

この1冊で合格！ AWS認定
ソリューションアーキテクト - アソシエイト
テキスト&問題集

模擬試験の解答・解説

Q1	Q2	Q3	Q4	Q5	Q6
A	C	C	D	A, D	B
Q7	Q8	Q9	Q10	Q11	Q12
A	D	B, D	A, C	C	C
Q13	Q14	Q15	Q16	Q17	Q18
B, C	B	C	B, D, E	C	B
Q19	Q20	Q21	Q22	Q23	Q24
A, B, C, D, E	B, C	A, B, D	A, C, F	B, C, E	A, C
Q25	Q26	Q27	Q28	Q29	Q30
B	A, B	B, C	A	B	B
Q31	Q32	Q33	Q34	Q35	Q36
B	C	A	B	A	C
Q37	Q38	Q39	Q40	Q41	Q42
C, D	A	B	A, D	B	A
Q43	Q44	Q45	Q46	Q47	Q48
E	B	D	A	D	D
Q49	Q50	Q51	Q52	Q53	Q54
B	C	D	C	B	C
Q55	Q56	Q57	Q58	Q59	Q60
D	A	A, B, D, E	B, C	D	A
Q61	Q62	Q63	Q64	Q65	
A, C, D	B, D, E	C	B	C	





解答と解説

Q1 答え A

Aは適切な選択肢です。AWS側でインスタンスのキャパシティに余裕がある場合は、その余裕や需要に応じた価格（スポット料金）でインスタンスが提供されます。ユーザーの設定した上限料金がスポット料金よりも高い場合に、スポットインスタンスを利用できます。スポット料金はインスタンスのキャパシティによって変動するため、スポット料金が上限料金を上回ると、インスタンスは中断（Terminate）され、その中のデータもなくなります。そのため、EC2インスタンスの障害対応と同等の対応が必要となります。

Bは不適切な選択肢です。リザーブドインスタンスでは、利用するキャパシティを予約することで最大75%の割引を受けることができます。

Cは不適切な選択肢です。オンデマンドインスタンスは、利用した時間の分だけ課金されるインスタンスです。

Q2 答え C

Aは不適切な選択肢です。Elastic IPアドレスは、プライベートではなくパブリックIPアドレスです。

Bは不適切な選択肢です。AMIにあらかじめプライベートIPアドレスを割り当てることはできません。

Cは適切な選択肢です。EC2インスタンスをサブネットで起動すれば、プライマリプライベートIPアドレスが割り当てられます。

Dは不適切な選択肢です。Route 53はDNSサービスを提供するものです。たとえば、AレコードでDNS名とIPアドレスの対応を設定できます。IPアドレスをEC2インスタンスに割り当てるサービスではありません。

Q3 答え C

Aは不適切な選択肢です。セキュリティグループはステートフルです。つまり、送信トラフィックが許可されていれば、受信トラフィックで許可されるプロトコルやポート番号を明示的に示さなくても許可されます。よって、これが理由ではありません。

Bは不適切な選択肢です。プライベートサブネットのルートテーブルについて言及していますが、パブリックサブネットに存在するEC2インスタンスからのインターネットへの送信には関係ありません。

Cは適切な選択肢です。インターネットにリクエストを送出するインスタンスは、リクエストの戻りを受けるためのパブリックなIPアドレスが必要です。

Dは不適切な選択肢です。ネットワークACLではデフォルトですべての送受信トラフィックが許可されています。トラフィックの制御は、ネットワークACLではなくセキュリティグループで行うのがベストプラクティスとされており、

ユーザーの設定は必須ではありません。パブリックサブネットのEC2インスタンスがインターネットにアクセスするのに、プライベートサブネットのルートテーブルは関係ありません。

Q4 答え D

Aは不適切な選択肢です。メトリクスフィルタは、CloudWatch Logsのログデータの中から、あらかじめ定義したパターンを検知するための機能です。

BとCは不適切な選択肢です。パターンや費用フィルタという機能はありません。

Dは適切な選択肢です。タグにより、部門や環境ごとに費用を確認できます。

Q5 答え A、D

AとDが適切な選択肢です。Elastic IPアドレスやパブリックIPアドレスは、VPC内のほかのEC2インスタンスからのアクセスには使用されません。

Q6 答え B

Aは不適切な選択肢です。マグネティックは、旧世代のボリュームタイプです。アクセス頻度の低いデータの場合やコストを最重要視する場合に利用し、パフォーマンスを求める場合には選択しません。

Bは適切な選択肢です。プロビジョンドIOPSは、汎用SSDでは処理しきれないI/O性能が要求される場合に利用します。

Cは不適切な選択肢です。汎用SSDは、突発的なピーク時に高いベースライン性能を発揮できます。システムブートボリュームや中小規模のデータベースに使用されることが多いといえます。

