AWS re:Invent

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

ARC331

Reliability, consistency, and confidence through immutability

Gunnar Grosch (he/him)
Senior Developer Advocate
Amazon Web Services

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutable:
not capable of or susceptible to change

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Traditional infrastructures

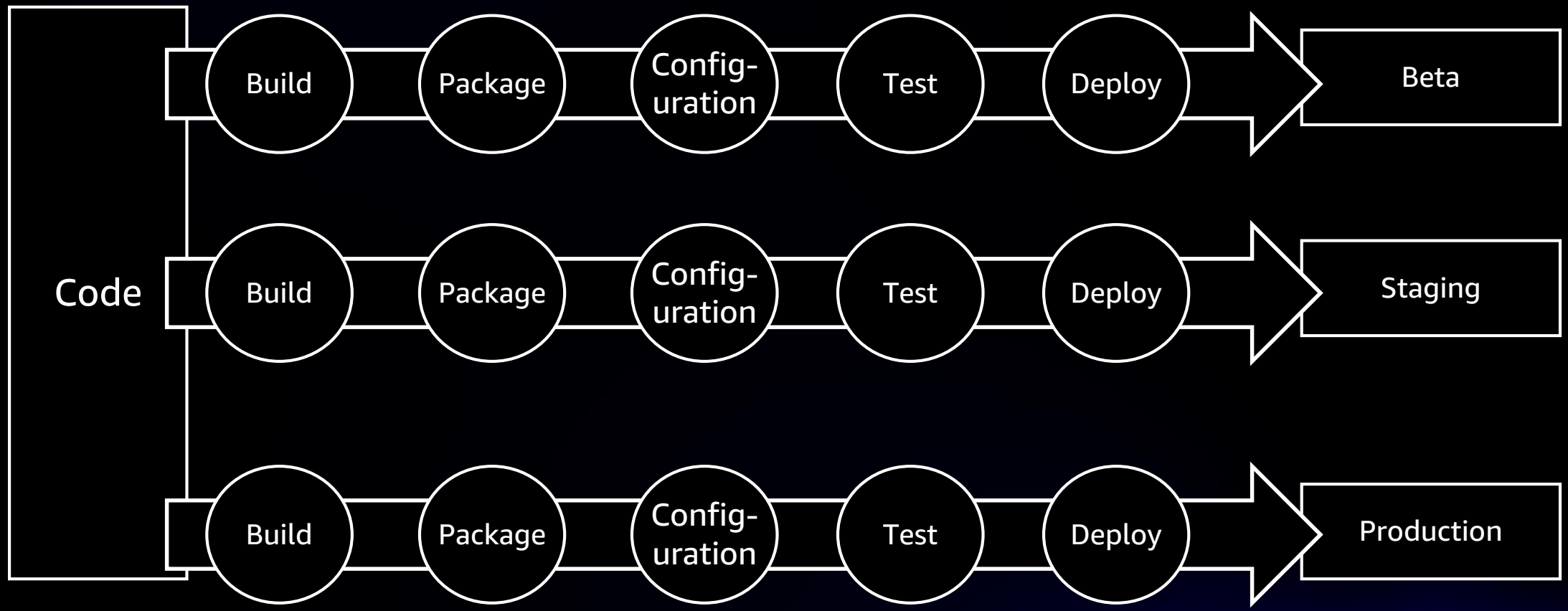
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Uptime



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Mutable deployments pipelines



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Running commands on Linux instance at launch with user data and shell scripts

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Installing dependencies

```
$ pip install -r requirements.txt
$ npm install
$ docker build
```

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the internet



NPM ERR!

How one programmer broke the internet by deleting a tiny piece of code

```
1  module.exports = leftpad;
2  function leftpad (str, len, ch) {
3    str = String(str);
4    var i = -1;
5    if (!ch && ch !== 0) ch = ' ';
6    len = len - str.length;
7    while (++i < len) {
8      str = ch + str;
9    }
10   return str;
11 }
12
13
14
15
16
17
18
19
20
```

By **Keith Collins**
Tech Reporter

March 27, 2016 · This article is more than 2 years old.

A man in Oakland, California, disrupted web development around the world last week by deleting 11 lines of code.

The story of how 28-year-old Azer Koçulu briefly broke the internet



A discussion about the breaking of the Internet

Mike Roberts Follow
Mar 23, 2016 · 5 min read

Hey everyone — I'm the head of messenger at Kik. I wish this didn't have to be my first post on Medium, but open source is something that I care about. I've published a few meager open source projects in the past, things that aren't groundbreaking but that I thought might be useful to other people, and I rely on countless others every day.

I found out about this problem like a lot of you, when our builds started failing because we use the extremely helpful JSCS. Through a long chain of dependencies, JSCS relied on left-pad@0.0.3, which was removed by the author yesterday. Our team was confused at the time as well.

https://medium.com/@mproberts/a-discussion-about-the-breaking-of-the-internet

https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutable infrastructure

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutable infrastructure is not a new idea



Chad Fowler

articles interviews contact speaking books

Trash Your Servers and Burn Your Code: Immutable Infrastructure and Disposable Components

