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

DOP301

The Amazon Builders' Library: 25 years of operational excellence at Amazon

Colm MacCárthaigh (he/him)

VP / Distinguished Engineer
Amazon Web Services

David Yanacek (he/him)

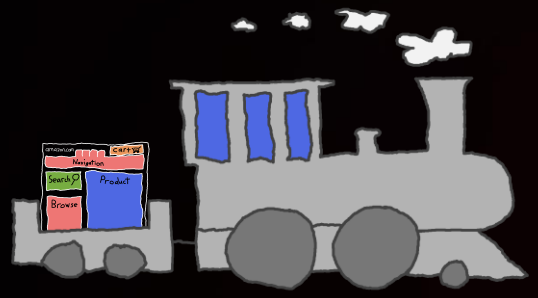
Sr. Principal Engineer
Amazon Web Services

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

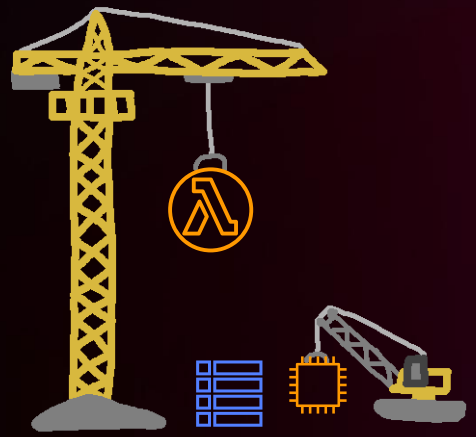
Four stories



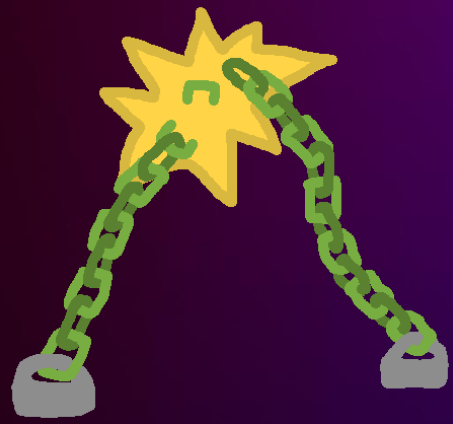
What is an event like?



Deploying software



Changing infrastructure



Breaking the unbreakable

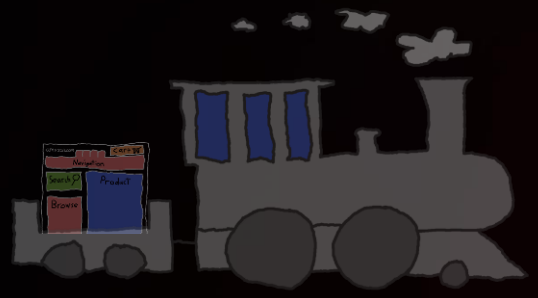
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

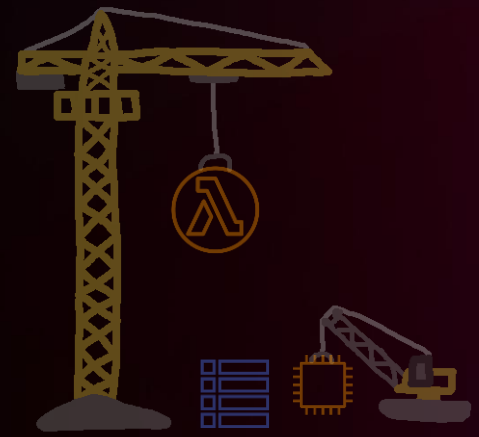
Chapter one



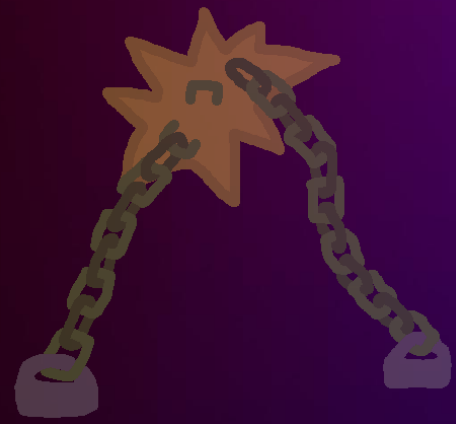
What is an event like?



Deploying software



Changing infrastructure



Breaking the unbreakable

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an event like?



When things go wrong, we call those *events*

Not all events impact customers

We also use event management process for game-days, degraded states, peak sales events, and very occasionally security response

Amazon has had an event management process for over 25 years

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an event like?

We use an event ticket and audio conference calls as our primary communication channel

Chat is a secondary communications channel

Calls are led by call-leaders

Facilitated by our safety engineering team



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

What is an event like?

AWS has dedicated and separate calls for technical issue handling and for customer communication

The technical call is singularly focused on mitigating the event and restoring full service ASAP

The communication call is focused on status dashboard updates and bi-directional communication with customers



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

S.A.F.E.

Stay Calm

Assess the situation

Focus on mitigation

Escalate Early

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Stay calm

Maintain urgency but cooler heads always prevail. Don’t Panic!

Calls have a mix of event experience levels

We want events to be rare. Inexperience is a good thing

It’s important to be deliberate and considered

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Assess the situation

Every participant in an event is expected to be active

That means tracking the updates in the call and being able to provide a summary of their own area

Scanning for unknown customer impact is critical

Confirming improvement with data

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Focus on mitigation

Most engineers have a strong bias to Root Cause Analysis and debugging

Root Cause Analysis is less important than mitigation

“First, stop the bleeding”

Avoid analysis until options such as rollback, flipping between primaries/secondaries, have been exhausted or can be parallelized

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Escalate early

Escalating and pulling in more experienced help is shown to lead to faster remediation time

Pull in a secondary, manager, more senior or more relevant SME

Automate when possible!

Be grateful for the escalation. Escalations are a very good thing

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Example event

July 29th 2016 – Event impacting Amazon EC2 API, Amazon Prime Instant Video, Amazon.com

Trigger was a low-level change a few days earlier in an SSL/TLS configuration

The call included leadership teams and engineers from Amazon.com, Prime Video, and AWS

Service restored by identifying changes, rolling back, and creating new network-level partitioning

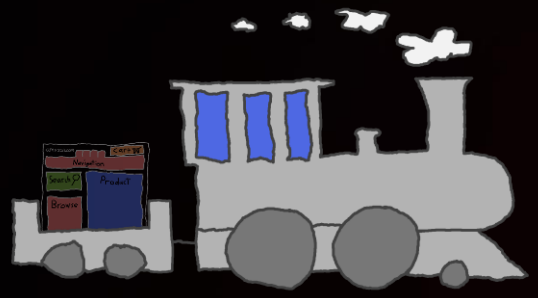
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

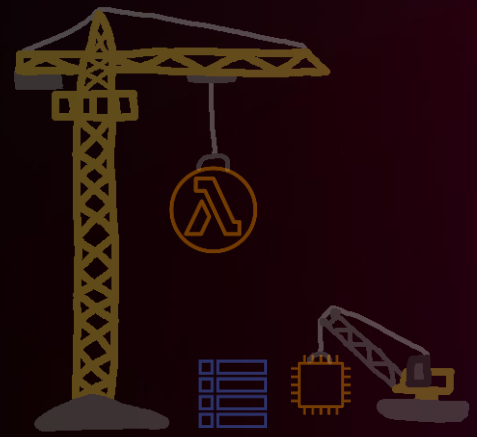
Chapter two



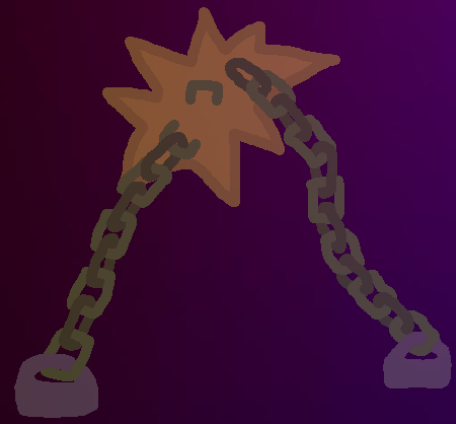
What is an event like?



Deploying software



Changing infrastructure



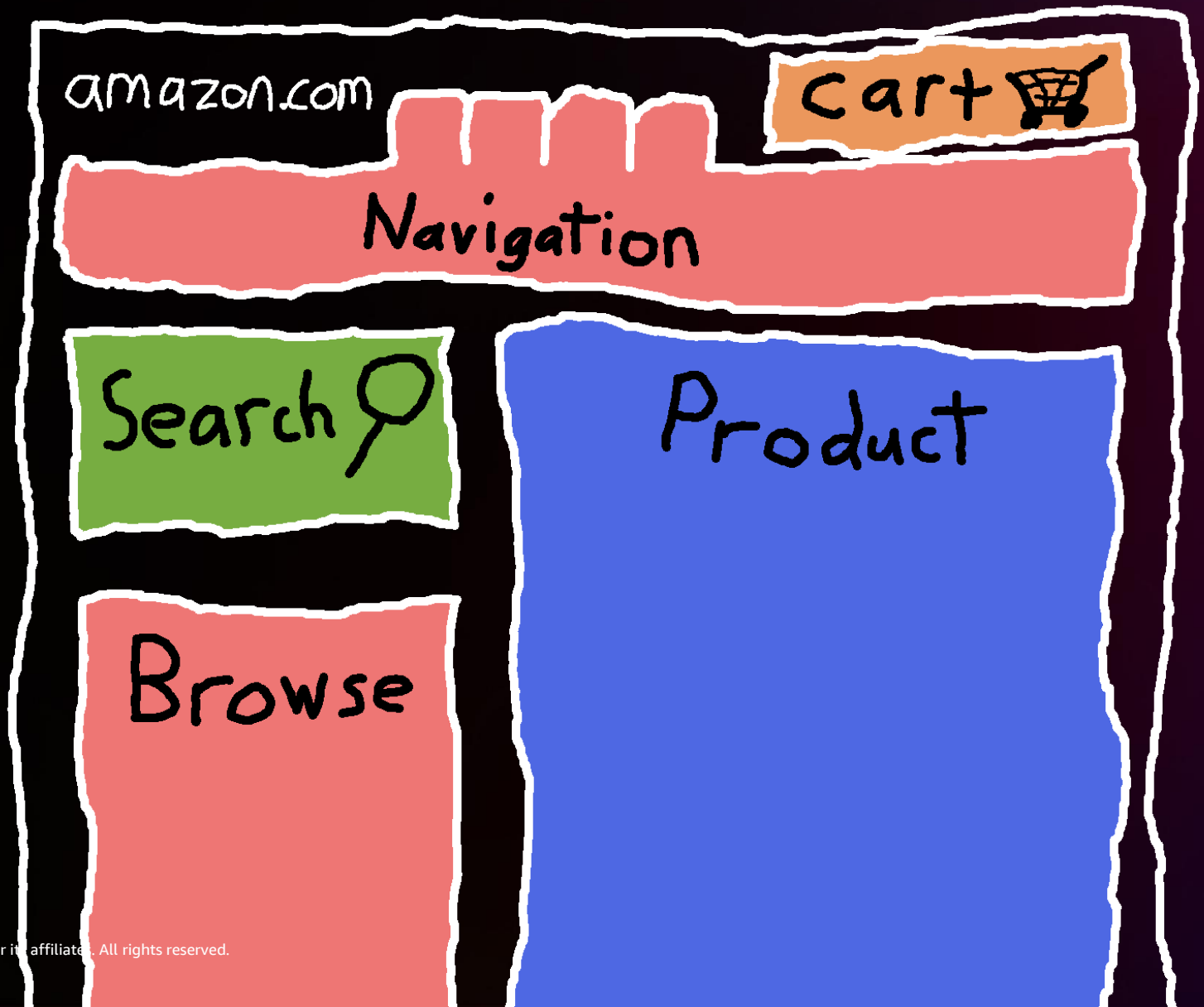
Breaking the unbreakable

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Story: Deployment automation at Amazon

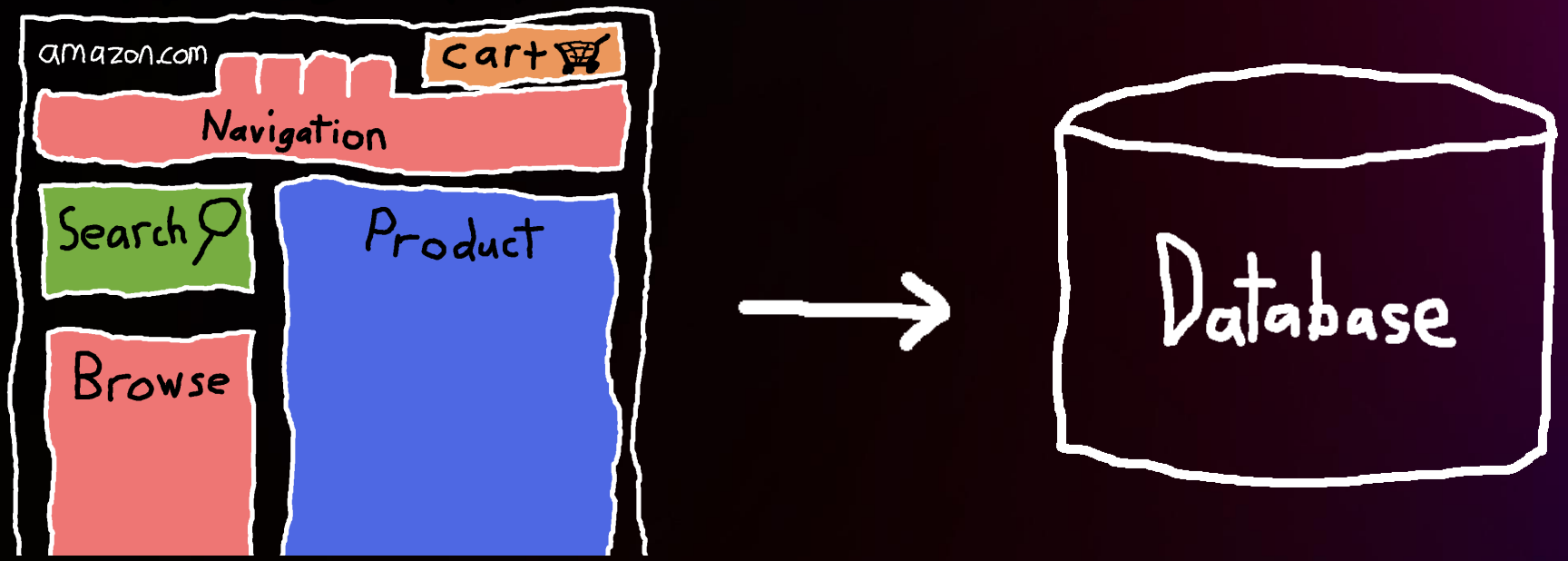
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Transformation at Amazon: Early 2000s



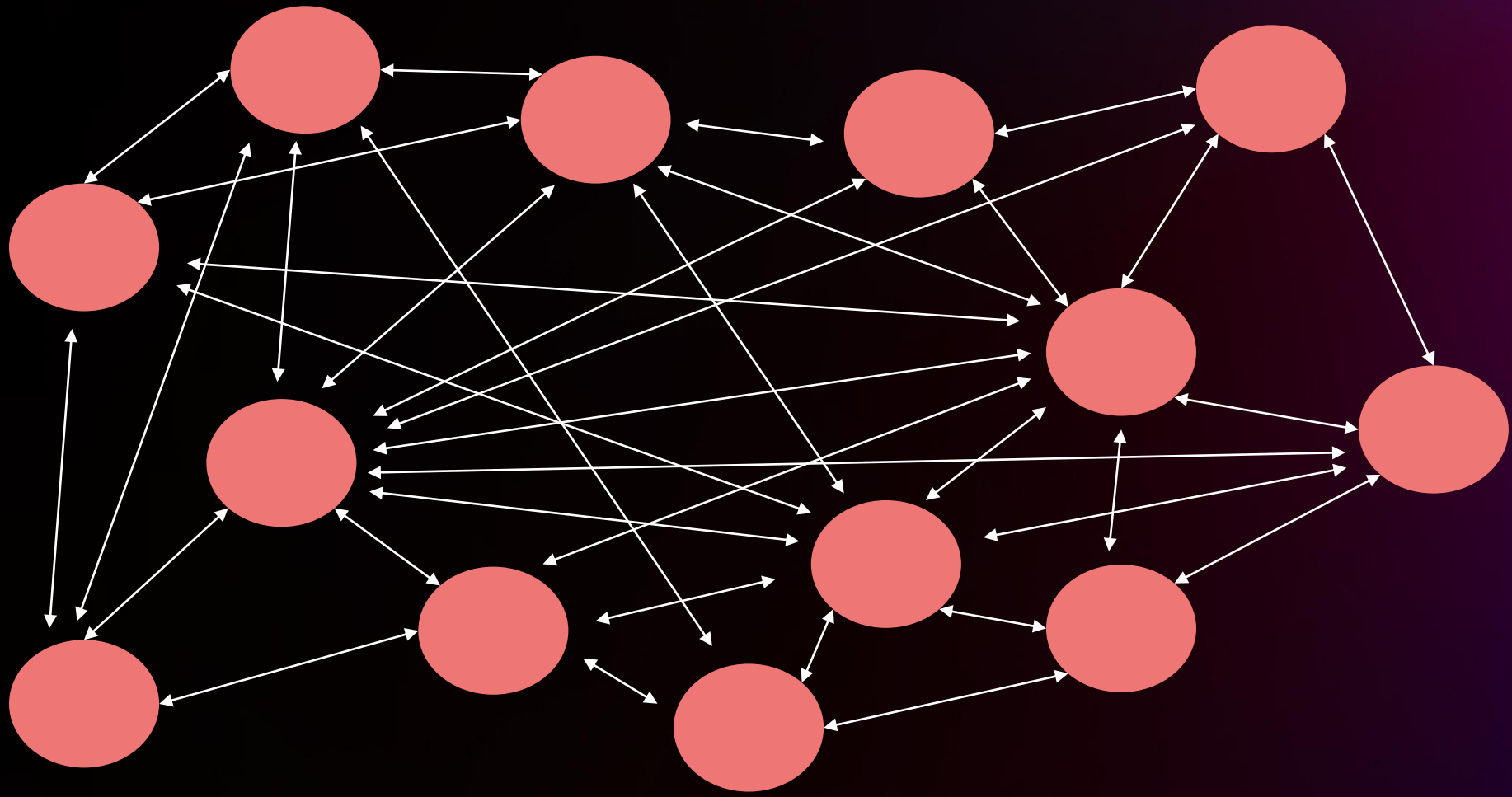
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Two-tier architecture



