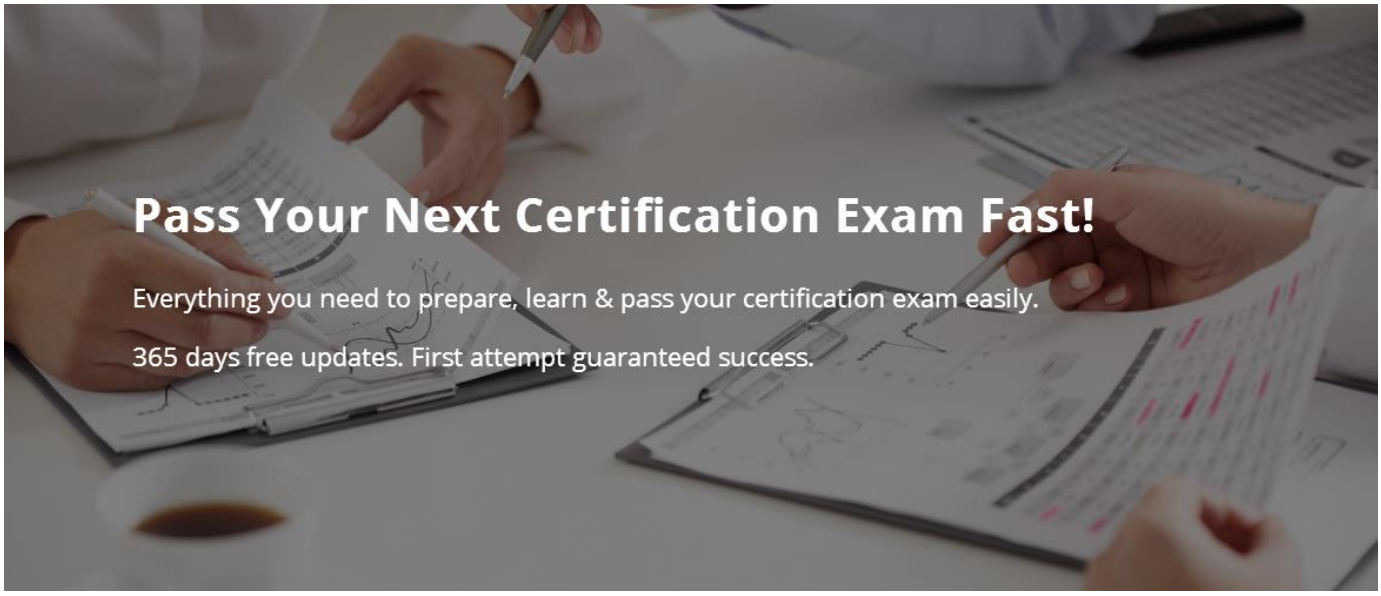
PrepPDF



Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.preppdf.com

Reasonable study tool and effective study materials - PrepPDF

Exam : **ANS-C01-JPN**

Title : AWS Certified Advanced Networking Specialty (ANS-C01日本語版)

Vendor : Amazon

Version : DEMO

QUESTION NO: 1
政府の請負業者は、顧客向けに複数の VPC
を備えたマルチアカウント環境を設計しています。ネットワーク セキュリティ
ポリシーでは、2 つの VPC 間のすべてのトラフィックがサードパーティ
アプライアンスによって透過的に検査されることが必要です。
顧客は、AWS Transit Gateway
を備えたソリューションを望んでいます。セットアップは複数のアベイラビリティーゾーンにわたって高可用性である必要があり、ソリューションは自動フェイルオーバーをサポートする必要があります。さらに、非対称ルーティングは検査アプライアンスではサポートされていません。
これらの要件を満たすソリューションの一部となる手順の組み合わせはどれですか?
(2つお選びください。)
A. 指定された検査 VPC
内の複数のアベイラビリティーゾーンにまたがる複数のアプライアンスで構成される 2
つのクラスターをデプロイします。VPC アタッチメントを使用して、検査 VPC
をトランジット ゲートウェイに接続します。ターゲット
グループを作成し、アプライアンスをターゲット グループに登録します。ネットワーク
ロード バランサー (NLB) を作成し、新しく作成したターゲット
グループに転送するように設定します。インスペクション VPC トランジット ゲートウェイ
サブネットに NLB へのデフォルト ルートを設定します。
B. 指定された検査 VPC
内の複数のアベイラビリティーゾーンにまたがる複数のアプライアンスで構成される 2
つのクラスターをデプロイします。VPC アタッチメントを使用して、検査 VPC
をトランジット ゲートウェイに接続します。ターゲット
グループを作成し、アプライアンスをターゲット グループに登録します。ゲートウェイ
ロード バランサーを作成し、新しく作成したターゲット
グループに転送するように設定します。インスペクション VPC のトランジット
ゲートウェイ サブネットに、ゲートウェイ ロード バランサー
エンドポイントに向かうデフォルト ルートを設定します。
C. トランジットゲートウェイ上に 2 つのルートテーブルを設定します。1 つのルート
テーブルをアプリケーション VPC のすべてのアタッチメントに関連付けます。他のルート
テーブルを検査 VPC のアタッチメントに関連付けます。すべての VPC
アタッチメントを検査ルート
テーブルに伝播します。アプリケーションルートテーブルに静的デフォルトルートを定義します。検査 VPC に接続するアタッチメントでアプライアンス モードを有効にします。
D. トランジットゲートウェイ上に 2 つのルートテーブルを設定します。1 つのルート
テーブルをアプリケーション VPC のすべてのアタッチメントに関連付けます。他のルート
テーブルを検査 VPC アタッチメントに関連付けます。すべての VPC
アタッチメントをアプリケーション ルート
テーブルに伝播します。検査ルートテーブルにスタティックデフォルトルートを定義します。検査 VPC に接続するアタッチメントでアプライアンス モードを有効にします。
E. トランジットゲートウェイ上にルートテーブルを 1
つ設定します。ルートテーブルをすべての VPC に関連付けます。すべての VPC
アタッチメントをルート
テーブルに伝播します。ルートテーブルに静的デフォルトルートを定義します。

Answer: B C

QUESTION NO: 2
ある企業は、us-east-
1リージョンの全アベイラビリティゾーンにまたがる2つの本番環境VPCで数百のAmazon EC2インスタンスを運用しています。本番環境VPCはそれぞれVPC AとVPC Bと名付けられています。
新しいセキュリティ規制により、本番環境のVPC間のすべてのトラフィックは、最終宛先にルーティングされる前に検査を受ける必要があります。同社は、ステートフルファイアウォールアプライアンスと、すべてのVPCにVPCアタッチメントが接続されたトランジットゲートウェイを含む新しい共有VPCをデプロイし、VPC AとVPC Bの間のトラフィックをファイアウォールアプライアンス経由でルーティングして検査を受けられるようにしました。テスト中に、同社は、トラフィックが2つのアベイラビリティゾーン間を移動するたびに、トランジットゲートウェイがトラフィックをドロップしていることに気付きました。
最小限の管理オーバーヘッドでこの問題を解決するには、ネットワークエンジニアは何をすべきでしょうか?
A.
共有VPCで、VPCアタッチメントをVPNアタッチメントに置き換えます。トランジットゲートウェイとファイアウォールアプライアンスの間にVPNトンネルを作成します。BGPを設定します。
B. VPC A と VPC B の VPC
アタッチメントでトランジットゲートウェイアプライアンスモードを有効にします。
C. 共有 VPC 内の VPC
アタッチメントでトランジットゲートウェイアプライアンスモードを有効にします。
D. 共有 VPC で、VPC A への VPC ピアリング接続を 1 つと、VPC B への別の VPC ピアリング接続を設定します。
Answer: C

