
AWS
re:Invent
NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

ARC304

Build for resilience using Amazon Route 53 Application Recovery Controller

Scott Wainstock

Software Development Manager, AWS Resilience Infrastructure & Solutions
AWS

Stanley Su

Principal Product Manager, AWS Resilience Infrastructure & Solutions
AWS

Agenda

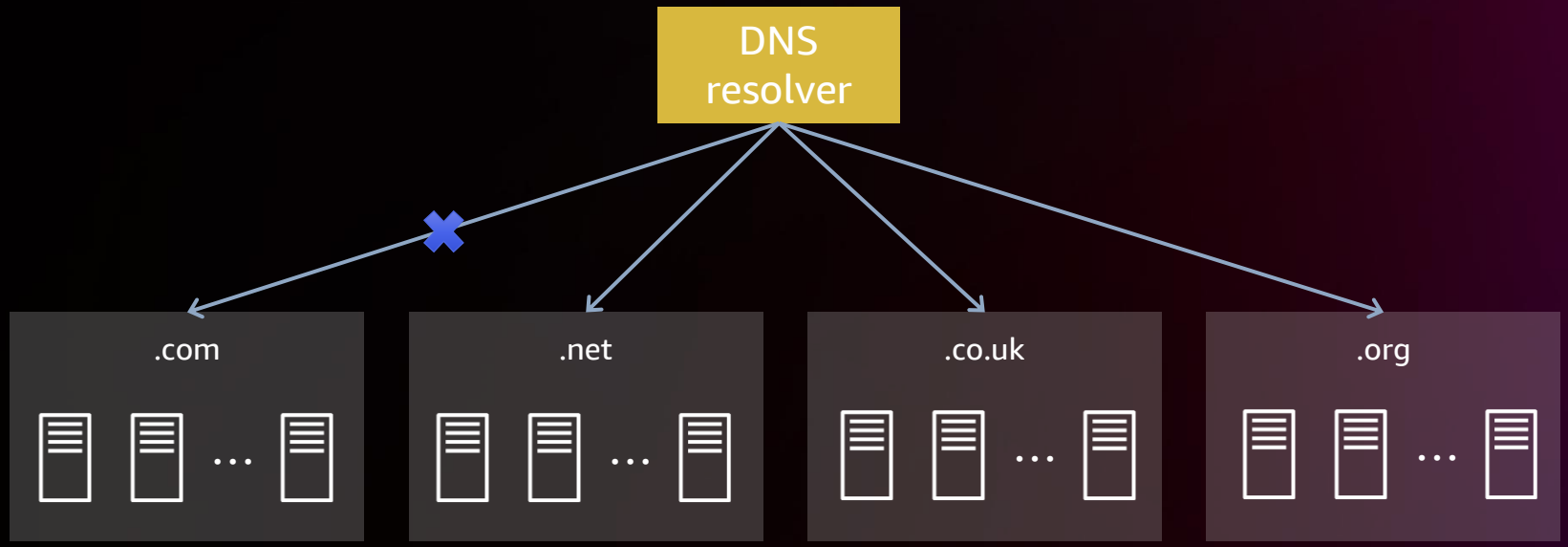
1. How AWS approaches high availability
2. Building resilient applications in the cloud
3. What is Amazon Route 53 Application Recovery Controller (ARC)?
4. Hands-on workshop on Route 53 ARC

“Everything fails, all the time”

Werner Vogels

VP and CTO, Amazon.com

Design for failure – Amazon Route 53

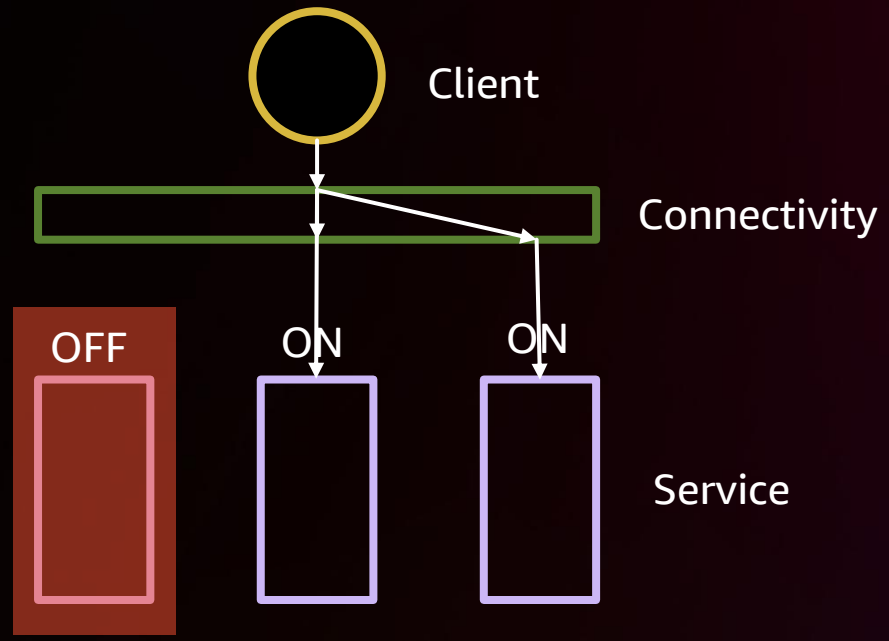


AWS Architecture Blog: “A Case Study in Global Fault Isolation”

https://aws.amazon.com/blogs/architecture/a-case-study-in-global-fault-isolation/

Design for application failures

- Anticipate application failures
- Apply cellular architecture – Isolate and contain failures
- Build and leverage robust failure recovery mechanisms



