Amazon EKS 2023 年 冬のアップデートを振り返ろう
～ EKS Pod Identity & Mountpoint for Amazon S3 CSI driver ～

2023/12/21

Kenta Goto

Amazon Web Services Japan G.K.
Solutions Architect

自己紹介

- 名前
  - 後藤 健汰（ Kenta Goto ）
- 所属
  - ISV/SaaS Solutions Architect
- 好きな AWS サービス
  - Amazon EKS
- 趣味
  - サウナ

X@kennygt51

Agenda

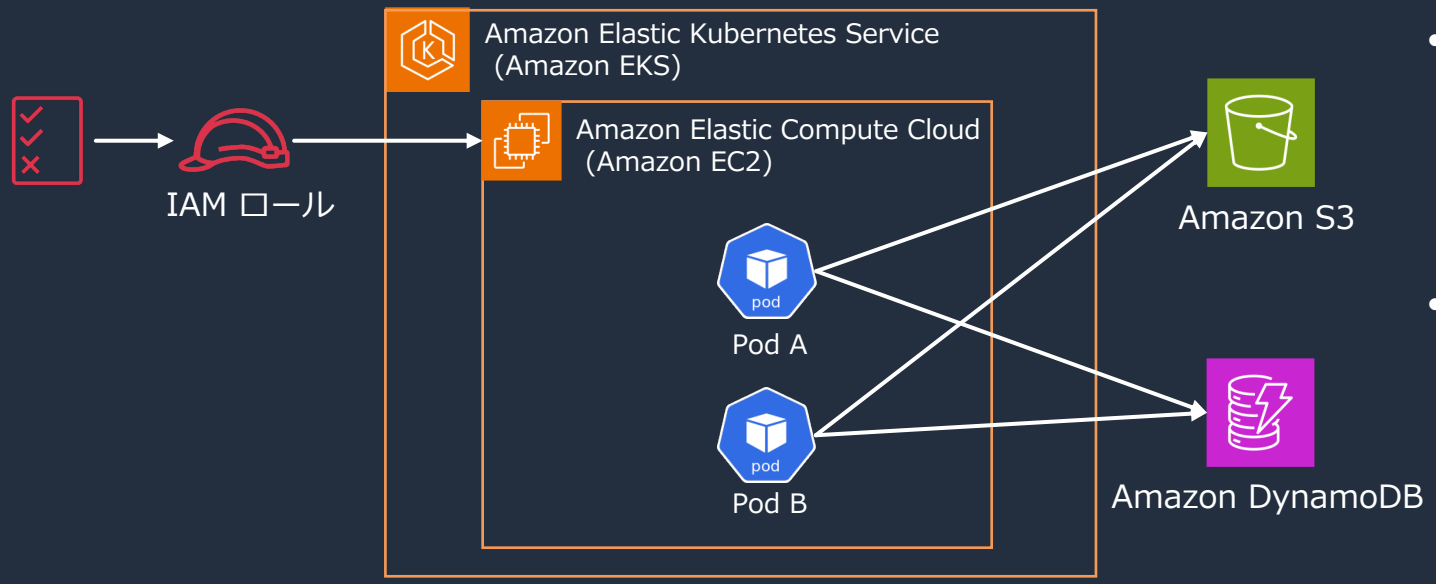
- EKS Pod Identity
- Mountpoint for Amazon S3 CSI driver
- まとめ

Agenda

- EKS Pod Identity
- Mountpoint for Amazon S3 CSI driver
- まとめ

Pod 単位での IAM ロールの割り当て

- 2019 年 9 月以前、Pod 単位での IAM ロールの割り当ては未サポート (※)
  - Worker Node (Amazon EC2) にアタッチされた IAM ロールに対して、Pod が必要とするポリシーを付与する必要があった
  - 最小権限の原則を守ることが困難だった

