Conceitos gerais de IAM

O AWS Identity and Access Management (IAM) é um serviço da web que ajuda você a controlar com segurança o acesso aos recursos da AWS.

Você usa o IAM para controlar quem está autenticado (conectado) e autorizado (tem permissões) para usar recursos.

O IAM facilita o fornecimento de acesso seguro a vários usuários aos recursos da AWS.

Ao criar uma conta da AWS pela primeira vez, você começa com uma identidade de login único que tem acesso completo a todos os serviços e recursos da AWS na conta.

Essa identidade é chamada de usuário raiz da conta da AWS e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta.

O IAM pode ser usado para gerenciar:

- Comercial.
- Grupos.
- Políticas de acesso.
- Funções.
- As credenciais do usuário.
- Políticas de senha do usuário.
- Autenticação multifator (MFA).
- Chaves de API para acesso programático (CLI).

O IAM fornece os seguintes recursos:

- Acesso compartilhado à sua conta da AWS.
- Permissões granulares.
- Acesso seguro aos recursos da AWS para aplicativos executados no Amazon EC2.
- Autenticação multifator.
- Federação de identidade.
- Informações de identidade para garantia.
- Conformidade com PCI-DSS.
- Integrado com muitos serviços da AWS.
- Eventualmente consistente.
- Livre para usar.

Por padrão, novos usuários são criados SEM acesso a nenhum serviço da AWS – eles só podem fazer login no console da AWS.

A permissão deve ser concedida explicitamente para permitir que um usuário acesse um serviço da AWS.

Os usuários do IAM são indivíduos que receberam acesso a uma conta da AWS.

Cada usuário do IAM tem três componentes principais:

- Um nome de usuário.
- Uma senha.
- Permissões para acessar vários recursos.

Você pode aplicar permissões granulares com o IAM.

Você pode atribuir aos usuários credenciais de segurança individuais, como chaves de acesso, senhas e dispositivos de autenticação multifator.

O IAM não é usado para autenticação no nível do aplicativo.

A Federação de Identidade (incluindo AD, Facebook etc.) pode ser configurada para permitir acesso seguro a recursos em uma conta da AWS sem criar uma conta de usuário do IAM.

A autenticação multifator (MFA) pode ser habilitada/imposta para a conta da AWS e para usuários individuais na conta.

A MFA usa um dispositivo de autenticação que gera continuamente códigos de autenticação aleatórios de seis dígitos e de uso único.

Você pode autenticar usando um dispositivo MFA das duas maneiras a seguir:

- Por meio do Console de gerenciamento da AWS – o usuário é solicitado a fornecer um nome de usuário, senha e código de autenticação.
- Usando a API da AWS – as restrições são adicionadas às políticas do IAM e os desenvolvedores podem solicitar credenciais de segurança temporárias e passar parâmetros de MFA em suas solicitações de API do AWS STS.
- Usar a AWS CLI obtendo credenciais de segurança temporárias do STS (aws sts get-session-token).

É uma prática recomendada sempre configurar a autenticação multifator na conta root.

O IAM é universal (global) e não se aplica a regiões.

O IAM replica dados em vários data centers em todo o mundo.

A “conta raiz” é a conta criada quando você configura a conta da AWS. Tem acesso de administrador completo e é a única conta que tem esse acesso por padrão.

É uma prática recomendada evitar usar a conta root para qualquer outra coisa que não seja cobrança.

O acesso de usuário avançado permite todas as permissões, exceto o gerenciamento de grupos e usuários no IAM.

As credenciais de segurança temporárias consistem no ID da chave de acesso da AWS, na chave de acesso secreta e no token de segurança.

O IAM pode atribuir credenciais de segurança temporárias para fornecer aos usuários acesso temporário a serviços/recursos.

Para entrar, você deve fornecer o ID da sua conta ou o alias da conta, além de um nome de usuário e senha.

