AWS re:Invent

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

FSI310

Fannie Mae: Migrating at scale without lifting and shifting

Ramon Richards
Chief Information Officer (CIO)
Fannie Mae

Satya Addagarla
VP, Lender & Servicer Technology & Enterprise Cloud Migration
Fannie Mae

Harsha Nippani
Principal Solutions Architect
Amazon Web Services

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

Agenda

Fannie Mae’s strategic objectives

Cloud strategy

Cloud migration journey

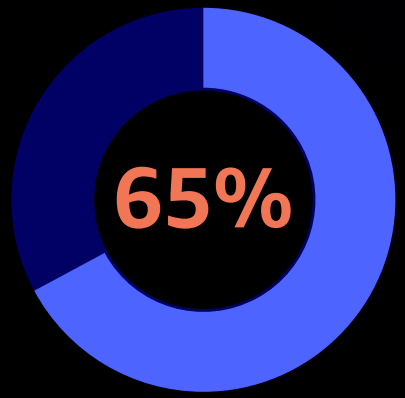
Business values realized and points to ponder

Technical patterns

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

Fannie Mae, America's most valued housing partner

Our mission: to facilitate equitable and sustainable access to homeownership and quality affordable rental housing across America



- ✓ Homeownership in United States
- ✓ ~$1.4T liquidity in 2020



~1 in 4

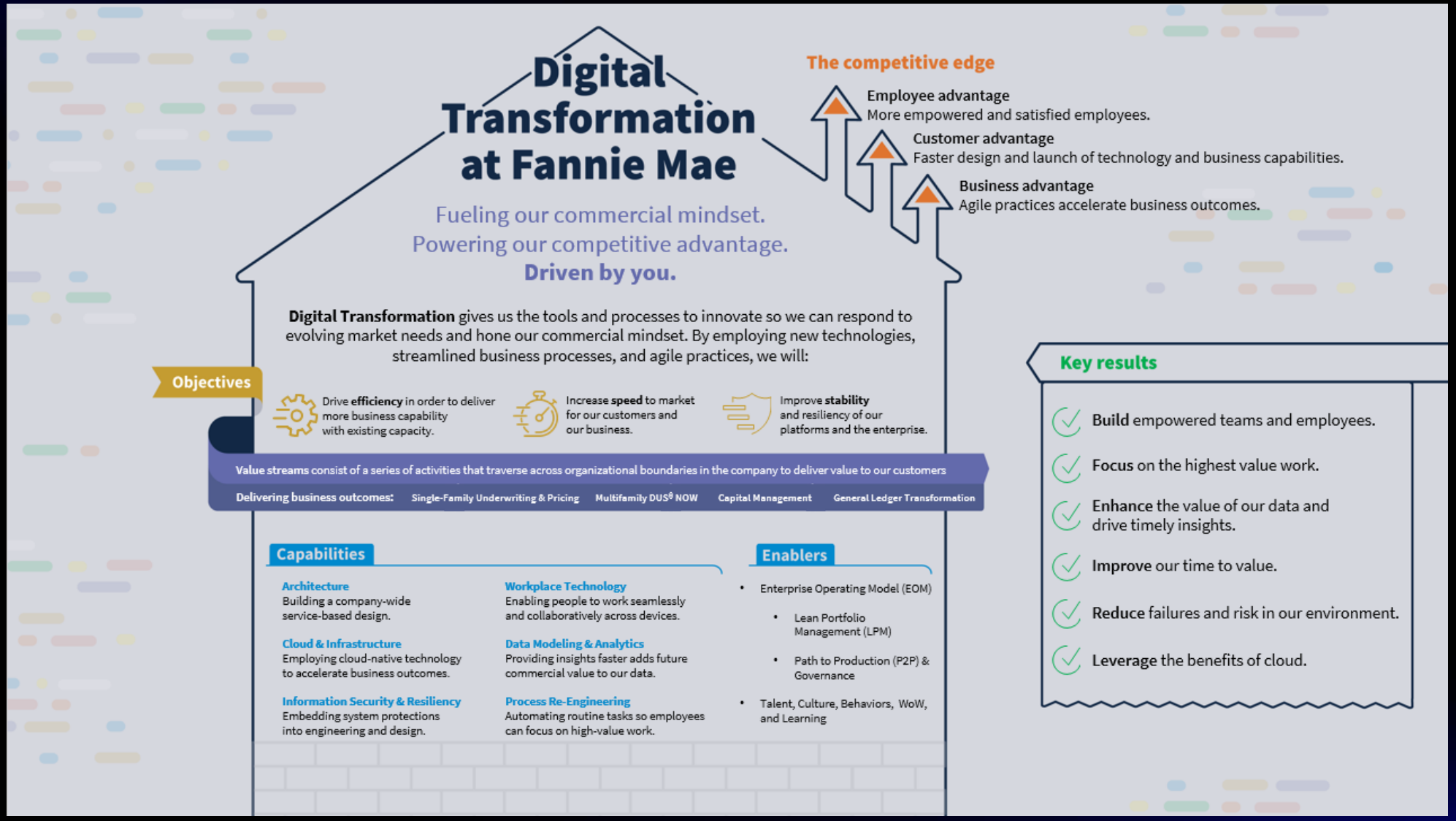


Homes financed by Fannie Mae

aws

© 2021 Fannie Mae, reproduced by permission

Digital transformation at Fannie Mae



© 2021 Fannie Mae, reproduced by permission

Cloud adoption is a key enabler for our digital transformation

We will provide the means to anticipate, sense, and respond to rapidly changing customer needs in the market in ways that create competitive advantage, balancing speed and stability, via a resilient cloud foundation, connected cloud capabilities, and new ways of working



TIME TO CUSTOMER VALUE

Increase the speed with which value is delivered to our customers



ORGANIZE FOR EFFECTIVENESS

Transform organization to efficiently operate in the cloud and reduce operating costs



DIGITAL STABILITY

Deliver cloud capabilities that are secure and resilient



BUSINESS INNOVATION AT SPEED

Rapidly prototype new capabilities and quickly scale them to production



ENABLE TRANSFORMATION

Enable refactoring of key digital transformation initiatives



INTELLIGENT AUTOMATION

Unlock capabilities to capture value differently

aws

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

On-premises footprint

~11,000 servers: physical and virtual

SUSE, Red Hat, Windows, Solaris, VMware



App servers ~5,700



Web servers ~800



DB servers ~1,800



Load balancer, grid, other servers ~2,700

~2,500 on-premises and cloud software assets

	On prem	Cloud
Applications	280	520
Utilities	270	264
Components	239	357
EUCs	256	89

Excludes ~260 external data assets

Technologies used

TIBCO BE, BW

SAS, R.grid

SQL Server, Oracle, Sybase

Autosys

C++, Java

COBOL/ IDMS

IBM M/W

Solaris/Linux/ Windows

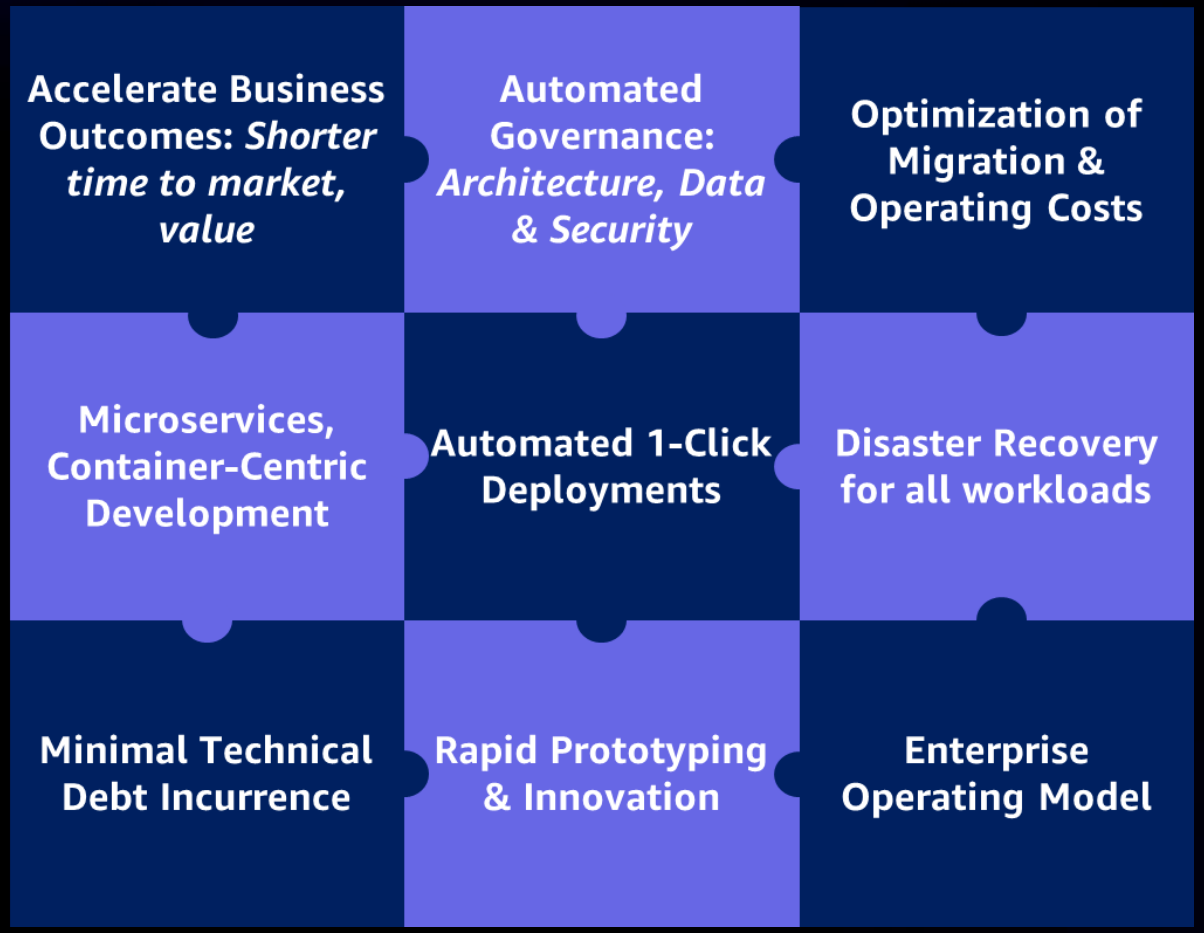
Ab Initio, Informatica

Jenkins

aws

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

Guardrails



Key measurements

1. % workloads operating in the cloud
2. % IT budget reduction YoY
3. # assets retired on premises (migrations)
4. No new on-premises assets
5. Deployment lead time
6. Deployment failure rate
7. # full-stack engineer development

