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

STG219

Building resilient architectures with Amazon EBS

Cami Tavares

Director, Product Management
Amazon EBS

Marc Olson

Senior Principal Engineer
Amazon EBS

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

Agenda

How to think about resiliency

Resiliency in AWS

Deep dive: EBS built-in resiliency

Taking charge of your application resiliency

Real-world examples

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

How to think about resiliency

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

How to think about resiliency



Understand risks and potential disruptions

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

How to think about resiliency

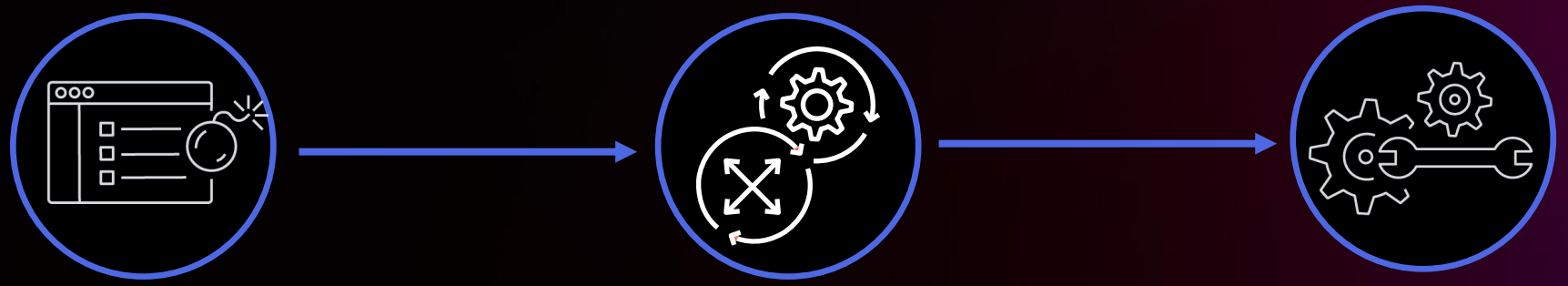


Understand risks and potential disruptions

Minimize scope of impact

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

How to think about resiliency



Understand risks and potential disruptions

Minimize scope of impact

Plan and automate recovery

aws

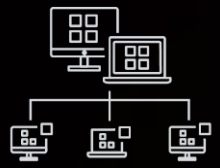
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

“Anything that can go wrong will go wrong.”

Murphy’s Law

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

Resilient workloads can withstand . . .



Component failures

Server crash
Disk failure
Network issues

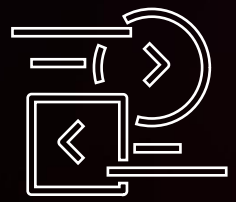
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilient workloads can withstand . . .



Component failures

Server crash
Disk failure
Network issues



Infrastructure events

Power failures
Natural disasters
Physical damage

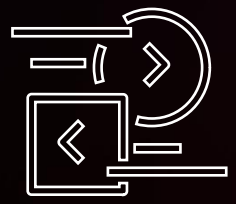
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilient workloads can withstand . . .



Component failures

Server crash
Disk failure
Network issues



Infrastructure events

Power failures
Natural disasters
Physical damage



Load Stress

Demand surge
Denial of Service
Poison pills

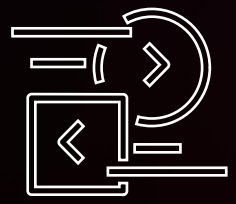
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resilient workloads can withstand . . .



Component failures

Server crash
Disk failure
Network issues



Infrastructure events

Power failures
Natural disasters
Physical damage

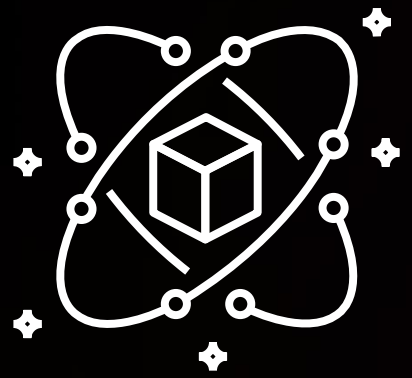


Load Stress

Demand surge
Denial of Service
Poison pills

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

Understand architecture risks



Identify your dependencies

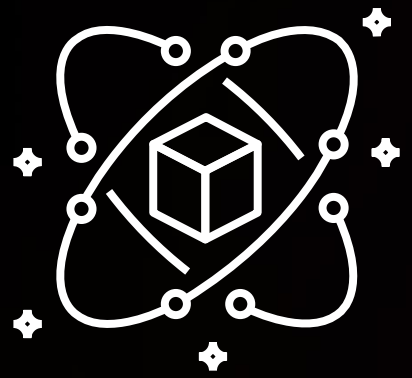
Recognize properties of your environment

Design for availability

aws

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

Understand architecture risks



Identify your dependencies

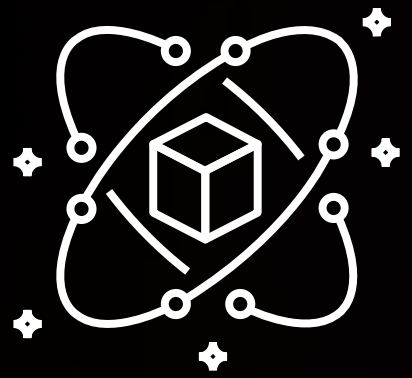
Recognize properties of your environment

Design for availability

aws

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

Understand architecture risks



Identify your dependencies

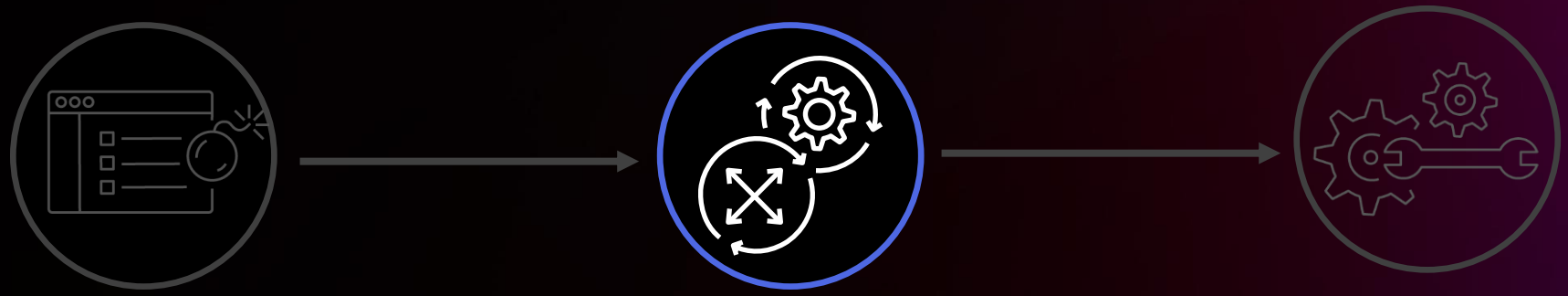
Recognize properties of your environment

Design for availability

aws

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

How to think about resiliency



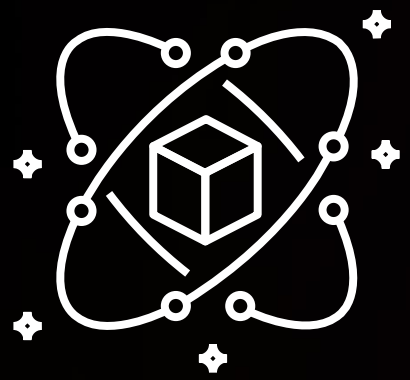
Understand risks and potential disruptions

Minimize scope of impact

Plan and automate recovery

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

Minimize scope of impact



Who is impacted?

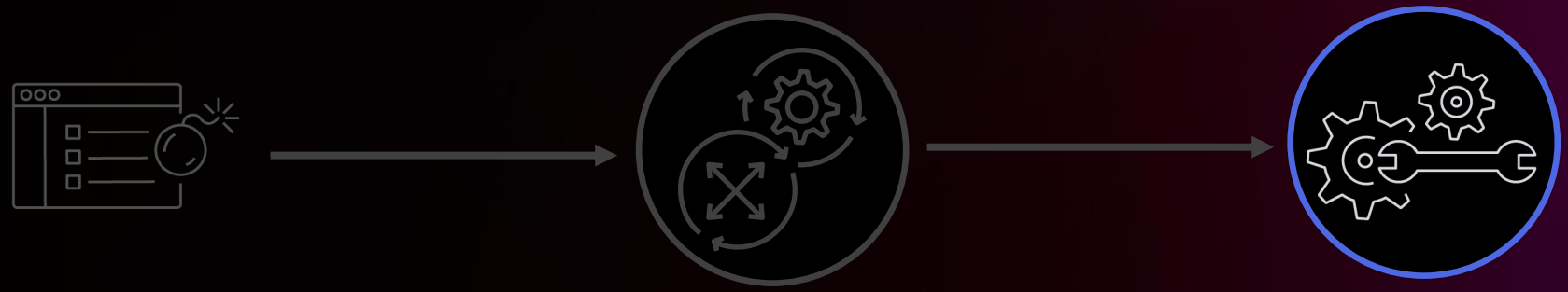
How many workloads?

What functionality?

How many locations?

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

How to think about resiliency



Understand risks and potential disruptions

Minimize scope of impact

Plan and automate recovery

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

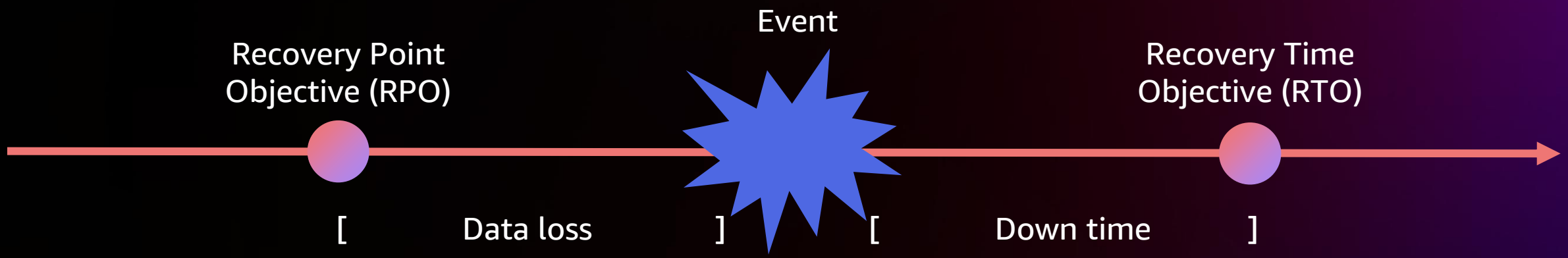
Recovery



What systems break if your service is unavailable?

