AWS SDK for PHPの認証情報管理

AWS Black Belt Online Seminar

Tomohiro Kamitani

Solutions Architect

2022/08

AWS Black Belt Online Seminarとは

- 「サービス別」「ソリューション別」「業種別」などのテーマに分け、アマゾン ウェブ サービス ジャパン合同会社が提供するオンラインセミナーシリーズです
- AWSの技術担当者が、AWSの各サービスやソリューションについてテーマごとに動画を公開します
- 動画を一時停止・スキップすることで、興味がある分野・項目だけの聴講も可能、スキマ時間の学習にもお役立ていただけます
- 以下のURLより、過去のセミナー含めた資料などをダウンロードすることができます
  - https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-service-cut/

内容についての注意点

- 本資料では2022年08月時点のサービス内容および価格についてご説明しています。最新の情報はAWS公式ウェブサイト(https://aws.amazon.com/)にてご確認ください
- 資料作成には十分注意しておりますが、資料内の価格とAWS公式ウェブサイト記載の価格に相違があった場合、AWS公式ウェブサイトの価格を優先とさせていただきます
- 価格は税抜表記となっています。日本居住者のお客様には別途消費税をご請求させていただきます

自己紹介

- 名前
  紙谷知弘 (かみたに ともひろ)

- 所属
  アマゾンウェブサービスジャパン株式会社
  技術統括本部
  エンタープライズ技術本部
  メディアソリューション部
  ソリューションアーキテクト

- 好きなAWSサービス

AWS SDK

AWS Cloud9

本セッションでお話しすること

1. AWS SDK for PHPでの認証情報設定の流れ
2. AWS SDK for PHPでの認証情報の設定パターン

AWS SDK for PHPと認証

SDKからAWS各種サービスにリクエストを行うには認証情報を提供する必要がある

AWS SDK for PHP 概要
https://www.youtube.com/watch?v=kU8dRwS4caw

認証情報の設定パターン

- デフォルトの認証情報プロバイダーチェーンを使用する**(推奨)**
- 特定の認証情報プロバイダー, プロバイダーチェーンを使用する
- 認証情報を自身で提供する

お客様のセキュリティのためにもルートアカウントではなく IAMユーザー/ロールをご利用いただくことを強くお勧めします。 (詳しくは[IAMのベストプラクティス]を参照)

デフォルトの認証情報プロバイダチェーン

デフォルトでは下記の順序で認証情報を使用します

1. 環境変数の認証情報を使用します

2. 共通の認証情報ファイルを利用します

3. IAMロールを継承します

```
$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE
```

```
[default]
aws_access_key_id = YOUR_AWS_ACCESS_KEY_ID
aws_secret_access_key = YOUR_AWS_SECRET_ACCESS_KEY
```

IAM Role

環境変数の認証情報を利用

```
# Linuxの場合

$ export AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

$ export AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

$ export AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of security token>
```

```
# Windowsの場合

C:¥> SET  AWS_ACCESS_KEY_ID=AKIAIOSFODNN7EXAMPLE

C:¥> SET  AWS_SECRET_ACCESS_KEY=wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

C:¥> SET AWS_SESSION_TOKEN=AQoDYXdzEJr...<remainder of security token>
```

- 環境変数に認証情報を含めることによって誤って認証情報を共有することを回避できます
- オンプレミスのサーバー、ローカル環境での利用時に用いると便利

認証ファイル 認証プロファイルを利用

- ホームディレクトリの.aws/配下のcredentialsファイルを利用する
- このファイルをAWS CLIなどで既に使用している場合は、何も変更することなく、SDKから利用できる

- 認証ファイル内に複数のprofileがある場合はクライアントをインスタンス化するときに指定可能

```
[default]
aws_access_key_id = YOUR_AWS_ACCESS_KEY_ID
aws_secret_access_key = YOUR_AWS_SECRET_ACCESS_KEY

[project1]
aws_access_key_id = ANOTHER_AWS_ACCESS_KEY_ID
aws_secret_access_key = ANOTHER_AWS_SECRET_ACCESS_KEY
```

```php
use Aws\DynamoDb\DynamoDbClient;

$client = new DynamoDbClient([
    'profile' => 'project1',
    'region'  => 'us-west-2',
    'version' => 'latest'
]);
```