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

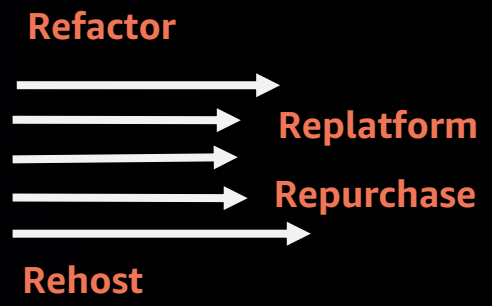
Cloud strategy

AWS serves as primary cloud for Fannie Mae; migrations aligned to the 6Rs

Workloads default to AWS



Asset types: applications, components, utilities, and EUC





EXCEPTIONS (other cloud: fit for purpose)

Is this a workplace productivity tool? → No → Is there a SaaS offering AND is the SaaS offering desired by the business? → No → Is there a technical or business rationale to keep the application on premises* → No → Does not fit identified exceptions → Fannie Mae's Cloud Governance Council

Yes → O365

Yes → SaaS

Yes → Remains as-is on premises

Includes applications scheduled for sunset

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

Migration journey



TECHNOLOGY

Establish architecture, patterns, pipelines, account structure, relevant automation, and migration capabilities

OPERATING MODEL

Creation, rollout, adoption, and optimization of enterprise operating model (Agile principles)

CHANGE MANAGEMENT

Comprehensive cloud training, upskilling, communications, video logs, self-service portals

GOVERNANCE

Adherence to application lifecycle stage gates, FedRAMP, NIST, SOX controls

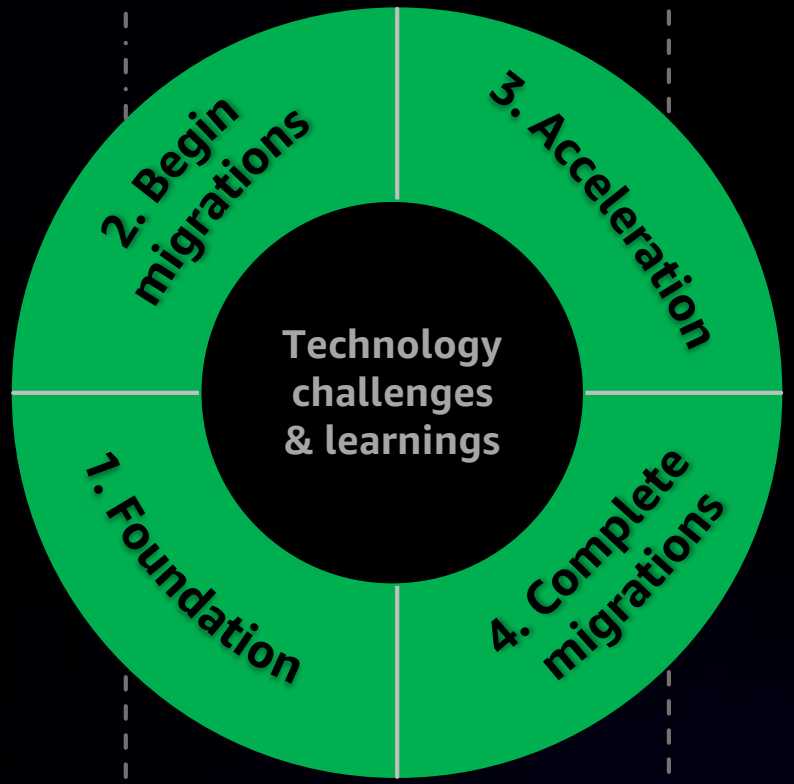
aws

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

Technology challenges and learnings

- Need for multi-account pattern identified; *Existing lifecycle-based accounts insufficient for enterprise cloud transformation efforts*
- Rehost: integration with interfaces was a challenge; *diminishing returns and security posture limited the scope of applications*
- Successful deployment of Amazon SageMaker ML models
- Value stream analysis/replatform: *inefficiencies largely identified with provisioning and rework*

- MVP: containers for web application, Tableau/ Amazon Redshift for data; *need for security patterns (Twistlock) and data access patterns*
- Replatforms: MVPs helped discover E2E activities required for migration; *squad-level gap in AWS cloud-native knowledge: tiger teams created*
- Technology reference models: target state architecture/services identified; *gap in availability and timeline for patterns*



- Homegrown tool for Infrastructure as Code (FLASH) developed; significant reduction in provisioning time and one-click deployments (resiliency)
- Built solution for YAML file creation from target state architecture, providing inputs to FLASH
- Tech debt for acceleration: ETL, batch jobs, SAS/R.grid, data access patterns; *FedRAMP, NIST guidelines required additional controls*
- Freedom to development team: move from Autosys and refactor to AWS Batch/AWS Lambda
- Docker Desktop enabled: Fast development–deployment cycle
- To achieve enhanced resiliency and automated deployments, prioritized workloads moved from old to new account structure
- No-code platform for end-user computing assets

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

Operating model and execution

Portfolio-level operating structure

Leadership and program office

Portfolio lead, stakeholders from business and COO organizations

Release train

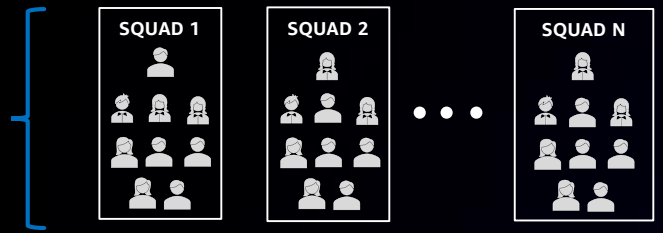
Dedicated resources at the portfolio level supporting applications and components through migration lifecycle

- ❑ Portfolio lead
- ❑ Enterprise architect
- ❑ Digital engineering
- ❑ Cloud CoE
- ❑ Enterprise DevOps
- ❑ Tiger team
- ❑ InfoSec
- ❑ Enterprise monitoring
- ❑ Data governance
- ❑ Path to production
- ❑ Production support

Dedicated portfolio squads

Squad members will spend 100% of their time assigned to cloud migrations only; team rotates to new application once migration is complete

Roles in squad
Product owner
Scrum master
Cloud-native engineers
SDET
SRE (YBYO)
DevOps
Transition/support engineers



Need basis
Cloud governance council

Monthly: S4
Technology and business leadership check-in

Weekly: S3
Cross-portfolio cloud migration check-in

Daily: S2
Problem-solve/Scrum of Scrum by release train

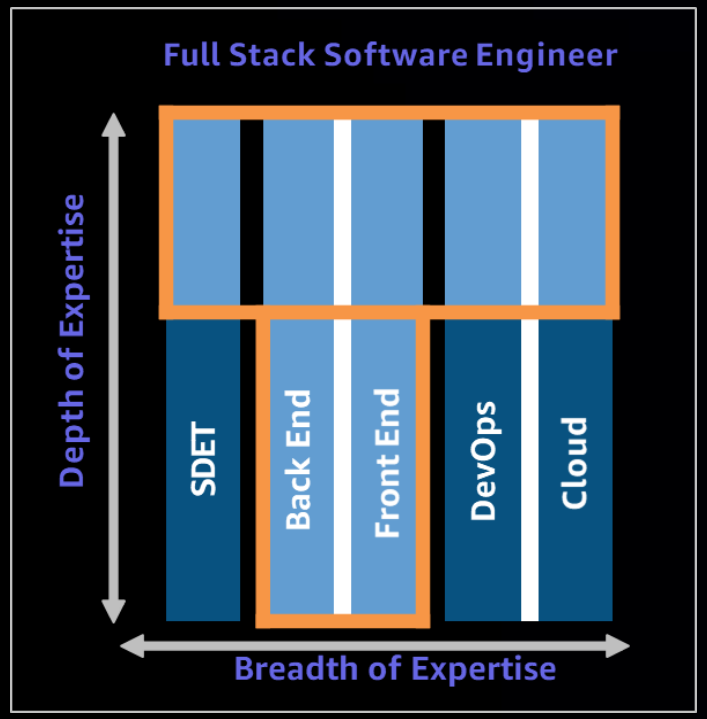
Daily: S1
Team standup

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

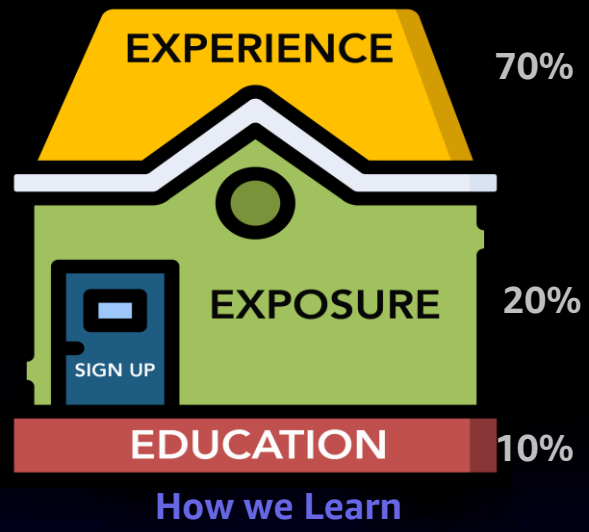
Change management (T-shaped talent)

- ❑ Engage business stakeholders: socialize, get buy-in, and onboard
- ❑ Cloud connects, townhalls: awareness and enablement of cloud program
- ❑ AWS Cloud Accelerator Academy: training and enablement of associates

Transform to T-shaped talent



1. Define full-stack engineer skillset
2. Map skillset to assessments
3. Assess skill level
4. Execute training plan
5. Track progress



How we Learn

aws

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

Balance governance with speed

1 Ideation | Permit to launch

Actors:					
Business	Intake	Scoping	Funding	Sponsor approval	Prioritization

2 Initiation | Permit to plan

Actors:					
BUCFO, business, and tech	SI planning	Define epics	Journey impact assessment (JIA)	Technology selection process	Initial investment review

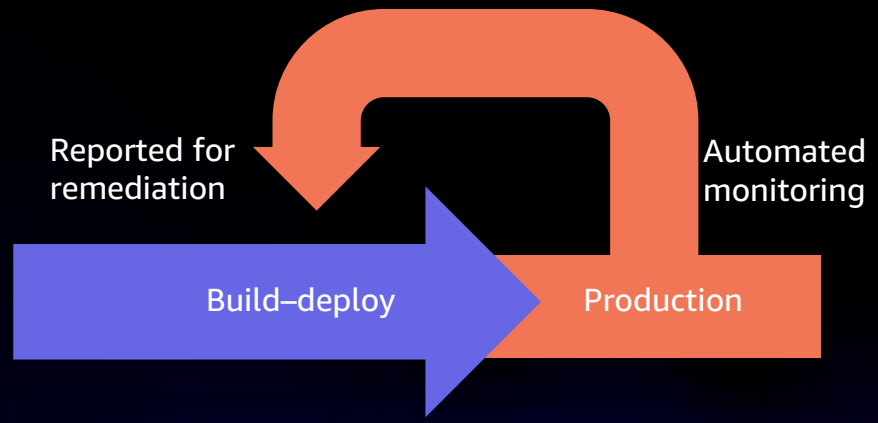
3 Planning | Permit to design/build

Actors:					
Business, tech, Agile teams	JIA – 2nd Iteration	Approved MVA	Features		Process, risk, and control owner engagement

