問題1: 不正解

あなたの会社はオンプレミス環境にWebアプリケーションを有しています。このWEBアプリケーションはロードバランサーと複数のLinux Apacheサーバーによって構成されたWeb層と、MySQLデータベースによるデータ層の2層アーキテクチャーで構成されています。先日、このWEBアプリケーションに対して、ファイル取得リクエストが急増したことによって、システムダウンが発生してしまい、ユーザー数の大幅な減少につながりました。このようなリスクを低減させるために、あなたはAWSを利用して最短で実現できるソリューションが求められています。

この要件を満たすためのAWSアーキテクチャを選択してください。

- ◉ オンプレミス環境とAWS間でAccelerated サイト間 VPN接続を構成した上で、最適なTTLを設定したCloudFrontを設置して、オンプレミス環境のWEBサーバーをオリジンに設定して、オフロードトラフィックを実現する。 (不正解)
- ○ オンプレミス環境とAWS間でDirect Connect接続を構成した上で、最適なTTLを設定したCloudFrontを設置して、オンプレミス環境のWEBサーバーをオリジンに設定して、オフロードトラフィックを実現する。
- ○ AWS RDS MySQLとEC2インスタンスとAuto Scalingを適用したサブ環境をAWS上に構築して、オンプレミス環境からAWSに移行する。
- ○ 最適なTTLを設定したCloudFrontを設置して、オンプレミス環境のWEBサーバーをオリジンに設定して、オフロードトラフィックを実現する。 (正解)

説明

CloudFrontを利用することでコンテンツ配信負荷をキャッシュ処理によって軽減します。それにより、オンプレミス環境のサーバー負荷を低減する構成を短期間で実現することが可能です。CloudFrontのカスタムオリジンには、WEBサーバーとなるEC2インスタンスだけでなく、オンプレミス環境にあるサーバーを設定できます。これによって、TTLを選択したキャッシュ処理が設定されたCloudFrontを前面に設置して、オンプレミス環境に対するオフロードトラフィックを実現することができます。この設定はCloudFront上のオリジンサーバー設定をオンプレミスサーバーに指定するだけで利用することが可能です。

したがって、オプション４が正解です。

オプション１と２は不正解です。この設定はCloudFrontでオリジンサーバー設定をオンプレミスサーバーに指定するだけで利用することが可能であり、回答のような複雑な設定は必要ありません。また、Direct Connect接続やVPN接続は必要ありません。

オプション３は不正解です。オンプレミス環境からAWSへの移行は時間がかかるため、最短の対応という要件に合致しません。

問題2: 正解

あなたの会社は、Jリーグの試合に対するデータ分析システムを開発しています。このシステムは平均ゴール、平均パス、その他多くのプレーに関する詳細データの統計データを記録して、レポートを生成して、Jリーグファンやスポーツメディアなどに提供します。これらのデータは永続的に保存する必要があるため、保存先は可用性・拡張性に優れている必要があります。リリース時はJリーグ開幕直前を予定しており、試合日には20万件を超えるクエリが発生すると予測されています。

これらの要件を満たす最も費用対効果の高いソリューションを選択してください。

- ◉ レポート作成用のリードレプリカ付のマルチAZ構成のAurora MySQLデータベースを設置して、レポートを保存する場所としてS3標準ストレージを利用する。さらにCloudFrontによる配信を実施する。 (正解)
- ○ レポート作成用のリードレプリカ付のマルチAZ構成のRDS MySQLデータベースを設置して、レポートを保存する場所としてS3 標準-IAストレージを利用する。配信のためにAPI Gatewayからのアクセスを可能にする。
- ○ レポート作成用のリードレプリカ付のマルチAZ構成のAurora MySQLデータベースを設置し、レポート生成と配信処理にElastiCacheを利用した高性能なデータ処理を実施する。
- ○ レポート作成用のリードレプリカ付のマルチAZ構成のRDS MySQLデータベースを設置し、レポート生成と配信処理にDynamoDBを利用した高性能なデータ処理を実施する。

説明

オプション１が正解となります。このアプリケーションが生成するレポートや試合データを保存するストレージとしてS3を利用することが最適です。S3のストレージクラスはそのデータの利用方法に応じて選択します。今回のケースのようにデータ分析で利用するデータは利用頻度が高く、かつ、そのデータ自体も重要なデータであるため標準ストレージが最適となります。その他のストレージクラスはIAクラスはアクセス頻度が低いデータ向け、RRSは低冗長の保存でも良い一時データ向けなど、利用用途が異なるため本件には合致しません。また、RRSは現在は非推奨ストレージとなっています。

可用性が高く、数百万のクエリ処理も可能なデータベースとしては、Auroraを利用します。Auroraは標準的なMySQLよりも５倍のスループット、標準的なPostgreSQLよりも３倍のスループットを実現することができるため、高パフォーマンスが求められる場合に最適なデータベースとなります。また、レポートファイルを世界中のユーザーに配布するためのコンテンツ配信ネットワークとしてCloudFrontを設置します。

オプション２と４は、Amazon AuroraデータベースではなくRDSを選択しているため不正解です。今回のケースではAuroraを優先して利用するべきです。リリース時点ではJリーグはオンシーズンとなっており、試合日には20万件を超えるクエリが発生すると予測されており、可用性が高く、数百万のクエリを処理できるように拡張できるデータベースとしてはAuroraを利用します。

オプション３は不正解です。レポート生成と配信処理にElastiCacheを利用しており、間違っています。ElastiCacheはキャッシュを利用した高速データ処理を可能にするインメモリDBです。ElastiCacheではなくCloudFrontが適切な選択肢となります。

問題3: 不正解

A社では多層Webアプリケーションを AWS上で構築しています。このアプリケーションはメインサーバーとなる1つのEC2インスタンスにホストされており、データベースにRDSを利用し、ストレージにEBSを使用しています。このEC2インスタンスには2つのアプリケーションコンポーネントが実装されており、それぞれが別個の業務タスクを実施するために外部システムとの通信処理を行うことが必要です。A社のセキュリティ規定では利用データの保護が必須となっているため、あなたはソリューションアーキテクトとして、個別のコンポーネントに2つの個別のSSL証明書を実装することが求められています。

1つのEC2インスタンスに対して、2つの個別のSSL証明書を実装する方法を選択してください。

- ◉ 複数のNATアドレスを付与したEC2インスタンスを設置し、NATアドレスが付与した2つのIPアドレスに個々のSSL認証を実行する (不正解)
- ○ 複数サブネットにEC2インスタンスを設置して、個別のIPアドレスを付与する。
- ○ 複数のセキュリティグループを設定したEC2インスタンスを設置する。そのEC2インスタンスに対して各IPアドレスへのトラフィックルールを設定する。
- ○ 複数のEIPを設定して複数ネットワークインターフェースを有したオンデマンドインスタンスを設置する。 (正解)

説明

1つのインスタンスにある複数の個別のコンポーネントに別々のSSL証明書を実装したい場合は単一のEC2インスタンスにElastic Network Interface（ENI）を使用して複数のElastic IPアドレスを付与することで達成できます。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。したがって、オプション4が正解です。

オプション1は不正解です。NATアドレスはEC2インスタンスに複数のIPアドレスを提供しないため、正しくありません。

オプション2は不正解です。2つの別々のサブネットまたはアベイラビリティーゾーンに同じEC2インスタンスを配置できないため、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主にインスタンスへの着信または発信トラフィックを制御するために使用され、EC2インスタンスに複数のIPアドレスを提供しないため、間違っています。

問題4: 正解

あなたはWEB解析を行っている企業の分析担当者です。WEBデータ解析にはオンプレミスのNoSQL型データベースを利用していますが、データベースの蓄積データ量の増加によって応答性が低下するなどのパフォーマンス低下が問題となっています。そのため、運用チームは現在のオンプレミスNoSQLデータベースからAWSのDynamoDBに移行することを決定しました。あなたは移行担当者に任命されて、DynamoDBのマッピングルールの設定を開始しました。しかしながら、オンプレミス環境のレガシーデータベースのタイプはCSVによるデータ抽出は可能ですが、AWS DMSなどのAWSの移行サービスには対応していないようです。

このNoSQLデータベースをDynamoDBに移行するための最適な方法を選択してください。

- ◉ レガシーデータベースから抽出したCSVファイルをS3にアップロードする。その上で、AWS DMSコンソールを利用してS3をソースエンドポイントに、DynamoDBをターゲットエンドポイントに指定して、テーブルマッピングを追加する。 (正解)
- ○ レガシーデータベースから抽出したCSVファイルをAWS DMSを設定したインスタンスにアップロードしてソースエンドポイントに指定する。次にDynamoDBをターゲットエンドポイントに指定して、テーブルマッピングを追加する。
- ○ 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設定し、アタッチしたEBSにCSVファイルをアップロードする。このEBSをソースエンドポイントに、DynamoDBをターゲットエンドポイントに指定して、テーブルマッピングを追加する。
- ○ RDS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設定し、CSVファイルをアップロードする。このDBインスタンスをソースエンドポイントに、DynamoDBをターゲットエンドポイントに指定して、テーブルマッピングを追加する。

説明

オプション1が正解となります。レガシーデータベースのデータ構造をDynamoDBへ移行するためには、最初にレガシーデータベースから抽出したCSVファイルをS3にアップロードします。その上で、AWS DMSコンソールを利用してS3をソースエンドポイントに、DynamoDBをターゲットエンドポイントに指定して、テーブルマッピングを追加することができます。

レガシーデータベースはAWS Database Migration Services（AWS DMS）を直接利用してデータベース移行することができないケースとなっています。その場合はCSV形式でデータをエクスポートできれば、CSVファイルからデータを移行またはプラットフォーム変更が可能です。DMSはS3にアップロードしたCSVファイルを使用した移行が可能となっています。

S3がソースエンドポイントである場合は外部テーブル定義が必要です。外部テーブル定義はAWS DMSがAmazon S3からのデータを解釈するためのJSONドキュメントです。JSONファイルをテーブルマッピングボックスに直接入力して定義することが可能です。

オプション2は不正解です。レガシーデータベースから抽出したCSVファイルを、AWS DMSを設定したインスタンスにアップロードするのではなく、S3にアップロードするのが最適です。

オプション3は不正解です。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設定し、アタッチしたEBSにアップロードするのは適切な方式ではありません。移行データはS3にアップロードして、AWS DMSコンソールを利用してS3をソースエンドポイントに設定することが求められます。

オプション4は不正解です。上記と同様にRDSインスタンスをデータをアップロードするために利用することはできません。

問題5: 不正解

あなたはAWS向けのソリューションアーキテクトとして、不動産企業に勤めています。この会社ではAWS Organizatronsを使用して複数のAWSアカウントの統合管理を始めました。マスターアカウントを利用する運用チームは、それぞれ2つのメンバーアカウントが所属する3つのOU（組織単位）を作成しました。全社的なセキュリティポリシーに準拠するために、CloudTrailによる監視が全AWSアカウントに必要です。このCloudTrailによる監視はマスターアカウントのみで実施して、統合管理することが求められています。

この統合監視を実現するための設定方法を選択してください。

- (●) AWS Organizations において、マスター管理を選択して、CloudTrail において組織の証跡を有効化する。メンバーアカウントではAWS CloudTrailを非有効化できない権限範囲をIAMポリシーで設定する。 (不正解)
- ( ) AWS Organizations において、すべての機能を選択して、CloudTrailにおいて組織の証跡を有効化する。メンバーアカウントではAWS CloudTrailを非有効化できない権限範囲をIAMポリシーで設定する。
- ( ) AWS Organizationsにおいて、一括請求機能を選択して、CloudTrailにおいて組織の証跡を有効化する。メンバーアカウントではAWS CloudTrailを非有効化できない権限範囲をSCPで設定する。
- ( ) AWS Organizationsにおいて、マスター管理を選択して、CloudTrailにおいて組織の証跡を有効化する。メンバーアカウントではAWS CloudTrailを非有効化できない権限範囲をSCPで設定する。
- ( ) AWS Organizationsにおいて、すべての機能を選択して、CloudTrailにおいて組織の証跡を有効化する。メンバーアカウントではAWS CloudTrailを非有効化できない権限範囲をSCPで設定する。 (正解)

説明

AWS Organizations には、2 つの利用可能な機能セットがあります。

■すべての機能 – この機能セットは AWS Organizations を使用するにあたって推奨され、一括請求機能も含まれています。組織を作成する際、デフォルトではすべての機能が有効化されています。すべての機能が有効になっていると、サービスコントロールポリシー (SCP) などの AWS Organizations で利用できる高度なアカウント管理機能を使用できます。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できます。

■一括請求機能 – 一括請求機能は請求処理をまとめてマスターアカウントが実施するための機能です。一括請求機能のみを使用して組織を作成する場合でも、後からすべての機能を有効にできます。このページでは、すべての機能を有効にするプロセスについて説明します。

AWS Organizations で「すべての機能」を選択すると、CloudTrailコンソールの設定機能で「組織の証跡」を有効化する設定が表示されるようになります。これを有効化すると、メンバーアカウントに対するCloudTrailによるログ設定が実施されるようになります。その上で、メンバーアカウントではAWS CloudTrailを非有効化できない権限を設定するSCPを設定することで、メンバーアカウントによる設定変更を防止できます。したがって、これが上記説明と合致しているため、オプション 5 が正解となります。

オプション 1 と 2 は不正解です。メンバーアカウントに対して権限範囲を制限する際はSCPを利用します。IAMは個別のユーザーに対する権限設定に利用される機能であり、今回のケースでは利用できません。

オプション 3 と 4 は不正解です。一括請求やマスター管理ではなく、AWS Organizations で「すべての機能」を選択することが必要となります。

問題6: 不正解

あなたはソリューションアーキテクトとして、ロードバランサーが付属するAmazon ECSクラスター上で実行されるDocker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ではDynamoDBを頻繁に使用していますが、その性能を向上させる必要があります。あなたはワークロードを均等に分散して、プロビジョニングされたスループットを効率的に使用することでmデータベースのパフォーマンスを向上させようと考えました。

白

上記のようにパフォーマンスを向上させるための、DynamoDBテーブルの設定方法を選択して下さい。

- ◉ DynamoDBにあるパーティションキーを削減する。 (不正解)
- ○ カーディナリティの低いパーティションキーを使用する
- ○ カーディナリティの高いパーティションキーを使用する (正解)
- ○ パーティションキーとソートキーで構成される複合プライマリーキーを利用する。

説明

オプション3の「カーディナリティの高いパーティションキーを使用する」が正解となります。DynamoDB はデータをパーティションに保存します。パーティションはソリッドステートドライブ (SSD) によってバックアップされ、AWS リージョン内の複数のアベイラビリティーゾーン間で自動的にレプリケートされるテーブル用のストレージの割り当てです。これらのパーティション管理は完全に DynamoDB によって処理されます。I/O要求を均等に分散しないパーティションキー設計では、「ホット」パーティションが作成されてスロットルが発生し、プロビジョニングされたI/O容量が非効率的に使用される可能性があります。

