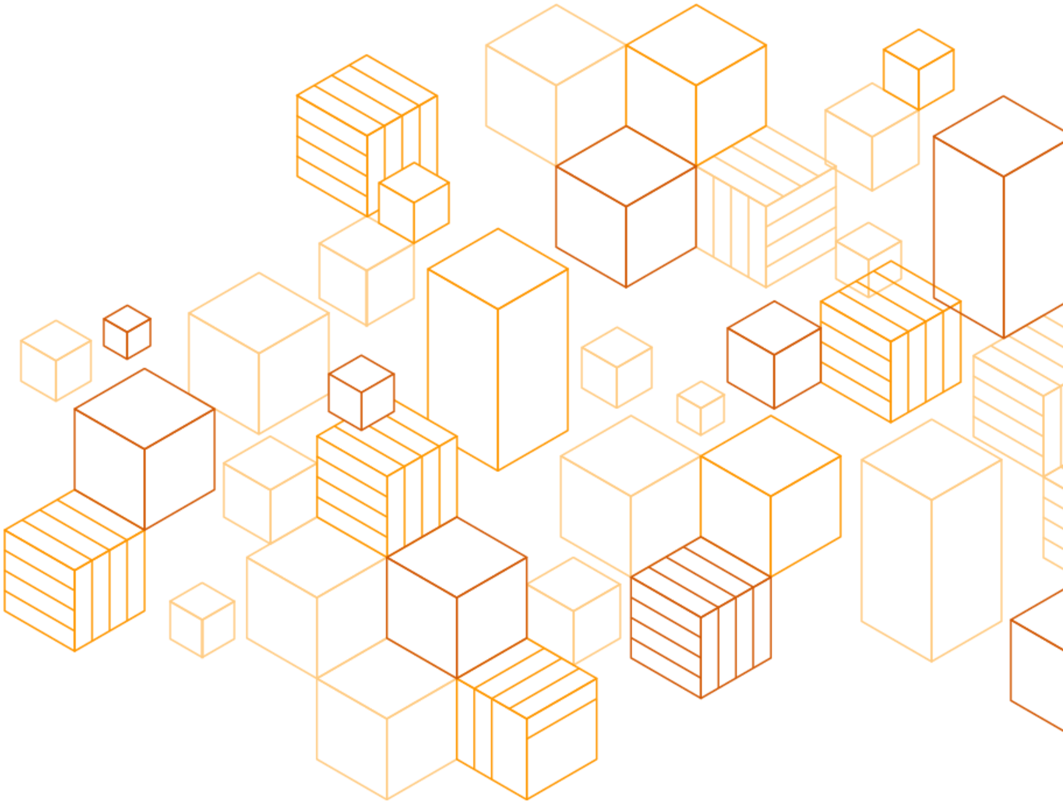
AWS Hybrid DNS with Active Directory

Technical Guide

June 9, 2021



Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

About this guide

The Domain Name System (DNS) is a foundational element of the internet that underpins many services offered by Amazon Web Services (AWS). In 2019, AWS released a whitepaper called *Hybrid Cloud DNS Options for Amazon VPC*, which discusses Amazon Route 53 Resolver for public domain names, Amazon Virtual Private Cloud (Amazon VPC), and Route 53 private hosted zones.

This whitepaper highlights hybrid DNS resolution, including Microsoft Active Directory Domain Services (AD DS), using DNS name resolution services to it make possible for services inside and outside of AWS to resolve namespaces. These solutions and considerations in advanced DNS architectures are meant to help customers who have workloads with unique on-premises resources that require AD DS DNS resolution between on-premises data centers and Amazon Elastic Compute Cloud (Amazon EC2) instances in Amazon VPCs.

Overview

When you review the architecture of AWS environments using Microsoft services, it is extremely important to define the AD site correctly, along with appropriate subnet definitions. This prevents the use of remote domain controllers, which causes greater latency.

Many organizations have both on-premises resources and resources in the cloud. DNS name resolution is essential for on-premises and cloud-based resources. if you have hybrid workloads which include on-premises and cloud-based resources, extra steps are necessary to configure DNS to work seamlessly across both environments. AWS services that require name resolution can include Elastic Load Balancing (ELB), Amazon Relational Database Service (Amazon RDS), Amazon Redshift, and Amazon EC2.

This whitepaper illustrates different architectures that you can implement on AWS using native and custom-built solutions. These architectures meet the need for name resolution of on-premises infrastructure from your Amazon VPC, and address constraints that have been only partially addressed by previously published solutions.

Key concepts

Before getting into the solutions, it is important to establish a few concepts and configuration options that are referenced throughout this whitepaper.

Amazon Route 53 Resolver endpoints and conditional forwarding rules

Route 53 provides several DNS features, including public DNS domain registration, the ability to create private DNS zones, hybrid DNS tools, and DNS name resolution. With DNS name resolution, Route 53 Resolver can perform recursive searches on public and local name servers.

The Resolver endpoint feature allows DNS queries originating in the on-premises and AD DS environment to resolve domains hosted on AWS. For on-premises environments, connectivity must be established between the local DNS infrastructure and AWS through AWS Direct Connect or a Virtual Private Network (VPN). Endpoints are configured by assigning an IP address to each subnet for which you want to provide a resolver.

For outbound DNS queries to work, they must be triggered using conditional forwarding rules. Domains hosted on your local DNS infrastructure can be configured as routing rules in Route 53 Resolver. The rules are triggered when a query is made in one of these domains, and they attempt to forward DNS requests to the DNS servers configured along with the rules. With this functionality, you have a set of features that allow two-way consultation between the on-premises environment or AD DS and AWS through private connections. See Amazon Route 53 Resolver for Hybrid Clouds.

Active Directory Domain Services (AD DS)

You can store information about objects in the environment, making that information easy for administrators and users to find and use. AD DS uses DNS name resolution services to enable customers to locate domain controllers, and enable the domain controllers that host the directory service to communicate with each other. When you create a new server and make a "domain join", the fully qualified domain name (FQDN) created in DNS is already integrated with AD.

Private hosted zone

A 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.

Elastic network interfaces (ENIs)

Elastic network interfaces (referred to as network interfaces in the Amazon EC2 console) are virtual network interfaces that you can attach to an instance in a VPC. They’re available only for instances running in a VPC. A virtual network interface, such as any network adapter, is the interface that a device uses to connect to a network. Each instance in a VPC, depending on the instance type, can have multiple network interfaces attached to it.

Amazon VPC DHCP options set

The Dynamic Host Configuration Protocol (DHCP) provides a standard for passing configuration information to hosts on a TCP / IP network. The **Options** field of a DHCP message contains configuration parameters such as `domain-name-servers`, `domainname`, `ntp-servers`, and `netbios-node-type`. In any Amazon VPC, you can create DHCP options sets and specify up to four DNS servers. Currently, these options sets are created and applied per VPC, which means that you can’t have a DNS server list at the Availability Zone level. For more information about DHCP options sets and configuration, see Overview of DHCP option sets in the Amazon VPC User Guide.

AWS Resource Access Manager (AWS RAM)

AWS Resource Access Manager (AWS RAM) is a service that enables you to easily and securely share AWS resources with any AWS account, or within AWS Organizations. You can share AWS Transit Gateways, subnets, AWS License Manager configurations, and Amazon Route 53 Resolver rules resources with Aws RAM. Many organizations use multiple accounts to create administrative or billing isolation, and to limit the impact of errors. AWS RAM eliminates the need to create duplicate resources in multiple accounts, reducing the operational overhead of managing those resources in every single account you own.

Constraints

Packet per second (PPS) per elastic network interface limit

Each network interface in an Amazon VPC has a hard limit of 1024 packets that it can send to the Amazon-provided DNS server every second. Therefore, a computing resource on AWS that has a network interface attached to it, and is sending traffic to the Amazon DNS resolver (for example, an Amazon EC2 instance or AWS Lambda function), falls under this hard-limit restriction. In this whitepaper, this limit is referred to as packet per second (PPS) per network interface.

When you’re designing a scalable solution for name resolution you must consider this limit, because failure to do so can result in queries to Route 53 Resolver going unanswered if the limit is reached. This limit is a key factor considered for the solutions proposed in this whitepaper. The limit is higher for Route 53 Resolver endpoints, which have a limit of approximately 10,000 queries per second (QPS) per elastic network interface.

Connection tracking

The number of simultaneous stateful connections that an Amazon EC2 security group can support by default is an extremely large value. The majority of standard TCP-based customers never encounter any issues with this. In rare cases, customers with restrictive security group policies and applications that create a large number of concurrent connections (for example, a self-managed recursive DNS server) may run into issues where they exhaust all simultaneous connection tracking resources. When that limit is exceeded, subsequent connections fail silently. In such cases, AWS recommends that you have a security group set up that you can use to disable connection tracking. To do this, set up permissive rules on both inbound and outbound connections.

Solutions

The solutions in this whitepaper present options and best practices to architect AWS hybrid name resolution with Active Directory domain services, considering criteria such as ease of implementation, management overhead, cost, resilience, and the distribution of DNS queries. With the increased use of Microsoft services in the AWS Cloud, AWS customers are integrating these services to better accommodate the name resolution architecture in the AWS Cloud in hybrid scenarios.

Most of these customers already have a local DNS infrastructure. When resources on AWS are created, AWS provides DNS services powered by Amazon Route 53 as a managed service.

This whitepaper covers the following solutions:

- **Amazon Route 53 outbound endpoint integration** — This solution allows Route 53 to resolve and forward DNS queries to DNS domains hosted outside of Route 53.
- **Amazon Route 53 inbound endpoint integration** — This solution allows AD DS DNS to consult Route 53 Resolver for DNS zones hosted on Route 53.
- **Multi-accounts with private hosted zones** — This solution addresses the scenario of organizations that have grown enough to have multi-account environments and create private hosted zones to have more name resolution controls in the AWS environment.

Amazon Route 53 outbound endpoint integration

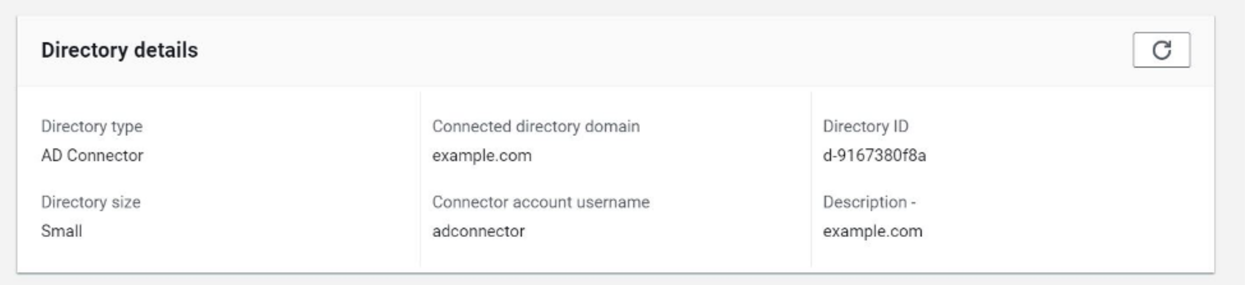
If you have Managed AD or AD Connector, when you create an instance of Windows EC2, it can automatically join Active Directory. This is called a seamless domain join. When you choose this setting, AWS defines the DNS settings on the network interface within the EC2 instance to the IP addresses of the DNS servers provided by the

Managed AD or AD Connector. Consequently, the instances are associated with the AD domain.

If you start an EC2 Linux or Windows instance and do not use the seamless domain join feature, the DNS settings for the instance will be provided by the DHCP settings of the VPC (`dhcp` option set).

By default, DHCP settings provide the Route 53 network address, “+2”; that is, if the subnet is `10.0.1.0/24`, the Route 53 endpoint will be at `10.0.1.2`. In this solution, the creation of a hybrid DNS infrastructure enables you to integrate local DNS infrastructures with Amazon Route 53 DNS.

In the on-premises environment (or Active Directory running in EC2), you have the “example.com” directory created. In AD Connector, you can list its Active Directory Server IP address (`10.0.0.166`).



Directory details

Directory type
AD Connector

Directory size
Small

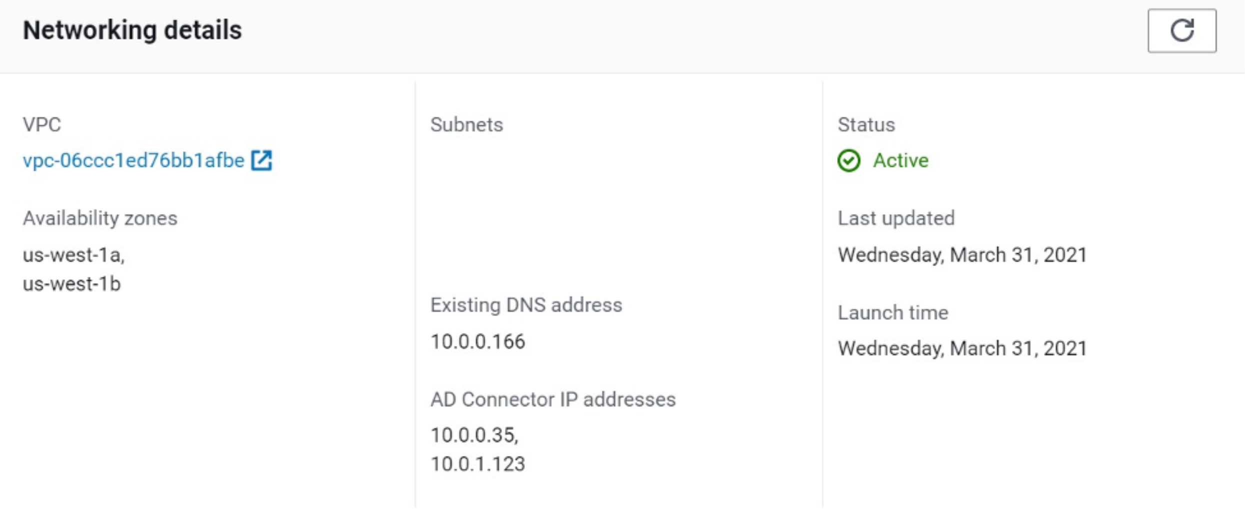
Connected directory domain
example.com

Connector account username
adconnector

Directory ID
d-9167380f8a

Description -
example.com

Directory details including the example.com directory



Networking details

VPC
vpc-06ccc1ed76bb1afbe

Availability zones
us-west-1a,
us-west-1b

Subnets

Existing DNS address
10.0.0.166

AD Connector IP addresses
10.0.0.35,
10.0.1.123

Status
Active

Last updated
Wednesday, March 31, 2021

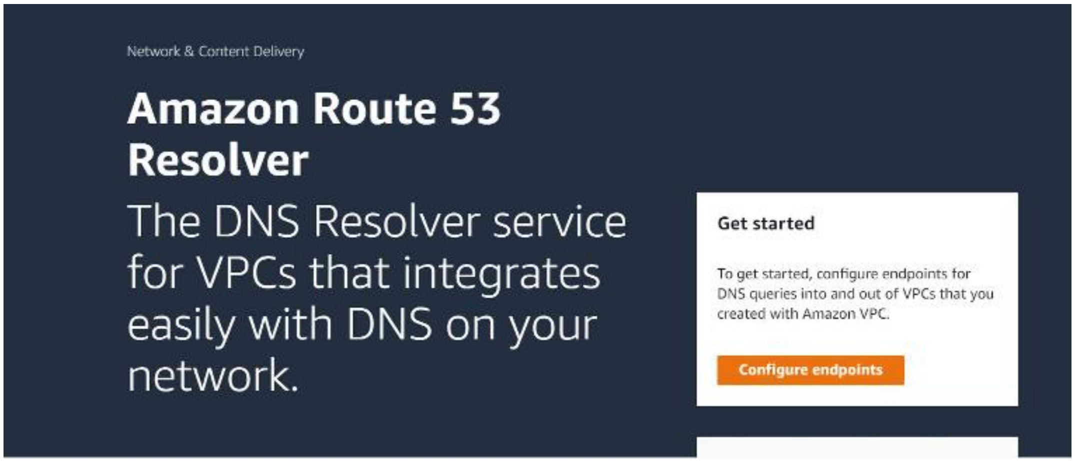
Launch time
Wednesday, March 31, 2021

Networking details

Although the inbound and outbound endpoints can be created in a single step, to facilitate the examples given in this whitepaper, it is demonstrated it in two separate steps. The first step for the solution is to create the Route 53 outbound endpoint, which allows Route 53 to resolve and forward DNS queries to DNS domains hosted outside of Route 53. When you create this outbound endpoint, AWS creates an elastic network interface (ENI) in the Availability Zones (AZ) that you specify.

To create the Route 53 outbound endpoint:

1. From the Route 53 console, choose **Resolver** > **Outbound Endpoint** and then **Configure endpoints**.



Network & Content Delivery

Amazon Route 53 Resolver

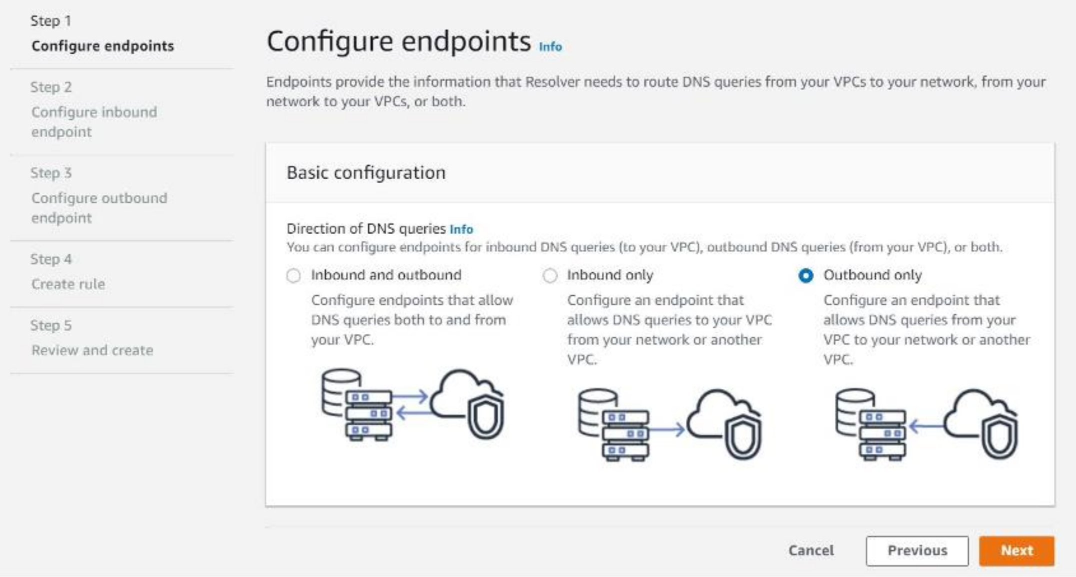
The DNS Resolver service for VPCs that integrates easily with DNS on your network.

