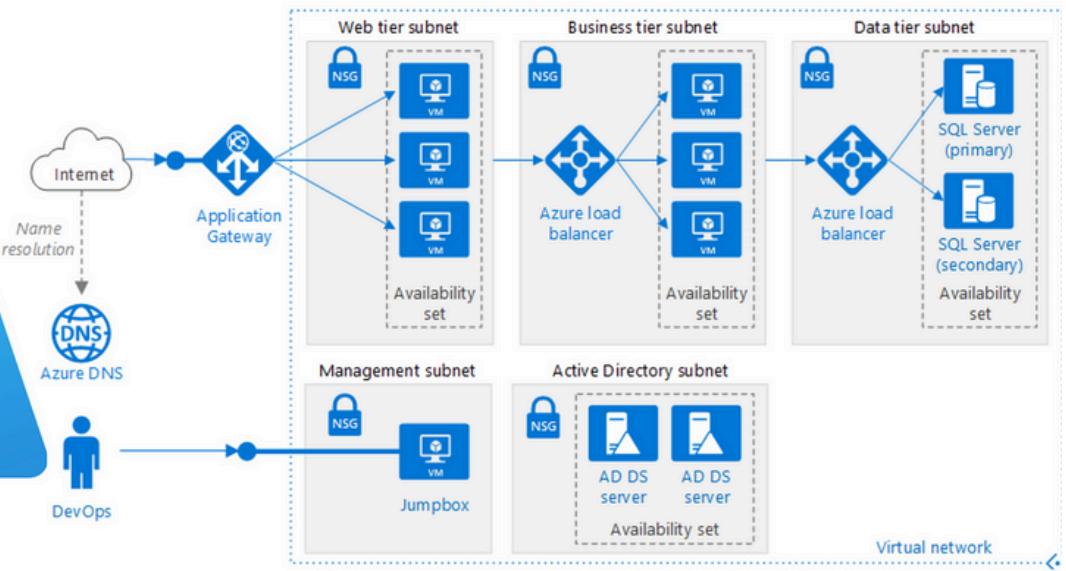


Azure Private DNS Lab: Implementing Secure Cross-VNet Connectivity

INTRODUCTION TO AZURE VIRTUAL NETWORKS



Introduction

In this post, I'll walk you through a lab that demonstrates how to set up Azure Private DNS for name resolution across multiple Virtual Networks (VNets). Azure Private DNS provides a secure and scalable way to manage domain names for your virtual machines (VMs) and other resources within Azure, without needing to deploy your own DNS servers. This is especially useful in scenarios where you have multiple VNets that need to communicate with each other. This blog post is structured around a Microsoft Learn lab, and I'll provide detailed steps and screenshots to help you navigate the Azure portal.

Prerequisites

- An Azure subscription
- Azure PowerShell installed
- Familiarity with Azure Virtual Networks

Lab Overview

This lab consists of the following key steps:

1. Create a Resource Group
2. Deploy a Bicep Template
3. Create a Private DNS Zone
4. Link Subnets for Auto Registration
5. Deploy Virtual Machines
6. Create VNet Peering
7. Verify DNS Resolution

Step-by-Step Instructions

Module 1: Design and Implement a Virtual Network in Azure

Consider the fictional organization Contoso Ltd, which is in the process of migrating infrastructure and applications to Azure. In your role as network engineer, you must plan and implement three virtual networks and subnets to support resources in those virtual networks.

+ Azure Virtual Network is a service that provides the fundamental building block for your private network in Azure. An instance of the service (a virtual network) enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. Ensure nonoverlapping address spaces. Make sure your virtual network address space (CIDR block) doesn't overlap with your organization's other network ranges.

+ All Azure resources in a virtual network are deployed into subnets within the virtual network. Subnets enable you to segment the virtual network into one or more subnetworks and allocate a portion of the virtual network's address space to each subnet. Your subnets shouldn't cover the entire address space of the virtual network. Plan ahead and reserve some address space for the future.

Task 1: Create the Contoso Resource Group

Use Azure PowerShell to create a resource group. This command creates a container for all the resources used in this lab.

```
New-AzResourceGroup -Name Contoso -Location <YourAzureRegion>
```

Name	Subscription	Location
ContosoResourceGroup	Azure subscription 1	East US
NetworkWatcherRG	Azure subscription 1	Germany West Central

```
$ /home/kvng>
$ /home/kvng> new-azresourcegroup -Name "ContosoResourceGroup" -Location 'eastus'
resourceGroupName : ContosoResourceGroup
location         : eastus
provisioningState : Succeeded
```

- **To verify in the Azure portal:**
 - Go to the Azure portal.
 - Search for "Resource groups".
 - Click on "Resource groups".
 - Confirm that "Contoso" is in the list.

Task 2: Create the CoreServicesVnet Virtual Network and Subnets

The Bicep template will handle this, but you can verify the configuration.

Add or remove favorites by pressing Cmd+Shift+F

```
PS /home/kvng>
PS /home/kvng> $date = Get-Date -Format "MM-DD-YY"
PS /home/kvng> $date
04-DD-YY
PS /home/kvng> $deploymentName = "AzInsiderDeployment"+$date
PS /home/kvng> $deploymentName
AzInsiderDeployment04-DD-YY
PS /home/kvng> New-AzRes
New-AzResource          New-AzResourceGroupDeploymentStack  New-AzRestorePoint
New-AzResourceGraphQuery New-AzResourceLock           New-AzRestorePointCollection
New-AzResourceGroup      New-AzResourceManagementPrivateLink
New-AzResourceGroupDeployment New-AzResourceMoveMoveCollection
PS /home/kvng> New-AzResourceGroupDeployment -Name $deploymentName -ResourceGroupName ContosoResourceGroup -TemplateFile .\main.bicep -TemplateParameterFile .\azuredeploy.parameters.json -confirm
```

Task 3: Create the ManufacturingVnet Virtual Network and Subnets

The Bicep template will handle this, but you can verify the configuration.

