

# Google Certified Professional - Cloud Architect (GCP) (Professional Cloud Architect Japanese Version)

1. 要件に準拠するには、EHR接続をアップグレードする必要があります。新しい接続設計は、ビジネスクリティカルなニーズをサポートし、同じネットワークおよびセキュリティポリシーの要件を満たす必要があります。あなたは何をするべきか？

- A. 新しいキャリアピアリング接続を追加します。
- B. 専用相互接続接続の帯域幅を100Gにアップグレードします。
- C. 新しい専用相互接続接続を追加します。
- D. 3つの新しいクラウドVPN接続を追加します。

Answer(s): A

---

2. あなたの会社は、Googleネットワークインテリジェンスセンターのファイアウォールインサイト機能を使用しています。ComputeEngineインスタンスに適用されるファイアウォールルールがいくつかあります。適用されたファイアウォールルールセットの効率を評価する必要があります。Google CloudConsoleでFirewallInsightsページを表示すると、表示するログ行がないことがわかります。問題のトラブルシューティングを行うにはどうすればよいですか？

- A. 仮想プライベートクラウド (VPC) フローログを有効にします。
- B. 監視するファイアウォールルールのファイアウォールルールログを有効にします。
- C. ユーザーアカウントにcompute.networkAdmin Identity and Access Management (IAM) ロールが割り当てられていることを確認します。
- D. Google Cloud SDKをインストールし、コマンドライン出力にファイアウォールログがないことを確認します。

**Answer(s): B**

---

3. あなたの会社は、敏感であり、顧客のニーズをすばやく満たすことに高い価値を置いています。主なビジネス目標は、リリーススピードと俊敏性です。あなたは誤って導入されたセキュリティエラーの可能性を減らそうとしています。どちらの行動をとることができますか？2つの回答を選択

A. すべてのコードチェックインがセキュリティSMEによってピアレビューされていることを確認します。

B. ソースコードセキュリティアナライザは、CI/CDパイプラインの一部として使用します。

C. コンポーネント間のすべてのインタフェースをユニットテストするためのスタブがあることを確認してください。

D. CI/CDパイプラインと統合されたコード署名と信頼できるバイナリリポジトリを有効にします。

E. 継続的統合/継続配信 (CI/CD) パイプラインの一部として脆弱性セキュリティスキャナを実行します。

**Answer(s): B,E**

---

4. あなたの会社には、科学的な計算を実行するステートレスWebAPIがあります。Web APIは、単一のGoogle Kubernetes Engine (GKE) クラスタで実行されます。クラスタは現在、us-central1にデプロイされています。あなたの会社は、Asiaの顧客にAPIを提供するように拡大しました。アジアのユーザーの待ち時間を短縮したいと考えています。あなたは何をするべきか？

A. クラウドCDNが有効になっているグローバルHTTP (s) ロードバランサーを使用する

B. asia-southeast1に2番目のGKEクラスタを作成し、LoadBalancerタイプのサービスを使用して両方のAPIを公開します。パブリックIPsをクラウドDNSゾーンに追加します

C. クラスタ内のアプリケーションに割り当てられているメモリとCPUを増やします

D. asia-southeast1に2番目のGKEクラスタを作成し、kubemciを使用してグローバルHTTP (s) ロードバランサーを作成します

**Answer(s): D**

---

5. 自動拡張インスタンスグループを設定して、次回の起動時にWebトラフィックを処理します。HTTP (S) ロードバランサへのバックエンドサービスとしてインスタンスグループを構成した後、毎分仮想マシン (VM) インスタンスが終了して再起動されます。インスタンスにパブリックIPアドレスがありません。curlコマンドを使用して、各インスタンスから適切なWeb応答が送信されていることを確認しました。バックエンドが正しく構成されていることを確認する必要があります。あなたは何をすべきか？