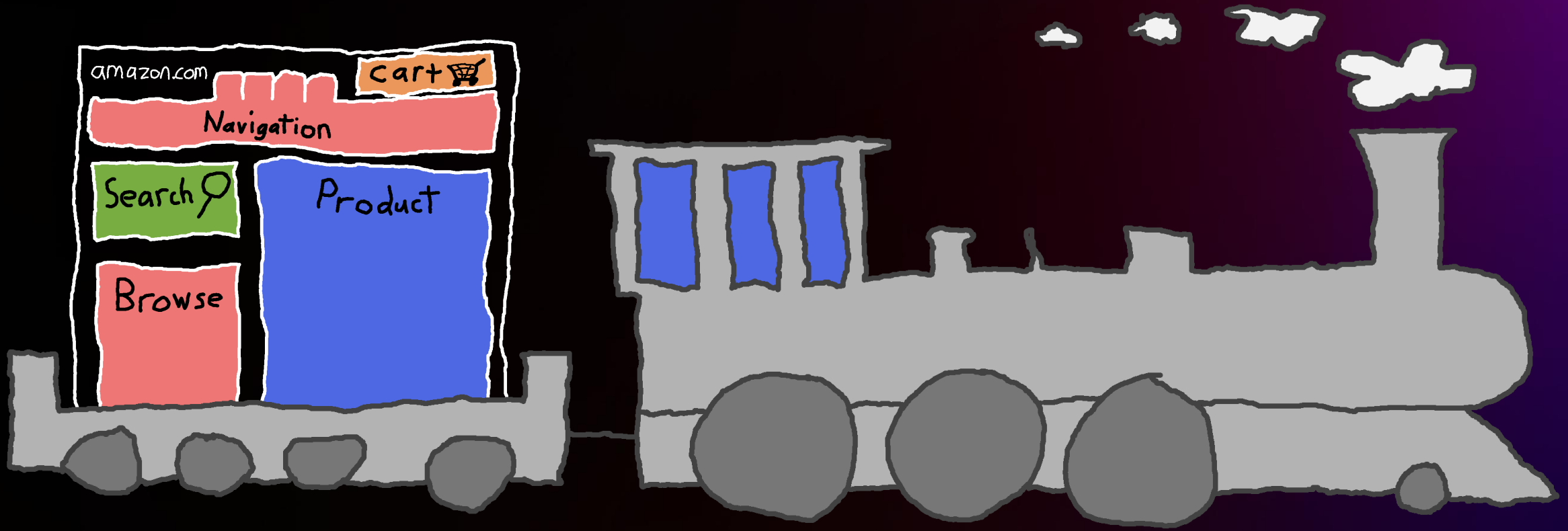
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The cost of coordination



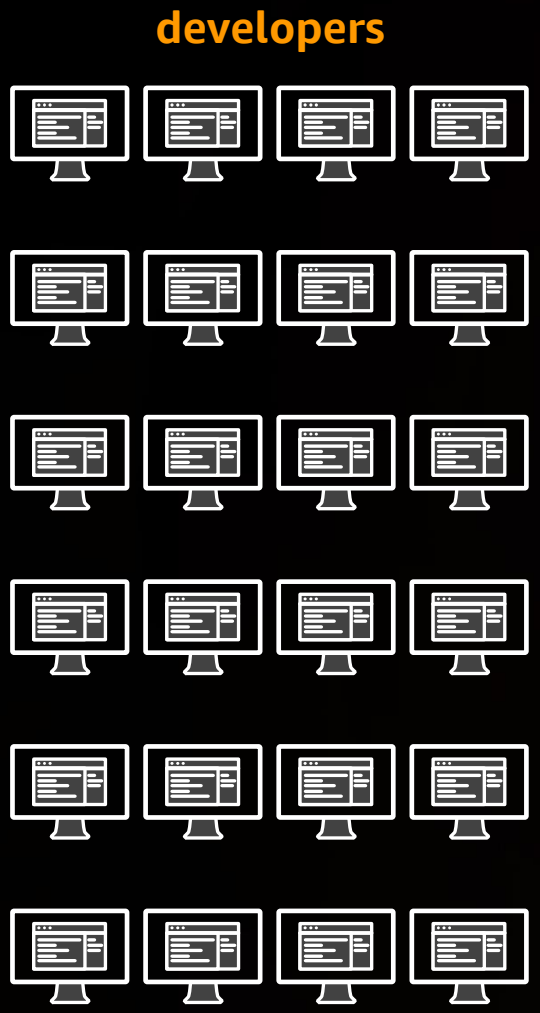
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Release train: build, test, deploy, monitor



aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

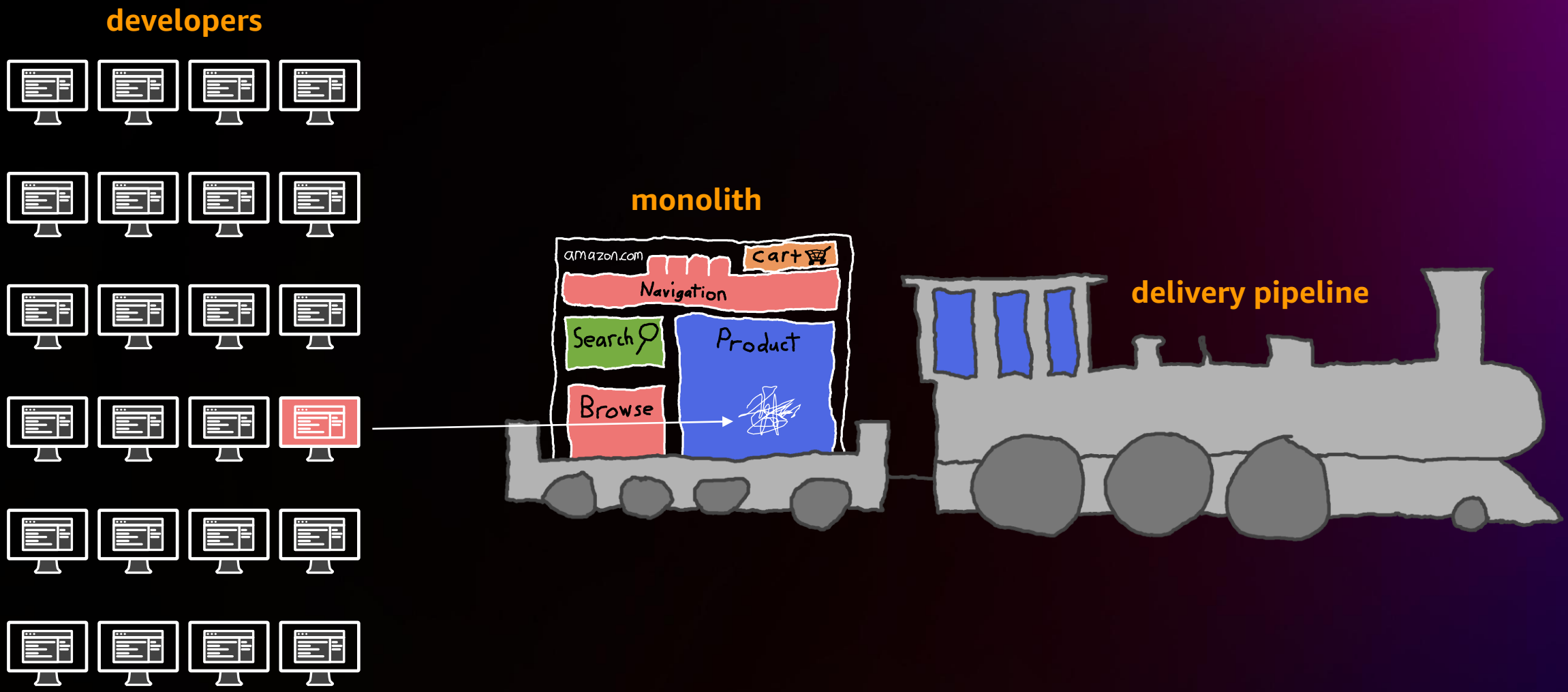
Lots of coordination





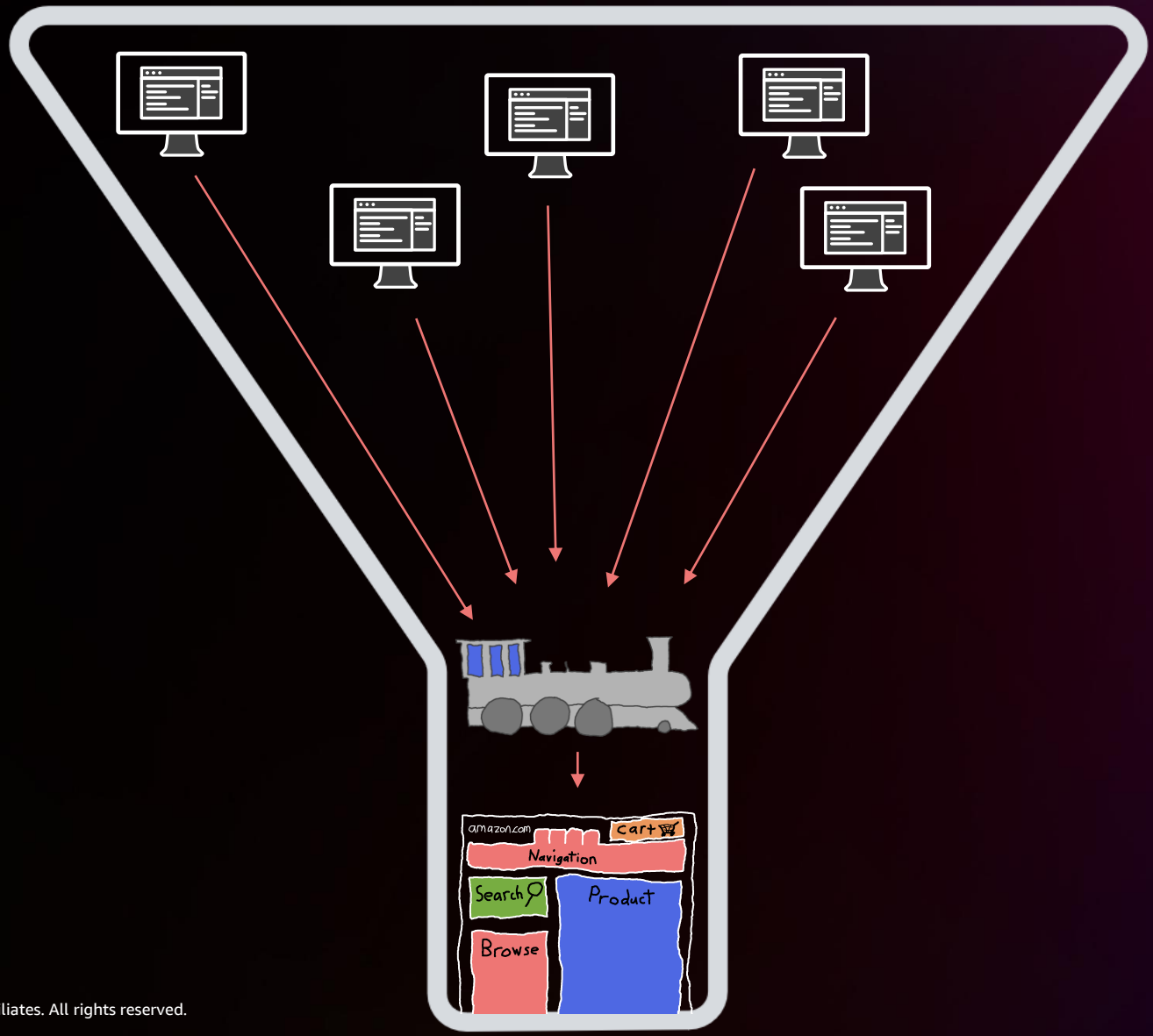
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Pipeline stalls



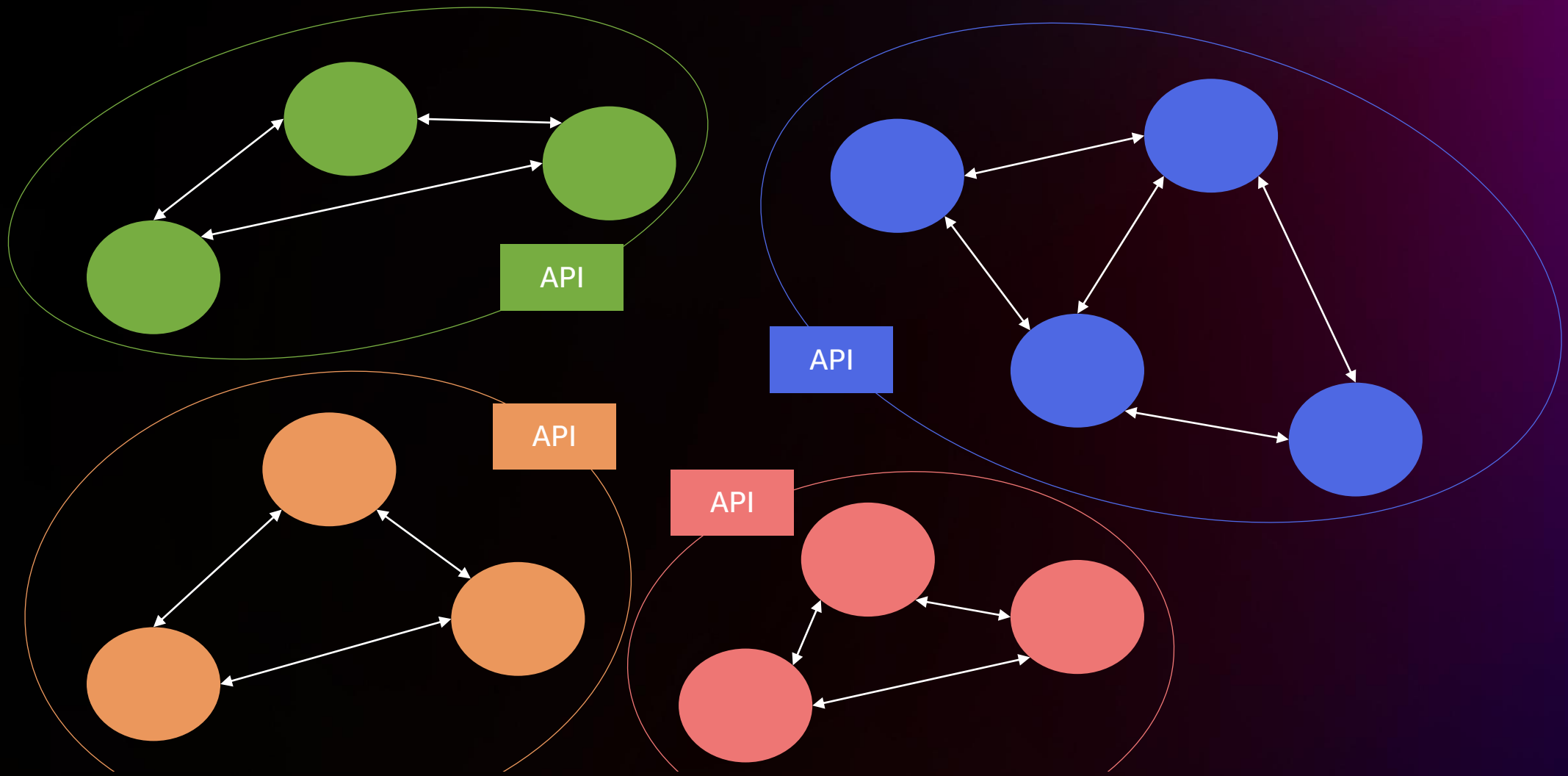
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Bottlenecked processes



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

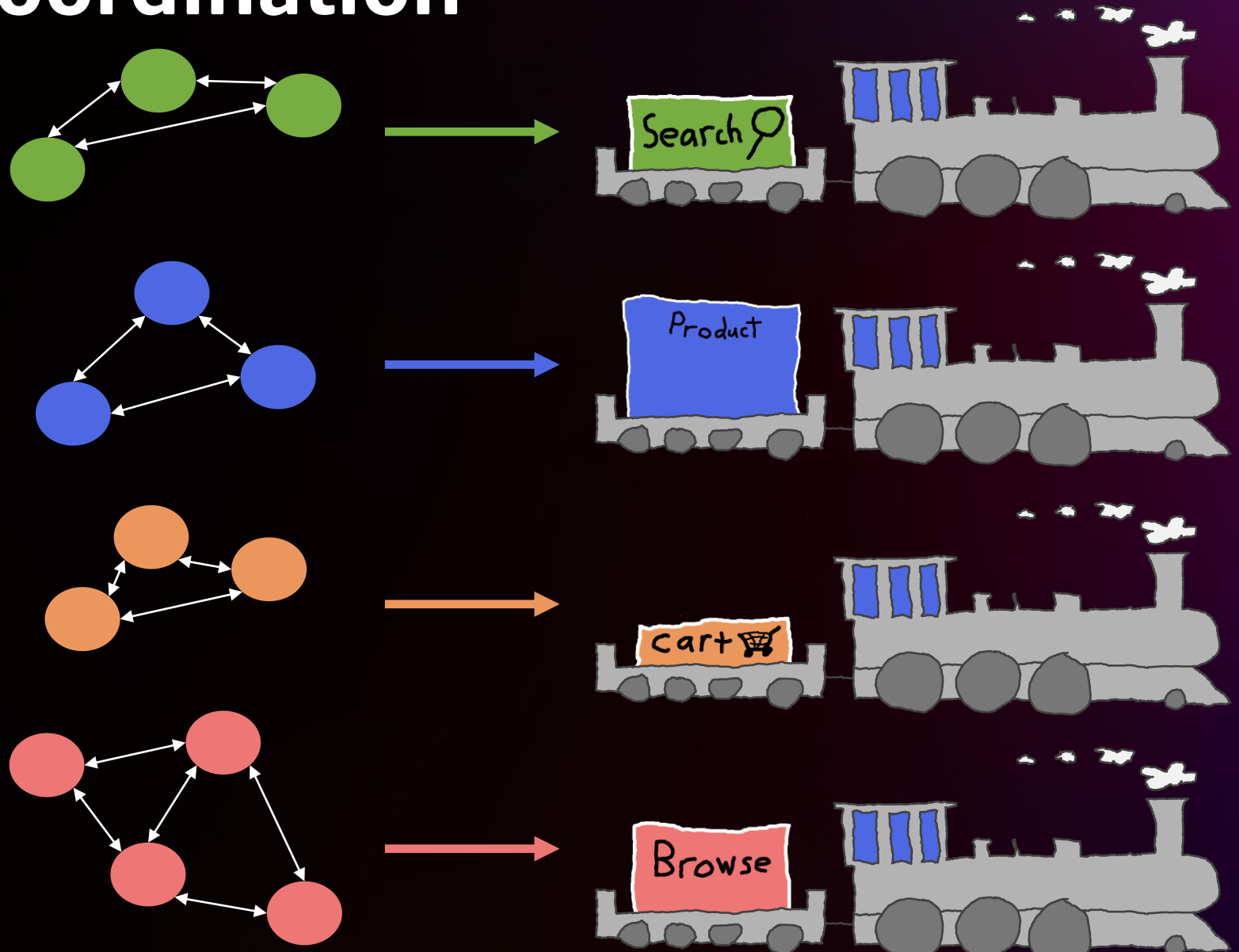
The distributed computing manifesto



https://www.allthingsdistributed.com/2022/11/amazon-1998-distributed-computing-manifesto.html