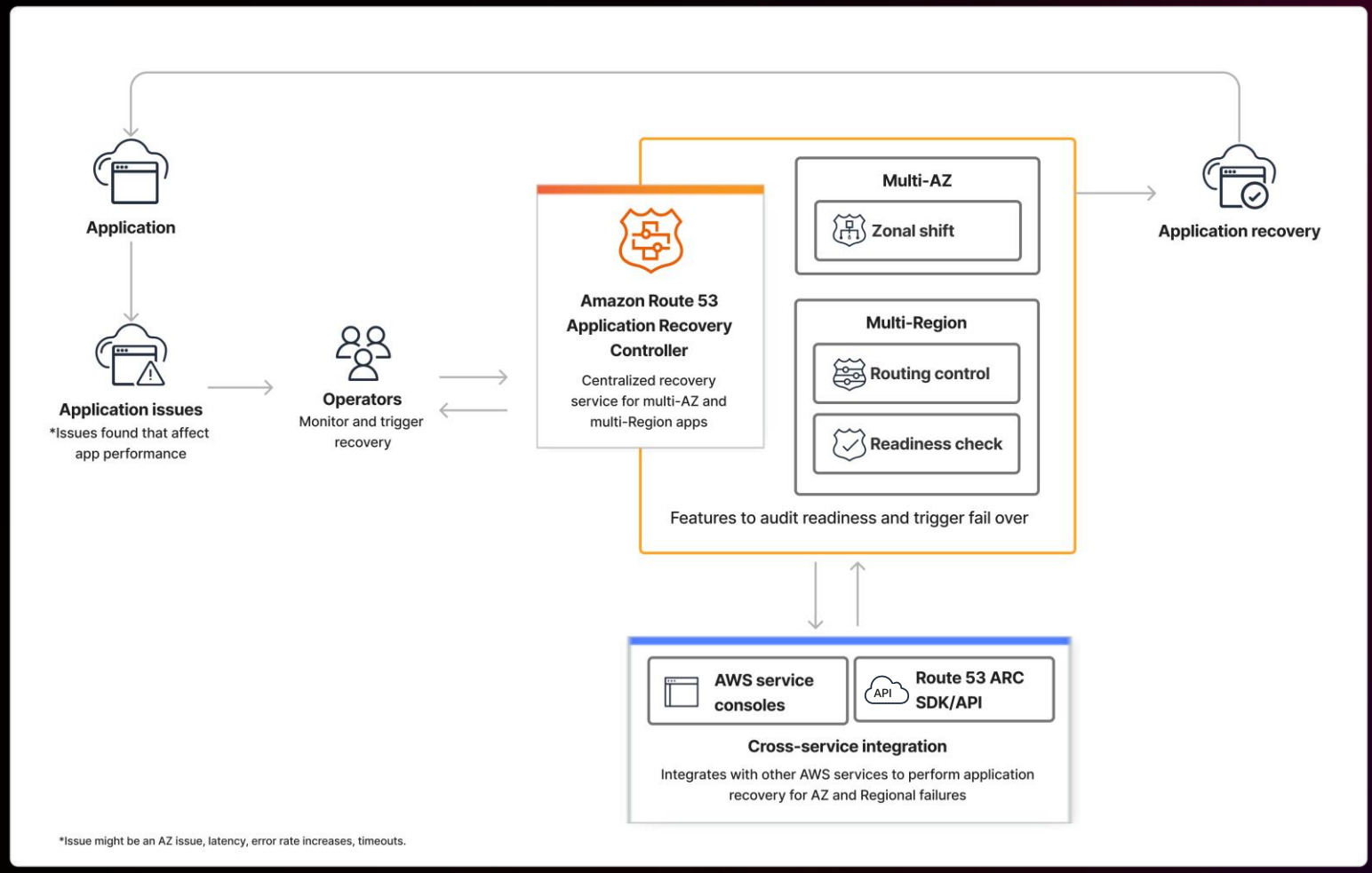
Design for application failures – Challenges

- Recovery mechanisms need to be reliable
- Cell replicas need to be properly scaled and configured
- Strict recovery time objective (RTO) and recovery point objective (RPO) require solid automation and processes

Amazon Route 53 Application Recovery Controller

Centralized, safe, and reliable way to manage cross-region and cross-AZ recovery

How does Route 53 ARC work?



Multi-AZ key capabilities

Zonal shift (in preview) is a capability that enables customer to reliably recover from an application failure in an AZ by temporarily shifting the application away from the AZ

ARC zonal shift

- Grant access and go – Zonal shift is available for ALB and NLB with cross-zone load balancing off with no cost
- Built-in safety rule – Zonal shift prevents you from accidentally moving application traffic away from more than 1 AZ

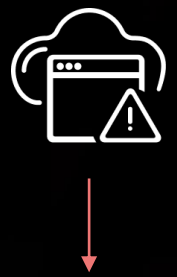
Key capabilities

- Start/Update/ Cancel zonal shift
- Resource level

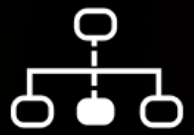
- Customizable auto expiration time for up to 3 days

- Prevent disabling the same resource from more than one AZ

How does a zonal shift work?



The health checks are passing but the synthetic monitoring on the ALB’s or NLB’s zonal endpoint indicates an increase in latency in a zone