QUESTION NO: 3
ネットワークエンジニアは、既存のネットワークへの2つ目のAWS Direct Connect接続を構成します。ネットワークエンジニアは、AWS Direct Connect Resiliency Toolkitを使用して、接続に対してテストを実行します。テストの結果は失敗です。フェイルオーバーイベント中、ネットワークエンジニアは、トラフィックがフェイルオーバー接続に移行する前に90秒間の中断を確認しました。
フェイルオーバーの時間を短縮できるソリューションはどれですか?
A. BGP hello タイマーを 5 秒に減らします。
B. 接続ソリューションにVPN接続を追加します。高速フェイルオーバーを実装します。
C. オンプレミス ルーターで双方向転送検出 (BFD) を構成します。
D. BGP ホールドダウン タイマーを 5 秒に減らします。
Answer: C

QUESTION NO: 4
ある企業が単一のAWSリージョンに3つのVPCを所有しています。各VPCには15個のAmazon EC2インスタンスが含まれており、VPC間の接続は確立されていません。

同社は3つのVPCすべてに新しいアプリケーションを導入しています。このアプリケーションはノード間の高帯域幅を必要とします。ネットワークエンジニアはVPC間の接続を実装する必要があります。
最高のスループットでこれらの要件を満たすソリューションはどれでしょうか?

A.
トランジットゲートウェイを設定します。各VPCをトランジットゲートウェイに接続します。各VPCで静的ルーティングを設定し、トラフィックをトランジットゲートウェイにルーティングします。

B.
3つのVPC間にVPCピアリングを設定します。3つのVPC間でトラフィックをルーティングするように静的ルーティングを設定します。

C.
トランジットVPCを設定します。各VPCにVPNゲートウェイを設定します。各VPCからトランジットVPCへのAWSサイト間VPNトンネルを作成します。BGPルーティングを使用して、VPCとトランジットVPC間のトラフィックをルーティングします。

D.
各VPC間のAWSサイト間VPN接続を設定します。各サイト間VPN接続のルート伝播を有効にして、VPC間のトラフィックをルーティングします。

Answer: B

QUESTION NO: 5
会社のネットワーク エンジニアは、AWS クラウド ワークロード用のハイブリッド DNS ソリューションを設計しています。個々のチームは、開発環境でアプリケーションの独自の DNS
ホスト名を管理したいと考えています。このソリューションでは、アプリケーション固有のホスト名とオンプレミス ネットワークからの一元管理される DNS
ホスト名を統合し、双方向の名前解決を提供する必要があります。また、ソリューションでは管理オーバーヘッドを最小限に抑える必要があります。
これらの要件を満たすために、ネットワーク
エンジニアはどの手順を組み合わせる必要がありますか?（3つお選びください。）

A. Amazon Route 53 リゾルバー インバウンド エンドポイントを使用します。
B. カスタム DNS サーバー値を設定して、DHCP オプション セットを変更します。
C. Amazon Route 53 Resolver アウトバウンドエンドポイントを使用します。
D. DNS プロキシ サーバーを作成します。
E. Amazon Route 53 プライベートホストゾーンを作成します。
F. Amazon Route 53 とオンプレミス DNS 間のゾーン転送を設定します。

Answer: A B E

QUESTION NO: 6
あるグローバル企業が、自社のプライマリデータセンターとセカンダリデータセンター、そしてVPC間のネットワーク接続を構築しています。ネットワークエンジニアは、接続の耐障害性とフォールトトレランスを最大限に高める必要があります。
ネットワーク帯域幅は 10 Gbps を超える必要があります。
これらの要件を最もコスト効率よく満たすソリューションはどれでしょうか?

A. プライマリデータセンターにAWS Direct Connect口ケーションで終端する100Gbps接続を設定します。セカンダリデータセンターに2つ目の100Gbps接続を設定し、2つ目のDirect Connect口ケーションで終端します。これらの接続は別々のプロバイダーによって管理されていることを確認してください。
B. プライマリデータセンターにAWS Direct Connect口ケーションで終端する10Gbps接続を設定します。セカンダリデータセンターに2つ目の10Gbps接続を設定し、2つ目のDirect Connect口ケーションで終端します。これらの接続は別々のプロバイダーによって管理されていることを確認してください。
C. プライマリデータセンターに、AWS Direct Connect の 1 つの口ケーションで終端する 10 Gbps 接続を 2 つ設定します。これらの接続が別々のプロバイダーによって管理されていることを確認してください。セカンダリデータセンターに、2 つ目の Direct Connect の口ケーションで終端する 10 Gbps 接続を 2 つ設定します。これらの接続が別々のプロバイダーによって管理されていることを確認してください。
D. プライマリデータセンターに10Gbpsの接続を設定し、AWS Direct Connectの口ケーションで終端します。セカンダリデータセンターにAWSサイト間VPN接続を設定し、会社のVPCと同じリージョンにある仮想プライベートゲートウェイで終端します。
Answer: C
Explanation:
Multiple 10 Gbps Connections: By setting up two 10 Gbps connections at each data center, the solution achieves an aggregate bandwidth of 20 Gbps per data center, exceeding the requirement of 10 Gbps. Using multiple 10 Gbps links is more cost-effective than deploying 100 Gbps links.
Separate Providers: Ensuring that the connections are managed by separate providers minimizes the risk of a single provider's failure affecting the network.
Two Direct Connect Locations: Terminating connections at two Direct Connect locations ensures geographic redundancy. This setup minimizes the impact of outages or disruptions at a single Direct Connect location.

QUESTION NO: 7
ある企業は、オフィスとVPCの間にAWSサイト間VPN接続を利用しています。ユーザーから、VPC内でホストされているアプリケーションへの接続が時々失敗するという報告がありました。ネットワークエンジニアは、カスタマーゲートウェイのログで、アプリケーションへの接続が失敗するとインターネットキー交換（IKE）セッションが終了することを発見しました。
IKE セッションがダウンした場合、ネットワーク エンジニアは IKE セッションを再開するために何をすべきでしょうか?
A.
デッドピア検出（DPD）タイムアウトアクションを「クリア」に設定します。VPCからオンプレミスへのトラフィックを開始します。
B.

デッドピア検出（DPD）タイムアウトアクションを「再起動」に設定します。オンプレミスからVPCへのトラフィックを開始します。

C.
デッドピア検出（DPD）タイムアウトアクションを「なし」に設定します。VPCからオンプレミスへのトラフィックを開始します。

D.
デッドピア検出（DPD）タイムアウトアクションを「キャンセル」に設定します。オンプレミスからVPCへのトラフィックを開始します。

Answer: B

QUESTION NO: 8
ある企業には、Amazon EC2 インスタンス群で実行されるアプリケーションがあります。新しい企業規則では、EC2 インスタンスとの間のすべてのネットワーク トラフィックを、コンテンツ検査のために一元化されたサードパーティの EC2 アプライアンスに送信することが義務付けられています。
これらの要件を満たすソリューションはどれでしょうか?

