Google Cloud Certified Professional Cloud DevOps Engineer Exam (Japanese Version)

1. Git ブランチが更新されたときに Terraform コードをデプロイする Cloud Build ジョブをデプロイしています。テスト中に、ジョブが失敗したことに気づきました。ビルド ログに次のエラーが表示されます。

A. ローカル状態を使用するように Terraform コードを変更します。

B. Terraform 構成で指定された名前でストレージ バケットを作成します。

C. ロール/所有者 Identity and Access Management (IAM) ロールをプロジェクトの Cloud Build サービス アカウントに付与します。

D. ロール/ストレージを付与します。objectAdmin Identity and Access Management (IAM) ロールを状態ファイル バケットの Cloud Build サービス アカウントに付与します。

Answer(s): D

---

2. Google Cloud Platform (GCP) 上で実行される高トラフィックの Web アプリケーションをサポートしているとします。アプリケーションにエンジニアリング上の変更を加えることなく、ユーザーの観点からアプリケーションの信頼性を測定する必要があります。あなたは何をするべきか？

A. 現在のアプリケーション メトリックを確認し、必要に応じて新しいメトリックを追加します。

B. ユーザー操作のための追加情報を取得するようにコードを変更します。

C. Web プロキシ ログのみを分析し、各リクエストの応答時間をキャプチャします。

D. 新しい合成クライアントを作成して、アプリケーションを使用したユーザー ジャーニーをシミュレートします。

E. 現在および過去のリクエスト ログを使用して、アプリケーションと顧客のやり取りを追跡します。

Answer(s): D,E

---

3. 組織の仮想マシン (VM|) のコストを削減する必要があります。さまざまなオプションを検討した結果、プリエンプティブル VM インスタンスを活用することにしました。どのアプリケーションがプリエンプティブル VM に適していますか?

A. スケーラブルなインメモリ キャッシュ システム

B. 組織の一般公開 Web サイト

C. 十分なクォーラムを持つ分散型の結果整合性のある NoSQL データベース クラスター

D. ビデオを取得してストレージ バケットに保存する、GPU 高速化ビデオ レンダリング プラットフォーム

Answer(s): D

---

4. サポートしている実稼働システムで多数の停止が発生しました。夜中に目が覚めるようなすべての停電に関するアラートを受け取ります。アラートは異常なシステムが原因で発生し、1 分以内に自動的に再起動されます。サイト信頼性エンジニアリングの実践に従って、スタッフの燃え尽き症候群を防ぐプロセスを設定したいと考えています。あなたは何をするべきか？

A. 対処できないアラートを削除します。

B. アラートごとにインシデント レポートを作成します。

C. 異なるタイムゾーンのエンジニアにアラートを配信します。

D. エラー バジェットが使い果たされないように、関連するサービス レベル目標を再定義します。

Answer(s): A

---

5. 組織では、複数の Google Cloud プロジェクトのすべてのアプリケーション ログが中央の Cloud Logging プロジェクトに保存されています。セキュリティ チームは、各プロジェクト チームがそれぞれのログのみを表示し、運用チームのみがすべてのログを表示できるというルール

を適用したいと考えています。コストを最小限に抑えながら、セキュリティ チームの要件を満たす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. プロジェクト チームごとにログを BigQuery テーブルにエクスポートします。プロジェクト チームにテーブルへのアクセスを許可します。中央ログ プロジェクトの運用チームにログ書き込みアクセス権を付与します。

B. プロジェクト チームごとにログ ビューを作成し、各プロジェクト チームのアプリケーション ログのみを表示します。運用チームに中央ログ プロジェクトの _ Al Il-jogs ビューへのアクセスを許可します。

C. 各プロジェクト チームに、中央ログ プロジェクトのプロジェクト _ デフォルト ビューへのアクセスを許可します。中央ログプロジェクトの運用チームにログ閲覧者アクセス権を付与します。

D. プロジェクト チームごとに Identity and Access Management（IAM）ロールを作成し、個々の Google Cloud プロジェクトの _ デフォルト ログ ビューへのアクセスを制限します。中央ログプロジェクトの運用チームに閲覧者アクセスを許可します。

Answer(s): B

---

6. 機密情報にアクセスする必要があるアプリケーションをデプロイしています。この情報が暗号化されていることを確認し、侵害が発生した場合でも漏洩のリスクを最小限に抑える必要があります。あなたは何をするべきか？