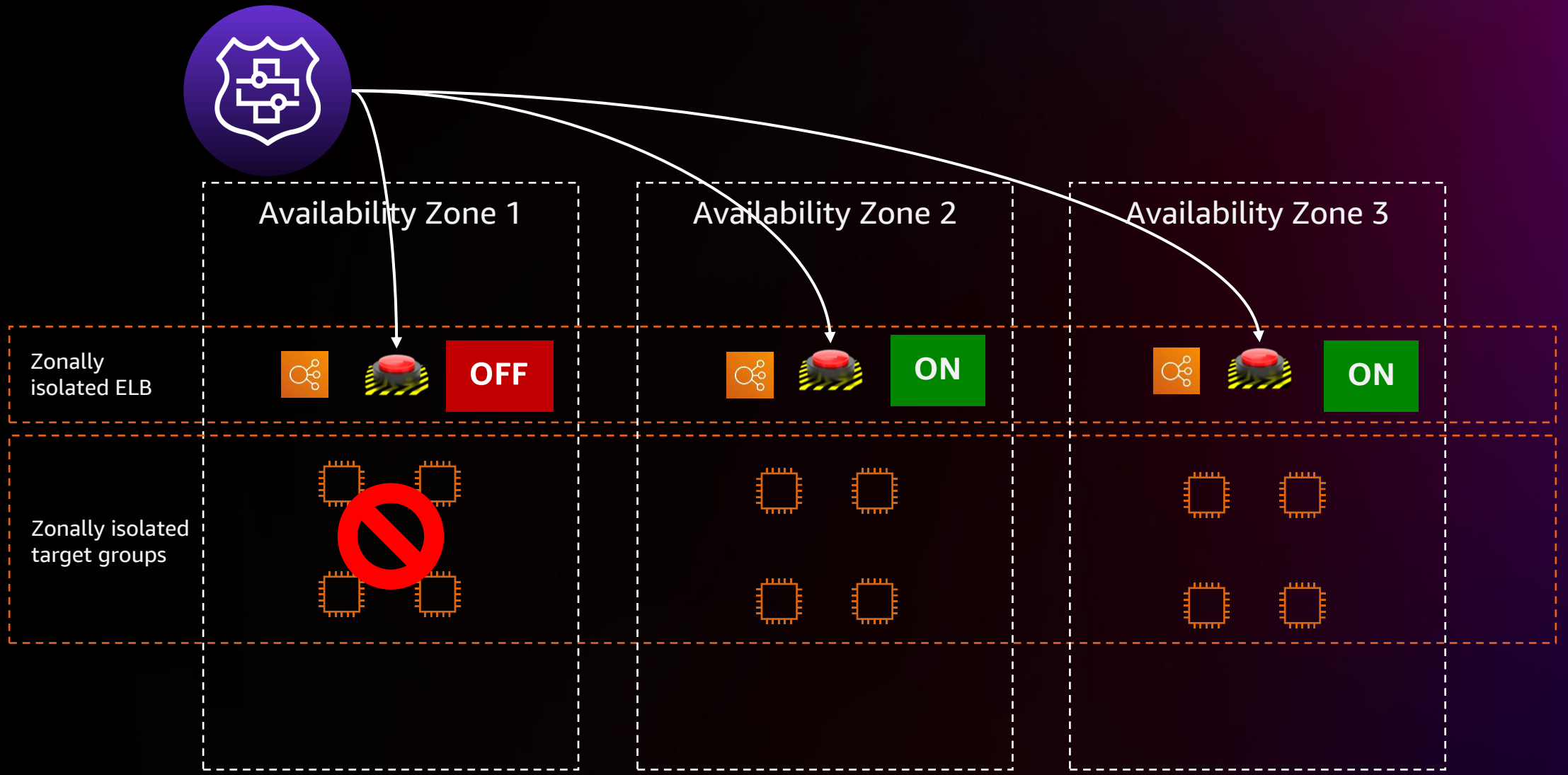
Start zonal shift to move traffic out from the AZ

