問題41: 不正解

大手保険会社ではAWSを利用した顧客管理アプリケーションを利用しています。この会社では毎年IT監査を実施することが義務付けられています。そのために大手監査会社の内部監査員が、会社の内部AWSサービスをレビューするためにアサインされました。あなたは運用担当者として、データのセキュリティを損なうことなく自社が利用するAWSサービスを監査するために必要なアクセス権限を監査人に提供することが求められています。

これらの要件に対応するため、最適なAWSソリューションを選択してください。

- ◉ 監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したSTSを設定し、それを監査人に提供する。 (不正解)
- ○ 監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したIAMロールを設定し、それにより監査人への一時的なアクセスを提供する。 (正解)
- ○ AWS Organizationsで監査人専用のOUを作成して、監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したSCPを設定する。
- ○ 監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したIAMポリシーを設定し、それを監査人専用のIAMユーザーにアタッチする。

説明

このシナリオでは、監査人に対して監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したIAMロールを使用することで、AWS リソースへのアクセスを委任することができます。したがって、オプション 2 が正解となります。

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ロールを使用して AWS リソースへの通常は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。たとえば、AWS アカウントユーザーに、通常はないリソースに対するアクセス許可を付与したり、ある AWS アカウントのユーザーに、別のアカウントのリソースに対するアクセス許可を付与したりできます。リソースを監査できるように、アカウントへのアクセス権を第三者に付与することができます。

詳細は以下のページをご参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_create_for-user_externalid.html

オプション 1 は不正解です。STSは一時認証機能を実現する際にアプリケーション上で実装されることはありますが、STSをIAMロールのように設定し、それを監査人に提供するといった使い方はできません。

オプション 3 は不正解です。監査範囲に権限を限定したAWSリソースの読み取り専用のアクセス権限を設定したSCPを設定するといった利用方法は、SCPにはできません。

オプション 4 は不正解です。IAMユーザーによって新規にユーザーを作成して権限を付与することもできなくはありませんが、監査人などの第三者アカウントに権限を委譲するにはIAMロールが最適な選択肢です。IAMユーザーは一時的に付与するものではなく、アカウント内のユーザーとして管理するために発行するものであるため、こういったケースでは利用しません。

問題42: 不正解

あなたの会社はオンプレミス環境において契約管理ポータルを運用しています。この契約管理ポータルを使用することで、会社間でいつでもどこでも契約書にデジタル署名を付与して交換することができ、契約行為の一部をクラウド上で自動化することができます。このポータルのアプリケーション層ではApacheサーバーを使用しています。データベース層ではRMANバックアップユーティリティを使用して定期的にバックアップされるOracleデータベースを使用しており、RMANバックアップによる復元処理が実施できる必要があります。現在、ApachサーバーとデータベースサーバーのバックアップはiSCSIインターフェイス経由でアプリケーションサーバーに接続されている512GBのAWS Storage Gateway保管型ボリュームに保存されます。オンプレミス環境が停止した場合に備えて、これらのポータルをAWSに復元することが必要となりました。

このバックアップを利用したAWS環境での復元ソリューションを選択してください。

- (●) ApacheサーバーをELBターゲットグループに設定されたいくつかのEC2インスタンスに展開する。OracleサーバーをRDSへと移行して、マルチAZ展開と自動バックアップを実施する。S3バケットにあるRMANオラクルバックアップからOracleデータベースを復元する。AWS Storage Gatewayの保管型ボリュームを利用して静的コンテンツをEBSボリュームに取得して、Apacheサーバーのデータ内容を復元する。 (不正解)
- ( ) ApacheサーバーをELBターゲットグループに設定されたいくつかのEC2インスタンスに展開する。OracleサーバーをRDSへと移行して、マルチAZ展開と自動バックアップを実施する。S3バケットにあるRMANオラクルバックアップからOracleデータベースを復元する。AWS Storage Gateway VTLから静的コンテンツを復元する。
- ( ) ApacheサーバーとOracleサーバーをELBターゲットグループに設定されたいくつかのEC2インスタンスに展開する。S3バケットにRMANオラクルバックアップを保存して復元時に利用する。S3バケットにあるRMANオラクルバックアップからOracleデータベースを復元する。AWS Storage Gateway VTLから静的コンテンツを復元する。
- ( ) ApacheサーバーとOracleサーバーをELBターゲットグループに設定されたいくつかのEC2インスタンスに展開する。AWS Storage Gatewayの保管型ボリュームにあるバックアップファイルを利用して、S3バケットにあるRMANオラクルバックアップからOracleデータベースを復元する。また、Apacheサーバーのバックアップを EC2インスタンスにアタッチされたEBSボリュームに取得して、Apacheサーバーのデータ内容を復元する。 (正解)

説明

このシナリオでは、オンプレミス環境にあるWEBサーバーとデータベースサーバーのバックアップをAWS Storage Gatewayの保管型ボリュームによって実施して、オンプレミス環境が停止した場合のAWS上での復元方法が問われています。

まずはApacheサーバーとOracleサーバーをELBターゲットグループが設定されたEC2インスタンス群に設定していくことになります。特にOracleサーバーはRMANオラクルバックアップを利用する構成であるため、RDSのOracleエンジンではRMANによるバックアップ自体は設定可能ですが、現時点では、RMAN による復元方式は Amazon RDS for Oracle の DB インスタンスでサポートされていません。したがって、RDSではなくEC2インスタンスにOracleサーバーを復元することが必要です。その際は、保管型ストレージゲートウェイを使用して、データを復元する必要があります。

ボリュームゲートウェイは、iSCSIプロトコルを使用してアプリケーションにブロックストレージを提供します。ボリューム上のデータはAmazon S3に保存されます。 AWSでiSCSIボリュームにアクセスするには、EBSボリューム作成に使用できるEBSスナップショットを利用します。したがって、オプション4が正解となります。

オプション1と2は間違いです。RDSはRMANバックアップユーティリティによるDBの復元処理をサポートしていないため、RDSを使用できません。代わりにEC2インスタンスにOracleサーバーをインストールすることで、データベースを立ち上げる必要があります。

オプション3は不正解です。AWS Storage Gateway VTLは仮想テープライブラリーで、テープや仮想テープライブラリシステムからクラウドにバックアップジョブを移行するサービスとなっています。今回は保管型ボリュームを利用して、静的コンテンツを保管しているため不適切です。

問題43: 不正解

B社ではWEBアプリケーションのデータベースとしてRDS MySQLを利用しています。本日、このMySQLデータベースが応答しなくなる障害が発生し、あなたは対応に追われています。初めに障害要因の解析のため、実行に時間を要したSQLステートメント内容を収集して、解析することになりました。

必要なSQLステートメント内容を収集するために必要となる設定はどれでしょうか。

- ◉ RDSの一般ログを有効にする (不正解)
- ○ RDSのMySQLエラーログを有効にする
- ○ RDSのスロークエリログを有効にする (正解)
- ○ RDSのSQLクエリログを有効にする

説明

オプション3が正解となります。MySQLでは、エラーログ、スロークエリログ、一般ログの3つのログをモニタリングできます。MySQLエラーログはデフォルトで生成されます。DBパラメータグループのパラメーターを設定することで、スロークエリと一般ログを生成できます。ログの中でも、トラブルシューティングのために実行に時間がかかったすべてのSQLステートメント内容を収集することができるのはスロークエリログであり、これを有効化することが求められます。

スロークエリログは、実行にlong_query_time秒以上かかるSQLステートメントで構成され、少なくともmin_examined_row_limit行を調べることで確認することができます。したがって、RDSでスロークエリログを有効にすることが正しいです。

AWSによる各ログの詳細は以下の通りです。

■一般ログ：
mysqld の実行内容の一般的な記録です。サーバーは、クライアントが接続または接続解除したときに情報をこのログに書き込み、クライアントから受け取った各 SQL ステートメントをログに記録します。一般クエリーログは、クライアント側でエラーが疑われるとき、クライアントが mysqld に送信した内容を正確に知りたい場合に非常に役立つことがあります。

■エラーログ
エラーログには mysqld が開始および停止された時期を示す情報と、サーバーが実行中に発生したあらゆるクリティカルエラーが格納されます。自動的にチェックまたは修復することが必要なテーブルが mysqld で検出された場合、エラーログに警告メッセージが書き込まれます。

■スロークエリログ
スロークエリーログは、実行に要した時間が long_query_time 秒を超え、少なくとも min_examined_row_limit 行を検査する必要があった SQL ステートメントで構成されます。 long_query_time の最小値およびデフォルト値は、それぞれ 0 および 10 です。値はマイクロ秒の精度まで指定できます。ファイルへのロギングの場合、時間はマイクロ秒の部分も含めて書き込まれます。テーブルへのロギングの場合、時間の整数部のみ書き込まれ、マイクロ秒の部分は無視されます。

問題44: 不正解

あなたはオンデマンド動画アプリケーションを提供しているメディア企業で働くAWSエンジニアです。この動画アプリケーションは動画ファイルをS3バケットに保存するアプリケーション構成となっています。あなたは会社のデジタル資産を保護するために、保存された動画データのアクセス権限がパブリックに公開されていないかどうかを通知する通知システムがセットアップするように依頼されました。動画データに対する不正アクセスが発覚した場合は、コンプライアンスチームへと通知することも必要です。

この要件を満たすためのAWSソリューションを選択してください。

- (●) AWS ConfigによりコンプライアンスS違反についてAmazon S3バケットのACLとバケットポリシーを監視する。IAMロールを使用してS3バケットのACLとバケットポリシーを確認し、コンプライアンス違反発生時に通知するLambda関数を作成する。AWS ConfigがS3バケットACLまたはバケットポリシーの違反を検出した際に、Lambda関数を起動するAmazon EventBridgeのイベントルールを設定する (不正解)
- ( ) AWS ConfigによりコンプライアンスS違反についてAmazon S3バケットのACLとバケットポリシーを監視する。IAMロールを使用してS3バケットのACLとバケットポリシーを確認し、コンプライアンス違反発生時に通知するSNSトピックを作成する。AWS ConfigがS3バケットACLまたはポリシーの違反を検出した際に、SNSを起動するAmazon EventBridgeのイベントルールを設定する (正解)
- ( ) Amazon CloudTrailによりコンプライアンス違反についてAmazon S3バケットのACLとバケットポリシーを監視する。IAMロールを使用してS3バケットのACLとバケットポリシーを確認し、コンプライアンス違反発生時に通知するLambda関数を作成する。CloudTrailがS3バケットACLまたはポリシーの違反を検出した際に、Lambda関数を起動するAmazon EventBridgeのイベントルールを設定する
- ( ) AWS Systems Manager Compliance RuleによりコンプライアンスS違反についてAmazon S3バケットのACLとバケットポリシーを監視する。IAMロールを使用してS3バケットのACLとバケットポリシーを確認し、コンプライアンス違反発生時に通知するSNSを作成する。AWS Systems Manager Compliance RuleがS3バケットACLまたはポリシーの違反を検出した際に、S3イベントを起動するAmazon EventBridgeのイベントルールを設定する

説明

AWS Config は、AWS リソースの設定を評価、監査、審査できるサービスです。これを利用して、パブリック読み取り、またはパブリック書き込みアクセスを許可する違反について、S3バケットACLとバケットポリシーに基づいて監視することができます。また、AWS ConfigがS3バケットACLまたはポリシー違反を検出した際に、SNSを起動するAmazon EventBridgeのイベントルールを設定することができます。これにより、AWS Configがポリシー違反を検出すると、Amazon EventBridgeのイベントルールによってトリガーされ、ポリシーに違反していることをAmazon SNSによって通知することができます。

これらの手順を考えると、オプション２が正解となります。

オプション１は不正解です。AWSではSNSによって通知機能を容易に作ることができます。したがって、コンプライアンス違反ポリシーをチームに通知するLambda関数を作成して通知を実行したり、イベントを確認したりするプロセスは非効率です。ConfigとSNSとAmazon EventBridgeイベントを構成すれば、独自のLambdaコードを利用する必要はありません。ただし、標準で利用できない監視ルールを設けたい場合は、Configのカスタムルールを利用してLambda関数による処理を構築することができます。

オプション３は不正解です。Amazon CloudTrailによりコンプライアンス違反について、ACLとポリシーを監視するというのは間違いです。AWS リソースの設定を評価、監査、審査できるのはConfigになります。

オプション４は不正解です。AWS Systems Manager Compliance Ruleはパッチ適用時にコンプライアンスルールを確認する仕組みとなっており、この問題で想定しているリソース構成のコンプライアンス確認に使用するものではないため、不正解となります。

問題45: 不正解

あなたはAWS上でNode.jsを利用したWEBアプリケーションを開発しています。現在はDynamoDBテーブルにおける読み込みキャパシティと書き込みキャパシティを設計しているところです。要件としては、1秒間に30回の書き込みを処理し、その後、1秒間に20回の結果整合性のある読み取りを処理する必要があり、両方の操作ですべてのアイテムのサイズが1KBになります。

テーブルにプロビジョニングする必要がある読み込みキャパシティーユニット（RCU）と書き込みキャパシティーユニット（WCU）の設定を選択してください。

- ◉ 20RCUと30WCU (不正解)
- ○ 10RCUと20WCU
- ○ 10RCUと30WCU (正解)
- ○ 10RCUと60WCU

説明

以下のキャパシティーユニットの計算方式からオプション3の「10RCUと30WCU」が正解となります。

■読み込みキャパシティーユニット（RCU）の計算方法

1つの読み込みキャパシティーユニットは、最大サイズ4 KBの項目について、1秒あたり1回の強力な整合性のある読み込み、あるいは1秒あたり2回の結果整合性のある読み込みを表します。例えば、10ユニットのプロビジョニングされた読み取りキャパシティーでテーブルを作成するとします。これにより、最大4 KBの項目について、1秒あたり10回の強い整合性のある読み込み、または20回の結果整合性のある読み込みを行えます。

