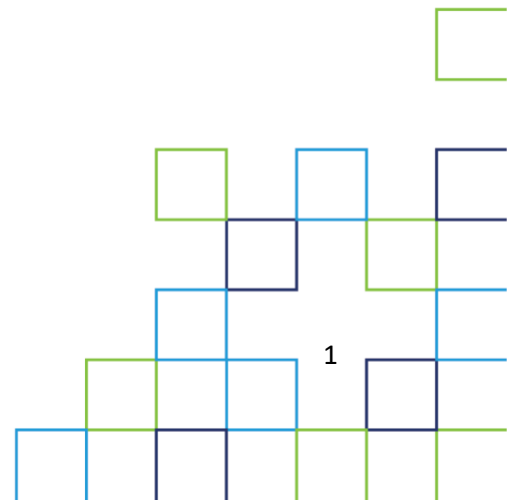


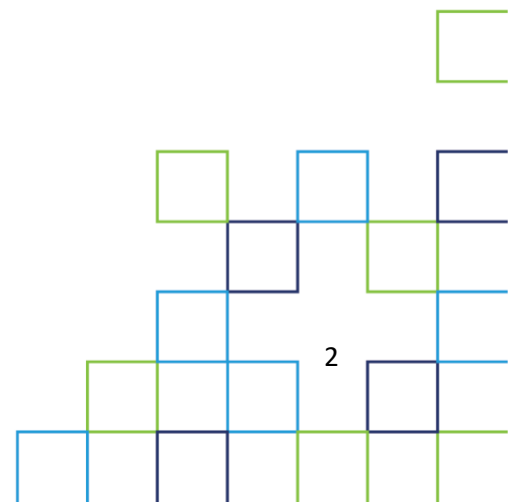
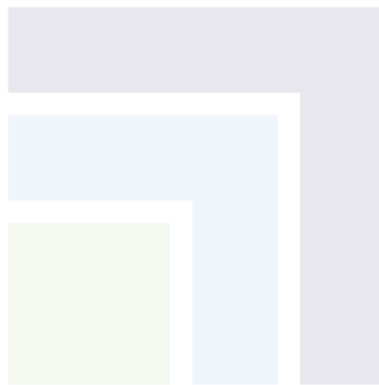
Configuration of Azure-Private DNS Environment in AACN – *aacn.org*

Prepared By:
--Shivam Shah
--Vatsal Patel

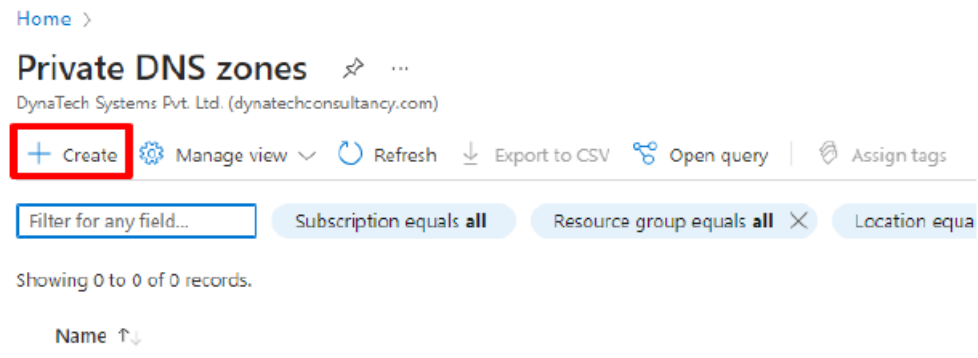


Pre-requisites:

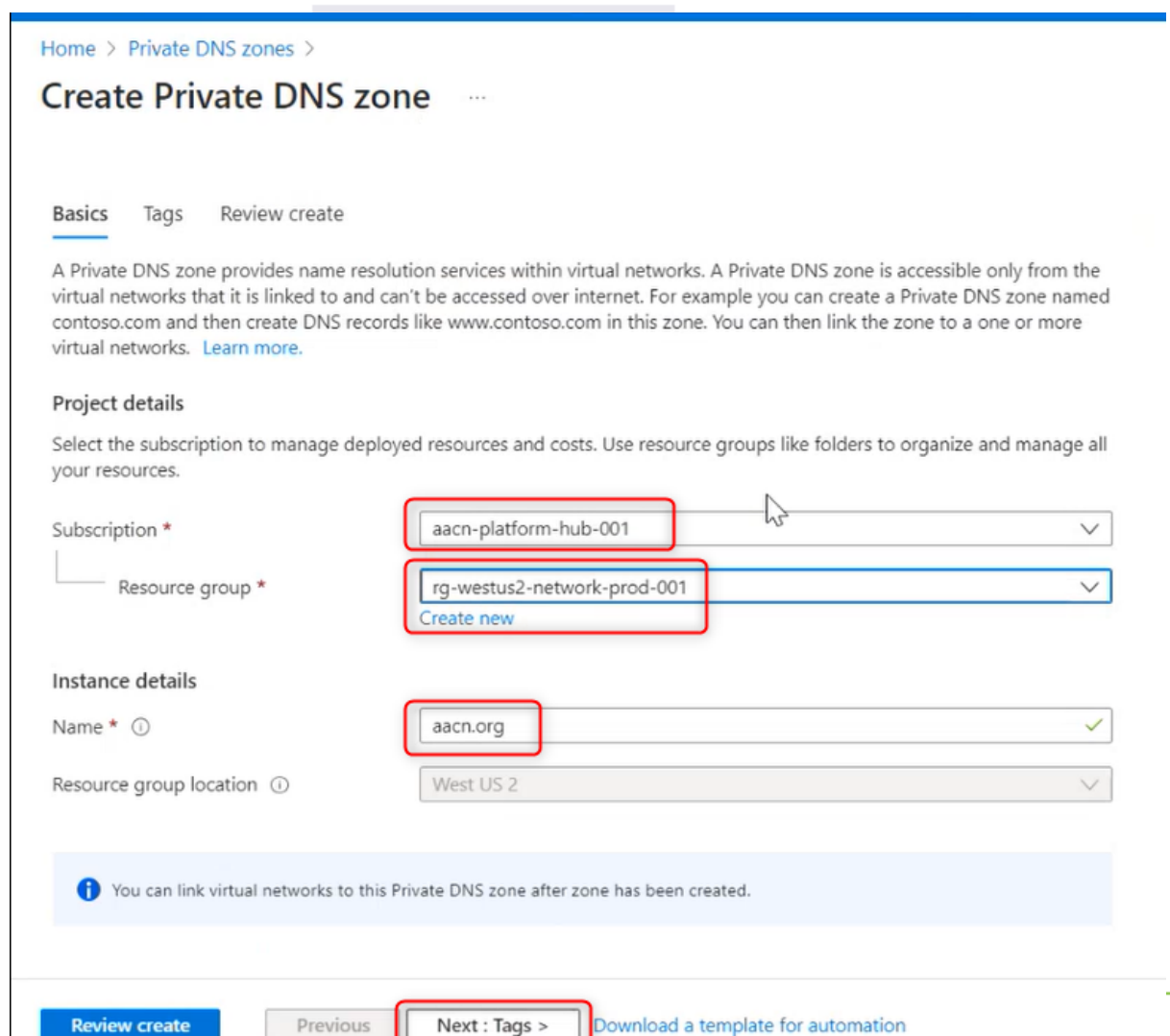
1. Make sure the vnet(site-to-site) is connected and active, and no restrictions are set between both endpoints.
2. Check Pinging to on-premises and on-premises to cloud using private IP address.



- Go to Azure -> Create private DNS zones.



- Select the Subscription, Resource Group, and Instance details name (it is your on prem Domain name).



Home > Private DNS zones >

Create Private DNS zone

Basics Tags Review create

A Private DNS zone provides name resolution services within virtual networks. A Private DNS zone is accessible only from the virtual networks that it is linked to and can't be accessed over internet. For example you can create a Private DNS zone named contoso.com and then create DNS records like www.contoso.com in this zone. You can then link the zone to a one or more virtual networks. [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 * aacn-platform-hub-001

Resource group * rg-westus2-network-prod-001

[Create new](#)

Instance details

Name * aacn.org

Resource group location West US 2

Next : Tags >

[Review create](#) [Previous](#) [Download a template for automation](#)

3

[Home](#) > [Private DNS zones](#) >

Create Private DNS zone

Basics **Tags** Review create

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about how to use tags to organize your Azure Resources](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value
environment	Production

[Review create](#) [Previous](#) [Next : Review create >](#) [Download a template for automation](#)

Home > Private DNS zones >

Create Private DNS zone ...

