Google.Professional-Cloud-Network-Engineer.v2022-07-19.q79

試験コード：	Professional-Cloud-Network-Engineer
試験名称：	Google Cloud Certified - Professional Cloud Network Engineer
認証ベンダー：	Google
無料問題の数：	79
バージョン：	v2022-07-19
ページの閲覧量：	720
問題集の閲覧量：	10223

https://www.jpnshiken.com/shiken/Google.Professional-Cloud-Network-Engineer.v2022-07-19.q79.html

質問: **1**
サービスアカウントを使用して認証を行う自動化にステップを追加しています。クラウドストレージバケットからファイルを取得する機能を自動化する必要があります。組織では、可能な限り最小限の特権を使用する必要があります。
あなたは何をするべきか？
A. compute.instanceAdminをユーザーアカウントに付与します。
B. ユーザーアカウントにiam.serviceAccountUserを付与します。
C. クラウドストレージバケットのサービスアカウントに読み取り専用権限を付与します。
D. クラウドストレージバケットのサービスアカウントにクラウドプラットフォーム権限を付与します。
正解: **(**正解を表示します**)**
https://cloud.google.com/compute/docs/access/iam

質問: **2**
クラウドDNS管理ゾーンの1つでDNSSECを無効にしています。ゾーンファイルからDSレコードを削除し、キャッシュから期限切れになるのを待って、ゾーンのDNSSECを無効にしました。DNSSEC検証解決がゾーン内の名前を解決できないというレポートを受け取ります。
あなたは何をするべきか？
A. ゾーンのTTLを更新します。
B. ゾーンをTRANSFER状態に設定します。
C. ドメインレジストラでDNSSECを無効にします。
D. ドメインの所有権を新しいレジストラに譲渡します。
正解: **(**正解を表示します**)**
使用する管理対象ゾーンのDNSSECを無効にする前に、ドメインレジストラでDNSSECを非アクティブ化して、DNSSEC検証リゾルバがゾーン内の名前を引き続き解決できるようにする必要があります。

https://cloud.google.com/dns/docs/dnssec-config

質問: **3**
あなたの会社には、ファイアウォールとSSL証明書を管理するセキュリティチームがあります。また、ネットワーキングリソースを管理するネットワーキングチームもあります。ネットワーキングチームはファイアウォールルールを読み取ることができる必要がありますが、それらを作成、変更、または削除することはできません。
ネットワーキングチームの権限をどのように設定する必要がありますか？
A. ネットワーキングチームのメンバーにcompute.networkUserロールを割り当てます。
B. ネットワーキングチームのメンバーにcompute.networkAdminロールを割り当てます。
C. ネットワーキングチームのメンバーに、compute.networks。*および compute.firewalls.list権限のみを持つカスタムロールを割り当てます。
D. ネットワーキングチームのメンバーにcompute.networkViewerロールを割り当て、compute.networks.use権限を追加します。
正解: **B** (コメントを発表する)
説明/参照 :https ://cloud.google.com/compute/docs/access/iam

質問: **4**
あなたの組織は、3つの別々の部門に1つのプロジェクトを展開しています。これらの部門のうち2つは相互にネットワーク接続を必要としますが、3番目の部門は分離したままにする必要があります。設計では、これらの部門間に個別のネットワーク管理ドメインを作成する必要があります。運用上のオーバーヘッドを最小限に抑える必要があります。
トポロジをどのように設計する必要がありますか？
A. 3つの別々の部門ごとに共有VPCホストプロジェクトとそれぞれのサービスプロジェクトを作成します。
B. 3つの別々のVPCを作成し、CloudVPNを使用して2つの適切なVPC間の接続を確立します。
C. 3つの個別のVPCを作成し、VPCピアリングを使用して2つの適切なVPC間の接続を確立します。
D. 単一のプロジェクトを作成し、特定のファイアウォールルールを展開します。ネットワークタグを使用して、部門間のアクセスを分離します。
正解: (正解を表示します)
共有VPCを使用して、共通のVPCネットワークに接続します。これらのプロジェクトのリソースは、内部IPを使用して、プロジェクトの境界を越えて安全かつ効率的に相互に通信できます。中央のホストプロジェクトからサブネット、ルート、ファイアウォールなどの共有ネットワークリソースを管理できるため、プロジェクト全体に一貫したネットワークポリシーを適用して適用できます。
共有VPCおよびIAMコントロールを使用すると、ネットワーク管理とプロジェクト管理を分離できます。この分離は、最小特権の原則を実装するのに役立ちます。たとえば、一元化されたネットワークチームは、参加しているプロジェクトへのアクセス許可がなくても

ネットワークを管理できます。同様に、プロジェクト管理者は、共有ネットワークを操作する権限がなくてもプロジェクトリソースを管理できます。

質問: **5**
gcloudコマンドラインツールを使用して、事前定義されたロールに対処することにより、プロジェクトに新しいカスタムロールを作成しています。次のエラーメッセージが表示されます。
INVALID_ARGUMENT：権限esourcemanager.projects.listが無効ですどうすればよいですか？
A. resourcemanager.projects.setIamPolicy権限を追加して、再試行してください。
B. 新しい名前で同じ権限を持つ別の役割で再試行してください。
C. resourcemanager.projects.get権限を追加して、再試行してください。
D. resourcemanager.projects.list権限を削除して、再試行してください。
正解: **(**正解を表示します**)**

質問: **6**
あなたの会社はパートナーと協力して、顧客にソリューションを提供しています。あなたの会社とパートナー組織の両方がGCPを使用しています。パートナーのネットワークには、会社のVPCの一部のリソースにアクセスする必要のあるアプリケーションがあります。VPC間にCIDRの重複はありません。
セキュリティを損なうことなく目的の結果を達成するために実装できる2つのソリューションはどれですか？ 2つ選択してください。）
A. VPCピアリング
B. 共有VPC
C. クラウドVPN
D. 専用相互接続
E. クラウドNAT
正解: **(**正解を表示します**)**
Google Cloud VPCネットワークピアリングでは、2つの仮想プライベートクラウド（VPC）ネットワークが同じプロジェクトに属しているか同じ組織に属しているかに関係なく、2つの仮想プライベートクラウド（VPC）ネットワーク間で内部IPアドレス接続が可能です。

質問: **7**
オンプレミスのデータセンターには、各ルーターのVPNを介してGCPに接続された2台のルーターがあります。すべてのアプリケーションが正しく機能しています。ただし、すべてのトラフィックは、必要に応じて2つの接続間で負荷分散されるのではなく、単一のVPNを通過します。
トラブルシューティング中に、次のことがわかります。
*各オンプレミスルーターは同じASNで構成されています。
*各オンプレミスルーターは同じルートと優先度で構成されています。

*両方のオンプレミスルーターは、単一のクラウドルーターに接続されたVPNで構成されています。
* VPNが接続しているとき、VPNログには提案が選択されていない回線があります。
*1つのオンプレミスルーターとクラウドルーターの間でBGPセッションが確立されていません。
この問題の最も可能性の高い原因は何ですか？
A. VPNセッションの1つが正しく構成されていません。
B. ファイアウォールが2番目のVPN接続を介したトラフィックをブロックしています。
C. ネットワークトラフィックの負荷を分散するためのロードバランサーがありません。
D. オンプレミスルーターとクラウドルーターの両方の間でBGPセッションが確立されていません。
正解: **(**正解を表示します**)**
VPNログに提案が選択されていないエラーが表示される場合、このエラーは、CloudVPNとピアVPNゲートウェイが一連の暗号について合意できなかったことを示します。IKEv1の場合、暗号のセットは完全に一致する必要があります。IKEv2の場合、各ゲートウェイによって提案された共通の暗号が少なくとも1つ存在する必要があります。サポートされている暗号を使用して、ピアVPNゲートウェイを構成していることを確認してください。https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting#:~:text=If%20the%20VPN%20logs%20show,of%20ciphers%20must%20match%20exactly.&text=Make %20sure%20that%20you%20use、configure%20your%20peer%20VPN%20gateway。

質問: **8**
セキュリティチームは、GCPの本番仮想マシンへの外部SSHアクセスを無効にしました。運用チームは、VMやその他のリソースをリモートで管理する必要があります。彼らは何ができますか？
A. 運用エンジニアがタスクを実行する必要があるときにクラウドVMへの一時的なSSHアクセスを許可する新しいアクセス要求プロセスを開発します。
B. 運用チームにGoogleCloudShellを使用するためのアクセス権を付与します。
C. 開発チームにAPIサービスを構築してもらい、運用チームが特定のリモートプロシージャコールを実行してタスクを実行できるようにします。
D. クラウドVMへのSSHアクセスを許可するようにGCPへのVPN接続を構成します。
正解: **B (**コメントを発表する**)**
運用チームにGoogleCloudShellを使用するためのアクセス権を付与します。
B（正解）運用エンジニアにGoogleCloudShellを使用するためのアクセス権を付与します。エンジニアが尋ねるのは、SSHを使用するのと同じようにVMにリモートアクセスすることだけです。したがって、マシンに外部IPアドレスがまだある場合、エンジニアはGoogleCloudShellを使用してSSH経由でVMにアクセスできます。

これは、要件を満たすための簡単で効果的な方法です。他のすべての回答は、ニーズに見合うだけの価値があるよりも多くのセットアップを必要とする可能性のあるオプションです。

