MASTERCLASS SERIES

AMAZON EC2

#awswebinar

MASTERCLASS SERIES

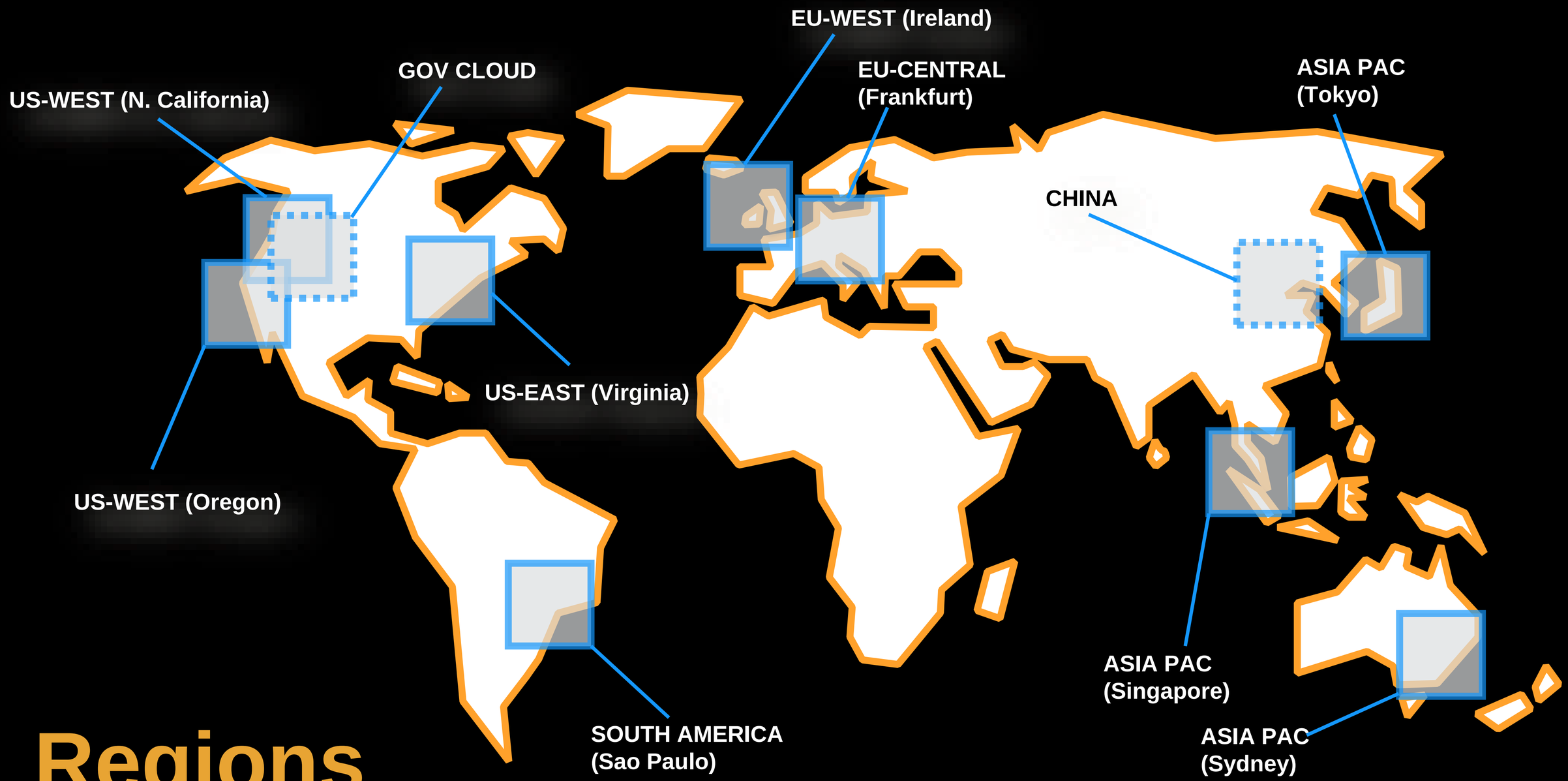
A technical deep dive beyond the basics
Help educate you on how to get the best from AWS technologies
Show you how things work and how to get things done
Broaden your knowledge in less than an hour

AMAZON
ELASTIC COMPUTE CLOUD
(EC2)

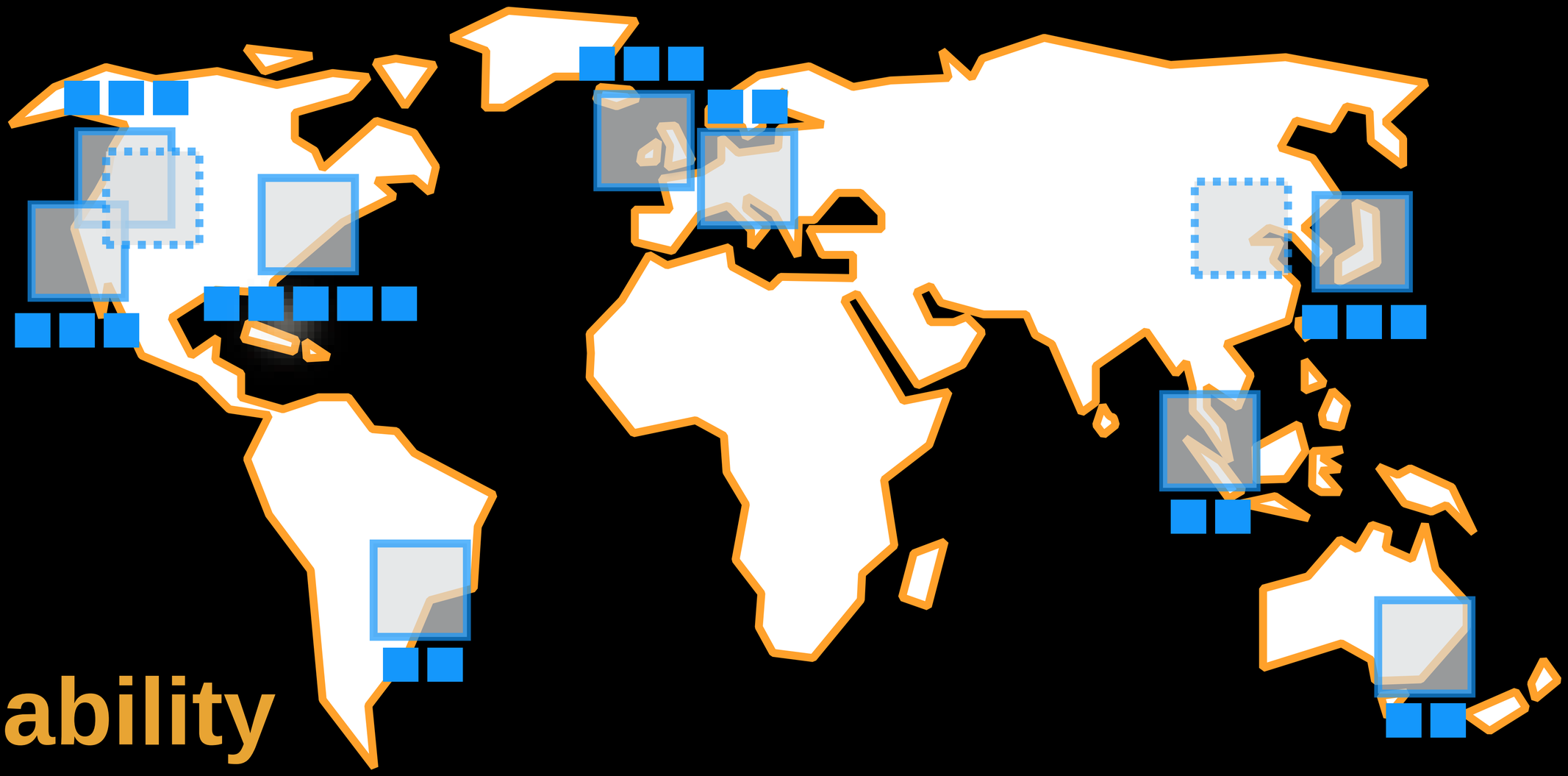
What we'll see

Instances
Storage
Network
Monitoring & Logs
Security & Access Control
Management Tools
Deployment
Cost Optimization
3rd Party Tools

INSTANCE


EU-WEST (Ireland)
GOV CLOUD
EU-CENTRAL
(Frankfurt)
ASIA PAC
(Tokyo)
US-WEST (N. California)
CHINA
US-EAST (Virginia)
US-WEST (Oregon)
ASIA PAC
(Singapore)
SOUTH AMERICA
(Sao Paulo)
ASIA PAC
(Sydney)

Regions



Availability Zones

Amazon EC2

Instance Families

Compute-Optimized

General Purpose

Burstable Performance

Memory-Optimized

Storage-Optimized

GPU Instances

Amazon EC2

Instance Generations

C1 / CC2 / C3 / C4

M1 / M3

T1 / T2

M2 / CR1 / R3

HI1 / I2 / HS1

G2

Amazon EC2

Instance Sizes

large

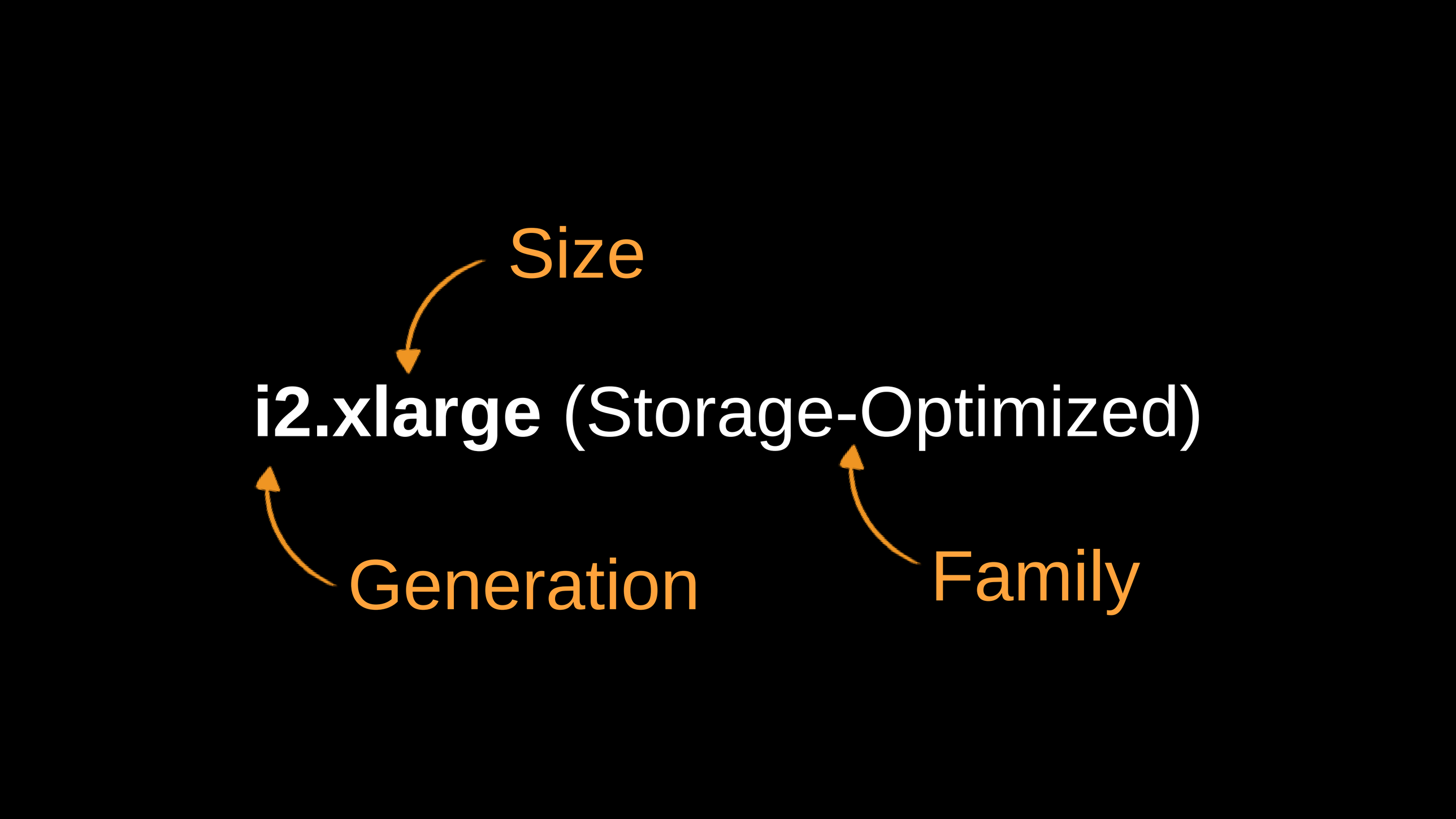
medium

micro

xlarge

xlarge

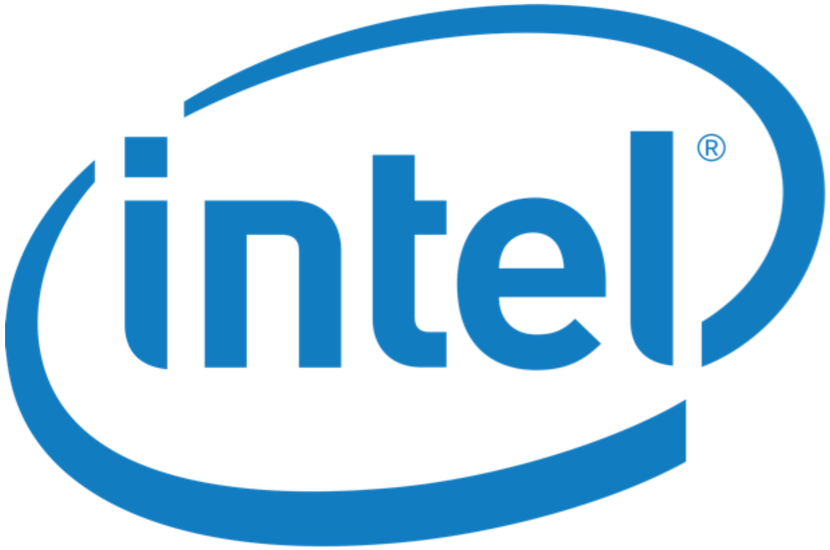
2xlarge


Size
i2.xlarge (Storage-Optimized)
Generation
Family

T2: Low Cost EC2 Instances with Burstable Performance

Instance Type	vCPUs	Mem (GiB)	Baseline Performance	CPU Credits / Hour
t2.micro	1	1.0	10%	6
t2.small	1	2.0	20%	12
t2.medium	2	4.0	40%	24

C4: Highest Compute Performance on Amazon EC2



Intel Xeon E5-2666 v3
Code name Haswell

2.9 GHz, up to 3.5 GHz
Max Turbo Frequency

Custom Processor
Optimized for EC2

C4: Highest Compute Performance on Amazon EC2

Instance Type	vCPUs	Mem (GiB)	Networking Performance	Dedicated EBS Throughput (Mbps)
c4.large	2	3.75	Moderate	500
c4.xlarge	4	7.5	Moderate	750
c4.2xlarge	8	15	High	1,000
c4.4xlarge	16	30	High	2,000
c4.8xlarge	36	60	10 Gigabit	4,000

HVM

Hardware Virtual Machine virtualization

Allows the guest VM to run as though it is on a native hardware platform

Enhanced Networking (SR-IOV)

PV

Paravirtual virtualization

Guests run a modified operating system that does not use hardware emulation

Amazon EC2

VM Import / Export

Easily **import** virtual machine images
from your existing environment
to Amazon EC2 instances
and **export** them back
to your on-premises environment

Amazon EC2

VM Import

VMware ESX and VMware Workstation VMDK images
Citrix Xen VHD images
Microsoft Hyper-V VHD images

Windows Server
Red Hat Enterprise Linux (RHEL) - using Cloud Access
CentOS
Ubuntu
Debian

Amazon EC2

VM Export

You can export previously imported EC2 instances to

VMware ESX VMDK
VMware ESX OVA
Microsoft Hyper-V VHD
Citrix Xen VHD

file formats

Amazon EC2

```
$ curl http://169.254.169.254/latest/meta-data/

ami-id
ami-launch-index
ami-manifest-path
block-device-mapping/
hostname
instance-action
instance-id
instance-type
kernel-id
local-hostname
local-ipv4
mac
network/
placement/
public-hostname
public-ipv4
public-keys/
reservation-id
security-groups
services/

$ curl http://169.254.169.254/latest/user-data

…
```

