet address range must be contained by the address space of the virtual network. You can't edit the address range of a subnet which is in use.
6. In the **Network security group** field, select the network security group that you created. If you don't want to use a network security group, select **None**.
7. In the **Services** field, select **Microsoft.Sql** and **Microsoft.Storage**
8. Click **Save**.

Create a virtual machine in the subnet

Create an Azure virtual machine to host your applications in the cloud on Windows and Linux operating systems.

1. In the search box, enter **Virtual machines** , and select **Virtual machines** in the search results.
2. Click **Create** > **Virtual machine**.



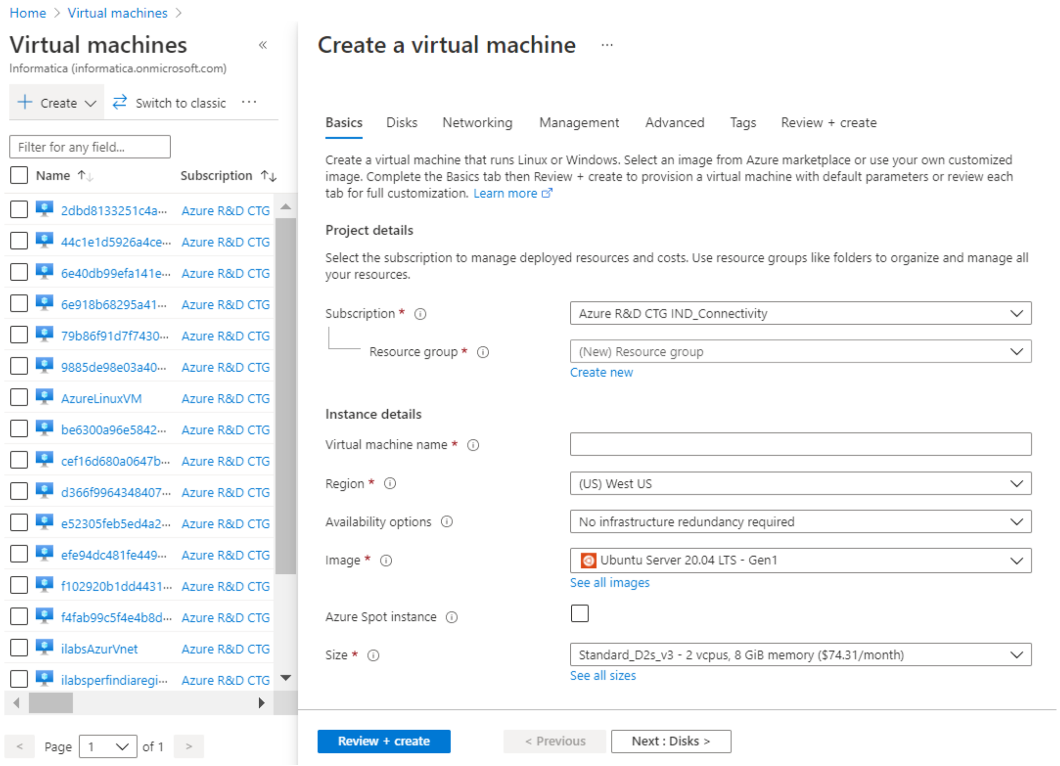
Virtual machines

Informatica (informatica.onmicrosoft.com)

Showing 1 to 20 of 20 records.

Name	Subscription	Resource group	Location	Status
2dbd8133251c4a72···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running
44c1e1d5926a4ce0a···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running
6e40db99efa141e99···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running
6e918b68295a4104···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running
79b86f91d7f74308a···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running
9885de98e03a40bcb···	Azure R&D CTG IND_Con···	databricks-rg-adapterQA-···	West US	Running

3. On the **Basics** tab, enter the project, instance, and authentication details.



Virtual machines

Informatica (informatica.onmicrosoft.com)

Name	Subscription
2dbd8133251c4a···	Azure R&D CTG
44c1e1d5926a4ce···	Azure R&D CTG
6e40db99efa141e···	Azure R&D CTG
6e918b68295a41···	Azure R&D CTG
79b86f91d7f7430···	Azure R&D CTG
9885de98e03a40···	Azure R&D CTG
AzureLinuxVM	Azure R&D CTG
be6300a96e5842···	Azure R&D CTG
cef16d680a0647b···	Azure R&D CTG
d366f9964348407···	Azure R&D CTG
e52305feb5ed4a2···	Azure R&D CTG
efe94dc481fe449···	Azure R&D CTG
f102920b1dd4431···	Azure R&D CTG
f4fab99c5f4e4b8d···	Azure R&D CTG
ilabsAzurVnet	Azure R&D CTG
ilabsperfindiaregi···	Azure R&D CTG

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. 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 * : Azure R&D CTG IND_Connectivity

Resource group * : (New) Resource group

Instance details

Virtual machine name * :

Region * : (US) West US

Availability options : No infrastructure redundancy required

Image * : Ubuntu Server 20.04 LTS - Gen1

Azure Spot instance : □

Size * : Standard_D2s_v3 - 2 vcpus, 8 GiB memory ($74.31/month)

a. In the **Subscription** field, select the subscription for which you want to create the virtual machine.

b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

c. In the **Virtual machine name** field, enter a name for the virtual machine.
Once you create the virtual machine, you can't change the virtual machine name.

d. In the **Region** field, select the region.

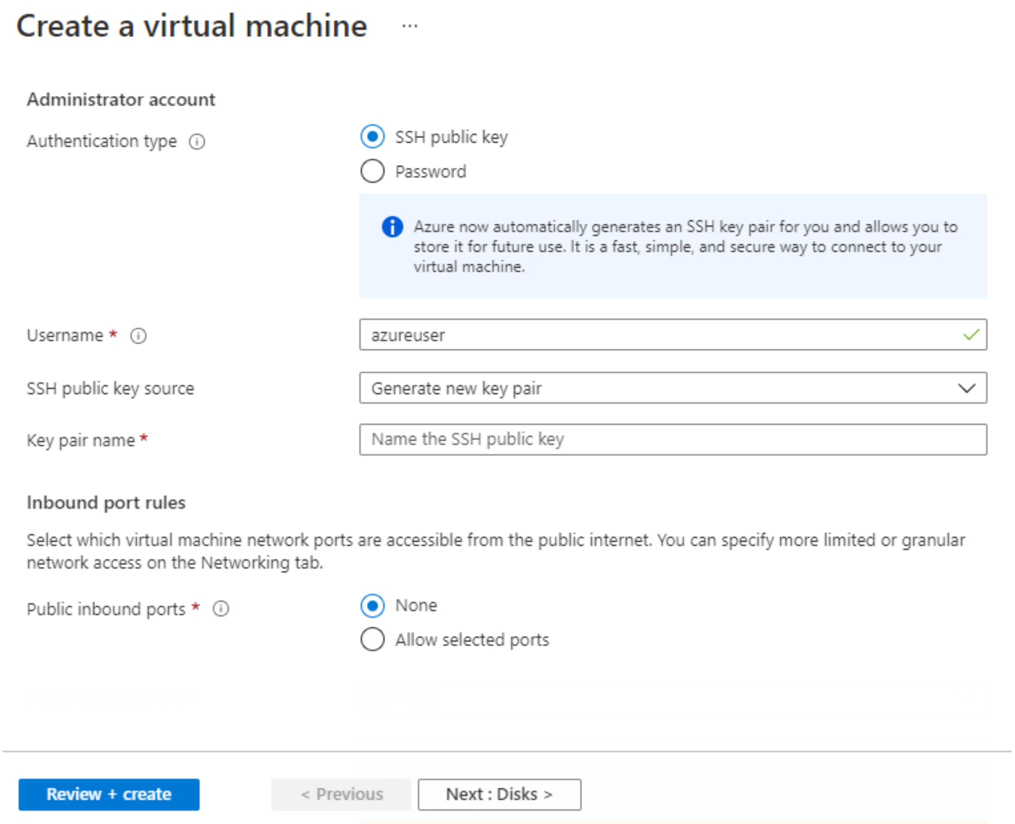
Note: Ensure that the subscription, resource group, and region for the virtual machine are the same as that of the virtual network.

e. In the **Availability** options field, you can choose to replicate the virtual machine in availability zones or availability sets to protect your applications and data from datacenter outages and maintenance events.

f. In the **Image** field, select the base operating system or application for the virtual machine.

g. In the **Size** field, select the size of the virtual machine that determines factors such as processing power, memory, and storage capacity.

h. In the **Authentication type** field, select if the administrator account must use the user name and password or SSH keys for authentication.



