25-26-27

1 あなたの会社は顧客の多様なニーズに応じてカスタムメイドの自転車を販売している自転車メーカーです。現在の製造プロセスは自転車を組み立てるために世界最高水準の製品評価システムを導入したプロセスを実行しており、利用するデータが豊富にあり、複雑なプロセスとなっています。製品の品質評価においては、人による評価とシステムによる自動評価が混合していますが、出来る限りのプロセスの自動化が求められています。プロセスでは子プロセスを作成して、画像識別による一時的な評価と人の目による二次的評価を実施した上で、親プロセスに評価結果を返信するためのフローが必要です。

この要件を満たすために、AWSを活用したソリューションアーキテクチャを選択してください。

- ○ Amazon SWFを利用して、評価プロセスと複雑なデータの移動を管理する品質評価プロセスを導入する。プレイスメントグループに入れたG4インスタンス群を利用して、Amazon Rekognitionによる自動評価の仕組みを導入する。
- ◉ AWS Step Functionsを利用して、評価プロセスと複雑なデータの移動を管理する品質評価プロセスを導入する。プレイスメントグループに入れたG4インスタンス群を利用して、製品検品AIソリューションを構築する。 (不正解)
- ○ Lambdaファンクションを利用して、評価プロセスと複雑なデータの移動を管理する品質評価プロセスを導入する。Amazon Rekognitionを設定したインスタンス群にAutoScalingグループを設定する。
- ○ Amazon SQSを利用して、評価プロセスと複雑なデータの移動を管理する品質評価プロセスを導入する。Amazon Maching Learningによる機械学習を利用した自動評価を実施してから、人の評価プロセスを実施する。
- ○ Amazon SWFを利用して、評価プロセスと複雑なデータの移動を管理する品質評価プロセスを導入する。プレイスメントグループに入れたG4インスタンス群を利用して、製品検品AIソリューションを構築する。 (正解)

説明

オプション５が正解となります。このシナリオでは、製品検品作業を自動化するワークフローに対してAIを導入して自動化する方法と、子プロセスと親プロセスに分岐したフロー作成の方法が問われています。その際にAI画像識別を利用した検品と人の目による検品の両方が必要であり、それを成立させるためにAmazon SWF を利用したプロセス管理を導入します。

Amazon SWF はクラウド内の完全マネージド型の状態トラッカー、およびタスクコーディネーターとして利用されるワークフローの作成サービスです。各種のAWSサービスを利用して、並行したステップまたは連続したステップがあるバックグラウンドジョブを構築、実行、スケールするのに役立ちます。子プロセスと親プロセスに分岐したフロー作成の方法が

AI画像解析には低レイテンシーネットワーキングでデータの高度なグラフィカル処理に特化したG2インスタンスを使用してインスタンスに組み込むことが求められます。AWS ではワークフロー作成にはSWFではなくAWS Step Functions の利用が推奨されていますが、プロセスの処理結果を親プロセスに返答する必要がある場合はAmazon SWFの使用が求められます。

詳細は以下をご参照ください。

https://aws.amazon.com/jp/step-functions/faqs/

画像検品作業にはAmazon Rekognitionを利用するか、Amazon GPUインスタンスタイプを利用した画像検品ソリューションを導入するかの２つの選択肢があります。今回は要件からG4インスタンスを利用した画像検品ソリューションを導入することが正解となります。Amazon Rekognitionは画像検品ソリューションに特化したサービスではないため、G4インスタンスによるソフトウェアを導入することが効率的なプロセスを実現することができます。低レイテンシネットワーキングを備えた高度なグラフィック処理サーバーについて言及する場合は、EC2インスタンスのG4インスタンスが最適です。

オプション１と３は不正解です。画像検品作業にはAmazon Rekognitionを利用したソリューションは可能ですが、これはAPIで提供されているため、G4インスタンスを必要としません。また、Lambda関数やAWS Data Pipelineでワークフローを実装することもできません。

オプション２は不正解です。AWS Step Functions では、AWS の複数のサービスをサーバーレスのワークフローに整理できるため、SWFよりも素早くアプリケーションをビルドおよび更新できます。これにより、SWFよりも視覚的に容易にワークフローを作成できるため、現在ではAWS Step Functionsの利用が推奨されています。しかしながら、プロセスにおいて介入する外部信号が必要な場合、または結果を親に返す子プロセスを起動する場合は、AWS Step Functions では対応できないため、Amazon SWFを使用することが求められています。

オプション４は不正解です。SQSでキューイング処理でプロセス間を連携することができても、ワークフロー自体を設定することはできないため、正しくありません。また、Amazon Machin Learningは主に数値データを利用した予測分析を得意としており、画像識別ソリューションには適していません。

大手印刷会社はWEBアプリケーションをオンプレミス環境にホストしています。サーバーの老朽化によってリプレースが必要となっており、新しいサーバーに切り替えるタイミングでAWSに移行することを決定しました。 オンプレミス環境では各種サーバーにおいて、DB2、SAP、Windowsオペレーティングシステムサーバー（仮想化サーバーとして利用）などのライセンスを使用しており、これらのライセンスごとAWSに移行する予定です。ライセンス管理ではライセンス数に応じた契約管理を実施しています。数年に１回ライセンス監査を受けることが必要であり、その管理と違反チェックが必要不可欠です。

この要件を満たすための移行方法とライセンス管理方法を選択してください。

- (◉) **ライセンスに見合ったRDS DBインスタンスやWindows OS AMIを利用してAWSへの移行を実施する。その上で、AWS License Managerによりライセンスルールを定義して、ライセンス対象となるソフトウェアをインストールしたEC2インスタンスに適用する。AWS License Managerコンソールを利用してライセンス利用状況を追跡する。** (不正解)

- ( ) **AWS MGNを利用してEC2インスタンスにライセンスソフトウェアをインストールして移行を実施する。その上で、AWS License Managerによりライセンスルールを定義して、ライセンス対象となるソフトウェアをインストールしたEC2インスタンスに適用する。AWS License Managerコンソールを利用してライセンス利用状況を追跡する。** (正解)

- ( ) **AWS Server Migration Serviceを利用してEC2インスタンスにライセンスソフトウェアをインストールして移行を実施する。その上でAWS License Managerによりライセンスルールを定義して、ライセンス対象となるソフトウェアをインストールしたEC2インスタンスに適用する。AWS License ManagerのCloudWatchログを有効化して、ライセンス利用状況を追跡する。**

- ( ) **AWS Server Migration Serviceを利用してEC2インスタンスにライセンスソフトウェアをインストールして移行を実施する。その上で、AWS License Managerによりライセンスルールを定義して、ライセンス対象となるソフトウェアをインストールしたEC2インスタンスに適用する。AWS License Managerコンソールを利用してライセンス利用状況を追跡する。**

説明

オプション２が正解となります。このシナリオではライセンスを継続する方式でのAWSへの移行方法と、そのライセンスの管理方法の２つの要件が求められています。前者はライセンスをそのままAWSに移行するために、EC2インスタンスに利用しているソフトウェアをインストールする方式が正解となります。そのためには、~~AWS Application Migration Service (AWS MGN)~~を利用して、EC2インスタンスへとアプリケーションを移行することが必要です。

AWS Application Migration Service は、ソースサーバーを物理インフラストラクチャ、仮想インフラストラクチャ、およびクラウドインフラストラクチャから AWS で実行可能なように自動的に変換することにより、時間のかかる、エラーが発生しやすい手動プロセスを最小限に抑えつつ、オンプレミス環境にあるサーバーをAWSへと移行します。

さらにAWS License Managerによってライセンスルールを定義して、ライセンス対象となるソフトウェアをインストールしたEC2インスタンスに適用することができます。また、AWS License Managerコンソールを利用してライセンス利用状況を追跡することができます。AWS License Manager は、ソフトウェアベンダーのライセンスを簡単に管理できるようになるサービスです。AWS License Manager により、管理者はライセンス契約の規約をエミュレートするカスタマイズされたライセンスルールを作成し、EC2 のインスタンスの起動時にそれらのルールを適用できます。管理者はこれらのルールを使用して、契約が定める以上のライセンスを使用する、または短期的に異なるサーバーにライセンスを再度割り当てるといったライセンス違反を規制することができます。

オプション１は不正解です。RDSはDB2をデータベースエンジンとして利用することができない上に、AWSのマネージド型のデータベースサービスで代替してしまうとライセンスを継続利用ができません。AWS Systems Managerにはライセンス管理機能はないため、正しくありません。

オプション３は不正解です。AWS License Managerの操作方法として間違った内容が記述されているため、正しくありません。また、AWS Server Migration Serviceは現在は利用停止したサービスとなっています。

オプション４は不正解です。AWS Server Migration Serviceは現在は利用停止したサービスとなっています。

https://aws.amazon.com/jp/application-migration-service/

3

B社はサードパーティのWEBアプリケーションを使用したいと考えています。このアプリケーションを利用するためには、B社のアカウント内で実行されているEC2インスタンスへのAPI経由によるアクセスを実施するアクセス権が必要となります。そのためには、サードパーティのWebアプリケーションに対してB社のAWSアカウントのEC2インスタンスへと連携するための外部アクセス設定が必要となります。B社のセキュリティポリシーによると、WEBアプリケーションの提供ベンダーが使用する資格情報は、そのベンダーのみが利用できるように制限することが必要です。したがって、第三者による目的外利用ができない形式で権限を付与することが必須となります。

これらの条件をすべて満たす方法を選択してください。

- ◉ **WEBアプリケーションが必要とする権限のみに限定したアクセス権限を付与したIAMポリシーを設定して、それに基づいたクロスアカウントアクセスが可能となるIAMロールを作成し、WEBアプリケーションに設定する。** (正解)
- ○ **EC2インスタンスへのAPIにアクセス権限を有したIAMロールをEC2インスタンスへと割り当てて、EC2インスタンスとWEBアプリケーションと連携する。**
- ○ **WEBアプリケーションが必要とする権限のみに限定したアクセス権限を有したIAMロールをAPI Gatewayに設定して、WEBアプリケーションと連携する。**
- ○ **WEBアプリケーションが必要とする権限のみに限定したアクセス権限ベンダーに与えるIAMユーザーを設定して、AWS Organizationsによるクロスアカウント連携を実施する。**

説明

WEBアプリケーションが必要とする権限のみに限定したアクセス権限を付与したIAMポリシーを設定して、それによってクロスアカウントアクセスが可能となるIAMロールを作成し、該当WEBアプリケーションに設定します。これにより、第三者に資格情報を漏洩することなく、IAMロールの管理によって第三者の情報もコントロールすることができるようになります。したがって、オプション1が正解となります。

異なるAWSアカウント上のリソースへのアクセスを委任する方法として、クロスアカウントアクセス許可とIAMロールを設定します。これによって、特定のアカウントにある特定のリソースを別のアカウントのユーザーと共有します。クロスアカウントアクセスを設定することで、利用者はアカウントごとにIAM ユーザーを作成する必要がなくなります。

オプション2は不正解です。この方式ではEC2インスタンスとWEBアプリケーションとを連携するための権限委任が必要となる可能性があり、かつ処理が複雑となるため非効率な方法となります。また、EC2インスタンスへのAPIにアクセス権限を有したIAMロールをEC2インスタンスに割り当てるだけでは、第三者への限定的な委任が明確に実施できません。

オプション3は不正解です。アクセス権限を有したIAMロールをAPI Gatewayに設定して、WEBアプリケーションと連携することでは、権限を第三者に割り当てることができません。API GatewayのAPIリクエストはIAMロールなどの権限がない外部システムやユーザーから実行が可能です。

オプション4は不正解です。AWS Organizationsはアカウントで IAM ロールを使って、特定のAWSアカウントのリソースへのアクセス権を別の AWS アカウントに付与できますが、その際はIAMユーザーを利用するわけではないため、説明文に誤りがあります。

4 大手商社では社内業務用のWEBアプリケーションをAWS上で構築しています。このサイトはパブリックサブネットに設置されたWebサーバーとして機能する一連のオンデマンドEC2インスタンスで構成されています。これらのEC2インスタンスはインターネットを経由して更新プログラムや重要なセキュリティパッチを取得して運用されていますが、その際はパッチ更新や社内WEBサイトからのアクセスなどの特定URLからのアクセスに限定したいと考えています。したがって、特定URLからのリクエストのみに限定したアクセスができるようEC2インスタンスを設定する必要があります。