4 KBを超える項目の読み込みには、より多くの読み取りキャパシティーユニットを消費します。たとえば、8 KB（4 KB × 2）の項目の強い整合性のある読み込みは、2ユニットの読み込みキャパシティーユニットを消費します。同じ項目の結果的に整合性のある読み込みは、読み込みキャパシティーを1ユニットしか消費しません。

したがって、RCUは10ユニットのプロビジョニングされた読み取りキャパシティーでテーブルに対して、20回の結果整合性のある読み込みを行えるため、10RCUが正しい設定となります。

■書き込みキャパシティーユニット（WCU）の計算方法

1つの書き込みキャパシティーユニットは、最大サイズが1KBの項目について、1秒あたり1回の書き込みを表します。

例えば、10ユニットのプロビジョニングされた書き込みキャパシティーでテーブルを作成するとします。これにより、1秒あたり最大でサイズが1KBの項目について、1秒あたり10回の書き込みを行えます。

書き込みの項目サイズは、次の1KBの倍数に切り上げられます。たとえば、500バイトの項目の書き込みは、1KBの項目の書き込みと同じスループットを消費します。

したがって、WCUは30ユニットのプロビジョニングされた読み取りキャパシティーのテーブルに対して、1秒あたり最大でサイズ1KBの項目について、1秒あたり30回の書き込みを行えます。

これを踏まえると、オプション3が正解となります。

問題40: 不正解

あなたの会社はいくつかのWEBアプリケーションをAWS Elastic Beanstalkを利用して展開・管理しています。現在展開しているアプリケーションは、WEBサイトのユーザー行動データを継続的に収集して、Amazon Kinesisストリームを利用してデータをフィードして解析します。ユーザー行動データはリアルタイムで集計されていますが、Kinesis内部でデータ処理を完結して、分析結果をDynamoDBテーブルに保存する仕組みとなっています。そのため、分析前データが保存できていないために問題となっており、S3に分析前のストリームデータを保存する仕組みを実装することになりました。

この要件を満たすことができるソリューションを選択してください。（2つ選択してください。）

- [x] Amazon Kinesisコネクトライブラリによって、データをKinesisからS3へと移行するアプリケーション機能を追加する。 (正解)
- [ ] Amazon Kinesis Data Firehoseによって、データをKinesisからS3へと移行するアプリケーション機能を追加する。 (正解)
- [ ] Amazon Kinesis Data Streamsによって、データをKinesisからS3へと移行するアプリケーション機能を追加する。
- [ ] Amazon Kinesis S3 マネジメントによって、データをKinesisからS3へと移行するアプリケーション機能を追加する。
- [ ] KCL Workersによって、データをKinesisからS3へと移行するアプリケーション機能を追加する。

説明

Amazon Kinesis コネクトライブラリまたはKinesisからS3バケットにデータをアーカイブするAmazon Kinesis Data Firehoseを使用して、取得データをS3にアーカイブすることでデータ損失を防ぐことができます。したがって、オプション１と２が正解となります。

Amazon Kinesis Data Firehose は、ストリーミングデータをデータレイクやデータストア、分析ツールに確実にロードする最も簡単な方法です。ストリーミングデータをキャプチャ・変換して、Amazon S3、Amazon Redshift、Amazon Elasticsearch Service、Splunk にロードして、現在お使いのビジネスインテリジェンスツールやダッシュボードでほぼリアルタイムに分析できます。

Amazon Kinesis S3コネクトライブラリを使用して Amazon Kinesis から Amazon S3 にデータをアーカイブすることができます。Amazon Kinesis コネクタライブラリを使用すると Amazon Kinesis を他の AWS サービスやサードパーティー製ツールと簡単に統合できるようになります。Amazon Kinesis コネクタライブラリを使用するには、Amazon Kinesis クライアントライブラリ (KCL) が必要です。このライブラリの現在のバージョンでは、Amazon DynamoDB、Amazon Redshift、Amazon S3、Amazon Elasticsearch Service に対するコネクタが提供されています。

オプション３は不正解です。Amazon Kinesis Data Streamsはストリームデータを取得して処理するための機能です。今回はAmazon Kinesis Data Firehoseによってデータを KinesisからS3へと移行する仕組みを作る必要があります。

オプション４は不正解です。Amazon Kinesis S3 マネジメントという機能はありません。

オプション５は不正解です。KCL WorkersによってデータをKinesisからS3へと移行する機能を作るのは適切ではありません。*KCL Worker*はStreamと対応してログを受け取るプログラムであり、Kinesisアプリケーションを構築する際に利用します。

問題47: 正解

あなたはエンジニアとして、画像共有システムを開発しています。このアプリケーションではユーザーが共有したい画像をS3バケットにアップロードして共有します。そのために、S3バケットおよび他のAWSリソースにファイルをアップロードするために必要なアクセス許可が設定された一時認証が利用されています。

アプリケーションがファイルをS3にアップロードするために、どのAPIコールを使用する必要がありますか？

- (●) AssumeRole (正解)
- ( ) AssumeRoleWithWebIdentity
- ( ) AssumeRoleWithSAML
- ( ) GetSessionToken

説明

オプション1が正解となります。IAMロールによってアプリケーションがファイルをS3にアップロードできるようにするためには、AssumeRoleのAPIコールを実行します。

一時的なセキュリティ認証情報をリクエストするには、AWS API で AWS Security Token Service (AWS STS) を使用できます。これには、AWS リソースへのアクセスを制御できる一時的セキュリティ認証情報を持つ、信頼されたユーザーを作成および提供するオペレーションが含まれます。一時認証情報を引き受けるためにアプリケーションはAWS STS AssumeRole APIオペレーションを呼び出し、使用するロールのARNを渡します。この操作により、一時的な資格情報で新しいセッションが作成されます。このセッションには、ロールベースのポリシーと同じ権限があります。

オプション2は不正解です。AssumeRoleWithWebIdentityはWeb IDプロバイダーを使用してモバイルアプリケーションまたはWebアプリケーションで認証されたユーザーの一連の一時的なセキュリティ認証情報を返します。プロバイダーの例には、Amazon Cognito、Amazon、Facebook、Google、またはOpenID Connectと互換性のあるIDプロバイダーによるログインが含まれます。Web IDプロバイダーを使用した認証は要件と合致しません。

オプション3は不正解です。AssumeRoleWithSAMLはSAML認証応答を介して認証されたユーザーの一時的なセキュリティ認証情報のセットを返します。このオペレーションは、ユーザー固有の認証情報や設定なしで、エンタープライズIDストアまたはディレクトリをロールベースのAWSアクセスに結び付けるメカニズムを提供します。エンタープライズIDストアまたはディレクトリを今回は利用しないため、今回の要件には合致しません。

オプション4は不正解です。GetSessionToken API オペレーションでは、既存の IAM ユーザーに一時的セキュリティ認証情報のセットが返ります。この API は、MFA が IAM ユーザーに対して有効なときに AWS リクエストを作成するなど、セキュリティを強化するために役立ちますが、今回の要件には合致しません。

問題48: 正解

Egames株式会社はモバイルアプリケーションゲームを専門に開発するゲーム会社です。アプリケーションは、各ユーザーがゲーム記録を取得するために、DyriamoDBテーブルにデータを保存するための権限を必要とします。そのためには、モバイルアプリユーザーに対してDynamoDBテーブルにアクセス許可を与えることが必要があります。

ユーザーのモバイルデバイスにアクセス権限を付与する設定方法を選択してください。

- (●) DynamoDBテーブルへのアクセス権限を設定したIAMロールを作成する。STSのAssumeRoleWithWebIdentityによるウェブIDフェデレーションを利用して、ユーザーがモバイルアプリにサインインする際に、一時的なセキュリティ認証を付与する。 (正解)
- ( ) DynamoDBテーブルへのアクセス権限を設定したIAMロールを作成する。ユーザーがサインインする際にIAMユーザーを新規に作成して、ユーザーがモバイルアプリにサインインする際に、一時的なセキュリティ認証を付与する。
- ( ) DynamoDBテーブルへのアクセス権限を設定したIAMポリシーを作成する。AWS Managed Microsoft ADを設置して、ユーザーがサインインする際のユーザーIDを作成して、このIAMポリシーを適用する。STSのAssumePolicyWithWebIdentityによるウェブIDフェデレーションを利用して、ユーザーがモバイルアプリにサインインする際に、一時的なセキュリティ認証を付与する。
- ( ) DynamoDBテーブルへのアクセス権限を設定したIAMロールを作成する。AWS Managed Microsoft ADを設置して、ユーザーがサインインする際のユーザーIDを作成してウェブIDフェデレーションを利用して、ユーザーがモバイルアプリにサインインする際に、一時的なセキュリティ認証を付与する。

説明

ウェブ ID フェデレーションを使用すれば、カスタムサインインコードを作成したり独自のユーザー ID を管理したりする必要なく、外部 ID プロバイダー (IdP) (例: Login with Amazon、Facebook、Google などの OpenID Connect (OIDC) 互換の IdP) を使用してサインインすることができます。認証トークンを受け取ったら、そのトークンを AWS アカウントのリソースを使用するためのアクセス許可を持つ IAM ロールにマッピングし、AWS の一時的セキュリティ認証情報に変換することができます。IdP を使用すると、アプリケーションで長期的なセキュリティ認証情報を埋め込んで配布する必要がないため、AWS アカウントの安全性の維持に役立ちます。

Amazon Cognito を使用しない場合は、コードを記述して、ウェブ IdP (例: Facebook) とやり取りし、AssumeRoleWithWebIdentity API を呼び出して、これらの IdP から取得した認証トークンを一時的な AWS セキュリティ認証情報と交換する必要があります。既存のアプリで既にこのアプローチを使用している場合は、それを使い続けることができます。

AWS Security Token ServiceのAssumeRoleWithWebIdentityはWeb IDプロバイダーを使用してモバイルアプリケーションまたはWebアプリケーションで認証されたユーザーの一連の一時的なセキュリティ認証情報を返します。プロバイダーの例には、Amazon Cognito、Amazon、Facebook、Google、またはOpenID Connectと互換性のあるIDプロバイダーによるログインが含まれます。したがって、オプション１が正解となります。

オプション２は不正解です。ユーザーがサインインする際に個別のIAMユーザーを生成してアプリケーションの認証機能を作成することはできません。IAMユーザーは個別のアプリケーションのユーザー認証には利用できません。

オプション３と４は不正解です。AWS Managed Microsoft ADによってアプリケーションのユーザー管理を実施することはできません。これはAWSとオンプレミス環境とのインフラの認証基盤として利用されるサービスです。

問題49: 不正解

携帯電話販売をしているA社では、ユーザーが自身のモバイル利用状況を確認して、最適な料金プランを維持できるモバイルコスト最適化アプリケーションを構築しています。このアプリケーションはSQSキューによってリクエストを処理して、DynamoDBテーブルに保存されたデータを取得して表示します。このアプリケーションはユーザーにサービスを、ダウンタイムを極力ゼロにして提供することがSLAで定められています。したがって、予期しないトラフィック負荷の高まりに対しても、ユーザーはデータが取得できる必要があります。

これらの要件を踏まえて、コスト効率の良い最適なAWSアーキテクチャを選択してください。

- ◉ AWS JavaScript SDKを利用してS3バケットを利用したWEBサイトを構築してポーリング処理結果を表示するクライアントページを実装する。CloudFrontとRoute53を利用してWEBサイトのトラフィック処理とコンテンツ配信を実施し、リクエスト処理は、SQSキューに応じたAutoScalingグループが設定されたEC2インスタンスによって、DynamoDBからデータを取得する。 (不正解)
- ○ S3バケットを利用した静的WEBサイトを構築してポーリング処理結果を表示するクライアントページを実装する。CloudFrontとRoute53を利用してWEBサイトのトラフィック処理とコンテンツ配信を実施し、リクエスト処理はSQSキューによるイベント通知によってEC2インスタンスによってDynamoDBからデータを取得する。
- ○ EC2インスタンスを利用してWEBアプリケーションを構築して、ポーリング処理結果を表示する。データベースにDynamoDBを利用してデータ保存・取得を行い、CloudFrontを利用してコンテンツ配信を実施する。リクエスト処理はSQSキューによるイベント通知と連携したLambda関数によってDynamoDBからデータを取得する。
- ○ AWS JavaScript SDKを利用してS3バケットを利用したWEBサイトを構築してポーリング処理結果を表示するクライアントページを実装する。CloudFrontとRoute53を利用してWEBサイトのトラフィック処理とコンテンツ配信を実施し、リクエスト処理はSQSキューによるイベント通知と連携したLambda関数によってDynamoDBからデータを取得する。 (正解)

説明

このアーキテクチャの重要なポイントは、DynamoDBデータ取得するためのアプリケーションをスケーラブルでコスト最適に実現することです。そのためには、EC2インスタンスベースのサーバー機能ではなく、SQSとLambda関数を連携させたサーバレスアプリケーションによって非同期実行処理を多数実施できるように構成します。Lambda関数はDynamoDBテーブル内のデータ取得と集計に向けた様々な機能開発が可能であり、レポート表示に向けたデータ集計には最適です。

ポーリング結果を表示するには、リクエストを読み込んで表示することができるJavaScriptサイトが必要となり、AWS JavaScript SDKを利用してS3バケットを利用したWEBサイトを構築してポーリング処理結果を表示するクライアントページを作成します。また、CloudFrontとRoute53によってWEBサイトへのアクセストラフィックと配信処理を高可用にすることができます。したがって、オプション４が正解となります。

オプション１と２は不正解です。EC2インスタンスを利用した構成でも処理は可能ですが、DynamoDBテーブルのデータ取得・集計にはLambda関数の方が、スケーラブルで低コストに実装することができるため、こちらを優先的に考えてください。

