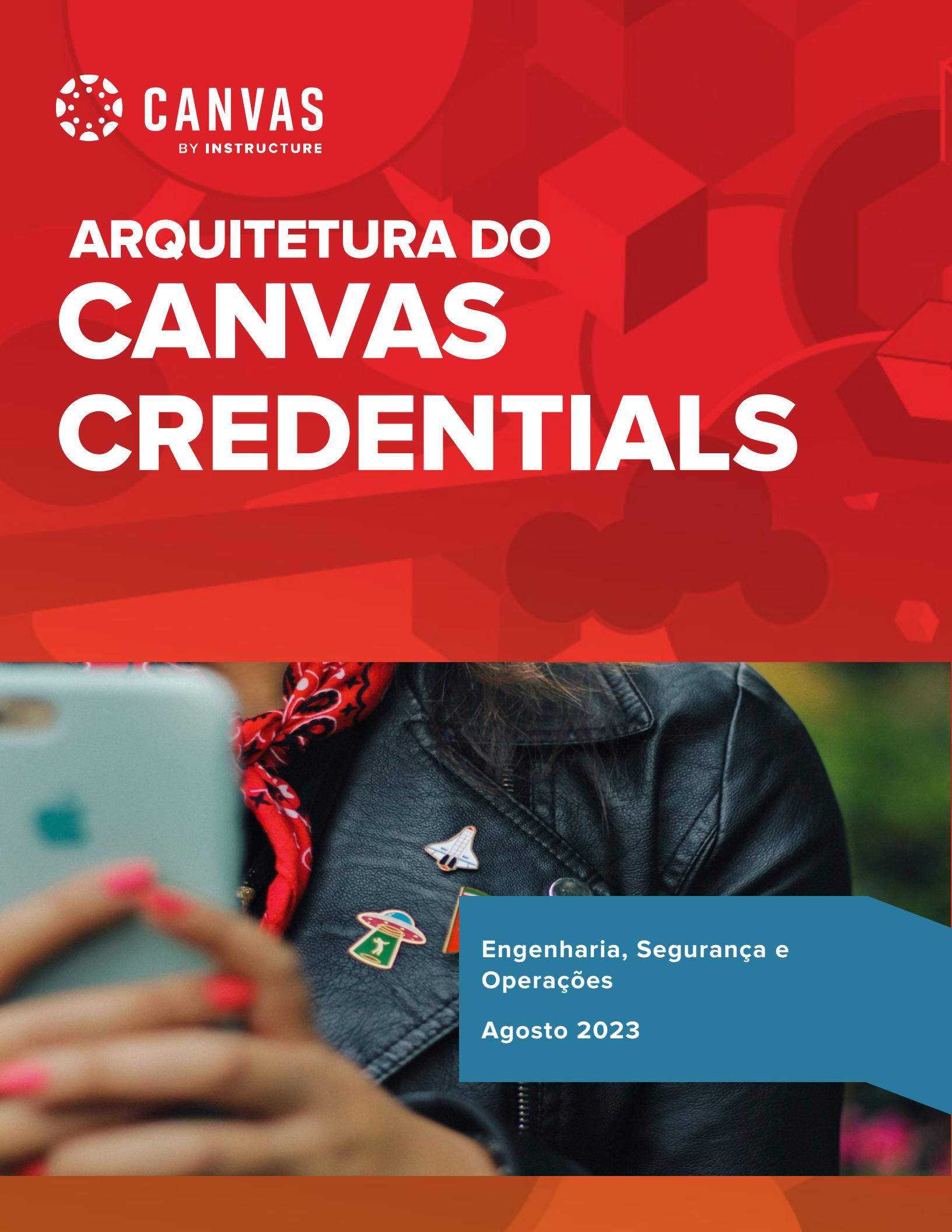




ARQUITETURA DO CANVAS CREDENTIALS



Engenharia, Segurança e
Operações

Agosto 2023

Índice

Introdução	3
Arquitetura	4
Continuidade Dos Negócios E Recuperação De Desastres.....	11
Privacidade	12
Conclusão	15



Introdução

Overview

Muito já foi escrito sobre o gap entre as habilidades que os graduados trazem para um empregador e as habilidades que eles realmente precisam para desempenhar bem um trabalho. No mundo tecnológico de hoje, isso levou à necessidade de os graduados provarem habilidades em um nível mais alto de granularidade do que um diploma ou que um diploma pode indicar, o que, por sua vez, levou as instituições a buscar novas maneiras inovadoras de apoiar os alunos que desejam uma maneira melhor para demonstrar habilidades e realizações para potenciais empregadores.

