Introdução ao IAM (Identity and Acess Management)

segunda-feira, 29 de maio de 2023

14:24

**O usuário para ter acesso ao IAM existem 3 formas**, Via console, CLI, API.

Tendo acesso ao IAM conseguimos criar Users, Role ( Regras ), Group, Federated users ( Usuários que utilizam Sing in, Sing on ), Applications.

A partir disso conseguimos gerenciar ou criar as políticas:

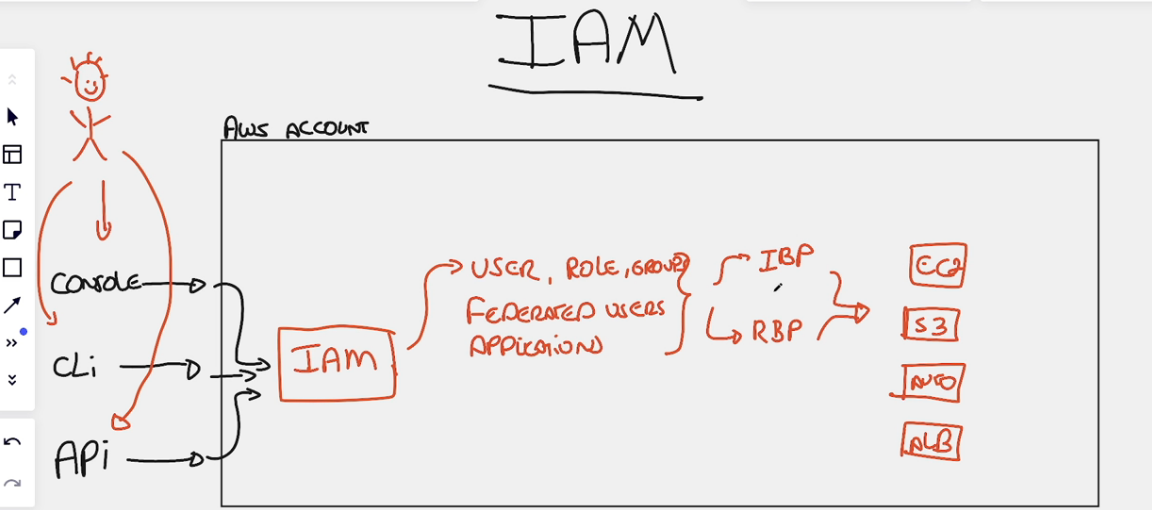
IBP - Identity Base Policy - Permitir ou bloquear uma identidade

RBP - Resource Base Policy - Permitir ou bloquear um recurso

A partir disso conseguimos acessar algum tipo de serviço

EC2 - S3 - ELB - Autoscalling

Todos os serviçõs são API - verificando usuário ou todos os outros tipos.



Entenda sobre usuários, Grupos, Policy, Roles

segunda-feira, 29 de maio de 2023

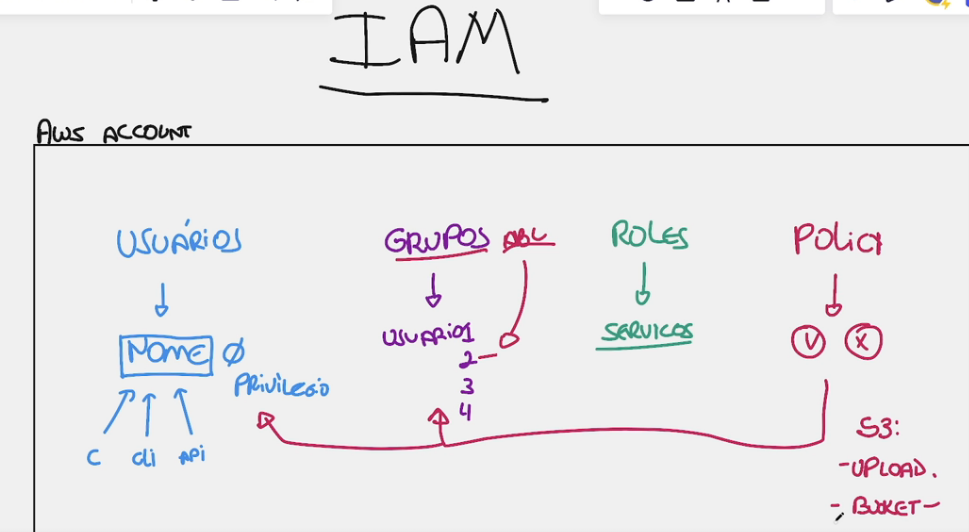
14:51

Os usuários são criados porém com 0 privilégios

Os Grupos são criados para inserir usuários específicos dependendo dos privilégios

As Roles ( Regras ) são determinadas para serviços, por exemplo conseguimos disponibilizar para um serviço S3, quem consegue acessar.

