Google Cloud Certified - Professional Cloud Security Engineer Exam (Japanese Version)

1. Compute Engine インスタンスで実行されているアプリケーションは、Cloud Storage バケットからデータを読み取る必要があります。あなたのチームは、Cloud Storage バケットをグローバルに読み取り可能にすることを許可しておらず、最小権限の原則を確保したいと考えています。

A. Compute Engine インスタンスの IP アドレスからの読み取り専用アクセスを許可し、アプリケーションが資格情報なしでバケットから読み取ることを許可する Cloud Storage ACL を作成します。

B. Cloud Storage バケットへの読み取り専用アクセス権を持つサービス アカウントを使用し、Compute Engine インスタンスのアプリケーションの構成にあるサービス アカウントへの認証情報を保存します。

C. Cloud Storage バケットへの読み取り専用アクセス権を持つサービス アカウントを使用して、インスタンス メタデータから認証情報を取得します。

D. Cloud KMS を使用して Cloud Storage バケット内のデータを暗号化し、アプリケーションが KMS 鍵を使用してデータを復号できるようにします。

Answer(s): C

---

2. 大規模な電子小売業者は、e コマース ウェブサイトを Google Cloud Platform に移行しています。同社は、顧客がオンラインでチェックアウトするときに、顧客のブラウザと GCP の間で支払い情報が確実に暗号化されるようにしたいと考えています。

A. L7 ロード バランサーで SSL 証明書を構成し、暗号化を要求します。

B. ネットワーク TCP ロード バランサーで SSL 証明書を構成し、暗号化を要求します。

C. ポート 443 で受信トラフィックを許可し、他のすべての受信トラフィックをブロックするようにファイアウォールを構成します。

D. ポート 443 でアウトバウンド トラフィックを許可し、他のすべてのアウトバウンド トラフィックをブロックするようにファイアウォールを構成します。

Answer(s): A

---

3. HTTPS リソースにアクセスするために、Identity and Access Management (IAM) ユーザーにどの Identity-Aware Proxy ロールを付与する必要がありますか?

A. セキュリティ レビュー担当者

B. IAP で保護されたトンネル ユーザー

C. IAP で保護された Web アプリ ユーザー

D. サービス ブローカー オペレーター

Answer(s): C

---

4. あなたは、侵害されたサービス アカウント キーを調査しているセキュリティ チームの一員です。サービス アカウントによって作成された新しいリソースを監査する必要があります。

A. データ アクセス ログを照会します。

B. 管理アクティビティ ログを照会します。

C. アクセスの透明性ログを照会します。

D. Stackdriver Monitoring ワークスペースをクエリします。

Answer(s): B

---

5. お客様は、VM でバッチ処理システムを実行し、出力ファイルを Cloud Storage バケットに保存したいと考えています。ネットワーキングおよびセキュリティ チームは、VM がパブリック インターネットに到達しないことを決定しました。

A. VM からのインターネット トラフィックをブロックするファイアウォール ルールを作成します。

B. Cloud Storage API エンドポイントにアクセスするための NAT ゲートウェイをプロビジョニングします。

C. VPC でプライベート Google アクセスを有効にします。

D. Cloud Storage バケットをすべての VM にローカル ファイル システムとしてマウントします。

Answer(s): C

---

6. あなたの会社のクラウド セキュリティ ポリシーでは、VM インスタンスに外部 IP アドレスを持たないように定めています。外部 IP アドレスのない VM インスタンスがインターネットに接続して VM を更新できるようにする GCP サービスを特定する必要があります。どのサービスを使用する必要がありますか?

A. Identity Aware-Proxy

B. クラウド NAT

C. TCP/UDP 負荷分散

D. クラウド DNS

Answer(s): B

---

7. 組織は、インスタンスのログ データをヨーロッパ内に保管するための規制に準拠する必要があります。ワークロードは、新しいプロジェクトのオランダのリージョン europe-west4 でホストされます。データを国内に保管するには Cloud Logging を構成する必要があります。