Dは不適切な選択肢です。スループット最適化HDDは、シーケンシャルアクセス時に高い性能を発揮します。ランダムアクセスが行われるデータベースには向いていません。

Q7 答え A

Aが適切な選択肢です。EBSをアタッチできるのは、同一のアベイラビリティゾーンの範囲内のEC2インスタンスです。この範囲を超えたスコープでEC2インスタンスにアタッチすることはできないため、その他の選択肢は不適切です。

Q8 答え D

Aは不適切な選択肢です。既存のEBSボリュームは、そのまま暗号化できません。

Bは不適切な選択肢です。新規にEBSボリュームを作成するときは、暗号化オプションを指定できますが、新規作成時だけではありません。

Cは不適切な選択肢です。暗号化されたEBSボリュームのスナップショットは

Aは適切な選択肢です。

Dが適切な選択肢です。一度スナップショットを取得し、そこからスナップショットのコピーを作成する際に暗号化のオプションを指定できます。

Q9 答え B、D

Aは不適切な選択肢です。EBSとインスタンスストアについて逆のことを述べています。

Bは適切な選択肢です。EBSの中のデータは永続的なものであり、EC2インスタンスを停止したり、削除したりしたときも同様です。また、インスタンスストアはEC2インスタンスが配置されているホストコンピュータに内蔵されているため、EC2インスタンスが再起動して別のホストコンピュータに移動すると、その中のデータは参照できなくなります。

Cは不適切な選択肢です。EBSはボリュームタイプを選択できますが、インスタンスストアはできません。

Dは適切な選択肢です。EBSはボリュームタイプを選択できます。

Q10 答え A、C

Aは適切な選択肢です。

Bは不適切な選択肢です。汎用SSDに限らずいかなるEBSの種類でも、EBSは1つのEC2インスタンスのみにアタッチできます。同時に2つ以上のEC2インスタンスにアタッチすることはできません。

Cは適切な選択肢です。EBSは、同じアベイラビリティーゾーンのEC2インスタンスのみにアタッチできます。ほかのアベイラビリティーゾーンのEC2インスタンスにアタッチして利用したいときは、ボリュームのバックアップであるスナップショットを取得します。任意のアベイラビリティーゾーンにそのスナップショットからボリュームを復元して、EC2インスタンスにアタッチします。

Dは不適切な選択肢です。EBSボリュームをそのままほかのリージョンにコピーすることはできません。一度、スナップショットに変換します。

※選択肢C、Dについて、EBSのスナップショットはリージョン間コピーを行うことができるため、「ほかのリージョンにコピーする」という表現をしています。

Q11 答え C

Aは最適な選択肢ではありません。テープ保管の代替ストレージはGlacierであり、S3標準より費用対効果が高くなっています。

Bは最適な選択肢ではありません。スポットインスタンスを利用する場合、スポット価格によってはインスタンスが削除されます。処理されたデータがS3に保存される前に削除されてしまう可能性があります（この事態を回避する実

装を行うことも可能ですが)。また、テープ保管の代替ストレージはGlacierであり、S3標準より費用対効果が高いです。

Cは適切な選択肢です。ジョブを処理するワーカーインスタンスは、SQSに蓄積された未処理のメッセージ数をトリガーとしたAuto Scalingでスポットインスタンスを利用することで費用対効果が高まります。また、テープ保管の代替ストレージとしては、Glacierが最もコストを抑えられます。

Dは不適切な選択肢です。SQSはワーカーインスタンス側から取り出してジョブを実行できますが、SNSの場合、プッシュでジョブが送信されるため、ワーカーインスタンスが常に起動している必要があります。また、EC2がターミネート処理されるとジョブの送信先がなくなる可能性があります。

Q12 答え C

Aは不適切な選択肢です。Multi-AZ構成のスタンバイインスタンスはアクセス不可です。レポート層の実装には利用できません。

BおよびDは不適切な選択肢です。DynamoDBやElastiCacheはデータベースであるため、リクエストが直接アクセスするレポート層を実装できません。

Cは適切な選択肢です。RDSリードレプリカを使用すれば、既存のデータベースに影響を与えることなくレポート層を実装できます。

Q13 答え B、C

Aは不適切な選択肢です。CloudTrailはユーザーのマネジメントコンソールへの操作やAPIアクセスを記録します。Webアプリケーションへのアクセスログは記録しません。

BとCは適切な選択肢です。ELBのログに加え、CloudFrontがキャッシュから応答したときのアクセスログを出力させます。CloudFrontによりキャッシュが返されると、ELBやEC2にはログが残りません。

Dは不適切な選択肢です。CloudFrontがキャッシュから応答したときのアクセスログは、EC2のアクセスログからは取得できいためです。

Q14 答え B

Bが適切な選択肢です。一括請求(Consolidated Billing)を設定するには、問題にある2つの新規AWSアカウントを、すでに利用しているマスターアカウントのメンバーアカウントとしてAWS Organizationsを構成する必要があります。

