AWS re:Invent

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

NET317-R2

Designing resilient applications using Amazon Route 53 ARC

Nate Dye (he/him)
Sr. Software Development Manager
Amazon Web Services

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

Agenda

1/ Designing for failure and automated recovery (15 mins)

2/ Amazon Route 53 application recovery controller (5 mins)

3/ Q&A (35 mins)

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

Recovery design goals

Reliable

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

Recovery design goals

Reliable

Safe

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

Recovery design goals

Reliable

Safe

Fast

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

Recovery design goals

Reliable

Safe

Fast

Categorical

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

Design for failure

Categories of failure

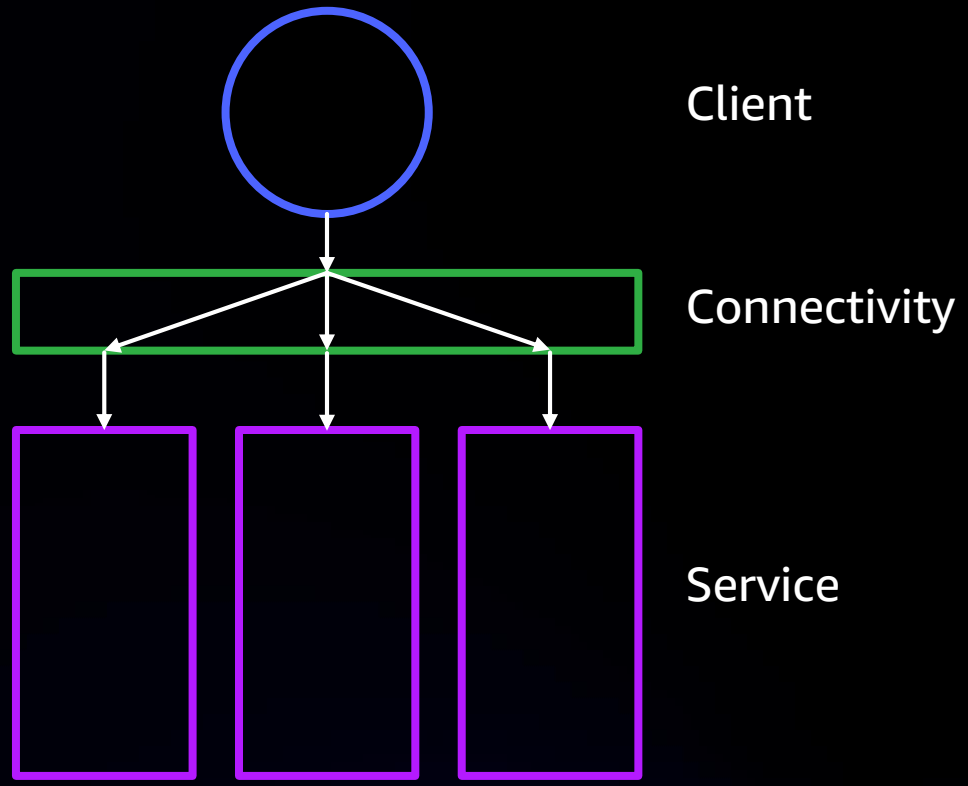
Code and config

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

Design for failure

Categories of failure

Code and config



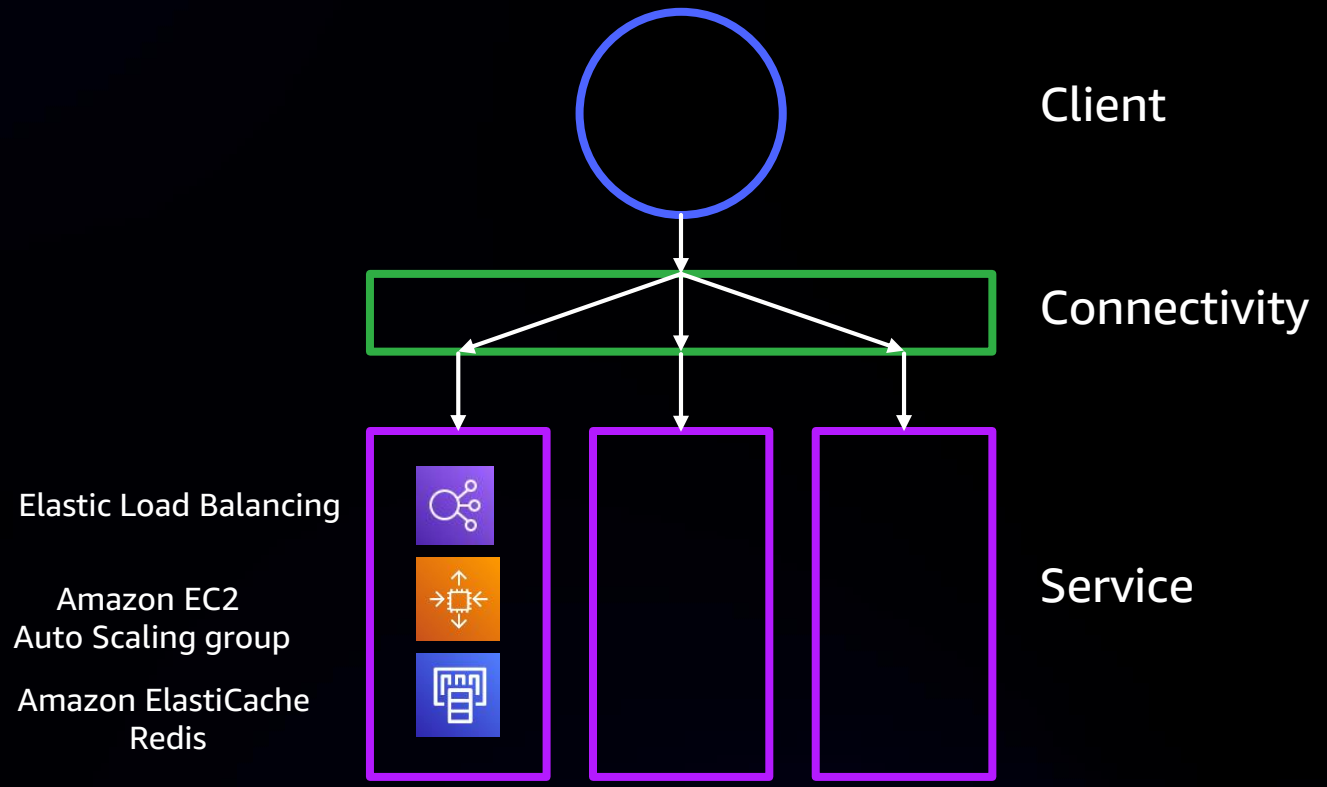
aws

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

Design for failure

Categories of failure

Code and config

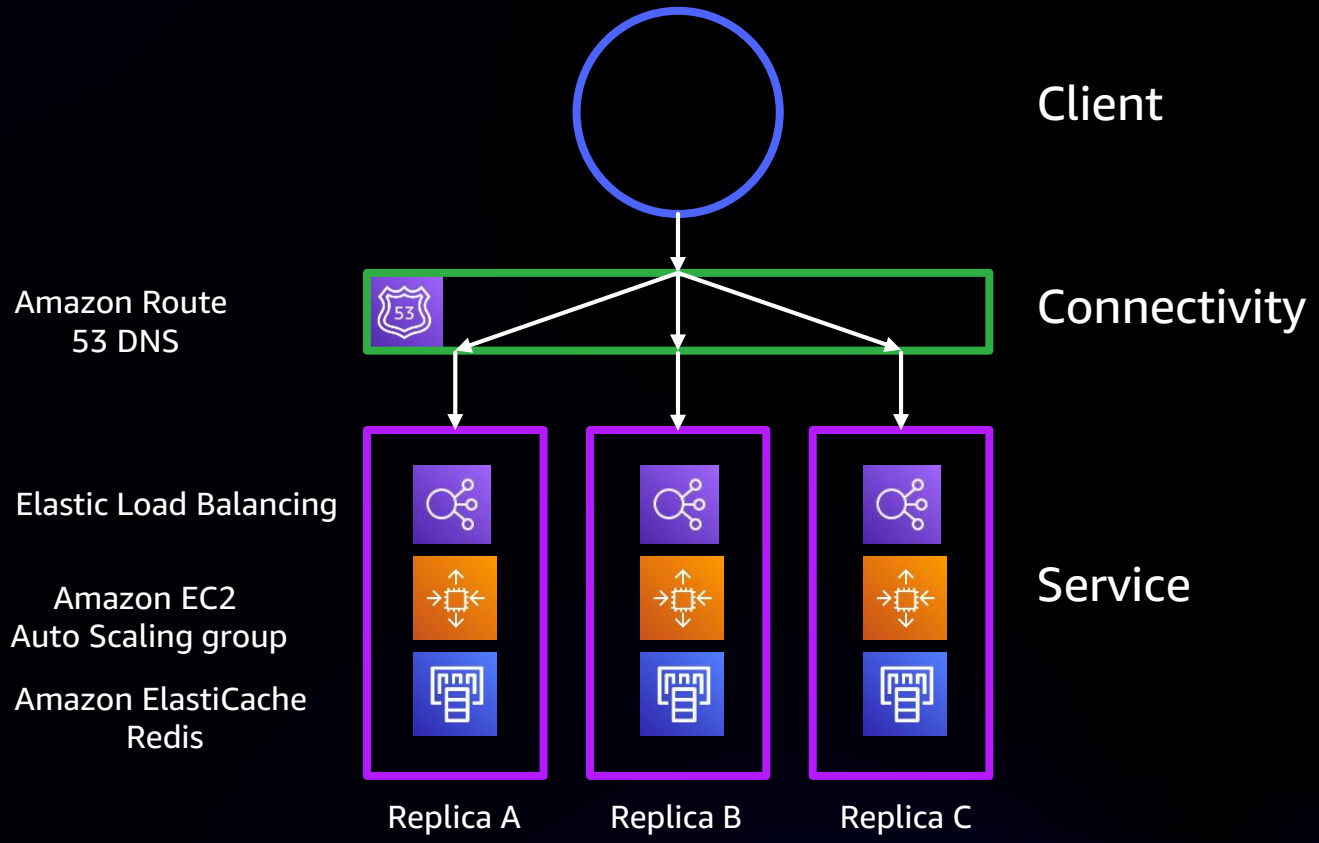


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

Code and config

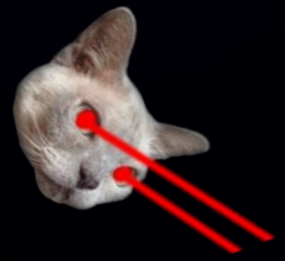


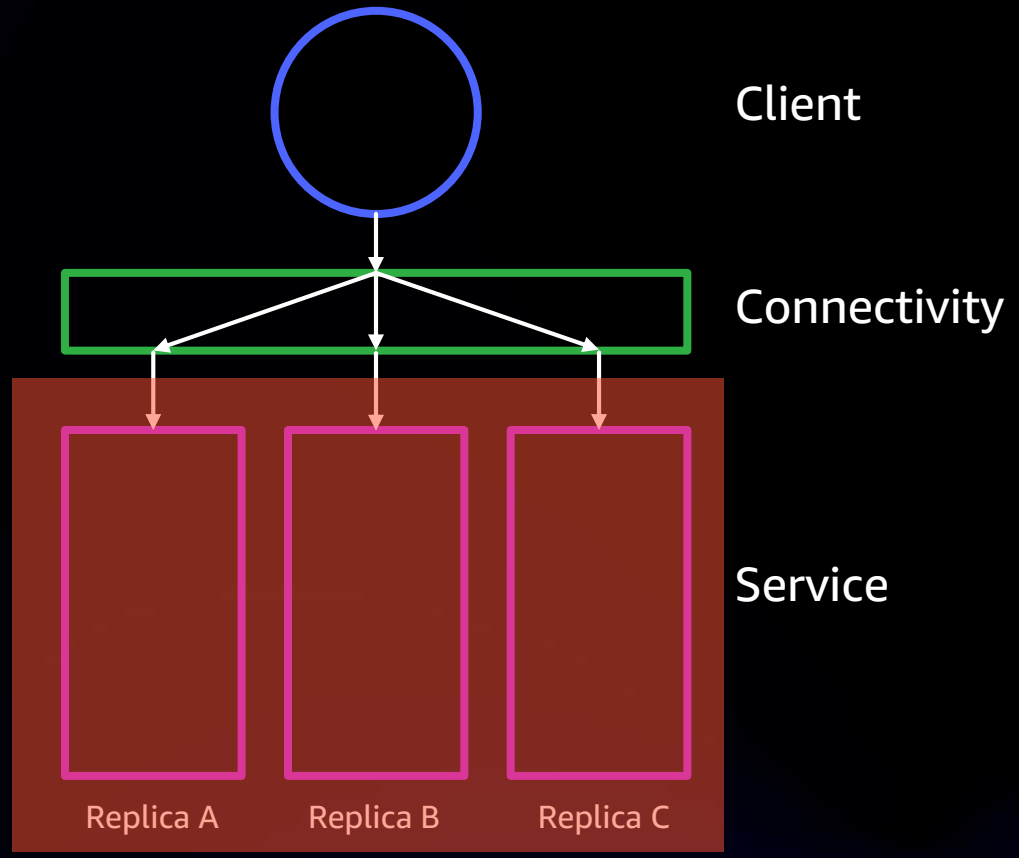
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

