Running Moodle on AWS: Architectures, scaling and security

MoodleMoot Finland 2024

Andreas Asuja (he/him)

Senior Solutions Architect
Public sector, Nordics

Moodle architecture overview

Moodle architecture overview - Components

Load balancer

When deployed in high availability, Moodle needs a load balancer to distribute traffic among the available application servers.

Application Server

Moodle is a web application written in PHP. Although is primary developed in Linux using Apache as webserver, it can run on other PHP-capable web servers such as Nginx or IIS. Moodle is also friendly with ARM CPU architecture.

Database

Moodle database backend can be PostgreSQL, MySQL, MariaDB, Microsoft SQL Server, Amazon Aurora PostgreSQL and, from version 3.9.4, Amazon Aurora MySQL.

Storage
moodledata/

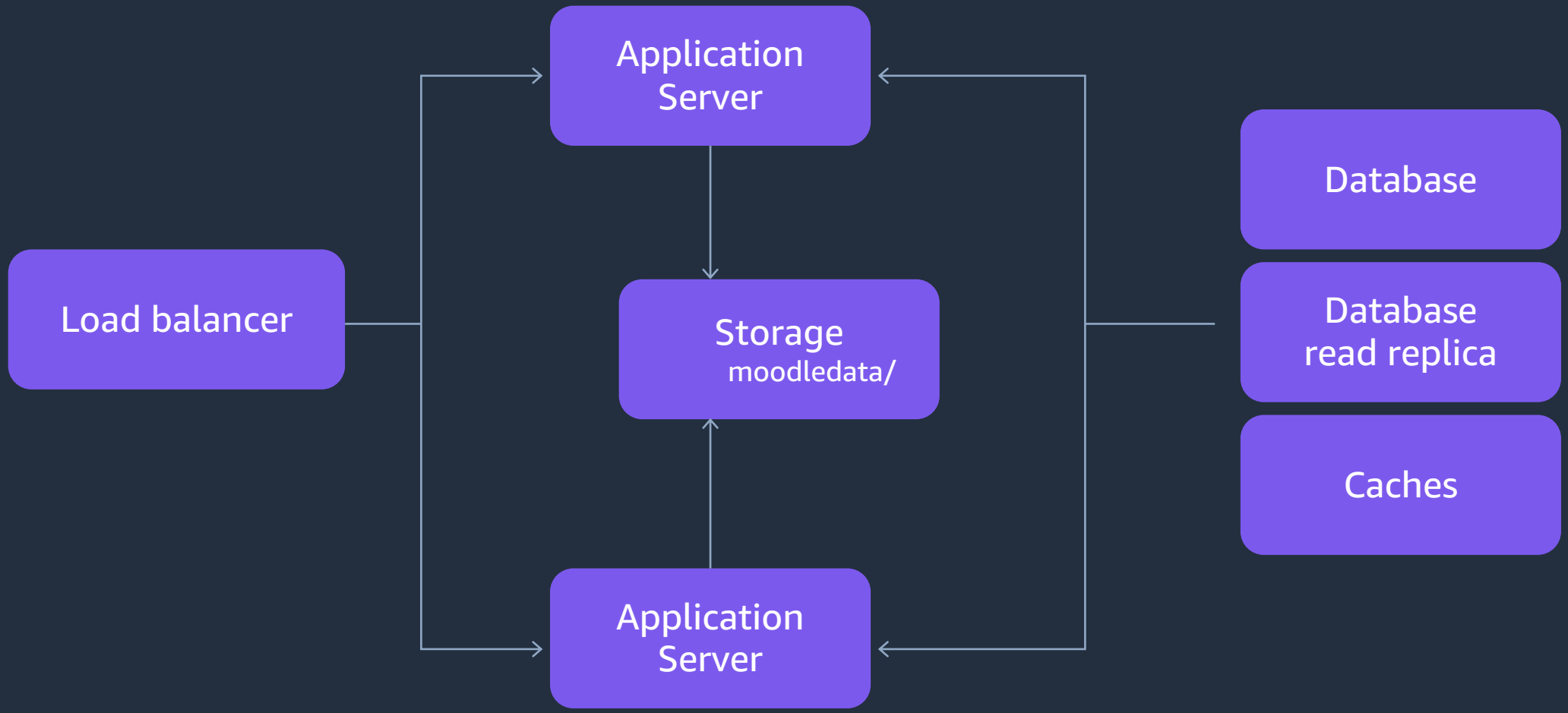
A file system shared between the application servers, used to store and retrieve content as well as a temporary file cache.

Cache

When deployed in high availability, Moodle requires two caches to be enabled: session and application cache. Supported cache technologies include Memcached and Redis.

