問題1: 不正解

あなたはソリューションアーキテクトとして、AWSを利用したインフラの運用を担当しています。パブリックサブネットで起動されたEC2インスタンスを運用するためには、定期的にインターネットを経由してソフトウェアアップグレードにアクセスできるようにする必要があります。これらのインフラはURLを介して運用管理ベンダーからアクセスされて、モニタリングやメンテナンスが実行されています。セキュリティ監査を実施したところ、このモニタリングやメンテナンスの仕組みにおいてネットワーク上の問題点があるとの報告を受けました。あなたはソリューションアーキテクトとして、VPC内のインスタンスからインターネットに対して、他のアウトバウンド接続を明示的に拒否する設定を行う必要があります。

このシナリオにおいて、要件を満たすための方法を選択してください。

- ◉ ネットワークACLを利用して、全てのネットワークに対して特定パッケージ配信の許可ルールを設定する。その他のアクセスは明示的拒否設定を行う。 (不正解)
- ○ フォワードプロキシサーバーを利用して、URLベースのアウトバウンドトラフィックアクセスのルールを管理する。また、デフォルトルートは削除する。 (正解)
- ○ セキュリティグループを作成してインターネットから特定のパッケージソフトウェアの更新ファイルにアクセスできる適切なアウトバウンドアクセスルールを設定する。
- ○ 全てのインスタンスをパブリックサブネットからプライベートサブネットに移動して、プライベートサブネットのルートテーブルにおいて、特定のパッケージソフトウェアの更新ファイルにアクセス可能となるアウトバウンドアクセスルールを設定する。

説明

オプション2が正解となります。フォワードプロキシサーバーを利用して制御することで要件を達成することができます。フォワードプロキシサーバーはクライアントからの要求をフィルターし、製品の更新に関連する要求のみを許可して、製品の更新以外の要求をフィルタリングすることができます。

フォワードプロキシサーバーは内部ネットワークのセキュリティを損なわずにネットワークの外部と接続できるようにする、LAN 上のコンピューターです。フォワードプロキシサーバーは内部コンピューターのアイデンティティを保護するために一般的に使用されています。 内部ユーザーおよびサーバーからの要求の仲介役として機能し、多くの場合、コンテンツをキャッシュして後続の要求を高速化します。 企業は通常、プロキシソリューションを実装して、URLおよびWebコンテンツフィルタリング、IDS / IPS、データ損失防止、監視、高度な脅威保護を提供します。 AWSにおいてはVPNまたはAWS Direct Connect接続を使用して既存の企業プロキシサーバーインフラストラクチャを活用したり、内部ELBを備えたSquidプロキシサーバーなどのソフトウェアを使用して、AWS上にフォワードプロキシファームを構築したりすることができます。

オプション1は不正解です。ネットワークACLはURLに基づいてリクエストをフィルター処理できないため、正しくありません

オプション3は不正解です。セキュリティグループはURLに基づいて要求をフィルター処理できないため、正しくありません

オプション4は不正解です。プライベートサブネットのルートテーブルにはフィルタリング機能はありません。

問題2: 不正解

大手商社では社内業務システムにおいてClassic Load Balancerを使用して、複数のリザーブドEC2インスタンスに均等に着信トラフィックを分散しています。最近、この業務システムのアプリケーションサーバーが原因と思われる断続的に使用不可となる状況が発生しています。この原因を究明するために、登録されたインスタンスから送信されたサーバーエラーを確認することが必要です。

サーバーエラーを確認するために必要なメトリクスを選択してください。

- (◉) HTTPCode_ELB_5XX (不正解)
- ( ) HTTPCode_Backend_3XX
- ( ) HTTPCode_Backend_4XX
- ( ) HTTPCode_Backend_5XX (正解)

説明

ロードバランサーはクライアントに送信されたHTTP応答コードのメトリクスをCloudWatchに送信することで、エラーの原因がロードバランサーなのか、登録済みインスタンスなのかを特定します。つまり、CloudWatchからロードバランサーに返されるメトリクスを使用して、問題のトラブルシューティングを行うことが必要です。

オプション4が正解となります。HTTPCode_Backend_5XXの原因は登録済みインスタンスからサーバーエラー応答が送信された場合に発生するため、正しいです。これを解決するには、インスタンスのアクセスログまたはエラーログを表示して、原因を特定することが必要です。

オプション1は不正解です。HTTPCode_ELB_5XXはロードバランサーまたは登録されたインスタンスがエラーが原因であるか、またはロードバランサーが応答を解析できなかった場合のメトリクスであり、正しくありません。

オプション2は不正解です。HTTPCode_Backend_3XXは登録済みインスタンスからリダイレクト応答が送信された場合のメトリクスであり、正しくありません。

オプション3は不正解です。HTTPCode_Backend_4XXは登録済みインスタンスからクライアントエラー応答が送信された場合のメトリクスであり、正しくありません。

問題3: 不正解

Fintech企業A社はビットコインなどの暗号通貨を売買できる仮想通貨取引プラットフォーム事業を開始しました。これは金融サービスとなるため、高いコンプライアンス要件が求められており、マネーロンダリング防止およびテロ対策資金調達対策を実施する必要があります。すべてのレポートファイルは、特定の国やその内部の特定の地域または個人が利用できないようにすることが要件となります。 これらのコンプライアンス要件を満たしつつ、コンテンツを世界中のユーザーに低レイテンシーで配信することが必要です。その際にCloudFrontディストリビューションに関連するファイルサブセットへのアクセスを制限することが必要です。

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。

- (●) 特定の国・地域からのアクセスを制限するためにCloudFrontディストリビューションを利用してエッジロケーションによる地域制限を有効化する (不正解)
- ( ) 特定の国・地域からのアクセスを制限するためにCloudFrontディストリビューションを利用しオリジンサーバーの設定で地域制限を有効化する
- ( ) 特定の国・地域からのアクセスを制限するためにCloudFrontディレクトリビューションのLambda@エッジを利用した制限アルゴリズムと連携する。
- ( ) 特定の国・地域からのアクセスを制限するためにRoute53を利用した地理的近接性ルーティングによる地域制限を有効化する
- ( ) 特定の国・地域からのアクセスを制限するためにサードパーティの位置情報サービスを利用してエッジロケーションによる地域制限を有効化する (正解)

解説

地域制限 (地理的ブロッキング) を使用すると、CloudFront ディストリビューションを通じて配信しているコンテンツへの特定の地域ユーザーによるアクセスを回避できます。地域制限を使用するには、次の 2 つの方法があります。

・CloudFront の地理制限機能の使用

エッジロケーションによる地理的制限を有効化することで、ディストリビューションに関連するすべてのファイルへのアクセスを制限します。国レベルでアクセスを制限する場合は、この方法を使用します。 、

・サードパーティの位置情報サービスの使用

ディストリビューションに関連するファイルのサブセットへのアクセスを制限する場合や、国レベルより詳細なレベルでアクセスを制限する場合は、この方法を使用します。特定の国やその内部の特定の地域または個人に対する制限を詳細に実施することが要件となっており、今回はこちらのケースが該当します。

したがって、オプション 5 が正解となります。

オプション 1 は不正解です。CloudFront の地理制限機能を利用する選択肢となりますが、これは全てのファイルに対するアクセス制限しかできません。このシナリオでは、ディストリビューションに関連するファイルのサブセットへのアクセスを制限することが必要であり、サードパーティの位置情報サービスを使用する方が要件に合致します。

オプション 2 は不正解です。地理的制限はエッジロケーションにおいて実施される機能になります。

オプション 3 は不正解です。CloudFrontにおいてLambda@エッジを利用した制限アルゴリズムと連携するといった機能はありません。

オプション 4 は不正解です。Route53の地理的近接性ルーティングによって地理的制限を有効化するといったことはできません。Route53は位置情報ルーティングによって特定地域へのルーティングを制御することができます。

問題4: 不正解

アート鑑賞SNSサービスをグローバルに展開しているベンチャー企業では、ユーザー情報を保存するためにPINTOR-CONFIGという名前のプライベートS3バケットを使用しています。データを保護するためにバージョン管理を有効にして、ユーザー構成情報に加えられた変更を追跡できるように設定しました。

【バージョン管理有効化時点のファイル】

・ユーザー構成情報ファイル

・共通設定ファイル

・ユーザー構成情報ファイル02

【変更移行に発生したイベント状況】

・バージョン管理後にタスクファイルとログファイルが追加されました。

・バージョン管理後にユーザー構成情報ファイルとユーザー構成情報ファイル02が更新されました。

このシナリオにおける、S3バケット内のオブジェクトに対するバージョンIDについての正しい内容を選択してください。（2つ選択してください。）

- [x] ユーザー構成情報ファイルの最初のバージョンIDは1つ目のIDである。 (不正解)
- [x] タスクファイルの最初のバージョンIDは1つ目のIDである。 (正解)
- [ ] ログファイルの最新バージョンはNullである。
- [ ] ユーザー構成情報ファイルとユーザー構成情報ファイル02の最初のバージョンはNullである。 (正解)
- [ ] タスクファイルの最初のバージョンIDはnullである。

説明

S3バケットのバージョニングとは、同じバケット内に保存されているオブジェクトの複数バージョンを保持する手段です。バージョニングを使用するとAmazon S3 バケットに格納されたあらゆるオブジェクトのあらゆるバージョンを、格納、取得、復元することができます。これにより、意図しないユーザーアクションからもアプリケーション障害からも、簡単に復旧できます。

このシナリオでは、既存バケットに既に３つのオブジェクトファイルが存在します。S3バージョン管理を有効にすると、既存のファイルはすべて、バージョンIDがNULLになります。追加される新しいファイルには、英数字のバージョンIDと、最初の4つのファイルの新しい更新が含まれます。

オプション２が正解となります。タスクファイルはバージョン管理後に追加されるので最新バージョンで最初のバージョンIDは1つ目のID（IDは一意のランダム値）となります。

オプション４が正解となります。バージョニング前に保存されていたユーザー構成情報ファイルとユーザー構成情報ファイル02はバージョンIDがふられていないため、最初のバージョンIDはNullとなります。

オプション１は不正解です。バージョニング前に保存されていたユーザー構成情報ファイルとユーザー構成情報ファイル02が保存されていた状態からバージョニングが発生しているため、最初のバージョンはNullとなります。

オプション３は不正解です。バージョニング後にログファイルがアップロードされたため、バージョニングIDが最初から採番されて利用されることとなり、最初のバージョンIDは1つ目のIDとなります。

オプション５は不正解です。バージョニング後にタスクファイルがアップロードされたため、バージョニングIDが最初から採番されて利用されることとなり、最初のバージョンIDは1つ目のIDとなります。

問題5: 不正解

AI開発企業のB社は防犯カメラの映像から万引き犯を特定するサービスを開発しています。このサービスは防犯カメラからのストリーミングビデオで顔認証を実施して、過去の万引き犯データとマッチングさせます。アプリケーションはビデオを介してリアルタイムで迅速に顔認識を実施し、ダウンストリーム処理に適した方法で出力結果を保存できる必要があります。 あなたはRekognitionを使用して、この識別サービスを開発したいと考えています。

Rekognitionを利用した最適なアーキテクチャを選択してください。 (3つ選択してください。)

- [x] Java SDKのPutMedia APIによりS3に蓄積されたビデオデータをAmazon Kinesis Data StreamsによりRekognition Videoへと送信する仕組みを構築する。 (不正解)
- [ ] Java SDKのPutMedia APIによるAmazon Kinesis Video Streamsによって、ストリーミングビデオをRekognition Videoへと送信する仕組みを構築する。 (正解)
- [ ] Amazon Rekognition Videoは、ストリーミングビデオの分析を開始および管理するために使用できるストリームプロセッサ（CreateStreamProcessor）により、ストリーミングビデオの分析を実施する。 (正解)
- [ ] 分析結果は、Amazon Rekognition VideoからKinesis Data Streamsに出力され、Amazon Kinesis Data Streams Client Libraryによって Kinesis Data Streams Consumerとして構築されたEC2インスタンスに読み取られる。 (正解)
- [ ] Java SDKのDetectFacesによるAmazon Kinesis Video StreamsによりストリーミングビデオをRekognition Videoへと送信する仕組みを構築する。
- [ ] 分析結果は、Amazon Rekognition VideoからKinesis Data Streamsに出力され、Kinesis Data Streams Analyticsによって読み取られる。

説明

Amazon Rekognition Video ではライブビデオストリーミングをリアルタイムで解析して、顔を検出し、判別できます。Amazon Kinesis Video Streams のストリーミングデータを Rekognition Video に入力し、最大数千万もの顔データと照らし合わせて、超低レイテンシーでの顔認識を行います。バッチ処理のユースケースとして、Amazon Rekognition Video では Amazon S3 に保存した録画データを解析することもできます。

Amazon Rekognition には、Amazon Rekognition API、AWS マネジメントコンソール、および AWS コマンドラインインターフェイス (CLI) を使用してアクセスできます。コンソール、API、CLI では、Rekognition API を使用して、ラベル検出、顔分析、顔照合、顔検索を行えます。AWS Lambda には Rekognition 用の設計図が用意されており、Amazon S3 や Amazon DynamoDB といった AWS データストアでのイベントに基づいて画像分析を簡単に開始できます。

Amazon Rekognition Videoは、Amazon Kinesis Video Streamsを使用してビデオストリームを受信および処理します。分析結果は、Amazon Rekognition VideoからKinesisデータストリームに出力され、クライアントアプリケーションによって読み取られます。Amazon Rekognition Videoは、ストリーミングビデオの分析を開始および管理するために使用できるストリームプロセッサ（CreateStreamProcessor）を提供します。したがって、これらの要素を説明した正解はオプション２，３，４です。

オプション１は正しくありません。ソースビデオは、Amazon Kinesis Data StreamsではなくAmazon Kinesis Video Streamsに配置する必要があるためです。その後、Rekognitionプロセッサーは Kinesisストリームのレコードを取得して処理します。

オプション5は正しくありません。ビデオ処理にはRekognition APIの「DetectFaces」を使用しないでください。「DetectFaces」は、入力として提供される画像内の顔を検出するために使用されます。代わりに、ストリームプロセッサ関連のAPIを使用する必要があります。

オプション6は正しくありません。分析結果は、Kinesis Data Streams AnalyticsではなくKinesis Data Streams Consumerに読み取られます。

問題6: 不正解

大手印刷会社はデータベースシステムとしてMySQLデータベースを[redacted]レミス環境で利用しています。最近になってAWSクラウドとのハイブリッド構成[redacted]していく方針が決定され、MySQLデータベースをAWSに移行することを検討しています。オンプレミス環境との同期を維持するには、AWS上のデータベース用のインスタンスが必要です。このデータベース移行後は徹底的にテストすることで、オンプレミス環境との齟齬がなくなった段階で、オンプレミスデータベースは廃止する予定です。あなたは移行担当者として、Amazon Database Migration Service（DMS）を利用したデータベースの移行方法を整理しています。