Code and config



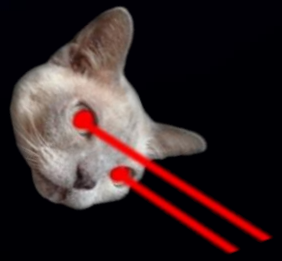


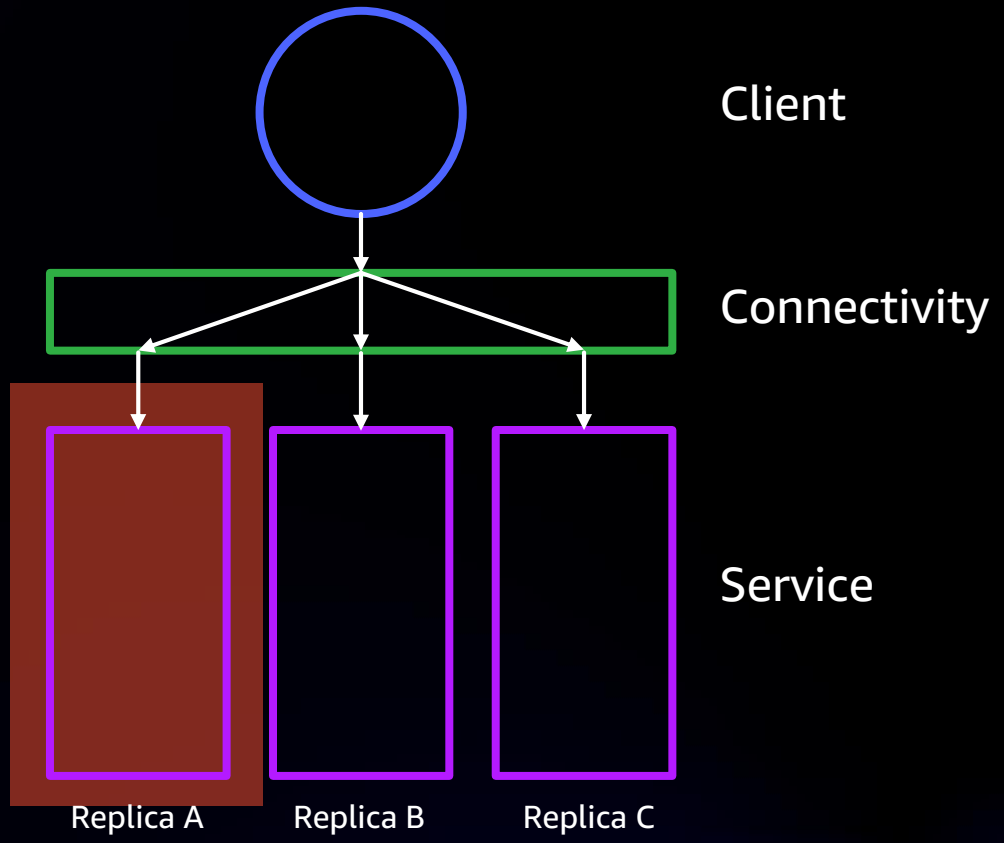
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

Code and config





Deploy to one replica at a time

aws

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

Design for failure

DEPLOY TO ONE REPLICA AT A TIME

Categories of failure

Code and config

Code and config failures

Bad code deployments
Application misconfiguration
Security group misconfiguration
Routing policy misconfiguration
TLS certificates misconfiguration

Cert and credential expiry

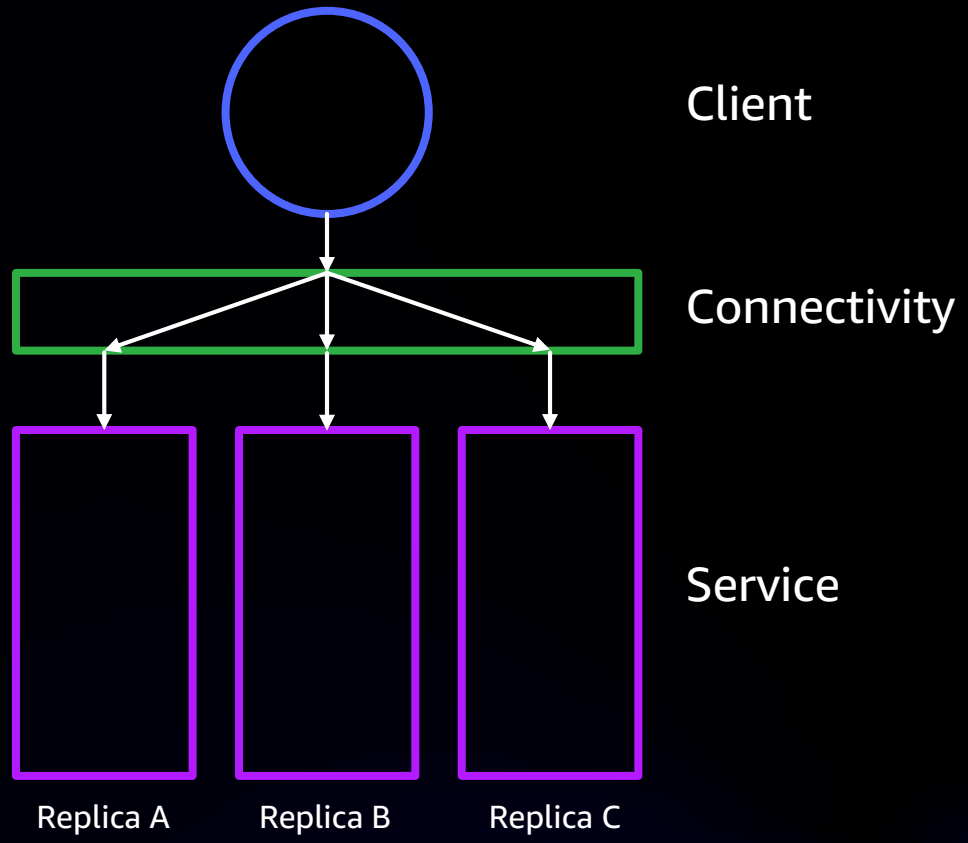
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

Code and config

Infrastructure



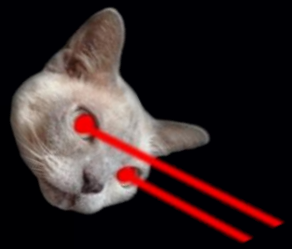
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

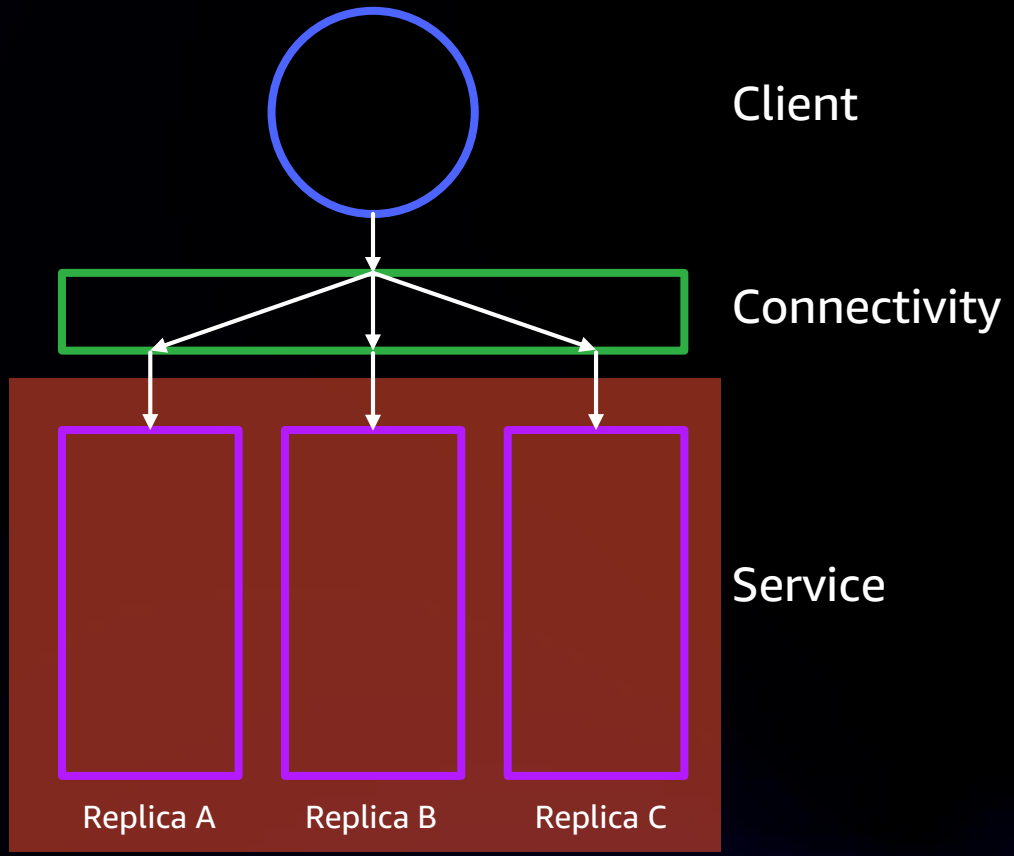
Design for failure

Categories of failure

Code and config

Infrastructure





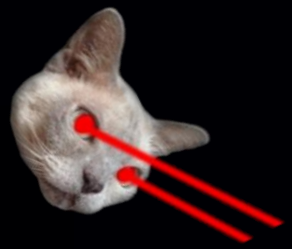
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