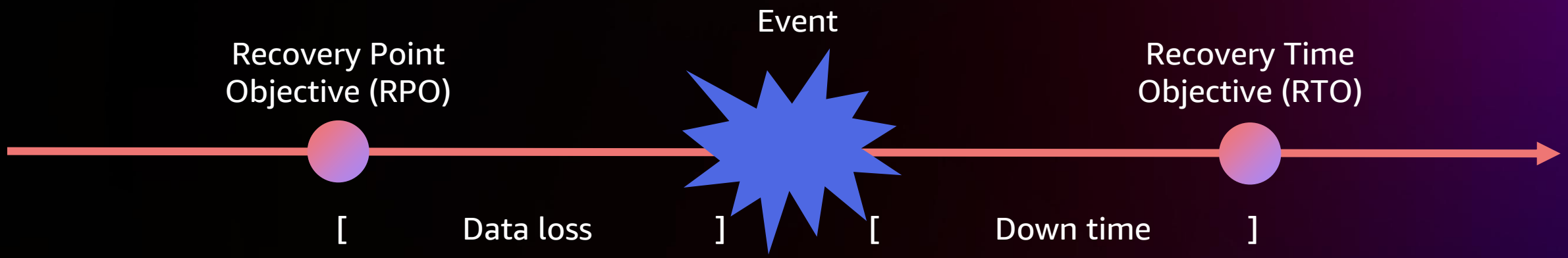
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recovery for business continuity



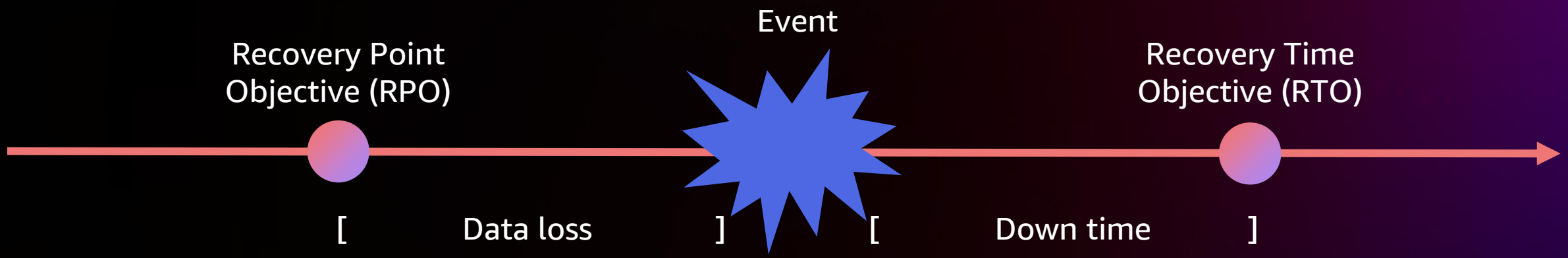
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recovery for business continuity



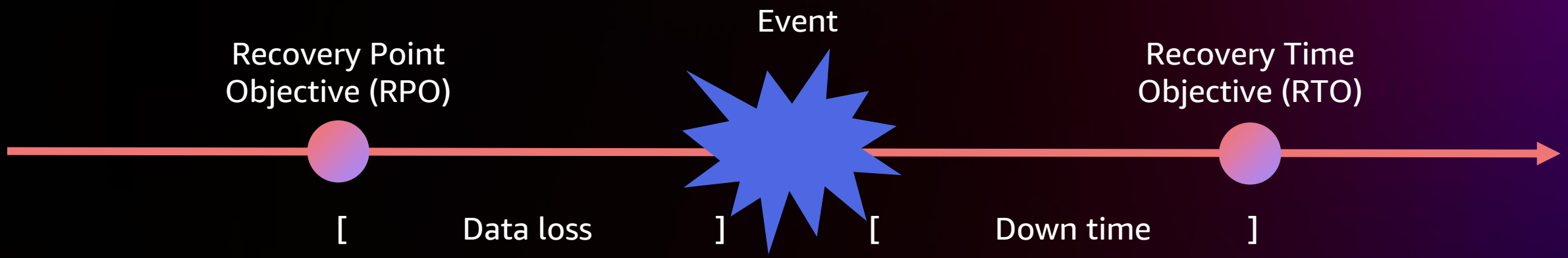
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recovery for business continuity



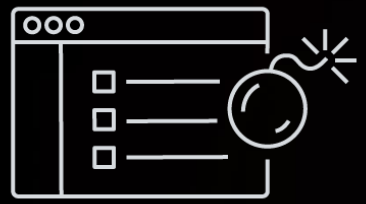
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Recovery for business continuity



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

On-premises challenges

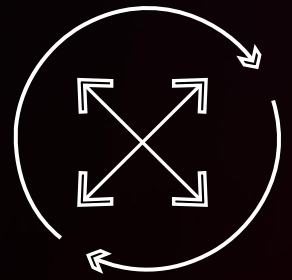


Risks

Network equipment

Hardware

Resource saturation



Scope of impact

Redundancy is expensive

Geographical expansion

Unintended shared fate



Recovery

Hardware replacement

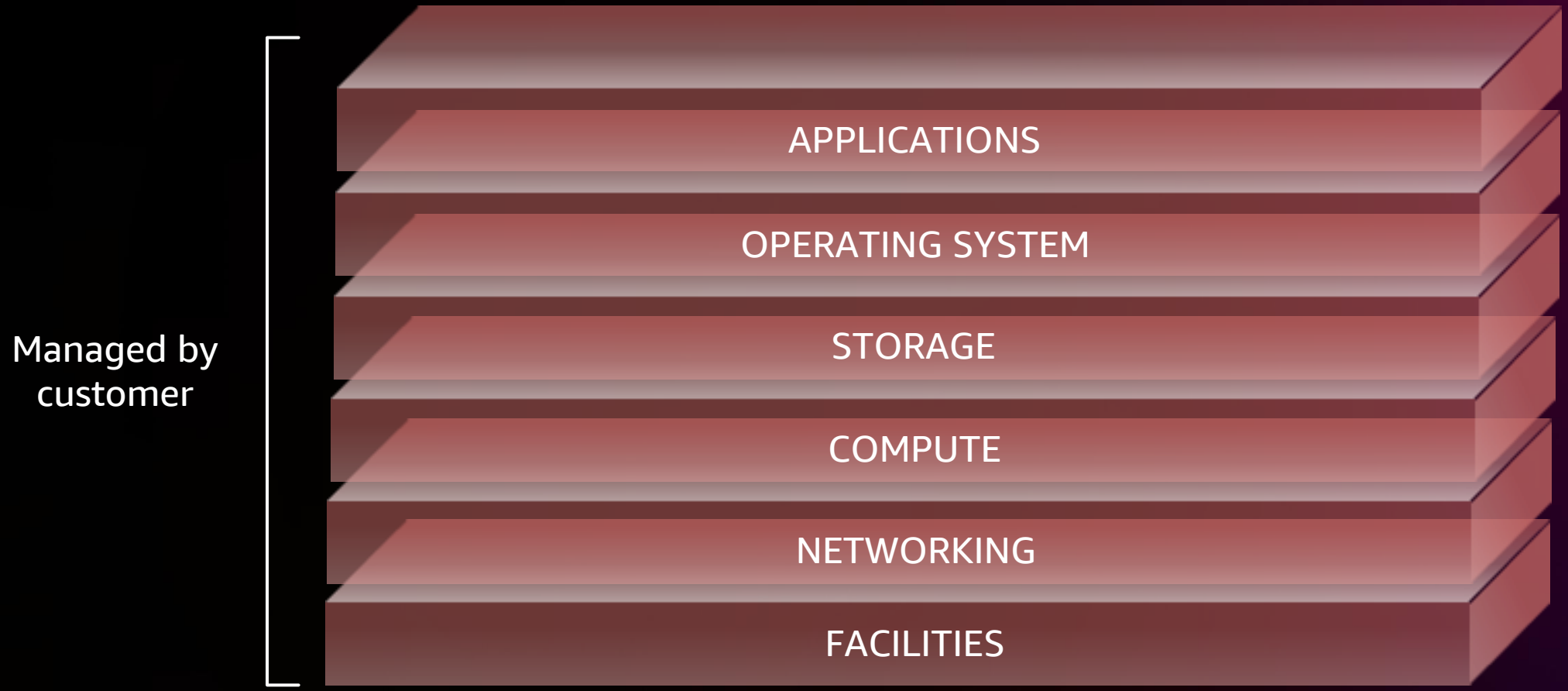
Procurement

Manual procedures

aws

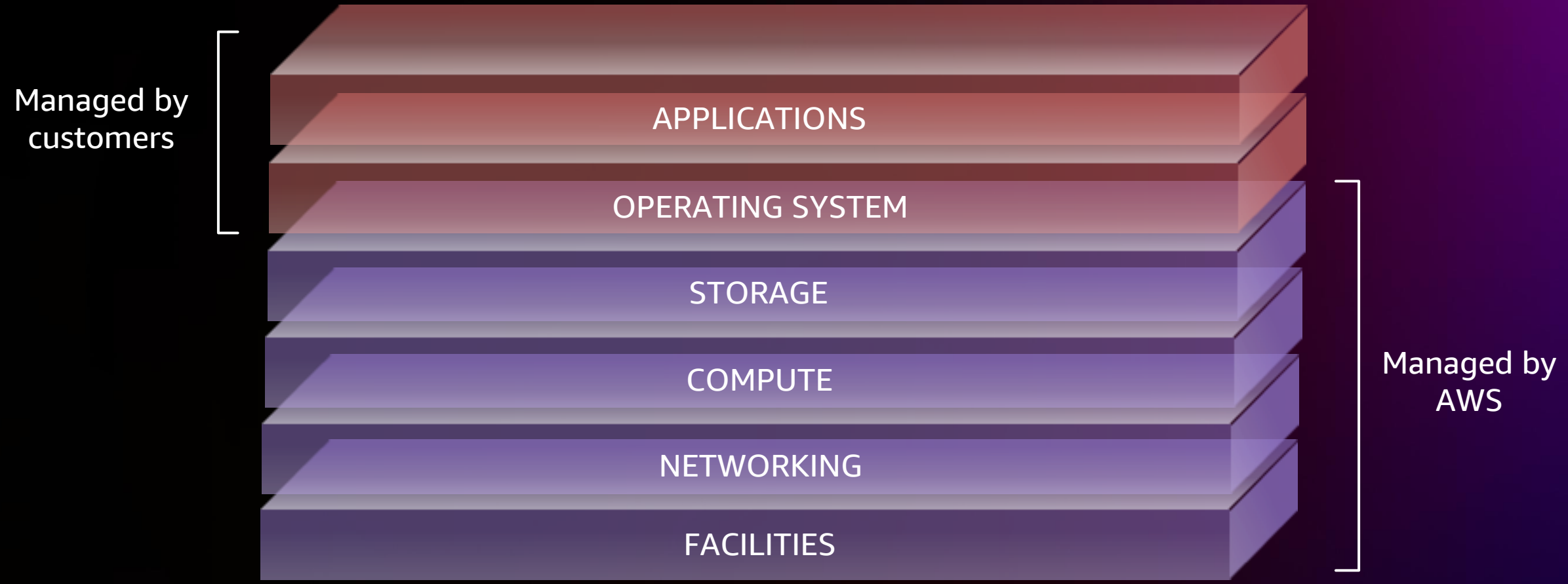
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

