

1) ある企業は、複数のアベイラビリティゾーンにまたがる VPC 内で、パブリック側の 3 層ウェブアプリケーションを実行しています。プライベートサブネットで行われているアプリケーション層の Amazon EC2 インスタンスでは、インターネットからソフトウェアパッチをダウンロードする必要があります。ただし、EC2 インスタンスにインターネットから直接アクセスすることはできません。

EC2 インスタンスが必要なパッチをダウンロードできるようにするために実行すべきアクションはどれですか。
(2 つ選択)

- A) パブリックサブネットに NAT ゲートウェイを構成する。
- B) インターネットトラフィック用の NAT ゲートウェイへのルートがあるカスタムルートテーブルを定義し、アプリケーション層のプライベートサブネットに関連付ける。
- C) Elastic IP アドレスを EC2 インスタンスに割り当てる。
- D) インターネットトラフィック用のインターネットゲートウェイへのルートがあるカスタムルートテーブルを定義し、アプリケーション層のプライベートサブネットに関連付ける。
- E) プライベートサブネットに NAT インスタンスを設定する。

2) あるソリューションアーキテクトは、会社が 2 週間一時休業する間に実行する必要のない Amazon EC2 インスタンスのコストを節約するため、ソリューションを設計したいと考えています。EC2 インスタンスで実行されているアプリケーションは、インスタンスが動作を再開するときに必要なデータをインスタンスメモリに格納します。

EC2 インスタンスをシャットダウンして再開するために、ソリューションアーキテクトが推奨すべきアプローチはどれですか。

- A) インスタンスストアボリュームにデータを格納するようにアプリケーションを変更する。ボリュームを再起動中に、再接続する。
- B) EC2 インスタンスを停止する前に、インスタンスのスナップショットを作成する。インスタンスの再起動後に、スナップショットを復元する。
- C) 休止状態が有効になっている EC2 インスタンスでアプリケーションを実行する。会社が 2 週間の一時休業に入る前に、インスタンスを休止状態にする。
- D) EC2 インスタンスを停止する前に、各インスタンスのアベイラビリティゾーンをメモしておく。2 週間の一時休業が終わったら、同じアベイラビリティゾーンでインスタンスを再起動する。

3) ある企業は、VPC において、Amazon EC2 インスタンスでモニタリングアプリケーションを実行する予定です。EC2 インスタンスへの接続は、そのプライベート IPv4 アドレスを使用して行われます。ソリューションアーキテクトは、アプリケーションに障害が発生して到達不能になった場合に、トラフィックをスタンバイ EC2 インスタンスに迅速に誘導できるソリューションを設計する必要があります。

これらの要件を満たすアプローチはどれですか。

- A) プライベート IP アドレスのリスナーで構成された Application Load Balancer をデプロイし、ロードバランサーにプライマリ EC2 インスタンスを登録する。障害発生時に、インスタンスを登録解除して、スタンバイ EC2 インスタンスを登録する。
- B) カスタム DHCP オプションセットを構成する。プライマリ EC2 インスタンスで障害が発生したときに、同じプライベート IP アドレスをスタンバイ EC2 インスタンスに割り当てるように DHCP を設定する。
- C) プライベート IP アドレスで設定された EC2 インスタンスに、セカンダリ Elastic Network Interface を添付する。プライマリ EC2 インスタンスが到達不能になった場合は、ネットワークインターフェイスをスタンバイ EC2 インスタンスに移動する。
- D) Elastic IP アドレスをプライマリ EC2 インスタンスのネットワークインターフェイスに関連付ける。障害発生時に Elastic IP とプライマリインスタンスの関連付けを解除し、スタンバイ EC2 インスタンスに関連付ける。

4) ある分析会社は、ユーザーにウェブ解析サービスを提供する予定です。このサービスでは、ユーザーのウェブページに、同社の Amazon S3 バケットに対して認証済み GET リクエストを行う JavaScript スクリプトが含まれている必要があります。

スクリプトを正常に実行するため、ソリューションアーキテクトが行うべきことは何ですか。

- A) S3 バケットでクロスオリジンリソース共有 (CORS) を有効にする。
- B) S3 バケットで S3 バージョニングを有効にする。
- C) ユーザーにスクリプトの署名付き URL を提供する。
- D) パブリック実行権限を許可するよう、S3 バケットポリシーを設定する。

5) ある企業のセキュリティチームは、クラウドに保存されているすべてのデータを、オンプレミスに保存された暗号化キーを使用して、保管時は常に暗号化する必要があります。

これらの要件を満たす暗号化オプションはどれですか。（2 つ選択）

- A) Amazon S3 で管理された暗号キー（SSE-S3）でサーバー側の暗号化を使用する。
- B) AWS KMS で管理された暗号化キー（SSE-KMS）でサーバー側の暗号化を使用する。
- C) 顧客提供の暗号化キー（SSE-C）でサーバー側の暗号化を使用する。
- D) クライアント側の暗号化を使用して、保存時の暗号化を行う。
- E) Amazon S3 イベントによって呼び出される AWS Lambda 関数を使用し、顧客のキーを使用してデータを暗号化する。

