Google.Professional-Cloud-Security-Engineer.v2026-03-06.q286

試験コード:	Professional-Cloud-Security-Engineer
試験名称:	Google Cloud Certified - Professional Cloud Security Engineer Exam
認定資格:	Google
無料問題数:	286
バージョン:	v2026-03-06
アクセス数:	125
ページビュー数:	2860
https://www.jpnpdf.com/Google.Professional-Cloud-Security-Engineer.v2026-03-06.q286-mondaishu.html	

最新問題: **1**
Google Cloud 上で実行される貴社のアプリケーションの運用は、貴社が責任を負います。アプリケーションのデータベースは、外部パートナーによって保守されます。パートナーチームにデータベースへのアクセスを許可する必要があります。このアクセスはデータベースのみに制限する必要があり、貴社のネットワーク内の他のリソースには拡張できません。貴社のソリューションは、Google が推奨するプラクティスに準拠する必要があります。どうすればよいですか？
A. アプリケーションのデータベースにパブリックIPアドレスを追加します。パートナーの従業員ごとにデータベースユーザーを作成します。これらのユーザーの資格情報をパートナーチームに安全に配布します。
B. パートナーチームに、自社の環境と ID プロバイダ内で Cloud Identity アカウントを設定するよう依頼します。パートナーの Cloud Identity アカウントにデータベースへのアクセス権を付与します。
C. 企業IDプロバイダにパートナーチームのアカウントを作成します。これらのアカウントをGoogle Cloud Identityと同期し、アカウントにデータベースへのアクセス権を付与します。
D. パートナーのWorkforce Identity Federationを構成します。IDプールプロバイダーをパートナーのIDプロバイダーに接続します。Workforceプールリソースにデータベースへのアクセスを許可します。
Answer: (解答を表示する**)**
Workforce Identity Federation は、外部パートナーに独自の ID プロバイダ（IdP）を使用して Google Cloud リソースへのアクセスを許可するための、Google が推奨する最新の方法です。これにより、独自のディレクトリにゲストアカウントを作成する際の「ID ライフサイクル管理」の負担を回避できます。
Google Cloud ドキュメント (Workforce Identity Federation の概要) によると、次のようになります。
Workforce Identity Federation を使用すると、外部 ID プロバイダ（IdP）を使用して、従業員、パートナー、請負業者などのユーザーグループである Workforce を認証および承認し、ユーザーが Google Cloud サービスにアクセスできるようになります。Workforce Identity Federation を使用すると、既存の IdP から Google Cloud ID にユーザー ID を同期する必要がありません。このアプローチのメリットは次のとおりです。
* 同期なし: Cloud Identity/Workspace でパートナー アカウントを作成または管理しません (オプション C は不要になります)。

* セキュリティ: パートナーの従業員が退職した場合、その従業員のホーム IdP アカウントが無効になると、Google Cloud データベースへのアクセスが自動的に取り消されます。
* スコープ指定アクセス: IAM ロール (roles/cloudsql.client など) を Workforce Pool またはそのプール内の特定のグループに明示的に付与し、他のリソースにアクセスできないようにします。
他のオプションが間違っている理由:
* A は不正解です。パブリック IP は大きなセキュリティ リスクであり、集中型の ID ガバナンスを提供しません。
* B は不正解です。フェデレーションなしでは、本番環境のデータベースに対して、安全かつ管理しやすい方法で別の組織の Cloud Identity のアカウントに直接「アクセス権を付与」することはできません。
参照：
Google Cloud ドキュメント: 「Workforce Identity Federation」(https://cloud.google.com/iam/docs/workforce-identity-federation)。
Google Cloud セキュリティ エンジニア 学習ガイド: 「高度な ID 管理 - フェデレーション」のセクション。

最新問題: **2**
貴社は、IT インフラストラクチャの大部分を Google Cloud に移行する予定です。既存のオンプレミス Active Directory を Google Cloud の ID プロバイダとして活用したいと考えています。貴社のオンプレミス Active Directory を Google Cloud と統合し、アクセス管理を構成するには、どの 2 つの手順を実行する必要がありますか（2 つ選択してください）。
A. Identity Platform を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
B. Cloud Identity SAML 統合を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
C. Google Cloud Directory Sync をインストールし、Active Directory と Cloud Identity に接続します。
D. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) ロールを作成します。
E. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) グループを作成します。
Answer: (解答を表示する**)**
説明
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing-user-accounts?

最新問題: **3**
貴社は、IT インフラストラクチャの大部分を Google Cloud に移行する予定です。既存のオンプレミス Active Directory を Google Cloud の ID プロバイダとして活用したいと考えています。貴社のオンプレミス Active Directory を Google Cloud と統合し、アクセス管理を構成するには、どの 2 つの手順を実行する必要がありますか（2 つ選択してください）。

A. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) ロールを作成します。
B. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) グループを作成します。
C. Cloud Identity SAML 統合を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
D. Google Cloud Directory Sync をインストールし、Active Directory と Cloud Identity に接続します。
E. Identity Platform を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
Answer: C,D (メーッセージを残す)

最新問題**: 4**
組織では、規制の厳しい業界に属するミッションクリティカルなワークロードを管理しています。このワークロードでは、エンドポイントのコンピュータから Cloud Storage にアップロードされた機密データを Compute Engine VM を使用して分析 処理しています。コンプライアンス チームは、このワークロードが機密データのデータ保護要件を満たしていないことを検出しました。以下の要件を満たす必要があります。
* Google Cloud 境界外でデータ暗号化キー (DEK) を管理します。
* サードパーティプロバイダーを通じて暗号化キーを完全に制御します。
* 機密データをクラウドストレージにアップロードする前に暗号化する
* Compute Engine VMでの処理中に機密データを復号化する
* Compute Engine VM で使用中にメモリ内の機密データを暗号化するにはどうすればよいでしょうか?
2つの回答を選択してください
A. 既存の Compute Engine VM と Cloud Storage バケット全体に VPC Service Controls のサービス境界を作成します。
B. 機密データにアクセスするために、Compute Engine VM を Confidential VMs に移行します。
C. Cloud 外部鍵マネージャーを設定して、機密データを Cloud Storage にアップロードする前に暗号化し、VM にダウンロードした後に復号化します。
D. 機密データにアクセスするための Confidential VM を作成します。
E. 顧客管理の暗号鍵を構成して、機密データを Cloud Storage にアップロードする前に暗号化し、VM にダウンロードした後に機密データを復号します。
Answer: C,D (メーッセージを残す)
https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance#considerations
Confidential VM はライブマイグレーションをサポートしていません。VM で Confidential Computing を有効にできるのは、インスタンスを初めて作成する場合のみです。https://cloud.google.com/confidential-computing/confidential-vm/docs
/cvmインスタンスの作成

最新問題**: 5**
You are auditing all your Google Cloud resources in the production project. You want to identity all principals who can change firewall rules.
What should you do?

A. Use Policy Analyzer lo query the permissions compute, firewalls, create ofcompute, firewalls. Create of compute,firewalls.delete.
B. Reference the Security Health Analytics - Firewall Vulnerability Findings in the Security Command Center.
C. Use Policy Analyzer to query the permissions compute, firewalls, get of compute, firewalls, list.
D. Use Firewall Insights to understand your firewall rules usage patterns.
Answer: (解答を表示する**)**
To identify all principals who can change firewall rules, you need to determine which users or service accounts have permissions that allow them to modify firewall rules in your Google Cloud project. The correct permissions to check for this are compute.firewalls.create and compute.firewalls.delete. These permissions enable a user to create and delete firewall rules, respectively.
The Policy Analyzer tool in Google Cloud allows you to query and analyze IAM policies to identify which principals have specific permissions. By using Policy Analyzer, you can effectively identify all principals with the compute.firewalls.create and compute.firewalls.delete permissions.
Open Policy Analyzer: Go to the Google Cloud Console, navigate to IAM & Admin, and select Policy Analyzer.
Set Up Query: Create a new query specifying the permissions compute.firewalls.create and compute.firewalls.delete.
Run Query: Execute the query to retrieve a list of principals who have these permissions.
Review Results: Analyze the results to identify all users and service accounts with the capability to modify firewall rules.
この方法により、ファイアウォール ルールを変更できるすべてのプリンシパルの包括的なリストが得られるため、監査とセキュリティ体制が強化されます。
Google Cloud Policy Analyzer のドキュメント
Google Cloud IAM ドキュメント

最新問題**: 6**
あるマネージャーは、コストを最小限に抑えながら、セキュリティイベントログを2年間保存したいと考えています。適切なログエントリを選択するためのフィルターを作成します。
ログはどこにエクスポートすればよいですか?
A. BigQueryデータセット
B. Cloud Storage バケット
C. StackDriver のログ
D. Cloud Pub/Sub トピック
Answer: (解答を表示する**)**
コストを最小限に抑える場合は、常にクラウド ストレージが考慮されます。

最新問題**: 7**
既存の VPC Service Controls 境界を新しいアクセスレベルに更新したいと考えています。この変更によって既存の境界が損なわれるのを防ぎ、ユーザーへの影響を最小限に抑えながらオーバーヘッドを最小限に抑える必要があります。どうすればよいでしょうか？

A. 既存の境界の完全なレプリカを作成します。レプリカに新しいアクセスレベルを追加します。アクセスレベルの検証が完了したら、元の境界を更新します。
B. 境界を、常に一致することのない新しいアクセスレベルに更新します。過度に許可されすぎないように、新しいアクセスレベルを、望ましい状態に一致するように一度に1つの条件ごとに更新します。
C. 境界でドライランモードを有効にします。新しいアクセスレベルを境界設定に追加します。
アクセス レベルが検証されたら、境界構成を更新します。
D. 境界でドライランモードを有効にします。新しいアクセスレベルを境界のドライラン設定に追加します。アクセスレベルの検証が完了したら、境界設定を更新します。
Answer: D (メーッセージを残す**)**
* ドライ ラン モードを有効にする: まず、VPC Service Controls 境界に対してドライ ラン モードを有効にします。
このモードでは、実際に変更を適用せずにテストできるため、現在の設定が中断されるのを防ぐことができます。
* アクセスレベルの追加：新しいアクセスレベルをドライラン設定に追加します。これにより、新しいアクセスレベルがどのように動作し、既存の設定とどのように連携するかを、実際の影響を与えることなく監視できます。
* 審査プロセス :ログを分析し、ドライランモードでの動作を監視することで、新しいアクセスレベルを慎重に審査します。新しい構成がセキュリティと運用の要件を満たしていることを確認します。
* 境界の更新：新しいアクセスレベルが既存のサービスに支障をきたさず、すべての要件を満たしていることが確認できたら、実際の境界構成を新しいアクセスレベルに更新します。このアプローチにより、変更内容が反映される前にテストできるため、リスクを最小限に抑え、中断を最小限に抑えながらシームレスな更新を実現できます。参考資料：
* Google Cloud - VPC サービス コントロールの構成
* Google Cloud - ドライランモードの使用

最新問題**: 8**
アプリケーションログを Cloud Storage にエクスポートしています。ログシンクが均一なバケットレベルのアクセスポリシーをサポートしていないというエラーメッセージが表示されます。このエラーをどのように解決すればよいですか？
A. バケットのアクセス制御モデルを変更する
B. 正しいバケットの宛先でシンクを更新します。
C. ログシンク ID のバケットに、roles/logging.logWriter Identity and Access Management (IAM) ロールを追加します。
D. ログシンク ID のバケットに、roles/logging.bucketWriter Identity and Access Management (IAM) ロールを追加します。
Answer: (解答を表示する**)**
https://cloud.google.com/logging/docs/export/troubleshoot
宛先に正しい権限を付与できません:

シンクが正しいサービス アカウント権限で正常に作成された場合でも、バケットの作成時に Cloud Storage バケットのアクセス制御モデルが均一アクセスに設定されていた場合は、このエラー メッセージが表示されます。
既存の Cloud Storage バケットの場合、バケット作成後 90 日間は [権限] タブを使用してアクセス制御モデルを変更できます。新しいバケットの場合は、バケット作成時にきめ細かなアクセス制御モデルを選択してください。詳細については、Cloud Storage バケットの作成をご覧ください。

最新問題**: 9**
Compute Engine でホストされている公開アプリケーションで障害が発生しているとユーザーから報告されています。ファイアウォール ルールの最近の変更が原因ではないかと考えています。ファイアウォール ルールが正しく動作しているかどうかをテストする必要があります。どうすればよいでしょうか？
A. 変更された最新のファイアウォールルールのログ記録を有効にします。ログエクスプローラを使用して、ルールが正しく動作しているかどうかを分析します。
B. VPC 内の要塞ホストに接続します。ネットワークトラフィックアナライザーを使用して、リクエストがブロックされているポイントを特定します。
C. 実稼働前の環境では、すべてのファイアウォール ルールを個別に無効にして、どのルールがユーザー トラフィックをブロックしているかを判断します。
D. VPC で VPC フローログを有効にします。ログエクスプローラーを使用して、ルールが正しく機能しているかどうかを分析します。
Answer: A (メーッセージを残す**)**
* 変更された最新のルールに対してファイアウォールルールのログ記録を有効にします。ログエクスプローラを使用して、ルールが正しく動作しているかどうかを分析します。
* Google Cloud Console を通じて、問題の特定のファイアウォール ルールのファイアウォール ルール ロギングを有効にします。
* ログ記録を有効にしたら、ログ エクスプローラーを使用してファイアウォール ログをフィルタリングして確認します。
* ログを分析して、ルールが意図したとおりにトラフィックを許可またはブロックしているかどうかを確認し、誤った構成や問題を特定します。
参考文献:
* ファイアウォールルールのログ
* ログエクスプローラーの使用

最新問題**: 10**
保存データの暗号化に使用する鍵が、組織のセキュリティ管理基準に準拠していることを確認する必要があります。あるセキュリティ管理基準では、鍵を90日ごとにローテーションすることが義務付けられています。鍵が適切にローテーションされているかどうかを検証するための効果的な検出戦略を実装する必要があります。では、どうすればよいでしょうか？
A. Cloud Logging を使用して、タイムリーなキー更新を確認する指標を定義します。キーがローテーションされていない場合、

90 日以内に、インシデント通知チャネルを通じてアラート メッセージを送信します。
B. Cloud Asset Inventory のデータを使用して、暗号鍵のバージョンを分析します。アクティブな鍵が90日以上経過している場合は、インシデント通知チャネルを通じてアラートメッセージを送信します。
C. セキュリティヘルスアナリティクスを使用して、ローテーションされていないキーを特定します。キーがローテーションされていない場合は、
90 日後、セキュリティ コマンド センターで検出結果が生成されます。
D. Cloud Run にコードを実装して、Cloud Key Management Service 内の鍵を評価します。鍵が 90 日経過してもローテーションされない場合は、Security Command Center で検出結果を報告します。
Answer: B (メッセージを残す**)**

最新問題**: 11**
Google Cloud 組織で、ユーザーがバケット内のオブジェクトを外部に公開できないようにするセキュリティ ポリシーを適用する必要があります。現在、組織内にバケットがありません。運用オーバーヘッドを最小限に抑えながらこの目標を達成するには、どのソリューションを積極的に実装すればよいでしょうか。
A. パブリック バケットを見つけて非公開にする Cloud Functions を実行する、1 時間ごとの cron ジョブを作成します。
B. 組織レベルで、constraints/storage.publicAccessPrevention 制約を有効にします。
C. 組織レベルで、constraints/storage.uniformBucketLevelAccess 制約を有効にします。
D. バケットを含むプロジェクト内の storage.googleapis.com サービスを保護する VPC Service Controls 境界を作成します。バケットを含む新しいプロジェクトをこの境界に追加します。
Answer: B (メッセージを残す**)**
説明
https://cloud.google.com/storage/docs/public-access-prevention
公開アクセス防止は、Cloud Storage バケットとオブジェクトが誤って公開されるのを防ぎます。バケットが組織内に含まれている場合は、プロジェクト、フォルダ、または組織レベルで組織ポリシー制約 storage.publicAccessPrevention を使用して、公開アクセス防止を適用できます。

最新問題**: 12**
組織の Cloud Storage バケットのデータがインターネット上で公開されないようにしたいと考えています。これをすべての Cloud Storage バケットに適用したいと考えています。どうすればよいでしょうか？
A. エンドユーザーから所有者のロールを削除し、Cloud Data Loss Prevention を構成します。
B. エンドユーザーから所有者の役割を削除し、組織のポリシーでドメイン制限の共有を適用します。
C. 均一なバケットレベルのアクセスを構成し、組織ポリシーでドメイン制限の共有を適用します。
D. すべてのロールから *.setIamPolicy 権限を削除し、組織ポリシーでドメイン制限の共有を適用します。
Answer: C (メッセージを残す**)**
- 均一なバケットレベルのアクセス: https://cloud.google.com/storage/docs/uniform-bucket-level-access#should-you-use
- ドメイン制限共有: https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#public_data_sharing

最新問題: **13**
オンプレミスのデータウェアハウスをBigQuery Cloud SQLとCloud Storageに移行しています。データウェアハウスでセキュリティサービスを構成する必要があります。会社のコンプライアンスポリシーでは、データウェアハウスに対して以下の要件が定められています。
* 暗号化キーの完全なライフサイクル管理により保存データを保護
* データ管理とは別のキー管理プロバイダを実装する
* すべての暗号化キー要求を可視化する
データ ウェアハウスの実装にはどのようなサービスを含める必要がありますか?
2つの回答を選択してください
A. 顧客管理の暗号化キー
B. 顧客提供の暗号化キー
C. キーアクセスの正当化
D. アクセスの透明性と承認
E. クラウド外部キーマネージャー
Answer: A,E (メーッセージを残す**)**
* 顧客管理暗号化キー (CMEK):
* CMEK を使用すると、Cloud Key Management Service (KMS) を使用して暗号化キーを管理できます。これにより、キーのローテーション、破棄、監査などのライフサイクルを制御できます。
* Cloud KMS キーリングを設定し、BigQuery、Cloud SQL、Cloud Storage のデータ保護に使用される暗号鍵を作成します。
* 保存データの暗号化に CMEK を使用するようにサービスを構成して、組織のセキュリティ ポリシーへの準拠を確保します。
* クラウド外部キーマネージャー (EKM):
* Cloud EKM を使用すると、外部の鍵管理プロバイダによって管理される鍵を使用して、Google Cloud サービス内のデータを暗号化できます。
* サポートされているプロトコルと API を使用して、外部のキー管理システムを Google Cloud と統合します。
* 暗号化に外部キーを使用するようにデータ ウェアハウス サービスを構成し、キー管理が Google Cloud 環境の外部で処理されるようにします。
* 主なアクセスの理由:
* キーアクセスの正当性を有効にすると、暗号化キーへのアクセス理由を可視化できます。これにより、キーの使用状況を監視および監査し、コンプライアンスとセキュリティを確保できます。
* キーアクセス要求をキャプチャして確認するためのポリシーとログを設定し、キーがどのように、なぜ使用されるかについての洞察を提供します。
* アクセスの透明性と承認:
* アクセスの透明性を実装して、Google によるデータと暗号化キーへのアクセスを可視化します。
* アクセス承認を設定して、Google サポートまたはエンジニアリングによるデータへのアクセスに明示的な承認を要求することで、セキュリティと制御をさらに強化できます。
参考文献:
* 顧客管理暗号化キー (CMEK)
* クラウド外部キーマネージャー (EKM)

* 主要なアクセスの正当化
* アクセスの透明性
* アクセス承認

最新問題: **14**
オンプレミスのデータ ウェアハウスを BigQuery、Cloud SQL、Cloud Storage に移行しています。
データウェアハウスでセキュリティサービスを構成する必要があります。会社のコンプライアンスポリシーでは、データウェアハウスに以下の要件が定められています。
- 暗号化されたライフサイクル管理で保存データを保護
キー。
- データ管理とは別のキー管理プロバイダーを実装します。
- すべての暗号化キー要求を可視化します。
データ ウェアハウスの実装にはどのようなサービスを含める必要がありますか? (2 つ選択してください。)
A. 顧客管理の暗号化キー
B. 顧客提供の暗号化キー
C. キーアクセスの正当化
D. アクセスの透明性と承認
E. クラウド外部キーマネージャー
Answer: C,E (メーッセージを残す**)**
https://cloud.google.com/assured-workloads/key-access-justifications/docs/overview
https://cloud.google.com/kms/docs/ekm

最新問題: **15**
お客様は、Google Cloud Platform（GCP）上で3層構造の社内ウェブアプリケーションを立ち上げる必要があります。お客様の社内コンプライアンス要件では、トラフィックが特定の既知の有効なCIDRから発信されていると思われる場合にのみ、エンドユーザーによるアクセスを許可する必要があります。お客様は、アプリケーションがSYNフラッドDDoS防御のみを備えるというリスクを承知しています。GCPネイティブのSYNフラッド防御機能の利用を希望しています。
これらの要件を満たすにはどの製品を使用すればよいでしょうか?
A. クラウド CDN
B. クラウド ID およびアクセス管理
C. VPC ファイアウォールルール
D. クラウドアーマー
Answer: (解答を表示する**)**

最新問題: **16**
セキュリティチームは、ユーザー管理キーが適切に管理されず、侵害されるリスクを軽減したいと考えています。そのためには、開発者が組織内のプロジェクトでユーザー管理サービスアカウントキーを作成できないようにする必要があります。どのように対策を講じるべきでしょうか？
A. サービス アカウント キーを管理するために Secret Manager を構成します。

B. 組織ポリシーを有効にして、サービス アカウントの作成を無効にします。
C. 組織ポリシーを有効にして、サービス アカウント キーが作成されないようにします。
D. ユーザーから iam.serviceAccounts.getAccessToken 権限を削除します。
Answer: C (メーッセージを残す**)**
https://cloud.google.com/iam/docs/サービスアカウントキーの管理に関するベストプラクティス
サービス アカウント キーの不要な使用を防ぐには、組織のポリシー制約を使用します。組織のリソース階層のルートで、 ₩サービス アカウント キーの作成を無効にする」および ₩サービス アカウント キーのアップロードを無効にする」制約を適用し、サービス アカウント キーの使用を禁止するデフォルトを設定します。必要に応じて、選択したプロジェクトの制約のいずれかをオーバーライドして、サービス アカウント キーの作成またはアップロードを再度有効にします。

最新問題**: 17**
ある多国籍企業の事業部門がGCPにサインアップし、ワークロードのGCPへの移行を開始しました。この事業部門は、数百のプロジェクトを含む組織リソースを使用してCloud Identityドメインを作成しました。
チームはこれを認識し、権限の管理とドメイン リソースの監査を引き継ぎたいと考えています。
この要件を満たすために、チームはどのタイプのアクセスを許可する必要がありますか?
A. 組織ロール管理者
B. セキュリティレビュー担当者
C. 組織管理者
D. 組織ポリシー管理者
Answer: A (メーッセージを残す**)**

最新問題**: 18**
アプリケーションをクラウドに移行しています。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。地域の規制要件により、暗号化に使用する鍵マテリアルを完全に管理する必要があり、鍵マテリアルにアクセスするための正当な理由が必要です。
何をすべきでしょうか?
A. 顧客管理の暗号鍵を使用して、Cloud Storageバケット内のデータを暗号化します。許可されていないグループに対して午前1時の拒否ポリシーを設定します。
B. Cloud ハードウェア セキュリティ モジュール (HSM) を基盤とする顧客管理の暗号鍵を使用して、Cloud Storage バケット内のデータを暗号化します。データアクセス ログを有効にします。

C. オンプレミス環境でキーを生成し、オンプレミスで管理されているハードウェア セキュリティ モジュール (HSM) に保存します。このキーを Cloud Key Management Service (KMS) の外部キーとして使用します。Key Access Justifications (KAJ) を有効化し、外部キーシステムを設定して不正アクセスを拒否します。
D. オンプレミス環境で鍵を生成し、データを Cloud Storage バケットにアップロードする前に暗号化します。鍵を Cloud Key Management Service (KMS) にアップロードします。Key Access Justifications (KAJ) を有効にして、外部鍵システムで不正アクセスを拒否します。
Answer: (解答を表示する**)**
オンプレミス環境で鍵を生成し、管理するHSMに保存することで、鍵マテリアルを完全に管理下に置くことができます。Cloud KMSで鍵を外部鍵として使用すると、Google Cloudに鍵を保存しなくても、Google Cloud サービスで鍵を使用できます。
Key Access Justifications (KAJ) を有効にすると、キーにアクセスするたびに理由が提供され、不正なアクセスの試みを拒否するように外部キー システムを設定できます。

最新問題**: 19**
顧客は、インターネット アクセスを制限する必要がある Compute Engine 上で分析ワークロードを実行しています。
チームは、インターネットへのすべてのトラフィックを拒否する (優先度 1000) 出力ファイアウォール ルールを作成しました。
Compute Engine インスタンスは、セキュリティアップデートを取得するために公開リポジトリにアクセスする必要があります。チームとして何をすべきでしょうか？
A. 優先度が 1000 を超えるリポジトリのホスト名へのトラフィックを許可する出力ファイアウォール ルールを作成します。
B. 優先度が 1000 未満のリポジトリのホスト名へのトラフィックを許可する出力ファイアウォール ルールを作成します。
C. 優先度が 1000 を超えるリポジトリの CIDR 範囲へのトラフィックを許可する出力ファイアウォール ルールを作成します。
D. 優先度が 1000 未満のリポジトリの CIDR 範囲へのトラフィックを許可する出力ファイアウォール ルールを作成します。
Answer: B (メーッセージを残す**)**

最新問題**: 20**
組織では機密性の高い医療情報を扱っています。仮想マシン（VM）での使用中はデータが暗号化されていることを確認する必要があります。そのためには、組織全体に適用するポリシーを作成する必要があります。
何をすべきでしょうか?
A. 組織全体で作成されたすべての VM リソースで顧客管理の暗号化キー (CMEK) 保護が使用されるようにする組織ポリシーを実装します。
B. 組織全体で作成されたすべての VM リソースが Confidential VM インスタンスであることを保証する組織ポリシーを実装します。
C. 組織全体で作成されたすべての VM リソースが Cloud 外部キー マネージャー (EKM) 保護を使用するようにする組織ポリシーを実装します。

