
Autenticação e Autorização AWS Cognito

— Prof. Raphael Rodrigues Pereira —

AWS Cognito - O que é

Serviço de autenticação e autorização da AWS

- Facilita o gerenciamento de cadastros e login de usuários em aplicações.
- Gerencia identidade de usuários
- Permite integração com redes sociais (Google, Facebook)

AWS Cognito - User Pool

User Pools são utilizados para gerenciar usuários e autenticação.

- Registro de usuários.
- Validação de e-mail/telefone.
- Login e autenticação com senha ou métodos alternativos (MFA).
- Integração com provedores externos (Google)

AWS Cognito - Identity Pool

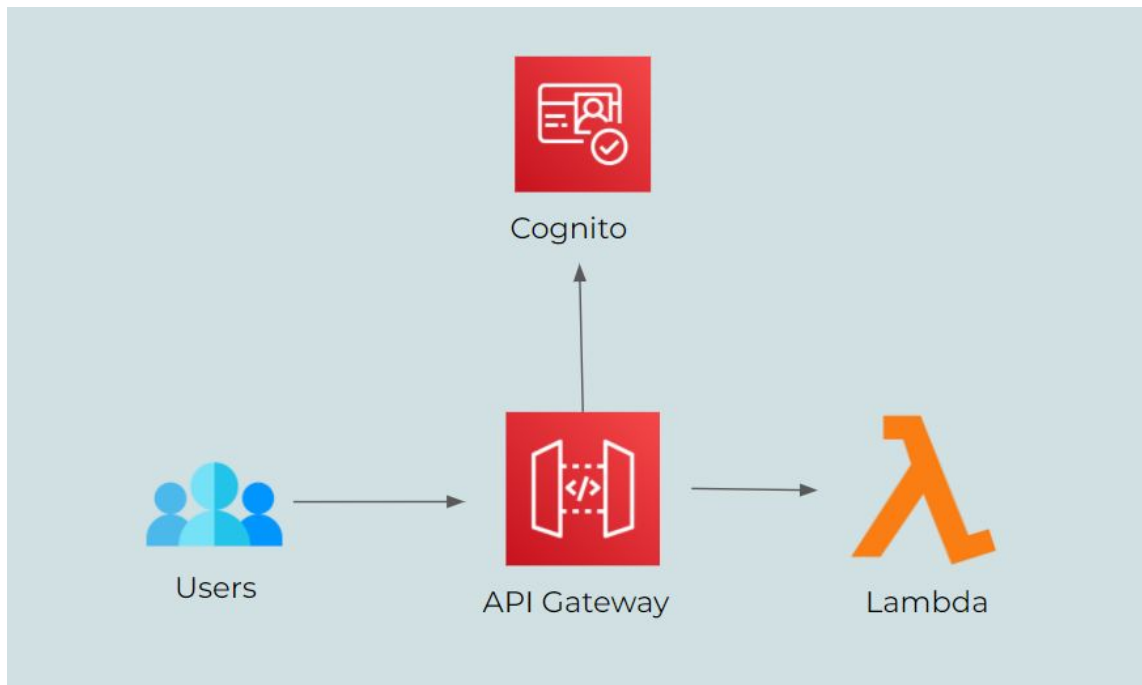
Identity Pool gerencia o controle de acesso à AWS.

- Associa credenciais temporárias da AWS a usuários autenticados.
- Acesso a serviços como DynamoDB, S3, etc.
- Integração com User Pools, provedores de redes sociais

Amazon Cognito no nível gratuito

Produto	Descrição	Detalhes da oferta de nível gratuito	Preços dos produtos
Amazon Cognito ①	Implemente um gerenciamento de identidade e acesso de clientes seguro e sem atrito, escalável.	SEMPRE GRÁTIS 10.000 MAUs por mês 10 GB de armazenamento de sincronização em nuvem 1.000.000 de operações de sincronização por mês	Preços do Amazon Cognito

AWS Cognito: Exemplo de aplicação



Exemplo Prático

Utilizando Cognito para gerenciar Login

Comece pelo seu caso de negócios

Adicione diretórios de usuários ao seu aplicativo ▼

Os pools de usuários do Amazon Cognito são um serviço gerenciado que permite adicionar autenticação e autorização seguras aos seus aplicativos e podem ser dimensionados para oferecer suporte a milhões de usuários.

Criar pool de usuários

Configurar experiência de login [Informações](#)

Os usuários do seu aplicativo podem entrar no seu pool de usuários com um nome de usuário e senha ou entrar com um provedor de identidade de terceiros.

Provedores de autenticação

Configure os provedores que estão disponíveis para os usuários quando eles efetuam login.

Tipos de provedores

Escolha se os usuários farão login no seu pool de usuários do Cognito, em um provedor de identidade federado ou em ambos. O Amazon Cognito tem preços diferentes para usuários federados e usuários do pool de usuários. [Saiba mais sobre preços](#)

☒ Pool de usuários do Cognito

Os usuários podem fazer login usando seu endereço de e-mail, número de telefone ou nome de usuário. Atributos de usuário, associações de grupo e configurações de segurança serão armazenados e configurados em seu pool de usuários.