On-premises challenges



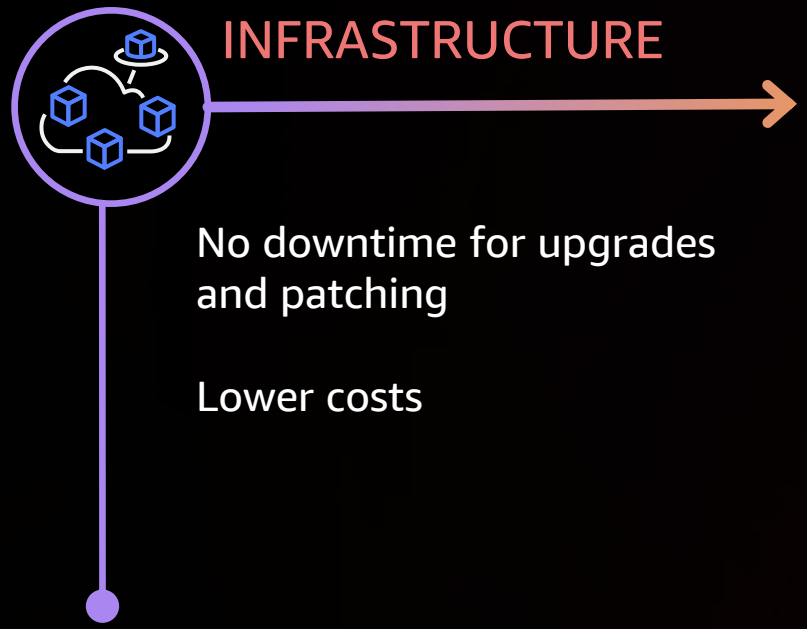
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency is easier in AWS



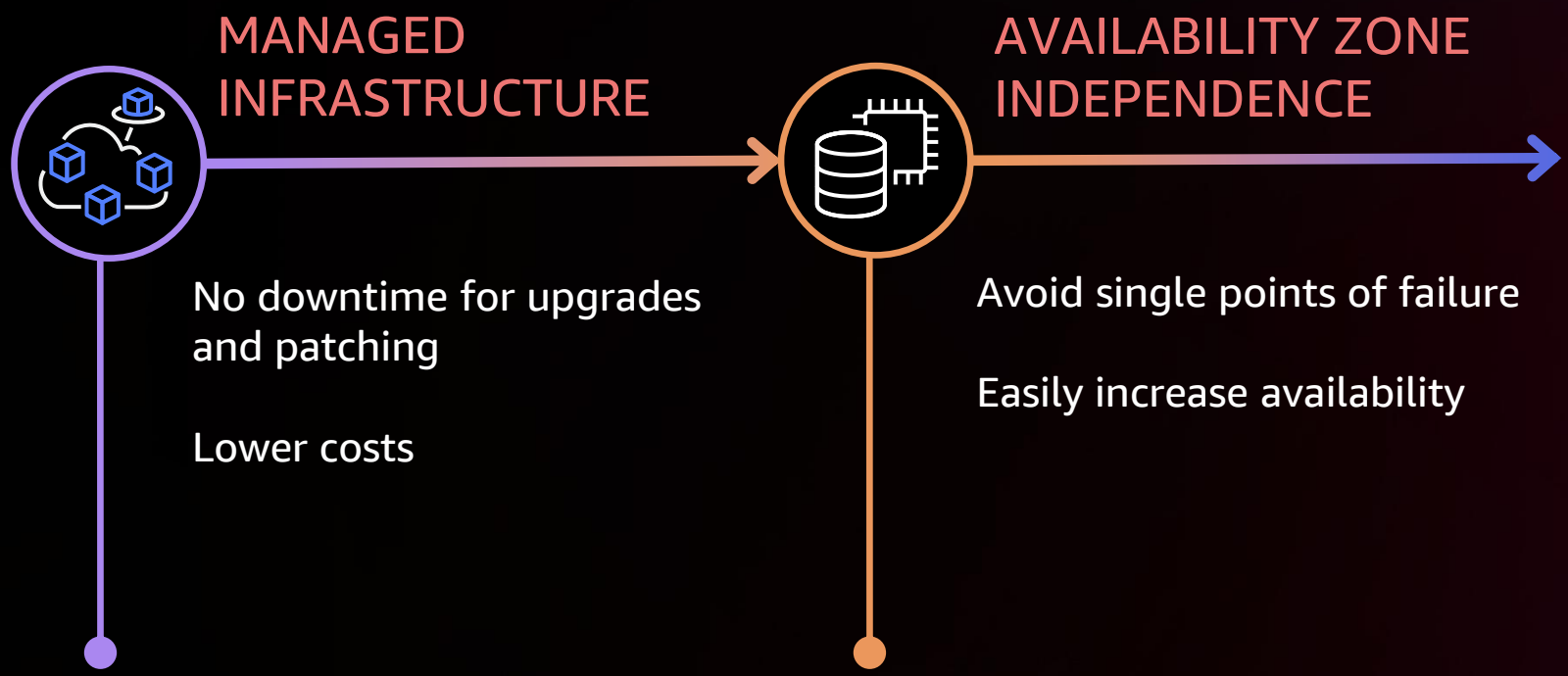
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency in AWS



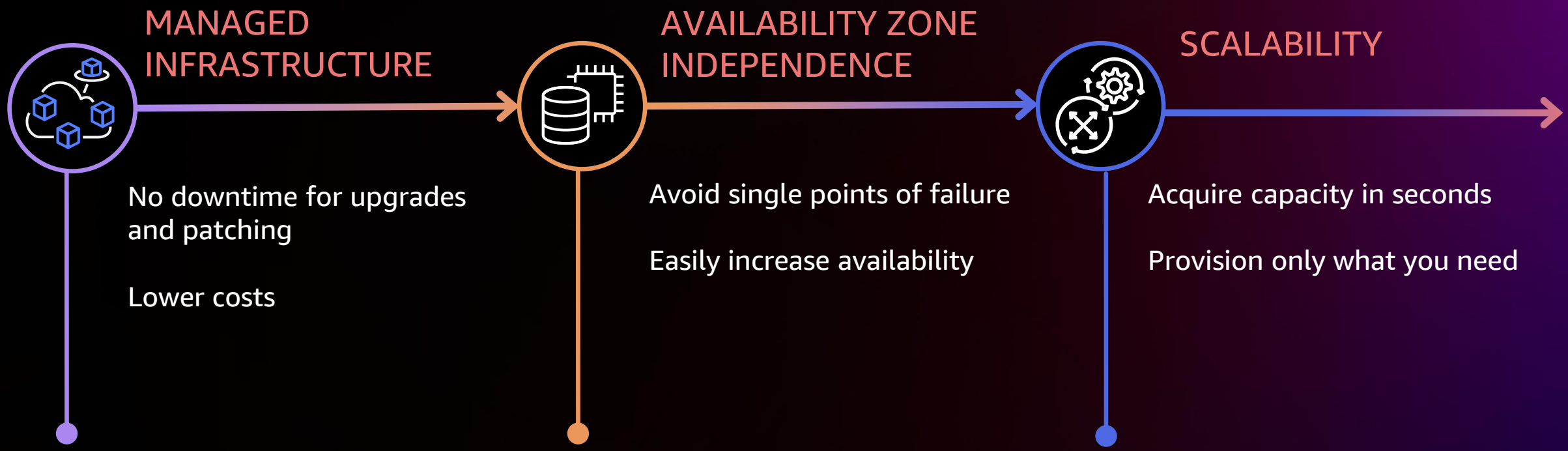
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency in AWS



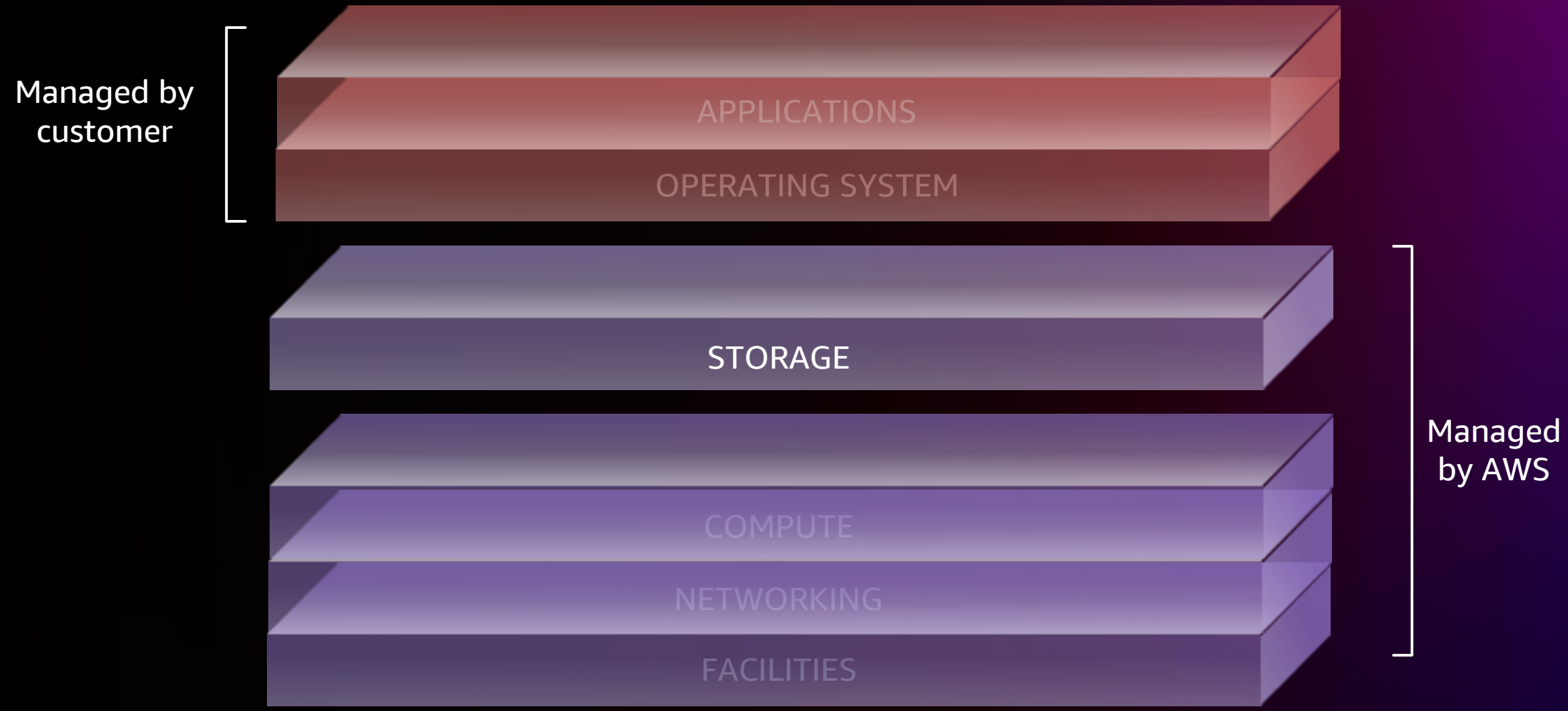
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Resiliency in AWS



