



# Designing and Implementing Microsoft Azure Networking Solutions

Exam Ref AZ-700

Charles Pluta

# **Exam Ref AZ-700 Designing and Implementing Microsoft Azure Networking Solutions**

**Charles Pluta**

Delegating a subnet is similar to assigning a user a role that has permissions to change the resource. By delegating the subnet to another Azure service, that service can then modify the configuration of the subnet to provide a managed and recommended configuration.

Subnet delegation can be configured during the creation of the subnet or after the subnet has been created. The Network Contributor role is the lowest-level role that has appropriate permissions to delegate the subnet to a service. Figure 2-8 displays the Delegate subnet to a service dropdown menu of an existing subnet.

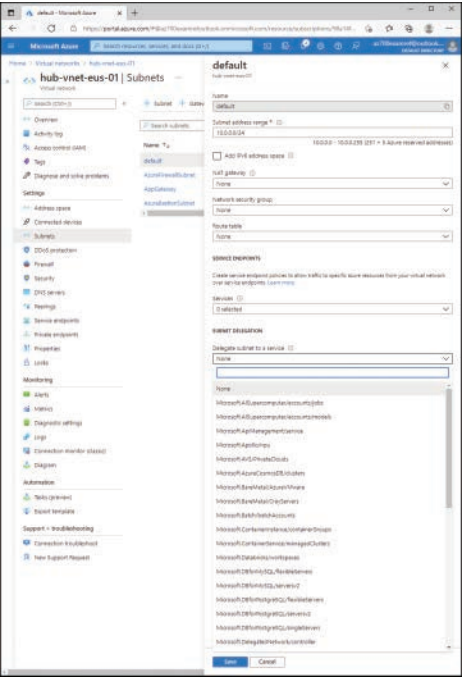


FIGURE 2-8 Subnet delegation

## Plan and configure subnetting for Azure Route Server

Azure Route Server is a service that simplifies the routing for hybrid connectivity. From a virtual network perspective, it is similar to the other services discussed in this skill section in that it requires a dedicated subnet with a specific name: *RouteServerSubnet*. Additionally, the minimum size of the subnet is /27. The virtual network that contains this subnet must be in the same Azure region as the route server that you plan to deploy.

## Skill 2.2: Design and implement name resolution

Name resolution is a critical part of any infrastructure design, and maybe more so in a cloud environment. In an on-premises environment, names are prevalent and commonly used, but

they map to static IP addresses a lot of times, and thus don't change often. However, in the cloud, more and more addresses and services use dynamic IP addresses, making DNS that much more important. Azure has two primary DNS solutions—public and private DNS zones—which are discussed in this skill section.

**This skill covers how to:**

- Design public DNS zones
- Design private DNS zones
- Design name resolution inside a virtual network
- Configure a public or private DNS zone
- Link a private DNS zone to a virtual network

## Design public DNS zones

Azure DNS is a PaaS service that provides an authoritative DNS service for a domain name in your environment. The domain name should be a public domain that you have the ability to configure the name servers for. After you create the public DNS zone, you must change the name servers with the domain registrar so that the records that you create will work properly. This will have an impact on any existing DNS configuration.

To create a public DNS zone, follow these steps:

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. In the search bar, search for and select **DNS zones**.
3. On the DNS zones page, click **Create**.
4. In the Subscription dropdown menu, select the subscription to create the zone in.
5. In the Resource group dropdown menu, create or select a resource group to logically organize the resource in.
6. In the Name field, provide a valid domain name that you own, for example **az700examref.com**.
7. Click **Review + Create**, and then click **Create**. Figure 2-9 displays the completed configuration.

After creating the DNS zone, take note of the name servers provided by the Azure service. These name servers must be configured with the domain so that the records that you create resolve correctly. Each registrar has its own steps and methods of updating the name servers for their domain names. Figure 2-10 displays the name servers assigned to the new az700examref.com zone.

