CANVAS
BY INSTRUCTURE

# CATALOG
## ARCHITECTURE OVERVIEW

Engineering, Security, and Operations

November 2022

# Table of Contents



CANVAS
BY INSTRUCTURE

# Canvas Catalog Architecture

Throughout history, we have seen many great pairings and partnerships. Batman and Robin. John and Paul. Peanut Butter and Jelly. At Instructure, we have a few of our own great pairings. One of them, Canvas LMS and Canvas Catalog. As a customizable storefront for your organization's course and program offerings, Canvas Catalog is a cornerstone solution in the Canvas Learning Management Platform. But it's not just a storefront. Catalog lets you go deeper into your listing management—where you can create custom landing pages to promote certain courses, make your offerings easily searchable, and, if applicable, integrate most payment systems for a seamless experience for students, teachers, and administrators alike. The following supplemental document describes the Canvas Catalog architecture for those curious technical types who love getting into the detail of just how we make this beautiful partnership work.

## Hosting Regions

For US customers, Canvas Catalog uses two Amazon Web Services (AWS) regions, ensuring that client data is not stored outside of the United States:

- US East (Northern Virginia)
- US West (Oregon)

For international clients, we use the following AWS regions:

- Canada Central (Montreal)
- EU West (Ireland)
- EU Central (Germany)
- Asia Pacific (Sydney)
- Asia Pacific (Singapore)

In each region we operate, we utilize three (3) Availability Zones (AZ) for redundancy.

## Security Program

Canvas Catalog is included as part of Instructure's robust information security program that runs on a continuous, PDCA-cycle. It was created based on guidance provided by ISO/IEC 27000:2018 and controls described in ISO/IEC 27001:2013, and is managed by Instructure's Chief Information Security

Officer. The security program is attested to by a number of current security certifications including ISO 27001, SOC 2, SOC 3, UK Cyber Essentials Plus, PCI DSS SAQ D and Attestation of Compliance.

Canvas Catalog has a software development lifecycle (SDLC) that incorporates secure coding practices and controls. All code goes through a developer peer-review process before it is merged into the code base repository. The code review includes security auditing based on the Open Web Application Security Project (OWASP) secure coding and code review documents (including the OWASP Top Ten) and other community sources on best security practices.

Instructure's Security Team regularly performs vulnerability scans on Canvas Catalog using a number of internal and external tools and techniques and we publicly publish the results of our annual third-party penetration tests because we believe that being open about all things - security included - enables us to build the best possible product for our customers. The most recent report can be found at https://www.instructure.com/security.

In addition to these measures, the Amazon Web Services infrastructure on which Canvas Catalog is hosted has a variety of formal accreditations. Some of the many certifications include:

DoD SRG • FedRAMP • FIPS • IRAP • ISO 9001 • ISO 27001 • ISO 27017 • ISO 27018 • MLPS Level 3 • MTCS • PCI DSS Level 1 • SEC Rule 17-a-4(f) • SOC 1 • SOC 2 • SOC 3 • UK Cyber Essentials Plus

For additional information about AWS security certifications and standards compliance, please refer to http://aws.amazon.com/security and http://aws.amazon.com/compliance/.

# Product Security

The following is an overview of Canvas Catalog' product security measures:

- All data is encrypted in transit with TLS v1.2.
- All data is stored at rest within AES-256-bit-encrypted volumes.
- The Catalog API (JSON) uses SSL for all requests.
- All environments are deployed into an AWS Virtual Private Cloud (VPC) within secure private networks. NAT Gateways are used to ensure that instances do not have routable IP addresses. Each component is protected by a security group with an appropriate, restrictive rule set. The only device that has access to the public internet is the Elastic Load Balancer (ELB).
- Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
- Minimal PII is captured, and Instructure maintains a Data Protection Policy reviewed annually.
- Instructure is compliant with the EU's national data privacy and protection law, the General Data Protection Regulation (“GDPR”).

# Separation of Tenant Data

Separation of tenants is accomplished in AWS via logical separation in natively multi-tenant software. Customer data is segregated via database sharding (horizontal partitioning). Horizontal partitioning is a design principle whereby rows of a database table are held separately, rather than splitting by columns (as for normalization). Each partition forms part of a shard. The advantage is the number of rows in each table is reduced, reducing index size, and improving performance.

Sharding is based on real-world aspect of the data (e.g., segmented by customer) and data cannot leak from one shard to another, nor can clients gain access to data in another shard as the method of inferring the client shard is accomplished after authentication. As client credentials are only valid for a single account, and therefore shard, user authentication is intrinsically tied to the shard identity. Validation of segregated client data occurs during weekly disaster recovery testing.