Investigate and fix issue in the AZ

Cancel zonal shift to resume the traffic to the AZ

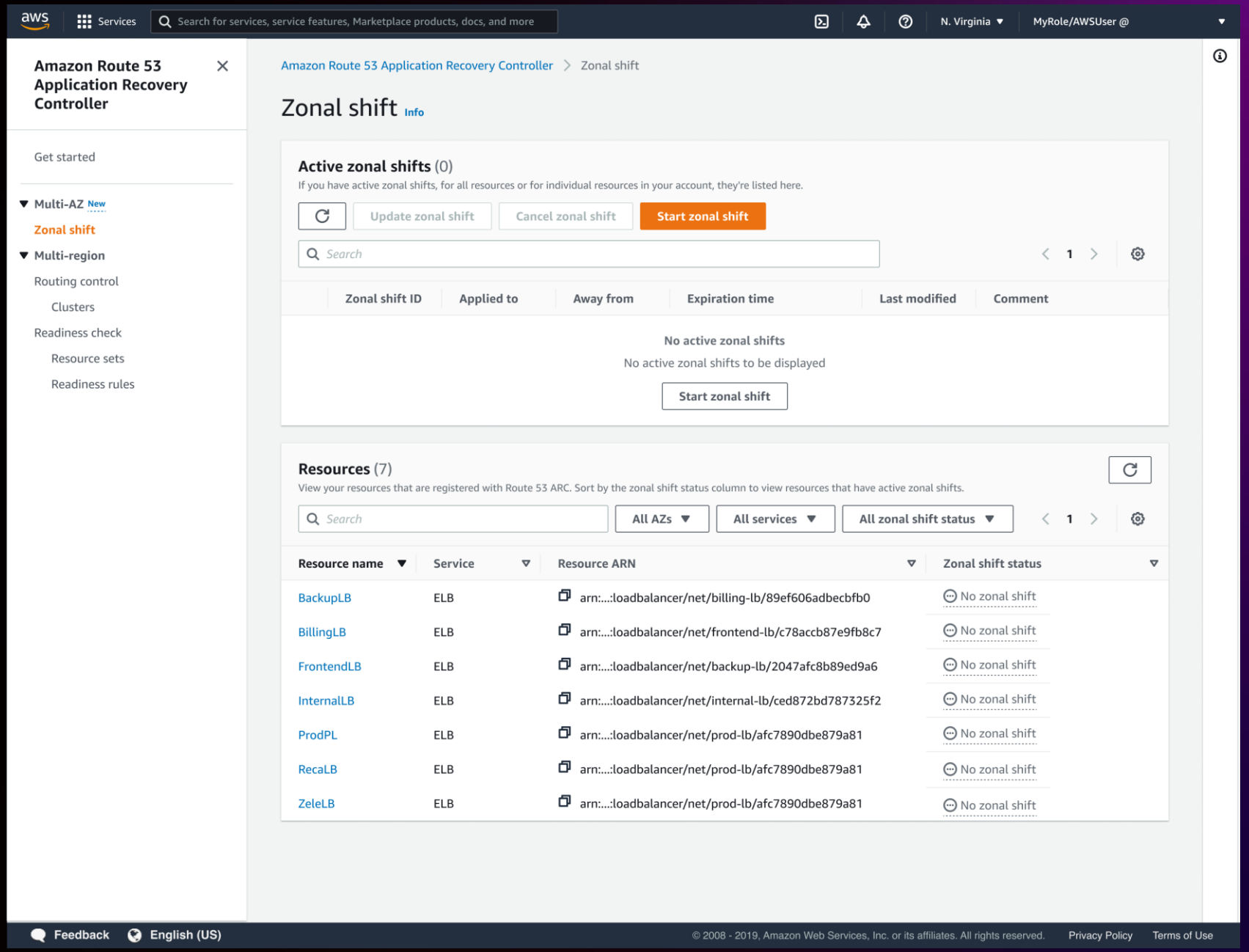
Zonal shift for AZ recovery

Zonal shift for AZ recovery

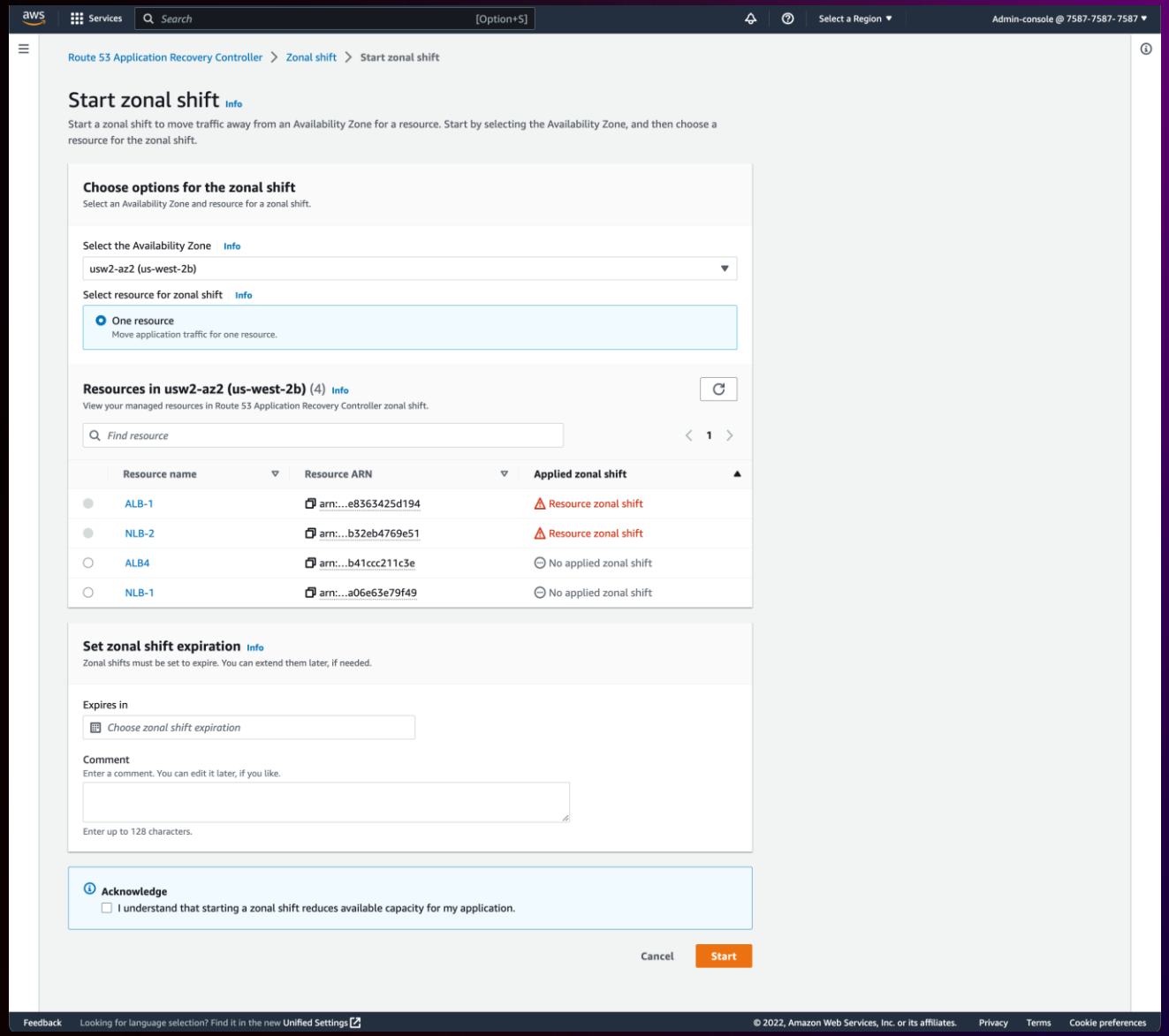


Zonal shift for AZ recovery

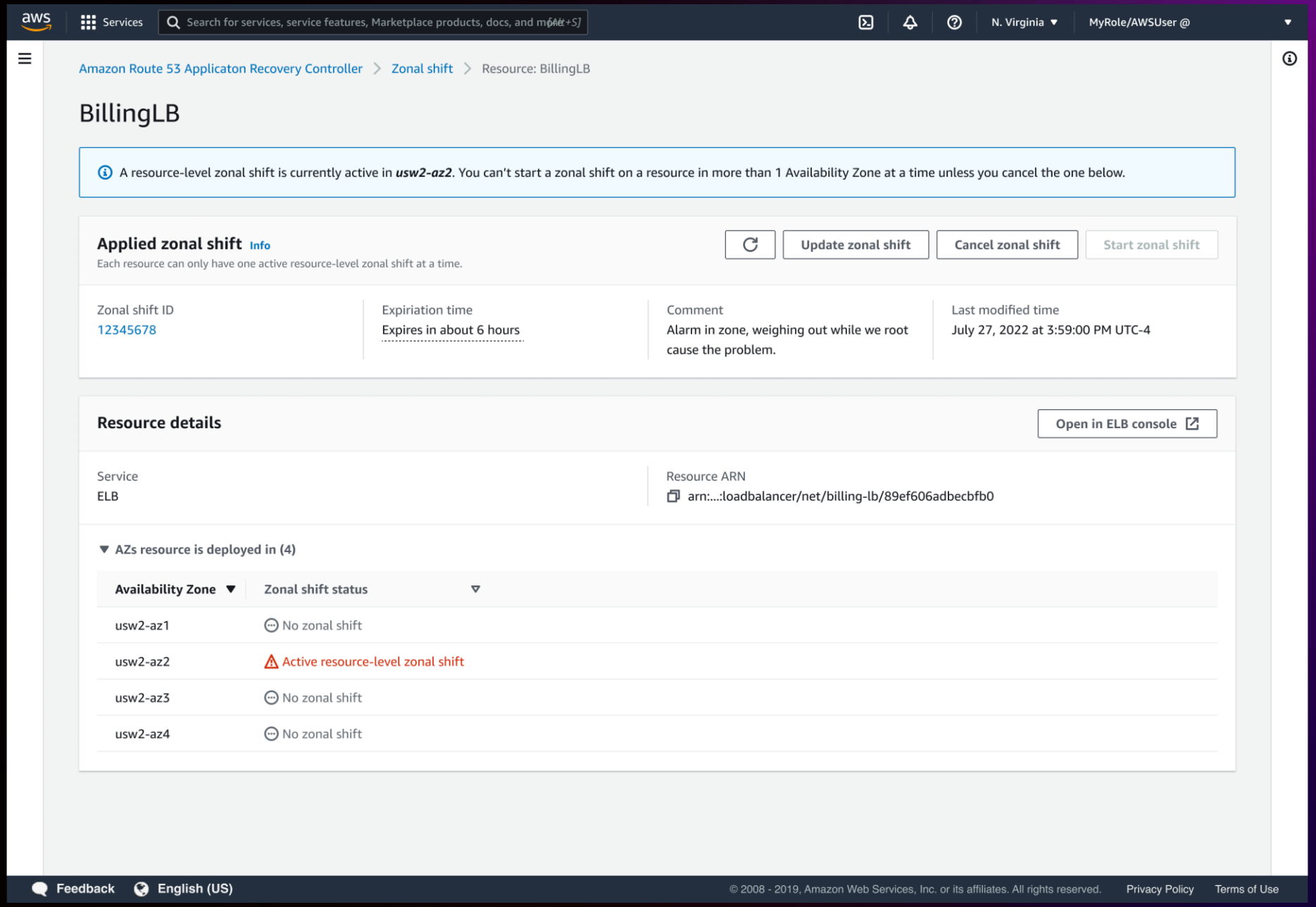
Navigate to Route 53 Application Recovery Controller



Shift resources away from an AZ



Safety rule



Best practices of zonal shift

- Turn off cross-zone load balancing for your ALB and NLB
