Introduction

In AWS, DNS comes with VPC as a service. This service accepts DNS queries at its own IP. Its IP is always at VPC's CIDR plus 2.

For example, if a VPC's CIDR is 10.0.0.0/16, the VPC's DNS service IP is 10.0.0.2.

DNS service resolves DNS lookup requests by checking record sets in its hosted zones. A hosted zone contains record sets that share a common domain. A record set is essentially a mapping between a domain name and its associated IP(s), plus a record set type that indicates what type of host it is or what the record set mapping does for the host.

DNS service can have multiple hosted zones for multiple domains.

In AWS, there are two types of zone, Public Hosted Zone, and Private Hosted Zone.

Public Hosted Zone has record sets used to resolve Internet DNS lookups
Private Hosted Zone has record sets used to resolve internal DNS lookups, either in one VPC, in multiple VPCs in one region, or multiple VPCs across regions within your AWS environment

When resolving a lookup, AWS DNS service consults with both Public and Private Hosted Zones, thereby covering both public and private DNS lookups. This comprehensive DNS service in AWS is called AWS Route 53.

In order to best suit your DNS needs in your AWS environment suing AWS Rout 53, certain planning is required to design and set up your public and private hosted zones appropriately and define record sets in those zones accordingly.

Here below are a few guidelines to follow when setting up and configuring Route 53 for your environment

For public domains, you set up and use Public Hosted Zones

1. To create a Public Hosted Zone for a new domain, you register the domain with AWS. AWS automatically creates the Public Hosted Zone for that domain for you at the registration.
2. To create a Public Hosted Zone for an existing domain that you registered with a registrar other than AWS in the past, you transfer that domain into AWS. AWS creates the Public Hosted Zone for that domain for you at the domain transfer.
3. If you do not register a domain with AWS nor transfer a domain into AWS but create a Public Hosted Zone that matches your intended domain in name, that domain will not work.

For VPC internal domains, you set up and use Private Hosted Zones

1. You can create a Private Hosted Zone using AWS Route 53 console or AWS CLI. When creating a Private Hosted Zone, you name the zone with your internal domain name. Your internal domain name does not have to be in compliance with IANA Top Level Domains (TLD). Specifically, your internal domain does not need to end with ".com", ".edu", ".net", or any other name found in

IANA TLD list. Rather, you may name your internal domain by naming the Private Hosted Zone with any a simple word to your liking, like “w2domain”, standing for US West-2 region’s domain.

2. Within your AWS environment, Private Hosted Zone is global. By “global”, it means that you can set up one Private Hosted Zone and associate multiple VPCs in one region or multiple VPCs across multiple regions with the zone. DNS lookups from any associated VPC within your AWS environment are resolvable with corresponding DNS record sets defined in the zone. This feature enables you to either centralize your internal DNS with one or few Private Hosted Zones or segment and isolate your internal DNS with multiple Private Hosted Zones that serve small pockets separately with added DNS security
3. From one VPC you can look up an EC2 instance running in another VPC using one Private Hosted Zone that both VPCs share. When you see the instance domain name is correctly resolved to its IP(s) in a remote VPC, it does not mean you can access that instance. Instance access across VPCs is always subject to inter-VPC routing or VPC Peering regardless if the instance is resolvable by internal DNS lookup across VPCs

In this article, we provided you with a Route 53 example. In the context of the example, we illustrate how Route 53 DNS works by running DNS lookups from multiple EC2 instances, and those instances are running in different subnets, VPCs, and have their own domain names in either internal domains, public domains, or in both.

Route 53 Example

In this example, there are six Route 53 hosted zones that serve 16 VPCs in four regions.
Of the six hosted zones, two are Public Hosted Zones, four are Private Hosted Zones

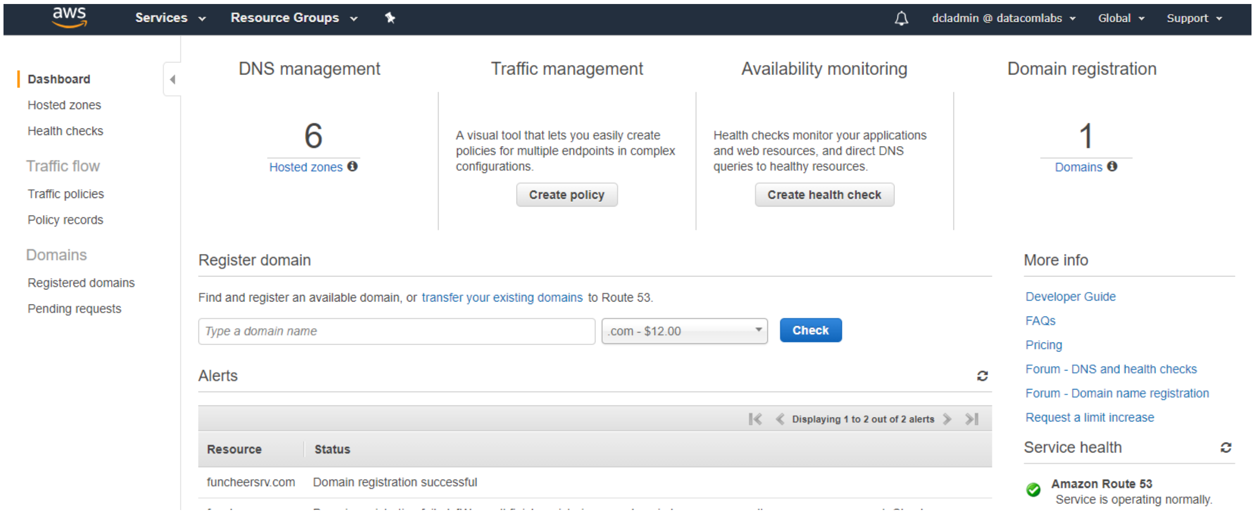
Public Hosted Zones

1. Datacommlabs.com – registered with a registrar other than AWS, not transferred into AWS, it was created using Route 53 console
2. Funcheersrv.com – registered with AWS, created by AWS at the time of registration

Private Hosted Zones

1. E1domain – created for N. Virginia (US East 1) region. Four VPCs in the region are associated with the zone
2. E2domain – created for Ohio (US East 2) region. Four VPCs in the region are associated with the zone
3. W1domain – created for N. California (US West 1) region. Four VPCs in the region are associated with the zone
4. W2domain – created for Oregon (US West 2) region. Four VPCs in the region are associated with the zone

Figure 1 – Route 53 Dashboard



6 Hosted zones

A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

1 Domains

Register domain

Find and register an available domain, or transfer your existing domains to Route 53.

