AWS無料オンラインテックセミナー
～AWSの権限管理を楽々一元管理
―

2021/10/07

株式会社オープントーン
ITエンジニアリング事業部 / 山岸 徹

目次

- 自己紹介
- 概要
- IAMロールとは
- IAMロールの活用事例
- まとめ
- 質疑応答

自己紹介

自己紹介

- 株式会社オープントーン
- ITエンジニアリング事業部 / 山岸 徹
- 得意な言語
  - Java
    - 最近はPHPも少々
- 最近の動向
  - 主にサーバーサイドの実装
  - AWSを使ったインフラ構築 / 運用 / 管理
  - Vue.js や nuxtを通してフロントエンジニアとしてのスキルを勉強中
- 趣味
  - ゲーム(モンスターハンター、JRPC)
    - 最近「Ghost of Tsushima」をクリア

概要

概要

AWSチームメンバーが、複数AWSアカウント管理をIAMロールを使って手間なく管理できるようにした事例を紹介しようと思います

IAMロールとは

IAMロールとは

IAMロールとは

- “IAM ロールは、特定のアクセス権限を持ち、アカウントで作成できる IAM アイデンティティです。IAM ロールは、**AWSで許可/禁止する操作を決めるアクセス権限ポリシーが関連付けられている**。AWS アイデンティティであるという点で、**IAM ユーザーと似ています**”
- “ロールを使用して、通常は AWS リソースへのアクセス権のないユーザー、アプリケーション、サービスにその**アクセス権を委任できます**”

このように記載されています。

※以降、原則ロール＝IAMロール、ユーザー＝IAMユーザーと表記する

引用：https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles.html

IAMロールとIAMユーザーの違い

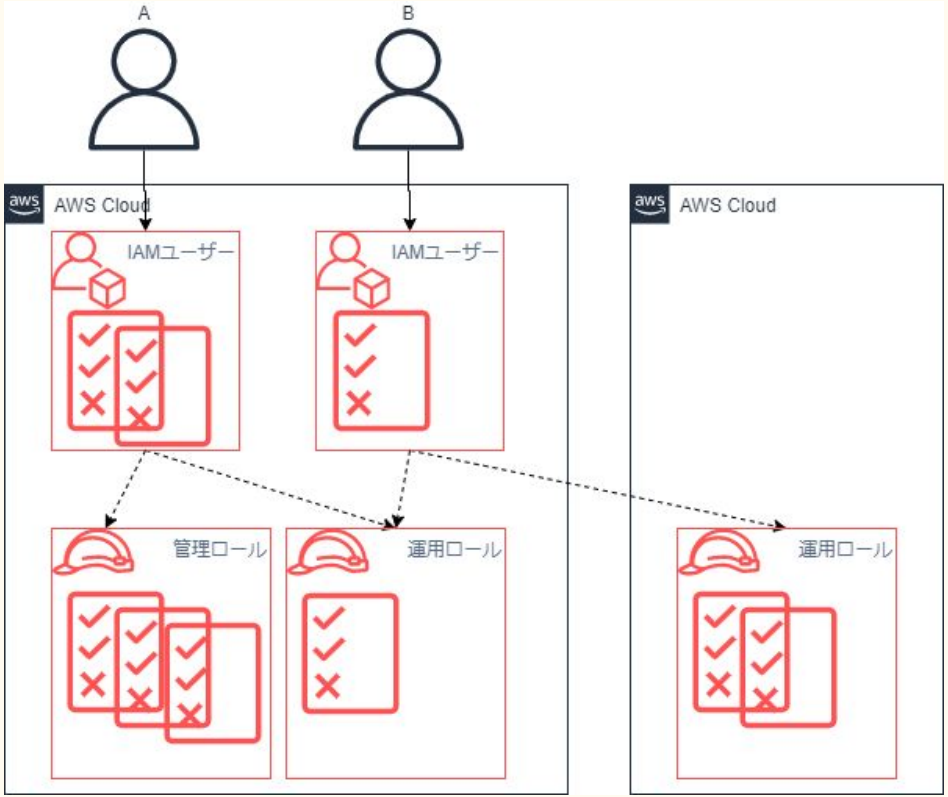
ロール

- 任意の人(サービス)に権限を 委任 することができる
    - 人以外のサービスやEC2などにも委任することができる
- 標準の長期認証情報 (パスワードやアクセスキーなど)を持たない
- 別のAWSアカウントにも委任できる