D. Google はデフォルトで使用中のデータを暗号化するため、アクションは必要ありません。
Answer: B (メッセージを残す**)**
仮想マシン（VM）での使用中にデータが暗号化され、組織全体にこのポリシーを適用するには、Confidential VMsインスタンスを使用する必要があります。手順は以下のとおりです。
* Confidential VM を有効にする:
* 選択したリージョンで Confidential VMs が使用可能であり、プロジェクトで有効になっていることを確認します。
* 組織ポリシーを設定する:
* 組織ポリシーを実装して、組織全体のすべての VM に Confidential VM インスタンスの使用を適用します。
* このポリシーを設定するには、Google Cloud Console または gcloud コマンドライン ツールを使用します。
コマンド例:
gcloud リソースマネージャー org-policies set-policy my_policy.yaml
* my_policy.yamlの例:
名前: organizations/1234567890/policies/compute.requireConfidentialCompute 仕様: ルール: - 強制: true
* 検証と監視:
* 組織全体で新しく作成されたすべての VM が Confidential VM であることを確認します。
* Google Cloud Console を通じてコンプライアンスを定期的に監視し、コンプライアンスに準拠していない VM が作成された場合にアラートを設定します。
利点：
* 使用中のデータ暗号化: Confidential VM は、データが保存中や転送中だけでなく、使用中も暗号化されることを保証します。
* ポリシーの適用: 組織ポリシーは、組織内のすべてのプロジェクトにわたってセキュリティ構成を適用する方法を提供します。
参考文献
* 機密コンピューティングドキュメント
* 組織ポリシーの作成と管理

最新問題**: 21**
貴社は、IT インフラストラクチャの大部分を Google Cloud に移行する予定です。既存のオンプレミス Active Directory を Google Cloud の ID プロバイダとして活用したいと考えています。貴社のオンプレミス Active Directory を Google Cloud と統合し、アクセス管理を構成するには、どの 2 つの手順を実行する必要がありますか（2 つ選択してください）。
A. Identity Platform を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
B. Cloud Identity SAML 統合を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
C. Google Cloud Directory Sync をインストールし、Active Directory と Cloud Identity に接続します。
D. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) ロールを作成します。
E. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (1AM) グループを作成します。
Answer: C,E (メッセージを残す**)**

* Google Cloud Directory Sync（GCDS）オンプレミスの Active Directory と Google Cloud Identity を同期するには、GCDS をインストールして設定します。このツールは、ローカルディレクトリと Google Cloud 間の整合性を維持するのに役立ちます。
* IAM グループ :Google Cloud で、Active Directory グループに対応する権限を持つ IAM グループを作成します。このマッピングにより、ユーザーは Active Directory グループのメンバーシップに基づいて適切な権限を継承できるようになります。
* 同期: オンプレミスの AD と Google Cloud の間でユーザーとグループの情報を最新の状態に保つために、定期的な同期スケジュールを設定します。
* アクセス管理 :これらのIAMグループを使用してGoogle Cloudリソースへのアクセスを管理し、権限が一貫して安全に適用されるようにします。このアプローチでは、既存のADインフラストラクチャをID管理に活用し、Google Cloudとのシームレスな統合を実現します。参考資料 :
* Google Cloud - Google Cloud ディレクトリ同期
* Google Cloud - IAM グループ

最新問題**: 22**
共有VPCに接続されたCompute EngineインスタンスとBigQueryデータセット間のアクセス拒否エラーをトラブルシューティングしています。データセットは、VPC Service Controls境界で保護されたプロジェクト内にあります。どうすればよいでしょうか？
A. 共有 VPC を含むホスト プロジェクトをサービス境界に追加します。
B. Compute Engine インスタンスが存在するサービス プロジェクトをサービス境界に追加します。
C. Compute Engine インスタンスが存在するサービス プロジェクトと、共有 VPC を含むホスト プロジェクトの間にサービス境界を作成します。
D. Compute Engine インスタンスが存在するサービス プロジェクトと、保護された BigQuery データセットを含む境界の間に境界ブリッジを作成します。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/vpc-service-controls/docs/service-perimeters#secure-google-managed-resources 共有 VPC を使用している場合は、共有 VPC に属するすべてのプロジェクトとともに、ホスト プロジェクトをサービス境界に含める必要があります。

最新問題**: 23**
gcloud コマンドラインツールを使用して、サードパーティのシングルサインオン（SSO）SAML ID プロバイダで認証を行いたいと考えています。サードパーティの ID プロバイダ（IdP）で認証がサポートされていることを確認するために必要なオプションはどれですか（2 つ選択してください）。
A. OpenIDコネクト
B. サードパーティのIdPとしてのSSO SAML
C. アイデンティティ認識プロキシ
D. クラウドアイデンティティ
E. アイデンティティプラットフォーム
Answer: (解答を表示する**)**

最新問題: **24**
セキュリティチームは、Cloud Storage バケットに保存されている機密データを保護するために、多層防御アプローチを実装したいと考えています。チームには以下の要件があります。
プロジェクト A の Cloud Storage バケットは、プロジェクト B からのみ読み取り可能です。
プロジェクト A の Cloud Storage バケットには、ネットワーク外部からアクセスできません。
Cloud Storage バケット内のデータは外部の Cloud Storage バケットにコピーできません。
セキュリティチームは何をすべきでしょうか?
A. 組織ポリシーでドメイン制限の共有を有効にし、Cloud Storage バケットに対する均一なバケットレベルのアクセスを有効にします。
B. VPC Service Controls を有効にし、プロジェクト A と B の周囲に境界を作成し、サービス境界構成に Cloud Storage API を含めます。
C. ネットワーク間の通信を許可する厳格なファイアウォール ルールを使用して、プロジェクト A と B の両方のネットワークでプライベート アクセスを有効にします。
D. ネットワーク間の通信を許可する厳格なファイアウォール ルールを使用して、プロジェクト A と B のネットワーク間の VPC ピアリングを有効にします。
Answer: B (メーッセージを残す**)**
VPC ピアリングは組織間のピアリングであり、組織内のプロジェクト間のピアリングではありません。つまり、共有 VPC です。この場合、両方のプロジェクトは同じ組織内にあるため、必要なルールを適用した VPC Service Controls を両方のプロジェクトに適用すれば問題ありません。
https://cloud.google.com/vpc-service-controls/docs/概要

最新問題: **25**
顧客は、証明機関 (CA) を備えたオンプレミスの公開キー インフラストラクチャ (PKI) を保有しています。
多くの HTTP ロードバランサ フロントエンドに対して証明書を発行する必要があります。
オンプレミスの PKI は多くの手動プロセスによる影響を最小限に抑える必要があり、ソリューションを拡張する必要があります。
何をすべきでしょうか?
A. オンプレミス PKI システムの Google 証明機関サービス内の下位 CA を使用して、ロードバランサの証明書を発行します。
B. オンプレミスのOpenSSLベースの下位CAから発行されたPKCS12証明書を持つウェブアプリケーションを使用します。インポートにはgcloudツールを使用します。外部HTTPロードバランサの代わりに、外部TCP/UDPネットワークロードバランサを使用します。
C. 証明書マネージャーを使用して、Google が管理する公開証明書を発行し、インフラストラクチャ アズ コード (IaC) 内の HTTP ロードバランサで証明書を構成します。
D. 証明書マネージャーを使用して、オンプレミスの PKI およびフロントエンドから発行された証明書をインポートします。
インポートには gcloud ツールを活用します。
Answer: A (メーッセージを残す**)**

最新問題: **26**
セキュリティチームは、Cloud Storage バケットに保存されている機密データを保護するために、多層防御アプローチを実装したいと考えています。チームには以下の要件があります。
* プロジェクト A の Cloud Storage バケットは、プロジェクト B からのみ読み取り可能です。
* プロジェクト A の Cloud Storage バケットには、ネットワーク外部からアクセスできません。
* Cloud Storage バケット内のデータは外部の Cloud Storage バケットにコピーできません。
セキュリティチームは何をすべきでしょうか?
A. 組織ポリシーでドメイン制限の共有を有効にし、Cloud Storage バケットに対する均一なバケットレベルのアクセスを有効にします。
B. VPC Service Controls を有効にし、プロジェクト A と B の周囲に境界を作成し、サービス境界構成に Cloud Storage API を含めます。
C. ネットワーク間の通信を許可する厳格なファイアウォール ルールを使用して、プロジェクト A と B の両方のネットワークでプライベート アクセスを有効にします。
D. ネットワーク間の通信を許可する厳格なファイアウォール ルールを使用して、プロジェクト A と B のネットワーク間の VPC ピアリングを有効にします。
Answer: B (メーッセージを残す**)**
説明
VPC ピアリングは組織間のピアリングであり、組織内のプロジェクト間のピアリングではありません。つまり、共有 VPC です。この場合、両方のプロジェクトは同じ組織内にあるため、必要なルールを適用した VPC Service Controls を両方のプロジェクトに適用すれば問題ありません。
https://cloud.google.com/vpc-service-controls/docs/概要

最新問題: **27**
アプリケーションは、グローバル外部HTTP(S)ロードバランサの背後に、高可用性のクロスリージョンソリューションとしてデプロイされています。複数のIPアドレスからのトラフィックが急増していることに気づきましたが、それらのIPアドレスが悪意のあるものであるかどうかは不明です。アプリケーションの可用性が懸念されます。
指定された時間間隔にわたってこれらのクライアントからのトラフィックを制限します。
何をすべきでしょうか?
A. Google Cloud Armor を使用してスロットル アクションを構成し、指定された時間間隔におけるクライアントあたりのリクエスト数を制限します。
B. Google Cloud Armor を使用して rate_based_ban アクションを設定し、ban_duration_sec パラメータを指定された時間間隔に設定します。
C. 識別された IP アドレスからのトラフィックを制限するために、VPC でファイアウォール ルールを設定します。
D. Google Cloud Armor を使用して拒否アクションを構成し、指定された時間間隔内に過剰なリクエストを発行したクライアントを拒否します。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/armor/docs/レート制限の概要#スロットルトラフィック

最新問題: **28**
オンプレミス ネットワークからアクセスされる新しいウェブ アプリケーションを Google Cloud 上に実装しようとしています。マルウェアなどの脅威からアプリケーションを保護するには、受信トラフィックにトランスポート層セキュリティ（TLS）インターセプションを実装する必要があります。どうすればよいでしょうか？
A. セキュア Web プロキシを構成します。ロードバランサーで TLS トラフィックをオフロードし、トラフィックを検査して、Web アプリケーションに転送します。
B. 内部プロキシロードバランサーを構成します。ロードバランサーでTLSトラフィックをオフロードし、トラフィックを検査して、Webアプリケーションに転送します。
C. 階層型ファイアウォールポリシーを設定します。Cloud Next Generation Firewall (NGFW) Enterprise を使用して TLS インターセプションを有効にします。
D. VPC ファイアウォールルールを設定します。Cloud Next Generation Firewall (NGFW) Enterprise を使用して TLS インターセプションを有効にします。
Answer: A (メーッセージを残す**)**
着信トラフィックの TLS インターセプションを実装してマルウェアなどの脅威から Web アプリケーションを保護するには、ロード バランサーで TLS オフロードを使用してセキュア Web プロキシを構成するのが効果的な方法です。
オプション A: セキュア Web プロキシを構成すると、ロード バランサーで TLS トラフィックをオフロードし、復号化されたトラフィックでマルウェアなどの脅威を検査し、検査済みのトラフィックを Web アプリケーションに転送できます。
このアプローチにより、転送中のデータのセキュリティを損なうことなく、暗号化されたトラフィックを安全に分析できるようになります。
オプション B: 内部プロキシ ロード バランサは、プライベート ネットワーク内でトラフィックを分散するように設計されており、外部ソースからの受信トラフィックを検査するために必要な TLS インターセプト機能をサポートしていない可能性があります。
オプション C: Google Cloud の階層型ファイアウォール ポリシーは、組織全体にセキュリティ ルールを適用するために使用されますが、TLS インターセプト機能は提供されません。
オプション D: VPC ファイアウォール ルールは、指定されたルールに基づいて VM インスタンスとの間のトラフィックを制御しますが、TLS インターセプトやトラフィック検査を実行する機能はありません。
したがって、オプション A は、セキュア Web プロキシを介した TLS インターセプションを可能にし、着信暗号化トラフィックを検査して、トラフィックが Web アプリケーションに到達する前にマルウェアなどの脅威を検出して軽減できるため、最も適切なソリューションです。
参考文献:
セキュアウェブプロキシの概要
クラウド負荷分散の概要

最新問題: **29**
オンプレミス環境からBigQueryデータセットへの日々のETLプロセスにおいて、機密性の高い個人情報（PII）がGoogle Cloud環境に取り込まれていることが判明しました。このデータを秘匿化してPIIを難読化する一方

で、データ分析のために再識別する必要があります。ソリューションではどのコンポーネントを使用すべきですか（2つ選択してください）。
A. シークレットマネージャー
B. クラウドキー管理サービス
C. 暗号化ハッシュを使用したクラウドデータ損失防止
D. 自動テキスト編集機能を備えたクラウドデータ損失防止
E. AES-SIV を使用した確定的暗号化によるクラウド データ損失防止
Answer: C,E (メーッセージを残す)
PII データの取り込みを処理し、分析目的で編集と再識別を確実に行うには、マスキングと暗号化のための適切な手法と Cloud Data Loss Prevention (DLP) を使用します。
* 暗号化ハッシュを使用したクラウドデータ損失防止 (DLP) (C):
* Cloud DLP を使用して、PII データに暗号ハッシュを適用します。ハッシュ化により、データは直接判読できない固定長の文字列に変換され、難読化レイヤーが提供されます。これにより、PII をマスキングしながらも、データの整合性を検証できるようになります。
* AES-SIV (E) を使用した確定的暗号化によるクラウド データ損失防止 (DLP):
* Cloud DLPを通じてAES-SIVを用いた確定的暗号化を適用します。確定的暗号化により、同じ入力からは常に同じ暗号化された出力が生成されるため、必要に応じて個人情報（PII）を再識別できます。この手法により、安全な暗号化を実現しながら、分析のためのデータ再識別が可能になります。
これら 2 つのアプローチを組み合わせることで、プライバシー保護のために PII を効果的にマスクし、後で分析で必要になったときに再識別することができます。
参考文献
* クラウドデータ損失防止ドキュメント
* データ編集とマスキング技術

最新問題: **30**
Cloud Functions の環境変数でシークレットが定期的にスキャンされ、Security Command Center に報告されるようにするための最適なソリューションはどれですか。
A. 環境変数を 1 日に複数回スキャンし、シークレットが検出された場合に Security Command Center で検出結果を作成する Cloud Functions を実装します。
B. 環境変数を評価し、Cloud Functions 内のシークレットを特定するために、定期的なピアレビューを実施します。シークレットが発見された場合は、セキュリティインシデントを報告します。
C. 機密データ保護を使用して、環境変数を 1 日に複数回スキャンします。秘密が検出された場合に、Security Command Center で検出結果を作成します。
D. Cloud Functions のアプリケーションコードをスキャンする CI/CD パイプラインに、動的アプリケーションセキュリティテストを統合します。シークレットが検出された場合は、ビルドプロセスを失敗させます。
Answer: C (メーッセージを残す)
問題は、デプロイされたリソース (Cloud Functions) の環境変数内の秘密 (機密データ パターン) をタイムリーかつ自動的に検出することです。

センシティブ データ保護（SDP）（旧称Cloud DLP）は、機密データパターンをスキャンして分類するためのGoogle Cloud専用サービスです。コード、構成、環境変数をスキャンし、その結果をSecurity Command Center（SCC）に直接統合するように設定できます。
抜粋:
「機密データ保護は、API キー、パスワード、その他の認証情報などの機密データを、事前に構築された情報タイプとカスタム情報タイプの両方を使用して、高度に構成可能な自動検出機能を提供します。」（出典8.1）
SDP は Cloud Functions やその他のリソース構成と統合して、環境変数や構成ファイルからシークレットをスキャンできます。違反は検出結果として Security Command Center に自動的にルーティングされます。(出典8.2) オプション D (DAST) はアプリケーションコードまたは実行中のアプリケーションロジックをスキャンしますが、要件ではシークレットは構成/デプロイメントメタデータの一部である環境変数にあると指定されているため、SDP は適切な検出ツールとなります。

最新問題**: 31**
社内のインシデント対応計画を策定中です。DevOps チームが Google Cloud 環境におけるデプロイメントの問題をレビューおよび調査する際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。
* 最小権限のアクセスを常に強制する必要があります。
* DevOps チームは、デプロイメントの問題発生時にのみ必要なリソースにアクセスできる必要があります。
Google が推奨するベスト プラクティスに従いながら、どのようにアクセスを許可すればよいですか?
A. プロジェクト閲覧者の ID およびアクセス管理 (1AM) ロールを DevOps チームに割り当てます。
B. リスト/表示権限が制限されたカスタムの 1AM ロールを作成し、DevOps チームに割り当てます。
C. サービスアカウントを作成し、プロジェクトオーナー 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。
D. サービスアカウントを作成し、限定的なリスト/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。
Answer: D (メーッセージを残す**)**
最小限の権限アクセスを確保し、デプロイメントの問題発生時にのみ DevOps チームに必要な権限を付与するには、次の手順に従います。
* サービス アカウントを作成します:
* Google Cloud プロジェクトで、DevOps チーム専用の新しいサービス アカウントを作成します。
* 制限付き権限の割り当て:
* サービスアカウントに必要なリスト/表示権限のみを付与します。例えば、compute.instances.list と compute.instances.get の権限を持つカスタム IAM ロールを作成できます。
* サービス アカウント ユーザー ロールを付与する:
* 作成した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チームメンバーに割り当てます。これにより、メンバーはサービスアカウントとして操作し、その権限を使用できるようになります。
* インシデント発生時のアクセス制御:
* デプロイメントの問題発生時、DevOps チームはサービスアカウントを一時的に使用してリソースにアクセスできます。これにより、問題の調査と解決に必要な最小限の権限でアクセスできるようになります。

* 自動化と監視:
* 必要に応じてサービス アカウント アクセスを有効または無効にする自動化を実装し、使用状況を監視して最小権限の原則に準拠していることを確認します。
利点：
* セキュリティ: 必要なものだけにアクセスを制限し、不正な変更のリスクを軽減します。
* 柔軟性: 永続的な昇格権限を付与することなく、インシデント発生時に必要なアクセスを提供します。
参考文献
* サービスアカウントの作成と管理
* サービスアカウントユーザーロール

最新問題: **32**
脆弱性に対するパッチがリリースされたため、DevOps チームは Google Kubernetes Engine (GKE) で実行中のコンテナを更新する必要があります。
DevOps チームはどのようにこれを実現すべきでしょうか?
A. Puppet または Chef を使用して、実行中のコンテナにパッチをプッシュします。
B. 自動アップグレードが有効になっていることを確認します。有効になっている場合、Google は GKE クラスタ内のノードをアップグレードします。
C. アプリケーション コードを更新するか、パッチを適用して新しいイメージをビルドし、再デプロイします。
D. Container Registry でベースイメージが利用可能になったときにコンテナが自動的にアップグレードされるように構成します。
Answer: B (メーッセージを残す**)**
説明/参考資料: https://cloud.google.com/kubernetes-engine/docs/security-bulletins

最新問題: **33**
アプリケーションは Cloud Run で実行しています。脆弱性スキャンのためのコンテナ分析はすでに有効になっています。
しかし、デプロイされるアプリケーションの制御が不十分であることが懸念されます。信頼できるコンテナイメージのみが Cloud Run にデプロイされるようにする必要があります。
何をすべきでしょうか?
2つの回答を選択してください
A. 既存の Kubernetes クラスターで Binary Authorization を有効にします。

B. 組織ポリシー制約の constraints/run.allowedBinaryAuthorizationPolicie を、許可された Binary Authorization ポリシー名のリストに設定します。
C. 組織ポリシー制約の constraints/compute.trustedimageProjects を、信頼できるコンテナ イメージを含む保護のリストに設定します。
D. 既存の Cloud Run サービスで Binary Authorization を有効にします。
E. Cloud Run ブレークグラスを使用して、デフォルトで Binary Authorization ポリシーを満たすイメージをデプロイします。
Answer: B,D (メーッセージを残す**)**
信頼できるコンテナ イメージのみが Cloud Run にデプロイされるようにするには、信頼できるイメージのみが使用されるようにするデプロイ時のセキュリティ制御である Binary Authorization を実装できます。
* バイナリ認証を設定する:
* Google Cloud Console に移動します。
* [セキュリティ] > [Binary Authorization] に移動します。
* 信頼できるイメージを検証する認証者を含めるようにポリシーを構成します。
* Cloud Run で Binary Authorization を有効にする:
* Cloud Run サービスに移動します。
* 適切な Binary Authorization ポリシーを選択して、既存の Cloud Run サービスで Binary Authorization を有効にします。
* 組織ポリシーを設定する:
* Google Cloud Console の [組織ポリシー] ページに移動します。
* constraints/run.allowedBinaryAuthorizationPolicies に制約を追加します。
* 組織全体に適用する許可された Binary Authorization ポリシー名のリストを指定します。
これらの手順により、Cloud Run にデプロイされたすべてのコンテナ イメージが指定された Binary Authorization ポリシーに対して検証され、信頼されていないイメージがデプロイされるのを防ぐことができます。
参考文献:
* バイナリ認証ドキュメント
* Cloud Run で Binary Authorization を有効にする

最新問題**: 34**
大手eコマース企業が、自社の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決済を行う際に、顧客のブラウザとGCPの間で決済情報が暗号化されることを保証したいと考えています。
彼らは何をすべきでしょうか?
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 の受信トラフィックを許可し、その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 の送信トラフィックを許可し、その他のすべての送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。
Answer: A (メッセージを残す**)**
説明
https://cloud.google.com/load-balancing/docs/load-balancing-overview#外部と内部のロードバランシング

最新問題**: 35**
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。チームでは、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、最小権限の原則を遵守したいと考えています。
どのオプションがチームの要件を満たしていますか?
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認証情報なしでバケットから読み取ることができる 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 インスタンス上のアプリケーションの構成にサービス アカウント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 キーを使用してデータを復号できるようにします。
Answer: C (メッセージを残す**)**
資格情報はメタデータ サーバーから取得されます。

最新問題**: 36**
あなたは最近、社内のGoogle Cloud実装をサポートするネットワークチームに加わりました。ファイアウォールルールの設定を理解し、ネットワークとGoogle Cloudの経験に基づいて推奨事項を提示することがあなたの任務です。優先度が同等またはそれより高い他のファイアウォールルールの属性と重複しているファイアウォールルールを検出するには、どの製品を推奨すべきでしょうか？
A. セキュリティコマンドセンター
B. ファイアウォールルールのログ記録
C. VPC フローログ
D. ファイアウォールインサイト
Answer: D (メッセージを残す**)**
https://cloud.google.com/network-intelligence-center/docs/firewall-
洞察/概念/概要#シャドウファイアウォールルール
ファイアウォールインサイトは、ファイアウォールルールを分析し、他のルールによってシャドウされているファイアウォールルールを検出します。シャドウされているルールとは、IPアドレスやポート範囲などの関連属性がすべて、シャドウイングルールと呼ばれる、より高いまたは同等の優先度を持つ1つ以上のルールの属性と重複しているファイアウォールルールのことです。

最新問題**: 37**

組織のオンプレミス ネットワークを、Production と Non-Production という 2 つのサブネットを持つ 1 つの共有 VPC を含む既存の Google Cloud 環境に接続する必要があります。以下の作業が必要です。
専用の交通機関をご利用ください。
オンプレミス環境からのプライベート API エンドポイントを介して Google Cloud API へのアクセスを構成します。
Google Cloud API が VPC Service Controls 経由でのみ使用されるようにします。
何をすべきでしょうか?
A. 1. オンプレミス環境と Google Cloud の間に Cloud VPN リンクを設定します。2. オンプレミスの DNS 構成で制限された googleapis.com ドメインを使用してプライベート アクセスを構成します。
B. 1. オンプレミス環境と Google Cloud の間に Partner Interconnect リンクを設定します。2.
オンプレミスの DNS 構成で private.googleapis.com ドメインを使用してプライベート アクセスを構成します。
C. 1. オンプレミス環境と Google Cloud の間に Direct Peering リンクを設定します。2. 両方の VPC サブネットにプライベート アクセスを構成します。
D. 1. オンプレミス環境と Google Cloud の間に Dedicated Interconnect リンクを設定します。2. オンプレミスの DNS 構成で、restricted.googleapis.com ドメインを使用してプライベート アクセスを構成します。
Answer: D (メーッセージを残す)
オンプレミス環境と Google Cloud の間に Dedicated Interconnect リンクを設定します。
Dedicated Interconnect は、オンプレミス ネットワークと Google ネットワーク間の直接的な物理接続を提供し、高スループット、低レイテンシの接続に最適です。
必要な帯域幅と場所を指定して、Google Cloud Console から Dedicated Interconnect をリクエストします。
プロビジョニングが完了したら、オンプレミス ルーターで接続を設定し、Google Cloud とルートを交換するように BGP セッションを構成します。
オンプレミスの DNS 構成で、restricted.googleapis.com ドメインを使用してプライベート アクセスを構成します。
オンプレミスのDNSサーバーを設定して、Google APIをrestricted.googleapis.comに解決します。これにより、トラフィックがGoogleネットワーク内に留まり、パブリックインターネットに公開されることがなくなります。
必要な API エンドポイントに restrict.googleapis.com を使用するように DNS 設定を更新します。
この設定により、すべての Google Cloud API トラフィックがプライベート リンク経由でルーティングされ、追加のセキュリティとコンプライアンスのために VPC Service Controls の対象となることが保証されます。
参考文献:
専用相互接続の概要
restrictive.googleapis.com を使用するように DNS を構成する

最新問題**: 38**
あなたは、複数のGoogle Cloudリージョンに顧客の機密データを保管しているeコマース企業で働いています。開発チームは注文処理用の新しい3層アプリケーションを構築し、本番環境に統合する必要があります。あなたは、新しいアプリケーションの強固なセキュリティ境界と分離を確保し、認定サードパーティベンダーに