Get started

To get started, configure endpoints for DNS queries into and out of VPCs that you created with Amazon VPC.

*Choose **Configure endpoints***

2. In the endpoint configuration, chose **Outbound only** to configure an endpoint that allows DNS queries from the VPC to the Active Directory DNS network.



Configure endpoints Info

Endpoints provide the information that Resolver needs to route DNS queries from your VPCs to your network, from your network to your VPCs, or both.

Basic configuration

Direction of DNS queries Info

You can configure endpoints for inbound DNS queries (to your VPC), outbound DNS queries (from your VPC), or both.

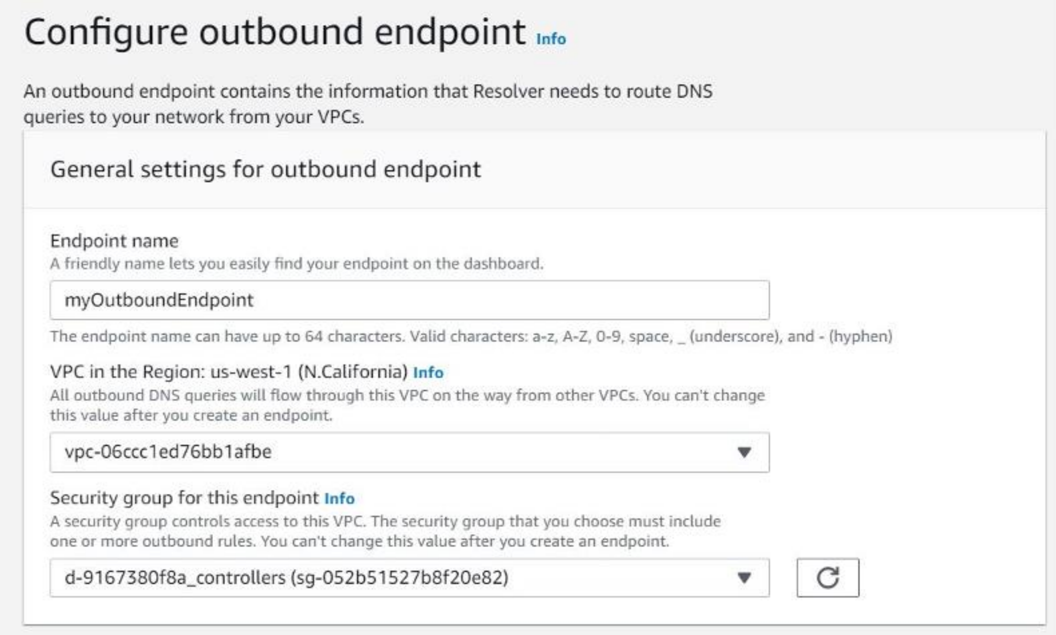
○ Inbound and outbound
Configure endpoints that allow DNS queries both to and from your VPC.

○ Inbound only
Configure an endpoint that allows DNS queries to your VPC from your network or another VPC.

● Outbound only
Configure an endpoint that allows DNS queries from your VPC to your network or another VPC.

*Choose **Outbound only***

3. Enter name for the endpoint and pick the VPC which will have the outbound DNS queries flow.
4. Select a security group that must have access “to-for” the fleet of Active Directory Domain Controllers.



Configure outbound endpoint Info

An outbound endpoint contains the information that Resolver needs to route DNS queries to your network from your VPCs.

General settings for outbound endpoint

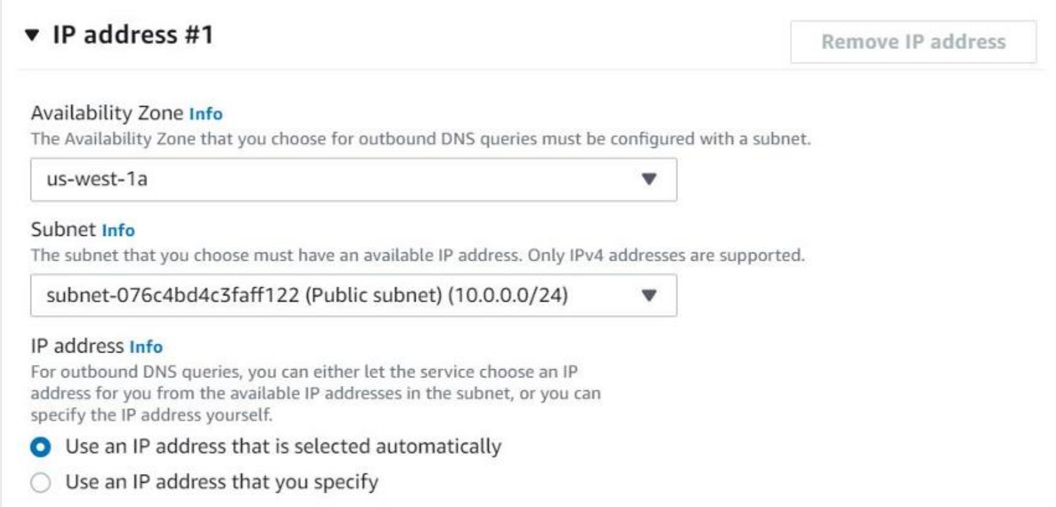
Endpoint name
A friendly name lets you easily find your endpoint on the dashboard.
myOutboundEndpoint
The endpoint name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

VPC in the Region: us-west-1 (N.California) Info
All outbound DNS queries will flow through this VPC on the way from other VPCs. You can't change this value after you create an endpoint.
vpc-06ccc1ed76bb1afbe ▼

Security group for this endpoint Info
A security group controls access to this VPC. The security group that you choose must include one or more outbound rules. You can't change this value after you create an endpoint.
d-9167380f8a_controllers (sg-052b51527b8f20e82) ▼

Enter the endpoint name and select a security group

5. Add two IP addresses in different Availability Zones to improve high availability.



▼ IP address #1

Availability Zone Info
The Availability Zone that you choose for outbound DNS queries must be configured with a subnet.
us-west-1a ▼

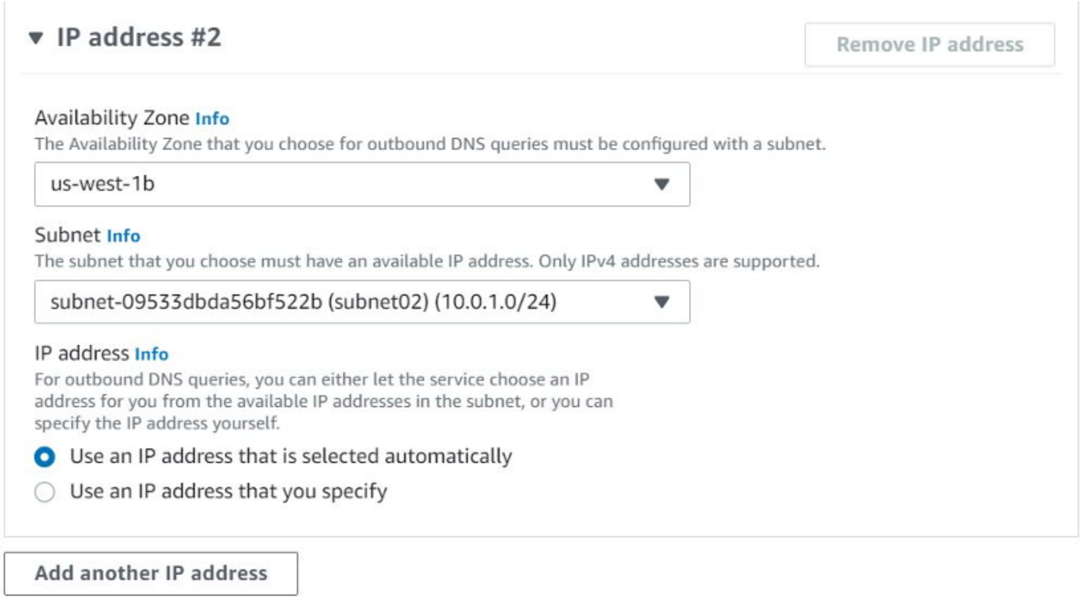
Subnet Info
The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.
subnet-076c4bd4c3faff122 (Public subnet) (10.0.0.0/24) ▼

IP address Info
For outbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

● Use an IP address that is selected automatically

○ Use an IP address that you specify

Add the first IP address and AZ



▼ IP address #2

Availability Zone Info
The Availability Zone that you choose for outbound DNS queries must be configured with a subnet.
us-west-1b

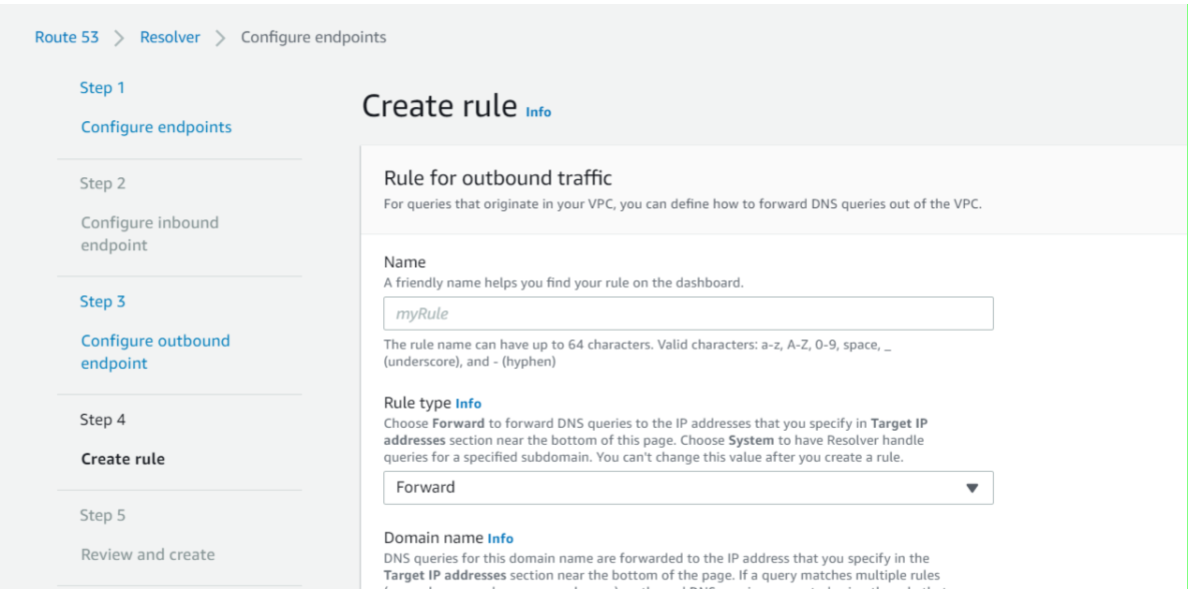
Subnet Info
The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.
subnet-09533dbda56bf522b (subnet02) (10.0.1.0/24)

IP address Info
For outbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

● Use an IP address that is selected automatically
○ Use an IP address that you specify

Add the second IP address and AZ

The setup automatically redirects you to the **Create rule** wizard.


Route 53 > Resolver > Configure endpoints
Step 1
Configure endpoints
Step 2
Configure inbound endpoint
Step 3
Configure outbound endpoint
Step 4
Create rule
Step 5
Review and create

Create rule Info

Rule for outbound traffic
For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

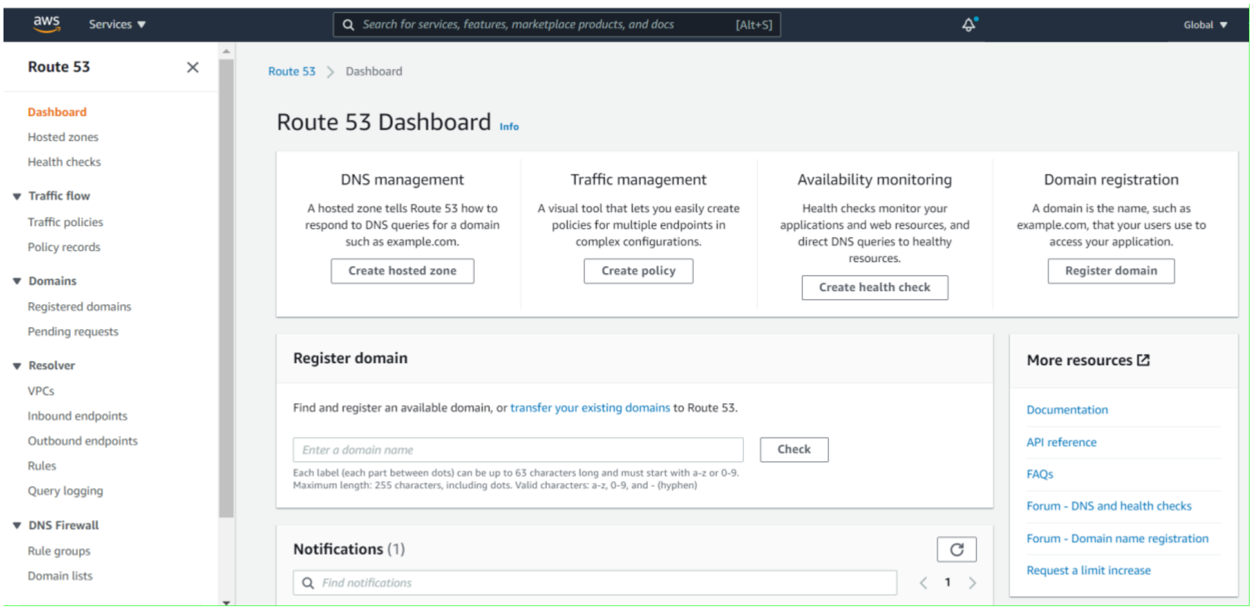
Name
A friendly name helps you find your rule on the dashboard.
myRule
The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

Rule type Info
Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.
Forward

Domain name Info
DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules

Create the rule

6. If you are adding rules manually and not in the **Configure endpoints** option of the **Create rule** wizard, from the Route 53 console, choose **Resolver** > **Rules**.



aws Services ▼ Search for services, features, marketplace products, and docs [Alt+S] Global ▼

Route 53 ×

Dashboard
Hosted zones
Health checks
▼ Traffic flow
Traffic policies
Policy records
▼ Domains
Registered domains
Pending requests
▼ Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
▼ DNS Firewall
Rule groups
Domain lists

Route 53 > Dashboard

Route 53 Dashboard Info

DNS management
A hosted zone tells Route 53 how to respond to DNS queries for a domain such as example.com.
Create hosted zone

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

Availability monitoring
Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.
Create health check

Domain registration
A domain is the name, such as example.com, that your users use to access your application.
Register domain

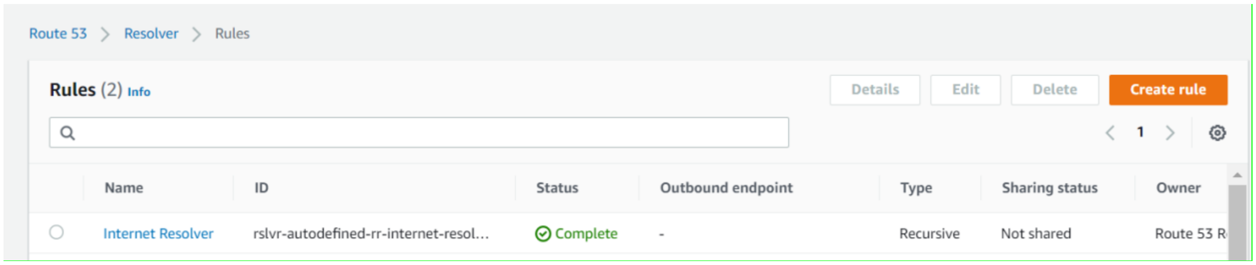
Register domain
Find and register an available domain, or transfer your existing domains to Route 53.
Enter a domain name — Check
Each label (each part between dots) can be up to 63 characters long and must start with a-z or 0-9. Maximum length: 255 characters, including dots. Valid characters: a-z, 0-9, and - (hyphen)

Notifications (1)
Find notifications < 1 >

More resources
Documentation
API reference
FAQs
Forum - DNS and health checks
Forum - Domain name registration
Request a limit increase

*Choose **Rules***

7. In the Route 53 Dashboard > Resolver > Rules, Choose **Create rule**.



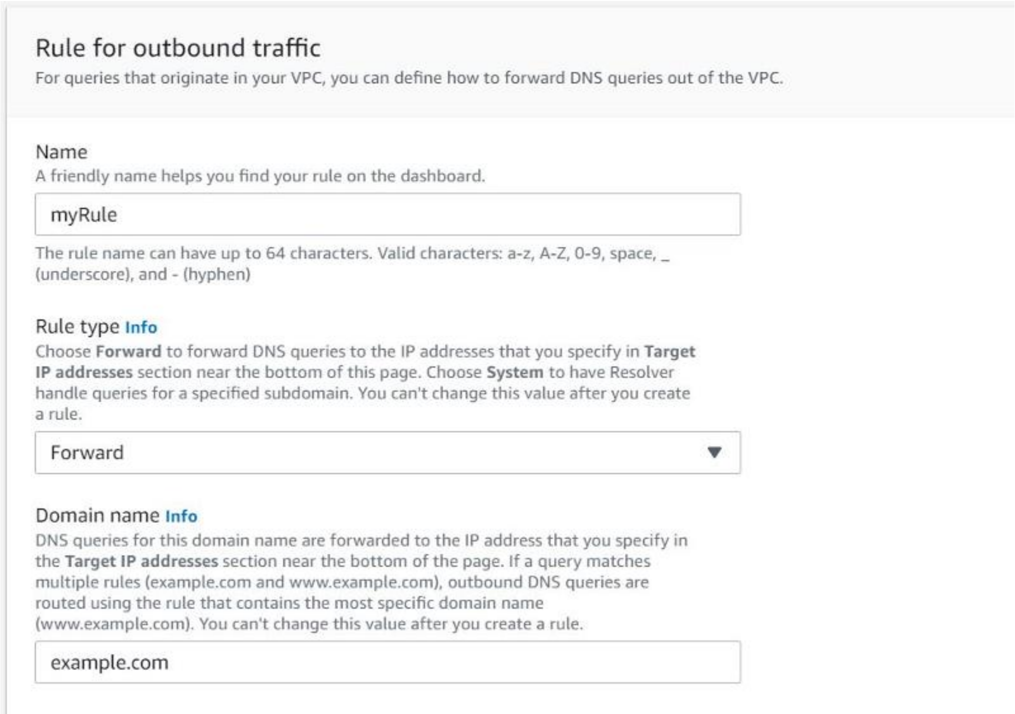
Route 53 > Resolver > Rules

Rules (2) Info — Details | Edit | Delete | Create rule

	Name	ID	Status	Outbound endpoint	Type	Sharing status	Owner
○	Internet Resolver	rslvr-autodefined-rr-internet-resol...	✓ Complete	-	Recursive	Not shared	Route 53 R

These rules allow two actions: *Forward* or *System*. The **Forward** action causes Route 53 Resolver to forward DNS queries for specific DNS domains to external DNS resolvers (Active Directory). With **System Rule**, Route 53 queries the hierarchy for name resolution (Private DNS zones, DNS VPC and Public DNS).