- Provision sufficient capacity in each AZ to withstand the loss of capacity in one AZ
- Ensure all zonal replicas are healthy and taking traffic
- Test in advance
- Practice using the API/CLI

Multi-Region key capabilities

Use cases

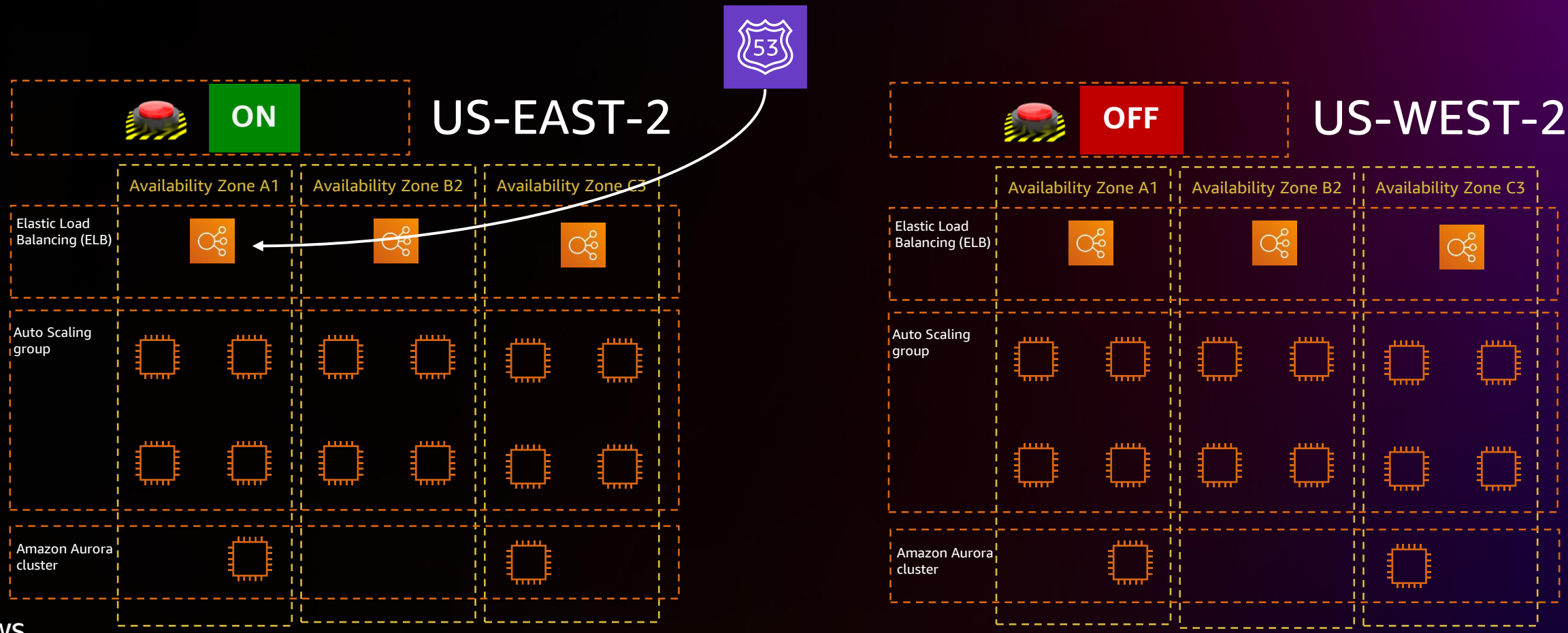
1. Mitigation of failures: Greater control over multi-Region recovery mechanisms
2. Recovery-oriented apps: Build and manage apps that can recover within minutes from almost all failures
3. Central control over application recovery operations across organizations

