



AWS
re:Invent

NOV. 29 – DEC. 3, 2021 | LAS VEGAS, NV

Amazon Route 53: A year in review

Jeffrey Damick (he/him)

Principal Software Development Engineer,
Amazon Route 53
AWS

Gavin McCullagh (he/him)

Principal System Development Engineer,
Amazon Route 53
AWS

Agenda

Route 53 Resolver

- Forwarding rules improvements
- IPv6 resolver support
- Resolver query logs
- Resolver DNS Firewall

Route 53 DNSSEC

Route 53 Application Recovery Controller (ARC)

Agenda

Route 53 Resolver

- Forwarding rules improvements
- IPv6 resolver support
- Resolver query logs
- Resolver DNS Firewall

Route 53 DNSSEC

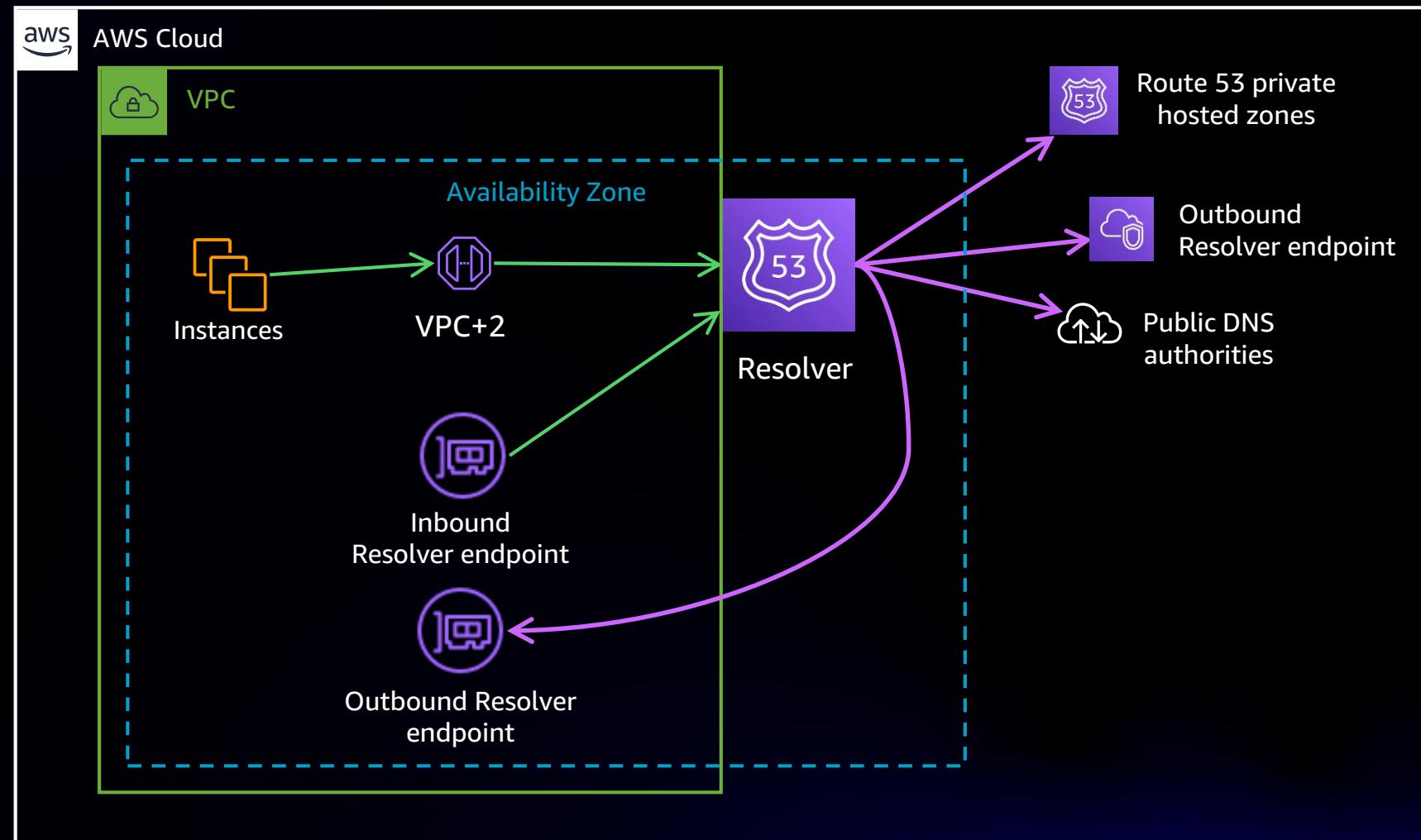
Route 53 Application Recovery Controller (ARC)

Route 53 Resolver



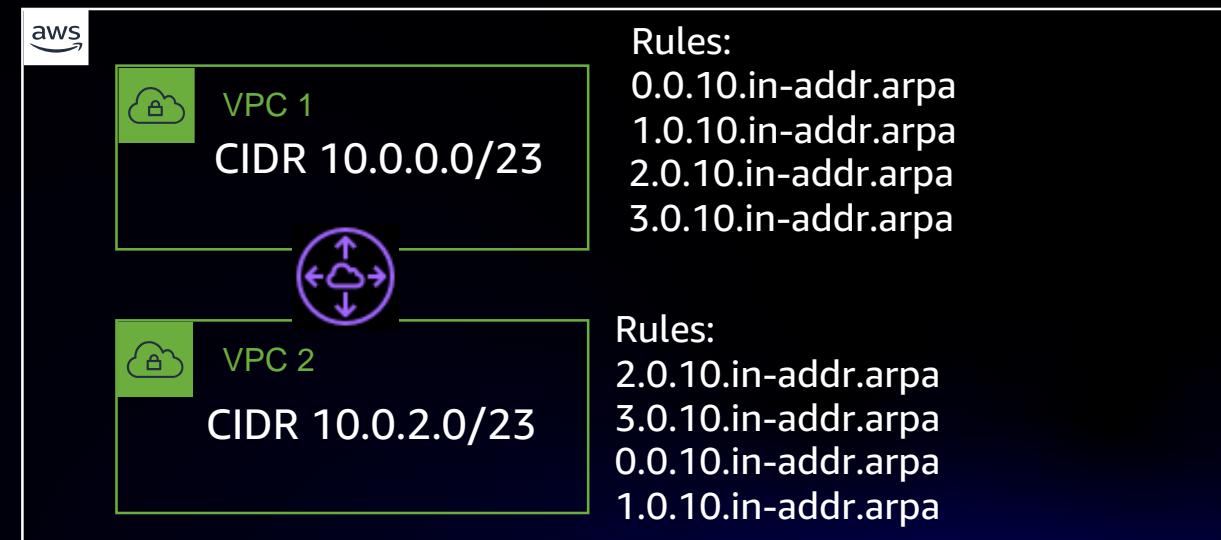
Route 53 Resolver

- Provides recursive DNS resolution
- Alternative names
 - AmazonProvidedDNS
 - VPC+2 Resolver
- Inbound Resolver endpoints
 - Provide resolution for resources outside a VPC
- Outbound Resolver endpoints
 - Forward DNS queries to a target server

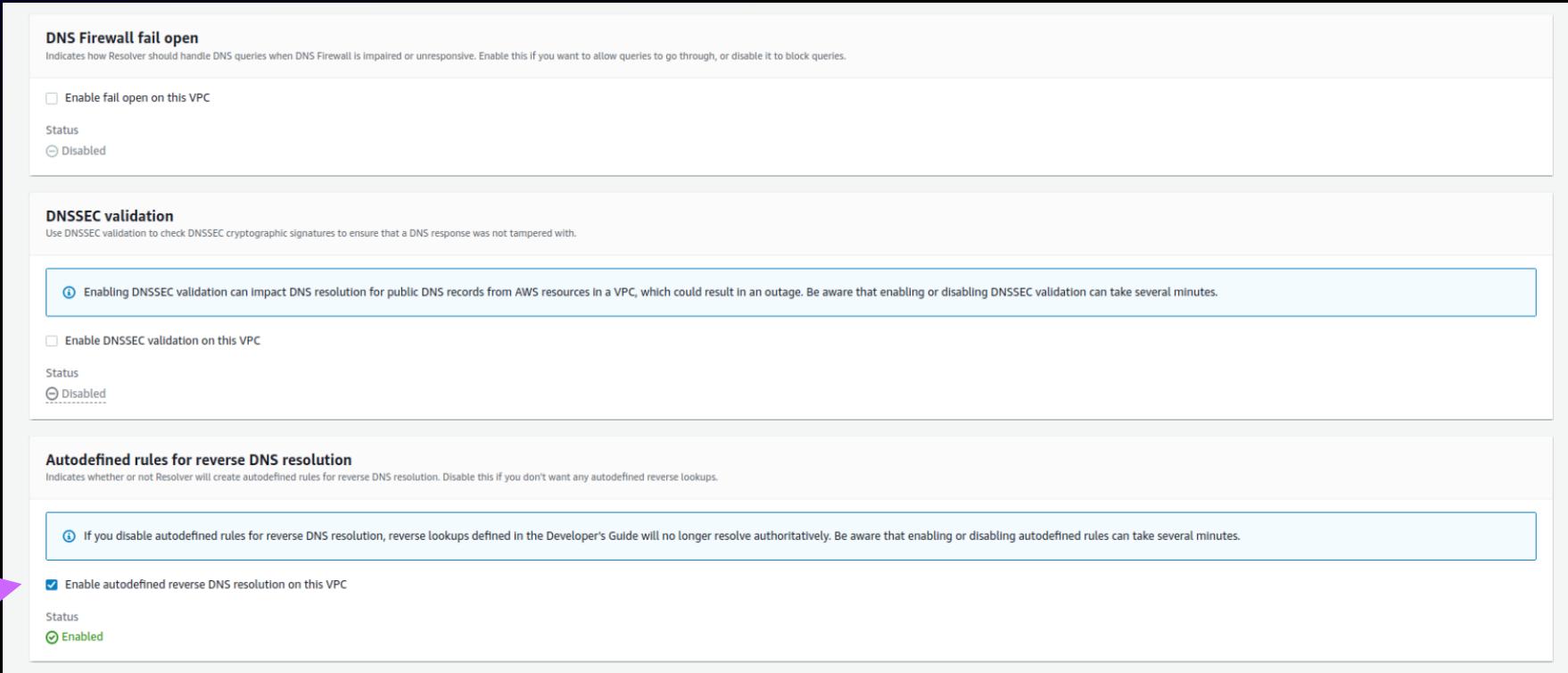


Reverse records

- Scenario: using Active Directory and want to it send PTR queries (reverse lookups)
- Previous solution: create Forward Rules for VPC CIDR blocks



Reverse records



DNS Firewall fail open
Indicates how Resolver should handle DNS queries when DNS Firewall is impaired or unresponsive. Enable this if you want to allow queries to go through, or disable it to block queries.

Enable fail open on this VPC
Status: Disabled

DNSSEC validation
Use DNSSEC validation to check DNSSEC cryptographic signatures to ensure that a DNS response was not tampered with.

ⓘ Enabling DNSSEC validation can impact DNS resolution for public DNS records from AWS resources in a VPC, which could result in an outage. Be aware that enabling or disabling DNSSEC validation can take several minutes.

Enable DNSSEC validation on this VPC
Status: Disabled

Autodefined rules for reverse DNS resolution
Indicates whether or not Resolver will create autodefined rules for reverse DNS resolution. Disable this if you don't want any autodefined reverse lookups.

ⓘ If you disable autodefined rules for reverse DNS resolution, reverse lookups defined in the Developer's Guide will no longer resolve authoritatively. Be aware that enabling or disabling autodefined rules can take several minutes.

Enable autodefined reverse DNS resolution on this VPC
Status: Enabled

- To disable autodefined rules for reverse DNS resolution, deselect the check box in the VPC details page
- Create a forwarding rule to Active Directory

IPv6

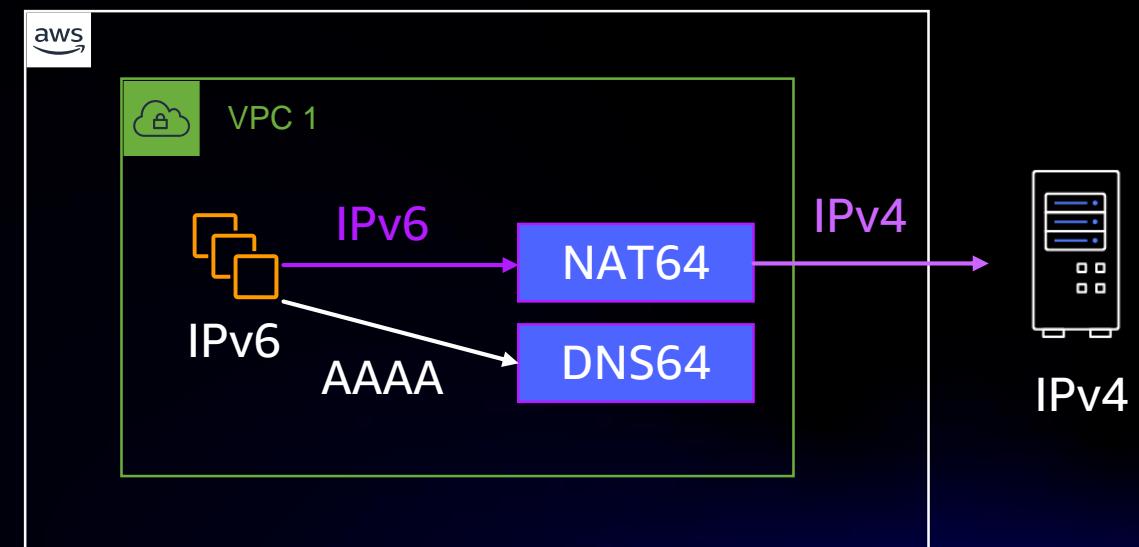
Scenario: transitioning to use IPv6 in a dual-stack environment with IPv4

- IPv4: 169.254.169.253
- Now IPv6: fd00:ec2::253 (Nitro)

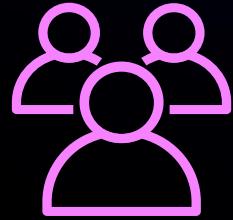
IPv6 and DNS64

Scenario: connect to IPv4 resources from an IPv6-only subnet

- DNS64: AAAA records synthesized for IPv4 addresses
- NAT64: IPv6 to IPv4 translation



Resolver query logging – Use cases



Compliance

Collect query logs, instances, and Resolver endpoints in a VPC



Debugging

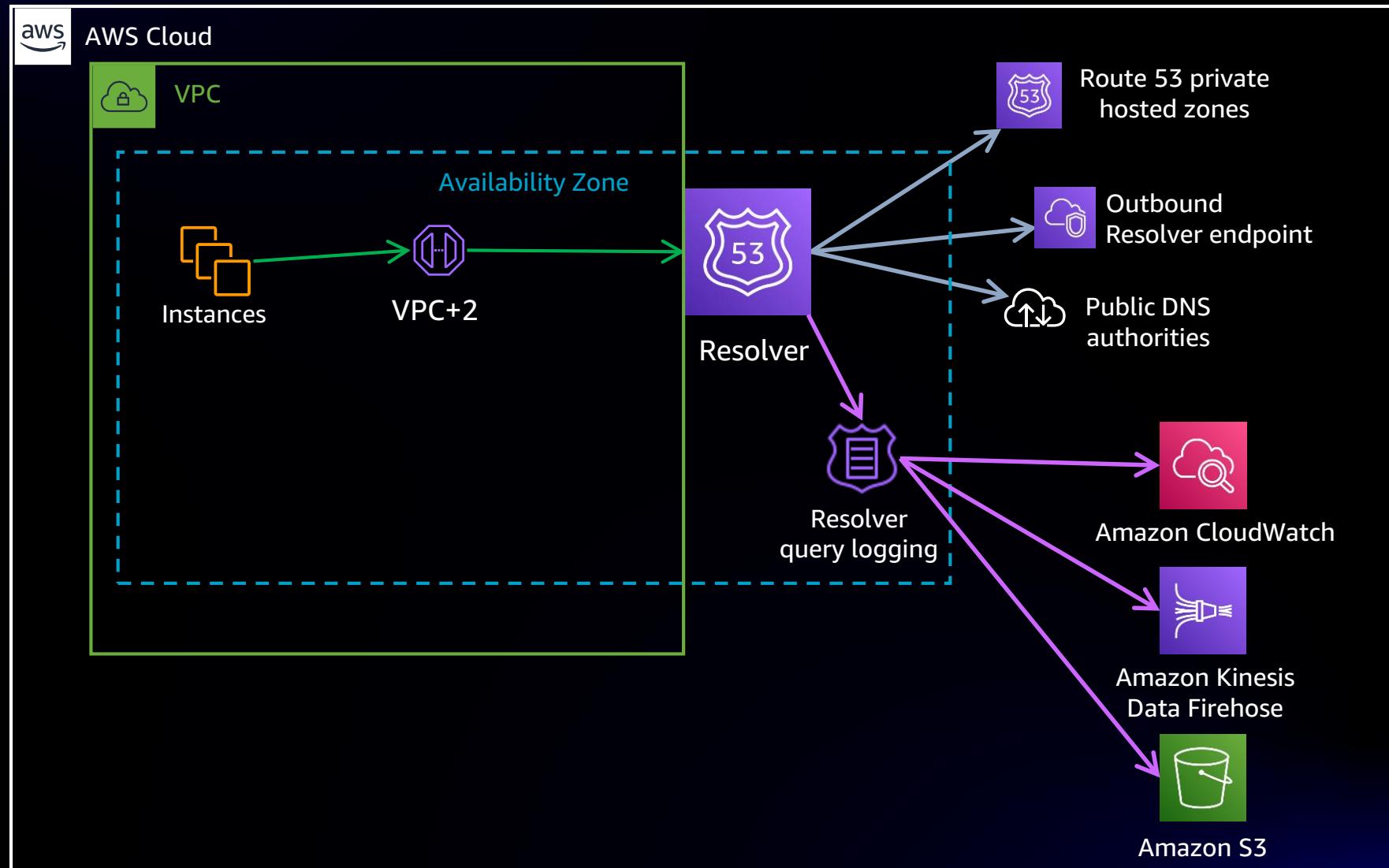
Find instances querying incorrect domain names



Threat Detection

Find instances querying malicious domain names

Resolver query logging

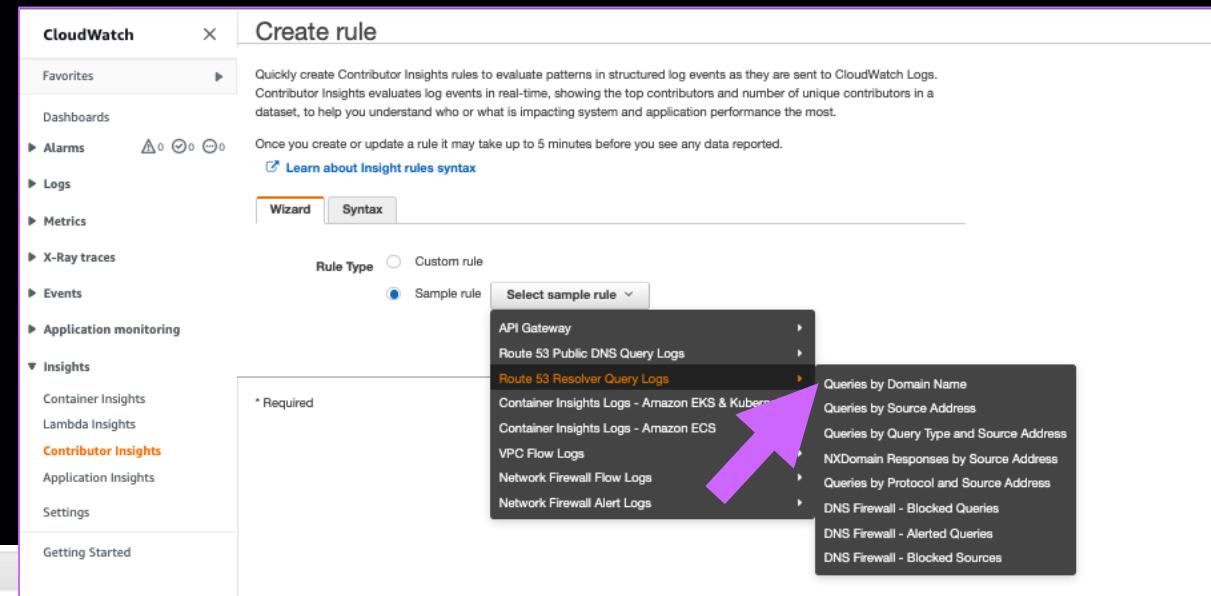
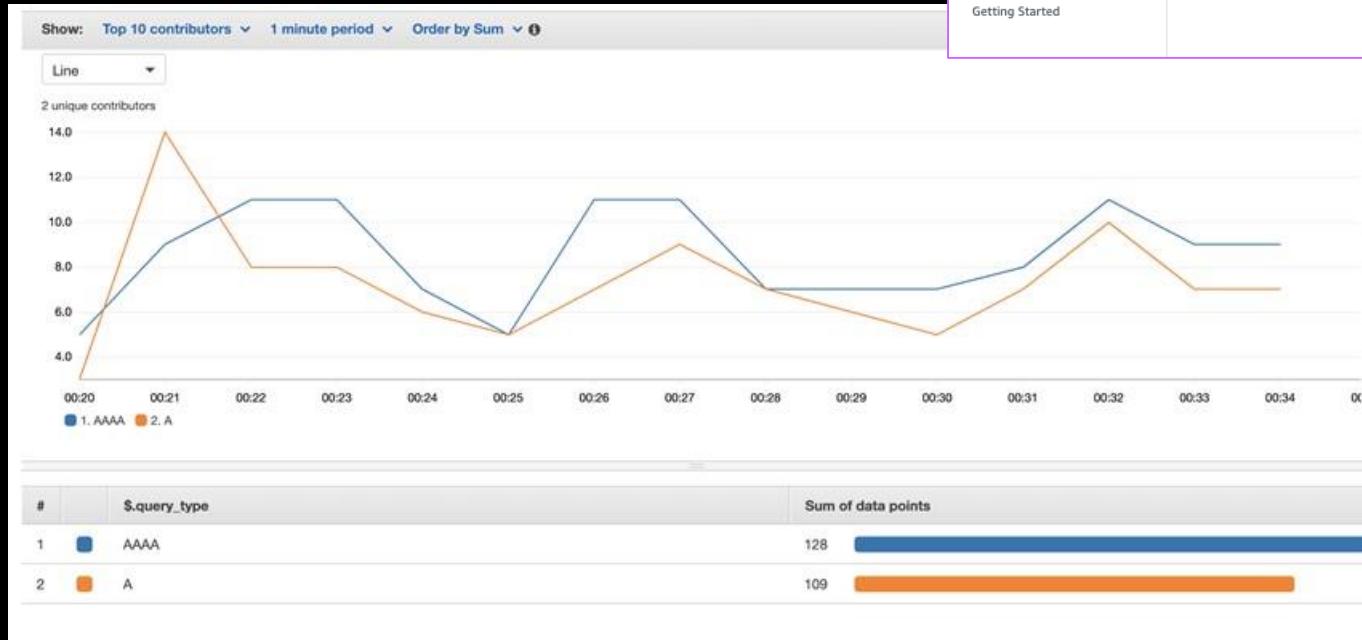


Resolver query logging

```
{  
    "version": "1.100000",  
    "account_id": "██████████",  
    "region": "us-west-2",  
    "vpc_id": "vpc-██████",  
    "query_timestamp": "2021-10-04T00:21:03Z",  
    "query_name": "damick.com.",  
    "query_type": "A",  
    "query_class": "IN",  
    "rcode": "NOERROR",  
    "answers": [],  
    "srcaddr": "172.31.10.87",  
    "srcport": "45586",  
    "transport": "UDP",  
    "srcids": {  
        "instance": "i-██████████"  
    },  
    "firewall_rule_action": "ALERT",  
    "firewall_rule_group_id": "rslvr-frg-██████████",  
    "firewall_domain_list_id": "rslvr-fdl-██████████"  
}
```

Resolver query logging

- Create Amazon CloudWatch Contributor Insights reports
- Track query types, rcode, query names, and more



Resolver query logging – Walkthrough

Configure query logging [Info](#)

Query logging configuration name

Name
A friendly name lets you find a Resolver query logging configuration in the dashboard.