A. europe-west4 に新しい tog バケットを作成します。そして、_Def ault buckKet を新しいバケットにリダイレクトします。

B. gcloud CLI ログ設定更新を使用して、ログ ストレージ リージョンを eurcpe-west4 に設定します。

C. すべてのログを europe-west4 の Cloud Storage バケットにエクスポートするようにログシンクを構成します。

D. 組織ポリシーの制約 gcp.resourceLocations を europe-west4 に構成します。

Answer(s): A

---

8. VPC ネットワークで定義されている暗黙のファイアウォール ルールを 2 つ選択してください。（2つ選んでください。）

A. すべてのアウトバウンド接続を許可するルール

B. すべてのインバウンド接続を拒否するルール

C. すべての受信ポート 25 接続をブロックするルール

D. すべてのアウトバウンド接続をブロックするルール

E. すべての受信ポート 80 接続を許可するルール

Answer(s): A,B

---

9. あなたは組織のセキュリティ チームのメンバーです。あなたのチームには、クレジット カード決済処理システムとウェブ アプリケーションおよびデータ処理システムを含む単一の GCP プロジェクトがあります。PCI 監査基準の対象となるシステムの範囲を縮小したいと考えています。

A. Web アプリケーションへの管理者アクセスに多要素認証を使用します。

B. PA-DSS に準拠することが認定されたアプリケーションのみを使用してください。

C. カード会員データ環境を別の GCP プロジェクトに移動します。

D. オフィスとクラウド環境間のすべての接続に VPN を使用します。

Answer(s): C

---

10. 組織の記録データは Cloud Storage に存在します。すべての記録データは少なくとも 7 年間保持する必要があります。このポリシーは永続的である必要があります。

A. * 1 レコードデータが含まれるバケットを識別します※2 保存ポリシーを適用し、7年間保存するように設定します。* 3 ログベースのアラートを使用してバケットを監視し、保持ポリシーの変更が発生しないようにします。

B. * 1 レコードデータを持つバケットを識別します※2 保存ポリシーを適用し、7年間保存するように設定します。※3 バケットロックを有効にする

C. * 1 レコードデータを持つバケットを識別します※2 保存ポリシーを適用し、7年間保存するように設定します。* 3 ストレージ バケットの更新権限を含む Identity and Access Management (IAM) ロールを削除します。

D. * 1 レコードデータを持つバケットを識別します*2 データが確実に保持されるようにするためにのみバケット ポリシーを有効にします。※3 バケットロックを有効にする

Answer(s): B

---

11. 小規模な新興企業のオフィス マネージャーは、支払いと請求書の照合と請求アラートの作成を担当しています。コンプライアンス上の理由から、オフィス マネージャーは、これらのタスクに必要な Identity and Access Management (IAM) 権限のみを持つことが許可されています。オフィス マネージャーが持つべき 2 つの IAM ロールはどれですか?（2つ選んでください。）

A. 組織管理者

B. プロジェクト作成者

C. 請求先アカウント閲覧者

D. 請求先アカウント コスト マネージャー

E. 請求先アカウント ユーザー

Answer(s): C,D

---

12. あなたは、Google Cloud 内のアプリケーション データ（転送中のデータ、使用中のデータ、保存中のデータを含む）のエンドツーエンドの暗号化を必要とするクライアントと相談しています。これを達成するには、どのオプションを利用する必要がありますか?（2つ選んでください。）

A. 外部キー マネージャー

B. 顧客提供の暗号化キー

C. ハードウェア セキュリティ モジュール

D. Confidential Computing と Istio

E. クライアント側の暗号化

Answer(s): D,E

---

13. Google Cloud に保存されている特定の BigQuery データを暗号化するには、Cloud External Key Manager を使用して暗号鍵を作成する必要があります。最初にどの手順を実行する必要がありますか?

A. 1. Google Cloud プロジェクトで一意の Uniform Resource Identifier (URI) を持つ既存のキーを作成または使用します。2. Google Cloud プロジェクトに、サポートされている外部鍵管理パートナー システムへのアクセス権を付与します。

B. 1. Cloud Key Management Service (Cloud KMS) で一意の Uniform Resource Identifier (URI) を持つ既存の鍵を作成または使用します。2. Cloud KMS で、キーを使用するためのアクセス権を Google Cloud プロジェクトに付与します。

C. 1. サポートされている外部キー管理パートナー システムで、一意の Uniform Resource Identifier (URI) を持つ既存のキーを作成または使用します。2. 外部鍵管理パートナー システムで、この鍵に Google Cloud プロジェクトを使用するためのアクセス権を付与します。

D. 1. Cloud Key Management Service (Cloud KMS) で一意の Uniform Resource Identifier (URI) を使用して外部キーを作成します。2. Cloud KMS で、キーを使用するためのアクセス権を Google Cloud プロジェクトに付与します。

Answer(s): C

---

14. 個人を特定できる情報 (PII) を含む機密性の高い BigQuery ワークロードがあり、インターネットからアクセスできないようにしたいと考えています。データの漏洩を防ぐため、承認された IP アドレスからのリクエストのみが BigQuery テーブルへのクエリを許可されます。