Feature 1: Routing controls

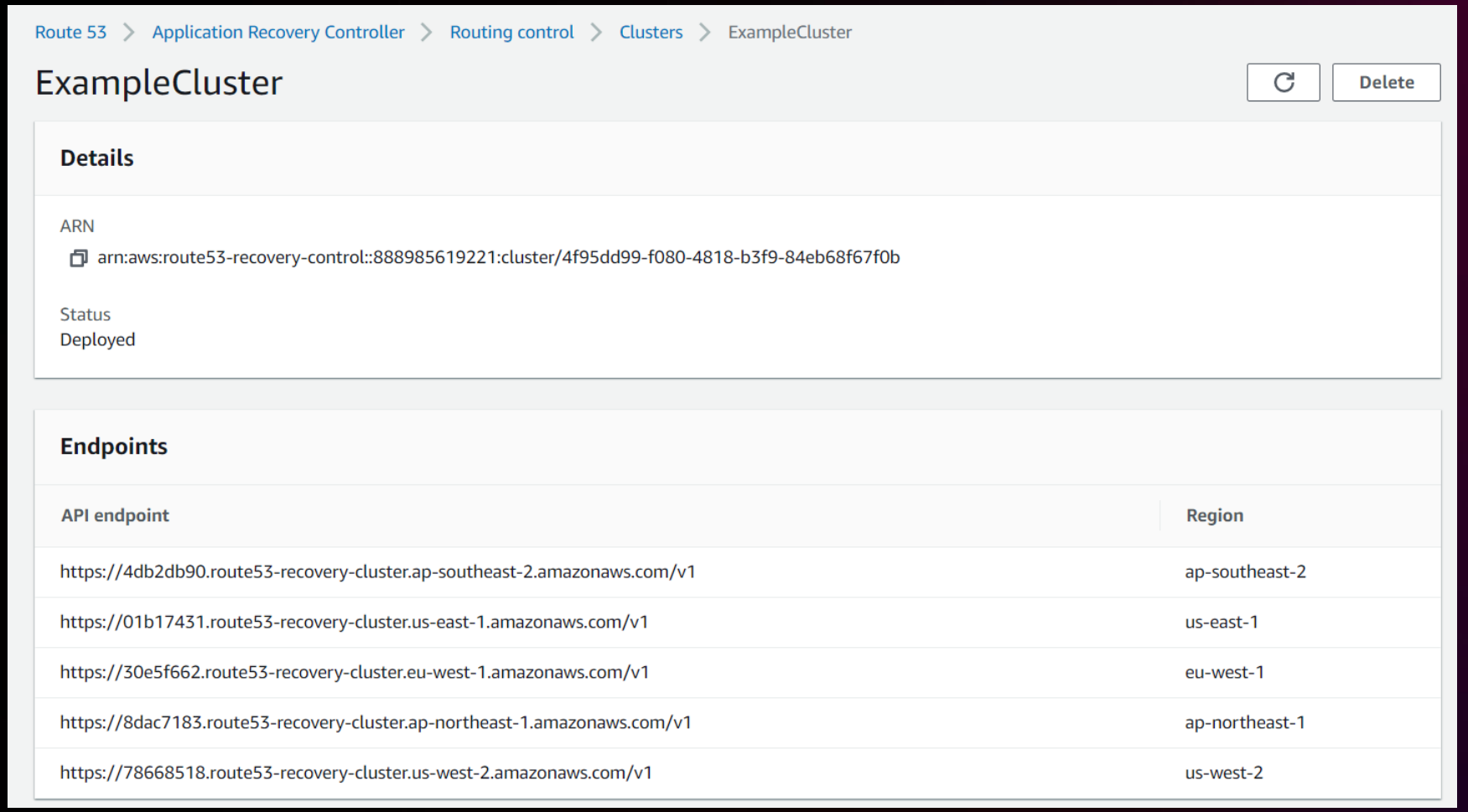
1. Reliable – Your routing controls are durably stored in five AWS Regions and can be changed through any one of five unique Regional endpoints
2. Single tenant – Your routing controls are hosted on Amazon EC2; changes to your routing control effect changes through Route53 data plane (100% availability SLA)

Feature 1: Routing control

On/off switches that can be used in place of health checks



Routing controls stored in 5 different Regions



Feature 2: Safety rules

Safety rules

Customer-configurable rules that set pre-conditions when making changes to routing controls

What are examples of safety rules?