DynamoDB は次の状況でテーブルに追加のパーティションを割り当てます。

■テーブルのプロビジョニングされたスループット設定を、既存のパーティションがサポートできる以上に増やす。

■既存のパーティションが容量いっぱいになり、より多くのストレージ領域が必要になる。

パーティションキー値の総数に対するアクセスされたパーティションキー値の比率が高いほど、プロビジョニングされたスループットをより効率的に使用します。その一例として、カーディナリティの高い属性を持つパーティションキーを使用することが挙げられます。これには、各項目に多数の異なる値があります。テーブルにカラムがある場合にカラムに格納されているデータの種類がどのくらいあるのか(カラムの値の種類の絶対値)を、カーディナリティといいます。そして、「カラムのデータの種類が、テーブルのレコード数に比べて多い場合、カーディナリティが高い」といいます。したがって、オプション3が正解となります。

オプション1は不正解です。DynamoDBテーブル内のパーティションキーの数を減らすのではなく、実際にI/O要求を均等に分散させ、「ホット」パーティションを回避するためにパフォーマンスを向上させるにパーティションキーの数を追加する必要があるため、正しくありません。

オプション2は不正解です。ワークロードがアクセスするパーティションキーの値が明確でないほど、区分化されたスペース全体に均等に分散されず、パフォーマンスが低下するため、正しくありません。

オプション4は不正解です。複合プライマリーキーを利用すると検索性を向上させることはできますが、パフォーマンスの向上にはつながりません。

問題7: 不正解

転職者専用の人材マッチングサービスを提供しているB社では、人材マッチングモバイルアプリをAWS上で開発しているところです。このモバイルアプリでは、多数の履歴書や応募要項などが蓄積されるため、20TB相当のファイルを保存する必要があり、他のデータも併せるとデータは最大60TBに達する可能性があります。また、数万人分にもなるファイルから特定のアイテムを簡単に見つけることができる検索機能が必要です。

この検索システムを機能させるための費用対効果の高い方法を選択してください。

- (●) S3標準ストレージに人材データを蓄積して、S3 Selectを利用してクエリ処理を行い、Elastic Beanstalkにより複数AZにWEBサイトを展開する。 (不正解)
- ( ) S3標準ストレージに人材データを蓄積して、CloudSearchを利用してクエリ処理を行い、Elasti Beanstalkにより複数AZにWEBサイトを展開する。 (正解)
- ( ) S3標準ストレージに人材データを蓄積して、S3のネイティブ検索機能を利用してクエリ処理を行い、Elastic Beanstalkにより複数AZにWEBサイトを展開する。
- ( ) S3標準ストレージに人材データを蓄積して、EMRを利用してクエリ処理を行い、Elastic Beanstalkにより複数AZにWEBサイトを展開する。

解説

S3は耐久性と拡張性に優れたオブジェクトストレージであり、大量のデータを保存する際は第一の選択になります。頻繁に利用するファイルは標準ストレージに保存し、頻繁に利用しない中長期保存するファイルはS3 IAかGlacierを選択します。ただし、S3ネイティブ検索機能はS3に簡易なクエリ検索を提供しますが、大規模な検索機能に用いることができません。したがって、検索機能には別のAWSサービスと連携させる必要があります。AWSでは検索機能としてElaticSearchまたはAmazon CloudSearchのどちらかを選択することになります。

Amazon 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。34 言語をサポートし、ハイライト表示、自動入力、地理空間検索などの人気のある検索機能を備えています。これらの選択は、アプリケーション上での仕様上のマッチングなどに合わせて選択することが必要となりますが、一般的な検索機能はどちらでも達成することが可能です。

したがって、オプション２はS3標準クラスを使用しており、クエリ処理にCloudSearchを使用して、マルチAZ展開によって高可用性を実現しているため、正しい回答となります。

オプション１は不正解です。S3 Selectを利用してクエリ処理を行うことで、オブジェクトデータの条件付きで検索・抽出することはできますが、大量データの検索機能としては不十分です。

オプション３は不正解です。S3のネイティブ検索機能を利用して、オブジェクトデータを簡単に検索することはできますが、大量データの検索機能としては不十分です。

オプション４は不正解です。EMRとAthenaはS3バケットに保存したデータ分析に利用するサービスであり、検索機能を実現することができません。

問題8: 不正解

衣料品ブランドのA社は、ECサイトで割引価格セールを実施する年末イベントを予定しています。このECサイトでは販売が始まると短期間で何万もの訪問者がアクセスします。最初に訪問者はFacebookまたはGoogleの資格情報を使用してサイトにログインし、アイテムをカートに追加します。購入後、ページにカートのアイテムと割引価格が表示されます。現在、あなたはイベントによるトラフィック急増に対処できる、スケーラブルで費用対効果の高い決済機能を実現することが依頼されています。

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。

- ◉ 最初にCognitoを利用したソーシャルログインを実施してユーザーを認証する。EC2インスタンスベースのWEBサーバーに対して、ELBとAutoScalingを設定し、CloudFrontによる商品データ配信を行う。Auroraサーバレスを利用した高速処理によって決済処理とデータの蓄積と処理を実行する。 (不正解)

- ○ 最初にCognitoを利用したソーシャルログインを実施してユーザーを認証する。EC2インスタンスベースのWEBサーバーに対してELBとAutoScalingを設定し、CloudFrontによる商品データ配信を行う。SQSを利用したキューによって並列処理したEC2インスタンスを利用した決済サーバーが決済処理を実施し、最終的な処理結果をDynamoDBに蓄積する。 (正解)

- ○ 最初にCognitoを利用したソーシャルログインを実施してユーザーを認証する。EC2インスタンスベースのWEBサーバーに対してELBとAutoScalingを設定し、CloudFrontによる商品データ配信を行う。EC2インスタンスを利用した決済サーバーが決済処理を実施し、最終的な処理結果をDynamoDBに蓄積する。

- ○ 最初にCognitoを利用したソーシャルログインを実施してユーザーを認証する。EC2インスタンスベースのWEBサーバーに対して、ELBとAutoScalingのを設定し、CloudFrontによる商品データ配信を実現する。DynamoDBを利用した高速処理によって決済トランザクションデータの蓄積と処理を実行する。

説明

このシナリオでは、年末商戦で多数のアクセスが予測されるECサイトに対する可用性やパフォーマンスが高いソリューションが問われています。ユーザー認証機能としては、要件からソーシャルログインが実施される必要があるため、Cognitoを利用したソーシャルログインが最適となります。

スケーラブルで高パフォーマンスな要件に対してはCloudFront、Elastic Load Balancer、AutoScaling、DynamoDBおよびSQSの組み合わせて、高度にスケーラブルなアーキテクチャを実装します。まずはEC2インスタンスベースのWEBサーバーに対して、ELBとAutoScalingを設定して、CloudFrontによる商品画像データ配信を行うという基本的な構成を実現します。

更に決済処理については、複数決済を同時並行で処理することが求められるため、SQSキューに基づいて決済サーバーとなるEC2インスタンスの並行処理を実現します。そして、決済処理結果となるデータをDynamoDBに蓄積することが望ましい構成となります。したがって、オプション2が正解となります。

DynamoDBは決済処理のユースケースに利用可能なＤＢです。決済処理の重複を防ぐためフラグを立てたり、決済情報などを保存したりするのに利用できます。決済処理はＲＤＢのようなリレーショナルなデータ処理ではなく、ワークプロセスの高速処理が必要であるため、DynamoDBによる高速処理が必要となります。

オプション1は不正解です。Auroraサーバレスを利用した高速処理によって決済トランザクションデータの蓄積と処理を実行する構成になっていますが、Auroraサーバレスだけではサーバーサイドの決済処理を実現できません。決済処理はEC2インスタンスなどのコンピューティングで実現することが必要です。

オプション3は不正解です。EC2インスタンスを利用した決済サーバーが決済処理をする構成だけではキュー処理による負荷軽減が実施できていないため、構成として不十分です。

オプション4は不正解です。DynamoDBだけでトランザクション処理を実現することはできないため、決済トランザクション処理の方式が不十分です。

問題9: 不正解

教育ベンチャー企業はオンライン学習システムを開発しました。アプリケーションアーキテクチャは、1つのアベイラビリティゾーンにある2つのオンデマンドEC2インスタンスに対して、ALBのターゲットグループとRoute53によるルーティングも設定しています。セキュリティ要件として、このオンライン学習システムではHTTPSを利用したセキュアな通信が求められています。

この要件を満たすための最適なAWSソリューションを選択してください。

- ◉ ACMを利用してパブリックな証明書を発行し、証明書をEC2インスタンスに設定することでHTTPSを利用した通信設定を実施する。 (不正解)
- ○ ACMを利用してプライベートな証明書を発行し、証明書をEC2インスタンスに設定することでHTTPSを利用した通信設定を実施する。
- ○ ACMを利用してパブリックな証明書を発行し、証明書をALBに設定することでHTTPSを利用した通信設定を実施する。 (正解)
- ○ ACMを利用してプライベートな証明書を発行し、ACMをALBに連携することでHTTPSを利用した通信設定を実施する。
- ○ ACMを利用してパブリックな証明書を発行し、証明書をRoute53に設定することでHTTPSを利用した通信設定を実施する。

説明

AWS Certificate Manager（ACM）を使用すると、サイトを保護するために使用できるパブリックまたはプライベートSSL／TLS証明書を生成できます。SSL/TLS証明書は、ネットワーク通信を保護し、プライベートネットワークのリソースと同様にインターネットで ウェブサイトのアイデンティティを確立するために使用されます。AWS Certificate Managerを使用すれば、SSL/TLS証明書の購入、アップロード、更新という時間のかかるプロセスを手動で行う必要がなくなります。パブリック証明書はELBに設定することになるため、オプション３が正解となります。

オプション１と２は不正解です。ACMから生成されたパブリック証明書は、Amazon CloudFront、Elastic Load Balancing、またはAmazon API Gatewayに使用できますが、プライベート証明書とは異なり、EC2インスタンスで直接使用することはできません。

オプション４は不正解です。ACMは証明書を発行管理していますが、直接にALBと連携して設定するものではありません。ALB側でACMで発行した証明書IDを設定することが必要です。

オプション５は不正解です。ACMで発行したSSL証明書は、CloudFront、ELBなどの配信先を利用して設定することができます。Route53だけではSSLをルーティング先を指定することができても、SSL証明書を設定することができません。

問題10: 不正解

メディア企業のA社はニュースメディアサイトをオンプレミスのWEBサーバーとOracleデータベースを利用して構築しています。あなたはソリューションアーキテクトとして、現在の環境からインフラストラクチャをAWSに移行し、ウェブサイトのパフォーマンスをさらに向上させる対応を行っています。会社はメディアサイトに配置された広告から収入を得ているため、データベースサーバーに障害が発生した場合でも、メディアサイトを引き続き利用可能にする可用性が求められています。

これらの要件を満たすために高可用なアーキテクチャをどのように実現するべきですか？

- ◉ RDSにオラクルデータベースタイプのインスタンスを起動して、リードレプリカを設定する。 (不正解)
- ○ RDSにオラクルデータベースタイプのインスタンスを起動して、マルチAZ構成を実現する。 (正解)
- ○ オラクルデータベースをEC2インスタンスに設定して、ELBによるトラフィック分散を実現する。
- ○ オラクルデータベースをEC2インスタンスに設定して、AutoScalingによるトラフィック分散を実現する。

説明

RDSにオラクルデータベースタイプのインスタンスを起動して、マルチAZ構成を実現することで、データベースサーバーに障害が発生した場合でもデータベースへのフェールオーバーが可能となるため、メディアサイトを引き続き利用可能に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。

Amazon RDS マルチ AZ 配置は、データベース (DB) インスタンスの拡張された可用性と持続性を提供し、運用データベース作業負荷に自然に適合させます。Multi-AZ DB インスタンスをプロビジョニングすると、Amazon RDS はプライマリ DB インスタンスを自動的に作成するのと同時に、異なるアベイラビリティーゾーン (AZ) にあるスタンバイインスタンスにデータを複製します。各アベイラビリティーゾーンは、物理的に独立したインフラストラクチャ上で稼動しています。また高い信頼性を保つように設計されています。インフラストラクチャ障害の場合、Amazon RDS はスタンバイ (Amazon Aurora の場合はリードレプリカ) に自動的にフェイルオーバーするので、フェイルオーバーが完了するとすぐにデータベースの動作を再開できます。

オプション1は不正解です。リードレプリカは読取処理を向上させるための対応としては正しいですが、DB自体がダウンしないような構成を実現するためにはマルチAZ構成が必須となります。したがって、この対応だけでは不十分です。

オプション3と4は不正解です。EC2インスタンスへのELB構成だけではEC2インスタンスの停止や負荷には対応できますが、AZ障害には弱いため不適切です。また、Auto Scalingだけはトラフィック制御を実施できません。EC2インスタンスベースのRDSを選択するべきケース以外においては、RDSのマネージド型サービスを選択することが求められます。

問題11: 不正解

製造企業A社はオンプレミス環境のデータセンターとAWSで構成されるハイブリッドクラウドアーキテクチャを利用しています。データセンターのネットワークからVPCへのIPsec VPN接続により、AWSへのアクセスを実現していますが、接続が不安定となっているようです。また、社内のAWSユーザーから4Gbpsを超えるようなデータ転送速度が必要であるとの依頼を受けています。あなたはソリューションアーキテクトとして、現在のネットワーク間接続を補完する専用のネットワーク接続を探しています。

これらの要件を満たすことができるAWSサービスを選択してください。

- [x] Accelerated サイト間 VPN を並列で実施することで、VPN パフォーマンスを改善する。 (不正解)
- [ ] Accelerated サイト間 VPN により、VPN パフォーマンスを改善する。
- [ ] 別のVPN接続をオンプレミスとVPC間に追加することで処理性能を向上させる。
- [ ] Direct Connectをオンプレミス環境とVPC間に追加することでハイブリッド環境を設定する。 (正解)

説明

このシナリオでは、オンプレミス環境からIPsec VPN接続によってAWSへのアクセスを実現していますが、接続が不安定であり、かつ4Gbpsを超えるデータ転送速度が実現できていないため、追加の専用ネットワーク接続を確立する方法が求められています。AWSの専用ネットワーク接続としては、AWS Direct Connect を選択するのが基本的な対応となります。したがって、オプション４が正解となります。

AWS Direct Connect はプレミスから AWS への専用ネットワーク接続の構築をシンプルにするクラウドサービスソリューションです。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提供します。

オプション１と２は不正解です。AWS Global Accelerator は、AWS グローバルネットワークと AWS エッジロケーションを介してトラフィックをインテリジェントにルーティングすることにより、VPN 接続のパフォーマンスを向上させる Accelerated サイト間 VPNを実現します。これはAcceleration を有効にして、AWS グローバルネットワークを使用してパフォーマンスを向上させられるものであり、データセンター・AWS間のVPN接続そのもののパフォーマンス改善には適していません。

オプション３は不正解です。これによって、IPsec VPN接続の可用性が高まりますが、通信パフォーマンス自体は向上しません。

問題12: 正解

あなたの会社はWEBアプリケーションをデータセンターにホストしていましたが、そこが閉鎖されることになりました。したがって、データセンター内で実行されているレガシーアプリケーションをホストする仮想マシンをAWSに移行する必要があります。しかしながら、AWSへの移行後も、このアプリケーションには、オフィスネットワークにあるオンプレミスアプリケーションへのアクセスが必要です。

