問題31: 不正解

フィンテック企業A社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。既存のいくつかのデータベースを高速処理が可能なAWSサービスに移行する作業が必要です。その際は、オンプレミス環境のアプリケーションからAWSリソースへとアクセスするための認証方式を実装することが必要となります。社内ではSAML 2.0をサポートしていないID認証システムによってユーザー管理を実施しており、この仕組みを今後も活用していく方針です。

これらの要件を考慮して、オンプレミス環境ユーザーにAWSリソースへの一時認証を付与するソリューションを選択してください。（2つ選択してください。）

- [x] AD Connectorを利用して、ユーザーを認証するためのカスタムIDブローカーを作成し、AssumeRole APIを利用して一時的なロールを取得してAWSリソースにアクセスする。 (不正解)
- [x] Amazon Congitoを利用して、ユーザーを認証するためのカスタムIDブローカーを作成し、AssumeRole APIを利用して一時的なアクセス認証情報を取得し、AWSリソースにアクセスする。 (不正解)
- [ ] 既存の資格情報を使用してユーザーを認証するためのカスタムIDブローカーアプリケーションを作成し、AssumeRole APIによって一時的なロールを取得してAWSリソースにアクセスする。 (正解)
- [ ] 既存の認証情報を使用してユーザーを認証するためのカスタムIDブローカーアプリケーションを作成し、GetFederationTokenによってSTSから一時的なアクセス認証情報を取得し、AWSリソースにアクセスする。 (正解)

説明

AWS Security Token Service (AWS STS) を使用して、AWS リソースへのアクセスをコントロールできる一時的セキュリティ認証情報をユーザーに提供することができます。さらに、このユーザーを認証するためのカスタムIDブローカーを作成し、認証手続きを進めることができます。

AssumeRoleは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のセットを返します。これらの一時的な資格情報は、アクセスキーID、シークレットアクセスキー、およびセキュリティトークンで構成されます。通常、AssumeRoleはアカウント内またはクロスアカウントアクセスに使用します。したがって、オプション3が正解となります。

GetFederationTokenはフェデレーションユーザーの一連の一時的なセキュリティ資格情報（アクセスキーID、シークレットアクセスキー、およびセキュリティトークンで構成される）を返します。IAMユーザーの長期的なセキュリティ認証情報を使用してGetFederationTokenオペレーションを呼び出す必要があります。その結果、この呼び出しにより、サーバーベースのアプリケーションにおいて資格情報を安全に保存することができます。したがって、オプション4も正解となります。

AD ConnectorとAmazon Congitoの組合せではユーザーを認証するためのカスタムIDブローカーを作成し、認証手続きを進めると設定ができないため、オプション1と2は不正解です。

ある金融機関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。現在AWSでは複数のEC２インスタンスをVPCのプライベートサブネットに構成しています。あなたは移行担当者として、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 接続を確立する対応を行っています。 Direct Connectリンクを設定してルートをオンプレミス環境に接続しましたが、これを有効化するための設定が別途必要です。

Direct Connectリンクのルートを確立するための最適な設定を選択してください。（2つ選択してください。）

- [x] 仮想プライベートゲートウェイ（VGW）への「ルート伝播（Route Propagation）」を設定する （正解）
- [ ] カスタマーゲートウェイ（CGW）への「ルート伝播（Route Propagation）」を設定する
- [ ] オンプレミス環境への返信ルートを追加することで、EC2インスタンスが設置されているVPCのプライベートサブネットにあるルートテーブルを更新する。 （正解）
- [ ] IPSec VPNへの「ルート伝播（Route Propagation）」を設定する
- [ ] Direct Connectがリンクされ ているVPCのルートテーブルを更新して、オンプレミス環境に設定されたカスタマーゲートウェイへの返信ルートを追加する。

説明

オプション１は正解となります。仮想プライベートゲートウェイ（VGW）は接続のAWS側にある接続機器です。Direct Connectを機能させるにはVGWでのルート伝播を有効にする必要があります。

オプション３は正解となります。EC2インスタンスがオンプレミス環境と通信できるようにルートテーブルを更新する必要があります。そのためには、AWS環境から顧客のオンプレミス環境へとトラフィックが戻るルートを追加しEC2インスタンスがホストされているサブネットのルートテーブルを変更します。

オプション２は不正解です。カスタマーゲートウェイ（CGW）ではなくて、仮想プライベートゲートウェイ（VGW）への「ルート伝播（Route Propagation）」を有効化する必要があるため、オプション２は正しくありません。

オプション４は不正解です。VPNのオプションを追加する必要はないため、オプション4は正しくありません。

オプション５は不正解です。Direct Connectがリンクされ ているVPCのルートテーブルを更新して、オンプレミス環境への返信ルートを追加するのではなく、VPCのプライベートサブネットに対してルートを設定することで、プライベートネットワーク間のアクセスを構成することが適切な設定方式となっています。

大手ECサービスを運営しているA社は自社のEコマースサイトをAWSにホストしています。このサイトは3つのアベイラビリティーゾーンに展開しているオンデマンドEC2インスタンスとALBで構成されます。最近になって、利用者の増加によって、ECサイトのピーク時に処理落ちが発生することがあり、ユーザーからのクレームが多発しています。したがって、あなたはソリューションアーキテクトとして、現在のアーキテクチャの改善を依頼されました。要件としては、負荷のピーク時にはマルチAZに負荷を分散してオートスケーリング処理ができる必要があります。その際にはスポットインスタンスを上手く利用して、コスト最適に実現することが必要です。

このシナリオにおいて、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。

- (◉) スポットフリートを利用した割り当て戦略を実施して、オンデマンドEC2インスタンスの代わりにリザーブドインスタンスを構成してAuto Scalingを設定し、各AZでピークロードを処理できるように設定する。平常時には現在の構成を維持する。 (不正解)
- ( ) 複数AZに対してEC2インスタンスのスポットインスタンスを起動できるようにAuto Scalingを設定して、ピークロードを割り当てて、常にスケーリングされている状態を維持する。
- ( ) EC2インスタンスのリザーブドインスタンスに設定されているALBをターゲットとしたAuto Scalingを設定して、ピークロードを処理できるように設定する。平常時には現在の構成を維持する。
- ( ) スポットフリートを利用した割り当て戦略を実施して、Auto Scalingを設定する。これにより、ピーク時にはAZにまたがってピークロードを処理できるように設定する。 (正解)

説明

今回のシナリオでは、負荷のピーク時にマルチAZに展開したインスタンスで分散してオートスケール処理ができる必要があります。その際は、スポットインスタンスを上手く利用してコスト最適に実現することが要件となっています。これに対して、スポットフリートを設定することで、あらかじめ入札価格とインスタンスタイプとAvailability Zoneを設定しておくことで、一番安いスポットインスタンスを最適な価格で取得できるように自動で調整出来るようになります。

スポットフリートは、スポットインスタンスのコレクションです。スポットフリートは、スポットフリートリクエストで指定した容量ターゲットを満たすようなスポットインスタンスとオンデマンドインスタンスを起動しようと構成します。スポットインスタンスへのリクエストは利用可能な容量があり、リクエストで指定した上限料金がスポット料金を超えている場合に実施されます。また、スポットインスタンスが中断した場合、スポットフリートはターゲット容量フリートを維持しようとします。

リザーブドインスタンスは定常処理を長期間にわたって使用する場合に有効な購入オプションであり、コスト最適にかつスポットフリートで対処するためには不適切なオプションです。したがって、オプション1と3は不正解です。

オプション2も不正解です。複数AZにまたがってEC2インスタンスのスポットインスタンスを起動できるようにAuto Scalingを設定して、ピークロードを割り当てて、常にスケーリングされている状態を維持することで、負荷分散は達成可能ですが、コスト最適を自動で達成するという要件にはスポットフリートを構成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、大手商社の事業継続性計画（BCP）の実行対応に携わっています。この会社のBCPガイドラインでは障害復旧時間（RTO）は1時間で、目標復旧時点（RPO）は15分前とされています。このBCPに準拠するために、例えば災害が発生したことで停電などが発生し、午後2時にサーバーが停止した場合において推定される障害復旧時間とデータ損失はどうなるでしょうか。

このシナリオにおいて想定される障害復旧時点とデータ損失範囲のセットとして正しい回答を選択してください。

- ◉ 障害復旧時点は1:30 データ損失範囲は1:45-2:00 (不正解)
- ○ 障害復旧時点は1:45 データ損失範囲は1:45-2:00 (正解)
- ○ 障害復旧時点は2:00 データ損失範囲は1:45-2:00
- ○ 障害復旧時点は2:00 データ損失範囲は2:00-2:15

説明

このシナリオでは、RPOは15分であるため、システムは午後1時45分までにシステムにあったすべてのデータを回復する必要があります。許容されるデータ損失は、午後1時45分から午後2時までです。これを覚えておくための簡単な公式は、災害発生時間からRPOの値を差し引くことで算出できます。したがって、正しい答えはオプション2です。

会社は社内の業務システムをEC2インスタンスとELBとDynamoDBを使用して構築しています。DynamoDBの設定時にUser_IDの主キーを持つTRANSACTIONSというテーブルを作成し、問題なく、IDの主キーに基づいてデータを照会できるように構成しました。このDynamoDBテーブルを利用して、ユーザーのアクセス頻度に応じて顧客をセグメンテーションした上で、その利用データを集計する機能が必要となります。その際にはUser_IDというパーティションキーに関連付けて絞り込み検索をすることが求められています。

上記の要件を満たすためにDynamoDBテーブルの構成方法を選択してください。

- ◉ **利用頻度をローカルセカンダリーインデックスとして利用するTRANSACTIONSテーブルを再構成する。** (正解)
- ○ **利用頻度をグローバルセカンダリーインデックスとして利用するTRANSACTIONSテーブルを構成する。**
- ○ **利用頻度をローカルセカンダリーインデックスとしてTRANSACTIONSテーブルに追加する。**
- ○ **利用頻度をグローバルセカンダリーインデックスとしてTRANSACTIONSテーブルに追加する。**

説明

オプション１が正解となります。利用頻度をローカルセカンダリーインデックスとして利用するTRANSACTIONSテーブルを構成することで、Webアプリケーションが利用頻度によってTRANSACTIONSテーブルを照会できるようになります。

テーブル内のデータに効率的にアクセスするため、DynamoDB はPrimary Key属性用にインデックスを作成することができます。アプリケーションはPrimary Key値を指定することで、迅速にデータを取得することができます。しかしながら、Primary Key値だけでは効率的に検索できないケースがあります。そのため、多くのアプリケーションでは、Primary Key以外の属性を使って、データに効率的にアクセスできるようにするセカンダリキーを１つ以上設定して検索性を向上させることができます。１つのテーブルで１つ以上のセカンダリインデックスを作成して、それらのインデックスに対してクエリリクエストを実行することができます。

DynamoDBではグローバルとローカルのセカンダリインデックスはどちらも、クエリの柔軟性を向上させます。ローカルセカンダリインデックスが特定のパーティションキーの値に関連付けられるのに対して、グローバルセカンダリインデックスはすべてのパーティションキーの値が対象となります。ローカルセカンダリインデックスの目的は、パーティションキーの値が同じで、ソートキーの値が異なる項目に対してクエリを実行することです。

今回はUser_IDというパーティションキーに関連付けて絞り込み検索をすることが求められているため、グローバルセカンダリインデックスではなく、ローカルセカンダリインデックスを設定することが必要です。また、ローカルセカンダリーインデックスはテーブルの作成時に設定する必要があり、既存のテーブルには追加することができません。したがって、オプション１の設定が正しい内容となります。

Amazon DynamoDB では、次の２種類のセカンダリインデックスをサポートしています。

■グローバルセカンダリインデックス

[illegible]。ベーステーブルのものとは異なる場合があります。グローバルセカンダリインデックスは、このインデックスに関するクエリが、すべてのパーティションにまたがり、ベーステーブル内のすべてのデータを対象とする可能性があるため、「グローバル」と見なされます。グローバルセカンダリインデックスにはサイズの制限はなく、読み込みアクティビティと書き込みアクティビティ用にプロビジョニングされた独自のスループット設定が、テーブルのものとは異なります。

■ローカルセカンダリインデックス

パーティションキーはベーステーブルと同じですが、ソートキーが異なるインデックスです。ローカルセカンダリインデックスは、ローカルセカンダリインデックスのすべてのパーティションの範囲が、同じパーティションキー値を持つベーステーブルのパーティションに限定されるという意味で「ローカル」です。その結果、任意の１つのパーティションキー値に対してインデックスが作成された項目の合計サイズが、10 GB を超えることはできません。また、ローカルセカンダリインデックスでは、読み込みアクティビティおよび書き込みアクティビティのプロビジョニングされたスループット設定が、インデックス作成中のテーブルと共有されます。

オプション２と４は不正解です。利用頻度をグローバルインデックスとして利用するのは間違いです。グローバルセカンダリインデックスは全てのパーティションキーに紐づいて（全ての＝であるためグローバル）検索値を追加することができます。したがって、検索要件に合致しません。

オプション３は不正解です。ローカルセカンダリーインデックスはテーブル作成時に設定する必要があり、既存のテーブルには追加することができません。

問題36: 不正解

ある会社では企業のアプリケーションログファイルから定期的な分析レポートを作成する監査用ログシステムを運用しています。すべてのログデータはAmazon S3バケットに収集され、その後、毎日のAmazon EMRのジョブによって分析が実行されます。その際は、日次レポートと集計テーブルをCSV形式で生成し、別のS3バケットに保存してから、Amazon Redshiftのデータウェアハウスに転送します。分析用データの使用頻度は不確実で、データ管理のライフサイクルポリシーをうまく設定できません。このシステムは今後も長期継続して利用することになるため、あなたはパフォーマンスやデータ整合性を損なうことなくコストを削減するよう依頼されました。

この要件を満たして、コストを削減する方法として最適なオプションはどれでしょうか。（3つ選択してください。）

- [x] Redshift向けにはオンデマンドインスタンスを利用する (不正解)
- [ ] Redshift向けにはリザーブドインスタンスを利用する (正解)
- [ ] EMRのコアノードとマスターノードにリザーブドインスタンスを利用して、タスクノードにはスポットインスタンスを設定する。 (正解)
- [ ] Amazon S3 Intelligent Tieringをストレージクラスとして選択する。 (正解)
- [ ] Amazon S3 Glacier（迅速）をストレージクラスとして選択する。
- [ ] EMRのコアノードにリザーブドインスタンスを利用して、マスターノードとタスクノードにはスポットインスタンスを設定する。

説明

オプション2は正解となります。RedshiftはDWHとして起動しており、一時的なデータ処理ではなく中長期利用となるため、オンデマンドインスタンスではなくリザーブドインスタンスを利用することでコスト削減を実現します。問題文に今後も継続して利用することになるため、とあり、一時的な利用ではないことが読み取れるようになっています。また目的も監査用の分析レポートです。監査用となるため1年単位で必要となることが理解できます。

オプション3は正解となります。EMRはノード別にインスタンスを設定することができます。マスターノードやコアノードにはリザーブドインスタンスを利用して、ジョブに割り当てられるタスクノードにはスポットインスタンスを使用することが望ましいです。リザーブドインスタンスとスポットインスタンスの組み合わせにより平均パフォーマンスが保証され、コストが削減さます。

オプション4は正解となります。S3 Intelligent-Tieringストレージクラスは、アクセス頻度の予測不能なデータに対してパフォーマンスへの影響や運用オーバーヘッドなしで、データを最も費用対効果の高いアクセス層に自動的に移動することにより、コストを最適化するため、コスト最適化に役立ちます。1つの層は頻繁なアクセス用に最適化され、もう1つの層は低頻度のアクセス用に最適化されます。

オプション1は不正解です。Redshiftは中長期利用されうるDWHとして起動しているためオンデマンドインスタンスではなくリザーブドインスタンスを利用することでコスト削減を実現します。

オプション5は不正解です。S3 Intelligent-Tieringストレージクラスを利用することでコスト最適を達成します。Amazon S3 Glacier（迅速）はデータ取り出しに数分かかるため、データ処理に支障をきたします。