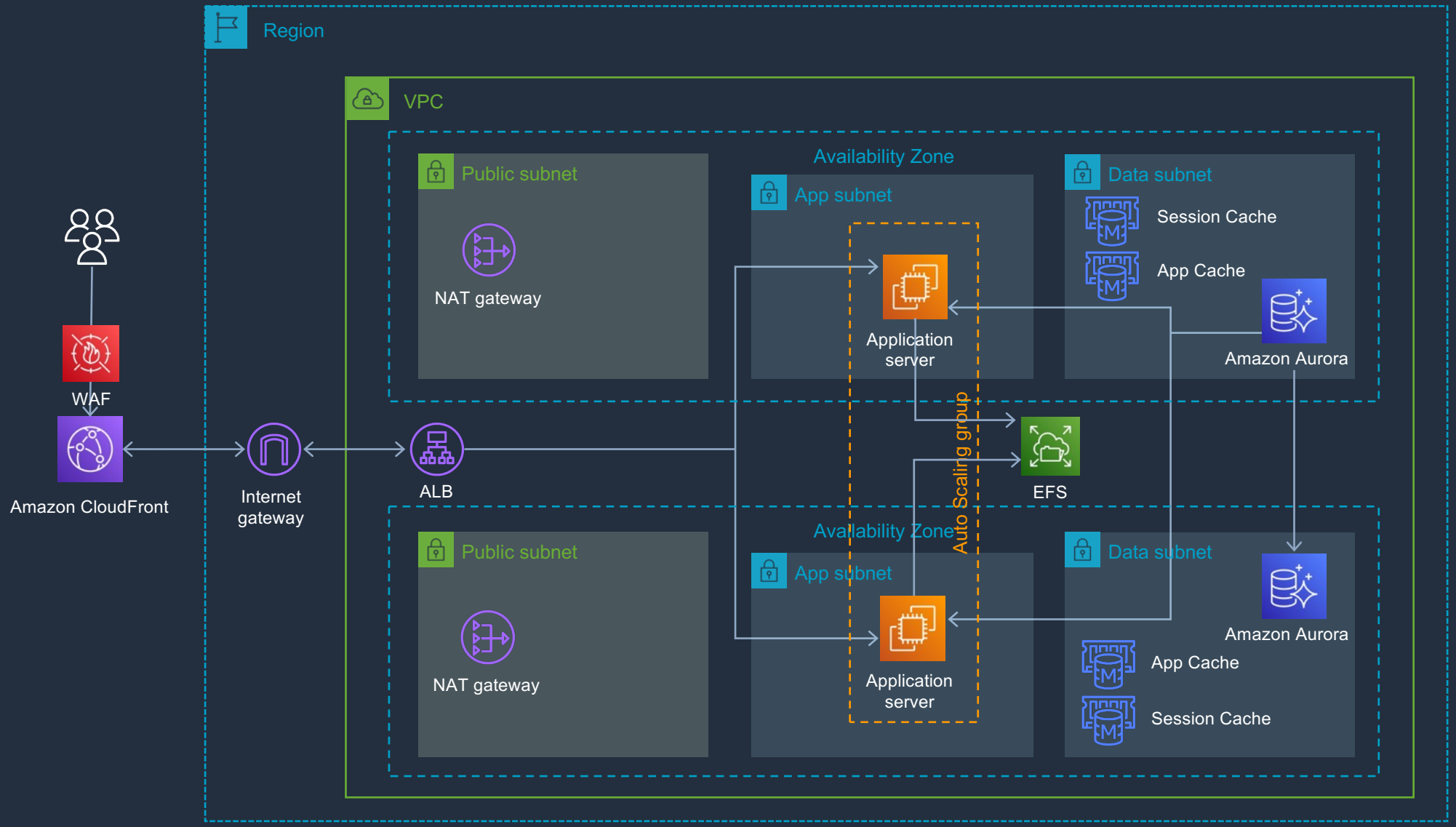
aws

Moodle architecture overview - Components



Moodle on AWS: EC2

Moodle on AWS - Reference architecture



https://github.com/aws-samples/aws-refarch-moodle

Container orchestration on AWS

