

4. Primeiros Passos com Acesso Seguro e Controle de Custos

Introdução

Agora que sua conta está segura, é hora de aprender a acessar a AWS programaticamente (via CLI) e controlar quanto você está gastando. Ninguém quer surpresas horríveis na fatura!

Sumário

- O que é IAM (revisão rápida)
- Chaves de Acesso para CLI
- Criando Grupos de Usuários
- Controlando Custos
- Questões
- Conclusão
- Referências

O que é IAM ?

IAM = Identity and Access Management

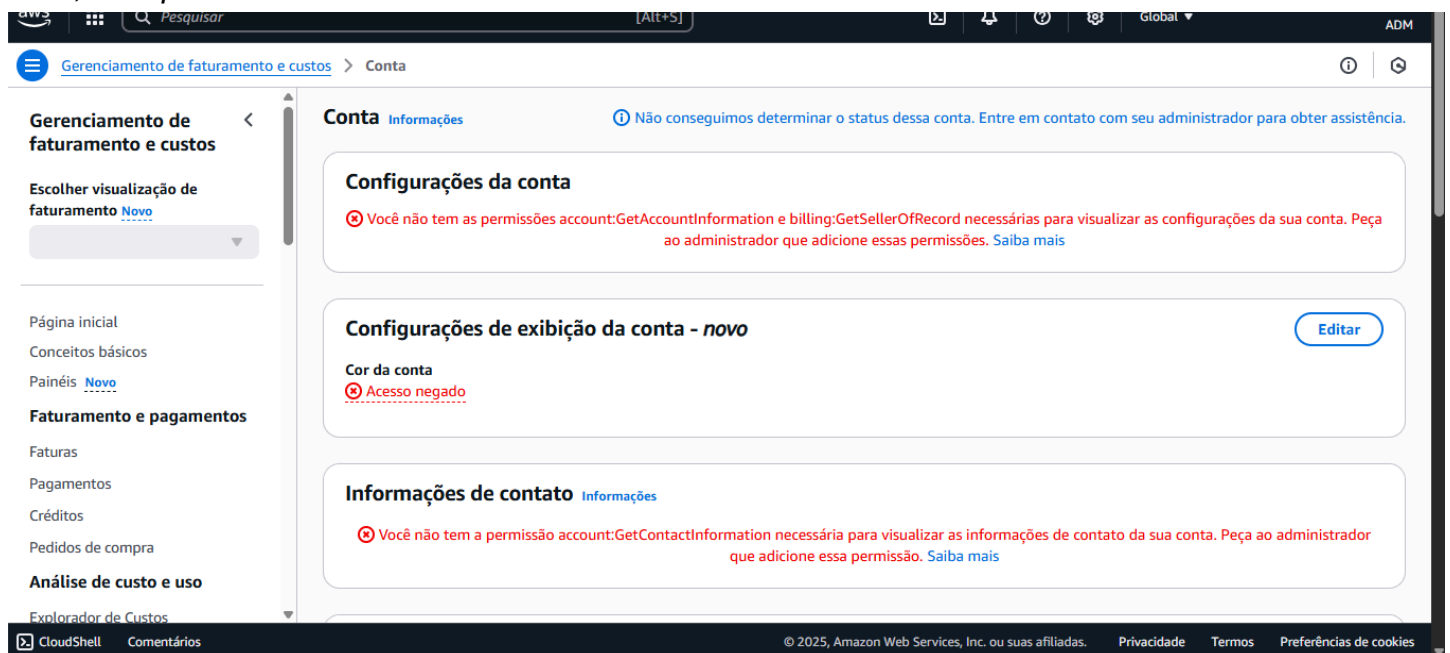
É o sistema que gerencia:

- Quem pode acessar o quê
- Com quais permissões
- De onde
- Quando

Simples assim.