Avoid turning off all the Regions for an application at the same time

Feature 3: Readiness check

Recovery group

Assessment criteria	Cell 1: Primary Region	Cell 2 : Standby Region
Provisioned capacity	500 RCU and 800 WCU	
Resource limits	DynamoDB read throughput limits not matched **Remediation in progress**	
Replication latency	RPO>30 seconds	
Custom readiness checks	<Custom CloudWatch alarm>	

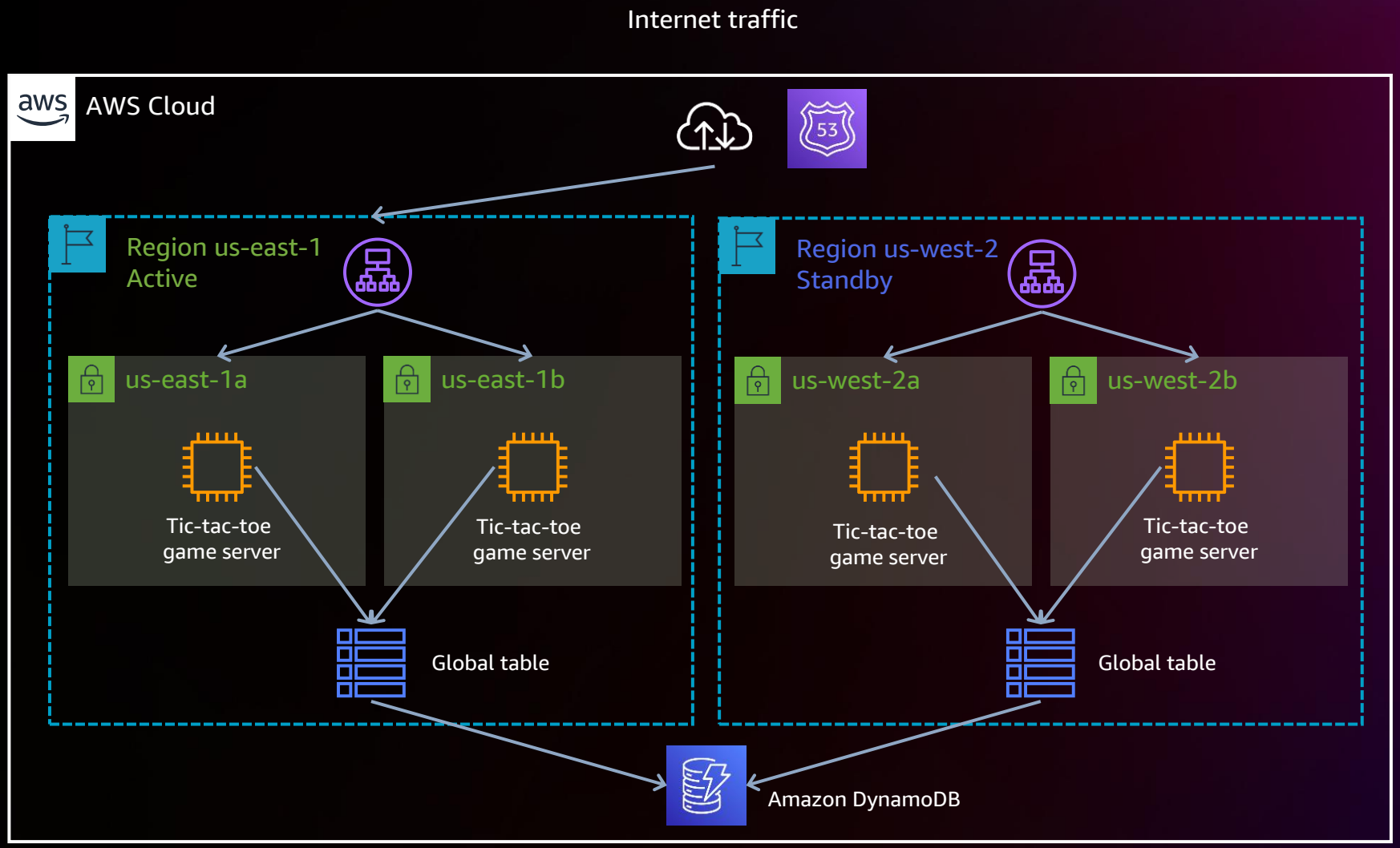
Checks can also be used for migration between Regions and/or accounts

Hands-on workshop

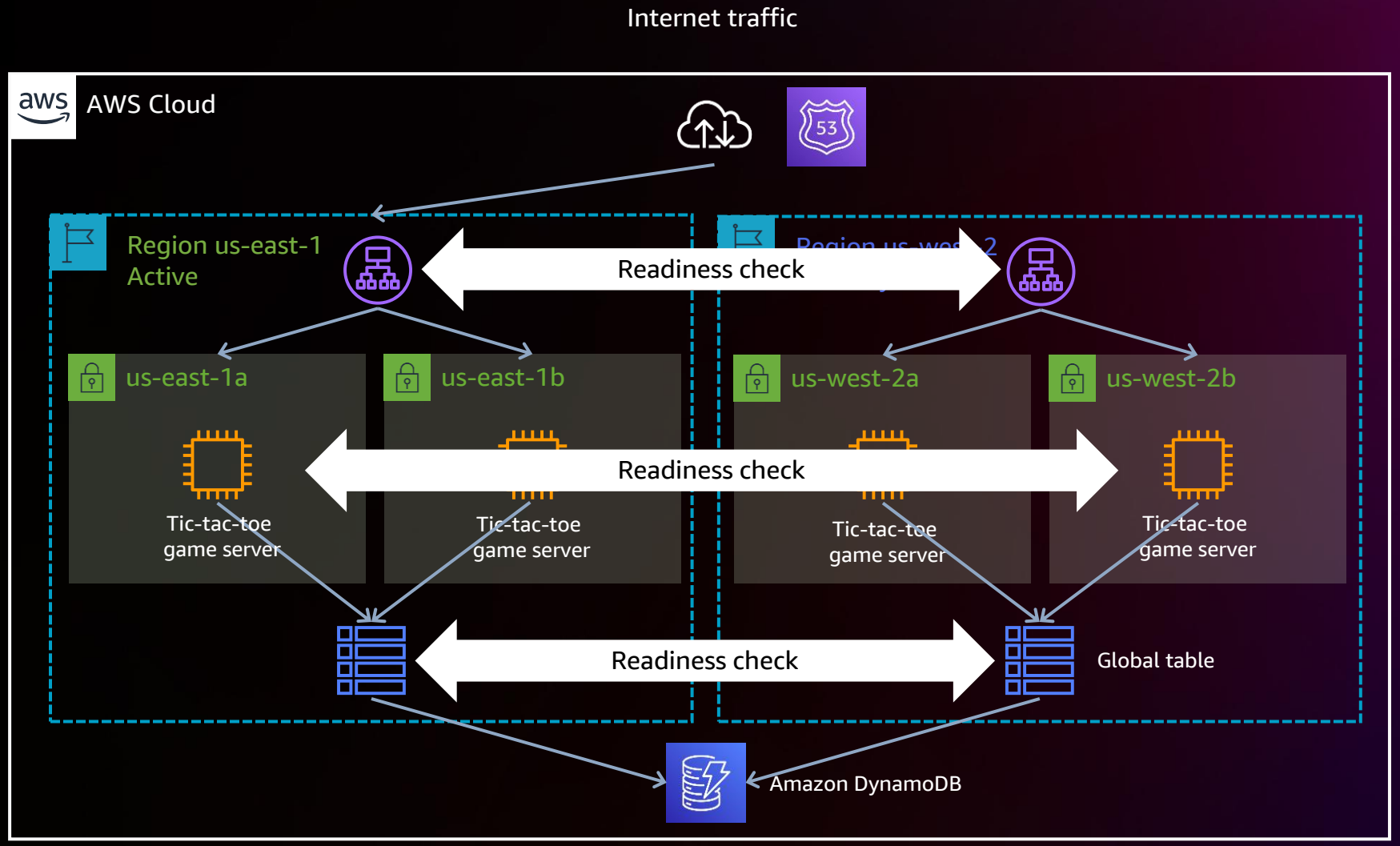
Let’s build!