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Unsecure resources	Recommendations	Changed resources
0	0	6

Showing 1 - 6 of 6. Display count: auto

```
PS /home/kvng>
Requesting a Cloud Shell. Succeeded.
Connecting terminal...
Subscription used to launch your CloudShell bd79b60f-58fb-4efb-ab99-a27fdec0753 is not registered to Microsoft.CloudShell Namespace. Please follow these instructions "https://aka.ms/RegisterCloudShell" to register. In future, unregistered subscriptions will have restricted access to CloudShell service.
Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.
MOTD: Azure Cloud Shell now includes Predictive IntelliSense! Learn more: https://aka.ms/CloudShell/IntelliSense
VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/kvng> [ ]
```

Task 4: Create the ResearchVnet Virtual Network and Subnets

The Bicep template will handle this, but you can verify the configuration.

Task 5: Verify the Creation of VNets and Subnets

- **To verify in the Azure portal:**

- Go to the Azure portal.
- Search for "Virtual networks".
- Click on "Virtual networks".
- Confirm that "CoreServicesVnet", "ManufacturingVnet", and "ResearchVnet" are in the list.
- Click on each VNet to verify the subnets:
 - CoreServicesVnet should have subnets: "CoreServicesSubnet"
 - ManufacturingVnet should have subnets: "ManufacturingSubnet"
 - ResearchVnet should have subnets: "ResearchSubnet"

The screenshot shows the Azure portal interface. On the left, there's a sidebar with navigation links like 'Create', 'Group by none', 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Diagnose and solve problems', 'Resource visualizer', 'Settings' (which is expanded), 'Subnets' (which is selected and highlighted in blue), 'Bastion', 'DDoS protection', 'Firewall', 'Microsoft Defender for Cloud', and 'Network manager'. Below this is a search bar and a table titled 'Subnets'. The table has columns for Name, IPv4, IPv6, Available IPs, Delegated to, Security group, and Route table. It lists four subnets: 'GatewaySubnet' (IPv4 10.20.0.0/27, Available IPs 251), 'SharedService...' (IPv4 10.20.10.0/24, Available IPs 251), 'DatabaseSubn...' (IPv4 10.20.20.0/24, Available IPs 251), and 'PublicWebSer...' (IPv4 10.20.30.0/24, Available IPs 251). At the bottom of the page, there's a terminal window showing a Cloud Shell session.

This screenshot is identical to the one above, showing the Azure portal interface with the 'Subnets' section selected. The left sidebar, search bar, and table of subnets are all present. The terminal window at the bottom shows a Cloud Shell session that has succeeded.

Module 2: Configure DNS Settings in Azure

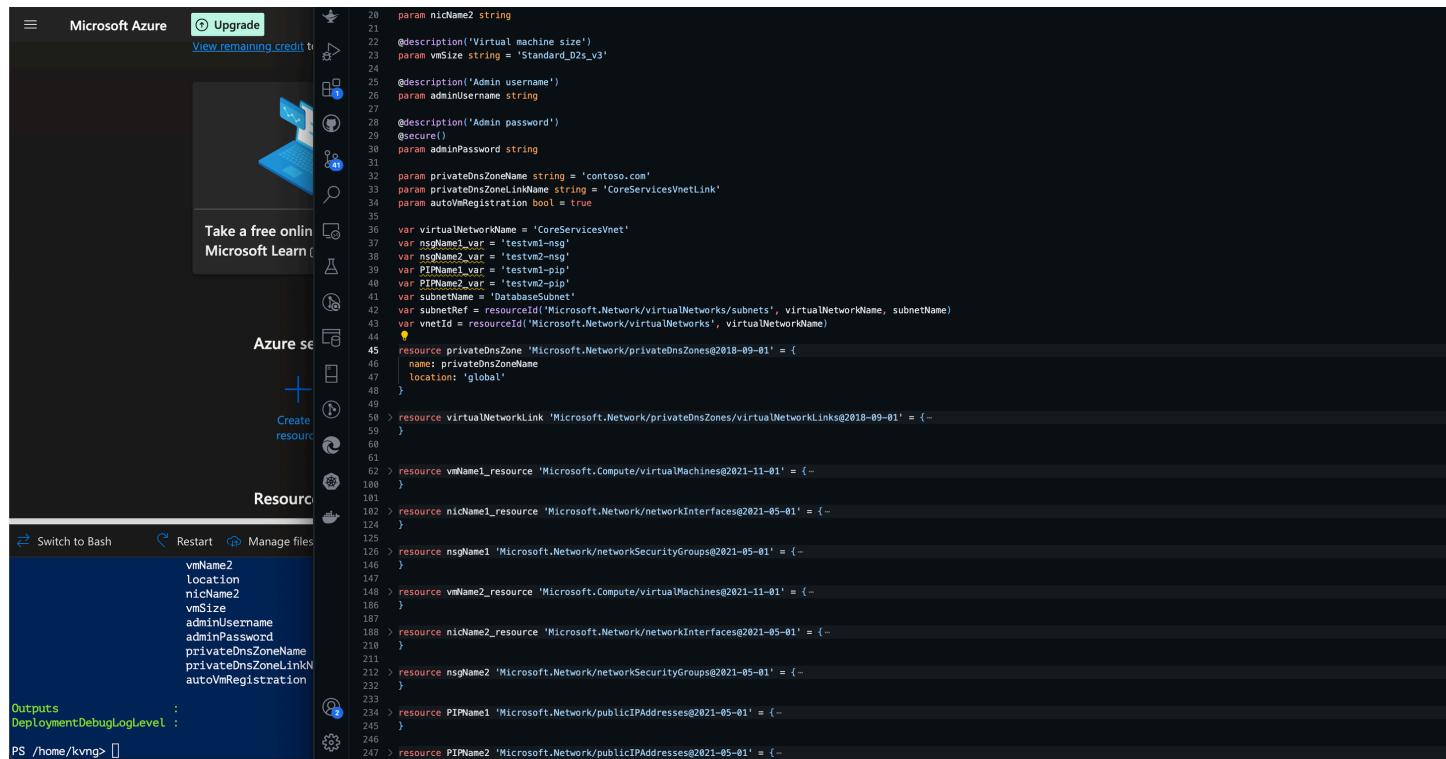
This module focuses on configuring the Private DNS Zone.

