
aws
SUMMIT
INDIA | MAY 25, 2023

SECR007

How Cisco achieved multi-region resilience for their learning platform with Amazon EKS

Jayesh Kumar Tank
Senior Cloud Architect
AWS Proserve India LLP

Raja Soundaramourty
Engineering Leader & Cybersecurity Officer - Applications and Platform
Cisco

Agenda

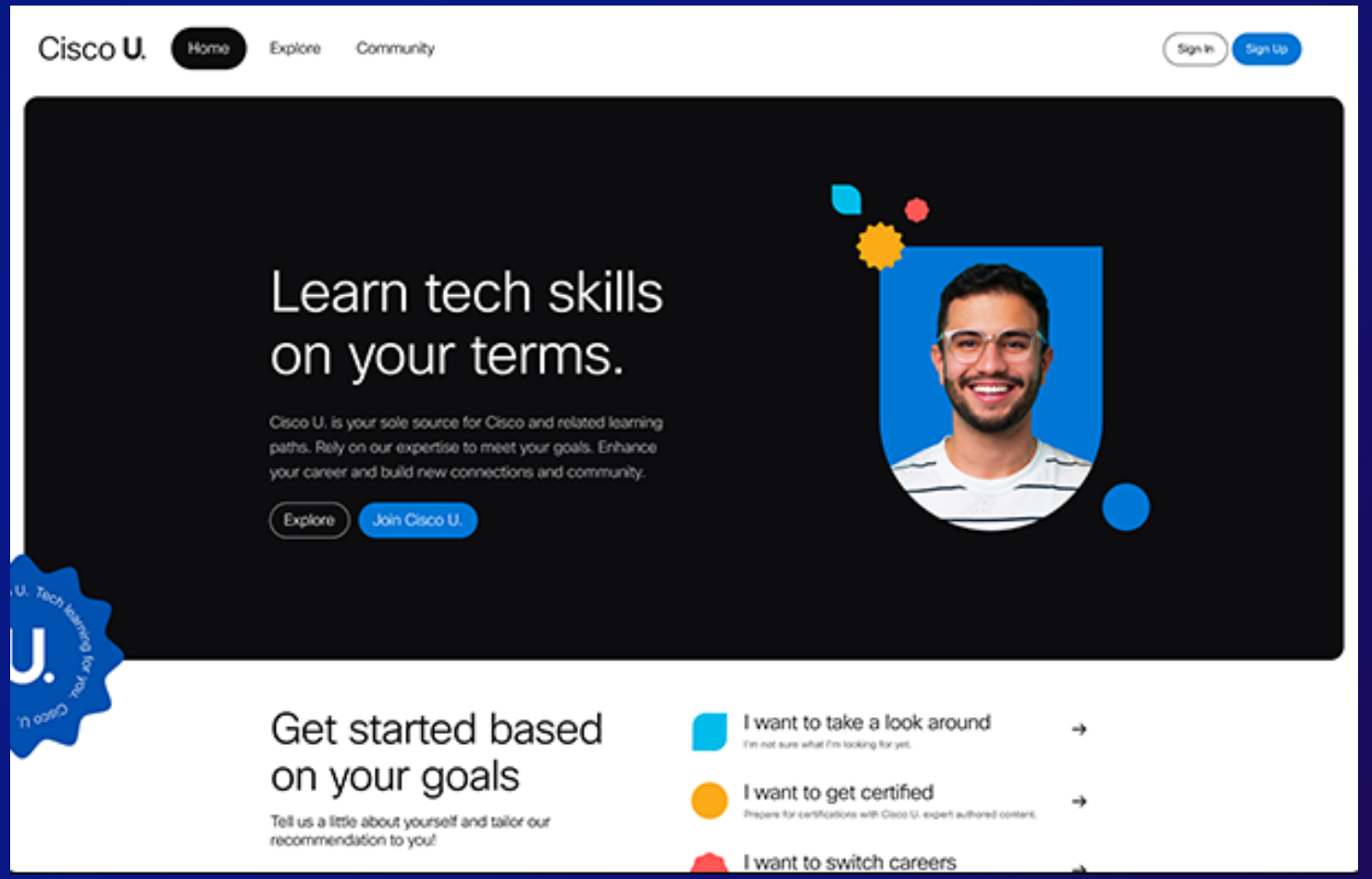
- Cisco U. learning and certification platform
- Challenges and opportunities
- Resilience introduction
- Architecture : Amazon EKS and Amazon Aurora Global Cluster
- Journey to multi-region resilient infrastructure
- Learnings and roadmap

Cisco U. : Tech learning shaped to you

New Digital Learning Experience

A digital learning experience build around the learner

- Goal based Learning Paths
- Solution oriented learning experience
- AI driven recommendations and personalization
- Solving multi-vendor environment learning expectations
- Driven by our community of 1M+ learners



