aws training and certification

AWS Certified SysOps Administrator-Associate (SOA-C01)
試験問題サンプル

1)企業は単一のサーバーから Application Load Balancer (ALB) の背後にある複数の Amazon EC2 インスタンスにレガシーの ウェブアプリケーションを移行しています。移行後、ユーザーがセッションの頻繁な切断、また再ログインを求められることを報告しています。

ユーザーから報告された問題を解決するために次のうちどの措置を講じる必要がありますか?

A) ALB がマルチ AZ 構成になっていないかの確認
B) ALB を基として Amazon CloudFront ディストリビューションの設定
C) ALB の前に Network Load Balancer をデプロイする
D) EC2 インスタンスのターゲットグループに対してスティッキーセッションの有効化。

2) 運用チームは、毎週 AWS Personal Health ダッシュボードで、次の AWS ハードウェアメンテナンスイベントをチェックしています。最近、一人のスタッフが休暇中であったためチームはメンテナンスの予定を見落とし、その結果サービスが停止しました。チームはダッシュボードの確認を一人のスタッフに頼るのではなく、全員が次のメンテナンスを周知できるような簡単な方法を求めています。

これに対処する方法は次のうちどれですか?

A) Personal Health ダッシュボードを監視する ウェブスクレーパーを構築する。新しいイベントが検出されたときに、チームで監視する Amazon SNS トピックに通知を送信する。
B) AWS Health サービスに基づいて Amazon CloudWatch Events イベントを作成し、チームで監視する Amazon SNS トピックに通知を送信する。
C) Personal Health ダッシュボードでメンテナンスの予定を表示するようチームにリマインドするために、チームで監視する Amazon SNS トピックに通知を送信し、Amazon CloudWatch Events を作成する。
D) すべての EC2 インスタンスに対し継続的に ネットワーク接続確認を実行して正常性を確認するために AWS Lambda 関数を作成する。これに失敗した場合は、チームにアラートを送信する。

3) VPC で稼働されているアプリケーションは異なるアカウントによって所有され、かつ別のリージョンの VPC で稼働されているインスタンスにアクセスする必要があります。コンプライアンスの観点から、トラフィックはパブリックインターネットを通過してはなりません。

これらの要件を満たすために、管理者はネットワークルーティングをどのように構成すべきでしょうか?

A) 各アカウント内に他のアカウントの仮想プライベートゲートウェイを示すルートを格納するカスタムルーティングテーブルを作成する。
B) 各アカウント内にそれぞれの VPC のパブリックサブネットに NAT ゲートウェイを設定する。次に、NAT ゲートウェイからのパブリック IP アドレスを使用し、2 つの VPC 間のルーティングを有効にする。
C) 1 つのアカウントで VPCs の間に VPN のサイト間の 接続を構成する。各アカウント内にリモート VPC の CIDR ブロックを示す VPC ルートテーブルにルートを追加する。
D) 1 つのアカウントから VPC ピアリング要求を作成する。他のアカウントの管理者が要求を受け入れた後、ピアリングされた VPC の CIDR ブロックを示す各 VPC のルートテーブルにルートを追加する。

4) Amazon EC2 インスタンスで稼働されているアプリケーションは、Amazon DynamoDB テーブルに格納されているデータにアクセスする必要があります。

最も安全な方法でアプリケーションにテーブルへのアクセスを許可するソリューションは、次のうちどれですか?

A) アプリケーションの IAM グループを作成し、必要な権限を持つアクセス許可ポリシーを添付するする。EC2 インスタンスを IAM グループに追加する。
B) Amazon EC2 に必要なアクセス許可を付与する DynamoDB テーブルの IAM リソースポリシーを作成する。
C) DynamoDB テーブルへのアクセスに必要な権限を持つ IAM ロールを作成する。ロールを EC2 インスタンスにアサインする。
D) アプリケーション用の IAM ユーザーを作成し、必要な権限を持つアクセス許可ポリシーを添付する。アクセスキーを生成し、そのキーをアプリケーションコードに埋め込む。

5) サードパーティのサービスは毎晩 Amazon S3 にオブジェクトがアップロードしています。場合によってはサービスにより、誤ってフォーマットされたバージョンのオブジェクトがアップロードされることもあります。このような場合、SysOps Administrator は旧バージョンのオブジェクトを回復する必要があります。

リモートサービスからオブジェクトを取得するせずにオブジェクトを回復する、最も効率的な方法は次のうちどれですか?

