Cloud DNS

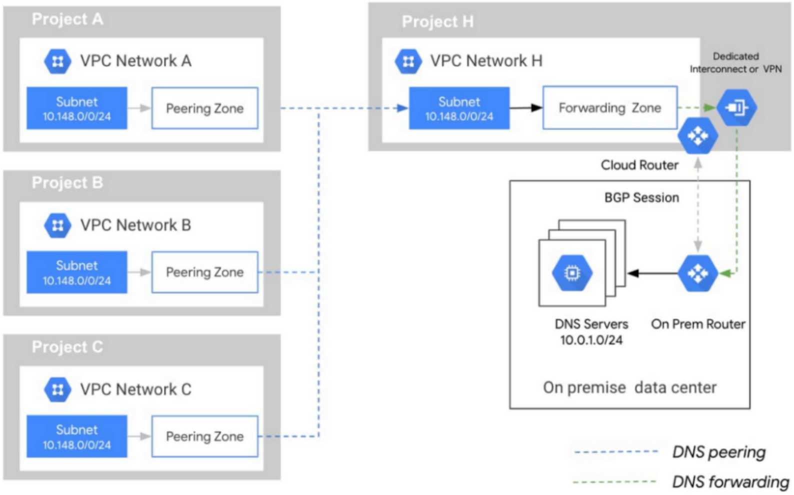
26 June 2021 13:27

Bullet Points: https://jayendrapatil.com/category/gcp/cloud-dns/

Key point

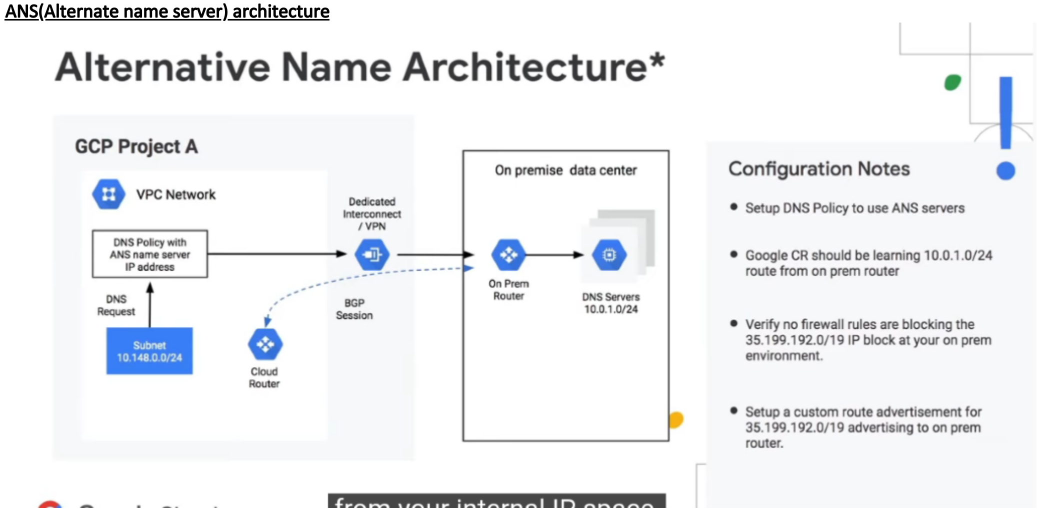
1. Zone (public, private)
2. Record (A -> ipV4, AAA->ipv6, CNAME -> ALIA, DS -> DNSSEC)
3. Inbound and outbound policy
4. Dns forwarding zone (consist of dns name)
5. DNS peering (Peering Zone, Producer Network)
6. TTL cache time
7. DNSSEC for authentication

1. Outbound forwarding dns resolve on-promises from gcp
2. Inbound forwarding dns resolve in gcp from on-promises
3. Dns peering used for dns resolution between two vpc. Vpc peering not required for dns peering.
4. ALT alternative name server forward all dns request, its something like binary.



DNS Architectures

ANS(Alternate name server) architecture



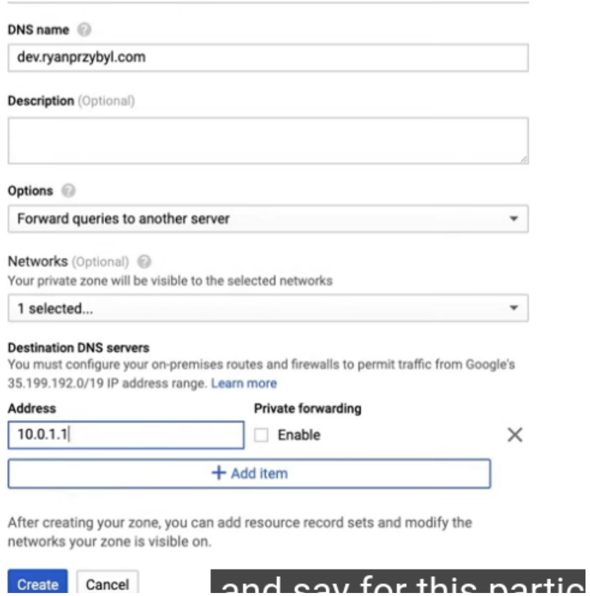
Alternative Name Architecture*

Configuration Notes

- Setup DNS Policy to use ANS servers
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement for 35.199.192.0/19 advertising to on prem router.