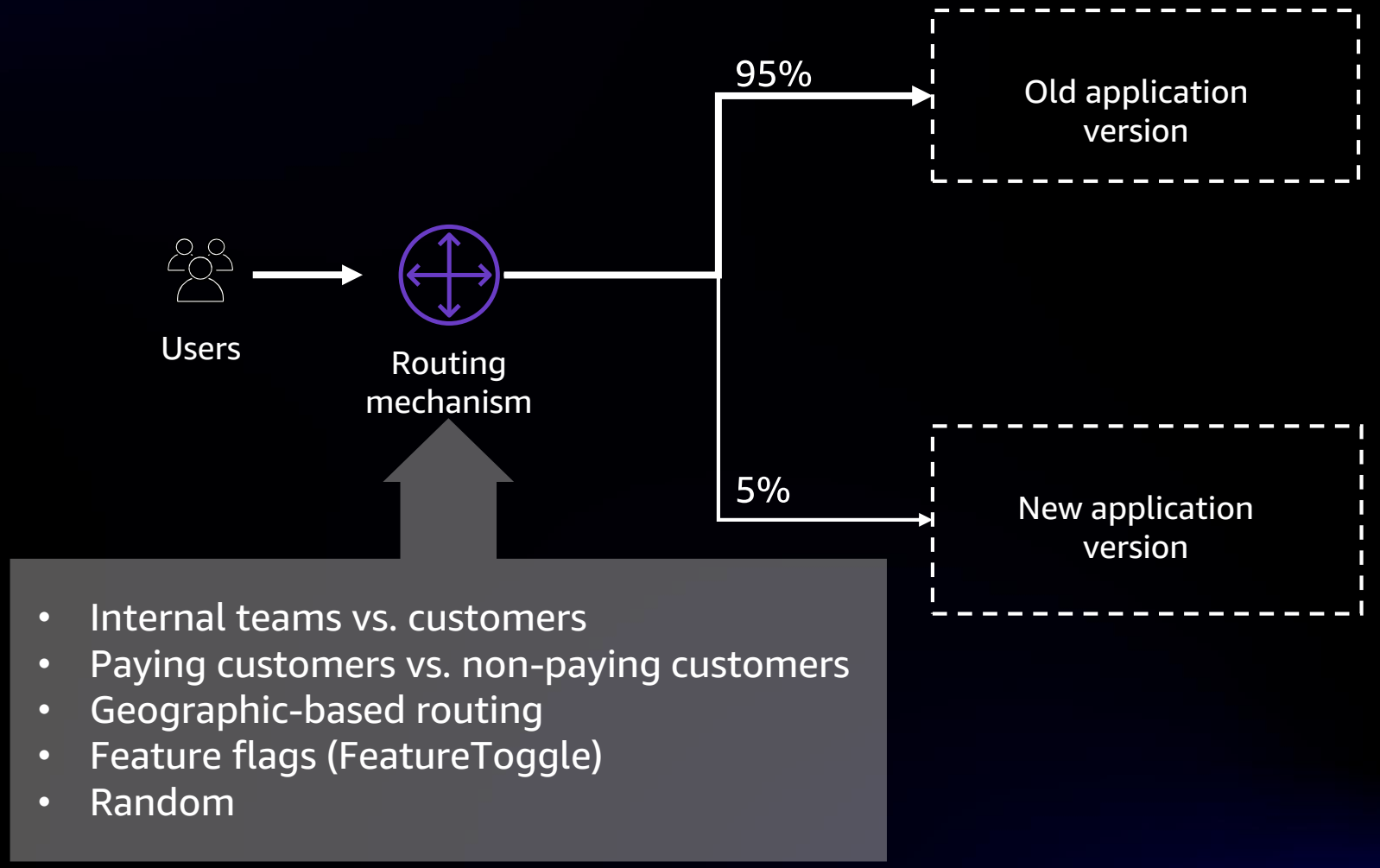
Jun 23, 2013

As a developer and sometimes system administrator, one of the scariest things I ever encounter is a server that's been running for ages which has seen multiple upgrades of system and application software.

Why? Because an old system inevitably grows warts. They start as one-time hacks during outages. A quick edit to a config file saves the day. "We'll put it back into Chef later," we say, as we finally head off to sleep after a marathon fire fighting session.

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Immutable (canary) deployment



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Canary deployments on AWS

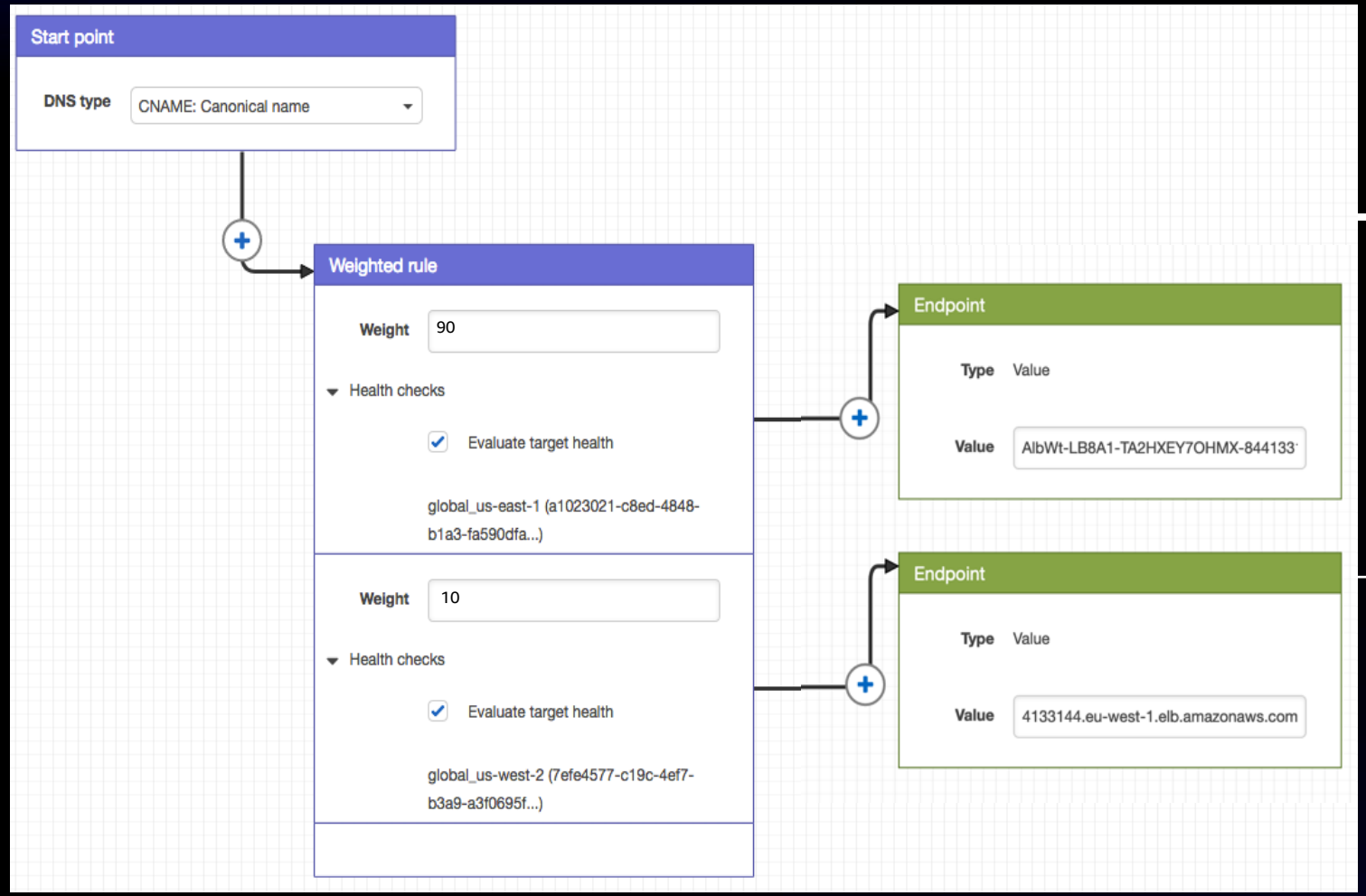
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