Success criteria

- Security first
- Operate at Scale
- Cost optimized based on utilization
- Operational efficiency with 100% automation
- Resiliency (Availability & Disaster Recovery) of workloads
- Uncompromised learner experience

Our journey

- About resiliency
  - Exponentially costly
  - Considered as pre-mature optimization
  - Requires significant efforts

Myth

Our key learnings

- About resiliency
  - NOT Exponentially costly
  - NOT pre-mature optimization
  - NOT Requires significant efforts

Resilience

Resilience in a nut shell

Resistance to common failures through design and operational mechanisms

+

Returning to operations within specific targets for more rare but highly impactful failures

HA (High Availability)

measured in 9's

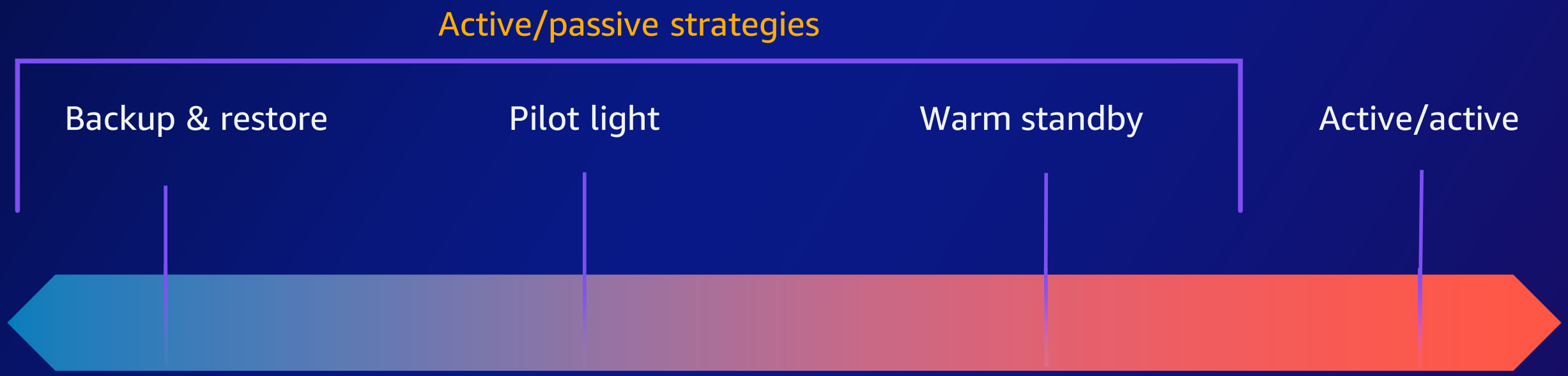
DR (Disaster Recovery)

RTO · RPO

Continuous Improvement

CI/CD, Code Refinement, Operational Testing, Observability/Monitoring

Strategies for disaster recovery



RPO / RTO: Hours

- Lower-priority use cases
- Provision all AWS resources after event
- Restore backups after event
- Cost $

RPO / RTO: 10s of minutes

- Data live
- Services idle
- Provision some AWS resources and scale after event
- Cost: $$