ユーザー

- ユーザーは一人の人に一意に関連付けられる
- 標準の長期認証情報 (パスワードやアクセスキーなど)を持っている

ユーザーとロールの関係図



- Aさんとユーザーは1:1で関連
- Aさんのユーザーは幾つかあるロールの1つを引き受けることができる
- Bさんは別AWSアカウントのロールを委任され引き受けることができる
- ロールはユーザーと直接関連していない
- ユーザーはどんなロールがあるか把握している必要があり、またロールを引き受けることを委任されている必要がある

IAMロールの活用事例

～AWSの権限管理を楽々一元管理

弊社におけるAWSアカウントの扱い

- 弊社ではAWSアカウントを案件や環境ごとに分けて運用している
- 社内で利用するAWSアカウントをシステム運用とは別にAWSチームが正常に運用されているか管理しています
- AWSチームに所属するメンバーは現在5名
- AWSチームのメンバーがAWSアカウントを作成しシステム管理者に受け渡す
- 同じ案件でも環境が違うとAWSアカウントも別なこともあるので、AWSアカウントはどんどん増えている
- システム管理者とアカウント管理者は別であることが多い

AWSアカウントが増えることの問題点

1. AWSチームメンバー全員がすべてのAWSアカウントにアクセスする必要があるため、アカウントごとにメンバー全員のIAMユーザーを作成/削除すると手間である
    - システム管理者からするとシステム運用に直接関係ないリソースは極力排除したい
2. AWSチームメンバーはすべてのAWSアカウントのサインイン情報（ユーザー名、パスワード）を個別に管理する必要がある

問題の解決方法

スイッチロールという方法で解決しました

簡単に説明すると

- 管理される側
  - 管理に必要な権限を持ったロールを 1つだけ作成し管理する側に委任する
- 管理する側
  - IAMユーザーがロールを引き受けれるように設定する
  - 管理が必要なときに **スイッチロール** を行い、管理される側のアカウントを管理する

