AWS re:Invent

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

NET304

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

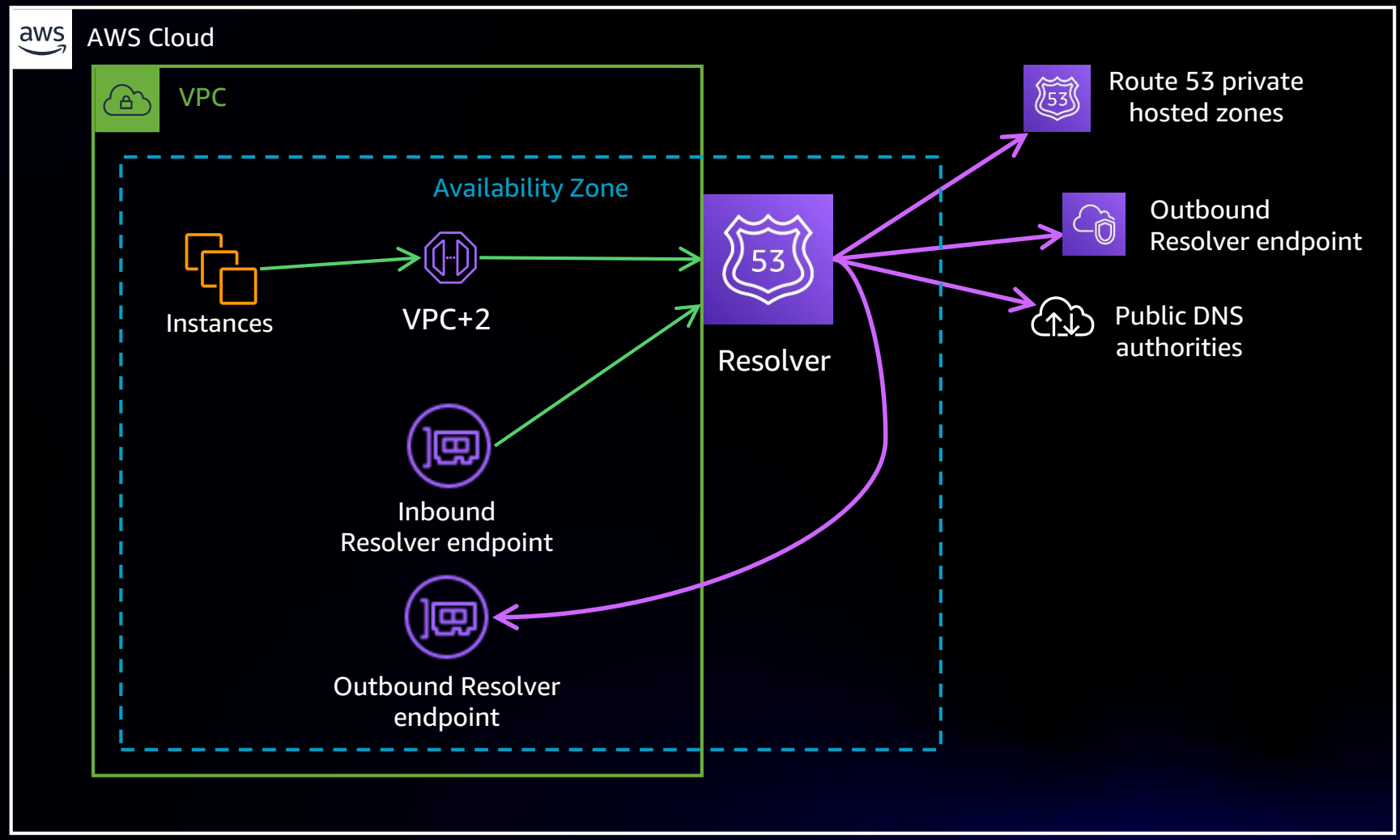
Route 53 DNSSEC

Route 53 Application Recovery Controller (ARC)

Route 53 Resolver

Route 53 Resolver

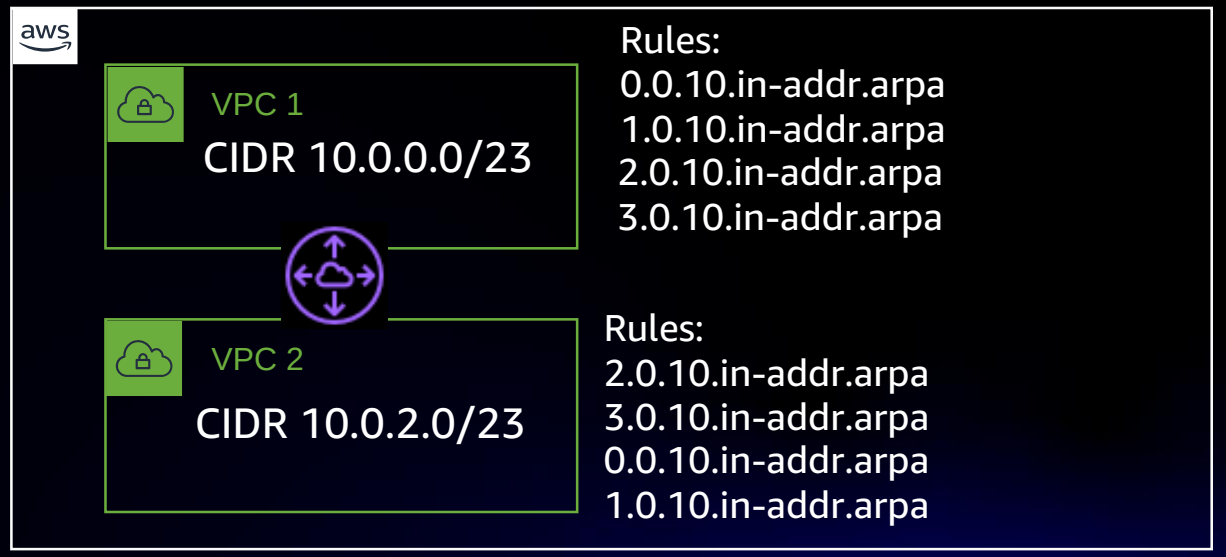
- Provides recursive DNS resolution
- Alternative names
  - AmazonProvidedDNS
  - VPC+2 Resolver
- Inbound Resolver endpoints
  - Provide resolution for resources outside a VPC
- Outbound Resolver endpoints
  - Forward DNS queries to a target server



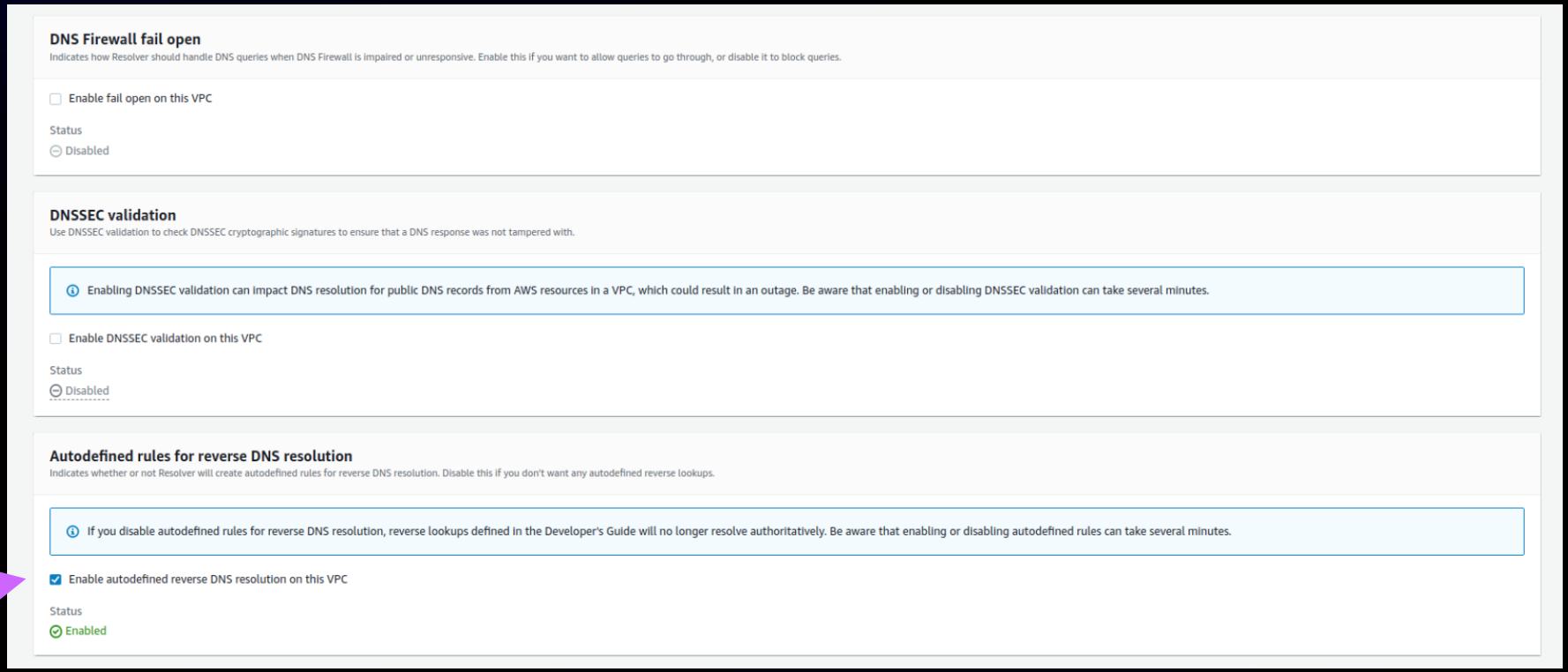
Reverse records

- Scenario: using Active Directory and want to it send PTR queries (reverse lookups)

- Previous solution: create Forward Rules for VPC CIDR blocks



Reverse records



- 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

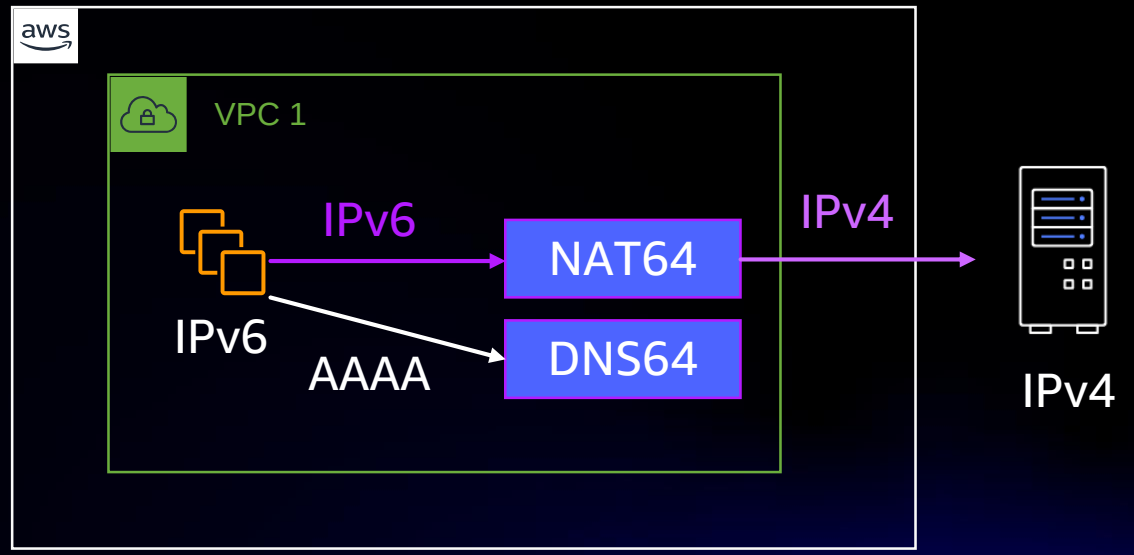
Scenario: transitioning to use IPv6 in a dual-stack environment with IPv4

- 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



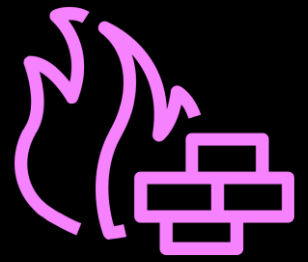
Resolver query logging – Use cases

Compliance

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

Debugging

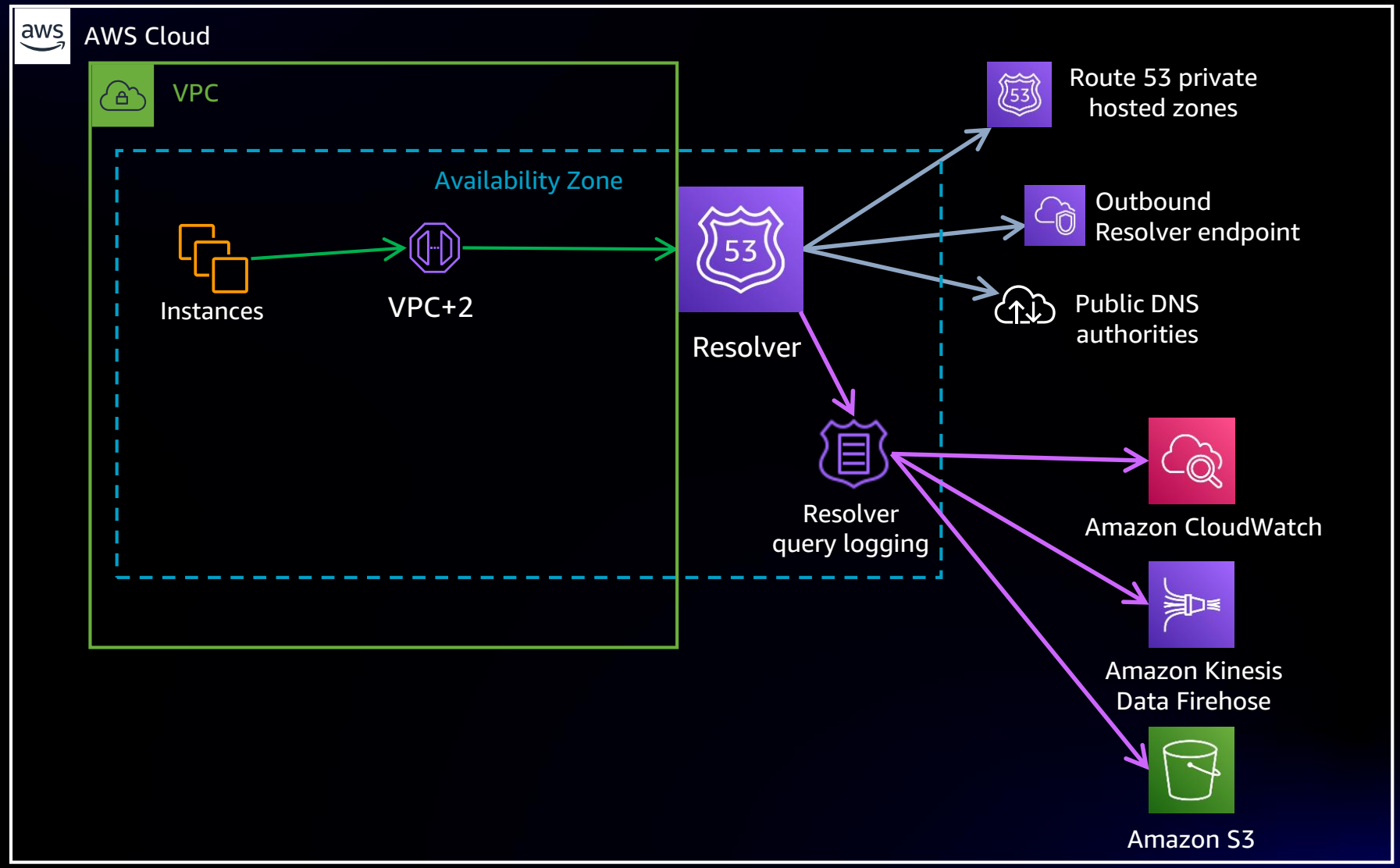
Find instances querying incorrect domain names



Threat Detection

Find instances querying malicious domain names

Resolver query logging

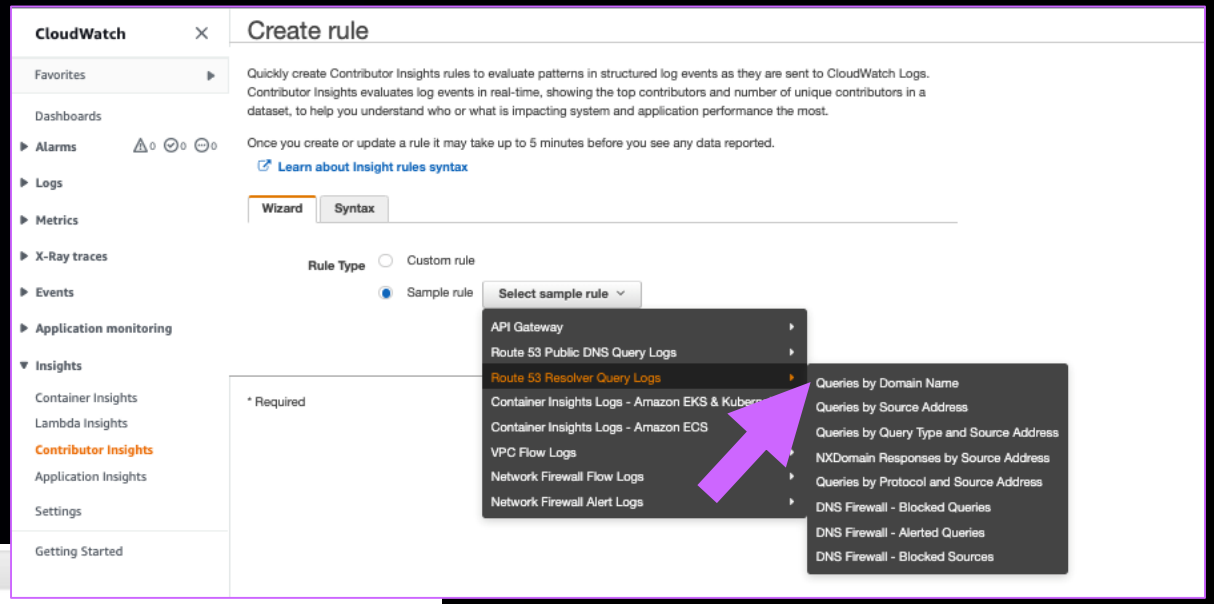


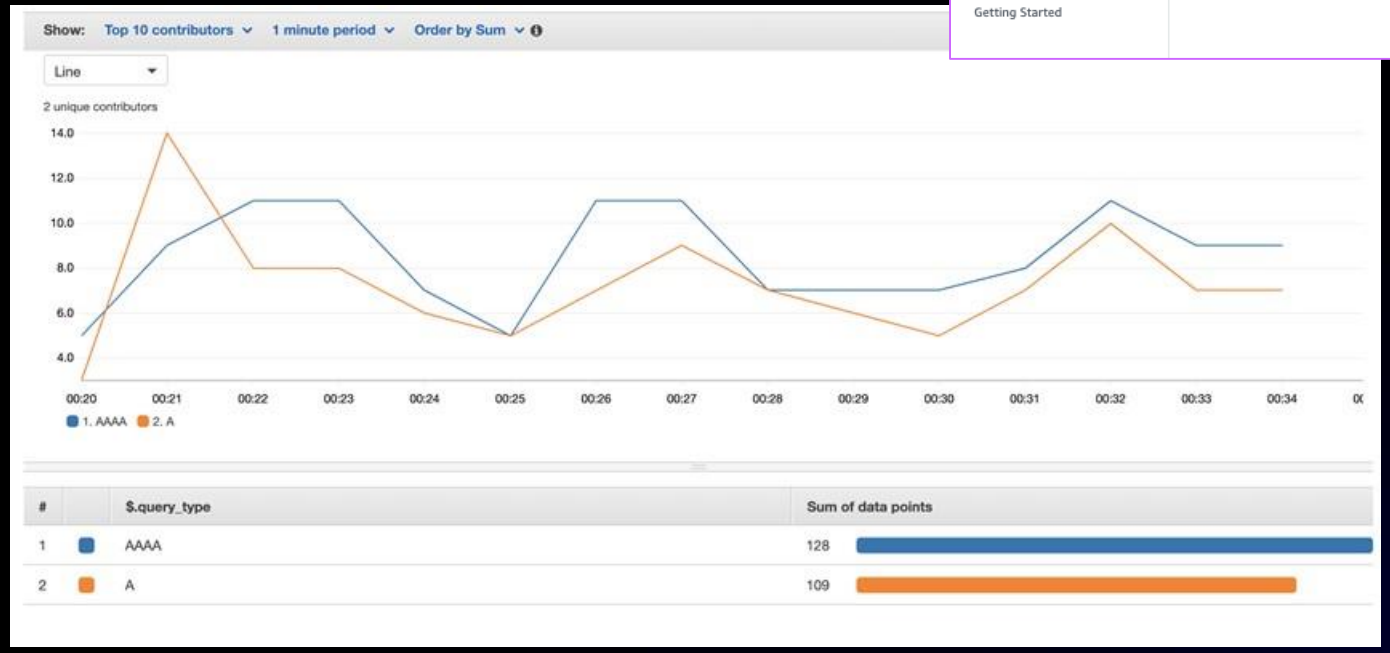
Resolver query logging


```
{
    "version": "1.100000",
    "account_id": "[redacted]",
    "region": "us-west-2",
    "vpc_id": "vpc-[redacted]",
    "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-[redacted]"
    },
    "firewall_rule_action": "ALERT",
    "firewall_rule_group_id": "rslvr-frg-[redacted]",
    "firewall_domain_list_id": "rslvr-fdl-[redacted]"
}
```

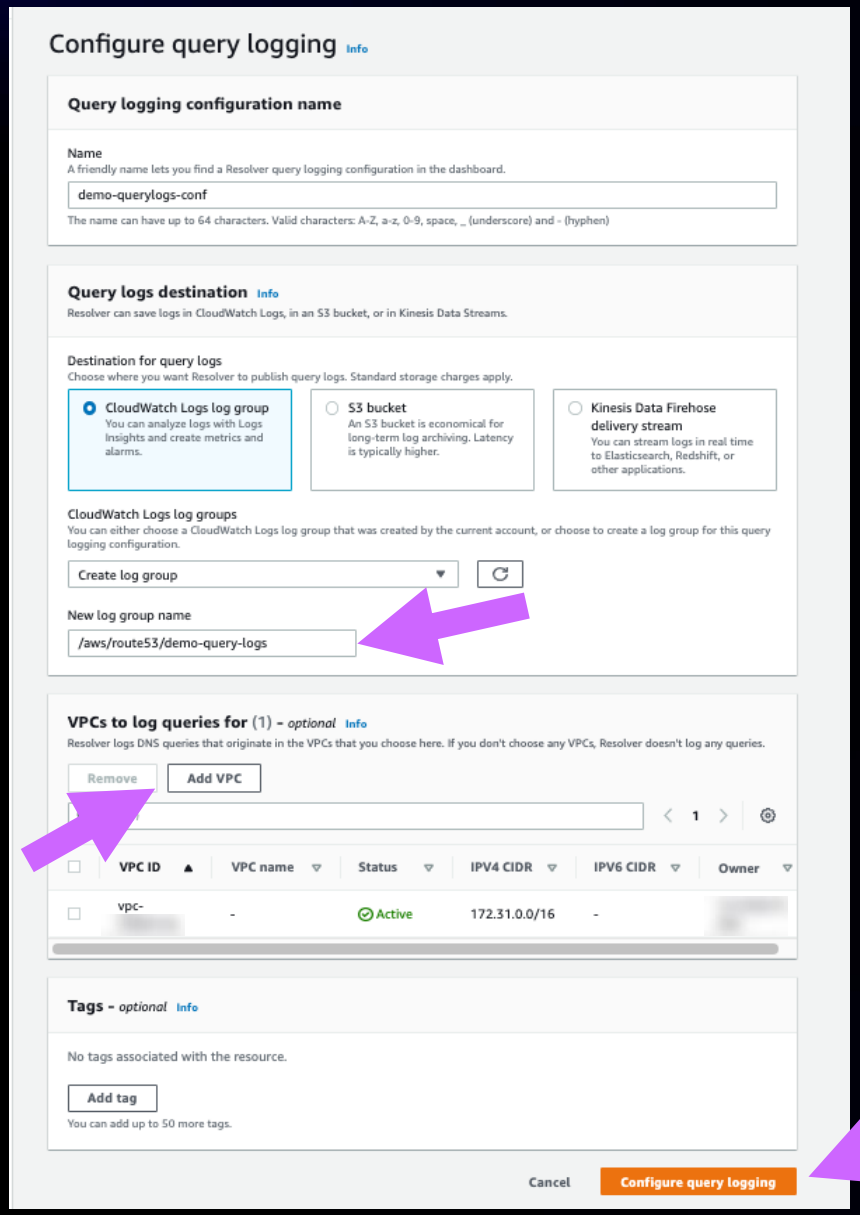
Resolver query logging

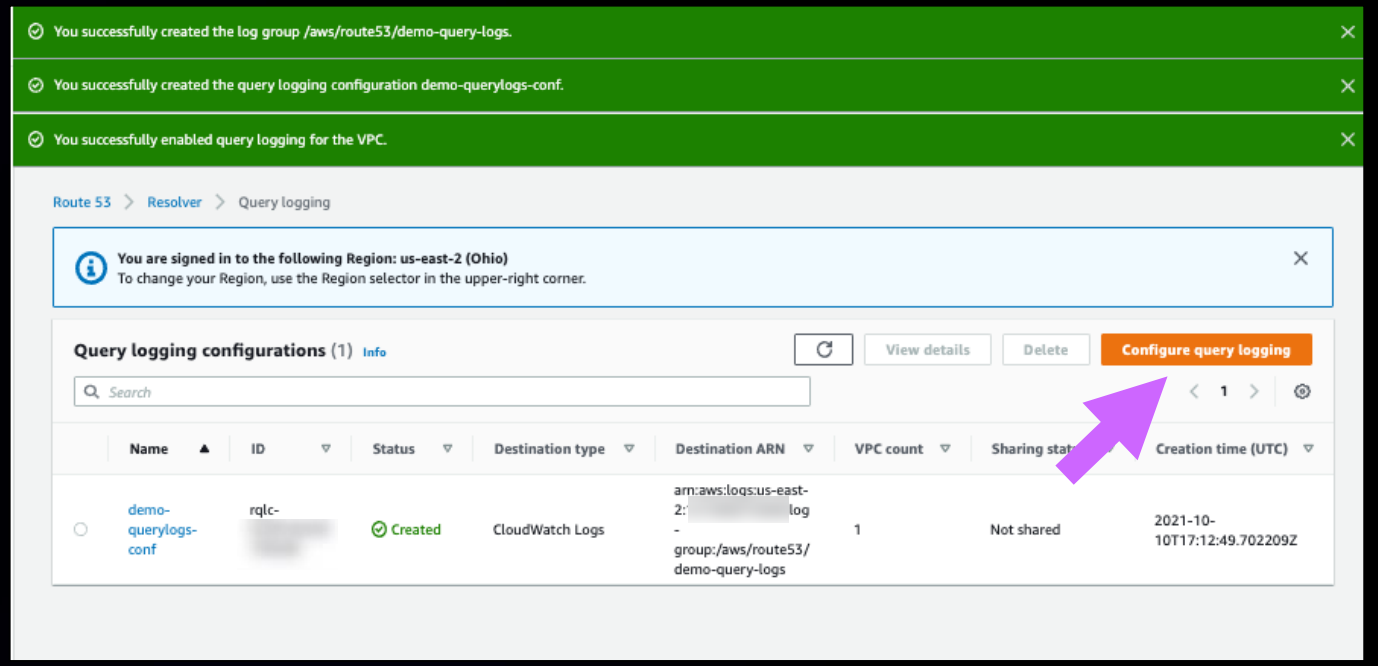
- Create Amazon CloudWatch Contributor Insights reports
- Track query types, rcode, query names, and more



