CANVAS
BY INSTRUCTURE

CREDENTIALS
ARCHITECTURE OVERVIEW

Engineering, Security, and Operations

September 2023

Table of Contents

Introduction 3
- Overview 3

Architecture 4
- Hosting 4
- Hosting Regions 4
- Languages 5
- Tech Stack 5
- Open Standards 5
- Product Security 5
- System Requirements 6
- Uptime SLA 6
- Architecture Diagram 8
- Accessibility 9
- Database Servers 9
- Distributed File Storage 10
- Data Centers 10

Disaster Recovery & Business Continuity 11
- Overview 11

Privacy 12
- Overview 12
- Sub-processors 12
- GDPR 12
- FERPA 13
- COPPA 14
- Data Protection Officer 14
- Termination of Service 14

Conclusion 15

CANVAS
BY INSTRUCTURE

Introduction

Overview

A lot has been written about the skills gap—the gap between the skills graduates bring to an employer and the skills they actually need to perform a job well. In today's tech-driven world, this has led to the need for graduates to prove skills at a higher level of granularity than a diploma or degree can indicate, which in turn has pushed institutions to seek innovative new ways to support students who want greater agency to demonstrate skills and achievements to potential employers.

Coupled with the pandemic turbocharging the need to prepare students for post-graduate careers, it's no surprise that the top priority of both institutions and students alike is being able to offer and obtain definable skills that match a course title or a degree.

Enter, Canvas Credentials. By using badges and Pathways to help students develop and demonstrate essential skills, students can gain verifiable, skill-aligned micro-credentials which are fast becoming the currency between those learning outcomes and employment opportunities. At Instructure, we know firsthand these stackable credentials can help to keep students motivated and rewarded on the way to their degrees.

Even K-12 institutions are embracing the power of digital badging, which at its heart is a student-centered strategy. Most students are familiar with the concept of earning badges from activities outside of school, from scouting to video games to martial arts. Using badges in K-12 supports the growing emphasis on a competency-based approach in elementary and secondary education. This is yet another way Instructure elevates student success and inspires everyone to learn together.

The following document provides insight into Canvas Credentials' architecture for those inquiring - and technical - minds among our customers and community.

Architecture

Hosting

Canvas Credentials (including Canvas Badges) services are hosted by Amazon Web Services (AWS), and services are based in countries and regions where our customers' data originates from (as required by data laws and regulations).

Canvas Credentials uses AWS' cloud infrastructure for all its computing resources for processing and storage. The AWS services currently in use are: ELB, CloudWatch, VPC, DynamoDB, EC2, ECR, ECS, RDS, S3, SQS, and IAM. Amazon acts as a full IaaS provider for Instructure and all hardware management is completely reserved to AWS facilities, including housing of machines, networking of machines, and virtualization of hardware to customers. The AWS infrastructure is designed and managed in accordance with security compliance standards and industry best practices including SOC 1, SOC 2 security and availability compliance, ISO 27001 compliance, and PCI-DSS compliance. For additional information about AWS security certifications and standards compliance, please refer to http://aws.amazon.com/security and http://aws.amazon.com/compliance

Canvas Credentials utilizes multiple AWS regions to segregate operational environments for security and stability. For example, within our US regions, we create fault tolerance through manually duplicated and maintained instances that operate on standby. Different zones are used for the different stages of the development lifecycle, one for development, one for user acceptance testing, and one for production.

Hosting Regions

For Canvas Credentials customers, Instructure uses Amazon Web Services (AWS) regions, ensuring that client data is not stored outside of a customer's region*. The current regions in use for Credentials are:

- US: Oregon and Virginia (us-west-2 / us-east-1)
- Canada: Canada Central (ca-central-1)
- EMEA: Ireland (eu-west-1)
- APAC: Sydney (ap-southeast-2)
- LATAM: Oregon and Virginia (us-west-2 / us-east-1)

*LATAM Canvas Credentials customers are hosted in US region.

