aws training and certification

AWS 認定高度なネットワーキング – 専門知識
AWS Certified Advanced Networking – Specialty
(ANS-C00) 認定試験の質問例

(1) ある企業において、オンプレミスネットワークに対して IP アドレス範囲 11.11.0.0/16 が割り当てられています。このネットワーク範囲内の IP アドレスだけをサーバー間通信に使用できます。クラウドに対しては、IP アドレス範囲 11.11.253.0/24 が割り当てられています。

ネットワークエンジニアが、AWS 上で VPC を設計する必要があります。この VPC 内のサーバーは、VPN 接続を使用してインターネット上およびオンプレミス環境のホストと通信できる必要があります。

これらの要件を満たすには、どうすればよいですか (2 つ選択してください)。

A) IP アドレス範囲 11.11.253.0/24 を割り当てるよう、VPC を構成する。
B) RFC 1918 で規定されているプライベート IP アドレス範囲 (例: 10.10.10.0/24) を割り当てるよう、VPC を構成する。すべての送信トラフィックに対して 10.10.10.0/24 と 11.11.253.0/24 の間での変換を実行するよう、NAT ゲートウェイを構成する。
C) 仮想プライベートゲートウェイとオンプレミスルーターの間の VPN 接続を構成する。すべてのトラフィックに対して、仮想プライベートゲートウェイをデフォルトゲートウェイとして設定する。トラフィックをインターネットに転送するよう、オンプレミスルーターを構成する。
D) 仮想プライベートゲートウェイとオンプレミスルーターの間の VPN 接続を構成する。11.11.0.0/24 宛のトラフィックに対して、仮想プライベートゲートウェイをデフォルトゲートウェイとして設定する。VPC サブネットルートを追加し、インターネットトラフィックに対して、デフォルトゲートウェイをインターネットゲートウェイに振り向ける。
E) RFC 1918 で規定されているプライベート IP アドレス範囲 (例: 10.10.10.0/24) を割り当てるよう、VPC を構成する。すべての送信パケットの送信元 IP アドレスを 11.11.0.0/16 に変換するよう、仮想プライベートゲートウェイを構成する。

(2) ネットワークエンジニアが、Amazon EC2 インスタンス上で動作するアプリケーション用のソリューションを設計する必要があります。このアプリケーションは、別の VPC 内および別のリージョン内にあるパブリックアクセス可能なマルチ AZ 配置の Amazon RDS データベースインスタンスに接続します。
トラフィックはインターネットを通過できないというセキュリティ要件が定められています。

トラフィックをインターネットにルーティングせず、インスタンスどうしがプライベート通信できるようにするには、どうすればよいですか。

A) VPC 間のピアリング接続を作成する。VPC 間でトラフィックをルーティングするよう、ルーティングテーブルを更新する。VPC ピアリング接続に対して DNS 解決サポートを有効化する。データベースインスタンスの DNS エンドポイントに接続するよう、アプリケーションを構成する。
B) データベースインスタンスへのゲートウェイエンドポイントを作成する。トラフィックをゲートウェイエンドポイントにルーティングするよう、アプリケーション VPC 内のルーティングテーブルを更新する。
C) VPC 間でトラフィックをプライベートにルーティングするよう、トランジット VPC を構成する。データベースインスタンスの DNS エンドポイントに接続するよう、アプリケーションを構成する。
D) EC2 インスタンスと同じサブネット内に NAT ゲートウェイを作成する。トラフィックを NAT ゲートウェイ経由でデータベースインスタンスの DNS エンドポイントにルーティングするよう、アプリケーション VPC 内のルーティングテーブルを更新する。

(3) ある企業が AWS 上に基幹環境を構築しました。コンプライアンス上の理由により、ネットワークエンジニアは、Amazon EC2 インスタンスが特定の承認済みセキュリティグループを使用しており、かつ特定の VPC に属していることを確認する必要があります。また、各インスタンスの構成履歴を記録し、コンプライアンス上の問題が発生した場合、インスタンスを自動停止する必要があります。