よる安全なリモートメンテナンスを容易にし、最小権限の原則に従うネットワークアーキテクチャを設計する必要があります。あなたは何をすべきでしょうか？
A. 各層ごとに個別のVPCネットワークを作成します。アプリケーション層とその他の必要なVPC間ではVPCピアリングを使用します。ベンダーには、メンテナンス目的でVPC内のインスタンスへのSSHキーとルートアクセスのみを提供します。
B. 単一のVPCネットワークを作成し、各層に異なるサブネットを作成します。サードパーティベンダー専用の新しいGoogleプロジェクトを作成し、ベンダーにネットワーク管理者のロールを付与します。VPNアプライアンスをデプロイし、ベンダーの設定を利用してサードパーティのアクセスを保護します。
C. 各層に個別のVPCネットワークを作成します。アプリケーション層とその他の必要なVPC間ではVPCピアリングを使用します。管理リソースへのリモートアクセスにはIdentity-Aware Proxy (IAP)を有効にし、アクセスを承認されたベンダーに制限します。
D. 単一のVPCネットワークを作成し、各層に異なるサブネットを作成します。サードパーティベンダー専用の新しいGoogleプロジェクトを作成します。ベンダーにそのプロジェクトの所有権と、共有VPC構成を変更する権限を付与します。
Answer: C (メーッセージを残す)
正確な抜粋からの包括的かつ詳細な説明：
この質問は、強力な分離 (セグメンテーション)、安全なリモート アクセス、最小権限という 3 つのセキュリティ要件を組み合わせたものです。
強力な分離: 各層(C)ごとに別々のVPCネットワークを作成すると、最も強力なネットワーク分離が実現します。
/segmentation により、サブネット (B、D) を持つ単一の VPC と比較して、影響範囲が制限されます。VPC ピアリングは、これらの個別の VPC 間で制御された通信を可能にする標準的な方法です。
抜粋: 「機密データを独自の VPC ネットワークに分離します。」(ソース 2.5) 個別の VPC によるセグメンテーションは、機密性の高いワークロードを分離するための標準的なベスト プラクティスです。
安全なリモートアクセスと最小権限：Identity-Aware Proxy（IAP）は、パブリックIPやVPNを必要とせずに仮想マシンインスタンスへの安全なリモートアクセスを提供するGoogle Cloudの推奨サービスです。これは、ユーザーのIDとコンテキストを検証することで、明示的な検証と最小権限というゼロトラスト原則に準拠しています。SSH認証鍵とルートアクセス（A）、ネットワーク管理者ロール（B）、またはプロジェクトオーナーシップ（D）を付与することは、最小権限の原則に違反します。
抜粋: 「アクセス制御: 次のようなソリューションを使用して、ユーザー ID とコンテキストに基づいてアクセス制御を実施します...」
Identity-Aware Proxy（IAP）。これにより、セキュリティをネットワーク境界から個々のユーザーやデバイスに移行できます。このアプローチにより、きめ細かなアクセス制御が可能になり、攻撃対象領域が縮小されます。（出典2.2）抜粋：「BeyondCorpは、…やIdentity-Aware ProxyなどのGoogle Cloudツールを使用して、境界をネットワークから個々のデバイスやユーザーへと拡大します。」（出典2.3）抜粋：「IAPは、アクセスを許可する前にユーザーのIDとコンテキストを検証することで、GCPでホストされるアプリケーションを保護します。…IAPによってユーザーにアプリケーションまたはリソースへのアクセスを許可すると、VPNを必要とせずに、使用中の製品によって実装されたきめ細かなアクセス制御が適用されます。」（出典2.3）オプションCは、個別の

VPC（強力な分離）とIAP（最小権限による安全なリモートアクセス）を使用することで、3つの要件すべてを満たす唯一の選択肢です。

最新問題: **39**
会社では機密データをCloud Storageに保存しています。暗号化プロセスではオンプレミスで生成された鍵を使用したいと考えています。
何をすべきでしょうか?
A. Cloud Key Management Service を使用して、データ暗号化キー (DEK) を管理します。
B. Cloud Key Management Service を使用して、キー暗号化キー (KEK) を管理します。
C. 顧客提供の暗号化キーを使用して、データ暗号化キー (DEK) を管理します。
D. 顧客提供の暗号化キーを使用して、キー暗号化キー (KEK) を管理します。
Answer: (解答を表示する**)**
https://cloud.google.com/security/encryption-at-rest/default-encryption/

最新問題: **40**
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。チームでは、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、最小権限の原則を遵守したいと考えています。
どのオプションがチームの要件を満たしていますか?
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認証情報なしでバケットから読み取ることができる 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 インスタンス上のアプリケーションの構成にサービス アカウント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 キーを使用してデータを復号できるようにします。
Answer: (解答を表示する**)**
環境変数 GOOGLE_APPLICATION_CREDENTIALS が設定されている場合、ADC はその変数が指すサービス アカウントキーまたは設定ファイルを使用します。環境変数 GOOGLE_APPLICATION_CREDENTIALS が設定されていない場合、ADC はコードを実行しているリソースに関連付けられているサービスアカウントを使用します。https://cloud.google.com/docs/authentication
/production#コードにサービスアカウントキーへのパスを渡す

最新問題: **41**
あなたは組織のセキュリティ管理者です。本番環境におけるサービスアカウント作成機能を制限する必要があります。これを組織全体で一元的に実現したいと考えています。どうすればよいでしょうか？
A. Identity and Access Management (IAM) を使用して、本番環境にアクセスできるすべてのユーザーとサービス アカウントのアクセスを制限します。

B. 組織ポリシーの制約/iam.disableServiceAccountKeyCreation ブール値を使用して、新しいサービス アカウントの作成を無効にします。
C. 組織ポリシーの制約/iam.disableServiceAccountKeyUpload ブール値を使用して、新しいサービス アカウントの作成を無効にします。
D. 組織ポリシーの制約/iam.disableServiceAccountCreation ブール値を使用して、新しいサービス アカウントの作成を無効にします。
Answer: (解答を表示する**)**
参考: https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts ブール制約 iam.disableServiceAccountCreation を使用すると、新しいサービスアカウントの作成を無効化できます。これにより、開発者がプロジェクトに対して持つ他の権限を制限することなく、サービスアカウントの管理を一元化できます。https://cloud.google.com/resource-manager/docs/organization- policy/restricting-service-accounts#disable_service_account_creation

最新問題**: 42**
DevOps チームは、次のプロセスで Packer を使用して Compute Engine イメージを構築します。
1 一時的な Compute Engine VM を作成します。
2 Cloud Storage バケットから VM のファイル システムにバイナリをコピーします。
3 VM のパッケージ マネージャーを更新します。
4 インターネットから外部パッケージを VM にインストールします。
セキュリティチームは、VM 上のパブリック IP アドレスの使用を制限する組織ポリシー consrtraints/compure.vnExtemallpAccess を有効化しました。これを受けて、DevOps チームはスクリプトを更新し、Compute Engine VM 上のパブリック IP アドレスを削除しましたが、接続の問題によりビルド パイプラインが失敗しています。
何をすべきでしょうか?
2つの回答を選択してください
A. Compute Engine VM と同じ VPC およびリージョンに Cloud NAT インスタンスをプロビジョニングします。
B. 管理対象外インスタンス グループ内の VM に HTTP ロードバランサをプロビジョニングして、インターネットから VM への受信接続を許可します。
C. インターネットとの間のトラフィックを許可するように VPC ルートを更新します。
D. Compute Engine VM と同じ VPC およびリージョンに Cloud VPN トンネルをプロビジョニングします。
E. Compute Engine VM がデプロイされているサブネット上でプライベート Google アクセスを有効にします。
Answer: (解答を表示する**)**
* Cloud NATインスタンスをプロビジョニングします。
* クラウド NAT (ネットワーク アドレス変換) により、外部 IP アドレスを持たないインスタンスでも安全にインターネットにアクセスできます。
* Google Cloud Console で、VPC ネットワーク セクションに移動し、Cloud NAT を選択します。

* Compute Engine VM がデプロイされている VPC とリージョンを指定して、新しい Cloud NAT 構成を作成します。
* Cloud NAT を構成する:
* 指定したサブネット内の VM に送信インターネット接続を提供するように Cloud NAT インスタンスが構成されていることを確認します。
* この設定により、VM はパブリック IP アドレスを必要とせずに、パッケージの更新や外部インストールのためにインターネットにアクセスできるようになります。
* プライベート Google アクセスを有効にする:
* プライベート Google アクセスを使用すると、サブネット内の VM は内部 IP アドレスを使用して Google API やサービスにアクセスできます。
* Google Cloud Console で、VPC ネットワーク セクションに移動し、サブネットを選択します。
* Compute Engine VM で使用されるサブネットを編集し、プライベート Google アクセスを有効にします。
* DevOps スクリプトを更新します。
* DevOps スクリプトが新しいネットワーク構成で動作するように更新されていることを確認します。
* ビルド プロセスをテストして、VM が必要なリソースにアクセスでき、ビルド パイプラインを正常に完了できることを確認します。
参考文献:
* クラウド NAT ドキュメント
* プライベートGoogleアクセス

最新問題**: 43**
個人情報（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する必要があります。データの漏洩を防ぐため、BigQueryテーブルへのクエリは、許可されたIPアドレスからのリクエストのみに許可されます。
何をすべきでしょうか?
A. サービス境界を使用し、承認された送信元 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. Cloud Data Loss Prevention (DLP) とともに、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使用します。
Answer: (解答を表示する**)**
* VPC サービスコントロールを有効にする:
* VPC Service Controls を使用すると、GCP リソースの周囲にセキュリティ境界を定義できるため、データ流出のリスクを軽減できます。
* BigQuery プロジェクトの周囲にサービス境界を設定し、定義された境界内にデータ アクセスを制限します。
* アクセスレベルの作成:
* Google Cloud Console で、Access Context Manager に移動します。

* IP アドレスの条件に基づいてアクセス レベルを定義し、BigQuery リソースへのアクセスが許可される承認済みソース IP アドレスを指定します。
* これらのアクセス レベルは、IP アドレスに基づいて機密データにアクセスできるユーザーを制限するポリシーを適用するために使用されます。
* アクセス レベルを使用してサービス境界を適用します。
* 作成されたアクセス レベルをサービス境界に適用して、指定された IP アドレスからのリクエストのみが BigQuery テーブルにアクセスできるようにします。
* この設定により、機密性の高い PII データに不正な IP アドレスからアクセスできなくなり、データ流出のリスクが軽減されます。
参考文献:
* VPC サービスコントロール
* アクセスコンテキストマネージャー
* アクセスレベルの定義

最新問題**: 44**
組織内でBigQuery分析データウェアハウスを管理しています。すべての顧客のデータを共通テーブルに保存しつつ、行と列の権限に基づいてクエリアクセスを制限したいと考えています。クエリ以外の操作はサポートしないようにする必要があります。
あなたは何をすべきでしょうか？ 2つ選択してください。）
A. フィルター式を TRUE に設定してクエリを実行するときに結果データを制限するための行レベルのアクセス ポリシーを作成します。
B. Cloud Key Management Service (KMS) で Authenticated Encryption with Associated Data (AEAD) 関数を使用して列レベルの暗号化を構成し、クエリ実行時に列へのアクセスを制御します。
C. フィルター式を FALSE に設定してクエリを実行するときに結果データを制限するための行レベルのアクセス ポリシーを作成します。
D. クエリ実行時に列へのアクセスを制御するために、動的データ マスキング ルールを構成します。
E. クエリ実行時に列へのアクセスを制御するために、列レベルのポリシー タグを作成します。
Answer: C,E (メーッセージを残す**)**
https://cloud.google.com/bigquery/docs/using-row-level-security-with-features#the_true_filter
https://cloud.google.com/bigquery/docs/column-level-security-intro#column-level_security_workflow

最新問題**: 45**
Compute Engine ディスク上のデータを、Cloud Key Management Service（KMS）で管理される鍵を使用して保存時に暗号化する必要があります。これらの鍵に対する Cloud Identity and Access Management（IAM）権限は、すべての鍵に対して同じ権限を持つ必要があるため、グループ化して管理する必要があります。
何をすべきでしょうか?
A. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。キーレベルでIAM権限を管理します。
B. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。IAM権限はキーリングレベルで管理します。

C. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーレベルで管理します。
D. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーリングレベルで管理します。
Answer: B (メーッセージを残す**)**
IAM権限をキーリングレベルで管理する方が、個々のキーレベルで管理するよりも効率的でスケーラブルです。単一のキーリングを作成し、その中にすべての暗号化キーを配置することで、キーリング全体に統一されたIAM権限を適用でき、権限管理が簡素化されます。
手順:
* KeyRing を作成する: 永続ディスクに必要なすべての暗号化キーに対して、Cloud KMS に単一の KeyRing を設定します。
* 暗号化キーの作成: このキーリング内に必要な暗号化キーを生成します。
* IAM 権限の設定: KeyRing に IAM ロールと権限を割り当てて、このレベルでのアクセス制御を管理し、KeyRing 内のすべてのキーがこれらの権限を継承するようにします。
参考文献:
* Google Cloud: クラウド キー管理サービス (KMS)
* リソースへのアクセスの管理

最新問題**: 46**
ブートディスクのソースとして使用できるイメージを制限したい場合、これらのイメージは専用のプロジェクトに保存されます。
何をすべきでしょうか?
A. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。許可操作で、信頼されたプロジェクトをホワイトリストとしてリストします。
B. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。信頼済みプロジェクトを拒否操作の例外としてリストします。
C. リソースマネージャーで、信頼されたプロジェクトのプロジェクト権限を編集します。組織を 「コンピューティングイメージユーザー」ロールのメンバーとして追加します。
D. リソースマネージャーで組織の権限を編集します。プロジェクトIDをロールを持つメンバーとして追加します。
コンピューティングイメージユーザー。
Answer: (解答を表示する**)**
説明/参考資料: https://cloud.google.com/compute/docs/images/restricting-image-access

最新問題: 47
Compute Engine 上で実行されるアプリケーションから機密性の高い設定データを保存および取得するためのソリューションを推奨するよう求められています。どのオプションを推奨すべきでしょうか？
A. クラウド キー管理サービス
B. Compute Engine ゲスト属性
C. Compute Engine カスタム メタデータ
D. シークレットマネージャー
Answer: D (メーッセージを残す)
* 目的: Compute Engine で実行されているアプリケーションの機密構成データを保存および取得します。
* ソリューション: Secret Manager を使用して、機密構成データを安全に保存し、アクセスを管理します。
* 手順:
* ステップ 1: Google Cloud Console を開きます。
* ステップ 2: Secret Manager セクションに移動します。
* ステップ 3: 新しいシークレットを作成し、機密構成データを追加します。
* ステップ 4: シークレットへのアクセスを制御するための適切な IAM ポリシーを設定します。
* ステップ 5: 適切なクライアント ライブラリまたは API を使用して、Secret Manager からシークレットを取得するようにアプリケーションを更新します。
Secret Manager は、きめ細かなアクセス制御と監査ログ機能を備え、機密情報を安全かつ集中的に管理する方法を提供します。
参考文献:
* シークレットマネージャーのドキュメント
* 秘密の保存とアクセス

最新問題: 48
組織には、人間とマシンのアクセスを管理するために使用されている一元化されたIDプロバイダがあります。この既存のID管理システムを活用して、オンプレミスのアプリケーションがハードコードされた認証情報なしでGoogle Cloudにアクセスできるようにしたいと考えています。どうすればよいでしょうか？
A. セキュア ウェブ プロキシを有効にします。セキュア ウェブ プロキシを導入するリージョンごとにプロキシサブネットを作成します。証明書マネージャーに SSL 証明書を導入します。Google Cloud サービスへのアクセスを許可するセキュア ウェブ プロキシのポリシーとルールを作成します。
B. Enable Workforce Identity Federation. Create a workforce identity pool and specify the on- premises identity provider as a workforce identity pool provider. Create an attribute mapping to map the on-premises identity provider token to a Google STS token. Create an IAM binding that binds the required role(s) to the external identity by specifying the project ID, workload identity pool, and attribute that should be matched.
C. Enable Identity-Aware Proxy (IAP). Configure IAP by specifying the groups and service accounts that should have access to the application. Grant these identities the IAP-secured web app user role.

D. Enable Workload Identity Federation. Create a workload identity pool and specify the on-premises identity provider as a workload identity pool provider. Create an attribute mapping to map the on- premises identity provider token to a Google STS token. Create a service account with the necessary permissions for the workload. Grant the external identity the Workload Identity user role on the service account.
Answer: D (メーッセージを残す)
Workload Identity Federation is used for applications when Workforce Identity Federation is used for humans.

最新問題**: 49**
PCIコンプライアンスの観点からGCPを評価したいと考えています。Google固有の管理機能を特定する必要があります。
情報を見つけるにはどの文書を確認する必要がありますか?
A. Google Cloud Platform: 顧客責任マトリックス
B. PCI DSS要件とセキュリティ評価手順
C. PCI SSC クラウドコンピューティングガイドライン
D. Compute Engine の製品ドキュメント
Answer: A (メーッセージを残す)
https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf

最新問題**: 50**
あるウェブサイトデザイン会社は最近、すべての顧客サイトをApp Engineに移行しました。一部のサイトはまだ移行中で、顧客と会社の従業員のみがどこからでも閲覧できるようにする必要があります。
進行中のサイトへのアクセスを制限するソリューションはどれですか?
A. Cloud Identity-Aware Proxy (IAP) を有効にし、顧客と従業員のユーザー アカウントを含む Google グループへのアクセスを許可します。
B. 顧客と従業員のネットワークからのアクセスを許可し、その他のすべてのトラフィックを拒否する App Engine ファイアウォール ルールを作成します。
C. Cloud VPN を使用して、関連するオンプレミス ネットワークと会社の GCP 仮想プライベート クラウド (VPC) ネットワークの間に VPN 接続を作成します。
D. 顧客と従業員のユーザー アカウントを含む .htaccess ファイルを App Engine にアップロードします。
Answer: A (メーッセージを残す)

最新問題**: 51**
Google Cloud リソースにアクセスする必要があるアプリケーションを Google Cloud の外部で実行しています。
ワークロード ID 連携を使用して外部 ID に Identity and Access Management (IAM) ロールを付与することで、サービス アカウント キーに関連するメンテナンスとセキュリティの負担を軽減しています。他のユーザーの ID を偽装して Google Cloud リソースに不正アクセスしようとする試みから保護する必要があります。
あなたは何をすべきでしょうか？ 2つ選択してください。）
A. IAM API のデータ アクセス ログを有効にします。
B. サービス アカウントを偽装できる外部 ID の数を制限します。

C. 専用のプロジェクトを使用して、ワークロード ID プールとプロバイダーを管理します。
D. 属性マッピングで不変の属性を使用します。
E. サービス アカウントがアクセスできるリソースを制限します。
Answer: C,D (メーッセージを残す**)**
https://cloud.google.com/iam/docs/best-practices-for-using-workload-identity-federation#protecting_against_spoofing_threats

最新問題**: 52**
チームは、オンプレミスの Active Directory サービスから GCP の IAM 権限を一元管理したいと考えています。また、AD グループのメンバーシップごとに権限を管理したいと考えています。
これらの要件を満たすためにチームは何をすべきでしょうか?
A. グループを同期するように Cloud Directory Sync を設定し、グループに IAM 権限を設定します。
B. SAML 2.0 シングル サインオン (SSO) を設定し、グループに IAM 権限を割り当てます。
C. Cloud Identity and Access Management API を使用して、Active Directory からグループと IAM 権限を作成します。
D. Admin SDK を使用してグループを作成し、Active Directory から IAM 権限を割り当てます。
Answer: A (メーッセージを残す**)**
既存のID管理システムを引き続き使用するには、ADとGCP IAM間でIDを同期する必要があります。そのために、GoogleはCloud Directory Syncというツールを提供しています。このツールは、AD内のすべてのIDを読み取り、GCP内に複製します。IDが複製されると、グループにIAM権限を適用できるようになります。その後、GoogleがサービスプロバイダとしてSAMLを設定し、ADFS、またはPingやOktaなどのサードパーティツールがIDプロバイダとして機能するようにします。
この方法により、認証を Google から自分の管理下にあるものに効果的に委任できます。」

最新問題**: 53**
組織では、Google Cloud 環境に保存されているデータの暗号化に使用する鍵を完全に制御したいと考えています。鍵は Google の外部で生成 保存し、BigQuery を含む多くの Google サービスと統合する必要があります。
何をすべきでしょうか?
A. インポートした鍵マテリアルを使用して Cloud Key Management Service（KMS）鍵を作成します。インポート中の保護のために鍵をラップします。信頼できるシステムで生成された鍵を Cloud KMS にインポートします。
B. Google が管理する FIPS 140-2 レベル 3 ハードウェア セキュリティ モジュール (HSM) に保存される KMS キーを作成します。Identity and Access Management (IAM) の権限設定を管理し、キーのローテーション期間を設定します。
C. サポートされているベンダーの外部ハードウェア セキュリティ モジュール (HSM) システムと統合する Cloud 外部キー管理 (EKM) を使用します。
D. 信頼できる外部システムで生成されたキーと顧客提供の暗号化キー (CSEK) を使用します。API 呼び出しの一部として生の CSEK を提供します。

Answer: (解答を表示する**)**
サポートされているベンダーの外部ハードウェア セキュリティ モジュール（HSM）システムと統合された Cloud 外部鍵管理（EKM）を使用します。Cloud EKM を使用すると、Google Cloud の外部で管理されている暗号鍵を使用できます。つまり、オンプレミスの HSM またはサポートされている他の外部 HSM サービスで鍵を生成して保存し、これらの鍵をさまざまな Google Cloud サービスと統合できます。
Google サービスとの統合：Cloud EKM は、BigQuery、Cloud Storage、Compute Engine など、多くの Google Cloud サービスとシームレスに統合されます。これにより、Google Cloud の強力なサービスを活用しながら、暗号鍵を完全に制御できます。
参照：
Cloud 外部鍵管理 (EKM) ドキュメント
外部キー管理の概要

最新問題**: 54**
ある顧客のデータサイエンス グループは、分析ワークロードに Google Cloud Platform（GCP）の利用を希望しています。会社のポリシーでは、すべてのデータは会社所有とし、すべてのユーザー認証は自社の Security Assertion Markup Language（SAML）2.0 ID プロバイダ（IdP）を経由する必要があると定められています。インフラストラクチャ運用システム エンジニアは、顧客のために Cloud Identity を設定しようとしたところ、そのドメインが既に G Suite で使用されていることに気付きました。
最小限の混乱で作業を進めるには、システム エンジニアにどのようなアドバイスをするのが最善でしょうか?
A. Google サポートに連絡し、新しい Cloud Identity ドメインでドメイン名を使用するためのドメイン競合プロセスを開始してください。
B. 新しいドメイン名を登録し、それを新しい Cloud Identity ドメインに使用します。
C. データ サイエンス マネージャーのアカウントを既存のドメインのスーパー管理者としてプロビジョニングするよう Google に依頼します。
D. 顧客の経営陣に、Google マネージド サービスのその他の用途を探してもらい、既存の特権管理者と連携します。
Answer: (解答を表示する**)**
https://support.google.com/cloudidentity/answer/7389973
既存のGoogle Workspaceのお客様の場合
Cloud Identity Premium に登録するには、次の手順に従います。
管理者アカウントを使用して、admin.google.com にある Google 管理コンソールにログインします。
管理コンソールのホームページの左上にあるメニュー アイコンをクリックし、[お支払い] をクリックして、[その他のサービスを取得] をクリックします。
Cloud Identity をクリックします。
Cloud Identity Premium の横にある [無料トライアルを開始] をクリックします。
ガイドの指示に従ってください。

最新問題**: 55**

組織では、Compute Engine の仮想マシン（VM）に大きく依存しています。チームの成長とリソース需要の増加により、VM の無秩序な増加が問題となっています。一貫したセキュリティ強化とタイムリーなパッケージ更新の維持は、ますます困難になっています。VM イメージ管理を一元化し、仮想マシンのライフサイクル全体にわたってセキュリティ ベースラインの適用を自動化する必要があります。どうすればよいでしょうか？
A. VM マネージャーを使用して、プロジェクト全体の YM にパッチを自動的に配布して適用します。
VM マネージャーを、中央リポジトリに保存されている強化された組織標準の VM イメージと統合します。
B. すべてのプロジェクトに対して Compute Engine の単一テナンシー機能を設定します。Policy Controller でカスタム組織ポリシーを設定し、チームが使用できるオペレーティング システムとイメージ ソースを制限します。
C. Cloud Buildトリガーを作成し、強化されたVMイメージを生成するパイプラインを構築します。パイプラインで脆弱性スキャンを実行し、スキャンに合格したイメージをレジストリに保存します。このレジストリを参照するインスタンステンプレートを使用します。
D. Security Command Center Enterprise を有効化します。VM 検出およびポスチャ管理機能を使用して、セキュリティ強化の状態を監視し、問題が検出されると自動応答をトリガーします。
Answer: A (メーッセージを残す**)**
VM Managerを使用すると、VMのパッチ適用、構成管理、コンプライアンス遵守を一元管理・自動化できます。
中央リポジトリに保存された強化されたVMイメージと統合することで、VMがセキュリティベースラインに基づいて常に作成され、定期的に更新されることが保証されます。
このソリューションは、自動化と集中管理を提供し、VM の拡散の課題と一貫したセキュリティの必要性の両方に対処します。