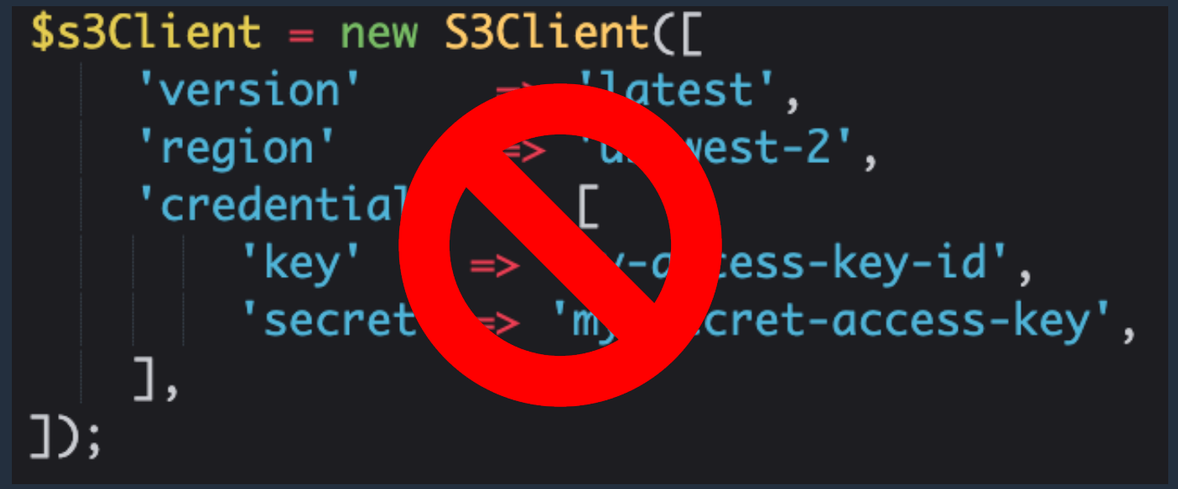
https://docs.aws.amazon.com/ja_jp/sdk-for-php/v3/developer-guide/guide_credentials_profiles.html

IAMロールを継承

- EC2 / ECS / Lambda / Elastic Beanstalk 等から各種サービスに接続するための認証情報を提供する方法として推奨

- 実際にアプリケーションをAWS上で稼働させる際にプログラム内に埋め込むのはセキュリティ上の問題、メンテナンス性から非推奨

- IAMの権限は必要最低限に絞っておく



https://docs.aws.amazon.com/ja_jp/sdk-for-php/v3/developer-guide/guide_credentials_hardcoded.html

意図しないアクセスキーの漏洩を防ぐためにもハードコードは避けましょう！

EC2からIAMロールを利用した認証

- アプリケーション実行時にメタデータサーバーにアクセスし認証情報(アクセスキーID,シークレットアクセスキー、セッショントークン、セッションの有効期間)を取得
- 認証情報が設定されその認証情報でサービスのAPIが呼び出される。
- 有効期限が切れた場合はリフレッシュ処理が走る
- セキュリティ面、メンテナンス性の両面からメリットのある実装方法

その他の認証方法

- 認証情報プロバイダを使用する
  - 独自のカスタムロジックを実装したい場合に利用

- AWS STSを利用した一時認証情報の利用
  - IDフェデレーション、クロスアカウント、IAMロールが利用される場合に利用

- ハードコードされた認証情報の使用**(NG!)**
  - 非推奨

- 匿名クライアントの作成
  - パブリックアクセスできるS3バケットに対して匿名でアクセスしたい時などに利用。

認証情報プロバイダの使用

- デフォルトの認証情報プロバイダ以外にも用途に応じた複数の認証情報プロバイダが提供されている
- 自身でカスタムプロバイダを作成して利用することも可能
- 認証情報プロバイダは遅延評価されるためコンストラクタに渡されたタイミングで認証情報が検証されるわけではない
- デフォルトのプロバイダではmemoize()が呼ばれ意識しなくてもメモ化がされているが、デフォルト以外を定義して利用する場合はmemoize()を明示的に呼び出すこと。

assumeRoleプロバイダの例

```php
use Aws\Credentials\CredentialProvider;
use Aws\Credentials\InstanceProfileProvider;
use Aws\Credentials\AssumeRoleCredentialProvider;
use Aws\S3\S3Client;
use Aws\Sts\StsClient;

$profile = new InstanceProfileProvider();
$ARN = "arn:aws:iam::123456789012:role/xaccounts3access";
$sessionName = "s3-access-example";

$assumeRoleCredentials = new AssumeRoleCredentialProvider([
    'client' => new StsClient([
        'region' => 'us-east-2',
        'version' => '2011-06-15',
        'credentials' => $profile
    ]),
    'assume_role_params' => [
        'RoleArn' => $ARN,
        'RoleSessionName' => $sessionName,
    ],
]);

$provider = CredentialProvider::memoize($assumeRoleCredentials);

$client = new S3Client([
    'region'      => 'us-east-2',
    'version'     => '2006-03-01',
    'credentials' => $provider
]);
```

https://docs.aws.amazon.com/ja_jp/sdk-for-php/v3/developer-guide/guide_credentials_provider.html

