

## **Roteiro 1 – Gerenciamento de Identidade e segurança de acesso aos recursos em nuvem**

**Professor Rodolfo Avelino**

**Objetivo:**

**Leitura preliminar:**

**Security best practices in IAM**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

[https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction\\_identity-management.html?icmpid=docs\\_iam\\_console#AccessControlMethods](https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_identity-management.html?icmpid=docs_iam_console#AccessControlMethods)

**Entrega:** 07/03/2024

### **Gerenciamento de credenciais**

Garantir a confidencialidade e a integridade dos dados é fundamental em uma era em que muitas organizações dependem de serviços em nuvem, conectividade da Internet das Coisas (IoT), Inteligência Artificial (IA) e aprendizado de máquina. Os usuários devem ser devidamente identificados, autenticados e autorizados a acessar dados e aplicativos sem comprometer a segurança das credenciais de login.

Existem vários protocolos IAM para oferecer suporte a políticas IAM fortes, protegendo os dados e garantindo sua integridade durante a transferência. Geralmente conhecidos como “Autenticação, Autorização, Contabilidade” (Authentication, Authorization, Accounting ou AAA), esses protocolos de gerenciamento de identidade fornecem padrões de segurança para simplificar o gerenciamento de acesso, auxiliar

na conformidade e criar um sistema uniforme para lidar com interações entre usuários e sistemas.

O gerenciamento de acesso é fundamental para proteger a nuvem. Entenda as diferenças entre funções e usuários do AWS IAM para restringir adequadamente o acesso aos recursos da AWS.

## **Funções (Roles) IAM**

As funções IAM são identidades com permissões específicas para proteger recursos e conceder acesso temporário a uma conta. Elas são aplicadas por administradores a usuários, cargas de trabalho ou serviços com credenciais para acessar recursos na nuvem. As funções permitem solicitações de API seguras e delegação de permissões de API. Elas são mais práticas e escaláveis do que provisionar e atualizar credenciais de instância individualmente, especialmente em um ambiente dinâmico de nuvem pública.


## **Usuários IAM**

É uma entidade composta por credenciais e permissões específicas, como funções, para controlar o acesso de pessoas ou aplicativos à plataforma de nuvem. Os usuários são associados a credenciais de longo prazo e normalmente são criados normalmente pelos administrados da nuvem. Para facilitar o gerenciamento, os administradores podem criar grupos de usuários que compartilham as mesmas permissões, tornando mais fácil a adição ou remoção de usuários em caso de mudanças organizacionais.

## Tarefa 1 - Criando um Usuário Administrador no IAM da AWS

**É obrigatório print nos itens das tarefas e a leitura dos materiais indicados nos links no início deste roteiro.**

1. Faça login no Console de Gerenciamento da AWS, com os acessos fornecidos para cada grupo.
2. Abra o serviço IAM (Identity and Access Management). Utilize o menu ou a busca na barra superior da página.
3. Clique em "Usuários" no menu lateral.
4. Clique em "Adicionar usuário".
5. Digite um nome de usuário, em seguida selecione o tipo de acesso:
  - Acesso programático: Permite o uso de chaves de acesso programáticas para acesso via API.
  - Acesso à AWS Management Console: Permite o acesso ao console da AWS. Observe que este tipo de usuário é selecionado a partir da configuração do campo abaixo.

☐ Fornecer acesso para os usuários ao Console de Gerenciamento da AWS - *opcional*  
Se você está fornecendo acesso ao console para uma pessoa, a [prática recomendada](#)  é gerenciar o acesso dela no Centro de Identidade do IAM.

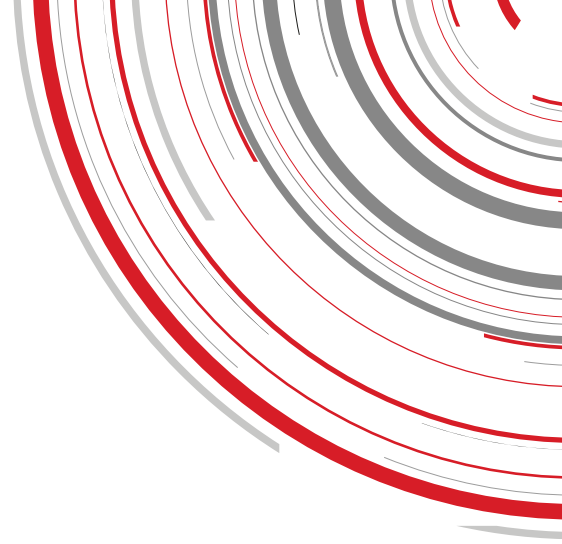
### 6. Defina as permissões:

- Adicionar ao grupo existente: Adicione o usuário a um grupo que tenha as permissões adequadas.
- Definir permissões de usuário diretamente: Defina políticas diretamente no usuário para conceder permissões específicas.

