Why Architect and Bring to Market ISV Solutions on AWS GovCloud (US)

Tres Vance
Lead Solutions Architect

OPS Track ATO Sales Kick Off 2019

Source: Cisco Global Cloud Index, 2015-2020 *
Workload = a virtual machine or a container

Public cloud trends are accelerating

BY 2020:

68% of cloud workloads will be in public cloud (35% CAGR from 2015 to 2020)

74% of cloud workloads will be Software-as-a-Service (SaaS) by 2020

$236B in public cloud + SaaS revenue by 2020

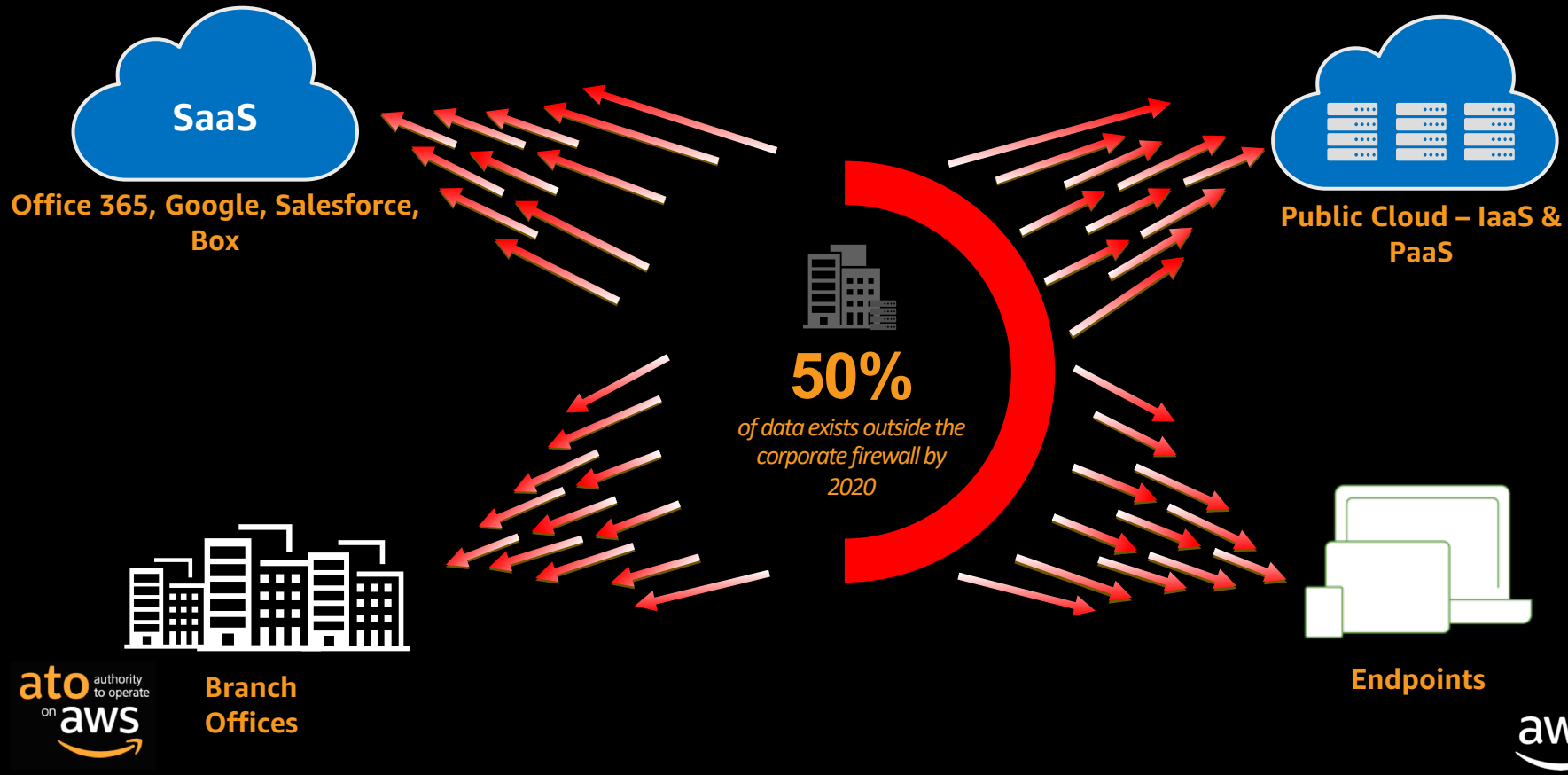
Enterprise software portfolio is in transition

ON-PREMISE SOFTWARE CATALOG:

STARTING POSITION

- 10-40% business applications developed in-house
- 30% open source/free software
- 70% COTS software
- ~200+ software product vendors
- Large EA/ELAs for top 50 vendors
- Long list of products not well known or tracked
- Upgrade cascades over 3-5 year cycle
- High potential for rationalization

The Data Center is No Longer the Center of Data



Source: Gartner

How do organizations implement software on AWS?

AWS SOFTWARE DEPLOYMENT OPTIONS

SOFTWARE PACKAGE INSTALLATION

Traditional software installation on an Amazon EC2 instance using Windows Installer (.MSI), Linux-based (.RPM), and Unix-based (.DEB) packages.

AMAZON MACHINE IMAGE (AMI)

Public or private software template that provides the information required to launch an AWS EC2 instance. Include root volume, launch permissions, and block device mappings.

SOFTWARE AS A SERVICE (SAAS)

Software licensing and delivery model whereby software is centrally managed and hosted on AWS and available to customers on a subscription basis.

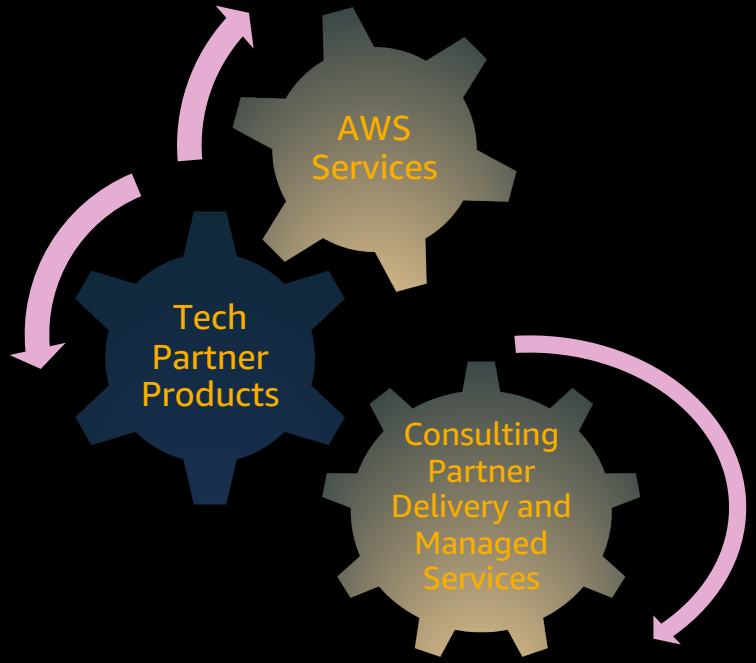
ato authority to operate on aws

aws

How ATO on AWS includes Partners

Partner Driven and Partner Led Solution

- AWS services provide AWS scale, durability, cloud economics and access to cloud-based analytics
- AWS Technology Partners Independent Software Vendors that offer advanced and differentiated solutions
- Consulting Partners help customers deploy and manage end-to-end business solutions



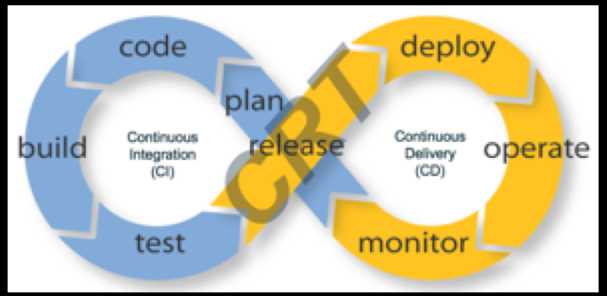
ato authority to operate on aws

aws

Solution Overview: SAO

Develop an **AWS Security Automation and Orchestration (SAO)** repository for constraining, tracking, publishing continuous security configurations, integration, deployments and treatments which are certified against common security frameworks (e.g. FedRAMP, DoD CC SRG, IRS 1075,CIS, PCI, etc.)

SAO will facilitate the orientation and association of **DevOps** and **Security** practices, changes and coordination of **Continuous Integration (CI)**, **Continuous Delivery (CD)** and **Continuous Risk Treatment (CRT)*** of an AWS customer account and/or multiple accounts.



* CRT is a process and technology approached which is designed to detect, maintain and in *MOST* case correct security, compliance and threats associated with an organization's solution and service deployment within their AWS account. CRT processes monitor security controls in real-time to ensure the risk and/or threat treatment (Control Intent) is working as designed or at least within an intended margin of acceptance base on guard rails, swim lanes and/or rules built into the control to allow for business operations.

How do organizations implement software on AWS?

AWS SOFTWARE DEPLOYMENT OPTIONS

SOFTWARE PACKAGE INSTALLATION

Traditional software installation on an Amazon EC2 instance using Windows Installer (.MSI), Linux-based (.RPM) and Unix-based (.DEB) packages.

AMAZON MACHINE IMAGE (AMI)

Public or private software template that provides the information required to launch an AWS EC2 instance. Include root volume, launch permissions and block device mappings.