RPO / RTO: Minutes

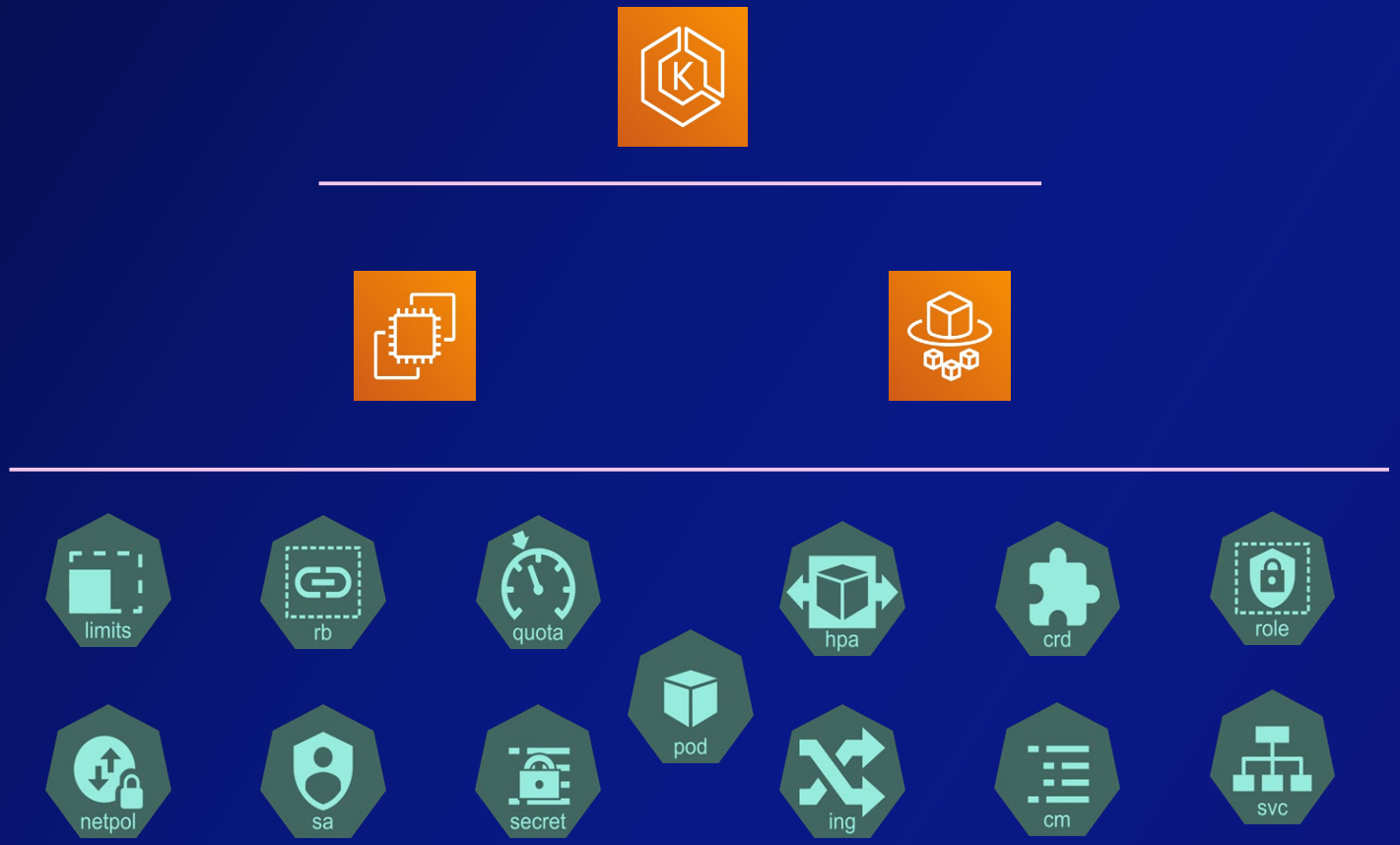
- Always running, but smaller
- Business critical
- Scale AWS resources after event
- Cost $$$