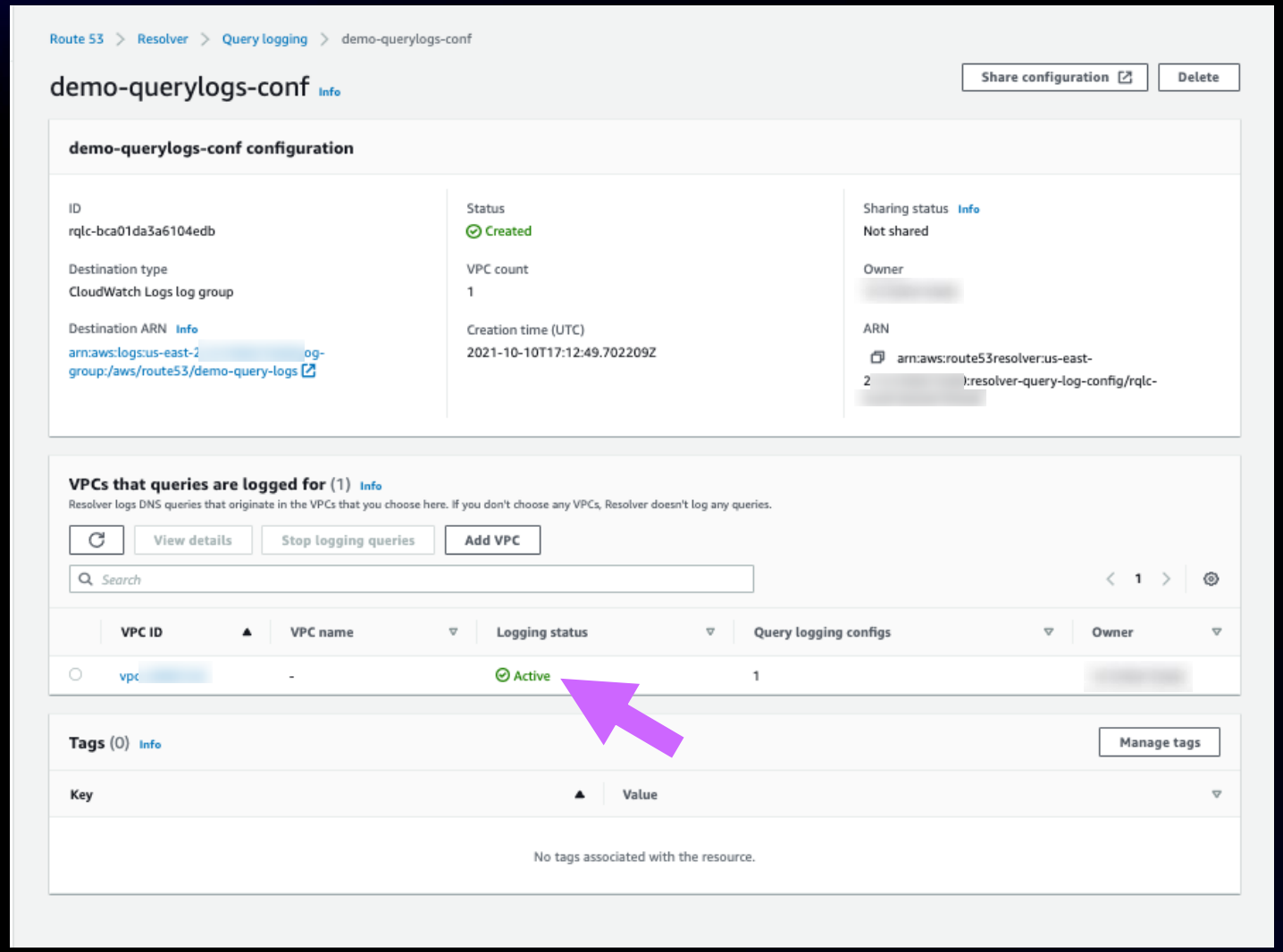


Resolver query logging – Walkthrough





Resolver query logging – Walkthrough



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 ~]$
```

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn mo

View as text | Actions | Create Metric Filter

Filter events

Message

No older events at this moment. Retry


```
{
    "version": "1.100000",
    "account_id":
    "region": "us-east-2",
    "vpc_id": "vpc-c06857a9",
    "query_timestamp": "2021-10-10T17:14:36Z",
    "query_name": "amazon.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": "55742",
    "transport": "UDP",
    "srcids": {
        "instance": "i-
    }
}
```

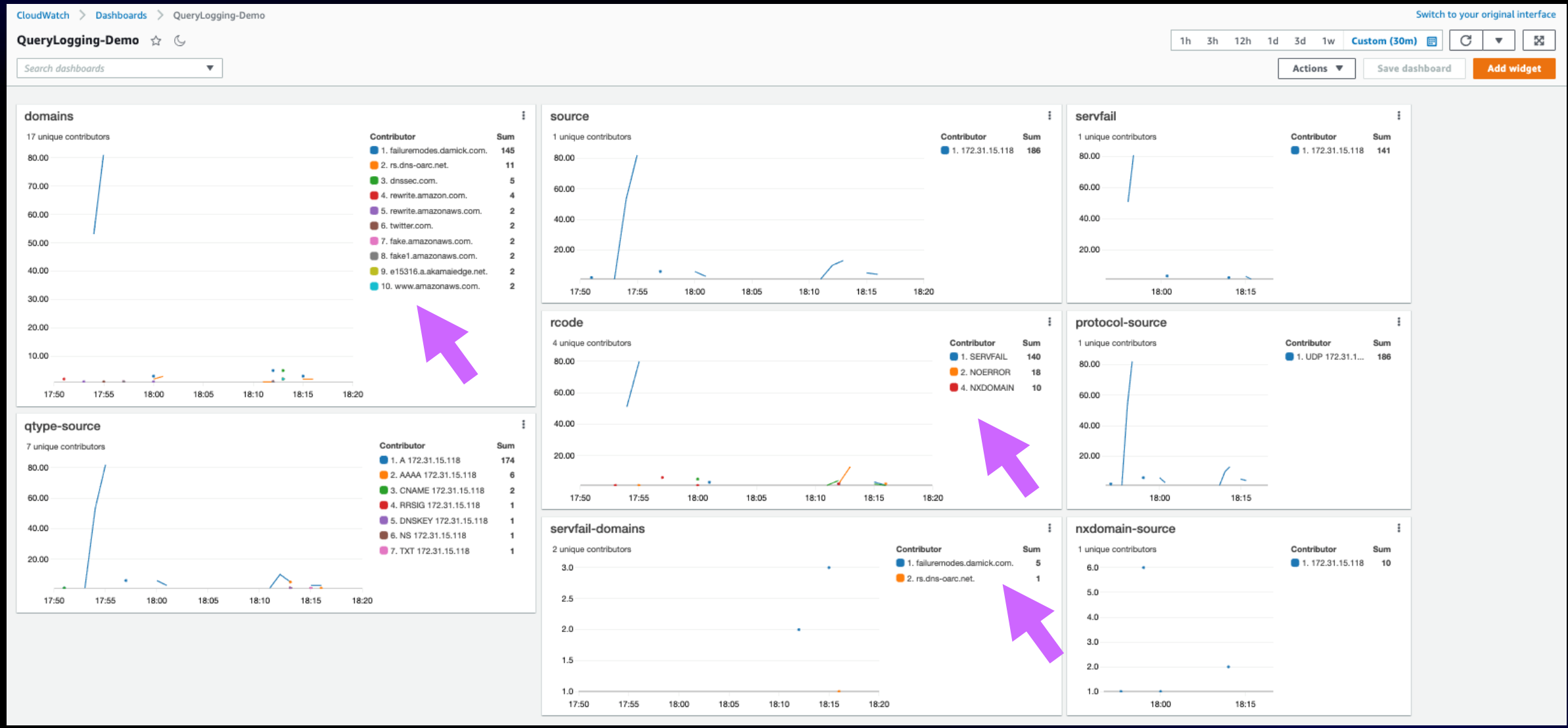

No newer events at this moment. *Auto retry paused.* Resume

```
[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 ~]$
```


```
{
    "version": "1.100000",
    "account_id":
    "region": "us-east-2",
    "vpc_id": "vpc-c06857a9",
    "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-
    }
}
```


No newer events at this moment. *Auto retry paused.* Resume

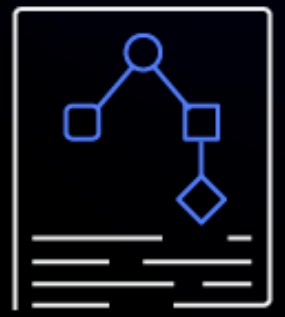
Resolver query logging – Walkthrough



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

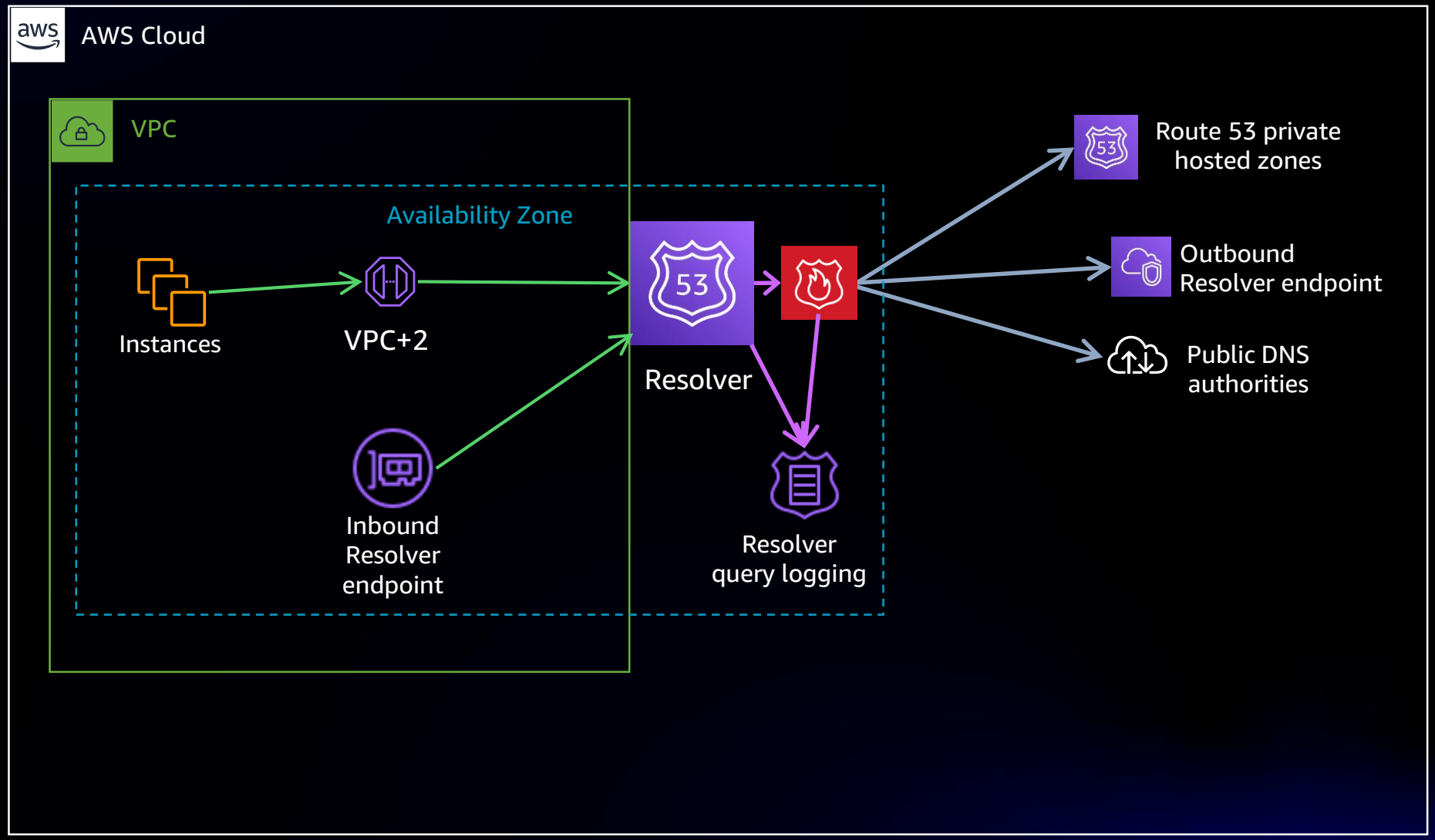
Managed domain lists

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

Visibility and reporting

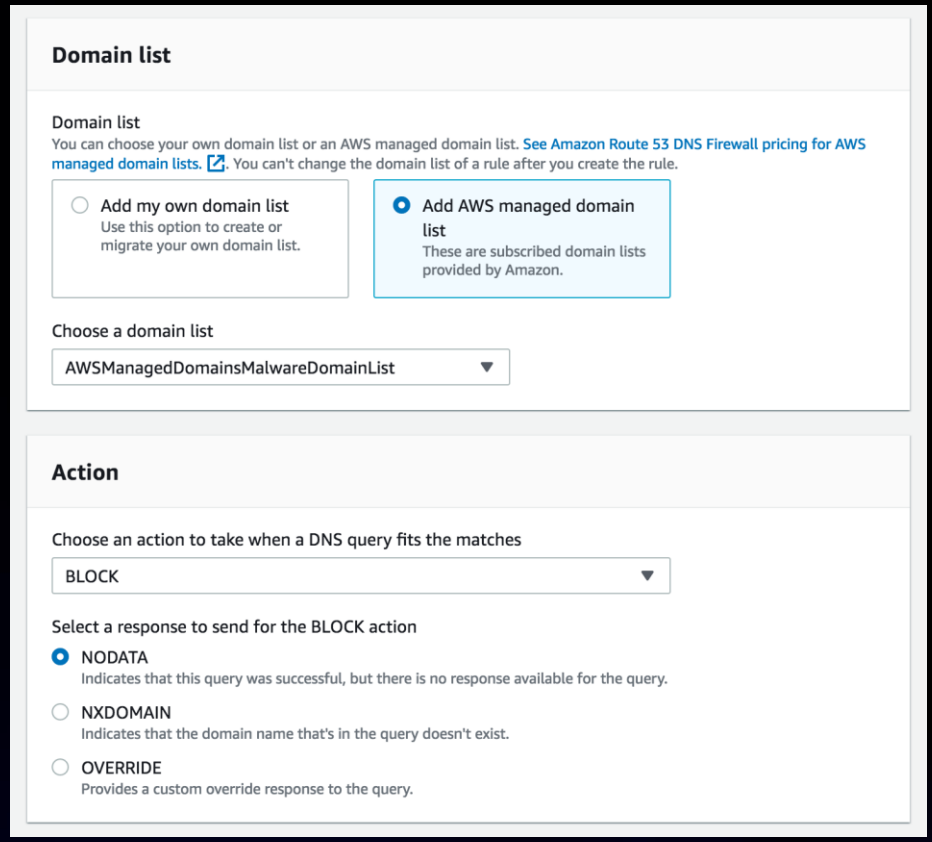
- Per-rule CloudWatch metrics
- Configurable logs sent to Amazon S3, CloudWatch, Kinesis (enabled by Resolver query logging)

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



DNS Firewall

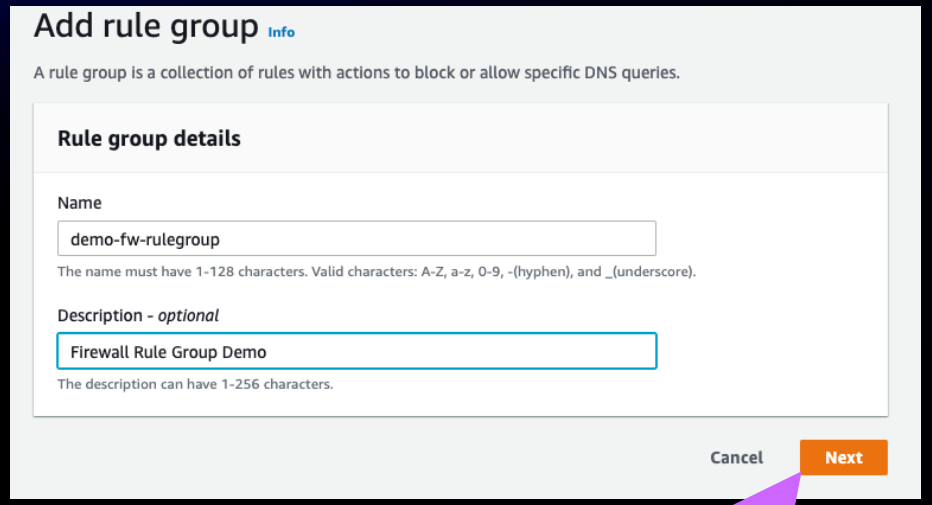
Amazon GuardDuty

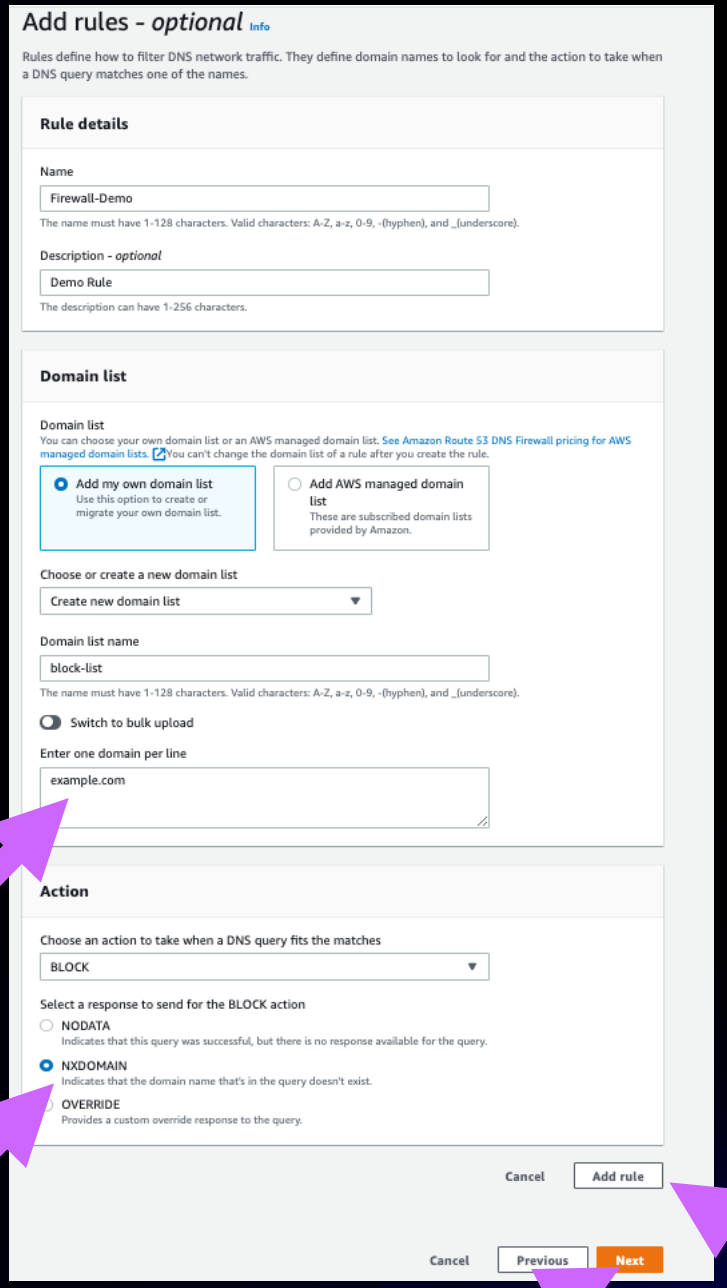
GuardDuty provides analysis and detection by using threat intelligence feeds, signatures, anomaly detection, and machine learning

Amazon Detective

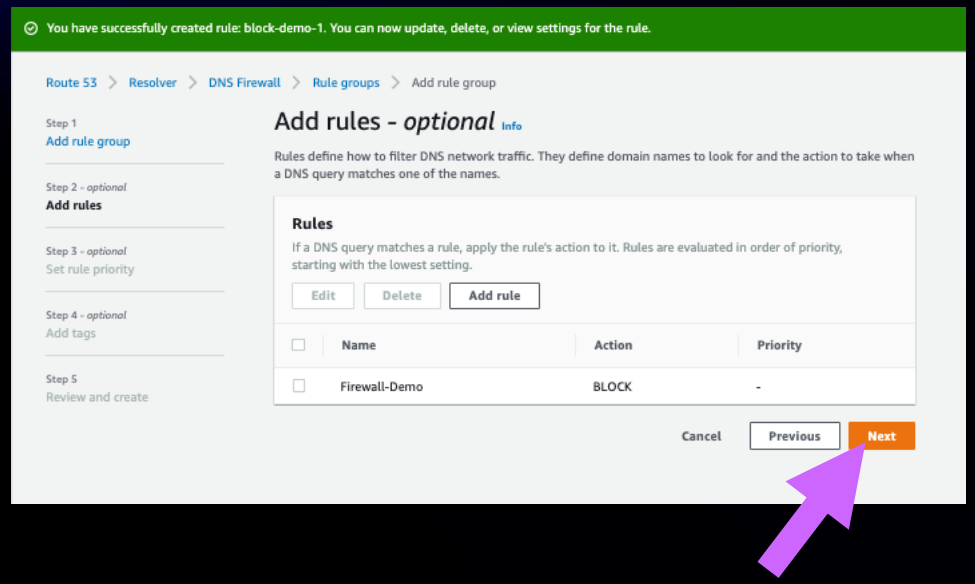
Detective makes it easy to analyze, investigate, and quickly identify the root cause of security findings or suspicious activities

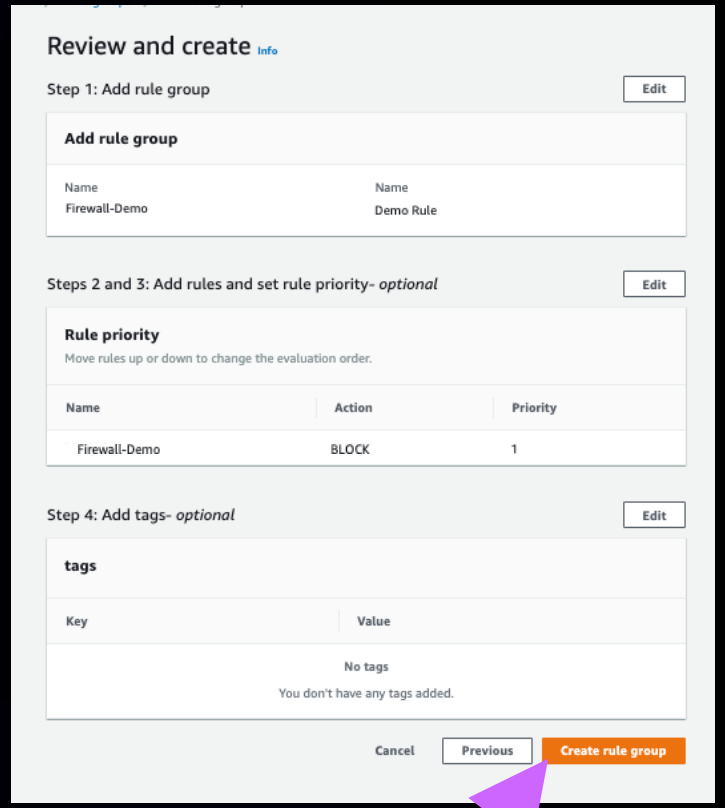
DNS Firewall

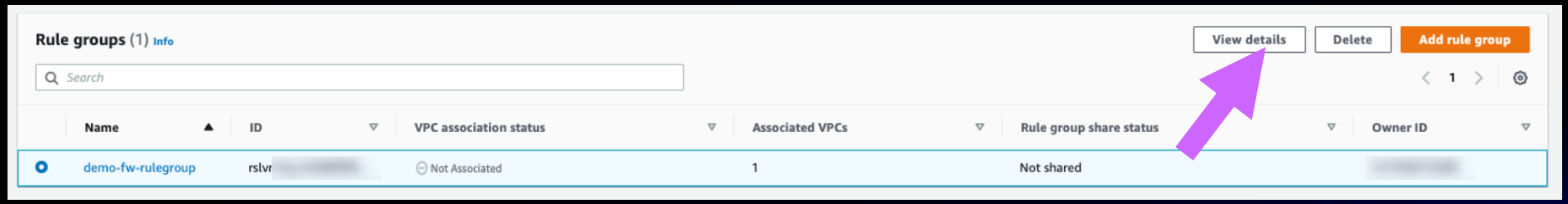




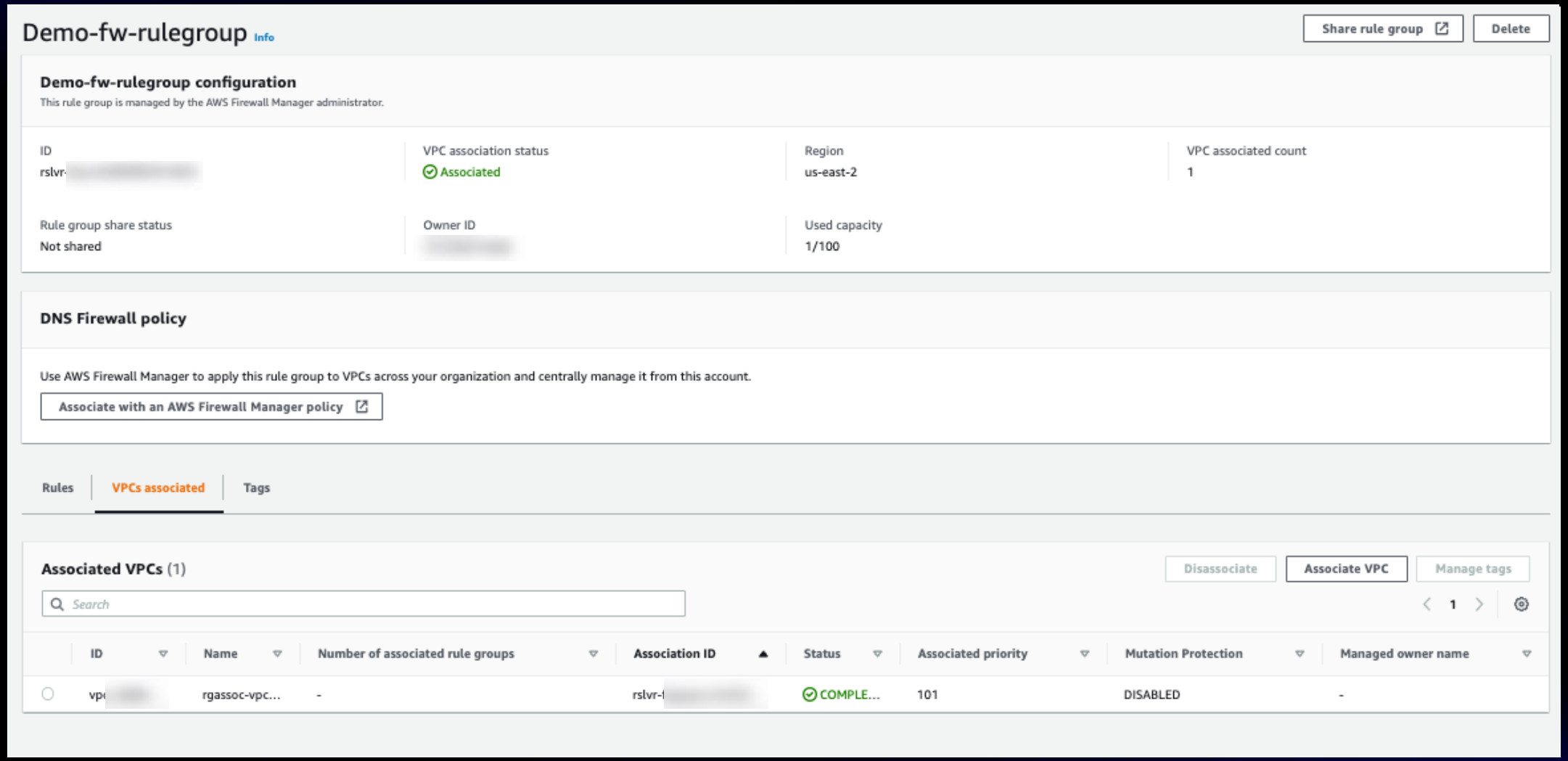
DNS Firewall



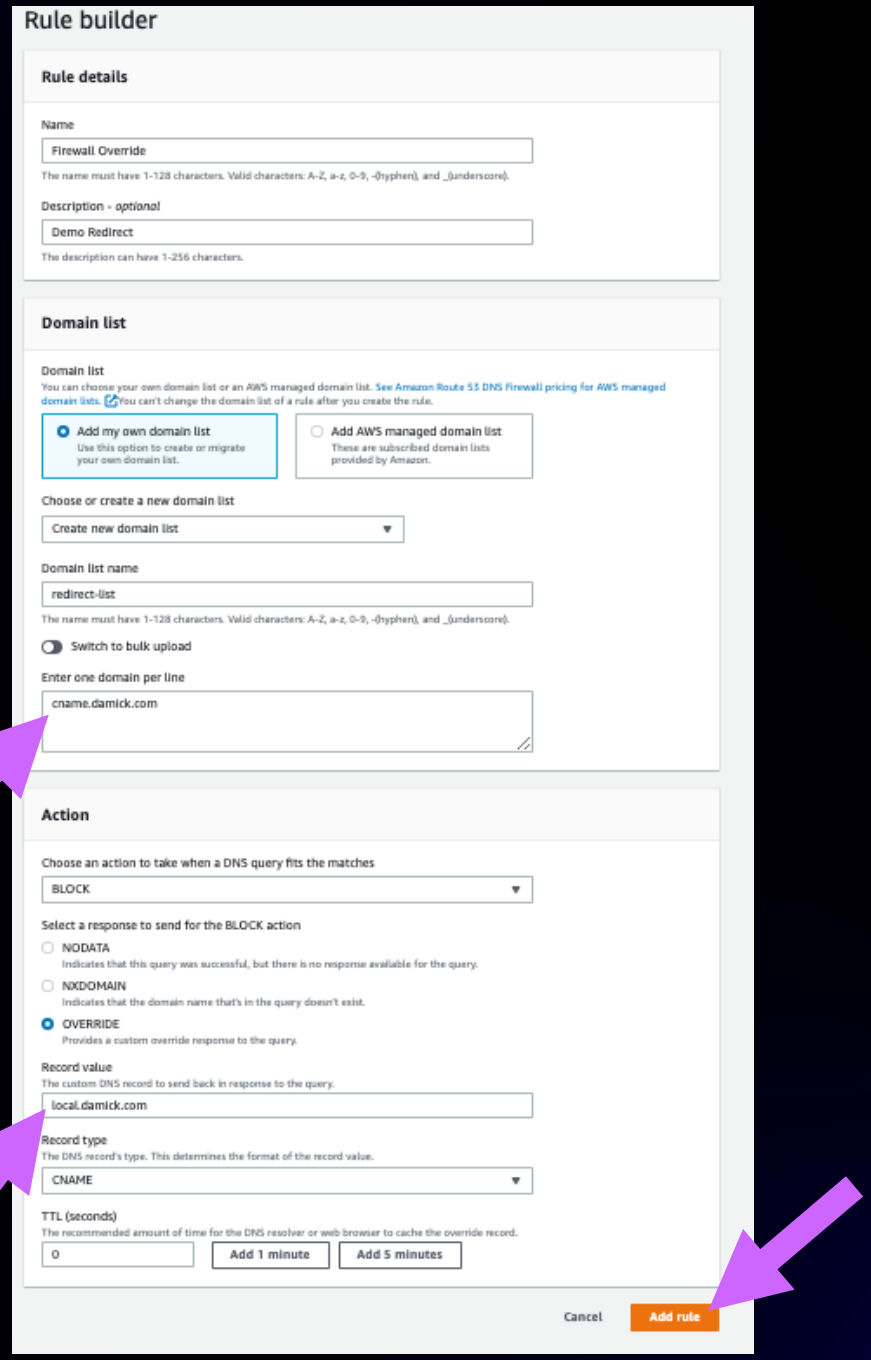




DNS Firewall



DNS Firewall



DNS Firewall

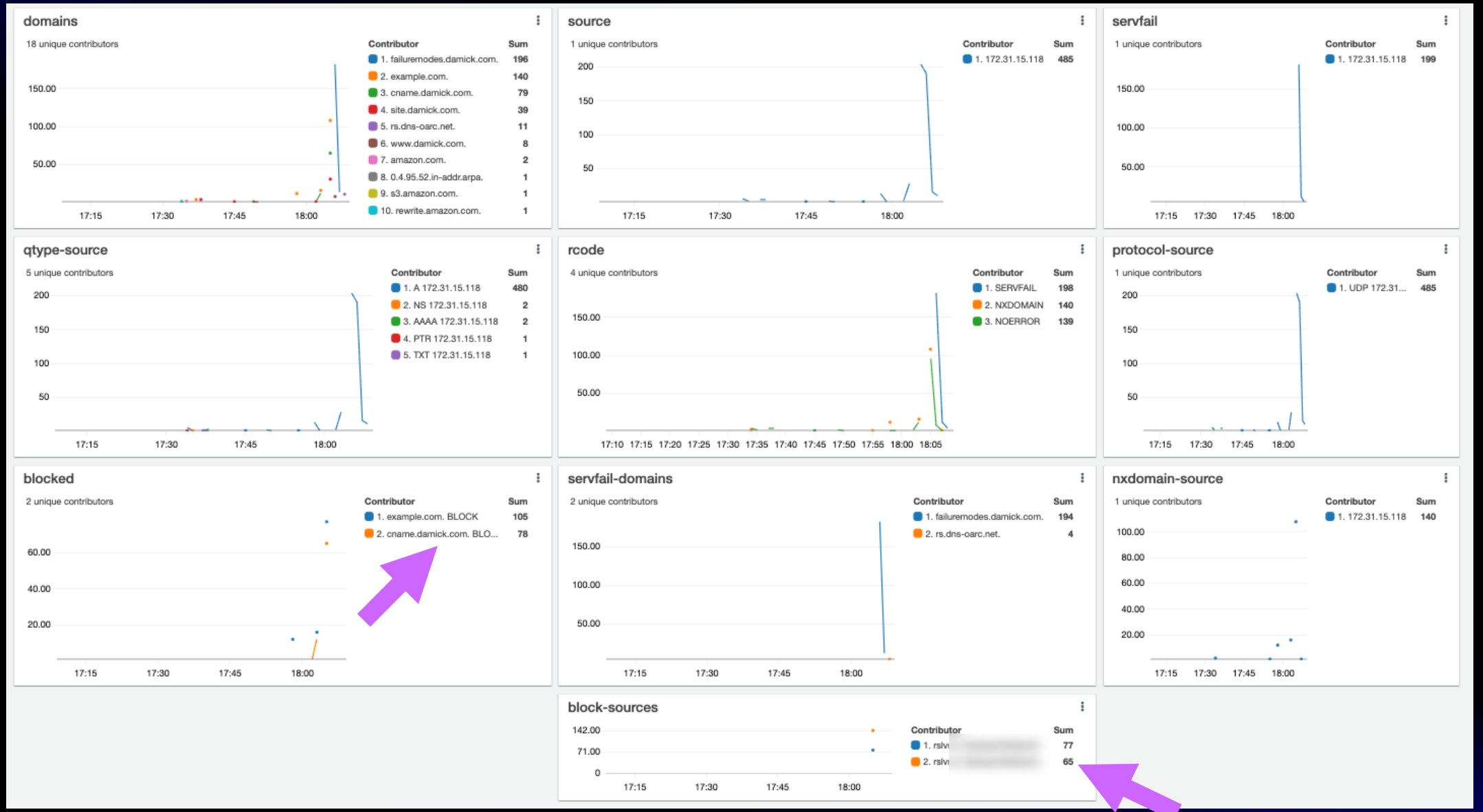
```
[ec2-user@ip-172-31-15-118 ~]$  dig example.com

