Managing Zones

This page provides directions for creating Cloud DNS managed zones (/dns/docs/overview#dns-managed-zones). Before you use this page, familiarize yourself with the Cloud DNS concepts (/dns/docs/overview#concepts).

Before you begin

The Cloud DNS API requires that you create a Cloud DNS project and enable the Cloud DNS API.

If you are creating an application that uses the REST API, you must also create an OAuth 2.0 client ID.

1. If you don't already have one, sign up for a Google account (https://accounts.google.com/SignUp).
2. Enable the Cloud DNS API in the Cloud Console (https://console.cloud.google.com/start/api?id=dns&credential=client_key). You can choose an existing Compute Engine or App Engine project, or you can create a new project.
3. If you need to make requests to the REST API, you will need to create an OAuth 2.0 ID: Setting up OAuth 2.0 (https://support.google.com/cloud/answer/6158849).
4. Note the following information in the project that you will need to input in later steps:
    - The client ID (`xxxxxx.apps.googleusercontent.com`).
    - The project ID that you wish to use. You can find the ID at the top of the **Overview** page in the Cloud Console. You could also ask your user to provide the project name that they want to use in your app.

If you have not run the `gcloud` command-line tool previously, you must run the following command to specify the project name and authenticate with the Cloud Console:

```
d auth login
```

If you want to run a `gcloud` command on Google Cloud resources in another project, specify the `--project` option for this command and the other `glcoud` commands throughout this page..

Creating managed zones

Each managed zone (/dns/docs/overview#dns-managed-zones) that you create is associated with a Google Cloud project (/resource-manager/docs/creating-managing-projects). The following sections describe how to create the type of managed zone that Cloud DNS supports.

Creating a public zone

To create a new managed zone:

Consolegcloud (#gcloud)API (#api)

1. Go to the Create a DNS zone page in the Cloud Console.

   Go to the Create a DNS zone page (https://console.cloud.google.com/networking/dns/zones/~n

2. Choose `Public` for the **Zone type**.
3. Enter a **Zone name**. For example, `my-new-zone`.
4. Enter a **DNS name** suffix for the zone using a domain name that you own. All records in the zone share this suffix, for example: `example.com`.
5. Under **DNSSEC**, select `Off`, `On`, or `Transfer`. For more information, see DNSSEC configuration (/dns/docs/dnssec-config#enabling).
6. Click **Create**. The **Zone details** page is displayed.

ant: Cloud DNS creates **NS** and **SOA** records for you automatically when you create the zone. Do not change th of your zone's **NS** record, and do not change the list of name servers that Cloud DNS selects for your zone.

Creating a private zone

To create a new managed private zone with private DNS records managed by Cloud DNS, follow these directions. For additional information, see Best practices for Cloud DNS private zones (/dns/docs/best-practices-dns#best_practices_for_private_zones).

Consolegcloud (#gcloud)API (#api)

1. Go to the Create a DNS zone page in the Cloud Console.

   Go to the Create a DNS zone page (https://console.cloud.google.com/networking/dns/zones/~n

2. Choose `Private` for the **Zone type**.
3. Enter a **Zone name**. For example, `my-new-zone`.
4. Enter a **DNS name** suffix for the private zone. All records in the zone share this suffix, for example: `example.private`.
5. Optionally, add a **Description**.
6. Select VPC networks to which the private zone is visible. Only the VPC networks that you select are authorized to query records in the zone.
7. Click **Create**.

Creating a Service Directory DNS zone

oduct or feature is covered by the Pre-GA Offerings Terms (/terms/service-terms#1) of the Google Cloud Plat of Service. Pre-GA products and features may have limited support, and changes to pre-GA products and feat ot be compatible with other pre-GA versions. For more information, see the launch stage descriptions lucts#product-launch-stages).

You can create a Service Directory zone that allows your Google Cloud-based services to query your Service Directory namespace through DNS.