これらの要件を満たすには、どうすればよいですか。

A) AWS CloudTrail を有効化し、カスタム Amazon CloudWatch アラームを作成して、必要な検査を実行する。CloudWatch アラームが失敗状態である場合、「このインスタンスを停止」アクションをトリガし、不適合 EC2 インスタンスを停止する。
B) 必要な検査を実行する AWS Lambda 関数を呼び出すよう、スケジュールされた Amazon CloudWatch Events イベントを構成する。不適合リソースが検出された場合、その EC2 インスタンスを停止する別の Lambda 関数を呼び出す。
C) 必要な検査を実行する AWS Lambda 関数をトリガする、EC2 インスタンス状態変更通知を発行するよう、Amazon CloudWatch Events イベントを構成する。不適合リソースが検出された場合、
その EC2 インスタンスを停止する別の Lambda 関数を呼び出す。
D) AWS Config を有効化し、カスタム AWS Config ルールを作成して、必要な検査を実行する。不適合リソースが検出された場合、修正アクションを使用して AWS Systems Manager ドキュメントを実行し、EC2 インスタンスを停止する。

(4) ある企業が、オンプレミスデータセンターを AWS に拡張しようとしています。ピーク時間帯の想定トラフィック量は、1 ～ 2 Gbps です。ネットワークエンジニアが、AWS とデータセンターの間の帯域幅を十分に確保し、ピーク時間帯のトラフィックを処理できるようにする必要があります。また、高い可用性と費用対効果を確保する必要があります。

これらの要件を満たすには、どうすればよいですか。

A) 10 Gbps の AWS Direct Connect 接続を 1 個展開する。バックアップ用に IPSec VPN を構成する。
B) リンクアグリゲーショングループ内に 1 Gbps の AWS Direct Connect 接続を 2 個展開する。
C) リンクアグリゲーショングループ内に、2 か所の AWS Direct Connect ロケーションへの 1 Gbps の Direct Connect 接続を 2 個ずつ展開する。
D) 2 か所の AWS Direct Connect ロケーションへの 10 Gbps の Direct Connect 接続を 1 個ずつ展開する。

(5) ネットワークエンジニアが、Amazon S3 バケットへのアクセスを、特定の送信元ネットワークにのみ許可する必要があります。

この要件を満たすには、どうすればよいですか。

A) S3 バケット内に ACL を作成し、指定ネットワークの CIDR ブロックにのみアクセスを許可する。
B) S3 バケット内にバケットポリシーを作成し、条件ステートメントを使用して、指定ネットワークの CIDR ブロックにのみアクセスを許可する。
C) セキュリティグループを作成し、指定ネットワークの CIDR ブロックにのみ受信アクセスを許可する。セキュリティグループを S3 バケットに適用する。
D) セキュリティグループを作成し、指定ネットワークの CIDR ブロックにのみ受信アクセスを許可する。S3 VPC エンドポイントを作成する。セキュリティグループを VPC エンドポイントに適用する。

(6) ある企業では、Web アプリケーションログを収集および分析し、悪意のある行為を見つけるというコンプライアンス要件が定められています。また、ネットワークエンジニアは、Web インスタンスのネットワークインターフェイスをリモートで変更しようとする行為を監視する必要があります。

これらの要件を満たすには、どうすればよいですか。

A) Amazon CloudWatch Logs エージェントを各 Web インスタンスにインストールし、アプリケーションログを収集する。VPC フローログを使用して、データを Amazon CloudWatch Logs に送信する。CloudWatch Logs メトリクスフィルタを使用して、ログデータ内で探すパターンを定義する。

B) すべての管理イベントとデータイベントをカスタム Amazon S3 バケットおよび Amazon CloudWatch Logs にロギングするよう、AWS CloudTrail を構成する。VPC フローログを使用して、データを Amazon CloudWatch Logs に送信する。CloudWatch Logs メトリクスフィルタを使用して、ログデータ内で探すパターンを定義する。

C) すべての管理イベントをカスタム Amazon S3 バケットおよび Amazon CloudWatch Logs にロギングするよう、AWS CloudTrail を構成する。Amazon CloudWatch Logs エージェントを各 Web インスタンスにインストールし、アプリケーションログを収集する。CloudWatch Logs Insights を使用して、ログデータ内で探すパターンを定義する。

D) AWS Config を有効化し、Web インスタンスに対するすべての構成情報変更内容を記録する。すべての管理イベントおよびデータイベントをカスタム Amazon S3 バケットにロギングするよう、AWS CloudTrail を構成する。Amazon Athena を使用して、Amazon S3 に格納されたログデータ内で探すパターンを定義する。