オプション6は不正解です。EMRジョブを管理するマスターノードやコアノードに対してスポットインスタンスのみがデータ処理に使用される場合、AWSによってスポットインスタンスがいつでも中断される可能性があるため、間違っています。このセットアップは最も費用対効果が高いですが、システムパフォーマンスに影響を与えかねないため、受け入れられません。

Amazon EMR の中心的なコンポーネントはクラスターです。クラスターとは、Amazon Elastic Compute Cloud (Amazon EC2) インスタンスのコレクションのことです。クラスター内の各インスタンスは、ノードと呼ばれます。各ノードには、クラスター内での役割があり、ノードタイプと呼ばれます。Amazon EMR は、各ノードタイプにさまざまなソフトウェアコンポーネントもインストールし、Apache Hadoop などの分散型アプリケーションでの役割を各ノードに付与します。

Amazon EMR のノードタイプは、次のとおりです。

マスターノード: 処理を行うために他のノード間でのデータおよびタスクの分散を調整するソフトウェアコンポーネントを実行することで、クラスターを管理するノードです。マスターノードはタスクのステータスを追跡し、クラスターの状態を監視します。すべてのクラスターにはマスターノードがあり、マスターノードのみで1つのノードクラスターを作成することができます。

コアノード: タスクを実行し、クラスター上の Hadoop Distributed File System (HDFS) にデータを保存するソフトウェアコンポーネントを持つノードです。マルチノードクラスターには、少なくとも1つのコアノードがあります。

タスクノード: タスクを実行するのみで、HDFS にデータを保存しないソフトウェアコンポーネントを持つノードです。タスクノードはオプションです。

あなたの会社では複数部門と支社でAWSサービスを利用しています。部門ごとにAWSアカウントを作成しており、各アカウントは、その特定アカウントのみにルートアクセス権を持つシステム管理者によって管理されています。あなたはセキュリティ責任者から、全社統一でAWSアカウントを統合することで内部統制を強化しつつ、コスト削減を行うように依頼されました。個々のアカウントまたはアカウントのグループに対して特定のAWSサービスを許可または拒否することにより、複数のAWSアカウントを集中管理する必要があります。

この要件を満たすことができる、効率的かつ最適な方法となるオプションはどれでしょうか。（2つ選択してください。）

- [x] AWS Organizationsを利用して、組織単位（OU）を作成して各部門にOUを設定する。サービス管理ポリシー（SCP）をアタッチして各メンバーアカウントが利用するAWSサービスリストの拒否・許可設定を実施する。 (正解)
- [ ] AWS Organizationsを利用して、組織単位（OU）を作成して各部門にOUを設定する。その上で、IAMポリシーをOUに設定して、各メンバーアカウントが利用するAWSサービスの拒否・許可設定を実施する。
- [ ] AWS Organizationsを利用して、クロスアカウントアクセス設定を実施する。
- [ ] OU内のアカウントのユーザーまたはロールに対してIAMポリシーを追加して、ユーザーレベルでのアクセス権限を付与する (正解)
- [ ] AWS Organizationsを利用して、IDフェデレーション機能を作成して各メンバーアカウントとOUを結びつける。

説明

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。 したがって、オプション 1 が正解となります。

SCP は必要ですが、アカウント内の個別のユーザー毎のアクセス権限設定には不十分です。組織のルートあるいは組織単位 (OU) に SCP をアタッチすると、組織ルートあるいは OU 内のアカウントがどのアクションを行うことができるかのガードレールを定義します。さらに、組織内のアカウントのユーザーまたはロールに [IAM ポリシー] を追加して、実際にアクセス権限を付与する必要があります。上述のアカウントに 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。したがって、オプション 4 が正解となります。

IAMポリシーをOUに設定することはできないため、オプション 2 は不正解です。

AWS Organizationsを利用して、クロスアカウントアクセス設定を実施すると、異なるアカウントのユーザーが、別のアカウントのリソースへとアクセスする設定ができます。本件の要件とは用途が異なるため、オプション 3 は不正解です。

オプション 5 は不正解です。AWS Organizationsを利用して、IDフェデレーション機能を作成して各メンバーアカウントとOUを結びつけるといった設定はありません。

39

あなたの会社は個人がいらなくなった物品を売り買いできるC to C専門のモバイルフリマサイトをAWSに構築しています。このモバイルフリマサイトでは、複数のAWSリージョン上にバックエンドAPIを起動しており、ユーザーに最も近いリージョンで販売および取引が処理されるようにルーティングされています。このアプリケーションを東京リージョンから東南アジアにも展開することになり、トランザクションがシンガポールリージョンにも自動的に複製されるようにレプリケーション構成を実現することが必要です。

次のうち、この要件を達成できるDynamoDBでの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] 東京リージョン内のDynamoDBテーブルのStreamsを有効化する。DynamoDBテーブルをシンガポールリージョン内にも作成する。 (正解)
- [ ] DynamoDBを作成して、マルチリージョン構成となる設定を行う。各リージョン内のトランザクション処理おける個別のトランザクション処理結果がレプリケーションされるように設定する。
- [ ] DynamoDBのグローバルテーブルをシンガポールリージョンにも作成して、レプリケーション自動化を有効化する。それによって、各リージョン内のトランザクション処理おける個別のトランザクション処理結果がレプリケーションされる。
- [ ] 該当する全てのリージョンに作成されたDynamoDBテーブルに対してグローバルテーブルを設定することで、これらのDynamoDBテーブル間のデータ変更を自動的にレプリケートする。 (正解)

説明
東京リージョンで行われたトランザクション処理がシンガポールリージョンにも自動的に複製するような設定するには、DynamoDB Streamsを有効化します。その上で、該当するシンガポールリージョンにも同じテーブルを作成します。さらに、該当する全てのリージョンに作成されたDynamoDBテーブルに対してグローバルテーブルを設定することで、これらのDynamoDBテーブル間のデータ変更を自動的にレプリケートするように構成します。したがって、オプション１と４が正解となります。

Amazon DynamoDB グローバルテーブルは、マルチリージョンにマルチマスターデータベースをデプロイするための完全マネージド型のソリューションです。独自のレプリケーションソリューションを構築および管理する必要はありません。グローバルテーブルを作成する際、そのテーブルの利用を許可する AWS リージョンを指定します。DynamoDB は、これらのリージョンに同一のテーブルを作成するのに必要なすべてのタスクを実行し、変更中のデータをすべてのテーブルに伝達します。

オプション2は不正解です。DynamoDBにはマルチリージョン構成という設定はありません。

オプション3は不正解です。DynamoDBのグローバルテーブルをシンガポールリージョンにも作成して、レプリケーション自動化を有効化するといった設定はありません。

大手ITソリューション企業A社ではAWS Organizationsを使用して複数の組織単位（OU）にグループ化されたさまざまなAWSアカウントを有しています。年度ITセキュリティ監査を実施したところ、一部のメンバーアカウント内において、許可されていないサードパーティのユーザーアカウントが作成されていました。該当アカウントの責任者からは、サードパーティーとのAPI連携を実施する際に必要な対応であり、問題のないものと確認されましたが、今後は許可のない外部アカウントの登録は拒否される必要があります。こうした違反をモニタリングして早期に発見することが求められています。

これらの要件に対応するため、最適なAWSソリューションを選択してください。（2つ選択してください。）

- [x] AWS ConfigによりAWS Organizationsのコンプライアンス状況をモニタリングして、SNSトピックとAmazon EventBridgeを利用して、変更に関する通知を設定する。 (正解)
- [ ] CloudWatchログによりAWS Organizationsのコンプライアンス状況をモニタリングして、SNSトピックまたはAmazon EventBridgeを利用して、変更に関する通知を設定する。
- [ ] Amazon CloudTrailを利用してAWS OrganizationsへのAPIコールをモニタリングする。その上で、Amazon EventBridgeとSNSを利用して、通知を実施する。 (正解)
- [ ] Amazon Systems Managerを利用してAWS OrganizationsへのAPIコールをモニタリングする。その上で、Amazon EventBridgeとSNSを利用して、通知を実施する。
- [ ] AWS Configを利用してAWS OrganizationsへのAPIコールをモニタリングする。その上で、Amazon EventBridgeとSNSを利用して、通知を実施する。

説明

オプション1は正解となります。~~AWS Configのマルチアカウント、マルチリージョンのデータ集約により、複数のアカウントおよびリージョンからのAWS Configデータを単一のアカウントに集約できます。~~ マルチアカウント、マルチリージョンのデータ集約は、中央のIT管理者が企業内の複数のAWSアカウントのコンプライアンスを監視するのに役立ちます。

オプション3は正解となります。AWS Organizations 機能を使用する場合は組織（OU）を指定し、その組織内のすべてのアカウントにアクセス許可を付与できます。たとえば、そのようなアクションの機密性のために、ほとんどの管理者は、誰かが組織内に新しいアカウントを作成するたびに、またはメンバーアカウントの管理者が組織を離れようとするたびに警告を受けます。これらのアクションを検索し、生成されたイベントを管理者が定義したターゲットに送信するAmazon EventBridgeのイベントルールを設定できます。ターゲットは、サブスクライバーに電子メールまたはテキストメッセージを送信するAmazon SNSトピックにすることができます。これをAmazon CloudTrailと組み合わせて、一致するAPI呼び出しが受信されるたびに起動するイベントを設定できます。

オプション2は不正解です。CloudWatchログではなく、AWS ConfigによりAWS Organizationsのコンプライアンス状況をモニタリングすることが必要です。

オプション4は不正解です。Amazon Systems Managerを利用してAWS OrganizationsへのAPIコールをモニタリングするといった対応はできません。

オプション5は不正解です。AWS Configではなく、Amazon CloudTrailを利用してAWS OrganizationsへのAPIコールをモニタリングします。

40

あなたは画像編集ソフトウェア企業A社で働いているソリューションアーキテクトです。開発部門では複数のAmazon S3バケットを使用して、さまざまなデジタル画像編集用の高解像度メディアファイルを保存しています。別のAWSアカウントを利用している運用部門において、このS3バケット内のデータを利用した既存アプリケーションとの連携機能が運用されることになりました。そのため、運用部門からS3バケットから複数のオブジェクトを頻繁に取得するケースが多くなっていますが、そのデータ転送コストが開発部門に請求されていることが問題となっています。

次のうちで、運用部門による利用コストを最適化するための対応を選択してください。

- ◉ バケットをS3 Intelligent-Tieringに変更することで、利用料が多いユーザーに対して自動で課金設定を実施できる。 (不正解)
- ○ バケットのバケットポリシー設定において利用ユーザーに対して、データ利用料に応じた価格設定をユーザーに実施する。
- ○ バケットのリクエスタ支払い設定を実施することで、データ利用料に応じた価格設定をユーザーに実施する。 (正解)
- ○ バケットの料金設定において利用ユーザーに対して、データ利用料に応じた価格設定をユーザーに実施する。

説明

オプション3が正解となります。Amazon S3 バケットのストレージおよびデータ転送にかかるコストはすべて、そのバケット所有者が負担することが基本設定となります。ただしバケット所有者は、バケットをリクエスタ支払いバケットとして設定することができます。リクエスタ支払いを利用すると、リクエストおよびバケットからのデータのダウンロードにかかるコストは、所有者でなくリクエストを実行したリクエスタが支払うことになります。データの保管にかかるコストは常にバケット所有者が支払います。このように、他者がバケット内のデータにアクセスする際に発生する費用を負担したくない場合に、リクエスタ支払いを設定します。

オプション1は不正解です。S3 Intelligent-Tieringに変更することで、利用料が多いユーザーに対して自動で課金設定を実施するといった機能はありません。

オプション2は不正解です。バケットポリシー設定において利用ユーザーに対して、データ利用料に応じた価格設定をユーザーに実施することはできません。

オプション4は不正解です。バケットの料金設定において利用ユーザーに対して、データ利用料に応じた価格設定をユーザーに実施するといった機能はありません。

41

あなたの会社はレガシーシステムをアップグレードする際にAWSへの移行を決定し、オンプレミスネットワークをAWSクラウドに移行することになりました。このネットワークは以下のように構成されています。

・VPC（10.0.0.0 / 16）
・パブリックサブネット（10.0.0.0 /24）
・プライベートサブネット（10.0.1.0 /24）

このネットワークに新しいパブリックサブネット（10.0.0.0 /16）を追加しようとしています。

この新しいパブリックサブネットを追加した場合にどうなりますか？

- (◉) CIDRブロック10.0.0.0 / 16を持つ新しいサブネットと、先に作ったサブネットとの間にオーバーラップエラーが発生する。 (正解)
- ( ) VPC内に2つ目のサブネットも問題なく起動する。
- ( ) CIDRブロック10.0.0.0 / 16を持つ新しいサブネットと、全く同じCIDRブロック10.0.0.0 / 16を持つVPCとの間にオーバーラップエラーが発生する。
- ( ) CIDRブロック10.0.0.0/24を持つ先に作ったサブネットと、CIDRブロック10.0.0.0/16を持つVPCとの間にオーバーラップエラーが発生する。

説明
オプション１が正解となります。CIDRブロック10.0.0.0/16を持つ新しいサブネットと先に作ったサブネットとの間にオーバーラップエラーが発生します。サブネットのCIDRブロックは、VPCのCIDRブロック（VPCの単一サブネットの場合）、またはVPCのCIDRブロックのサブセットと同じにすることができます。許可されるブロックサイズは、/ 28ネットマスクと/ 16ネットマスクの間です。VPCで複数のサブネットを作成する場合、サブネットのCIDRブロックは重複できません。したがって、10.0.0.0/16の別のサブネットのCIDRブロックは10.0.0.0/24の範囲を含めてしまっているため、重複エラーが発生してしまいます。

オプション２は不正解です。上記のようにオーバーラップエラーが発生するため作成ができません。

オプション３は不正解です。CIDRブロック10.0.0.0 / 16を持つ新しいサブネットと、全く同じCIDRブロック10.0.0.0 / 16を持つVPCはエラーが発生せずに作成が可能です。

オプション４は不正解です。CIDRブロック10.0.0.0/24を持つ先に作ったサブネットと、CIDRブロック10.0.0.0/16を持つVPCとの間にオーバーラップエラーは発生しません。

あなたの会社ではデータセンターを利用して社内インフラを運用しています。オンプレミスのデータセンターではホワイトリストに登録した信頼できるIPアドレスを使用するサプライチェーンアプリケーションをホストしています。最近になって、経営陣はこのアプリケーションを含めてオンプレミス環境のインフラをAWSへと移行することを決定しました。その際にオンプレミス環境で利用しているIPアドレスを変更することなく、VPCに移行することが求められています。

この要件を満たす最も費用対効果の高い方法は次のうちどれですか？

- (◉) Route53を利用したIPアドレス範囲をレコード内に設定して、そのIPアドレス範囲がDNSとしてルーティングできるように設定する。 (不正解)
- ( ) アドレス範囲を地域インターネットレジストリに登録し、Registry Data Access Protocol (RDAP) を利用して自己署名付きのX509証明書を発行する。 (正解)
- ( ) CloudFrontディストリビューションを構成して、セクセス設定においてホワイトリストのIPアドレス範囲を許可設定する。
- ( ) 複数のEIPを作成して、ホワイトリストのIPアドレス範囲を許可設定する。

説明

このシナリオでは、オンプレミス環境で利用しているパブリックIPv4アドレス範囲をVPCに移行する方法が問われています。その際は、「BYOIP」を利用して、アドレス範囲をAWSに持ち込むことで、アドレスプールが表示されて、移行したパブリックIPv4アドレス範囲でElastic IPアドレスを作成することができるようになります。そして、このElastic IPアドレスをEC2インスタンス、NATゲートウェイ、ネットワークロードバランサーなどのAWSリソースに使用できます。

そのための設定プロセスにおいて、アドレス範囲は、地域インターネットレジストリ (RIR、Regional Internet registry) に登録する必要があります。Route Origin Authorization (ROA) は、利用している RIR を介して作成できる電子署名付き証明書です。これには、アドレス範囲、そのアドレス範囲を公開することを許可された自律システム番号 (ASN)、および有効期限が含まれています。ROA は Amazon が特定の AS 番号のアドレス範囲を公開することを承認します。ただし、その AWS アカウントに対して、アドレス範囲を AWS に持ち込むことを承認するわけではありません。AWS アカウントに対してアドレス範囲を AWS に持ち込むことを承認するには、アドレス範囲について Registry Data Access Protocol (RDAP) の注釈で自己署名付きの X509 証明書を発行する必要があります。証明書にはパブリックキーが含まれており、AWS はこれを使用してあなたが提供する認証コンテキスト署名を確認します。プライベートキーを安全に管理し、これを使用して認証コンテキストメッセージを署名する必要があります。