アプリケーション移行後にも、オンプレミス環境のアプリケーションにアクセス可能とするためには、どのようなソリューションが必要でしょうか？（2つ選択してください。）

- [x] AWS Direct Connect またはSite to Site VPNなどでオンプレミス環境とVPCを接続して、ハイブリッドインフラ構成を実現する。 (正解)
- [x] オンプレミスネットワークとVPCにおいて、IPアドレス範囲や利用している個々のIPアドレスに重複がないように設定する。 (正解)
- [ ] VMインポート/エクスポートを利用してオンプレミス側にある仮想マシンをVPC側に移行する。
- [ ] Amazon Sever Migration Serviceを利用してオンプレミス側にある仮想マシンをVPC側に移行する。
- [ ] VPCのCIDR範囲を10.0.0.0/16に設定した場合は、その範囲内にオンプレミス側のIPアドレスを付与するようにオンプレミス側のIP構成を再編成する。

説明

このシナリオでは、データセンターにあるレガシーアプリケーションをAWS環境に移行した上で、オフィスで利用されているアプリケーションをAmazon VPCに接続する必要があります。したがって、相互の接続を確立するためにはDirect ConnectまたはVPNを利用してハイブリッド接続を実施することが必要です。Direct Connectはオンプレミスのデータセンターとの間に専用線接続を構成するため、オプション１は正しいです。

また、オンプレミスサーバーのIPアドレスとVPC内のインスタンスが通信するためにIPアドレス間でアドレスが競合しないように設定する必要があります。したがって、オプション２も正解となります。

オプション５は不正解です。 VPCのCIDR範囲を10.0.0.0/16に設定した場合は、その範囲内にオンプレミス側のIPアドレスを付与するようにオンプレミス側のIP構成を再編成する必要はありません。VPCのCIDR範囲はVPC内部のみで利用可能なものだからです。

オンプレミス環境にある仮想マシンを移行する際にはVM Import／Exportサービスや Amazon Sever Migration Serviceを使用することができます。しかしながら、このシナリオでは、AWSリソースとオンプレミス環境のサーバーとの連携や接続方式が問われていますので、オプション３，４は不正解です。

問題13: 不正解

B社はモバイルアプリケーションを開発・運用しているソフトウェア企業です。あなたはソリューションアーキテクトとして、クライアント証明書認証を使用してWebサーバーでHTTPS通信を認証するSSL/TLSソリューションを設計しています。このWEBアプリケーション構成には、EC2インスタンスにホストされたWEBサーバーを利用することが決まっていますが、ELBまたはRoute53の利用要否は決まっておらず、これらの設定方式と合わせてHTTPS通信の設定方式を決める予定です。

Webサーバーで HTTPS通信を認証するために必要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] WebサーバーのElastic Network Interfaces(ENI)を設置して、Route53レコードセットに設定して、クライアントリクエストを直接ルーティングする。 (不正解)
- [x] WebサーバーのElastic IPアドレス（EIP）を設置して、Route53レコードセットに設定して、クライアントリクエストを直接ルーティングする。 (正解)
- [ ] ELBのHTTPSリスナーを使用して、WEBサーバーに配置する。
- [ ] ELBのTCPリスナーを使用して、WEBサーバーに配置する。 (正解)
- [ ] ELBのSSLリスナーを使用して、WEBサーバーに配置する。

説明

このシナリオでは、HTTPS通信がクライアント側の証明書によって認証されるようにWebサーバーをセットアップする方法が問われています。これを設計するには、ELBを使用する場合とELBを使用しない場合の2つの方法があります。

■ELBを使用しない場合

Webサーバーを直接使用してクライアントと通信するか、WebサーバーのパブリックIPアドレスをRoute53レコードセットに設定して、クライアントリクエストが直接ルーティングされるように設定します。そのためには、WebサーバーにElastic IPアドレス（EIP）を設定し、Route53レコードセットを設定して、クライアントリクエストを直接ルーティングします。そして、Webサーバー側にサードパーティーのSSL/TLS証明書を設置してHTTPSクライアントを直接に認証するようにします。したがって、この内容を説明しているオプション2は正解となります。

■ELBを使用する場合

TCPリスナーを使用してサーバー側の証明書を展開します。HTTPSリスナーを利用した場合は、ELBを終端としてSSL通信が終了してしまうため、クライアント証明書によるHTTPS通信が不可能になってしまいます。そのため、TCP通信によってELB側でSSL通信を終端とする構成をとらないようにして、クライアント端末側のSSL認証を実現します。そして、Webサーバー側にサードパーティーのSSL/TLS証明書を設定して、HTTPSクライアントを直接に認証するようにします。したがって、この内容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は不正解です。WebサーバーのElastic Network Interfaces(ENI)ではなく、Elastic IPアドレス（EIP）を設置して、Route53レコードセットを設定して、クライアントリクエストを直接ルーティングすることが必要です。

オプション3と5は不正解です。HTTPSリスナーやSSLリスナーではなく、ELBのTCPリスナーを使用して、WEBサーバーを配置することが求められます。

問題14: 不正解

あなたの会社はクラウド化のトレンドを受けてオンプレミスのデータセンターにあるレガシーアプリケーションをAWSに移行することを決定しました。このアプリケーションは複数のアプリケーションサーバーとデータベースサーバーを備えた2層アーキテクチャ構成となっています。移行に向けて、アプリケーションサーバーは2つのAZに配置したEC2インスタンスを利用し、データベースサーバーにはマルチAZ構成となるRDS MySQLインスタンスを使用します。既存のレガシーアプリケーションに接続する際は、リモートクライアントからTCPを使用してアプリケーションサーバーに接続しており、アプリケーションサーバーはTCPソケットからクライアント情報を取得しています。今後もTCPを利用したアクセスを継続することが要件となっています。

この要件を達成することができるトラフィック処理方式を選択してください。

- ◉ Route53のレイテンシールーティング設定においてELBを指定して、TCPリスナーを設定する。Route53のレイテンシールーティングが異なるAZにおける2つのアプリケーションサーバーのロード分散を実施する。 (不正解)
- ○ Proxy Protocolを実装したELBにTCPリスナーを設定する。ELBがProxy Protocolを利用してAZにおける2つのアプリケーションサーバーのロード分散を実施する。 (正解)
- ○ クロスゾーンロードバランシングを実装して、ELBを連携してTCPリスナーを設定する。ELBのクロスゾーンロードバランシングが異なるAZにおける2つのアプリケーションサーバーのロード分散を実施する。
- ○ Route53のシンプルルーティング設定においてELBを指定して、TCPリスナーを設定する。Route53のシンプルルーティングがシンプル異なるAZにおける2つのアプリケーションサーバーのロード分散を実施する。

説明

オプション2が正しい内容となります。ELBはProxy Protocolをサポートしています。Proxy Protocolは、接続をリクエストする送信元から、接続がリクエストされる送信先に接続情報を伝達するために使用されるインターネットプロトコルです。ELBではProxy Protocolのバージョン1を使用します。このバージョンでは、人が読んで理解できるヘッダー形式が使われます。

Proxy Protocolヘッダーは、バックエンド接続にTCPを使用するロードバランサーがある場合に、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とインスタンス間のトラフィックをインターセプトするため、インスタンスからのアクセスログには、発信元クライアントではなくロードバランサーのIPアドレスが含まれます。リクエストの最初の行を解析して、クライアントのIPアドレスとポート番号を取得できます。

オプション3は不正解です。クロスゾーンロードバランシングを実装すると高可用性が得られますが、クライアントのIPアドレスを提供しないため、要件に合致しません。

オプション1と4は不正解です。Route53のレイテンシールーティングとシンプルルーティングを利用しても、異なるAZにおける2つのアプリケーションサーバーのロード分散することができません。ELBを指定しているため、分散処理をするのはELB側の機能となるためです。

問題15: 正解

あなたの会社はS3バケットを利用したドキュメント管理システムを運用しています。このS3バケットではデータ転送中と静止データを保存している間のデータ保護が必要です。転送中のデータ保護に対しては、Amazon S3と他リソース間のデータ転送を保護する必要性があります。静止データの保護に対しては、S3に保存されたデータ自体を暗号化します。静止データ保護の際にはS3バケットには様々な形式の暗号化を利用できます。

SSE-S3暗号化方法の仕組みの説明として、正しい内容はどれでしょうか？

- ◉ SSE-S3暗号化ではS3オブジェクトに強い多要素暗号化を利用しており、データキーでデータを暗号化する。 (正解)
- ○ SSE-S3暗号化ではS3オブジェクトとメタデータに対して強い多要素暗号化を利用しており、カスタマーマスターキーでデータを暗号化する。
- ○ SSE-S3暗号化ではS3オブジェクトのみ強い多要素暗号化を利用しており、キー自体はKMSを利用して管理を行う。
- ○ SSE-S3暗号化ではS3オブジェクトとメタデータに対して強い多要素暗号化を利用しており、キー自体はKMSを利用して管理を行う。
- ○ SSE-S3暗号化ではS3オブジェクトに強い多要素暗号化を利用しており暗号化を実施し、カスタマーマスターキーでデータを暗号化する。

説明

オプション１が正解です。SSE-S3暗号化ではS3オブジェクトに対して強い多要素暗号化を利用しており、またデータキーがデータを暗号化しています。

KMSの暗号化では、

・カスタマーマスターキーで暗号化キーを暗号化する。

・データキーでデータを暗号化する。

という二層の構造になっています。

Amazon S3 で管理された暗号化キーによるサーバーサイド暗号化 (SSE-S3) を使用したデータ保護により、保管データを保護します。Amazon S3 は各オブジェクトを一意のキーで暗号化します。追加の安全策として、キー自体を定期的にローテーションするマスターキーで暗号化キー (データキー) を暗号化することもできます。定期的にマスターキー (カスタマーマスターキー) をローテーションすることでマスターキーが漏洩するリスクを防ぐことになります。

Amazon S3 サーバーサイド暗号化は、利用可能な最も強力なブロック暗号の 1 つである 256 ビットの Advanced Encryption Standard (AES-256) を使用してデータを暗号化します。サーバー側の暗号化では、オブジェクトのメタデータではなく、オブジェクトデータのみが暗号化されます。Amazon S3 で管理されたキー (SSE-S3) を使用したサーバー側の暗号化の特徴は以下の通りです。

■各オブジェクトは、強力な多要素暗号化を使用する一意のデータキーで暗号化されます。

■SSE-S3 は、定期的に回転するカスタマーマスタキーを使用してデータキーを暗号化します。

■S3 のサーバーサイド暗号化は、256ビット高度な暗号化標準 (AES-256)、データを暗号化するために利用可能な最強のブロック暗号のいずれかを使用しています。

■サーバーサイド暗号化はAWS マネジメントコンソールまたは HTTP リクエストヘッダーを使用しているため、事前に署名された URL を使ってアップロードする場合には適用できません。

オプション２と４は不正解です。メタデータに対して強い多要素暗号化を利用していないため、正しくありません。

オプション３は不正解です。SSE-S3キーの管理はAWS側が実行するため、正しくありません。

オプション２と５は不正解です。カスタマーマスターキーは暗号化キーを生成する際に利用する基軸となるキーです。暗号化と復号化自体は暗号化キーを利用して実行します。

問題16: 不正解

あなたはソリューションアーキテクトとして、AWS上でエンタープライズシステムの構築を行っています。このシステムではキューからワークロードを実行する分散並列処理を実施するという要件があります。 この要件に対応するために、SQS FIFOキューと連携するスポットEC2インスタンスフリートにワーカーアプリケーションをデプロイしました。次に実施する対応としては、AWSの認証情報を使用してEC2インスタンスがSQSキューにフルアクセスできるように認証情報を設定する必要があります。

AWS認証情報を使用してEC2インスタンスがSQSキューにフルアクセスできる構成をどのように達成すれば良いでしょうか。

- (●) SQSへのアクセスを許可するIAMユーザーをEC2インスタンスへと割り当てて、そのEC2インスタンスを起動する。次にEC2インスタンスメタデータからロールの資格情報を取得する。 (不正解)
- ( ) SQSへのアクセスを許可するIAMロールをEC2インスタンスへと割り当てて、そのEC2インスタンスを起動する。次にEC2インスタンスのインスタンスストアからロールの資格情報を取得する。
- ( ) SQSへのアクセスを許可するIAMロールをEC2インスタンスへと割り当てられるようにスポットフリートを設定する。次にEC2インスタンスメタデータからロールの資格情報を取得する。 (正解)
- ( ) EC2インスタンスへと処理結果を連携するLambdaファンクションを構築する。次に、SQSへのアクセスを許可するIAMロールをLambdaのファンクションへと割り当てて、API Gatewayからファンクションを実行する。

説明

オプション3が正しい回答です。SQSへのアクセスを許可するケースではIAMロールを付与するのが最適です。その際にスポットインスタンス構成に対してIAMロールの付与が必要であるため、スポットフリート上で起動されるEC2インスタンスにIAMロールが付与されるように設定をする必要があります。

IAMロールはEC2インスタンスなどのリソースに付与されるアクセス権限です。IAMロールには標準の長期資格情報（パスワードまたはアクセスキー）が関連付けられていません。 代わりにユーザーが役割を引き受ける場合、一時的なセキュリティ認証情報が動的に作成され、ユーザーに提供されます。よって、SQSキューにアクセスする必要があるケースでは、IAMユーザーの代わりにIAMロールを使用する必要があります。

IAMロールのアクセス許可権限がEC2インスタンスに設定されると、資格情報がEC2インスタンスのメタデータに保存され、利用する際にメタデータから取得されます。したがって、正しい回答はオプション3となります。

オプション1は不正解です。SQSへのアクセスを許可するIAMユーザーではなく、IAMロールによってEC2インスタンスへと割り当てを設定します。

オプション2は不正解です。インスタンスストアからロールの資格情報を取得するのではなく、メタデータからロールの資格情報を取得します。

オプション4は不正解です。EC2インスタンスへと処理結果を連携するLambdaファンクションを構築する必要はありません。EC2インスタンスのサーバーとサーバレスであるLambdaの双方を利用するのは非効率です。

問題17: 正解

あなたはニュースメディア企業でWEBサイトを運用しているエンジニアです。現在はAWSを利用した新情報サイトの立ち上げプロジェクトに参画しています。この新情報サイトはWEBサーバーにEC2インスタンスを利用して、データベースにDynamoDBを利用する構成をとっています。EC2インスタンスがDynamoDBテーブルの読み込みと書き込みを実施することになりますが、API資格情報を公開せずにWEBサーバーがDynamoDBテーブルにアクセスできるようにして、セキュリティを確保することが求められています。

このシナリオにおいて、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。

- ◉ DynamoDBへの読み込み／書き込み処理権限を付与するIAMロールを作成して、WEBサーバーのインスタンスプロファイルのプロパティにおいて、そのロールを参照する (正解)
- ○ DynamoDBへの読み込み／書き込み処理権限を付与するIAMロールを作成して、WEBサーバーのインスタンスプロファイルを参照することでIAMロールをアプリケーションに関連付ける。
- ○ DynamoDBへの読み込み／書き込み処理権限を付与するIAMユーザーを作成して、WEBサーバーのインスタンスプロファイルにおいて、そのロールを参照する
- ○ DynamoDBへの読み込み／書き込み処理権限を付与するIAMユーザーを作成して、WEBサーバーのインスタンスプロファイルを参照することでIAMロールをアプリケーションに関連付ける。