8. Enter a name for the rule.
9. Under **Rule type**, choose **Forward**.
10. Enter the name of the local domain (`example.com`). DNS queries for that domain name are forwarded to the Active Directory IP addresses specified in the **Target IP addresses** section near the bottom of the page.



Rule for outbound traffic

For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

Name

A friendly name helps you find your rule on the dashboard.

myRule

The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

Rule type Info

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

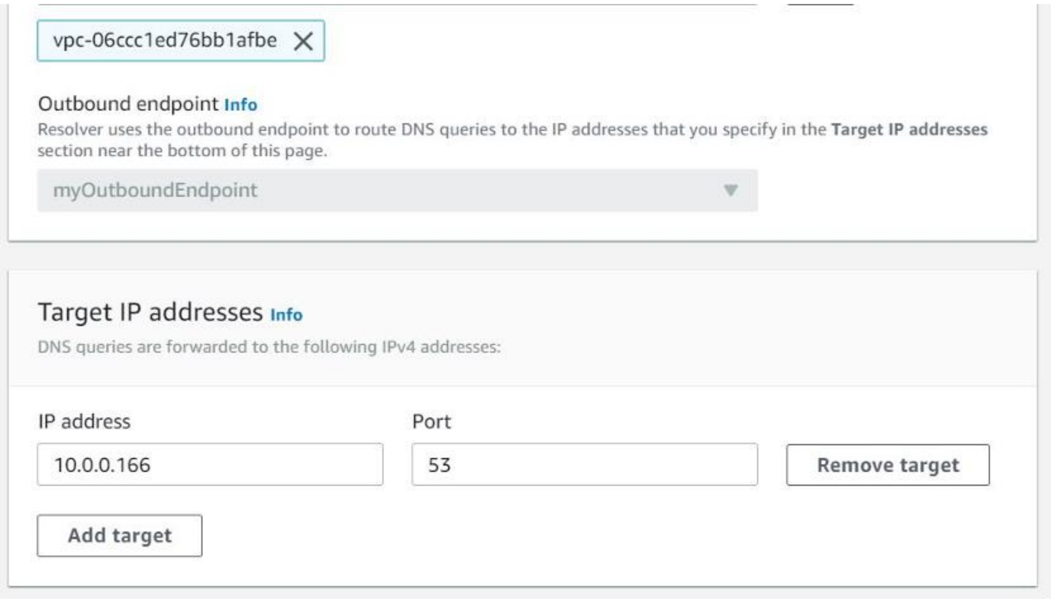
Forward ▼

Domain name Info

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

example.com

Enter the rule name, select the rule type (Forward) and select the domain name (example.com)



vpc-06ccc1ed76bb1afbe ✕

Outbound endpoint Info

Resolver uses the outbound endpoint to route DNS queries to the IP addresses that you specify in the **Target IP addresses** section near the bottom of this page.

myOutboundEndpoint ▼

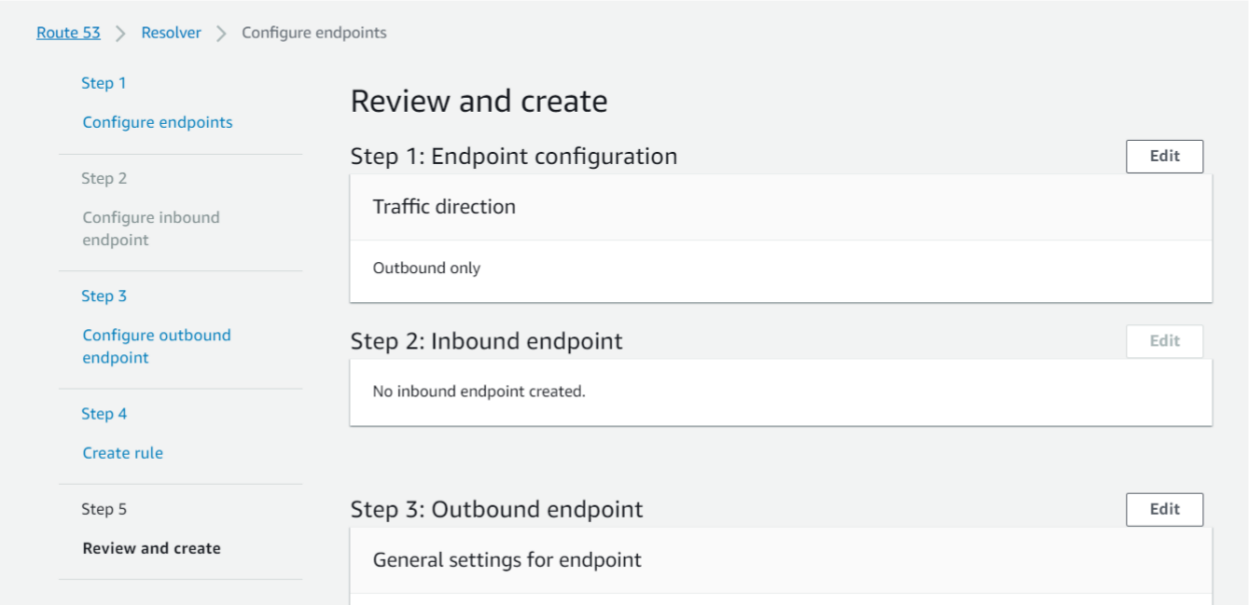
Target IP addresses Info

DNS queries are forwarded to the following IPv4 addresses:

IP address	Port	
10.0.0.166	53	Remove target

Setting DNS queries to `example.com` *forwarding rule to IP Address* `10.0.0.166`.

11. Choose **Next**.
12. Review the options.


Route 53 > Resolver > Configure endpoints
Step 1
Configure endpoints
Step 2
Configure inbound endpoint
Step 3
Configure outbound endpoint
Step 4
Create rule
Step 5
Review and create
Edit
Edit
Edit

Review and create

Step 1: Endpoint configuration

Traffic direction

Outbound only

Step 2: Inbound endpoint

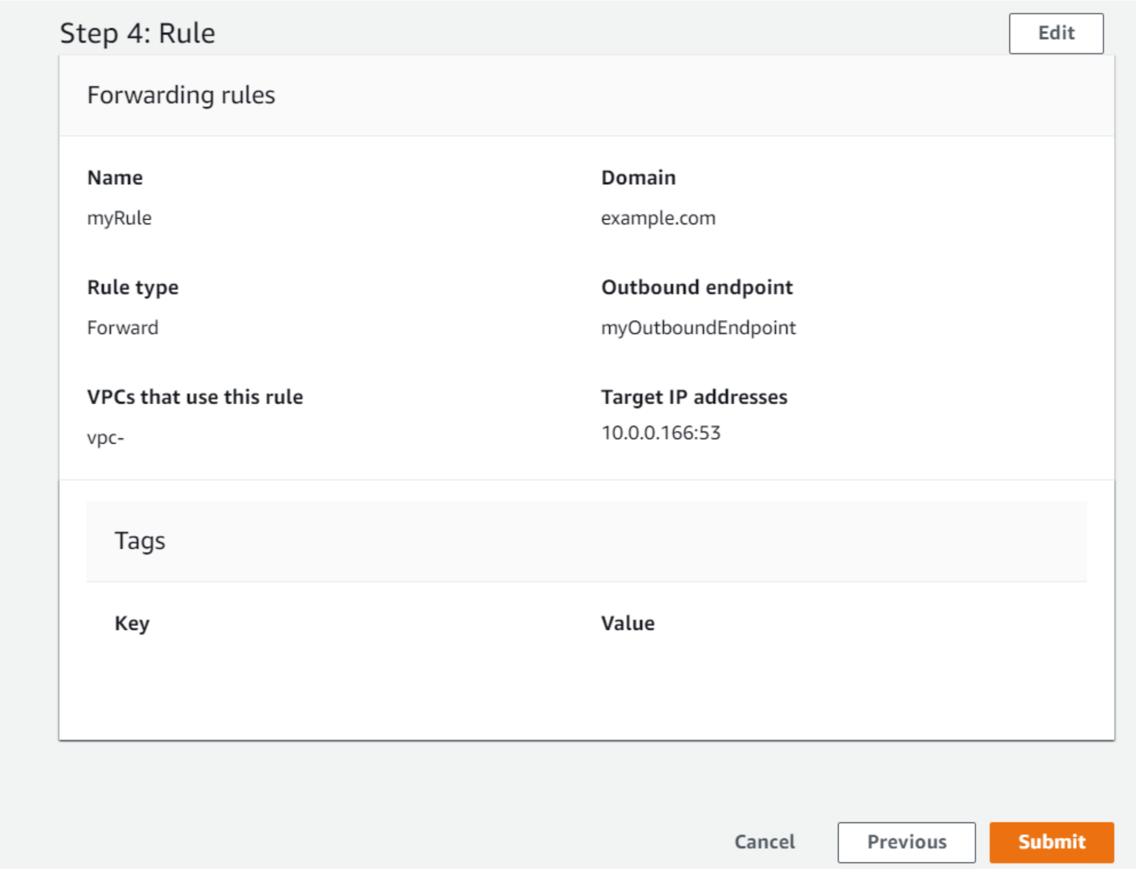
No inbound endpoint created.

Step 3: Outbound endpoint

General settings for endpoint

Review the endpoint options

13. Choose **Submit** to create the outbound endpoint and the outbound endpoint will be created.



Step 4: Rule

Forwarding rules

Name: myRule

Domain: example.com

Rule type: Forward

Outbound endpoint: myOutboundEndpoint

VPCs that use this rule: vpc-

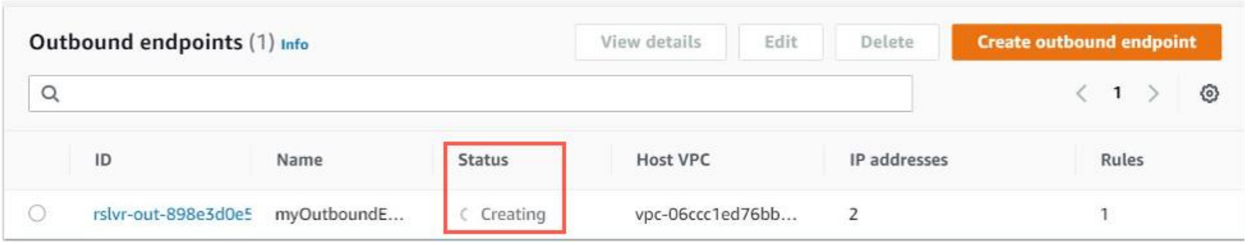
Target IP addresses: 10.0.0.166:53

Tags

Key	Value

Choose **Submit**.

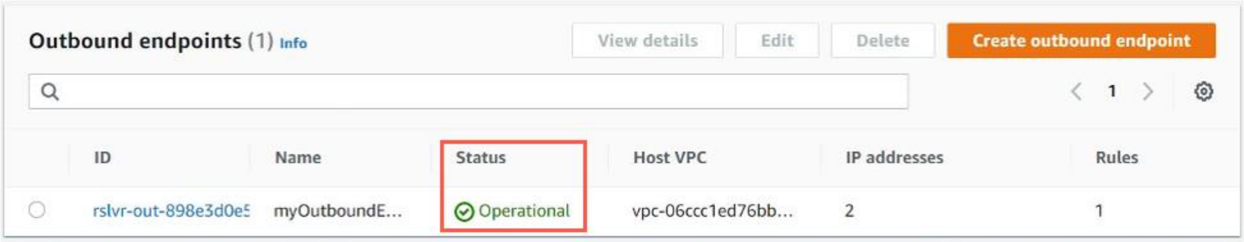
The endpoint is now being created. Watch the **Status** field. When you see "Operational," the endpoint is created.



Outbound endpoints (1) Info

	ID	Name	Status	Host VPC	IP addresses	Rules
○	rslvr-out-898e3d0e5	myOutboundE...	Creating	vpc-06ccc1ed76bb...	2	1

The outbound endpoint has the status of "Creating"

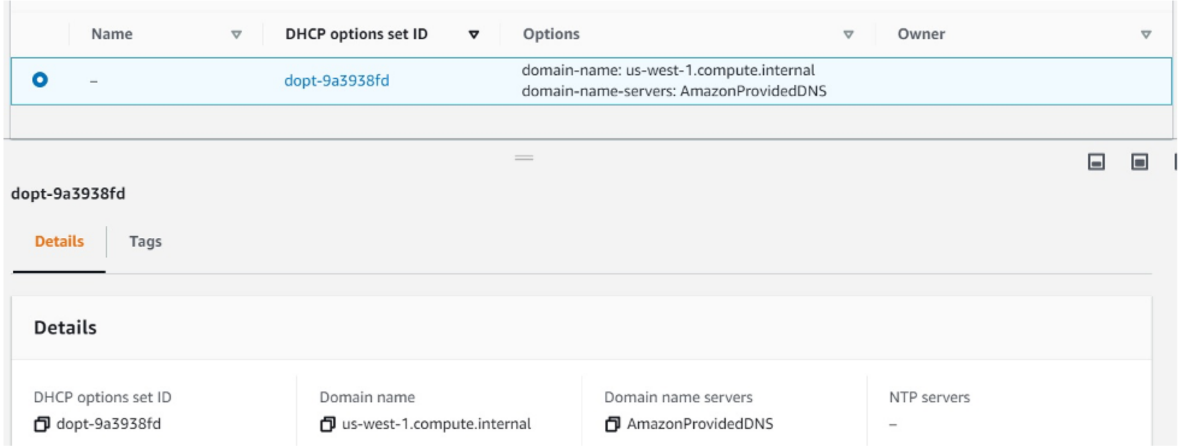


Outbound endpoints (1) Info

	ID	Name	Status	Host VPC	IP addresses	Rules
○	rslvr-out-898e3d0e5	myOutboundE...	✓ Operational	vpc-06ccc1ed76bb...	2	1

The outbound endpoint is operational.