Policy são regras específicas para usuários acessarem um serviço, exemplo usuário 2 consegue apenas fazer upload na bucket.



Criando usuário na IAM

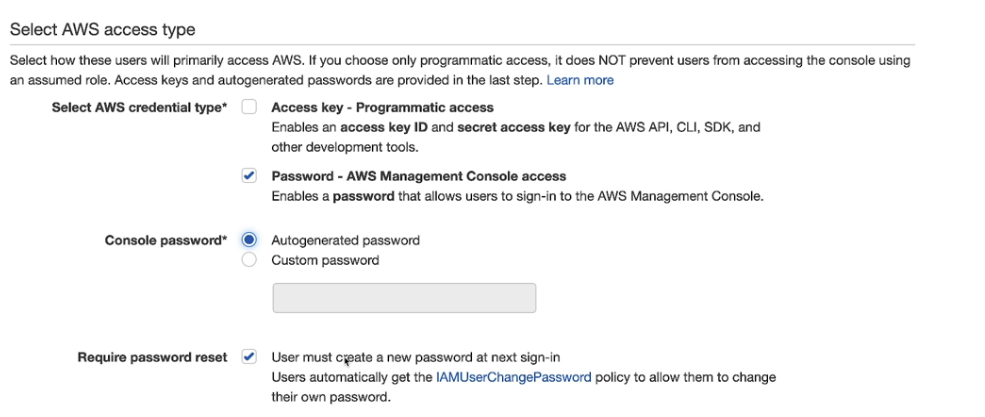
segunda-feira, 29 de maio de 2023

14:55

O usuário principal é o Root - Não é recomendado utilizar o usuário Root, por questões de segurança

IAM > Usuários > Criar usuários

Podemos criar mais de um usuários > Acess Key ( Ferramenta de desenvolvimento ) ou Password ( Acesso a console ) > Senhas podem ser autogenerated ( auto-geradas ) ou Custom ( criadas pelo usuário root ) > Required password reset ( quando o usuário logar a primeira vez mudar a senha .



* Se não configurar nada de grupos esse usuário não terá permissão.
* Após a criação do usuário, tem um link de acesso para passar para o usuário.

* Copie a senha para passar para o usuário.

Aplicando a política ao usuário

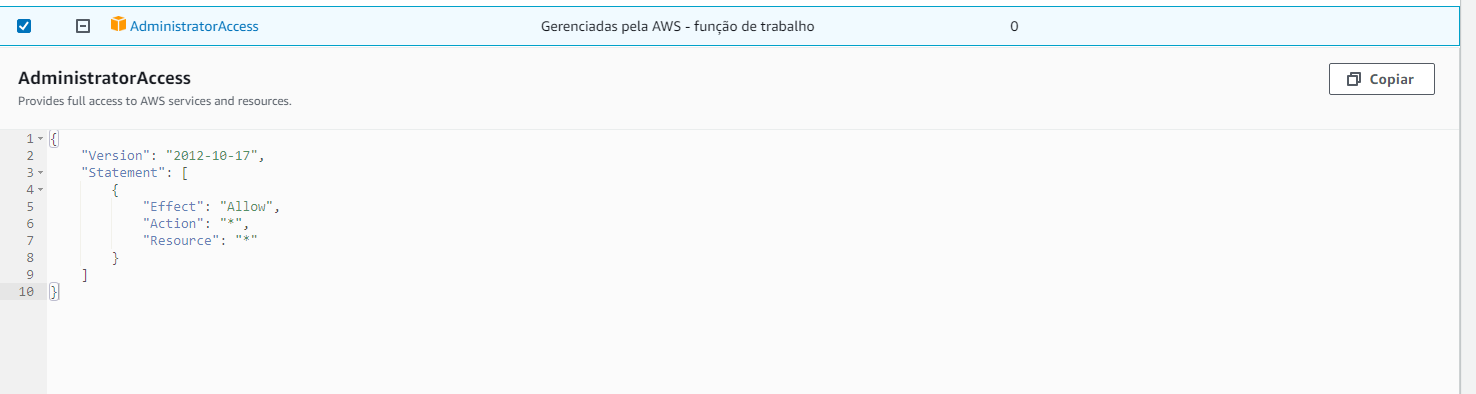
segunda-feira, 29 de maio de 2023

15:30

Clicando em IAM > users > selecione o usuário > add permissions > Attach existing policies directly

Podemos dar permissão - criando um grupo ou copiando permissões existentes ou inserindo políticas existentes.