Chaves de Acesso para CLI

Erros: Os erros que estavam aparecendo eram porque o usuário ADM não tinha as permissões corretas. Não foi necessário criar uma permissão em JSON, pois a permissão que eu precisava era de acesso total, como ADM. Como ela já constava na lista da AWS junto com outras permissões, apliquei-a como permissão direta. Os erros foram resolvidos e agora tenho acesso total à conta ADM, sem precisar acessar a conta root toda hora.



Quando você quer usar a AWS via terminal (CLI), precisa se autenticar. Mas não pode digitar senha toda hora!

Solução: Chaves de Acesso

O que é? Um par de credenciais que você gera:

1. **Access Key ID** → tipo um "usuário"

2. **Secret Access Key** → tipo uma "senha"

Access Key ID: AKIAIOSFODNN7EXAMPLE

Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

Como funciona:

Você no terminal: `aws s3 ls`

↓

CLI envia suas credenciais

↓

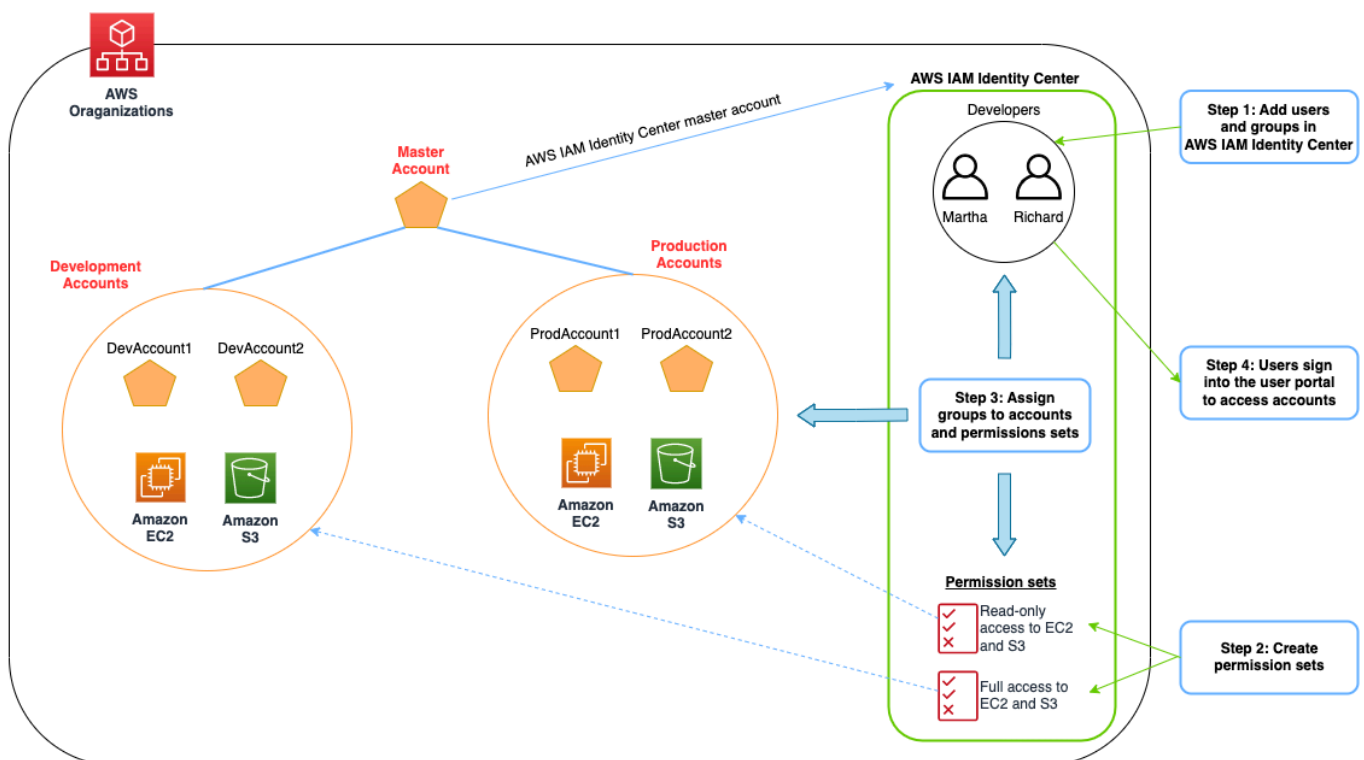
AWS verifica: "é você mesmo?"