Instance Metadata

Amazon EC2
User Data

Linux

```
#!…
```

E.g.

```
#!/bin/bash
yum update -y
```

Windows

```
<script>…</script>
```

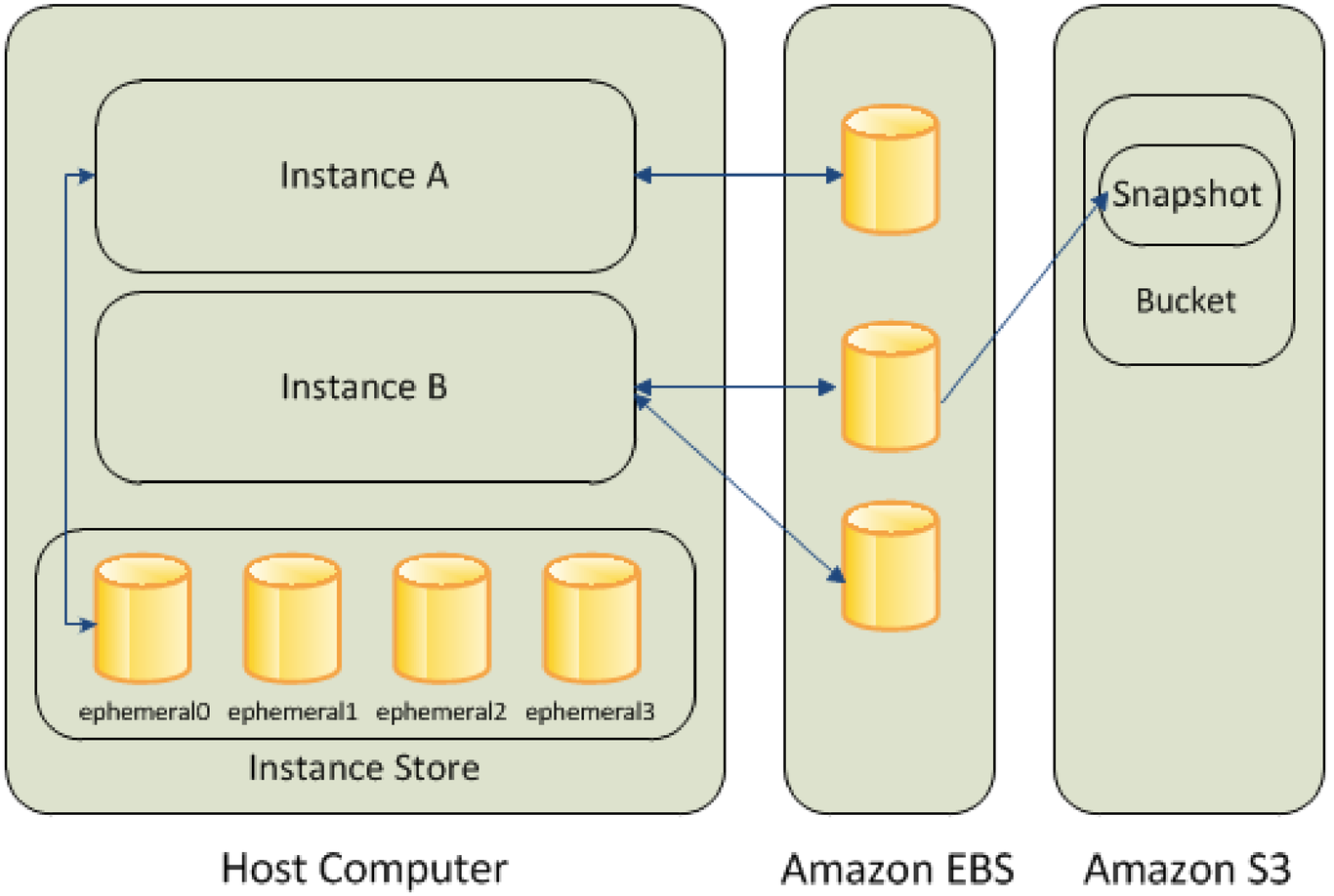
or

```
<powershell>…</powershell>
```

STORAGE

Amazon EC2

Data Storage Options



Instance Store

Physically attached
to the host computer

Type and amount differs
by instance type

Data **dependent** upon
instance lifecycle

Amazon EBS

Persistent block level
storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of
instance lifecycle

Instance Store

Physically attached
to the host computer

Type and amount differs
by instance type

Data **dependent** upon
instance lifecycle

Instance store data **persists** if:

- The OS in the instance is rebooted
- The instance is restarted

Instance store data is **lost** when:

- An underlying instance drive fails
- An EBS-backed instance is stopped
- The instance is terminated

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

EBS Volumes

EBS volumes automatically **replicated** within the **Availability Zone (AZ)** in which are created

Use EBS-optimized instances to deliver **dedicated throughput** between Amazon EC2 and Amazon EBS, with options between 500 and 4,000 Mbps, depending on the instance type

EBS Volumes

EBS volumes **attached** to a running instance automatically detach from the instance with their data intact when that instance is terminated.

EBS volumes created and attached to an instance at **launch** are deleted when that instance is terminated. You can modify this behavior by changing the value of the flag **DeleteOnTermination**.

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

EBS Snapshots

An EBS snapshot is a **point-in-time backup copy** of an EBS volume that is stored in Amazon S3

Snapshots are **incremental**, only the blocks that have changed after your most recent snapshot are saved

EBS Snapshots

When you delete a snapshot, only the data **exclusive** to that snapshot is removed

Can be **shared** across AWS accounts or **copied** across AWS regions

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

EBS Encryption

Data stored at rest on the volume, disk I/O, and snapshots created from the volume are **all** encrypted

The encryption occurs on the servers that **host** Amazon EC2 instances, providing encryption of **data-in-transit** from EC2 instances to EBS storage

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

Amazon EBS

Persistent block level storage volumes

Magnetic
General Purpose (SSD)
Provisioned IOPS (SSD)

Data **independent** of instance lifecycle

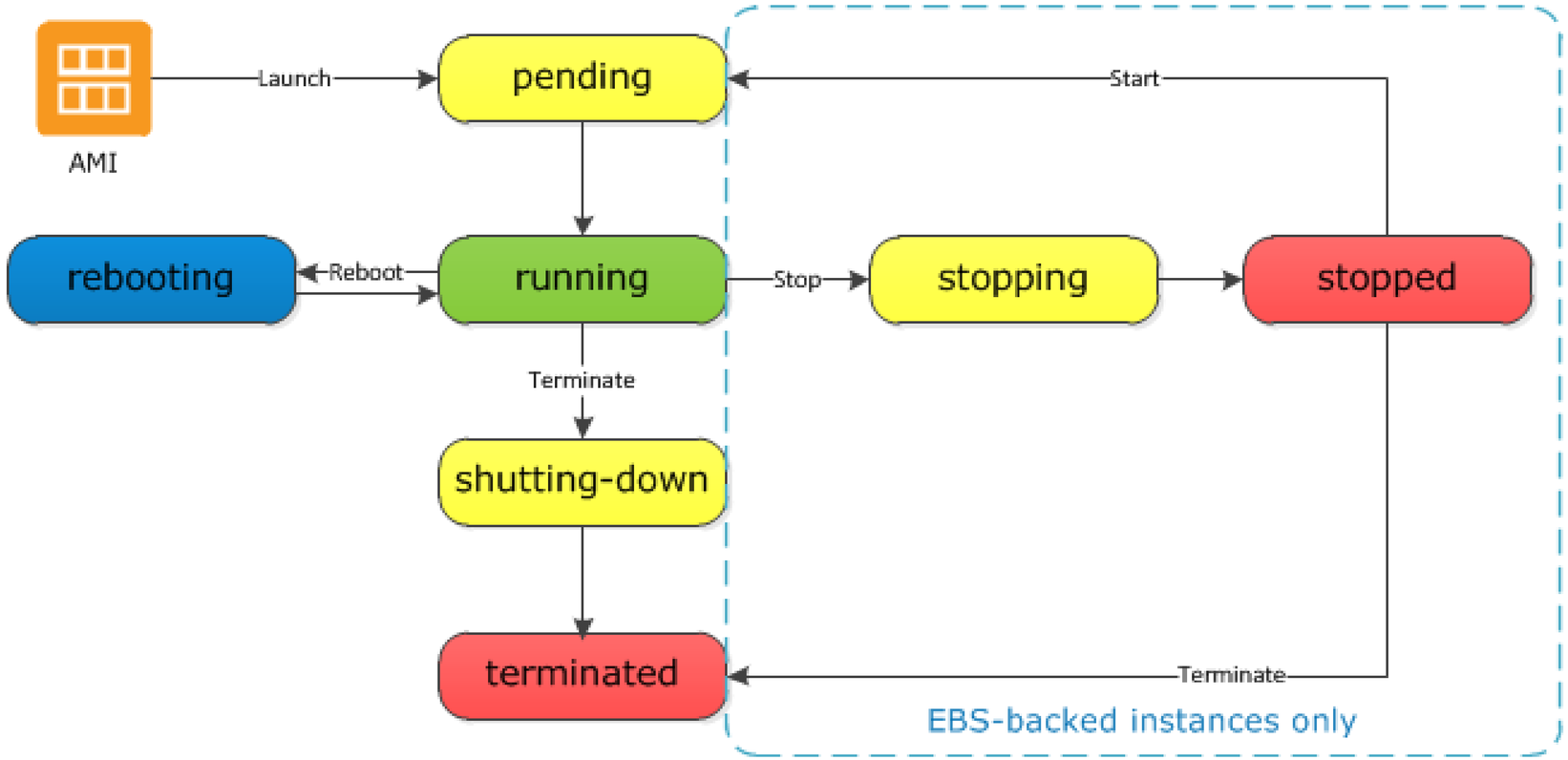
EBS Encryption

Uses **AWS Key Management Service** (AWS KMS) master keys unless you select a **Customer Master Key** (CMK).

Creating **your own CMK** gives you the ability to create, rotate, disable, define access controls, and audit the encryption keys.

Amazon EC2

Instance Lifecycle



New EBS Volumes: Larger & Faster

General Purpose (SSD)

Up to 16TB
10,000 IOPS (burst)
Up to 160 MBps

Provisioned IOPS (SSD)

Up to 16TB
20,000 IOPS
Up to 320 MBps

NETWORK

NETWORK

VIRTUAL PRIVATE CLOUD

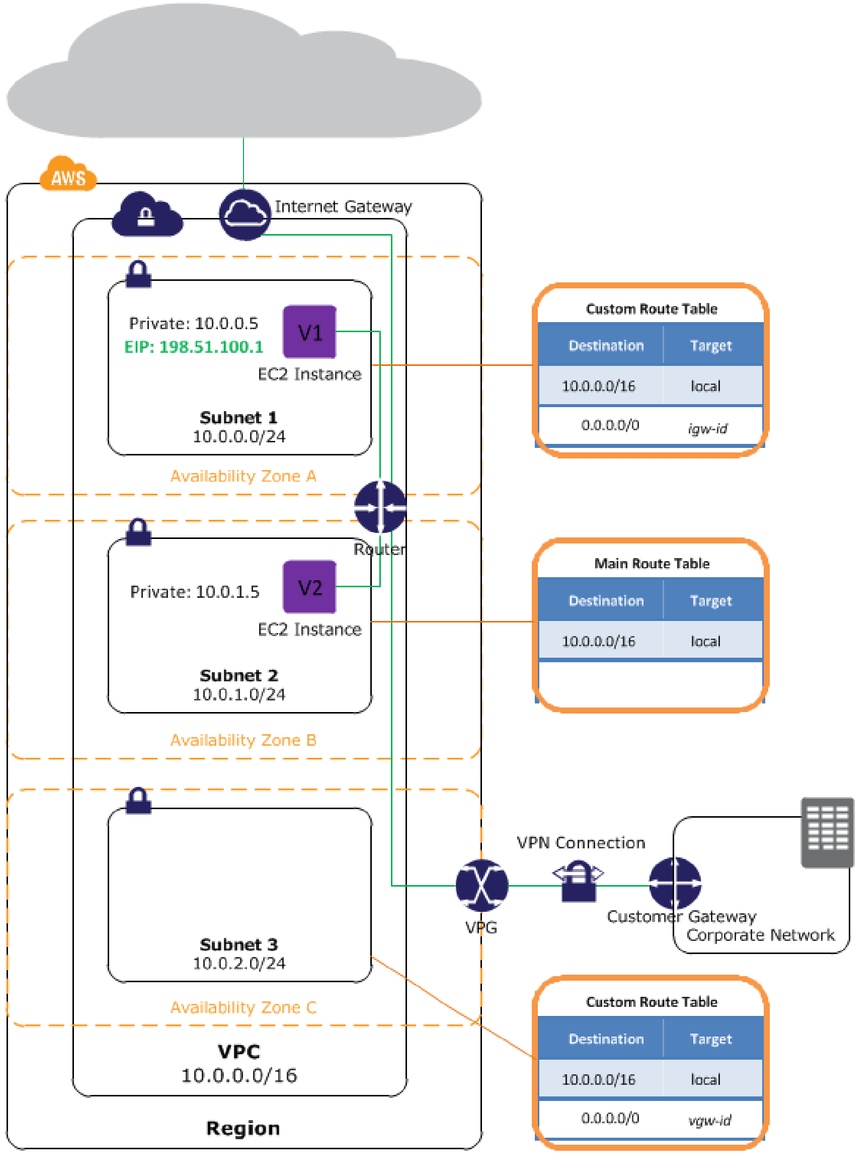
Amazon VPC

Virtual Private Cloud

A virtual network in your own **logically isolated area** within the AWS cloud populated by infrastructure, platform, and application services that share common **security** and **interconnection**.

VPC Networking

Elastic Network Interface (ENI)
Subnet
Network Access Control List (NACL)
Route Table
Internet Gateway
Virtual Private Gateway
Route 53 Private Hosted Zone



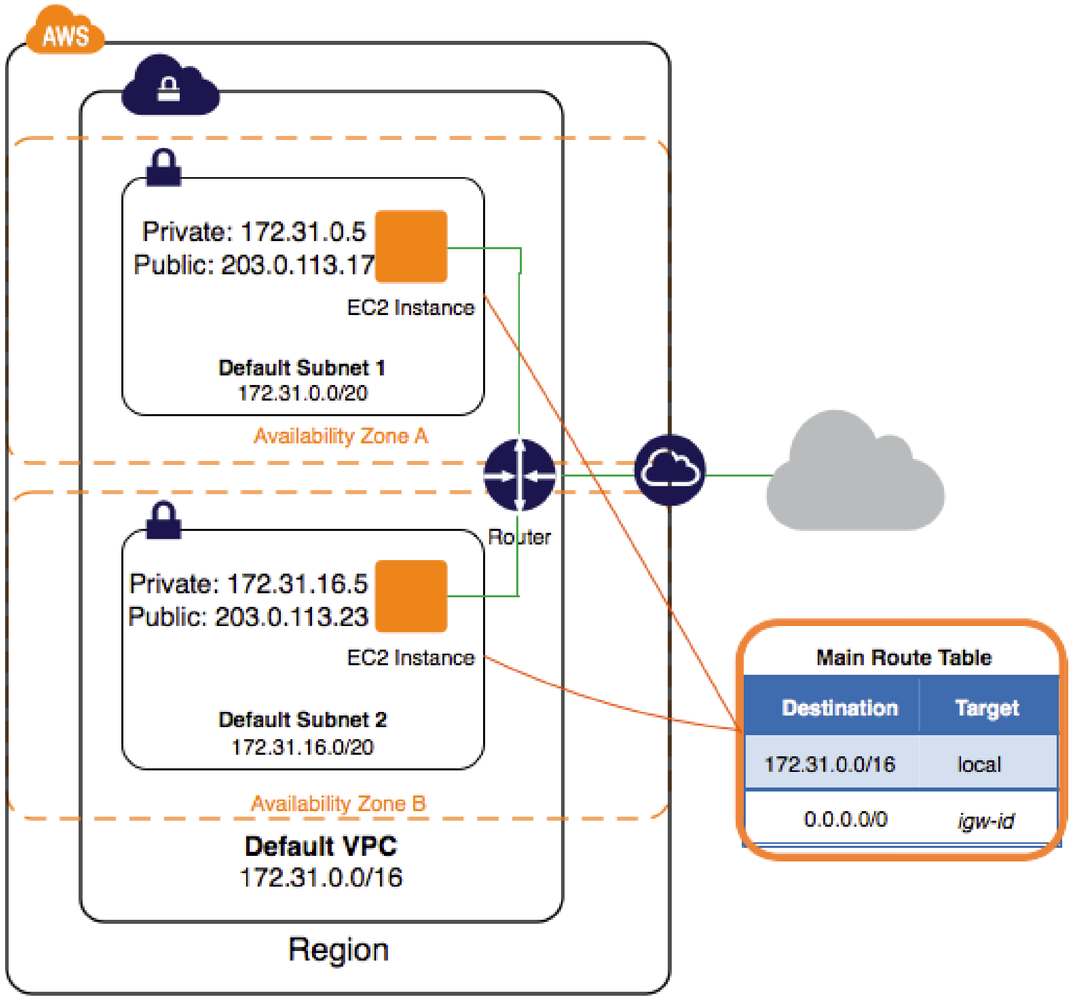
Sample VPC

with 1 Public Subnet, 2 Private Subnets, 1 of which can route through the VPN

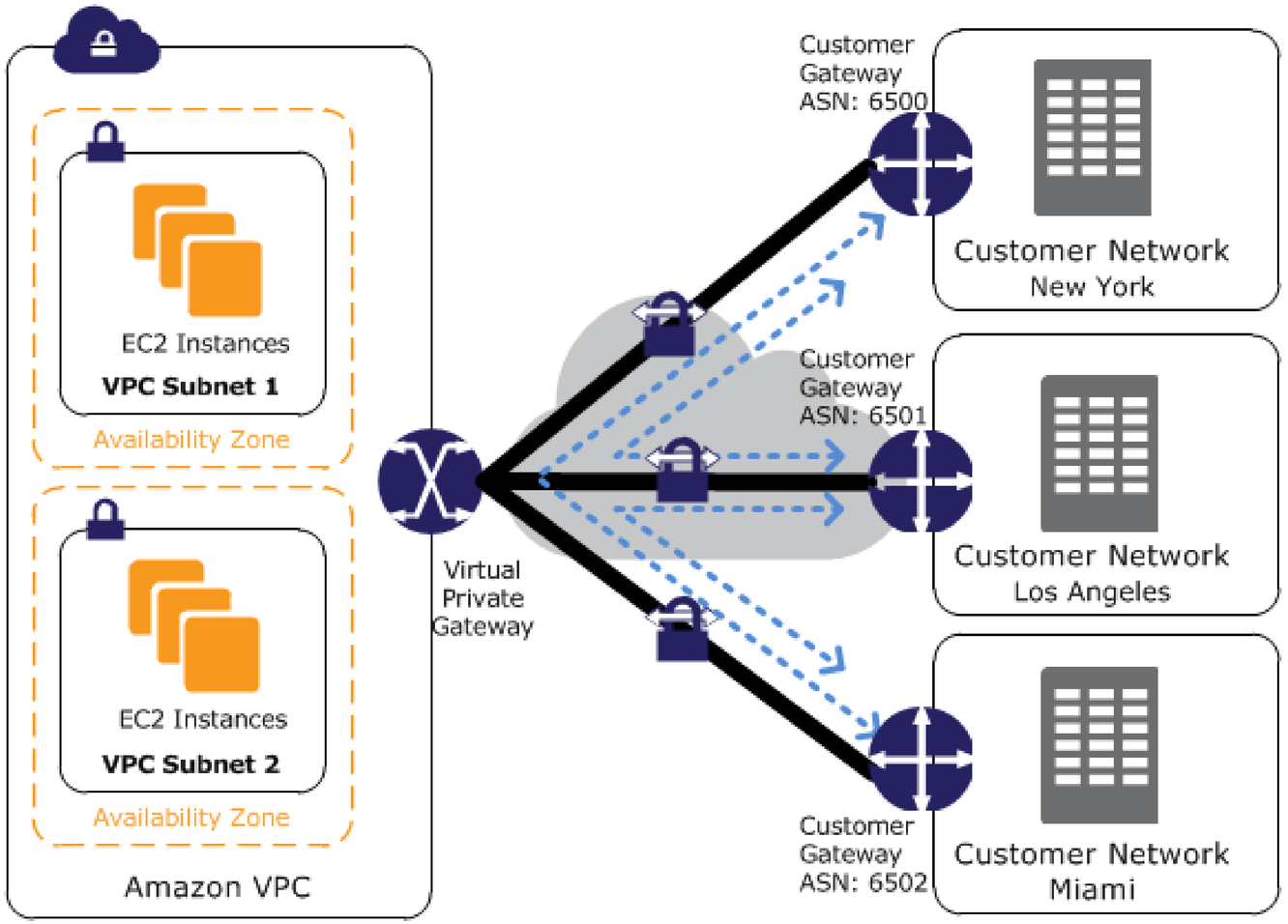
Best Practice

A VPC can span multiple AZs,
but subnet must reside
entirely within one AZ

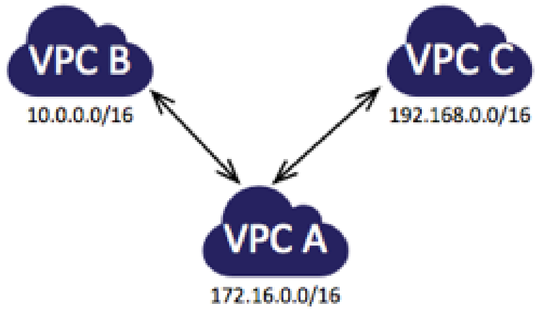
Use at least 2 subnets
in different AZs
for each layer of your network