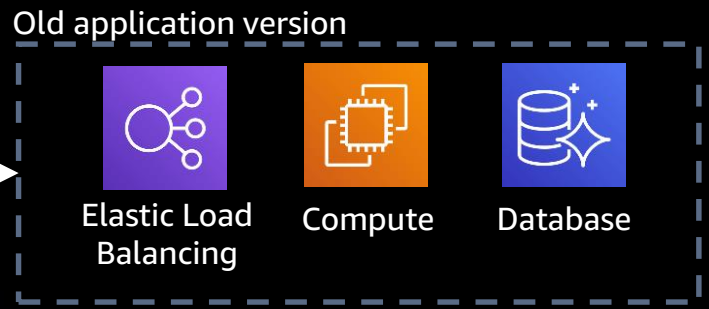
1. Amazon Route 53 with weighted routing policy

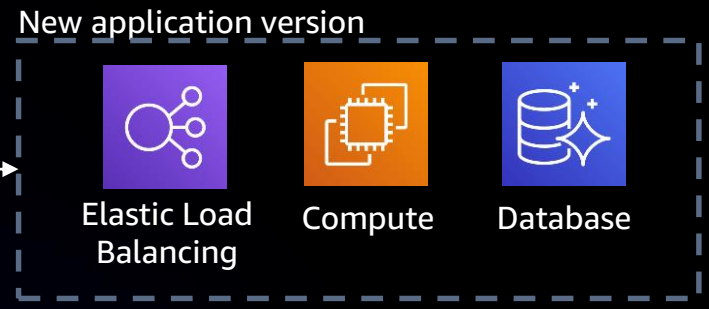


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

1. Route 53 with weighted routing policy





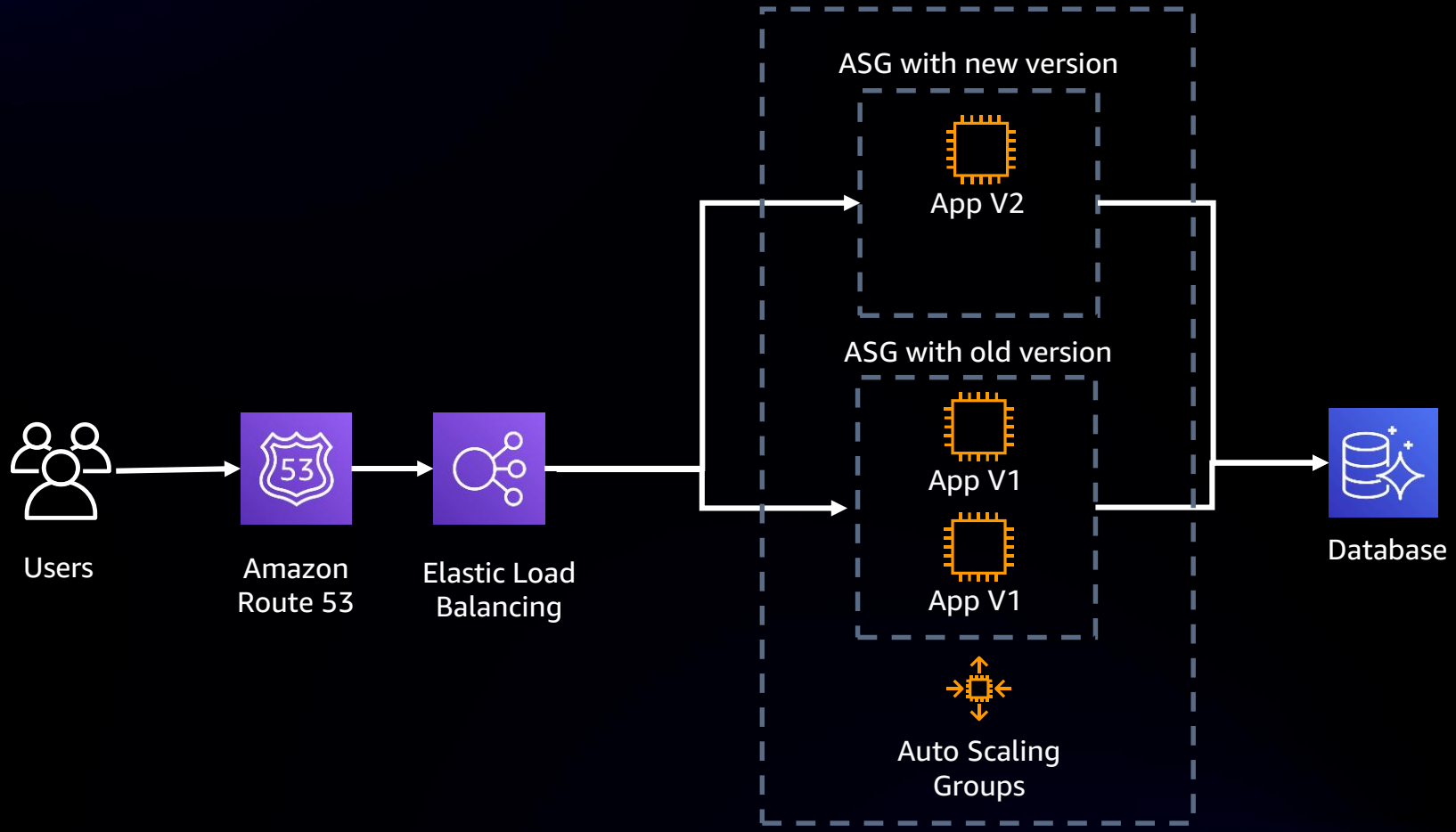




DNS propagation!