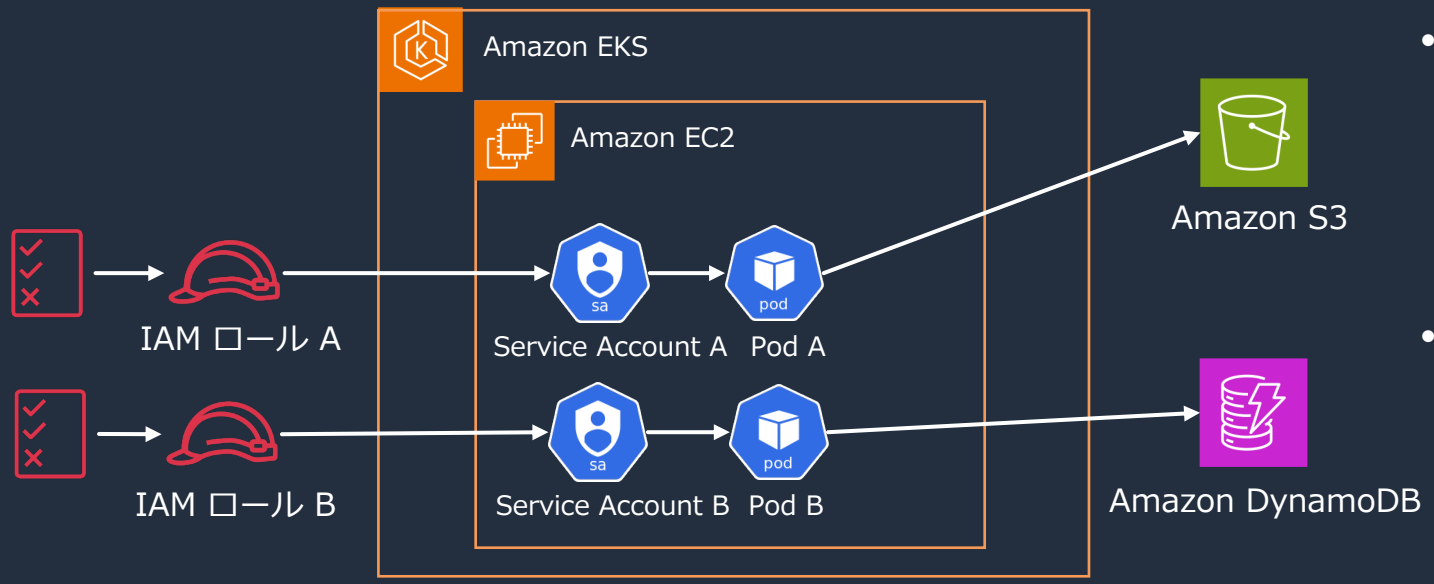


- Pod A には Amazon Simple Storage Service (Amazon S3)、Pod B には Amazon DynamoDB へのアクセスを許可したい場合
- Pod 単位での IAM ロールの割り当てが未サポートだったため、同一 Woker Node で起動している別の Pod にも権限が付与されてしまう

※ OSS ソリューションを活用することで実現は可能だった

IAM Roles for Service Accounts (IRSA) の登場

- 2019 年 9 月、 IAM Roles for Service Accounts (IRSA) がリリース (※)
  - Kubernetes ServiceAccount に IAM ロールを紐付ける機能
  - Pod 単位でのきめ細やかな AWS リソースへのアクセス制御を実現