A. 暗号化キーをクラウド キー管理サービス (KMS) に保存し、キーを頻繁にローテーションします。

B. 暗号化された構成管理システムを介して、インスタンス作成時にシークレットを注入します。

C. アプリケーションをシングル サインオン (SSO) システムと統合し、アプリケーションにシークレットを公開しない

D. アプリケーションのインスタンスごとに複数のバージョンのシークレットを生成する継続的なビルドパイプラインを活用します。

Answer(s): A

---

7. 単一の Compute Engine インスタンス上で実行される本番サービスをサポートしているとします。クラッシュしたインスタンスを削除し、関連するイメージに基づいて新しいインスタンスを作成することで、サービスを再作成するのに定期的に時間を費やす必要があります。サイト信頼

性エンジニアリングの原則に従いながら、手動操作の実行にかかる時間を削減したいと考えています。あなたは何をするべきか？

A. 単一インスタンスでマネージド インスタンス グループを作成し、ヘルス チェックを使用してシステム ステータスを判断します。

B. Compute Engine インスタンスの前にロードバランサを追加し、ヘルスチェックを使用してシステムのステータスを判断します。

C. SMS アラートを備えた Stackdriver Monitoring ダッシュボードを作成して、クラッシュしたインスタンスの再作成をクラッシュ後にすぐに開始できるようにします。

D. 開発チームにバグを報告し、クラッシュしたインスタンスの根本原因を見つけられるようにします。

Answer(s): A

---

8. 主力サービスの半年ごとの容量計画を実行している 今後 6 か月間、サービス ユーザーの増加率が前月比 10% になると予想している サービスは完全にコンテナ化されており、Google Kubemetes Engine (GKE) 標準で実行されていますクラスターの自動スケーリングが有効になっている 3 つのゾーンにわたるクラスター 現在、展開されている合計 CPU 容量の約 30% を消費しており、ゾーンの障害に対する回復力が必要です。不必要なコストを回避しながら、この増加またはゾーン障害の結果としてユーザーが経験する悪影響を最小限に抑えたいと考えています。予測される増加に対処するためにどのような準備をすればよいでしょうか?

A. 最大ノード プール サイズを確認し、水平ポッド オートスケーラーを有効にしてから、予想されるリソースのニーズを確認しないようにロードを実行します。

B. GKE にサービスをデプロイし、クラスタ オートスケーラーを使用しているため、GKE クラスタは成長率に関係なく自動的にスケーリングされます。

C. デプロイされた CPU 容量の 30% のみを使用しているため、かなりの余裕があり、この増加率に対して追加の容量を追加する必要はありません。

D. 6 か月間の 10% の増加率に対応するためにノード容量を 80% 追加し、負荷テストを実行して十分な容量があることを確認します。

Answer(s): A

---

9. あなたの会社は HTTPS リクエストを使用して、Cloud Run がホストするパブリック サービスをトリガーしています。

A. gcioud rundeploybooking-engine-no-traffic --ag dev コマンドを実行します。https://dev----booking-engine-abcdef。 a ．走る。テスト用のアプリの URL

B. Runthegcioud run services update-traffic Booking-engine -to-revisions LATEST*! コマンド ht tps: //booking-engine-abcdef を使用します。 a ．走る。テスト用のape URL

C. curl -K "Authorization: Hearer S(gclcud auth print-identity-token)" 認証トークンを渡します https: / を使用します/予約エンジン-abcdef. a ．走る。非公開でテストするアプリの URL

D. 役割を付与/実行します。予約エンジン サービスをテストする開発者に対する呼び出し者の役割 https://予約エンジン-abcdef. プライベート。走る。テスト用のアプリの URL

Answer(s): B

---

10. ロード バランサーを使用せずに HTTP エンドポイントを公開するアプリケーションを管理しています。HTTP 応答の遅延は、ユーザー エクスペリエンスにとって重要です。すべてのユーザーが経験している HTTP 遅延を把握したいと考えています。Stackdriver Monitoring を使用します。あなたは何をするべきか？

A. * アプリケーションで、metricKind を DELTA に設定し、valueType を DOUBLE に設定してメトリックを作成します。* Stackdriver の Metrics Explorer では、緩み棒グラフを使用して指標を視覚化します。