これらの要件を満したAmazon DMSを利用した実施方法を選択してください。（3つ選択してください。）

- [x] EC2インスタンスを構築して、移行プロセスを管理するAmazon Database Migration Serviceの実行サーバーとしてセットして、レプリケーション用インスタンスとして定義する。 (不正解)
- [x] Amazon Database Migration Serviceを構成して、オンプレミス環境のデータベースとRDSとを接続するためには必ずデータ移行専用のVPN接続を確立することが必要となる。 (不正解)
- [x] 移行プロセスを管理するAmazon Database Migration Serviceコンソールを利用して、移行に必要となるCPUなどを設定したレプリケーション用インスタンスを配置する。 (正解)
- [ ] MySQLを利用したオンプレミスデータベースをソースエンドポイントに指定して、RDS MySQL DBインスタンスをターゲットデータベースのエンドポイントに指定する (正解)
- [ ] 利用するテーブルとレプリケーションプロセスを定義するタスクセットを構成して、移行タイプとして"migrate existing data and replicate ongoing changes"を指定する。 (正解)

説明

AWS Database Migration Service を使用すると、オンプレミス環境にあるデータベースを短期間で安全に AWS に移行できます。移行中でもソースデータベースは完全に利用可能な状態に保たれ、データベースを利用するアプリケーションのダウンタイムを最小限に抑えられます。また、AWS DMSは広く普及しているほとんどの商用データベースとオープンソースデータベース間のデータ移行で利用できます。この問題では詳細なAWS DMSの設定方法が問われています。[redacted]

オプション３は正解です。AWS DMSによりデータベースを移行する際の最初のタスクは、ソースデータベースからターゲットデータベースにデータを割り当てて、移行タスクを実行するために十分なストレージと処理能力を持つレプリケーションインスタンスを作成することです。

オプション4は正解です。ソースとターゲットのエンドポイントを選択するために必要な手順であるため、データベースエンジンは「MySQL」である必要があります。

オプション5は正解です。移行ターゲットデータベースに新しいテーブルの作成方式を指定するには、移行タイプには "migrate existing data and replicate ongoing changes"を指定したタスク設定が必要です。

AWS DMSタスクは、すべての処理が行われる場所です。ログ記録要件、制御テーブルデータ、エラー処理など、移行と特別な処理に使用するテーブルとスキーマを指定します。次のようにタスクを設定します。

・移行タスクを作成する前に、DMSコンソールでソースエンドポイント、ターゲットエンドポイント、およびレプリケーションインスタンスを作成します。
・移行タスクを調整するために多くのタスク設定を指定できます。それらは、AWS マネジメントコンソール、AWS Command Line Interface (AWS CLI)、またはAWS DMS APIを使用して設定できます。これらの設定には、利用するテーブル構成、レプリケーションプロセス、移行エラーの処理方法、エラーのログ記録、および制御テーブル情報を指定することが含まれます。移行のタイプは "migrate existing data and replicate ongoing changes"を指定します。
・タスクを作成した後、直ちに実行できます。必要なメタデータ定義を含むターゲットテーブルが自動的に作成されてロードされるため、継続的なレプリケーションを指定できます。
・デフォルトでは、タスクを作成するとすぐに、AWS DMS によりタスクが開始されます。ただし、状況によっては、タスクの開始を延期できます。たとえば、AWS CLI を使用するとき、タスクを作成するプロセスと、トリガーイベントに基づいてタスクを開始する別のプロセスが存在する場合があります。必要に応じて、タスクの開始を延期できます。
・AWS DMS コンソール、AWS CLI、またはAWS DMS API を使用して、タスクのモニタリング、停止、再開を行うことができます。

オプション１は正しくありません。AWS DMSはレプリケーションインスタンスには、EC2インスタンスに設定するのではなく、DMSコンソールで作成する必要があります。

オプション2は正しくありません。AWS DMSによりオンプレミス側とAWSリソースを接続するためには、NATゲートウェイを介したアドレス変換通信やDirect Connectによる専用線接続などの様々な手段での接続を確立することができます。必ずしもVPN接続である必要はありません。

問題7: 正解

ある金融機関では、自社ネットワークとAWSのクラウドインフラストラクチャを接続するハイブリッドクラウドアーキテクチャを採用しました。そして、そこにEC2インスタンスとELBとS3バケットで構成されたアプリケーションを展開しました。この金融機関のソリューションアーキテクトとして、あなたはデータ暗号化に使用されるSSLキーの安全性を確保するように依頼されました。アプリケーションログは、S3バケットにアクセス権限のある少数のユーザーのみが復号化できるようにするために、S3の暗号化機能を利用することが必要です。

これらの要件を満たす設定方法を選択してください。

- (◉) ELBを利用してEC2インスタンスへのTCPロードバランシングによるトラフィック制御を実施し、AWS CloudHSMを利用してSSLトランザクションを実行する。その上で、SSEによる暗号化を実行してアプリケーションログをS3ストレージに蓄積する。 (正解)
- ( ) ELBを利用してEC2インスタンスへのUDPロードバランシングによるトラフィック制御を実施し、AWS KMSを利用してSSLトランザクションを実行する。その上で、SSEによる暗号化を実行してアプリケーションログをS3ストレージに蓄積する。
- ( ) ELBを利用してEC2インスタンスへのTCPロードバランシングによるトラフィック制御を実施し、AWS CloudHSMを利用してSSLトランザクションを実行する。その上で、ランダム生成したAESキーによる暗号化を実行してアプリケーションログをS3ストレージに蓄積する。
- ( ) ELBを利用してEC2インスタンスへのUDPロードバランシングによるトラフィック制御を実施し、AWS KMSを利用してSSLトランザクションを実行する。その上で、ランダム生成したAESキーによる暗号化を実行してアプリケーションログをS3ストレージに蓄積する。

説明

オプション1が正解となります。データの暗号化に使用されるSSLキーの安全性を確保するためには、CloudHSMを使用し、アプリケーションサーバーログがサーバーサイド暗号化（SSE）を使用してS3バケットに保持する仕組みを構築していくのが最適です。CloudHSMは、WebサーバーのSSL処理をオフロードしてアプリケーションログが永続的かつ安全に保存されるような暗号化を実施します。

AWS CloudHSM は、クラウドベースのハードウェアセキュリティモジュール (HSM) です。これにより、AWS クラウドで暗号化キーを簡単に生成して使用できるようになります。AWS CloudHSMを使用して、WebサーバーのSSL / TLS処理をオフロードできます。この処理にCloudHSMを使用すると、Webサーバーの負担が軽減され、Webサーバーの秘密キーをCloudHSMに保存することでセキュリティが強化されます。SSLおよびTLSは、Webサーバーの IDを確認し、インターネット上で安全なHTTPS接続を確立するために使用されます。

オプション2と4は不正解です。AWS KMSはAWS CloudHSMのようにSSL処理をオフロードするといった対応はできないため、KMSは不適切です。

オプション3は不正解です。S3バケットはSSEを利用した暗号化が標準機能として設定されています。したがって、S3バケットにアクセス権限のある少数のユーザーのみが復号化できるようにするためには、S3の暗号化機能を利用することが必要です。アプリケーションログをランダム生成したAESキーによって暗号化を実施するのではなく、SSEによって暗号化してS3ストレージに蓄積します。独自のAESキーによる暗号化だけでは、少数ユーザーへの権限制限が実行されているかを確認することができないため、回答として不十分となっています。

問題8: 不正解

B社では社内用インフラにAWSを使用しています。彼らは、世界中の顧客がアクセスする企業独自のコールセンターシステムを構築しています。このアプリケーションはコールセンターのピーク時には非常に負荷が高まりますが、夜間や朝早い時間帯では負荷が高まることはありません。また、ピーク時の発生時間はまちまちであり、事前に準備することが難しくなっています。したがって、アプリケーションによってピーク時の処理が問題なく実施されるスケーラブルな構成が必要不可欠です。データベースはオンライントランザクション処理（OLTP）が実施されており、この処理も同様にスケーラブルにする必要があります。

これらの要件を満たすためのAWSアーキテクチャ設計パターンを選択してください。

- ◉ EC2インスタンスベースのWEBサーバーをマルチAZ構成にして、ELBとAutoScalingの設定を行うインフラ構成を展開する。さらにOLTP処理にはRDSをRoute53によるフェールオーバー構成で利用する。 (不正解)
- ○ EC2インスタンスベースのWEBサーバーをマルチAZ構成にして、ELBとAutoScalingの設定を行うインフラ構成を展開する。さらにOLTP処理にはAuroraのマルチクラスター構成を利用する。
- ○ EC2インスタンスベースのWEBサーバーをマルチAZ構成にして、ELBとAutoScalingの設定を行うインフラ構成を展開する。さらにOLTP処理にはAurora Serverlessを利用する。 (正解)
- ○ EC2インスタンスベースのWEBサーバーをマルチAZ構成にして、ELBとAutoScalingの設定を行うインフラ構成を展開する。さらにOLTP処理にはRDSをマルチAZ構成で利用する。

説明

オプション3が正解となります。このシナリオでは、EC2インスタンスのWEBサーバーとOLTP処理を行うデータベースの両方をスケーラブルな構成によって可用性を高める必要があります。したがって、複数のアベイラビリティーゾーンにまたがるEC2インスタンスにAuto Scalingグループ とELBを設定することで高可用でスケーラブルなアーキテクチャが必要となります。これに加えて、データベース処理には不規則なピークが発生することからAurora Serverlessを利用します。

Aurora ServerlessはDB インスタンスクラスのサイズを指定せずにデータベースエンドポイントを作成できます。最小と最大のキャパシティーを設定します。 Aurora Serverlessでは、データベースエンドポイントがプロキシフリートに接続されます。このプロキシフリートでは、ワークロードをルーティングする先のリソースのフリートがオートスケーリングされます。プロキシフリートを使用すると、最小と最大のキャパシティー仕様に基づいて Aurora Serverless がリソースを自動的にスケールするため、接続が途切れることはありません。

オプション1は不正解です。Route53によるフェールオーバー設定によって、EC2インスタンスやRDSをマルチリージョン構成に直接に展開することができますが、まずはマルチAZ構成を利用することが基本的な設定となります。また、今回は不規則な需要に対する処理としてAurora Serverlessが最適となります。

オプション2と4は不正解です。RDSやAuroraではなく、Aurora Serverlessを利用した構成が適したケースです。AuroraやRDSではオートスケールによって自動で拡張することができません。要件に合致するのはAurora Serverlessになります。

問題9: 正解

A社は証券取引プラットフォームを運用するフィンテック企業です。取引プラットフォームは東京リージョン内の複数のアベイラビリティーゾーン（AZ）[ ]されています。取引プラットフォームが処理する大規模な金融取引量を考慮すると、システムがスケーラブルで可用性が非常に高く、災害に強い構成であることが必要不可欠です。コンプライアンス要件を満たす目標復旧時間（RTO）は2時間未満であり、目標復旧時点（RPO）は10分と定められています。あなたはソリューションアーキテクトとして、既存のアーキテクチャーを検証して、障害が発生した場合にコンプライアンス要件を満たせる構成となるように強化することが求められています。

このシナリオでは、システム障害が発生したときにRDSにおいてRTOおよびRPOの要件を達成するために、データベースレイヤーに対して、どのような対応が必要となりますか？

- ◉ 5分ごとにトランザクションログをS3 標準ストレージに蓄積して、日次でS3 標準ストレージにバックアップを取得する。 (正解)
- ○ 1時間ごとにトランザクションログをS3 標準ストレージに蓄積して、15分ごとにS3 標準ストレージにバックアップを取得する。
- ○ 10分ごとにトランザクションログをGlacier（標準）に蓄積して、2時間ごとにGlacier（標準）にバックアップも取得する。
- ○ データベースのマルチAZ構成によって、フェールオーバーを実行することで、即時に回復できるようにする。

説明

このシナリオでは、RDSにおいてRTOとRPOの要件を満たすために、永続的なストレージとデータベースのバックアップを使用する必要があります。よって、日次でRDSのバックアップを取得していれば、RDSは容易に2時間以内の復旧することが可能です。それを利用してデータベースなどを復元することができれば、2時間以内の復旧も可能となります。

RPOとは、情報システムから失われたデータをバックアップから復元する際に、過去のどの時点まで遡ることを許容するかを表す目標値となります。したがって、10分前までのログが必要です。5分ごとにトランザクションログが存在すれば、5分前の内容までデータを10分のRPO要件を満たすことが出来ます。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。1時間ごとにトランザクションログをS3 標準ストレージに蓄積して、15分ごとにS3 標準ストレージにバックアップを取得することでは、10分前までの処理やデータを回復させることができません。

オプション3は不正解です。RTOを達成するためにAmazon Glacierは理想的なソリューションではありません。 Glacierの標準的な取得時間は3〜5時間であり、その時間ではRTOを達成できません。

オプション4は不正解です。データベースのマルチAZ構成によって、フェールオーバーを実行することで、即時に回復できるようにすることは可能ですが、リージョンが停止した場合の想定や、データベース以外の回復性が考慮されていないため不正解です。

問題10: 不正解

スタートアップのA社は、現在新しいARモバイルゲームを作成しています。すべてのサーバー、データベースなどのリソースは、AWSのクラウドインフラストラクチャにホストされています。新しいゲームをテストすると、静的コンテンツを含めたゲームアセットやデータの読み込み時間や、リアルタイム計算処理が非常に遅いことがわかりました。あなたはソリューションアーキテクトとして、コンテンツ配信とゲームのリアルタイムデータの計算処理を改善するために、アプリケーションにキャッシュ処理を追加することが必要と考えています。

このゲームアプリケーションに推奨できるキャッシュ利用方法を選択してください。

- ◉ CloudFrontを利用して静的コンテンツ配信を行い、DynamoDB DAXによるキャッシュ構成をインメモリDBとして利用する。 (不正解)
- ○ CloudFrontを利用して静的コンテンツ配信を行い、ElastiCache Redisをインメモリ DBとして利用する。 (正解)
- ○ CloudFrontを利用して静的コンテンツ配信を行い、ElastiCache Memcachedをインメモリ DBとして利用する。
- ○ CloudFrontを利用して静的コンテンツ配信を行い、MySQLのオプション設定のMemcachedをインメモリDBとして利用する。

説明

オプション2が正解となります。このシナリオでは、CloudFrontを利用して静的コンテンツ配信を最適にした上で、Amazon ElastiCache for Redis をインメモリデータストアとしてキャッシュ高速化処理を実現することが最善の選択肢です。 Amazon ElastiCache for Redis はリアルタイムゲーム処理に利用するのに最適なサービスとなっています。適切なユースケースに適切なデータストレージを使用し、データアクセスパターンを考慮することで、パフォーマンスが大幅に向上するだけでなく、費用対効果の高いソリューションも提供します。Amazon ElastiCache for Redis はゲーム業界で役立つ他のデータ構造を提供しており、ゲームのリアルタイムデータの計算処理を改善するためには最適なソリューションです。

オプション3は不正解です。Memcached はデータをミリ秒で検索できる、オープンソースの分散型メモリ内キー値ストアです。Memcached でサイトのインフォメーションを得ることによって、コストを管理しつつ、サイトのパフォーマンスとスケーラビリティを向上することができます。セッションデータ管理など単純な処理を高速化する際はRedisではなく、Memcachedの方が運用が容易であり望ましいユースケースとなりますが、今回のようなリアルタイムデータの計算処理には、Redisを選択する方が良いユースケースとなります。