このシナリオに対応する最適なアーキテクチャは次のうちどれですか？

- ◉ WEBアプリケーションを設置したサブネットに対して、明確な拒否ルールを設定したネットワークACLを設定して、全ての特定URLアクセスをコントロールする。 (不正解)
- ○ 新しいNATゲートウエイをVPCに設置して、プライベートサブネットにあるEC2インスタンスをNATゲートウエイに接続できるようにする。このNATゲートウエイがアウトバンドのURL制限を管理する。
- ○ 新しいNATインスタンスをVPCに設置して、プライベートサブネットにあるEC2インスタンスをNATインスタンスに接続できるようにする。このNATインスタンスによってアウトバンドのURL制限を管理する。
- ○ 新しいプロキシサーバーを設置して、WEBアプリケーションによって提供される特定URLからのアクセスのみを許可するようにVPCのルート設定を変更する。 (正解)
- ○ WEBアプリケーションのEC2インスタンスに対して、明確な拒否ルールを設定したセキュリティグループを設定して、全ての特定URLアクセスをコントロールする。

説明

オプション4が正解となります。VPCにおけるデフォルトのネットワークルートを削除して、新しいプロキシサーバーへのルートを設定することが必要です。プロキシサーバーはWEBアプリケーションによって提供される特定URLからのアクセスのみを許可することで、EC2インスタンスは、ユーザーからのインバウンドリクエストに限定したアクセスに制限することができます。また、VPCのルートテーブルがインターネットゲートウェイ経由でアクセスする方式になっているデフォルトルートが設定されている場合は、そのルートを変更または削除してからプロキシサーバー経由のルートに再設定します。

プロキシサーバーは通常、内部リソース（サーバー、ワークステーションなど）とインターネット間のリレーとして機能し、プライベートネットワークを離れるネットワークアクティビティをフィルタリング、加速、およびログを記録することができます。

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

オプション2は不正解です。プライベートサブネットにあるEC2インスタンスを設置することを前提とした構成となっており、正しくありません。このシナリオではパブリックサブネット内のインスタンスの制御方法が問われています。

オプション3は不正解です。EC2インスタンスがパブリック向けのWebサーバーとして使用されるため、パブリックサブネットに展開する必要があり、間違っています。また、プライベートサブネット上のNATインスタンスに接続されているインスタンスは、WEBアプリケーションへのインバウンド接続を受け入れることができません。

オプション5は不正解です。セキュリティグループはURLに基づいて要求をフィルター処理できないため、正しくありません

5 あなたの会社はニュースメディア配信アプリケーションをAWSにホストしています。このWEBアプリケーションは東京リージョンに展開されており、EC2インスタンスを利用したワイヤレスセンサーの管理サーバーとLinux バックエンドサーバーによって構成されています。ユーザー情報を保存するためのMySQLデータベースが利用されています。最近発生した東京リージョンでのAZ障害によって、バックエンドサーバーが停止するというトラブルを受けて、現在はシステム構成の可用性を高める対応を行っています。バックエンドサーバーは１つのAZで利用されていることや、NATゲートウェイも同じAZのみに展開されていることで、単一のAZ障害に耐えられなかったことが障害の大きな原因となっています。バックエンドサーバーのEC2インスタンスは、インターネットに接続して、定期的にパッチをダウンロードすることが必要であり、セキュリティ上の理由からジャンプホストへのSSHポートのみを開くことが要件となっています。

これらの要件に対応するために、最もコスト効率がよく最適なアーキテクチャを選択してください。

○ 東京リージョンの1つのアベイラビリティゾーンにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネットに設置する。バックエンドサーバーも複数AZに展開して、内部Route53の内部DNSレコードによる分散処理とAutoScalingを設定する。次にBastionホストをパブリックサブネットに配置し、Bastionホストのセキュリティグループからのインバウンドトラフィックの**HTTP**アクセス（ポート80）を許可する。

○ 東京リージョンの2つのアベイラビリティゾーンにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネットに設置する。バックエンドサーバーも複数AZに展開して、内部ELBによる分散処理とAutoScalingを設定する。次にシンガポールリージョンに同じ構成を移設して、Route53を設定して、フェールオーバー構成を実施する。その上で、ネットワークACLによってインバウンドトラフィックの**SSH**アクセス（ポート22）を許可する。

◉ 東京リージョンの2つのアベイラビリティゾーンにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネットに設置する。バックエンドサーバーも複数AZに展開して、内部ELBによる分散処理とAutoScalingを設定する。次にBastionホストをパブリックサブネットに配置し、Bastionホストのセキュリティグループからのインバウンドトラフィックの**SSH**アクセス（ポート22）を許可する。 (正解)

○ 東京リージョンの2つのアベイラビリティゾーンにおいてパブリックサブネットとプライベートサブネットを構成して、NATゲートウェイを各パブリックサブネットに設置する。バックエンドサーバーも複数AZに展開して、内部ELBによる分散処理とAutoScalingを設定する。次にRoute53を利用した内部DNSによるルーティングによって、インバウンドトラフィックの**SSH**アクセス（ポート22）を許可する。

説明

ボトルネックとなっているNATゲートウェイによるアドレス変換構成を高可用なアーキテクチャとするために、２つ以上のアベイラビリティゾーンのパブリックサブネットとプライベートサブネットを両方使用する構成を検討する必要があります。そのため、バックエンドサーバーを複数AZのプライベートサブネットに展開して、内部ELBによる分散処理とAutoScalingを設定することが必要です。

NATゲートウェイが１つのパブリックサブネットに設定されているのも問題となっています。これもマルチAZに対応できるように複数AZの複数パブリックサブネットに設置することが必要となります。これにより、単一のアベイラビリティゾーンが停止した場合でも、他のNATゲートウェイからインターネットトラフィックを処理できるようになります。

EC2インスタンスはジャンプホストへのSSHポートのみを開くという要件から、Bastionホストをパブリックサブネットに配置する必要があります。その際にセキュリティグループは、Bastionホストセキュリティグループからのインバウンドトラフィックに**SSH**アクセス（ポート22）を許可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。これでは東京リージョンの1つのアベイラビリティゾーンのみを利用しており、十分な可用性を提供できていません。また、Route53ではなくELBによるトラフィック分散を実施する構成が必要です。インバウンドトラフィックのHTTPアクセス（ポート80）を許可ではなく、SSHによる通信がセキュリティ上必要となります。

オプション２は不正解です。シンガポールリージョンに同じ構成を移設して、Route53を設定して、フェールオーバー構成を実施することで高可用性は担保されるものの、リージョン障害に対応した事業継続性計画で稼働率を最大化するような構成となっており、コスト効率が良いという要件に合致していません。

オプション４は不正解です。Bastionホストセキュリティグループからのインバウンドトラフィックに**SSH**アクセス（ポート22）を許可する設定がないと、プライベートサブネットのEC2インスタンスへのアクセスが不可能となります。Route53によってそういった設定はできません。

6 大手メディア企業はAWSにおいてユーザー間でニュースコンテンツを共有する新しいWEBサービスをリリースしました。このWebサービスは、2つのパブリックサブネットと2つのプライベートサブネットを持つVPC（10.0.0.0/16）内に設置されています。プライベートサブネットからのインターネットへの返信処理用のNATゲートウェイが各パブリックサブネットに配置されています。データベース用のEC2インスタンスは、NATゲートウェイに関連付けたルートテーブルを持つプライベートサブネットに配置されています。社内で将来的な展開を見据えて、IPv6によるIPアドレス管理が実施されることになりました。したがって、このアプリケーションにおいても、IPv6を利用した構成に変更することが求められています。

IPv6の追加に必要な設定方法を選択してください。（3つ選択してください。）

- [x] パブリックサブネットにおいて、Egress-onlyインターネットゲートウェイを設定して、インターネット経由のIPv6トラフィックをすべてルーティングするルートを作成する。プライベートサブネットのインターネットゲートウェイにIPv6トラフィックをルーティングするルートを作成する。 (不正解)
- [ ] カスタムネットワークACLルールを作成してサブネットに出入りするトラフィックの流れを制御している場合は、IPv6トラフィックのルールを追加する。 (正解)
- [x] IPv6 CIDRブロックをVPCおよびサブネットに関連付ける。 (正解)
- [x] パブリックサブネットに関連付けたインターネットゲートウェイに、IPv6トラフィックをルーティングするルートを作成する。プライベートサブネットにはEgress-onlyインターネットゲートウェイにインターネット経由のIPv6トラフィックをルーティングするルートを作成する。 (正解)
- [ ] VPCおよびサブネットに関連付けているIPv4 CIDRブロックをIPv6 CIDRブロックへと変更する。

説明

現在利用しているVPC構成はIPv4のみに対応しており、サブネット内のリソースがIPv4のみを使用するように設定している場合は、既存のVPCとリソースに対してIPv6の利用を有効化することでデュアルスタックモードで動作させることができます。これにより、VPCはIPv4またはIPv6あるいは両方を経由して通信できるようになります。IPv6の使用を有効にするためのステップは、次の通りです。

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

⇒したがって、オプション3は正解となります。また、VPCおよびサブネットに関連付けているIPv4 CIDRブロックをIPv6 CIDRブロックへと変更するといった、オプション5は間違った手順となります。

2．IPv6トラフィックがルーティングされるようにルートテーブルを更新します。パブリックサブネットの場合、サブネットからインターネットゲートウェイにIPv6トラフィックをすべてルーティングするルートを作成します。プライベートサブネットの場合、サブネットからEgress-onlyインターネットゲートウェイにインターネット経由のIPv6トラフィックをすべてルーティングするルートを作成します。

⇒したがって、オプション4が正解となります。またオプション1は間違った設定手順となります。

3．IPv6アドレスのルールを含めて、セキュリティグループルールを更新します。これにより、IPv6トラフィックはインスタンスに出入りできるようになります。カスタムネットワークACLルールを作成して、サブネットに出入りするトラフィックの流れを制御している場合は、IPv6トラフィックのルールを含める必要があります。

⇒したがって、オプション2が正解となります。

4．インスタンスタイプがIPv6をサポートしていない場合は、インスタンスタイプを変更します。

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

6．IPv6を使用するように設定されていないAMIからインスタンスが起動された場合は、インスタンスに割り当てられているIPv6アドレスが認識されるように手動でインスタンスを設定する必要があります。

したがって、オプション2，3，4が正解となります。

7 大手印刷会社はWEBアプリケーションをオンプレミス環境で利用しています。オンプレミスサーバーの老朽化によるリプレースが必要となっており、経営陣は新サーバーに切り替えるタイミングでAWSに移行することを決定しました。現在、VMware環境内の高度にカスタマイズされたWindows VM仮想環境を利用したアプリケーションが実行されています。これらのシステム環境の移行は週末の土日2日間で実施しなければならないという制約があり、効率的で迅速な対応が不可欠となっています。

この要件を踏まえて、最もコスト効率がよく最適な移行方法を選択してください。（2つ選択してください。）

- [ ] AWS Import / Exportを使用してVMware vSphereインフラストラクチャからAmazon EC2に仮想マシンをインポートする。
- [ ] VMのバックアップをS3に保存して、S3からAmazon EC2に仮想マシン設定を復元する。
- [x] 移行対象となるオンプレミス環境のVMwareサーバーに対して、AWS Application Migration Service用のAWS Replication Agentをインストールする。その上で、AWS Application Migration Serviceを利用して、このエージェントを利用してAmazon EC2に仮想マシンをインポートする。 (正解)
- [x] VM Import/Exportを利用して、オンプレミス環境のイメージを取得して、新規にEC2インスタンスを起動する。それによって、EC2インスタンスに対してオンプレミス環境と同じサーバー構成をセッティングすることで、AWS側でサーバー構成を復元する。 (正解)

説明

オプション３が正解となります。AWS Application Migration Serviceを利用して、VMware vSphereインフラストラクチャを利用したアプリケーション構成をAmazon EC2のインスタンスにインポートすることができます。

AWS Application Migration Serviceを利用した移行には、移行対象となるソースサーバーに AWS Replication Agent をインストールすることが必要です。これによって、AWS Replication Agent はレプリケーション設定を表示および定義できます。AWS Application Migration Service (AWS MGN) はこれらの設定を使用して、Replication Server および低コストのステージング Amazon EBS ボリュームとして機能する軽量の Amazon EC2 インスタンスを備えた Staging Area Subnet を作成および管理します。

オプション４も正解となります。VM Import/Export を使用すると、仮想マシン (VM) イメージを既存の仮想環境から Amazon EC2 にインポートして復元することができます。この方法を使うと、アプリケーションおよびワークロードを Amazon EC2 へ移行したり、VM イメージカタログを Amazon EC2 にコピーしたり、バックアップと災害対策のために VM イメージのリポジトリを作成することができます。