For detailed instructions on how to create a Service Directory DNS zone, see Configuring a Service Directory DNS zone (/service-directory/docs/configuring-service-directory-zone).

For instructions on how to query your Service Directory using DNS, see Querying using DNS (/service-directory/docs/query-dns).

Creating a managed reverse lookup private zone

A managed reverse lookup zone is a private zone with a special attribute that instructs Cloud DNS to perform a PTR lookup against Compute Engine DNS data. You must set up managed

reverse lookup zones for Cloud DNS to correctly resolve non-RFC 1918 PTR records for your VMs.

Consolegcloud (#gcloud)

1. Go to the Create a DNS zone page in the Cloud Console.

   Go to the Create a DNS zone page (https://console.cloud.google.com/networking/dns/zones/~n

2. Choose `Private` for the **Zone type**.
3. Enter a **Zone name**. For example, `my-new-zone`.
4. Enter a **DNS name** suffix for the zone. The suffix **must** end with `in-addr.arpa` to be a reverse zone. This DNS name must match the reverse lookup name of the non-RFC 1918 PTR records you are trying to resolve through Cloud DNS. For example, if you are trying to match the PTR record for `20.20.1.2`, you must create a reverse look up zone with the dns name of `2.1.20.20.in-addr.arpa`.

   ★ **Note:** Cloud DNS also supports matching of any child zone. For example, if you create a managed reverse lookup zone with the DNS name **`20.in-addr.arpa.`**, the zone will match any VPC-owned address **`20. * . * . *`**.

5. Optionally, add a **Description**.
6. Under **Options**, select `Managed reverse lookup zone`.
7. Select the networks to which the private zone will be visible.
8. Click **Create**.

Creating a forwarding zone

To create a new managed private forwarding zone (/dns/docs/overview#dns-forwarding-zones), follow these directions. Before you begin, ensure that you understand the differences between standard and private routing (/dns/docs/overview#fz-targets) and the network requirements (/dns/zones#firewall-rules) for forwarding targets.

For additional information, see Best practices for Cloud DNS forwarding zones (/dns/docs/best-practices-dns#best_practices_for_dns_forwarding_zones).

1. Go to the **Create a DNS zone** page in the Cloud Console.

   Go to the Create a DNS zone page (https://console.cloud.google.com/networking/dns/zones/~n

2. Choose `Private` for the **Zone type**.
3. Enter a **Zone name**. For example, `my-new-zone`.
4. Enter a **DNS name** suffix for the private zone. All records in the zone share this suffix. For example, `example.private`.
5. Optionally, add a **Description**.
6. Under **Options**, select **Forward queries to another server**.
7. Select the networks to which the private zone will be visible.
8. Click **Add item** to add the IPv4 addresses of a forwarding target. You can add multiple IP addresses.
9. To force private routing to the forwarding target, check the box next to **Enable** under **Private forwarding**. For important background information about routing methods to forwarding targets, see Forwarding targets and routing methods (/dns/docs/overview#fz-targets).
10. Click **Create**.

Creating a peering zone

Create a new managed private peering zone when you need one VPC network, called a *consumer network* to query the VPC name resolution order of another VPC network called the *producer network*. For important background information, see DNS peering (/dns/docs/overview#dns-peering).

Consolegcloud (#gcloud)

Note: You must be logged into the Cloud Console as an IAM member who has the DNS Peer (/dns/docs/access-control#roles) role to the project containing the producer VPC network. You can use a service account with this role if you follow the **`gcloud`** directions instead.

1. Go to the Create a DNS zone page in the Cloud Console.

   Go to the Create a DNS zone page (https://console.cloud.google.com/networking/dns/zones/~n

2. Choose `Private` for the **Zone type**.
3. Enter a **Zone name**. For example, `my-new-zone`.
4. Enter a **DNS name** suffix for the private zone. All records in the zone share this suffix, for example: `example.private`.
5. Optionally, add a **Description**.
6. Select the networks to which the private zone must be visible.
7. Under **DNS peering**, select the box next to **Enable DNS peering**.
8. Under **Peer project**, select a peer project.
9. Under **Peer network**, select a peer network.
10. Click **Create**.