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> example.com
;; 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: 4096
;; QUESTION SECTION:
;example.com.                   IN      A

;; 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
```


```
{
    "version": "1.100000",
    "account_id": [redacted],
    "region": "us-east-2",
    "vpc_id": "vpc[redacted]",
    "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[redacted]
    },
    "firewall_rule_action": "BLOCK",
    "firewall_rule_group_id": "rslvr-[redacted]
    "firewall_domain_list_id": "rslvr[redacted]
}
```


```
[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
```


```
{
    "version": "1.100000",
    "account_id": [redacted],
    "region": "us-east-2",
    "vpc_id": "vpc-[redacted]",
    "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": "47570",
    "transport": "UDP",
    "srcids": {
        "resolver_endpoint": "rslvr-in-[redacted]
        "resolver_network_interface": "[redacted]
    },
    "firewall_rule_action": "BLOCK",
    "firewall_rule_group_id": "rslvr-[redacted]
    "firewall_domain_list_id": "rslvr[redacted]
}
```

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)

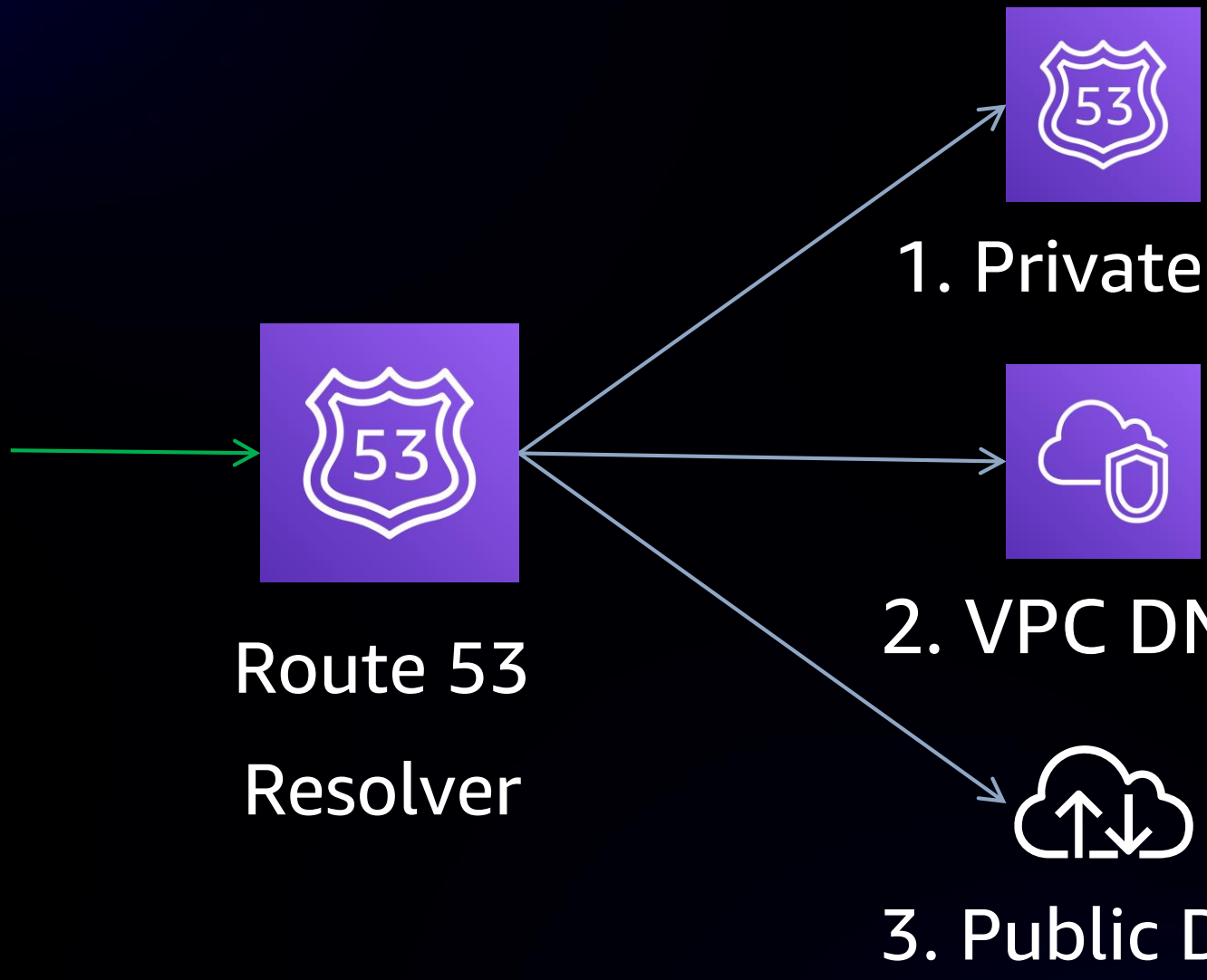
Route 53 DNSSEC

What problem does DNSSEC solve?

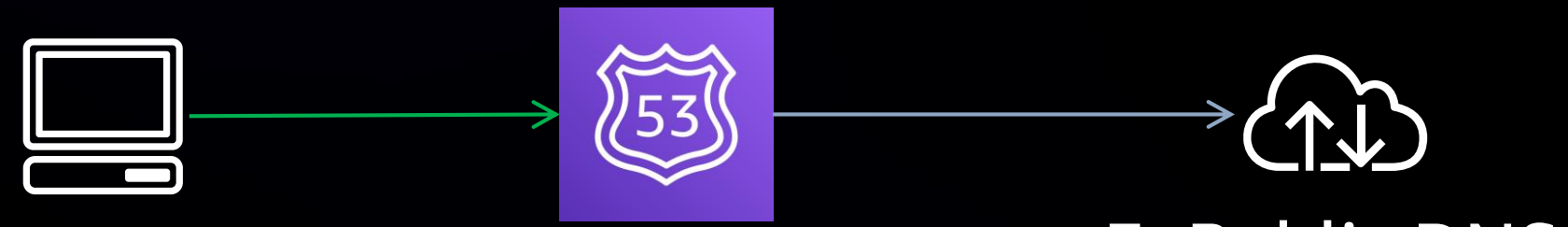
- You want to authenticate DNS when connecting to web services
- You want your clients to authenticate DNS connecting to your services
- Compliance
  - NIST SP 800-53 SC-21
    - SC-20 SECURE NAME/ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)
    - SC-21 SECURE NAME/ADDRESS RESOLUTION SERVICE (RECURSIVE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

What is DNSSEC?

Query: www.gavinmc.com/A



Query: www.gavinmc.com/A



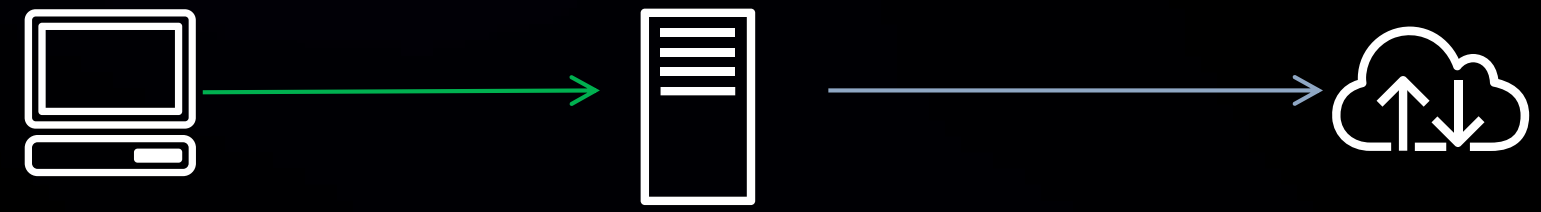
Client

Route 53

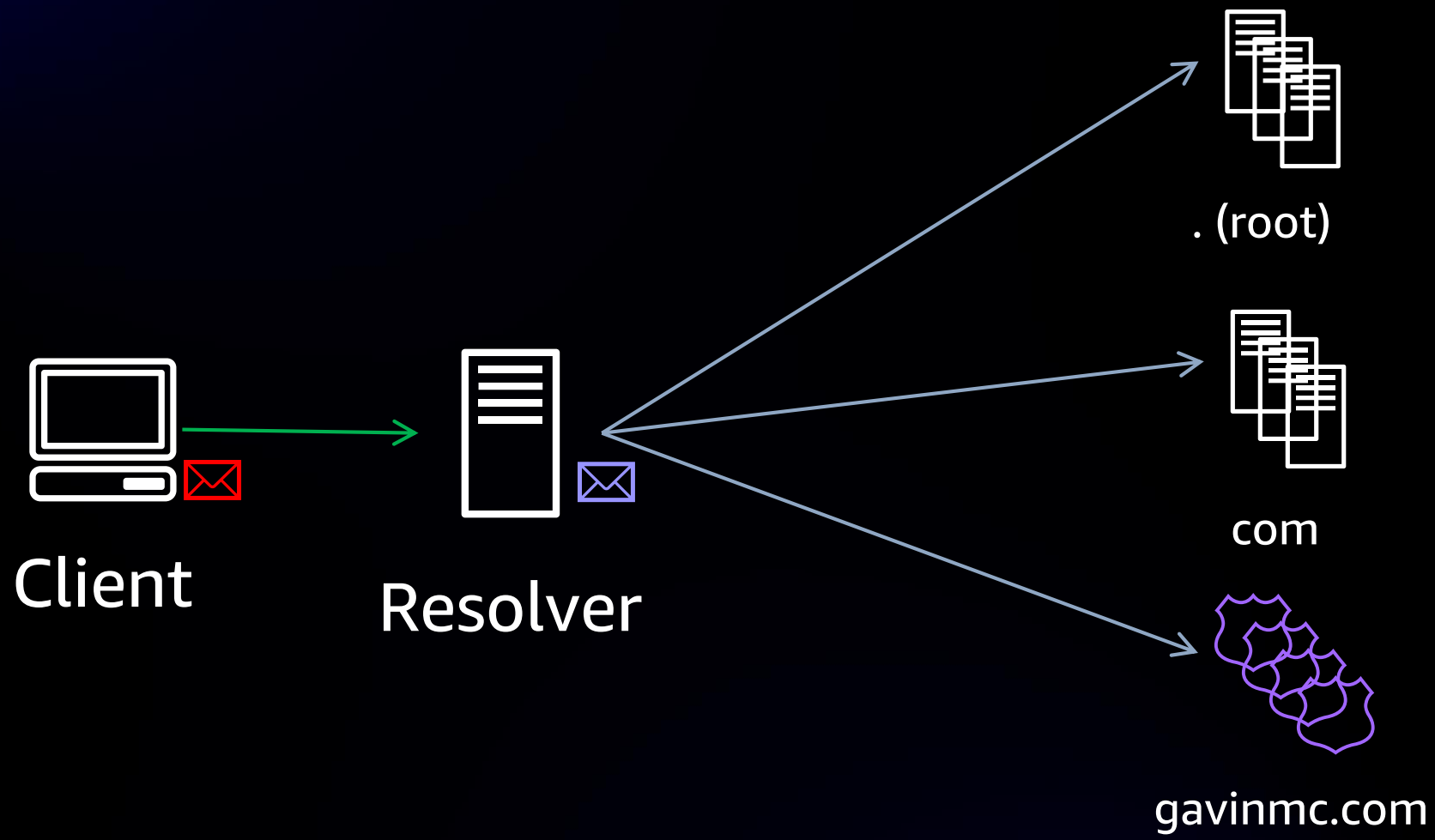
Resolver

3. Public DNS

Query: www.gavinmc.com/A

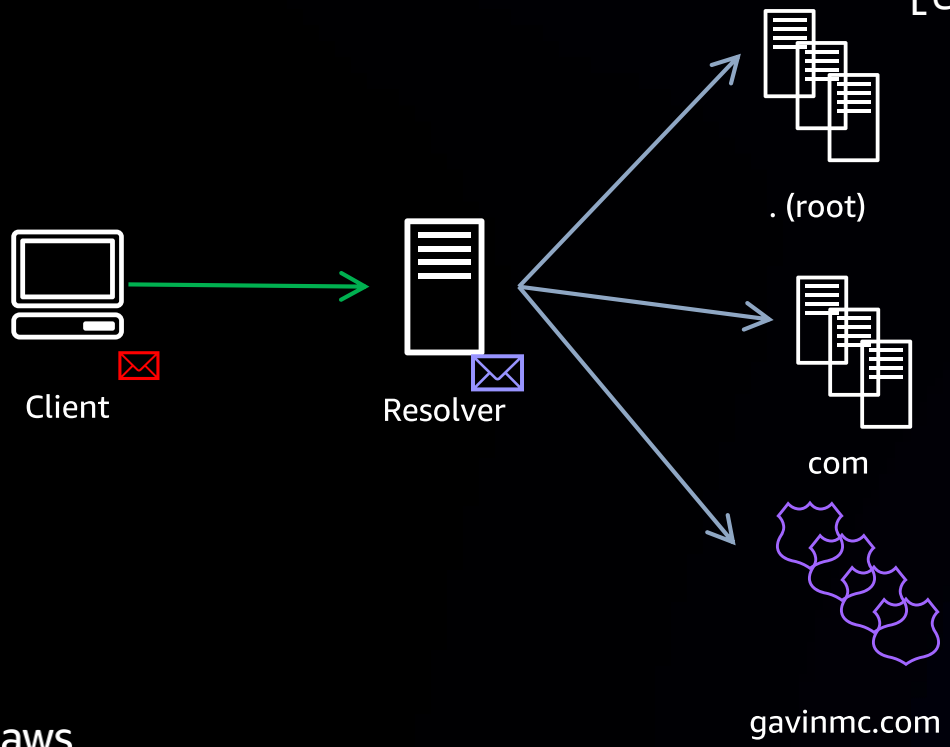


Query: www.gavinmc.com/A



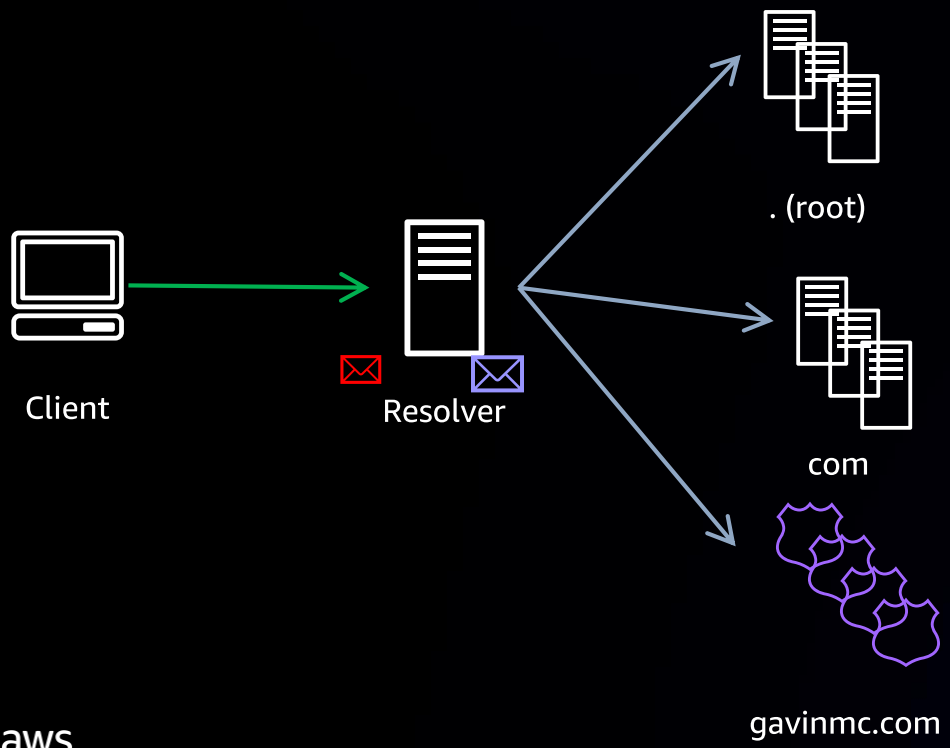
Query: www.gavinmc.com/A

```
;; 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.
[etc]
```



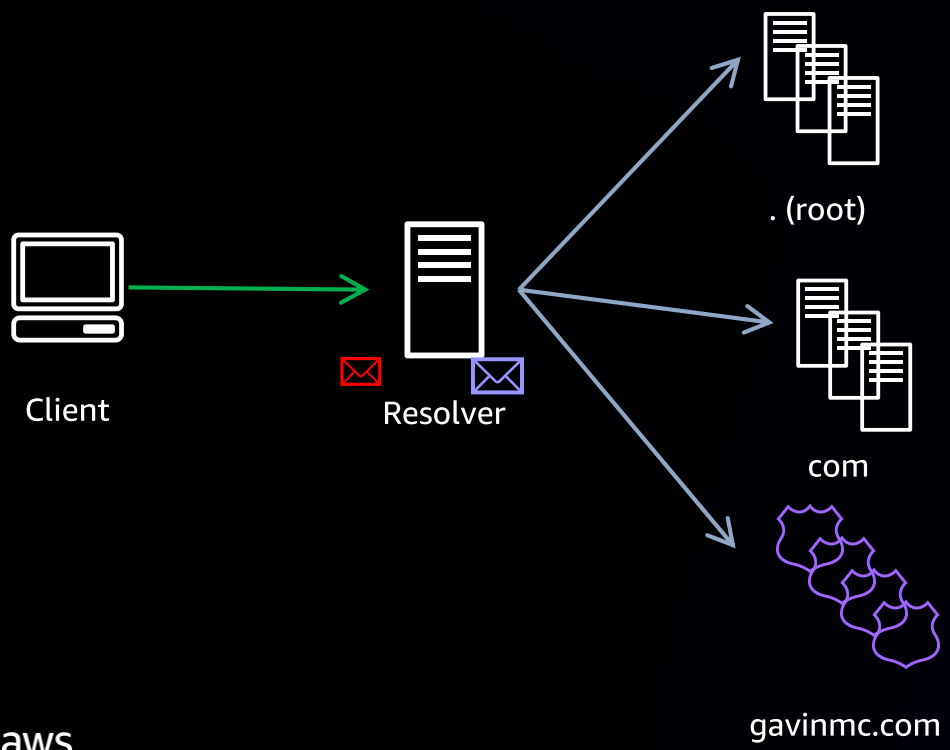
Query: www.gavinmc.com/A

```
;; 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

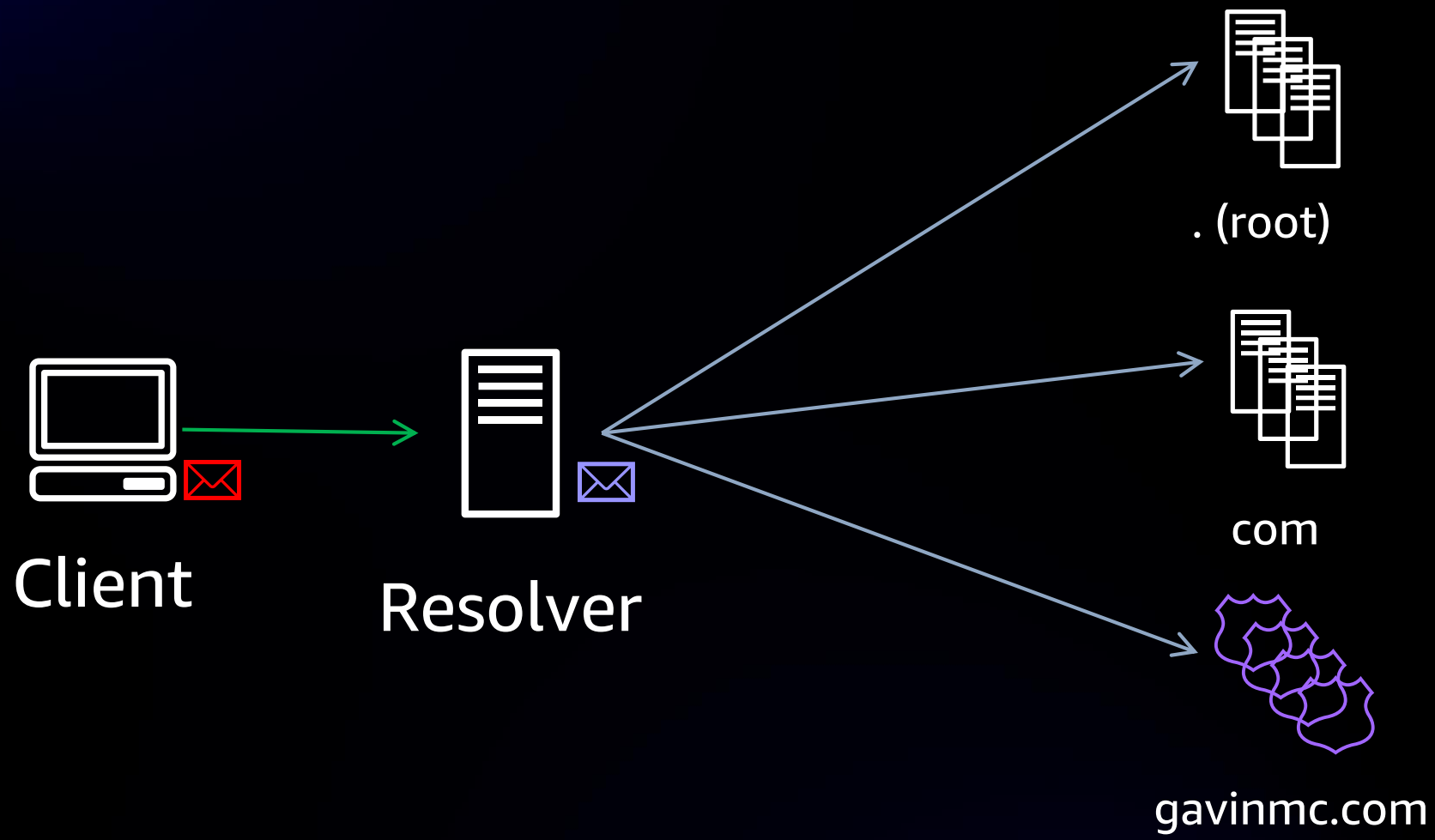
Unencrypted

- 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

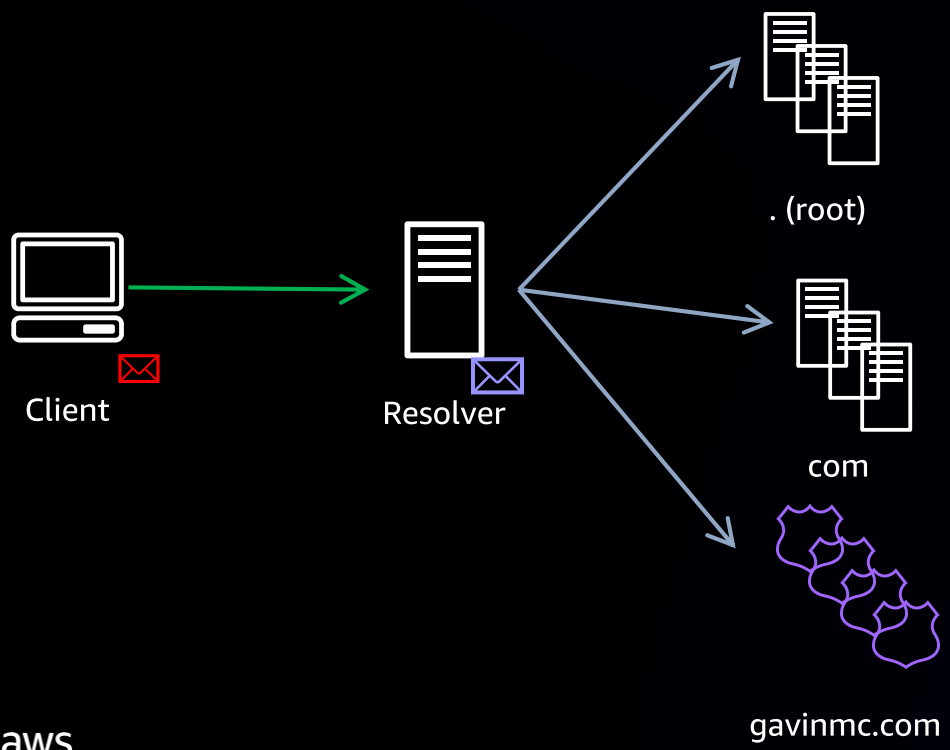
Q: How do the Resolvers verify the answers are correct?