↓

AWS: "Sim, pode usar S3"

↓

Você vê os arquivos



Posso usar a mesma chave da conta root?

NÃO!

Por quê?

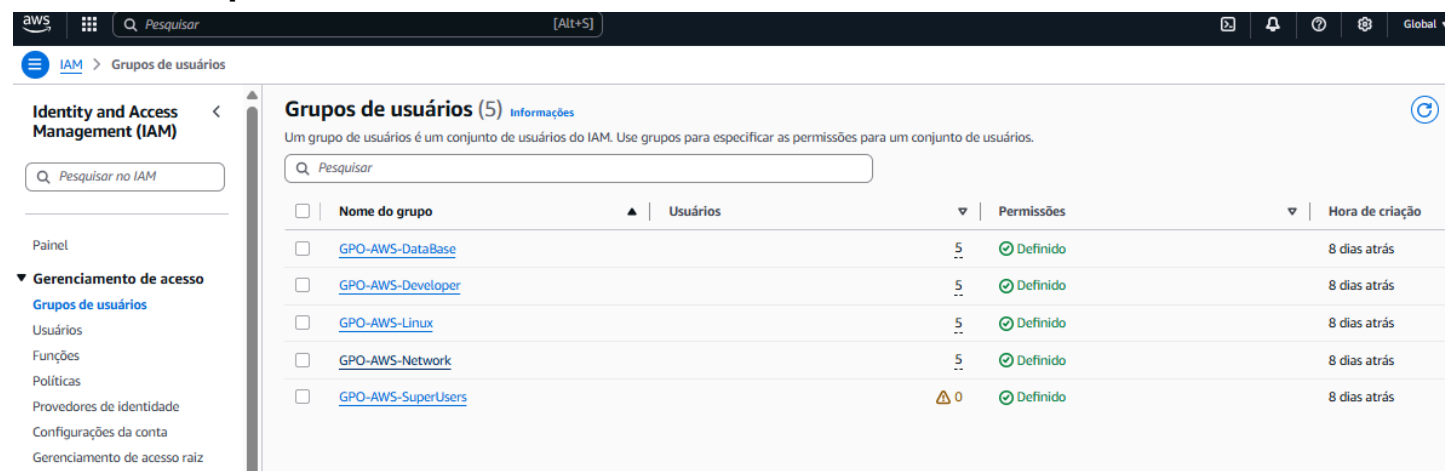
- Root tem acesso total
- Se a chave vazar, hackers têm tudo
- É arriscado demais

O correto:

1. Crie um usuário IAM (exemplo: "João-CLI")
2. Dê permissões específicas a esse usuário
3. Gere chaves de acesso para "João-CLI"
4. Use essas chaves no terminal

Se a chave vazar, só João-CLI está em risco, não toda a conta!

Criando Grupos de Usuários



The screenshot shows the AWS IAM console interface. On the left, there's a navigation menu with 'Identity and Access Management (IAM)' selected. The main area is titled 'Grupos de usuários (5) Informações'. Below the title, there's a search bar and a table listing the groups. The table has columns for 'Nome do grupo', 'Usuários', 'Permissões', and 'Hora de criação'. The groups listed are GPO-AWS-DataBase, GPO-AWS-Developer, GPO-AWS-Linux, GPO-AWS-Network, and GPO-AWS-SuperUsers. The 'GPO-AWS-SuperUsers' group has a warning icon and a count of 0.