In-Bound Forwarding Architecture

Create a private forwarding zone (Outbound forwarding zone)



DNS name
dev.ryanprzybyl.com

Description (Optional)

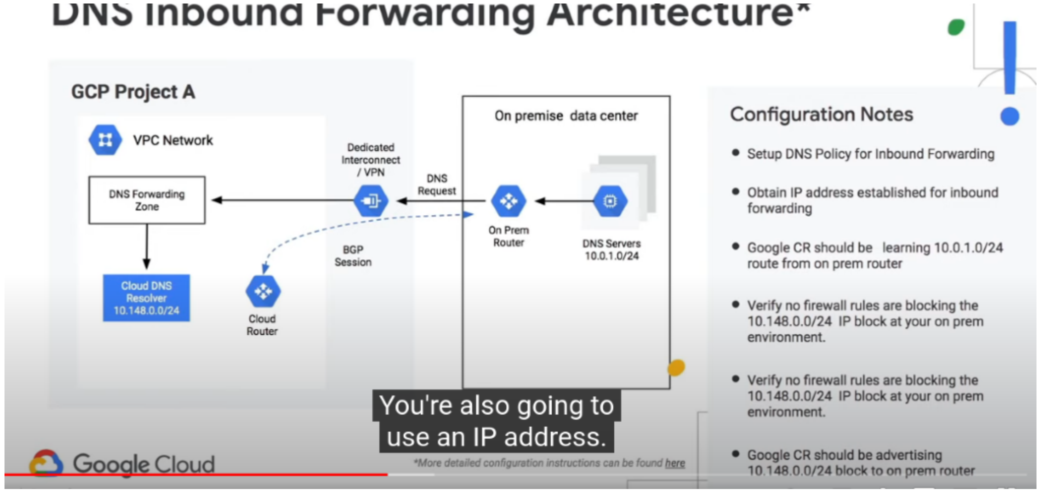
Options
Forward queries to another server

Networks (Optional)
Your private zone will be visible to the selected networks
1 selected...

Destination DNS servers
You must configure your on-premises routes and firewalls to permit traffic from Google's 35.199.192.0/19 IP address range. Learn more

Address: 10.0.1.1
Private forwarding: □ Enable

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.



DNS Inbound Forwarding Architecture*

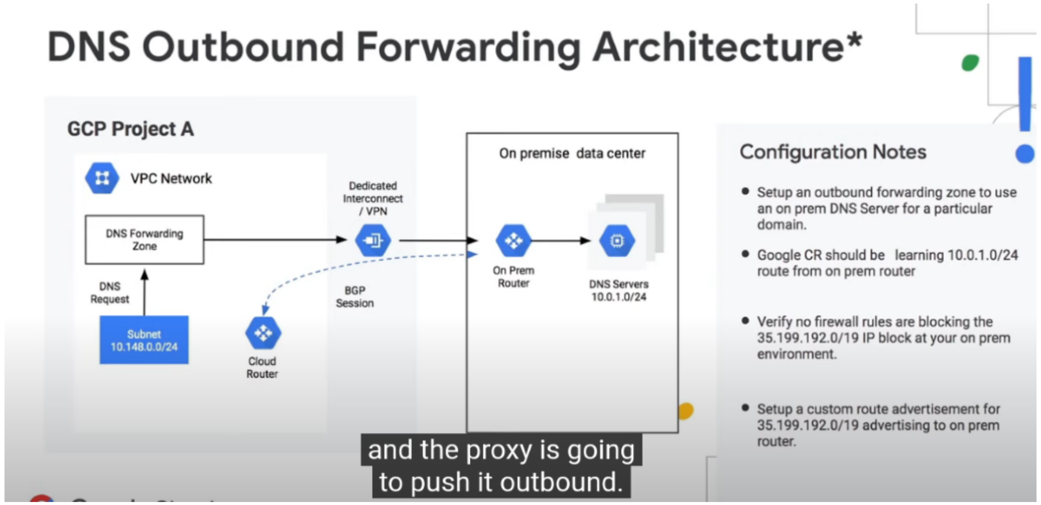
Configuration Notes

- Setup DNS Policy for Inbound Forwarding
- Obtain IP address established for inbound forwarding
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 10.148.0.0/24 IP block at your on prem environment.
- Verify no firewall rules are blocking the 10.148.0.0/24 IP block at your on prem environment.
- Google CR should be advertising 10.148.0.0/24 block to on prem router

*More detailed configuration instructions can be found here

You're also going to use an IP address.

DNS Outbound Forwarding Architecture



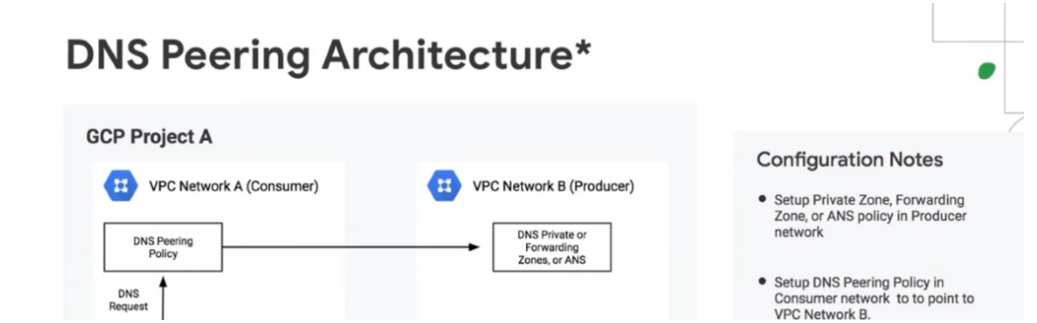
DNS Outbound Forwarding Architecture*

Configuration Notes

- Setup an outbound forwarding zone to use an on prem DNS Server for a particular domain.
- Google CR should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement for 35.199.192.0/19 advertising to on prem router.

and the proxy is going to push it outbound.

DNS Peering



DNS Peering Architecture*

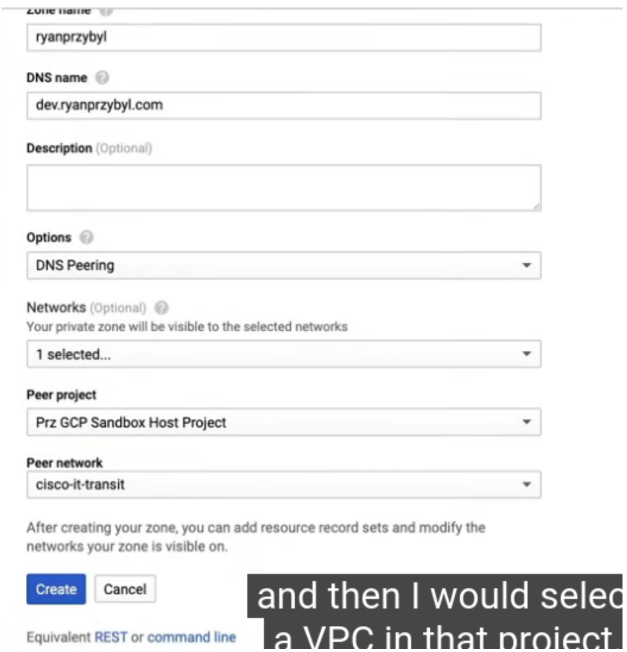
Configuration Notes

- Setup Private Zone, Forwarding Zone, or ANS policy in Producer network
- Setup DNS Peering Policy in Consumer network to point to VPC Network B.