A. 各 EC2 ネットワーク インターフェイスで VPC フロー ログを設定します。フロー ログを Amazon S3 バケットに公開します。サードパーティの EC2 アプライアンスを作成して、S3 バケットからフロー ログを取得します。アプライアンスにログインして、ネットワーク コンテンツを監視します。

B. ネットワークロードバランサー (NLB) が前面にある Auto Scaling グループにサードパーティの EC2 アプライアンスを作成します。ミラーセッションを設定します。NLB をミラーターゲットとして指定します。ミラーセッションのソースの受信トラフィックと送信トラフィックをキャプチャするためのミラーフィルターを指定し、アプリケーションをホストするすべてのインスタンスの EC2 Elastic Network Interface を指定します。

C. ミラーセッションを設定します。ミラーターゲットとして Amazon Data Firehose 配信ストリームを指定します。受信トラフィックと送信トラフィックをキャプチャするためのミラーフィルターを指定します。ミラーセッションのソースには、アプリケーションをホストするすべてのインスタンスの EC2 Elastic Network Interface を指定します。サードパーティの EC2 アプライアンスを作成します。すべてのトラフィックを Firehose 配信ストリーム経由でアプライアンスに送信し、コンテンツを検査します。

D. 各 EC2 ネットワーク インターフェイスで VPC フロー ログを設定します。ログを Amazon CloudWatch に送信します。サードパーティの EC2 アプライアンスを作成します。CloudWatch フィルターを設定して、フロー ログを Amazon Data Firehose に送信し、アプライアンスにログをロードします。

Answer: D

QUESTION NO: 9
ある会社が AWS で外部 Web サイトをホストすることを計画しています。Web サイトには、Web サーバー、アプリケーション ロジック サービス、データベースなどの複数の層が含まれます。会社は AWS ネットワーク ファイアウォールを使用したいと考えています。

ネットワークセキュリティのための AWS WAR および VPC セキュリティグループ。
企業は、ネットワーク ファイアウォールが関連する VPC
内に適切にデプロイされていることを確認する必要があります。また、ネットワーク
ファイアウォールと AWS WAF
ルールにデプロイされているポリシーを一元管理する機能も必要です。さらに、アプリケーション チームが独自のセキュリティ グループを管理できるようにしながら、セキュリティ グループが過度に許可されたアクセスを許可しないようにする必要があります。
これらの要件を満たす最も運用効率の高いソリューションは何でしょうか?
A. ネットワークファイアウォールファイアウォールを定義します。AWS WAFv2 ウェブ ACL。ネットワークファイアウォールポリシー、およびコード内の VPC
セキュリティグループ。AWS CloudFormation
を使用して、オブジェクトと初期ポリシーおよびルールグループをデプロイします。CloudFormation を使用して、AWS WAFv2 ウェブ
ACL、ネットワークファイアウォールポリシー、および VPC
セキュリティグループを更新します。Amazon GuardDuty
を使用して、過度に許可されたルールを監視します。
B. ネットワークファイアウォールファイアウォールを定義します。AWS WAFv2 ウェブ ACL。ネットワークファイアウォールポリシー、およびコード内の VPC
セキュリティグループ。AWS マネジメントコンソールまたは AWS CLI を使用して、AWS WAFv2 ウェブ ACL、ネットワークファイアウォールポリシー、および VPC
セキュリティグループを管理します。Amazon GuardDuty を使用して AWS Lambda
関数を呼び出し、設定されたルールを評価し、過度に許可されたルールを削除します。
C. AWS CloudFormation を使用して AWS WAFv2 IP セットと AWS WAFv2 ウェブ ACL をデプロイします。AWS Firewall Manager を使用して、必要に応じて Network Firewall ファイアウォールと VPC セキュリティグループをデプロイし、AWS WAFv2 ウェブ ACL、Network Firewall ポリシー、および VPC セキュリティグループを管理します。
D. Network Firewall ファイアウォールを定義します。AWS WAFv2 ウェブ ACL。Network Firewall ポリシー、およびコード内の VPC セキュリティグループ。AWS CloudFormation を使用して、オブジェクトと初期ポリシーおよびルールグループをデプロイします。AWS Firewall Manager を使用して、AWS WAFv2 ウェブ ACL、Network Firewall
ポリシー、および VPC セキュリティグループを管理します。Amazon GuardDuty
を使用して、過度に許可されたルールを監視します。
Answer: D

QUESTION NO: 10
ある企業は Amazon S3 を使用して財務データをアーカイブすることを計画しています
ａ．現在、データはオンプレミスのデータセンターに保存されています。同社は、オンプレミス データセンターに接続するために、Direct Connect ゲートウェイとトランジット
ゲートウェイを備えた AWS Direct Connect
を使用しています。データは公共のインターネット上で転送することはできないため、転送中に暗号化する必要があります。
これらの要件を満たすソリューションはどれですか?
A. Direct Connect パブリック VIF を作成します。Amazon S3
にアクセスするには、パブリック VIF 経由で IPsec VPN
接続をセットアップします。通信にはHTTPSを使用します。

B. トランジット VIF 経由で IPsec VPN 接続を作成します。VPC を作成し、その VPC をトランジット ゲートウェイにアタッチします。VPC で、Amazon S3 のインターフェイス VPC エンドポイントをプロビジョニングします。通信にはHTTPSを使用します。
C. VPC を作成し、VPC をトランジット ゲートウェイにアタッチします。VPC で、Amazon S3 のインターフェイス VPC エンドポイントをプロビジョニングします。通信にはHTTPSを使用します。
D. Direct Connect パブリック VIF を作成します。パブリック VIF 経由でトランジット ゲートウェイへの IPsec VPN 接続をセットアップします。Amazon S3 のアタッチメントを作成します。通信にはHTTPSを使用します。
Answer: B
Explanation:
https://docs.aws.amazon.com/vpn/latest/s2svpn/private-ip-dx.html
An IPsec VPN connection over the transit VIF can encrypt traffic between the on-premises network and AWS without using public IP addresses or the internet2. A VPC endpoint for Amazon S3 can enable private access to S3 buckets within the same region. HTTPS can provide additional encryption for communication.