In this unit, you will configure DNS name resolution for Contoso Ltd. You will create a private DNS zone named contoso.com, link the VNets for registration and resolution, and then create two virtual machines and test the configuration.

- + Azure DNS is a cloud service that allows you to host and manage domain name system (DNS) domains, also known as DNS zones.
- + Azure DNS public zones host domain name zone data for records that you intend to be resolved by any host on the internet.
- + Azure Private DNS zones allow you to configure a private DNS zone namespace for private Azure resources.
- + A DNS zone is a collection of DNS records. DNS records provide information about the domain.

Task 1: Create a Private DNS Zone

The Bicep template automates this.



The screenshot shows the Azure portal interface with a Bicep code editor. The code defines parameters and resources for setting up a private DNS zone 'contoso.com' across two virtual networks ('CoreServicesVnet' and 'testvnet2'). It includes configurations for VMs ('vmName1', 'vmName2'), network interfaces ('nicName1', 'nicName2'), and network security groups ('nsGName1', 'nsGName2'). The Bicep file is titled 'CreatePrivateDnsZone.bicep' and contains approximately 250 lines of code.

```
param nicName2 string
param vmSize string = 'Standard_D2s_v3'
param adminUsername string
param adminPassword string
param privateDnsZoneName string = 'contoso.com'
param privateDnsZoneLinkName string = 'CoreServicesVnetLink'
param autoVmRegistration bool = true
var virtualNetworkName = 'CoreServicesVnet'
var nsGName1_var = 'testvnet1-nsg'
var nsGName2_var = 'testvnet2-nsg'
var PIPName1_var = 'testvnet1-pip'
var PIPName2_var = 'testvnet2-pip'
var subnetName = 'DatabaseSubnet'
var subnetRef = resourceId('Microsoft.Network/virtualNetworks/subnets', virtualNetworkName, subnetName)
var vnetId = resourceId('Microsoft.Network/virtualNetworks', virtualNetworkName)
resource privateDnsZone 'Microsoft.Network/privateDnsZones@2018-09-01' = {
    name: privateDnsZoneName
    location: 'global'
}
resource virtualNetworkLink 'Microsoft.Network/privateDnsZones/virtualNetworkLinks@2018-09-01' = {
    ...
}
resource vmName1_resource 'Microsoft.Compute/virtualMachines@2021-11-01' = {
    ...
}
resource nicName1_resource 'Microsoft.Network/networkInterfaces@2021-05-01' = {
    ...
}
resource nsGName1 'Microsoft.Network/networkSecurityGroups@2021-05-01' = {
    ...
}
resource vmName2_resource 'Microsoft.Compute/virtualMachines@2021-11-01' = {
    ...
}
resource nicName2_resource 'Microsoft.Network/networkInterfaces@2021-05-01' = {
    ...
}
resource nsGName2 'Microsoft.Network/networkSecurityGroups@2021-05-01' = {
    ...
}
resource PIPName1 'Microsoft.Network/publicIPAddresses@2021-05-01' = {
    ...
}
resource PIPName2 'Microsoft.Network/publicIPAddresses@2021-05-01' = {
```

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Filter for any field... Subscription equals all Resource Group equals all Type equals all Location equals all + Add filter

Unsecure resources Recommendations Changed resources

<input type="checkbox"/>	contoso.com	... Private DNS zone	ContosoResourceGroup	Global	Azure subscription 1
<input type="checkbox"/>	CoreServicesVnet	... Virtual network	ContosoResourceGroup	East US	Azure subscription 1
<input type="checkbox"/>	ManufacturingVnet	... Virtual network	ContosoResourceGroup	West Europe	Azure subscription 1
<input type="checkbox"/>	NetworkWatcher_eastus	... Network Watcher	NetworkWatcherRG	East US	Azure subscription 1
<input type="checkbox"/>	NetworkWatcher_southeastasia	... Network Watcher	NetworkWatcherRG	Southeast Asia	Azure subscription 1
<input type="checkbox"/>	NetworkWatcher_westeurope	... Network Watcher	NetworkWatcherRG	West Europe	Azure subscription 1
<input type="checkbox"/>	ResearchVnet	... Virtual network	ContosoResourceGroup	Southeast Asia	Azure subscription 1
<input type="checkbox"/>	testvm1	... Virtual machine	ContosoResourceGroup	East US	Azure subscription 1
<input type="checkbox"/>	testvm1-nic	... Network Interface	ContosoResourceGroup	East US	Azure subscription 1
<input type="checkbox"/>	testvm1-nsg	... Network security group	ContosoResourceGroup	East US	Azure subscription 1
<input type="checkbox"/>	testvm1-pip	... Public IP address	ContosoResourceGroup	East US	Azure subscription 1
<input type="checkbox"/>	testvm1_disk1_0c01e59395f748fca625021b86b43fa3	... Disk	CONTOSORESOURCEGROUP	East US	Azure subscription 1
<input type="checkbox"/>	testvm2	... Virtual machine	ContosoResourceGroup	East US	Azure subscription 1

Showing 1 - 17 of 17. Display count: 20 Give feedback

- **To verify in the Azure portal:**

- Go to the Azure portal.
- Search for "Private DNS zones".
- Click on "Private DNS zones".
- Confirm that the private DNS zone (e.g., "contoso.com") is in the list.
- Click on the private DNS zone to view its properties.
- Verify the Name servers are listed.