解決された問題1

1. AWSチームメンバー全員がすべてのAWSアカウントにアクセスする必要があるため、アカウントごとにメンバー全員のIAMユーザーを作成/削除すると手間である

- 管理される側にロールを1つだけ作成するだけでよい
  - CFnテンプレート化してロール作成の手間も軽減

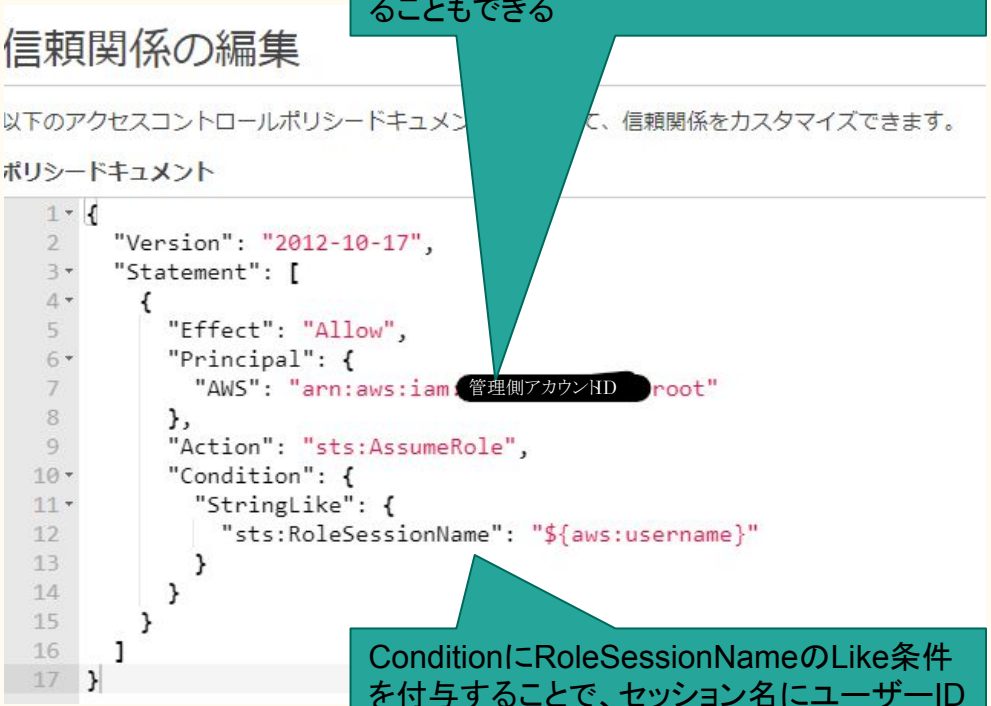
解決された問題2

2. AWSチームメンバーはすべてのAWSアカウントのサインイン情報（ユーザー名、パスワード）を個別に管理する必要がある

- 管理する側のアカウントのユーザーだけ管理すればよい
- ユーザーを管理する側のアカウントに一元管理できる

設定方法 - 管理される側

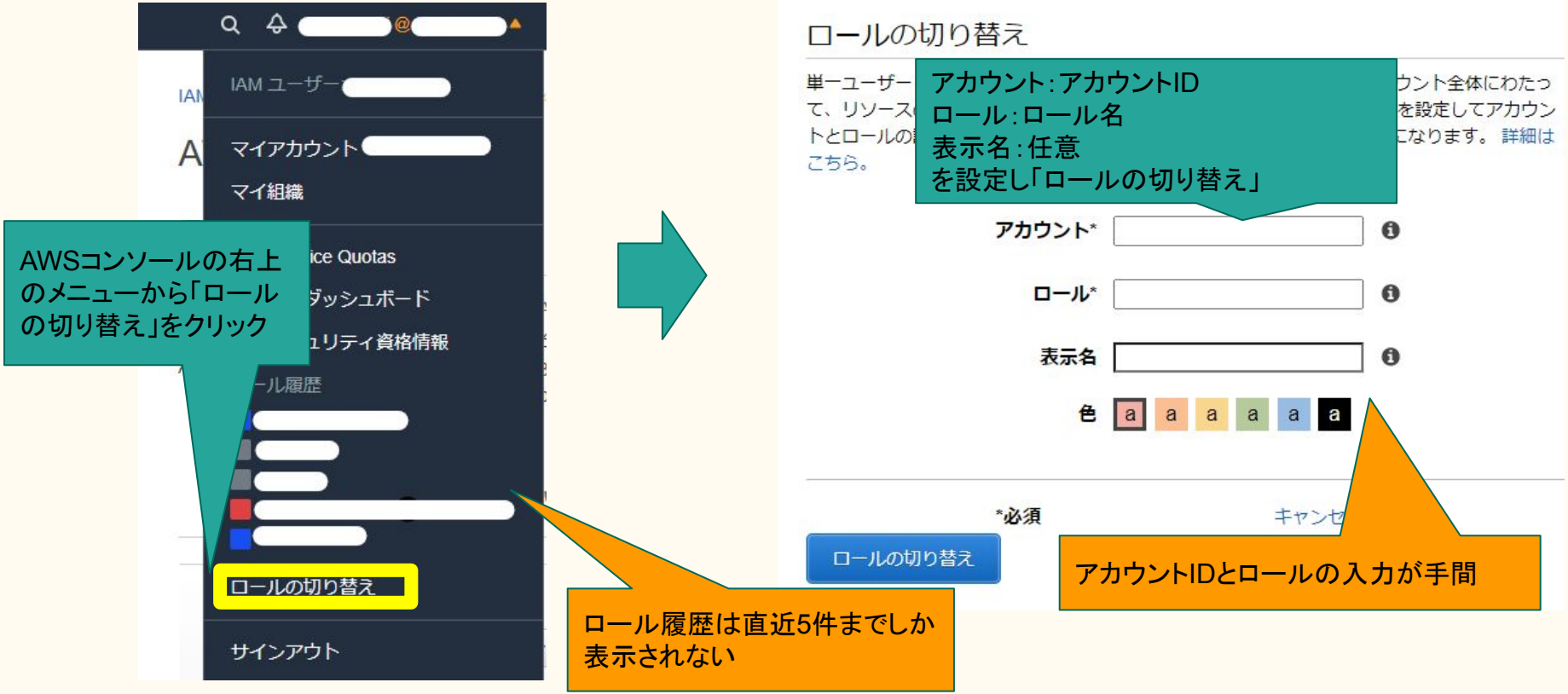
- AWSアカウント作成し引き渡す前にロールを作成します
- ロール名は「admin-role」などすべてのAWSアカウントで統一しておくと管理が楽です
- ロールの信頼関係には右のように設定します