Languages

Canvas Credentials (including Badges) is made up of several components, with some variation of programming language:

- The backend application (server) serving the UI is written in Kotlin (JVM family), using the Spring framework.
- The Credentials frontend UI is a modern Angular framework application written in TypeScript.
- Using the Django framework in Python, the server application is the source of truth for Open Badges verification, and the original API.
- Other languages and DSLs/notable tool configuration frameworks include Flask, Ansible, Scala, Dockerfiles and Bash.

Tech Stack

Canvas Credentials is a mixture of technologies, most notable of which are AWS ECS, AWS Fargate, AWS Lambda, AWS Aurora Serverless (MySQL), AWS Elasticache (Redis), Docker, and MongoDB Atlas.

Open Standards

Canvas Credentials uses the open standard, Open Badges. Open Badges is a free, open specification which enables a type of digital badge that is verifiable, portable, and packed with information about skills and achievements. Open Badges can be issued, earned, and managed by using a certified Open Badges platform, such as Canvas Credentials.

Open Badges include information on the organization or individual who issued the badge; the criteria that the badge has been assessed against, evidence, when the badge was issued, a verifiable reference to the recipient and a number of other required an optional properties. Some badges contain links to detailed evidence, expiration dates, searchable tags, and alignments to educational standards or frameworks.

Product Security

The following is an overview of Canvas Credentials' 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 Credentials API uses OAuth2 for most operations.

- 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 fully compliant with the EU's national data privacy and protection law, the General Data Protection Regulation (“GDPR”).

System Requirements

For best performance, Canvas Credentials should be used on the current or first previous major release of Chrome, Firefox, Edge, or Safari. Because it's built using web standards, Credentials runs on Windows, Mac, Linux, iOS, Android, or any other device with a modern web browser.

Credentials only requires an operating system that can run the latest compatible web browsers. Your computer operating system should be kept up to date with the latest recommended security updates and upgrades.

Supported Browsers

Credentials supports the current and first previous major releases of the following browsers:

- Chrome

- Firefox (*Extended Releases are not supported)

- Edge

- Safari

Uptime SLA

Instructure will use commercially reasonable efforts to ensure that the Canvas Credentials, and Canvas Badges platforms maintain a Monthly Uptime Percentage (MUP) of at least 99.9% as observed by an External Monitoring Service (EMS).

Scope

This Service Commitment applies to Unplanned Outages only. Any outage that occurs during that services' scheduled maintenance period will not be calculated as part of the MUP. During these agreed upon periods, monitoring will be disabled so as to not skew the data.

Definitions

- Monthly Uptime Percentage (MUP): is calculated by subtracting from 100% the percentage of minutes during the month that your site was Unreachable.
- External Monitoring Service (EMS): is provided by Pingdom. More information can be found here: https://www.pingdom.com/product/uptime-monitoring
- Unreachable: is defined as the service not returning a 200 OK response when its homepage / base URL is requested.
- Unplanned Outage: is defined as any outage that is not pre-agreed upon by Instructure and the Customer.