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

Query logs destination [Info](#)
Resolver can save logs in CloudWatch Logs, in an S3 bucket, or in Kinesis Data Streams.

Destination for query logs
Choose where you want Resolver to publish query logs. Standard storage charges apply.

CloudWatch Logs log group
You can analyze logs with Logs Insights and create metrics and alarms.

S3 bucket
An S3 bucket is economical for long-term log archiving. Latency is typically higher.

Kinesis Data Firehose delivery stream
You can stream logs in real time to Elasticsearch, Redshift, or other applications.

CloudWatch Logs log groups
You can either choose a CloudWatch Logs log group that was created by the current account, or choose to create a log group for this query logging configuration.

Create log group

New log group name

VPCs to log queries for (1) – optional [Info](#)
Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.

VPC ID	VPC name	Status	IPv4 CIDR	IPv6 CIDR	Owner
vpc-	-	Active	172.31.0.0/16	-	-

Tags – optional [Info](#)
No tags associated with the resource.

Add tag
You can add up to 50 more tags.

You successfully created the log group /aws/route53/demo-query-logs.

You successfully created the query logging configuration demo-querylogs-conf.

You successfully enabled query logging for the VPC.

Route 53 > Resolver > Query logging

You are signed in to the following Region: us-east-2 (Ohio)
To change your Region, use the Region selector in the upper-right corner.

Query logging configurations (1) [Info](#)

Name	ID	Status	Destination type	Destination ARN	VPC count	Sharing status	Creation time (UTC)
demo-querylogs-conf	rqlc-	Created	CloudWatch Logs	arn:aws:logs:us-east-2:log-group:/aws/route53/demo-query-logs	1	Not shared	2021-10-10T17:12:49.702Z

Resolver query logging – Walkthrough

Route 53 > Resolver > Query logging > demo-querylogs-conf

demo-querylogs-conf Info

demo-querylogs-conf configuration

ID rqlc-bca01da3a6104edb	Status Created	Sharing status <small>Info</small> Not shared
Destination type CloudWatch Logs log group	VPC count 1	Owner
Destination ARN <small>Info</small> arn:aws:logs:us-east-2:og-group:/aws/route53/demo-query-logs	Creation time (UTC) 2021-10-10T17:12:49.702209Z	ARN arn:aws:route53resolver:us-east-2:resolver-query-log-config/rqlc-

VPCs that queries are logged for (1) Info
Resolver logs DNS queries that originate in the VPCs that you choose here. If you don't choose any VPCs, Resolver doesn't log any queries.

	View details	Stop logging queries	Add VPC	
	<input type="text" value="Search"/>			
VPC ID	VPC name	Logging status	Query logging configs	Owner
	vpc	Active	1	

Tags (0) Info

Key	Value
No tags associated with the resource.	

[Manage tags](#)

Resolver query logging – Walkthrough

```
[ec2-user@ip-172-31-15-118 ~]$ dig amazon.com
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <>> amazon.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 12380
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
;amazon.com.           IN      A

;; ANSWER SECTION:
amazon.com.        24      IN      A      205.251.242.103
amazon.com.        24      IN      A      54.239.28.85
amazon.com.        24      IN      A      176.32.103.205

;; Query time: 2 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Sun Oct 10 17:14:36 UTC 2021
;; MSG SIZE rcvd: 87

[ec2-user@ip-172-31-15-118 ~]$ 
```

The screenshot shows the AWS CloudWatch Metrics Log Events interface. It displays a single log event for a DNS query from an EC2 instance to the Amazon resolver endpoint. The log includes the query timestamp, source and destination IP addresses, port numbers, and the specific A record being resolved.

```
{ "version": "1.100000", "account_id": "REDACTED", "region": "us-east-2", "vpc_id": "vpc-c0685709", "query_timestamp": "2021-10-10T17:14:36Z", "query_name": "test.amazonaws.com.", "query_type": "A", "query_class": "IN", "rcode": "NOERROR", "answers": [ { "Rdata": "54.239.28.85", "Type": "A", "Class": "IN" }, { "Rdata": "176.32.103.205", "Type": "A", "Class": "IN" }, { "Rdata": "205.251.242.103", "Type": "A", "Class": "IN" } ], "srcaddr": "172.31.15.118", "srcport": "48292", "transport": "UDP", "srcids": { "instance": "i-0685709" } }
```

No newer events at this moment. Auto retry paused. [Resume](#)

```
[ec2-user@ip-172-31-15-118 ~]$ dig test.amazonaws.com
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <>> test.amazonaws.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NXDOMAIN, id: 52442
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 4096
;; QUESTION SECTION:
;test.amazonaws.com.           IN      A

;; AUTHORITY SECTION:
amazonaws.com.        300     IN      SOA     pdns1.ultradns.net. hostmaster.amazon.com. 2014064290 180 60 2592000 3593

;; Query time: 13 msec
;; SERVER: 172.31.0.2#53(172.31.0.2)
;; WHEN: Sun Oct 10 17:23:56 UTC 2021
;; MSG SIZE rcvd: 119

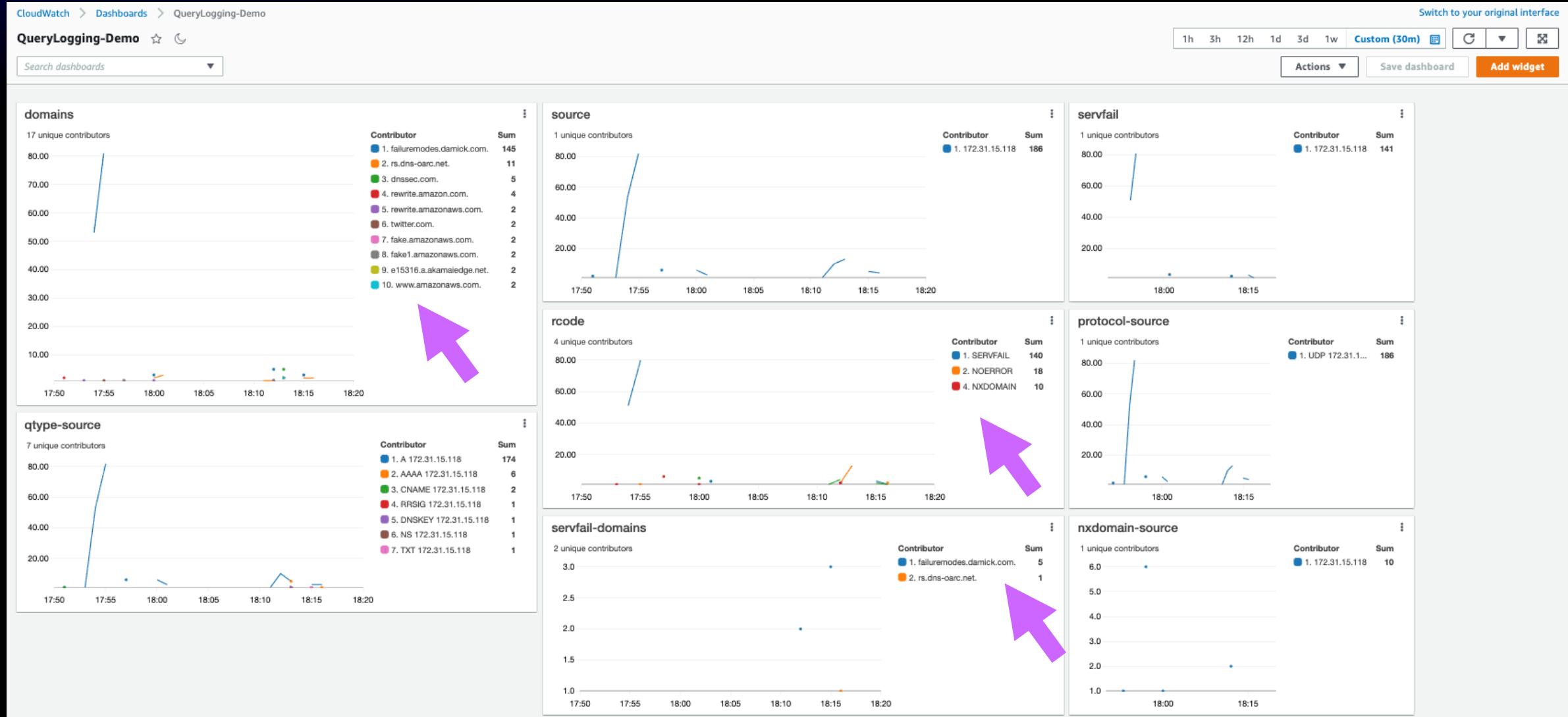
[ec2-user@ip-172-31-15-118 ~]$ 
```

The screenshot shows the AWS CloudWatch Metrics Log Events interface. It displays a single log event for a DNS query from an EC2 instance to the test.amazonaws.com resolver endpoint. The log shows the NXDOMAIN status and the authority section containing the AmazonSOA record.

```
{ "version": "1.100000", "account_id": "REDACTED", "region": "us-east-2", "vpc_id": "vpc-c0685709", "query_timestamp": "2021-10-10T17:23:56Z", "query_name": "test.amazonaws.com.", "query_type": "A", "query_class": "IN", "rcode": "NXDOMAIN", "answers": [], "srcaddr": "172.31.15.118", "srcport": "48292", "transport": "UDP", "srcids": { "instance": "i-0685709" } }
```

No newer events at this moment. Auto retry paused. [Resume](#)

Resolver query logging – Walkthrough

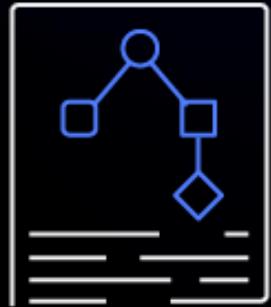


DNS Firewall – Use cases

- Protect from exfiltration
- Block unwanted site access
- Block malware domains
- Create a walled garden



DNS Firewall features



DNS filtering

- Domain name-based filtering
- Create: denylists, allowlists
- Custom deny actions
 - NXDOMAIN
 - OVERRIDE
 - NoData
- Filtering on Resolver and Resolver endpoints



Managed domain lists

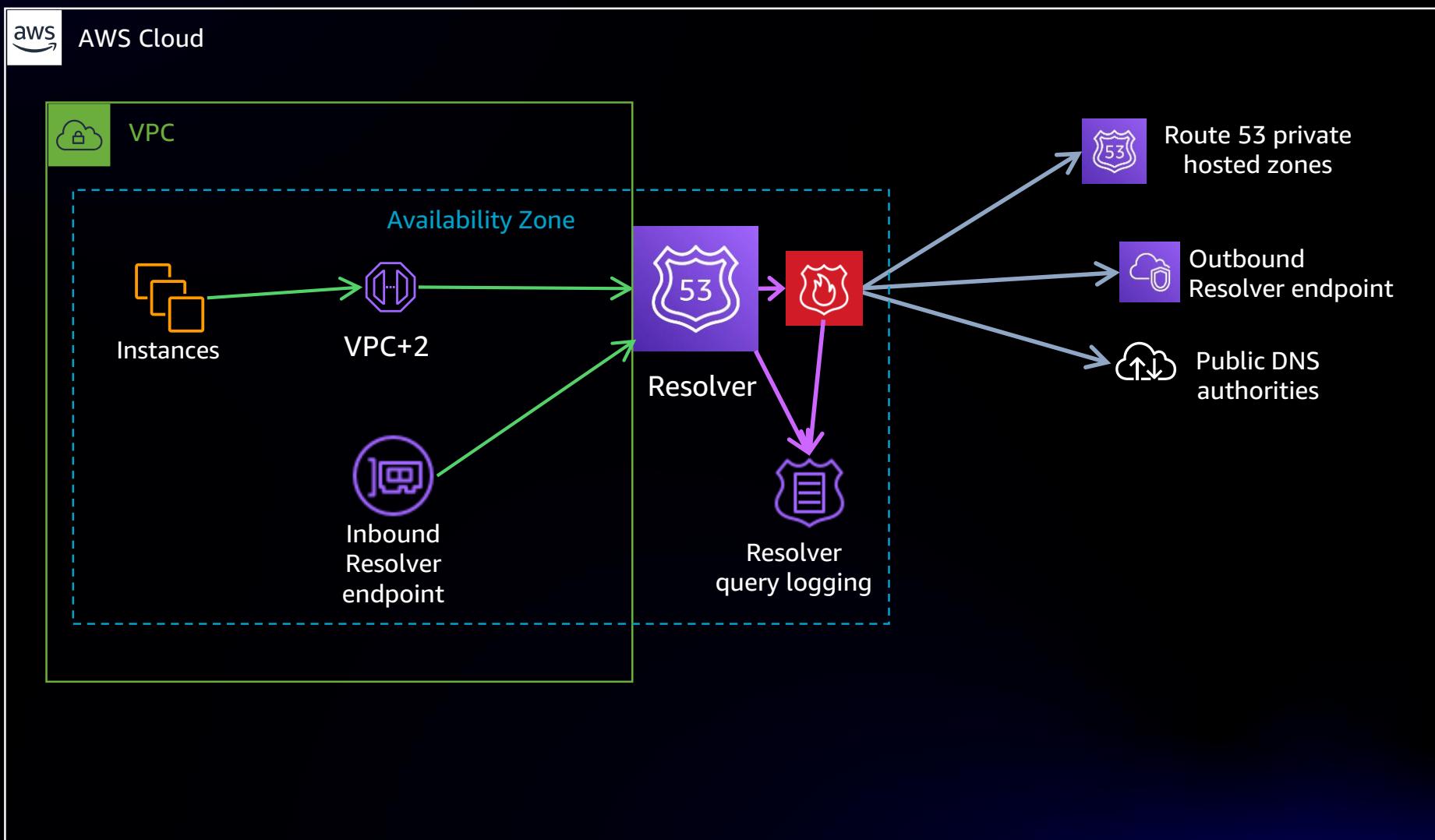
- Domain name-based lists managed by AWS
- Provide protection against
 - Malware
 - Botnet command and control (C&C)



Visibility and reporting

- Per-rule CloudWatch metrics
- Configurable logs sent to Amazon S3, CloudWatch, Kinesis (enabled by Resolver query logging)

DNS Firewall



DNS Firewall

- Create a DNS Firewall rule group
- Create or add a domain list
- Choose an action
- Associate to VPCs or use AWS Firewall Manager

The screenshot shows the configuration interface for a DNS Firewall rule group. It is divided into two main sections: 'Domain list' and 'Action'.

Domain list: This section allows you to choose a domain list. It provides two options: 'Add my own domain list' (which is unselected) and 'Add AWS managed domain list' (which is selected). A note states that you can't change the domain list of a rule after it's created. Below this is a dropdown menu labeled 'Choose a domain list' containing the option 'AWSManagedDomainsMalwareDomainList'.

Action: This section defines the action taken when a DNS query matches the rule. It starts with a dropdown 'Choose an action to take when a DNS query fits the matches' set to 'BLOCK'. Below this is a heading 'Select a response to send for the BLOCK action' with three options: 'NODATA' (selected), 'NXDOMAIN', and 'override'. Each option has a detailed description.

DNS Firewall



Amazon GuardDuty

GuardDuty provides analysis and detection by using threat intelligence feeds, signatures, anomaly detection, and machine learning



Amazon Detective

Detective makes it easy to analyze, investigate, and quickly identify the root cause of security findings or suspicious activities

DNS Firewall

Add rule group Info

A rule group is a collection of rules with actions to block or allow specific DNS queries.

Rule group details

Name

demo-fw-rulegroup

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Description - optional

Firewall Rule Group Demo

The description can have 1-256 characters.

Cancel

Next

Add rules - optional Info

Rules define how to filter DNS network traffic. They define domain names to look for and the action to take when a DNS query matches one of the names.

Rule details

Name

Firewall-Demo

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Description - optional

Demo Rule

The description can have 1-256 characters.

Domain list

Domain list

You can choose your own domain list or an AWS managed domain list. See [Amazon Route 53 DNS Firewall pricing for AWS managed domain lists](#). You can't change the domain list of a rule after you create the rule.

Add my own domain list

Use this option to create or migrate your own domain list.

Add AWS managed domain list

These are subscribed domain lists provided by Amazon.

Choose or create a new domain list

Create new domain list

Domain list name

block-list

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, -(hyphen), and _(underscore).

Switch to bulk upload

Enter one domain per line

example.com

Action

Choose an action to take when a DNS query fits the matches

BLOCK

Select a response to send for the BLOCK action

NODATA

Indicates that this query was successful, but there is no response available for the query.

NXDOMAIN

Indicates that the domain name that's in the query doesn't exist.

OVERRIDE

Provides a custom override response to the query.

Cancel

Add rule

Cancel

Previous

Next



DNS Firewall

You have successfully created rule: block-demo-1. You can now update, delete, or view settings for the rule.

Route 53 > Resolver > DNS Firewall > Rule groups > Add rule group

Step 1
Add rule group

Step 2 - optional
Add rules

Step 3 - optional
Set rule priority

Step 4 - optional
Add tags

Step 5
Review and create

Add rules - optional Info

Rules define how to filter DNS network traffic. They define domain names to look for and the action to take when a DNS query matches one of the names.

Rules

If a DNS query matches a rule, apply the rule's action to it. Rules are evaluated in order of priority, starting with the lowest setting.

<input type="checkbox"/>	Name	Action	Priority
<input type="checkbox"/>	Firewall-Demo	BLOCK	-

Cancel Previous **Next**

Review and create Info

Step 1: Add rule group Edit

Add rule group

Name	Name
Firewall-Demo	Demo Rule

Step 2 and 3: Add rules and set rule priority- optional Edit

Rule priority

Move rules up or down to change the evaluation order.

Name	Action	Priority
Firewall-Demo	BLOCK	1

Step 4: Add tags- optional Edit

tags

Key	Value
No tags	

No tags
You don't have any tags added.

Cancel Previous **Create rule group**

Rule groups (1) Info

Search

Name	ID	VPC association status	Associated VPCs	Rule group share status	Owner ID
demo-fw-rulegroup	rslvr	Not Associated	1	Not shared	

View details **Delete** **Add rule group**



DNS Firewall

Demo-fw-rulegroup [Info](#)

Demo-fw-rulegroup configuration
This rule group is managed by the AWS Firewall Manager administrator.

ID rslvr-[REDACTED]	VPC association status Associated	Region us-east-2	VPC associated count 1
Rule group share status Not shared	Owner ID [REDACTED]	Used capacity 1/100	

DNS Firewall policy

Use AWS Firewall Manager to apply this rule group to VPCs across your organization and centrally manage it from this account.

[Associate with an AWS Firewall Manager policy](#)

[Rules](#) [VPCs associated](#) [Tags](#)

Associated VPCs (1)

ID	Name	Number of associated rule groups	Association ID	Status	Associated priority	Mutation Protection	Managed owner name
vpc-[REDACTED]	rgassoc-vpc...	-	rslvr-[REDACTED]	COMPLETE	101	DISABLED	-

DNS Firewall

Rule builder

Rule details

Name: The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Description (optional): The description can have 1-256 characters.

Domain list

Domain list You can choose your own domain list or an AWS managed domain list. See Amazon Route 53 DNS Firewall pricing for AWS managed domain lists. You can't change the domain list of a rule after you create the rule.

Add my own domain list Use this option to create or migrate your own domain list.

Add AWS managed domain list These are subscribed domain lists provided by Amazon.

Choose or create a new domain list:

Domain list name: The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Switch to bulk upload

Enter one domain per line:

Action

Choose an action to take when a DNS query fits the matches:

Select a response to send for the BLOCK action:

NODATA Indicates that this query was successful, but there is no response available for the query.

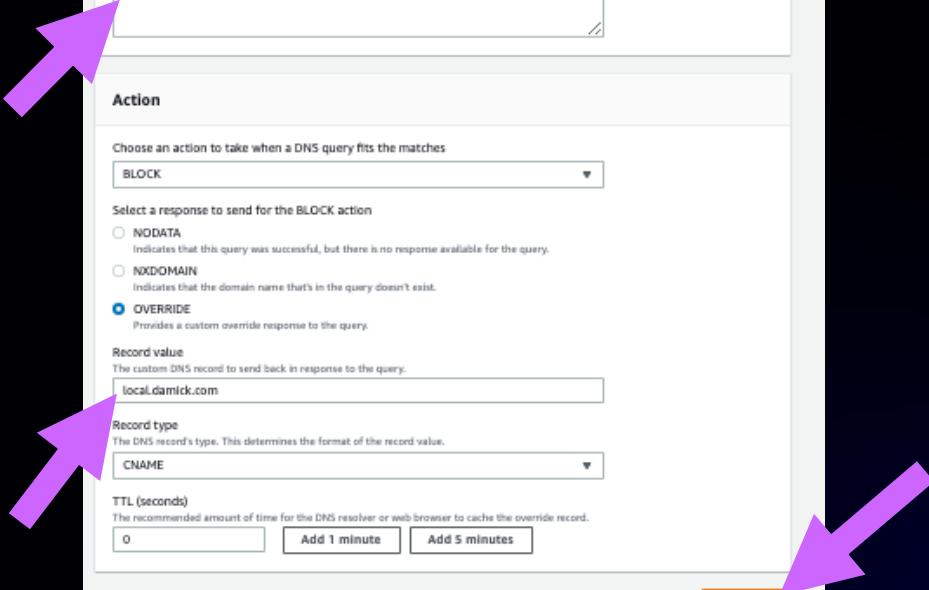
NXDOMAIN Indicates that the domain name that's in the query doesn't exist.

OVERRIDE Provides a custom override response to the query.

Record value: The custom DNS record to send back in response to the query.

Record type: The DNS record's type. This determines the format of the record value.

TTL (seconds): The recommended amount of time for the DNS resolver or web browser to cache the override record.



