

# Design Solution Review - Eduquation

## Prepared by:

Leonardo Bonato Bizaro  
Pedro de Souza Silva  
Ariel Pereira dos Santos  
EC8

---

## Introdução

Nos dias de hoje, a tecnologia tem sido cada vez mais utilizada em diversas áreas, inclusive no ambiente acadêmico. O uso de recursos computacionais em pesquisas, análises e outras atividades acadêmicas é fundamental, mas nem sempre é fácil ou acessível para todos os estudantes e pesquisadores. A conexão remota de recursos computacionais via cloud tem se mostrado uma solução promissora para esses desafios, permitindo que usuários acessem recursos poderosos e especializados de qualquer lugar, a qualquer hora, sem a necessidade de hardware ou software caros e complexos. Neste contexto, este projeto tem como objetivo trazer facilidade e acessibilidade a ambientes acadêmicos, através da conexão remota de recursos computacionais via AWS Cloud. Com isso, espera-se democratizar o acesso a recursos computacionais avançados e permitir que mais estudantes e pesquisadores possam realizar suas atividades com eficiência e qualidade.

## Problema e Oportunidade

A conexão remota de recursos computacionais via cloud apresenta diversas oportunidades e desafios para o ambiente acadêmico. Por um lado, essa tecnologia pode trazer uma série de benefícios, como o acesso a recursos poderosos e especializados que não estariam disponíveis de outra forma, a possibilidade de trabalhar de qualquer lugar, e a economia de recursos financeiros e de tempo. Por outro lado, o uso dessa tecnologia também pode apresentar desafios, como a necessidade de infraestrutura de rede adequada para suportar conexões remotas, a preocupação com a segurança dos dados e sistemas, e a curva de aprendizado para usuários que não estão familiarizados com essa tecnologia.

Entretanto, com a implementação adequada e a adoção consciente por parte das instituições acadêmicas, a conexão remota de recursos computacionais via cloud pode trazer grandes oportunidades para o ambiente acadêmico, facilitando o trabalho de estudantes e pesquisadores e impulsionando o avanço da ciência e tecnologia.

### OPORTUNIDADE DE NEGÓCIO

Atualmente, a maior parte das instituições acadêmicas do país realizam o aporte de máquinas computacionais através do aluguel de computadores, com quantidade conforme número de alunos esperado e processamento de acordo com o necessário para utilização de softwares que serão úteis nos cursos acadêmicos disponibilizados. Dessa forma, os alugueis das máquinas duram um período determinado de tempo e quando solicitados, limitam a capacidade de recursos que podem ser utilizados conforme o escopo das especificações daquela CPU.

Afim de resolver a limitação da restrição de recursos computacionais e trazer como vantagem a capacidade de estudantes e pesquisadores utilizarem componentes básicos de infraestrutura para acessar sistemas que ampliam as possibilidades de pesquisa e colaboração no ambiente acadêmico, foram propostas as seguintes soluções.

### CASOS DE USO

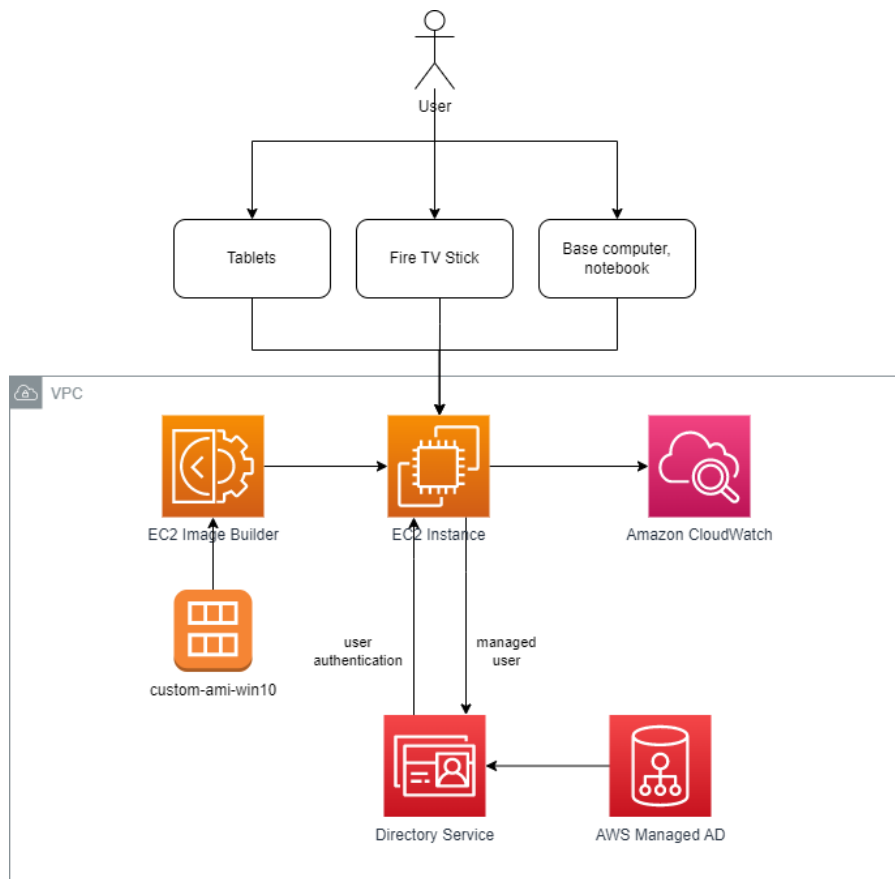
1. **Escolas e Faculdades:** possibilidade de compartilhamento de recursos, onde vários usuários podem ter acesso a um mesmo ambiente de trabalho, facilitando a colaboração em projetos acadêmicos. Com a adoção dessa tecnologia, é

