GOOGLE CLOUD PLATFORM

CLOUD DNS

WHAT IS CLOUD DNS

- DNS is a hierarchical distributed database that lets you store IP addresses and other data, and look them up by name.
- Cloud DNS lets you publish your zones and records in the DNS without the burden of managing your own DNS servers and software.
- Cloud DNS offers both public and private managed DNS zones. A public zone is visible to the public Internet, while a private zone is visible only from one or more VPC networks that you specify.
- You can create a private zone with a different set of DNS records, specific to your VPC network called a split horizon DNS

PUBLIC ZONES

- A public zone is visible to the Internet.
- Cloud DNS has public authoritative name servers that respond to queries about public zones regardless of where the queries originate.
- You can create DNS records in a public zone to publish your service on the Internet.
- Cloud DNS assigns a set of name servers when a public zone is created.

DNS Name	Type	TTL (seconds)	Data
www.example.com	A	300	[public_ip_address]

PRIVATE ZONES

- Private zones enable you to manage custom domain names for your virtual machines, load balancers, and other GCP resources without exposing the underlying DNS data to the public Internet.

- A private zone can only be queried by resources in the same project where it is defined.

- For example, you can create a private zone for dev.gcp.example.com to host internal DNS records for experimental applications.

- GCP creates internal DNS names for VMs automatically, even if you do not use Cloud DNS.

- Private zones do not support DNS security extensions (DNSSEC).

DNS FORWARDING

- You can set up DNS forwarding between your non-GCP name servers and GCP's internal name servers.
- Configuring bi-directional forwarding allows instances in your VPC network to look up the addresses of hosts in your on-premises or multi-cloud networks
- This allows hosts on linked networks to look up addresses for resources in your VPC network.
- A DNS server policy allows you to configure inbound and outbound DNS forwarding for a VPC network. You can apply one DNS server policy to a given VPC network.

INBOUND DNS FORWARDING

- Each VPC network provides DNS name resolution services to the VM instances that use it.
- By default, the VPC network's name resolution services are not available outside of that network.
- You can make them available to systems in on-premises networks connected using Cloud VPN or Cloud Interconnect by creating a DNS policy to enable inbound DNS forwarding to the VPC network.
- When a DNS policy is configured, GCP allocates an internal IP address in a subnet (in a region) of your VPC network to serve as a proxy for inbound DNS requests.

OUTBOUND DNS FORWARDING

- You can configure a DNS policy for outbound forwarding by specifying a alternative name servers with internal IP addresses of other GCP VMs in your VPC network or systems
- You can also specify alternative name servers using public IP addresses, which must be accessible on the Internet.
- You can also setup outbound DNS forwarding through the definition of a forwarding zone
- All matching queries for a forwarding zone are forwarded to a set of destination DNS servers

SPLIT HORIZON DNS

- You can use a combination of public and private zones in a split horizon DNS configuration.
- Split horizon DNS is useful if you have separate development, corporate, and production VPC networks:
    - You can define a private zone and authorize access from a development VPC network so that queries from VMs in that network for DNS records in that zone are directed to other VMs in the same network.
    - You can define a second private zone serving the same DNS records with different answers, authorizing access from a corporate network.
    - You can define a third, public zone serving the same DNS records with appropriate public answers suitable for production.

SPLIT HORIZON DNS - EXAMPLE

- For example, suppose you have created both a public zone and a private zone for gcp.example.com
- You've configured the registrar for gcp.example.com to use Cloud DNS name servers, so that your public zone is accessible on the Internet, and you've authorized access to the private zone from your VPC network.
- In the private zone, you create a single record:

DNS Name	Type	TTL (seconds)	Data
foo.gcp.example.com	A	5	10.128.1.35

- In the public zone, you create two records:

DNS Name	Type	TTL (seconds)	Data
foo.gcp.example.com	A	5	104.198.6.142
bar.gcp.example.com	A	50	104.198.7.145

DEMO: CREATE A MANAGED PUBLIC ZONE

1. Go to the Create a DNS zone page in the GCP Console.
2. Choose Public for the **Zone type**.
3. Enter my-new-zone for the **Zone name**.
4. Enter a **DNS name** prefix for the zone using a domain name that you own. For example, example.com.
5. Under **DNSSEC**, keep the Off setting selected.
6. Click **Create**.

DEMO: CREATE A MANAGED PRIVATE ZONE

1. Go to the Create a DNS zone page in the GCP Console.
2. Choose Private for the **Zone type**.
3. Enter my-new-zone for the **Zone name**.
4. Enter a **DNS name** prefix for the zone using a domain name that you own. For example, example.com.
5. Optionally, add a **Description**.
6. Select the networks to which the private zone will be visible.
7. Click **Create**.

DEMO: RECORDS

Create a new record to point the domain to an external IP address

1. Go to the Create a DNS zone page in the GCP Console.
2. Click the zone where you want to add a record set.
3. Click **Add record set**.
4. To create an A record, select A from the **Resource Record Type** menu. To create an AAAA record, select AAAA.
5. Under **IPv4 Address** or **IPv6 Address** section, enter the IP address you want to use with this domain.

Create a CNAME record for the www subdomain

1. Click **Add record set**.
2. Under **DNS Name**, enter www.
3. Under **Resource Record Type**, choose CNAME.
4. Under **Canonical name**, enter the domain name, followed by a period. For example, example.com..
5. Click **Create**.