QUESTION NO: 11
あるスタートアップ企業のアプリケーションチームが、AWSクラウドに新しい多層アプリケーションをデプロイしようとしています。このアプリケーションは、パブリックアクセス可能なネットワークロードバランサー（NLB）の背後にあるAuto Scalingグループで実行されるAmazon EC2インスタンス群でホストされます。このアプリケーションでは、クライアントがUDPトラフィックとTCPトラフィックの両方に対応する必要があります。
当面は、アプリケーションは同じ地理的な場所にいるユーザーのみにサービスを提供します。アプリケーションチームは、アプリケーションを世界中のユーザーに拡張し、エンドユーザーにより近い場所にアプリケーションを届けるために、世界中の複数のAWSリージョンにデプロイを移行する予定です。アプリケーションチームは、新しいリージョンを使用してアプリケーションの新バージョンをデプロイし、これらのロールアウト中に各リージョンが受信するトラフィック量を制御できるようにしたいと考えています。さらに、アプリケーションチームは、エンドユーザーにとってのファーストバイトレイテンシーとジッター（ランダム遅延）を最小限に抑える必要があります。
アプリケーション チームは、これらの要件を満たすアプリケーションのネットワーク アーキテクチャをどのように設計する必要がありますか?
A. 各リージョンのデプロイメントに合わせて Amazon CloudFront ディストリビューションを作成します。各リージョンの NLB を各 CloudFront ディストリビューションのオリジンとして設定します。Amazon Route 53 の加重ルーティングポリシーを使用して、新しいリージョンのデプロイメントへのトラフィックを制御します。
B. 必要なポート用のAWS Global Acceleratorアクセラレータとリスナーを作成します。各リージョンのエンドポイントグループを設定します。エンドポイントグループにトラフィックダイヤルを設定し、新しいリージョンデプロイメントへのトラフィックを制御します。エンドポイントグループにNLBを登録します。
C. 各リージョンのアプリケーションに Amazon S3 Transfer Acceleration

を使用します。各リージョンが Transfer Acceleration エンドポイントからリージョン NLB に受信するトラフィック量を調整します。
D. オリジングループを含む Amazon CloudFront ディストリビューションを作成します。各リージョンの NLB をオリジングループのオリジンとして設定します。Amazon Route 53 レイテンシールーティングポリシーを使用して、新しいリージョンデプロイメントへのトラフィックを制御します。
Answer: B

QUESTION NO: 12
ある企業はAWSクラウドの導入初期段階にあります。アジアのオンプレミスデータセンターでアプリケーションを運用しており、新しいアプリケーションをus-east-1リージョンにデプロイする必要があります。
クラウド内のアプリケーションは、オンプレミスのデータセンターに接続する必要があります。
同社はAWSとデータセンター間の通信チャネルを構築する必要があります。このソリューションでは、レイテンシを改善し、パブリックインターネットを介した大陸間ルーティングによるパフォーマンスへの影響を最小限に抑え、転送中のデータを暗号化する必要があります。
最短時間でこれらの要件を満たすソリューションはどれでしょうか?
A. アクセラレーションを有効にした AWS サイト間 VPN 接続を作成します。仮想プライベートゲートウェイを作成します。サイト間 VPN 接続を仮想プライベートゲートウェイに接続します。仮想プライベートゲートウェイを、アプリケーションをデプロイする VPC に接続します。
B.
アクセラレーションを有効にしたAWSサイト間VPN接続を作成します。トランジットゲートウェイを作成します。
サイト間VPN接続をトランジットゲートウェイに接続します。アプリケーションがデプロイされるVPCにトランジットゲートウェイアタッチメントを作成します。
C. AWS Direct Connect 接続を作成します。仮想プライベートゲートウェイを作成します。仮想プライベートゲートウェイを使用するパブリック VIF とプライベート VIF を作成します。パブリック VIF を介して AWS サイト間 VPN 接続を作成します。
D.
アクセラレーションをオフにしたAWSサイト間VPN接続を作成します。トランジットゲートウェイを作成します。サイト間VPN接続をトランジットゲートウェイに接続します。アプリケーションをデプロイするVPCにトランジットゲートウェイアタッチメントを作成します。
Answer: B

QUESTION NO: 13
ある会社では、プロセスワークフローの要件を満たすために、AWS 上で API ベースのアプリケーションを開発しています。API は、会社のオンプレミスデータセンターのクライアントによって呼び出されます。会社は、オンプレミスと AWS の間に AWS Direct Connect 接続を設定しました。ネットワーク エンジニアは、Amazon

API Gateway でプライベート REST API として API
を実装することにしました。ネットワーク
エンジニアは、クライアントがプライベート通信を通じて API
エンドポイントに到達できるようにしたいと考えています。
ネットワーク エンジニアが追加のインフラストラクチャをセットアップせずに API
を呼び出すために使用できるソリューションはどれですか。

A. プライベート DNS 名を有効にした API Gateway のインターフェイス VPC
エンドポイントを作成します。エンドポイントのプライベート DNS 名を使用して API
にアクセスします。

B. プライベート DNS 名を有効にした API Gateway のインターフェイス VPC
エンドポイントを作成します。エンドポイントの Amazon Route 53 エイリアスを使用して
API にアクセスします。

C. API Gateway のインターフェイス VPC
エンドポイントを作成します。エンドポイントをプライベート REST API に関連付けます。
エンドポイントの Amazon Route 53 エイリアスを使用して API にアクセスします。

D. プライベート DNS 名を有効にした API Gateway のインターフェイス VPC
エンドポイントを作成します。エンドポイントのパブリック DNS 名を使用して API
にアクセスします。

Answer: A

QUESTION NO: 14

ある企業は、異なるAWSリージョンにある2つのVPCでアプリケーションを実行しています。1つのVPCはus-east-1リージョンにあり、もう1つのVPCはus-west-1リージョンにあります。この企業は、2つのVPC間の接続を確立する必要があります。また、オンプレミスデータセンターで実行されるアプリケーションにこれらのVPCを接続する必要もあります。
現在、VPC間のトラフィック要件は月間50
##です。VPC間のトラフィック量は今後増加すると予想しています。VPCからオンプレミスデータセンターへのトラフィック要件は月間10
##です。VPCとデータセンター間のトラフィック量は一定に維持されると予想しています。
これらの要件を最もコスト効率よく満たすソリューションはどれでしょうか?

A.
各リージョンにトランジットゲートウェイを作成します。トランジットゲートウェイからオンプレミスファイアウォールへのVPN接続を作成します。トランジットゲートウェイ間にピアリング接続を作成します。

B.
各リージョンに仮想プライベートゲートウェイを作成します。オンプレミスファイアウォールから仮想プライベートゲートウェイへのVPN接続を作成します。オンプレミスファイアウォールを設定して、2つのVPC間のトラフィックをルーティングします。

C.
各リージョンに仮想プライベートゲートウェイを作成します。オンプレミスのファイアウォールから仮想プライベートゲートウェイへのVPN接続を作成します。2つのVPC間にVPCピアリング接続を作成します。

D.
各リージョンに仮想プライベートゲートウェイを作成します。オンプレミスのファイアウォ

ールから仮想プライベートゲートウェイへのVPN接続を作成します。仮想プライベートゲートウェイ間にVPN接続を作成します。

Answer: A

Explanation:

Traffic Volume Consideration: The traffic volume between the VPCs (50 TB per month and increasing) justifies the use oftransit gateways, which are designed for scalable, high-throughput interconnectivity. A VPC peering connection would not scale as efficiently for this traffic volume.

On-Premises Connectivity: Establishing VPN connections from the on-premises firewall to the transit gateways ensures secure connectivity between the on-premises data center and both VPCs.

Transit Gateway Peering: Creating a peering connection between the transit gateways allows for efficient inter-Region communication between the VPCs without routing through the on-premises data center, reducing latency and costs.

Cost Efficiency: Transit gateway peering provides a cost-effective solution for large inter-Region traffic volumes compared to alternatives like routing all traffic through the on-premises data center, which would incur higher egress costs and potentially create a bottleneck.