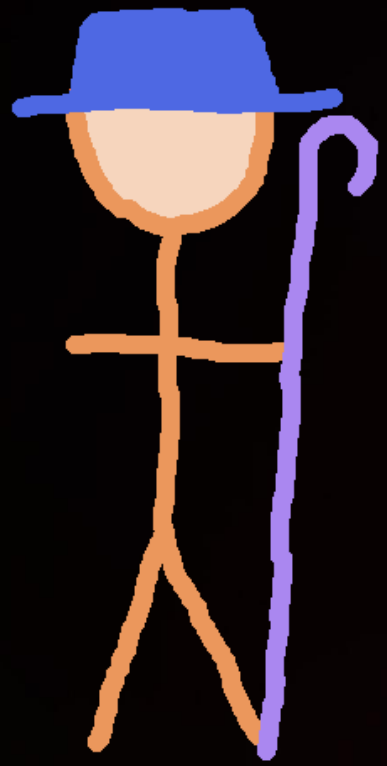
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

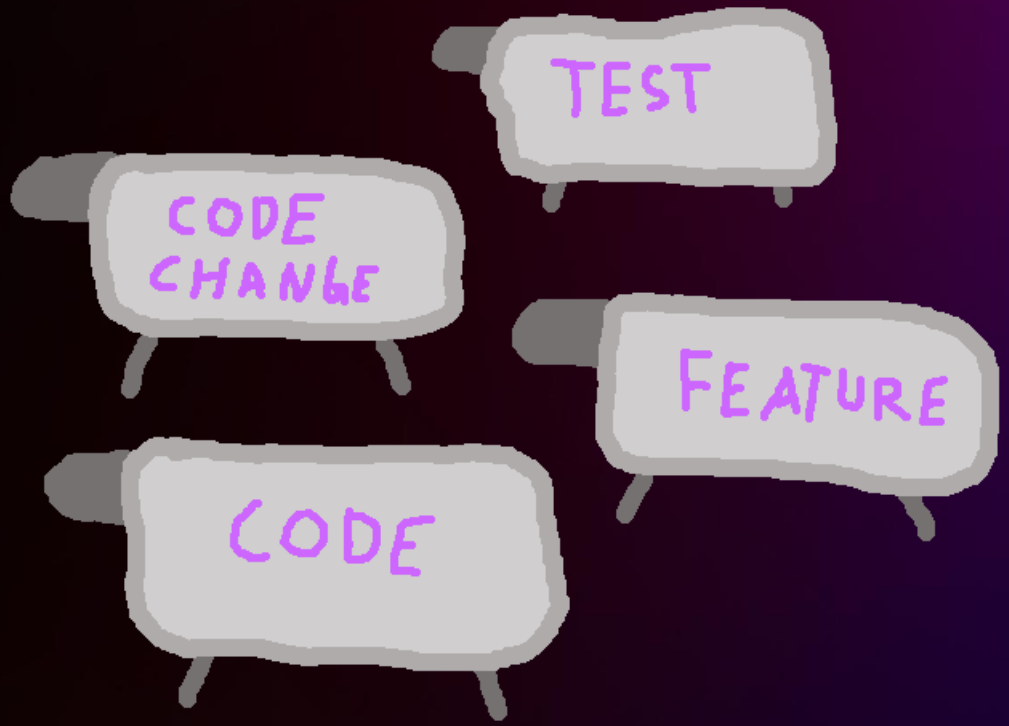
Reduced coordination



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

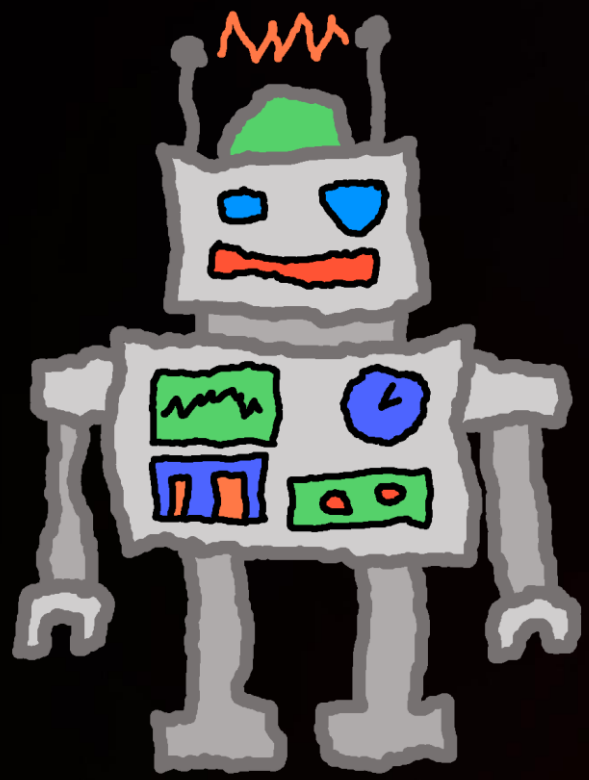
With independence comes responsibility

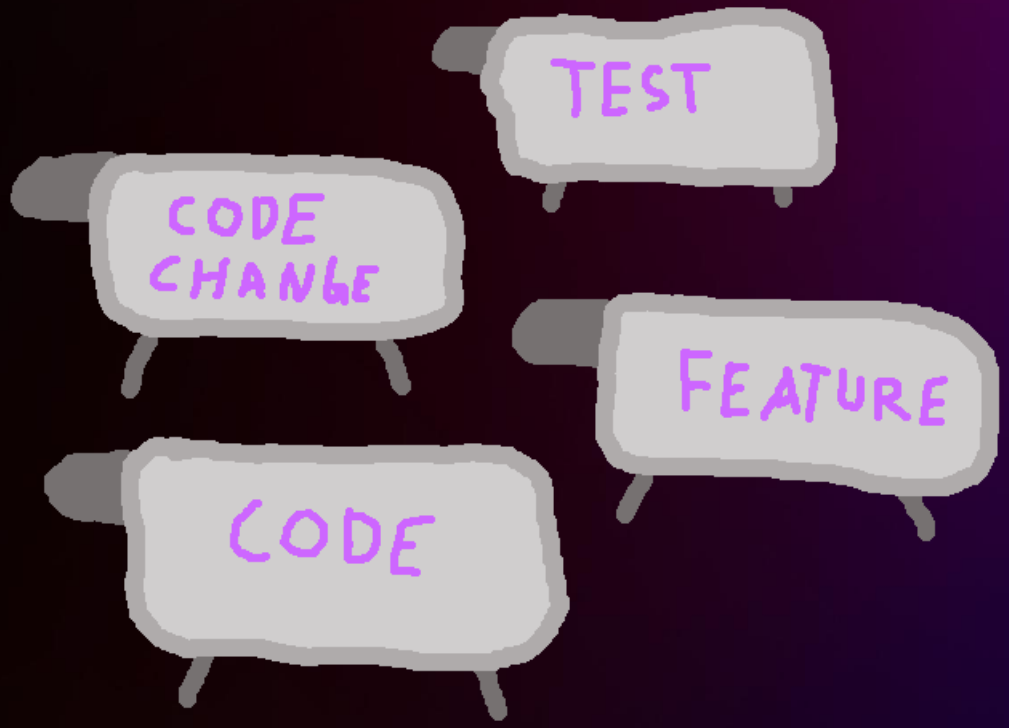




aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Deployment automation





aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automated deployment pipelines

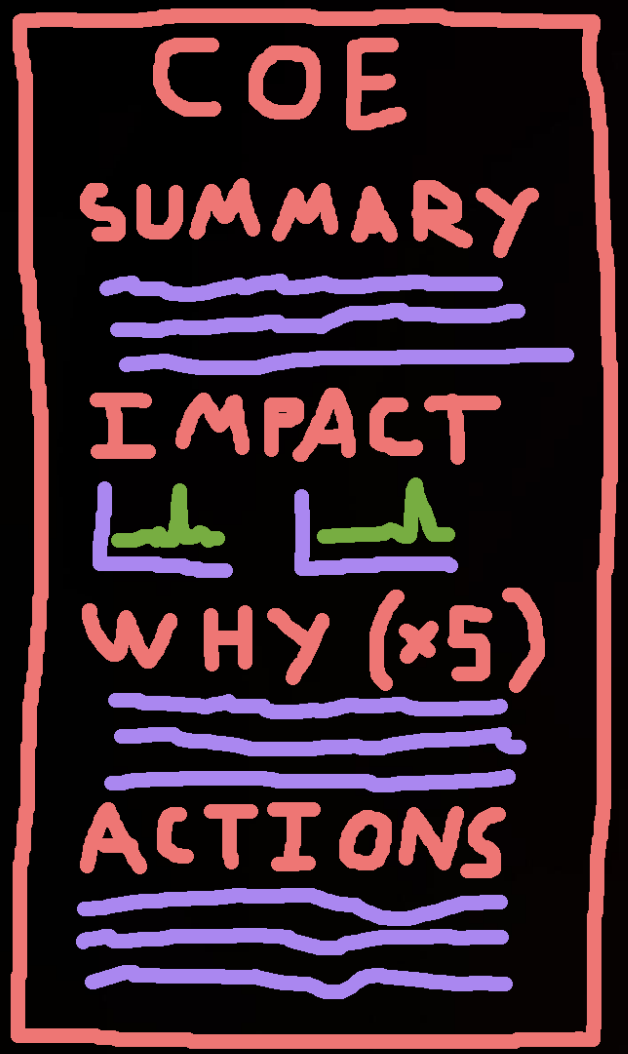


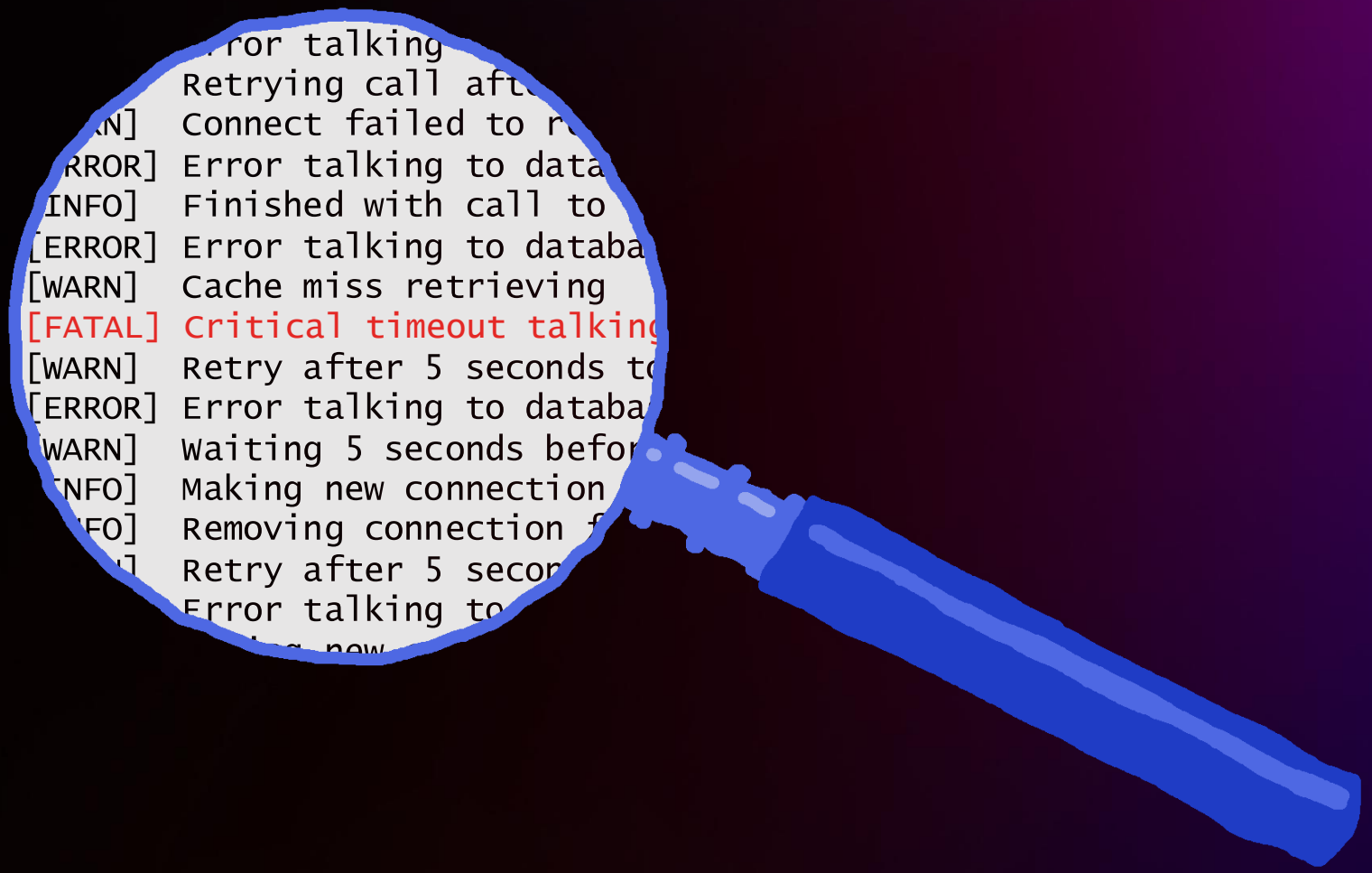
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Learning, improving