Create a virtual machine ···

Administrator account

Authentication type ⓘ ● SSH public key ○ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username * ⓘ azureuser ✓

SSH public key source: Generate new key pair

Key pair name *: Name the SSH public key

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ● None ○ Allow selected ports

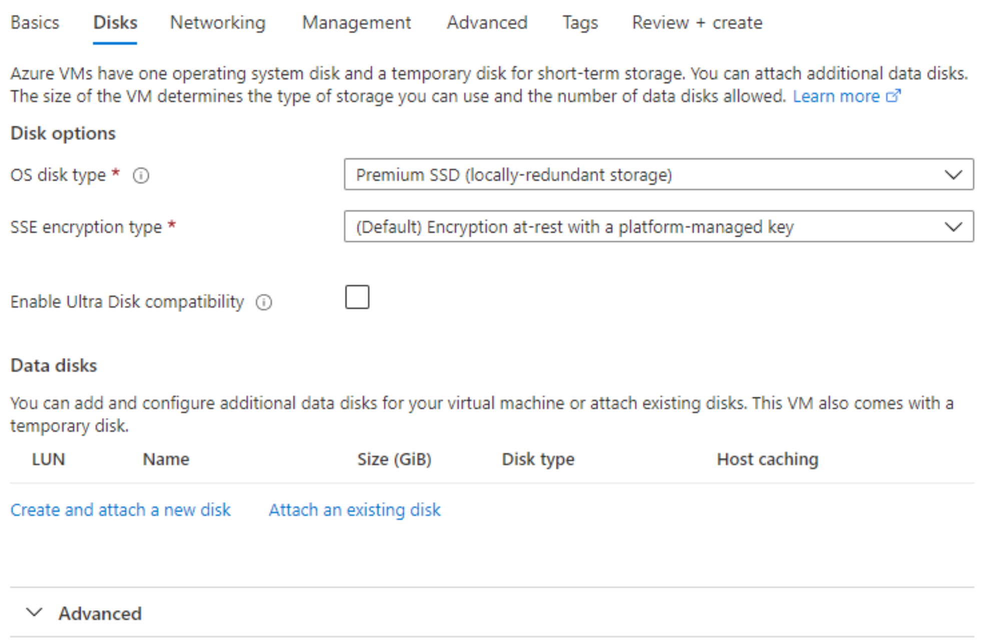
If you select the **SSH public key** option, enter the user name and key pair name.

If you select the **Password** option, enter the values in the username, password, and confirm password fields.

i. In the **Public inbound ports** field, select **None**.

j. Click **Next : Disks**.

4. On the **Disks** tab, you can select the disk type for your virtual machine or use the default disk type. You can also configure additional data disks or attach existing disks.



Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

Disk options

OS disk type * : Premium SSD (locally-redundant storage)

SSE encryption type * : (Default) Encryption at-rest with a platform-managed key

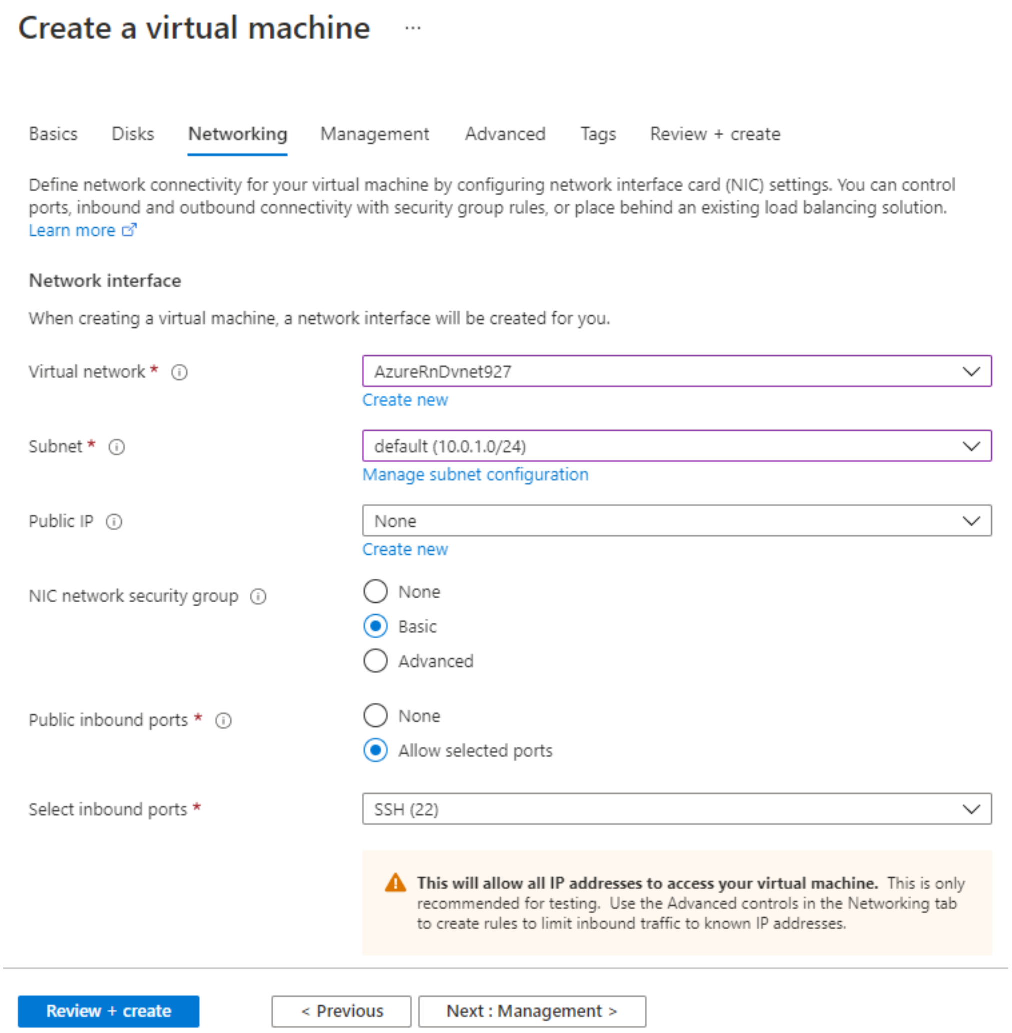
Enable Ultra Disk compatibility ☐

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching

5. Click **Next : Networking**.
6. On the **Networking** tab, select the virtual network and the subnet that you created, and then click **Review + create**.



Create a virtual machine ...

