2023 INTERNET2 TECHNOLOGY exchange

MOVING FROM VIRTUAL MACHINES TO CLOUD-NATIVE CONTAINERS

PRESENTER NAME:

University of California, Office of the President

- Khalid Ahmadzai, Sr. Cloud Engineer

About Us

University of California:

- 10 Campuses - undergraduate/graduate
- 6 Academic Health Centers
- 3 National Laboratories

University of California, Office of the President (UCOP):

- Systemwide infrastructure services
- Local infrastructure services
- > 50 cloud accounts

Khalid Ahmadzai
Sr. Cloud Engineer

Amazon Elastic Container Service (ECS)

AMAZON ECS ON FARGATE | OVERVIEW

- **What is it?**
  - https://docs.aws.amazon.com/AmazonECS/latest/developerguide/Welcome.html
  - ECS is a fully managed container orchestration service that helps you easily deploy, manage, and scale containerized applications.
- **What problem did it fix for us?**
  - Deploy & Manage Applications
    - Focus on building and operating your application
    - Avoid the operational overhead of scaling, securing, and managing servers
  - Security Isolation
    - Each pod runs on dedicated kernels
    - Do not share CPU, memory, or network resources
    - Uses encrypted images
  - Right-Sized Resources
    - Launch and scale the compute to match the right-sized resource

AMAZON ECS | OVERVIEW

Why did we choose ECS over other tools?

- **Scalability:** ECS automatically scales your applications based on demand, allowing you to easily handle changes in traffic or workload.
- **High availability:** ECS provides built-in availability and fault tolerance, ensuring that your applications are always up and running.
- **Cost-effective:** ECS enables you to optimize your infrastructure costs by scaling resources based on demand and only paying for what you use.
- **Integration:** ECS integrates with other AWS services such as ECR, Fargate, CloudWatch, load balancer, and IAM.
- **Security:** ECS provides a secure environment to run your applications, with features such as IAM roles for tasks, VPC isolation, and encryption at rest.

AMAZON ECS | SECURITY

How do we secure containers?

- **Identity and Access Management (IAM):** Rule-based policies for authentication and authorization.
- **Network Security:** Encryption-in-transit, network segmentation, and isolation.
- **Secrets Management:** API keys and database credentials are stored in the secrets manager.
- **Logging and Monitoring:** Sending all log information to CloudWatch Logs and S3 in a separate account.
- **Container Storage:** Are encrypted by KMS.
- **Container connection:** Accept inbound traffic only from the load balancer.
- **Image Vulnerabilities:** Images are regularly scanned by Amazon Inspector.
- **Read-Only Root File Systems:** Root file systems are set to read-only to reduce security attack vectors.
- **Monthly Patching:** All containers are automatically rebuilt monthly to get the latest security patches.
- **Secure Load Balancer:** HTTPS listeners to secure communication between clients and load balancers.
- **Web Application Firewall (WAF):** All Load Balancers are integrated with WAF.

AMAZON ECS | FEATURES

Which ECS features do we use?

- **AWS Fargate:** Let our developers focus more on development and less on cluster configuration, provisioning, and patch management.
- **Blue/Green Deployments:** Reduces downtime during application deployments and updates.
- **Sidecar Container:** Runs alongside the main container to provide additional services.
- **Integration:** It integrates with the AWS load balancer to distribute traffic.
- **Native Docker Support:** Amazon ECS supports Docker out of the box, allowing developers to package applications locally and deploy them at scale without configuration changes.
- **Programmatic Control:** Allows developers to integrate and extend their service through APIs.
- **Container Auto-Recovery:** Automatically recover failed containers.
- **Scheduling:** Containers can be scheduled to deploy at a specific time and date.

AMAZON ECS | MIGRATIONS

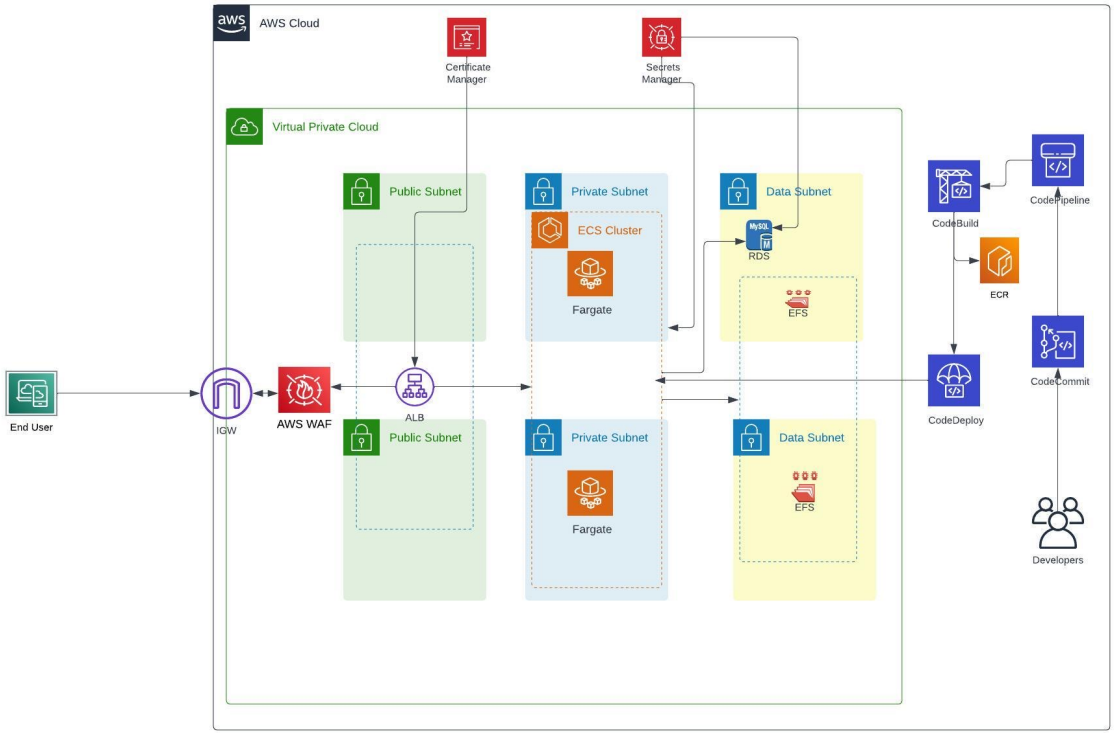
How many applications we migrated?

- 19 out of 37 Prod Applications
- 24 out of 37 QA Applications
- 27 out of 37 Dev Applications

AMAZON ECS | DIAGRAM

How do we use it?

- VPC with 6 subnets
- CICD Pipeline
- ECS Cluster
- RDS
- Secrets Manager
- EFS
- Load Balancer
- Certificate Manager
- WAF



UCOP @ Technology Exchange

Join us for our 2023 Technology Exchange presentations by UCOP team members:

- Moving from VM to Cloud Native Containers with Khalid Ahmadzai, Tuesday 11:20 am-12:10 pm
- Cloud Security By Default with Matthew Stout and George Holbert, Thursday 10:20 am-11:10 am
- Control Chaos with IaC & Automation with Josh Whitlock, Thursday 1:40 pm-2:30 pm

2022 Technology Exchange presentation by UCOP's own Khalid Ahmadzai, Kari Robertson, Matt Stout

- Moving from Cloud Chaos to Standards:
  https://internet2.edu/wp-content/uploads/2022/12/techex22-Cloud-MovingfromCloudChaostoStandards-AhmadzaiStoutRobertson.pdf

QUESTIONS