A. HTTP / HTTPSのソーストラフィックがロードバランサに到達できるようにするファイアウォールルールが存在することを確認します。

B. 各インスタンスにパブリックIPを割り当て、ロードバランサがインスタンスのパブリックIPに到達できるようにファイアウォールルールを構成します。

C. ロードバランサのヘルスチェックがインスタンスグループ内のインスタンスに到達できるようにするファイアウォールルールが存在することを確認します。

D. ロードバランサの名前で各インスタンスにタグを作成します。ロードバランサの名前をソースとして、インスタンスタグを宛先としてファイアウォールルールを構成します。

**Answer(s): C**

---

6. この質問については、Dress4Winのケーススタディを参照してください。

A. Dress4Winを利用可能な最小のインスタンスで本番環境にデプロイし、それらを経時的に監視し、目的のパフォーマンスに達するまでマシンタイプをスケールアップすることをお勧めします。

B. オンプレミスの物理ハードウェアコアとRAMを、クラウド内の最も近いマシンタイプにマッピングします。

C. アプリケーションサーバー仮想マシンに関連付けられている仮想コアとRAMの数を特定し、それらをクラウド内のカスタムマシンタイプに合わせ、パフォーマンスを監視し、目的のパフォーマンスに達するまでマシンタイプをスケールアップします。

D. Dress4Winは、使用可能なRAMとCPUの比率が最も高いマシンタイプにアプリケーションサーバーを展開することをお勧めします。

**Answer(s): A**

---

7. あなたは医療データを処理する機関で働いています

A. 正しいノードグループで各ワークロードをホストするために、ComputeEngineインスタンスを作成するときにネットワークタグとしてノードグループ名を追加します。

B. 正しいノードで各ワークロードをホストするために、ComputeEngineインスタンスを作成するときにネットワークタグとしてノード名を追加します。

C. Compute Engineインスタンスを作成するときに、ノードグループ名に基づいたノードアフィニティラベルを使用して、正しいノードグループで各ワークロードをホストします。

D. Compute Engineインスタンスを作成するときに、ノード名に基づいたノードアフィニティラベルを使用して、各ワークロードを正しいノードでホストします。

**Answer(s): D**

---

8. あなたの会社は、外部ユーザーがファイルをアップロードして共有できるようにするモノリシックな3層アプリケーションを開発しました。

A. 新しいアプローチは大幅にコストを削減し、基盤となるインフラストラクチャの管理を容易にし、CI / CDパイプラインを自動的に管理します。

B. モノリシックソリューションは、Dockerを使用してコンテナに変換できます。生成されたコンテナは、Kubernetesクラスタにデプロイできます。

C. 新しいアプローチにより、インフラストラクチャをアプリケーションから切り離し、新機能を開発およびリリースし、基盤となるインフラストラクチャを管理し、CI / CDパイプラインを管理し、A / Bテストを実行し、必要に応じてソリューションを拡張することが容易になります。

D. プロセスはMigrate for ComputeEngineで自動化できます。

**Answer(s): C**

---

9. あなたの会社は、バックエンドとしていくつかのパブリックAPIを使用して信頼性の高いWebアプリケーションを構築することを望んでいます。

A. HTMLや画像などの静的コンテンツをCloudCDNに保存します。App EngineでAPIをホストし、ユーザーデータをCloudSQLに保存します。

B. HTMLや画像などの静的コンテンツをCloudStorageバケットに保存します。複数のゾーンにワーカーノードがあるゾーンのGoogleKubernetes EngineクラスターでAPIをホストし、ユーザーデータを

CloudSpannerに保存します。

C. HTMLや画像などの静的コンテンツをCloudCDNに保存します。 Cloud Runを使用してAPIをホストし、ユーザーデータをCloudSQLに保存します。

D. HTMLや画像などの静的コンテンツをCloudStorageバケットに保存します。 Cloud Functionsを使用してAPIをホストし、ユーザーデータをFirestoreに保存します。

**Answer(s): D**

---

10. あなたの会社では、Windows Server 2022 をオンプレミスのデータセンターから Google Cloud に移行する予定です。 オンプレミスの仮想マシンで現在使用されているライセンスを、ターゲットのクラウド環境に移行する必要があります。 どうすればよいでしょうか。