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

2. Rolling deployments for auto scaling

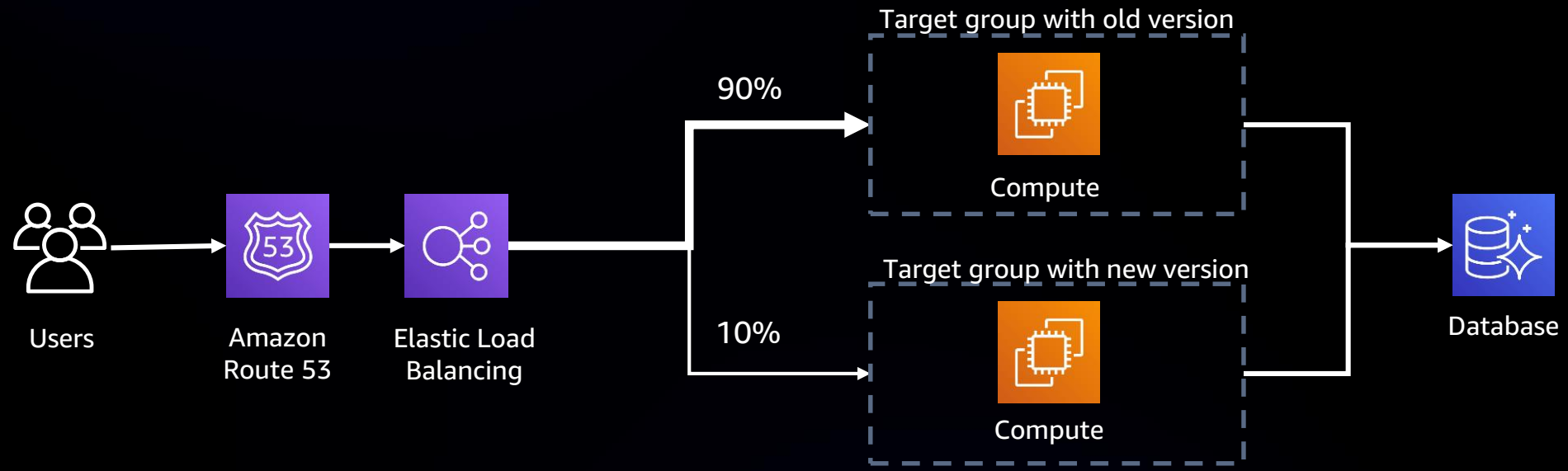


https://aws.amazon.com/blogs/aws/three-new-features-for-aws-cloudformation/

https://engineering.klarna.com/simple-canary-releases-in-aws-how-and-why-bf051a47fb3f

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

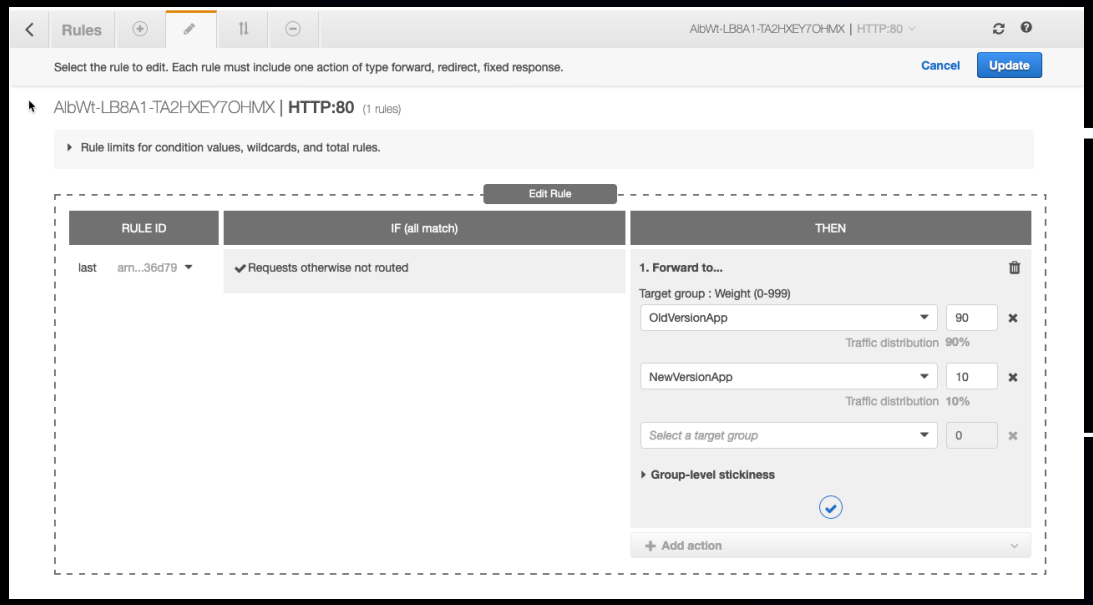
3. Application load balancer and weighted target groups