Type a domain name | .com - $12.00

Alerts

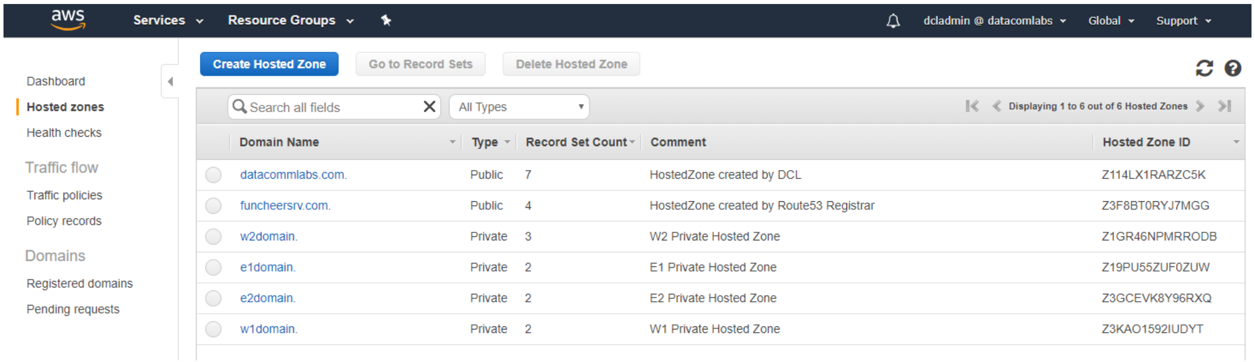
Displaying 1 to 2 out of 2 alerts

Resource	Status
funcheersrv.com	Domain registration successful

Service health

Amazon Route 53
Service is operating normally.

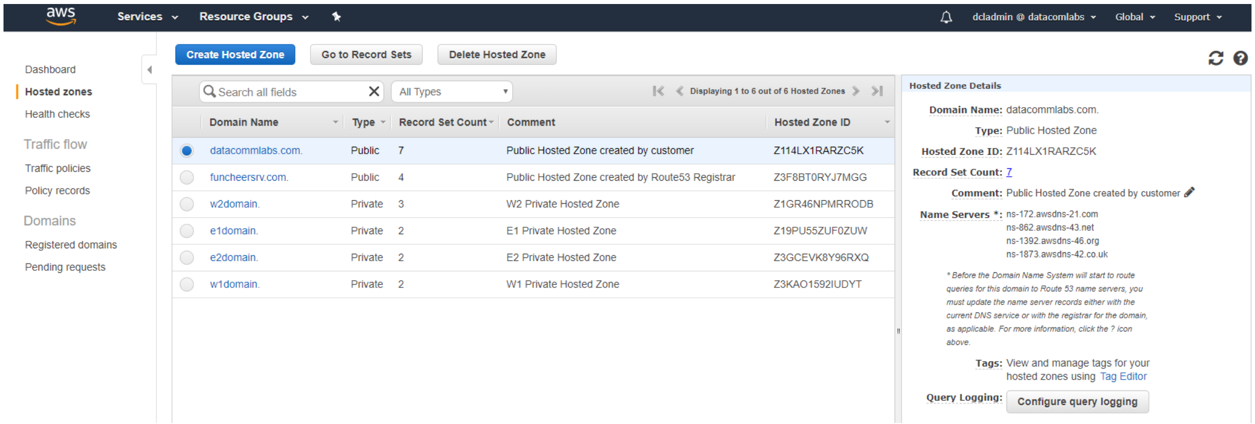
Figure 2 - Six (6) Route 53 Hosted Zones



Displaying 1 to 6 out of 6 Hosted Zones

Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
datacommlabs.com.	Public	7	HostedZone created by DCL	Z114LX1RARZC5K
funcheersrv.com.	Public	4	HostedZone created by Route53 Registrar	Z3F8BT0RYJ7MGG
w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB
e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT

Figure 3 – Public Hosted Zone created by customer



Displaying 1 to 6 out of 6 Hosted Zones

	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
●	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
○	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
○	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB
○	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
○	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
○	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT

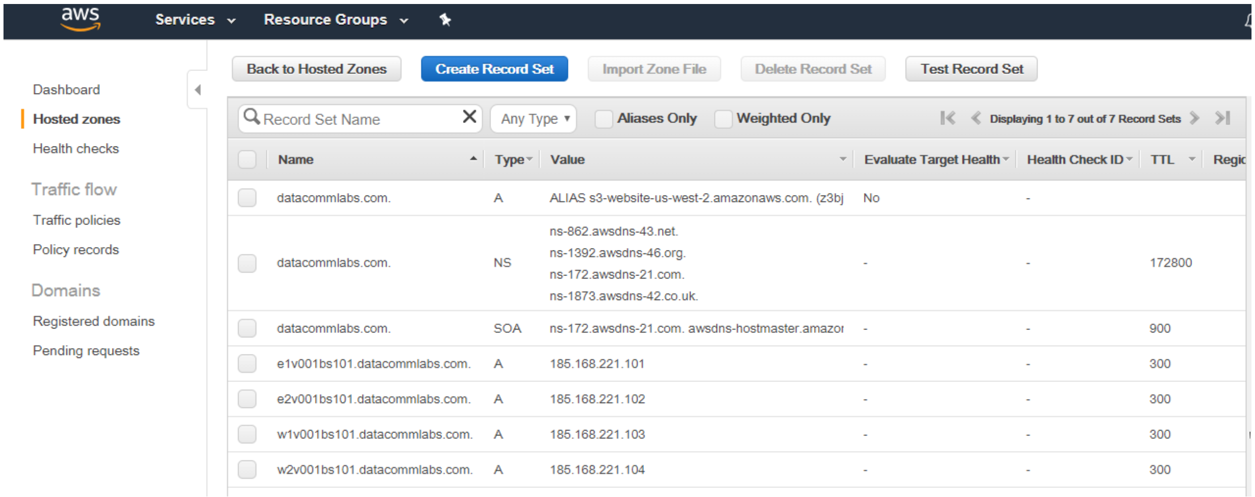
Hosted Zone Details

Domain Name: datacommlabs.com.
Type: Public Hosted Zone
Hosted Zone ID: Z114LX1RARZC5K
Record Set Count: 7
Comment: Public Hosted Zone created by customer
Name Servers *: ns-172.awsdns-21.com
ns-862.awsdns-43.net
ns-1392.awsdns-46.org
ns-1873.awsdns-42.co.uk

*Before the Domain Name System will start to route queries for this domain to Route 53 name servers, you must update the name server records either with the current DNS service or with the registrar for the domain, as applicable. For more information, click the ? icon above.