DNS Firewall

```
[ec2-user@ip-172-31-15-118 ~]$ dig example.com      INFO      +RipDnsForwarder  
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <>> example.com      INFO      +RipDnsForwarder  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 33728  
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 51096  
;; QUESTION SECTION:  
;example.com.          IN      A      ANSROperatorTools/ruby2.3.x/110/  
;example.com.          IN      A      ANSROperatorTools/ruby2.3.x/110/  
;; Query time: 3 msec  
;; SERVER: 172.31.0.2#53(172.31.0.2)  
;; WHEN: Thu Oct 14 18:11:30 UTC 2021  
;; MSG SIZE rcvd: 40
```

The diagram illustrates the flow of a DNS query through a system. On the left, a terminal window shows a DNS query for 'example.com' using the 'dig' command. An arrow points from this window to a central JSON object representing a firewall rule. Another arrow points from the JSON object to a second terminal window on the right.

```
{  
    "version": "1.10000",  
    "account_id": "██████████",  
    "region": "us-east-2",  
    "vpc_id": "vpc-██████████",  
    "query_timestamp": "2021-10-14T18:11:30Z",  
    "query_name": "example.com.",  
    "query_type": "A",  
    "query_class": "IN",  
    "rcode": "NXDOMAIN",  
    "answers": [],  
    "srcaddr": "172.31.15.118",  
    "srcport": "44223",  
    "transport": "UDP",  
    "srcids": {  
        "instance": "i-██████████",  
    },  
    "firewall_rule_action": "BLOCK",  
    "firewall_rule_group_id": "rslvr-",  
    "firewall_domain_list_id": "rslvr-"}  
}
```

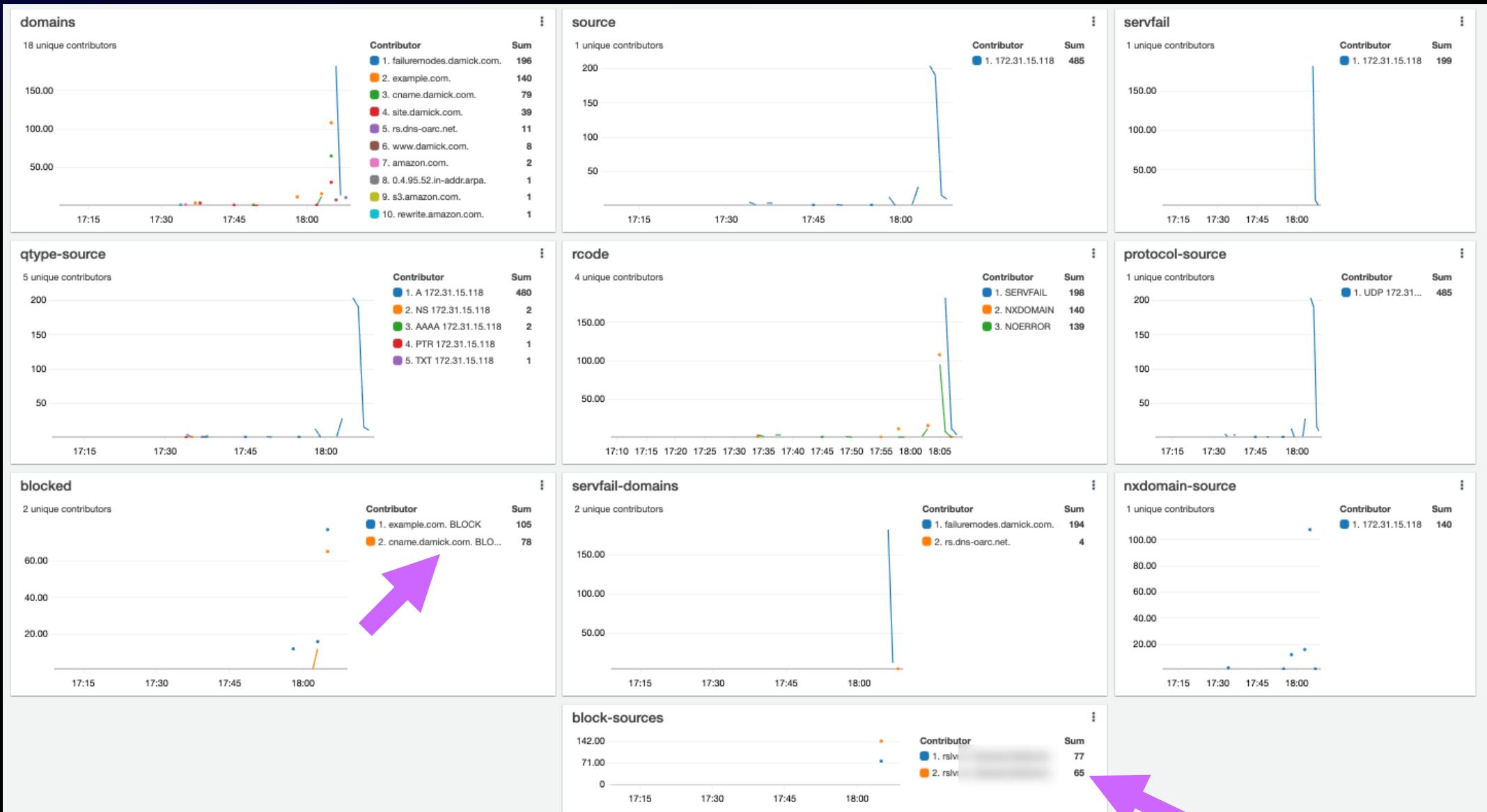
```
[ec2-user@ip-172-31-15-118 ~]$ dig @172.31.21.185 cname.damick.com  
; <>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <>> @172.31.21.185 cname.damick.com  
; (1 server found)  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7594  
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0  
;;  
;; QUESTION SECTION:  
;cname.damick.com.          IN      A  
;;  
;; ANSWER SECTION:  
cname.damick.com.      0      IN      CNAME   local.damick.com.  
local.damick.com.     300    IN      A       127.0.0.1  
;; Query time: 5 msec  
;; SERVER: 172.31.21.185#53(172.31.21.185)  
;; WHEN: Thu Oct 14 18:11:22 UTC 2021  
;; MSG SIZE rcvd: 70
```

The diagram illustrates the flow of a DNS query through a system. On the left, a terminal window shows a DNS query for 'cname.damick.com' using the 'dig' command. An arrow points from this window to a second terminal window on the right. Another arrow points from the second terminal window to a JSON object representing a firewall rule.

```
{  
    "version": "1.10000",  
    "account_id": "██████████",  
    "region": "us-east-2",  
    "vpc_id": "vpc-██████████",  
    "query_timestamp": "2021-10-14T18:11:22Z",  
    "query_name": "cname.damick.com.",  
    "query_type": "A",  
    "query_class": "IN",  
    "rcode": "NOERROR",  
    "answers": [  
        {  
            "Rdata": "local.damick.com.",  
            "Type": "CNAME",  
            "Class": "IN"  
        },  
        {  
            "Rdata": "127.0.0.1",  
            "Type": "A",  
            "Class": "IN"  
        }  
    ],  
    "srcaddr": "172.31.15.118",  
    "srcport": "47579",  
    "transport": "UDP",  
    "srcids": {  
        "resolver_endpoint": "rslvr-in-",  
        "resolver_network_interface": "eth0"  
    },  
    "firewall_rule_action": "BLOCK",  
    "firewall_rule_group_id": "rslvr-",  
    "firewall_domain_list_id": "rslvr-"}  
}
```



DNS Firewall



Agenda

Route 53 Resolver

- Forwarding rules improvements
- IPv6 resolver support
- Resolver query logs
- Resolver DNS Firewall

Route 53 DNSSEC

Route 53 Application Recovery Controller (ARC)

Route 53 DNSSEC

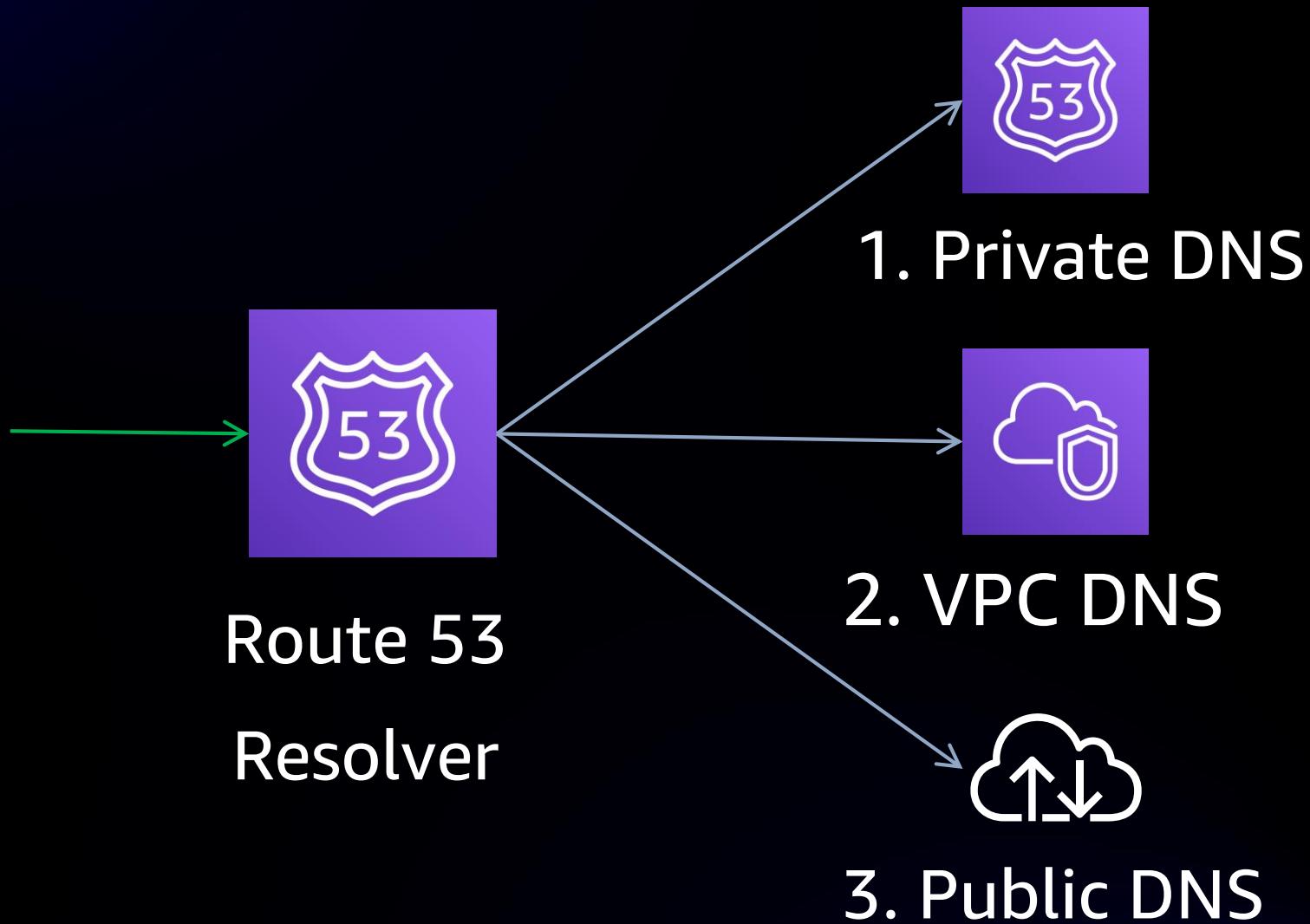


What problem does DNSSEC solve?

- You want to authenticate DNS when connecting to web services
- You want your clients to authenticate DNS connecting to your services
- Compliance
 - NIST SP 800-53 SC-21
 - SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
 - SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)
 - NOT for privacy/encryption

What is DNSSEC?

Query: www.gavinmc.com/A

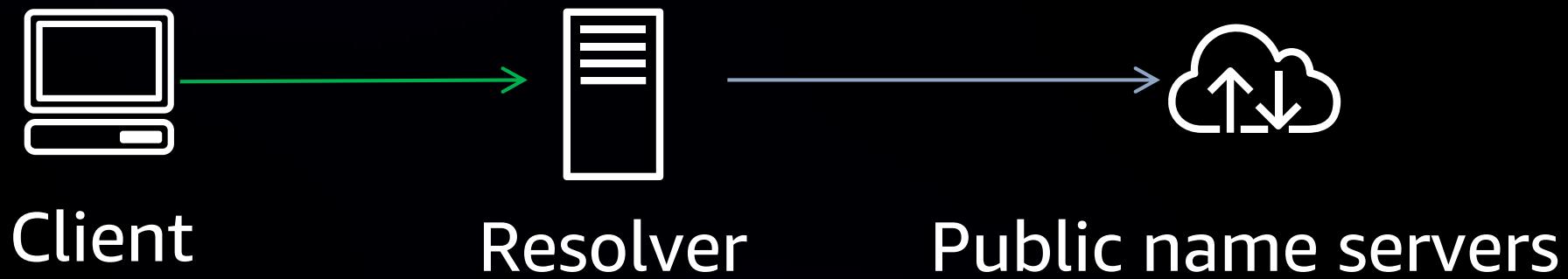


Query: www.gavinmc.com/A

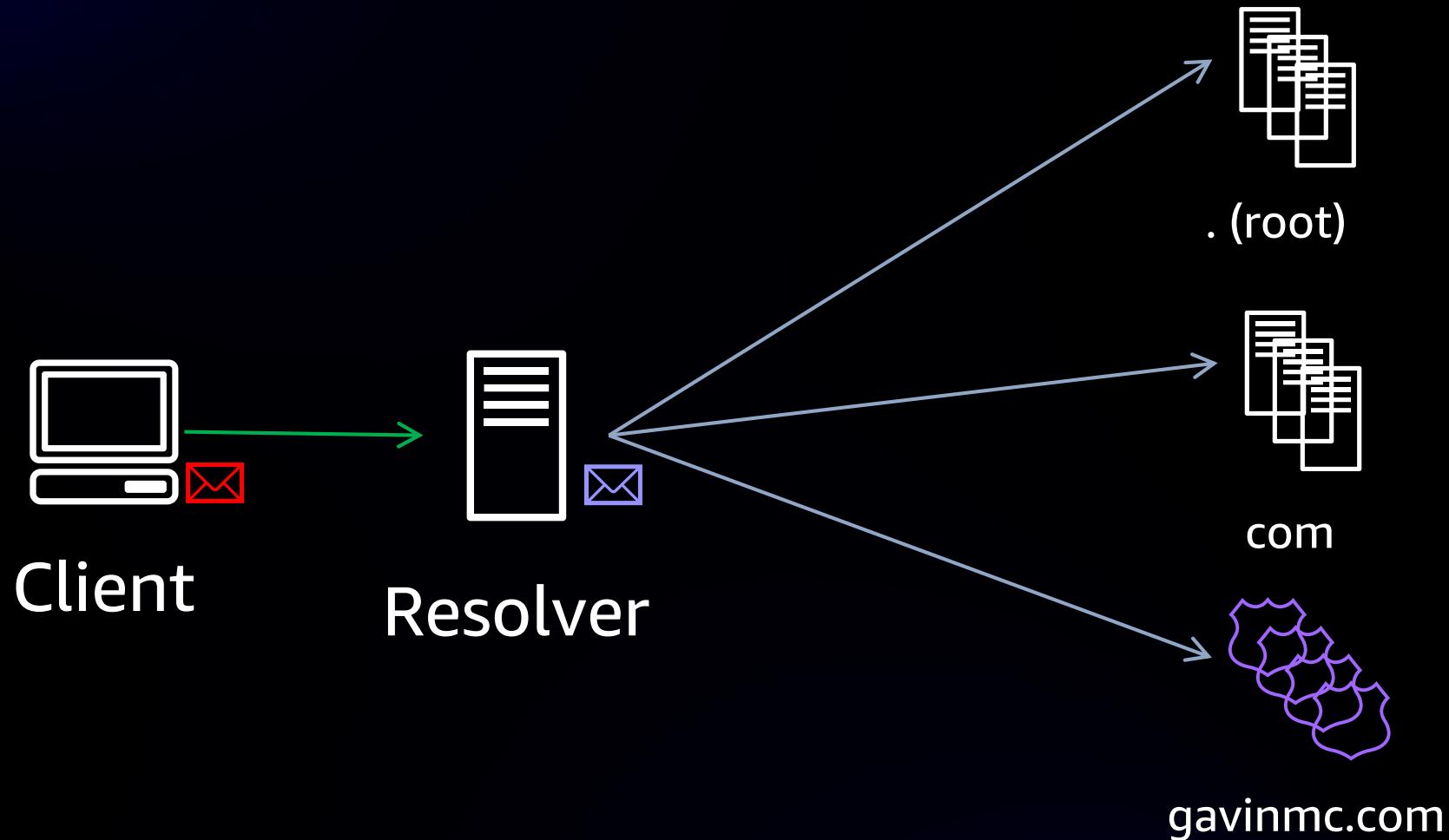


3. Public DNS

Query: www.gavinmc.com/A

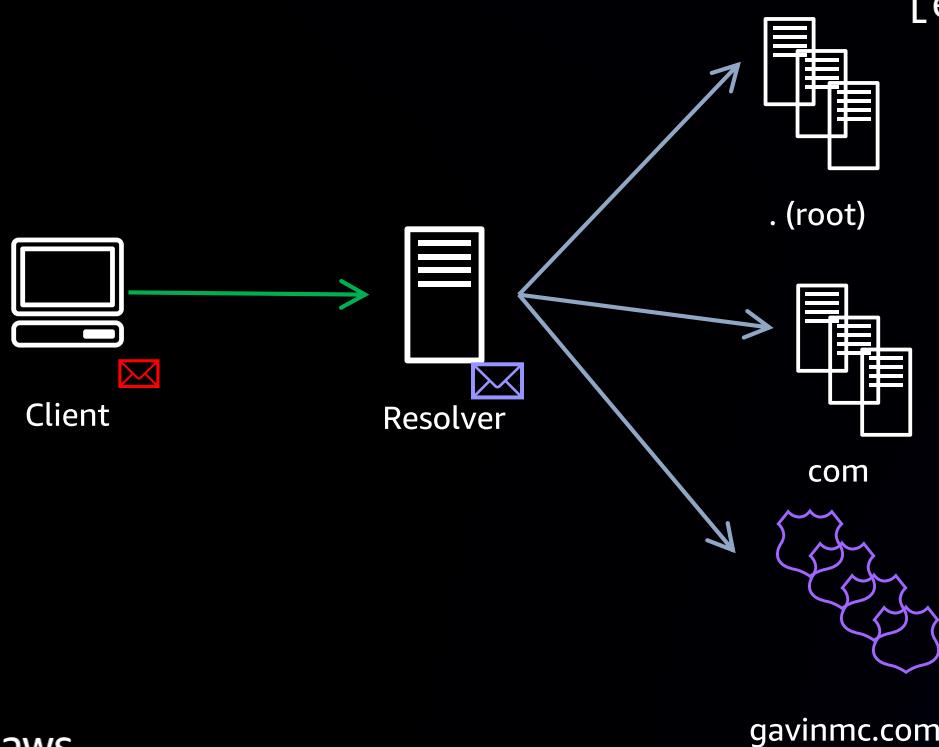


Query: www.gavinmc.com/A



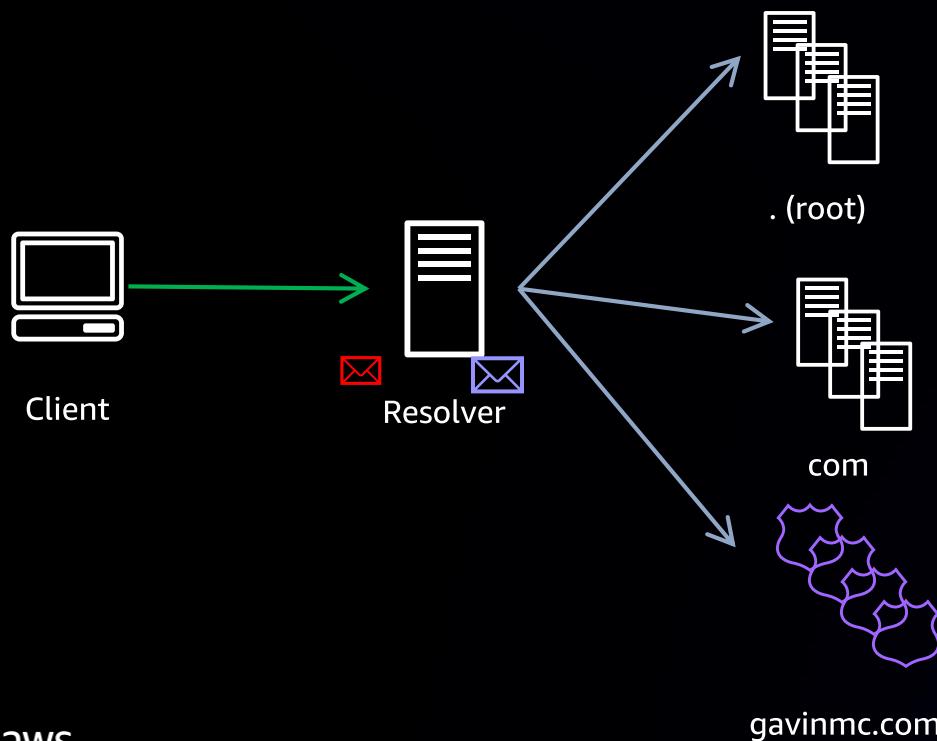
Query: www.gavinmc.com/A

```
; ; QUESTION SECTION:  
;www.gavinmc.com. IN A  
  
; ; AUTHORITY SECTION:  
com. 172800 IN NS a.gtld-servers.net.  
com. 172800 IN NS b.gtld-servers.net.  
com. 172800 IN NS c.gtld-servers.net.  
com. 172800 IN NS d.gtld-servers.net.
```



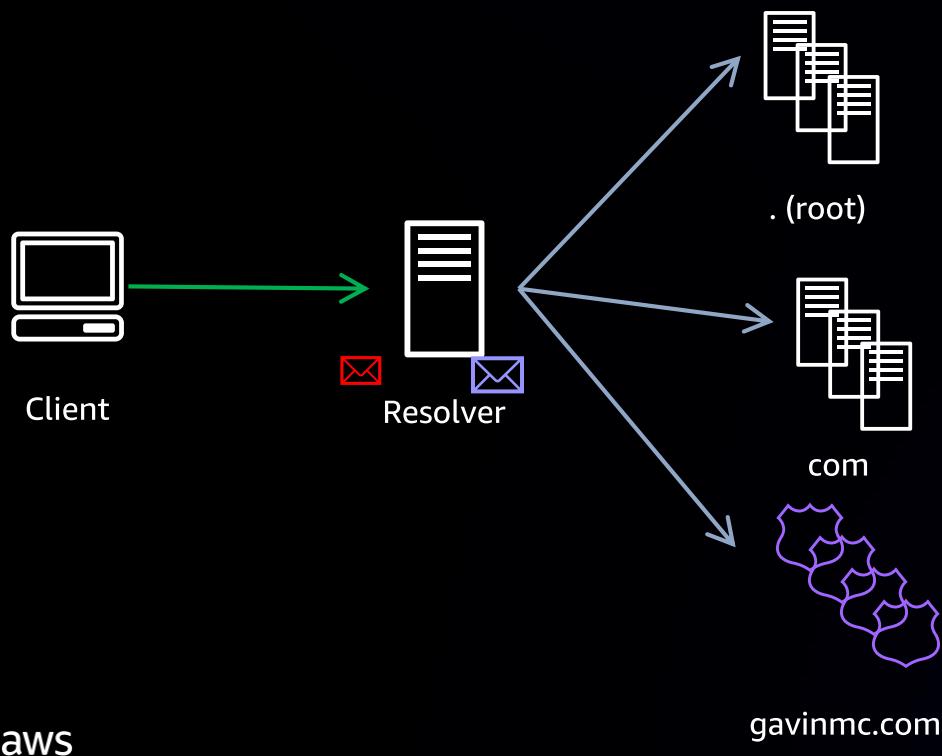
Query: www.gavinmc.com/A

```
; ; QUESTION SECTION:  
;www.gavinmc.com. IN A  
  
; ; AUTHORITY SECTION:  
gavinmc.com. 172800 IN NS ns-190.awsdns-23.com.  
gavinmc.com. 172800 IN NS ns-634.awsdns-15.net.  
gavinmc.com. 172800 IN NS ns-1084.awsdns-07.org.  
gavinmc.com. 172800 IN NS ns-1831.awsdns-36.co.uk.
```