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

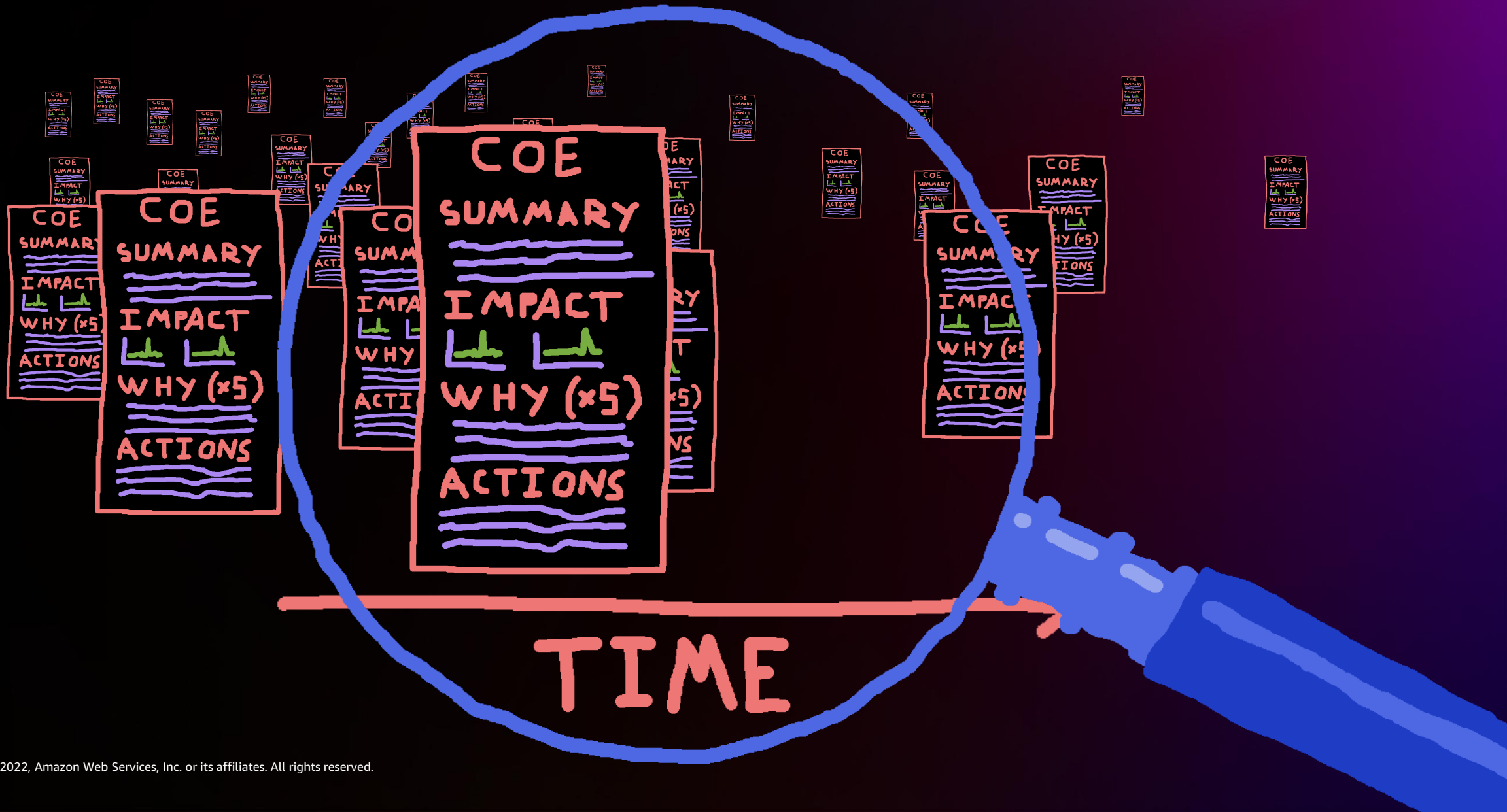
Post-incident retrospectives





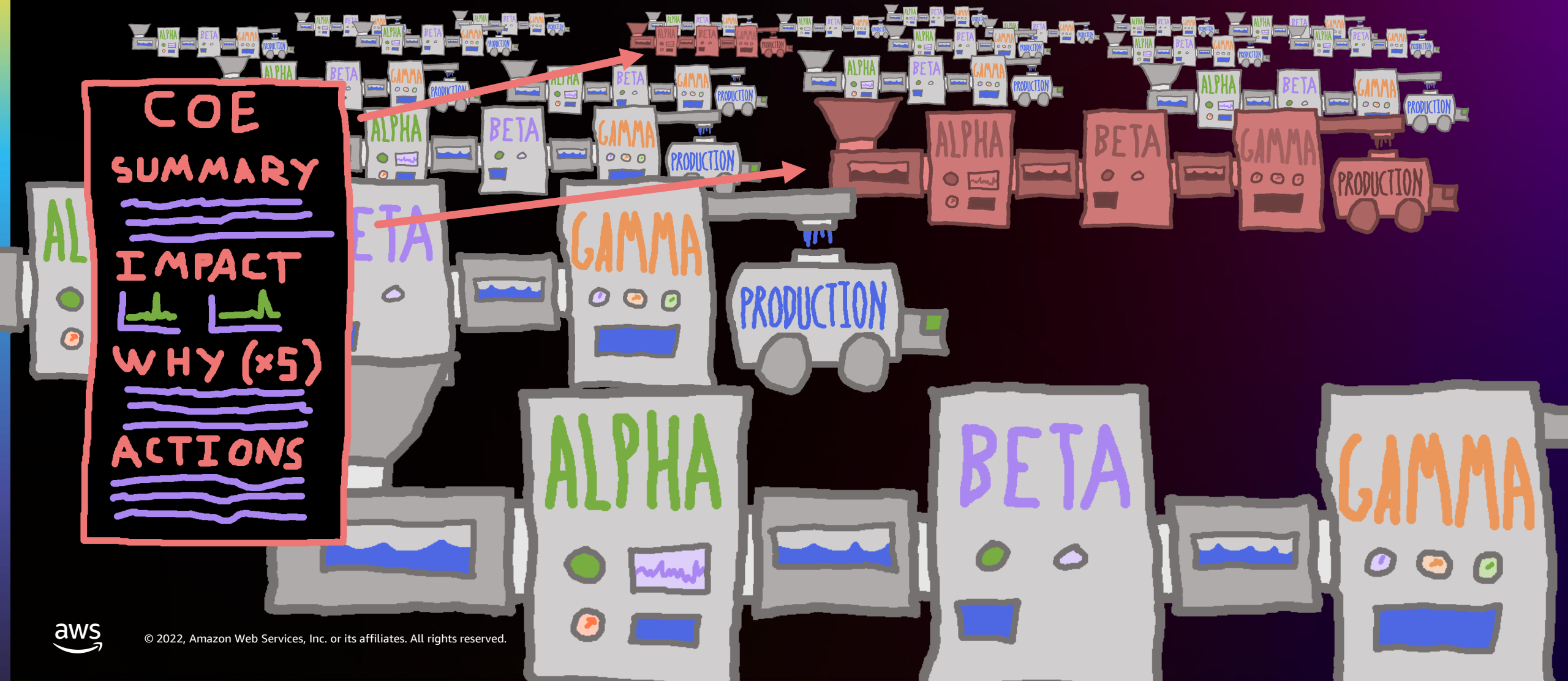
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Post-incident retrospectives



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Scanning for good practices

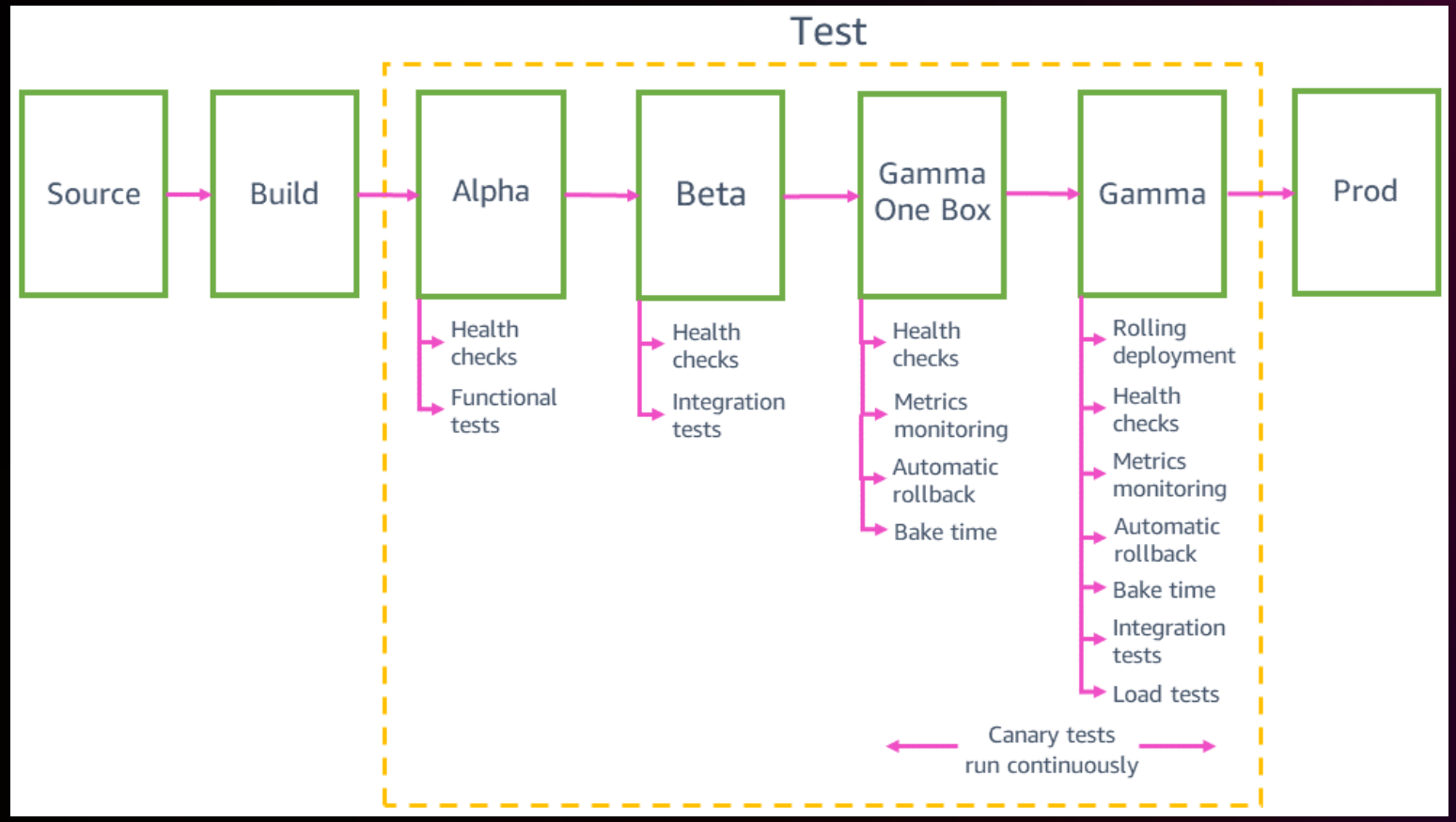


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Categories of safe deployment practices

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

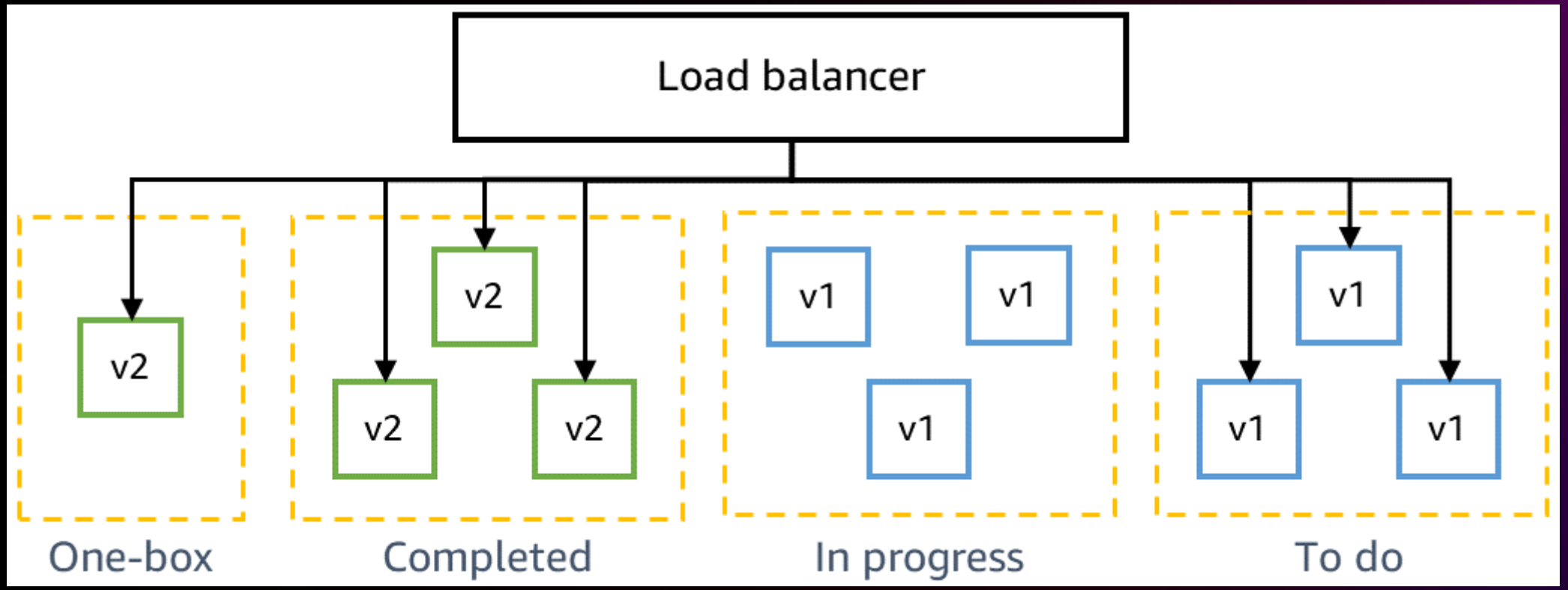
Pre-validation and testing



https://aws.amazon.com/builders-library/automating-safe-hands-off-deployments/

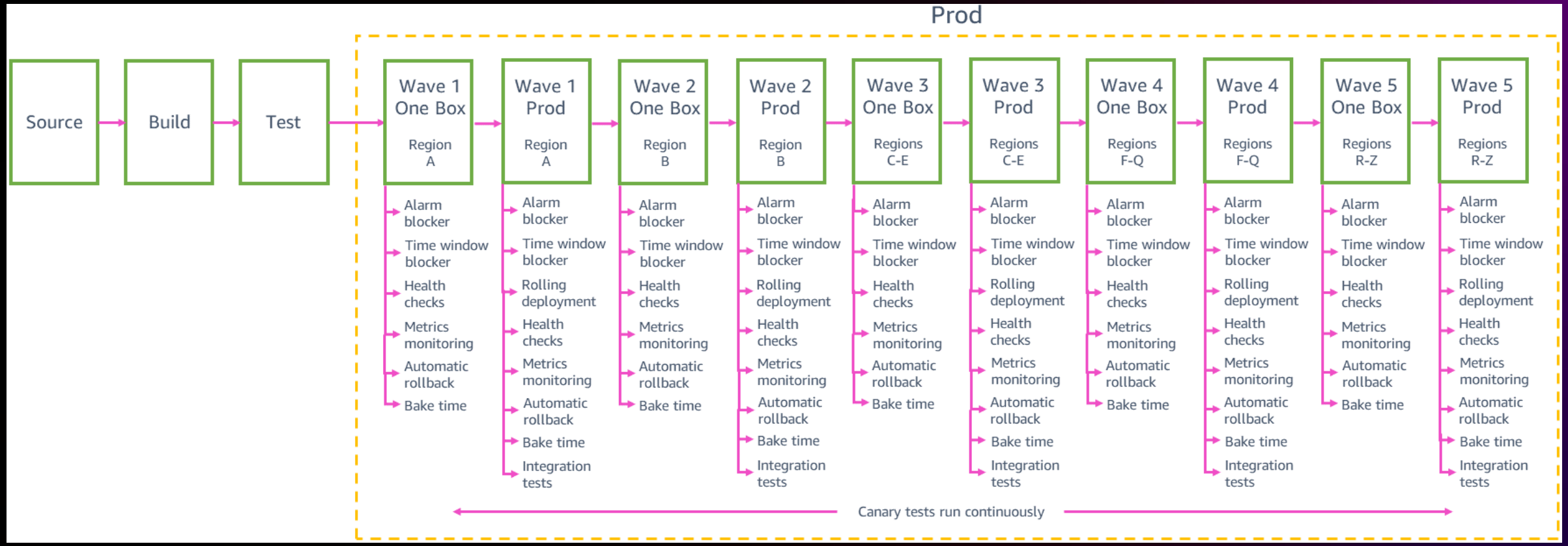
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental deployment



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

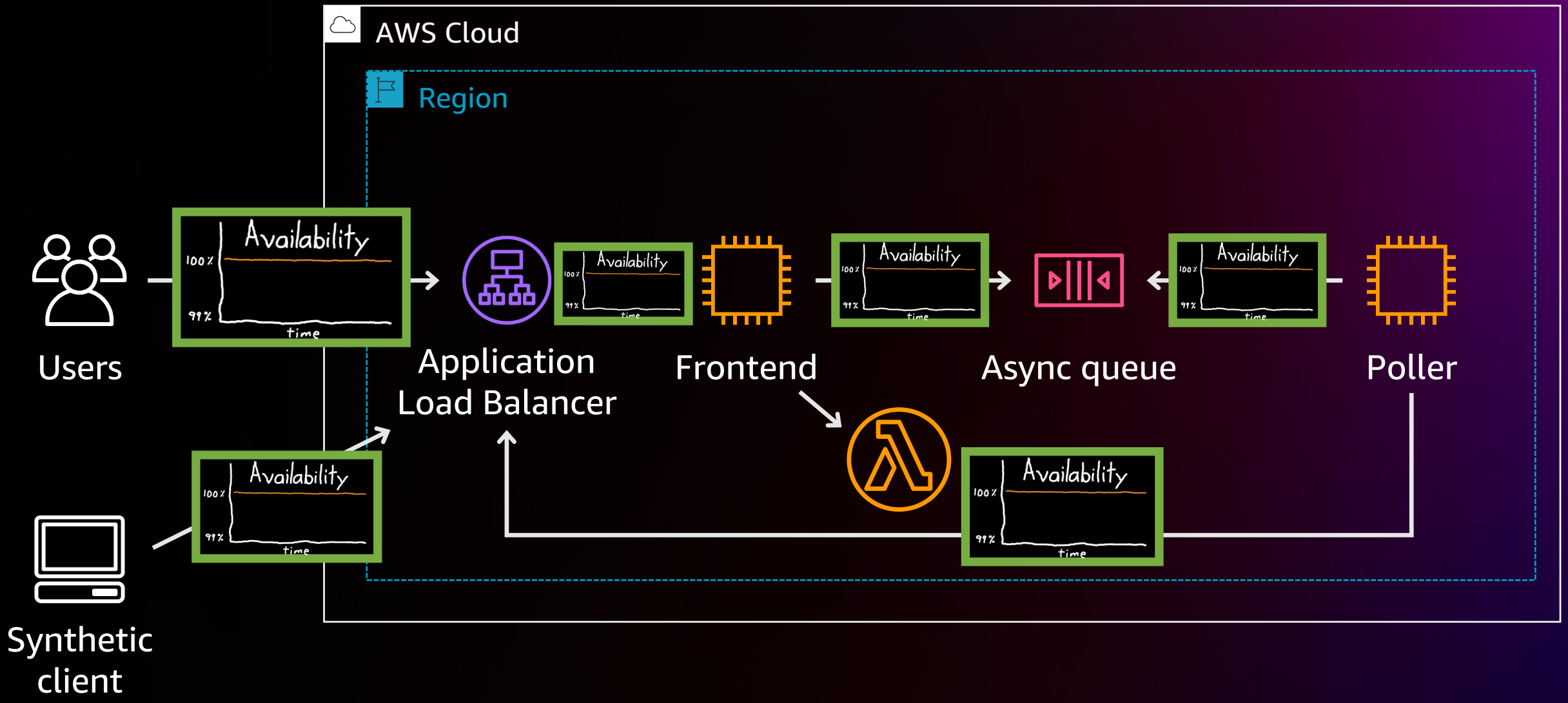
Incremental rollout



https://aws.amazon.com/builders-library/going-faster-with-continuous-delivery/

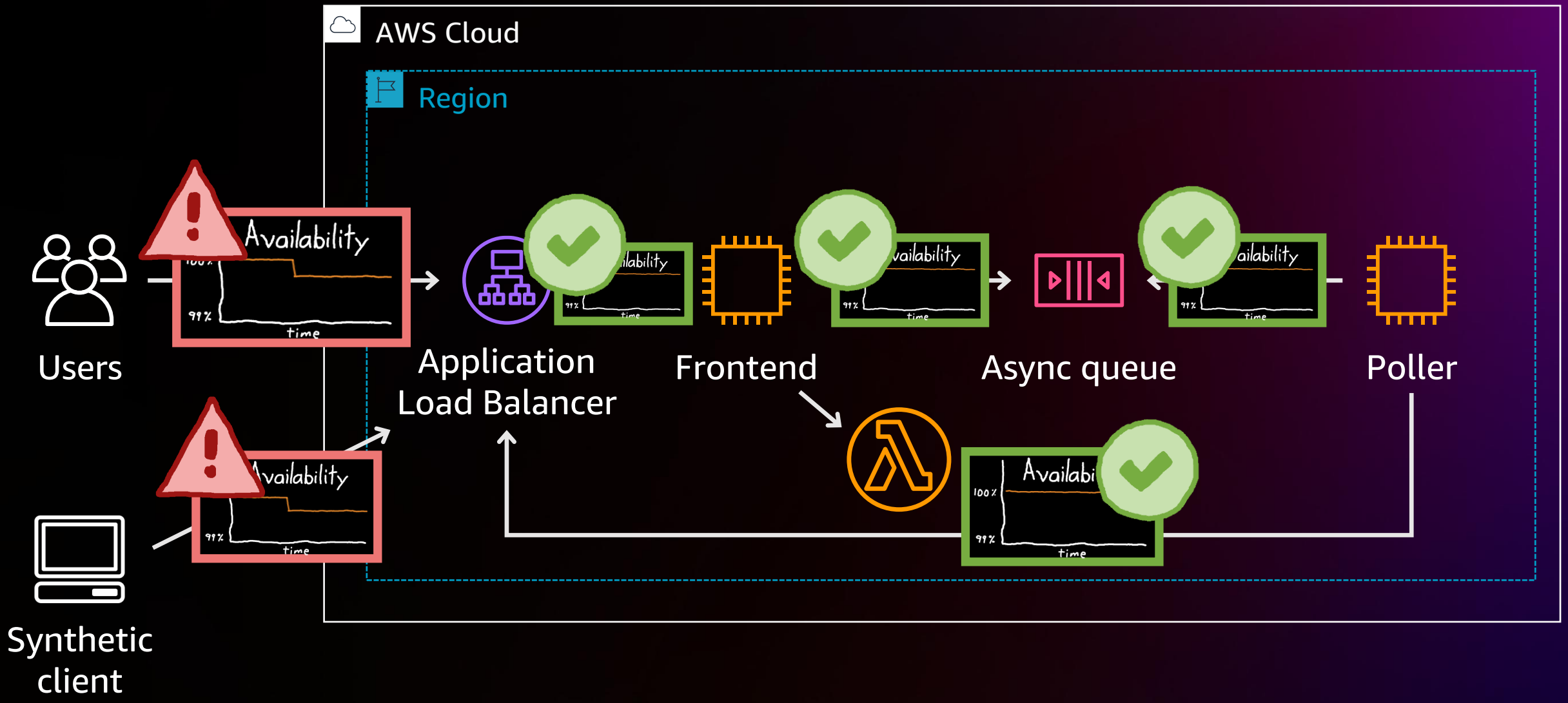
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Measure from everywhere