Sample VPC
with
2 Public Subnets

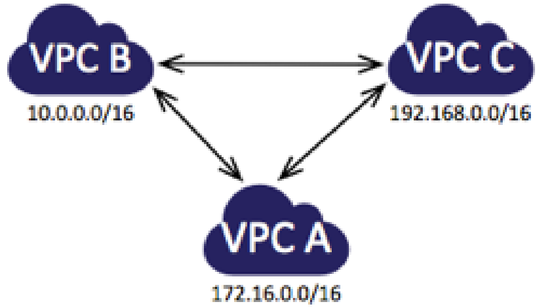


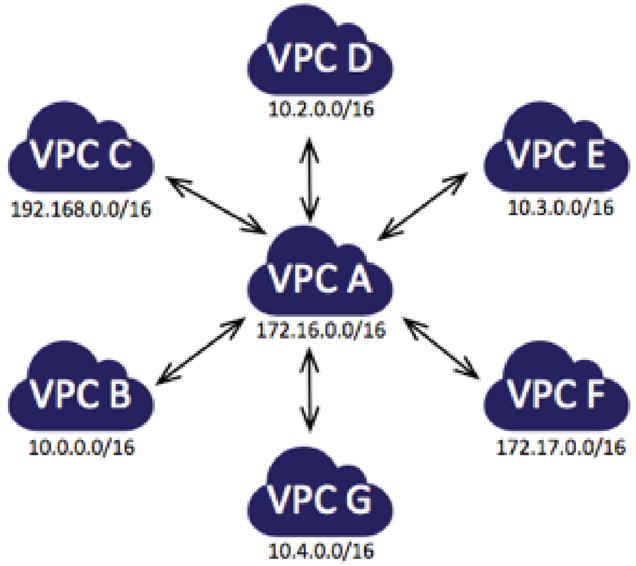
Sample VPN CloudHub



VPC Peering

A networking connection between two VPCs



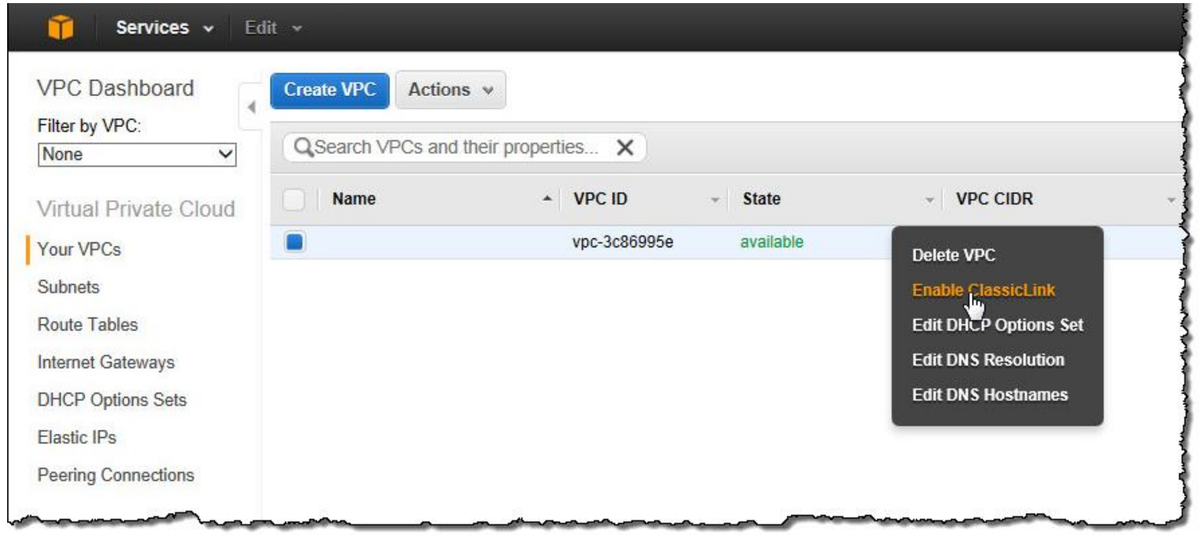


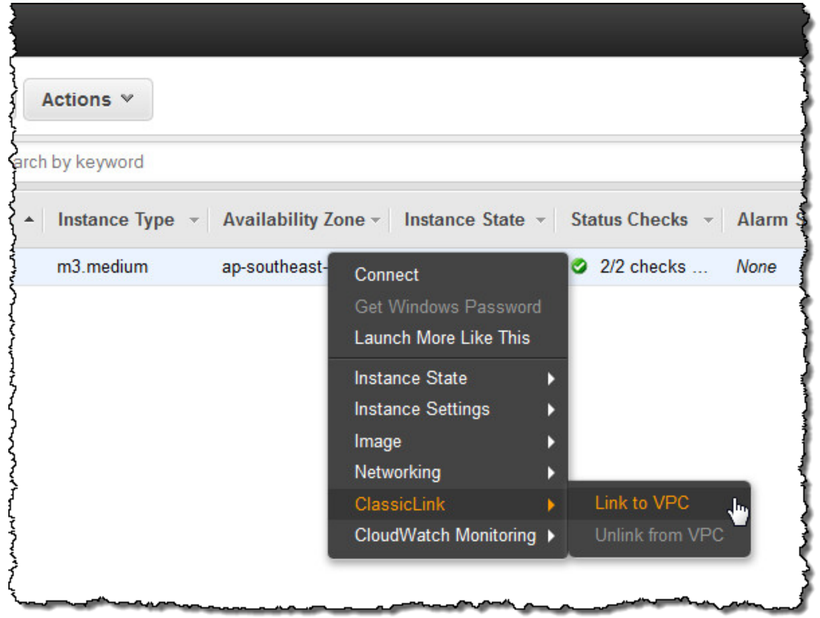
ClassicLink

Link your EC2-Classic instance to a VPC in your account, within the same region.

Associate VPC **security groups** with an EC2-Classic instance, enabling communication between your EC2-Classic instance and instances in your VPC using **private IP addresses**