最新問題**: 56**
御社では集中型セキュリティ サービスを導入しました。Google Cloud で実行されるすべてのアプリケーションは、このサービスにデータを送信する必要があります。開発者がプロジェクト内でファイアウォール ルールを自由に設定できるようにしつつ、集中型セキュリティ サービスへのアクセスが誤ってブロックされるのを防ぐ必要があります。どうすればよいでしょうか？
A. 中央のセキュア Web プロキシをデプロイし、すべての VPC ネットワークに接続します。中央セキュリティ サービスへのトラフィックを許可するセキュア Web プロキシポリシーを作成します。
B. 中央セキュリティ サービスへの接続を許可し、他のすべてのトラフィックを後続のファイアウォール レベルに送信することで、中央セキュリティ サービスを優先する階層型ファイアウォール ポリシーを実装します。
C. 他のすべてのプロジェクトからアクセスできる共有 VPC ネットワークを管理するための中央プロジェクトを作成します。
このプロジェクト内のすべてのファイアウォール ルールを集中管理します。
D. Terraform を使用して、すべてのプロジェクトで必要なファイアウォールルールの作成を自動化します。
ルールの変更権限は、Terraform サービスアカウントのみに制限します。
Answer: B (メーッセージを残す**)**
この問題には 2 つの重要な要件があります。
すべてのアプリケーションは、集中化されたセキュリティ サービスにデータを送信する必要があります。
開発者はプロジェクト内のファイアウォール ルールに対して高い自律性を必要とします。

中央セキュリティ サービスへのアクセスが誤ってブロックされるのを防ぎます。
このシナリオでは、プロジェクト レベルの柔軟性を維持しながら、リソース階層の上位レベルで重要なネットワーク ポリシーを適用するメカニズムが必要です。
階層型ファイアウォール ポリシー :Google Cloud の階層型ファイアウォール ポリシー（HFP）は、まさにこの目的のために設計されています。管理者は組織レベルまたはフォルダレベルでファイアウォール ルールを定義でき、これらのルールは階層内のすべてのプロジェクトと VPC ネットワークに継承されます。重要なのは、HFP ルールに優先順位を付けられることです。優先度の高い（数値が小さい）ルールが最初に評価されます。つまり、プロジェクト レベルのファイアウォール ルールではオーバーライドまたはブロックできない、重要なサービスに対して優先度の高い「許可」ルールを作成できます。抜粋参照：「階層型ファイアウォール ポリシーを使用すると、組織全体で一貫したネットワーク セキュリティ ポリシーを定義し、適用できます。ポリシーは組織レベルまたはフォルダレベルで適用でき、その階層内のすべてのプロジェクトと VPC ネットワークに継承されます。」および「階層型ファイアウォール ポリシー内のルールは、優先度に基づいて VPC ネットワーク ファイアウォール ルールよりも優先されます。優先度の値が低いルールは、優先度の値が高いルールよりも優先されます。」（Google Cloud ドキュメント :https://cloud.
google.com/vpc/docs/ファイアウォールポリシーの概要
偶発的なブロックを防止しながら自律性を確保：階層型ファイアウォールポリシーにおいて、中央セキュリティサービスに高優先度の「許可」ルールを設定することで、開発者がプロジェクトレベルのファイアウォールルールをどのように設定しても、このトラフィックが常に許可されることが保証されます。これにより、重要な接続性を確保しながら、開発者はプロジェクト内の重要度の低いファイアウォールルールを高い自律性で管理できます。
他のオプションを評価してみましょう。
A) 中央のセキュア Web プロキシをデプロイし、すべての VPC ネットワークに接続します。中央セキュリティサービスへのトラフィックを許可するセキュア Web プロキシポリシーを作成します。セキュア Web プロキシは、外部 Web サービスへの HTTP/S アウトバウンドトラフィック用です。中央セキュリティサービスは必ずしも外部 Web サービスではない可能性があり、このソリューションはアプリケーション層プロキシに重点を置いており、内部サービスへのデータ送信などの一般的なネットワーク接続には対応していません。また、開発者がプロジェクトレベルのファイアウォールルールでアクセスをブロックするという課題にも直接対応していません。
C). 他のすべてのプロジェクトからアクセスできる共有 VPC ネットワークを管理するための中央プロジェクトを作成します。
このプロジェクト内のすべてのファイアウォールルールを一元管理します。共有VPCはネットワーク管理を一元化しますが、すべてのファイアウォールルールが一元管理されることを意味します。これは、開発者が「プロジェクト内でファイアウォールルールを高いレベルで自由に設定できる」という要件と真っ向から矛盾します。共有VPCでは、この特定のシナリオでは制御が一元化されすぎてしまいます。
D) Terraform を使用して、すべてのプロジェクトで必要なファイアウォールルールの作成を自動化します。ルール変更権限は Terraform サービスアカウントのみに制限します。このアプローチではルールの作成は自動化されますが、開発者がプロジェクト内で競合するルールや上書きするルールを作成することを防ぐことはできません（ただし、すべてのルールを Terraform で管理している場合は、自律性が失われます）。また、すべてのファイアウォールルールに対する IAM 権限を制限する必要があるため、開発者の「高い自律性」要件に反しま

す。階層型ファイアウォールポリシーは、特定のルールを上書きおよび適用するための、より堅牢でネイティブなソリューションを提供します。
したがって、階層型ファイアウォール ポリシーを実装することが最も効果的なソリューションです。これにより、重要なセキュリティ サービスの接続をより高いレベルで強制しながら、開発者にプロジェクト固有のファイアウォール ルールに対する必要な自律性を与えることができます。

最新問題: **57**
あなたは最近、社内のGoogle Cloud実装をサポートするネットワークチームに加わりました。ファイアウォールルールの設定を理解し、ネットワークとGoogle Cloudの経験に基づいて推奨事項を提示することがあなたの任務です。優先度が同等またはそれより高い他のファイアウォールルールの属性と重複しているファイアウォールルールを検出するには、どの製品を推奨すべきでしょうか？
A. セキュリティコマンドセンター
B. VPC フローログ
C. ファイアウォールインサイト
D. ファイアウォールルールのログ記録
Answer: C (メーッセージを残す**)**

最新問題: **58**
セキュリティチームは、ユーザー管理キーが適切に管理されず、侵害されるリスクを軽減したいと考えています。そのためには、開発者が組織内のプロジェクトでユーザー管理サービスアカウントキーを作成できないようにする必要があります。どのように対策を講じるべきでしょうか？
A. サービス アカウント キーを管理するために Secret Manager を構成します。
B. 組織ポリシーを有効にして、サービス アカウントの作成を無効にします。
C. 組織ポリシーを有効にして、サービス アカウント キーが作成されないようにします。
D. ユーザーから iam.serviceAccounts.getAccessToken 権限を削除します。
Answer: C (メーッセージを残す**)**
開発者がユーザー管理のサービス アカウント キーを作成することを防ぎ、キーの管理ミスのリスクを軽減するには、これらのキーの作成を明確に禁止する組織ポリシーを有効にする必要があります。
* 組織ポリシーを有効にして、サービス アカウント キーが作成されないようにします (C):
* Google Cloud は、サービス アカウント キーの作成を含む様々な操作を制限する組織ポリシーを適用する機能を提供しています。このポリシーを有効にすると、開発者がユーザー管理のサービス アカウント キーを新規作成できないようにすることができ、キーの不適切な管理や潜在的なセキュリティ侵害のリスクを最小限に抑えることができます。
参考文献
* サービスアカウントのドキュメント
* 組織ポリシーサービスドキュメント

最新問題: **59**
組織向けにGoogle Cloudにセキュアウェブプロキシインスタンスを実装しました。テストインスタンスでこの構成をテストしたところ、インターネットにアクセスできました。しかし、開発者はGoogle Cloud上のLinuxイ

ンスタンスからセキュアウェブプロキシインスタンスで許可されたURLにアクセスできません。開発者と協力してこの問題を解決したいと考えています。どうすればよいでしょうか？
A. 開発者インスタンスのサブネットからのインターネット アクセスを有効にするために Cloud NAT ゲートウェイを構成します。
B. 開発者がインスタンスを再起動し、HTTP サービスが有効になっていることを確認します。
C. 開発者がインスタンス上でプロキシ アドレスを明示的に構成していることを確認します。
D. 開発者インスタンスからの HTTP/S を許可するようにファイアウォール ルールを構成します。
Answer: C (メーッセージを残す**)**
https://cloud.google.com/secure-web-proxy/docs/概要
セキュアWebプロキシは、送信Webトラフィック（HTTP/S）のセキュリティ確保を支援するクラウドファーストのサービスです。クライアント側でセキュアWebプロキシをゲートウェイとして明示的に使用するように設定してください。

最新問題**: 60**
あなたは会社のために新しい Google Cloud 組織を作成する責任を負っています。特権管理者アカウントを作成する際に実行する必要がある 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. Google 管理コンソールでアクセス レベルを作成し、スーパー管理者が Google Cloud にログインできないようにします。
B. Google Cloud Console の組織レベルで、特権管理者の Identity and Access Management（IAM）ロールを無効にします。
C. 物理トークンを使用して、多要素認証 (MFA) でスーパー管理者の資格情報を保護します。
D. 資格情報がインターネット経由で送信されないように、プライベート接続を使用してスーパー管理者アカウントを作成します。
E. スーパー管理者ユーザーに、日常業務のために非特権 ID を提供します。
Answer: (解答を表示する**)**
https://cloud.google.com/resource-manager/docs/super-admin-best-
実践#スーパー管理者アカウントの使用を控える
- セキュリティキーまたはその他の物理的な認証デバイスを使用して2段階認証を強制する
- スーパー管理者に別のログインを必要とする別のアカウントを与える

最新問題**: 61**
組織はPCIデータセキュリティ基準（PCI DSS）に準拠する必要があります。監査に備えるには、Google Cloud ランディングゾーンのIaaS（Infrastructure as a Service）レベルで逸脱を検出する必要があります。
何をすべきでしょうか?
A. 支払いに関連するすべてのデータタイプを網羅するデータプロファイルを作成します。Google Cloud Sensitive Data Protection でデータ検出とリスク分析ジョブを構成し、検出結果を分析します。
B. Google Cloud コンプライアンス レポート マネージャーを使用して、PCI DSS レポートの最新バージョンをダウンロードしてください。レポートを分析して、逸脱を検出してください。

C. Google Cloud 組織内に Assured Workloads フォルダを作成します。既存のプロジェクトをこのフォルダに移行し、PCI DSS の逸脱を監視します。
D. Security Command Center Premium を有効化します。コンプライアンス監視製品を使用して、PCI DSS に準拠していない可能性のある検出結果をフィルタリングします。
Answer: D (メーッセージを残す)
Google Cloud 内のインフラストラクチャ アズ ア サービス (IaaS) レベルでペイメント カード業界データ セキュリティ基準 (PCI DSS) への準拠を確保するには、コンプライアンス要件からの逸脱を検出できる継続的なモニタリングおよび評価ツールが不可欠です。
* オプション A: Google Cloud の機密データ保護でデータ プロファイルを作成し、データ検出ジョブを構成することで、機密データの識別と分析に重点を置いていますが、インフラストラクチャのコンプライアンス監視には直接対応していません。
* オプション B: コンプライアンス レポート マネージャーから最新の PCI DSS レポートをダウンロードすると、静的なコンプライアンス レポートが提供されますが、特定の環境内での逸脱をリアルタイムで検出することはできません。
* オプション C: Assured Workloads を利用すると、特定のコンプライアンス要件を満たす環境を作成するのに役立ちますが、既存のプロジェクトをそのようなフォルダーに移行しても、逸脱は積極的に検出されません。主に、新しいワークロードが事前定義されたポリシーに準拠していることを確認します。
* オプション D: Security Command Center (SCC) Premium を有効化し、コンプライアンス モニタリング機能を活用することで、PCI DSS 要件に照らして Google Cloud 環境を継続的に評価できます。SCC は、構成ミス、脆弱性、コンプライアンス違反をリアルタイムで特定し、問題に迅速に対処するための実用的な分析情報を提供します。
したがって、オプション D は、PCI DSS 監査に備えて IaaS レベルでの逸脱を検出する最も効果的なアプローチです。
参考文献:
* セキュリティコマンドセンターの概要
* セキュリティコマンドセンターコンプライアンス監視

最新問題**: 62**
Compute Engine でホストされるウェブアプリケーションをデプロイしています。ビジネス要件により、アプリケーションログは12年間保存され、データは欧州域内に保管されることが義務付けられています。オーバー

ヘッドを最小限に抑え、費用対効果の高いストレージソリューションを実装したいと考えています。どうすればよいでしょうか？
A. EUROPE-WEST1 リージョンにログを保存するための Cloud Storage バケットを作成します。アプリケーションコードを変更して、ログをバケットに直接送信し、効率性を高めます。
B. Google Cloud のオペレーション スイートの Cloud Logging エージェントを使用して、12 年間のカスタム保持期間でアプリケーション ログを EUROPE-WEST1 リージョンのカスタム ログバケットに送信するように Compute Engine インスタンスを構成します。
C. Pub/Sub トピックを使用して、アプリケーション ログを EUROPE-WEST1 リージョンの Cloud Storage バケットに転送します。
D. EUROPE-WEST1 リージョンの Google Cloud オペレーション スイートのログバケットに 12 年間のカスタム保持ポリシーを構成します。
Answer: (解答を表示する**)**
https://youtu.be/MI4iG2GIZMA

最新問題**: 63**
チームは、特定の Compute Engine 仮想マシンインスタンスから指定された Cloud Storage バケットへのデータ転送を認証するためにサービスアカウントを使用しています。エンジニアが誤ってサービスアカウントを削除してしまい、アプリケーションの機能が停止してしまいました。セキュリティを損なうことなく、できるだけ早くアプリケーションを復旧したいと考えています。
何をすべきでしょうか?
A. Cloud Storage バケットの認証を一時的に無効にします。
B. undelete コマンドを使用して、削除されたサービス アカウントを回復します。
C. 削除されたサービス アカウントと同じ名前で新しいサービス アカウントを作成します。
D. 別の既存のサービス アカウントの権限を更新し、その資格情報をアプリケーションに提供します。
Answer: B (メーッセージを残す**)**
* 目的: データ転送に使用された削除されたサービス アカウントをすばやく回復します。
* 解決策: gcloud コマンドライン ツールで使用可能な undelete コマンドを使用して、サービス アカウントを回復します。
* 手順:
* ステップ 1: Google Cloud Console で Cloud Shell を開きます。
* 手順 2: 削除されたサービス アカウントを一覧表示するには、次のコマンドを実行します。
gcloud iam サービスアカウントリスト --filter="削除済み: true"
* ステップ 3: 削除されたサービス アカウントの名前と ID を特定します。
* ステップ 4: undelete コマンドを使用してサービス アカウントを回復します。
gcloud iam service-accounts undelete [SERVICE_ACCOUNT_ID]
* ステップ 5: サービス アカウントが復元されたことを確認し、必要な権限を再割り当てします。
undelete コマンドを使用すると、セキュリティを損なうことなく、サービス アカウントをすばやく復元し、アプリケーションの機能を再開できます。
参考文献:
* 削除されたサービスアカウントの復元

* gcloud iam サービスアカウントの削除取り消し

最新問題: **64**
アプリケーションは、ビルド時または実行時に「シークレット」と呼ばれる小さな機密データへのアクセスを必要とすることがよくあります。GCP 上でこれらのシークレットを管理する管理者は、GCP プロジェクト内で「誰が、どこで、いつ、何をしたか」を追跡したいと考えています。
管理者が探している情報を提供するログ ストリームはどれですか (2 つ選択してください)。
A. 管理アクティビティログ
B. システムイベントログ
C. データアクセスログ
D. VPC フローログ
E. エージェントログ
Answer: A,C (メーッセージを残す**)**
GCPプロジェクト内で「誰が、どこで、いつ、何をしたか」を追跡するには、管理者は管理アクティビティログとデータアクセスログに重点を置く必要があります。これら2つのログストリームがなぜ重要なのか、以下に詳しく説明します。
管理者アクティビティログ:
これらのログには、Google Cloud リソースで実行された管理アクションが記録されます。これには、リソースの作成、変更、削除などのアクションが含まれます。
管理アクティビティ ログには、アクションを実行したユーザー、影響を受けたリソース、実行されたアクション、およびタイムスタンプに関する詳細情報が提供されます。
データアクセスログ:
これらのログには、Google Cloud サービス内のデータの読み取りおよび書き込み操作が記録されます。これには、データベースやストレージバケットなどに保存されているデータへのアクセスや変更などのアクションが含まれます。
データ アクセス ログは、ユーザーとサービスによる機密データへのアクセス パターンを追跡するのに役立ち、誰がいつどのデータにアクセスしたかに関する分析情報を提供します。
ログを有効にしてアクセスする手順:
Google Cloud Console に移動します。
左側のメニューの「ログイン」に移動します。
まだ有効になっていない場合は、管理アクティビティ ログとデータ アクセス ログを有効にします。
ログ エクスプローラーを使用して、要件に基づいて特定のログをフィルタリングして表示します。
管理アクティビティ ログとデータ アクセス ログの両方を監視することで、管理者は GCP リソースとデータに対して実行されたアクションを包括的に把握でき、堅牢なセキュリティとコンプライアンスの追跡を確保できます。
参照：
Google Cloud Logging ドキュメント
監査ログの概要

最新問題: **65**
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。チームでは、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、最小権限の原則を遵守したいと考えています。
どのオプションがチームの要件を満たしていますか?
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認証情報なしでバケットから読み取ることができる 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 インスタンス上のアプリケーションの構成にサービス アカウント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 キーを使用してデータを復号できるようにします。
Answer: C (メーッセージを残す**)**
説明
環境変数 GOOGLE_APPLICATION_CREDENTIALS が設定されている場合、ADC はその変数が指すサービス アカウントキーまたは構成ファイルを使用します。環境変数 GOOGLE_APPLICATION_CREDENTIALS が設定されていない場合、ADC はコードを実行しているリソースに関連付けられているサービスアカウントを使用しま
す。https://cloud.google.com/docs/authentication/production#passing_the_path_to_the_service_account_key_in

最新問題: **66**
あなたは会社のセキュリティ管理者です。Google が推奨するベスト プラクティスに従い、ドメイン制限付き共有の組織ポリシーを実装し、必要なドメインのみがプロジェクトにアクセスできるようにしました。ところが、エンジニアリング チームから、組織ドメイン外の外部パートナーのユーザーにプロジェクト内のリソースへのアクセスを許可できないという報告を受けました。規定のベスト プラクティスに従いながら、パートナーのドメインに対して例外を設定するにはどうすればよいでしょうか。
A. ドメイン制限共有組織ポリシーを無効にします。ポリシー値を 「すべて許可」に設定します。
B. ドメイン制限共有の組織ポリシーをオフにします。Google の Identity and Access Management（IAM）サービスを使用して、外部パートナーに必要な権限を付与します。
C. ドメイン制限共有の組織ポリシーをオフにします。各パートナーの Google Workspace 顧客 ID を Google グループに追加し、その Google グループを組織ポリシーの例外として追加してから、ポリシーを再度オンにします。
D. ドメイン制限共有の組織ポリシーをオフにします。ポリシーの値を 「カスタム」に設定します。各外部パートナーの Cloud Identity または Google Workspace の顧客 ID を組織ポリシーの例外として追加し、ポリシーを再度オンにします。
Answer: D (メーッセージを残す**)**
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy ドメイン制限制約はリスト制約の一種です。Google Workspace の

お客様 ID は、ドメイン制限制約の allowed_values リストに追加したり、リストから削除したりできます。ドメイン制限制約では拒否値はサポートされておらず、deny_values リストに ID が含まれている組織ポリシーを保存することはできません。
allowed_values にリストされている Google Workspace アカウントに関連付けられているすべてのドメインは、組織のポリシーによって許可されます。それ以外のドメインは、組織のポリシーによって拒否されます。

最新問題**: 67**
ある企業は、Google Cloud Platform にアプリケーションをデプロイしています。会社のポリシーでは、少なくとも 2 つの地理的な場所にデータを自動的に複製できるソリューションを使用して、長期データを保存する必要があります。
どのストレージ ソリューションの使用が許可されていますか?
A. クラウド ビッグテーブル
B. クラウド BigQuery
C. Compute Engine SSD ディスク
D. Compute Engine 永続ディスク
Answer: A (メーッセージを残す**)**
Cloud Bigtableは、大規模な分析および運用ワークロードに対応するために設計されたフルマネージドNoSQLデータベースサービスです。その主要機能の一つは、複数の地理的な場所にデータを自動的に複製し、高い可用性と復元力を確保することです。以下に詳細を説明します。
レプリケーション :Cloud Bigtable は、異なる地理的リージョンにまたがるマルチクラスタ ルーティングとレプリケーションをサポートしています。つまり、データはリージョン内の複数のゾーン、あるいはリージョンをまたがって複製され、地理的な冗長性が確保されます。
自動処理 :Bigtableは一度設定すれば、手動操作を必要とせずにレプリケーションを自動的に管理します。これは、少なくとも2つの地理的な場所への自動レプリケーションを必要とする長期データストレージに関する同社のポリシーに沿ったものです。
ユースケースの適合性: Bigtable は、大量のデータへの低レイテンシのアクセスを必要とするアプリケーションに最適であり、分析アプリケーション、IoT、金融データ処理などのさまざまなユースケースに適しています。
設定 :レプリケーションの設定には、複数のゾーンにインスタンスを作成し、それらをデータ複製するように設定する作業が含まれます。Google Cloud の管理インターフェースと API を活用すれば、設定と監視が簡単に行えます。
参照：
Google Cloud Bigtable ドキュメント
Google Cloud Storage オプション

最新問題**: 68**
会社のストレージチームは、特定のGoogle Cloudプロジェクト内のすべての製品イメージを管理しています。管理を維持するために、このプロジェクトのCloud Storageへのアクセスを分離し、ストレージチームがプロジェクトレベルで制限を管理できるようにする必要があります。また、会社のコンピュータのみを使用するように制限する必要があります。どうすればよいでしょうか？

A. 組織レベルのファイアウォール ルールを適用し、Cloud Storage へのすべてのトラフィックをブロックします。プロジェクト内のストレージ チームが使用する特定のサービス アカウントに対しては例外を作成します。
B. 組織全体のサービス境界をすべてのプロジェクトで確立することで、VPC Service Controls を実装します。IP アドレス範囲に基づいて Cloud Storage へのアクセスを制限する上り（内向き）ルールと下り（外向き）ルールを設定します。
C. コンテキストアウェアアクセスを使用します。必要なコンテキストを定義するアクセスレベルを作成します。これを組織ポリシーとしてプロジェクトレベルで適用し、そのコンテキストに基づいて Cloud Storage へのアクセスを制限します。
D. ストレージ チームのプロジェクト内でプロジェクト レベルで Identity and Access Management (IAM) ロールを使用します。プロジェクトの Cloud Storage リソースに対するきめ細かな権限をストレージ チームに付与します。
Answer: C (メーッセージを残す**)**
重要な要件は、クライアントデバイス（つまり「企業内コンピュータ」）に基づいてアクセスを制限することです。コンテキストアウェアアクセス（CAA）は、デバイスのセキュリティステータスやIPアドレスなどのコンテキスト要因に基づいてアクセスを制限するように設計されたGoogle Cloud専用のツールです。
コンテキスト制限: コンテキスト認識アクセスを使用すると、デバイス ポリシーのコンプライアンス、オペレーティング システム、IP アドレスの範囲などの属性に基づいてアクセス レベルを定義できます。これにより、「企業のコンピューター」の要件に対応できます。
分離と制御: アクセス レベルは、プロジェクト レベル (またはフォルダ/組織レベル) で適用された組織ポリシーを通じて適用され、このプロジェクトの Cloud Storage へのアクセスを分離し、特定のリソース (Cloud Storage) へのアクセスを制限するという要件を満たします。
VPC Service Controls（VPC SC）オプションB）は、プロジェクトの分離とデータ流出防止に優れていますが、主なアクセス制限メカニズムはIPアドレス範囲に基づいており、きめ細かなデバイスセキュリティ体制とユーザーIDの組み合わせに基づいていません。そのため、デバイス固有の適用にはCAAの方がより正確なツールとなります。また、エンドユーザーアクセスにIPアドレスに基づいてVPC SCの上り（内向き）/下り（外向き）を適用することは、CAAよりも複雑で柔軟性に欠ける可能性があります。
IAM (オプション D) は、リソースにアクセスできるユーザー (ID) のみを制御し、どこからどのように (コンテキスト) アクセスするかは制御しません。
抜粋:
「コンテキストアウェア アクセス（CAA）は、Google Workspace または Cloud Identity と統合され、ユーザーの位置情報、デバイスのセキュリティ ステータス、IP アドレスなどのコンテキストに基づいて、Google Cloud リソースへのきめ細かなアクセス制御を実現します。」（出典7.1）
Cloud Storage などの Google Cloud リソースに CAA を適用するには、必要なコンテキスト（企業管理デバイスのみなど）を定義するアクセスレベルを作成し、組織ポリシーの制約（例：
プロジェクト レベルで、iam.allowedServices などのサービス属性を明示的に許可する必要があります。(出典7.2)
CAAを使用すると、デバイスのセキュリティ状況に基づいてアクセスを制限できます。これは、セキュリティを強化するための重要な要件です。

企業コンピュータへのアクセス」（出典.3）

最新問題: **69**
あなたの組織では、サードパーティ企業向けに金融サービスアプリケーションを Compute Engine インスタンス上でホストしています。このアプリケーションを利用するサードパーティ企業のサーバーも、別の Google Cloud 組織内の Compute Engine 上で実行されています。これらの Compute Engine インスタンス間に安全なネットワーク接続を構成する必要があります。以下の要件があります。
ネットワーク接続は暗号化されている必要があります。
サーバー間の通信はプライベート IP アドレス経由で行う必要があります。
何をすべきでしょうか?
A. 組織の VPC ネットワークと、VPC ファイアウォール ルールによって制御されるサードパーティのネットワーク間の Cloud VPN 接続を構成します。
B. 組織の VPC ネットワークと、VPC ファイアウォール ルールによって制御されるサードパーティのネットワーク間の VPC ピアリング接続を構成します。
C. Compute Engine インスタンスの周囲に VPC Service Controls 境界を設定し、アクセスレベルを介してサードパーティにアクセスを提供します。
D. Compute Engine でホストされるアプリケーションを API として公開し、サードパーティのみにアクセスを許可する TLS で暗号化された Apigee プロキシを構成します。
Answer: (解答を表示する**)**
説明
Google は、Google または Google の委託を受けていない物理的な境界外にデータが移動する場合、1 つ以上のネットワーク レイヤで転送中のデータを暗号化し、認証します。VPC ネットワーク内およびピアリングされた VPC ネットワーク内のすべての VM 間トラフィックは暗号化されます。https://cloud.google.com/docs/security/encryption-in-transit#cio-level_summary