SOFTWARE AS A SERVICE (SAAS)

Software licensing and delivery model whereby software is centrally managed and hosted on AWS and available to customers on a subscription basis.

ato authority to operate on aws

© 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws

Architecting Approaches for AWS

Cloud Migrator

- **Deploy existing apps in AWS with minimal re-design**
- Good strategy if starting out on AWS, or if application can't be re-architected due to cost or resource constraints
- Primarily use core services such as EC2, EBS, VPC

Cloud Forward

- **Evolve architecture for existing app to leverage AWS services**
- Gain cost and performance benefits from using AWS services such as Auto Scaling Groups, RDS, SQS, and so on

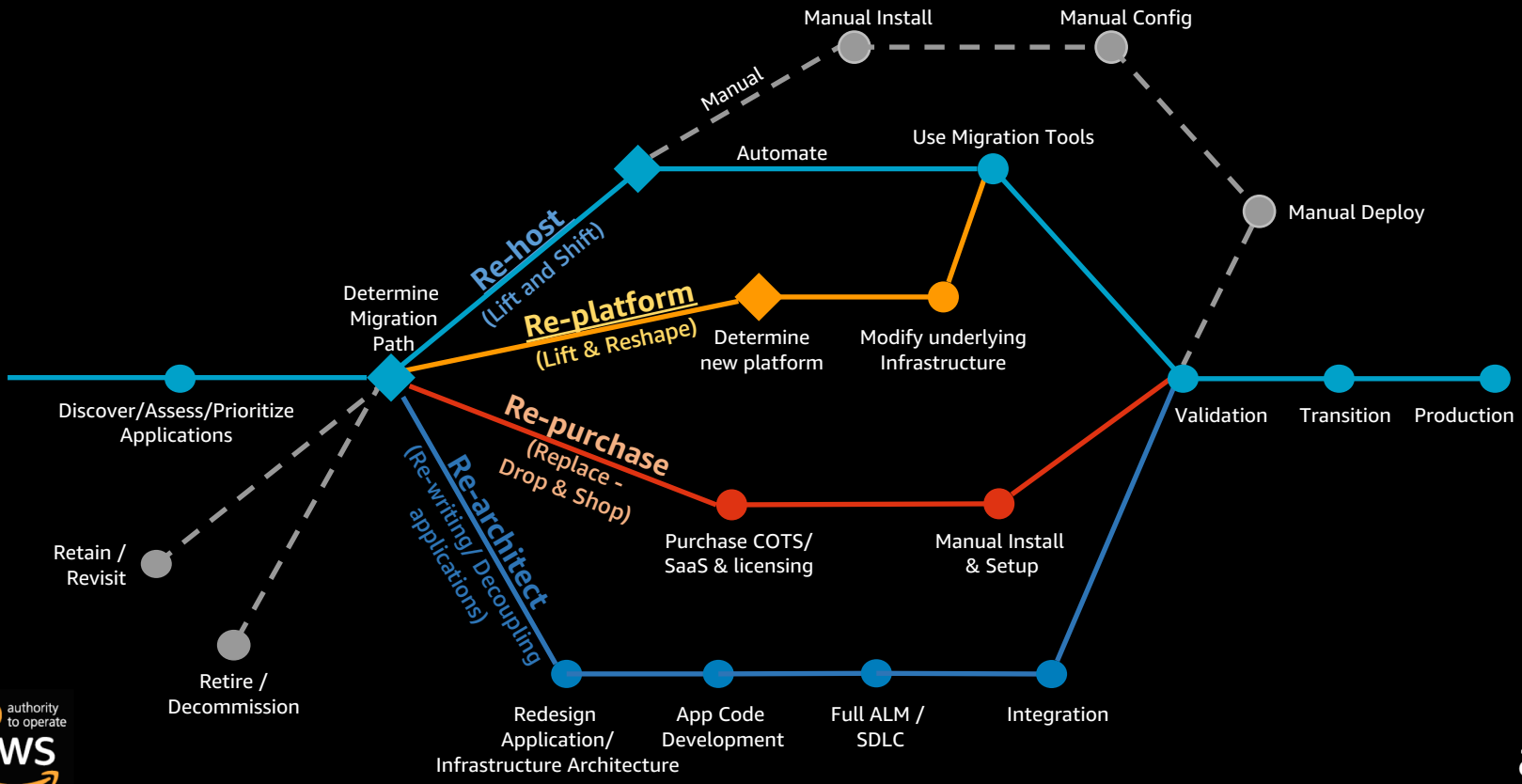
Cloud Native Architecture

- **Architect app to be cloud-native from the outset**
- Leverage the full AWS portfolio
- Truly gain all the benefits of AWS (security, scalability, cost, durability, low operational burden, etc)

ato authority to operate on aws

aws

Application migration patterns



ato authority to operate on aws

aws

Infrastructure as Code is a practice by where traditional infrastructure management techniques are supplemented and often replaced by using code based tools and software development techniques.

ato authority to operate on aws

aws

Shared responsibility model

Customer

Responsible for security **IN** the cloud

- Customer Data
- Platform, Applications, Identity & Access Management
- Operating System, Network & Firewall Configuration
- Client-side Data Encryption & Data Integrity Authentication
- Server-side Encryption (File System and/or Data)
- Network Traffic Protection (Encryption, Integrity, and/or Identity)

Compute

Responsible for security **OF** the cloud

- Compute
- Storage
- Database
- Networking

- AWS Global Infrastructure
- Regions
- Availability Zones
- Edge Locations

ato authority to operate on aws

aws

Strengthen your security posture

- Over 60 global compliance certifications and accreditations
- Benefit from AWS industry leading security teams 24/7, 365 days a year
- Security infrastructure built to satisfy military, global banks, and other high-sensitivity organizations
- Leverage security enhancements from 1M+ customer experiences

” In the last four years as we transitioned to the cloud, I have come to realize that as a relatively small organization, we can be far more secure in the cloud and achieve a higher level of assurance at a much lower cost, in terms of effort and dollars invested. We determined that security in AWS is superior to our on-premises data center across several dimensions, including patching, encryption, auditing and logging, entitlements, and compliance.

John Brady
FINRA CISO

ato authority to operate on aws

aws

Access a deep set of cloud security tools

Networking

Virtual Private Cloud
Isolated cloud resources

Web Application Firewall
Filter Malicious Web Traffic

Shield
DDoS protection

Certificate Manager
Provision, manage, and deploy SSL/TSL certificates

Encryption

Key Management Service
Manage creation and control of encryption keys

CloudHSM
Hardware-based key storage

Server-Side Encryption
Flexible data encryption options

Identity & Management

IAM
Manage user access and encryption keys

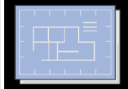
SAML Federation
SAML 2.0 support to allow on-prem identity integration

Directory Service
Host and manage Microsoft Active Directory

Organizations
Manage settings for multiple accounts

Compliance

Service Catalog
Create and use standardized products

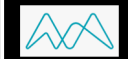


Config
Track resource inventory and changes

CloudTrail
Track user activity and API usage

CloudWatch
Monitor resources and applications

Inspector
Analyze application security

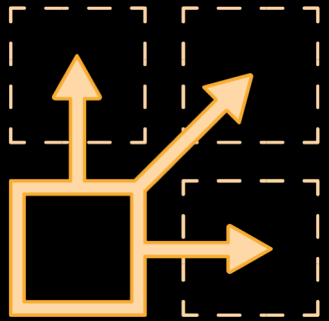


Macie
Discover, Classify & Protect data

ato authority to operate on aws

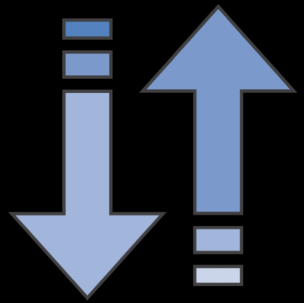
aws

Benefits

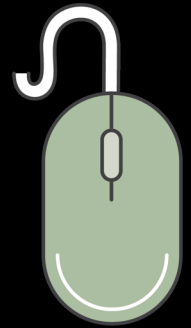


Templated resource provisioning

Infrastructure as code



Declarative and flexible



Easy to use

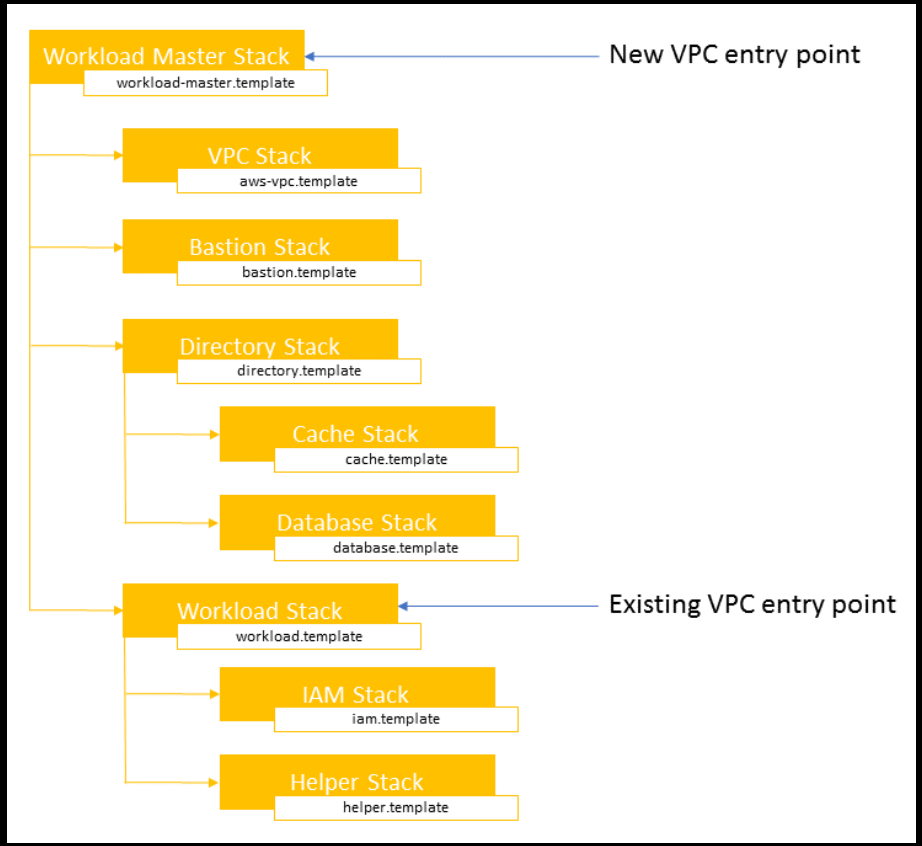
ato authority to operate on aws

aws

Modularity

Create a master template that deploys one or many nested stacks:

- This ensures that the reference is repeatable and does not change unexpectedly.
- One or more of those nested stacks will deploy the actual workload of the ATO On AWS Accelerator, while the others will be referenced as submodules
- Allows the workloads to be managed and scaled independently



ato authority to operate on aws

aws

Cloud Architecture Best Practices

1. Design for failure and nothing fails
2. Build security in every layer
3. Leverage different storage options
4. Implement elasticity

   Think parallel
6. Loose coupling sets you free
7. Don’t fear constraints

ato authority to operate on aws

aws

Design for Failure and Nothing Fails

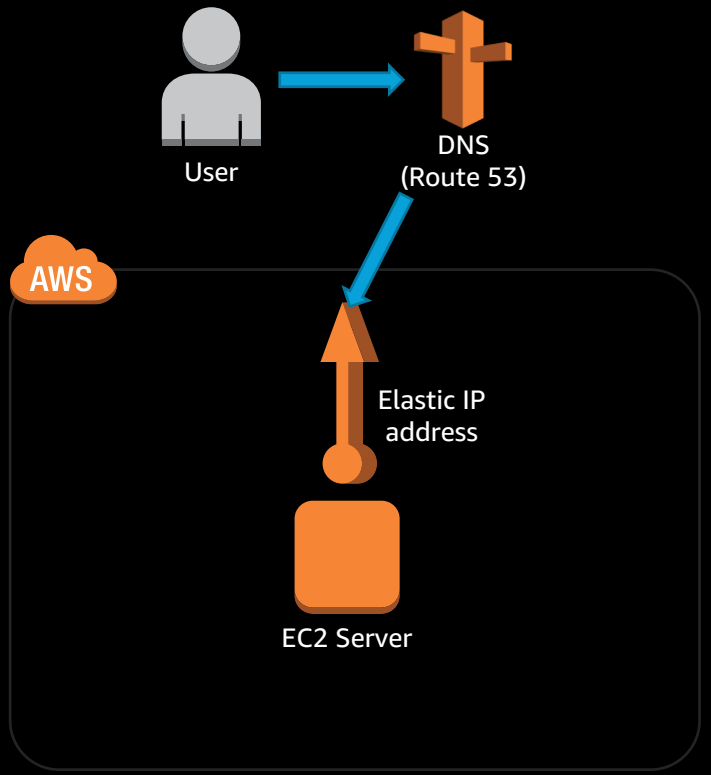
ato authority to operate on aws

aws

Design for Failure: A Single User

Single Points of Failure:

- A single Elastic IP
  - Gives a server a static Public IP address
- A single Amazon Elastic Compute Cloud (EC2) instance
  - Full stack on single host
    - Web application
    - Database
    - Management, etc…



ato authority to operate on aws

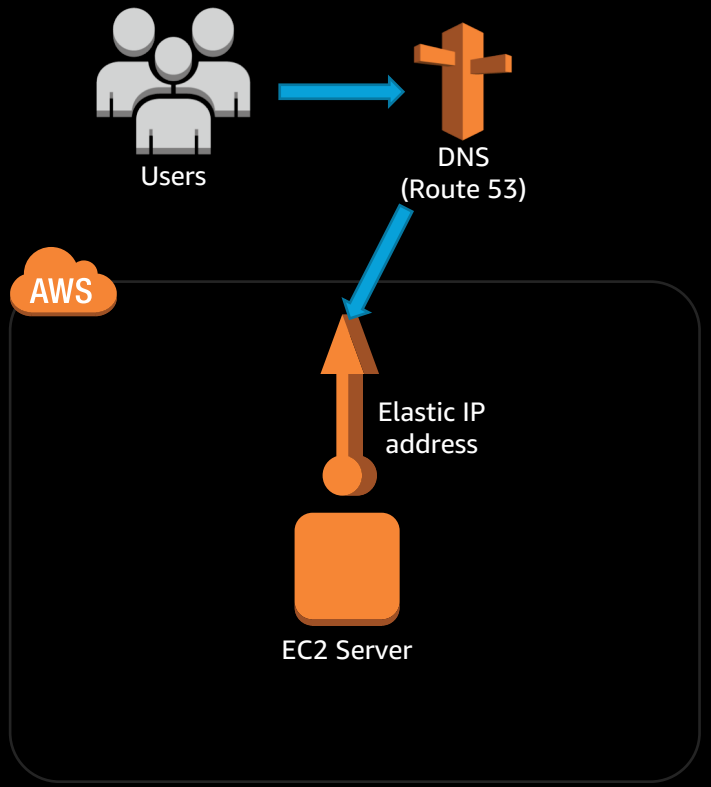
aws

Design for Failure: Difficulties Scaling to Many Users

We could potentially get to a few hundred to a few thousand users depending on application complexity and traffic, but…

There may be difficulty scaling to many more users due to:

- **All eggs in one basket**
- **No failover or redundancy**



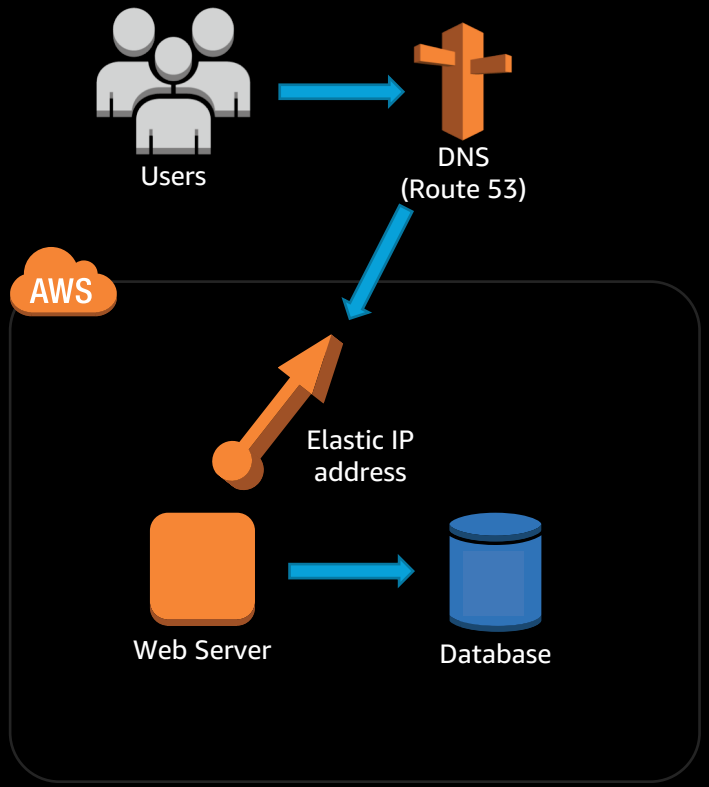
ato authority to operate on aws

aws

Design for Failure: Solving "All Eggs in One Basket"

Separate single EC2 Server into web and database tiers:

- Web Server on EC2
- Database on EC2 or RDS
  - Amazon Relational Database Service (RDS) can take care of management overhead such as patching, backups, and failure detection



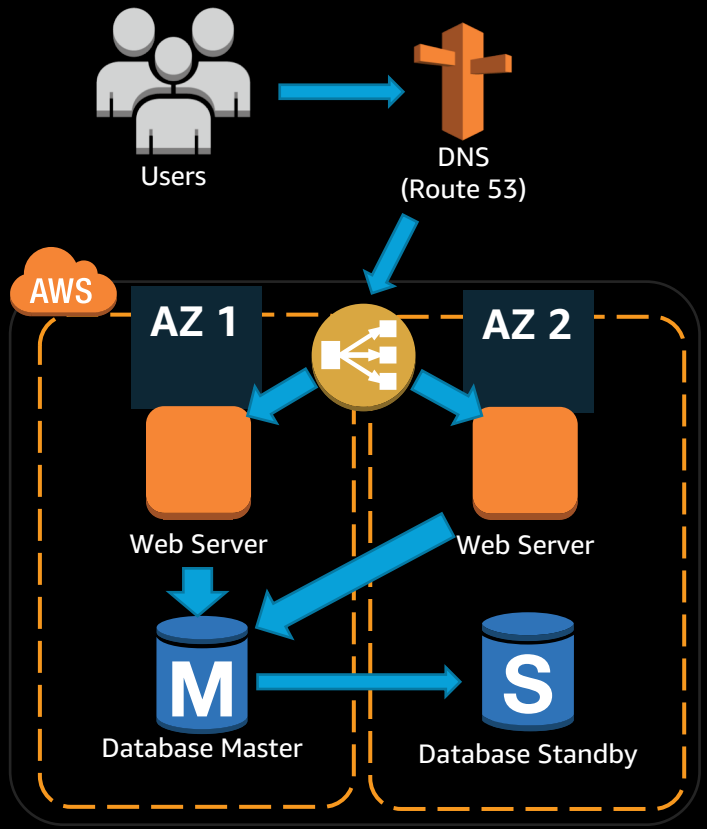
ato authority to operate on aws

aws

Design for Failure: Solving No Failover/Redundancy

Leverage multiple Availability Zones for redundancy and high availability.