Juntamente com a pandemia que impulsiona a necessidade de preparar os alunos para carreiras de pós-graduação, não é surpresa que a principal prioridade de ambas as instituições e alunos seja poder oferecer e obter habilidades definíveis que correspondam a um título de curso ou diploma.

Com isso, temos o Canvas Credentials. Ao usar badges e Pathways para ajudar os alunos a desenvolver e demonstrar habilidades essenciais, os alunos podem obter microcredenciais verificáveis e alinhadas às habilidades que estão rapidamente se tornando a moeda entre esses resultados de aprendizado e oportunidades de emprego. Na Instructure, sabemos em primeira mão que essas credenciais empilháveis podem ajudar a manter os alunos motivados e recompensados no caminho para seus diplomas.

Até mesmo as instituições de ensino fundamental e médio estão adotando o poder do selo digital, que em sua essência é uma estratégia centrada no aluno. A maioria dos alunos está familiarizada com o conceito de ganhar distintivos de atividades fora da escola, de escotismo a videogames e artes marciais. O uso de badges no K-12 apoia a crescente ênfase em uma abordagem baseada em competência no ensino fundamental e médio. Essa é mais uma maneira pela qual a Instructure eleva o sucesso dos alunos e inspira todos a aprenderem juntos.

O documento a seguir fornece informações sobre a arquitetura do {{canvas}} Credentials para as mentes questionadoras - e técnicas - entre nossos clientes e comunidade.



Arquitetura

Hospedagem

Os serviços Canvas Credentials (incluindo Canvas Badges)] são hospedados pela Amazon Web Services (AWS), e os serviços são baseados em países e regiões de onde os dados de nossos clientes são originários (conforme exigido por leis e regulamentos de dados).

O Canvas Credentials usa a infraestrutura de nuvem da AWS para todos os seus recursos de computação para processamento e armazenamento. Os serviços da AWS atualmente em uso são: ELB, CloudWatch, VPC, DynamoDB, EC2, ECR, ECS, RDS, S3, SQS e IAM. A Amazon atua como um provedor IaaS completo para a Instructure e todo o gerenciamento de hardware é totalmente reservado às instalações da AWS, incluindo alojamento de máquinas, rede de máquinas e virtualização de hardware para clientes. A infraestrutura da AWS é projetada e gerenciada de acordo com os padrões de conformidade de segurança e as melhores práticas do setor, incluindo conformidade de segurança e disponibilidade SOC 1, SOC 2, conformidade com ISO 27001 e conformidade com PCI-DSS. Para obter informações adicionais sobre as certificações de segurança da AWS e a conformidade com os padrões, consulte <http://aws.amazon.com/security> e <http://aws.amazon.com/compliance>.

O Canvas Credentials utiliza várias regiões da AWS para segregar ambientes operacionais para segurança e estabilidade. Por exemplo, em nossas regiões dos EUA, criamos tolerância a falhas por meio de instâncias duplicadas e mantidas manualmente que operam em espera. Diferentes zonas são usadas para os diferentes estágios do ciclo de vida de desenvolvimento, uma para desenvolvimento, uma para teste de aceitação do usuário e outra para produção.

Regiões de Hospedagem

Para clientes do Canvas Credentials, a Instructure usa regiões da Amazon Web Services (AWS), garantindo que os dados do cliente não sejam armazenados fora da região do cliente. As regiões atuais em uso para o Credentials são:

- EUA e LATAM: Oregon e Virgínia (us-west-2 / us-east-1)
- Canadá: Canadá Central (ca-central-1)
- EMEA: Irlanda (eu-west-1)
- APAC: Sydney (ap-southeast-2)

Linguagens de Programação

O Canvas Credentials (incluindo Badges) é composto por vários componentes, com algumas variações de linguagem de programação:

- O aplicativo de backend (servidor) que atende a UI é escrito em Kotlin (família JVM), usando o framework Spring.
- A interface do usuário front-end Credentials é um aplicativo de estrutura Angular moderno escrito em TypeScript.
- Usando o framework Django em Python, o aplicativo do servidor é a fonte de verdade para verificação de Open Badges e a API original.
- Outras linguagens e DSLs/estruturas de configuração de ferramentas notáveis incluem Flask, Ansible, Scala, Dockerfiles e Bash.