Equivalent REST or command line

and say for this partic zone, dev.ryanprzybyl.c

DNS Peering private zone setup



Zone name: ryanprzybyl

DNS name: dev.ryanprzybyl.com

Description (Optional)

Options: DNS Peering

Networks (Optional)
Your private zone will be visible to the selected networks
1 selected...

Peer project: Prz GCP Sandbox Host Project

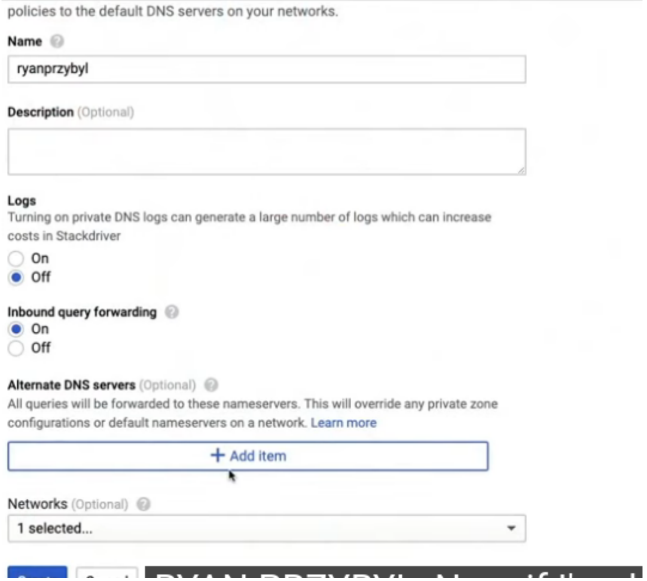
Peer network: cisco-it-transit

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.

Equivalent REST or command line

and then I would selec a VPC in that project

Inbound Forwarding Policy need to be setup in DNS policy section



policies to the default DNS servers on your networks.

Name: ryanprzybyl

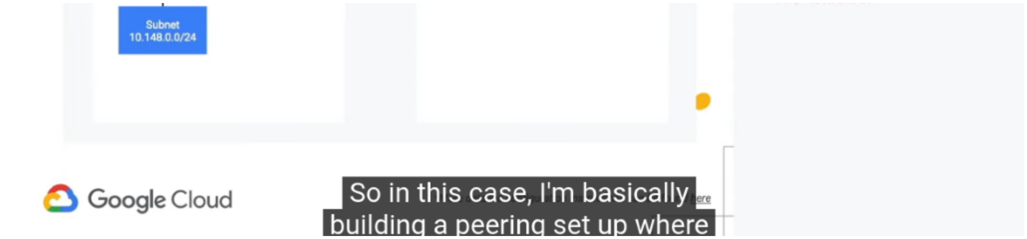
Description (Optional)

Logs
Turning on private DNS logs can generate a large number of logs which can increase costs in Stackdriver
○ On
● Off

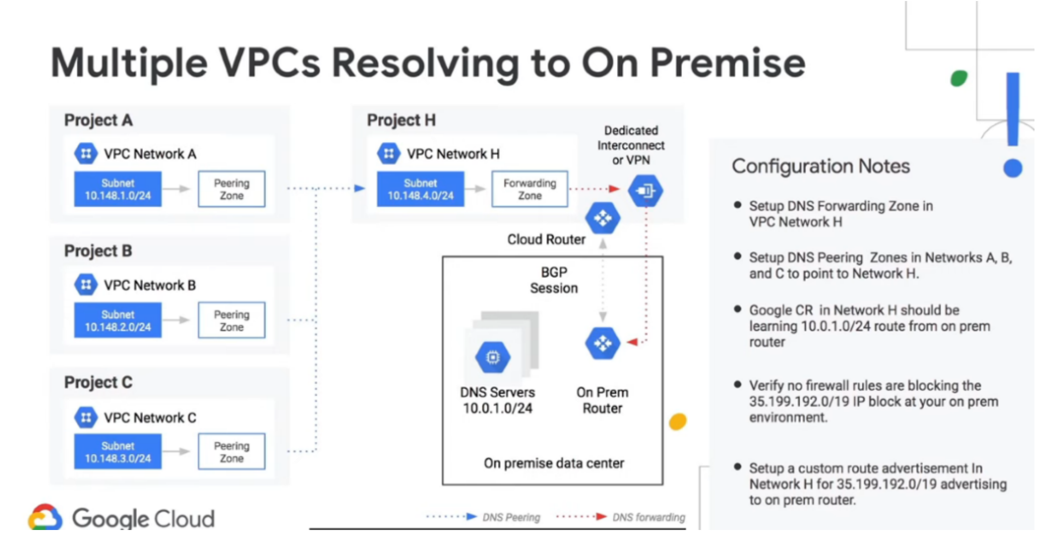
Inbound query forwarding
● On
○ Off

Alternate DNS servers (Optional)
All queries will be forwarded to these nameservers. This will override any private zone configurations or default nameservers on a network. Learn more

Networks (Optional)
1 selected...