Container orchestration on AWS

ECS

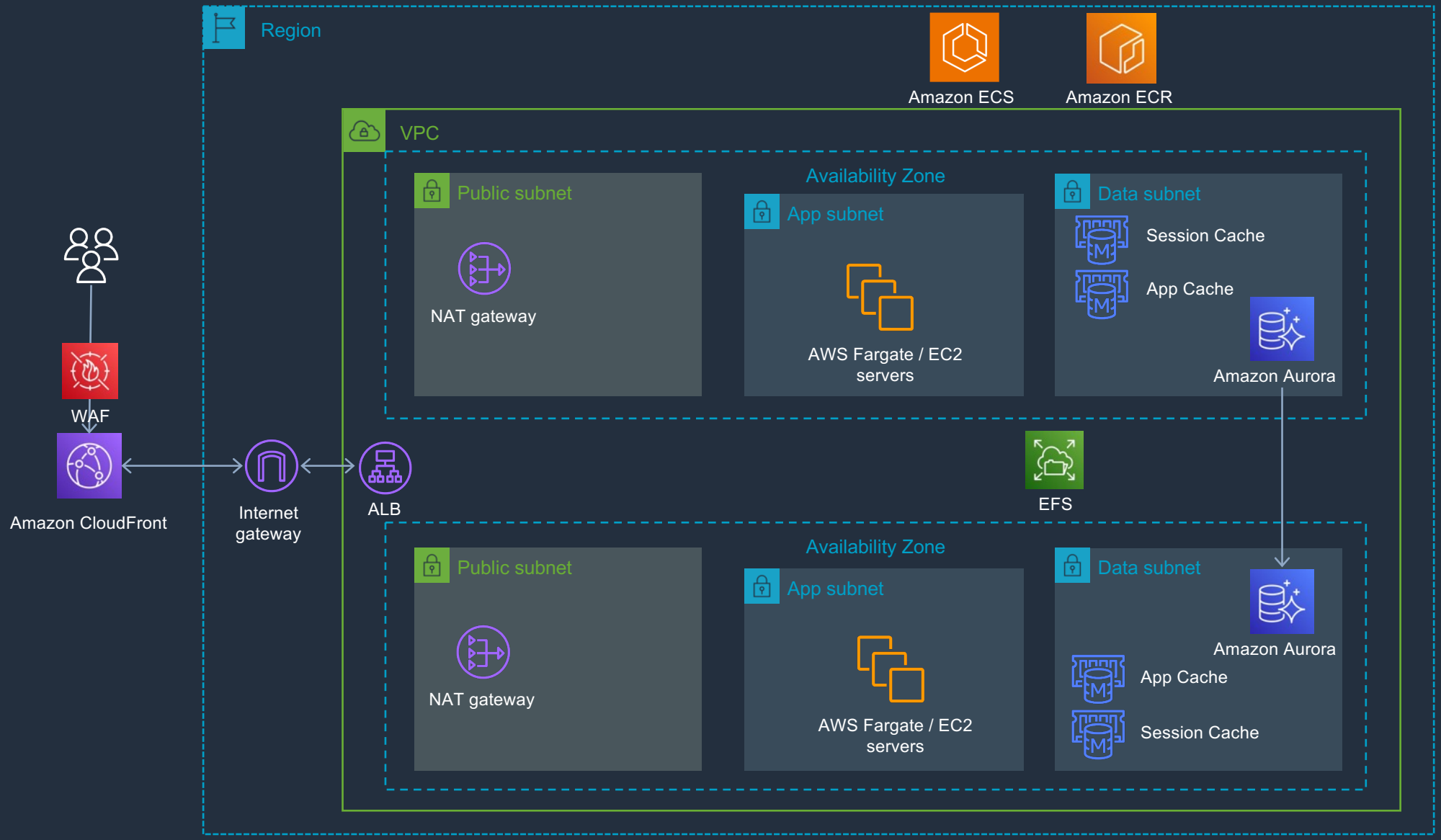
Powerful simplicity

EKS

Open flexibility

Moodle on AWS: Elastic Container Service - ECS

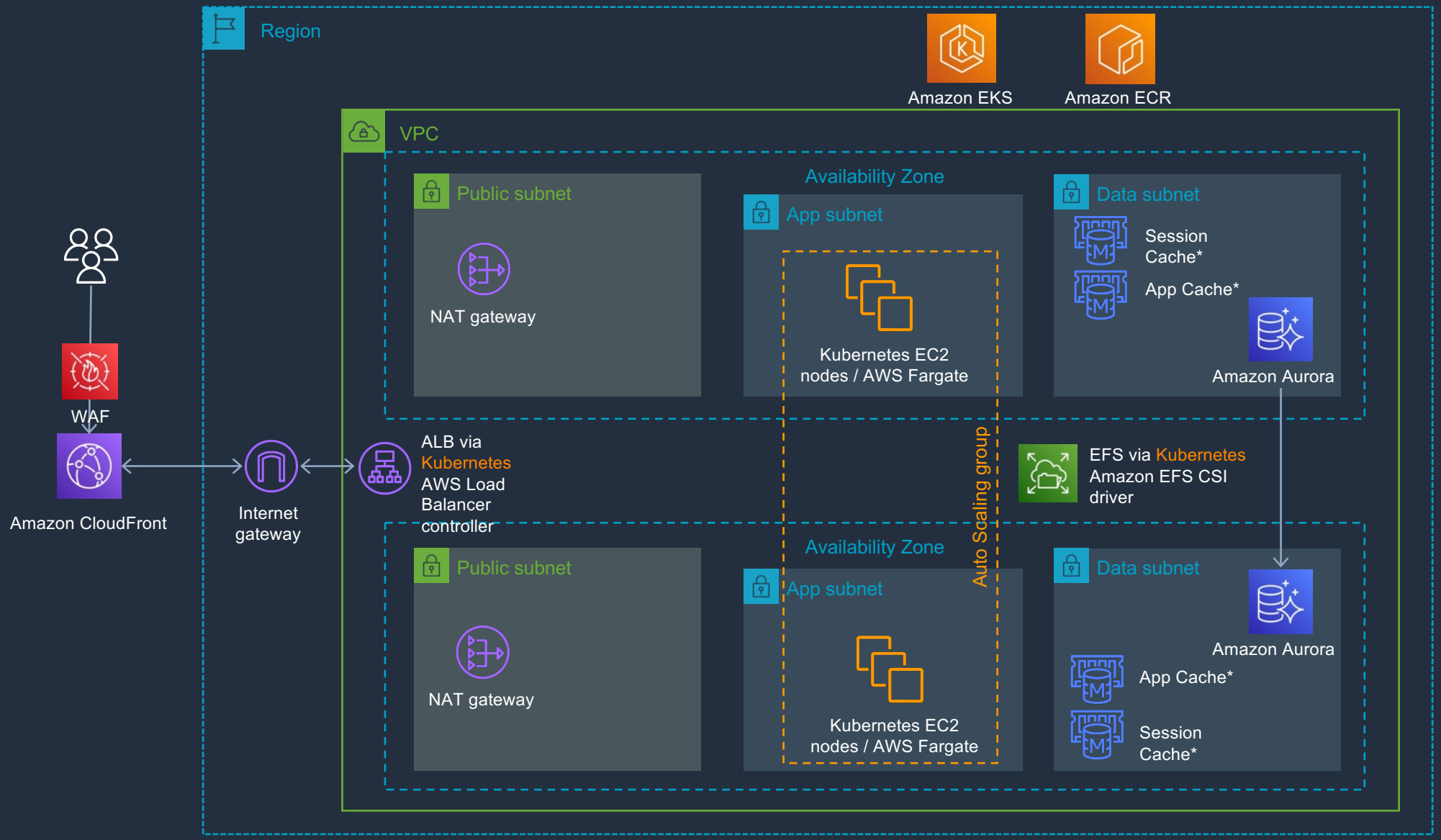
Moodle on AWS - ECS physical architecture