Padrões Abertos

O Canvas Credentials usa o padrão aberto, Open Badges. O Open Badges é uma especificação aberta e gratuita que permite um tipo de badge digital verificável, portátil e repleto de informações sobre habilidades e conquistas. Os Open Badges podem ser emitidos, conquistados e gerenciados usando uma plataforma certificada de Open Badges, como o Canvas Credentials.

Open Badges incluem informações sobre a organização ou indivíduo que emitiu o badge; os critérios pelos quais o badge foi avaliado, evidências, quando o badge foi emitido, uma referência verificável ao destinatário e uma série de outras propriedades opcionais exigidas. Alguns selos contêm links para evidências detalhadas, datas de validade, tags pesquisáveis e alinhamentos com padrões ou estruturas educacionais.

Segurança de Produto

A seguir está uma visão geral das medidas de segurança do produto Canvas Credentials:

- Todos os dados são criptografados em trânsito com TLS v1.2
- Todos os dados são armazenados em repouso em volumes criptografados por AES-256 bits.
- A API do Credentials usa OAuth2 para a maioria das operações.
- Todos os ambientes são implantados em uma Nuvem Privada Virtual (VPC) da AWS em redes privadas seguras. Gateways NAT são usados para garantir que as instâncias não tenham endereços IP roteáveis. Cada componente é protegido por um grupo de segurança com um conjunto de regras restritivo apropriado. O único dispositivo que tem acesso à Internet pública é o Elastic Load Balancer (ELB).



- As verificações de vulnerabilidades baseadas em host são realizadas pelo menos trimestralmente em todos os sistemas externos. Vulnerabilidades críticas e altas são rastreadas até a correção.
- Dados Privados mínimos são capturados e a Instructure mantém uma Política de Proteção de Dados revisada anualmente.
- A Instructure está em conformidade com a lei nacional de privacidade e proteção de dados da UE, o Regulamento Geral de Proteção de Dados (“GDPR”).

Requisitos de Sistema

Para melhor desempenho, o Canvas Credentials deve ser usado na versão principal atual ou na primeira versão anterior do Chrome, Firefox, Edge ou Safari. Por ser desenvolvido usando padrões da Web, o Credentials é executado em Windows, Mac, Linux, iOS, Android ou qualquer outro dispositivo com um navegador da Web moderno.

O Canvas Credentials requer apenas um sistema operacional que possa executar os navegadores da Web compatíveis mais recentes. O sistema operacional do seu computador deve ser mantido atualizado com as últimas atualizações e atualizações de segurança recomendadas.

Navegadores compatíveis

Credentials é compatível com as versões principais atuais e anteriores dos seguintes navegadores:

- Chrome
- Firefox (*Versões estendidas não são compatíveis)
- Edge
- Safari

SLA Tempo de Atividade

A Instructure fará esforços comercialmente razoáveis para garantir que as plataformas Canvas Credentials e Canvas Badges mantenham uma Porcentagem de Tempo de Atividade Mensal de pelo menos 99.9% conforme observado por um Serviço de Monitoramento Externo.

Escopo

Este Compromisso de Serviço se aplica apenas a Interrupções Não Planejadas. Qualquer interrupção que ocorra durante o período de manutenção programada desses serviços não será calculada como parte do tempo de atividade mensal. Durante esses períodos acordados, o monitoramento será desabilitado para não distorcer os dados.



Definições

- Porcentagem de tempo de atividade mensal (MUP): é calculada subtraindo de 100% a porcentagem de minutos durante o mês em que seu site estava inacessível.
- Serviço de Monitoramento Externo (EMS): é fornecido pela Pingdom. Mais informações podem ser encontradas aqui: <https://www.pingdom.com/product/uptime-monitoring>
- Inacessível: é definido como o serviço que não retorna uma resposta 200 OK quando sua página inicial / URL base é solicitada.
- Interrupção Não Planejada: é definida como qualquer interrupção que não seja pré-acordada pela Instructure e pelo Cliente.

