Workshop #4
Global Infrastructure, Security, Monitoring & Analytics

Announcement: Rebranding!

We are now an official AWS club!

We will be rebranding to the AWS Cloud Club in the coming days.

AWS Community Code of Conduct (amazon.com)

Membership: Please join the Meetup.com

Check-In

Last Workshop

Networking

Practice your skills on AWS Skill Builder regularly to stay sharp on your skills!

AWS Global Infrastructure

“To understand the AWS global infrastructure, consider the coffee shop. If an event such as a parade, flood, or power outage impacts one location, customers can still get their coffee by visiting a different location only a few blocks away”

Region

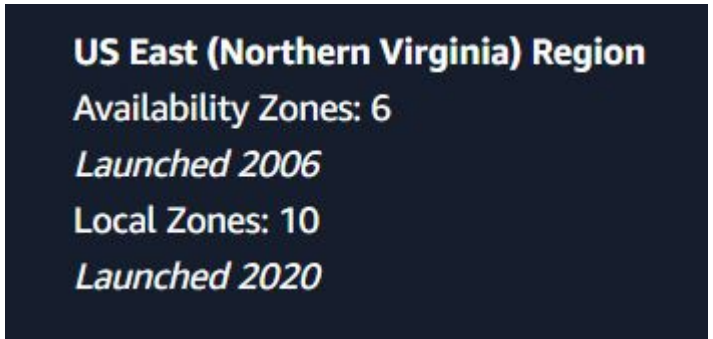
- Consists of:
  - Data centers
  - Networking
  - All the hardware for AWS services
- Regions are isolated from each other
  - Governance compliance

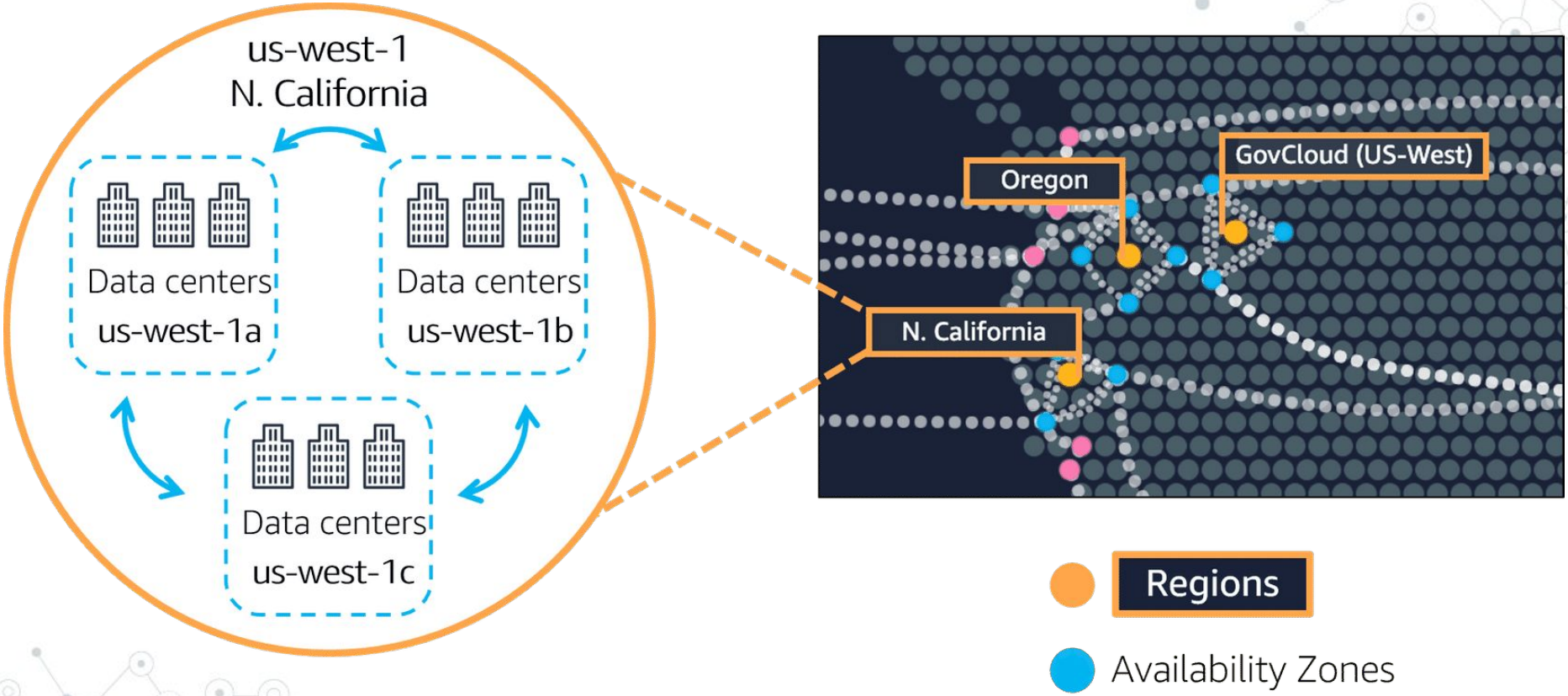
What Region Do I Pick?