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : AzureRnDvnet927

Create new

Subnet * : default (10.0.1.0/24)

Manage subnet configuration

Public IP : None

Create new

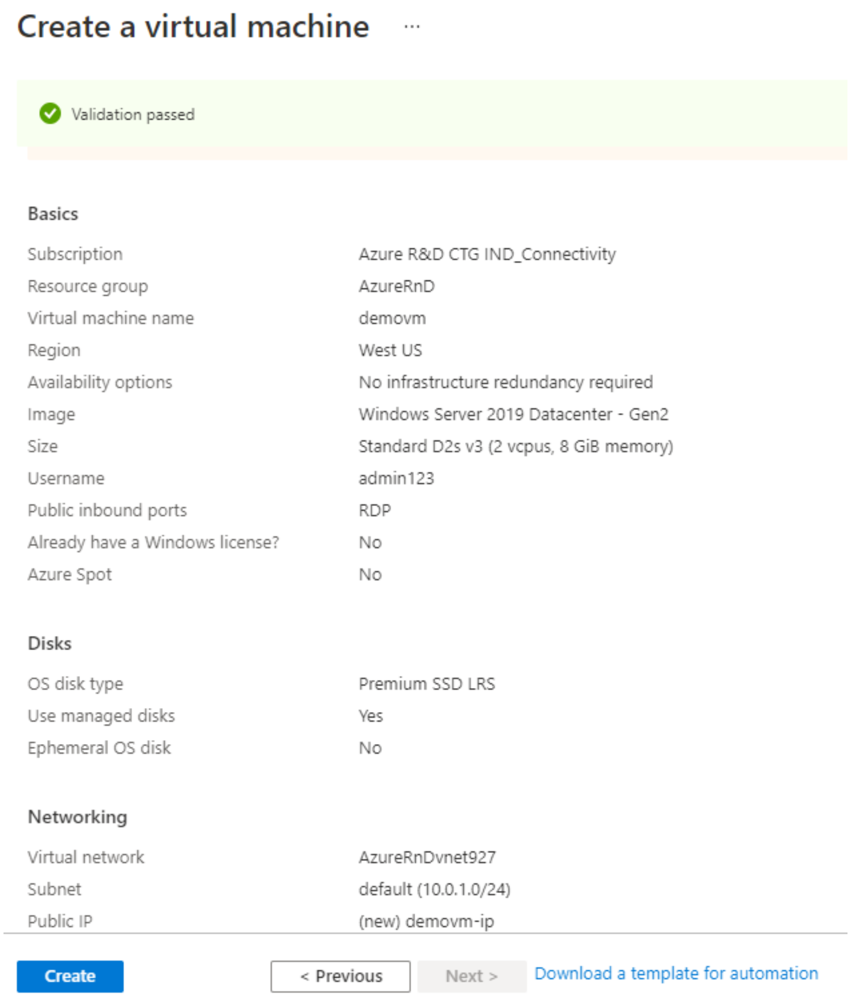
NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

7. On the **Review + create** tab, verify the configurations for the virtual machine.



Create a virtual machine ...

Validation passed

Basics

Subscription	Azure R&D CTG IND_Connectivity
Resource group	AzureRnD
Virtual machine name	demovm
Region	West US
Availability options	No infrastructure redundancy required
Image	Windows Server 2019 Datacenter - Gen2
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	admin123
Public inbound ports	RDP
Already have a Windows license?	No
Azure Spot	No

Disks

OS disk type	Premium SSD LRS
Use managed disks	Yes
Ephemeral OS disk	No

Networking

Virtual network	AzureRnDvnet927
Subnet	default (10.0.1.0/24)
Public IP	(new) demovm-ip

8. Click **Create**.

Create an Azure private endpoint

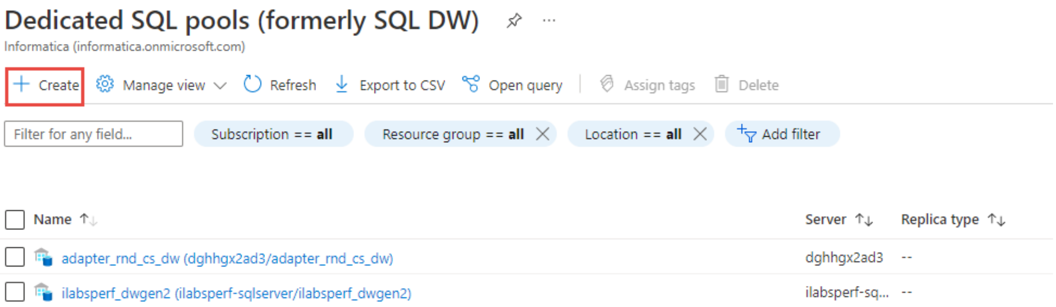
Create an Azure private endpoint for secured connectivity between clients on your virtual network and your Microsoft Azure Synapse SQL account.

You can create a private endpoint for an existing or a new Microsoft Azure Synapse SQL account.

Create a private endpoint for a new Microsoft Azure Synapse SQL account

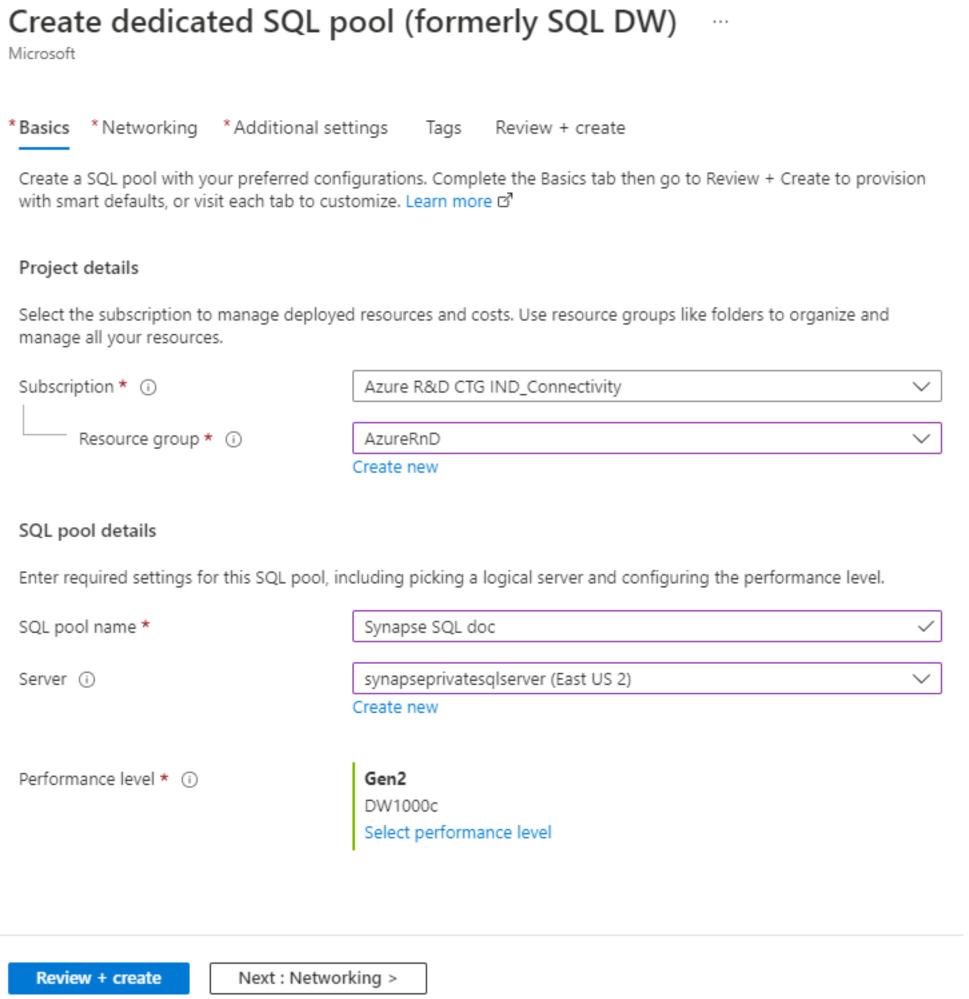
1. In the search box, enter **Dedicated SQL pools**, and then select **Dedicated SQL pools** in the search results.

2. On the **Dedicated SQL pools** page, click **Create** to create a new Microsoft Azure Synapse SQL account.



Name	Server	Replica type
adapter_rnd_cs_dw (dghhgx2ad3/adapter_rnd_cs_dw)	dghhgx2ad3	--
ilabsperf_dwgen2 (ilabsperf-sqlserver/ilabsperf_dwgen2)	ilabsperf-sq...	--

3. On the **Basics** tab, enter the project and SQL pool details.



Create a SQL pool with your preferred configurations. Complete the Basics tab then go to Review + Create to provision with smart defaults, or visit each tab to customize. 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 *: Azure R&D CTG IND_Connectivity

Resource group *: AzureRnD

Create new

SQL pool details

Enter required settings for this SQL pool, including picking a logical server and configuring the performance level.