Query: www.gavinmc.com/A

```
; ; QUESTION SECTION:  
;www.gavinmc.com. IN A  
  
; ; ANSWER SECTION:  
www.gavinmc.com. 300 IN A 2.1.1.1  
www.gavinmc.com. 300 IN A 170.1.1.1  
www.gavinmc.com. 300 IN A 4.1.1.1
```



DNS: Unencrypted, unauthenticated

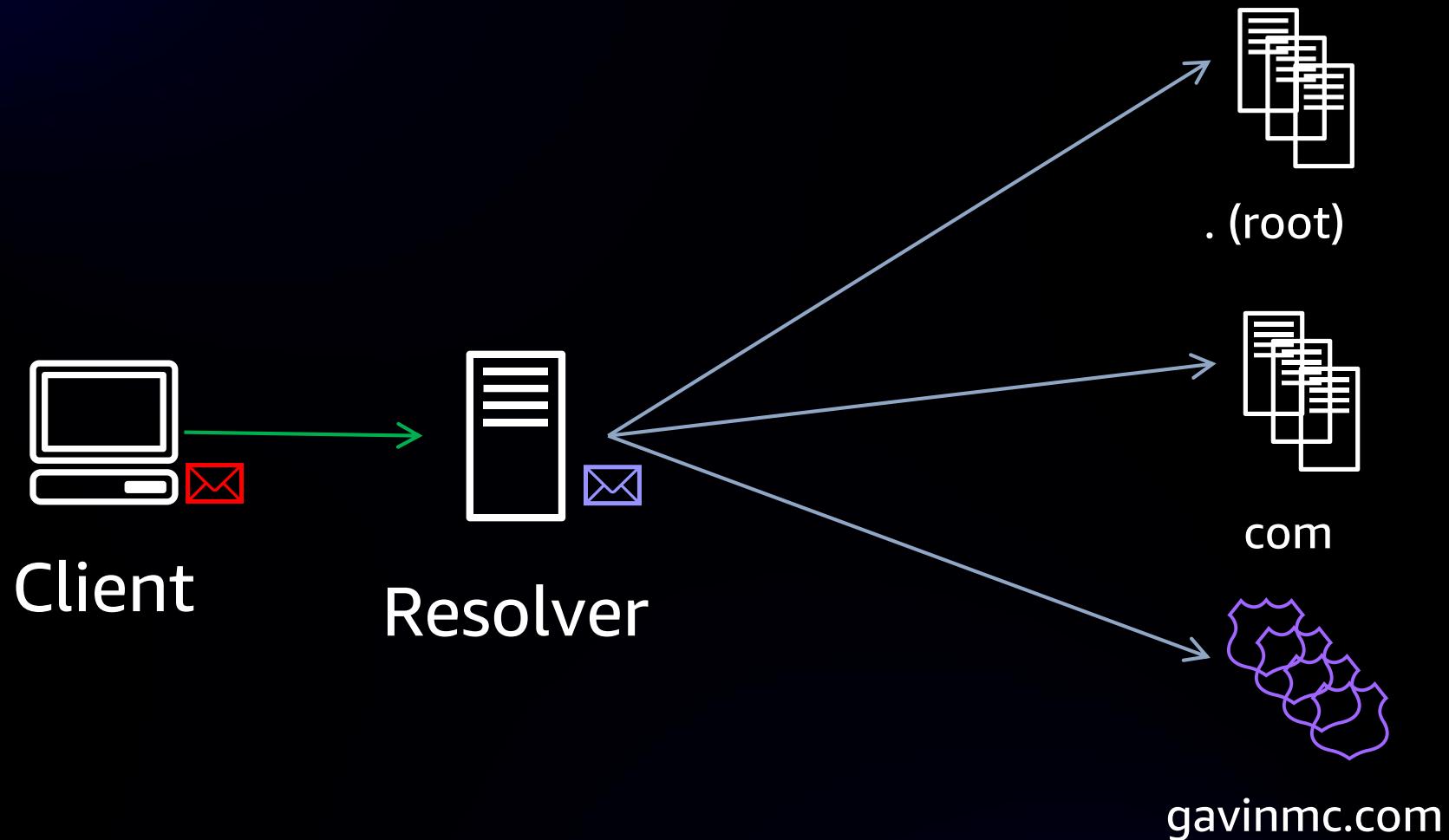
Unencrypted

- All queries between Resolver and authority are readable on the wire
- DNSSEC does **not** change this!

Unauthenticated

- DNS Resolver cannot tell if answer is authentic
- DNSSEC adds cryptographic signatures to responses for **authenticity**

Query: www.gavinmc.com/A



DNSSEC

Q: How do the Resolvers verify the answers are correct?

Authorities sign answers to Resolvers

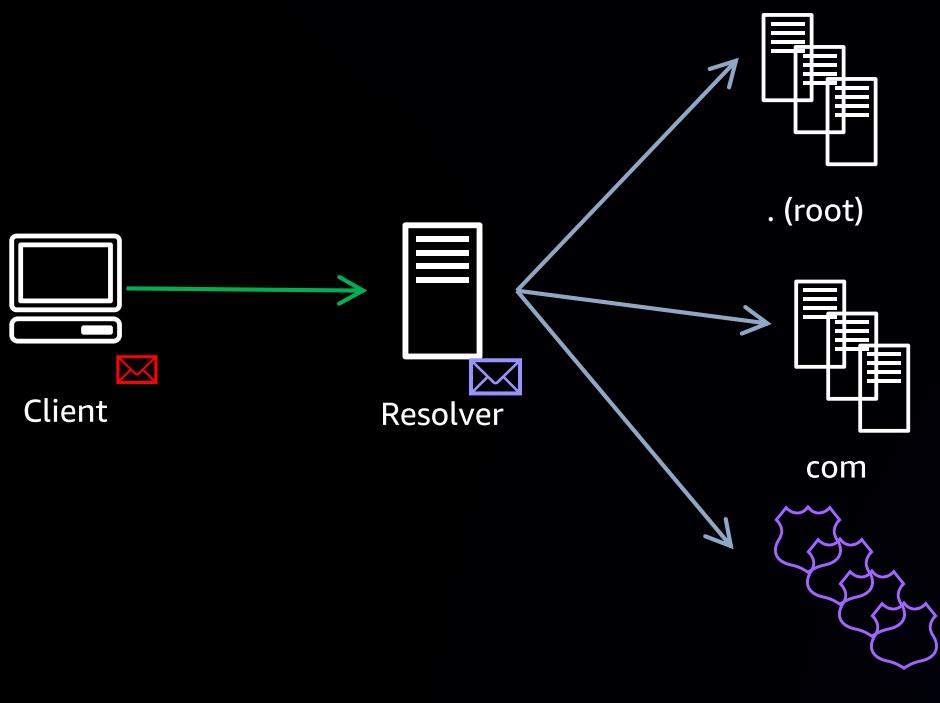
- Every zone has a zone signing key pair: **DNSKEY**
- Every delegation has a delegation signer (**DS**)
- Most record sets have a resource record set signature (**RRSIG**)

A: Resolver uses these keys and signatures to establish a chain of trust

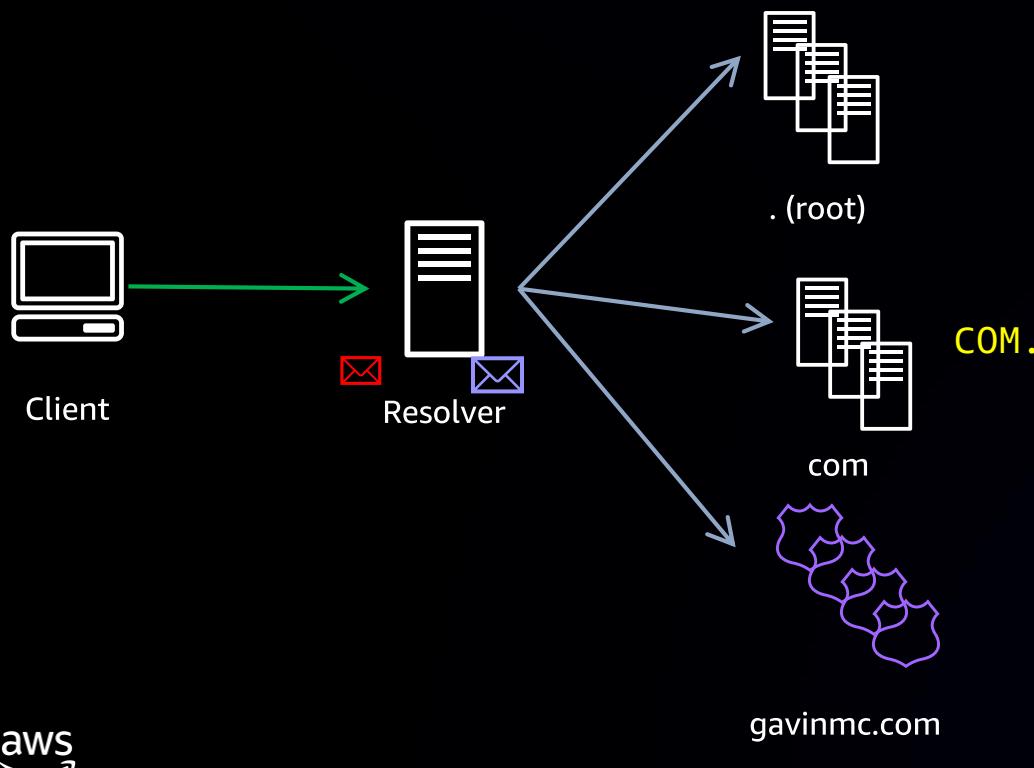
Query: www.gavinmc.com/A

```
;; QUESTION SECTION:
;www.gavinmc.com.          IN      A

;; AUTHORITY SECTION:
com.           172800  IN      NS      a.gtld-servers.net.
com.           172800  IN      NS      b.gtld-servers.net.
com.           172800  IN      NS      c.gtld-servers.net.
com.           172800  IN      NS      d.gtld-servers.net.
[etc]
com.           86400   IN      DS      30909 8 2
E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CF
C41A5766
com.           86400   IN      RRSIG   DS 8 1 86400
20211015050000 20211002040000 14748 .
IdySHCgszyXDxPxMjEuIK/z9oLeY2SFfvnWPczaff/zEf7bb1hbXXDy
SI88ZVYILET21G1/he8cqiRbVxUE7N84lathHOR7wmWJSzVZx0coaWvW
wq8wCKkKg+THHMIInySuFLh66ycUFGBp3UFMCsi51FNhavc7HZX5Bnysp
gz8fKrFEPWcVCsbqkAgCfGz8r74MI6ivtA+I16doIbGAcIqbbSjrRNC
L1YNQzmdkCaMFu8Ijwkweu4TeMW8ZH+w9NM8N2YuKJ+69hekk1gnjsu6
TP2K0z9had4EUn/sE/X/DH+uUnYJqq0j7KXXqfiuAz8eJ6InYfbbxRz6
7KL1Eg==
```



Query: www.gavinmc.com/A



```
;; QUESTION SECTION:
;com.          IN      DNSKEY

;; ANSWER SECTION:
COM.          86400   IN      DNSKEY  256 3 8
AwEAAcVw3p3LhwaxLdBQR AoXB0vo3GA3kZcycjjJ+D3QbR0DmSw+f3gz
uT1PEJYUik2dMwnkZSMqR3DPn73f7DZTVDeLte9IreZfWcp4QMMinrgF
LbvPbrK7rNKJV6j6jpjqBQ5ziwK9+yU+KX2tIU VyDjJaRR+OSi0JSMCb
khvH+5q1EsEP0GACKL70qn/ptReSr7XyTZU58dfMptMYj6n01J8=
86400   IN      DNSKEY  257 3 8
AQPDzldNmMvZFX4NcNJ0uEnKDg7tmv/F3MyQR0lpBmVcNcsIszxNFxsB
fKNW9JYCYqpik8366LE7VbIcNRzfp2h9008HR1+H+E08zauK8k7evWE
u/6od+2boggPoiEfGNyvNPaSI7FOIroDsnu/taggzHRX1Z7S0i0iPWPN
IwSUyW0Z79Vm cQ1GLkC6N1YvG3HwYmy nQv6oFwGv/KELSw7ZSdrbTQ0H
XvZbqMUI7BaMs kmvgm1G7oKZ1YiF709ioVNc0+7ASbqmZN7Z98EGU/Qh
2K/BgUe8Hs0XVcdPKrtyYnoQHd2ynKPcMM1TEih2/2HDHjRPJ2aywIpK
Nnv4oPo/
86400   IN      RRSIG    DNSKEY 8 1 86400
20211121182421 20211106181921 30909 com.
Mi80vLm2bB344kzs kEbI1AecHfYBBjwx972Qha2+3A+urXjgPA94ZvUJ
dWw+k1gl8jHZwLgK0P4UG7ChMNGIPWJyg3ZuMuZUnn/tUFQ1hfw5mDvS
Tt+Fe6vdJ 7TLDYcg9Pb+Ch0U1L1eoJVwIuU1E61f8070jIqUf27E5Uav
WAzcarnXSvbtJEDpzEurkSLeCqtZcVDpSaYtdfpZjeVzDdirASn042Wm
2xRe0k7qf2NA njkU2W4Tmyk07Q140sWKcR15GJ/UkvfqwCrJczuy5SZK
GKi21kn3HJ/2ZiUvT/5oTP Ivse2S9tmh1X4GR30h922cpJp6j1GVrpAz
ZEqJUw
```

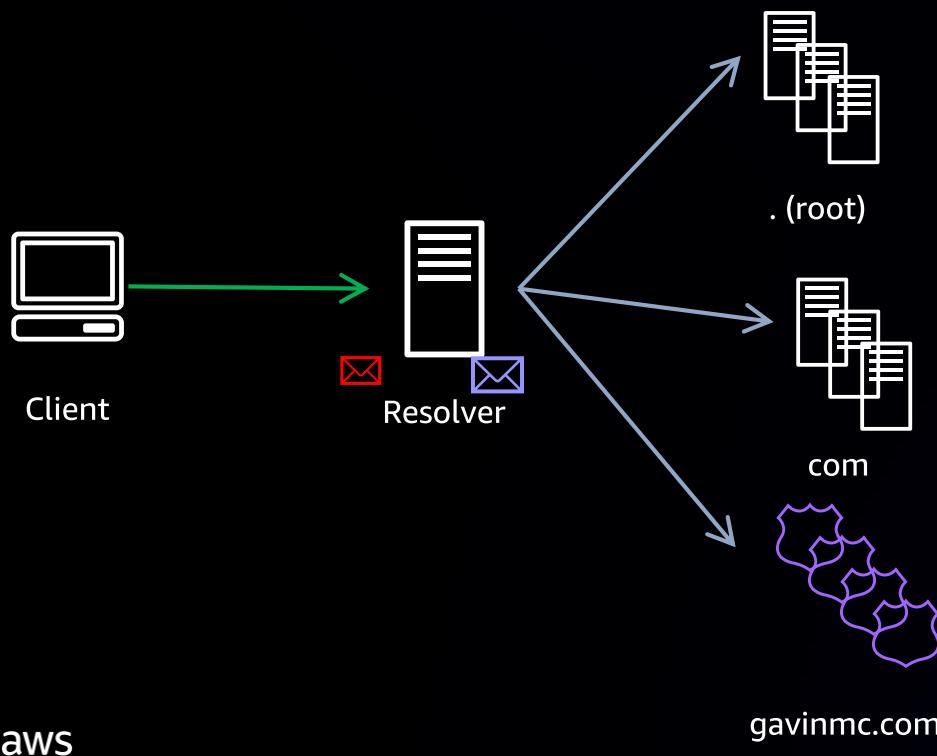
Query: www.gavinmc.com/A

; ; QUESTION SECTION:

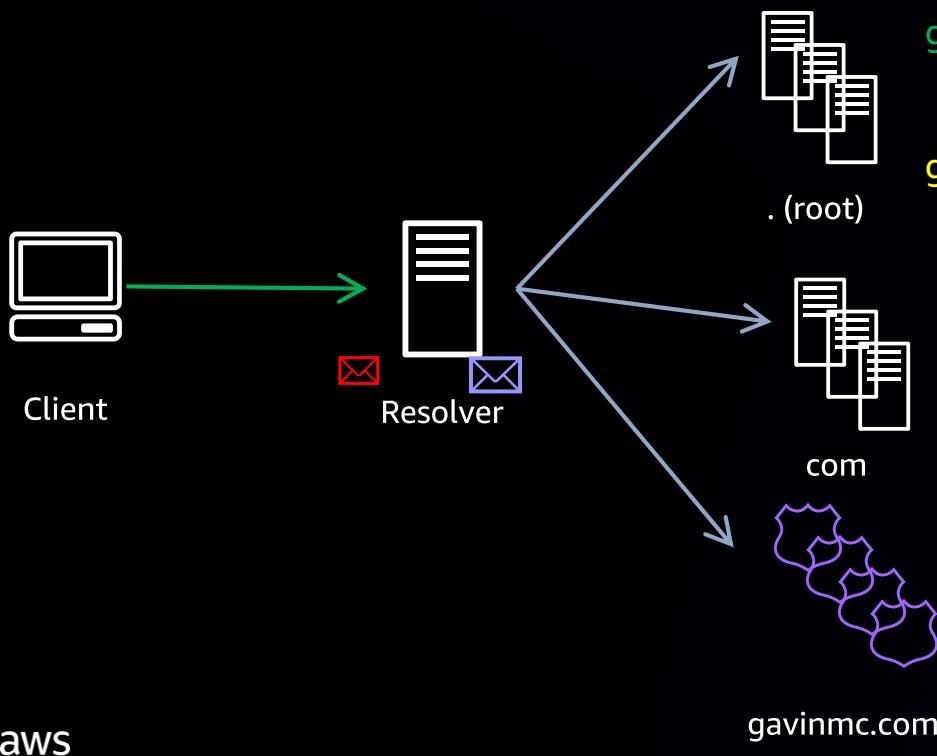
;www.gavinmc.com. IN A

; ; AUTHORITY SECTION:

gavinmc.com.	172800	IN	NS	ns-190.awsdns-23.com.
gavinmc.com.	172800	IN	NS	ns-634.awsdns-15.net.
gavinmc.com.	172800	IN	NS	ns-1084.awsdns-07.org.
gavinmc.com.	172800	IN	NS	ns-1831.awsdns-36.co.uk.
gavinmc.com.	86400	IN	DS	30454 13 2 4E6A1A3BD530207F5E83A9C8F42937EA5BCC446293E072B02FC783B6 C61EECEA
gavinmc.com.	86400	IN	RRSIG	DS 8 2 86400 202110090505 20211002035507 39343 com. jykss3qsRJ1k8PMFME/4sQK1lInp0FH059Up2o4YIfjGvFsQc8M+fWf3 9UhXy07kLUw4ofaYwzY5FXns7qBxB3W5DXWVj7voU7CYr5RvtBs2NVWY 3U1xAkVWTsJGko6IiTFgGJyi3VzfYGD3y06Rzp2U8QsPrw+21k154QUx CwEg0gq2Zi1SEGJ0TL4Bk8RPdSU70KF3GU6Rpr3lpHRUPQ==



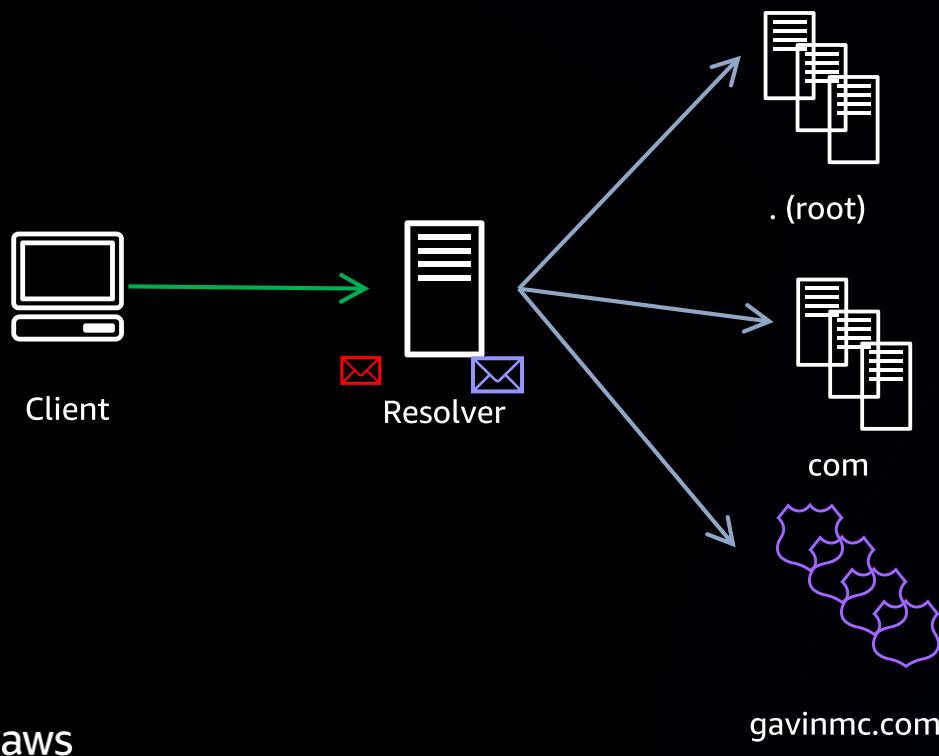
Query: www.gavinmc.com/A



```
; ; QUESTION SECTION:  
;gavinmc.com. IN DNSKEY  
  
; ; ANSWER SECTION:  
gavinmc.com. 3600 IN DNSKEY 256 3 13  
qTMInLY5MKQWaNJXqS4imCKVSPhTS18zbSLoF46w0g72fbhuBsjT5/Fg  
DPZ/X0J2YRF7FUMUBCX1Ijs9e5KagQ==  
gavinmc.com. 3600 IN DNSKEY 256 3 13  
uiJP307nLBI9mjydV0wDtr2lhvtChk/nsgvdA35PSYgy5kDTVcuj/RUu  
vM8jn4wE2UUivboNB/71PEg0fdJQow==  
gavinmc.com. 3600 IN DNSKEY 257 3 13  
zZPPc+JLlriRpycjpg0h0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUBINs  
Ed/TnnLvEZMKsqgiYPWG2RduakNEhw==  
gavinmc.com. 3600 IN RRSIG DNSKEY 13 2 3600  
2021111202000 2021111150000 30454 gavinmc.com.  
QU+0191WsP2J6nLL2aIzDaTpNqwYQ2oz+YS1Ck0RlrgVoV1RfxYkEpsF  
yVoaoNYh9v0MJreZEH+fRJ1sNTVCVw==
```

Query: www.gavinmc.com/A

```
; ; QUESTION SECTION:  
;www.gavinmc.com. IN A  
  
; ; ANSWER SECTION:  
www.gavinmc.com. 300 IN A 2.1.1.1  
www.gavinmc.com. 300 IN A 170.1.1.1  
www.gavinmc.com. 300 IN A 4.1.1.1  
www.gavinmc.com. 300 IN RRSIG A 13 3 300 20211002062859  
20211002042359 13004 gavinmc.com.  
DPWVzmwhnoEZQ0pfLQEDF300JqoItc3/Tvz6Z01UPFtg7zhI78rGW4FD  
2S+VsNxyJP59ja2VVVDrrETDHhm4rg==
```



Route 53 DNSSEC design tenets

- Make DNSSEC as safe, simple, and easy to use as possible
- Signing is automatic
- Key management is automatic
- All Route 53 features work as before
 - Weighting, MVA, geolocation, latency-based routing, traffic flow
 - Health checks, aliases
 - Query logging

Three Route 53 DNSSEC tasks

1. Enable DNSSEC validation
2. Enable DNSSEC signing
3. Disable DNSSEC signing

Three Route 53 DNSSEC tasks

1. **Enable DNSSEC validation**
2. Enable DNSSEC signing
3. Disable DNSSEC signing

Route 53 Resolver DNSSEC validation

The screenshot shows the AWS Route 53 Resolver service page. The sidebar on the left lists various options under the 'Route 53' heading, with 'Resolver' expanded to show 'VPCs' (highlighted by a purple arrow) and other options like 'Inbound endpoints', 'Outbound endpoints', 'Rules', 'Query logging', 'DNS Firewall', and 'Application Recovery Controller'. The main content area is titled 'Amazon Route 53 Resolver' and describes it as 'The DNS Resolver service for VPCs that integrates easily with DNS on your network.' Below this is a section titled 'How it works' with a diagram showing a VPC icon in the 'Region us-west-1'.