オプション３は不正解です。今回利用するWEBサイトはポーリング処理結果を表示させるための簡素なものであるため、EC2インスタンスを利用したWEBアプリケーション構成はコスト効率が悪いです。S3の静的WEBサイトを使用する方が良いでしょう。

問題50: 不正解

あなたはAPIコールでDynamoDBテーブルからデータを取得するサーバレスアーキテクチャを実装しています。このアプリケーションはLambdaプロキシ統合を使用してAPIゲートウェイと連携していますが、一連の処理を完了するのに長い時間を要しています。一定時間を超過すると、一部のリクエストにタイムアウトが発生しています。APIコールの応答性とLambda関数の実行状況をモニタリングして、問題が発生した場合に対応する仕組みが必要です。

APIコールの応答性とLambda関数の実行状況をモニタリングするためのCloudWatchの設定方法を選択してください。（2つ選択してください。）

- [x] BackendLatencyメトリックスを監視して、バックエンドの応答性を測定する。 (不正解)
- [x] CountLatencyメトリックスを監視して、API呼び出しの全体的な応答性を測定する。 (不正解)
- [ ] CountLatencyメトリックスを監視して、バックエンドの応答性を測定する。
- [ ] Latencyメトリックスを監視して、API呼び出しの全体的な応答性を測定する。 (正解)
- [ ] IntegrationLatencyメトリックスを監視して、バックエンドの応答性を測定する。 (正解)
- [ ] IntegrationLatencyメトリックスを監視して、API呼び出しの全体的な応答性を測定する。

説明

CloudWatchを使用してAPIの実行状況を監視できます。CloudWatchはAPI Gatewayから生データを収集して処理して、リアルタイムで確認可能なメトリックに変換して2週間記録します。ユーザーはこの履歴情報にアクセスして、Webアプリケーションまたはサービスのパフォーマンスを正確に把握できます。デフォルトではAPI Gatewayメトリックスデータは1分間隔でCloudWatchに自動的に送信されます。API Gatewayの名前空間には以下のメトリクスが含まれます。

-4XXError：指定された期間に取得されたクライアント側エラーの数。
-5XXError：指定された期間に取得されたサーバー側エラーの数。
-CacheHitCount：指定された期間内にAPIキャッシュから配信されたリクエストの数。
-CacheMissCoun：APIキャッシュが有効になっている特定の期間における、バックエンドから提供されたリクエストの数。
-Count：指定された期間内のAPIリクエストの合計数。
-IntegrationLatency：API Gatewayがバックエンドにリクエストを中継してから、バックエンドからレスポンスを受け取るまでの時間。
-Latency：API Gatewayがクライアントからリクエストを受け取ってから、クライアントにレスポンスを返すまでの時間。

Latencyメトリクスには統合されたLatencyとその他API Gatewayオーバーヘッド情報が含まれます。したがって、このシナリオではLatencyおよびIntegrationLatencyを設定することが必要となります。オプション4と5が正解となります。

問題51: 正解

あなたの企業はAWSを利用したデータウェアハウスを構築して、業務データ解析を実施して経営に活かしています。このデータウェアハウスはRedshiftを使用していますが、現在、その設定変更を実施しているところです。次第にデータ量が増加したことでパフォーマンスが悪化したため、1つのワークロードにより実施していたデータ分析プロセスを、2つの異なるグループで実施できるように設定し直します。最初のグループが発行した各クエリはデータ分析に約1~2時間かかりますが、2番目のグループが実行するクエリは、データ分析に5分から10分程度しかかかりません。したがって、最初のグループのクエリが完了するまで、2番目のグループのクエリを待機させないようにする必要があります。

2つの分析プロセスを分割するための最適なソリューションは次のうちどれですか？

- ◉ Amazon Redshift のワークロード管理 (WLM) を利用して、2つの異なるワークロード管理グループを作成して、2つのデータ分析プロセスを設定する。 (正解)
- ○ Amazon SQSによるキューイングプロセスをAmazon Redshift のプロセスに適用して、2つのデータ分析プロセスを並列処理できるようにする。
- ○ Amazon Redshift のマルチクラスター構成を利用して、2つの異なるクラスターグループを作成して、2つのデータ分析プロセスを設定する。
- ○ Amazon Redshift のAutoScalingを有効化して、2つの異なるマネジメントグループを作成して、2つのデータ分析プロセスを設定する。

説明

オプション1が正解となります。Amazon Redshift のワークロード管理 (WLM) を使用すると、ユーザーはワークロード内の優先順位を柔軟に管理して、短くて実行速度の速いクエリが実行時間の長いクエリの後に溜まらないように管理できます。これにより、2つの異なるワークロード管理グループを作成して、2つのデータ分析プロセスを設定することができます。

Amazon Redshift WLM はサービスクラスに従って実行時にクエリキューを作成します。サービスクラスでは、内部システムキューやユーザーアクセス可能キューなどのさまざまな種類のキューに対する設定パラメータが定義されています。ユーザーがクエリを実行すると、WLM はユーザーのユーザーグループに従ってクエリをキューに割り当てるか、キューの設定でリストされているキューグループとユーザーが実行時に設定したキューグループラベルを照合することによってクエリをキューに割り当てます。

オプション2は不正解です。Amazon SQSによるキューイングプロセスをAmazon Redshift のプロセスに適用して、処理をポーリングさせることは可能ですが、Redshift自体の機能であるWLMを利用して優先度を設定する方が効率的かつ容易に構成することが可能です。

オプション3は不正解です。Amazon Redshift のマルチクラスター構成を利用して、2つの異なるクラスターグループを作成するといった設定方法はありません。

オプション4は不正解です。Amazon Redshift の同時実行スケーリング機能を有効化にすることで、伸縮自在にクエリ処理力を自動でスケーリングして一貫性のある高速パフォーマンスを提供し、何百ものクエリを同時に処理できます。同時実行スケーリングのリソースが増加するにつれ、ご利用の Redshift クラスターに数秒で透過的に追加されるため、待機することなくクエリを処理できます。これによって、処理負荷に対応することが可能ですが、2つにワークプロセスが影響を与えないように分割する方が最適な対応となるため不正解です。

問題52: 不正解

あなたの企業はAWSを利用したデータウェアハウスを構築して、業務データ解析を経営に活かしています。あなたはソリューションアーキテクトとして、データ分析作業を効率化するためにAmazon Redshiftに保存されているデータの分析ワークロード処理用の新しいモバイルアプリケーションを開発しています。このアプリケーションがAmazon Redshiftクラスターにアクセスするために、実用的でセキュリティの高い最適な方法を検討しています。

この要件を満たすために最適なソリューションを選択してください。

- ◉ RedshiftクラスターがHSM証明書を使用してクライアントのHSMに接続し、クラスターデータベースの暗号化に使用されるキーを保存および取得する (不正解)
- ○ RedshiftクラスターがIAMロールを使用してクライアントのHSMに接続し、クラスターデータベースの暗号化に使用されるキーを保存および取得する
- ○ Redshiftへの読み取り専用ポリシーを作成してIAMユーザーに付与して、AWSリソースにアクセスするためにアプリケーションに認証キーを埋め込む
- ○ Redshiftへの最小特権アクセスを許可するIAMロールを作成して、ウェブIDフェデレーションによってID認証を行って、Redshiftへ一時アクセスを許可する認証情報をユーザーに与える。 (正解)

説明

分析用アプリケーションに対してRedshiftへの最小特権アクセスを許可するためには、そのアクセス権限ポリシーを有したIAMロールを作成して、ウェブIDフェデレーションによるID認証でRedshiftへの一時アクセス許可をユーザーに与えることで、必要な設定を実現することができます。したがって、オプション4が正解となります。

IAMロールはAWSリソースへの最小特権アクセスを許可し、ウェブIDフェデレーションはユーザーIDを保証し、AWSリソースにアクセスするための一時的な認証情報がユーザーに与えられることによって、AWSリソースへのアクセスを認証することができます。

オプション1と2は不正解です。ハードウェアセキュリティモジュール(HSM)では、不正使用防止策の施されたハードウェアデバイス内での、安全なキー保管と暗号化操作が可能になります。これはデータ暗号化に利用される仕組みです。

オプション3は不正解です。Redshiftへの読み取り専用ポリシーを作成してIAMユーザーではなく、IAMロールを設定する必要があります。

問題53: 不正解

あなたの会社はデータセンターにインフラ構成をホストして利用しています。ライセンス付ソフトウェアを仮想サーバー内で複数利用しており、それには単一のMACアドレスが添付されています。最近になって、会社はこれらのインフラ環境をAWSへと移行するを決定しました。その際は、EC2インスタンスにこれらのソフトウェアをインストールして利用を継続する予定です。新しいインスタンスの起動中に新しいMACアドレスを受信できるようにするため、EC2インスタンスがライセンス用に単一のMACアドレスを維持できるようにする必要があります。

この要件を満たすことができる最適なソリューションを選択してください。

- ◉ Elastic IPアドレスを作成してEC2インスタンスにアタッチしてElastic IPアドレスにMACアドレスを付与する。これにより、既存のEC2インスタンスを停止した場合に、新しいインスタンスに再アタッチできるようにする。 (不正解)
- ○ ENIを作成してEC2インスタンスにアタッチしてENIにMACアドレスを付与する。これにより、既存のEC2インスタンスを停止した場合に、新しいインスタンスに再アタッチできるようにする。 (正解)
- ○ MACアドレスを各EC2インスタンスに付与して、自動でMACアドレスをディタッチとアタッチすることで新しいEC2インスタンスに付与する。
- ○ プライベートサブネットにMACアドレスを付与して、そのサブネット内にEC2インスタンスを起動する。これにより、既存のEC2インスタンスを停止した場合に、新しいインスタンスを当該サブネット内に起動することができる。

説明

EC2インスタンスにMACアドレスを付与する場合はElastic Network Interface（ENI）を使用します。EC2がそのENIを有している限り、MACアドレスは変更されません。Elastic Network Interfaceは、仮想ネットワークカードを表す VPC 内の論理ネットワーキングコンポーネントです。 ネットワークインターフェイスには以下の属性を含めることができます。

- VPC の IPv4 アドレス範囲からのプライマリプライベート IPv4 アドレス
- VPC の IPv4 アドレス範囲からの 1 つ以上のセカンダリプライベート IPv4 アドレス
- プライベート IPv4 アドレスごとに 1 つの Elastic IP アドレス (IPv4)
- 1 つのパブリック IPv4 アドレス
- 1 つ以上の IPv6 アドレス
- 1 つ以上のセキュリティグループ
- MAC アドレス
- 送信元/送信先チェックフラグ

したがって、MACアドレスを持つENIをEC2インスタンスに割り当てることができるため、オプション2が正解となります。

オプション 1 は不正解です。EC2インスタンスにアタッチしてElastic IPアドレスにMACアドレスを付与するといった設定はできません。

オプション 3 は不正解です。MACアドレスを直接に各EC2インスタンスに付与するといった設定はできません。

オプション 4 は不正解です。プライベートサブネットにMACアドレスを付与するといった設定はできません。

問題64: 不正解

あなたはAIを利用したレントゲン写真診断システムを構築しているヘルステックベンチャー企業のソリューションアーキテクトです。このベンチャー企業の診断システムではレントゲン写真の蓄積処理段階において入力ストリームで画像を分析し、ファイルごとに結果データを出力ストリームに書き込みます。1日あたりの入力ファイル数は増加しつづけており、入力データの保存先としてはEBSボリュームを持つEC2インスタンスを使用していますが、ピーク時にはそのデータ量を保存しきれなくなっています。また、大量の画像データを処理するため、その処理時間が膨大にかかっていることも問題です。

入力データ処理時間を短縮し、ソリューションの可用性を向上させるための最適なアーキテクチャを選択してください。

- ◉ I/OファイルをプロビジョンドIOPS EBSに蓄積して、SQSによってEC2インスタンスのホストサーバーによる並行処理できるようにする。実行用のEC2インスタンスはSQSキューの処理要求の増加に応じてAutoScalingグループでスケーリングする。 (不正解)
- ○ I/OファイルをプロビジョンドIOPS EBSに蓄積して、AutoScalingグループに接続したEC2インスタンスのホストサーバーによってデータ処理を実現する。
- ○ I/OファイルをEBSではなくS3バケットに蓄積して、AutoScalingグループに接続したEC2インスタンスのホストサーバーによって処理する。このデータ処理はSNSによって並行処理できるようにする。
- ○ I/OファイルをEBSではなくS3バケットに蓄積して、SQSによってEC2インスタンスのホストサーバーによる並行処理できるようにする。実行用のEC2インスタンスはSQSキューの処理要求の増加に応じてAutoScalingグループでスケーリングする。 (正解)

説明

このシナリオでは、I/OファイルをEBSボリュームに蓄積・処理するのが限界にきていることがわかります。そのため、より容量と耐久性の高いストレージとしてS3バケットに変更します。プロビジョンドIOPS EBSはプロビジョンドIOPSの最大性能は64,000 IOPS、1,000 MB/sのスループットを設定可能な高性能はストレージで、EC2インスタンス上で常にデータ変動があり、I/O処理が多い場合に最適なストレージタイプです。しかしながら、今回のケースでは、画像診断システム用の画像入力データを蓄積することが主要な利用方法であり、データ蓄積に画像コンテンツを無制限に蓄積できるS3バケットを利用するべきです。

次に画像を処理するEC2インスタンスの処理性能も限界にきていることがわかります。ここでは、EC2インスタンスのAutoScalingは全体的な処理時間を短縮し、SQSはコマンド/タスクをEC2インスタンスのグループに分散することで、可用性を高めることができます。したがって、これらの要素を取り入れたアーキテクチャであるオプション4が正解です。

オプション1と2はEBSボリュームにデータを蓄積しており、最適なソリューションとは言えないため不正解です。

オプション3はSQSではなく、SNSによる負荷分散を実施しており、不適切です。SNSはメッセージングによる処理連携を実装することはできますが、プッシュ通知がメインであり、ポーリング処理による並行稼働に利用できるSQSを選択する必要があります。