オプション１は不正解です。AWS Import/Exportは、大量データを物理ストレージデバイスから AWS 環境に移行するのに使用する古いAWSサービスです。ポータブルストレージドライブを AWS に移行することでAmazon の高速内部ネットワークを使用してストレージデバイスからデータを直接転送します。この機能ではオンプレミスのVMをインポートできないため、正しくありません

オプション２は不正解です。S3にオンプレミス環境のバックアップを保存することは可能ですが、S3からEC2に仮想マシン設定を復元するといった、作業はできないため不正解となります。

8 あなたの会社はAWSでニュースメディア配信アプリケーションをホストしています。このWEBアプリケーションはアプリケーションサーバーとしてec2インスタンスを利用し、ELBとAuto-Scalingグループを設定しています。さらにユーザー情報を保存するためのMySQLデータベースが利用されています。会社は現在のMySQLからPosgreSQLへとデータベースを移行することを決定し、あなたはソリューションアーキテクトとして、データベースの移行方法を検討しています。

上記の移行要件に対して最適な移行方法を選択してください。（3つ選択してください。）

- [x] RDSの移行機能によりMySQLからPostgreSQLへの移行タスクを設定して実行する。その際は、JSONファイルを利用して移行対象テーブルや移行方式を詳細にタスクとして設定する。 (不正解)
- [x] Amazon Database Migration ServiceによりMySQLからPostgreSQLへの移行タスクを設定して実行する。その際は、テーブルマッピングを利用して移行対象テーブルや移行方式を詳細にタスクとして設定する。 (正解)
- [x] RDSの移行機能によりMySQLからPostgreSQLへの移行タスクを設定して実行する。その際は、RDSコンソールを利用して移行対象テーブルや移行方式を詳細にタスクとして設定する。 (不正解)
- [ ] Amazon Database Migration ServiceによりMySQLからPostgreSQLへの移行タスクを設定して実行する。その際は、DMSコンソールを利用して移行対象テーブルや移行方式を詳細にタスクとして設定する。 (正解)
- [ ] Amazon Database Migration ServiceによりMySQLからPostgreSQLへの移行タスクを設定して実行する。その際は、JSONファイルを利用して移行対象テーブルや移行方式を詳細にタスクとして設定する。 (正解)

説明

オプション2は正しいです。 AWS Database Migration Serviceのテーブルマッピング機能を利用して、データソース、ソーススキーマ、データ、そしてタスク実行中に必要なすべての変換を指定する複数のルールタイプを設定することができます。テーブルマッピングを使用して、データベース移行対象となる個々のテーブルやスキーマを指定できます。また、フィルタを使用して、レプリケートする特定テーブルの列からデータを指定することができ、変換機能によりターゲットデータベースに書き込むデータを変更できます。

オプション4は正しいです。AWS Database Migration Serviceコンソールから、移行タスクを定義して、実行する詳細設定が可能となっています。詳細は以下のページをご覧ください。

https://docs.aws.amazon.com/ja_jp/dms/latest/userguide/CHAP_SettingUp.html

オプション5は正しいです。テーブルマッピングはJSON 形式で作成されます。AWS DMS マネジメントコンソールを使用して移行タスクを作成する場合、JSON を直接テーブルマッピングボックスに入力できます。CLI または API を使用して移行を実行する場合、JSON ファイルを作成して移行中に適用するテーブルマッピングを指定できます。

詳細は以下のページをご覧ください。

https://docs.aws.amazon.com/ja_jp/dms/latest/userguide/CHAP_Tasks.CustomizingTasks.TableMapping.html

その他の選択肢は、間違った設定方法の説明となっており、不正解です。

https://docs.aws.amazon.com/ja_jp/dms/latest/userguide/CHAP_SettingUp.html

https://docs.aws.amazon.com/ja_jp/dms/latest/userguide/CHAP_Tasks.CustomizingTasks.TableMapping.html

9 新規事業用アプリケーションを構築しているベンチャー企業では、RDS MySQLを利用した顧客管理データベースを構築しています。そこでは、多数の顧客の基本情報や、ユーザーによる売買記録などが保存されており、今後の分析などに利用される予定です。あなたはソリューションアーキテクトとしてRDS上に保存されたデータにアクセスしてデータ処理を実行するLambdaベースのサーバレスアプリケーションを開発しています。その際にはRDSへのコネクション接続を最適にする必要があります。

この要件を満たす最適なソリューションを選択してください。

- ◉ **Lambda関数をSQSによるポーリング処理と連携して、RDSのデータ処理を分散化する。** (不正解)
- ○ **Lambda関数からRDSエンドポイントに接続してデータ処理を実施することで、効率的な非同期並列実行を可能にするデータ処理アプリケーションを構築する。**
- ○ **RDSのスティッキーセッションを有効化する。これによって、Lambda関数による効率的な非同期並列実行を可能にするデータ処理アプリケーションを構築する。**
- ○ **Lambda関数からRDS Proxyに接続してデータ処理を実施することで、Lambda関数による効率的な非同期並列実行を可能にするデータ処理アプリケーションを構築する。** (正解)

説明

オプション4が正解となります。RDS Proxyは、アプリケーションとRDSデータベース間の仲介役として機能するプロキシ機能です。Lambda関数からRDS DBインスタンスへのコネクションプールを確立および管理して、アプリケーションからのデータベース接続を少なく抑えることができます。

Lambda関数とRDS Proxyを連携させることで、LambdaはDBインスタンスに直接対話するのではなく、RDS Proxyと対話します。そして、RDS ProxyはLambda関数の同時実行によって作成された大量の同時接続をスケーリングするために必要なコネクションをプーリングします。これにより、Lambdaアプリケーションは、Lambda関数コールごとに新しいコネクションを作成するのではなく、既存のコネクションを再利用することができます。

オプション1は不正解です。Lambda関数をSQSによるポーリング処理と連携してRDSへのデータ処理を分散化するといった構成は非効率であり、ポーリング処理が要件として必要でない限りはLambda関数単体で処理を分散化させることが可能です。また、Lambda関数はRDS Proxyを利用しない場合はRDSとコネクション接続が多数発生してしまいます。

オプション2は不正解です。Lambda関数とRDSエンドポイントを接続する構成は可能ですが、非推奨アーキテクチャ構成となっています。Lambda関数とRDSエンドポイントを接続すると、Lambdaが複数同時実行されることによってコネクションが多数確立されてしまい、RDSの処理能力を悪化させます。

オプション3は不正解です。RDSのスティッキーセッションという機能はありません。

10 グローバルな国際決済サービスを提供するスタートアップ企業は、iOSおよびAndroidモバイルで利用できる飲食店クーポンモバイルアプリを展開しています。現在、このアプリに費用対効果の高いロケーションベースのアラート機能を追加開発しています。この追加機能では、GPSを利用して、ユーザーが近隣店舗に近づいた際にその店舗を紹介するチャットボットによって、レコメンデーションやクーポン提示が行われるサービスを提供します。

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

◉ ユーザーのGPSから取得したロケーション情報をDynamoDBの位置情報テーブルに定期的に格納する。その上で、EC2インスタンスが近接地域の店舗情報をDynamoDBの店舗テーブルから取得して、配信処理を実行する。データ処理結果は、AWS MQを利用したモバイルプッシュ機能を利用して、モバイルアプリにプッシュ通知が配信される。その通知内容に基づいてAmazon Lexが会話を実施する。 (不正解)

○ ユーザーのGPSから取得したロケーション情報をDynamoDBの位置情報テーブルに定期的に格納する。その上で、オンデマンドEC2インスタンスがロケーション情報と店舗情報をマッチングさせて、レコメンデーションのアルゴリズムを起動し、最適なクーポン情報を別のDynamoDBの店舗テーブルから取得する。このEC2インスタンス処理はSQSによるキューイング処理によって並列で実行し、かつSQSキューの深さをトリガーとしたAutoScalingによって負荷を軽減する。店舗情報はLambda関数によって、Amazon Lexに通知される。 (正解)

○ API gatewayを利用したRestベースでユーザーのロケーション情報をオンデマンドインスタンスに通知して、EC2インスタンスが近接地域の店舗情報をDynamoDBから引き出して配信処理を実行する。データ処理結果は、AWS AppSyncを利用したモバイルプッシュ機能を利用して、モバイルアプリにプッシュ通知が配信される。その通知内容に基づいてAmazon Lexが会話を実施する。

○ Route53の位置情報ルーティング機能を利用してユーザーのロケーション情報を通知して、その上で、オンデマンドEC2インスタンスがロケーション情報と店舗情報をマッチングさせて、レコメンデーションのアルゴリズムを起動し、最適なクーポン情報を別のDynamoDBの店舗テーブルから取得する。このEC2インスタンス処理はSQSによるキューイング処理によって並列で実行され、かつSQSキューの深さをトリガーとしたAutoScalingによって負荷を軽減する。データ処理結果は、SNSを利用したモバイルプッシュ機能を利用して、Amazon Lexに通知される。

説明

このシナリオでは、ロケーションベースのリアルタイム処理を実施する通知アプリケーションを構築することが求められています。ユーザーのロケーション情報の取得には、スマートフォンなどに搭載されたGPSを利用してユーザーロケーション情報をDynamoDBに定期的に格納することが最適な構成となります。DynamoDBは車両追跡データなどのGPS座標データを大量に保持するのに適したデータベースです。その上で、オンデマンドEC2インスタンスがロケーション情報のマッチングとレコメンデーションのアルゴリズムを起動して、最適なクーポン情報を別のDynamoDBの店舗テーブルから取得します。このアプリケーションはユーザーの位置情報テーブルと店舗情報テーブルの2つのDynamoDBテーブルを利用しています。その上で、それらのデータをマッチングさせて、レコメンデーションを実施するアルゴリズムをEC2インスタンスが実行します。

次に、こうした処理が高負荷となった場合に耐えられるアーキテクチャとすることが必要となります。そこで、EC2インスタンス処理をSQSキューによって並列で実行することが求められます。また、SQSキューの深さに応じたAutoScalingを設定することでキューにメッセージが増加した場合の負荷を軽減することができる構成とします。

データ処理結果は、SNSを利用したモバイルプッシュ機能を利用して、モバイルアプリにプッシュ通知が配信されます。最終的なインターフェースはチャットボットでの会話となるため、Lambda関数によってAmazon Lexに通知されるように実装します。

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。このアーキテクチャではAutoScalingが設定されておらず、高負荷に耐えられる対応が不足しています。また、データ処理結果は、AWS MQを利用したモバイルプッシュ機能を利用して、モバイルアプリにプッシュ通知が配信されるのではなく、Lambda関数によってAmazon Lexに会話を実行することが必要です。

オプション3は不正解です。オンデマンドEC2インスタンスとAPI Gatewayの組み合わせでスケーラブルなコンピューティングシステムを提供できますが、API gatewayを利用したRestベースでユーザーのロケーション情報をオンデマンドインスタンスに通知するにはロケーション情報自体を取得処理する仕組みが必要です。また、モバイルデバイスへのプッシュ通知にAWS AppSyncを使用するのは間違っていることも不正解の理由です。代わりにSNSを使用する必要があります。

オプション4は不正解です。Route53の位置情報ルーティング機能には、ユーザーにロケーション情報を通知するといった機能はありません。

B銀行はAWSとオンプレミスサイトを併用したハイブリッドアーキテクチャを採用しています。データ保存向けにはAWS Storage Gatewayのボリュームゲートウェイを使用して、iSCSIを介したハイブリッド構成のデータ共有システムを利用しています。最近になって、セキュリティチームがデータ共有システムのネットワークに対するDDoS攻撃や不正アクセスなどの攻撃や不正傍受が多発していることを発見しました。

あなたは銀行のソリューションアーキテクトとして、iSCSIを介したハイブリッド構成に対して、どのような対策を実施するべきでしょうか。

- ○ **iSCSI接続向けにCHAP（Challenge Handshake Authentication Protocol）を構成し、プレイバック攻撃に対してネットワークを保護する。**
- ◉ **iSCSIブロックインターフェースをiSCSI仮想テープライブラリーインターフェースに変更して、ネットワーク攻撃から接続先を保護する。** (不正解)
- ○ **iSCSIブロックインターフェースをより安全性の高いプロトコルであるCIFSに変更する。**
- ○ **iSCSI接続向けにCHAP（Challenge Handshake Authentication Protocol）を構成し、iSCSIとイニシエーター接続を認証する。** (正解)