4 Delivery | Permit to operate

Actors:					
Agile teams	Register release	JIA – final iteration	Sprinting	Op. readiness	Deployment approval

- ❑ Simplified governance and staying compliant, adhering to standards
- ❑ Evidence gathering through the process is automated
- ❑ Post-deployment, continuous monitoring in place and findings reported for remediation



aws

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

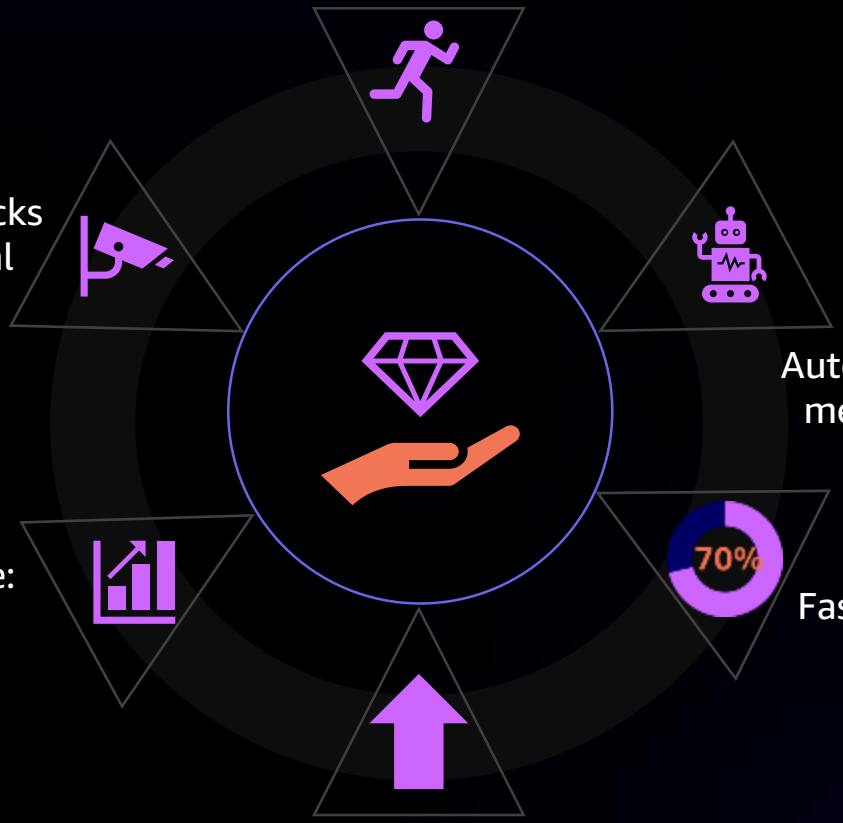
View of the overall journey

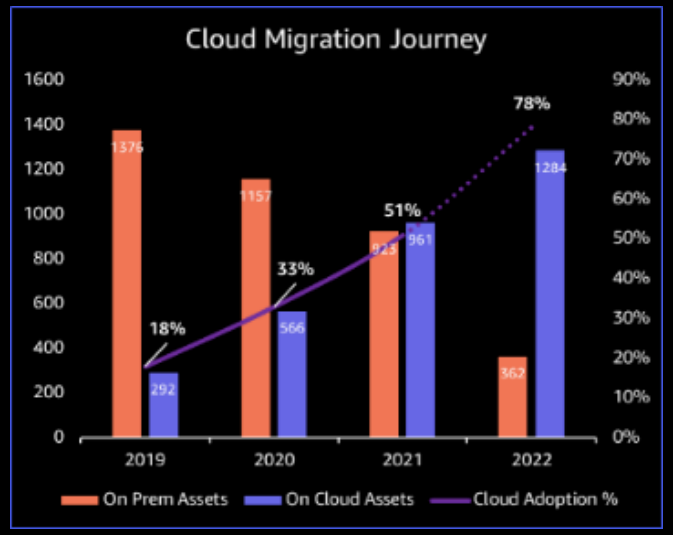


© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Business values realized so far

Swift COVID-19 response efforts
Forbearance and *Know Your Options*





Prevented 2 DDoS attacks on MBS Trading Portal

Automated and governed regulatory reporting capital metrics for conservatorship capital reporting (CCR): 2 billion calculations per month

Handled 3x more volume: underwriting and investor direct

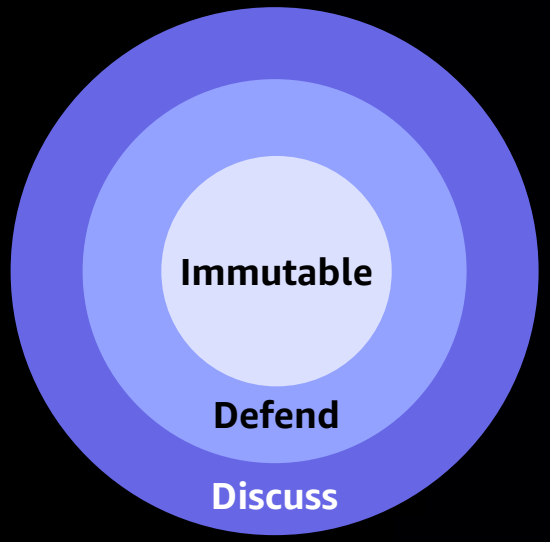
Faster time-to-market infra provisioning for MF DUS360 and payment service

Increased confidence of go-to-market of positive rent payment

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

Points to ponder

- Business strategy evolves during the multi-year cloud transformation journey
- Harmony and alignment: infrastructure, development, and operations
- 3-tiered decision strategy



Multi-account strategy, networking, VPC, security

Chaos testing, disaster recovery, transitional security posture

Database refactoring, application microservices

aws

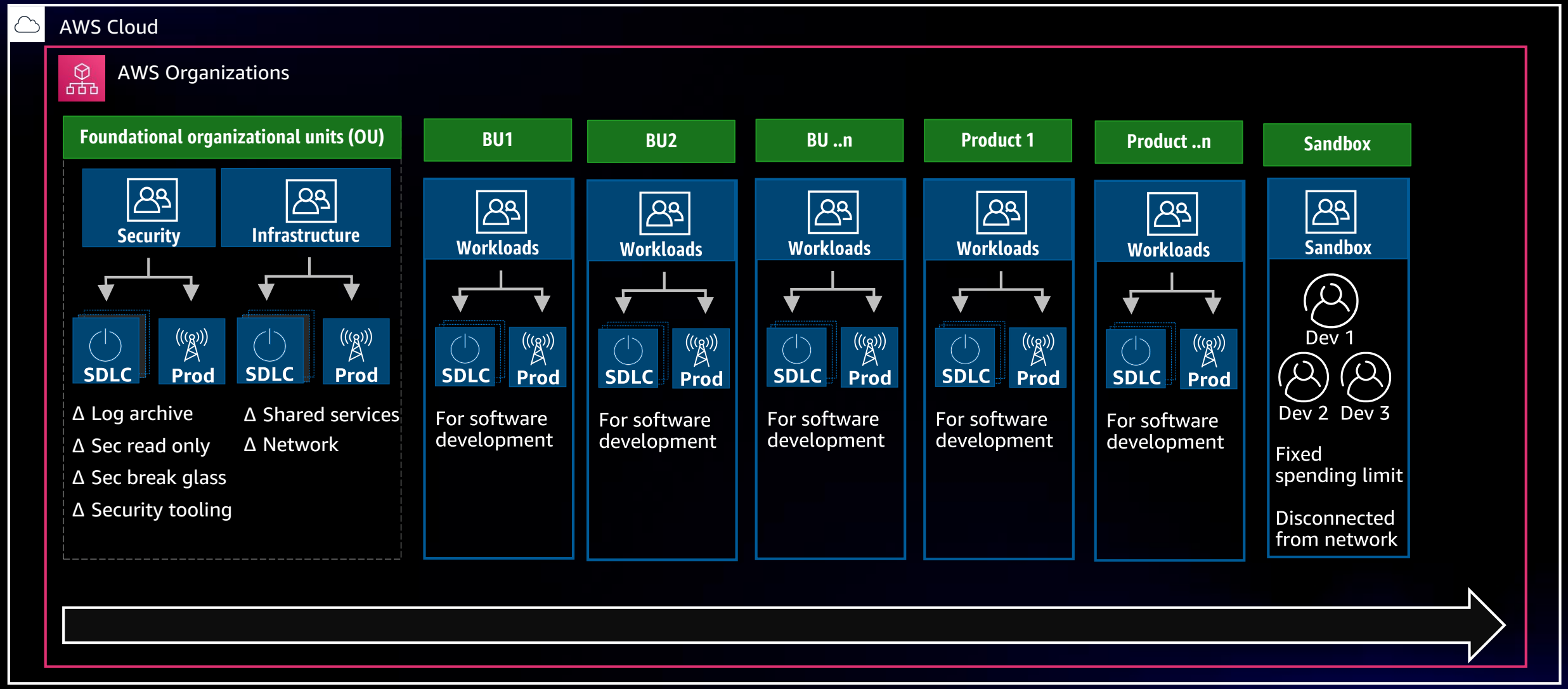
© 2021, Amazon Web Services, Inc. or its affiliates. All rights reserved.

