CANVAS
BY INSTRUCTURE

STUDIO

ARCHITECTURE OVERVIEW

Engineering, Security, and Operations

December 2022

Table of Contents

CANVAS
BY INSTRUCTURE

Canvas Studio Architecture

Early in the development of our flagship product, the Canvas Learning Management System, we saw the writing on the wall - video learning was gaining traction in all sectors of education, mainly because the learners of today were raised with a smart phone in-hand - they're used to and expect high quality digital experiences in all facets of their lives, including in the ways they learn. This is why we built Canvas Studio, a learning video platform that integrates seamlessly with Canvas LMS, allowing dynamic and engaging collaboration between teacher and student, whether in class, remote, or a mix of both. Robust, easy-to-use tools let teachers and designers alike create and deliver interactive learning experiences that hold attention and stand up to distraction, so there's no temptation for learners to sneak over to a TikTok tab and check their feed. Students can even produce and submit their own video creations in Canvas Studio and easily collaborate and comment on each other's work. Everybody stays engaged. And just like that, Canvas Studio took its rightful place alongside Canvas LMS as the next-generation video education platform.

The following supplemental document describes the Canvas Studio architecture for those curious technical types who love getting into the detail of just how we serve up hours and hours of video learning content without a hitch.

Hosting Regions

For US customers, Canvas Studio 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 Studio 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, and UK Cyber Essentials Plus.

Canvas Studio 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 Studio 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 Studio 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 Studio's 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 Studio API is secured by OAuth.
- 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).

- A Web Application Firewall further protects the application from potential exploits, filtering traffic before it even reaches the 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”).

Format Support

Canvas Studio supports modern video formats and codecs, including:

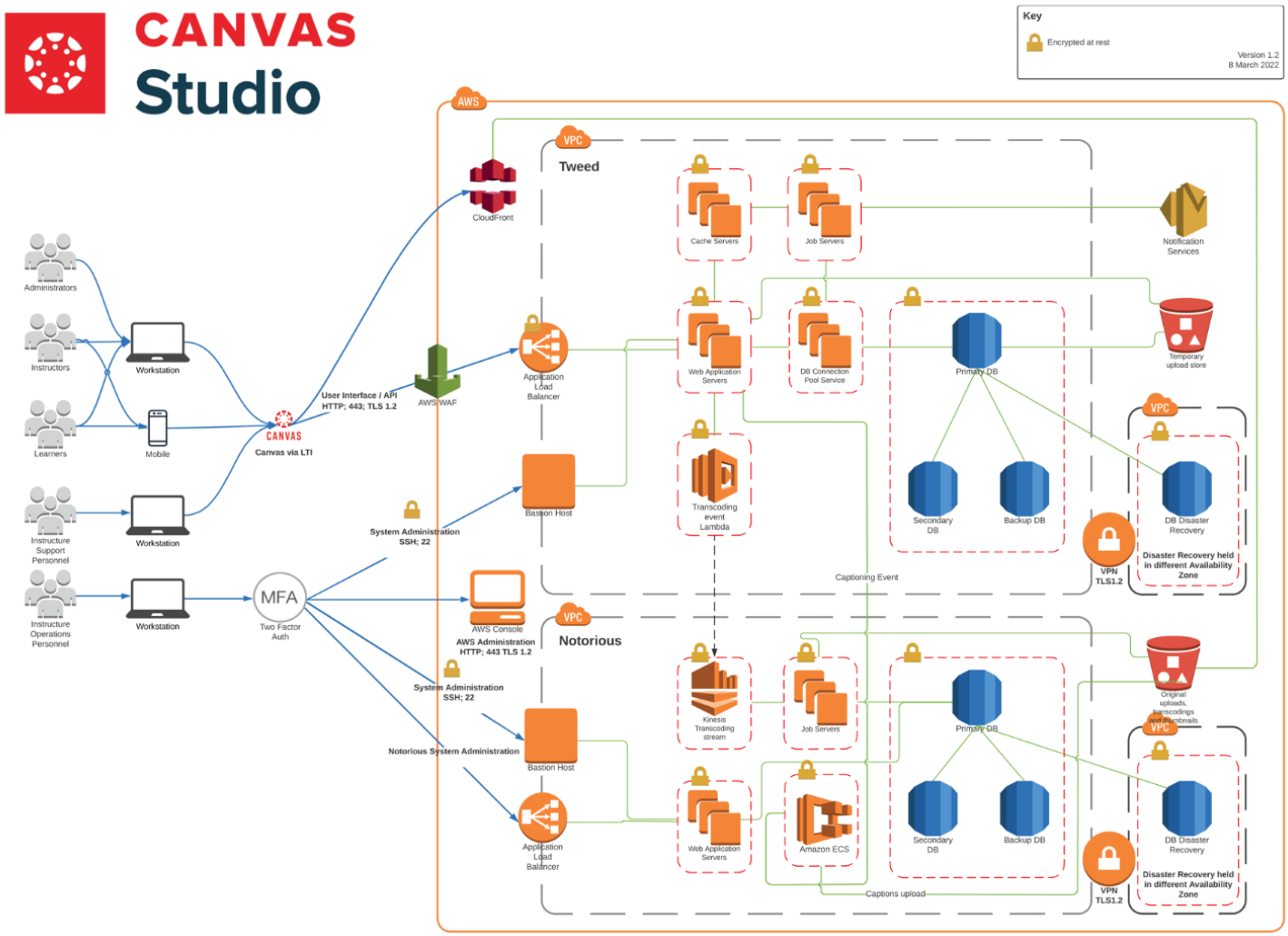
- asf – Windows Media
- qt – Apple QuickTime
- mov – Apple QuickTime
- mpg – Digital Video Format
- mpeg – Digital Video Format
- avi – Digital Video Format
- m4v – Digital Video Format
- wmv – Windows Media
- mp4 – Digital Video Format
- 3gp – Multimedia Mobile Format

