モジュール2 知識の確認

- AWS では、すべてのサービスは API によって管理される

- ○

- Amazon CloudWatch を使用すると、EC2インスタンスのCPU、ディスク I/O、ネットワークをモニタリングできる

- ○
- 「**CloudWatch標準メトリクス**」ではCPU、ディスクI/O、ネットワークI/Oなどをモニタリングできる。
- 「**CloudWatchカスタムメトリクス**」を使用すると、OS内の情報（メモリ情報など）や、アプリケーション独自のデータもモニタリングできる。

- AWS CloudTrail では、リクエストを行ったIAMユーザーや、リクエストの内容を確認できる

- ○
- なお、**AWS X-Rayでは、リクエストを行ったIAMユーザーは確認できない**。

- 500 番台のエラーコードは、クライアントエラー（アプリケーション内のエラー）を示す

- ×
- 400番台＝クライアントエラー
- 500番台＝サーバーエラー

- SDK を直接使用することも、CLI と AWS コンソールを使用することもできる

- ○
- なお、**APIも直接（HTTPS等で）呼び出すことができる**が、通常はSDKを使用する。

- サービスクライアント API とリソースAPI では、 サービスクライアント APIのほうが、より高いレベルの抽象化が提供される

- ×
- クライアントAPI＝低レベル
- リソースAPI＝高レベル

モジュール3 知識の確認

- アクセスキーIDとシークレットアクセスキーを持つユーザーは AWS マネジメントコンソールにサインインできる

- ×
- マネジメントコンソールにログインするには、ユーザーIDとパスワードが必要である。

- IAM ユーザーを新規作成した（パスワードは発行していない）。このIAMユーザーは、デフォルトで AWS マネジメントコンソールにサインインできる

- ×
- **デフォルトでは、マネジメントコンソールログイン用のパスワードも、アクセスキー・シークレットアクセスキーも発行されない**。したがってデフォルトではマネジメントコンソールにはログインできない。

- 管理ポリシーには「AWS管理ポリシー」と「カスタマー管理ポリシー」がある。お客様は AWS 管理ポリシーを編集できない

- ○
- 「**カスタマー管理ポリシー**」は編集できる。

- アクセスキーID、シークレットアクセスキーは、アプリケーションの設定ファイル内に保存するのが適切である。

- ×
- ユーザーのホームディレクトリ以下の設定ファイル（**~/.aws/credentials**）に保存する。

- AWS リソースにアクセスするには、適切な権限を設定したIAM ユーザーが必要である。ただし、EC2やLambdaを使用する場合は、IAMロールを使用して必要な権限を取得することができるため、必ずしもIAMユーザーは作る必要がない。

- ○

- AWSのアカウントを開設した直後は、「ルートユーザー」が存在する（メールアドレスとパスワードを使用してログインすることができる）。IAM ユーザーは自動的には作成されないので、必要に応じて明示的にIAMユーザーを作成しなければならない。

- ○

モジュール4 知識の確認

- データはオブジェクトとして S3 バケットに保存される。テキスト、動画、写真、その他のバイナリ形式など、あらゆる種類のファイルを保存できる。オブジェクトの最大サイズは5TBだが、バケットにはサイズの制限がない。

- ○

- バケットは、特定のリージョンに属する。

- ○

- CORS （Cross-Origin Resource Sharing、オリジン間リソース共有）は、あるドメインでロードされたクライアントウェブアプリケーションが、別のドメインにあるリソースにアクセスできるようにする仕組みである。S3はCORSをサポートしている。

- ○

- オブジェクトをアップロードする前に、オブジェクトのメタデータを設定すると、パフォーマンスが向上する。

- ○

- すべてのオブジェクトとバケットは、デフォルトでプライベート（非公開）である

- ○

- S3のアクセスを制御する仕組みとして、ACL（アクセス・コントロール・リスト）を使用する方法と、IAMの仕組みを使用する方法（バケットポリシー、IAMポリシー）がある。ACLを使用すると、他のアカウントや、パブリック（世界中のユーザー）に対するアクセスをコントロールすることができる。

- ○

モジュール6 知識の確認

- Amazon DynamoDB は、アプリケーション向けの高速で柔軟性の高いデータベースである。DynamoDBではSQLを使用して操作を行うことができる。

- ×
- DynamoDBはNoSQLデータベース。

- 1つのグローバルテーブルは、1つ以上の「レプリカテーブル」で構成される。1つの「グローバルテーブル」に含まれる「レプリカテーブル」は、1つのアカウントに所属する。（アカウントをまたいで、レプリカテーブルを作成することはできない）