RPO / RTO: Real-time

- Zero downtime
- Near-zero data loss
- Mission Critical Services
- Cost $$$$

Resilience with Amazon EKS

Amazon EKS architectural considerations

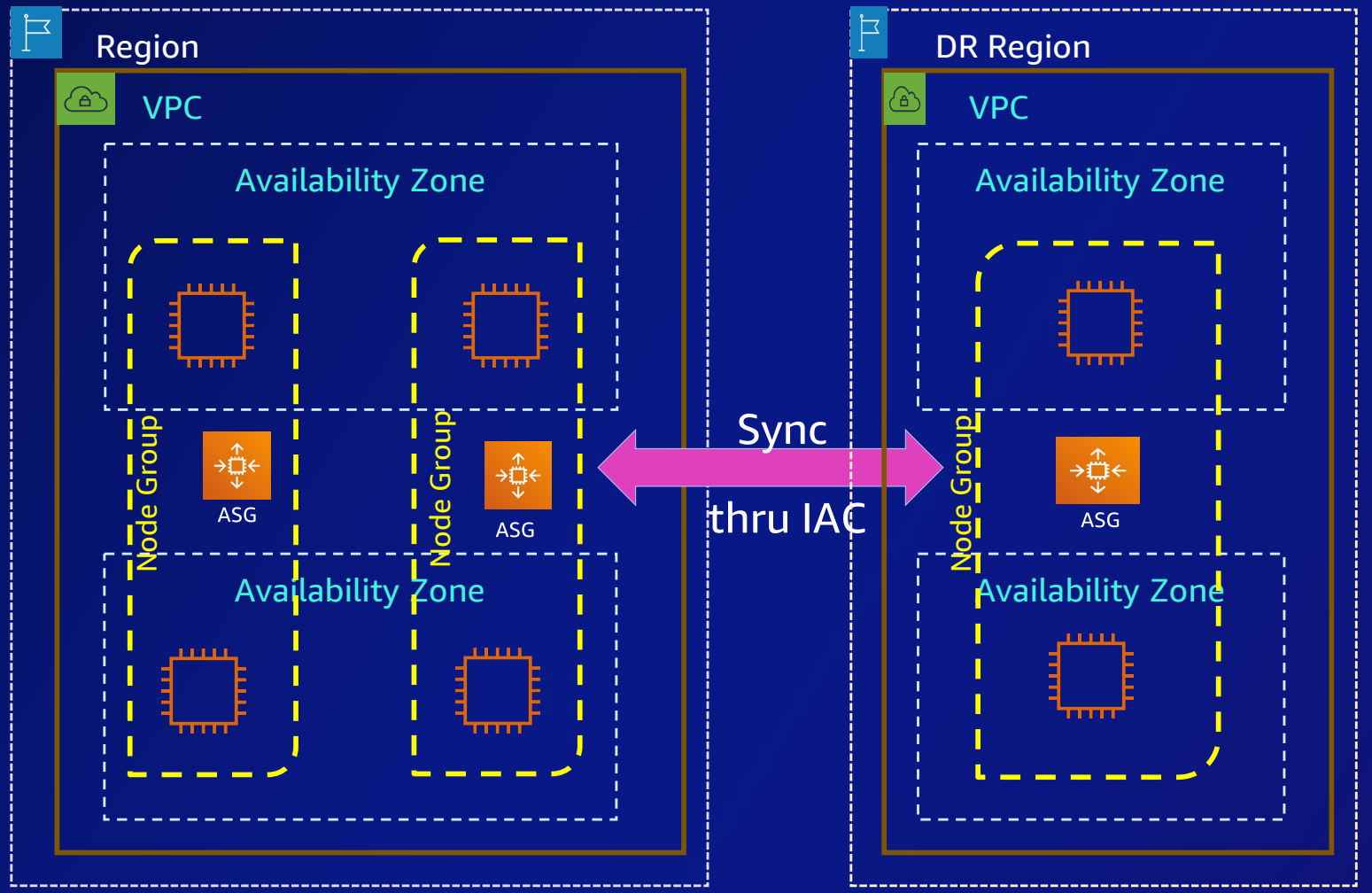


Control Plane, managed by AWS → Active-Active Control Plane : Cross region

Compute, managed by Customer → Reduced number of nodes in DR cluster

K8s objects, managed by Customer → App Deployment on DR cluster (after validation)

Node groups – Warm standby



Terraform

RTO in minutes

Minimal nodes in DR node groups

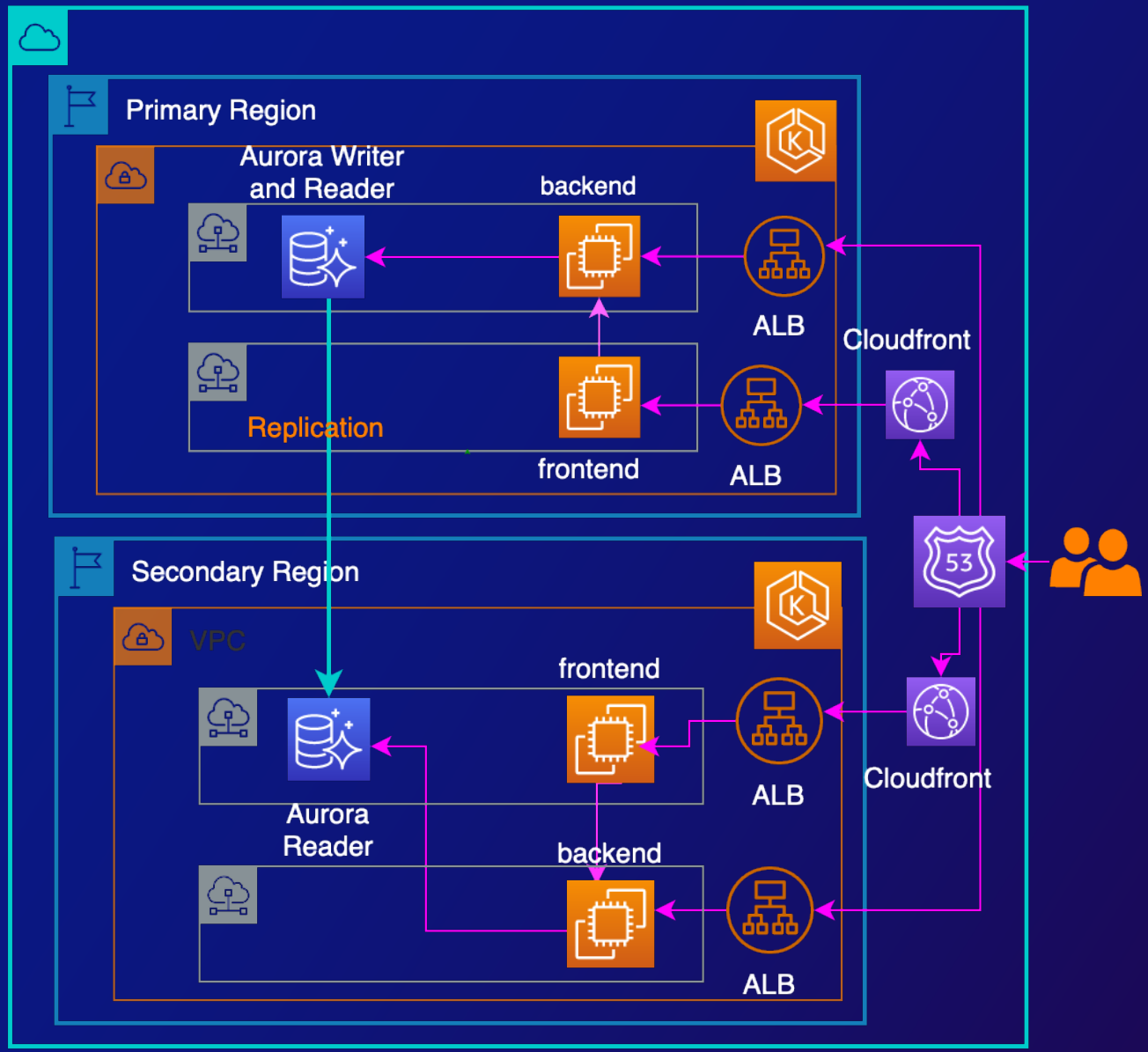
Minimal application footprint in DR region