ClassicLink

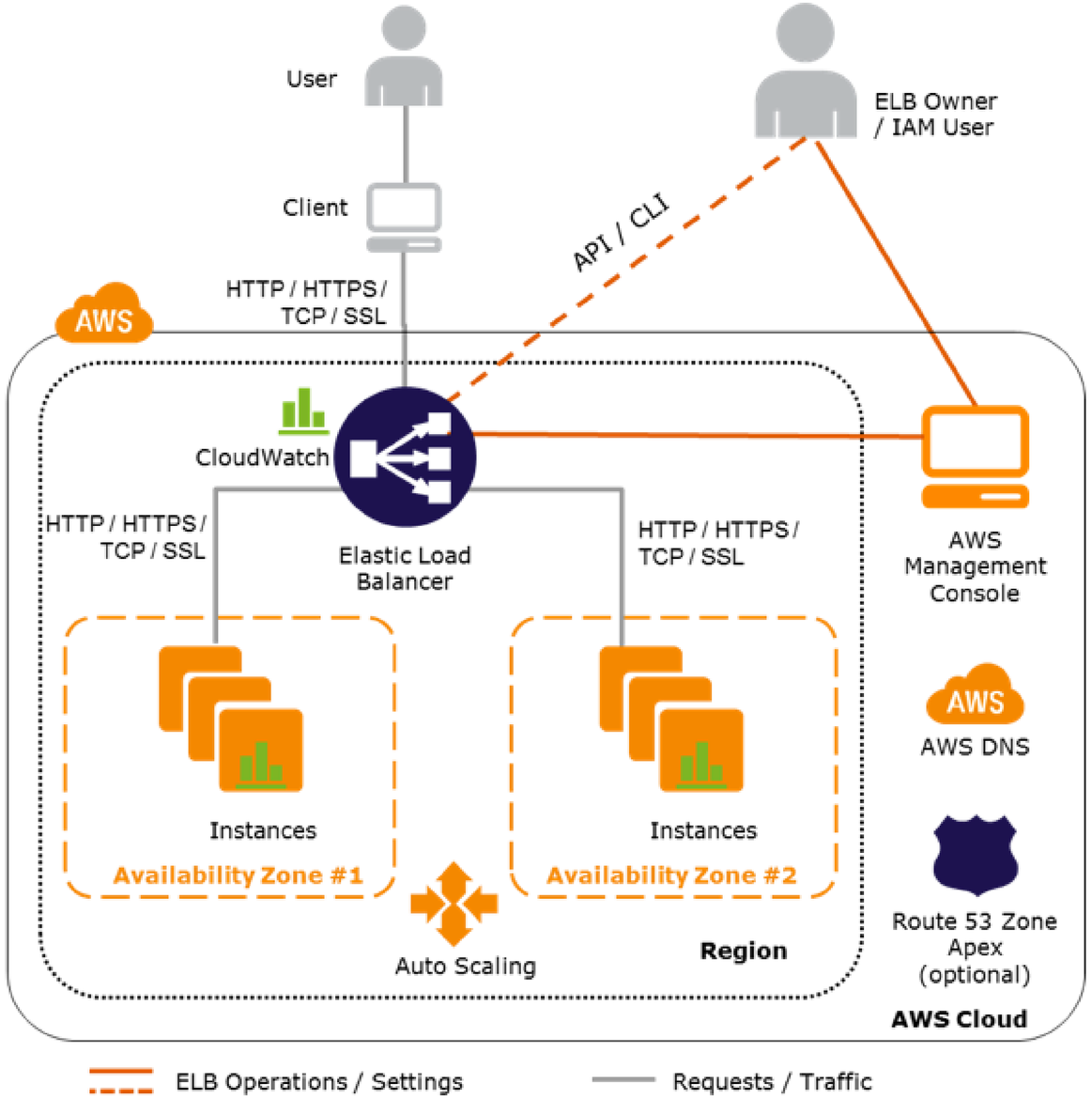




NETWORK

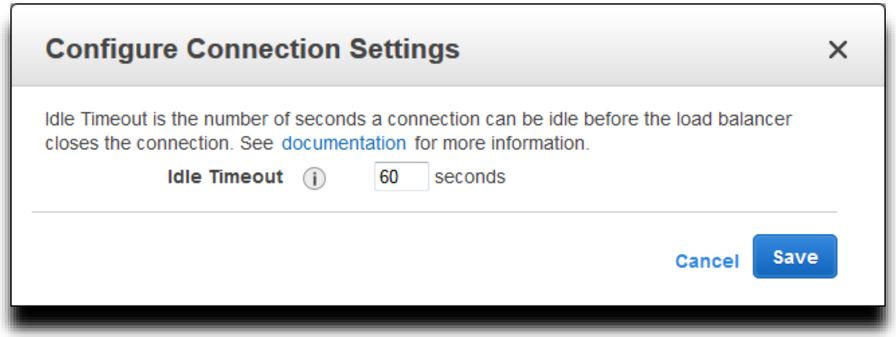
ELASTIC LOAD BALANCING

Elastic Load Balancing

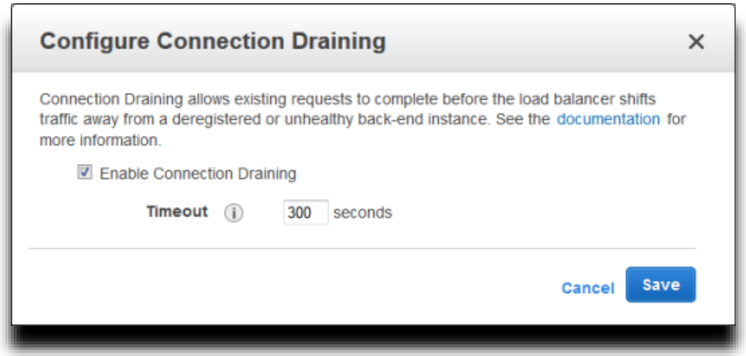


Elastic Load Balancing

Timeout Configuration



Connection Draining



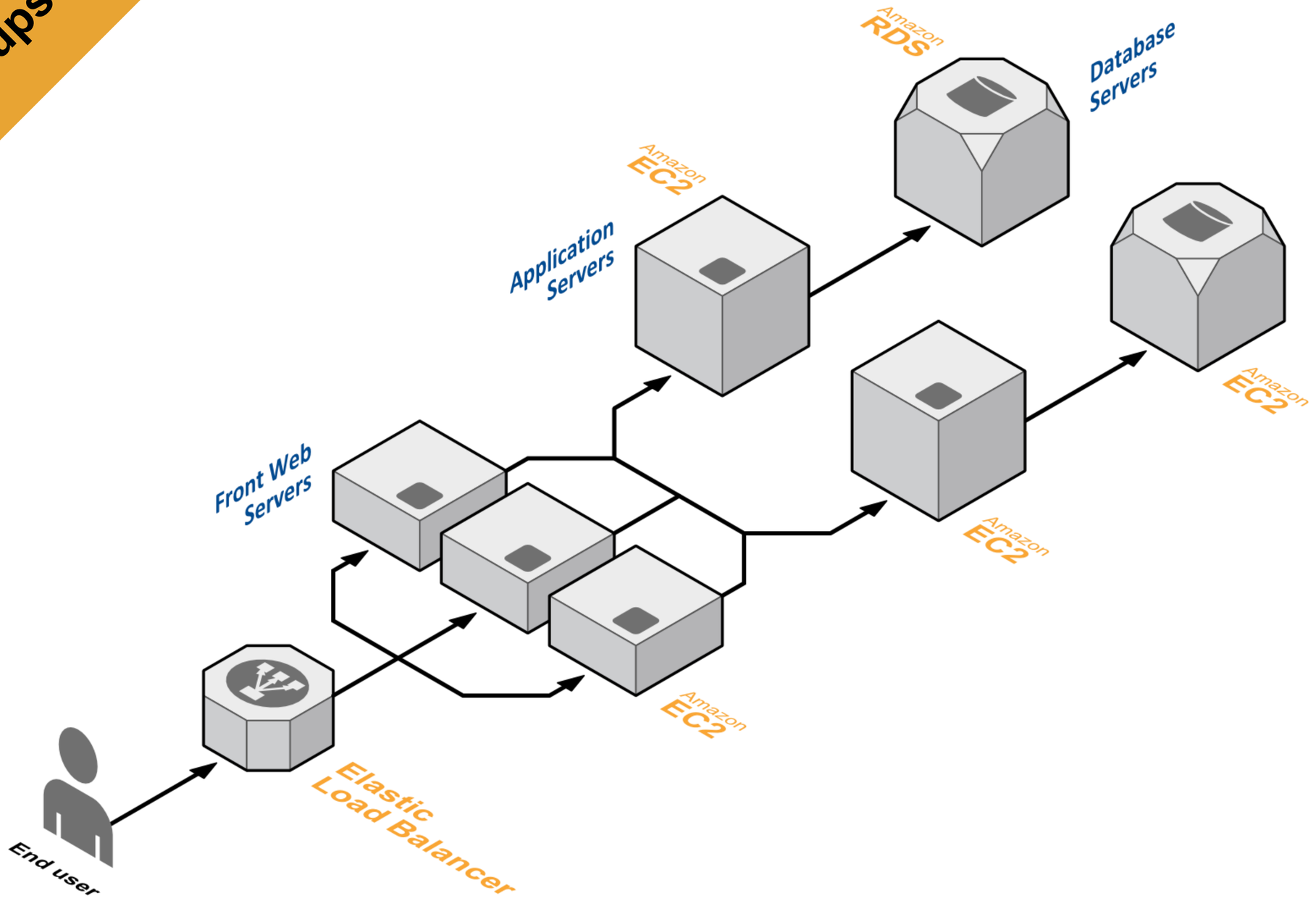
Cross-zone Load Balancing

SECURITY & ACCESS CONTROL

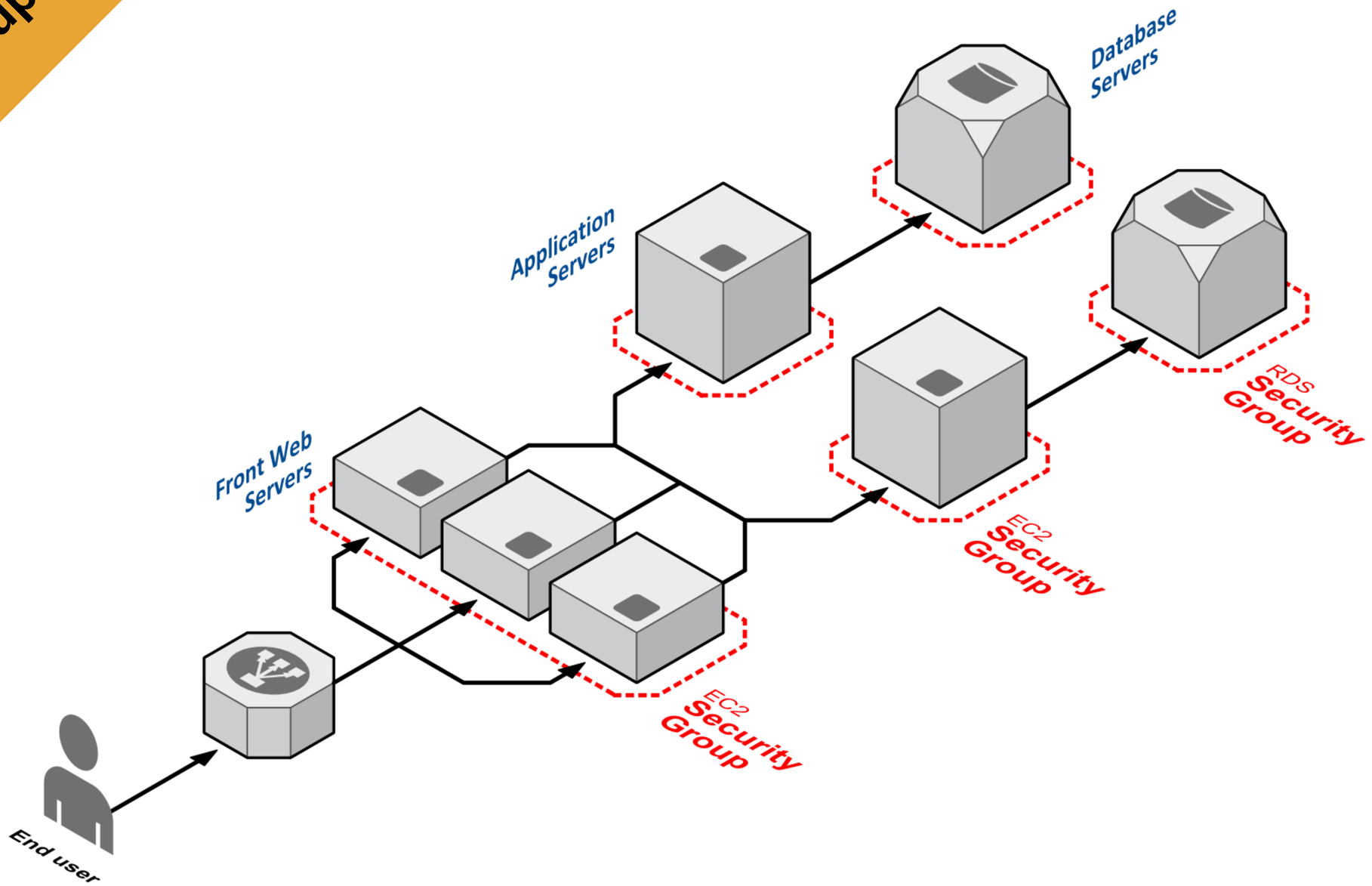
SECURITY & ACCESS CONTROL

SECURITY GROUPS & NETWORK ACLs

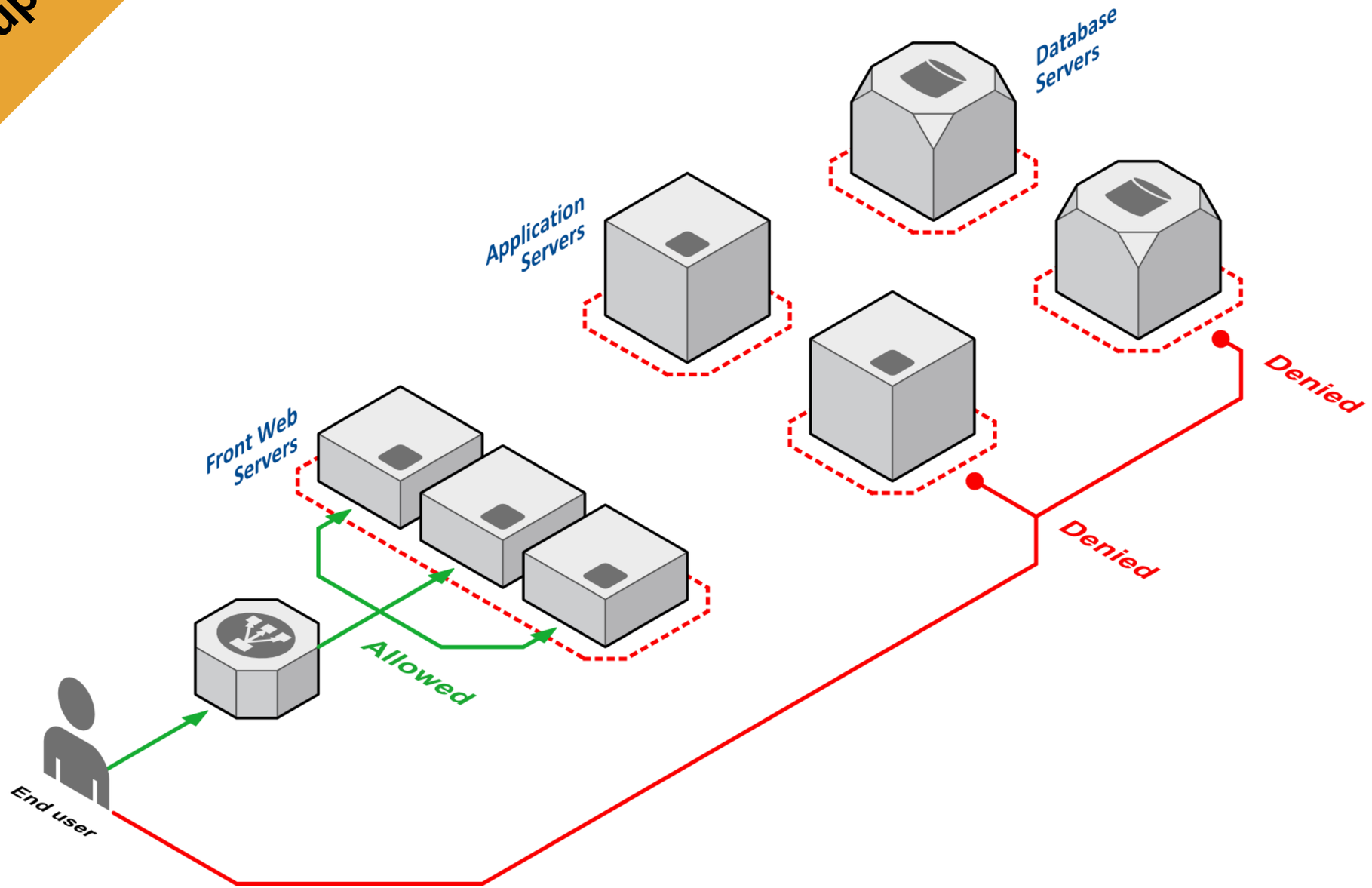
Security Groups



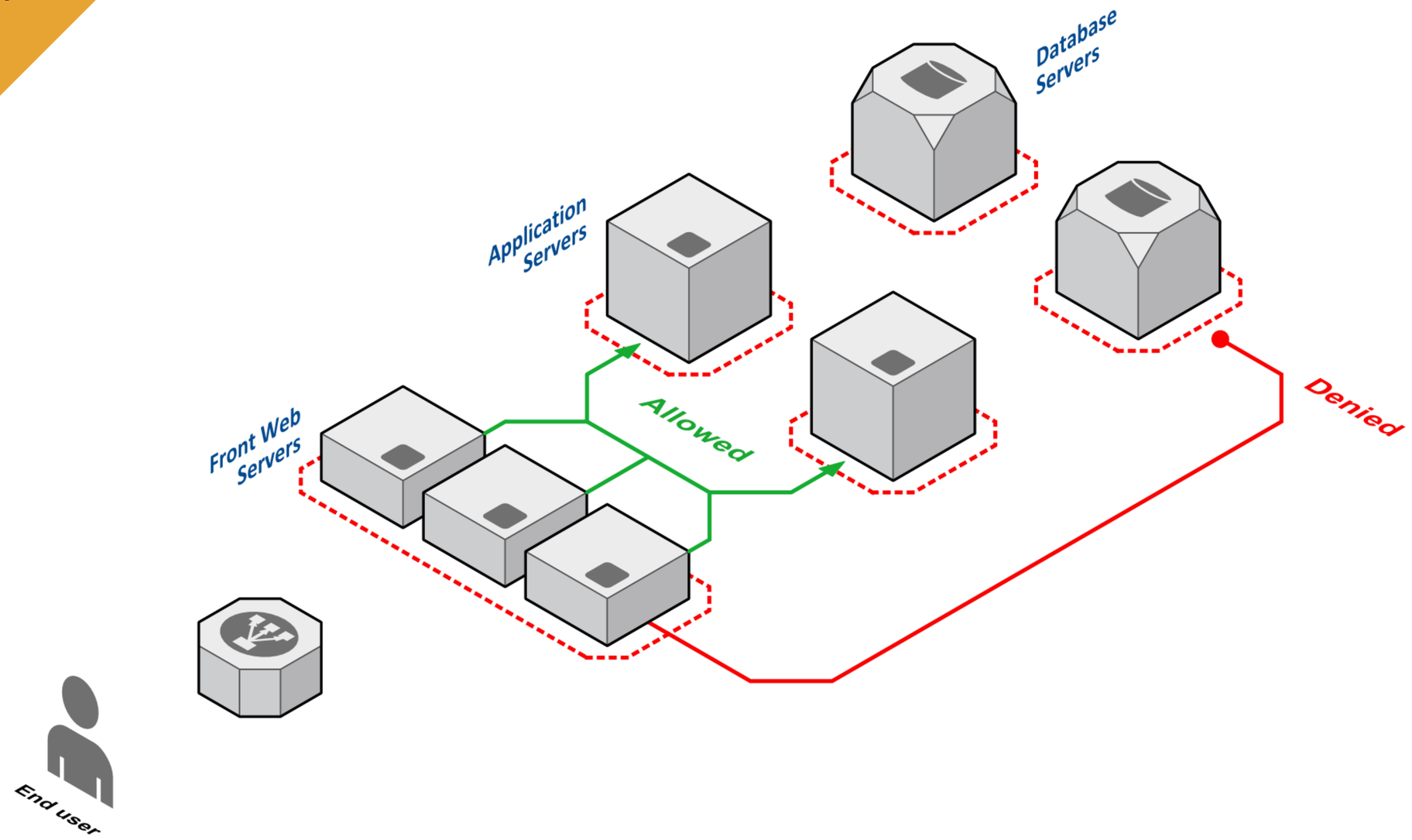
Security Groups



Security Groups



Security Groups



Security Group

A virtual firewall for your instance

STATEFUL

Responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa

Network ACLs

A firewall for controlling traffic in and out of a subnet

STATELESS

Responses to allowed inbound traffic are subject to the rules for outbound traffic, and vice versa

SECURITY & ACCESS CONTROL

ACCESS CREDENTIALS & KEY PAIRS

Access Credentials

Access key and secret key used to authenticate when accessing AWS APIs

Key Pairs

Public key and private key used to authenticate when accessing an Amazon EC2 instance

Best Practice

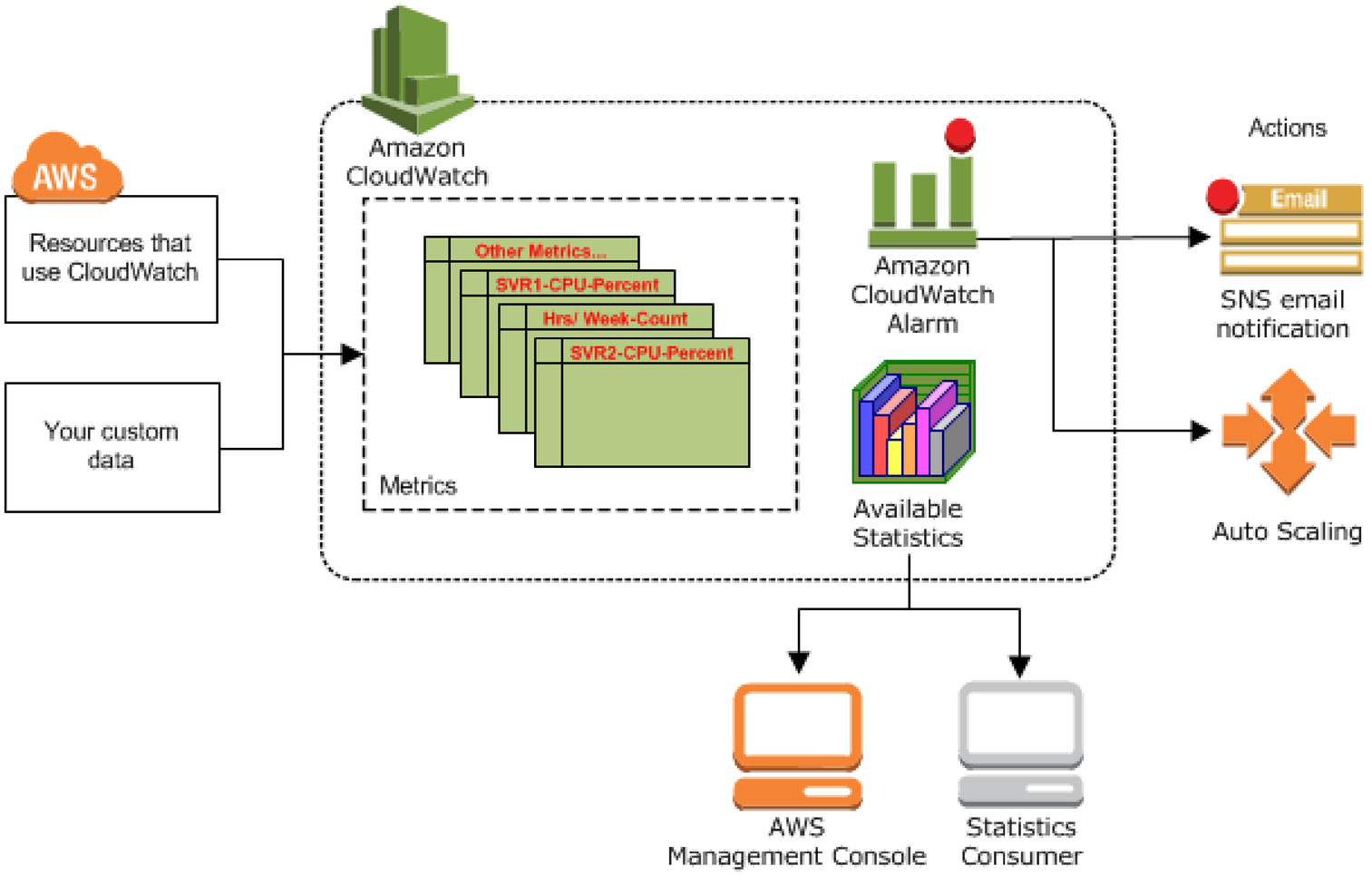
Use IAM Roles to pass access credentials to an instance

Best Practice

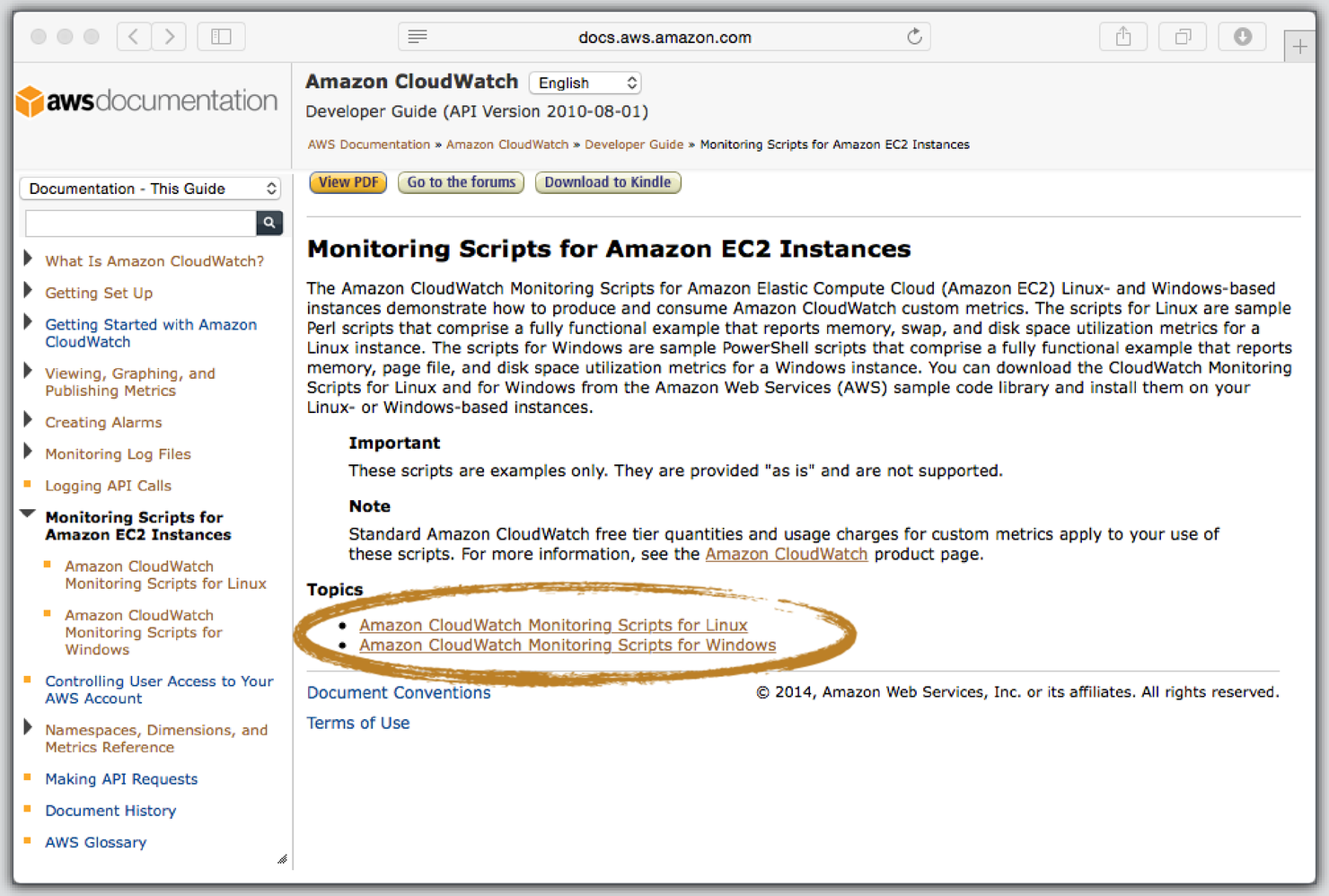
“If you need to SSH into your instance, **your deployment process is broken**.”