Nome do grupo	Usuários	Permissões	Hora de criação
GPO-AWS-DataBase	5	Definido	8 dias atrás
GPO-AWS-Developer	5	Definido	8 dias atrás
GPO-AWS-Linux	5	Definido	8 dias atrás
GPO-AWS-Network	5	Definido	8 dias atrás
GPO-AWS-SuperUsers	0	Definido	8 dias atrás

Comentários sobre a prática: Criei os grupos e subi a permissão conforme cada setor, além da permissão para alterar a própria senha.

Adendo: o professor cria uma pasta com todas as atividades, então, antes de enviar pelo Git Bash, é necessário ter essa pasta. Ao todo, são 20 usuários, e o envio é feito de uma só vez.

Controlando Custos

AWS pode ficar caro RÁPIDO se você não tomar cuidado. Um servidor rodando 24/7 que você esqueceu pode custar centenas de dólares ao fim do mês.

O que fazer?

1. Configure Alertas de Orçamento

Na AWS, você vai em Faturamento → Alertas de Orçamento

"Se eu gastar mais de \$100 por mês, me avisa"

Você pode criar múltiplos alertas:

- "Se gastar mais de \$50, aviso"
- "Se gastar mais de \$100, aviso!"
- "Se gastar mais de \$200, aviso URGENTE"

2. Use o Free Tier

A AWS oferece **1 ano grátis** para novos usuários em certos serviços.

O que entra no Free Tier:

- 750 horas/mês de EC2 (um computador)
- 5 GB em S3 (armazenamento)
- 1 milhão de requisições Lambda
- Banco de dados RDS grátis

O que NÃO entra:

- Se você exceder os limites
- Alguns serviços como dados de saída (download de muita coisa)

Importante: Depois que o Free Tier acaba, você começa a pagar! Se você não desativar recursos, continua pagando.

3. Desligue o que não está usando

- Servidor de teste parado? Desliga
- Banco de dados de desenvolvimento? Apaga se não vai usar
- Volumes de armazenamento antigos? Remove

Cada recurso rodando = dinheiro saindo

O CloudShell é seu Amigo

É um terminal dentro do site da AWS.

[Abre AWS] → [Clica em CloudShell] → [Terminal abre dentro do navegador]

Vantagem: Sem instalar CLI localmente, sem configurar chaves de acesso no seu PC

Rápido e seguro!

Questões

1. O que é IAM?

- ☐ Um serviço de armazenamento
- ☒ Identity and Access Management
- ☐ Um banco de dados
- ☐ Um tipo de servidor

2. Chaves de acesso são para:

- ☐ Fechar a porta
- ☐ Acessar o console web
- ☒ Autenticar via CLI/programaticamente
- ☐ Criar novos usuários

3. É recomendado usar a chave root para CLI?

- ☐ Sim
- ☒ Não
- ☐ Às vezes
- ☐ Só em segunda-feira

4. O Free Tier dura quanto tempo?

- ☐ 3 meses
- ☐ 6 meses
- ☒ 1 ano
- ☐ Sempre grátis

5. Qual é a melhor forma de controlar custos?

- ☐ Esperar a fatura chegar
- ☐ Rezar para não ficar caro
- ☒ Configurar alertas de orçamento
- ☐ Desligar a AWS

6. Depois que o Free Tier acaba, você para de pagar?

- ☐ Sim
- ☒ Não, precisa cancelar ou desligar recursos
- ☐ Depende
- ☐ AWS avisa antes

Conclusão

Segurança e controle de custos são os dois pilares do sucesso na AWS. Use IAM para gerenciar acesso, chaves de acesso para CLI, agrupe usuários para facilitar, e sempre configure alertas de custo. Assim você trabalha tranquilo sem medo de surpresas.

Referências

- AWS IAM: <https://aws.amazon.com/iam/>
- AWS Billing Alerts: https://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/monitor_estimated_charges_with_cloudwatch.html
- AWS CLI Documentation: <https://docs.aws.amazon.com/cli/latest/userguide/>