PORTFOLIUM

Architecture Overview

Instructure Security, Engineering, and Operations

July 2021

In this guide, you'll learn:

How Portfolium has been architected as a native cloud application, providing unmatched availability, scalability, and reliability for our customers.

Table of Contents

Architecture Overview

CLOUD INFRASTRUCTURE

Portfolium is hosted with Amazon Web Services (AWS). The AWS Cloud infrastructure is built around Regions and Availability Zones (AZs). AWS Regions provide multiple, physically separated, and isolated Availability Zones which are connected with low latency, high throughput, and highly redundant networking. These Availability Zones allow Portfolium to efficiently design and operate its applications and databases, making them more highly available, fault tolerant, and scalable than traditional single datacenter infrastructures or multi-datacenter infrastructures.

NETWORK ARCHITECTURE

Portfolium utilizes Amazon VPC (Virtual Private Cloud) to isolate and control access, both into and out of its network. On top of the AWS network, all DNS traffic is routed through CloudFlare's world-renowned private DNS network, enhancing performance and security as it prevents DDoS and other known attacks.

DATA STORAGE

Portfolium utilizes Amazon S3 (Simple Storage Service) to store user-uploaded artifacts (documents, images, etc.). Amazon S3 provides a highly durable storage infrastructure designed for mission-critical and primary data storage. Objects are redundantly stored on multiple devices across multiple facilities in an Amazon S3 region.

Amazon S3 also regularly verifies the integrity of data stored using checksums. If Amazon S3 detects data corruption, it is repaired using redundant data. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Amazon S3's standard storage is:

- Backed with the Amazon S3 Service Level Agreement
- Designed to provide 99.999999999% durability and 99.99% availability of objects over a given year
- Designed to sustain the concurrent loss of data in two facilities

LOAD MONITORING

Portfolium uses New Relic at the server and application layer to probe and test various layers of the platform. If there is an alert, and email will be triggered, then after 5 minutes if nothing was resolved, a text message will be sent out. Pingdom is used as a secondary ping check on Portfolium.com as well.

We have a stateless web architecture that grows horizontally. Using AWS OpsWorks based on load, memory usage, or CPU level, the system can automatically spin up a new web server and add it to the layer whether it be at the web layer or API layer.

Portfolium successfully scales to launch multiple 30K+ student universities in a single day, alongside their 100K+ alumni networks.

FILE STORAGE

All files that are uploaded to Portfolium are stored on a private S3 bucket in AWS (Amazon Web Services). When requested to view and/or download, based on authentication and access rules of the artifact, the application generates an access token for the browser to download the file from the file store. e-Portfolio data in movement on Portfolium is encrypted over HTTPS with a TLS v1.2 SSL cert. Password data at rest is 1-way salted then one-way hashed with a SHA-1 algorithm.

e-Portfolio data backups are encrypted using enterprise-grade encryption (AES 256-bit key). The data is encrypted before it leaves the server and remains encrypted while stored. Portfolium's servers, from power supplies to the internet connection to the air purifying systems, operate at full redundancy. Our systems are engineered to stay up and online even if multiple servers fail

Our state-of-the-art servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center.

24/7/365 onsite staff provides additional protection against unauthorized entry and security breaches. Our software infrastructure is updated regularly with the latest security patches. While perfect security is a moving target, we work with security researchers to keep up with the state-of-the-art in web security.

BACKUP ENVIRONMENT

Portfolium uses various techniques to provide system redundancy, including an available backup environment.

Each AWS service used (EC2, RDS, etc) is configured to be redundant and available in different Availability Zones within the AP-SOUTHEAST-2 region. Each Availability Zone is designed as an independent failure zone. This means that Availability Zones are physically separated within a typical metropolitan region and are located in lower risk flood plains (specific flood zone categorization varies by AWS Region). In addition to discrete uninterruptible power supply (UPS) and onsite backup generation facilities, they are each fed via different grids from independent utilities to further reduce single points of failure. Availability Zones are all redundantly connected to multiple tier-1 transit providers

US-BASED CLIENTS

Portfolium's multi-tenant database is backed up via RDS services and stored in the US-EAST-1 region (primary). Daily database backups are sent to US-WEST-2.

Portfolium's server configuration is scripted using AWS OpsWorks and Chef. In the event of a cataclysmic disaster in US-EAST-1, the system would be able to use the RDS backups in US-WEST-2 and spin up a new stack and update the DNS in CloudFlare to point to the new Load Balancers in US-WEST-2.

AUSTRALIA-BASED CLIENTS

Portfolium's multi-tenant database is backed up via RDS services and stored in the AP-SOUTHEAST-2 region (primary). Daily database backups are sent to AP-SOUTHEAST-1.

Portfolium's server configuration is scripted using AWS OpsWorks and Chef. In the event of a cataclysmic disaster in US-EAST-1, the system would be able to use the RDS backups in AP-SOUTHEAST-1 and spin up a new stack and update the DNS in CloudFlare to point to the new Load Balancers in AP-SOUTHEAST-1.

© 2021 Instructure Inc. All rights reserved.