最新問題: **70**
Google Cloud における会社の ID 管理は、あなたに責任があります。会社では全ユーザーに 2 段階認証プロセス（2SV）を適用しています。ユーザーのアクセスをリセットする必要があるのですが、ユーザーは 2 つ目の要素を失くしてしまいました。
2SV。リスクを最小限に抑えたい場合、どうすればいいでしょうか？
A. Google 管理コンソールで適切なユーザー アカウントを選択し、ユーザーがログインできるようにバックアップ コードを生成します。ユーザーに 2 番目の要素を更新するよう依頼します。
B. Google 管理コンソールで、全ユーザーに対して 2 段階認証の要件を一時的に無効にします。ユーザーにログインして、新しい 2 段階認証要素をアカウントに追加するよう依頼します。その後、全ユーザーに対して 2 段階認証の要件を再度有効にします。
C. Google 管理コンソールで適切なユーザー アカウントを選択し、このアカウントの 2SV を一時的に無効にします。ユーザーに 2 番目の要素を更新するよう依頼してから、このアカウントの 2SV を再度有効にします。
D. Google 管理コンソールで、特権管理者アカウントを使用してユーザー アカウントの認証情報をリセットします。

最初のログイン後にユーザーに資格情報を更新するよう依頼します。
Answer: (解答を表示する**)**
ユーザーが 2 段階認証 (2SV) の 2 番目の要素を紛失した場合、バックアップ コードを生成することで、最小限のリスクでアクセスを回復できるようにすることができます。
* バックアップコードを生成する (A):
* Google 管理コンソールで、ユーザーのアカウント設定に移動します。
* ユーザーのバックアップコードを生成します。このコードを使用すると、通常の2要素認証にアクセスできない場合でもサインインできます。
* ユーザーにバックアップ コードを使用してログインし、アカウント設定で 2 番目の要素を更新するように指示します。
この方法により、影響を受けるユーザーのアクセスのみが一時的に調整され、全体的なセキュリティ ポリシーを維持しながらリスクが最小限に抑えられます。
参考文献
* Google 管理コンソールの 2 段階認証プロセスに関するドキュメント

最新問題**: 71**
ある企業は、ミッションクリティカルなアプリケーションのコンテナ イメージで Google Kubernetes Engine（GKE）を使用しています。この企業は、イメージをスキャンして既知のセキュリティ問題を検出し、Google Cloud の外部に公開することなく、レポートをセキュリティ チームと安全に共有したいと考えています。
何をすべきでしょうか?
A. 1. Security Command Center プレミアム レベルで Container Threat Detection を有効にします。
* 2. サポートされているバージョンの GKE ではないすべてのクラスターを、可能な限り最新の GKE バージョンにアップグレードします。
* 3. セキュリティコマンドセンターから結果を表示して共有する
B. * 1. Cloud Build のオープンソース ツールを使用してイメージをスキャンします。
* 2. gsutil を使用して、Cloud Storage 内の一般公開バケットにレポートをアップロードする
* 3. スキャンレポートのリンクをセキュリティ部門と共有します。
C. * 1. Artifact Registry 設定で脆弱性スキャンを有効にします。
* 2. Cloud Buildを使用してイメージをビルドする
* 3. 自動スキャンのためにイメージを Artifact Registry にプッシュします。
* 4. Artifact Registry でレポートを表示します。
D. * 1. GitHub サブスクリプションを取得します。
* 2. Cloud Buildでイメージをビルドし、GitHubに保存して自動スキャンする
* 3. GitHubからレポートをダウンロードし、セキュリティチームと共有する
Answer: (解答を表示する**)**
説明
「このサービスは、すべての変更とリモート アクセスの試行を評価し、ランタイム攻撃をほぼリアルタイムで検出します。」:

https://cloud.google.com/security-command-center/docs/concepts-container-threat-detection-overview これは、イメージ内の既知のセキュリティ脆弱性とは何の関係もありません。

最新問題: **72**
顧客はアプリケーションを App Engine にデプロイし、Open Web Application Security Project (OWASP) の脆弱性をチェックする必要があります。
これを実現するにはどのサービスを使用すればよいでしょうか?
A. クラウドアーマー
B. Google Cloud 監査ログ
C. クラウドセキュリティスキャナー
D. 大統領セキュリティ
Answer: C (メーッセージを残す**)**
https://cloud.google.com/security-scanner/

最新問題: **73**
Google Cloud 内でアプリケーション データ（転送中データ、使用中データ、保存中データを含む）のエンドツーエンド暗号化を必要とするクライアントとコンサルティングを行っています。これを実現するには、どのオプションを利用すべきですか 2 つ選択してください）。
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. 機密コンピューティングとIstio
E. クライアント側暗号化
Answer: D,E (メーッセージを残す**)**
WAN経由のデータ暗号化について追加の要件があるGoogle Cloudのお客様は、ユーザーからアプリケーションへ、または仮想マシンから仮想マシンへデータを移動する際に、追加の保護を実装できます。これらの保護には、IPSecトンネル、Gmail S/MIME、マネージドSSL証明書、Istioが含まれます。https://cloud.google.com/docs/security/encryption-in-transit

最新問題: **74**
チームは、特定の Compute Engine 仮想マシンインスタンスから指定された Cloud Storage バケットへのデータ転送を認証するためにサービスアカウントを使用しています。エンジニアが誤ってサービスアカウントを削除してしまい、アプリケーションの機能が停止してしまいました。セキュリティを損なうことなく、できるだけ早くアプリケーションを復旧したいと考えています。
何をすべきでしょうか?
A. Cloud Storage バケットの認証を一時的に無効にします。
B. undelete コマンドを使用して、削除されたサービス アカウントを回復します。
C. 削除されたサービス アカウントと同じ名前で新しいサービス アカウントを作成します。
D. 別の既存のサービス アカウントの権限を更新し、その資格情報をアプリケーションに提供します。
Answer: B (メーッセージを残す**)**

https://cloud.google.com/iam/docs/creating-managing-service-
アカウント#サービスアカウントの削除の取り消し

最新問題: **75**
あなたの会社は、顧客の年齢層に応じて信用スコアの向上を支援するために、どのような商品を開発できるかを検討したいと考えています。そのためには、会社の銀行アプリのユーザー情報と、サードパーティから取得した顧客の信用スコアデータを統合する必要があります。この生データを使用することでこのタスクは完了しますが、機密データが露出し、新しいシステムに伝播される可能性があります。
このリスクに対処するには、データベース全体の参照整合性を維持しながら、Cloud Data Loss Prevention による匿名化とトークン化を行う必要があります。これらの要件を満たすには、どの暗号トークン形式を使用すべきでしょうか？
A. 安全なキーベースのハッシュ
B. 決定論的暗号化
C. 暗号ハッシュ
D. フォーマット保持暗号化
Answer: (解答を表示する**)**

最新問題: **76**
Google Cloud に規制対象のワークロードをデプロイしています。規制には、データの所在地とデータアクセスに関する要件が定められています。また、サポートはデータが存在する場所と同じ地理的な場所から提供される必要があります。
何をすべきでしょうか?
A. Assured Workloads をデプロイします。
B. アクセスの透明性のログ記録を有効にします。
C. データ所在地要件で許可されたリージョンにのみリソースを展開します
D. データ アクセス ログとアクセスの透明性ログを使用して、ユーザーが別のリージョンのデータにアクセスしていないことを確認します。
Answer: A (メーッセージを残す**)**

最新問題: **77**

セキュリティチームは、ユーザー管理キーが適切に管理されず、侵害されるリスクを軽減したいと考えています。そのためには、開発者が組織内のプロジェクトでユーザー管理サービスアカウントキーを作成できないようにする必要があります。どのように対策を講じるべきでしょうか？
A. サービス アカウント キーを管理するために Secret Manager を構成します。
B. 組織ポリシーを有効にして、サービス アカウントの作成を無効にします。
C. 組織ポリシーを有効にして、サービス アカウント キーが作成されないようにします。
D. ユーザーから iam.serviceAccounts.getAccessToken 権限を削除します。
Answer: C (メーッセージを残す**)**
https://cloud.google.com/iam/docs/サービスアカウントキーの管理に関するベストプラクティス
サービス アカウント キーの不要な使用を防ぐには、組織のポリシー制約を使用します。
組織のリソース階層のルートで、 ₩サービス アカウント キーの作成を無効にする」および ₩サービス アカウント キーのアップロードを無効にする」制約を適用して、サービス アカウント キーが許可されないデフォルトを設定します。
必要に応じて、選択したプロジェクトの制約の 1 つをオーバーライドして、サービス アカウント キーの作成またはアップロードを再度有効にします。

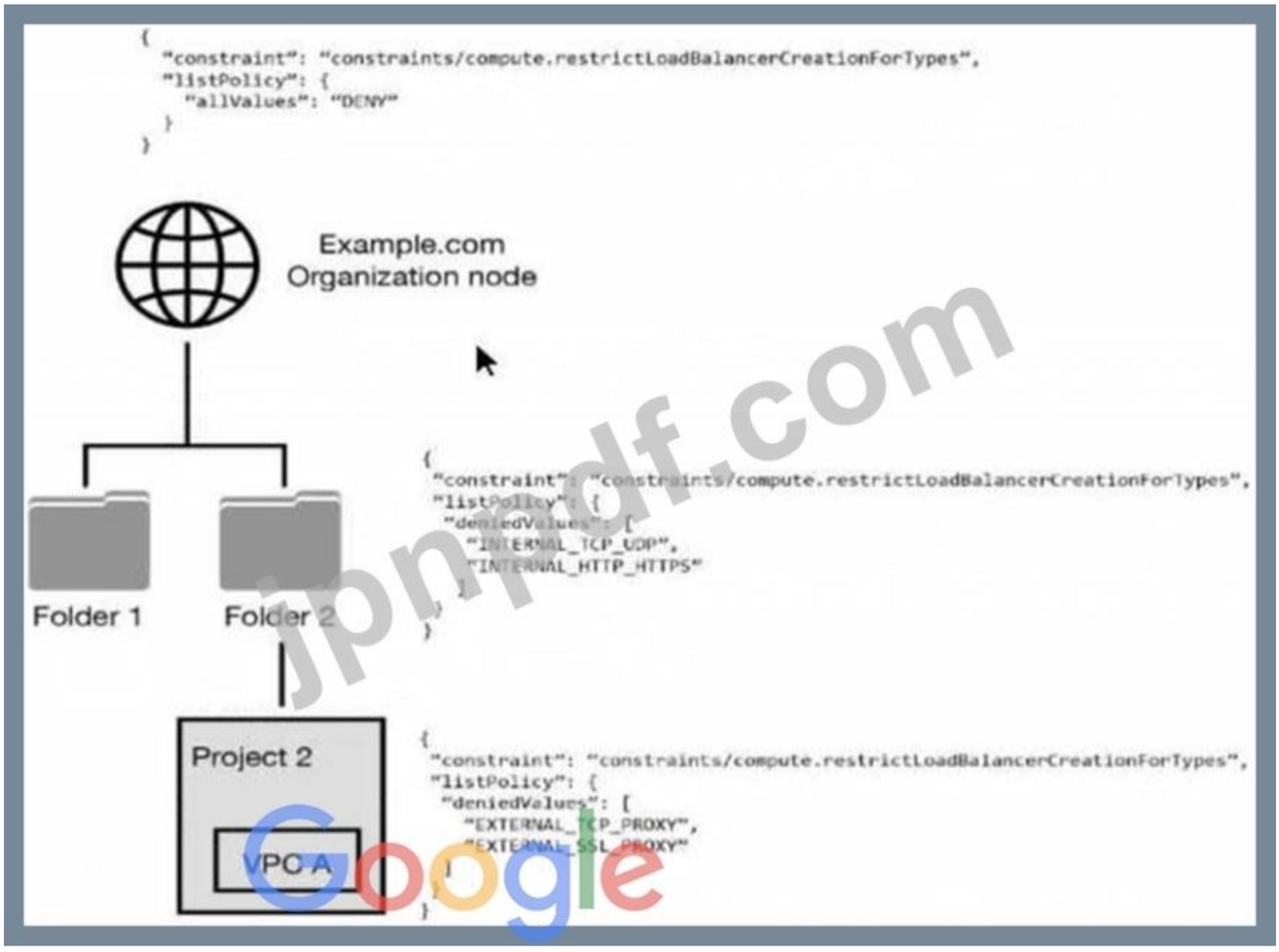
最新問題**: 78**
会社では、多数のコンテナ化されたアプリケーションを GKE にデプロイしています。既存の CI/CD パイプラインでは、Cloud Build を使用してコンテナ イメージを作成し、そのイメージを Artifact Registry に転送してから、GKE にデプロイしています。脆弱性スキャンに合格し、特定の企業ポリシーを満たしているイメージのみがデプロイされるようにする必要があります。プロセスを自動化し、既存の CI/CD パイプラインに統合する必要があります。どうすればよいでしょうか?
A. サードパーティの脆弱性スキャンツールを使用するカスタムスクリプトを Cloud Build パイプラインに実装し、脆弱性が見つかった場合はビルドを失敗させます。
B. 特定の信頼できる Artifact Registry リポジトリからのイメージのみを使用するように GKE を構成します。このリポジトリにプッシュする前に、すべてのイメージを手動で検査します。
C. Binary Authorization でポリシーを構成して、Artifact Analysis の脆弱性スキャンを使用し、スキャンに合格したイメージのみが GKE クラスタにデプロイされるようにします。
D. アーティファクト分析の脆弱性スキャンを有効にし、アーティファクトレジストリ内のイメージを定期的にスキャンします。展開前に脆弱性要件を満たさないイメージを削除します。
Answer: C (メーッセージを残す**)**
問題を解決するには、脆弱性スキャンに合格し、企業ポリシーを満たしているイメージだけが GKE にデプロイされるようにする必要があります。このプロセスは自動化され、既存の CI/CD パイプラインに統合されています。Binary Authorization: この Google Cloud サービスは、Google Kubernetes Engine (GKE)、Cloud Run、その他のデプロイ可能なプラットフォームでイメージを実行する前に、イメージにデプロイ ポリシーを適用するために特別に構築されています。ポリシーに準拠していないイメージのデプロイを防ぐポリシー ゲートとして機能します。抜粋リファレンス: Binary Authorization は、信頼できるコンテナ イメージだけが Google Kubernetes Engine (GKE)、Cloud Run、Anthos クラスタにデプロイされるようにする、デプロイ時のセキュリティ制御です」および Binary Authorization を使用すると、信頼できる機関によるイメージの署名を要求し、デ

プロイ中に検証ポリシーを適用できます」(Google Cloud ドキュメント: Binary Authorization の概要」 - https://cloudgooglecom/binary-authorization/docs/overview) Artifact Analysis (Container Analysis の一部): Artifact Analysis (Container Analysis を含む) は、Artifact Registry に保存されているコンテナ イメージの脆弱性スキャン機能を提供します。脆弱性に関する検出結果とメタデータを生成します。抜粋リファレンス: Container Analysis は、イメージをスキャンして既知の脆弱性を検出し、そのメタデータを提供するサービスです。(Google Cloud ドキュメント: 概要 | Container Analysis」 - https://cloudgooglecom/container-analysis/docs/overview) Binary Authorization は、Artifact Analysis (またはその他の認証者) と統合して、デプロイ ポリシーの一部として脆弱性スキャンの結果を確認するように構成できます。統合と自動化: Binary Authorization ポリシーでは、デプロイ前に認証を要求することができます。認証は、イメージが特定の基準を満たしていることを確認します (例: 脆弱性スキャンに合格した、承認された CI/CD プロセスによって署名されている、企業ポリシーに準拠している)。Cloud Build は、脆弱性スキャンが成功した後にこれらの認証を生成するように構成できます (Artifact Analysis を使用)。これにより、プロセスが完全に自動化され、CI/CD パイプラインに直接統合されます。抜粋参照: Binary Authorization では、要件を適用するポリシーを作成します。ポリシーでは、デプロイを管理するルールを定義します。たとえば、ポリシーでは、デプロイ前にすべてのイメージが信頼できる認証局によって署名されていることを要求できます。(Google Cloud ドキュメント: Binary Authorization他のオプションを評価してみましょう。
A Cloud Build のカスタム スクリプト ビルドを失敗させる: ビルド中にスキャンを実行するのは良い方法ですが (シフトレフト セキュリティ)、ビルドを失敗させるとイメージがプッシュされなくなるだけです。開発者や自動プロセスが Artifact Registry に既に存在する可能性のある古いイメージや非準拠のイメージを手動でデプロイしたり、ビルド システムをバイパスしたりすることを防ぐことはできません。強制はデプロイ時に行う必要があります。B 特定の信頼できる Artifact Registry リポジトリのイメージのみを使用するように GKE を構成します。すべてのイメージを手動で検査する: イメージを手動で検査することは自動化されておらず、 多数のコンテナ化されたアプリケーション」には拡張できません。また、脆弱性スキャンの結果や企業ポリシーをプログラムで強制することもできません。D Artificial Analysis の脆弱性スキャンを有効にし、イメージを定期的にスキャンします。デプロイ前に、基準を満たしていないイメージを削除します: これは、重要なスキャンと修復について説明します。ただし、これはプロアクティブな強制 (デプロイが許可されているイメージのみ」) ではなく、リアクティブなアプローチ (すべてのイメージを削除する」) です。非準拠のイメージが削除される前にデプロイされる可能性がある時間はまだあります。Binary Authorization は強制ゲートです。したがって、Binaryアーティファクト分析と統合されたポリシー または結果に基づいて証明書を要求するポリシー）による承認は、脆弱性スキャンと企業コンプライアンスに基づいて導入ポリシーを適用するための、最も堅牢で自動化された Google 推奨のソリューションです。

最新問題**: 79**
Compute Engine ディスク上のデータを、Cloud Key Management Service（KMS）で管理される鍵を使用して保存時に暗号化する必要があります。これらの鍵に対する Cloud Identity and Access Management（IAM）権限は、すべての鍵に対して同じ権限を持つ必要があるため、グループ化して管理する必要があります。
何をすべきでしょうか?
A. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーリングレベルで管理します。

B. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。キーレベルでIAM権限を管理します。
C. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーレベルで管理します。
D. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。IAM権限はキーリングレベルで管理します。
Answer: C (メーッセージを残す)

最新問題: **80**
以下のリソース階層があります。階層内の各ノードには、図に示すように組織ポリシーが適用されます。VPCAで拒否されるロードバランサーの種類はどれですか？



A. 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。
B. 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。
C. EXTERNAL_TCP_PROXY、EXTERNAL_SSL_PROXY はプロジェクトのポリシーに従って拒否されます。
D. INTERNAL_TCP_UDP、INTERNAL_HTTP_HTTPS はフォルダーのポリシーに従って拒否されます。
Answer: A (メーッセージを残す)
https://cloud.google.com/load-balancing/docs/org-policy-constraints#gcloud

最新問題: **81**
チームは、オンプレミスの Active Directory サービスから GCP IAM 権限を一元管理したいと考えています。
チームは、AD グループのメンバーシップごとに権限を管理したいと考えています。
これらの要件を満たすためにチームは何をすべきでしょうか?
A. グループを同期するように Cloud Directory Sync を設定し、グループに IAM 権限を設定します。
B. SAML 2.0 シングル サインオン (SSO) を設定し、グループに IAM 権限を割り当てます。
C. Cloud Identity and Access Management API を使用して、Active Directory からグループと IAM 権限を作成します。
D. Admin SDK を使用してグループを作成し、Active Directory から IAM 権限を割り当てます。
Answer: A (メーッセージを残す**)**
説明
既存のID管理システムを引き続き使用するには、ADとGCP IAMの間でIDを同期する必要があります。Google はこれを実現するために、Cloud Directory Syncというツールを提供しています。このツールは、AD内のすべてのIDを読み取り、GCP内に複製します。IDが複製されると、グループにIAM権限を適用できるようになります。その後、Googleがサービスプロバイダとして機能するようにSAMLを設定し、ADFS、またはPingやOktaなどのサードパーティツールがIDプロバイダとして機能するようにします。これにより、Googleから管理下にあるものに認証を効果的に委任できます。

最新問題: **82**
機密データの暗号鍵の管理について懸念を抱いているクライアントと連携しています。クライアントは、暗号鍵を、その鍵で暗号化するデータと同じクラウド サービス プロバイダ (CSP) に保存することを希望していません。このクライアントに推奨すべき Google Cloud 暗号化ソリューションはどれですか (2 つ選択してください)。
A. クラウド外部キーマネージャー
B. 顧客管理の暗号化キー
C. 顧客が提供する暗号化キー。
D. Google のデフォルトの暗号化
E. シークレットマネージャー
Answer: A,C (メーッセージを残す**)**

最新問題: **83**
Compute Engine 上で実行されるアプリケーションから機密性の高い設定データを保存および取得するためのソリューションを推奨するよう求められています。どのオプションを推奨すべきでしょうか？
A. クラウド キー管理サービス
B. Compute Engine ゲスト属性
C. Compute Engine カスタム メタデータ
D. シークレットマネージャー
Answer: D (メーッセージを残す**)**
説明

Secret Manager は、API キー、パスワード、証明書、その他の機密データを安全かつ便利に保管できるストレージ システムです。Secret Manager は、Google Cloud 全体のシークレットを管理、アクセス、監査するための一元的な場所と、信頼できる唯一の情報源を提供します。https://cloud.google.com/secret-manager

最新問題: **84**
ある企業は、専用サーバールームでワークロードを実行しています。これらのワークロードへのアクセスは、社内のプライベートネットワーク内からのみ行う必要があります。これらのワークロードには、Google Cloud Platform プロジェクト内の Compute Engine インスタンスから接続する必要があります。
要件を満たすために、どの 2 つのアプローチを取ることができますか? (2 つ選択してください。)
A. Cloud VPN を使用してプロジェクトを構成します。
B. 共有 VPC を使用してプロジェクトを構成します。
C. Cloud Interconnect を使用してプロジェクトを構成します。
D. VPC ピアリングを使用してプロジェクトを構成します。
E. すべての Compute Engine インスタンスをプライベート アクセスで構成します。
Answer: D,E (メーッセージを残す**)**
説明/参考資料: https://cloud.google.com/solutions/secure-data-workloads-use-cases

最新問題: **85**
企業のユーザー アカウント全体でフィッシング攻撃の数が増加していることに気付きました。
暗号署名を使用してユーザーを認証し、ログインページのURLを検証するGoogle 2段階認証（2SV）オプションを実装したいと考えています。どのGoogle 2SVオプションを使用すべきでしょうか？
A. Titan セキュリティ キー
B. Google プロンプト
C. Google 認証システムアプリ
D. クラウドHSMキー
Answer: A (メーッセージを残す**)**
https://cloud.google.com/titan-security-key
セキュリティ キーは公開キー暗号化を使用してユーザーの ID とログイン ページの URL を検証し、たとえユーザー名とパスワードを入力するよう誘導されたとしても攻撃者がアカウントにアクセスできないようにします。

最新問題: **86**
オンプレミス ネットワークからアクセスされる新しいウェブ アプリケーションを Google Cloud 上に実装しようとしています。マルウェアなどの脅威からアプリケーションを保護するには、受信トラフィックにトランスポート層セキュリティ（TLS）インターセプションを実装する必要があります。どうすればよいでしょうか？
A. セキュア Web プロキシを構成します。ロードバランサーで TLS トラフィックをオフロードし、トラフィックを検査して、Web アプリケーションに転送します。
B. 内部プロキシロードバランサーを構成します。ロードバランサーでTLSトラフィックをオフロードし、トラフィックを検査してWebアプリケーションに転送します。

C. 階層型ファイアウォールポリシーを設定します。Cloud Next Generation Firewall (NGFW) Enterprise を使用して TLS インターセプションを有効にします。
D. VPC ファイアウォールルールを設定します。Cloud Next Generation Firewall (NGFW) Enterprise を使用して TLS インターセプションを有効にします。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/secure-web-proxy/docs/tls-inspection-overview
セキュアWebプロキシは、TLSトラフィックを傍受、検査、そしてセキュリティポリシーの適用を可能にするTLSインスペクションサービスを提供します。このアプローチにより、受信トラフィックはアプリケーションに到達する前に、脅威がないか徹底的に検査されます。

最新問題**: 87**
組織では、ターゲットを絞ったマーケティングキャンペーンに向けた顧客行動を予測するための高度な機械学習（ML）モデルを開発しています。トレーニングに使用するBigQueryデータセットには、機密性の高い個人情報が含まれています。AI/MLパイプラインのセキュリティ管理を設計する必要があります。モデルのライフサイクル全体を通じてデータのプライバシーを維持し、トレーニングプロセスで個人データが使用されないようにする必要があります。さらに、データセットへのアクセスを承認された一部のユーザーのみに制限する必要があります。どうすればよいでしょうか？
A. パイプラインの顧客管理の暗号化キー (CMEK) を使用して、保存時の暗号化を実装します。BigQuery へのアクセスを制御するために、厳格な Identity and Access Management (IAM) ポリシーを実装します。
B. Cloud Data Loss Prevention (DLP) API を使用してモデルのトレーニング前に機密データを匿名化し、厳格な Identity and Access Management (IAM) ポリシーを実装して BigQuery へのアクセスを制御します。
C. Identity-Aware Proxy を実装して、ユーザー ID とデバイスに基づいて BigQuery とモデルへのコンテキスト認識アクセスを強制します。
D. 使用中のデータとコードの保護を強化するために、モデルを Confidential VMs にデプロイします。BigQuery へのアクセスを制御するために、厳格な Identity and Access Management (IAM) ポリシーを実装します。
Answer: B (メーッセージを残す**)**
セキュリティとプライバシーの核となる要件は、トレーニングプロセスにおける個人データの使用を防ぐことであり、そのためには匿名化が必要です。クラウドデータ損失防止（DLP）は、機密データ保護（SDP）とも呼ばれ、この目的に特化したGoogle Cloudツールです。二次的な要件であるアクセス制限は、IAMによって処理されます。
抜粋:
「機密データ保護（SDP）...匿名化により、データの有用性を維持しながらデータリスクを軽減するためにデータを変換できます。」（出典4）
暗号化などの匿名化技術は、データ内の生の機密識別子を難読化します。これらの技術により、結合や分析のためのデータの有用性を維持しながら、データの取り扱いリスクを軽減できます。（出典1）
「DLP は、データ内の機密要素や不要なコンテンツを分類し、匿名化するツールを提供します...

