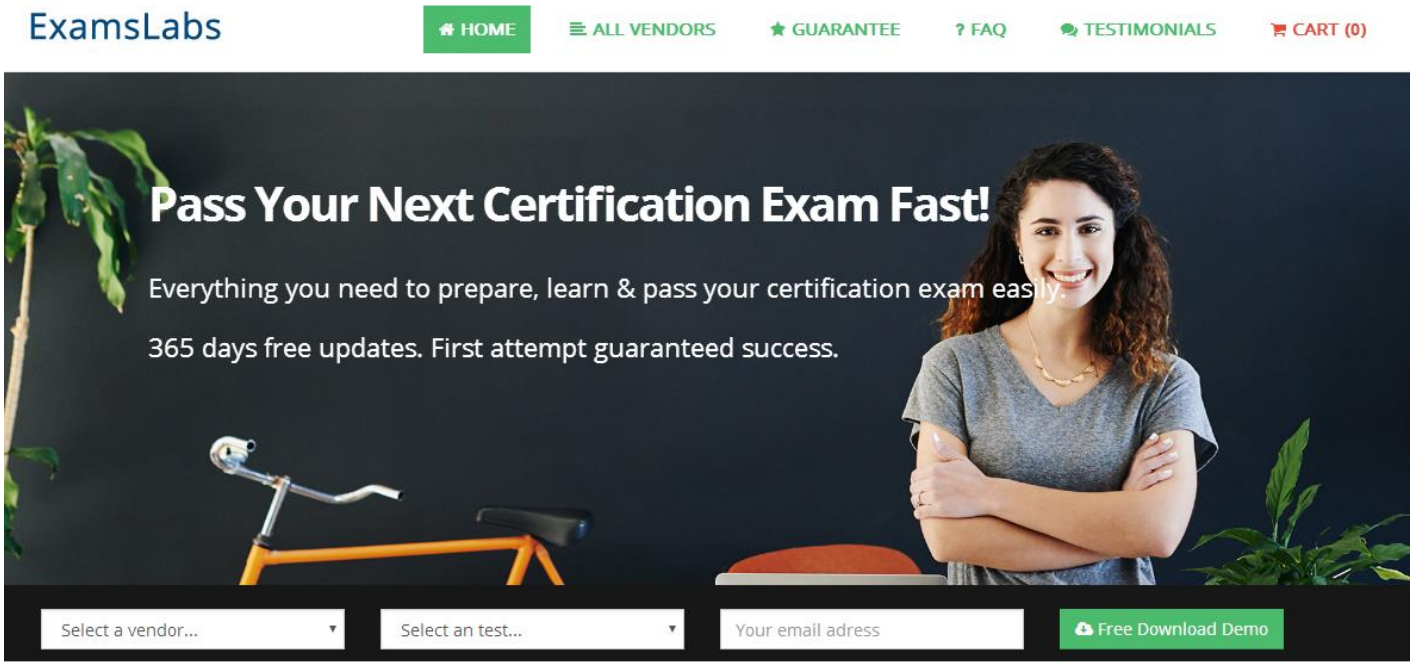
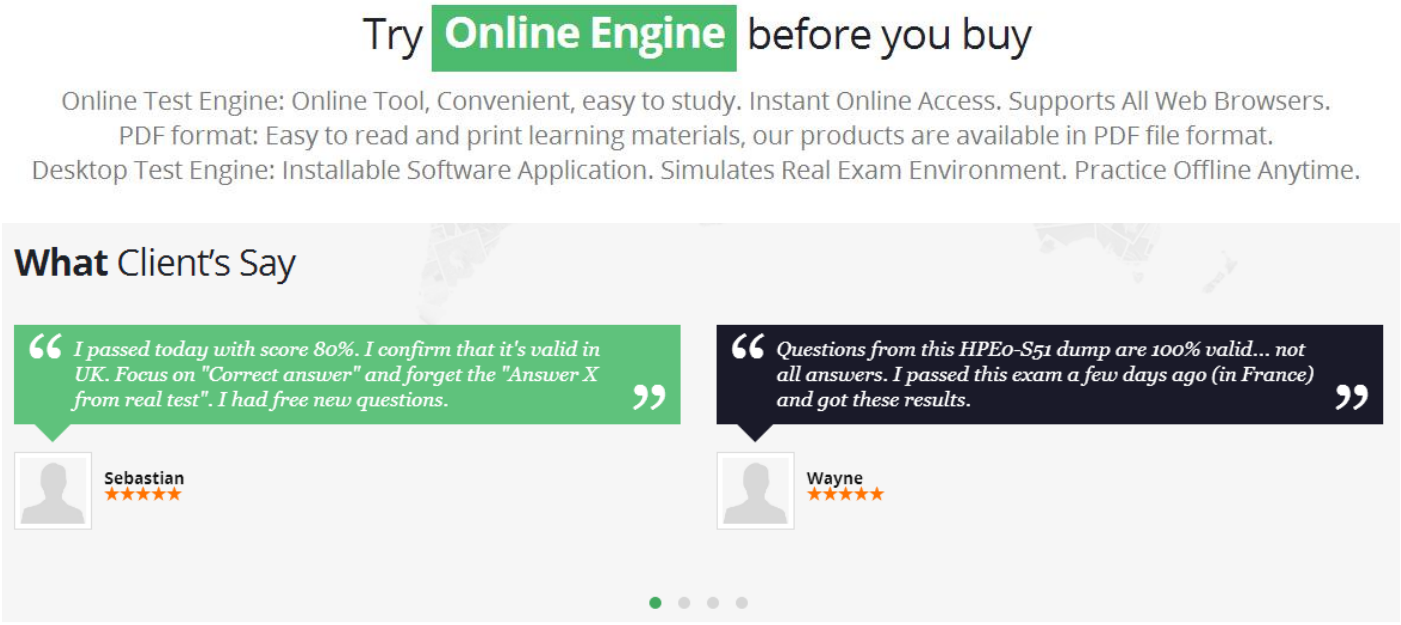
ExamsLabs





