問題41: 不正解

あなたはソリューションアーキテクトとして、AWS開発タスクを受託しています。現在担当している大手製造企業から、全ログストリーム、アクセスログ、アプリケーションログ、およびセキュリティログを単一のシステムにて統合管理する仕組みを作ってほしいと依頼されました。要件としては、これらのログを継続的に取得しリアルタイムでログ解析を実施することができる必要があります。

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] Kinesis ログを設定してデータを収集し、Amazon Kinesis Data Firehoseを使用してエンドツーエンドのデータ配信ストリームを作成する。 (不正解)
- [x] KCL Workersを設定してデータを収集し、Amazon Kinesis Data Firehoseを使用してエンドツーエンドのデータ配信ストリームを作成する。 (不正解)
- [ ] Kinesis Agent を設定してデータを収集し、Amazon Kinesis Data Firehoseを使用してエンドツーエンドのデータ配信ストリームを作成する。 (正解)
- [ ] Amazon Kinesis Data Analytics で SQL クエリを使用して、受信ログデータを分析する。 (正解)
- [ ] Amazon EMRで SQL クエリを使用して、受信ログデータを処理する。EMR から処理済みデータをロードして、可視化を実施する。

説明

Amazon Kinesisを使用すると、リアルタイムのストリーミングデータの収集、処理、分析をする仕組みを構築することができます。これによって、ログなどのデータ解析に関してタイムリーな洞察を得て、新しい情報にすばやく対応できます。

このシナリオではEC2インスタンスにKinesis Agent を設定してデータを収集するアプリケーションを構築して、Amazon Kinesis Data Firehoseを使用してエンドツーエンドのデータ配信ストリームを作成します。その上で、Amazon Kinesis Data Analytics で SQL クエリを使用してリアルタイム分析を実施することができます。したがって、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。Kinesis ログではなく、Kinesis Agent を設定してデータを収集できるようにします。

オプション2は不正解です。KCL Workersではなく、Kinesis Agent を設定してデータを収集できるようにします。

オプション5は不正解です。Amazon EMRによってログ解析を実施することは可能ですが、EMRは一般的なSQL クエリを使用した分析には向いていません。また、ログデータを処理する前に、ログデータを収集する仕組みを構築する必要があります。

問題42: 正解

あなたは大手製造業のソリューションアーキテクトとしてAWSインフラの管理を担当しています。この会社では部署ごとにAWSアカウントを有しており、AWS Organizationsによる複数アカウントの統合管理をしています。新規案件として、AWSアカウントAのAWSリソースが、AWSアカウントBが所有するAmazon S3などのいくつかのAWSリソースにアクセスする機能を開発しています。その際は、リソース共有の許可設定や、信頼できるアカウントのみで作業できるような権限制御をする仕組みが必要不可欠となります。

このシナリオを実現する上で、必要となるポリシー設定はどれでしょうか？

- ◉ リソースベースのポリシーのクロスアカウントアクセス (正解)
- ○ ユーザーベースのポリシーのクロスアカウントアクセス
- ○ サービスコントロールポリシーのクロスアカウントアクセス
- ○ サービスベースのポリシーのクロスアカウントアクセス

説明

オプション1が正解となります。Amazon S3などのいくつかのAWSリソースに対して、他のアカウントからのアクセス権限を提供するためには、リソースベースポリシーのクロスアカウントアクセスを設定します。

一部のAWSサービスはリソースに対するクロスアカウントアクセス許可を付与できます。これを行うには、プロキシとしてロールを使用する代わりに、共有するリソースに直接ポリシーをアタッチします。共有するリソースは、リソースベースのポリシーをサポートしている必要があります。ユーザーベースのポリシーとは異なり、リソースベースのポリシーでは、誰がリソースにアクセスできるかをAWSアカウントID番号を指定します。

具体的にはAmazon S3バケットではリソースベースのポリシーとして、バケットポリシーが利用されています。リソースベースのクロスアカウントポリシーを利用することで、プリンシパルとしてのアクセス許可をAWSアカウントに付与した後、AWSアカウントに属している特定のユーザーやグループにアクセス許可を委任できます。

オプション2は不正解です。ユーザーベースのポリシーのクロスアカウントアクセスではなく、リソースベースのポリシーを利用します。ユーザーベースのポリシーとは異なり、リソースベースのポリシーでは、誰がリソースにアクセスできるかをAWSアカウントID番号で指定することが可能です。

オプション3は不正解です。サービスコントロールポリシーは組織（OU）単位でのリソースに対するアクセス許可と拒否を設定することができますが、他のアカウントへのアクセス許可を提供する設定はできません。

オプション4は不正解です。サービスベースのポリシーという概念はなく、リソースベースのポリシーにクロスアカウントアクセスを設定します。

問題43: 不正解

あなたは大手製造業のソリューションアーキテクトとしてAWSインフラの管理を行っています。この会社では部署ごとにAWSアカウントを有しているため、複数のAWSアカウントで起動される様々なAWSリソースが多岐にわたって存在しており、リソース管理が適切に出来ていないことが問題となっています。例えば、起動しているEC2インスタンスがどのユーザーやグループで利用されているかなどが整理できて[redacted]ん。一部タグが利用されており、把握できるリソースもありますが、全てのリソースにタグが設定されているわけではないようです。今後は全部門がEC2およびEBSボリュームなどのAWSリソースに対してタグを付与することで、リソースの所属を明確化できるように規則を作る必要があります。

最小限の労力でこのタグ戦略をどのように実現するべきでしょうか？

- ◉ AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定する。タグポリシーで必要なタグの有無や利用するべきタグ文字の標準化を設定して、各OUに適用する。 (不正解)
- ○ AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定する。タグポリシーで必要なリソース制御を設定した上で、OUメンバーアカウント内のユーザーに付与された既存のIAMポリシーを修正して、ForAllValues修飾子を使用して、OUごとにタグ付けを要求する設定とする。
- ○ AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定する。次に既存のSCPを修正して、aws：TagKeys修飾子を使用してOUごとにタグ付けを要求する設定として、そのSCPと関連付けたIAMポリシーを全てのOUに適用する。
- ○ AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定する。タグポリシーを設定して、OUメンバーアカウントに対してタグ作成を規則化する。
- ○ AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定する。SCPで必要なリソース制御を設定した上で、OUメンバーアカウント内のユーザーに付与された既存のIAMポリシーを修正して、ForAllValues修飾子を使用しOUごとにタグ付けを要求する設定とする。 (正解)

説明

オプション５が正解となります。IAMポリシーに条件を適用することで、EC2インスタンスとEBSボリュームなど特定のリソースを作成する際に、タグ付けを必須化することができます。

AWS Organizationsを使用すると、すべてのAWSアカウントを統合して、ビジネスユニットを個別の組織ユニット（OU）にグループ化できます。OUに属するメンバーアカウント内のユーザーは既存のIAMポリシーを修正して、ForAllValues修飾子を使用しOUごとにタグ付けを要求することが可能です。ForAllValues修飾子を使用してポリシー上定義されているすべてのタグを適用する場合にのみ、ユーザーがEC2インスタンスを起動してEBSボリュームを作成できるようにIAMポリシーを設定できます。ユーザーがポリシーに含まれていないタグを適用すると、アクションは拒否されます。

オプション１は不正解です。タグポリシーによりルールを標準化することはできても、タグ付けを強制する設定ではないので、特定のタグ付けを強制したい場合はIAMポリシー側で設定することになります。AWS Organizationsを利用して、AWSアカウントを持つ全部門をOUとして設定して、タグポリシーで必要なタグの有無や利用するべきタグ文字の標準化ができます。

オプション２は不正解です。タグポリシーではなく、SCPで必要なリソース制御を設定することが必要です。

オプション３は不正解です。さらにタグ情報に大文字と小文字を区別するには、条件aws：TagKeysを使用しますが、これは必須ではありません。

オプション４は不正解です。AWS Organizations タグポリシー はAWSサービスが生成する各リソースに付与可能な タグの標準化 を各AWSアカウントに規則化します。しかしながら、これはタグの記載方法を準拠させることができますが、タグを利用しないことを防ぐことができません。

問題44: 不正解

あなたの会社ではAWSにホストされた営業支援アプリケーションの開発しています。このアプリケーションは社内の営業活動を記録するWEBアプリケーションとなっており、営業担当者は外出先からインターネット経由で、AWS内のプライベートネットワーク内に配置されたアプリケーションにアクセスして、営業記録などをタイムリーに記録してシェアすることが必要となります。あなたは導入担当者として、アプリケーションサーバーをホストするEC2インスタンスがインターネットにパブリックに公開されないようにしつつ、このような外部アクセスを可能にするソリューション導入を行っています。

この要件を満たすことができる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。

- ◉ VPCにパブリックサブネットを設置しアプリケーションを展開して、アプリケーション内のサブネット内へのアクセスをネットワークACLによって規定する。IAMポリシーによって従業員が認証されると、オンラインポータルへのアクセスが許可される。 (不正解)
- ○ VPN接続によってAWSとオンプレミス環境をセキュアな接続を実施し、VPCにプライベートサブネットを設置してアプリケーションを展開する。ネットワークACLによってサブネットへのアクセスを制御して、オンプレミスのオフィス環境端末から認証してアクセスできるようにする。
- ○ パブリックサブネット内にSSL VPNソリューションを実装して、従業員のPC端末にSSL VPNクライアントソリューションをインストールする。VPCにプライベートサブネットを設置して、アプリケーションを展開する。SSLによって認証されると、オンラインポータルへのアクセスが許可される。
- ○ プライベートサブネット内にSSL VPNソリューションを実装して、アプリケーションを展開する。従業員のPC端末にSSL VPNクライアントソリューションをインストールする。PC端末からSSL認証されると、オンラインポータルへのアクセスが許可される。 (正解)

説明

このシナリオでは営業担当者は外出先からインターネット経由で、AWS内のプライベートネットワーク内のアプリケーションにアクセスして、営業記録などをタイムリーに記録してシェアすることが必要となります。ソリューションとしては、営業担当者が接続に利用するSSL VPNソリューションを実装して、これによって認証された従業員のみがインターネットを介してアプリケーションにAWSリソースにアクセスできる仕組みを作ることができます。

そのためには、セキュリティを考慮するとプライベートサブネット内にSSL VPNソリューションを実装して、営業担当者のPC端末にSSL VPNクライアントソリューションをインストールすることが必要となります。営業担当者が認証されると、オンラインポータルへのアクセスが許可されます。AWSクライアントVPN接続を実施することで、プライベートサブネット内のリソースへのアクセスが可能となります。

AWS VPNを介したVPN接続により、ユーザーはAWSのプライベートサブネットへの直接的な接続が可能となります。このシナリオでは、従業員のPC端末からクライアントVPNを利用して、プライベートサブネットにアクセスすることができます。したがって、オプション4が正解となります。

オプション1と3は不正解です。パブリックサブネットにSSL VPNソリューションを実装して、展開することは可能ですが、セキュリティ的にプライベートネットワークに設定することが要件に合致しているため、不正解となります。

オプション2は不正解です。オンプレミスのオフィス環境端末から認証してアクセスするのでは、どこでもアクセスができるという要件に合致せず、ソリューションとして不適切です。

問題45: 不正解

あなたの会社はAWSとオンプレミス環境を利用したハイブリッドクラウドアーキテクチャ環境を利用しています。現在、同社のITサービスチームは2つの既存のオンプレミスデータセンターをAWSクラウドに拡張して、様々な店舗で利用できるオンライン予約受付サービスを提供しています。このアプリケーションを利用するためにはオンプレミス環境とAWS環境とをデュアルトンネルVPNで接続することが必要でした。しかしながら、このVPCの接続点が単一障害点となっているため、改善が必要です。