B. * アプリケーションで、metricKind を CUMULATIVE に設定し、valueType を DOUBLE に設定してメトリックを作成します。* Stackdriver の Metrics Explorer では、折れ線グラフを使用して指標を視覚化します。

C. * アプリケーションで、metricKind をゲージに設定し、valueType を distribution に設定してメトリックを作成します。* Stackdriver の Metrics Explorer では、ヒートマップ グラフを使用して指標を視覚化します。

D. * アプリケーションで、metricKind を使用してメトリックを作成します。METRlc_KIND_UNSPECIFIED に設定し、valueType を INT64 に設定します。* Stackdriver の Metrics Explorer では、積み上げ面グラフを使用して指標を視覚化します。

Answer(s): C

---

11. あなたは最近、サービスの 1 つが現在のローリング ウィンドウ期間のエラー バジェットを超えていることに気づきました。あなたの会社の製品チームは、新しい機能をリリースしようとしています。サイト信頼性エンジニアリング (SRE) プラクティスに従いたいと考えています。

A. エラー バジェットが使い果たされたことをチームに通知します。リリースの凍結についてチームと交渉するか、ユーザー エクスペリエンスの多少の悪化を許容します。

B. 製品に関連する他のメトリクスを調べて、残りのエラー バジェットを持つ SLO を見つけます。エラー バジェットを再割り当てし、機能の起動を許可します。

C. 状況をエスカレーションし、追加のエラー バジェットを要求します。

D. エラー バジェットの不足についてチームに通知し、すべてのテストが成功することを確認して、立ち上げによってエラー バジェットがさらに危険にさらされないようにする。

Answer(s): A

---

12. 年末商戦期には事後分析を組織に導入する必要があります。Web アプリケーションが短期間に大量のトラフィックを受信すると予想されます。イベント中の潜在的な障害に備えてアプリケーションを準備する必要があります。どうすればよいでしょうか?

A. 増加した容量要件を確認し、必要なクォータ管理を計画します。

B. アプリケーション上で Anthos Service Mesh を構成し、トポロジ マップの問題を特定します。

C. アプリケーションで発生するすべての一般的な障害について、Cloud Monitoring でアラートを作成します。

D. 平均パーセンタイル遅延についてサービスの遅延を監視します。

E. 関連するシステム指標が Cloud Monitoring でキャプチャされていることを確認し、関心のあるレベルでアラートを作成します。

Answer(s): A,E

---

13. 今後の分析のために Cloud Logging から BigQuery にログエントリをエクスポートする Cloud Logging シンクを作成しています。組織には、開発プロジェクトを含む Dev という名前の Google Cloud フォルダと、本番環境プロジェクトを含む Prod という名前のフォルダがあります。開発プロジェクトのログエントリは dev_dataset にエクスポートする必要があります。運用

プロジェクトのログ エントリは prod_dataset にエクスポートする必要があります。 作成されるログ シンクの数を最小限に抑える必要があり、ログ シンクが将来のプロジェクトに確実に適用されるようにしたい場合はどうすればよいですか?

A. 組織レベルで単一の集約ログ シンクを作成します。

B. プロジェクトごとにログシンクを作成します

C. 組織レベルで 2 つの集約ログ シンクを作成し、プロジェクト ID でフィルターします。

D. Dev フォルダーと Prod フォルダーに集約 log シンクを作成します。

Answer(s): D

---

14. あなたの会社は、Google Kubernetes Engine (GKE) を使用してサービスを実行しています。開発環境の GKE クラスタは、詳細ログを有効にしてアプリケーションを実行します。開発者は、kubect1 logs コマンドを使用してログを表示し、Cloud Logging は使用しません。アプリケーションには、統一されたロギング構造が定義されていません。GKE 運用ログを収集しながら、アプリケーション ロギングに関連するコストを最小限に抑える必要があります。

A. 開発クラスタに対して gcloudcontainerclusterupdate--logging-SYSTEM コマンドを実行します。

B. 開発クラスタに対して gcloudcontainerclusterupdatelogging=WORKLOAD コマンドを実行します。

C. 開発環境に関連付けられたプロジェクトで gcloudloggingsinksupdate_Defau1t --disabled コマンドを実行します。

D. 重大度 >= DEBUG リソースを追加します。開発環境に関連付けられたプロジェクトのデフォルトのログ シンクに「k83 コンテナ」除外フィルターを入力します。

Answer(s): A

---

15. あなたの会社は、Pub/Sub、App Engine スタンダード環境、GO で書かれたアプリケーションを使用して、IoT データを大規模に処理しています。ピーク負荷時にパフォーマンスが一貫して低下していることに気づきました。ワークステーションではこの問題を再現できませんでした。コード内の遅いパスを特定するには、運用環境のアプリケーションを継続的に監視する必要があります。パフォーマンスへの影響と管理オーバーヘッドを最小限に抑えたいと考えています。あなたは何をするべきか？