- Compliance with governments
- Proximity to customers
  - Lower latency when closer
- Availability of products in regions
- Pricing
  - Ex: Brazil is more expensive due to their tax structure

Availability Zones (AZ)

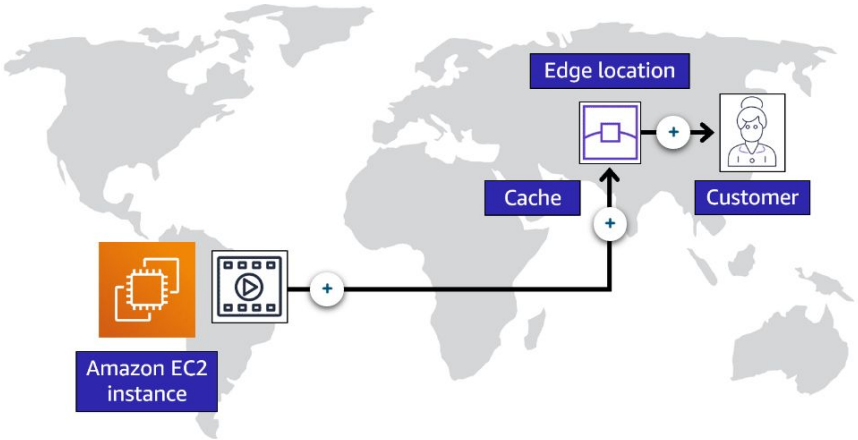
- A single (or group of) data center(s)
- Redundant power, networking, and connectivity
- Region consists of multiple isolated
- Best practice is to have operations in multiple AZs




us-west-1
N. California
Data centers
us-west-1a
Data centers
us-west-1b
Data centers
us-west-1c
Oregon
GovCloud (US-West)
N. California
Regions
Availability Zones

Edge Locations

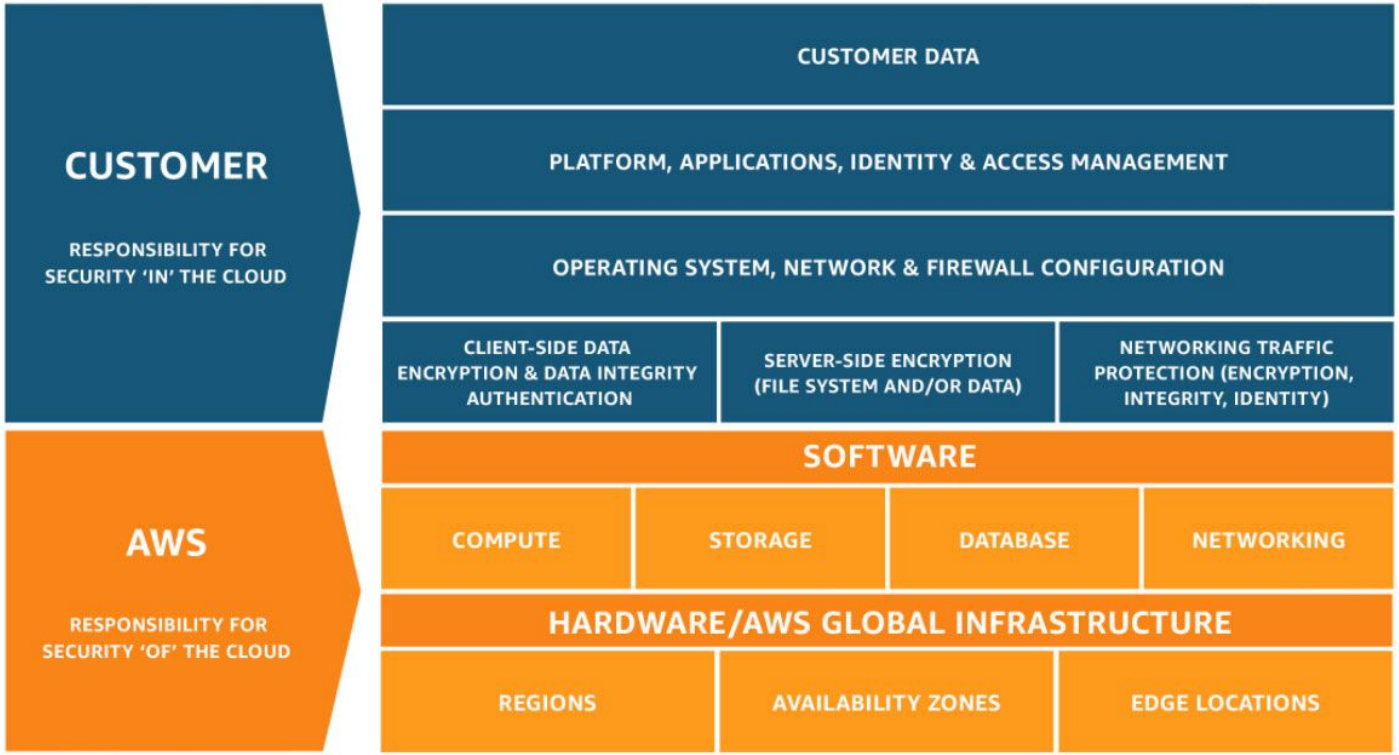
- Caching service to deliver content faster