ネットワーク接続の可用性を高めるための最適なソリューションを選択してください。

- ◉ データセンターに別のNATゲートウェイを使用して、別のデュアルトンネルVPN接続をセットアップする。 (不正解)
- ○ データセンターに別のカスタマーゲートウェイを導入して、別のデュアルトンネルVPN接続をセットアップする。 (正解)
- ○ データセンターに別のインターネットゲートウェイを導入して、別のデュアルトンネルVPN接続をセットアップする。
- ○ データセンターに追加のDirect Connectを導入して、広帯域の接続による二重接続をセットアップする。

説明

オンプレミス環境とAWS環境のVPN接続の可用性を高めるために、2重のデュアルトンネルVPN接続を設定することが可能です。そのためには、データセンターに別のカスタマーゲートウェイを作成し、別のデュアルトンネルVPN接続をセットアップします。これにより、アプリケーションやインフラの高可用性が確保されます。したがって、オプション2が正解となります。

AWS VPNを利用して、オンプレミス環境となる特定のデータセンター などをVPCにVPN接続することができます。カスタマーゲートウェイはその接続先のアンカーとなります。VPN 接続の AWS 側のアンカーは仮想プライベートゲートウェイと呼ばれます。オンプレミスとAWSを接続するカスタマーゲートウェイと仮想プライベートゲートウェイ間のVPN 接続の可用性を高めるためには、新しく別のカスタマーゲートウェイを導入して、別のデュアルトンネルVPN接続を追加することです。AWS でデバイス障害が発生した場合、VPN 接続は自動的に 2 番目のトンネルにフェールオーバーして、アクセスが中断されないようにします。

オプション1は不正解です。データセンターに別のNATゲートウェイではなく、カスタマーゲートウェイを使用して、別のデュアルトンネルVPN接続をセットアップする必要があります。

オプション3は不正解です。データセンターに別のインターネットゲートウェイではなく、カスタマーゲートウェイを使用して、別のデュアルトンネルVPN接続をセットアップする必要があります。

オプション4は不正解です。データセンターに追加のDirect Connectを導入して、広帯域の接続を実施することは本件の要件では求められていません。あくまでも、VPNの可用性を強化することが要件となっています。

問題46: 不正解

あなたはA社のソフトウェアエンジニアとして、Ruby on Railsベースで開発したコンテンツ管理プラットフォームを運用しています。このRubyアプリケーションは開発、ステージング、およびプロダクション用の複数のスタックを備えたOpsWorksを使用して、アプリケーションをデプロイおよび運用しています。現在、あなたはRubyではなくPythonの使用を開始したいと考えています。しかしながら、新しい言語のアプリケーション展開が既存ユーザーに悪影響を及ぼし始めた場合に備えて、Rubyを使用して古いアプリケーションに戻すことができるように、新しいアプリケーションを展開する必要があります。

これらのアプリケーションの展開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。

- ◉ OpsWorksを利用して新しいアプリケーション展開用スタックを生成する。CloudFormation内でOpsWorksを設定して、新しいStackと旧Ruby版のStackにブルーグリーン展開戦略を設定する。新しいスタックは、最初に本番トラフィックのごく一部でのみテストされ、新しいデプロイメントにエラーがある場合、古いデプロイメントスタックに戻るようにする。 (不正解)
- ○ OpsWorksを利用して新しいアプリケーション展開用スタックを生成する。ブルーグリーン展開戦略を設定して新しいスタックは、最初に本番トラフィックが実行され、新しいデプロイメントにエラーがある場合は展開を停止し、古いデプロイメントスタックに戻るようにする。 (正解)
- ○ OpsWorksを利用して新しいアプリケーション展開用スタックを生成する。CloudFormation内でOpsWorksを設定して、新しいStackと旧Ruby版のStackにロールバック展開方式を設定し、最初に本番トラフィックのごく一部でのみテストされ、新しいデプロイメントにエラーがある場合は古いデプロイメントスタックに戻るようにする。
- ○ OpsWorksを利用して新しい展開用スタックを生成する。新しいStackと旧Ruby版のStackにロールバック方式を設定し、最初に本番トラフィックが実行され、新しいデプロイメントにエラーがある場合は展開を停止し、古いデプロイメントスタックに戻るようにする。

説明

オプション2は、ブルーグリーン展開戦略を利用することで新しいスタックの展開を並行して実施できます。これにより、新しいスタックは、最初に本番トラフィックの一部でテストがされます。その際に、新しいデプロイメントにエラーがある場合は古いデプロイメントスタックに戻ります。

Blue-Green Deployment 戦略は、個別のスタックを効率的に使用して、更新版アプリケーションに不具合がないようにデプロイする一般的な方法の1つです。

・Blue 環境は、現在のアプリケーションをホストする本稼働スタックです。
・Green 環境は、更新されたアプリケーションをホストするステージングスタックです。

OpsWorksでBlue-Green Deployment 戦略を実施するには、更新されたアプリケーションを本稼働にデプロイするように準備して、Blue スタックから新しい本稼働スタックとなる Green スタックにユーザートラフィックを切り替えます。その後、古い Blue スタックを削除します。

CloudFomationとの連携は今回は必要としていないため、オプション1と3の設定は不適切です。

新しいStackと旧Ruby版のStackをロールバック方式で設定するのではなく、ブルーグリーン方式で設定する必要があるため、オプション4は不適切です。

問題47: 不正解

大手メディア企業はAWSクラウドを使用したハイブリッドクラウドインフラストラクチャを採用しました。あなたはソリューションアーキテクトとして、RAC構成でOracleデータベースを使用するソーシャルメディアアプリケーションを移行することを計画しています。現在利用しているソーシャルメディアアプリケーションはIPv4アドレスに対応していますが、今後はIPv6アドレスを利用できるようにすることが必要です。そして、アプリケーションはインターネットへの発信トラフィックを送信できますが、インターネットからの着信をブロックする必要があります。

このアプリケーションをAWSに適切に移行するための最適なソリューションを選択してください。

- ◉ RDSのデータベースエンジンでOracleデータベースを選択して、別のEC2インスタンスにWEBサーバーを起動してから、Egress-Onlyインターネットゲートウェイをセットアップする。 (不正解)
- ○ RDSのデータベースエンジンでOracleデータベースを選択して、別のEC2インスタンスにWEBサーバーを起動してから、NATゲートウェイをセットアップする。
- ○ OracleデータベースをEC2インスタンスにホストして、別のEC2インスタンスにWEBサーバーを起動してから、NATゲートウェイをセットアップする。
- ○ OracleデータベースをEC2インスタンスにホストして、別のEC2インスタンスにWEBサーバーを起動してから、Egress-Onlyインターネットゲートウェイをセットアップする。 (正解)

説明

オプション4が正解となります。Oracle RAC(Real Application Clusters)とは 複数のサーバで一つのデータベースを構成するクラスタ環境です。 RAC環境は従来のアクティブ/スタンバイ(HA)構成ではなく、アクティブ/アクティブで構成されるためサーバのリソースを100%活用できることが特徴です。しかしながら、Amazon RDSではRAC構成のOracleデータベースを使用することができません。したがって、Oracleデータベースを EC2インスタンスにホストして構成することが必要です。その上で、別のEC2インスタンスでWEBサーバーを起動してから、Egress-Only インターネットゲートウェイをセットアップします。

Egress-Only インターネットゲートウェイは水平的に拡張され、冗長で、高度な可用性を持つ VPC コンポーネントで、IPv6 経由での VPC からインターネットへの送信を可能にし、インスタンスとの IPv6 接続が開始されるのを防ぎます。

IPv6 アドレスはグローバルに一意であるため、デフォルトでパブリックアドレスになっています。インスタンスにインターネットにアクセスさせる場合にインターネット上のインスタンスにインスタンスとの通信を開始させないようにするためには、Egress-Only インターネットゲートウェイを使用できます。これを行うには、Egress-Only インターネットゲートウェイを VPC に作成し、次にすべての IPv6 トラフィック (::/0) または特定の IPv6 アドレス範囲をポイントするルートテーブルに、Egress-Only インターネットゲートウェイへのルートを追加します。ルートテーブルに関連付けられるサブネットの IPv6 トラフィックは、Egress-Only インターネットゲートウェイにルーティングされます。

オプション1と2は不正解です。RDSはRAC構成のOracleデータベースを使用することができません。

オプション3は不正解です。この設定ではIPv6を利用しているため、NATゲートウェイによるアドレス変換ではなく、Egress-Only インターネットゲートウェイを使用してインターネットからのアクセスを防ぐことが必要です。

問題48: 不正解

あなたの会社はAWS上に社内インフラをホストしています。その中で顧客管理システムはEC2インスタンスにホストされたMySQLデータベースを利用しています。最近になって会社が災害復旧計画を立案したことで、災害復旧（DR）対応を検討するようにマネージャーから指示されました。顧客データなどの機密性の高いデータはセカンダリーDBを利用して可用性を高めることが要件となっています。したがって、あなたはAWS上にあるEC2インスタンス（MySQLサーバー）のデータを、オンプレミスのデータセンターに移行することにしました。

高速性よりもコスト最適な対応を実現するソリューションを選択してください。

- ◉ AWS Storage Gatewayを利用して、VPCとオンプレミスデータセンターを接続して、次にmysqldumpを利用して、MySQLサーバーから外部のMySQLデータベースへの移行を実施する。 (不正解)
- ○ IPSec VPN接続を構成して、VPN/仮想ゲートウェイを利用してAWSクラウド内のVPCとオンプレミスデータセンターを接続する。次にmysqldumpを利用して、MySQLサーバーから外部のMySQLデータベースへと移行する。 (正解)
- ○ Direct Connectを利用して、VPCとオンプレミスデータセンターを接続して、スナップショットを利用してMySQLサーバーから外部のMySQLデータベースへの移行を実施する。
- ○ IPSec VPN接続を構成して、VPN/仮想ゲートウェイを利用してAWSクラウド内のVPCとオンプレミスデータセンターを接続する。次にスナップショットを利用して、MySQLサーバーから外部のMySQLデータベースへと移行する。
- ○ AWS Storage Gatewayを利用して、VPCとオンプレミスデータセンターを接続して、次にスナップショットを利用して、MySQLサーバーから外部のMySQLデータベースへの移行を実施する。

説明

このシナリオでは、EC2インスタンスベースのMySQLデータベースのオンプレミス環境への移行方法が問われています。RDSを移行する場合はスナップショットを利用して簡易に対応が可能ですが、EC2インスタンスやオンプレミスサーバーにインストールされたMySQLデータベースではスナップショットは利用できません。

その場合は、MySQLデータベースの機能であるmysqldumpを使用してMySQLデータをエクスポートして、移行先にインポートすることが必要です。これにより、MySQL間のデータ移行が可能となります。また、VPN/仮想ゲートウェイを使用して、オンプレミスネットワークとVPC間にセキュアなIPSec VPN接続をセットアップすることが可能です。今回はコスト効率が良い対応が必要であるため、より値段が高いDirect Connectではなく、VPNによるセキュアなデータ転送を優先します。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は不正解です。AWS Storage Gatewayは、オンプレミスから実質無制限のクラウドストレージへのアクセスを提供するハイブリッドクラウドストレージサービスです。Storage Gatewayを使用して、ストレージ管理を簡素化し、主要なハイブリットクラウドストレージのユースケースでコストを削減できます。これは、あくまでもストレージ用のバックアップ・拡張構成であるため、不正解です。また、設定方式として、AWS Storage Gatewayを利用してVPCとオンプレミスデータセンターを接続するのではなく、AWS Storage Gatewayを利用してS3とオンプレミス環境のストレージを接続することが必要となります。

オプション3は不正解です。接続形式はバックアップ用であるため高速性よりもコスト最適な対応が求められています。したがって、Direct Connectはパフォーマンスは VPNよりも高いものの、コスト最適ではないため不適切です。

