Google Cloud Certified - Professional Cloud Network Engineer (Japanese Version)

1. あなたは、3 層アプリケーション アーキテクチャをオンプレミスから Google Cloud に移行しています。移行の最初のステップとして、外部 HTTP(S) ロード バランサを使用して新しい Virtual Private Cloud (VPC) を作成します。このロード バランサーは、プレゼンテーション層を実行するオンプレミスのコンピューティング リソースにトラフィックを転送します。悪意のあるトラフィックが VPC に入り、エッジでリソースを消費するのを阻止する必要があるため、IP アドレスをフィルタリングし、クロスサイト スクリプティング (XSS) 攻撃を阻止するようにこのポリシーを構成する必要があります。あなたは何をするべきか？

A. Google Cloud Armor ポリシーを作成し、インターネット ネットワーク エンドポイント グループ (NEG) バックエンドを使用するバックエンド サービスに適用します。

B. 階層型ファイアウォール ルールセットを作成し、VPC の親組織リソース ノードに適用します。

C. VPC ファイアウォール ルールセットを作成し、それを非マネージド インスタンス グループ内のすべてのインスタンスに適用します。

D. Google Cloud Armor ポリシーを作成し、アンマネージド インスタンス グループ バックエンドを使用するバックエンド サービスに適用します。

Answer(s): A

---

2. IPv4 と IPv6 の両方のアドレスを使用して外部ロード バランサーの背後に公開され、ポート 443 での TCP パススルーをサポートする新しい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たいと考えています。どの構成を使用する必要がありますか?

A. 両方のリージョンのバックエンドでグローバル SSL プロキシ負荷分散を使用します。

B. 両方のリージョンでネットワーク負荷分散を使用し、DNS ベースの負荷分散を使用してトラフィックを最も近いリージョンに送信します。

C. 両方のリージョンのバックエンドでグローバル TCP プロキシ ロード バランシングを使用します。

D. 両方のリージョンのバックエンドでグローバル外部 HTTP(S) 負荷分散を使用します。

Answer(s): B

---

3. あなたの組織には、リージョン us-west2 の仮想マシンからのすべての出力トラフィック ペイロードを監視することを要求する新しいセキュリティ ポリシーがあります。新しいポリシーを満たすために、同じリージョンに侵入検知システム (IDS) 仮想アプライアンスをデプロイしました。us-west2 からのすべての出力トラフィック ペイロードを監視するには、IDS を環境に統合する必要があります。あなたは何をするべきか？

A. ファイアウォール ログを有効にし、フィルタリングされたすべての出力ファイアウォール ログを IDS に転送します。

B. VPC フロー ログを有効にします。Cloud Logging でシンクを作成し、フィルタリングされた下り VPC フロー ログを IDS に送信します。

C. パケット ミラーリング用の内部 TCP/UDP ロード バランサーを作成し、出力トラフィック用のパケット ミラーリング ポリシー フィルターを追加します。

D. パケット ミラーリング用の内部 HTTP(S) ロード バランサを作成し、出力トラフィック用のパケット ミラーリング ポリシー フィルタを追加します。

Answer(s): B

---

4. あなたの会社には、Cloud Interconnect を使用してオンプレミス ネットワークからアクセスできる、Google Cloud にデプロイされた単一の Virtual Private Cloud (VPC) ネットワークがあります。サービス レベル アグリーメント (SLA) が適用されたハイブリッド接続を介して、VPC Service Controls によってサポートされる Google API およびサービスへのアクセスのみを構成する必要があります。あなたは何をするべきか？