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は間違いです。Route53を利用したIPアドレス範囲をレコード内に設定して、そのIPアドレス範囲がDNSとしてルーティングできるように設定するといった方法はありません。

オプション3は不正解です。CloudFrontディストリビューションを構成して、アクセス設定においてホワイトリストのIPアドレス範囲を許可設定することはできません。WAFを利用してIP制御をすることが必要です。

オプション4は不正解です。複数のEIPを作成して、ホワイトリストのIPアドレス範囲を許可設定するという機能はEIPではできないため、間違いとなります。

問題43: 不正解

あなたは大手ITソリューション企業のAWSエンジニアとして勤務しています。現在のクライアントから、オンプレミスネットワークをAWSクラウドに接続するハイブリッドクラウドアーキテクチャを実現するために、必要な認証方式を準備するように依頼されました。この会社ではオンプレミス環境において、サードパーティーのSAML IdPを利用したログインを実施しています。

この要件に対応するため、最適な認証設定を選択してください。 (2つ選択してください。)

- [x] オンプレミスデータセンターにおいてSAML 2.0 IDプロバイダーを使用して、IAMユーザーにAWSリソースへのアクセスを設定する。 (不正解)
- [ ] IAMグループを作成して、データセンターを利用したフェデレーションユーザーへのAWSリソースへのアクセス権限を割り当てる。
- [ ] IAMユーザーを作成して、データセンターを利用したフェデレーションユーザーへのAWSリソースへのアクセス権限を割り当てる。
- [ ] IAMロールを作成して、データセンターを利用したフェデレーションユーザーへのAWSリソースへのアクセス権限を割り当てる。 (正解)
- [ ] AWS マネジメントコンソールまたはAWS CLIを使用して、IAM SAML 2.0 IDプロバイダーをAWSに作成する。 (正解)
- [ ] IAMロールを使用して、IAM SAML 2.0 IDプロバイダーのエンティティを作成する。

説明

このシナリオでは、SAML 2.0 ベースのフェデレーションによるSSOの設定が求められています。IAMフェデレーションを利用して、ユーザーが SAML 2.0 互換 IdP でホストされる組織のポータルにサインインして、AWS に移動するオプションを選択すると、追加でサインインの情報を入力しなくてもコンソールにリダイレクトされます。サードパーティーの SAML IdP を使用してコンソールへの SSO アクセスを確立するか、外部ユーザーのコンソールアクセスを有効にするカスタム IdP を作成することができます。

オプション 5 が正解となります。このシナリオでは、SAML対応のシングルサインオンを実装して、個々のIAMユーザーを作成しなくても企業ユーザーがAWSコンソールにアクセスできるようにすることが求められています。これを実装するには、IAM コンソールで、SAML ID プロバイダーのエンティティを作成します。このプロセスの一環として、組織の IdP によって生成された SAML メタデータドキュメントを アップロードすることが求められます。

オプション 4 が正解となります。IAM では1 つ以上の IAM ロールを作成します。そして、ロールの信頼ポリシーで SAML プロバイダーを、組織と AWS 間の信頼関係を確立するプリンシパルとして設定します。ロールのアクセス許可ポリシーは、AWS で組織のユーザーが実行できることを設定します。その上で、オンプレミス環境の IdP において、オンプレミス環境のユーザーまたはグループを IAM ロールにマッピングするアサーションを定義します。

オプション 1 は不正解です。オンプレミスデータセンターにおいてSAML 2.0 IDプロバイダーを使用して、IAMユーザーにAWSリソースへのアクセスを設定するという設定方式では、直接にAWSユーザーへのアクセス設定をSAML 2.0 IDプロバイダーが実施することになってしまいます。つまり、SSOの設定を実施する回答とはなっておらず、オンプレミス環境にあるSAML 2.0 IDプロバイダーを使用することは不可能となります。

IAMグループやIAMユーザーではなく、IAMロールの設定が必要であるため、オプション 2 と 3 は間違いです。

IAMロールを使用して、IAM SAML 2.0 ID プロバイダーをAWSに作成することはできないため、オプション 6 は間違いです。

問題44: 正解

あなたは趣味の写真とその解説を共有することができる写真共有アプリケーションをAWSを利用して構築しています。このアプリケーションは、ELBとAutoScalingが設定された複数のEC2インスタンスがアプリケーションサーバーとして利用され、写真保存用にS3ストレージが利用され、文字情報を保存するためにAmazon DynamoDBが利用されています。あなたはアプリケーションサーバーからDynamoDBテーブルへの連携処理を実装しているところです。このアプリケーションではモバイル認証を実施して、DynamoDBへのアクセスすることが必要ですが、機能を比較検討したところAmazon Cognitoを利用しない方式をとることになりました。

この要件を満たすことができるソリューションを選択してください。

- (◉) **Web IdP（Amazon、Facebook、Google、またはその他のOIDC互換IdPでログイン）に登録して、AssumeRoleWithWebIdentity APIを呼び出すことで認証を実現する。次にIAMロールでDynamoDBアクセスの適切な許可設定を実施する。** (正解)
- ( ) **API Gatewayを利用して、AssumeRoleWithWebIdentity APIを呼び出すことで認証を実現する。次にIAMロールでDynamoDBアクセスの適切な許可設定を実施する。**
- ( ) **IAMロールを利用して、AssumeRoleWithWebIdentity APIを呼び出すことで認証を実現する。次にIAMロールでDynamoDBアクセスの適切な許可設定を実施する。**
- ( ) **WEBプロバイダー用のSCPを作成して、S3からのデータ取得とDynamoDBへの登録処理を許可する設定を行う。**

説明

~~モバイル認証を実現するためには、Amazon Cognitoを利用することが一般的です。~~

Amazon Cognitoを使用しない場合は、Web IdP（Amazon、Facebook、Google、またはその他のOIDC互換IdPでログイン）とやり取りするカスタムコードまたはアプリを作成し、AssumeRoleWithWebIdentity APIを呼び出すことで認証を実現します。

一時的セキュリティ認証情報をコードで使用するには、AWS STS API (AssumeRole など) をプログラムで呼び出し、結果の認証情報とセッショントークンを抽出し、これらの値を後続の AWS リソースからの呼び出しにより認証情報として使用します。次にDynamoDBに対する適切なアクセス許可を設定し、S3の静的ホスティングを利用してWebサイトをホストします。 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。API GatewayはAssumeRoleWithWebIdentity APIを呼び出して認証を実現する機能や構成は実現できません。API Gatewayはあくまでも APIを作成・管理するための機能であり、認証サービスではないからです。

オプション３は不正解です。IAMロール自体には、AssumeRoleWithWebIdentity APIを呼び出すことで認証を実現する機能はありません。

オプション４は不正解です。WEBプロバイダー用のSCPによって、認証情報を処理したり、リソース間の許可権限を設定するといった対応はできません。SCPは組織単位でアクセス許可・拒否の範囲を設定するポリシーであり、認証とは無関係です。

問題45: 不正解

大手金融機関ではAWSにおいて決済管理システムや顧客管理ポータルを運用しています。同社の運用グループはWindowsおよびLinux EC2インスタンスの毎月のパフォーマンスチェックを行っています。金融関連システムということもあり、実稼働環境では200を超えるオンデマンドEC2インスタンスを利用しています。各インスタンスからメモリ使用量、ディスク容量、その他のメトリクスなどのさまざまなシステム詳細情報ログを収集して、分析することが必要です。

この要件を満たす、最適なAWSソリューションを選択してください。

- (●) CloudTrailエージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する。次にAmazon Athenaを利用してログ情報を分析し、QuickSightを利用して解析結果を可視化する。 (不正解)
- ( ) CloudWatch エージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する。次にCloudWatch Logs Insightsを利用してログ情報を分析・可視化する。 (正解)
- ( ) 統合CloudWatch Logs エージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する。次にAmazon Athenaを利用してログ情報を分析、CloudWatchダッシュボードを利用して解析結果を可視化する。
- ( ) CloudTrailエージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する。次にCloudWatch ダッシュボードを利用してログ情報を分析・可視化する。
- ( ) 統合CloudWatch Logs エージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する。次にCloudWatch Logs Insightsを利用してログ情報を分析・可視化する。

説明

CloudWatch エージェントを使用すると、オペレーティングシステム全体で Amazon EC2 インスタンスからより多くのシステムレベルのメトリクスを収集することができます。このメトリクスには、EC2 インスタンスのメトリクスに加えて、ゲスト内メトリクスを含めることができます。他の CloudWatch メトリクスと同様に、CloudWatch エージェントで収集したメトリクスはCloudWatch において保存して表示することができます。CloudWatch エージェントによって収集されたログは、以前の CloudWatch Logsエージェントによって収集されたログと同様に、処理されて Amazon CloudWatch Logs に格納されます。

CloudWatch Logs Insights はクラウドスケールで動作するよう設計され、セットアップやメンテナンスが不要なフルマネージドのサービスです。これは大量のログを数秒で操作して、インタラクティブなクエリの実行と可視化を提供します。CloudWatch Logs Insightsは洗練されたアドホッククエリ言語をサポートしており、希望するフィールドを取得するためのコマンドや、フィルタベースの条件指定、統計データの計算（パーセンタイルや時系列集計など）、希望するフィールドでのソート、クエリで返されるイベント件数の制限が行えます。データをイベントのフィールドから取り出すには正規表現が利用できます。クエリ結果は折れ線グラフやスタックエリアチャートで可視化でき、CloudWatch ダッシュボード に追加することが可能です。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と４は不正解です。CloudTrailエージェントをEC2インスタンスにインストールして設定し、ログデータを自動取得する対応ではなく、CloudWatchエージェントをインストールする必要があります。

オプション３は不正解です。Amazon Athenaを利用してログ情報を分析するにはCloudWatchではなく、S3などにログファイルを蓄積して、そのデータを解析するといった構成が必要となります。本件ではCloudWatch内での一貫した解析が要件であるため、正しくありません。

オプション３と５は不正解です。CloudWatch Logs エージェントはCloudWatch エージェントの古いバージョンであり、利用することは可能ですが、CloudWatchエージェントを利用することが推奨されています。

問題46: 不正解

あなたの会社ではLambda関数を使用したサーバーレスアーキテクチャによるアプリケーションを運用しています。そこで、あなたはソリューションアーキテクトとして、Lambda関数を使ったシステムコンポーネントの設計・実装を担当しています。WEB上でLambda関数を実行して、別のVPC内のホストされているデータベースに処理結果を保存する機能を構築しました。このLambda関数を実行してVPC内のプライベートサブネットにあるデータベースにアクセスを試みましたが、Lambda関数は動作を停止してしまいました。

この問題を解決するために必要な対応を選択してください。 (2つ選択してください)

- [x] VPCエンドポイントにEIPを設定してアクセス可能にする。 (不正解)
- [x] Lambdaファンクションのセキュリティグループのアウトバウンドトラフィックの許可設定を適切なものに変更する。 (正解)
- [ ] VPCにNATゲートウェイを追加する。 (正解)
- [ ] Lambdaファンクションのアクセス制限の上限値を超えているため、AWS側に許可申請を実施する。
- [ ] Lambdaファンクションの処理がスタックしないように、SQSを前方に設置して、キューイング処理を行うようにする。

説明

このシナリオでは、Lambda関数を実行してVPC内のデータベースにアクセスしたところ、Lambda関数は動作を停止してしまい、処理を完了できなかったことが問題となっています。この処理では、VPCにホストされているデータベースに既存のLambda関数処理結果を保存することが必要であり、Lambda関数がVPC内のAWSリソースに対してアクセス可能である必要があります。したがって、Lambda関数が動作を停止し、変更後に処理を完了できなかったということは、AWSリソースへのアクセスが上手くいっていない可能性が高いです。

Lambda関数はWEB上でサーバレスアプリケーションの実行しており、AWSのプライベートサブネット内での処理についてはNATゲートウェイ経由での返信処理が設定されていなければレスポンスを受け取ることができません。Lambda関数でインターネットアクセスが必要な場合は、VPC内でNATインスタンスかNATゲートウェイを使用することが必要となります。また、Lambda関数の関連付けられたセキュリティグループがアウトバウンド接続を許可されていることを確認する必要があります。したがって、オプション2と3が正解となります。

【詳細は以下をご参照ください】

https://docs.aws.amazon.com/ja_jp/lambda/latest/dg/configuration-vpc.html

オプション1は不正解です。Lambda関数がVPC環境で実行されるためには、ユーザーが所有するVPCに接続するようにLambdaを設定し、カスタマーVPC内にElastic Network Interfaces (ENI) が作成され、クロスアカウント接続が行われます。このENIは、Lambda関数からプライベートリソースへのネットワークアクセスを許可します。VPCエンドポイントにEIPを設定する必要はありません。VPCエンドポイントを利用することでインターネットを介せずにLambda関数がVPC内のリソースへとアクセスが可能となることは正しいですが、今回の要件では求められていません。

オプション4は不正解です。Lambda関数のアクセス制限の上限値を超えた場合のエラーではなく、1つの実行処理自体が完了しないというエラーが発生しており、問題の認識に誤りがあります。

オプション5は不正解です。Lambda関数の実行数が多いためにエラーが発生しているわけではないため、SQSを前方に設置して、キューイング処理を行っても問題は改善されません。

https://docs.aws.amazon.com/ja_jp/lambda/latest/dg/configuration-vpc.html

問題47: 不正解

B金融機関はフィンテック事業として新しい仮想通貨取引システムを運用しています。あなたは開発担当者として、今年リリースしたモバイルから仮想通貨取引に参加できるアプリケーションをサーバレスアーキテクチャにより実装しています。このモバイルアプリケーションはグローバルに何10万人ものユーザーを抱えており、CloudFrontによってコンテンツが配信されることで最適な配信構成を実現していましたが、最近になってHTTP 504エラーが発生しているようです。特にログイン時にはコンテンツ表示に時間がかかっているようです。

この問題を解決するための最も費用対効果の高いAWSソリューションを選択してください。 (2つ選択してください。)

- [x] ユーザーに近い場所での認証プロセスを実施し、CloudFrontを利用したコンテンツ配信処理プロセスを実行するためにLamdba Edgeを利用する。 (正解)
- [x] ユーザーに近い場所での認証プロセスを実施し、CloudFrontを利用したコンテンツ配信処理プロセスを実行するためにCloudFrontの地域制限を有効化する。 (不正解)
- [ ] 2つのオリジンサーバーによるオリジングループを作成して、オリジンフェイルオーバーを構成する。1つをプライマリオリジン、もう1つはセカンダリーオリジンとして、プライマリオリジンに障害が発生したときにCloudFrontが自動的な切替対象とする。 (正解)
- [ ] 2つのオリジンサーバーによるオリジングループを作成して、オリジンフェイルオーバーを構成する。1つをプライマリオリジン、もう1つは、プライマリオリジンに障害が発生時にLambda関数が切替わるセカンダリーオリジンとする。
- [ ] ユーザーに近い場所での認証プロセスを実施し、CloudFrontを利用したコンテンツ配信処理プロセスを実行するためにRoute53の位置情報ルーティングを利用する。

説明

このシナリオでは、モバイルアプリケーションへのアクセス時にHTTP 504エラーが発生する問題が多発しており、その改善が求められています。この原因としては、グローバルなコンテンツ配信処理のパフォーマンスが低下していることが考えられます。

オプション 1 が正解となります。Lambda Edgeを使用して、Lambda関数でCloudFrontが配信するコンテンツをカスタマイズし、ユーザーに近いAWSロケーションで認証プロセスを実行できます。これによって、グローバルなユーザーに適した認証プロセスが実施できることでモバイルアプリケーションのログイン遅延に対応することができます。

Lambda@Edge では、Node.js Lambda 関数を実行して CloudFront が発信するコンテンツをカスタマイズし、ビューワーに近い AWS 地域でこの関数を実行できます。この関数は、プロビジョニングや管理の必要なく、CloudFront イベントに応答を実行します。Lambda 関数を使用して、次の時点で CloudFront リクエストとレスポンスを変更できます。