SQL pool name *: Synapse SQL doc

Server: synapseprivatesqlserver (East US 2)

Create new

Performance level *: Gen2 DW1000c

Select performance level

a. In the **Subscription** field, select the subscription in which you want to create the account.

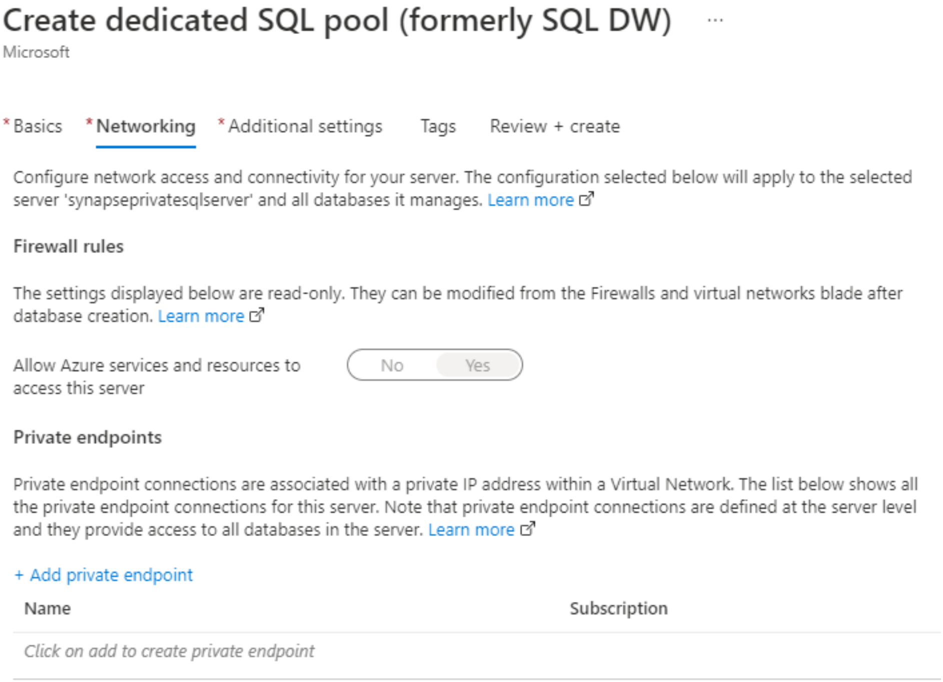
b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

c. In the **SQL pool name** field, enter a name for the Microsoft Azure Synapse SQL account.

   Note: The name must be unique in the server, must not exceed 60 characters in length, and must not contain reserved words.

d. In the **Server** field, select an existing SQL server or create a new server.

4. On the **Networking** tab, click **Add private endpoint**.



Create dedicated SQL pool (formerly SQL DW) ...

Microsoft

*Basics *Networking *Additional settings Tags Review + create

Configure network access and connectivity for your server. The configuration selected below will apply to the selected server 'synapseprivatesqlserver' and all databases it manages. Learn more

Firewall rules

The settings displayed below are read-only. They can be modified from the Firewalls and virtual networks blade after database creation. Learn more

Allow Azure services and resources to access this server: No [✓ Yes]

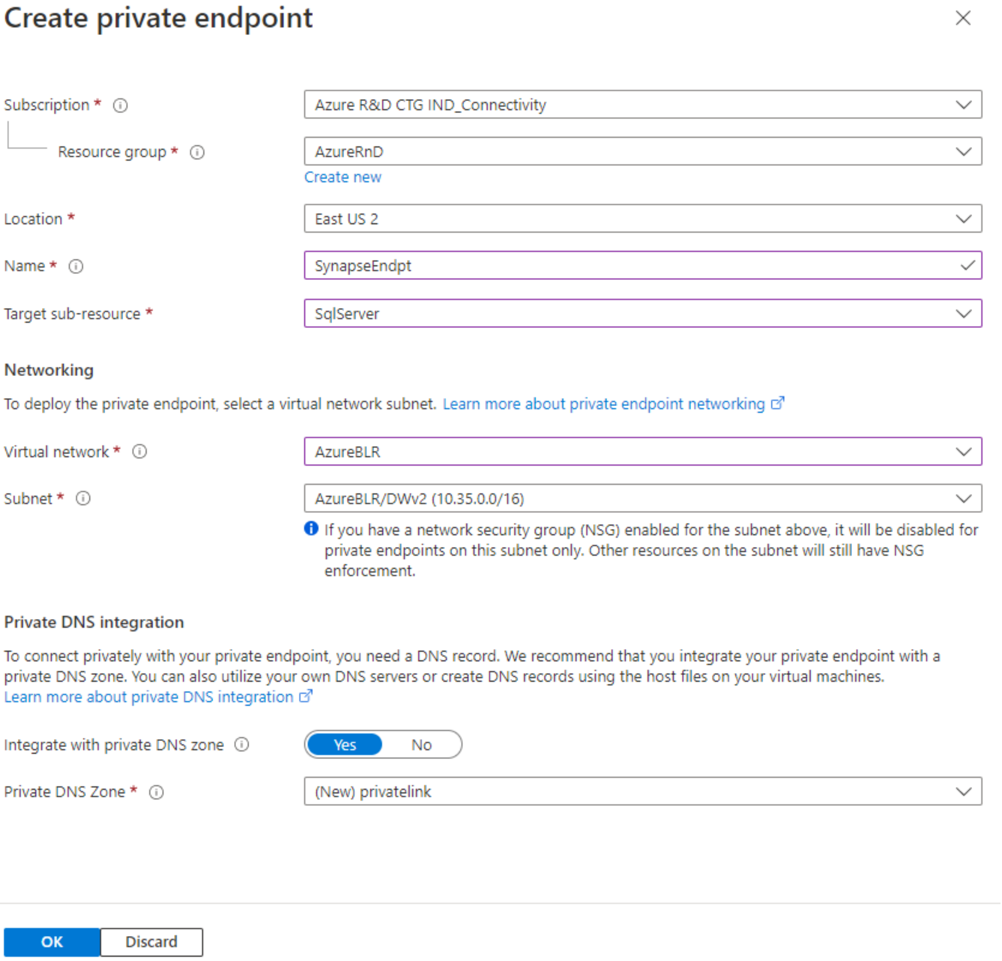
Private endpoints

Private endpoint connections are associated with a private IP address within a Virtual Network. The list below shows all the private endpoint connections for this server. Note that private endpoint connections are defined at the server level and they provide access to all databases in the server. Learn more

+ Add private endpoint

Name	Subscription
Click on add to create private endpoint	

a. In the **Subscription** field, select the subscription for which you want to create the private endpoint.



Create private endpoint

Subscription *	Azure R&D CTG IND_Connectivity
Resource group *	AzureRnD Create new
Location *	East US 2
Name *	SynapseEndpt
Target sub-resource *	SqlServer

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more about private endpoint networking

Virtual network *	AzureBLR
Subnet *	AzureBLR/DWv2 (10.35.0.0/16)

If you have a network security group (NSG) enabled for the subnet above, it will be disabled for private endpoints on this subnet only. Other resources on the subnet will still have NSG enforcement.

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more about private DNS integration

Integrate with private DNS zone	[✓ Yes] No
Private DNS Zone *	(New) privatelink

b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

c. In the **Location** field, select the location.

   Note: Ensure that the subscription, resource group, and location for the private endpoint are the same as that of the virtual network.

d. Enter a name for the private endpoint.

e. In the **Target sub-resource** field, select **SqlServer**.