**Create DNS zone**

**Basics** | Tags | Review + create

A DNS zone is used to host the DNS records for a particular domain. For example, the domain 'contoso.com' may contain a number of DNS records such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site). Azure DNS allows you to host your DNS zone and manage your DNS records, and provides name servers that will respond to DNS queries from end users with the DNS records that you create. [Learn more.](#)

**Project details**

Subscription \* Azure Pass - Sponsorship (98a14f31-5601-497f-a903-e874130a9362)

Resource group \* Networking [Create new](#)

**Instance details**

☐ This zone is a child of an existing zone already hosted in Azure DNS. ⓘ

Name \* az700examref.com ✓

Resource group location ⓘ East US

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

FIGURE 2-9 Create DNS zone

**az700examref.com** DNS zone

Search (Ctrl+/) ⌵ + Record set + Child zone → Move ▾ Delete zone Refresh

**Overview**

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
  - Properties
  - Locks
- Monitoring
  - Alerts
  - Metrics
- Automation
  - Tasks (preview)

**Essentials** [JSON View](#)

Resource group (change) : networking

Subscription (change) : Azure Pass - Sponsorship

Subscription ID : 98a14f31-5601-497f-a903-e8...

Name server 1 : ns1-36.azure-dns.com.

Name server 2 : ns2-36.azure-dns.net.

Name server 3 : ns3-36.azure-dns.org.

Name server 4 : ns4-36.azure-dns.info.

Tags (change) : [Click here to add tags](#)

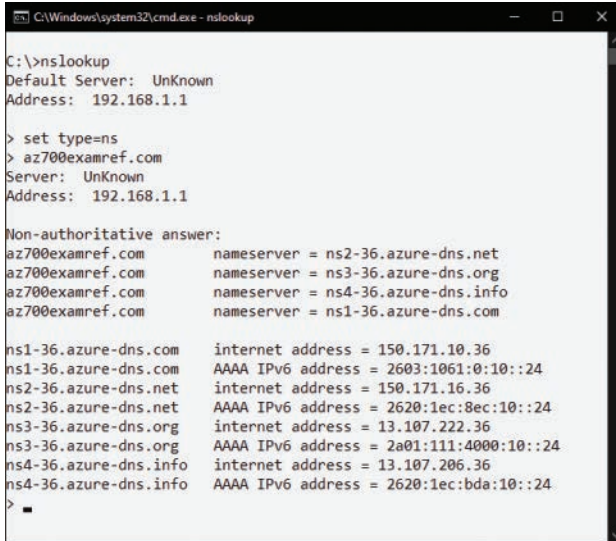
You can search for record sets that have been loaded on this page. If you don't see what you're looking for, you can try scrolling to allow more record sets to load.

Search record sets

Name	Type	TTL	Value
@	NS	172800	ns1-36.azure-dns.com. ns2-36.azure-dns.net. ns3-36.azure-dns.org. ns4-36.azure-dns.info.

FIGURE 2-10 Assigned name servers

After you have made the name server change with the domain registrar, you can verify that the change is accurately propagated on the internet by using *nslookup*. Figure 2-11 shows the *nslookup* utility being used to query the name servers for the *az700examref.com* domain.



```
C:\Windows\system32\cmd.exe - nslookup
C:\>nslookup
Default Server:  UnKnown
Address:  192.168.1.1

> set type=ns
> az700examref.com
Server:  UnKnown
Address:  192.168.1.1

Non-authoritative answer:
az700examref.com      nameserver = ns2-36.azure-dns.net
az700examref.com      nameserver = ns3-36.azure-dns.org
az700examref.com      nameserver = ns4-36.azure-dns.info
az700examref.com      nameserver = ns1-36.azure-dns.com

ns1-36.azure-dns.com  internet address = 150.171.10.36
ns1-36.azure-dns.com  AAAA IPv6 address = 2603:1061:0:10::24
ns2-36.azure-dns.net  internet address = 150.171.16.36
ns2-36.azure-dns.net  AAAA IPv6 address = 2620:1ec:8ec:10::24
ns3-36.azure-dns.org  internet address = 13.107.222.36
ns3-36.azure-dns.org  AAAA IPv6 address = 2a01:111:4000:10::24
ns4-36.azure-dns.info internet address = 13.107.206.36
ns4-36.azure-dns.info AAAA IPv6 address = 2620:1ec:bda:10::24
>
```

FIGURE 2-11 nslookup utility

## Design private DNS zones

Private DNS zones are similar to public zones in that they still contain records for resources and can even be public domain names. However, with a private zone, you do not need to modify the public name servers. Instead, you link the private DNS zone to the virtual networks where you would like name resolution to work. Resolution will then only occur from within the virtual network, and not externally or publicly. This means that the domain name does not even need to be a valid or routable domain.