AWS Edge Locations

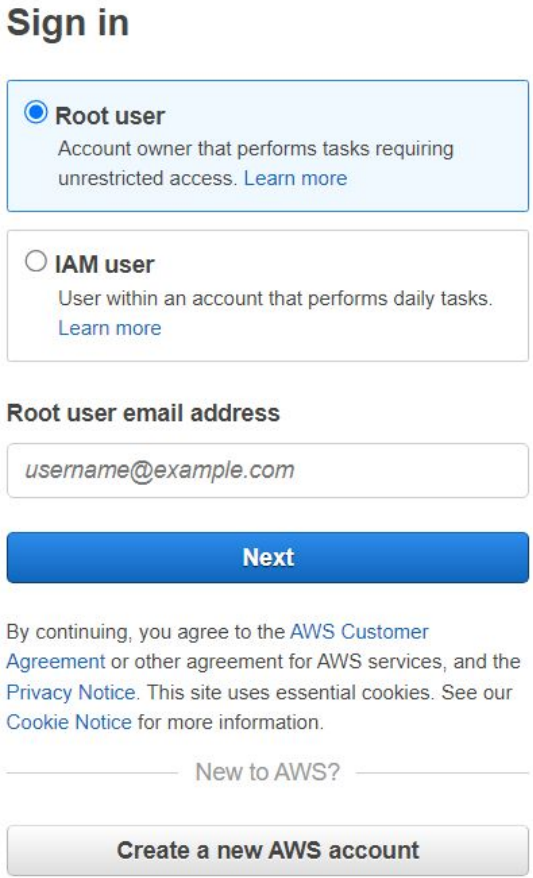
Edge locations - Ashburn, VA; Atlanta GA; Boston, MA; Chicago, IL; Dallas/Fort Worth, TX; Denver, CO; Hillsboro, OR; Houston, TX; Jacksonville, FL; Los Angeles, CA; Miami, FL; Minneapolis, MN; Montreal, QC; New York, NY; Newark, NJ; Palo Alto, CA; Phoenix, AZ; Philadelphia, PA; Querétaro, MX; San Jose, CA; Seattle, WA; Toronto, ON; Vancouver, BC