■ CloudFront がビューワーからリクエストを受信した後 (ビューワーリクエスト)

■CloudFront がリクエストをオリジンサーバーに転送する前 (オリジンリクエスト)

■CloudFront がオリジンからレスポンスを受信した後 (オリジンレスポンス)

■CloudFront がビューワーにレスポンスを転送する前 (ビューワーレスポンス)

オプション 3 は正解となります。CloudFrontではプライマリオリジンに障害が発生したときにCloudFrontが自動的に切り替える2番目のオリジンとして2つのオリジンを持つオリジングループを作成することにより、オリジンフェールオーバーを設定できます。これにより、不定期のHTTP 504エラーが軽減されます。

高可用性が必要なシナリオでは、オリジンフェイルオーバーを使用して CloudFront を設定できます。開始するには、オリジングループを作成し、CloudFront のプライマリオリジンとプライマリオリジンが特定の HTTP ステータスコードの失敗応答を返したときに CloudFront が自動的に切り替わる セカンダリーオリジンを指定します。

オプション 2 は不正解です。CloudFrontの地域制限を有効化することで、特定地域での配信を制限する設定ができます。これは本件の対応には無関係な対応となります。

オプション 4 は不正解です。これは、プライマリオリジンに障害が発生した際にLambda関数が切替わるのではなく、CloudFrontが自動的な切替対象とする構成となります。

オプション 5 は不正解です。Route53の位置情報ルーティングによって、CloudFrontの配信プロセスにおける遅延を解消するという組合せはありません。

問題48: 正解

A社は動画再生アプリケーションをAWSにホストして構築しています。このアプリケーションでは動画データをS3に保存しつつ、EC2インスタンスによる動画処理を実施し、グローバルにユーザーに利用してもらう配信プラットフォームであるため、CloudFrontを前面に設定しています。あなたはソリューションアーキテクトとして、動画配信のセキュリティ制御を実装しているところです。要件としては、暗号化によって配信データと保存データを保護する必要があります。また、直接S3バケットへのアクセスを制限することも必要です。

これらのアプリケーション要件を踏まえて最適なソリューションを選択してください。

- ◉ **Advanced Encryption Standard (AES-256)を利用して保存中のデータとストリーミング用のトランスコーディングしたデータを暗号化する。次にCloudFrontにOrigin Access Identityを利用して、CloudFrontからのみコンテンツを利用できるように設定する。** (正解)
- ○ **CloudFrontにSSLを設定して保存中のデータとストリーミング用のトランスコーディングしたデータを暗号化する。次にCloudFrontにOrigin Access Identityを利用して、CloudFrontからのみコンテンツを利用できるように設定する。**
- ○ **CloudHSMを利用して保存中のデータとストリーミング用のトランスコーディングしたデータを暗号化する。次にCloudFrontに署名付きURLを利用して、CloudFrontからのみコンテンツを利用できるように設定する。**
- ○ **CloudFrontにSSLを設定して保存中のデータとストリーミング用のトランスコーディングしたデータを暗号化する。次にCloudFrontにIAMポリシーを利用して、CloudFrontからのみコンテンツを利用できるように設定する。**

説明

このシナリオでは、S3バケットへのアップロードした動画やストリーミングされる動画を暗号化によって保護する対応が求められています。そのためには、Advanced Encryption Standard (AES-256)を利用して保存中のデータとストリーミング用のトランスコーディングしたデータを暗号化して、CloudFrontにOrigin Access Identityを利用して、CloudFrontからのみコンテンツを利用できるように設定することで対応が可能です。したがって、オプション1が正解となります。

サーバーサイド暗号化は、ストレージやデータベースで保存された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ており、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します。Amazon S3 サーバーサイド暗号化では、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ています。

CloudFront では OAI を使用してファイルアクセス許可を構成することで、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ができなくなります。

オプション2と3は不正解です。SSLはデータ通信処理時の暗号化を実現しますが、データ保存時の暗号化には利用できません。

オプション4は不正解です。 Amazon S3の暗号化にはSSE-S3とKMSを利用することができますが、CloudHSMは鍵の作成管理用のサービスであり不適切です。

問題49: 不正解

A社では多層Webアプリケーションをオンプレミス環境からAWSへと移行したところです。現在、WEB層においてプレースメントグループを構成している9つのEC2インスタンスが実行されています。最近になってEC2インスタンスの処理負荷が増加したことを受けて、このプレイスメントグループに対して2つの新しいインスタンスを追加することになりました。このインスタンスは既存のものと同じタイプのインスタンスです。

どのようにしてプレイスメントグループにEC2インスタンスを追加できますか？

- (●) 現在起動しているプレイスメントグループに既存のEC2インスタンスと同じインスタンスタイプを新規に2つ追加して、それらを起動させる。 (不正解)
- ( ) 現在起動しているプレイスメントグループに既存のEC2インスタンスよりパフォーマンスが優れたインスタンスタイプを新規に2つ追加して、それらを起動させる。
- ( ) 一旦プレイスメントグループを削除した上で、既存のEC2インスタンスよりパフォーマンスが優れたインスタンスタイプを新規に2つ追加してから、プレイスメントグループにあるEC2インスタンスを再起動する。
- ( ) 既存のEC2インスタンスと同じインスタンスタイプを2つ新規作成して停止させた上で、AWS CLIを使用して利用しているプレイスメントグループにインスタンスを移動する (正解)

説明

このシナリオではプレイスメントグループへの適切なインスタンスの追加方法が求められています。インスタンスグループに新規にインスタンスの追加したり、クラスタープレイスメントグループ内に異なるインスタンスタイプを使用すると、「容量エラー」が発生する可能性があります。しかしながら、今回の追加インスタンスは既存のものと同じタイプのインスタンスです。

既存のプレイスメントグループに新規EC2インスタンスを追加する際は、既存のEC2インスタンスと同じインスタンスタイプを新規に2つ起動して、その状態を停止させます。その上でAWS CLIを使用して利用しているプレイスメントグループにインスタンスを移動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 CLIを使用してプレイスメントグループにインスタンスを移動するには

1. stop-instancesコマンドを使用して、インスタンスを停止します。
2. modify-instance-placementコマンドを使用し、インスタンスの移動先のプレイスメントグループの名前を指定します。

```
aws ec2 modify-instance-placement --instance-id i-0123a456700123456 --group-name MySpreadGroup
```

3. start-instancesコマンドを使用してインスタンスを起動します。

オプション1は不正解です。現在起動しているプレイスメントグループに別のインスタンスを後から追加することはできません。

オプション2と3は不正解です。プレイスメントグループ内のインスタンスタイプは同じものである必要があります。

【参照】

プレイスメントグループ - Amazon Elastic Compute Cloud

問題50: 不正解

あなたの会社はIoTデータによる農業データ管理システムを運用しています。このシステムは、毎日の実行タスクとして、その日の農地のかかる土壌および水分データを取得して、最適な育成環境であるかをモニタリングしつつ、機械学習によって最適な施策をレコメンデーションしています。この機能を実施するためには、リアルタイム土壌分析処理と、リアルタイム栄養素分析処理の２つのトランザクション処理を実施することが必要とされています。2つのトランザクション機能が効率的にデータを処理できるように、２つの処理には同じトランザクションデータが確実に配信されて、シリアルにデータ順序が保証されている必要があります。

これらのアプリケーション要件を踏まえて最適なソリューションを選択してください。

- (◉) Amazon SQSを利用してポーリング処理のFIFO設定を行うことで、２つのトランザクション処理に同じデータを渡して別々の時間帯に実行させる。 (不正解)
- ( ) AWS DataPipelineを利用して、２つのトランザクション処理に同じデータを渡して別々の時間帯に実行させる。
- ( ) Amazon Kinesis Data Streamsを利用して、２つのトランザクション処理に同じデータを渡して別々の時間帯に実行させる。 (正解)
- ( ) Amazon Kinesis Data Streamsによりデータを取得し、Amazon SQSへと配信する。SQSはポーリング処理のFIFO設定を行うことで、２つのトランザクション処理に同じデータを渡して別々の時間帯に実行させる。

説明

オプション３が正解となります。このシナリオでは、トランザクション処理が発生する度に同じデータを2つのアプリケーション機能に送信する仕組みを作ることが要件になっています。常に同じデータを送信するためにはストリーミング処理が必要となり、これはストリーミングデータのリアルタイム処理を可能にするAmazon Kinesis Data Streamsを使用することで達成できます。Amazon Kinesis Data Streamsはレコードの順序付け、および複数のAmazon Kinesisアプリケーションに対して同じ順序でレコードを読み取ったり再生したりする機能を提供します。KCLにより、特定のパーティションキーのすべてのレコードを同じレコードプロセッサに配信し、同じAmazon Kinesisデータストリームから読み取る複数のアプリケーションを構築することができます。

SQSを利用したオプション１と４は不正解です。Amazon SQSポーリング処理のFIFO設定を行うことで、データを順番に最低一回の配信を確保しながら並列処理を構成することができますが、~~ストリーミングデータ~~処理には利用できません。ストリーミングデータを処理するためには、Amazon Kinesis Data Streamsが必要となるため不正解です。また、Amazon Kinesis Data Streamsの機能だけで済むため、SQSとAmazon Kinesis Data Streamsを一緒に利用する必要はありません。

オプション２は不正解です。AWS DataPipelineは指定された間隔で、AWS サービスとオンプレミスのデータソース間で、信頼性の高いデータ処理やデータ移動を実行するデータパイプラインを作成するサービスです。今回のようなストリーミングデータ処理には適していません。

問題51: 正解

あなたはAWSを利用したネットワーク構成を実装しています。VPCのDHCP（Dynamic Host Configuration Protocol）は、構成情報をTCP/IPネットワーク上のホストに提供しています。DHCPオプションの最初のセットを作成してAmazonのDNSサーバーを利用してVPCに関連付けましたが、エラーが発生してしまいました。

この問題を解決するため最適なソリューションを選択してください。

- ◉ 新しいDHCPオプションを作成して、domain-name-servers=AmazonProvidedDNSを指定してVPCに関連付けを実施する。 (正解)
- ○ VPC内にあるEC2インスタンスを全て停止して、DHCP設定をリフレッシュする。
- ○ 新しいDHCPオプションを作成して、domain-name=domain-name-for-your-regionを指定してVPCに関連付けを実施する。
- ○ AWS Command Line Interfaceを利用することで、DHCPオプションを修正することができる。

説明

オプション1が正解となります。DHCPはTCP/IPネットワークのホストに設定情報を渡すための規格です。このDHCPメッセージのoptionsフィールドの内容は設定パラメータとなり、VPCのDHCPオプションセットに設定できます。VPCでは一度DHCPオプションセットを作成すると変更できないため、変更時にはDHCPオプションの新しいセットを作成し、VPCに関連付ける必要があります。 したがって、新しいDHCPオプションを作成して、domain-name-servers=AmazonProvidedDNSを指定してVPCに関連付けを実施することで、エラーを回避することが必要です。

VPCを作成する際、DHCPオプションセットを自動的に作成してVPCに関連付けます。このセットには、domain-name-servers=AmazonProvidedDNSとdomain-name=domain-name-for-your-regionがオプションとして用意されています。AmazonProvidedDNSはAmazonのDNSサーバーです。このオプションは、VPCのインターネットゲートウェイを介して通信する必要があるインスタンスに対してDNSを有効にします。文字列Amazon ProvidedDNSは、リザーブドIPアドレスで実行中のDNSサーバーにマップされ、VPC IPv4ネットワークの範囲に2をプラスした値です。今回の設定では、domain-name-servers=AmazonProvidedDNSを有効化する設定が必要となります。

オプション2は不正解です。VPC内にあるEC2インスタンスを全て停止して、DHCP設定をリフレッシュしても、DHCPオプション変更が必要なため、このエラーは解消されません。

オプション3は不正解です。domain-name=domain-name-for-your-regionではなく、domain-name-servers=AmazonProvidedDNSを指定してVPCに関連付けを実施する必要があります。

オプション4は不正解です。AWS Command Line Interfaceを利用することで、エラーとなったDHCPのオプションを修正することはできません。今回のケースでは、新規に設定をやり直す必要があります。

問題52: 不正解

大手ソフトウェア会社はエンドユーザーが作成および取得できるスケジュールをモバイルで作成・共有できるタスク管理アプリケーションサービスを開発しています。日々のデータはDynamoDBテーブルに蓄積される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、アプリケーションのデータ処理においてサーバレス機能を実装しています。この機能では、APIゲートウェイからLambda関数を呼び出すことで、DynamoDBテーブルのデータを取得してデータ集計を行います。実装にはLambda関数によるDynamoDBテーブルへのアクセスが必要となり、Lambda関数にIAMロールを設定することが求められます。

このLamdba関数のアクセス権限を適切に設定するためのプロセスを選択して下さい。（2つ選択してください。）

- [x] LamdbaからDynamoDBのアクセス許可を設定するためインラインポリシーのResourceには「dynamodb：GetItem」と「dynamodb：PutItem」を含める (不正解)
- [x] IAMポリシーを利用して、Amazon API Gatewayサービスプリンシパル（apigateway.amazonaws.com）にLambda関数を呼び出すアクセス許可を付与する。 (不正解)
- [ ] add-permission AWS Lambdaコマンドを実行して、Amazon API Gatewayサービスプリンシパル（apigateway.amazonaws.com）にLambda関数を呼び出すアクセス許可を付与する。 (正解)
- [ ] LamdbaからDynamoDBのアクセス許可を設定するためインラインポリシーのActionには「dynamodb：GetItem」と「dynamodb：PutItem」を含める (正解)

説明

HTTPS エンドポイントで API を呼び出すと、Amazon API Gatewayから Lambda 関数を呼び出すことができます。Lamdbaに必要なアクセス許可が含まれていることを確認するために、以下の設定作業が必要となります。

・POST リクエストで送信するリクエストペイロードによって、DynamoDB オペレーションが識別され、必要なデータが提供されます。

・次にLambdaにはDynamoDBのアクセスが必要です。LamdbaからDynamoDBのアクセスが許可を設定するためインラインポリシーのActionには 「dynamodb：GetItem」と「dynamodb：PutItem」が必要です。

・最後に、Lambda関数に関連付けられたアクセス許可ポリシーにアクセス許可を追加する必要があります。 add-permission AWS Lambdaコマンドを実行して、Amazon API Gatewayサービスプリンシパル（apigateway.amazonaws.com）にLambda関数を呼び出すアクセス許可を付与します。

したがって、実行すべきプロセスとして上記の内容と合致するオプション３と４が正解となります。

オプション１は不正解です。LamdbaからDynamoDBのアクセス許可を設定するためインラインポリシーのResourceではなく、Actionに「dynamodb：GetItem」と「dynamodb：PutItem」を含める必要があります。

オプション２は不正解です。IAMポリシーを利用するのではなく、add-permission AWS Lambdaコマンドを実行して、Amazon API Gatewayサービスプリンシパル（apigateway.amazonaws.com）にLambda関数を呼び出すアクセス許可を付与する必要があります。

問題53: 不正解

A銀行は金融システム向けのAWSクラウド環境を構築しています。会社にはシステム開発・運用の各段階を分けるためにAWS Organizationsで統合管理された3つのアカウントがあります。利用しているアカウントは開発、テスト、本番環境用の3つのAWSアカウントです。開発アカウントは、AZ：ap-northeast-1dでインスタンスタイプがm4.largeの3つのリザーブドインスタンスを購入しました。また、開発アカウントが実行しているインスタンスはありませんが、AZ：ap-northeast-1dにある本番環境アカウントでは、5つのm4.largeインスタンスを利用することになりました。

この状況でリザーブドインスタンスの価格割引の恩恵をうけることができるAWSアカウントはどれでしょうか？

- ◉ 本番アカウントが既に複数のインスタンスを起動してるAZ：ap-northeast-1d内にリザーブドインスタンスを購入したため、開発アカウントが価格割引の恩恵を受けることができる。 (不正解)
- ○ 開発アカウントが購入したリザーブドインスタンスを設置しているAZ：ap-northeast-1dで、インスタンスを起動している本番環境アカウントが統合請求による価格割引の恩恵を受けることができる。 (正解)
- ○ 開発アカウントと本番環境アカウントが共にAZ：ap-northeast-1d内でリザーブドインスタンスとオンデマンドインスタンスを起動しているので、合計金額をインスタンス保有数で割った金額を支払うことになる。
- ○ 開発アカウントが購入したリザーブドインスタンス分の利用料を支払うことになるが、起動していないため無課金となる。