モデルをトレーニングする前に、データから機密要素を見つけて削除します。」(出典 1.4) IAM ポリシーは、「データセットへのアクセスを許可された一部のユーザーのみに制限する」という要件を満たす標準的なメカニズムです。オプション B は、プライバシー (DLP 匿名化) のための正確な技術的ソリューションと必要なアクセス制御 (IAM) を組み合わせたものです。

最新問題: **88**
Google Cloud フットプリントのネットワークセグメンテーションを監査する必要があります。現在、本番環境と非本番環境の Infrastructure as a Service（IaaS）環境を運用しています。すべての VM インスタンスは、サービスアカウントのカスタマイズなしでデプロイされています。
カスタム ネットワーク内のトラフィックを観察すると、トラフィックを適切にセグメント化するためにタグベースの VPC ファイアウォール ルールが設定されているにもかかわらず、すべてのインスタンスが優先度 1000 で自由に通信できることに気付きました。この動作の最も可能性の高い理由は何でしょうか。
A. すべての VM インスタンスにそれぞれのネットワーク タグがありません。
B. すべての VM インスタンスは同じネットワーク サブネットに存在します。
C. すべての VM インスタンスは同じネットワーク ルートで構成されています。
D. VPC ファイアウォール ルールは、優先度 999 の同じサービス アカウントに基づいて、ソース/ターゲット間のトラフィックを許可しています。
E. VPC ファイアウォール ルールは、優先度 1001 の同じサービス アカウントに基づいて、ソース/ターゲット間のトラフィックを許可しています。
Answer: D (メーッセージを残す**)**
ファイアウォール ルール分析: 既存の VPC ファイアウォール ルールを分析して、同じサービス アカウントに基づいて VM インスタンス間のトラフィックを許可する可能性のあるルールを特定します。
優先度チェック :これらのルールの優先度を確認してください。優先度が1000未満（例999）のルールは、タグベースのルールよりも優先されます。
サービスアカウントの設定 :VMインスタンスはサービスアカウントをカスタマイズせずにデプロイされているため、デフォルトのサービスアカウントが使用されている可能性があります。このデフォルトのサービスアカウントを使用するインスタンス間のトラフィックを許可するファイアウォールルールは、優先度が高い場合、タグベースのルールよりも優先されます。
テストと検証 :タグベースのセグメンテーションが正しく機能するかどうかをテストするため、優先度999のルールを無効にするか、優先度を調整してください。トラフィックが意図した設定通りにセグメント化されていることを確認してください。参考 :
Google Cloud - VPC ファイアウォール ルール
Google Cloud - サービス アカウント

最新問題: **89**
あなたの会社では、現在 us-central-1 の Google Cloud ロードバランサの背後にデプロイされ、スタンダードティア ネットワークを使用するように構成されたアプリケーション インスタンス グループを運用しています。インフラストラクチャ チームは、2 つ目の Google Cloud リージョンである us-east-2 への拡張を考えてい

ます。両方のリージョンのインスタンス グループに新しいリクエストを分散するために、単一の外部 IP アドレスを設定する必要があります。
何をすべきでしょうか?
A. インスタンス グループの代わりにネットワーク エンドポイント グループを使用するようにロードバランサーのバックエンド構成を変更します。
B. プレミアム ティア ネットワークを使用するようにロードバランサーのフロントエンド構成を変更し、新しいインスタンス グループを追加します。
C. 標準層ネットワークを使用して us-east-2 に新しいロードバランサーを作成し、静的な外部 IP アドレスを割り当てます。
D. 2 つのリージョン間に Cloud VPN 接続を作成し、Google プライベート アクセスを有効にします。
Answer: B (メーッセージを残す**)**
標準レベルの LB では、バックエンドは同じリージョンに存在する必要があります。
https://cloud.google.com/load-balancing/docs/load-balancing-
概要#バックエンドリージョンとネットワーク

最新問題**: 90**
GCP リソースに直接アクセスする必要がある開発者と運用スタッフそれぞれに、Google Cloud で企業ユーザーアカウントを提供する必要があります。企業ポリシーでは、ユーザー ID をサードパーティの ID 管理プロバイダで管理し、シングル サインオンを活用することが義務付けられています。多くのユーザーが企業ドメインのメールアドレスを個人の Google アカウントに使用していることが判明したため、Google の推奨プラクティスに従って、既存の管理対象外ユーザーを管理対象アカウントに変更する必要があります。
取るべき行動は 2 つありますか? (2 つ選択してください。)
A. Google Cloud Directory Sync を使用して、ローカル ID 管理システムを Cloud Identity と同期します。
B. Google 管理コンソールを使用して、再設定用のメールアドレスに個人アカウントを使用している管理対象ユーザーを確認します。
C. 管理対象の Google アカウントにユーザーを追加し、ユーザーに個人アカウントに関連付けられているメール アドレスを変更するよう強制します。
D. 管理対象外ユーザー向け移行ツール (TTUU) を使用して、競合するアカウントを持つユーザーを見つけ、個人の Google アカウントを移行するよう依頼します。
E. 従業員全員にメールを送信し、個人の Google アカウントに会社のメール アドレスを使用しているユーザーに、個人アカウントを直ちに削除するよう依頼します。
Answer: (解答を表示する**)**
https://cloud.google.com/architecture/identity/migrating-consumer-accounts#initiating_a_transfer

最新問題**: 91**
あなたはセキュリティ チームの一員であり、プロジェクト A の Cloud Storage バケットがプロジェクト B からのみ読み取り可能であることを保証したいと考えています。また、ユーザーが正しい認証情報を持っている場合でも、ネットワーク外部の Cloud Storage バケットから Cloud Storage バケット内のデータにアクセスしたり、そのバケットにデータをコピーしたりできないようにしたいと考えています。

何をすべきでしょうか?
A. VPC Service Controls を有効にし、プロジェクト A と B で境界を作成し、Cloud Storage サービスを含めます。
B. Cloud Storage バケットでドメイン制限共有組織ポリシーとバケット ポリシーのみを有効にします。
C. 厳格なファイアウォール ルールを使用してプロジェクト A および B のネットワークでプライベート アクセスを有効にし、ネットワーク間の通信を許可します。
D. 厳格なファイアウォール ルールを使用してプロジェクト A と B のネットワーク間の VPC ピアリングを有効にし、ネットワーク間の通信を許可します。
Answer: A (メーッセージを残す**)**
目標: プロジェクト A の Cloud Storage バケットはプロジェクト B からのみ読み取り可能であることを確認し、正しい認証情報を使用しても、ネットワーク外部の Cloud Storage バケットへのデータ アクセスやコピーを防止します。
解決策: VPC Service Controls を使用してセキュリティ境界を作成します。
手順:
ステップ 1: Google Cloud Console を開きます。
ステップ 2: VPC Service Controls ページに移動します。
ステップ 3: 新しいサービス境界を作成します。
ステップ 4: プロジェクト A とプロジェクト B をサービス境界に追加します。
ステップ 5: 境界構成に Cloud Storage サービスを含めます。
ステップ 6: アクセス レベルを定義して、境界内のリソースのみが Cloud Storage バケットにアクセスできるようにします。
VPC Service Controls 境界を設定することで、定義済みのプロジェクト内にデータへのアクセスと移動を制限するセキュリティ境界を適用でき、IAM 権限を超えた追加の保護レイヤーを提供できます。
参照 :
VPC サービスコントロールの概要
VPC サービスコントロールの構成

最新問題**: 92**
組織では最近、Google Kubernetes Engine に新しいアプリケーションをデプロイしました。このアプリケーションを保護するためのソリューションをデプロイする必要があります。ソリューションの要件は次のとおりです。

スキャンは少なくとも週に1回実行する必要があります
クロスサイトスクリプティングの脆弱性を検出できる必要がある
Googleアカウントを使用して認証できる必要があります
どのソリューションを使用すべきでしょうか?
A. Google クラウド アーマー
B. Webセキュリティスキャナー
C. セキュリティヘルス分析
D. コンテナ脅威検出
Answer: (解答を表示する**)**
参照：
Web セキュリティ スキャナは、App Engine、Google Kubernetes Engine（GKE）、Compute Engine ウェブ アプリケーションのセキュリティ上の脆弱性を特定します。https://cloud.google.com/security-command-center/docs/concepts-web-security-scanner-overview

最新問題**: 93**
社内で Cloud Data Loss Prevention (DLP) API の導入が進むにつれ、コスト削減のために利用を最適化する必要があります。DLP 対象データは Cloud Storage と BigQuery に保存されます。場所とリージョンはリソース名のサフィックスとして識別されます。
どのようなコスト削減オプションを推奨すべきでしょうか?
A. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットに適切な bytesLimitPerFile 値を設定します。
B. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットの変換単位を最小限に抑えます。
C. rowsLimit と bytesLimitPerFile を使用してデータをサンプリングし、CloudStorageRegexFileSet を使用してスキャンを制限します。
D. FindingLimits と TimespanContfig を使用してデータをサンプリングし、変換単位を最小限に抑えます。
Answer: C (メーッセージを残す**)**
説明/リファレンス: https://cloud.google.com/dlp/docs/reference/rest/v2/InspectJobConfig

最新問題**: 94**
お客様は、証明機関（CA）を利用したオンプレミスの公開鍵基盤（PKI）をご利用です。多数のHTTPロードバランサのフロントエンドに証明書を発行する必要があります。多くの手動プロセスによるオンプレミスPKIへの影響を最小限に抑える必要があり、ソリューションは拡張性も備えています。
何をすべきでしょうか?
A. 証明書マネージャーを使用して、Google が管理する公開証明書を発行し、インフラストラクチャ内の HTTP ロードバランサでコードとして構成します (IaC)。
B. 証明書マネージャーを使用して、オンプレミスの PKI およびフロントエンドから発行された証明書をインポートします。
インポートにはgcloudツールを活用する

C. オンプレミス PKI システムの Google 証明機関サービス内の下位 CA を使用して、ロードバランサの証明書を発行します。
D. オンプレミスのOpenSSLベースの下位CAから発行されたPKCS12証明書を持つウェブアプリケーションを使用します。インポートにはgcloudツールを使用します。外部HTTPロードバランサの代わりに、外部TCP/UDPネットワークロードバランサを使用します。
Answer: (解答を表示する**)**
説明
このアプローチにより、既存のオンプレミスPKIインフラストラクチャを活用しながら、その影響と手動プロセスを最小限に抑えることができます。Googleの証明機関サービスに従属CAを作成することで、HTTPロードバランサのフロントエンドへの証明書発行プロセスを自動化できます。このソリューションは、ロードバランサの数が増えても適切に拡張できます。

最新問題**: 95**
管理アプリケーションは、ポートの管理対象グループ内の仮想マシン (VM) 上で実行されています
現在インターネットにアクセスできないVirtual Private Cloud（VPC）インスタンス内の5601ポート。ユーザーにポート5601のウェブインターフェースを公開し、Google認証情報による認証と認可を強制したいと考えています。
何をすべきでしょうか?
A. パブリック ネットワークに Secure Shell Access (SSH) 要塞ホストを構成し、その要塞ホストのみがポート 5601 でアプリケーションに接続できるようにします。要塞ホストをジャンプ ホストとして使用して、アプリケーションに接続します。
B. VPC ルーティングを変更し、デフォルトルートポイントをデフォルトインターネットゲートウェイに設定します。VPC ファイアウォールルールを変更し、インターネット 0.0.0.0/0 からアプリケーションインスタンスのポート 5601 へのアクセスを許可します。
C. OS ログインを有効にして要塞ホストを設定し、VPC ファイアウォールでポート 5601 への接続を許可します。Google Cloud コンソールからブラウザ内 SSH を使用して要塞ホストにログインし、その後ウェブアプリケーションにログインします。
D. Google 認証情報を使用して、Identity-Aware Proxy（IAP）保護を適用したマネージドグループを指す HTTP ロードバランシングインスタンスを設定します。VPC ファイアウォールを変更し、IAP ネットワーク範囲からのアクセスを許可します。
Answer: D (メーッセージを残す**)**

最新問題**: 96**
コンプライアンス上の理由から、組織はPCI Kubernetesの対象となるポッドが 対象となる」ノードにのみ配置されていることを確認する必要があります。これらのノードには、 対象となる」ポッドのみを配置できます。
組織はこの目的をどのように達成すべきでしょうか?
A. inscope: true というラベルの付いたノードのみを使用するように、ポッド構成に nodeSelector フィールドを追加します。

B. ラベル inscope: true を持つノード プールと、そのラベルを持つノードでのみポッドの実行を許可するポッド セキュリティ ポリシーを作成します。
C. ラベル inscope: true、効果 NoSchedule、および Pod 構成に一致する toleration を使用して、ノードに taint を配置します。
D. 名前空間「in-scope-pci」内のすべてのスコープ内ポッドを実行します。
Answer: A (メッセージを残す**)**
nodeSelectorは、ノード選択制約の最もシンプルな推奨形式です。Pod仕様にnodeSelectorフィールドを追加し、対象ノードに付与するノードラベルを指定できます。Kubernetesは、指定されたラベルを持つノードにのみPodをスケジュールします。=> https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector ポッドにはTolerationが適用されます。Tolerationにより、スケジューラは一致するtaintを持つポッドをスケジュールできます。Tolerationはスケジュールを可能にしますが、スケジュールを保証するものではありません。
スケジューラは、その機能の一部として他のパラメータも評価します。=> https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/

最新問題**: 97**
ある顧客がGoogle Cloud Platform（GCP）上で分析ワークロードを実行しており、Compute EngineインスタンスがCloud Storageに保存されているデータにアクセスしています。あなたのチームは、このワークロードがインターネットにアクセスできないように、また、このワークロードが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。
これらの要件を満たすためにチームが使用すべき 2 つの戦略はどれですか? (2 つ選択してください。)
A. Compute Engine クラスタが別のサブネット上で実行されていることを確認します。
B. Cloud NAT ゲートウェイを構成します。
C. Compute Engine サブネットでプライベート Google アクセスを構成する
D. Compute Engine クラスタにパブリック IP アドレスを割り当てないでください。
E. クラスタ内の Compute Engine インスタンスの IP 転送をオフにします。
Answer: B,D (メッセージを残す**)**

最新問題**: 98**
安全なコンテナ イメージを作成するときに、可能であればビルドに組み込む必要がある 2 つの項目はどれですか (2 つ選択してください)。
A. アプリが PID 1 として実行されていないことを確認します。
B. 単一のアプリをコンテナーとしてパッケージ化します。
C. アプリに必要のない不要なツールを削除します。
D. パブリック コンテナ イメージをアプリのベース イメージとして使用します。
E. 機密情報を非表示にするために、多くのコンテナ イメージ レイヤーを使用します。
Answer: B,C (メッセージを残す**)**

安全なコンテナイメージを作成する際には、脆弱性を最小限に抑え、コンテナが意図したとおりに動作することを保証するためのベストプラクティスに従うことが不可欠です。ここでは、2つの重要なプラクティスをご紹介します。
単一のアプリをコンテナとしてパッケージ化 :コンテナ内に単一のアプリケーションのみをパッケージ化することで、複雑さと潜在的な攻撃対象領域を削減できます。この方法は単一責任の原則に合致しており、各コンテナに明確で明確な目的を持たせることができます。
不要なツールの削除 :アプリケーションに不要なツールやソフトウェアは、コンテナイメージから削除する必要があります。これにより、潜在的な脆弱性の数を最小限に抑え、攻撃対象領域を縮小できます。また、コンテナイメージを最小限にすることで、イメージサイズが小さくなり、デプロイ時間が短縮されます。
これらのプラクティスは、より安全で効率的なコンテナ イメージの作成に貢献します。
参照：
コンテナセキュリティのベストプラクティス
コンテナイメージのセキュリティ保護

最新問題**: 99**
あなたの会社ではGoogle Cloudを利用しており、ネットワーク資産を公開しています。ソフトウェアツールを使用して、これらの資産を検出し、セキュリティ監査を最短時間で実施したいと考えています。
何をすべきでしょうか?
A. 組織内のすべてのインスタンスでプラットフォーム セキュリティ スキャナーを実行します。
B. 監査を実行するには、Google 認定のセキュリティ ベンダーに問い合わせてください。
C. 保留中の監査について Google に通知し、確認を待ってからスキャンを実行します。
D. Cloud Asset Inventory を使用してすべての外部資産を識別し、それらに対してネットワーク セキュリティ スキャナーを実行します。
Answer: (解答を表示する**)**

最新問題**: 100**
Google Kubernetes Engine（GKE）上の本番環境クラスタにコンテナ化されたアプリケーションをデプロイするためのCI/CDパイプラインを構築しています。既知の脆弱性を持つコンテナのデプロイを防ぐ必要があります。ソリューションには以下の要件があります。
クラウドネイティブであること
コスト効率がよいこと
運用オーバーヘッドを最小限に抑える
これをどのように達成すればよいですか? (2 つ選択してください。)
A. Cloud Source Repositories リポジトリ内のコンテナテンプレートの変更を監視する Cloud Build パイプラインを作成します。ビルドを続行する前に、Container Analysis の結果を分析するステップを追加します。
B. Google Cloud のオペレーション スイートのログイベントによってトリガーされる Cloud Functions を使用して、Container Registry 内のコンテナ イメージを自動的にスキャンします。
C. Compute Engine インスタンスで cron ジョブを使用して、既存のリポジトリをスキャンし、既知の脆弱性を検出し、準拠していないコンテナ イメージが見つかった場合はアラートを発します。

D. GKE に Jenkins をデプロイし、コンテナを Container Registry にデプロイするための CI/CD パイプラインを構成します。コンテナをクラスタにデプロイする前に、コンテナイメージを検証するステップを追加します。
E. CI/CD パイプラインで、脆弱性が見つかっていない場合は、コンテナイメージにアテステーションを追加します。Binary Authorization ポリシーを使用して、アテステーションのないコンテナのクラスターへのデプロイをブロックします。
Answer: (解答を表示する**)**

最新問題**: 101**
非機密データの鍵管理の複雑さを軽減し、機密データを保護し、同時に鍵の保管場所とローテーションスケジュールを柔軟に管理できる、保存時暗号化戦略を実装する必要があります。すべてのデータタイプでFIPS 140-2 L1準拠が必須です。どうすればよいでしょうか？
A. Cloud Key Management Service を使用して、非機密データと機密データを暗号化します。
B. 機密性が低いデータは Google のデフォルトの暗号化で暗号化し、機密データは Cloud Key Management Service で暗号化します。
C. Cloud External Key Manager を使用して、非機密データと機密データを暗号化します。
D. 機密性が低いデータは Google のデフォルトの暗号化で暗号化し、機密性の高いデータは Cloud External Key Manager で暗号化します。
Answer: A (メーッセージを残す**)**

最新問題**: 102**
社内用のApp Engineアプリケーションを作成し、ユーザーに代わってGoogleドライブにアクセスする必要があります。社内では、現在のユーザーの認証情報に依存したくありません。また、Googleが推奨するプラクティスにも従いたいと考えています。
何をすべきでしょうか?
A. 新しいサービス アカウントを作成し、すべてのアプリケーション ユーザーにサービス アカウント ユーザーの役割を付与します。
B. 新しいサービスアカウントを作成し、すべてのアプリケーションユーザーをGoogleグループに追加します。このグループにサービスアカウントユーザーの役割を付与します。
C. 専用の G Suite 管理者アカウントを使用し、これらの G Suite 認証情報を使用してアプリケーションの操作を認証します。
D. 新しいサービスアカウントを作成し、G Suite ドメイン全体の委任を付与します。アプリケーションでそのアカウントを使用してユーザーを偽装します。
Answer: D (メーッセージを残す**)**
ユーザーの認証情報に依存せず、Google が推奨するプラクティスに従わずにユーザーに代わって Google ドライブにアクセスするには、ドメイン全体の委任が可能なサービス アカウントを使用する必要があります。
サービス アカウントを作成します。
Cloud Console に移動し、[IAM と管理] > [サービス アカウント] に移動します。
「サービス アカウントの作成」をクリックし、必要な詳細を入力します。

ドメイン全体の委任を許可する:
サービス アカウントを編集して、G Suite ドメイン全体の委任」を有効にします。
JSON キー ファイルをダウンロードします。
G Suite で API アクセスを構成する:
Google 管理コンソールに移動します。
[セキュリティ] > [API コントロール] > [ドメイン全体の委任] に移動します。
新しい API クライアントを追加し、サービス アカウントのクライアント ID を使用します。
必要な API スコープを承認します (例: https://www.googleapis.com/auth/drive)。
アプリケーションに実装:
希望する言語の Google API クライアント ライブラリを使用します。
サービス アカウントの認証情報を読み込み、ユーザーの偽装を実行して Google ドライブにアクセスします。
参照：
ドメイン全体の権限委譲
サーバー間アプリケーションにおける OAuth 2.0 の使用

最新問題**: 103**
貴社は規制の厳しい環境で事業を展開しており、顧客データの保護に関する厳格なコンプライアンス要件を遵守しています。規制遵守のため、使用中のデータを暗号化する必要があります。どうすればよいでしょうか？
A. Google Compute Engine VM で顧客指定の暗号化キー（CSEK）の使用を有効にして、組織が VM ディスクの暗号化を最大限に制御できるようにします。
B. Confidential VM を使用して信頼できる実行環境を確立します。
C. シールドされた VM を使用して、アプリケーション環境の整合性監視によるセキュア ブートを確保します。
D. 顧客管理の暗号鍵（CMEK）と Cloud KSM を使用して、組織が Cloud SQL でのデータ暗号化に使用する鍵を制御できるようにします。
Answer: B (メッセージを残す**)**
https://cloud.google.com/confidential-computing/confidential-vm/docs/confidential-vm-overview

最新問題**: 104**
小売顧客は、ユーザーがコメントや製品レビューをアップロードすることを許可しています。コメントやレビューを公開する前に、顧客はテキストに機密情報が含まれていないことを確認する必要があります。
これを実現するにはどの Google Cloud サービスを使用すればよいですか?
A. クラウドデータ損失防止 API
B. クラウドセキュリティスキャナー
C. クラウドキー管理サービス
D. ビッグクエリ
Answer: B (メッセージを残す**)**

最新問題**: 105**

ある企業は、さまざまな Google Cloud Platform リージョンに冗長メール サーバーを保有しており、場所に基づいて顧客を最も近いメール サーバーにルーティングしたいと考えています。
企業はどのようにこれを達成すべきでしょうか?
A. TCP プロキシ負荷分散を、ポート 995 でリッスンするグローバル負荷分散サービスとして構成します。
B. 場所に基づいてトラフィックを転送する転送ルールを使用して、TCP ポート 995 をリッスンする Network Load Balancer を作成します。
C. HTTP(S) ロードバランサによるクロスリージョン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ルーティングします。
D. Cloud CDN を使用して、クライアント IP アドレスに基づいてメール トラフィックを最も近い元のメール サーバーにルーティングします。
Answer: (解答を表示する**)**
説明
https://cloud.google.com/load-balancing/docs/tcp
TCP プロキシ ロード バランシングは、グローバルに分散された GFE に実装されています。ネットワーク サービス ティアのプレミアム ティアを選択した場合、TCP プロキシ ロードバランサはグローバルになります。プレミアム ティアでは、バックエンドを複数のリージョンにデプロイでき、ロードバランサはユーザー トラフィックを最も近い容量のあるリージョンに自動的にリダイレクトします。スタンダード ティアを選択した場合、TCP プロキシ ロードバランサは単一リージョン内のバックエンド間でのみトラフィックをリダイレクトできます。https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing

最新問題**: 106**
先週、ある企業がBigQueryにログを書き込む新しいApp Engineアプリケーションをデプロイしました。プロジェクトでは他のワークロードは実行されていません。BigQueryに書き込まれたすべてのデータがApp Engineのデフォルトサービスアカウントを使用して行われたことを検証する必要があります。
何をすべきでしょうか?
A. 1. StackDriver Logging を使用して、BigQuery 挿入ジョブをフィルタリングします。
2. 認証フィールドで、App Engine のデフォルトのサービス アカウントに対応するメール アドレスをクリックします。
3. 「一致するエントリを表示」をクリックします。
4. 結果のリストが空であることを確認します。
B. 1. BigQuery で関連するデータセットを選択します。
2. データセットに書き込むことができるアカウントが App Engine のデフォルトのサービス アカウントのみであることを確認します。
C. 1. プロジェクトの IAM セクションに移動します。
2. App Engine のデフォルト サービス アカウントが、BigQuery に書き込むことができるロールを持つ唯一のアカウントであることを確認します。
D. 1. StackDriver Logging を使用して、BigQuery 挿入ジョブをフィルタリングします。

2. 認証フィールドで、App Engine のデフォルトのサービス アカウントに対応するメール アドレスをクリックします。
3. 「一致するエントリを非表示」をクリックします。
4. 結果のリストが空であることを確認します。
Answer: B (メーッセージを残す)