All resources Default Directory

contoso.com | Recordsets Private DNS zone

Search + Add Refresh Delete Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings DNS Management Records

Fetched 3 record set(s). 0 record sets selected

Name	Type	TTL	Value	Auto registered
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
testvm1	A	10	10.20.20.5	True
testvm2	A	10	10.20.20.4	True

Showing 1 - 17 of 17. Display count: 20 Add or remove favorites by pressing Cmd+Shift+F

Task 2: Link Subnet for Auto Registration

The Bicep template links the subnets to the Private DNS Zone, enabling automatic registration of VMs in those subnets.

- As mentioned before, when you link a VNet to your private DNS Zone (think of it as a local organization phonebook), you're telling the VNet's resources to use this private zone for name resolution. If multiple VNets are linked to the same private DNS Zone, it's like giving all those separate network spaces the same custom phonebook. This allows VMs in different VNets to find each other using the names in your private DNS Zone.
- **To verify in the Azure portal:**

- In the Private DNS zone, go to "Virtual network links".
- Confirm that the virtual networks (CoreServicesVnet, ManufacturingVnet, and ResearchVnet) and their corresponding subnets are listed and linked.
- Check the "Auto registration" column to ensure it is enabled.

Task 3: Create Virtual Machines to Test the Configuration

The Bicep template creates the VMs.

testvm1 Virtual machine

Help me copy this VM in any region

Overview

Resource group (move) : ContosoResourceGroup

Status : Running

Location : East US

Subscription (move) : Azure subscription 1

Subscription ID : bd79b60f-58fb-aba9-a27fdecc0753

Tags (edit) : Add tags

Operating system : Windows (Windows Server 2019 Datacenter)

Size : Standard D2s v3 (2 vcpus, 8 GiB memory)

Public IP address : 172.190.255.96

Virtual network/subnet : CoreServicesVnet/DatabaseSubnet

DNS name : Not configured

Health state : -

Time created : 4/19/2025, 3:01 PM UTC

Properties **Monitoring** **Capabilities (8)** **Recommendations** **Tutorials**

Virtual machine

Computer name	testvm1
Operating system	Windows (Windows Server 2019 Datacenter)
VM generation	V1
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1149
Hibernation	Disabled
Host group	-
Host	-

Networking

Public IP address	172.190.255.96 (Network interface testvm1-nic)
Public IP address (IPv6)	-
Private IP address	10.20.20.5
Private IP address (IPv6)	-
Virtual network/subnet	CoreServicesVnet/DatabaseSubnet
DNS name	Configure

Size

Size	Standard D2s v3
------	-----------------

JSON View

All resources

Default Directory

+ Create ... Group by none

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

- NetworkWatcher_eastus
- NetworkWatcher_southeastasia
- NetworkWatcher_westeuropa
- ResearchVnet
- testvm1
- testvm1-nic
- testvm1-nsg
- testvm1-pip
- testvm1_disk1_0c01e59395f7489
- testvm2
- testvm2-nic
- testvm2-nsg
- testvm2-pip
- testvm2_disk1_8edd3344d83742

Showing 1 - 17 of 17. Display count: 20

testvm2 Virtual machine

Help me copy this VM in any region

Overview

Computer name : testvm2

Operating system : Windows (Windows Server 2019 Datacenter)

VM generation : V1

VM architecture : x64

Agent status : Ready

Agent version : 2.7.41491.1149

Hibernation : Disabled

Host group : -

Proximity placement group : -

Colocation status : N/A

Capacity reservation group : -

Disk controller type : -

Azure Spot

Azure Spot : -

Azure Spot eviction policy : -

Availability + scaling

Availability zone : (edit)

Networking

Public IP address	52.147.203.81 (Network interface testvm2-nic)
Public IP address (IPv6)	-
Private IP address	10.20.20.4
Private IP address (IPv6)	-
Virtual network/subnet	CoreServicesVnet/DatabaseSubnet
DNS name	Configure

Size

Size	Standard D2s v3
vCPUs	2
RAM	8 GiB

Source image details

Source image publisher : MicrosoftWindowsServer

Source image offer : WindowsServer

Source image plan : 2019-Datacenter

Disk

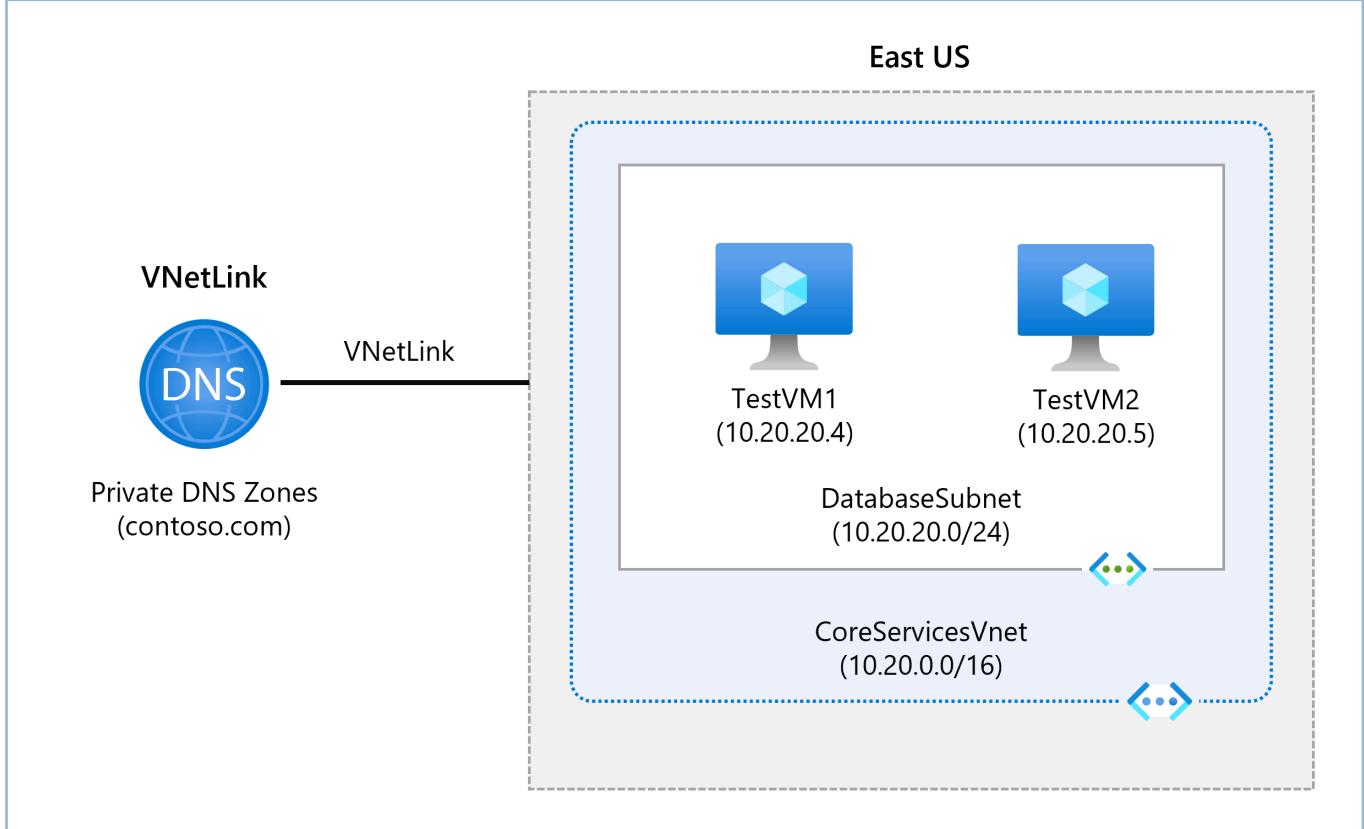
OS disk	testvm2_disk1_8edd3344d83742e097ec6b818a217ff6
Encryption at host	Disabled
Azure disk encryption	Not enabled