その他の選択肢にあるクロスアカウントアクセスによるSwitch Roleでは、請求情報の確認はできますが、一括請求はできません。

Q15 答え C

Aは不適切な選択肢です。作成済みのボリュームをそのまま暗号化することはできません。

Bは不適切な選択肢です。スナップショットに暗号化オプションは設定できません。

Cは適切な選択肢です。EBSボリュームを暗号化するには、一度EBSボリュームのスナップショットを作成してからコピーを行い、その際に暗号化オプションを有効にします。

Dは不適切な選択肢です。既存のEBSボリュームでは暗号化オプションを有效地にできません。

Q16 答え B、D、E

Aは不適切な選択肢です。S3が暗号化対応しているとは限りません。

B、D、Eは適切な選択肢です。

S3の暗号化には3つの方法があります。AWS KMSを使用したサーバーサイド暗号化、S3管理キーを使用したサーバーサイド暗号化、ユーザー独自のキーを使用したクライアントサイド暗号化です。通常は、S3に保存する際にどの暗号化を使用するかを指定します。なにも指定していない場合は、バケットポリシーによってデフォルト暗号化が指定されていれば、指定された方法で暗号化されます。

Cは不適切な選択肢です。EC2キーペアでは、S3のサーバーサイド暗号化はできません。

Q17 答え C

Aは不適切な選択肢です。インスタンスのアクセスキーといった場合、EC2インスタンスのプログラムで利用されるアクセスキーとなります。EC2インスタンスからアクセスキーが漏洩するリスクもあります。そのため、アクセスキーの厳重な管理やローテーションが必要となります。

Bは不適切な選択肢です。Aと同様、アクセスキーの厳重な管理やローテーションが必要となります。

Cは適切な選択肢です。EC2からDynamoDBへのアクセスでは、IAMユーザーのアクセスキーではなく、EC2に設定したIAMロールによる一時的セキュリティ認証情報を利用することで、アクセスキーの厳重な管理やローテーションが必要となり、より安全なアクセスを実現できます。

Dは不適切な選択肢です。VPCエンドポイントを使用したDynamoDBへのアクセスにより、アクセス経路を安全にはできますが、DynamoDBのアクセス権を制御することはできません。

Q18 答え B

数百万規模のユーザーからのアクセスが想定される場合、データベースとしてはスケーラビリティの観点で、RDSではなくDynamoDBを選びます。

Aは不適切な選択肢です。RDSを利用し、前段にアプリケーションを経由して

アクセスする場合には、EC2をスケールするように管理する必要があり、費用対効果の面で課題があります。また、500万人のユーザーが定期的にアクセスするには、RDSのスケーラビリティでは厳しいといえます。

Bは適切な選択肢です。DynamoDBテーブルの項目と属性に対し、ウェブIDフェデレーションで認証された外部ユーザーIDに基づいたアクセス制限をかけることで、ユーザーは自分自身に必要な属性にのみアクセスできます。モバイルアプリケーションから直接DynamoDBにアクセスすることで、十分にスケールできます。

Cは不適切な選択肢です。Aと同様、スケーラビリティの面でRDSは厳しいといえます。

Dは最適な選択肢ではありません。50KBのサイズはDynamoDBに収まるため、S3にユーザー情報を保存し、DynamoDBにS3へのポインタを設定するようなオーバーヘッドを実装する必要はありません。

Q19 答え A、B、C、D、E

EBSは、暗号化ボリュームを使用することですべてのデータを暗号化できます。Glacier、DynamoDB、Storage Gateway、SQSは、S3と同様にサーバーサイドで暗号化が可能です。インスタンスストアは暗号化に対応していません。

Q20 答え B、C

Aは不適切な選択肢です。Directory Service Simple ADは、既存のADと連携できません。

BとCは適切な選択肢です。Directory Service AD Connectorは、既存のオンプレミスにあるADに認証をリダイレクトし、IAMロールで設定されたアクセス権限をADユーザーに与えてAWS管理コンソールにアクセスさせることができます。

DとEは不適切な選択肢です。IAMユーザーやグループだけでは、ADと連携することができません。

Q21 答え A、B、D

AとBは適切な選択肢です。EC2インスタンスにCloudWatchエージェントをインストールすることで、カスタムログファイルをCloudWatch Logsに配信できます。

Cは不適切な選択肢です。Kinesis Firehoseでは、CloudWatchへのログの配信やSNSによるアラーム設定ができません。

Dは適切な選択肢です。CloudWatch Logsでメトリクスフィルタを設定して監視する文字列を指定し、アラームを設定することで、SNSからアラートを通知できます。