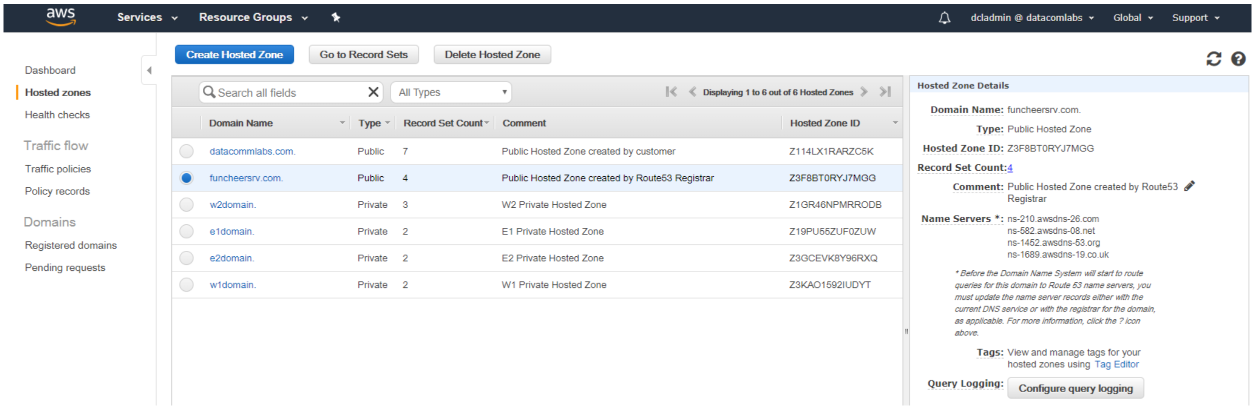
Tags: View and manage tags for your hosted zones using Tag Editor
Query Logging:

Figure 4 – Seven (7) record sets in the customer created Public Hosted Zone



Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Regic
datacommlabs.com.	A	ALIAS s3-website-us-west-2.amazonaws.com. (z3bj	No	-		
datacommlabs.com.	NS	ns-862.awsdns-43.net. ns-1392.awsdns-46.org. ns-172.awsdns-21.com. ns-1873.awsdns-42.co.uk.	-	-	172800	
datacommlabs.com.	SOA	ns-172.awsdns-21.com. awsdns-hostmaster.amazoı	-	-	900	
e1v001bs101.datacommlabs.com.	A	185.168.221.101	-	-	300	
e2v001bs101.datacommlabs.com.	A	185.168.221.102	-	-	300	
w1v001bs101.datacommlabs.com.	A	185.168.221.103	-	-	300	
w2v001bs101.datacommlabs.com.	A	185.168.221.104	-	-	300	

Figure 5 – Public Hosted Zone created by Route 53 at the domain registration with AWS



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
●	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
○	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB
○	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
○	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
○	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT

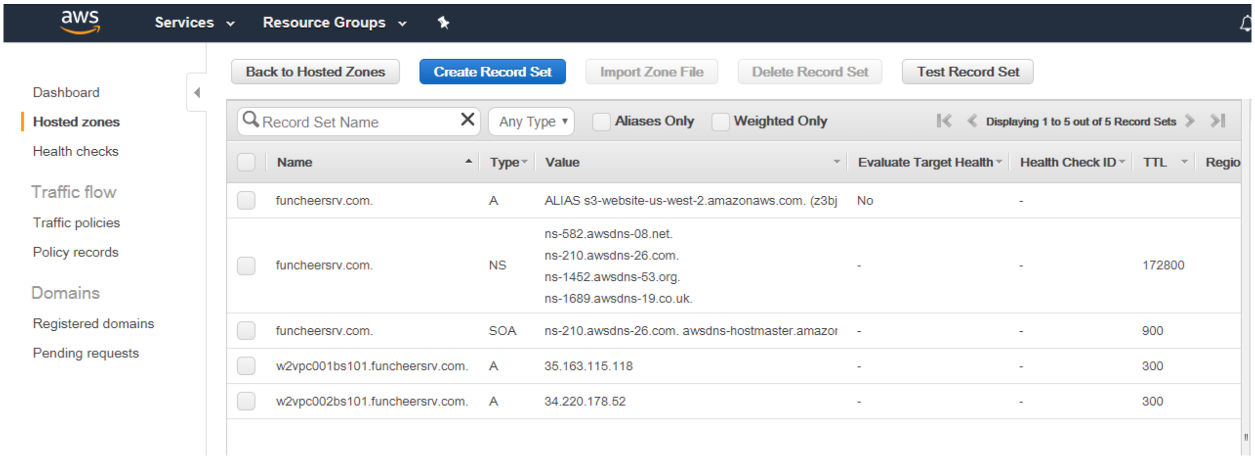
Hosted Zone Details

Domain Name: funcheersrv.com.
Type: Public Hosted Zone
Hosted Zone ID: Z3F8BT0RYJ7MGG
Record Set Count: 4
Comment: Public Hosted Zone created by Route53 Registrar
Name Servers *: ns-210.awsdns-26.com
ns-582.awsdns-08.net
ns-1452.awsdns-53.org
ns-1689.awsdns-19.co.uk

** Before the Domain Name System will start to route queries for this domain to Route 53 name servers, you must update the name server records either with the current DNS service or with the registrar for the domain, as applicable. For more information, click the ? icon above.*