Infrastructure Pipelines + IAC

Solution architecture

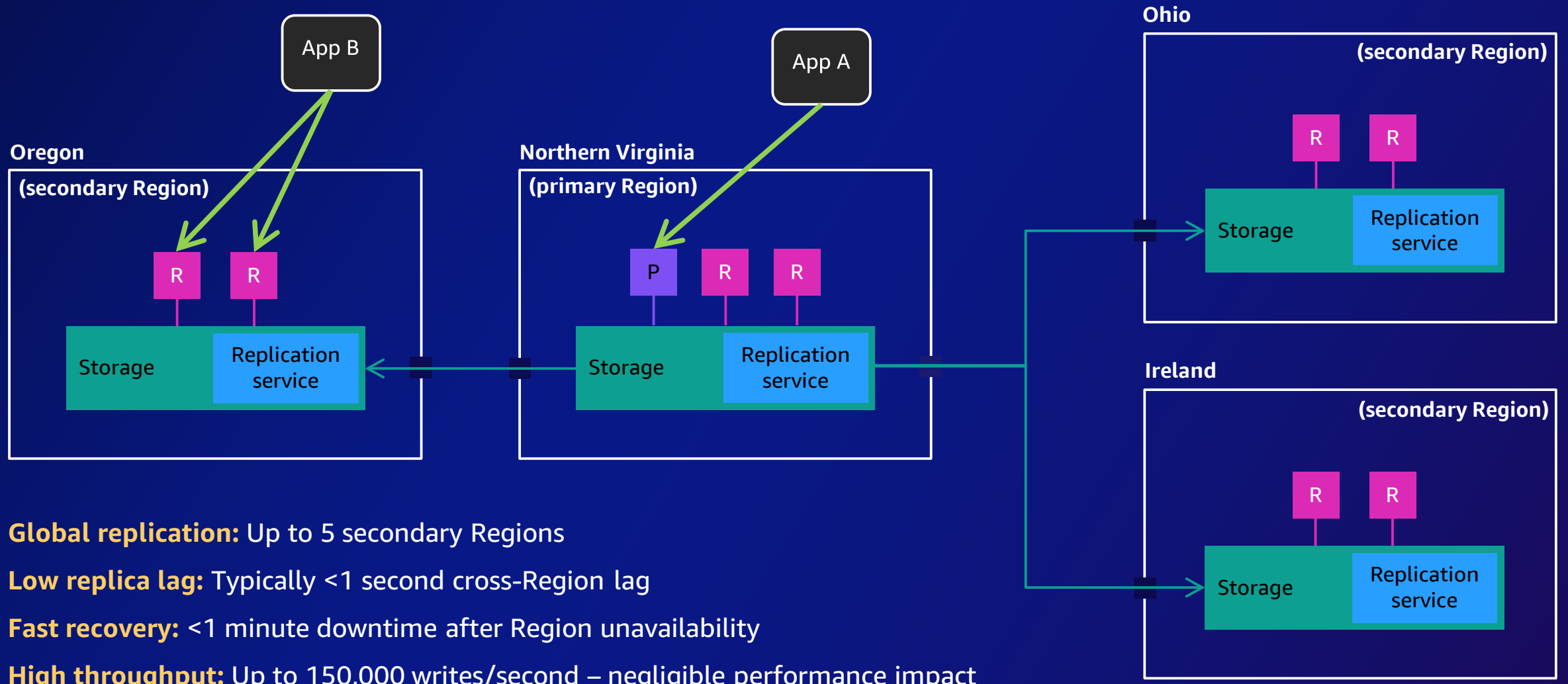
Cisco U.