✓ Validation passed

Basics Tags Review create

Basics

Subscription: aacn-platform-hub-001
 Resource group: rg-westus2-network-prod-001
 Resource group location: westus2
 Name: aacn.org

Tags

environment: Production

Create Previous Next Download a template for automation

Delete
 Cancel
 Redeploy
 Download
 Refresh

Deployment is in progress

Deployment name : NoMarketplace-20230731231531
 Subscription : aacn-platform-hub-001
 Resource group : rg-westus2-network-prod-001

Start time : 7/31/2023, 11:17:09 PM
 Correlation ID : 4132b8c3-2d00-4480-a998-0b89f6e5ece9

Deployment details

Resource	Type	Status	Operation details
✓ aacn.org	Private DNS zone	OK	Operation details

Delete
Cancel
Redeploy
Download
Refresh

Your deployment is complete

Deployment name : NoMarketplace-20230731231531
Subscription : aacn-platform-hub-001
Resource group : rg-westus2-network-prod-001

Start time : 7/31/2023, 11:17:09 PM
Correlation ID : 4132b8c3-2d00-4480-a998-0b89f6e5ece9

Deployment details

Resource	Type	Status	Operation details
aacn.org	Private DNS zone	OK	Operation details

Next steps

Go to resource

5. Go to Virtual network link and add:

Home > NoMarketplace-20230731231531 | Overview > aacn.org

aacn.org | Virtual network links

Private DNS zone

Search
Add
Refresh

Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration
No results.			

Settings

Virtual network links

Properties

Locks

Monitoring

Home > NoMarketplace-20230731231531 | Overview > aacn.org

Add virtual network link

aacn.org

Link name *

link-westus2-aacnorg-prod-001

Virtual network details

i 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 **i**

Subscription * **i**

aacn-platform-hub-001

Virtual network *

vnet-westus2-platform-hub-prod (rg-westus2-network-prod-001)

Select the virtual network used to connect site to site

Configuration

☒ Enable auto registration **i**

This option will auto-registered the VM created using this virtual network

OK

aacn.org | Virtual network links ☆ ...

Private DNS zone

Search

+ Add Refresh

Overview

Activity log

Access control (IAM)