質問: **9**
あなたの会社には、ファイアウォールとSSL証明書を管理するセキュリティチームがあります。また、ネットワーキングリソースを管理するネットワーキングチームもあります。ネットワーキングチームはファイアウォールルールを読み取ることができる必要がありますが、それらを作成、変更、または削除することはできません。
ネットワーキングチームの権限をどのように設定する必要がありますか？
A. ネットワーキングチームのメンバーに、compute.networks。*およびcompute.firewalls.list権限のみを持つカスタムロールを割り当てます。
B. ネットワーキングチームのメンバーにcompute.networkUserロールを割り当てます。
C. ネットワーキングチームのメンバーにcompute.networkViewerロールを割り当て、compute.networks.use権限を追加します。
D. ネットワーキングチームのメンバーにcompute.networkAdminロールを割り当てます。
正解: **(**正解を表示します**)**

質問: **10**
現在、us-central1リージョンでホストされているWebアプリケーションがあります。ユーザーは、アジアを旅行するときに高い遅延を経験します。ネットワークロードバランサーを構成しましたが、ユーザーはパフォーマンスの向上を経験していません。レイテンシーを減らしたい。
あなたは何をするべきか？
A. トラフィックに優先順位を付けるようにポリシーベースのルートルールを構成します。
B. アプリケーションをホストしているサブネットの動的ルーティングを構成します。
C. DNSゾーンのTTLを構成して、更新間の時間を短縮します。
D. HTTPロードバランサーを構成し、トラフィックをそれに転送します。
正解: **(**正解を表示します**)**

質問: **11**
ソフトウェアチームは、RFC1918アドレス空間を使用してGCPのComputeEngineインスタンスに直接接続する必要があるオンプレミスのウェブアプリケーションを開発しています。次の仕様を前提として、オンプレミス環境からGCPへの接続ソリューションを選択する必要があります。
* ISPはGoogleパートナー相互接続プロバイダーです。
*オンプレミスVPNデバイスのインターネットアップリンクおよびダウンリンク速度は10Gbpsです。
*オンプレミスゲートウェイとGCP間のテストVPN接続は、最大速度で実行されていますパケット損失のために500Mbps。

*ほとんどのデータ転送はGCPからオンプレミス環境に行われます。
*アプリケーションは、相互接続を介したピーク転送中に最大1.5Gbpsまでバーストする可能性があります。
*ソリューションのコストと複雑さは最小限に抑える必要があります。
接続ソリューションをどのようにプロビジョニングする必要がありますか？
A. パケット損失を考慮して複数のVPNトンネルを作成し、ECMPを使用して帯域幅を増やします。
B. ISPを介してパートナー相互接続をプロビジョニングします。
C. VPNを介してネットワーク圧縮を使用して、VPNを介して送信できるデータの量を増やします。
D. VPNの代わりに専用の相互接続をプロビジョニングします。
正解: **(**正解を表示します**)**

質問: **12**
組織では、可能性のある法的手続きで将来分析するために、すべてのアプリケーションのメトリックを5年間保持する必要があります。どのアプローチを使用する必要がありますか？
A. すべてのプロジェクトのStackdriver Monitoringを設定し、BigQueryにエクスポートします。
B. デフォルトの保持ポリシーを使用してすべてのプロジェクトのStackdriverMonitoringを構成します。
C. すべてのプロジェクトのStackdriver Monitoringを構成し、GoogleCloudStorageにエクスポートします。
D. セキュリティチームに各プロジェクトのログへのアクセスを許可します。
正解: **C (**コメントを発表する**)**
BとDはいずれも要件に適したソリューションではないため、すぐに除外できます。
5年間保持」
AとCでは、BigQueryとCloudStorageのどちらを保存するかが異なります。主な関心事は保管期間の延長であるため、C（正解の方が適切であり、 将来の分析のために5年間保持」することで、たとえばColdlineストレージクラスを使用するなど、さらに適格になります。
BigQueryに関しては、低コストのストレージでもありますが、主な目的は分析です。
また、Cloud Storageのログは、必要なときにいつでもBigQueryに簡単に転送できます。

質問: **13**
TFTPサーバーで使用する複数のComputeEngine仮想マシンインスタンスを作成します。どのタイプのロードバランサーを使用する必要がありますか？
A. TCPプロキシロードバランサー
B. SSLプロキシロードバランサー
C. HTTP $) ロードバランサー

D. ネットワークロードバランサー
正解: **(**正解を表示します**)**

質問: **14**
共有VPCアーキテクチャを設計しています。ネットワークおよびセキュリティチームは、部門間で公開されるルートを厳密に制御します。制作部門とステージング部門は相互に通信できますが、特定のネットワークを介してのみ通信できます。Googleが推奨する方法に従いたい。
このトポロジをどのように設計する必要がありますか？
A. 共有VPCホストプロジェクト内に2つの共有VPCを作成し、それらの間でVPCピアリングを有効にします。ファイアウォールルールを使用して、特定のネットワーク間のアクセスをフィルタリングします。
B. 共有VPCホストプロジェクト内に2つの共有VPCを作成し、それらの間にCloud VPN /CloudRouterを作成します。フレキシブルルートアドバタイズメント（FRA）を使用して、特定のネットワーク間のアクセスをフィルタリングします。
C. 共有VPCサービスプロジェクト内に2つの共有VPCを作成し、それらの間にクラウドVPN/クラウドルーターを作成します。フレキシブルルートアドバタイズメント（FRA）を使用して、特定のネットワーク間のアクセスをフィルタリングします。
D. 共有VPCホストプロジェクト内に1つのVPCを作成し、個々のサブネットをサービスプロジェクトと共有して、特定のネットワーク間のアクセスをフィルタリングします。
正解: **(**正解を表示します**)**
説明/参照：https ://cloud.google.com/vpc/docs/shared-vpc

質問: **15**
キャッシュ可能なコンテンツのオリジンとしてHTTP（S）負荷分散を使用してCloudCDNを構成しました。圧縮はWebサーバーで構成されますが、CloudCDNによって提供される応答は圧縮されません。
問題の最も可能性の高い原因は何ですか？
A. CloudCDNで圧縮を構成していません。
B. 異なる圧縮タイプでWebサーバーとクラウドCDNを構成しました。
C. ロードバランサーの背後にあるWebサーバーは、さまざまな圧縮タイプで構成されています。
D. リクエストにViaヘッダーが含まれている場合でも、応答を圧縮するようにWebサーバーを構成する必要があります。
正解: **D (**コメントを発表する**)**
Cloud CDNによって提供される応答が圧縮されていないが圧縮されている必要がある場合は、インスタンスで実行されているWebサーバーソフトウェアが応答を圧縮するように構成されていることを確認してください。デフォルトでは、一部のWebサーバーソフトウェアは、Viaヘッダーを含むリクエストの圧縮を自動的に無効にします。Viaヘッダーの存在は、リクエストがプロキシによって転送されたことを示します。HTTP（S）負荷分散などの

HTTPプロキシは、HTTP仕様で要求されているように、各リクエストにViaヘッダーを追加します。
圧縮を有効にするには、Webサーバーのデフォルト構成をオーバーライドして、要求にViaヘッダーが含まれている場合でも応答を圧縮するように指示する必要がある場合があります。
https://cloud.google.com/cdn/docs/troubleshooting-steps

質問: **16**
Googleへの10Gbpsの直接ピアリング接続とgsutilツールを使用して、オンプレミスサーバーからCloudStorageバケットにファイルをアップロードしています。オンプレミスサーバーは、Googleピアリングポイントから100ミリ秒離れています。アップロードで利用可能な10Gbpsの全帯域幅が使用されていないことに気づきました。接続の帯域幅使用率を最適化する必要があります。
オンプレミスサーバーで何をすべきですか？
A. tarなどのユーティリティを使用してファイルを圧縮し、送信されるデータのサイズを縮小します。
B. gsutilコマンドでperfdiagパラメーターを使用して、パフォーマンスを高速化します：gsutil perfdiag gs ://[バケット名]。
C. オンプレミスサーバーでTCPパラメーターを調整します。
D. gsutilコマンドから-mフラグを削除して、シングルスレッド転送を有効にします。
正解: **B** (コメントを発表する)

質問: **17**
あなたの会社は、収益を生み出す新しい重要なWebアプリケーションを立ち上げました。管理対象インスタンスグループ、自動スケーリング、およびネットワークロードバランサーをフロントエンドとして使用して、スケーラビリティーのためにアプリケーションをデプロイしました。ある日、自動スケーリングがインスタンスの最大数に達する原因となった深刻なバーストトラフィックに気付き、アプリケーションのユーザーはトランザクションを完了できません。調査の結果、これはDDOS攻撃だと思います。アプリケーション

へのユーザーアクセスをすばやく復元し、コストを最小限に抑えながらトランザクションを成功させる必要があります。
どの2つのステップを実行する必要がありますか？ 2つ選択してください。）
A. Cloud Armorを使用して、攻撃者のIPアドレスをブラックリストに登録します。
B. グローバルHTTP ＄）ロードバランサーを作成し、アプリケーションバックエンドをこのロードバランサーに移動します。
C. 深刻なバーストトラフィックに対応するために、最大自動スケーリングバックエンドを増やします。
D. GCPでアプリケーション全体を数時間シャットダウンします。アプリケーションがオフラインになると、攻撃は停止します。
E. バックエンドのコンピューティングエンジンインスタンスにSSHで接続し、認証ログとsyslogを表示して、攻撃の性質をさらに理解します。
正解: **C,E** (コメントを発表する)