possível que estudantes e pesquisadores tenham acesso a recursos de alta capacidade sem precisar investir em infraestrutura própria, ampliando as possibilidades de pesquisa e colaboração no ambiente acadêmico.

2. **Centros de Pesquisa:** a conexão remota de recursos via cloud permite a realização de experimentos em ambientes virtualizados, permitindo que estudantes e pesquisadores testem diferentes cenários em ambientes seguros e controlados, permitindo o processamento de grandes volumes de dados em áreas como a inteligência artificial e aprendizado de máquina, com recursos de alta capacidade de processamento, como servidores com GPUs especializadas.
3. **Pequenas empresas e startups:** o escopo deste projeto permite que seja avaliado, para empresas de pequeno porte em número de funcionários, a capacidade de disponibilizar aos colaboradores a realização do trabalho remotamente (home-office) ou num modelo híbrido caso preferível. É possível estabelecer uma relação de confiança entre o domínio AD gerenciado da AWS e o domínio local utilizado pela empresa, gerenciando facilmente os usuários já existentes e sua capacidade de acesso ao novo ambiente disponibilizado na nuvem.

## Soluções Propostas

### SOLUÇÃO A



Instâncias gerenciadas através do Amazon EC2, que seriam criadas diretamente com conexão ativa ao AD gerenciado da AWS, este por sua vez responsável pelo gerenciamento de todos os usuários que serão criados para aquela instituição. As instâncias seriam criadas a partir de imagens customizadas de Windows 10, criadas via pipeline do EC2 Image Builder, contendo os softwares e ferramentas básicas para realização de determinados cursos.

## Vantagens:

- Maior influência do usuário na criação de instâncias, pois ao ser realizado diretamente via EC2, permitem a utilização de todo o escopo do serviço no que diz respeito ao gerenciamento de instâncias por parte do próprio cliente, tomando maiores responsabilidades.
- Utilização do EC2 Image Builder garante a capacidade de possuir pipelines de imagens customizadas, acelerando a facilidade com que mudanças de sistema operacional, atualizações e adições de novos softwares sejam refletidos em máquinas a serem utilizadas pelos cursos da instituição.
- Instâncias de EC2 possuem uma forma mais complexa de controle de tráfego, totalmente customizável dentro da VPC aplicada, garantindo maior segurança dentro da infraestrutura da instituição.

## Desvantagens:

- A capacidade do cliente exercer maior influência na criação de instâncias pelo Amazon EC2 não necessariamente se aplica como algo vantajoso dependendo do ponto de vista à quem a solução se destina. Neste caso, tendo em consideração as instituições acadêmicas como cliente final, o ideal seria uma solução que trouxesse a menor responsabilidade possível ao cliente no que diz respeito ao gerenciamento de instâncias.
- Instâncias de EC2 não possuem a forma mais otimizada de garantia de acesso, já que devem ser controladas pela VPC e recursos de permissão de tráfego, como Security Groups.
- Custos: o uso de instâncias EC2 e AD gerenciado da AWS pode ser caro, especialmente se não houver um planejamento cuidadoso dos recursos necessários e da capacidade de armazenamento.
- Complexidade: configurar e gerenciar uma infraestrutura AWS pode ser complexo e exigir conhecimentos específicos em cloud computing, o que pode levar a erros e problemas de segurança se não for feito corretamente.
- Necessidade de parar a execução das instâncias manualmente para economizar custos quando as mesmas não estiverem sendo utilizadas, ou utilizar outro serviço como Amazon EventBridge para programar pausa/início das instâncias utilizando Scheduler.