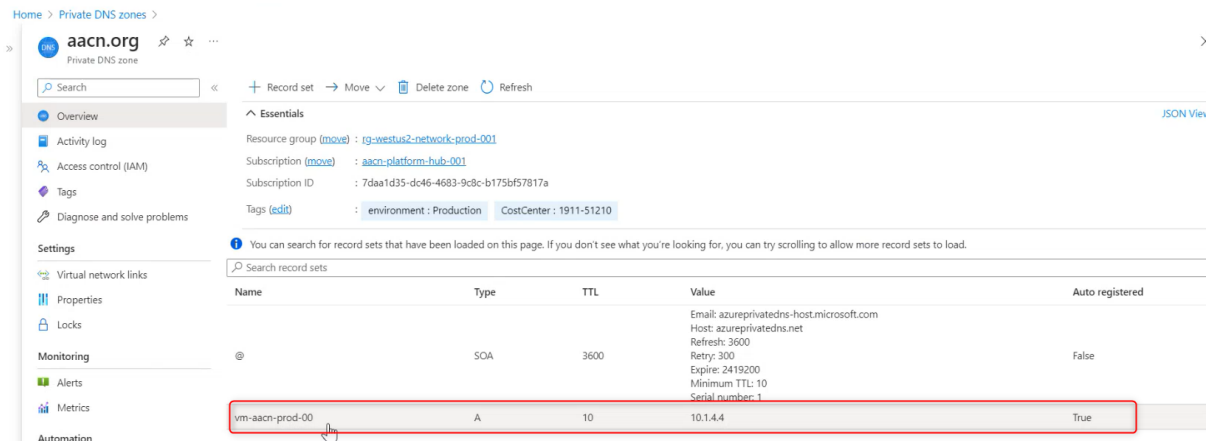
Tags

Diagnose and solve problems

Settings

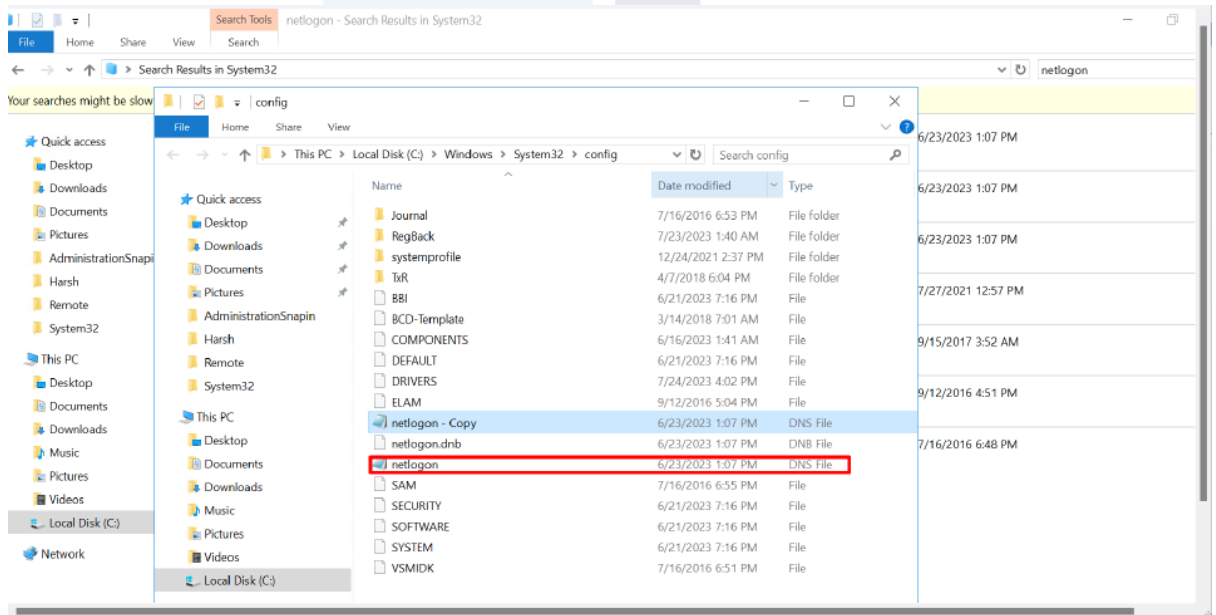
Search virtual network links

Link Name	Link status	Virtual network	Auto-Registration
link-westus2-aacnorg-prod-001	Completed	vnet-westus2-platform-hub-prod	Enabled



6. Go to on-premises AD and go to below path:

Run->"%SystemRoot%\System32\config". Copy netlogon.dns file in your local system.
Need to add those records in Azure Private DNS.



➔ These records are of global catlogs, forest, Domains, Kerberos, Idap purposes.

Name	Type	Value	Priority	Minimum TTL	Serial number
_kerberos_tcp.aacn.org._ldap._msdcs	SRV	0 100 88 DC01.aacn.org	60	False	1
_ldap_tcp.aacn.org._ldap._msdcs	SRV	0 100 88 DC01.aacn.org	60	False	1
_kerberos_tcp._ldap._msdcs	SRV	0 100 88 DC01.aacn.org	60	False	1
_ldap_tcp._ldap._msdcs	SRV	0 100 88 DC01.aacn.org	60	False	1
_ldap_tcp.096288a3-d943-4339-856e-427110c0d6f5.domains._msdcs	SRV	0 100 88 DC01.aacn.org	60	False	1
614689f4-2239-4025-8462-2544b05a23a2._msdcs	CNAME	DC01.aacn.org	60	False	1
gc._msdcs	A	172.16.0.5	60	False	1