説明

オプション４が正解となります。iSCSI接続を実施するためにCHAP（Challenge Handshake Authentication Protocol）を構成して、iSCSIとイニシエーター接続を認証することで、ボリュームとVTLデバイスターゲットへのアクセスの認証時に、iSCSIイニシエータのアイデンティティを定期的に確認してプレイバック攻撃から保護することができます。

AWS Storage Gateway はCHAPを使用して、ゲートウェイと iSCSI イニシエータ間の認証を行うことができます。 CHAP はボリュームと VTL デバイスターゲットへのアクセスの認証時に、iSCSI イニシエータのアイデンティティを定期的に確認することにより、プレイバック攻撃から保護します。

CHAP を設定するには、AWS Storage Gateway コンソールと、ターゲットへの接続に使用される iSCSI イニシエータソフトウェアの両方で、設定を行う必要があります。Storage Gateway では相互 CHAP が使用され、イニシエータがターゲットを認証するときに、ターゲットもイニシエータを認証します。

オプション１は不正解です。iSCSI接続を実施するためにCHAP（Challenge Handshake Authentication Protocol）を構成するだけでは設定は不十分です。その上で、iSCSIとイニシエーター接続を認証する必要があります。

オプション２は不正解です。iSCSI仮想テープライブラリーインターフェースはAWS Storage Gateway によるテープや仮想テープライブラリシステムからクラウドにバックアップジョブを移行するシームレスな方法であり、今回の要件には無関係な機能です。

オプション３は不正解です。CIFSとはCommon Internet File Systemの略で、Windowsのファイル共有の仕組みであるSMB（the Server Message Block）をWindows以外でも利用できるようにしたものです。プレイバック攻撃からの保護には利用されません。

02

画像識別を利用したアプリケーション開発を得意とするベンチャー企業は動物画像検索アプリを開発しています。このアプリケーションでは、ユーザーが動物写真をアップロードすることで、類似した動物を画像検索できます。または、一連の写真をアップロードして、特定の画像が利用された時間を検索することもできます。開発チームはアプリケーションの開発と運用を低コストに実施するために、マネージド型のAWSサービスを利用して、このアプリケーションを構築したいと考えています。

この要件を実装するのに最も低コストで容易なソリューションを選択してください。

- ◉ EC2インスタンスを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得する。EC2インスタンスが取得した画像をS3バケットに保存して、エンドユーザー側の端末に表示させるプロセスを実装する。 (不正解)
- ○ Lambdaファンクションを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得する。Lambdaファンクションが取得した画像をS3バケットに保存して、エンドユーザー側の端末に表示させるプロセスを実装する。 (正解)
- ○ Lambdaファンクションを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得する。Lambdaファンクションが取得した画像をDynamoDBに保存して、エンドユーザー側の端末に表示させるプロセスを実装する。
- ○ EC2インスタンスを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得する。EC2インスタンスが取得した画像をDynamoDBに保存して、エンドユーザー側の端末に表示させるプロセスを実装する。

説明

オプション2が正解となります。Lambdaファンクションを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得します。Lambdaファンクションが取得した画像をS3バケットに保存して、エンドユーザー側の端末に表示させるプロセスを実装することで、低コストなサーバレスアプリケーションを構築することができます。

~~AWSでの画像認識の利用にはAmazon Rekognitionの利用を第一に検討します。~~ Amazon Rekognitionでは、画像分析と動画分析をアプリケーションに簡単に追加できます。LambdaとRekognitionを組み合わせることにより、低コストで可用性の高い画像識別アプリケーションを容易に構築することができます。

Lambdaファンクションを利用してRekognition APIを呼び出して、JSONフォーマットで情報を取得します。可用性と安定性を確保しながらコスト最適に利用できるためには、画像の保存場所はS3バケットが最適となります。DynamoDBは画像を保存する場所としては不適切です。

オプション1，4は不正解です。最も低コストで容易なソリューションという要件からEC2インスタンスではなく、Lambdaによるサーバレスアプリケーションを優先します。

オプション3は不正解です。DynamoDBは画像を保存するのに適していません。

13

C社は現在オンプレミスネットワーク上にホストされているインフラとアプリケーション全般をAWSクラウドに移行することを決定しました。このオンプレミス環境には、タイムリーかつ費用対効果の高い方法でS3バケットに移動する必要がある合計150TBのデータがあります。 既存のインターネット回線の空き容量を使用してデータをAWSにアップロードするのためには1週間以上かかり、かつ途中で回線異常などで断線する可能性があるため、移行方法としては不適切と判断しました。

この要件に合致する最適なデータ移行方法を選択してください。

- (●) Snowballストレージを2つ利用してデータ移行を実施する。 (不正解)
- ( ) Snowball Edge Storage Optimizedを1つ利用してデータ移行を実施する。
- ( ) AWS Storage Gatewayサービスを使用してFile Gatewayを起動し、ファイルゲートウェイマウントポイントを使用してデータ移行を実施する。
- ( ) Direct Connectを一から接続して、データ移行を実施する。
- ( ) Snowball Edge Storage Optimized を２つ利用してデータ移行を実施する。 (正解)

説明

オプション５は正解です。Snowball Edge Storage Optimizedは80TB、Snowball Edge Compute Optimizedは42TBのストレージ容量があります。したがって、150TBのデータ転送にはSnowball Edge Storage Optimizedを2台利用することが正解となります。

オプション１は不正解です。Snowball はペタバイト規模のデータ転送ソリューションで、AWSクラウド内外に大容量データを転送できます。Snowball を使用すると、高いネットワークコストに長時間かかる転送、セキュリティ面の懸念といった、大規模なデータ転送に関する一般的な課題を解決できます。しかしながら、現在はSnowball Edgeのみが利用可能であり、Snowballは利用できなくなっています。

オプション２は不正解です。Snowball Edge Storage Optimizedは80TB、Snowball Edge Compute Optimizedは42TBのストレージ容量があります。150TBのデータ転送にはSnowball Edgeが2台必要となるため、正しくありません。

オプション３は不正解です。AWS Storage Gatewayサービスの File Gatewayはデータ転送ではなく、主にオンプレミスストレージのバックアップ取得に利用されます。

オプション４は不正解です。Direct Connectはオンプレミス環境とAWS間との専用線接続に利用されます。これを利用して回線経由でデータ転送も可能ですが、今回は接続形式を増やすのではなくデータ移行のみが目的となっているため、Snowball Edge Storage Optimizedを利用する方が最適なオプションとなります。

A社は3層で構成されたニュースサイトアプリケーションを運用しています。このアプリケーションはオンプレミス環境にデプロイされていますが、スケーラビリティと弾力性を高めるためにAWSに移行することを決定しました。このアプリケーションは、Web層とアプリケーション層を組み合わせた読み取り専用のニュースレポートサイトと、予測不可能な大規模なトラフィック要求を受け取ることができるデータベース層があり、トラフィック変動に自動的に対応する必要があります。この構成にはできるだけシンプルなモデルが必要です。

次の中から、これらの要件を満たす最適なAWSサービスの構成方法を選択してください。

- ◉ **ステートレスインスタンスを使用してELBとAutoScalingグループを設定する。WEBサーバーからのDB読み取り処理向けにElastiCache Redisを使用する。最後にRDSのリードレプリカを増やして読み取り処理を分散化する。** (不正解)
- ○ **ステートレスインスタンスを使用してELBとAutoScalingグループを設定する。WEBサーバーからのDB読み取り処理向けにElastiCache Memcachedを使用する。最後にRDSのリードレプリカを増やして読み取り処理を分散化する。** (正解)
- ○ **ステートレスインスタンスを使用してELBとAutoScalingグループを設定する。Webサーバーの読み取り操作にElastiCache Redisを使用する。最後にRDSのマルチマスター構成を利用する。**
- ○ **ステートフルインスタンスを使用してELBとAutoScalingグループを設定する。WEBサーバーからのDB読み取り処理向けにElastiCache Memcachedを使用する。最後にRDSのマルチAZ構成を使用する。**
- ○ **ステートフルインスタンスを使用してELBとAutoScalingグループを設定する。WEBサーバーからのDB読み取り処理向けにElastiCache Redisを使用する。最後にRDSのマルチAZ構成を使用する。**

オプション２が正解となります。ステートレスインスタンスを使用してELBとAutoScalingグループを設定します。Webサーバーの読み取り操作にElastiCache Memcachedを使用して、最後にRDSのリードレプリカを使用することで、予測不可能な大規模なトラフィック要求を処理できる可用性の高い柔軟な構成を達成することができます。

このシナリオでは読み取りの多いWeb層とデータベース層のパフォーマンス向上ソリューションが求められており、~~ElastiCache、CloudFrontを利用したキャッシュソリューション~~が選択肢としてそろえられます。今回のケースではWEBサーバーからのデータベースの読み取り処理を高速化するために~~ElastiCacheを選択し~~でRDSへの~~キャッシュ~~処理を可能にします。その際は、読み取り処理を支援するために利用するというシンプルなデータ処理になるため、Redisではなく~~ElastiCache Memcached~~の利用が最適です。さらにRDBの読み取り処理負荷を軽減するためには~~リードレプリカを増やします~~。

次にステートレスまたはステートフルなインスタンスのどちらを利用するかも重要となります。ステートフルなインスタンスは、クライアントとWebサーバー間の状態または接続であるため、セッションがアクティブである限りデータベースが使用されたままになるため、分散システムには適していません。したがって、サーバーだけでなくデータベースの負荷も増加します。一方でステートレスインスタンスは分散されており、スケールイン/スケールアウトが容易です。したがって、ステートレスアプリケーションは、分散アプリケーションのパフォーマンスを向上させる傾向があります。

上記の理由からステートフルインスタンスを利用しているオプション４と５は不正解です。

オプション１と３は不正解です。オプション１と３はWebサーバーのDB読み取り操作にElastiCache Redisを使用しており、最適な構成になっていません。Redisでも同様の構成は可能ですが、できるだけシンプルな構成にはElastiCache Memcachedの利用が最適です。

また、オプション３と４は最後にRDSのマルチAZ構成を使用しており、高可用性を達成できますが、これは処理性能を向上させる効果はありません。

あなたはソリューションアーキテクトとして、S3バケットにデータを保存するモバイルアプリケーションを構築しています。このアプリケーションでは、ユーザーがS3バケット内のデータを利用する際に一時認証を利用しています。具体的にはSTSを利用して一時認証情報を取得して、ユーザーにアクセスを許可する構成としてます。認証テストを実施したところ、一部の一時認証情報のアクセス権限が間違っており、必要なリソースへのアクセスが提供されていないことが判明しました。

一時認証情報によって付与されたアクセス権を取り消すにはどうすればよいですか？

- (●) IAMダッシュボードにおいて、ユーザーに提供した特定のSTSを選択して、STS情報を削除する。 (不正解)
- ( ) IAMダッシュボードにおいて、ユーザーに提供した特定のロールを選択し、ロールの有効期限を0に変更する。
- ( ) IAMダッシュボードにおいて、ユーザーに提供した特定のSTSを選択して、STSの有効期限を0に変更する。
- ( ) IAMダッシュボードにおいて、ユーザーに提供した特定のロールを選択して、取り消し処理を実行する。 (正解)

説明

オプション4が正解となります。STSによって間違った権限を付与してしまった場合。IAMダッシュボードにおいて、ユーザーに提供した特定のロールを選択して、手動でSTSの許可ロールを取り消すことができます。一時認証情報はIAMロールを利用して設定されるため、IAMロールを選択することが正解となります。

STSなどの一時認証情報をユーザーに付与すると、セッションの有効期間 (12 時間など) を使用した場合は、時間内であれば一時認証情報がすぐに期限切れになることはありません。

ユーザーが意図せずに間違ったアクセス権限を付与した認証情報を第三者に設定してしまった場合は、第三者は期間中は付与されたリソース権限に対してアクセスできるようになってしまいます。ただし、必要がある場合は、こうしたアクセス許可をすぐに取り消すことができます。取り消すためには、IAMダッシュボードにおいて、ユーザーに提供した特定のロールを選択し、取り消し設定を利用して許可ロールを取り消します。

16

A社では社内アプリケーションに対するDDoS攻撃によって大規模なシステム障害が発生しました。そこで、あなたはソリューションアーキテクトとして、AWS上にホストしている自社アプリケーションを保護するためにDDoS攻撃などの外部攻撃を軽減するアーキテクチャを設定するように依頼されました。具体的に防止するべき攻撃リストは以下の通りです。