## CUSTOS

Observação: os cálculos de custos a seguir foram baseados na região de São Paulo - Brasil (sa-east-1).

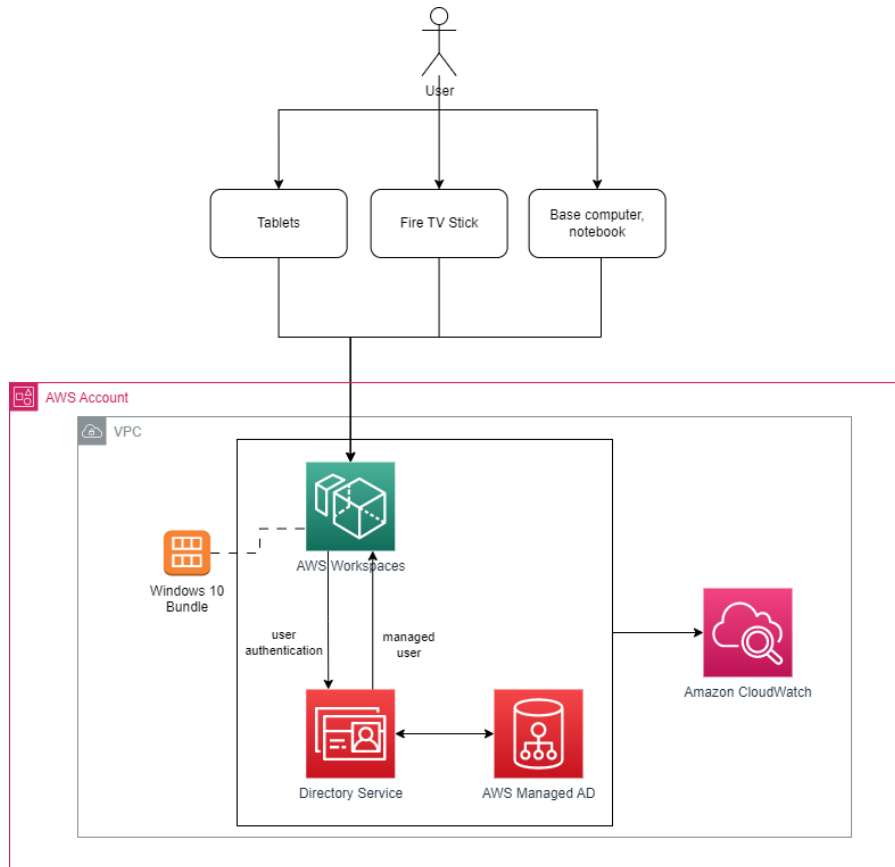
Utilizando como base uma faculdade que possui 1440 alunos, é possível atingir os seguintes cálculos:

- Directory Service AWS Managed Microsoft AD - Standard Edition ~USD 86.40/mês, incluindo dois controladores de domínio para alta disponibilidade com 30 dias de free-trial.
- Amazon CloudWatch - Métricas padrões das instâncias não recorrem a custos adicionais; os Logs gerados e armazenados possuem valor de 0,90 USD por GB para Coleta, e 0,0408 USD por GB para Armazenamento. Neste caso, para utilizar o Armazenamento de Logs será necessário realizar configurações adicionais nas instâncias.
- Instâncias de EC2 - Considerando instâncias On-Demand com pagamento mensal, e operando 24h/dia:

	Power	Storage Volume SSD gp3(EBS)	Monthly Pricing EBS	Instance Pricing
1	t3.small - 2 vCPU, 2 GB memory	80 GB	\$9.70	\$0.052/hour
2	t3a.medium - 2 vCPU, 4 GB memory	130 GB	\$19.70	\$0.0789/hour
3	t3.large - 2 vCPU, 8 GB memory	170 GB	\$20.70	\$0.16/hour

Com o valor de execução da instância e o valor mensal de armazenamento do volume EBS, totaliza-se 77\$/mês por instância. O custo total de instâncias destinadas para todos os alunos da instituição, utilizando a base de 1440 alunos, daria em torno de \$104.555. Para reduzir o tempo diário que uma instância está em execução, afim de reduzir custos e mantê-la ativa apenas durante horários pertinentes de acesso ao aluno, é necessário implementar um recurso que gerencie automaticamente o tempo de atividade de instâncias EC2, como o Amazon EventBridge Scheduler.