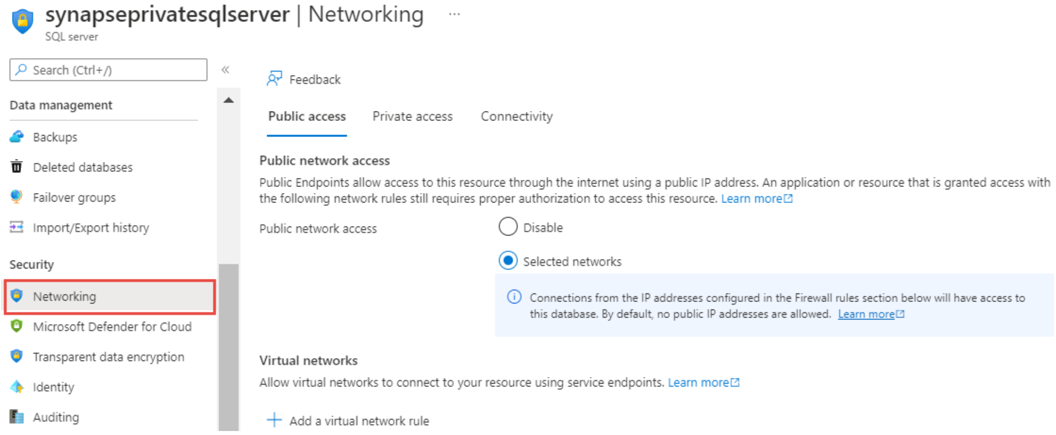
f. In the **Networking** section, select the virtual network and the subnet that you created.

g. Click **OK**

5. On the **Review + Create** tab, verify the details, and then click **Create**.

Create a private endpoint for an existing Microsoft Azure Synapse SQL account

1. Navigate to the SQL server that contains the Microsoft Azure Synapse SQL account for which you want to create a private endpoint.
2. Click **Networking**.



Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource. Learn more

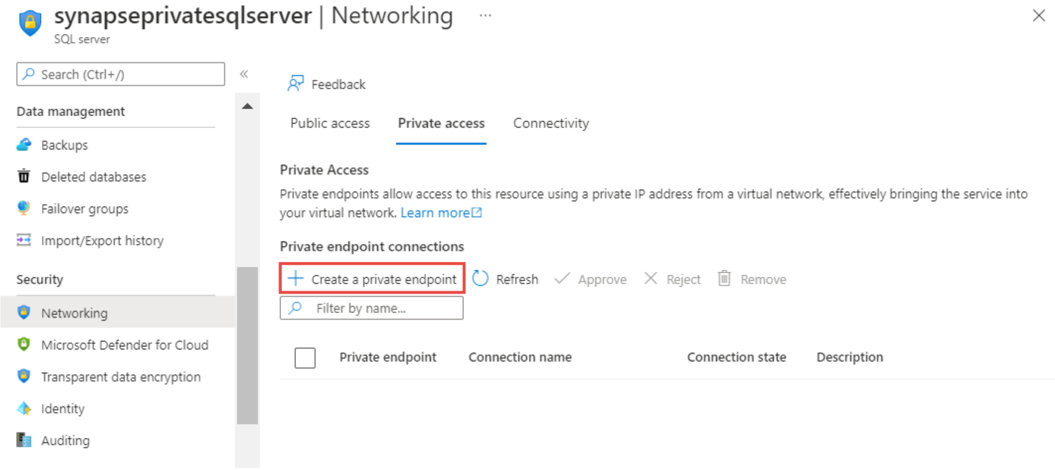
Public network access ○ Disable ● Selected networks

Connections from the IP addresses configured in the Firewall rules section below will have access to this database. By default, no public IP addresses are allowed. Learn more

Virtual networks

Allow virtual networks to connect to your resource using service endpoints. Learn more

3. On the **Public access** tab, select **Selected networks**.
4. On the **Private access** tab, click **Create a private endpoint**.



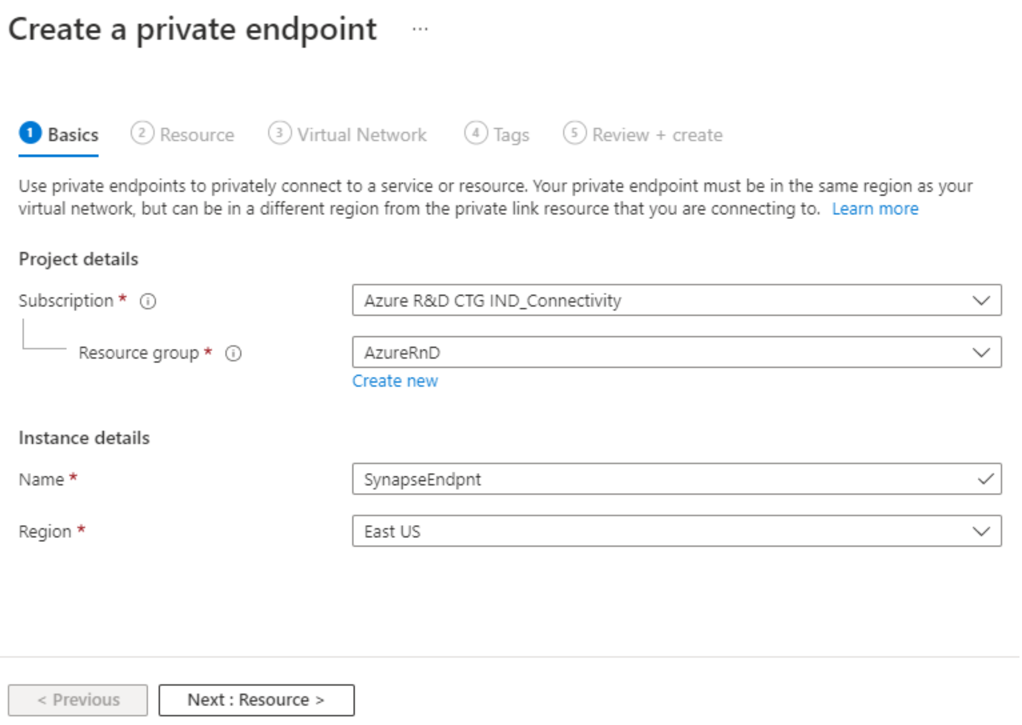
Private Access

Private endpoints allow access to this resource using a private IP address from a virtual network, effectively bringing the service into your virtual network. Learn more

Private endpoint connections

□	Private endpoint	Connection name	Connection state	Description

5. On the **Basics** tab, enter the project and instance details.



Create a private endpoint

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. Learn more

Project details

Subscription * : Azure R&D CTG IND_Connectivity

Resource group * : AzureRnD

Instance details

Name * : SynapseEndpnt

Region * : East US

a. In the **Subscription** field, select the subscription for which you want to create the private endpoint.

b. In the **Resource group** field, select the resource group in which the Azure resources are deployed and managed.

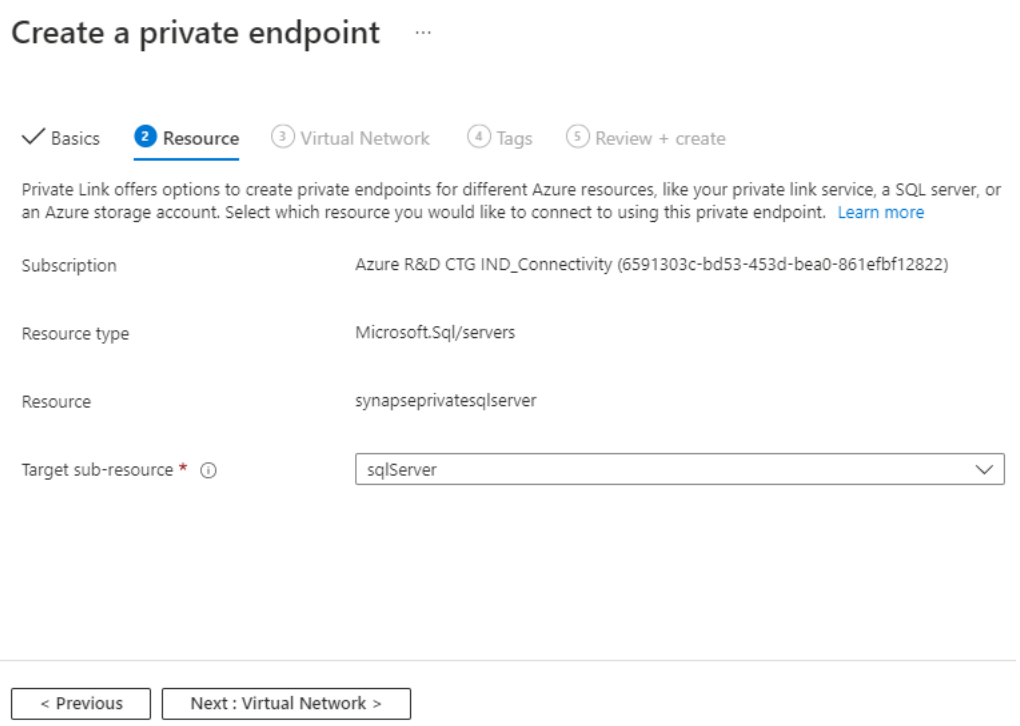
c. Enter a name for the private endpoint.

d. In the **Region** field, select the location for the private endpoint.