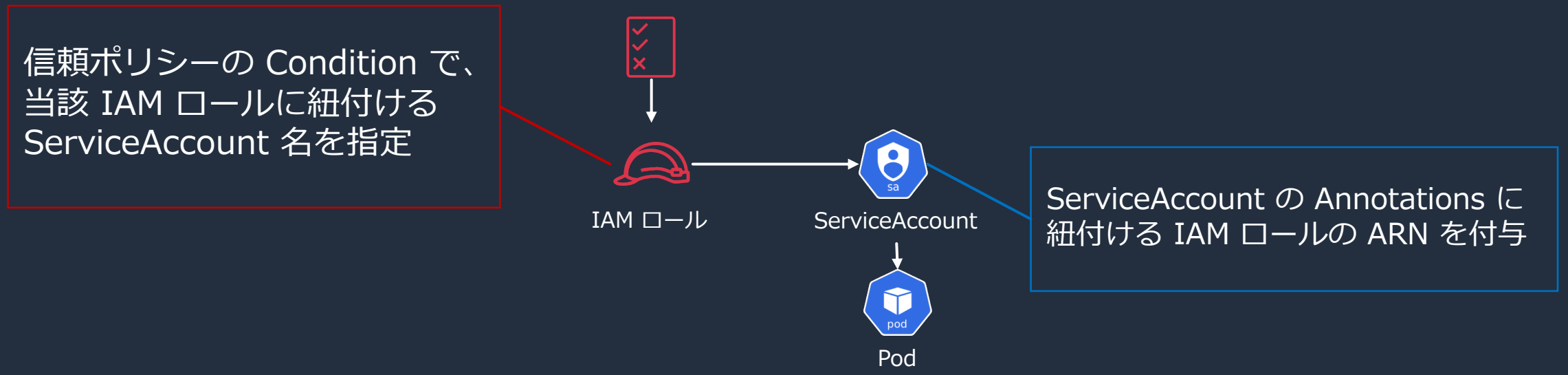


- ServiceAccount に IAM ロールを紐づけ、Pod spec で ServiceAccount を指定する
- 最小権限の原則に基づいて、適切なアクセス権限の付与を実現

※ https://aws.amazon.com/blogs/opensource/introducing-fine-grained-iam-roles-service-accounts/

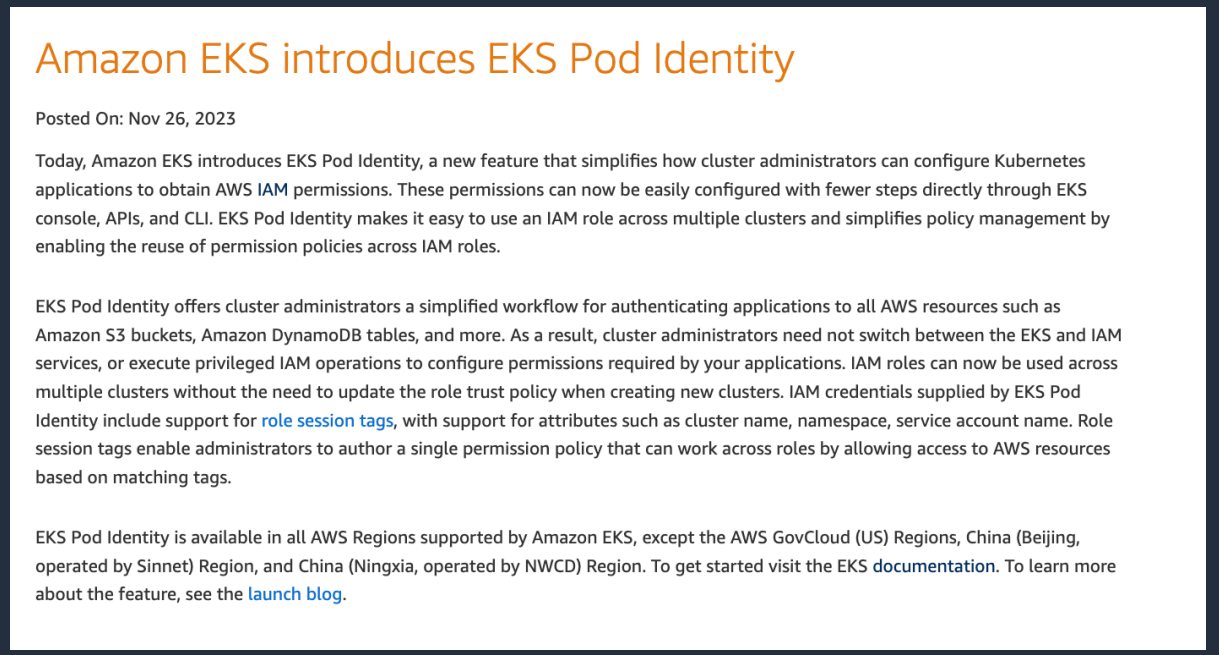
IAM Roles for Service Accounts (IRSA) の設定方法

- ユーザーが利用するには、以下のステップで設定を行う
  1. 紐付ける IAM ロールにおける信頼ポリシーの Condition に、紐づけ先の ServiceAccount 名を指定
  2. Kubernetes ServiceAccount に Annotations を追加
- Kubernetes リソースと AWS リソースの両方を編集する必要があった



EKS Pod Identity の登場

- 2023 年 11 月、EKS Pod Identity がリリース
  - IRSA と同様に、Kubernetes ServiceAccount に IAM ロールを紐付ける機能
  - 紐付けるための設定が簡素化



Amazon EKS introduces EKS Pod Identity

Posted On: Nov 26, 2023

Today, Amazon EKS introduces EKS Pod Identity, a new feature that simplifies how cluster administrators can configure Kubernetes applications to obtain AWS IAM permissions. These permissions can now be easily configured with fewer steps directly through EKS console, APIs, and CLI. EKS Pod Identity makes it easy to use an IAM role across multiple clusters and simplifies policy management by enabling the reuse of permission policies across IAM roles.