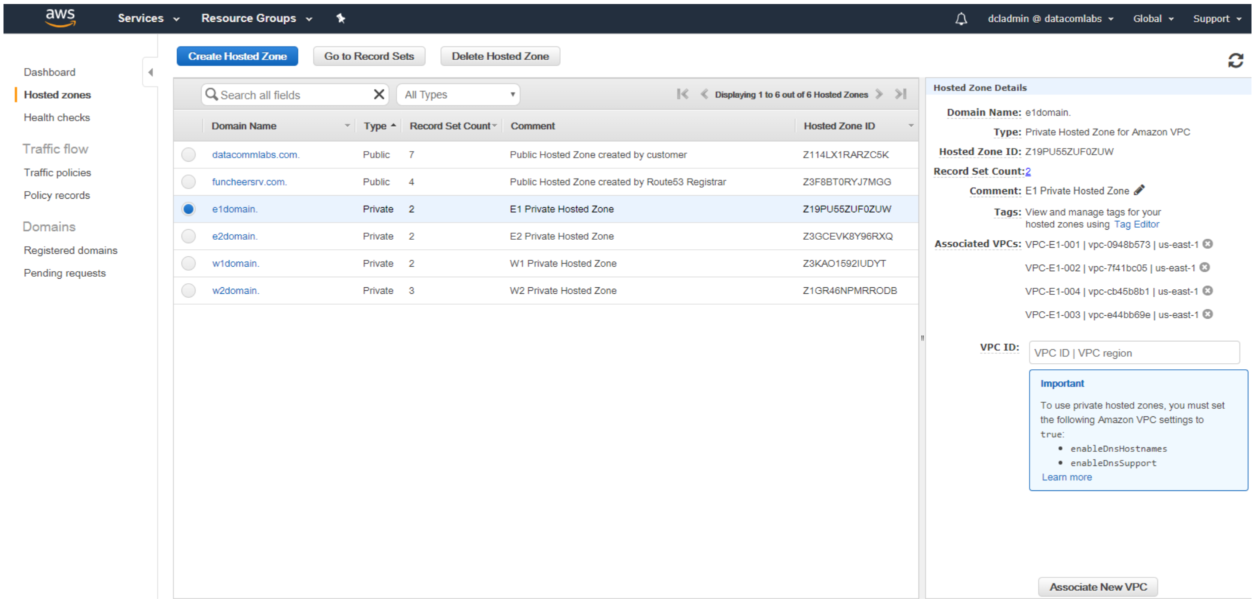
Tags: View and manage tags for your hosted zones using Tag Editor
Query Logging: Configure query logging

Figure 6 – Five (5) record sets in the zone



Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Regio
funcheersrv.com.	A	ALIAS s3-website-us-west-2.amazonaws.com. (z3bj	No	-		
funcheersrv.com.	NS	ns-582.awsdns-08.net. ns-210.awsdns-26.com. ns-1452.awsdns-53.org. ns-1689.awsdns-19.co.uk.	-	-	172800	
funcheersrv.com.	SOA	ns-210.awsdns-26.com. awsdns-hostmaster.amazoı	-	-	900	
w2vpc001bs101.funcheersrv.com.	A	35.163.115.118	-	-	300	
w2vpc002bs101.funcheersrv.com.	A	34.220.178.52	-	-	300	

Figure 7 – Private Hosted Zone for N. Virginia (US East-1) region, with four (4) associated VPCs



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
○	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
●	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
○	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
○	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT
○	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB

Hosted Zone Details

Domain Name: e1domain.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z19PU55ZUF0ZUW
Record Set Count: 2
Comment: E1 Private Hosted Zone
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: VPC-E1-001 | vpc-0948b573 | us-east-1
VPC-E1-002 | vpc-7f41bc05 | us-east-1
VPC-E1-004 | vpc-cb45b8b1 | us-east-1
VPC-E1-003 | vpc-e44bb69e | us-east-1

VPC ID: VPC ID | VPC region

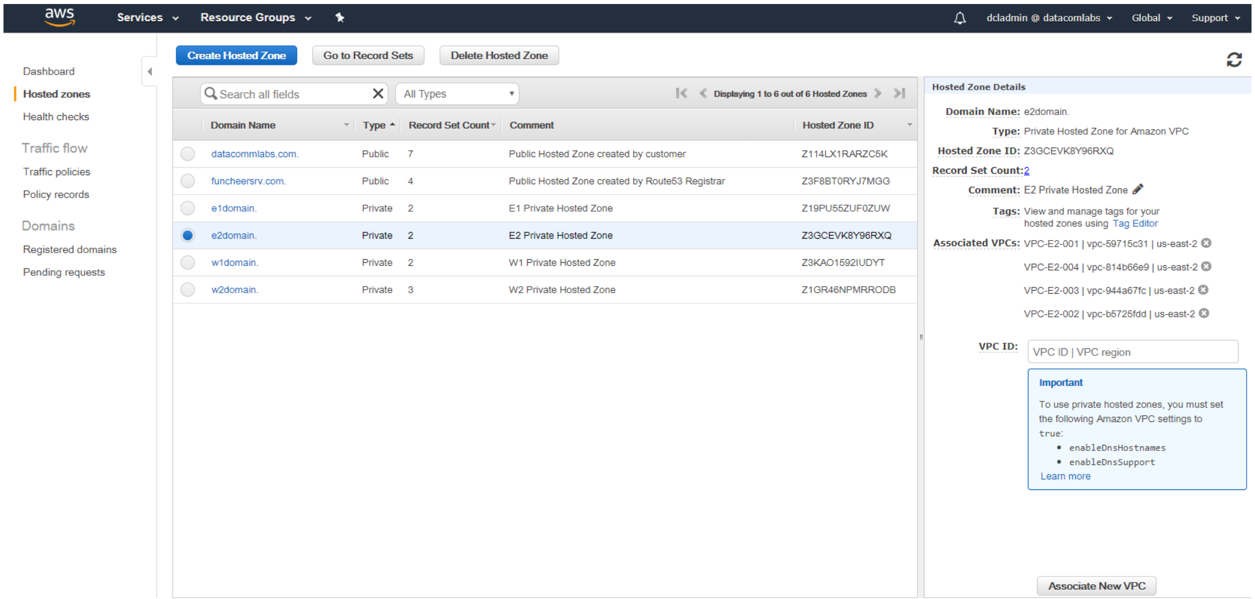
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Learn more

Figure 8 – Private Hosted Zone for Ohio (US East-2) region, with four (4) associated VPCs



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
○	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
○	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
●	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
○	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT
○	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB

Hosted Zone Details

Domain Name: e2domain.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z3GCEVK8Y96RXQ
Record Set Count: 2
Comment: E2 Private Hosted Zone
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: VPC-E2-001 | vpc-59715c31 | us-east-2
VPC-E2-004 | vpc-814b66e9 | us-east-2
VPC-E2-003 | vpc-944a67fc | us-east-2
VPC-E2-002 | vpc-b5725fdd | us-east-2