詳細は以下を参照ください。

https://aws.amazon.com/jp/blogs/news/building-a-real-time-gaming-leaderboard-with-amazon-elasticache-for-redis/

オプション1は不正解です。DynamoDBはNoSQLデータベースであり、初めからキャッシングおよびインメモリデータストアとして利用する際はElastiCacheの利用が優先されます。DAXはあくまでもDynamoDBの処理において更に高速処理を実現する仕組みとして利用します。

オプション4は不正解です。RDSのMySQLのオプション機能を有効化するとMemcachedを利用することができるようになります。これはMySQLの読み込み処理をキャッシュ処理によって高速化するためのものであるため、今回の要件には利用できません。

問題11: 不正解

ベンチャー企業のB社はAWSを利用した開発環境を整備して、様々なアプリケーションを開発しています。現在、社内には開発環境、テスト環境、および本番環境のそれぞれを利用する開発中のWEBアプリケーションがあります。このアプリケーションの展開とバージョン管理にはAWS Elastic Beanstalkを使用します。テストチームはアプリケーションのリリース準備をしており、テストチーム専用のEC2インスタンスによってテスト済みの実稼働データをRDS MySQLに保存します。開発チームは本番リリース用のEC2インスタンスによって同じ実稼働データにアクセスすることが必要です。

上記の要件を満たす永続性とセキュリティが確保された最適なソリューションを選択してください。

- ◉ RDS DBインスタンスを個別に作成して、RDSのDNS名を使用してアプリケーションに接続する。本番用のEC2インスタンス用のセキュリティグループを作成して、DBインスタンスのセキュリティグループへのトラフィックを許可する。 (不正解)
- ○ AWS Elastic BeanStalkのデプロイ構成において本番用のRDSのDBインスタンスを作成して、RDSのDNS名を使用してアプリケーションに接続する。クライアントマシン用のセキュリティグループを作成して、DBインスタンスのセキュリティグループへのトラフィックを許可する。Elastic BeanStalk設定においてDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施する。 (正解)
- ○ RDS DBインスタンスを個別に作成して、そのIPアドレスを使用してアプリケーションに接続する。クライアントマシン用のセキュリティグループを作成して、DBインスタンスのセキュリティグループへのトラフィックを許可する。Elastic BeanStalk設定においてRDSのDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施する。
- ○ AWS Elastic BeanStalkのデプロイ構成において本番用のRDS DBインスタンスを作成して、そのIPアドレスを使用してアプリケーションに接続する。クライアントマシン用のセキュリティグループを作成して、DBインスタンスのセキュリティグループへのトラフィックを許可する。

説明

オプション2が正解となります。このシナリオでは、テストチームと開発チームがそれぞれ専用のEC2インスタンスを介してRDS内の実稼働データにアクセスするために、EC2インスタンスからの限定的なRDSデータベースアクセス権限が必要となります。また、この状態は本番環境にも利用されるため、一時的なアクセスではなく永続性があることが要件になっています。

AWS ElasticBeanstalkでは環境作成オプションとしてRDS DBインスタンスを紐付けて作成することが可能ですが、ElasticBeanstalk構成から作成されたRDSインスタンスはElasticBeanstalk環境のライフサイクルに紐付けられているため本番環境としては、個別にRDS DBインスタンスを用意して接続することがAWSでは推奨されていました。つまり、Elastic Beanstalk設定からRDS DBインスタンスを作成すると、その後の挙動や管理をするためにデカップリングを実施することが必要となりますが、Elastic Beanstalkがデカップリングを実施するとDBインスタンスを削除してしまうため、DB管理が難しくなっていました。

しかしながら、2021年末に新機能として、Elastic BeanStalk設定においてRDSのDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施する。ということができるようになり、ライフサイクルに紐づけられていて問題になることを回避できるようになりました。したがって、Elastic BeanStalk設定から本番用のRDSのDBインスタンスを作成して、RDSのDNS名を使用してアプリケーションに接続した上で、Elastic BeanStalk設定においてRDSのDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施することができます。

オプション1は不正解です。Elastic Beanstalkでは環境作成オプションとしてRDS DBインスタンスを紐付けて作成することが可能ですが、作成されたRDSはBeanstalk環境のライフサイクルに紐付けられているため本番環境としては、個別にRDSを用意して接続することがAWSでは推奨されていましたが、現在はElastic BeanStalk設定においてRDSのDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施することができます。

オプション3は不正解です。RDSのDBインスタンスの接続方式としてIPアドレスではなくDNS名を利用することが接続方式となっています。したがって、DNS名を利用したアクセス設定を構成することになります。

オプション4は不正解です。Elastic Beanstalkでは環境作成オプションとしてRDS DBインスタンスを紐付けて作成することが可能ですが、その際はElastic BeanStalk設定においてRDSのDBインスタンスのデータベース削除ポリシーの「保持」を有効化して、RDSのデカップリングを実施することが必要です。

問題12: 不正解

あなたの会社は画像診断アプリや顔認証システム開発を得意としたベンチャー企業です。あなたはソリューションアーキテクトとして、新しい画像分析アプリケーションを運用しています。このアプリケーションは画像データ分析を実行後、いくつかのファイルにわけて出力ストリーム上で書き込み処理を実施します。1日あたりのデータ処理用の入力ファイル数が大変多く、特に日中の数時間にデータ分析処理が集中しています。現在の構成では、入力データとデータ分析処理結果を保存する単一のEBSボリュームをアタッチしたEC2インスタンスを利用してデータ処理を行っています。このプロセスを完了するために1日あたり約10時間も要しているため、改善が必要となっています。

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

◉ 利用していたEBSの汎用ストレージにI/Oファイルを保存した上で複数インスタンスからのアクセスが可能なようにマルチアタッチ機能を有効化する。データ処理をするEC2インスタンスに対してAutoScalingを設定して高負荷時にスケーリング可能として、ELBによるトラフィック分散を実現する。さらにSQSキューによってタスク処理を分散化することで、全体の処理時間を短縮する。 (不正解)

○ EBSのプロビジョンドIOPSにI/Oファイルを保存した上で複数インスタンスからのアクセスが可能なようにマルチアタッチ機能を有効化する。データ処理をするEC2インスタンスに対してSQSによるキューイング処理を設定して並列処理が実行できるようにした上で、SQSキューの負荷メトリクスに応じたAutoScalingを設定する。 (正解)

○ 利用していたEBSの汎用ストレージにI/Oファイルを保存した上で複数インスタンスからのアクセスが可能なようにマルチアタッチ機能を有効化する。データ処理をするEC2インスタンスに対してAutoScalingを設定して、ELBによるトラフィック分散を実現する。さらにRoute53によるルーティング処理を行う。

○ S3 Standardストレージに I/Oファイルを保存した上で複数インスタンスからのアクセスが可能なようにマルチアタッチ機能を有効化する。データ処理をするEC2インスタンスに対してAutoScalingを設定する。さらにSQSキューによってタスク処理を分散化することで、全体の処理時間を短縮する。

説明

オプション2が正解となります。このシナリオの要件を実現するためには、EC2インスタンスをAutoScalingグループに配置してスケーリングができる構成とした上で、高可用で処理性能が高いストレージを選択してコスト最適化をはかり、SQSキューによるタスクの並行処理を実現することが考えられます。

特に、EBSボリュームに単一のEC2インスタンスが処理をしているため、一処理負荷が集中していることが問題となっています。これを改善するには、EBSのプロビジョンドIOPSにI/Oファイルを保存した上で複数インスタンスからのアクセスが可能なようにマルチアタッチ機能を有効化することが必要です。通常のEBSは単一のインスタンスからのみアクセスを可能にする仕組みですが、EBSのプロビジョンドIOPSボリュームは複数インスタンスからのアクセスを可能にするマルチアタッチ機能を有しています。

さらにデータ処理をするEC2インスタンスに対してAutoScalingを設定しスケーリングできるようにした上で、SQSを連携してタスク処理を分散化します。その上で、キューにメッセージが大量に蓄積された場合に備えて、SQSキューの負荷メトリクスに対してAutoScalingを設定することで自動スケーリングを実現します。

オプション1と3は不正解となります。EBSの汎用ストレージは複数のEC2インスタンスからアクセスすることができません。また、処理能力が劣るため、プロビジョンドIOPSを利用する方が最適なパフォーマンスを発揮できます。

オプション4は不正解です。EC2インスタンスに対してAutoScalingを設定するのではなく、SQSキューサイズなどに対してAutoScalingを設定することが必要となります。また、S3ストレージを利用しているオプション4は不正解となります。

【参照】

Amazon EBS マルチアタッチを使用した複数のインスタンスへのボリュームのアタッチ - Amazon Elastic Compute Cloud

問題13: 不正解

あなたの会社は大規模なEコマースサイトを運営しているソフトウェア企業です。あなたはWEBマーケティング担当者として、Eコマースサイト上の顧客のクリックストリームデータを分析して、行動分析ソリューションを開発する必要があります。会社は顧客がクリックしたWEBページに対する広告の影響を把握して、商品が購入される場合のユーザーのWEB行動パターンを解析したいと考えています。

これらのデータ分析要件を満たすアーキテクチャとして、間違っている内容を選択してください。

- ◉ Amazon Kinesis Data Streamsを利用してクリックによるセッションデータを取得して、アプリケーション側にKCLワーカーを組み込んで行動分析を実施する。 (不正解)
- ○ Amazon Kinesis Data Streamsを利用してクリックによるセッションデータを取得して、Amazon Kinesis Data Analyticsを利用して行動分析を実施する。
- ○ Amazon Kinesis Data Streamsを利用してクリックによるセッションデータを取得して、Kinesisエージェントを利用して行動分析を実施する。 (正解)
- ○ Amazon Kinesis Data Streamsを利用してクリックによるセッションデータを取得して、Kinesis Client Libraryを利用して行動分析を実施する。

説明

このシナリオでは、Amazon Kinesis Data Streamsアプリケーションと呼ばれるストリームデータを利用したデータ処理アプリケーションを作成することが求められています。

オプションの中で、Amazon Kinesis Data Streamsアプリケーションを構築する上で無関係な説明はオプション3になります。Kinesis エージェントだけでは行動分析を実施することはできません。Kinesis エージェントはスタンドアロンの Java ソフトウェアアプリケーションであり、データを収集して Kinesis Data Streams に送信する簡単な方法を提供する仕組みです。

オプション1は正しい説明です。Amazon Kinesis Data Streamsによって処理されたレコードはダッシュボードに送信されて、さまざまなAWSサービスへのデータ送信に使用できます。分析処理を実現するために、アプリケーション側にKCLワーカーを組み込んで行動分析を実施することができます。

オプション2は正しい説明です。Amazon Kinesis Data Analytics は、ストリーミングデータの分析に利用するサービスです。Amazon Kinesis Data Analytics を利用して、ストリーミングアプリケーションを構築し、管理することができます。したがって、Amazon Kinesis Data Analyticsを利用して、ストリーミングアプリケーションを構築し、分析処理を実現することが可能です。

オプション4は正しい説明です。典型的なAmazon Kinesis Data Streamsアプリケーションは、Amazon Kinesisストリームからデータをデータレコードとして読み取ります。これらのアプリケーションはAmazon Kinesis Client Library（KCL）を使用することでAmazon EC2インスタンスで実行するデータ分析アプリケーションを作成することができます。

問題14: 不正解

ある会社ではEC2インスタンスに対してALBとAuto Scalingグループを設定したWEBアプリケーションを構築しています。あなたはプライベートサブネット内にあるデータレイヤーにおいて、リザーブドインスタンスにPostgreSQLデータベースサーバーをセットアップしているところです。データベースサーバーの命名規則を簡素化するために、データベースにカスタムドメイン名を割り当てることが必要です。

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。

- (●) Route 53でパブリックホストゾーンを設定して、sample.comなどのCNAMEレコードを作成し、データベースサーバーのIPアドレスを指定する。 (不正解)
- ( ) Route 53でパブリックホストゾーンを設定して、sample.comなどのAまたはAAAAレコードを作成し、データベースサーバーのIPアドレスを指定する。
- ( ) Route 53でプライベートホストゾーンを設定して、sample.comなどのCNAMEレコードを作成し、データベースサーバーのIPアドレスを指定する。
- ( ) Route 53でプライベートホストゾーンを設定して、sample.comなどのAまたはAAAAレコードを作成し、データベースサーバーのIPアドレスを指定する。 (正解)

説明
データベースサーバーの命名規則を簡素化するために、データベースにカスタムドメイン名を割り当てるにはRoute53のプライベートホストゾーンを利用したドメイン指定を行います。プライベートホストゾーンは、1つ以上のVPC内のドメインとそのサブドメインに対するDNSクエリにAmazon Route 53が応答する方法に関する情報を保持するコンテナです。プライベートホストゾーンの動作は次のとおりです。

1．example.comなどのプライベートホストゾーンを作成して、そのホストゾーンに関連付けるVPCを指定します。

2．VPC内およびVPC間でドメインとサブドメインのDNSクエリにRoute 53が応答する方法を決定するホストゾーンにレコードを作成します。たとえば、プライベートホストゾーンに関連付けたVPCの1つで、EC2インスタンスで実行されるデータベースサーバーがある場合です。AまたはAAAAレコードを作成し(例: db.example.com)、データベースサーバーのIPアドレスを指定します。

3．アプリケーションがdb.example.comへのDNSクエリを送信すると、Route 53は対応するIPアドレスを返します。また、アプリケーションは、example.comプライベートホストゾーンに関連付けたVPCでEC2インスタンスを実行している必要があります。

4．アプリケーションは、Route 53から取得したIPアドレスを使用して、データベースサーバーとの接続を確立します。

したがって、正しい設定方法を説明しているオプション4が正解となります。

オプション1と2は不正解です。今回はプライベートネットワーク上のデータレイヤーの設定をしています。したがって、データベース自体にパブリックホストゾーンを利用してドメインを関連付けることは不適切な対応となります。VPC内部での処理を実施するために、プライベートホストゾーンを設定してカスタム名称を設定することが必要です。

問題15: 不正解

ある会社ではデータウェアハウスとしてAmazon Redshiftを使用しています。このRedshiftでは複数のデータ処理プロセスを実施しています。１つの処理は数分で終了するようなデータ処理ですが、これは頻繁に発生するため、速やかに実行される必要があります。もう１つの処理は財務情報データ分析であり、これには大量のデータ処理が必要なため完了までに数時間かかりますが、発生頻度は低いです。また、それぞれのデータ処理は担当者が異なります。あなたはソリューションアーキテクトとして、Redshiftへの高負荷を発生させるため、長時間かかるデータ処理が全体のクエリパフォーマンスに影響がないようにする必要があります。

この問題を改善するためのAWSアーキテクチャ設計パターンを選択してください。

- ◉ Redshiftクラスターのレプリカを起動させて、各データ処理の処理性能を向上させる。 (不正解)
- ○ ２つのIAMグループによってRedshiftの利用権限を分離して、該当する権限を持ったグループに担当者を割り当てる。
- ○ Redshiftにおいて2つのワークロード管理（WLM)）を作成して、それぞれのデータ処理の担当者を割り当てる。 (正解)
- ○ タグ名によりRedshiftの利用権限範囲を２つに分離することで、ワークロードを分割する。