A. 1. オンプレミスの仮想マシンのイメージを作成し、Cloud Storage にアップロードします。 2. イメージを Compute Engine 上の仮想ディスクとしてインポートします。

B. 1. Compute Engine に標準インスタンスを作成します。 2. オンプレミス環境で現在使用されている Microsoft Windows バージョンと同じバージョンを OS として選択します。

C. 1. オンプレミスの仮想マシンのイメージを作成します。 2. イメージを Compute Engine 上の仮想ディスクとしてインポートします。 3. オンプレミス環境で現在使用されているものと同じ Microsoft Windows バージョンを OS として選択して、Compute Engine に標準インスタンスを作成します。 4. 作成したイメージに一致するデータを含むデータ ディスクを接続します。

D. 1. オンプレミスの仮想マシンのイメージを作成します。 2. --os=windows-2022-dc-v を使用して、Compute Engine にイメージを仮想ディスクとしてインポートします。 3. インポートしたディスクをブートディスクとして使用する単一テナンシー インスタンスを Compute Engine 上に作成します。

**Answer(s): D**

---

11. お客様の組織では、Google Cloud Platformの同じネットワークに3層のWebアプリケーションが導入されています。

A. 各階層を異なるサブネットワークに追加します。

B. 個々のVMにソフトウェアベースのファイアウォールを設定します。

C. 各階層にタグを追加し、目的のトラフィックフローを許可するルートを設定します。

D. 各ティアにタグを追加し、ファイアウォールルールを設定して、目的のトラフィックフローを許可します。

**Answer(s): D**

---

12. あなたのチームは、Google Kubernetes Engine (GKE) にデプロイされるウェブアプリケーションを開発しています。CTOは起動が成功することを期待しており、アプリケーションが数万人のユーザーの予想される負荷を処理できることを確認する必要があります。現在のデプロイメントをテストして、アプリケーションの待機時間が特定のしきい値を下回っていることを確認する必要があります。あなたは何をすべきか？

A. 負荷テストツールを使用して、アプリケーションへの同時ユーザーの予想数とリクエストの総数をシミュレートし、結果を調べます。

B. すべてのGoogleCloudリージョンの複数のGKEクラスターにアプリケーションを複製します。グローバルHTTP(S)ロードバランサーを構成して、単一のグローバルIPアドレスでさまざまなクラスターを公開します。

C. GKEクラスターで自動スケーリングを有効にし、アプリケーションデプロイメントで水平ポッド自動スケーリングを有効にします。アプリケーションにcurlリクエストを送信し、自動スケーリングが機能するかどうかを検証します。

D. 開発環境でCloud Debuggerを使用して、さまざまなマイクロサービス間のレイテンシーを理解します。

**Answer(s): A**

---

13. この質問については、ヘリコプターレーシングリーグ(HRL)のケーススタディを参照してください。最近、HRLは南アフリカのケープタウンで新しい地域レーシングリーグを開始しました。ケープタウンの顧客に優れたユーザーエクスペリエンスを提供するために、HRLはコンテンツ配信ネットワークプロバイダーのFastlyと提携しました。HRLは、すべてのFastly IPアドレス範囲からVirtual Private Cloudネットワーク(VPCネットワーク)へのトラフィックを許可する必要があります。あなたはHRLセキュリティチームのメンバーであり、外部HTTP(S)

ロード バランサーを介して Fastly IP アドレス範囲のみを許可する更新を構成する必要があります。どのコマンドを使用する必要がありますか。

A. Fastly の名前付き IP リストを使用して、外部ロードバランサーに Cloud Armor セキュリティ ポリシーを適用します。

B. Fastly が公開した IP アドレスを使用して、外部ロードバランサーに Cloud Armor セキュリティ ポリシーを適用します。 C. Fastly IP アドレス範囲のポート 443 に VPC ファイアウォール ルールを適用します。