A. サービス境界を使用し、許可された送信元 IP アドレスを条件としてアクセス レベルを作成します。

B. グローバル HTTPS ロードバランサで承認された IP アドレスの許可リストを定義する Google Cloud Armor セキュリティ ポリシーを使用します。

C. Cloud Data Loss Prevention (DLP) とともに、許可される Google Cloud API とサービスを制限する組織ポリシー制約を使用します。

D. リソース サービスの使用を制限する組織ポリシー制約をクラウド データ損失防止 (DLP) とともに使用します。

Answer(s): A

---

15. 次のリソース階層があります。示されているように、階層内の各ノードに組織ポリシーがあります。VPC A で拒否されるロードバランサーのタイプはどれですか?

A. フォルダーとプロジェクトのポリシーに従って、EXTERNAL_TCP_PROXY、EXTERNAL_SSL_PROXY、INTERNAL_TCP_UDP、および INTERNAL_HTTP_HTTPS が拒否されます。

B. プロジェクトのポリシーに従って、EXTERNAL_TCP_PROXY、EXTERNAL_SSL_PROXY は拒否されます。

C. フォルダーのポリシーに従って、INTERNAL_TCP_UDP、INTERNAL_HTTP_HTTPS を拒否します。

D. グローバル ノードのポリシーに従って、すべてのロード バランサ タイプが拒否されます。

Answer(s): A

---

16. Google Cloud 上には多数のプライベート仮想マシンがあります。場合によっては、リモートの場所から Secure Socket Shell (SSH) を介してサーバーを管理する必要があります。セキュリティとコスト効率を最適化する方法でサーバーへのリモート アクセスを構成したいと考えています。

A. パブリック IP アドレスを使用してサーバー インスタンスを構成する 企業 IP からのトラフィックのみを許可するファイアウォール ルールを作成します。

B. パブリック IP を使用してジャンプ ホスト インスタンスを作成します。ジャンプ ホスト経由で接続してインスタンスを管理します。

C. Identity-Aware Proxy (IAP) IP 範囲からのアクセスを許可するファイアウォール ルールを作成します。 IAP で保護されたトンネル ユーザーの役割を管理者に付与します。

D. 企業ネットワークから Google Cloud へのサイト間 VPN を作成します。

Answer(s): C

---

17. あなたは会社のインシデント対応計画を策定しています。DevOps チームが Google Cloud 環境でのデプロイの問題を確認および調査するときに使用するアクセス戦略を定義する必要があります。主な要件は次の 2 つです。

A. サービス アカウントを作成し、プロジェクト オーナーの 1AM ロールを付与します。このサービス アカウントのサービス アカウント ユーザー ロールを DevOps チームに付与します。

B. サービス アカウントを作成し、制限付きのリスト/表示権限を付与します。このサービス アカウントのサービス アカウント ユーザー ロールを DevOps チームに付与します。

C. リスト/ビュー権限が制限されたカスタム 1AM ロールを作成し、DevOps チームに割り当てます。

D. Project Viewer Identity and Access Management (1AM) ロールを DevOps チームに割り当てます。

Answer(s): B

---

18. VPC Service Controls を有効にして、リソースへのアクセスを妨げずに、既存の環境の境界を変更できるようにする必要があります。どの VPC Service Controls モードを使用する必要がありますか?

A. クラウドラン

B. 強制

C. ネイティブ

D. ドライラン

Answer(s): D

---

19. 顧客は、クラウド コンピューティングの伸縮自在な性質を利用するアプリケーションを Compute Engine にデプロイしました。

A. パッチが利用可能になったら新しい基本イメージを構築し、CI/CD パイプラインを使用して VM を再構築し、段階的に展開します。

B. ドメイン コントローラを Compute Engine にフェデレートし、グループ ポリシー オブジェクトを介して毎週パッチをロールアウトします。

C. Deployment Manager を使用して、更新された VM を新しいインスタンス グループ (IG) にプロビジョニングします。

D. 毎週のメンテナンス期間中にすべての VM を再起動し、スタートアップ スクリプトがインターネットから最新のパッチをダウンロードできるようにします。

Answer(s): A

---

20. あなたは、データを Google Cloud に移行することを計画しているクライアントと協力しています。暗号化されたキーを管理するための暗号化サービスを推奨するのは、お客様の責任です。次の要件があります。

A. Cloud Key Management Service を使用した顧客管理の暗号鍵

B. Cloud HSM を使用した顧客管理の暗号鍵

C. 顧客提供の暗号化キー

D. Google が管理する暗号鍵

Answer(s): B