説明

オプション１が正解となります。このシナリオでは、EC2インスタンスがAPI資格情報を使用せずにDynamoDBテーブルにアクセスできる必要があります。そのようなシナリオでは、IAMロールを使用してリソース間のアクセスができるようにします。WEBサーバーとなるEC2インスタンスのインスタンスプロファイルにおいて、そのロールを参照することでアクセス許可が実行されることになります。

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 ロールは、 AWSで許可/禁止する操作を決めるアクセス権限ポリシーが関連付けられている AWS アイデンティティであるという点で、IAM ユーザーと似ています。ただし、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、ロールはそれを必要とする任意の人やアプリケーションなどのAWSリソースへと付与でき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。

【参照】

https://dev.classmethod.jp/articles/do_you_know_iaminstanceprofile/

オプション２は不正解です。インスタンスプロファイルを参照することでIAMロールをアプリケーションに関連付けているわけではないため正しくありません。

オプション３と４は不正解です。IAMユーザーではなく、IAMロールが適切であるため正しくありません。

問題18: 不正解

あなたはベンチャー企業の立上げに参画しており、AWSを利用したアプリケーションの新規開発を行っています。このアプリケーションはELBとAuto Scalingを設定した一連のオンデマンドEC2インスタンスで構成されており、EC2インスタンスで実行された処理結果はDynamoDBに保存されます。アプリケーションのバージョン展開は1週間に1回行われるため、アプリケーションサーバー用の新しいAMIを自動的に作成およびテストする方法が必要です。

最近になって、サービスに対する問い合せが増加しているため、新しいチャットサービス機能をカスタマーサポートに追加することを決定しました。この機能は、ユーザーがサービス担当者とチャットできるように別のサーバーセットにホストする必要があります。また、チャット後の会話解析ツールも別サーバーを利用して追加する予定です。これらの2つの新機能はOpsWorksスタックを利用して展開されます。既存アプリケーションはレイヤー設定としてELBやDBレイヤーなどを分けずに、1つのWEBアプリケーションレイヤーで展開しています。

既存アプリケーションに2つの新機能を統合したOpsWorksの展開設定を選択してください。

- ◉ 1つのレイヤーと1つのレシピを利用した1つのAWS OpsWorksスタックを作成する。 (不正解)
- ○ 2つのレイヤーと1つのレシピを利用した2つのAWS OpsWorksスタックを作成する。
- ○ 3つのレイヤーと1つのレシピを利用した1つのAWS OpsWorksスタックを作成する。 (正解)
- ○ 2つのレイヤーと1つのレシピを利用した1つのAWS OpsWorksスタックを作成する。

説明

オプション3が正解となります。このシナリオでは、チャット機能と分析機能を既存アプリケーションとは別のサーバーセットに展開することが求められており、その際のOpsWorksスタックの設定方法が問われています。

前提条件として、既存のOpsWorksスタックのレイヤー設定は、1つのWEBアプリケーションレイヤーによって展開しています。つまり、既存の1つのレイヤーに加えて、チャット機能と会話解析機能という2つの異なるサーバーセットを追加することが求められます。したがって、基軸となるWEBアプリケーションレイヤーと、チャット機能のレイヤーと、会話分析機能を提供するレイヤーが最低限必要となり、合計で3つの異なるレイヤーに配置することが求められます。つまり、1つのスタックと3つのレイヤーを使用することになります。

AWS OpsWorks スタックは、スタックとアプリケーションを作成および管理するシンプルで柔軟な方法を提供します。OpsWorksはスタックとレイヤーをプロビジョニングします。スタックは、最上位のAWS OpsWorks Stacksエンティティです。これは、一般的にPHPアプリケーションの提供などの共通の目的があるため、集合的に管理する一連のインスタンスを表します。スタックは、コンテナとしての機能に加えて、アプリケーションやクックブックの管理など、インスタンスのグループ全体に適用されるタスクを処理します。

スタックは AWS OpsWorks スタックの中心となるコンポーネントです。これは基本的に AWS リソース用のコンテナです。目的が共通で、論理的に一括して管理されます。スタックにより、ユーザーはこれらのリソースをグループで管理することができます。また、インスタンスのオペレーティングシステムや AWS リージョンなどの一部のデフォルトの構成設定もスタックにより定義されます。ユーザーの直接操作から分離する必要のあるスタックコンポーネントがある場合、そのスタックを VPC 内で実行することもできます。

■スタック内の各レイヤーには少なくとも1つのインスタンスが必要であり、オプションで複数のインスタンスを持つことができます。

■スタック内の各インスタンスは、登録済みインスタンスを除き、少なくとも1つのレイヤーのメンバーでなければなりません。 SSHキーやホスト名などの基本設定を除き、インスタンスを直接構成することはできません。適切なレイヤーを作成および構成し、インスタンスをレイヤーに追加する必要があります。

問題19: 不正解

あなたはAWSクラウドの導入コンサルタントとしてIT企業で働いています。現在のクライアント企業A社はスケーラブルで高可用性があり、運用管理をなるべく自動化する必要があるWebアプリケーションの構築を求めています。開発チームはアプリケーションのWebサーバーとデータベースサーバーをホストするために、一連のEC2インスタンスを展開しました。WebサーバーはVPCのパブリックサブネットに、データベースサーバーはプライベートサブネットにデプロイされています。さらに、このアーキテクチャの可用性と負荷分散のためにELBまたはRoute53を設定した構成が必要です。

ELBとRoute53を組み合わせて利用した場合と、Route53のみを利用した場合の構成パターンを選択してください。（2つの選択してください。）

- [x] CLBをEC2インスタンスに設定してトラフィック分散を実施する。その上で、Route53を利用して新しいALIASレコードにロードバランサーのDNSネームをマップする。 (不正解)
- [ ] Route53を利用してALIASレコードに「No」と設定して、複数値回答ルーティングを選択し、WEBアプリケーションの全IPアドレスを設定する。 (正解)
- [ ] Route53を利用してALIASレコードの生成して、複数値回答ルーティングを選択し、WEBアプリケーションの全IPアドレスを設定する。
- [ ] ALBをEC2インスタンスに設定してトラフィック分散を実施する。その上で、Route53を利用して新しいCNAMEレコードにロードバランサーのDNSネームをマップする。
- [ ] ALBをEC2インスタンスに設定してトラフィック分散を実施する。その上で、Route53を利用して新しいALIASレコードにロードバランサーのDNSネームをマップする。 (正解)

説明

このシナリオでは、EC2インスタンスを利用したアプリケーション構成に対して、ELBを利用した場合の構成パターンとRoute53のみを利用した場合の構成パターンが問われています。

オプション２は正解となります。Route 53のみを利用する場合は、ALIAS（エイリアス）レコードに「No」と設定し、複数値回答ルーティングを使用すると、DNSクエリに応答して、WebサーバーのIPアドレスなどの複数の値を返すようにAmazon Route 53を構成できます。ほとんどすべてのレコードに複数の値を指定できますが、複数値の回答ルーティングでは各リソースの正常性も確認できるため、Route 53は正常なリソースの値のみを返します。これはロードバランサーの代わりにはなりませんが、複数のヘルスチェック可能なIPアドレスを返すため、DNSを使用した可用性とロードバランシングを改善する方法です。

オプション５は正解となります。ELBを利用する場合はRoute53のALIASレコードを使用する構成を実施します。WebサーバーがELBの背後にある場合、Webサーバーの負荷が均一に分散されます。今回はWEBサーバーに標準的に利用するALBを利用するべきシナリオです。NLBは１００万アクセスなどの高負荷な特殊なアプリケーションなどに構成します。CLBは現在利用が推奨されていません。また、Route 53を使用して、ELBエンドポイントを指すALIASレコードを設定することもできます。

オプション１は不正解です。CLBはTCPリスナーを利用したい場合など特殊なケース用の古いロードバランサーです。NLBは１００万アクセスなどの高負荷な特殊なアプリケーションなどに構成します。通常のWEBアプリケーションにはALBを利用することが求められています。

オプション３は不正解です。複数値回答ルーティングを設定する際はRoute53を利用してALIASレコードの生成したら、「No」の設定が必要となります。

オプション４は不正解です。ALBをEC2インスタンスに設定してトラフィック分散を実施し、Route53を利用して新しいCNAMEレコードにではなく、ALIASレコードにロードバランサーのDNSネームをマップする必要があります。

問題20: 不正解

あなたはグローバル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です。彼らの事務所は世界中の52か所にあり、アメリカ、ヨーロッパ、アジアリージョンにいくつかのVPCを有しています。内部インフラ監査の一環として、あなたは単一のダッシュボードを設定して、ここで異なるAWSリージョンにある全オフィスすべてのEC2インスタンスを集合的に監視したいと考えています。

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？

- ◉ 各リージョンでCloudWatchダッシュボードを設定した上で、モニタリングに必要なメトリクスを指定する。その上で、AWS Organizationsの統合ダッシュボードを利用して全データを一元管理する。 (不正解)
- ○ 各リージョンでCloudWatchのモニタリングに必要なメトリクスを指定する。その上で、マスターアカウントの設定ナビゲーションバーで、リージョンを選択することで各リージョンにあるCloudWatchを指定し、マスタアカウントにおいてメトリクスを集約することができる。
- ○ 各リージョンにCloudWatchエージェントを起動させることで、1つのCloudWatchダッシュボードによって、複数リージョンに跨いだAWSリソースの監視を実施することが可能である。
- ○ CloudWatchの設定ナビゲーションバーにおいて、リージョンを選択することで1つのCloudWatchに対して、他リージョンのAWSリソースのメトリクスを表示することができる。 (正解)

説明

1つの CloudWatch ダッシュボードを使用して複数のリージョンにある AWS リソースを統合的にモニタリングできます。たとえば、us-west-2 リージョンにある EC2 インスタンスの CPU 使用率と us-east-1 リージョンにある請求メトリクスを表示するダッシュボードを作成できます。 1つのダッシュボードで、複数のリージョンのリソースをモニタリングするには 以下の手順を実施します。

■https://console.aws.amazon.com/cloudwatch/にある CloudWatch コンソールを開きます。
■ナビゲーションペインで メトリクスを選択します。
■ナビゲーションバーで、リージョンを選択します。
■ダッシュボードに追加するメトリクスを選択します。
■[アクション] で、[ダッシュボードに追加] を選択します。
■[追加] で、新しいダッシュボードの名前を入力し、[ダッシュボードに追加] を選択します。 または、既存のダッシュボードに追加するには、[既存のダッシュボード] を選択し、ダッシュボードを選択して、[ダッシュボードに追加] を選択します。
■別のリージョンからメトリクスを追加するには、次のリージョンを選択し、以下のステップを繰り返します。
■[ダッシュボードを保存] を選択します。

この設定に従うと、ナビゲーションバーにてリージョンを選択するという、オプション4が正解となります。

オプション1と2と3は不正解です。1つの CloudWatch ダッシュボードを使用して複数のリージョンにある AWS リソースをモニタリングできます。したがって、各リージョンにて個別にCloudWatchを設定する必要はありません。

問題21: 不正解

あなたはソリューションアーキテクトとして、ヘルステックベンチャーでAWS上にホストされた健康管理アプリケーションの開発を行っています。このアプリケーションは患者のさまざまな日々の体調データなどをウェアラブルデバイスから取得して、データ解析を行っています。大量のデータ処理が毎日発生するため、Web層とアプリケーション層および大規模なデータ処理を行うデータベース層からなる、スケーラブルな構成にすることが求められています。また、高速性能を維持するためには、セッション管理には非常にシンプルで高性能な仕組みが必要となります。

この要件を満たすAWSアーキテクチャ設計パターンを選択してください。

- [x] WEBアプリケーションをホストするEC2インスタンス群に対して、AutoScalingを設定する。データベース層におけるセッション処理にElastiCache Redisを利用して、CloudWatchによるモニタリングを実施する。その上で、リードレプリカを設定したRDSをデータベースとして利用する。 (不正解)
- [ ] WEBアプリケーションをホストするEC2インスタンス群に対して、AutoScalingを設定する。データベース層におけるセッション処理にElastiCache Memcachedを利用して、CloudWatchによるモニタリングを実施する。その上で、リードレプリカを設定したRDSをデータベースとして利用する。 (正解)
- [ ] WEBアプリケーションをホストするEC2インスタンス群に対して、AutoScalingを設定する。データベース層におけるセッション処理にELBを利用して、CloudWatchによるモニタリングを実施する。その上で、リードレプリカを設定したRDSをデータベースとして利用する。
- [ ] WEBアプリケーションをホストするEC2インスタンス群に対して、AutoScalingを設定する。データベース層におけるセッション処理にRoute53を利用して、CloudWatchによるモニタリングを実施する。その上で、リードレプリカを設定したRDSをデータベースとして利用する。

説明

オプション２が正解となります。このアプリケーションでは、ユーザーまたはサービスがアプリケーションと対話する際は、セッションを形成して一連の対話を実行します。セッションはコンピュータ間で通信される際に、接続を確立してから切断するまでの一連の通信コネクションのことです。このセッション処理がボトルネックにならないように高性能かつシンプルな仕組みが求められています。

ソリューションとしては、まずはWEBアプリケーションをホストするEC2インスタンス群に対して、AutoScalingを設定します。データベース層のセッション処理にElastiCache Memcachedを利用して、CloudWatchによるモニタリングを実施し、リードレプリカを設定したRDSをデータベースとして利用する構成とします。

このシナリオでの最適なオプションは、Elasticache、Cloudwatch、およびRDSリードレプリカの組み合わせを使用することです。ウェブサーバーは、読み取り操作にElastiCache Memcachedを使用し、トラフィックの変動を監視してそれに応じてスケールイン/スケールアウトするように自動スケーリンググループに通知するCloudWatchを使用します。さらに、RDSのリードレプリカを使用して、読み取りが多いワークロードを処理します。

ElastiCache Memcached は使いやすく、高パフォーマンスなインメモリデータストアです。ミリ秒未満の応答時間を実現するスケーラブルなソリューションを構成することができます。セッション管理において非常にシンプルで高性能な構成が必要な場合にはElastiCache Memcached を利用することが多いです。一方で、Redisはより高性能でスナップショットやレプリケーションなどの機能が充実しており、複雑な設定が可能となります。今回はセッション管理には非常にシンプルで高性能な構成を利用するため、ElastiCache Memcached を選択します。したがって、オプション１は不正解です。

また、ELBやRoute53にはそういった機能はありません。したがって、オプション３と４は不正解です。

問題22: 正解

B社ではメディアサイトをAWSにホストして運用しています。このメディアサイトではメディア広告が重要な収益源になっており、あなたはソリューションアーキテクトとして、広告収益の分析システムを構築することになりました。要件としては、メディア訪問者のWEBサイト内でのクリックを分析して、訪問者がクリックしたページと広告シーケンスが適切にマッチしているかを分析する必要があります。また、訪問者がメディアサイト内をクリックするときに適切な広告が表示されるようにタイムリーな処理が求められています。