14. Test the configurations by accessing an instance that is not domain joined, but has the standard DHCP option set.



	Name	DHCP options set ID	Options	Owner
●	–	dopt-9a3938fd	domain-name: us-west-1.compute.internal domain-name-servers: AmazonProvidedDNS	

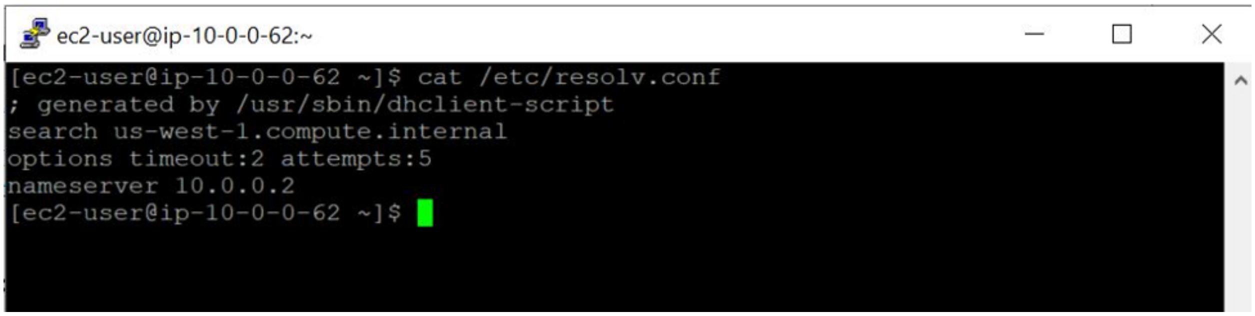
dopt-9a3938fd

Details

DHCP options set ID	Domain name	Domain name servers	NTP servers
dopt-9a3938fd	us-west-1.compute.internal	AmazonProvidedDNS	–

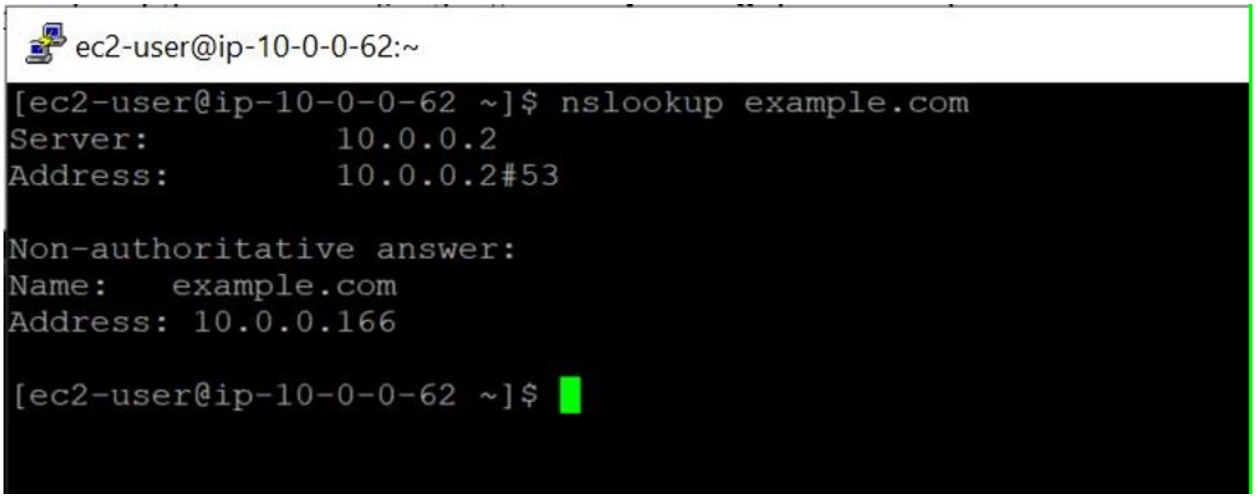
DHCP options set for the selected VPC, with the standard configuration.

15. In this instance, confirm the DNS settings.
16. Run a query for the `example.com` domain.



```
[ec2-user@ip-10-0-0-62 ~]$ cat /etc/resolv.conf
; generated by /usr/sbin/dhclient-script
search us-west-1.compute.internal
options timeout:2 attempts:5
nameserver 10.0.0.2
[ec2-user@ip-10-0-0-62 ~]$
```

Confirm that EC2 is using the default .2 Resolver DNS from the DHCP Option Set



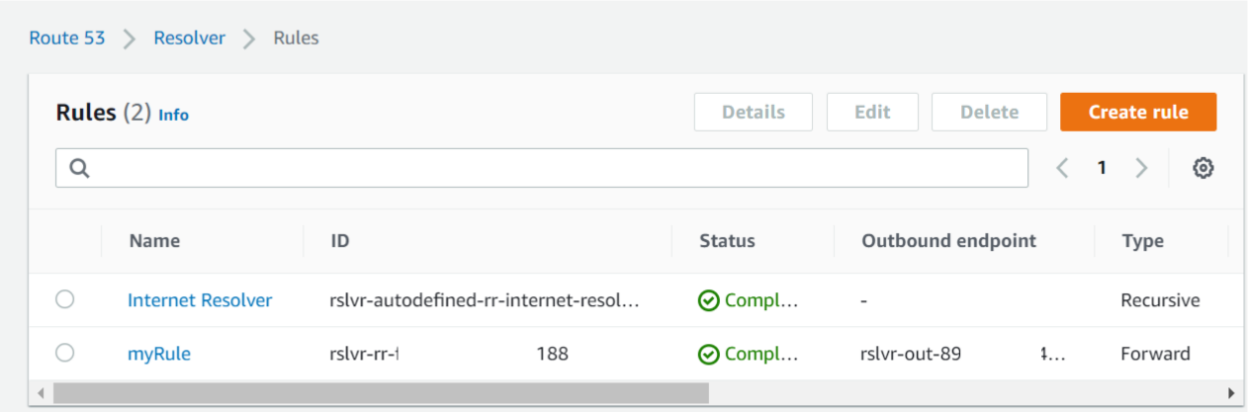
```
[ec2-user@ip-10-0-0-62 ~]$ nslookup example.com
Server:         10.0.0.2
Address:        10.0.0.2#53

Non-authoritative answer:
Name:   example.com
Address: 10.0.0.166

[ec2-user@ip-10-0-0-62 ~]$
```

Successfully query for “example.com”

Reverse DNS (Optional)

In some scenarios, Reverse DNS is needed to not only resolve the hostname of a server, but also resolve the IP address of a host and obtain the associated fully qualified domain name (FQDN). In Route 53, this can be achieved using rules for the special domain “*.in-addr.arpa*”.

1. In the Route 53 Dashboard > Resolver > Rules, Choose **Create rule**.



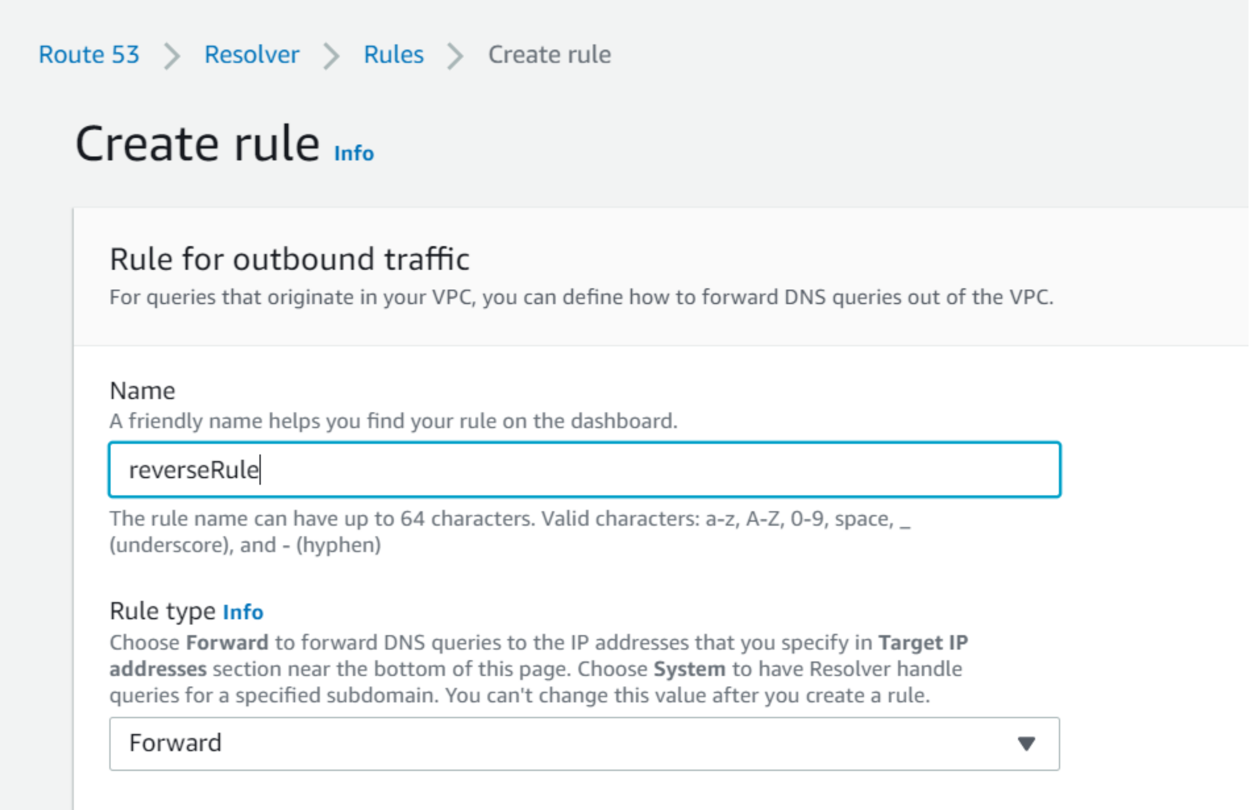
Route 53 > Resolver > Rules

Rules (2) Info

	Name	ID	Status	Outbound endpoint	Type
○	Internet Resolver	rslvr-autodefined-rr-internet-resol...	✓ Compl...	-	Recursive
○	myRule	rslvr-rr- 188	✓ Compl...	rslvr-out-89 1...	Forward

Creating a new rule.

2. Enter a name for the rule. Under **Rule type**, choose **Forward**.



Route 53 > Resolver > Rules > Create rule

Create rule Info

Rule for outbound traffic

For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

Name

A friendly name helps you find your rule on the dashboard.

reverseRule

The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

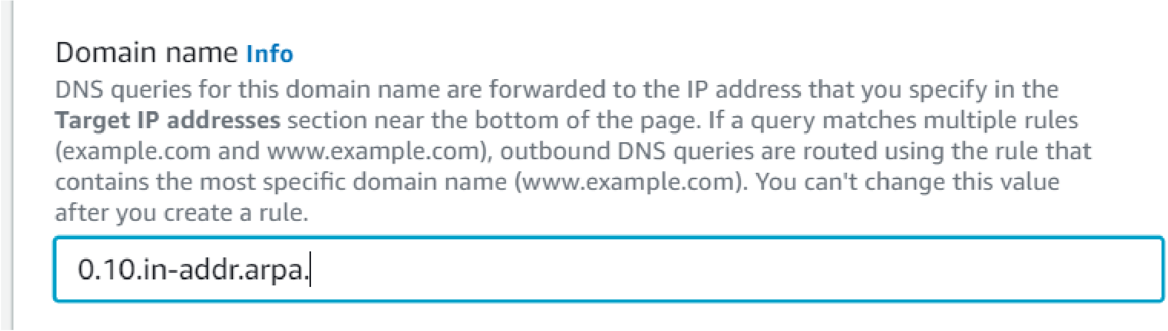
Rule type Info

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

Forward ▼

Creating a new forwarding rule.

3. For the domain name, specify the net address in reverse with .in-addr.arpa as suffix. For example: 0.10.in-addr.arpa.



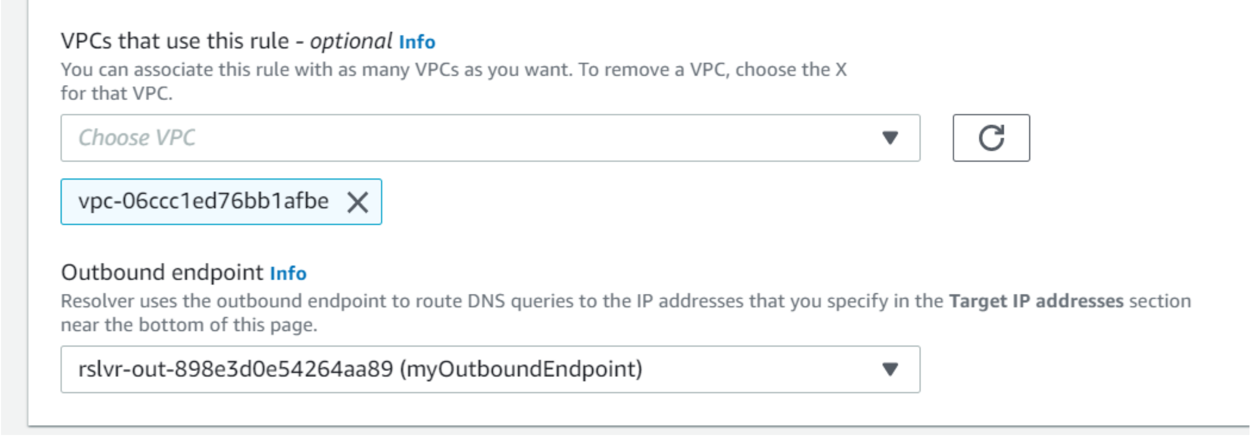
Domain name Info

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

0.10.in-addr.arpa.

Specifying the net address in reverse.

4. Associate the rule with the VPC and select the **Outbound endpoint** created in the previous steps.



VPCs that use this rule - *optional* Info

You can associate this rule with as many VPCs as you want. To remove a VPC, choose the X for that VPC.

Choose VPC

vpc-06ccc1ed76bb1afbe

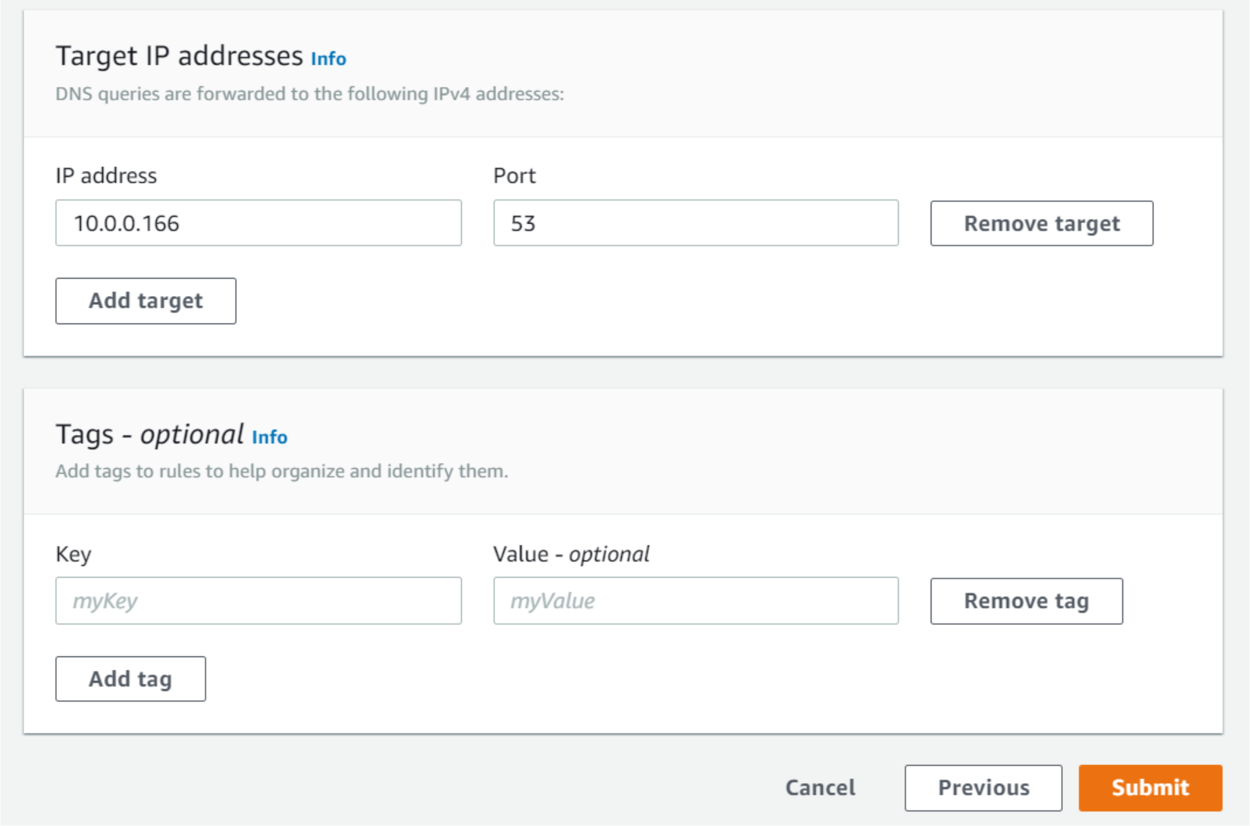
Outbound endpoint Info

Resolver uses the outbound endpoint to route DNS queries to the IP addresses that you specify in the **Target IP addresses** section near the bottom of this page.

rslvr-out-898e3d0e54264aa89 (myOutboundEndpoint)

Using the previously created Outbound Endpoint.

5. Specify the target IP addresses for this rule and click **Submit**. This will forward requests to the Active Directory containing the PTR records of the hosts.



Target IP addresses Info

DNS queries are forwarded to the following IPv4 addresses:

IP address: 10.0.0.166

Port: 53

Tags - *optional* Info

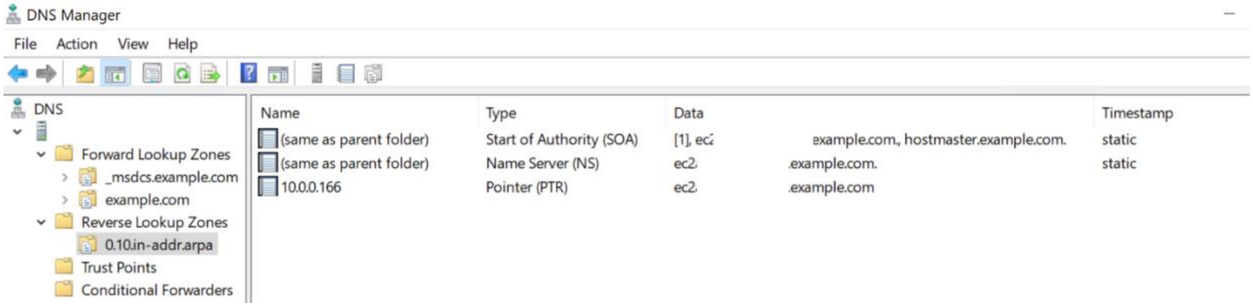
Add tags to rules to help organize and identify them.

Key: *myKey*

Value - *optional*: *myValue*

Setting DNS queries to `10.0.0.166` *forwarding rule to IP Address* `10.0.0.166`

6. In Active Directory DNS Manager, we confirm that the Reverse Lookup Zone has the Pointer (PTR) for the hosts which need Reverse DNS lookup.