VPC ID: VPC ID | VPC region

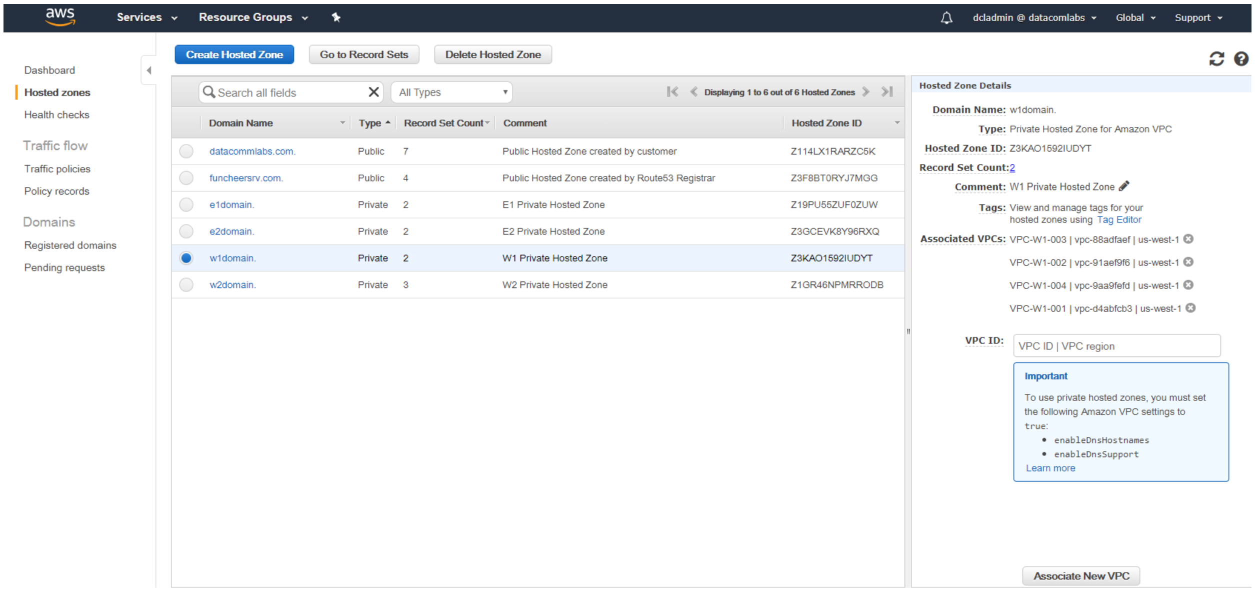
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Learn more

Figure 9 – Private Hosted Zone for N. California (US West-1) region, with four (4) associated VPCs



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
○	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
○	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
○	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
●	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT
○	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB

Hosted Zone Details

Domain Name: w1domain.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z3KAO1592IUDYT
Record Set Count: 2
Comment: W1 Private Hosted Zone
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: VPC-W1-003 | vpc-88adfaef | us-west-1
VPC-W1-002 | vpc-91aef9f6 | us-west-1
VPC-W1-004 | vpc-9aa9fefd | us-west-1
VPC-W1-001 | vpc-d4abfcb3 | us-west-1

VPC ID: VPC ID | VPC region

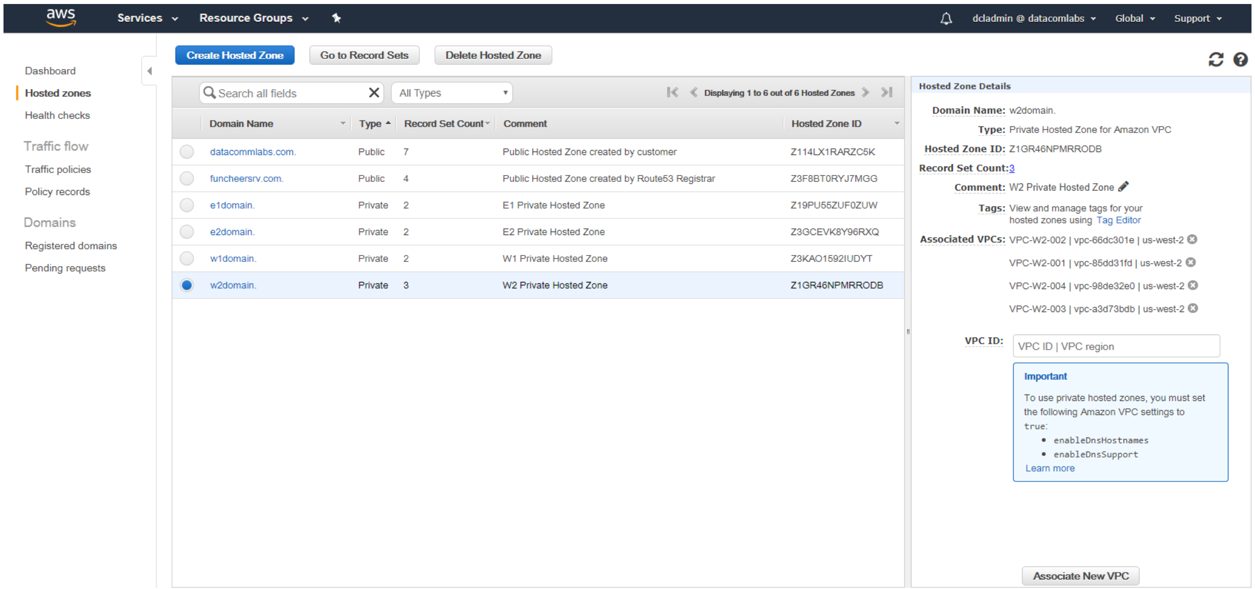
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

Learn more

Figure 10 – Private Hosted Zone for Oregon (US West-2) region, with four (4) associated VPCs



	Domain Name	Type	Record Set Count	Comment	Hosted Zone ID
○	datacommlabs.com.	Public	7	Public Hosted Zone created by customer	Z114LX1RARZC5K
○	funcheersrv.com.	Public	4	Public Hosted Zone created by Route53 Registrar	Z3F8BT0RYJ7MGG
○	e1domain.	Private	2	E1 Private Hosted Zone	Z19PU55ZUF0ZUW
○	e2domain.	Private	2	E2 Private Hosted Zone	Z3GCEVK8Y96RXQ
○	w1domain.	Private	2	W1 Private Hosted Zone	Z3KAO1592IUDYT
●	w2domain.	Private	3	W2 Private Hosted Zone	Z1GR46NPMRRODB