説明

このシナリオでは、開発アカウントが購入した同じインスタンスタイプのリザーブドインスタンスを設置しているAZでインスタンスを起動している本番環境アカウントにおいて、統合請求による価格割引の恩恵を受けることができることになります。したがって、オプション2が正解となります。

AWS Organizationsを利用して一括請求を設定すると、ボリュームディスカウントやリザーブドインスタンスの割引適用を登録されたメンバーアカウント全体で共有することができるメリットがあります。たとえば、Amazon EC2 リザーブドインスタンスの購入方法の例として、ボブとスーザンが組織内でそれぞれアカウントを持っているとします。スーザンは 5 つの同じタイプのリザーブドインスタンスを持っていて、ボブは何も持っていません。ある特定の時間内に、スーザンが 3 つのインスタンスを使用し、ボブが 6 つを使用し、組織の一括請求において合計 9 つのインスタンスが使用されました。AWS は 5 個のインスタンスをリザーブドインスタンスとして請求し、残り 4 つのインスタンスを通常のインスタンスとして請求します。

スーザンがリザーブドインスタンスを購入したのと同じ利用可能ゾーンでボブがインスタンスを起動する場合にのみ、ボブはスーザンのリザーブドインスタンスのコスト利点を受けることができます。たとえば、スーザンがリザーブドインスタンス購入の際に us-west-2a を指定した場合、ボブが組織の一括請求でコストメリットを得るためには、ボブは自分のインスタンス起動時に us-west-2a を指定する必要があります。しかし、Availability Zone の実際のロケーションは、アカウント間で独立しています。たとえば、ボブのアカウントの us-west-2a アベイラビリティーゾーンは、スーザンのアカウントのロケーションとは異なるロケーションにある可能性があります。

問題54: 不正解

あなたは新しいSNSアプリケーションをAWSにホストして構築しています。このアプリケーションでは日常の写真などを共有したりメッセージを発信したりすることができます。アプリケーションは2つのアベイラビリティーゾーンにデプロイされたEC2インスタンスに対してAuto Scalingグループ とELBを使用した構成となっており、静的なコンテンツを配信するためにCloudFrontを使用しています。このSNSサイトはHTTPS / SSLを利用していないため、Google検索ランキングが低くなっていることが問題となっており、あなたは改善することになりました。

ユーザーとCloudFront間通信にHTTPSを利用するために、適切な設定方式を選択してください。（3つ選択してください。）

- [x] CloudFrontでViewer Protocol Policyとして HTTPS setを設定する。 (不正解)
- [x] CloudFrontでViewer Protocol Policyとして HTTPS Onlyを設定する。 (正解)
- [ ] CloudFrontでViewer Protocol PolicyとしてRedirect HTTP to HTTPSを設定する。 (正解)
- [x] CloudFrontでViewer Protocol PolicyとしてSSL / TLS onlyを設定する。 (不正解)
- [ ] CloudFrontのViewer Protocol Policyの設定でSSL / TLS証明書を利用できる設定にする。 (正解)

説明

オプション２と３と５が正解となります。ユーザーとCloudFront間の通信にHTTPSを利用するための、AWS側での設定として次の３つの方法を選択できます。

■CloudFrontでViewer Protocol Policyとして HTTPS Onlyを設定する。

■CloudFrontでViewer Protocol PolicyとしてRedirect HTTP to HTTPSを設定する。

■CloudFrontのViewer Protocol Policyの設定でSSL / TLS証明書を利用できる設定にする。

CloudFront ディストリビューション内で１つ以上のキャッシュ動作を設定して、ビューワーと CloudFront との通信で HTTPS利用を必須にできます。また、１つ以上のキャッシュ動作で HTTP と HTTPS の両方を許可するように構成して、CloudFront における一部のオブジェクトで HTTPS を必須にすることもできます。CloudFront がディストリビューションに割り当てたドメイン名を使用している場合 (d111111abcdef8.cloudfront.net など)、１つ以上のキャッシュ動作の [Viewer Protocol Policy] 設定を変更して、HTTPS 通信を必須にします。この設定で、CloudFront は SSL/TLS 証明書を提供します。

独自のドメイン名 (example.com など) を使用している場合、CloudFront のいくつかの設定を変更する必要があります。そのためには、AWS Certificate Manager (ACM) が提供する SSL/TLS 証明書を使用するか、サードパーティー認証機関からの証明書を ACM または IAM 証明書ストアにインポートするか、自己署名した証明書を作成しインポートする必要があります。

したがって、CloudFrontのViewer Protocol Policyの設定でSSL / TLS証明書を利用できる設定にするという、オプション５は正解となります。

１つ以上のキャッシュ動作でビューワーと CloudFront との間で HTTPS を必須とするためには、次の手順を実行します。

・ビューワーと CloudFront との間で HTTPS が必須になるよう CloudFront を設定する
・AWS マネジメントコンソール にサインインし、
https://console.aws.amazon.com/cloudfront/ にある、CloudFront コンソールを開きます。
・CloudFront コンソールの上部のペインで、更新するディストリビューションの ID を選択します。
・[Behaviors] タブで、更新するキャッシュ動作を選択した後、[Edit] を選択します。
・[Viewer Protocol Policy] として次のいずれかの値を指定します。
  -Redirect HTTP to HTTPS
  -HTTPS Only

したがって、これらの手順を踏まえると、オプション２と３が正解となります。

問題55: 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の構築など、画像AIや画像分析を得意としたベンチャー企業です。現在開発している顔認証システムは、オンデマンドEC2インスタンスを複数利用してELBとAuto Scalingグループを構成しています。エラーを引き起こしている特定のインスタンスが1つあり、これを迅速に終了する必要があります。

AWS CLIを使用して、グループのサイズを更新せずに指定されたAuto Scalingグループからインスタンスを終了するコマンド操作を選択してください。

- ○ terminate-instance-in-auto-scaling-group --instance-id YOUR-INSTANCE-ID --no-should-decrement-desired-capacity (正解)
- ○ detach-instances --instance-id YOUR-INSTANCE-ID --no-should-decrement-desired-capacity --auto-scaling-group-name YOUR-ASG-NAME
- ○ terminate-instance-in-auto-scaling-group --instance-id
- ◉ --no-should-decrement-desired-capacity (不正解)

説明

オプション1が正解となります。terminate-instance-in-auto-scaling-group CLIコマンドにより、指定されたインスタンスを終了し、必要に応じて必要なグループサイズを調整します。この呼び出しは、インスタンスがただちに終了しないように、終了要求を行います。このコマンドを実行する際は--should-decrement-desired-capacity または --no-should-decrement-desired-capacityを利用して、インスタンス数の調整オプションの設定が必要です。

オプション2は不正解です。このコマンドを使用して、EC2 Auto Scaling グループからインスタンスをデタッチします。

オプション3は不正解です。terminate-instance-in-auto-scaling-group --instance-idには--should-decrement-desired-capacityパラメーターまたは--no-should-decrement-desired-capacityパラメーターが必要であるため、正しくありません。

オプション4は不正解です。--no-should-decrement-desired-capacityはterminate-instance-in-auto-scaling-group --instance-idコマンドのオプションであり、これだけではEC2インスタンスを終了することはできません。

問題56: 正解

大手不動産会社ではAWSを利用した不動産ポータルサイトを構築しています。このポータルサイトでは、パブリックサブネットに設定されたEC2インスタンスベースのWebサーバーが、全IPアドレスからトラフィックを受信できるように設定されています。

このインスタンスに対して、さらに追加で１つのバックエンド処理を実行することが必要となりました。このバックエンド接続では、EC2インスタンスが選択したIP範囲からのみSSHトラフィックを受信することが必要です。これらの処理は全て１つのEC2インスタンス上で実現することが必要です。したがって、１つのEC2インスタンスに対して、バックエンド処理用のIPアドレスとインターネットからの通信トラフィック制御用のIPアドレスの２つのパブリックIPアドレスを利用することが要件となっています。

この要件を満たすための、最適なソリューションを選択してください。

- ◉ 2つのElastic Network Interfaces(ENI)を作成してEC2インスタンスに設定する。それにより、ENIの1つをインターネットトラフィック用に、もう1つをバックエンド処理用に利用する。 (正解)
- ○ 利用しているEC2インスタンスのIPアドレスとVPCの設定をIPv4からIPv6に変更して、2つのトラフィックを別に処理できるようにする。
- ○ 2つのElastic IPアドレスを作成してEC2インスタンスに設定する。それにより、Elastic IPアドレスの1つをインターネットトラフィック用に、もう1つをバックエンドトラフィック用に利用する。
- ○ 利用しているEC2インスタンスのセキュリティグループでインターネットとバックエンド接続の2つのトラフィック制御設定を実施する。

説明

オプション１が正解となります。このシナリオでは、単一のオンデマンドEC2インスタンスでWebアプリケーションの２つのIPアドレスを利用した処理を実行させるための設定が求められています。したがって、2つのエラスティックネットワークインターフェイス（ENI）を作成してEC2インスタンスに設定することで、ENIの1つをインターネットトラフィック用に、もう1つをバックエンドトラフィック用に利用することができます。

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す。 ENIを作成し、インスタンスにアタッチし、インスタンスからデタッチし、別のインスタンスにアタッチできます。ネットワークインターフェイスの属性は、インスタンスにアタッチまたはデタッチされ、別のインスタンスに再アタッチされるときに、それを継続することができます。

1つのインスタンスから別のインスタンスにENIを移動すると、ネットワークトラフィックは新しいインスタンスにリダイレクトされます。よって、2つのElastic Network Interfaces(ENI)を作成してEC2インスタンスに設定することで、ENIの1つをインターネットトラフィック用に、もう1つをバックエンドトラフィック用に利用することが可能となります。

オプション２は不正解です。IPアドレスとVPCの設定をIPv4からIPv6に変更しても、2つのトラフィックを別に処理できるようになるわけではありません。ENIを利用して２つのIPアドレスを利用できるようにすることが必要です。

オプション３は不正解です。Elastic IPアドレスだけではIPアドレスを２つ設定するといった構成はできません。ENIを利用して２つのIPアドレスを利用できるようにすることが必要です。

オプション４は不正解です。セキュリティグループでインターネットとバックエンド接続の2つのトラフィック制御をするといった対応はできません。

問題57: 不正解

ある衣料品ブランドは複数のEC2インスタンスとELBを使用したeコマース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デバイスプラットフォームをサポートしており、モバイルやPC端末など多様なデバイスからアクセスして利用される予定です。このモバイルアプリケーションでは複数のドメインからSSLによるセキュアな通信方式を設定することが必要となっています。

この要件を満たすために複数のCA証明書をセットアップ方法を選択してください。

- ◉ CLBを作成して複数のSSL証明書を設定する。 (不正解)
- ○ ELBに接続したRoute53を新たに設置して、ELBのヘルスチェックを利用したルーティング構成を行う。Route53のルーティングによってプラットフォームタイプごとに独自のスティッキーセッションと分離したSSL管理の構成を実施する。
- ○ ALBを作成して複数のSSL証明書を設定する。 (正解)
- ○ 個別のSSL認証を管理できるハイブリッドアーキテクチャを構成して、1つのELBで全体の分散処理を実現する。

説明

オプション3が正解となります。複数の証明書と Server Name Indication (SNI) を使用したスマートな証明書選択をサポートする Application Load Balancer (ALB) または Network Load Balancer (NLB) のどちらかを使用することで、複数ドメインに応じてSSL通信を設定することができます。複数の異なるドメインへの証明書をロードバランサーに追加するには、次のいずれかを実行します。

- AWS Certificate Manager (ACM) で、サブジェクト代替名 (SAN) 証明書を使ってロードバランサーの背後にある複数のドメイン (ワイルドカードドメインを含む) を検証する。
- 複数の証明書と Server Name Indication (SNI) を使用したスマートな証明書選択をサポートする Application Load Balancer (ALB) または Network Load Balancer (NLB) のどちらかを使用する。

【参照】

ACM を使用して複数のドメインの証明書を ELB にアップロードする (amazon.com)

オプション1は不正解です。Classic Load Balancer では複数の証明書の追加機能をサポートしていません。

オプション2は不正解です。Route53には、ルーティングによってデバイスタイプごとに独自のスティッキーセッションと分離したSSL管理の構成を実施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。個別のSSL認証を管理できるハイブリッドアーキテクチャによって、1つのELBによって全体を分散処理では、各デバイスタイプに応じた分散処理を実現はできません。

問題58: 不正解

A社はAWS上にインフラストラクチャを構成してAIベースの交通監視アプリケーションを構築しています。このシステムは都市の安全管理に使用されるため、間違った情報を利用したり、途中で障害が発生して不必要なダウンタイムが発生すると大きな問題となりかねません。よって、システムダウンを極力回避するために可用性と耐障害性を高める必要があります。フロントサイドのWEBサーバーはEC2インスタンスにホストされており、そのアプリケーションからバックエンド処理を実行します。バックエンド処理には別の複数のEC2インスタンスサーバーを利用して並行処理を実施することが必要です。また、データベース処理にはSQLクエリ処理が必要となります。

この要件に対応するための最も適切なアーキテクチャはどれですか？

- ◉ ELBを使用して、EC2インスタンスへのトラフィックを分散して、EC2インスタンスにAuto Scalingグループを設定して、トラフィック量増加に応じてEC2インスタンスをスケーリングする。データベースはDynamoDBを利用してグローバルテーブルを実行して、最後にRoute53のAliasレコードでELBを指定する。 (不正解)
- ○ ELBを使用して、EC2インスタンスへのトラフィックを分散して、SQSによってバックエンドタスク処理を並列化する。EC2インスタンスにAuto Scalingグループを設定して、SQSキューサイズに応じてEC2インスタンスをスケーリングする。データベースはAuroraを利用してマルチマスター構成として、最後にRoute53のAliasレコードでELBを指定する。 (正解)
- ○ ELBを使用して、EC2インスタンスへのトラフィックを分散して、EC2インスタンスにAuto Scalingグループを設定して、トラフィック量増加に応じてEC2インスタンスをスケーリングする。データベースはAuroraを利用してマルチマスター構成として、最後にRoute53のAliasレコードでELBを指定する。
- ○ ELBを使用して、EC2インスタンスへのトラフィックを分散して、SQSによりバックエンドタスク処理を並列化する。EC2インスタンスにAuto Scalingグループを設定して、SQSキューサイズに応じてEC2インスタンスをスケーリングする。データベースはDynamoDBを利用してグローバルテーブルを実行して、最後にRoute53のAliasレコードでELBを指定する。

説明

このシナリオでは、高可用なシステムを構築するためにELB／AutoScaling／Route53／RDS マルチAZ構成などの組合せによって、ダウンタイムを極力低減させるシステムアーキテクチャを設計することが求められています。この構成では、ELBによってEC2インスタンスのトラフィック負荷を分散して、SQSと別のEC2インスタンス群でバックエンド処理を並列化しています。

ELBを使用してEC2インスタンスへのトラフィックを分散できます。これにより、アプリケーションの可用性が向上します。インスタンスを複数のアベイラビリティーゾーンに配置することで、アプリケーションの耐障害性も向上します。1つのアベイラビリティーゾーンが停止した場合はトラフィックは他のアベイラビリティーゾーンにルーティングされます。

バックエンド処理用のEC2インスタンスはSQSによって並列処理を可能にします。その際にAutoScalingを設定して、SQSキューサイズに応じてスケーリングさせることが可能です。

データベース処理にはSQLクエリ処理が必要となるため、RDSやAuroraまたはRedshiftなどを利用することになります。したがって、DynamoDBは不正解です。今回は通常のRDSよりも高速処理性能が高いAuroraを選択します。設定としてマルチマスター構成を利用します。Auroraマルチマスターは複数ノードに書き込みが行える高可用性なクラスタ構成です。現在は1つのリージョン内で複数のAZに跨って構成できます。そもそもAmazon Auroraはシングルマスタ・クラスタでもSLAが99.99%を誇りますが、マルチマスター構成により更に高い可用性を期待できる構成となります。

