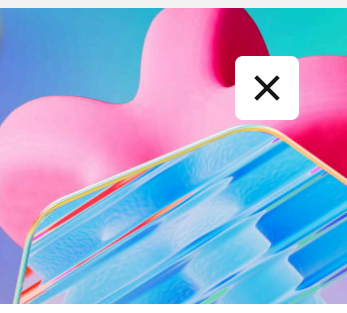

Overview of DNS zones and records

Article • 10/30/2024 • 18 contributors Feedback

In this article

This article explains the key concepts of domains, DNS zones, DNS records, and record sets. You learn how they're supported in Azure DNS.

Domain names

The Domain Name System is a hierarchy of domains. The hierarchy starts from the `root` domain, whose name is simply '.'. Below this come top-level domains, such as `com`, `net`, `org`, `uk` or `jp`. Below the top-level domains are second-level domains, such as `org.uk` or `co.jp`. The domains in the DNS hierarchy are globally distributed, hosted by DNS name servers around the world.

A domain name registrar is an organization that allows you to purchase a domain name, such as `contoso.com`. Purchasing a domain name gives you the right to control the DNS hierarchy under that name, for example allowing you to direct the name `www.contoso.com` to your company web site. The registrar might host the domain on its own name servers on your behalf or allow you to specify alternative name servers.

Azure DNS provides a globally distributed and high-availability name server infrastructure that you can use to host your domain. By hosting your domains in Azure DNS, you can manage your DNS records with the same credentials, APIs, tools, billing, and support as your other Azure services.

Azure DNS currently doesn't support purchasing of domain names. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar. Your domains then can be hosted in Azure DNS for record management. For more information, see Delegate a domain to Azure DNS.

Download PDF

DNS zones

A DNS zone is used to host the DNS records for a particular domain. To start hosting your domain in Azure DNS, you need to create a DNS zone for that domain name. Each DNS record for your domain is then created inside this DNS zone.

For example, the domain 'contoso.com' may contain several DNS records, such as 'mail.contoso.com' (for a mail server) and 'www.contoso.com' (for a web site).

When creating a DNS zone in Azure DNS:

- The name of the zone must be unique within the resource group, and the zone must not exist already. Otherwise, the operation fails.
- The same zone name can be reused in a different resource group or a different Azure subscription.
- Where multiple zones share the same name, each instance is assigned different name server addresses. Only one set of addresses can be configured with the domain name registrar.

> **Note**
>
> You do not have to own a domain name to create a DNS zone with that domain name in Azure DNS. However, you do need to own the domain to configure the Azure DNS name servers as the correct name servers for the domain name with the domain name registrar.
>
> For more information, see **Delegate a domain to Azure DNS**.

DNS records

Record names

In Azure DNS, records are specified by using relative names. A *fully qualified* domain name (FQDN) includes the zone name, whereas a *relative* name does not. For example, the relative record name `www` in the zone `contoso.com` gives the fully qualified record name `www.contoso.com`.

An *apex* record is a DNS record at the root (or *apex*) of a DNS zone. For example, in the DNS zone `contoso.com`, an apex record also has the fully qualified name `contoso.com` (this is sometimes called a *naked* domain). By convention, the relative name '@' is used to represent apex records.

Record types

Each DNS record has a name and a type. Records are organized into various types according to the data they contain. The most common type is an 'A' record, which maps a name to an IPv4 address. Another common type is an 'MX' record, which maps a name to a mail server.

Azure DNS supports all common DNS record types: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV, and TXT. Note that SPF records are represented using TXT records.

Record sets

Sometimes you need to create more than one DNS record with a given name and type. For example, suppose the 'www.contoso.com' web site is hosted on two different IP addresses. The website requires two different A records, one for each IP address. Here is an example of a record set:

```dns
www.contoso.com.        3600    IN    A    134.170.185.46
www.contoso.com.        3600    IN    A    134.170.188.221
```

Azure DNS manages all DNS records using *record sets*. A record set (also known as a *resource* record set) is the collection of DNS records in a zone that have the same name and are of the same type. Most record sets contain a single record. However, examples like the one above, in which a record set contains more than one record, are not uncommon.