Porcentagem de tempo de atividade mensal

Um MUP de 99.9% define os seguintes períodos de tempo de inatividade/indisponibilidade potencial:

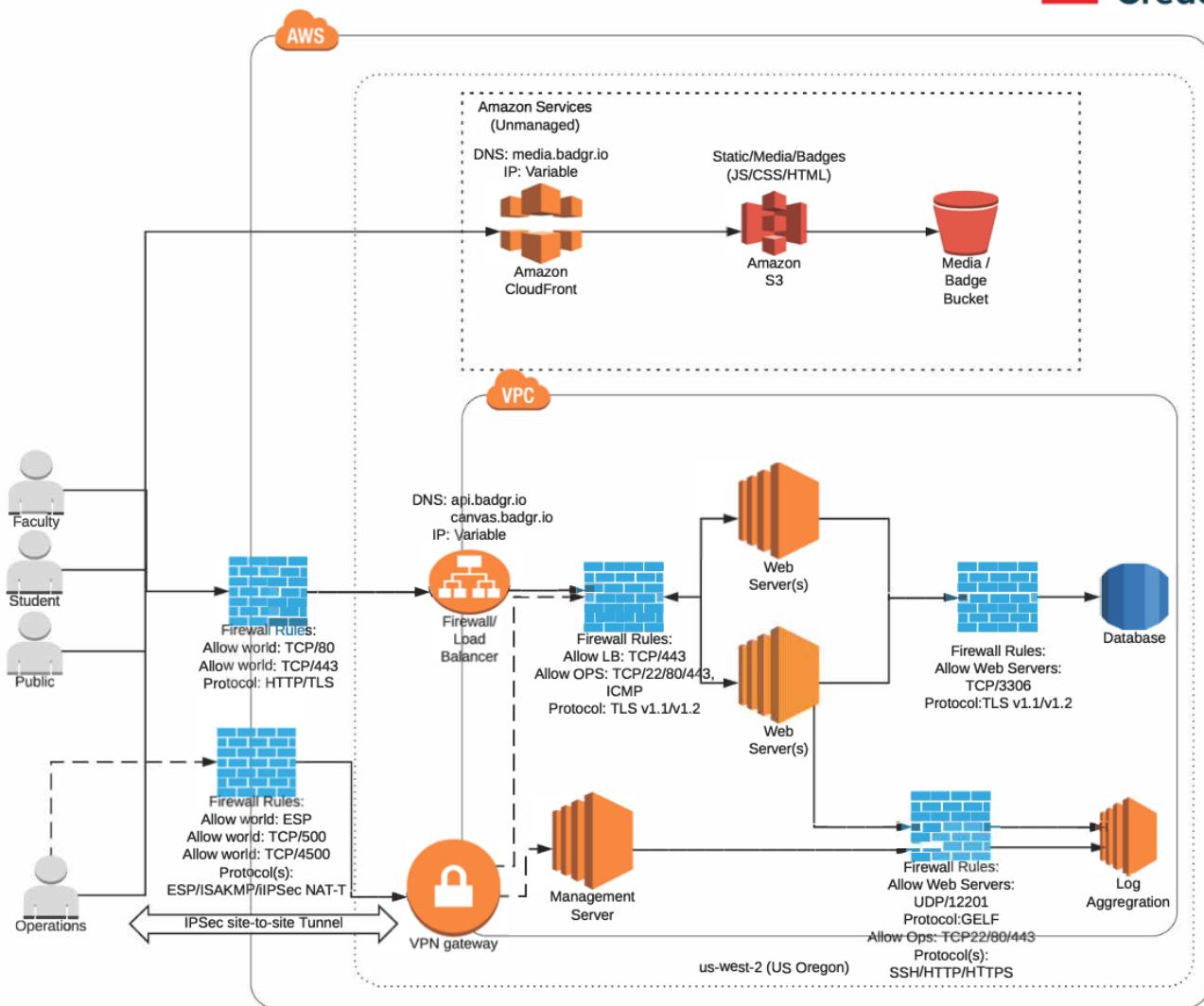
- **Diariamente:** 1m 26s
- **Semanal:** 10m 4s
- **Mensal:** 43m 49s
- **Trimestral:** 2h 11m 29s
- **Anual:** 8h 45m 56s

Status

O tempo de atividade e o status do Canvas Credentials (anteriormente Badgr) podem ser visualizados em: <https://status.badgr.com/>