A. 継続的プロファイリング ツールを Compute Engine にインストールします。プロファイリング データをツールに送信するようにアプリケーションを構成します。

B. アプリケーション インスタンスに対して go tool pprof コマンドを定期的に実行します。フレーム グラフを使用して結果を分析します。

C. Cloud Profiler を構成し、アプリケーション内の/go/profiler ライブラリを初期化します。

D. Cloud Monitoring を使用して、App Engine の CPU 使用率指標を評価します。

Answer(s): C

---

16. あなたのチームは Google Kubernetes Engine (GKE) でマイクロサービスを実行しています。顧客を保護し、リリース ポリシーを定義するためにエラー バジェットの消費を検出したいと考えています。どうすればよいですか?

A. メトリックから SLI を作成する サービスが通過しない場合のアラート ポリシーを有効にする

B. Anthos Service Mesh の指標を使用してマイクロサービスの健全性を測定します。

C. SLO の作成 select_slo_bum_rate のアラート ポリシーの作成

D. SLO を作成し、サービスの稼働時間チェックを構成します。サービスが合格しない場合のアラート ポリシーを有効にします。

Answer(s): C

---

17. あなたは、ユーザーに深刻な影響を与えたインシデントの事後分析を書いています。今後同様の事故が起こらないようにしたいと考えています。次の 2 つのセクションのうち、事後分析に含める必要があるのはどれですか? (2つお選びください。)

A. インシデントの根本原因の説明

B. インシデントを引き起こした責任のある従業員のリスト

C. 再発防止に向けた取り組み項目のリスト

D. 過去のインシデントと比較したインシデントの深刻さに関するあなたの意見

E. インシデントの影響を受けたすべてのサービスの設計ドキュメントのコピー

Answer(s): A,C

---

18. あなたは、一連の Google Kubernetes Engine (GKE) クラスターへの本番環境のデプロイを管理しています。信頼できる CI/CD パイプラインによって正常に構築されたイメージのみが実稼働環境にデプロイされるようにしたいと考えています。あなたは何をするべきか？

A. クラスターで Cloud Security Scanner を有効にします。

B. コンテナー レジストリで脆弱性分析を有効にします。

C. Kubernetes Engine クラスターをプライベート クラスターとしてセットアップします。

D. Binary Authorization を使用して Kubernetes Engine クラスターをセットアップします。

Answer(s): D

---

19. Google Kubernetes Engine (GKE) クラスター上で実行される携帯電話ゲームのバックエンドをサポートしているとします。アプリケーションはユーザーからの HTTP リクエストを処理します。ネットワーク コストを削減するソリューションを実装する必要があります。あなたは何をするべきか？

A. VPC を共有 VPC ホスト プロジェクトとして構成します。

B. ネットワーク サービスをスタンダード ティアで構成します。

C. Kubernetes ダスターをプライベート クラスターとして構成します。

D. Google Cloud HTTP ロードバランサを Ingress として構成します。

Answer(s): B

---

20. あなたはグローバル組織で働いており、限られたエンジニアリング リソースで 99% の可用性目標を設定してサービスを実行しています。現在の暦月では、サービスの可用性が 99 5% で

あることがわかりました。サービスが定義された可用性目標を満たし、今後の新機能のリリースを含むビジネスの変化に対応できることを確認する必要があります。また、運用コストを最小限に抑えながら技術的負債を削減する必要があります。Google が推奨するプラクティスに従いたいです。どうすればよいですか?

A. サービス レベルの可用性に対するエラー バジェットを定義し、残りのエラー バジェットを最小限に抑えます。

B. 反復的なタスクを自動化することで、労力を特定、測定、排除します

C. 可用性が目標内に収まるようにしながら、利用可能なエンジニアを機能バックログに割り当てます。

D. 追加のコンピューティング リソースをサービスに追加することで、サービスに N+1 冗長性を追加します。

Answer(s): A