Route 53 Resolver DNSSEC validation

The screenshot shows the AWS Route 53 Resolver VPCs configuration page. On the left, a sidebar menu lists various options under the 'Resolver' section, with 'VPCs' currently selected. The main content area displays a table of VPCs. A single row is present in the table, corresponding to the selected VPC. A purple arrow points to the 'ID' column of this row, which contains the value 'vpc-ac9247c5'. Another purple arrow points to the 'DNSSEC validation' column, which shows the status 'Disabled'.

ID	Name	Rules	Outbound endpoints	Inbound endpoints	DNSSEC validation
vpc-ac9247c5	-	1	0	0	Disabled

Route 53 Resolver DNSSEC validation

The screenshot shows the AWS Route 53 Resolver configuration interface. On the left, a sidebar lists options: Resolver (VPCs, Inbound endpoints, Outbound endpoints, Rules, Query logging), DNS Firewall, and Application Recovery Controller. The main panel displays two sections: 'DNS Firewall fail open' and 'DNSSEC validation'. The 'DNS Firewall fail open' section contains a checkbox for 'Enable fail open on this VPC' which is unchecked, and a status indicator 'Disabled'. The 'DNSSEC validation' section contains a note about potential impact, a checked checkbox for 'Enable DNSSEC validation on this VPC', and a status indicator 'Enabling'. Two pink arrows point from the bottom towards the 'Enable DNSSEC validation' checkbox and its status.

DNS Firewall fail open
Indicates how Resolver should handle DNS queries when DNS Firewall is impaired or unresponsive. Enable this if you want to allow queries to go through, or disable it to block queries.

Enable fail open on this VPC
Status: Disabled

DNSSEC validation
Use DNSSEC validation to check DNSSEC cryptographic signatures to ensure that a DNS response was not tampered with.

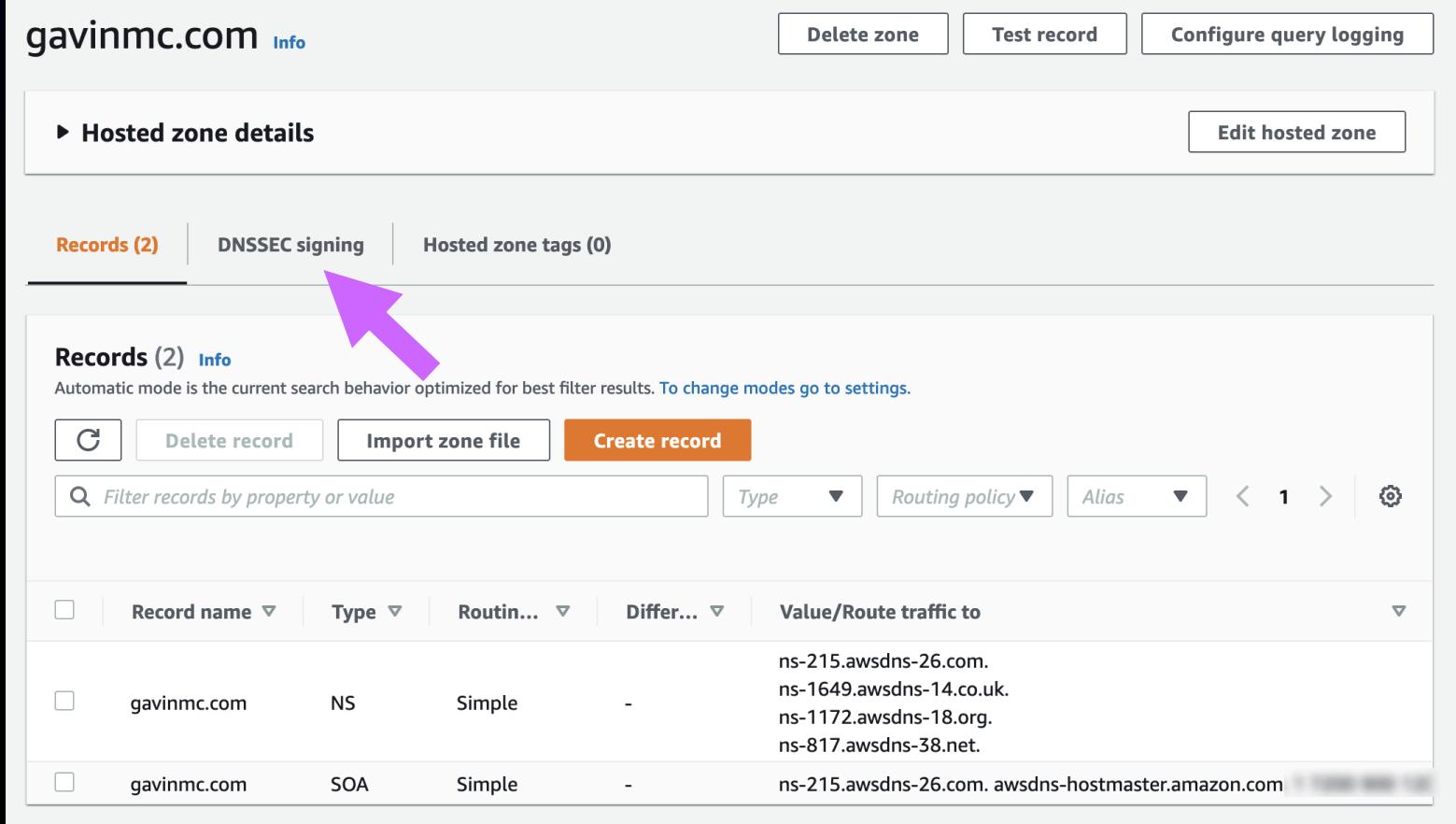
i Enabling DNSSEC validation can impact DNS resolution for public DNS records from AWS resources in a VPC, which could result in an outage. Be aware that validation can take several minutes.

Enable DNSSEC validation on this VPC
Status: Enabling

Three Route 53 DNSSEC tasks

1. Enable DNSSEC validation
2. **Enable DNSSEC signing**
 1. **Enable DNSSEC signing on the hosted zone**
 2. Wait for expiry (up to 2 days)
 3. Insert the delegation signer (DS) record at the parent zone
3. Disable DNSSEC signing

Route 53 DNSSEC signing



The screenshot shows the AWS Route 53 Hosted Zone Details page for the domain `gavinmc.com`. The top navigation bar includes options for `Delete zone`, `Test record`, and `Configure query logging`. Below this, a sub-navigation bar for the `Hosted zone details` section offers links to `Records (2)`, `DNSSEC signing` (which is highlighted with a purple arrow), and `Hosted zone tags (0)`. The main content area displays the `Records (2)` table. The table has columns for `Record name`, `Type`, `Routine...`, `Differ...`, and `Value/Route traffic to`. It lists two records: one NS record for `gavinmc.com` pointing to four AWS nameservers, and one SOA record for `gavinmc.com` pointing to `awsdns-hostmaster.amazon.com`.

<input type="checkbox"/>	Record name	Type	Routine...	Differ...	Value/Route traffic to
<input type="checkbox"/>	gavinmc.com	NS	Simple	-	ns-215.awsdns-26.com. ns-1649.awsdns-14.co.uk. ns-1172.awsdns-18.org. ns-817.awsdns-38.net.
<input type="checkbox"/>	gavinmc.com	SOA	Simple	-	ns-215.awsdns-26.com. awsdns-hostmaster.amazon.com

Route 53 DNSSEC signing

The screenshot shows the AWS Route 53 DNSSEC signing configuration page for the hosted zone `gavinmc.com`. The top navigation bar includes options like `Delete zone`, `Test record`, and `Configure query logging`. Below the navigation, there's a section titled `Hosted zone details` with a `Edit hosted zone` button. The main content area has tabs for `Records (2)`, `DNSSEC signing` (which is currently selected), and `Hosted zone tags (0)`. The `DNSSEC signing` section displays the `DNSSEC signing` status as `Not signing`. To the right of this status is a large `Enable DNSSEC signing` button, which is highlighted with a purple arrow. Below this section is a table for `Key-signing keys (KSKs) (0)`, featuring columns for `Name`, `Status`, and `Creation date`. A message at the bottom of this table states `No key-signing keys created.`

Route 53 DNSSEC signing

Enable DNSSEC signing [Info](#)

Complete the DNSSEC signing steps in order [Info](#)
If you don't complete all of the steps, or you complete them out of order, your domain might become unavailable on the internet.

Key-signing key (KSK) creation
On this page, Route 53 will create the key-signing key (KSK) for your hosted zone, based on a customer managed customer master key (CMK) that you choose.

Provide KSK name [Info](#)
Provide a name for the KSK Route 53 creates for you automatically.

The name must have 3 - 128 characters. Valid characters: A-Z, a-z, and 0-9.

Customer managed CMK in AWS KMS [Info](#)
Route 53 creates the KSK for you based on a customer managed CMK in the AWS Key Management Service (AWS KMS). It's important that you don't change permissions or other configurations for the customer managed CMK after Route 53 uses it to create the KSK.

Choose customer managed CMK

Create customer managed CMK
Additional charges apply.

Create customer managed CMK alias
Enter an alias for this key. Be aware that specific AWS KMS permissions are required to modify the key after it's created. [Learn more](#)

► Key properties

[Cancel](#) [Create KSK and enable signing](#)

Route 53 DNSSEC signing

The screenshot shows the AWS Route 53 hosted zone details for the domain `gavinmc.com`. The `DNSSEC signing` tab is selected. The status is shown as `Signing`, indicated by a green checkmark icon. A pink arrow points to this status indicator. Below the status, there is a table for `Key-signing keys (KSKs)`, showing one entry named `gavinmc.comkey` which is `Active` and was created on `October 02, 2021, 15:10 (UTC:-07:00)`.

gavinmc.com [Info](#)

Delete zone [Test record](#) [Configure query logging](#)

▶ Hosted zone details [Edit hosted zone](#)

Records (2) [DNSSEC signing](#) [Hosted zone tags \(0\)](#)

DNSSEC signing [Info](#) [View information to create DS record](#) [Disable DNSSEC signing](#)

DNSSEC signing status `Signing`

Key-signing keys (KSKs) (1) [Info](#) [View details](#) [Switch to advanced view](#)

Name	Status	Creation date
<code>gavinmc.comkey</code>	<code>Active</code>	October 02, 2021, 15:10 (UTC:-07:00)

AWS KMS key

KMS > Customer managed keys

Customer managed keys (3)

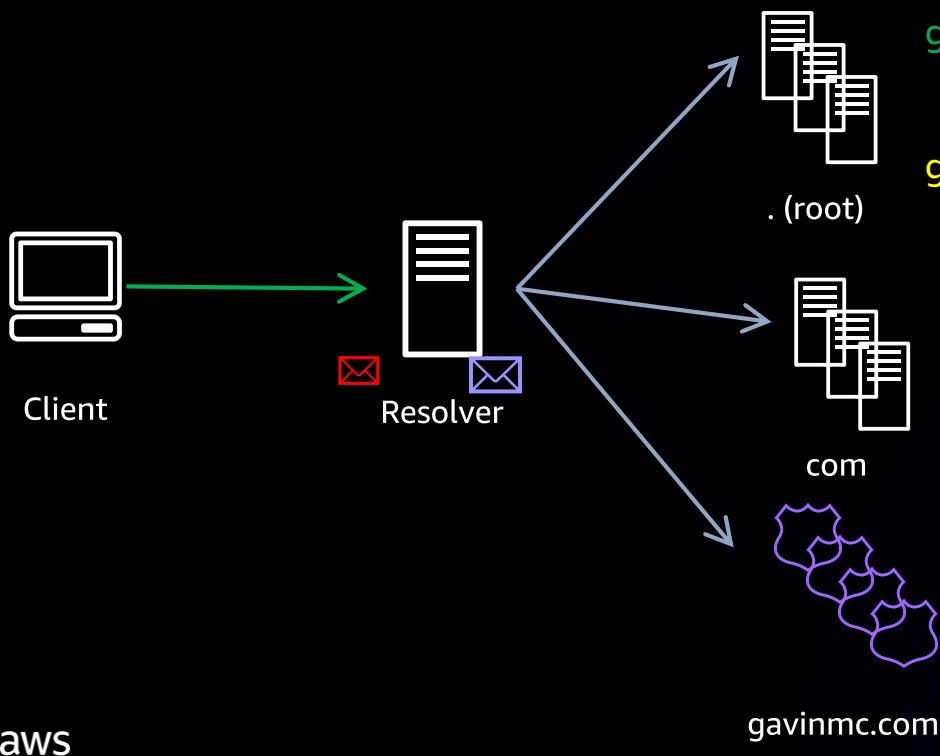
Key actions ▾ **Create key**

Filter keys by properties or tags

< 1 >

<input type="checkbox"/>	Aliases ▾	Key ID	Status	Key spec ⓘ	Key usage
<input type="checkbox"/>	gavinmc-com-ksk	4acfa04e-c7d6-4f6b-bd90-e0d2e9969c23	Enabled	ECC_NIST_P256	Sign and verify
<input type="checkbox"/>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
<input type="checkbox"/>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

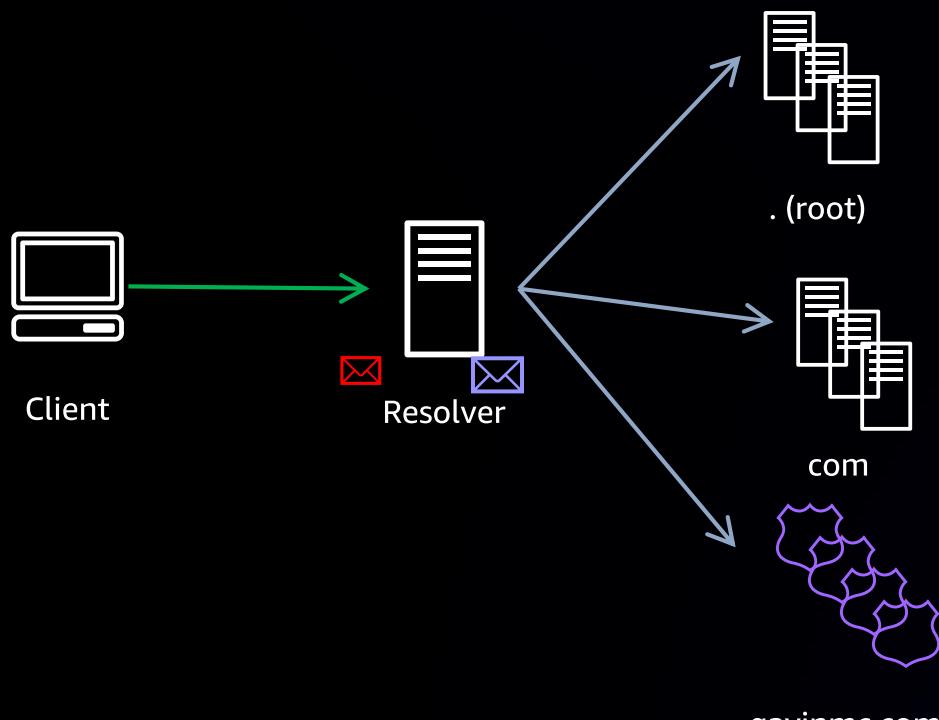
Query: www.gavinmc.com/A



```
; ; QUESTION SECTION:  
;gavinmc.com. IN DNSKEY  
  
; ; ANSWER SECTION:  
gavinmc.com. 3600 IN DNSKEY 256 3 13  
hADpPOR0q+eXTZZ86uVLJ0yUXrdSisGDFoH18eRNE25JY9dMhFDndTEx  
1QePVnLskcrqbS9RxrdTpjmX/bNLzQ==  
gavinmc.com. 3600 IN DNSKEY 256 3 13  
rwHpEFvTH/D9+yF4FPi0xn1YBZ3awZqtnpm6y9y5zoNa7oxWXqRlnfwU  
whj1T7u8Qtjo/4naYq50Y6wyYmjQvw==  
gavinmc.com. 3600 IN DNSKEY 257 3 13  
zZPPc+JLlriRpvcjPg0h0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUB1Ns  
Ed/TnnLvEZMKsqgiYPWG2RduakNEhw==  
gavinmc.com. 3600 IN RRSIG DNSKEY 13 2 3600  
2021111202000 2021111150000 30454 gavinmc.com.  
QU+0191WsP2J6nLL2aIzDaTpNqwYQ2oz+YS1Ck0RlrgVoV1RfxYkEpsF  
yVoaoNYh9v0MJreZEH+fRJ1sNTVCVw==
```

Query: www.gavinmc.com/A

```
; ; QUESTION SECTION:  
;www.gavinmc.com. IN A  
  
; ; ANSWER SECTION:  
www.gavinmc.com. 300 IN A 2.1.1.1  
www.gavinmc.com. 300 IN A 170.1.1.1  
www.gavinmc.com. 300 IN A 4.1.1.1  
www.gavinmc.com. 300 IN RRSIG A 13 3 300 20211002062859  
20211002042359 13004 gavinmc.com.  
DPWVzmwhnoEZQ0pfLQEDF300JqoItc3/Tvz6Z01UPFtg7zhI78rGW4FD  
2S+VsNxyJP59ja2VVVDrrETDHhm4rg==
```



Wait (up to 2 days!)



Three Route 53 DNSSEC tasks

1. Enable DNSSEC validation on Route 53 Resolver in my VPC
2. **Enable DNSSEC signing on my Route 53 public hosted zone**
 1. Enable DNSSEC signing on the hosted zone
 2. Wait for expiry (up to 2 days)
 3. **Insert the delegation signer (DS) record at the parent zone**
3. Disable DNSSEC signing

Insert parent DS record

The screenshot shows the AWS CloudFront Hosted Zone Details page for the domain `gavinmc.com`. The top navigation bar includes options like `Delete zone`, `Test record`, and `Configure query logging`. Below the domain name, there's a section titled `Hosted zone details` with a `Edit hosted zone` button. The main content area has tabs for `Records (2)`, `DNSSEC signing` (which is selected), and `Hosted zone tags (0)`. Under the `DNSSEC signing` tab, there are buttons for `View information to create DS record` and `Disable DNSSEC signing`. A purple arrow points to the `View information to create DS record` button. Below this, the `DNSSEC signing status` is shown as `Signing` (indicated by a green checkmark). The `Key-signing keys (KSKs) (1)` section shows one key named `gavinmc.comkey` which is `Active` (also indicated by a green checkmark). The creation date is listed as `October 02, 2021, 15:10 (UTC-07:00)`.

Insert parent DS record

gavinmccomksk

▼ Establish a chain of trust Info

To establish a chain of trust for DNSSEC, you must update the parent zone for your hosted zone with the DNSSEC information provided here. The updates that you make depend on if you use Route 53 or another registrar.

▼ Route 53 registrar

Update your parent zone using the following information.

Key type

KSK

Signing algorithm

ECDSAP256SHA256

Public key

zZPPc+JLriRpvcjpgOh0Zg0Ve57ut2z
b2yfuTbsPmHqmGeWy7hUBINsEd/TnnLvE
ZMKsqgiYPWG2RduakNEhw==

AWS KMS key

gavinmccomksk

▼ Establish a chain of trust Info

To establish a chain of trust for DNSSEC, you must update the parent zone for your hosted zone with the DNSSEC information provided here. The updates that you make depend on if you use Route 53 or another registrar.

► Route 53 registrar

Update your parent zone using the following information.

▼ Another domain registrar

Update the parent zone for your hosted zone using the following information. At some registrars, you can create a DS record with all the required values. At other registrars, you must use the other values provided.

Domain name	Digest algorithm	Signing algorithm
<input type="checkbox"/> gavinmc.com	<input type="checkbox"/> SHA-256	<input type="checkbox"/> ECDSAP256SHA256
Key tag	Digest algorithm type	Signing algorithm type
<input type="checkbox"/> 30454	<input type="checkbox"/> 2	<input type="checkbox"/> 13
Flags	Digest	Public key
<input type="checkbox"/> 257	<input type="checkbox"/> 4E6A1A3BD530207F5E83A9C8F42937EA5 BCC446293E072B02FC783B6C61EECEA	<input type="checkbox"/> zZPPc+JLlriRpycjpgOh0Zg0Ve57ut2zb2yfu TbsPmHqmGeWy7hUBINsEd/TnnLvEZMKsqqiYP WG2RduakNEhw==
		DS record
		<input type="checkbox"/> 30454 13 2 4E6A1A3BD530207F5E83A9C 8F42937EA5BCC446293E072B02FC783B6C61EE CEA

AWS KMS key

Registered domains > gavinmc.com

Edit contacts

Manage DNS

Delete domain

Domain gavinmc.com

Transfer lock

Enabled ([disable](#))

Name servers

ns-1084.awsdns-07.org

Registration date 2016-04-25

Authorization code

[Get code](#)

Expiration date 2022-04-25 ([extend](#))

Domain name status code

clientTransferProhibited

Auto renew Enabled ([disable](#))

Tag

View and manage tags for your
domains using [Tag editor](#)

DNSSEC status

Disabled

[Manage keys](#)

Registrant contact

Gavin McCullagh

gavinmc@amazon.com
+1 206 555 1234
Seattle, WA 98101
US

Administrative contact

Gavin McCullagh

gavinmc@amazon.com
+1 206 555 1234
Seattle, WA 98101
US

Technical contact

Gavin McCullagh

gavinmc@amazon.com
+1 206 555 1234
Seattle, WA 98101
US



AWS KMS key

gavinmc.com Transfer lock Enabled (Disable) Name server

Creation date 2016-04-25 Authorization code Get code

Manage DNSSEC keys X

i After you configure DNSSEC with your DNS service, add the applicable public key to the domain. [Learn more](#)

Key type 257 - KSK

Algorithm 13 - ECDSAP256SHA256

Public key zZPPc+JLlriRpycjpg0h0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUBlNsEd/TnnLvEZM
KsqgiYPWG2RduakNEhw==

Add Close

AWS KMS key

Creation date ⓘ 2016-04-25 Authorization code ⓘ Get code

Manage DNSSEC keys

Info After you configure DNSSEC with your DNS service, add the applicable public key to the domain. [Learn more](#)

Success Your request for the creation of this DNSSEC entry was successfully submitted. It will be a few minutes before the listing is updated. You will receive an email when it is done, or if further action is necessary.