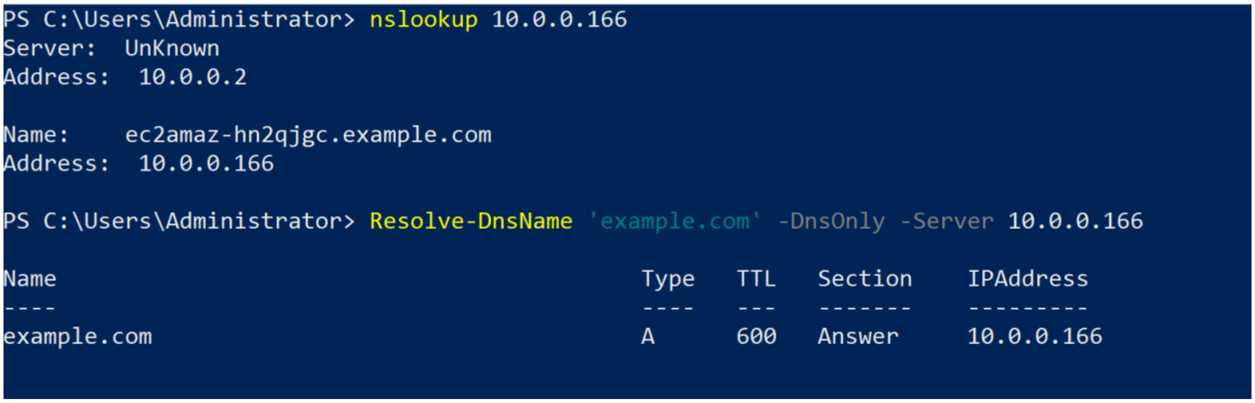


DNS Manager

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[1], ec example.com., hostmaster.example.com.	static
(same as parent folder)	Name Server (NS)	ec2. .example.com.	static
10.0.0.166	Pointer (PTR)	ec2. .example.com	

Reverse Lookup Zone "0.10.in-addr.arpa" with a PTR for 10.0.0.166.

7. Test Reverse DNS lookup, from EC2.



```
PS C:\Users\Administrator> nslookup 10.0.0.166
Server:  UnKnown
Address:  10.0.0.2

Name:    ec2amaz-hn2qjgc.example.com
Address:  10.0.0.166

PS C:\Users\Administrator> Resolve-DnsName 'example.com' -DnsOnly -Server 10.0.0.166

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
example.com                                    A      600   Answer     10.0.0.166
```

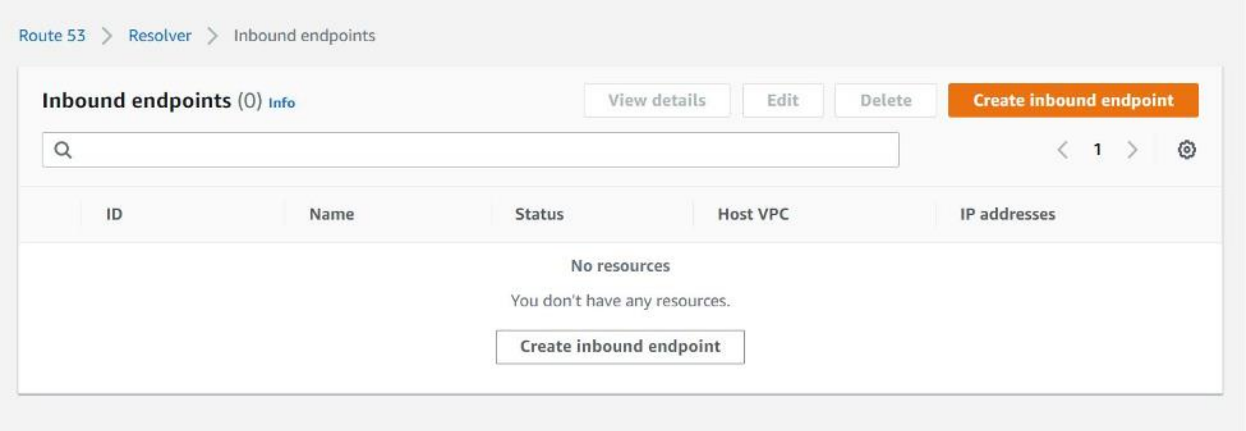
Testing the Reverse DNS Lookup with nslookup and Resolve-DnsName.

Amazon Route 53 inbound endpoint integration

To allow the local DNS infrastructure (AD DS DNS) to consult Route 53 Resolver for DNS zones hosted on Route 53, you must create inbound endpoints. Inbound endpoints allow other services to query Route 53 for DNS resolution. When you create inbound endpoints, AWS creates an elastic network interface (ENI) in each specified AZ to receive incoming DNS queries.

To create an inbound endpoint:

1. From the Route 53 console, choose **Inbound Endpoint** > **Create Inbound Endpoint**.



Route 53 > Resolver > Inbound endpoints
Inbound endpoints (0) Info
View details
Edit
Delete
Create inbound endpoint
1

ID	Name	Status	Host VPC	IP addresses

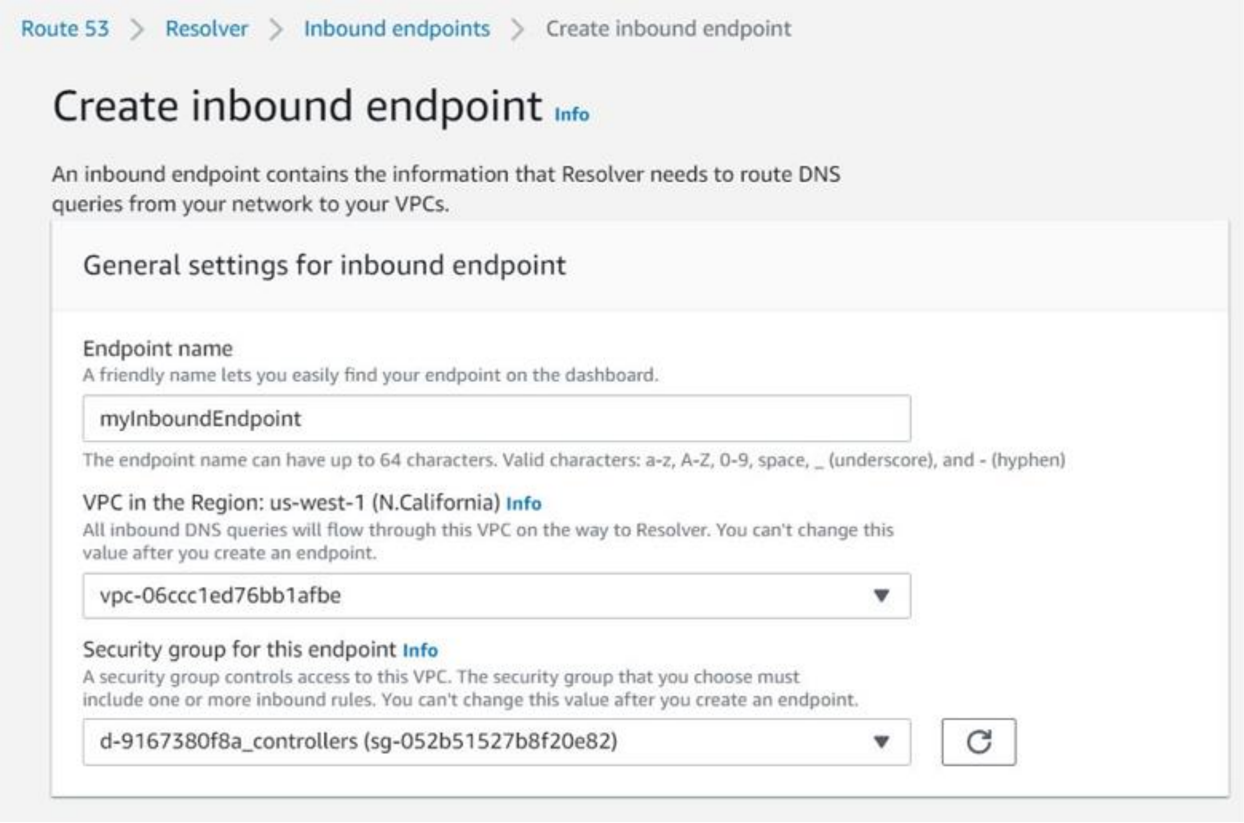
No resources

You don't have any resources.

*Select **Create inbound endpoint***

2. Enter a name for the endpoint.
3. Choose the VPC which will receive inbound DNS queries.

4. Select a security group that must have access “to-for” the fleet of Active Directory Domain Controllers.



Route 53 > Resolver > Inbound endpoints > Create inbound endpoint

Create inbound endpoint Info

An inbound endpoint contains the information that Resolver needs to route DNS queries from your network to your VPCs.

General settings for inbound endpoint

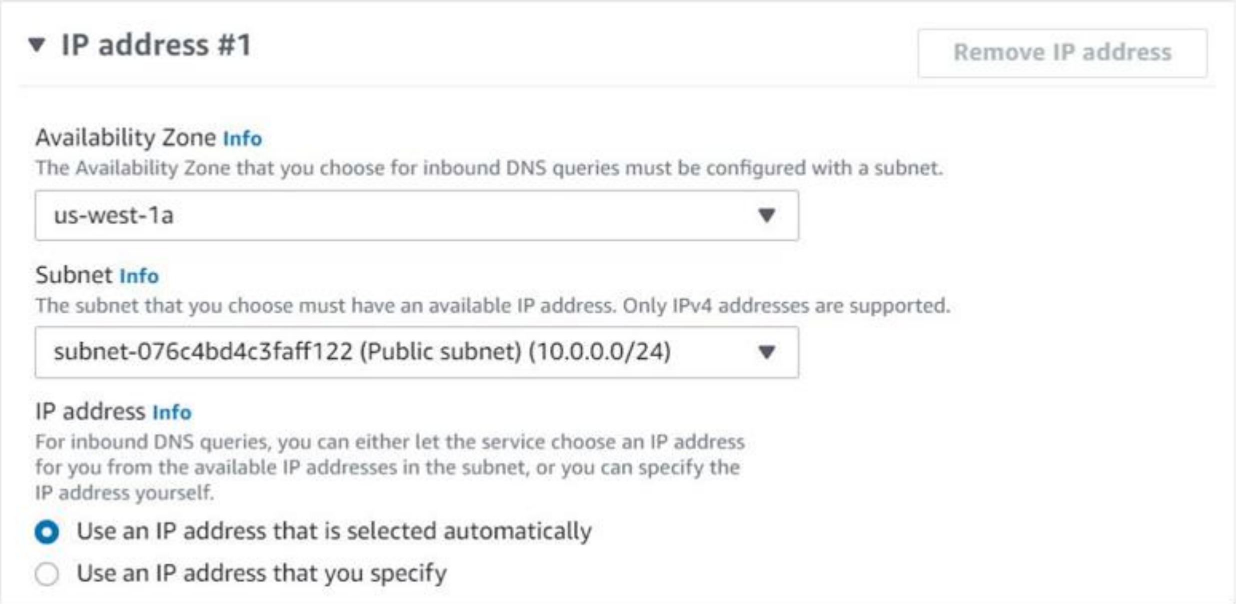
Endpoint name
A friendly name lets you easily find your endpoint on the dashboard.
myInboundEndpoint
The endpoint name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

VPC in the Region: us-west-1 (N.California) Info
All inbound DNS queries will flow through this VPC on the way to Resolver. You can't change this value after you create an endpoint.
vpc-06ccc1ed76bb1afbe ▼

Security group for this endpoint Info
A security group controls access to this VPC. The security group that you choose must include one or more inbound rules. You can't change this value after you create an endpoint.
d-9167380f8a_controllers (sg-052b51527b8f20e82) ▼

Enter endpoint name, choose a VPC, then choose a security group

5. Add two IP addresses in different Availability Zones to improve high availability.



Availability Zone Info
The Availability Zone that you choose for inbound DNS queries must be configured with a subnet.
us-west-1a ▼

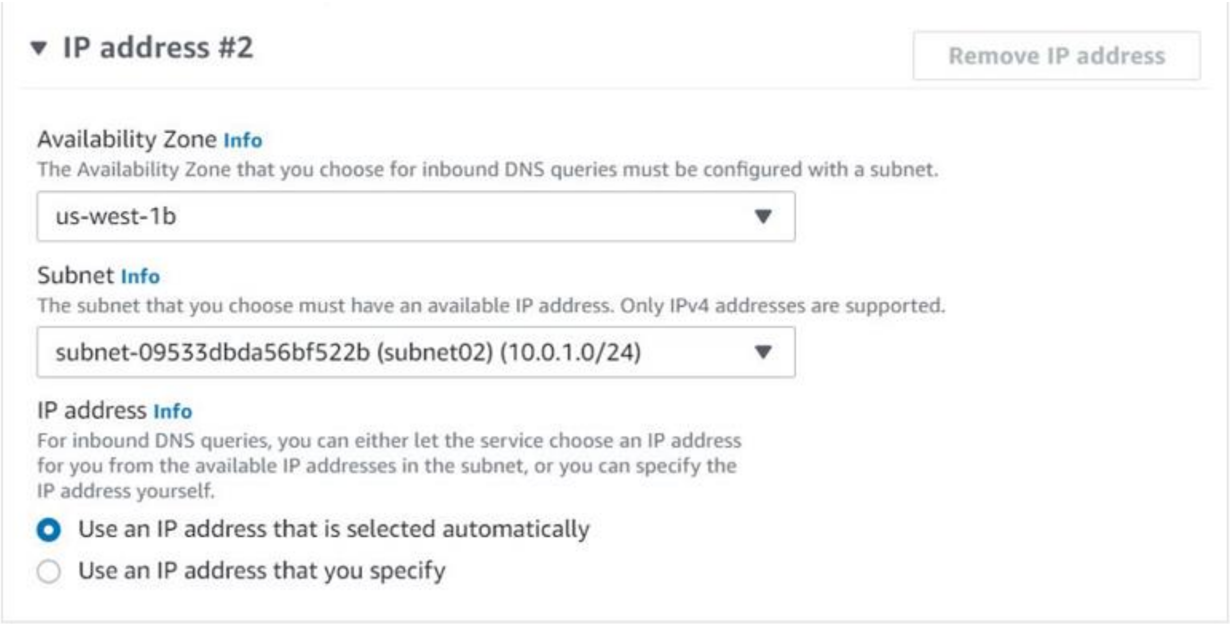
Subnet Info
The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.
subnet-076c4bd4c3faff122 (Public subnet) (10.0.0.0/24) ▼

IP address Info
For inbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

● Use an IP address that is selected automatically

○ Use an IP address that you specify

Add the first IP address



Availability Zone Info

The Availability Zone that you choose for inbound DNS queries must be configured with a subnet.

us-west-1b ▼

Subnet Info

The subnet that you choose must have an available IP address. Only IPv4 addresses are supported.

subnet-09533dbda56bf522b (subnet02) (10.0.1.0/24) ▼

IP address Info

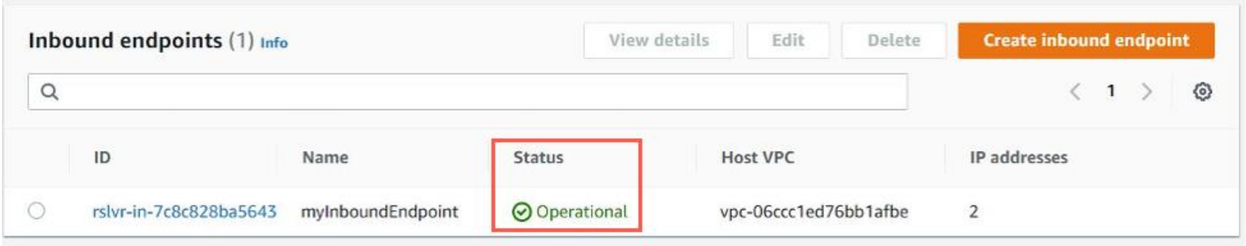
For inbound DNS queries, you can either let the service choose an IP address for you from the available IP addresses in the subnet, or you can specify the IP address yourself.

● Use an IP address that is selected automatically

○ Use an IP address that you specify

Add the second IP address

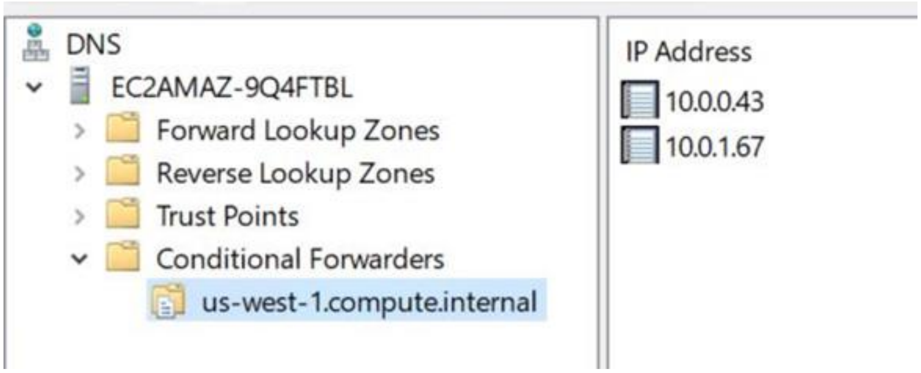
6. Review the options and click **Submit** to create the outbound endpoint.