Module 3: Connect two Azure Virtual Networks using global virtual network peering

Virtual network peering enables you to seamlessly connect two Azure virtual networks. The virtual networks appear as one for connectivity purposes. Azure supports connecting virtual networks within the same Azure region and across Azure regions (global). The traffic between virtual machines in peered virtual networks is routed directly through the Microsoft backbone infrastructure, not through a gateway or over the public Internet. You can resize the address space of Azure virtual networks that are peered without incurring any downtime on the currently peered address space. Enhance Security by not providing default Outbound access. Therefore, to enable Connectivity for VMs within this Subnet, it's necessary to explicitly grant Outbound access. A NAT Gateway is the Recommended way to provide connectivity for Virtual machines in the subnet "Subnets without public IP Address".

Enable Cross-Virtual Network Connectivity with Peering: Allows you to connect separate VNets with Optimal Network performance, whether they are in the Same Region [Regional VNet peering] or in different regions [Global VNet peering]. Traffic between peered VNets is private. For connectivity purposes, once peered, the VNets appear as One. This offers the following Benefits:

- Low Latency, high-bandwidth connection b/w Resources in different VNets.
- Ability to apply Network Security Groups in either VNet to block access to other VNets or subnets.
- Ability to transfer data b/w VNets across Azure subscriptions, Entra Tenants, Deployment models, and Regions.
- Ability to peer a VNet created through the Resource Manager to one created through classic deployment.
- No downtime to Resources in other VNets is required when creating/after creating peering.



Azure Private DNS Domains

AZURE DNS - A hosting service for DNS domains, providing name resolution using AZURE infrastructure. Supports private DNS domains. In addition to internet-facing public domains, AZURE supports private DNS Domains used locally within Azure.