オプション4と5は不正解です。MySQLデータベースはRDS用のスナップショットを利用することができません。そのため、外部のMySQLデータベースへの移行を実施するには、mysqldumpを利用します。

問題49: 不正解

あなたの会社は自分で撮影した動画をユーザー間でPCやモバイルなどの様々なデバイスで共有することができる動画プラットフォームを構築しています。モバイルアプリケーションや動画を撮影すると、ユーザーの動画フォルダにMP4形式で保存され、好きなように動画をカスタマイズして他のユーザーにシェアする仕組みです。配信の際には、主にモバイルデバイス上でグローバルにストリーミングされることになります。

この要件を満たすことができる最適なアーキテクチャを選択してください。（2つ選択してください。）

- [x] MP4ファイルをS3にアップロードして、Amazon Rekognition Videoを利用してMP4からHTTP Live Streaming (HLS)形式へと変換して、S3に保存する。 (不正解)
- [x] MP4ファイルをS3にアップロードして、AWS Elemental MediaConvertを利用してMP4からHTTP Live Streaming (HLS)形式へと変換して、S3に保存する。 (正解)
- [ ] HLSによるオンデマンド・トランスコーディングをサーバー上で実施するためにS3バケットを動画ソースとして利用するストリーミング処理用のEC2インスタンスを起動する。EC2ストリーミングサーバーをオリジンサーバーとしてCloudFrontディストリビューションを設定する。 (正解)
- [ ] MP4ファイルをS3にアップロードして、Amazon Video Streamingを利用してMP4からHTTP Live Streaming (HLS)形式へと変換して、S3に保存する。
- [ ] HLSによるオンデマンド・トランスコーディングをサーバー上で実施するためにS3バケットを動画ソースとして利用するストリーミング処理用のEC2インスタンスを起動する。ストリーミングサーバーをオリジンサーバーとしてAWS Elemental MediaConvertによるストリーミング配信を設定する。

説明

AWS Elemental MediaConvertを使用して動画をさまざまな形式にトランスコードすることができます。ストリーミング配信にはモバイルでHLSを使用してS3リソースを利用して、CloudFront配布をダウンロードオプション付きで使用することが可能です。オンデマンドストリーミングの場合、動画コンテンツはAmazon S3に保存されます。したがって、オプション2と3が正解となります。

AWS Elemental MediaConvert はクラウドのメディア変換サービスです。複数のプラットフォームデバイスで、メディアがMP4形式でグローバルにストリーミングを処理できます。高度なスケーラビリティ、使いやすさ、高い費用効率性を実現する設計で、開発者や企業は、メディアファイルをその元のソース形式からスマートフォン、タブレット、PC などのデバイスで再生可能できるバージョンに変換できます。

オプション1は不正解です。Amazon Rekognition Videoを利用してMP4からHTTP Live Streaming (HLS)形式へと変換することはできません。Amazon Rekognition Videoは動画専用AIによる画像識別を実行するサービスです。

オプション4は不正解です。Amazon Video Streamingではなく、AWS Elemental MediaConvertを利用してMP4からHTTP Live Streaming (HLS)形式へと変換します。

オプション5は不正解です。AWS Elemental MediaConvertによるストリーミング配信を実施できません。AWS Elemental MediaConvertは動画をさまざまな形式にトランスコードするサービスです。

問題50: 不正解

あなたの会社はVPCのプライベートサブネット内に社内業務アプリケーションをホストしています。このアプリケーションは内部の特定ユーザーしか利用していないためパブリックアクセスを必要としていませんが、運用上、定期的にパッチをダウンロードしてソフトウェアアップデートを実行することが必要です。そのために一つのAZにNATインスタンスが設置されていますが、このNATインスタンスは単一障害やトラフィックパフォーマンスのボトルネックとなっています。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、NATのフォールトトレランスを高めるような改善策を実施しています。

この要件を満たすために最適なNATインスタンスの改善方法を選択してください。（2つ選択してください。）

- [x] 2つの異なるVPCに2つのNATインスタンスを起動して、プライベートサブネットからのルート設定をそれぞれのNATインスタンスに実施する。 (不正解)
- [x] NATインスタンスをNATゲートウェイに変更する。2つの異なるAZにあるパブリックサブネットに2つのNATゲートウェイを起動して、プライベートサブネットからのルート設定をそれぞれのNATゲートウェイに実施する。 (正解)
- [ ] 2つの異なるAZにあるパブリックサブネットに2つのNATインスタンスを起動して、プライベートサブネットからのルート設定をそれぞれのNATインスタンスに実施する。
- [ ] NATインスタンスをマルチAZ構成に設定して、障害発生時の適切な処理をするためのスクリプトを設定する。 (正解)
- [ ] NATゲートウェイをマルチAZ構成に設定して、障害発生時の適切な処理をするためのスクリプトを設定する。

説明

オプション２が正解となります。NATインスタンスよりもAWSから提供されているNATゲートウェイに変更することで、より高性能なNATパフォーマンスを提供することができます。また、NATゲートウェイは１つのAZにあるとAZ障害に弱いため、２つのAZにそれぞれ１つのパブリックサブネットを構成してNATゲートウェイを設定します。その上で、プライベーサブネットにあるインスタンスからそれぞれのNATゲートウェイに対するルートを作成することでNATゲートウェイの冗長性を担保することができます。

オプション４が正解となります。対策の1つはNATインスタンスに障害が発生した場合に相互に引き継ぐことができる複数のNATインスタンスによるマルチ構成を実現することです。1つのNATインスタンスに障害が発生した場合、設定したスクリプトにより、動作しているNATインスタンスがアウトバウンドトラフィックを引き継ぐことができ、失敗したインスタンスを停止および再起動することで修正しようとします。

オプション１は不正解です。2つの異なるVPCに2つのNATインスタンスを起動するのではなく、さらに別のAZに構成されたパブリックサブネットを指定して設定する必要があります。１つのAZに２つのVPCとサブネットを設定しただけでは、その構成はAZ障害に弱い構成となってしまいます。

オプション３は不正解です。これはNATインスタンス構成をマルチAZにしているため、オプション４と同じ構成となりますが、障害発生時の適切な処理をするためのスクリプトを設定することが必要です。

オプション５は不正解です。この設定はNATインスタンスには実施できましたが、NATゲートウェイには設定できないため、不正解です。

問題51: 不正解

A社は3層アプリケーション構成となっているEコマースサイトをオンプレミス環境で運用しているファッションブランド企業です。A社の経営陣は現在オンプレミス環境にあるEコマースサイトのスケーラビリティと耐久性を高めるために、AWSに移行することを決定しました。移行に必要な要件は以下の通りです。

■WEB層：Webサーバーは負荷分散とスケーリングを実現する。また、大量のデータを保存可能なストレージを使用してデータ参照を実施する。
■アプリケーション層：アプリケーションサーバーはIPユニキャストを利用してユーザーのセッション状態を維持する。
■データベース層：データベースはプライマリとセカンダリに分けたフェールオーバー構成として、複数の読み取り専用レプリカを使用する。また、保存データは日次でバックアップする。

このオンプレミス上の構成をAWSに移行するための最適なアーキテクチャを選択してください。

- ◉ アプリケーションサーバーとしてEC2インスタンスを起動して、ELBとAutoScalingグループを設定する。アプリケーションからの参照用データはEBSに保存し、アプリケーションサーバーはDynamoDBとIPユニキャストを組合わせて利用してセッション状態を保持する。データベースにもDynamoDBを利用したマルチマスター構成を展開して、バックアップはグローバルテーブルによるレプリケーションを実施する。 (不正解)
- ○ アプリケーションサーバーとしてEC2インスタンスを起動して、ELBとAutoScalingグループを設定する。アプリケーションから参照するデータはS3に保存し、アプリケーションサーバーはDynamoDBとIPユニキャストを組合わせてセッション状態を保持する。データベースはRDSをマルチAZ構成としてリードレプリカを追加した上で、バックアップはDBスナップショットを日次で取得する。 (正解)
- ○ アプリケーションサーバーとしてEC2インスタンスを起動して、ELBとAutoScalingグループを設定する。読み取りデータはEBSに保存・利用して、アプリケーションサーバーはRDSとIPユニキャストを組合わせて利用してセッション状態を保持する。データベースはOracleデータベースサーバーをEC2インスタンスにインストールして、バックアップはAMIによって日次で取得する。
- ○ アプリケーションサーバーとしてEC2インスタンスを起動して、ELBとAutoScalingグループを設定する。読み取りデータはS3に保存・利用して、アプリケーションサーバーはEC2インスタンスにIPユニキャストを実装してセッション状態を共有する。データベースはOracleデータベースサーバーをEC2インスタンスにインストールして利用して、リードレプリカを追加する。バックアップはAMIとDBスナップショットを日次で取得する。

説明
このシナリオでは、以下の要件をAWS上で実現するアーキテクチャーが求められています。

■WEB層では、Webサーバーは負荷分散とスケーリングが可能とし、大量データを保存可能なストレージを使用してデータ参照を実施することが必要です。これを実現するためには、アプリケーションサーバーとしてEC2インスタンスを起動して、ELBとAutoScalingグループを設定することが必要です。また、ストレージとしては大量データを保存するためEBSではなく、S3 Standardを利用して、データを参照処理を実装します。

■アプリケーション層では、アプリケーションサーバーはIPユニキャストを利用してユーザーのセッション状態を維持することが必要です。セッション管理にはDynamoDBを利用することが最適です。DynamoDBとIPユニキャストを使用してWebサーバーが状態を共有する構成とします。DynamoDBではセッション管理が最適なユースケースとされています。

■データベース層では、データベースはプライマリとセカンダリに分けたフェールオーバー構成として、複数の読み取り専用レプリカを使用する。また、保存データは日次でバックアップすることが必要です。したがって、RDSをマルチAZ構成としてリードレプリカを追加することで要件を満たすことができます。また、バックアップの要件を満たすためには、DBスナップショットを使用してデータの日次バックアップウィンドウを設定することが必要です。

したがって、これらの要件を全て満たしている、オプション２が正解となります。

オプション１は不正解です。大量データを保存可能なストレージとしてはEBSではなくS3が最適です。また、データベースにはリードレプリカとフェールオーバー構成が必要であり、DynamoDBではリードレプリカを利用することができません。

オプション３は不正解です。大量データを保存可能なストレージとしてはEBSではなくS3が最適です。また、RDSのリードレプリカが使用されていないため、要件の達成が不十分です。 バックアップはAMIによりEBSボリュームだけでは不十分であり、データベース自体のバックアップが必要です。

オプション４は不正解です。RDSではなく、EC2インスタンスをデータベースに利用していますが、今回のケースでは問題文からはRDSを利用できない要素がないため、その場合はマネージドサービスであるRDSを優先して利用することになります。必然性がない場合にEC2インスタンスにデータベースソフトウェアをインストールして利用するのは非効率です。

問題52: 不正解

開発チームはVPCのプライベートサブネット内に複数のEC2インスタンスを立ち上げました。このEC2インスタンスを利用して、高パフォーマンスな処理が可能なワーカープロセスを実装します。このワーカープロセスでは高い帯域幅で最大 100 Gbps のネットワーク速度をサポートする必要があります。しかしながら、現在の設定ではそれが達成できていないようです。

この要件を満たすことができる最適なソリューションを選択してください。

- ◉ Intel 82599 Virtual Function (VF)タイプの拡張ネットワークをサポートするインスタンスタイプに変更する。 (不正解)
- ○ Elastic Network Adapter (ENA)タイプの拡張ネットワークをサポートするインスタンスタイプに変更する。 (正解)
- ○ パフォーマンスが高いインスタンスサイズに変更する。
- ○ EBSのボリュームタイプをプロビジョンドIOPSに変更する。

説明

このシナリオでは、EC2インスタンスのネットワーキングとして高い帯域幅、最大 100 Gbps のネットワーク速度) の高いパフォーマンス、常に低いインスタンス間レイテンシーを実現したいと考えています。