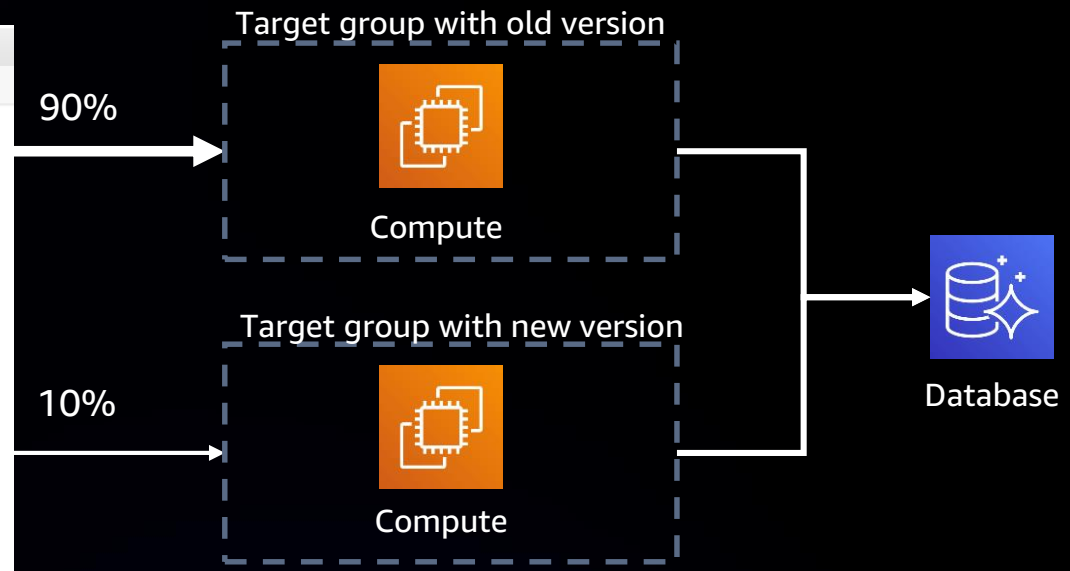


https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

3. Application load balancer and weighted target groups

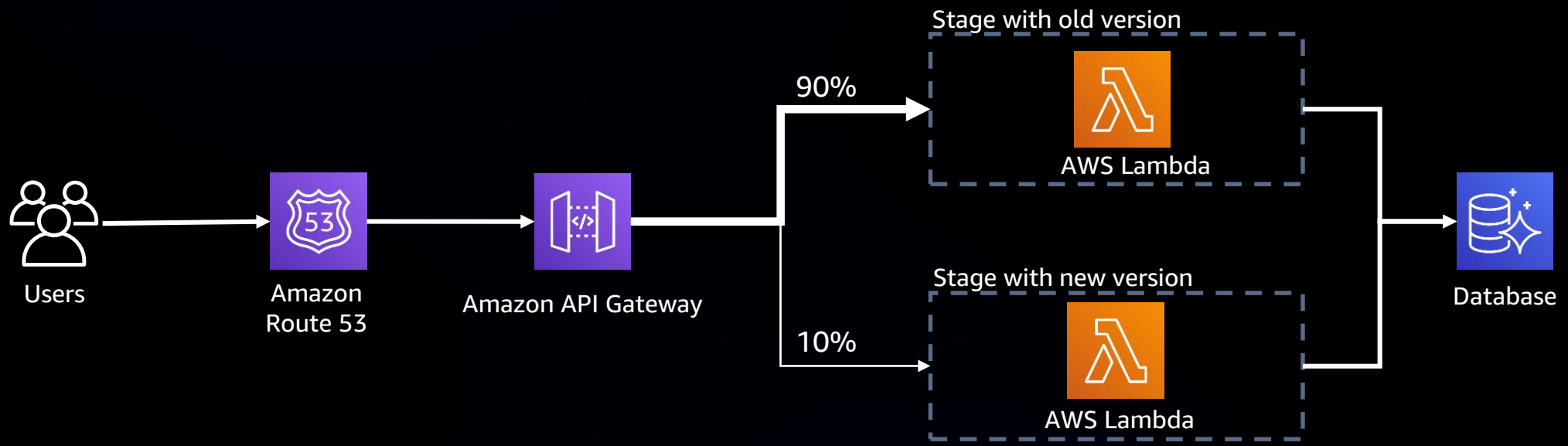




https://aws.amazon.com/blogs/aws/new-application-load-balancer-simplifies-deployment-with-weighted-target-groups/

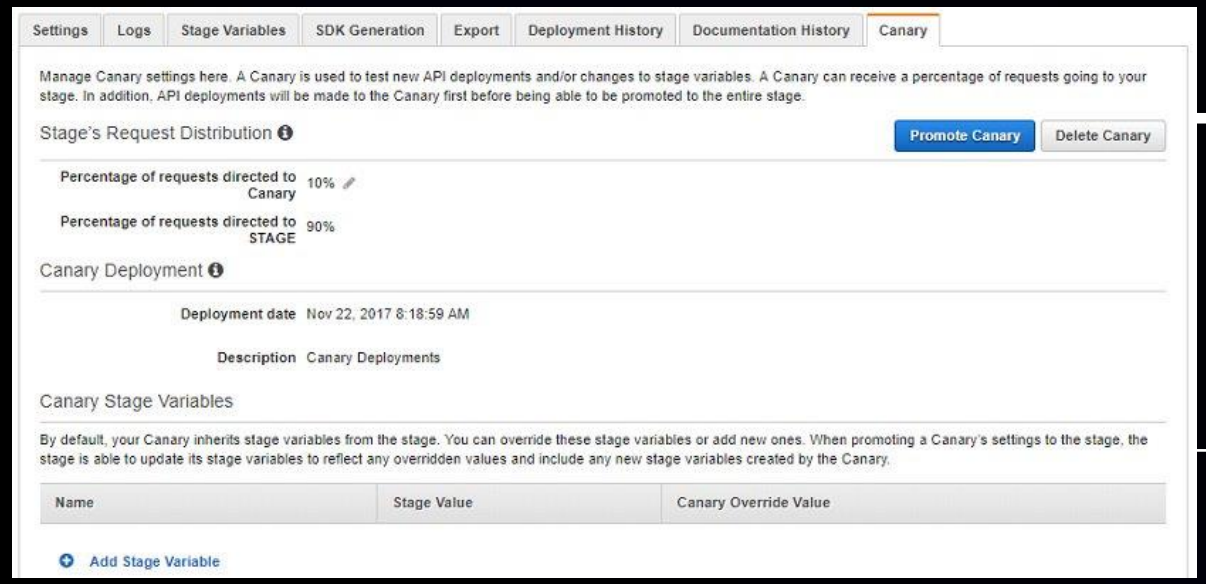
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