Key type 257 - KSK

Algorithm 13 - ECDSAP256SHA256

Public key `zZPPc+JLlriRpycj...KsqgiYPWG2RduakNEhw==`

Add

Close

AWS KMS key

Registered domains > gavinmc.com

Edit contacts Manage DNS Delete domain

Domain	gavinmc.com	Transfer lock	Enabled (disable)	Name servers	ns-1084.awsdns-07.org ns-190.awsdns-23.com ns-634.awsdns-15.net ns-1831.awsdns-36.co.uk Add or edit name servers
Registration date	2016-04-25	Authorization code	Get code	DNSSEC status	30454 - KSK - ECDSAP256SHA256 Manage keys
Expiration date	2022-04-25 (extend)	Domain name status code	clientTransferProhibited		
Auto renew	Enabled (disable)	Tag	View and manage tags for your domains using Tag editor		

Registarant contact Gavin McCullagh

Administrative contact
Gavin McCullagh

Technical contact
Gavin McCullagh

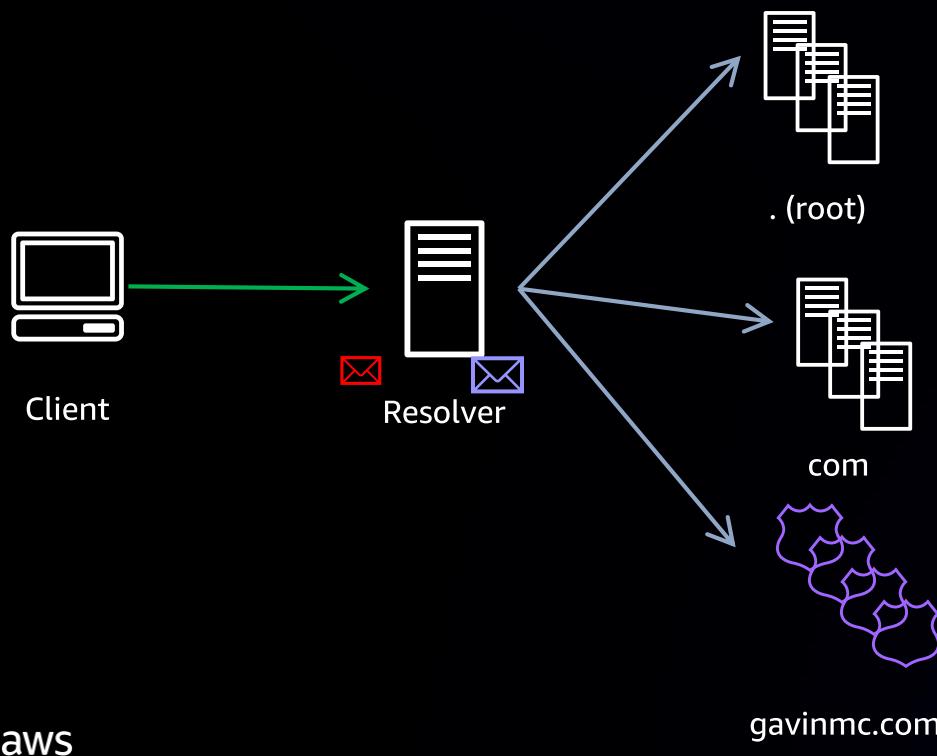
Query: www.gavinmc.com/A

; ; QUESTION SECTION:

;www.gavinmc.com. IN A

; ; AUTHORITY SECTION:

gavinmc.com.	172800	IN	NS	ns-190.awsdns-23.com.
gavinmc.com.	172800	IN	NS	ns-634.awsdns-15.net.
gavinmc.com.	172800	IN	NS	ns-1084.awsdns-07.org.
gavinmc.com.	172800	IN	NS	ns-1831.awsdns-36.co.uk.
gavinmc.com.	86400	IN	DS	30454 13 2 4E6A1A3BD530207F5E83A9C8F42937EA5BCC446293E072B02FC783B6 C61EECEA
gavinmc.com.	86400	IN	RRSIG	DS 8 2 86400 202110090505 20211002035507 39343 com. jykss3qsRJ1k8PMFME/4sQK1lInp0FH059Up2o4YIfjGvFsQc8M+fWf3 9UhXy07kLUw4ofaYwzY5FXns7qBxB3W5DXWVj7voU7CYr5RvtBs2NVWY 3U1xAkVWTsJGko6IiTFgGJyi3VzfYGD3y06Rzp2U8QsPrw+21k154QUx CwEg0gq2Zi1SEGJ0TL4Bk8RPdSU70KF3GU6Rpr3lpHRUPQ==



Three Route 53 DNSSEC tasks

1. Enable DNSSEC validation on Route 53 Resolver in my VPC
2. Enable DNSSEC signing on my Route 53 public hosted zone
3. **Disable DNSSEC signing**
 1. Remove the DS at the parent
 2. Wait for expiry (up to 2 days)
 3. Disable DNSSEC and remove keys

Remove the DS record set

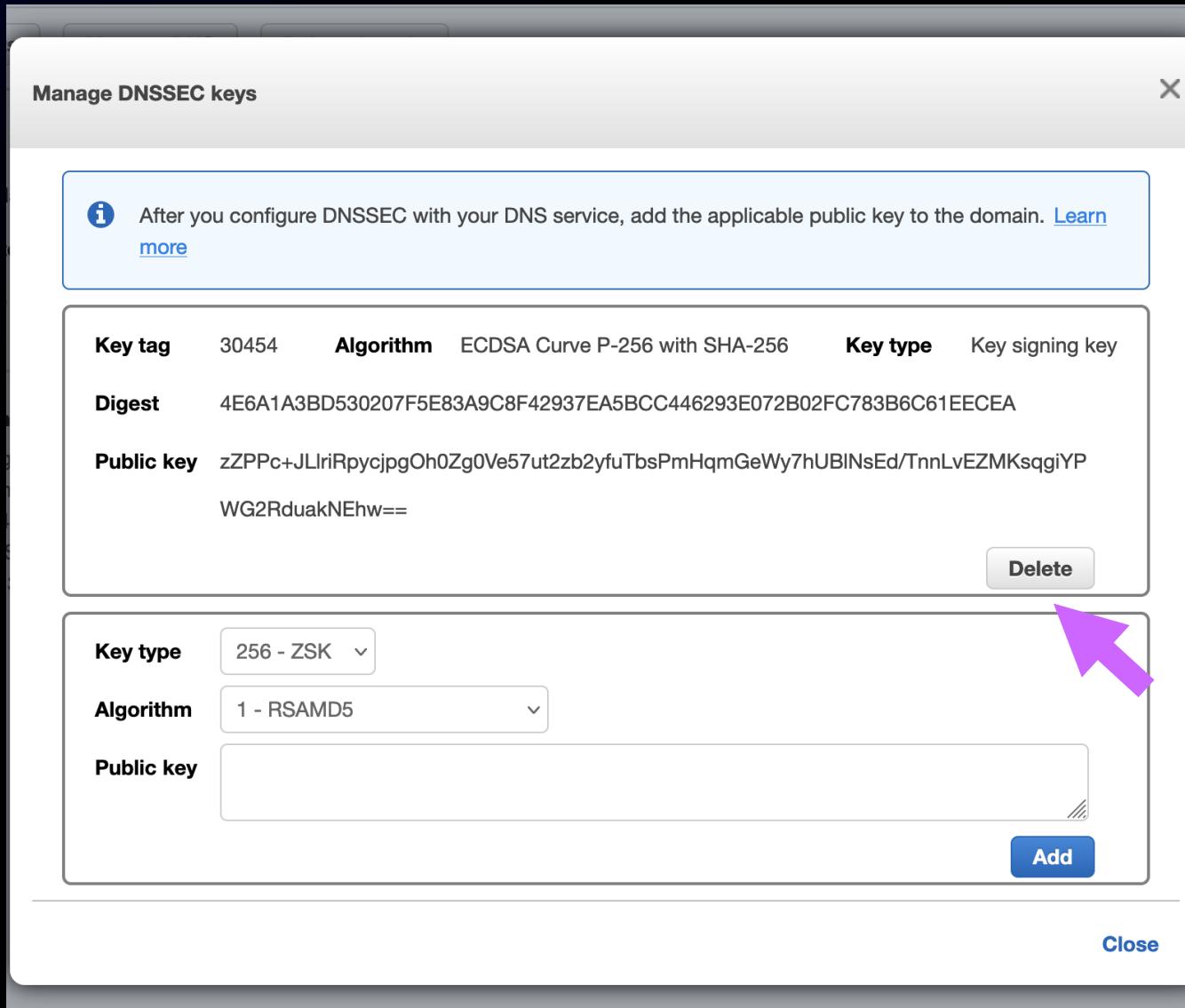
Registered domains > gavinmc.com

Edit contacts Manage DNS Delete domain

Domain	gavinmc.com	Transfer lock	Enabled (disable)	Name servers	ns-1084.awsdns-07.org ns-190.awsdns-23.com ns-634.awsdns-15.net ns-1831.awsdns-36.co.uk Add or edit name servers
Registration date	2016-04-25	Authorization code	Get code		
Expiration date	2022-04-25 (extend)	Domain name status code	clientTransferProhibited	DNSSEC status	30454 - KSK - ECDSAP256SHA256 Manage keys
Auto renew	Enabled (disable)	Tag	View and manage tags for your domains using Tag editor		
Registrant contact	Verified	Administrative contact	Gavin McCullagh	Technical contact	Gavin McCullagh



Remove the DS record set



Wait (up to 2 days!)



Disable DNSSEC

gavinmc.com [Info](#)

Delete zone [Test record](#) [Configure query logging](#)

▶ Hosted zone details [Edit hosted zone](#)

Records (2) [DNSSEC signing](#) [Hosted zone tags \(0\)](#)

DNSSEC signing [Info](#) [View information to create DS record](#) [Disable DNSSEC signing](#)

DNSSEC signing status [Signing](#)

Key-signing keys (KSKs) (1) [Info](#) [View details](#) [Switch to advanced view](#)

Name	Status	Creation date
gavinmc.comkey	<input checked="" type="checkbox"/> Active	October 02, 2021, 15:10 (UTC-07:00)

Should you enable DNSSEC?

- If you want to learn/experiment, yes!
- If you need it for compliance reasons, yes!
- Otherwise, think carefully about the tradeoffs
 - Some security benefits
 - Availability tradeoffs
 - Be aware of caching

Route 53 DNSSEC best practices

- Set a CloudWatch alarm on the signing error metric
- If you need to rotate the key-signing key, practice it on a non-production domain first
 - <https://aws.amazon.com/blogs/networking-and-content-delivery/configuring-dnssec-signing-and-validation-with-amazon-route-53/>
- You must disable DNSSEC before migrating to/from Route 53

Agenda

Route 53 Resolver

- Forwarding rules improvements
- IPv6 resolver support
- Resolver query logs
- Resolver DNS Firewall

Route 53 DNSSEC

Route 53 Application Recovery Controller (ARC)

Route 53 Application Recovery Controller (ARC)



Application Recovery Controller

- Extremely reliable applications (for example, < 5 mins interruption per year)
- Failure minutes = number of failures * minutes per failure
- Availability = MTBF * MTTR
- Availability ~ Prevention * recovery time

Recovery Oriented Computing



Recovery Oriented Computing

- *Recovery Oriented Computing (ROC): Motivation, Definition, Techniques, and Case Studies*
 - David Patterson et al., 2002
 - http://roc.cs.berkeley.edu/papers/ROC_TR02-1175.pdf
- Failures are inevitable
 - Plan and design for them
 - Have a means to recover

Recovery Oriented Computing

Key system design ideas

- Redundant, isolated units
- Tested recovery mechanisms

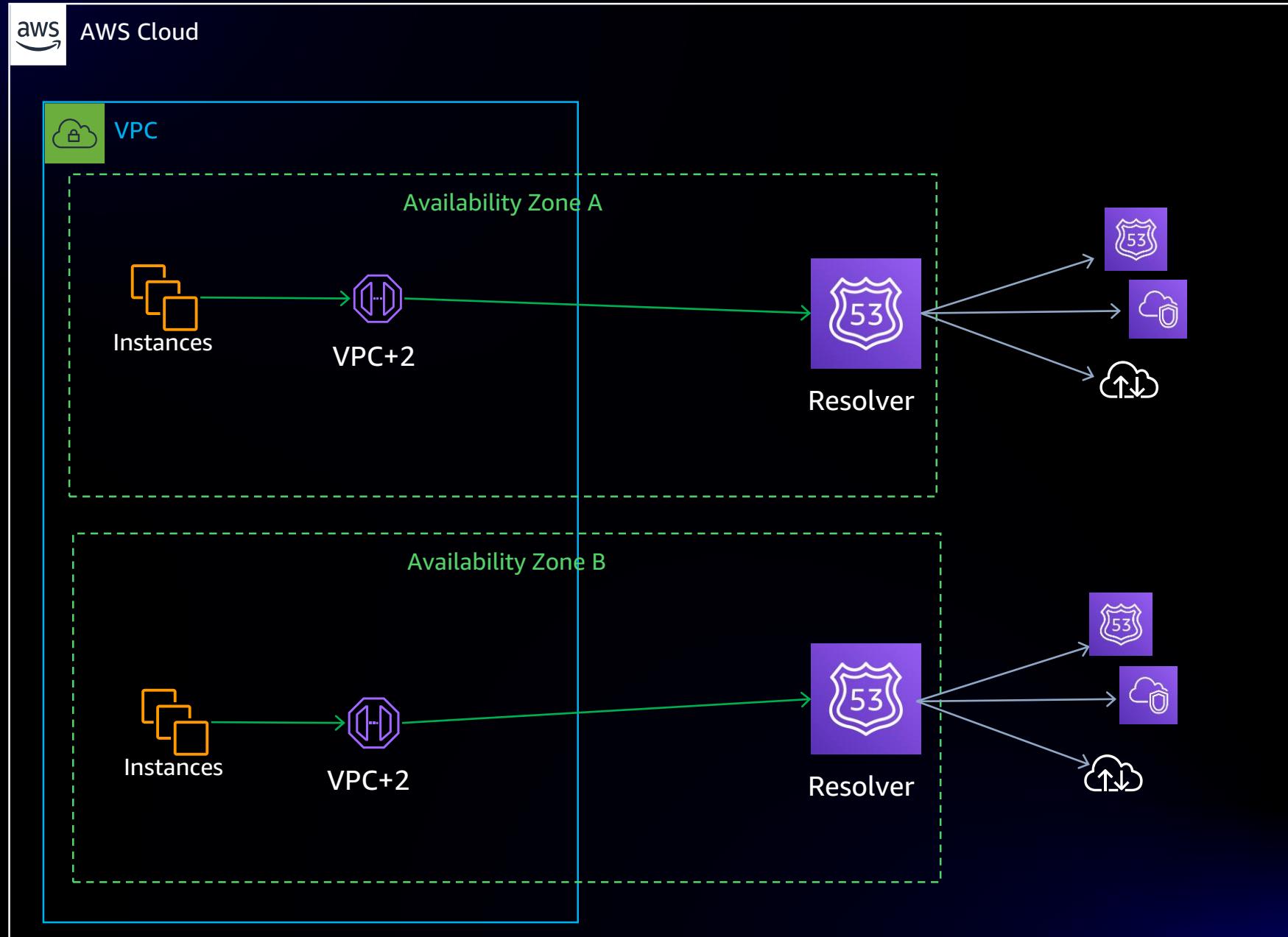
Hugely influential on Amazon and AWS

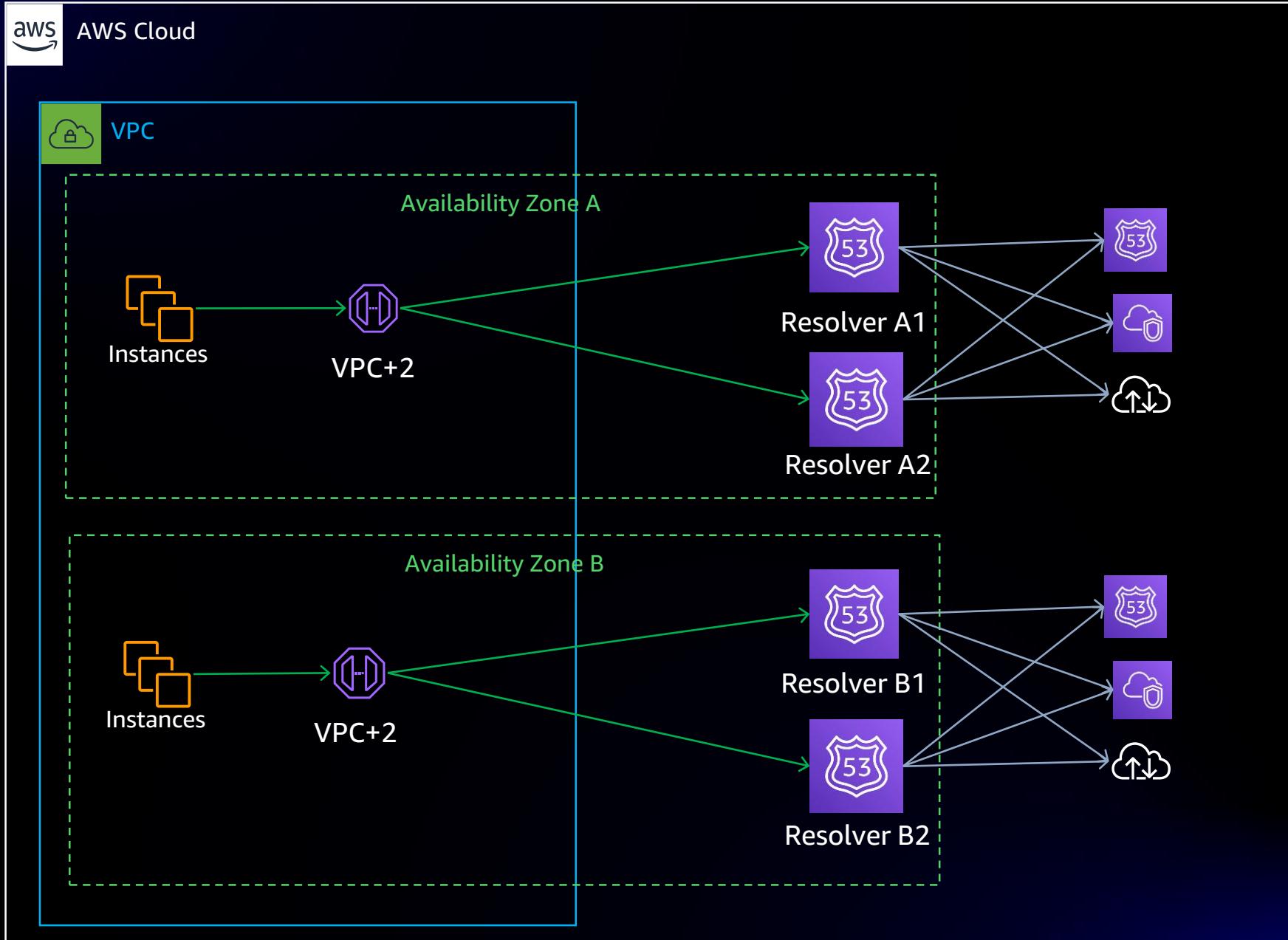
Ensuring you can recover

1. Build redundant replicas of your application
2. Ensure all replicas are always ready
3. Minimize shared fate
4. When one replica fails, recover quickly by removing it