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)

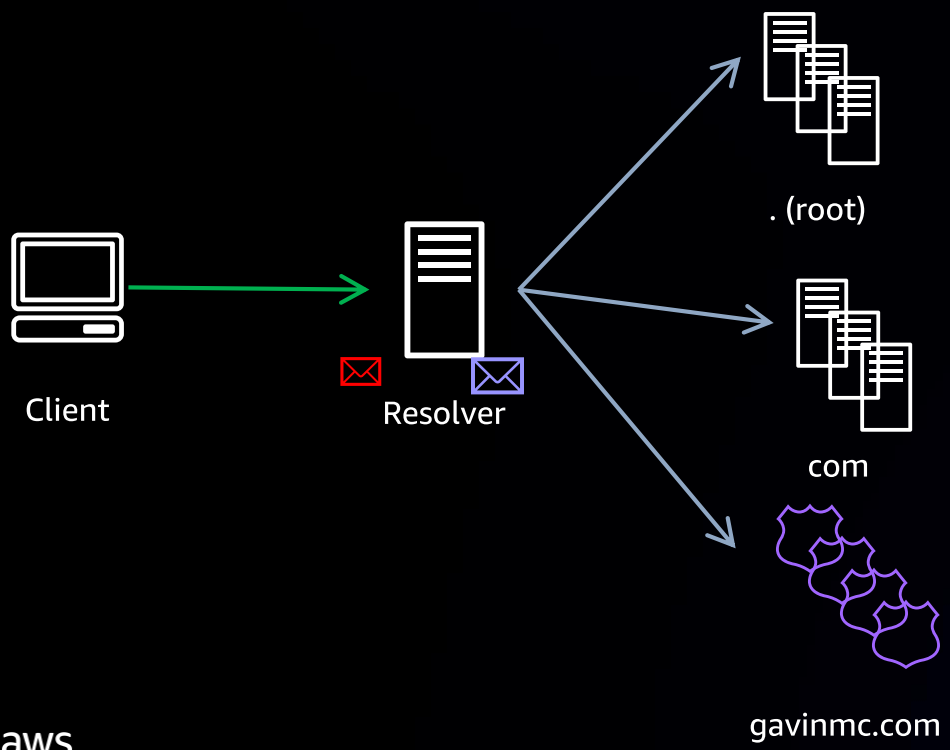
A: Resolver uses these keys and signatures to establish a chain of trust

Query: www.gavinmc.com/A



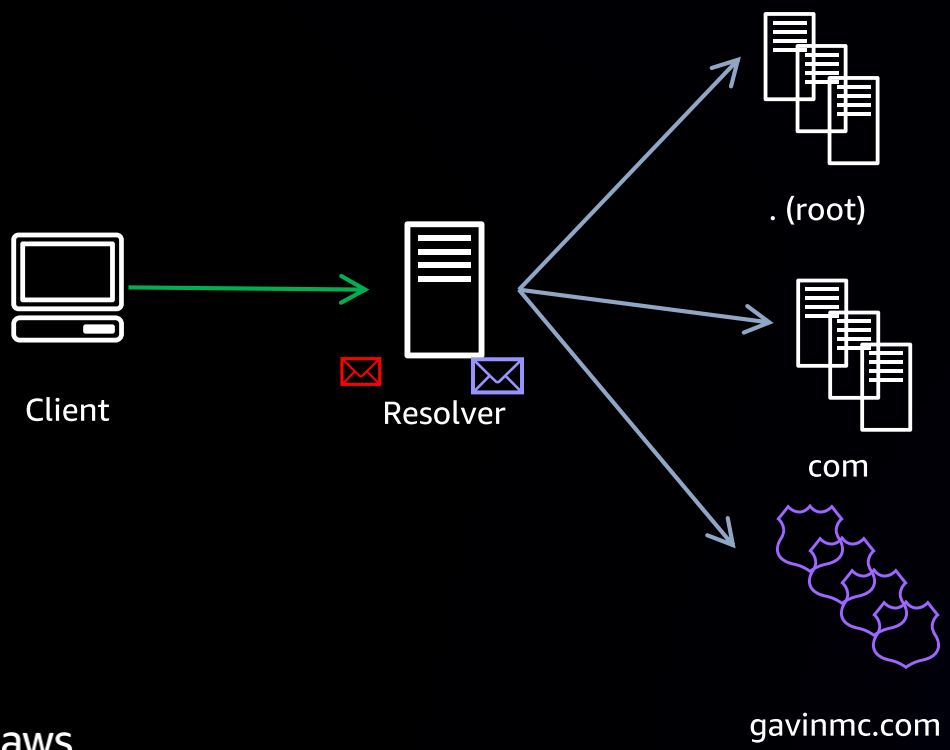

```
;; QUESTION SECTION:
;www.gavinmc.com.          IN      A

;; 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 .
        IdySHCgsyzyXDxPxMjEuIK/z9oLeY2SFfvnWPczafF/zEf7bb1hbXXDy
        SI88ZVYILET2lGl/he8cqiRbVxUE7N84lathHOR7wmWJSzVZx0coaWvW
        wq8wCKkKg+THHMInySuFLh66ycUFGBp3UFMCsi51FNhavc7HZX5Bnysp
        gz8fKrFEPWWcVCsbqkAgCfGz8r74MI6ivtA+I16doIbGAcIqbbSjrRNc
        L1YNQzmdkCaMFu8Ijwkweu4TeMW8ZH+w9NM8N2YuKJ+69hekk1gnjsu6
        TP2KOz9had4EUn/sE/X/DH+uUnYJqqOj7KXXqfiuAz8eJ6InYfbbxRz6
        7KL1Eg==
```

Query: www.gavinmc.com/A




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

;; ANSWER SECTION:
COM.            86400   IN      DNSKEY  256 3 8
        AwEAAcVw3p3LhwaxLdBQRAoXB0vo3GA3kZcycjjJ+D3QbR0DmSw+f3gz
        uTlPEJYUik2dMwnkZSMqR3DPn73f7DZTVDeLte9IreZfWcp4QMMinrgF
        LbvPbrK7rNKJV6j6jpjqBQ5ziwK9+yU+KX2tIUVyDjJaRR+OSiOJSMCb
        khvH+5q1EsEP0GACKL70qn/ptReSr7XyTZU58dfMptMYj6n01J8=
COM.            86400   IN      DNSKEY  257 3 8
        AQPDzldNmMvZFX4NcNJ0uEnKDg7tmv/F3MyQR0lpBmVcNcsIszxNFxsB
        fKNW9JYCYqpik8366LE7VbIcNRzfp2h9OO8HRl+H+E08zauK8k7evWEm
        u/6od+2boggPoiEfGNyvNPaSI7FOIroDsnw/taggzHRX1Z7SOiOiPWPN
        IwSUyWOZ79VmcQ1GLkC6NlYvG3HwYmynQv6oFwGv/KELSw7ZSdrbTQ0H
        XvZbqMUI7BaMskmvgm1G7oKZ1YiF7O9ioVNc0+7ASbqmZN7Z98EGU/Qh
        2K/BgUe8Hs0XVcdPKrtyYnoQHd2ynKPcMMlTEih2/2HDHjRPJ2aywIpK
        Nnv4oPo/
COM.            86400   IN      RRSIG   DNSKEY 8 1 86400
        20211121182421 20211106181921 30909 com.
        Mi80vLm2bB344kzskEbI1AecHfYBBjwx972Qha2+3A+urXjgPA94ZvUJ
        dWw+klgl8jHZwLgKOP4UG7ChMNGIPWJyg3ZuMuZUnn/tUFQlhfw5mDvS
        Tt+Fe6vdJ 7TLDYcg9Pb+Ch0U1L1eoJVwIuUlE61f8O70jIqUf27E5Uav
        WAzcarnXSvbtJEDpzEurkSLeCqtZcVDpSaYtdfpZjeVzDdirASnO42Wm
        2xReOk7qf2NAnjkU2W4TmykO7Ql4OsWKcRl5GJ/UkvfqwCrJczuy5SZK
        GKi21kn3HJ/2ZiUvT/5oTPIvse2S9tmhlX4GR3Oh922cpJp6jlGVrpAz
        ZEqJUw
```

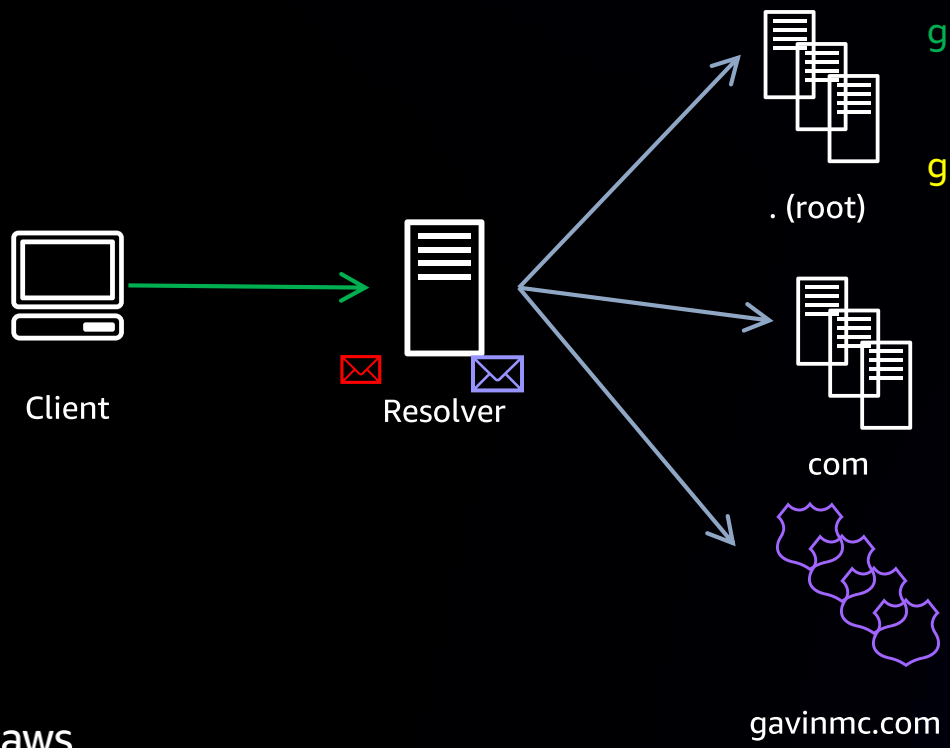
Query: www.gavinmc.com/A




```
;; 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.
        jykss3qsRJlk8PMFME/4sQK1lInp0FHO59Up2o4YIfjGvFsQc8M+fWf3
        9UhXy07kLUw4ofaYwzY5FXns7qBxB3W5DXWVj7voU7CYr5RvtBs2NVWY
        3UlxAkVWTsJGko6IiTFgGJyi3VzfYGD3yO6Rzp2U8QsPrw+21kl54QUx
        CwEg0gq2Zi1SEGJ0TL4Bk8RPdSU70Kf3GU6Rpr3lpHRUPQ==
```

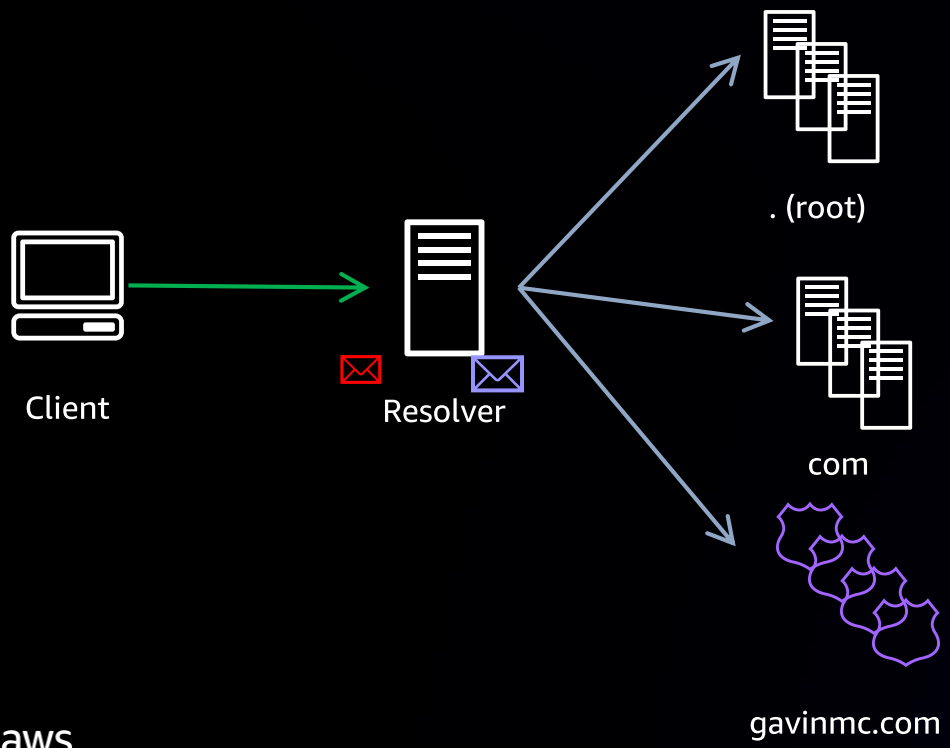
Query: www.gavinmc.com/A

```
;; 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
        uiJP307nLBI9mjydVOwDtr2lhvtChk/nsgvdA35PSYgy5kDTVcuj/RUu
        vM8jn4wE2UUivboNB/7lPEgOfdJQow==
gavinmc.com.     3600    IN      DNSKEY  257 3 13
        zZPPc+JLlriRpycjpgOh0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUBlNs
        Ed/TnnLvEZMKsqgiYPWG2RduakNEhw==
gavinmc.com.     3600    IN      RRSIG   DNSKEY 13 2 3600
        20211112020000 20211111150000 30454 gavinmc.com.
        QU+0l9lWsP2J6nLL2aIzDaTpNqwYQ2oz+YSlCkORlrgVoV1RfxYkEpsF
        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.
        DPWVzmwhnoEZQOpfLQEDF30OJqoItc3/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