説明

Amazon Redshiftのワークロード管理（WLM）機能を使用すると、ユーザーはワークロード内の優先順位を柔軟に管理できるため、長時間実行されるクエリキューによって、短時間で高速に実行されるクエリ処理が停滞しないように調整することができます。よって、ワークロード管理によって２つのワークロード処理を分割することが適切な対応となり、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。Redshiftクラスターにレプリカを起動させる機能はありません。Amazon Redshift データウェアハウスは、ノードと呼ばれるコンピューティングリソースの集合で、クラスターと呼ばれるグループに構成されています。通常はノードのタイプやノード数を調整してパフォーマンスを改善します。

オプション２は不正解です。本件では同じRedshiftによるワークロードの処理分割が求められており、IAMグループによるRedshiftの利用権限を分離するといった対応は必要ありません。

オプション４は不正解です。タグ名によりRedshiftクラスターに名称を追加することは可能ですが、タグによって同じRedshiftクラスター内で権限を分割をすることはできません。

問題16: 正解

あなたの会社はAWSのEC2インスタンスを利用した Windows Server にホストしたアプリケーションを運用しています。アプリケーションスタックの更新プロセスを改善するために、システムの更新方式としてインプレースアップグレードと並行アップグレードのどちらが良いかを検討して、あなたはマネージャーに説明することになりました。

インプレースアップグレードと並行アップグレードの説明として正しい内容を選択してください。（2つ選択してください。）

- [x] インプレースアップグレードはオペレーティングシステムファイルをアップグレードして、個人の設定およびファイルは維持する。 (正解)
- [x] 並行アップグレードでは元のEC2インスタンスの設定、構成、データを取り込んで、これらの情報を新しいAmazon EC2インスタンスの新しいバージョンのオペレーティングシステムに移行する。 (正解)
- [ ] インプレースアップグレードは古いインスタンスを終了してから、新しいEC2インスタンスを展開する。
- [ ] インプレースアップグレードでは、新しいインスタンスがアクティブになるまで、元のEC2インスタンスを一時的なものとして利用する。
- [ ] 並行アップグレードはオペレーティングシステムファイルをアップグレードして、個人の設定およびファイルは維持する。

説明

インスタンスで実行している旧バージョンの Windows Server をアップグレードするには、インプレースアップグレードと並行アップグレード)の２通りの方法があります。

・インプレースアップグレードはオペレーティングシステムファイルをアップグレードし、個人の設定およびファイルは維持されます。インプレースアップグレードは、一貫したロールアウトスケジュールによる迅速な展開に役立ちます。これはセッションレスアプリケーション用に設計されています。ローリングデプロイメントスケジュールを実装することにより、ステートフルアプリケーションにインプレースアップグレード方式を引き続き使用できます。

・並行アップグレードでは、元のEC2インスタンスの設定、構成、データを取り込んで、この情報を新しい Amazon EC2 インスタンス上のより新しいバージョンのオペレーティングシステムに移行します。並行アップグレードでは、アプリケーションに不明な依存関係があるかどうかを簡単に知ることができます。移行中は新しいインスタンスがアクティブになるまで、元のEC2インスタンスを一時的なものとして利用されます。新しいリリースでは、古いインスタンスを終了することにより、EC2インスタンスの新しいセットがロールアウトされます。

したがって、オプション１と２が正解です。

オプション３は不正解です。並行アップグレードが古いインスタンスを終了して新しいEC2インスタンスのセットを展開します。

オプション４は不正解です。並行アップグレードにおいて、新しいインスタンスがアクティブになるまで、元のEC2インスタンスを一時的なものとして利用されます。

オプション５は不正解です。イングレースアップグレードがオペレーティングシステムファイルをアップグレードし、個人の設定およびファイルは維持する方式です。

問題17: 不正解

あなたはソリューションアーキテクトとして、AWS上に建設現場の進捗共有モバイルアプリを作成しています。このアプリケーションでは建設現場の写真をアップロードして、ユーザー間で共有することで視覚的に進行状況を管理することができます。モバイル端末で撮影した写真をアプリケーションにアップロードすると、アプリケーションは写真をEC2インスタンスにホストされているWebサーバーに送信し、プロジェクトの詳細と撮影日を含む各写真に透かしを追加します。こうした画像データ[白]バケットにアップロードして永続的に保存することが必要です。

EC2インスタンスがS3バケットに画像をアップロードする際の、安全な設定方法を選択してください。

- (●) S3オブジェクトへのアクセス権限を付与したIAMユーザーを作成して、EC2インスタンスにアタッチする。EC2インスタンスはインスタンスユーザーデータから資格情報を取得して、S3にアクセスして写真をアップロードする。 (不正解)
- ( ) S3オブジェクトへのアクセス権限を付与したIAMロールを作成して、EC2インスタンスにアタッチする。EC2インスタンスはインスタンスユーザーデータから資格情報を取得して、S3にアクセスして写真をアップロードする。
- ( ) S3オブジェクトへのアクセス権限を付与したIAMロールを作成して、EC2インスタンスにアタッチする。EC2インスタンスはインスタンスメタデータから資格情報を取得して、S3にアクセスして写真をアップロードする。 (正解)
- ( ) S3オブジェクトへのアクセス権限を付与したサービス管理ポリシー（SCP）を作成して、EC2インスタンスにアタッチする。EC2インスタンスはインスタンスメタデータから資格情報を取得して、S3にアクセスして写真をアップロードする。
- ( ) S3オブジェクトへのアクセス権限を付与したサービス管理ポリシー（SCP）を作成して、EC2インスタンスにアタッチする。EC2インスタンスはインスタンスユーザーデータから資格情報を取得して、S3にアクセスして写真をアップロードする。

説明

オプション3が正解となります。アプリケーションサーバーはEC2インスタンスで実行されており、アプリケーションは写真を保存する際にS3にリクエストを実施することが必要となります。その際にEC2インスタンスに対してS3バケットへのアクセス権限が付与されたIAMロールが必要です。EC2インスタンスにアタッチできるIAMロールを作成して、EC2インスタンスに対してS3バケットなどの他のAWSリソースへのアクセスに使用できる一時的なセキュリティ認証情報を提供することができます。これらのアクセスに利用する資格情報はインスタンスのメタデータに保持されています。

オプション1はIAMロールではなくIAMユーザーを認証情報として利用しているため、不正解です。リソース間の権限付与にはIAMロールを利用する必要があります。

オプション2は不正解です。インスタンスユーザーデータではなく、メタデータから資格情報を取得することになります。

オプション4と5は不正解です。AWS OrganizationsにおいてSCPを使用すると、組織（OU）に対してアカウントレベルでアカウントのユーザー、グループ、およびロールが実行できるサービスとアクションを制限することができます。これはユーザーやロールへの個別のアクセス権限を付与することはできないので、本件の要件では使用しません。

問題18: 正解

あなたはソリューションアーキテクトとして、不動産企業のB社にに勤めています。この会社ではAWS Organizationsを使用して、統合された複数のAWSアカウントを有しています。現在会社では、非公開の不動産プロパティ専用のオンラインポータルサイトを構築しています。オンラインポータルでは、セキュリティを強化するためにSSLを使用することが必要です。X.509証明書にはプライベートキーが含まれ、AWS Certificate Manager（ACM）に保存されます。要件としてセキュリティチームのみがアプリケーションのX.509証明書に排他的にアクセスできる権限設定が必要です。なお、開発チームはEC2インスタンスへの管理権限を有しています。

この要件を満たす最適なオプションは次のうちどれですか？

- ◉ X.509証明書にアクセスできる権限をセキュリティチームに与えるために、ELBとACMに対するIAMポリシーを設定して、ELBがこの証明書を使用してSSL接続を終了する構成を追加する。 (正解)
- ○ X.509証明書にアクセスできる権限をセキュリティチームに与えるために、ACMに対するIAMポリシーを設定して、ELBがこの証明書を使用してSSL接続を終了する構成を追加する。
- ○ X.509証明書にアクセスできる権限をセキュリティチームに与えるために、ACMに対するIAMポリシーを設定して、EC2インスタンスがこの証明書を使用してSSL接続を終了する構成を追加する。
- ○ X.509証明書にアクセスできる権限をセキュリティチームに与えるために、ELBとACMに対するIAMポリシーを設定して、EC2インスタンスがこの証明書を使用してSSL接続を終了する構成を追加する。

説明

このシナリオでは、セキュリティチームのみがアプリケーションのX.509証明書に排他的にアクセスできるように権限管理をすることが必要です。そのためには、IAMポリシーによってセキュリティチームへのACMに対するアクセス権限を設定することが必要です。

ELBを利用したEC2インスタンスへのSSL通信を設定する場合は、ELB側またはEC2インスタンスがACMが生成した証明書を使用してSSL接続を終了して、クライアントからのリクエストを復号します。前者を選択した場合、X.509証明書はELBにのみ存在し、後者を選択した場合、X.509証明書はEC2インスタンス内に保存されます。

開発チームはEC2インスタンスへのアクセス権限を有しているため、開発チームが証明書にアクセスできないようにするためには、EC2インスタンスではなくELBレベルでSSLを終了することが必要です。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。IAMポリシーによるアクセス権限設定はSSL認証情報が付与されている、ACMとELBのどちらにも設定することが必要となります。

オプション３と４は不正解です。開発チームが証明書にアクセスできないようにするためには、EC2ではなくELBレベルでSSLを終了することが望ましいです。

問題19: 不正解

あなたは社内のシステム運用担当者として、AWS環境を管理しています。現在は、開発環境用のAWSアカウントとテスト環境用のAWSアカウントの２つのアカウントが利用されています。あなたは全てのAWSアカウントをまとめて予算管理をする必要があるため、一括請求を有効にして各アカウントの請求をマスターアカウントに統合しました。これによって、予算の統合管理が可能になり、運用の一元化とコストメリットを得ることができます。追加の要件として、AWSの利用コストを予算内に収めるために、マスターアカウント管理者が、開発環境用のアカウントとテスト環境用のアカウントの両方のアカウントでリソースを停止、削除、および終了できる必要となります。

このシナリオにおいて、上記の要件を満たす設定方法を選択してください。

- ◉ マスターアカウントのフル管理者権限を有するIAMユーザーによって、開発環境とテスト環境に対するクロスアカウントロールを付与する。 (不正解)
- ○ 各メンバーアカウントにおいて、IAMユーザーと開発環境アカウントとテスト環境アカウントへのフル管理者権限を有するクロスアカウントロールを作成して、マスターアカウントに権限を譲渡する。
- ○ マスターアカウントにおいてIAMユーザーを作成する。次に、開発環境とテスト環境のアカウントをメンバーアカウントとした上で、マスターアカウントに対してクロスアカウントロールを付与する。 (正解)
- ○ マスターアカウントにメンバーアカウントを招待するとデフォルト設定で、配下にあるアカウントに対するフル管理者権限とクロスアカウントロールが付与されるため、それを利用することで目的を達成できる。

説明

オプション３が正解となります。AWS Organizations コンソールを使用してメンバーアカウントを作成すると、アカウントの IAM ロール権限である OrganizationAccountAccessRole が自動的に作成されます。このロールには、メンバーアカウントの完全な管理権限が含まれます。また、このロールにも、組織のマスターアカウントへのアクセス権限が付与されています。このIAMロールを使用してメンバーアカウントにアクセスするためには、マスターアカウントに対してクロスアカウントアクセスを設定することことが必要です。そうすることで各アカウントに個別のIAMユーザーを作成する必要がなくなります。

したがって、マスターアカウントの管理者が、開発環境とテスト環境の両方のアカウントでリソースを停止、削除、および終了できるようにするためには、マスターアカウントから開発環境とテスト環境のアカウントをメンバーアカウントとして招待して、その後 OrganizationAccountAccessRole によるクロスアカウント権限を付与することが必要です。

オプション１は不正解です。フル管理者権限を有するIAMユーザーによって、開発環境とテスト環境に対するクロスアカウントロールを付与することはできないため、正しくありません。クロスアカウントロールを設定するには、IAMユーザー側に他のアカウント側から権限を付与することが必要です。

オプション２は不正解です。各メンバーアカウントにおいて、IAMユーザーと開発環境アカウントとテスト環境アカウントへのフル管理者権限を有するクロスアカウントロールを作成して、マスターアカウントに対して権限を譲渡するといった設定はありません。マスターアカウント側でクロスアカウントロールを作成することができます。

オプション４は不正解です。メンバーアカウントを招待した場合、マスターアカウントのデフォルト設定で、配下にあるアカウントに対するフル管理者権限とクロスアカウントロールは付与されてはいません。

問題20: 正解

あなたはソリューションアーキテクトとして、オンプレミスのデータセンターでホストされるコンテンツ管理システム（CMS）を構築しています。このCMSは、アプリケーション層ではWINDOWSアプリケーションサーバーを利用し、データベース層ではOracleデータベースを利用した構成となっています。このデータベースは非常に重要なデータを保存しているため、Oracle Recovery Managerにより定期的にAWS上のストレージにバックアップを保存して、シェルアクセスによる権限設定を行います。

バックアップに基づいた回復性を高めるソリューションを選択してください。

- ◉ EC2インスタンスを利用してWEBアプリケーションサーバーとオラクルデータベースを設定して、S3バケットに復元用のバックアップファイルを保存する。 (正解)
- ○ Oracleソフトウェアを選択したRDSをデータベースサーバとした上で、EC2インスタンスを利用してWEBアプリケーションサーバーを設定する。その上で、S3バケットに復元用のバックアップファイルを保存する。
- ○ EC2インスタンスを利用してWEBアプリケーションサーバーとオラクルデータベースを設定して、Glacierに復元用のバックアップファイルを保存する。
- ○ Oracleソフトウェアを選択したRDSをデータベースサーバとした上で、EC2インスタンスを利用してWEBアプリケーションサーバーを設定する。その上で、Glacierに復元用のバックアップファイルを保存する。

説明

オプション1が正解となります。RDSをマネージドサービスとして利用するために、Amazon RDS は DB インスタンスへのシェルアクセスを提供していません。また、高度な特権を必要とする特定のシステムプロシージャやテーブルへのアクセスを制限しています。したがって、今回の要件を達成するためにはRDSではなく、EC2インスタンスにOracleデータベースソフトウェアをインストールして構成することが必要となります。

Oracle Recovery Manager（Oracle RMAN）は、あらゆるOracleデータ形式の高度なパフォーマンス要求や、管理性の高いバックアップおよびリカバリへの要望に応える製品です。高可用性やディザスタ・リカバリに対する完全な戦略を実現するには、信頼できるデータのバックアップ、リストア、およびリカバリの手順が必要です。Oracle RMANは、Oracleデータベースを効率的にバックアップおよびリカバリするための包括的な基盤を提供します。これはサーバーと緊密に連携するよう設計されており、バックアップおよびリストア中のブロック・レベルの破損を検出する機能を提供します。

また、AWS上のデータベースのバックアップ先として最適なストレージはS3 Standardです。S3 Standardはリージョンベースで非常の可用性と耐久性が高いバックアップの保存が可能となります。また、即時にデータをとりだすことができるため、リカバリ時間を短縮することが可能となります。

