CANVAS
BY INSTRUCTURE

ARQUITECTURA DO CANVAS LMS

Engenharia, Segurança e Operações

Julho 2023

Table of Contents

CANVAS
BY INSTRUCTURE

Arquitetura do Canvas

Nos últimos anos, não é surpresa que o Software as a Service (SaaS) tenha se tornado a coisa mais importante. Empresas de todo o mundo passaram a entender e ver as enormes vantagens que o SaaS pode trazer para suas organizações, em oposição às soluções tradicionais on-premise. É por isso que o Canvas - o Sistema de Gerenciamento de Aprendizagem líder mundial - nasceu na nuvem. Desde o início, nossos fundadores desenvolveram o Canvas para ser uma solução multi-tenant nativa da nuvem, arquitetada para dimensionar e atender automaticamente milhões de usuários simultâneos em todo o mundo. O Canvas não é apenas entregue como um modelo SaaS conveniente, onde nossos clientes nunca precisam se preocupar com service packs, atualizações, versões, backups e segurança, mas também o desenvolvemos usando padrões e tecnologias abertas que se reúnem em um ambiente integrado e fácil de usar, permitindo que nossos usuários concentrem seu tempo onde mais importa; em sua capacidade de ensinar, aprender e se envolver em uma ampla variedade de ambientes, independentemente do dispositivo, sistema operacional ou local. O documento a seguir descreve a arquitetura do Canvas para aqueles curiosos técnicos que adoram entrar nos detalhes de como fazemos o Canvas fazer sua**.**

Hospedagem

A família de produtos da Instructure, incluindo nosso carro-chefe Canvas LMS, é hospedada na nuvem pela Instructure e fornecida pela Internet por meio do provedor de nuvem pública mais confiável do mundo, Amazon Web Services (AWS). Os blocos de construção básicos da AWS incluem serviços como Elastic Compute Cloud (EC2), Elastic Load Balancing (ELB), Auto Scaling Groups (ASG), Simple Storage Service (S3), Elastic Block Store (EBS), Virtual Private Cloud (VPC), Simple Email Service (SES) e Identity and Access Management (IAM). Também usamos recursos avançados da plataforma AWS, incluindo Amazon Kinesis, AWS Lambda, AWS Fargate, AWS Elastic Kubernetes Service (“EKS”) e Amazon Relational Database Services (“RDS”). Os produtos da Instructure são projetados para fazer uso total da redundância em tempo real e dos recursos de capacidade oferecidos pela AWS, executados em várias zonas de disponibilidade em regiões em todo o mundo. O armazenamento primário é fornecido pelo Amazon S3, projetado para durabilidade superior a 99,99999999%.

Regiões de Hospedagem

Para clientes dos EUA, a Instructure usa duas regiões Amazon Web Services (AWS), garantindo que os dados do cliente não sejam armazenados fora dos Estados Unidos:

- Leste dos EUA (Virgínia do Norte)
- Oeste dos EUA (Oregon)

Para clientes internacionais, a Instructure usa as seguintes regiões da AWS:

- Canadá Central (Montreal)
- Oeste da União Europeia (Irlanda)
- Centro da União Europeia (Alemanha)
- Ásia Pacífico (Sydney)
- Ásia Pacífico (Cingapura)

Em cada região que operamos, utilizamos três (3) Zonas de Disponibilidade (AZ) para redundância.

Segurança do Produto

A Instructure possui as seguintes certificações que são auditadas de forma independente por terceiros:

- SOC 2 Tipo II
- ISO/IEC 27001:2013
- Certificação TX-RAMP Nível 2

O relatório SOC 2 pode ser disponibilizado sob um Acordo Mútuo de Não Divulgação (MNDA). O certificado de conformidade ISO 27001 pode ser disponibilizado a qualquer pessoa mediante solicitação.

Como um dos benefícios da utilização da infraestrutura em nuvem da AWS, também herdamos as seguintes certificações de segurança:

- Relatórios SOC 1 Tipo II (ISAE 3402), SOC 2 Tipo II e SOC 3 Tipo II
- Certificações ISO 9001, 27001 (CSA Star Level 2), 27017 e 27018
- Provedor de serviços PCI-DSS nível 1
- Nível de operação moderado da FISMA
- Pronto para GDPR, compatível com FERPA (modelo de responsabilidade compartilhada)
- Certificação Cyber Essentials PLUS

Separação dos dados de locatários

A separação de locatários é realizada na AWS por meio da separação lógica em software multi-tenant nativo. Os dados do cliente são segregados por meio de fragmentação de banco de dados (particionamento horizontal). O particionamento horizontal é um princípio de design pelo qual as linhas de uma tabela de banco de dados são mantidas separadamente, em vez de dividir por colunas (como para normalização). Cada partição faz parte de um fragmento. A vantagem é que o número de linhas em cada tabela é reduzido, reduzindo o tamanho do índice e melhorando o desempenho.