QUESTION NO: 15

世界的な映画制作会社である同社は、AWS
クラウドを利用してビデオコンテンツを配信前にエンコードおよび保存しています。同社の世界3拠点は、BGP
ルーティングが有効化されているトランジットゲートウェイを終端とする AWS サイト間 VPN リンクを介して us-east-1 リージョンに接続されています。
同社は最近、8Kストリーミングに対応するため、より高解像度のコンテンツ制作を開始しました。コンテンツファイルのサイズは以前のフォーマットの3倍に増加し、Amazon EC2インスタンスへのファイルのアップロード時間は以前のフォーマットの10倍にもなっています。
アップロード時間を短縮するために、ネットワーク
エンジニアはどのようなアクションを推奨すべきですか? (2 つ選択してください。)

A.
各オフィスからトランジットゲートウェイへの2つ目のVPNトンネルを作成します。等コストマルチパス (ECMP) ルーティングを有効にします。

B. トランジット ゲートウェイを変更して、各オフィスの場所への VPN トンネルで Jumbo MTU を有効にします。

C. 既存の VPN
トンネルを、アクセラレーションが有効になっている新しいトンネルに置き換えます。

D.
各EC2インスタンスを最新のインスタンスタイプにアップグレードします。オペレーティングシステムでJumbo MTUを有効にします。

E. 既存の VPN トンネルを、IGMP が有効になっている新しいトンネルに置き換えます。

Answer: A C

QUESTION NO: 16

ある企業は、DNS のニーズに Amazon Route 53 を使用しています。会社のセキュリティ チームは、DNS
インフラストラクチャを更新して最新のセキュリティ体制を提供したいと考えています。
セキュリティ チームは、ドメインの DNS セキュリティ拡張機能 (DNSSEC)
を構成しました。セキュリティ チームは、DNSSEC
キーのローテーションの責任者をネットワーク
エンジニアに説明してもらいたいと考えています。
ネットワーク管理者はセキュリティ チームにどの説明を提供する必要がありますか?
A. AWS はゾーン署名キー (ZSK) をローテーションします。同社は鍵署名鍵 (KSK)
をローテーションします。
B. 会社はゾーン署名キー (ZSK) とキー署名キー (KSK) をローテーションします。
C. AWS は、AWS Key Management Service (AWS KMS) キーとキー署名キー (KSK)
をローテーションします。
D. 会社は AWS Key Management Service (AWS KMS) キーをローテーションします。 AWS はキー署名キー (KSK) をローテーションします。
Answer: A

QUESTION NO: 17
あなたの会社は、us-east-1 AWS
リージョンで米国市場向けのアプリケーションを実行しています。このアプリケーションは、Amazon Elastic Compute Cloud (EC2) インスタンス上で独自の TCP および UDP
プロトコルを使用します。エンド ユーザーは、ローカル PC
上でリアルタイムのフロントエンド アプリケーションを実行します。このフロントエンド アプリケーションは、サービスの DNS ホスト名を認識しています。
グローバル展開に向けてシステムを準備する必要があります。エンドユーザーは、待ち時間を最小限に抑えてアプリケーションにアクセスする必要があります。
これらの要件を満たすには、AWS のサービスをどのように使用する必要がありますか?
A. サービス ホストの IP アドレスを Amazon Route 53
のレイテンシーベースのルーティング
ポリシーを使用して「A」レコードとして登録し、これらのホストに対して Route 53
ヘルスチェックを設定します。
B. Elastic Load Balancing (ELB)
ロードバランサーをサービスのホストの前に設定し、メイン サービス ホストの ELB 名を Route 53 のレイテンシーベースのルーティング ポリシーを持つ ALIAS
レコードとして登録します。
C. Amazon CloudFront をサービスのホストの前に設定し、メインサービスの CloudFront 名を ALIAS レコードとして Route 53 に登録します。
D. Amazon
APIゲートウェイをサービスの前に設定し、メインサービスのAPIゲートウェイ名をALIASレコードとしてRoute 53に登録します。
Answer: B

QUESTION NO: 18
ある会社には、プライベートサブネットで Amazon EC2 インスタンスをホストする VPC があります。EC2 インスタンスは、インターネット接続に NAT

ゲートウェイとインターネットゲートウェイを使用して、特定のインターネット Web サイトからデータを取得します。この会社は、AWS ネットワークファイアウォールを使用して送信トラフィックをフィルタリングしたいと考えています。
これらの要件を満たすためにネットワーク エンジニアは何をすべきでしょうか?

A. 1. NAT ゲートウェイ サブネットにファイアウォールを作成します。
2. EC2 インスタンスのサブネット ルート テーブルを設定して、宛先が 0.0.0.0/0 のトラフィックを NAT ゲートウェイに送信します。
3. 宛先が 0.0.0.0/0 のトラフィックをファイアウォール エンドポイントに送信するように NAT ゲートウェイ サブネット ルート テーブルを構成します。
4. 宛先が 0.0.0.0/0 のトラフィックをインターネット ゲートウェイに送信するようにファイアウォール サブネット ルート テーブルを構成します。

B. 1. 新しいサブネットにファイアウォールを作成します。
2. 宛先が 0.0.0.0/0 のトラフィックをファイアウォール エンドポイントに送信するように EC2 インスタンス サブネット ルート テーブルを設定します。
3. 宛先が 0.0.0.0/0 のトラフィックを NAT ゲートウェイに送信するようにファイアウォール サブネット ルート テーブルを構成します。
4. 宛先が 0.0.0.0/0 のトラフィックをインターネット ゲートウェイに送信するように NAT ゲートウェイ サブネット ルート テーブルを設定します。

C. 1. EC2 インスタンスのサブネットにファイアウォールを作成します。
2. 宛先が 0.0.0.0/0 のトラフィックをファイアウォール エンドポイントに送信するように EC2 インスタンス サブネット ルート テーブルを設定します。
3. 宛先が 0.0.0.0/0 のトラフィックを NAT ゲートウェイに送信するようにファイアウォール サブネット ルート テーブルを構成します。
4. 宛先が 0.0.0.0/0 のトラフィックをインターネット ゲートウェイに送信するように NAT ゲートウェイ サブネット ルート テーブルを設定します。

D. 1. 新しいサブネットにファイアウォールを作成します。
2. EC2 インスタンスのサブネット ルート テーブルを設定して、宛先が 0.0.0.0/0 のトラフィックを NAT ゲートウェイに送信します。
3. 宛先が 0.0.0.0/0 のトラフィックをファイアウォール エンドポイントに送信するように NAT ゲートウェイ サブネット ルート テーブルを構成します。
4. 宛先が 0.0.0.0/0 のトラフィックをインターネット ゲートウェイに送信するようにファイアウォール サブネット ルート テーブルを構成します。

Answer: B

QUESTION NO: 19
ある企業が AWS に新しいアプリケーションをデプロイしています。アプリケーションは動的マルチキャストを使用します。同社には 5 つの VPC があり、それらはすべてトランジット ゲートウェイに接続されています。各 VPC の Amazon EC2 インスタンスは、マルチキャスト送信を受信するために動的に登録できる必要があります。
これらの要件を満たすために、ネットワーク エンジニアは AWS リソースをどのように構成すればよいでしょうか?