7. Clique em "Avançar: Tags" para adicionar tags opcionais.
8. Clique em "Avançar: Revisar" para revisar as configurações.
10. Clique em "Criar usuário".

OBS: Anote a chave de acesso e a chave secreta para o usuário. Estes são necessários caso você tenha configurado algum acesso programático.

**Agora, crie um usuário para cada componente do grupo.**



## Tarefa 2 - Criando as instâncias para o e-commerce

### Pacotes necessários:

- Apache2
- Mysql Server
- PHP
- Wordpress
- plugin WooCommerce

### Instalando o Servidor de aplicação

- Crie uma instância **micro** na região North Virginia com a distribuição GNU/Linux debian ou ubuntu;
- Configure o NSG (Network Security Group) para permitir os acessos padrão de um web server;
- Instale os pacotes básicos para o servidor receber o Wordpress:  
`sudo apt install apache2 php php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip`
- Configure o arquivo de configuração no diretório `/etc/apache2/sites-enable`, para o domínio da ABC Place.
- Instale o processo certbot para a instalação do certificado digital.

## 2) Criar uma base de dados no banco de dados para ser utilizado no Wordpress

- A) Criar um usuário no Mysql específico para o wordpress;
- B) Criar base de dados;
- C) Conceder privilégios totais do usuário para a nova base.

## 3) Instalar Wordpress

- A) Transfira o pacote do Wordpress disponível no Black Board para a raiz do web server (/var/www/html);
- B) Descompactar o pacote e seguir o processo de instalação do Wordpress pelo navegador (Browser);
- C) Após concluir a instalação, no menu administrativo do Wordpress, acesse o menu "Plugin" e instale o WooCommerce.

## 4) Criando instância para banco de dados

- A) Crie uma instância **micro** na região North Virginia com a distribuição GNU/Linux debian ou ubuntu em sub rede diferente da instância da aplicação;
- B) Instalar o pacote Mysql-server;
- C) Conceder as permissões adequadas para o acesso remoto da aplicação. Mostre como ficou a alteração no arquivo de configuração.

## Tarefa 3 - Configurando CDN, DNS e WAF

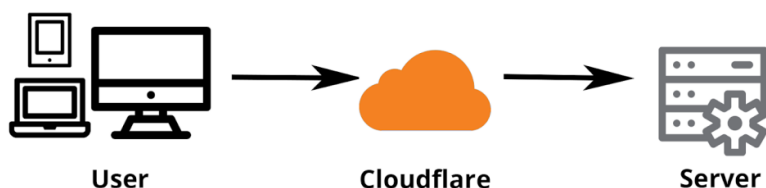
A Content Delivery Network (CDN), também conhecida como Rede de Distribuição de Conteúdo, é uma rede de servidores que distribuem conteúdo para usuários em todo o mundo. Para o nosso projeto iremos adotar a CDN da Cloudflare. Seus servidores estão espalhados globalmente e são sincronizados para atualizações rápidas, proporcionando aos usuários uma comunicação eficiente com os servidores, independentemente de sua localização no mundo. Isso reduz consideravelmente a latência e melhora a velocidade do site.



Figura 1: Rede Global da Cloudflare. Fonte: <https://www.cloudflare.com/pt-br/network/>

Além disso, a CDN da Cloudflare oferece uma opção de proxy que garante o anonimato dos apontamentos do domínio do usuário, ou seja, você consegue “ocultar” o IP de seu servidor, pois seu domínio estará associado a um IP da Cloudflare.. Isso significa que, ao tentar rastrear o IP de um domínio hospedado na Cloudflare, as

pessoas receberão apenas os IPs fixos da Cloudflare, não os IPs reais do servidor do usuário.



1. **Crie uma conta na Cloudflare:** Inicie o processo de configuração clicando em adicionar site e em seguida coloque as informações do domínio fornecido para seu grupo.
2. **Configurando o Domínio da ABC Place:** Configurar o domínio para ser acessado com ou sem WWW. Crie uma instância **micro** na região North Virginia com a distribuição GNU/Linux debian ou ubuntu;
3. **Criar 5 regras de WAF que estejam alinhados com seu plano de ação criado a partir da matriz de riscos incluindo também estes controles:**
  - a. Permitir apenas o acesso ao marketplace a partir de IPs do Brasil.
  - b. Criar regra de rate limiting para suspender um IP após 5 solicitações no caminho de URI /wp-admin.

Tirar print das telas do DNS e regras do waf.



## Tarefa 4 – Responda as questões

- 1) Em quais situações é indicado o uso das funções versus usuários IAM?
- 2) No Apache, qual a função do vhost?
- 3) Como você pode verificar se o Apache está instalado e em execução em um sistema Linux?
- 4) Qual é a função do arquivo .htaccess no Apache?
- 5) Em uma configuração do Apache, como você pode garantir que seu servidor esteja acessível somente através de uma conexão HTTPS?