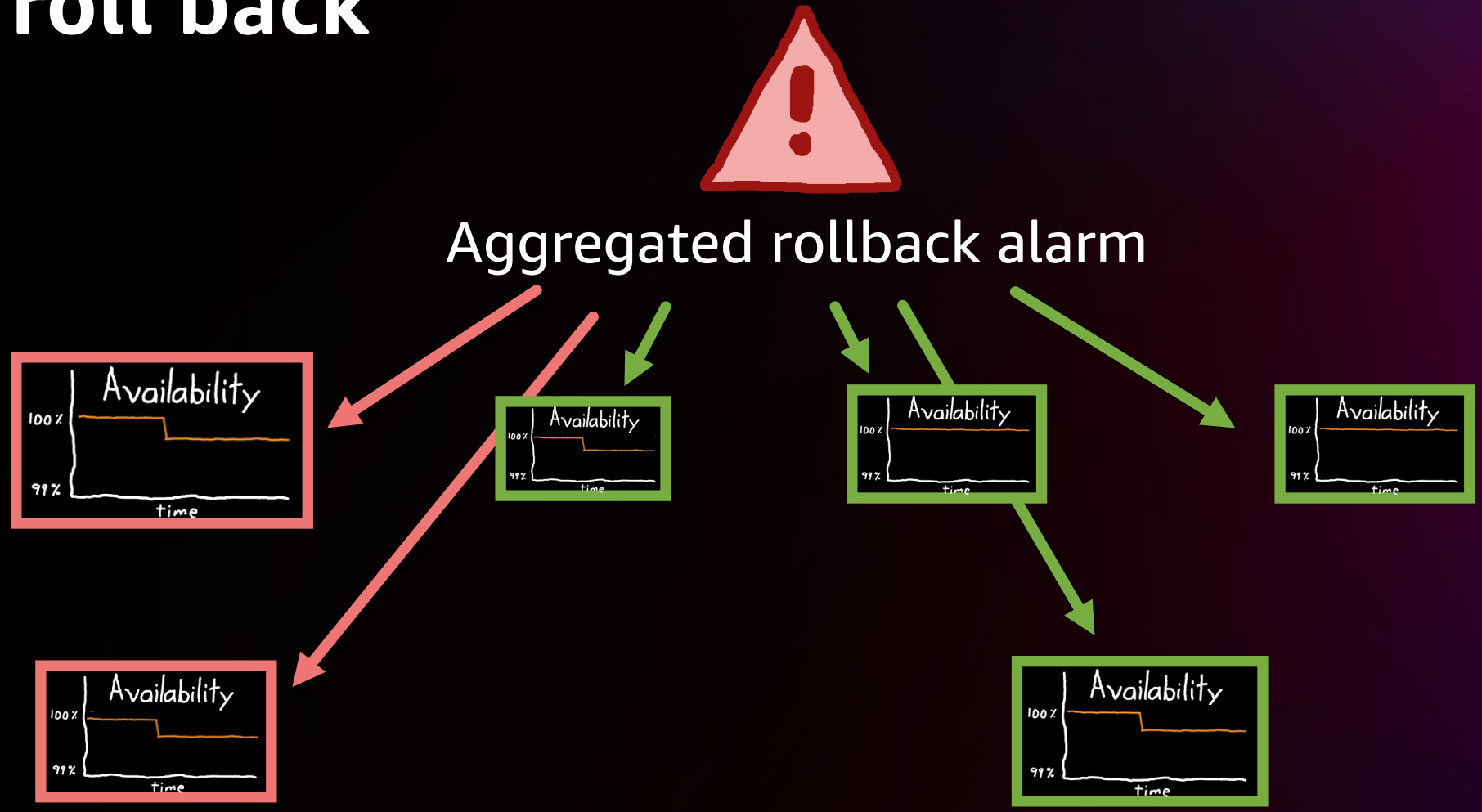
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Measure from everywhere



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Just roll back



https://aws.amazon.com/builders-library/ensuring-rollback-safety-during-deployments/

aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary: Deployment safety practices

- Deploy incrementally
- Perform thorough pre-checks
- Roll back first, ask questions later
- Have great monitoring and alarming

https://aws.amazon.com/builders-library/automating-safe-hands-off-deployments/

https://aws.amazon.com/builders-library/ensuring-rollback-safety-during-deployments/

https://aws.amazon.com/builders-library/going-faster-with-continuous-delivery/

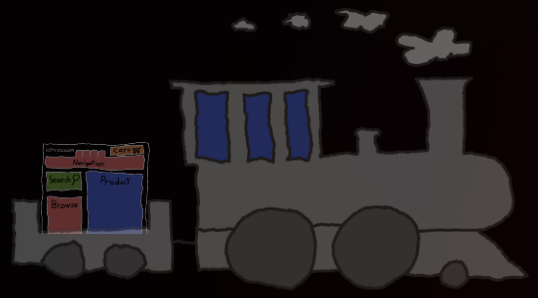
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

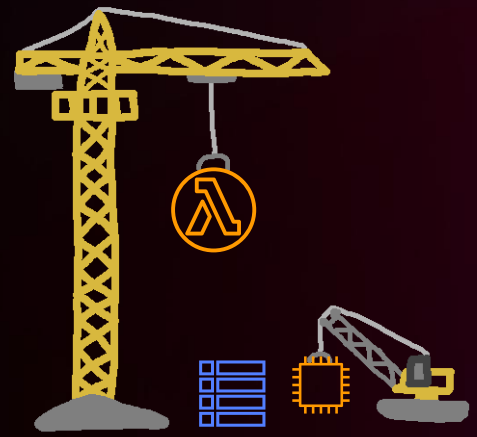
Chapter three



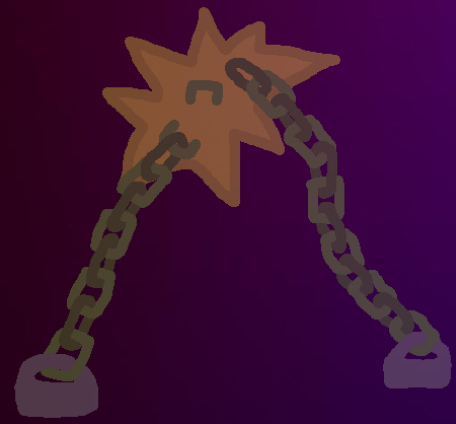
What is an event like?



Deploying software



Changing infrastructure



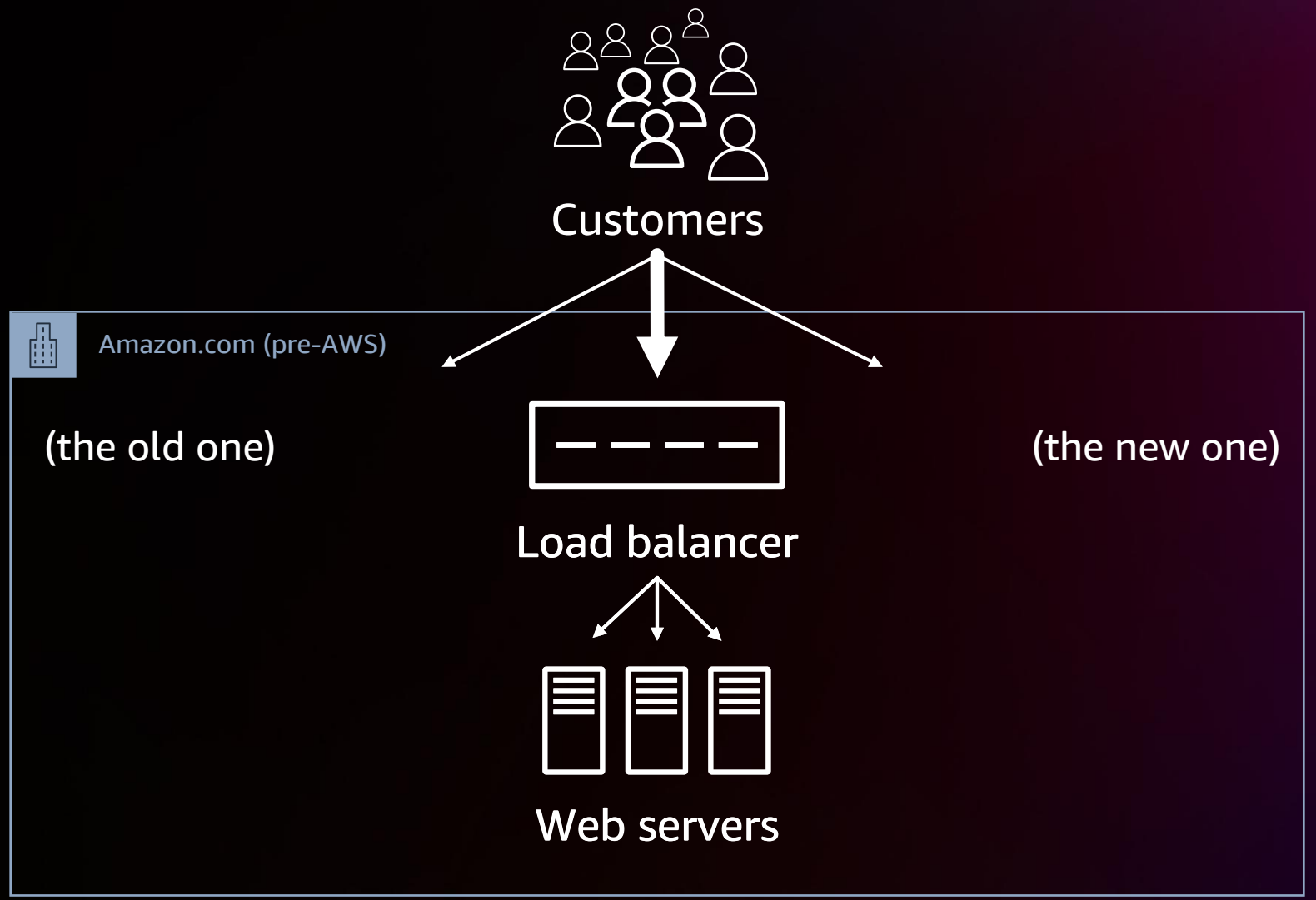
Breaking the unbreakable

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Story: Manual load balancer changes

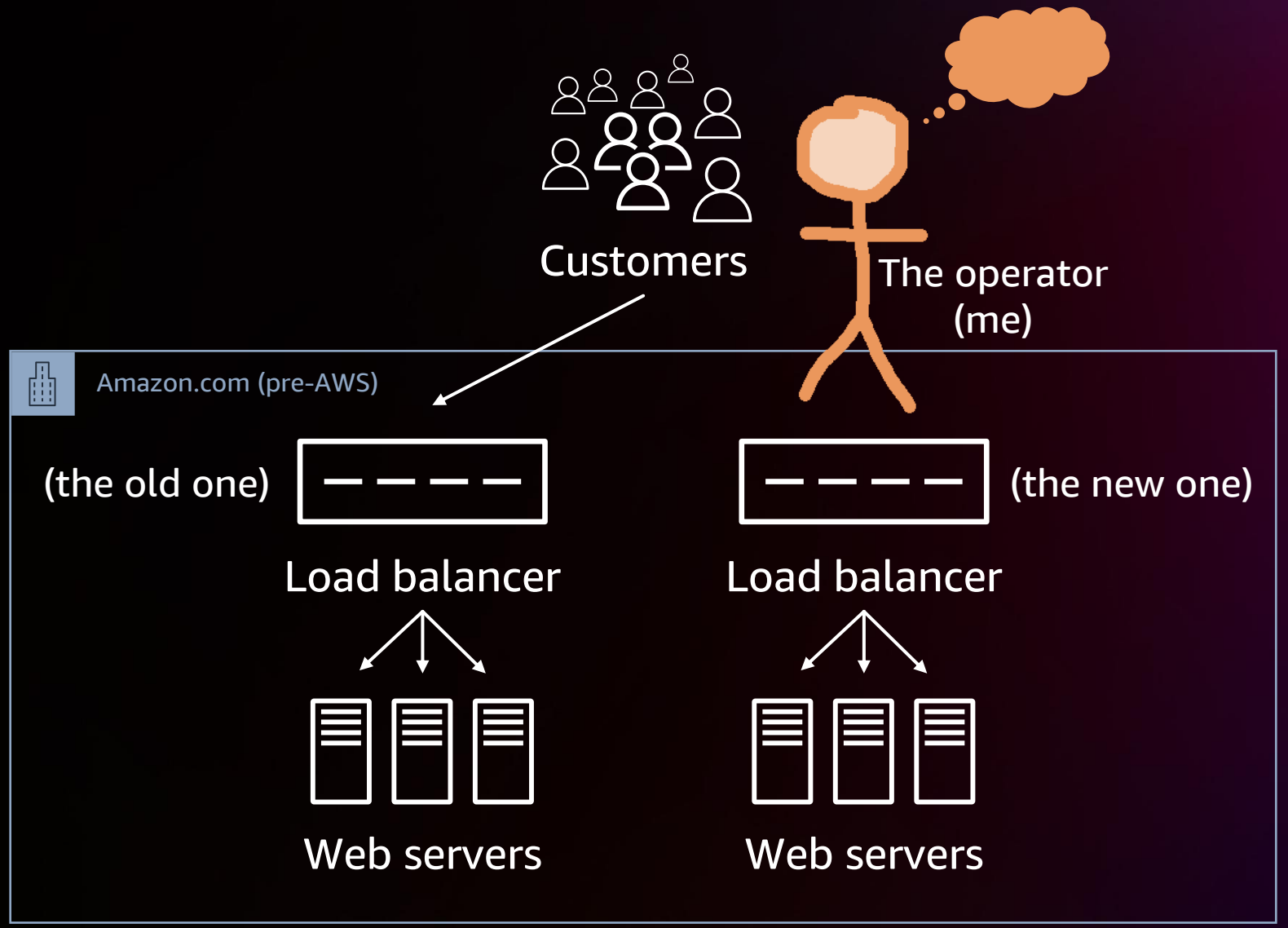
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure changes



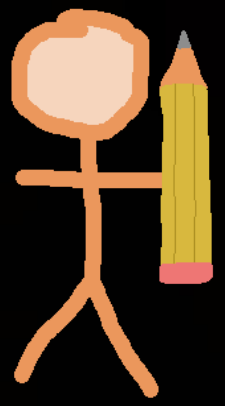
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure changes



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Making manual infrastructure changes



The operator (me)

Pre-checklist

- Is it configured correctly?
- Does it have its certificates?
- Is it monitored?
- Is it scaled?
- Are its web servers scaled?
- Does it work?