- DDoS攻撃
- SYNフラッド
- UDPリフレクション攻撃
- SQLインジェクション
- クロスサイトスクリプティング
- 不正IP取得によるアカウントアクセス
- ネットワーク情報の取得

これらの要件を満たす、AWSアーキテクチャ設計パターンを選択してください。（3つ選択してください。）

- [x] AWS Shield Standardを利用して高度なDDoS攻撃及びSYNフラッドやUDPリフレクション攻撃を検出を実施して、アプリケーションレイヤー上のリアルタイム通知を実施する。 (不正解)
- [ ] Amazon Route 53 のシャッフルシャーディングと anycast ルーティング機能により、DDoS 攻撃を回避して、エンドユーザーがアプリケーションにアクセスできるようにする。 (正解)
- [x] AWS Shield Standardを利用して、SQLインジェクション、クロスサイトスクリプティング攻撃などを検出して、アプリケーションレイヤー上のリアルタイム通知を実施する。 (不正解)
- [x] AWS Shield Advancedを利用して高度なDDoS攻撃検出を実施して、アプリケーションレイヤー上のモニタリングを実施する。 (正解)
- [ ] AWS WAFを利用してセキュリティルールをカスタマイズして、アプリケーションに対するトラフィックを制御する。 (正解)

説明

オプション2が正解となります。Amazon Route 53にはシャッフルシャーディングとanycastルーティングとにより、DDoS攻撃中にエンドユーザーがアプリケーションにアクセスできるようにする2つの機能があります。これによって、AWS上でDDoS 攻撃を受けていても、エンドユーザーがアプリケーションにアクセスできるように対応することができます。

AWS Shield AdvancedとAWS WAFは、クラウドインフラストラクチャに最適なDDoS攻撃の緩和とレイヤー7セキュリティリスクから保護する2つのサービスです。したがって、オプション4と5は正しい内容です。

AWS WAF は、アプリケーションの可用性に対する影響、セキュリティの侵害、過剰なリソース消費を生じる可能性がある一般的なウェブエクスプロイトからウェブアプリケーションを保護するために役立つウェブアプリケーションファイアウォールです。AWS WAF では、**カスタマイズ可能なウェブセキュリティルールを定義することによって**、ウェブアプリケーションに対するどのトラフィックを許可またはブロックするかを制御できます。AWS WAF は、SQL インジェクションまたはクロスサイトスクリプティングなどの一般的な攻撃パターンをブロックするカスタムルール、および特定のアプリケーションのために設計されたルールを作成して制御できます。

AWS Shield Advanced は、Amazon CloudWatchによるリアルタイム通知と、AWS WAFとAWS Shieldマネジメントコンソールあるいは API における診断によって、DDoS 攻撃に対する完全な可視性を与えてくれます。また、マネジメントコンソールから以前の攻撃の要約を表示することもできます。

オプション1，3は正しくありません。 AWS Shield Standardはレイヤー3またはレイヤー4攻撃を軽減できますが、詳細なリアルタイム通知や可視化機能が提供されていないため、今回の要件にはAdvanced版を利用することが必要です。

あなたはソリューションアーキテクトとして、S3とRDSを利用したデータ共有アプリケーションを運用しています。画像をS3バケットに保存し、RDSに顧客データを記録します。アプリケーション向けのインフラ構成を展開するためにCloudFormationテンプレートを利用して、インフラ構成をテンプレートから整備しているため、インフラ構成の複製が容易に可能になっています。基本運用期間が終了したため、このアプリケーションはサービスを停止することになりましたが、いつでも再開できるようにする準備が必要です。したがって、インフラを終了するのと同時にデータを保持する設定を行います。

このシナリオにおいて、要件を満たすCloudFromationテンプレート設定を選択してください。

- ◉ **CloudFormationのDeletionPolicy属性により、S3リソース宣言文に対してSnapshotを設定する。RDSリソースに対しては、Snapshotを設定する。** (不正解)
- ○ **CloudFormationのDeletionPolicy属性により、S3リソース宣言文に対してRetainを設定する。RDSリソースに対しては、Snapshotを設定する。** (正解)
- ○ **CloudFormationのDeletionPolicy属性により、S3リソース宣言文に対してSnapshotを設定する。RDSリソースに対しては、Retainを設定する。**
- ○ **CloudFormationのDeletionPolicy属性により、S3リソース宣言文に対してRetainを設定する。RDSリソースに対しては、Retainを設定する。**

説明

オプション2が正解となります。このシナリオでは、CloudFormationテンプレートの設定によってデータ保存方式を設定することが求められています。その際に、S3のDeletionPolicyをRetainに設定して、RDSのスナップショットを使用するように設定することで、S3バケットとRDSにデータを保持することができます。S3はスナップショットを取得できないためRetainがデータ保持の選択となります。RDSは一時停止してコストを削減したいため、スナップショットを取得しておくことで復元可能とします。

このシナリオではアプリケーション停止後にデータを保持することが求められています。そのため、制御する各リソースに対して DeletionPolicy 属性を指定することが必要となります。CloudFormationのDeletionPolicy 属性を使用すると、スタックが削除された際にリソースを保持またはバックアップできます。DeletionPolicy 属性が設定されていない場合、AWS CloudFormation ではデフォルトでリソースが削除されます。

AWS CloudFormation のDeletionPolicyには以下のようなポリシーがあります。

・Snapshot：スナップショットをサポートするリソース (AWS::EC2::Volume など) の場合は、Snapshot を指定できます。これにより AWS CloudFormation は、スナップショットを作成したうえで、リソースを削除するようになります。 このポリシーはスナップショットが作成できるリソースにのみ追加することができます。

・Retain：AWS CloudFormation はスタックを削除する際、リソースやコンテンツを削除せず保持します。この削除ポリシーは、あらゆるリソースタイプに追加することができます。

・Delete：AWS CloudFormation はスタックの削除時にリソースと (該当する場合) そのすべてのコンテンツを削除します。この削除ポリシーは、あらゆるリソースタイプに追加することができます。

18

製造業のA社はAWS上にエンタープライズシステムをホストしています。最近になって、そのシステムが突如停止するという障害が発生しました。あなたが運用責任者として調査したところ、一人のエンジニアが本番環境のEC2インスタンスを誤って終了してしまい、サービス中断を引き起こしたことが判明しました。また、実稼働するアプリケーション向けのインフラ構成を操作できる開発者が多数存在するという事実も同時に判明しました。

この種の障害が再び発生するのを防ぐための、適切な対応はどれでしょうか？（2つ選択してください。）

- [x] すべてのEC2インスタンスに適切なタグ設定を行い、タグ情報に基づいて本番環境向けインスタンスの削除を拒否する権限を設定する。それによって、開発者の権限を所属するグループタグ内でのリソース操作に限定する。 (正解)
- [x] 開発者向けのIAMポリシーを修正して、EC2インスタンスの停止権限の許可ポリシーを削除する。 (不正解)
- [ ] 開発者グループのIAMグループのIAMポリシーを修正して、EC2インスタンスへの操作権限を削除する。
- [ ] AWS Organizationsを利用して開発者グループとそれ以外とを分割管理する組織ルールを適用して、開発者がアクセスできるインスタンスを制限する。
- [ ] 開発環境向けのVPCを新たに設置して、開発者のアクセス権限を開発者向けVPC内に制限する。その上で、IAMポリシーによってVPCごとに権限設定を割り振ることで、開発者グループが利用できるVPC内リソースを制限する。 (正解)

説明

オプション1は正解となります。タグを利用することで、インスタンス、イメージ、およびその他のAmazon EC2リソースを管理しやすくするメタデータを各リソースに割り当てることができます。タグは目的、所有者、環境など、さまざまな方法でAWSリソースを分類できます。これによって、開発グループなどのグループごとに割り当てられたタグに基づいて特定のリソースへの権限を付与することが可能となります。

オプション5は正解となります。VPCによってシステム環境を開発環境、本番環境、テスト環境などに分割して、それぞれ利用者を限定することで、開発者が本番環境に影響を及ぼさないように権限を設定することができます。

オプション2は不正解です。一番単純な方式は開発者向けのIAMポリシーを修正して、EC2インスタンスの停止権限の許可ポリシーを削除することです。これにより開発者はEC2インスタンスを起動・操作できますが、削除ができなくなります。しかしながら、開発者はすべてのEC2インスタンス削除ができなくなるため、こうした権限設定は今後の開発作業に支障をきたす恐れがあり、開発グループに付与するべきではありません。

オプション3は不正解です。開発者グループのIAMポリシーにおいてEC2インスタンスへの操作権限を削除してしまうと、開発者がEC2インスタンスを利用できなくなってしまうため、今後の開発に支障をきたします。

オプション4は不正解です。AWS OrganizationsではSCPを利用してAWSリソースへのアカウント毎のアクセス許可・拒否を設定することができますが、IAMポリシーと比較して開発向けインスタンス以外へのアクセスを管理するといった細かい設定はできません。一方で、SCPではなくタグポリシーを利用することで、タグ付けを有効化することはできるため、それによって開発者グループ用のタグ管理を義務化することは有効な手段となります。

19 あなたは美術鑑賞向けSNSサービスを運用するPINTORで働くAWSエンジニアです。PINTORアプリケーションでは、ドメイン名pintor.comを利用してCloudFrontディストリビューションを設定し、コンテンツ配信を高速化することになりました。その際は、HTTPS通信を実施することが要件となっています。また、CloudFrontのビューアリクエストの割合を増やすことにより、パフォーマンスを改善しつつ、コストを抑える対応も依頼されています。

このシナリオにおいて、上記の要件を満たす設定方法を選択してください。（2つの選択してください。）

- [x] **AWS Certificate ManagerによりSSL/TLS認証を生成して、これをCloudFrontに設定することでセキュアHTTPS通信を可能にする。** (正解)
- [ ] **CloudFrontのオリジンサーバー設定において、Cache-control max-age directiveに対してオブジェクトと最適なキャッシュ保持期間を設定する。オリジンでのZIP圧縮によって配信ボリュームを低下させることで、コストを最適化する。**
- [x] **CloudFrontのオリジンサーバー設定において、Cache-control max-age directiveに対してオブジェクトと最適なキャッシュ保持期間を設定する。エッジロケーションでのZIP圧縮によって配信ボリュームを低下させることで、コストを最適化する。** (正解)
- [ ] **AWS Certificate ManagerによりSSL/TLS認証を生成して、これを対象となるEC2インスタンスに設定することでセキュアHTTPS通信を可能にする。**
- [ ] **CloudFrontのエッジ設定において、エッジロケーションのロケーション数のmax値を増加させることで配信処理を向上させる。エッジロケーションでのZIP圧縮によって配信ボリュームを低下させることで、コストを最適化する。**

説明

オプション1は正解となります。AWS Certificate Managerを利用して、証明書をすばやくリクエストして、ELB、CloudFrontなどに証明書をデプロイできます。AWS Certificate Managerは、AWSのサービスとユーザーの内部接続リソースで使用するパブリックとプライベートのSSL/TLS証明書のプロビジョニング、管理、デプロイを簡単にします。SSL/TLS証明書は、ネットワーク通信を保護し、プライベートネットワークのリソースと同様にインターネットでウェブサイトのアイデンティティを確立して、HTTPS通信を可能にします。

オプション3は正解となります。コンテンツ配信の際に、CloudFrontエッジキャッシュから提供されるビューアリクエストの割合を増やすことにより、配信時のパフォーマンスを改善できます。これによって、CloudFrontディストリビューションのキャッシュヒット率を改善することができます。キャッシュヒット率を上げるには、オブジェクトにCache-Control max-ageディレクティブを追加するようにオリジンを設定し、max-ageに対して最長値を指定します。キャッシュ期間が短いと、CloudFrontはリクエストをオリジンに転送して、オブジェクトが変更されたかどうかを判断して、変更された場合は最新バージョンを取得する頻度を増やしてしまいます。

また、コスト削減策としては、エッジロケーション上のZIP圧縮によって配信ボリュームを低下させることで、コストを最適化することができます。ビューワーがリクエストヘッダーにAccept-Encoding: gzipを含めるリクエストをした場合は、CloudFrontが自動的にファイル圧縮して、供給するように設定できます。コンテンツが圧縮されるとファイルが小さくなるため、ダウンロード時間が短縮されます。場合によっては、オリジナルの4分の1以下のサイズになることがあります。

オプション2は不正解です。CloudFrontはオリジンでのZIP圧縮ではなく、エッジロケーションでの圧縮を行い配信します。

オプション4は不正解です。SSL/TLS認証はEC2インスタンスに設定するのではなく、CloudFrontに設定することが必要です。SSL/TLS認証はトラフィックを制御するサービスに設定することになり、CloudFrontまたはELBに設定することが一般的な利用方法となります。