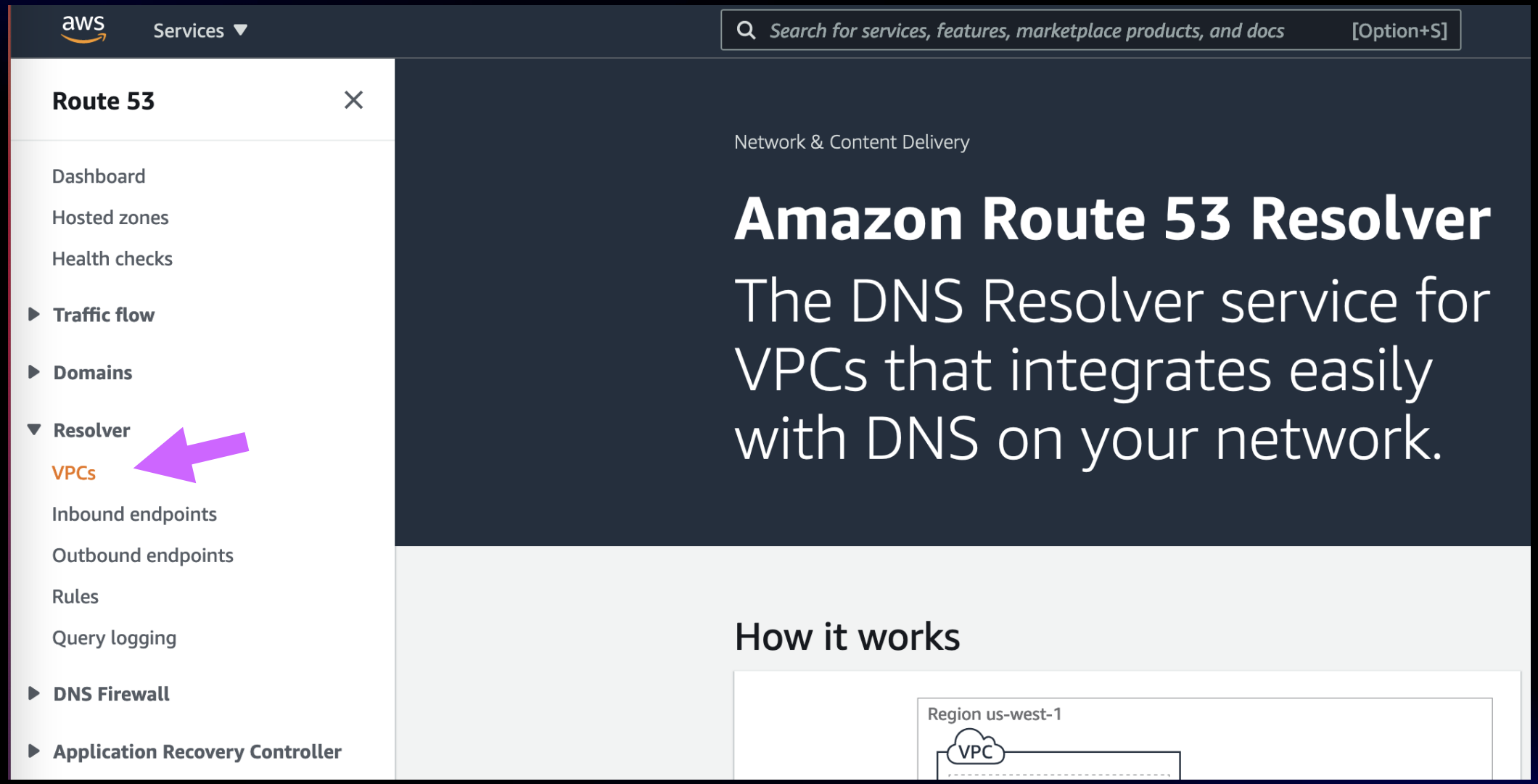
Three Route 53 DNSSEC tasks

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

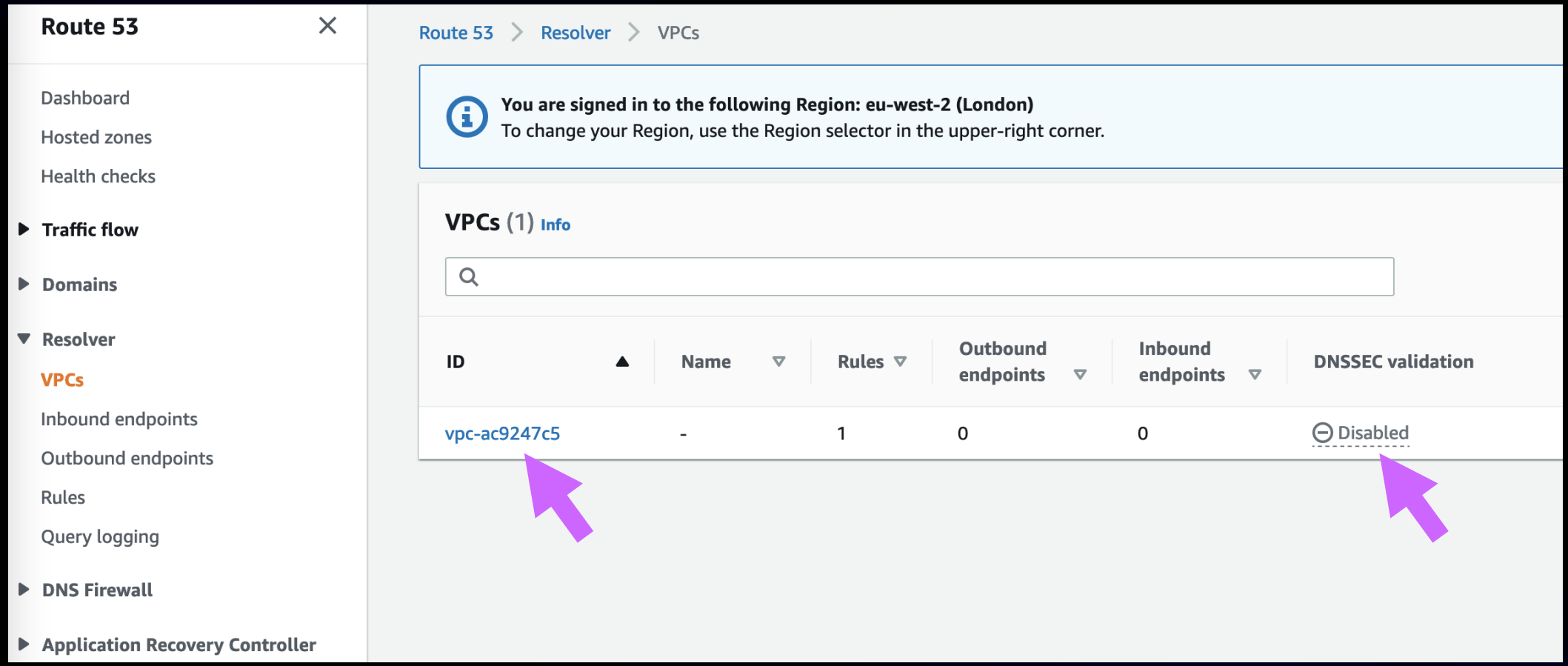
Three Route 53 DNSSEC tasks

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

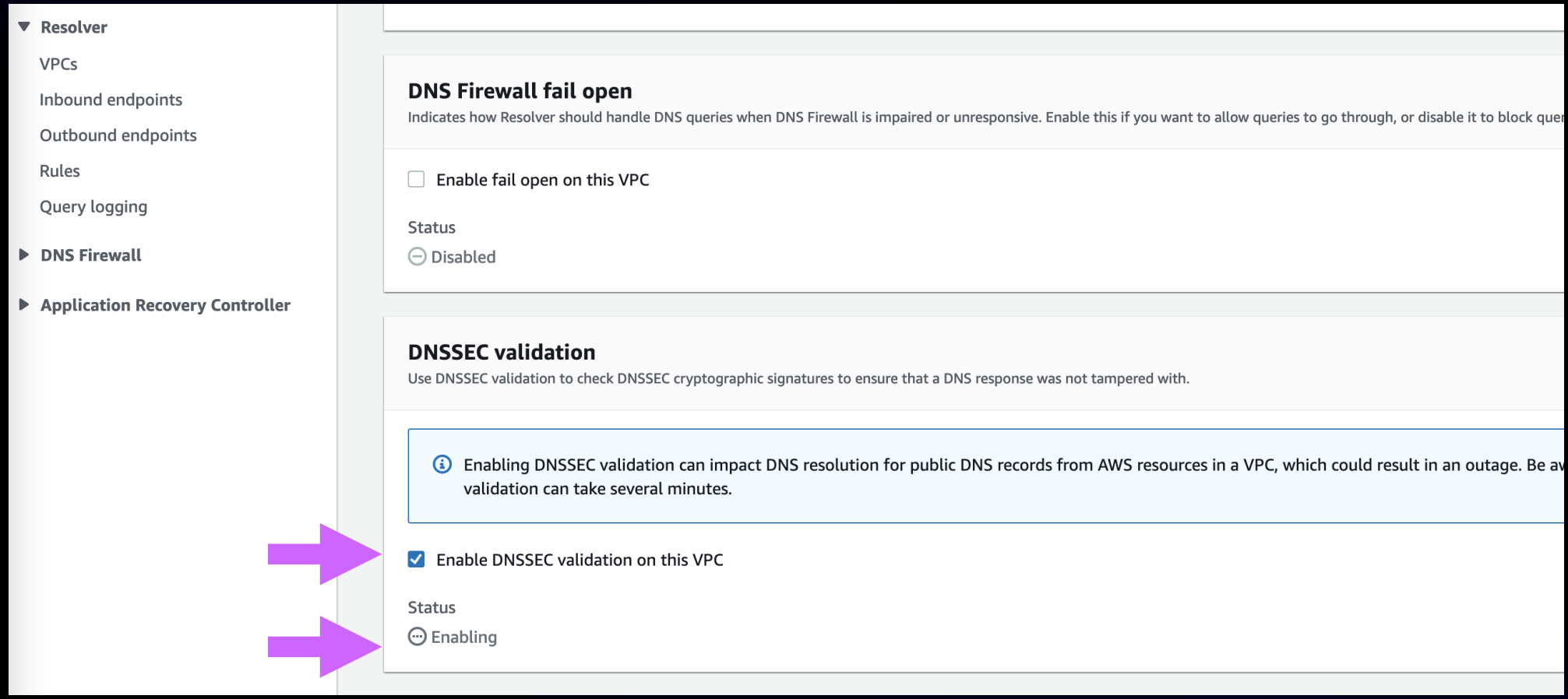
Route 53 Resolver DNSSEC validation



Route 53 Resolver DNSSEC validation



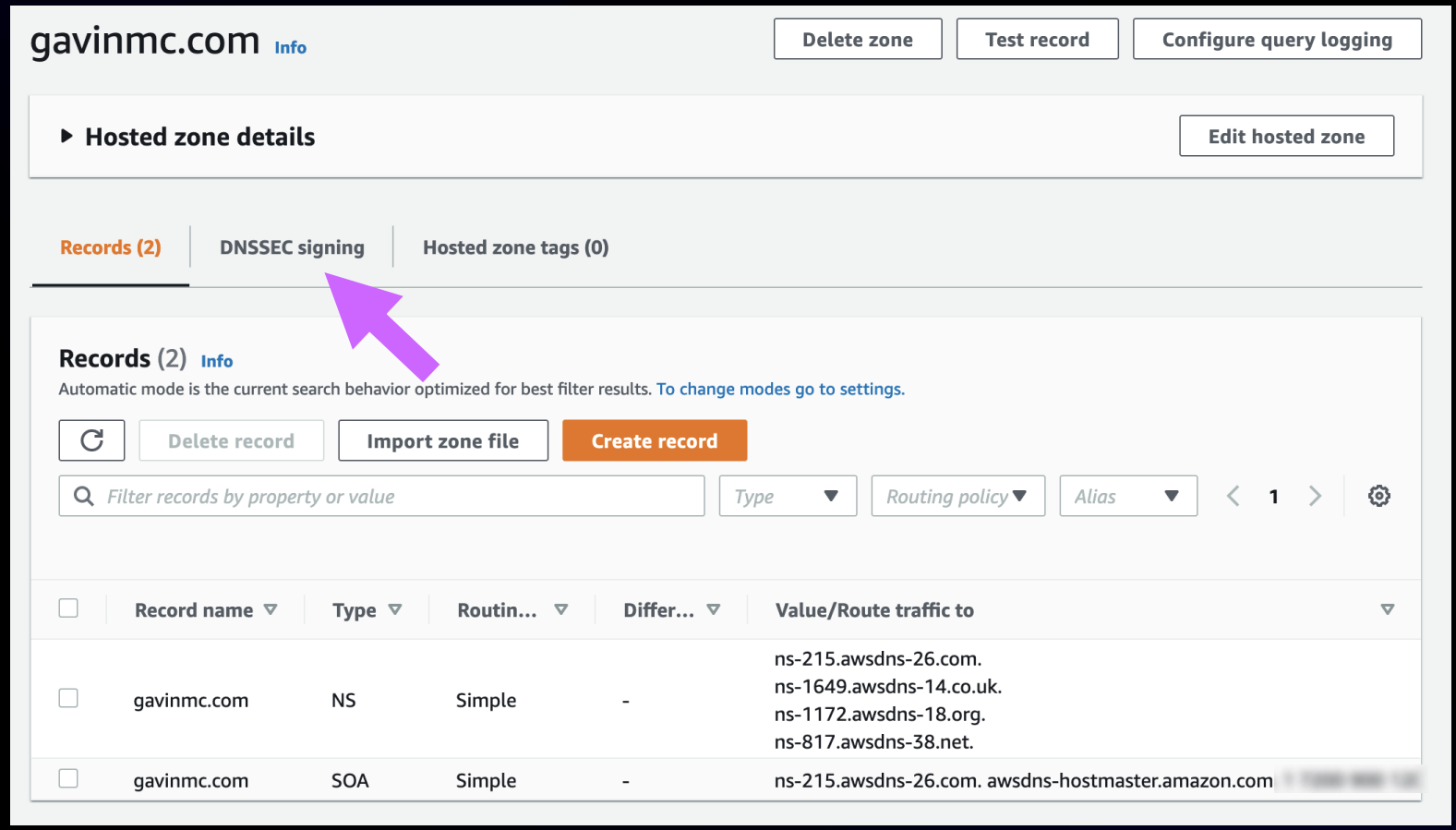
Route 53 Resolver DNSSEC validation



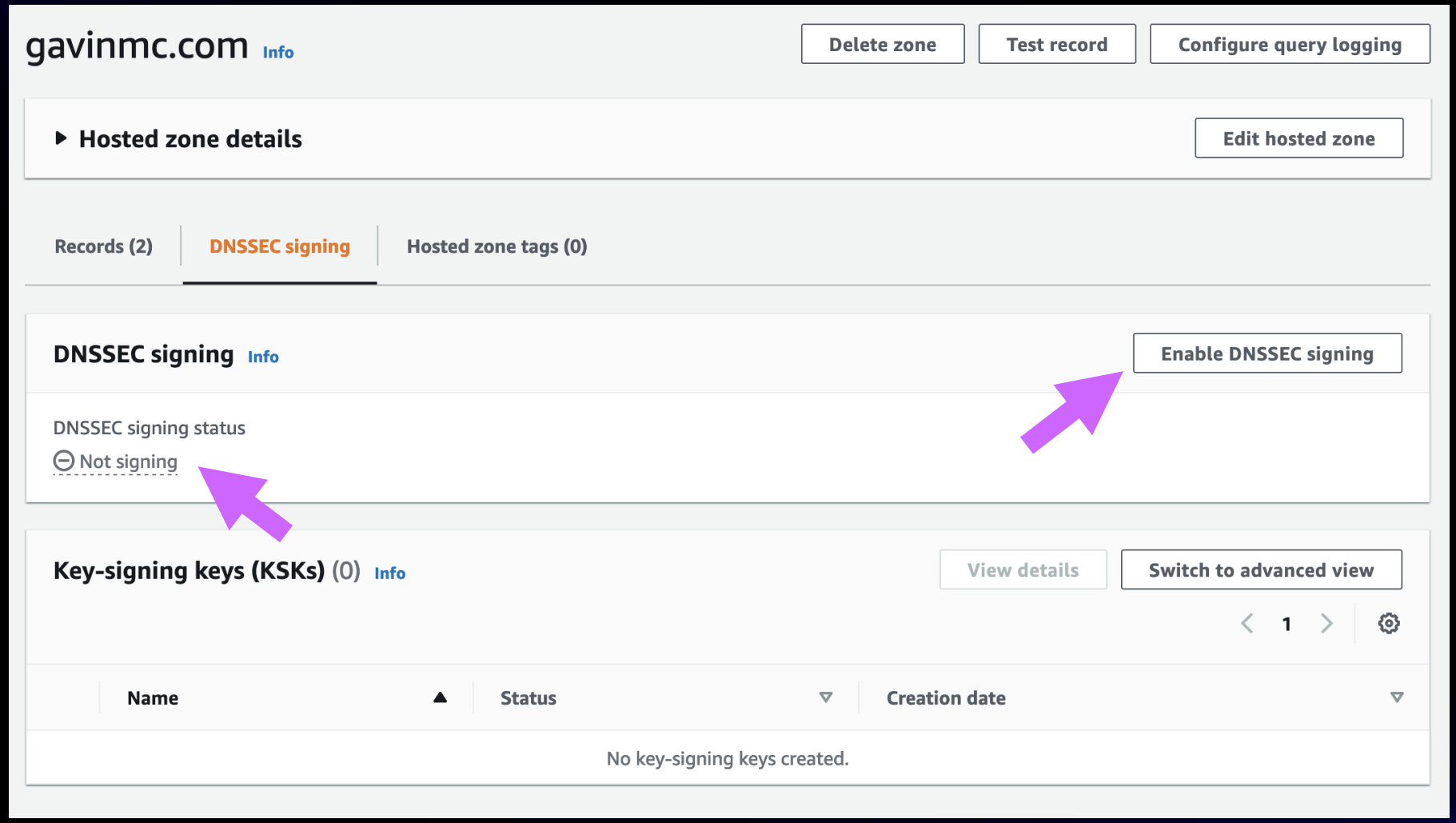
Three Route 53 DNSSEC tasks

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

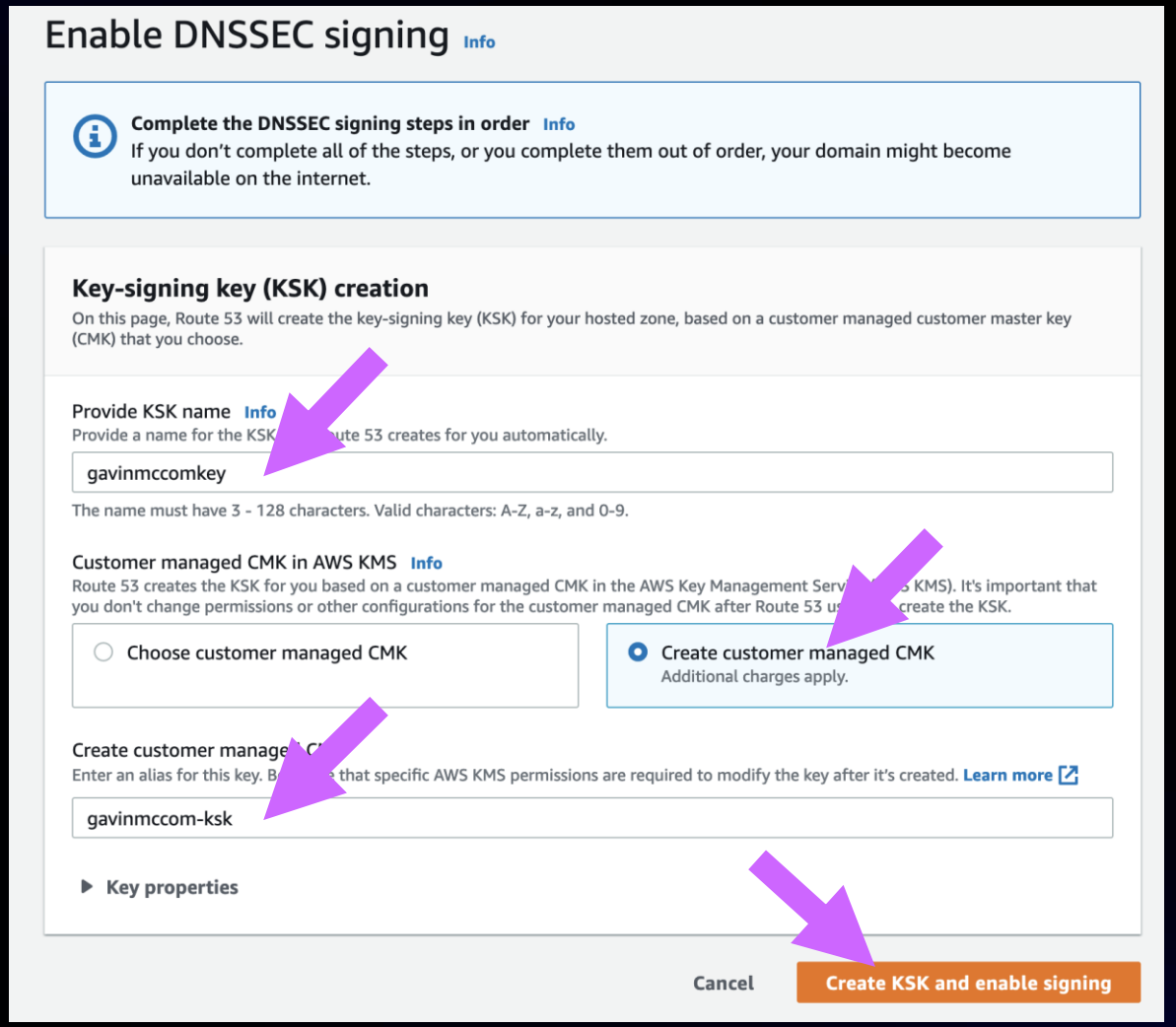
Route 53 DNSSEC signing



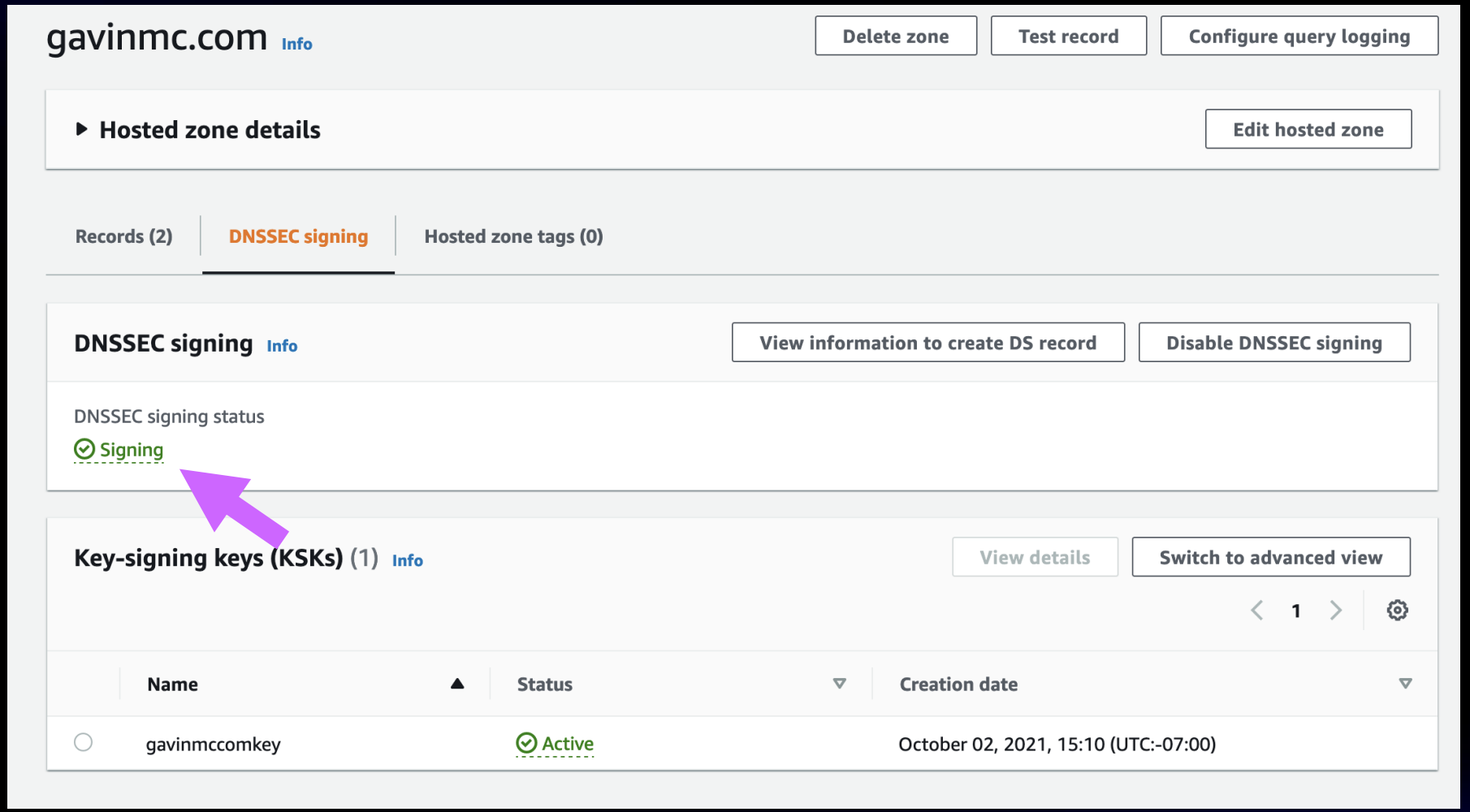
Route 53 DNSSEC signing



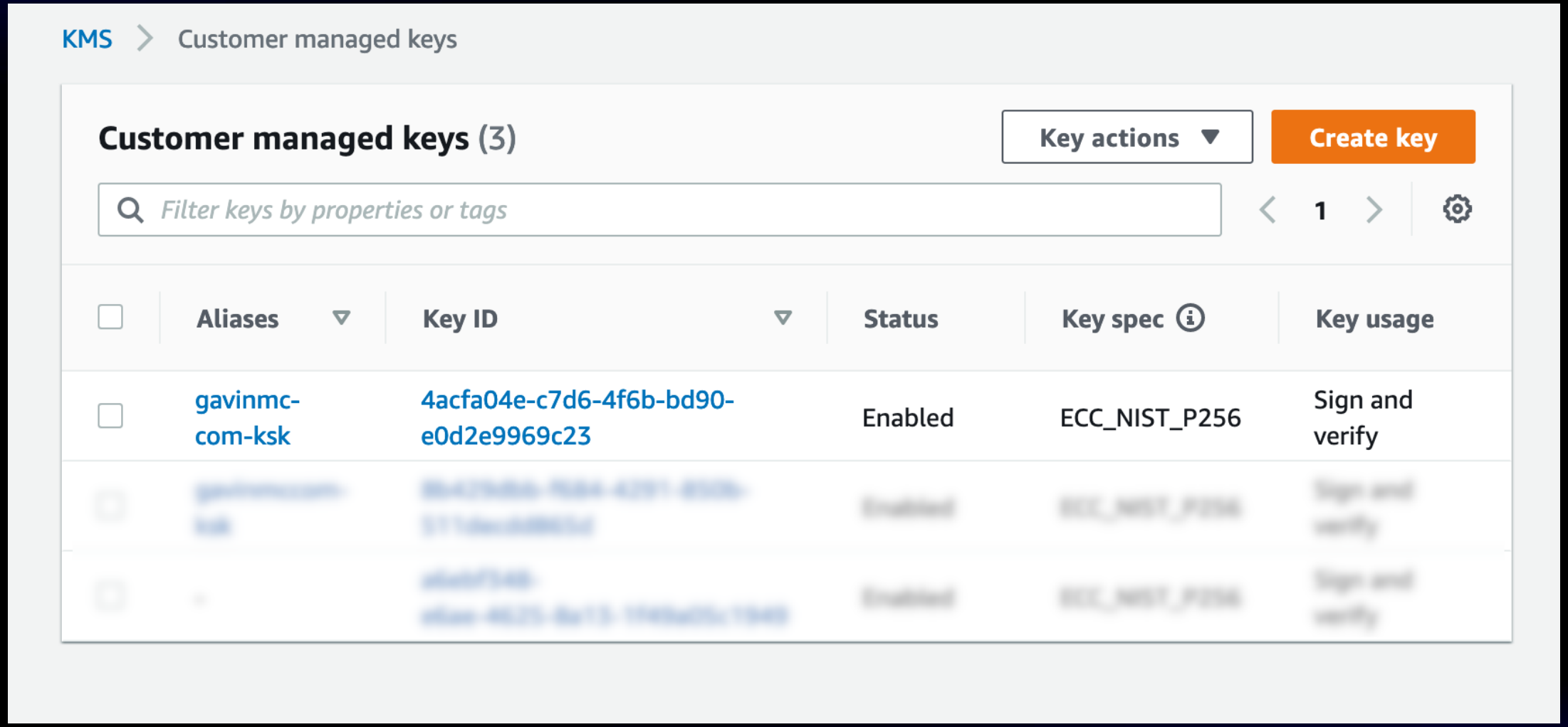
Route 53 DNSSEC signing



Route 53 DNSSEC signing

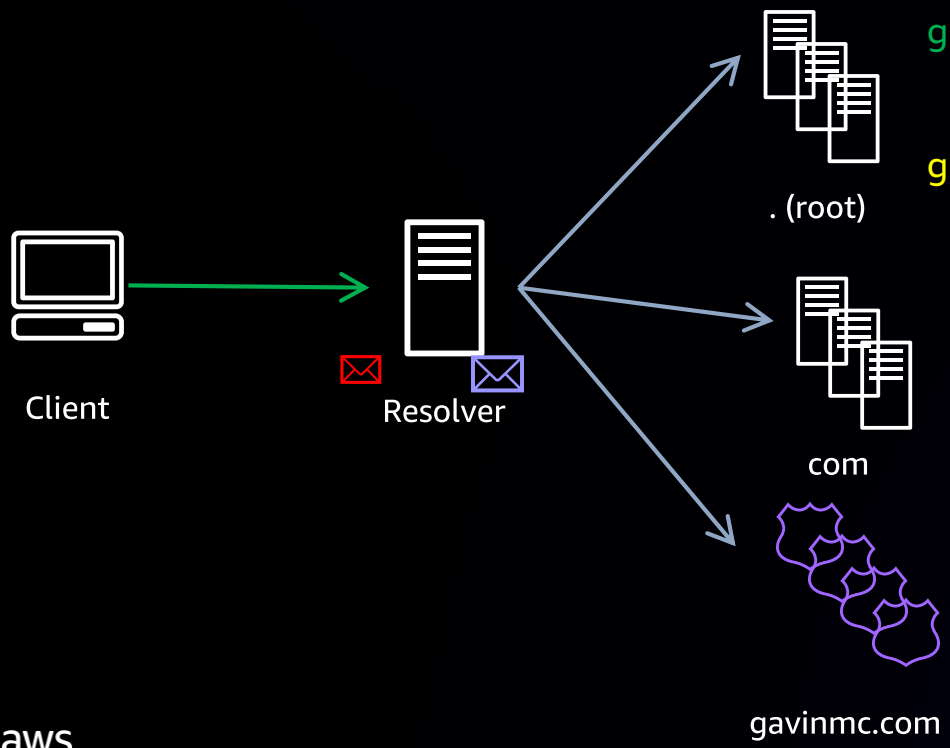


AWS KMS key



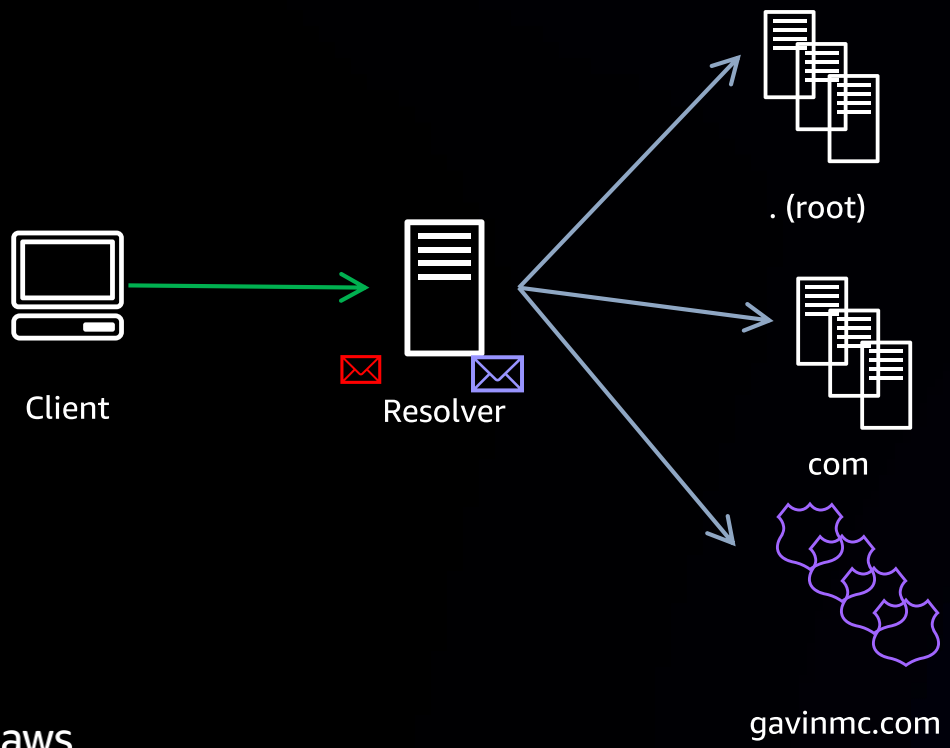
Query: www.gavinmc.com/A

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

;; ANSWER SECTION:
gavinmc.com.    3600    IN      DNSKEY  256 3 13
        hADpPOR0q+eXTZZ86uVLJOyUXrdSisGDFoHl8eRNE25JY9dMhFDndTEx
        1QePVnLskcrqbS9RxrdTpjmX/bNLzQ==
gavinmc.com.    3600    IN      DNSKEY  256 3 13
        rwHpEFvTH/D9+yF4FPiOxnlYBZ3awZqtnpm6y9y5zoNa7oxWXqRlnfwU
        whj1T7u8Qtjo/4naYq50Y6wyYmjQvw==
gavinmc.com.    3600    IN      DNSKEY  257 3 13
        zZPPc+JLlriRpycjpgOh0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUBlNs
        Ed/TnnLvEZMKsqgiYPWG2RduakNEhw==
gavinmc.com.    3600    IN      RRSIG   DNSKEY 13 2 3600