Route53のCNAMEレコードではなくAliasレコードでELBを指定することで、DNSクエリを削減して効率的なDNS処理を行うことができます。

したがって、これらの構成に合致しているオプション２が正解となります。

オプション３は不正解です。今回の要件では、システムダウンを極力回避するために可用性と耐障害性を高める必要があり、より可用性を高めて、複数の処理を実行できるアーキテクチャを選択することが求められます。オプション３の構成も可能なアーキテクチャではありますが、より処理能力を高めて、システムダウンを極力回避することができるようにキューを利用したアーキテクチャ構成の方が優先されるため、オプション2の方が望ましい回答となります。

問題59: 不正解

あなたの会社はフィンテックベンチャー企業です。この会社では新しいタイプのAI保険を開発・販売しており、この保険をAPIで提供するアプリケーションをAWS上に構築しています。このアプリケーションはIPv4 CIDRブロック10.0.0.0/24のVPCに設置していましたが、IPアドレスが枯渇してしまいました。したがって、現在のVPC CIDR範囲を拡張するが必要です。

この要件に対応するための最も適切なアーキテクチャはどれですか？

- ◉ VPCの拡張設定を有効化することで、IPアドレス範囲を追加する。 (不正解)
- ○ 4つのセカンダリーIPv4のCIDRブロックを追加することで既存のVPCを拡張させる。 (正解)
- ○ VPCのサブネットを全て削除した上で、IPアドレス数を確保した新しいCIDRによるサブネットを設定する。
- ○ IPアドレス付きのプライベートリンク型のVPCエンドポイントを設置して、IPアドレス範囲を拡張する。

説明
VPC はAWS アカウント専用の仮想ネットワークです。 VPC を作成するときに、IPv4 アドレスの範囲を Classless Inter-Domain Routing (CIDR) ブロックの形式で指定する必要があります (例: 10.0.0.0/16)。これは VPC のプライマリ CIDR ブロックです。 VPCを作成したら、1つを最大4つのセカンダリーCIDRブロックに関連付けてVPCに追加することが可能です。これにより、ネットワークをさらに拡張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。

説明
VPC はAWS アカウント専用の仮想ネットワークです。 VPC を作成するときに、IPv4 アドレスの範囲を Classless Inter-Domain Routing (CIDR) ブロックの形式で指定する必要があります (例: 10.0.0.0/16)。これは VPC のプライマリ CIDR ブロックです。 VPCを作成したら、1つを最大4つのセカンダリーCIDRブロックに関連付けてVPCに追加することが可能です。これにより、ネットワークをさらに拡張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。

問題60: 不正解

あなたはヘルステック企業A社のエンジニアとして健康管理アプリケーションをAWS上に構築しています。このアプリケーションはELBとAutoScalingグループが設定された複数のEC2インスタンスにホストされています。機密性の高い健康記録データは、EC2インスタンスによって処理されて、EBSに保存されます。会社ではセキュリティとコンプライアンスの一環として、クラウドインフラストラクチャに保存されているすべてのデータを適切に保護および暗号化することが義務付けられており、あなたはソリューションアーキテクトとして、暗号化方式を検討しているところです。

健康管理データの暗号化方法として正し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] Amazon CloudHSMを利用して、EBSボリュームの暗号化を実施する。 (不正解)
- [x] EBSボリューム作成時にデータ暗号化を有効化する。 (正解)
- [ ] AWS KMSを利用してEBSボリュームの暗号化を実施する。 (正解)
- [ ] IAMロールを使用して、EBSボリュームへのアクセス権限を設定して、SSLによる暗号化を実施する。

説明

・Amazon EBSの暗号化 は、EBS リソースのために、独自のキー管理インフラストラクチャの構築、保守、および保護を必要としない暗号化ソリューションを提供します。EBSデータは設定で暗号化機能を有効化するだけで、データを暗号化することができます。 したがって、オプション2は正解となります。

暗号化されたボリュームとスナップショットを作成する際にKMSが使用して暗号化を実施することができます。 したがって、オプション3は正解となります。

オプション1は不正解です。Amazon CloudHSMを利用して、EBSボリュームの暗号化を実施することはできません。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。

オプション4は不正解です。IAMロールを使用して、EBSボリュームへのアクセス権限を設定して、SSLによる暗号化を実施するといった対応もできません。

問題61: 正解

あなたの会社は顧客管理用のWEBアプリケーションを運用しているソフトウェア企業です。この会社ではハイブリッドアーキテクチャを採用することになり、先だってデータベースをAmazon RDSに移行することができました。そのため、オンプレミス環境にあるWEBアプリケーションがLDAP（Lightweight Directory Access Protocol）サーバーによる認証を行いつつ、AWS上にあるAmazon RDS MySQLの顧客データにアクセスすることが必要です。

この要件を実現するために最適なアーキテクチャを選択してください。

- ○ IAMロールによってLDAPによるユーザー認証を実施し、STSから一時的なセキュリティトークンを取得し、IAMフェデレーションユーザー認証情報を使用してRDSにアクセスする。
- ◉ IDブローカーによってLDAPによるユーザー認証を実施し、STSから一時的なセキュリティトークンを取得し、IAMフェデレーションユーザー認証情報を使用してRDSにアクセスする。 (正解)
- ○ Direct ConnectとAmazon Cognitoを使用して、LDAPによるユーザー認証を実施し、STSからセキュリティトークンを取得し、一時的な資格情報を使用してRDSにアクセスする。
- ○ Simple Active Directoryを使用してユーザーを適切に認証し、STSからセキュリティトークンを取得し、一時的な資格情報を使用してRDSにアクセスする。

説明

このシナリオでは、オンプレミスのLDAP（Lightweight Directory Access Protocol）サーバーによる認証によって、AWSリソースにアクセスできるようにハイブリッド構成の認証を実現することが求められています。カスタムIDブローカーによってLDAPによるユーザー認証を実施することで、オンプレミス環境からAWSリソースにアクセス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。

LDAPを利用して認証を行っている従業員がAWSリソースにアクセスするためには、カスタムIDブローカーを設置する必要があります。カスタムIDブローカーは、従業員が会社の既存IDおよび認証システムにサインインしていることを確認します。その後、IDブローカーは、従業員の一時的なセキュリティ認証情報を取得します。一時的なセキュリティ認証情報を取得するために、STSでAssumeRoleまたはGetFederationTokenアクションを呼び出して、一時的なセキュリティ認証情報を取得し、IAMフェデレーションユーザー認証情報を使用してRDSにアクセスします。

オプション1は不正解です。IAMロールによってLDAPによるユーザー認証を実施するといった対応はできないため、正しくありません。

オプション3は不正解です。Direct ConnectとAmazon Cognitoを使用して、LDAPによるユーザー認証を実施するといった対応はできないため、正しくありません。

オプション4は不正解です。Simple Active Directoryは、Samba 4 Active Directory Compatible Serverを使用するスタンドアロンのマネージド型ディレクトリです。AWS環境にActive Directory機能を構築して、ユーザー管理に利用するものであり、オンプレミス環境との連携に用いられるものではありません。

問題62: 不正解

大手金融機関A社では複数部門でAWSアカウントを保有し、様々なAWSリソースを利用しています。あなたはIT運用部門の責任者として、複数アカウントを管理するためにAWS Organizationsを利用した統合管理・一括請求の仕組みを設定しています。組織内のすべてのリソースを適切に管理するには、すべてのアカウントでリソースが作成された際には適切なタグが追加されるようにする必要があります。

この要件を実現するために最適なソリューションを選択してください。 (3つ選択してください。)

- [x] AWS Service Catalogからデプロイされたリソースにポートフォリオ、製品、ユーザーを識別するためのタグが自動的に付与されるように設定する。 (正解)
- [x] CloudFormationテンプレート内のリソース設定に自動的に適切なタグを設定するように構成する。 (正解)
- [ ] AWS Systems Managerからデプロイされたリソースにポートフォリオ、製品、ユーザーを識別するためのタグが自動的に付与されるように設定する。
- [ ] AWS Organizationsのタグポリシーを利用して、メンバーアカウント内のタグ設定を必須化する。 (正解)
- [ ] AWS Tag Managerからデプロイされたリソースにポートフォリオ、製品、ユーザーを識別するためのタグが自動的に付与されるように設定する。

説明

AWS Service Catalogを利用すると、デプロイされたリソースにポートフォリオ、製品、ユーザーを識別するためのタグが自動的に付与されるようになります。したがって、オプション1は正解となります。

AWS Service Catalog ではAWS での使用が承認された IT サービスのカタログを作成および管理できます。この IT サービスには仮想マシンイメージ、サーバー、ソフトウェア、データベースから包括的な多層アプリケーションアーキテクチャまで、あらゆるものが含まれます。AWS Service Catalog は一般的にデプロイされた IT サービスを集中管理でき、一貫性のあるガバナンスを実現し、コンプライアンス要件を満たすと同時に、ユーザーは必要な承認済みの IT サービスのみをすばやくデプロイできます。したがって、オプション1が正解となります。

また、CloudFormationのResource Tags プロパティを使用してリソースにタグを適用し、それらのリソースの識別や分類に役立てることができます。タグを適用できるのは、AWS CloudFormation がタグ付けをサポートしているリソースのみです。したがって、オプション2が正解となります。

オプション4は正解です。AWS Organizationsのタグポリシーを利用して、メンバーアカウント内のタグ設定を統一することができます。タグポリシーを使用して、タグキーおよびタグ値の大文字と小文字の処理方法の設定など、一貫したタグを維持できます。

詳細は以下の内容をご確認ください。

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-instance.html#cfn-ec2-instance-tags

タグポリシー - AWS Organizations (amazon.com)

オプション3は不正解です。AWS Systems Managerからデプロイされたリソースにポートフォリオ、製品、ユーザーを識別するためのタグが自動的に付与されるように設定するといった対応はできません。

オプション5は不正解です。AWS Tag Managerというサービスは存在しません。

問題63: 不正解

あなたの会社は不動産情報サイトを運用する不動産テック企業です。このサイトでは仲介業者を介さずに物件の内見予約が出来る"内見くん"などのアプリケーションをAWSを利用して展開しています。このアプリケーションは２つのAZに展開された８つのEC2インスタンスによって構成されています。このアプリケーションに対して、負荷テストを実施したところ、ユーザーセッションは両方のAZのEC2インスタンスに均等に分散していましたが、負荷テストツールのトラフィックは１つのAZにあるEC2インスタンスのみを利用しており、負荷分散が遂成されていないようです。

この問題を対処するための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] ELBで利用しているスティッキーセッションの設定を非有効化することでEC2インスタンスへの負荷分散を均等化する。 (正解)
- [ ] 負荷テストツールを展開しているサーバー群に設置されているDNSをルーティング設定をクリアする。
- [x] 負荷テストツールをAWS専用のNative ツールに変更して実施する。 (不正解)
- [ ] グローバルに分散化したクライアントやサーバーからのリクエスト送信ができるサードパーティーの負荷分散テストを利用する。 (正解)

説明

このシナリオの根本的な原因は、スティッキーセッション機能によって負荷テストツールがリクエストで同じCookieを使用している可能性があることです。Cookieはルーティングするインスタンスを決定するためにELBによって使用されています。１つの方法は、ELBで利用しているスティッキーセッションの設定を非有効化することでEC2インスタンスへの負荷分散を均等化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。

スティッキーセッションを有効化したままでも、グローバルに分散化したクライアントやサーバーからのリクエスト送信ができるサードパーティーの負荷分散テストを利用することで、対処することもできます。これらの設定により、新しいリクエストごとに新しいCookieが使用され、実際にはELBがそれらを毎回異なるEC2インスタンスにルーティングします。したがって、オプション４が正解となります。

問題64: 不正解

B社ではCloudFormationを利用した環境構築の自動化を行っています。CloudFormationスタック全体の起動に失敗した場合に自動的にロールバックするCloudFormationテンプレートを準備する必要があります。要件としては、アプリケーションのスタックを適切に実行するには、最初に前提条件となるパッケージをインストールする必要があります。また、このCloudFormationの展開が完了するには約1時間ほどかかる場合があります。

この要件を満たすために、CloudFormationテンプレートに何を追加する必要がありますか？

- (●) UpdatePolicy属性のResourceSignalパラメーターで、2時間のTimeoutプロパティを追加する。 (不正解)
- ( ) UpdatePolicy属性のResourceTimingパラメーターで、2時間のTimeoutプロパティを追加する。
- ( ) CreationPolicy属性のResourceSignalパラメーターで、2時間のTimeoutプロパティを追加する。 (正解)
- ( ) CreationPolicy属性のResourceTimingパラメーターで、2時間のTimeoutプロパティを追加する。

説明

オプション3が正解となります。CreationPolicy属性をリソースに関連付けて、AWS CloudFormationが指定された数の成功シグナルを受信するか、タイムアウト期間を超えるまで、ステータスが作成完了にならないようにします。リソースに信号を送るには、cfn-signalヘルパースクリプトまたはSignalResource APIを使用できます。 AWS CloudFormationは、有効なシグナルをスタックイベントに発行するため、送信されたシグナルの数を追跡できます。CreationPolicは、AWS CloudFormationが関連付けられたリソースを作成するときにのみ呼び出されます。

オプション1と2は不正解です。UpdatePolicy 属性を使用して、AWS CloudFormationが、AWS::AutoScaling::AutoScalingGroup、AWS::ElastiCache::ReplicationGroup、AWS::Elasticsearch::Domain、またはAWS::Lambda::Alias のリソースに対する更新を処理する方法を指定できます。これは要件に合致しません。

オプション4は不正解です。CreationPolicy属性のResourceTimingパラメーターではなく、ResourceSignalパラメーターで、2時間のTimeoutプロパティを追加します。

問題65: 正解

あなたはソリューションアーキテクトとして、S3を利用したコンテンツ共有システムの仕組みを構築しています。このコンテンツ共有システムは、利用するユーザーからのアクセスに限定する必要があり、特定のIPアドレスからのみS3バケット内のオブジェクトにアクセスできるように設定することが要件となっています。

この要件を達成するためのソリューションを選択してください。

- ◉ バケットポリシーにCloudFrontのOAIを設定して、CloudFrontのWAF設定によってIP制限を実施する。 (正解)
- ○ Direct Connectにより、VPCと既存アプリケーションが実行されているオンプレミスネットワーク間でLink S3に特定IPアドレスへのアクセスに限定したセキュリティグループを設定する。
- ○ Route53によるアクセス制限をCloudFrontに対して設定することで、特定のIPアドレスからの制限を実施する。
- ○ S3の署名付きURLを利用したコンテンツ共有を実装する。

説明

オプション1が正解となります。CloudFrontのOAI機能とWAFの機能を利用することで、特定のIPアドレスのみがS3バケットにアクセスできるように制限することができます。~~OAIはオリジンアクセスアイデンティティ（OAI）と呼ばれる特別なCloudFrontユーザーです。~~これを作成し、S3バケットポリシーの利用ユーザーに設定することで、CloudFrontのみがS3バケットにアクセス可能なように構成することができます。そのうえで、CloudFrontで標準的に連携されているAWS WAFを利用して、特定のIPアドレスのみがCloudFront経由でアクセスできるように制限することができます。

オプション2は不正解です。S3にセキュリティグループを設定することはできません。

オプション3は不正解です。Route53によるアクセス制限をCloudFrontに対して設定することで、特定のIPアドレスのみに制限を実施するといった設定をすることはできません。CloudFrontはWAFと連携してアクセス制限を実施することができます。

オプション4は不正解です。S3の事前署名付きURLを作成した場合、そのURLの有効期限内での特定プロジェクトの共有ができます。これはオブジェクトの制限付き共有で利用するものです。

問題66: 不正解

ベンチャー企業ではAWSを利用してアプリケーション開発を実施しています。あなたは社内の運用担当者として、インターネットを介してVPCに接続し、パブリックサブネットとプライベートサブネットの両方で実行されている全てのEC2インスタンスを管理しています。Microsoft Remote Desktop Protocol（RDP）アクセスによるリモートアクセスを実現したいと考えていますが、EC2インスタンスへのインターネットアクセスを制限して安全なものにするため、Bastionホストを利用したインターネットアクセスを構成する必要があります。