https://github.com/aws-samples/aws-cdk-ecs-refarch-moodle

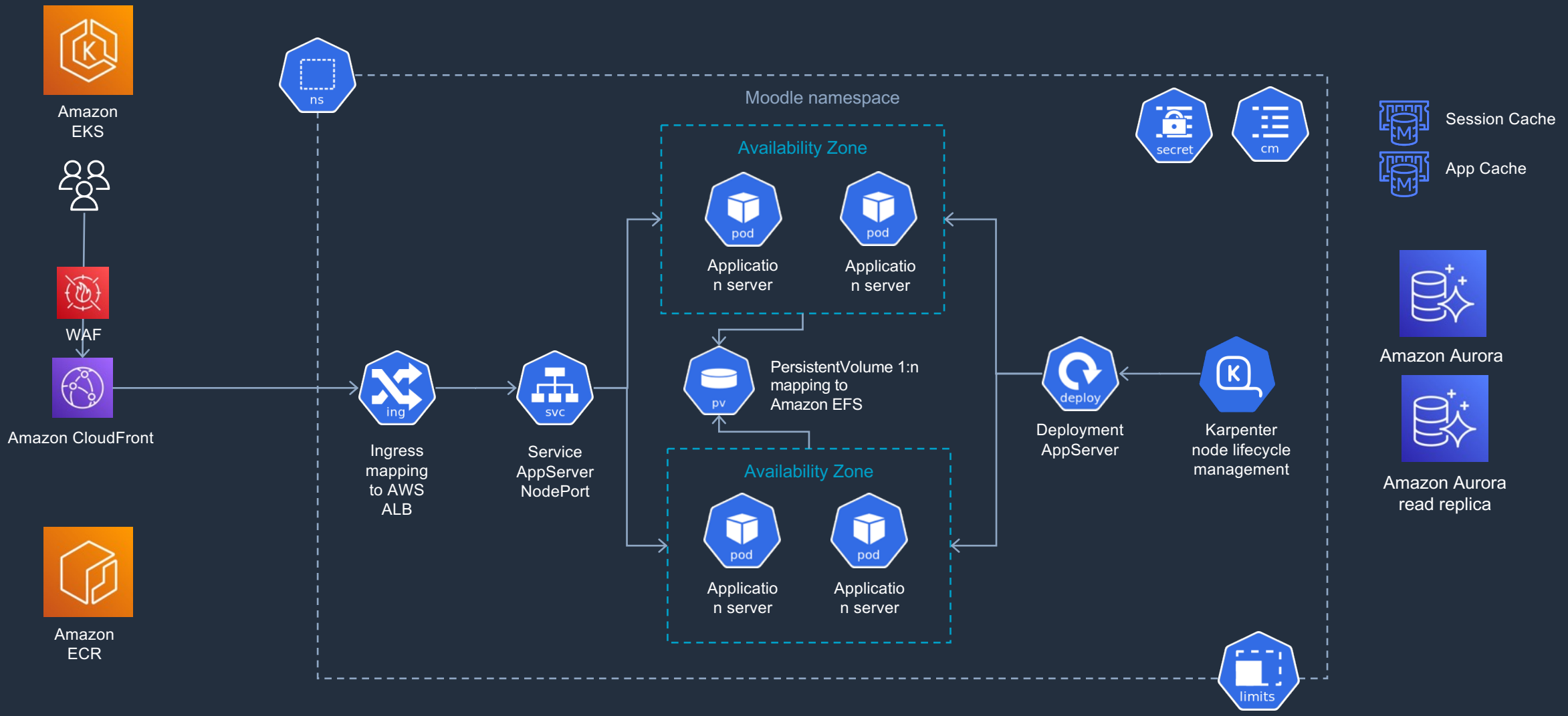
Moodle on AWS: Kubernetes - Elastic Kubernetes Service - EKS