A. Google API のパブリック仮想 IP アドレスをアドバタイズするように既存の Cloud Router を構成します。

B. limited.googleapis.com 仮想 IP アドレスを持つオンプレミス ホストには限定公開の Google アクセスを使用します。

C. ダイレクト ピアリング リンクを追加し、パブリック仮想 IP アドレスを使用する Google API への接続に使用します。

D. デフォルト ルートをアドバタイズするように既存の Cloud Router を構成し、Cloud NAT を使用してオンプレミス ネットワークからのトラフィックを変換します。

Answer(s): B

---

5. 新しいアプリケーションを作成していて、パブリック IP アドレスなしで VPC インスタンスから Cloud SQL にアクセスする必要があるとします。

A. プロジェクトでサービス ネットワーキング API をアクティブ化します。

B. プロジェクトで Cloud Datastore API をアクティブ化します。

C. サービス プロデューサーへのプライベート接続を作成します。

D. トラフィックが Cloud SQL API に到達できるようにするカスタム静的ルートを作成します。

E. プライベート Google アクセスを有効にします。

Answer(s): C,E

---

6. Partner Interconnect を使用してオンプレミス ネットワークを VPC に接続したいと考えています。すでに相互接続パートナーがいます。

A. パートナーのポータルにログインし、そこで VLAN アタッチメントを要求します。

B. Interconnect パートナーに、Google への物理接続をプロビジョニングするよう依頼します。

C. GCP Console で Partner Interconnect タイプの VLAN アタッチメントを作成し、ペアリング キーを取得します。

D. gcloud compute interconnectattachments Partner update <attachment> / --region <region> --admin-enabled を実行します。

Answer(s): B

---

7. データの漏洩を防ぐために、境界内に 2 つの Google Cloud プロジェクトがあります。3 番目のプロジェクトを境界内に移動する必要があります。ただし、この動きは既存の環境に悪影響を与える可能性があります。変更の影響を検証する必要があります。あなたは何をするべきか？

A. 境界内の Resource Manager 監査ログを監視します。

B. 既存の VPC Service Controls ポリシーを変更して、新しいプロジェクトをドライラン モードに含めます。

C. 3 番目のプロジェクト内でファイアウォール ルールのログを有効にします。

D. 3 番目のプロジェクト内の VPC フロー ログを有効にし、悪影響がないかログを監視します。

Answer(s): B

---

8. Compute Engine 仮想マシン インスタンスを NAT ゲートウェイとして構成しました。次のコマンドを実行します。

A. sudo sysctl -w net.ipv4.ip_forward=1

B. gcloud compute インスタンス add-tags [既存のインスタンス] --tags no-ip

C. gcloud builds submit --config=cloudbuild.waml --substitutions=TAG_NAME=no-ip

D. gcloud compute インスタンスが example-instance --networkcustom-network1 を作成します \

Answer(s): B

---

9. マルチリージョン VPC には、企業ネットワークに接続された「リージョン 1」に長年 HA VPN が設定されています。同じ企業ネットワークに接続するために、「リージョン 2」に 2 つの 10 Gbps Dedicated Interconnect 接続と VLAN アタッチメントを追加する予定です。トラフィックが Dedicated Interconnect 接続をプライマリ パスとして使用し、HA VPN をセカンダリ パスとして使用するように、VPC と企業ネットワーク間の接続を計画する必要があります。どうすればよいですか?

A. VPC でリージョン ダイナミック ルーティング モードを有効にします。「リージョン 1」の HA VPN に関連付けられた BGP を、基本優先度値 100 を使用するように設定します。VLAN アタッチメントに関連付けられた BGP を、基本優先度 20000 を使用するように設定します。オンプレミス ルーターを、同様のマルチエグジット識別子 (MED) 値を使用するように設定します。

B. VPC でグローバル ダイナミック ルーティング モードを有効にします。「リージョン 1」の HA VPN に関連付けられた BGP を、基本優先度値 100 を使用するように設定します。VLAN アタッチメントに関連付けられた BGP を、基本優先度 20000 を使用するように設定します。オンプレミス ルーターを、同様のマルチエグジット識別子 (MED) 値を使用するように設定します。