        20211112020000 20211111150000 30454 gavinmc.com.
        QU+0l9lWsP2J6nLL2aIzDaTpNqwYQ2oz+YSlCkORlrgVoV1RfxYkEpsF
        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.
        DPWVzmwhnoEZQOpfLQEDF30OJqoItc3/Tvz6Z01UPFtg7zhI78rGW4FD
        2S+VsNxyJP59ja2VVVDrrETDHhm4rg==
```

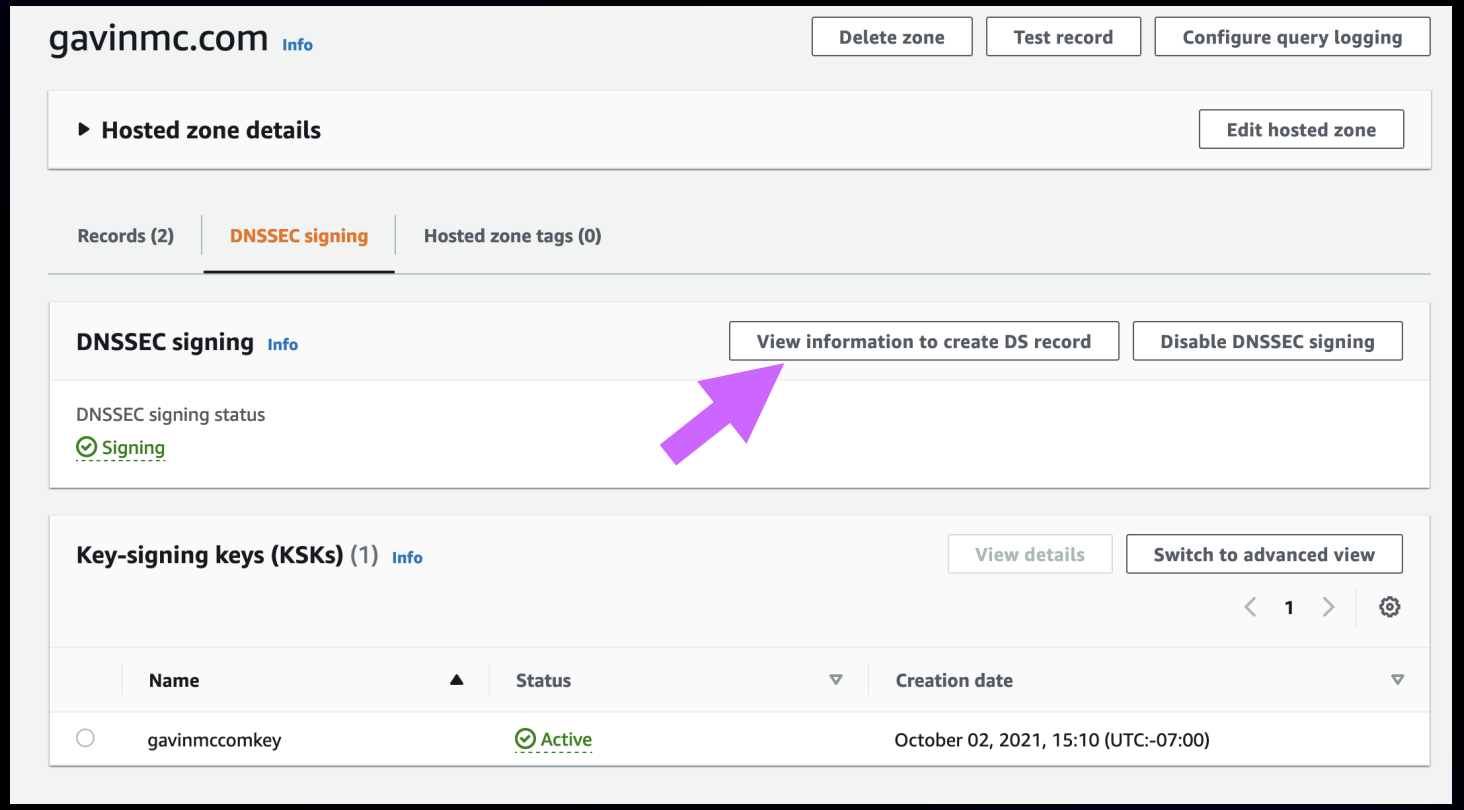


Wait (up to 2 days!)

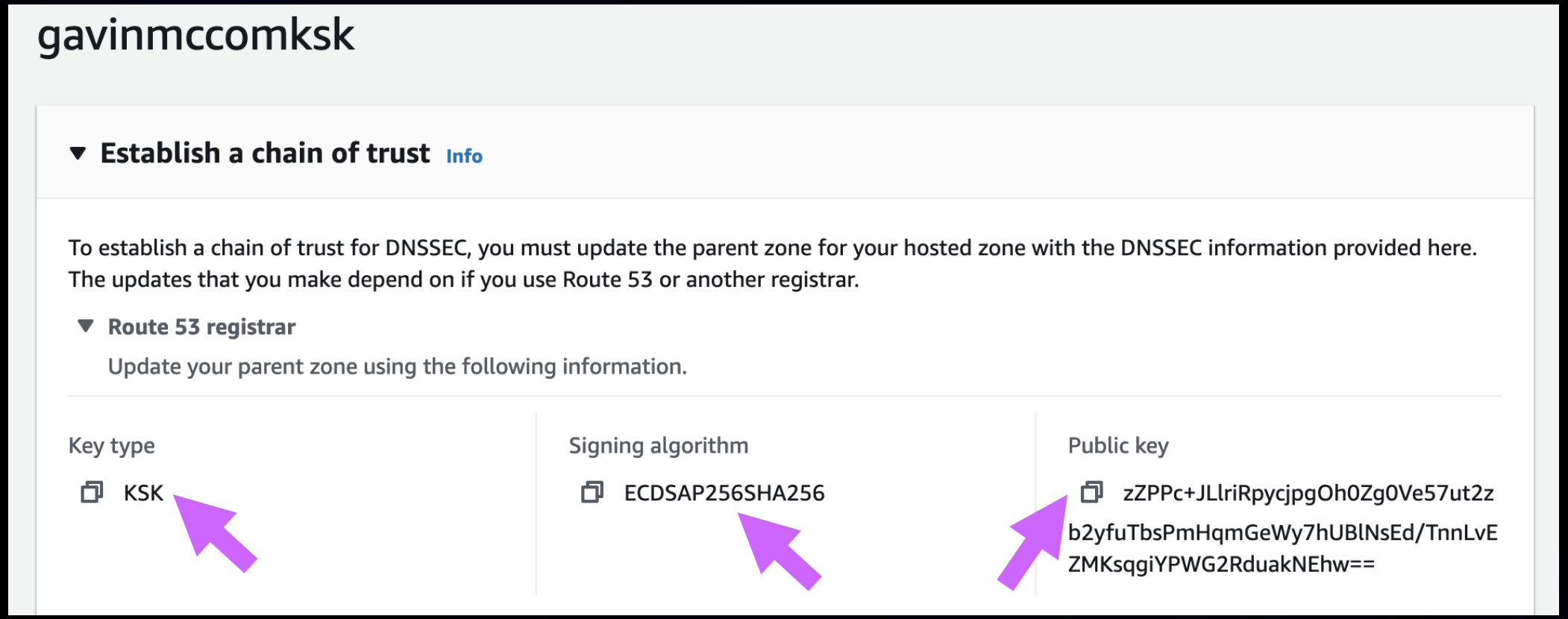
Three Route 53 DNSSEC tasks

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



Insert parent DS record



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 gavinmc.com	Digest algorithm SHA-256	Signing algorithm ECDSAP256SHA256
Key tag 30454	Digest algorithm type 2	Signing algorithm type 13
Flags 257	Digest 4E6A1A3BD530207F5E83A9C8F42937EA5BCC446293E072B02FC783B6C61EECEA	Public key zZPPc+JLlriRpycjpgOh0Zg0Ve57ut2zb2yfuTbsPmHqmGeWy7hUBlNsEd/TnnLvEZMKsqgiYPWG2RduakNEhw==
		DS record 30454 13 2 4E6A1A3BD530207F5E83A9C8F42937EA5BCC446293E072B02FC783B6C61EECEA

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		
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 Verified

Gavin McCullagh

[redacted]

Administrative contact

Gavin McCullagh

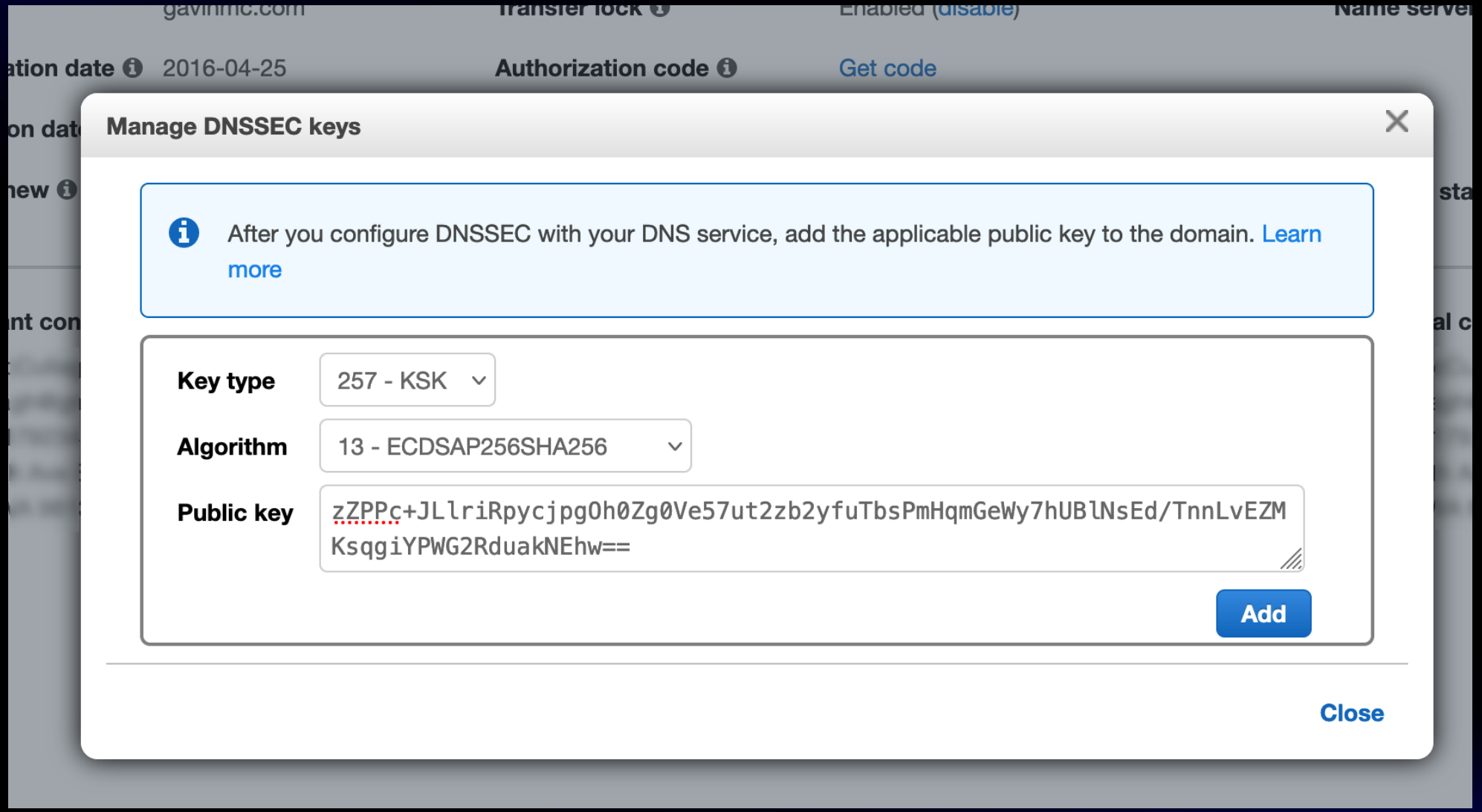
[redacted]

Technical contact

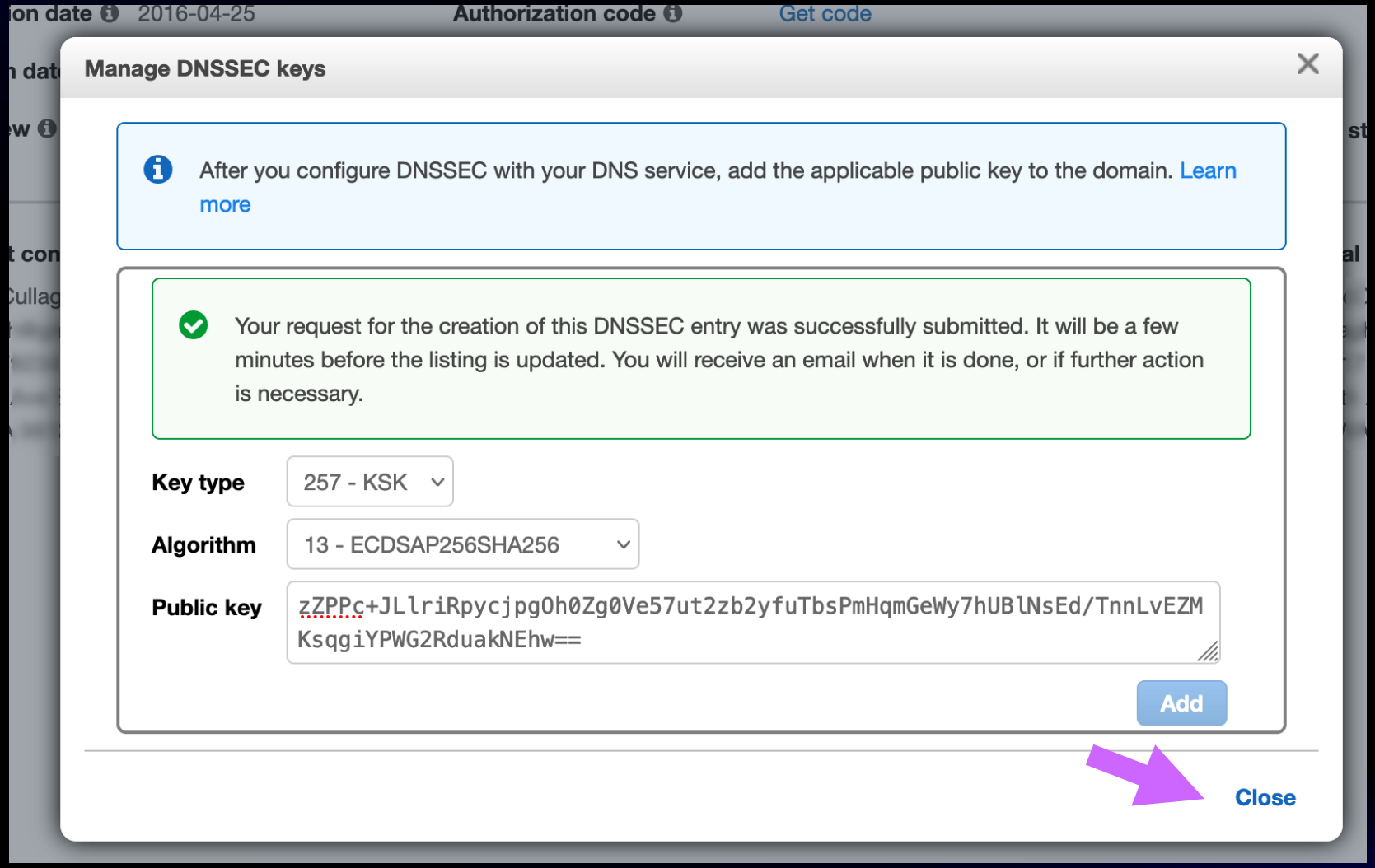
Gavin McCullagh

[redacted]

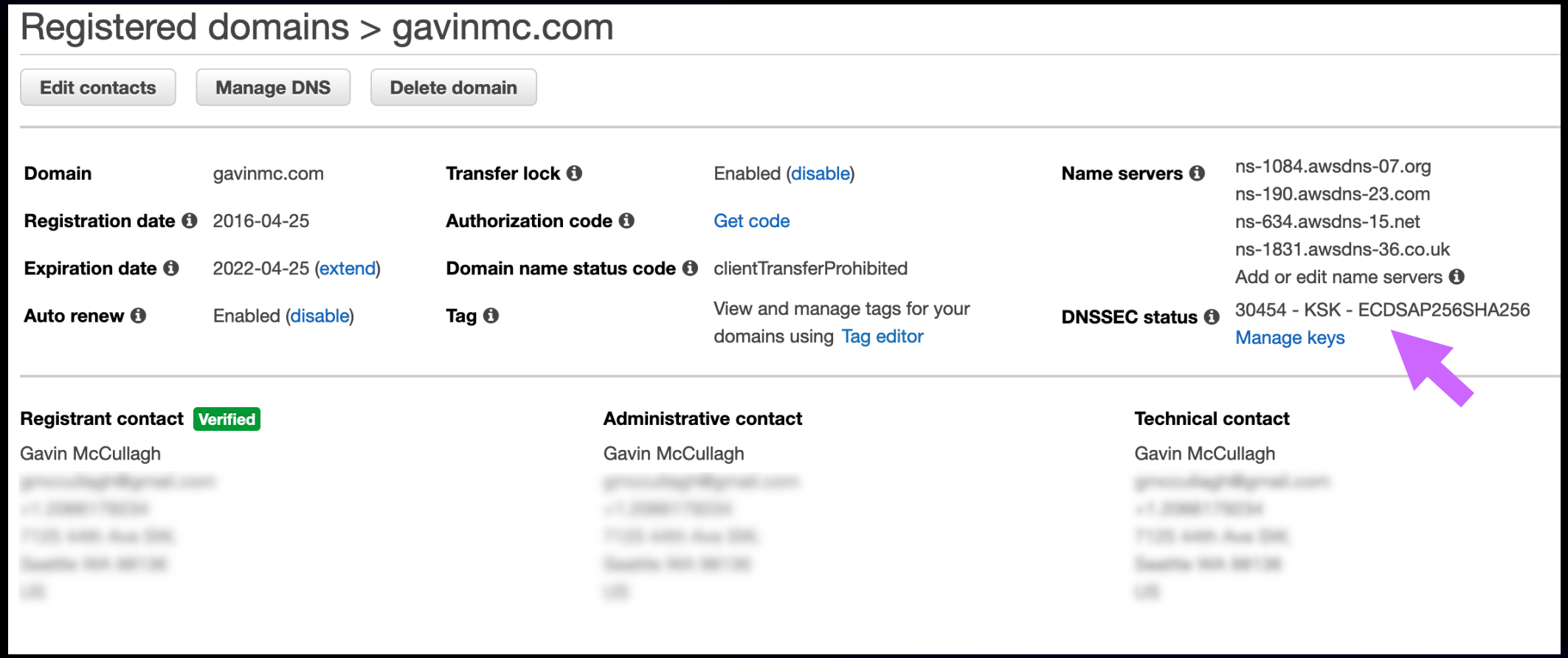
AWS KMS key



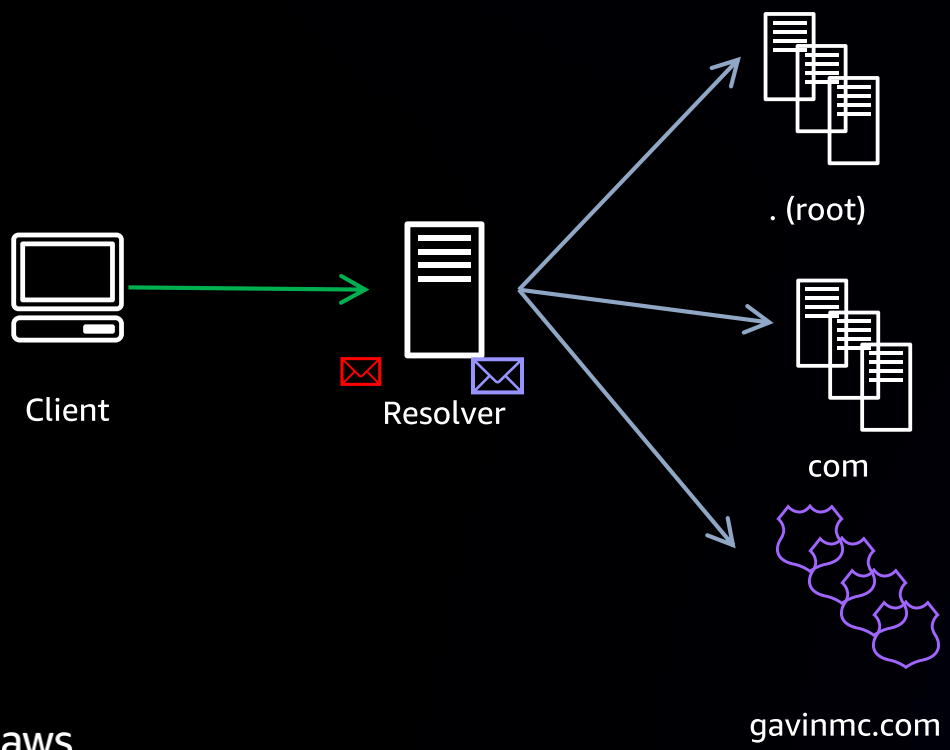
AWS KMS key



AWS KMS key



Query: www.gavinmc.com/A

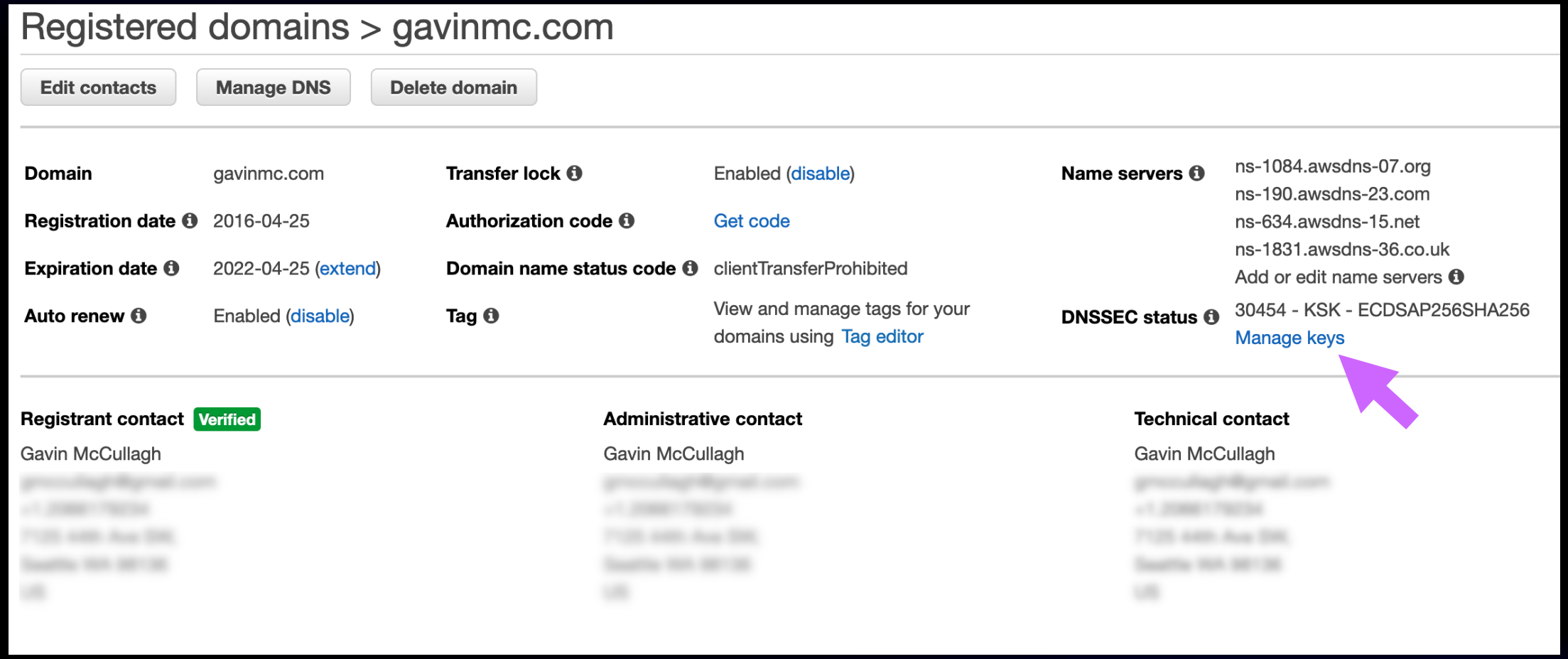