## SOLUÇÃO B



Instâncias gerenciadas através do AWS Workspaces, que seriam criadas diretamente com conexão ativa ao AD gerenciado da AWS, este por sua vez responsável pelo gerenciamento de todos os usuários que serão criados para aquela instituição. As instâncias seriam criadas a partir de imagens de Windows 10 padronizadas em Bundles do Workspaces, e teriam agendamento de iniciar e pausar instâncias através do EventBridge Scheduler.

### Vantagens:

- Instâncias criadas através do Workspaces descartam a necessidade de gerenciar servidores por parte do cliente no que diz respeito à criação de instâncias e gerenciamento de networking.
- AutoStop no WorkSpaces, iniciando automaticamente quando o usuário loga, e então permanece ativo por um número determinado de horas até a instância ser pausada automaticamente. AutoStop também cria uma snapshot do desktop no volume raiz do WorkSpaces quando possível.
- Gerenciamento de usuários e instâncias do AD gerenciado é realizado de forma automática durante a configuração do Workspaces, evitando a necessidade de realizar configurações mais complexas no acesso ao domínio.

## Desvantagens:

- O uso do Workspaces pode ser mais caro do que outras opções de instâncias EC2, principalmente se houver muitos usuários ou se forem necessárias instâncias com maior capacidade de processamento e armazenamento.
- Embora seja possível personalizar as imagens do Windows 10 usadas para criar as instâncias do Workspaces, essa personalização pode ser limitada em comparação com o uso de instâncias EC2 personalizadas.
- Embora a utilização do AD gerenciado da AWS possa simplificar o gerenciamento de usuários e permissões, a criação e gerenciamento das instâncias do Workspaces pode ser mais complexa em comparação com outras opções de instâncias EC2.

## CUSTOS

Observação: os cálculos de custos a seguir foram baseados na região de São Paulo - Brasil (sa-east-1).

Utilizando como base uma faculdade que possui 1440 alunos, é possível atingir os seguintes cálculos:

- Directory Service AWS Managed Microsoft AD - Standard Edition ~USD 86.40/mês, incluindo dois controladores de domínio para alta disponibilidade com 30 dias de free-trial.
- Amazon CloudWatch - Métricas padrões das instâncias não recorrem a custos adicionais; os Logs gerados e armazenados possuem valor de 0,90 USD por GB para Coleta, e 0,0408 USD por GB para Armazenamento. Neste caso, para utilizar o Armazenamento de Logs será necessário realizar configurações adicionais nas instâncias.
- Workspaces - Standard with Windows 10 e preços baseados em poder de CPU e processamento:

	Power	Root Volume	User Volume	Monthly Pricing	Hourly Pricing
1	2 vCPU, 4 GB memory	80 GB	10 GB	\$51	\$10.00/month + \$0.50/hour
2	2 vCPU, 4 GB memory	80 GB	50 GB	\$56	\$14.00/month + \$0.50/hour
3	2 vCPU, 4 GB memory	80 GB	100 GB	\$62	\$21.00/month + \$0.50/hour
4	2 vCPU, 4 GB memory	175 GB	100 GB	\$74	\$31.00/month + \$0.50/hour

Com AutoStop configurado para 4h/dia de execução durante segunda à sexta, totaliza-se, em média, 54\$/mês por instância. O custo total de instâncias destinadas para todos os alunos da instituição daria em torno de \$77.760.