A. トランジット ゲートウェイ内に静的なソース マルチキャスト ドメインを作成します。VPC および該当するサブネットをマルチキャスト ドメインに関連付けます。マルチキャスト送信者のネットワーク インターフェイスをマルチキャスト ドメインに登録します。ネットワーク ACL を調整して、送信元からすべての受信者への UDP トラフィックを許可し、マルチキャスト グループ アドレスに送信される UDP トラフィックを許可します。
B. トランジット ゲートウェイ内に静的なソース マルチキャスト ドメインを作成します。VPC および該当するサブネットをマルチキャスト ドメインに関連付けます。マルチキャスト送信者のネットワーク インターフェイスをマルチキャスト ドメインに登録します。ネットワーク ACL を調整して、送信元からすべての受信者への TCP トラフィックを許可し、マルチキャスト グループ アドレスに送信される TCP トラフィックを許可します。
C. トランジット ゲートウェイ内にインターネット グループ管理プロトコル (IGMP) マルチキャスト ドメインを作成します。VPC および該当するサブネットをマルチキャスト ドメインに関連付けます。マルチキャスト送信者のネットワーク インターフェイスをマルチキャスト ドメインに登録します。ネットワーク ACL を調整して、送信元からすべての受信者への UDP トラフィックを許可し、マルチキャスト グループ アドレスに送信される UDP トラフィックを許可します。
D. トランジット ゲートウェイ内にインターネット グループ管理プロトコル (IGMP) マルチキャスト ドメインを作成します。VPC および該当するサブネットをマルチキャスト ドメインに関連付けます。マルチキャスト送信者のネットワーク インターフェイスをマルチキャスト ドメインに登録します。ネットワーク ACL を調整して、送信元からすべての受信者への TCP トラフィックを許可し、マルチキャスト グループ アドレスに送信される TCP トラフィックを許可します。
Answer: C

QUESTION NO: 20
ある企業は、自社のVPC内のリソースを、SaaSプロバイダーのSaaS（Software as a Service）ソリューションに安全に接続しています。このSaaSソリューションはAWSクラウドでホストされており、AWS PrivateLinkを利用しています。この企業は、PrivateLinkエンドポイントを使用して、SaaSプロバイダーのネットワークロードバランサー（NLB）の背後にあるSaaSソリューションにアクセスしています。
同社は最近、VPCに新しいアベイラビリティゾーンとサブネットを追加しました。ネットワークエンジニアは、新しいアベイラビリティゾーンにSaaSソリューション用の新しいインターフェイスVPCエンドポイントをデプロイできません。
この問題の原因は何ですか？
A. 新しいサブネットの CIDR ブロックが SaaS プロバイダーの CIDR ブロックと競合しています。
B. 新しいアベイラビリティーゾーンの新しいサブネットで、enableDnsHostnames 属性と enableDnsSupport 属性が設定されていませんでした。
C. SaaS プロバイダーは新しいアベイラビリティーゾーンでソリューションを提供しておらず、NLB のゾーン間負荷分散を構成していません。

D. 新しいサブネットには、VPC インターネットゲートウェイへのルートがありません。
Answer: C

QUESTION NO: 21
ある会社の VPC には、パブリックインターネット経由で AWS サービスと通信する Amazon EC2
インスタンスがあります。会社は、パブリックインターネット経由で通信が行われないように接続を変更する必要があります。
同社は、VPC に AWS PrivateLink エンドポイントをデプロイしています。PrivateLink エンドポイントをデプロイした後、EC2 インスタンスは必要な AWS
サービスとまったく通信できなくなります。
AWS
サービスとの通信を回復するために、ネットワークエンジニアが実行する必要がある手順の組み合わせはどれですか? (2 つ選択してください。)
A. VPC ルートテーブルで、PrivateLink エンドポイントを宛先とするルートを追加します。
B. VPC の enableDnsSupport 属性が True に設定されていることを確認します。各 VPC エンドポイントで DNS サポートが有効になっていることを確認します。
C. VPC エンドポイント ポリシーが通信を許可していることを確認します。
D. すべてのサービスに対して Amazon Route 53 パブリックホストゾーンを作成します。
E. 各サービスのカスタム名を含む Amazon Route 53
プライベートホストゾーンを作成します。
Answer: B C
Explanation:
To use AWS PrivateLink, you need to create interface type VPC endpoints for the services that you want to access privately from your VPC1. These endpoints appear as elastic network interfaces (ENIs) with private IPs in your subnets2. To enable DNS resolution for these endpoints, you need to set the enableDnsSupport attribute to True for your VPC, and enable DNS support for each endpoint3. You also need to ensure that the VPC endpoint policy allows communication between your VPC and the service4. You do not need to create any route table entries or Route 53 hosted zones for the endpoints, as they are not required for PrivateLink5.
AWS PrivateLink FAQs - Amazon Web Services 2: AWS PrivateLink and service endpoint - Amazon EC2 Overview and Networking Introduction for Telecom Companies 3: VPC Endpoints: Secure and Direct Access to AWS Services 4: AWS PrivateLink and service endpoint - Amazon EC2 Overview and Networking Introduction for Telecom Companies 5: AWS Private Link vs VPC Endpoint - Stack Overflow

QUESTION NO: 22
ある企業がハイブリッドクラウド環境を運用しています。この企業は、AWS Organizations 内の組織の一部として複数の AWS アカウントを保有しています。AWS
内のリソースへのアクセスを許可する IPv4
オンプレミスホストのリストを管理するためのソリューションが必要です。このソリューションは、IPv4 アドレスリストのバージョン管理機能を提供し、組織内の AWS
アカウントがリストを利用できるようにする必要があります。
これらの要件を満たすソリューションはどれでしょうか?

A. カスタマーマネージドプレフィックスリストを作成します。オンプレミス IPv4 ホストの初期リストにエントリを追加します。AWS Resource Access Manager でリソース共有を作成します。マネージドプレフィックスリストをリソース共有に追加します。
リソースを組織と共有します。
B. カスタマーマネージドプレフィックスリストを作成します。オンプレミス IPv4 ホストの初期リストにエントリを追加します。AWS Firewall Manager を使用して、マネージドプレフィックスリストを組織と共有します。
C. セキュリティグループを作成します。オンプレミスの IPv4 ホストの初期リストにインバウンドルールのエントリを追加します。AWS Resource Access Manager でリソース共有を作成します。リソース共有にセキュリティグループを追加します。リソースを組織と共有します。
D. Amazon DynamoDB テーブルを作成します。オンプレミス IPv4 ホストの初期リストにエントリを追加します。組織内の各 AWS アカウントでロールを引き受け、DynamoDB テーブルのエントリに基づいてセキュリティグループのインバウンドルールを承認する AWS Lambda 関数を作成します。
Answer: A

QUESTION NO: 23
ある企業は、複数の AWS リージョンにまたがる複数の VPC にデプロイされる新しいアプリケーションを開発しています。
VPC は AWS Transit Gateway を介して接続されます。VPC にはプライベートサブネットとパブリックサブネットが含まれます。
プライベートサブネット内のすべての送信インターネットトラフィックは監査および口グ記録される必要があります。同社のネットワークエンジニアはAWS Network Firewallの使用を計画しており、Network Firewallを通過するすべてのトラフィックが監査とアラートのために完全に口グ記録されるようにする必要があります。
これらの要件を満たすために、ネットワーク エンジニアはネットワーク ファイアウォールの口グ記録をどのように構成する必要がありますか?
A. Amazon CloudWatch でネットワークファイアウォールの口グ記録を設定し、すべてのアラートをキャプチャします。口グは Amazon CloudWatch Logs の口ググループに送信します。
B. ネットワーク ファイアウォールでネットワーク ファイアウォールの口グ記録を構成して、すべてのアラートとフロー口グをキャプチャします。
C. ファイアウォールエンドポイントのVPCフローログを設定して、ネットワークファイアウォールの口グ記録を設定します。口グはAmazon CloudWatch Logsの口ググループに送信します。
D. データイベントをキャプチャするように AWS CloudTrail を構成して、ネットワークファイアウォールの口グ記録を構成します。