Example #1

Route 53 Resolver



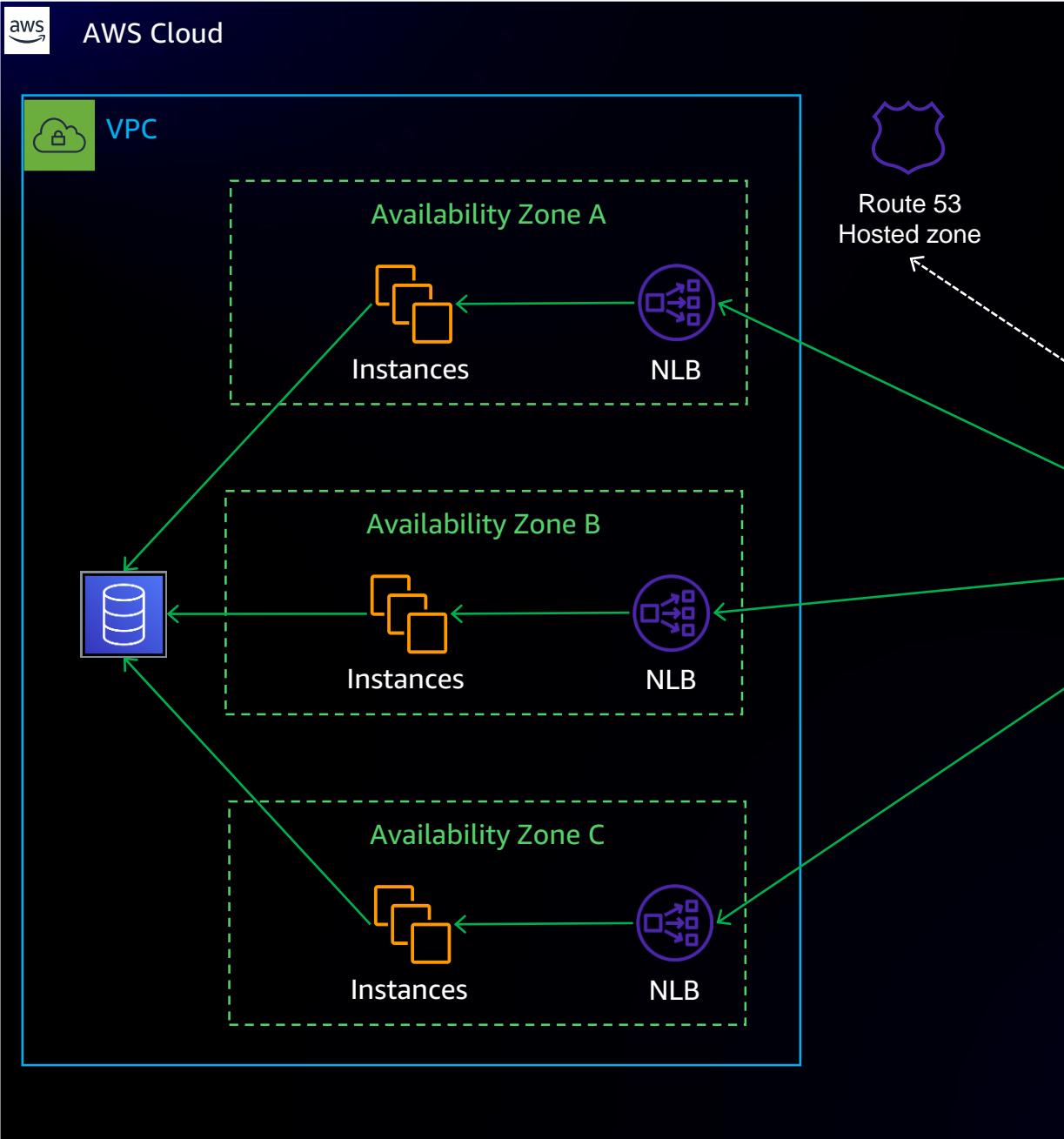


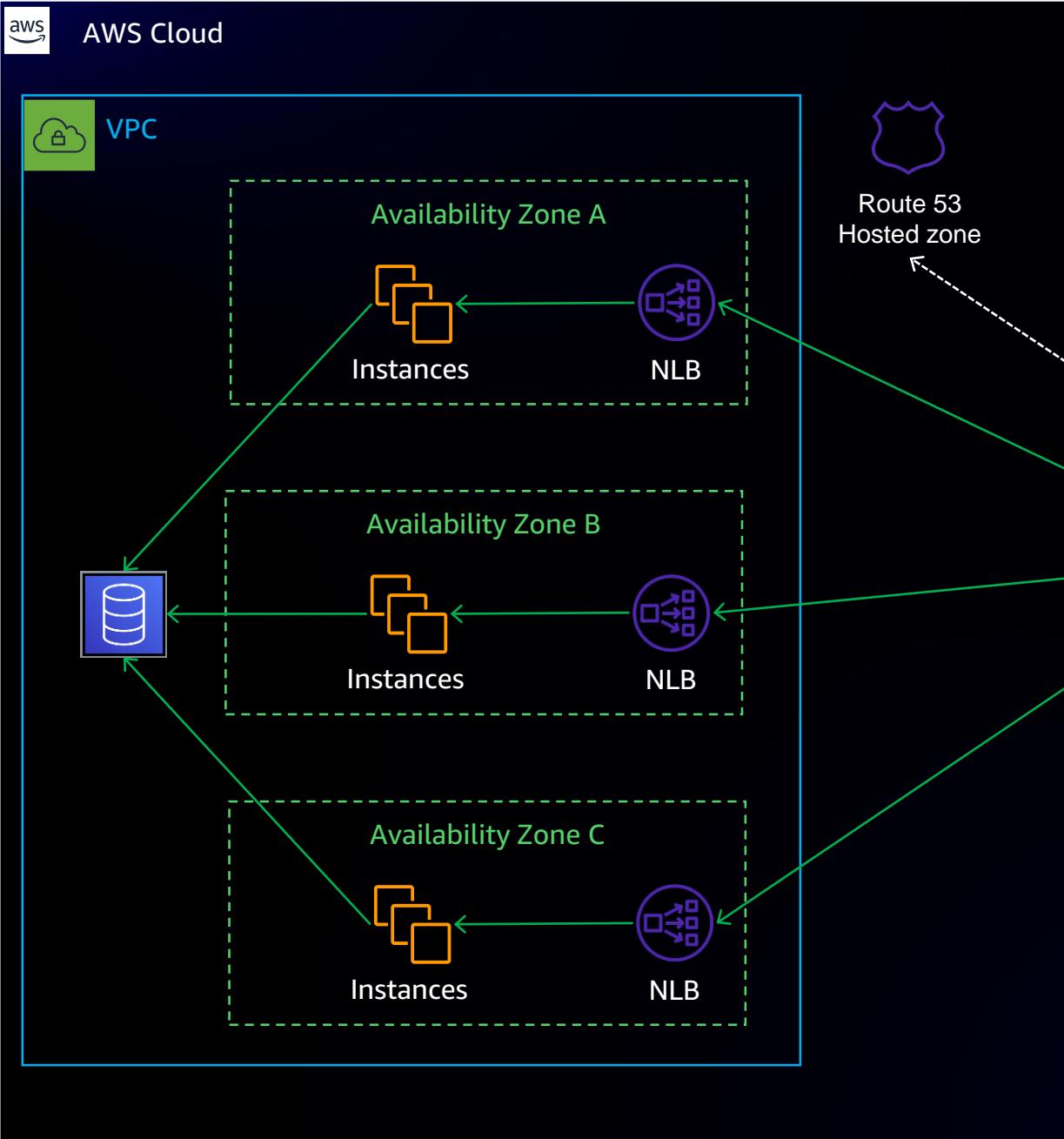
Example #2

3-AZ Web Service

Building a fault tolerant web service







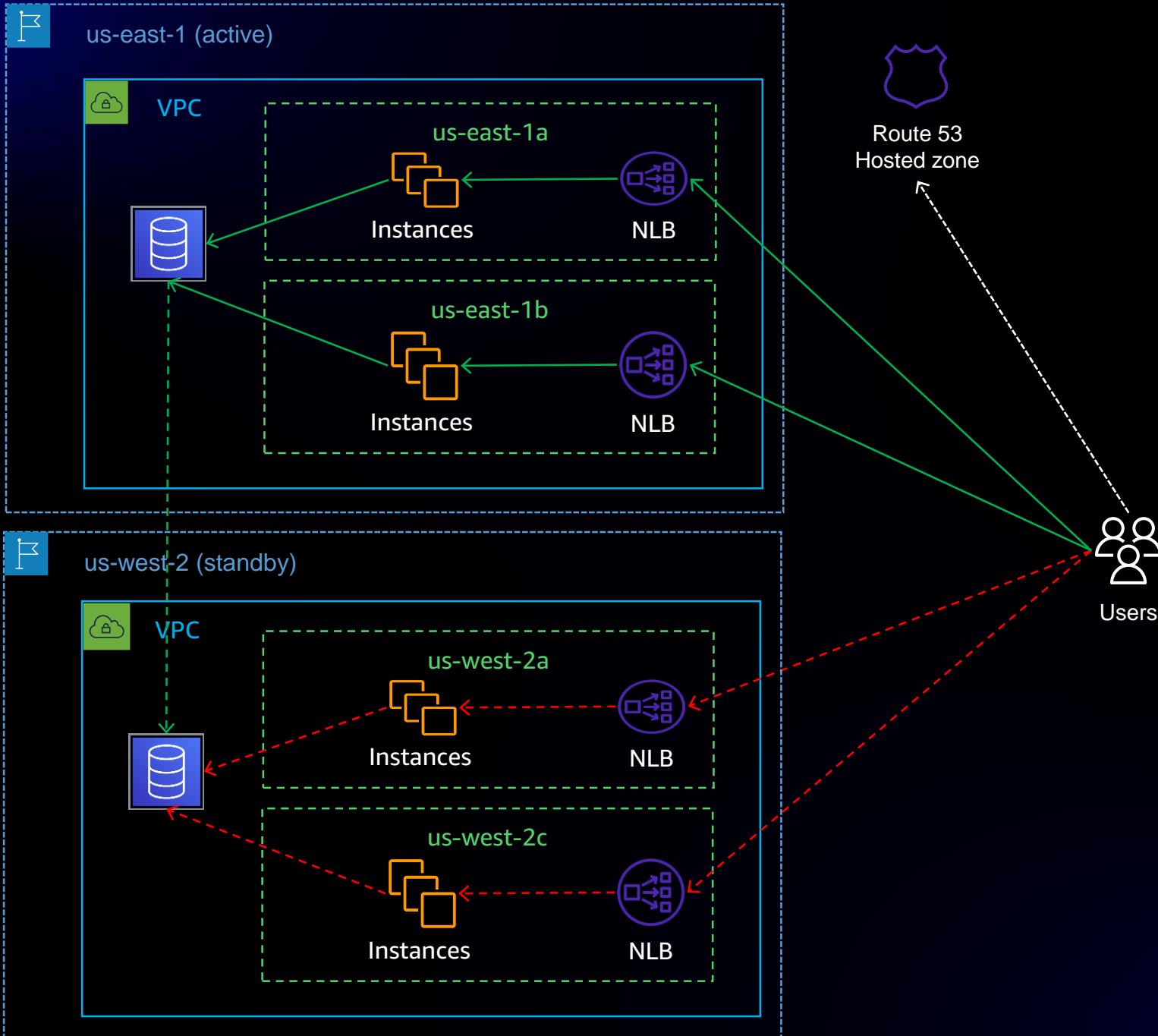
- Active-active setup
- What recovery mechanisms do we use if AZ B is failing?
- How do we make sure only one AZ is removed at a time?

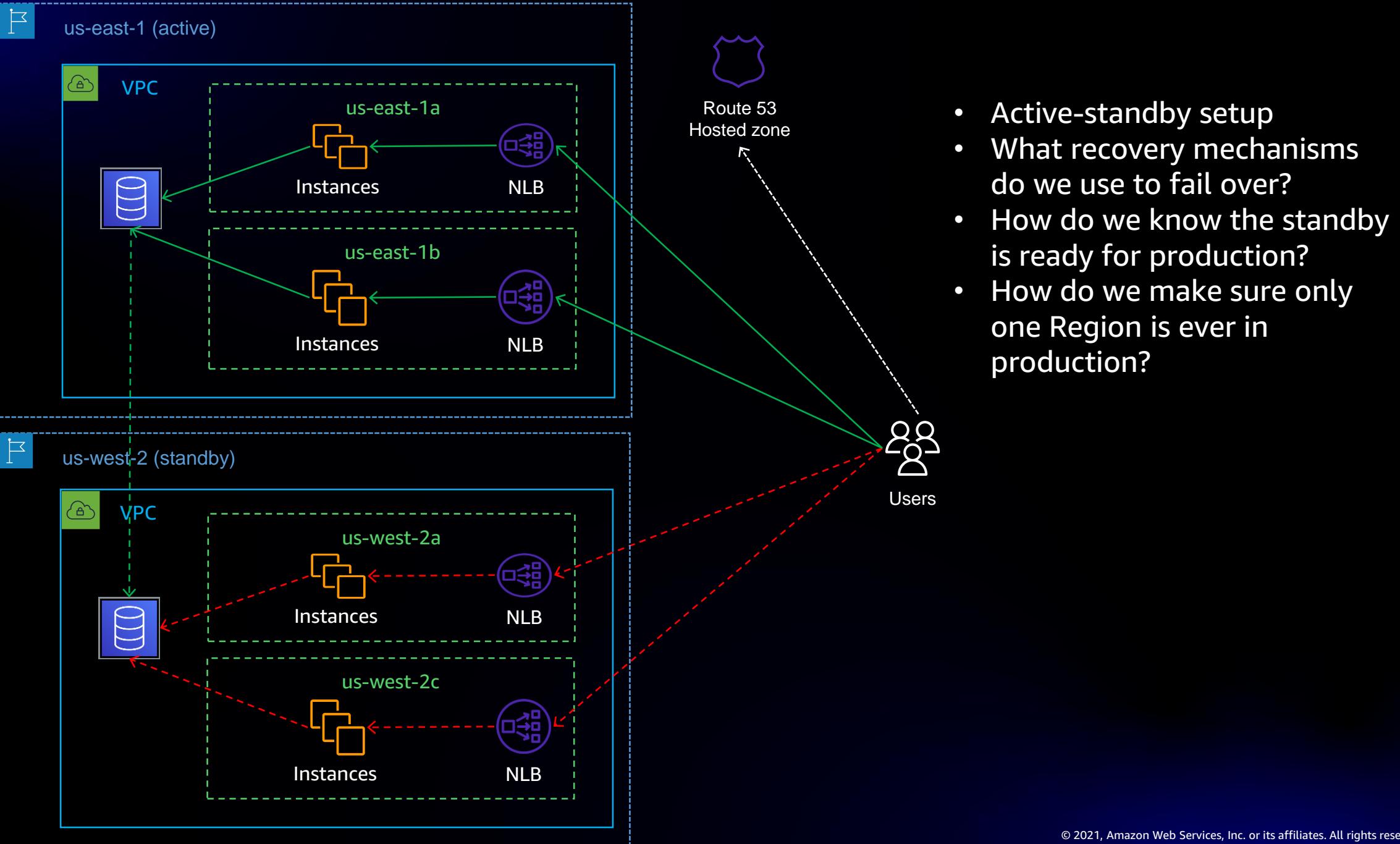
Example #3

Web service with multi-Region DR

A web service that can recover from
major natural disasters, for example







Route 53 Application Recovery Controller (ARC)



Application Recovery Controller features

Now we have multiple replicas

- How do we know we are ready to take a replica out?
- What recovery mechanism do we use?
- How do we make sure failover is safe?

Application Recovery Controller features

Now we have multiple replicas

- **How do we know we are ready to take a replica out?**
- What recovery mechanism do we use?
- How do we make sure failover is safe?

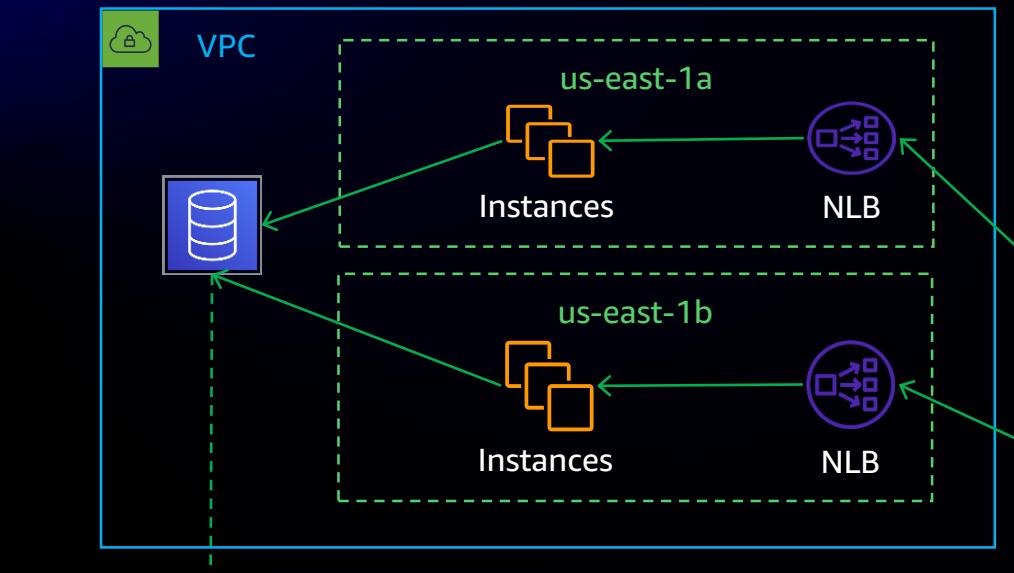
Readiness checks

Recovery Group

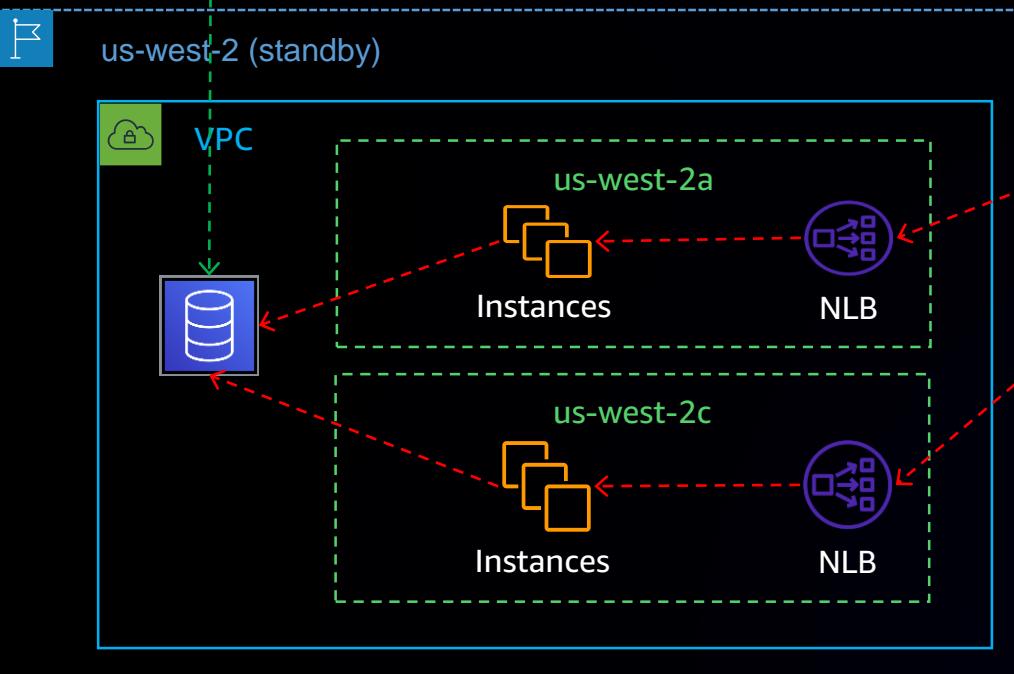
Assessment Criteria	Cell 1: Primary Region	Cell 2 : Standby Region
Provisioned Capacity	-	 Capacity is underscaled by 30 C4 instance; 500 RCU and 800 WCU
Resource Limits	-	 Amazon DynamoDB read throughput limits not matched; remediation in progress
Replication latency	-	 RPO>30 seconds
Custom Readiness checks	<Custom CloudWatch alarm>	<Custom CloudWatch alarm>



us-east-1 (active)



us-west-2 (standby)



Route 53
Hosted zone

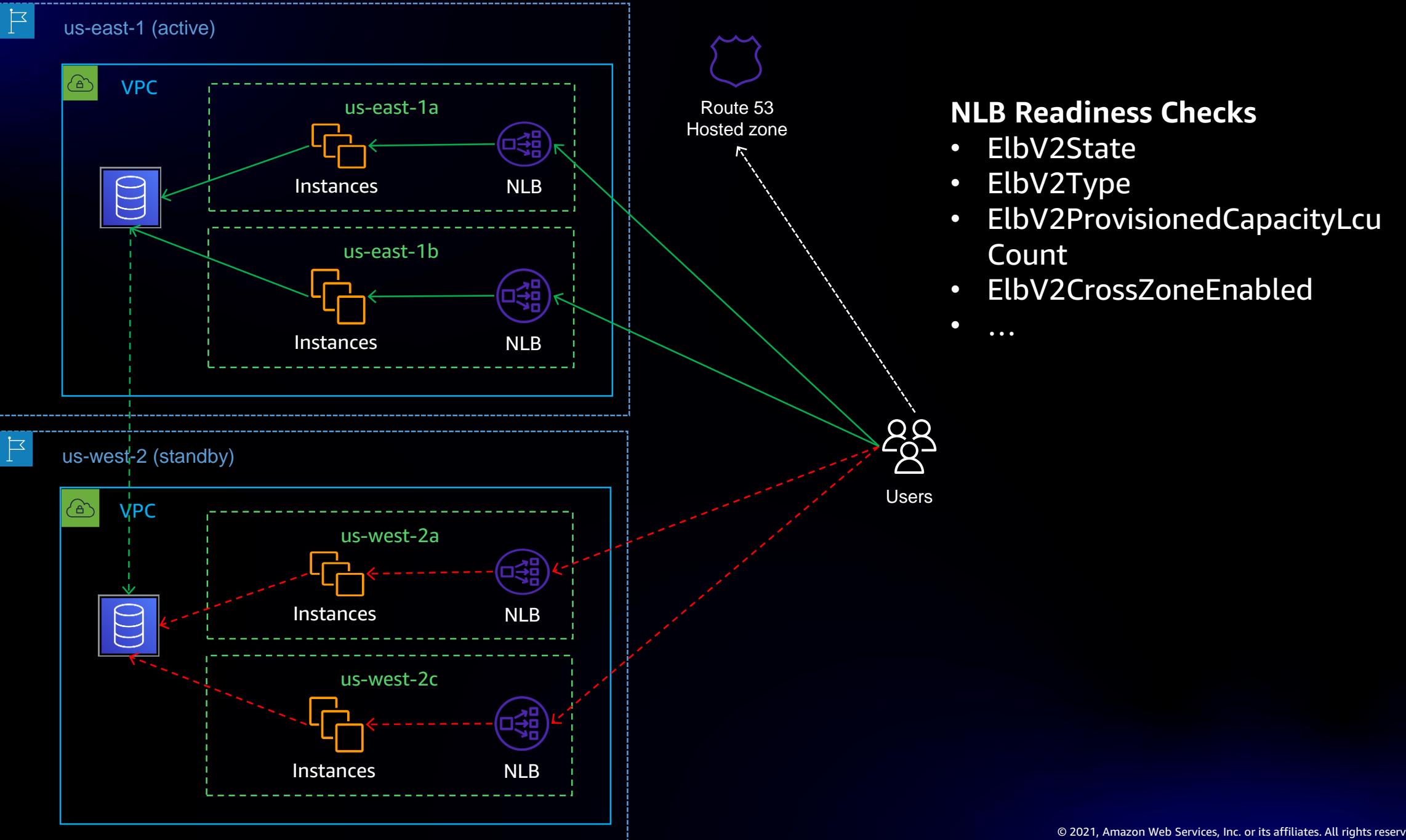
ASG Readiness Checks

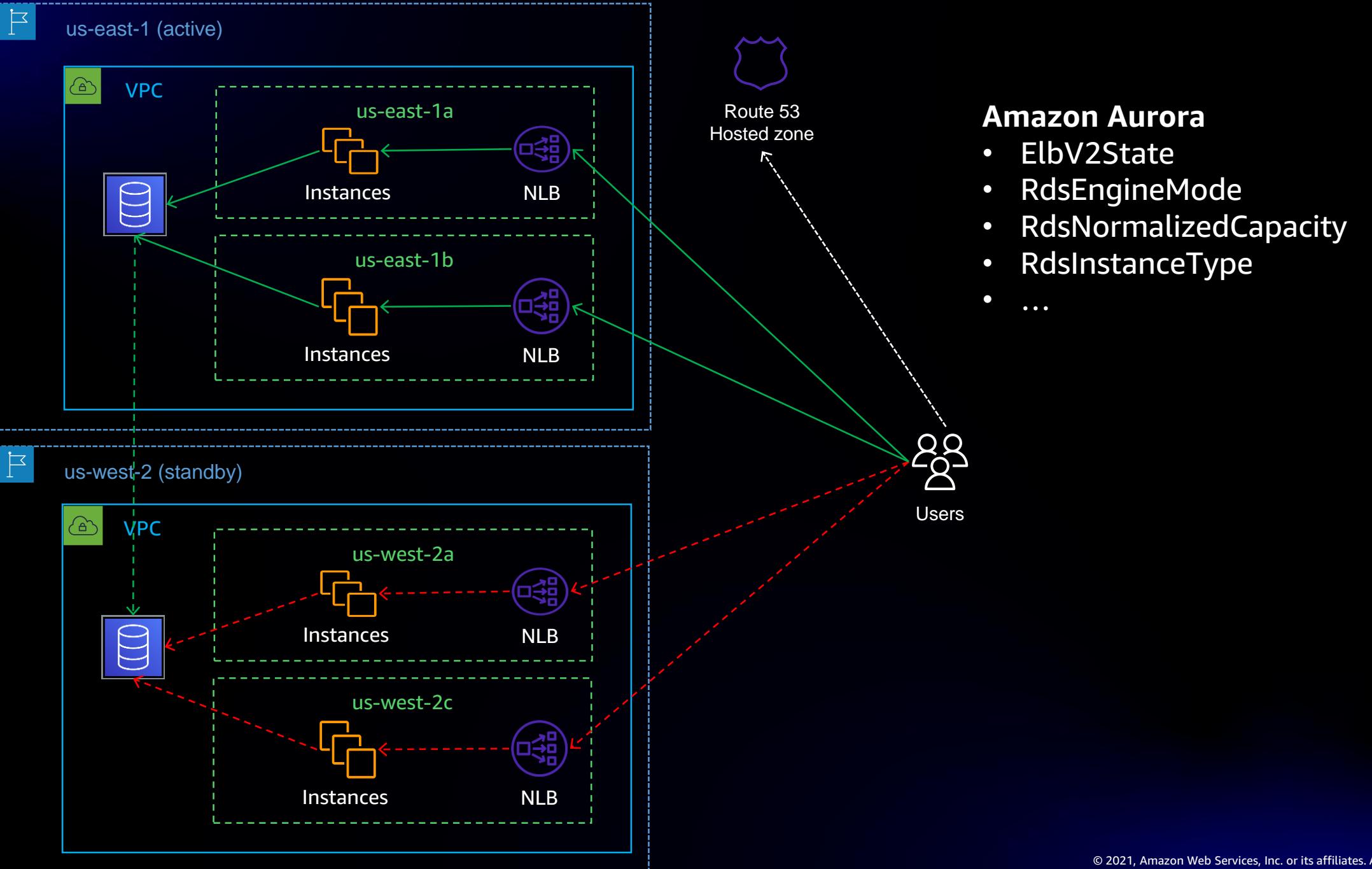
- `AsgMinSizeAndMaxSize`
- `AsgAZCount`
- `AsgInstanceTypes`
- `AsgInstanceSizes`
- ...