AdministratorAcess - Permite ter todos os acessos parecidos com o root - é uma Job Function

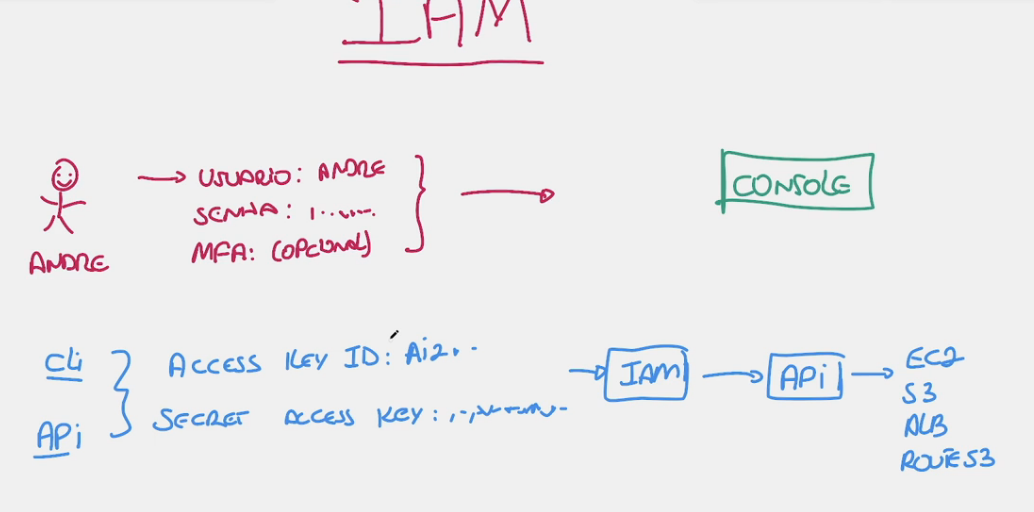


Os privilégios são em JSON.

Autenticação AWS

segunda-feira, 29 de maio de 2023

15:44



Dessa forma conseguimos verificar o tipo de acesso e quem está logando na conta.

MFA

terça-feira, 30 de maio de 2023

14:45

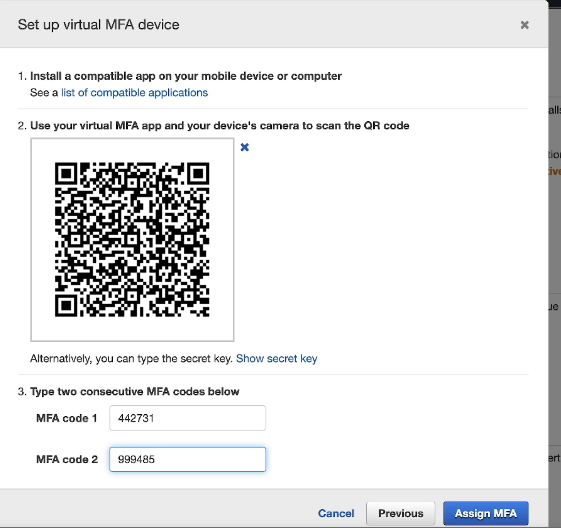
MFA - Multi Factor Autenticathion

Além do usuário e senha, existe uma autenticação extra para logar.

MFA - Pode ser virtual ( app - Google autenticator ) ou físico ( Token - Parecido com um pen drive - é um dispositivo físico ).

Para adicionar uma MFA devemos logar na conta > Adicionar MFA > na parte Multi Factor Authentication (MFA) > Assign MFA device > Virtual MFA device

Use o + do app google authentication para adicionar uma MFA, devemos adicionar o primeiro código, esperar 30 segundos e adicionar o segundo.



Com isso é gerado um ARM.

No próximo login, o aws pede o código do google authentication.

STS

terça-feira, 30 de maio de 2023

15:27

STS - Service Token Service

Quando queremos acessar uma bucket no S3 porém não queremos criar um usuário dentro da nossa máquina virtual (EC2)

Devemos criar um IAM Role fora do EC2 que é uma regra de IAM, que tem policy que podemos adicionar para a instância EC2 para acessar a bucket.

A bucket espera por uma acess key ( CLI ) e uma Secret Key (API) para ser acessada, com isso existe a STS que cria essas 2 Keys para acesso temporárias.