Answer: B

QUESTION NO: 24
ある企業は、複数の AWS アカウントを備えたハイブリッド
アーキテクチャを使用して、ネットワークを AWS
クラウドに拡張しました。同社は、オンプレミスのデータセンターと会社のオフィスに接続するための共有 AWS
アカウントを設定しました。ワークロードは、内部使用のためのプライベート Web
ベースのサービスで構成されます。これらのサービスは、異なる AWS
アカウントで実行されます。オフィスベースの従業員は、example.internal
という名前のオンプレミス DNS ゾーン内の DNS
名を使用して、これらのサービスを利用します。
AWS で実行される新しいサービスを登録するプロセスでは、内部 DNS
に対する手動で複雑な変更リクエストが必要です。このプロセスには多くのチームが関与します。
同社は、サービス作成者に DNS レコードを登録できるアクセス権を与えることで、DNS
登録プロセスを更新したいと考えています。ネットワーク
エンジニアは、この目標を達成するソリューションを設計する必要があります。ソリューションは費用対効果を最大化し、必要な構成変更の回数を最小限に抑える必要があります。
これらの要件を満たすために、ネットワーク
エンジニアはどの手順を組み合わせる必要がありますか？（3つお選びください。）
A. ローカルのプライベートホストゾーン (serviceA.account1.aws.example.internal)
に各サービスのレコードを作成します。この DNS
レコードをアクセスが必要な従業員に提供します。
B. 共有アカウント VPC に Amazon Route 53 リゾルバー インバウンド
エンドポイントを作成します。オンプレミスの DNS サーバー上に aws.example.internal
という名前のドメインの条件付きフォワーダーを作成します。転送 IP
アドレスを、作成された受信エンドポイントの IP アドレスに設定します。
C. onprem.example.internal に対して行われたクエリをオンプレミスの DNS
サーバーに転送する Amazon Route 53 リゾルバー ルールを作成します。
D. このドメインのクエリを解決するために、共有 AWS アカウントに aws.example.internal
という名前の Amazon Route 53 プライベートホストゾーンを作成します。
E. 共有 AWS アカウントで 2 つの Amazon EC2
インスタンスを起動します。各インスタンスに BIND をインストールします。各 BIND
サーバー上に DNS 条件付きフォワーダーを作成し、aws.example.internal
の下の各サブドメインのクエリを各 AWS
アカウントの適切なプライベートホストゾーンに転送します。オンプレミスの DNS
サーバー上に aws.example.internal
という名前のドメインの条件付きフォワーダーを作成します。転送先 IP アドレスを BIND
サーバーの IP アドレスに設定します。
F. サービスを実行するアカウントごとに、共有 AWS
アカウントにプライベートホストゾーンを作成します。ドメイン内に aws.example.internal
を含むようにプライベートホストゾーンを設定します
(account1.aws.example.internal)。プライベートホストゾーンを、サービスを実行する VPC
および共有アカウント VPC に関連付けます。

Answer: A B D
Explanation:
To meet the requirements of updating the DNS registration process while maximizing cost-effectiveness and minimizing configuration changes, the network engineer should take the following steps:
* Create an Amazon Route 53 Resolver inbound endpoint in the shared account VPC. Create a conditional forwarder for a domain named aws.example.internal on the on-premises DNS servers. Set the forwarding IP addresses to the inbound endpoint's IP addresses that were created (Option B).
* Create an Amazon Route 53 private hosted zone named aws.example.internal in the shared AWS account to resolve queries for this domain (Option D).
* Create a record for each service in its local private hosted zone (serviceA.account1.aws.example.
internal). Provide this DNS record to the employees who need access (Option A).
These steps will allow service creators to register their DNS records while keeping costs low and minimizing configuration changes.

QUESTION NO: 25
ある企業では、AWS
クラウドのさまざまなアカウントに複数の本番アプリケーションがあります。同社は us-east-1
リージョンのみで運営されています。特定のパートナー企業のみがアプリケーションにアクセスできます。アプリケーションは、Application Load Balancer (ALB) の背後の Auto Scaling グループにある Amazon EC2 インスタンス上で実行されます。EC2
インスタンスはプライベート サブネット内にあり、ALB
からのトラフィックのみを許可します。ALB はパブリック サブネット内にあり、ポート 80 を超えるパートナー ネットワーク IP
アドレス範囲からの受信トラフィックのみを許可します。
企業が新しいパートナーを追加する場合、各アカウントの ALB
に関連付けられているセキュリティ グループでパートナー ネットワークの IP
アドレス範囲を許可する必要があります。ネットワーク エンジニアは、パートナー
ネットワークの IP
アドレス範囲を一元管理するソリューションを実装する必要があります。
最も運用効率の高い方法でこれらの要件を満たすソリューションはどれですか?
A. Amazon DynamoDB テーブルを作成して、更新する必要があるすべての IP
アドレス範囲とセキュリティ
グループを維持します。会社が新しいパートナーを追加したときに、新しい IP
アドレス範囲で DynamoDB テーブルを更新します。AWS Lambda
関数を呼び出して、DynamoDB テーブルから新しい IP アドレス範囲とセキュリティ
グループを読み取り、セキュリティ
グループを更新します。このソリューションをすべてのアカウントにデプロイします。
B. 新しいプレフィックス リストを作成します。許可されているすべての IP
アドレス範囲をプレフィックス リストに追加します。新しい IP
アドレス範囲がプレフィックス リストに追加されるたびに、Amazon EventBridge (Amazon CloudWatch Events) ルールを使用して AWS Lambda 関数を呼び出し、セキュリティ

グループを更新します。このソリューションをすべてのアカウントにデプロイします。
C. 新しいプレフィックス リストを作成します。許可されているすべての IP アドレス範囲をプレフィックス リストに追加します。AWS Resource Access Manager (AWS RAM) を使用して、異なるアカウント間でプレフィックス リストを共有します。パートナー IP アドレス範囲の代わりにプレフィックス リストを使用するようにセキュリティ グループを更新します。会社が新しいパートナーを追加したときに、新しい IP アドレス範囲でプレフィックス リストを更新します。
D. Amazon S3 バケットを作成して、更新する必要があるすべての IP アドレス範囲とセキュリティ グループを維持します。会社が新しいパートナーを追加したときに、新しい IP アドレス範囲で S3 バケットを更新します。AWS Lambda 関数を呼び出して、S3 バケットから新しい IP アドレス範囲とセキュリティ グループを読み取り、セキュリティ グループを更新します。このソリューションをすべてのアカウントにデプロイします。
Answer: C
Explanation:
Creating a new prefix list and adding all allowed IP address ranges to the prefix list wouldenable grouping of CIDR blocks that can be referenced in security group rules3. Sharing the prefix list across different accounts by using AWS Resource Access Manager (AWS RAM)would enable central management of the partner network IP address ranges5. Updating security groups to use the prefix list instead of the partner IP address range would enable simplification of security group rules3. Updating the prefix list with the new IP address range when the company adds a new partner would enable automatic propagation of the changes to all security groups that use the prefix list3.