■Elastic Network Adapter (ENA) は、サポート対象のインスタンスタイプに対して最大 100 Gbps のネットワーク速度をサポートします。

C5, C5d, C5n, F1, G3, G4, H1, I3, I3en, Inf1, m4.16xlarge, M5, M5a, M5ad, M5d, M5dn, M5n, P2, P3, R4, R5, R5a, R5ad, R5d, R5dn, R5n, T3, T3a, u-6tb1.metal, u-9tb1.metal, u-12tb1.metal, u-18tb1.metal, u-24tb1.metal, X1, X1e, and z1d インスタンスでは、拡張ネットワーキングで Elastic Network Adapter を使用します。

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 は不正解です。Intel 82599 Virtual Function インターフェイスでは、サポートされているインスタンスタイプについて最大 10 Gbps のネットワーク速度がサポートされています。

利用可能な最新のインスタンスタイプおよびアダプターについては、「Linux の拡張ネットワーキング」および「Windows インスタンスで Intel 82599 VF インターフェイスを使用して拡張ネットワーキングを有効化する」を参照してください。

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/sriov-networking.html

問題53: 不正解

C社はフィンテック企業として決済プラットフォームを運用しています。この決済プラットフォームはEC2インスタンスにELBターゲットグループとAuto Scalingを設定した構成となっており、AWS Elastic Beanstalkを使用して展開・バージョニング管理をしています。数週間後、この決済プラットフォームの新しいバージョンを展開する必要が出てきました。あなたはソリューションアーキテクトとして、Elastic Beanstalkで使用できる有効なデプロイポリシーを検討しています。

次の選択肢のうちで、有効ではないデプロイポリシーはどれでしょうか？

- ◉ All at once (不正解)
- ○ Rolling
- ○ Rolling with additional batch
- ○ Immutable
- ○ Swap (正解)

説明

AWS Elastic Beanstalk はデプロイを実施するためのいくつかのデプロイポリシーオプションを提供しています。これらのオプションによって、バッチサイズやデプロイ中のヘルスチェックの動作を設定できます。AWS Elastic Beanstalk のデプロイオプションの以下の通りです。したがって、オプション 5 が正しくない選択肢となります。

SWAPはElasti Beanstalkを利用してブルーグリーンデプロイメントを実行する際に利用しますが、デプロイポリシーのオプションで実行するものではありません。環境の概要ページで、**環境アクション** を選択し、**[環境 URL のスワップ]** を選択します。詳細は以下をご参照ください。

https://docs.aws.amazon.com/ja_jp/elasticbeanstalk/latest/dg/using-features.CNAMESwap.html

■All at once

新しいバージョンをすべてのインスタンスに同時に展開します。環境内のすべてのインスタンスは、展開が行われている間、短時間サービスが停止します。これは、展開に必要な合計時間を最短にする方法です。

■Rolling(ローリング)

Elastic Beanstalk は環境の EC2 インスタンスを複数のバッチに分割し、アプリケーションの新しいバージョンを一度に 1 つのバッチにデプロイするため、環境内の残りのインスタンスは古いアプリケーションバージョンを実行した状態になります。つまりローリングデプロイ中は、アプリケーションの古いバージョンでリクエストを処理するインスタンスもあり、新しいバージョンでリクエストを処理するインスタンスも存在します。

■Rolling with additional batch

新しいバージョンをバッチで展開しますが、最初にインスタンスの新しいバッチを起動して、展開プロセス中に完全な容量を確保します。

■Immutable

変更不可能な更新を実行して、古いバージョンを起動しているインスタンスと並行しながら、別の Auto Scaling グループにあるアプリケーションの新しいバージョンを起動している新しいインスタンスのフルセットを起動します。[Immutable] デプロイは、部分的に完了したローリングデプロイにより発生する問題を防止できます。新しいインスタンスがヘルスチェックをパスしなかった場合、Elastic Beanstalkはそれを終了し、元のインスタンスをそのまま残します。

問題54: 不正解

あなたの会社ではRDS MySQLを利用したOLTPデータベースによる分析システムを運用しています。あなたは分析担当として、このOLTPデータベースの分析プロセス上のバッチプロセスを管理していますが、このプロセスはデータ読込処理に非常に時間がかかっています。分析処理が完了するとメール通知をトリガーとしてオンプレミス環境にあるダッシュボードに分析結果が表示されます。このデータ処理の遅延やダッシュボードへの最新データの反映が遅いことが問題となっており、改善する必要があります。

パフォーマンスの問題を解決し、プロセスを可能な限り自動化するための最適なAWSソリューションを選択してください。

- ◉ RDSからデータを取得してAWS Batchによるデータ解析バッチ処理を設定する。次に、Amazon SNSを利用してオンプレミス側に更新作業を通知する。 (不正解)
- ○ RDSにリードレプリカを増設してデータ解析バッチ処理向けの読取処理パフォーマンスを向上させる。次に、Amazon SNSを利用してオンプレミス側に更新作業を自動通知する。 (正解)
- ○ Redshiftのマルチクラスター構成を設定して、読取処理パフォーマンスを向上させる。次に、Amazon SNSを利用してオンプレミス側に更新作業を自動通知する。
- ○ RDSにリードレプリカを増設してデータ解析バッチ処理向け読取処理パフォーマンスを向上させる。次に、Amazon MQを利用してオンプレミス側に更新作業を自動通知する。

説明

OLTPデータベースの分析プロセスパフォーマンスを改善するには、データ解析時の読み取り処理を向上させる必要があります。よって、Amazon RDSリードレプリカの使用が最適なオプションです。これによりデータ分析時のデータベース（DB）インスタンスのパフォーマンスと耐久性を強化します。読み取りが多いデータベースワークロードの場合、単一のDBインスタンスの容量の制約を超えて柔軟にスケールアウトできます。障害時にはリードレプリカを昇格させて、スタンドアロンDBインスタンスにすることもできます。

また、今回はメール通知をトリガーに更新を通知する仕組みを利用しているため、SNSを利用してアラートを自動設定することで更新作業を自動化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は正しくありません。AWS Batchによる、数十万件のバッチコンピューティングジョブをAWSで簡単かつ効率的に実行できますが、データベースの読込処理がパフォーマンス上のボトルネックとなっているため、これは効果がありません。

オプション3は正しくありません。このオプションはRDSではなくRedshiftを利用していますが、Redshiftにはマルチクラスター構成を設定することで読込処理を向上させる機能はありません。

オプション4は正しくありません。SNSのようにAWSネイティブで通知処理を生成する際に利用するのではなく、Amazon MQはApache ActiveMQ向けのマネージド型メッセージブローカーサービスです。Apache ActiveMQを利用したメッセージング処理を利用したい際に選択します。

問題55: 不正解

あなたの会社ではオンプレミス環境とAWSクラウドを利用したハイブリッドインフラストラクチャーへと移行することを決定しました。そこで、あなたはソリューションアーキテクトとして、オンプレミスのリモートネットワークとAmazon VPC間の接続ソリューションを設計するように求められました。要件としては、この接続によってオンプレミスサーバーとVPCで実行されているEC2インスタンス間の通信を安全に実施することが必要です。あなたはVPNゲートウェイを使用してインターネット経由でIPSecトンネルを確立することを検討しています。

IPSecトンネルについて間違っているものを1つ選択してください。

- ◉ 仮想プライベートゲートウェイ（VGWとカスタマーゲートウェイ（CGW）の間にIPSecトンネルが確立される。 (不正解)
- ○ IPSecトンネルを経由して送信されるデータはSSLによって暗号化される (正解)
- ○ IPSecトンネル経由で送信されるデータは整合性を保持することができる。
- ○ AWSのSite-to-Site VPN 接続によって、IPSecトンネルを確立することができる。
- ○ AWS Classic VPN またはAWS VPNを利用することができる。

説明

デフォルトではAmazon VPC 内に起動されるインスタンスとユーザー独自のリモートネットワークとの通信はできません。VPC から独自のリモートネットワークへのアクセスを可能にするには、仮想プライベートゲートウェイを VPC に関連付けて、カスタムルートテーブルを作成して、セキュリティグループ規則を更新し、AWS Site-to-Site VPN接続を作成することが必要となります。Site-to-Site VPN は、インターネットプロトコルセキュリティ (IPsec) VPN 接続をサポートしています。

【IPSecの特徴は以下の通り】

・Site-to-Site VPN 接続は、AWS Classic VPN または AWS VPN のいずれかです。
・IPSecトンネル経由で送信されるデータの整合性を保持する。
・IPSecトンネルを経由して送信されるデータは暗号化される。
・IPSecはインターネット経由で送信中のデータを保護する。
・IPSecトンネルのセットアップ中にIDが認証される。
・VPNゲートウェイ（VPG）とカスタマーゲートウェイ（CGW）の間にIPSecトンネルが確立される。

上記の特徴から、IPSecトンネルを経由して送信されるデータは暗号化されますが、その際にSSLを利用してはいないため、間違った選択肢はオプション２になります。

問題56: 不正解

ある会社ではオンラインショッピングサイトをELBとAutoScalingが設定されたEC2インスタンスにホストしています。このショッピングサイトはサードパーティの支払いサービスを使用して、プラットフォーム上でクレジットカードによる決済処理をしています。ユーザーが支払いを行うと、システムは支払トランザクションを完了するためにインターネット経由で支払いサービスに接続する必要があります。しかしながら、サードパーティの決済ソフトウェアの利用上の制限によって、一度に最大４つのIPアドレスまでしか連携することができないようです。このIPアドレスの最大保有数の制限によって、トランザクション処理量が制限されてしまうため、決済処理が遅延する可能性があります。あなたは改善対応を依頼されました。

この問題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？

◉ 支払い処理用のEC2インスタンスにEIPを設定して、支払いリクエストがルーティングされる設定を行う。ELBに登録されたElastic IPアドレスをアタッチすることで、複数IPアドレスをトラフィックできるようにする。 (不正解)

○ 支払い処理を実施するEC2インスタンスへのAutoScalingの最大上限を5台から増加させることで、ピーク時の処理能力を向上させる。

○ Elastic Network Interfaces(ENI)を新しく設定して、EC2インスタンスへの支払いリクエストがルーティングされる設定を行う。

○ VPCにNATゲートウェイを設置してEC2インスタンスへの支払いリクエストがルーティングされる設定を行う。NATゲートウェイに決済システムのホワイトリストに登録されたElastic IPアドレスをアタッチする。 (正解)

説明

このシナリオではサードパーティソフトウェアの利用上の制限があり、一度に最大４つのIPアドレスまでしか連携することができないため、最大で４つのEC2インスタンスによる支払い処理しかできないことがボトルネックになっています。そのため、支払い処理リクエストが大量に発生して高負荷になったとしても、AutoScalingを利用したスケーリングができないことが問題となっています。

解決先としてはNATゲートウェイを介してEC2インスタンスへの支払いリクエストがサードパーティソフトウェアにルーティングされるように設定することです。こうすることで、NATゲートウェイのIPアドレスとサードパーティソフトウェアとを連携させて、直接にEC2インスタンスをソフトウェアに接続しない構成を実現することができます。NATゲートウェイに決済システムに登録されたElastic IPアドレスをアタッチして、それにサードパーティーのクレジットカード支払いシステムを連携させれば、NATゲートウェイの後ろでEC2インスタンスは5台以上利用することが可能になります。

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。支払い処理用のEC2インスタンスにEIPを設定して、支払いリクエストがルーティングされる設定を行ったとしても、EC2インスタンスのIPアドレスと連携させると４つのEC2インスタンスによる処理しかできません。

オプション２は不正解です。支払い処理を実施するEC2インスタンスへのAutoScalingの最大上限を４台から増加させたとしても、支払い処理リクエストを直接にEC2インスタンスのIPアドレスと連携させると４つのEC2インスタンスによる処理しかできません。