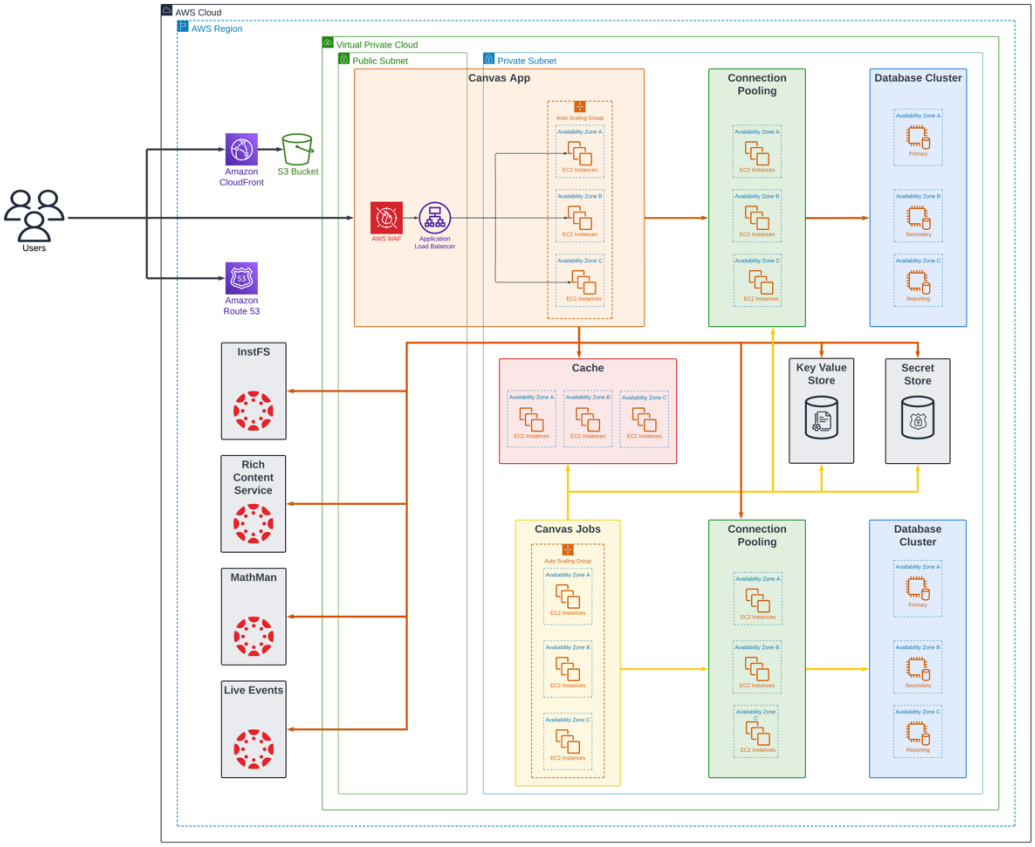
A fragmentação é baseada no aspecto do mundo real dos dados (por exemplo, segmentados por cliente) e os dados não podem vazar de um fragmento para outro, nem os clientes podem obter acesso aos dados em outro fragmento, pois o método de inferir o fragmento do cliente é realizado após a autenticação. Como as credenciais do cliente são válidas apenas para uma única conta e, portanto, o shard, a autenticação do usuário está intrinsecamente ligada à identidade do shard. A validação dos dados segregados do cliente ocorre durante o teste semanal de recuperação de desastres.

Diagrama de Arquitetura

CANVAS BY INSTRUCTURE

Canvas LMS Architecture

Commercial in Confidence
Last Updated June 2023



Escalonamento, Backup, Recovery e Redundância

Os sistemas elétricos e de rede do data center da AWS são projetados para serem totalmente redundantes e de fácil manutenção, sem impacto nas operações, 24 horas por dia, sete dias por semana. Unidades de fonte de alimentação ininterrupta (UPS) estão disponíveis no caso de uma falha elétrica para cargas críticas e essenciais na instalação. Os datacenters usam geradores para fornecer energia de backup para toda a instalação.

A arquitetura do Canvas LMS replica dados quase em tempo real e é feito backup dos dados diariamente. A Instructure cria backups diários externos de banco de dados de dados e conteúdo do Canvas, incluindo conteúdo do curso, envios de alunos, conteúdo criado por alunos, análises, rubricas, resultados de aprendizagem e metadados. Os dados são armazenados de forma redundante em vários data centers e locais geográficos por meio do Amazon S3.