Monthly Uptime Percentage

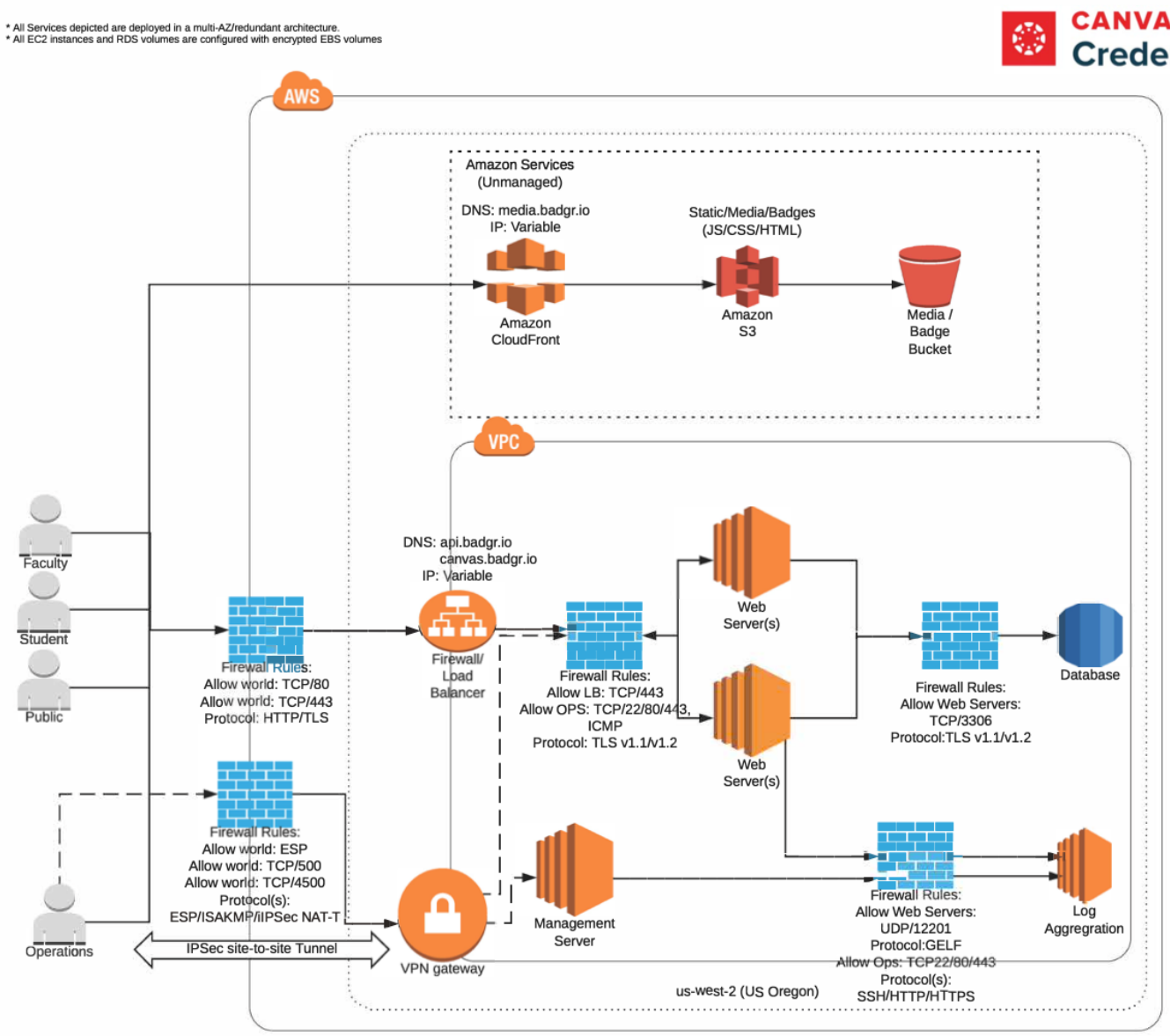
A MUP of 99.9% defines the following periods of potential downtime/unavailability:

- **Daily:** 1m 26s
- **Weekly:** 10m 4s
- **Monthly:** 43m 49s
- **Quarterly:** 2h 11m 29s
- **Yearly:** 8h 45m 56s

Status

Uptime and status for Canvas Credentials (formerly Badgr) can be viewed at: https://status.badgr.com/

Architecture Diagram



Accessibility

Canvas Credentials is tested for conformance with a target of the AA level of the WCAG 2.0 accessibility standards. As part of the Credentials development process, new and changed interfaces are evaluated for continued compliance with the WCAG. We employ accessibility experts to go above and beyond the written guidelines to ensure we keep advancing the product toward an enjoyable experience for people with a range of accessibility needs, including those using assistive technologies.

Accessibility Statement

Canvas Credentials has been built using code compliant with W3C standards for HTML and CSS. To help us make using badges a good experience for everyone, we strive to conform to Level AA of the World Wide Web Consortium (W3C) Web Content Accessibility Guidelines (WCAG) 2.1. These guidelines explain how to make web content more accessible for people with disabilities, and user-friendly for everyone.

As a browser-based web application, Canvas Credentials fully supports:

- Standard browser magnification and contrast adjustments.
- Browser spellcheck.
- Standard keyboard navigation and input functions (such as the Tab key to move between input fields, the arrow keys to move between list items, and the Space or Enter keys to make selections).
- Standard HTML and WAI-ARIA techniques for providing text equivalents of non-text elements.
- Contrast requirements of 4.5:1 and no use of italics, continuous capitals or underlining.