- AZURE DNS resolves domain names in a Virtual network without the need to add a Custom DNS solution.
- Private DNS Zones allow you to use your own custom domain names rather than the Azure-provided names.
- It provides name Resolution for VMs within a virtual network and between virtual networks.
- You can configure zone names with a split-horizon view - allowing a private & public DNS zone to share the same name.
- VNet is used to store & organize information about various elements of your cloud.

```

99 resource nsgName1 'Microsoft.Network/networkSecurityGroups@2021-05-01' = {
100 }
101
102 resource PIPName1 'Microsoft.Network/publicIPAddresses@2021-05-01' = {
103     name: PIPName1_var
104     location: location
105     sku: {
106         name: 'Basic'
107         tier: 'Regional'
108     }
109     properties: {
110         publicIPAddressVersion: 'IPv4'
111         publicIPAllocationMethod: 'Dynamic'
112     }
113 }
114
115 //This creates a peering from CoreServicesVnet-to-ManufacturingVnet
116 resource peer1 'microsoft.network/virtualNetworks/virtualNetworkPeerings@2020-05-01' = {
117     name: '${vnet0}/to-ManufacturingVnet'
118     properties: {
119         allowVirtualNetworkAccess: true
120         allowForwardedTraffic: false
121         allowGatewayTransit: false
122         useRemoteGateways: false
123         remoteVirtualNetwork: {
124             id: resourceId(remoteVnetRg, 'Microsoft.Network/virtualNetworks', vnet1)
125         }
126     }
127     dependsOn: [
128         vmName1_resource
129     ]
130 }
131
132 //This creates a peering from ManufacturingVnet-to-CoreServicesVnet
133 resource peer4 'microsoft.network/virtualNetworks/virtualNetworkPeerings@2020-05-01' = {
134     name: '${vnet1}/to-CoreServicesVnet'
135     properties: {
136         allowVirtualNetworkAccess: true
137         allowForwardedTraffic: false
138         allowGatewayTransit: false
139         useRemoteGateways: false
140         remoteVirtualNetwork: {
141             id: resourceId(remoteVnetRg, 'Microsoft.Network/virtualNetworks', vnet0)
142         }
143     }
144     dependsOn: [
145         vmName1_resource
146     ]
147 }
148
149 }
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168

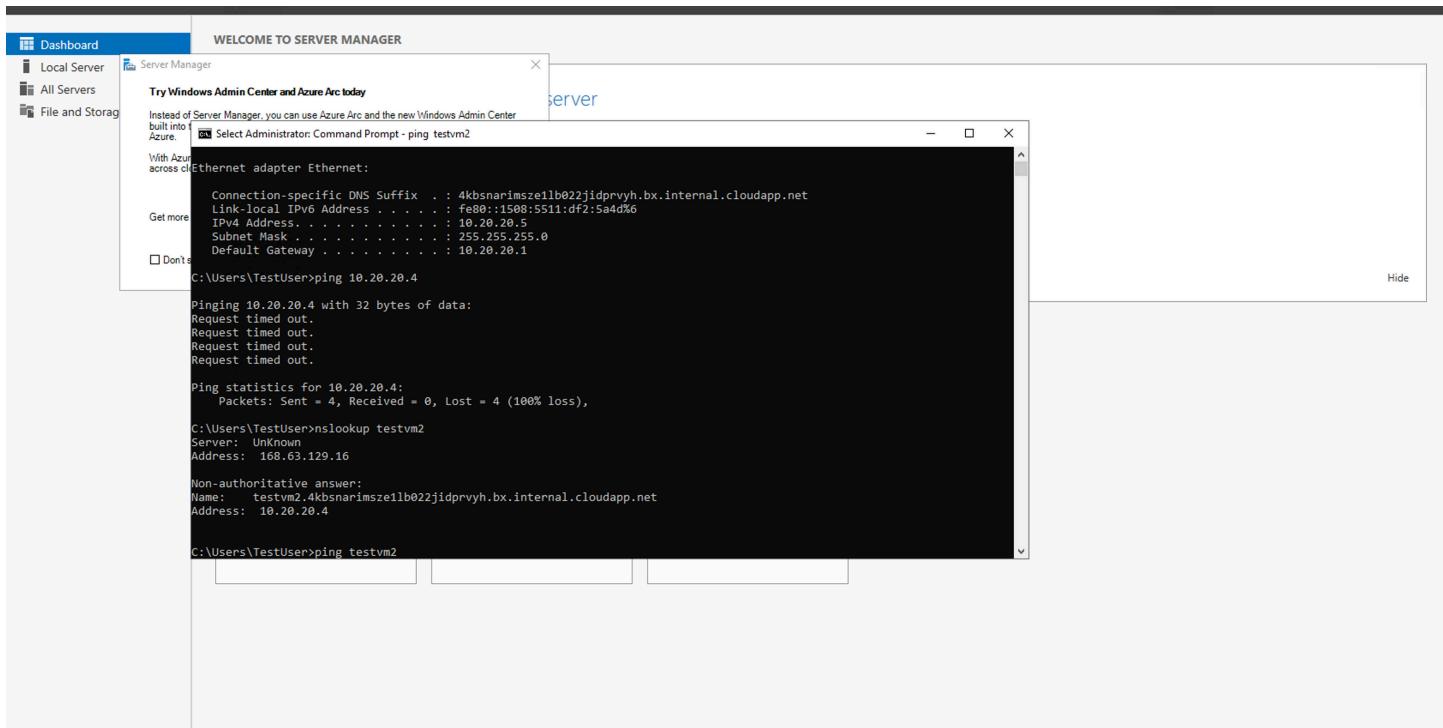
```

Task 1: Create a Virtual Machine to test the configuration

The Bicep template creates the VMs.

Task 2: Connect to the Test VMs using RDP

Use Remote Desktop Protocol (RDP) to connect to the VMs.



- **To connect via RDP:**
 - In the Azure portal, go to the Virtual Machine.
 - Click "Connect".
 - Select "RDP".
 - Download the RDP file.
 - Use the downloaded RDP file and the username/password you provided during VM creation to connect.

Task 3: Test the connection between the VMs

The Bicep template creates the VMs.

```

id: "/subscriptions/bd79b60f-58fb-4efb-aba9-a27fdecc0753/resourceGroups/ContosoResourceGroup/providers/Microsoft.Network/virtualNetworks/CoreServicesVnet/virtualNetworkPeerings/to-ManufacturingVnet"
  name: "to-ManufacturingVnet"
  properties.allowForwardedTraffic: false
  properties.allowGatewayTransit: false
  properties.allowVirtualNetworkAccess: true
  properties.remoteVirtualNetwork.id: "/subscriptions/bd79b60f-58fb-4efb-aba9-a27fdecc0753/resourceGroups/azinsider_demo/providers/Microsoft.Network/virtualNetworks/ManufacturingVnet"
  properties.useRemoteGateways: false
  type: "Microsoft.Network/virtualNetworks/virtualNetworkPeerings"

+ Microsoft.Network/virtualNetworks/ManufacturingVnet/virtualNetworkPeerings/to-CoreServicesVnet [2020-05-01]
  apiVersion: "2020-05-01"
id: "/subscriptions/bd79b60f-58fb-4efb-aba9-a27fdecc0753/resourceGroups/ContosoResourceGroup/providers/Microsoft.Network/virtualNetworks/ManufacturingVnet/virtualNetworkPeerings/to-CoreServicesVnet"
  name: "to-CoreServicesVnet"
  properties.allowForwardedTraffic: false
  properties.allowGatewayTransit: false
  properties.allowVirtualNetworkAccess: true
  properties.remoteVirtualNetwork.id: "/subscriptions/bd79b60f-58fb-4efb-aba9-a27fdecc0753/resourceGroups/azinsider_demo/providers/Microsoft.Network/virtualNetworks/CoreServicesVnet"
  properties.useRemoteGateways: false
  type: "Microsoft.Network/virtualNetworks/virtualNetworkPeerings"

* Microsoft.Compute/disks/testvm1_disk1_0c01e59395f748fc625021b86b43fa3
* Microsoft.Compute/disks/testvm2_disk1_bedd3344d83742e097ec6b818a217ff
* Microsoft.Compute/virtualMachines/testvm1
* Microsoft.Compute/virtualMachines/testvm2
* Microsoft.Network/networkInterfaces/testvm1-nic
* Microsoft.Network/networkInterfaces/testvm2-nic
* Microsoft.Network/networkSecurityGroups/testvm1-nsg
* Microsoft.Network/networkSecurityGroups/testvm2-nsg
* Microsoft.Network/privateDnsZones/contoso.com
* Microsoft.Network/privateDnsZones/contoso.com/virtualNetworkLinks/CoreServicesVnetLink
* Microsoft.Network/publicIPAddresses/testvm1-pip
* Microsoft.Network/publicIPAddresses/testvm2-pip
* Microsoft.Network/virtualNetworks/CoreServicesVnet
* Microsoft.Network/virtualNetworks/ManufacturingVnet
* Microsoft.Network/virtualNetworks/ResearchVnet

Resource changes: 6 to create, 15 to ignore.

Are you sure you want to execute the deployment?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

```

Task 4: Create VNet peerings between CoreServicesVnet and ManufacturingVnet

The Bicep template creates the VNet peerings.