   Note: Ensure that the subscription, resource group, and location for the private endpoint are the same as that of the virtual network.

e. Click **Next : Resource**.

6. On the **Resource** tab, select the **Target sub-resource** as **sqlServer** and then click **Next : Virtual Network**.



Create a private endpoint ···

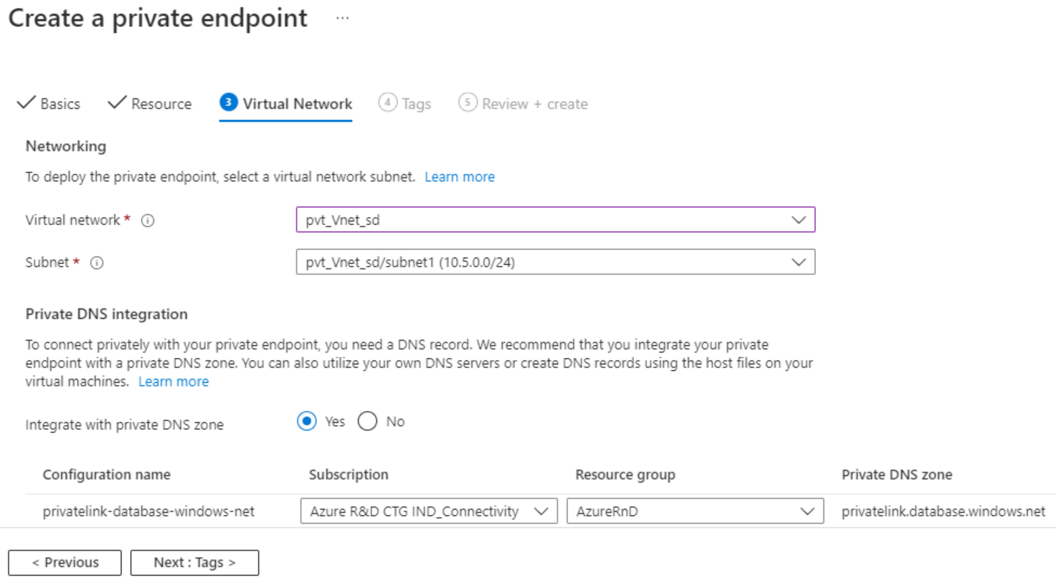
✓ Basics (2) Resource (3) Virtual Network (4) Tags (5) Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. Learn more

Subscription	Azure R&D CTG IND_Connectivity (6591303c-bd53-453d-bea0-861efbf12822)
Resource type	Microsoft.Sql/servers
Resource	synapseprivatesqlserver
Target sub-resource * ⓘ	sqlServer

< Previous Next : Virtual Network >

7. On the **Virtual Network** tab, select the virtual network and subnet that you created, and then click **Next : Tags**.



Create a private endpoint ···

✓ Basics ✓ Resource (3) Virtual Network (4) Tags (5) Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. Learn more

Virtual network * ⓘ	pvt_Vnet_sd
Subnet * ⓘ	pvt_Vnet_sd/subnet1 (10.5.0.0/24)

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. Learn more

Integrate with private DNS zone ● Yes ○ No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-database-windows-net	Azure R&D CTG IND_Connectivity	AzureRnD	privatelink.database.windows.net

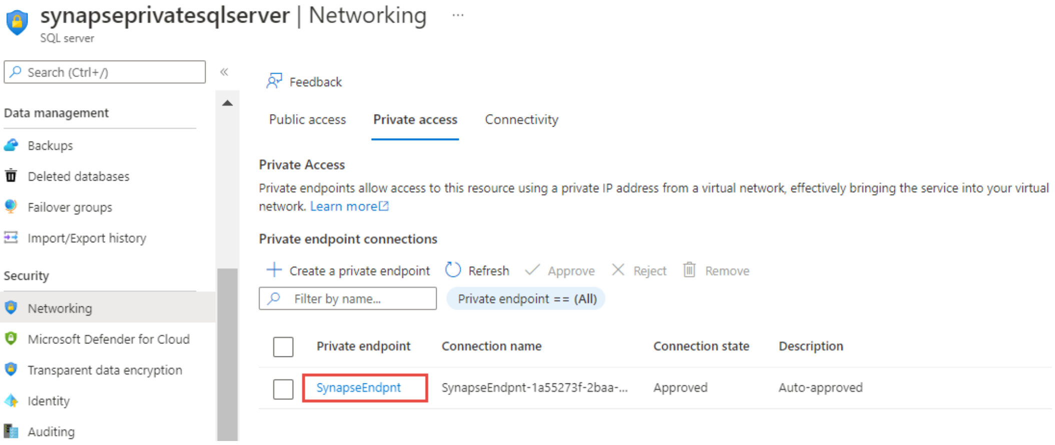
< Previous Next : Tags >

8. Optional. On the **Tags** tab, create tags to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups, and then click **Next : Review + Create**.
9. On the **Review + Create** tab, verify the details, and then click **Create**.

Create a virtual network link

Create a virtual network link to link the virtual network to the private DNS zone of the private endpoint. Once linked, virtual machines hosted in that virtual network can access the private DNS zone.

1. Go to the **Networking** tab of the SQL server that contains the Microsoft Azure Synapse SQL account for which you have created the private endpoint.
2. On the **Private access** tab, click the name of the private endpoint that you created.



synapseprivatesqlserver | Networking

SQL server

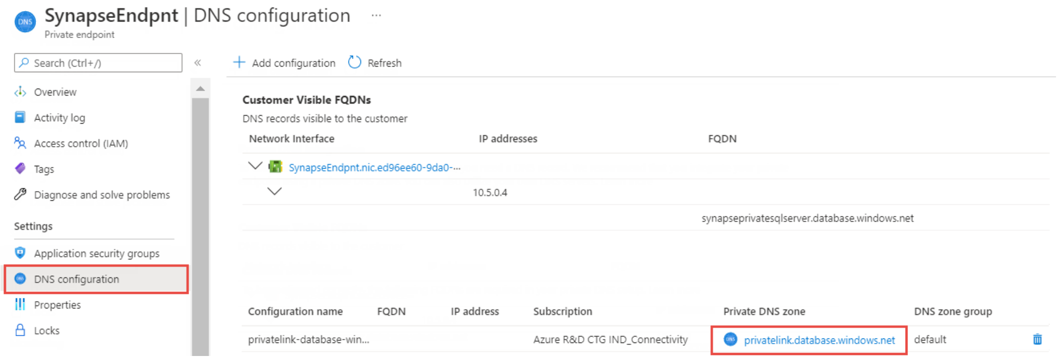
Private Access

Private endpoints allow access to this resource using a private IP address from a virtual network, effectively bringing the service into your virtual network. Learn more

Private endpoint connections

Private endpoint	Connection name	Connection state	Description
SynapseEndpnt	SynapseEndpnt-1a55273f-2baa-...	Approved	Auto-approved