Q22 答え A、C、F

- Aは適切な選択肢です。旧管理者のパスワードは使用しません。
- Bは不適切な選択肢です。AWSコンソールへのログインにIPアドレスの制限をかけることは可能ですが（利用できる機能に一部制限があり）、それだけでは不十分です。
- Cは適切な選択肢です。旧管理者のIAMユーザーは削除します。
- Dは不適切な選択肢です。AWSアカウント自体を削除すると、当該AWSアカウントで動作しているEC2インスタンスなどのAWSサービスがすべて削除されてしまいます。
- Eは不適切な選択肢です。EC2にアタッチされているロールは一時的セキュリティ認証情報を利用するため、変更する必要はありません。
- Fは適切な選択肢です。ルートユーザーのアクセスキーの使用は、セキュリティ上の理由から推奨されていません。

Q23 答え B、C、E

- Aは不適切な選択肢です。AWS Configでは、ユーザーのアクティビティログを取得できません。
- Bは適切な選択肢です。CloudTrailを使用することで、AWSアクティビティの証跡ログを取得できます。
- CとEは適切な選択肢です。CloudTrailからCloudWatch Logsへのログ転送を有効化すると、ログに記録されたAWSイベントからメトリクスフィルタによってアラームを作成できます。アラームでSNSのアクションを定義します。
- Dは不適切な選択肢です。このケースの場合、SQSは利用しません。

Q24 答え A、C

- Aは適切な選択肢です。IAMのユーザー一覧では、アクセスキーの古さやMFAの有効／無効を確認できます。
- Bは不適切な選択肢です。CloudTrailは、マネジメントコンソールへのアクセスやAPIアクセスを記録します。
- Cは適切な選択肢です。AWS Configルールにおいて、IAMユーザーはMFAを有効とするルールとアクセスキーーローテーションは最大60日とするルールを作成することにより、ルールに準拠していないIAMユーザーを抽出できます。
- Dは不適切な選択肢です。CloudWatchでは検出できません。
- Eは不適切な選択肢です。Trusted Advisorでは、IAMユーザーのMFAが有効かどうかを調べられません。アクセスキーについても、90日以上ローテーションしていないIAMユーザーは調べられますか、60日は調べられません。

Q25 答え B

- Aは不適切な選択肢です。Elastic Beanstalkでは、AWSに設定されたWebア

プリケーションの実行環境を展開できますが、CloudFormationでは問題文にあるようなより広範囲のリソースを構成できます。また、Elastic Beanstalkは、CloudFormationが展開する1つのリソースです。

Bは適切な選択肢です。CloudFormationを使用して標準化したAWSリソース構成のテンプレートを作成することで、同一構成のシステムを自動展開できます。

Cは不適切な選択肢です。Configは構成管理を行うサービスです。

Dは不適切な選択肢です。VPC全体やAWSアカウント全体のコピーを行うことはできません。

Eは不適切な選択肢です。

Q26 答え A、B

Aは適切な選択肢です。EKSにおけるコンテナ管理サービスはKubernetesです。

Bは適切な選択肢です。ECSにおけるコンテナ管理サービスはAWSの独自のサービスです。

Cは不適切な選択肢です。Dockerはコンテナ仮想化技術そのものです。

Dは不適切な選択肢です。Docker SwarmはDocker社のコンテナ管理サービスです。

Q27 答え B、C

Aは不適切な選択肢です。EKSはコントロールプレーンです。

BとCは適切な選択肢です。ECSのデータプレーンはFargateとEC2をサポートしています。一方、EKSはEC2のみのサポートです。

Dは不適切な選択肢です。EBSはストレージサービスです。

Q28 答え A

Aは適切な選択肢です。S3にファイルをアップロードするイベントをトリガーとして短時間の処理を行うにはLambda関数が適しています。

Bは不適切な選択肢です。頻度が一定でない動的な処理のため、EC2インスタンスによる構成よりもプログラムの稼働量に課金されるLambdaが適しています。

Cは不適切な選択肢です。ファイルの保存先としては、Kinesis Data Streamsよりも低コストで永続的に保存できるS3のほうが優れています。

Dは最適な選択肢ではありません。静的ウェブホスティングを用いてアップロードサイトを用意するのはよいソリューションですが、縮小処理について具体的な記載がないため、Aのほうがより適切といえます。

Q29 答え B

Aは不適切な選択肢です。CloudWatch AlarmはCloudWatchの通知機能であり、

収集されたログをフィルタする機能はありません。

Bは適切な選択肢です。ログメッセージを検出して加工する場合には、CloudWatch Logs から Lambda 関数を実行し、Lambda 関数でメッセージの加工処理を行います。加工したメッセージは、Lambda 関数から SNS を利用してプッシュ通知します。