The screenshot shows the Azure Cloud Shell interface. At the top, there's a message: "You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience." Below this are filter options for "Subscription equals all" and "Location equals all". The main area displays deployment history:

```

Are you sure you want to execute the deployment?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): Y

DeploymentName : AzInsiderDeployment04-19-2025
ResourceGroupName : ContosoResourceGroup
ProvisioningState : Succeeded
Timestamp : 4/19/2025 3:36:29 PM
Mode : Incremental
TemplateLink :
Parameters :
  Name Type Value
  ====== ====== =====
  location String "westeurope"
  vnName1 String "ManufacturingVNet"
  nicName1 String "ManufacturingVM-nic"
  vnSize String "Standard_D2s_v3"
  adminUsername String "TestUser"
  adminPassword SecureString null

Outputs :
DeploymentDebugLogLevel : 

PS /home/kvng>

```

To the right, a large JSON object represents the configuration for VNet peering between ManufacturingVnet and CoreServicesVnet.

```

124   name: 'Basic'
125   tier: 'Regional'
126 }
127 properties: {
128   publicIpAddressVersion: 'IPv4'
129   publicIPAllocationMethod: 'Dynamic'
130 }
131
132 //This creates a peering from CoreServicesVnet-to-ManufacturingVnet
133 resource peer1 'microsoft.network/virtualNetworks/virtualNetworkPeerings@2020-05-01' = {
134   name: '$(vnet0)/to-ManufacturingVnet'
135   properties: {
136     allowVirtualNetworkAccess: true
137     allowForwardedTraffic: false
138     allowGatewayTransit: false
139     useRemoteGateways: false
140     remoteVirtualNetwork: {
141       id: resourceId(remoteVnetRg, 'Microsoft.Network/virtualNetworks', vnet1)
142     }
143   }
144   dependsOn: [
145     vmName1_resource
146   ]
147 }
148
149 //This creates a peering from ManufacturingVnet-to-CoreServicesVnet
150 resource peer4 'microsoft.network/virtualNetworks/virtualNetworkPeerings@2020-05-01' = {
151   name: '$(vnet1)/to-CoreServicesVnet'
152   properties: {
153     allowVirtualNetworkAccess: true
154     allowForwardedTraffic: false
155     allowGatewayTransit: false
156     useRemoteGateways: false
157     remoteVirtualNetwork: {
158       id: resourceId(remoteVnetRg, 'Microsoft.Network/virtualNetworks', vnet0)
159     }
160   }
161   dependsOn: [
162     vmName1_resource
163   ]
164 }
165
166

```

- To verify VNet peering in the Azure portal:**
 - Go to the Azure portal.
 - Search for "Virtual networks".
 - Click on "Virtual networks".
 - Click on "CoreServicesVnet".
 - Go to "Peering".
 - Confirm that a peering exists with "ManufacturingVnet" and that the peering status is "Connected".
 - Repeat the process for "ManufacturingVnet" to confirm the reciprocal peering.
- Important Note:** Before configuring VNet peering, you might find that pinging a host in one VNet from a host in another VNet fails due to firewall restrictions. This highlights a key benefit of VNet peering.

The screenshot shows the Azure portal page for managing VNet peering. It details a peering connection named "to-CoreServicesVnet" between "ManufacturingVnet" and "CoreServicesVnet".

Remote virtual network summary:

- Remote Vnet Id: /subscriptions/bd79b60f-58fb-4efb-aba9-a27fdecc0753/resourceGroups/C ...
- IP address space: 10.20.0.0/16

Local virtual network summary:

- Peering link name: to-CoreServicesVnet
- Peering state: Connected

Local virtual network peering settings:

- Allow 'ManufacturingVnet' to access 'CoreServicesVnet':
- Allow 'ManufacturingVnet' to receive forwarded traffic from 'CoreServicesVnet':
- Allow gateway or route server in 'ManufacturingVnet' to forward traffic to 'CoreServicesVnet':

At the bottom are "Save" and "Cancel" buttons, and a "Give feedback" link.

The address space for a virtual network is composed of one or more non-overlapping address ranges that are specified in CIDR notation. IP Address Management (IPAM) is recommended to simplify address management and avoid overlapping address space. When not using IPAM, it is recommended to use an address range that is not globally routable, such as 172.16.0.0/12, or a range defined in RFC 1918 or RFC 6598. [Learn more](#)

Address space	Address range	Address count
10.20.0.0/16	10.20.0.0 - 10.20.255.255	65,536

Add additional address range

Peered virtual network address space

Peering name	Peered to	Address space	Address range
to-ManufacturingVnet	ManufacturingVnet	10.30.0.0/16	10.30.0.0 - 10.30.255.255

Save Cancel Give feedback

Task 5: Test the connection between the VMs

Once the deployment is complete, we need to verify that DNS resolution and network connectivity are working correctly.

When you link a VNet to your private DNS Zone (local organization phonebook), it tells the VNet's resources to use this private zone for name resolution. If multiple VNets were linked to the same private DNS Zone, it's like giving all those separate network spaces the same custom phonebook; this allows VMs in different VNets to find each other using the names in your private DNS Zone.