http://www.examslabs.com/

Latest Study Materials, Valid Dumps - ExamsLabs

Exam : **Professional-Cloud-Network-Engineer-JPN**

Title : Google Cloud Certified - Professional Cloud Network Engineer (Professional-Cloud-Network-Engineer日本語版)

Vendor : Google

Version : DEMO

QUESTION NO: 1
新しいGKE標準クラスタを作成しています。GKEノードの送信元IPを使用して、ポッドが192.168.0.0/24サブネット内のGoogle
Cloud内の他のVMにアクセスできるように、クラスタを構成する必要があります。どうすればよいでしょうか？
A. Q GKE PodのIPアドレス範囲を10.0.0.0/8に設定します。-disable-def ault-snatフラグを設定します。
B. Q GKE PodのIPアドレス範囲を10.0.0.0/8に収まるように設定してください。-disable-default-snatフラグは設定しないでください。
C. Q GKE PodのIPアドレス範囲を10.0.0.0/8に収まらない範囲に設定してください。-disable- default-snatフラグは設定しないでください。
D. Q 10.0.0.0/8 に収まらない GKE Pod の IP アドレス範囲を設定します。-disable-default-snat フラグを設定します。
Answer: A
Explanation:
By default, GKE uses SNAT (Source Network Address Translation) for pod egress traffic to destinations outside the cluster's IP ranges but within RFC 1918 private IP ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0
/16). This means that traffic from pods leaving the cluster for these private IP destinations will have their source IP address translated to the node's IP address.
To ensure pods can reach VMs in the 192.168.0.0/24 subnet using the source IP of the GKE nodes, you want the default SNAT behavior to apply to this destination. The default SNAT rule applies when the destination is an RFC 1918 address and the source is a pod IP that is not within the same RFC 1918 range as the destination (e.g., if your pods are in a 10.x.x.x range and the destination is 192.168.x.x).
Therefore, you should:
Set a GKE pod IP address range that fits in 10.0.0.0/8: This ensures that the pod IPs are within an RFC 1918 range different from 192.168.0.0/24.
Do NOT configure the --disable-default-snat flag: If you disable default SNAT, pods would use their own IP addresses as source IPs, which might not be routable to the 192.168.0.0/24 subnet unless specific routes are configured. The goal is to use the node's IP.
The combination of having pod IPs in a different RFC 1918 range and not disabling default SNAT ensures that GKE performs SNAT, making the node's IP the source for traffic destined for the 192.168.0.0/24 subnet.
Exact Extract:
"By default, GKE performs SNAT (Source Network Address Translation) for egress traffic from pods to destinations outside the cluster's IP address ranges but within the private IP address ranges defined in RFC
1918 (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16). When SNAT occurs, the source IP address of the egress packets is the node's IP address instead of the pod's IP address."
"The --disable-default-snat flag, when used, disables this default SNAT behavior. If you want traffic to use the node's IP as the source when reaching internal RFC 1918 destinations, do not set this flag."Reference:
Google Kubernetes Engine Documentation - IP masquerade agent, Private IP addresses for GKE Pods and Services

QUESTION NO: 2
Compute Engine 上で実行されているアプリケーションがあり、BigQuery を使用して結果を生成し、Cloud Storage に保存しています。どのアプリケーション インスタンスも外部 IP アドレスを持たないようにしたいと考えています。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
A. すべてのサブネットで限定公開の Google アクセスを有効にします。
B. VPC でプライベート Google アクセスを有効にします。
C. VPC でプライベート サービス アクセスを有効にします。
D. VPC と BigQuery の間にネットワーク ピアリングを作成します。
E. クラウド NAT を作成し、NAT ゲートウェイ経由でアプリケーション トラフィックをルーティングします。
Answer: A E
Explanation:
https://cloud.google.com/nat/docs/overview#interaction-pga Specifications
https://cloud.google.com/vpc/docs
/configure-private-google-access#specifications