Hosted Zone Details

Domain Name: w2domain.
Type: Private Hosted Zone for Amazon VPC
Hosted Zone ID: Z1GR46NPMRRODB
Record Set Count: 3
Comment: W2 Private Hosted Zone
Tags: View and manage tags for your hosted zones using Tag Editor
Associated VPCs: VPC-W2-002 | vpc-66dc301e | us-west-2
VPC-W2-001 | vpc-85dd31fd | us-west-2
VPC-W2-004 | vpc-98de32e0 | us-west-2
VPC-W2-003 | vpc-a3d73bdb | us-west-2

VPC ID: VPC ID | VPC region

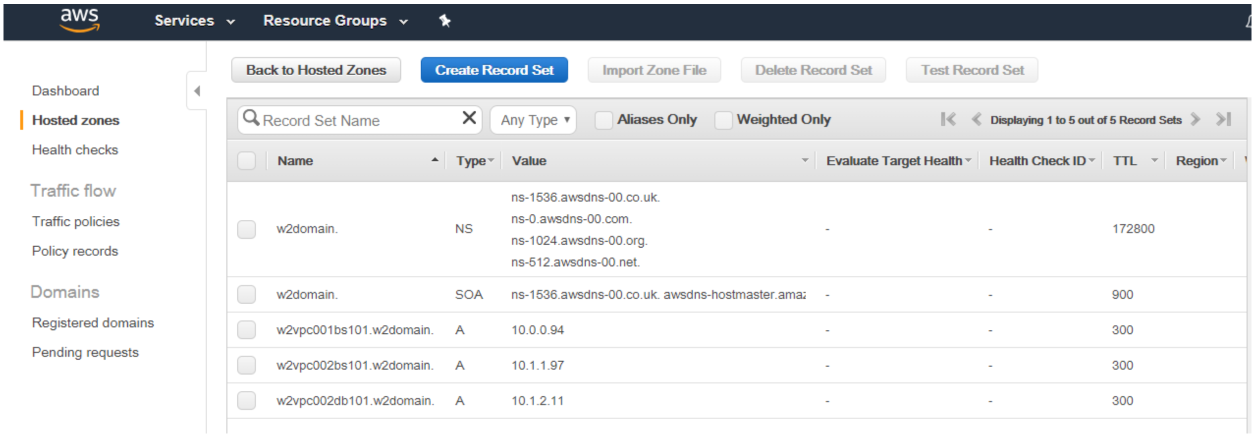
Important

To use private hosted zones, you must set the following Amazon VPC settings to `true`:

- `enableDnsHostnames`
- `enableDnsSupport`

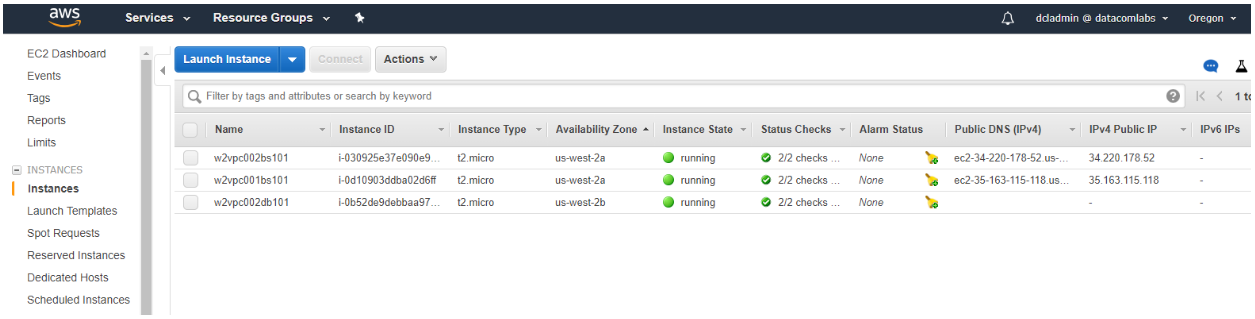
Learn more

Figure 11 – Five (5) record sets in Private Hosted Zone for Oregon (US West-2) region



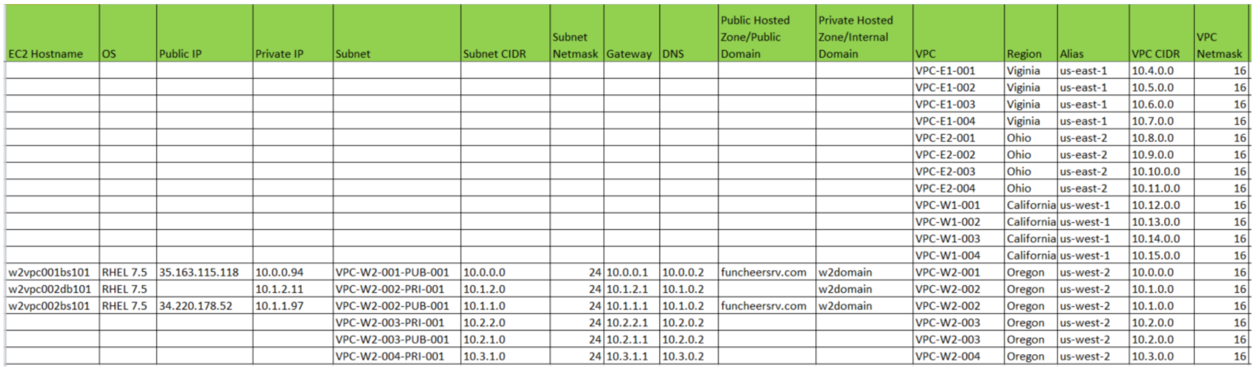
Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region
w2domain.	NS	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.	-	-	172800	
w2domain.	SOA	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.ama;	-	-	900	
w2vpc001bs101.w2domain.	A	10.0.0.94	-	-	300	
w2vpc002bs101.w2domain.	A	10.1.1.97	-	-	300	
w2vpc002db101.w2domain.	A	10.1.2.11	-	-	300	