Subnet
10.148.0.0/24
Google Cloud
So in this case, I'm basically
building a peering set up where

[Multiple VPC from on-perm](#)



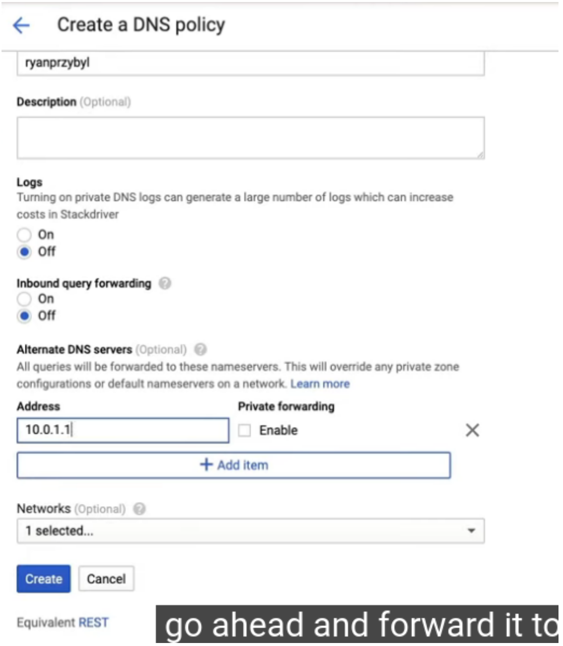
Multiple VPCs Resolving to On Premise

Configuration Notes

- Setup DNS Forwarding Zone in VPC Network H
- Setup DNS Peering Zones in Networks A, B, and C to point to Network H.
- Google CR in Network H should be learning 10.0.1.0/24 route from on prem router
- Verify no firewall rules are blocking the 35.199.192.0/19 IP block at your on prem environment.
- Setup a custom route advertisement In Network H for 35.199.192.0/19 advertising to on prem router.

VPC A,B and C can not be connected directly to on-perm because each vpc use dns proxy 35.x.x.x so on-perm can not decide to which vpc to response to with dns response.

Alternative Name Server Setting with DNS policy



Create a DNS policy

ryanprzybyl

Description (Optional)

Logs
Turning on private DNS logs can generate a large number of logs which can increase costs in Stackdriver

○ On
● Off

Inbound query forwarding
○ On
● Off

Alternate DNS servers (Optional)
All queries will be forwarded to these nameservers. This will override any private zone configurations or default nameservers on a network. Learn more

Address	Private forwarding
10.0.1.1	□ Enable

Networks (Optional)
1 selected...

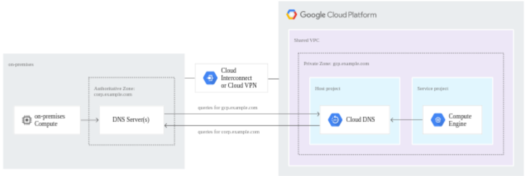
Example architecture

If you use Shared VPC networks within your organization, you must host all the private zones on Cloud DNS within the host project. All service projects automatically can access the records in private zones attached to the Shared VPC network.

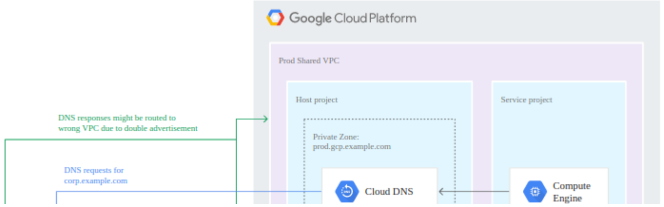
DNS Forwarding Use Case

To make sure that you can query DNS records in your on-premises environment, set up a forwarding zone for the domain that you're using on-premises for your corporate resources (such as *corp.example.com*). This approach is preferred over using a [DNS policy that enables an alternative name server](#). It preserves access to Compute Engine internal DNS names, and public IP addresses are still resolved without an extra hop through an on-premises name server.

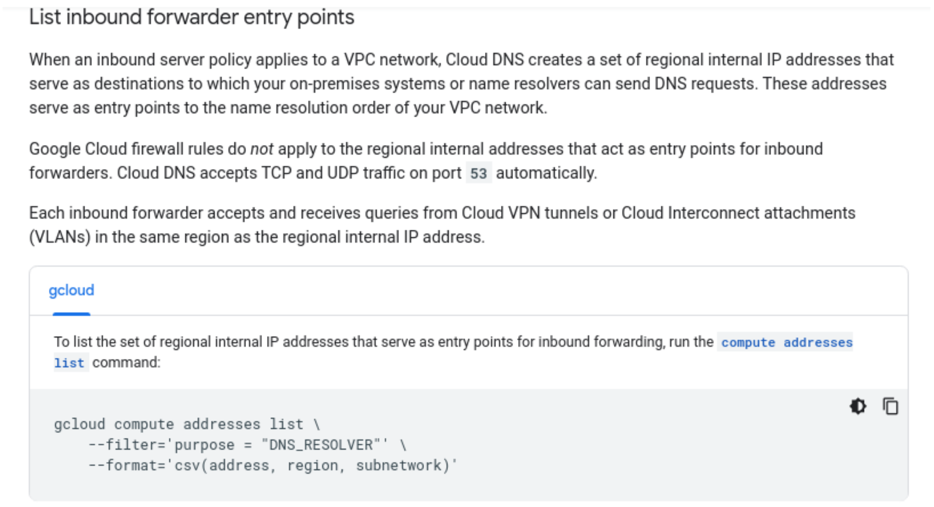
DNS policy use case


Google Cloud Platform
Shared VPC
Private Zone: gcp.example.com
Host project
Service project
Cloud DNS
Compute Engine
Cloud Interconnect or Cloud VPN
on-premises
Authoritative Zone: corp.example.com
on-premises Compute
DNS Server(s)
queries for gcp.example.com
queries for corp.example.com

Private zones hosted in a Shared VPC network (click to enlarge)


Google Cloud Platform
Prod Shared VPC
Host project
Service project
Private Zone: prod.gcp.example.com
Cloud DNS
Compute Engine
DNS responses might be routed to wrong VPC due to double advertisement
DNS requests for corp.example.com

To allow on-premises hosts to query DNS records that are hosted in Cloud DNS private zones (for example, *gcp.example.com*), create a DNS server policy using inbound DNS forwarding. Inbound DNS forwarding allows your system to query all private zones in the project as well as internal DNS IP addresses and peered zones.