C. scurceiplisr-fasrly タグが付けられたネットワーク リソースのポート 443 に VPC ファイアウォール ルールを適用します。

**Answer(s): C**

---

14. 要求されているURLパスに基づいてグローバルロードバランシングのためのソリューションを設計する必要があります。

A. URLマップを使用してクロスリージョンロードバランサーを作成してください。

B. URLマップを使用してHTTPSロードバランサーを作成します。

C. 適切なインスタンスグループとインスタンスを作成します。 SSLプロキシロードバランシングを設定します。

D. グローバル転送ルールを作成します。 SSLプロキシバランシングを設定します。

**Answer(s): B**

---

15. サードパーティのアプリケーションを最適化されたオンプレミスの仮想マシンから GoogleCloudに移行します。最適なCPUとメモリのオプションがわかりません。アプリケーションには、複数の週にわたって一貫した使用パターンがあります。最小のコストでリソースの使用を最適化する必要があります。あなたは何をすべきか？

A. アプリケーションの現在のオンプレミス仮想マシンと同様のCPUおよびメモリオプションを使用してコンピューティングエンジンインスタンスを作成します。クラウド監視エージェントをインストールし、サードパーティのアプリケーションをデプロイします。サードパーティアプリケーションで通常のトラフィックレベルでロードを実行し、クラウドコンソールのRightizingRecommendationsに従ってください

B. App Engineの柔軟な環境を作成し、Dockerファイルとカスタムランタイムを使用してサードパーティアプリケーションをデプロイします。 app.yamlファイルで、アプリケーションの現在のオンプレミス仮想マシンと同様のCPUとメモリのオプションを設定します。

C. 使用可能な最小のマシントイプでインスタステンプレートを作成し、現在のオンプレミス仮想マシンから取得したサードパーティアプリケーションのイメージを使用します。平均CPUを使用してグループ内のインスタンス数を自動スケーリングするマネージドインスタンスグループを作成します。実行中のインスタンスの数を最適化するために、平均CPU使用率のしきい値を変更します。

D. CPUとメモリのオプションを変えて複数のComputeEngineインスタンスを作成します。クラウド監視エージェントをインストールし、それぞれにサードパーティのアプリケーションをデプロイします。アプリケーションでトラフィックレベルの高い負荷テストを実行し、その結果を使用して最適な設定を決定します。

**Answer(s): A**

---

16. Webアプリケーションは、欧州連合の一般データ保護規則（GDPR）の要件に準拠している必要があります。あなたはあなたのWebアプリケーションの技術的アーキテクチャに対して責任があります。あなたは何をすべきか？

A. Googleは既にさまざまな認定を受けており、ネイティブ機能を使用すると「パスオン」コンプライアンスを提供するため、WebアプリケーションでGoogle Cloud Platformのネイティブ機能とサービスのみを使用するようにしてください。

B. アプリケーション内で使用されている各サービスについて、GCPConsole内の関連するGDPR準拠設定を有効にします。

C. コンプライアンスのギャップを埋めるために、Cloud Security Scannerがテスト計画戦略の一部であることを確認してください。

D. GDPR要件を満たすWebアプリケーション内のデータのセキュリティのための設計を定義します。

**Answer(s): D**

---

17. Webアプリケーションを提供するためにKubernetes Engine上でクラスターを実行しています。アプリケーションの特定の部分が応答しなくなったことをユーザーが報告しています。展開のすべてのポッドが2秒後に再起動し続けることに気付くでしょう。アプリケーションはログを標準出力に書き込みます。問題の原因を見つけるためにログを検査したいと思います。あなたはどのアプローチを取ることができますか？

A. アプリケーションの応答しない部分を処理している特定のKubernetes EngineコンテナのStackdriverログを確認します。

B. クラスタ内のノードとして機能している各Compute EngineインスタンスのStackdriverログを確認してください。

C. gcloud認証情報を使用してクラスターに接続し、いずれかのポッドのコンテナに接続してログを読み取ります。

D. クラスタ内のノードとして機能している各Compute Engineインスタンスのシリアルポートログを確認します。

**Answer(s): A**

---

18. 会社のユーザーフィードバックポータルは、2つのゾーンに複製された標準のLAMPスタックで構成されています。これはus-central1リージョンにデプロイされ、データベースを除くすべてのレイヤーで自動スケーリングされたマネージドインスタンスグループを使用します。現在、ポータルにアクセスできるのは一部の顧客の少数のグループのみです。ポータルは