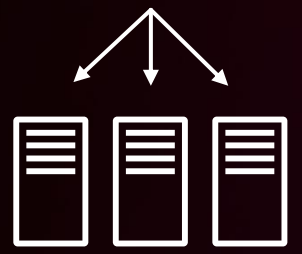


Customers



(the new one)

Load balancer

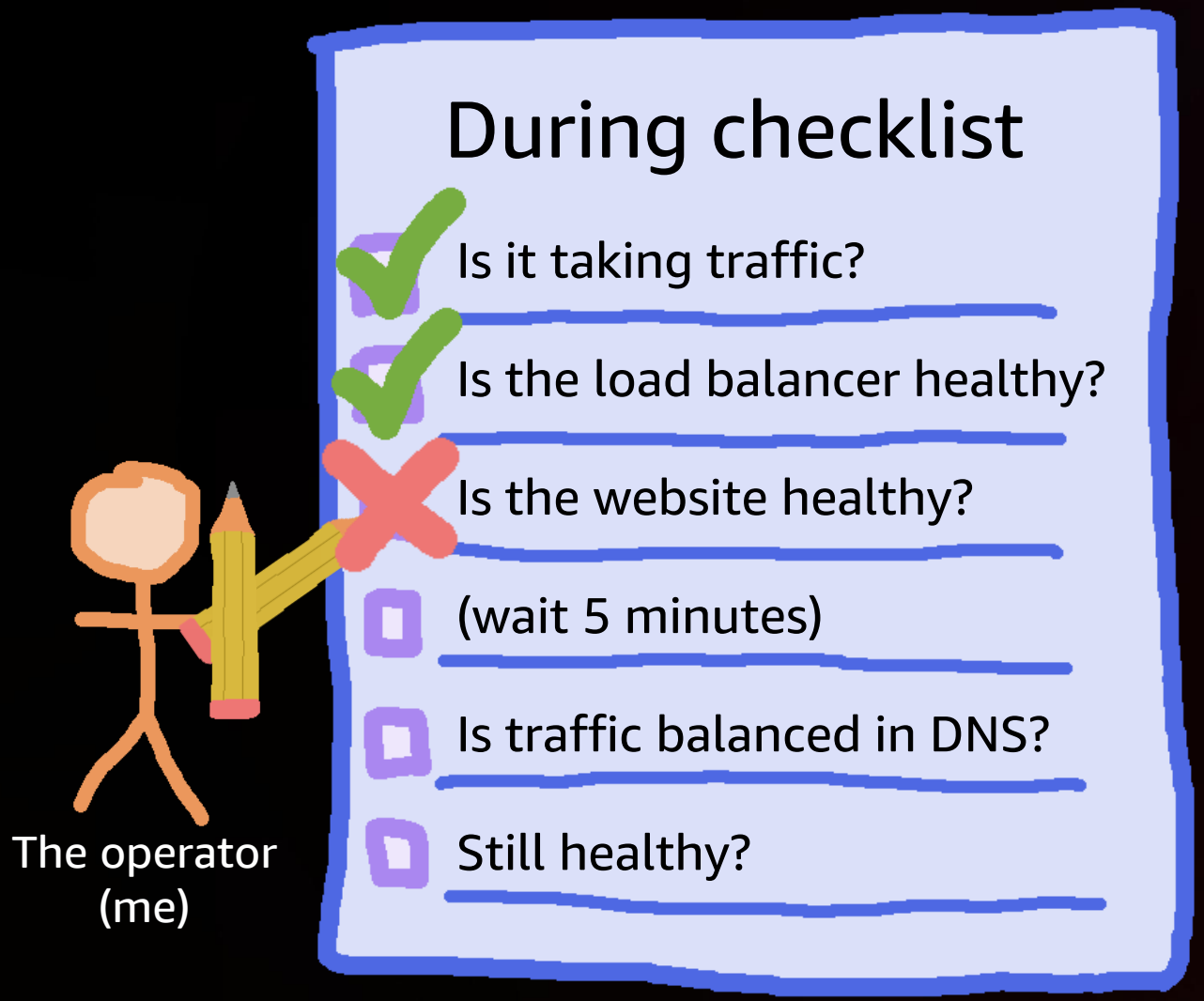


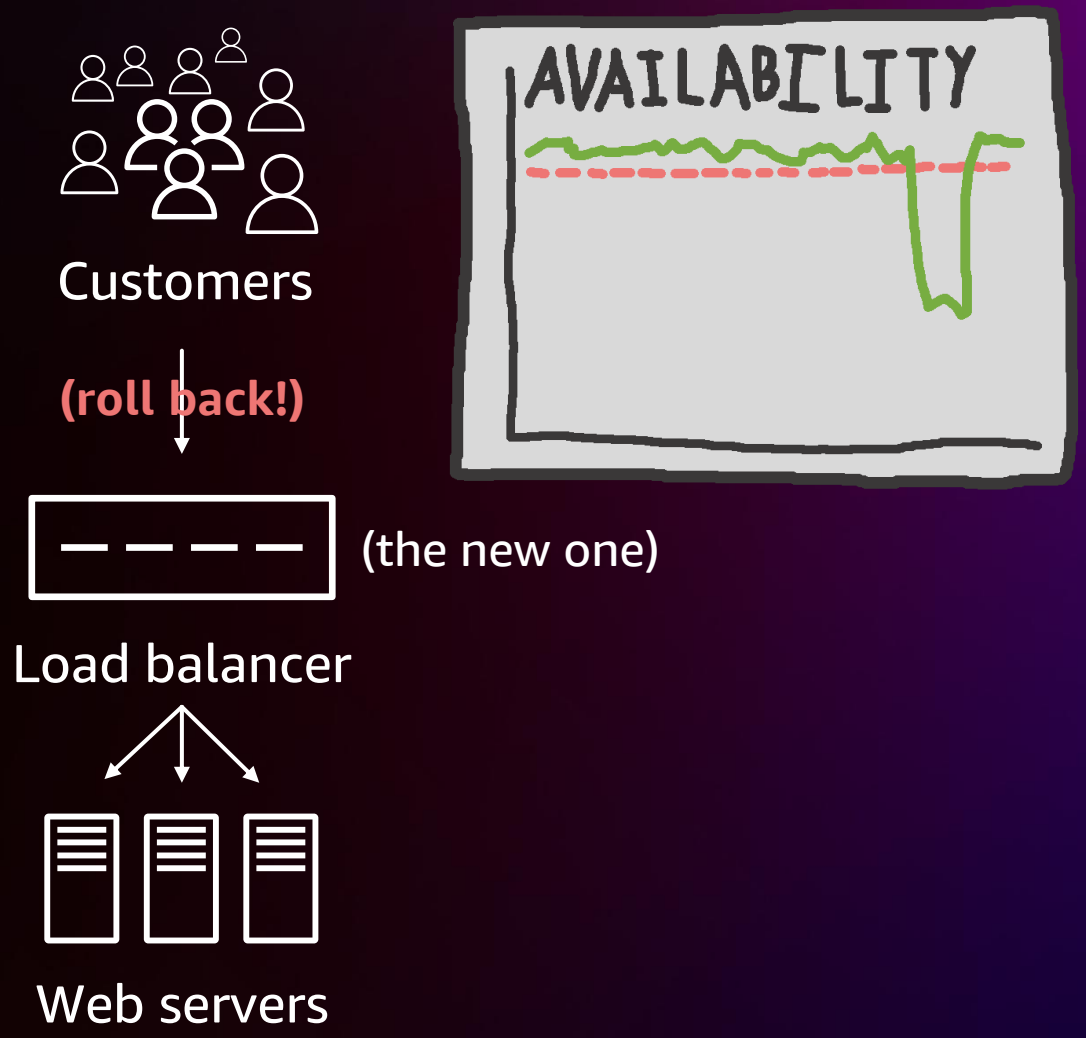
Web servers

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Making manual infrastructure changes





© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automating infrastructure changes

```
"LoadBalancer2": {
   "Type": "AWS::ElasticLoadBalancing::LoadBalancer",
    "AvailabilityZones": ["us-west-1a"],
    "Instances": [
        { "Ref": "Instance3" },
        { "Ref": "Instance4" }
    ],
    "Listeners": [ {
      "LoadBalancerPort": "443",
      "InstancePort": "8443",
      "Protocol": "HTTPS",
    } ],
...
```



AWS CloudFormation

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Automating infrastructure changes

```
const lb2 = new elbv2.ApplicationLoadBalancer(this, 'LB', {
  vpc,
  internetFacing: true
});

const listener2 = lb2.addListener('Listener', {
  port: 443,
});

listener2.addTargets('Target', {
  port: 8443,
  targets: [asg2]
});
```

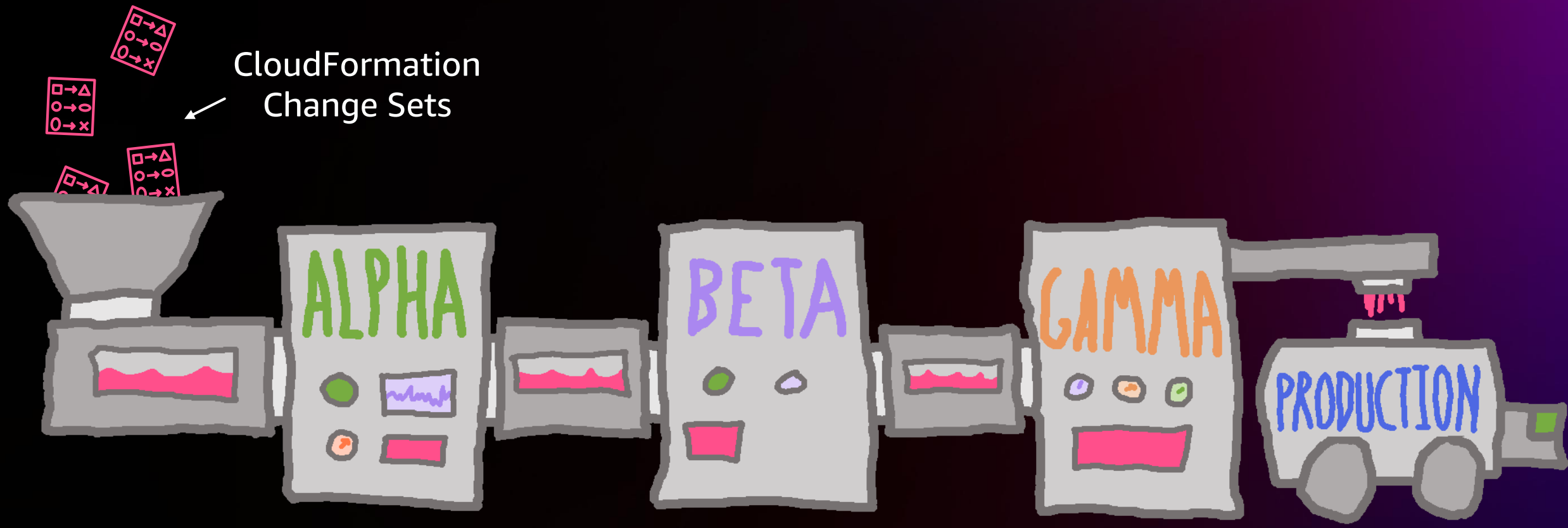


AWS Cloud Development Kit
(AWS CDK)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure pipelines



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

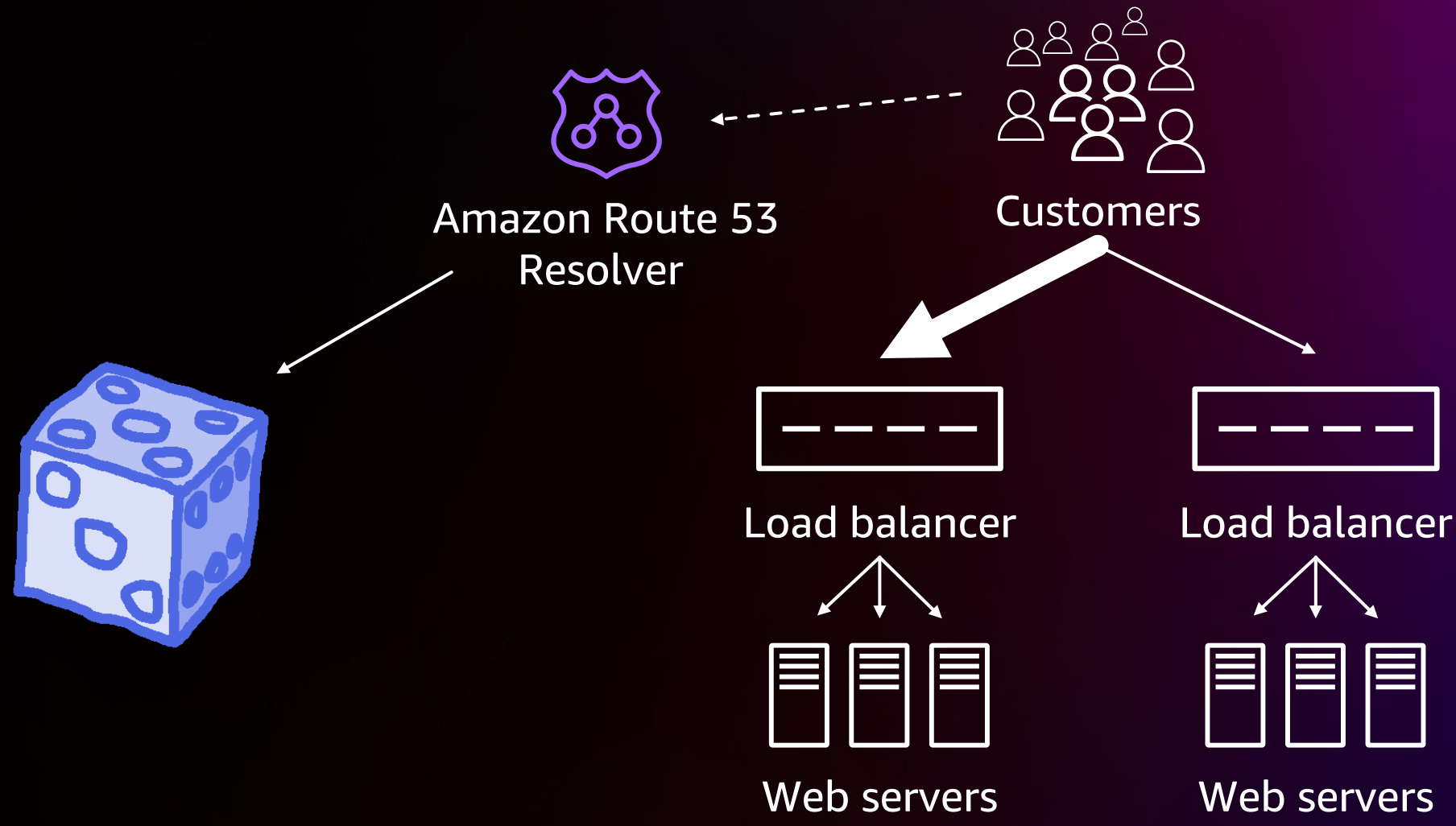
Infrastructure change best practices

- Roll back first, ask questions later
- Have great monitoring and alarming
- Deploy incrementally
- Perform thorough pre-checks

aws

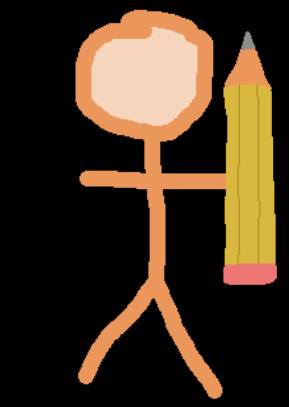
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

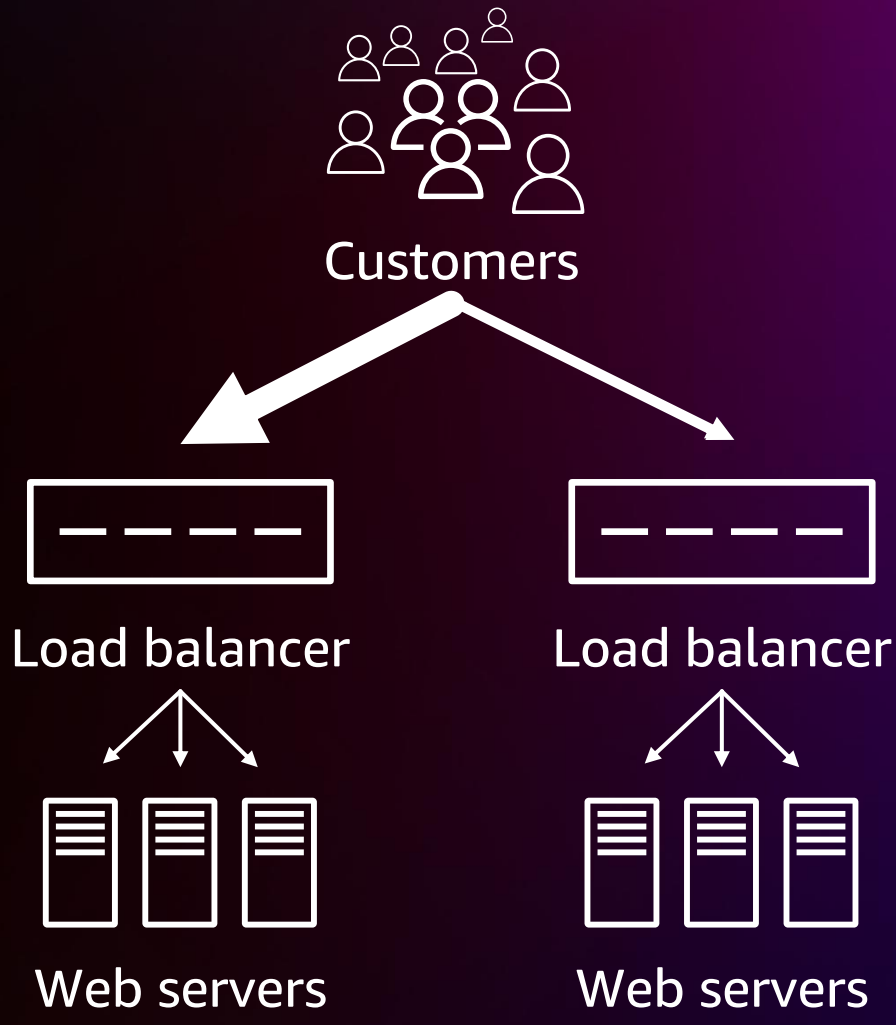
Incremental infrastructure changes



The operator (me)

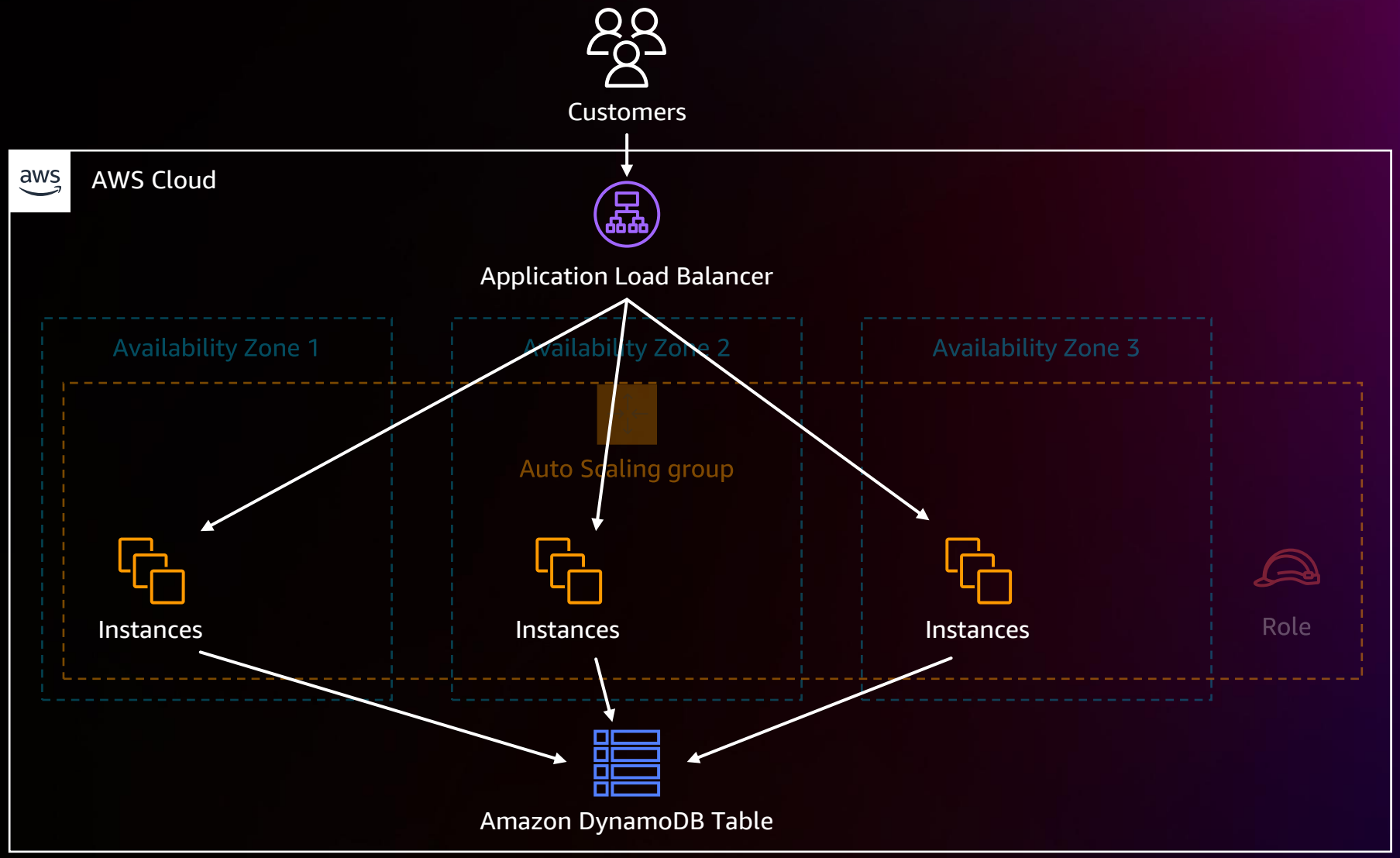
During checklist

- [ ] Dial up DNS 1%?
- [ ] Is the load balancer healthy?
- [ ] Is the website healthy?
- [ ] (wait 5 minutes)
- [ ] Repeat at 5%, 10%, 25%
- [ ] Repeat at 50%, 75%, 100%