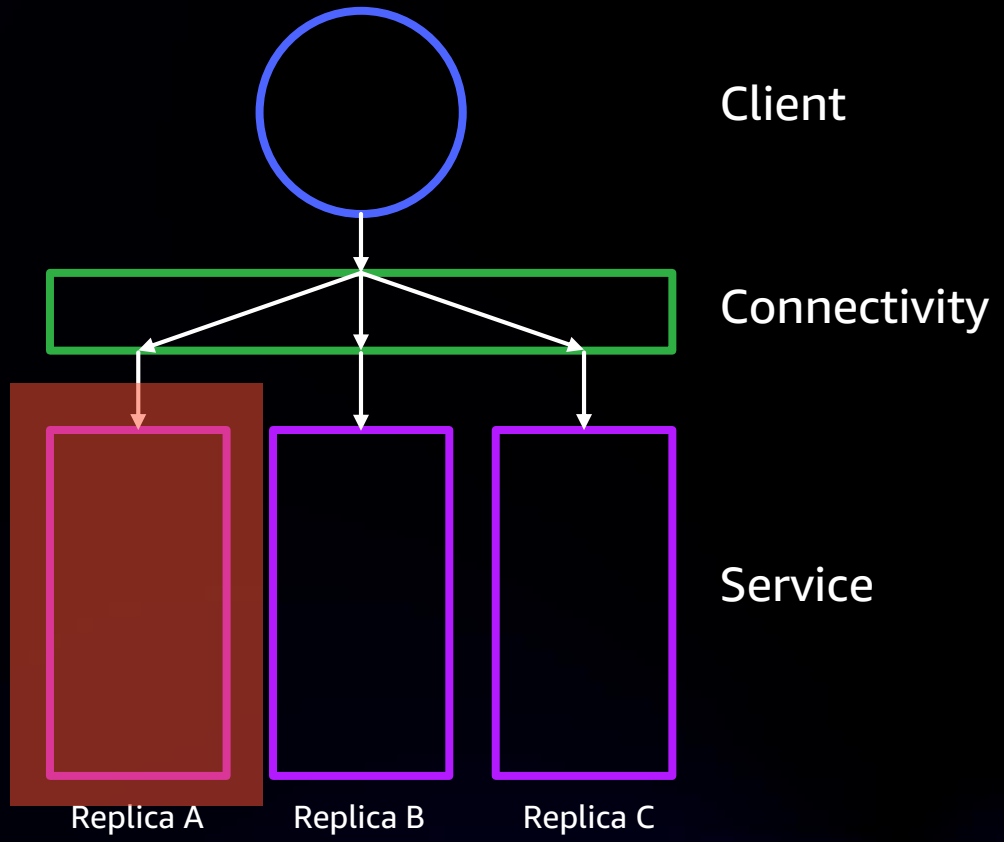
Design for failure

Categories of failure

Code and config

Infrastructure





Place replicas on independent infrastructure

aws

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

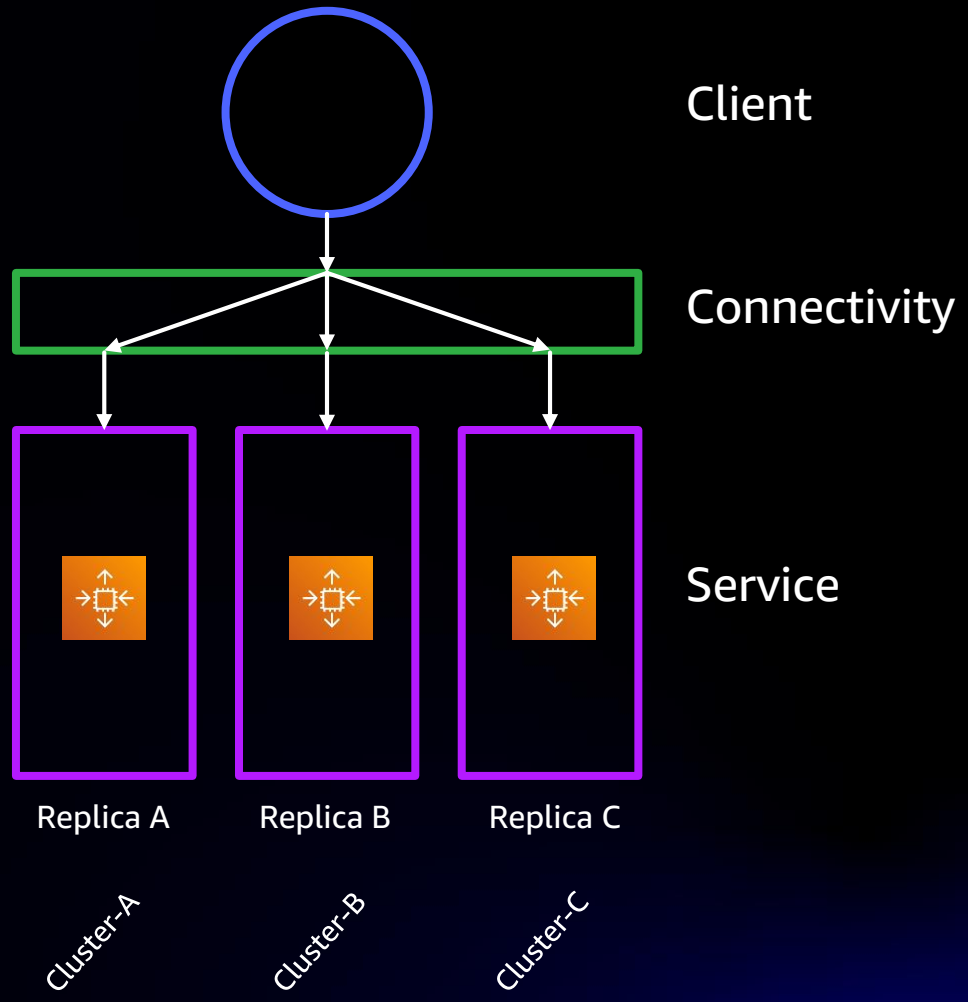
Design for failure

PLACE REPLICAS ON INDEPENDENT INFRASTRUCTURE

EC2 placement groups

Availability Zones

Regions



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

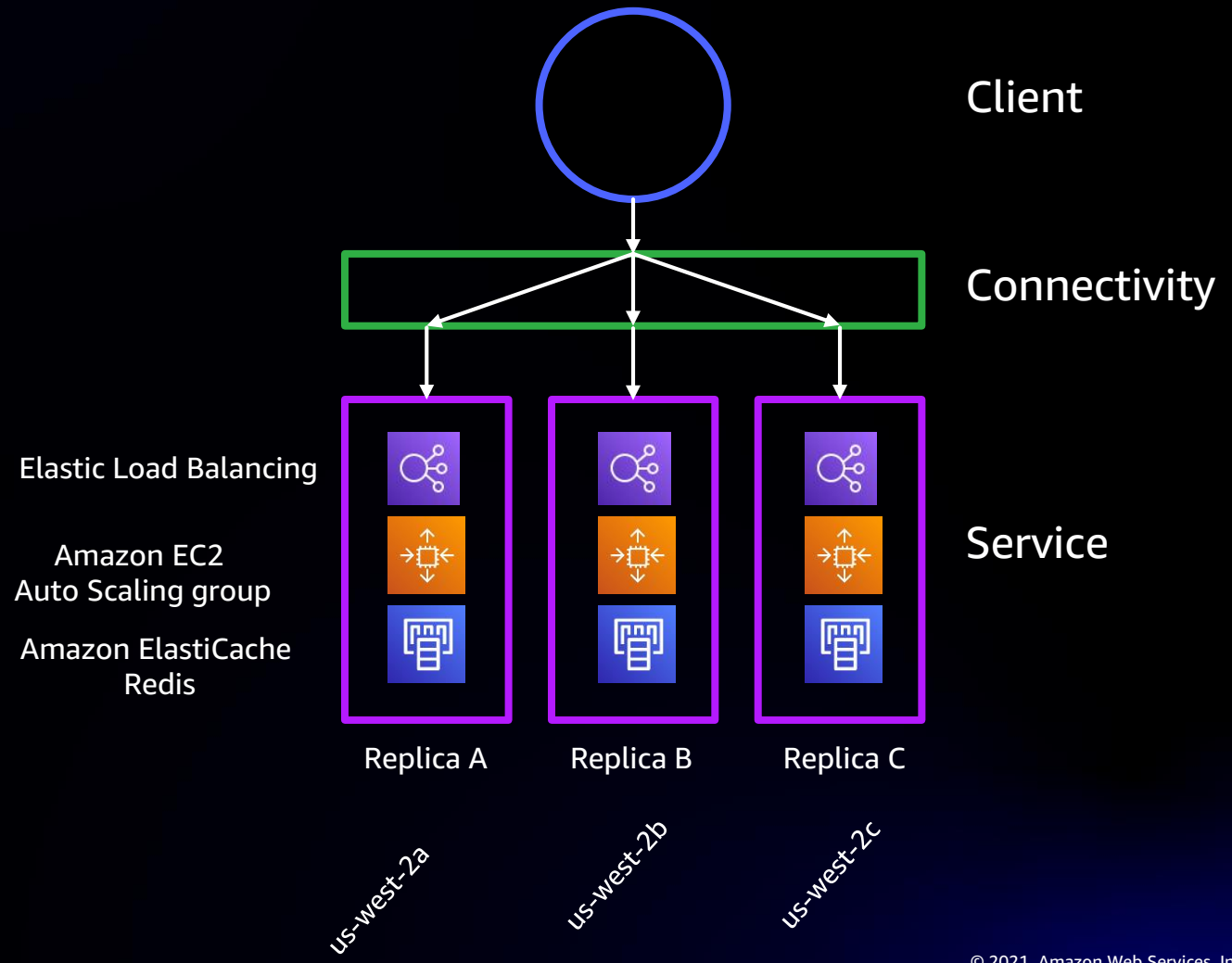
Design for failure

PLACE REPLICAS ON INDEPENDENT INFRASTRUCTURE

EC2 placement groups

Availability Zones

Regions



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

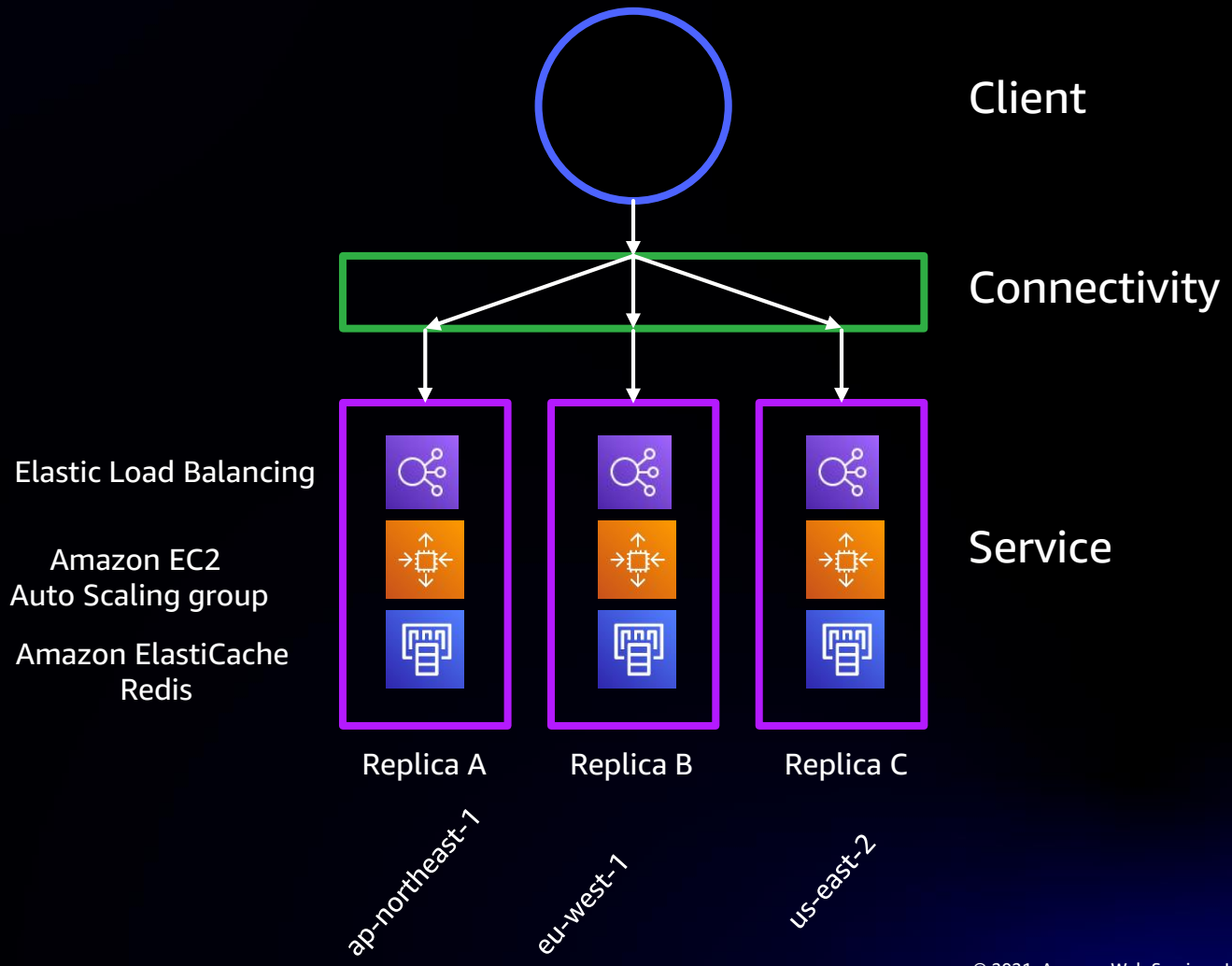
Design for failure

PLACE REPLICAS ON INDEPENDENT INFRASTRUCTURE

EC2 placement groups

Availability Zones

Regions

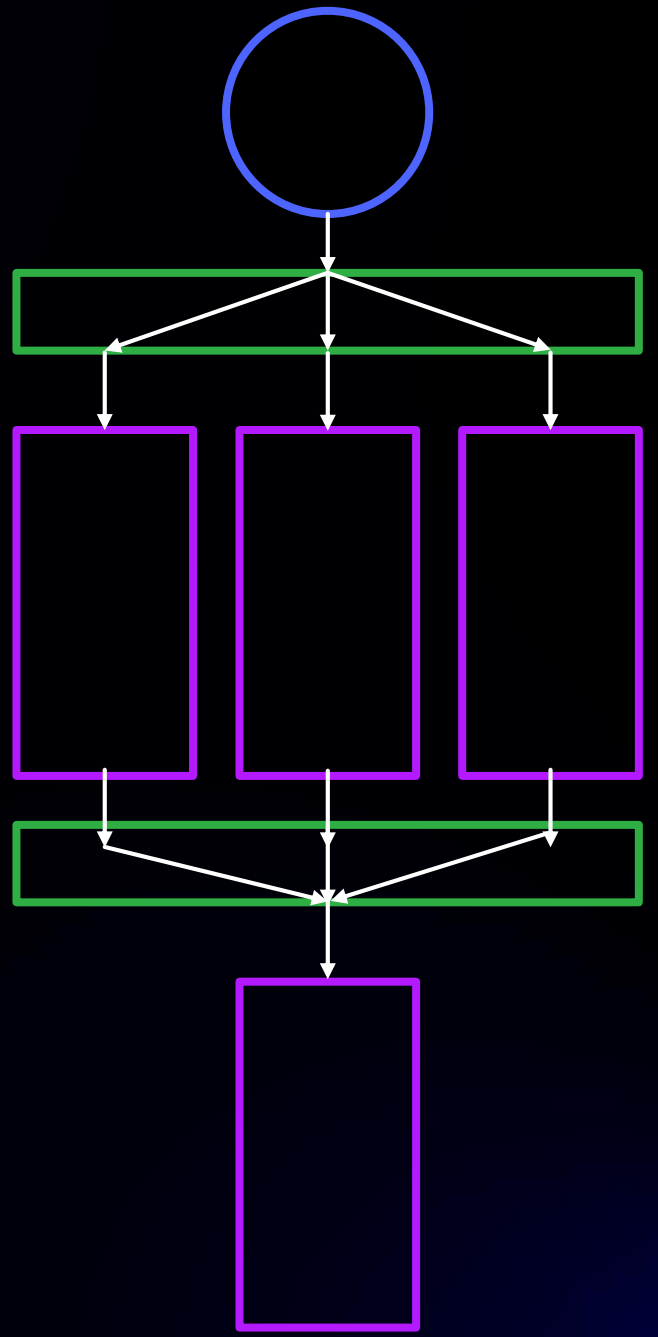


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies



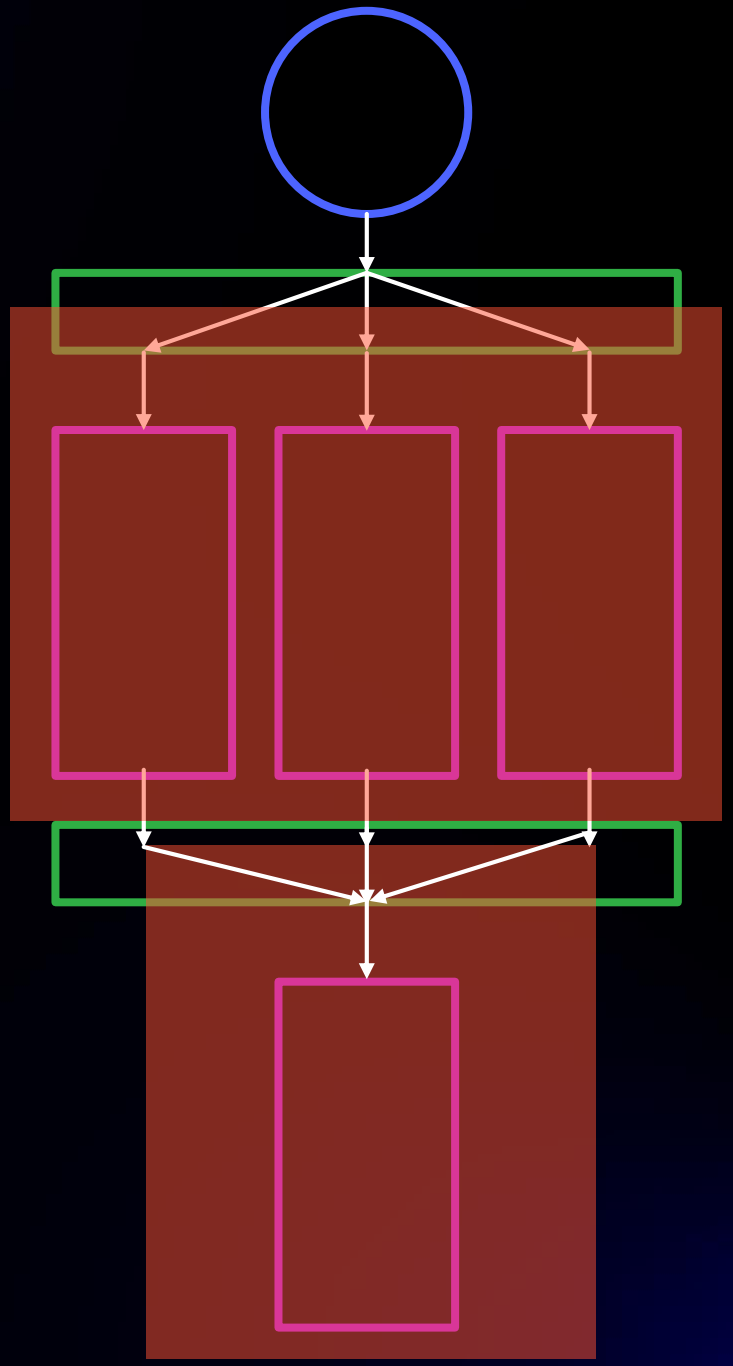
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies





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

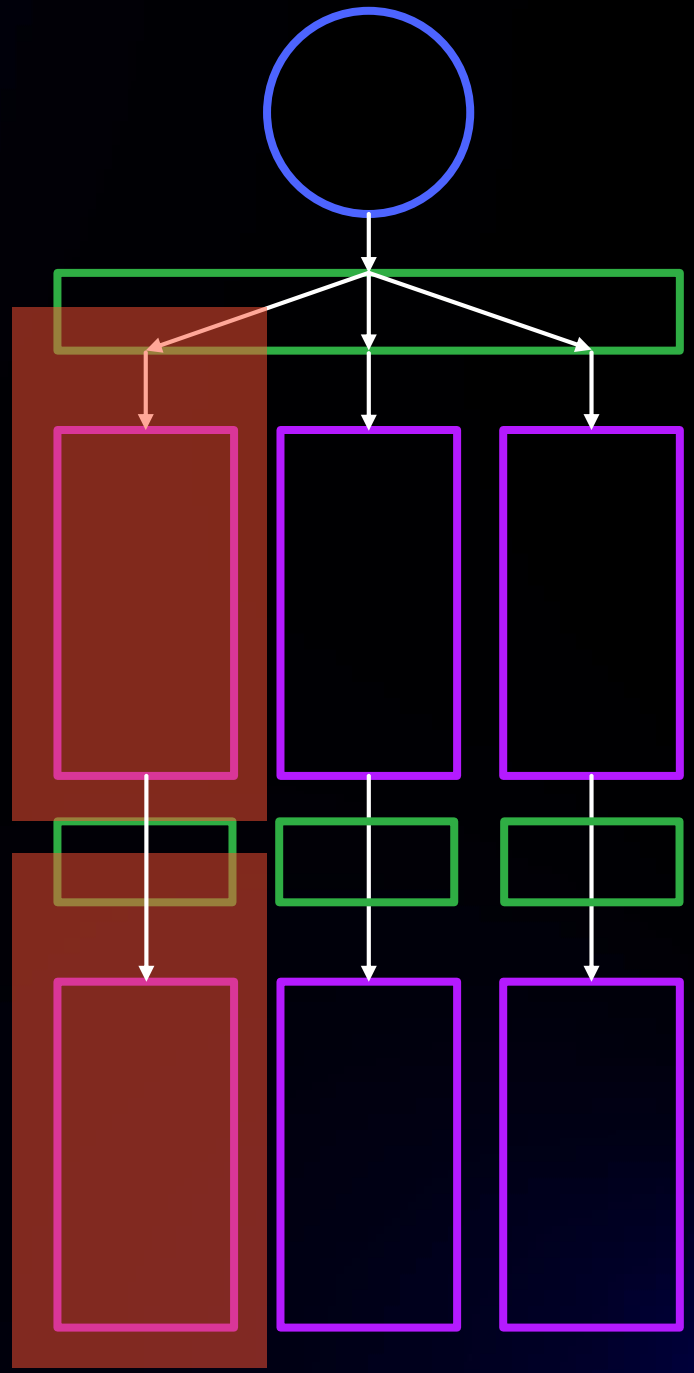
Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies



Use independent dependencies

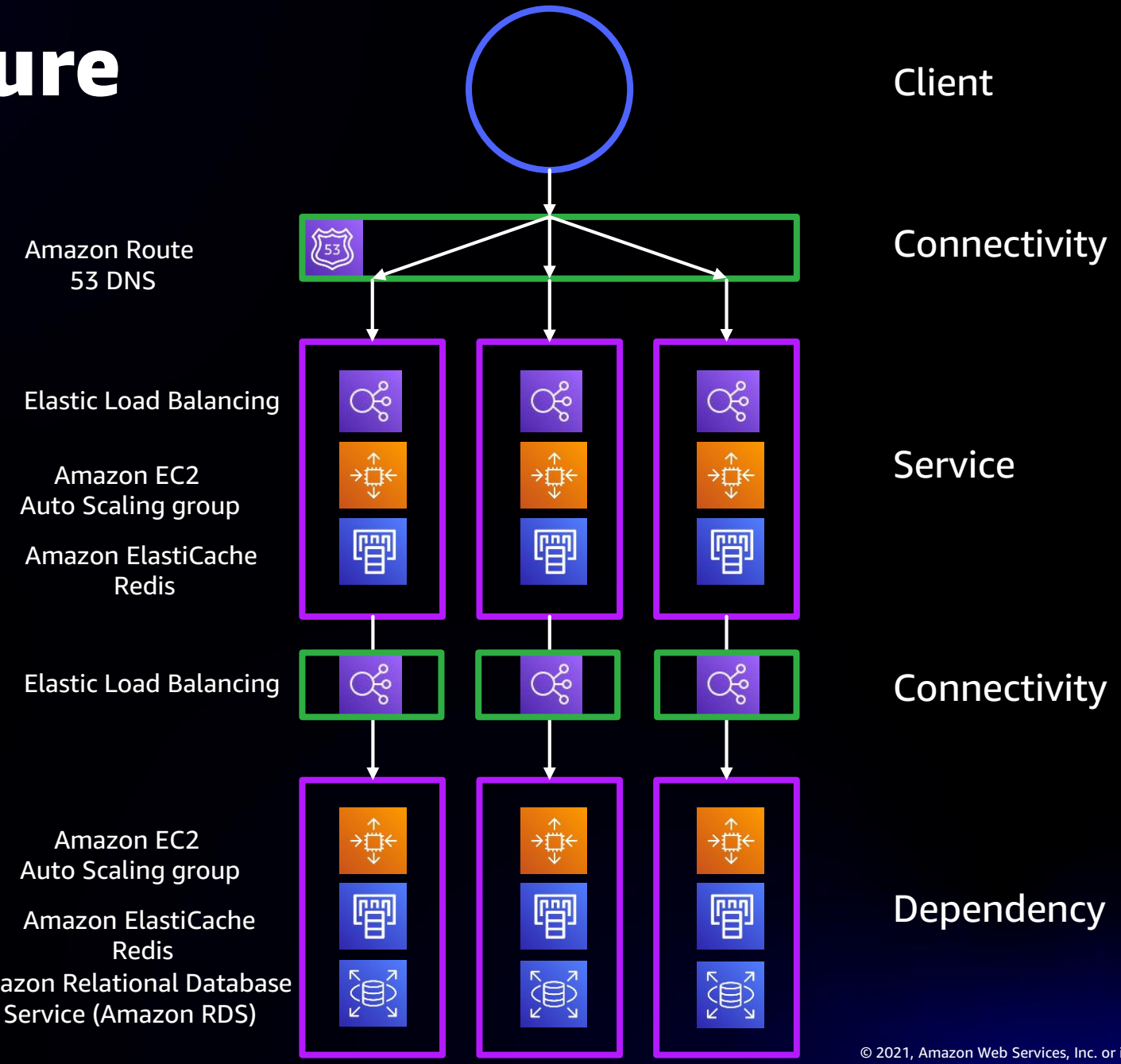


aws

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

Design for failure

USE INDEPENDENT DEPENDENCIES

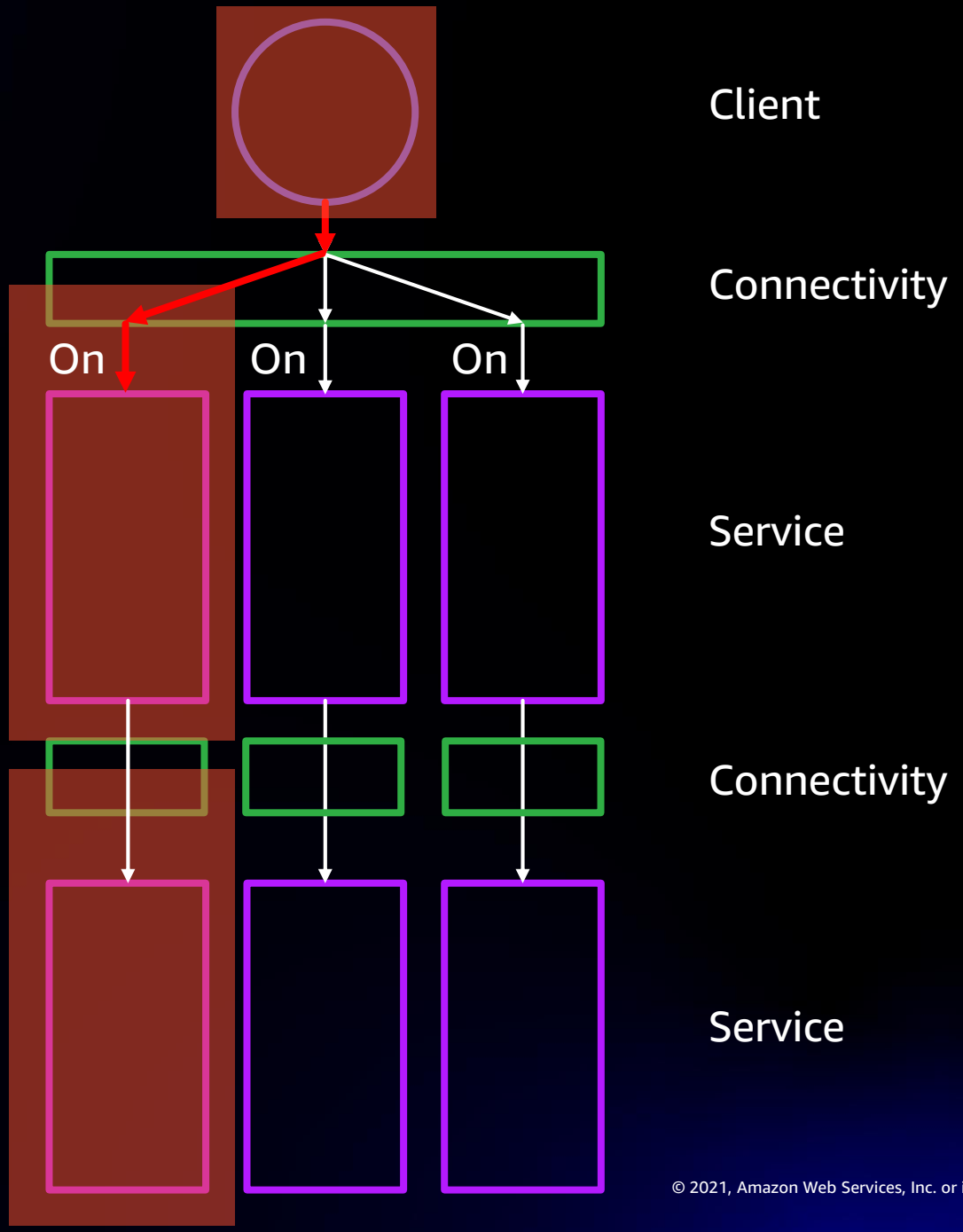


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies

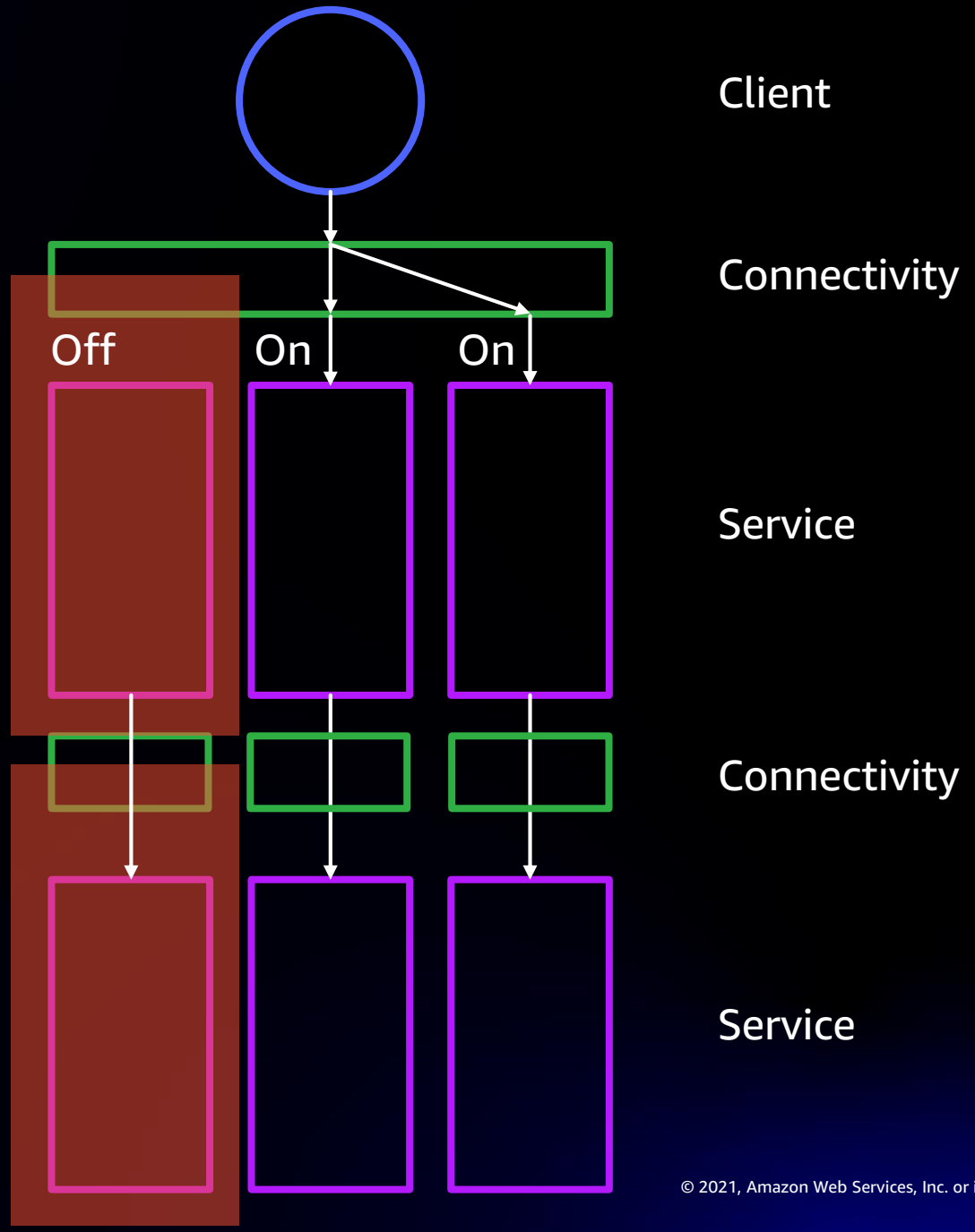


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies



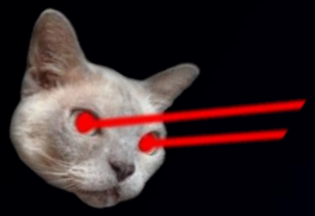
aws

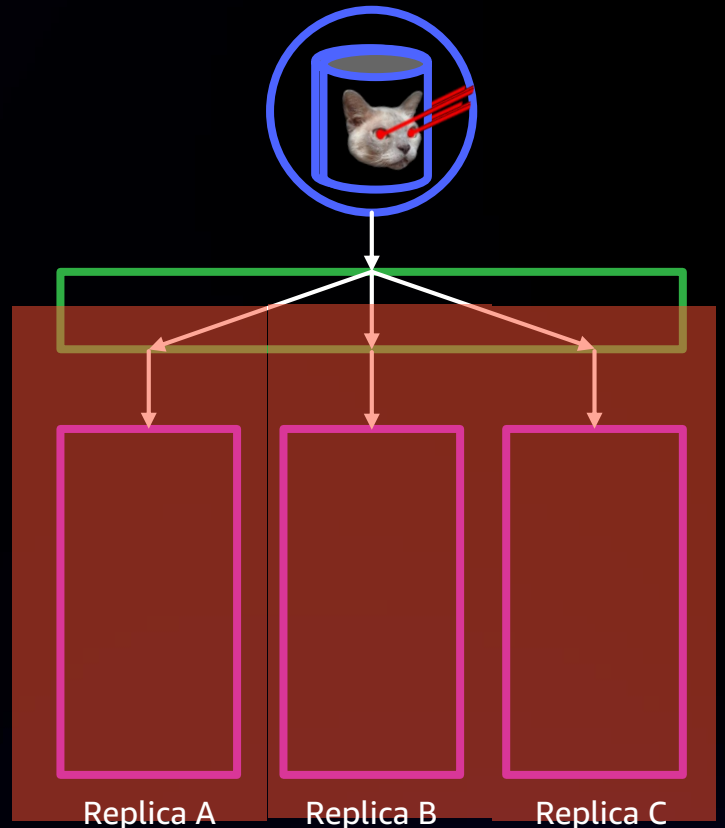
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies
- Data and state