List inbound forwarder entry points

When an inbound server policy applies to a VPC network, Cloud DNS creates a set of regional internal IP addresses that serve as destinations to which your on-premises systems or name resolvers can send DNS requests. These addresses serve as entry points to the name resolution order of your VPC network.

Google Cloud firewall rules do *not* apply to the regional internal addresses that act as entry points for inbound forwarders. Cloud DNS accepts TCP and UDP traffic on port `53` automatically.

Each inbound forwarder accepts and receives queries from Cloud VPN tunnels or Cloud Interconnect attachments (VLANs) in the same region as the regional internal IP address.

To list the set of regional internal IP addresses that serve as entry points for inbound forwarding, run the `compute addresses list` command:

```
gcloud compute addresses list \
    --filter='purpose = "DNS_RESOLVER"' \
    --format='csv(address, region, subnetwork)'
```

DNS peering use case

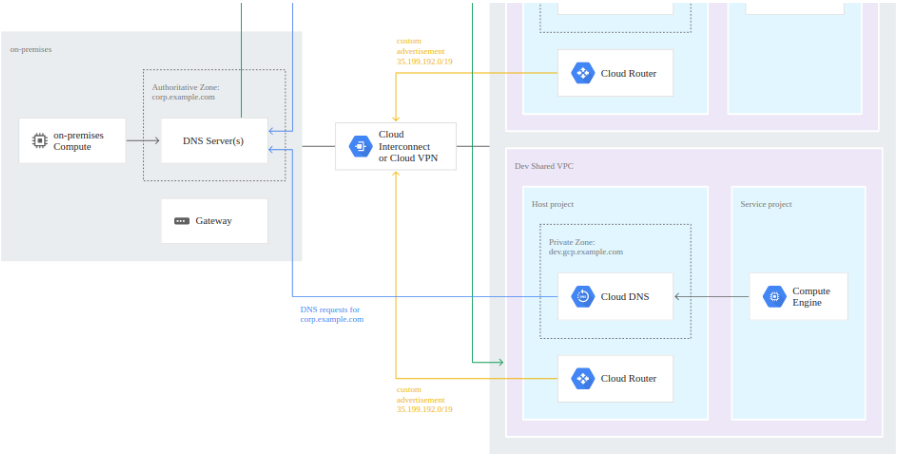
Cloud DNS uses the 35.199.192.0/19 source range for all customers. This range is *only* accessible from a Google Cloud VPC network or from an on-premises network connected to a VPC network.

Do not use outbound forwarding to your on-premises DNS servers from multiple VPC networks because it creates problems with the return traffic. Google Cloud accepts responses from your DNS servers only if they're routed to the VPC network from which the query originated. However, queries from any VPC network have the same IP range 35.199.192.0/19 as source. Therefore, responses can't be routed correctly unless you have separate environments on-premises.

We recommend that you designate a single VPC network to query on-premises name servers by using outbound forwarding. Then, additional VPC networks can query the on-premises name servers by targeting the designated VPC network with a DNS peering zone. Their queries would then be forwarded to on-premises name servers according to the name resolution order of the designated VPC network.

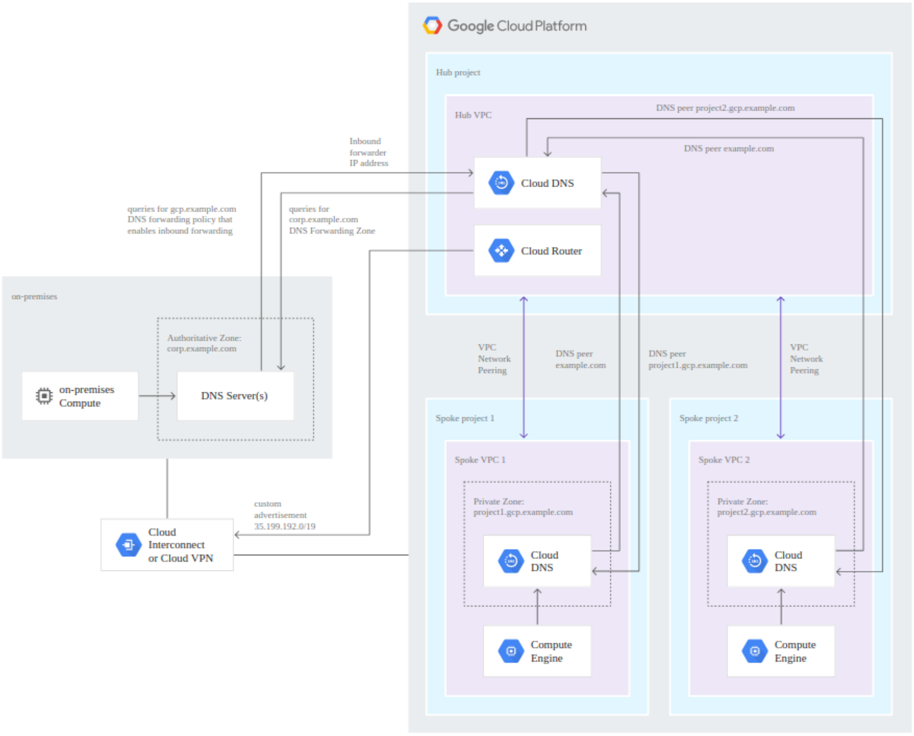
Hub and spoke network

Another option is to use Cloud Interconnect or Cloud VPN to connect the on-premises infrastructure to a single hub VPC network. You use VPC Network Peering to peer this VPC network with several spoke VPC networks. Each spoke VPC network hosts its own private zones on Cloud DNS. Custom routes on VPC Network Peering, along with custom route advertisement on Cloud Router, allow full route exchange and connectivity between on-premises and all spoke VPC networks. DNS peering runs in parallel with VPC Network Peering connections to allow name resolution between environments.