A. 既存のユーザー入力をキャプチャし、リソース使用率が80%を超えるまで、キャプチャしたユーザー負荷を再生します。また、アプリの既存のユーザーの使用状況に基づいて推定ユーザー数を導き出し、予想される負荷の200%を処理するのに十分なリソースをデプロイします。

B. 合成ランダムユーザー入力を作成し、自動スケールロジックが少なくとも1つのレイヤーでトリガーされるまで合成ロードを再生し、両方のゾーンでランダムリソースを終了することにより、システムに「カオス」を導入します。

C. 既存のユーザー入力をキャプチャし、キャプチャされたユーザー負荷をすべてのレイヤーで自動スケールがトリガーされるまで再生します。同時に、いずれかのゾーンのすべてのリソースを終了します。

D. 新しいシステムをより多くのユーザーグループに公開し、自動スケールロジックがすべてのレイヤーで変更されるまで、グループのサイズを毎日増やします。同時に、両方のゾーンでランダムなリソースを終了します。

**Answer(s): C**

---

19. あなたの会社には、データウェアハウジングに BigQuery を使用する Google Cloud プロジェクトがあります。個人を特定できる情報 (PII) を含むテーブルがいくつかあります。コンプライアンス チームのみが PH にアクセスできます。テーブル内のその他の情報は、データサイエ

ンス チームが利用できる必要があります。テーブルへの適切なアクセス権の割り当てにかかるコストと時間を最小限に抑えたい何をすべきか？

A. 1 ソース データがあるデータセットから、PII を除く、共有するテーブルのビューを作成します。2 適切なプロジェクト レベルの IAM ロールをデータサイエンス チームのメンバーに割り当てる3 ビューを含むデータセットにアクセス制御を割り当てる

B. 1 ソース データがあるデータセットから、PII を除いて共有したいテーブルのマテリアライズド ビューを作成します。2 適切なプロジェクト レベルの IAM ロールをデータサイエンス チームのメンバーに割り当てます。 3. ビューを含むデータセットにアクセス制御を割り当てます。

C. 1 データサイエンス チーム用のデータセットを作成する2 PII を除いて共有したいテーブルのビューを作成する3 適切なプロジェクト レベルの IAM ロールをデータサイエンス チームのメンバーに割り当てる4 ビューを含むデータセットにアクセス制御を割り当てる5 ソース データセットへのアクセスをビューに許可する

D. 1. データサイエンス チーム用のデータセットを作成します。2. PII を除く、共有したいテーブルのマテリアライズド ビューを作成します。3. 適切なプロジェクト レベルの IAM ロールをデータサイエンス チームのメンバーに割り当てる4 ビューを含むデータセットにアクセス制御を割り当てる5 ソース データセットへのアクセスをビューに許可する

Answer(s): C

20. あなたは、メンバーの年齢が8歳から30歳までのスポーツ協会で働いています。協会は、持続的な怪我など、大量の健康データを収集しています。このデータをBigQueryに保存しています。現在の法律では、件名の要求に応じてそのような情報を削除する必要があります。このような要求に対応できるソリューションを設計する必要があります。あなたは何をするべきか？

A. 個人ごとに一意の識別子を使用します。削除リクエストがあった場合は、この識別子を使用してBigQueryからすべての行を削除します。

B. BigQueryで新しいデータを取り込むときは、データ損失防止 (DLP) APIを介してデータを実行し、個人情報を特定します。DLPスキャンの一部として、結果をデータカタログに保存します。削除リクエストがあった場合は、データカタログにクエリを実行して、個人情報を含む列を見つけます。

C. すべてのデータを含むテーブル上にBigQueryビューを作成します。削除リクエストがあった場合、サブジェクトのデータに影響を与える行をこのビューから除外します。すべての分析タスクで、ソーステーブルの代わりにこのビューを使用します。

D. 個人ごとに一意の識別子を使用します。削除要求時に、その値のソルトされたSHA256を使用して一意の識別子で列を上書きします。

**Answer(s):** A

---