- **Verify records are present in the private DNS Zone:** Check the Azure portal to confirm that the DNS records for the VMs have been created in the Private DNS Zone.
 - In the Private DNS zone, go to "Overview".
 - Confirm that the expected DNS records (A records) for your VMs are present. The names should match the VM names.
- **RDP into any of the deployed VMs to do a nslookup:**
 - Use Remote Desktop Protocol (RDP) to connect to one of the VMs.
 - Open Command Prompt.
 - Use the nslookup command to query the DNS records of the other VM. For example: nslookup <other_vm_name>. This will confirm that the private DNS zone is correctly resolving the VM names to their IP addresses.
 - *(Include screenshots of the Azure portal showing the DNS records and the nslookup command output)*
- **Test VM-to-VM Connectivity:**
 - From one VM, ping the private IP address of the other VM. For example: ping <other vm private ip address>.
 - The test connection should succeed, and you will see a result similar to the following:
![[Powershell window with Test-NetConnection 10.20.20.4 -port 3389 showing TCP test succeeded: true]]
 - **Crucially, after successfully configuring VNet peering, this ping should now succeed.** This demonstrates that VNet peering has correctly configured the network to allow traffic to flow between the two VNets.

Route Type	Subnet	IP Prefix	Next Hop
Default		25.176.0.0/13	None
Default		25.152.0.0/14	None
Default		25.184.0.0/14	None
Default		25.4.0.0/14	None
Default		25.148.0.0/15	None
Default		198.18.0.0/15	None
Default		25.150.0.0/16	None
Default		25.156.0.0/16	None
Default		25.159.0.0/16	None
Default		40.109.0.0/16	None
Default		192.168.0.0/16	None
Default		104.147.0.0/16	None
Default		157.59.0.0/16	None
Default		40.108.0.0/17	None
Default		104.146.0.0/17	None
Default		23.103.0.0/18	None
Default		20.35.252.0/22	None
Default		10.30.0.0/16	Virtual network
Default		10.20.0.0/16	VNetGlobalPeering

Conclusion

By following these steps, you've successfully set up Azure Private DNS for cross-VNet name resolution. This provides a secure and efficient way for your VMs and services in different VNets to communicate with each other. Azure Private DNS simplifies network management and eliminates the need for manual DNS configuration or custom DNS servers. The Bicep template automates much of the deployment, and the Azure portal provides a user-friendly way to verify the configuration and troubleshoot any issues. The importance of VNet peering in enabling this cross-VNet communication is clearly demonstrated by the change in ping behavior before and after its configuration. For More Resources, Check the link below

- + [Design an IP addressing schema for your Azure deployment]
(<https://learn.microsoft.com/training/modules/design-ip-addressing-for-azure/>).
- + [Introduction to Azure Virtual Networks]
(<https://learn.microsoft.com/training/modules/introduction-to-azure-virtual-networks/>).
- + [Introduction to Azure Virtual Networks]
(<https://learn.microsoft.com/training/modules/introduction-to-azure-virtual-networks/>).
- + [Distribute your services across Azure virtual networks and integrate them by using virtual network peering](<https://learn.microsoft.com/training/modules/integrate-vnets-with-vnet-peering/>).
- + [Introduction to Azure DNS] (<https://learn.microsoft.com/training/modules/intro-to-azure-dns/>).
- + [Host your domain on Azure DNS] (<https://learn.microsoft.com/training/modules/host-domain-azure-dns/>).

Clean up resources

****Note**:** Remember to remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.

The screenshot shows the Azure portal interface. On the left, there's a navigation bar with 'Home > Resource groups >'. Below it, a 'Resource groups' section has a 'Create' button and a note about viewing a new version of the browse experience. In the center, the 'ContosoResourceGroup' details page is shown with tabs for 'Overview', 'Activity log', 'Access control (IAM)', 'Tags', 'Resource visualizer', 'Events', and 'Settings'. A search bar and filter options ('Type equals all', 'Location equals all') are at the top. Below is a list of resources: contoso.com, CoreServicesVnet, and ManufacturingVM. On the right, a 'Delete a resource group' dialog box is open, asking for confirmation to delete the group. It includes a checkbox for 'Apply force delete for selected Virtual machines and Virtual machine scale sets' and a text input field with 'ContosoResourceGroup'. At the bottom of the dialog are 'Delete' and 'Cancel' buttons. At the very bottom of the screen, a Cloud Shell terminal window is visible, showing a command to remove the resource group.

Home > Resource groups >

Resource groups

Default Directory

+ Create ... Group by none

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Showing 1 - 2 of 2. Display 20 count

ContosoResourceGroup Resource group

Overview Activity log Access control (IAM) Tags Resource visualizer Events Settings

Filter for any field... Type equals all Location equals all

Showing 1 to 19 of 19 records. Show hidden types

Name ↑

contoso.com CoreServicesVnet ManufacturingVM

Delete a resource group

The following resource group and all its dependent resources will be permanently deleted.

Resource group to be deleted

ContosoResourceGroup

Apply force delete for selected Virtual machines and Virtual machine scale sets

Enter resource group name to confirm deletion *

ContosoResourceGroup

Delete Cancel

Switch to Bash Restart Manage files New session Editor Web preview Settings Help

Requesting a Cloud Shell. **Succeeded**. Connecting terminal...

Subscription used to launch your CloudShell bd79b60f-58fb-4efb-aba9-a27fdecc0753 is not registered to Microsoft.CloudShell Namespace. Please follow these instructions "https://aka.ms/RegisterCloudShell" to register. In future, unregistered subscriptions will have restricted access to CloudShell service.

Your Cloud Shell session will be ephemeral so no files or system changes will persist beyond your current session.

MOTD: SqlServer has been updated to Version 22!

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/kvng> Remove-AzResourceGroup -Name 'ContosoResourceGroup' -Force -AsJob

ID	Name	PSJobTypeName	State	HasMoreData	Location	Command
1	Long Running O...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup

PS /home/kvng> █