_ldap_tcp.aacn.org._ldap._msdcs	SRV	0 100 3268 DC01.aacn.org	60	False	1
_ldap_tcp._ldap._msdcs	SRV	0 100 3268 DC01.aacn.org	60	False	1
_ldap_tcp._ldap._msdcs	SRV	0 100 389 DC01.aacn.org	60	False	1
_gc_tcp.aacn.org._ldap	SRV	0 100 3268 DC01.aacn.org	60	False	1
_kerberos_tcp.aacn.org._ldap	SRV	0 100 389 DC01.aacn.org	60	False	1
_ldap_tcp.aacn.org._ldap	SRV	0 100 389 DC01.aacn.org	60	False	1
_gc_tcp	SRV	0 100 3268 DC01.aacn.org	60	False	1
_kerberos_tcp	SRV	0 100 88 DC01.aacn.org	60	False	1
_ldap_tcp	SRV	0 100 464 DC01.aacn.org	60	False	1
_ldap_tcp	SRV	0 100 389 DC01.aacn.org	60	False	1
_kerberos_udp	SRV	0 100 88 DC01.aacn.org	60	False	1
_ldap_tcp_udp	SRV	0 100 464 DC01.aacn.org	60	False	1
dc01	A	172.16.0.5	60	False	1
domaindnszones	A	172.16.0.5	60	False	1
_ldap_tcp.aacn.org._ldap._msdcs	SRV	0 100 389 DC01.aacn.org	60	False	1
_ldap_tcp._ldap._msdcs	SRV	0 100 389 DC01.aacn.org	60	False	1
forestdnszones	A	172.16.0.5	60	False	1
_ldap_tcp.aacn.org._ldap._msdcs	SRV	0 100 389 DC01.aacn.org	60	False	1
_ldap_tcp._ldap._msdcs	SRV	0 100 389 DC01.aacn.org	60	False	1
vm-aacn-prod-02	A	10.1.4.4	10	True	1