Alterando Políticas de senha

terça-feira, 30 de maio de 2023

15:55

A políticas de senha vai muito de acordo com a empresa, podendo ter diversas formas de alterar a solicitação dessa senha, podendo ser alterada a cada 90 dias

Acessamos em Configuração de conta > Política de senha

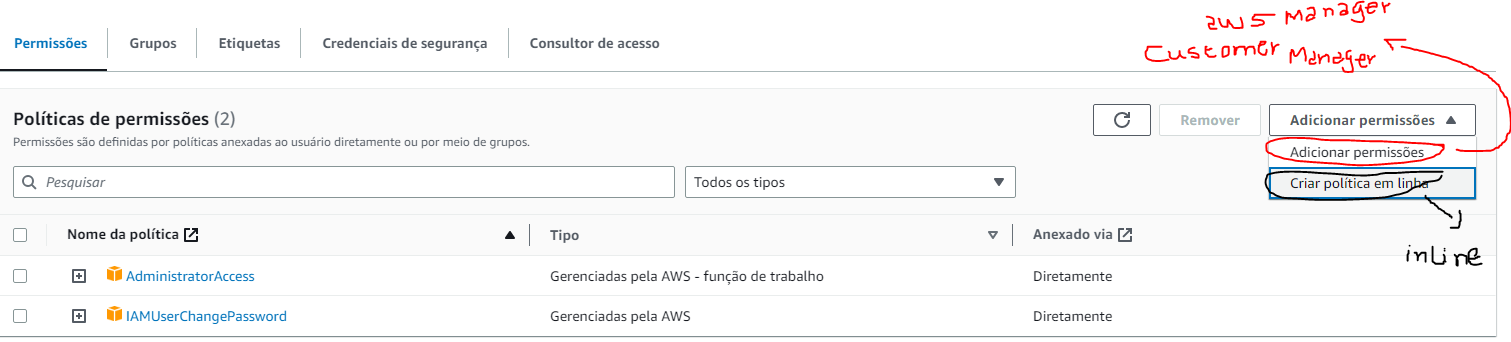
Politicas de Recursos e identidade

terça-feira, 30 de maio de 2023

16:01

**Identity Policy**

* InLine Policy - é uma política para um usuário ou para uma regra sempre de 1 pra 1.
* AWS manager ou Customer Manager - podem ser adicionado aos 3.



**Resource Policy**

Podemos adicionar policys aos serviços diretamente.

EC2 e no S3 - usuário neto pode acessar a S3 e fazer upload.

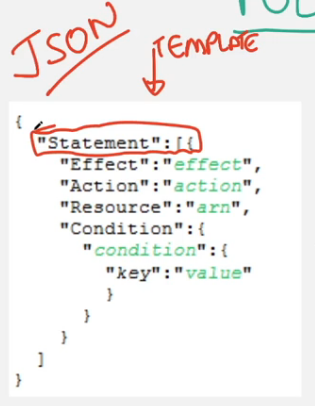
As políticas podem ser adicionados a usuário, grupo de usuários, Role.

Acessando um usuário > Permission Policies

As Estruturas das Policies

terça-feira, 30 de maio de 2023

18:34



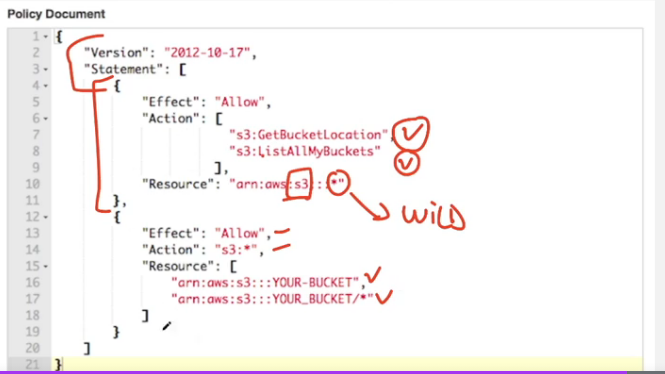
Statement - indica que você vai escrever as regras, a partir de agora vou escrever o que vai acontecer na politica

Effect - podem ser 2 coisas - Allow ou Deny

Action - Ação acima de um recurso

Resource - S3 ou EC2, qual o recurso vai ser implementada a política

Condition - seriam as exceções as regras, aplicações as regras, condições.



Boas Práticas IAM

terça-feira, 30 de maio de 2023

18:55

* Não utilize a conta Root - Crie uma User account
* Crie contas IAM individuais
* Crie grupos - Associe as policies aos grupos - se for criado por usuário perde a referência o que foi dado para cada usuário - Exemplo crie grupos de dev e de infra e coloquem dentro do grupo de permissões específicas
* Permita o mínimo - Mínimo de permissões
* Se estiver iniciando IAM agora - Utilize primeiro as Aws Manager e depois aprenda a usar as customers policies
* É sempre recomendado a utlização do MFA - Multi Factor Authentication para manter a segurança dos serviços
* Revise as policy password sempre que possível, adicionando regras recomendadas.