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

Resiliency in Amazon EBS



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

Most of you are already using Amazon EBS and you may not even know it

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

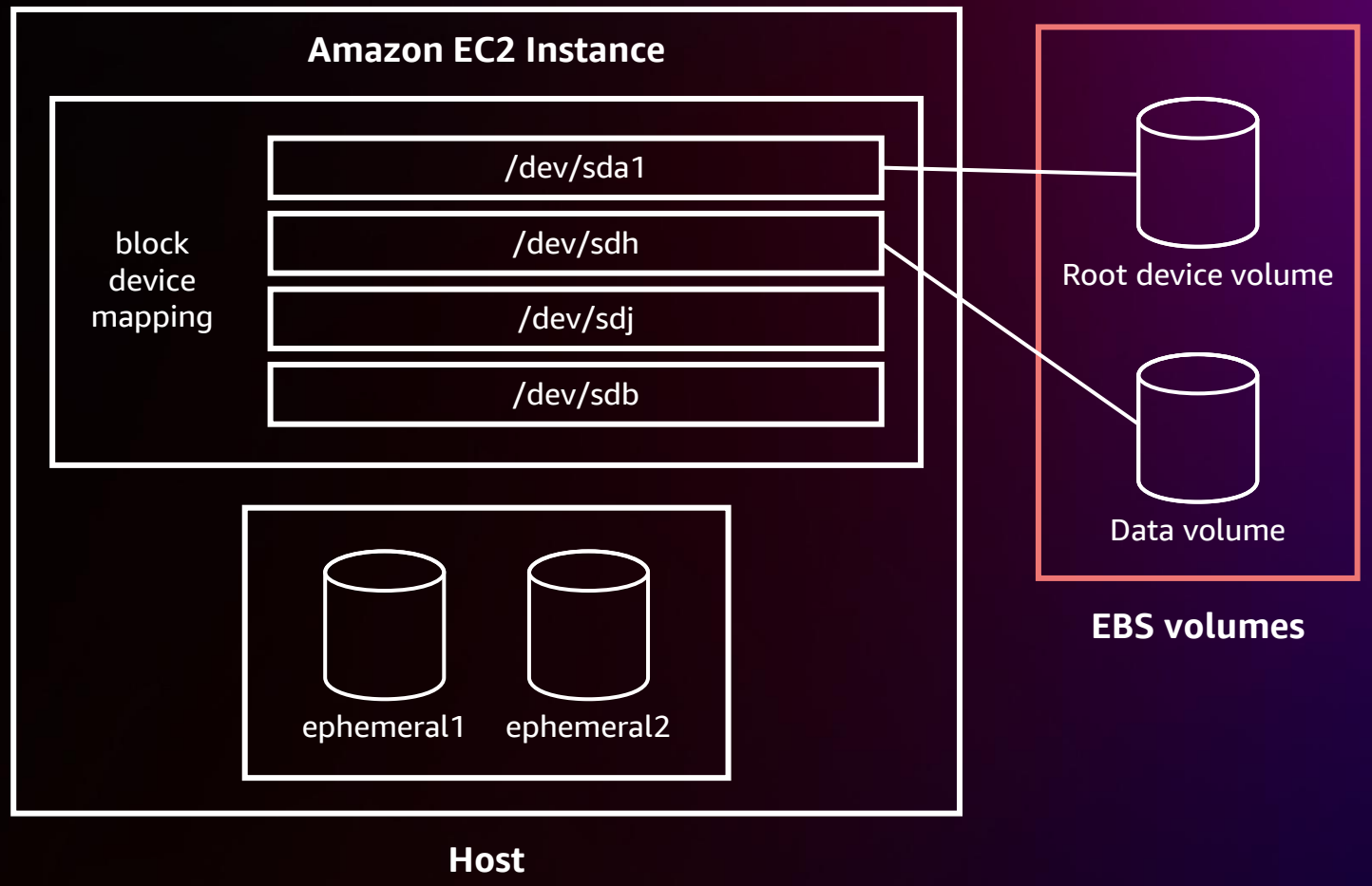
Amazon EBS Overview

Network-attached block storage volumes as a service

Attach to any Amazon EC2 instance in the same Availability Zone

Data volumes and boot volumes (EBS-backed AMIs)

Persistent storage (vs. ephemeral local Instance storage)

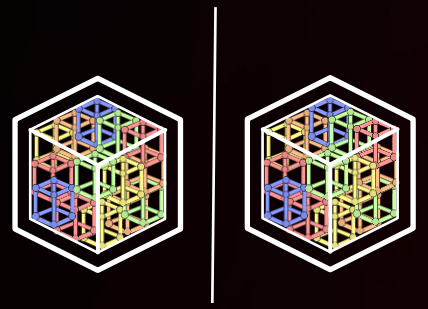


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS built-in resiliency



Built-in redundancy



Fault reduction

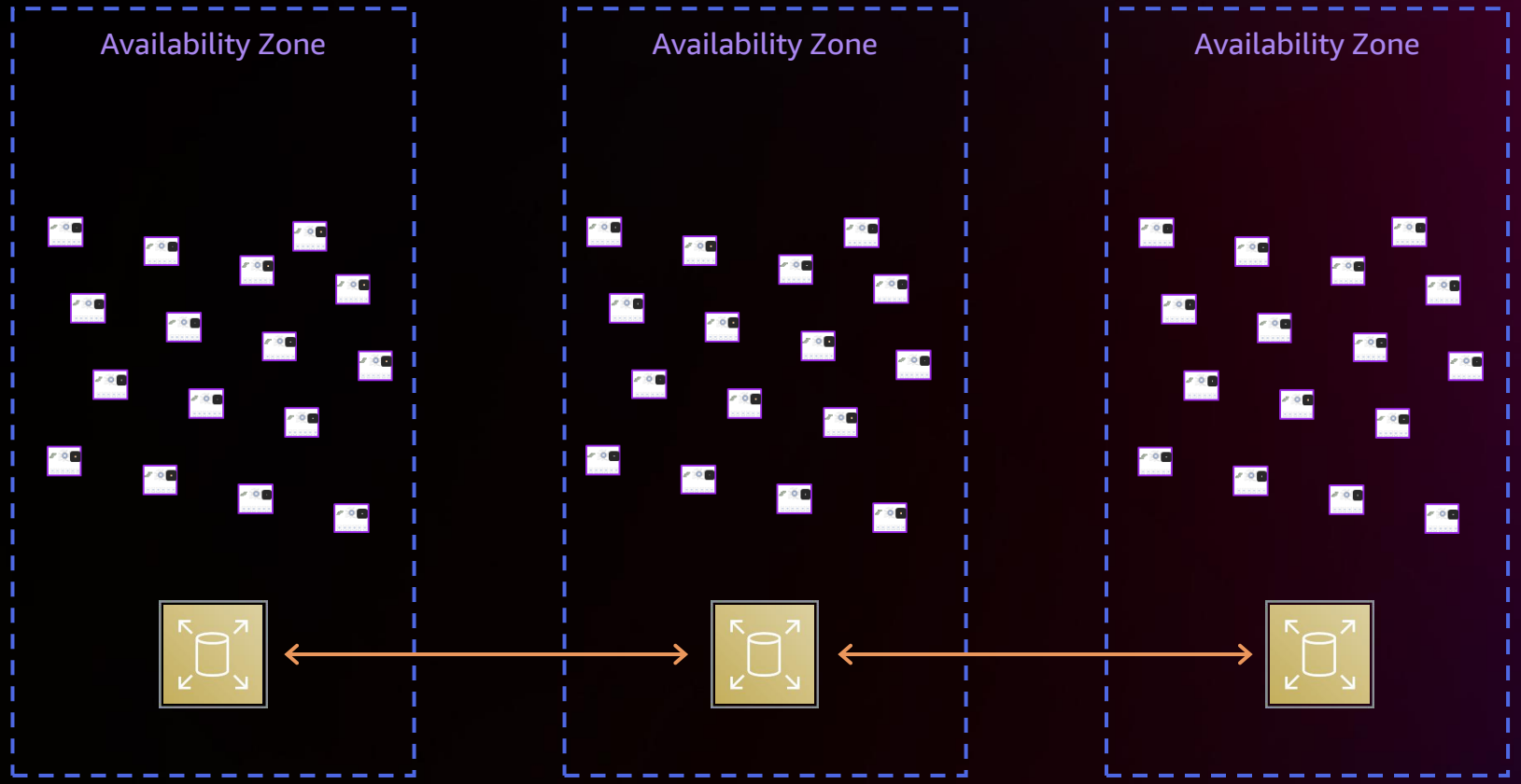


Automated recovery

aws

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

In the beginning



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

Amazon EBS data plane vs. control plane

Control plane

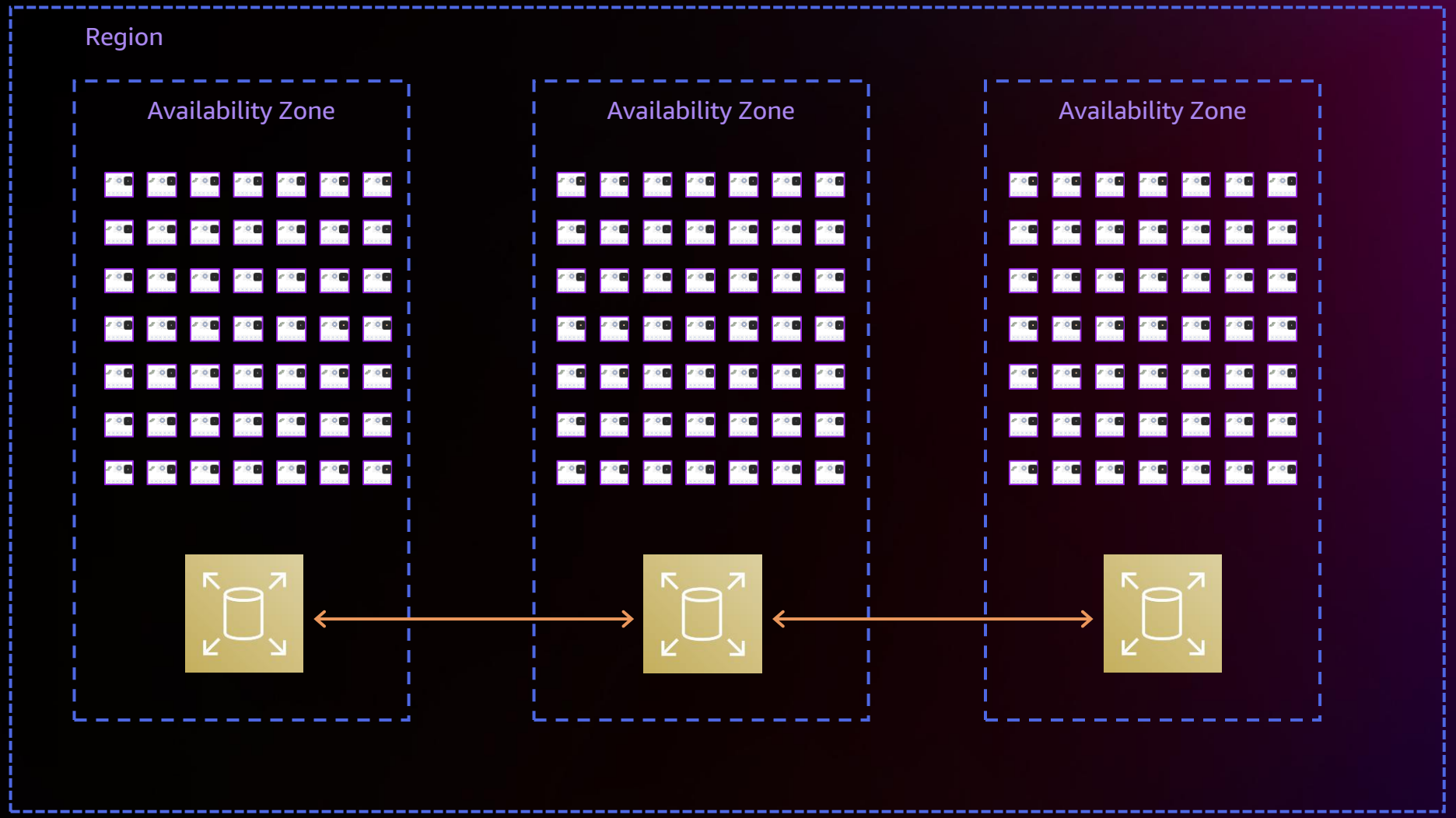
Manage & configure data plane
(create/attach/delete volumes, manage EBS resources)