	ID	Name	Status	Host VPC	IP addresses
○	rslvr-in-7c8c828ba5643	myInboundEndpoint	✓ Operational	vpc-06ccc1ed76bb1afbe	2

The inbound endpoint is operational

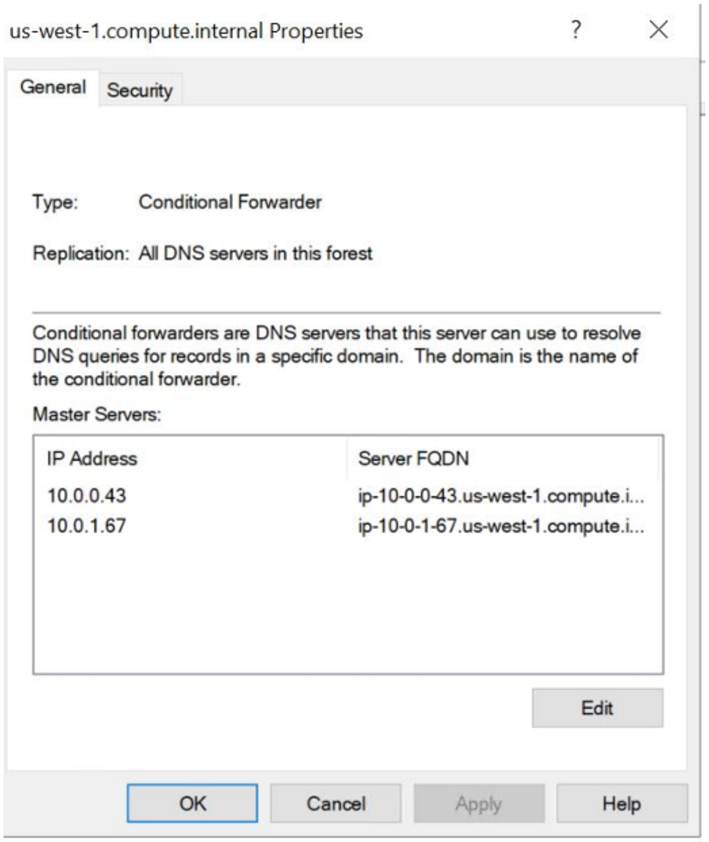
7. Create Resolver rules to resolve the direct lookup of the AWS DNS zone. This enables local DNS clients to issue DNS forwarding queries to AWS instances by their internal DNS names.



DNS
EC2AMAZ-9Q4FTBL
Forward Lookup Zones
Reverse Lookup Zones
Trust Points
Conditional Forwarders
us-west-1.compute.internal

IP Address
10.0.0.43
10.0.1.67

Inside Active Directory DNS, create conditional forwarders with the IP addresses of the previously created Route 53 Inbound endpoint.



us-west-1.compute.internal Properties

Type: Conditional Forwarder

Replication: All DNS servers in this forest

Conditional forwarders are DNS servers that this server can use to resolve DNS queries for records in a specific domain. The domain is the name of the conditional forwarder.

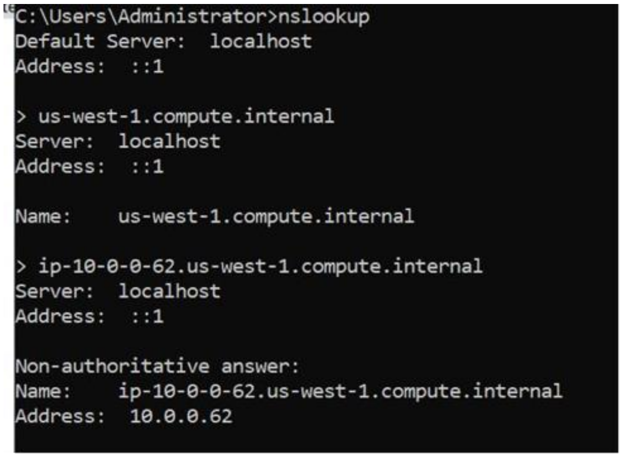
Master Servers:

IP Address	Server FQDN
10.0.0.43	ip-10-0-0-43.us-west-1.compute.i...
10.0.1.67	ip-10-0-1-67.us-west-1.compute.i...

The conditional forwarder lists the IP addresses of the previously created Route 53 Inbound endpoint

Note: If you have an AWS Managed Microsoft Active Directory environment, these servers are in your VPC. Use the "VPC +2 Resolver" for the blind forwarder. Do not use 169.254.169.253 for the blind forwarder in your AWS Managed Microsoft AD deployment. Use the "VPC +2 Resolver" where the AWS Managed Microsoft AD resides. The AWS Managed Microsoft AD domain controllers will not route request to 169.254.169.253 in your VPC. In the example for this solution, the VPC CIDR 10.0.0.0/16 has a conditional of sa-east-1.compute.internal for IP 10.0.0.2, and not the IP addresses of the Route 53 inbound endpoint.

You can test these configurations for the inbound endpoint using a computer in the on-premises environment using the nslookup tool for the internal address of an EC2 instance.



```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  ::1

> us-west-1.compute.internal
Server:  localhost
Address:  ::1

Name:    us-west-1.compute.internal

> ip-10-0-0-62.us-west-1.compute.internal
Server:  localhost
Address:  ::1

Non-authoritative answer:
Name:    ip-10-0-0-62.us-west-1.compute.internal
Address:  10.0.0.62
```

Inside the Domain Controller, test a query to us-west-1.compute.internal. This query will be successfully forwarded to the inbound endpoint.

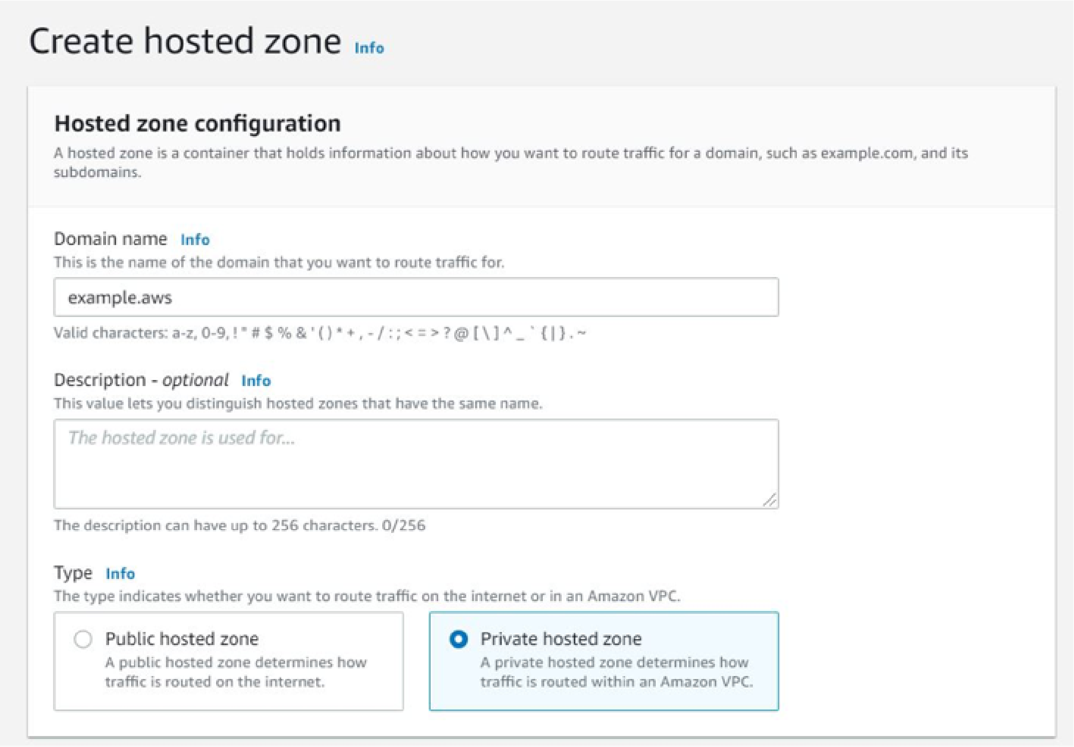
Multi-accounts with private hosted zones

While the solutions described in this whitepaper help for the .2 resolver FQDNs, other organizations have multi-account environments. These organizations create Private Hosted Zones (PHZs) to have more name resolution controls in their AWS environment.

This solution enables hybrid name resolution in multi-account environments with Active Directory and Amazon Route 53 environments. First, create a Private Hosted Zone (PHZ).

To create a Private Hosted Zone:

1. From the Route 53 console, choose **Hosted Zones** > **Create Hosted Zone**.
2. In the setup for the PHZ, enter the domain name.
3. Choose **Private Hosted Zone** and associate it with a VPC.



Create hosted zone Info

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name Info

This is the name of the domain that you want to route traffic for.

example.aws

Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Description - *optional* Info

This value lets you distinguish hosted zones that have the same name.

The hosted zone is used for...

The description can have up to 256 characters. 0/256

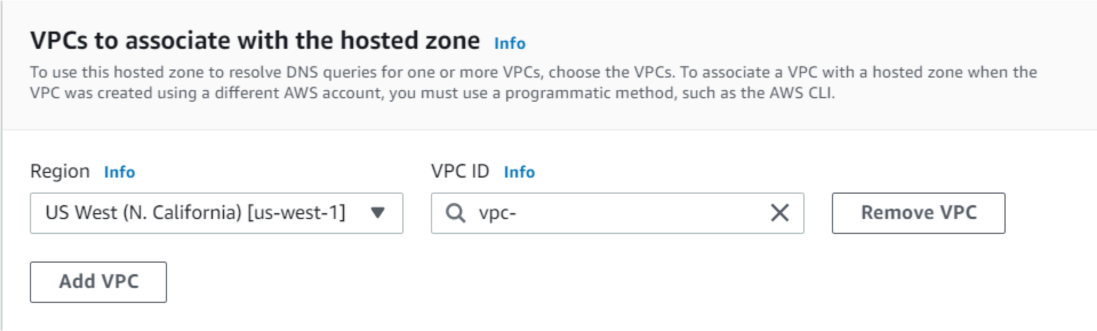
Type Info

The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

○ Public hosted zone
A public hosted zone determines how traffic is routed on the internet.

● Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.

Choose ***Private hosted zone***



VPCs to associate with the hosted zone Info

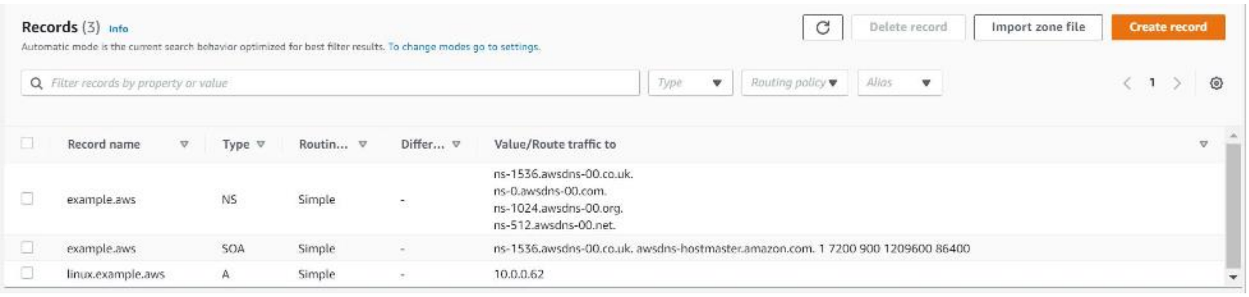
To use this hosted zone to resolve DNS queries for one or more VPCs, choose the VPCs. To associate a VPC with a hosted zone when the VPC was created using a different AWS account, you must use a programmatic method, such as the AWS CLI.

Region Info: US West (N. California) [us-west-1]

VPC ID Info: vpc-

Associate the PHZ with a VPC

4. Create an “`A`” record with the IP of one server in this VPC.
5. Add the record name `linux.example.aws` for the IP address `10.0.0.62`.
6. Choose **Create record**.

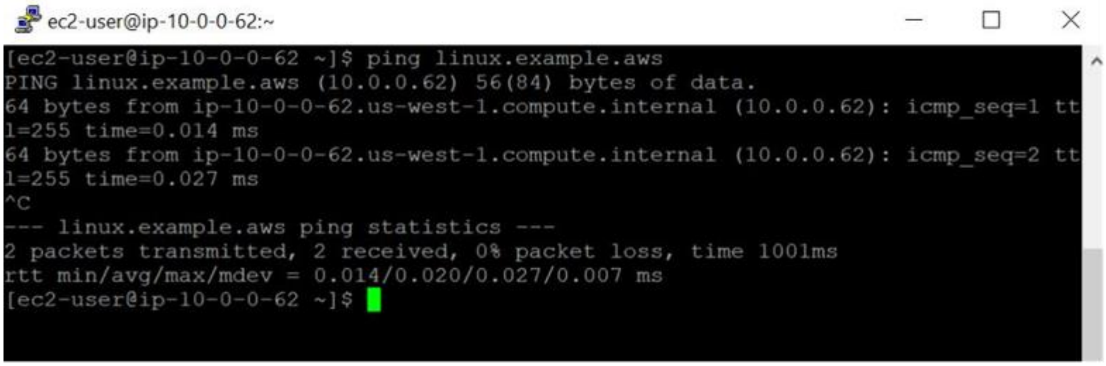


Records (3) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Delete record
Import zone file
Create record
Filter records by property or value
Type
Routing policy
Alias
1

□	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	example.aws	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
□	example.aws	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
□	linux.example.aws	A	Simple	-	10.0.0.62

Add `linux.example.aws`

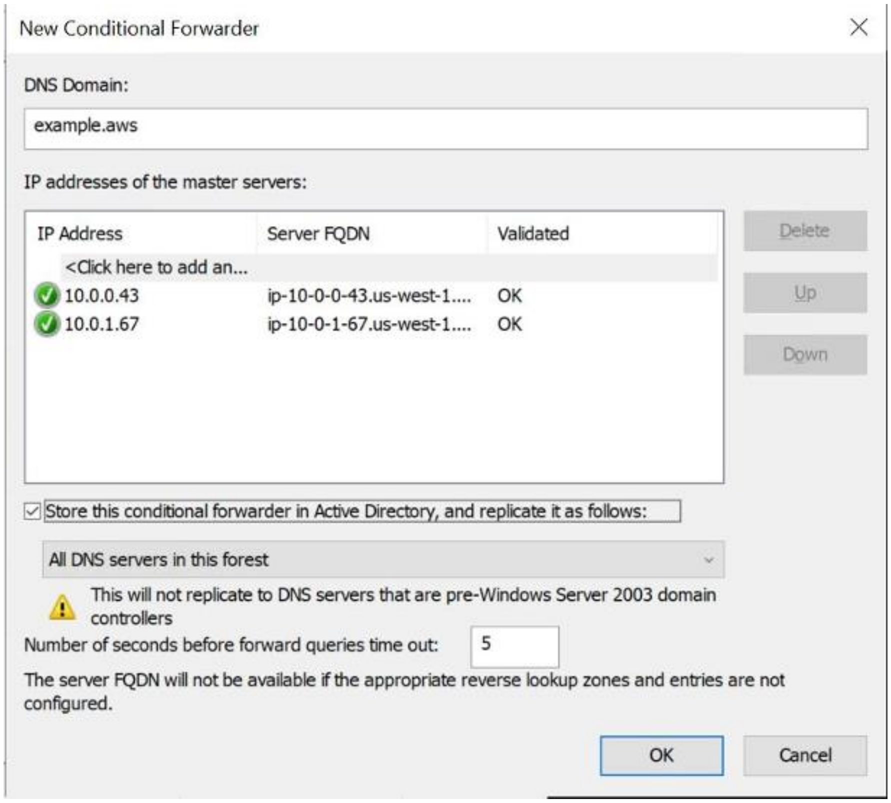
7. As the inbound and PHZ for this VPC are associated, a host of this VPC must resolve the name `linux.example.aws` to the IP `10.0.0.62`. If you have created the PHZ and associated it to a different VPC, simply create a new inbound endpoint to the VPC being used.



```
[ec2-user@ip-10-0-0-62 ~]$ ping linux.example.aws
PING linux.example.aws (10.0.0.62) 56(84) bytes of data.
64 bytes from ip-10-0-0-62.us-west-1.compute.internal (10.0.0.62): icmp_seq=1 tt
l=255 time=0.014 ms
64 bytes from ip-10-0-0-62.us-west-1.compute.internal (10.0.0.62): icmp_seq=2 tt
l=255 time=0.027 ms
^C
--- linux.example.aws ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.014/0.020/0.027/0.007 ms
[ec2-user@ip-10-0-0-62 ~]$
```

EC2 10.0.0.62, which resides in the associated VPC, will successfully query `linux.example.aws`

8. Enable the Active Directory DNS to resolve the names of this PHZ with the creation of a conditional forwarder for the Amazon Route 53 inbound endpoint IPs. After this change, hosts using DNS servers from this AD environment must resolve the name `linux.example.aws` to the IP `10.0.0.62`.



New Conditional Forwarder

DNS Domain:

example.aws

IP addresses of the master servers:

IP Address	Server FQDN	Validated
<Click here to add an...		
✓ 10.0.0.43	ip-10-0-0-43.us-west-1....	OK
✓ 10.0.1.67	ip-10-0-1-67.us-west-1....	OK

☑ Store this conditional forwarder in Active Directory, and replicate it as follows:

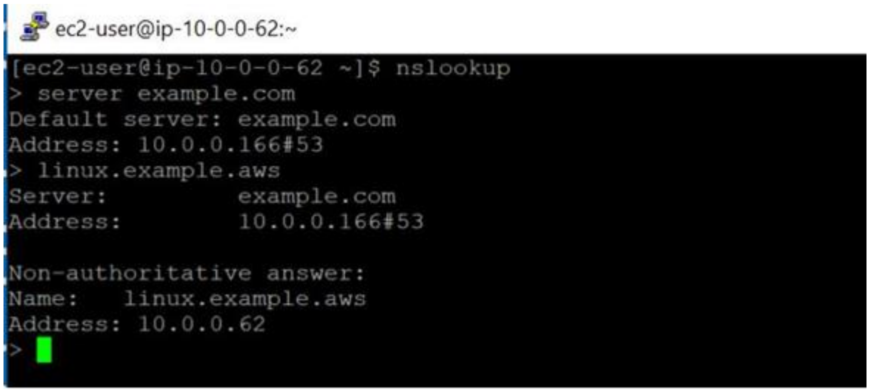
All DNS servers in this forest

⚠ This will not replicate to DNS servers that are pre-Windows Server 2003 domain controllers

Number of seconds before forward queries time out: 5

The server FQDN will not be available if the appropriate reverse lookup zones and entries are not configured.