AWS STSを利用した一時認証情報の利用

- STSのクライアントを初期化する際にSTSのエンドポイントの指定ができる(legacy か regional)

- legacyを選択した場合はグローバルエンドポイントである、’sts.amazonaws.com’が利用される
- regionalを選択した場合はリージョナルエンドポイントが利用される(例. us-west-2の場合:sts.us-west-2.amazonaws.com)

- デフォルトはlegacyになっているがグローバルエンドポイントを用いることによるレイテンシの増加が懸念されるため、regionalを明示的に選択したほうがよい

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_credentials_temp_enable-regions.html

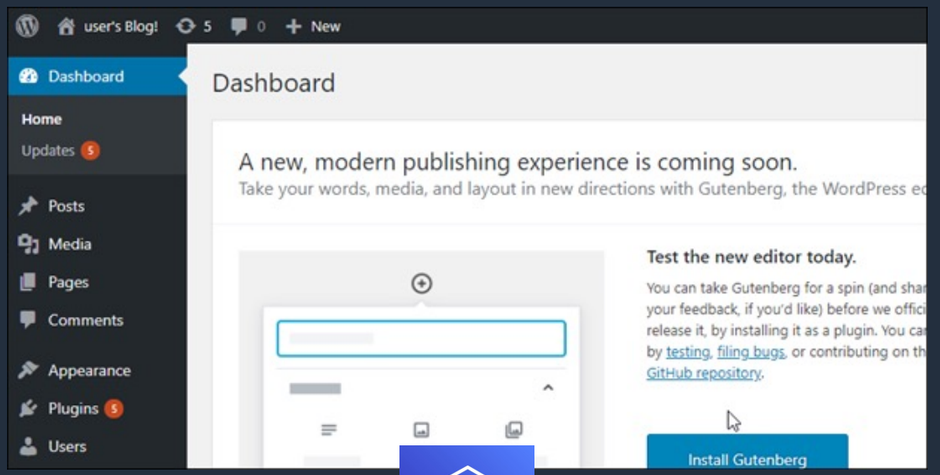
https://docs.aws.amazon.com/ja_jp/sdk-for-php/v3/developer-guide/guide_credentials_temporary.html

assumeRoleしてS3のバケットの一覧表示

```php
use Aws\S3\S3Client;
use Aws\Sts\StsClient;
use Aws\Sts\RegionalEndpoints\Configuration;

$config = new Configuration('regional');

$sts = new StsClient(
  [
    'version' => 'latest',
    'region' => 'us-west-2',
    'profile' => 'default',
    'sts_regional_endpoints' => $config,
  ]
);

$roleToAssumeArn = 'arn:aws:iam::Example:role/BlackbeltRole';

$result = $sts->assumeRole([
  'RoleArn' => $roleToAssumeArn,
  'RoleSessionName' => 'assumeSession'
]);

$s3 = new S3Client([
  'version' => 'latest',
  'region'  => 'us-west-2',
  'credentials' =>  [
    'key'    => $result['Credentials']['AccessKeyId'],
    'secret' => $result['Credentials']['SecretAccessKey'],
    'token'  => $result['Credentials']['SessionToken']
  ],
]);

$s3->listBuckets([]);
```

ハードコードされた認証情報の使用について

- Wordpressなどのソフトウェアのプラグインには AWSとの連携のため認証情報をハードコードする形式のものもあります
- プラグインを利用する際にはまずIAMロールでの認証が可能なものの検討を
- ハードコードするタイプのプラグインを利用される場合も定期的な認証情報の変更の実施をオススメします
- 連携のための認証情報には連携に必要な最小限のアクセス権を付与する



AWS SDK for PHP

本資料に関するお問い合わせ・ご感想

技術的な内容に関しましては、有料のAWSサポート窓口へ
お問い合わせください

https://aws.amazon.com/jp/premiumsupport/

料金面でのお問い合わせに関しましては、カスタマーサポート窓口へ
お問い合わせください（マネジメントコンソールへのログインが必要です）

https://console.aws.amazon.com/support/home#/case/create?issueType=customer-service

具体的な案件に対する構成相談は、後述する個別相談会をご活用ください

ご感想はTwitterへ！ハッシュタグは以下をご利用ください
#awsblackbelt

その他コンテンツのご紹介

ウェビナーなど、AWSのイベントスケジュールをご参照いただけます

https://aws.amazon.com/jp/events/

ハンズオンコンテンツ

https://aws.amazon.com/jp/aws-jp-introduction/aws-jp-webinar-hands-on/

AWS 個別相談会

AWSのソリューションアーキテクトと直接会話いただけます

https://pages.awscloud.com/JAPAN-event-SP-Weekly-Sales-Consulting-Seminar-2021-reg-event.html

Thank you!