Diagrama de Arquitetura

* All Services depicted are deployed in a multi-AZ/redundant architecture.
 * All EC2 instances and RDS volumes are configured with encrypted EBS volumes



Acessibilidade

O Canvas Credentials é testado quanto à conformidade com uma meta do nível AA dos padrões de acessibilidade WCAG 2.0. Como parte do processo de desenvolvimento para o Credentials, interfaces novas e alteradas são avaliadas para conformidade contínua com as regras WCAG. Empregamos especialistas em acessibilidade para ir além das diretrizes escritas para garantir que continuemos avançando o produto em direção a uma experiência agradável para pessoas com uma variedade de necessidades de acessibilidade, incluindo aquelas que usam tecnologias assistivas.

Declaração de Acessibilidade

O Canvas Credentials foi construído usando código compatível com os padrões W3C para HTML e CSS. Para nos ajudar a tornar o uso do Credentials uma boa experiência para todos, nos esforçamos para estar em conformidade com o Nível AA do World Wide Web Consortium (W3C) [Web Content Accessibility Guidelines \(WCAG\) 2.1](#). Essas diretrizes explicam como tornar o conteúdo da Web mais acessível para pessoas com deficiência e fácil de usar para todos.

Como um aplicativo da web baseado em navegador, o Canvas Credentials suporta totalmente:

- Ampliação e ajustes de contraste padrão do navegador
- Verificação ortográfica do navegador
- Navegação do teclado padrão e funções de entrada (como a tecla Tab para mover entre os campos de entrada, as teclas de seta para mover entre os itens da lista e as teclas Espaço ou Enter para fazer seleções).
- Técnicas padrão de HTML e WAI-ARIA para fornecer equivalentes em texto de elementos não textuais.
- Requisitos de contraste de 4,5:1 e sem uso de itálico, maiúsculas contínuas ou sublinhado.

Para obter mais detalhes, consulte o VPAT do Credentials (anteriormente Badgr) (com base no VPAT versão 2.4) de agosto de 2021, incluído no Pacote de segurança do Canvas Credentials.

Servidores de Banco de Dados

O Canvas Credentials usa MongoDB e MySQL. O MongoDB Atlas é o provedor de armazenamento de dados onde residem os clusters de banco de dados de produção. No caso improvável de falha simultânea de componentes ou corrupção de dados, os instantâneos de backup podem ser usados para restaurar para um cluster recém-criado. Os bancos de dados estão disponíveis apenas para endereços RFC1918 adjacentes da camada 2. Eles não têm acesso público fora da VPC.

Armazenamento de Arquivos Distribuídos

Badges, mídia, arquivos de imagem etc. são armazenados fora do banco de dados do Credentials em um bucket separado e escalável do Amazon Simple Storage Service (S3) projetado para durabilidade superior a 99,99999999%. Todos os objetos nos buckets do S3 são criptografados e replicados entre sites geograficamente separados e têm o controle de versão ativado para que as versões anteriores de um objeto possam ser restauradas com o mínimo de esforço.

Data Centers

Os sistemas elétricos e de rede do data center da AWS são projetados para serem totalmente redundantes e passíveis de manutenção sem impacto nas operações, 24 horas por dia, sete dias por semana. Unidades de fonte de alimentação ininterrupta (UPS) estão disponíveis em caso de falha elétrica para cargas críticas e essenciais na instalação. Os data centers usam geradores para fornecer energia de backup para toda a instalação.

O Instructure cria backups diários de dados e conteúdo do banco de dados, incluindo crachás e mídia. Os dados são armazenados de forma redundante em vários data centers e várias localizações geográficas por meio do Amazon S3. *Para mais detalhes sobre backups, consulte o Documento de Continuidade de Negócios e Recuperação de Desastres da Instructure.*

Por meio de dimensionamento automático e tecnologia de provisionamento automatizado, o Canvas Credentials ajusta os recursos da nuvem para lidar com grandes cargas de uso antes que causem lentidão. Quando o número de usuários simultâneos aumenta, a plataforma adiciona recursos automaticamente para que os usuários não sofram interrupções ou lentidão.