オプション2と4は不正解です。マネージドサービスを提供するために、Amazon RDS は DB インスタンスへのシェルアクセスを提供していません。

オプション3は不正解です。Glacierに保存されたバックアップによる復元はS3よりも遅くなってしまうため、リカバリ時間が長時間となり、データベースの最適なバックアップ先ではありません。

問題21: 不正解

大手会計ファームでは東京リージョンを起点として、日本国内の会計サービス向けの決済アプリケーションをローンチしました。このアプリケーションは[白]ージョン内の3つのVPCを利用してデプロイされています。このアプリケーションが最適に動作するためには、すべてのVPCのすべてのリザーブドEC2インスタンスが相互に通信できることが必要です。また、VPC間で制限なしに相互にリソースを共有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。

- ◉ IPv6用に1つのVPCが2つのVPCとピアリング接続を実施する。 (不正解)
- ○ 1つのVPCに対して、残り2つのVPCがVPCピアリング接続を実施する。
- ○ 3つのVPC間でVPCピアリングのフルメッシュ設定を利用する。 (正解)
- ○ 3つのVPC間で推移的なピア接続関係を構成する。

説明

オプション3が正解となります。以下のようなフルメッシュ設定に[白]3つのVPCを相互にピアリング接続します。VPCはすべて、同じAWSアカウントに存在し、重複するCIDRブロックはありません。

・VPC AはVPCピアリング接続 pcx-aaaabbbb によりVPC Bにピアリング接続しています。

・VPC AはVPCピアリング接続 pcx-aaaacccc によりVPC Cにピアリング接続しています。

・VPC BはVPCピアリング接続 pcx-bbbbcccc によりVPC Cにピアリング接続しています。

VPC間で制限なしに相互にリソースを共有する必要がある場合に、このフルメッシュ設定を使用することが必要です。たとえば、ファイル共有システムなどがユースケースとなります。各VPCのルートテーブルは、該当するVPCピアリング接続を指して、ピアVPCのCIDRブロック全体にアクセスします。

オプション1は不正解です。この設定では、各VPCのルートテーブルは該当するVPCピアリング接続を示し、ピアVPCのIPv6 CIDRブロック全体にアクセスします。これは3つのVPC間での接続を可能にするものではありません。

オプション2は不正解です。1つのVPCに対して、残り2つのVPCをVPCピアリング接続を実施するだけでは、残り2つのVPC間での通信ができません。

オプション4は不正解です。VPCピアリング接続は、2つのVPC間の1対1の関係となります。自分の各VPCに対して複数のVPCピア接続を作成できますが、推移的なピア接続関係はサポートされません。VPCと直接ピア関係にないVPCとのピア関係を作成することはできません。

問題22: 不正解

大手商社A社ではアプリケーションをオンプレミス環境において実行しています。このアプリケーションはトラフィックの大幅な増加が予想されており、スケーリングなどの負荷軽減策が必要不可欠となっています。残念ながら、トラフィック増加の予定期間内にアプリケーションをAWSに移行することはできません。あなたはソリューションアーキテクトとして、現在のオンプレミスアプリケーションを使用して、トラフィックの一部をAWSにオフロードすることで、短期間にスケーリングを実現することが必要です。また、このアプリケーションが提供するコンテンツなどの変更事項が即時に反映されることが必要です。

この要件を達成する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。

- ◉ Route53を構成してMaximum TTLを100／Default TTLを0／Minimum TTLを100に設定する。DNSをAWSにオフロードしてトラフィックを処理し、オンプレミスサーバーをオリジンとしてピーク時のトラフィックを処理する (不正解)
- ○ CloudFrontを構成してMaximum TTLを0／Default TTLを0／Minimum TTLを0に設定する。DNSをAWSにオフロードしてトラフィックを処理し、オンプレミスサーバーをオリジンとしてピーク時のトラフィックを処理する (正解)
- ○ CloudFrontを構成してMaximum TTLを100／Default TTLを0／Minimum TTLを0に設定する。DNSをAWSにオフロードしてトラフィックを処理し、オンプレミスサーバーをオリジンとしてピーク時のトラフィックを処理する
- ○ CloudFrontを構成してMaximum TTLを100／Default TTLを0／Minimum TTLを100に設定する。DNSをAWSにオフロードしてトラフィックを処理し、オンプレミスサーバーをオリジンとしてピーク時のトラフィックを処理する
- ○ Route53を構成してMaximum TTLを0／Default TTLを0／Minimum TTLを0に設定する。DNSをAWSにオフロードしてトラフィックを処理し、オンプレミスサーバーをオリジンとしてピーク時のトラフィックを処理する

説明

このシナリオではAWSに移行する時間はないため、アプリケーションをAWSに移行するのではなく、オンプレミス環境にとどまる必要があります。その上で、ピーク時のトラフィックを処理し、オンデマンドでスケーリングするためのAWSサービスを活用することが必要です。

CloudFrontはオンプレミスサーバーをカスタムオリジンとして設定できるため、短期間の設定でオンプレミス環境にあるオリジンサーバーの負荷を分散することができます。このアプリケーションはコンテンツなどの変更点が即時に反映されなければならないという要件があるため、設定は全てのTTLを0に設定します。こうすることで、コンテンツは変更されると即時にオリジンから配信されます。したがって、オプション2が正解となります。

オプション1と5は不正解です。Route53ではなく、CloudFrontを利用してキャッシュ処理によるオフロードを実現します。

オプション3と4は不正解です。このアプリケーションはコンテンツの変更点が即時に反映されるという要件があるため、設定は全てのTTLを0に設定することが必要です。

問題23: 不正解

あなたの会社は社内の顧客管理システムにおいてOracleデータベースを利用しています。 このオラクルデータベースはAWSパブリッククラウドでOracle RAC構成を実装しています。あなたは社内のソリューションアーキテクトとして、 Oracle RAC構成の耐久性を高めるために、RACクラスターでバックアップを構成するように依頼されています。

このデータベースのバックアップを構成するための、最適なソリューションを選択してください。

- (●) RDS Oracleデータベースを立上げてフェールオーバー構成を有効化して、バックアップ取得に利用する。 (不正解)
- ( ) RAC用の自動バックアップを有効化して、定期的にバックアップを取得する。
- ( ) RDS Oracleデータベースを立上げて自動バックアップを有効化して、定期的にバックアップを取得する。
- ( ) RAC用に展開されたEC2インスタンスに付随するEBSボリュームのスナップショットを取得するスクリプトを実行する。 (正解)

説明

Oracle Real Application Cluster（RAC）は、1つのデータベース（複数のデータファイルのセット）を1台、もしくは複数のサーバインスタンスで構成して、複数クライアントから同時にアクセス可能にするOracle社によるシェアードエブリシング型のデータベースクラスターテクノロジーです。RACを使用すると、Oracle Databaseをクラスター化できます。Oracle RACでは、インフラストラクチャとしてOracle Clusterwareを使用し、複数のサーバーを関連付けてそれらが単一のシステムとして動作するように構成します。

現在、RACはAmazon RDS Oracleではサポートされておらず、RDSを利用してORACLEをデータベースエンジンとしてもRACを使用することはできませんが、AWSマーケットプレイス上のAMIを使ってRACをAmazon EC2上にデプロイすることが可能になりました。Amazon EC2環境でOracle RACにノードを追加することはいくつかのAPIコールもしくはコマンドを実行するだけで簡単に実行できます。バックアップを取得するには、RAC用に展開されたEC2のEBSボリュームスナップショットの形式でバックアップを取得する必要があります。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３はRDSを利用しているため、不正解です。RDSを利用してORACLEをデータベースエンジンとしてもRACを使用することはできません

オプション２も不正解です。RAC用の自動バックアップを有効化して、定期的にバックアップを取得するといった機能は、AWSでは提供されていません。

問題24: 不正解

あなたはソリューションアーキテクトとして、Aurora Serverlessを社内で適用できないか検討しています。通常のAmazon Auroraはインスタンスサイズを固定化してDBインスタンスを構成しますが、Aurora Serverlessではオンデマンドのオートスケーリングサーバーレス構成を提供します。これにより、アプリケーションのニーズに基づいて容量を自動的に起動、シャットダウン、スケールアップまたはスケールダウンしてくれるようになります。

Aurora Serverlessを使用するのに適しているユースケースを選択してください。 (3つ選択してください。)

- [x] 就業時間中にデータベースを使用しているが、夜間や週末にはデータベースは起動しないデータベース処理システム (正解)
- [x] 1日または1週間に数回、数分間のみ使用される小規模なブログサイト (正解)
- [ ] 人事毎日または年に数回に数時間をピークに軽度に使用される人事評価管理システム (正解)
- [ ] 高性能なパフォーマンスを必要としている経理システム向けのデータベース処理システム
- [ ] 銀行の決済管理システムに利用される絶対に止められないトランザクション処理用のデータベース

説明

Amazon Aurora Serverless は、Amazon Auroraのオンデマンド自動スケーリング設定です。データベースの容量はアプリケーションのニーズに基づいて自動的に起動、シャットダウン、スケールアップまたはスケールダウンされます。Aurora Serverless を使用すれば、データベースインスタンスを管理せずにクラウド内でデータベースを実行できます。Aurora Serverless は、低頻度、断続的、または予測不能なワークロード向けの、シンプルでコスト効率の良いオプションです。

データベースの容量を手動で管理すると、貴重な時間が奪われ、データベースリソースの非効率的な使用につながる恐れがあります。Aurora Serverless では、データベースエンドポイントを作成し、必要に応じてデータベースの容量範囲を指定し、アプリケーションを接続するだけです。データベースがアクティブなときに使用するデータベースの容量に対しては、秒単位の料金を支払う形式となります。

AWS公式では以下のようなAurora Serverlessのユースケースが提示されています。したがって、オプション1と2と3が最適なユースケースといえます。

■使用頻度の低いアプリケーション
小規模のブログサイトなど、1日または1週間に数回、数分間のみ使用されるアプリケーションがあり、アクティブなときにのみ料金を支払うコスト効率の良いデータベースを必要としています。Aurora Serverless では、消費するデータベースリソースに対する料金のみをお支払いいただきます。

■新規アプリケーション
新しいアプリケーションをデプロイしていますが、必要なインスタンスサイズがわかりません。Aurora Serverless を使用すると、エンドポイントを作成するだけで、データベースがアプリケーションの容量要件に合わせて自動的にスケールされます。

■可変ワークロード
人事、予算編成、運用報告など、毎日または年に数回、30 分から数時間をピークに軽度に使用されるアプリケーションを実行しています。ピーク時の容量をプロビジョニングして、継続的に使用していないリソースに対して料金を支払う必要はもうありません。また、平均的な容量をプロビジョニングして、パフォーマンスの問題やユーザーエクスペリエンスの低下のリスクを招く必要ももはやありません。

■予測不可能なワークロード
1日を通してデータベースを使用するワークロードを実行しています。そしてアクティビティのピークを予測することは困難です。例えば、雨が降り始めたときにアクティビティが急増する交通サイトです。Aurora Serverless を使用すると、データベースはアプリケ ションのピーク負荷のニーズを満たすために自動的に容量をスケールし、アクティビティの急増が収まったときにはスケールダウンします。

■開発およびテスト用データベース
ソフトウェア開発およびQAチームは就業時間中にデータベースを使用していますが、夜間や週末にはデータベースを必要としません。Aurora Serverless では、データベースが使用されていないときには自動的にシャットダウンし、翌日の業務開始時にはより迅速に起動します。

■マルチテナントアプリケーション
ウェブベースのアプリケーションでお客様ごとのデータベースを使用しています。Aurora Serverless を使用すると、フリート内の各アプリケーションのデータベース容量を個別に管理する必要はもうありません。Aurora では個々のデータベース容量が管理されるため、貴重な時間を節約できます。

問題25: 不正解

あなたはDevOpsエンジニアとしてAWSを利用したインフラ整備を担当しています。あなたの構築しているシステムでは、Webサーバーは2つのアベイラビリティーゾーンに配置されたEC2インスタンスにホストされ、ELBを介して接続されます。最近になってトラフィック調査を実施したところ、猶信Webトラフィックがアベイラビリティーゾーン全体に均等に分散されていないことが分かりました。それによって、一部のインスタンスへの負荷上昇がシステム処理を遅らせています。

このシナリオにおいて、問題を解決するための最適な方法を選択してください。

- (●) ELBのConnection Drainingを有効化する。 (不正解)
- ( ) ELBのヘルスチェック期間が長すぎるので短縮化することで、適切なヘルスチェックを可能とする。
- ( ) ELBのスティッキーセッションを非有効化する。 (正解)
- ( ) ELBのマルチAZ分散に設定する。

説明

オプション3が正解となります。ELBにスティッキーセッション機能が有効化されていると、トラフィックがインスタンス毎に均等に分散されなくなります。ELBはデフォルトで最小の負荷で登録されたインスタンスに各リクエストを個別にルーティングします。スティッキーセッションは、ターゲットグループ内の同じターゲットにリクエストをルーティングするメカニズムです。これは、クライアントに連続したエクスペリエンスを提供するために状態情報を維持するサーバーに役立ちますが、1つのCookieからのアクセスや処理が長時間にわたるケースではトラフィック分散を不均衡にしてしまう可能性があります。その場合は、ELBのスティッキーセッションを非有効化することで、不均衡な分散を解消することができます。

オプション1は不正解です。ELBのConnection Drainingを有効化することで、ELBが既存の接続を開いたまま、登録解除中のインスタンスまたは異常の発生したインスタンスにリクエストを送信しないようにします。これにより、ロードバランサーは、登録解除中のインスタンスまたは異常の発生したインスタンスに対する未処理のリクエストを完了できます。これは不均衡な分散を解消するのには利用されません。

オプション2は不正解です。ELBのヘルスチェック期間が長すぎると、異常なEC2インスタンスへのトラフィックを停止することができない可能性がありますが、これは不均衡な分散を解消するためには利用されません。

オプション4は不正解です。ELBにはマルチAZ分散に設定といった機能はありません。代わりに、クロスゾーン負荷分散が有効な場合、各ロードバランサーノードは、有効なすべてのアベイラビリティーゾーンの登録済みターゲットにトラフィックを分散します。

問題26: 不正解

B銀行は口座管理ポータルサイトをAWS上に構築しています。ユーザーはポータルサイトを利用して、自身の口座利用履歴などの情報を受け取れることができます。最近になってセキュリティ監査を実施したところ、直接機密情報を利用することがないユーザーがS3バケットに保存された全てのオブジェクトに対してアクセス可能となっていることが判明しました。したがって、個人情報を利用する本人と本人から許可を受けたユーザー以外は、これらの機密ファイルに直接アクセスできないようにするように求められました。