Cは不適切な選択肢です。Aと同様の理由です。

Dは不適切な選択肢です。メッセージを加工する処理は、EC2よりも Lambda のほうがコスト面と開発面で効率的に構成できます。

Q30 答え B

Aは不適切な選択肢です。S3にデータを格納するのは、大量のリクエストに対応できる応答性の要件に適していません。大量のリクエストが見込まれるサービスのデータベースは、S3以外のデータベースを選択します。

Bは適切な選択肢です。月に数回しか稼働せず、稼働するときは大量のトラフィックが予想される動的なシステム構成が要件です。Lambda 関数は、プログラムの稼働量での従量課金のため、この場合の要件に適しています。

Cは不適切な選択肢です。EC2 インスタンスによる構成は、継続的に課金されるためコスト効率が悪く、要件に適していません。リザーブドインスタンスを利用したとしても、Lambda のほうが費用対効果が高いといえます。RDS の利用可否については、アクセス数に依存するため、明確に判断できませんが、EC2 を選択している時点でこの選択肢は除外します。

Dは不適切な選択肢です。EC2 インスタンスによる構成は、継続的に課金されるためコスト効率が悪く、要件に適していません。また、S3 にデータを格納するのは、大量のリクエストに対応できる応答性の要件に適していません。大量のリクエストが見込まれるサービスのデータベースについては、S3以外のデータベースを選択します。

Q31 答え B

Aは不適切な選択肢です。保管型ボリュームゲートウェイは、キャッシュ型ボリュームゲートウェイと同じくスナップショットを S3 に保存しますが、データのプライマリコピーはオンプレミスに存在します。

Bは適切な選択肢です。キャッシュ型ボリュームゲートウェイは問題文にあるとおりです。よく使われるデータのみキャッシュとしてオンプレミスに保存します。

Cは不適切な選択肢です。テープゲートウェイは、仮想テープライブラリ対応バックアップソフトウェアを利用し、Storage gateway 経由でデータを S3 に保存します。

Dは不適切な選択肢です。ファイルゲートウェイは、S3 をオンプレミスの NFS 共有ファイルシステムのバックエンドストレージとして利用します。

Q32 答え C

Aは不適切な選択肢です。もしこの設定が間違っているのであれば、ほかのインスタンスもインターネットに対するアクセスが不可能となります。

Bは不適切な選択肢です。Aと同様です。

Cは適切な選択肢です。サブネット内のインスタンスがインターネットと通信できるようにするにはパブリックからアクセスできるIPアドレスが必要です。選択肢の中では、CのElastic IP アドレスが該当します。

Dは不適切な選択肢です。Aと同様です。

Q33 答え A

Aが適切な選択肢です。システム管理で一般的に用いられる構成です。公開用と管理用でネットワークインターフェイスとサブネットを分けるのがセキュアな方法です。管理用ネットワークインターフェイスを設けることを「バックネット」と呼びます。

Q34 答え B

Aは不適切な選択肢です。インターネットゲートウェイにはルートテーブルを設定できません。ルートテーブルはサブネットに設定します。

Bは適切な選択肢です。インターネットから直接DBにアクセスできるような設定は、セキュリティリスクとなります。パブリックサブネット内に構築したEC2を経由してDBにアクセスするのが、よりセキュアな構成です。

Cは最適な選択肢ではありません。この情報だけでは、インターネットからEC2はアクセスできると想定できますが、EC2からRDSに対するアクセスの可否が不明です。

Dは不適切な選択肢です。プライベートサブネットはインターネットからアクセスできないため、プライベートサブネットにEC2を構築する場合、そのEC2はインターネットから直接アクセスできなくなります。EC2はパブリックサブネットに配置すべきです。

Q35 答え A

Aは適切な選択肢です。外部からインターネット接続を行わず、内部からのみインターネット接続を行う場合は、パブリックサブネットでNATゲートウェイを利用します。NATゲートウェイのルーティング設定としては、パブリックサブネットのルートテーブルで、インターネットゲートウェイへのルーティングの設定を行います。

Bは最適な選択肢ではありません。EC2を用いてNATを構築することもできますが、マネジドサービスであるNATゲートウェイの利用が推奨されます。

Cは不適切な選択肢です。ワークフローサーバーは社内向けのため、プライベートサブネットに配置されていることが想定されます。そのため、インターネッ

トゲートウェイではなく、NATゲートウェイへのルーティングを設定すべきです。

Dは最適な選択肢ではありません。Cと同様です。ただし、実際にはVPCから仮想プライベートゲートウェイを経由してオンプレミスへ行き、さらにそこからインターネットにアクセスするケースもあります。今回はそこまでの情報が問題文に記載されていないため、確実にワークフローサーバーがインターネットとアクセスできるAもしくはBを選択します。

Q36 答え C

Aは不適切な選択肢です。「再起動後にIPアドレスにアクセスできなくなった」ということから、再起動前にはアクセスができており、セキュリティグループには問題がなかったことがわかるためです。