3. Click **DNS configuration**.



SynapseEndpnt | DNS configuration

Private endpoint

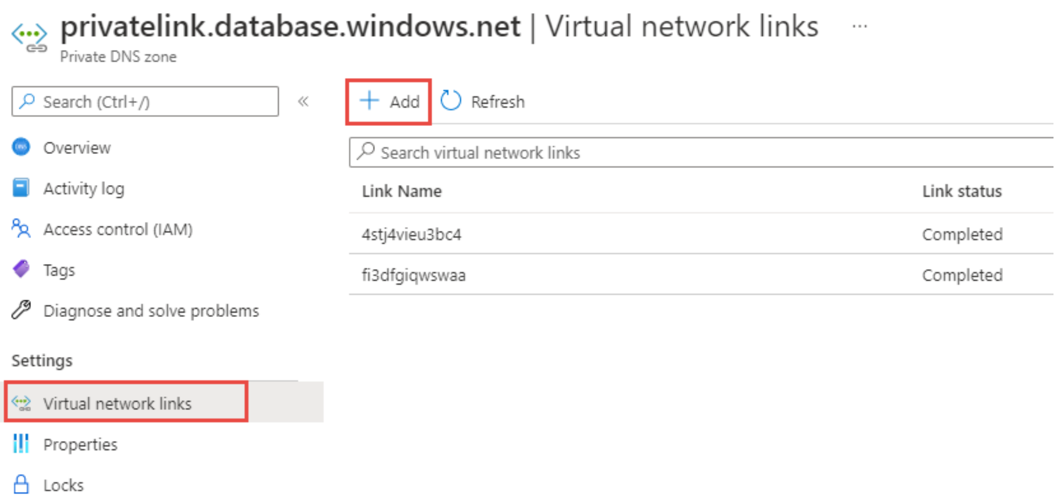
Customer Visible FQDNs

DNS records visible to the customer

Network Interface	IP addresses	FQDN
SynapseEndpnt.nic.ed96ee60-9da0-...		
	10.5.0.4	
		synapseprivatesqlserver.database.windows.net

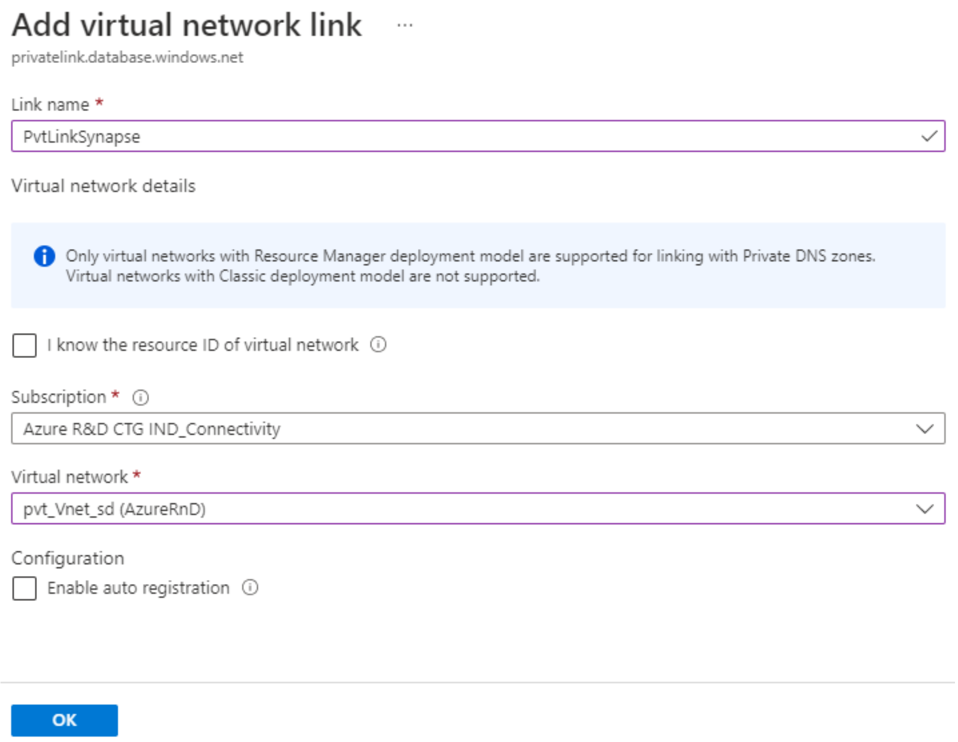
Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
privatelink-database-win...			Azure R&D CTG IND_Connectivity	privatelink.database.windows.net	default

4. On the **DNS configuration** page, click the Private DNS zone for the private endpoint.
5. Click **Virtual network links**, and then click **Add**.



Link Name	Link status
4stj4vieu3bc4	Completed
fi3dfgiqwswaa	Completed

6. In the **Link name** field, enter a name for the virtual network link.



Link name * PvtLinkSynapse

Only virtual networks with Resource Manager deployment model are supported for linking with Private DNS zones. Virtual networks with Classic deployment model are not supported.

□ I know the resource ID of virtual network

Subscription * Azure R&D CTG IND_Connectivity

Virtual network * pvt_Vnet_sd (AzureRnD)

□ Enable auto registration

7. Select the **Subscription** and the **Virtual network** you want to link with.
8. Click **OK**.

Verify the Azure private endpoint configuration

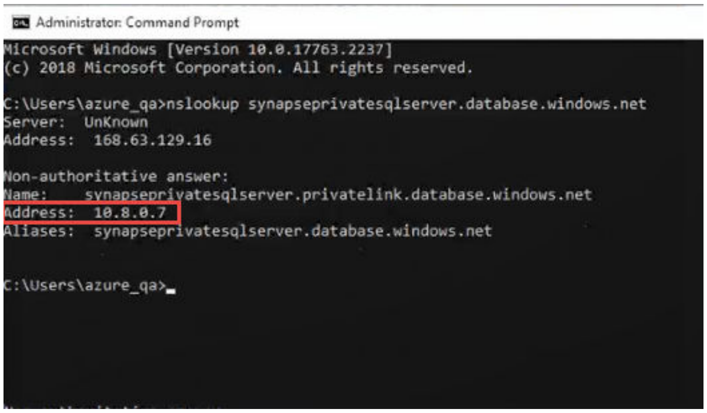
After you configure the private endpoint, verify if the requests to Microsoft Azure Synapse SQL go through the private endpoint.

1. Log in to the virtual machine that you created.

2. Open the command prompt and enter the command in the following format:
   `nslookup <SQL server name>.database.windows.net`

   For example, `nslookup synapseprivatesqlserver.database.windows.net`.

   If the requests to Microsoft Azure Synapse SQL go through the private endpoint, the command prompt shows the IP address of the private endpoint.



```
Microsoft Windows [Version 10.0.17763.2237]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\azure_qa>nslookup synapseprivatesqlserver.database.windows.net
Server:  UnKnown
Address:  168.63.129.16

Non-authoritative answer:
Name:    synapseprivatesqlserver.privatelink.database.windows.net
Address:  10.8.0.7
Aliases:  synapseprivatesqlserver.database.windows.net


C:\Users\azure_qa>_
```

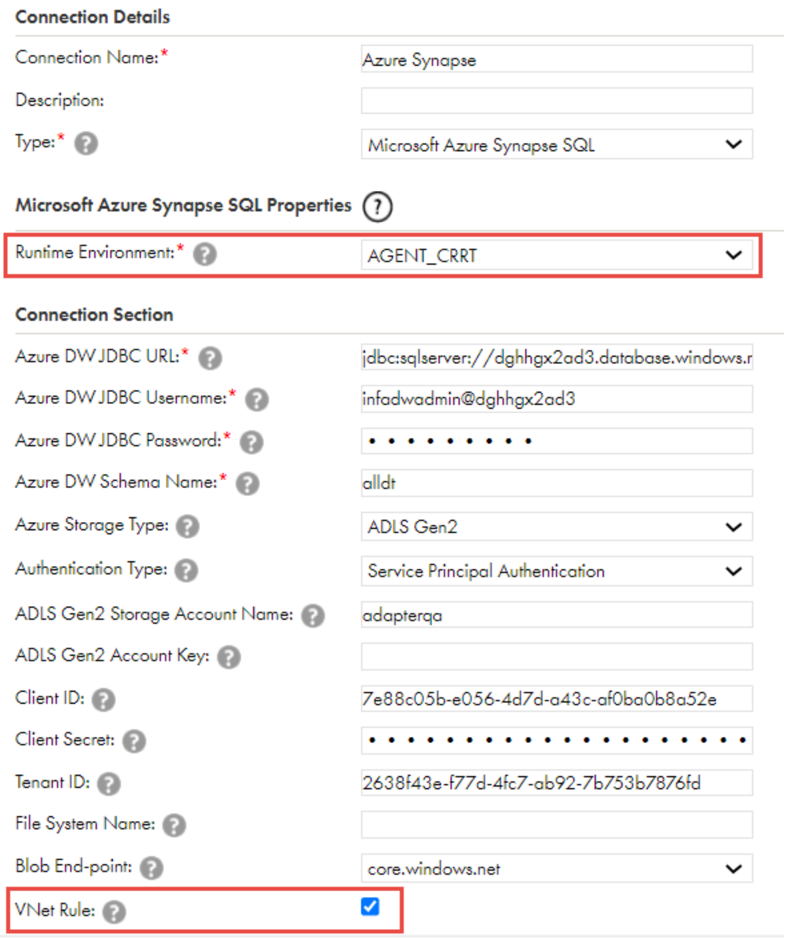
Configure settings for Microsoft Azure Synapse SQL connection