- ○

- グローバルテーブルの「レプリカテーブル」は複数のリージョンに配置される。あるリージョンの「レプリカテーブル」に書き込みを行うと、他のリージョンの「レプリカテーブル」にも書き込みが反映される。

- ○

- DynamoDBのテーブルがある。プライマリキーではない属性に対して「クエリ（Query）」を実行する必要がある場合は、グローバルセカンダリインデックスを作成する

- ○

- RCU は、最大 2 KB の項目に対して、読み込みを 1 秒間に何回行うかを表す値である。

- ×
- 1 RCUで、**最大4KBの項目**の読み込みを1秒間に1回行うことができる。

- 読み書きが集中するパーティションのことを「ホットスポット」という。性能を最大化するには、パーティションキーを慎重に選択して、ホットスポットを回避する

- ○

モジュール7 知識の確認

- Lambdaでは、サーバーの管理はサービス内で行われるため、お客様がサーバーをデプロイしたり、キャパシティを管理する必要がない。

- ○

- AWS Lambda 関数に関連する権限としては「呼び出し権限」（Lambda関数ポリシーで設定される）と「実行権限」（IAMロールのポリシーで設定）がある。Lambda関数が、アカウント内の別の AWS リソース（たとえばS3バケット）にアクセスするには、「実行権限」が必要である

- ○

- AWS Lambda では、アイドル（関数が実行されていない）状態のときに料金が発生しない。

- ○

- Lambda 関数の開発と作成は、マネジメントコンソール内（ AWS Lambda コンソール）でのみ可能である

- ×
- CLIやAWS SAMを使用してLambda関数を作成することができる。

- DynamoDBテーブルに対して「ストリーム」を有効化することができる。Lambda関数では、ストリームをポーリングして、テーブルに対する変更をすべて取得することができる。

- ○

- Lambda 関数はコードと設定で構成される

- ○

モジュール8 知識の確認

- API Gateway を使用すると、開発者は API の開発、公開、メンテナンス、モニタリング、保護を行うことができる

- ○

- スロットリング（時間あたりの呼び出し回数制限）は、「ステージ」レベル、または「メソッド」レベルで設定できる。クライアントレベルのスロットリングは設定できない。

- ×
- **「使用量プラン」**を使用して、クライアントレベルのスロットリングを行うこともできる。

- スロットリングは、Rate（1秒間での最大呼び出し回数）とBurst（最大同時リクエスト数）を設定できる。Rateは最大は10,000、Burstの最大は5,000に設定できる。これらの制限値は引き上げることはできない。

- ×
- RateとBurstの制限値は、必要であれば、**AWSサポート**に問い合わせて、引き上げることが可能である。

- リソースポリシーを作成することで、API へのアクセスを保護できる

- ○
- APIの呼び出しを、特定のIAMユーザーにのみ許可したり、特定のIPアドレスからの呼び出しのみ許可したりすることができる。

- VPC クライアントからのみアクセス可能なプライベート API エンドポイントを作成することで、API へのアクセスを保護できる

- ○
- 特定のVPCからのみアクセス可能な、プライベートなAPIエンドポイントを作成することができる。VPC側からは「インターフェイスVPCエンドポイント」を経由してAPIにアクセスする。

- AWS Lambda 関数を CRUD バックエンドとして使用することで、多様なAPI呼び出しをインテリジェントに処理できる
- ※CRUD=Create,Read,Update,Delete。データの操作。

- ○
- API GatewayとLambda関数を使用して、CRUDを処理することができる。

モジュール9 知識の確認

- SQS を使用すると、 パブリッシャーはキューにメッセージを保存できる。コンシューマは、キューからメッセージを取り出して処理することができる。パブリッシャーは、コンシューマーの処理を待つ必要がない。

- ○

- SQS 標準キューによって、メッセージの順序が変わることはない

- ×

- SQS キューのロングポーリングは、シングルスレッドアプリケーションで適切に機能する（ポーリング以外の処理に影響を与えない）

- ×
- ロングポーリングを使用すると、**キューにメッセージがない場合にポーリング処理が待ち状態になる**。したがって、シングルスレッドアプリケーションの場合、ポーリング以外の処理が停止する。

