

200 XP 

What is Azure DNS?

7 minutes

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure.

In this unit, you'll learn what DNS is and how it works. Then learn about Azure DNS, and why you would use it.

What is DNS?

DNS, or the Domain Name System, is a protocol within the TCP/IP standard. DNS serves an essential role of translating the human-readable domain names, for example, `www.wideworldimports.com`, into a known IP address. IP addresses enable computers and network devices to identify and route requests between themselves.

DNS uses a global directory hosted on servers around the world. Microsoft is part of that network that provides a DNS service through Azure DNS.

A DNS server is also known as a DNS name server, or just a name server.

How does DNS work?

A DNS server carries out one of two primary functions:

- Maintains a local cache of recently accessed or used domain names and their IP addresses. This cache provides a faster response to a local domain lookup request. If the DNS server can't find the requested domain, it passes the request to another DNS server. This process repeats at each DNS server until either a match is made, or the search times out.
- Maintains the key-value pair database of IP addresses and any host or subdomain that the DNS server has authority over. This function is often associated with mail, web, and other internet domain services.

DNS server assignment

In order for a computer, server, or other network-enabled device to access web-based resources, it must reference a DNS server.

When you connect by using your on-premises network, the DNS settings come from your server. When you connect by using an external location, like a hotel, the DNS settings come from the internet service provider (ISP).

Domain lookup requests

Here's a simplified overview of the process a DNS server uses when it resolves a domain name lookup request:

- Checks to see if the domain name is stored in the short-term cache. If so, the DNS server resolves the domain request.
- If the domain isn't in the cache, it contacts one or more DNS servers on the web to see if they have a match. When a match is found, the DNS server updates the local cache and resolves the request.
- If the domain isn't found after a reasonable number of DNS checks, the DNS server responds with a *domain cannot be found* error.

IPv4 and IPv6

Every computer, server, or network-enabled device on your network has an IP address. An IP address, within your domain, is unique. There are two standards of IP address: IPv4 and IPv6.

- **IPv4** is composed of four numbers, in the range 0 to 255, separated by a dot. Example: 127.0.0.1. Today, IPv4 is the most commonly used standard. Yet, with the increase in IoT devices, the IPv4 standard will eventually be unable to keep up.
- **IPv6** is a relatively new standard and will eventually replace IPv4. It's made up of eight groups of hexadecimal numbers, each separated by a colon. Example: fe80:11a1:ac15:e9gf:e884:edb0:ddee:fea3.

Many network devices are now provisioned with both an IPv4 and an IPv6 address. The DNS name server can resolve domain names to both IPv4 and IPv6 addresses.

DNS settings for your domain

Whether the DNS server for your domain is hosted by a third party or managed in-house, you'll need to configure it for each host type you're using. Host types include web, email, or other services you're using.

As the administrator for your company, you want to set up a DNS server by using Azure DNS. In this instance, the DNS server will act as a start of authority (SOA) for your domain.

DNS record types

The configuration information for your DNS server is stored as a file within a zone on your DNS server. Each file is called a record. The following record types are the most commonly created and used:

- **A** is the host record, and is the most common type of DNS record. It maps the domain or host name to the IP address.
- **CNAME** record indicates that the name it refers to is *not* an alias. In other words, all other records are aliases. If you had different domain names that all accessed the same website, you would use CNAME.
- **MX** is the mail exchange record. It maps mail requests to your mail server, whether hosted on-premises or in the cloud.
- **TXT** is the text record. It's used to associate text strings with a domain name. Azure and Microsoft 365 use TXT records to verify domain ownership.


Additionally, there are the following record types:

- Wildcards
- CAA (certificate authority)
- NS (name server)
- SOA (start of authority)
- SPF (sender policy framework)
- SRV (server locations)

The SOA and NS records are created automatically when you create a DNS zone by using Azure DNS.

Record sets

Some record types support the concept of record sets, or resource record sets. A record set allows for multiple resources to be defined in a single record. For example, here is an A record that has one domain with two IP addresses:

					 Copy
www.wideworldimports.com.	3600	IN	A	127.0.0.1	
www.wideworldimports.com.	3600	IN	A	127.0.0.2	

SOA and CNAME records can't contain record sets.

What is Azure DNS?

Azure DNS allows you to host and manage your domains by using a globally distributed name server infrastructure. It allows you to manage all of your domains by using your existing Azure credentials.

Azure DNS acts as the SOA for the domain.

You can't use Azure DNS to register a domain name. You use a third-party domain registrar to register your domain.

Why use Azure DNS to host your domain?

Azure DNS is built on the Azure Resource Manager service, which offers the following benefits:

- Improved security
- Ease of use
- Private DNS domains
- Alias record sets

At this time, Azure DNS doesn't support Domain Name System Security Extensions. If you require this security extension, you should host those portions of your domain with a third-party provider.

Security features

Azure DNS provides the following security features:

- Role-based access control, which gives you fine-grained control over users' access to Azure resources. You can monitor their usage, and control the resources and services they have access to.
- Activity logs, which let you track changes to a resource, and pinpoint where faults occurred.
- Resource locking, which gives a greater level of control to restrict or remove access to resource groups, subscriptions, or any Azure resources.

Ease of use

Azure DNS can manage DNS records for your Azure services, and provide DNS for your external resources. Azure DNS uses your same Azure credentials, support contract, and billing as your other Azure services.

You can manage your domains and records by using the Azure portal, Azure PowerShell cmdlets, or the Azure CLI. Applications that require automated DNS management can integrate with the service by using the REST API and SDKs.

Private domains

Azure DNS handles the translation of external domain names to an IP address. Azure DNS lets you create private zones. These provide name resolution for virtual machines (VMs) within a virtual network, and between virtual networks, without having to create a custom DNS solution. This allows you to use your own custom domain names rather than the Azure-provided names.

To publish a private DNS zone to your virtual network, you specify the list of virtual networks that are allowed to resolve records within the zone.

Private DNS zones have the following benefits:

- There's no need to invest in a DNS solution. DNS zones are supported as part of the Azure infrastructure.
- All DNS record types are supported: A, CNAME, TXT, MX, SOA, AAAA, PTR, and SVR.
- Host names for VMs in your virtual network are automatically maintained.
- Split-horizon DNS support allows the same domain name to exist in both private and public zones. It resolves to the correct one based on the originating request location.

Alias record sets

Alias records sets can point to an Azure resource. For example, you can set up an alias record to direct traffic to an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network endpoint.

The alias record set is supported in the following DNS record types:

- A
- AAAA
- CNAME

Check your knowledge

1. What does Azure DNS allow you to do?

- ☐ Manage the security and access to your website.
- ☐ Register new domain names, removing the need to use a domain registrar.
- ☐ Manage and host your registered domain and associated records.

2. What security features does Azure DNS provide?

- ☐ Role-based access control, activity logs, and resource locking
- ☐ Role-based access control, activity logs, and Azure threat detection
- ☐ Role-based access control, activity logs, and Azure infrastructure security

3. What type of DNS record should you create to map one or more IP addresses against a single domain?

- ☐ CNAME
- ☐ A or AAAA
- ☐ SOA

Check your answers