A) 毎晩行われるオブジェクトのアップロードの前に S3 バケットをバックアップするための AWS Lambda 関数をトリガーする、Amazon CloudWatch Events スケジュールイベントを設定する。その際不良オブジェクトが検出された場合は、バックアップバージョンを復元する。
B) オブジェクト作成時に、オブジェクトを Amazon Elasticsearch Service (Amazon ES) クラスターにコピーする S3 イベントを作成する。その際不良オブジェクトが検出された場合は、Amazon ES から以前のバージョンを取得する。
C) 別のアカウントが所有する S3 バケットにオブジェクトをコピーする AWS Lambda 関数を作成します。S3 で新しいオブジェクトが作成されたときに関数をトリガーします。不良オブジェクトが検出された場合は、他のアカウントから以前のバージョンを取得します。
D) S3 バケットのバージョン管理を有効にする。その際不良オブジェクトが検出された場合は、CLI または AWS 管理コンソールを使用して以前のバージョンにアクセスする。

6) AWS 共有責任モデルによると、次の Amazon EC2 アクティビティのうち、AWS が責任を負うのはどれですか? (2 つ選択し)

A) ネットワーク ACL の設定
B) ネットワークインフラストラクチャのメンテナンス
C) メモリ使用率の監視
D) オペレーティングシステムへのパッチ適用
E) ハイパーバイザーへのパッチ適用

7) セキュリティおよびコンプライアンスチームは、すべての Amazon EC2 ワークロードで承認済みの Amazon Machine Images (AMI) を使用する必要があります。SysOps Administrator は未承認の AMI から起動された EC2 インスタンスを検知するプロセスを実装しなければなりません。

これらの要件を満たすソリューションは次のうちどれですか?

A) AWS Systems Manager インベントリを使用してカスタムレポートを作成し、未承認の AMI を識別する。
B) 各 EC2 インスタンスで Amazon Inspector を実行し、未承認の AMI を使用している場合はインスタンスにフラグを立てる。
C) AWS Config ルールを使用し、未承認の AMI を識別する。
D) AWS Trusted Advisor を使用し、未承認の AMI を使用する EC2 ワークロードを識別する。

8) SysOps Administrator は Application Load Balancer で大量の不正な HTTP リクエストを監視しています。そのリクエストはさまざまな IP アドレスから発信されています。それによりサーバーの負荷とコストが増加しています。

SysOps Administrator はこの不正なリクエストをブロックするために何を行う必要がありますか?

A) 不正なリクエストをブロックするために、Amazon EC2 インスタンスに Amazon Inspector をインストールする。
B) Amazon GuardDuty を使用し、ウェブサーバーをボットやスクレーパーから保護する。
C) AWS Lambda を使用し、ウェブサーバーのログの分析及びボットトラフィックの検出を行い、セキュリティグループの IP アドレスをブロックする。
D) AWS WAF レートベースのブラックリストを使用し、しきい値を超えたときにトラフィックをブロックする。

9) SysOps Administrator は AWS 上で運用されているウェブアプリケーションのセキュリティグループポリシーを設定しています。Elastic Load Balancer は Amazon EC2 インスタンスのフリートに接続します。各 Amazon EC2 インスタンスはポート 1521 を通じて Amazon RDS データベースに接続します。セキュリティグループの名称はそれぞれ elbSG、ec2SG、 rdsSG です。

これらのセキュリティグループをどのように設定すべきでしょうか?