こ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。

- (●) Amazon Kinesisを利用してWEBクリックデータをセッション毎に取得して、ワーカーによりWEB行動データ分析を実施する。 (正解)
- ( ) Lambdaファンクションにより WEBクリックデータを取得して、DynamoDBに蓄積してWEB行動データ分析を実施する。
- ( ) Amazon Kinesisを利用してWEBクリックデータをセッション毎に取得して、Kinesis Agentにより WEB行動データ分析を実施する。
- ( ) Lambdaファンクションにより WEBクリックデータを取得して、Kinesis AnalyticsにてWEB行動データ分析を実施する。

説明

オプション1が正解となります。このシナリオでは、Amazon Kinesisを利用したクリックストリーム処理によって要件を達成することができます。Amazon Kinesisはストリーミングデータをリアルタイムで収集、処理、分析を実施するサービスです。Kinesis アプリケーションは複数のアプリケーションインスタンスを持つことができ、ワーカーは各アプリケーションインスタンスに対応する処理ユニットです。1つのワーカーは1つまたは複数のレコードプロセッサにマッピングされます。1つのレコードプロセッサは1つのシャードに対応し、そのシャードからのデータレコードを処理します。このワーカーを利用して、ユーザーのクリックストリームデータに基づいて、WEB行動を解析するアプリケーションを構成できます。

オプション2と4は不正解です。Lambda関数によってストリームデータに対して何らかの処理をプログラミングすることは可能ですが、マネージドサービスとして提供されているKinesis Data Streamsを利用する方が、容易にプロセスを構築可能です。また、データはリアルタイムで処理され、訪問者がWebポータルをクリックするときにページレイアウトが変換される必要があり、リアルタイム処理が基本となります。この場合、リアルタイムデータ処理に特化した、Kinesisを使うべきです。

オプション3は不正解です。Kinesis Agent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、これを利用してデータを収集して Kinesis Data Streams に送信する方法を提供します。しかしながら、これはデータ分析を実行する機能ではないため不正解です。

問題23: 不正解

B社はグローバルなEコマースサイトを展開しているグローバル企業です。このEコマースサイトはグローバルに対応するためにマルチリージョンにEC2インスタンスを展開しており、ウェブ層とアプリケーション層の両方でELBを使用し、Eコマースに表示する画像データなどにS3に保存された静的コンテンツを使用しています。また、データ層では顧客データ管理用にRDSを使用しています。セキュリティ監査によってサイトの脆弱性が発見されたため、このWEBサイトに対する悪意のあるアクセスを遮断する設定を行うことになりました。

このアプリケーションに対して、悪意のあるアクセスを遮断するためのソリューションを選択してください。

- (●) Amazon Sheldを2つのELBの間に配置して、すべてのトラフィックを処理する。Amazon Sheldにより悪意のあるリクエストをフィルタリングし、フィルタリング後に別のELBで悪意のないリクエストを受信して、処理のためにEC2インスタンスに送信する。 (不正解)
- ( ) WAFレイヤーを各ELBの前面にそれぞれ配置して、すべてのトラフィックを処理する。WAFにより悪意のあるリクエストをフィルタリングし、フィルタリング後に別のELBで悪意のないリクエストを受信して、処理のためにEC2インスタンスに送信する。
- ( ) WAFレイヤーを2つのELBの間に配置して、すべてのトラフィックを処理する。WAFにより悪意のあるリクエストをフィルタリングし、フィルタリング後に別のELBで悪意のないリクエストを受信して、処理のためにEC2インスタンスに送信する。 (正解)
- ( ) ELBの前面にRoute53を設置して、その前面にWAFレイヤーを配置して、すべてのトラフィックを処理する。WAFにより悪意のあるリクエストをフィルタリングし、フィルタリング後に別のELBで悪意のないリクエストを受信して、処理のためにEC2インスタンスに送信する。

説明

AWSリソースに対する不正なアクセスを防ぐソリューションを設計するようなシナリオでは、Web Application Firewall（WAF）を利用します。WAFの設置方法としては、オプション3のサンドウィッチ方式が正解となります。WAFレイヤーを2つのELBの間に配置して、すべてのトラフィックを処理できるようにする必要があります。これによって、WAFにより悪意のあるリクエストをフィルタリングし、フィルタリング後の悪意のないリクエストを送信する別のELBで悪意のないリクエストを受信し、処理のためにEC2インスタンスに送信することができます。

WAFレイヤーが防御の最前線として機能し、既知の攻撃ソースを除外し、SQLインジェクションやクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックします。これはWAFサンドウィッチと呼ばれており、WAFレイヤーが2つのELBの間に配置されます。1つはWebに面することで、すべてのトラフィックを受信し、その後にWAFが悪意のあるリクエストをフィルタリングして、フィルタリング後に後ろのELBが悪意のないリクエストを受信して、EC2インスタンスに当該リクエストを送信します。

オプション1は不正解です。AWS Shield はマネージド型の分散サービス妨害 (DDoS) に対する保護サービスで、AWS で実行しているアプリケーションを保護します。AWS Shieldも必要なサービスではありますが、今回のような悪意のあるアクセスのフィルタリングにはAWS ShieldではなくWAFを利用するため、不十分です。

オプション2は不正解です。WAFレイヤーを各ELBの前面にそれぞれに配置するのではなく、EC2インスタンスを持つWAFレイヤーが2つのELBの間に配置されます。

オプション4は不正解です。ELBの前面にRoute53を設置して、その前面にWAFレイヤーを配置するのではなく、EC2インスタンスを持つWAFレイヤーが2つのELBの間に配置されます

問題24: 正解

B社はモバイルアプリケーションを開発・運用しているソフトウェア企業です。最近になって睡眠改善アプリケーションをリリースし、既に5万人のユーザーを獲得している人気アプリになっています。睡眠改善アプリはミドルウェアに5分ごとに1 KBの睡眠状態データを送信して、一連のEC2インスタンスによってデータ処理後にDynamoDBテーブルにデータを書き込みます。朝10時になるとテーブルをスキャンして昨夜のデータをユーザーごとに集計して、集計結果をAmazon S3に保存します。ユーザーはAmazon SNSモバイルプッシュ通知によって新しいデータが利用可能であることが通知され、自身の睡眠状態や健康状態に関するアドバイスを受け取ることができます。このアプリのユーザーの増加に伴って、コストが増加していることが課題となっています。また、毎朝のデータ処理の負荷が高まっており、その負荷軽減対応も必要です。

このアーキテクチャに対してコスト削減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] Amazon DynamoDBテーブルを毎日新しく作成して、元データと日々のデータ解析結果をS3に保存した後に、古い前日データを保存しているDynamoDBテーブルを削除することで、データ保存に係るコストを削減する。 (正解)
- [x] Amazon SQSのキューイングによってデータ書き込み処理を並列化することでDynamoDBテーブルの書き込み処理スループットを軽減する。また、DynamoDBテーブルのAutoScalingを有効化して、一時的なスループットキャパシティを増加させる。 (正解)
- [ ] Amazon DynamoDBテーブルのレプリケーションを有効化して、元データと日々のデータ解析結果をS3に保存した後に、古いDynamoDBレプリケートテーブルを削除することで、データ保存に係るコストを削減する。
- [ ] Amazon DynamoDBグローバルテーブルを作成して、複数リージョンにデータを保存することで、S3へのデータ保存をやめてデータレイヤーを統合する。
- [ ] Lambdaファンクションによるデータ処理を実行して、実行結果をS3に保存することで、DynamoDBテーブルを廃止する。
- [ ] Amazon SQSのキューイングによってデータ書き込み処理を並列化することでDynamoDBテーブルの書き込み処理スループットを軽減する。また、DynamoDBテーブルのDAXを有効化して、一時的なスループットキャパシティを増加させる。

説明

このアプリケーションのデータ処理形式では、保存されるデータは古いデータと最近のデータまでが同じように膨大に保存されており、日々膨大なデータが蓄積されるためにDynamoDBテーブルのコスト増をまねいています。実際に利用されるデータは当日データのみとなります。前日までのデータは今後使われる可能性はあるものの、利用頻度が低いためDynamoDB上でのデータ処理は必要ありません。つまり、全てのデータをDynamoDBテーブルに保存する仕組みは非効率でコスト効率も悪い状態となります。したがって、不要なデータをDynamoDBテーブルに保持しない仕組みにするオプション１が正解となります。

また、SQSを使用した並行処理を実行することで、DynamoDBがプロビジョニングされた容量を超えないように処理負荷を軽減させることができます。また、DynamoDBテーブルのAutoScalingを有効化して、一時的なスループットキャパシティを増加させることができます。したがって、オプション２も正解となります。

オプション３は不正解です。Amazon DynamoDBテーブルをレプリケーションして、クロスリージョンレプリケーションを利用できます。これは複数の AWS リージョンにまたがって自動的にレプリケートされるテーブルを作成できます。マルチマスター書き込みは完全にサポートされています。これにより、レプリケーションプロセスを管理することなく、高速で大規模にスケールされたグローバルユーザーベースのアプリケーションを構築できます。しかしながら、この構成は高性能になりますが、逆にコストが上がってしまうため不適切です。

オプション４は不正解です。Amazon DynamoDBグローバルテーブルを作成して、複数リージョンにデータを保存することでデータ冗長性を高めることができますが、逆にコストが上がってしまうため不適切です。

オプション５は不正解です。Lambdaファンクションによるデータ処理を実行することで、実行結果をS3に保存することは、データ処理としては可能です。このシナリオでは、一連のEC2インスタンスによってDynamoDBテーブルにデータを書き込みます。朝10時になるとテーブルをスキャンして昨夜のデータをユーザーごとに集計することが必要です。その際にDynamoDBテーブルを利用した高速データ処理が必須になります。S3に保存するデータはあくまでもアーカイブとなり、高速データ処理には向いていません。

オプション６は不正解です。DAXはキャッシュによってテーブル内のデータ処理を高パフォーマンス化するDynamoDB機能です。これは一時的な高パフォーマンスではなく、DAXが起動している間定常的にパフォーマンスをキープすることになるため、要件にあっていません。またDAXは高コストですので、コスト増をまねいてしまいます。

問題25: 不正解

ベンチャー企業ではオンプレミスとAWSの両方の環境でアプリケーション開発を実施しています。開発チームはCI/CD環境を整備してアプリケーション開発を進めています。現在開発しているWEBアプリケーションはEC2インスタンス上にホストされ、その展開をなるべく自動化することが求められています。そのため、AWS CodePipeline、OpsWorks、CloudFormationなどのサービスを組み合わせてパイプラインを構築することが、あなたのタスクです。

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。

- ◉ CloudFormationでスタックとレイヤーを設定し、インスタンスを起動するアプリコードをAmazon S3バケットにアップロードする。AWS CloudFormationのリソース設定でAWS OpsWorksスタックを展開方式として設定する。CodePipelineでパイプラインを利用してCloudFormationテンプレートを指定して実行する。 (不正解)
- ○ CodeDeployでスタックとレイヤーを設定し、インスタンスを起動するアプリコードをAmazon S3バケットにアップロードする。AWS CodePipelineでパイプラインを利用してS3バケットからのアプリリソースのデータ取得を指定し、AWS OpsWorksスタックを展開方式として設定する。
- ○ CloudFormationでスタックとレイヤーを設定し、インスタンスを起動するアプリコードをAmazon S3バケットにアップロードする。AWS CodePipelineでパイプラインを利用してS3バケットからのアプリリソースのデータ取得を指定し、AWS OpsWorksスタックを展開方式として設定する。
- ○ AWS OpsWorks Stacksでスタックとレイヤーを設定し、インスタンスを起動するアプリコードをAmazon S3バケットにアップロードする。AWS CodePipelineでパイプラインを利用してS3バケットからのアプリリソースのデータ取得を指定し、AWS OpsWorksスタックを展開方式として設定する。 (正解)

説明

AWS CodePipeline により、トラックコードが CodeCommit、S3、GitHub などのソースから変更されるパイプラインを作成できます。CodePipeline からシンプルなパイプラインを作成し、AWS OpsWorks スタックレイヤーで実行するコードのデプロイツールとして使用することができます。AWS CodePipelineをAWS OpsWorksスタックで使用する詳細な手順については、以下を参照してください。

- AWS OpsWorks Stacksでスタック、レイヤー、およびインスタンスを作成する
- アプリコードをAmazon S3バケットにアップロードする
- アプリをAWS OpsWorksスタックに追加する
- AWS CodePipelineでパイプラインを作成する
- AWS OpsWorks Stacksでのアプリのデプロイの確認する。

この手順を踏まえた回答としては、オプション４が正解となります。

その他のオプションは上記手順のいづれかが間違った内容となっています。

問題26: 正解

B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。ハイブリッドクラウドを実現するためにオンプレミス環境からAWSへの Direct Connect接続を確立しています。会社は東京を拠点としているため、AWSへのDirect Connectが東京リージョンに接続されています。その後、東京リージョンとシドニーリージョンをつないだマルチリージョン構成を実現する要件が発生しました。実施すべき要件は以下の通りです。

・シドニー支店のオフィスとシドニーリージョンを専用線で接続する。

・シドニーリージョンと東京リージョンを接続する。その際にDirect Connect接続を活かして東京リージョンとシドニーリージョンとの間の通信を安全でコスト最適に実施する。

・インターネットを介さずS3とDynamoDBへの接続を実施する。

シドニーリージョンに対する安全な接続のための、最適なソリューションを選択してください。

- ◉ パブリック仮想インターフェースをシドニーリージョンに作成してDirect Connect接続を実施する。さらにデータ保護のためにパブリック仮想インターフェイスを介した安全な接続により東京リージョンとVPN接続を実施する。 (正解)
- ○ プライベート仮想インターフェースをシドニーリージョンに作成しDirect Connect接続を実施する。さらにデータ保護のためにプライベート仮想インターフェイスを介した安全な接続により東京リージョンと専用線接続を実施する。
- ○ プライベート仮想インターフェースをシドニーリージョンに作成しDirect Connect接続を実施する。さらにデータ保護のためにプライベート仮想インターフェイスを介した安全な接続により東京リージョンとVPN接続を実施する。
- ○ パブリック仮想インターフェースをシドニーリージョンに作成しDirect Connect接続を実施する。さらにデータ保護のためにパブリック仮想インターフェイスを介した安全なVPN CloudHubにより東京リージョンと専用線接続を実施する。

解説

このシナリオでは、東京リージョンとオンプレミス環境で利用しているDirect Connect接続を活かして東京リージョンとシドニーリージョン間の通信を最適化することが求められています。AWS Direct Connect 接続の使用を開始するには、次のいずれかの仮想インターフェイスを作成する必要があります。

■プライベート仮想インターフェイス:
プライベート IP アドレスを使って Amazon VPC にアクセスするには、プライベート仮想インターフェイスを使用する必要があります。

■パブリック仮想インターフェイス:
パブリック仮想インターフェイスは、パブリック IP アドレスを使用してすべての AWS パブリックサービスにアクセスできます。

■トランジット仮想インターフェイス:
Direct Connect ゲートウェイに関連付けられた 1 つまたは複数の Amazon VPC トランジットゲートウェイ にアクセスするには、トランジット仮想インターフェイスを使用する必要があります。

パブリック仮想インターフェイスを利用することで、Direct ConnectはVPC上で作成したサブネットとの通信だけでなく、S3やDynamoDBといった従来インターネット経由でアクセスしていたAWSサービスにもDirect Connect専用線を経由して直接通信することができます。それにより、従来インターネット経由でアクセスしていたAWSクラウド上のサービスや、VPCを経由していたサービスも、より信頼性の高い直接的な接続が可能になります。