QUESTION NO: 3
あなたの会社では、各部門の親フォルダーとサブフォルダーを含むリソース階層を定義しています。各部門は、割り当てられたフォルダ内でそれぞれのプロジェクトと VPC を定義し、Google Cloud ファイアウォール ルールを作成するための適切な権限を持っています。VPC 間でトラフィックが流れることを許可してはなりません。他の VPC を含むあらゆる送信元からのすべてのトラフィックをブロックし、VPC 内のファイアウォール ルールのみをそれぞれの部門に委任する必要があります。あなたは何をするべきか ?
A. 各 VPC に VPC ファイアウォール ルールを作成し、優先度 0 で任意の送信元からのトラフィックをブロックします。
B. 各 VPC に VPC ファイアウォール ルールを作成し、優先度 1000 であらゆる送信元からのトラフィックをブロックします。
C. 部門のフォルダーごとに 2 つの階層型ファイアウォール ポリシーを作成し、それぞれに 2 つのルールを作成します。1 つはそれぞれの VPC に割り当てられたプライベート CIDR からのトラフィックと一致し、アクションを許可するように設定する優先度の高いルール、もう 1 つはブロックする優先度の低いルールです。他のソースからのトラフィック。
D. 部門のフォルダーごとに 2 つの階層型ファイアウォール ポリシーを作成し、それぞれに 2 つのルールを作成します。1 つはそれぞれの VPC に割り当てられたプライベート CIDR からのトラフィックと一致し、アクションを goto_next に設定する優先度の高いルール、もう 1 つはブロックする優先度の低いルールです。他のソースからのトラフィック。
Answer: B

QUESTION NO: 4
サブネット レベルの分離を提供するには、あるサブネットのインスタンス A が、別のサブネットのインスタンス B と呼ばれるセキュリティ

アプライアンスを経由するようにルーティングする必要があります。
あなたは何をするべきか？
A. システム生成のサブネット ルートよりも具体的なルートを作成し、ネクスト ホップをタグなしでインスタンス B に向けます。
B. システム生成のサブネット ルートよりも具体的なルートを作成し、インスタンス A に適用されたタグを使用してネクスト ホップをインスタンス B に向けます。
C. システム生成のサブネット ルートを削除し、インスタンス A に適用されたタグを使用してインスタンス B への特定のルートを作成します。
D. インスタンス B を別の VPC に移動し、マルチ NIC を使用してインスタンス B のインターフェイスをインスタンス A のネットワークに接続します。トラフィックがインスタンス A に強制的に通過するように適切なルートを構成します。
Answer: B

QUESTION NO: 5
Google Cloud 内に HA VPN をデプロイしています。オンプレミス ゲートウェイと Google Cloud の間でルートを動的に交換する必要があります。HA VPN ゲートウェイとピア VPN ゲートウェイ リソースはすでに作成されています。何をすればよいでしょうか。
A. Cloud Router を作成し、VPN トンネルを追加して、BGP セッションを構成します。
B. 2 番目の HA VPN ゲートウェイを作成し、VPN トンネルを追加して、グローバル動的ルーティングを有効にします。
C. Cloud Router を作成し、VPN トンネルを追加して、グローバル動的ルーティングを有効にします。
D. Cloud Router を作成し、VPN トンネルを追加して、サブネット範囲への静的ルートを構成します。
Answer: A
Explanation: To dynamically exchange routes between Google Cloud and your on-premises gateway, you need to create a Cloud Router and configure BGP sessions after adding VPN tunnels. BGP allows for dynamic route exchange, which is essential for establishing proper communication between the environments.
Google Cloud HA VPN with BGP

QUESTION NO: 6
質問：
会社の現在のネットワーク アーキテクチャには、3 つの VPC Service Controls 境界があります。
* 本番環境のストレージバケットを保護するための 1 つの境界 (PERIMETER_PROD)
* 非本番環境のストレージバケットを保護するための 1 つの境界 (PERIMETER_NONPROD)
* 単一の VPC (VPC_ONE) を含む 1 つの境界 (PERIMETER_VPC)
この単一の VPC (VPC_ONE) では、IP_RANGE_PROD は本番環境ワークロードのサブネット専用であり、IP_RANGE_NONPROD は非本番環境ワークロードのサブネット専用です。これら 2 つの範囲外にワークロードを作成することはできません。最小限のセットアップ作業で、本番環境ワークロードが本番環境ストレージ バケットにのみアクセスでき、非本番環境ワークロードが非本番環境ストレージ