設定方法 - 管理する側

- スイッチさせたいユーザーにポリシーを設定する
- このとき同時にIAMポリシー「AdministratorAccess」を関連付けていると、すべてのリソースにアクセスできてしまうので、このポリシーは意味がなくなるので注意

スイッチロールの方法


IAM ユーザー
マイアカウント
マイ組織
ロールの切り替え
サインアウト
AWSコンソールの右上のメニューから「ロールの切り替え」をクリック
ロール履歴は直近5件までしか表示されない
ロールの切り替え
単一ユーザー
て、リソース
トとロールの
こちら。
ウント全体にわたっ
を設定してアカウン
になります。 詳細は
アカウント:アカウントID
ロール:ロール名
表示名:任意
を設定し「ロールの切り替え」
アカウント*
ロール*
表示名
色
*必須
ロールの切り替え
アカウントIDとロールの入力が手間

スイッチロール後

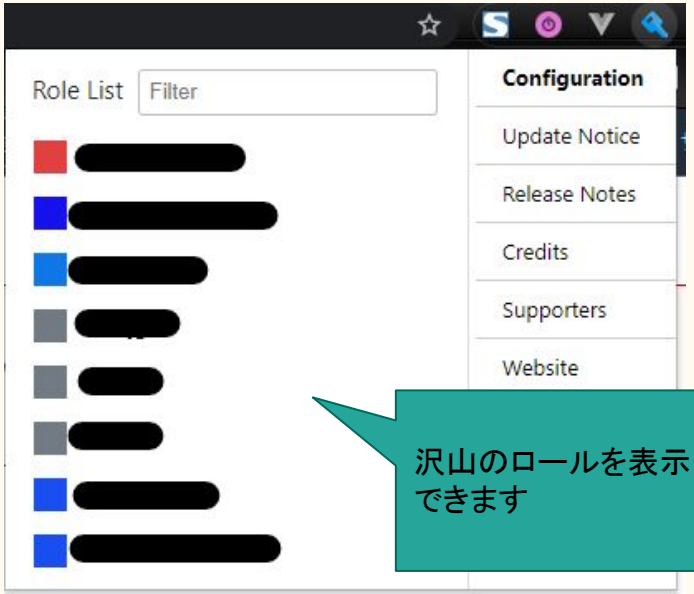
スイッチロール中は
AWSコンソールの右上のメニューの表示は
- 左が管理する側
- 右が管理される側

の情報が表示されるようになります

AWS Extend Switch Roles

簡単にスイッチロールをChromeの機能拡張を使います

https://github.com/tilfinltd/aws-extend-switch-roles




```
[profile marketingadmin]
role_arn =
arn:aws:iam::123456789012:role/marketingadmin
color = ffaaee

[anotheraccount]
aws_account_id = 987654321987
role_name = anotherrole
region=ap-northeast-1

[athirdaccount]
aws_account_id = 987654321988
role_name = athirdrole
image = "https://via.placeholder.com/150"
```

設定はJSONなので、AWSチーム内で共有することでアカウントIDの管理を一元化できます

まとめ

- AWSアカウントを複数管理したいときは、管理される側にIAMユーザーを作成するのではなくIAMロールを作成することでアクセス管理の手間を大幅に削減できる
- スイッチロールを簡単にするためのChrome機能拡張がある(AWS Extend Switch Roles)

以上になります

質疑応答