最新問題**: 107**
組織はサプライチェーンを攻撃から守りたいと考えています。デプロイメントパイプラインの脆弱性を自動的にスキャンし、スキャン 検証済みのコンテナのみが本番環境で実行されるようにする必要があります。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。どうすればよいでしょうか？
A. すべてのコンテナ イメージをステージング環境にデプロイし、コンテナ脅威検出を使用して悪意のあるコンテンツを検出してから、本番環境に昇格させます。
B. 本番環境へのデプロイ前にコンテナイメージをレビューし、公開されている脆弱性データベースを使用して既知の脆弱性がないか確認します。GrafeasとKritisを使用して、ビルドパイプラインを使用して構築されていないコンテナのデプロイを防止します。
C. トラフィック検査機能を備えた Cloud Next Generation Firewall (Cloud NGFW) Enterprise を使用して、本番環境でのコンテナ化されたアプリケーションへのアクセスを制限します。
D. Artifact Registry の脆弱性スキャンと Binary Authorization を CI/CD パイプラインに統合し、検証済みのイメージのみが本番環境にデプロイされるようにします。
Answer: D (メーッセージを残す)
コンテナ サプライ チェーンのセキュリティを確保するには、可視性 (スキャン) と適用 (ポリシー) の 2 つが必要です。
Google Cloud は、この問題を解決するために、Artifact Analysis（Artifact Registry と統合）と Binary Authorization を提供しています。
Google Cloud ドキュメント (ソフトウェア サプライ チェーン セキュリティ) によると、次のようになります。サプライチェーンのセキュリティを確保するには、Artifact Registryと自動脆弱性スキャンを使用してイメージ内のリスクを特定します。次に、Binary Authorizationを使用して、イメージをGKEまたはCloud Runにデプロイする前に、信頼できる機関（認証者）による署名を要求するポリシーを定義します。これにより、セキュリティチェック（脆弱性スキャンなど）に合格したイメージのみが実行できるようになります。仕組み：
* スキャン: イメージが Artifact Registry にプッシュされるたびに、CVE が自動的にスキャンされます。

* 構成証明: スキャンが成功すると (例: 「重大な」脆弱性がない)、イメージに「署名」する (構成証明を作成する) CI/CD ステップがトリガーされます。
* 適用: GKE アドミッションコントローラ (Binary Authorization) はこの署名をチェックします。署名が欠落しているか無効な場合、デプロイはブロックされます。
他のオプションが間違っている理由:
* A は誤りです。コンテナ脅威検出は実行時（実行後）を対象としています。サプライチェーンセキュリティは、展開前の予防を目的としています。
* B は不正解です。Grafeas/Kritis はオープンソースの基盤ですが、オプション D は「管理オーバーヘッドを最小限に抑える」マネージド Google Cloud サービスを表します。
* C は不正解です。ファイアウォールはネットワーク トラフィックを検査しますが、コンテナ イメージ自体の整合性や脆弱性の状態は検査しません。
参照：
Google Cloud ドキュメント：「Binary Authorization の概要」(https://cloud.google.com/binary-authorization/docs/overview)。
Google Cloud ドキュメント: 「Artifact Registry の脆弱性スキャン」(https://cloud.google.com/artifact-registry/docs/analysis)。

最新問題**: 108**
あなたは会社のセキュリティ管理者です。Cloud Storage バケットには 3,000 個のオブジェクトがあります。各オブジェクトへのアクセスを個別に管理したくありません。また、オブジェクトのアップロード者に常にオブジェクトのフルコントロール権限を与えることも望んでいません。しかし、バケットへのアクセス管理には Cloud Audit Logs を使用したいと考えています。
何をすべきでしょうか?
A. allUsers のスコープに OWNER 権限を持つ ACL を設定します。
B. allUsers のスコープに READER 権限を持つ ACL を設定します。
C. デフォルトのバケット ACL を設定し、IAM を使用してユーザーのアクセスを管理します。
D. Cloud Storage バケットに均一なバケットレベルのアクセスを設定し、IAM を使用してユーザーのアクセスを管理します。
Answer: (解答を表示する**)**
説明/参照:
参考: https://cloud.google.com/storage/docs/access-control/lists

最新問題**: 109**
エンベロープ暗号化を使用してデータを暗号化する手順は何ですか?
A. キー暗号化キー (KEK) をローカルで生成します。
データ暗号化キー (DEK) をローカルで生成します。KEKを使用してデータを暗号化します。
暗号化されたデータとラップされた DEK を保存します。
B. データ暗号化キー (DEK) をローカルで生成します。
DEK を使用してデータを暗号化します。

鍵暗号化鍵（KEK）を使用してDEKをラップします。暗号化されたデータとラップされたDEKを保存します。
C. データ暗号化キー (DEK) をローカルで生成します。
DEKをキー暗号化キー（KEK）でラップします。KEKでデータを暗号化します。
暗号化されたデータとラップされた KEK を保存します。
D. キー暗号化キー (KEK) をローカルで生成します。
KEKを使用してデータ暗号化キー（DEK）を生成します。DEKを使用してデータを暗号化します。
暗号化されたデータとラップされた DEK を保存します。
Answer: B (メーッセージを残す**)**

最新問題**: 110**
組織におけるGoogle Cloudの利用が大幅に増加し、多くのグループがそれぞれ異なるクラウドリソースを個別に利用しています。組織全体で共通する構成ミスやコンプライアンス違反を特定し、ダッシュボードで改善策の実施に必要な調査結果を追跡する必要があります。どうすればよいでしょうか？
A. Cloud Asset Inventory でフィルタ セットを作成し、高い権限を持つサービス アカウントと Gmail ドメインの IAM プリンシパルを識別します。
B. Security Command Center Premium の Secure Health Analytics 検出器を使用して、脆弱性と誤った構成をスキャンして警告します。
C. Cloud Audit Logs にフィルタを設定して、特定のリスクのある API 呼び出しのログエントリにフラグを付け、Cloud Log Analytics ダッシュボードに呼び出しを表示します。
D. イベント脅威検出検出器を使用して、環境内で検出された新たな攻撃を警告および追跡します。
Answer: (解答を表示する**)**
https://cloud.google.com/security-command-center/docs/concepts-security-health-analytics Security Health Analytics は、攻撃を受ける可能性のある一般的な誤った構成がないかクラウド環境をスキャンする Security Command Center のマネージド サービスです。
Security Command Center を有効にすると、Security Health Analytics が自動的に有効になります。

最新問題**: 111**
組織では複雑なアプリケーションを Google Cloud に移行しています。このアプリケーションには複数の内部コンポーネントがあり、それらは複数の Google Cloud プロジェクト間で相互に連携します。
セキュリティは大きな懸念事項であり、最小権限と職務分離の原則に沿った管理者向けの認証スキームを設計する必要があります。どうすればよいでしょうか？
A. アプリケーションを移行するユーザーを特定し、デフォルトのユーザー ロールを取り消して、意図的に作成されたカスタム ロールをユーザーに割り当てます。
B. 異なる SAML プロファイルを使用するように構成された複数の外部 ID プロバイダー (IdP) を使用し、各アプリケーション コンポーネントの IdP をフェデレーションします。
C. 多要素認証 (MFA) を構成して、アプリケーションを移行するすべてのユーザーに対して物理トークンの使用を強制します。
D. 何もする必要はありません。Google Cloud 組織が作成されると、ドメイン内のすべてのユーザーに適切な権限が自動的に割り当てられます。

Answer: A (メーッセージを残す)

最新問題: **112**
gcloud コマンドラインツールを使用して、サードパーティのシングルサインオン (SSO) SAML ID プロバイダで認証を行いたいと考えています。サードパーティの ID プロバイダ (IdP) で認証がサポートされていることを確認するために必要なオプションはどれですか (2 つ選択してください)。
A. サードパーティのIdPとしてのSSO SAML
B. アイデンティティプラットフォーム
C. OpenIDコネクト
D. アイデンティティ認識プロキシ
E. クラウドアイデンティティ
Answer: A,C (メーッセージを残す)
説明
ユーザーに選択したクラウド アプリへの SSO ベースのアクセスを提供するために、IdP としての Cloud Identity は、OpenID Connect (OIDC) および Security Assertion Markup Language 2.0 (SAML) プロトコルをサポートしています。https://cloud.google.com/identity/solutions/enable-sso

最新問題: **113**
チームは、オンプレミスの Active Directory サービスから GCP の IAM 権限を一元管理したいと考えています。また、AD グループのメンバーシップごとに権限を管理したいと考えています。
これらの要件を満たすためにチームは何をすべきでしょうか?
A. グループを同期するように Cloud Directory Sync を設定し、グループに IAM 権限を設定します。
B. SAML 2.0 シングル サインオン (SSO) を設定し、グループに IAM 権限を割り当てます。
C. Cloud Identity and Access Management API を使用して、Active Directory からグループと IAM 権限を作成します。
D. Admin SDK を使用してグループを作成し、Active Directory から IAM 権限を割り当てます。
Answer: A (メーッセージを残す)
既存のID管理システムを引き続き使用するには、ADとGCP IAMの間でIDを同期する必要があります。Google はこれを実現するために、Cloud Directory Syncというツールを提供しています。このツールは、AD内のすべてのIDを読み取り、GCP内に複製します。IDが複製されると、グループにIAM権限を適用できるようになります。その後、Googleがサービスプロバイダとして機能するようにSAMLを設定し、ADFS、またはPingやOktaなどのサードパーティツールがIDプロバイダとして機能するようにします。これにより、Googleから管理下にあるものに認証を効果的に委任できます。

最新問題: **114**
PCI DSS 要件を満たすために、顧客はすべての送信トラフィックが承認されていることを保証したいと考えています。
追加の補償制御なしでこの要件を満たすクラウド オファリングはどれですか? (2 つ選択してください。)
A. App Engine
B. クラウド関数

C. コンピューティングエンジン
D. Google Kubernetes Engine
E. クラウドストレージ
Answer: (解答を表示する**)**
参照：
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

最新問題**: 115**
組織の Google Cloud プロジェクト（プロジェクト A）を管理しています。AVPC Service Control（SC）境界により、このプロジェクトへの API アクセス リクエスト（Pub/Sub を含む）がブロックされています。別のプロジェクト（プロジェクト B）のサービス アカウントで実行されているリソースが、プロジェクト内の Pub/Sub トピックからメッセージを収集する必要がありますが、プロジェクト B は VPC SC 境界に含まれていません。最小権限の原則に基づき、プロジェクト B からプロジェクト A の Pub/Sub トピックへのアクセスを提供する必要があります。
何をすべきでしょうか?
A. プロジェクト A の境界に対して上りポリシーを設定し、プロジェクト B のサービス アカウントがメッセージを収集できるようにアクセスを許可します。
B. プロジェクト B の開発者がプロジェクト A にある Pub/Sub トピックをサブスクライブできるようにするアクセス レベルを作成します。
C. プロジェクト A とプロジェクト B の間に境界ブリッジを作成し、両方のプロジェクト間で必要な通信を可能にします。
D. プロジェクト A の境界構成内の制限されたサービスのリストから Pub/Sub API を削除します。
Answer: A (メーッセージを残す**)**
VPC Service Controls（VPC SC）を使用する場合、承認されたリソースのみが機密データやサービスにアクセスできるようにすることが重要です。セキュリティを損なうことなく、プロジェクト B のリソースがプロジェクト A の Pub/Sub にアクセスできるようにするには、プロジェクト A のサービス境界に上り（内向き）ポリシーを設定する必要があります。
* サービス アカウントを特定する: プロジェクト B で Pub へのアクセスを必要とするサービス アカウントを特定します。
/プロジェクト A のサブトピック。
* 入力ポリシーを構成する:
* Google Cloud Console に移動します。
* [セキュリティ] > [VPC サービス コントロール] に移動します。
* プロジェクト A のサービス境界を選択します。
* プロジェクト B のサービス アカウントを指定し、必要な Pub/Sub リソースへのアクセスを許可する Ingress ルールを追加します。
* 条件の定義: イングレス ポリシーが最小権限の原則に準拠し、Pub/Sub トピックからメッセージを収集するために必要な権限のみを付与することを確認します。
* 保存して適用: ポリシーを保存し、変更を適用して新しいアクセス制御を適用します。

このアプローチにより、VPC SC によって設定されたセキュリティ境界が維持され、プロジェクト B からプロジェクト A への必要なアクセスが可能になります。
VPC サービスコントロールのドキュメント
入力ポリシーの設定

最新問題: **116**
組織ではActive Directoryを使用しており、Security Assertion Markup Language （SAML）の設定を希望しています。すべてのユーザーに対してシングルサインオン （SSO）を設定し、適用する必要があります。
何をすべきでしょうか?
A. 1. 新しい SAML プロファイルを作成します。
2. サインイン ページとサインアウト ページの URL を入力します。
3. X.509 証明書をアップロードします。
4. IdP でエンティティ ID と ACS URL を設定します。
B. 1. Active Directory (AD) テナントで OpenID Connect (OIDC) の前提条件を構成します。
2. AD ドメインを確認します。
3. SAML を使用するユーザーを決定します。
4. 事前設定されたプロファイルを、選択した組織単位 (OU) とグループに割り当てます。
C. 1. 新しい SAML プロファイルを作成します。
2. X.509 証明書をアップロードします。
3. パスワード変更 URL を有効にします。
4. IdP でエンティティ ID と ACS URL を設定します。
D. 1. SAML プロファイルの割り当てを管理します。
2. Active Directory (AD) テナントで OpenID Connect (OIDC) を有効にします。
3. ドメインを検証します。
Answer: A (メーッセージを残す**)**
https://support.google.com/cloudidentity/answer/12032922?hl=ja

最新問題: **117**
Vertex AI 上で実行されるカスタムトレーニングジョブのセキュリティ確保に、開発者と連携しています。コンプライアンス上の理由から、サポートされるすべてのデータタイプは、ヨーロッパ地域に存在し、組織が管理する鍵マテリアルを使用して暗号化する必要があります。暗号化アクティビティは、Vertex AI のトレーニング操作に影響を与えてはなりません。どうすればよいでしょうか？
A. コード、トレーニング データ、メタデータを Google のデフォルトの暗号化方式で暗号化します。Cloud Storage バケットにエクスポートされるトレーニング済みモデルには、顧客管理の暗号鍵 （CMEK）を使用します。
B. コード、トレーニング データ、メタデータ、エクスポートされたトレーニング済みモデルを顧客管理の暗号化キー (CMEK) を使用して暗号化します。
C. コード、トレーニング データ、エクスポートされたトレーニング済みモデルを顧客管理の暗号化キー (CMEK) を使用して暗号化します。

D. コード、トレーニング データ、メタデータを Google のデフォルトの暗号化方式で暗号化します。Cloud KMS のロケーションをヨーロッパ リージョンに制限する制約を適用する組織ポリシーを実装します。
Answer: C (メッセージを残す**)**
https://cloud.google.com/vertex-ai/docs/general/cmek#resources
通常、CMEK 鍵は、ジョブ名やリージョン、データセットの表示名など、オペレーションに関連付けられたメタデータを暗号化しません。オペレーションに関連付けられたメタデータは、常に Google のデフォルトの暗号化メカニズムを使用して暗号化されます。

最新問題**: 118**
会社で承認されたコンピューティング イメージを、イメージ リポジトリとして使用されている単一の Google Cloud プロジェクトに保存しています。このプロジェクトは VPC Service Controls で保護されており、組織内の他のプロジェクトと共に境界内に存在します。これにより、他のプロジェクトはイメージ リポジトリ プロジェクトからイメージをデプロイできます。あるチームでは、外部の Google Cloud 組織に保存されているサードパーティのディスク イメージをデプロイする必要があります。境界にデプロイできるように、ディスク イメージへの読み取りアクセス権を付与する必要があります。
何をすべきでしょうか?
A. 組織ポリシーを使用して外部プロジェクトを許可します。
制約/compute.trustedImageProjects。
B. 1. 境界を更新します。
2. egressTo フィールドを設定して、許可されたリソースとして外部 Google Cloud プロジェクト番号を含め、serviceName を compute.googleapis.com に設定します。
3. egressFrom フィールドを構成して、identityType を ANY_IDENTITY に設定します。
C. 1. 境界を更新します。
2. ingressFrom フィールドを構成して、identityType を ANY_IDENTITY に設定します。
3. ingressTo フィールドを設定して、許可されたリソースとして外部の Google Cloud プロジェクト番号を含め、serviceName を compute.googleapis.com に設定します。
D. 1. 境界を更新します。
2. egressTo フィールドを構成して、identityType を ANY_IDENTITY に設定します。
3. egressFrom フィールドを設定して、許可されたリソースとして外部 Google Cloud プロジェクト番号を含め、serviceName を compute.googleapis.com に設定します。
Answer: B (メッセージを残す**)**
サービス境界内の Compute Engine クライアントが、境界外にあるイメージ リソースに対して Compute Engine 作成オペレーションを呼び出しています。
https://cloud.google.com/vpc-service-controls/docs/ingress-egress-
ルール番号:~:text=エグレスとは、アクセス、リソースが境界外にあることを意味します。

最新問題**: 119**
DevOps チームは、次のプロセスで Packer を使用して Compute Engine イメージを構築します。
1. 一時的な Compute Engine VM を作成します。

2. Cloud Storage バケットから VM のファイル システムにバイナリをコピーします。
3. VM のパッケージ マネージャーを更新します。
4. インターネットから外部パッケージを VM にインストールします。
セキュリティチームは、VM 上のパブリック IP アドレスの使用を制限する組織ポリシー（constraints/compute.vmExternalIpAccess）を有効化しました。これを受けて、DevOps チームはスクリプトを更新し、Compute Engine VM 上のパブリック IP アドレスを削除しましたが、接続の問題によりビルド パイプラインが失敗しています。
あなたは何をすべきでしょうか？ 2つ選択してください。）
A. 管理対象外インスタンス グループ内の VM に HTTP ロードバランサをプロビジョニングして、インターネットから VM への受信接続を許可します。
B. Compute Engine VM と同じ VPC およびリージョンに Cloud NAT インスタンスをプロビジョニングします。
C. Compute Engine VM がデプロイされているサブネット上でプライベート Google アクセスを有効にします。
D. インターネットとの間のトラフィックを許可するように VPC ルートを更新します。
E. Compute Engine VM と同じ VPC およびリージョンに Cloud VPN トンネルをプロビジョニングします。
Answer: (解答を表示する**)**
Cloud NAT インスタンスをプロビジョニングする（オプション B）Cloud NAT を使用すると、パブリック IP アドレスを持たない Compute Engine インスタンスが、組織のポリシーで課せられたセキュリティ制限を維持しながらインターネットにアクセスできるようになります。Compute Engine VM と同じ VPC およびリージョンに Cloud NAT インスタンスをプロビジョニングすることで、これらの VM のアウトバウンド接続が可能になります。
プライベート Google アクセスを有効にする（オプション C）Compute Engine VM がデプロイされているサブネットでプライベート Google アクセスを有効にすると、これらのインスタンスはプライベート IP アドレス範囲を介して Google Cloud サービスにアクセスできるようになります。これにより、VM をパブリック インターネットに公開することなく、Packer イメージのビルドプロセス中に必要な外部リソースにアクセスできるようになります。

最新問題**: 120**
顧客の社内セキュリティ チームは、Cloud Storage 上のデータを暗号化するために独自の暗号化キーを管理する必要があり、顧客指定の暗号化キー (CSEK) を使用することを決定しました。
チームはこのタスクをどのように完了する必要がありますか?
A. 暗号化キーを Cloud Storage バケットにアップロードし、オブジェクトを同じバケットにアップロードします。
B. gsutil コマンドライン ツールを使用してオブジェクトを Cloud Storage にアップロードし、暗号化キーの場所を指定します。
C. Google Cloud Platform Console で暗号化キーを生成し、指定されたキーを使用してオブジェクトを Cloud Storage にアップロードします。

D. オブジェクトを暗号化し、gsutil コマンドライン ツールまたは Google Cloud Platform Console を使用してオブジェクトを Cloud Storage にアップロードします。
Answer: B (メーッセージを残す**)**
Cloud Storage 上のデータを暗号化するために顧客指定の暗号鍵 (CSEK) を使用するには、次の手順に従います。
暗号化キーの生成 :256ビットのAES暗号化キーを生成します。このキーはBase64でエンコードされている必要があります。
シュ
コードをコピー
openssl rand -base64 32
CSEK を使用したオブジェクトのアップロード: gsutil コマンドライン ツールを使用してオブジェクトを Cloud Storage にアップロードし、-o オプションを使用して暗号化キーの場所を指定します。
gsutil -o "GSUtil:encryption_key=<base64-encoded-key>" cp [LOCAL_OBJECT_PATH] gs://[BUCKET_NAME]/ 暗号化の確認: オブジェクトをアップロードした後、オブジェクトのメタデータをチェックすることで、提供された CSEK を使用して暗号化されていることを確認できます。
gsutil stat gs://[バケット名]/[オブジェクト名]
鍵管理：暗号化鍵が安全に保管・管理されていることを確認してください。スクリプトやアプリケーションにハードコードしないでください。
gsutil ツールを使用して暗号化キーを指定すると、アップロード プロセス中に顧客が指定した暗号化キーを使用してオブジェクトが暗号化されることが保証されます。
参照：
顧客提供暗号化キー（CSEK）ドキュメント
gsutil コマンドラインツールのドキュメント

最新問題**: 121**
小規模スタートアップ企業のオフィスマネージャーは、請求書と支払い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にはこれらのタスクに必要なIdentity and Access Management（IAM）権限のみが許可されています。オフィスマネージャーが持つべきIAMロールは2つありますか？ （2つ選択してください。）
A. 請求アカウント費用管理者
B. プロジェクト作成者
C. 請求アカウント閲覧者
D. 組織管理者
E. 請求先アカウントユーザー
Answer: (解答を表示する**)**

最新問題: **122**
お客様が他社と共同で、Compute Engine 上にアプリケーションを構築しています。お客様は自社の GCP 組織でアプリケーション層を構築し、他社は別の GCP 組織でストレージ層を構築しています。これは 3 層ウェブアプリケーションです。アプリケーションの各部分間の通信は、いかなる手段を用いてもパブリックインターネットを経由してはいけません。
どの接続オプションを実装する必要がありますか?
A. VPCピアリング
B. クラウドVPN
C. クラウド相互接続
D. 共有VPC
Answer: A (メーッセージを残す**)**
* 目標: 異なる GCP 組織内のアプリケーション層間のプライベート通信を確保する。
* 解決策: VPC ピアリングを使用して、パブリック インターネットを経由せずにプライベート通信を有効にします。
* 手順:
* ステップ 1: Google Cloud Console を開きます。
* ステップ 2: VPC ネットワーク ピアリング ページに移動します。
* ステップ 3: アプリケーション層をホストしているプロジェクトに新しい VPC ピアリング接続を作成します。
* ステップ 4: ピアリングする他の組織 (ストレージ層をホストしている組織) 内の VPC ネットワークを指定します。
* ステップ 5: 他のプロジェクトでピアリング要求を承認します。
* ステップ 6: ピアリングされた VPC ネットワーク間のトラフィックを許可するために必要なルートとファイアウォール ルールを構成します。
VPC ピアリングを使用すると、2 つの VPC ネットワークをプライベートかつ直接接続できるため、それらの間のトラフィックがパブリック インターネットを通過しないことが保証されます。
参考文献:
* GCP VPC ピアリングのドキュメント
* VPC ネットワーク ピアリング ガイド

最新問題: **123**
PCIコンプライアンスの観点からGCPを評価したいと考えています。Google固有の管理機能を特定する必要があります。
情報を見つけるにはどの文書を確認する必要がありますか?
A. Google Cloud Platform: 顧客責任マトリックス

B. PCI DSS要件とセキュリティ評価手順
C. PCI SSC クラウドコンピューティングガイドライン
D. Compute Engine の製品ドキュメント
Answer: (解答を表示する**)**
Google Cloud Platform（GCP）のPCIコンプライアンスを評価し、Google固有のセキュリティ対策を確認するには、「Google Cloud Platform：顧客責任マトリックス」をご確認ください。このドキュメントでは、共有責任モデルに関する詳細な情報を提供し、Googleが管理するセキュリティ対策とお客様が責任を負うセキュリティ対策の概要を説明しています。
ドキュメントにアクセスして使用する手順:
* ドキュメントにアクセスする:
* Google Cloud コンプライアンス リソース センターにアクセスします。
* PCI DSS コンプライアンスの「顧客責任マトリックス」を見つけます。
* 固有の制御を確認する:
* このドキュメントでは、さまざまなコントロールをリストし、それらが Google によって管理されるか、顧客によって管理されるか、またはその両方によって管理されるかを指定します。
* インフラストラクチャのセキュリティ、データ保護、コンプライアンス要件などのさまざまな側面をカバーします。
* PCIコンプライアンスを分析:
* マトリックスを使用して、Google Cloud が本質的にどの PCI DSS 要件に対応しているかを理解します。
* 完全なコンプライアンスを確保するために、顧客として実装および管理する必要がある制御を特定します。
このドキュメントを確認することで、Google Cloud が提供する固有の制御と、PCI コンプライアンスを達成するために果たす必要がある責任について包括的に理解できるようになります。
Google Cloud コンプライアンス ドキュメント
Google Cloud における PCI DSS コンプライアンス

最新問題**: 124**
組織では、Google Cloud のプライマリ ID プロバイダとして Google Workspace を使用しています。組織内のユーザーは最初にパスワードを作成しましたが、最近のセキュリティ イベントが発生したため、パスワードのセキュリティを強化する必要があります。どうすればよいでしょうか？
A. 監査および調査ツールを使用して、疑わしいログインのユーザー アクティビティを監査します。
B. セキュリティ意識向上トレーニング セッションを実施し、パスワードの有効期限設定をより頻繁な更新を必要とするように設定します。
C. [強力なパスワードを強制する] ボックスをオンにして、パスワードの有効期限がより頻繁に発生するように設定します。
D. [強力なパスワードを適用する] チェックボックスをオンにし、[次回のサインイン時にパスワード ポリシーを適用する] チェックボックスをオンにします。
Answer: D (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：