Moodle on AWS - Kubernetes physical architecture



* can be moved into the EKS cluster

Moodle on AWS - Kubernetes logical architecture



Comparison of the architectures

EC2

Pros:

- No containers?
- First setup easy

Cons:

- No scaling
- Patching servers
- Manual operations
- Servers become pets

EC2 with auto-scaling

Pros:

- No containers?

Cons:

- Slowest scaling
- Patching servers

ECS

Pros:

- Simplest to setup and operate

Cons:

- ?

EKS

Pros:

- Kubernetes!
- Fastest scaling with Karpenter

Cons:

- Kubernetes?
- Hardest one to setup and operate
- Kubernetes updates needed regularly
- Also nodes need to be updated

Demo: Scaling Moodle on AWS ECS

Securing Moodle on AWS

Identity and Access Management

- Use **multiple AWS accounts** to reduce scope of impact

AWS accounts provide administrative isolation between workloads across different lines of business, regions, stages of production and classes of data.

- Use **limited roles** and grant **temporary security credentials**

IAM roles and temporary security credentials mean you don't always have to manage long-term credentials and IAM users for each entity that requires access to a resource.

- **Federate** to an existing identity service

Control access to AWS resources, and manage the authentication and authorization process without needing to recreate all your corporate users as IAM users.

Logging and Monitoring

- **Turn on logging** in all accounts, for all services, in all regions

AWS CloudTrail

Amazon GuardDuty

The AWS API history in CloudTrail enables security analysis, resource change tracking, and compliance auditing. GuardDuty provides managed threat intelligence and findings.

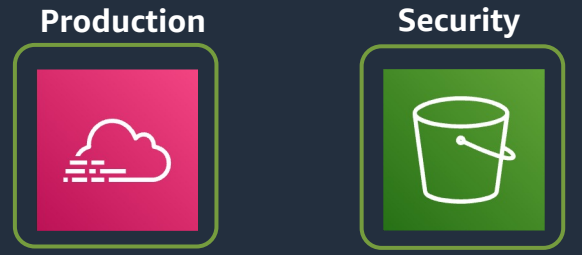
- Use the AWS platform's built-in **monitoring and alerting** features

AWS Security Hub

AWS Config

Monitoring a broad range of sources will ensure that unexpected occurrences are detected. Establish alarms and notifications for anomalous or sensitive account activity.

- Use a separate AWS account to fetch and **store copies of all logs**



Configuring a security account to copy logs to a separate bucket ensures access to information which can be useful in security incident response workflows.

Infrastructure Security

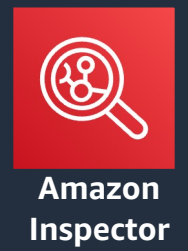
- Create a **threat prevention layer** using AWS edge services

Use the hundreds of worldwide points of presence in the AWS edge network to provide scalability, protect from denial-of-service attacks, and protect from web application attacks.

- Create **network zones** with Virtual Private Clouds (VPCs) and security groups