MONITORING & LOGS

CloudWatch Metrics & Alarms



Monitoring Scripts for Amazon EC2 Instances

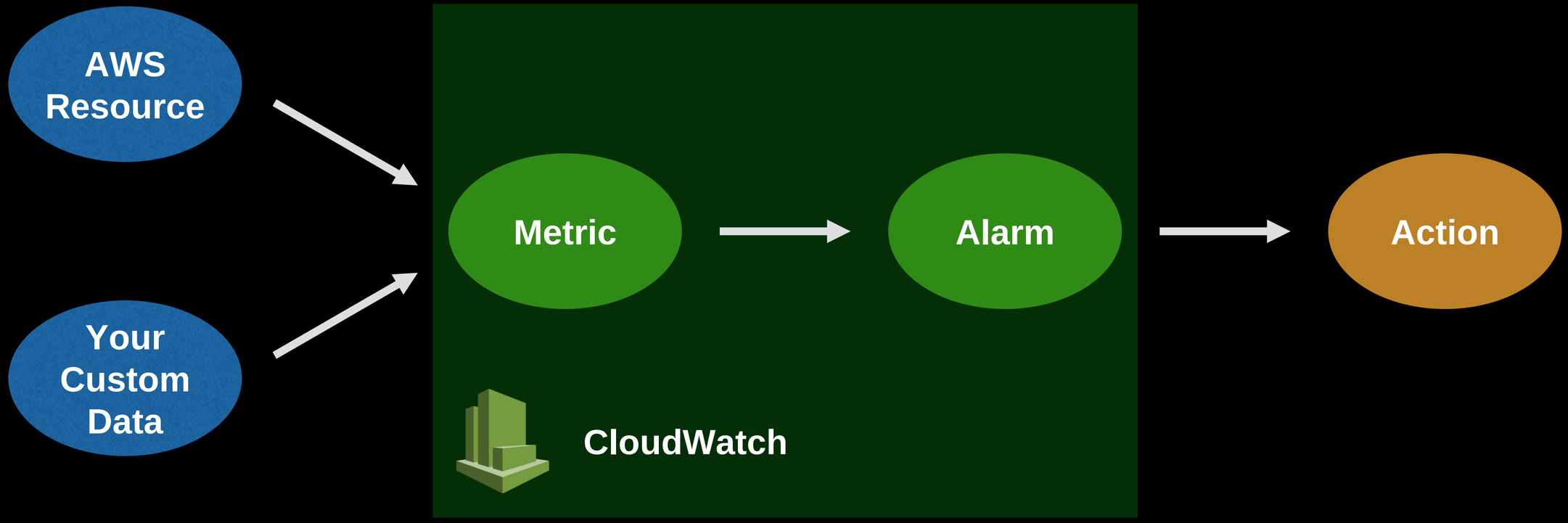


CloudWatch Logs

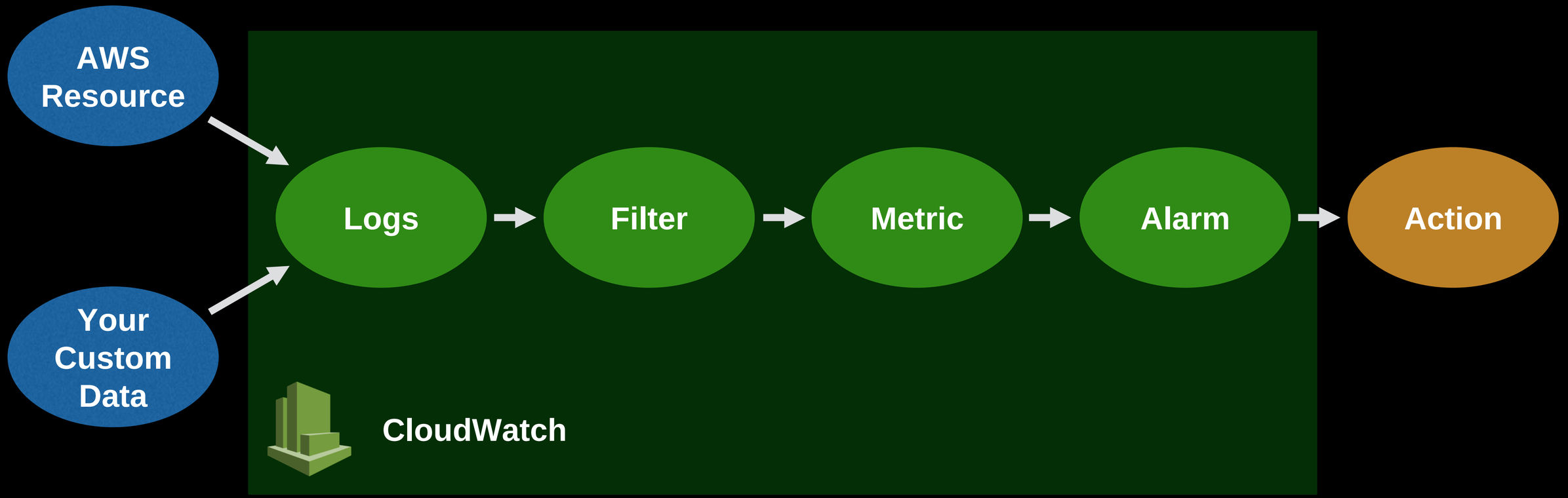
Monitor applications and systems using log data
Store in a highly durable storage and set retention
Access your log files via Web, CLI or SDK

Amazon EC2 (Linux & Windows)
CloudTrail
AWS Lambda
…

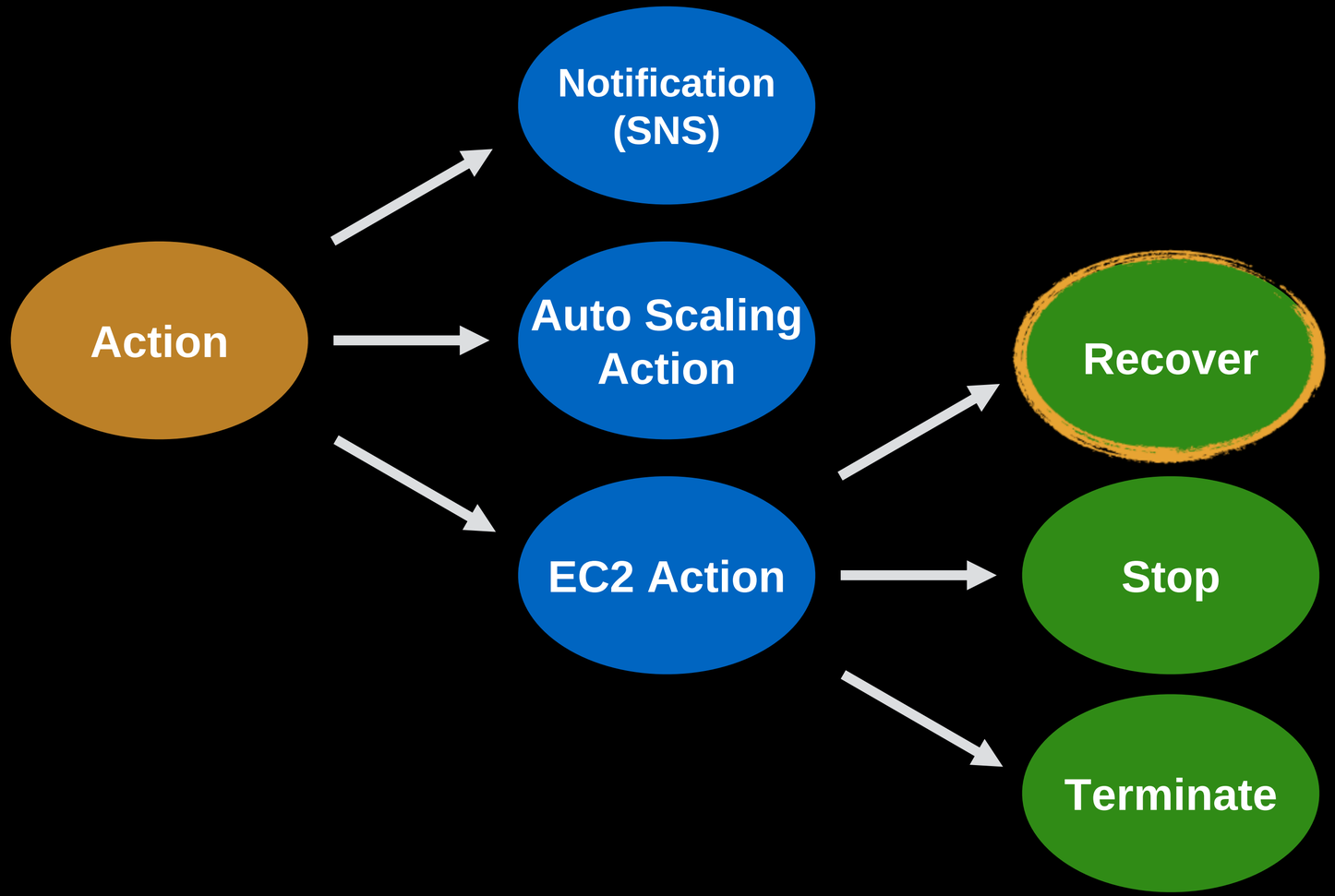
CloudWatch Metrics & Alarms



CloudWatch Logs + Filter



Alarm Actions



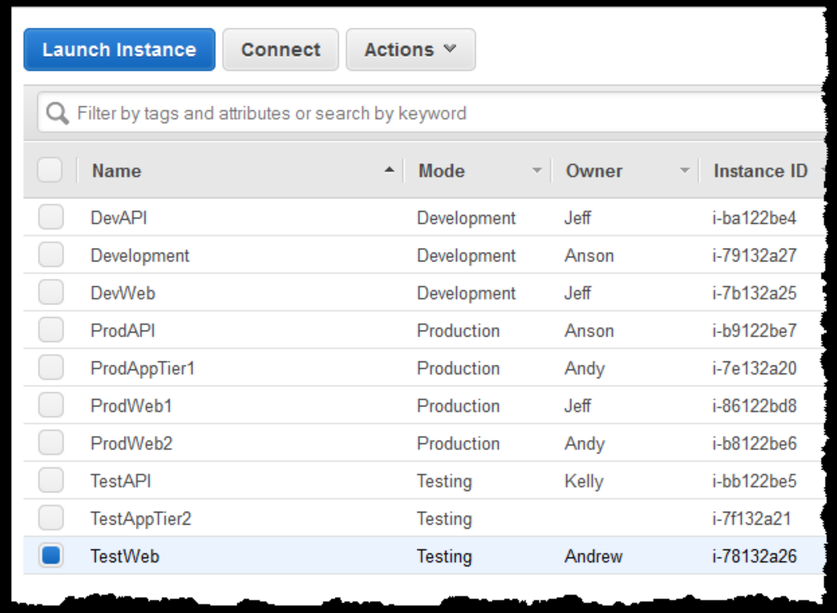
Amazon EC2 Auto Recovery

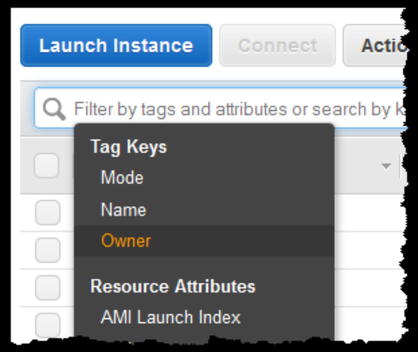
Use this action together with Status Checks to automate instance recovery

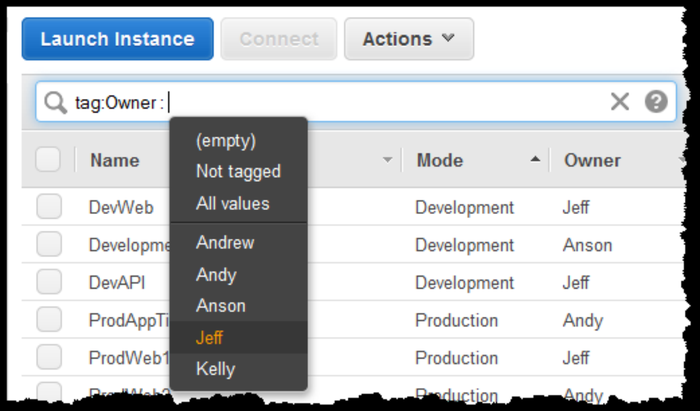
MANAGEMENT

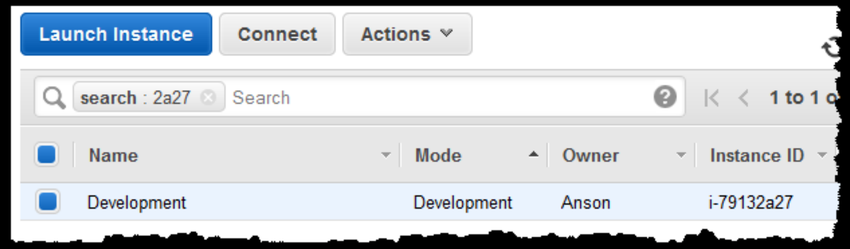
AWS Management Console

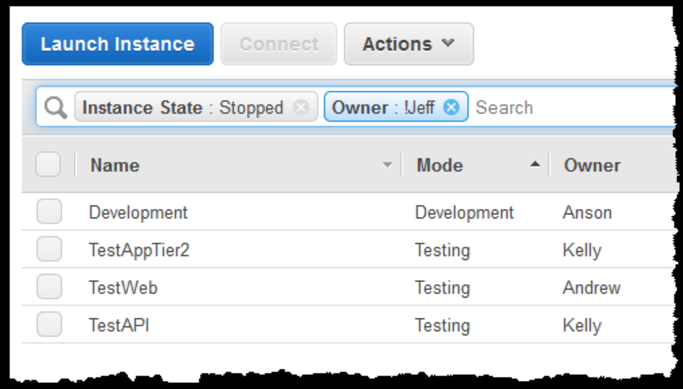
Query Your EC2 Instances Using Tag and Attribute Filtering