オプション３は不正解です。Elastic Network Interfaces(ENI)を新しく設定して、EC2インスタンスへの支払いリクエストがルーティングされる設定を行っても、一度に最大４つのIPアドレスを利用できるという限界には対応できていません。

問題57: 不正解

フィンテックベンチャーA社ではAWS Organizationsを使用して管理する複数のAWSアカウントを使用しています。この会社ではキャッシュレス決済モバイルアプリケーションをAWS上に構築してサービスを提供しています。金融サービスとしての認証を得るために、会社では金融庁から要求されたIT監査を実施することが求められています。そのためには、すべてのAWSリソースに加えられた変更をグローバルに追跡することができ、かつログファイルは安全に保護され、絶対に削除されない状態を保証する必要があります。

この問題を解決するために最適なアーキテクチャを選択してください。

- ◉ マスターアカウントに対して単一のCloudTrailを有効化して、ターゲットアカウント設定において他の子アカウントをターゲット設定する。S3バケットにログ情報を取得して、SNSを利用して会社の監査用管理システムに通知するアプリケーションを構築する。S3バケットにおいてデータ暗号化とMFA認証によるファイル削除の保護を行う。 (不正解)

- ○ マスターアカウントのCloudTrailにおいて「組織の証跡」を有効化する。S3バケットにログ情報を取得して、SNSを利用して会社の監査用管理システムに通知するアプリケーションを構築する。S3バケットにおいてデータ暗号化とバケット内データが削除不可能となる設定を実施して、ログファイルが削除できないようにする。 (正解)

- ○ マスターアカウントに対して単一のCloudTrailを有効化して、ターゲットアカウント設定において他の子アカウントをターゲット設定する。S3バケットにログ情報を取得して、SNSを利用して会社の監査用管理システムに通知するアプリケーションを構築する。S3バケットにおいてデータ暗号化とバケット内データが削除不可能となる設定を実施して、ログファイルが削除できないようにする。

- ○ マスターアカウントのCloudTrailにおいて「組織の証跡」を有効化して、S3バケットにログ情報を取得して、SNSを利用して会社の監査用管理システムに通知するアプリケーションを構築する。S3バケットにおいてデータ暗号化とMFA認証によるファイル削除の保護を行う。

説明

オプション2が正解となります。 AWS Organizationsを利用していれば、CloudTrailにより全てのAWSアカウントをまとめてログ取得することが可能です。「組織の証跡」とは、組織内のマスターアカウントとすべてのメンバーアカウントの CloudTrail イベントを同じ Amazon S3 バケット、CloudWatch Logs、CloudWatch イベント に配信できるようにする設定です。組織の証跡を有効化すると、組織のための統一されたイベントログ記録戦略を定義することができ、自分の組織に属するすべての AWS アカウントに指定した名前の証跡が作成されます。メンバーアカウントで CloudTrail アクセス許可を持つユーザーはAWS アカウントから AWSCloudTrail コンソールにログインしたとき、または describe-trails などの AWS CLI コマンドを実行したときにこの証跡 (証跡 ARN を含む) を表示することができます。

各AWSアカウントでアクティビティが発生すると、そのアクティビティはCloudTrailイベントに記録されます。イベント履歴に移動すると、CloudTrailコンソールで最近のイベントを簡単に表示できます。マルチリージョンおよびグローバルイベントの追跡を有効にすることもできます。

デフォルトでは、CloudTrailによってバケットに配信されるログファイルは、Amazon S3 管理の暗号化キー（SSE-S3）を使用したAmazonサーバーサイド暗号化によって暗号化されます。直接管理可能なセキュリティレイヤーを提供するために、CloudTrailログファイルにAWS KMS管理キー（SSE-KMS）を使用したサーバーサイド暗号化を使用できます。さらにログを保護するには、S3バケットを暗号化して、バケット作成時にデータの削除不可の設定を行うことで、永続的にログを保存することが可能となります。

オプション1と3は不正解です。マスターアカウントに対して単一のCloudTrailを有効化して、ターゲットアカウント設定において、他の子アカウントをターゲット設定するのではなく、 AWS Organizationsを利用して、CloudTrailの「組織の証跡」を利用することで、他の子アカウントにも自動的にCloudTrailログを設定することが可能となります。

オプション4は不正解です。MFA認証によるデータ削除の保護は、利用者を限定するという意味では適切ですが、絶対に削除させないという要件には不十分です。

問題58: 不正解

あなたの会社ではオンプレミス環境から社内インフラをAWS環境へと移行することを決定しました。移行対象となるアプリケーションの一部はTCPのみをサポートしているため、ポート80および8080で動作することなります。また、AWSに移行する際は、アプリケーションに対してELBおよびAuto Scalingを使用して、アプリケーションのスケーラビリティを確保する構成を実現したいと考えています。

この要件を実現するための最適なリスナー構成を選択してください。

- ◉ インスタンスプロトコルをTCP80ポートと、TCP8080ポートに設定する。ELBをHTTP80ポートと、HTTP8080ポートに設定する。 (不正解)
- ○ ELBとしてCLBを選択し、インスタンスとの通信プロトコルをTCP80ポートと、TCP8080ポートに設定する。 (正解)
- ○ ELBとしてALBを選択し、インスタンスとの通信プロトコルをTCP80ポートと、TCP8080ポートに設定する
- ○ インスタンスプロトコルをHTTP80ポートと、HTTP8080ポートに設定する。ELBへの通信はTCP80ポートと、TCP8080ポートに設定する。

説明

今回のシナリオでは、アプリケーションサーバーに対してELBを設定する構成が必要です。その構成でTCPによる通信を実施します。Elastic Load Balancing は次のプロトコルをサポートしています。

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

TCPはCLBとNLBのみが利用し、ALBはHTTPとHTTPSがプロトコルとして利用されます。したがって、このシナリオではフロントエンド接続とバックエンド接続においてTCPを使用することが必要なため、CLBとインスタンスのプロトコルをTCP80ポートとTCP8080ポートに設定することが必要です。オプション２が正解となります。

問題59: 不正解

あなたの会社はオンラインホテル予約システムを運用しているベンチャー企業です。このオンラインホテル予約システムは、様々なホテル予約サイトから最安値価格を選択して顧客にオファーすることで利用ユーザーを伸ばしています。予約から決済まで一元的に実施しており、かつ最近ではグローバルに利用されているため、EC2インスタンスのWebサーバーをCloudFrontのオリジンにしてグローバル配信を行っています。クライアントからのHTTP接続要求とHTTPS接続要求の両方を処理できる必要があるため、あなたはオリジンとの通信がHTTPまたはHTTPSを介して行われるような[redacted]を行っています。

この要件に対応するためのオリジンプロトコルポリシー設定を選択してください。

- ◉ HTTP and HTTPS Onlyを指定する。 (不正解)
- ○ Any Protocolを設定した上で、HTTPS利用を有効化する。
- ○ HTTP Onlyを設定した上で、HTTPS利用を有効化する。
- ○ Match Viewerを指定する。 (正解)

説明

ウェブディストリビューションでは、オブジェクトのリクエストでビューワーがHTTPやHTTPS を使用するように CloudFront を設定して、CloudFront とビューワーとの通信を設定するポリシーを選択できます。これをOrigin Protocol Policyと呼びます。

Origin Protocol Policyの値として選択できる3つのオプションがあります。

- HTTP Only
- HTTPS Only
- Match Viewer

HTTP Onlyの場合、CloudFrontはHTTPのみを使用してオリジンにアクセスします。
HTTPS Onlyの場合、CloudFrontはHTTPSのみを使用してオリジンにアクセスします。
Match Viewerの場合、CloudFrontはビューアーリクエストのプロトコルに応じてHTTPまたはHTTPSを使用してオリジンと通信します。したがって、オプション４が正解となります。

問題60: 不正解

大手製造業はEC2インスタンスを利用したサーバーなどのインフラストラクチャーに構成された複数のWEBアプリケーションを利用しています。この会社ではデータウェアハウスとしてRedshiftを利用していますが、その災害復旧対応が準備されていません。そこで、あなたはRedshiftクラスターの災害復旧（DR）対策を実施するように依頼されました。バックアップを地理的に離れた場所に保存して、そのバックアップは暗号化によって保護される必要があります。

このシナリオで、要件に対応するための最適なアーキテクチャを選択してください。（2つ選択してください。）

- [x] DR先リージョンのマスターキーのスナップショットコピー許可を設定する。 (正解)
- [x] DR先リージョンにおいてAWS KMSで暗号化されたクラスターのクロスリージョンスナップショットコピーを有効にする。 (不正解)
- [ ] DR元リージョンのマスターキーのスナップショットコピー許可を設定する。
- [ ] DR元リージョンにおいてAWS KMSで暗号化されたクラスターのクロスリージョンスナップショットコピーを有効にする。 (正解)
- [ ] DR元リージョンにおいてマルチマスター構成を実施した上で、クラスターのクロスリージョンスナップショットコピーを有効にする。

説明

Amazon Redshiftクラスターを起動するときに、AWS KMSのマスターキーで暗号化することを選択できます。その際のAWS KMSキーはリージョン固有なキーとなります。DR元リージョンにおいてAWS KMSで暗号化されたクラスターのクロスリージョンスナップショットコピーを有効にすることで、DR先のリージョンに、Redshiftクラスターのスナップショットをコピーして移転させることができます。したがって、オプション4が正解となります。

この設定には、Amazon Redshiftが宛先リージョンで暗号化操作を実行できるように、宛先リージョンのマスターキーのスナップショットコピーを許可する設定が必要です。Amazon Redshiftのスナップショットはクラスターのポイントインタイムバックアップです。スナップショットには自動と手動の2つのタイプがあります。Amazon Redshiftは、暗号化されたSSL接続を使用して、これらのスナップショットをAmazon S3の内部に保存できます。 したがって、オプション1も正解となります。

オプション2は不正解です。DR先リージョンにおいてではなく、DR元リージョンにおいて、AWS KMSで暗号化されたクラスターのクロスリージョンスナップショットコピーを有効にします。

オプション3は不正解です。DR元リージョンではなく、DR先リージョンのマスターキーのスナップショットコピー許可を設定することが必要です。

オプション5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おり、RedshiftにおいてはDR元リージョンにおいてマルチマスター構成を実施することができません。

問題61: 不正解

あなたは美術SNSアプリケーションを構築しているエンジニアです。アプリケーションは様々なWebドメインからのトラフィックを処理するALBと、Autoscalingグループが設定された一連のオンデマンドEC2インスタンスにホストされています。さらにGoogle検索対応としてHTTPからHTTPS通信に変更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、新しいドメイン名を追加するたびに証明書を再認証および再プロビジョニングする必要なく、複数のドメインに対してSSL通信処理を可能とする設定を行っています。

上記の要件を満たすための有効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] CloudFrontディストリビューションを設定して、CNAMEフィールドにすべてのドメイン名を入力する。その上で、すべてのドメイン名に関連付けられている SSL証明書を追加する。 (正解)
- [x] AWS Certificate Managerを設定して特定IPアドレスからのHTTPSリクエストによるアクセスに限定する。これにより、この特定IPアドレスをドメイン名と関連付けて、エッジロケーション処理がHTTPS経由で実施されるようにする。 (不正解)
- [ ] IAM証明書管理を使用してALBのドメインにすべてのSSL証明書をアップロードし、複数の証明書をロードバランサーの同じセキュアリスナーにバインドする。ALBはサーバー名表示（SNI）を使用して、各クライアントに最適なTLS証明書を自動的に選択する。
- [ ] ACMコンソールを使用してALBのドメインにすべてのSSL証明書を追加して、複数の証明書をロードバランサーの同じセキュアリスナーにバインドする。ALBはサーバー名表示（SNI）を使用して、各クライアントに最適なSSL/TLS証明書を自動的に選択する。 (正解)