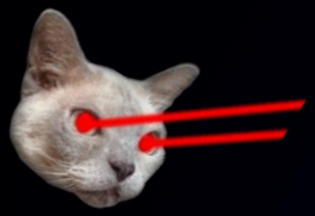


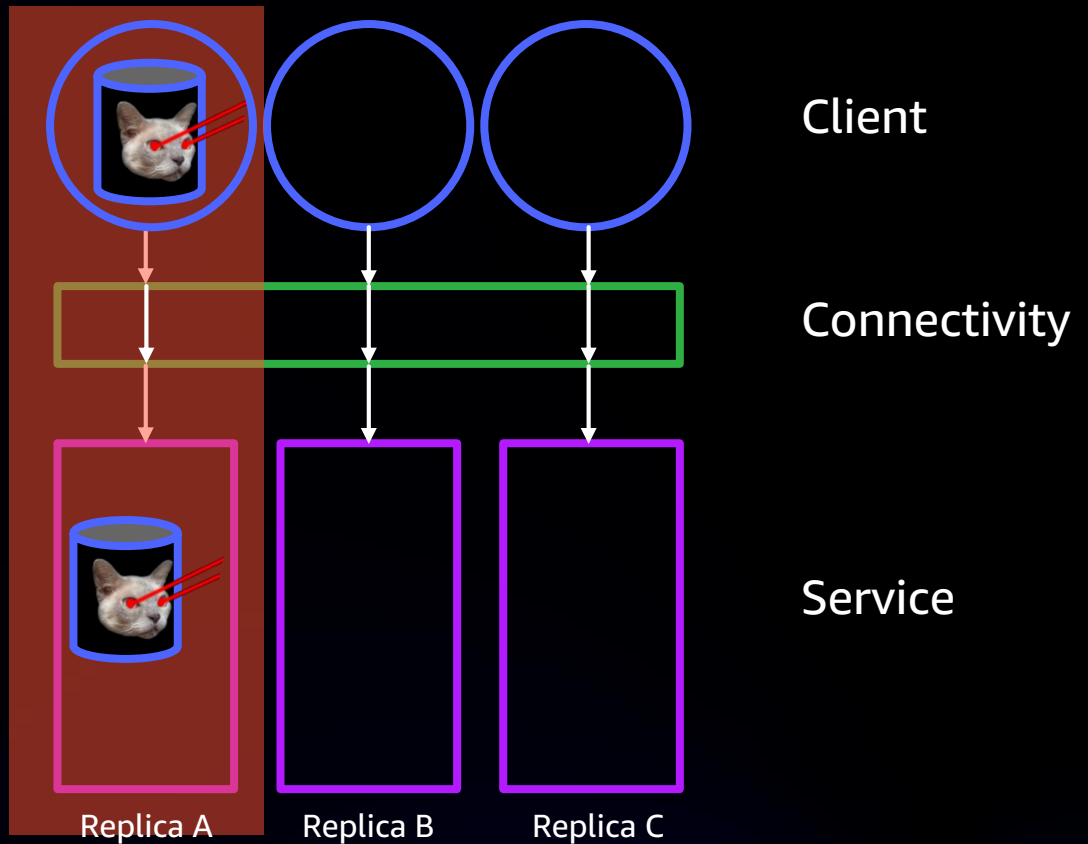
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Design for failure

Categories of failure

- Code and config
- Infrastructure
- Dependencies
- Data and state





Shard workloads and data

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

Design for failure

SHARD WORKLOADS AND DATA

Amazon Builder’s Library: Workload isolation using shuffle-sharding

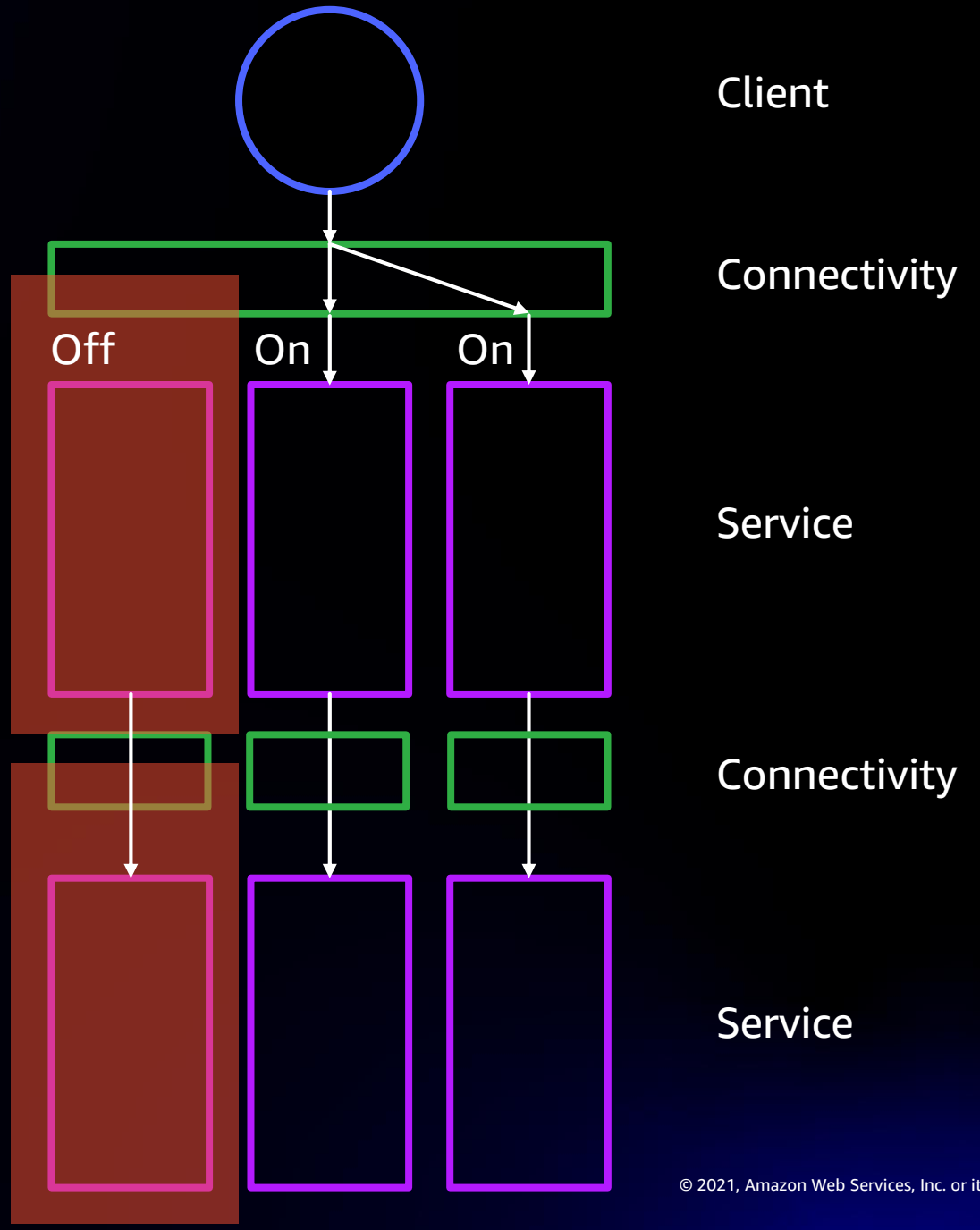
AWS re:Invent 2018: How AWS Minimizes the Blast Radius of Failures (ARC338)