Bは不適切な選択肢です。パブリックサブネット内のEC2インスタンスからインターネットへのアクセスには、インターネットゲートウェイへのルーティング設定が必要ですが、これがないからといって、インターネットからEC2インスタンスにアクセスできない現象の理由とはなりません。

Cは適切な選択肢です。EC2を再起動するたびにパブリックIPアドレスは変更されます。したがって、外部から特定のIPアドレスにアクセスするためにはEIPの設定が必要です。

Dは不適切な選択肢です。NATゲートウェイはパブリックサブネットに配置され、プライベートサブネット内のEC2インスタンスはこれを経由して、インターネットにアクセスを行います。今回の問題とは関係がありません。

Q37 答え C、D

Aは不適切な選択肢です。上限緩和申請はベーシック／開発者／ビジネス／エンタープライズのすべてのサポートプランで利用できます。

Bは不適切な選択肢です。この中で無償のサポートプランはベーシックだけです。

Cは適切な選択肢です。Trusted Advisorのすべてのサービスを利用できるのはビジネスとエンタープライズのみとなります。一部のサービスはそのほかのプランでも利用できます。

Dは適切な選択肢です。問い合わせの際、組織に特有のユースケースや要件を考慮したアドバイスを必要とする場合は、ビジネスもしくはエンタープライズが必要です。

Q38 答え A

Aは適切な選択肢です。Auto Scalingでグループを作成した場合、Desired Capacityの数だけインスタンスが生成されます。この設問の場合は、Desired Capacityを12に設定し、3つのアベイラビリティゾーンに4個ずつのEC2インスタンスを実行させます。仮に1つのアベイラビリティゾーンが停止し

ても、残りの8個のインスタンスは稼働しているので、最小限必要な8個のEC2インスタンスの稼働を維持できます。

その他の選択肢は上記の考え方から、要件を満たすことはできません。

Q39 答え B

Bは適切な選択肢です。その他の選択肢は用語を入れ替えたものです。

Q40 答え A、D

Aは適切な選択肢です。インターネットゲートウェイがなければ、アクセスはできません。

Bは不適切な選択肢です。NATゲートウェイは、たとえばプライベートサブネットに配置されたEC2インスタンスがNATゲートウェイを経由してインターネットにアクセスするためにパブリックサブネットに配置されます。

Cは不適切な選択肢です。Direct ConnectはオンプレミスとAWSの間の専用線の接続サービスです。

Dは適切な選択肢です。

Q41 答え B

Aは不適切な選択肢です。ALBの解説です。

Bは適切な選択肢です。NLBの解説です。

Cは不適切な選択肢です。CLBの解説です。

Dは不適切な選択肢です。「ロードバランサーのヘルスチェックは、ターゲットのインスタンスの正常性や異常の検知を行うが、ターゲットのインスタンスそのものを再起動したり、ほかのインスタンスをターゲットに自動登録するといった回復機能を持っていない」が正しい解説です。回復機能はAuto Scalingの機能です。

Q42 答え A

Aが適切な選択肢です。アクセスが集中する日時が予測できる場合は、スケジュールスケーリングが最も適しています。

Q43 答え E

Eが適切な選択肢です。Auto Scalingは、EC2以外にEC2スポットフリート、ECS、DynamoDB、Auroraにおいて利用できます。

Q44 答え B

Bが適切な選択肢です。動的スケーリングのうち、特定のメトリクスのターゲット値に基づいてインスタンスを増減するスケーリング方式は、Target tracking scalingです。

Q45 答え D

Dが適切な選択肢です。簡易で低成本のSorryページを構築するという要件から、コンテンツサーバーとしてS3静的ウェブサイトホスティングを選定します。Sorryページは、常時アクセスされる性質のものではなく、コンテンツサイズも小さいです。また、障害対応の要件であることから、高い可用性も必要となるため、S3静的ウェブサイトホスティングが適切です。Webサイトで障害が発生した際、S3静的ウェブサイトにフェイルオーバーするように、Route 53のルーティングポリシーを「Failover」にしておく必要があります。

これらの観点から、A、B、Cは不適切な選択肢となります。

Q46 答え A

Aは適切な選択肢です。社内向けインターネットサイトであるため、プライベートホストゾーンを構成します。また、エンドポイントであるELBロードバランサーにTLDでアクセスさせるという要件があるため（Zone Apex）、ELBロードバランサーのDNS名にエイリアスレコードを作成します。

Bは不適切な選択肢です。リクエストが最初に到達するELBロードバランサーのDNS名に対して、エイリアスレコードを作成することが必要です。

Cは不適切な選択肢です。インターネットのため、パブリックホストゾーンではなく、プライベートホストゾーンを構成します。

Dは不適切な選択肢です。Zone Apexは、CNAMEレコードではなく、エイリアスレコードを作成します。

Q47 答え D

Dが適切な選択肢です。サーバーごとに性能の偏りがある場合などに、それぞれのサーバーに加重をかけてトラフィックを分散させるには、加重ルーティングを構成します。D以外の選択肢のルーティングポリシーについては、本書を参照してください。