説明

オプション１は正解となります。HTTPS を介して CloudFront から複数のドメインを提供するには、CloudFrontにおいて、以下の設定を行います。

１．[代替ドメイン名 (CNAME)] フィールドにすべてのドメイン名を入力します。たとえば、ドメイン名 **example1.com** と **example2.com** を使用するには、両方のドメイン名を [代替ドメイン名 (CNAME)] に入力します。
２．すべてのドメイン名に関連付けられている SSL 証明書を追加してください。AWS Identity and Access Management (IAM) にアップロードされた証明書、または AWS Certificate Manager (ACM) でリクエストされた証明書のいずれか一方を追加することができます。

ACMを利用してALBに関連づいたドメインに全てのSSL証明書を追加し、複数の証明書をロードバランサーの同じセキュアリスナーにバインドします。ALBは、サーバー名表示（SNI）を使用して、各クライアントに最適なTLS証明書を自動的に選択します。したがって、オプション4は正解となります。

SNIカスタムSSLは、Transport Layer Securityプロトコルの SNI拡張機能に依存しています。これにより、視聴者が接続しようとしているホスト名を含めることで、複数のドメインが同じIPアドレスでSSLトラフィックを処理できます。

オプション２は不正解です。AWS Certificate ManagerはSSL証明書を作成・管理する際に利用するサービスですが、これによりSSL証明書を発行した上で、ELB、Route53、CloudFrontなどを利用してSSL証明書の設定が別途必要となります。

オプション３は不正解です。IAM証明書管理ではなく、通常はACMを使用してALBのドメインにすべてのSSL証明書をアップロードし、複数の証明書をロードバランサーの同じセキュアリスナーにバインドすることが必要となります。

詳細は以下を参照ください。

HTTPS CloudFront ディストリビューションから複数のドメインにサービスを提供 (amazon.com)

https://aws.amazon.com/jp/premiumsupport/knowledge-center/acm-add-domain-certificates-elb/

問題62: 正解

ある会社では多数のEC2インスタンスにホストされたアプリケーションを利用しています。サーバーとして利用するEC2インスタンスは30にも及んでいるため、パッチ管理を自動化することが運用上求められています。さらに、運用管理としてEC2インスタンスの構成状況が適切であることをモニタリングすることが求められており、その中でパッチ適用による変更点などを記録することも必要です。

この要件に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。

- (◉) AWS Systems Managerによってパッチ適用プロセスを自動化する。その上で、AWS Configを利用して、EC2インスタンスへのOSセキュリティパッチの適用状況などを記録する。 (正解)
- ( ) AWS Batchによってパッチ適用プロセスを自動化する。その上で、AWS Configを利用して、EC2インスタンスへのOSセキュリティパッチの適用状況などを記録する。
- ( ) Amazon Simple Workflowによってパッチ適用プロセスを自動化する。その上で、AWS Configを利用して、EC2インスタンスへのOSセキュリティパッチの適用状況などを記録する。
- ( ) Amazon DataPipelineによってパッチ適用プロセスを自動化する。その上で、AWS Configを利用して、EC2インスタンスへのOSセキュリティパッチの適用状況などを記録する。

説明

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において、インスタンスにパッチを適用するプロセスを自動化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。

また、パッチおよび関連付けのコンプライアンスステータスに対する全ての変更を記録するために、AWS Configを使用します。 AWS ConfigはAWSリソースの構成を評価、監査、評価できるサービスです。 Configは、AWSリソース設定を継続的に監視および記録し、記録された設定の評価を目的の設定に対して自動化します。

したがって、この２つを組み合わせたオプション１が正解となります。

オプション２は不正解です。AWS Batchを利用してもパッチ適用プロセスを構成することは可能ですが、その場合にはレコードを管理する運用体制が不可欠であり、これだけでは今回の要件には不十分です。

オプション３は不正解です。AWS SWFは複数のサーバーでパッチ等の自動処理の順番や振り分け管理を行うワークフローサービスです。これを利用してワークフローを自動化する際に利用することができますが、パッチ処理自体に特化したサービスではありません。展開・レコード・管理を実施する管理体制のためにはAWS Systems Manager PatchManagerとConfigを利用した仕組みによって、記録管理まで徹底して実施することができます。

オプション４は不正解です。AWS Data Pipeline は指定された間隔で、AWS のさまざまなコンピューティングサービスやストレージサービスや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支援するウェブサービスです。パッチプロセスの自動化には利用できません。

問題63: 正解

A社はオンプレミスとAWSの両方の環境でアプリケーション開発を行っているベンチャー企業です。開発チームはアジャイル開発を採用して、Chefを利用したCI/CDが実現できる開発環境を整備しています。最近になって、A社ではオンプレミス環境にホストされたRubyベースのアプリケーションを短期間でAWSプラットフォームに移行することになりました。新しい環境では可用性が高く、インフラストラクチャがコード化され、バージョンが適切に管理されることが要件となっています。また、開発チームのノウハウを活かした移行方式が望まれています。

この要件を満たすことができる最適なソリューションを選択してください。

- ◉ CloudFormationテンプレートのリソースタイプを AWS::OpsWorks::Stackとして、OpsWorksスタックを作成するための CloudFormationテンプレートを設定する。Rubyアプリケーションのレイヤーを Stackに追加する。 (正解)
- ○ OpsWorksを利用して、Chefを利用したインフラストラクチャーの自動設定を実現する。
- ○ OpsWorksスタックを作成するCodeDeployを設定する。設定内容としては CodeDeployのリソースタイプをAWS::OpsWorks::Stackとして、Javaレイヤーを Stackに追加する。
- ○ OpsWorksを利用して、Chefを利用したインフラストラクチャーのデプロイ構成を設定し、AWS Configと連携してバージョン管理を実施する。

説明

AWSリソースを利用したインフラ設定をコード化するという要件から、まずはCloudFormationの利用を検討します。また、開発チームのChefノウハウを利用するという要件から、OpsWorksも利用していくことになります。したがって、この2つを組み合わせた最適な利用方法が本件では問われています。

CloudFormationをAWS OpsWorksに連携して、インフラ整備を実行することができます。CloudFormationテンプレート内でOpsWorksコンポーネントをモデリングし、それらをCloudFormationスタックとしてプロビジョニングすることができます。これにより、OpsWorksの構成を文書化、バージョン管理、および共有できます。

統一されたCloudFormationテンプレートまたは個別のCloudFormationテンプレートを使用して、OpsWorksコンポーネントおよびAmazon VPCやAWS Elastic Load Balancerなどの他の関連AWSリソースを柔軟にプロビジョニングできます。設定内容としてはCloudFormationテンプレートのリソースタイプをAWS::OpsWorks::Stackとして、Rubyレイヤーを Stackに追加することが正しい設定となります。したがって、オプション1が正解となります。

オプション3は不正解です。CodeDeployではなく、CloudFormationを設定することが適切な設定方法となります。

オプション2と4も不正解です。OpsWorksを利用して、Chefを利用したインフラストラクチャーのデプロイ構成を設定するだけでは、バージョン管理などの高度な管理には不十分です。また、AWS Configと連携してバージョン管理という機能はありません。

問題64: 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、不動産企業に勤務しています。この会社でAWS Organizations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は組織全体の管理を担当します。1つのメンバーアカウントは調達部門に属しています。この調達部門が新規事業計画によってアウトソーシング化されることが決定されたため、既存のOUから削除することが求められています。ただし、マスターアカウント担当者がOUからメンバーアカウントを削除しようとすると、「アクセスが拒否されました」というメッセージが表示されました。

この失敗の原因として考えられる内容を選択してください。

- ◉ マスターアカウントでなければ、AWS OrganizationsのOUからメンバーアカウントを削除することができない。 (不正解)
- ○ メンバーアカウントが改めてルートアクセスキーからルートユーザー権限を設定しなければ、メンバーアカウントを削除できない。
- ○ メンバーアカウントの請求設定をIAMユーザーアクセスで有効化しないと、メンバーアカウントを削除できない。 (正解)
- ○ メンバーアカウントを独立させるためには再度AWSアカウントとしてクレジットカード情報登録から申請しなおす必要があり、メンバーアカウントを削除できない。

説明

組織をメンバーアカウントとして残したり、メンバーアカウントをマスターアカウントとして削除しようとすると、「アクセスが拒否されました」というメッセージが表示される原因は次の2つです。

■メンバーアカウントの請求設定をIAMユーザーアクセスで有効にした後でのみ、メンバーアカウントを削除できます。

■アカウントがスタンドアロンアカウントとして動作するために必要な情報を持っている場合にのみ、組織からアカウントを削除できます。

AWS Organizationsコンソール、API、AWS CLIコマンドを使用して組織内にアカウントを作成した場合、その情報が自動的に収集されるわけではありません。スタンドアロンとして使用する各アカウントについて、まずAWSカスタマーアグリーメントに同意してサポートプランを選択し、必須の連絡先情報を入力および確認して、支払方法を入力する必要があります。

したがって、オプション3が正解となります。

オプション1は不正解です。アカウントを独自に利用するためには必ずしもマスターアカウントとする必要はありません。メンバーアカウントも単独のAWSアカウントとして利用することが可能です。

オプション2は不正解です。メンバーアカウントはもともとは別個のAWSアカウントですので、ルートアカウントは設定されています。改めてルートアカウントを設定することは必要ありません。

オプション4は不正解です。メンバーアカウントを独立させるためには、再度AWSアカウントとしてクレジットカード情報の登録から実施する必要があるわけではありません。請求情報が登録されていない場合にかぎって、必須の連絡先などを登録しなおす必要があります。

問題65: 正解

あなたの会社はEC2インスタンスに対して、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。さらにカスタムドメイン名を持つCloudFrontを使用して、静的アセットと動的コンテンツを配信しています。現在CloudFront Webディストリビューションのキャッシュヒット率が10%未満であることが分かり、キャッシュヒット率を高める対応が必要です。

この要件を満たすことができる最適なソリューションの組合せを選択してください。 (2つ選択してください。)

- [x] オリジンが一意のオブジェクトを返すクエリ文字列パラメータのみを転送するように CloudFront を設定する。 (正解)
- [x] Cache-Control max-age に対して最も長い実用的な値を指定するようにオリジンを設定する。 (正解)
- [ ] エッジエンドポイントにおけるキャッシュ保持期間を最大化する。
- [ ] 署名付きURLを利用してコンテンツを配信する。
- [ ] 署名付きCookieを利用してコンテンツを配信する。

説明

このシナリオでは、CloudFront 配信のキャッシュヒット率が10%未満であることがわかり、キャッシュヒット率を高める設定方法が問われています。コンテンツのオリジンサーバーにアクセスするのではなく、CloudFront エッジキャッシュへのリクエストの比率を増やすことで、パフォーマンスを向上させる、つまりディストリビューションのキャッシュヒット率を向上させることができます。クエリ文字列パラメータに基づいてキャッシュするように CloudFrontを設定する場合、オリジンが一意のオブジェクトを返すクエリ文字列パラメータのみを転送するようにCloudFront を設定するなどしてキャッシュヒット率を改善できます。したがって、オプション1が正解となります。

Cache-Control max-age ディレクティブをオブジェクトに追加し、max-ageに対して最も長い実用的な値を指定するようにオリジンを設定することによって、キャッシュヒット率を向上させることができます。したがって、オプション 2 が正解となります。

オプション 3 は不正解です。エッジエンドポイントと呼ばれるロケーションがそもそもありません。

オプション 4 は不正解です。署名付きURLを利用してコンテンツを配信することで、コンテンツを閲覧できるユーザーを制限することができます。キャッシュ率の向上には利用されません。

オプション 5 は不正解です。署名付きCookieを利用してコンテンツを配信することで、コンテンツを閲覧できるユーザーを制限することができます。キャッシュ率の向上には利用されません。