Figure 12 – Three (3) EC2 instances used to demo Route 53 DNS



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
w2vpc002bs101	i-030925e37e090e9...	t2.micro	us-west-2a	● running	✓ 2/2 checks ...	None	ec2-34-220-178-52.us-...	34.220.178.52	-
w2vpc001bs101	i-0d10903ddba02d6ff	t2.micro	us-west-2a	● running	✓ 2/2 checks ...	None	ec2-35-163-115-118.us...	35.163.115.118	-
w2vpc002db101	i-0b52de9debbaa97...	t2.micro	us-west-2b	● running	✓ 2/2 checks ...	None		-	-

Table 1 – Three (3) EC2 Instances used to demo Route 53



EC2 Hostname	OS	Public IP	Private IP	Subnet	Subnet CIDR	Subnet Netmask	Gateway	DNS	Public Hosted Zone/Public Domain	Private Hosted Zone/Internal Domain	VPC	Region	Alias	VPC CIDR	VPC Netmask
											VPC-E1-001	Viginia	us-east-1	10.4.0.0	16
											VPC-E1-002	Viginia	us-east-1	10.5.0.0	16
											VPC-E1-003	Viginia	us-east-1	10.6.0.0	16
											VPC-E1-004	Viginia	us-east-1	10.7.0.0	16
											VPC-E2-001	Ohio	us-east-2	10.8.0.0	16
											VPC-E2-002	Ohio	us-east-2	10.9.0.0	16
											VPC-E2-003	Ohio	us-east-2	10.10.0.0	16
											VPC-E2-004	Ohio	us-east-2	10.11.0.0	16
											VPC-W1-001	California	us-west-1	10.12.0.0	16
											VPC-W1-002	California	us-west-1	10.13.0.0	16
											VPC-W1-003	California	us-west-1	10.14.0.0	16
											VPC-W1-004	California	us-west-1	10.15.0.0	16
w2vpc001bs101	RHEL 7.5	35.163.115.118	10.0.0.94	VPC-W2-001-PUB-001	10.0.0.0	24	10.0.0.1	10.0.0.2	funcheersrv.com	w2domain	VPC-W2-001	Oregon	us-west-2	10.0.0.0	16
w2vpc002db101	RHEL 7.5		10.1.2.11	VPC-W2-002-PRI-001	10.1.2.0	24	10.1.2.1	10.1.0.2		w2domain	VPC-W2-002	Oregon	us-west-2	10.1.0.0	16
w2vpc002bs101	RHEL 7.5	34.220.178.52	10.1.1.97	VPC-W2-002-PUB-001	10.1.1.0	24	10.1.1.1	10.1.0.2	funcheersrv.com	w2domain	VPC-W2-002	Oregon	us-west-2	10.1.0.0	16
				VPC-W2-003-PRI-001	10.2.2.0	24	10.2.2.1	10.2.0.2			VPC-W2-003	Oregon	us-west-2	10.2.0.0	16
				VPC-W2-003-PUB-001	10.2.1.0	24	10.2.1.1	10.2.0.2			VPC-W2-003	Oregon	us-west-2	10.2.0.0	16
				VPC-W2-004-PRI-001	10.3.1.0	24	10.3.1.1	10.3.0.2			VPC-W2-004	Oregon	us-west-2	10.3.0.0	16

Table 2 - Predicted Route 53 Behavior

1. Public Hosted Zone (Public Domain) datacommlabs.com does not work as it was not registered with AWS nor transferred into AWS
2. Public Hosted Zone (Public Domain) funcheersrv.com works as it was created by AWS Route 53 at AWS domain registration
3. Private Hosted Zone (Internal Domain) w2domain works in VPC-W2-001 (V1) as well as in VPC-W2-002 (V2) because both VPCs are associated with w2domain despite that
    a. V1 and V2 are in two different CIDRs
    b. V1 and V2 have different Route 53 DNS Service IPs

Table 3 - Demonstrated Route 53 Behavior

1. Public Hosted Zone (Public Domain) datacommlabs.com does not work as it was not transferred into AWS

    DNS lookups from Internet failed

```
C:\Users\tshen\Downloads>nslookup datacommlabs.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    datacommlabs.com
Address:  184.168.221.50


C:\Users\tshen\Downloads>nslookup e1v001bs101.datacommlabs.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

*** cdns01.comcast.net can't find e1v001bs101.datacommlabs.com: Non-existent domain

C:\Users\tshen\Downloads>nslookup e2v001bs101.datacommlabs.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

*** cdns01.comcast.net can't find e2v001bs101.datacommlabs.com: Non-existent domain

C:\Users\tshen\Downloads>nslookup w1v001bs101.datacommlabs.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

*** cdns01.comcast.net can't find w1v001bs101.datacommlabs.com: Non-existent domain

C:\Users\tshen\Downloads>nslookup w2v001bs101.datacommlabs.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1
```

```
*** cdns01.comcast.net can't find w2v001bs101.datacommlabs.com: Non-existent domain

C:\Users\tshen\Downloads>
```

2. Public Hosted Zone (Public Domain) funcheersrv.com works as it was created by AWS Route 53 at AWS domain registration

   DNS lookups from Internet succeeded

```
C:\Users\tshen\Downloads>nslookup w2vpc001bs101.funcheersrv.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    w2vpc001bs101.funcheersrv.com
Address:  35.163.115.118


C:\Users\tshen\Downloads>nslookup w2vpc002bs101.funcheersrv.com
Server:  cdns01.comcast.net
Address:  2001:558:feed::1

Non-authoritative answer:
Name:    w2vpc002bs101.funcheersrv.com
Address:  34.220.178.52


C:\Users\tshen\Downloads>
```

3. Private Hosted Zone (Internal Domain) w2domain works in VPC-W2-001 (V1) as well as in VPC-W2-002 (V2) because both VPCs are associated with w2domain despite that
   c. V1 and V2 are two different CIDRs
   d. V1 and V2 have different Route 53 DNS Service IPs

   DNS lookups from w2vpc001bs101 in VCP1, Subnet 1 (Public)