Data plane

Handles customer data
(read/write bytes, interface to Amazon EC2)

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

Scaling



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

Amazon EBS is designed for

99.999%

service availability

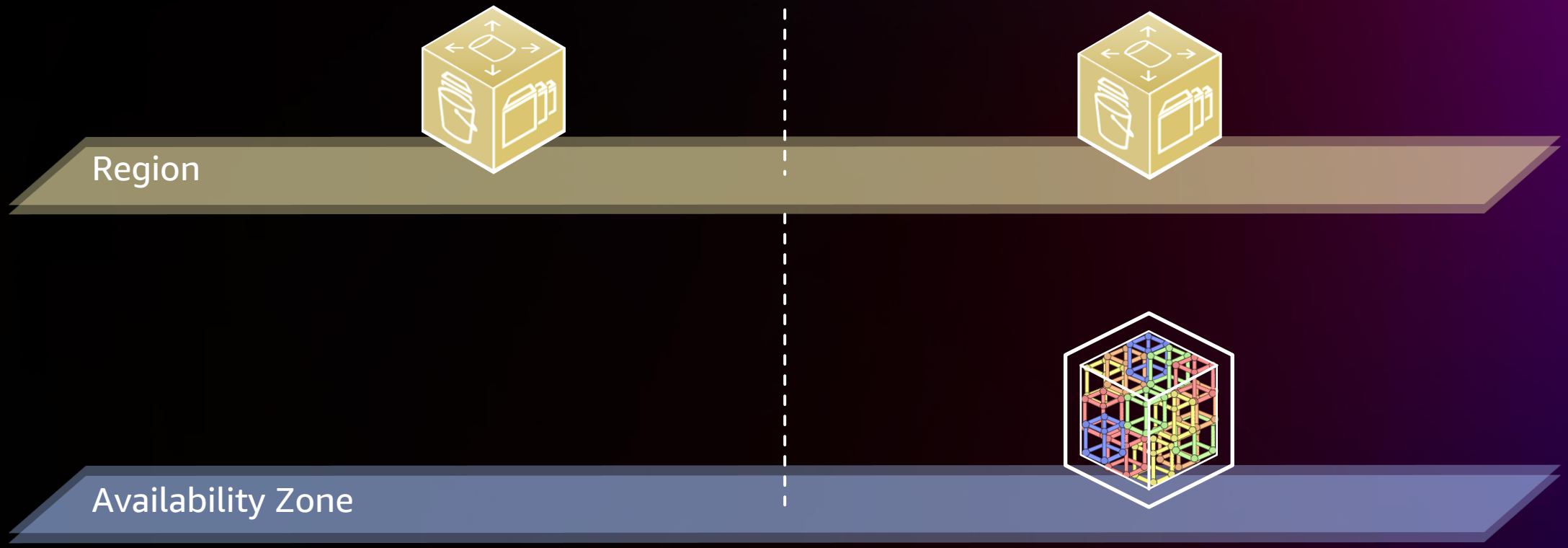
up to

99.999%

durability

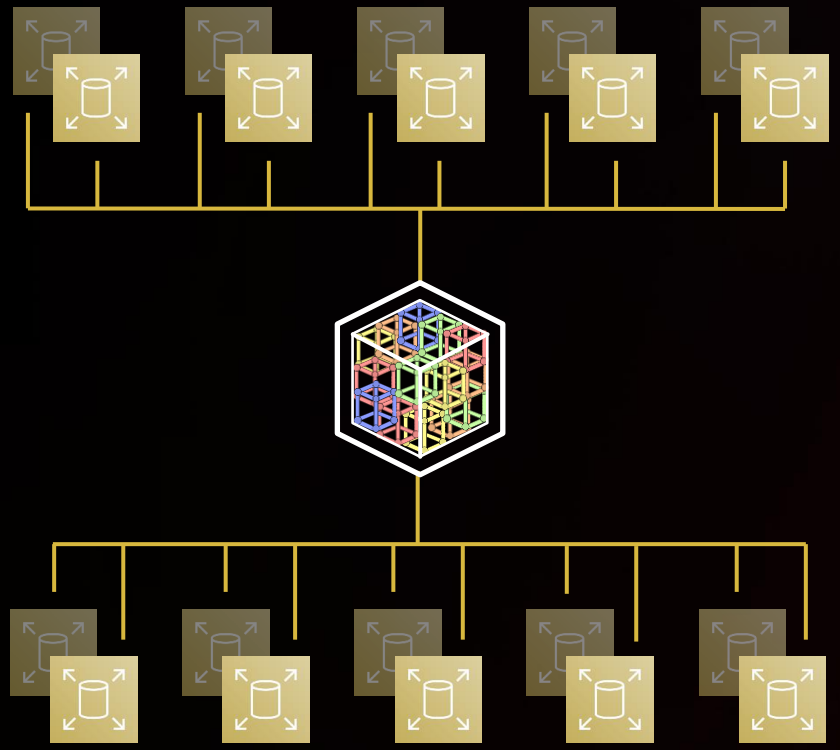
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Amazon EBS fault reduction



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

EBS fault reduction: Configuration manager

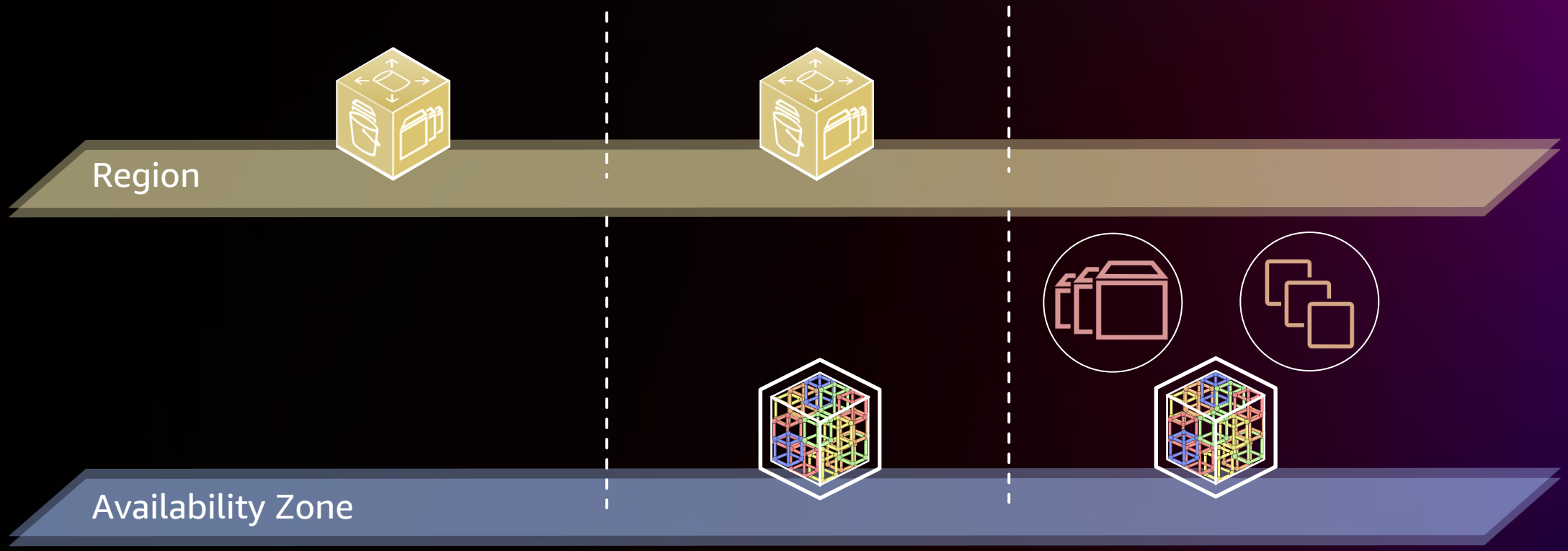


- Authority map for host and volume
- Wholly contained in Availability Zone
- Standalone service
- Paxos-based replication

