

Only you can see this message



This story's distribution setting is on. You're in the Partner Program, so this story is eligible to earn money. [Learn more](#)

# How to access a Route 53 Private Zone across multiple VPCs

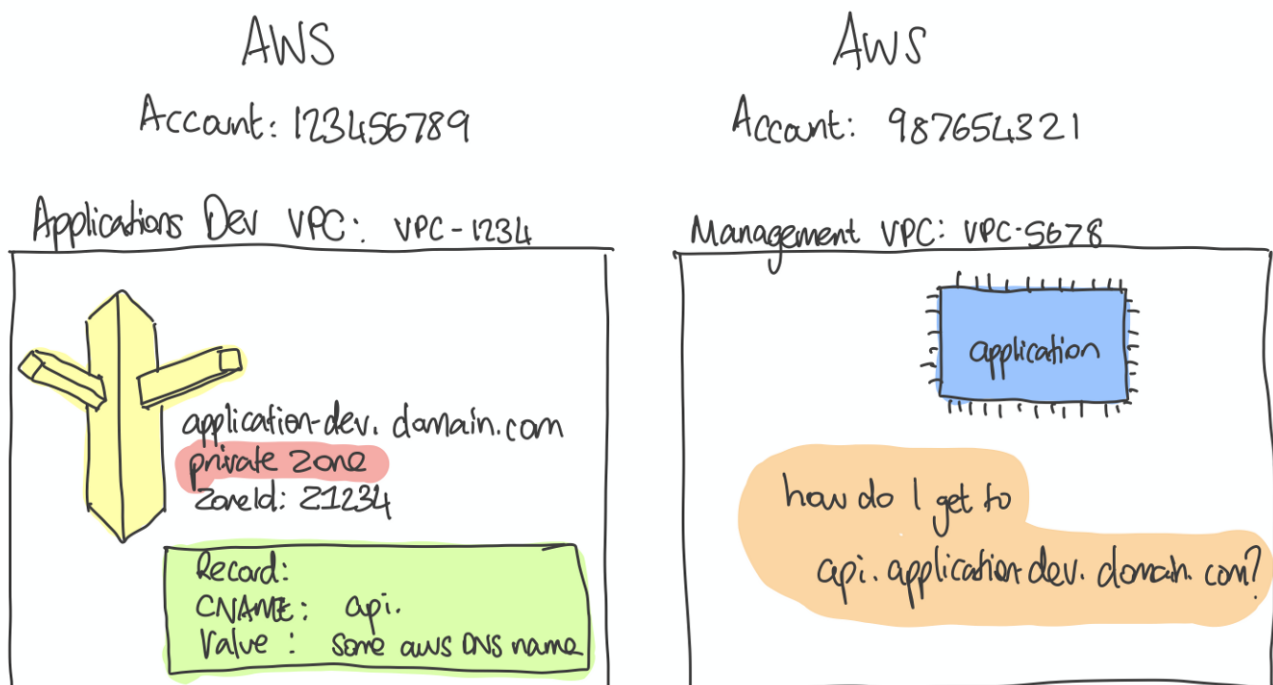


Craig Godden-Payne  
Jun 8 · 2 min read ★

*A route 53 private hosted zone is a container that holds information about how you want Amazon Route 53 to respond to DNS queries for a domain and its subdomains within one or more VPCs that you create with the Amazon VPC service.*

Private zones are convenient when you want to register services for DNS, but then don't want to make the DNS records available publicly.

**Here is an example:**



An application in account 987654321 wants to call a service in account 123456789. A DNS record exists in account 123456789 with the name of api.application-dev.domain.com, but since this is private, it is shared only with its own VPC.

This post only describes how to allow the zone to be associated with multiple VPCs, it is not intended to go over how to peer or connect the vpcs using a transit gateway, that is intended for another post.

## How to associate the private zone with another VPC?

As far as I am aware, this can only be done via the CLI, and not within the AWS console.