問題55: 正解

A社はグローバルな保険会社で、この会社の保険申請システムはグローバルに利用されています。様々な国からアクセスしてくる顧客に応じるために、A社が保管しているデータは増え続けるため、既存のテープベースのバックアップインフラストラクチャからAWSクラウドにデータをアーカイブすることになりました。あなたはソリューションアーキテクトとして、耐久性があり費用対効果の高いソリューションを構築することを要求されています。

この要件に対応するための最適な方法を選択してください。

- ◉ Amazon S3データへのバックアップ接続するためのテープゲートウェイを設定して、既存のテープベースのバックアップインフラストラクチャを利用してAmazon Glacierにデータを保存する。 (正解)
- ○ Amazon S3データへのバックアップ接続するための保管型ゲートウェイを設定して、iSCSIを介してAmazon Glacierにデータを保存する。
- ○ Amazon S3データへのバックアップ接続するためのキャッシュ型ゲートウェイを設定して、iSCSIを介してAmazon Glacierにデータを保存する。
- ○ Amazon S3データへのバックアップ接続するためのテープゲートウェイを設定して、DatePipelineを利用して仮想テープライブラリーにデータを保存する。

説明

今回のケースでは、既存のオンプレミス環境にあるテープベースのバックアップからAWSクラウドにデータをアーカイブするため方法へと移行します。Amazon S3にあるデータに対してバックアップ用テープゲ　トウェイを設定することで、既存のテープベースのバックアップインフラストラクチャからAmazon Glacierにデータを保存することができます。したがって、オプション１が最適な選択肢となります。

テープゲートウェイ は、データを AWS クラウドにアーカイブすることで、耐久性が高く、コスト効率的なソリューションを提供します。仮想テープライブラリ (VTL) のインターフェイスを使用することで、既存のテープベースのバックアップインフラストラクチャを利用して、テープゲートウェイ 上に作成する仮想テープカートリッジにデータを保存できます。各 テープゲートウェイ にはメディアチェンジャーとテープドライブがあらかじめ組み込まれています。これらは、既存のクライアントバックアップアプリケーションから iSCSI デバイスとして利用できます。データをアーカイブするには、必要に応じてテープカートリッジを追加します。

オプション２と３は間違いです。キャッシュ型ゲートウェイや保管型ゲートウェイはテープライブラリーのデータバックアップには利用できません。

オプション４は間違いです。DatePipelineを利用して仮想テープライブラリーにデータを保存するといった設定方法はできません。

問題56: 不正解

大手メディア企業は著名人とコメントのやり取りができる相互的なニュースメディアサービスを立ち上げました。このニュースポータルはELBとAutoScalingグループを設定したオンデマンドEC2インスタンス群によって実行されます。AutoScalingによって起動されるEC2インスタンスにはスポットインスタンスが利用されます。社内アプリケーションとの連携のために、ニュースポータルのデータベースはオンプレミスのデータセンターで実行されています。しかしながら、このデータベースを利用したコンテンツ配信処理のレイテンシーが企業の目標を達成していません。クライアントビューワーによるコンテンツ読込処理には問題がなく、バックエンド処理のコメントデータの読込処理に時間を要しているようです。

このニュースポータルのユーザーの読み込み時間を短縮するために、最も適切なアーキテクチャはどれですか？

- ◉ オンプレミス環境のデータベースに対してCloudFrontディストリビューションを設定して、ニュース配信をキャッシュ処理によって実施する。 (不正解)
- ○ オンプレミス環境のデータベースに対してAmazon ElastiCache Memcachedのインメモリキャッシュを連携してネットワークレイテンシーを削減し、データベースの負荷を軽減する。Memcachedレプリケーションを有効化して、高可用クラスター構成とする。
- ○ オンプレミス環境のデータベースに対してAmazon ElastiCache Redisのインメモリキャッシュを連携してネットワークレイテンシーを削減し、データベースの負荷を軽減する。Redisレプリケーションを有効化して、高可用クラスター構成とする。 (正解)
- ○ オンプレミスデータベースをAmazon Auroraに移行しデータベース処理能力を向上させる。Amazon Auroraはリードレプリカを最大15個まで設置することが出来るため、ユーザーからの読み取り処理能力を大きく向上させることができる。

説明

このシナリオでは、ニュースポータルの読込時間が長くなっているのが問題となっています。クライアントビューワーによるコンテンツ読込処理には問題がありませんが、原因はバックエンド処理のコメントデータの読込処理が追い付いていないことにあります。したがって、バックエンドデータベースへのレイテンシーが関係しているため、正しい答えはAmazon ElastiCacheに基づいたメモリ内キャッシュを使用してネットワークレイテンシーを削減し、データベースの負荷を軽減することです。Amazon ElastiCacheはオンプレミス環境のデータベースと連携してキャッシュ処理を実行することが可能です。

【参照】

Amazon ElastiCache を使用して、ハイブリッド型アーキテクチャのレイテンシーを削減する | Amazon Web Services ブログ

このソリューションにより、データ取得の待ち時間が大幅に短縮されます。また、Amazon ElastiCacheは秒あたり2,000万を超える非常に高いリクエストレートを提供できるため、リクエスト量も大幅にスケーリングします。Elasticacheの設定としては、Redisを選択してインメモリキャッシュを使用してネットワークレイテンシを削減し、データベースの負荷を軽減し、Redisレプリケーションを有効化して、高可用クラスター構成とすることが望ましいです。

したがって、オプション３が正解となります。

オプション1は不正解です。CloudFrontディストリビューションはコンテンツの配信処理を向上させることができますが、バックエンドデータベースへのレイテンシーが遅延原因となっているため、問題の解決になっていません。

オプション２は不正解です。このシナリオでは、RedisもMemcachedもどちらも利用できるケースです。しかしながら、レプリケーション機能はMemcachedにはないため、間違った設定方法となっています。

オプション４は不正解です。ニュースポータルで現在使用されているデータベースエンジンがAmazon Auroraでサポートされている保証がないため、正しくありません。Auroraに移行するためにはMySQLかPosgreSQLの互換性のあるバージョンが利用されていることが重要です。

問題57: 正解

あなたの会社はキャッシュレス決済アプリを運用するフィンテック企業です。このアプリでは、１つ１つのトランザクション処理を効率的にコスト最適に実行するためにDynamoDB Streamsと統合されたLambda関数を使用しています。このLambda関数の新バージョンを展開する際はCodeDeployを使用して、Lambda関数への着信トラフィックを増分形式でシフトする必要があります。新バージョン移行時のトラブルを避けるために、段階的移行を実施しており、着信トラフィックの20%を新しいバージョンにシフトし、残りの80%を20分後に展開する移行方式をとっています。また、Lambda関数が行ったダウンストリーム呼び出しを含む、Lambda関数の呼び出したイベントソースを追跡する必要があります。

この問題に対応するための最も適切なAWSリソースの設定方法はどれですか？

- ◉ **CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する** (正解)
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ **CodeDeployの設定タイプで [Linear] を指定して、[Interval (間隔)] を２０分と設定する。**
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ **Lamdbaの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する。**
  Lambda関数でデプロイステータスの追跡を有効化する。
- ○ **Lamdbaの設定タイプで [Linear] を指定して、[Interval (間隔)] を２０分と設定する。**
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ **CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する**
  Lambda関数でデプロイステータスの追跡を有効化する。

説明

オプション１が正解となります。 CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定することで、着信トラフィックの20%を新しいバージョンにシフトし、残りの80%を20分後に展開することが可能となります。また、CodeDeployでデプロイステータスの追跡を有効化することで、Lambda関数のコールしたイベントソースを追跡することができます。

AWS CodeDeployを利用してAWS Lambdaコンピューティングプラットフォームにデプロイする場合、デプロイ構成によって、アプリケーションの新しいLambda関数バージョンにトラフィックをシフトする方法を指定することができます。[Interval (間隔)] には時間 (分数) を入力します。設定タイプが [Canary] の場合、この値は最初と２回目のトラフィック移行の時間 (分) を示します。設定タイプが [Linear (リニア)] の場合、この値は各増分の移行間の時間 (分) を示します。

AWS CodeDeployでデプロイのステータスは追跡を有効化にすることで、 AWS マネジメントコンソール、 AWS コマンドラインインターフェイス (AWS CLI)、 AWS SDK、 AWS CodeDeploy API を使用して追跡できます。デプロイ全体のステータスを確認することも、各インスタンスのステータス、およびインスタンスの各デプロイのライフサイクルイベントのステータスを詳しく確認することもできます。また、失敗に対応するログエントリも確認できるため、インスタンスにログインする必要がなく、デプロイの問題のデバッグが容易になります。

オプション２は不正解です。CodeDeployの設定タイプで [Linear] を指定した場合は、[Interval (間隔)] の値は各増分の移行間の時間 (分) を示すため、移行間隔をずらすには CodeDeployの設定タイプで [Canary]を指定する必要があります。

オプション３と４は不正解です。Lamdbaの設定タイプではなく、CodeDeployの設定タイプで [Canary]を指定する必要があります。

問題58: 不正解

ある会社ではデータウェアハウスとしてRedshiftを利用したOLTP分析アプリケーションの構築を行っています。あなたはソリューションアーキテクトとして、このアプリケーションの構築を担当しており、EC2やS3などの基本構成に加えて、データ分析用のRedshift WLMキューなどのAWSリソースを設定しました。チームはコーディング作業を完了し、AWSにこのアプリケーションをデプロイしました。しかしながら、起動後にRedshift上でクエリがまったく応答しなくなるトラブルが発生してしまいました。

この問題を解決する可能性がある、Redshiftの対処方法を選択してください。（2つ選択してください。）

- [x] VACUUM コマンドを実行して、データが再編成されてソート順序が維持され、パフォーマンスが復旧される。 (不正解)
- [x] STL_LOAD_ERRORS にクエリして、特定のロード中に発生したエラーを見つける。 (不正解)
- [ ] 並列処理を最大限に活用できるようにテーブルのソートキー、分散スタイル、および圧縮エンコードを設定する。
- [ ] カーソルを使用して、結果セットをクライアントアプリケーションに返す。 (正解)
- [ ] 最大送信単位 (MTU) のサイズを小さくする。 (正解)

説明

このシナリオでは、Amazon Redshift クエリ処理で発生する可能性のある一般的な問題と重大な問題を特定し、それらの問題に対処することが求められています。起動後に問題なく動いていたはずのRedshiftで、しばらくしてクエリがまったく応答しなくなるトラブルの原因としては、「クエリがハングした」可能性が高いです。したがって、今回のケースでは、以下の選択肢から合致する内容としてオプション４と５が対処方法となりえます。

クエリがハングする

■データベースへの接続が中断された 最大送信単位 (MTU) のサイズを小さくします。MTU サイズにより、ネットワーク接続を介して 1 つのイーサネットフレームで転送できるパケットの最大サイズ (バイト単位) が決まります。

■データベースへの接続がタイムアウトした COPY コマンドなどの長いクエリを実行すると、データベースへのクライアント接続がハングまたはタイムアウトしているように見えます。この場合、Amazon Redshift コンソールにはクエリが完了したと表示されますが、クライアントツール自体はまだクエリを実行しているように見えることがあります。接続がいつ停止したかに応じて、クエリの結果がないか、不完全になる可能性があります。この効果は、中間ネットワークコンポーネントによってアイドル接続が終了すると発生します。

■ODBC 使用時にクライアント側のメモリ不足エラーが発生する クライアントアプリケーションが ODBC 接続を使用し、クエリで作成される結果セットが大きすぎてメモリが足りなくなる場合、カーソルを使用して、結果セットをクライアントアプリケーションに返すことができます。

■JDBC 使用時にクライアント側のメモリ不足エラーが発生する JDBC 接続で大規模な結果セットを取得しようとすると、クライアント側のメモリ不足エラーが発生する可能性があります。

クエリに時間がかかりすぎる場合は、今回のエラー内容と異なるため、以下の対応は不正解となります。

■テーブルが最適化されていない 並列処理を最大限に活用できるようにテーブルのソートキー、分散スタイル、および圧縮エンコードを設定します。

■クエリがディスクに書き込みを行っている クエリが少なくともクエリ実行の一部でディスクに書き込みを行っている可能性があります。詳細については、「クエリパフォーマンスの向上」を参照してください。

■クエリが他のクエリの終了を待つ必要がある クエリキューを作成し、別の種類のクエリを適切なキューに割り当てることで、システムの全体的なパフォーマンスを改善できる可能性があります。

■クエリが最適化されていない 説明プランを分析して、クエリを書き換えることが可能かどうか、またはデータベースを最適化することが可能かどうかを調べます。

■クエリの実行により多くのメモリが必要である 特定のクエリにより多くのメモリが必要な場合は、wlm_query_slot_count を増やすことによって使用可能なメモリを増やすことができます。

■データベースに対して VACUUM コマンドを実行する必要がある 大量の行数を追加、削除、変更した場合、データをソートキー順序でロードしていなければ、VACUUM コマンドを実行します。VACUUM コマンドを実行すると、データが再編成され、ソート順序が維持され、パフォーマンスが復旧されます。

問題57: 正解

あなたの会社はキャッシュレス決済アプリを運用するフィンテック企業です。このアプリでは、１つ１つのトランザクション処理を効率的にコスト最適に実行するためにDynamoDB Streamsと統合されたLambda関数を使用しています。このLambda関数の新バージョンを展開する際はCodeDeployを使用して、Lambda関数への着信トラフィックを増分形式でシフトする必要があります。新バージョン移行時のトラブルを避けるために、段階的移行を実施しており、着信トラフィックの20%を新しいバージョンにシフトし、残りの80%を20分後に展開する移行方式をとっています。また、Lambda関数が行ったダウンストリーム呼び出しを含む、Lambda関数の呼び出したイベントソースを追跡する必要があります。