aws

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

Amazon EBS: AZ independence

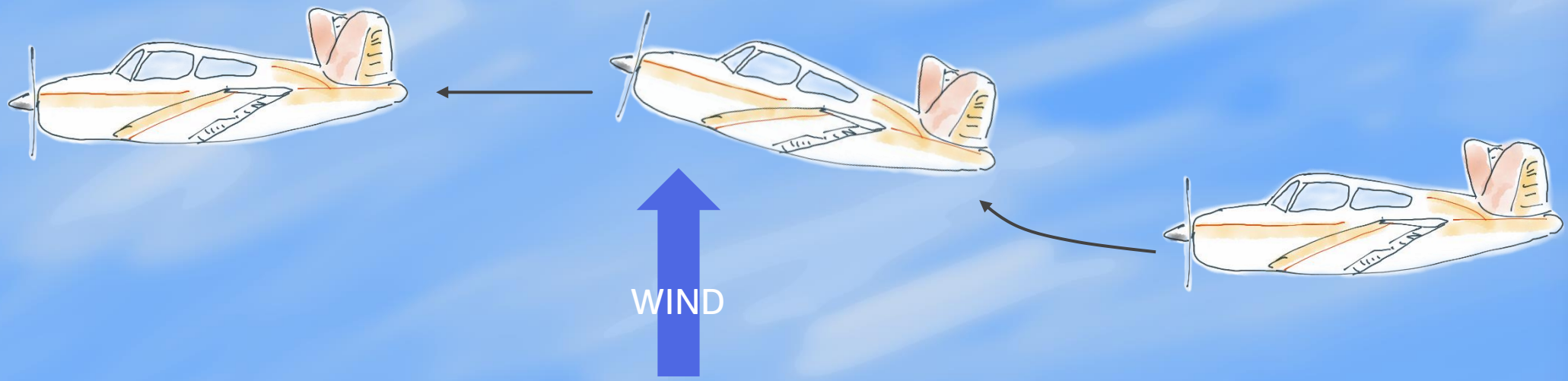


© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Static Stability

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

Static Stability



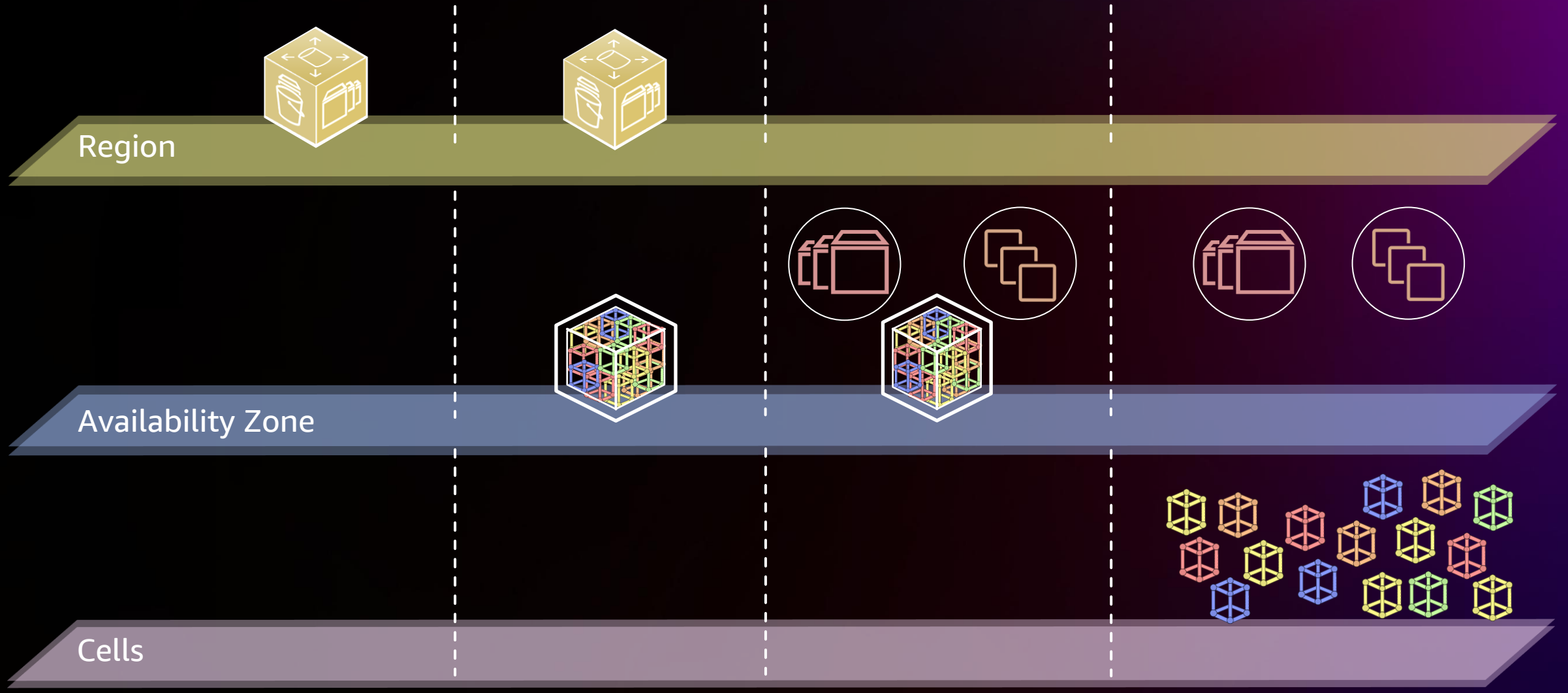
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Static Stability

The ability for systems to return to steady state after small disturbances

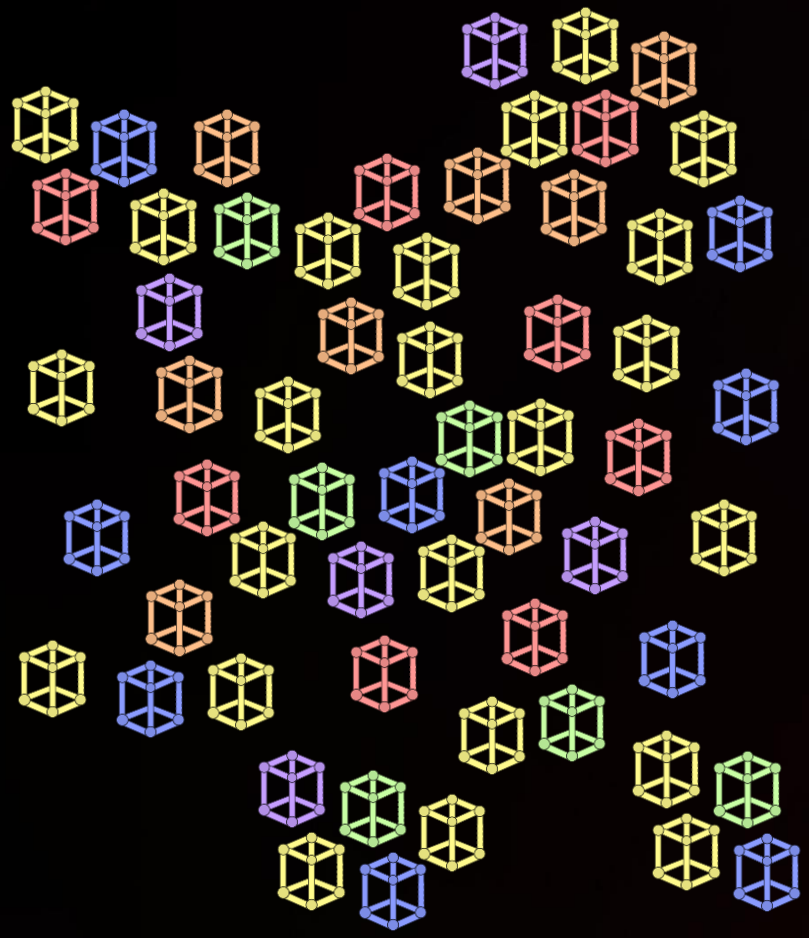
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Physalia



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

Blast radius reduction: Physalia



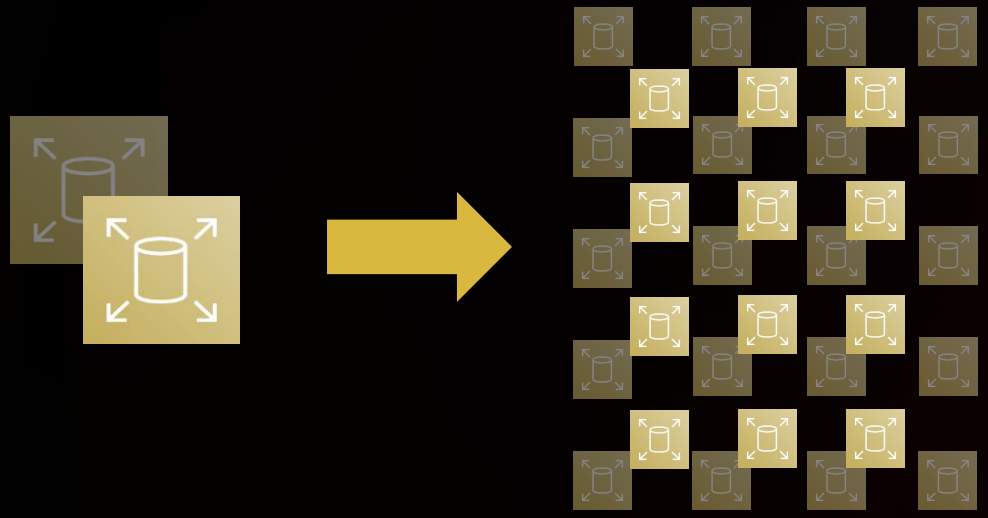
- Small number of clients per database
- Simple to manage
- Cell can reside near clients
- Reduced blast radius
- Each cell is a 7-node Paxos cluster

Learn more:

aws

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

Rethinking Amazon EBS volumes



Split volumes into shards

No longer constrained by individual storage nodes

Faster to replicate in failure

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

Amazon EBS volume repair



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

Amazon EBS volume repair



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

Amazon EBS volume repair



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

Amazon EBS volume repair



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

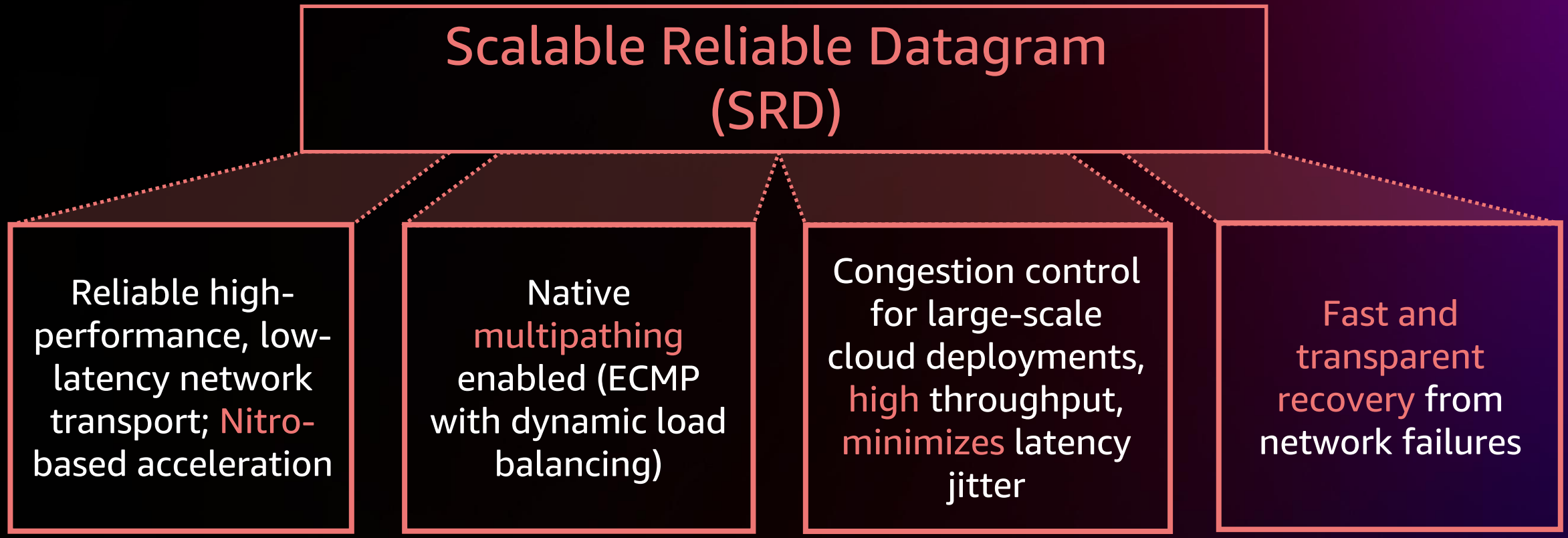
Building a better network protocol



- Difficult to offload in hardware
- Slow to recover in failure

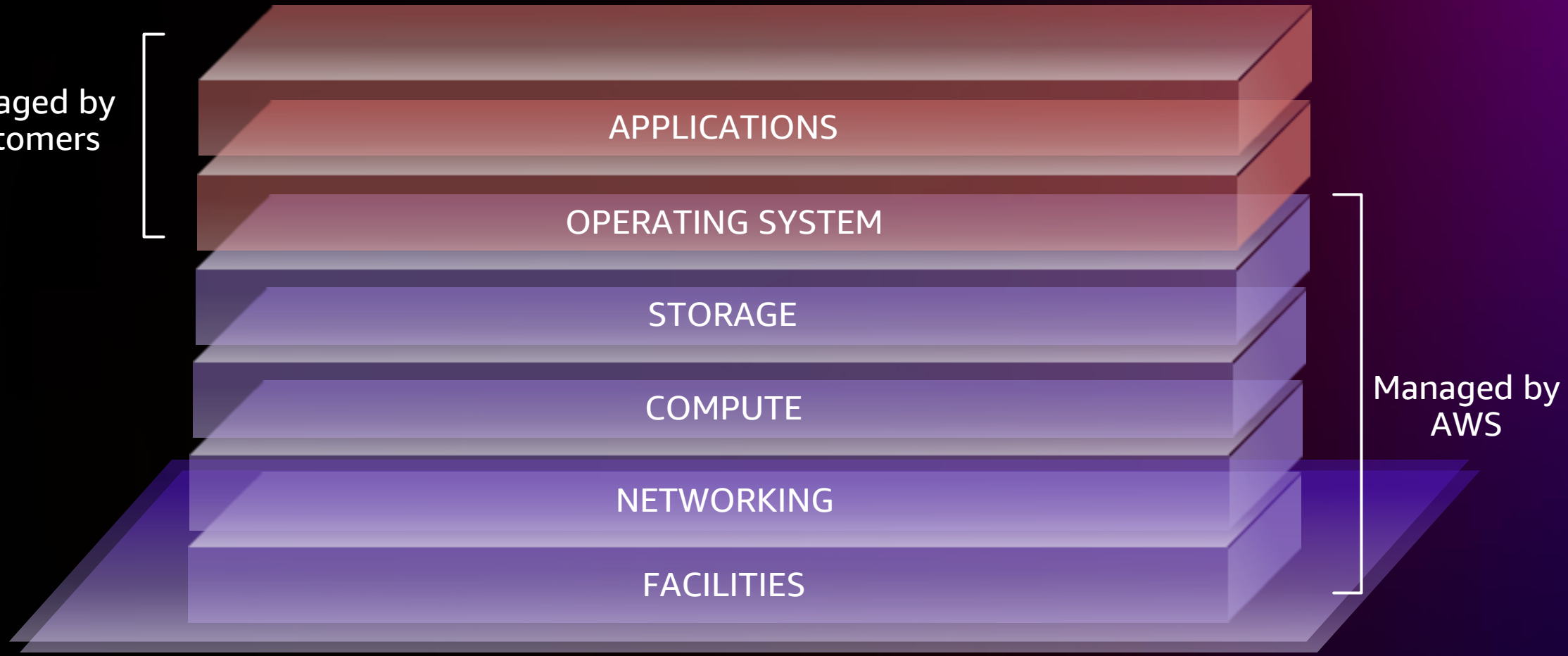
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