Technical patterns – Enabling migrations

1. AWS multi-account pattern
2. Networking, VPC, and DNS patterns
3. Application microservices pattern
4. Database refactoring pattern
5. Chaos testing and disaster recovery pattern (future state)

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

1. AWS multi-account pattern



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

Fannie Mae's multi-account framework

- AWS accounts are segmented by business function and lifecycle
- Crown jewel applications are segmented into separate lifecycle accounts

Benefits of using a multi-account AWS environment

- Group workloads based on business purpose and ownership
- Apply distinct security controls by environment
- Constrain access to sensitive data
- Promote innovation and agility
- Limit scope of impact from adverse events
- Support multiple IT operating models
- Manage costs
- Distribute AWS service quotas and API request rate limits

Multi-account AWS environment: https://tinyurl.com/awsmultiac

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

Account deployment pattern – AWS Control Tower



Automated landing zone with best-practice blueprints



Guardrails for policy management



Account factory for account provisioning



Dashboard for visibility and actions



Built-in identity and access management



Preconfigured log archive and audit access to accounts



Built-in monitoring and notifications



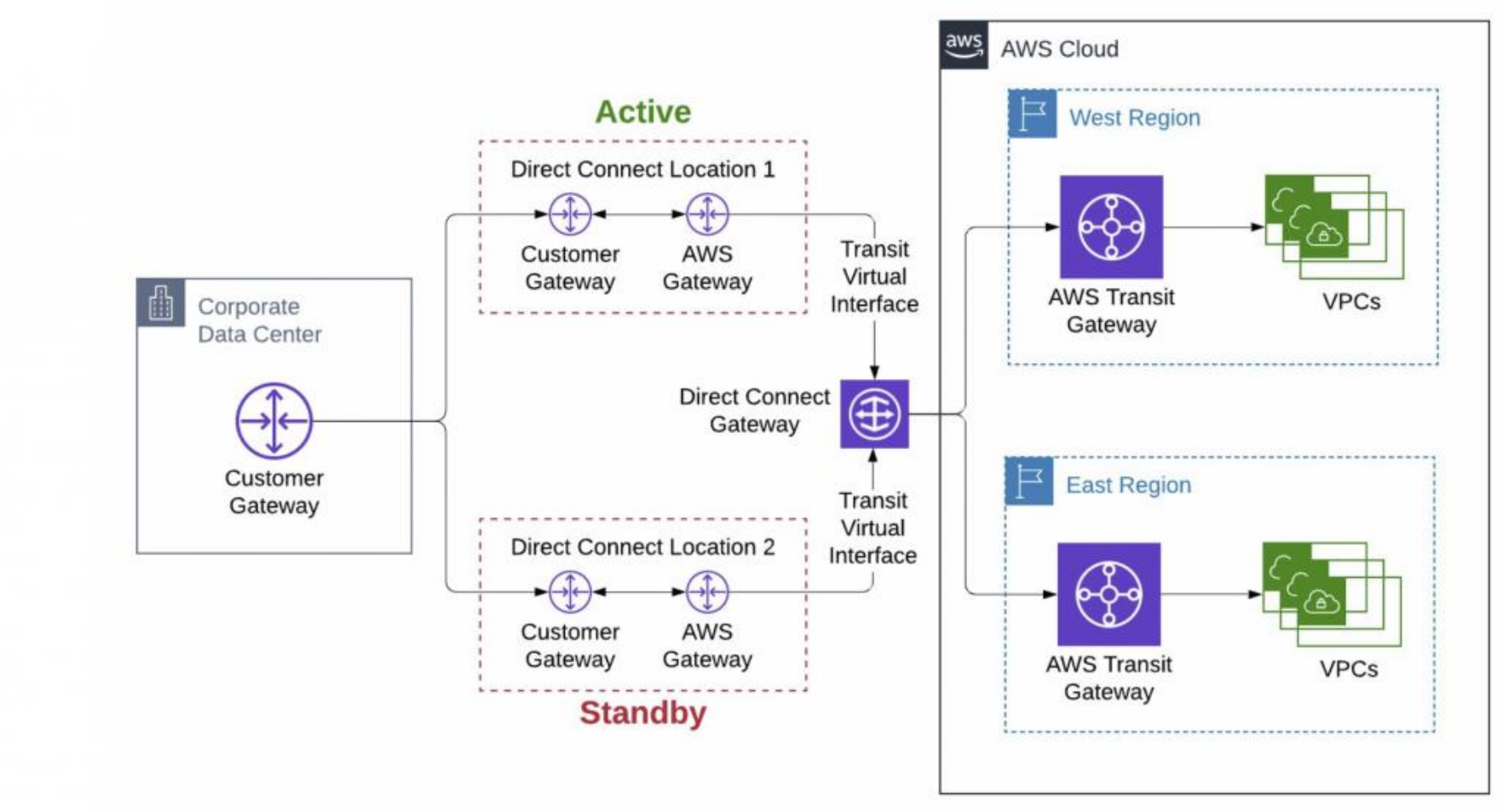
Automatic updates

AWS Control Tower: https://tinyurl.com/setuplaunch

aws

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

2. Network connectivity pattern (from on premises to AWS)

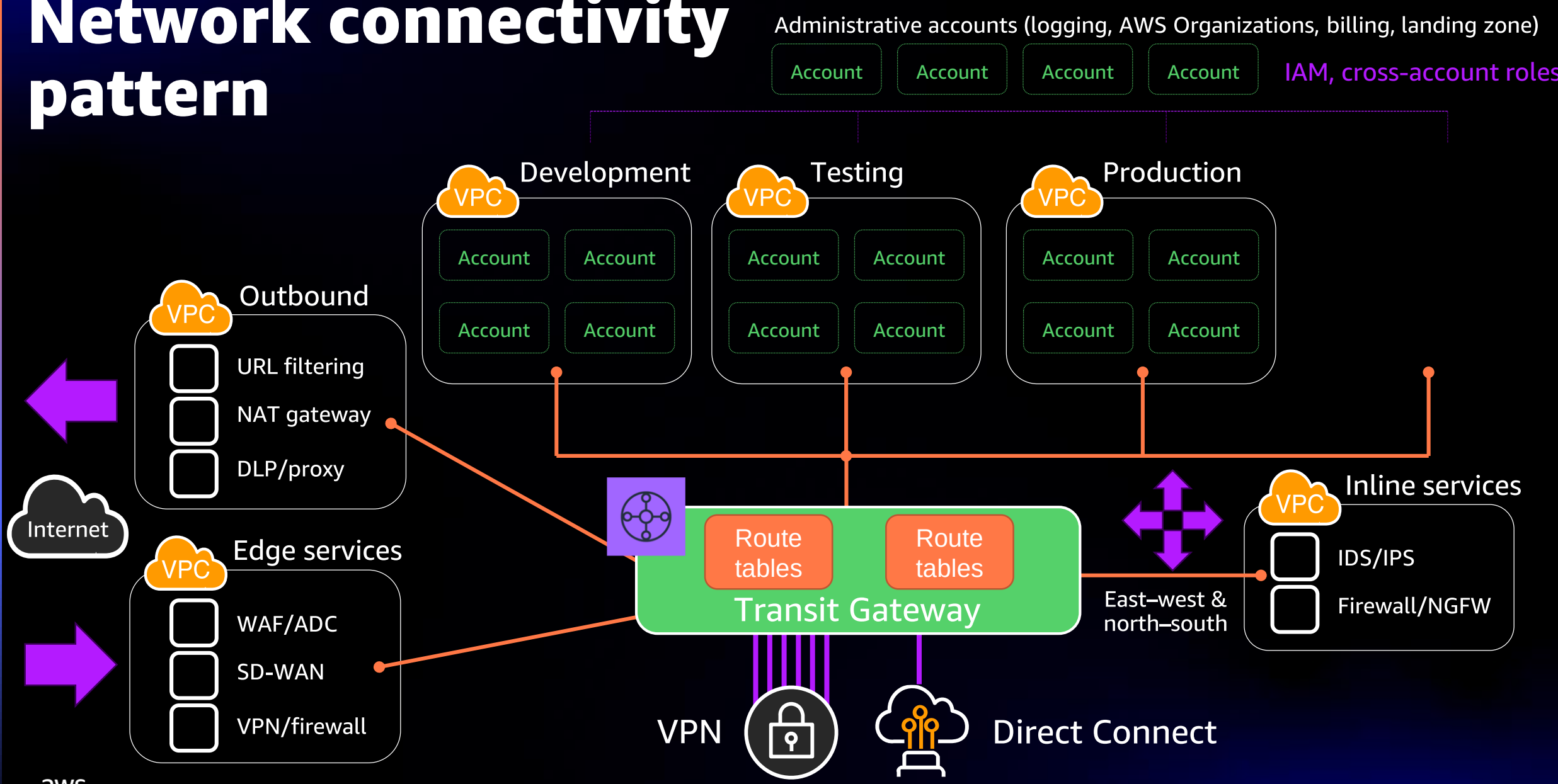


- Fannie Mae uses AWS Direct Connect gateway and Transit Gateway for hybrid connectivity
- Connect 1,000s of VPCs at scale
- Max 3 Transit Gateways can be connected to a Direct Connect gateway
- Can advertise max 20 CIDRs per Transit Gateway to on premises via a transit VIF
- Can advertise max 100 CIDRs from on premises to AWS via a transit VIF