EKS Pod Identity offers cluster administrators a simplified workflow for authenticating applications to all AWS resources such as Amazon S3 buckets, Amazon DynamoDB tables, and more. As a result, cluster administrators need not switch between the EKS and IAM services, or execute privileged IAM operations to configure permissions required by your applications. IAM roles can now be used across multiple clusters without the need to update the role trust policy when creating new clusters. IAM credentials supplied by EKS Pod Identity include support for role session tags, with support for attributes such as cluster name, namespace, service account name. Role session tags enable administrators to author a single permission policy that can work across roles by allowing access to AWS resources based on matching tags.

EKS Pod Identity is available in all AWS Regions supported by Amazon EKS, except the AWS GovCloud (US) Regions, China (Beijing, operated by Sinnet) Region, and China (Ningxia, operated by NWCD) Region. To get started visit the EKS documentation. To learn more about the feature, see the launch blog.

https://aws.amazon.com/about-aws/whats-new/2023/11/amazon-eks-pod-identity/

EKS Pod Identity の利用手順

- EKS Pod Identity の利用手順
  1. EKS Add-ons から Amazon EKS Pod Identity エージェントを EKS クラスターにインストール
  2. IAM ロールを作成し、信頼ポリシーの Principal として *pods.eks.amazonaws.com* を指定
  3. コンソール、または AWS API を用いて、IAM ロールを ServiceAccount にマッピングする
- **AWS API のみで、Kubernetes ServiceAccount への IAM ロールの紐付けが完結**

EKS Pod Identity の考慮事項

- 考慮事項
  - Windows と AWS Fargate での利用は未サポート
  - EKS Pod Identity と IRSA は併用可能
  - IAM ロールにおける信頼ポリシーの設定により、特定の ServiceAccount、Namespace、EKS クラスターに対しのみ紐付けを許可するといった制御が可能

