

Como boa prática, é melhor isolarmos nosso trabalho em usuários específicos, e não trabalharmos direto na conta principal (root). Esta conta serve mais para gerenciar a sua própria relação com a AWS e possui domínio total sobre toda sua conta AWS.

Por isso, aplique as boas práticas de segurança e crie um usuário para seu estudo nesse curso.

1. Crie um novo user no serviço IAM;

Especificar detalhes do usuário

Detalhes do usuário

Nome do usuário

UsuárioLab365

O nome de usuário pode ter até 64 caracteres. Caracteres válidos: A-Z, a-z, 0-9, and + = , _ @ - (ñífen)

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.

Se você estiver criando acesso programático por meio de chaves de acesso ou credenciais específicas de serviço para o AWS CodeCommit ou o Amazon Keyspaces, poderá gerá-las depois de criar esse usuário do IAM.

Saiba mais

Cancelar

Próximo

2. Configure as permissões de acesso;

Definir permissões

Adicione usuário a um grupo existente ou crie um novo. Usar grupos é uma prática recomendada para gerenciar as permissões do usuário por funções de trabalho. [Saiba mais](#)

Opções de permissões

Adicionar usuário ao grupo

Adicione o usuário a um grupo existente ou crie um novo grupo. Recomendamos usar grupos para gerenciar permissões de usuário por função de trabalho.

Copiar permissões

Copie todas as associações a grupos, políticas gerenciadas anexadas e políticas em linha de um usuário existente.

Anexar políticas diretamente

Anexe uma política gerenciada diretamente a um usuário. Como prática recomendada, recomendamos anexar políticas a um grupo. Em seguida, adicione o usuário ao grupo apropriado.

Grupos de usuários (1)

Criar grupo

Pesquisar grupos

<input type="checkbox"/>	Nome do grupo	▲	Usuários	▼	Políticas anexadas	▼	Criado	▼
<input type="checkbox"/>	Devs1		0		Nenhum		2023-05-31 (1 minuto atrás)	

► Limite de permissões - opcional

Defina um limite de permissões para controlar o número máximo de permissões para esse usuário. Use esse recurso avançado para delegar o gerenciamento de permissões a outros usuários. [Saiba mais](#)

Cancelar

Anterior

Próximo

3. Configure a autenticação multifator (MFA).

UsuarioLab365

Excluir

Resumo

ARN

arn:aws:iam::272282841126:user/UsuarioLab365

Acesso ao console

Desabilitado

Chave de acesso 1

Não habilitado

Criado

May 31, 2023, 20:20 (UTC-03:00)

Último login no console

-

Chave de acesso 2

Não habilitado

Permissões

Grupos (1)

Etiquetas

Credenciais de segurança

Consultor de acesso

Login do console

Habilitar acesso ao console

Link de login do console

https://272282841126.signin.aws.amazon.com/console

Senha do console

Não habilitado

Autenticação multifator (MFA) (1)

Use a MFA para aumentar a segurança do seu ambiente da AWS. Fazer login com a MFA requer um código de autenticação de um dispositivo MFA. Cada usuário pode ter no máximo oito dispositivos MFA atribuídos. [Saiba mais](#)

Remover

Sincronizar novamente

Atribuir dispositivo com MFA

Tipo de dispositivo	Identificador	Criado em
<input type="radio"/> Virtual		4 minutos atrás