- Use an Elastic Load Balancer (ELB) across AZs for availability and failover
- If using RDS, use the Multi-AZ feature for managed replication and a standby instance
    - If not, use failover and replication features native to your database engine

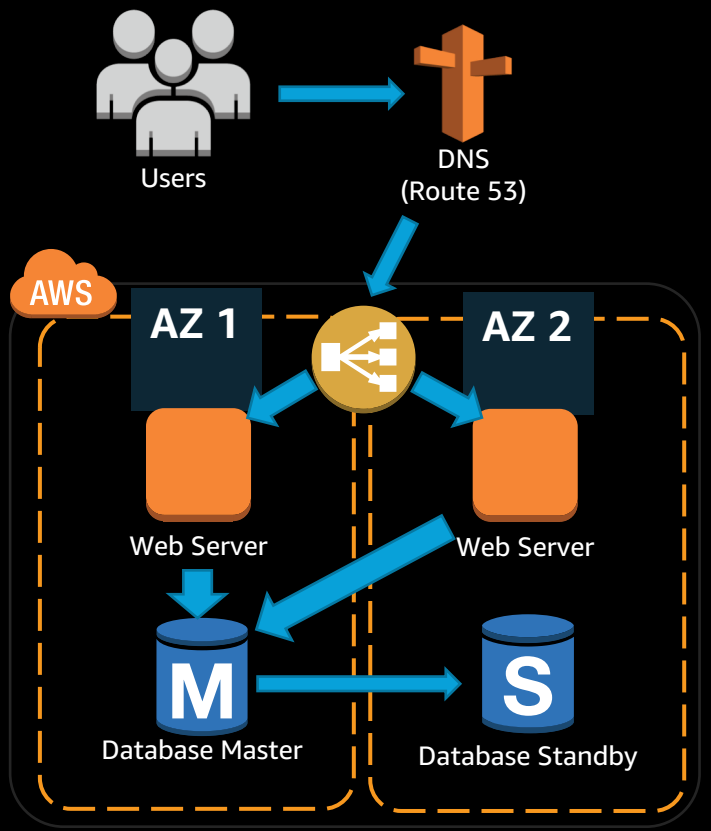


ato authority to operate on aws
aws

Design for Failure: Best Practices

Best Practices:

- Eliminate single points of failure
- Use multiple Availability Zones
- Use Elastic Load Balancing
- Do real-time monitoring with CloudWatch
- Create a database standby across Availability Zones



ato authority to operate on aws
aws

Design for Failure

Avoid single points of failure

Assume everything fails and design backwards

- When, not if, an individual component fails, the application does not fail
  - Think of your servers as cattle, not pets
- Leverage Route 53 DNS Pilot-light or Warm-standby strategies to implement Disaster Recovery
- Auto Scaling groups can be used to detect failures and self-heal, thus protecting against AZ level outages