SRD Storage Fabric – not just performance



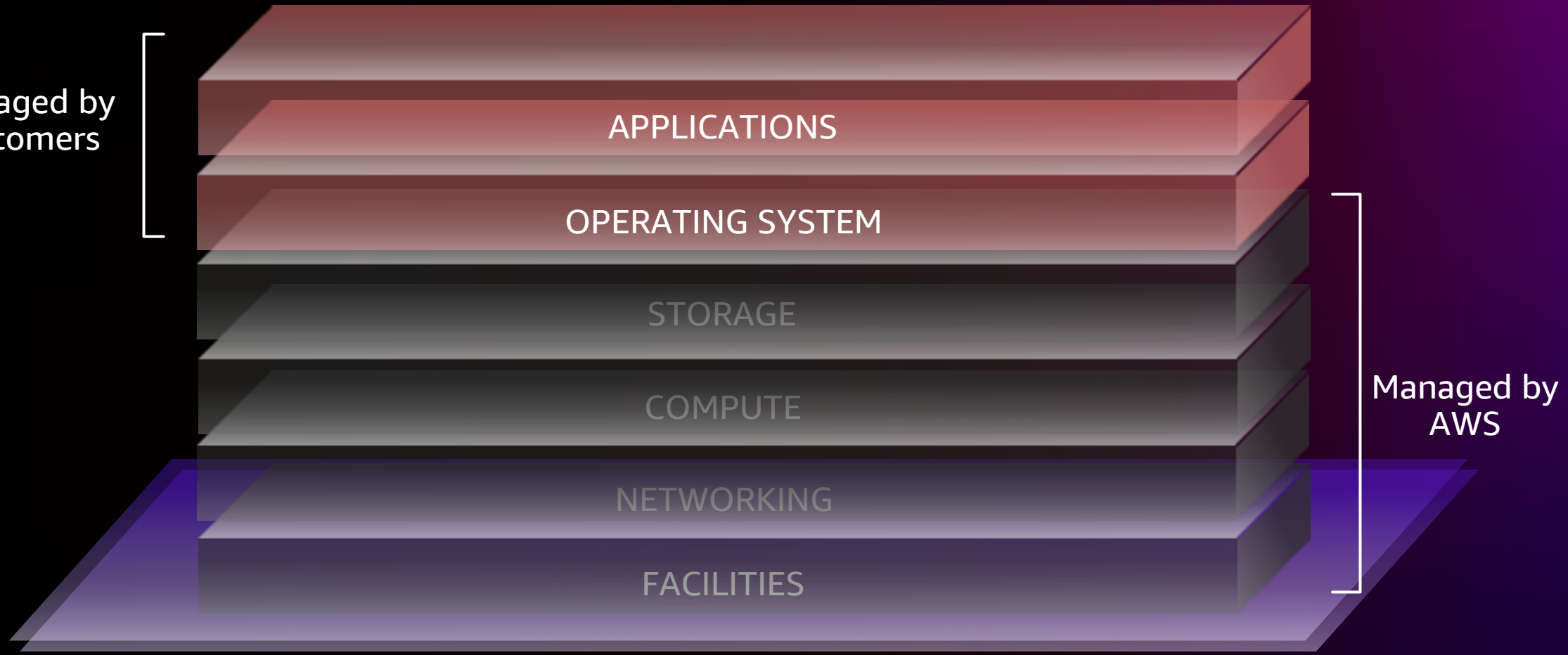
aws
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Take charge of your resiliency



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

Take charge of your resiliency



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

Understand your mission



Would my customers or my business be impacted by degradation or an outage?

Mission critical workloads should run on io2/Block Express

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

Understand your mission



Would my customers or my business be impacted by degradation or an outage?

Mission critical workloads should run on io2/Block Express

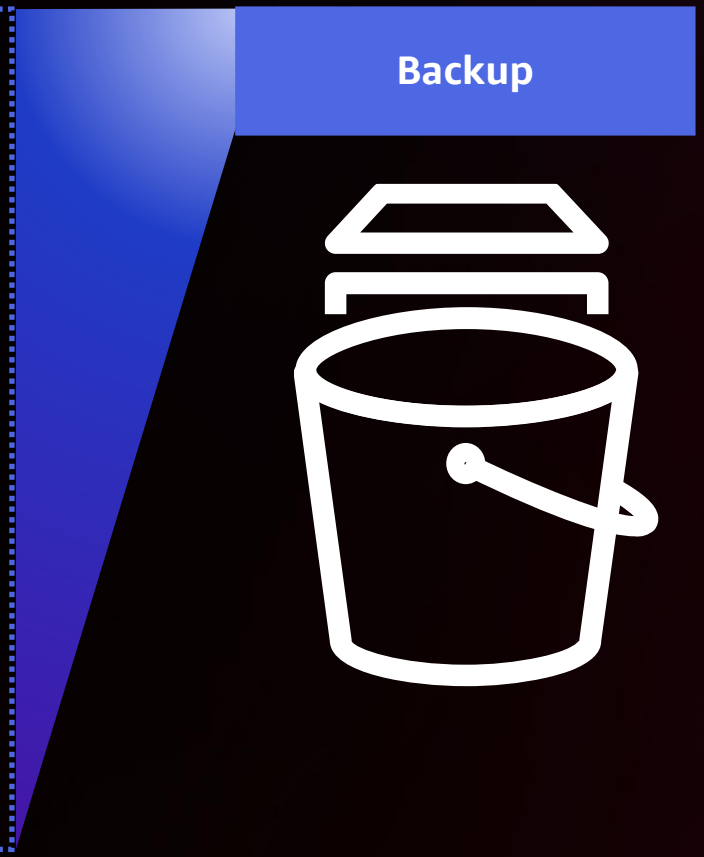
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Back up your EBS volumes with snapshots

Point-in-time copy of EBS volume

Stored in Amazon S3
11 9s of durability

Crash consistent



aws

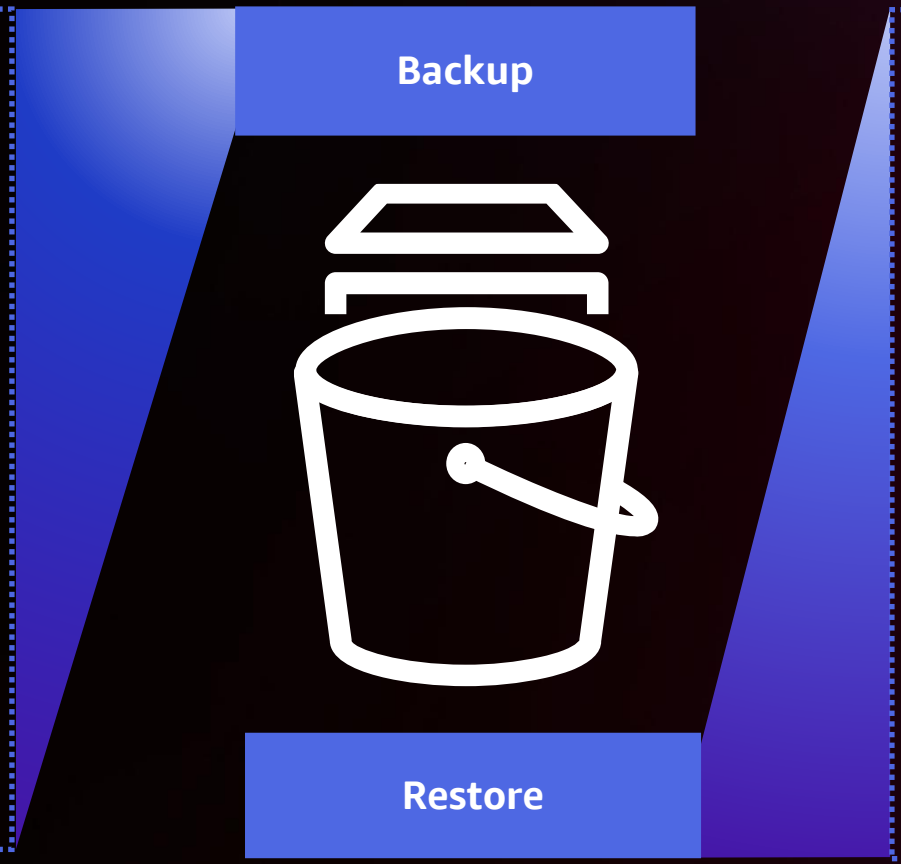
© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Back up your EBS volumes with snapshots

Point-in-time copy of EBS volume

Stored in Amazon S3
11 9s of durability

Crash consistent



Contains all data to recover a volume

Copy volumes within or across Availability Zones for redundancy

Copy volumes to another region for Disaster Recovery

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

Automate backups



Amazon Data Lifecycle Manager (DLM)

Schedule backups and automate lifecycle management for Amazon EBS snapshots and Amazon EBS-backed AMIs



AWS Backup

Automate backup and recovery across multiple storage types including Amazon EBS

aws

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

Build your own redundancy



Avoid RAID1 for redundancy

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

Build your own redundancy



Avoid RAID1 for redundancy

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

Multi-AZ redundancy



- Application-level replication
- OS-level replication (DRBD)
- AWS Elastic Disaster Recovery
- Use snapshots to create volumes across Availability Zones

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

Multi-AZ redundancy



- Application-level replication
- OS-level replication (DRBD)
- AWS Elastic Disaster Recovery
- Use snapshots to create volumes across Availability Zones

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

Monitoring



Amazon CloudWatch Metrics

- Monitor individual volumes
- Monitor volume performance at the Amazon EC2 instance level
- Monitor at the OS layer using custom metrics

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

Monitoring



Amazon CloudWatch Metrics

- Monitor individual volumes
- Monitor volume performance at the Amazon EC2 instance level
- Monitor at the OS layer using custom metrics

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

Testing

Take advantage of the AWS products and services

to validate recovery procedures

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

Testing



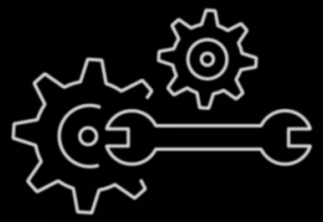
Run tests in a different account

Copy snapshots and create volumes in different accounts

Test continuously as your application changes

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

Recovery



Define thresholds to trigger recovery workflows

Automate recovery

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

Recovery



CloudWatch Alarms
Define recovery triggers



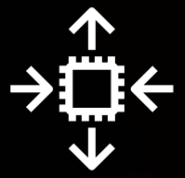
Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



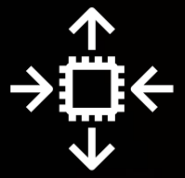
Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Recovery



CloudWatch Alarms
Define recovery triggers



Pre-provision capacity
Static stability



Amazon EC2 auto-recovery
Trigger on CloudWatch alarms



Disaster Recovery
Copy snapshots to another Region



AWS Auto Scaling groups
Health check replacements



Fast Snapshot Restore
6x lower recovery time objective

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

Have a failover plan



How long can you afford to wait?