Q48 答え D

Aは不適切な選択肢です。最もコストの高いソリューションとなります。

Bは不適切な選択肢です。インターネットVPNを引くよりも、既存の専用線にVIFを構成するほうがコストは安くなります。

Dは適切な選択肢です。プロジェクトで独立したネットワーク環境が必要であり、最も低いコストで簡易に実現するという要件であるため、現在利用しているDirect Connect接続に対してVIFを構成します。また、独立したネットワーク環境という要件から、Cは不適切な選択肢となります。

Q49 答え B

Aは不適切な選択肢です。インターネットVPNは、経路上のほかのネットワークの影響を受けやすく、インターネットの範囲における障害調査が困難な場

合があります。

Bは適切な選択肢です。安定した通信と万が一の障害時の迅速な対応および低コストのネットワーク要件から、Direct Connect接続を構成します。また、2Gbpsの帯域を必要としていることから、共有型で必要な帯域を利用します。

Cは不適切な選択肢です。占有型では1Gbpsか10Gbpsの帯域のみ利用可能となります。2Gbpsの帯域を用意することができません。

Dは不適切な選択肢です。VIFは必ず設定します。この設問では、占有型か共有型かが問題になります。

Q50 答え C

AとBは不適切な選択肢です。同じコンテンツを各リージョンに用意するよりは、CloudFrontを利用すべきです。

Cは適切な選択肢です。Webサイトをグローバルに効率よく展開するには、CloudFrontが適しています。CloudFrontの位置情報DBにより、グローバルに展開されているCloudFrontのエッジサーバーにトラフィックが適切に分散されます。また、キャッシング機能により、オリジンサーバー(コンテンツサーバー)の負荷を軽減できます。

Dは不適切な選択肢です。同じコンテンツを各リージョンに用意するよりは、CloudFrontを利用すべきです。

Q51 答え D

Dが適切な選択肢です。クライアントとエッジサーバー間の通信を暗号化することが要件であるため、BまたはDが正解の候補となります。独自ドメイン名を利用するため、CloudFrontにX.509 PEM形式のSSL証明書をインポートし、暗号化通信を構成します。BのデフォルトのSSL証明書では、独自ドメイン名を利用できません。

Q52 答え C

Aは不適切な選択肢です。EC2インスタンスにデータベースを導入する場合には、OSの設定やデータベースの導入作業が必要となります。

Bは不適切な選択肢です。RDS for MySQLは、CのAuroraと比較した場合、フェイルオーバー時に数分間のデータを損失する可能性があるという短所があります。

Cは適切な選択肢です。高可用性と応答性の要件を最も簡単に満たす構成は、Auroraによるデータベースです。

Dは不適切な選択肢です。DynamoDBはNoSQLのため、ミッションクリティカルなシステムで必要とされるレベルのトランザクション処理をサポートしていません。

Q53 答え B

Bは適切な選択肢です。RDSをバックアップからリストアする場合は、新しいプライマリDBインスタンス上にスナップショットを復元したあと、エンドポイントを新しいプライマリDBインスタンスに書き換えます。

A、C、Dは不適切な選択肢です。

Q54 答え C

Aは不適切な選択肢です。トランザクションログからは今回の要件であるレポートを作成できません。

Bは不適切な選択肢です。スタンバイDBインスタンスにはアクセスができません。

Cは適切な選択肢です。データベースに与える影響を最小限にしてレポートを作成するには、リードレプリカを構成し、リードレプリカにクエリを行うことでレポートを生成する仕組みを構成します。プライマリDBインスタンスやスタンバイDBインスタンスに直接クエリを行うと、レスポンスに影響が生じることがあります。

Dは不適切な選択肢です。ElastiCacheは、一時的なデータのみが格納されているため、アクセスログのレポートを生成する要件には適していません。

Q55 答え D

Aは不適切な選択肢です。EC2インスタンスのコストを下げるための手段の1つです。

Bは不適切な選択肢です。EC2インスタンスのコストを下げるための手段の1つです。

Cは不適切な選択肢です。CloudTrailは、コスト削減の手段ではなく、ユーザーの操作やAPIアクセスを記録するためのサービスです。

Dは適切な選択肢です。AWS上でリソースの使い方に問題があり、コストが必要以上にかかっている場合は、まずTrusted Advisorを確認します。選択肢にはありませんが、Cost Explorerも有効な手段です。現在のサービスごとのコストとその将来予測を得ることができます。