Tech Stack / Languages

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

- The backend application is Ruby on Rails, with an additional Ruby application that acts as a separate service to store (AWS S3) and transcode videos.
- The Studio frontend is a React application written in TypeScript and JavaScript.

Architecture and Data Flow Diagram (AWS)



API

Canvas Studio has a public API with endpoints covering a wide range of overall functionality, including data management. The API is fully documented and an included GitHub repository includes example operations.

Learning Tools Interoperability (LTI)

Studio is connected to Canvas via LTI and the LTI integration between Canvas and Studio is rather simple.

Every time a Canvas LMS user opens Studio or a course containing Studio media in Canvas, Canvas will send an LTI launch request to the Studio instance with the details of the action: the course id, ids of the Canvas instance and user-based PII limited to name, email address and avatar of the user.

Based on the data in the request, Studio tries to find the user data in its database (or create it if it's the first request from a user) and then fulfil the request.

Third-Party Integrations

The Canvas ecosystem, including Canvas Studio, 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. Some tools are also used to add functionality to Studio. For example, for screen recording in Canvas Studio we use ScreenCast-O-Matic's Screen Recorder for our users to make recordings of their screens and/or web camera and edit these videos before upload. This can be easily downloaded on first run. Additionally, some of the services exposed in Canvas Studio require opt-in by the end user or remote activation by a third-party service provider upon contract with the Institution (e.g., Zoom Conferencing).

Backup & Restore

Digital-site recovery backups are created daily and encrypted using the AES-GCM 256-bit algorithm and stored on encrypted AWS EBS volumes, within a highly secured location that provides physical and environmental security measures. Instead of providing full or partial backups, customers can extract full or partial data from Studio via our API using the Admin Data Management endpoint(s) which can include media, metadata, and analytics. In the event of a system level outage or data loss, Instructure's operations teams will restore the system and data. If the client deletes/removes data we recommend engaging our support team which will escalate internally for us to investigate whether restoration is possible.

Compliance

ISO compliance

Instructure has invested in a robust quality management and security program that's founded on the guidance provided by the International organization for Standardisation's (ISO) 27000 suite of standards and we hold ISO 27001:2013 certification, of which, Canvas Studio is included in scope.

SOC 2

Canvas Studio has been audited in accordance with SSAE 18, and a SOC 2 Type II report is available for review upon execution of a non-disclosure agreement. A copy of the SOC 3 report is provided in the Canvas Studio Security Package.

Accessibility

Instructure is committed to ensuring its products are inclusive and meet the diverse accessibility needs of our users. Canvas Studio strives for WCAG 2.1 Level A/AA and Section 508 conformance. Regular testing (both internal and by a third party) is conducted to identify conformance issues, with processes in place for timely remediation of accessibility issues that are identified.

Canvas Studio has been evaluated by Instructure and WebAIM according to WCAG 2.1 standards. Testing is regularly conducted using automated tools, assistive technology (such as screen readers, keyboard testing, etc.), and coding best practices. Third party accessibility evaluation occurs regularly with internal audits conducted with each release. Mechanisms are in place for logging and fixing accessibility defects.

The Canvas Studio VPAT is available at: https://www.instructure.com/accessibility/canvas/canvas-studio-vpat

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) in Studio is minimal and comes from Canvas LMS. The only PII captured during use from a user is the user's full name, display name and email address, as well as the Canvas LMS instance's LMS id (UUID) and the LTI id (lti_lms_id), identifying the user in Canvas.

Conclusion

As with all our products, Canvas Studio is developed and delivered using a robust information security program that runs on a continuous, PDCA-cycle. For more information, including access to the Canvas Studio SOC 2 report, please contact your Customer Success Manager, or info@instructure.com. The SOC 3 report and ISO 27001 Certificate for Canvas Studio is included in the Canvas Studio Security Package.