その他の方法については以下を参照してください。
https://docs.aws.amazon.com/ja_jp/AmazonCloudFront/latest/DeveloperGuide/cache-hit-ratio.html

問題66: 不正解

あなたの会社はAWSを利用して新しい決済管理システムを構築しています。このシステムでは将来を見越して、IPv6アドレスをサポートすることが要件となっています。あなたは構築に向けて、単一のパブリックサブネットとインターネットゲートウェイを使用して仮想プライベートクラウド（VPC）をセットアップし、インターネット経由の通信を可能にする設定を行っているところです

この要件を満たすための設定方法を選択してください。

- ◉ /16 の IPv4 CIDR ブロックを持つ VPC を作成し、/16 の IPv6 CIDR ブロックを VPC と関連付ける。 (不正解)
- ○ /16 の IPv4 CIDR ブロックを持つ VPC を作成し、/56 の IPv6 CIDR ブロックを VPC と関連付ける。 (正解)
- ○ /56 の IPv4 CIDR ブロックを持つ VPC を作成し、/56 の IPv6 CIDR ブロックを VPC と関連付ける。
- ○ /56の IPv4 CIDR ブロックを持つ VPC を作成し、/16 の IPv6 CIDR ブロックを VPC と関連付ける。

説明

EC2インスタンスがIPv6を介してインターネットと通信できるようにするには、VPCで次の設定を行う必要があります。

・IPv6 CIDR ブロックと 1 つのパブリックサブネットを持つデフォルトでない VPC を作成します。サブネットを使うと、インスタンスをセキュリティや運用上の必要に応じてグループ化することができます。その際には、/16 の IPv4 CIDR ブロックを持つ VPC を作成し、/56 の IPv6 CIDR ブロックを VPC と関連付けます。IPv6 CIDR ブロックのサイズ (/56) は固定されており、IPv6 アドレスの範囲は、Amazon の IPv6 アドレスのプールから自動的に割り当てられます (独自の IPv6 アドレス範囲を指定することはできません)。

・特定のポートのみからトラフィックを許可するセキュリティグループをインスタンスに作成します。

・サブネット内に Amazon EC2 インスタンスを起動し、起動時に IPv6 アドレスをインスタンスに関連付けます。IPv6 アドレスはグローバルに一意であり、インスタンスがインターネットと通信できるようにします。

・VPC の IPv6 CIDR ブロックをリクエストできます。このオプションを選択すると、IPV6 CIDR ブロックをアドバタイズする場所であるネットワーク境界グループを設定できます。ネットワーク境界グループを設定すると、CIDR ブロックがこのグループに制限されます。

したがって、オプション 2 が正解となります。

問題67: 不正解

B社ではオンプレミス環境に読み取り集中型のMySQLデータベースを有しています。最近になって、このデータベースを含めたオンプレミス環境にあるインフラをAWSに移行することが決定されました。あなたは移行担当者として、 VPC内に移行するデータベースに対して、最大限に高可用性とスケーラビリティを確保するように依頼されました。

この要件を満たすために最適なソリューションを選択してください。

- ◉ RDSをマルチAZで展開してフェールオーバー構成を実現する。さらに別リージョンに同じ構成を再現して、Route53によるフェールオーバールーティングを設定する。 (不正解)
- ○ クロスリージョンレプリケーション（CRR）はS3の機能であるため、クロスリージョンレプリケーション機能を有効にする。
- ○ MySQLデータベースのAuroraクラスターを作成し、Auto Scalingを使用してAuroraリードレプリカを自動的にプロビジョニングする。 (正解)
- ○ RDSをマルチAZで展開してフェールオーバー構成を実現する。

説明

オプション3が正解となります。このシナリオでは、 VPC内に移行するデータベースに対して、最大限に高可用性とスケーラビリティを確保することが必要です。したがって、RDSではなく、Amazon Auroraを利用した構成を活用します。Amazon Aurora は、標準的な MySQL データベースと比べて最大で 5 倍、標準的な PostgreSQL データベースと比べて最大で 3 倍高速化することが可能なリレーショナルデータベースです。

さらにワークロード要件を満たすために、Aurora Auto Scalingを設定します。Aurora Auto Scalingはシングルマスターレプリケーションを使用して、Aurora DB クラスターは急激な接続やワークロードの増加を処理できます。接続やワークロードが減ると、Aurora Auto Scaling は未使用のプロビジョニングされた DB インスタンスに対する料金が発生しないように不要な Aurora レプリカを削除します。 したがって、MySQLデータベースのAuroraクラスターを作成し、Auto Scalingを使用してAuroraリードレプリカを自動的にプロビジョニングするのが正しい答えです。

オプション 1 と 4 は不正解です。RDSではなくAuroraを利用することで最大限の高可用性とスケーラビリティを確保することが必要です。また、AuroraでもRDSでもリードレプリカをマルチリージョンに展開することで、マルチリージョン構成が可能となります。

オプション 2 は不正解です。クロスリージョンレプリケーション（CRR）はS3の機能であるため、クロスリージョンレプリケーション機能を有効にすることは正しくありません。

問題68: 不正解

B社ではCloudFormationを利用したインフラ構築のテンプレート化を整備しているところです。あなたはソリューションアーキテクトとして、大規模なオンデマンドEC2インスタンスを起動し、サードパーティアプリケーションパッケージをインストールするCloudFormationテンプレートを設計しています。今回の作業では、 CloudFormation スタックの更新中に Auto Scaling グループを更新する設定が必要です。

この要件を満たすために最適なソリューションを選択してください。

- ◉ cfn-signalヘルパースクリプトを使用して、AutoScalingリソースのCreatePolicy属性とAutoScalingRollingUpdate ポリシーを利用して、更新方法を設定する。 (不正解)
- ○ cfn-signalヘルパースクリプトを使用して、AutoScalingリソースのUpdatePolicy属性とWaitOnResourceSignalsIsUpdataポリシーを利用して、更新方法を設定する。
- ○ cfn-signalヘルパースクリプトを使用して、AutoScalingリソースのUpdatePolicy属性とAutoScalingRollingUpdate ポリシーを利用して、更新方法を設定する。 (正解)
- ○ cfn-signalヘルパースクリプトを使用して、AutoScalingリソースのCreatePolicy属性とWaitOnResourceSignalsCreateポリシーを利用して、更新方法を設定する。

説明

cfn-signalヘルパースクリプトはAWS CloudFormationに信号を送り、Amazon EC2インスタンスが正常に作成されるか、更新されたかどうかを示すことができます。インスタンスにソフトウェアアプリケーションをインストールして設定する場合、それらのソフトウェアアプリケーションの準備ができたらCloudFormationにシグナルを送ることができます。

AWS::AutoScaling::AutoScalingGroup リソースは、UpdatePolicy 属性 を使用して、CloudFormation スタックが更新されるときの Auto Scaling グループリソースの更新方法を定義します。UpdatePolicy 属性が正しく設定されていない場合、ローリング更新によって予期しない結果が生成される可能性があります。 CloudFormation は AutoScalingRollingUpdate ポリシー を使用して Auto Scaling グループのローリング更新を制御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。

問題69: 不正解

あなたは新しいSNS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ではユーザーが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。この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を設定した構成になっています。SSL通信を最適化するためには、定期的にロードバランサーにデプロイされた既存のCA証明書を、IAMにアップロードされている新しい証明書に置き換える必要があります。 このタスクは、AWS CLIを使用してプログラムで実行する必要があります。

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

- [x] set-load-balancer-policies-for-backend-serverコマンドを使用して、新しい証明書をロードバランサーに追加する。 (不正解)
- [x] aws acm renew-certificateコマンドを使用して証明書を更新する。 (不正解)
- [ ] set-load-balancer-listener-ssl-certificateコマンドを使用して証明書を設定する。 (正解)
- [ ] get-server-certificateコマンドを使用して、証明書のARNを取得する。 (正解)
- [ ] aws acm reset-certificateコマンドを使用して証明書を更新する。

説明

ウェブサイトまたは AWS にホストされたアプリケーションへの HTTPS 接続を有効にするには、SSL/TLS サーバー証明書が必要です。AWS Certificate Manager (ACM) によってサポートされているリージョンの証明書では、ACM を使用して、サーバー証明書をプロビジョン、管理、およびデプロイすることが推奨されています。サポートされていないリージョンでは、IAM を Certificate Manager として使用する必要があります。各証明書には有効期限があるため、有効期間が終了する前に、証明書を更新または置き換えることが必要です。

IAM API を使用して証明書を取得するには、GetServerCertificate リクエストを送信します。get-server-certificateコマンドを使用して、証明書のARNを取得することができます。したがって、オプション 4 は正解となります。

取得した証明書を設定するためには、set-load-balancer-listener-ssl-certificateコマンドを使用して証明書を設定します。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。 set-load-balancer-policies-for-backend-server コマンドを使用して、my-authentication-policy を HTTPS のインスタンスポートに設定することができます。これは証明書の設定には利用しません。

オプション 2 は不正解です。aws acm renew-certificateコマンドはありません。

オプション 5 は不正解です。aws acm reset-certificateコマンドはありません。

問題70: 不正解

あなたはソリューションアーキテクトとして、AWS上に進捗共有モバイルアプリを運用しています。このアプリでは建設現場の最新写真をアップロードして共有することで視覚的に進行状況を管理することができます。S3バケットの内容を変更し、インターネット経由でパートナー企業にレポートを送信する機能を追加することになりました。そこで、あなたはVPCのプライベートサブネットでホストされる追加機能アプリケーションを開発しています。この要件のためにS3のゲートウェイVPCエンドポイントを作成しました。

この要件を満たすために実施すべきエンドポイントの設定を選択してください。

- ◉ NATゲートウェイを使用してトラフィックをS3向けのVPCエンドポイントへのルートを設定する。 (不正解)
- ○ プライベートサブネットのルートテーブルを更新してS3向けのVPCエンドポイントへのルートを設定し、アウトバウンドのインターネットトラフィックをNATゲートウェイに送信する。 (正解)
- ○ プライベートサブネットのルートテーブルを更新して、すべてのトラフィックをパブリックVPCエンドポイントに直接送信する。
- ○ パブリックサブネットのルートテーブルを更新してS3向けのVPCエンドポイントへのルートを設定し、アウトバウンドのインターネットトラフィックをインターネットゲートウェイに送信する。

説明

VPCエンドポイントは、AWS PrivateLinkを使用するAWSサービスやVPCエンドポイントサービスにVPCをプライベートに接続できます。このシナリオでは、インターネット経由でパートナー企業にS3バケット内に保存されたレポートを送信する機能を追加することになり、S3バケットに対するVPCエンドポイントを介した接続設定が求められています。これを実現するため、プライベートサブネットのルートテーブルを更新してS3向けのVPCエンドポイントへのルートを設定し、アウトバウンドインターネットトラフィックをNATゲートウェイに送信できます。したがって、オプション2が正解となります。

オプション1は不正解です。インターネット接続要件にNATゲートウェイを使用することはできますが、VPCエンドポイントトラフィックをNATゲートウェイ経由で転送できないため、正しくありません。

オプション3は不正解です。プライベートサブネットからインターネットにトラフィックを送信するにはNATゲートウェイが必要であるため、正しくありません。

オプション4は不正解です。パブリックサブネットではなく、プライベートサブネットのルートテーブルによって設定をする必要があります。

問題71: 正解

A銀行はAWSを利用したハイブリッドネットワークアーキテクチャを採用しています。そして、金融機関として機密データ保護の観点から年に一度システム監査を実施しています。最近の監査において重要な銀行レコードを保存するためのS3バケットのオブジェクトデータに対して暗号化が実施されていないことが問題であると指摘されました。よって、あなたはソリューションアーキテクトとして、S3バケットにSSE-Cを使用したサーバーサイド暗号化を実装して、保管時のデータセキュリティを確保する対応を実施しています。