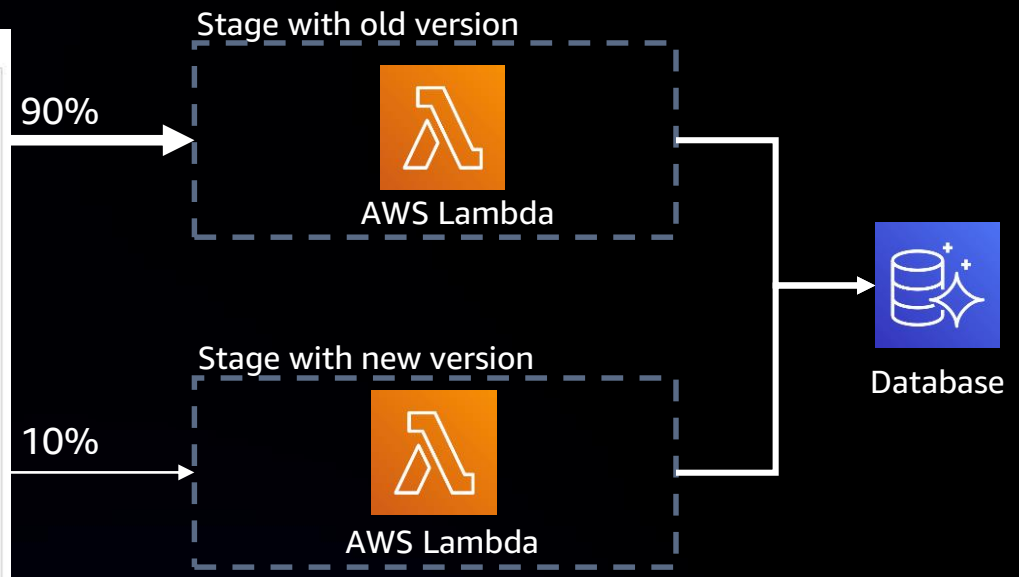
4. Amazon API Gateway release deployments



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

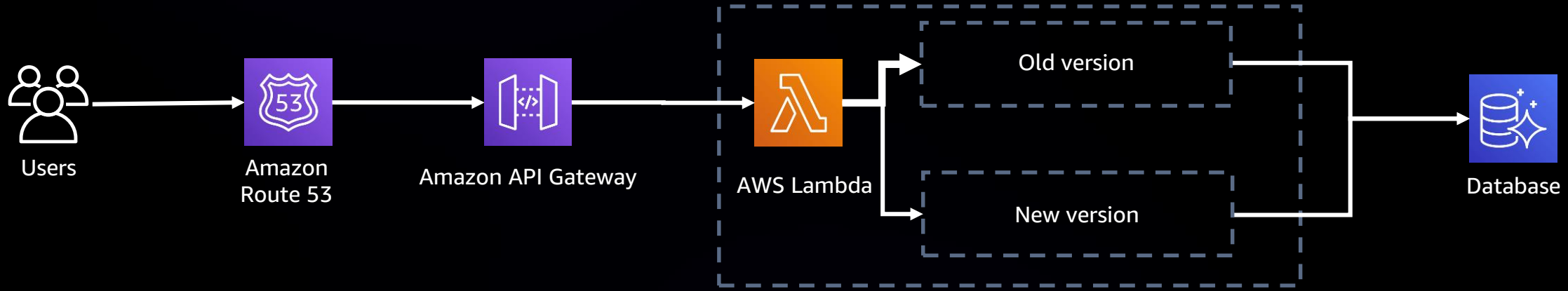
4. Amazon API Gateway release deployments





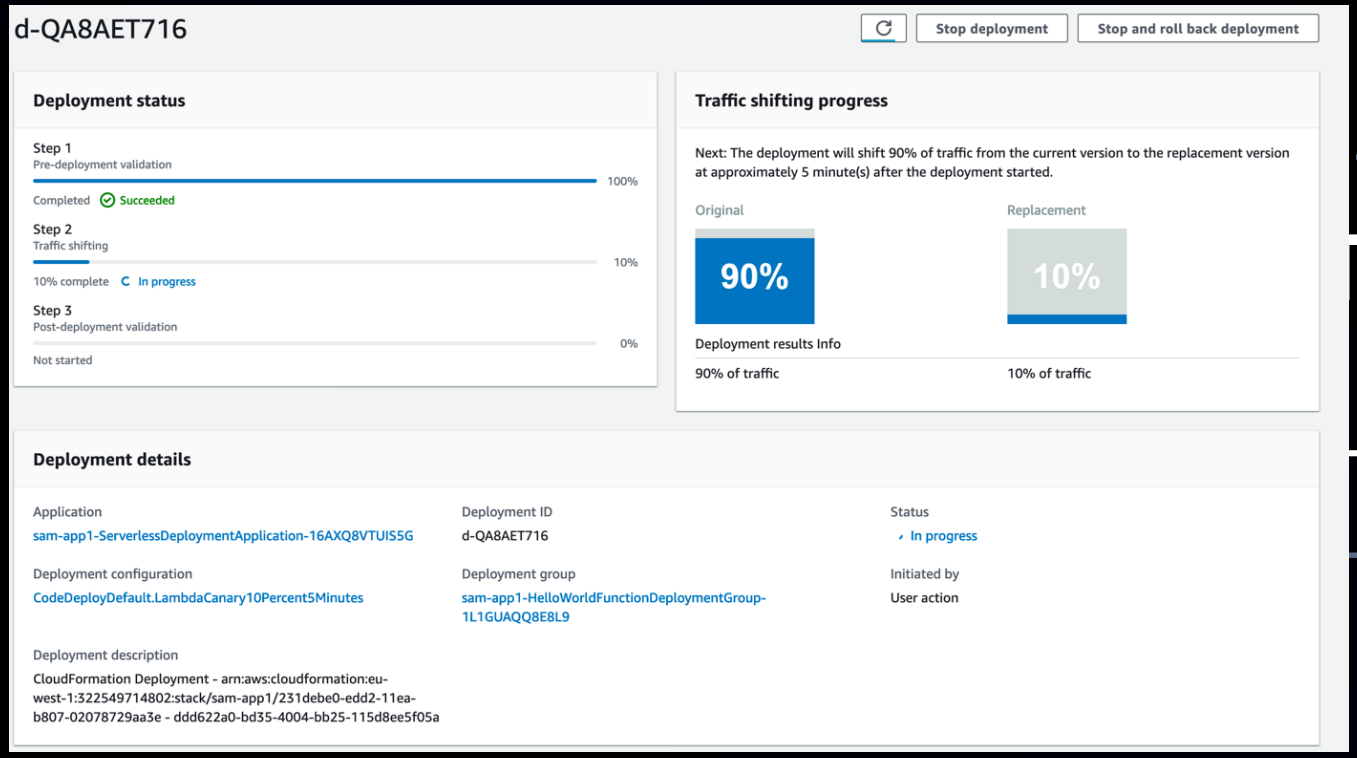
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