質問: **18**
プロジェクト内のすべてのインスタンスは、カスタムメタデータのenable-oslogin値をFALSEに設定し、プロジェクト全体のSSHキーをブロックするように構成されています。どのインスタンスにもSSHキーが設定されておらず、プロジェクト全体のSSHキーが構成されていません。ファイアウォールルールは、任意のIPアドレス範囲からのSSHセッションを許可するように設定されています。SSHで1つのインスタンスにしたいとします。
あなたは何をするべきか？
A. gcloudcomputesshを使用してインスタンスへのCloudShellSSHを開きます。
B. カスタムメタデータenable-osloginをTRUEに設定し、puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
C. 新しいSSHキーペアを生成します。秘密鍵の形式を確認し、それをインスタンスに追加します。
puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
D. 新しいSSHキーペアを生成します。公開鍵の形式を確認し、プロジェクトに追加します。
puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
正解: **B** (コメントを発表する)
https://cloud.google.com/compute/docs/storing-retrieveing-metadata

質問: **19**
組織のGoogleCloud環境でCloudRouterの新しいインスタンスを構成して、新しい専用インターコネクトを介してデータセンターに接続できるようにします。セールス、マーケティング、ITには、それぞれ組織のホストプロジェクトにサービスプロジェクトがアタッチされています。
クラウドルーターインスタンスはどこに作成する必要がありますか？

A. すべてのプロジェクトのVPCネットワーク
B. ITプロジェクトのVPCネットワーク
C. ホストプロジェクトのVPCネットワーク
D. 販売、マーケティング、ITプロジェクトのVPCネットワーク
正解: **C** (コメントを発表する)
参照：
https://cloud.google.com/interconnect/docs/how-to/dedicated/using-interconnects-other-projects

質問: **20**
自動モードでRetailという名前のVPCネットワークを作成しました。Distributionという名前のVPCネットワークを作成し、それをRetailVPCとピアリングします。
ディストリビューションVPCをどのように構成する必要がありますか？
A. 自動モードでディストリビューションVPCを作成します。ネットワークピアリングを介して両方のVPCをピアリングします。
B. カスタムモードでディストリビューションVPCを作成します。CIDR範囲10.0.0.0/9を使用します。必要なサブネットを作成し、ネットワークピアリングを介してそれらをピアリングします。
C. カスタムモードでディストリビューションVPCを作成します。CIDR範囲10.128.0.0/9を使用します。必要なサブネットを作成し、ネットワークピアリングを介してそれらをピアリングします。
D. デフォルトのVPCの名前を Distribution」に変更し、ネットワークピアリングを介してピアリングします。
正解: (正解を表示します)
https://cloud.google.com/vpc/docs/vpc#ip-ranges

質問: **21**
Cloud DNSに移行していて、BINDゾーンファイルをインポートしたいと考えています。
どのコマンドを使用する必要がありますか？
gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE
A. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone
B. MANAGED_ZONE
gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE
C. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone
D. MANAGED_ZONE
正解: **C** (コメントを発表する)
他のプロバイダーからエクスポートされたファイルを取得したら、gcloud dnsrecord-setsimportコマンドを使用してファイルを管理対象ゾーンにインポートできます。
レコードセットをインポートするには、dnsrecord-setsimportコマンドを使用します。--zone-file-formatフラグは、BINDゾーン形式のファイルを予期するようにimportに指示しま

す。このフラグを省略すると、インポートではYAML形式のレコードファイルが必要になります。
参照：https://medium.com/@prashantapaudel/gcp-certification-series-2-4-planning-and-configuring-network-resources-8045ac2cc2ac

質問: **22**
ネットワーク管理者権限のみが割り当てられている共有VPCのファイアウォールルールを更新しようとしています。ファイアウォールルールを変更することはできません。組織では、必要最小限の特権を使用する必要があります。
どのレベルの権限を要求する必要がありますか？
A. 共有VPC管理者からのセキュリティ管理者権限。
B. 共有VPC管理者からのサービスプロジェクト管理者権限。
C. 組織管理者からの共有VPC管理者権限。
D. 組織管理者からの組織管理者権限。
正解: **A** (コメントを発表する)
説明/参照：https://cloud.google.com/vpc/docs/shared-vpc

質問: **23**
プロジェクト内のすべてのインスタンスで個人のSSHキーが機能することを確認する必要があります。これを可能な限り効率的に達成したいと考えています。
あなたは何をするべきか？
A. 公開sshキーをプロジェクトのメタデータにアップロードします。
B. 公開sshキーを各インスタンスのメタデータにアップロードします。
C. 公開sshキーが埋め込まれたカスタムGoogleComputeEngineイメージを作成します。
D. gcloudcompute sshを使用して、パブリックsshキーをインスタンスに自動的にコピーします。
正解: (正解を表示します)
概要SSHキーを作成および管理することにより、ユーザーがサードパーティのツールを介してLinuxインスタンスにアクセスできるようにすることができます。SSHキーは、次のファイルで構成されています。インスタンスレベルのメタデータまたはプロジェクト全体のメタデータに適用される公開SSHキーファイル。ユーザーがローカルデバイスに保存するプライベートSSHキーファイル。ユーザーが秘密のSSHキーを提示すると、Google Cloudプロジェクトのメンバーでなくても、サードパーティのツールを使用して、一致する公開SSHキーファイルで構成されているインスタンスに接続できます。したがって、1つ以上のインスタンスの公開SSHキーメタデータを変更することで、ユーザーがアクセスできるインスタンスを制御できます。https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey

質問: **24**

あなたはcloudtech5という組織で働いています。あなたの組織は、ホストされている製品と人気のあるGitOps方法論のみを使用して、Google Cloud Platformに継続的インテグレーションとデリバリー（CI / CD）パイプラインを実装することを決定しました。アーキテクチャには、頻繁に更新されてロールバックされる多くのマイクロサービスが含まれています。使用する製品を選択してください。
A. クラウドソースリポジトリ、クラウドビルド、コンテナレジストリ、Google Kubernetes Engine
B. BitBucket、Cloud Build、Container Registry、GoogleKubernetesEngine。
C. クラウドソースリポジトリ、Compute Engine上のJenkins、Container Registry、GoogleKubernetesEngine。
D. クラウドストレージ、クラウドデータフロー、コンピューティングエンジン。
正解: **A** (コメントを発表する)
オプションAが正しい選択です。これは、Cloud Sourceリポジトリが、Google Cloudでホストされている、完全な機能を備えたスケーラブルなプライベートGitリポジトリであるためです。Cloud Buildは、GoogleCloudPlatformインフラストラクチャでビルドを実行するサービスです。Cloud Buildは、Google Cloud Storage、Cloud Source Repositories、GitHub、またはBitbucketからソースコードをインポートし、仕様に合わせてビルドを実行し、Dockerコンテナ やJavaアーカイブなどのアーティファクトを生成できます。Container Registryは、GoogleCloudPlatformで実行されるプライベートコンテナイメージレジストリです。Google Kuberenetes Engineは、すばやく更新およびロールバックできる小さなサービスをデプロイするのに理想的です。
オプションBは正しくありません。これは、BitBucketがGoogle Cloudでホストされているサービスではないためですが、同じ結果を達成するために使用できます。
コンピューティングエンジン上のJenkinsはGoogleがホストする製品ではないため、オプションCは正しくありません。クラウドビルドは、Google Cloudによって管理されるサービスであるため、正しい選択です。
オプションDは正しくありません。これは、目的がデータ処理パイプラインではなくCI/CDパイプラインを実装することであるためです。

質問: **25**
組織用にGoogleKubernetesEngine（GKE）クラスタを設計しています。現在のクラスターサイズは、ノードあたり20ポッド、150サービスの10ノードをホストすると予想されます。今後2年間で新しいサービスが移行されるため、100ノード、ノードあたり200ポッド、1500サービスの成長が計画されています。アドレスの消費を最小限に抑えながら、エイリアスIP範囲を持つVPCネイティブクラスターを使用する必要があります。
このトポロジをどのように設計する必要がありますか？
A. サイズ/ 25のサブネットを作成し、2つのセカンダリ範囲をポッド用に/ 17、サービス用に/21にします。
VPCネイティブクラスターを作成し、それらの範囲を指定します。

B. サイズ/28のサブネットを作成します。2つのセカンダリ範囲はポッドの場合は/24、サービスの場合は/24です。
VPCネイティブクラスターを作成し、それらの範囲を指定します。サービスを展開する準備ができたら、サブネットのサイズを変更します。
C. gcloud container cluster create [CLUSTER NAME]-enable-ip-aliasを使用して、VPCネイティブクラスターを作成します。
D. gcloud container cluster create [CLUSTER NAME]を使用して、VPCネイティブクラスターを作成します。
正解: **B (**コメントを発表する**)**
https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters

質問: **26**
オンプレミスとGCPの間でCloudVPNの使用を増やしており、単一のトンネルで処理できるよりも多くのトラフィックをサポートしたいと考えています。CloudVPNを使用して使用可能な帯域幅を増やしたい。
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トンネルを同じCloudVPNゲートウェイ上に作成します。
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。同じIP範囲を転送するが、新しいオンプレミスゲートウェイIPを指す2番目のトンネルを既存のクラウドVPNゲートウェイに作成します。
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CloudVPNゲートウェイを追加します。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IPアドレスを指す2番目のクラウドVPNゲートウェイに新しいトンネルを作成します。
正解: **(**正解を表示します**)**
説明/参照：

質問: **27**
HTTP（S）負荷分散サービスを作成しました。バックエンドインスタンスが正しく応答していることを確認する必要があります。
ヘルスチェックをどのように構成する必要がありますか？
A. リクエストパスをヘルスチェックに使用される特定のURLに設定し、プロキシヘッダーをPROXY_V1に設定します。
B. ヘルスチェックに使用される特定のURLにrequest-pathを設定し、ヘルスチェックを識別するカスタムホストヘッダーを含めるようにhostを設定します。
C. ヘルスチェックに使用される特定のURLにrequest-pathを設定し、バックエンドサービスが常に応答本文で返す文字列に応答を設定します。
D. プロキシヘッダーをデフォルト値に設定し、ヘルスチェックを識別するカスタムホストヘッダーを含めるようにホストを設定します。

正解: **C** (コメントを発表する)
https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based_health_checks

質問: **28**
ネットワーク管理者権限のみが割り当てられている共有VPCのファイアウォールルールを更新しようとしています。ファイアウォールルールを変更することはできません。組織では、必要最小限の特権を使用する必要があります。
どのレベルの権限を要求する必要がありますか？
A. 組織管理者からの組織管理者権限。
B. 共有VPC管理者からのセキュリティ管理者権限。
C. 共有VPC管理者からのサービスプロジェクト管理者権限。
D. 組織管理者からの共有VPC管理者権限。
正解: (正解を表示します)

質問: **29**
VPNゲートウェイを導入して、オンプレミスネットワークをGCPに接続する必要があります。BGP対応ではないオンプレミスVPNデバイスを使用しています。ネットワークが拡大したときのダウンタイムと運用オーバーヘッドを最小限に抑える必要があります。デバイスはIKEv2のみをサポートしており、Googleが推奨する方法に従う必要があります。
あなたは何をするべきか？
A. CloudVPNインスタンスを作成します。
サブネットごとにポリシーベースのVPNトンネルを作成します。
ローカルネットワークとリモートネットワークに一致するように、適切なローカルトラフィックセレクターとリモートトラフィックセレクターを構成します。
適切な静的ルートを作成します。
B. CloudVPNインスタンスを作成します。
ポリシーベースのVPNトンネルを作成します。
ローカルネットワークとリモートネットワークに一致するように、適切なローカルトラフィックセレクターとリモートトラフィックセレクターを構成します。
適切な静的ルートを構成します。
C. CloudVPNインスタンスを作成します。
ルートベースのVPNトンネルを作成します。
ローカルネットワークとリモートネットワークに一致するように、適切なローカルトラフィックセレクターとリモートトラフィックセレクターを構成します。
適切な静的ルートを構成します。
D. CloudVPNインスタンスを作成します。
ルートベースのVPNトンネルを作成します。
適切なローカルおよびリモートのトラフィックセレクターを0.0.0.0/0に構成します。

適切な静的ルートを構成します。
正解: **(**正解を表示します**)**
https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing

質問: **30**
gcloudコマンドを使用して、ポリシーベースのルーティング用に構成されたCloudVPNゲートウェイの背後にあるオンプレミスリソースへの静的ルートを構成する必要があります。
どのネクストホップを選ぶべきですか？
A. デフォルトのインターネットゲートウェイ
B. CloudVPNゲートウェイのIPアドレス
C. クラウドVPNトンネルの名前と地域
D. VPNトンネルのリモート側にあるインスタンスのIPアドレス
正解: **C (**コメントを発表する**)**
参照：
https://cloud.google.com/vpn/docs/how-to/creating-static-vpns

質問: **31**
開発チーム用に新しいVPCを作成しました。SSH経由でのみこのVPCのリソースへのアクセスを許可する必要があります。
ファイアウォールルールをどのように構成する必要がありますか？
A. 2つのファイアウォールルールを作成します。1つは優先度0のすべてのトラフィックをブロックし、もう1つは優先度1000のポート22を許可します。
B. 2つのファイアウォールルールを作成します。1つは優先度65536のすべてのトラフィックをブロックし、もう1つは優先度1000のポート3389を許可します。
C. 優先度1000のポート22を許可する単一のファイアウォールルールを作成します。
D. 優先度1000のポート3389を許可する単一のファイアウォールルールを作成します。
正解: **C (**コメントを発表する**)**
参照：
https://geekflare.com/gcp-firewall-configuration/

質問: **32**
Apache Tomcat 8.XをGoogleCloudのコンピューティングエンジンのポート8085にインストールし、同じマシンのカスタムポートにJenkinsをインストールしました。ポート8085へのトラフィックを許可するファイアウォールルールを作成しました。XXXX :8085を参照するとApache Tomcatページが表示されますが、XXXX :customポートを参照すると、Jenkinsページが読み込まれません。可能な解決策は何でしょうか？正しい選択をしてください。
A. ファイアウォールルールを作成します。正しいネットワークを選択し、ネットワーク内のすべてのインスタンスとしてターゲットを選択し、カスタムポートとプロトコルを指定します。
B. ファイアウォールルールを作成します。正しいネットワークを選択し、ターゲットタグを作成して、そのタグをコンピューティングエンジンインスタンスにアタッチし、Jenkinsでマップされたカスタムポートへのトラフィックを許可します。
C. ファイアウォールルールを作成します。計算エンジンを備えた正しいサブネットを選択し、すべてのプロトコルとポートを許可します。
D. ファイアウォールルールを作成します。正しいサブネットを選択し、ターゲットタグを作成して、それをコンピューティングエンジンインスタンスにアタッチし、すべてのプロトコルとポートを許可します。
正解: **(**正解を表示します**)**
オプションBが正しい選択です。タグを作成してそれをコンピューティングエンジンインスタンスにアタッチし、カスタムポートへのトラフィックを許可することは、許容度が低いためです。
ネットワーク内のすべてのインスタンスとしてターゲットを選択すると、すべてのインスタンスへのトラフィックが許可されるため、オプションAは正しくありません。
すべてのプロトコルとポートを許可することはセキュリティ上の脅威であり、常に最も許容度の低い原則に従うため、オプションCは正しくありません。
すべてのプロトコルとポートを許可するとセキュリティ障害が発生する可能性があるため、オプションDは正しくありません。常に、許容度が最も低いという原則に従ってください。

質問: **33**
GCPコンソールでDedicatedInterconnectを注文しました。物理的な接続を完了するには、クロスコネクトプロバイダーに承認書/接続機能の割り当て（LOA-CFA）を渡す必要があります。
これを達成できる2つのアクションはどれですか？（2つ選択してください。）
A. クラウド相互接続カテゴリでクラウドサポートチケットを開きます。

B. gcloudcomputeinterconnectsdescribe<interconnect>を実行します。
C. 注文プロセス中に指定したNOC連絡先のアカウントの電子メールを確認します。
D. クロスコネクトプロバイダーに連絡して、GoogleがLOA / CFAをメールで自動的に送信したことを伝え、接続を完了します。
E. GCPコンソールの[ハイブリッド接続]セクションからLOA-CFAをダウンロードします。
正解: **C,E** (コメントを発表する)

質問: **34**
10.1.1.0/24ネットワークと172.16.45.0/24ネットワークの両方でインスタンスがIPアドレスを持つことを可能にする新しいVPCネットワークを作成する必要があります。
あなたは何をするべきか？
A. 目的のIPアドレスにトラフィックを送信するサービスごとに一意のDNSレコードを作成します。
B. 172.16.45.0/24が正しいインスタンスを指すようにグローバル負荷分散を構成します。
C. VPCピアリングを使用して、トラフィックが10.1.0.0/24ネットワークと172.16.45.0/24ネットワークの間をルーティングできるようにします。
D. 10.1.1.0/24のVPCサブネット内の仮想インスタンスで172.16.45.0/24のエイリアスIP範囲を構成します。
正解: (正解を表示します)

質問: **35**
Google Kubernetes Engine（GKE）にデプロイされているアプリケーションに新しいCloudArmorポリシーを適用したいとします。CloudArmorポリシーに使用するターゲットを見つけ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ポッド
B. GKE入力
C. GKEノード
D. GKEクラスター
正解: (正解を表示します)

質問: **36**
VPCで将来の新しいGKEクラスターのアドレスプランを定義する必要があります。これはVPCネイティブクラスターになり、デフォルトのポッドIP範囲の割り当てが使用されます。クラスタを作成する前に、必要なすべてのVPCサブネットとそれぞれのIPアドレス範囲を事前にプロビジョニングする必要があります。クラスタには最初は単一のノードがありますが、必要に応じて最大3つのノードに拡張されます。最小数のポッドIPアドレスを割り当てる必要があります。
ポッドIPアドレス範囲にどのサブネットマスクを使用する必要がありますか？
A. / 21