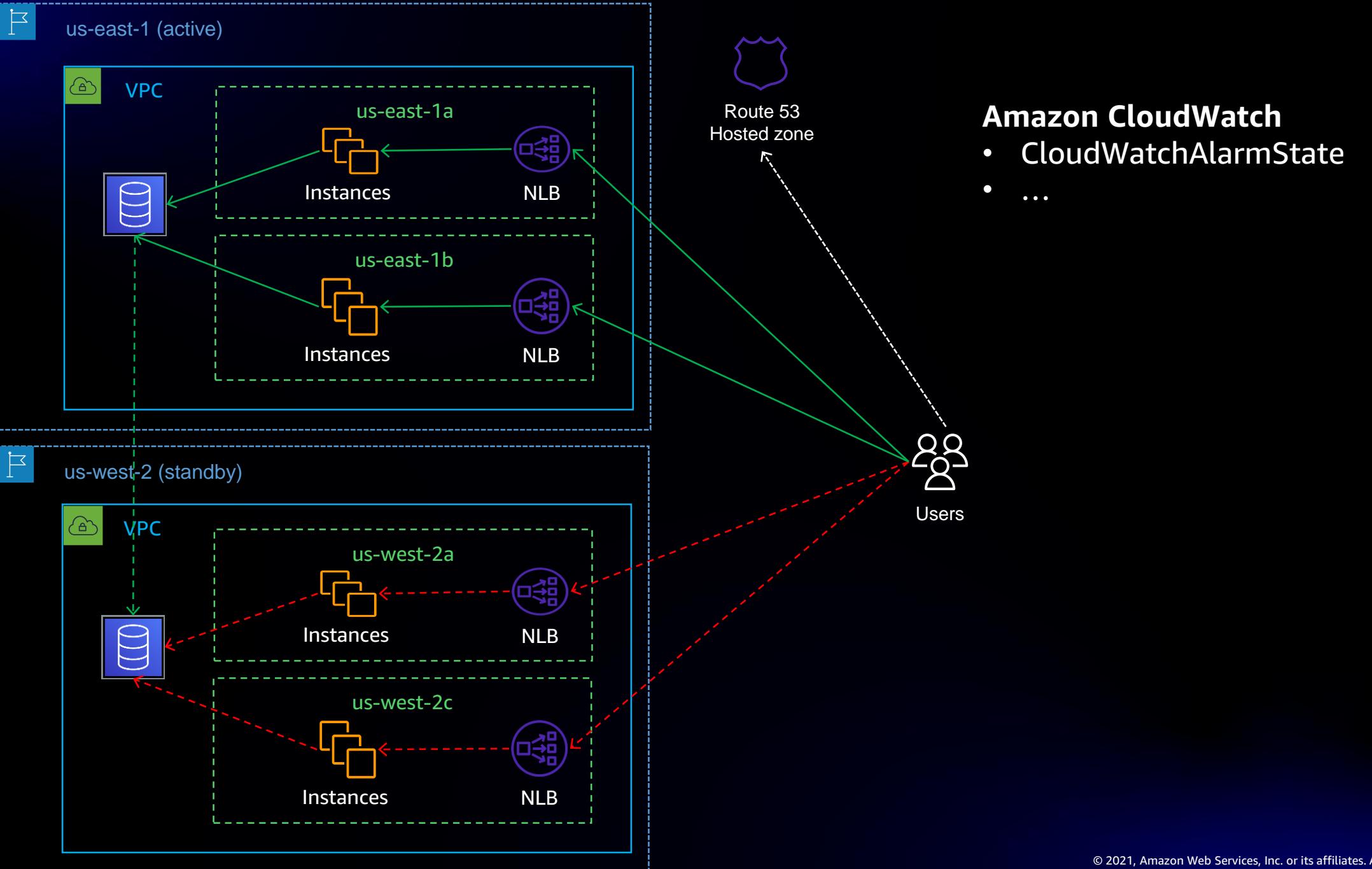


Users









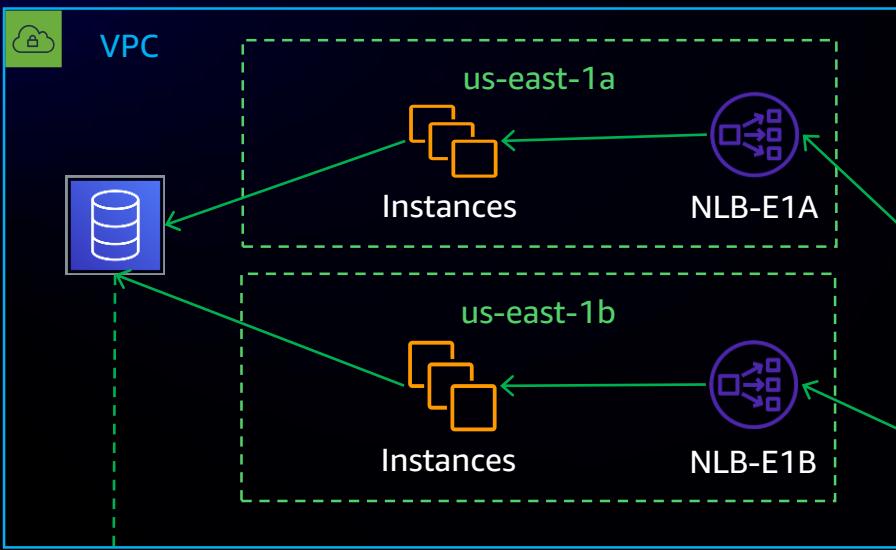
Route 53 ARC features

Now we have multiple replicas

- How do we know we are ready to take a replica out?
- **What recovery mechanism do we use?**
- How do we make sure failover is safe?



us-east-1 (active)



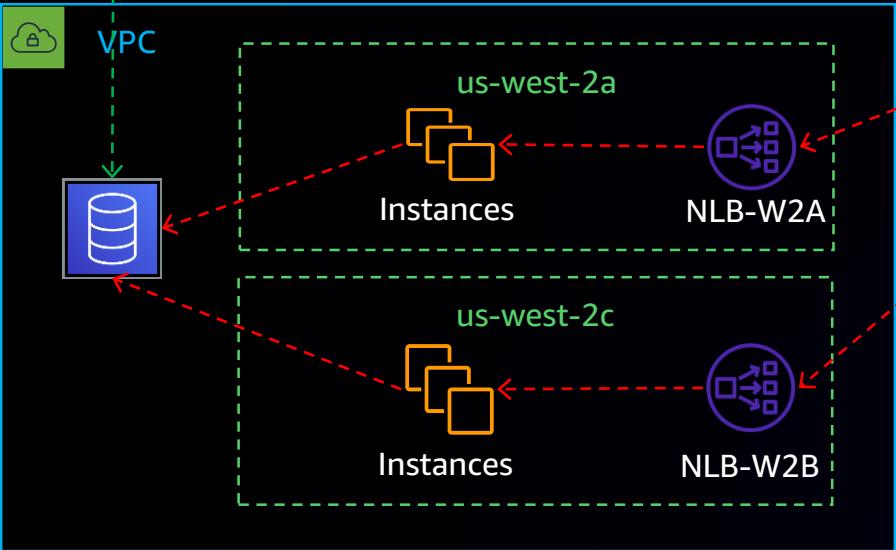
Route 53
Hosted zone



Users



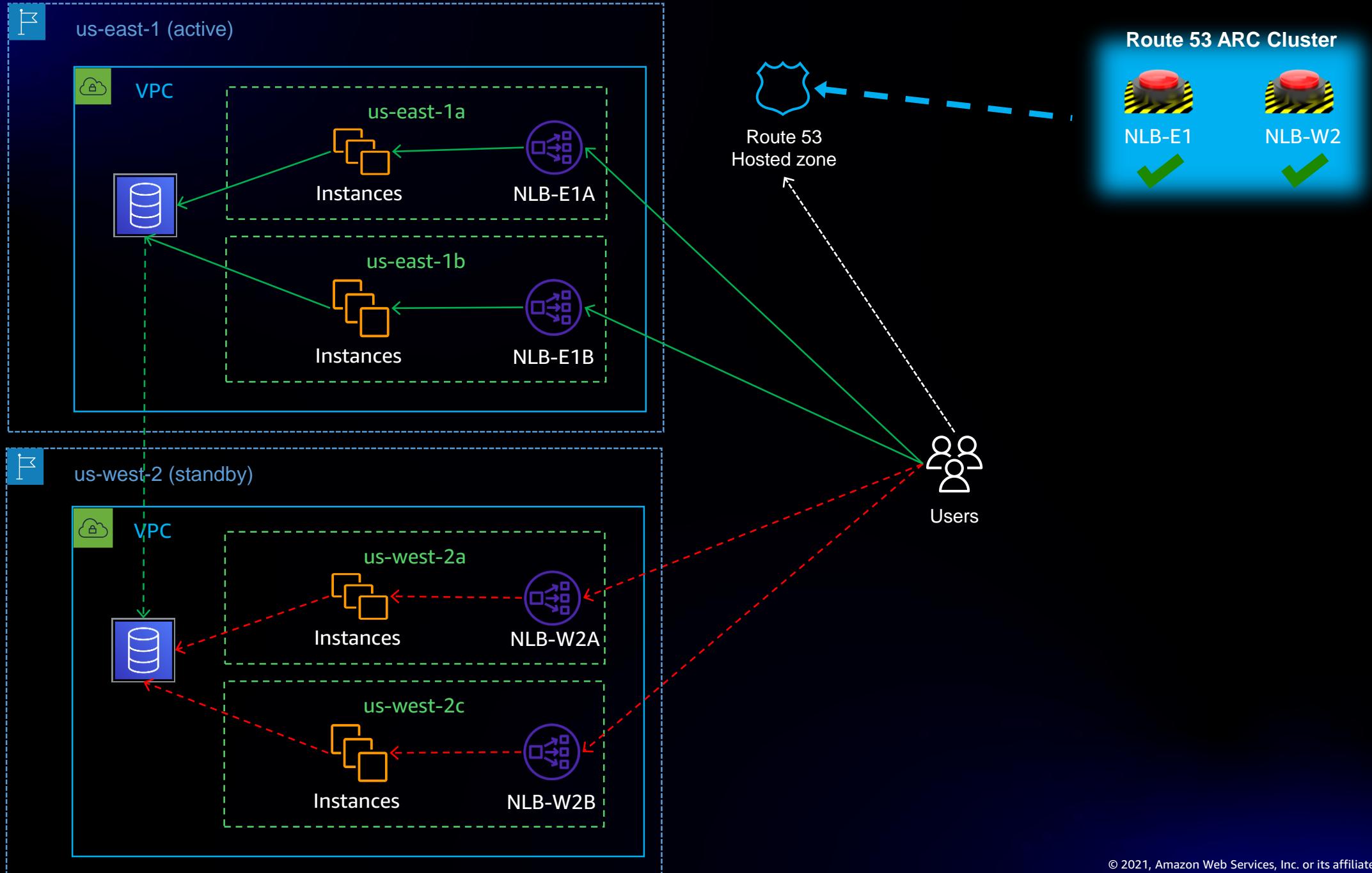
us-west-2 (standby)

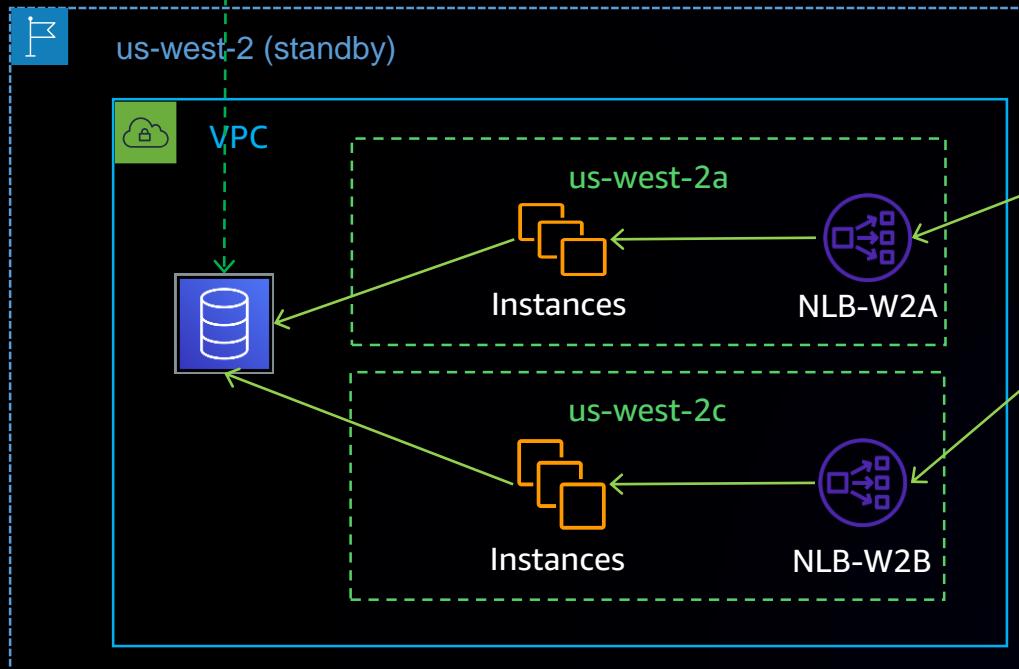
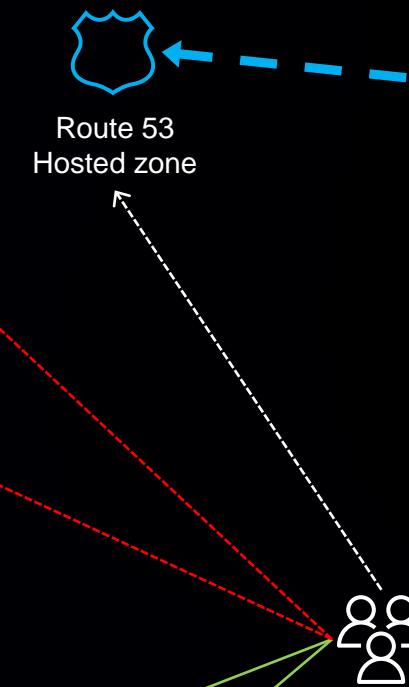
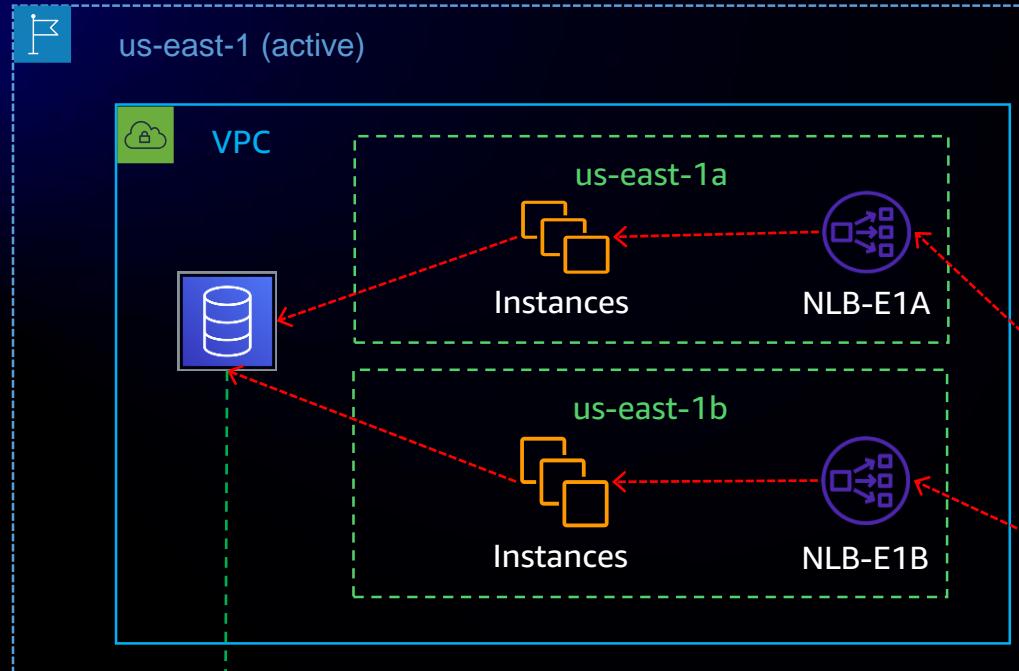


Feature #2: ARC routing controls

API to directly control failover

1. Highly reliable – data plane hosted across 5x regional endpoints
2. Ordered – routing control changes are strictly ordered, even across endpoints





Users

Route 53 ARC features

Now we have multiple replicas

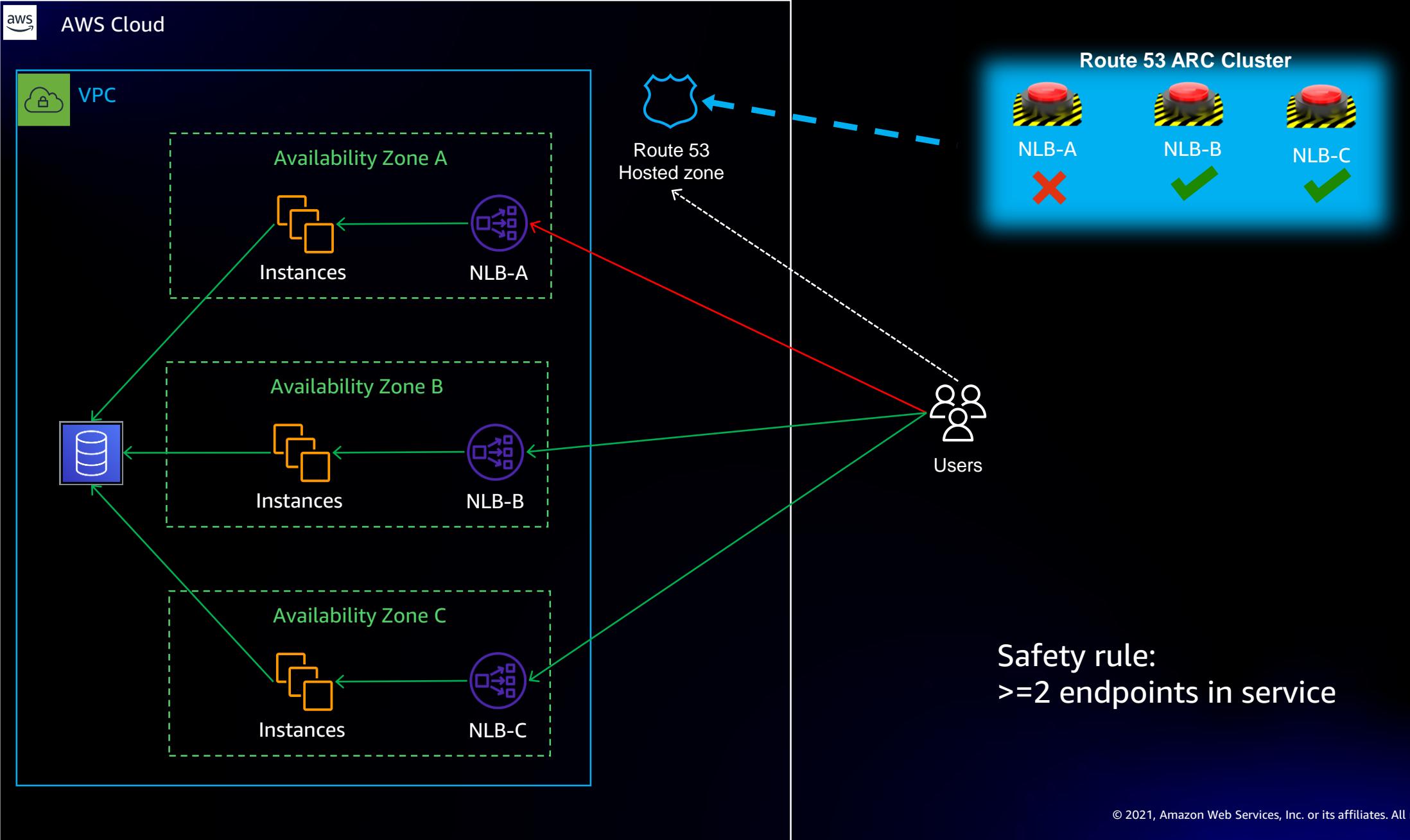
- How do we know we are ready to take a replica out?
- What recovery mechanism do we use?
- How do we make sure failover is safe?

Safety rules

Rules that set preconditions when changing routing controls

Examples?

- Never turn off too many cells for an application at the same time
- Never turn on active and standby together



Related sessions

NET322 – *Building for high availability: Architecture and recovery*

Builders' Session

Wed., Dec. 1st, 10-11 a.m. Academy 417, Caesar's Forum

NET317-R2 – *Designing resilient applications using Amazon Route 53 ARC*

Chalk Talk

Wed., Dec. 1st, 1-2 p.m.

Palmer 2, Wynn Level 1



Agenda

Route 53 Resolver

- Forwarding rules improvements
- IPv6 resolver support
- Resolver Query Logs
- Resolver DNS Firewall

Route 53 DNSSEC

Route 53 Application Recovery Controller (ARC)

Thank you!