バケットにのみアクセスできるようにする必要があります。どうすればよいでしょうか?
A. IP_RANGE_PROD 境界と IP_RANGE_NONPROD 境界を使用して 2 つのアクセス レベルを作成し、各アクセス レベルが単一の範囲を参照する設計を開発します。2 つのイングレス アクセス ポリシーを作成し、各アクセス ポリシーが 2 つのアクセス レベルのいずれかを参照するようにします。PERIMETER_PROD 境界と PERIMETER_NONPROD 境界を更新します。
B. PERIMETER_VPC 境界を削除する設計を開発します。PERIMETER_NONPROD 境界を更新して、VPC_ONE を含むプロジェクトを含めます。PERIMETER_PROD 境界を削除します。
C. VPC_ONE と同じプロジェクトに新しい VPC (VPC_NONPROD) を作成する設計を開発します。
すべての非本番環境ワークロードを VPC_ONE から PERIMETER_NONPROD 境界に移行します。
PERIMETER_VPC 境界を削除します。PERIMETER_PROD 境界を更新して VPC_ONE を含め、PERIMETER_NONPROD 境界を更新して VPC_NONPROD を含めます。
D. PERIMETER_VPC 境界を削除する設計を開発します。PERIMETER_PROD 境界を更新して、VPC_ONE を含むプロジェクトを含めます。PERIMETER_NONPROD 境界を削除します。
Answer: A
Explanation:
Using IP range-based access levels for VPC Service Controls allows segmentation of production and non- production resources within the same VPC. By creating separate access levels and ingress policies for each IP range, you ensure that only production subnets access production buckets and non-production subnets access non-production buckets, providing the required isolation.
Reference: Google Cloud - VPC Service Controls and Access Levels

QUESTION NO: 7
オンプレミスと GCP の間で Cloud VPN の使用量が増加しており、単一のトンネルで処理できるより多くのトラフィックをサポートしたいと考えています。Cloud VPN を使用して利用可能な帯域幅を増やしたいと考えています。
あなたは何をするべきか ?
A. オンプレミス VPN ゲートウェイの MTU を 1460 バイトから 2920 バイトに 2 倍にします。
B. 同じ Cloud VPN ゲートウェイ上に、同じ宛先 VPN ゲートウェイ IP アドレスを指す 2 つの VPN トンネルを作成します。
C. 別のパブリック IP アドレスを持つ 2 番目のオンプレミス VPN ゲートウェイを追加します。既存の Cloud VPN ゲートウェイ上に 2 番目のトンネルを作成します。このトンネルは同じ IP 範囲を転送しますが、新しいオンプレミス ゲートウェイ IP をポイントします。
D. 既存の VPN ゲートウェイとは異なるリージョンに 2 番目の Cloud VPN ゲートウェイを追加します。2 番目の Cloud VPN ゲートウェイ上に、同じ IP 範囲を転送するが、既存のオンプレミス VPN ゲートウェイの IP

アドレスを指す新しいトンネルを作成します。
Answer: C
Explanation:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#redundancy-options

QUESTION NO: 8
Web サービス チームへの ID
およびアクセス管理の権限と電子メールの配布をできるだけ効率的に一元管理する必要があります。
あなたは何をするべきか？
A. Web サービス チームの Google グループを作成します。
B. Web サービス チーム用の G Suite ドメインを作成します。
C. Web サービス チーム用に新しい Cloud Identity ドメインを作成します。
D. WebServices チームのすべてのメンバーに対して新しいカスタム ロールを作成します。
Answer: A

QUESTION NO: 9
あなたは、Google Cloud への移行を進めている大学で働いています。
クラウドの要件は次のとおりです。
10 Gbps によるオンプレミス接続
クラウドへの最小遅延アクセス
集中ネットワーク管理チーム
新しい部門は、プロジェクトへのオンプレミス接続を求めています。キャンパスを Google Cloud
に接続するために、最もコスト効率の高い相互接続ソリューションをデプロイしたいと考えています。
あなたは何をするべきか？
A. 共有 VPC を使用し、VLAN アタッチメントと Dended Interconnect をホスト プロジェクトにデプロイします。
B. 共有 VPC を使用し、サービス プロジェクトに VLAN アタッチメントをデプロイします。VLAN アタッチメントを共有 VPC のホスト プロジェクトに接続します。
C. スタンドアロン プロジェクトを使用し、個々のプロジェクトに VLAN アタッチメントを展開します。VLAN アタッチメントをスタンドアロン プロジェクトの専用インターコネクトに接続します。
D. スタンドアロン プロジェクトを使用し、個々のプロジェクトのそれぞれに VLAN アタッチメントと専用インターコネクトを展開します。
Answer: A

QUESTION NO: 10
Google Kubernetes Engine (GKE) にデプロイされたアプリケーションに新しい Cloud Armor ポリシーを適用したいと考えています。Cloud Armor
ポリシーにどのターゲットを使用するかを調べたいと考えています。
どの GKE リソースを使用する必要がありますか?