- Active-Warm standby Clusters
- Amazon Aurora Global database for faster DR needs
- Amazon Route 53 as routing layer
- Continuous deployment on DR EKS (post validation on the primary)
- Automated Secret replication and Amazon Cognito sync across regions
- Centralized observability across clusters via Amazon Managed service for Prometheus and Amazon managed service for Grafana



Database resiliency

Amazon Aurora global database



Global replication: Up to 5 secondary Regions

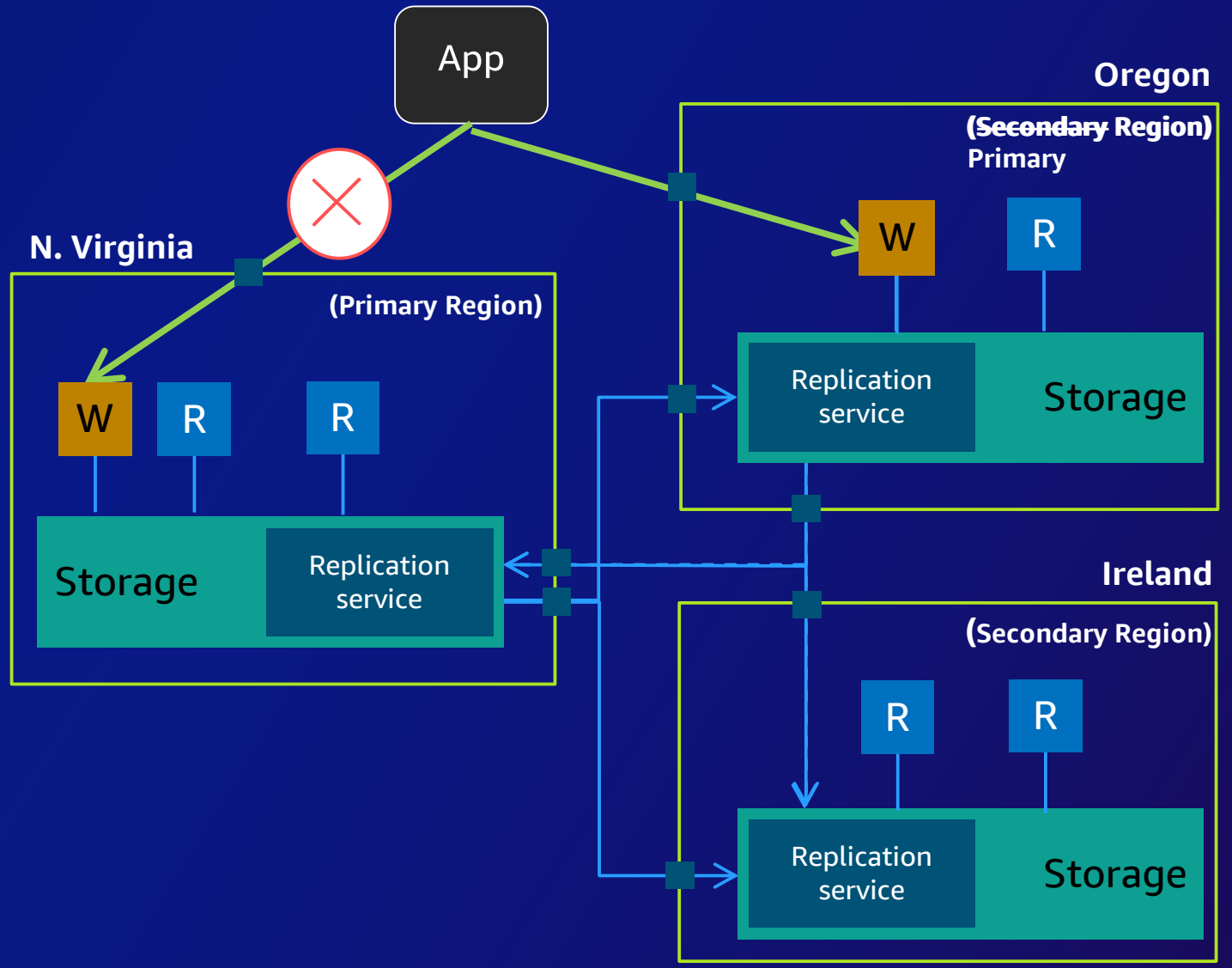
Low replica lag: Typically <1 second cross-Region lag