A) elbSG: 0.0.0.0/0 からポート 80 および 443 を許可する。
ec2SG: elbSG からポート 443 を許可する。
rdsSG: ec2SG からポート 1521 を許可する。

B) elbSG: 0.0.0.0/0 からポート 80 および 443 を許可する。
ec2SG: elbSG と rdsSG からポート 80 および 443 を許可する。
rdsSG: ec2SG からポート 1521 を許可する。

C) elbSG: ec2SG からポート 80 および 443 を許可する。
ec2SG: elbSG と rdsSG からポート 80 および 443 を許可する。
rdsSG: ec2SG からポート 1521 を許可する。

D) elbSG: ec2SG からポート 80 および 443 を許可する。
ec2SG: elbSG からポート 443 を許可する。
rdsSG: elbSG からポート 1521 を許可する。

10) E コマース関連企業は 1 日の売上を集計し、その結果を Amazon S3 に保存する夜間処理のコストを削減したいと考えています。その処理は複数のオンデマンドインスタンスで実行され、処理が完了するまでに 2 時間弱かかります。処理は夜間にいつでも実行できます。何らかの理由により処理が失敗した場合は、最初から処理を開始する必要があります。

この要件に基づいて、最もコスト効率の良いソリューションは次のうちどれですか?

A) 予約インスタンスを購入する。
B) スポットブロックのリクエストを作成する。
C) すべてのスポットインスタンスのリクエストを作成する。
D) オンデマンドインスタンスとスポットインスタンスを併用する。

解答

1) D - 一つのサーバーで実行するように設計されたこれまでのアプリケーションは、セッションデータを頻繁にローカルに格納します。これらのアプリケーションがロードバランサーの背後にある複数のインスタンスに配備されると、ユーザーのリクエストはラウンドロビンルーティングアルゴリズムを使用してインスタンスにルーティングされます。1 つのインスタンスに格納されているセッションデータは、他のインスタンスには存在しません。スティッキーセッションを有効にすると、Cookie を使用してユーザーのリクエストを追跡し、後続のリクエストを同じインスタンスに送信し続けます。

2) B - AWS Health Service では、Amazon CloudWatch Events を公開しています。CloudWatch Events により Amazon SNS 通知をトリガーできます。この方法は追加のコーディングやインフラストラクチャは必要ありません。予定されているイベントをチームに自動的に通知し、ウェブスクレイピングのような脆弱なソリューションに依存しません。

3) D - VPC ピアリング接続は各 VPC のプライベート IP アドレスを同じネットワーク内にあるかのように使用するルーティングを可能にします。リージョン間 VPC ピアリングを使用するトラフィックは、常にグローバル AWS バックボーン上に留まり、パブリックインターネットを通過することはありません。

4) C - IAM ロールを使用することにより、Amazon EC2 インスタンスで稼働されているアプリケーションに対するアクセスを許可し、AWS API リクエストで一時的な資格情報を使用することができます。

5) D - バージョン管理を有効することが簡単な解決策です。(A) はカスタムコードの記述を含み、(C) にはバージョン管理がないため、エラーがすぐに検出されない場合は古いバージョンが適切ではないバージョンで上書きされます。(B) にはオブジェクトに適さない高価なストレージが含まれます。

6) B、E - AWS は Amazon EC2 をサポートするハードウェアおよびハイパーバイザーソフトウェアのメンテナンスを含む、クラウドのセキュリティを提供します。お客様は EC2 インスタンス内のメンテナンスまたは監視および VPC インフラストラクチャの構成に対して責任を負います。

7) C - AWS Config にはこの状況に対処できるマネージドルールが含まれています。

8) D - AWS WAF には HTTP フラッディング攻撃からウェブアプリケーションを保護できるルールがあります。

9) A - elbSG はインターネットからすべてのウェブトラフィック (HTTP および HTTPS) を許可する必要があります。ec2SG はこの場合、elbSG からのトラフィックとして識別されるロードバランサーのみからのトラフィックに限り許可する必要があります。データベースは、この場合、ec2SG からのトラフィックとして識別される EC2 インスタンスのみからのトラフィックを許可する必要があります。

10) B - ソリューションはスポット価格設定を利用しますが、スポットインスタンスの代わりにスポットブロックを使用することにより会社は処理が継続することを保証できます。