C. VPC でリージョン ダイナミック ルーティング モードを有効にします。「リージョン 1」の HA VPN に関連付けられた BGP を、基本優先度値 20000 を使用するように設定します。VLAN アタッチメントに関連付けられた BGP を、基本優先度 100 を使用するように設定します。オンプレミス ルーターを、同様のマルチエグジット識別子 (MED) 値を使用するように設定します。

D. VPC でグローバル ダイナミック ルーティング モードを有効にします。「リージョン 1」の HA VPN に関連付けられた BGP を、基本優先度値 20000 を使用するように設定します。VLAN アタッチメントに関連付けられた BGP を、基本優先度 100 を使用するように設定します。オンプレミス ルーターを、同様のマルチエグジット識別子 (MED) 値を使用するように設定します。

Answer(s): B

---

10. あなたの組織は、ホスト プロジェクトと 3 つのサービス プロジェクトを持つ共有 VPC アーキテクチャを使用しています。サービス プロジェクト内に Compute Engine インスタンスが存在します。オンプレミスのデータセンターには重要なワークロードがあります。ハイブリッド接続を確立するためにデプロイした D dedicated Interconnect を介して、Google Cloud インスタンスがオンプレミスのホスト名を解決できることを確認する必要があります。あなたは何をするべきか？

A. プライベート ゾーンをオンプレミス DNS サーバーに転送する、共有 VPC のホスト プロジェクトに Cloud DNS プライベート転送ゾーンを作成します。Cloud Router で、IP 169.254 169.254 のカスタム ルート アドバタイズメントをオンプレミス環境に追加します。

B. 共有 VPC のホスト プロジェクトで Cloud DNS プライベート ゾーンを構成します。オンプレミス DNS サーバー上の Google Cloud プライベート ゾーンへの DNS 転送を設定し、ホスト プロジェクトの受信フォワーダー IP アドレスを指すようにします。共有 VPC で DNS ポリシーを構成し、オンプレミスの DNS サーバーを代替 DNS サーバーとして使用した受信クエリの転送を許可します。

C. 共有 VPC のホスト プロジェクトで Cloud DNS プライベート ゾーンを構成します。オンプレミス DNS サーバー上の Google Cloud プライベート ゾーンへの DNS 転送を設定し、ホスト プロジェクトの受信フォワーダー IP アドレスを指すようにします。 Cloud Router で、IP 169.254 169 254 のカスタム ルート アドバタイズメントをオンプレミスに追加します。環境。

D. プライベート ゾーンをオンプレミス DNS サーバーに転送する、共有 VPC のホスト プロジェクトに Cloud DNS プライベート転送ゾーンを作成します。Cloud Router で、IP 35.199.192.0/19 のカスタム ルート アドバタイズメントをオンプレミス環境に追加します。

Answer(s): B

---

11. インスタンス グループを作成しているため、HTTP(s) ロード バランシング用の新しいヘルス チェックを作成する必要があります。

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 Console 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 Console でロードバランサのバックエンド構成を完了したら、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 Console 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。

Answer(s): A,C

---

12. IPv6 を使用して GCP でサービスを作成したいと考えています。

A. 指定した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 アドレスを使用して TCP プロキシを構成します。

C. 指定したIPv6アドレスでグローバルロードバランサを設定します。

D. 指定された IPv6 アドレスを使用して内部ロード バランサーを構成します。

Answer(s): C

---

13. あなたの会社は Google Kubernetes Engine への移行を計画しています。アプリケーション チームは、ノードあたり最小 60 ポッド、ノードあたり最大 100 ポッドが必要であると通知しました。ノードあたりどのポッド CIDR 範囲を使用する必要がありますか?