```
;; QUESTION SECTION:
;www.gavinmc.com.          IN      A

;; 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.
        jykss3qsRJlk8PMFME/4sQK1lInp0FHO59Up2o4YIfjGvFsQc8M+fWf3
        9UhXy07kLUw4ofaYwzY5FXns7qBxB3W5DXWVj7voU7CYr5RvtBs2NVWY
        3UlxAkVWTsJGko6IiTFgGJyi3VzfYGD3yO6Rzp2U8QsPrw+21kl54QUx
        CwEg0gq2Zi1SEGJ0TL4Bk8RPdSU70Kf3GU6Rpr3lpHRUPQ==
```

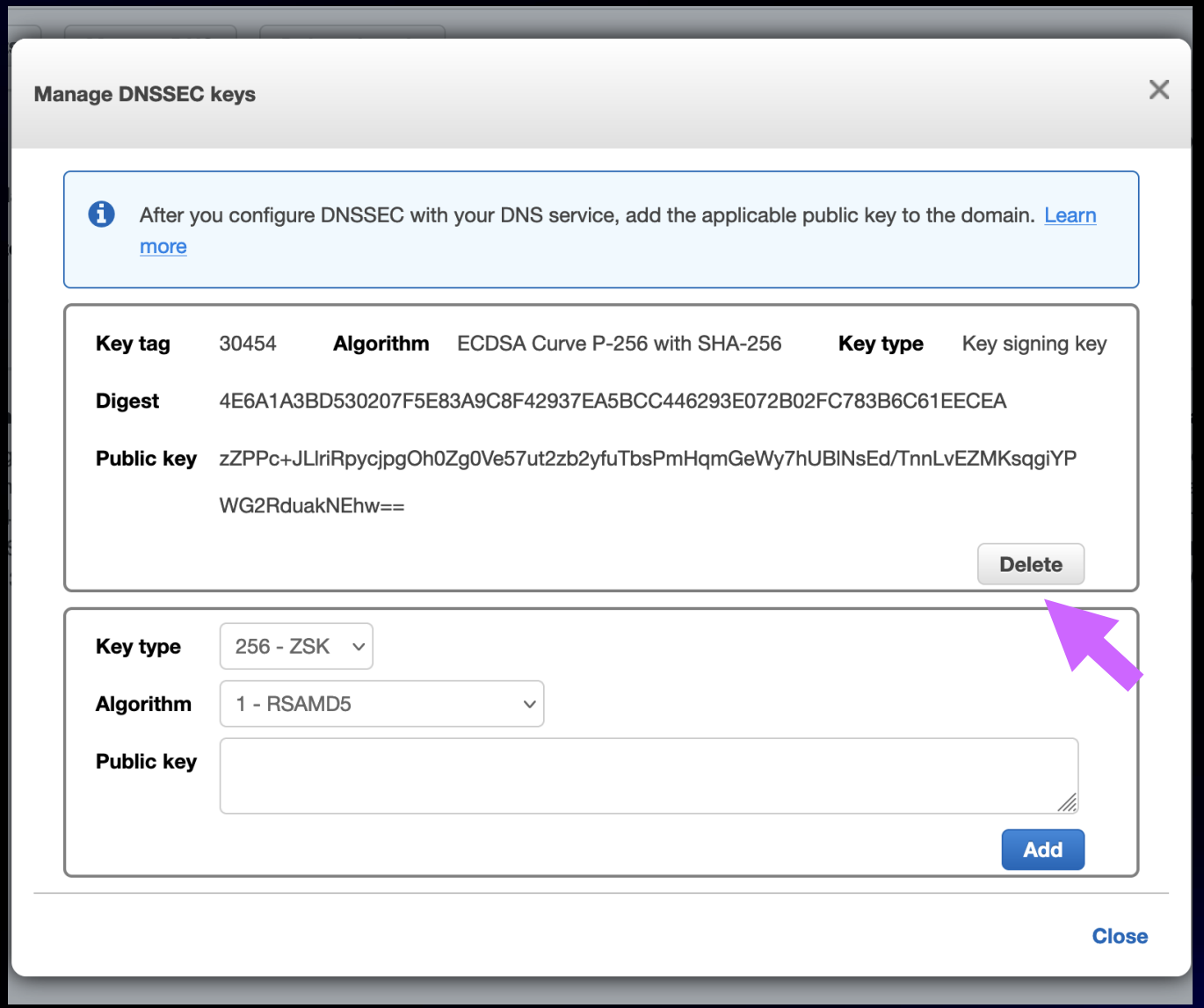
Three Route 53 DNSSEC tasks

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

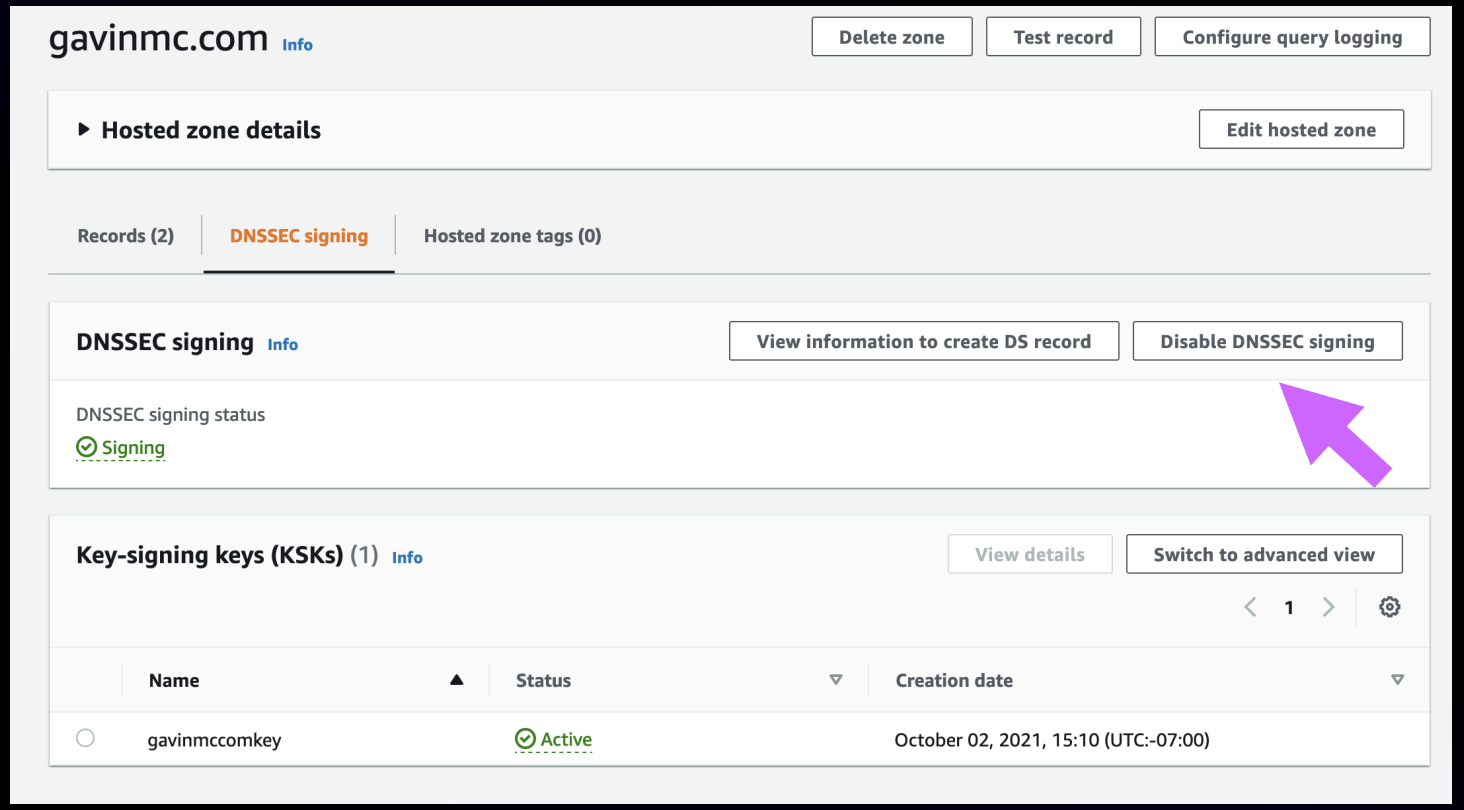


Remove the DS record set



Wait (up to 2 days!)

Disable DNSSEC



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

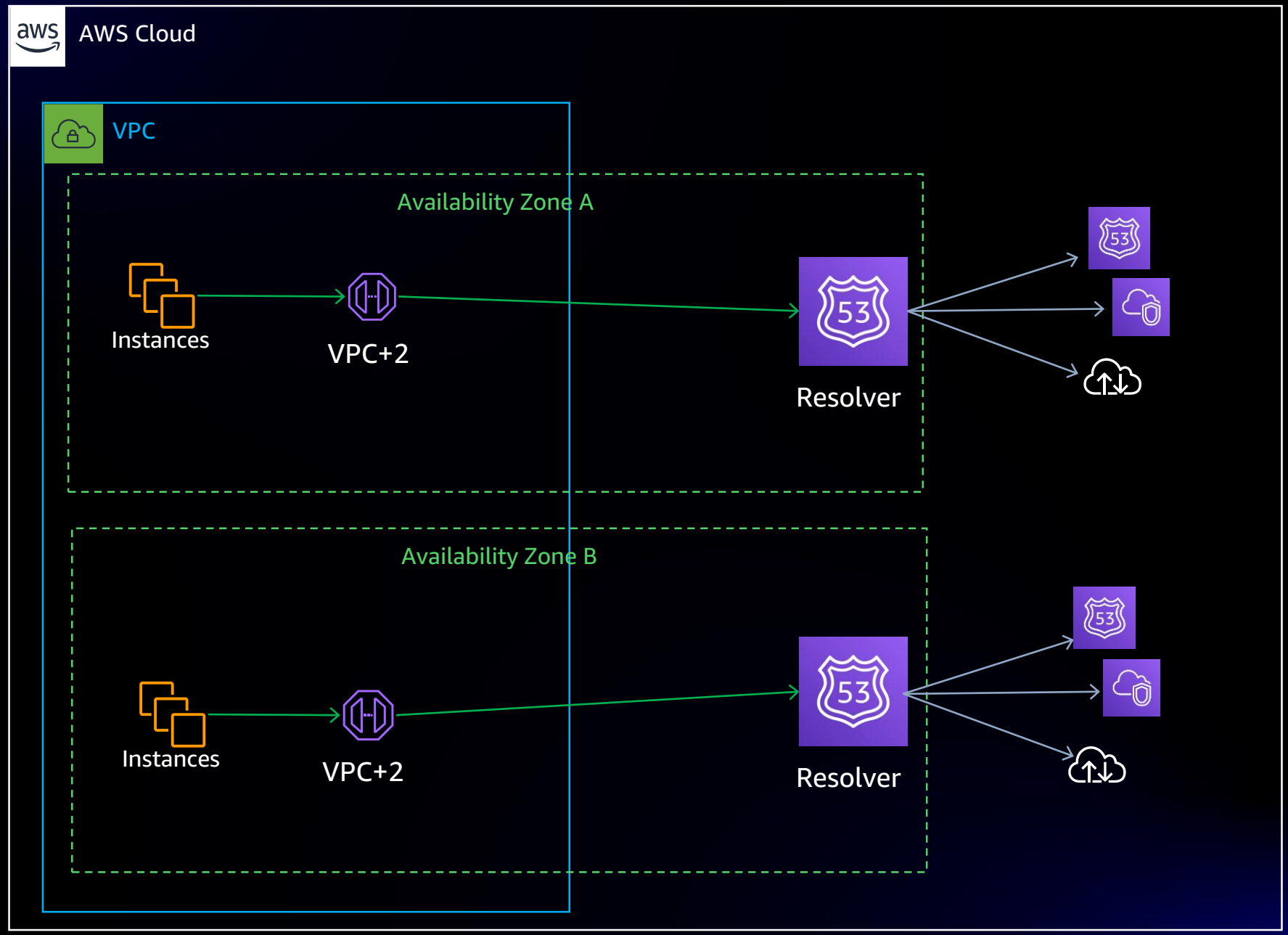
- Redundant, isolated units
- Tested recovery mechanisms

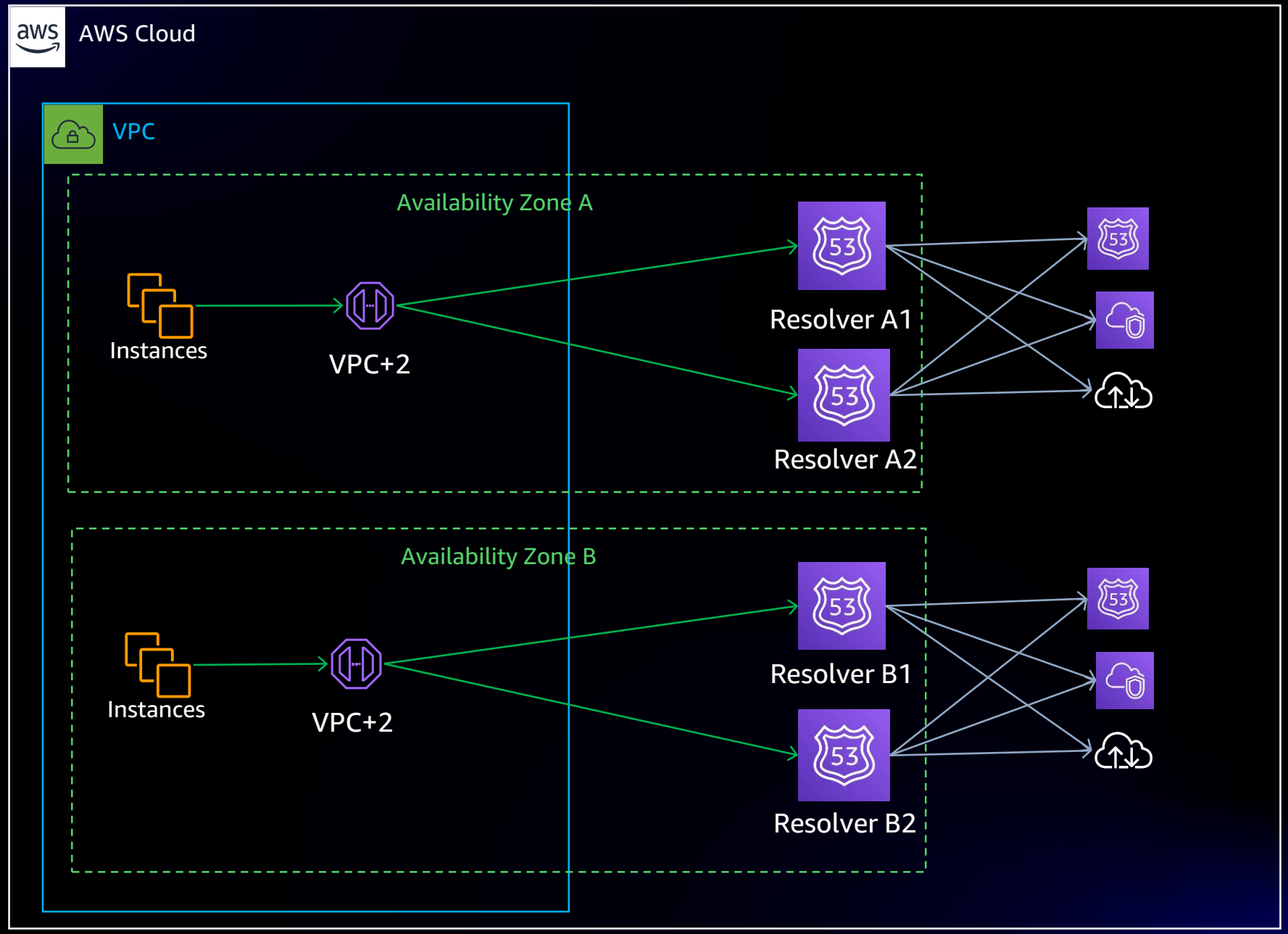
Hugely influential on Amazon and AWS

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

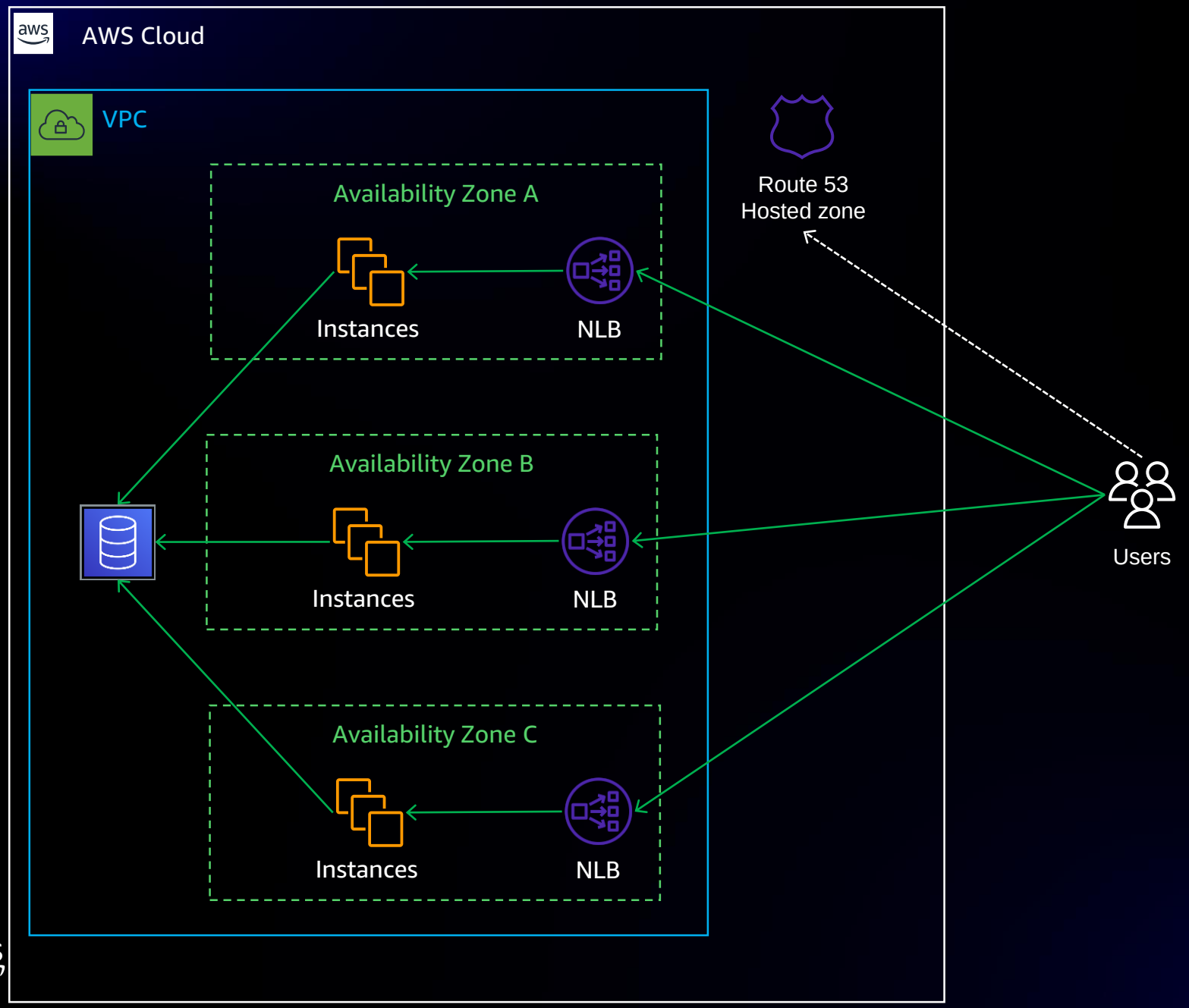
Example #1
Route 53 Resolver

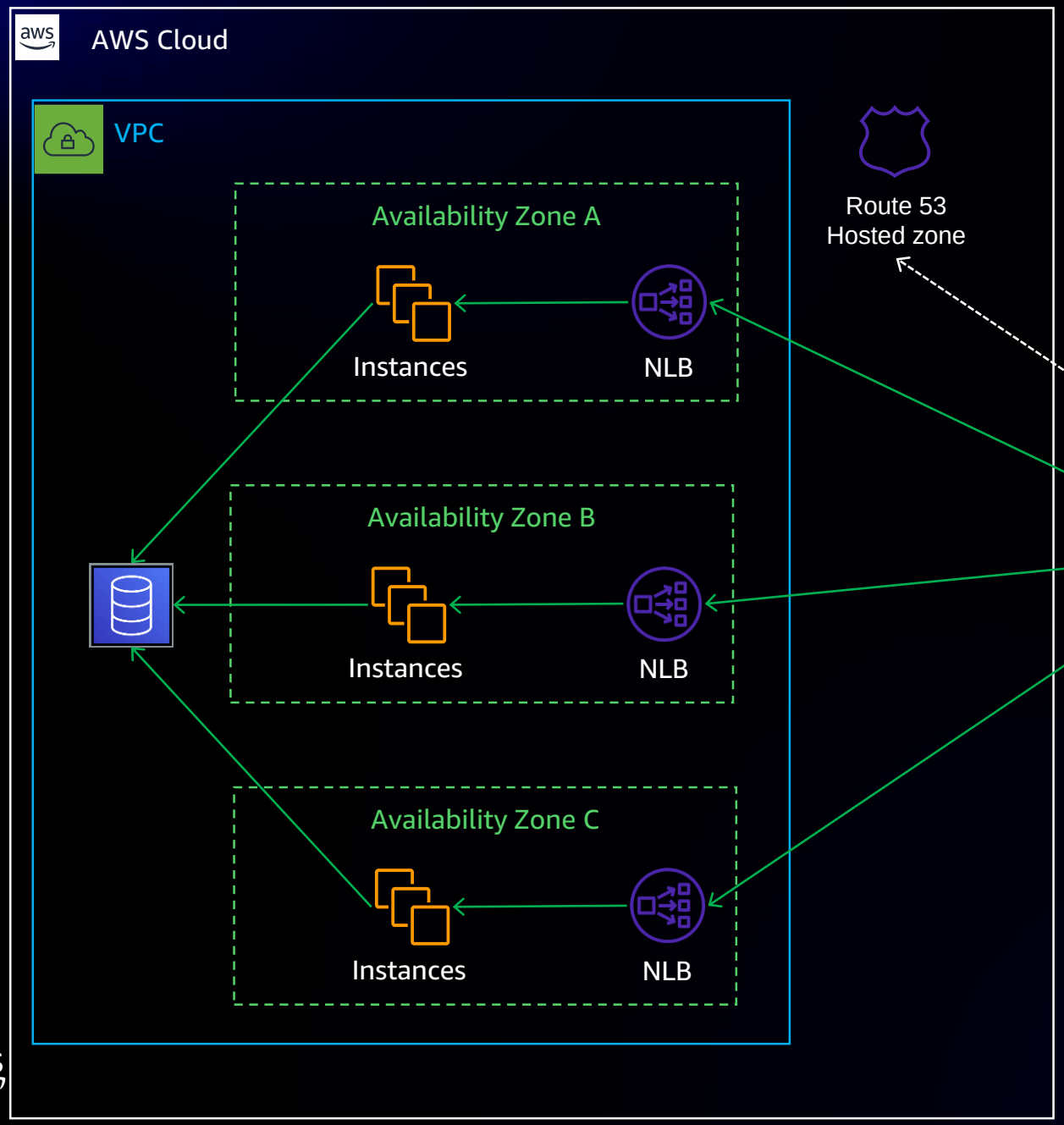




Example #2
3-AZ Web Service

Building a fault tolerant web service

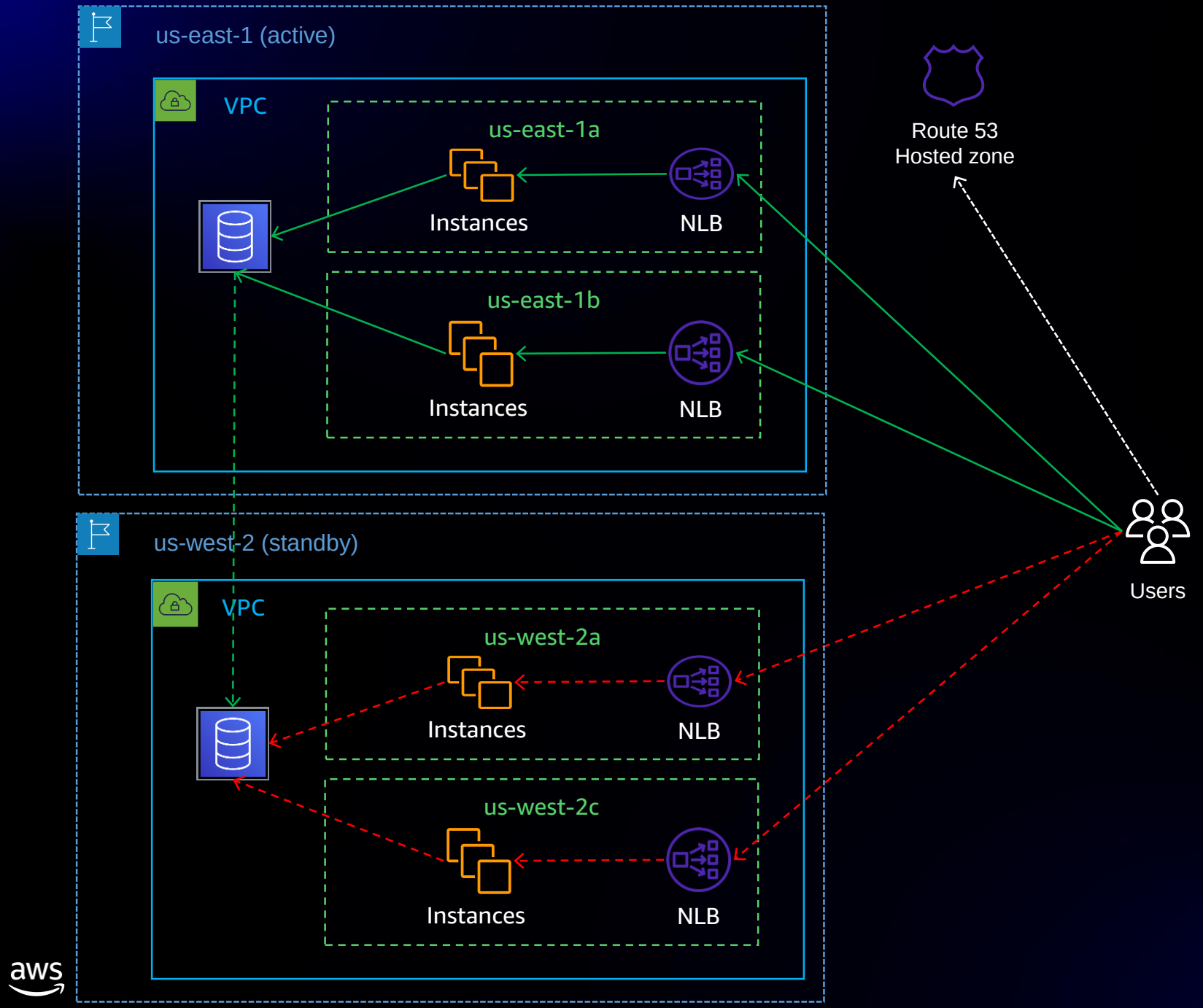


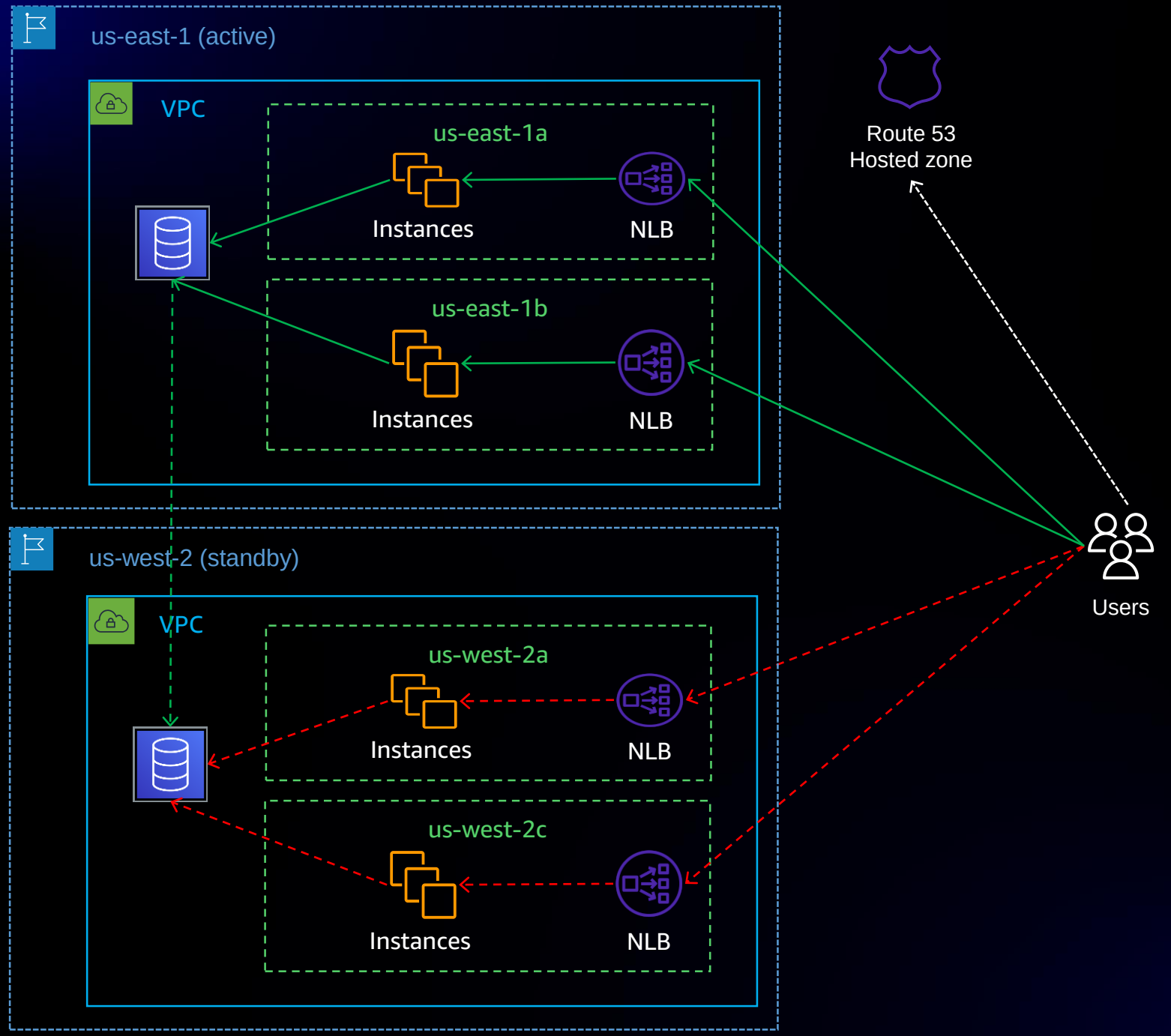


- Active-active setup
- What recovery mechanisms do we use if AZ B is failing?
- How do we make sure only one AZ is removed at a time?

Example #3
Web service with multi-Region DR

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





- Active-standby setup
- What recovery mechanisms do we use to fail over?
- How do we know the standby is ready for production?
- How do we make sure only one Region is ever in production?