この問題に対応するための最も適切なAWSリソースの設定方法はどれですか？

- ◉ CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する (正解)
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ CodeDeployの設定タイプで [Linear] を指定して、[Interval (間隔)] を２０分と・設定する。
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ Lamdbaの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する。
  Lambda関数でデプロイステータスの追跡を有効化する。
- ○ Lamdbaの設定タイプで [Linear] を指定して、[Interval (間隔)] を２０分と設定する。
  CodeDeployでデプロイステータスの追跡を有効化する。
- ○ CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定する
  Lambda関数でデプロイステータスの追跡を有効化する。

説明

オプション１が正解となります。 CodeDeployの設定タイプで [Canary] を指定して、[Interval (間隔)] を２０分と設定することで、着信トラフィックの20%を新しいバージョンにシフトし、残りの80%を20分後に展開することが可能となります。また、CodeDeployでデプロイステータスの追跡を有効化することで、Lambda関数のコールしたイベントソースを追跡することができます。

AWS CodeDeployを利用してAWS Lambdaコンピューティングプラットフォームにデプロイする場合、デプロイ構成によって、アプリケーションの新しいLambda関数バージョンにトラフィックをシフトする方法を指定することができます。[Interval (間隔)] には時間 (分数) を入力します。設定タイプが [Canary] の場合、この値は最初と２回目のトラフィック移行の時間 (分) を示します。設定タイプが [Linear (リニア)] の場合、この値は各増分の移行間の時間 (分) を示します。

AWS CodeDeployでデプロイのステータスは追跡を有効化にすることで、 AWS マネジメントコンソール、 AWS コマンドラインインターフェイス (AWS CLI)、 AWS SDK、 AWS CodeDeploy API を使用して追跡できます。デプロイ全体のステータスを確認することも、各インスタンスのステータス、およびインスタンスの各デプロイのライフサイクルイベントのステ　タスを詳しく確認することもできます。また、失敗に対応するログエントリも確認できるため、インスタンスにログインする必要がなく、デプロイの問題のデバッグが容易になります。

オプション２は不正解です。CodeDeployの設定タイプで [Linear] を指定した場合は、[Interval (間隔)] の値は各増分の移行間の時間 (分) を示すため、移行間隔をずらすにはCodeDeployの設定タイプで [Canary]を指定する必要があります。

オプション３と４は不正解です。Lamdbaの設定タイプではなく、CodeDeployの設定タイプで [Canary]を指定する必要があります。

問題58: 不正解

ある会社ではデータウェアハウスとしてRedshiftを利用したOLTP分析アプリケーションの構築を行っています。あなたはソリューションアーキテクトとして、このアプリケーションの構築を担当しており、EC2やS3などの基本構成に加えて、データ分析用のRedshift WLMキューなどのAWSリソースを設定しました。チームはコーディング作業を完了し、AWSにこのアプリケーションをデプロイしました。しかしながら、起動後にRedshift上でクエリがまったく応答しなくなるトラブルが発生してしまいました。

この問題を解決する可能性がある、Redshiftの対処方法を選択してください。 (2つ選択してください。)

- [x] VACUUMコマンドを実行して、データが再編成されてソート順序が維持され、パフォーマンスが復旧される。 (不正解)
- [x] STL_LOAD_ERRORSにクエリして、特定のロード中に発生したエラーを見つける。 (不正解)
- [ ] 並列処理を最大限に活用できるようにテーブルのソートキー、分散スタイル、および圧縮エンコードを設定する。
- [ ] カーソルを使用して、結果セットをクライアントアプリケーションに渡す。 (正解)
- [ ] 最大送信単位(MTU)のサイズを小さくする。 (正解)

説明

このシナリオでは、Amazon Redshift クエリ処理で発生する可能性のある一般的な問題と重大な問題を特定し、それらの問題に対処することが求められています。起動後に問題なく動いていたはずのRedshiftで、しばらくしてクエリがまったく応答しなくなるトラブルの原因としては、「クエリがハングした」可能性が高いです。したがって、今回のケースでは、以下の選択肢から合致する内容としてオプション4と5が対処方法となりえます。

クエリがハングする

■データベースへの接続が中断された 最大送信単位 (MTU) のサイズを小さくします。MTU サイズにより、ネットワーク接続を介して 1 つのイーサネットフレームで転送できるパケットの最大サイズ (バイト単位) が決まります。

■データベースへの接続がタイムアウトした COPY コマンドなどの長いクエリを実行すると、データベースへのクライアント接続がハングまたはタイムアウトしているように見えます。この場合、Amazon Redshift コンソールにはクエリが完了したと表示されますが、クライアントツール自体はまだクエリを実行しているように見えることがあります。接続がいつ停止したかに応じて、クエリの結果がないか、不完全になる可能性があります。この効果は、中間ネットワークコンポーネントによってアイドル接続が終了すると発生します。

■ODBC 使用時にクライアント側のメモリ不足エラーが発生する クライアントアプリケーションが ODBC 接続を使用し、クエリで作成される結果セットが大きすぎてメモリが足りなくなる場合、カーソルを使用して、結果セットをクライアントアプリケーションに渡すことができます。

■JDBC 使用時にクライアント側のメモリ不足エラーが発生する JDBC 接続で大規模な結果セットを取得しようとすると、クライアント側のメモリ不足エラーが発生する可能性があります。

クエリに時間がかかりすぎる場合は、今回のエラー内容と異なるため、以下の対応は不正解となります。

■テーブルが最適化されていない 並列処理を最大限に活用できるようにテーブルのソートキー、分散スタイル、および圧縮エンコードを設定します。

■クエリがディスクに書き込みを行っている クエリが少なくともクエリ実行の一部でディスクに書き込みを行っている可能性があります。詳細については、「クエリパフォーマンスの向上」を参照してください。

■クエリが他のクエリの終了を待つ必要がある クエリキューを作成し、別の種類のクエリを適切なキューに割り当てることで、システムの全体的なパフォーマンスを改善できる可能性があります。

■クエリが最適化されていない 説明プランを分析して、クエリを書き換えることが可能かどうか、またはデータベースを最適化することが可能かどうかを調べます。

■クエリの実行により多くのメモリが必要である 特定のクエリにより多くのメモリが必要な場合は、wlm_query_slot_count を増やすことによって使用可能なメモリを増やすことができます。

■データベースに対して VACUUM コマンドを実行する必要がある 大量の行数を追加、削除、変更した場合、データをソートキー順序でロードしていなければ、VACUUM コマンドを実行します。VACUUM コマンドを実行すると、データが再編成され、ソート順序が維持され、パフォーマンスが復旧されます。

問題59: 不正解

あなたはAWS専門のエンジニアとして、IoTデータをキャプチャしてAmazon Kinesis Data Streamsに送信するモバイルアプリケーションを構築しています。このアプリケーションは、EC2インスタンスにKCLを組み込んでKinesisと連携しています。カスタムメトリックに基づいて、インスタンスがCPU使用率を最大限に活用しており、Amazon Kinesis Data Streamsに流れるデータレートを処理するにはKinesisのシャードが不十分なようです。

この問題を解決するためのソリューションを選択してください。（2つ選択してください。）

- [x] 利用しているEC2インスタンスのインスタンスサイズを増強する。 (正解)
- [ ] Kinesisのシャードを分割する。 (正解)
- [ ] Kinesisのシャードをマージする。
- [ ] 利用しているEC2インスタンスのEBSボリュームを増強する。
- [ ] Kinesisストリームを有効化する。

説明

イプション１と２が正解となります。Amazon Kinesis Data Streamsに流れるデータレートを処理する際に、Kinesisシャードが不十分な場合には、リシャーディングによりシャードを分割するか、インスタンスサイズを増強するかで対応することでパフォーマンスを向上させることができます。

■リシャーディング

シャードの分割では１つのシャードを２つシャードに分けます。シャードの結合では、２つシャードを１つのシャードに組み合わせます。リシャーディングは、1回のオペレーションでシャードに分割できる数と1回のオペレーションで結合できるシャードの数が２個以下に限られるという意味で、常にペアワイズです。リシャーディングオペレーションの対象となるシャードまたはシャードペアは、親シャードと呼ばれます。リシャーディングオペレーションを実行した結果のシャードまたはシャードペアは、子シャードと呼ばれます。分割によりストリーム内のシャードの数が増え、したがってストリームのデータ容量は増えます。シャード単位で請求されるため、分割によりストリームのコストが増えます。

■シャードに合わせたインスタンスサイズの増強

Kinesisストリーム内のインスタンスのサイズとシャード数を増やすことで、インスタンスがインスタンス内で並行して実行されるより多くのレコードプロセッサを処理できるようにします。また、ストリームが送信されるデータのレートに適切に対応できるようにします。ストリームのデータ容量は、ストリームに指定するシャードの数の関数です。

オプション３は不正解です。Kinesisのシャードをマージすることによって、逆に処理能力を落とすことができます。

オプション４は不正解です。EC2インスタンスのEBSボリュームは、あくまでもEC2インスタンスのデータ処理能力であり、Kinesisのストリーム処理能力を高める場合は、インスタンスサイズを増強させることが必要です。

オプション５は不正解です。Kinesisストリームはそもそも実行されており、有効化という概念はありません。

問題60: 不正解

あなたが開発したサーバーレスアプリケーションは、複数のAPI Gatewayを利用してアプリケーションのリリースライフサイクルごとにLambdaを呼び出して、ユーザーから送信されたアドホックリクエストを処理します。このアプリのリリースは段階的に、テストリリース、本番リリースなど複数のリリースを実施するため、単一のAPIゲートウェイに統合する必要があります。たとえば、クライアントはtest.pintor.comエンドポイントとmain.pintor.testエンドポイントを介したテスト版リリースを使用して、本番リリースに接続できる必要があります。

この要件を達成するために必要な設定方法を選択してください。

- ◉ 各リリースにおいてリリース変数を設定する。 (不正解)
- ○ 各リリースにおいてステージ変数を設定する。 (正解)
- ○ API Gatewayコンソールにおけるマッピングテンプレートを利用してリリース後の関係性を設定する。
- ○ API Gatewayコンソールにおける関連性変数でリリース後の関係性を設定する。
- ○ Lambda関数のレイヤー機能を利用して、複数レイヤーに各リリースバージョンを分割設定する。

説明

ステージ変数は、REST API のデプロイステージと関連付けられた設定属性として定義できる名前と値のペアです。環境変数と同様に機能し、API のセットアップやマッピングテンプレートで使用できます。各リリースにおいてステージ変数を設定することで、リリースの段階を管理することができます。したがって、オプション 2 が正解となります。

API Gateway のデプロイステージでは、アルファ、ベータ、プロダクションなど、各 API 用の複数のリリースステージを管理できます。ステージ変数を使用することで、異なるバックエンドのエンドポイントとやり取りするよう API デプロイステージを設定できます。それによって、test.pintor.comエンドポイントとmain.pintor.testエンドポイントを介したテスト版リリースを使用して、本番リリースに接続するといった設定が可能です。

オプション 1 は不正解です。各リリースにおいて設定するリリース変数という変数はありません。

オプション 3 は不正解です。API Gatewayコンソールにおけるマッピングテンプレートというものを利用して、リクエストとレスポンスのデータマッピングをセットアップすることができます。これはリリース段階を管理するために利用されないため、正しくありません。

オプション 4 は不正解です。API Gatewayコンソールにおける関連性変数といった変数はありません。

オプション 5 は不正解です。Lambda関数のレイヤー機能を利用して、複数レイヤーに各リリースバージョンを分割設定するといった対応はできません。これは、複数のLambda関数でライブラリを共有する仕組みです。

問題61: 不正解

あなたの会社はグローバルコンサルティング企業であり、顧客ポータルをAWSにホストして利用しています。このポータルはAuto Scalingグループが設定されたEC2インスタンスで構成されており、複数のAWSリージョンに展開されています。最近1つのリージョンで、大きな停電が発生したことで、顧客ポータルサイトに長時間のダウンタイムを発生させてしまいました。こうした、ダウンタイムがほとんど発生しないタイプのフェールオーバー構成が不可欠となっています。

このアプリケーションのダウンタイムを回避するために最適なインフラストラクチャーを選択してください。

- ◉ Route53のレイテンシールーティングを選択してDNSアクティブ/アクティブ・フェールオーバーを構成して、ELBをターゲットに指定する。ターゲットの"Evaluate Target Health"の設定をFalseに有効化する。 (不正解)
- ○ Route53のレイテンシールーティングを選択してDNSアクティブ/パッシブ・フェールオーバーを構成して、ELBをターゲットに指定する。ターゲットの"Evaluate Target Health"の設定をFalseに有効化する。
- ○ Route53のレイテンシールーティングを選択してDNSアクティブ/アクティブ・フェールオーバーを構成して、ELBをターゲットに指定する。 (正解) ターゲットの"Evaluate Target Health"の設定をTrueに有効化する。
- ○ Route53のレイテンシールーティングを選択してDNSアクティブ/パッシブ・フェールオーバーを構成して、ELBをターゲットに指定する。ターゲットの"Evaluate Target Health"の設定をTrueに有効化する。

説明

オプション3が正解となります。Route53のレイテンシールーティングを選択してDNSアクティブ/アクティブ・フェールオーバーを構成して、ELBをターゲットに指定し、ターゲットの"Evaluate Target Health"の設定をTrueに有効化することで、Route53によるアクティブ/アクティブフェールオーバー構成を実現できます。今回は、ダウンタイムがほとんど発生しないタイプのフェールオーバー構成が要件となっており、パッシブ系への切り替え時にダウンタイムが多少発生してしまうアクティブ/パッシブではなく、常に稼働している状態を維持できるアクティブ/アクティブ・フェールオーバーを構成することが必要です。アクティブ/アクティブ・フェールオーバーではRoute 53 を使用してリソースが正常な状態かどうかを確認し、DNS クエリに対する応答として正常なリソースのみ返るようにすることができます。