https://tinyurl.com/dxg2tgw

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

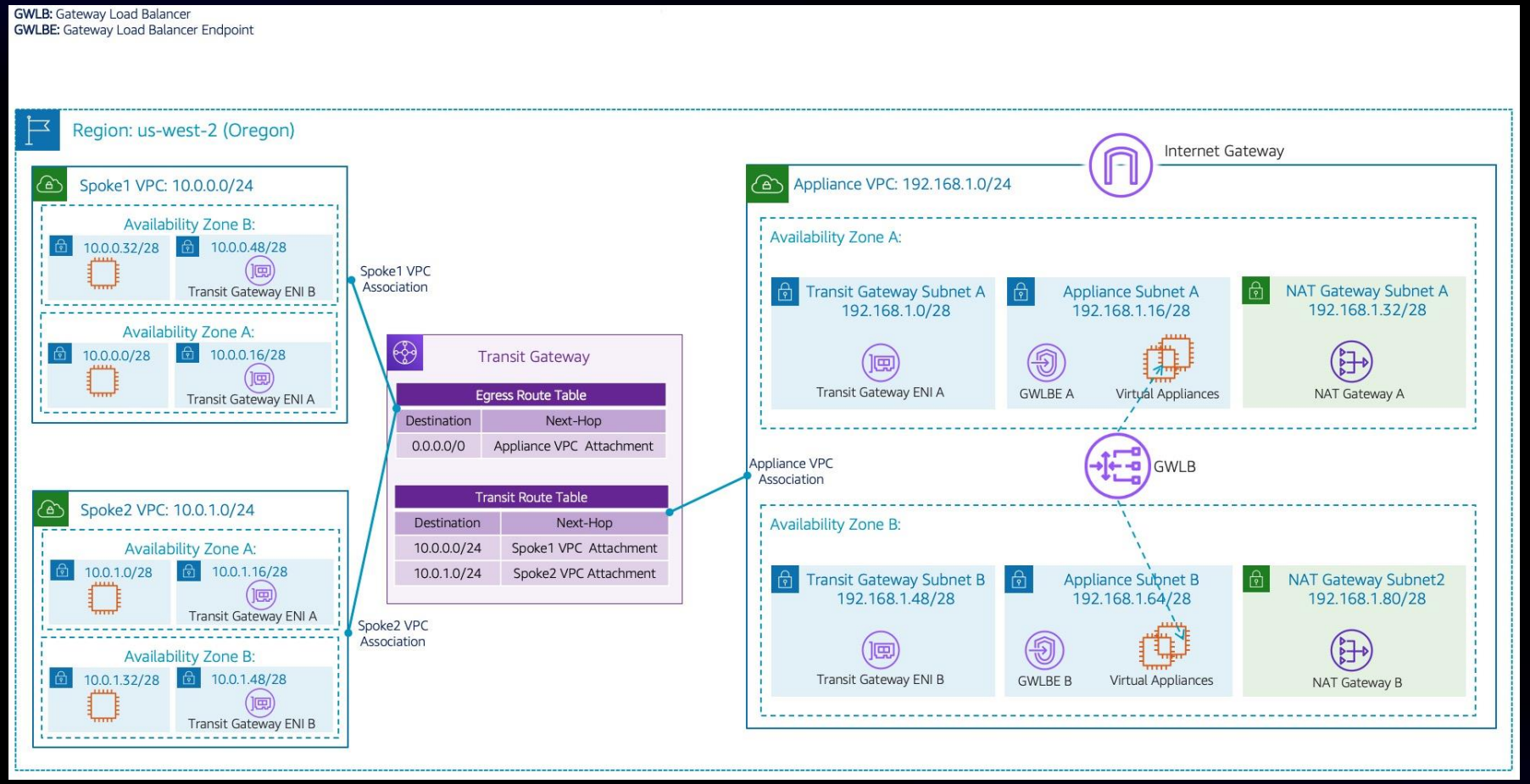
Network connectivity pattern



https://tinyurl.com/dxg2tgw

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

Network connectivity pattern (inspection VPC)

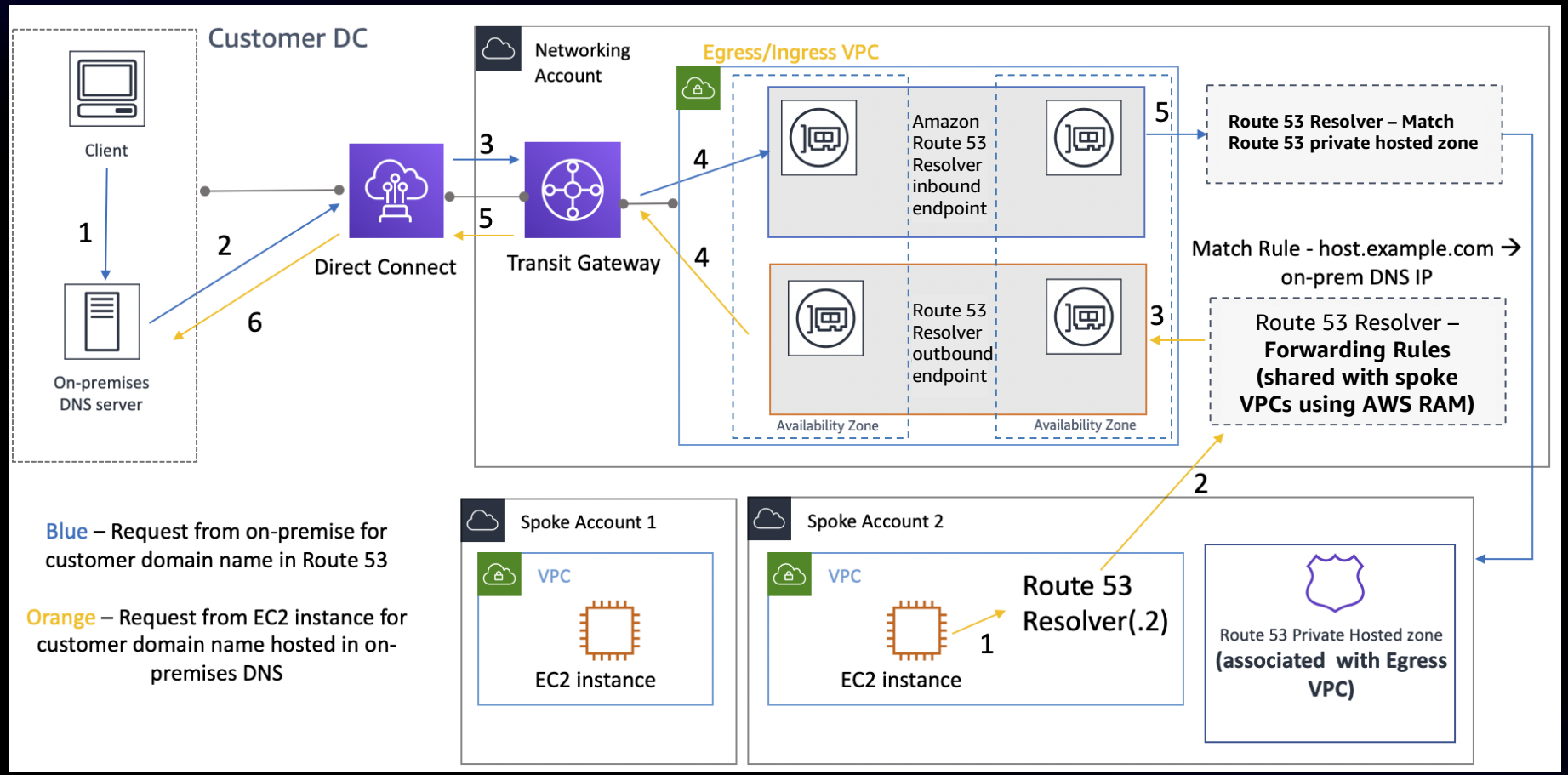


tinyurl.com/gwlbscan

- Inspect network traffic to meet security and compliance mandates
- Traffic inspection with FW appliances and GWLB
- Centralized security architecture
- Inspect VPC-to-VPC traffic
- Inspect VPC-to-on-premises traffic

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

Hybrid DNS pattern

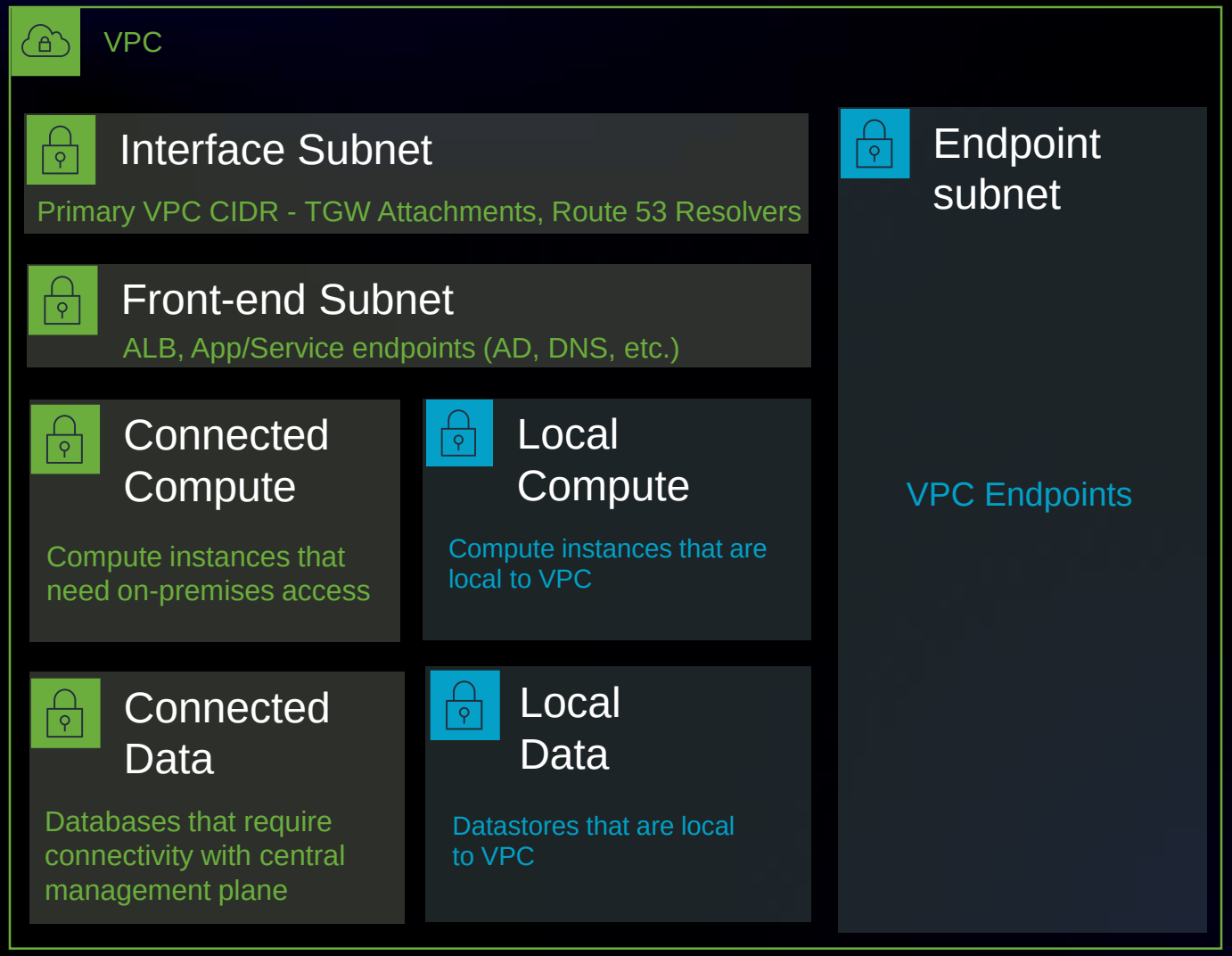


- DNS queries from VPC to on premises are forwarded via Route 53 Resolver outbound endpoints
- DNS queries from on premises to VPC are forwarded to Route 53 Resolver inbound endpoints
- It is NOT recommended to create Route 53 Resolver endpoints in every VPC – centralize them