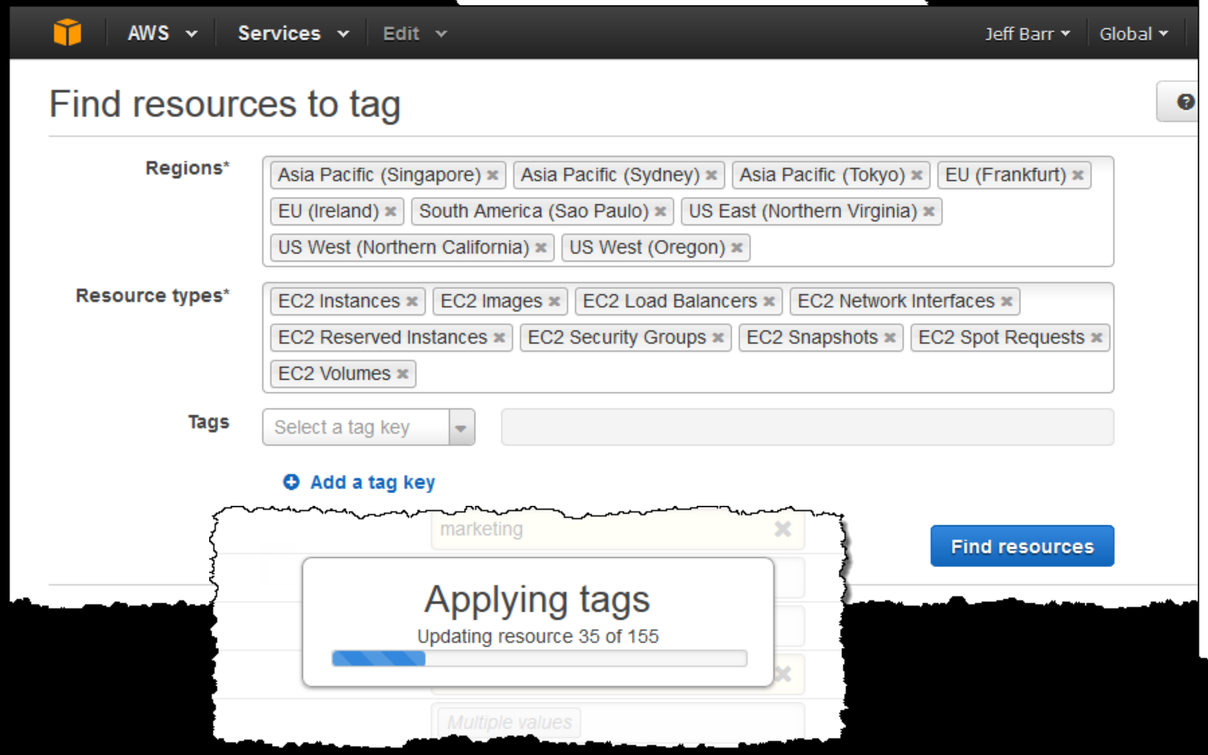


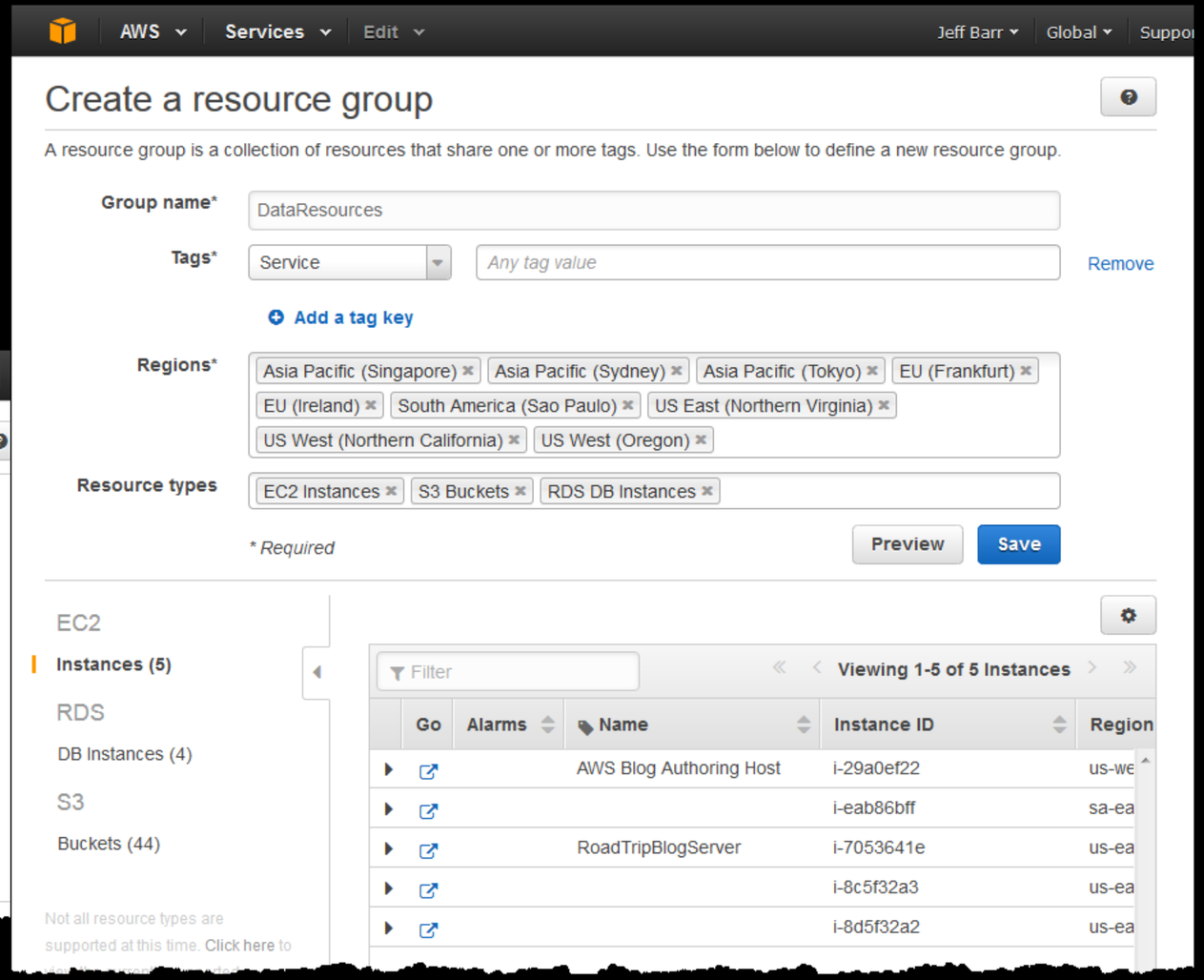




AWS Management Console

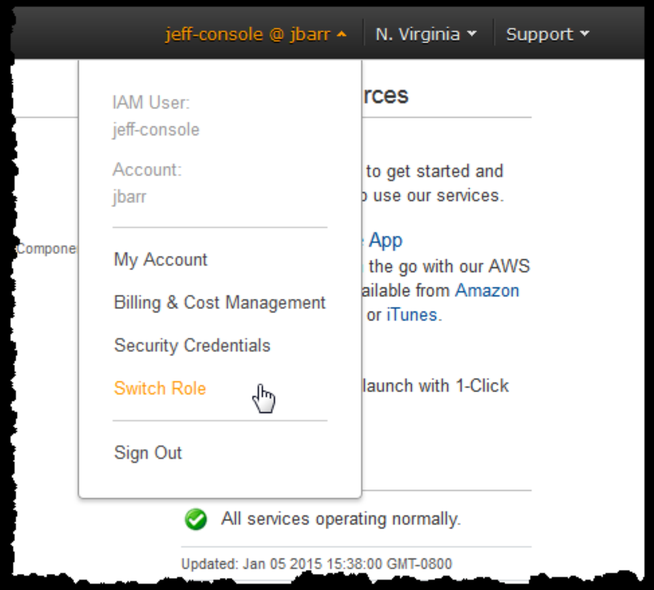
Resource Groups and Tagging

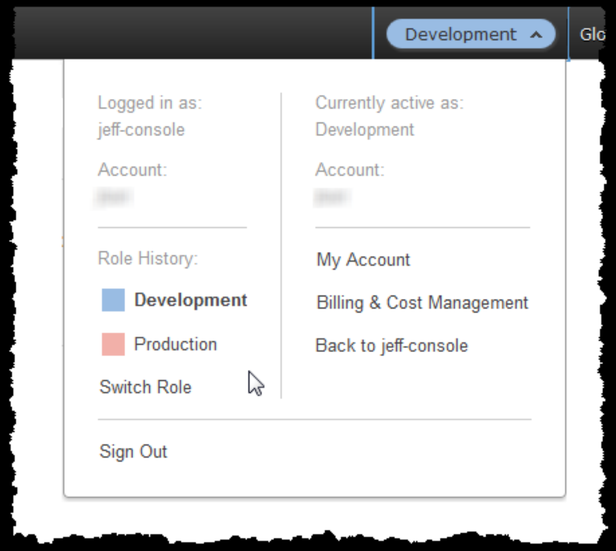




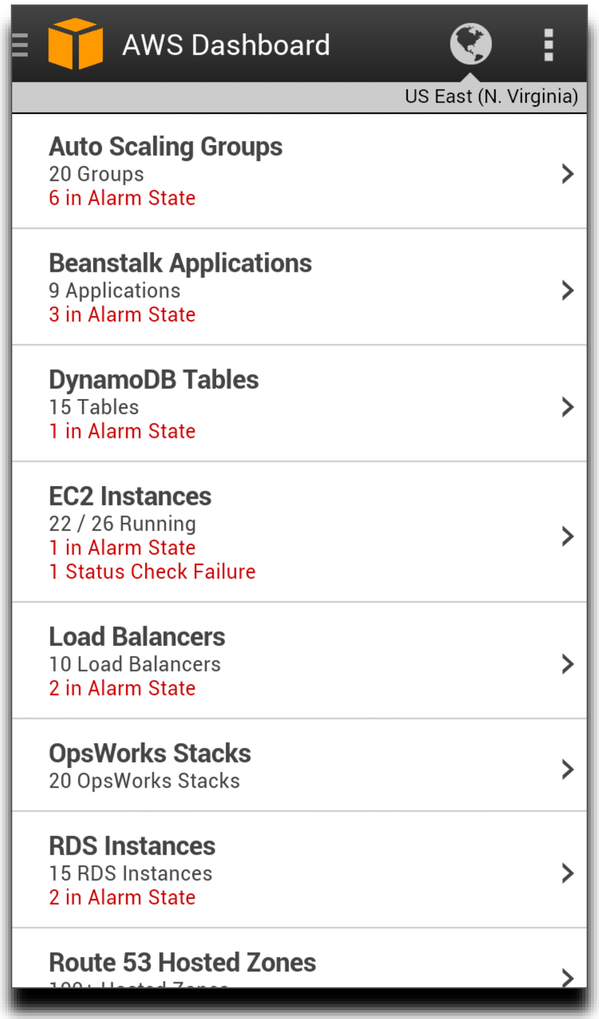
AWS Management Console

Cross account login (IAM)





AWS Console Mobile App



AWS
Command Line Interface

A unified tool to manage your AWS services

Windows - Mac - Linux

```
$ aws ec2 describe-instances
$ aws ec2 start-instances --instance-ids i-1348636c
```

AWS
Command Line Interface

```
$ aws ec2 describe-volumes --output table
```

```
-------------------------------------------------------------------------------------------------------------
|                                                DescribeVolumes                                            |
+-----------------------------------------------------------------------------------------------------------+
||                                                 Volumes                                                 ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
|| AvailabilityZone |        CreateTime         | Size  |  SnapshotId    |  State  |   VolumeId     | VolumeType  ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
||  us-west-2a      |  2013-09-17T00:55:03.000Z |  30   |  snap-f23ec1c8 |  in-use |  vol-e11a5288  |  standard   ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
|||                                              Attachments                                              |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
|||        AttachTime        |  DeleteOnTermination  |   Device    | InstanceId   |   State   |   VolumeId    |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
|||  2013-09-17T00:55:03.000Z |  True                 |  /dev/sda1  |  i-a071c394  |  attached |  vol-e11a5288 |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
||                                                 Volumes                                                 ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
|| AvailabilityZone |        CreateTime         | Size  |  SnapshotId    |  State  |   VolumeId     | VolumeType  ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
||  us-west-2a      |  2013-09-18T20:26:15.000Z |  8    |  snap-708e8348 |  in-use |  vol-2e410a47  |  standard   ||
|+------------------+---------------------------+-------+----------------+---------+----------------+-------------+|
|||                                              Attachments                                              |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
|||        AttachTime        |  DeleteOnTermination  |   Device    | InstanceId   |   State   |   VolumeId    |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
|||  2013-09-18T20:26:16.000Z |  True                 |  /dev/sda1  |  i-4b41a37c  |  attached |  vol-2e410a47 |||
||+--------------------------+-----------------------+-------------+--------------+-----------+---------------+||
```

AWS Command Line Interface

```
$ aws ec2 describe-volumes \
  --query 'Volumes[*].[VolumeId,Attachments[0].InstanceId,AvailabilityZone,Size]' \
  --output table

-------------------------------------------------
|                DescribeVolumes                |
+--------------+-------------+--------------+-----+
|  vol-e11a5288|  i-a071c394  |  us-west-2a  |  30 |
|  vol-2e410a47|  i-4b41a37c  |  us-west-2a  |  8  |
+--------------+-------------+--------------+-----+

$ aws ec2 describe-volumes \
  --query 'Volumes[*].{ID:VolumeId,InstanceId:Attachments[0].InstanceId,AZ:AvailabilityZone,Size:Size}' \
  --output table

-----------------------------------------------------
|                  DescribeVolumes                  |
+------------+---------------+--------------+-------+
|     AZ     |      ID       | InstanceId   | Size  |
+------------+---------------+--------------+-------+
|  us-west-2a|  vol-e11a5288  |  i-a071c394  |  30   |
|  us-west-2a|  vol-2e410a47  |  i-4b41a37c  |  8    |
+------------+---------------+--------------+-------+
```

RESOURCES

re:Invent CLI video:
https://www.youtube.com/watch?v=vP56l7qThNs
AWS CLI Docs: http://aws.amazon.com/cli/

AWS Tools
for Windows PowerShell

Manage your AWS services from the Windows PowerShell scripting environment

```
PS C:\> Start-EC2Instance -InstanceIds i-10a64379
```

AWS Tools
for Windows PowerShell

```
foreach ($i in Get-ChildItem C:\Logs)
{
    if ($i.CreationTime -lt ($(Get-Date).AddDays(-7)))
    {
        if ($i.Length -gt 0)
        {
            Write-S3Object -BucketName mylogbucket `
                           -Key Logs/$i `
                           -File $i.FullName
        }
        Remove-Item $i.FullName
    }
}
```

AWS SDKs

SDKs

Simplify using AWS services in your applications with an API tailored to your programming language or platform.

Android

Install »
Documentation »
Learn more »

Browser

Install »
Documentation »
Learn more »

iOS

Install »
Documentation »
Learn more »

Java

Install »
Documentation »
Learn more »

.NET

Install »
Documentation »
Learn more »

Node.js

Install »
Documentation »
Learn more »

PHP

Install »
Documentation »
Learn more »

Python

Install »
Documentation »
Learn more »

Ruby

Install »
Documentation »
Learn more »

DEPLOYMENT

DEPLOYMENT

AMAZON MACHINE IMAGE (AMI)

Amazon maintained

Set of **Linux** and **Windows** images

Kept up to date by Amazon in each region

Community maintained

Images published by **other AWS users**

Managed and maintained by **Marketplace partners**

Your machine images

AMIs **you have created** from EC2 instances

Can be kept **private or shared** with other accounts

Bake an AMI

Start an instance
Configure the instance
Create an AMI from your instance
Start new ones from the AMI

Bake an AMI

Start an instance
Configure the instance
Create an AMI from your instance
Start new ones from the AMI

Vs.

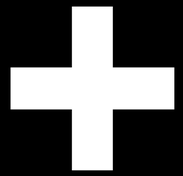
Configure dynamically

Launch an instance
Use metadata service and cloud-init to perform actions on instance when it launches

Bake an AMI

Build your base images and setup custom initialisation scripts

Maintain your ‘golden’ base



Configure dynamically

Use bootstrapping to pass custom information in and perform post launch tasks like pulling code from SVN

Bake an AMI

Configure dynamically

Time consuming configuration

startup time

Static configurations

less change management

Bake an AMI

Configure dynamically

Continuous deployment

latest code

Environment specific

dev-test-prod

Instance Store-backed

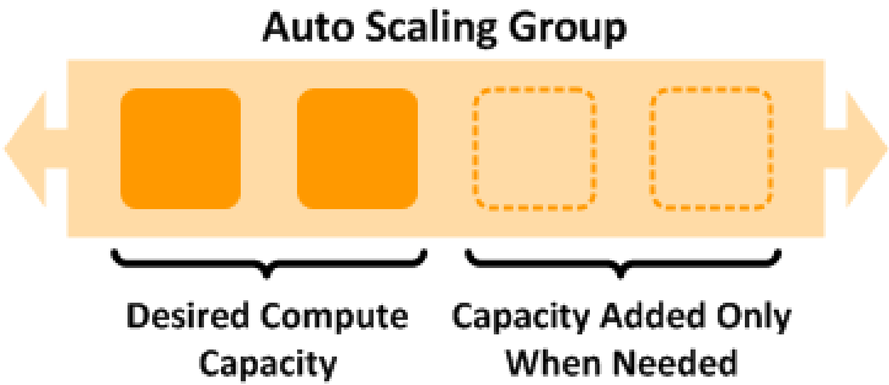
Vs.