For more details, see the Credentials (formerly Badgr) VPAT (Based on VPAT version 2.4) August 2021, included with the Canvas Credentials Security Package.

Database Servers

Canvas Credentials uses both MongoDB and MySQL. MongoDB Atlas is the datastore provider where the production database clusters reside. In the unlikely event of simultaneous component failure or data corruption, backup snapshots can be used to restore to a newly created cluster. Databases are only available to Layer 2 adjacent RFC1918 addresses. They do not have public access outside of the VPC.

Distributed File Storage

Badges, media, image files, etc. are stored outside the Credentials database in a separate and scalable Amazon Simple Storage Service (S3) bucket that is designed for durability exceeding 99.99999999%. All objects within the S3 buckets are encrypted and replicated between geographically separate sites and have version control enabled so previous versions of an object can be restored with minimal effort.

Data Centers

AWS data center electrical and network systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, seven days a week. Uninterruptible Power Supply (UPS) units are available in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Instructure creates daily database backups of data and content including badges and media. Data is stored redundantly in multiple data centers and multiple geographic locations through Amazon S3. *For further detail on backups, please see Instructure's Business Continuity & Disaster Recovery Paper.*

Through automatic scaling and automated provisioning technology, Canvas Credentials adjusts cloud resources to handle large usage loads before they cause slowdowns. When concurrent user numbers grow, the platform automatically adds resources, so users don't experience outages or slowdown.

Assuring the recovery and redundancy of the Credentials platform, we take advantage of multiple geographically separate sites and Availability Zones which provide resilience in the face of most failure modes including natural disasters or system failures. The application is designed to make full use of the real-time redundancy and capacity capabilities offered by AWS, running across multiple availability zones in regions throughout the world. Primary storage is provided by Amazon S3, which is designed for durability exceeding 99.99999999%.

The architecture is also resilient to failure and capable of rapid recovery from component failure. The application, its media and file storage, and its databases are each independently redundant. If an application hosting node were to fail, all traffic would transfer to living nodes. If load increases, an automated provisioning system ensures that more hosting nodes are made available to handle the traffic—either in response to increased load or in predictive anticipation of future workloads. The database and file stores are also horizontally scalable, adding capacity for both additional storage and load as needed.

Disaster Recovery & Business Continuity

Overview

Canvas Credentials databases and media (badges) are backed up automatically daily, with replication to another AWS region. The databases are backed up with Point in Time (PIT) snapshots with a 5-minute granularity. Recovery capability is tested quarterly.

All data stored on Canvas Credentials file servers, email servers, network servers, web servers, database servers, domain controllers, firewalls and remote access servers are stored in offsite backups, rotated using a Grandfather-father-son methodology where we always have the last 24 hours, last 7 days, and last (1) month for the previous 13 months.

The following backup retention rules apply to pertinent Canvas Credentials information:

- Daily incremental backups are saved for one week.
- Weekly backups are stored for the previous 4 weeks.
- Monthly backups are stored for the previous 13 months.
- Full backups are saved for 13 months.

For more detail on Instructure's approach to Disaster Recovery, please see our *Business Continuity & Disaster Recovery Paper* which covers DR topics such as Incident Management, Recovery Objectives, and Communication. This is available at: https://www.instructure.com/products/canvas/security

Privacy

Overview

Instructure diligently protects users' privacy and Canvas Credentials collects only low risk personal data, limited to first name, last name, email address and badges. It protects the transmission of PII using a combination of SSL certificates and TLS. Any data gathered by Canvas Credentials is in relation to a user's interaction with the different tools and functionality. This data is sent to the customer-designated server and stored for the purposes of fulfilling the contractual obligations. Upon request, all data about a specific user will be permanently deleted. There will be no subsequent collection of data pertaining to that specific user for any other purposes. If requested, Instructure will provide all data collected about a specific user. Requests about deletion of data and requests about data gathered about a specific user can be sent to privacy@instructure.com. Requests about deleting data will be handled within 48 hours from when the request is made to Instructure. Requests about data collected about a specific user will be handled within 48 hours from when the request is made. The data will only be processed to fulfill a customer contract. No other processing of the data will take place without the written instruction of the controller. No data will, at any time, without the prior written permission of the data controller, be transferred to any third party. The data will only be processed by Instructure employees that have signed a confidentiality agreement, and only for the purposes of fulfilling the contractual obligations.