ato authority to operate on aws

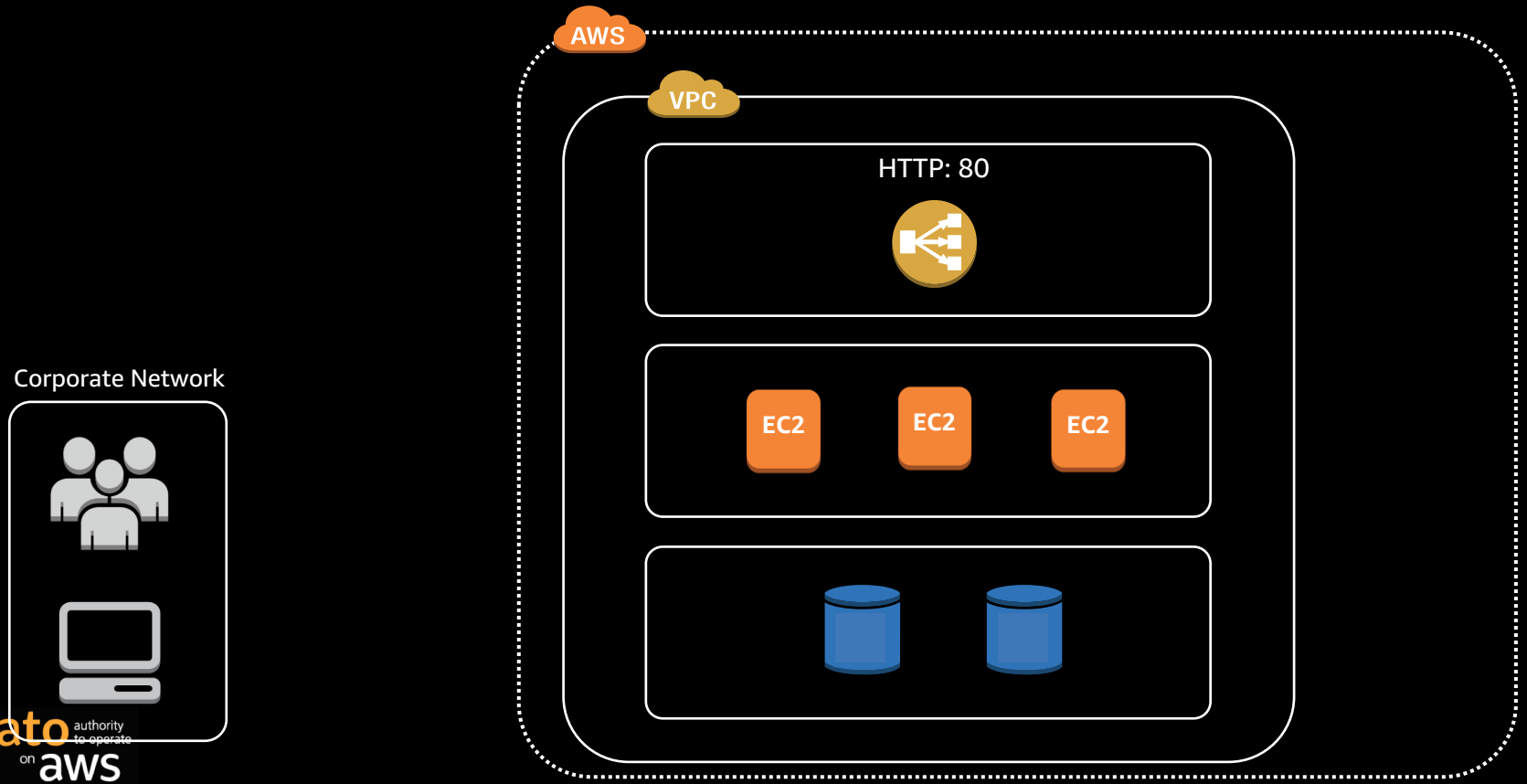
aws

Build Security in Every Layer

ato authority to operate on aws

aws

Build Security in Every Layer

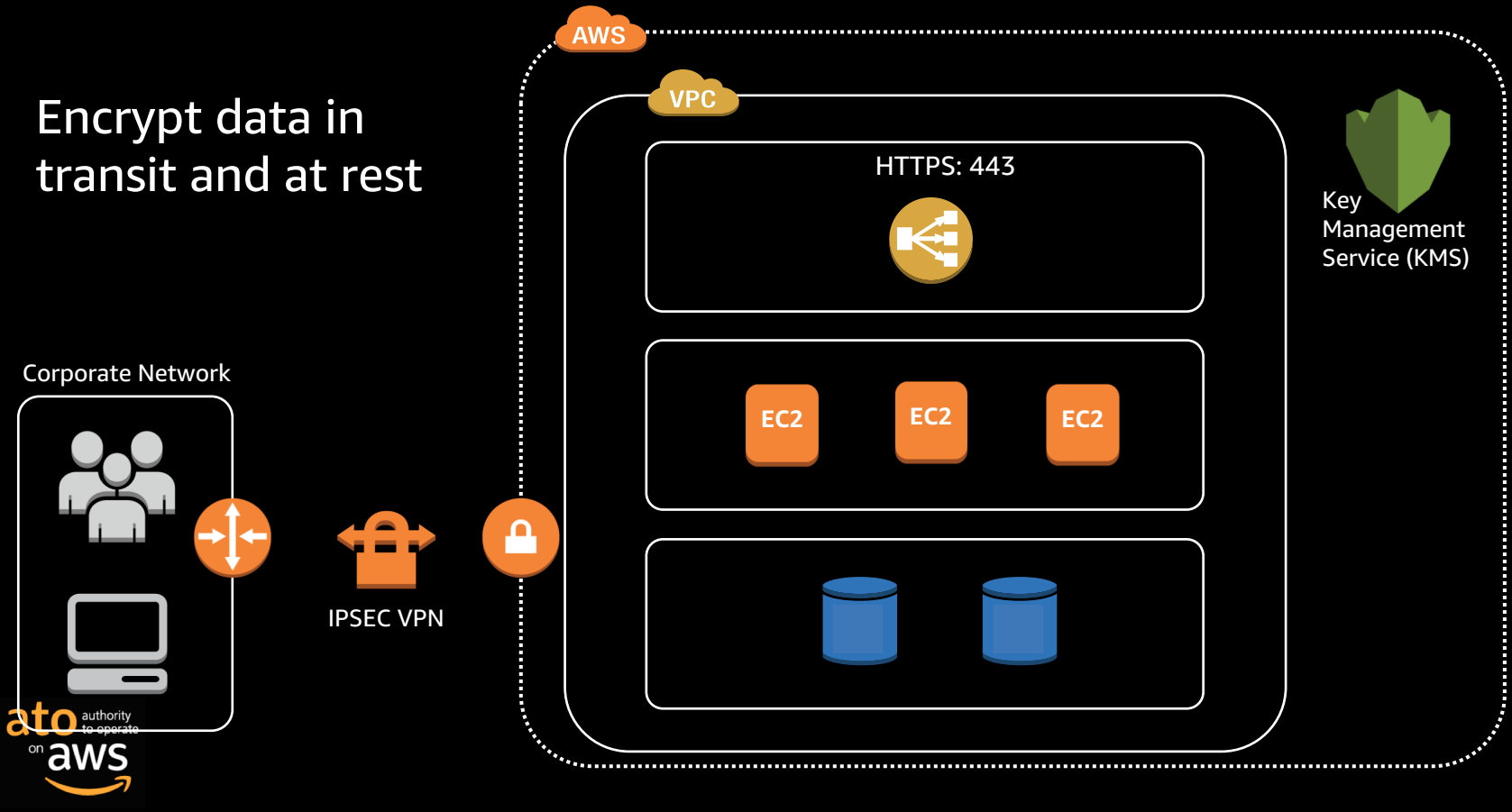


ato authority to operate on aws

aws

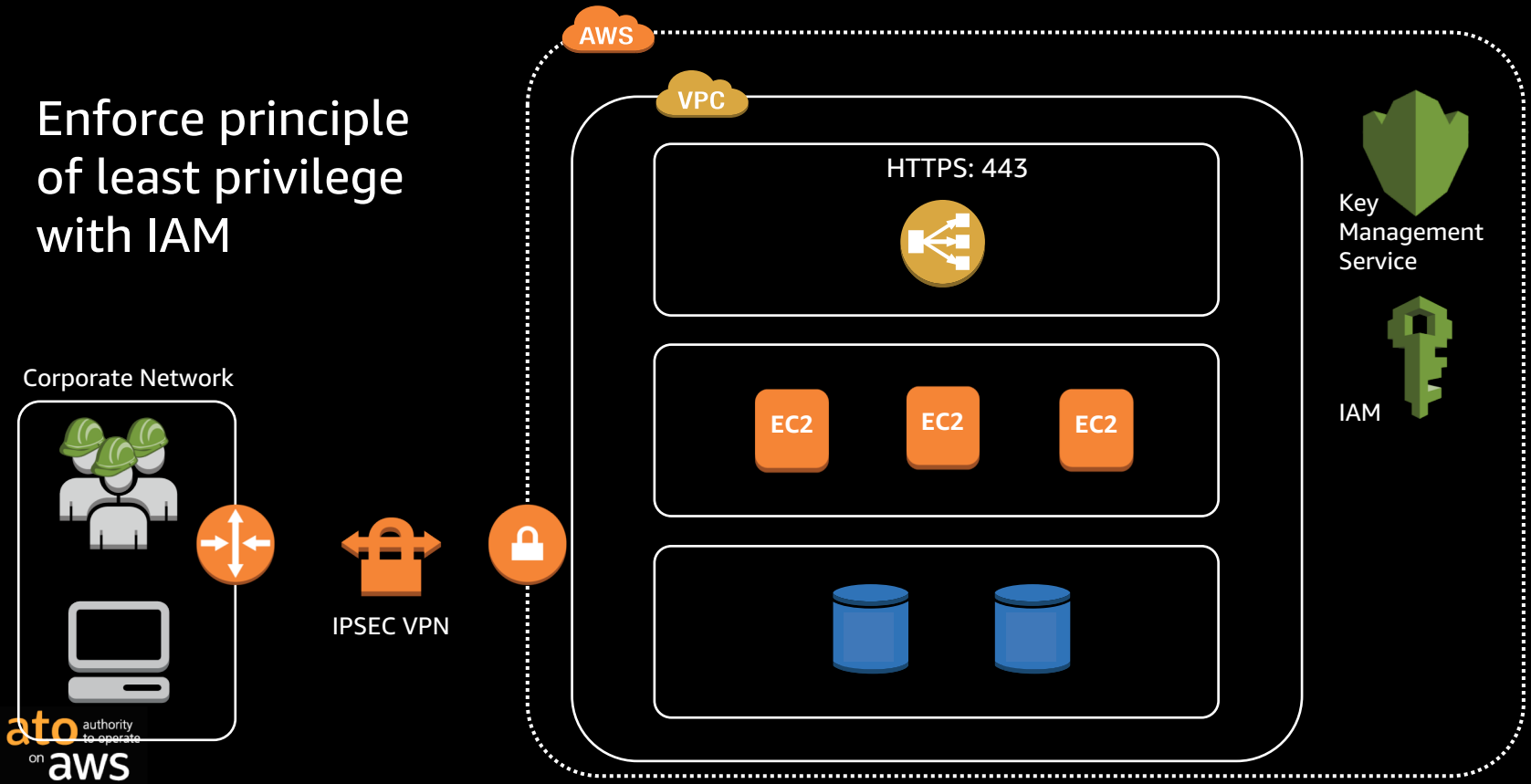
Build Security in Every Layer

Encrypt data in transit and at rest



Build Security in Every Layer

Enforce principle of least privilege with IAM

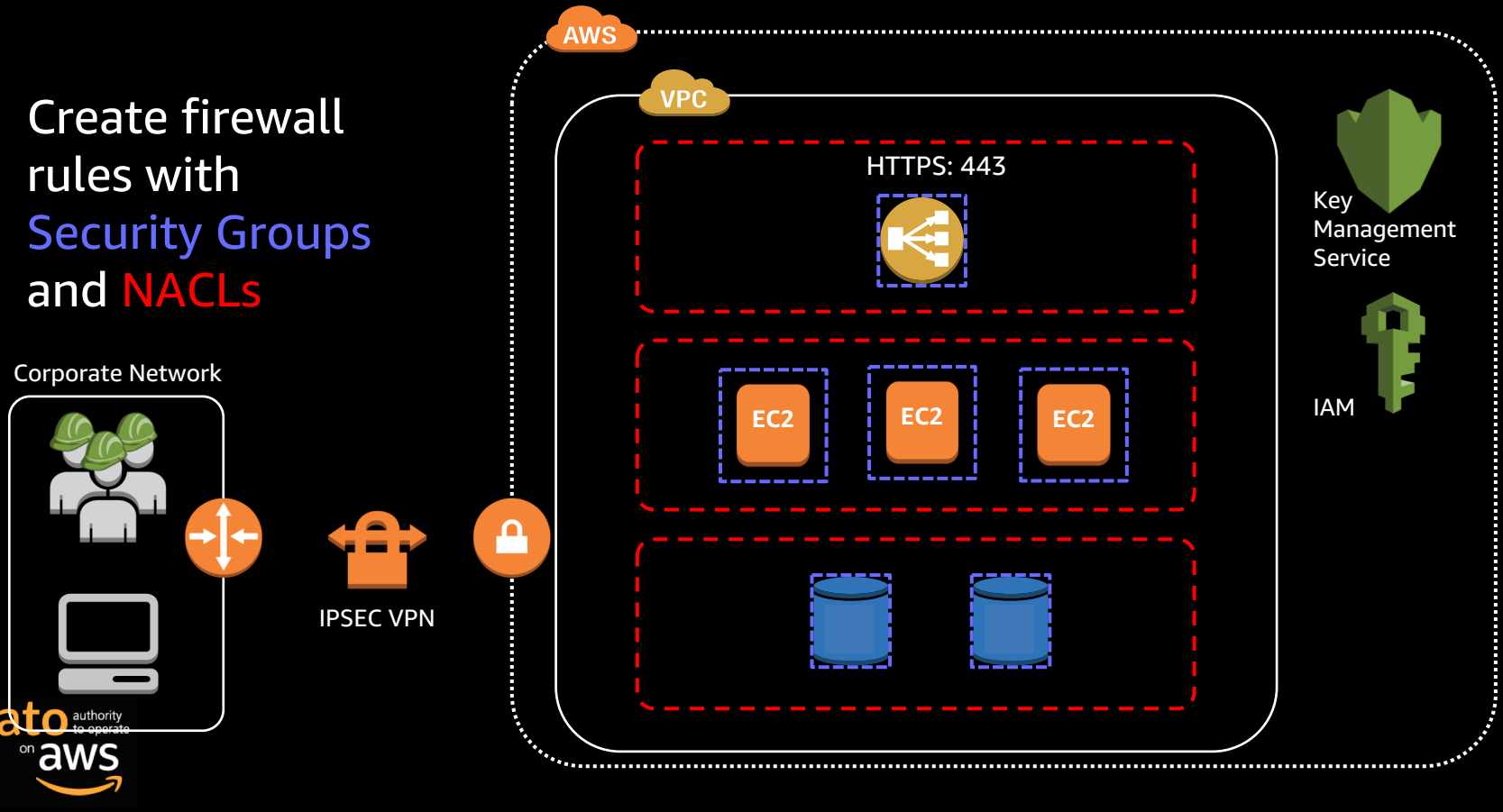


ato authority to operate on aws

aws

Build Security in Every Layer

Create firewall rules with Security Groups and NACLs



ato authority to operate on aws

aws

Build Security in Every Layer

More Tools for your Security Toolbox:

- Amazon Inspector
- Amazon Certificate Manager
- AWS Shield
- AWS Web Application Firewall (WAF)
- AWS Config

ato authority to operate on aws

aws

Leverage Many Storage Options

ato authority to operate on aws

aws

Leverage Many Storage Options

One size does NOT fit all

- **Amazon Elastic Block Storage (EBS)** – persistent block storage
- **Amazon EC2 Instance Storage** – ephemeral block storage
- **Amazon RDS –** managed relational database
- **Amazon CloudFront** – content distribution network
- **Amazon S3** – object/blob store, good for large objects
- **Amazon DynamoDB** – non-relational data (key-value)
- **Amazon ElastiCache** – managed Redis or Memcached

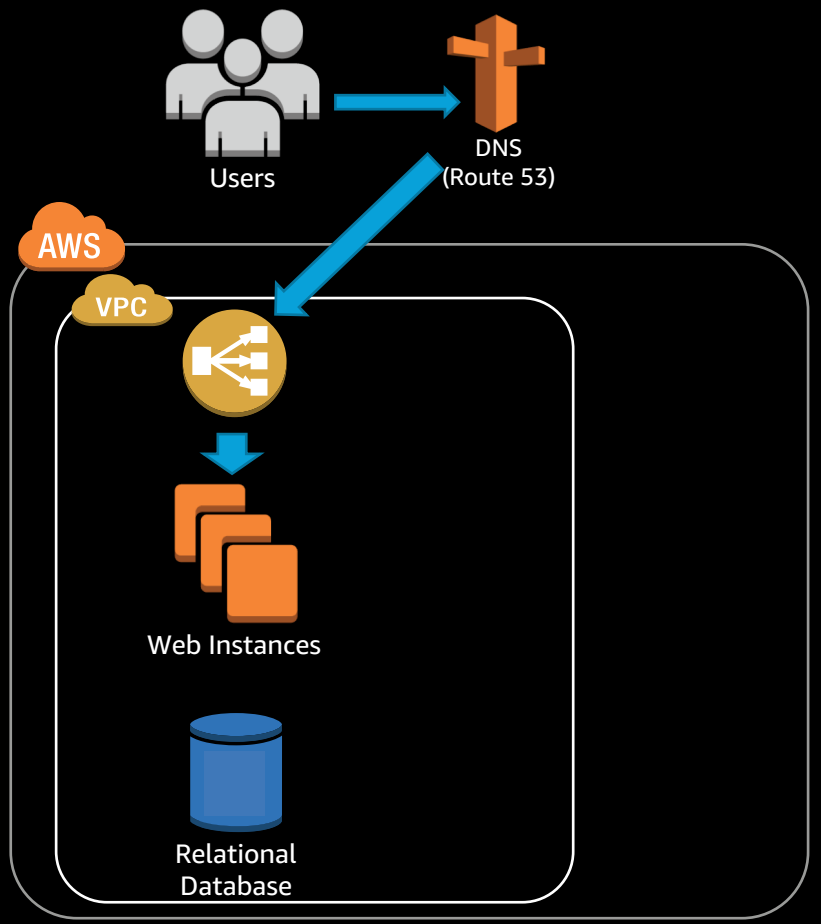
ato authority to operate on aws

aws

Leverage Many Storage Options

Current State:

- All load handled by one stack
  - Elastic Load Balancer (ELB)
  - EC2 Web App cluster
  - Relational Database
- No caching layer(s)
- All persistent data in database or Web instances' Elastic Block Storage (EBS) volumes



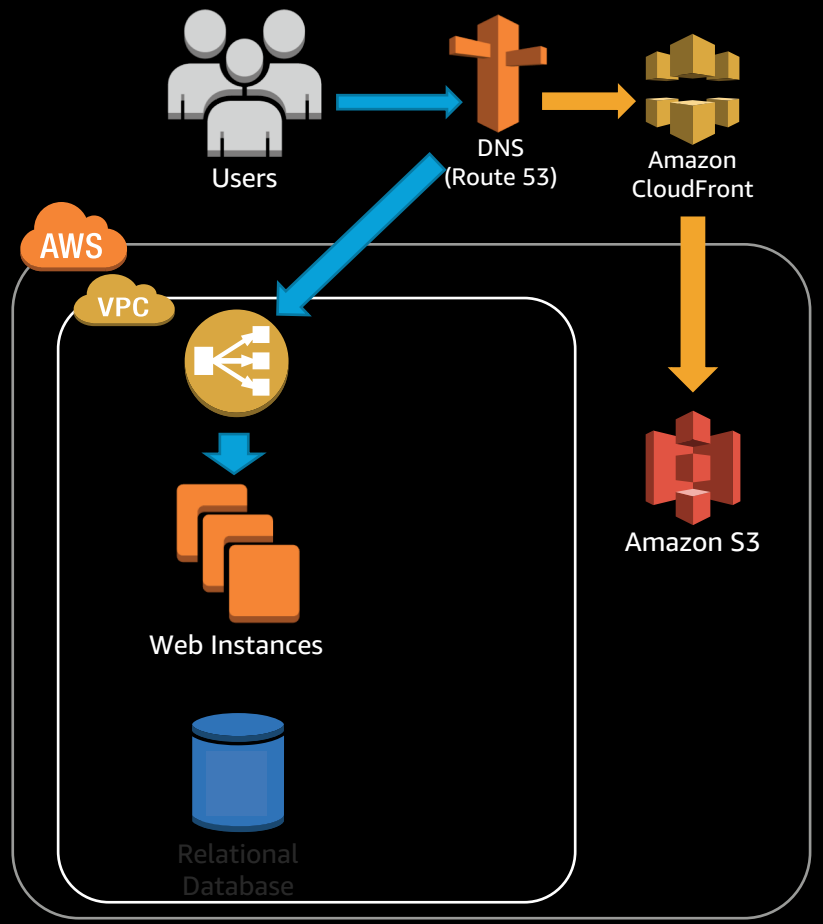
ato authority to operate on aws

aws

Leverage Many Storage Options

Offload and cache requests for static assets:

- Store large/static objects in Simple Storage Service (S3)
- Use a Content Delivery Network (CDN) like CloudFront to cache responses using points of presence all around the world



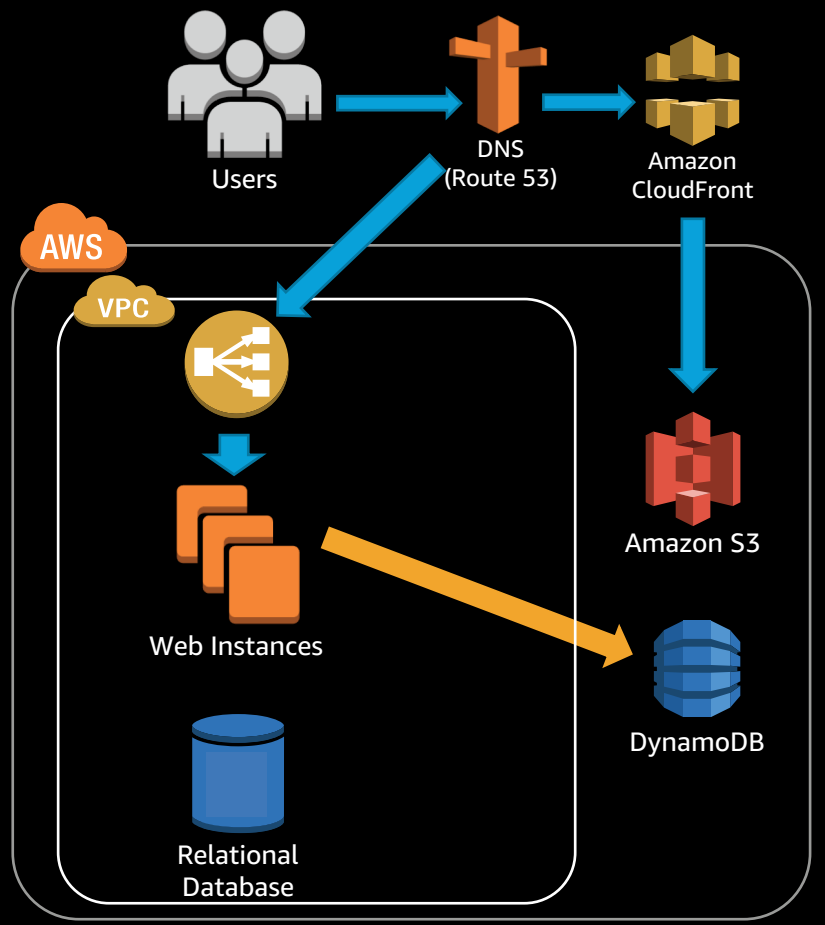
ato authority to operate on aws

aws

Leverage Many Storage Options

Save user session data in a database to avoid interrupting the user experience if a web host becomes unresponsive:

- Store session/state data in DynamoDB, a managed NoSQL key-value store

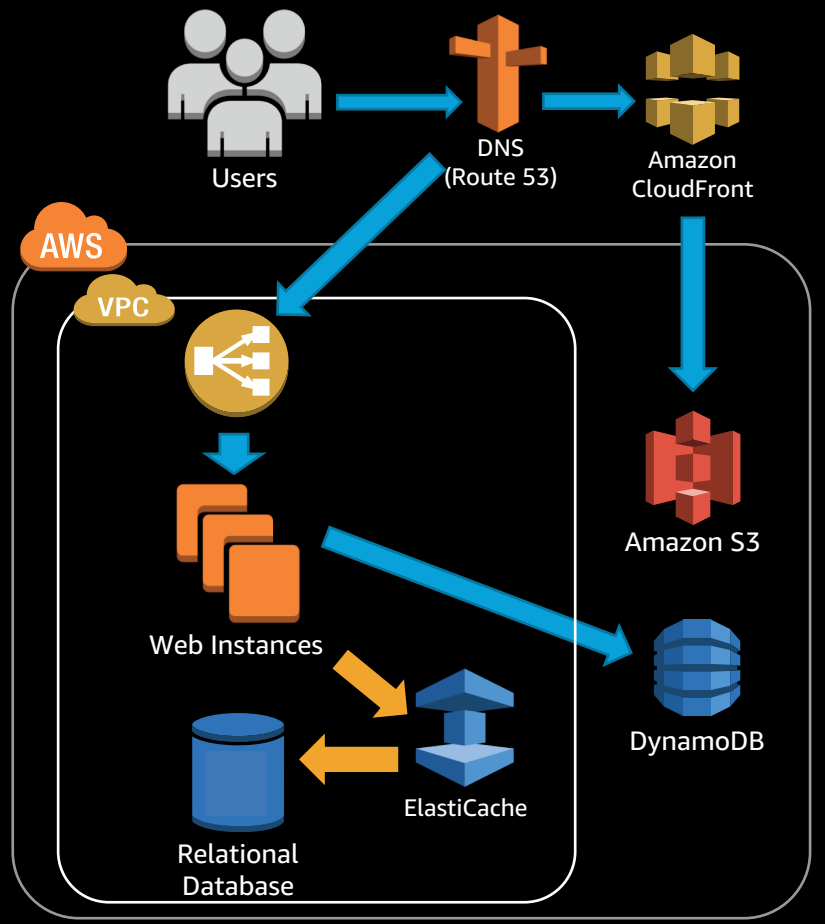


ato authority to operate on aws
aws

Leverage Many Storage Options

Cache frequent queries to shift the load off of your database:

- Put ElastiCache as a caching layer between the web hosts and the database



ato authority to operate on aws

aws

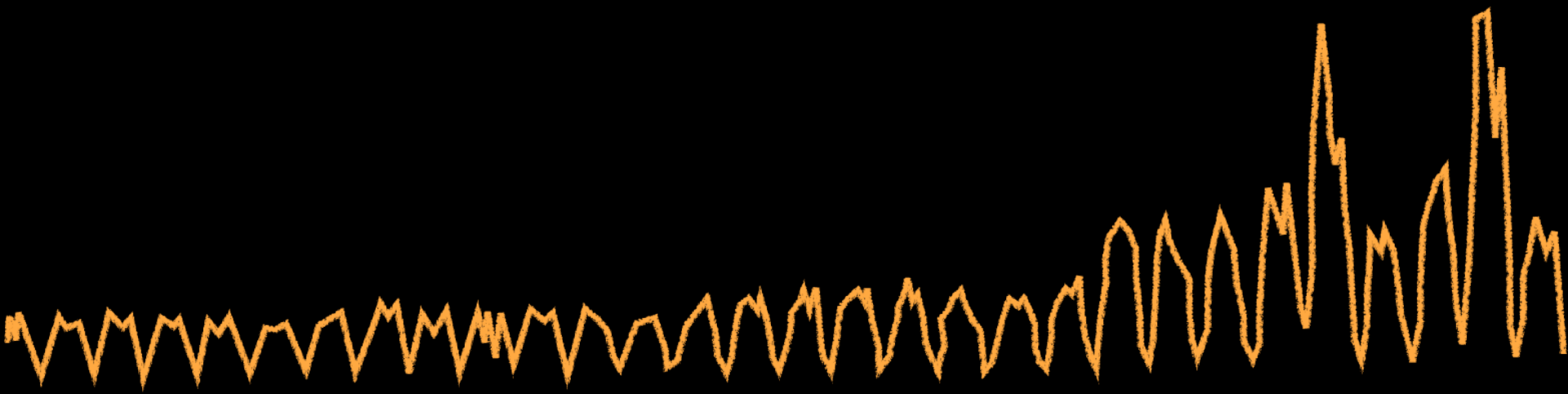
Implement Elasticity

ato authority to operate on aws

aws

November traffic to Amazon.com

Provisioned capacity

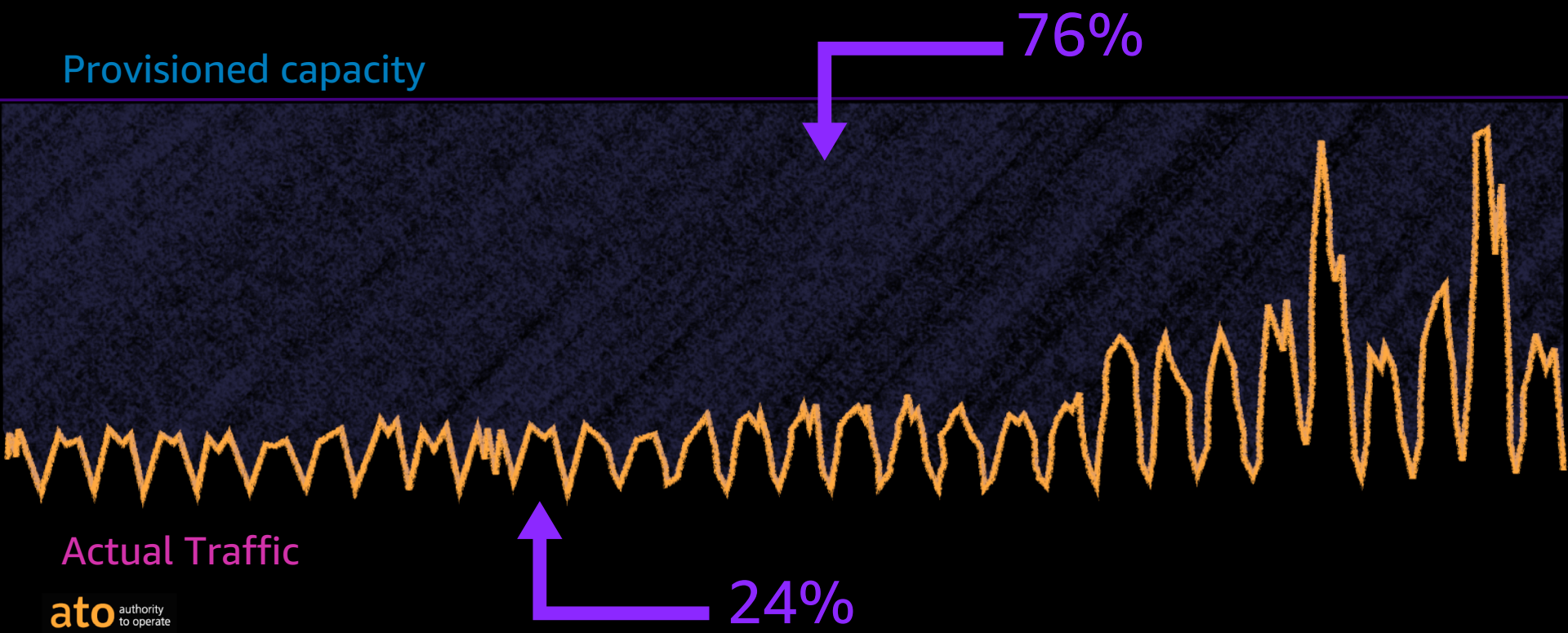


Actual Traffic

ato authority to operate on aws

aws

November traffic to Amazon.com

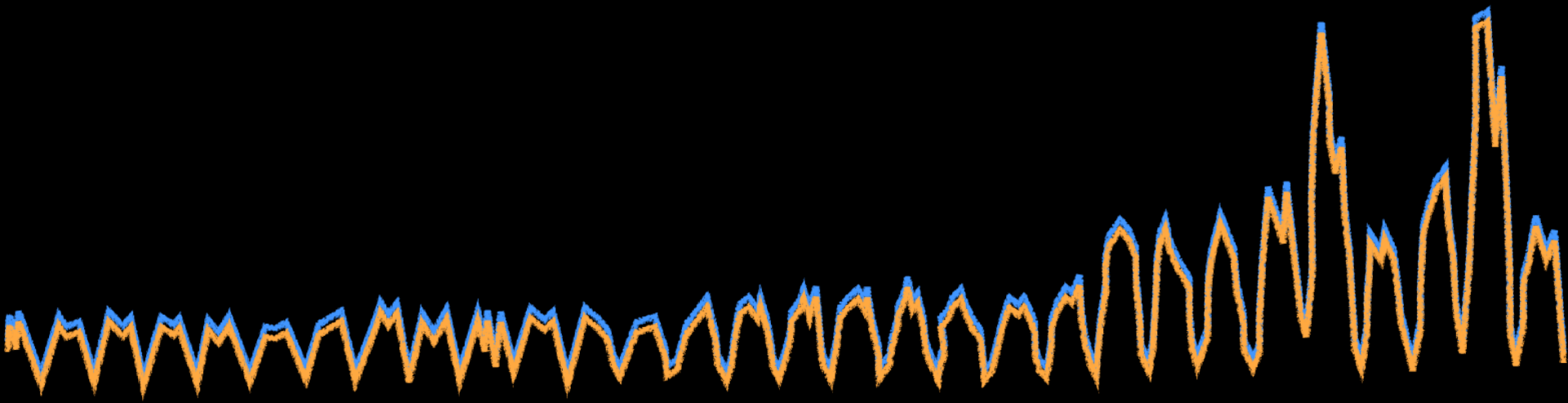


ato authority to operate on aws

aws

November traffic to Amazon.com

Provisioned capacity



Actual Traffic

ato authority to operate on aws

aws

Implement Elasticity

How To Guide:

- Write Auto Scaling policies with your specific application access patterns in mind
- Prepare your application to be flexible: don't assume the health, availability, or fixed location of components
- Architect resiliency to reboot and relaunch
    - When an instance launches, it should ask "*Who am I and what is my role?*"
- Leverage highly scalable, managed services such as S3 and DynamoDB

ato authority to operate on aws

aws

Think Parallel

ato authority to operate on aws

aws

Think Parallel

Scale Horizontally, Not Vertically

- Decouple compute from state/session data
- Use ELBs to distribute load
- Break up big data into pieces for distributed processing
    - AWS Elastic Map Reduce (EMR) – managed Hadoop

ato authority to operate on aws

aws

Think Parallel

Faster doesn’t need to mean more expensive

- With EC2 On Demand, the following will cost the same:
  - 12 hours of work using 4 vCPUs
  - 1 hour of work using 48 vCPUs
- Right Size your infrastructure to your workload to get the best balance between cost and performance

ato authority to operate on aws

aws

Think Parallel

Parallelize using native managed services

- Get the best performance out of S3 with parallelized reads/writes
  - Multi-part uploads (API) and byte-range GETs (HTTP)
- Take on high concurrency with Lambda
  - Initial soft limit: 1000 concurrent requests per region

ato authority to operate on aws

aws

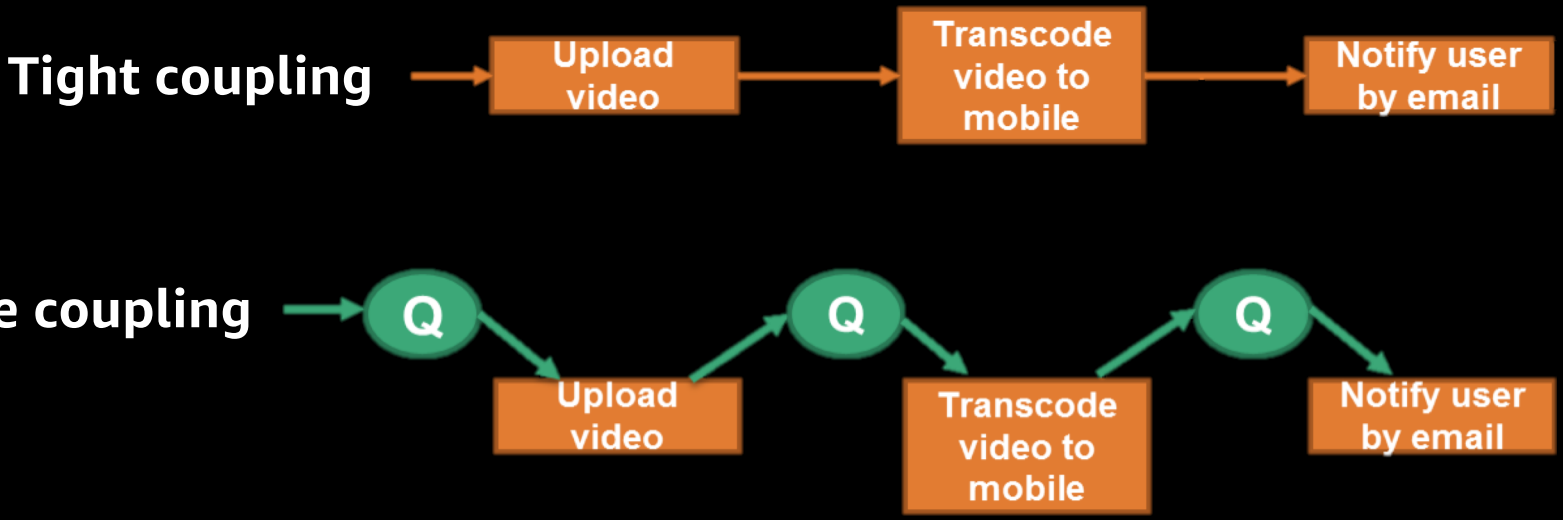
Loose Coupling Sets You Free

ato authority to operate on aws

aws

Loose Coupling Sets You Free: Queueing

Use Amazon Simple Queue Service (SQS) to pass messages between loosely coupled components



ato authority to operate on aws
aws

Loose Coupling Sets You Free: Don't Reinvent the Wheel

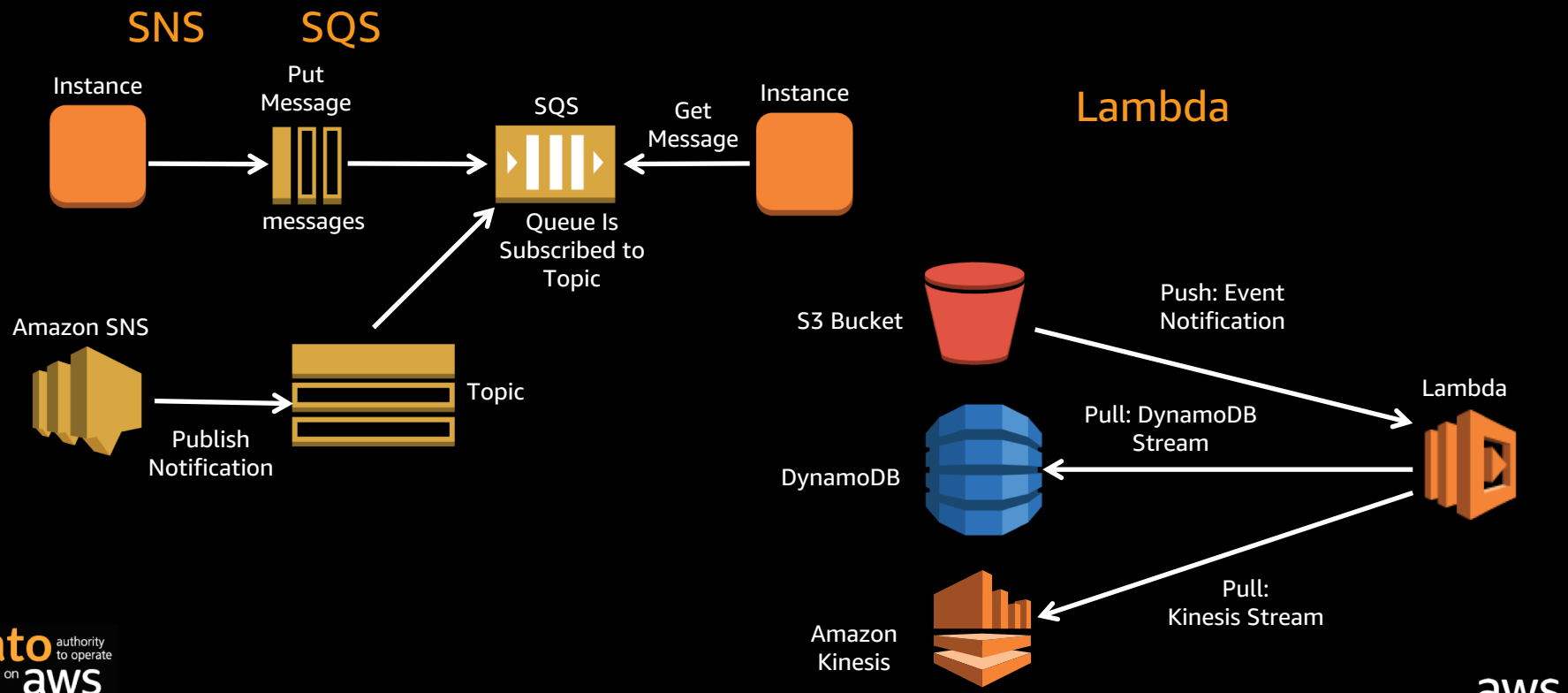
Nearly everything in AWS is an API call. Leverage AWS Native Services for…

- Queuing
- Transcoding
- Search
- Databases
- Email
- Monitoring
- Metrics
- Logging
- Compute

ato authority to operate on aws

aws

Loose Coupling Sets You Free



ato authority to operate on aws

aws

Don’t Fear Constraints

ato authority to operate on aws

aws

Don’t Fear Constraints

Rethink traditional architectural constraints

Need more RAM?

- Don’t: vertically scale
- Do: distribute load across machines or a shared cache

Need better IOPS for database?

- Don’t: rework schema/indexes or vertically scale
- Do: create read replicas, implement sharding, add a caching layer

Hardware failed or config got corrupted?

- Don’t: waste production time diagnosing the problem
- Do: “Rip and replace” – stop/terminate old instance and relaunch

Need a Cost Effective Disaster Recovery (DR) strategy?

- Don’t: double your infrastructure costs when you don’t need to
- Do: implement Pilot Light or Warm Standby DR stacks

ato authority to operate on aws

aws

Any Questions?

ato authority to operate on aws

aws