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

Design for failure

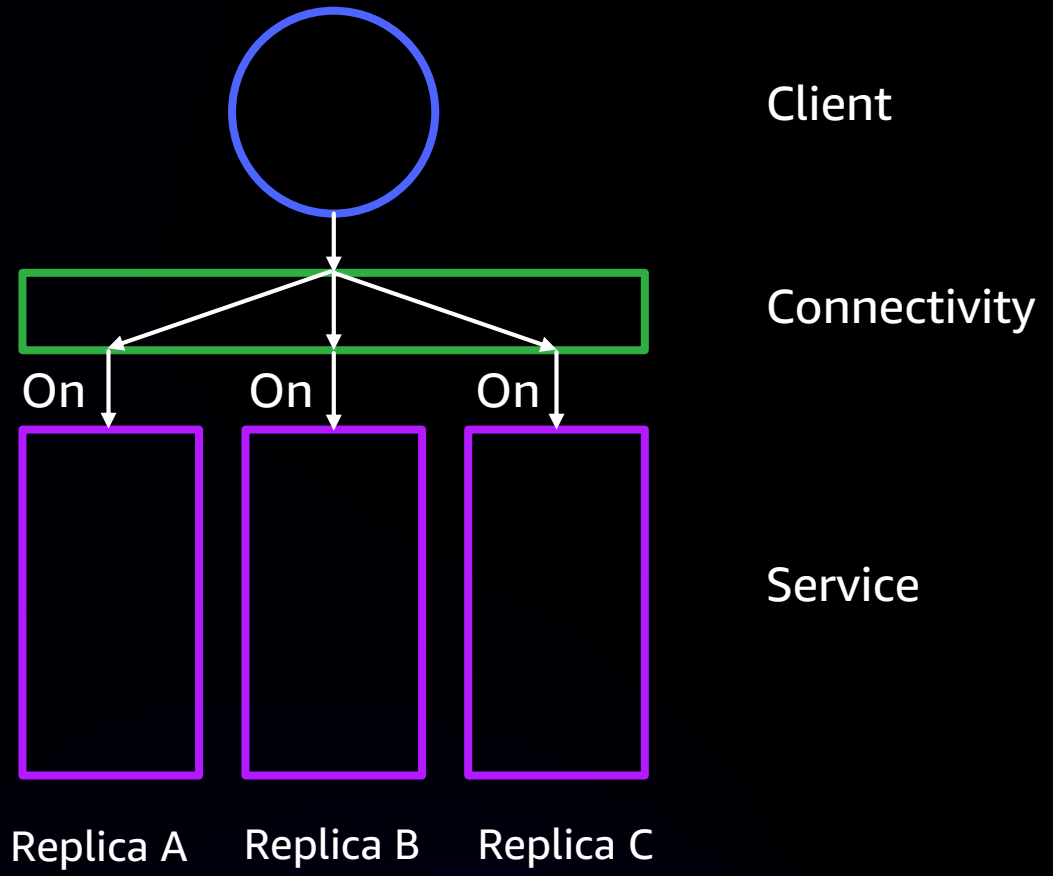
Categories of failure

- Code and config
- Infrastructure
- Dependencies
- Data and state



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

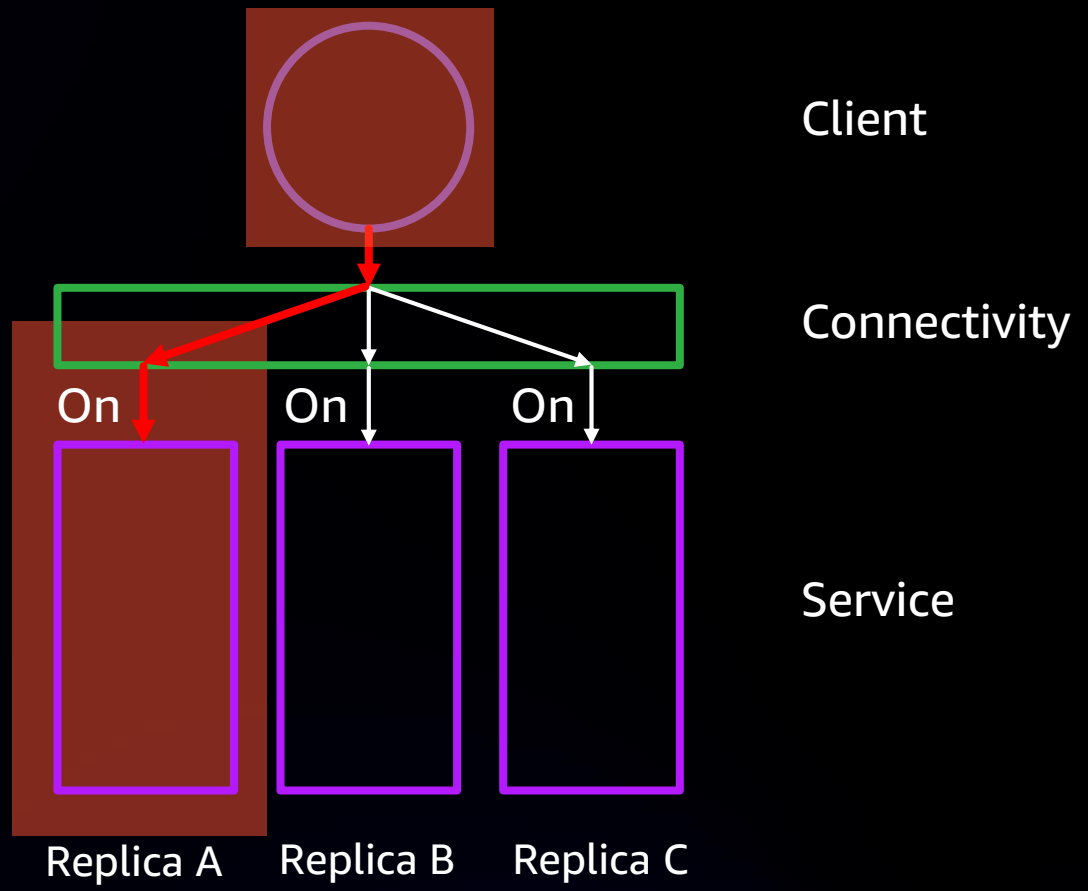
Detecting failure



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

Detecting failure

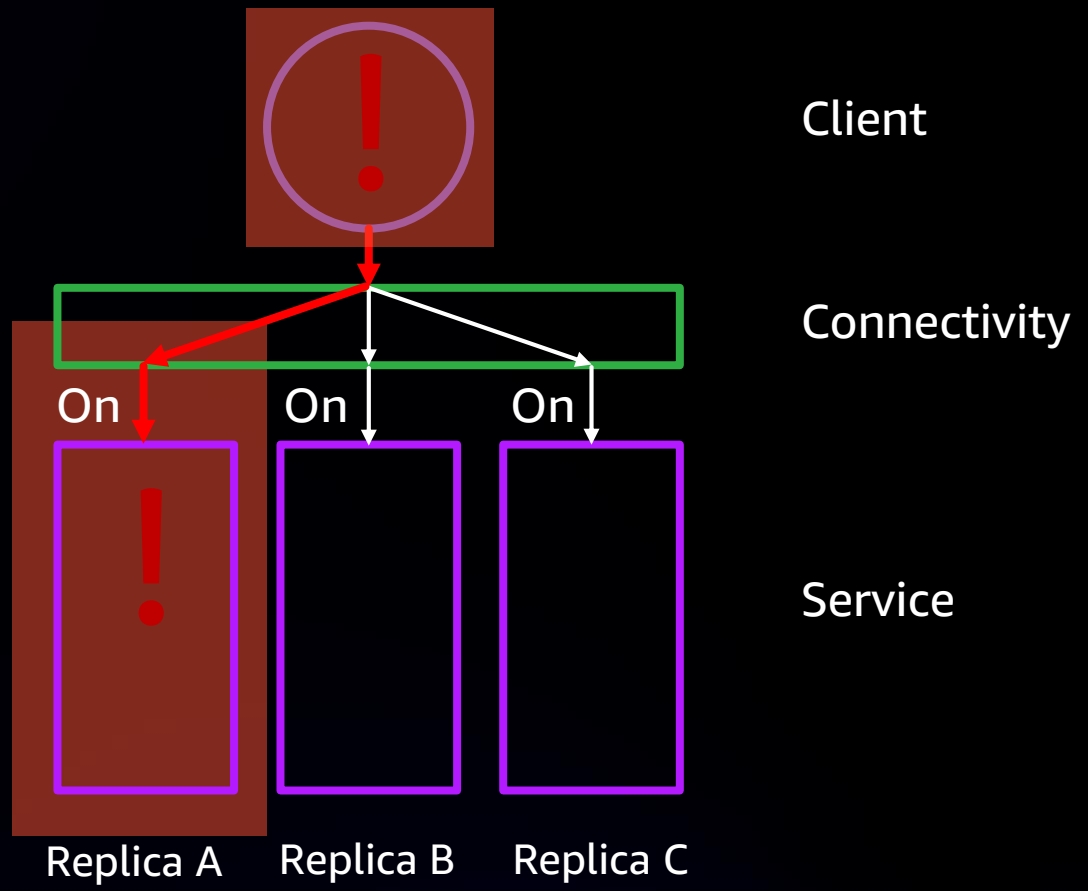
1. A replica failure impacts clients



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

Detecting failure

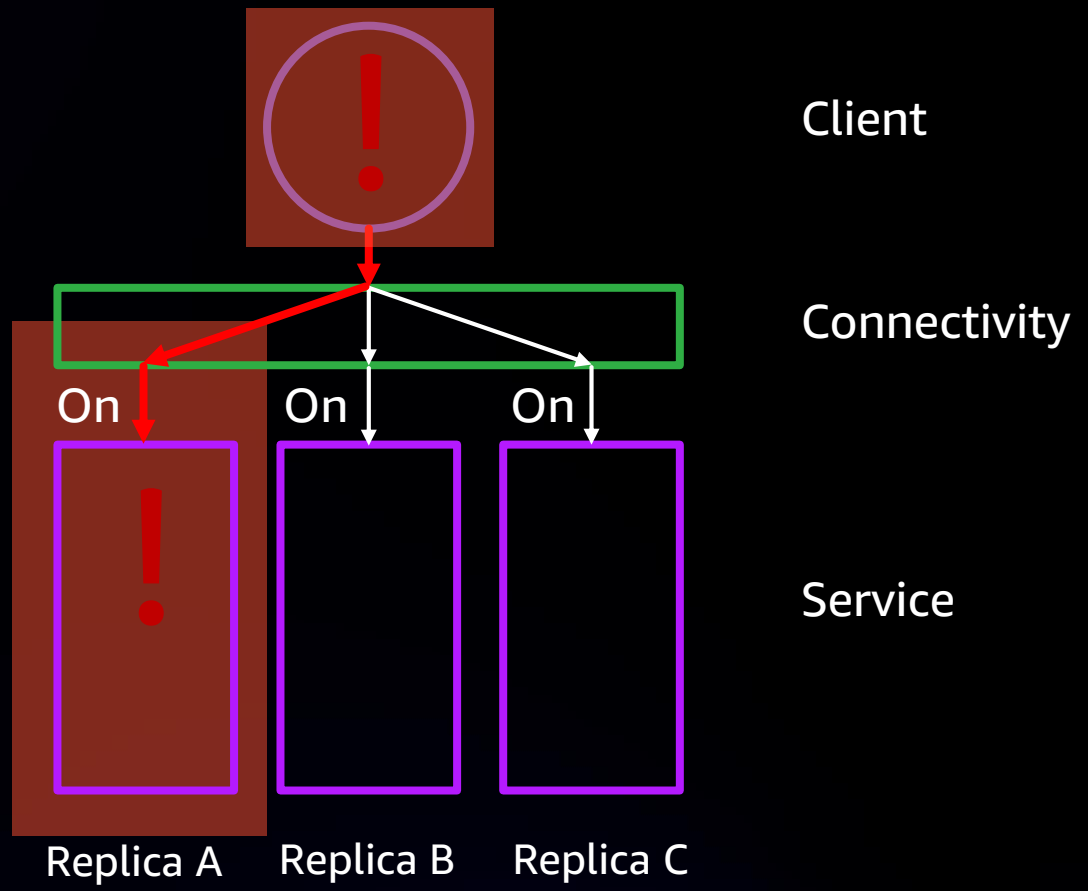
1. A replica failure impacts clients
2. Application monitors alert:
    a) Client impact



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

Detecting failure

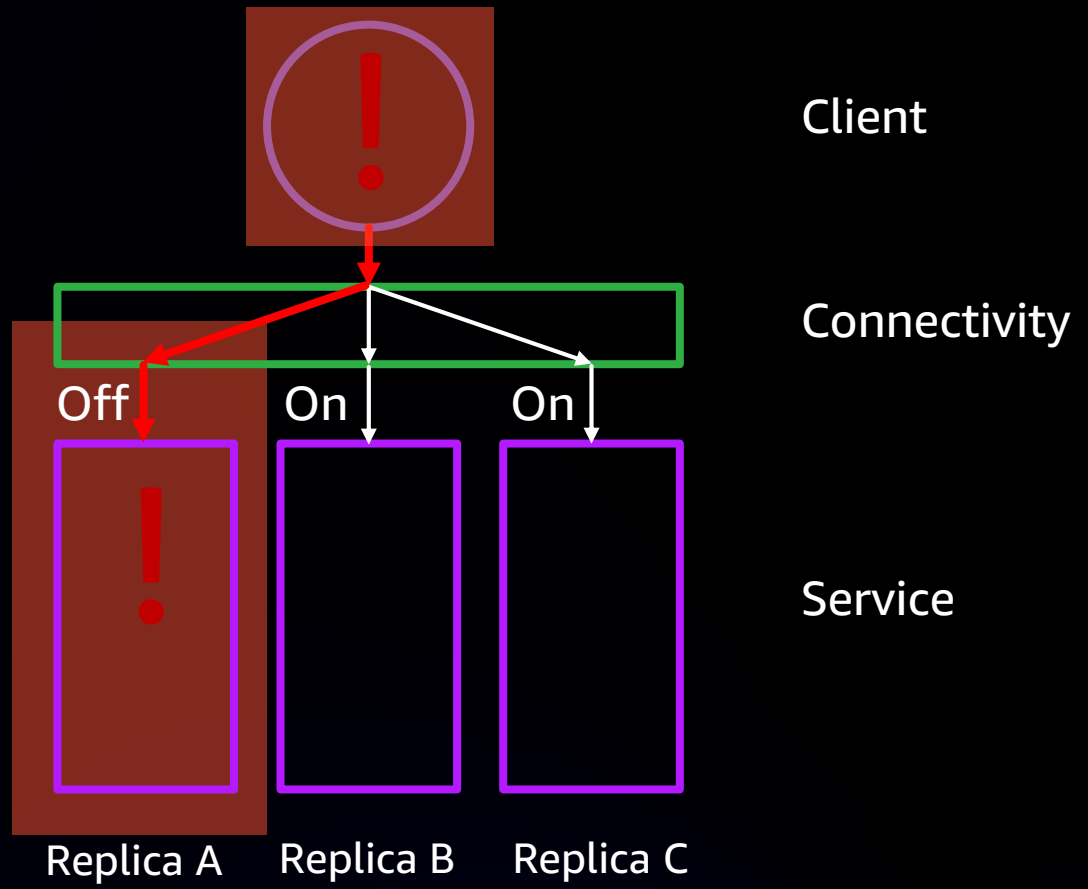
1. A replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) Replica A failure



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

Detecting failure

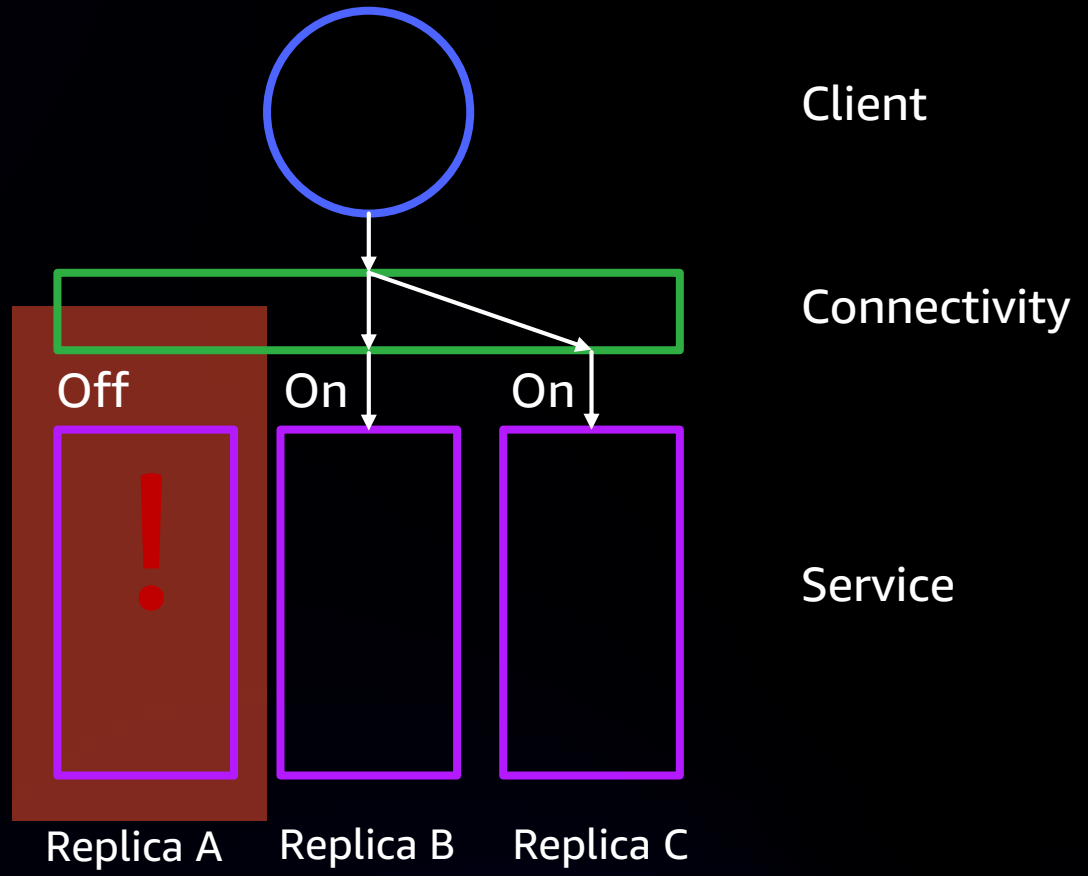
1. A replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) Replica A failure
3. Disable Replica A