Route53を利用したDNS フェイルオーバーの以下の 2 つのタイプがあります。

■アクティブ/パッシブフェールオーバー

Route 53 のフェールオーバールーティングポリシーを利用したフェールオーバー方式です。プライマリリソースをアクティブに返します。エラーが発生すると、Route 53 はバックアップリソースを返します。フェイルオーバーポリシーを使用して設定されます。プライマリリソースまたはリソースグループをほとんどの時間で利用可能にして、すべてのプライマリリソースが使用できなくなった場合に備えて、セカンダリリソースまたはリソースグループをスタンバイ状態にする場合にフェイルオーバー (アクティブ/パッシブ) を使用します。クエリへの応答で Route 53 が返すのは、正常なプライマリリソースのみです。すべてのプライマリリソースで異常が発生した場合、Route 53 は、DNS クエリへの応答として、正常なセカンダリリソースのみを返します。

■アクティブ/アクティブフェールオーバー

Route 53 のヘルスチェック機能を利用したフェールオーバー方式です。ルーティングポリシーには様々なフェールオーバールーティング以外のルーティングポリシーを利用可能です。Route 53 は複数のリソースをアクティブに返します。エラーが発生すると、Route 53 は正常なリソースに戻します。フェイルオーバー (アクティブ/アクティブ)はすべてのリソースをほとんどの時間で利用できるようにします。リソースが利用できなくなると、そのリソースを Route 53 が異常として検出し、以後、クエリへの応答に含めることを控えます。

したがって、このシナリオでは、アクティブ/アクティブフェールオーバーを設定して、ターゲットの"Evaluate Target Health"の設定をTrueに有効化することが正解となります。

オプション1と2は不正解です。このシナリオに対する設定では、ELBをターゲットに指定し、ターゲットの"Evaluate Target Health"の設定をTrueに有効化することが求められます。

オプション4は不正解です。Route53のレイテンシールーティングを選択してDNS アクティブ/パッシブ・フェールオーバーを構成ではなく、DNS アクティブ/アクティブ・フェールオーバーを構成する必要があります。このシナリオではダウンタイムが発生しないことが求められています。アクティブ/パッシブの場合は待機系への切り替え時にダウンタイムが発生するため、ダウンタイムの発生がないアクティブアクティブを優先して選択します。

問題62: 不正解

大手製造業B社はデータセンター内で仮想マシンサーバーなどのインフラストラクチャーを利用して、複数のWEBアプリケーションをホストしています。そこで、あなたはソリューションアーキテクトとして、AWSへの移行計画を立案しています。所有コスト（TCO）分析を実行し、オンプレミスネットワークでAWSにホストされているシステムのコスト最適化移行計画が必要とされています。したがって、移行を行う前にオンプレミス上のワークロードを理解できるように、オンプレミスサーバーの構成、使用状況、および動作に関するデータを収集する必要があります。

この要件を満たすために最適なソリューションを選択してください。

- ◉ AWS Migration Supportを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成する。 (不正解)
- ○ AWS Prescriptive Guidanceを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成する。
- ○ AWS Server Migration Serviceを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成する。
- ○ AWS Application Discovery Serviceを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成する。 (正解)
- ○ AWS Migration HUBを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成する。

説明

オプション４が正解となります。AWS Application Discovery Serviceを利用してオンプレミスデータセンターの情報を収集し、そのデータに基づいてTCOを算出して移行計画を作成することができます。

ADSはオンプレミスデータセンターに関する情報を収集し、移行プロジェクト計画を立案することを支援するAWSサービスです。データセンター移行計画には何千ものワークロードが存在し、多くの場合それらが相互に深く依存しあっています。サーバーの使用率データや依存関係のマッピングは、移行プロセス初期の重要なステップです。ADSでは、サーバーの設定データ、使用状況データ、動作データが収集されて、ユーザーに提供されます。これにより、ユーザーはワークロードを十分に把握することができます。

収集されたデータは、ADS のデータストアに暗号化形式で保存されます。このデータを CSV ファイルとしてエクスポートし、AWS で稼働した場合の総所有コスト (TCO) の見積もりや、AWS への移行計画に使用できます。また、このデータは AWS Migration Hub でも利用できます。このサービスでは、検出したサーバーを AWS に移行し、AWS に移行する際の進捗を追跡できます。

オプション１は不正解です。AWS Migration Supportというサービスはありません。

オプション２は不正解です。AWS Prescriptive Guidanceは移行に関するガイダンスを提供しています。

オプション３は不正解です。AWS Server Migration Serviceは数千のオンプレミスワークロードを従来よりも簡単に、かつ短時間でAWSに移行できるエージェントレスサービスです。

オプション５は不正解です。AWS Migration Hub では、AWS およびパートナーの複数のソリューション間におけるアプリケーション移行の進行状況を１つの場所で追跡できます。Migration Hub を使用すると、ニーズに最も適する AWS およびパートナーの移行ツールを選択でき、アプリケーションのポートフォリオ全体で移行状態の可視性が得られます。Migration Hub では、移行にどのようなツールが使われていても、個々のアプリケーションの主要なメトリクスと進行状況を取得することもできます。

問題63: 不正解

ある会社はAPIを利用したアプリケーション間のデータ連携を他の会社と行っています。その際は、AWSの仕組みとしてAPI GatewayからLambdaファンクションを呼び出して、DynamoDBテーブルからデータを取得するサーバーレスアプリケーションを利用しています。アプリケーションは、オンラインオークションサービス用のもので、全期間を通じてリアルタイムで個々のユーザーとメッセージを送受信します。しかしながら、アプリケーションはHTTP 504エラーが度々発生するなど、ユーザーエクスペリエンスが損なわれるトラブルが発生しており、あなたは原因を調査して対応を検討しています。

この問題の最も可能性の高い原因を選択してください。（2つ選択してください。）

- [x] 実行中のLambdaファンクションが29秒以上処理時間を要している。 (正解)
- [ ] API GatewayにおけるINTEGRATION_FAILUREエラーが発生している。
- [ ] API GatewayにおけるINTEGRATION_TIMEOUTエラーが発生している。 (正解)
- [ ] LambdaファンクションにおけるINTEGRATION_TIMEOUTエラーが発生している。
- [ ] LambdaファンクションにおけるINTEGRATION_FAILUREエラーが発生している。

説明

このシナリオでは、ユーザーがオンラインオークションでHTTP 504エラーを受け取っているという断続的な問題があります。API Gatewayと統合したLambdaアプリケーション上でのHTTP 504エラー は、INTEGRATION_FAILUREまたはINTEGRATION_TIMEOUTのどちらかを意味しています。これは、Lambda関数が基本は正常に機能しているが、ときどき処理が遅れる場合があることを意味します。したがって、Lambda関数とAPI Gatewayとの統合失敗を示すINTEGRATION_FAILUREではなく、Lambdaファンクションが実行しない場合にのみINTEGRATION_TIMEOUTエラーが発生していると考えます。したがって、正しい答えはオプション3です。

API Gatewayのゲートウェイタイムアウトは定義された応答タイプによって識別されます。応答は、HTTPステータスコード、パラメーターマッピングで指定された追加ヘッダーのセット、および非VTL（Apache Velocity Template Language）マッピングテンプレートで生成されたペイロードで構成されます。APIレベルで、サポートされている応答タイプのゲートウェイ応答をセットアップできます。APIゲートウェイのHTTP 504エラーに関連付けられているゲートウェイ応答タイプは次のとおりです。

■INTEGRATION_FAILURE
統合失敗のゲートウェイ応答です。応答タイプが指定されていない場合、この応答はデフォルトでDEFAULT_5XXタイプになります。
■INTEGRATION_TIMEOUT
統合タイムアウトエラーのゲートウェイ応答です。応答タイプが指定されていない場合、この応答はデフォルトでDEFAULT_5XXタイプになります。

統合タイムアウトの範囲は、Lambda、Lambdaプロキシ、HTTP、HTTPプロキシ、AWS統合を含むすべての統合タイプの50ミリ秒から29秒です。実行中のLambdaファンクションが29秒以上処理時間を要している場合にはタイムアウトになってしまいます。したがって、オプション1も正解となります。

オプション2は不正解です。API GatewayにおけるINTEGRATION_FAILUREエラーが発生している場合は、基本的に統合自体に失敗しており、正常に動いていない場合です。

オプション4と5は不正解です。Lambdaファンクションにおけるエラーではなく、API Gatewayにおけるエラーになります。

問題64: 不正解

大手製造業B社では、データセンター内で仮想マシンを利用したサーバーなどのインフラストラクチャーを利用して、複数のWEBアプリケーションを運用しています。そこで、あなたはソリューションアーキテクトとして、オンプレミスネットワークでホストされているさまざまな多層アプリケーションを管理しています。今後は、クラウドコンピューティングを活用するために、経営陣は全システムをAWSに移行することを決定しました。その際には、MQTTメッセージングプロトコルをサポートするActiveMQメッセージングブローカーサービスをリプラットフォーム形式でAWSに移行する必要があります。

最小構成でメッセージングサービスを移行するために最適なソリューションを選択してください。

- (●) Amazon SNSを利用して既存の多層アプリケーションのメッセージングブローカーとして利用する。 (不正解)
- ( ) Amazon MQを利用して既存の多層アプリケーションのメッセージングブローカーとして利用する。 (正解)
- ( ) Amazon SQSを利用して既存の多層アプリケーションのメッセージングブローカーとして利用する。
- ( ) Amazon SESを利用して既存の多層アプリケーションのメッセージングブローカーとして利用する。

説明

オプション2が正解です。Amazon MQ、Amazon SQS、およびAmazon SNSはAWS上で利用可能なメッセージングサービスです。それぞれの要件に応じて使い分ける必要があります。今回は移行要件がリプラットフォーム形式であるため、Apache ActiveMQ の機能そのものをAWS環境で再現することが求められています。これらのソフトウェアと互換性がある場合で、メッセージングサービスを迅速かつ簡単にクラウドに移行する場合はAmazon MQを利用します。Amazon MQでは業界標準のAPIとプロトコルをサポートしているため、アプリケーションのメッセージングコードを書き換えることなく、標準ベースのメッセージブローカーからAmazon MQに切り替えることができます。

Amazon MQ は、クラウド内のメッセージブローカーを容易に設定し運用できる、Apache ActiveMQ 向けのマネージド型メッセージブローカーサービスです。メッセージブローカーではさまざまなソフトウェアシステムを使用して、情報のやり取りや交換を実行します。Amazon MQ では、人気の高いオープンソースのメッセージブローカーである ActiveMQ のプロビジョニング、セットアップ、メンテナンスを管理することでオペレーション上の読み込みを減らします。業界標準 API や、JMS、NMS、AMQP、STOMP、MQTT、WebSocket などのメッセージング用のプロトコルを使用しているため、現在のアプリケーションを簡単に Amazon MQ に接続することができます。

一方で、クラウドでまったく新しいアプリケーションを構築する場合は、Amazon SQSとAmazon SNSを検討することが推奨されています。 Amazon SQSおよびSNSは、軽量で完全に管理されたメッセージキューおよびトピックサービスであり、ほぼ無限にスケーリングし、シンプルで使いやすいAPIを提供します。 Amazon SQSとSNSを使用して、マイクロサービス、分散システム、サーバーレスアプリケーションを分離および拡張し、信頼性を向上させることができます。しかしながら、今回の要件とは合致しないため、オプション１と３は不正解です。

オプション４は不正解です。SESはメール機能を実装することが可能なAWSサービスであり、MQなどのメッセージサービスではないため本件の要件には適していません。

問題65: 不正解

シューズメーカーC社は発送まで平均3〜4日を必要とするパーソナライズされたシューズを販売する受注オーダーサービスを展開しています。この販売用アプリケーションはAWS上で構築されており、顧客データと注文データを保存するRDS MySQLインスタンスを備えたWebサイト用のEC2インスタンスを利用しています。また、その展開とバージョン管理にはAWS Elastic Beanstalkを利用しています。

注文は増加傾向にあり、6か月後に1日あたり1000件、12か月後に10,000件の注文が発生するものと予想されているため、スケーリングが必要不可欠となっています。この注文プロセスでは、生産品質管理、出荷、支払い処理プロセスを全体でチェックする必要があり、注文内容の変更・支払いの失敗などの重大な問題が発生した場合は管理者に通知が必要です。

注文処理プロセスはどのように実現すれば良いでしょうか。

- ◉ AWS StepFunctionsを利用した注文プロセスを実装して、CloudWatchを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。 (不正解)
- ○ AWS StepFunctionsを利用した注文プロセスを実装して、CloudTrailを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。
- ○ AWS StepFunctionsを利用した注文プロセスを実装して、CloudWatchとCloudTrailの2つを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。 (正解)
- ○ Amazon SWFを利用した注文プロセスを実装して、AWS Configを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。
- ○ Amazon SWFを利用した注文プロセスを実装して、CloudTrailを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。
- ○ Amazon SWFを利用した注文プロセスを実装して、CloudWatchとCloudTrailの2つを使ってプロセスをモニタリングし、管理者へのメール配信をSNSを連携して実現する。

説明

AWS Step Functions はAWS の複数のサービスをサーバーレスのワークフローに統合することができるサービスです。Step Functions を使用すると、AWS Lambda、AWS Fargate および Amazon SageMaker などのサービスをつなげて機能豊富なアプリケーションにまとめるワークフローを設計して実行できます。ワークフローは一連のステップで構成され、あるステップの出力が次のステップへの入力になります。

AWS Step Functions はワークフローおよびアクティビティを追跡し、選択したしきい値にアラームを設定するために CloudWatch のメトリクスを提供しています。メトリクスはCloudWatchコンソールを使用して表示できます。