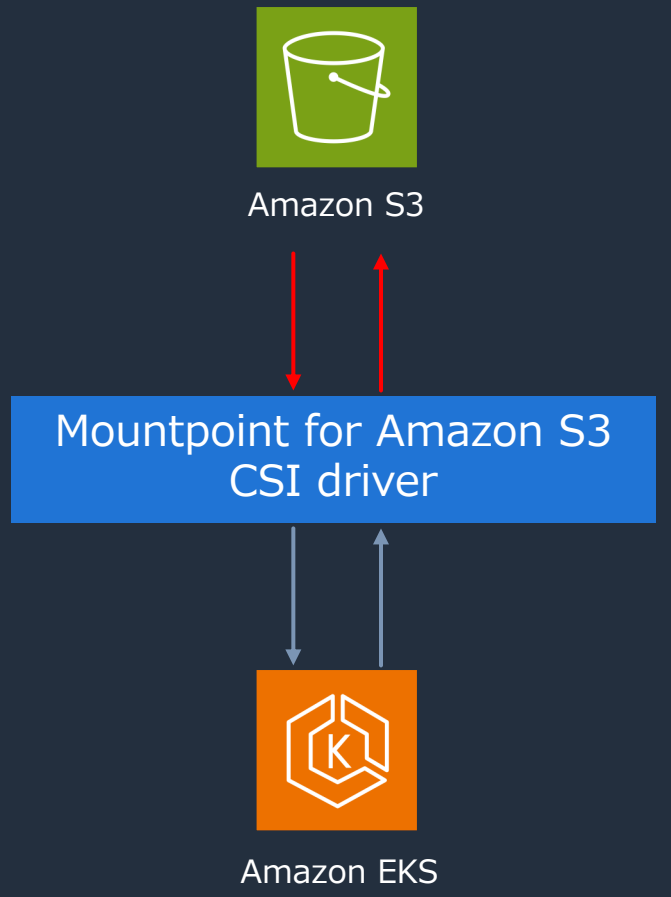
デモ

Agenda

- EKS Pod Identity
- Mountpoint for Amazon S3 CSI driver
- まとめ

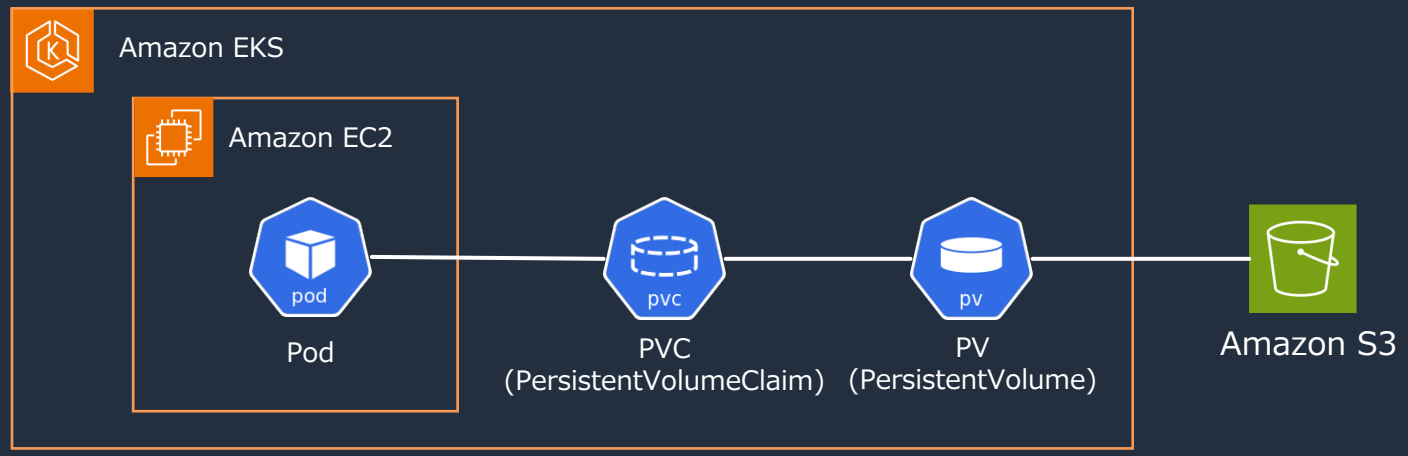
Mountpoint for Amazon S3 CSI driver

- 2023 年 8 月、S3 バケットをローカルファイルシステムとしてマウントするクライアントツール、Mountpoint for Amazon S3 が GA
- 2023 年 11 月、Container Storage Interface (CSI) に対応した Mountpoint for Amazon S3 CSI driver がリリース
- Kubernetes Pod から Amazon S3 内のオブジェクトに対して、ファイルシステムのインタフェースを介してのアクセスを実現



Mountpoint for Amazon S3 CSI driver の利用手順

- 利用手順
  1. EKS Add-on から Mountpoint for Amazon S3 CSI driver を導入
     - 事前に、必要な権限 (※) を付与した IAM ロールを作成しておく
  2. マウントする Amazon S3 バケットを作成
  3. PersistentVolume、PersistentVolumeClaim、Pod を作成



※ https://docs.aws.amazon.com/eks/latest/userguide/s3-csi.html#s3-create-iam-role

Mountpoint for Amazon S3 CSI driver の考慮事項

- 考慮事項
  - Windows、AWS Fargateでの利用は未サポート
  - 静的プロビジョニングのみをサポート
    - 動的プロビジョニング、つまり新しいバケットの作成は未サポート
  - すべての POSIX ファイル システム機能をサポートするわけではない点に注意
  - 2023 年 12 月現在、Mount point for Amazon S3 CSI driver に IAM ロールを割り当てる際には、IRSA を使用する必要がある

デモ

Agenda

- EKS Pod Identity
- Mountpoint for Amazon S3 CSI driver
- まとめ

まとめ

- EKS Pod Identity
  - ServiceAccount と IAM ロールの紐づけを簡素化する
  - コンソール、または AWS API で作業が完結する
  - 既存の仕組み (IRSA) とは併用が可能

- Mountpoint for Amazon S3 CSI driver
  - Amazon S3 バケットを Kubernetes Pod からマウント
  - EKS Add-on から簡単にインストールが可能

- ぜひ、お手元の環境で試してみてください

Thank you!