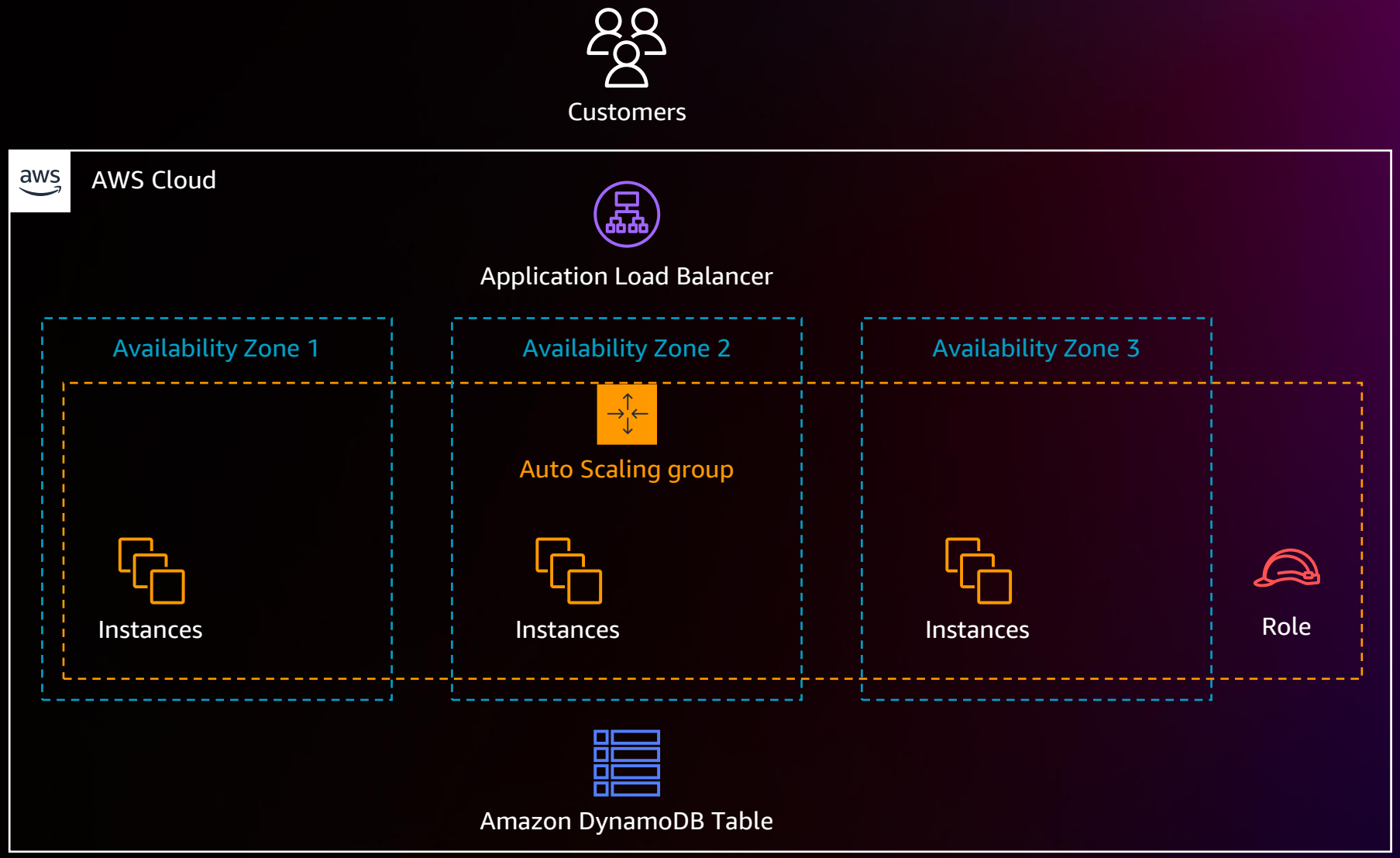
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



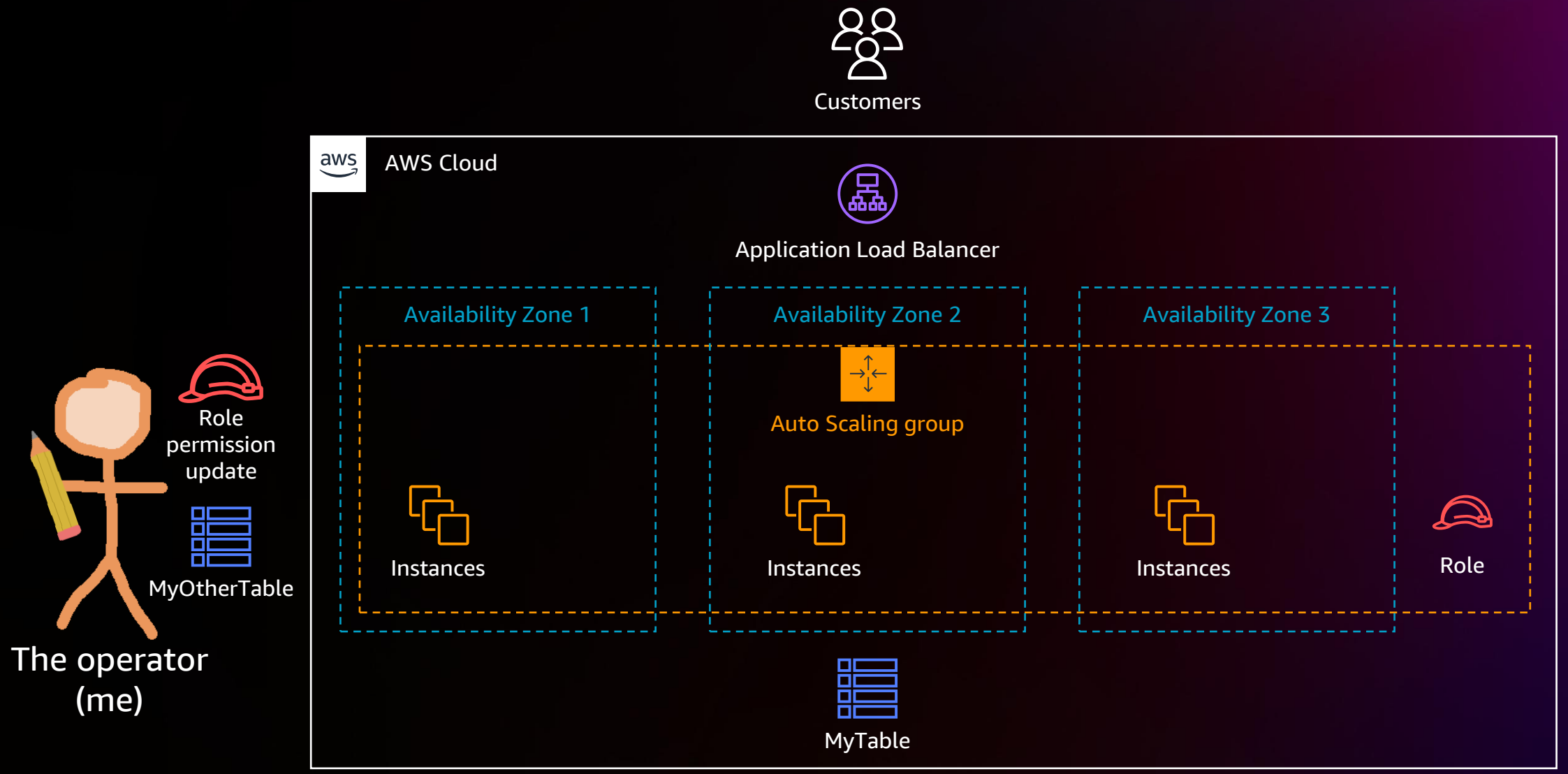
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes

```
{
  "Effect": "Allow",
  "Action": [ "dynamodb:Query" ],
  "Resource": [
    "arn:aws:dynamodb:*:*:table/MyTable"
  ]
}
```

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Adding access to a new table

```
{
  "Effect": "Allow",
  "Action": [ "dynamodb:Query" ],
  "Resource": [
-   "arn:aws:dynamodb:*:*:table/MyTable"
+   "arn:aws:dynamodb:*:*:table/MyTable",
+   "arn:aws:dynamodb:*:*:table/MyOtherTable"
  ]
}
```

(Added comma to this line)

(Added access to new table)

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

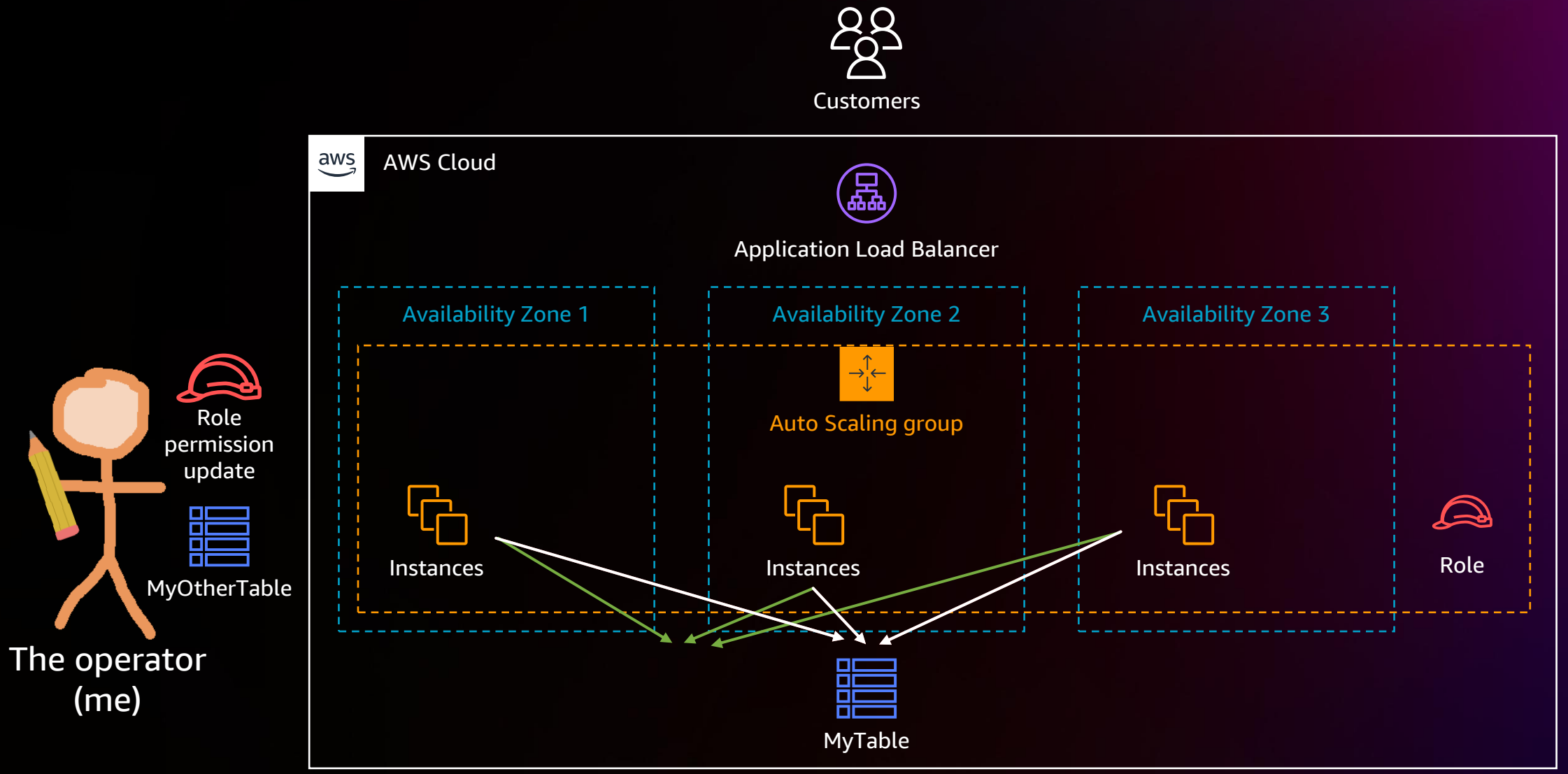
Making a mistake

```
{
  "Effect": "Allow",
  "Action": [ "dynamodb:Query" ],
  "Resource": [
-   "arn:aws:dynamodb:*:*:table/MyTable"
+   "arn:aws:dynamodb:*:*:table/MyOtherTable"
  ]
}
```

(Oops! Dropped access to old table)

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



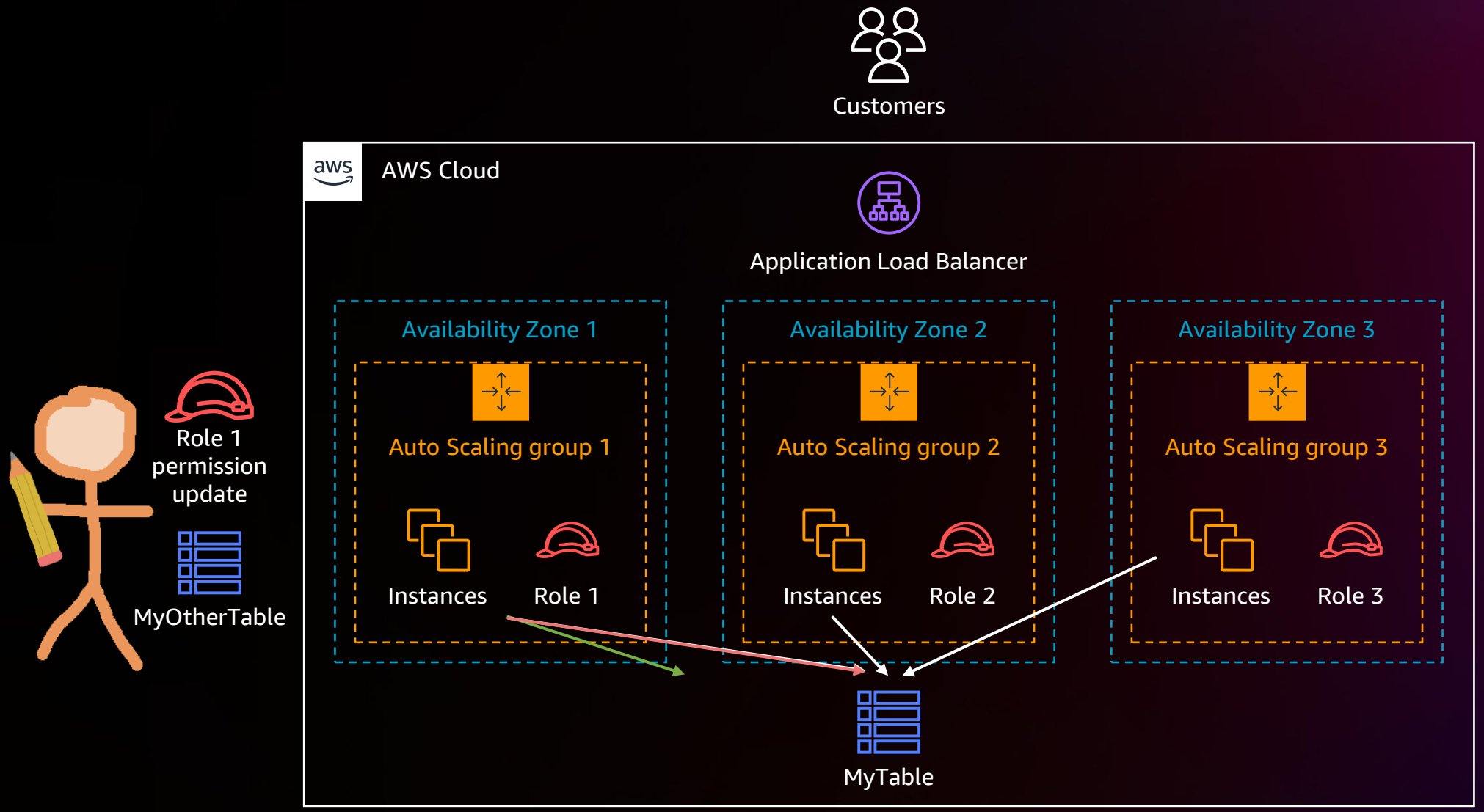
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure change safety practices

- Roll back first, ask questions later
- Have great monitoring and alarming
- **Deploy incrementally**
- Perform thorough pre-checks

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Incremental infrastructure changes