Create a conditional forwarder for `example.aws`, pointing to the IP addresses of the IP addresses of the inbound connector

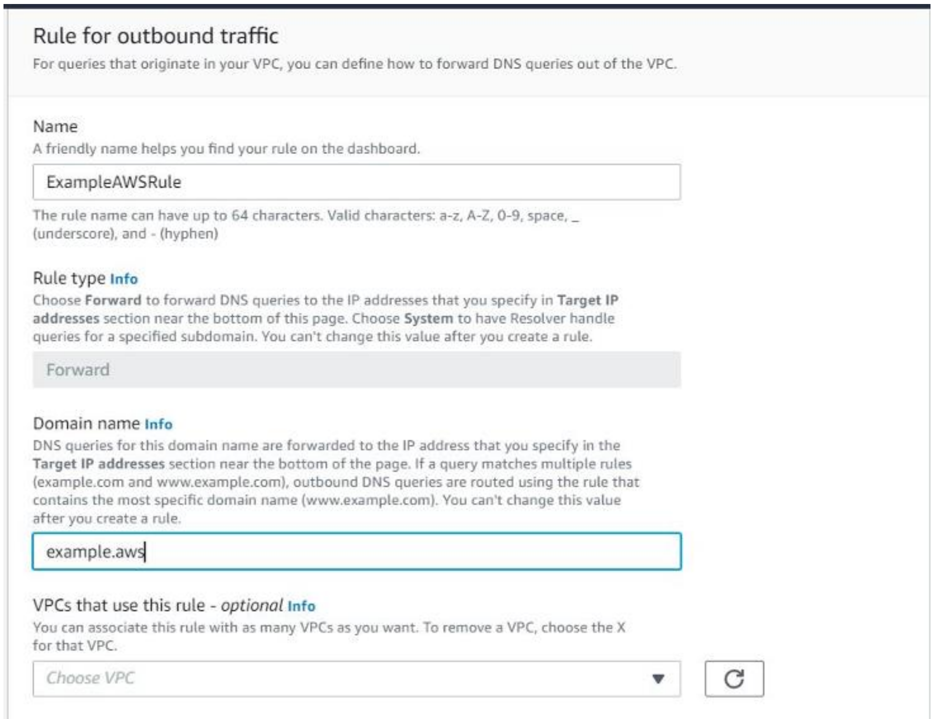


ec2-user@ip-10-0-0-62:~

```
[ec2-user@ip-10-0-0-62 ~]$ nslookup
> server example.com
Default server: example.com
Address: 10.0.0.166#53
> linux.example.aws
Server:         example.com
Address:        10.0.0.166#53

Non-authoritative answer:
Name:   linux.example.aws
Address: 10.0.0.62
> 
```

When using the IP address of the Active Directory DNS server as the nameserver, you can successfully query `linux.example.aws`.

9. For other AWS accounts to resolve the FQDNs of the Private Zone (`example.aws`), create a new forwarding rule in the outbound endpoint, pointing `example.aws` to the IPs of your inbound endpoints. This enables these accounts to forward to these IPs. In this step, **the rule is not associated with any VPC**. The rule serves only to forward name resolutions.



Rule for outbound traffic

For queries that originate in your VPC, you can define how to forward DNS queries out of the VPC.

Name

A friendly name helps you find your rule on the dashboard.

ExampleAWSRule

The rule name can have up to 64 characters. Valid characters: a-z, A-Z, 0-9, space, _ (underscore), and - (hyphen)

Rule type Info

Choose **Forward** to forward DNS queries to the IP addresses that you specify in **Target IP addresses** section near the bottom of this page. Choose **System** to have Resolver handle queries for a specified subdomain. You can't change this value after you create a rule.

Forward

Domain name Info

DNS queries for this domain name are forwarded to the IP address that you specify in the **Target IP addresses** section near the bottom of the page. If a query matches multiple rules (example.com and www.example.com), outbound DNS queries are routed using the rule that contains the most specific domain name (www.example.com). You can't change this value after you create a rule.

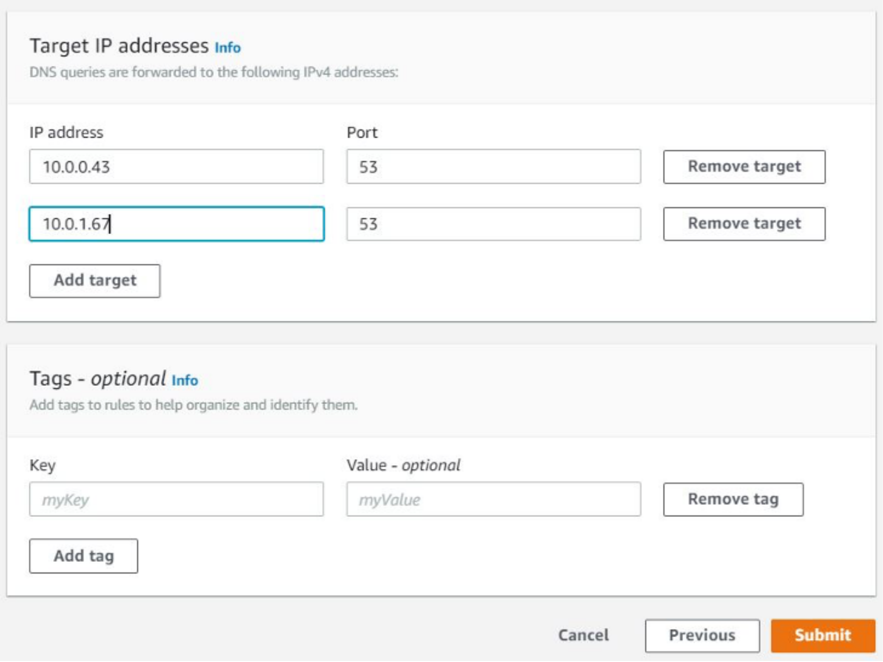
example.aws

VPCs that use this rule - *optional* Info

You can associate this rule with as many VPCs as you want. To remove a VPC, choose the X for that VPC.

Choose VPC

Create a new forwarding rule in the outbound endpoint



Target IP addresses Info

DNS queries are forwarded to the following IPv4 addresses:

IP address	Port	
10.0.0.43	53	Remove target
10.0.1.67	53	Remove target

Add target

Tags - *optional* Info

Add tags to rules to help organize and identify them.

Key	Value - *optional*	
myKey	*myValue*	Remove tag

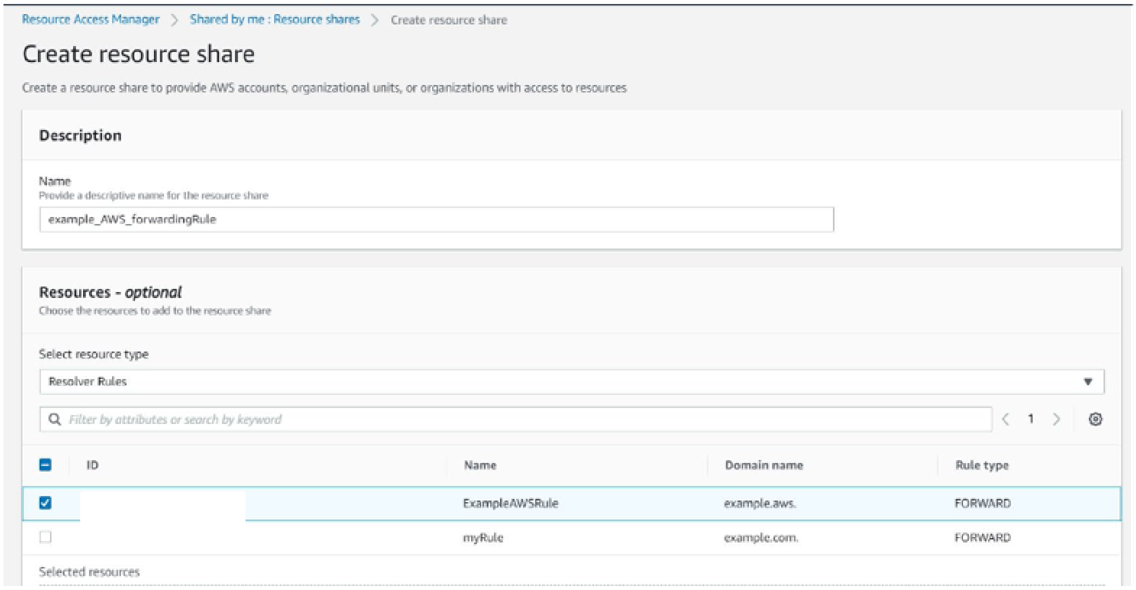
Add tag

Cancel Previous Submit

Point `example.aws` to the IPs of the inbound endpoints

Taking in consideration that these accounts have network communication between each other, the next step is to expand this configuration to multi-accounts. Use Resource Access Manager (RAM) to share resources between accounts.

10. Share the outbound endpoint rules for the secondary accounts in the **Resource Access Manager** > **Resource shares** > **Create resource share option**.



Resource Access Manager > Shared by me : Resource shares > Create resource share

Create resource share

Create a resource share to provide AWS accounts, organizational units, or organizations with access to resources

Description

Name
Provide a descriptive name for the resource share
example_AWS_forwardingRule

Resources - *optional*
Choose the resources to add to the resource share

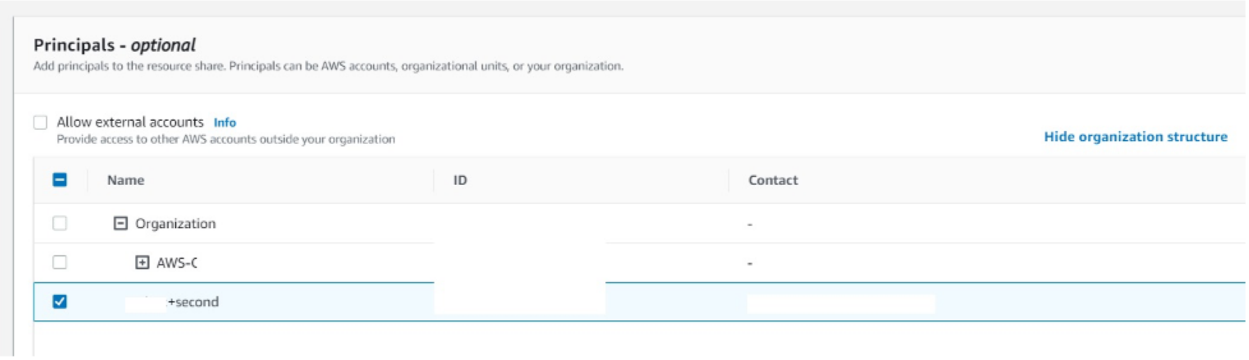
Select resource type
Resolver Rules ▼

Filter by attributes or search by keyword

	ID	Name	Domain name	Rule type
☑		ExampleAWSRule	example.aws.	FORWARD
□		myRule	example.com.	FORWARD

Selected resources

*The **Create resource share** dialog*



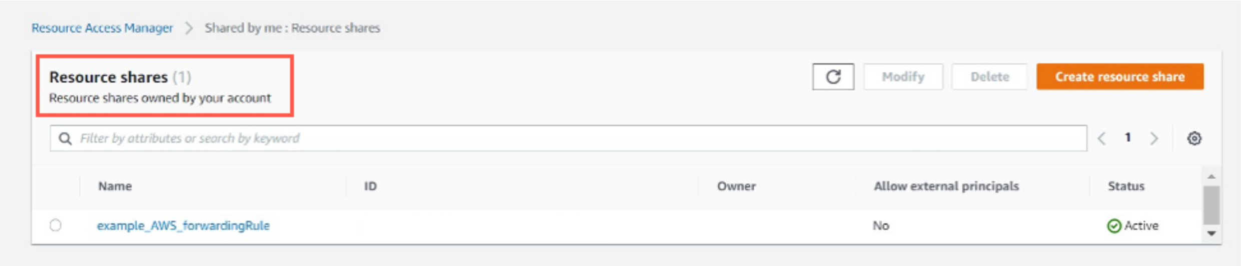
Principals - *optional*
Add principals to the resource share. Principals can be AWS accounts, organizational units, or your organization.

□ Allow external accounts Info
Provide access to other AWS accounts outside your organization

Hide organization structure

	Name	ID	Contact
□	⊟ Organization		-
□	⊞ AWS-(		-
☑	+second		

Select the account to which the resource will be shared.



Resource Access Manager > Shared by me : Resource shares

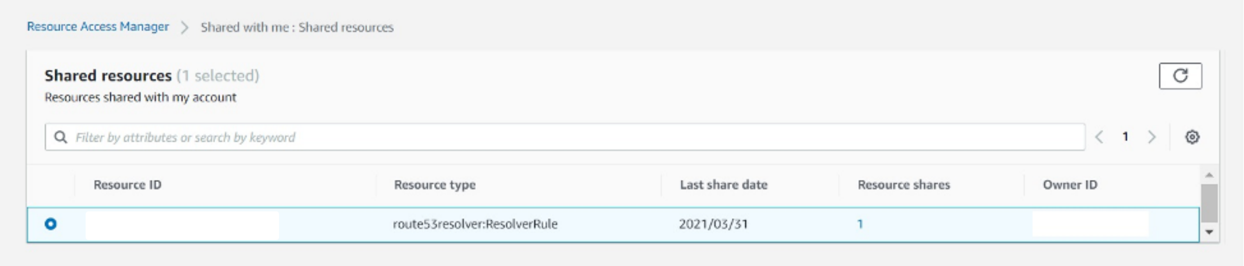
Resource shares (1)
Resource shares owned by your account

Filter by attributes or search by keyword

	Name	ID	Owner	Allow external principals	Status
○	example_AWS_forwardingRule			No	Active

The forwarding rule resource shows as shared by the account

11. In the shared account, list the resolver rule in **Resource Access Manager** > **Shared with me**.

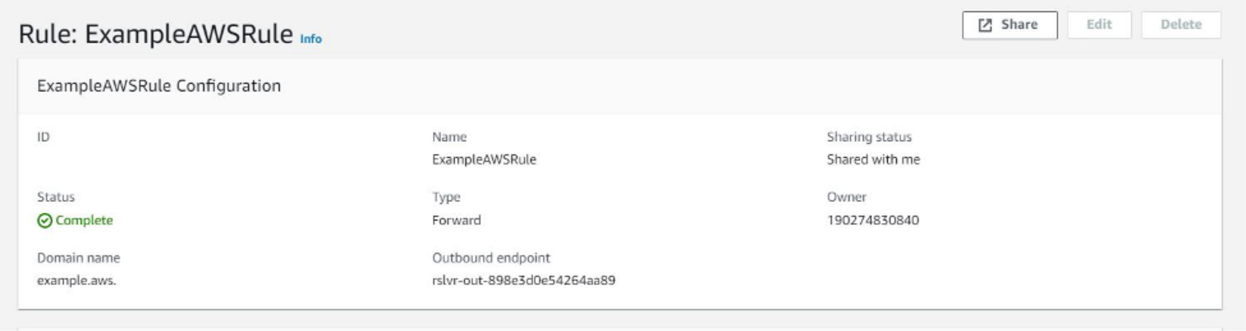


Resource Access Manager > Shared with me : Shared resources

Shared resources (1 selected)
Resources shared with my account

	Resource ID	Resource type	Last share date	Resource shares	Owner ID
●		route53resolver:ResolverRule	2021/03/31	1	

*The **Shared with me** dialog*



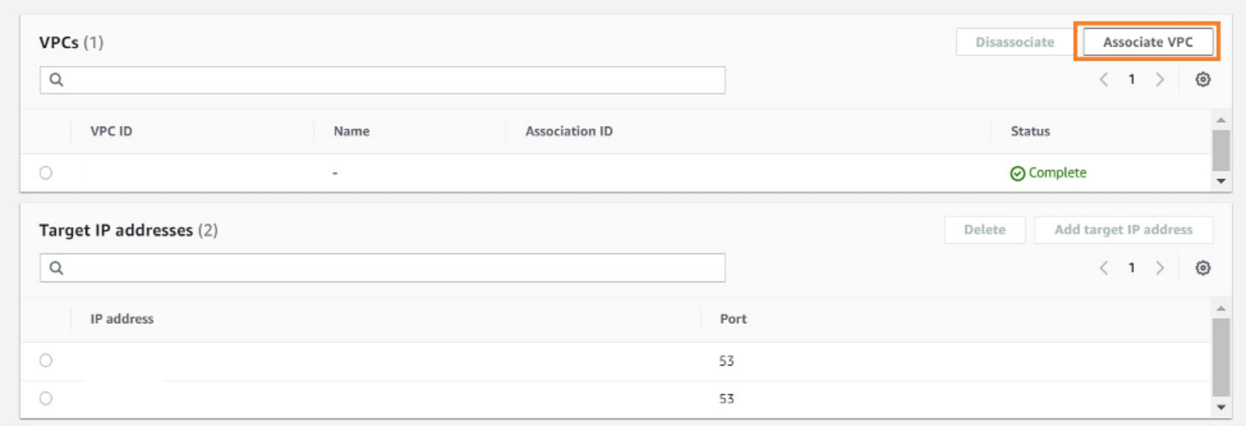
Rule: ExampleAWSRule Info

ExampleAWSRule Configuration

ID	Name ExampleAWSRule	Sharing status Shared with me
Status Complete	Type Forward	Owner 190274830840
Domain name example.aws.	Outbound endpoint rslvr-out-898e3d0e54264aa89	

Choose the resource to see its configuration

12. Associate the rules for the secondary account VPC by choosing **Associate VPC**.



VPCs (1)

	VPC ID	Name	Association ID	Status
○		-		Complete

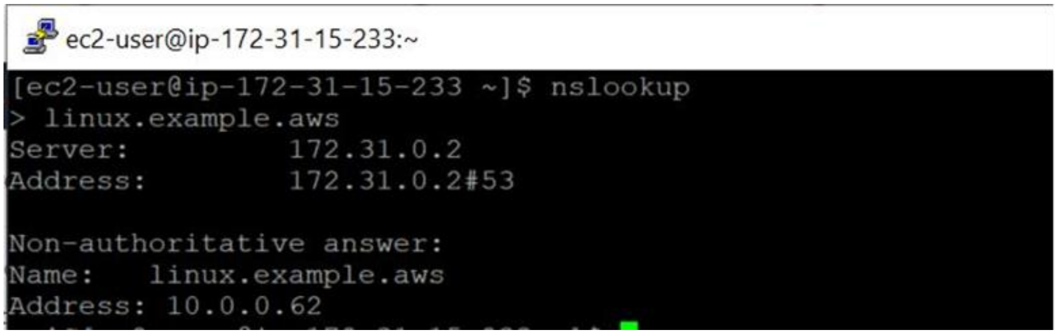
Target IP addresses (2)

	IP address	Port
○		53
○		53

*Choose **Associate VPC***

13. Launch a server in the VPC of the secondary account.

14. With the premise that networking exists between VPCs (peering, routing, and security groups configured correctly), query the DNS again. PHZ name resolution for primary account `linux.example.aws`.