   In DNS lookup output below, lines in blue indicated success; yellow, failure

   Public domain DNS lookups

```
[ec2-user@w2vpc001bs101 ~]$ nslookup datacommlabs.com
Server:        10.0.0.2
Address:       10.0.0.2#53

Non-authoritative answer:
Name:   datacommlabs.com
Address: 184.168.221.33
```

```
[ec2-user@w2vpc001bs101 ~]$ nslookup e1v001bs101.datacommlabs.com
Server:        10.0.0.2
Address:       10.0.0.2#53

** server can't find e1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc001bs101 ~]$ nslookup e2v001bs101.datacommlabs.com
Server:        10.0.0.2
Address:       10.0.0.2#53

** server can't find e2v001bs101.datacommlabs.com: NXDOMAIN


[ec2-user@w2vpc001bs101 ~]$ nslookup w1v001bs101.datacommlabs.com
Server:        10.0.0.2
Address:       10.0.0.2#53

** server can't find w1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc001bs101 ~]$ nslookup w2v001bs101.datacommlabs.com
Server:        10.0.0.2
Address:       10.0.0.2#53

** server can't find w2v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc001bs101 ~]$

[ec2-user@w2vpc001bs101 ~]$ nslookup funcheersrv.com
Server:        10.0.0.2
Address:       10.0.0.2#53

Non-authoritative answer:
Name:   funcheersrv.com
Address: 52.218.240.155

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc001bs101.funcheersrv.com
Server:        10.0.0.2
Address:       10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc001bs101.funcheersrv.com
Address: 35.163.115.118

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc001bs101
Server:        10.0.0.2
```

```
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc001bs101.funcheersrv.com
Address: 35.163.115.118

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc001bs101.w2domain
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc001bs101.w2domain
Address: 10.0.0.94

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc002bs101.w2domain
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc002bs101.w2domain
Address: 10.1.1.97

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc002bs101
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc002bs101.funcheersrv.com
Address: 34.220.178.52

[ec2-user@w2vpc001bs101 ~]$ nslookup w2vpc002db101
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   w2vpc002db101.w2domain
Address: 10.1.2.11
```

DNS resolver configuration on w2vpc001bs101

```
[ec2-user@w2vpc001bs101 ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
search funcheersrv.com w2domain us-west-2.compute.internal
nameserver 10.0.0.2
[ec2-user@w2vpc001bs101 ~]$
```

DNS lookups from w2vpc002bs101 in VCP2, Subnet 1 (Public)

```
[ec2-user@w2vpc002bs101 ~]$ nslookup datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   datacommlabs.com
Address: 184.168.221.60

[ec2-user@w2vpc002bs101 ~]$ nslookup e1v001bs101.datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find e1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002bs101 ~]$ nslookup e2v001bs101.datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find e2v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002bs101 ~]$ nslookup w1v001bs101.datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find w1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002bs101 ~]$ nslookup w2v001bs101.datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find w2v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002bs101 ~]$ nslookup funcheersrv.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   funcheersrv.com
Address: 52.218.144.23

[ec2-user@w2vpc002bs101 ~]$ nslookup w2vpc001bs101.funcheersrv.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
```

```
Name:   w2vpc001bs101.funcheersrv.com
Address: 35.163.115.118

[ec2-user@w2vpc002bs101 ~]$ nslookup w2vpc002bs101.funcheersrv.com
Server:        10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   w2vpc002bs101.funcheersrv.com
Address: 34.220.178.52

[ec2-user@w2vpc002bs101 ~]$ nslookup w2vpc002db101
Server:        10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   w2vpc002db101.w2domain
Address: 10.1.2.11

[ec2-user@w2vpc002bs101 ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search funcheersrv.com w2domain us-west-2.compute.internal
nameserver 10.1.0.2
[ec2-user@w2vpc002bs101 ~]$
```

DNS lookups from w2vpc002db101 in VCP2, Subnet 2 (Private)

```
[ec2-user@w2vpc002db101 ~]$ nslookup datacommlabs.com
Server:        10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   datacommlabs.com
Address: 184.168.221.60

[ec2-user@w2vpc002db101 ~]$ nslookup e1v001bs101.datacommlabs.com
Server:        10.1.0.2
Address:        10.1.0.2#53

** server can't find e1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002db101 ~]$ nslookup e2v001bs101.datacommlabs.com
Server:        10.1.0.2
Address:        10.1.0.2#53

** server can't find e2v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002db101 ~]$ nslookup w1v001bs101.datacommlabs.com
```

```
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find w1v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002db101 ~]$ nslookup w2v001bs101.datacommlabs.com
Server:         10.1.0.2
Address:        10.1.0.2#53

** server can't find w2v001bs101.datacommlabs.com: NXDOMAIN

[ec2-user@w2vpc002db101 ~]$ nslookup funcheersrv.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   funcheersrv.com
Address: 54.231.176.163

[ec2-user@w2vpc002db101 ~]$ nslookup w2vpc001bs101.funcheersrv.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   w2vpc001bs101.funcheersrv.com
Address: 35.163.115.118

[ec2-user@w2vpc002db101 ~]$ nslookup w2vpc002bs101.funcheersrv.com
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   w2vpc002bs101.funcheersrv.com
Address: 34.220.178.52

[ec2-user@w2vpc002db101 ~]$ nslookup w2vpc002db101
Server:         10.1.0.2
Address:        10.1.0.2#53

Non-authoritative answer:
Name:   w2vpc002db101.w2domain
Address: 10.1.2.11

[ec2-user@w2vpc002db101 ~]$ cat /etc/resolv.conf
# Generated by NetworkManager
search funcheersrv.com w2domain us-west-2.compute.internal
nameserver 10.1.0.2
[ec2-user@w2vpc002db101 ~]$
```

Conclusion

1. Demonstrated Route 53 behavior in Table 2 confirmed Predicated Route 53 behavior in Table 1
2. Route 53 provides DNS service for entire customer AWS environment universally
3. Route 53 covers both public and internal domain lookups
4. Route 53 allows internal DNS segmentation and isolation, using multiple Private Hosted Zones so as to achieve added DNS security
5. Universal Route 53 DNS coverage within a customer's AWS environment does not mean universal routing. Routing across VPCs requires VPC Peering, and VPC Peering does not support transitive VPC connectivity. Hence networking between or among VPCs is not easy, plus with significant monetary and performance costs to pay and substantial added management overhead. Best practice, therefore, is to avoid as much as possible running workloads across VPCs, and across AWS VPCs and on premise data centers. The practice, obviously, requires using large and fewer VPCs instead of smaller and more VPCs so as not to have to interconnect VPCs often. VPC was intended to be a cloud, a self-sufficient, self-contained data center. Always treat VPC as a software-defined data center, and not merely a subnet or a VLAN, or one's AWS implementation will go against VPC original design intent and likely lead to undesired issues down the road.