The AWS shared responsibility model



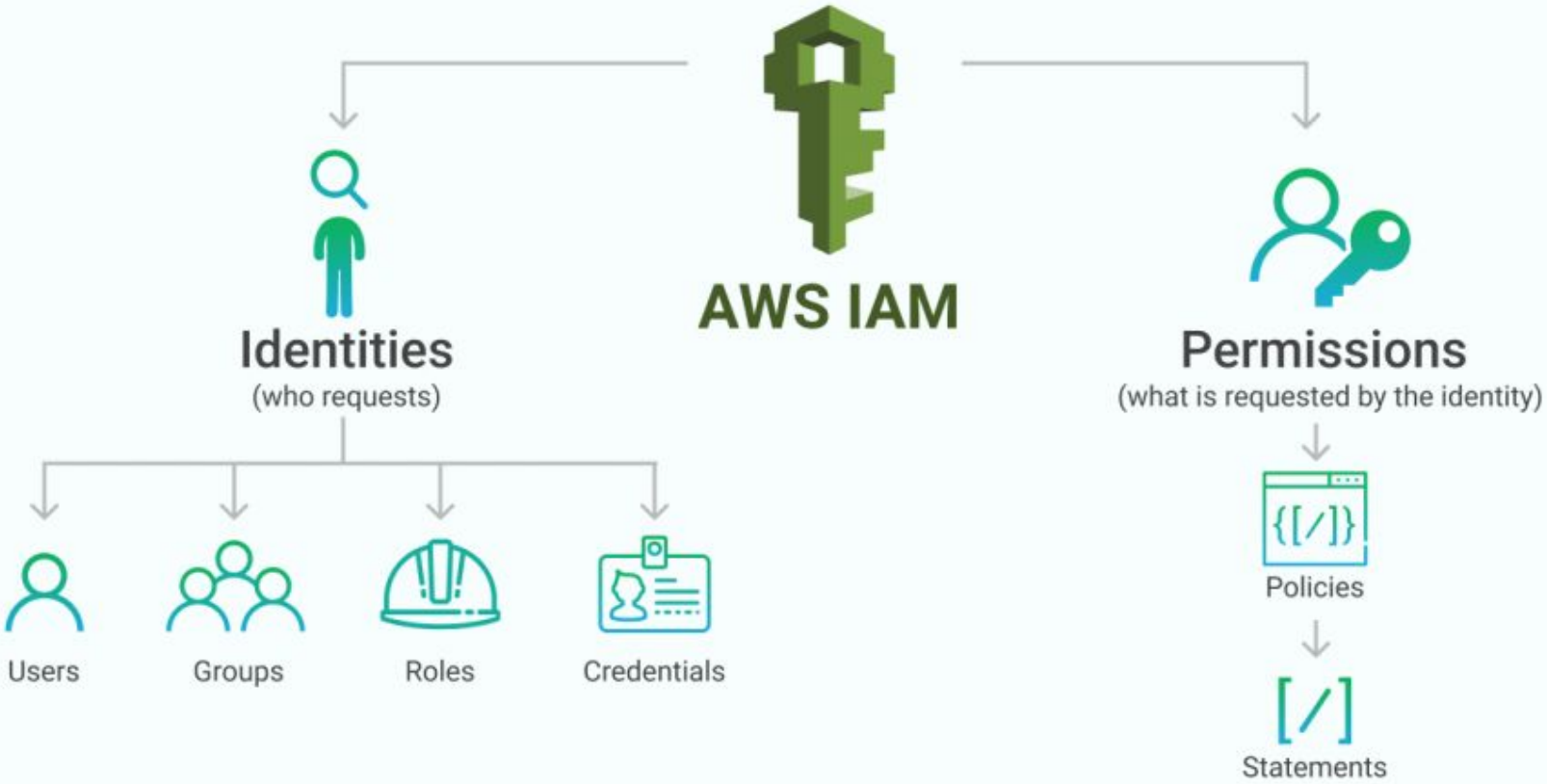
AWS Users

- Root users
  - User when you create AWS account
  - Complete access to all AWS account services and resources
- IAM users
  - AWS Identity and Access Management (IAM) allows you to configure security settings
  - You create IAM users
  - You assign IAM users permissions to what they can access
    - New user has no permissions