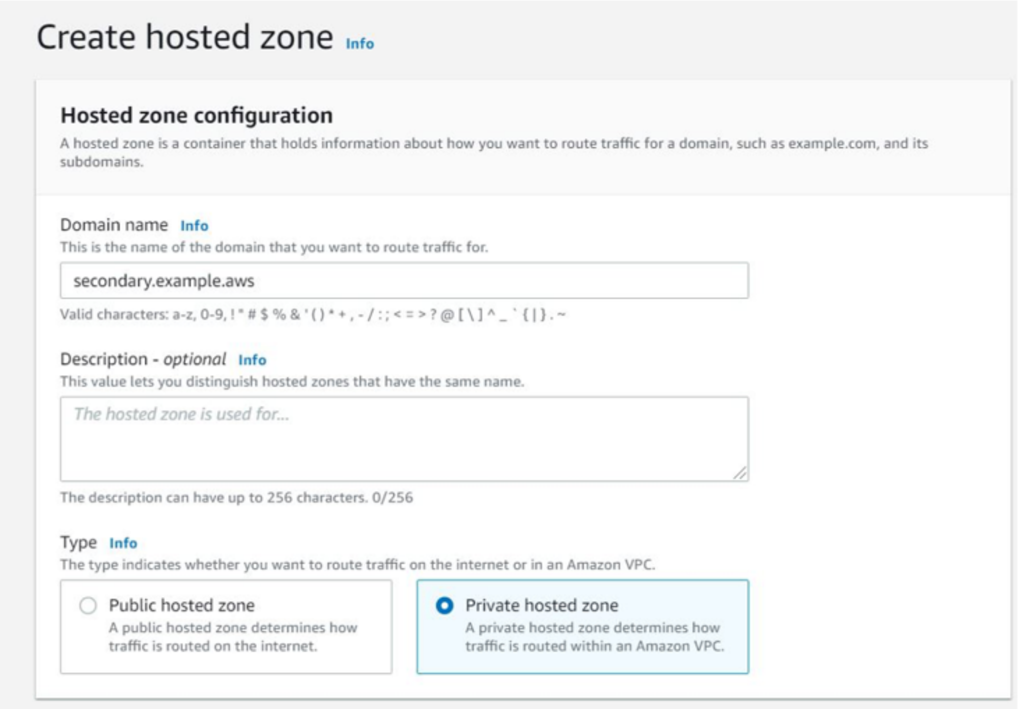
ec2-user@ip-172-31-15-233:~

```
[ec2-user@ip-172-31-15-233 ~]$ nslookup
> linux.example.aws
Server:         172.31.0.2
Address:        172.31.0.2#53

Non-authoritative answer:
Name:   linux.example.aws
Address: 10.0.0.62
```

Query the DNS

With this solution, any record created in a Private Zone in this secondary account is resolved by the on-premises environment, and also by the primary account.

15. In Route 53 of the secondary account, create a second PHZ (`secondary.example.aws`) with an `A` record.



Create hosted zone Info

Hosted zone configuration

A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

Domain name Info
This is the name of the domain that you want to route traffic for.
secondary.example.aws
Valid characters: a-z, 0-9, ! " # $ % & ' ( ) * + , - / : ; < = > ? @ [\ ] ^ _ ` { | } . ~

Description - *optional* Info
This value lets you distinguish hosted zones that have the same name.
The hosted zone is used for...
The description can have up to 256 characters. 0/256

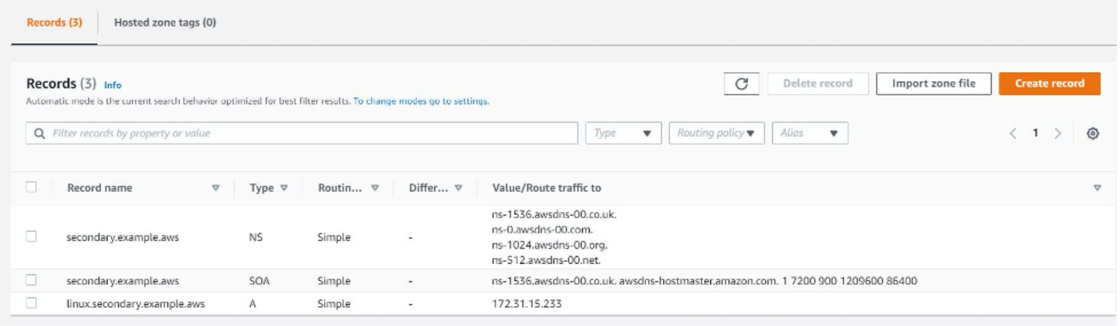
Type Info
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

○ Public hosted zone
A public hosted zone determines how traffic is routed on the internet.

● Private hosted zone
A private hosted zone determines how traffic is routed within an Amazon VPC.

Create a second PHZ

16. Create an `A` record named “`linux.secondary.example.com`”, which points to the IP address of the EC2 host previously launched in step 13.



Records (3)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

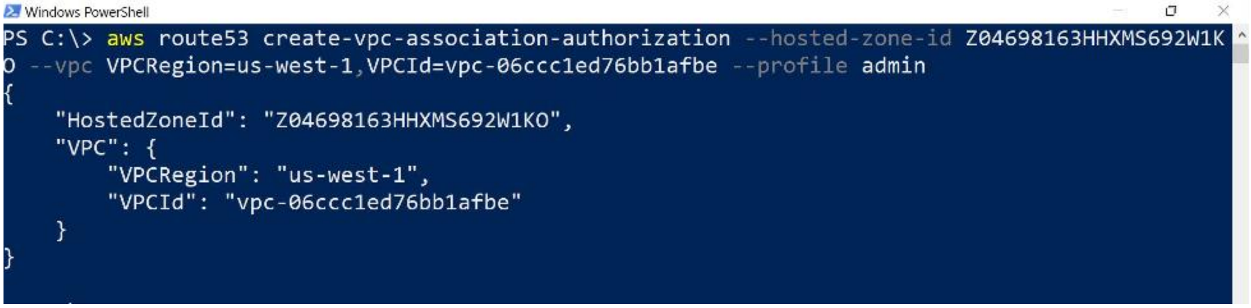
□	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	secondary.example.aws	NS	Simple	-	ns-1536.awsdns-00.co.uk. ns-0.awsdns-00.com. ns-1024.awsdns-00.org. ns-512.awsdns-00.net.
□	secondary.example.aws	SOA	Simple	-	ns-1536.awsdns-00.co.uk. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
□	linux.secondary.example.aws	A	Simple	-	172.31.15.233

Create an `A` *record named “*`linux.secondary.example.com`*”*

In the next steps, you will associate the Private Zone with the DNS from the primary account. This will make the primary account's DNS the “resolver” between AWS accounts. As the resources exist in different accounts, you will create the authorization request from the account that has the Private Zone (secondary) for the primary account.

a. In the **secondary** account, create the authorization using the Private ID of the zone (`secondary.example.aws`) and information from the Region and the ID of the primary VPC:

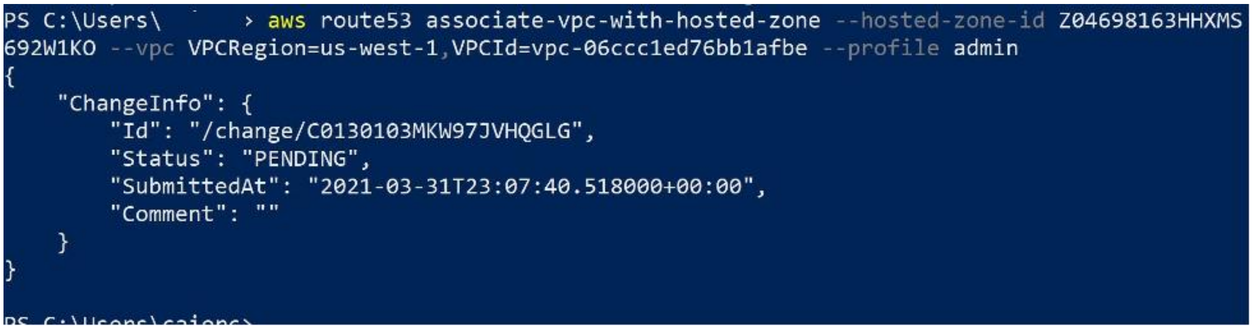
```
aws route53 create-vpc-association-authorization --hosted-
zone-id <hosted-zone-id> --vpc VPCRegion=<region>
,VPCId=<vpc-id>
```



```
PS C:\> aws route53 create-vpc-association-authorization --hosted-zone-id Z04698163HHXMS692W1K
O --vpc VPCRegion=us-west-1,VPCId=vpc-06ccc1ed76bb1afbe --profile admin
{
    "HostedZoneId": "Z04698163HHXMS692W1KO",
    "VPC": {
        "VPCRegion": "us-west-1",
        "VPCId": "vpc-06ccc1ed76bb1afbe"
    }
}
```

Secondary account VPC association authorization.

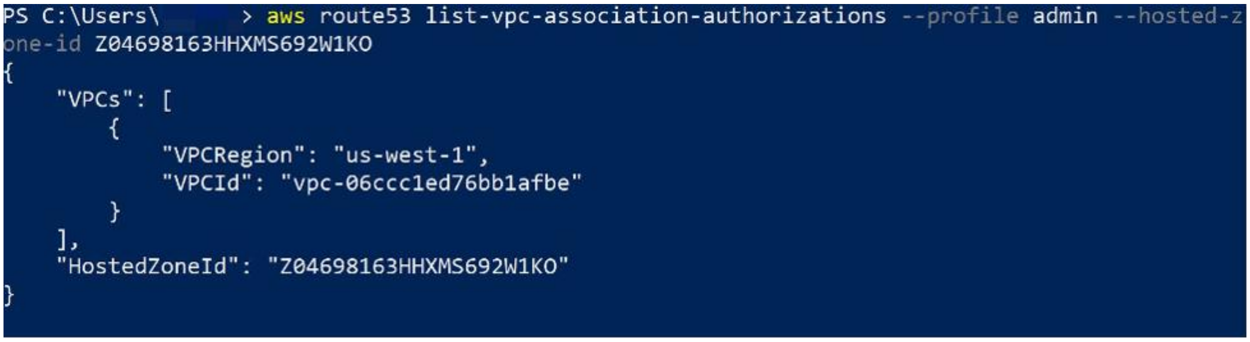
b. In the primary account, associate the VPC with the Private Hosted Zone of the secondary account:



```
PS C:\Users\[redacted]> aws route53 associate-vpc-with-hosted-zone --hosted-zone-id Z04698163HHXMS
692W1KO --vpc VPCRegion=us-west-1,VPCId=vpc-06ccc1ed76bb1afbe --profile admin
{
    "ChangeInfo": {
        "Id": "/change/C0130103MKW97JVHQGLG",
        "Status": "PENDING",
        "SubmittedAt": "2021-03-31T23:07:40.518000+00:00",
        "Comment": ""
    }
}

PS C:\Users\caiones>
```

Primary account, VPC association with the PHZ of the secondary account.

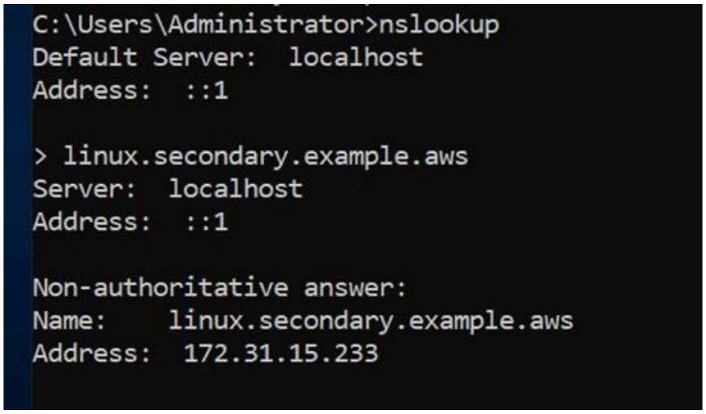
c. Confirm the association by running the command `aws route53 list-vpc-associationauthorizations` in the secondary account.



```
PS C:\Users\[redacted]> aws route53 list-vpc-association-authorizations --profile admin --hosted-z
one-id Z04698163HHXMS692W1KO
{
    "VPCs": [
        {
            "VPCRegion": "us-west-1",
            "VPCId": "vpc-06ccc1ed76bb1afbe"
        }
    ],
    "HostedZoneId": "Z04698163HHXMS692W1KO"
}
```

Confirming the VPC association.

After this last step, you can reach the `A` record created for the Private Hosted Zone of the secondary account from the primary account VPC.



```
C:\Users\Administrator>nslookup
Default Server:  localhost
Address:  ::1

> linux.secondary.example.aws
Server:  localhost
Address:  ::1

Non-authoritative answer:
Name:    linux.secondary.example.aws
Address:  172.31.15.233
```

Query `linux.secondary.example.aws` from the primary account

> **Note**: For running the cmdlets of the configuration of the VPC association, you can use [AWS CLI v2 integrated with AWS SSO](#).

Additional considerations

- Use domain controllers as DNS servers, because domain controllers support features such as dynamic updates from Windows DNS clients. Other types of DNS servers (such as DNS without the Domain Controller role) may not support these features.
- Try to maintain local DNS name resolution in the AWS Region to reduce latency.
- Share centralized Route 53 Resolver endpoints across all VPCs in your organization. Create conditional forwarders on local DNS servers for all Route 53 DNS zones and DNS zones in AWS Managed AD (or AD DS in EC2 on-premises) and point them to the Route 53 resolver endpoints.
- Use Amazon DNS Server (Route 53) as a “forwarder” (conditional forwarder) for all other DNS domains that are not authorized on your DNS servers on AD domain controllers. This configuration enables your domain controllers to recursively resolve records in the Amazon Route 53 private zone and use the Route 53 Resolver conditional forwarders.
- Use Route 53 Resolver endpoints to create a DNS resolution hub and manage DNS traffic by creating conditional forwarders.
- Some administrators add the DHCP option set information by pointing to Active Directory DNS servers. Although this works for Active Directory resolution, you lose the `ec2.internal` resolution, forcing you to create a conditional forwarder in Active Directory for this resolution pointing to Route 53.
- The Amazon EC2 instance limits the number of packets that can be sent to the DNS server provided by Amazon, at a maximum of 1024 packets per second per network interface. This limit cannot be increased. If you encounter this performance limit, AWS recommends configuring this post for conditional forwarding to Amazon Route 53 private zones to use the Resolver service as well as root hints (DNS data sorted in a DNS server) for internet name resolution.
- If using an AD Connector, a recommended way to simplify your AD Connector deployment is to use Route 53 inbound endpoints for the DNS IP addresses and use a Route 53 outbound endpoint with a Resolver rule for the on-premises domain. If you ever need to update the on-premises DNS IPs, simply call the `UpdateResolverRule` API to update the Resolver rule with the new on-premises DNS IPs.

Conclusion

For organizations with AD DS, operating in a hybrid architecture is a necessary part of the cloud adoption process. This whitepaper discussed concepts as well as constraints to help you gain a better understanding of the fundamental building blocks of the solutions provided here, as well as the limitations that help create the most optimal solution for your workload.

The solutions provided include how to use Route 53 outbound and inbound endpoints, and AD DS conditional forwarder. The paper also provided guidance on how to select the appropriate solution for your intended multi-account workload, using VPC Association and Resource Access Manager. By using the architectures provided, you can achieve the most ideal private DNS interoperability between AD DS and Amazon Web Services.

Contributors

Contributors to this document include:

- Andrew Riley, Enterprise Support Lead
- Caio Ribeiro César, Principal Microsoft Specialist Solutions Architect
- Daniel Pires, Sr. Technical Account Manager
- Jeremy Girven, Sr. Microsoft Specialist Solutions Architect
- Vladimir Provorov, Sr. Directory Services Solutions Architect
- Syed Ahmad, Sr. Microsoft Specialist Solutions Architect

Appendix: CFN example (JSON)

For testing this with CloudFormation automation, please click here for the latest JSON code.

Document revisions

Date	Description
June 9, 2021	First publication