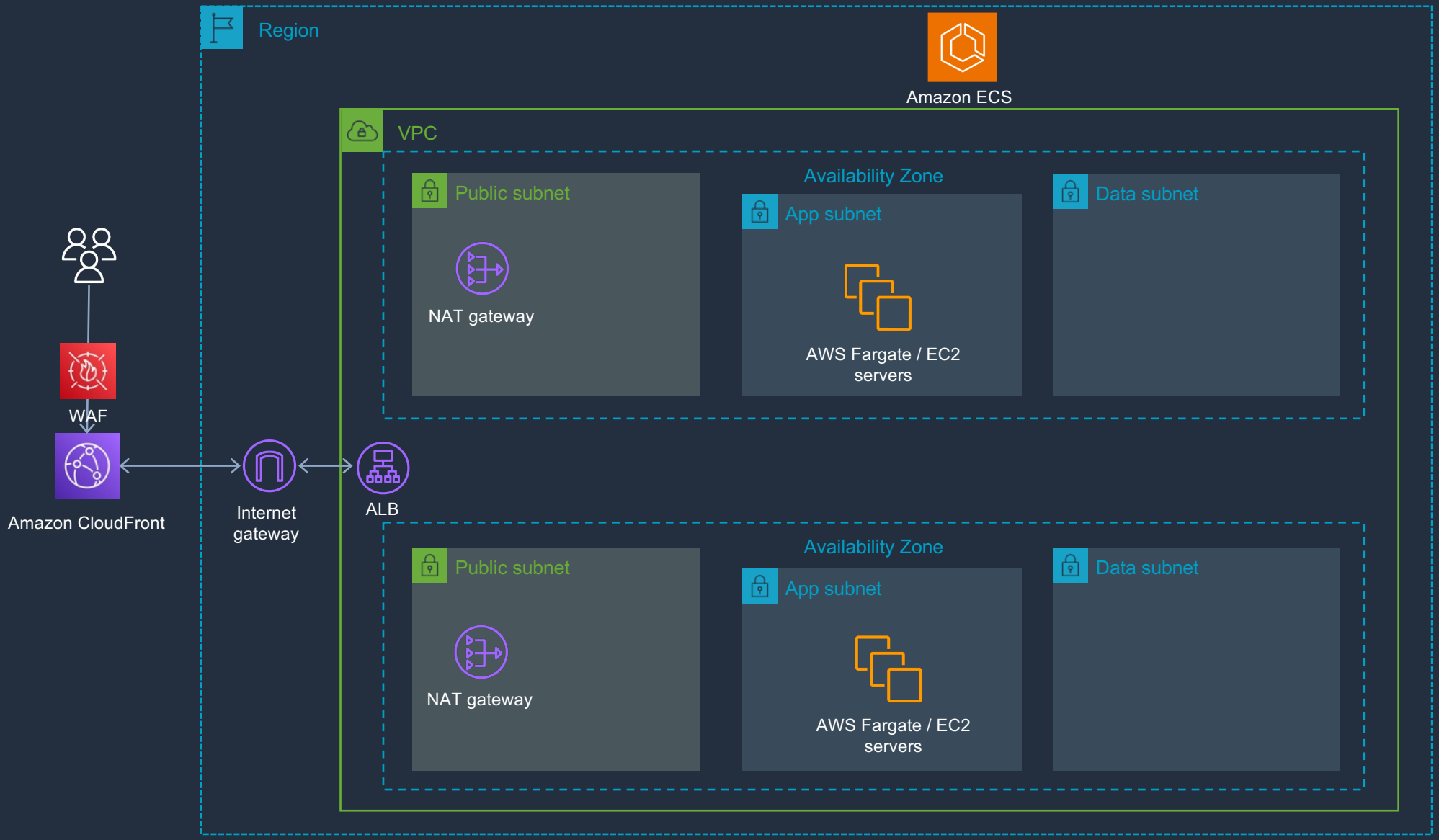
Implement security controls at the boundaries of hosts and virtual networks within the cloud environment to enforce access policy.