☐ Provedores de identidade federados

Os usuários podem fazer login usando credenciais de provedores de identidade social como Facebook, Google, Amazon e Apple; ou usando credenciais de diretórios externos por meio de SAML ou Open ID Connect. Você pode gerenciar mapeamentos de atributos de usuário e segurança para usuários federados em seu pool de usuários.

Opções de login do pool de usuários do Cognito [Informações](#)

Escolha os atributos no seu pool de usuários que são usados para fazer login. Se você selecionar apenas um atributo, ou selecionar um nome de usuário e pelo menos um outro atributo, seu usuário poderá fazer login com todas as opções selecionadas. Se você selecionar apenas número de telefone e e-mail, seu usuário será solicitado a selecionar uma das duas opções de login quando se inscrever.

- ☐ Nome de usuário
- ☒ E-mail
- ☐ Número de telefone

 As opções de login do pool de usuários do Cognito não podem ser alteradas após a criação do pool de usuários.

Cancelar

Próximo

Criando User Pool para fazer login com e-mail

Configurar requisitos de segurança [Informações](#)

Defina um requisito de senha forte, além da autenticação multifator, para proteger os usuários do comprometer acidentalmente suas credenciais.

Política de senha [Informações](#)

Crie uma política de senha para definir o comprimento e a complexidade das senhas que seus usuários podem

Modo de política de senha [Informações](#)



Padrões Cognito

Use os requisitos de senha padrão.



Personalizado

Use os requisitos de senha que

Comprimento mínimo da senha

8 caracteres

Requisitos de senha

Contém pelo menos 1 número

Contém pelo menos 1 caractere especial

Contém pelo menos 1 letra maiúscula

Contém pelo menos 1 letra minúscula

As senhas temporárias definidas pelos administradores expiram em

7 dia(s)

Autenticação multifatorial

Configure o acesso seguro ao seu aplicativo aplicando autenticação multifator (MFA) durante o processo de login do usuário. As configurações de MFA são aplicadas a todos os clientes do aplicativo.

Aplicação do MFA [Informações](#)



Exigir MFA - Recomendado

Os usuários devem fornecer um fator de autenticação adicional ao fazer login.



MFA opcional

Os usuários podem fazer login com um único fator de autenticação e podem optar por adicionar fatores de autenticação adicionais.



Sem MFA

Os usuários só podem fazer login com um único fator de autenticação. Esta é a opção menos segura.

Recuperação de conta de usuário

Configure como os usuários recuperarão suas contas quando esquecerem suas senhas. Taxas de dados e mensagens de destinatário se aplicam.

Recuperação de conta de autoatendimento [Informações](#)



Habilitar recuperação de conta de autoatendimento - Recomendado

Permita operações de esquecimento de senha no seu pool de usuários. Na página de login da IU hospedada, um link "Esqueceu sua senha?" é exibido. Quando esse recurso não está habilitado, os administradores redefinem as senhas com a API do Cognito.

Método de entrega para mensagens de recuperação de conta de usuário [Informações](#)

Selecione como seu pool de usuários entregará mensagens quando os usuários solicitarem um código de recuperação de conta. Mensagens SMS são cobradas separadamente pelo Amazon SNS. Mensagens de e-mail são cobradas separadamente pelo Amazon SES. [Saiba mais sobre preços.](#)



Somente e-mail



Somente SMS



E-mail se disponível, caso contrário, SMS



SMS se disponível, caso contrário, e-mail



SMS se disponível, caso contrário, envie e-mail e permita que o usuário redefina sua senha via SMS se também a estiver usando para MFA

Definição de padrão de senha, MFA e recuperação de senha


Inscrição de autoatendimento [Informações](#)

Escolha se novos usuários do seu aplicativo podem registrar uma conta.

Auto-registo [Informações](#)

☒ Habilitar auto-registro

Exiba um link "Inscreva-se" na página de login na IU hospedada e permita o uso de APIs públicas para criar novas contas de usuário. Quando esse recurso não está habilitado, as operações de API administrativas e de federação criam perfis de usuário.

 Se você ativar a inscrição de usuário no seu pool de usuários, qualquer pessoa na internet poderá se inscrever para uma conta e entrar em seus aplicativos. Não habilite o autoregistro no seu pool de usuários até que você queira abrir seu aplicativo para inscrição pública. [Saiba mais](#)

Required attributes [Info](#)

Choose the attributes that are required when a new user is created. Cognito assigns all users a set of standard attributes based on the OpenID Connect (OIDC) standard.

Required attributes based on previous selections

email

Additional required attributes


Select attributes

birthdate X

name X

phone_number X

profile X

 Required attributes can't be changed once this user pool has been created.

▼ Custom attributes - optional

Personalize the sign-up experience by adding up to 50 custom attributes. Custom attribute names can't be changed after a user pool has been created.

Name	Type	Min - optional	Max - optional	Mutable	
matricula	String ▼	10	10	<input checked="" type="checkbox"/>	Remove


Name must be 20 characters or fewer.

Length must be 2048 bytes or fewer.

Length must be 2048 bytes or fewer.

Add another

You can add 49 more custom attributes

 Custom attribute names cannot be changed once this user pool has been created. Cognito will prepend "custom:" to your attribute names once they are created.

Configuração sobre inscrição - auto cadastro - campos para preenchimento