A. GKE ノード
B. GKE ポッド
C. GKE クラスタ
D. GKE Ingress
Answer: D
Explanation:
Cloud Armour is applied at load balancers Configuring Google Cloud Armor through Ingress. https://cloud.
google.com/kubernetes-engine/docs/how-to/ingress-features Security policy features Google Cloud Armor security policies have the following core features: You can optionally use the QUIC protocol with load balancers that use Google Cloud Armor. You can use Google Cloud Armor with external HTTP(S) load balancers that are in either Premium Tier or Standard Tier. You can use security policies with GKE and the default Ingress controller.

QUESTION NO: 11
デフォルトの Virtual Private Cloud (VPC) 内の仮想マシン (VM) の 1 つがサービス拒否攻撃を受けている疑いがあります。トラフィックの送信元を理解するには、VM の受信トラフィックを分析する必要があります。あなたは何をするべきか？
A. VPC のデータアクセス監査ログを有効にします。ログを分析し、subnetworks.get フィールドから送信元 IP アドレスを取得します。
B. サブネットの VPC フロー ログを有効にします。ログを分析し、接続フィールドから送信元 IP アドレスを取得します。
C. VPC の VPC フロー ログを有効にします。ログを分析し、src_location フィールドから送信元 IP アドレスを取得します。
D. サブネットのデータ アクセス監査ログを有効にします。ログを分析し、networks.get フィールドから送信元 IP アドレスを取得します。
Answer: B

QUESTION NO: 12
あなたの組織には、デフォルトの VPC 構成を使用する us-east1、us-west4、europe-west4 のサブネットを持つ Google Cloud Virtual Private Cloud (VPC) があります。ヨーロッパの支社の従業員は、HA VPN を使用して VPC 内のリソースにアクセスする必要があります。europe-west4 にデプロイされた Cloud Router を使用して、組織の Google Cloud VPC に関連付けられた HA VPN を構成しました。ブランチ オフィスのユーザーが VPC 内のすべてのリソースに迅速かつ簡単にアクセスできるようにする必要があります。あなたは何をするべきか？
A. サブネットごとにカスタムのアドバタイズされたルートを作成します。
B. Cloud VPN を使用してブランチ オフィスに接続するように各サブネットの VPN 接続を構成します。
C. VPC 動的ルーティング モードをグローバルに設定します。
D. Cloud Router のアドバタイズされたルートをグローバルに設定します。
Answer: C

QUESTION NO: 13
Cloud VPN を介してオンプレミス ネットワークと VPC の間に IPSec
トンネルを実装したいと考えています。トンネル経由の到達可能性を特定のローカル
サブネットに制限する必要がありますが、ボーダー ゲートウェイ プロトコル (BGP)
を通信できるデバイスがありません。
どのルーティング オプションを選択する必要がありますか?
A. Cloud Router を使用した動的ルーティング
B. デフォルトのトラフィック セレクターを使用したルートベースのルーティング
C. カスタム ローカル トラフィック セレクターを使用したポリシーベースのルーティング
D. デフォルトのローカル トラフィック
セレクターを使用したポリシーベースのルーティング
Answer: C
Reference: https://cloud.google.com/vpn/docs/concepts/overview

QUESTION NO: 14
あなたは、新しいプライベート Google Kubernetes Engine (GKE) クラスターの IP アドレス
スキームを設計しています。企業内の RFC 1918 アドレス空間の IP
アドレスが枯渇したため、新しいダスターにはプライベートに使用されるパブリック IP
空間を使用する予定です。Google
が推奨するプラクティスに従いたいと考えていますが、IP
スキームを設計した後は何をすべきですか?
A. クラスターに使用可能な最小限の RFC 1918 プライマリおよびセカンダリ サブネット IP
範囲を作成します。複数のプライベート GKE クラスタにわたってポッドのセカンダリ
アドレス範囲を再利用します。
B. クラスタに使用可能な最小限の RFC 1918 プライマリおよびセカンダリ サブネット IP
範囲を作成します。複数のプライベート GKE クラスタにわたるサービスのセカンダリ
アドレス範囲を再利用します。
C. クラスター用にプライベートに使用されるパブリック IP
のプライマリおよびセカンダリのサブネット範囲を作成します。--enab1e-ip-a1ias と
--enable-private-nodes のオプションを選択して、プライベート GKE
クラスタを作成します。
D. クラスター用にプライベートに使用されるパブリック IP
のプライマリおよびセカンダリのサブネット範囲を作成します。次のオプションを選択し、
- siable-default-snat、--enable-ip-alias、および -enable-private-nodes
を使用して、プライベート GKE クラスタを作成します。
Answer: D
Explanation:
The correct answer is D. Create privately used public IP primary and secondary subnet ranges for the clusters.
Create a private GKE cluster with the following options selected: --disable-default-snat, --enable-ip-alias, and
--enable-private-nodes.
This answer is based on the following facts:
* Privately used public IP (PUPI) addresses are any public IP addresses not owned by