O URL de login inclui o ID da conta ou o alias da conta, por exemplo:

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

Como alternativa, você pode fazer login no seguinte URL e inserir o ID ou o alias da sua conta manualmente:

https://console.aws.amazon.com/ (https://console.aws.amazon.com/)

O IAM se integra a muitos serviços diferentes da AWS.

Métodos de autenticação

Senha do console: (password + mfa) usado para AWS Management Console

- Uma senha que o usuário pode inserir para fazer login em sessões interativas, como o Console de gerenciamento da AWS.
- Você pode permitir que os usuários alterem suas próprias senhas.
- Você pode permitir que usuários selecionados do IAM alterem suas senhas desativando a opção para todos os usuários e usando uma política do IAM para conceder permissões aos usuários selecionados.

Chaves de acesso: (accesskeys [access key ID + Secret access key]) CLI e API

- Uma combinação de um ID de chave de acesso e uma chave de acesso secreta.
- Você pode atribuir duas teclas de acesso ativas a um usuário por vez.
- Eles podem ser usados para fazer chamadas programáticas para a AWS ao usar a API no código do programa ou em um prompt de comando ao usar a AWS CLI ou as ferramentas AWS PowerShell .
- Você pode criar, modificar, visualizar ou girar chaves de acesso.
- Quando criado, o IAM retorna o ID da chave de acesso e a chave de acesso secreta.
- O acesso secreto é retornado apenas no momento da criação e, se perdido, uma nova chave deve ser criada.
- Certifique-se de que as chaves de acesso e as chaves de acesso secretas sejam armazenadas com segurança.
- Os usuários podem ter acesso para alterar suas próprias chaves por meio da política do IAM (não do console).
- Você pode desabilitar a chave de acesso de um usuário, o que impede que ela seja usada para chamadas de API.

Certificados do servidor: (SSL/TLS usado para autentiar alguns serviços da AWS)

- Certificados SSL/TLS que você pode usar para autenticar com alguns serviços da AWS.
- A AWS recomenda que você use o AWS Certificate Manager (ACM) para provisionar, gerenciar e implantar seus certificados de servidor.
- Use o IAM somente quando precisar dar suporte a conexões HTTPS em uma região que não seja compatível com o ACM.

Usuários do IAM

Um usuário do IAM é uma entidade que representa uma pessoa ou serviço.

Pode ser atribuído:

- Um ID de chave de acesso e uma chave de acesso secreta para acesso programático à API, CLI, SDK e outras ferramentas de desenvolvimento da AWS.
- Uma senha para acesso ao console de gerenciamento.

Por padrão, os usuários não podem acessar nada em sua conta.

As credenciais do usuário root da conta são o endereço de e-mail usado para criar a conta e uma senha.

A conta root tem permissões administrativas totais e elas não podem ser restringidas.

Prática recomendada para contas root:

- Não use as credenciais do usuário root.
- Não compartilhe as credenciais do usuário root.
- Crie um usuário do IAM e atribua permissões administrativas conforme necessário.
- Ativar MFA.

Os usuários do IAM podem ser criados para representar aplicativos e são conhecidos como “contas de serviço”.

Você pode ter até 5.000 usuários por conta da AWS.

Cada conta de usuário tem um nome amigável e um ARN que identifica exclusivamente o usuário na AWS.

Também é criado um ID exclusivo que é retornado somente quando você cria o usuário usando a API, Tools for Windows PowerShell ou a AWS CLI.

Você deve criar contas individuais do IAM para usuários (prática recomendada para não compartilhar contas).

O ID da chave de acesso e a chave de acesso secreta não são iguais a uma senha e não podem ser usados para fazer login no console da AWS.

A ID da chave de acesso e a chave de acesso secreta só podem ser usadas uma vez e devem ser regeneradas se forem perdidas.

Uma política de senha pode ser definida para impor o comprimento da senha, complexidade etc. (aplica-se a todos os usuários).

Você pode permitir ou não a capacidade de alterar senhas usando uma política do IAM.

As chaves de acesso e as senhas devem ser alteradas regularmente.