Sub-processors

Canvas Credentials use customer designated servers for storing and processing data. The data in rest and data in transit are encrypted and no personnel at the hosting providers site have access to the data. Canvas Credentials will not use any other sub-processor without the written consent of the data controller. The current list of sub-processors that Canvas Credentials utilizes can be located at Annex 3 of our Badgr Data processing Addendum, https://www.instructure.com/badgr-data-processing-addendum-instructure-policy

GDPR

Instructure has complied with the GDPR since the enforcement date (25 May 2018).

To ensure ongoing compliance with the GDPR, Instructure does the following:

- Educates the organization about GDPR and its requirements.

- Has conducted a GDPR gap analysis with the help of a reputable outside law firm experienced with GDPR, and has closed those gaps.
- Maintains an up-to-date listing of personal data Instructure holds, where it came from, and who Instructure may share it with.
- Maintains current privacy notices that comply with the GDPR.
- Ensures existing procedures cover all the rights individuals have under GDPR.
- Identifies our lawful basis for processing personal data, documenting it, and updating our privacy notice to explain it to individuals.
- Reviews how Instructure obtains, records, and manages consent.
- Reviews and updates contracts with third parties to ensure our privacy obligations are up to date.
- Ensures the right procedures are in place to detect, report, and investigate a personal data breach.
- Maintains processes for Data Protection Impact Assessments.
- Has appointed a Data Protection Officer.

FERPA

Family Educational Rights and Privacy Act (FERPA) restricts the student data that educational institutions may share with web services and the public. Instructure complies with FERPA as a school official. Minimal personal data about students is shared with Canvas Credentials when educational institutions award badges to those students. Make sure your use of Canvas Credentials is consistent with the information permitted by your FERPA directory information disclosure categories to be shared with our services and to be published in awarded badges. Typically, institutions ensure student email addresses and academic awards or honors are permitted to be shared. When you use Canvas Credentials to award badges, either manually or automatically through the LTI tool(s), ensure that the data stored in badges is consistent with your institutional policy. This may mean bypassing the evidence features to include data that doesn't fall under directory information disclosures, such as grades or graded work.

COPPA

Canvas Credentials is not currently compliant with the Children's Online Privacy Protection Act (COPPA) and we restrict usage of Canvas Credentials to children 13 years and older. Our Credentials product team is working on updating the product for compliance with an ETA of Q4 2023.

Data Protection Officer

Canvas Credentials has an appointed a Data Protection Officer, in accordance with GDPR Article 39. The Data Protection Officer is responsible for the following tasks;

- Inform and advise the customer and employees of their obligations pursuant to the GDPR regulations
- Monitor the compliance with the GDPR regulations including assignment of responsibilities, awareness-raising, and training of staff.
- Provide advice when requested.
- Cooperate with the customers with regards to GDPR questions or issues.
- Act as a point of contact for the customer.

Any questions with regards to the GDPR or other privacy matters can be sent to privacy@instructure.com.

Termination of Service

Upon termination of the Canvas Credentials service, we can return or delete customer data. Note, however, that revocation of issued Badges will result in the Badges becoming unverifiable which is contrary to the intended purpose of the Open Badge Specification. Issued Badges and their associated metadata will remain viewable online until such time as the Badge Recipient requests deletion of the Badge or the issuer of the Badge affirmatively deletes the Badge.

Conclusion

Canvas Credentials empowers learners through their personal educational journey – whether they be traditional, non-traditional, career shifters and a little bit of everything in-between. Canvas Credentials empowers Higher Ed, K-12, Associations, Workforce Development, Technical Training and Corporate companies to combine and connect badges from multiple sources into a meaningful pathway for learners. To motivate and engage students with visual, stackable, and shareable pathways while empowering them to carry their skills throughout their educational journey. Utilizing EMSI data, Canvas Credentials connects students to real world applications of their skills and progress to visualize career outlook and salary expectations.