Google that a customer can use privately on Google Cloud1. You can use PUPI addresses for GKE pods and services in private clusters to mitigate address exhaustion.
* A private GKE cluster is a cluster that has no public IP addresses on the nodes2. You can use private clusters to isolate your workloads from the public internet and enhance security.
* The --disable-default-snat option disables source network address translation (SNAT) for the cluster3.
This option allows you to use PUPI addresses without conflicting with other public IP addresses on the internet.
* The --enable-ip-alias option enables alias IP ranges for the cluster4. This option allows you to use separate subnet ranges for nodes, pods, and services, and to specify the size of those ranges.
* The --enable-private-nodes option enables private nodes for the cluster5. This option ensures that the nodes have no public IP addresses and can only communicate with other Google Cloud resources in the same VPC network or peered networks.
The other options are not correct because:
* Option A is not suitable. Creating RFC 1918 primary and secondary subnet IP ranges for the clusters does not solve the problem of address exhaustion. Re-using the secondary address range for pods across multiple private GKE clusters can cause IP conflicts and routing issues.
* Option B is also not suitable. Creating RFC 1918 primary and secondary subnet IP ranges for the clusters does not solve the problem of address exhaustion. Re-using the secondary address range for services across multiple private GKE clusters can cause IP conflicts and routing issues.
* Option C is not feasible. Creating privately used public IP primary and secondary subnet ranges for the clusters is a valid step, but creating a private GKE cluster with only --enable-ip-alias and --enable- private-nodes options is not enough. You also need to disable default SNAT to avoid IP conflicts with other public IP addresses on the internet.

QUESTION NO: 15
パブリック IP アドレス経由で Cloud SQL にアクセスでき、サードパーティのサービス プロバイダを必要としない、Google への専用接続を確立したいと考えています。
どの接続タイプを選択する必要がありますか?
A. キャリアピアリング
B. ダイレクトピアリング
C. 専用インターコネクト
D. パートナー相互接続
Answer: B
Explanation:
When established, Direct Peering provides a direct path from your on-premises network to Google services, including Google Cloud products that can be exposed through one or more public IP addresses. Traffic from Google's network to your on-premises network also takes that direct path, including traffic from VPC networks in your projects. Google Cloud customers must request that direct egress pricing be enabled for each of their projects after they have established Direct Peering with Google. For more information, see Pricing.
Reference: https://cloud.google.com/interconnect/docs/how-to/direct-peering

QUESTION NO: 16
あなたの組織は、Virtual Private Cloud (VPC) 内の重要な Compute Engine インスタンスでハブアンドスポーク アーキテクチャを使用しています。あなたは、Google Cloud の Cloud DNS の設計を担当します。オンプレミスのデータセンターから Cloud DNS プライベート ゾーンを解決し、ハブアンドスポーク VPC 設計からオンプレミスの名前解決を有効にできる必要があります。あなたは何をするべきか？
A. ハブ VPC でプライベート DNS ゾーンを構成し、オンプレミス サーバーへの DNS 転送を構成します。
スポーク VPC からハブ VPC への DNS ピアリングを構成します。
B. ハブ VPC で DNS ポリシーを構成し、スポーク VPC からの受信クエリの転送を許可します。
プライベート ゾーンを使用してスポーク VPC を構成し、ハブ VPC への DNS ピアリングを設定します。
C. スポーク VPC で DNS ポリシーを構成し、オンプレミス DNS を代替 DNS サーバーとして構成します。
プライベート ゾーンを使用してハブ VPC を構成し、各スポーク VPC への DNS ピアリングを設定します。
D. ハブ VPC で DNS ポリシーを構成し、オンプレミス DNS を代替 DNS サーバーとして構成します。
プライベート ゾーンを使用してスポーク VPC を構成し、ハブ VPC への DNS ピアリングを設定します。
Answer: C