Download the code and instructions from https://tinyurl.com/ya2kzb44

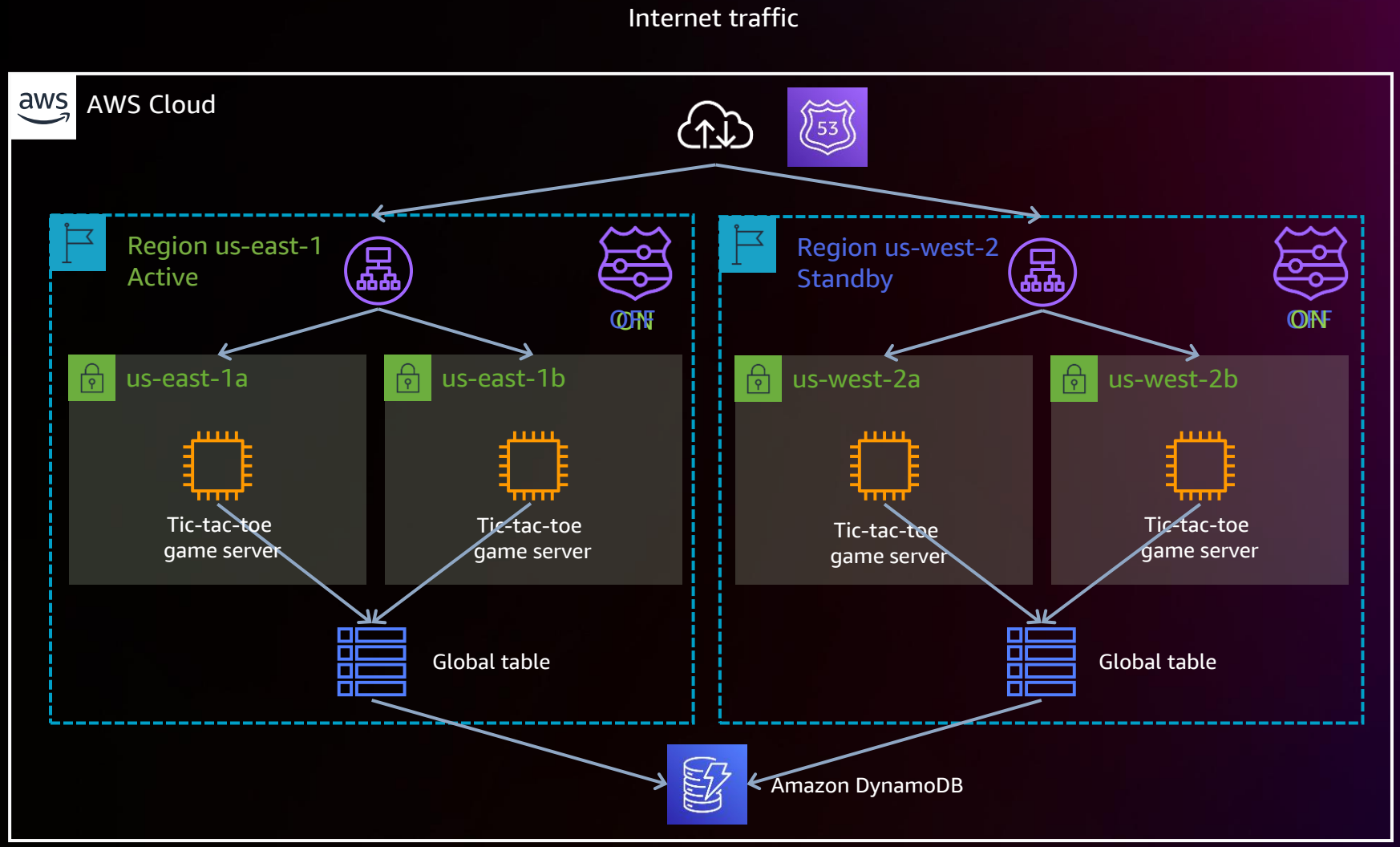
1. Set up a multi-Region application



2. Use readiness checks



3. Use routing controls and perform failover



Thank you!

Scott Wainstock
wainstoc@amazon.com

Stanley Su
sustanle@amazon.com

Please complete the session survey in the **mobile app**