また、AWS Step FunctionsはAWS CloudTrail と統合されています。CloudTrail は、イベントとして AWS Step Functions に対するすべての API コールをキャプチャします。キャプチャされた呼び出しには、AWS Step Functionsコンソールの呼び出しと、AWS Step FunctionsAPI オペレーションへのコード呼び出しが含まれます。証跡を作成する場合は、AWS Step Functionsのイベントなど、Amazon S3 バケットへの CloudTrail イベントの継続的な配信を有効にすることができます。

したがって、オプション3が正解です。

この問題では、AWS Step Functionsによるワークフローとそのモニタリング方法が問われています。AWS Step Functionsは人の作業によるアクティブティとシステム利用状況の双方のモニタリングが必要となります。アクティビティに関してはCloudTrailが必要となり、システム状況はCloudWatchが必要となり、モニタリング体制には両方の情報を利用することが必要となります。オプション1と2はどちらか1つしか設定がされていないため不正解となっています。

オプション4と5と6は不正解です。今回の処理ではStep Functionsを利用することが優先されます。AWS Step Functions では、より生産的かつ機敏なアプローチにより、視覚的ワークフローを使用してアプリケーションコンポーネントを調整できるため、新しいアプリケーションには AWS Step Functions を使用することが推奨されています。プロセスにおいて介入する外部信号が必要な場合、または結果を親に返す子プロセスを起動する場合など、限定的なケースにおいてはAmazon Simple Workflow Service (Amazon SWF) を使用します。

問題66: 不正解

B社は1つのパブリックサブネットを持つVPCを設置して、AWSリソースを展開しています。 会社には、m3.large タイプのEC2インスタンスにデプロイした新しいブロックチェーンアプリケーションがあります。 デプロイから1か月後に、このアプリケーションがIPv6アドレスをサポートできるように変更することが必要となりました。あなたはソリューションアーキテクトとして、この対応を依頼されました。

この要件を満たすために最適なソリューションを選択してください。 (2つ選択してください)

- [x] egress only インターネットゲートウェイをVPCとサブネットに接続する。 (不正解)
- [x] EC2インスタンスで拡張ネットワークを有効にする。 (不正解)
- [ ] インスタンスタイプをm4.largeに変更する。 (正解)
- [ ] IPv6 CIDRブロックをVPCおよびサブネットに関連づける。 (正解)
- [ ] VPCコンソールにおいてIPv6を有効化したVPCを構成して、m3.largeインスタンスのVPCを切り替える。

説明

このシナリオでは、m3.largeインスタンスタイプのEC2インスタンスが配置されたVPCとサブネットに対してIPv6を使用できるようにすることが必要です。m3.largeインスタンスタイプはIPv6をサポートしないため、インスタンスのサイズを、サポートされているインスタンスタイプ（m4.largeなど）に変更する必要があります。したがって、オプション３が正解となります。

オプション４は正解となります。IPv4を利用しているVPCに対して、IPv6を有効にするためには、IPv6 CIDRブロックをVPCおよびサブネットに関連づけることで、IPv6が利用可能になります。IPv4のみをサポートする既存のVPCと、IPv4のみを使用するように構成されたサブネットのリソースがある場合、次の手順でVPCとリソースのIPv6サポートを有効にできます。

１．IPv6 CIDRブロックをVPCおよびサブネットに関連付ける
Amazonが提供するIPv6 CIDRブロックをVPCおよびサブネットに関連付けます。

２．ルートテーブルを更新する
ルートテーブルを更新して、IPv6トラフィックをルーティングします。パブリックサブネットの場合、すべてのIPv6トラフィックをサブネットからインターネットゲートウェイにルーティングするルートを作成します。プライベートサブネットの場合、インターネットからのすべてのIPv6トラフィックをサブネットから出力専用のインターネットゲートウェイにルーティングするルートを作成します。

３．セキュリティグループルールを更新する
セキュリティグループルールを更新して、IPv6アドレスのルールを含めます。これにより、インスタンスとの間でIPv6トラフィックが流れるようになります。サブネットとの間のトラフィックのフローを制御するカスタムネットワークACLルールを作成した場合、IPv6トラフィックのルールを含める必要があります。

４．インスタンスタイプの変更
インスタンスタイプがIPv6をサポートしていない場合は、インスタンスタイプを変更します。インスタンスタイプがIPv6をサポートしていない場合、インスタンスのサイズをサポートされているインスタンスタイプに変更する必要があります。この例では、インスタンスはm3.largeインスタンスタイプであり、IPv6をサポートしていません。インスタンスのサイズを、サポートされているインスタンスタイプ（m4.largeなど）に変更する必要があります。

５．インスタンスにIPv6アドレスを割り当てる
サブネットのIPv6アドレス範囲からインスタンスにIPv6アドレスを割り当てます。

６．インスタンスでIPv6を構成する
DHCPv6を使用するように構成されていないAMIからインスタンスを起動した場合、インスタンスに割り当てられたIPv6アドレスを認識するようにインスタンスを手動で構成する必要があります。

問題67: 不正解

あなたの会社では４つのEC2インスタンスにAutoScalingとELBを設定したインフラ構成を利用してECサイトを構築しています。過去2か月間システムを監視した結果、最小負荷を処理するには4つのWebサーバーが必要と判明しており、これは長い期間利用する必要があります。年末のクリスマスシーズンの1週間ほどは10台のサーバーが安定稼働に必要となり、ピーク時には最大で14台起動する必要があると予測されました。そのため、高可用性を提供しながら、コストを最小限に抑えるようにリファクタリングが必要です。

この要件を満たすために、最適なソリューションを選択してください。

- ◉ 10のオンデマンドインスタンスを購入し、４つのリザーブドインスタンスをAutoScaling向けに設定する。 (不正解)
- ○ 10のオンデマンドインスタンスを購入し、４つのスポットインスタンスをAutoScaling向けに設定する。
- ○ ４つのリザーブドインスタンス、６つのオンデマンドインスタンスを購入し、４つのスポットインスタンスをAutoScaling向けに設定する。 (正解)
- ○ ４つのオンデマンドインスタンス、10のオンデマンドインスタンスを購入する。

説明

最小負荷を処理するには少なくとも４つのインスタンスが必要であるため、システムの可用性を確保するには、４つのリザ- ブドインスタンスが最も費用効果が高くなります。これは中長期利用されることがわかっているため、予約が可能になるからです。

年末のクリスマスシーズンの1週間ほど10台のサーバーが安定稼働に必要となり、6つのオンデマンドEC2を使用して必要なときにいつでも要件を満たすことができます。 オンデマンドインスタンスにすることでシーズンが終了後に数を減少させて、コストを最適化することができます。

そして、処理負荷がピ - クになった際には最大14台のサーバーを必要とする可能性がありますが、これはピーク時の一時的な利用であるためスポットインスタンスを設定します。

したがって、４つのリザーブドインスタンス、６つのオンデマンドインスタンスを購入し、４つのスポットインスタンスをAutoScaling向けに設定することが最適な構成と言えます。オプション３が正解となります。

問題68: 正解

あるWEBアプリケーションではデータ管理やアクセス制御用にDynamoDBテーブルを利用しています。あなたはソリューションアーキテクトとして、データ処理をモニタリングするために1秒あたり1000レコードにもなるメトリクスデータを収集する設定を担当しています。その際には、カスタム名前空間を使用してCloudWatchにこれらのデータを送信したいと考えています。

この要件を満たすために最適なソリューションを選択してください。

- (●) CloudWatch にクライアント側のメトリクスデータを集約して、PutMetricData API コールを利用して送信する。 (正解)
- ( ) すべてのデータの1つのcsvファイルを作成し、CloudWatchに単一のファイルを送信する。
- ( ) CloudWatchコンソールから統計集約を実施して、SendMetricData API コールを利用して送信する。
- ( ) CloudWatch により集約データを作成して、SendMetricData API コールを利用して送信する。

説明

オプション 1 が正解となります。Amazon CloudWatch でクライアント側のメトリクスデータを集約して、単一の PutMetricData API コールでパブリッシュできるようになりました。これにより、大量のメトリクスデータを効率よくインジェストしながら、API コール数が減ることでコストを削減することもできます。

メトリクスデータは、値とカウント数による配列のヒストグラム形式でパブリッシュすることも、CloudWatch エージェントを活用してパブリッシュすることもできます。CloudWatch では、集約データからパーセンタイルの統計が自動作成されます。この統計により異常が可視化されるため、外れ値を除外してアラームのノイズを低減できます。

オプション 2 は不正解です。すべてのデータの1つのcsvファイルを作成し、CloudWatch に単一のファイルを送信するといった設定をする必要はありません。Amazon CloudWatch でクライアント側のメトリクスデータを集約して、単一の PutMetricData API コールでパブリッシュすることが容易に実行できます。

オプション 3 と 4 は不正解です。SendMetricData API コールではなく、PutMetricData API コールを利用して集約したデータを送信する必要があります。

問題69: 不正解

ある銀行ではALBの背後にある複数のアベイラビリティーゾーンにまたがるAmazon EC2インスタンスのAuto Scalingグループでホストされる WEBアプリケーションを構築しています。HTTPおよびHTTPSトラフィックを許可するために、ALBおよびEC2インスタンスに対してセキュリティグループを設定して、サブネットにはネットワークACLを設定して、ポート80および443でのインバウンドトラフィックを許可しました。しかしながら、インターネットからWEBアプリケーションへと接続することができませんでした。

この問題を解決するために最適なソリューションを選択してください。

- ◉ ポート32768-65535のインバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。 (不正解)
- ○ ポート32768-65535のアウトバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。
- ○ ポート49152～65535のアウトバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。
- ○ ポート1024～65535のアウトバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。 (正解)
- ○ ポート49152～65535のインバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。
- ○ ポート1024～65535のインバウンドトラフィックを許可することにより、ネットワークACLで一時ポートを許可する。

説明

オプション4が正解となります。VPC内のパブリックに面したインスタンスに対して、トラフィックを開始することができる多様なクライアントを対象にするには、アウトバウンドルールに対して一時ポート1024～65535を開く必要があります。

インスタンスで実行されているサービスへの接続を有効化するには、関連付けられたネットワークACLにおいて、サービスがリッスンしているポートのインバウンドトラフィックと、エフェメラルポートからのアウトバウンドトラフィックの両方を許可する必要があります。エフェメラルポートはインターネットプロトコルを用いた通信を行うため、TCP/IPプロトコルスタックが事前に定義されている範囲内から自動的に割り当てるポートです。この設定には（1024～65535）を使用します。クライアントがサーバーに接続すると、一時ポート範囲（1024～65535）からのランダムポートがクライアントのソースポートになります。

リクエストを開始するクライアントは、一時ポートの範囲を選択します。範囲は、クライアントのオペレーティングシステムによって変わります。

・多くのLinuxカーネル(Amazon Linuxカーネルを含む)は、ポート32768～61000を使用します。
・Elastic Load Balancingが送信元のリクエストは、ポート1024～65535を使用します。
・Windows Server 2003を介するWindowsオペレーティングシステムは、ポート1025～5000を使用します。
・Windows Server 2008以降のバージョンでは、ポート49152～65535を使用します。
・NATゲートウェイはポート1024～65535を使用します。
・AWS Lambda関数は、ポート1024-65535を使用します。

したがって、ポート49152～65535とポート32768-65535は対象クライアントが異なるため、オプション1と2と3と5は不正解です。

また、エフェメラルポートからのアウトバウンドトラフィックを許可する必要があるため、オプション6は不正解です。

問題70: 不正解

あなたはWindows 2019 AMIを使用してオンデマンドAmazon EC2インスタンスを起動しました。このインスタンスにアクセスするために、ポート3389でリモートデスクトッププロトコル（RDP）を介してインスタンスに接続しようとしましたが、エラーが発生します。同じネットワーク構成を使用して別のAMIから2番目のEC2インスタンスをデプロイしてみると、そのインスタンスには接続できるようです。

最初のインスタンスのトラブル原因を特定するためのアクションを選択してください。

- (●) EC2インスタンスに設定したフローログを集約したCloudWatch logsを利用して、オペレーティングシステムのログファイルを収集する。 (不正解)
- ( ) Amazon Macieを利用して分析用のオペレーティングシステムログファイルの収集する。
- ( ) EC2Rescue for EC2 Windowsを利用して、オペレーティングシステムのログファイルを収集する。 (正解)
- ( ) CloudWatchによるメトリクス分析を実施する。

説明

オプション3が正解となります。EC2Rescue for Windows Serverは、Amazon EC2 Windows Serverインスタンス上で動作し、潜在的な問題の診断とトラブルシューティングを行うことができる使いやすいツールです。ログファイルを収集して問題を解決するだけでなく、問題がありそうな部分をプロアクティブに検索することができます。他のインスタンスからAmazon EBSルートボリュームを調べて、そのボリュームを使用するWindows Serverインスタンスをトラブルシューティングするために必要なログを収集することもできます。したがって、EC2Rescueツールを使用して分析のためにオペレーティングシステムのログファイルを収集することで原因を特定します。

オプション1は不正解です。EC2インスタンスに設定したフローログではトラフィックのログしか確認できないため、分析のためにオペレーティングシステムのログファイルを収集することができません。

オプション2は不正解です。Amazon Macieは、機械学習によってAWS内の機密データを自動的に検出、分類、保護するセキュリティサービスです。分析のためにオペレーティングシステムのログファイルを収集することができません。

オプション4は不正解です。CloudWatchによりメトリクスを収集することはできますが、分析のためにオペレーティングシステムのログファイルを収集することができません。

問題71: 正解

あなたは新規にVPCを設置して、新しいアプリケーションを構築したいと考えています。まずはCIDR 10.0.0.0/24でVPCを作成し、パブリックサブネット（10.0.0.0/28）およびプライベートサブネット（10.0.0.16/28）を構成しました。次に各サブネット内に複数のEC2インスタンスを起動しました。開発を進めるうちに、CIDRのすべてのIPアドレスを使用してしまったため、VPCのサイズを増やしたいと考えています。