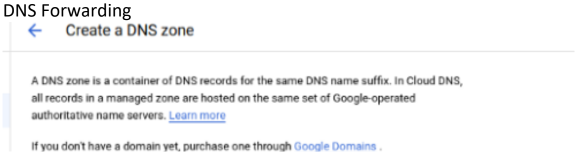
on-premises
Authoritative Zone: corp.example.com
on-premises Compute
DNS Server(s)
Gateway
custom advertisement 35.199.192.0/19
Cloud Router
Cloud Interconnect or Cloud VPN
Dev Shared VPC
Host project
Service project
Private Zone: dev.gcp.example.com
Cloud DNS
Compute Engine
DNS requests for corp.example.com
Cloud Router
custom advertisement 35.199.192.0/19

Hub and Spoke Network



Google Cloud Platform
Hub project
Hub VPC
DNS peer project2.gcp.example.com
DNS peer example.com
Inbound forwarder IP address
Cloud DNS
Cloud Router
queries for gcp.example.com DNS forwarding policy that enables inbound forwarding
queries for corp.example.com DNS Forwarding Zone
on-premises
Authoritative Zone: corp.example.com
on-premises Compute
DNS Server(s)
VPC Network Peering
DNS peer example.com
DNS peer project1.gcp.example.com
VPC Network Peering
Spoke project 1
Spoke VPC 1
Private Zone: project1.gcp.example.com
Cloud DNS
Compute Engine
Spoke project 2
Spoke VPC 2
Private Zone: project2.gcp.example.com
Cloud DNS
Compute Engine
custom advertisement 35.199.192.0/19
Cloud Interconnect or Cloud VPN

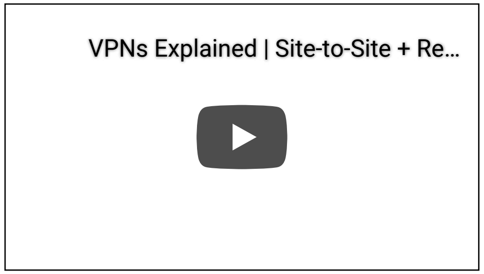
DNS Forwarding

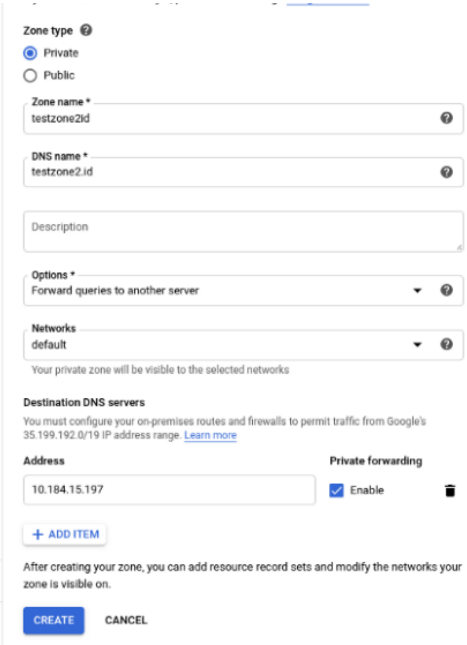


Create a DNS zone

A DNS zone is a container of DNS records for the same DNS name suffix. In Cloud DNS, all records in a managed zone are hosted on the same set of Google-operated authoritative name servers. Learn more

If you don't have a domain yet, purchase one through Google Domains .





Zone type

● Private

○ Public

Zone name *
testzone2id

DNS name *
testzone2.id

Description

Options *
Forward queries to another server

Networks
default

Your private zone will be visible to the selected networks

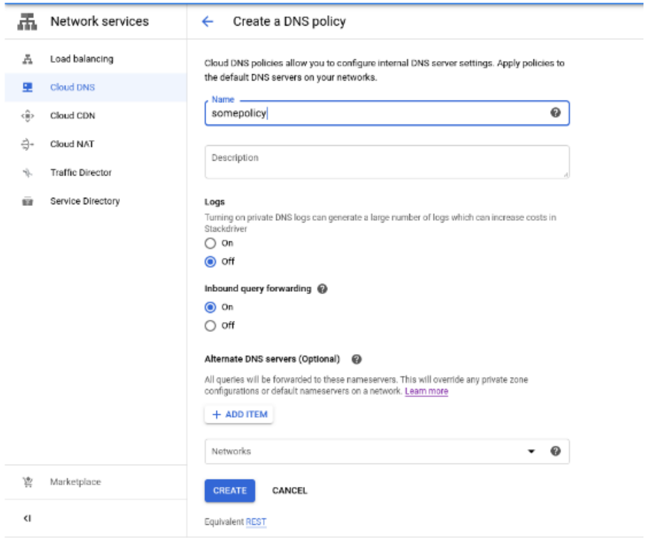
Destination DNS servers

You must configure your on-premises routes and firewalls to permit traffic from Google's 35.199.192.0/19 IP address range. Learn more

Address	Private forwarding
10.184.15.197	☑ Enable

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.

Inbound query forwarding



Create a DNS policy

Cloud DNS policies allow you to configure internal DNS server settings. Apply policies to the default DNS servers on your networks.

Name
somepolicy

Description

Logs

Turning on private DNS logs can generate a large number of logs which can increase costs in Stackdriver

○ On

● Off

Inbound query forwarding

● On

○ Off

Alternate DNS servers (Optional)

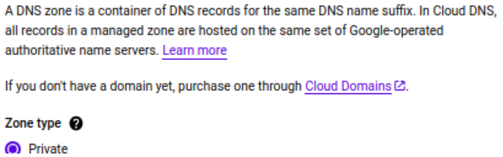
All queries will be forwarded to these nameservers. This will override any private zone configurations or default nameservers on a network. Learn more

Equivalent REST

Create DNS Zone

DNS Zone: Identifies a DNS zone for the project. Must be unique in the project.