B. / 22
C. / 23
D. / 25
正解: **(**正解を表示します**)**
参照：
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips

質問: **37**
クラウドDNS管理ゾーンの1つでDNSSECを無効にしています。ゾーンファイルからDSレコードを削除し、キャッシュから期限切れになるのを待って、ゾーンのDNSSECを無効にしました。DNSSEC検証解決がゾーン内の名前を解決できないというレポートを受け取ります。
あなたは何をするべきか？
A. ドメインレジストラでDNSSECを無効にします。
B. ゾーンをTRANSFER状態に設定します。
C. ゾーンのTTLを更新します。
D. ドメインの所有権を新しいレジストラに譲渡します。
使用する管理対象ゾーンのDNSSECを無効にする前に、ドメインレジストラでDNSSECを非アクティブ化して、DNSSEC検証リゾルバがゾーン内の名前を引き続き解決できるようにする必要があります。
正解: **(**正解を表示します**)**

質問: **38**
特定のIPアドレスのみが接続できるように、GoogleCloud負荷分散アプリケーションへのアクセスを制限する必要があります。
あなたは何をするべきか？
A. VPC Service Controlsを使用して安全な境界を作成し、ロードバランサーを許可されたクライアントのソースIP範囲とGoogleヘルスチェックIP範囲に制限されたサービスとしてマークします。
B. バックエンドインスタンスに &application」のタグを付け、ターゲットタグ &application」と許可されたクライアントのソースIP範囲およびGoogleヘルスチェックのIP範囲を使用してファイアウォールルールを作成します。
C. VPCServiceControlsのAccessContextManager機能を使用して安全な境界を作成し、許可されたクライアントのソースIP範囲とGoogleヘルスチェックIP範囲へのアクセスを制限します。
D. バックエンドインスタンスに &application」というラベルを付け、ターゲットラベル &application」と許可されたクライアントのソースIP範囲およびGoogleヘルスチェックIP範囲を使用してファイアウォールルールを作成します。
正解: **(**正解を表示します**)**

質問: **39**
あなたの組織は、3つの別々の部門に1つのプロジェクトを展開しています。これらの部門のうち2つは相互にネットワーク接続を必要としますが、3番目の部門は分離したままにする必要があります。設計では、これらの部門間に個別のネットワーク管理ドメインを作成する必要があります。運用上のオーバーヘッドを最小限に抑える必要があります。
トポロジをどのように設計する必要がありますか？
A. 3つの個別のVPCを作成し、VPCピアリングを使用して2つの適切なVPC間の接続を確立します。
B. 3つの別々のVPCを作成し、CloudVPNを使用して2つの適切なVPC間の接続を確立します。
C. 3つの別々の部門ごとに共有VPCホストプロジェクトとそれぞれのサービスプロジェクトを作成します。
D. 単一のプロジェクトを作成し、特定のファイアウォールルールを展開します。ネットワークタグを使用して、部門間のアクセスを分離します。
共有VPCを使用して、共通のVPCネットワークに接続します。これらのプロジェクトのリソースは、内部IPを使用して、プロジェクトの境界を越えて安全かつ効率的に相互に通信できます。中央のホストプロジェクトからサブネット、ルート、ファイアウォールなどの共有ネットワークリソースを管理できるため、プロジェクト全体に一貫したネットワークポリシーを適用して適用できます。
共有VPCおよびIAMコントロールを使用すると、ネットワーク管理とプロジェクト管理を分離できます。この分離は、最小特権の原則を実装するのに役立ちます。たとえば、一元化されたネットワークチームは、参加しているプロジェクトへのアクセス許可がなくてもネットワークを管理できます。同様に、プロジェクト管理者は、共有ネットワークを操作する権限がなくてもプロジェクトリソースを管理できます。
正解: **(**正解を表示します**)**

質問: **40**
特定のIPアドレスのみが接続できるように、GoogleCloud負荷分散アプリケーションへのアクセスを制限する必要があります。
あなたは何をするべきか？
A. VPCServiceControlsのAccessContextManager機能を使用して安全な境界を作成し、許可されたクライアントのソースIP範囲とGoogleヘルスチェックIP範囲へのアクセスを制限します。
B. VPC Service Controlsを使用して安全な境界を作成し、ロードバランサーを許可されたクライアントのソースIP範囲とGoogleヘルスチェックIP範囲に制限されたサービスとしてマークします。
C. バックエンドインスタンスに 'application」のタグを付け、ターゲットタグ 'application」と許可されたクライアントのソースIP範囲およびGoogleヘルスチェックのIP範囲を使用してファイアウォールルールを作成します。

D. バックエンドインスタンスに &application」というラベルを付け、ターゲットラベル &application」と許可されたクライアントのソースIP範囲およびGoogleヘルスチェックIP範囲を使用してファイアウォールルールを作成します。
正解: **(**正解を表示します**)**
https://cloud.google.com/load-balancing/docs/https/setting-up-https#sendtraffic

質問: **41**
グローバル外部TCP負荷分散ソリューションを展開していて、元のレイヤー3ペイロードの送信元IPアドレスを保持したいと考えています。
どのタイプのロードバランサーを使用する必要がありますか？
A. HTTP $)ロードバランサー
B. ネットワークロードバランサー
C. 内部ロードバランサー
D. TCP/SSLプロキシロードバランサー
正解: **(**正解を表示します**)**
参照：
https://cloud.google.com/load-balancing/docs/network

質問: **42**
プロジェクト内のすべてのインスタンスで個人のSSHキーが機能することを確認する必要があります。これを可能な限り効率的に達成したいと考えています。
あなたは何をするべきか？
A. 公開sshキーを各インスタンスのメタデータにアップロードします。
B. 公開sshキーが埋め込まれたカスタムGoogleComputeEngineイメージを作成します。
C. 公開sshキーをプロジェクトのメタデータにアップロードします。
D. gcloudcompute sshを使用して、パブリックsshキーをインスタンスに自動的にコピーします。
正解: **(**正解を表示します**)**

質問: **43**
VPCで将来の新しいGKEクラスターのアドレスプランを定義する必要があります。これはVPCネイティブクラスターになり、デフォルトのポッドIP範囲割り当てが使用されます。クラスタを作成する前に、必要なすべてのVPCサブネットとそれぞれのIPアドレス範囲を事前にプロビジョニングする必要があります。クラスタには最初は単一のノードがありますが、必要に応じて最大3つのノードに拡張されます。最小数のポッドIPアドレスを割り当てる必要があります。
ポッドIPアドレス範囲にどのサブネットマスクを使用する必要がありますか？
A. / 21
B. / 22
C. / 23

D. / 25
正解: **D** (コメントを発表する)
説明/参照 :https ://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips

質問: **44**
あなたの会社はパートナーと協力して、顧客にソリューションを提供しています。あなたの会社とパートナー組織の両方がGCPを使用しています。パートナーのネットワークには、会社のVPCの一部のリソースにアクセスする必要のあるアプリケーションがあります。VPC間にCIDRの重複はありません。
セキュリティを損なうことなく目的の結果を達成するために実装できる2つのソリューションはどれですか？ 2つ選択してください。）
A. VPCピアリング
B. 共有VPC
C. クラウドVPN
D. 専用相互接続
E. クラウドNAT
正解: **C,D** (コメントを発表する)
https://cloud.google.com/vpc/docs/vpc

質問: **45**
Cloud DNSに移行していて、BINDゾーンファイルをインポートしたいと考えています。どのコマンドを使用する必要がありますか？
A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE
B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE
C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE
D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE
正解: (正解を表示します)
他のプロバイダーからエクスポートされたファイルを取得したら、gcloud dns record-setsimportコマンドを使用してファイルを管理対象ゾーンにインポートできます。
レコードセットをインポートするには、dns record-setsimportコマンドを使用します。--zone-file-formatフラグは、BINDゾーン形式のファイルを予期するようにimportに指示します。このフラグを省略すると、インポートではYAML形式のレコードファイルが必要になります。

質問: **46**
オンプレミスホストにHTTPおよびTFTPサービスを提供する新しい内部アプリケーションを展開しました。複数のComputeEngineインスタンスにトラフィックを分散できるように

する必要がありますが、クライアントが両方のサービスの特定のインスタンスに固定されていることを確認する必要があります。
どのセッションアフィニティを選択する必要がありますか？
A. なし
B. クライアントIP
C. クライアントIPとプロトコル
D. クライアントのIP、ポート、プロトコル
正解: **(**正解を表示します**)**

質問: **47**
エンドユーザーは、us-east1とeurope-west1のすぐ近くにいます。それらのワークロードは相互に通信する必要があります。コストを最小限に抑え、ネットワーク効率を向上させたいと考えています。
このトポロジをどのように設計する必要がありますか？
A. それぞれ独自のリージョンと個別のサブネットを持つ2つのVPCを作成します。2つのVPNゲートウェイを作成して、これらのリージョン間の接続を確立します。
B. それぞれが独自のリージョンと個別のサブネットを持つ2つのVPCを作成します。インスタンスで外部IPアドレスを使用して、これらのリージョン間の接続を確立します。
C. 2つのリージョナルサブネットを使用して1つのVPCを作成します。グローバルロードバランサーを作成して、リージョン間の接続を確立します。
D. 2つのリージョナルサブネットで1つのVPCを作成します。これらのサブネットにワークロードを展開し、プライベートRFC1918IPアドレスを使用して通信させます。
正解: **(**正解を表示します**)**
https://cloud.google.com/vpc/docs/using-vpc#create-auto-network
自動モードで1つのVPCネットワークを作成し、各GoogleCloudリージョンに1つのサブネットを自動的に作成します。したがって、リージョンus-east1とeurope-west1は同じネットワーク内にあり、異なるリージョンにある場合でも、内部IPアドレスを使用して通信できます。彼らはGoogleのグローバルファイバーネットワークを利用しています。

