IAM

概要

設計

ポリシー適用

クロスアカウント

アクセスアナライザ

Organizationsの概要

Organizationsの設定

概要

AWS　identity access management

AWS利用者認証実施

Accessポリシー

個人またはグループにポリシーを適用

主要トピック

IAMユーザ

IAMポリシーを割り当てられたユーザ

エンティティ

・ルートアカウント（IAMではない）

ルートのメアドやPASS設定

課金情報アクセス  
 Route53のドメイン登録

逆引きDNS設定　など

・管理者権限

・パワーユーザ　IAM以外のサービスにフルアクセス権がある

IAMグループ

作ってユーザを入れていくのが使い方の基本

IAMポリシー

JSON形式で設定される

アクセス権限

Effect　 ・・・　Allow許可 Deny拒否

Action ・・・　対象のＡＷＳサービス　例“S3.Get“

Resouce ・・・ 対象のAWＳリソース　ARNで記述

Condition・・・　アクセス制御が有効となる条件(IPアドレスなど)

IAＭロール

ＡＷＳのリソース間でのアクセス権限設定

認証方式

アクセスキー　シークレットアクセスキー

ＣＬＩやＡＰＩ利用時

ＥＣ２インスタンス接続などＲＥＳＴ/Ｑｕｅｒｙ方式

X.509

使わない

ＡＷＳマネジメントコンソールへのアクセス

ＭＦＡ

ワンタイムパスワードなどを追加で要求できる

アクティビティの記録

ＩＡＭアクセスアナライザ

不正なアクセスを特定

AccessAdviserのServiceLastAccessData

IAＭエンティティが最後にＡＷＳサービスにアクセスした日付と時刻を

表示する機能

Credentinal Report

利用日時などが記録されているレポートファイル

AWS　Config

IAMのユーザ、グループ、ポリシー、ロールの変更履歴

構成変更を確認することが出来る機能

AWS　Cloud　Trail

AWSインフラストラクチャー全体のログを監視して保持する機能

ベストプラクティスにのっとってIAMを利用していこう！！！

IAM設計

AWS利用組織　　セキュリティポリシー

↓　　　　　　↓

自社に最適な設計

少数利用のみIAMユーザを使う程度がユースケース

中規模以上は絶対にグループ推奨

①AWS利用者と役割の洗い出し

AWS利用者の特定

利用者の役割と利用範囲を整理

②利用グループへと集約

同じ役割や利用範囲をまとめる

グループ別の名称と最小限利用範囲を確定すること

**ケーススタディ**

IT管理者 フルアクセス管理者権限　MFA必須

運用管理者 運用ツール全般 開発環境のアクセスを付与してDevOpsに参加可能

アプリ開発 担当しているアプリの開発範囲でのみアクセス権限を付与

IT管理者　 管理ポリシー　Administrator

運用管理者 ELB・EC2・RDS・S3・Auto-Scaling・VPC

Config・Trail・Cloud Watch

アプリ開発者　　ELB・EC2・RDS・Auto-Scaling・VPC

IDプロバイダ　フェデレーションアクセス

オンプレミスのパスとIDを連携させて外部サービスと連携する

STS　一時的な認証とパスワードポリシーを確認可能

アクセス管理

アクセスアナライザ

作成すると不正なアクセスを分析してくれる

認証情報レポート

資格情報などがレポートに保存されている

組織アクティビティ

AWS　Organizations使用

SCP

AWS　Organizationsで使用

ポリシー

インライン　・　ユーザ定義　・ＡＷＳ側が提供

ユーザのポリシー

サービス

アクション　　細かい設定したいならすべて展開して行う

例：タグ作成は可能　削除は不可能など

アプリ開発者用

なぜかEC2の利用の中にVPCが入っている

ロール設計

ロール向けポリシー作成

バッチ処理　API連携　などのリソース権限を割り当てる

EC２がS3にバッチ処理のアクセス権限を振る

IAMロールの権限移譲

信頼ポリシー

権限を委譲

IAMロールの権限操作

エンティティに権限を与える

対象

出来ること

アカウントAのマネージメントコンソールにアカウントBがアクセスする

権限移譲の際に覚えておくこと

ロール名

ARN　（アマゾンリソースネーム）

対象アカウントID

AWＳ　Organizations

複数accountの統合管理

IAMのアクセス管理を大きな組織で管理する

出来ること

・複数アカウントの一元管理

・新規アカウント作成の自動化

・一括請求

マスターアカウントが別アカウントに招待

メンバーアカウントとして登録

OU（組織単位）

SCPを設定する

機能

支払一括代行のみ

アカウントの全体管理

SCPはIAMポリシーとほぼ同じ

境界設定のみ適用はされない

SCP設定　→　アタッチ

OUの範囲を設定