# PCI DSS

For payments, Canvas Catalog redirects users to integrated payment gateways set up by the client institution, e.g., Stripe, PayPal, etc. Canvas Catalog is compliant with PCI DSS as demonstrated by Instructure's self-assessment questionnaire (SAQ) form D and the Canvas Catalog PCI Responsibility Matrix. These documents are made available in the Canvas Catalog Supplemental Security Package provided by Instructure.

# Payment Gateways

Canvas Catalog can integrate with specific gateways used to process payments for paid Catalog listings. Multiple payment gateways can also be set up via individual sub-catalogs. The following payment gateways are supported in Canvas Catalog:

- Authorize.net (Accept Hosted)*
- CCP*
- CommWeb
- CyberSource
- Mercado Pago*
- Nelnet
- OneStop Secure*
- PayU
- PayPal*

- PayPal Payflow*
- Stripe
- TouchNet*
- Transact (requires both Checkout and Gateway)

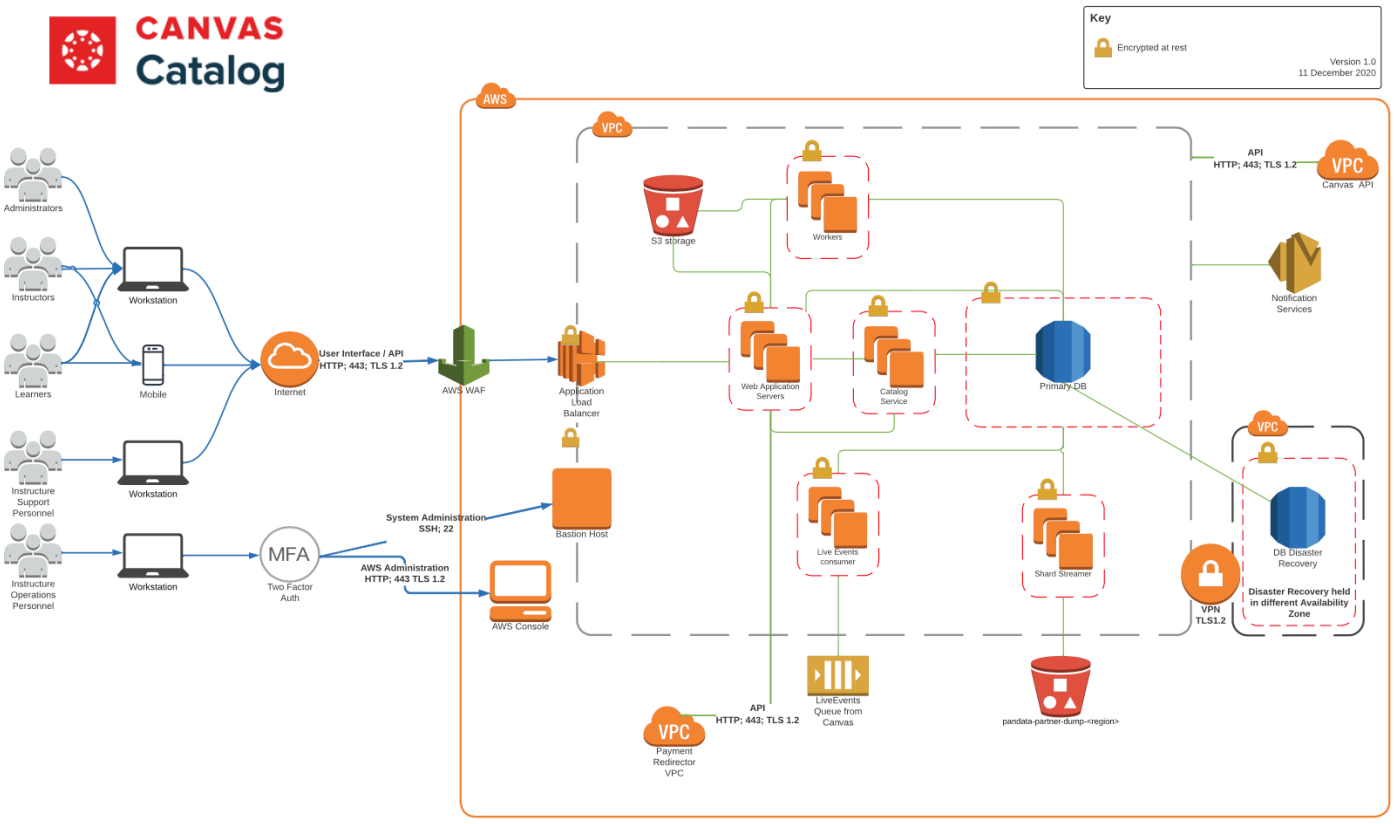
*Purchase receipts are itemized.