Updating managed zones

Cloud DNS allows you to modify certain attributes of your managed public or managed private zone.

Updating public zones

You can change the description or DNSSEC configuration (/dns/docs/dnssec-config#enabling) of a public zone.

Consolegcloud (#gcloud)

1. Go to the Cloud DNS page in the Cloud Console.

   Go to the Cloud DNS page (https://console.cloud.google.com/networking/dns/zones/)

2. Click the public zone you want to update.
3. Click **Edit**.
4. To change DNSSEC settings, under **DNSSEC**, select `Off`, `On`, or `Transfer`. For more information, see DNSSEC configuration (/dns/docs/dnssec-config#enabling).

★ **Note:** Before you disable DNSSEC for a managed zone that you still want to use, you must deactivate DNSSEC for your zone at your domain registrar to ensure that DNSSEC-validating resolvers can still resolve names in the zone. For details, see Disabling DNSSEC for managed zones (/dns/docs/dnssec-config#disabling).

5. Optionally update the description.
6. Click **Save**.

Updating authorized networks for a private zone

To modify the VPC networks to which a private zone is visible:

Consolegcloud (#gcloud)

1. Go to the Cloud DNS page in the Cloud Console.

   Go to the Cloud DNS page (https://console.cloud.google.com/networking/dns/zones/)

2. Click the private zone you want to update.
3. Click **Edit**.
4. Select the VPC networks to which the private zone is visible. Only the selected VPC networks are authorized to query records in the zone.
5. Click **Save**.

Updating labels

To add new, change existing, remove selected, or clear all labels on a managed zone, use the dns managed-zones update (/sdk/gcloud/reference/dns/managed-zones/update) commands as shown:

```
d dns managed-zones update name \
-update-labels=labels
```

```
d dns managed-zones update name \
-remove-labels=labels
```

```
d dns managed-zones update name \
-clear-labels
```

Replace the following command options:

- ***name***: A name for your zone
- ***labels***: An optional comma-delimited list of key-value pairs such as `Dept:Marketing` or `Project:project1`. For more details, see the SDK documentation (/sdk/gcloud/reference/dns/managed-zones/create#--labels).

Listing and describing managed zones

Listing managed zones

To list all of your zones within a project:

Consolegcloud (#gcloud)

1. Managed zones are shown on the Cloud DNS zone page in the Cloud Console.

   Go to the Cloud DNS page (https://console.cloud.google.com/networking/dns/zones/)

Describing a managed zone

To view attributes of a managed zone:

Consolegcloud (#gcloud)

1. Go to the Cloud DNS zone page in the Cloud Console.

Go to the Cloud DNS page (https://console.cloud.google.com/networking/dns/zones/)

2. Click the zone that you want to inspect.

Deleting a managed zone

You must remove all records in the zone before you can delete the zone.

Consolegcloud (#gcloud)

1. Go to the Cloud DNS page in the Cloud Console.

   Go to the Cloud DNS page (https://console.cloud.google.com/networking/dns/zones/)

2. Click the managed zone that you want to delete.
3. Remove all records in the zone except for the `SOA` and `NS` records. For more information, see Adding or removing a record (/dns/records#adding_or_removing_a_record).
4. Click **Delete zone**.

Forwarding target network requirements

When Cloud DNS sends requests to forwarding targets, it sends packets with the source ranges listed in the following table. For additional background information about the different types of targets, see forwarding targets and routing methods (/dns/docs/overview#fz-targets).

Forwarding target type	Source ranges
• Type 1 targets (VMs in a VPC network authorized to use the forwarding zone) • Type 2 targets (On-premises, connected to a VPC network authorized to use the forwarding zone)	`35.199.192.0/19` Cloud DNS uses the `35.199.192.0/19` source range for all customers. This range is *only* accessible from a Google Cloud VPC network or from an on-premises network connected to a VPC network.