6) ある企業は、データ処理ワークロードを実行するために、Amazon EC2 リザーブドインスタンスを使用しています。毎夜のジョブは通常、実行に 7 時間かかり、10 時間以内に終了する必要があります。同社は、毎月末に需要が一時的に増加するため、現在のリソースの容量では、ジョブが制限時間以内に終わらないと予想しています。いったん開始された処理ジョブは完了するまで中断できません。同社は、できる限りコスト効率よくリソース容量を提供できるソリューションを実装したいと考えています。

これを達成するために、ソリューションアーキテクトは何をすべきでしょうか。

- A) 需要が高まる期間中にオンデマンドインスタンスをデプロイする。
- B) 追加のインスタンス用に 2 つ目の EC2 予約を作成する。
- C) 需要が高まる期間中にスポットインスタンスをデプロイする。
- D) ワークロードの増加をサポートするために、EC2 予約の EC2 インスタンスのサイズを増やす。

7) ある企業は、毎週生放送されるテレビ番組のオンライン投票システムを運用しています。放送中、Auto Scaling グループで実行される Amazon EC2 インスタンスのフロントエンドフリートに、ユーザーから数十万という票が送られてきます。EC2 インスタンスは Amazon RDS データベースに票を書き込みます。しかし、データベースは EC2 インスタンスからのリクエストに迅速に対応することができません。ソリューションアーキテクトは、最も効率的な方法で、ダウンタイムなしに票を処理するソリューションを設計する必要があります。

これらの要件を満たすのはどのソリューションですか。

- A) フロントエンドアプリケーションを AWS Lambda に移行する。Amazon API Gateway を使用して、ユーザーリクエストを Lambda 関数にルートする。
- B) データベースをマルチ AZ 配置に変換することで、データベースを水平方向にスケールする。プライマリとセカンダリの両方の DB インスタンスに書き込むよう、フロントエンドアプリケーションを設定する。
- C) Amazon Simple Queue Service (Amazon SQS) キューに票を送信するよう、フロントエンドアプリケーションを設定する。SQS キューを読み取り、投票情報をデータベースに書き込むよう、ワーカーインスタンスをプロビジョニングする。
- D) Amazon EventBridge (Amazon CloudWatch Events) を使用してスケジュールされたイベントを作成し、投票期間中、大規模なメモリ最適化インスタンスでデータベースを再プロビジョニングする。投票が終了したら、サイズの小さいインスタンスを使用するよう、データベースを再プロビジョニングする。

8) ある企業には、パブリックサブネットとプライベートサブネットで実行される 2 層アプリケーションアーキテクチャがあります。ウェブアプリケーションを実行している Amazon EC2 インスタンスはパブリックサブネットにあり、データベースの EC2 インスタンスはプライベートサブネットで実行されています。ウェブアプリケーションインスタンスとデータベースは単一のアベイラビリティゾーン (AZ) で実行されています。

このアーキテクチャで高可用性を実現するために、ソリューションアーキテクトが取るべきステップの組み合わせはどれですか。(2 つ選択)

- A) 新しいパブリックサブネットとプライベートサブネットを同一の AZ に作成する。
- B) 複数の AZ にまたがる Amazon EC2 Auto Scaling グループと Application Load Balancer をウェブアプリケーションインスタンス用に作成する。
- C) 既存のウェブアプリケーションインスタンスを Application Load Balancer の背後にある Auto Scaling グループに追加する。
- D) 新しいパブリックサブネットとプライベートサブネットを新しい AZ に作成する。新しい AZ にあるパブリックサブネットに EC2 インスタンスを使用してデータベースを作成する。古いデータベースの内容を新しいデータベースに移行する。
- E) 新しいパブリックサブネットとプライベートサブネットを同一の VPC 内の、それぞれ新しい AZ に作成する。Amazon RDS マルチ AZ DB インスタンスをプライベートサブネットに作成する。古いデータベースの内容を新しい DB インスタンスに移行する。

9) ある Web サイトでは、毎日正午に大量のトラフィックを受信するカスタムウェブアプリケーションが実行されています。ユーザーは毎日新しい写真やコンテンツをアップロードしていますが、タイムアウトについて苦情を寄せています。このアーキテクチャでは Amazon EC2 Auto Scaling グループが使用され、起動時にアプリケーションが起動してからユーザーのリクエストに応答するまでに 1 分かかります。

変化するトラフィックに的確に対応するために、ソリューションアーキテクトはアーキテクチャをどのように再設計すべきでしょうか。

- A) Network Load Balancer をスロースタートに設定する。
- B) Amazon ElastiCache for Redis を設定し、EC2 インスタンスからの直接リクエストをオフロードする。
- C) EC2 インスタンスのウォームアップ条件で Auto Scaling ステップスケーリングポリシーを設定する。
- D) Application Load Balancer をオリジンとして使用するよう、Amazon CloudFront を設定する。