この要件を満たすために必要となるアプリケーション上の設定方式を選択してください。

- (●) Amazon S3 REST APIコールにおいて、HTTPリクエストヘッダーに次の要素を入れる。
  x-amz-server-side-encryption-customer-algorithm (正解)
  x-amz-server-side-encryption-customer-key
  x-amz-server-side-encryption-customer-key-MD5
- ( ) Amazon S3 REST APIコールにおいて、HTTPリクエストヘッダーに次の要素を入れる。
  x-amz-server-side-encryption-customer-algorithm
- ( ) Amazon S3 REST APIコールにおいて、HTTPリクエストヘッダーに次の要素を入れる。
  x-amz-server-side-encryption-customer-key
  x-amz-server-side-encryption-customer-key-MD5
- ( ) Amazon S3 REST APIコールにおいて、HTTPリクエストヘッダーに次の要素を入れる。
  x-amz-server-side-encryption-customer-algorithm
  x-amz-server-side-encryption-customer-key-MD5

説明

Amazon S3にオブジェクトをアップロードすると、Amazon S3はSS[redacted]より提供された暗号化キーを使用してデータにAES-256暗号化を適用して暗号化[redacted]します。アプリケーション上でSSE-Cを利用するためには、Amazon S3 REST API呼び出し時に、次の3つのHTTPリクエストヘッダーを全て含める必要があります。

x-amz-server-side-encryption-customer-algorithm
x-amz-server-side-encryption-customer-key
x-amz-server-side-encryption-customer-key-MD5

したがって、オプション1が正解となります。

問題72: 不正解

大手ゲーム企業はAWSを利用したモバイルアプリケーションを構築しています。Webサービスは複数のEC2インスタンスで実行され、CLBとAutoScalingが設定されており、EC2インスタンスが2つのアベイラビリティーゾーンに均等に分割されています。データ層にはDynamoDBが利用されており、セッション管理に利用されています。アプリケーションの公式リリース後、多くのユーザーが製品に同時に接続するために、着信トラフィックが急増しています。それによって、一部のユーザーがゲームからタイムアウトするという問題が発生しているようです。

この問題に関連した詳細情報を把握することができるCloudWatchメトリクスはどれでしょうか？（2つ選択してください。）

- [x] HealthyHostCoun (不正解)
- [x] SurgeQueueLength (正解)
- [ ] UnHealthyHostCount
- [ ] SpilloverCount (正解)
- [ ] RequestCount

説明

SurgeQueueLengthメトリクスは正常なインスタンスへのルーティングを保留中のリクエスト (HTTP リスナー) または接続 (TCP リスナー) の合計数を提供してくれます。これによって、保留中のリクエスト総数を把握することで、着信トラフィックの状況を確認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。

オプション4も正解となります。着信トラフィックが急増した場合に、SpilloverCountはサージキューがいっぱいとなったために拒否されたリクエストの総数を返します。これは着信トラフィックが急増した際に拒否数を把握する際に利用します。

オプション1は不正解です。HealthyHostCountメトリクスはロードバランサーに登録された正常なインスタンス数のみを示します。これは、すべてのインスタンスが正常であることを知っているため、あまり役に立ちません。

オプション3は不正解です。UnHealthyHostCountはロードバランサーに登録された異常なインスタンス数のみを示すため、正しくありません。

オプション5は不正解です。RequestCountは指定された間隔 (1分または5分) の間に完了したリクエスト数、または接続数を確認します。これは単純な総数ですので、トラフィックの問題点を把握するのには不十分な情報です。

問題73: 不正解

A社は動画再生プラットフォームをAWSを利用して構築しています。これはグローバルな規模で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によるエッジ配信を行うCDNを設定しました。しかしながら、実行するとAmazon CloudFront が "The request could not be satisfied.Bad Request. (リクエストに失敗しました。無効なリクエストです。)" というエラーを返してしまいます。

このエラーに対応するための解決策として正しい組み合わせはどれでしょうか？（2つ選択してください。）

- [x] ビューワーのプロトコルポリシーにおいて、「HTTP only」を選択する。 (不正解)
- [x] ビューワーのプロトコルポリシーにおいて、「HTTP and HTTPS」 または「Redirect HTTP to HTTPS」のいずれかを選択する。 (正解)
- [ ] CloudFrontディストリビューションと関連付ける CNAME を設定する。 (正解)
- [ ] CloudFrontディストリビューションと関連付けるALIAS を設定する。
- [ ] CloudFrontディストリビューションと関連付けるARNを設定する。
- [ ] ビューワーのプロトコルポリシーにおいて、「HTTPS only」を選択する。

説明

この "The request could not be satisfied.Bad Request. (リクエストに失敗しました。無効なリクエストです。)" というエラーメッセージは、クライアントからのエラーであり、次のいずれかの理由で発生する可能性があります。

■リクエストが HTTP を通じて開始されたが、CloudFront ディストリビューションは HTTPS のリクエストだけを許可するように設定されている。

この場合は、ビューワーのプロトコルポリシーにおいて、(HTTP and HTTPS または Redirect HTTP to HTTPSのいずれかを選択します。したがって、オプション 2 が正解となります。

■リクエストされた代替ドメイン名 (CNAME) が CloudFront ディストリビューションと関連付けられていない。

この場合はICloudFront ディストリビューションと関連付ける CNAME を入力します。したがって、オプション 3 が正解となります。

問題74: 不正解

あなたはサーバレスアーキテクチャーを得意としたエンジニアです。現在はA社のAWS開発者として勤務しています。あなたはCloudFormationを使用して、API GatewayからLambdaを呼び出して、DynamoDBへとデータを記録・取得するサーバーレスアプリケーションをデプロイしています。その際に、AWS SAM構文において、SAMバージョンを指定する必要があるテンプレート上にリソースを宣言することが必要です。

CloudFormationテンプレートにおいて、リソースセクション以外に設定するべき内容を選択してください。（2つ選択してください。）

- [x] AWS::Serverless に AWS SAMのバージョンを指定する。 (正解)
- [x] AWS::SAM に使用する AWS SAMのバージョンを指定する。 (不正解)
- [ ] AWS::Serverless オプションの AWS SAM の有効化を設定する。
- [ ] AWS::Serverless オプションの Transform を設定する。 (正解)
- [ ] AWS::SAM オプションのTransform を設定する。

説明

このシナリオでは、Lambdaサーバーレスアプリケーションをデプロイする際に、CloudFormationテンプレート上でリソースセクション以外に設定するべき内容を選択することが求められています。そのためには、AWS::Serverless Transformの設定において、使用する AWS SAM バージョンを指定することが必要です。したがって、オプション１と４が正解となります。

CloudFormationのオプションの Transform セクションでは、CloudFormation テンプレートを処理するために使用するマクロを１つ以上指定します。Transform セクションではテンプレート内で１つ以上のマクロを宣言できます。マクロはAWS CloudFormation によって、指定された順序で実行されます。変更セットを作成すると、AWS CloudFormation は処理されたテンプレートコンテンツを含む変更セットを生成します。その後、変更内容を確認して変更セットを実行できます。

オプション２は不正解です。AWS::SAMではなく、AWS::Serverless に使用する AWS SAMのバージョンを指定する必要があります。

オプション３は不正解です。AWS::Serverless オプションでは、AWS SAM の有効化を設定するといった対応は実施しません。Transform の設定をすることが必要です。

オプション５は不正解です。AWS::SAM オプションにTransform を設定するのではなく、AWS::Serverless オプションに Transform を設定する必要があります。

問題75: 不正解

デザイン会社はオンプレミス環境のデザインツールを利用して、デザイン用写真を大量に保存・編集しています。その際は、オンプレミス環境の専用サーバー群を使用して一定サイズのキューによる分散処理によってデータを並行処理しています。処理前のデータはオンプレミス環境にあるストレージに保存され、処理後のデータはテープに送られて、オフサイトのストレージにアーカイブされ、利用時にデータ取得されます。処理後のデータはたまに利用される程度であり、データ取得には数分要しても問題ありません。あなたはソリューションアーキテクトとして、このオンプレミス環境のデータ処理の仕組みをAWSへと移行することで、コスト最適化を進めるように依頼されました。

要件を達成することができる、最もコスト効率がよいアーキテクチャ構成を選択してください。

- ◉ SQSにキューイングによってポーリングされたオンデマンドインスタンスによって並列処理を実行する。その上で、SQSキューサイズによってトリガーされるAutoScalingを設定して負荷に応じてスポットインスタンスを増強する。処理前のデータはS3 RRSストレージに保存してデータ処理プロセスを進めて、処理後のデータはGlacierへと保存する。 (不正解)

- ○ SQSにキューイングによってポーリングされたオンデマンドインスタンスによって並列処理を実行する。その上で、CloudWatchカスタムメトリクスによってキューの最適なメトリクスを設定した上で、AutoScalingを設定して負荷に応じてスポットインスタンスを増強する。処理前のデータはS３標準ストレージに保存してデータ処理プロセスを進めて、処理後のデータはGlacierへと保存する。 (正解)

- ○ SQSにキューイングによってポーリングされたオンデマンドインスタンスによって並列処理を実行する。その上で、ELBのトラフィック処理量応じてトリガーされるAutoScalingを設定して負荷に応じてオンデマンドインスタンスを増強する。処理前のデータはS3 RRSストレージに保存してデータ処理プロセスを進めて、処理後のデータはGlacierへと保存する。

- ○ SQSにキューイングによってポーリングされたオンデマンドインスタンスによって並列処理を実行する。その上で、ELBのトラフィック処理量に応じてトリガーされるAutoScalingを設定して負荷に応じてスポットインスタンスを増強する。処理前のデータはS３標準ストレージに保存してデータ処理プロセスを進めて、処理後のデータはGlacierへと保存する。

説明

このシナリオでは、オンプレミス環境で実行しているデータ処理の仕組みと写真のアーカイブとメッセージング処理をAWSサービスに置き換えて、移行することが求められています。したがって、並列処理が必要な複数サーバーでのプロセス処理にはSQSメッセージによるポーリングを利用することが望ましいです。SQSキューイング処理に対してAutoScalingを設定する場合は、CloudWatchカスタムメトリクスによってキューの最適なメトリクスを設定して、それに応じてAutoScalingが実行できるように設定します。

S3ストレージのRRSは現在は利用されていないため、処理前データはRRSではなくS3標準ストレージを利用します。処理が進んでアーカイブの段階になったら中長期保存用にGlacierへとデータ移行します。長期保存にはRRSやIAクラスよりも中長期保存に向いていてコストも一番安いGlacierが最適です。今回はデータの取り出しに高速性は求められていないためGlacierで問題ありません。したがって、オプション２が正解となります。

GlacierはS3とはことなり、ストレージクラスのように取り出し方式が事前に決定されているわけではありません。データ取り出しを実施する際に迅速取り出しを設定して抽出することが可能です。そのため、Glacierを選択すれば数分での取り出しは保証されていることになります。

SQSのスケーリングについての詳細は以下のページを参照ください。

https://docs.aws.amazon.com/ja_jp/autoscaling/ec2/userguide/as-using-sqs-queue.html

オプション１は不正解です。SQSキューサイズによってトリガーされるAutoScalingを設定して負荷に応じてスポットインスタンスを増強することも可能ですが、今回のケースでは、もともとサイズが固定されたキューによる分散処理が行われているため、負荷ピークになってもキューサイズが増強されることがありません。そのため、スケーリングトリガーとしては不適切です。また、S3 RRSストレージは推奨されていません。

オプション３と４は不正解です。回の構成では、SQSにキューイングのメッセージ量に応じてスケーリングすることが必要となるため、ELBのトラフィック処理量に基づいたスケーリングでは意味がないため、不正解となっています。