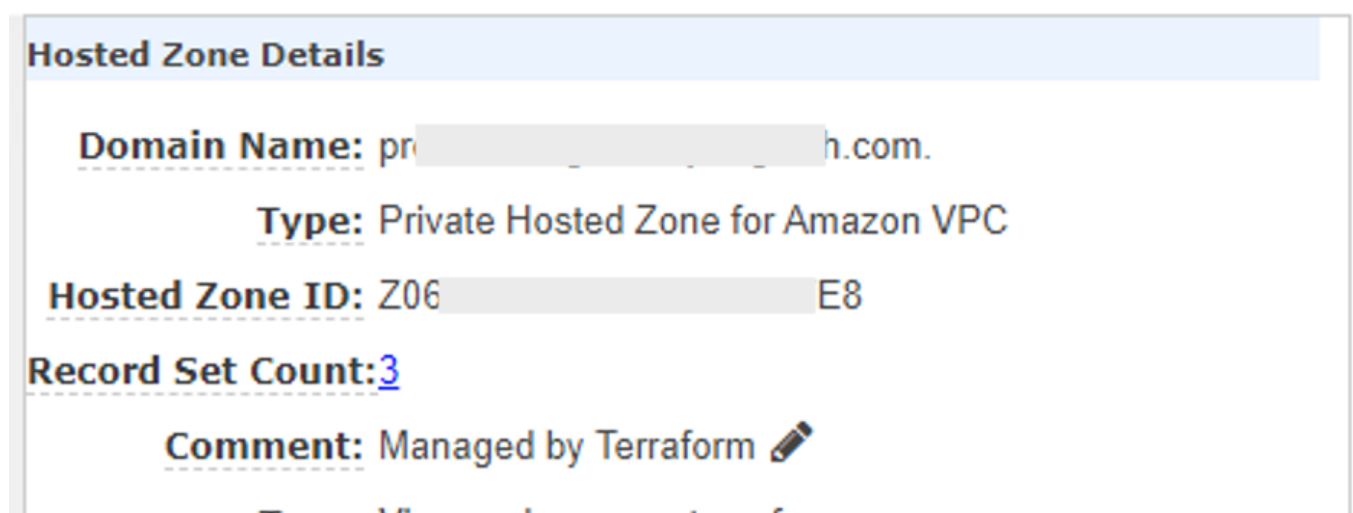
First you need to create a vpc association authorisation, to allow the hosted zone to be shared with the management account. This command is run against the applications-dev account, and the vpc needs to be the management vpc.

```
AWS_PROFILE=applications-dev aws route53 create-vpc-association-authorization --hosted-zone-id=Z1234 --vpc VPCRegion=eu-west-2,VPCId=vpc-5678
```

Next, you need to associate the vpc with the hosted zone. This command is run against the management account, and the vpc needs to be the management vpc.

```
AWS_PROFILE=shared aws route53 associate-vpc-with-hosted-zone --hosted-zone-id=Z1234 --vpc VPCRegion=eu-west-2,VPCId=vpc-5678
```

You will notice now on your zone, that multiple VPCs are now included in the list



The screenshot displays the 'Hosted Zone Details' page in the AWS console. It shows the following information:

- Domain Name:** pr[redacted]h.com.
- Type:** Private Hosted Zone for Amazon VPC
- Hosted Zone ID:** Z06[redacted]E8
- Record Set Count:** 3
- Comment:** Managed by Terraform

At the bottom, there is a link to 'View and manage tags for your zone'.

Tags: view and manage tags for your hosted zones using Tag Editor

Associated VPCs: prod- d12 | eu-west-2 ✕

New Association → vpc- 55 | eu-west-2 ✕

If you perform an NSlookup from VPC2, you will resolve the records you expected, from VPC1's private zone.

Route 53   AWS   DevOps

About   Help   Legal

Get the Medium app