To create a private DNS zone, follow these steps:

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. In the search bar, search for and select **Private DNS zones**.
3. On the Private DNS zones page, click **Create**.
4. In the Subscription dropdown menu, select the subscription to create the zone in.
5. In the Resource group dropdown menu, create or select a resource group to logically organize the resource in.

6. In the Name field, provide a valid domain name that you own, for example **az700examref.private**.
7. Click **Review + Create**, and then click **Create**. Figure 2-12 displays the completed configuration.

The screenshot shows the 'Create Private DNS zone' page in the Microsoft Azure portal. The page is titled 'Create Private DNS zone' and includes a close button (X) in the top right corner. The page is divided into two main sections: 'Project details' and 'Instance details'. In the 'Project details' section, the 'Subscription' is set to 'Azure Pass - Sponsorship (96a14f31-5601-497f-a903-e874130a9362)' and the 'Resource group' is 'Networking'. In the 'Instance details' section, the 'Name' is 'az700examref.private' and the 'Resource group location' is 'East US'. A message states: 'You can link virtual networks to this Private DNS zone after zone has been created.' At the bottom, there are buttons for 'Review + create', 'Previous', 'Next: Tags >', and 'Download a template for automation'.

**FIGURE 2-12** Private DNS zone creation

#### **NOTE** USING ALTERNATE TOP-LEVEL DOMAINS

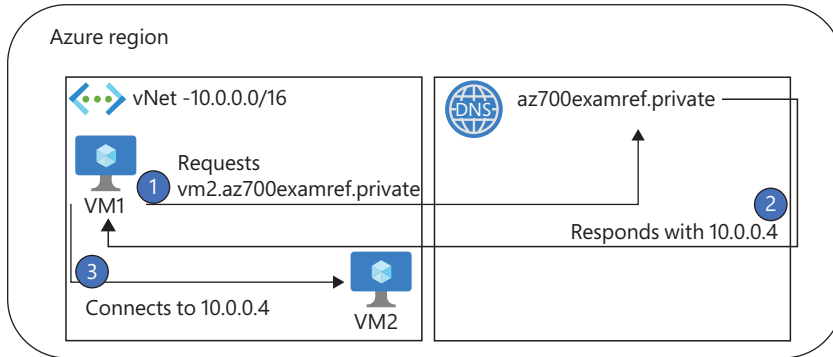
Although we are using a *.private* top-level domain (TLD) name in this scenario to show that the service supports it, it is not recommended to use alternate TLDs because not all operating systems support them.

After a private DNS zone is created and linked to a virtual network, the name resolution occurs within the virtual network. The diagram in Figure 2-13 displays the three steps for VM1 resolving the IP address of VM2:

1. VM1 wants to connect to VM2.az700examref.private but does not know the IP address and requests it from the virtual network's DNS server.



2. The private DNS zone has a record for VM2 and responds to the DNS request with an IP address of 10.0.0.4.
3. VM then connects directly to VM2 using the 10.0.0.4 IP address.



**FIGURE 2-13** Private DNS steps

## Design name resolution inside a virtual network

Determining whether to use public DNS zones, private DNS zones, or a combination of the two is the primary factor for designing how name resolution works in the environment. Private zones give you the flexibility to use a desired naming solution within your virtual network without modifying external, public DNS records. Private zones also give you the ability to configure “split-horizon” DNS where the same fully qualified name, such as `app1.contoso.com`, resolves to one service internally and another service externally. Other benefits of using private zones include:

- Automatic hostname management
- Hostname resolution between virtual networks
- Reverse DNS lookups, but only within the virtual network

Private DNS zones also have limitations. When using automatic registration of hostnames, then the virtual network can only be linked to one private DNS zone. The DNS zone can still have multiple virtual networks linked. Another limitation is that conditional forwarding does not have native support and requires additional configuration to resolve on-premises names.

Both public and private DNS zones in Azure use the same dedicated IP address for DNS queries: `168.63.129.16`. This is a static IP address, and it does not change per zone, subscription, or tenant.