(7) ある企業が、機密データを処理するアプリケーションを使用しています。このデータは現在、オンプレミスデータセンターに格納されています。ネットワークエンジニアが、ワークロードを AWS に移行しようとしています。データを AWS に送信する際、送信中データの機密性と整合性を確保する必要があります。この企業は、AWS Direct Connect 接続を既に作成しています。

オンプレミスデータセンターと AWS の間に最も費用対効果の高い接続を作成するには、どうすればよいですか (2 つ選択してください)。

A) インターネットゲートウェイを VPC にアタッチする。

B) AWS Direct Connect 接続上で仮想パブリックインターフェイスを構成する。

C) 仮想プライベートゲートウェイに対する仮想プライベートインターフェイスを構成する。

D) カスタマーゲートウェイと Amazon EC2 上のソフトウェア VPN の間に IPSec トンネルを作成する。

E) 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の間に Site-to-Site VPN を作成する。

(8) ある企業が、e コマース Web サイトの新機能を作成しようとしています。これらの機能は、マイクロサービスとして展開されます。その際、サービスごとに別々のドメイン名が使用されます。この企業では、すべての一般向け Web サイトに対して HTTPS の使用を義務付けています。また、このアプリケーションは、クライアントの送信元 IP アドレスを必要とします。

これらの要件を満たすには、どうすればよいですか (2 つ選択してください)。

A) Network Load Balancer を使用して、トラフィックを各サービスに分散する。
B) Application Load Balancer を使用して、トラフィックを各サービスに分散する。
C) X-Forwarded-For ヘッダーを使用してクライアントの IP アドレスを取得するよう、アプリケーションを構成する。
D) X-Forwarded-Host ヘッダーを使用してクライアントの IP アドレスを取得するよう、アプリケーションを構成する。
E) PROXY プロトコルヘッダーを使用してクライアントの IP アドレスを取得するよう、アプリケーションを構成する。

(9) ネットワークエンジニアが、AWS 上で高パフォーマンスのコンピューティングソリューションを設計しています。このシステムは、Amazon EC2 インスタンスのクラスターから成ります。インスタンス間で低レイテンシーの通信を行う必要があります。

これらの要件を満たすには、どうすればよいですか。

A) インスタンスを起動し、クラスターに必要なインスタンス数と同サイズの 1 個のサブネットに追加する。
B) クラスタープレースメントグループを作成する。Elastic Fabric Adapter (EFA) 対応インスタンスを起動し、プレースメントグループに追加する。
C) 上限数のコアおよび RAM を備えた Amazon EC2 インスタンスを起動する。Amazon EBS プロビジョンド IOPS (PIOPS) ボリュームをアタッチする。クラスター内のすべてのインスタンス間で使用される共有メモリシステムを実装する。
D) 拡張ネットワーキング機能を備えた Amazon EC2 インスタンスタイプを選択する。10 Gbps の非ブロッキング Elastic Network Interface を各インスタンスにアタッチする。

(10) ある企業の社内セキュリティチームが、「社内ネットワークから Amazon S3 にアクセスすることを許可してほしい」という要望を受けました。社内ファイアウォールを使用して、すべての外部トラフィックを明示的に許可する必要があります。

これらの要件を満たすには、どうすればよいですか。

A) AWS 開発者フォーラムの告知から Amazon S3 の IP アドレスプレフィックスをダウンロードするスクリプトをスケジューリングする。その結果に応じてファイアウォールルールを更新する。
B) ip-ranges.json ファイルから Amazon S3 IP アドレスプレフィックスをダウンロードして解析するスクリプトをスケジューリングする。その結果に応じてファイアウォールルールを更新する。
C) Amazon S3 エンドポイント上で DNS ルックアップを実行するスクリプトをスケジューリングする。その結果に応じて、ファイアウォールルールを更新する。
D) AWS Direct Connect を使用して、データセンターを VPC に接続する。データセンターから Amazon S3 VPC エンドポイントにトラフィックを転送するルートを作成する。

回答

(1) A、C – VPC に対して、割り当てられた IP アドレス範囲内の CIDR ブロックを使用する必要があります。また、データセンターとオーバーラップしないようにする必要があります。VPC 宛でないトラフィックはすべて、(ルートが仮定されている) 仮想プライベートゲートウェイにルーティングされます。その後、
これらのトラフィックは、オンプレミス環境に届いたときにインターネットに転送されなければなりません。B および E は不正解です。割り当てられた IP アドレス範囲内にないからです (VPC 内では、RFC 1918 で規定されていない IP アドレスを使用できます)。D は不正解です。トラフィックがインターネットゲートウェイ経由でインターネットに振り向けられるからです。