また、パブリック仮想インターフェイスによるDirect Connect 接続で VPC にVPN 接続を確立することができます。これはインターネット経由の VPC よりも速くて安全です。Direct Connect 接続の AWS VPN 接続では、一貫性のあるスループットレベルを確保し、データを保護する暗号化アルゴリズムを実現します。

したがって、シドニーリージョンへのパブリック仮想インターフェイスを作成し、東京リージョン間とのVPN接続を実現することで信頼の高い接続を確立することができます。オプション 1 が正解となります。

オプション 2 と 3 は不正解です。プライベート仮想インターフェイスによってリージョン間を専用線接続することは可能ですが、その際にインターネットを介したS3とDynamoDB間への接続も必要となっており、パブリック仮想インターフェイスにする必要があります。

オプション 3 は不正解です。VPN接続を実施するためには、パブリック仮想インターフェイスにする必要があります。

オプション 4 は不正解です。VPN CloudHubによる接続ではないため、不正解です。

問題27: 不正解

大手車両メーカーは大規模なエンタープライズシステムを有しており、オンプレミスデータセンターにはOracle Real Application Clusters（RAC）データベースがあり、AWSへの移行を予定しています。あなたはソリューションアーキテクトとして、AWSに移行する際に、デ- タベ ースが実行されるオペレーティングシステムのパッチ管理プロセスとバックアッププロセスを自動化する対応を行っているところです。

コスト最適な方法で、このシナリオの要件を満たすにはどうすればよいですか？

- ◉ EC2インスタンスを利用してOracle Real Application Clusters（RAC）データベースをインストールして利用する。SSM AgentをEC2インスタンスにインストールして、パッチジョブの自動化をAWS System Managerを利用して実現する。さらにAmazon DataPipelineを利用してEBSボリュームのスナップショット取得を定期的に実行する。 (不正解)
- ○ RDSを利用してOracleデータベースを選択して利用する。SSM AgentをEC2インスタンスにインストールして、パッチジョブの自動化をAWS System Managerを利用して実現する。さらにAmazon DLMを利用してEBSボリュームのスナップショット取得を定期的に実行する。
- ○ EC2インスタンスを利用してOracle Real Application Clusters（RAC）データベースをインストールして利用する。SSM AgentをEC2インスタンスにインストールして、パッチジョブの自動化をAWS System Managerを利用して実現する。さらにAmazon DLMを利用してEBSボリュームのスナップショット取得を定期的に実行する。 (正解)
- ○ RDSを利用してOracleデータベースを選択して利用する。SSM AgentをEC2インスタンスにインストールして、パッチジョブの自動化をAWS Batchを利用して実現する。さらにAmazon DLMを利用してEBSボリュームのスナップショット取得を定期的に実行する。

説明

Amazon RDSは、マルチテナントデータベース、Real Application Clusters（RAC）、統合監査、Database Vaultなど、Oracleの特定の機能をサポートしていません。したがって、Oracle RACデータベースはRDSではなくEC2インスタンスにのみ移行できるため、オプション２と４は不正解となります。

AWS Systems Manager Patch Managerは、セキュリティ関連の更新で管理対象インスタンスにパッチを適用するプロセスを自動化します。 Linuxベースのインスタンスの場合、セキュリティ以外の更新プログラムのパッチをインストールすることもできます。オペレーティングシステムの種類ごとに、Amazon EC2インスタンスのフリートまたはオンプレミスサーバーと仮想マシン（VM）にパッチを適用できます。インスタンスをスキャンして、欠落しているパッチのレポートのみを表示できます。 また不足しているすべてのパッチをスキャンして自動的にインストールできます。 Amazon DLMを利用してEBSボリュームノスナップショット取得を定期的に実行することができます。したがって、オプション３が正解となります。

オプション１は不正解です。Amazon DataPipelineではなく、Amazon DLMを利用してEBSボリュームのスナップショット取得を定期的に実行することが求められます。

問題28: 正解

大手商社は社内のエンタープライズシステムをハイブリッドアーキテクチャで構成しています。オンプレミスのデータセンターとAWSとは、単一VPCのLink Aggregation Group（LAG）を構成した複数のAWS Direct Connectを利用して接続されています。システム運用時には、各種サーバーOSに対してパッチを適用することが必要です。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使用されているパッチベースラインに基づいて、VPC内にあるEC2インスタンスへのパッチ適用スケジュールを自動化するタスクを設定しているところです。

コスト最適な方法で、この要件を満たすにはどうすればよいですか？

- (●) オンプレミスデータセンターのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するAWS Systems Manager Patch Managerを設定する。SSM Agentを全てのインスタンスにインストールし、AWS Systems Managerメンテナンスウィンドウを利用したパッチアクションのスケジュール設定を行う。 (正解)
- ( ) オンプレミスデータセンターのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するAWS Batchを設定する。SSM Agentを全てのインスタンスにインストールし、AWS Systems Managerメンテナンスウィンドウを利用したパッチアクションのスケジュール設定を行う。
- ( ) オンプレミスデータセンターのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するAWS Systems Manager Patch Managerを設定する。SSM Agentを全てのインスタンスにインストールし、AWS WorkFlow Managerを利用したパッチアクションのスケジュール設定を行う。
- ( ) オンプレミスデータセンターのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するAWS Batchを設定する。SSM Agentを全てのインスタンスにインストールし、AWS WorkFlow Managerを利用したパッチアクションのスケジュール設定を行う。

説明

オプション１が正解となります。オンプレミスデータセンターのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するためには、AWS Systems Manager Patch Managerを利用することができます。

AWS Systems Manager Patch Manager は、セキュリティ関連のアップデートと他のタイプのアップデートの両方でマネージドインスタンスにパッチを適用するプロセスを自動化します。Patch Manager を使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。オペレーティングシステムのタイプ別に、Amazon EC2 インスタンスまたはオンプレミスサーバー、および仮想マシン (VM) にパッチを適用できます。Windows Server、Ubuntu Server、Red Hat Enterprise Linux (RHEL)、SUSE Linux Enterprise Server (SLES)、CentOS、Amazon Linux、Amazon Linux 2 のサポートされているバージョンが対象になります。

これをEC2インスタンスに適用するためには、SSM Agentを全てのインスタンスにインストールして、AWS Systems Manager メンテナンスウィンドウにおいてパッチアクションのスケジュール設定を行います。AWS Systems Managerメンテナンスウィンドウ では、オペレーティングシステムのパッチ適用、ドライバーの更新、ソフトウェアやパッチのインストールなどのアクションを実行するスケジュールを定義できます。メンテナンスウィンドウ ではS3バケット、SOSキュー、AWS KMSキーなど、多くの AWS リソースタイプでアクションをスケジュールすることもできます。

オプション2は不正解です。オンプレミスデータセンターからのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するのにはAWS Batchではなく、AWS Systems Manager Patch Managerを利用します。

オプション3は不正解です。SSM Agentを全てのインスタンスにインストールし、AWS WorkFlow Managerではなく、AWS Systems Manager メンテナンスウィンドウ利用したパッチアクションのスケジュール設定を行います。

オプション4は不正解です。オンプレミスデータセンターからのパッチベースラインに基づいてEC2インスタンスのセキュリティパッチを展開・管理するためにはAWS Batchではなく、AWS Systems Manager Patch Managerを利用します。SSM Agentを全てのインスタンスにインストールし、AWS WorkFlow Managerではなく、AWS Systems Manager メンテナンスウィンドウ利用したパッチアクションのスケジュール設定を行います。

問題29: 不正解

ある会社は複数部門で複数のAWSアカウントを使用して大規模にAWSを利用しています。各部門は適用アカウントにリソースを持つ1つ以上のAWSアカウントを有しています。最近、営業部門メンバーが誤って情報システム部門が管理しているEC2インスタンスを停止してしまい、大規模なシステム障害が発生してしまいました。今後はこのようなミスを予防することが必要です。あなたはソリューションアーキテクトとして、部門別のEC2インスタンスの管理を制御する設定を依頼されました。

次のうち、このシナリオの要件を満たす最適な方法を選択してください。

- ◉ AWS Organizationsを利用して、組織単位（OU）を使用してアカウントをグループ化し、EC2インスタンスの削除操作ができる開発アカウント向けのOUにSCPを設定して、自部門のインスタンスのみを操作できる設定を行う。OUの全メンバーアカウントに対してクロスアカウントアクセスを有効化し、さらにアカウント内部ではSCPに基づく権限を付与する。 (不正解)
- ○ AWS Organizationsを利用して、組織単位（OU）を使用してアカウントをグループ化し、EC2インスタンスの削除操作ができる開発アカウント向けのOUにSCPを設定して、自部門のインスタンスのみを操作できる設定を行う。OUの全メンバーアカウントに対してクロスアカウントアクセスを有効化し、さらにアカウント内部ではIAMポリシー設定に基づく権限を付与する。 (正解)
- ○ AWS Organizationsを利用して、組織単位（OU）を使用してアカウントをグループ化し、EC2インスタンスの削除操作ができる開発アカウントに自部門のインスタンスのみを操作できるIAMロールを設定する。OUの全メンバーアカウントに対してクロスアカウントアクセスを有効化し、さらにアカウント内部ではIAMポリシー設定に基づく権限を付与する。
- ○ AWS Organizationsを利用して、組織単位（OU）を使用してアカウントをグループ化し、EC2インスタンスの削除操作ができる開発アカウントにIAMロールを作成して、自部門のインスタンスのみを操作できる設定を行う。OUの全メンバーアカウントに対してクロスアカウントアクセスを有効化し、さらにアカウント内部ではSCPに基づく権限を付与する。

説明

SCPとIAMポリシーの違いと設定方法をどう理解しているかが問われている問題です。今回のケースでは、SCPによって別メンバーアカウントへのアクセス権限を取得したうえで、アカウント内部ではIAMポリシーによってユーザーに対する細かい権限設定を行うという回答になります。

アカウントに SCP がアタッチされていると、アイデンティティのポリシーおよびリソースベースのポリシーは、それらのポリシーと SCP によってアクションが許可されている場合にのみ、エンティティにアクセス許可を付与します。SCPは組織単位のリソースへのアクション権限を設定し、その中でさらにユーザー単位でのリソースへのアクション権限を設定することになります。OU内のメンバーアカウントでは、別途IAMポリシーによって適切な権限を付与されたIAMユーザーまたはIAMグループを設定します。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4は不正解です。SCPはOUに対してのみリソースの拒否と許可を指定するだけなので、ユーザーに直接権限を付与することはできません。SCPは組織に対してアクセス許可する点はIAMポリシーに似ていますが、ユーザー自体のリソースのアクセス許可を付与しない点が異なります。特定のEC2インスタンスの削除操作ができる開発アカウントにはSCPではなく、IAMポリシーを利用した詳細な設定が別途必要になります。

オプション３は不正解です。特定のEC2インスタンスの削除操作ができる開発アカウントに自部門のインスタンスのみを操作できるIAMロールを設定するとしており、IAMポリシーではなくIAMロールを利用しているため正しくありません。

問題30: 不正解

あなたの会社では社内データベースをRDSなどのAWSのマネージドサービスとして提供されているリレーショナルデータベースサービスに移行することにより、データセンター管理に費やしている運用管理コストを削減したいと考えています。さらに、データセンターでホストされているWEBアプリケーションに対してAWS Elastic Beanstalkを利用したバージョン管理を適用して、効率化することも検討しています。その際は、WEBサーバーを利用したアプリケーションのコアアーキテクチャは変更しないで再利用します。

この要件を満たすための最も費用対効果の高い移行方式を選択してください

- ◉ リファクタリング/リアーキテクト (不正解)
- ○ リプラットフォーム (正解)
- ○ ドロップアンドショップ
- ○ リホスト

説明

代表的な移行方式について以下の通りです。この中から、今回の要件に合致する内容はリプラットフォームになります。したがって、オプション2が正解となります。

■リプラットフォーム

リプラットフォームでは既存アプリケーションのコアアーキテクチャを変更せずにクラウドプラットフォームへと切り替えを行います。たとえば、これはAmazon Relational Database Service（RDS）などの管理されたリレーショナルデータベースサービスに移行する、またはAWS Elastic Beanstalkなどの完全に管理されたプラットフォームにアプリケーションを移行することにより、データベースインスタンスの管理に費やす時間を削減したい場合に利用されます。

したがって、今回の要件に合致しており、オプション2が正解となります。

その他の移行方式は以下の通りです。

■リホスト

リホストはビジネスケースを満たすために組織がその移行とスケーリングを迅速に実装しようとしている大規模なレガシー移行方法です。アプリケーションの大部分がリホストされます。ほとんどのリホスティングは、AWS SMSなどのツールを使用して自動化できますが、レガシーシステムをクラウドに適用する方法を学習するときに手動で行うこともできます。また、アプリケーションがクラウドで既に実行されていると、再設計が容易になることもあります。

■再購入

再購入とは移行に際して別の製品に移行する決定であり、組織が使用している既存のライセンスモデルを変更する場合に用いられます。

■リファクタリング/リアーキテクト

リファクタリングはアプリケーションの既存環境では達成することが困難な機能やスケール、またはパフォーマンスを追加する強いビジネスニーズによって推進されます。例えば全体のアーキテクチャ構成を大きく変更し、サービス指向アーキテクチャ（SOA）に移行することで俊敏性を高め、ビジネスの継続性を改善する場合などがあります。

■引退

利用することがないIT資産を識別して廃止します。継続されるリソースの維持に集中する際に利用されます。

■保持

移行準備ができていない場合にITリソースの一部を保持します。

問題31: 不正解

あなたの会社はグローバルにオフィスを展開する会計企業です。あなたは本社のAWS運用担当者として、AWS Organizations上で、AWSアカウントをメンバーアカウントに設定しました。これにより、さまざまな部門や支社が有する複数のAWSアカウントの支払いを一括管理できるようになります。アメリカ支社のソリューションアーキテクトの1人が、新しいサプライチェーンアプリケーション用に10個のリザーブドインスタンスを購入しました。これらのインスタンスはシステム構成を整備してから1カ月後に利用を開始する予定です。同社のセキュリティ要件としては、これらのリザーブドインスタンスを他の部署や支社と共有できないようにする必要があります。

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。

- ◉ リザーブドインスタンスはアカウント毎に購入されるため、アカウント内でのみ利用可能である。 (不正解)
- ○ メンバーアカウントによってリザーブドインスタンス共有設定を非有効化する。
- ○ リザーブドインスタンスのリージョン制限をアメリカ支社地域に限定することで、制限することができる。
- ○ マスターアカウントによってリザーブドインスタンス共有設定を非有効化する。 (正解)

説明

オプション4が正解となります。AWS Organizationsを利用すると、単に請求処理を統合するだけでなく、組織全体で共有してリソースを購入・利用するといったことが可能になります。それによってボリュームディスカウントが設定されているリソース料金を下げることができるため、大変有意義な仕組みです。そのため、リザーブドインスタンスをメンバーアカウントで購入すると、それらのリソースを他のアカウントとシェアすることが可能となります。