QUESTION NO: 26
2 つの会社が合併します。両社は複数の VPC を備えた大規模な AWS プレゼンスを持ち、AWS ネットワーク間の接続を設計しています。両社とも、Direct Connect ゲートウェイを備えた AWS Direct Connect を使用しています。また、各社にはトランジットゲートウェイと、トランジットゲートウェイからオンプレミスのリソースへの複数の AWS サイト間 VPN 接続があります。
新しいソリューションでは、ネットワークの可視性、スループット、ログ記録、監視を最適化する必要があります。
これらの要件を満たすソリューションはどれでしょうか?
A. 各社のトランジットゲートウェイ間のサイト間 VPN 接続を設定し、それぞれのネットワーク間の到達可能性を確立します。すべての VPC の VPC フローログを設定します。フローログを Amazon CloudWatch に公開します。VPC Reachability Analyzer を使用して接続を監視します。
B. 各社のトランジットゲートウェイ間のサイト間 VPN 接続を設定し、それぞれのネットワーク間の到達可能性を確立します。すべての VPC の VPC フローログを設定します。フローログを Amazon CloudWatch に公開します。AWS Transit Gateway Network Manager を使用して、トランジットゲートウェイとそれぞれの接続を監視します。
C.
各社のトランジットゲートウェイ間のトランジットゲートウェイピアリングを設定します。

すべての VPC の VPC フローログを設定します。フローログを Amazon CloudWatch に公開します。VPC Reachability Analyzer を使用して接続を監視します。

D.
各社のトランジットゲートウェイ間のトランジットゲートウェイピアリングを設定します。すべての VPC の VPC フローログを設定します。フローログを Amazon CloudWatch に公開します。AWS Transit Gateway Network Manager を使用して、トランジットゲートウェイ、それぞれの接続、およびトランジットゲートウェイピアリングリンクを監視します。

Answer: D

QUESTION NO: 27
開発チームは、AWS クラウドで新しい Web アプリケーションを構築しています。会社のメインドメイン example.com は現在、会社の実稼働 AWS アカウントの 1 つにある Amazon Route 53 パブリックホストゾーンでホストされています。
開発者は、example.com ドメインの下のパブリックに解決可能なサブドメインを使用して、必要に応じて DNS レコードを作成および削除し、会社のステージング AWS アカウントで Web アプリケーションをテストしたいと考えています。開発者はステージング アカウント内の Route 53 ホストゾーンに完全にアクセスできますが、本番環境の AWS アカウントのリソースにアクセスすることはできません。
開発者が example.com ドメインの下にレコードを作成できるようにするには、ネットワークエンジニアがどの手順の組み合わせを実行する必要がありますか? (2 つ選択してください。)

A. ステージング アカウントに example.com のパブリック ホストゾーンを作成します。

B. example.com ドメインに staging.example.com NS レコードを作成します。staging.example.com ドメインのネームサーバーを値に入力します。ルーティング ポリシー タイプをシンプル ルーティングに設定します。

C. ステージング アカウントに stagmg.example.com のプライベートホストゾーンを作成します。

D. staging.example.com ドメインに example.com NS レコードを作成します。example.com ドメインのネームサーバーを値に入力します。ルーティングポリシーの種類をシンプルルーティングに設定します。

E. ステージング アカウントに staging.example.com のパブリックホストゾーンを作成します。

Answer: B E
Explanation:
When a client queries a DNS server for a domain name, the DNS server typically starts by looking for NS records to determine which name servers are authoritative for the domain. The DNS server then queries the authoritative name servers to obtain the information about the domain that the client requested. For example, suppose you own the domain example.com, but you want to delegate control of the subdomain sub.example.
com to a different set of name servers. You would create NS records in the example.com

zone file that point to the name servers for sub.example.com. This tells DNS servers that the name servers for sub.example.com are authoritative for that subdomain, and they should query those name servers for any requests related to sub.
example.com.

QUESTION NO: 28
ある企業は、Application Load Balancer (ALB) の背後にある Amazon EC2 インスタンスで Web アプリケーションをホストしています。ALB は、Amazon CloudFront
ディストリビューションのオリジンです。同社は、認証された顧客にトークンを提供するカスタム認証システムを実装したいと考えています。
Web アプリケーションは、コンテンツを配信する前に、GET/POST
リクエストが認証された顧客からのものであることを確認する必要があります。ネットワーク エンジニアは、Web
アプリケーションが許可された顧客を識別できるように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最も運用効率の高いソリューションは何ですか?
A. ALB を使用して、GET/POST リクエスト
ペイロード内の承認されたトークンを検査します。AWS Lambda
関数を使用してカスタマイズされたヘッダーを挿入し、認証された顧客リクエストを Web アプリケーションに通知します。
B. AWS WAF を ALB と統合して、GET/POST リクエスト
ペイロード内の承認されたトークンを検査します。カスタマイズされたヘッダーを挿入して、認証された顧客リクエストを Web アプリケーションに通知するように ALB
リスナーを構成します。
C. AWS Lambda@Edge 関数を使用して、GET/POST リクエスト
ペイロード内の承認されたトークンを検査します。Lambda@Edge
関数を使用して、認証された顧客リクエストを Web
アプリケーションに通知するカスタマイズされたヘッダーを挿入することもできます。
D. GET/POST リクエスト
ペイロード内の承認されたトークンを検査するサードパーティのパケット検査ツールを備えた EC2
インスタンスをセットアップします。カスタマイズされたヘッダーを挿入して、認証された顧客リクエストを Web アプリケーションに通知するようにツールを構成します。
Answer: C

QUESTION NO: 29
ある企業は最近、AWS Client VPN を導入し、リモートユーザーが複数のピアリングされた VPC
内のリソースと自社のオンプレミスデータセンター内のリソースにアクセスできるようにしました。Client VPN エンドポイントのルートテーブルには、0.0.0.0/0 というエントリが 1 つだけあります。Client VPN
エンドポイントは、インバウンドルールのない新しいセキュリティグループと、0.0.0.0/0 へのすべてのトラフィックを許可する単一のアウトバウンドルールを使用しています。
複数のユーザーから、Web
検索結果にユーザーの地理的位置情報がかなり誤って表示されているとの報告があります。

サービスの中断を最小限に抑えながらこの問題を解決するために、ネットワーク
エンジニアはどのような手順の組み合わせを実行する必要がありますか? (3
つ選択してください。)
A. ユーザーを AWS サイト間 VPN に切り替えます。
B. クライアント VPN エンドポイントでスプリット トンネル オプションを有効にします。
C. ピアリングされた VPC とオンプレミスのデータセンターのルートをクライアント VPN
ルートテーブルに追加します。
D. クライアント VPN エンドポイントが使用するセキュリティ グループから 0.0.0.0/0
送信ルールを削除します。
E. 別の VPC でクライアント VPN エンドポイントを削除して再作成します。
F. クライアント VPN エンドポイント ルート テーブルから 0.0.0.0/0
エントリを削除します。
Answer: B C F