https://tinyurl.com/hybriddns

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

VPC pattern – Modular structure

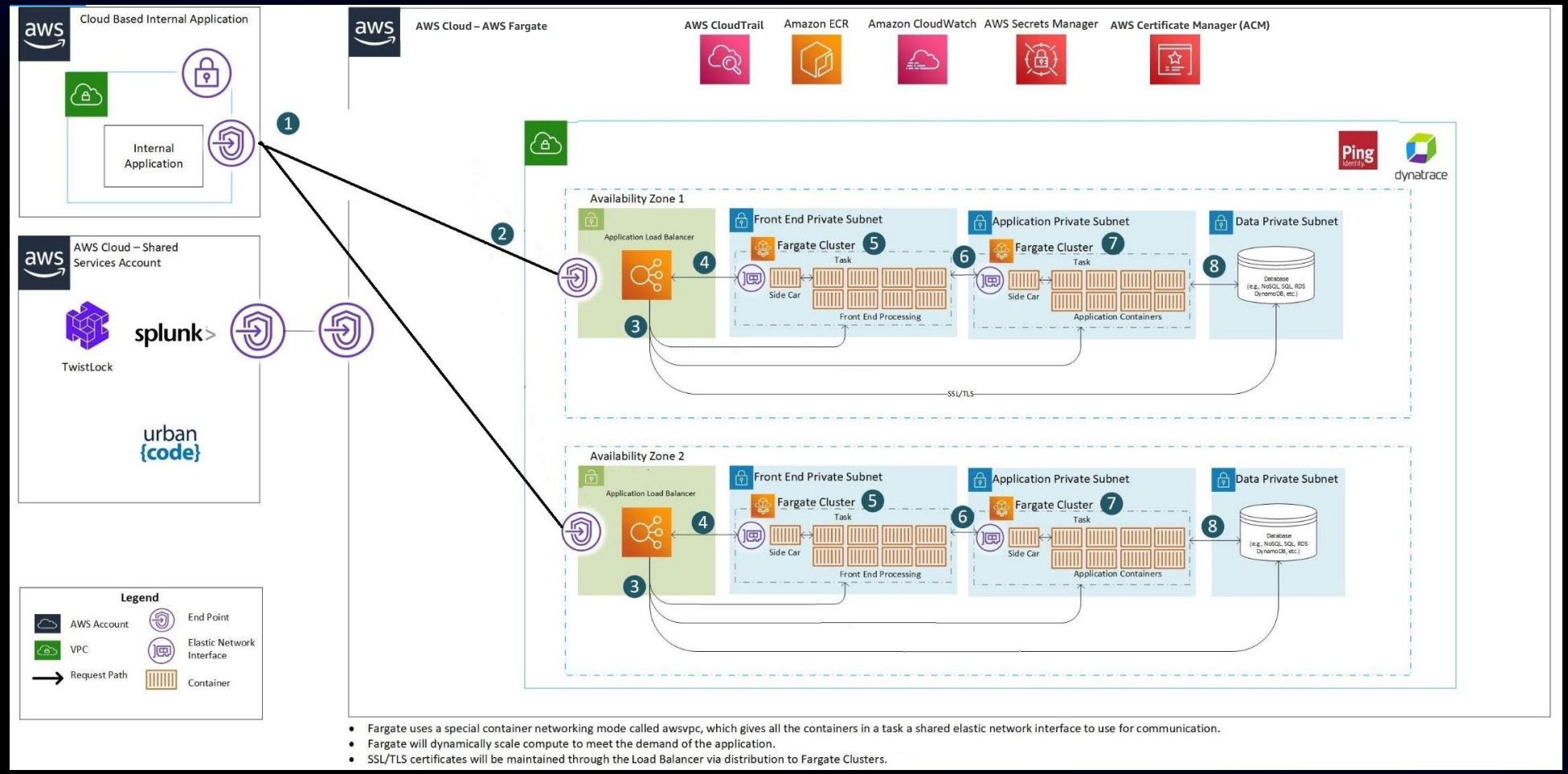


- Modular VPC design with multiple secondary CIDRs
- Routable and non-routable subnets
- Non-routable secondary CIDRs can be reused across VPCs to preserve IP space
- T-shirt sizing of VPC CIDRs

T-Shirt Size	Summerized Block	IP Count	Subnet CIDR	IP Count Per AZ
XS	/25	128	/27	32
S	/24	256	/26	64
M	/23	512	/25	128
L	/22	1024	/24	256
XL	/21	2048	/23	512
XXL	/20	4096	/22	1024

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

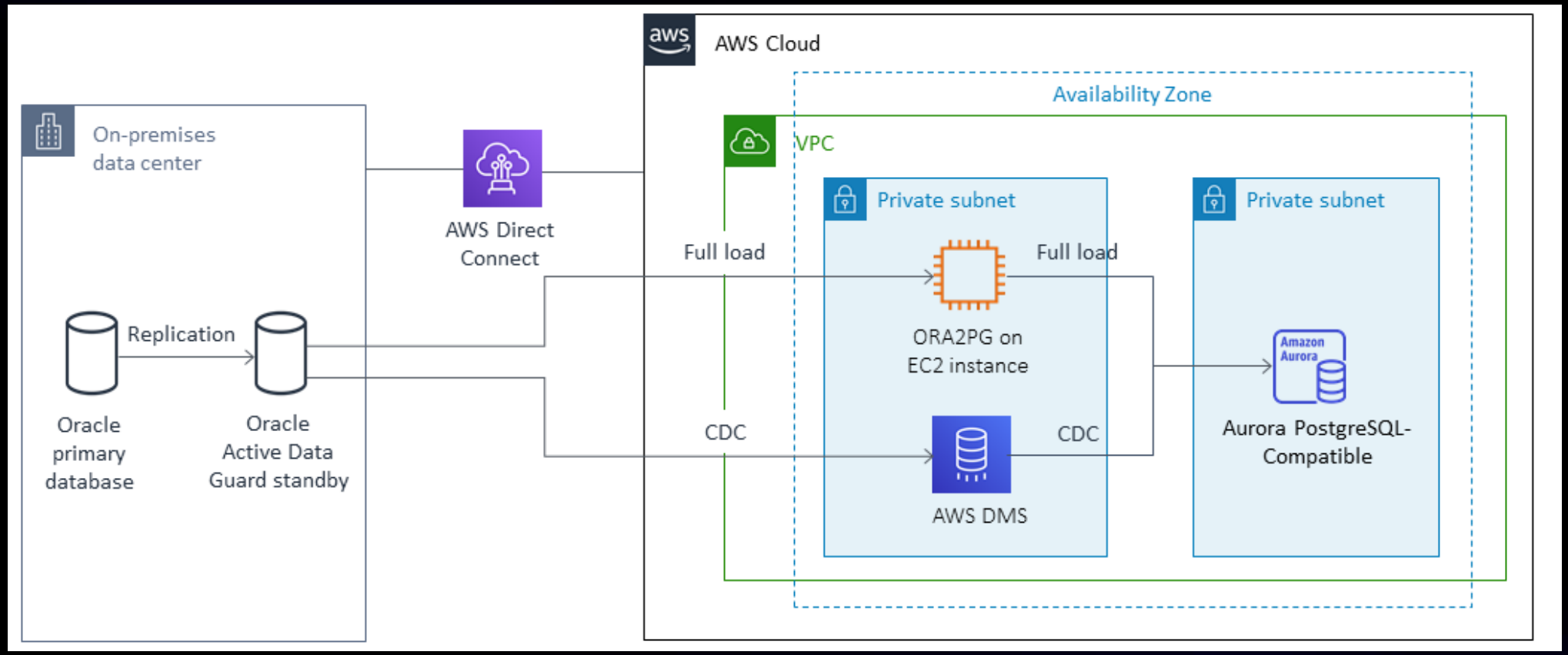
3. Application microservices pattern



- Container deployment architecture with Amazon ECS/Fargate
- Container image build with Jenkins, Nexus
- Container scanning with Twistlock
- CI/CD deployment with UCD/Jenkins
- Container image repo with Amazon ECR
- Container orchestration with Amazon ECS/ Fargate

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

4. OLTP database pattern – Amazon Aurora PostgreSQL-Compatible Edition

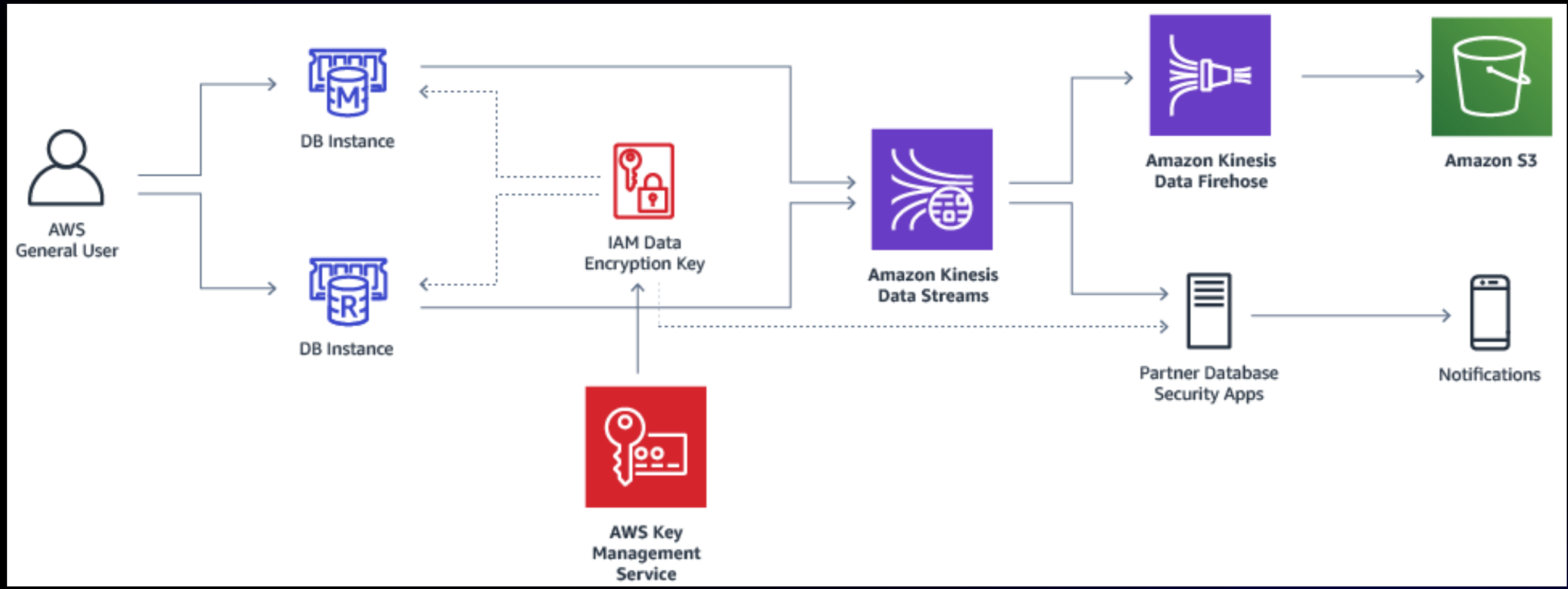


https://tinyurl.com/ora2AWSpg

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

Database Activity Streams (DAS)