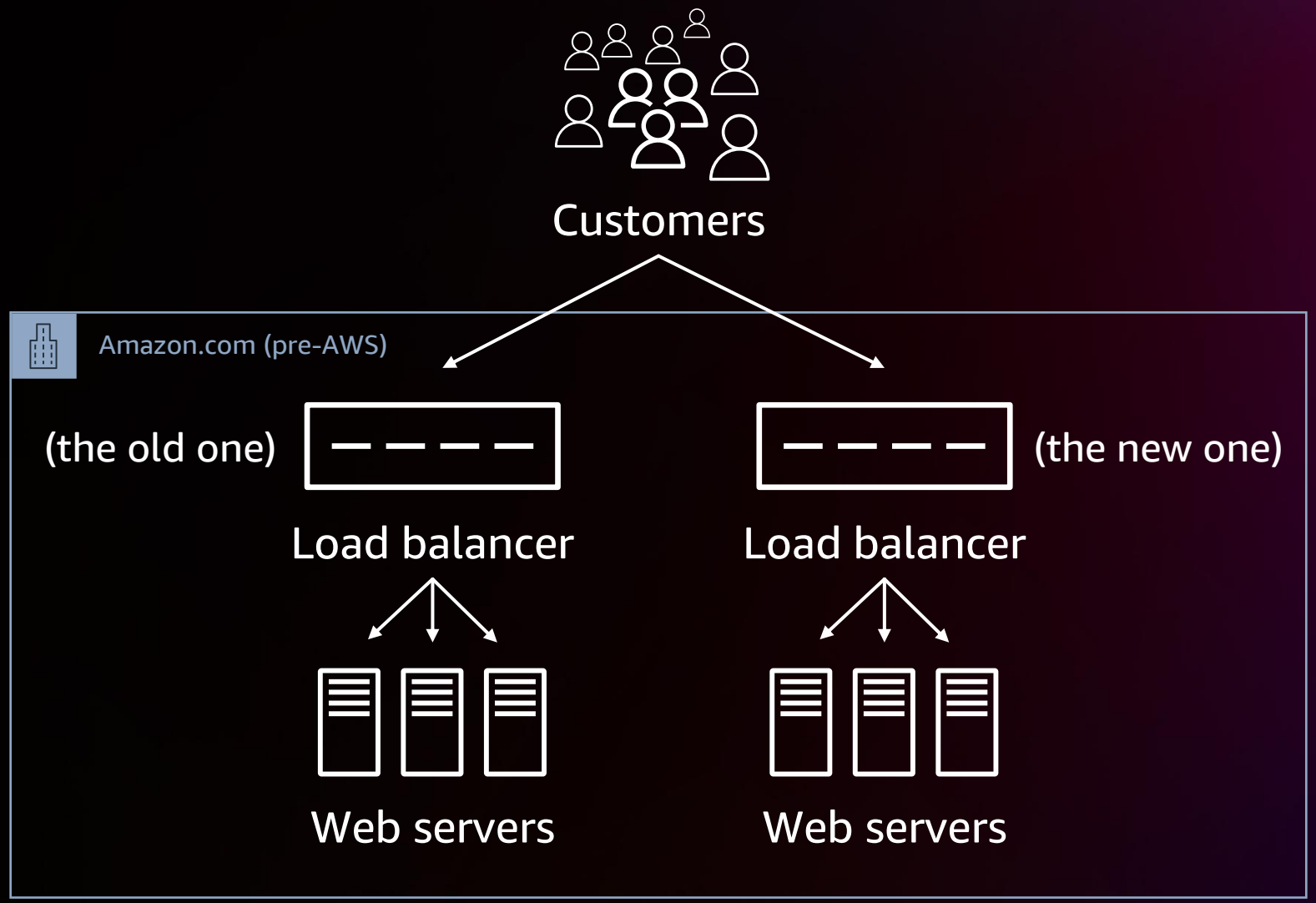
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure change safety practices

- Roll back first, ask questions later
- Have great monitoring and alarming
- Deploy incrementally
- **Perform thorough pre-checks**

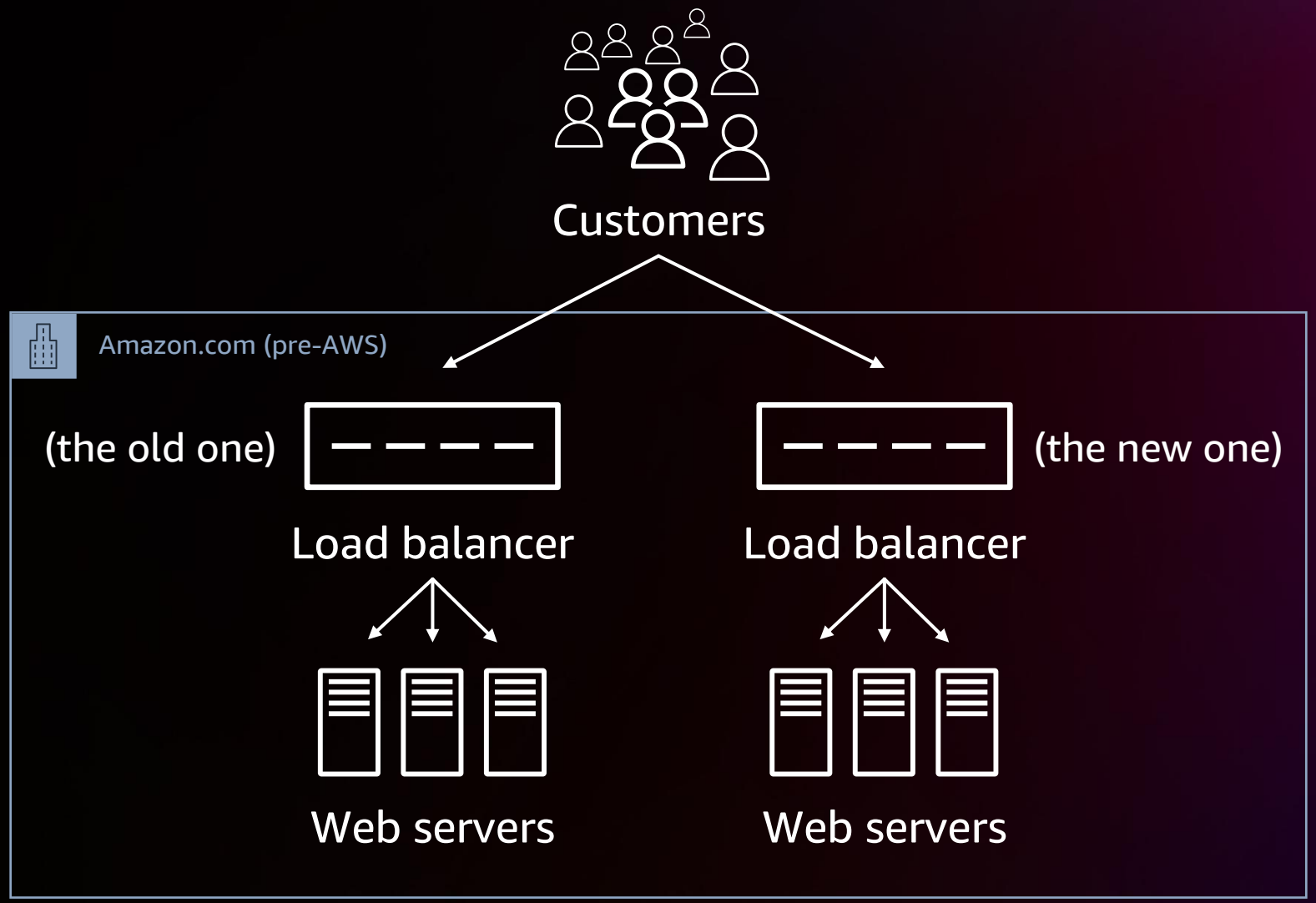
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Migrating infrastructure



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Decommissioning infrastructure

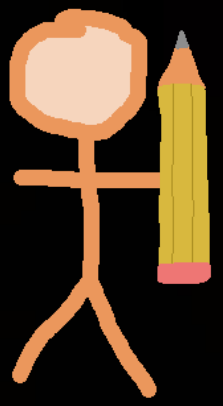


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Decommissioning infrastru



Bring back the pre-checks!



The operator (me)

Pre-delete checklist

- [ ] Are you sure?
- [ ] Is it in use?
- [ ] Is it backed up?
- [ ] Can you roll back?
- [ ] Is this a “do not delete” db?
- [ ] Are you really sure?

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Prevention: the ultimate pre-check

Edit termination protection for YourApplication?

Termination protection on a stack prevents it from being deleted accidentally.

Termination protection

- ○ Disabled
- ◉ Enabled

`DeletionPolicy` attribute



AWS CloudFormation

Enable termination protection



AWS Identity and Access Management (IAM)

```
"Effect": "Deny",
"Action": "dynamodb:DeleteTable",
"Resource": "*"
```



Amazon Elastic Compute Cloud (Amazon EC2)

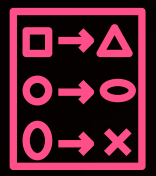
aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

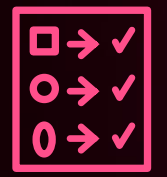
Other pre-checks?



AWS CloudFormation



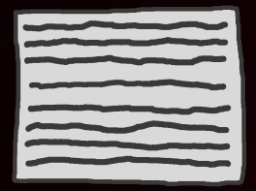
Change sets



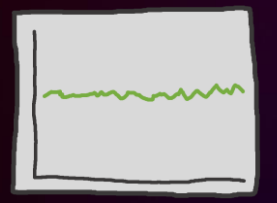
Hooks



Evaluate policy



Check CloudTrail logs



Query utilization metrics

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Infrastructure change safety practices

- **Roll back first, ask questions later**
- Have great monitoring and alarming
- Deploy incrementally
- Perform thorough pre-checks

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Rolling back deletes

- CloudFormation rollbacks
- Back up state (and practice restore) before deleting
- Isolate before delete (block traffic first, then delete)
- Stop instances before deleting
- Deny access before deleting
- Scale down before deleting



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Summary: Change safety practices

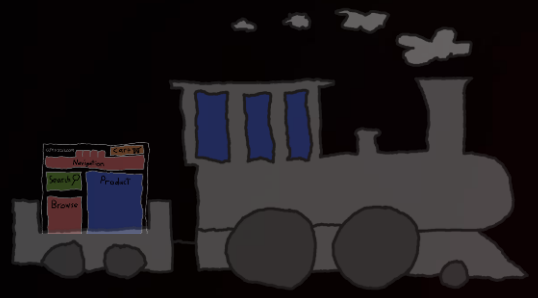
- Roll back first, ask questions later
- Have great monitoring and alarming
- Deploy incrementally
- Perform thorough pre-checks

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

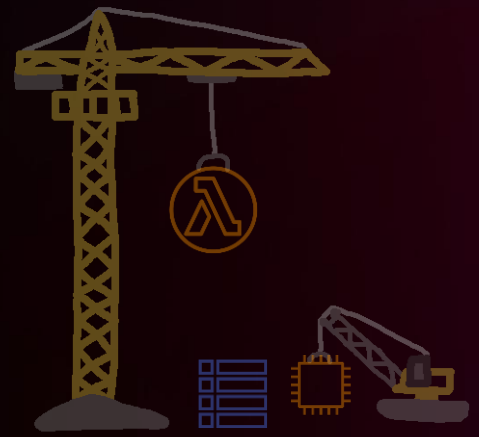
Chapter four



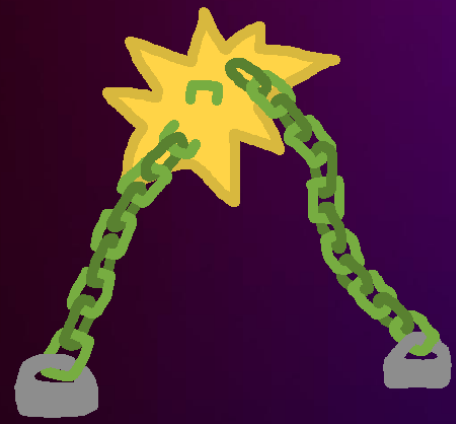
What is an event like?



Deploying software



Changing infrastructure



Breaking the unbreakable

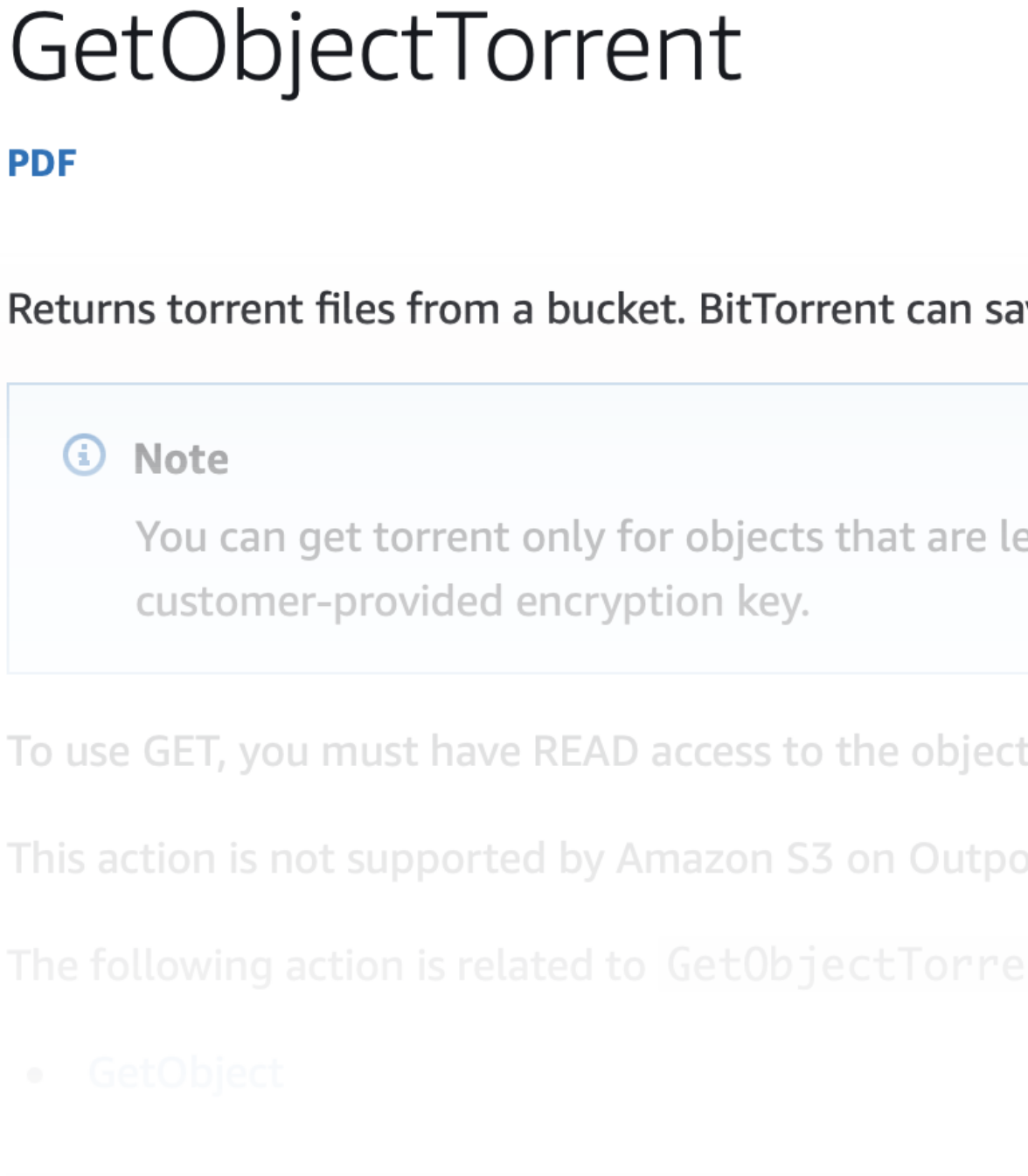
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the unbreakable

At AWS, every API is treated as a promise

We still support the original SOAP and WSDL APIs for our early services

S3 BitTorrent still works!



aws © 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the unbreakable

Occasionally, we do need to change something in an incompatible way

Every such change is reviewed by the AWS leadership team

Every approved change is shepherded by an executive sponsor

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the unbreakable

EC2 instances became so popular that we moved to 63-bit longids

Security improvements can obsolete older versions of protocols, and compliance frameworks insist on turning off the old versions

~~SSLv3~~ ~~TLSv1.0~~ ~~TLSv1.1~~ TLSv1.2 TLSv1.3

~~RC4~~ ~~3DES~~ AES-GCM ChaCha20-Poly1305

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the unbreakable

We treat deprecations as a long-running operational process

These processes can range from one to three years depending on the complexity

First, instrument and ideally empower customers

Limit customer engagement to easy to action notifications

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Breaking the unbreakable

Give customers resource, account, or organization level visibility and controls as appropriate

Make it as easy as possible to flag anything that may break in advance

Have a “fake out” before any “real” deadline

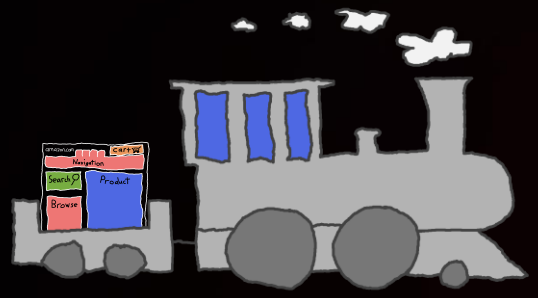
Learn as many lessons as possible for future agility

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

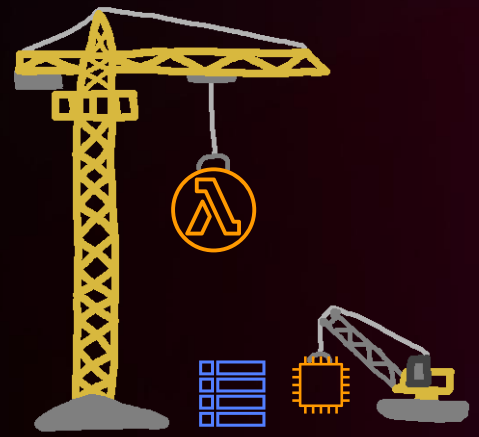
In conclusion



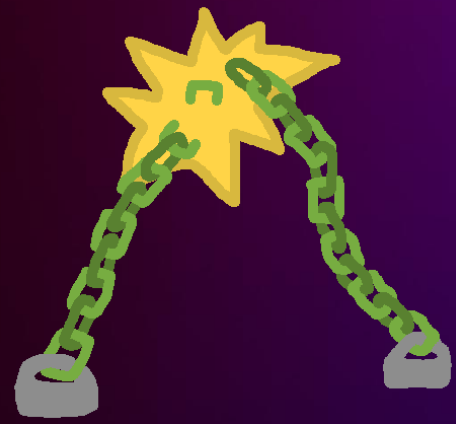
What is an event like?



Deploying software



Changing infrastructure



Breaking the unbreakable

aws

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Conclusion

$$Dev = Ops$$

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

The Amazon Builders' Library

Firsthand articles from engineers who built AWS services:

- Caching
- Retries
- Fairness
- Safety
- More…



https://aws.amazon.com/builders-library/

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Thank you!

Colm MacCárthaigh
@colmmacc

David Yanacek
@dyanacek



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

© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.