質問: **48**
プロジェクト内のすべてのインスタンスは、カスタムメタデータのenable-oslogin値をFALSEに設定し、プロジェクト全体のSSHキーをブロックするように構成されています。どのインスタンスにもSSHキーが設定されておらず、プロジェクト全体のSSHキーが構成されていません。ファイアウォールルールは、任意のIPアドレス範囲からのSSHセッションを許可するように設定されています。SSHで1つのインスタンスにしたいとします。
あなたは何をするべきか？
A. gcloudcomputesshを使用してインスタンスへのCloudShellSSHを開きます。
B. カスタムメタデータenable-osloginをTRUEに設定し、puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
C. 新しいSSHキーペアを生成します。公開鍵の形式を確認し、プロジェクトに追加します。puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
D. 新しいSSHキーペアを生成します。秘密鍵の形式を確認し、それをインスタンスに追加します。puttyやsshなどのサードパーティツールを使用してインスタンスにSSHで接続します。
正解: **(**正解を表示します**)**

質問: **49**
オンプレミスのデータセンターで重要なアプリケーションを実行するためのネットワーク容量が不足しています。アプリケーションをGCPに移行する必要があります。また、セキュリティチームがComputeEngineインスタンスとの間のトラフィックを監視する機能を失わないようにする必要があります。
ソリューションに組み込む必要がある2つの製品はどれですか？ 2つ選択してください。）
A. VPCフローログ
B. ファイアウォールログ
C. クラウド監査ログ
D. Stackdriverトレース
E. ComputeEngineインスタンスのシステムログ
正解: **(**正解を表示します**)**
A :VPCフローログの使用VPCフローログは、GKEノードとして使用されるインスタンスを含むVMインスタンスとの間で送受信されるネットワークフローのサンプルを記録します。これらのログは、ネットワークモニタリング、フォレンジック、リアルタイムのセキュリティ分析、および経費の最適化に使用できます。https://cloud.google.com/vpc/docs/using-flow-logs B）ファイアウォールルールログの概要ファイアウォールルールログを使用すると、ファイアウォールルールの効果を監査、検証、分析できます。たとえば、トラフィックを拒否するように設計されたファイアウォールルールが意図したとおりに機能しているかどうかを判断できます。ファイアウォールルールログは、特定のファイアウォールルールの影響を受ける接続の数を特定する必要がある場合にも役立ちます。接続をログに記録する必要があるファイアウォールルールごとに、ファイアウォールルールのログを個別に有効にします。ファイアウォールルールロギングは、ファイアウォールルールのオプションで

す。ルールのアクション（許可または拒否）または方向（入力または出力）に関係なく。https://cloud.google.com/vpc/docs/firewall-rules-logging

質問: **50**
Google Kubernetes Engineプライベートクラスタを作成し、kubectlを使用してポッドのステータスを取得したいとします。
インスタンスの1つでは、クラスターが稼働しているにもかかわらず、マスターが応答していないことに気付きます。
問題を解決するためにあなたは何をすべきですか？
A. インスタンスがマスターと通信できるように、適切なマスター承認済みネットワークエントリを作成します。
B. マスターノードのIPアドレスからインスタンスへのトラフィックを許可するために、VPCに適切なファイアウォールポリシーを作成します。
C. インスタンスにパブリックIPアドレスを割り当てます。
D. デフォルトのインターネットゲートウェイを指す、マスターに到達するためのルートを作成します。
正解: **(**正解を表示します**)**

質問: **51**
オンプレミスとGCPの間でCloudVPNの使用を増やしており、単一のトンネルで処理できるよりも多くのトラフィックをサポートしたいと考えています。CloudVPNを使用して使用可能な帯域幅を増やしたい。
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トンネルを同じCloudVPNゲートウェイ上に作成します。
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。
同じIP範囲を転送するが、新しいオンプレミスゲートウェイIPを指す2番目のトンネルを既存のクラウドVPNゲートウェイに作成します。
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CloudVPNゲートウェイを追加します。
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IPアドレスを指す2番目のクラウドVPNゲートウェイに新しいトンネルを作成します。
正解: **(**正解を表示します**)**
https://cloud.google.com/vpn/docs/concepts/classic-topologies

質問: **52**
オンプレミスのデータセンターには、各ルーターのVPNを介してGoogleCloud環境に接続された2台のルーターがあります。すべてのアプリケーションが正しく機能しています。た

だし、すべてのトラフィックは、必要に応じて2つの接続間で負荷分散されるのではなく、単一のVPNを通過します。
トラブルシューティング中に、次のことがわかります。
*各オンプレミスルーターは一意のASNで構成されます。
*各オンプレミスルーターは同じルートと優先度で構成されています。
*両方のオンプレミスルーターは、単一のクラウドルーターに接続されたVPNで構成されています。
* BGPセッションは、オンプレミスルーターとクラウドルーターの両方の間で確立されます。
*オンプレミスルーターのルートのうち1つだけがルーティングテーブルに追加されています。
この問題の最も可能性の高い原因は何ですか？
A. オンプレミスルータで使用されているASNが異なります。
B. ネットワークトラフィックの負荷を分散するためのロードバランサーがありません。
C. ファイアウォールが2番目のVPN接続を介したトラフィックをブロックしています。
D. オンプレミスルーターは同じルートで構成されています。
正解: **(**正解を表示します**)**

質問: **53**
2つのオブジェクトを含むストレージバケットがあります。バケットでCloudCDNが有効になっており、両方のオブジェクトが正常にキャッシュされています。ここで、2つのオブジェクトのいずれかがキャッシュされなくなり、常にオリジンから直接インターネットに提供され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. キャッシュしたくないオブジェクトが公開されていないことを確認します。
B. 新しいストレージバケットを作成し、チェックしたくないオブジェクトをその中に移動します。次に、バケット設定を編集して、プライベート属性を有効にします。
C. 2つのオブジェクトを含むストレージバケットに適切なライフサイクルルールを追加します。
D. もうキャッシュしたくないオブジェクトのメタデータにプライベートな値を持つCache-Controlエントリを追加します。以前にキャッシュされたすべてのコピーを無効にします。
正解: **A (**コメントを発表する**)**
参照：
https://developers.google.com/web/ilt/pwa/caching-files-with-service-worker

質問: **54**
2つのオブジェクトを含むストレージバケットがあります。バケットでCloudCDNが有効になっており、両方のオブジェクトが正常にキャッシュされています。ここで、2つのオブ

ジェクトのいずれかがキャッシュされなくなり、常にオリジンから直接インターネットに提供され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. キャッシュしたくないオブジェクトが公開されていないことを確認します。
B. 新しいストレージバケットを作成し、チェックしたくないオブジェクトをその中に移動します。次に、バケット設定を編集して、privateattributeを有効にします。
C. 2つのオブジェクトを含むストレージバケットに適切なライフサイクルルールを追加します。
D. もうキャッシュしたくないオブジェクトのメタデータにプライベートな値を持つCache-Controlentryを追加します。以前にキャッシュされたすべてのコピーを無効にします。
正解: **A** (コメントを発表する)
説明/参照：https ://developers.google.com/web/ilt/pwa/caching-files-with-service-worker

質問: **55**
共有VPCアーキテクチャを設計しています。ネットワークおよびセキュリティチームは、部門間で公開されるルートを厳密に制御します。制作部門とステージング部門は相互に通信できますが、特定のネットワークを介してのみ通信できます。Googleが推奨する方法に従いたい。
このトポロジをどのように設計する必要がありますか？
A. 共有VPCホストプロジェクト内に2つの共有VPCを作成し、それらの間でVPCピアリングを有効にします。
ファイアウォールルールを使用して、特定のネットワーク間のアクセスをフィルタリングします。
B. 共有VPCホストプロジェクト内に2つの共有VPCを作成し、それらの間にCloud VPN /CloudRouterを作成します。
フレキシブルルートアドバタイズメント（FRA）を使用して、特定のネットワーク間のアクセスをフィルタリングします。
C. 共有VPCサービスプロジェクト内に2つの共有VPCを作成し、それらの間にクラウドVPN/クラウドルーターを作成します。
フレキシブルルートアドバタイズメント（FRA）を使用して、特定のネットワーク間のアクセスをフィルタリングします。
D. 共有VPCホストプロジェクト内に1つのVPCを作成し、個々のサブネットをサービスプロジェクトと共有して、特定のネットワーク間のアクセスをフィルタリングします。
正解: (正解を表示します)
https://cloud.google.com/vpc/docs/shared-vpc

質問: **56**
オンプレミスのデータセンターで重要なアプリケーションを実行するためのネットワーク容量が不足しています。

アプリケーションをGCPに移行する必要があります。また、セキュリティチームがComputeEngineインスタンスとの間のトラフィックを監視する機能を失わないようにする必要があります。
ソリューションに組み込む必要がある2つの製品はどれですか？ 2つ選択してください。）
A. VPCフローログ
B. ファイアウォールログ
C. クラウド監査ログ
D. Stackdriverトレース
E. ComputeEngineインスタンスのシステムログ
正解: **(**正解を表示します**)**
説明/参照 :https ://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