マスターアカウントはその組織のメンバーアカウントのリザーブドインスタンスのリソース共有設定をオフにすることができます。これにより、リザーブドインスタンスがそのメンバーアカウントと他のメンバーアカウント間で共有されません。ただし、リザーブドインスタンスの共有をオフにすると、統合的なボリュームディスカウントが適用されなくなるため、月額請求額が高くなる可能性があることに注意してください。

したがって、マスターアカウントによってリザーブドインスタンス共有設定を非有効化することが正解となります。

オプション1は不正解です。リザーブドインスタンスはアカウント毎に購入されるため、アカウント内でのみ利用可能という説明は間違っています。AWS Organizationsを利用するとリザーブドインスタンスはメンバーアカウント内で共有されます。

オプション2は不正解です。メンバーアカウントによってリザーブドインスタンス共有設定を非有効化するのではなく、マスターアカウントの権限操作によってリザーブドインスタンス共有設定を非有効化する必要があります。

オプション3は不正解です。リザーブドインスタンスのリージョン制限といった機能はありません。

問題32: 不正解

あなたの会社はEC2インスタンス群に対してAuto ScalingグループとALBが設定されたWebアプリケーションを利用しています。AWSのサーバレスアーキテクチャを社内で新規採用することになり、このWEBアプリケーションはサーバレスアーキテクチャに差し替えることで大幅にコストが抑えられ、かつ性能を向上させることができると判明しています。よって、これまでのWEBアプリケーションからAWS Lambda、API Gateway、およびDynamoDBで構成される新しいサーバーレスアーキテクチャへと移行することが決まりました。こうしたサーバレスアプリケーション開発を効率的に実施するためにCI / CDパイプラインを設定して、プロジェクト管理体制を整備することが要件として求められています。

AWSで新しいアーキテクチャを構築・テスト・デプロイするための最適なプロジェクト管理方法はどれですか？

- ◉ CloudFormationにより、必要となるサーバレスアーキテクチャのコンポーネントをリソースとして記述して、展開するためのテンプレートとして実行する。 (不正解)
- ○ Elastic Beanstalkにより、必要となるサーバレスアーキテクチャのコンポーネントをリソースとして記述して、展開するためのテンプレートとして実行する。
- ○ AWS サーバーレスアプリケーションモデルを利用してAWS CodeBuildとCodeDeployとCodePipelineを利用したパイプラインを作成し、AWS CodeStarによってプロジェクトを管理する。 (正解)
- ○ OpsWorksにより、必要となるサーバレスアーキテクチャのコンポーネントをリソースとして記述して、展開するためのテンプレートとして実行する。

説明

オプション３が正解となります。AWS サーバーレスアプリケーションモデルは、サーバーレスアプリケーション構築用のオープンソースフレームワークです。迅速に記述可能な構文で関数、API、データベース、イベントソースマッピングを表現できます。リソースごとにわずか数行で、任意のアプリケーションを定義してYAMLを使用してモデリングできます。AWS サーバーレスアプリケーションモデルを連携させつつ、CodeBuild、CodeDeploy、およびCodePipelineを連携することもできます。さらにAWS CodeStarを使用して、プロジェクトを生成して、集中管理された単一のダッシュボードから管理できます。AWS SAMはCodeStarとも連携しているため、CodeStar上で管理するようにCodeBuild、CodeDeploy、CodePipelineを構成することができます。

オプション１は不正解です。CloudFormation自体はサーバレスアプリケーションの展開には適していません。CloudFormationはSAMと連携して利用することが必要です。

オプション２は不正解です。Elastic Beanstalkにより、必要となるサーバレスアーキテクチャのコンポーネントをリソースとして記述して、展開するためのテンプレートとして実行することはできません。Elastic BeanstalkはWEBアプリケーションの展開や管理に活用されるサービスであり、サーバレスアプリケーション向けのサービスではありません。

オプション４は不正解です。OpsWorksにより、必要となるサーバレスアーキテクチャのコンポーネントをリソースとして記述して、展開するためのテンプレートとして実行することはできません。OpsWorksを利用するとChefなどのオープンソースのツールを利用して、インフラ展開を管理することができます。

問題33: 不正解

あなたの会社はオンラインでビジネス情報をAPI経由で取得してダッシュボードに表示するビジネスサイトを構築しています。このサイトはEC2インスタンスのWEBサーバーにホストされており、API GatewayによってAPIが作成・管理されて、データベースにはRDSを利用します。あるときAPIアクセスに対するSQLインジェクションの脆弱性によって、ポータルがアクセス不能となるインシデントが発生しました。あなたはソリューションアーキテクトとして、今後同様の問題が発生しないように改善策を検討しています。

SQLインジェクション攻撃を予防する費用対効果の高い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] VPCのネットワークACLを利用してWEBアクセスコントロールリスト（WEB ACL）をAPI Gatewayの前に設定して、悪意のあるSQLコードを予防する。 (不正解)
- [ ] AWS Shieldを利用してWEBアクセスコントロールリスト（WEB ACL）をAPI Gatewayの前に設定して、悪意のあるSQLコードを予防する。
- [ ] ファイアーウォールの構成が適切なものとなっているか保証するためAWS Configを利用して、WEBアクセスコントロールリストの変更履歴を追跡して管理できるようにする。 (正解)
- [ ] AWS WAFを利用してWEBアクセスコントロールリスト（WEB ACL）をAPI Gatewayの前に設定して、悪意のあるSQLコードを予防する。 (正解)
- [ ] AWS Systems Managerを利用して、WEBアクセスコントロールリストの変更履歴を追跡して、管理できるようにする。
- [ ] CloudTrailを利用して、APIコールのログ作成・取得する。

説明

WAFのウェブアクセスコントロールリスト(ウェブACL)を使用すると、ウェブリクエストをきめ細かく制御して、API Gateway API、CloudFrontディストリビューション、またはALBなどで応答できます。具体的には次の種類のリクエストを許可または拒否することができます。

・特定のIPアドレスまたはIPアドレス範囲が送信元である
・特定の国が送信元である
・リクエストの特定の部分が、指定した文字列を含むか、正規表現パターンと一致する
・指定した長さを超えている
・悪意のあるSQLコード(通称SQLインジェクション)が含まれている可能性がある
・悪意のあるスクリプト(通称クロスサイトスクリプト)が含まれている可能性がある

また、これらの条件の組み合わせをテストしたり、指定された条件を満たすだけでなく、5分間にわたって指定された数のリクエストを超えるウェブリクエストをブロックまたはカウントすることもできます。

したがって、オプション4が正解となります。

AWS WAF、AWS Shield アドバンスド、およびAWS Firewall Manager はAWS CloudTrailと統合されています。このサービスは、ユーザーやロール、またはAWSのサービスによって実行されたアクションを記録するサービスですが、ファイアウォール関連のルールの変更履歴を追跡するためにはAWS Configを利用します。したがって、オプション3が正解となります。

オプション1は不正解です。VPCのネットワークACLを利用してWEBアクセスコントロールリスト（WEB ACL）をAPI Gatewayの前に設定するということはできません。WAFによる設定が不可欠です。

オプション2は不正解です。AWS Shieldを利用することで、DDoS攻撃を予防することはできますが、WEBアクセスコントロールリスト（WEB ACL）ベースの対応は機能として有していません。

オプション5は不正解です。AWS Systems Managerではなく、Configを利用して、WEBアクセスコントロールリストの変更履歴を追跡して、管理できるようにする必要があります。

オプション6は不正解です。CloudTrailを利用して、すべてのAPIコールをログ作成・取得することはできるため、説明は正しいです。しかしながら、本件のSQLインジェクション攻撃への対応にはAPIコールのログは必要ありません。

問題34: 不正解

大手製造業A社は業務アプリケーションをオンプレミス環境にホストしており、このアプリケーションは頻繁にデータベースへの書き込み・読み取りを行っており、高速な処理が必要不可欠です。社内のクラウド化の方針を受けて、A社でもオンプレミスデータセンターからAWSクラウドに業務アプリケーションを移行することを決定しました。この業務アプリケーションはDB2データベースと連携することが必要ですが、社内のセキュリティ規定のために、データベースはデータセンターに残しておく必要があります。

この業務アプリケーションをAWSに移行する最適な方式を選択してください。

- ◉ AWSのVPC内にパブリックサブネットを設置して、業務アプリケーション用のサーバーとなるEC2インスタンスを起動し、データベースはRDSを同じくパブリックサブネットに設置する。Amazon DLMを利用して、mysqldumpをオンプレミス環境へと定期的にミラーリングする。 (不正解)
- ○ AWSのVPC内にパブリックサブネットを設置して、業務アプリケーション用のサーバーとなるEC2インスタンスを起動し、データベースはオンプレミス環境に残す。IPSec VPNを構成してVPCと接続する。
- ○ AWSのVPC内にパブリックサブネットを設置して、業務アプリケーション用のサーバーとなるEC2インスタンスを起動し、データベースはRDSを同じくパブリックサブネットに設置する。Amazon DatePipelineを利用して、mysqldumpをオンプレミス環境へと定期的にミラーリングする。
- ○ AWSのVPC内にパブリックサブネットを設置して、業務アプリケーション用のサーバーとなるEC2インスタンスを起動し、データベースはオンプレミス環境に残す。Direct Connectを構成してオンプレミス環境とVPCとを接続する。 (正解)

説明

オプション4が正解となります。このシナリオでの主なアーキテクチャ上の考慮事項は、データベースがクライアントのデータセンターに残るということです。データベースはクラウドでホストされるべきではないため、AWSのサブネットにデータベースを配置することはできません。したがって、AWSのVPC内にパブリックサブネットを設置して、業務アプリケーション用のサーバーとなるEC2インスタンスを起動し、データベースはオンプレミス環境に残し、Direct Connectを構成してオンプレミス環境とVPCとを接続するというのが最適なソリューションとなります。高速な処理が必要不可欠との特性を踏まえるとVPNよりもDirect Connectによる専用線接続を実施することで、ネットワークがボトルネックにならないように予防する必要があります。

オプション2は不正解です。この方式でも、アプリケーションサーバーをパブリックサブネットに配置し、データベースサーバーをクライアントのデータセンターに保持するため、要件を達成できるソリューションとなります。しかしながら、このアプリケーションは頻繁にデータベースへの書き込み・読み取りを行っており、高速な処理が必要不可欠との特性を踏まえるとVPNよりもDirect Connectによる専用線接続を実施するべきです。

オプション1と3は不正解です。データベースはRDSを同じくパブリックサブネットに設置し、mysqldumpでオンプレミス環境へと定期的にミラーリングという形式は、あくまでのバックアップや冗長構成のためのソリューションであり、オンプレミス側にデータベースを置いておくアプリ構成を実現する要件とは異なるため、正しくありません。

問題35: 正解

大手ソフトウェア企業A社はWEBアプリケーションをオンプレミス環境にホストしていましたが、AWSを利用したハイブリッド構成に移行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、クラウドおよびオンプレミス環境においてアプリケーションのインフラストラクチャの一部を管理するため、新しいハイブリッドアーキテクチャ構成を整備しています。インフラストラクチャの一部として、大量のデータを転送するために、AWSへの低レイテンシーで高い一貫性を担保するトラフィック通信が必要です。同社はコストを可能な限り低く抑えることを目指しており、通信障害が発生した場合に低速のトラフィックは問題としない方針です。

これらの要件を考慮して、ハイブリッドアーキテクチャを設計する最適なソリューションを選択してください。

- ◉ **Direct Connectを一貫した帯域幅を提供するプライマリ接続として直接接続を設定し、障害発生時用に低コストのソリューションであるVPNを設定する。** (正解)
- ○ **Direct Connectはマネージド型サービスとしてAWS側で冗長構成をとっているため、Direct Connectによる接続設定だけで障害発生時のセカンダリー接続も対応可能である。**
- ○ **低コストのソリューションであるVPNを二重に設置して冗長構成を高めることで、コスト最適化と可用性の向上を目指す。**
- ○ **Direct Connectを二重に設置して冗長構成を高めることで、コスト最適化と可用性の向上を目指す。**

説明

ハイブリッド構成でオンプレミスとVPCとを接続する際に性能を第一に考えるならばDirect Connectで決まりです。しかしながら、このケースではコストを限りなく抑えるために通信障害が発生した場合に低速のトラフィックは気にしないことが要件となっており、バックアップオプションはDirect Connectの代わりにVPN接続を使用する方が最適となります。したがって、大量のデータを転送するための高い帯域幅を提供するプライマリ接続用にDirect Connectを設定し、障害が発生した場合に低コストのソリューションであるVPNを設定するというオプション１が正解となります。

AWS Direct Connect はオンプレミスから AWS への専用ネットワーク接続の構築をシンプルにするクラウドサービスソリューションです。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提供できます

VPN接続は、インターネット経由のゲートウェイを介してオンプレミスリソースに与えられるAWSリソースへの低コストで、安全にインターネットを利用したアプライアンスベースのアクセスです。 AWS Direct Connectと比較すると、インターネットの予測不能性により、接続速度が遅くなる可能性があり、帯域幅が制限される場合があります。

オプション２は不正解です。Direct Connectによる接続設定だけでは障害発生時のセカンダリー接続には対応できないため、間違っています。実際はDirect Connectを二重に構成するなどのセカンダリーの設定が必要となります。

オプション３は不正解です。低コストのソリューションであるVPNを二重に設置して冗長構成を高めることで、コスト最適化は達成しますが、Direct Connectを利用した高速・広帯域接続より性能が劣るため、この方式は正しくありません。

オプション４は不正解です。Direct Connectを二重に設置して冗長構成を高めることで、可用性の向上されますが、これは最もコストがかかる方式です。主要な障害が発生した場合に低速のトラフィックは問題にしないで、コスト最適化を目指す要件に合致しません。

問題36: 不正解

あなたはソリューションアーキテクトとして、社内のデータセキュリティを強化するために、Webアプリケーションと基盤となるクラウドリソースに関する脆弱性を改善するように依頼されています。はじめにAWSリソースのシステム脆弱性をチェックしたところ、WEBアプリケーションへのDDoS攻撃に対する予防が取られていないことがわかりました。このWEBアプリケーションでは一連のEC2インスタンスにALBによるトラフィック処理が実施されています。

DDoS攻撃を予防するための、CloudFrontによる最適な設定方法を選択してください。（2つ選択してください。）

- [x] CloudFrontにAWS ShieldとAWS WAFを統合して利用し、WEBの不審なアクセスからの保護を実施する。 (正解)
- [x] CloudFrontを利用したコンテンツ配信設定によって、SQLインジェクションなどの攻撃を予防する。さらにCloudWatchアラームを追加して、CPU使用率とネットワークインのメトリクスを設定して異常が発生しないかモニタリングする。 (不正解)
- [ ] CloudFrontを利用したコンテンツ配信設定によって、SYNフラッドやUDPリフレクション攻撃などから保護する。さらにAWS Shield Standard を別途設定することで、広範囲にDdos攻撃から保護することが可能になる。
- [ ] Amazon Sheild Standard を利用してアプリケーション利用端末のセキュリティ認証を徹底して、登録外端末からのアクセスを監視・確認する。
- [ ] CloudFrontを利用したコンテンツ配信設定によって、SYNフラッドやUDPリフレクション攻撃などからデフォルトで保護することができる。さらにCloudWatchアラームを追加して、CPU使用率とネットワークインのメトリクスを設定して異常が発生しないかモニタリングする。 (正解)

