**Resumo - IAM**

O AWS Identity and Access Management (IAM) é um serviço da AWS que ajuda a controlar quem está autenticado (assinado) e autorizado (tem permissões) para usar os recursos da AWS.

Aqui estão os principais pontos sobre o IAM:

1. **Controle Granular de Acesso a AWS**: Com o IAM, você pode criar usuários, grupos, papéis e políticas de permissão para controlar o acesso aos serviços e recursos da AWS de uma maneira granular. Por exemplo, você pode permitir que um usuário tenha acesso somente leitura ao Amazon S3 e acesso total ao EC2.
2. **Compartilhamento Seguro de Acesso**: O IAM permite compartilhar o acesso à sua conta AWS de maneira segura. Em vez de compartilhar suas credenciais de root, você pode criar vários usuários IAM, cada um com suas próprias credenciais e permissões.
3. **Identidade Federada**: Com o IAM, você também pode permitir usuários que já tenham senhas em outros lugares, como na sua rede corporativa ou em um provedor de identidade baseado em SAML, a obter acesso temporário à sua conta AWS.
4. **Compatível com Multi-Fator Authentication (MFA)**: O IAM é compatível com a autenticação de vários fatores para fornecer uma camada adicional de proteção de segurança ao gerenciar o acesso aos serviços e recursos da AWS.
5. **Integrado com AWS Services**: O IAM está integrado com todos os serviços da AWS, o que significa que você pode definir permissões para qualquer serviço que desejar.
6. **Auditoria com AWS CloudTrail**: Com o AWS CloudTrail, você pode registrar todas as ações de usuários e APIs IAM para fins de auditoria.
7. **Gratuito**: O IAM é um recurso gratuito da AWS; você só paga pelos outros recursos da AWS que seus usuários acessam.

Em suma, o AWS IAM é um serviço de segurança crítico que ajuda a proteger o acesso aos recursos da AWS, permitindo que você controle quem pode fazer o quê em sua conta AWS.