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

Detecting failure

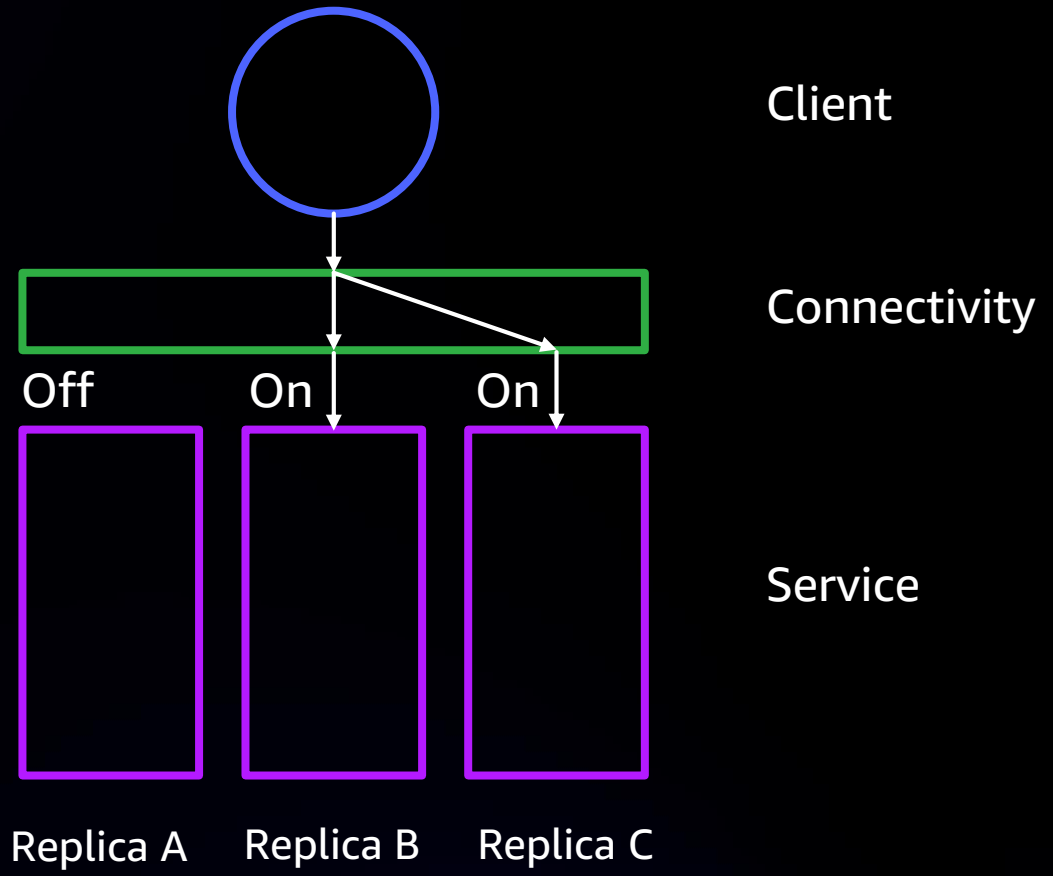
1. A replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) Replica A failure
3. Disable Replica A
4. Client impact mitigated, alarm clears



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

Detecting failure

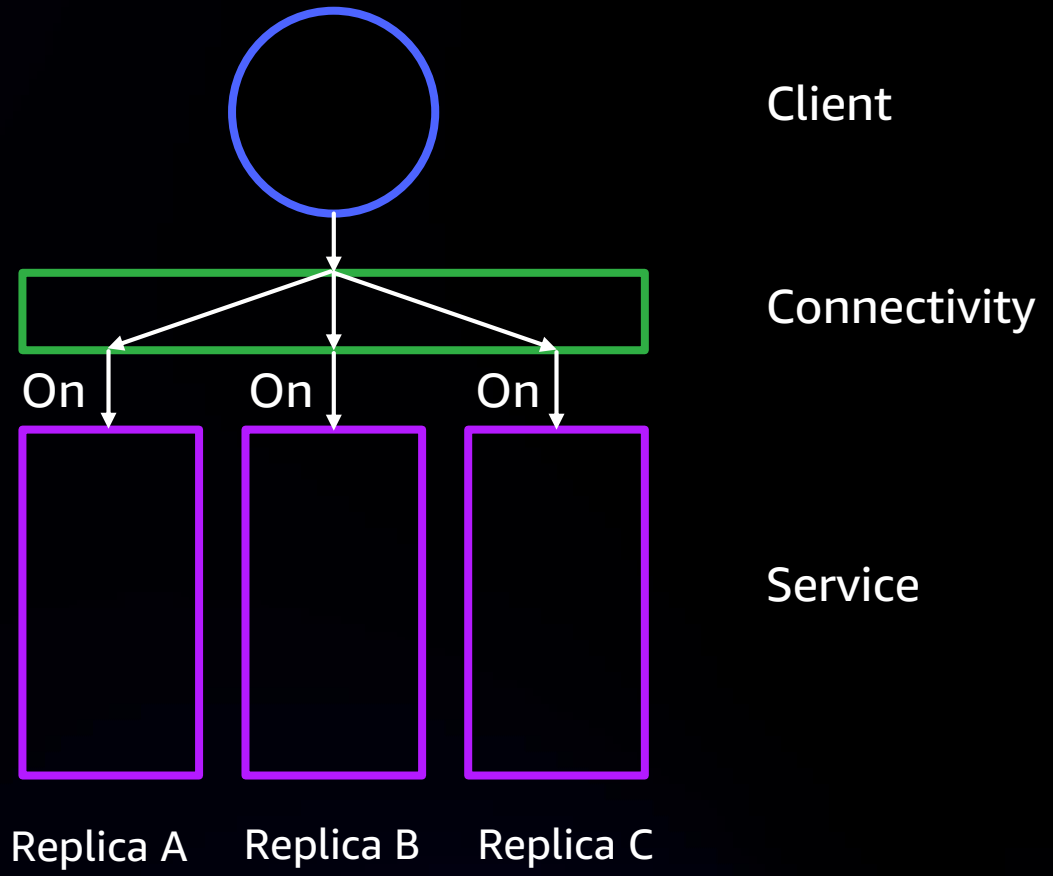
1. A replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) Replica A failure
3. Disable Replica A
4. Client impact mitigated, alarm clears
5. Replica A rollback or repair, alarm clears



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

Detecting failure

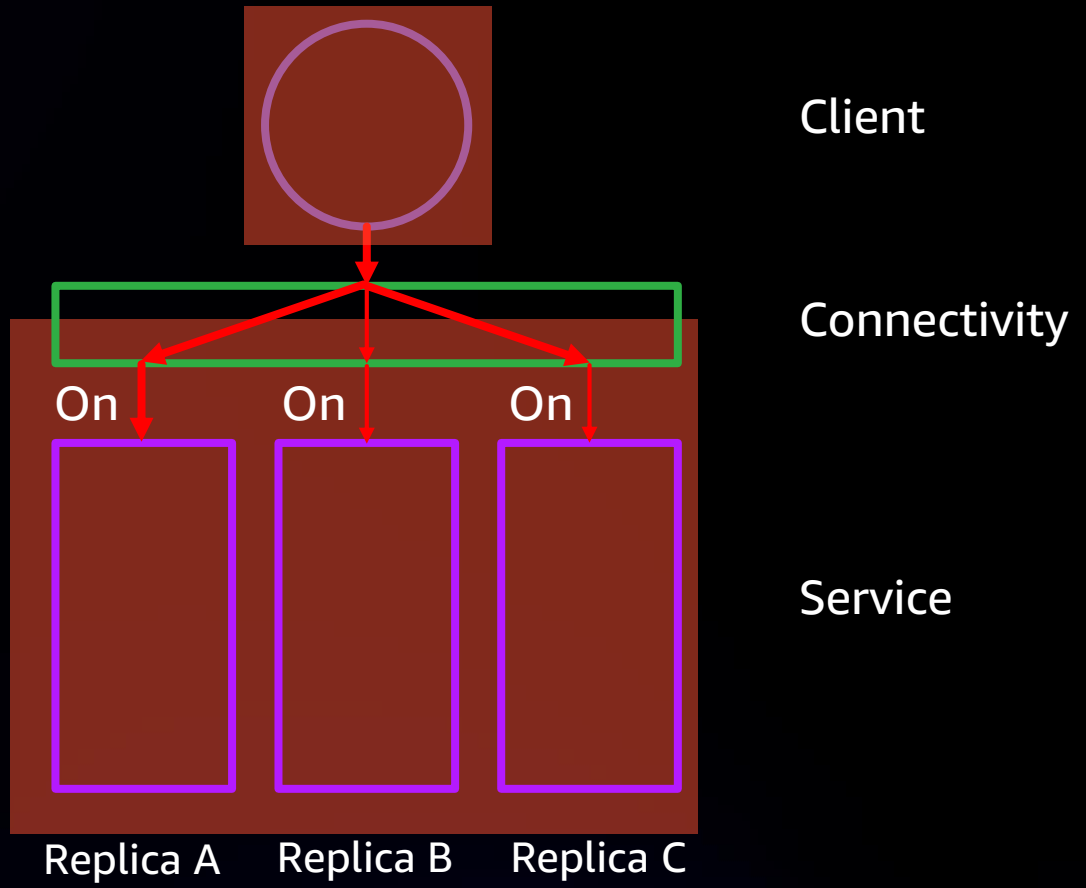
1. A replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) Replica A failure
3. Disable Replica A
4. Client impact mitigated, alarm clears
5. Replica A rollback or repair, alarm clears
6. Return Replica A to service



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

Detecting failure

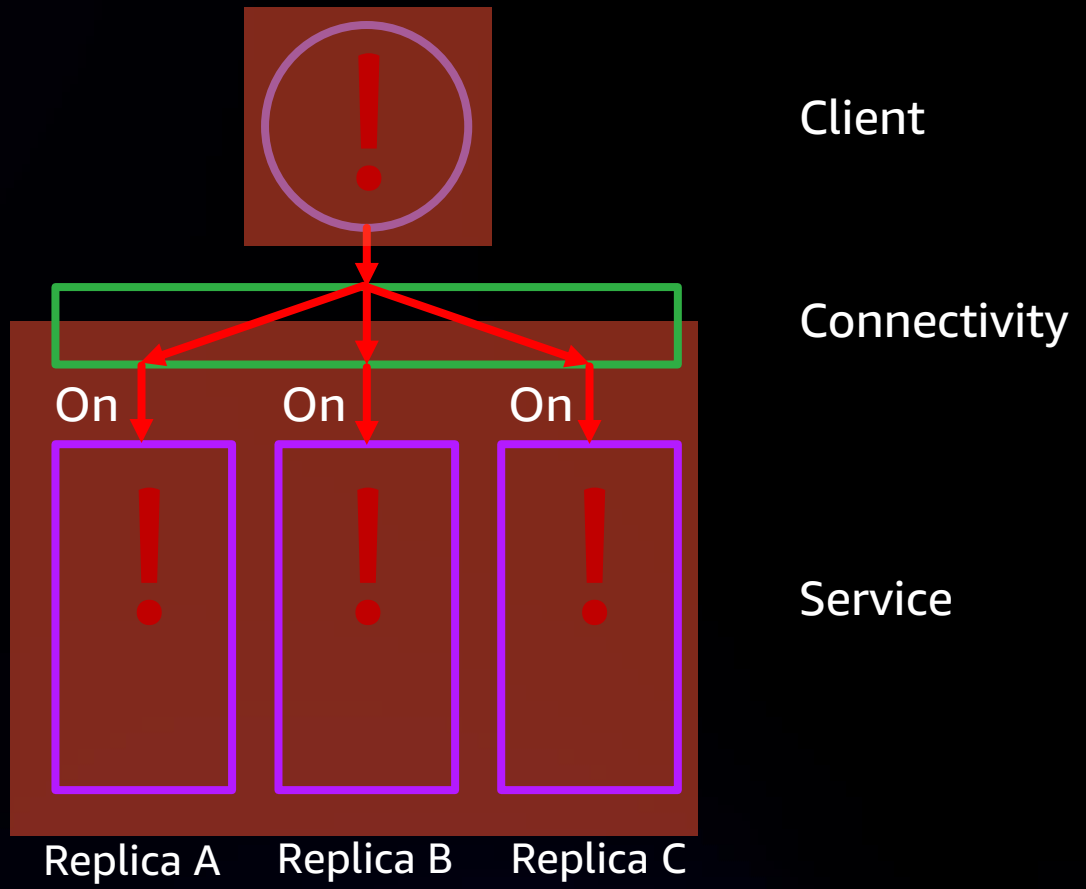
1. **Multi**-replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) All replicas impacted



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

Detecting failure

1. **Multi**-replica failure impacts clients
2. Application monitors alert:
   a) Client impact
   b) All replicas impacted
3. Disable change and deploy pipelines
4. Disable automated recovery
5. Page operator



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

Detecting failure

Monitor	Alarm threshold
Synthetic canaries	2 consecutive **or** 2 of last 10
Faults/5xx	>1% **or** >10 in 1 min
Errors/4xx	>75%
Request volume/2xx	>90% drop
Latency	10x @ 90th percentile

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

Detecting failure

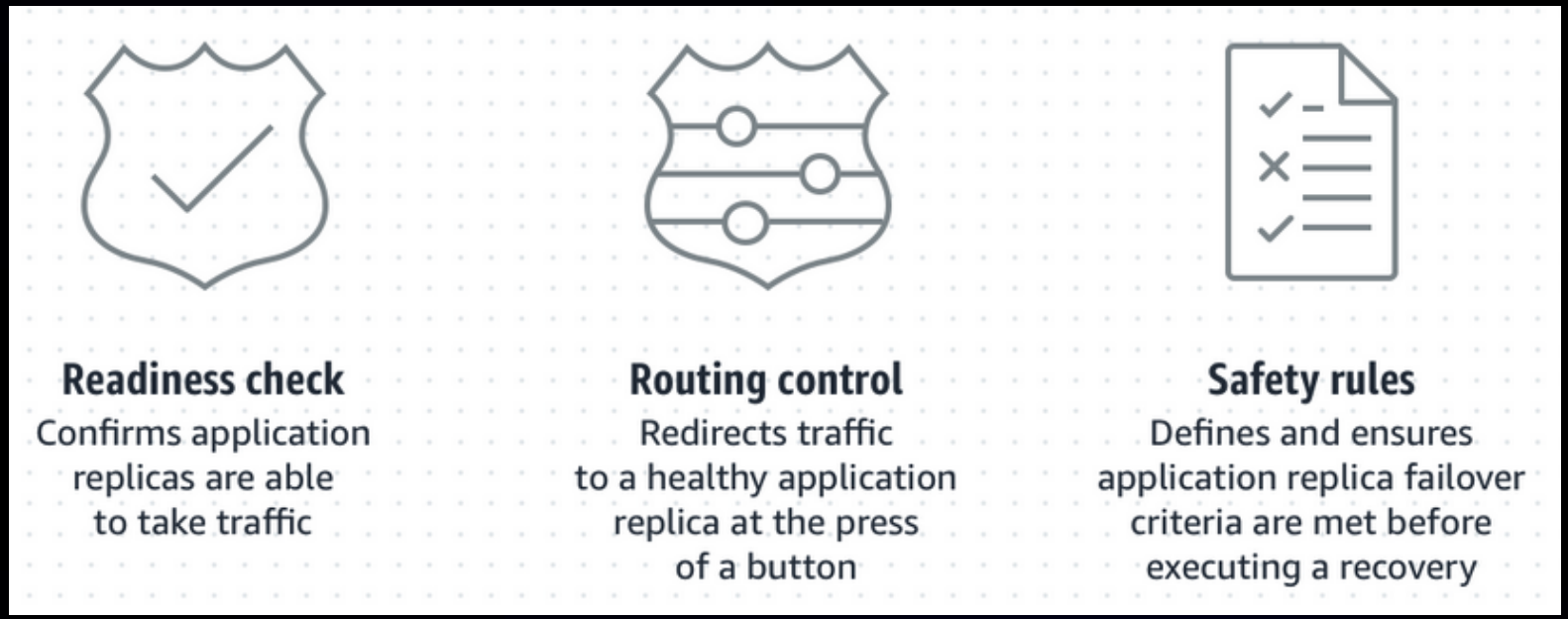
Monitor	Alarm threshold
Synthetic canaries	2 consecutive **or** 2 of last 10
Faults/5xx	>1% **or** >10 in 1 min
Errors/4xx	>75%
Request volume/2xx	>90% drop
Latency	10x @ 90th percentile