Grupos

Grupos são coleções de usuários e têm políticas anexadas a eles.

Um grupo não é uma identidade e não pode ser identificado como principal em uma política do IAM.

Use grupos para atribuir permissões aos usuários.

Use o princípio de privilégio mínimo ao atribuir permissões.

Você não pode aninhar grupos (grupos dentro de grupos).

Roles (funções)

As funções são criadas e então “assumidas” por entidades confiáveis e definem um conjunto de permissões para fazer solicitações de serviço da AWS.

Com as funções do IAM, você pode delegar permissões a recursos para usuários e serviços sem usar credenciais permanentes (por exemplo, nome de usuário e senha).

Os usuários do IAM ou os serviços da AWS podem assumir uma função para obter credenciais de segurança temporárias que podem ser usadas para fazer chamadas de API da AWS.

Você pode delegar usando funções.

Não há credenciais associadas a uma função (senha ou chaves de acesso).

Os usuários do IAM podem assumir temporariamente uma função para obter permissões para uma tarefa específica.

Uma função pode ser atribuída a um usuário federado que entra usando um provedor de identidade externo.

As credenciais temporárias são usadas principalmente com funções do IAM e expiram automaticamente.

As funções podem ser assumidas temporariamente por meio do console ou programaticamente com a AWS CLI , Tools for Windows PowerShell ou API.

Funções do IAM com instâncias do EC2:

- As funções do IAM podem ser usadas para conceder permissões de aplicativos executados em instâncias do EC2 para solicitações de API da AWS usando perfis de instância.
- Apenas uma função pode ser atribuída a uma instância do EC2 por vez.
- Uma função pode ser atribuída no momento da criação da instância do EC2 ou a qualquer momento posterior.
- Ao usar a AWS CLI ou os perfis de instância de API devem ser criados manualmente (é automático e transparente por meio do console).
- Os aplicativos recuperam credenciais de segurança temporárias dos metadados da instância.

Delegação de função:

- Crie uma função do IAM com duas políticas:
  - Política de permissões – concede ao usuário da função as permissões necessárias em um recurso.
  - Política de confiança – especifica as contas confiáveis que têm permissão para assumir a função.
- Curingas (*) não podem ser especificados como principal.
- Uma política de permissões também deve ser anexada ao usuário na conta confiável.

Políticas

Políticas são documentos que definem permissões e podem ser aplicadas a usuários, grupos e funções.

Os documentos de política são escritos em JSON (par chave-valor que consiste em um atributo e um valor).

Todas as permissões são negadas implicitamente por padrão.

A política mais restritiva é aplicada.

O simulador de políticas do IAM é uma ferramenta para ajudá-lo a entender, testar e validar os efeitos das políticas de controle de acesso.

O elemento Condition pode ser usado para aplicar lógica condicional adicional.

STS

O AWS Security Token Service (STS) é um serviço da web que permite solicitar credenciais temporárias com privilégios limitados para usuários do IAM ou para usuários que você autentica (usuários federados).

As credenciais de segurança temporárias funcionam de maneira quase idêntica às credenciais de chave de acesso de longo prazo que os usuários do IAM podem usar

Práticas recomendadas de IAM

Bloqueie as chaves de acesso do usuário root da AWS.

Crie usuários individuais do IAM.

Use as políticas definidas pela AWS para atribuir permissões sempre que possível.

Use grupos para atribuir permissões a usuários do IAM.

Conceda o mínimo de privilégio.

Use os níveis de acesso para revisar as permissões do IAM.

Configure uma política de senha forte para usuários.

Ativar MFA.

Use funções para aplicativos executados em instâncias do AWS EC2.

Delegue usando funções em vez de compartilhar credenciais.

Gire as credenciais regularmente.

Remova credenciais desnecessárias.

Use as condições da política para segurança extra.

Monitore a atividade em sua conta da AWS.

Access Adivisor

Fornece informações sobre quando os usuários e funções ddo IAM tentaram acessar os serviços da AWS pela última vez