この要件を満たすBastionホストの展開シナリオを選択してください。

- ○ EIPをBastionホストにアタッチしてパブリックサブネットに配置し、SSH接続を許可する。
- ◉ Bastionホストをパブリックサブネットに配置し、VPC内のインスタンスからのRDPアクセスを許可する。 (不正解)
- ○ Bastionホストをパブリックサブネットに配置し、会社のIPアドレスからのRDPアクセスをフルオープン（0.0.0.0/0）で許可して、（RD）ゲートウェイサーバーを設置する。 (正解)
- ○ Bastionホストをプライベートサブネットに配置し、会社のIPアドレスからのRDPアクセスを社内IPアドレスに限定して許可して、（RD）ゲートウェイサーバーを設置する。
- ○ Bastionホストをプライベートサブネットに配置し、会社内のIPアドレスからのRDPアクセスをフルオープン（0.0.0.0/0）で許可して、（RD）ゲートウェイサーバーを設置する。

説明

オプション3が正解となります。このシナリオでは、RDPによるリモートデスクトップ接続を使用して、自宅のコンピューターからオフィスのコンピューターのプログラム、ファイル、およびネットワークリソースをすべて使用できるように構成するための安全なアクセス制御が求められています。

解決策としては、Bastionホストをパブリックサブネットに配置し、会社内のIPアドレスからのRDPアクセスを許可します。そして、RDゲートウェイを利用して、インターネット上のすべてのIPからHTTPS（TCP/443）経由の接続を受け入れ、RDPポート（TCP/3389）を使用して他のWindowsインスタンスにプロキシするように構成することで、RDPアクセスを安全に制御することができます。

EC2でMicrosoft Windowsインスタンスを実行する場合、リモート管理にリモートデスクトッププロトコル（RDP）を使用します。EC2インスタンスのRDPポート（TCP/3389）への接続を許可されるソースIPを定義するには、インスタンスのセキュリティグループルールを構成します。セキュリティグループの設定時には、管理者が接続するIPアドレスからRDPポートへの接続のみを許可し、他のすべてを拒否するという最小特権の原則を適用します。

ただし、管理者がインターネットのどこからでも接続できるようにするには、許可IPを決定するのは困難であるため、すべてのIP（0.0.0.0/0）を許可するようにRDPアクセス用のセキュリティグループを設定することになります。このシナリオでは、Bastionホストを利用したインターネットアクセスを構成する設定となっており。要件にインターネットアクセスを可能にすることが必要です。そのため、社内のIPアドレスを許可する設定の際に、限定的に範囲を絞るのではなく外部のインターネットからのリモートアクセスも可能なように構成することが必要です。

しかしながら、このセキュリティグループ設定ではネットワーク層で最小限権限を構成できません。この問題の解決策の1つは、Bastionとしてセットアップされたマイクロソフトリモートデスクトップ（RD）ゲートウェイサーバーを使用して、ネットワーク層でWindowsインスタンスを保護することです。RDゲートウェイは、インターネット上のすべてのIPからHTTPS（TCP/443）経由の接続を受け入れ、RDPポート（TCP/3389）を使用して他のWindowsインスタンスにプロキシするように構成できます。RDゲートウェイインスタンスを認証するユーザーのみが、プロキシの背後にある保護されたWindowsインスタンスに進むことができます。 RDゲートウェイを構成するための基本的な手順は次のとおりです。

1．Windows EC2インスタンスを作成し、RDPアクセスを許可するセキュリティグループルールを構成します。
2．そのインスタンスにRDゲートウェイをインストールして構成します。
3．RDゲートウェイインスタンスおよび他のすべてのWindowsサーバーインスタンスでセキュリティグループを再構成して、許可する接続を制御します。
4．RDゲートウェイを介してWindowsインスタンスに接続できることを確認します。

オプション1は不正解です。EIPをBastionホストにアタッチするといった対応は必ずしも必要ではありません。また、この回答では（RD）ゲートウェイサーバーを設置する対応がなされていないなど、設定が不十分です。

オプション2は不正解です。VPC内のインスタンスからのRDPアクセスを許可するのではなく、会社内のIPアドレスからのRDPアクセスを許可することが必要です。

オプション4と5は不正解です。Bastionホストをプライベートサブネットではなく、パブリックサブネットに配置してプロキシサーバーとして機能させる必要があります。

問題67: 正解

B社はグローバルに展開しているEコマースサイトを運営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インスタンスを設置しています。社内のコンプライアンス規定に適合するためには、B社では世界中のリージョンに展開されたEC2インスタンス全てのパフォーマンスを監視する必要があります。

複数リージョンのEC2インスタンスを監視するためにCloudWatchをどのようにセットアップしますか？

- ◉ 異なる複数リージョンからのメトリクスを単一のCloudWatchにより取得して、一つのダッシュボードに表示させる。 (正解)
- ○ 各リージョンにCloudWatchを設定して、取得したメトリクスをAWS Organizationsで設定したマスターアカウントのダッシュボードに表示する。
- ○ 異なる複数リージョンからのメトリクスを単一のCloudWatchにより取得して、取得したメトリクスをAWS Organizationsで設定したマスターアカウントのダッシュボードに表示する。
- ○ 異なる複数リージョンからのメトリクスを複数のCloudWatchの設定により取得して、メインとなる一つのダッシュボードに表示させる。

説明

オプション1が正解となります。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。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ように設定します。

・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。

問題68: 不正解

あなたはソリューションアーキテクトとして、社内用モバイルで閲覧できるデータ共有システムをAWS上に構築しています。このシステムは、ユーザーが直接アップロードしたデータを単一のAmazon S3バケットに保存し、ユーザーはAmazon S3バケットから直接自分がアップロードしたデータをダウンロードすることができます。1万人ものユーザーが存在するため、データにアクセスする際に一時的に、可能な限り安全にデータにアクセスできる必要があります。

このモバイルアプリのユーザー登録フローにおけ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] IAMロールを作成してアクセスキーを利用できるようにする。作成したアクセスキーを利用しモバイルアプリに対する一時利用資格を作成する。これらの資格情報はモバイルアプリのメモリ内に保存され、S3へのアクセスに利用される。 (不正解)
- [x] IAMロールを作成して許可設定を与える。モバイル向けのAmazon CognitoからSTSを実行することで、モバイルアプリに対する一時利用資格を作成する。これらの資格情報はモバイルアプリのメモリ内に保存され、S3へのアクセスに利用される。 (正解)
- [ ] KMSを利用した認証キーを作成して許可設定を与える。モバイル向けのAmazon Cognitoを利用してモバイルアプリに対する一時利用資格を作成する。これらの資格情報はモバイルアプリのメモリ内に保存され、S3へのアクセスに利用される。
- [ ] IAMロールを作成して許可設定を与える。STS AssumeRoleを利用してモバイルアプリに対する一時利用資格を作成する。これらの資格情報はモバイルアプリのメモリ内に保存され、S3へのアクセスに利用される。 (正解)

説明

システムのセキュリティを高める最適な認証方法はIAMロールとSTSを組み合わせて使用することです。STS AssumeRoleは、通常はアクセスできないAWSリソースにアクセスする一時的なセキュリティ認証情報のセットを返します。これらの一時的な資格情報は、アクセスキーID、シークレットアクセスキー、およびセキュリティトークンで構成されます。通常、クロスアカウントアクセスまたはフェデレーションにはAssumeRoleを使用します。

このシナリオでは、適切なアクセス許可でIAMロールを作成し、STS AssumeRoleを使用して一時的なセキュリティ認証情報を生成することが求められるため、オプション4が正しい内容です。

Amazon Cognito を利用することで、ウェブアプリケーションやモバイルアプリケーションのユーザー認証、許可、管理ができます。ユーザーは、ユーザー名とパスワードを使用して直接サインインするか、Facebook、Amazon、Google などのサードパーティーを通じてサインインできます。Amazon CognitoからSTS AssumeRoleを呼び出すAPIコールによって、一時利用資格を取得することが可能です。したがって、オプション2も正解となります。

オプション1は不正解です。アクセスキーを利用してモバイルアプリに対して一時利用資格を作成するといった対応はできません。アクセスキーはあくまでもIAMユーザー側がEC2インスタンスなどにアクセスする際に利用する方式であり、実装したアプリケーションのユーザー管理に利用する仕組みではありません。

オプション3は不正解です。KMSを利用した認証キーを作成して許可設定を与えるのではなく。RDSにユーザー情報を蓄積して、IAMロールを作成して許可設定を与えることが必要です。

問題69: 不正解

金融機関の決済システムは、同じアベイラビリティゾーン（AZ）の2つの異なるサブネットに対して設置された、2つのEC2インスタンス群にホストされます。1つのEC2インスタンス群はデータベースを実行しており、もう1つのEC2インスタンス群はデータベースからデータを取得するWebサーバーとして機能しています。このWEBアプリケーションが正しく機能するためには、各EC2インスタンス群内の通信パフォーマンスを最適にした上で、EC2インスタンス群間で相互に接続できることを確認する必要があります。また、インスタンスに関連付けられたセキュリティ構成の変更履歴を追跡する必要があります。

次の仕組みの中で、どれがこの要件を満たすことができますか？

◉ 各インスタンス群においてパーティションプレイスメートグループを設定してインスタンス間の通信処理を最適化した上で、インスタンスの拡張ネットワークを有効化する。ネットワークACLにより2つのサブネット間の通信を可能にして、セキュリティグループの設定によって、適切なインスタンス間の処理が行えるように設定する。その上で、CloudWatchエージェントをインストールしてEC2インスタンスへのセキュリティ構成に関わる変更履歴を追跡可能とする。 (不正解)

○ 各インスタンス群においてパーティションプレイスメートグループを設定してインスタンス間の通信処理を最適化した上で、インスタンスの拡張ネットワークを有効化する。ネットワークACLにより2つのサブネット間の通信を可能にして、セキュリティグループの設定によって、適切なインスタンス間の処理が行えるように設定する。その上で、NATインスタンスとインターネットゲートウエイに対するルーティング設定を適切なものにして、その中のセキュリティ構成の変更履歴追跡をオンに設定する。

○ 各インスタンス群においてクラスタープレイスメートグループを設定してインスタンス間の通信処理を最適化した上で、インスタンスの拡張ネットワークを有効化する。ネットワークACLにより2つのサブネット間の通信を可能にして、セキュリティグループの設定によって、適切なインスタンス間の処理が行えるように設定する。その上で、AWS Configを利用してEC2インスタンスへのセキュリティ構成に関わる変更履歴を追跡可能とする。 (正解)

○ 各インスタンス群においてクラスタープレイスメートグループを設定してインスタンス間の通信処理を最適化した上で、インスタンスの拡張ネットワークを有効化する。ネットワークACLにより2つのサブネット間の通信を可能にして、セキュリティグループの設定によって、適切なインスタンス間の処理が行えるように設定する。その上で、CloudWatchエージェントをインストールしてEC2インスタンスへのセキュリティ構成に関わる変更履歴を追跡可能とする。

説明

このシナリオでは、各インスタンス群内での通信最適化、インスタンス群間のので通信許可の設定、インスタンスのセキュリティ構成管理という3つの対応が求められています。

インスタンス群内での通信最適化については、プレイスメントグループを設定します。プレイスメントグループ内のインスタンスを起動して、低レイテンシグループに論理的にクラスタリングするか、ハードウェア全体に分散して同時障害のリスクを低減します。クラスタープレイスメントグループは、単一のアベイラビリティーゾーン内のインスタンスを論理的にグループ化したものです。クラスタープレイスメントグループは、同じリージョン内の複数のピア VPC にまたがることができます。同じクラスタープレイスメントグループ内のインスタンスは、TCP/IP トラフィックのフローあたりのスループット上限が高くなり、ネットワークの二分帯域幅の広い同じセグメントに配置されます。

また、拡張ネットワークは高い帯域幅、1秒あたりのパケット (PPS) の高いパフォーマンス、一貫して低いインスタンス間レイテンシーを実現します。

インスタンス群間のので通信許可の設定には、セキュリティグループとネットワークACLを設定します。セキュリティグループはインスタンスのインバウンドおよびアウトバウンドトラフィックを制御し、ネットワークACLはVPCとサブネットのインバウンドおよびアウトバウンドトラフィックを制御します。2つのサブネット間通信の設定はネットワークACLを利用することが最適です。一方でセキュリティグループはインスタンスへのアクセス制御に用いられます。これによって適切なインスタンス間の通信を制御することが可能です。

インスタンスのセキュリティ構成の管理にはAWS Configを利用します。 AWS Config は、AWS リソースの設定を評価、監査、審査できるサービスです。Config では、AWS リソースの設定が継続的にモニタリングおよび記録され、望まれる設定に対する記録された設定の評価を自動的に実行できます。Config を使用すると、AWS リソース間の設定や関連性の変更を確認し、詳細なリソース設定履歴を調べ、社内ガイドラインで指定された設定に対する全体的なコンプライアンスを確認できます。これにより、コンプライアンス監査、セキュリティ分析、変更管理、運用上のトラブルシューティングを簡素化できます。

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と２は不正解です。パーティションプレイスメントグループは、アプリケーションに関連するハードウェア障害の頻度を軽減するための機能であり、要件に合致しません。パーティションプレイスメントグループを使用する場合、Amazon EC2 は各グループをパーティションと呼ばれる論理的なセグメントに分割します。Amazon EC2 では、プレイスメントグループ内の各パーティションにそれぞれ一連のラックがあります。各ラックには独自のネットワークおよび電源があります。プレイスメントグループ内のパーティション同士が同じラックを共有することはありません。これにより、アプリケーション内でのハードウェア障害による影響を隔離できます。また、NATインスタンスとインターネットゲートウエイに対するルーティング設定には、セキュリティ構成の変更履歴追跡といった機能はありません。

オプション４は不正解です。CloudWatchエージェントをインストールしてEC2インスタンスへのセキュリティ構成に関わる変更履歴を追跡可能とすることはできません。CloudWatchエージェントをインストールすると、詳細なログ情報を取得することができるようになります。

問題70: 不正解

アメリカに本社を持つメディア企業A社は、グローバルにニュースを配信している英語ニュースサイトをAWS上で運用しています。各記事には多数の画像が含まれ、そのコンテンツは少なくとも200語以上あります。新しい記事は最初の1か月間で最も閲覧されており、記者は公開後最初の1か月間は頻繁に記事を更新する傾向があります。このデータベースにはRDS MySQLを利用しており、ニュース記事のデータ処理にはクエリ処理が多数利用されるため、リレーショナルモデルが必要不可欠です。最近になって、このニュースメディアの利用者が急増しており、コンテンツの読込時間が長いというクレームが発生するようになりました。

この問題を解決するために最も効果的な高パフォーマンスなソリューションの仕組みを選択してください。

- ◉ RDSからmysqlimportコマンドで移行ファイルを作成し、それを利用してAuroraデータベースエンジンで再度DBをAuroraベースで起動しなおす。その上で、AuroraをマルチAZに展開して、15個のリードレプリカを起動させることで、データ処理性能を向上させる。また、CloudFrontによる配信処理を設定する。 (不正解)
- ○ RDSからスナップショットを取得して、それを利用してAuroraデータベースエンジンで再度DBをAuroraベースで起動しなおす。その上で、AuroraをマルチマスタクラスターでRDSに展開して15個のリードレプリカを起動させることで、データ処理性能を向上させる。また、CloudFrontによる配信処理を設定する。定する。
- ○ DynamoDB（DAX）の高速データ処理をリレーショナルデータベースの前面に配置する。その上で、マルチAZ展開とDynamoDBオートスケールを有効化することで、データ処理性能を向上させる。また、CloudFrontによる配信処理を設定する。
- ○ RDSからスナップショットを取得して、それを利用してAuroraデータベースエンジンで再度DBをAuroraベースで起動しなおす。その上で、AuroraをマルチAZに展開して15個のリードレプリカを起動させることで、データ処理性能を向上させる。また、CloudFrontによる配信処理を設定する。 (正解)