QUESTION NO: 17
あなたの会社は人気のあるゲーム サービスを提供しています。インスタンスはプライベート IP アドレスを使用してデプロイされ、外部アクセスはグローバル ロード バランサーを通じて許可されます。潜在的な悪意のある攻撃者を特定したと考えていますが、正しいクライアント IP アドレスを持っているかどうかはわかりません。正規ユーザーへの混乱を最小限に抑えながら、この攻撃者を特定したいと考えています。
あなたは何をするべきか？
A. トラフィックを拒否する Cloud Armor ポリシー ルールを作成し、必要なログを確認します。
B. トラフィックを拒否する Cloud Armor ポリシー ルールを作成し、プレビュー モードを有効にし、必要なログを確認します。
C. トラフィックを拒否する VPC ファイアウォール ルールを作成し、ログ記録を有効にして強制を無効に設定し、必要なログを確認します。
D. トラフィックを拒否する VPC ファイアウォール ルールを作成し、ログ記録を有効にして強制を有効に設定し、必要なログを確認します。
Answer: B
Explanation:
https://cloud.google.com/armor/docs/security-policy-concepts#preview_mode

QUESTION NO: 18
あなたの会社の Google Cloud にデプロイされたストリーミング
アプリケーションは、複数の言語をサポートしています。アプリケーション開発チームから、オーディオとビデオのトラフィックをさまざまなバックエンドの Google Cloud
ストレージ
バケットに分割することをどのようにサポートすべきかという質問がありました。彼らは URL
マップを使用し、運用上のオーバーヘッドを最小限に抑えたいと考えています。現在、次のディレクトリ構造を使用しています。
/fr/ビデオ
/in/ビデオ
/en/ビデオ
/../ビデオ
/fr/オーディオ
/オーディオで
/en/オーディオ
/../オーディオ
どのソリューションをお勧めしますか?
A. ディレクトリ構造を再配置し、URL マップを作成し、/video/* や /audio/* などのパス ルールを活用します。
B. ディレクトリ構造を再配置し、ビデオとオーディオの DNS
ホスト名エントリを作成し、/video/* や /audio/* などのパス ルールを利用します。
C. ディレクトリ構造をそのままにして、URL マップを作成し、\/[az]{2}\/video などのパス ルールを利用します。
\/[az]{2}\/オーディオ。
D. ディレクトリ構造をそのままにして、URL マップを作成し、/*/video や /*/ audio などのパス ルールを利用します。
Answer: A
Explanation:
https://cloud.google.com/load-balancing/docs/url-map#configuring_url_maps Path matcher constraints Path matchers and path rules have the following constraints: A path rule can only include a wildcard character (*) after a forward slash character (/). For example, /videos/* and /videos/hd/* are valid for path rules, but /videos* and /videos/hd* are not. Path rules do not use regular expression or substring matching. For example, path rules for either /videos/hd or /videos/hd/* do not apply to a URL with the path /video/hd-abcd. However, a path rule for /video/* does apply to that path. https://cloud.google.com
/load-balancing/docs/url-map-concepts#pm-constraints

QUESTION NO: 19
ポート 80、8080、および 443 を使用して、IPv4 と IPv6 の両方の仮想 IP
アドレスの背後で外部に公開される新しい HTTP アプリケーションを構成しています。us-west1 と us-east1 の 2
つのリージョンにバックエンドがあります。高可用性と自動スケーリングを確保しながら、可能な限り低い遅延でコンテンツを提供し、HTTP ホスト名とリクエスト
パスを使用してネイティブ コンテンツ

ベースのルールを作成したいと考えています。ロード バランサーに接続するクライアントの IP
アドレスは、バックエンドから認識できる必要があります。どの構成を使用する必要がありますか?
A. ネットワーク負荷分散を使用する
B. PROXY プロトコルを有効にして TCP プロキシ ロード バランシングを使用します。
C. URL マップとカスタム ヘッダーを使用して外部 HTTP(S) 負荷分散を使用する
D. URL マップと X-Forwarded-For ヘッダーを使用した外部 HTTP(S) ロード
バランシングを使用する
Answer: D

QUESTION NO: 20
Cloud CDN でプライベート Cloud Storage バケットでホストされている
https://www.example.com/images/spacetime.png
静的画像ファイルを提供する必要がある場合 VSE ORIG.-X_NZADERS キャッシュ
モードを使用している場合 HTTP を受信する場合ファイルを開くときに 403
エラーが発生する ブラウザで、HTTP 応答に Cache-control: private, max-age=O
ヘッダーがあることがわかります。この問題はどのように修正すればよいでしょうか?
A. Storage Legacy Object Reader ロールを付与する Cloud Storage
バケット権限を構成します。
B. キャッシュ モードを変更して、すべてのコンテンツをキャッシュします。
C. バックエンド サービスのデフォルトの存続期間 (TTL) を増やします。
D. バックエンド バケットのネガティブ キャッシュを有効にする
Answer: A
Explanation:
The correct answer is A. Configure a Cloud Storage bucket permission that gives the Storage Legacy Object Reader role.
This answer is based on the following facts:
* Cloud CDN can serve private content from Cloud Storage buckets, but you need to grant the appropriate permissions to the Google-managed service account that represents your load balancer1.
* The Storage Legacy Object Reader role grants read access to objects in a bucket2.
* The Cache-control: private header indicates that the object is not publicly readable and requires authentication3.
* The USE_ORIGIN_HEADERS cache mode instructs Cloud CDN to cache responses based on the Cache-Control and Expires headers from the origin server4. Changing the cache mode, increasing the TTL, or enabling negative caching will not affect the 403 error.