A arquitetura do Canvas LMS é horizontalmente escalável e usa uma combinação de tecnologias desenvolvidas internamente e fornecidas pela AWS, permitindo responder a picos de uso em tempo real e acomodar o uso expandido de longo prazo. Através de escalonamento automático e tecnologia de provisionamento automatizado, o Canvas ajusta os recursos da nuvem para lidar com grandes cargas de uso antes que causem lentidão. Quando o número de usuários simultâneos aumenta, o Canvas adiciona recursos automaticamente para que os usuários não tenham interrupções ou lentidão.

Garantindo a recuperação e redundância da plataforma Canvas LMS, tiramos proveito de vários locais geograficamente separados e zonas de disponibilidade que fornecem resiliência em face da maioria dos modos de falha, incluindo desastres naturais ou falhas do sistema. O aplicativo Canvas foi projetado para fazer uso total da redundância em tempo real e dos recursos de capacidade oferecidos pela AWS, executando em várias zonas de disponibilidade em regiões em todo o mundo. O armazenamento primário é fornecido pelo Amazon S3, projetado para uma durabilidade superior a 99,99999999%.

A arquitetura do Canvas LMS também é resiliente a falhas e capaz de rápida recuperação de falhas de componentes. O aplicativo Canvas, sua mídia e armazenamento de arquivos e seus bancos de dados são redundantes de forma independente. Se um nó de hospedagem de aplicativo falhasse, todo o tráfego seria transferido para nós vivos. Se a carga aumentar, um sistema de provisionamento automatizado garante que mais nós de hospedagem sejam disponibilizados para lidar com o tráfego - seja em resposta ao aumento da carga ou em antecipação preditiva de cargas de trabalho futuras. O

banco de dados e os armazenamentos de arquivos também são horizontalmente escaláveis, adicionando capacidade para armazenamento adicional e carga conforme necessário.

Escalonamento Preditivo

O Canvas LMS é um Software-as-a-Service (SaaS), hospedado pelo provedor de hospedagem em nuvem mais estabelecido e confiável do mundo: Amazon Web Services. Desde o lançamento do Canvas em 2011 como o primeiro LMS nativo da nuvem, a Instructure fornece e suporta exclusivamente a plataforma de tecnologia educacional SaaS totalmente hospedada na nuvem. Durante esse período, analisamos dados e coletamos tendências de uso, o que nos permite prever quando é provável que ocorra um pico de uso para um determinado cliente.

É com esses dados que aproveitamos as tecnologias EC2 Auto Scaling da AWS para levar o dimensionamento a um nível totalmente novo para lidar com ciclos às vezes imprevistos de maior volume. O uso do Predictive Scaling nos permite prever quando é provável que ocorra um pico de uso para um determinado cliente. Ele aprende com padrões passados e lança instâncias antes da demanda prevista, dando às instâncias tempo para se aquecerem e ficarem prontas preventivamente antes que uma situação de alta demanda exista, e não em resposta a uma. Além disso, ele fornece downscaling flexível, garantindo que os recursos do sistema não sejam removidos muito rapidamente quando a carga começar a cair.

Levando isso um passo adiante, também utilizamos a própria tecnologia de dimensionamento da Instructure chamada HotTub. O HotTub é um mecanismo de dimensionamento automático reativo especificamente para o Canvas LMS que pode dimensionar nossos clusters de aplicativos em resposta a saltos inesperados na atividade do usuário até 20 vezes mais rápido do que o próprio serviço de dimensionamento automático da Amazon. Como podemos olhar para dias ou semanas anteriores e prever quais recursos serão necessários com antecedência, nosso dimensionador HotTub pode ter um pool de servidores de aplicativos pré-aquecidos que estão prontos para serem colocados em serviço a qualquer momento. Entre esses dois serviços, o Canvas oferece estabilidade e escalabilidade incomparáveis, independentemente da carga do usuário.

Load Balancers

Os balanceadores de carga do AWS Elastic são implantados em uma configuração ativa / ativa altamente disponível, que lida com as solicitações de entrada e despacha as conexões subjacentes uniformemente para os servidores de aplicativos disponíveis. O balanceador de carga mantém uma lista dinâmica de servidores de aplicativos disponíveis para envio. O balanceador de carga envia pulsações regulares - uma mensagem de rede simples - para verificar se o servidor de aplicativos está íntegro, disponível e capaz de receber trabalho adicional. O balanceador de carga não enviará trabalho para servidores de aplicativos que não respondem. Capacidade adicional é adicionada automaticamente ao conjunto de balanceamento de carga conforme o tráfego e a demanda aumentam.