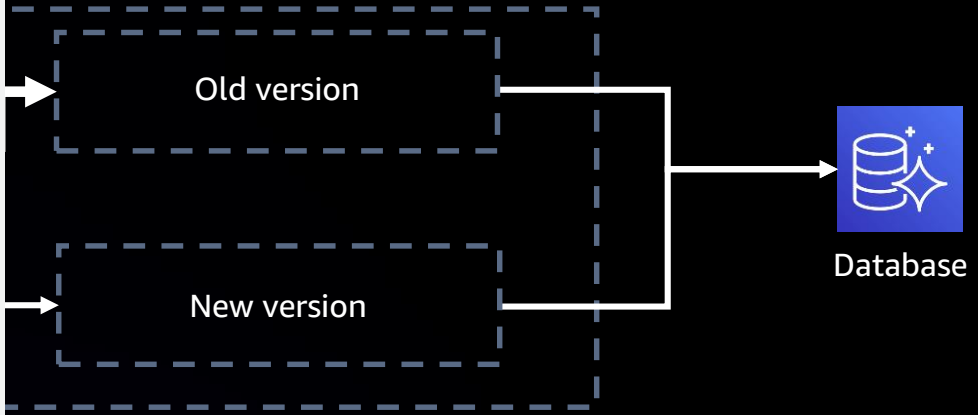
5. AWS Lambda alias traffic shifting



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

5. AWS Lambda alias traffic shifting





Via AWS CodeDeploy

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Security considerations

AUTOMATED RESPONSES THAT RUN IN RESPONSE TO EVENTS

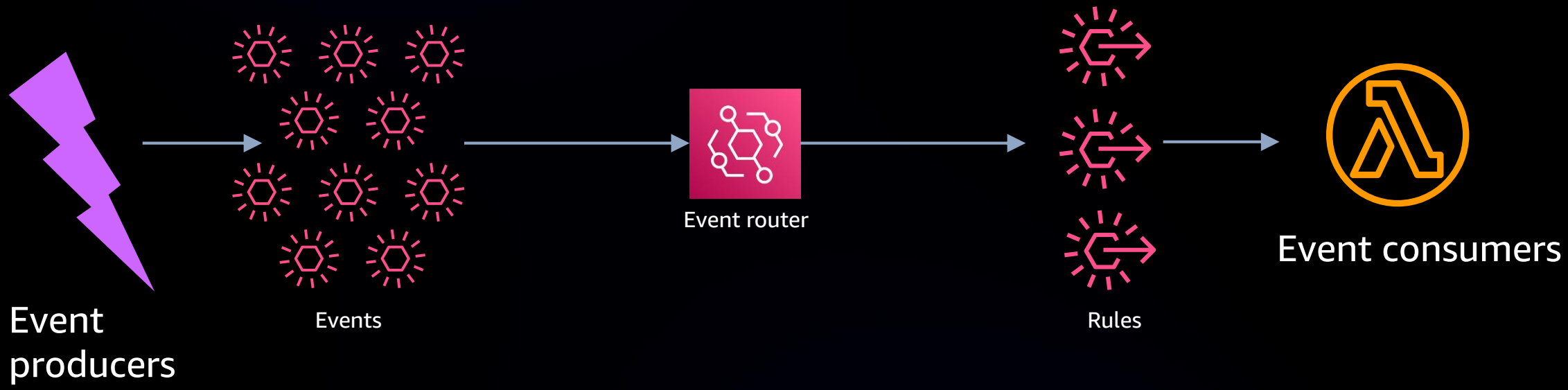


Mutability is one of the most critical event vectors for cyber crimes

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

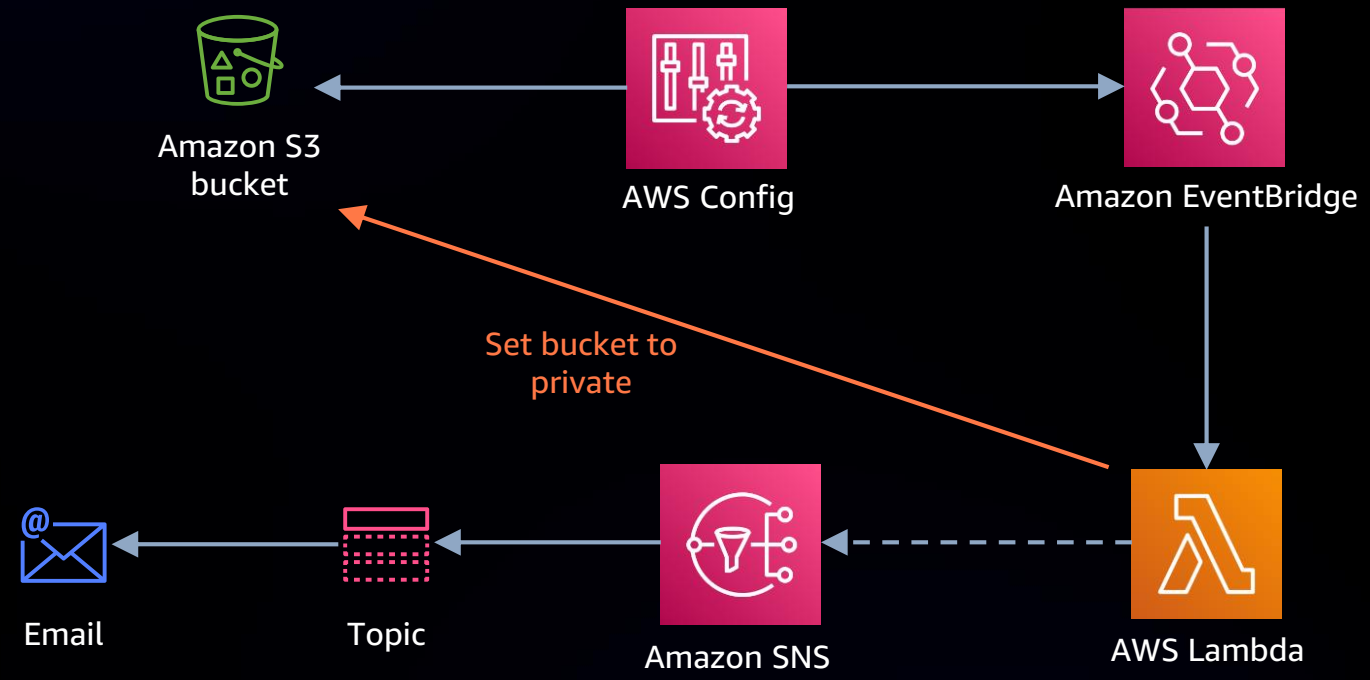
Event-driven patterns

AUTOMATED RESPONSES THAT RUN IN RESPONSE TO EVENTS



© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

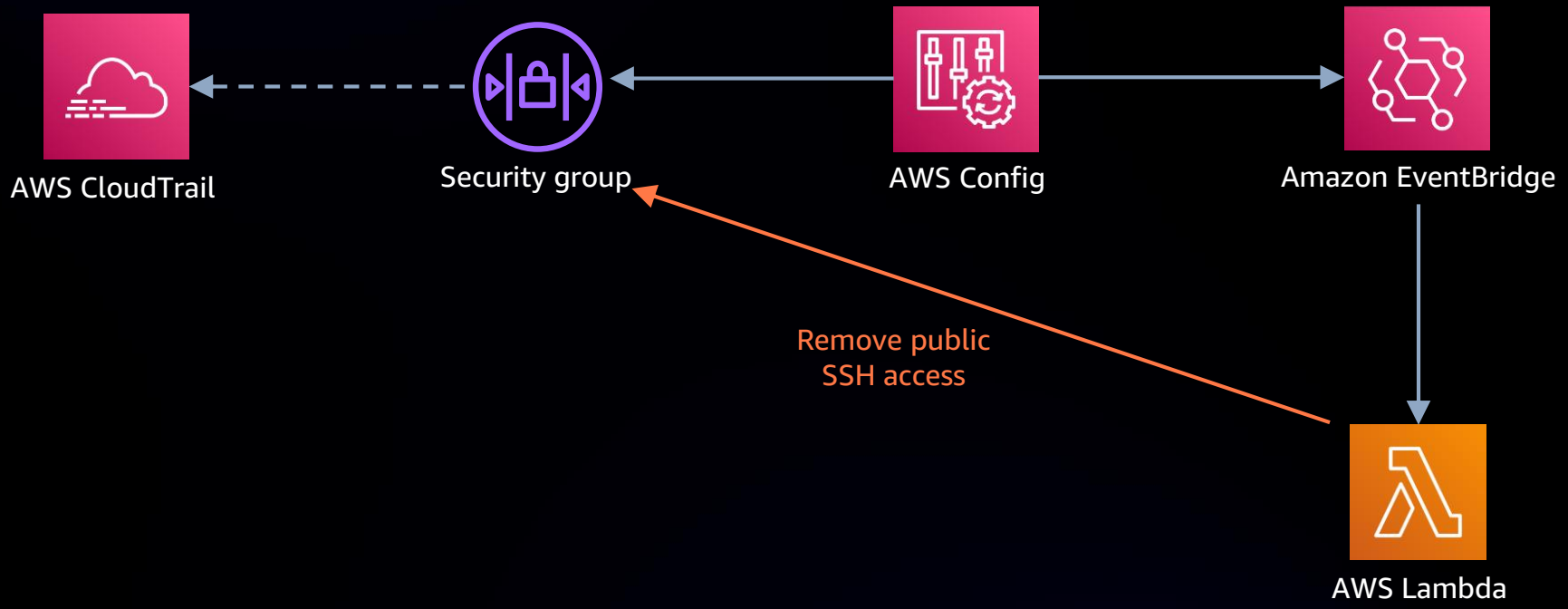
Public Amazon S3 bucket remediation



https://github.com/awslabs/aws-config-rules/tree/master/aws-config-conformance-packs

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Public SSH access remediation



https://github.com/adhorn/ssh-restricted

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Benefits of immutable architecture

- Reduction in configuration drifts
- Simplified deployments
- Reliable atomic deployments
- Safer deployments with fast rollback and recovery processes
- Consistent testing and debugging environments
- Increased scalability
- Simplified toolchain
- Increased security

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Architecture resources

AWS Well-Architected Framework

Best practices for Architecting in the AWS Cloud

https://aws.amazon.com/architecture/well-architected

AWS Architecture Center

Official AWS repository for all Architecture resources

https://aws.amazon.com/architecture

AWS Well-Architected Labs

Hands-on labs to help you learn, measure, and build using architectural best practices

https://wellarchitectedlabs.com/

AWS Solutions Library

Vetted reference implementations and Well-Architected patterns

https://aws.amazon.com/solutions/

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Gunnar Grosch

@gunnargrosch
in/gunnargrosch
ggrosch@amazon.com

© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.