質問: **57**
オンプレミスとGCPの間でCloudVPNの使用を増やしており、単一のトンネルで処理できるよりも多くのトラフィックをサポートしたいと考えています。CloudVPNを使用して使用可能な帯域幅を増やしたい。
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トンネルを同じCloudVPNゲートウェイ上に作成します。
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。同じIP範囲を転送するが、新しいオンプレミスゲートウェイIPを指す2番目のトンネルを既存のクラウドVPNゲートウェイに作成します。
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CloudVPNゲートウェイを追加します。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IPアドレスを指す2番目のクラウドVPNゲートウェイに新しいトンネルを作成します。
正解: **(**正解を表示します**)**
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#redundancy-options

質問: **58**
VPCの1つのインスタンスは、プライベートIPアドレスのみで実行するように構成されています。このインスタンスが削除された場合でも、現在のプライベートIPアドレスが別のインスタンスに自動的に割り当てられないようにする必要があります。
GCPコンソールで何をすべきですか？
A. インスタンスにパブリックIPアドレスを割り当てます。
B. 新しい予約済みの内部IPアドレスをインスタンスに割り当てます。
C. インスタンスの現在の内部IPアドレスを静的に変更します。

D. キーinternal-addressとvalueが予約されているインスタンスにカスタムメタデータを追加します。
正解: **(**正解を表示します**)**
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#reservenewipここからhttps://cloud.google.com/compute/docs/ip-addresses/reserve -static-internal-ip-address＃reservenewip 既存のサブネットから自動的に割り当てられたアドレスまたは未使用のアドレス」と記述されています。

質問: **59**
ユーザーが3つのVPCすべてのリソースにアクセスできるように、3つの仮想プライベートクラウドネットワーク、Sales、Marketing、Financeの間にネットワーク接続を確立する必要があります。SalesVPCとFinanceVPCの間でVPCピアリングを設定します。また、MarketingVPCとFinanceVPC間のVPCピアリングを設定します。構成を完了すると、一部のユーザーはSalesVPCおよびMarketingVPCのリソースに接続できなくなります。問題を解決したい。
あなたは何をするべきか？
A. フルメッシュでVPCピアリングを設定します。
B. ルーティングテーブルを変更して、非対称ルートを解決します。
C. ネットワークタグを作成して、3つのVPCすべて間の接続を許可します。
D. レガシーネットワークを削除して再作成し、推移的なピアリングを許可します。
正解: **(**正解を表示します**)**
https://cloud.google.com/vpc/docs/using-vpc-peering

質問: **60**
IPv6を使用してGCPでサービスを作成したいとします。
あなたは何をするべきか？
A. 指定されたIPv6アドレスでインスタンスを作成します。
B. 指定されたIPv6アドレスでグローバルロードバランサーを構成します。
C. 指定されたIPv6アドレスで内部ロードバランサーを構成します。
D. 指定されたIPv6アドレスでTCPプロキシを設定します。
正解: **(**正解を表示します**)**

質問: **61**
ユーザーが3つのVPCすべてのリソースにアクセスできるように、3つの仮想プライベートクラウドネットワーク、Sales、Marketing、Financeの間にネットワーク接続を確立する必要があります。SalesVPCとFinanceVPCの間でVPCピアリングを設定します。また、MarketingVPCとFinanceVPC間のVPCピアリングを設定します。構成を完了すると、一部のユーザーはSalesVPCおよびMarketingVPCのリソースに接続できなくなります。問題を解決したい。

あなたは何をするべきか？
A. ルーティングテーブルを変更して、非対称ルートを解決します。
B. 3つのVPCすべて間の接続を可能にするネットワークタグを作成します。
C. フルメッシュでVPCピアリングを設定します。
D. レガシーネットワークを削除して再作成し、推移的なピアリングを許可します。
正解: **(**正解を表示します**)**

質問: **62**
2つのクラウドルーターを設定して、一方がアクティブなボーダーゲートウェイプロトコル（BGP）セッションを持ち、もう一方がスタンバイとして機能するようにします。
オンプレミスルーターでどのBGP属性を使用する必要がありますか？
A. AS-Path
B. コミュニティ
C. ローカルプリファレンス
D. 複数出口弁別器
正解: **(**正解を表示します**)**
説明/参照：https://cloud.google.com/router/docs/concepts/overview

質問: **63**
ネットワーク変更ウィンドウの後、会社のアプリケーションの1つが動作を停止します。アプリケーションは、アプリケーションからトラフィックを受信しなくなったオンプレミスデータベースサーバーを使用します。データベースサーバーのIPアドレスは10.2.1.25です。変更リクエストを確認します。唯一の変更は、3つの追加のVPCサブネットが作成されたことです。作成された新しいVPCサブネットは、10.1.0.0 / 16、10.2.0.0 / 16、および10.3.1.0/24/です。オンプレミスルーターは10.0.0.0/8をアドバタイズします。
この問題の最も可能性の高い原因は何ですか？
A. あまり具体的でないVPCサブネットルートが優先されます。
B. 変更中に、オンプレミスデータベースサーバーへのトラフィックをブロックするクラウドファイアウォールルールが作成されました。

C. オンプレミスルーターはデータベースサーバーのルートをアドバタイズしていません。
D. より具体的なVPCサブネットルートが優先されます。
正解: **B** (コメントを発表する)

質問: **64**
オンプレミスのデータセンターには、各ルーターのVPNを介してGoogleCloud環境に接続された2台のルーターがあります。すべてのアプリケーションが正しく機能しています。ただし、すべてのトラフィックは、必要に応じて2つの接続間で負荷分散されるのではなく、単一のVPNを通過します。
トラブルシューティング中に、次のことがわかります。
*各オンプレミスルーターは一意のASNで構成されます。
*各オンプレミスルーターは同じルートと優先度で構成されています。
*両方のオンプレミスルーターは、単一のクラウドルーターに接続されたVPNで構成されています。
* BGPセッションは、オンプレミスルーターとクラウドルーターの両方の間で確立されます。
*オンプレミスルーターのルートのうち1つだけがルーティングテーブルに追加されています。
この問題の最も可能性の高い原因は何ですか？
A. オンプレミスルーターは同じルートで構成されています。
B. ファイアウォールが2番目のVPN接続を介したトラフィックをブロックしています。
C. ネットワークトラフィックの負荷を分散するためのロードバランサーがありません。
D. オンプレミスルーターで使用されているASNが異なります。
正解: (正解を表示します)
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting#ecmp

質問: **65**
オンプレミスネットワークとクラウドVPNを介したVPCの間にIPSecトンネルを実装する必要があります。トンネルを介した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、ボーダーゲートウェイプロトコル (BGP) を話すことが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. クラウドルーター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
正解: (正解を表示します)
参照：
https://cloud.google.com/vpn/docs/concepts/overview

質問: **66**
インスタンスグループを作成しており、HTTPの負荷分散のための新しいヘルスチェックを作成する必要があります。
これを達成するために使用できる2つの方法はどれですか？ (2つ選択してください。)
A. gcloudコマンドラインツールを使用して新しいヘルスチェックを作成します。
B. GCPコンソールの[VPCネットワーク]セクションを使用して、新しいヘルスチェックを作成します。
C. GCPコンソールでロードバランサーのバックエンド設定を完了したら、新しいヘルスチェックを作成するか、既存のヘルスチェックを選択します。
D. gcloudコマンドラインツールを使用して、新しいレガシーヘルスチェックを作成します。
E. GCPコンソールの[ヘルスチェック]セクションを使用して、新しいレガシーヘルスチェックを作成します。
正解: **A,E** (コメントを発表する)
参照：
https://cloud.google.com/load-balancing/docs/health-checks

質問: **67**
gcloudコマンドを使用して、ポリシーベースのルーティング用に構成されたCloudVPNゲートウェイの背後にあるオンプレミスリソースへの静的ルートを構成する必要があります。
どのネクストホップを選ぶべきですか？
A. デフォルトのインターネットゲートウェイ
B. CloudVPNゲートウェイのIPアドレス
C. クラウドVPNトンネルの名前と地域
D. VPNトンネルのリモート側にあるインスタンスのIPアドレス
正解: (正解を表示します)
Cloud Consoleを使用してルートベースのトンネルを作成すると、Classic VPNは次の両方のタスクを実行します。トンネルのローカルおよびリモートトラフィックセレクターを任意のIPアドレス (0.0.0.0/0)に設定します。リモートネットワークIP範囲の各範囲について、Google Cloudは、宛先 (プレフィックス)が範囲のCIDRであり、ネクストホップがトンネルであるカスタム静的ルートを作成します。https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns

質問: **68**
ストレージバケット内のすべてのオブジェクトに対してCloudCDNを有効にする必要があります。ストレージバケット内のすべてのオブジェクトがCDNによって提供されることを確認する必要があります。
GCPコンソールで何をすべきですか？