Make the decision upfront

Separate your recovery from our recovery

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

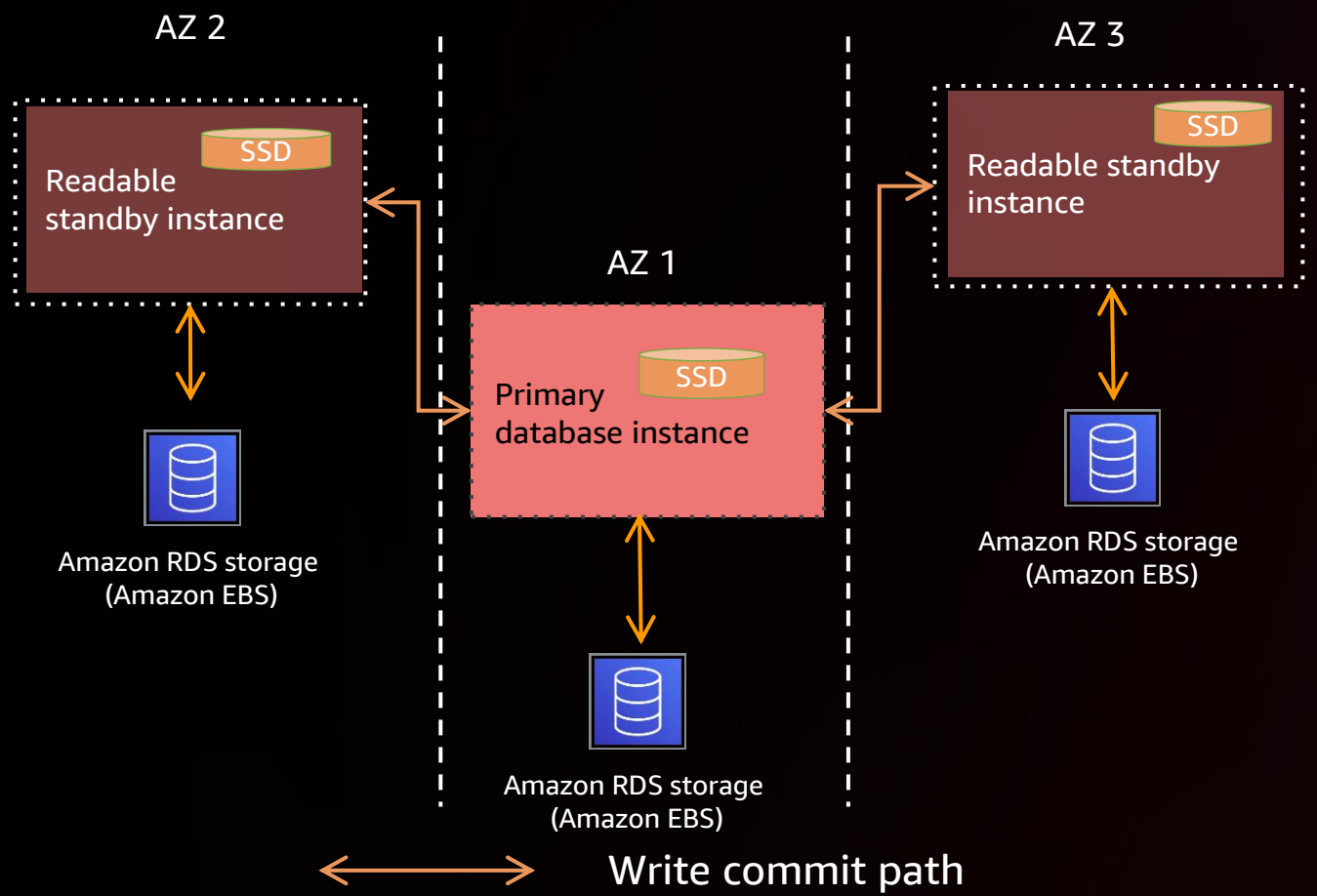
Real-world examples

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

Real-world examples

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

Amazon RDS Multi-AZ



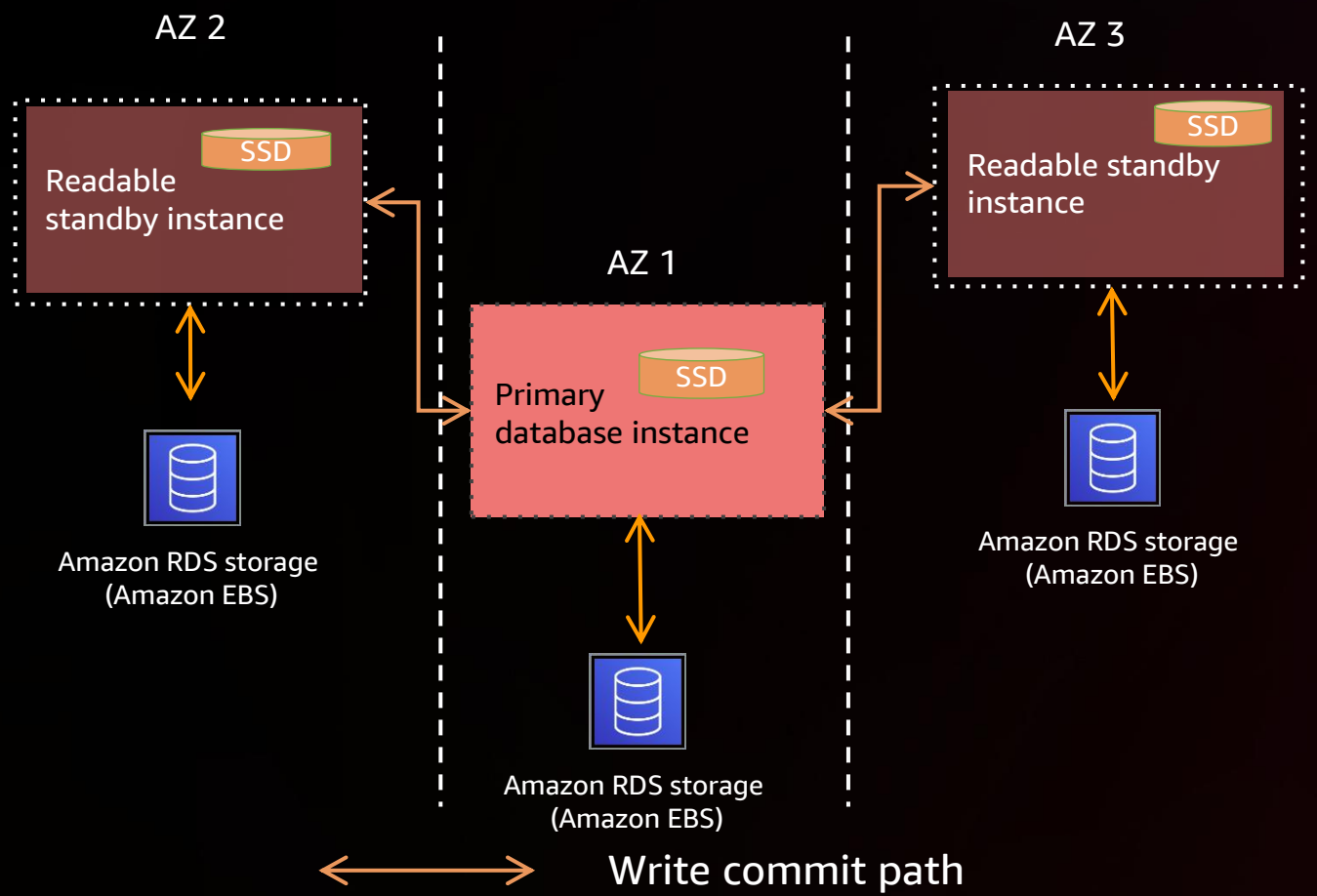
Commits writes on primary only after first standby acknowledges writing to SSD

Moves data asynchronously to Amazon EBS for durability

Serves reads from cache or from Amazon EBS

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

Amazon RDS Multi-AZ



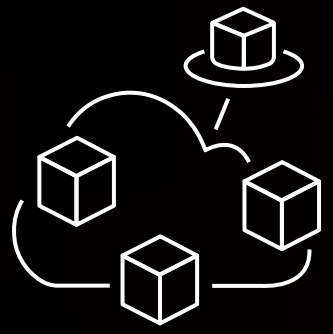
Commits writes on primary only after first standby acknowledges writing to SSD

Moves data asynchronously to Amazon EBS for durability

Serves reads from cache or from Amazon EBS

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

Lift-and-shift back office system



Availability Zone as failure domain

Snapshots to set restore points for different AZs or Regions

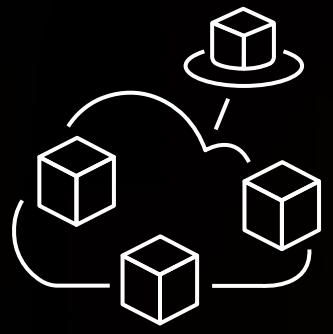
Block-level replication (DRBD) for applications that don’t have built-in replication

Recovery tools like Amazon EC2 auto recovery

aws

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

Lift-and-shift back office system



Availability Zone as failure domain

Snapshots to set restore points for different AZs or Regions

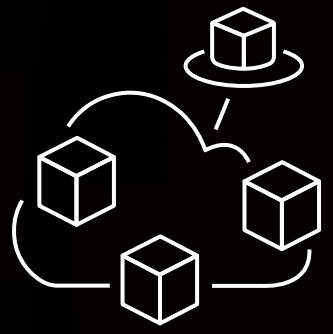
Block-level replication (DRBD) for applications that don’t have built-in replication

Recovery tools like Amazon EC2 auto recovery

aws

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

Lift-and-shift back office system



Availability Zone as failure domain

Snapshots to set restore points for different AZs or Regions

Block-level replication (DRBD) for applications that don’t have built-in replication

Recovery tools like Amazon EC2 auto recovery

aws

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

If you remember nothing else . . .

- Define your own availability and recovery plan
  - What is your threshold for an unresponsive I/O?
  - When should your application time out?
  - Be willing to fail over
  - Test your failover workflows

aws

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

Thank you!

Cami Tavares
@camismusings

Marc Olson
@molson



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

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