説明

AWSではDDoS対策の一環として、WEBアプリケーションに対するファイアウォールとしてWAFを導入していきます。これによって、アプリケーションの脆弱性を悪用しようとするSQLインジェクションやCSRFなどの攻撃を防ぐことができます。WAFはALBまたはCloudFrontの両方と統合して設定することが可能です。AWS Shield アドバンスドはAWS WAFと統合することによって、レイヤー7も含めたWEBアプリケーションへの攻撃を防御をするようになっております。AWSではAWS Shield とAWS WAFの両方を設定することで、DDoS攻撃への対応をすることが推奨されています。したがって、オプション1は正解となります。

Amazon CloudFrontはデフォルトでDDoS攻撃用のAmazon Sheild Standardが適用されており、Webアプリケーションを保護できます。これによりSYNフラッドやUDPリフレクション攻撃などの多くの一般的なDDoS攻撃がオリジンに到達するのを防ぎます。また、Amazon CloudWatchアラームを追加してこうした攻撃による影響発生をモニタリングしつつ、Auto Scalingを開始するために使用することができます。したがって、オプション5は正解となります。

オプション2は不正解です。CloudFront単独ではSQLインジェクションなどの攻撃を予防することはできないため、別途設定するWAFによって防ぐ必要があります。

オプション3と4は不正解です。CloudFrontを使うことで追加料金なくAWS Shield Standardが自動で適用されます。SSL(https)にも対応しており安全なコンテンツを訪問者へ届けられます。したがって、CloudFrontを設定することでAWS Shield Standardを別途設定することは正しくありません。

問題37: 正解

ある会社では本番環境、開発環境およびテスト環境を用意して、大規模にAWS上での開発を行っています。これらの環境は複数のAWSサービスと数十にも及ぶEC2インスタンスが利用される大規模なインフラ構成となっています。そのため、多数のOSにパッチ適用管理を実施することが必要となり、あなたはAWS Systems Managerサービスを利用した適用方法を検討しているところです。EC2インスタンスのOSにパッチを適用するためには、適用前に各環境の異なるベースラインとなるパッチ要件に合致しているかを検証することが必要です。

AWS Systems Managerサービスを利用したパッチ適用の設定方法を選択してください。

- (●) OS環境に応じたEC2インスタンスのタグ設定を実施し、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成する。EC2インスタンスをパッチグループで分類して、パッチベースラインを適用する。 (正解)
- ( ) OS環境に応じたEC2インスタンスのリソースネーム設定を実施し、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成する。EC2インスタンスをプレイスメントグループで分類して、パッチベースラインを適用する。
- ( ) OS環境に応じたEC2インスタンスのタグ設定を実施し、AWS Patch Managementを利用してパッチベースラインを各環境に対して作成する。EC2インスタンスをパッチグループで分類して、パッチベースラインを適用する。
- ( ) OS環境に応じたEC2インスタンスのリソースネーム設定を実施し、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成する。EC2インスタンスをパッチグループで分類して、パッチベースラインを適用する。
- ( ) OS環境に応じたEC2インスタンスのリソースネーム設定を実施し、AWS Patch Managementを利用してパッチベースラインを各環境に対して作成する。EC2インスタンスをプレイスメントグループで分類して、パッチベースラインを適用する。

説明

オプション1は正解となります。OS環境に応じてEC2インスタンスに対してタグを設定し、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成して、EC2インスタンスをパッチグループで分類した上で、パッチベースラインを適用します。これによって、要件に合致したパッチ適用プロセスを整備することができます。

AWS Systems Manager Patch Managerは、セキュリティ関連のアップデートと他のタイプのアップデートの両方でマネージドインスタンスにパッチを適用するプロセスを自動化します。Patch Managerを使用して、オペレーティングシステムとアプリケーションの両方にパッチを適用することができます。

Patch Managerのパッチベースラインには、リリースから数日以内にパッチを自動承認するためのルールと、承認済みパッチおよび拒否済みパッチのリストが含まれています。パッチ適用をSystems Managerのメンテナンスウィンドウタスクとして実行するようにスケジュールすることで、パッチを定期的にインストールできます。また、パッチはEC2インスタンスのタグを使用して個別のインスタンスまたは大規模なグループのインスタンスに分類してインストールできます。作成または更新するときに、タグをパッチベースライン自体に追加できます。

オプション2は不正解です。OS環境に応じたEC2インスタンスのリソースネーム設定ではなく、タグ設定を実施することが必要です。また、AWS Systems Manager Patch Managerを利用する際は、EC2インスタンスをプレイスメントグループで分類するのではなく、パッチグループによってパッチベースラインを適用する必要があります。

オプション3は不正解です。AWS Patch Managementではなく、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成することが必要です。

オプション4は不正解です。OS環境に応じたEC2インスタンスのリソースネーム設定ではなく、タグ設定を実施することが必要です。

オプション5は不正解です。OS環境に応じたEC2インスタンスのリソースネーム設定ではなく、タグ設定を実施することが必要です。AWS Patch Managementではなく、AWS Systems Manager Patch Managerを利用してパッチベースラインを各環境に対して作成することが必要です。

問題38: 正解

あなたの会社はクラウド化のトレンドを受けてオンプレミスのデータセンターからAWSにデータベースを移行することを決定しました。あなたはソリューションアーキテクトとして、データセンター内にあるアプリケーションを順次AWSへと移行する作業を担当しています。とあるアプリケーションでは、オンプレミスのOracleデータベースをPostgreSQLに変換して移行することが決まりました。データを正常に移行するには、最初にスキーマとコードの変換を行う必要があります。

この移行要件に合致した最適なデータベース移行方式を選択してください。

- (◉) AWS Schema Conversion Toolを使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Database Migration Serviceを使用してOracleデータベースからRDS PosgreSQLデータベースへとデータ移行する。 (正解)
- ( ) AWS Migration Hub使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Migration Toolを使用してOracleデータベースからRDS PosgreSQLデータベースへとデータ移行する。
- ( ) AWS Migration Hubを使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Database Migration Serviceを使用してOracleデータベースからRDS PosgreSQLデータベースへとデータ移行する。
- ( ) AWS Database Migration Service使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Migration Toolを使用してOracleデータベースからRDS PosgreSQLデータベースへとデータ移行する。

解説

オプション1が正解となります。AWS Schema Conversion Toolを使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Database Migration Serviceを使用してOracleデータベースからRDS PosgreSQLデータベースへとデータ移行することができます。

AWS Database Migration Service を使用すると、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。AWS DMS ではOracle から Oracle のような同種のデータベース間の移行も、Oracle または Microsoft SQL から Amazon Aurora といった異なるデータベースプラットフォーム間の移行もサポートされます。データを高可用性を維持しつつ継続的にレプリケートし、Amazon Redshift と Amazon S3 にデータをストリーミングすることで、データベースをペタバイト規模のデータウェアハウスに統合できます。

AWS Database Migration Service の実施プロセスは以下の通りです。

■AWS Schema Conversion Toolを使用してソーススキーマとコードをターゲットデータベースのそれに一致するように変換し、次にAWS Database Migration Serviceを使用して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移行します。

■必要なデータ型の変換はすべて、移行中にAWS Database Migration Serviceによって自動的に行われます。

■ソースデータベースは、Amazon EC2インスタンスで実行されているAWS以外の独自の施設に配置することも、Amazon RDSデータベースにすることもできます。

■ターゲットは、Amazon EC2またはAmazon RDSのデータベースに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と3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。今回の目的とは異なるため不正解です。

オプション4は不正解です。AWS Migration Toolというサービスは存在しないツールです。AWS Schema Conversion Toolを使用して移行を進めることが必要です。

問題39: 不正解

あるアプリ開発企業はAWSを利用した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では複数のモバイルデバイスを使用してアクセスするユーザーに対して、ユーザー認証データをAWS上に保存して、複数デバイスからの認証を可能にする仕組みを実装することになりました。各ユーザーの設定データサイズが70KBほどであり、既存アプリケーションを利用する30万人のユーザーが、この新しいモバイルアプリケーションを利用することが想定されています。また、ユーザー認証を容易にするためにソ・シャルログインアカウントを使用することも要件となっています。

これらの要件に対応する最適で安全なモバイル認証ソリューションを選択してください。

- ◉ モバイルアプリが直接参照・登録するユーザーの設定データ用のS3バケットを作成する。次にSTSとウェブIDフェデレーションとS3のネットワークACLによるモバイル認証を実施する。 (不正解)
- ○ モバイルアプリが直接参照・登録するユーザーの設定データ用のDynamoDBテーブルを作成する。それに対して、Amazon Cognitoによるモバイル認証を実施する。
- ○ モバイルアプリが直接参照・登録するユーザーの設定データ用のDynamoDBテーブルを作成する。次にSTSとウェブIDフェデレーションとDynamoDBのFGAC（Fine Grained Access Control）によるモバイル認証を実施する。 (正解)
- ○ モバイルアプリが直接参照・登録するユーザーの設定データ用のS3バケットを作成する。次にAmazon CognitoとS3のネットワークACLによるモバイル認証を実施する。

説明

このシナリオでは、30万人分のユーザー設定データをAWS上に保存して、ソーシャルログインによるモバイル認証を実現することが要件となっています。AWSでソーシャルログインの使用するにはウェブIDフェデレーションを利用します。ウェブ ID フェデレーションを使用すると、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はありません。ウェブ ID フェデレーションではよくFacebookなどの知られている外部 ID プロバイダー (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。

ユーザー認証データをDynamoDBテーブルに保存することで、強固なセキュリティによる高速な認証処理を実現することが可能です。DynamoDBテーブルのFGAC (Fine Grained Access Control) は DynamoDBがセキュリティ、アクセス制限を実現する仕組みで、これにより、ソーシャルログイン対応とあわせて、モバイルユーザが直接DynamoDBを利用することが可能となります。したがって、オプション３が正解となります。

FGAC（Fine Grained Access Control）とは、DynamoDB テーブルの所有者がテーブル内のデータに対して詳細なコントロールを行うための機能です。具体的には、テーブル所有者は誰（呼び出し元）がテーブルのどの項目や属性にアクセスでき、どのようなアクション（読み込み/書き込み）を実行できるかを指定できます。FGAC はIAMと組み合わせて使用されます。セキュリティ認証情報および対応するアクセス権限の管理は、IAM で行います。

オプション１は不正解です。STSとネットワークACLの組み合わせでモバイル認証を実施する機能はありません。

オプション２は不正解です。Amazon Cognito を使用すれば、Google、Facebook、Amazon などのソーシャル ID プロバイダーや、SAML による Microsoft Active Directory などのエンタープライズ ID プロバイダーを通してサインインすることができますが、DynamoDBテーブルによる認証情報の提供する仕組みとしてのFGACが設定されておらず、今回の要件には利用できません。

オプション４は不正解です。モバイルアプリが直接参照・登録するユーザーの設定データについては、クエリ処理によるデータ確認が必要です。このようなセッションデータ管理はS3ではなくDynamoDBの適しているユースケースとなっています。また次にAmazon CognitoとS3のネットワークACLによるモバイル認証というのも組合せとして不明です。ネットワークACLをモバイル認証に利用することはありません。

問題40: 正解

あなたは大手ソフトウェア会社においてソリューションアーキテクトとして勤務しています。このソフトウェア会社では人材マッチングオンラインポータルを運用しており、このポータルは毎日のトランザクション量が多いため、その監視・運用があなたの主な仕事になっています。最近になって、会社はEC2インスタンスとRDS MySQLインスタンスを使用して新しいポータルをデプロイすることを決定しました。そこで、あなたはアプリケーションおよびデータベースサーバーに障害が発生した場合でも利用が継続できるように、OpsWorksを利用した展開方式を設定しています。

OpsWorksを利用してポータルサイトのダウンタイムや新サイトの不具合の影響を最小限にした、展開方式を選択してください。

- (◉) OpsWorksにより、EC2インスタンスにAutoScalingとELBターゲットグループを設定して、マルチAZ構成によりオンラインポータルを展開し、同様にRDSもマルチAZ構成で展開する。その際にブルーグリーン展開戦略を利用しつつ、OpsWorksの自動ヒーリングを有効化する。 (正解)
- ( ) OpsWorksにより、EC2インスタンスにAutoScalingとELBターゲットグループを設定して、マルチAZ構成によりオンラインポータルを展開し、同様にRDSもマルチAZ構成で展開する。その際にブルーグリーン展開戦略を利用しつつ、CloudWatchモニタリングによってAutoScalingを起動する設定を行う。
- ( ) OpsWorksにより、EC2インスタンスにAutoScalingとELBターゲットグループを設定して、マルチAZ構成によりオンラインポータルを展開し、RDSはリードレプリカを利用して展開する。その際にローリングデプロイ戦略を利用しつつ、OpsWorksの自動ヒーリングを有効化する。
- ( ) OpsWorksにより、EC2インスタンスにAutoScalingとELBターゲットグループを設定して、マルチAZ構成によりオンラインポータルを展開し、RDSはマルチAZ構成に加えてリードレプリカを利用して展開する。その際にローリングデプロイ戦略を利用しつつ、CloudWatchイベントによって異常発生時のスケーリングを自動化する。

説明

このシナリオでは、OpsWorksを利用したデプロイ構成によって、オンラインポータルの可用性を確保することが主な優先事項です。アプリケーションサーバーとデータベースサーバーは、OpsWorksスタックの自動ヒーリングとRDS Multi-AZ構成を使用して高可用性を実現する必要があります。またOpsWorksのデプロイ戦略としては、Blue-Green Deployment 戦略を利用することで、デプロイに失敗したときの影響を最小限に抑えることが可能です。したがって、オプション1が正解となります。

OpsWorksの自動ヒーリングは、インスタンスが Amazon EC2 ヘルスチェックに合格した場合でも、スタック内にある異常なインスタンスまたは失敗したインスタンスを再起動します。スタックのレイヤー設定では、自動ヒーリングがデフォルトで有効化されています。自動ヒーリングが有効になっている場合、ポータルのダウンタイムを回避するために、失敗したEC2インスタンスは自動的に置き換えられます。

Blue-Green Deployment 戦略では稼働中のインフラ構成をブルーとして、新しい構成をグリーンとして並列で移行を進める方式です。動作確認が問題なければ新しいアプリケーションに切り替えますが、問題があった場合は既存のアプリケーションを継続して、展開をロールバックします。

オプション2は不正解です。OpsWorksスタックの自動ヒーリングとRDS Multi-AZ展開を使用して高可用性を実現することが求められており、CloudWatchモニタリングによってAutoScalingを起動する設定を行うだけでは不十分です。OpsWorksの自動ヒーリングなどの構成も必要となります。

オプション3と4は不正解です。ローリングデプロイは本番サーバーに段階的に切り替える移行方式です。短時間に実施が可能となりますが、問題があった場合の影響が大きくなります。一時的に新旧サイトが混在することで、OpsWorksを利用してポータルサイトのダウンタイムや新サイトの不具合の影響が多少なり発生することになります。この方式ではブルーグリーンデプロイメントに比較すると最小限に抑えることができていないため、ブルーグリーンデプロイメントの方が適切な戦略となります。