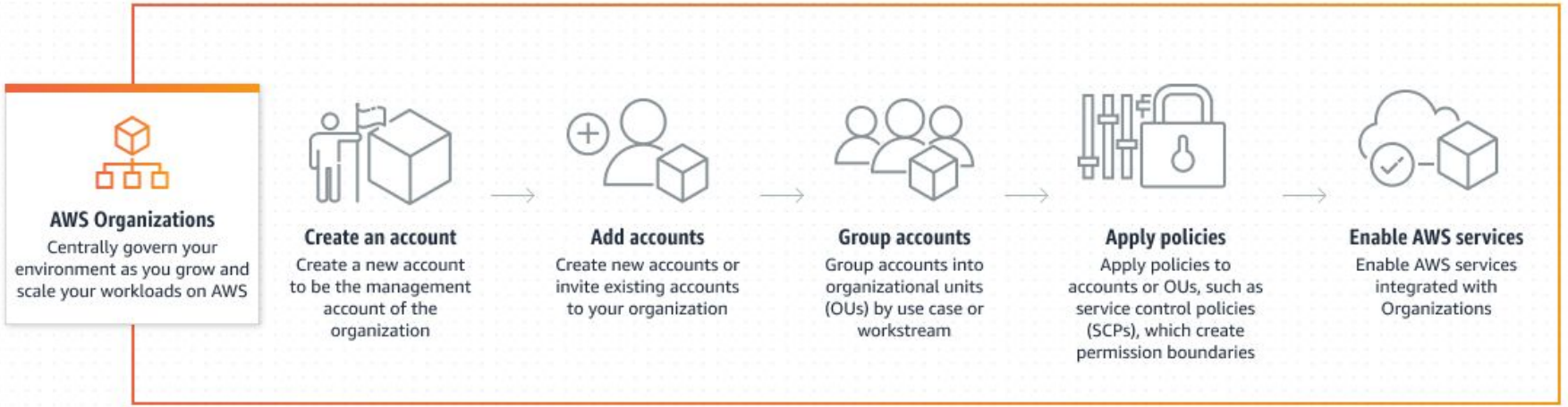
IAM Policy, Groups, and Roles

- Policy
  - Allows a specific action
    - Ex: Attach policy to let user view S3 bucket
- IAM Groups
  - A collection of IAM users
  - You can assign policies to IAM Groups
    - Ex: Group “students” given certain policies
- IAM Roles
  - “An IAM role is an identity that you can assume to gain temporary access to permissions.”


AWS IAM
Identities
(who requests)
Users
Groups
Roles
Credentials
Permissions
(what is requested by the identity)
Policies
Statements

AWS Organizations

- Some companies have multiple AWS accounts
- Can use an Organization to manage all those AWS accounts in a central location
  - Ex: consolidated billing, compliance, security, and resources
- Service Control Policies (SCP)
  - Organizational equivalent of IAM Policy
- Organizational Unit (OU)
  - Organizational equivalent of IAM Group


AWS Organizations
Centrally govern your environment as you grow and scale your workloads on AWS
Create an account
Create a new account to be the management account of the organization
Add accounts
Create new accounts or invite existing accounts to your organization
Group accounts
Group accounts into organizational units (OUs) by use case or workstream
Apply policies
Apply policies to accounts or OUs, such as service control policies (SCPs), which create permission boundaries
Enable AWS services
Enable AWS services integrated with Organizations

AWS Compliance Services

- AWS Artifact
  - On demand access to AWS compliance and security reports
  - Artifact Agreements
    - Company can sign agreement on AWS about how certain data is used
  - Artifact Reports
    - Report of possibility relevant regulatory information for your project
- Customer Compliance Center
  - White papers and documentation on certain compliance information

AWS Security Services

AWS Shield

- AWS Shield
  - Service to protect against DDOS
    - Standard(no cost), Advanced(cost)

AWS KMS

- AWS Key Management Service (AWS KMS)
  - Performs encryption of cryptographic keys

AWS WAF

- AWS Web Application Firewall (WAF)
  - Monitor network requests that come into web applications
- Amazon Inspector
  - Perform automated security assessments

- AWS GuardDuty
  - Intelligently detects threats; Continuously monitors network activity

AWS Monitoring & Analytics Services

- Amazon CloudWatch
  - Monitor services

- AWS CloudTrail
  - Monitor Account Activity

- AWS Trusted Advisor
  - Advising how to use your AWS stuff better

Amazon CloudWatch

- “Amazon CloudWatch is a web service that enables you to monitor and manage various metrics and configure alarm actions based on data from those metrics.”
- Alarms
  - Set alarms that send you notifications when predefined thresholds are passed
- Dashboard
  - Allows you to see utilization metrics from a consolidated location

AWS CloudTrail

- “AWS CloudTrail records API calls for your account. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, and more”
- Insights
  - CloudTrail Insights can automatically detect unusual API activity on your AWS account
- Logging service for AWS account

AWS Trusted Advisor

- “AWS Trusted Advisor is a web service that inspects your AWS environment and provides real-time recommendations in accordance with AWS best practices.”
- Five categories of monitorization

Hands-on Demo

Please fill out this Post-Event Survey!

THANK YOU!