Q56 答え A

Aが適切な選択肢です。FIFOキューでは、メッセージが送信された順序のとおりに配信され、1回限りで配信されることが保証されています。なお、標準キューでは、配信順序がベストエフォートであり、1回以上で配信されます。

Q57 答え A、B、D、E

SNSは、HTTP/S、Eメール、SQS、Mobile Push、SMS、Lambdaに対応しています。

Q58 答え B、C

Aは不適切な選択肢です。POP3はPost Office Protocol 3の略で、メールサーバーから自分のメールを取り出すときに使用するメール受信用のプロトコルです。

Bは適切な選択肢です。HTTP REST APIはアプリケーションから直接メールを送信する場合に利用します。

Cは適切な選択肢です。SMTPエンドポイントは、SMTPを前提としてプログラムから直接利用する場合に利用します。

Dは不適切な選択肢です。JSONはJavaScript Object Notationの略で、データ交換の形式です。

Q59 答え D

Aは最適な選択肢ではありません。当然ながらRedshiftで分析が可能ですが、コスト効率を考慮した場合、DのRedshift Spectrumを選択します。S3上に置いたファイルを外部テーブルとして利用します。

Bは不適切な選択肢です。DynamoDBは、Webのセッション情報、ストレージのインデックスなどのメタデータ、ユーザーIDの保存に適しており、通常、分析用途には利用しません。

Cは不適切な選択肢です。分析のためのデータを保存する用途としては可能ですが、ペタバイトまでのデータの保存ができません。

Dは適切な選択肢です。巨大なデータを扱うデータ分析には、Redshiftデータベースが適しています。このケースのようにデータ容量が大規模になる場合、コンピューティングの追加によってRedshiftのコスト効率が低下するので、それを避けるためにRedshift Spectrumを選択します。

Q60 答え A

Aが適切な選択肢です。Redshiftのコンピューティングノードの障害は自動的に検知され、代替ノードがプロビジョニングされます。ほかのノードからデータが複製され、自動的にクラスターに構成されてサービスが継続されます。ただし、代替ノードが復旧されるまでは更新できることに注意が必要です。

B、C、Dは不適切な選択肢です。手動による操作が入っています。

Q61 答え A、C、D

A、C、Dは適切な選択肢です。DynamoDBは、Webのセッション情報、ストレージのインデックスなどのメタデータ、ユーザーIDの保存に適しています。

Bは不適切な選択肢です。バイナリーデータや大量のデータの保存には適していません。この場合、S3が適しています。

Eは不適切な選択肢です。この場合、S3 Glacierが適しています。

Q62 答え B、D、E

B、D、Eは適切な選択肢です。Redis用ElastiCacheは次のケースでの利用に適しています。

- ・データ型：複雑
- ・暗号化：あり
- ・コンプライアンス認証：あり
- ・マルチスレッド：なし
- ・高可用性：あり
- ・自動フェイルオーバー：必須
- ・バックアップと復元：あり

なお、Memcached用ElastiCacheが適しているのはAとCです。扱うデータ型／暗号化／高可用性構成／コンプライアンスなどへの対応が不要のシンプルな利用に適しています。

Q63 答え C

Aは不適切な選択肢です。ElastiCacheはアプリケーションが高速なI/Oを必要とする場合に利用するキャッシュサービスです。

Bは最適な選択肢ではありません。ユーザー情報は構造化もしくは半構造化されているケースが多いため、EBSよりはデータベースのほうがのちほど活用しやすいといえます。

Cは適切な選択肢です。データによって属性数が異なっていても保存しやすい、NoSQLのKey-Value型データベースであるDynamoDBが適しています。また、DynamoDBは書き込みと同時に複数のアベイラビリティゾーンに複製されるため、耐障害性にも優れています。一般的に、DynamoDBは、Webのセッション情報、ストレージのインデックスなどのメタデータ、ユーザーIDをはじめとするユーザーデータの保存に適しています。

Dは最適な選択肢ではありません。Bと同じ理由に加え、I/Oが高くなる可能性を考えると、S3よりもDynamoDBのほうが適しています。

Q64 答え B

Bは適切な選択肢です。

AはCloudFormationデザイナー、CはElastic Beanstalk、DはCloudFormationの説明です。

Q65 答え C

Aは不適切な選択肢です。プライベートIPアドレスの付与では解決しません。

Bは不適切な選択肢です。NATゲートウェイはパブリックサブネットに配置されます。プライベートサブネットにあるEC2インスタンスなどのリソースが、NATゲートウェイ経由でインターネットにアクセスします。NATゲートウェ

イの有無は今回の問題には関係がありません。

Cは適切な選択肢です。インターネットからのアクセスには、パブリックIPアドレスが必要です。

Dは不適切な選択肢です。この設定はパブリックサブネットのEC2インスタンスがインターネットにアクセスするために必要となります。今回の問題には関係がありません。選択肢中のルートテーブルの設定も同様です。