A. /24

B. /25

C. /26

D. /28

Answer(s): B

---

14. あなたの会社は最近、EMEA ベースの事業を APAC に拡大しました。世界中に分散しているユーザーから、SMTP サービスと IMAP サービスが遅いと報告されています。あなたの会社ではエンドツーエンドの暗号化が必要ですが、SSL 証明書にアクセスできません。

A. SSL プロキシ ロード バランサ

B. ネットワークロードバランサー

C. HTTPS ロードバランサ

D. TCP プロキシ ロード バランサ

Answer(s): D

---

15. 組織には、大量のデータを扱う地理的に分散したアプリケーションがあります。HTTPS ワークロードをグローバルに公開し、トラフィック コストを最小限に抑える設計を作成する必要があります。どうすればよいでしょうか。

A. 標準ネットワーク サービス ティアを使用して、リージョン外部アプリケーション ロード バランサーをデプロイします。

B. プレミアム ネットワーク サービス ティアを使用して、リージョン外部アプリケーション ロード バランサーをデプロイします。

C. 標準ネットワーク サービス ティアでグローバル外部プロキシ ネットワーク ロード バランサーをデプロイします。

D. プレミアム ネットワーク サービス ティアを使用してグローバル外部アプリケーション ロード バランサーをデプロイします。

Answer(s): D

---

16. 最近、アプリケーションへのトラフィックを管理するために Google Cloud Armor セキュリティ ポリシーを構成しました。Google Cloud Armor がアプリケーションへの一部のトラフィックを誤ってブロックしていることに気づきました。トラフィックを誤ってブロックしている Web アプリケーション ファイアウォール (WAF) ルールを特定する必要があります。あなたは何をするべきか？

A. VPC フロー ログを有効にし、Cloud Logging でログを表示します。

B. ファイアウォール ログを有効にし、ファイアウォール インサイトでログを表示します。

C. Google Cloud Armor 監査ログを有効にし、Google Cloud Console の [アクティビティ] ページでログを表示します。

D. サンプリング レートを 1 に設定して HTTP(S) ロード バランシングのログを有効にし、Cloud Logging でログを表示します。

Answer(s): B

---

17. 組織には、us-west2 リージョンの仮想マシンからのすべての出力トラフィック ペイロードを監視することを要求する新しいセキュリティ ポリシーがあります。新しいポリシーを満たすために、同じリージョンに侵入検知システム (IDS) 仮想アプライアンスを導入しました。次に、us-west2 からのすべての出力トラフィック ペイロードを監視するために、IDS を環境に統合する必要があります。どうすればよいでしょうか。

A. ファイアウォールのログ記録を有効にし、フィルタリングされたすべての出力ファイアウォール ログを IDS に転送します。

B. パケットミラーリング用の内部 HTTP(S) ロードバランサーを作成し、出力トラフィック用のパケットミラーリングポリシーフィルターを追加します。

C. パケットミラーリング用の内部 TCP/UDP ロードバランサーを作成し、出力トラフィック用のパケットミラーリングポリシーフィルターを追加します。

D. VPC フローログを有効にします。Cloud Logging にシンクを作成し、フィルタリングされた出力 VPC フローログを IDS に送信します。

Answer(s): C

---

18. 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 を構成したいと考えています。

A. クラウド NAT

B. IP 転送が有効になっているインスタンス

C. iptables SNAT ルールで構成されたインスタンス

D. iptables DNAT ルールで構成されたインスタンス

Answer(s): A

---

19. あなたの会社は最近、オンプレミス データセンターと Google Cloud Virtual Private Cloud (VPC) の間に Cloud VPN トンネルを設置しました。オンプレミス サーバーの Cloud Functions API へのアクセスを構成する必要があります。構成は次の要件を満たす必要があります。

A. 199.36.153.4/30 のアドレス範囲を使用して、restricted.googleapis.com の A レコードを作成します。A レコードを指す *.googleapis.com の CNAME レコードを作成します。A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。オンプレミスのファイアウォールを構成して、restricted.googleapis.com アドレスへのトラフィックを許可します。