DNS Name: The DNS name suffix of the zone



A DNS zone is a container of DNS records for the same DNS name suffix. In Cloud DNS, all records in a managed zone are hosted on the same set of Google-operated authoritative name servers. Learn more

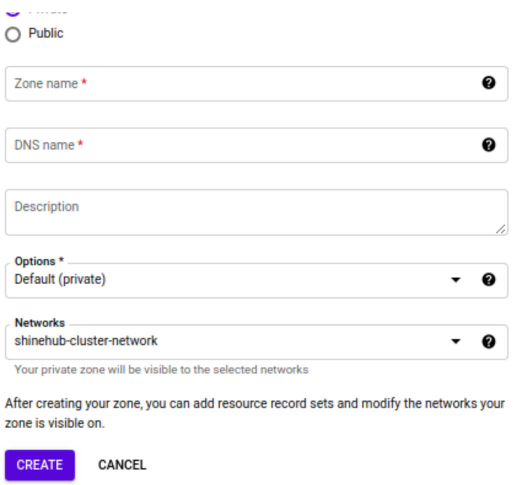
If you don't have a domain yet, purchase one through Cloud Domains.

Zone type

● Private

Concept

[What is DNS? | How a DNS Server (Domain Name System) works | DNS Explained](https://onedrive.live.com)



○ Public

Zone name *

DNS name *

Description

Options *
Default (private)

Networks
shinehub-cluster-network

Your private zone will be visible to the selected networks

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.

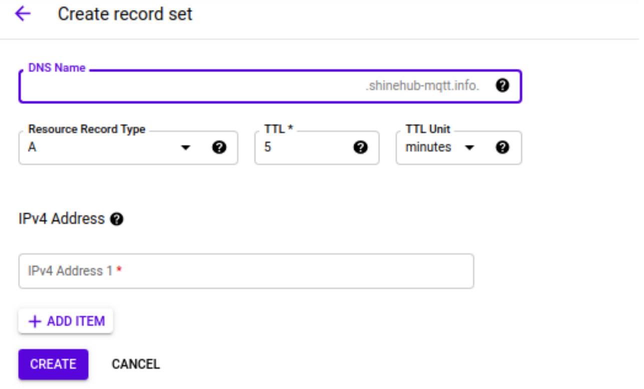
Add record set

A Record set : map a DNS Name(Subdomain of dns zone) to IPv4
AAAA record set: map a DNS Name(Subdomain of dns zone) to IPv6
CNAME: Map an alias subdomain (DNS Name) to a subdomain (A or AAAA type) in Canonical Name
TTL: The resource record's time to live, the amount of time it can be cached

DNSSEC (It defines the server from where we are getting dns server is authentic it doesn't do any encryption)

Cloud DNS supports managed DNSSEC, protecting your domains from spoofing and cache poisoning attacks. When you use a validating resolver like [Google Public DNS](https://developers.google.com/speed/public-dns), DNSSEC provides strong authentication (but not encryption) of domain lookups. For more information about DNSSEC, see [Managing DNSSEC configuration](https://cloud.google.com/dns/docs/dnssec-config).

After enabling DNSSEC for your zone, you must activate DNSSEC at your registrar. You do this by creating a DS record for your domain in the parent zone, so that resolvers know your domain is DNSSEC-enabled and can validate its data.



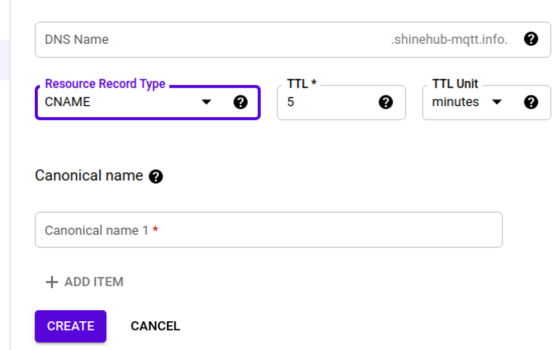
Create record set

DNS Name .shinehub-mqtt.info.

Resource Record Type: A
TTL *: 5
TTL Unit: minutes

IPv4 Address

IPv4 Address 1 *

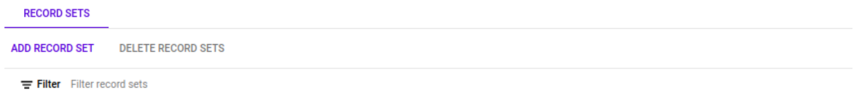


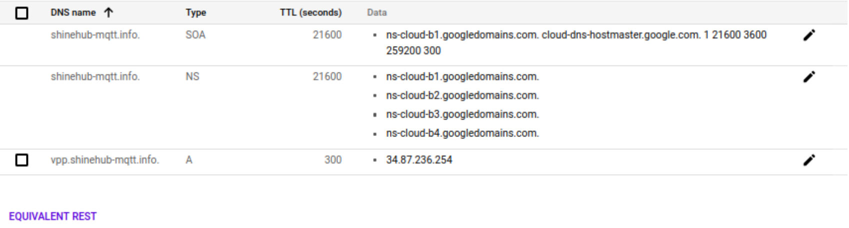
DNS Name .shinehub-mqtt.info.

Resource Record Type: CNAME
TTL *: 5
TTL Unit: minutes

Canonical name

Canonical name 1 *





☐	DNS name ↑	Type	TTL (seconds)	Data	
	shinehub-mqtt.info.	SOA	21600	• ns-cloud-b1.googledomains.com. cloud-dns-hostmaster.google.com. 1 21600 3600 259200 300	✎
	shinehub-mqtt.info.	NS	21600	• ns-cloud-b1.googledomains.com. • ns-cloud-b2.googledomains.com. • ns-cloud-b3.googledomains.com. • ns-cloud-b4.googledomains.com.	✎
☐	vpp.shinehub-mqtt.info.	A	300	• 34.87.236.254	✎