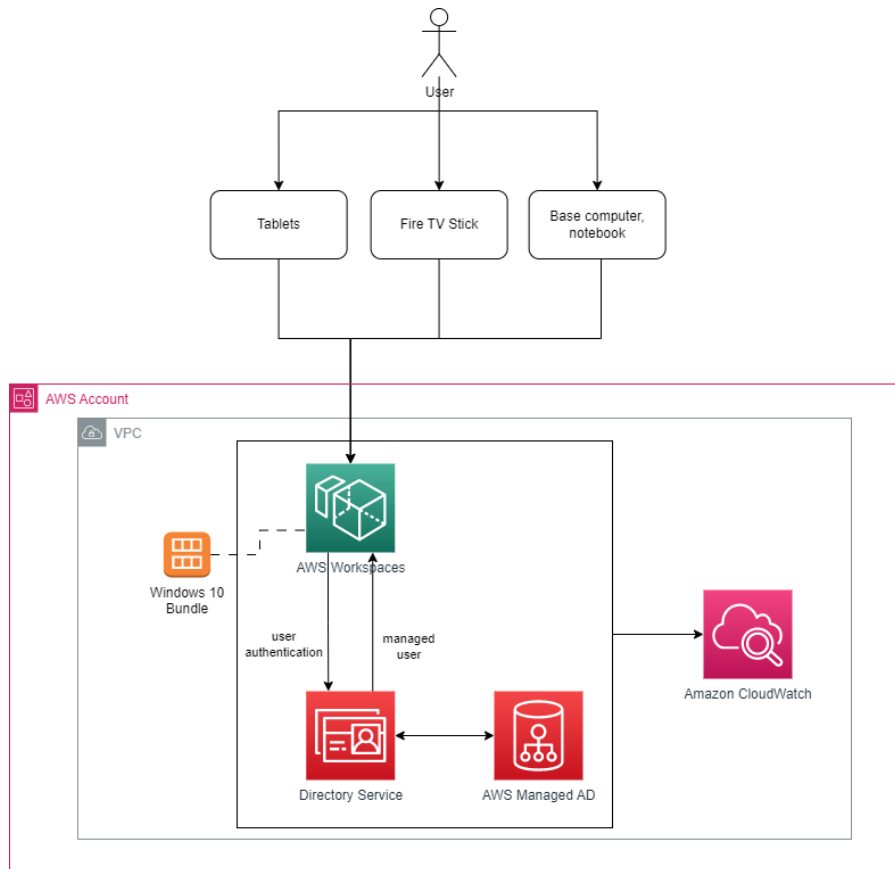
## EDUCATION PRICING

O preço educacional está disponível para WorkSpaces for Qualified Educational Users do Microsoft Windows. Com esta oferta, as organizações educacionais economizam US\$ 3,52 por usuário por mês ou US\$ 0,03 por usuário por hora usando os descontos de licenciamento da Microsoft. Você pode aproveitar esse desconto se estiver qualificado, com base nos [Termos e Documentação de Licenciamento da Microsoft](#). Caso a instituição esteja elegível para este desconto, ela pode solicitar através do [suporte AWS](#).

## Solução Adotada

Dados os pontos mencionados em ambas as propostas a solução B foi escolhida para ser adotada, pois ela garante vantagens como a ausência da necessidade de gerenciar servidores e o alocamento de recursos destas instâncias de forma

automática e direcionada para cada usuário.



## BENEFÍCIOS DE ARQUITETURA

- Capacidade de disponibilidade dos recursos em duas Zonas de Disponibilidade utilizando Multi-AZ deployment, garantindo maior resiliência e resistência à falhas.
- Workspaces com AutoStop configurado para 4 horas (tempo médio de um dia de aula de um curso), garantindo que a instância entre em “stop” automaticamente após o tempo definido, reduzindo custos e exposição à acessos indesejados.
- Capacidade de estabelecer uma relação de confiança com o AD local da instituição, permitindo a utilização dos usuários já cadastrados.
- Garantia de controle de ambiente através do Amazon CloudWatch, adquirindo métricas que podem ser visualizadas em dashboards customizados à seu gosto, obtendo informações referentes à utilização de CPU, banda de network utilizada, etc.
- Fim da necessidade de manutenciar e gerenciar servidores, pagar contas de luz e serviços de segurança externos, licenças de sistemas operacionais e etc, substituindo despesas de capitais (CapEx) por despesas operacionais (OpEx).
- Escalabilidade na capacidade de provisionar novas instâncias a qualquer momento de necessidade, melhorar recursos computacionais à qualquer momento, além de poder alocar recursos de armazenamentos de forma fácil e prática via console.
- Snapshots do Directory Service realizados automaticamente, garantindo backups que podem ser utilizados em qualquer momento caso alguma falha ocorra.