- Manage vulnerabilities through **patching and scanning**

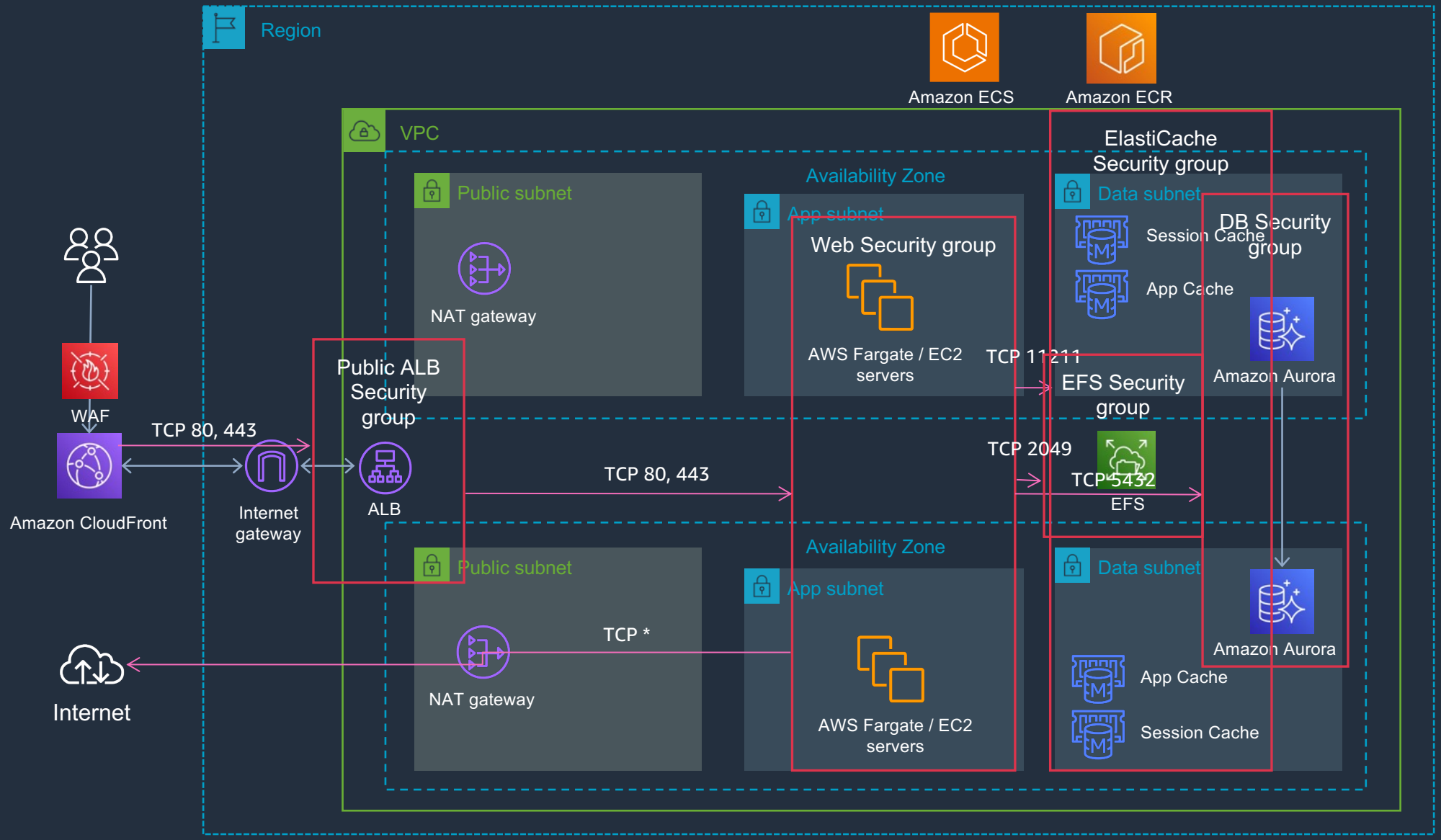


Test virtual machine images and snapshots for operating system and application vulnerabilities throughout the build pipeline, and into the operational environment.

Network security – Network segmentation

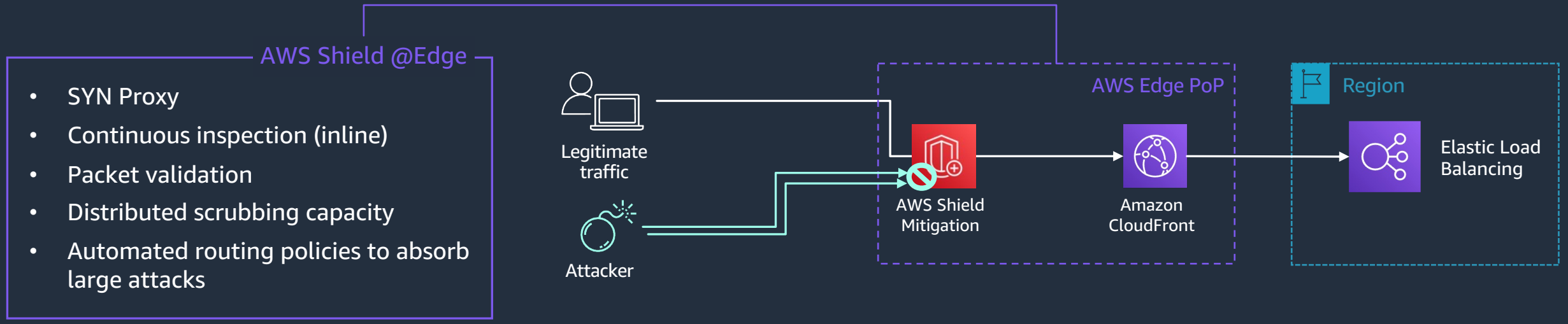


Network security – Security Groups



Infrastructure (L3-4) Protection with AWS Shield

AWS Shield DDoS **mitigation systems** are present at the AWS network border and at AWS edge locations.



Application (L7) Protection with AWS WAF

Seamless Integration

Amazon CloudFront

AWS Application Load Balancer

Amazon API Gateway

AWS AppSync

Guidelines for Implementing AWS WAF
https://docs.aws.amazon.com/whitepapers/latest/guidelines-for-implementing-aws-waf/guidelines-for-implementing-aws-waf.html

Features

AWS Managed Rules: Baseline, Use Case Specific, IP Reputation List and Anonymous IP List (Tor, Cloud Providers, etc.)

Custom Rules: Rate-based, Geo Location, IP Set Match, Size Constraint, String Match, etc.

Bot Protection: One click protection, allow common bots while blocking pervasive bots by category

WAF Automation on AWS: automatically deploys a set of AWS WAF rules that filter common web-based attacks

Partner Managed Rules: Available in the Partner Marketplace

Data Protection

- Encrypt **data at rest (**with occasional exceptions)

AWS KMS

Amazon S3

Enabling encryption at rest helps ensure the confidentiality and integrity of data. Consider encrypting everything that is not public.

- Use **server-side encryption** with provider managed keys

AWS KMS

Data Encryption Key

AWS Key Management Service (KMS) is seamlessly integrated with multiple AWS services. You can use a default master key or select a custom master key, both managed by AWS.