10) AWS で実行されているあるアプリケーションは、そのデータベースに Amazon Aurora マルチ AZ DB クラスターデプロイメントを使用します。あるソリューションアーキテクトが、パフォーマンスメトリクスを評価したところ、データベースの読み取りによって I/O が高くなり、データベースに対する書き込み要求のレイテンシーが増大していることを発見しました。

ソリューションアーキテクトは、読み取り要求と書き込み要求を分けるために何をすべきですか。

- A) Aurora データベースでリードスルーキャッシュを有効にする。
- B) マルチ AZ スタンバイインスタンスから読み取るよう、アプリケーションを更新する。
- C) Aurora レプリカを作成し、適切なエンドポイントを使用するようにアプリケーションを変更する。
- D) 2 つ目の Aurora データベースを作成し、リードレプリカとしてプライマリデータベースにリンクする。

解答

- 1) A、B - [NAT ゲートウェイ](#)は、プライベートサブネット内の EC2 インスタンスからインターネットや他の AWS のサービスにトラフィックを転送し、その応答をインスタンスに送り返します。NAT ゲートウェイを作成した後、プライベートサブネットのルートテーブルを更新して、インターネットトラフィックを NAT ゲートウェイに向ける必要があります。
- 2) C - EC2 インスタンスを[休止状態にする](#)ことで、インスタンスメモリの内容が Amazon Elastic Block Store (Amazon EBS) ルートボリュームに保存されます。インスタンスが再起動すると、インスタンスメモリの内容が再ロードされます。
- 3) C - [セカンダリ Elastic Network Interface](#) を EC2 インスタンスに追加できます。プライマリネットワークインターフェイスをインスタンスからデタッチすることはできませんが、セカンダリネットワークインターフェイスをデタッチして別の EC2 インスタンスに添付することはできます。
- 4) A - ウェブブラウザが、Web ページと異なるドメイン名を持つサーバーから作成されたスクリプトの実行をブロックします。[Amazon S3 を CORS で設定し](#)、スクリプトの実行を許可する HTTP ヘッダーを送信できます。
- 5) C、D - [顧客が提供するキー \(SSE-C\) を使用したサーバー側の暗号化](#)を使用すると、Amazon S3 は PUT リクエストで提供される暗号化キーを使用してオブジェクトサーバー側を暗号化できます。Amazon S3 がオブジェクトを復号化するには、GET リクエストでも同じキーを指定する必要があります。顧客には、Amazon S3 にアップロードする前にクライアント側でデータを暗号化するオプションもあり、この場合、ダウンロードしてからデータを復号化できます。AWS ソフトウェア開発キット (SDKs) は、プロセスを合理化する S3 暗号化クライアントを提供します。
- 6) A - [スポットインスタンス](#)は最もコストのかからないオプションですが、中断できないジョブや一定期間内に完了しなければならないジョブには適していません。[オンデマンドインスタンス](#)では、実行秒数に対して請求が行われます。
- 7) C - 票の取り込みをデータベースから[切り離し](#)、投票システムがデータベースへの書き込みを待たずに投票の処理を継続できるようにします。[SQS キュー](#)から読み取る専用ワーカーを追加し、制御可能な速度で票をデータベースに入力できるようにします。票はデータベースが処理可能な速度でデータベースに追加されますが、票が失われることはありません。
- 8) B、E - 新しいサブネットを新しいアベイラビリティゾーン (AZ) に作成し、冗長ネットワークを実現します。[ロードバランサーの背後にある 2 つの AZ にインスタンスの Auto Scaling グループ](#)を作成し、ウェブアプリケーションの高可用性を確保し、2 つのパブリック AZ 間でウェブトラフィックを再分散させます。2 つのプライベートサブネットに RDS DB インスタンスを作成し、[データベース層の高可用性](#)も実現します。

9) C – 現在の設定では、新しい EC2 インスタンスはトランザクションに応答する前に稼働状態になります。これにより、インスタンスの規模が過度に拡大される可能性もあります。[ステップスケーリングポリシー](#)では、新しく起動されたインスタンスの[ウォームアップ](#)にかかる秒数を指定できます。その指定されたウォームアップ期間が終了するまで、EC2 インスタンスは Auto Scaling グループの集合メトリクスの対象になりません。スケールアウト中、Auto Scaling ロジックは、ウォームアップ中の EC2 インスタンスを、Auto Scaling グループの現在の容量の一部と見なしません。したがって、ステップ調整値の同じ範囲に入るアラーム超過が複数発生した場合でも、規模の拡大や縮小は一度だけとなります。これにより、必要以上のインスタンスが追加されることがなくなります。

10) C – [Aurora レプリカ](#)は、読み取りトラフィックをオフロードする方法を提供します。Aurora レプリカはメインデータベースと同じ[基本ストレージ](#)を共有するため、通常、遅延は非常に短くなります。Aurora レプリカには独自のエンドポイントがあるため、読み取りトラフィックを新しいエンドポイントに送信するようアプリケーションを設定する必要があります。