QUESTION NO: 21
あなたの会社は人気のあるゲーム サービスを提供しています。インスタンスはプライベート IP アドレスを使用してデプロイされ、外部アクセスはグローバル ロード
バランサーを通じて許可されます。最近トラフィック スクラビング
サービスを利用しており、トラフィック スクラビング
サービスからの接続のみを許可するようにオリジンを制限したいと考えています。
あなたは何をするべきか ?

A. トラフィック スクラブ サービスを除くすべてのトラフィックをブロックする Cloud Armor セキュリティ ポリシーを作成します。
B. トラフィック スクラブ サービスを除くすべてのトラフィックをブロックする VPC ファイアウォール ルールを作成します。
C. トラフィック スクラブ サービスを除くすべてのトラフィックをブロックする VPC サービス コントロール境界を作成します。
D. トラフィック スクラビング サービスを除くすべてのトラフィックをブロックする IPTables ファイアウォール ルールを作成します。
Answer: A
Explanation:
Global load balancer will proxy the connection . thus no trace of session origin IP. you should use Cloud Armor to geofence your service.
https://cloud.google.com/load-balancing/docs/https

QUESTION NO: 22
マネージド インスタンス
グループで実行されているアプリケーションがあります。開発チームは、十分にテストされていない新機能を含む更新されたインスタンス
テンプレートをリリースしました。新しいテンプレートにバグがある場合、ユーザーへの影響を最小限に抑えたいと考えています。
インスタンスをどのように更新すればよいでしょうか?
A. 一部のインスタンスに手動でパッチを適用し、インスタンス
グループでローリング再起動を実行します。
B. 新しいインスタンス テンプレートを使用して、インスタンス
グループ内のすべてのインスタンスに対してローリング
アップデートを実行します。ロールアウトが完了したら、新機能を確認します。
C. 新しいインスタンス
グループをデプロイし、そのグループ内の更新されたテンプレートをカナリアします。新しい Canary インスタンス グループの新機能を確認し、元のインスタンス
グループを更新します。
D. ローリング
アップデートを開始し、インスタンスが新しいテンプレートを受信するためのターゲット サイズを指定することにより、カナリア アップデートを実行します。Canary
インスタンスで新しい機能を確認し、残りのインスタンスにロールフォワードします。
Answer: D
Explanation:
https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance- groups#starting_a_canary_update
https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

QUESTION NO: 23
Partner Interconnect 接続をプロビジョニングして、オンプレミス データセンターから Google Cloud への接続を拡張しました。Cloud Router を構成し、VPC

内のリソースに接続するための VLAN アタッチメントを作成する必要があります。関連する Cloud Router で使用する自律システム番号（ASN）を構成し、VLAN アタッチメントを作成する必要があります。
あなたは何をするべきか？
A. 4 バイトのプライベート ASN 4200000000-4294967294 を使用します。
B. 2 バイトのプライベート ASN 64512-65535 を使用します。
C. 公開されている Google ASN 15169 を使用します。
D. パブリック Google ASN 16550 を使用します。
Answer: B

QUESTION NO: 24
あなたは、GCP への移行を進めている多国籍企業に勤めています。
クラウドの要件は次のとおりです。
* 米国のオレゴン州とニューヨークにあるオンプレミス データ センターで、クラウド リージョン us-west1 (プライマリ本社) と us-east4 (バックアップ) に接続された専用インターコネクトを備えています。
* ヨーロッパとアジア太平洋に複数の支社を設置
* europe-west1 および australia-southeast1 では地域データ処理が必要です
* 集中ネットワーク管理チーム
セキュリティおよびコンプライアンス チームは、URL フィルタリングの L7 インスペクションを実行するために仮想インライン セキュリティ アプライアンスを必要としています。アプライアンスを us-west1 にデプロイしたいと考えています。
あなたは何をするべきか？
A. * 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。* ホスト プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。 * ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
B. * 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。* サービス プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。 * ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
C. * 共有 VPC ホスト プロジェクトに 1 つの VPC を作成します。* ホスト プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの us-west1 サブネットに NIC0 を接続します。* NIC1 を接続します。ホスト プロジェクトの us-west1 サブネットに* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。

D. * 共有 VPC サービス プロジェクトに 1 つの VPC を作成します。* サービス プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* サービス プロジェクトの us-west1 サブネットに NIC0 を接続します。* NIC1 を接続します。サービス プロジェクトの us-west1 サブネットに* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。

Answer: B

Explanation:

https://cloud.google.com/vpc/docs/shared-vpc