Amazon EBS-backed

DEPLOYMENT

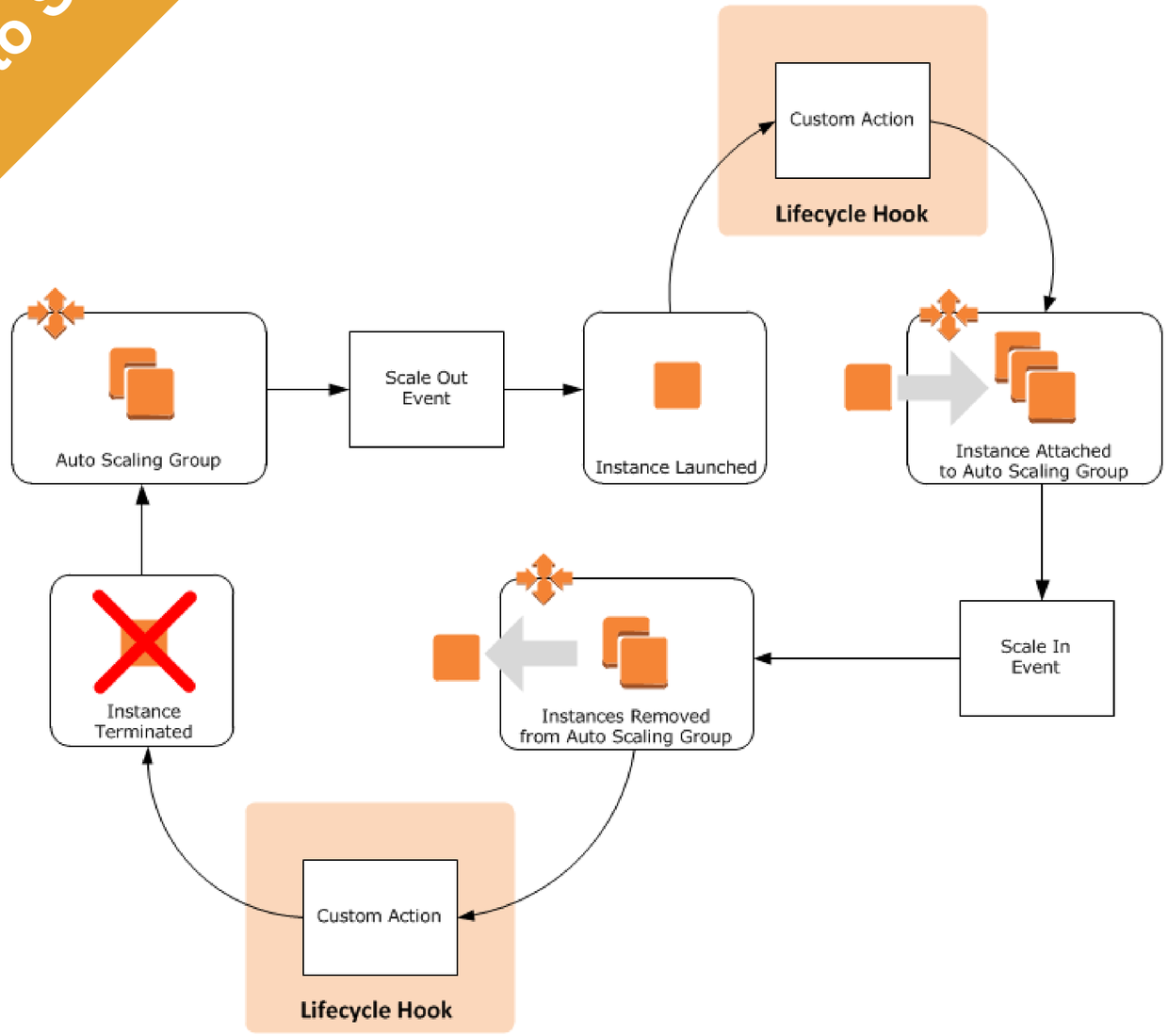
AUTO SCALING

Auto Scaling



Auto Scaling

Lifecycle Hooks



Sample Use Cases

Installing Software to Pending Instances

Filling a Cache of Servers

Retrieving Logs from Terminating Instances

Auto Scaling

Integrated with AWS CodeDeploy

DEPLOYMENT

DOCKER CONTAINERS

Amazon Linux

A supported and maintained Linux image provided by Amazon Web Services

AWS Elastic Beanstalk

For deploying and scaling web applications and services

Amazon EC2 Container Service

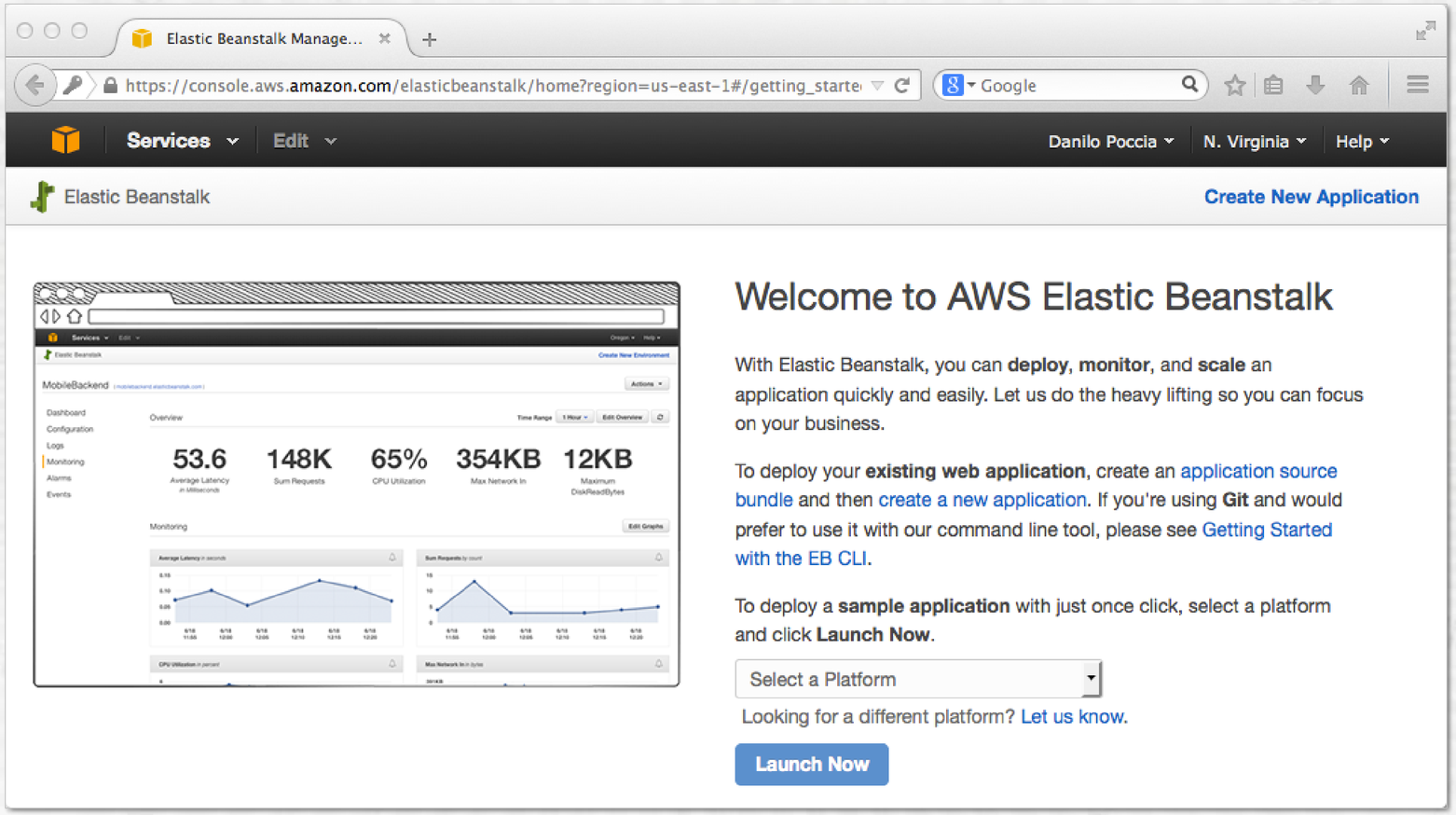
Highly scalable, high performance container management service

Amazon Linux

```
sudo yum install docker
sudo service docker start
sudo docker …
```

AWS
Elastic Beanstalk

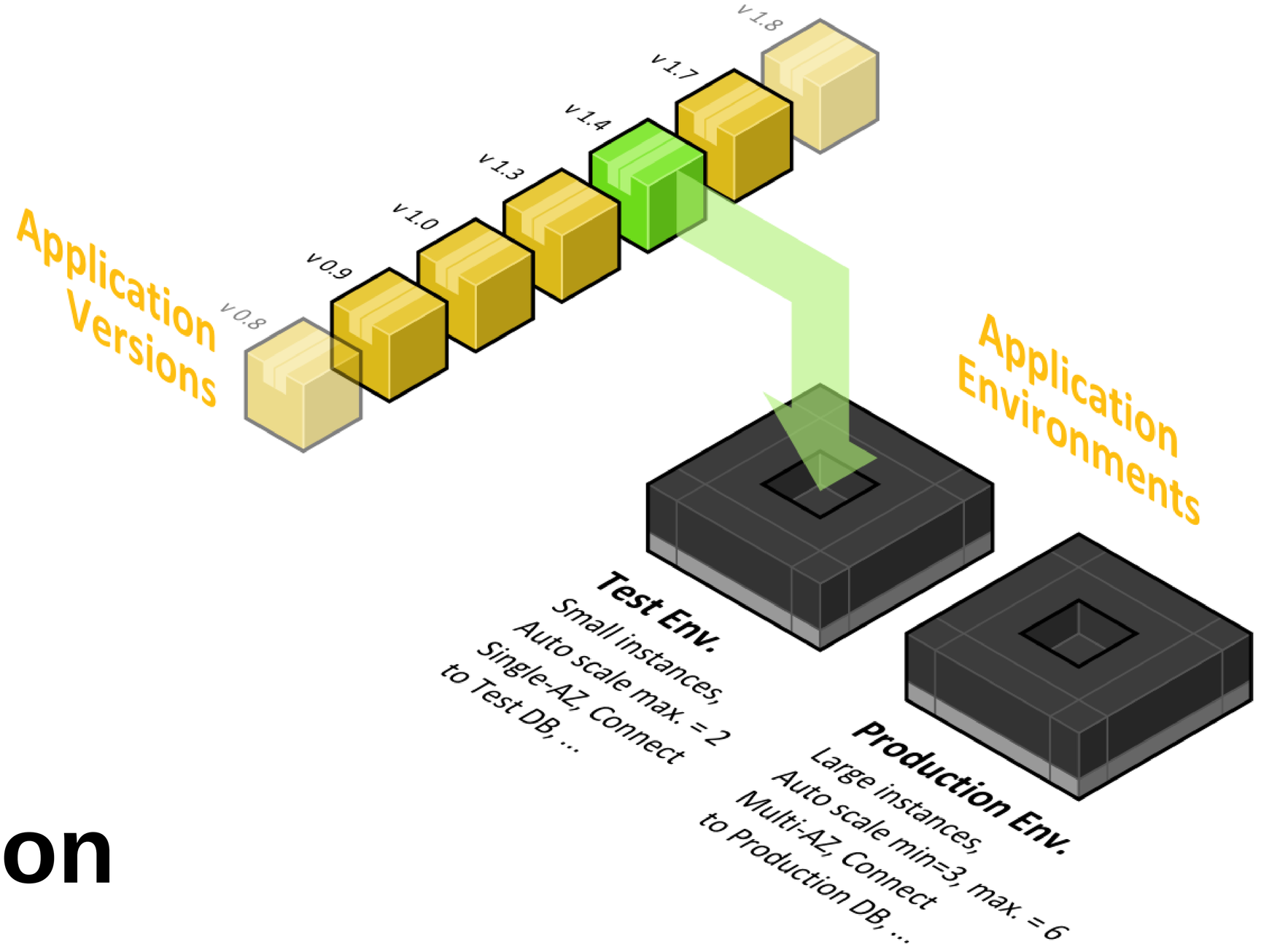
Choose Your Platform



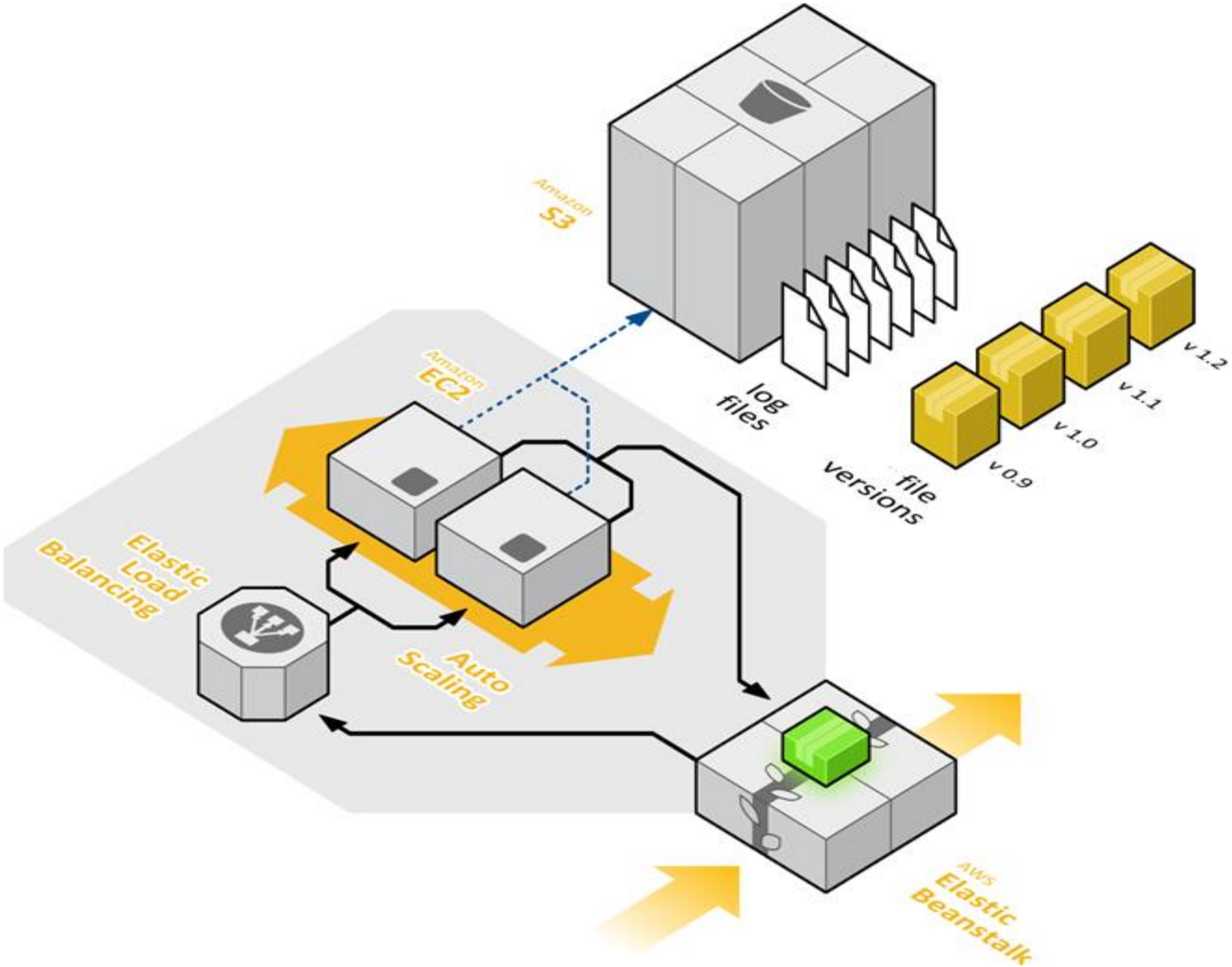
IIS Node.js PHP Python Ruby Tomcat Docker

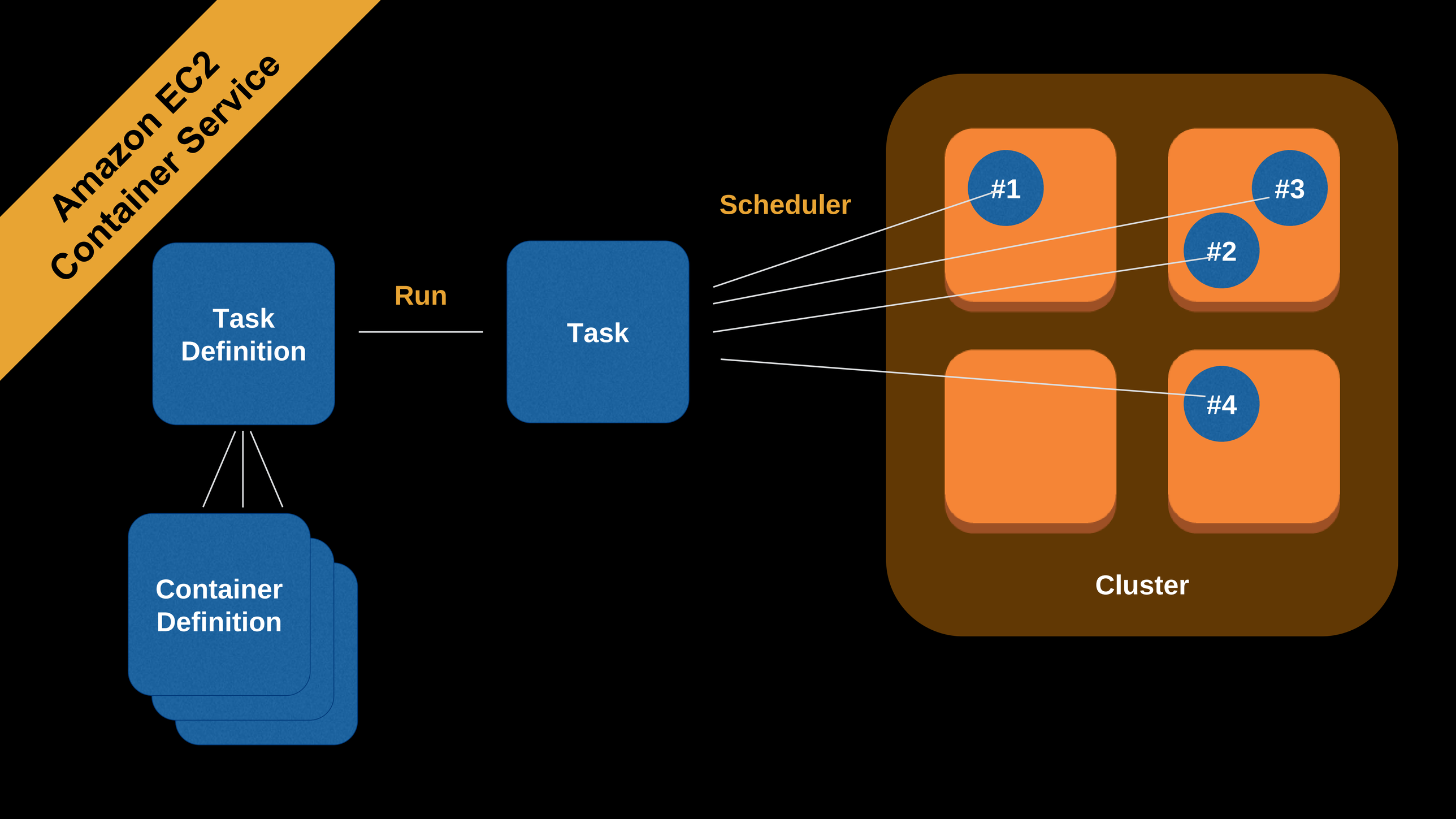
AWS
Elastic Beanstalk

Deploy Your Backend Application



AWS Elastic Beanstalk




Amazon EC2
Container Service
Task
Definition
Run
Task
Scheduler
#1
#3
#2
#4
Container
Definition
Cluster

COST OPTIMIZATION

COST OPTIMIZATION

RESERVED INSTANCE

EC2
Reserved Instance

Up to 75% discount compared to On-Demand Instance pricing

1 or 3 year terms

EC2 Reserved Instance

		Payment		
		Upfront	Monthly	Hourly
On Demand Instance				X
Reserved Instance	No Upfront		X	
	Partial Upfront	X	X	
	All Upfront	X		