- SNS トピックでは、メッセージをフィルタリングできない。サブスクライバーは常に、パブリッシュされたすべてのメッセージを受信する

- ×
- 「フィルタリング」の設定で、受信するメッセージを絞り込むことができる。

- Amazon SNS から Amazon SQS にメッセージが送信されるとき、メッセージは JSON ドキュメントとしてエンコードされる

- ○

- Amazon MQ は、JMS、NMS、AMQP、STOMP、MQTT、WebSocket プロトコルに対応
  している

- ○

モジュール10 知識の確認

- ステートマシンのすべての作業はアクティビティによって実行される。

- ×
- ステートマシンのすべての作業は**タスク**によって実行されます

- Pass ステートでは、何も作業が実行されずに、入力がそのまま出力される。

- ○

- ステートマシンでは、分岐、並列実行、再試行/エラー処理、タスクの実行をサポートしている。

- ○

- Choice ステートに指定できる Next タスクは 2 つのみである。

- ×
- Choice ステートには(2つのみではなく)**1 つ以上の Next がある**。

- ステートマシンは JSON で定義され、ユーザーはこれをコンソールで可視化し、モニタリングできる。

- ○

- API Gateway で HTTPS/AJAX コールをインターセプトして、ステートマシンを開始できる。

- ○

モジュール11 知識の確認

- データのアクセス頻度が低い場合にキャッシュを検討する。

- ×

- ElastiCacheの内部処理において、Memcached はマルチスレッド、Redis は単一スレッドでの実行となる。Memcachedのほうが、多くのCPUコアを同時に利用することができ、より多くの操作を同時に処理できる。

- ○

- マルチ AZ、自動フェイルオーバー機能を使用できるのは Redis のみである。

- ○

- 有効期限 (TTL) は、キーの有効期限が切れるまでの秒数を指定する整数値である。

- ○

- 書き込みスルー戦略では、データベースにデータを書き込むときに、キャッシュのデータを追加/更新する。

- ○

- Memcached には Pub/Sub 機能がある。

- ×
- Memcached には Pub/Sub 機能はありません。Pub/Sub 機能は Redis に含まれています

モジュール12 知識の確認

- コンテナは、開発者がアプリケーションをパッケージ化してデプロイするための手段としてますます重要になっている。

- ○

- コンテナ内では、あらゆるアプリケーションとプログラミング言語を使用できる。

- ○

- ECS では、コンテナオーケストレーション ソフトウェアのインストールと操作に加え、仮想マシンのクラスターの管理とスケールが必要である。

- ×
- ECS では、コンテナオーケストレーション ソフトウェアのインストールと操作や、仮想マシンのクラスターの管理とスケールは必要ありません

- コンテナを削除するには、docker rmi コマンドを使用する。

- ×
- コンテナを削除するには、docker rm コマンドを使用します。docker rmi コマンドは、イメージを削除する場合に使用します。

- AWS Fargate は、基盤となるインフラストラクチャの管理作業を必要としない、コンテナをデプロイおよび管理するためのテクノロジーである。

- ○

- Amazon ECR は Amazon ECS と統合されているが、コンテナイメージを Docker Hub に保存することもできる。

- ○

モジュール13 知識の確認

- AWS Certificate Manager が生成したプライベートキーはダウンロードできる

- ×
- AWS Certificate Manager が生成したプライベートキーはダウンロードできません

- AWS Security Token Service の一時的なセキュリティ認証情報は、失効すると再利用できない

- ○
- 一時的なセキュリティ認証情報の有効期限には制限があり (デフォルトで 3,600 秒)、有効期限を設定できます。認証情報が有効な期間を指定できます。一時的セキュリティ認証情報が失効すると、再利用することはできません。

- AWS Secrets Manager はデータベース認証情報を更新することができる

- ○

- Cognito フェデレーテッドアイデンティティを使用してお客様のユーザー名とパスワードを保存できる

- ○

- Amazon Cognito ユーザープールはデバイス間でのユーザーデータの同期を可能にする

- ○
- **複数デバイスでの、ユーザーデータの同期**が可能。

- Amazon Cognito ユーザープールでは、SAML および OpenID Connectを使用した認証を実装することができる。

- ○

モジュール14 知識の確認

- DevOps は製品に関係するチーム間の共同作業を必要とする方法論である

- ○

- リリースプロセスは大抵、ソース、ビルド、テスト、本番環境、モニタリングという 5 つの段階に簡略化できる

- ○

- ブルー/グリーン間のトラフィックルート変更には、DNS カットオーバーと Auto Scaling グループの交換という 2 つの方法が、最も一般的な手法として用いられている

- ○

- AWS CodeStar では、ソースコードのコンパイル、テストの実行、すぐにデプロイできるソフトウェアパッケージの生成を行う

- ×

- Elastic Beanstalk では、アプリケーションの新しいバージョンをローリング更新で既存のスタックの上にリリースできる

- ○

- A/B デプロイ戦略は、ブルー/グリーンデプロイ戦略とは機能が大きく異なっている

- ×
- A/B デプロイ戦略は、実行している環境の 2 つのコピーを使用するという点でブルー/グリーンと同じように機能します