説明

このシナリオの要件はWebサイトを最も効果的で高パフォーマンスなアーキテクチャを提供することで。そのため、既存のRDSではなく、より大規模に構成できて高速性能を担保できるAuroraを利用することが最適です。Auroraをマルチ AZ構成でリードレプリカを最大15個まで利用する構成によって、毎月数百万の接続トラフィックにスケーラビリティと高可用性を提供できます。RDS MySQLからの移行方法は容易で、スナップショットからの復元時にデータベースエンジンをAuroraに指定して起動することだけです。

このニュースサイトは画像を多く含んだニュースをグローバルに配信しています。そのため、S3バケットを使用して、Webサイトの画像やその他の静的メディアコンテンツを永続的に保存しつつ、CloudFrontをCDNとして使用してグローバルな配信を効率的に実施できるようにすること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。

オプション１は不正解です。RDSからAuroraへの移行はスナップショットによって実行します。mysqlimportコマンドで移行ファイルを作成することは必要ありません。

オプション３は不正解です。Auroraをマルチマスタクラスターで展開した場合はリードレプリカを利用することができません。マルチマスタークラスターのアーキテクチャは、他の種類の Aurora クラスターとは異なります。マルチマスタークラスターでは、すべての DB インスタンスに読み書き機能が備わっています。他の種類の Aurora クラスターには、すべての書き込みオペレーションを実行する単一の専用 DB インスタンスがありますが、他の DB インスタンスはすべて読み取り専用で、 SELECT クエリのみを処理します。マルチマスタークラスターには、プライマリインスタンスまたは読み取り専用の Aurora レプリカはありません。

オプション３は不正解です。DynamoDBではなくElastiCacheを前面に配置することで集中的なキャッシュ処理を高速で実行することが可能となり、それによりRDSの処理を低減させることができます。また、リレーショナルデータベースが必要となっており、DynamoDBのDAXを利用した処理は今回は不適切です。

【参照】

Aurora マルチマスタークラスターを使用する - Amazon Aurora

問題7: 不正解

Fintech企業B社はビットコインなどの仮想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。取引実行データの分析においてRedshiftクラスターを実行しています。あなたはソリューションアーキテクトとして、Redshiftの災害対応の構成を検討しています。要件は以下の通りです。

・リージョン内の１つのAZが停止した際に即時に対応できる構成とする。
・リージョン自体が停止した際は1日で回復できる構成とする。

このRedshiftクラスターの回復ニーズに合致した最適な構成を選択してください。（２つ選択してください。）

- [x] 自動スナップショットを有効化して、プライマリーのRedshiftクラスターから自動スナップショットコピーを実施し、DR用Redshiftクラスターへと適用する。 (正解)
- [x] Redshiftクラスターのマルチ AZ構成を有効化する。 (不正解)
- [ ] Redshiftクラスターの構成を別リージョンにレプリケーションして、フェールオーバーを実現する。
- [ ] Redshiftクラスターの構成を別リージョンにレプリケーションして、Route53を利用したフェールオーバールーティングを実施する。
- [ ] ２つの Amazon Redshift データウェアハウスクラスターをそれぞれ別のアベイラビリティーゾーンに配置し、同じ Amazon S3 入力ファイルセットからデータをロードする。 (正解)

説明
オプション１が正解となります。リージョンの停止障害に対しては、自動スナップショットを有効化して、プライマリーのRedshiftクラスターから自動スナップショットコピーを実施し、別リージョンにコピーしておくことで、障害が発生した際にそのスナップショットからRedshiftを復元すれば数十分～数時間で復元することができます。したがって、目標となる回復性を達成できます。

Amazon Redshift は前回のスナップショット以降にクラスターに加えられた増分変更を追跡する、増分スナップショットを自動的に作成します。自動スナップショットは、スナップショットからクラスターを復元するために必要なすべてのデータを保持します。自動スナップショットをいつ作成するかを制御するためにスナップショットスケジュールを作成できます。また、いつでも手動スナップショットを作成することもできます。これにより、プライマリーのRedshiftクラスターから自動スナップショットコピーを実施し、DR用Redshiftクラスターへと適用することができます。

オプション５は正解となります。Amazon Redshift はシングル AZ 配置のみをサポートしています。データウェアハウスクラスターを複数のアベイラビリティーゾーンで運用するには、２つの Amazon Redshift データウェアハウスクラスターをそれぞれ別のアベイラビリティーゾーンに配置し、同じ Amazon S3 入力ファイルセットからデータをロードすることが必要です。

オプション２は不正解です。Amazon Redshift はシングル AZ 配置のみをサポートしています。Redshiftの機能としてのマルチAZ構成はできないため、正しくありません。

オプション３は不正解です。Redshiftクラスターは、その構成を別リージョンにレプリケーションして、フェールオーバーを実現することができませんが、同一リージョン内の新規アベイラビリティーゾーンに対して既存のスナップショットを復元することができます。最も高い頻度でアクセスされるデータが最初に復元されるため、可能な限り速やかにクエリの実行を再開できます。

オプション４は不正解です。RedshiftクラスターはRoute53を利用したフェールオーバールーティングを実施することができません。

問題72: 不正解

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

この問題を解決するために最適なソリューションを選択してください。

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

説明

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

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

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

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

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

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

問題73: 不正解

金融機関C社はフィンテック企業として、様々な新金融サービスを展開しています。現在、あなたが開発しているオンライン決済プラットフォームは、Auto ScalingグループとELBを設定したEC2インスタンスにホストされています。運用においてはAWS Systems Managerを使用してEC2インスタンスグループを監視し、運用タスクを処理することになりました。これらのインスタンスにメンテナンスやOSパッチなどのパッチ操作がある場合は、Systems Managerを使用してこれらのアクティビティを自動的に実施する設定が必要です。

EC2インスタンスに対してSystems Managerの自動化で実行できるタスクを選択してください。（2つ選択してください。）

- [x] Systems Managerのステップファンクション機能によるワークフローを構成する。 (不正解)
- [x] AWS Systems Managerエージェントにタスクスクリプトを定義して、EC2インスタンスにインストールする。 (不正解)
- [ ] Systems Manager Automationを利用して自動化ワークフローを構成する。 (正解)
- [ ] AWS Systems Managerエージェントから取得した情報をCloudwatchログに連携して、自動化タスクとワークフローに関する通知を受け取る
- [ ] Systems Managerコンソールで自動化の進行状況と実行の詳細を監視して、Amazon EventBridgeを使用して自動化タスクとワークフローに関する通知を受け取る (正解)

説明

オプション3が正解となります。Systems Manager Automationは、Amazon EC2インスタンスおよび他のAWSリソースの一般的なメンテナンスとデプロイのタスクを簡素化します。自動化ワークフローを構築して、インスタンスおよびAWSリソースを設定し、管理します。独自のカスタムワークフローを作成するか、またはAWSによって管理された定義済みのワークフローを使用します。

【実施できる主なタスク】

・Amazon EventBridge を使用して自動化タスクおよびワークフローに関する通知を受信します。
・Amazon EC2 または AWS Systems Manager コンソールを使用して、自動化の進捗状況および実行の詳細を監視します。
・Systems Manager オートメーションドキュメントは、オートメーションワークフロー（Systems Manager がマネージドインスタンスおよび AWS リソースで実行するアクション）を定義します。
・自動化には、いくつかの自動化ドキュメントが事前に定義されており、1つ以上のAmazon EC2 インスタンスの再起動や、Amazon マシンイメージ (AMI) の作成といった一般的なタスクを実行する際に使用することができます。

オプション5が正解となります。Systems Managerコンソールで自動化の進行状況と実行の詳細を監視して、Amazon EventBridge を使用して自動化タスクとワークフローに関する通知を受け取る設定を実施できます。インスタンスのメトリクスとログを収集するには、SSM エージェントを使用する代わりに、Amazon CloudWatch エージェントを設定します。SSM エージェントよりも CloudWatch エージェントを使用したほうが、Amazon EC2 インスタンスのメトリクスを多く収集できます。また、CloudWatch エージェントを使用すると、オンプレミスのサーバーからもメトリクスを収集できます。

オプション1は不正解です。Systems Managerのステップファンクション機能というものは存在しないため、正しくありません。

オプション2は不正解です。AWS Systems Managerエージェントにタスクスクリプトを定義することはできません。AWS Systems Manager エージェント (SSM エージェント) は、Amazon EC2 インスタンス、オンプレミスサーバー、または仮想マシン (VM) にインストールして設定することができる Amazon のソフトウェアです。SSM エージェントにより、Systems Manager がこれらのリソースを更新、管理、および設定できるようにします。エージェントは、AWS クラウド上の Systems Manager サービスからのリクエストを処理し、リクエストに指定されたとおりに実行します。

オプション4は不正解です。AWS Systems Manager エージェントから取得した情報をCloudwatchログではなく、Amazon EventBridge を使用して自動化タスクとワークフローに関する通知を受け取る構成を作ることができます。

問題74: 不正解

大手商社では海外展開に向けて、AWSの既存リソースの一部を別リージョンに移行する対応を行っています。まず実行すべきタスクは、すべてのAmazon Machine Image（AMI）を東京リージョンからシンガポールリージョンにコピーすることです。しかしながら、AMIをコピーするだけでは該当EC2インスタンスにアクセスすることができません。シンガポールリージョンに向けてコピーされたAMIを起動する際に、最適なPEMキーを指定して起動することが必要となります。この会社では管理方針としてPEMキーを単一のキーで一元的に利用することが求められています。

AMIがリージョン間でPEMキーを共有する方式はどれでしょうか？（2つ選択してください。）

- [x] OSなどのライセンス認証情報はAMIによってリージョン全体にコピーされるが、PEMキーはコピーされないため、AWS CLIを利用してPEMキーをインポートする必要がある。 (正解)
- [x] AMIを別リージョンにコピーをするとPEMキーもコピーされるが、その認証キーを改めて設定する必要がある。 (不正解)
- [ ] OSなどのライセンス認証情報がAMIに含まれているため、AMIを別リージョンにコピーをするとPEMキーもコピーされる。
- [ ] OSなどのライセンス認証情報はAMIによってリージョン全体にコピーされるが、PEMキーはコピーされないため、EC2コンソールを利用してPEMキーをインポートする必要がある。 (正解)
- [ ] OSなどのライセンス認証情報とともにPEMの認証情報はAMIによってリージョン全体にコピーされるが、PEMキーが使えるようにAWS CLIによるアクティベイトの設定が必要である。

説明

オプション１と４が正解となります。利用するOSなどのライセンス認証情報はAMIに含まれているため、AMIの内容はリージョン全体にコピーされます。ただし、その際にPEMキーはコピーされないため、別途明示的にインポートする必要があります。AWSコンソールまたはAWS CLIを利用することでPEMキーを別リージョンにコピーすることができます。

Amazon EC2 において既に利用しているPEMキーやサードパーティー製のツールにより生成したパブリックキーを Amazon EC2 にインポートすることができます。たとえば、**ssh-keygen** (標準 OpenSSH インストールで提供されるツール) を使用して、キーペアを作成できます。また、Java、Ruby、Python などのさまざまなプログラミング言語では、RSA キーペアの作成に使用できる標準ライブラリが提供されています。

以下の形式がサポートされています。

- OpenSSH パブリックキー形式
- Base64 でエンコードされた DER 形式
- SSH パブリックキーファイル形式 (RFC4716 で指定)
- SSH プライベートキーファイルの形式が PEM である必要があります (たとえば、`ssh keygen -m PEM` を使用して、OpenSSH キーを PEM 形式に変換)。
- RSA キーを作成します。Amazon EC2 では DSA キーは使用できません。
- サポートされている長さは 1024、2048、および 4096 です。

したがって、この機能を利用して、現在利用している PEMキーをインポートして別リージョンで利用することが可能です。

詳細は以下のページをご覧ください。

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-key-pairs.html#how-to-generate-your-own-key-and-import-it-to-aws

https://docs.aws.amazon.com/ja_jp/AWSEC2/latest/UserGuide/ec2-key-pairs.html#how-to-generate-your

問題75: 不正解

あなたの会社はAWSでアプリケーションをホストして社内システムとして利用しています。セキュリティ強化の一環として、全てのVPCに侵入検知・防止システムを実装することが必要となりました。このシステムにはVPC内で実行されている数百にも及ぶインスタンスを拡張できる機能が必要であり、現在会社ではVPCを12個も利用しているため、すべてのVPCのトラフィックを監視する効率的な方法が不可欠となります。

上記の要件を満たすために、どのようにソリューションを設計する必要がありますか？（2つ選択してください）

- [x] 監視ソフトウェアを使用してインスタンスを構成し、Elastic ネットワークインターフェイス (ENI) をプロミスキャスモードパケットスニッフィングに設定して、VPC 全体のトラフィックを確認する。 (不正解)
- [x] AWS Transit Gatewayを導入して、各VPCのコネクションをまとめる。その上で、スケーラブルな仮想化 IDS/IPS プラットフォームを設置する。このAWS Transit Gatewayに集約される全トラフィックをルーティングを AWS Transit Gateway network managerを利用して、侵入検知・防止システムと連携する。 (不正解)
- [ ] AWS Transit Gatewayを導入して、各VPCのコネクションをまとめる。その上で、スケーラブルな仮想化 IDS/IPS プラットフォームを設置する。このAWS Transit Gatewayに集約される全トラフィックをルーティングを IDS/IPS を利用してして検査する。 (正解)
- [ ] すべてのネットワークトラフィックを収集するエージェントを各VPCに構成して、そのトラフィックを IDS/IPS プラットフォームに送信して検査を行う。
- [ ] トラフィックを集約する検査用VPC を作成し、AWS Network Firewall を設置する。この VPC を使用して、プライマリアプリケーション VPC からの全トラフィックをルーティングして検査する。 (正解)

説明

オプション 3 が正解となります。AWS Transit Gateway を利用して、多数のVPCのトラフィックを管理することができます。AWS Transit Gateway によって中央のゲートウェイからネットワーク上にある Amazon VPC、オンプレミスのデータセンター、リモートオフィスそれぞれに単一の接続を構築して管理することができます。Transit Gateway がハブの役割を果たし、トラフィックがスポークのように接続されたネットワーク間をどのようにルーティングするか等をすべて制御することが可能となります。

AWS Transit Gateway では統計とログが提供されます。これらは、Amazon CloudWatch や Amazon VPC フローログなどのサービスで使用することが可能です。そして、トランジットゲートウェイをファイアウォールまたは IPS（侵入防止システム）に接続したり、ネットワークのすべての入出力トラフィックを処理する単一の VPC を作成することもできます。

オプション 5 が正解となります。AWS Network Firewall を使用すると、カスタマイズしたルールを実装して、VPC が不正ドメインにアクセスするのを防ぐことができます。また、何千もの既知の危険な IP アドレスをブロックしたり、シグニチャベースの検出を使用して、悪意のあるアクティビティを特定したりできます。Network Firewallには、以下のように複数のデプロイモデルがあります。

- 分散型：個々のVPCにデプロイするモデル
- 集約型：East-West（VPCからVPC）やNorth-South（インターネットやオンプレミスへの通信）のトラフィックを集約する検査用VPCにデプロイするモデル
- 複合型：上記モデルの組み合わせ。例として、インターネットからVPC内への通信は個々のVPCにデプロイしたNetwork Firewallで検査、VPC同士の通信は検査用VPCにデプロイした Network Firewallで検査するようなモデル

したがって、集約型モデルを利用してトラフィックを集約する検査用VPC を作成し、AWS Network Firewallを設置することで、この VPC を使用して、プライマリアプリケーション VPC からの全トラフィックをルーティングして検査することが可能となります。

オプション 1 は不正解です。プロミスキャスモードはAWSではサポートされていないため、正しくありません。

オプション 2 は不正解です。AWS Transit Gateway network manager は、ネットワークトポロジーの変更、ルーティングの更新、接続ステータスの更新に関する組み込みイベント通知を提供します。これらのイベントは CloudWatch Events を通じて配信されます。これは侵入防止システムとは機能が異なるため間違いです。

オプション 4 は不正解です。すべてのネットワークトラフィックを収集するエージェントはスケーラブルなソリューションではないため、VPC内で実行されているインスタンスを拡張可能とするといった要件にあっていないため不正解です。

【参照】

AWS Network Firewallのデプロイモデル | Amazon Web Services ブログ