CloudFrontを利用して、この要件を満たすための最適な方法を選択してください。（2つ選択してください。）

- [x] CloudFrontにWAFを連携してReferer制限をしつつ、Origin Access Identity（OAI)機能を利用することで、S3バケットのオブジェクトへのアクセスを制限する。 (不正解)
- [x] CloudFrontにWAFを連携してReferer制限を利用して、S3バケットのオブジェクトへのアクセスを制限する。 (不正解)
- [ ] CloudFrontに署名付きURLとOrigin Access Identity（OAI)機能を利用して、S3バケットのオブジェクトへのアクセスを制限する。 (正解)
- [ ] CloudFrontに署名付きCookieとOrigin Access Identity（OAI)機能を利用して、S3バケットのオブジェクトへのアクセスを制限する。 (正解)

説明

CloudFrontディストリビューションのオリジンとしてAmazon S3バケットを使用している場合、バケット内のオブジェクトへの読み取りがすべてのユーザーに付与されてしまいます。これによって、誰でもAmazon S3 URLを使用してオブジェクトにアクセスできてしまいます。したがって、このシナリオでは特定のオブジェクトへのアクセス権限を特定のユーザーに限定することが求められています。

Amazon S3 バケットから配信するコンテンツへのアクセスを制限するには、CloudFront 署名付き URL または署名付き Cookie を作成して Amazon S3 バケット内のファイルへのアクセスを制限してから、オリジンアクセスアイデンティティ (OAI) という特別な CloudFront ユーザーを作成してS3バケットポリシーに設定することが必要です。これによりユーザーは S3 バケットへの直接 URL を使用してファイルにアクセスすることはできなくなります。これらのステップを踏むことは、CloudFront を通じてユーザーが提供するファイルへの安全なアクセスを維持するのを助けます。したがって、オプション 3，4が正解となります。

オプション１と２は不正解です。WAFを連携してReferer制限によってS3オブジェクトのアクセスを明示的に禁止することができますが、アクセスを特定ユーザーに限定するといった本来の意図とは異なります。また、WAFを連携してReferer制限においてオリジンアクセスアイデンティティ (OAI) と連携することはありません。OAIの制限はWAFではなく、CloudFrontの機能での設定となります。

問題27: 不正解

B社はユーザーに対する旅行情報の提供サービスを展開しています。このサービスでは機械学習を利用して最適化することができます。今月になって、複数のコンポーネントで構成されるホテル検索アプリケーションを新しく展開しました。このアプリケーションのすべてのコンポーネントは、単一のオンデマンドEC2インスタンスでホストされています。アプリケーションの通信処理でSSLの実装が必須となったため、あなたは単一のEC2インスタンスによって構成されているモジュールに対して、2つのSSL証明書を設定して、SSL通信を実施したいと考えています。

このシナリオにおいて、要件を満たすための最適な方法を選択してください。

- ◉ SSLを利用するために拡張ネットワークを有効化した新しいオンデマンドEC2インスタンスを起動する。 (不正解)
- ○ 複数サブネットを利用したVPCを設置して、EC2インスタンスを各サブネットに展開する。その上で、セキュリティグループを利用してEC2インスタンスにおいて複数のSSL証明書を利用する。
- ○ マルチサブネットとしたVPCにオンデマンドEC2インスタンスを展開して、プレースメントグループを設定する。
- ○ 複数のENI（Elastic Network Interface）と複数のEIPを付与した新しいオンデマンドEC2インスタンスを起動する。 (正解)

説明

1つのEC2インスタンスに複数のENI（Elastic Network Interface）を接続することで対応ができます。ENIは、仮想ネットワークカードを表すVPCの論理ネットワークコンポーネントであり、このシナリオでは、2つのENIをオンデマンドEC2インスタンスに接続して、2つのSSL通信を処理できるよう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は不正解です。拡張ネットワークは高性能ネットワークを提供する機能であり、複数のSSL証明書を処理する複数のネットワークインターフェイスは提供しないため、正しくありません。

オプション2は不正解です。セキュリティグループを使用してEC2インスタンスを構成して複数のSSL証明書を処理することはできません。

オプション3は不正解です。プレイスメントグループでEC2インスタンス間の通信を最適化するグループを設定できます。これを起動しても要件を満たさないため、正しくありません。ENIを使用する必要があります。

問題28: 不正解

組織はAWSとオンプレミスの２つの環境を利用して、エンタープライズアーキテクチャを設計し、様々なアプリケーションを運用しています。オンプレミス環境にあるアプリケーションがAWSサービスにアクセスできるようにすることで、これらのアプリケーション間の機能連携を実現したいと考えています。そのためには、オンプレミス側の社内WEBアプリケーションにログインすることで、AWSに対してSAML 2.0 によるエンタープライズ ID プロバイダーを使用したシングルサインオン（SSO）が実施される必要があります。

これらの要件を満たすために役立つソリューションは次のうちどれですか？（2つ選択してください。）

- [x] CognitoによりIAMを利用したIDフェデレーションを実装する。 (不正解)
- [x] Amazon Cognito ユーザープールでAWS SSOをIdPとして設定する (正解)
- [ ] CognitoによりIAMとActive Directoryを統合する。
- [ ] AWS Single Sign-On により全てのAWSアカウントにおける SSO アクセスとユーザーアクセス権限の一元管理を実行する。 (正解)
- [ ] AWS Single Sign-On により、IDフェデレーションとCognitoの統合を実現する。

説明

Amazon Cognito を使用すれば、ウェブアプリケーションおよびモバイルアプリに素早く簡単にユーザーのサインアップ/サインインおよびアクセスコントロールの機能を追加できます。Amazon Cognito ユーザープールでAWS SSOをIdPとして設定することで、CognitoのSAML連携を実施して、シングルサインオンを実現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。

AWS Single Sign-On (SSO) は、複数の AWS アカウントやビジネスアプリケーションへの SSO アクセスを簡単に一元管理できるクラウド SSO サービスです。これにより、ユーザーは AWS SSO で構成する資格情報が既存の社内認証情報を使用してユーザーポータルにサインインし、割り当てられたすべてのアカウントとアプリケーションに 1 か所からアクセスできます。AWS SSO アプリケーション設定ウィザードを使用することで、Security Assertion Markup Language (SAML) 2.0 の統合を作成し、SSO アクセスを任意の SAML 対応アプリケーションに拡張できます。AWS SSO には、Salesforce、Box、Office 365 など多くのビジネスアプリケーションに対する組み込みの SAML 統合が含まれています。クリック数回だけの操作により、独自のインフラストラクチャを運用するための先行投資や継続的なメンテナンス費用なしで、可用性の高い SSO サービスを有効にできます。

したがって、オプション４が正解となります。

問題29: 不正解

あなたはグローバルにオフィスを持つコンサルティングファームのソリューションアーキテクトとして働いています。そこでは、AWS Organizationsを使用して、各支社が使用している複数のAWSアカウントを管理しています。先日、1つの組織単位（OU）に新しいAWSアカウントがメンバーアカウントとして追加されました。この新しいAWSアカウントでは、全てのサービスにリンクされたロールがアタッチされたAmazon ECSクラスターを使用しており、セキュリティ上問題があることが確認されました。社内のセキュリティ規定に準拠するために、新しいアカウントのECS利用に対する特定のアクションを拒否するカスタムSCPを作成して、OUに付与しました。しかしながら、このポリシーを適用後も、このアカウントは実行が制限されているはずのECSアクションを実行可能な状態が継続していることが判明しました。

このシナリオで、ECSの実行アクションを操作できる状態が継続している原因は次のうちどれですか？

- ◉ デフォルトのSCPは全OUやメンバーアカウントに対して全ての許可権限がアタッチされているため、ECSの権限を制限するにはSCPを差し替える必要がある。 (不正解)
- ○ SCPは個別のサービスにリンクされたロールには影響を与えないため、カスタムSCPが適用されなかった。 (正解)
- ○ SCPは適用するOU全体の許可・拒否を設定できるため、ECSの実行アクションを制限できるが、2つ以上のSCPが設定されている場合は、最初に設定されているSCPが優先される。今回のケースでは初期設定の許可設定されたSCPが継続的に影響を与えているため、ECSの実行アクションが拒否されていない。
- ○ SCPは適用するOU全体の許可・拒否を設定できるため、ECSの実行アクションを制限できるが、2つ以上のSCPが設定されている場合は、後から設定されているSCPが優先される。今回のケースでは後から許可設定されたSCPが継続的に影響を与えているため、ECSの実行アクションが拒否されていない。

説明

オプション2が正解となります。AWS OrganizationsのSCPはサービスにリンクされたIAMロールには影響しないようになっています。そのため、サービスにリンクされたロールによって、他のAWSサービスの利用を継続することが可能です。したがって、SCPを適用した後も、新しいアカウントは実行が制限されているはずのECSの実行アクションを操作できる状態が継続することになってしまいました。

Amazon ECSはAWSリソースと連携する際にIAMロールを使用します。サービスにリンクされたロールは、Amazon ECS に直接リンクされた一意のタイプの IAM ロールです。サービスにリンクされたロールは、Amazon ECS による事前定義済みのロールであり、ユーザーに代わってサービスから AWS の他のサービスを呼び出すために必要なすべてのアクセス権限を備えています。これはSCPによって制御することができません。

AWS Organizationsのサービスコントロールポリシー (SCP) は、組織を管理するために使用できるポリシーのタイプです。SCP は、組織内のすべてのアカウントの最大使用アクセス権限を一元的に管理できる機能を提供し、アカウントが組織のアクセスコントロールガイドラインに沿って活動することを確実にします。SCP はすべての機能が有効になっている組織でのみ使用できます。SCPはサービスにリンクされたロールには影響しないようになっています。サービスにリンクされたロールにより、他のAWSサービスをAWS組織と統合でき、SCPによって制限することはできません。したがって、ECSに付与されたIAMロールによるアクセス許可は、そのECSを利用しているAWSアカウントへのSCPでは制限できないことになります。

その他の選択肢は誤答を促すための、偽りの選択肢であり、正しくありません。

問題30: 不正解

A社は国内外にいくつかの支店をもっており、複数のリージョンに複数のVPCを有しています。それらのVPCはオンプレミス環境の本社ネットワークにリンクする必要があります。そのため、本社オフィスには専用のプライベートネットワーク回線を介したリージョンを跨いだVPCアクセスが必要となります。あなたはAWS担当者として、セキュリティを強化しつつ、データ転送パフォーマンスを向上させるためにネットワークメッシュを迅速に構築し、接続を維持するための管理オーバーヘッドを最適化することが求められています。

最適な方法で、これらの要件を満たすにはどうすればよいですか？

- ◉ VPCピアリングはリージョン間を跨いだVPC接続を有効化するため、各VPC間のリージョン間VPCピアリングを有効化する。 (不正解)
- ○ Link Aggregation Control Protocol（LACP）を使用してリージョンを跨いだVPCアクセスを実施する。各VPCに仮想プライベートゲートウェイを構築して、プライベート仮想インターフェースをLink Aggregation Control Protocol（LACP）に接続する。
- ○ パブリック仮想インターフェイスを利用して、リージョンを跨いだVPCアクセスを実施する。各VPCに仮想プライベートゲートウェイを構築して、パブリック仮想インターフェースをDirect Connect Gatewayに接続する。
- ○ AWS Direct Connect Gatewayを利用して、リージョンを跨いだVPCアクセスを実施する。各VPCに仮想プライベートゲートウェイを構築して、プライベート仮想インターフェースをDirect Connect Gatewayに接続する。 (正解)

説明

このシナリオでは、本社オフィスには専用のプライベートネットワーク回線を介したリージョンを跨いだVPCアクセスを構築する必要があります。それはセキュリティが高く、データ転送パフォーマンスを向上させるためにネットワークメッシュを迅速に構築することが必要であり、接続を維持するための管理オーバーヘッドを最適化することも要件となっています。

これに対して、AWS Direct Connect Gatewayを利用して、リージョン間VPCアクセスを構築することで、要件に対応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。

AWS Direct Connect GatewayはAWS Direct Connect の機能の1つです。Direct Connect はオンプレミスから AWS への専用ネットワーク接続を実現する専用線サービスです。AWS Direct Connect を使用すると、AWS とデータセンター、オフィス、またはコロケーション環境との間にプライベート接続を確立することができます。これにより、多くの場合、ネットワークのコストを削減し、帯域幅のスループットを向上させ、インターネットベースの接続よりも安定したネットワークエクスペリエンスを利用することができます。

Direct connect gatewayによって、複数のリージョンにあるVPCに対して、オンプレミス環境から1つのDirect connect からアクセスができるように接続を構成することができます。

詳細は以下のイメージをご参照下さい。

https://docs.aws.amazon.com/ja_jp/directconnect/latest/UserGuide/direct-connect-gateways-intro.html

オプション1は不正解です。VPCピアリングを構成することでVPC間を接続することはできますが、データ転送パフォーマンスを向上させるためにネットワークメッシュを迅速に構築し、接続を維持する要件を満たすためには、Direct Connectを利用して本社オフィスと接続することが必要です。

オプション2は不正解です。Link Aggregation Control Protocol（LACP）は単一のAWS Direct Connectエンドポイントで複数の接続を集約する単なる論理インターフェースであるため、今回の要件には無関係です。

オプション3は不正解です。このシナリオでは、パブリック仮想インターフェイスではなく、Direct Connectゲートウェイを利用する必要があるからです。

問題31: 正解

あなたの会社はアートオークションを運営しています。アートオークションをオンライン化するために、過去の価格データを検索して利用できるサービスを作成することになりました。カタログデータをスキャンしてPNG画像形式にして、光学文字認識（OCR）ソフトウェアを使用して画像をテキストファイルに自動的に変換することで、データ化プロセスを自動化します。これらの仕組みをAWSに移行し、スケーラブルで耐久性と可用性の高いアーキテクチャを構築することが必要です。

このシナリオにおいて、要件を満たす最適なソリューションを選択してください。

- ◉ カタログデータの取り込みにAmazon Rekognitionを利用して、S3バケットを作成してスキャン画像データを取得・蓄積する。これらのアート画像はCloudFrontによって配信する。Elastic Beanstalkを利用してマルチAZ構成でウェブアプリケーションを展開して、検索用にCloudSearchによるクエリ処理を設定する。 (正解)
- ○ カタログデータの取り込みにAmazon Visionを利用して、S3バケットを作成してスキャン画像データを取得・蓄積する。これらのアート画像はCloudFrontによって配信する。CloudFormationテンプレートを利用してマルチAZ構成でウェブアプリケーションを展開して、検索用にCloudSearchによるクエリ処理を設定する。
- ○ カタログデータの取り込みにAmazon Visionを利用して、S3バケットを作成してスキャン画像データを取得・蓄積する。これらのアート画像はCloudFrontによって配信する。Elastic Beanstalkを利用してマルチAZ構成でウェブアプリケーションを展開して、検索用にS3のネイティブ検索エンジンによるクエリ処理を設定する。
- ○ カタログデータの取り込みにAmazon Rekognitionを利用して、S3バケットを作成してスキャン画像データを取得・蓄積する。これらのアート画像はCloudFrontによって配信する。Elastic Beanstalkを利用してマルチAZ構成でウェブアプリケーションを展開して、検索用にS3のネイティブ検索エンジンによるクエリ処理を設定する。