オプション5は不正解です。CloudFrontのエッジ設定ではなく、オリジンサーバー設定において、Cache-control max-age directiveに対するオブジェクトと最適なキャッシュ保持期間を設定することが求められています。

20

A社は顧客データ管理用のJavaアプリケーションをAWS上に構築しています。WEBサーバーにはEC2インスタンスを利用して、RDS MySQLには顧客情報データを蓄積します。EC2インスタンスは付属したストレージを介したデータ処理が多数発生するため、オンデマンドEC2インスタンスのフリート設定を利用して、インスタンス構成を展開しつつ、高速通信を可能にする構成が必要となります。

要件を満たすことができる費用対効果の高いインスタンス構成は、次のうちどれですか？

- ◉ クラスタープレイスメントグループを設定した上で、G4インスタンス群を起動する。その上で、拡張ネットワークを有効化する。 (不正解)
- ○ G4インスタンス群を起動した上で、プレイスメントグループを構成する。その上で、拡張ネットワークを有効化する。
- ○ T3インスタンス群を起動した上で、プレイスメントグループを構成する。その上で、拡張ネットワークを有効化する。
- ○ クラスタープレイスメントグループを設定した上で、I3インスタンス群を起動する。その上で、拡張ネットワークを有効化する。 (正解)

説明

オプション4が正解となります。ストレージ最適化インスタンスであるI3インスタンスを使用して、データ処理が多発する一連のEC2インスタンスのCPUパフォーマンスのベースラインレベルを保証することができます。 I3 インスタンスには、低レイテンシー、超高ランダム I/O パフォーマンス、高シーケンシャル読み込みスループット向けに最適化された不揮発性メモリエクスプレス (NVMe) 対応 SSD ベースのインスタンスストレージが含まれており、低コストで高い IOPS を実現します。I3 インスタンスでは最大 25 Gbps のネットワーク帯域幅と最大 14 Gbps の Amazon Elastic Block Store (Amazon EBS) 専用帯域幅を利用できます。

新しい EC2インスタンスを起動する場合、EC2は相関性のエラーを最小限に抑えるために、すべてのインスタンスが基盤となるハードウェアに分散されるようにインスタンスを配置します。クラスタープレイスメントグループを使用することで、インスタンス間の通信制御を高速化することができます。この設定は先にプレイスメントグループを構成した上で、その中にインスタンスタイプとインスタンス数を指定して、起動する順番で実行することが必要です。

EC 2インスタンスの高速通信を可能にするためには拡張ネットワーキングを利用します。拡張ネットワーキングは高い帯域幅、1秒あたりのパケット (PPS) の高いパフォーマンス、常に低いインスタンス間レイテンシーを実現します。1秒あたりのパケットレートが切り上げ値に達していると表示された場合は、仮想ネットワークインターフェイスドライバーの上限しきい値に到達した可能性が高いため、拡張ネットワーキングに移行することを検討します。

オプション1と2は不正解です。G4インスタンスは、業界内で最も費用対効果の高いGPU インスタンスで、機械学習モデルの本番環境へのデプロイやグラフィックスを多用するアプリケーションに適しています。高機能ですがI3インスタンスよりも高価なインスタンスであるため、今回の要件にはコスト最適なインスタンスとは言えません。

オプション3は不正解です。プレイスメントグループの設定手順として、先にプレイスメントグループを構成した上で、その中でインスタンスタイプとインスタンス数を決定することが必要です。

21 B社はモバイルアプリケーションを開発・運用しているソフトウェア企業です。AWS上の複数のEC2インスタンスに対してAutoScalingグループとELBが設定されたアプリケーションを展開しています。B社のセキュリティポリシーでは、これらのインスタンスから仮想プライベートクラウド内の他のサービスへの全てのアウトバウンド接続はSSL認証が不可欠です。

【B社のVPC構成】

・VPC A には外部ELB、AutoScaling グループを設定したEC2 インスタンスにホストされたアプリケーションが起動している。

・VPC B には 内部 ELB、AutoScaling グループを設定したEC2 インスタンスにホストされたアプリケーションが起動している。

この構成において、VPC A の EC2 インスタンスから、VPC B の EC2 インスタンスにアクセスするために、一意のSSL認証が利用されることが必要となります。

この要件を達成することができる最適なソリューションを選択してください。

- (●) AMIにおいて、KMSを利用したキー設定を予めスクリプトに記述しておく。新しいEC2インスタンスがAutoScalingグループで起動されると、適用されたAMIのBootstrapによって新しいキーが生成されて、自動で新しいEC2インスタンスに適用される。 (不正解)
- ( ) 新しいEC2インスタンスがAutoScalingグループで起動されると、Amazon SNSによってX.509証明書を生成するようにAWS ACMに通知される設定をする。AWS ACMが新しいキーを生成して、新しいEC2インスタンスに適用する。
- ( ) AWS ACMを利用してSSL証明書を作成し、EC2インスタンスが配置されているELBに対して設定する。 (正解)
- ( ) AMIにおいて、CloudHSMを利用してキー設定を予めスクリプトに記述しておく。新しいEC2インスタンスがAutoScalingグループで起動されると、適用されたAMIのBootstrapによって新しいキーが生成されて、自動で新しいEC2インスタンスに適用される。

説明

このシナリオでは、VPC A の EC2 インスタンスから、VPC B の EC2 インスタンスにアクセスするために、一意のSSL認証が利用されることが必要であり、~~AutoScalingグループ~~で作成された新しいEC2インスタンスに対しても、SSL証明書を利用した認証が実行されるようにします。そのためにはEC2インスタンス単位ではなく、AWS ACMを利用してSSL証明書を作成し、EC2インスタンスが配置されているELBに対してSSL証明書を設定することが最適な対応となります。したがって、オプション3が正解となります。

~~AWS Certificate Manager~~ はSSL/TLS 証明書をプロビジョニングし、Elastic Load Balancer、Amazon CloudFront ディストリビューションや Amazon API Gateway の API でデプロイできます。AWSリソースで証明書をデプロイするには、AWS マネジメントコンソールのドロップダウンリストでデプロイする証明書を選択します。または、AWS API や AWS CLI を呼び出して、証明書をリソースに関連付けることもできます。その後、AWS Certificate Manager により、選択されたリソースに証明書がデプロイされます。

オプション 1 は不正解です。AMIのBootstrapによって新しいキーが生成されるといった設定は不可能です。

オプション 2 は不正解です。Amazon SNSによりX.509証明書を生成するように通知することはできますが、AWS ACMが新しいキーを生成して、新しいEC2インスタンスに適用するのではなく、EC2インスタンスが配置されているELBに対して、X.509証明書を設定することが必要となります。

オプション 4 は不正解です。AMIのBootstrapによって新しいキーが生成されるといった設定は不可能です。

22

あなたの会社は顧客管理システムとしてAWSクラウド上に2層アプリケーションを構築しています。アプリケーションレイヤーではEC2インスタンスによるデータ処理を実施し、データレイヤーではS3バケットにデータを保存しており、EC2インスタンスとAmazon S3との間で毎秒5 Gbpsを超えるデータ送信が発生します。 その際は、アプリケーションレイヤーはプライベートサブネット上にあり、そこからAmazon S3にデータを転送しています。また、このEC2インスタンスのデータ処理にはサードパーティーのソフトウェアが利用されているため、定期的にソフトウェアのパッチ更新が必要です。

このアプリケーションに対してデータ処理性能を向上させるソリューションを選択してください。

- (◉) EC2インスタンスとS3バケットとでVPCエンドポイントを利用したデータ通信を行うため、NATゲートウェイを維持して、新規にエンドポイントを作成し、ネットワークACLを使用してS3バケットにアクセスできるVPCとVPCエンドポイントを指定する。 (不正解)
- ( ) EC2インスタンスとS3バケットとでVPCエンドポイントを利用したデータ通信を行うため、NATゲートウェイを維持して、新規にエンドポイントを作成し、S3バケットポリシーを使用してS3バケットにアクセスできるVPCとVPCエンドポイントを指定する。 (正解)
- ( ) EC2インスタンスとS3バケットとでVPCエンドポイントを利用したデータ通信を行うため、NATゲートウェイを削除して、新規にエンドポイントを作成し、S3バケットポリシーを使用してS3バケットにアクセスできるVPCとVPCエンドポイントを指定する。
- ( ) EC2インスタンスとS3バケットとでVPCエンドポイントを利用したデータ通信を行うため、NATゲートウェイを削除して、新規にエンドポイントを作成し、ネットワークACLを使用してS3バケットにアクセスできるVPCとVPCエンドポイントを指定する。

説明

オプション2が正解となります。EC2 インスタンスから S3 バケットへ接続するために、S3用のVPCエンドポイントを作成し、S3バケットポリシーを使用してS3バケットにアクセスできるVPCとVPCエンドポイントを指定することが必要です。VPC エンドポイントを使うことで、EC2 インスタンスから S3 バケットへ接続する際にインターネットゲートウェイや NAT ゲートウェイが不要となりますが、このシナリオではプライベートサブネット内で処理を行っていることがわかります。したがって、このEC2インスタンスの処理にはサードパーティーのソフトウェアが利用して定期的にパッチ更新が必要となるため、VPCに構成したインスタンスへの処理向けにNATゲートウェイを維持することが必要です。

Amazon S3用のVPCエンドポイントは、設定が簡単で信頼性が高く、NATゲートウェイやNATインスタンスを必要としないS3への安全な接続を提供します。 VPCのプライベートサブネットで実行されているEC2インスタンスは、VPCと同じリージョンにあるS3バケット、オブジェクト、およびAPI関数へのアクセスを制御できます。 S3バケットポリシーを使用して、S3バケットにアクセスできるVPCとVPCエンドポイントを指定できます。

オプション1は不正解です。エンドポイントを設定する際はバケットポリシーを利用して構成します。

オプション3と4は不正解です。このシナリオでは、VPC エンドポイントを使うことにより、EC2 インスタンスから S3バケット へ接続する際にインターネットゲートウェイや NAT ゲートウェイが不要となりますが、パッチ適用のためにNATゲートウェイを維持する必要があります。

A社では社内データ共有システムをデータセンターにホストして運用しています。社内データはデータセンターのストレージに保存される仕組みとなっていますが、これらのデータは中長期保存用のため、迅速なデータ抽出は必要ありません。現在、このデータ処理のためにキューを利用したジョブ管理を行っています。また、データはテープライブラリによってアーカイブするBCP（事業継続性計画）対応をオンプレミスで実施しています。 あなたはソリューションアーキテクトとして、これらのシステムをAWSに移行するように依頼されました。

上記要件を満たすコスト最適なAWSアーキテクチャ設計パターンを選択してください。

- ◉ **AutoScalingを設定したリザーブドインスタンスを処理サーバーとして利用し、メッセージの処理にSQSを使用して連携する。社内データはS3 Standardに保存する。** (不正解)
- ○ **AutoScalingを設定したスポットインスタンスを処理サーバーとして利用し、メッセージの処理にSNSを使用して連携する。社内データはGlacierに保存する。**
- ○ **AutoScalingを設定したリザーブドインスタンスを処理サーバーとして利用し、メッセージの処理にSNSを使用して連携する。社内データはS3 Standardに保存する。**
- ○ **AutoScalingを設定したスポットインスタンスを処理サーバーとして利用し、メッセージの処理にSQSを使用して連携する。社内データはGlacierに保存する。** (正解)

説明

オプション４が正解となります。この要件を満たすコスト最適な構成としては、メッセージ処理においてAmazon SQSを利用してキューによるタスク処理を行えるようにして、ストレージオプションとしてGlacierの組み合わせます。GlacierはS3 Standardよりも中長期保存するデータを安く保存することができるストレージタイプであり、コスト最適に要件を達成するために最適です。さらにAutoScalingを設定して、高負荷時にスポットインスタンスによるスケーリングを可能にすることで、コスト最適に高負荷時の処理を可能にします。

オプション１と３は不正解です。社内データは中長期の保存され、かつ迅速なデータ取り出しを必要としないため、S3 Standardではなく、Glacierを利用することが最適です。

また、メッセージの処理にはSNSではなく、SQSによるポーリング処理による並列ワーカー処理を構築することが最適となります。したがって、オプション２と３は不正解です。