# Languages

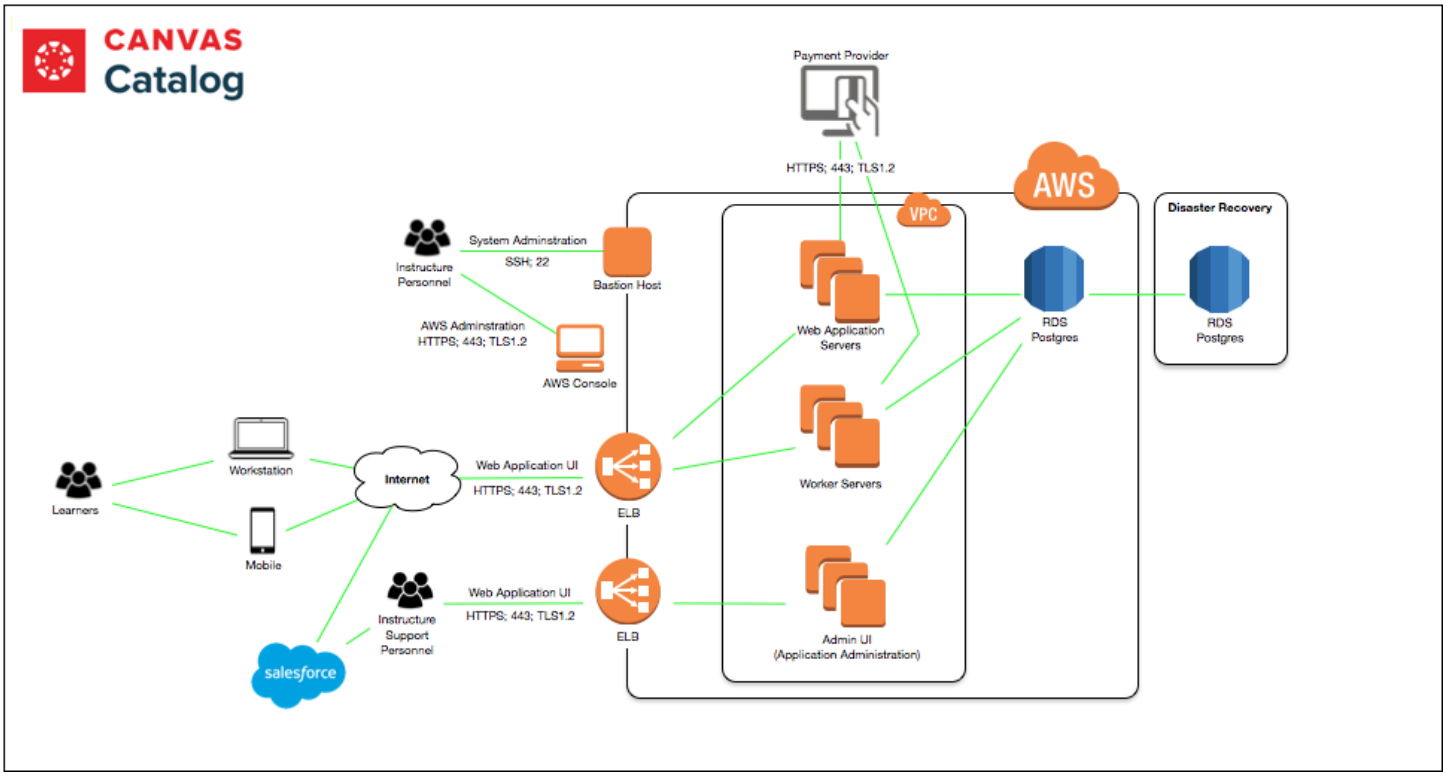
Canvas Catalog is made up of several components, with some variation of programming language:

- The backend application is Ruby on Rails, with a Java service that controls critical workflows such as enrollments and order creation
- The Catalog frontend UI is a modern React.js web application

# Architecture and Data Flow Diagram (AWS)



# Payment Redirector Architecture and Data Flow (AWS)




# API

Canvas Catalog has a RESTful API (JSON) with endpoints covering a wide range of overall functionality. The API is fully documented and can be accessed from within the Catalog Admin dashboard.

# Backups

Canvas Catalog is backed up daily and backups are retained as follows:

- Last 60 daily backups retained
- Last 60 monthly backups retained

# Third-Party Integrations

The Canvas ecosystem, including Canvas Catalog, provides integration points with various third-party tools and services. Most of the services integrated into the core of the Canvas ecosystem are done so as modular plugins which leverage the APIs of the remote system. Additionally, some of the services exposed in Canvas Catalog require opt-in by the end user or remote activation by a third-party service provider upon contract with the Institution (e.g., Payment Gateways).