説明

Amazon Rekognition を利用することで画像分析と動画分析などの画像解析機能をアプリケーションに簡単に追加できます。Rekognition API に画像または動画をアップロードすれば対象物、人、テキスト、シーン、アクティビティ、それに不適切なコンテンツまで検出することができます。したがって、カタログデータの取り込みにAmazon Rekognitionを利用して、S3バケットにスキャン画像データを取得・蓄積することが仕組みを構築することができます。 アート画像の配信にはCloudFrontによるCDNを利用したコンテンツ配信を設定することでスケーラブルな読み取りを実現します。また、Elastic Beanstalkを利用してマルチAZ構成でウェブアプリケーションを展開することで、バージョンアップなどの管理を効率的に実施することが可能です。

S3バケット内のデータ検索にはAmazon CloudSearchによるクエリ処理を設定します。CloudSearch は AWS クラウドにおけるマネージド型サービスであり、ウェブサイトまたはアプリケーション向けの検索ソリューションを容易かつコスト効率良く設定、管理、スケールできます。S3のネイティブ検索エンジンは簡易なクエリ検索を実行する機能であり、検索サービス向けに利用するには性能的に不十分です。これらの要素を踏まえるとオプション１が正解となります。

オプション２は不正解です。CloudFormationはAWSリソースの展開をテンプレート化しますが、WEBアプリケーションの展開には不向きです。

オプション２と３は不正解です。Amazon Visionというサービスは存在しません。代わりにAmazon Rekognition を利用する必要があります。

オプション４は不正解です。S3のネイティブ検索エンジンによるクエリ処理では、十分な検索性能を実現することができません。

問題32: 不正解

あなたの会社ではCLBと複数のEC2インスタンスで構成されたWEBアプリケーションを運用しています。東京リージョンのAZ 1aには、3つの実行中のEC2インスタンスがあり、AZ 1bには6つのEC2インスタンスがあり、CLBを介してトラフィックを分散処理しています。着信トラフィックの半分がAZ 1aに送られ、3つのインスタンスが過剰に使用されており、、AZ 1bの6つのインスタンスが十分に使用されていないことが判明しました。

この問題の最も可能性の高い原因を選択してください。

- ◉ ELBのスティッキーセッションが有効化されている。 (不正解)
- ○ クライアントがDNSルックアップをキャッシュする環境において、クロスゾーン負荷分散が無効になっている。 (正解)
- ○ AZ1aに対して加重ルーティングが設定されている。
- ○ AZ1aに対してConnection Drainingが設定されている。

説明

クロスゾーン負荷分散を使用すると、Classic Load Balancer の各ノードは、有効なすべてのアベイラビリティーゾーンに登録されたインスタンスにリクエストが均等に分散されます。クロスゾーン負荷分散が無効な場合は、各ノードは、そのアベイラビリティーゾーンの登録されたインスタンスにのみリクエストが均等に分散されます。

クライアントがDNSルックアップをキャッシュする環境では、着信リクエストがいずれかのアベイラビリティーゾーンを優先する場合があります。今回のシナリオでは、そのために特定のアベイラビリティーゾーンへの負荷が集中したことが考えられます。したがって、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。スティッキーセッション機能を使用することによって、ロードバランサーがユーザーセッションを特定のインスタンスにバインドするように設定できます。これによって、特定のEC2インスタンスが継続的に処理を行うことになり、継続処理が効率的になる反面、EC2インスタンス間での負荷傾斜がアンバランスになる可能性があります。しかしながら、これはインスタンス間の不均衡を生み出す可能性がありますが、AZ間での負荷傾斜の説明としては不十分です。

オプション3は不正解です。CLBでは加重ルーティングを設定することはできません。

オプション4は不正解です。Connection Draining により、ロードバランサーは、登録解除中のインスタンスまたは異常の発生したインスタンスに対する未処理のリクエストを完了できます。これによって、特定のAZにトラフィックを集中することはありません。

問題33: 不正解

あなたの会社はオンプレミスの社員管理システムを利用して社員の出退勤や入退室などを管理しています。会社はシステムをAWSに移行して、可能であればいくつかの新しいテクノロジーを使用することで刷新化することを決定しました。特に大規模ファイルシステム上で顔認証を利用したいと考えています。会社は顔認証システムを独自に開発してサービス展開したいとも考えていますが、多大なコストを費やすことを望んでおらず、できるだけ早く開発を終えることを望んでいます。

この要件を達成する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。 (2つ選択してください。)

- [x] Rekognition CLIからAmazon Rekognition を使用して画像を分析し、顔認証を利用した入退室システムを実装する。 (不正解)
- [x] AWS Rekognition CLI for face detection からAmazon Rekognition を使用して画像を分析し、顔認証を利用した入退室システムを実装する。 (不正解)
- [ ] AWS CLIからAmazon Rekognition を使用して画像を分析し、顔認証を利用した入退室システムを実装する。 (正解)
- [ ] Rekognition API からAmazon Rekognition を使用して画像を分析し、顔認証を利用した入退室システムを実装する。 (正解)

解説

Amazon Rekognitionは、画像分析機能を容易に実現することができるAPIサービスです。 Rekognitionを使用すると、画像内のオブジェクト、シーン、顔を検出できます。顔を検索して比較することもできます。 AWS CLI または Rekognition API を使用して設定することで、強力な視覚的検索と発見をアプリケーションに簡単に組み込むことができます。 Amazon Rekognitionは分析した画像と保存した顔のメタデータに対してのみ料金を支払います。したがって、オプション３と４が正解となります。

Rekognition CLIやAWS Rekognition CLI for face detection といったサービスはAWSでは提供されていないため、オプション１と２は不正解です。

問題34: 不正解

ベンチャー企業B社はAWSを利用した複数のアプリケーションサービスを展開しています。現在開発しているアプリケーションでは、顧客とのメッセージングを実施するRest API形式の連携が必要となります。あなたはソリューションアーキテクトとして、API処理向けに、API GatewayとLambdaファンクションを連携したコスト効率の良いサーバレスアーキテクチャによって、アプリケーションを構築することを決めました。その設定において、Lambda関数とAPI Gatewayとのリソース間の権限設定が不可欠となっています。

API GatewayとLambda関数との連携処理に必要な権限設定を選択してください。（2つ選択してください。）

- [x] Lambda 関数のアクションを呼び出す IAMポリシーを設定し、API Gateway がユーザーに代わって Lambda 関数を呼び出すことを許可する権限を持つ IAM ロールを設定する。 (不正解)
- [x] Lambda コンソールで API Gateway Lambda オーソライザー関数を作成し、API Gateway がユーザーに代わって Lambda 関数を呼び出すことを許可する権限を持つ IAM ロールを設定する。 (正解)
- [ ] API Gatewayコンソールを利用して、Lambdaプロキシ統合によってLambdaファンクションを呼び出すクライアントを有効化するAPIを構築する。
- [ ] Lambda 関数のアクションを呼び出す ARN を設定し、API Gateway がユーザーに代わって Lambda 関数を呼び出すことを許可する権限を持つ IAM ロールを設定する。 (正解)

説明

API GatewayとLambdaファンクションを統合するには Lambda カスタム統合とLambda プロキシ統合の２つの方式があります。Lambda カスタム統合では、プロキシ統合のセットアップ手順に加えて、受信リクエストデータがどのように統合リクエストにマッピングされるか、統合レスポンスデータの結果がメソッドレスポンスにどのようにマッピングされるかを指定します。

本件の統合要件では、こうしたマッピングが要求されていないため、簡単な統合方法であるLambdaプロキシ統合を使用することが正解となります。

Lambda プロキシ統合ではAPI にコンテンツのエンコーディングやキャッシュが不要な場合は、統合の HTTP メソッドを POST に設定し、統合エンドポイント URI を特定の Lambda 関数のアクションを呼び出す Lambda 関数の ARNを設定し、認証情報となる API Gateway がユーザーに代わって Lambda 関数を呼び出すことを許可する権限を持つ IAM ロールを設定するすることが求められます。したがって、オプション4が正解となります。

Lambdaでは、ユーザーの関数が呼び出される際に実行ロールを引き受けた後、そのロールを使用して AWS SDK の認証情報が作成され、イベントソースからデータが読み込まれます。

Lambda オーソライザーは、Lambda 関数を使用して API へのアクセスを制御する API Gateway の機能です。Auth や SAML などのベアラートークン認可戦略を使用しています。発信者 ID を判断するためにリクエストパラメータを使用するカスタム認証スキームを実装する場合に有効です。この設定には、Lambda コンソールで API Gateway Lambda オーソライザー関数を作成し、API Gateway がユーザーに代わって Lambda 関数を呼び出すことを許可する権限を持つ IAM ロールを設定することが必要です。したがって、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。この統合を実現するためには、Lambda 関数のアクションを呼び出す IAMポリシーを設定するのではなく、API Gateway Lambda オーソライザーを作成することが必要です。

オプション３は不正解です。Lambda プロキシ統合によってLambdaファンクションを呼び出すクライアントを有効化するAPIを構築することはできないため、これは偽の選択肢となります。

問題35: 不正解

金融機関B社は複数のAWSアカウントを利用してインフラを構築しています。金融システムの安全性確保を目的に、年一回のIT監査を実施することが定められています。その際は、監査人はAWS上のすべてのAPIイベントを記録するログファイルにアクセスする必要があります。監査人はログファイルへの読み取り専用アクセスのみが必要であり、各AWSアカウントでの直接のアクセス権限は必要ありません。会社には複数のAWSアカウントがありますが、任意の監査人が全ての必要なログにアクセスすることで監査を実施します。

監査人に対する権限設定として、AWS Organizationsを利用した場合と利用しない場合における最適な方法を選択してください。（2つ選択してください。）

- [x] 単一のCloudTrailを各AWSアカウントに設定して、全てのログを単一のS3バケットに配信する。そして、このS3バケットへの読み取り専用アクセスを設定したIAMユーザーを監査人に提供する。 (不正解)
- [x] AWS Organizationsを利用してマスターアカウントのCloudTrailの組織の証跡を有効化して、各メンバーアカウントに関連するログをプライマリアカウントの単一のS3バケットに配信する。そして、このS3バケットへの読み取り専用アクセスを設定したIAMロールを監査人に提供する。 (正解)
- [ ] 各AWSアカウントでCloudTrailの証跡を有効化して、各アカウントに関連するログをAWSアカウントの単一のS3バケットに配信する。そして、このS3バケットへの読み取り専用アクセスを設定したIAMロールを監査人に提供する。 (正解)
- [ ] ログファイルの配信先S3バケットのバケットポリシーを利用して、各AWSアカウントに利用するCloudTrail へのクロスアカウントアクセス権限を付与することで、各CloudTrailから1つのS3バケットにログを収集する。
- [ ] AWS Organizationsを利用してメンバーアカウント全てのCloudTrailの組織の証跡を有効化する。各メンバーアカウントに関連するログをプライマリアカウントの単一のS3バケットに配信する。そして、このS3バケットへの読み取り専用アクセスを設定したIAMロールを監査人に提供する。
- [ ] AWS Organizationsを利用してメンバーアカウント全てのCloudTrailの組織の証跡を有効化する。マスターアカウントにクロスアカウントアクセスを付与することで各メンバーアカウントに関連するログをプライマリアカウントの単一のS3バケットに配信する。そして、このS3バケットへの読み取り専用アクセスを設定したIAMロールを監査人に提供する。

説明

オプション2が正解となります。AWS Organizationsを利用してマスターアカウントのCloudTrailの組織の証跡を有効化することで、全てのメンバーアカウントでのログ取得を可能にすることができます。それにより、各AWSアカウントに関連するログをプライマリアカウントの単一のS3バケットに配信する設定が可能となります。

オプション3も正解となります。AWS Organizationsを利用しない場合は、各AWSアカウントでCloudTrailの証跡を有効化して、各アカウントに関連するログをAWSアカウントの単一のS3バケットに配信します。そして、このS3バケットへの読み取り専用アクセスを設定したIAMロールを監査人に提供することができます。

複数の AWS アカウントのログファイルを 1 つの Amazon S3 バケット [白] 信するように CloudTrail を設定できます。たとえば、4 つの AWS アカウントがあって、それぞれのアカウント ID が 111111111111、222222222222、333333333333、444444444444 である場合に、それら 4 つのアカウントのログファイルをすべて、アカウント 111111111111 に属するバケットへと配信するように CloudTrail を設定する必要があるとします。そのためには以下の手順を実行します。

1．配信先バケットが配置されるアカウント (この例では 111111111111) で、CloudTrail を有効にします。その他のアカウントでは、まだ CloudTrail を有効にしないでください。

2．配信先バケットのバケットポリシーを更新して、CloudTrail にクロスアカウントのアクセス権限を付与します。

3．その他のアカウント (この例では、222222222222、333333333333、444444444444) で、CloudTrail を有効にします。これらのアカウントについては、手順 1 で指定したアカウントに属する同じバケット (この例では 111111111111) を使用するように CloudTrail を設定します。

権限付与の際にはIAMユーザーではなく、IAMロールを利用しています。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 ユーザーは 1 人の特定の人に一意に関連付けられますが、IAMロールはそれを必要とする任意の人が引き受けるようになっています。また、ロールには標準の長期認証情報 (パスワードやアクセスキーなど) も関連付けられません。代わりに、ロールを引き受けると、ロールセッション用の一時的なセキュリティ認証情報が提供されます。これはAWS の外部 (社内ディレクトリなど) に ID をすでに持っているユーザーに AWS へのアクセスを許可することが必要になる場合に利用でき、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。

オプション1は不正解です。単一のCloudTrailを各AWSアカウントに設定して、全てのログを単一のS3バケットに配信する設定するのではなく、マスターアカウントで一括に組織としてCloudTrailを設定することが必要です。単一のCloudTrailを各AWSアカウントに設定して、全てのログを単一のS3バケットに配信する設定ことができないため、単一のCloudTrailではなく、各アカウントでCloudTrailを有効化します。

オプション4は不正解です。ログファイルの配信先S3バケットに付与されるバケットポリシーを利用して、各AWSアカウントのCloudTrail にクロスアカウントアクセス権限を

付与するといった設定はできません。

オプション5と6は不正解です。AWS Organizationsを利用してメンバーアカウント全てのCloudTrailを有効化するのではなく、AWS Organizationsを利用してマスターアカウントのCloudTrailにおいて組織の証跡を有効化することで、全てのメンバーアカウントでのログ取得を可能にすることができます。

問題36: 不正解

大手製造業はレイヤー4を利用した業務アプリケーションをオンプレミスデータセンターにホストしています。このアプリケーションをAWSクラウドに移行[由]とを決定しました。あなたはソリューションアーキテクトとして、この移行作業を担当しています。移行に際して、ELBを使用したトラフィック制御のみをレガシーアプリケーションに直接設定して制御可否をテストします。 ELBは、ヘルスチェックポートとしてHTTPポート80を使用しています。ELBが正常に動いているのかテストしたところ、アプリケーションはWebサイトのポート80に応答していましたが、ヘルスチェックが正常として登録される適切な時間が経過しても、インスタンスは正常登録されていません。

この問題を改善するための、最適なソリューションを選択してください

- (●) ELBのリスナーポートをHTTP ポート80からTCPポート404へと変更する。 (不正解)
- ( ) ELBのリスナーポートをHTTP ポート80からHTTPSポート404へと変更する。
- ( ) ELBのリスナーポートをHTTP ポート80からHTTPSポート80へと変更する。
- ( ) ELBのリスナーポートをHTTP ポート80からTCPポート80へと変更する。 (正解)
- ( ) ELBのリスナーポートをHTTP ポート80からUDPポート80へと変更する。