Servidores de Aplicação

Os servidores de aplicação processam as solicitações de entrada dos balanceadores de carga. Eles são responsáveis por executar a lógica de negócios, renderizar HTML e retornar alguns ativos estáticos para o navegador do usuário do Canvas LMS. Além disso, esses servidores são balanceados em várias zonas de disponibilidade para garantir tolerância máxima a falhas.

Os servidores de aplicativos são constantemente monitorados individualmente para informações de carga e capacidade. Quando todos os servidores de aplicativos atingem um determinado limite de carga, um novo servidor de aplicativos é fornecido e implementado automaticamente. A automação interna da Instructure pode agendar de forma dinâmica e inteligente novos servidores de aplicativos em antecipação a tempos de alta carga, como durante o início e o final dos semestres.

Servidores de Cache

A camada de cache fornece otimização de desempenho. Um cache saudável significa que os servidores de aplicação precisam fazer menos viagens para o banco de dados, o que acelera os tempos de resposta. A camada de cache é composta por várias máquinas que executam o Redis. Os dados são distribuídos uniformemente por todas as máquinas. Além disso, o Amazon Cloudfront (um cache CDN) é usado para entregar rapidamente ativos estáticos aos usuários do Canvas. Esses pontos de extremidade CDN são globalmente distribuídos, tornando o caminho de rede para essas solicitações o mais eficiente possível.

Os servidores de cache são monitorados constantemente. Quando um servidor de cache falha, um novo é provisionado e implantado para substituí-lo. Quando um servidor de cache falha, os dados que seriam armazenados nele são simplesmente recuperados do banco de dados.

Os servidores de cache são totalmente baseados em memória. O uso da memória é monitorado continuamente. Quando as taxas de acerto do cache caem abaixo de um limite aceitável, novos servidores de cache são provisionados e implantados.

Servidores de Banco de Dados

Os dados do curso e do usuário são armazenados em bancos de dados relacionais. Os bancos de dados são particionados por instituição-cliente para fins de desempenho e isolamento de dados. Cada instituição utiliza um par de bancos de dados: um banco de dados primário e um banco de dados secundário em uma zona de disponibilidade separada.

Também há um terceiro servidor de backup em cada região e (se disponível) em uma zona de disponibilidade separada. Todas as alterações do banco de dados são transmitidas em tempo real umas para as outras e para uma camada de dados durável (S3). Isso significa que as informações do banco de dados do Canvas LMS para clientes dos EUA e América Latina são armazenadas em três locais separados geograficamente. Os clientes canadenses se beneficiam de dois locais separados geograficamente. Além disso, backups de banco de dados (uma forma diferente de redundância de dados para diferentes propósitos) são testados semanalmente.

Se o banco de dados primário falhar, o secundário será promovido a primário e um novo banco de dados secundário provisionado e implantado. Em caso de falha do banco de dados secundário, um novo banco de dados secundário é provisionado e implantado. No caso improvável de falha simultânea de componentes ou corrupção de dados, o servidor de backup em espera pode ser usado para criar um novo par de banco de dados.

Os bancos de dados são constantemente monitorados quanto ao uso de recursos e tempo de resposta. Se qualquer um dos bancos de dados se aproximar do pico de carga, os clientes individuais serão realocados em clusters com capacidade disponível.

Armazenamento de Arquivos Distribuídos

A mídia do curso, incluindo vídeos, arquivos de imagem, gravações de áudio, etc. e arquivos carregados por alunos, como tarefas, documentos e artefatos de aprendizagem, são armazenados fora do banco de dados em um depósito Amazon Simple Storage Service (S3) separado e escalonável projetado para durabilidade superior a 99,99999999%. Todos os objetos dentro dos depósitos S3 são criptografados e replicados entre sites separados geograficamente e têm o controle de versão habilitado para que as versões anteriores de um objeto possam ser restauradas com o mínimo de esforço.

Conclusão

Seguindo as melhores práticas, criamos um aplicativo da Web nativo da nuvem, dinâmico e altamente escalável que se tornou o Sistema de Gerenciamento de Aprendizagem mais confiável do mundo e usado por instituições de ensino respeitadas, como todas as oito escolas da Ivy League, Universidade de Oxford , University of Birmingham, KTH Royal Institute of Technology, London Business School, University of Amsterdam e muito mais. Ao tomar muito cuidado e diligência na criação de um aplicativo SaaS de ponta, nossa arquitetura se destaca no setor de tecnologia educacional por sua robustez, proteção, escalabilidade e confiabilidade.