- Encrypt **data in transit** (with no exceptions)

Amazon CloudFront

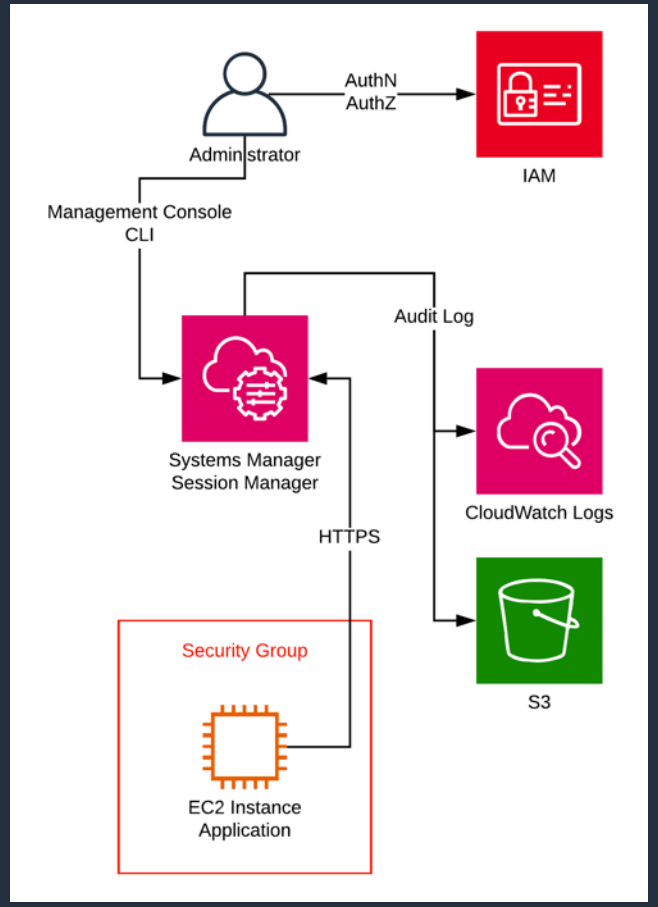
Certificate Manager

SSL / TLS / HTTPS

Encryption of data in transit provides protection from accidental disclosure, verifies the integrity of the data, and can be used to validate the remote connection.

AWS Systems Manager - Session Manager

Securely connect to a Managed Instance or container, without having to open an inbound port or manage SSH keys



AWS Blog: Moodle https://aws.amazon.com/blogs/publicsector/tag/moodle/

AWS Public Sector Blog

Tag: moodle

Modernize Moodle LMS with AWS serverless containers

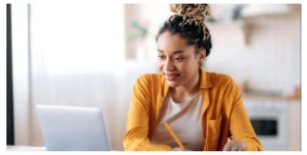
by Hendry Anwar | on 07 SEP 2022 | in Containers, Education, Public Sector, Technical How-to | Permalink | Comments | Share

Moodle is a popular open source learning management system (LMS). Many education institutions are deploying and running Moodle on a physical hardware or virtual machine (VM) environment. They are looking to improve the scalability of their Moodle application to simplify operations and monitoring, and also optimize operating costs. One way to approach this is to use containers technology. In this blog post, learn how to deploy and run Moodle using serverless containers technology on AWS.

How to scale and optimize Moodle LMS on AWS

by Yusuf Mayet | on 24 NOV 2021 | in Amazon EC2, Amazon RDS, AWS CloudFormation, AWS Database Migration Service, AWS Schema Conversion Tool, Education, Migration, Public Sector, Technical How-to | Permalink | Comments | Share

Moodle is an open-source learning management system (LMS). Moodle has more than 300 million users worldwide across both academic and enterprise organizations, and is the world's most widely used learning platform. There are many ways to get started with Moodle on AWS. In this blog post, I focus on how to scale and optimize Moodle once you are already serving students. In this case, you may need to deal with migrating data from an existing platform and making sure the new environment caters to thousands of students, and still be cost-effective — we cover additional considerations in this walkthrough.



How one Caribbean university digitally transformed and saved money by migrating to the cloud

by Reeve Ramharry, Manuel Cuellar, and Reiza Haniff | on 09 JUL 2021 | in Amazon EC2, Amazon Elastic File System (EFS), Amazon RDS, Amazon VPC, Auto Scaling, AWS Application Migration Service, AWS Well-Architected, AWS Well-Architected Tool, Customer Solutions, Education, Higher education, Migration, Public Sector | Permalink | Comments | Share

Moodle learning management system (LMS) and the UWIOC website, while saving 50 percent total cost of ownership along the way.

Moving to AWS helped The University of the West Indies, Open Campus (UWIOC) improve performance of systems and operational efficiency while optimizing costs. Learn how UWIOC migrated more than 70 virtual machines, 10 applications, and five networks, plus their

How UCL migrated its Moodle virtual learning environment to the cloud in 10 weeks

by Ray Rogers | on 29 JUN 2021 | in Amazon Aurora, Amazon EC2, Amazon Elastic Block Store (Amazon EBS), Customer Solutions, Education, Higher education, Public Sector | Permalink | Share

University College London's (UCL) virtual learning environment, built on the Moodle learning management system, is at the heart of its digital education infrastructure and used by students all over the world. Before migrating to Amazon Web Services (AWS), its system could handle 2,500 concurrent users. But when the pandemic drove schools and universities to predominantly online teaching, the UCL team wanted to support six times this amount in just 10 weeks. Here's how they did it with AWS.

Thank you!