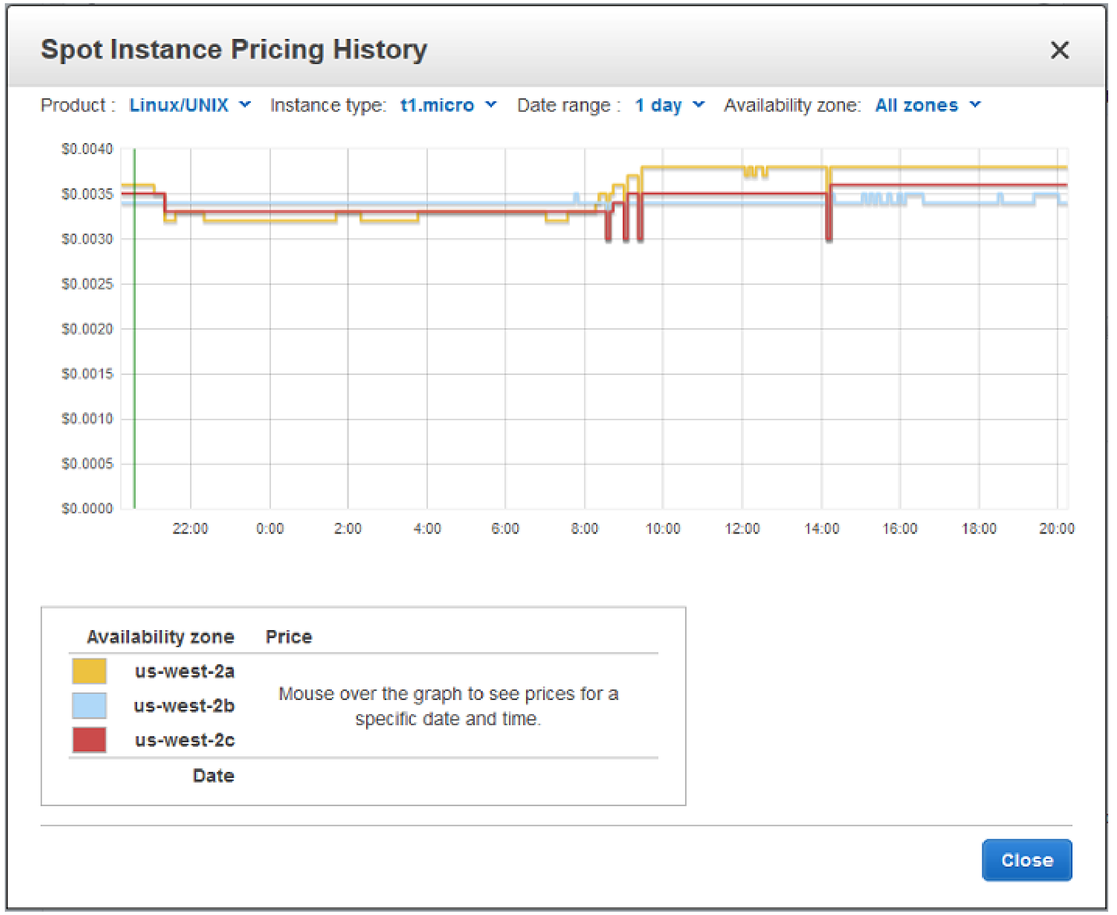
COST OPTIMIZATION

SPOT INSTANCE

EC2
Spot Instance

Bid on unused EC2 capacity

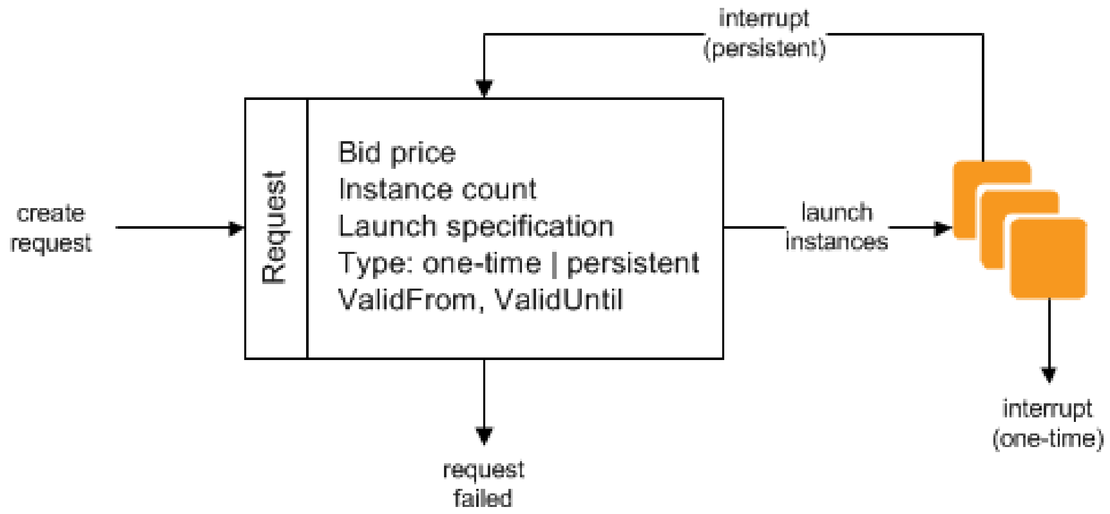
Spot Price based on supply/demand, determined automatically



EC2
Spot Instance

Bid on unused EC2 capacity

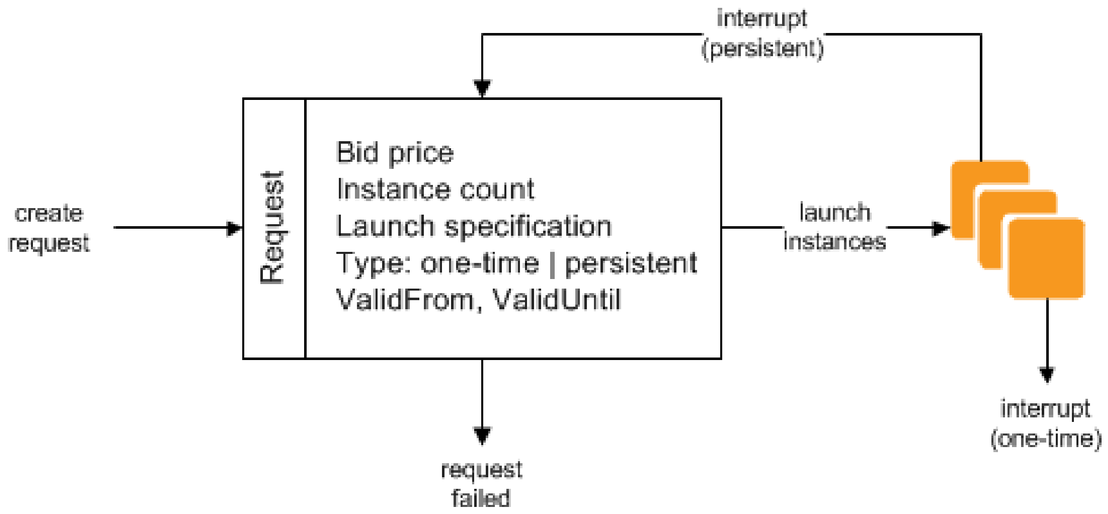
Spot Price based on supply/demand, determined automatically



EC2
Spot Instance

Bid on unused EC2 capacity

Spot Price based on supply/demand, determined automatically



Spot Instance Termination Notice
two-minute warning

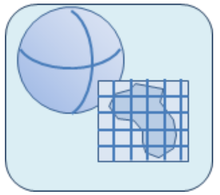
EC2
Spot Instance

Spot Instance Use Cases

Analytics

Big Data

Financial Modeling and Analysis



Geospatial Analysis

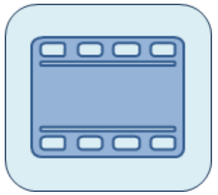
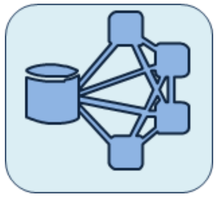


Image and Media Encoding



Scientific Computing

Testing

Web Crawling

3RD PARTY TOOLS

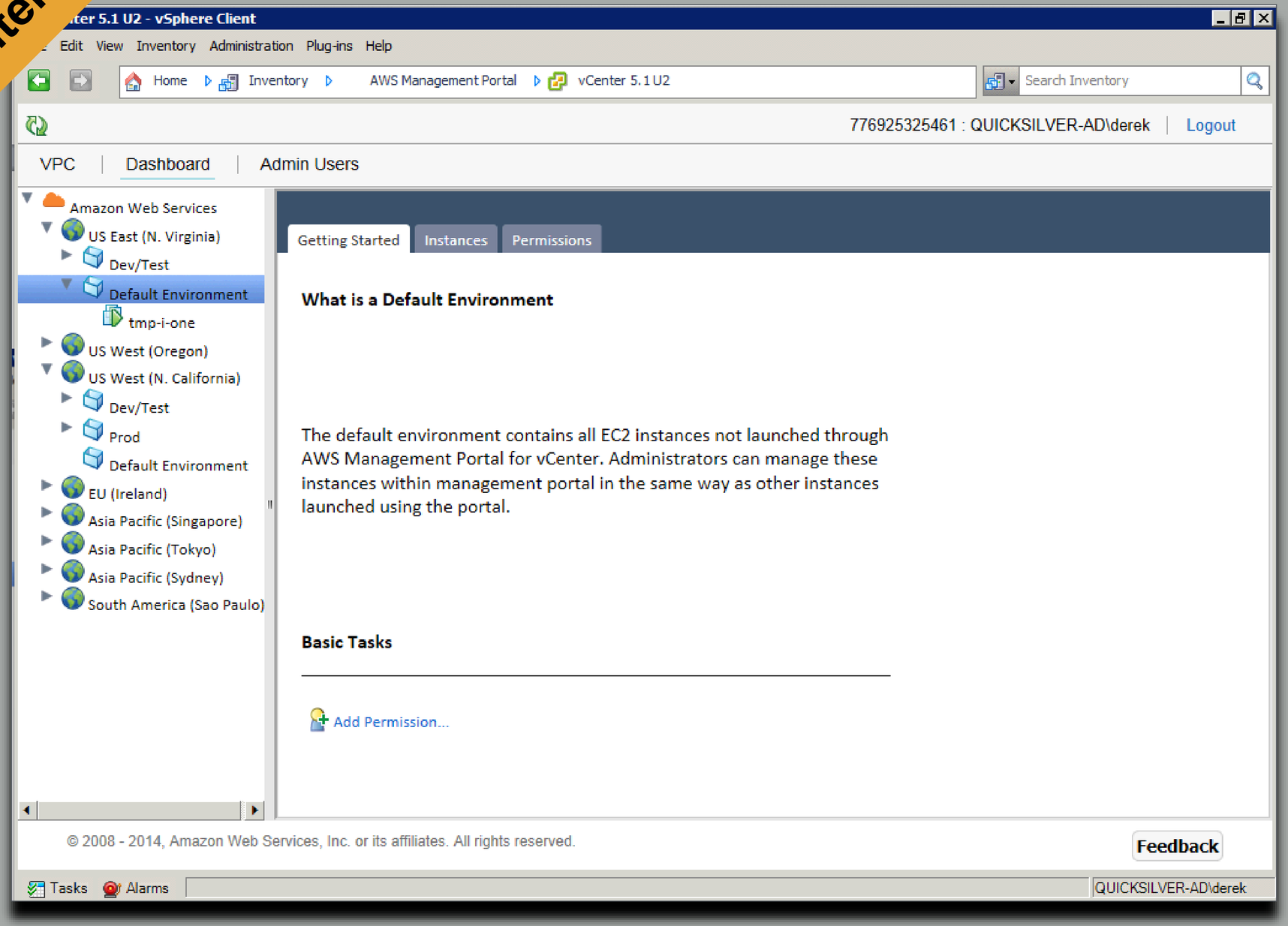
AWS Management Portal for vCenter

Manage your AWS resources using VMware vCenter

A vCenter plug-in
within your existing vCenter environment

Once installed, it enables you to
migrate VMware VMs to Amazon EC2
and **manage** AWS resources from within vCenter

AWS Management Portal for vCenter



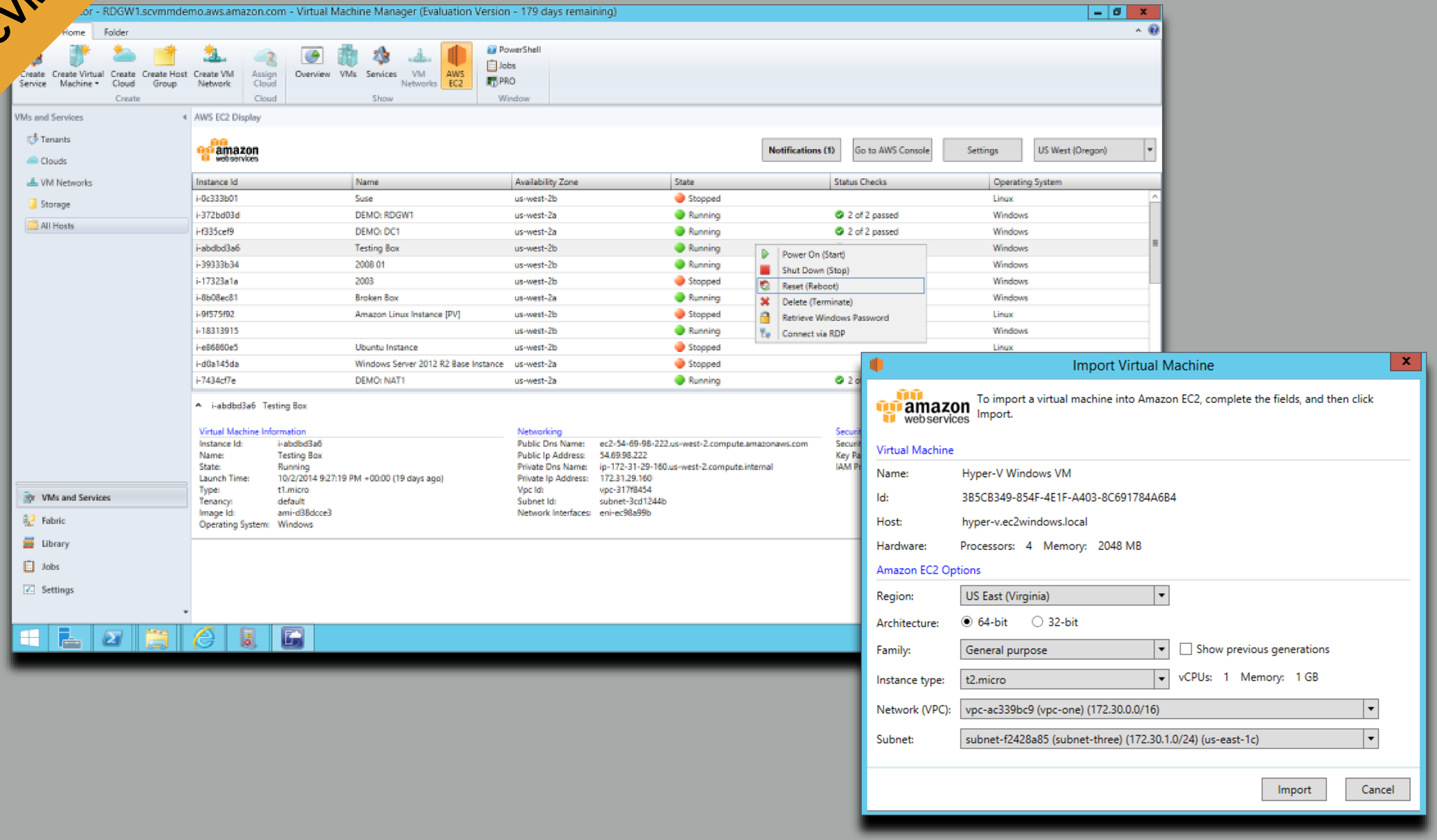
AWS Add-ins for Microsoft System Center

Use the familiar System Center interface to view and manage your Amazon EC2 for Microsoft Windows Server resources within the AWS Cloud, as well as Windows Servers installed on-premises.

AWS Management Pack for Microsoft System Center Operations Manager (**SCOM**)

AWS Systems Manager for Microsoft System Center Virtual Machine Manager (**SCVMM**)

AWS Systems Manager for Microsoft SCVMM



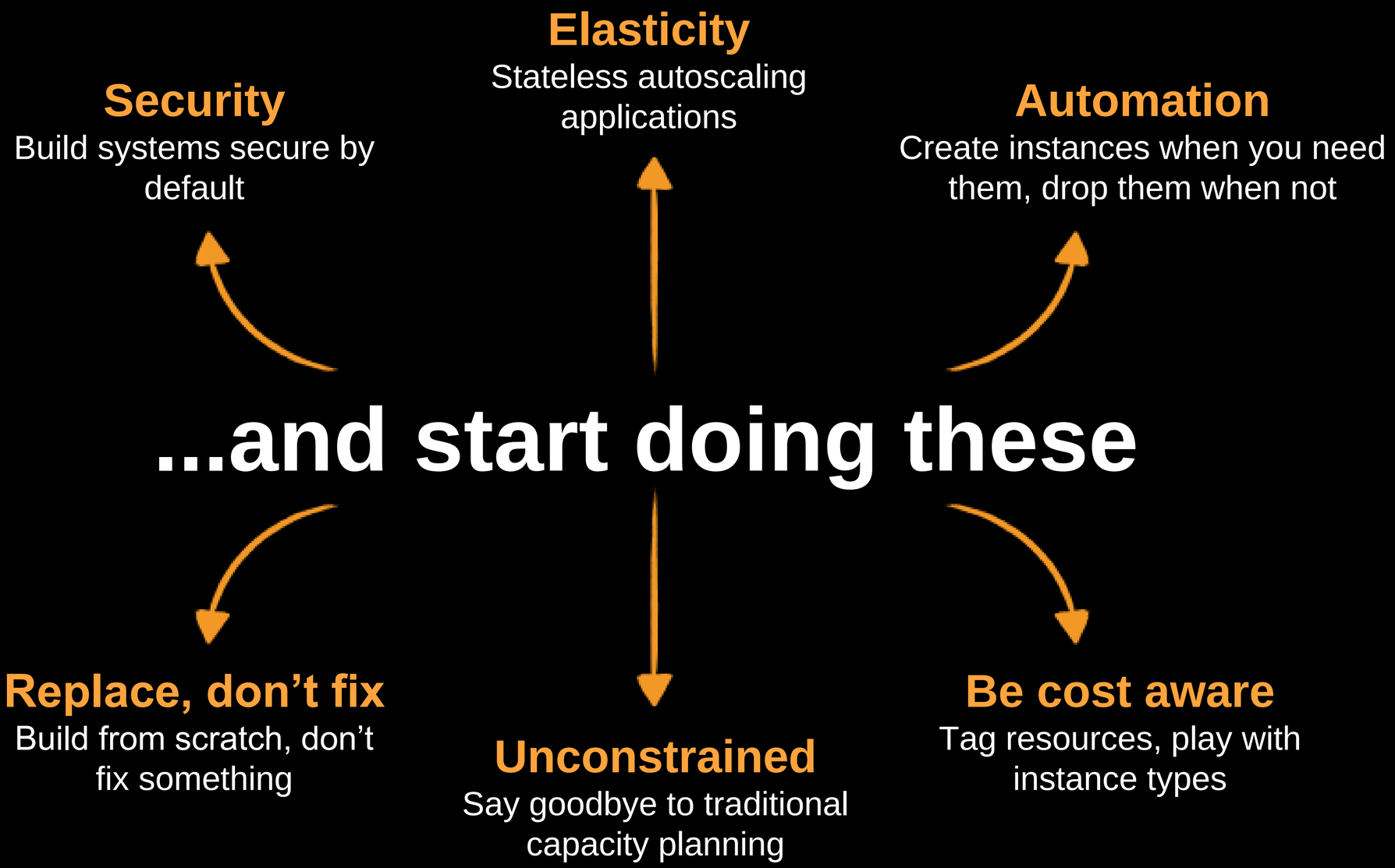
SUMMARY

What we just saw

Instances
Storage
Network
Monitoring & Logs
Security & Access Control
Management Tools
Deployment
Cost Optimization
3rd Party Tools

Stop doing these...

Provisioning and fixing servers
Treating compute as physical things
Thinking of compute as a finite commitment


Elasticity
Stateless autoscaling applications
Security
Build systems secure by default
Automation
Create instances when you need them, drop them when not
...and start doing these
Replace, don’t fix
Build from scratch, don’t fix something
Unconstrained
Say goodbye to traditional capacity planning
Be cost aware
Tag resources, play with instance types

#awswebinar