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

A arquitetura também é resiliente a falhas e capaz de recuperação rápida de falhas de componentes. O aplicativo, sua mídia e armazenamento de arquivos e seus bancos de dados são cada um independentemente redundantes. Se um nó de hospedagem de aplicativo falhar, todo o tráfego será 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 de futuras cargas de trabalho. O banco de dados e os armazenamentos de arquivos também são escaláveis horizontalmente, adicionando capacidade para armazenamento adicional e carga conforme necessário.

Continuidade Dos Negócios E Recuperação De Desastres

Overview

O backup dos bancos de dados e mídia (badges) do Canvas Credentials é feito automaticamente diariamente, com replicação para outra região da AWS. O backup dos bancos de dados é feito com instantâneos Point in Time (PIT) com granularidade de 5 minutos. A capacidade de recuperação é testada trimestralmente.

Todos os dados armazenados em servidores de arquivos do Canvas Credentials, servidores de e-mail, servidores de rede, servidores web, servidores de banco de dados, controladores de domínio, firewalls e servidores de acesso remoto são armazenados em backups externos, alternados usando uma metodologia Avô-pai-filho onde sempre temos o último 24 horas, últimos 7 dias e último (1) mês para os 13 meses anteriores.

As seguintes regras de retenção de backup se aplicam às informações pertinentes do Canvas Credentials:

- Os backups incrementais diárias são salvos por uma semana.
- Os backups semanais são armazenados para as 4 semanas anteriores.
- Os backups mensais são armazenados para os 13 meses anteriores.
- Os backups completos são salvos por 13 meses.

Para obter mais detalhes sobre a abordagem da Instructure para Recuperação de Desastres, consulte nosso Documento de Continuidade de Negócios e Recuperação de Desastres, que abrange tópicos de DR, como Gerenciamento de Incidentes, Objetivos de Recuperação e Comunicação. Disponível em: <https://www.instructure.com/pt-br/canvas/seguranca>



Privacidade

Overview

A Instructure protege diligentemente a privacidade dos usuários e o Canvas Credentials coleta apenas dados pessoais de baixo risco, limitados a nome, sobrenome, endereço de e-mail e badges. Ele protege a transmissão de PII usando uma combinação de certificados SSL e TLS. Quaisquer dados coletados pelo Canvas Credentials estão relacionados à interação de um usuário com as diferentes ferramentas e funcionalidades. Esses dados são enviados para o servidor designado pelo cliente e armazenados para fins de cumprimento das obrigações contratuais. Mediante solicitação, todos os dados sobre um usuário específico serão excluídos permanentemente. Não haverá coleta subsequente de dados pertencentes a esse usuário específico para quaisquer outros fins. Se solicitado, a Instructure fornecerá todos os dados coletados sobre um usuário específico. Solicitações sobre exclusão de dados e solicitações sobre dados coletados sobre um usuário específico podem ser enviadas para privacy@instructure.com. As solicitações sobre a exclusão de dados serão tratadas dentro de 48 horas a partir do momento em que a solicitação for feita à Instructure. Solicitações sobre dados coletados sobre um usuário específico serão tratadas dentro de 48 horas a partir do momento em que a solicitação for feita. Os dados serão processados apenas para cumprir um contrato de cliente. Nenhum outro processamento dos dados ocorrerá sem a instrução escrita do controlador. Nenhum dado será, a qualquer momento, sem a permissão prévia por escrito do controlador de dados, ser transferido para terceiros. Os dados serão tratados apenas por colaboradores da Instructure que tenham assinado um acordo de confidencialidade, e apenas para efeitos de cumprimento das obrigações contratuais.

Subprocessadores

O Canvas Credentials usa servidores designados pelo cliente para armazenar e processar dados. Os dados em repouso e os dados em trânsito são criptografados e nenhum pessoal no site do provedor de hospedagem tem acesso aos dados. O Canvas Credentials não usará nenhum outro subprocessador sem o consentimento por escrito do controlador de dados. A lista atual de subprocessadores que o O Canvas Credentials utiliza pode ser localizada no Anexo 3 do nosso Adendo de processamento de dados Badgr, <https://www.instructure.com/badgr-data-processing-addendum-instructure-policy>.



GDPR

A Instructure está em conformidade com o GDPR desde a data de aplicação (25 de maio de 2018).