説明[由]

このアプリケーションはレイヤー4を利用したカスタム開発されたアプリケーションであるため、標準のHTTPアプリケーションとなっておらず、TCPポートを開けておく必要があります。したがって、オプション４が正解となります。フロントエンド接続とバックエンド接続の両方にTCP (レイヤー 4) を使用する場合、ロードバランサーはヘッダーを変更せずにバックエンドインスタンスにリクエストを転送します。ロードバランサーはリクエストを受け取った後、リスナー設定で指定されたポートを使ってバックエンドインスタンスに対するTCP 接続を開こうと試みます。

ELBを使用開始する前に は1つ以上のリスナーを設定する必要があります。リスナーとは接続リクエストをチェックするプロセスです。リスナーは、フロントエンド（クライアントからロードバランサー）接続用のプロトコルとポート、およびバックエンド（ロードバランサーからバックエンドインスタンス）接続用のプロトコルとポートを使用して設定します。 ELBは次のプロトコルをサポートしています。

- HTTP
- HTTPS（セキュア HTTP)
- TCP
- SSL (セキュア TCP)

HTTPSプロトコルは、HTTP レイヤー経由のセキュアな接続を確立するためにSSLプロトコルを使用します。SSLプロトコルは、TCP レイヤー経由のセキュアな接続を確立する場合にも使用することができます。フロントエンド接続がTCP またはSSLを使用している場合、バックエンド接続はTCP またはSSL を使用できます。フロントエンド接続がHTTP またはHTTPS を使用している場合、バックエンド接続はHTTP またはHTTPS を使用できます。

TCPポートでは80番を設定することが必要であるため、オプション１は不正解です。

その他の選択肢は、TCPポート以外を設定しているため不正解です。

問題37: 不正解

あなたの会社ではAWSを利用したWEBアプリケーションを構築しています。このWEBアプリケーションは複数のオンデマンドEC2インスタンスを利用したWEBサーバーがマルチAZに展開されており、それらにELBとAutoScalingが設定された構成となっています。あなたはソリューションアーキテクトとして、この構成に、Route53によるプライベートホストゾーンを設定して、内部的なルーティングを設定しています。設定後にインターネットアクセスを検証したところ、EC2インスタンスにパブリックDNSホスト名がないことに気付きました。また、インスタンスがAmazonが提供するプライベートDNSホスト名を解決できていないようです。

このような問題を解決するためのAWS上の最適な解決策を選択してください。 (2つ選択してください。)

- [x] プライベートホストゾーンにEC2インスタンスが起動しているプライベートサブネットを関連付ける。 (不正解)
- [x] プライベートホストゾーンにEC2インスタンスが起動しているVPCを関連付ける。 (正解)
- [ ] VPCにあるenableDnsHostNamesとenableDnsSupportをTrueに変更する。 (正解)
- [ ] VPCにあるenableDnsHostNamesとenableDnsSupportをFalseに変更する。

説明

このシナリオでは、新しいEC2インスタンスにパブリックDNSホスト名を自動的に設定し、Amazon提供のプライベートDNSホスト名も解決するようにVPCを設定する必要があります。プライベートホストゾーンは、Amazon VPC サービスで作成する 1 つ以上の VPC 内のドメインとそのサブドメインに対するDNSクエリへのAmazon Route 53の応答方法に関する情報を保持するコンテナです。

プライベートホストゾーンの設定方法は以下の通りです。

1.example.com などのプライベートホストゾーンを作成して、そのホストゾーンに関連付ける VPC を指定します。したがって、オプション 2 が正解となります。

2.VPC 内および VPC 間でドメインとサブドメインの DNS クエリに Route 53 が応答する方法を決定するホストゾーンにレコードを作成します。

3.VPCにあるenableDnsHostNamesとenableDnsSupportをTrueに変更します。 したがって、オプション 3 が正解となります。

4.アプリケーションが db.example.com への DNS クエリを送信すると、Route 53 は対応する IP アドレスを返します。また、アプリケーションは、example.com プライベートホストゾーンに関連付けたいずれかの VPC で EC2 インスタンスを実行している必要があります。

問題38: 不正解

あなたの会社は人材マッチングサービスを提供しています。会社は「必要なスキルを持った人材が登録されると、そのスキルを利用したい会社などからオファーが来るWEBアプリケーション」をAWS上で構築しているところです。このアプリケーションは全ての応募者データを保存するEBSボリュームを備えた単一のEC2インスタンスにホストされています。このアプリケーションは、文書や写真などのユーザーからの情報を取得すると、自動で検証して、申請者のスキル適正などに基づいて機械学習を利用してマッチング先を探し出します。しかしながら、このアプリケーションは一度に沢山の申請者が利用されると、負荷に耐えられず停止する可能性があります。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がなるべく停止しないように高可用性を達成するように依頼されました。また、安全性の強化のためにデータはインターネットからのアクセスができないストレージを利用する必要があります。

このアプリケーションを高可用性とスケーラビリティを向上させる、最適なアーキテクチャを選択してください。（2つ選択してください。）

- [x] EBSボリュームの代わりにS3を使用して複数のEC2インスタンスからデータを共有できるように構成する。 (不正解)
- [x] EBSボリュームの代わりにEFSを使用して複数のEC2インスタンスからデータを共有できるように構成する。 (正解)
- [ ] EC2インスタンスを高可用性アーキテクチャとするためにSQSおよびAuto Scalingを備えたキューイングシステムを実装する。最後にCloudFormationを利用して同じアーキテクチャを別リージョンにもレプリケートする。
- [ ] EC2インスタンスを高可用性アーキテクチャとするためにSQSおよびAuto Scalingを備えたキューイングシステムを実装する。最後にCloudFormationを利用して同じアーキテクチャを別リージョンにもレプリケートして、Route53を利用してフェイルオーバー構成を実施する。 (正解)
- [ ] EC2インスタンスを高可用性アーキテクチャとするためにSQSおよびAuto Scalingを備えたキューイングシステムを実装する。次にElasti Beanstalkを利用して同じアーキテクチャを別リージョンにもレプリケートする。

説明

このシナリオでは、既存のアプリケーションサービスのインフラ構成を全面的に見直して、高可用性とスケーラビリティを向上させるアーキテクチャに刷新することが求められています。アプリケーションを動かしている既存のEC2インスタンスはリクエスト数が急増すると、負荷に耐えられずダウンしてしまいます。この場合、SQSおよびAuto Scalingを備えたキューイングシステムを実装することで解決することができます。AutoScalingによるスケーリングに加えて、SQSによる並行処理によって単一のEC2インスタンスへの負荷を軽減することができます。

さらに別リージョンにCloudFormationを利用してレプリケートを実施した上で、Route53を利用したフェールオーバー構成を実施することが必要です。よって、正解はオプション４となります。

オプション２も正解となります。EBSボリュームは限られたストレージ容量しか提供できず、スケーラブルではないため、代わりにEFSを使用することで、複数EC2インスタンスで処理ができるように冗長化します。EFSはS3と異なりインターネットからデータに直接アクセスができません。

オプション１は不正解です。EBSボリュームの代わりにS3を使用して複数のEC2インスタンスからデータをシェアする構成は可能ですが、S3はEFSと異なりインターネットからのデータに直接アクセスができるため要件に合致しません。また、EC２インスタンスからアプリケーションプロセス上でデータを蓄積しつつデータ処理を実行する際のストレージとしては、EBSまたはEFSを利用する方が最適となります。S3はEC２インスタンスからのデータ処理を実行するストレージではなく、データを保存・蓄積するストレージに向いています。S3を利用するケースは、たとえば画像や動画コンテンツはS3に保存しつつ、データ処理はEBSを利用するといったアプリケーション構成となります。

オプション３は不正解です。このアプリケーションはなるべく停止しないような冗長化を達成するように依頼されているため、Route53を利用してフェイルオーバー構成を実施することで、冗長化を高める必要があります。

オプション５は不正解です。この場合のインフラ構成を展開するためElastic Beanstalkでは不適切です。Elastic Beanstalkはウェブアプリケーションの展開とバージョン管理の自動化に適したサービスです。

問題39: 不正解

あなたは健康管理アプリケーションを開発・運用しているFingi TechnologiesのAWSエンジニアです。このモバイルアプリではジムなどのトレーニング実施時の生体情報を毎秒収集し、POST APIリクエストを通じてWebポータルに送信して身体データのモニタリングを実施しています。あなたのタスクは、バイオメトリックデータを受け入れてデータ処理し、ユーザーに身体データ傾向と健康レポートを提供するAPIサービスとWebポータルを設計することです。ポータルは、リアルタイムの生体認証データ分析を表示するための追加機能を備えており、非常に耐久性があり、高可用で、スケーラブルでなければなりません。

この要件を満たすために、AWS上の最適なアーキテクチャ設計を選択してください。

- ◉ Amazon Kinesis Data Streamsを利用して生体データを収集して、Lambdaファンクションを利用してリアルタイムにデータ解析をアプリのダッシュボードに表示する。その上で、これらのストリームデータをDynamoDBに保存して、蓄積データに対してRedshiftによる複雑なデータ解析を実施する。 (不正解)
- ○ Amazon EMRを利用して生体データを収集しつつ、リアルタイムにデータ解析結果をアプリのダッシュボードに表示する。その上で、これらのストリームデータをDynamoDBに保存して、蓄積データに対してRedshiftによる複雑なデータ解析を実施する。
- ○ Amazon Kinesis Data Streamsを利用して生体データを収集して、Amazon Kinesis Data AnalyticsやKinesis Client Library（KCL）を利用してリアルタイムにデータ解析結果をアプリのダッシュボードに表示する。その上で、これらのストリームデータをS3に保存して、蓄積データに対してRedshiftによる複雑なデータ解析を実施する。 (正解)
- ○ Amazon Kinesis Data Streamsを利用して生体データを収集して、Amazon Kinesis Data Firehoseを利用してリアルタイムにデータ解析結果をアプリのダッシュボードに表示する。その上で、これらのストリームデータをDynamoDBに保存して、蓄積データに対してRedshiftによる複雑なデータ解析を実施する。

説明

オプション3が正解となります。Amazon Kinesis Data Streamsを利用して生体データを収集して、Amazon Kinesis Data AnalyticsやKinesis Client Library（KCL）を利用してリアルタイムにデータ解析結果を、アプリのダッシュボードに表示することができます。その上で、これらのストリームデータをS3に保存して、蓄積データをRedshiftによる複雑なデータ解析することが可能です。

Amazon Kinesis Data Streamsは、大規模にスケーラブルで持続的なリアルタイムのデータストリーミングサービスです。Kinesis Data StreamsはWEBサイトクリックストリームやデータベースイベントストリームや金融取引、ソーシャルメディアフィード、ITログ、ロケーション追跡イベントなど何十万ものソースから毎秒ギガバイトのデータを継続してキャプチャできます。また、Amazon Kinesis Data Analytics はストリーミングデータの分析をリアルタイムで実施可能なサービスです。この2つを組み合わせることでストリームデータのリアルタイム分析を実施することができます。

Kinesis Client Library（KCL）を使用すると、Kinesisアプリケーションを構築し、ストリーミングデータを使用してリアルタイムダッシュボードの強化、アラートの生成、動的な価格設定と広告の実装などを行うことができます。Kinesis Data StreamsからAmazon S3、Amazon Redshift、Amazon EMR、AWS Lambdaなどの他のAWSサービスにデータを送信することが可能です。今回は目的であれば、大量のストリームデータをS3に蓄積して、Redshiftによる解析を実施することができます。

オプション1は不正解です。Lambda関数を利用してデータ解析アプリケーションを構成することはできますが、Amazon Kinesis Data Streamsを利用したデータ解析にはAmazon Kinesis Data AnalyticsやKinesis Client Library（KCL）を利用した方式が標準的であり、効率的にアプリケーションを構築することが可能です。

オプション2は不正解です。Amazon EMRはKinesisと連携して利用することが望ましく、Kinesisでデータ蓄積をしたうえで、EMRによるデータ分析を実施するのが適切な構成となります。

オプション4は不正解です。Amazon Kinesis Data Firehoseはデータを蓄積する際に変換して、S3などへと連携することができる機能であり、データ解析を実現することはできません。

問題40: 不正解

あなたの会社ではAWS上で顧客分析アプリケーションを運用してい[白]あなたはソリューションアーキテクトとして、データ分析部門からアプリケーションにレポート機能を追加するように依頼されました。この新しいコンポーネントは、マルチAZ構成のRDS MySQLデータベースインスタンスに保存されているユーザー行動データから1時間ごとにデータを集約して、ステータスレポートを抽出することができます。このレポート機能は既存のデータベース処理に影響を与えないように最適な処理が必要です。

この要件を満たすことができる、AWS上の最適なアーキテクチャ設計を選択してください。

- ◉ RDSからレポート向けデータをS3に取得して、S3側でS3 Selectによるクエリ解析を実施した上で、QuickSightによりレポートを生成・表示させる。 (不正解)
- ○ RDSのリードレプリカを起動して、RDSのプロキシ機能を利用してリードレプリカからデータを取得して集計するLambda関数を構築して、レポートを生成する。 (正解)
- ○ ElastiCacheを利用してレポート用データをキャッシュに取得し、そのデータを利用してQuickSightによりレポートを生成・表示させる。
- ○ RDSのリードレプリカを起動して、RDSのリードレプリカのエンドポイントからデータを取得して集計するLambda関数を構築して、レポートを生成する。

説明

このシナリオでは、データ分析レポートを生成するコンポーネントの追加によって、既存のデータ処理能力に影響がないようにする必要があります。RDSプロキシを利用してLambda関数によってRDSからデータ取得と集計を実施するサーバレスアプリケーションを構築することができます。RDS Proxyは、アプリケーションとRDSデータベースの間の仲介役として機能します。RDS Proxyは必要となるデータベースへのコネクションプールを確立および管理し、アプリケーションからのデータベース接続を少なく抑える機能です。RDS Proxyは、Lambda関数からデータベースに直接流れるすべてのデータベーストラフィックを処理します。

また、RDSのリードレプリカを起動して、そこからレポート処理をすることで既存のデータベース処理に負荷をかえることなくレポート生成が可能となります。

したがって、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。RDSからレポート向けデータをS3に取得する時点で、データ読み取り処理が発生しています。リードレプリカを利用した構成に比較して、二重にデータを保存して、データ読み取り処理も二重に発生することになり非効率です。

オプション3は不正解です。ElastiCacheを利用してレポート用データをキャッシュに取得する対応は可能ですが、ElastiCacheは高性能なリアルタイム分析や計算処理や、キャッシュアクセスに利用されるべき機能であり、今回のレポート生成用向けとしてはコスト的に非効率です。

オプション4は不正解です。プロキシを使用せずにRDSのリードレプリカからデータを取得して集計するLambda関数を構築して、レポートを生成すると、RDSとのコネクションが乱立してしまい、Lambda関数処理が上手くいかない可能性があります。