AWSクラウド演習

AWSクラウド演習講義資料

I AM(AWS IDENTITY AND ACCESS MANAGEMENT)

- I AM(AWS Identitiy and Access Manegemetn)とは

  AWSにおける認証・認可の仕組みのことです。各サービスへの制御することで安全にAWSを操作することができます。IAMではユーザーだけでなく、リソースに対しても設定することができます。

  IAM を使用すると、**ユーザー**、アクセスキーなどの**セキュリティ認証情報**、ユーザーがアクセスできるAWSリソースを制御する**アクセス許可**を一元管理できます。

- IAMの主要な項目

  IAMの主要な項目として**ユーザー、グループ、ポリシー、ロール**の4つがあります。

IAMユーザー

- ユーザーの種類

  AWSでのユーザーにはルートユーザーとIAMユーザーの2つがあります。

- ルートユーザー(ルートアカウント)

  すべてのリソースにアクセスできる**完全な権限**を持つユーザー。AWSとの契約した最初に作成されるユーザーです。AWSアカウントの停止などルートユーザーにのみ許可されているもがあり、一般的に**作業する時は使用しないユーザー**です。

- IAMユーザー

  最小の権限を持つユーザー。設定された**ポリシー**に従いリソースにアクセスできます。5000ユーザーまで作成可能。

IAMユーザー(認証)

- 認証の方法は次のようなものがあります。
  デフォルトでは承認は**暗黙の拒否**になります。

- MFA(Multi-Factor Authentication)
  物理デバイスなどを利用した認証方式です。2段階認証などが該当します。

- STS(Security Token Service)
  トークンサービスのこと。動的にIAMユーザーを作成し、一時的にトークンを発行します。Webサービスなどで利用されます。

- その他(アクセスキーID/シークレットアクセスキー、X.509 Certificate)

IAMグループ

- IAMグループ

  同じアクセス権限を持つグループのこと。作成したIAMユーザーをグループに追加することで同じ権限を持たせることができます。グループの作成は100まで可能。
  グループを他のグループへは追加することはできません。

- IAMグループへの登録手順

  ＊IAMユーザーを参加させるIAMグループは事前に作成しておいてください。

  ①IAMユーザーの作成

  ②IAMグループへ登録

IAMポリシー

- IAMポリシーとは

  IAMユーザーやグループなどへ**付与する権限**のことです。IAMユーザーは割り当てられたポリシーで許可されたサービスのみ使用できます(誰にどのAWSのサービスを使用させるか定義したもの)。ポリシーはログインからログアウトするまで有効です。ポリシーの種類は管理ポリシーとインラインポリシーがあります。ポリシーはユーザーだけでなく**リソースに対しても適用**することができます。

- 管理ポリシー

  AWSが提供しているポリシーです。多くのポリシーがAWSにより提供されています。

- インラインポリシー

  ユーザー自身が作成するポリシーです。

IAMロール(役割)

- IAMロール(役割)とは

  ポリシーをグループ化したもの。**一時的なアクセス権限を与えたい時などに使用します。**また、リソースに対しても設定ができます(あるプログラムが動く時にあるロールを使用するなど)。

  <例>

  あるEC2のみ特定のS3にアクセスすることができる。

  あるプログラムの中でのみS3にアクセスことができる。

- ロールを使用した場合

  ロールを使用した時にポリシーの権限はなくなります。