VPCのサイズを変更するにはどうすればよいですか？

- ◉ セカンダリIPv4 CIDR（10.0.1.0/24）を追加する。 (正解)
- ○ セカンダリIPv4 CIDR（10.0.0.0/16）を追加する
- ○ セカンダリIPv4 CIDR（10.0.1.0/16）を追加する
- ○ セカンダリIPv4 CIDR（10.0.0.0/24）を追加する

説明

VPC に対してセカンダリ IPv4 CIDR ブロックを関連付けることでIPアドレス範囲を拡張できます。セカンダリCIDR ブロックを VPC に関連付けると、ルートが VPC ルートテーブルに自動的に追加され、VPC 内でのルーティングが可能になります。これによって、IPアドレスを増やすことが可能です。

セカンダリCIDR ブロックは、VPCルートテーブルのいずれかのルートの CIDR 範囲と同じ、またはそれ以上に大きくすることはできません。たとえば、プライマリ CIDR ブロックが 10.0.0.0/24である VPC では、範囲が 10.0.1.0/24 のセカンダリ CIDR ブロックを関連付けることができます。したがって、オプション 1 が正解となります。

説明

VPC に対してセカンダリ IPv4 CIDR ブロックを関連付けることでIPアドレス範囲を拡張できます。セカンダリCIDR ブロックを VPC に関連付けると、ルートが VPC ルートテーブルに自動的に追加され、VPC 内でのルーティングが可能になります。これによって、IPアドレスを増やすことが可能です。

セカンダリCIDR ブロックは、VPC ルートテーブルのいずれかのルートの CIDR 範囲と同じ、またはそれ以上に大きくすることはできません。たとえば、プライマリ CIDR ブロックが 10.0.0.0/24である VPC では、範囲が 10.0.1.0/24 のセカンダリ CIDR ブロックを関連付けることができます。したがって、オプション 1 が正解となります。

問題72: 正解

ベンチャー企業のA社はAWSを利用したアプリケーションサービスを展開しており、ユーザーデータを保存するためにRDS MySQLデータベースを使用しています。このRDS MySQLデータベースは高パフォーマンスを達成するために、リードレプリカを5台起動した上で、インスタンスサイズも高性能なものを利用しています。しかしながら、このRDSへの処理負荷が高まっており、読み取り処理における競合処理が増えてしまっています。したがって、あなたはRDS MySQLデータベースからAuroraへと切り替えることを決定しました。

Auroraを使用して読み取り競合を抑えるための、最適な構成方法を選択してください。

- (●) MySQLスナップショットからAmazon Aurora MySQLクラスターをエンジンタイプに選択して、復元処理をすることでAurora MySQLへと移行する。その上で、リードレプリカを15台起動する。読取負荷が高まった際には、Aurora MySQLインスタンスをスケーリングするときにAurora DBリーダーエンドポイントを利用する。 (正解)
- ( ) MySQLスナップショットからAmazon Aurora MySQLクラスターをエンジンタイプに選択して、復元処理をすることでAurora MySQLへと移行する。その上で、MySQL DBインスタンスのスレーブとしてAurora MySQLのレプリケーションを利用して、Route53を利用してフェールオーバー構成を実施する。
- ( ) MySQLスナップショットからAmazon Aurora MySQLクラスターをエンジンタイプに選択して、復元処理をすることでAurora MySQLへと移行する。その上で、Amazon Aurora MySQL マルチマスターを有効化して、Aurora MySQLインスタンスをスケーリングするときにAurora DBクラスターエンドポイントを利用する。
- ( ) MySQLスナップショットからAmazon Aurora MySQLクラスターをエンジンタイプに選択して、復元処理をすることでAurora MySQLへと移行する。その上で、MySQL DBインスタンスのスレーブとしてAurora MySQLのレプリケーションを設定して、RDSのMySQL DBインスタンスに適用する。

説明

このシナリオでは、RDS MySQLデータベースの読み取りの競合が増えており、RDS MySQLからAurora MySQLへとリプレースすることで、高パフォーマンスな処理を可能にする構成方法が問われています。そのためには、Auroraの具体的な移行・展開方法を回答することが必要です。

RDS MySQLデータベースは高パフォーマンスを達成するために、リードレプリカを5台起動していましたが、パフォーマンスが低下してしまいました。したがって、Auroraに移行したうえで、リードレプリカをさらに増強することでパフォーマンスを向上させることができます。

Aurora の MySQL 互換エディションでは、同じハードウェアで実行する標準的な MySQL と比較して、最大 5 倍のスループットが実現されています。変更を加えることなく既存の MySQL アプリケーションやツールを活用できます。移行の際は、通常のRDSのスナップショットを利用することで容易にAuroraへと移行することが可能です。Auroraは読み取りのキャパシティーとパフォーマンスをスケールするために、3 つのアベイラビリティーゾーン間でレイテンシーの低いリードレプリカを最大 15 個追加できます。Auroraを使用してMySQL DBインスタンスを読み取りスケーリングするには、Amazon Aurora MySQL DBクラスターを作成し、Aurora DBリーダーエンドポイントを利用してMySQL DBインスタンスのレプリケーションスレーブすることができます。

したがって、オプション1が正解となります。

オプション2は不正解です。 Route53を利用したフェールオーバー構成は読み取りワークロードを拡張するためには利用できないため不正解です。

オプション3は不正解です。Amazon Aurora MySQL マルチマスターを構築して、Aurora MySQLインスタンスをスケーリングする際にAurora DBクラスターエンドポイントを利用する場合は、Amazon Aurora MySQL マルチマスターではなく、Amazon Aurora MySQLクラスターを構築することが必要となります。またクラスターエンドポイントは書き込み処理をするインスタンスに適用されるエンドポイントであるためリードレプリカには適用できません。

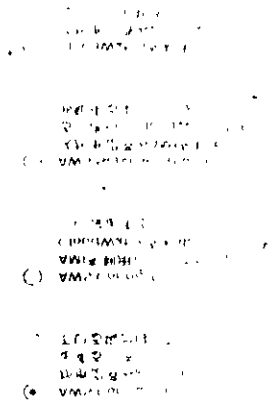
オプション4は不正解です。リードレプリカの構成が利用されておらず、構成としては不十分となっています。

問題73: 不正解

B社ではAWSを利用したアプリケーション開発を行っています。このアプリケーションはALBを設定した複数のEC2インスタンスによって構成されています。アプリケーションにリクエストしているクライアントのIPアドレスをキャプチャすることが必要ですが、現在キャプチャされているすべてのIPアドレスがALBのIPアドレスとなってしまっています。

クライアント固有のIPアドレスを取得する方法を選択してください。

- (●) バックエンドのX-Forwarded-Fromヘッダーを確認する。 (不正解)
- ( ) バックエンドのX-Forwarded-Forヘッダーを確認する。 (正解)
- ( ) バックエンドのX-Forwarded-Portヘッダーを確認する。
- ( ) バックエンドのX-Forwarded-Protoヘッダーを確認する。



説明

オプション 2 が正解となります。ELBはクライアントの IP アドレスを X-Forwarded-For リクエストヘッダーに格納し、このヘッダーをサーバーに渡します。したがって、X-Forwarded For リクエストヘッダーを確認することでクライアント個別のIPアドレスを取得することができます。

HTTP リクエストと HTTP レスポンスは、ヘッダーフィールドを使用して HTTP メッセージに関する情報を送信します。ヘッダーフィールドはコロンで区切られた名前と値のペアであり、キャリッジリターン (CR) とラインフィード (LF) で区切ります。HTTP ヘッダーフィールドの標準セットが RFC 2616 の「Message Headers」で定義されています。アプリケーションで広く使用されている標準以外の HTTP ヘッダーもあります。標準以外の HTTP ヘッダーには X-Forwarded というプレフィックスが付いている場合があります。クラシックロードバランサー は、次の X-Forwarded ヘッダーをサポートしています。

X-Forwarded-For リクエストヘッダーは、HTTP または HTTPS ロードバランサーを使用する場合に、クライアントの IP アドレスを識別するのに役立ちます。ロードバランサーはクライアント/サーバー間のトラフィックをインターセプトするので、サーバーアクセスログにはロードバランサーの IP アドレスのみが含まれます。クライアントの IP アドレスを確認するには、X-Forwarded-For リクエストヘッダーを使用します。

問題74: 正解

あなたの会社では独自の顧客管理システムをAWS上で運用しています。このシステムでは、EBSボリュームが接続されたWindowsサーバーのEC2インスタンスを使用しています。社内ではシステム開発者が未承認のAMIを使用してインスタンスを起動することは開発ポリシーによって禁止されており、AMIの準拠状況をモニタリングすることが必要となります。あなたはソリューションアーキテクトとして、上記のすべてのインスタンスを監視する仕組みを検討しています。

この要件を満たすためのAWSソリューションを選択してください。

- (●) AWS Configマネージドルールを利用して、起動するEC2インスタンスが承認済みAMIを利用しているかを自動でチェックする管理ルールを設定する。さらにCloudWatchを利用して、未承認AMIがVPC内に起動している場合は通知するように設定する。 (正解)
- ( ) AWS Configカスタムルールを利用して、起動するEC2インスタンスが承認済みAMIを利用しているかを自動でチェックする管理ルールを設定する。さらにCloudWatchを利用して、未承認AMIがVPC内に起動している場合は通知するように設定する。
- ( ) AWS Service Catalogによる標準化ルールを利用して、起動するEC2インスタンスが承認済みAMIを利用しているかを自動でチェックする管理ルールを設定する。さらにCloudWatchを利用して、未承認AMIがVPC内に起動している場合は通知するように設定する。
- ( ) CloudWatchを利用して、AMIの利用状況を監視して、起動するEC2インスタンスが承認済みAMIか未承認のAMIを利用しているかを自動でチェックし、SNSを設定して通知する管理ルールを設定する。

説明

オプション1が正解となります。AWS Config は、AWSマネージドルールを提供して監視を行うことができます。マネージドルールは、定義済みのカスタマイズ可能なルールであり、AWS リソースが一般的なベストプラクティスに準拠しているかどうかを評価するために AWS Config で使用することができます。たとえば、マネージドルールを使用することで、Amazon EBSボリュームが暗号化されているかどうか、または 特定のタグがリソースに適用されているかどうかをすばやく評価できます。マネージドルールは、AWS Config コンソールの手順に従って設定および有効化できます。AWS Command Line Interface または AWS Config API を使用して、マネージドルールの設定を定義する JSON コードを渡すこともできます。

オプション2は不正解です。AMIのモニタリングにはカスタムルールではなくAWS マネージドルールが利用できるため、本件には合致しません。AWS Config に対してはカスタムルールを作成して 追加できます。各カスタムルールは AWS Lambda 関数と関連付けます。この関数にはAWS リソースがルールに準拠しているかどうかを評価するロジックが含まれています。

オプション3は不正解です。AWS Service CatalogはAMIの利用状況を監視することはできません。

オプション4は不正解です。CloudWatchはAMIの利用状況を監視して、起動するEC2インスタンスが承認済みAMIか未承認のAMIを利用しているかを確認することができません。

問題75: 不正解

あなたの会社ではAWSにホストしたオンラインモバイルゲームを運用しています。このゲームでは、参加者によるバトルトーナメントが開催されており、ゲーム上でユーザー同士が競い合います。そして、結果としてのユーザーランキングを表示するランキング機能を有しています。ランキング機能は、ElastiCacheを利用して作成されており、データを並べ替えてランク付けするためのRedisの並べ替えセットを使用して、リアルタイムでランキングが更新されます。新しい要件として、このElastiCacheクラスターのデータ耐久性を強化することが必要となり、あなたは費用対効果の高いフォールトトレラントキャッシングレイヤーを構築するように依頼されました。

この要件を満たすことができる費用対効果の高いAWSソリューションを選択してください。（3 つ選択して下さい）

- [x] Redisのリードレプリカ用クラスターを追加する。 (不正解)
- [x] Redisのクラスターを動かすインスタンスタイプを高性能なものに置換する。 (不正解)
- [ ] Redis の AOF機能を有効にする (正解)
- [ ] Redisの自動フェイルオーバーを備えたマルチAZのセットアップを実施する。 (正解)
- [ ] 自動バックアップを有効化する。 (正解)

説明

ElastiCache Redisクラスターはキャッシュデータのディザスターリカバリーまたはフォールトトレランスを実装するために、以下のような機能を提供しています。

1．自動バックアップ
2．Redis AOFを使用した手動バックアップ
3．自動フェイルオーバーを備えたマルチAZのセットアップ

データの耐久性が必要な場合、Redis の AOF (Append-Only File) 機能を有効にすることができます。この機能を有効にすると、キャッシュノードは、キャッシュデータを変更するすべてのコマンドを Append-Only File に書き込みます。ノードが再起動され、キャッシュエンジンが起動すると、AOF が「再生」されます。その結果、すべてのデータがそのままのウォーム Redis キャッシュが作成されます。

AOF はデフォルトでは無効になっています。Redis を実行しているクラスターで AOF を有効にするには、appendonly パラメータを yes に設定してパラメータグループを作成する必要があります。次に、そのパラメータグループをクラスターに割り当てます。appendfsync パラメータを変更して、Redis が AOF ファイルに書き込む頻度を制御することもできます。したがって、オプション３が正解となります。

オプション４も正解となります。Redis はマルチAZ構成により、キャッシュノードの障害検知とプライマリーノードの自動フェイルオーバーが実施できます。

オプション５も正解となります。Redisは自動バックアップによってデータ損失を防ぐことが可能です。

オプション１は不正解です。Redis クラスターに対するリードレプリカノードの追加や削除することで、手動ステップやアプリケーションの変更なしに、簡単に読み取り処理をスケールすることや、Redis クラスター環境の可用性を向上させることができます。今回は読込処理のスケーリングが求められているわけではないため、不十分な対応となります。

オプション２は不正解です。Redisのクラスターを動かすインスタンスタイプではなく、ノードタイプを変更することで、性能を向上させることができます。