A DNS name, or domain name system name, is a human-readable name used to identify a resource on a network, such as a website, application, or service. DNS names are mapped to IP addresses, which are used by computers to locate and communicate with the resource.

In Azure, a DNS name is used to identify various resources, including virtual machines, web apps, Azure SQL databases, and more. When you create a resource in Azure, you have the option to specify a DNS name that will be used to access the resource.

For example, when you create an Azure App Service web app, you can specify a custom DNS name that will be used to access the web app. This allows you to use a custom domain name for your web app, such as myapp.azurewebsites.net or mycustomdomain.com.

Similarly, when you create an Azure App Gateway, you'll need to specify a DNS name that will be used to access the gateway. This DNS name is typically associated with the public IP address of the gateway, and it's used to route traffic to the appropriate backend targets.

DNS names are managed through DNS servers, which are responsible for resolving DNS names to IP addresses. Azure provides its own DNS service called Azure DNS, which can be used to manage DNS names for Azure resources.

In Azure, a DNS zone is a container that holds information about a specific domain, such as example.com. A DNS zone contains information about the DNS records that define the resources associated with the domain, such as web servers, email servers, and other services.

DNS zones are created and managed using the Azure DNS service, which is a hosting service for DNS domains. Azure DNS provides highly available and scalable DNS resolution for Azure services and third-party services hosted on Azure.

When you create a DNS zone in Azure, you'll specify the name of the domain that the zone will hold information for, such as example.com. You can then create DNS records within the zone to define the resources associated with the domain.

For example, you might create an A record within the zone that points to the IP address of a web server hosting a website for the domain. You can also create other types of records, such as MX records for email servers, CNAME records for aliasing one domain name to another, and more.

DNS zones in Azure can be either public or private. Public DNS zones are used to host DNS records for domains that are publicly accessible on the internet. Private DNS zones, on the other hand, are used to host DNS records for resources that are only accessible within an Azure virtual network.

Overall, DNS zones in Azure provide a centralized way to manage the DNS records for your domains, and can be used to provide highly available and scalable DNS resolution for your Azure services and third-party services hosted on Azure.

In the context of DNS, named servers (also known as name servers or DNS servers) are servers that are responsible for resolving DNS queries for a specific domain or set of domains. When a DNS query is made for a domain name, the named servers are responsible for providing the IP address associated with that domain.

Named servers can be authoritative or recursive. Authoritative name servers are responsible for providing the definitive answers to DNS queries for a specific domain. Recursive name servers, on the other hand, are responsible for resolving DNS queries on behalf of clients, by querying authoritative name servers and caching the results for future use.

In the context of Azure DNS, named servers are used to host DNS zones and provide DNS resolution for Azure services and third-party services hosted on Azure. When you create a DNS zone in Azure, you'll be provided with a set of named servers that are responsible for resolving DNS queries for that zone.

Azure DNS provides highly available and scalable DNS resolution, with automatic failover and load balancing across multiple named servers. This ensures that DNS queries for your domains are resolved quickly and reliably, even in the face of network failures or high traffic loads.

Overall, named servers play a critical role in the functioning of the DNS system, and are essential for providing reliable and scalable DNS resolution for domains on the internet.

In Azure DNS, a record set is a collection of DNS records that share the same name and type. A record set defines the set of resources associated with a specific DNS name.

For example, suppose you have a DNS zone for the domain "example.com", and you want to create a record set for the subdomain "www.example.com". You might create a record set with the name "www" and the type "A", which specifies that the record set will contain one or more A records that define the IP address associated with the "www.example.com" subdomain.

Once you've created the record set, you can add or remove individual records within the set, such as A records, MX records, CNAME records, and more. You can also update the properties of the record set, such as the TTL (Time-To-Live) value, which determines how long DNS resolvers should cache the records in the set.

Record sets can also be used to implement advanced DNS features, such as geo-location based routing and traffic management. For example, you might create multiple record sets with the same name and type, but with different values depending on the location of the client making the DNS query. This can allow you to route traffic to different resources based on the location of the client, providing a better user experience and improved performance.

Overall, record sets in Azure DNS provide a flexible and powerful way to manage the DNS records for your domains, and can be used to implement a wide range of DNS features and configurations.

A CNAME (Canonical Name) record is a type of DNS record used to alias one domain name to another.

When a DNS resolver encounters a CNAME record while processing a query, it will replace the original domain name with the canonical domain name specified in the CNAME record, and then continue processing the query using the new name. This allows a single domain name to be used to refer to multiple resources, without requiring changes to the DNS infrastructure.

For example, suppose you have a web server with the domain name "www.example.com", and you want to alias it to the domain name "webserver.example.com". You might create a CNAME record with the name "www" and the canonical name "webserver.example.com". When a user enters "www.example.com" in their web browser, the DNS resolver will see the CNAME record and replace the name with "webserver.example.com", which will then be used to retrieve the IP address of the web server.

CNAME records can also be used for load balancing and failover. For example, you might create multiple CNAME records with the same name but different canonical names, each pointing to a different web server. When a DNS resolver encounters the CNAME record, it will return one of the IP addresses associated with the canonical names, based on a variety of factors such as geographic location or server availability.

Overall, CNAME records are a powerful and flexible tool for managing DNS resolution and can be used for a wide range of purposes, including aliasing domain names, load balancing, and failover.