Fast recovery: <1 minute downtime after Region unavailability

High throughput: Up to 150,000 writes/second – negligible performance impact

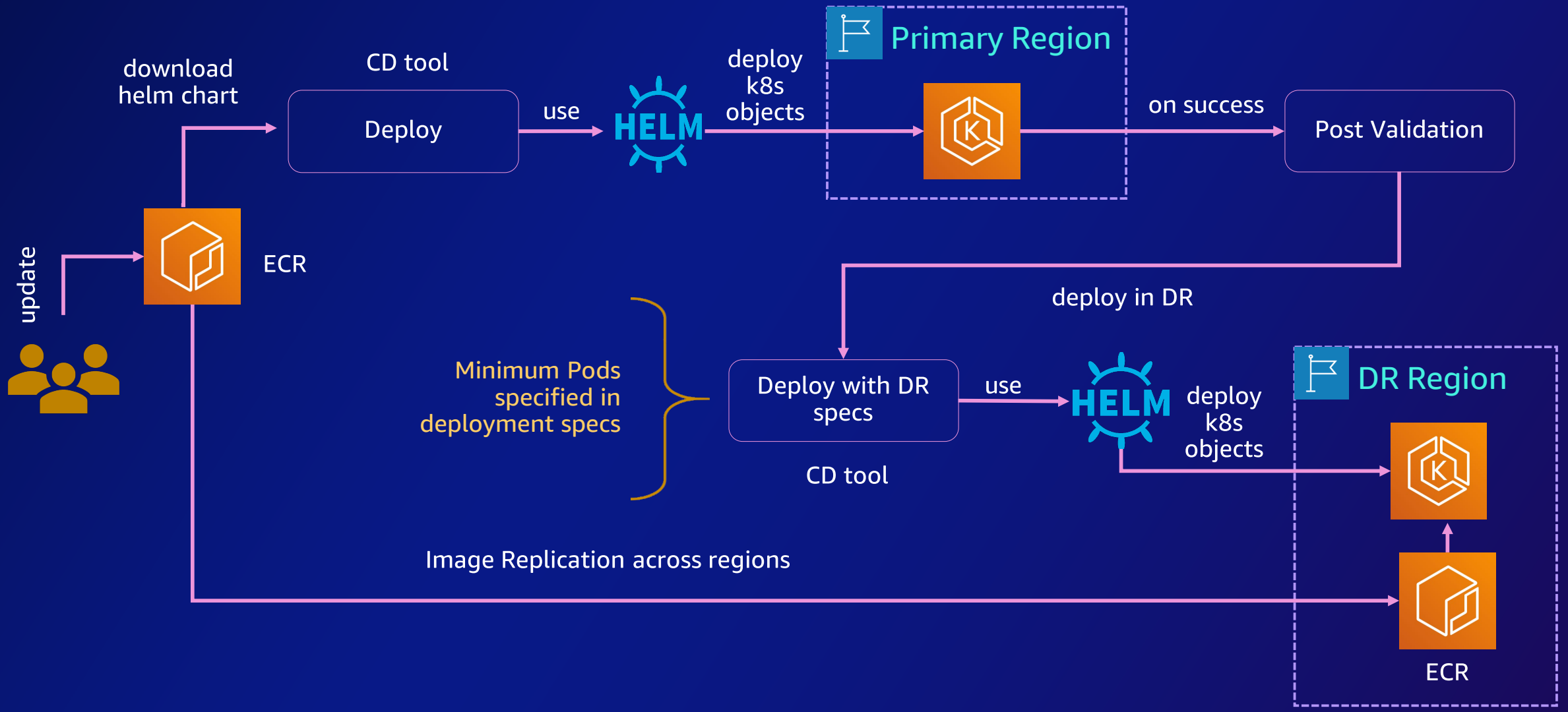
DB Region disaster scenario

- Entire DR flow is automated via lambda and Terraform
- An outage dictates decision to failover
- Identify Region with least replication lag
- Detach and promote chosen Region to be a “standalone” cluster
- Example: Oregon becomes primary
- Once up, application can point to the new endpoint
- Delete stranded clusters in other Regions
- Rebuild secondary Regions when needed/available; fail-back using managed planned failover