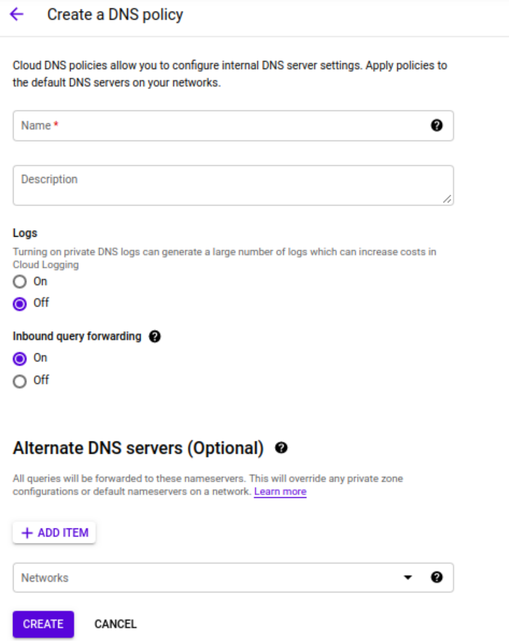
DNS Server Policy

Please refer to below page for DNS policy overview

https://cloud.google.com/dns/docs/server-policies-overview

Alternate DNS servers: Allows to forward all DNS queries for the network to the configured destinations

Inbound query forwarding: Allows users to route DNS queries directly to the Google Cloud default DNS name server



Create a DNS policy

Cloud DNS policies allow you to configure internal DNS server settings. Apply policies to the default DNS servers on your networks.

Name *

Description

Logs

Turning on private DNS logs can generate a large number of logs which can increase costs in Cloud Logging

○ On
● Off

Inbound query forwarding

● On
○ Off

Alternate DNS servers (Optional)

All queries will be forwarded to these nameservers. This will override any private zone configurations or default nameservers on a network. Learn more

DNS Forwarding

In Domain Name System (DNS) terms, a DNS forwarder is a DNS server that is used **to forward DNS queries for external DNS names to DNS servers outside that network**. It does it to DNS queries that it cannot resolve locally, meaning DNS queries that it has no personal knowledge of.

Inbound DNS Forwarding

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 enabled, systems in the connected networks can query an internal IP address in your VPC network in order to make use of its name resolution services.

Outbound DNS forarding

You can change the VPC name resolution order by creating a DNS policy that specifies a list of alternative name servers. When you do this, the alternative name servers become the only source that GCP queries for all DNS requests submitted by VMs in the VPC using their metadata server.

Forwarding Zone
This is similar in setup to a private zone in that it is associated with a DNS name and can be bound to multiple networks. However, the forwarding zone does not contain any records. All matching queries for a forwarding zone are forwarded to a set of destination DNS servers instead. As is the case with alternative name server, the destination is a list of IP addresses.

Ref: https://www.infoq.com/news/2019/01/google-cloud-dns-forwarding/

DNS Peering

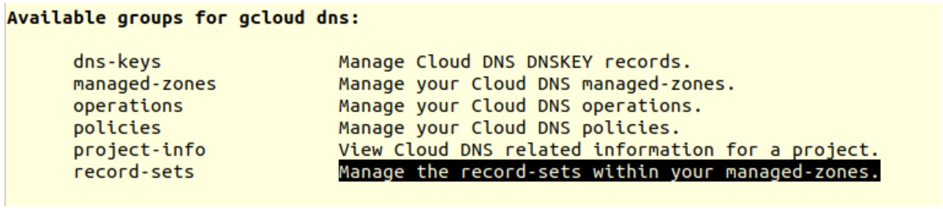
To provide DNS peering, you must create a Cloud DNS peering zone and configure it to perform DNS lookups in a VPC network where the records for that zone's namespace are available. The VPC network where the DNS peering zone performs lookups is called the *DNS producer network*.

Transitive routing using DNS peering

You can use a Cloud DNS peering zone to fix this invalid scenario:

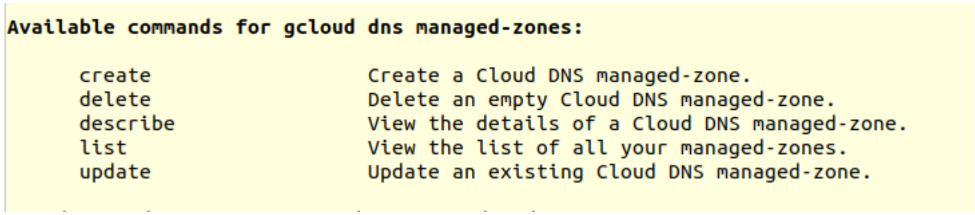
1. Create a Cloud DNS peering zone authorized for vpc-net-b that targets vpc-net-a.
2. Create a forwarding zone authorized for vpc-net-a whose forwarding targets are on-premises name servers.

Gcloud



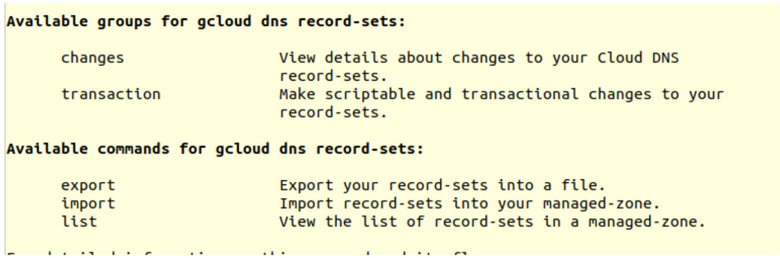
```
Available groups for gcloud dns:

      dns-keys                 Manage Cloud DNS DNSKEY records.
      managed-zones            Manage your Cloud DNS managed-zones.
      operations               Manage your Cloud DNS operations.
      policies                 Manage your Cloud DNS policies.
      project-info             View Cloud DNS related information for a project.
      record-sets              Manage the record-sets within your managed-zones.
```



```
Available commands for gcloud dns managed-zones:

      create                   Create a Cloud DNS managed-zone.
      delete                   Delete an empty Cloud DNS managed-zone.
      describe                 View the details of a Cloud DNS managed-zone.
      list                     View the list of all your managed-zones.
      update                   Update an existing Cloud DNS managed-zone.
```



```
Available groups for gcloud dns record-sets:

      changes                  View details about changes to your Cloud DNS
                               record-sets.
      transaction              Make scriptable and transactional changes to your
                               record-sets.

Available commands for gcloud dns record-sets:

      export                   Export your record-sets into a file.
      import                   Import record-sets into your managed-zone.
      list                     View the list of record-sets in a managed-zone.
```