• Type 3 targets (internet accessible)	Google Public DNS source ranges (https://developers.google.com/speed/public-dns/faq#locations)
• Type 4 targets (VMs in a different VPC network authorized to use the forwarding zone)	Google Public DNS source ranges (https://developers.google.com/speed/public-dns/faq#locations)

Type 1 and type 2 targets

Cloud DNS requires the following in order to access a Type 1 or a Type 2 target. These requirements are the same whether the target is an RFC 1918 IP address and you're using standard routing or if you've explicitly chosen private routing:

- **Firewall configuration for `35.199.192.0/19`**: For Type 1 targets, create an ingress allow firewall rule (/vpc/docs/firewalls) for TCP and UDP port `53` traffic, applicable to your forwarding targets in each authorized VPC network. For Type 2 targets, configure an on-premises network firewall and similar equipment to permit TCP and UDP port `53`.
- **Route to the forwarding target**: For Type 1 targets, Cloud DNS uses a subnet route (/vpc/docs/routes#subnet-routes) to access the target in the VPC network authorized to use the forwarding zone. For Type 2 name targets, Cloud DNS uses either custom dynamic or custom static routes (/vpc/docs/routes#custom-routes), except for tagged static routes, to access the forwarding target.
- **Return route to `35.199.192.0/19` through the same VPC network**: For Type 1 targets, Google Cloud automatically adds a special return route (/vpc/docs/routes#cloud-dns) for the `35.199.192.0/19` destination. For Type 2 targets, your on-premises network must have a route for the `35.199.192.0/19` destination, whose next hop is in the same VPC network and region where the request originated, through a Cloud VPN tunnel or Cloud Interconnect attachment (VLAN). For information on how to meet this requirement, see return route strategies for type 2 targets (#return-route).
- **Direct response from target**: Cloud DNS requires that the forwarding target that receives packets be the one that sends replies to `35.199.192.0/19`. If your forwarding target sends the request to a *different* name server, and that *other* name server responds to `35.199.192.0/19`, Cloud DNS ignores the response. For security reasons, Google Cloud expects the source address of each target name server's DNS reply to match the IP address of the forwarding target.

Return route strategies for type 2 targets

Cloud DNS *cannot* send responses from Type 2 forwarding targets over the internet, through a different VPC network, or to a different region (even if it is in the same VPC network). Responses *must* return to the same region and VPC network, though they can use any Cloud VPN tunnel or Cloud Interconnect attachment (VLAN) in that same region and same network.

- For Cloud VPN tunnels that use static routing, manually create a route in your on-premises network whose destination is `35.199.192.0/19` and whose next hop is the Cloud VPN tunnel. For Cloud VPN tunnels that use policy-based routing, configure the Cloud VPN's local traffic selector (/vpn/docs/concepts/choosing-networks-routing#traffic-selectors) and the on-premises VPN gateway's remote traffic selector to include `35.199.192.0/19`.
- For Cloud VPN tunnels that use dynamic routing or for Cloud Interconnect, configure a custom route advertisement (/router/docs/how-to/advertising-custom-ip) for `35.199.192.0/19` on the BGP session of the Cloud Router that manages the tunnel or interconnect attachment (VLAN).

Type 3 targets

When Cloud DNS accesses a non-RFC 1918 IP address using standard routing, it expects the forwarding target to be publicly accessible.

Type 4 targets

When Cloud DNS accesses a non-RFC 1918 IP address of a VM in a different VPC network, it expects the forwarding target to be publicly accessible. Forwarding zones or policies with Type 4 targets must use default routing. Private routing to Type 4 targets is not supported.

Next steps

- Cloud DNS Overview (/dns/docs/overview)
- Troubleshooting Cloud DNS (/dns/docs/troubleshooting)
- Applying Cloud DNS server policies (/dns/docs/policies)

Last updated 2020-07-31 UTC.