B. 199.36.153.8/30 のアドレス範囲を使用して、private.googleapis.com の A レコードを作成します。A レコードを指す *.googleapis.com の CNAME レコードを作成します。A レコードで使用したアドレスの

ネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。Cloud VPN トンネルが終了する VPC からデフォルトのインターネット ゲートウェイを削除します。

C. 199.36.153.8/30 のアドレス範囲を使用して、private.googleapis.com の A レコードを作成します。A レコードを指す *.googleapis.com の CNAME レコードを作成します。A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。private.googleapis.com アドレスへのトラフィックを許可するようにオンプレミスのファイアウォールを構成します。

D. 199.36.153.4/30 のアドレス範囲を使用して、restricted.googleapis.com の A レコードを作成します。A レコードを指す *.googleapis.com の CNAME レコードを作成します。A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。Cloud VPN トンネルが終了する VPC からデフォルトのインターネット ゲートウェイを削除します。

Answer(s): D

---

20. フロントエンド アプリケーション VM とバックエンド データベース VM はすべて同じ VPC にデプロイされていますが、サブネットは異なります。グローバル ネットワーク ファイアウォール ポリシー ルールは、フロントエンド VM からバックエンド VM へのトラフィックを許可するように構成されています。最近のコンプライアンス要件に基づき、このトラフィックは、同じ VPC にデプロイされているネットワーク仮想アプライアンス (NVA) ファイアウォールによって検査される必要があります。NVA は完全なネットワーク プロキシとして構成されており、NAT 許可トラフィックを送信します。NVA がサブネット間のトラフィックを検査できるように、VPC ルーティング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. NVA を ilb1 という名前の内部パススルー ネットワーク ロード バランサーの背後に配置します。グローバル ネットワーク ファイアウォール ポリシー ルールを追加して、NVA を通過するトラフィックを許可します。バックエンド VM サブネットの宛先 IP 範囲、フロントエンド インスタンス タグ、および ilb1 のネクストホップを使用して、カスタム静的ルートを作成します。フロントエンド VM にフロントエンド ネットワーク タグを追加します。

B. 複数のインターフェイスを持つ NVA を作成します。バックエンド サブネットの NVA 用に NIC0 を構成します。フロントエンド サブネットの NVA 用に NIC1 を構成します。NVA を ilb1 という名前の内部パススルー ネットワーク ロード バランサーの背後に配置します。グローバル ネットワーク ファイアウォール ポリシー ルールを追加して、NVA を通過するトラフィックを許可します。バックエンド VM サブネットの宛先 IP 範囲、フロントエンド インスタンス タグ、および ilb1 のネクストホップを使用して、カスタムの静的ルートを作成します。フロントエンド VM にフロントエンド ネットワーク タグを追加します。

C. NVA を ilb1 という名前の内部パススルー ネットワーク ロード バランサーの背後に配置します。グローバル ネットワーク ファイアウォール ポリシー ルールを追加して、NVA を通過するトラフィックを許可します。バックエンド VM サブネットの送信元 IP 範囲、フロントエンド VM サブネットの宛先 IP 範

囲、および ilb1 のネクストホップを使用して、ポリシー ベース ルート (PBR) を作成します。バックエンド ネットワーク タグを使用して、PBR の範囲を VM に設定します。バックエンド サーバーにバックエンド ネットワーク タグを追加します。

D. NVA を ilb1 という名前の内部パススルー ネットワーク ロード バランサーの背後に配置します。グローバル ネットワーク ファイアウォール ポリシー ルールを追加して、NVA を通過するトラフィックを許可します。フロントエンド VM サブネットのソース IP 範囲、バックエンド VM サブネットの宛先 IP 範囲、および ilb1 のネクストホップを使用して、ポリシー ベース ルート (PBR) を作成します。フロントエンド ネットワーク タグを使用して、PBR のスコープを VM に設定します。フロントエンド サーバーにフロントエンド ネットワーク タグを追加します。

Answer(s): D