For example, suppose you have already created an A record 'www' in the zone 'contoso.com', pointing to the IP address '134.170.185.46' (the first record above). To create the second record you would add that record to the existing record set, rather than create an additional record set.

The SOA and CNAME record types are exceptions. The DNS standards don't permit multiple records with the same name for these types, therefore these record sets can only contain a single record.

Time-to-live

The time to live, or TTL, specifies how long each record is cached by clients before being queried. In the above example, the TTL is 3600 seconds or 1 hour.

In Azure DNS, the TTL gets specified for the record set, not for each record, so the same value is used for all records within that record set. You can specify any TTL value between 1 and 2,147,483,647 seconds.

Wildcard records

Azure DNS supports wildcard records. Wildcard records get returned in response to any query with a matching name, unless there's a closer match from a non-wildcard record set. Azure DNS supports wildcard record sets for all record types except NS and SOA.

To create a wildcard record set, use the record set name '*'. You can also use a name with '*' as its left-most label, for example, '*.foo'.

CAA records

CAA records allow domain owners to specify which Certificate Authorities (CAs) are authorized to issue certificates for their domain. This record allows CAs to avoid mis-issuing certificates in some circumstances. CAA records have three properties:

- **Flags**: This field is an integer between 0 and 255, used to represent the critical flag that has special meaning per RFC6844
- **Tag**: an ASCII string that can be one of the following:
  - **issue**: if you want to specify CAs that are permitted to issue certs (all types)
  - **issuewild**: if you want to specify CAs that are permitted to issue certs (wildcard certs only)
  - **iodef**: specify an email address or hostname to which CAs can notify for unauthorized cert issue requests
- **Value**: the value for the specific Tag chosen

CNAME records

CNAME record sets can't coexist with other record sets with the same name. For example, you can't create a CNAME record set with the relative name `www` and an A record with the relative name `www` at the same time.

Since the zone apex (name = '@') will always contain the NS and SOA record sets during the creation of the zone, you can't create a CNAME record set at the zone apex.

These constraints arise from the DNS standards and aren't limitations of Azure DNS.

NS records

The NS record set at the zone apex (name '@') gets created automatically with each DNS zone and gets deleted automatically when the zone gets deleted. It can't be deleted separately.

This record set contains the names of the Azure DNS name servers assigned to the zone. You can add more name servers to this NS record set, to support cohosting domains with more than one DNS provider. You can also modify the TTL and metadata for this record set. However, removing or modifying the prepopulated Azure DNS name servers isn't allowed.

This restriction only applies to the NS record set at the zone apex. Other NS record sets in your zone (as used to delegate child zones) can be created, modified, and deleted without constraint.

SOA records

A SOA record set gets created automatically at the apex of each zone (name = '@'), and gets deleted automatically when the zone gets deleted. SOA records can't be created or deleted separately.

You can modify all properties of the SOA record except for the `host` property. This property gets preconfigured to refer to the primary name server name provided by Azure DNS.

The zone serial number in the SOA record isn't updated automatically when changes are made to the records in the zone. It can be updated manually by editing the SOA record, if necessary.

> **Note**
>
> Azure DNS doesn't currently support the use of a dot (.) before the '@' in the SOA hostmaster mailbox entry. For example: `john.smith@contoso.xyz` (converted to john.smith.contoso.xyz) and `john\.smith@contoso.xyz` are not allowed.

SPF records

Sender policy framework (SPF) records are used to specify which email servers can send email on behalf of a domain name. Correct configuration of SPF records is important to prevent recipients from marking your email as junk.

The DNS RFCs originally introduced a new SPF record type to support this scenario. To support older name servers, they also allowed the use of the TXT record type to specify SPF records. This ambiguity led to confusion, which was resolved by RFC 7208. It states that SPF records must be created by using the TXT record type. It also states that the SPF record type is deprecated.

SPF records are supported by Azure DNS and must be created by using the TXT record type. The obsolete SPF record type isn't supported. When you import a DNS zone file, any SPF records that use the SPF record type are converted to the TXT record type.