Configure the settings for the Microsoft Azure Synapse SQL connection to use the private endpoint.

When you set up the Microsoft Azure Synapse SQL connection, select the Secure Agent installed on the virtual machine that you created and enable the virtual network.

You can use a private endpoint when you stage files in Microsoft Azure Data Lake Storage Gen2 and use the service principal authentication or shared key authentication to connect to the storage.

1. Log in to Informatica Intelligent Cloud Services.
2. Click **Administrator**.
3. Edit an existing connection or create a new connection.
4. Select the Secure Agent installed on the virtual machine and enable the virtual network in the connection properties.



Connection Details

Connection Name:*	Azure Synapse
Description:	
Type:*	Microsoft Azure Synapse SQL

Microsoft Azure Synapse SQL Properties

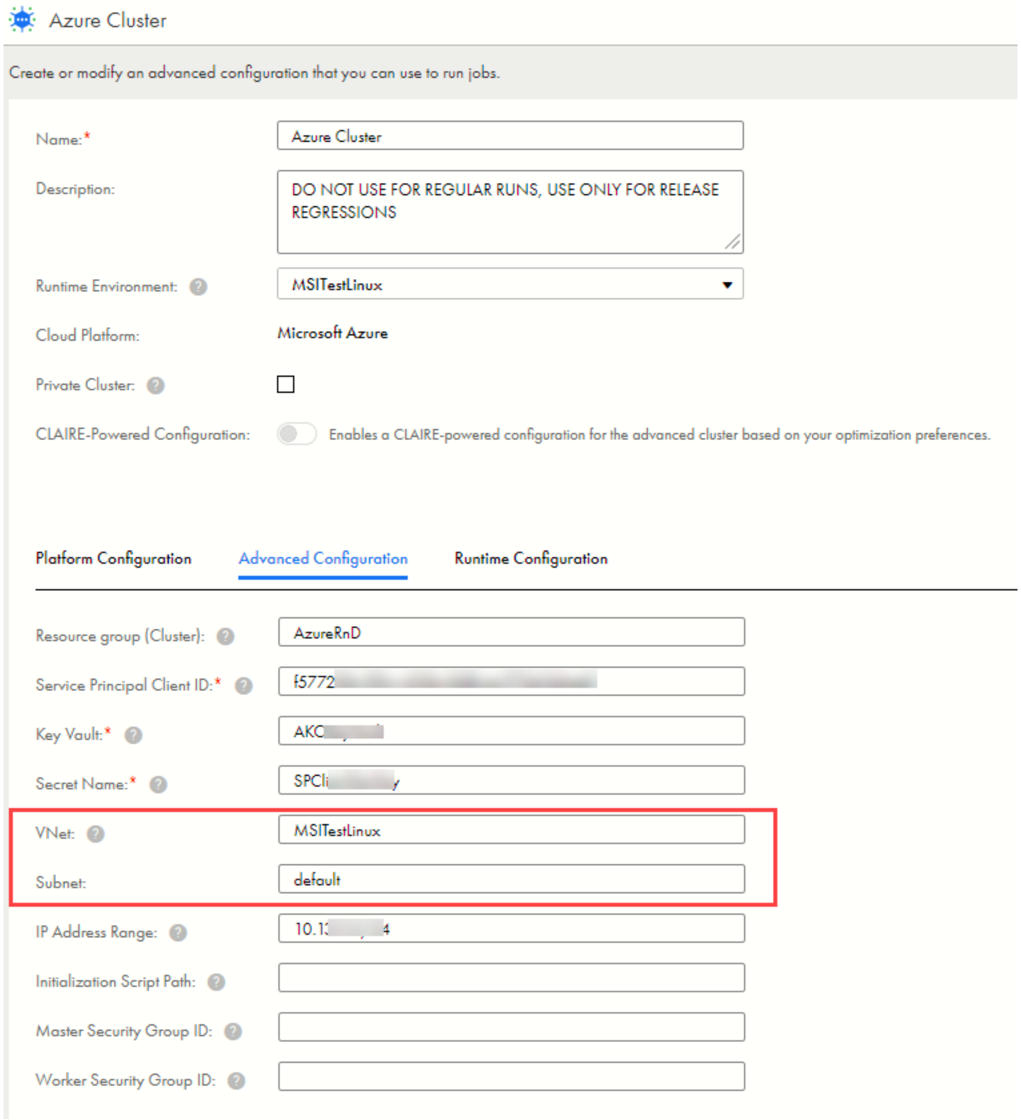
Runtime Environment:*	AGENT_CRRT

Connection Section

Azure DW JDBC URL:*	jdbc:sqlserver://dghhgx2ad3.database.windows.r
Azure DW JDBC Username:*	infadwadmin@dghhgx2ad3
Azure DW JDBC Password:*	••••••••••
Azure DW Schema Name:*	alldt
Azure Storage Type:	ADLS Gen2
Authentication Type:	Service Principal Authentication
ADLS Gen2 Storage Account Name:	adapterqa
ADLS Gen2 Account Key:	
Client ID:	7e88c05b-e056-4d7d-a43c-af0ba0b8a52e
Client Secret:	•••••••••••••••••••••
Tenant ID:	2638f43e-f77d-4fc7-ab92-7b753b7876fd
File System Name:	
Blob End-point:	core.windows.net
VNet Rule:	☑

5. Click **Test Connection**, and then click **Save**.
6. In **Administrator**, navigate to **Advanced Clusters** to create or modify an Advanced Configuration.

7. In the **Advanced Configuration** tab, add the Vnet and Subnet properties that is linked with the private DNS zone. This helps to spawn the cluster resources under this subnet and provide access to the private DNS zone.



Azure Cluster

Create or modify an advanced configuration that you can use to run jobs.

Name:*	Azure Cluster
Description:	DO NOT USE FOR REGULAR RUNS, USE ONLY FOR RELEASE REGRESSIONS
Runtime Environment:	MSITestLinux
Cloud Platform:	Microsoft Azure
Private Cluster:	□
CLAIRE-Powered Configuration:	Enables a CLAIRE-powered configuration for the advanced cluster based on your optimization preferences.

Platform Configuration | Advanced Configuration | Runtime Configuration

Resource group (Cluster):	AzureRnD
Service Principal Client ID:*	f5772[redacted]
Key Vault:*	AKC[redacted]
Secret Name:*	SPCli[redacted]y
VNet:	MSITestLinux
Subnet:	default
IP Address Range:	10.1[redacted]4
Initialization Script Path:	
Master Security Group ID:	
Worker Security Group ID:	

You can also configure a private endpoint to connect to Microsoft Azure Data Lake Storage Gen2 to stage files.

For more information, see the Informatica How-To Library article, Connecting to an Azure storage account using an Azure private endpoint.

Author

Adrija Pandya

Acknowledgements

The author would like to acknowledge Nirosha V for her technical assistance with this article.