24

大手薬局では自社のエンタープライズシステム向けに、データセンターをAWSクラウドに拡張するハイブリッドクラウドインフラストラクチャを利用することになりました。その際は、オンプレミス側とAWSクラウド側で2つの個別のログインアカウントを持ってしまうことで、複数の資格情報を保存することを避ける必要があります。したがって、社内アカウントを使用して既にサインインしているオンプレミス環境のユーザーが、個別のIAMユーザーを作成せずにAWSリソースを利用する構成が求められています。

このシナリオにおいて、要件を満たすためのAWSアーキテクチャ設計パターンを選択してください。

- (●) SAML 2.0 IDプロバイダーを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からAssumeRole WithWebIdentityを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与する (不正解)
- ( ) SAML 2.0 IDプロバイダーを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からシングルサインオン（SSO）エンドポイントを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与する (正解)
- ( ) OAuth 2.0 IDプロバイダーを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からシングルサインオン（SSO）エンドポイントを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与する
- ( ) OPEN IDを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からシングルサインオン（SSO）エンドポイントを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与する
- ( ) OPEN IDを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からAssumeRole WithWebIdentityを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与する

説明

このシナリオでは、既にオンプレミス環境上でユーザー管理をしている場合において、AWSとのハイブリッドアーキテクチャを実装する際に、シングルサインオンを構築する方法が問われています。したがって、ユーザーがオンプレミスネットワークで一度サインインするだけで、AWSクラウドに同時にアクセスできるようにシングルサインオン認証をセットアップすることが必要です。

AWSではSAML 2.0を使用した ID フェデレーションが提供されています。これは、多くの ID プロバイダー (IdP) により使用されているオープンスタンダードな技術です。この機能はフェデレーティッドシングルサインオン (SSO) を有効にします。したがって、組織内の全員について IAM ユーザーを作成しなくても、ユーザーは AWS マネジメントコンソール にログインしたり、AWS API オペレーションを呼び出したりできるようになります。

SAML 2.0 IDプロバイダーを使用してユーザーに対して、AWSリソースへのフェデレーションアクセスを提供し、オンプレミス環境からシングルサインオン（SSO）エンドポイントを使用してユーザーを認証し、フェデレーションアクセスを提供する前にアクセストークンを付与することでシングルサインオンを実現することができます。したがって、オプション２が正解となります。

詳細は以下のページをご参照ください。

https://docs.aws.amazon.com/ja_jp/IAM/latest/UserGuide/id_roles_providers_enable-console-saml.html

オプション１は不正解です。 AssumeRoleWithWebIdentityはWeb Identity Federation（Facebook、Google、およびその他のソーシャルログイン）専用の認証方式です。

オプション３は不正解です。 このシナリオでは、OAuth 2.0ではなく、SAML 2.0 IDプロバイダーを使用してSSOを実現する必要があるため、正しくありません。

オプション４が不正解です。OPEN IDはFacebook、Google、およびその他のソーシャルログインで使用されるログイン形式であり、シングルサインオン認証と併用はできますが、シングルサインオン認証を有効化するための機能ではないため正しくありません。

25 ⊗

あなたの会社は、Amazon Elastic Container Service（ECS）を使用したDockerベースのエンタープライズアプリケーションを構築しています。そのデータベース層では、マルチAZ構成でリードレプリカを持つRDS MySQLデータベースを利用しています。このように、データベース層は既に高可用でスケーラブルに構成されていますが、アプリケーション層にもスケーラビリティを確保することが求められています。そのため、ECSクラスターに対するオートスケーリング設定を実施することにしました。

このシナリオにおいて、要件を満たすための最適な方法を選択してください。

- ◉ **Capacity Provider Reservationを利用してAuto Scalingグループを構成して、ECS Cluster Auto ScalingによるECSクラスターのオートスケーリングを実施する。** (正解)
- ○ **Capacity Provider Reservationを利用してAuto Scaling グループを構成して、既存のAuto ScalingグループをECSに設定する。**
- ○ **AutoScalingポリシーによってAuto Scalingグループを構成して、ECS Cluster Auto ScalingによるECSクラスターのオートスケーリングを実施する。ECSの起動インスタンスをEC2起動タイプにすることで、オートスケーリングを適用する。**
- ○ **AutoScalingポリシーによってAuto Scalingグループを構成して、ECS Cluster Auto ScalingによるECSクラスターのオートスケーリングを実施する。ECSの起動インスタンスをEC2起動タイプからFargate起動タイプにすることで、オートスケーリングを適用する。**

説明

Amazon ECS Cluster Auto Scalingによって、ECSクラスターのオートスケーリングを設定することができます。この機能は、スケールアウトを高速化し信頼性を向上させて、クラスター内の空きキャパシティ管理の提供と、スケールイン時に終了されるインスタンスの自動管理を提供し、クラスターの自動スケーリングをより使いやすいものにします。

Amazon ECS Cluster Auto Scalingの設定方法は以下の通りです。

・ECS Cluster Auto Scalingを有効にするには、Capacity Providerと呼ばれる新たな項目を設定する必要があります。1つのCapacity Providerは1つのEC2 Auto Scalingグループに関連付けられます。Auto ScalingグループにECS Capacity Providerを関連付け、ECSクラスターにCapacity Providerを追加すると、ECSクラスターを自動スケールできるようになります。

・Capacity Provider Reservationという新しいメトリックに対応するスケーリングポリシーが自動的に生成され、Auto Scalingグループにアタッチされます。

したがって、オプション１が正解となります。

オプション２は不正解です。Capacity Provider Reservationという新しいメトリクスに対応するスケーリングポリシーが自動的に生成され、Auto Scalingグループに構成して、既存のAuto ScalingグループをECSに設定するのではなく、Amazon ECS Cluster Auto Scalingと呼ばれる専用機能を利用した構成を行います。

オプション３は不正解です。AutoScalingポリシーによってAuto Scaling グループを構成するのではなく、Capacity Provider Reservationを利用します。

オプション４は不正解です。Fargateにもオートスケーリング機能がありますが、この質問で問われているのは、既存のECSの仕組みをスケーリングさせることです。Fargate起動タイプとEC２起動タイプは互換性があるわけではなく、ユースケースが異なるため、現在のEC２起動タイプからFargate起動タイプに再構成するのは容易な対応ではありません。

25

大手車両メーカA社では複数アカウントで複数部門がAWSを利用しています。社内の統合管理のために全社共通のIT運用部門では、AWS Organizationsを使用して、マルチアカウントおよびマルチリージョンのAWSアカウントを管理しています。現在、AWSアカウントAとAWSアカウントBとAWSアカウントCという３つのアカウントを管理していますが、アカウントAのユーザーがアカウントBのEC2インスタンスへのアクセスを定期的に実施するタスクが発生しました。あなたはソリューションアーキテクトとして、このクロスアカウント処理が必要となる定期タスクを自動化するように依頼されました。

上記の要件を満たす有効なソリューションは次のうちどれですか？

- ◉ **AWS Configにより所有する特定のAWSリソースを他のAWSアカウントと共有する。AWS Config CLIから、enable-sharing-with-aws-organizationsコマンドを使用して、Trusted Accessを有効化することで、特定の構成変更を自動で反映する設定を行う。** (不正解)
- ○ **AWS Organizations により所有する特定のAWSリソースを他のAWSアカウントと共有する。AWS Organizations CLIから、enable-sharing-with-aws-organizationsコマンドを使用して、Trusted Accessを有効化することで、特定の構成変更を自動で反映する設定を行う。**
- ○ **AWS Resource Share (RAS)を利用したリソース共有化を実現する。RAS CLIから、enable-sharing-with-aws-organizationsコマンドを使用して、Trusted Accessを有効化することで、特定の構成変更を自動で反映する設定を行う。**
- ○ **AWS Resource Access Manager (RAM)を利用したリソース共有化を実現する。AWS RAM CLIから、enable-sharing-with-aws-organizationsコマンドを使用して、Trusted Accessを有効化することで、特定の構成変更を自動で反映する設定を行う。** (正解)

説明

AWS Organizationsにおいて、Trusted Accessを使用して、指定したAWSサービスを有効化することで、組織とそのアカウントでタスクを自動で実行する設定を行うことができます。これには、信頼できるサービスへのアクセス許可の付与が含まれますが、IAMユーザーまたはロールのアクセス許可には影響しません。アクセスを有効にすると、信頼できるサービスは、組織のすべてのアカウントにサービスにリンクされたロールと呼ばれるIAMロールを作成できます。そのロールには、信頼できるサービスがそのサービスのドキュメントに記載されているタスクを実行できるようにする許可ポリシーがあります。これにより、信頼できるサービスに代わって組織のアカウントで維持する設定と構成の詳細を指定できます。

AWS Resource Access Manager（AWS RAM）を使用すると、所有する特定のAWSリソースを他のAWSアカウントと共有できます。 AWS OrganizationsにおいてTrusted Accessを有効にするにはAWS RAM CLIから、enable-sharing-with-aws-organizationsコマンドを使用します。したがって、オプション４が正解となります。

オプション１は不正解です。AWS Configにより所有する特定のAWSリソースを他のAWSアカウントと共有して、AWS Config CLIからTrusted Accessを有効化するといった操作はできません。

オプション２は不正解です。(AWS Organizations のクロスアカウントアクセスによって、所有する特定のAWSリソースを他のAWSアカウントと共有することは可能ですが、Trusted Accessを有効化するといった対応ではないため、このオプションは設定方法に間違いがあります。)

オプション３は不正解です。AWS Resource Share (RAS)というサービスはありません。AWS RAM CLIを利用する必要があります。

あるベンチャー企業ではAWSを利用したCI/CD環境を整備しています。開発環境などは全てDocker形式で展開できるようにしており、Fargate起動タイプを使用するAmazon ECSクラスターを利用しています。今回は社内製品を販売するためのECサイトを構築することになりました。ECSでの実装において、環境変数を使用して顧客データベースの資格情報をECサイトに提供する必要があります。その際には、資格情報がデータ保持とイメージ転送が安全であることが保障され、かつクラスター自体で表示できないようにセキュリティを徹底することが求められています。また、資格情報の保持にはライフサイクル管理が必要となります。

このシナリオで、上記要件を満たす有効なソリューションは次のうちどれですか？

- ◉ **Systems Managerパラメーターストアを利用して資格情報を保持して、AWS KMSを利用して暗号化を実施する。Amazon ECSの実行ロールとAWS Secrets ManagerとAWS KMSへのアクセス許可を付与したIAMロールを作成する。その上で、コンテナーに設定する環境変数の名前とコンテナーに提示する機密データを含むSystems Managerパラメーターストアのフル ARNでシークレットを指定して管理を実施する。** (不正解)

- ○ **AWS Secrets Managerを利用して資格情報を保持して、AWS KMSを利用して暗号化を実施する。Amazon ECSの実行ロールとAWS Secrets ManagerとAWS KMSへのアクセス許可を付与したIAMロールを作成する。その上で、コンテナーに設定する環境変数の名前とコンテナーに提示する機密データを含むSecrets Managerシークレットのフル ARNで、シークレットを指定して管理を実施する。** (正解)

- ○ **Amazon Cognitoパラメーターストアを利用して資格情報を保持して、AWS KMSを利用して暗号化を実施する。Amazon ECSの実行ロールとAWS Secrets ManagerとAWS KMSへのアクセス許可を付与したIAMロールを作成する。その上で、コンテナーに設定する環境変数の名前とコンテナーに提示する機密データを含むAmazon CognitoのフルARNでシークレットを指定して管理を実施する。**

- ○ **AWS Secrets Managerを利用して資格情報を保持して、AWS KMSを利用して暗号化を実施する。Amazon ECSの実行ロールとAWS Secrets ManagerとAWS KMSへのアクセス許可を付与したIAMロールを作成する。その上で、コンテナーに設定する環境変数の名前とコンテナーに提示する機密データを含むAmazon CognitoのフルARNでシークレットを指定して管理を実施する。**

説明

オプション２が正解となります。資格情報がECSのイメージに渡される際の安全性を高めるためには、AWS Secrets Managerを利用して資格情報を保持して、AWS KMSを利用して暗号化を実施することが求められます。Amazon ECSの実行ロールとAWS Secrets ManagerとAWS KMSへのアクセス許可を付与したIAMロールを作成します。その上で、コンテナーに設定する環境変数の名前とコンテナーに提示する機密データを含むSecrets Managerシークレットのフル ARNでシークレットを指定して管理を実施することができます。

単純に１つのストアを利用する場合はパラメータストアを利用することができますが、ライフサイクル管理を備えたシークレット専用のストアが欲しい場合、シークレットマネージャーを利用することが必要となります。