SRV records

SRV records are used by various services to specify server locations. When specifying an SRV record in Azure DNS:

- The *service* and *protocol* must be specified as part of the record set name, prefixed with underscores, such as '_sip._tcp.name'. For a record at the zone apex, there's no need to

specify '@' in the record name, simply use the service and protocol, such as '_sip._tcp'.
- The *priority*, *weight*, *port*, and *target* are specified as parameters of each record in the record set.

TXT records

TXT records are used to map domain names to arbitrary text strings. They're used in multiple applications, in particular related to email configuration, such as the Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

The DNS standards permit a single TXT record to contain multiple strings, each of which can be up to 255 characters in length. Where multiple strings are used, they're concatenated by clients and treated as a single string.

When calling the Azure DNS REST API, you need to specify each TXT string separately. When you use the Azure portal, PowerShell, or CLI interfaces, you should specify a single string per record. This string is automatically divided into 255-character segments if necessary.

The multiple strings in a DNS record shouldn't be confused with the multiple TXT records in a TXT record set. A TXT record set can contain multiple records, *each of which* can contain multiple strings. Azure DNS supports a total string length of up to 4096 characters in each TXT record set (across all records combined).

Tags and metadata

Tags

Tags are a list of name-value pairs and are used by Azure Resource Manager to label resources. Azure Resource Manager uses tags to enable filtered views of your Azure bill and also enables you to set a policy for certain tags. For more information about tags, see Using tags to organize your Azure resources.

Azure DNS supports using Azure Resource Manager tags on DNS zone resources. It doesn't support tags on DNS record sets, although as an alternative, metadata is supported on DNS record sets as explained below.

Metadata

As an alternative to record set tags, Azure DNS supports annotating record sets using *metadata*. Similar to tags, metadata enables you to associate name-value pairs with each record set. This feature can be useful, for example to record the purpose of each record set. Unlike tags, metadata can't be used to provide a filtered view of your Azure bill and can't be specified in an Azure Resource Manager policy.

Etags

Suppose two people or two processes try to modify a DNS record at the same time. Which one wins? And does the winner know that they have overwritten changes created by someone else?

Azure DNS uses Etags to handle concurrent changes to the same resource safely. Etags are separate from Azure Resource Manager 'Tags'. Each DNS resource (zone or record set) has an Etag associated with it. Whenever a resource is retrieved, its Etag is also retrieved. When updating a resource, you can choose to pass back the Etag so Azure DNS can verify the Etag on the server matches. Since each update to a resource results in the Etag being regenerated, an Etag mismatch indicates a concurrent change has occurred. Etags can also be used when creating a new resource to ensure the resource doesn't already exist.

By default, Azure DNS PowerShell uses Etags to block concurrent changes to zones and record sets. The optional *-Overwrite* switch can be used to suppress Etag checks, in which case any concurrent changes that have occurred are overwritten.

At the level of the Azure DNS REST API, Etags are specified using HTTP headers. Their behavior is given in the following table:

Expand table

Header	Behavior
None	PUT always succeeds (no Etag checks)
If-match <etag>	PUT only succeeds if resource exists and Etag matches
If-match *	PUT only succeeds if resource exists
If-none-match *	PUT only succeeds if resource doesn't exist

Limits

The following default limits apply when using Azure DNS:

Public DNS zones

Expand table

Resource	Limit
Public DNS zones per subscription	250 [1]
Record sets per public DNS zone	10,000 [1]
Records per record set in public DNS zone	20
Number of Alias records for a single Azure resource	20

[1]If you need to increase these limits, contact Azure Support.

Next steps

- To start using Azure DNS, learn how to create a DNS zone and create DNS records.
- To migrate an existing DNS zone, learn how to import and export a DNS zone file.

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Additional resources

Training

Module
Host your domain on Azure DNS - Training

Learn how to host the Domain Name System (DNS) records for your domains on Azure infrastructure by using Azure DNS.

Certification
Microsoft Certified: Azure Administrator Associate - Certifications

Demonstrate key skills to configure, manage, secure, and administer key professional functions in Microsoft Azure.