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

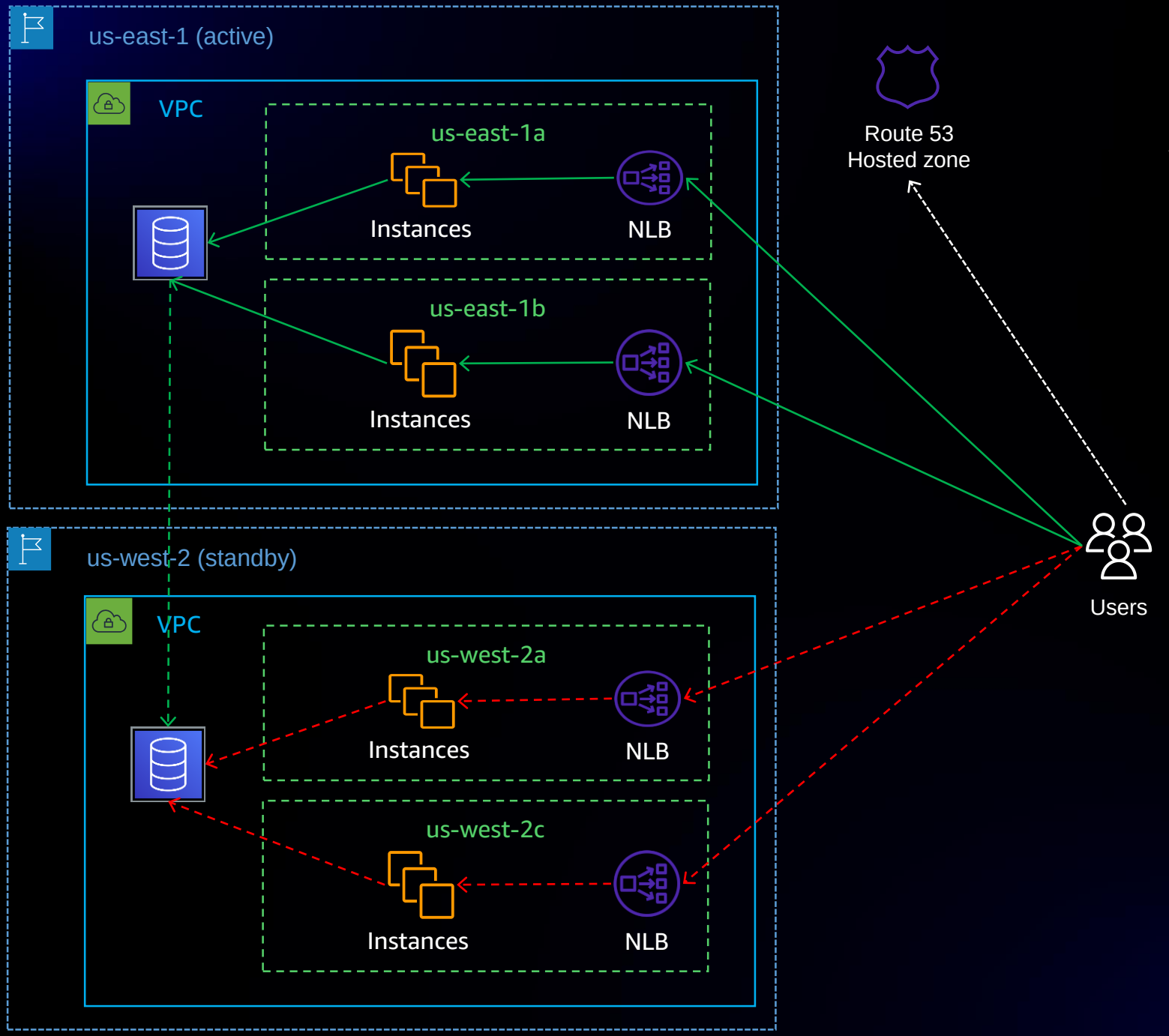
Now we have multiple replicas

- **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

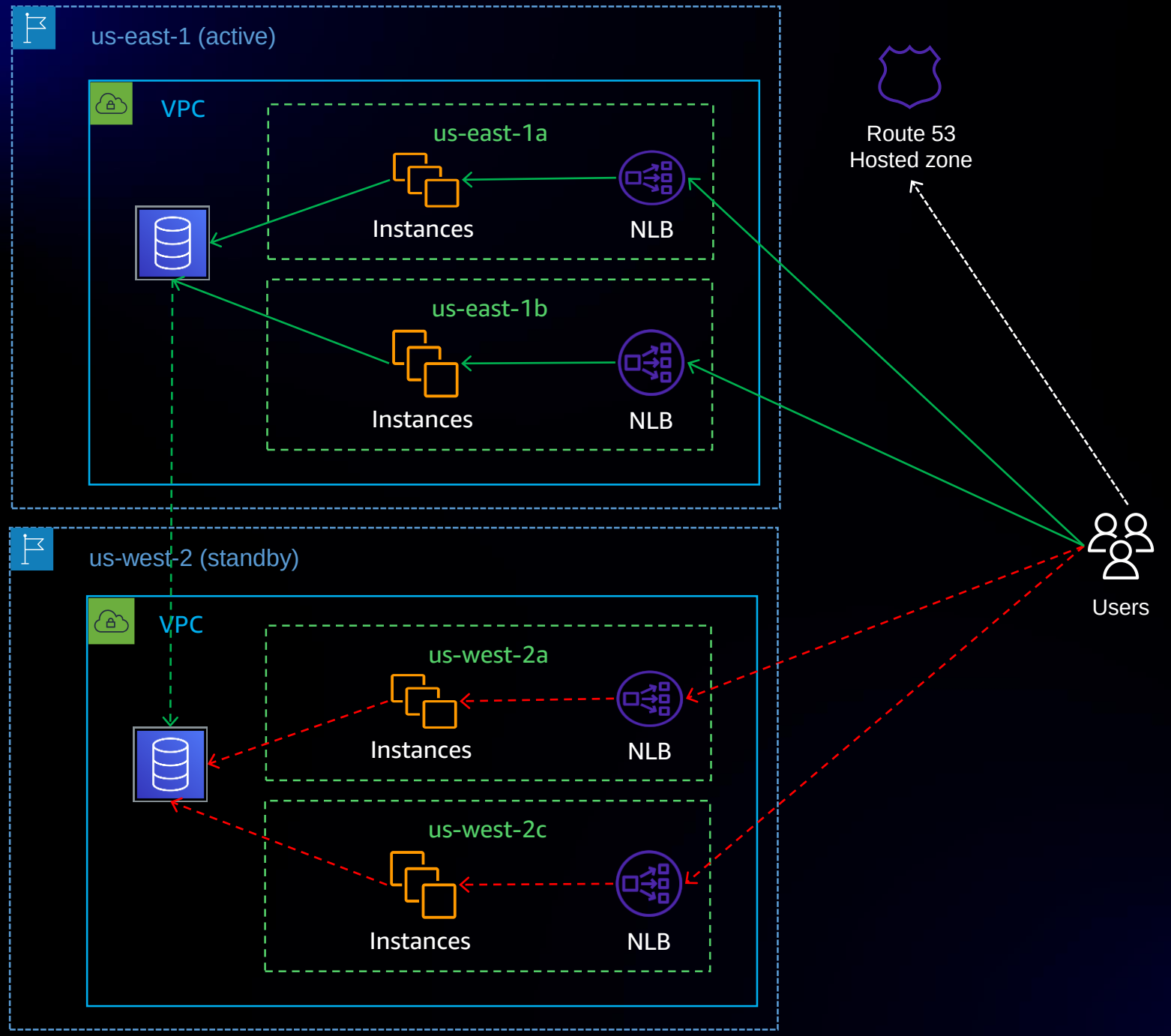
Recovery Group

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>



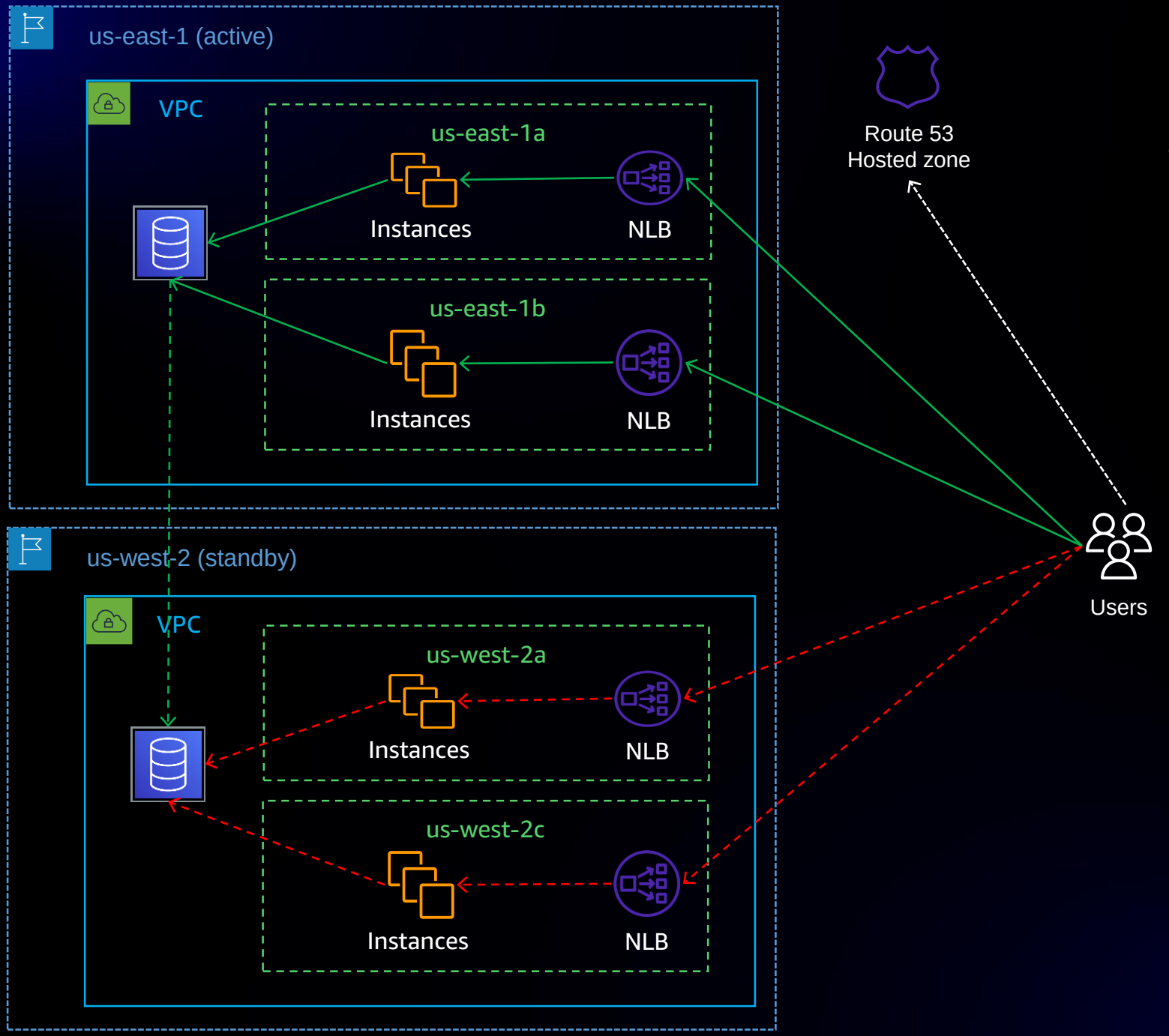
ASG Readiness Checks

- AsgMinSizeAndMaxSize
- AsgAZCount
- AsgInstanceTypes
- AsgInstanceSizes
- …



NLB Readiness Checks

- ElbV2State
- ElbV2Type
- ElbV2ProvisionedCapacityLcu Count
- ElbV2CrossZoneEnabled
- …

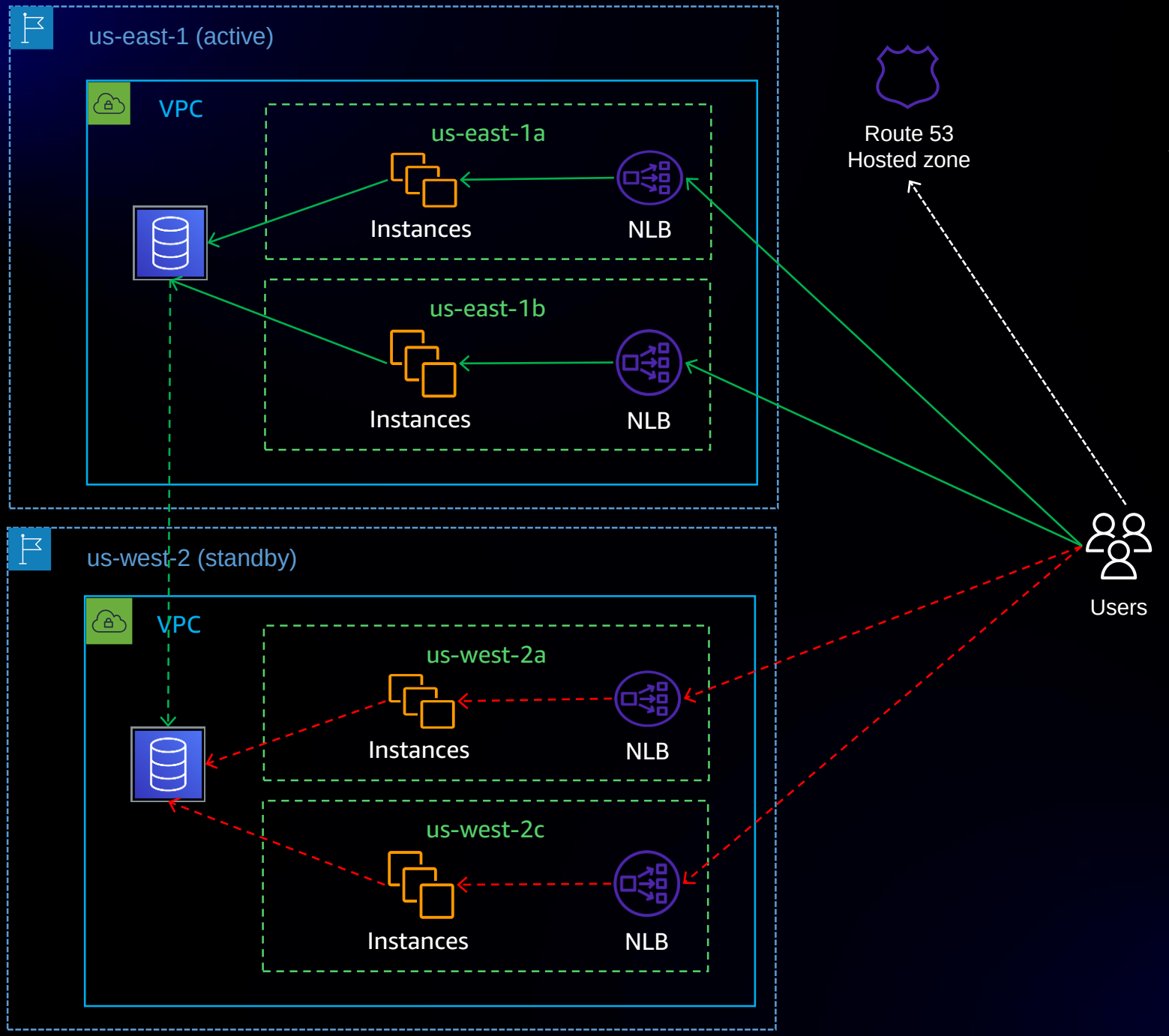


Route 53
Hosted zone

Users

Amazon Aurora

- ElbV2State
- RdsEngineMode
- RdsNormalizedCapacity
- RdsInstanceType
- …



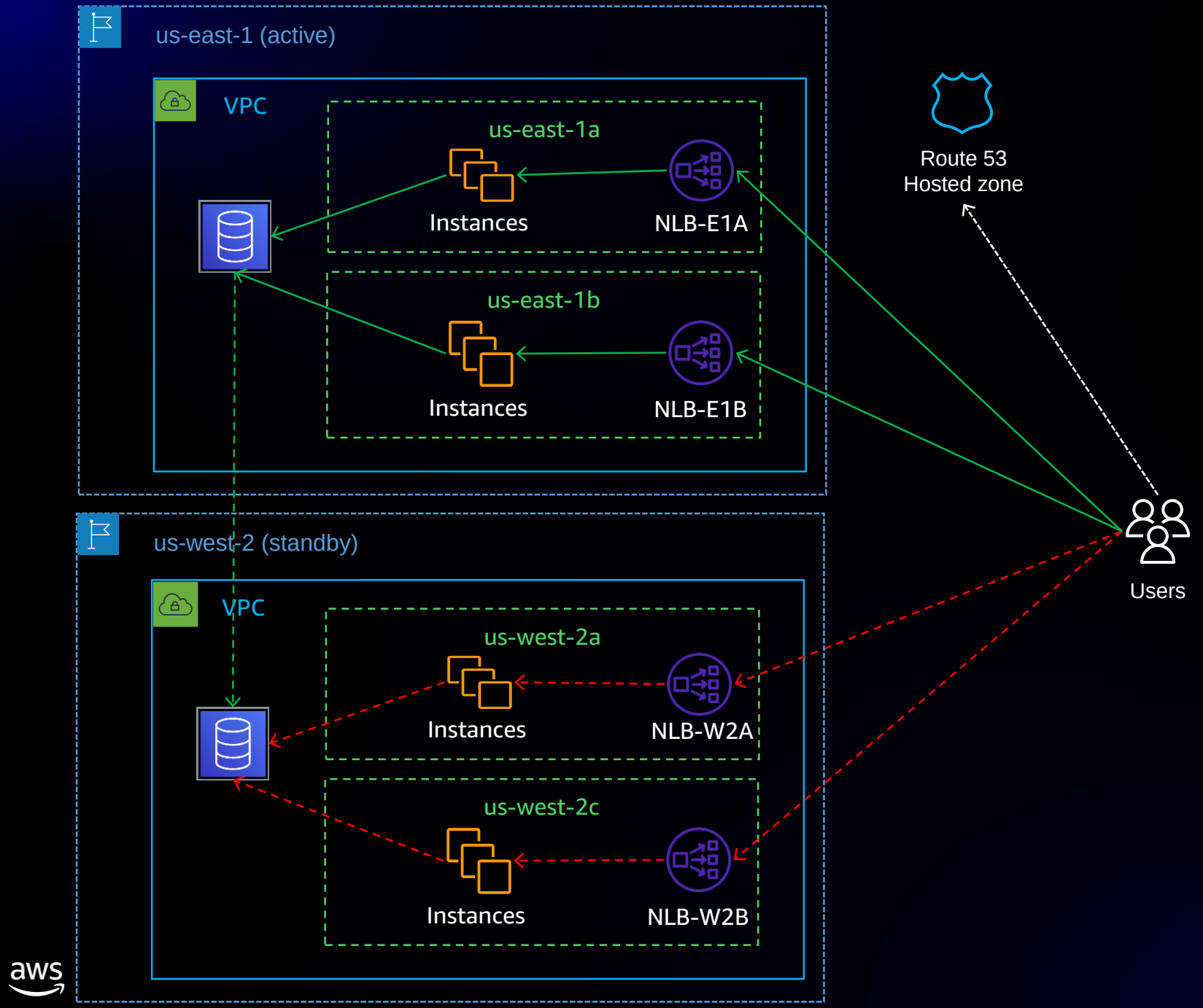
Amazon CloudWatch

- CloudWatchAlarmState
- …

Route 53 ARC features

Now we have multiple replicas

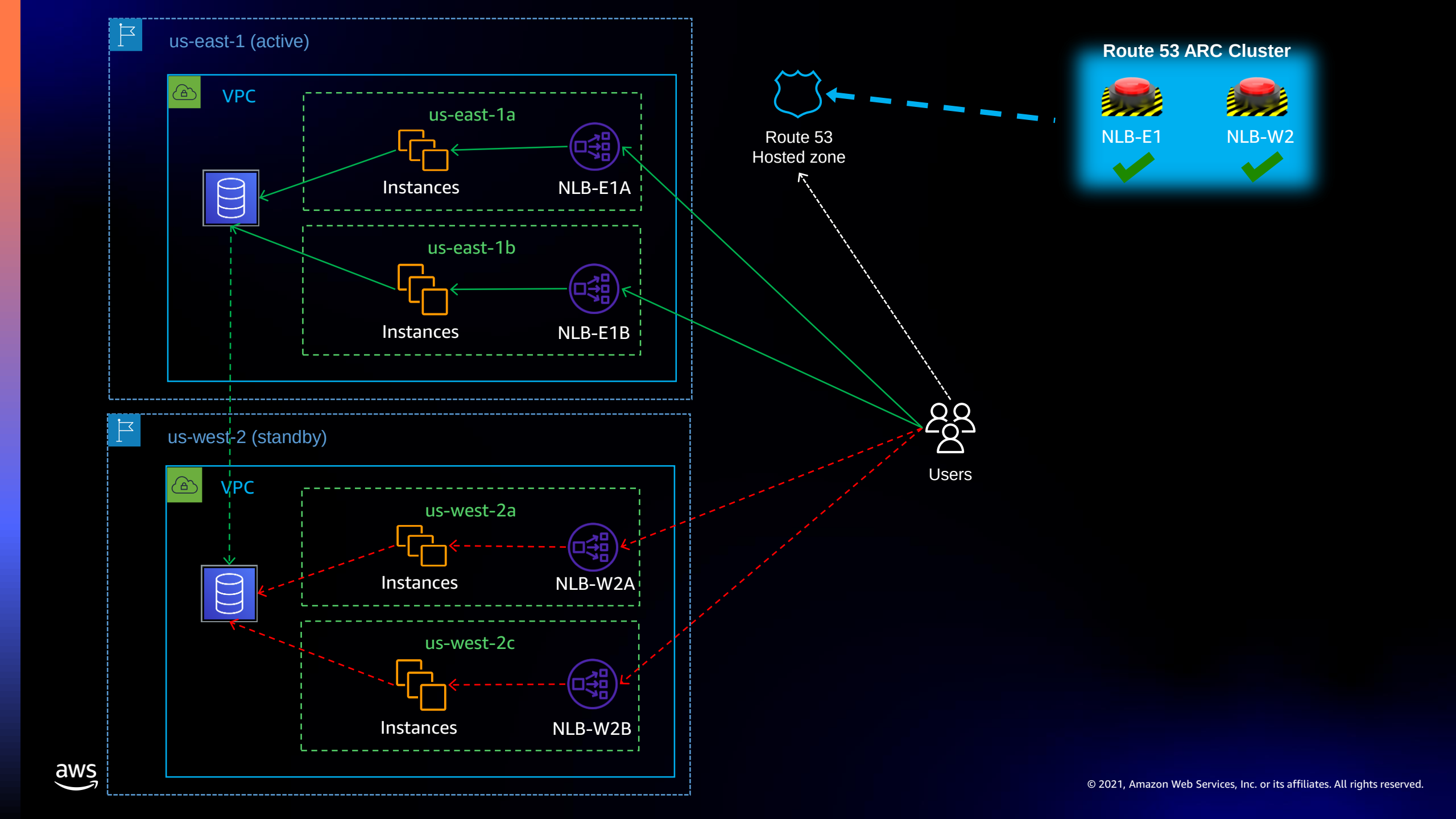
- How do we know we are ready to take a replica out?
- **What recovery mechanism do we use?**
- How do we make sure failover is safe?

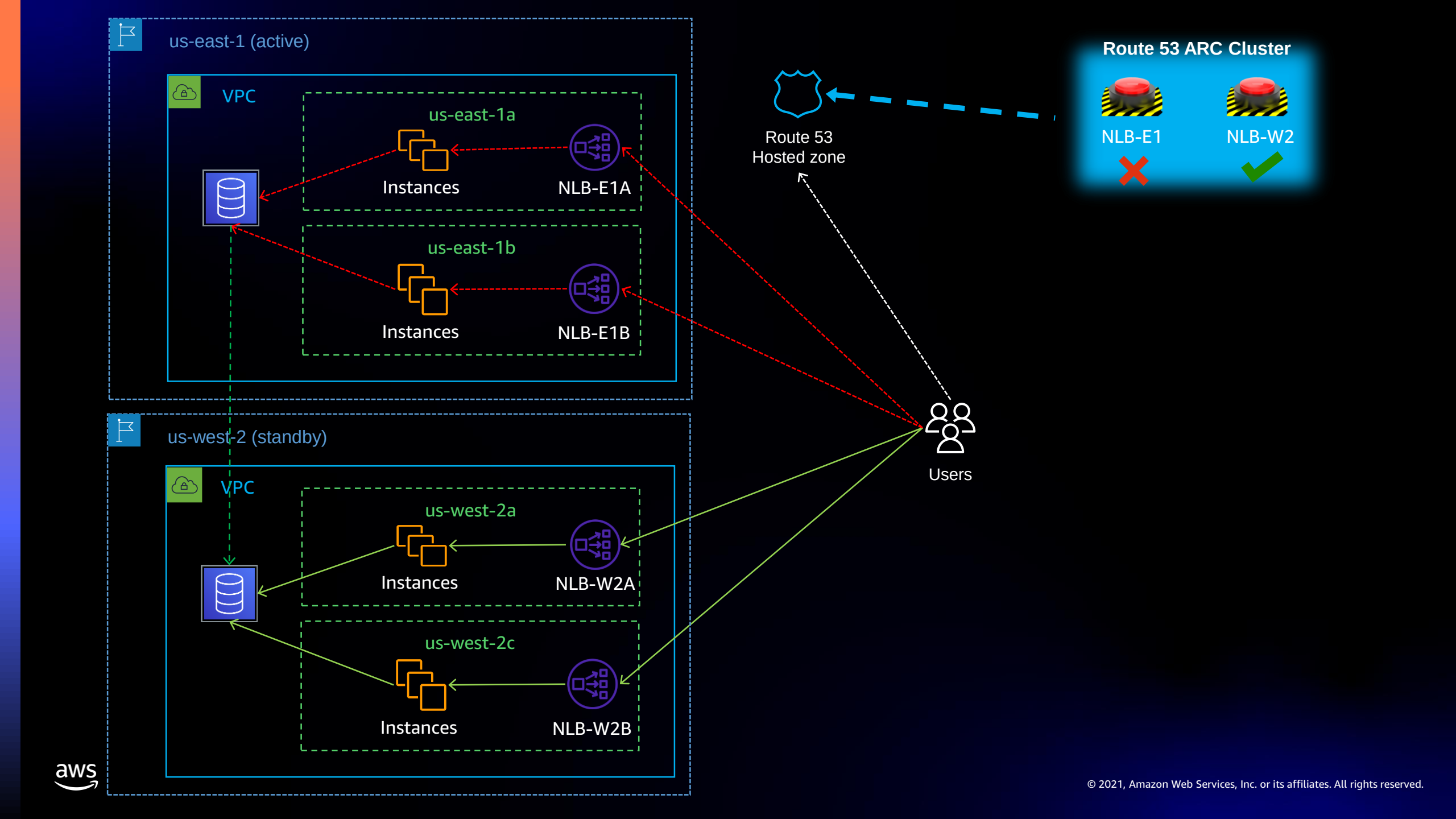


Feature #2: ARC routing controls

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





Route 53 ARC features

Now we have multiple replicas

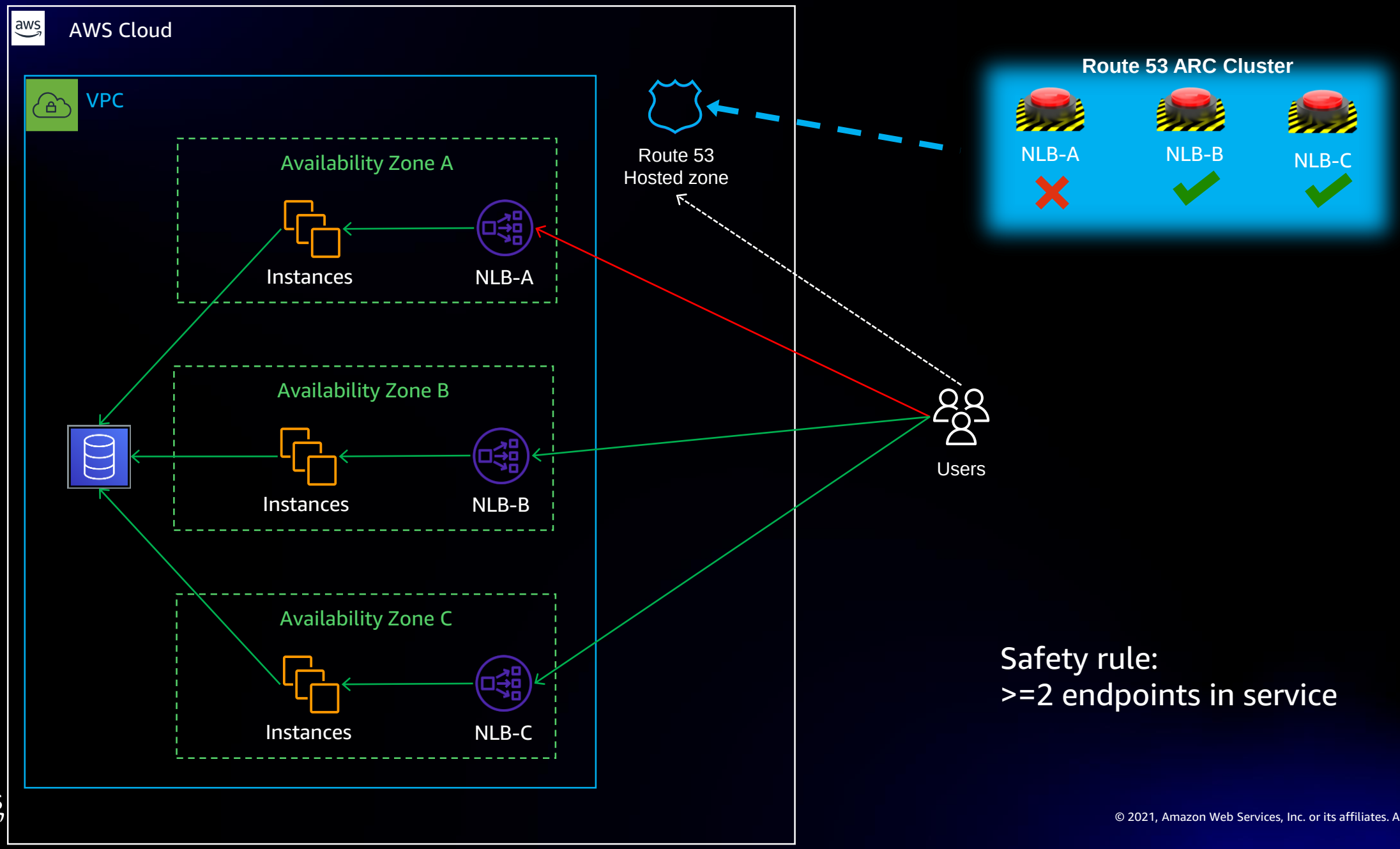
- How do we know we are ready to take a replica out?
- What recovery mechanism do we use?
- How do we make sure failover is safe?

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



Safety rule:
>=2 endpoints in service

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!