Amazon Elastic Container Service (Amazon ECS) は、Docker コンテナをサポートする拡張性とパフォーマンスに優れたコンテナオーケストレーションサービスです。これにより、コンテナ化されたアプリケーションを AWS で簡単に実行およびスケールできます。Amazon ECSでは、AWS Secrets ManagerシークレットまたはAWS Systems Manager Parameter Storeパラメーターのいずれかに機密データを保存し、コンテナー定義でそれらを参照することにより、機密データをコンテナーに注入できます。この機能は、EC2とFargateの両方の起動タイプを使用するタスクでサポートされています。

コンテナー定義内で、コンテナーに設定する環境変数の名前と、コンテナーに提示する機密データを含むSecrets ManagerシークレットまたはSystems Managerパラメーターストアパラメーターの完全なARNでシークレットを指定します。AWS Secrets Manager は、アプリケーション、サービス、IT リソースへのアクセスに必要なシークレットの保護を支援します。

Secrets Manager は、Amazon RDS、Amazon Redshift、Amazon DocumentDB への統合を組み込むことでシークレットのローテーションを提供します。また、このサービスは API キーや OAuth トークンなど他のタイプのシークレットにも使えます。さらに、Secrets Manager は、AWS クラウド、サードパーティーサービス、オンプレミスのリソースに対して中央でのきめ細かいアクセス許可と、シークレットローテーションの監査を用いて、シークレットへのアクセスをお客様がコントロールできるようにします。構成とシークレット用の単一のストアが必要な場合は、パラメーターストアを使用できます。ライフサイクル管理を備えた専用のシークレットストアが必要な場合は、AWS Secrets Managerを使用します。

オプション１と３は不正解です。このシナリオでは、AWS Secrets Managerを利用して資格情報を保持する必要があるためです。ライフサイクル管理を備えたシークレット専用のストアが欲しい場合、シークレットマネージャーを利用することが必要です。また、Cognitoにはパラメーターストアという機能はありません。

28

大手のグローバル会計ファームはAWSにホストされるウェブベースの会計アプリケーションを有しています。現在、このアプリケーションのインターフェースとなるフロントサーバー群はAWSのパブリックサブネット上で利用されており、社内のネットワークからのみAWSサイト間VPN接続によって利用することができます。 会社ではリモートワークを推進しており、外部Wifiがある環境であればどこからでもリモート接続して作業ができる機能を実装することになりました。外部からのアクセスが頻繁に発生することや、機密性の高いデータを扱っていることから、セキュリティ性能をできる限り高めることが課題となっています。

このシナリオで、上記要件を満たす有効なソリューションは次のうちどれですか？

○ プライベートサブネットを構成してNATゲートウェイを設定し、パブリックサブネットにあるアプリケーションサーバーをプライベートサブネットに移行する。利用しているVPCのパブリックサブネットにAWS クライアントVPNを構成する。会計アプリの全ユーザーが利用するラップトップPCにOpenVPN ベースの VPN クライアントソフトウェアをインストールする。 (正解)

◉ プライベートサブネットを構成してNATゲートウェイを設定し、パブリックサブネットにあるアプリケーションサーバーをプライベートサブネットに移行する。SSL通信をELBとEC2インスタンス間とで実施する設定を行い、全クライアントとのSSLによるセキュアな通信を実現する。 (不正解)

○ プライベートサブネットを構成してNATゲートウェイを設定し、パブリックサブネットにあるアプリケーションサーバーをプライベートサブネットに移行する。セキュリティグループの設定で全ユーザーのIPアドレスを登録して許可設定を行う。

○ プライベートサブネットを構成してNATゲートウェイを設定し、パブリックサブネットにあるアプリケーションサーバーをプライベートサブネットに移行する。サブネット内のネットワークACL設定で全ユーザーのIPアドレスを登録して許可設定を行う。

説明

オプション 1 が正解となります。利用しているVPCのパブリックサブネットにAWS クライアントVPNを構成して、会計アプリの全ユーザーが利用するラップトップPCに OpenVPN ベースの VPN クライアントアプリケーションをインストールします。これによって、ラップトップPCからのリモートVPN接続が可能となります。さらにプライベートサブネットを構成して、アプリケーションサーバーを移行します。

~~VPN接続はパブリックインターネット経由でアクセスティングアプリケーションへの安全な接続を提供する最適なソリューションです。~~ AWS クライアントVPN はAWS リソースやオンプレミスネットワーク内のリソースに安全にアクセスできるようにするクライアントベースのマネージド VPN サービスです。クライアント VPN を使用すると、OpenVPN ベースの VPN クライアントを使用して、どこからでもAWSリソースにアクセスできます。

AWS クライアントVPN においては、クライアント VPN エンドポイントの管理者およびクライアントとやり取りする 2 つのタイプのユーザーがいます。

■管理者はサービスの設定を担当します。このプロセスには、クライアント VPN エンドポイントの作成、ターゲットネットワークの関連付け、認証ルールの設定、および追加のルート (必要な場合) の設定が含まれます。クライアント VPN エンドポイントを設定した後、管理者は クライアント VPN エンドポイント設定ファイルをダウンロードして、アクセスが必要なクライアントに配布します。クライアント VPN エンドポイント設定ファイルには、クライアント VPN エンドポイントの DNS 名と、VPN セッションを確立するために必要な証明書情報が含まれています。

■クライアントはエンドユーザーです。これは、VPN セッションを確立するために クライアント VPN エンドポイントに接続する人です。クライアントは OpenVPN ベースの VPN クライアントアプリケーションを使用して、ローカルコンピュータまたはモバイルデバイスから VPN セッションを確立します。VPN セッションが確立されたら、関連付けられているサブネットが存在する VPC のリソースに安全にアクセスできます。必要なルートと認証ルールが設定されている場合は、AWS またはオンプレミスネットワークの他のリソースにもアクセスできます。

オプション 2 は不正解です。SSL通信をELBとEC2インスタンス間とで実施する設定だけでは、HTTPSプロトコルによる接続ができるだけです。これではVPNソフトウェアを利用した外部インターネットからのリモート通信を確立することができません。

オプション 3 は不正解です。セキュリティグループの設定で全ユーザーのIPアドレスを登録して許可設定を行う方式では、特定IPアドレスをすべて限定する必要があり、リモートアクセスができなくなってしまいます。またセキュリティグループによってEC2インスタンスへのアクセス権限を個別に設定する方式は非効率です。

オプション 4 は不正解です。ネットワークACLによる設定もセキュリティグループと同様に、特定IPアドレスがすべて限定する必要があり、リモートアクセスができなくなってしまいます。

2

大手商社はオンプレミス環境において、以前からMicrosoft Active Directoryを使用して、すべての従業員アカウントとデバイスを管理しています。最近になって、経営陣がAWSクラウドを利用したハイブリッドアーキテクチャを採用することを決定しました。新規にAWSにおいてIAM管理を実施することは非効率であるため、既存のWindowsアカウントパスワードを使用して様々なAWSリソースに接続して使用できるように、AWS Directory Serviceを設定することが必要となります。

既存のADワークロードをAWS側に移行しつつ、シングルサインオンの認証ソリューションを選択してください。

- ○ **AWS Directory Serviceを利用して、既存のMS Active DirectoryとAWSリソース管理とを統合し、AWS Managed Microsoft ADを利用してシングルサインオンを実現する。** (正解)
- ○ **AWS Organizationsを利用して、既存のMS Active DirectoryとAWSリソース管理とを統合し、AD Connectorを利用してシングルサインオンを実現する。**
- ◉ **IAMダッシュボードとAWS Directory Service Connectを利用して、既存のMS Active DirectoryとAWSリソース管理とを統合し、AWS Managed Microsoft ADを利用してシングルサインオンを実現する。** (不正解)
- ○ **AWS Directory Serviceを利用して、既存のMS Active DirectoryとAWSリソース管理とを統合し、AD Connectorを利用してシングルサインオンを実現する。**

説明

オプション1が正解となります。~~AWS Directory Serviceを利用して、既存のMS Active Directoryと AWSリソース管理とを統合し~~、AWS Managed Microsoft ADを利用してシングルサインオンを実現することができます。

既存のオンプレミス環境にあるMS ADを利用して、AD対応ワークロードをAWSクラウドに移行する場合は、AWS Managed Microsoft ADを利用します。AD間の信頼を確立して、AWS Managed Microsoft ADを既存のADに接続できます。これにより、AD対応アプリケーションとAWSアプリケーションにオンプレミスAD認証情報でアクセスすることが可能となります。たとえば、ユーザーは既存のADユーザー名とパスワードを使用して、AWSマネジメントコンソールとAmazon WorkSpacesにサインインできます。また、AWS Managed Microsoft ADでSharePointなどのAD対応アプリケーションを使用すると、ログインしたWindowsユーザーは認証情報の再入力なし、これらのアプリケーションにアクセスできるようになります。

オプション2は不正解です。AWS OrganizationsはDirectory Serviceの構築には利用されないため、正しくありません。

オプション3は不正解です。IAMダッシュボードとAWS Directory Service Connectを統合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。AD Connectorを利用してもシングルサインインを実現することは可能です。Windows Server 2003以降で実行されるドメインコントローラをVPCにプロキシすることで、ADドメインのログイン情報でAWSのManagement Consoleにシングルサインオン(SSO)とすることができます。しかしながら、~~既存のAD対応ワークロードをAWSクラウドに移行する場合は、AWS Managed Microsoft ADが最適であり~~、不正解となります。

30

大手商社ではAWSをクラウドソリューションとして導入することが決定されました。そのためには、AWSとオフィスネットワークとを接続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、リモートネットワークをAmazon VPC環境に接続するための接続設定を実施しています。 社内の要件は以下の通りです。

・予測可能で十分なネットワークパフォーマンスを提供する
・安全なIPsec VPN接続を実現する
・コスト効率の良い方法で可用性を達成する。

クライアントの要件を達成することができる最適な接続方式を選択してください。

- ◉ **AWS Direct Connectによる専用線接続を実施して、AWS VPN CloudHubによるプライベートリンクを実施する。その上で、別途AWS VPNを構成して可用性を高める。** (不正解)
- ○ **AWS Direct Connectによる専用線接続を実施して、さらに別途AWS Direct Connectを構成して可用性を高める。**
- ○ **AWS Direct Connectによる専用線接続を実施して、IPSecハードウェアVPNによるプライベートリンクを実施する。その上で、別途AWS VPNを構成して可用性を高める。**
- ○ **AWS Direct Connect with IPSecによる専用線接続を実施する。その上で、別途AWS Direct Connectを構成して可用性を高める。**
- ○ **AWS Direct Connectによる専用線接続を実施して、IPSecハードウェアVPNによるプライベートリンクを実施する。** (正解)

説明

予測可能で十分なネットワークパフォーマンスを提供するという要件からVPNなどのネットワーク接続ではなく専用線によるAWS Direct Connectが最適な選択となります。
Amazon VPCはAWS上に論理的に独立した仮想クラウドを作成する機能ですが、このVPCと既存データセンターやホームネットワークなどをIPSec VPNにて接続するAWSハードウェアVPN接続を利用可能です。Direct Connectは、AWS ハードウェア VPN 接続と組み合わせて、IPsec で暗号化された接続を作成することができます。

安全なIPsec VPN接続を実現することや、コスト効率の良い方法で可用性を達成するためには、[redacted] VPN を Direct Connect 接続のフェールオーバーオプションとして設定することが必要です。VPN 接続は、ほとんどの Direct Connect 接続で利用できる帯域幅と同じレベルを提供することはできませんが、安価なバックアップとして利用することができます。したがって、オプション 5 が正解となります。

オプション 1 は不正解です。AWS VPCとだけでなく、リモートサイトが相互に通信したいときにCloudHubが使用されるため、正しくありません。複数の AWS Site-to-Site VPN 接続がある場合は、AWS VPN CloudHub を使用して、安全なサイト間通信を提供することができます。これで、リモートサイトを有効にして、VPC のみとではなく、相互に通信を可能にすることができます。

オプション 2 は不正解です。Direct Connectの二重構成はコストが高いため、コスト効率の良い方法という要件に合致していません。

オプション 3 は不正解です。別途AWS VPNを構成して可用性を高めるという対応が不要です。既にIPSecハードウェアVPNによるプライベートリンクを実施することでDirect Connect接続とVPN接続の冗長化構成を実現しているため、その上で、別途AWS VPNを構成して可用性を高める必要はありません。

オプション 4 は不正解です。AWS Direct Connect with IPSecというサービスはありません。