7. Add DNS Ips in virtual networks ->Custom DNS servers (public and Private):

Virtual network: vnet-westus2-platform-hub-prod | DNS servers

Virtual machines and Application gateways(v2 SKU) within this virtual network must be restarted to utilize the updated DNS server settings.

DNS servers

☐ Default (Azure-provided)

☒ Custom

IP Address

172.16.0.5

172.16.0.12

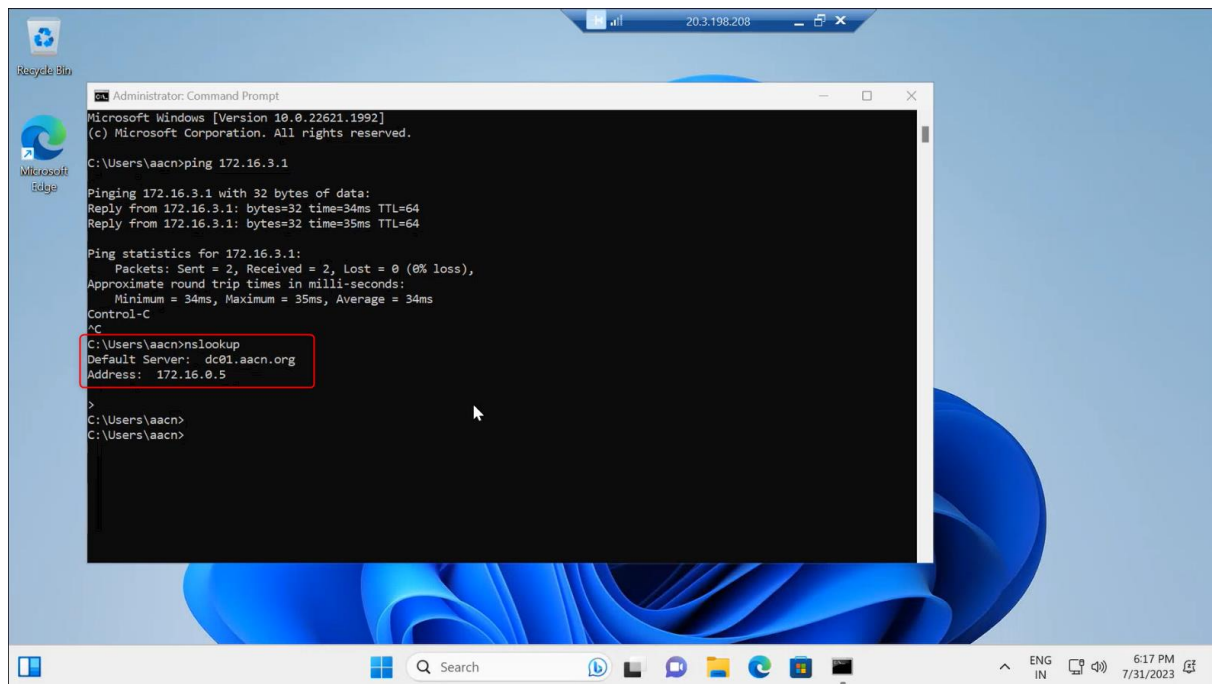
8.8.8.8

8.8.4.4

Add DNS server

Save Cancel

8. Restart the Azure VM:
nslookup should be your private DNS server IP and able to connect using DNS name:



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

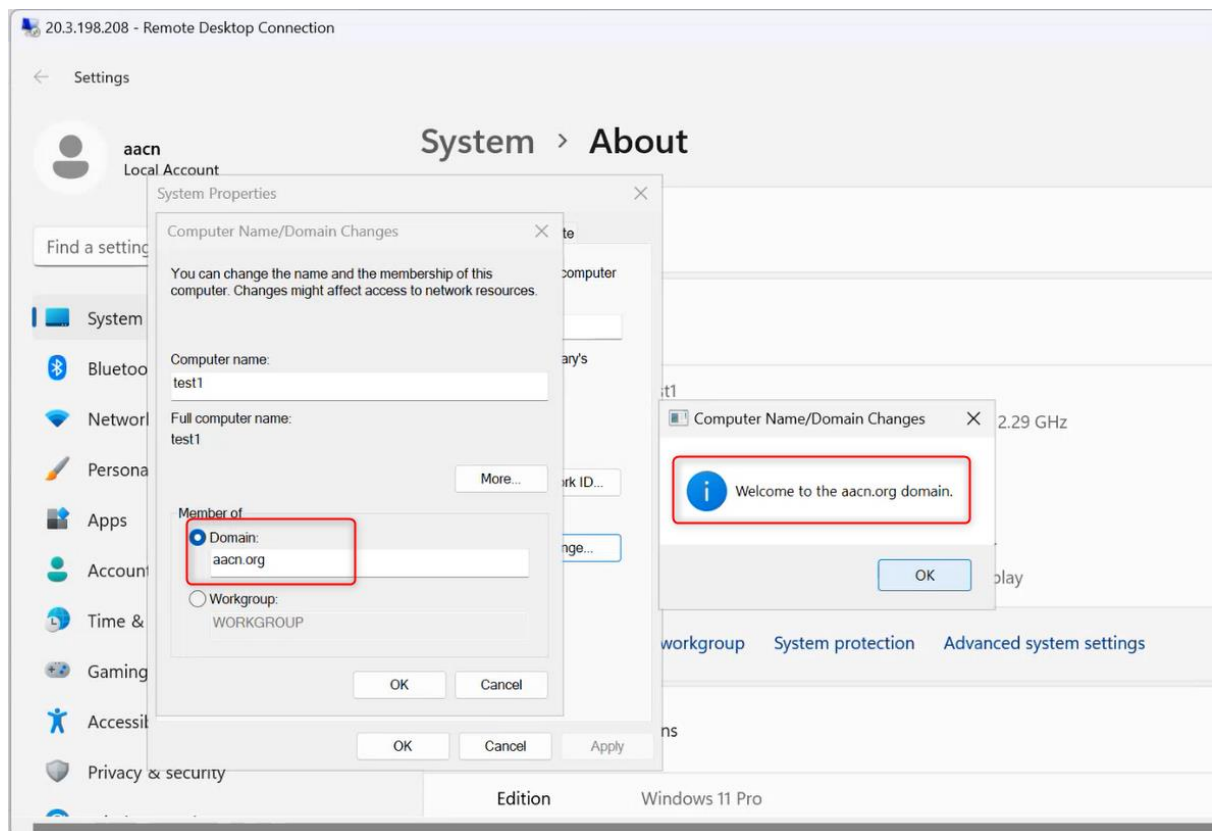
C:\Users\aacn>ping 172.16.3.1

Pinging 172.16.3.1 with 32 bytes of data:
Reply from 172.16.3.1: bytes=32 time=34ms TTL=64
Reply from 172.16.3.1: bytes=32 time=35ms TTL=64

Ping statistics for 172.16.3.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 34ms, Maximum = 35ms, Average = 34ms
Control-C
^C
C:\Users\aacn>nslookup
Default Server: dc01.aacn.org
Address: 172.16.0.5

>
C:\Users\aacn>
C:\Users\aacn>
```

9. Add the Azure VM in LocalAD:



10. Restart the VM. Once, VM is restarted, make sure: Able to see azure VM DNS entry in Local DNS.