A. 新しいクラウドストレージバケットを作成し、その上でクラウドCDNを有効にします。
B. 新しいSSLプロキシロードバランサーを作成し、ストレージバケットをバックエンドとして選択してから、バックエンドでCloudCDNを有効にします。
C. 新しいTCPロードバランサーを作成し、ストレージバケットをバックエンドとして選択してから、バックエンドでCloudCDNを有効にします。
D. 新しいHTTPロードバランサーを作成し、バックエンドとしてストレージバケットを選択し、バックエンドでCloud CDNを有効にして、ストレージバケット内の各オブジェクトがパブリックに共有されていることを確認します。
正解: **A** (コメントを発表する)

質問: **69**
Google Kubernetes Engine（GKE）にデプロイされているアプリケーションに新しいCloudArmorポリシーを適用したいとします。CloudArmorポリシーに使用するターゲットを見つけ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クラスター
D. GKE入力
正解: **B** (コメントを発表する)
https://cloud.google.com/kubernetes-engine/docs/how-to/cloud-armor-backendconfig

質問: **70**
Cloud Interconnectを使用して、オンプレミスネットワークをGCPVPCに接続するとします。存在点（POP）の場所の1つでGoogleに会うことはできず、オンプレミスルーターはボーダーゲートウェイプロトコル（BGP）構成を実行できません。
どの接続モデルを使用する必要がありますか？
A. ダイレクトピアリング
B. 専用相互接続
C. レイヤー2パートナーとのパートナー相互接続
D. レイヤー3パートナーとのパートナー相互接続
正解: (正解を表示します)
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overviewレイヤー3接続の場合、サービスプロバイダーは、VLAN接続ごとにクラウドルーターとそのエッジルーターの間にBGPセッションを確立します。オンプレミスルーターでBGPを構成する必要はありません。Googleとサービスプロバイダーは、正しい構成を自動的に設定します。
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview#connectivity-type

質問: **71**
単一のサブネットを持つDevという名前の新しいVPCネットワークを作成しました。ネットワーク開発にファイアウォールルールを追加して、HTTPトラフィックのみを許可し、ロギングを有効にしました。リモートデスクトッププロトコルを介してサブネット内のインスタンスにログインしようとすると、ログインは失敗します。Stackdriver Loggingでファイアウォールルールログを探しますが、ブロックされたトラフィックのエントリは表示されません。ブロックされたトラフィックのログを表示する必要があります。
あなたは何をするべきか？
A. インスタンスのVPCフローログを確認します。
B. SSH経由でインスタンスに接続してみて、ログを確認してください。
C. ポート22からのトラフィックを許可し、ログを有効にする新しいファイアウォールルールを作成します。
D. 優先度65500の新しいファイアウォールルールを作成して、すべてのトラフィックを拒否し、ログを有効にします。
正解:
DVPCフローログの入力パケットは、入力ファイアウォールルールの後にサンプリングされます
。入力ファイアウォールルールがインバウンドパケットを拒否する場合、それらのパケットはVPCフローログによってサンプリングされません。ブロックされたトラフィックのログを確認したいので、ファイアウォールログでそれらを探す必要があります。https://cloud.google.com/vpc/docs/flow-logs#key_properties

質問: **72**
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アドレスでデプロイされ、外部アクセスはグローバルロードバランサーを介して許可されます。最近、トラフィックスクラビングサービスを利用していて、オリジンを制限して、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CloudArmor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VPCサービス制御境界を作成します。
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。
正解: **(正解を表示します)**

グローバルロードバランサーは接続をプロキシします。したがって、セッションオリジンIPのトレースはありません。サービスをジオフェンスするには、CloudArmorを使用する必要があります。
https://cloud.google.com/load-balancing/docs/https

質問: **73**
サードパーティの次世代ファイアウォールを使用してトラフィックを検査しています。出力トラフィックをファイアウォールにルーティングするために、0.0.0.0/0のカスタムルートを作成しました。パブリックIPアドレスのないVPCインスタンスが、ファイアウォールを介してトラフィックを送信せずに、BigQueryおよびCloud Pub /SubAPIにアクセスできるようにする必要があります。
あなたはどちらの2つの行動を取るべきですか？ 2つ選択してください。）
A. サブネットレベルでプライベートGoogleアクセスをオンにします。
B. VPCレベルでプライベートGoogleアクセスをオンにします。
C. VPCレベルでプライベートサービスアクセスをオンにします。
D. デフォルトのインターネットゲートウェイを介してGoogleAPIとサービスの外部IPアドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
E. デフォルトのインターネットゲートウェイを介してGoogleAPIとサービスの内部IPアドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
正解: **A,D (**コメントを発表する**)**
https://cloud.google.com/vpc/docs/private-access-options#pga内部IPアドレスのみ（外部IPアドレスなし）のプライベートGoogleAccessVMインスタンスはプライベートGoogleAccessを使用できます。GoogleAPIとサービスの_外部IPアドレス_に到達できます。

質問: **74**
Google Kubernetes Engineプライベートクラスタを作成し、kubectlを使用してポッドのステータスを取得したいとします。インスタンスの1つでは、クラスターが稼働しているにもかかわらず、マスターが応答していないことに気付きます。
問題を解決するためにあなたは何をすべきですか？
A. インスタンスにパブリックIPアドレスを割り当てます。
B. デフォルトのインターネットゲートウェイを指す、マスターに到達するためのルートを作成します。
C. マスターノードのIPアドレスからインスタンスへのトラフィックを許可するために、VPCに適切なファイアウォールポリシーを作成します。
D. インスタンスがマスターと通信できるように、適切なマスター承認済みネットワークエントリを作成します。
正解: **(**正解を表示します**)**
https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#cant_reach_cluster

https://cloud.google.com/kubernetes-engine/docs/how-to/authorized-networks

質問: **75**
サードパーティの次世代ファイアウォールを使用してトラフィックを検査しています。出力トラフィックをファイアウォールにルーティングするために、0.0.0.0 / 0のカスタムルートを作成しました。パブリックIPアドレスのないVPCインスタンスが、ファイアウォールを介してトラフィックを送信せずに、BigQueryおよびCloud Pub / SubAPIにアクセスできるようにする必要があります。
あなたはどちらの2つの行動を取るべきですか？ 2つ選択してください。）
A. デフォルトのインターネットゲートウェイを介してGoogleAPIとサービスの外部IPアドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
B. サブネットレベルでプライベートGoogleアクセスをオンにします。
C. VPCレベルでプライベートサービスアクセスをオンにします。
D. VPCレベルでプライベートGoogleアクセスをオンにします。
E. デフォルトのインターネットゲートウェイを介してGoogleAPIとサービスの内部IPアドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
正解: **C,E (**コメントを発表する**)**

質問: **76**
オンプレミスとGCPの間でCloudVPNの使用を増やしており、単一のトンネルで処理できるよりも多くのトラフィックをサポートしたいと考えています。CloudVPNを使用して使用可能な帯域幅を増やしたい。
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. 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。同じIP範囲を転送するが、新しいオンプレミスゲートウェイIPを指す2番目のトンネルを既存のクラウドVPNゲートウェイに作成します。
C. 同じ宛先VPNゲートウェイIPアドレスを指す2つのVPNトンネルを同じCloudVPNゲートウェイ上に作成します。
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CloudVPNゲートウェイを追加します。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IPアドレスを指す2番目のクラウドVPNゲートウェイに新しいトンネルを作成します。
正解: **(**正解を表示します**)**

質問: **77**
オンプレミスネットワークブロックとGCPの間でアドレス変換を実行するようにNATを設定する必要があります。
どのNATソリューションを使用する必要がありますか？
A. IP転送が有効になっているインスタンス
B. クラウドNAT
C. iptablesDNATルールで構成されたインスタンス
D. iptablesSNATルールで構成されたインスタンス
正解: **(**正解を表示します**)**

質問: **78**
インスタンスを単一のComputeEngineゾーンに手動で配置することにより、概念実証アプリケーションをデプロイしました。現在、アプリケーションを本番環境に移行しているため、アプリケーションの可用性を高め、自動スケーリングできるようにする必要があります。
インスタンスをどのようにプロビジョニングする必要がありますか？
A. 単一のマネージドインスタンスグループを作成し、目的のリージョンを指定して、場所として[複数のゾーン]を選択します。
B. リージョンごとに管理対象インスタンスグループを作成し、場所として[単一ゾーン]を選択して、そのリージョン内のゾーン全体にインスタンスを手動で分散します。
C. 単一ゾーンにアンマネージドインスタンスグループを作成してから、インスタンスグループのHTTPロードバランサーを作成します。
D. ゾーンごとにアンマネージドインスタンスグループを作成し、インスタンスを目的のゾーンに手動で分散します。
正解: **B (**コメントを発表する**)**
説明/参照 :https ://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

質問: **79**
Cloud DNSに移行していて、BINDゾーンファイルをインポートしたいと考えています。
どのコマンドを使用する必要がありますか？
A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE
B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE
C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE

D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE

正解: **(**正解を表示します**)**

他のプロバイダーからエクスポートされたファイルを取得したら、gcloud dnsrecord-setsimportコマンドを使用してファイルを管理対象ゾーンにインポートできます。

レコードセットをインポートするには、dnsrecord-setsimportコマンドを使用します。--zone-file-formatフラグは、BINDゾーン形式のファイルを予期するようにimportに指示します。このフラグを省略すると、インポートではYAML形式のレコードファイルが必要になります。

https://medium.com/@prashantapaudel/gcp-certification-series-2-4-planning-and-configuring-network-resources-8045ac2cc2ac