Para garantir a conformidade contínua com o GDPR, a Instructure faz o seguinte:

- Educa a organização sobre o GDPR e seus requisitos.
- Conduziu uma análise de lacunas do GDPR com a ajuda de um escritório de advocacia externo respeitável com experiência em GDPR e fechou essas lacunas.
- Mantém uma lista atualizada dos dados pessoais que a Instructure detém, de onde veio e com quem a Instructure pode compartilhá-los.
- Mantém os avisos de privacidade atuais que estão em conformidade com o GDPR.
- Garante que os procedimentos existentes cubram todos os direitos que os indivíduos têm sob o GDPR.
- Identifica nossa base legal para processar dados pessoais, documentá-los e atualizar nosso aviso de privacidade para explicá-los aos indivíduos.
- Analisa como o Instructure obtém, registra e gerencia o consentimento.
- Revisa e atualiza contratos com terceiros para garantir que nossas obrigações de privacidade estejam atualizadas.
- Garante que os procedimentos corretos estejam em vigor para detectar, relatar e investigar uma violação de dados pessoais.
- Mantém processos para Avaliações de Impacto de Proteção de Dados.
- Nomeou um Encarregado de Proteção de Dados.

LGPD

A Instructure está em conformidade com a Lei Geral de Proteção de Dados brasileira. A Lei Geral de Proteção de Dados (13.709/2018) tem como principal objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O objetivo desta Política de Proteção de Dados Pessoais adotada pela Instructure é descrever a conformidade da Instructure com o processamento de Dados Pessoais de acordo com a Lei Geral de Proteção de Dados do Brasil.

Essa Política se aplica a Instructure Inc. e suas subsidiárias integrais (coletivamente "Instructure") que processam Dados Pessoais (definidos no documento sobre LGPD a Instructure).



FERPA

A Lei de Privacidade e Direitos Educacionais da Família (FERPA) restringe os dados do aluno que as instituições educacionais podem compartilhar com os serviços da web e o público. Dados pessoais mínimos sobre os alunos são compartilhados com o Canvas Credentials quando as instituições educacionais concedem crachás a esses alunos. Certifique-se de que o uso do Canvas Credentials é consistente com as informações permitidas pelas categorias de divulgação de informações do seu diretório FERPA a serem compartilhadas com nossos serviços e a serem publicadas em crachás premiados. Normalmente, as instituições garantem que os endereços de e-mail dos alunos e prêmios ou honrarias acadêmicas possam ser compartilhados. Ao usar o Canvas Credentials para conceder badges, manualmente ou automaticamente por meio da(s) ferramenta(s) LTI, certifique-se de que os dados armazenados nos badges sejam consistentes com sua política institucional. Isso pode significar ignorar os recursos de evidência para incluir dados que não se enquadram nas divulgações de informações do diretório, como notas ou trabalho avaliado.

Diretor de Proteção de Dados

O Canvas Credentials nomeou um Diretor de Proteção de Dados, de acordo com o artigo 39 do GDPR. O Diretor de Proteção de Dados é responsável pelas seguintes tarefas;

- Informar e aconselhar o cliente e os funcionários sobre suas obrigações de acordo com os regulamentos do GDPR
- Monitorar a conformidade com os regulamentos do GDPR, incluindo atribuição de responsabilidades, conscientização e treinamento de funcionários.
- Dar conselhos quando solicitado.
- Cooperar com os clientes em relação a questões ou problemas do GDPR.
- Atuar como ponto de contato para o cliente.

Quaisquer dúvidas sobre o GDPR ou outras questões de privacidade podem ser enviadas para privacy@instructure.com.



Conclusão

Conclusão

O Canvas Credentials capacita os alunos por meio de sua jornada educacional pessoal – sejam eles tradicionais, não tradicionais, que mudam de carreira e um pouco de tudo entre eles. O Canvas Credentials capacita empresas de ensino superior, K-12, associações, desenvolvimento de força de trabalho, treinamento técnico e empresas corporativas a combinar e conectar crachás de várias fontes em um caminho significativo para os alunos. Motivar e envolver os alunos com caminhos visuais, empilháveis e compartilháveis, ao mesmo tempo em que os capacita a levar suas habilidades ao longo de sua jornada educacional. Utilizando dados EMSI, o Canvas Credentials conecta os alunos a aplicações do mundo real de suas habilidades e progresso para visualizar perspectivas de carreira e expectativas salariais.





© 2023 Instructure Inc. All rights reserved.