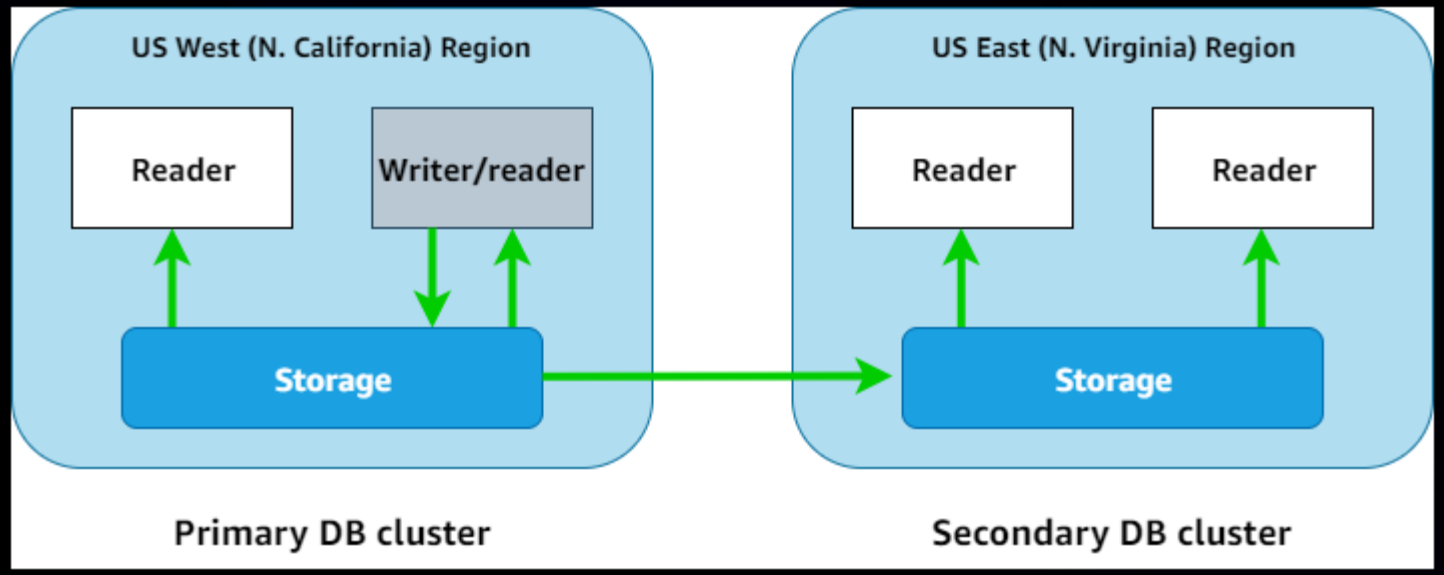
Monitoring database activity with DAS to meet regulatory requirement



https://tinyurl.com/AWSDAS

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

Aurora global database – DR replication

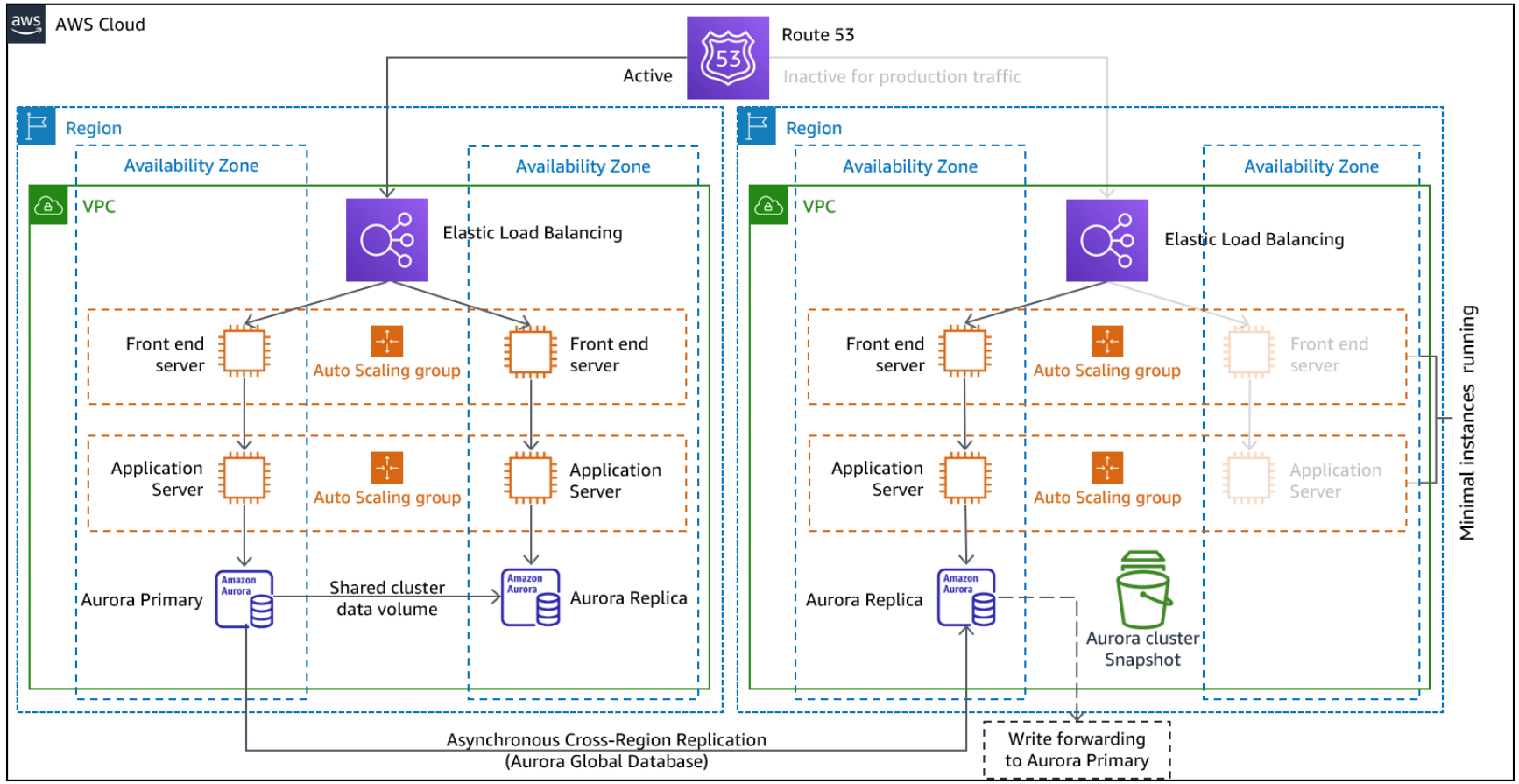


tinyurl.com/AuroraPGCRR

- Aurora PostgreSQL-Compatible global database is the default DB engine, over 100+ production applications in Fannie use Aurora PostgreSQL DB
- DR – achieve low RTO/RPO with Aurora PostgreSQL-Compatible global database (see blog)
- Migrate on-premises commercial DBs to Aurora PostgreSQL using AWS DMS
- Highly secure with VPC network Isolation and supports AWS KMS for data-at-rest encryption
- Use Database Activity Streams (DAS) for monitoring DB activities

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

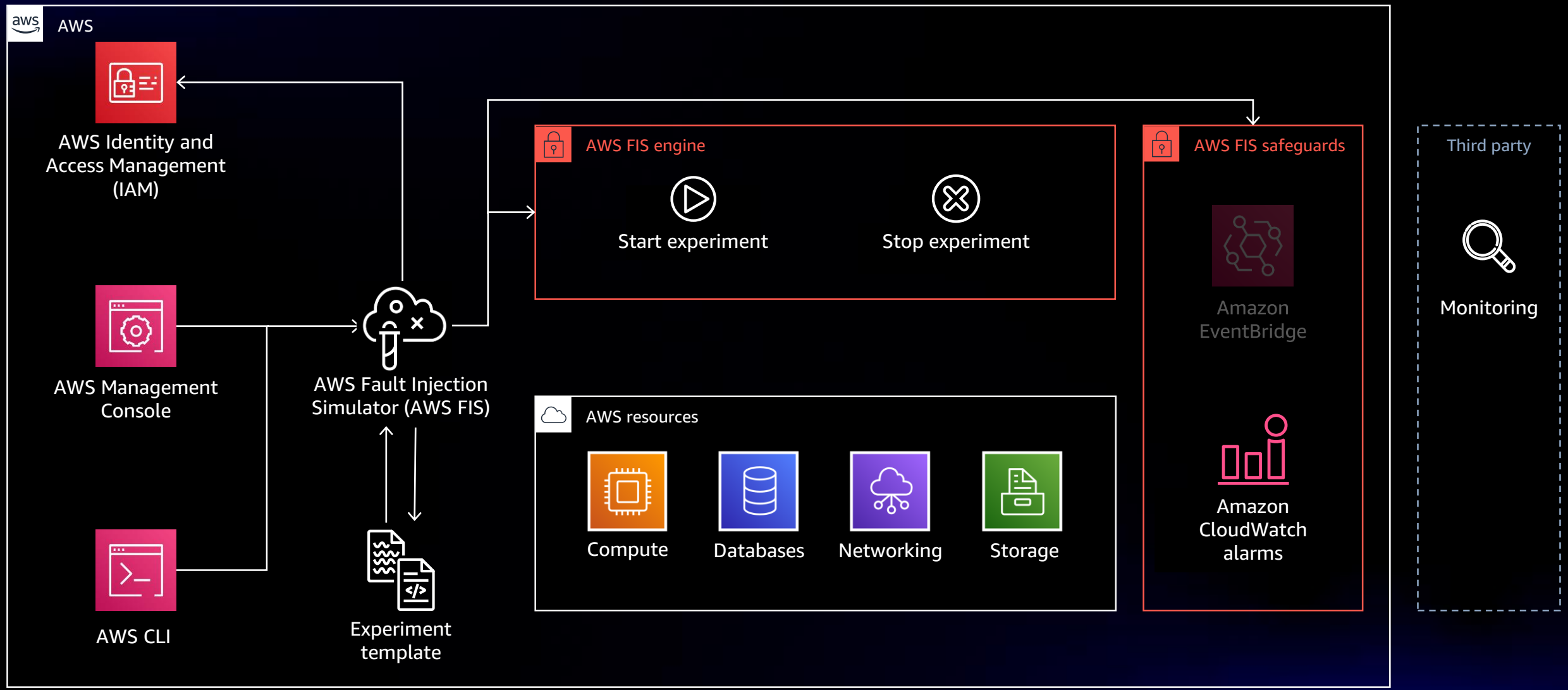
5. Disaster recovery – Active/standby pattern



- Fannie Mae uses two AWS Regions as part of their DR strategy
- Fannie Mae has adopted the "warm standby" pattern for most production applications
- RTO/RPO varies based on application "recovery groups"

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

Chaos testing – AWS Fault Injection Simulator (AWS FIS)