(2) A – VPC ピアリング接続上で DNS 解決を構成した場合、アプリケーション VPC からのクエリがデータベースインスタンスのプライベート IP アドレスに変換されるので、トラフィックがインターネットにルーティングされることはありません。B は不正解です。Amazon RDS はゲートウェイエンドポイントによってサポートされていないからです。C および D は不正解です。データベースエンドポイントがパブリック IP アドレスに変換され、トラフィックがインターネットにルーティングされるからです。

(3) D – AWS Config を使用した場合、あるユーザーの AWS アカウント内の AWS リソースの詳細な構成情報がわかります。また、AWS Config ルールと AWS Systems Manager 自動化ドキュメントを併用することにより、不適合リソースを自動修正できます。

(4) C – 十分な帯域幅と高可用性を確保するには、リンクアグリゲーショングループ内に、2 か所の AWS Direct Connect ロケーションへの Direct Connect 接続を 2 個ずつ展開する必要があります。一方の Direct Connect ロケーションで障害が発生した場合、もう一方の Direct Connect ロケーション内の 2 個の Direct Connect 接続がバックアップとして機能します。他の選択肢の場合、接続が失われたときにピーク時間帯のトラフィックに対応できません。

(5) B – Amazon S3 バケットポリシーの中で条件ステートメントを使用することにより、特定の IP アドレス範囲から送信されたリクエストによるアクセスを制限できます。A は不正解です。S3 の ACL では、特定の IP アドレスからのアクセスを制限できないからです。C は不正解です。S3 バケットにはセキュリティグループを適用できないからです。D は不正解です。S3 VPC エンドポイントにはセキュリティグループを適用できないからです。

(6) C – Web アプリケーションログはオペレーティングシステム内にあります。また、Amazon CloudWatch Logs Insights と CloudWatch エージェントを併用することにより、ログを収集および分析できます。AWS CloudTrail によって、すべての AWS API 処理が監視されます。CloudTrail を使用して、特定の API 呼び出しを監視し、Web インスタンスのネットワークインターフェイスをリモートで変更しようとする行為を特定することができます。

(7) B、E – AWS Direct Connect 接続上に VPN を作成した場合、送信中データのセキュリティが確保されます。VPN を作成するには、まず、仮想パブリックインターフェイスを作成します。次に、仮想パブリックインターフェイスを使用して、データセンターと仮想プライベートゲートウェイの間に Site-to-Site VPN を作成します。A は不正解です。トラフィックがパブリックインターネットに送信されるからです。C は不可能です。VPN トンネルの IP アドレスを通知するには、仮想パブリックインターフェイスが必要となるからです。D は不正解です。既存の Direct Connect 接続を使用しないからです。

(8) B、C – Application Load Balancer はホストベースのルーティングをサポートしています。この機能は、ドメイン名に基づいてトラフィックをさまざまなマイクロサービスにルーティングするのに必要です。X-Forwarded-For は、クライアントの送信元 IP アドレスを特定する際に使用するリクエストヘッダーです。

(9) B – 高パフォーマンスのコンピューティングアプリケーションを作成する場合、クラスタープレースメントグループと Elastic Fabric Adapter (EFA) を使用することが推奨されます。これにより、アプリケーションのネットワークレイテンシーが小さくなるか、ネットワークスループットが大きくなります (あるいはその両方)。A は不正解です。サブネットのサイズはネットワークパフォーマンスに影響しないからです。C は不正解です。Amazon EC2 インスタンス間で Amazon EBS ボリュームを共有することはできないからです。D は半分だけ正解です。拡張ネットワーキングは、EC2 インスタンスのネットワーク挙動には影響しますが、インスタンス間のネットワークインフラストラクチャには影響しないからです。

(10) B – ip-ranges.json ファイルには、AWS によって使用された IP アドレスの最新リストが格納されています。開発者フォーラム告知に IP アドレスプレフィックスが投稿されることはもうありません。DNS ルックアップを実行しても、IP アドレスプレフィックスの完全なリストを取得することはできません。D の場合、推移的ルーティングが必要ですが、実行できません。