## DEPENDÊNCIAS

- Existência de um recurso com processamento (notebooks, FireStick, tablets, etc) para estabelecer conexão com o WorkSpaces.
- Dependência da conexão à internet: O AWS Workspaces requer uma conexão à internet estável para funcionar corretamente, o que pode ser um problema em áreas com acesso limitado ou com problemas de conectividade.
- Manutenção e atualização de software: A manutenção e atualização regular de software e firmware é crucial para garantir a segurança e o desempenho da infraestrutura. Isso inclui atualizações de patches de segurança, atualizações de sistema operacional e atualizações de firmware de dispositivos de rede.
- Gerenciamento de capacidade e escalabilidade: É importante gerenciar a capacidade da infraestrutura e garantir que ela possa ser escalada facilmente para atender às demandas de uso. Isso inclui o monitoramento do uso de recursos, a projeção de necessidades futuras de capacidade e a implementação de planos de escalabilidade.

## LIMITES DA SOLUÇÃO

- Limitação do AD gerenciado AWS: dependendo da configuração das instâncias e do AD gerenciado da AWS, pode haver limitações de recursos, como capacidade de armazenamento, memória e processamento, o que pode afetar o desempenho das aplicações.
- Logs e métricas do Amazon CloudWatch são atualizadas num período em torno de ~5 minutos, sendo “quase” em tempo real.
- Atualizações na imagem do Windows 10 utilizado para subir as instâncias de WorkSpaces não atualiza automaticamente as instâncias que já estão em serviço. Para isso, é necessário atualizar manualmente cada máquina, ou utilizar serviços autogerenciáveis como o Systems Manager Fleet Manager.

# Dependências de Operação

## TRATAMENTO DE RISCOS

Para o tratamento de riscos em uma infraestrutura AWS como essa, é importante seguir as práticas recomendadas de segurança da AWS, que incluem:

- Controle de acesso: é necessário configurar as permissões de acesso para limitar o acesso a recursos apenas para os usuários que precisam acessá-los. O uso de políticas de controle de acesso baseadas em funções e grupos pode ajudar a evitar que usuários mal-intencionados acessem recursos não autorizados.
- Segurança de rede: é importante configurar as regras de segurança de rede apropriadas para garantir que apenas o tráfego necessário entre os recursos seja permitido. O uso de grupos de segurança pode ajudar a proteger os recursos contra acesso não autorizado.
- Monitoramento: o monitoramento contínuo de eventos de segurança é importante para detectar atividades suspeitas e reagir a elas de forma rápida. A AWS oferece diversas ferramentas de monitoramento, como o AWS CloudTrail e o Amazon GuardDuty, que podem ajudar na detecção de atividades suspeitas.
- Backup e recuperação de desastres: é importante fazer backup regularmente de dados e configurar a recuperação de desastres para garantir a disponibilidade contínua dos recursos em caso de falhas ou desastres.
- Gerenciamento de patches: é importante manter os sistemas e softwares atualizados com os patches de segurança mais recentes para proteger contra vulnerabilidades conhecidas.

Além disso, é importante realizar avaliações regulares de risco e implementar controles de segurança adequados para mitigar os riscos identificados. A AWS oferece diversas ferramentas e serviços de segurança para ajudar na proteção da infraestrutura e dos dados.

## SEGURANÇA

A AWS oferece dois níveis de proteção contra ataques DDoS: AWS Shield Standard e AWS Shield Advanced. O AWS Shield Standard é incluído automaticamente sem nenhum custo extra além do que você já paga pelo AWS WAF e outros serviços da AWS. Para proteção adicional contra ataques DDoS, a AWS oferece o AWS Shield Advanced, uma proteção expandida contra ataques DDoS para suas instâncias do Amazon EC2, balanceadores de carga do Elastic Load Balancing, distribuições do Amazon CloudFront e zonas hospedadas do Amazon Route 53.

Também é possível utilizar o AWS WAF para bloquear ou permitir solicitações com base nas condições especificadas, como endereços IP de origem das solicitações ou valores nas solicitações, além do AWS Firewall Manager que simplifica suas tarefas de administração e manutenção do AWS WAF em várias contas e recursos.

Levando em consideração o escopo do projeto, é válido a utilização do AWS Shield Standard além de boas praticas de desenvolvimento de arquitetura, já que a utilização dos outros serviços trariam custos desnecessários em relação às vantagens oferecidas nas documentações.

## FAQ

- Programa de apoio a faculdades, instituições de ensino no geral: [https://w.amazon.com/bin/view/AWS\\_Academy/](https://w.amazon.com/bin/view/AWS_Academy/)
- Qualificação de Educational Pricing para instâncias do WorkSpaces: <https://support.console.aws.amazon.com/support/home#/case/create?issueType=customer-service&serviceCode=billing&categoryCode=qualify-as-educational-institution>