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

AWS FIS – Experiment templates

- Name
- Description
- IAM role
- Stop conditions
- Targets
- Actions

```
{
   "tags": {
        "Name": "StopAndRestartRandomInstance"
   },
   "description": "Stop and Restart One Random Instance",
   "roleArn": "arn:aws:iam::0123456789:role/MyFISExperimentRole”,
   "stopConditions": [
        {
            "source": "aws:cloudwatch:alarm",
            "value": " "arn:aws:cloudwatch:us-east-
1:0123456789:alarm:No_Traffic"
        }
   ],
   "targets": {
        "myInstance": {
            "resourceTags": {
                "Env": "test"
            },
            "resourceType": "aws:ec2:instance",
            "selectionMode": "COUNT(1)"
        }
   },
   "actions": {
        "StopInstances": {
            "actionId": "aws:ec2:stop-instances",
            "description": "stop the instances",
            "parameters": {
                "startInstancesAtEnd": "true",
                "duration": "PT2M",
            },
            "targets": {
                "Instances": "myInstance"
            }
        }
    }
}
```

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

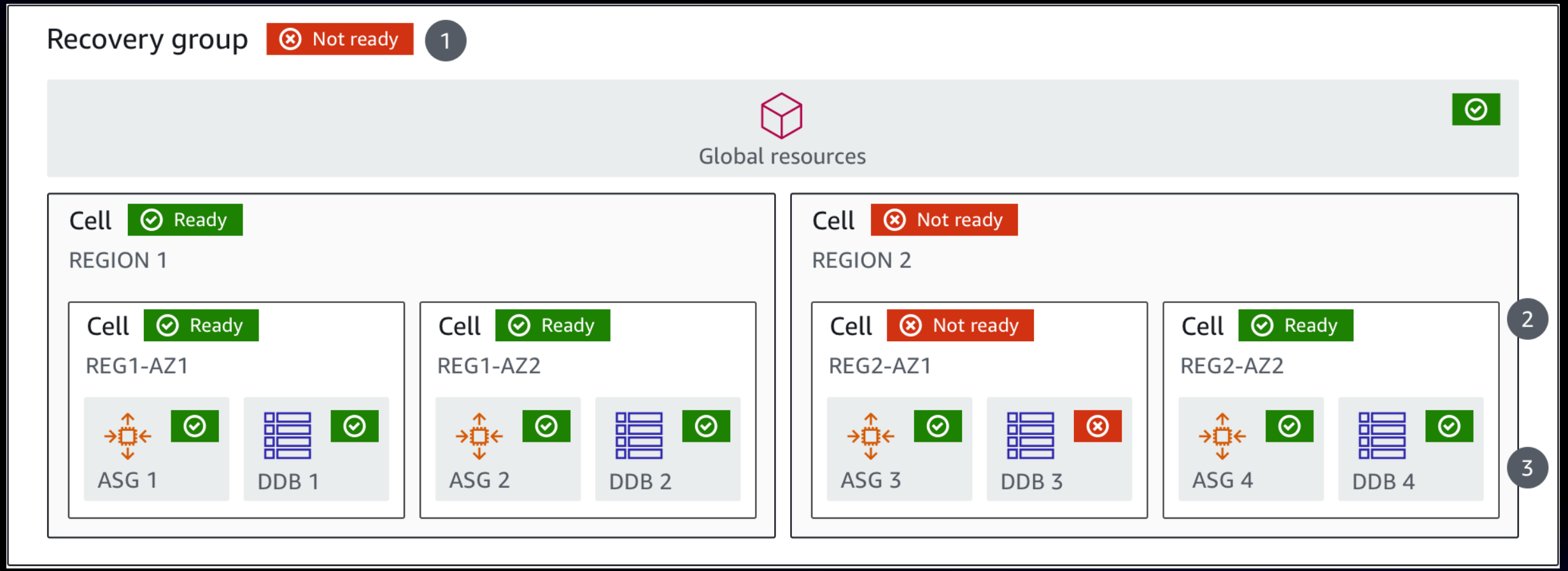
AWS FIS – Actions

Supported fault injections

- Server error (Amazon EC2)
- Stop, reboot, and terminate instance(s) (Amazon EC2)
- API throttling
- Increased memory or CPU load (Amazon EC2)
- Kill process (Amazon EC2)
- Latency injection (Amazon EC2)
- Container instance termination (Amazon ECS)
- Increase memory or CPU consumption per task (ECS)
- Terminate nodes (Amazon EKS)
- Database stop, reboot, and failover (Amazon RDS)
- And more to come in 2022

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

DR failover – Amazon Route 53 Application Recovery Controller



1. Readiness status
2. Cells and nested cells
3. Resources

aws

https://aws.amazon.com/route53/application-recovery-controller/

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

DR failover – Amazon Route 53 Application Recovery Controller

Benefits

- Designed for applications with low RTO (<5 minutes) or >99.99% availability
- Mitigating cross–Availability Zone or cross-Region recovery
- Supports active-standby or active-active architectures
- Central control over application recovery operations across orgs

Features

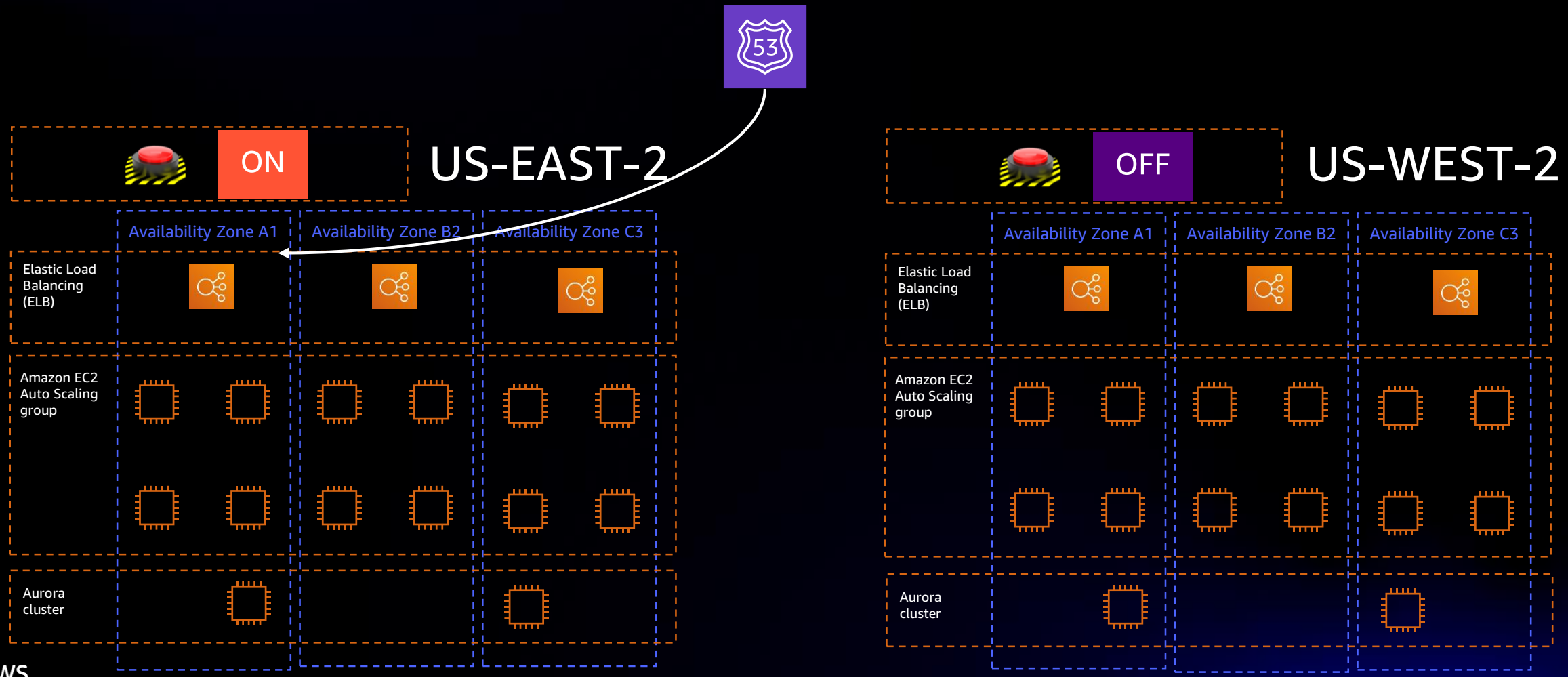
- Readiness check – confirms application replicas are able to take traffic
- Routing control – redirects traffic to a healthy application replica at the press of a button
- Safety rules – defines and ensures application replica failover criteria are met before executing a recovery

aws

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

Amazon Route 53 ARC: Routing control

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



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

Continuous Resilience – AWS Resilience Hub

- Protect mission-critical applications
- Validate continuous resilience of applications
- Optimize business continuity while reducing recovery costs



https://aws.amazon.com/resilience-hub/

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

Key technical takeaways

- **Used multi-account AWS environment** for rapid innovation, flexible security controls and simplified billing; automate account provisioning with AWS Control Tower
- **Built modular VPCs** and centralized networking with Direct Connect gateway and Transit Gateway
- **Built inspection VPC** for centralized traffic inspection with Gateway Load Balancer (GWLB)
- **Hybrid DNS** with Route 53 Resolvers
- **Application Refactoring with Amazon ECS/ Fargate** for agility and rapid deployments of containerized workloads, along with CI/CD toolset
- **Database refactoring with Aurora PostgreSQL-Compatible** for globally distributed applications using Multi-AZ and global database features
- **Chaos testing with AWS FIS** to simulate real-world scenarios and improve application resilience
- **Route 53 Application Recovery Controller** to automate DR failover for application with low RTO/RPO
- **AWS Resilience Hub** to prepare and protect your applications from disruptions

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

Resources – Disaster recovery

Multi-Region infrastructure code deployments

- CI/CD pipeline: https://tinyurl.com/MultiRegionIAC

Cross-Region data replication

- Amazon DynamoDB global tables: https://tinyurl.com/AWSDDBCRR
- Amazon Aurora global database: https://tinyurl.com/AWSAuroraCRR
- Amazon S3 CRR: https://tinyurl.com/AWSS3CRR
- Amazon EBS CRR: https://tinyurl.com/EBSCRSnap

DR Preparedness

- Amazon FIS: https://aws.amazon.com/fis/
- Route 53 ARC: https://tinyurl.com/awsR53ARC
- AWS Resilience Hub: https://tinyurl.com/awsreshub
- Testing Disaster Recovery: https://tinyurl.com/AWSDRWPP

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

Thank you!

Ramon Richards

Satya Addagarla

Harsha Nippani

Twitter: @HarshaNippani

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