Per-replica metrics **and** whole-service metrics

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

Recovering from failure

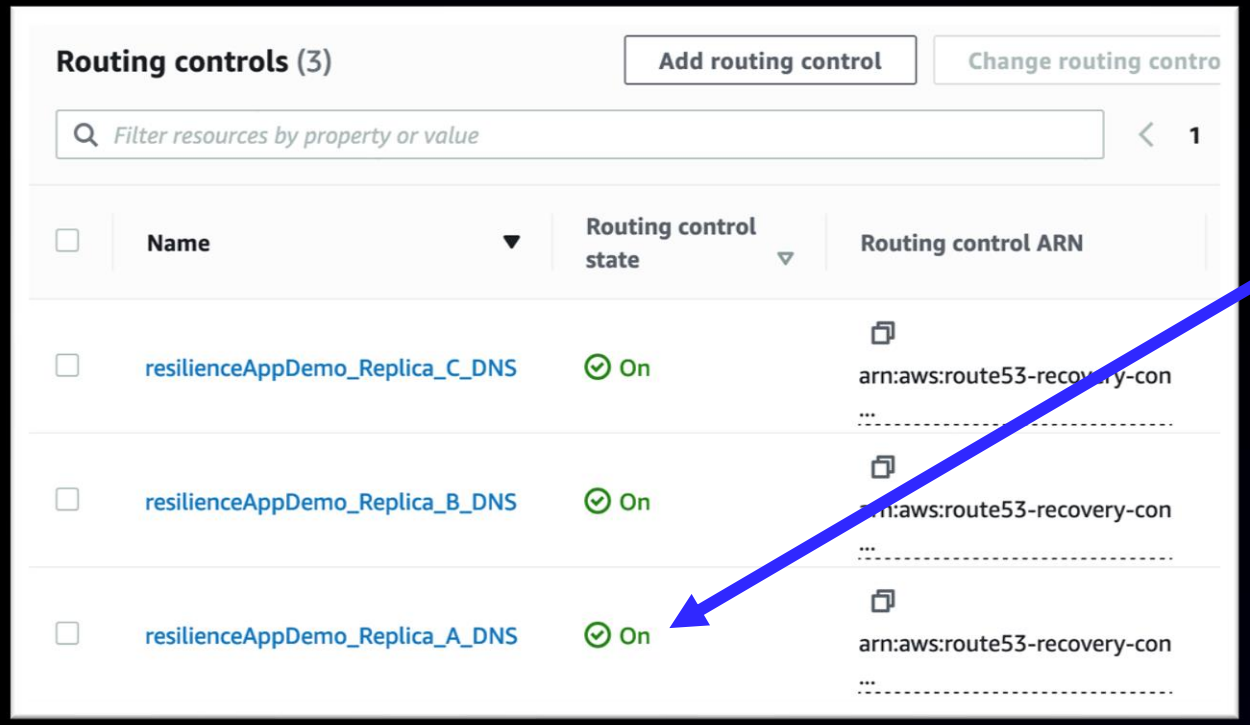
Amazon Route 53 Application Recovery Controller

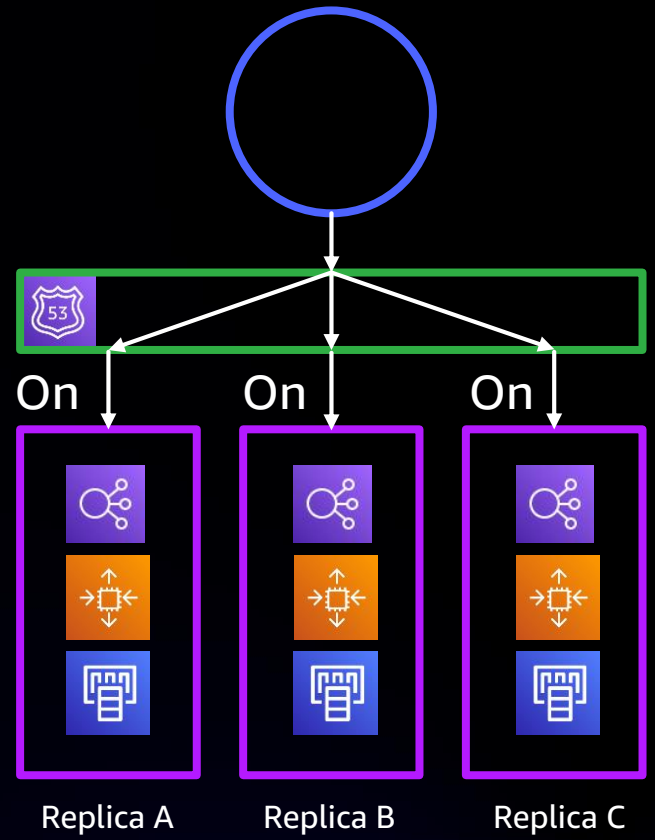


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Route 53 Application Recovery Controller

ROUTING CONTROLS





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

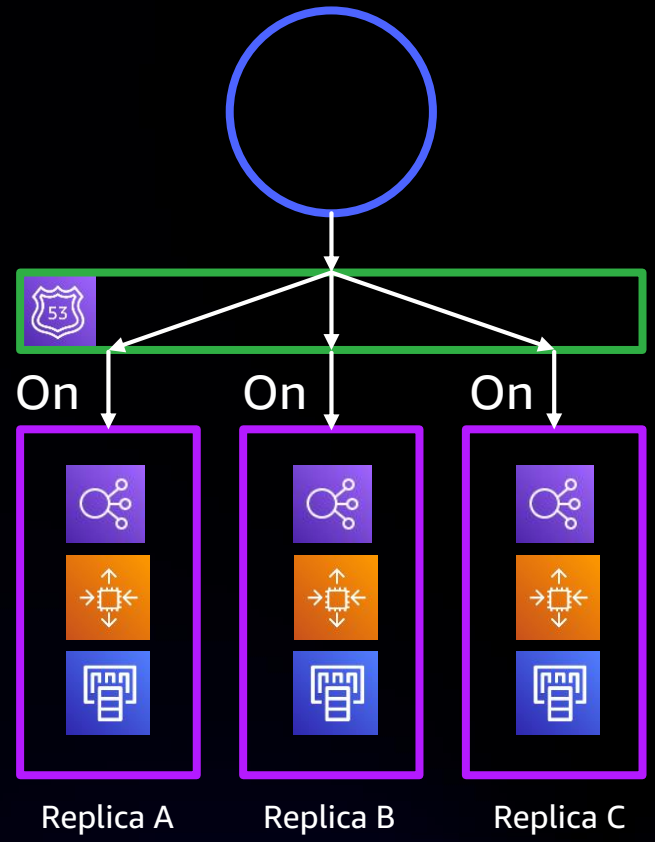
Route 53 Application Recovery Controller

SAFETY RULES

Safety rules (2)

Filter resources by property or value

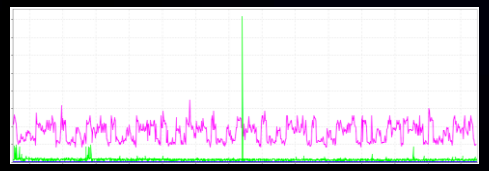
Name	Type
Disable_Automated_Recovery	Gating
2_Replicas_Online	Assertion



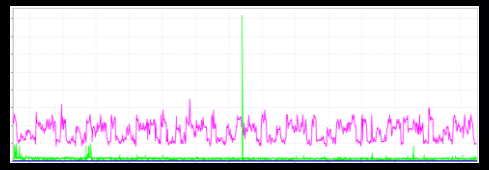
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automated recovery in <3 minutes

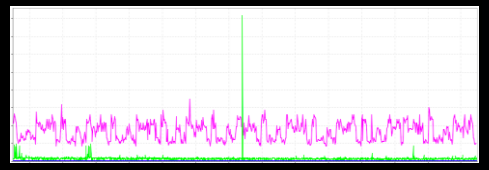
Synthetic canary **or**



Elevated 5xx errors **or**



Elevated 4xx errors **or**



Unhealthy replica alarm

Alarm-trigged Lambda

Routing controls

On
Replica A

On
Replica B

On
Replica C

Safety checks

2 Replicas online (true)

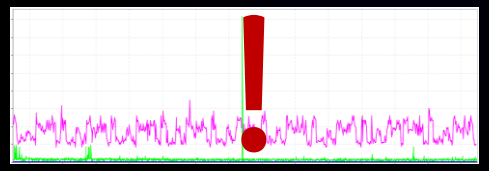
Disable automated recovery (false)

Routing update

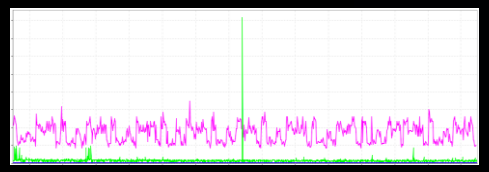
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automated recovery in <3 minutes

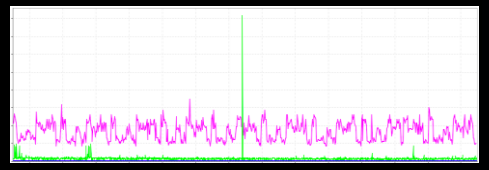
Synthetic canary **or**



Elevated 5xx errors **or**



Elevated 4xx errors **or**



Unhealthy replica alarm

Alarm-trigged Lambda

Routing controls

- Off — Replica A
- On — Replica B
- On — Replica C

Safety checks

- 2 Replicas online (true)
- Disable automated recovery (false)

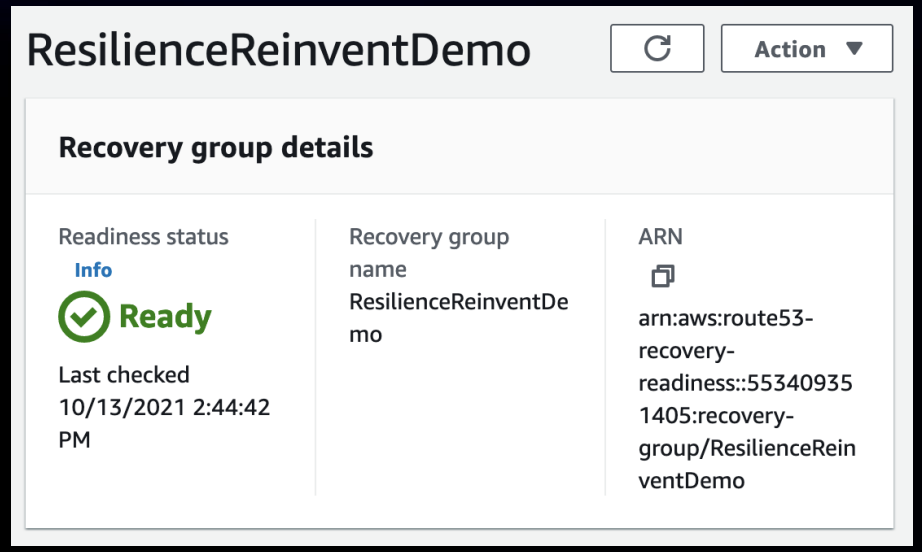
Routing update

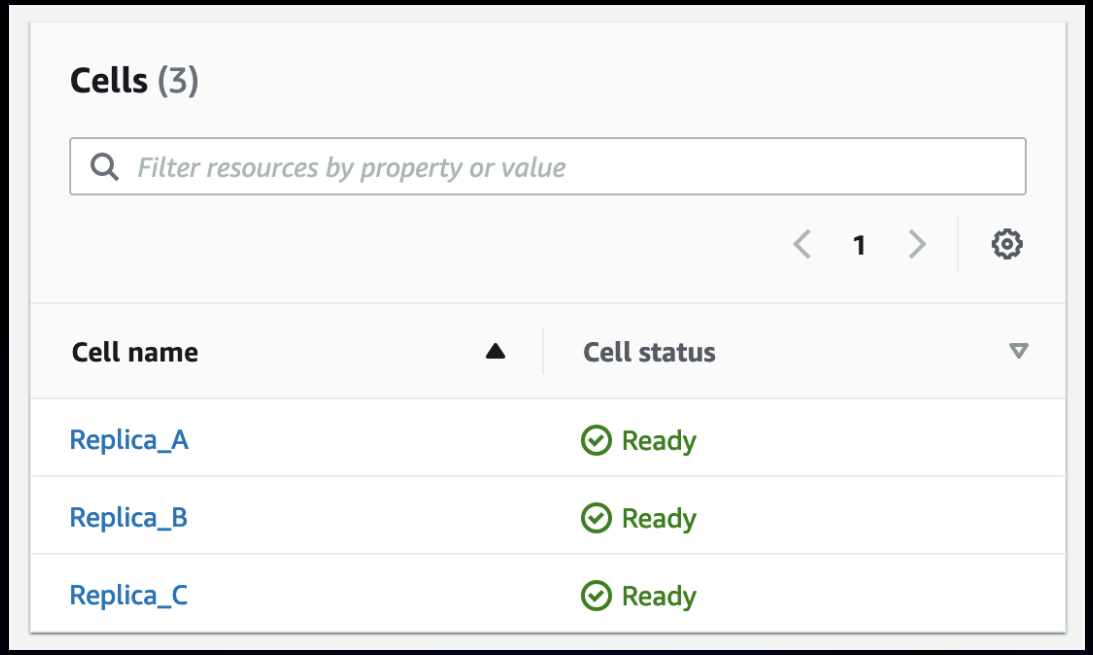
aws

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

Route 53 Application Recovery Controller

READINESS CHECKS





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

Upcoming sessions

Builder’s sessions:

NET322
Building for high availability:
Architecture and recovery

NET317-R2
Designing resilient applications
using Amazon Route 53 ARC (Repeat)

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

Thank you!

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