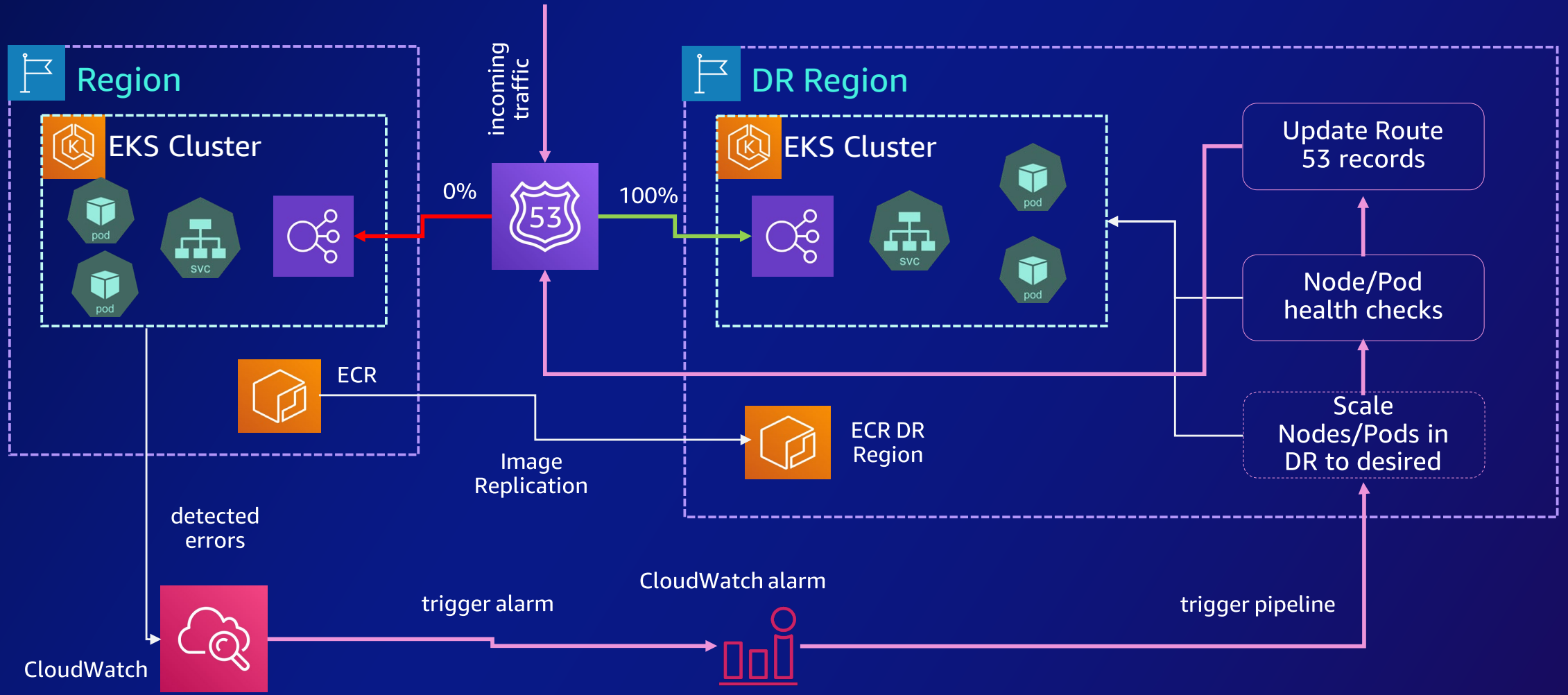
Disaster recovery for K8s objects

Cisco U. application rollout



Switching to DR region

Switching to DR region



Learnings

Avoid control plane operations for recovery strategies

AWS IAM

What will work	What may not work
IAM Policies will continue to be evaluated	CRUDL IAM policies

Amazon Route 53

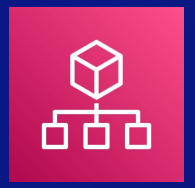
DNS resolution and health checks	Updates to routing policies

Route 53 Application recovery controller

Changes to routing controls	CRUDL routing controls

Amazon CloudFront

What will work	What may not work
Will continue to cache and serve content	CRUDL CloudFront distributions



AWS Organizations

Service Control Policies (SCP)	View or update organization structure

AWS Global Accelerator

Edge routing will continue to function	Add/modify endpoints

Key Takeaways

- Automation and IaC is the key, DR drills are very important
- Images and Secrets needs to be replicated in DR region
- Failover and failback automation should be hosted in DR region
- EKS Cluster and add-on upgrades should be validated in silos
- Final RPO numbers would be determined by monitoring replication lag on aurora secondary regions
- Observability stack should be hosted in a centralized account and should have aggregated data points from both clusters
- Fail back strategy is essential too

Roadmap

skillbuilder.aws

Your time is now

Build in-demand cloud skills your way

Thank you!

Please complete the session survey

Jayesh Kumar Tank
Senior Cloud Architect
AWS Proserve India LLP

Raja Soundaramourty
Engineering Leader & Cybersecurity Officer - Applications and Platform
Cisco