当面の目標は、パスワードのセキュリティを強化し、最近の出来事を受けて変更を強制することです。これは、Google Cloud ユーザーの ID プロバイダを管理する Google Workspace 管理コンソールを通じて行われます。
パスワード セキュリティの強化: 最も効果的な制御は、強力なパスワード ポリシーを適用して、ユーザーに長くて複雑で推測不可能なパスワードの使用を義務付け、セキュリティの根本的な弱点に対処することです。
即時適用: 次回のサインイン時にパスワード ポリシーを適用するオプションをオンにすると、現在のすべてのユーザーに対して、弱いパスワードを新しい強力なポリシー要件を満たすパスワードに直ちに変更するように求めるメッセージが表示されます。
オプションCは、パスワードの頻繁な有効期限切れという時代遅れのセキュリティ対策に基づいています。この対策では、ユーザーが脆弱で予測可能なパスワード（例Spring2025 -> Summer2025）を選択してしまうことがよくあります。現代では、頻繁な有効期限切れではなく、強力なパスワードと多要素認証が推奨されています。
オプション A は検出制御であり、パスワードの強度を向上させる予防策ではありません。
抜粋:
Google Workspace 管理コンソールでは、強力なパスワード ポリシーを満たすパスワードの使用をユーザーに要求できます。強力なパスワードとは、最小文字数や文字の組み合わせなど、最低限の複雑さの要件を満たすパスワードのことです。(出典 6.1)
パスワードポリシーを変更した後、「次回サインイン時にすべてのユーザーにパスワードの変更を要求する」オプションを選択できます。これは、組織全体に新しいポリシーを即座に適用する最も迅速な方法です。（出典：6.2）
Google Cloud が推奨する ID セキュリティのベスト プラクティスでは、頻繁なパスワードの有効期限切れよりも、強力なパスワードと多要素認証 (MFA) を優先します。(出典 6.3)

最新問題**: 125**
ある組織のセキュリティおよびリスク管理チームは、Google Cloud Platform（GCP）で実行している特定の本番環境ワークロードに対する責任の所在と、Googleの責任の所在について懸念を抱いています。彼らは主にApp EngineをはじめとするGoogle CloudのPlatform-as-a-Service（PaaS）サービスを使用してワークロードを実行しています。
App Engine を使用する際に、テクノロジー スタック内のどの領域に主な責任として重点を置く必要がありますか。
A. VPC フローログの設定と監視
B. XSSおよびSQLi攻撃からの防御
C. ゲスト OS の最新のアップデートとセキュリティ パッチを管理します
D. 保存されているすべてのデータを暗号化する
Answer: B (メーッセージを残す**)**

最新問題**: 126**
チームは、Compute Engine インスタンスがインターネットや Google API またはサービスにアクセスできないようにする必要があります。

これらの要件を満たすには、どの 2 つの設定を無効のままにしておく必要がありますか? (2 つ選択してください。)
A. パブリックIP
B. IP転送
C. プライベート Google アクセス
D. 静的ルート
E. IAM ネットワーク ユーザー ロール
Answer: (解答を表示する**)**
Compute Engine インスタンスがインターネットや Google API またはサービスにアクセスできないようにするには、次の設定を無効にする必要があります。
パブリックIP :パブリックIPアドレスを無効にすると、インスタンスがインターネットに直接接続されなくなります。パブリックIPアドレスがないと、インスタンスはインターネットから直接アクセスしたり、インターネットと直接通信したりできなくなります。
プライベート Google アクセス :プライベート Google アクセスを無効にすると、インスタンスは Google 社内ネットワーク経由で Google API やサービスにアクセスできなくなります。プライベート Google アクセスを有効にすると、パブリック IP を持たないインスタンスでもプライベート IP アドレスを使用して Google API やサービスにアクセスできますが、無効にするとこのパスがブロックされます。
これらの設定を無効にすると、インスタンスはパブリック インターネットと Google の内部 API サービスの両方から効果的に分離されます。
参照：
Google Cloud VPC ドキュメント - 概要
プライベートGoogleアクセスの設定
Compute Engine ネットワークの概要

最新問題**: 127**
あなたはセキュリティ チームの一員であり、プロジェクト A の Cloud Storage バケットがプロジェクト B からのみ読み取り可能であることを確認したいと考えています。
また、ユーザーが正しい認証情報を持っている場合でも、ネットワーク外部の Cloud Storage バケットから Cloud Storage バケット内のデータにアクセスしたり、そのバケットにデータをコピーしたりできないようにする必要があります。
何をすべきでしょうか?
A. VPC Service Controls を有効にし、プロジェクト A と B で境界を作成し、Cloud Storage サービスを含めます。
B. Cloud Storage バケットでドメイン制限共有組織ポリシーとバケット ポリシーのみを有効にします。
C. 厳格なファイアウォール ルールを使用してプロジェクト A および B のネットワークでプライベート アクセスを有効にし、ネットワーク間の通信を許可します。
D. 厳格なファイアウォール ルールを使用してプロジェクト A と B のネットワーク間の VPC ピアリングを有効にし、ネットワーク間の通信を許可します。
Answer: B (メーッセージを残す**)**
参照：

https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains

最新問題: **128**
社内のユーザーはBigQueryテーブルのデータにアクセスします。ユーザーがデータにアクセスできるのは勤務時間中のみにすることを希望しています。
何をすべきでしょうか?
A. 指定された勤務時間中に BigQuery の組織ポリシー制約を変更する Cloud Functions インスタンスをトリガーするように Cloud Scheduler を構成します。
B. 指定された勤務時間中に毎日ユーザーを追加および削除するサービス アカウントに BigQuery データ閲覧者ロールを割り当てます。
C. 指定された勤務時間にアクセスを制限する 1AM 条件とともに、BigQuery データ閲覧者ロールを割り当てます。
D. BigQuery データ閲覧者のロールを割り当てる gsuttl スクリプトを実行し、指定された営業時間内にのみそのロールを削除します。
Answer: C (メーッセージを残す**)**

最新問題: **129**
Google Kubernetes Engine（GKE）上の本番環境クラスタにコンテナ化されたアプリケーションをデプロイするためのCI/CDパイプラインを構築しています。既知の脆弱性を持つコンテナのデプロイを防ぐ必要があります。ソリューションには以下の要件があります。
- クラウドネイティブであること
- コスト効率がよいこと
- 運用オーバーヘッドを最小限に抑える
これをどのように達成すればよいですか? (2 つ選択してください。)
A. Cloud Source Repositories リポジトリ内のコンテナテンプレートの変更を監視する Cloud Build パイプラインを作成します。ビルドを続行する前に、Container Analysis の結果を分析するステップを追加します。
B. Google Cloud のオペレーション スイートのログイベントによってトリガーされる Cloud Functions を使用して、Container Registry 内のコンテナ イメージを自動的にスキャンします。
C. Compute Engine インスタンスで cron ジョブを使用して、既存のリポジトリをスキャンし、既知の脆弱性を検出し、準拠していないコンテナ イメージが見つかった場合はアラートを発します。
D. GKE に Jenkins をデプロイし、コンテナを Container Registry にデプロイするための CI/CD パイプラインを構成します。コンテナをクラスタにデプロイする前に、コンテナイメージを検証するステップを追加します。
E. CI/CD パイプラインで、脆弱性が見つかっていない場合は、コンテナイメージにアテステーションを追加します。Binary Authorization ポリシーを使用して、アテステーションのないコンテナのクラスターへのデプロイをブロックします。
Answer: A,E (メーッセージを残す**)**
オンデマンド コンテナ分析は、Cloud Build パイプラインに統合できます。
https://cloud.google.com/container-analysis/docs/ods-cloudbuild
また、バイナリ認証は「クラウドネイティブ」の補完的なメカニズムです。

最新問題: **130**
あなたの組織は、ソフトウェアイノベーションにおけるマーケットリーダーを目指しています。開発者がVertex AIのGeminiを既存のアプリケーションに統合するテストや、新しいプロジェクトの作成を行えるよう、多数のGoogle Cloud環境を提供しています。組織には200人の開発者と5人のセキュリティチームがいます。Google Cloud 環境全体にわたって適切なセキュリティ ポリシーを防止および検出する必要があります。何をすべきでしょうか？ 2 つ選択してください）
A. Security Command Center Enterprise または Premium レベルの Vertex AI で、Gemini に事前定義された AI 推奨セキュリティ ポスチャ テンプレートを適用します。
B. アプリケーションを安全に開発するための内部ポリシーと明確なガイドラインを公開します。
C. 誤った構成を防ぐために、最小限の権限を持つ Identity and Access Management ロールを実装します。
D. 組織のポリシー制約を適用します。セキュリティヘルス分析を使用してドリフトを検出し、監視します。
E. Cloud Logging を使用してログフィルタを作成し、構成ミスを検出します。Cloud Run 関数をトリガーして構成ミスを修正します。
Answer: C,D (メーッセージを残す**)**
特に大規模な開発者ベースと小規模なセキュリティ チームを抱える多数の Google Cloud 環境全体で適切なセキュリティ ポリシーを維持するには、自動化されたスケーラブルなセキュリティ対策を実装することが重要です。
* オプション A: AI が推奨するセキュリティ ポスチャ テンプレートを適用すると効果的ですが、現時点では、Security Command Center 内の Vertex AI には Gemini 用の特定の定義済みテンプレートはありません。
* オプション B: 内部ポリシーとガイドラインを公開することは、安全な開発プラクティスを促進するために不可欠ですが、セキュリティ ポリシーを適用または検出するにはそれだけでは不十分な場合があります。
* オプション C: Identity and Access Management (IAM) ロールを通じて最小権限の原則を実装すると、ユーザーにタスクに必要な権限のみが付与されるため、構成ミスや不正アクセスのリスクが最小限に抑えられます。
* オプションD：組織ポリシーの制約を適用することで、プロジェクト全体に特定の構成と制限を適用できます。セキュリティヘルスアナリティクスを活用することで、これらのポリシーからの逸脱を検出 監視し、潜在的なセキュリティ問題に関するインサイトを自動的に提供できます。
* オプション E: Cloud Logging を使用して構成ミスを検出し、修復のために Cloud Run 関数をトリガーすると、複雑さが生じ、大幅なメンテナンスが必要になる可能性があるため、小規模なセキュリティ チームにとってはあまり実用的ではありません。
したがって、オプションCとDが最も効果的な戦略です。これらは、組織の規模とリソースを考慮したスケーラブルなソリューションのニーズに応え、セキュリティポリシーの自動適用と監視を提供します。
参考文献:
* アイデンティティとアクセス管理（IAM）の概要
* 組織ポリシーサービスの概要
* セキュリティヘルス分析の概要

最新問題: **131**

セキュリティ監査により、プロジェクトのIdentity and Access Management（IAM）設定に複数の不整合が見つかりました。一部のサービスアカウントのロール権限が過度に高く、一部の外部協力者には必要以上のアクセス権が付与されています。IAMポリシーの変更、ユーザーアクティビティ、サービスアカウントの動作、機密性の高いプロジェクトへのアクセス状況を詳細に把握する必要があります。どうすればよいでしょうか？
A. Cloud Monitoring のメトリックス エクスプローラーを有効にして、サービス アカウントの認証イベントを追跡し、それにリンクされたアラートを作成します。
B. Cloud Audit Logs を使用します。ログエクスポートシンクを作成し、これらのログをセキュリティ情報イベント管理（SIEM）ソリューションに送信して、他のイベントソースとの相関関係を確認します。
C. IAM ポリシーの変更によって Google Cloud Functions がトリガーされるように設定します。ポリシーシミュレータを使用して変更を分析し、リスクの高い変更があった場合にアラートを送信し、イベントの詳細を保存します。
D. OS Config Management エージェントを VM に展開します。OS Config Management を使用して、パッチ管理ジョブを作成し、システムの変更を監視します。
Answer: B (メーッセージを残す)
プロジェクトの Identity and Access Management（IAM）構成の不整合に対処し、IAM ポリシーの変更、ユーザー アクティビティ、サービス アカウントの動作、機密プロジェクトへのアクセスを包括的に可視化するには、Google Cloud の監査機能を活用することが不可欠です。
* オプション A: Cloud Monitoring の Metrics Explorer は特定の指標を追跡できますが、IAM ポリシーの変更やユーザー アクティビティの詳細なログを提供するようには設計されていません。
* オプションB :Cloud Audit Logs は、IAM ポリシーの変更や認証などの管理アクティビティの詳細な記録を提供します。ログエクスポートシンクを作成することで、これらのログをセキュリティ情報イベント管理（SIEM）ソリューションに転送し、他のイベントソースとの相関分析や包括的な分析が可能になります。このアプローチにより、IAM 構成とユーザーアクティビティに関する必要な可視性が得られます。
* オプションC :IAMポリシーの変更に基づいてCloud Functionsをトリガーし、ポリシーシミュレーターで分析することは、プロアクティブなアプローチです。ただし、SIEMソリューションが提供するような詳細な履歴データや包括的な分析機能は提供されない可能性があります。
* オプション D: OS Config Management エージェントの導入では、VM 構成とパッチ管理に重点が置かれており、IAM ポリシーの監視やユーザー アクティビティの追跡には直接対応していません。
したがって、オプション B は、IAM 関連のアクティビティの詳細な可視性を獲得し、特定された不一致に対処するための最も効果的なソリューションです。
参考文献:
* クラウド監査ログの概要
* SIEMへのログのエクスポート

最新問題**: 132**
お客様は、Google Cloud Platform（GCP）でホストされているCRMウェブインターフェースに、モバイルワーカーが簡単にアクセスできるようにしたいと考えています。CRMには、企業ネットワーク上のユーザーのみがアクセスできます。お客様は、CRMをインターネット経由で利用できるようにしたいと考えています。あなた

のチームでは、アプリケーションの前に2要素認証をサポートする認証レイヤーが必要です。これらの要件を満たすために、お客様はどのGCPプロダクトを導入すべきでしょうか？
A. クラウドアーマー
B. クラウドエンドポイント
C. クラウド ID 認識プロキシ
D. クラウドVPN
Answer: D (メーッセージを残す)

最新問題**: 133**
顧客は別の企業と協力して Compute Engine 上にアプリケーションを構築しています。
お客様は自社のGCP組織内にアプリケーション層を構築し、相手企業は別のGCP組織内にストレージ層を構築しています。これは3層ウェブアプリケーションです。
アプリケーションの各部分間の通信は、いかなる手段によってもパブリック インターネットを通過してはなりません。
どの接続オプションを実装する必要がありますか?
A. VPCピアリング
B. クラウドVPN
C. クラウド相互接続
D. 共有VPC
Answer: A (メーッセージを残す)
https://cloud.google.com/vpc/docs/vpc-peering

最新問題**: 134**
組織は一般データ保護規則（GDPR）に準拠したいと考えています。DevOps チームがヨーロッパ地域でのみ Google Cloud リソースを作成できるようにしたいと考えています。
何をすべきでしょうか?
A. Google Cloud 組織ノードで組織ポリシー制約「リソース サービスの使用を制限する」* を使用します。
B. Identity and Access Management (1AM) のカスタム ロールを使用して、DevOps チームがヨーロッパ地域でのみリソースを作成できるようにします。
C. Google Cloud 組織ノードで組織ポリシー制約「Google Cloud Platform - リソース ロケーションの制限」を使用します。
D. Access Context Manager で Identity-Aware Proxy（IAP）を使用して、Google Cloud リソースの場所を制限します。
Answer: C (メーッセージを残す)
* Google Cloud 組織ノードで組織ポリシー制約「Google Cloud Platform - リソース ロケーション制限」を使用します。この組織ポリシー制約を使用すると、リソースを作成できるロケーションを制限できます。この制約をヨーロッパリージョンのみに設定すると、GDPR やその他の地域規制への準拠が確保されます。
* 実装: これを実装するには、組織ポリシーに制約constraints/gcp.resourceLocationsを設定する必要があります。europe-west1やeurope-west4などの許可されたリージョンを指定することで、これらのロケーションにのみリソースが作成されるようにすることができます。

参考文献
* リソースの場所の制限に関するドキュメント
* Google Cloud における GDPR コンプライアンス

最新問題**: 135**
組織の Cloud Storage バケットのデータがインターネット上で公開されないようにしたいと考えています。これをすべての Cloud Storage バケットに適用したいと考えています。どうすればよいでしょうか？
A. エンドユーザーから所有者のロールを削除し、Cloud Data Loss Prevention を構成します。
B. エンドユーザーから所有者の役割を削除し、組織のポリシーでドメイン制限の共有を適用します。
C. 均一なバケットレベルのアクセスを構成し、組織ポリシーでドメイン制限の共有を適用します。
D. すべてのロールから *.setIamPolicy 権限を削除し、組織ポリシーでドメイン制限の共有を適用します。
Answer: C (メーッセージを残す**)**
* 均一なバケットレベルのアクセス: すべての Cloud Storage バケットに対して均一なバケットレベルのアクセスを有効にします。
この機能により、アクセス制御がバケット レベルで一貫して適用されるため、管理が簡素化され、セキュリティが向上します。
* ドメイン限定共有：組織ポリシーを通じてドメイン限定共有を適用します。このポリシーにより、組織のドメイン内のユーザーのみがバケット内のデータにアクセスでき、データの公開を防止できます。
* ポリシーの適用：必要なIAMポリシーを適用し、バケットがパブリックアクセスを許可されていないことを確認します。これらの設定を組み合わせることで、Cloud Storageバケット内のデータは非公開のままとなり、組織内の承認されたユーザーのみがアクセスできるようになります。参考資料：
* Google Cloud - 均一なバケットレベルのアクセス
* Google Cloud - 組織ポリシー サービス

最新問題**: 136**
Compute Engine VM のみを 1 日に 1 回使用する新しいアプリケーションを開発しています。このアプリケーションは 5 つの異なるバッチジョブを実行します。各バッチジョブには、アプリケーション外部の Google Cloud リソースに対する専用の権限セットが必要です。バッチジョブに対して、最小権限の原則に準拠した安全なアクセス コンセプトを設計する必要があります。どうすればよいでしょうか？
A. 1. バッチ ジョブを調整するための一般的なサービス アカウント「g-sa」を作成します。
* 2. バッチジョブごとに1つのサービスアカウント（b-sa-[1-5]）を作成し、個々のバッチジョブを実行するために必要な権限のみをサービスアカウントに付与します。
* 3. g-saにサービスアカウントトークン作成者のロールを付与します。g-saを使用してb-sa-[1-5]の短期アクセストークンを取得し、b-sa-[1-5]の権限でバッチジョブを実行します。
B. 1. バッチジョブを実行するための一般的なサービス アカウント **g-sa" を作成します。
* 2 バッチジョブを実行するために必要な権限を g-sa に付与します。
* 3. g-saに付与された権限でバッチジョブを実行する
C. * 1. バッチ ジョブを調整するための一般的なサービス アカウント「g-sa」を作成します。

* 2 バッチジョブごとに1つのサービスアカウントを作成します 'b-sa-[1-5)\ 個々のバッチジョブを実行するために必要な権限のみをサービスアカウントに付与し、各サービスアカウントのサービスアカウントキーを生成します
* 3. サービスアカウントキーをSecret Managerに保存します。g-saにSecret Managerへのアクセスを許可し、b-sa-[1-5]の権限でバッチジョブを実行します。
D. 1. ワークロード ID プールを作成し、バッチジョブごとにワークロード ID プール プロバイダを構成する
* 2 プロバイダーで構成された各 ID にワークロード ID ユーザー ロールを割り当てます。
* 3. バッチジョブごとに1つのサービスアカウント（b-sa-[1-5]）を作成し、個々のバッチジョブを実行するために必要な権限のみをサービスアカウントに付与します。
* 4 各プロバイダーの資格情報設定ファイルを生成します。これらのファイルを使用して、b-sa-[1-5]の権限でバッチジョブを実行します。
Answer: A (メーッセージを残す**)**

最新問題**: 137**
組織では、Cloud Identity と Microsoft Active Directory 間の同期と SAML 連携を実装しています。Google Cloud ユーザー アカウントが不正使用されるリスクを軽減したいと考えています。
何をすべきでしょうか?
A. 強力なパスワード設定を含む Cloud Identity パスワード ポリシーを作成し、Google 管理コンソールでセキュリティ キーを使用して 2 段階認証プロセスを設定します。
B. 強力なパスワード設定を含む Cloud Identity パスワード ポリシーを作成し、Google 管理コンソールでテキスト メッセージまたは電話による確認コードを使用した 2 段階認証プロセスを設定します。
C. 強力なパスワード設定を含む Active Directory ドメイン パスワード ポリシーを作成し、Google 管理コンソールでセキュリティ キーを使用して SSO（シングル サインオン）後の 2 段階認証プロセスを設定します。
D. 強力なパスワード設定を含む Active Directory ドメイン パスワード ポリシーを作成し、Google 管理コンソールでテキスト メッセージまたは電話による確認コードを使用して、SSO（シングル サインオン）後の 2 段階認証プロセスを設定します。
Answer: (解答を表示する**)**
* 目標: Google Cloud ユーザー アカウントが侵害されるリスクを軽減します。
* 解決策: セキュリティ キーを使用して、強力なパスワード ポリシーと SSO 後の 2 段階認証を実装します。
* 手順:

* 手順 1: Active Directory で、強力な設定 (複雑さ、長さ、有効期限など) を持つドメイン パスワード ポリシーを構成します。
* ステップ 2: Google 管理コンソールで、セキュリティ設定に移動します。
* ステップ 3: 2 段階認証を有効にし、SSO 後の認証にセキュリティ キーを使用するように設定します。
* ステップ 4: すべてのユーザーがセキュリティ キーを使用して 2 段階認証プロセスに登録していることを確認します。
Active Directory の強力なパスワード ポリシーと、SSO 後の 2 段階認証のセキュリティ キーを使用すると、アカウント侵害に対するセキュリティが強化されます。
参考文献:
* Active Directory パスワードポリシー
* Google 管理コンソールの 2 段階認証プロセス

最新問題**: 138**
組織では、アプリケーションの開発とホスティングに Google Cloud を使用しています。Google が推奨するプラクティスに従い、開発チームと本番環境向けの専用プロジェクトを作成しました。開発チームはカナダとドイツに拠点を置いています。運用チームは現地の法律を遵守するため、ドイツからのみ業務を行っています。Google Cloud API への管理者アクセスをこれらの国と環境に限定する必要があります。どうすればよいでしょうか？
A. 組織レベルで各環境専用のファイアウォールポリシーを作成し、プロジェクトに適用します。位置情報に基づいてアクセスを制限するルールを作成します。
B. 開発プロジェクトと本番環境プロジェクトをすべて別々のフォルダにグループ化します。フォルダの組織ポリシーを有効化し、要件に応じてリソースの配置場所を制限します。
C. 開発プロジェクトと本番環境プロジェクト専用の VPC Service Controls 境界を作成します。それぞれの国からのアクセスを許可するため、異なる上り（内向き）ポリシーを設定します。
D. カナダとドイツの開発者専用のIAMグループを作成します。要件に応じて、開発プロジェクトと本番環境プロジェクトへのアクセスを許可します。
Answer: C (メーッセージを残す**)**
この問題では、地理的な場所（カナダとドイツ）と環境（開発プロジェクトと本番環境プロジェクト）に基づいて、Google Cloud API への管理者アクセスを制限する必要があります。
VPC Service Controls（VPC SC）：VPC Service Controls は、Google Cloud のリソースとサービスの周囲にセキュリティ境界を作成するように設計されています。その主な目的は、データの流出を防ぎ、リクエストのコンテキスト（送信元IP アドレスを含む）に基づいて Google Cloud API へのアクセスを制御することです。
抜粋参照: 「VPC Service Controls は、Identity and Access Management（IAM）に依存しない、Google Cloud サービス向けのセキュリティ防御層を追加します。IAM ではきめ細かい ID ベースのアクセス制御が可能ですが、VPC Service Controls では、境界を越えたデータ送信の制御など、より広範なコンテキストベースの境界セキュリティが可能になります。」(Google Cloud ドキュメント: 「VPC Service Controls の概要」 - https://cloud.google.com/vpc-service-controls/docs/overview) 環境のサービス境界: 開発プロジェクトと本番環境プロジェクトに専用の境界を作成することで、環境を論理的に分離できます。これは、「開発と本番環境の専用プロジェクト」構造と一致します。

地理的制限を伴う上り（イングレス）ポリシー：VPC Service Controls は、「上り（イングレス）ルール」を使用して、サービス境界にリクエストを送信できるユーザーと送信元を定義します。これらの上り（イングレス）ルールは、リクエストの送信元 IP アドレスなど、さまざまな属性に基づいてアクセスを許可するように設定できます。カナダとドイツに対応する特定の IP 範囲からのアクセスを許可することで、これらの国からの API への管理アクセスを効果的に制限できます。「アクセスレベル」（IP サブネットや地理的な発信元を含む）を定義し、上り（イングレス）ポリシーに適用できます。
抜粋リファレンス：「リソースへの上り（内向き）を許可するには、VPC Service Controls はソースと identityType 属性を AND 条件として評価します。accessLevel またはリソース（Google Cloud プロジェクトまたは VPC ネットワーク）を指定するか、accessLevel 属性を * に設定する必要があります。」（Google Cloud ドキュメント：「上り（内向き）ルールと下り（外向き）ルール | VPC Service Controls」- https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules）抜粋リファレンス「アクセスレベルの基盤となるコンテキストアウェア アクセスについて）：「アプリへのアクセスには、IP、デバイス、地理的な発信元、カスタム アクセスレベル属性など、さまざまな種類のコンテキストアウェア アクセス ポリシーを作成できます。」（Google Workspace 管理者ヘルプ：「コンテキストアウェア アクセスでビジネスを保護する」- https://support.google.com/a/answer/9275380) - これは Workspace アプリを参照していますが、Access Context Manager (VPC SC で使用される) の基盤となるメカニズムは地理的制限をサポートしています。
他のオプションを評価してみましょう。
A) 専用のファイアウォールポリシーを作成し、位置情報に基づいてアクセスを制限します。VPC ファイアウォールルールは、VPC 内のネットワークレベル（レイヤー 3/4）で動作します。VM インスタンス間またはネットワークサービスにおけるインターネットとの間のトラフィックを制御します。VPC 外部からの Google Cloud API への管理者アクセス（コンソール経由や gcloud CLI 呼び出し経由など）を直接制御することはありません。
B). フォルダの組織ポリシーを有効化し、リソースの場所を制限します。リソースの場所の制限という組織ポリシー制約は、新しいリソースを作成または保存できる場所（例データレジデンシー要件）を制限します。管理者がこれらのリソースを管理したりAPIにアクセスしたりするために接続できる場所は制限しません。
D). 専用のIAMグループを作成する…アクセス権限の付与：IAM（Identity and Access Management）は、誰がどのリソースにアクセスでき、どのようなアクションを実行できるかを制御します。アクセス元（国固有のIPアドレスなど）をネイティブに制御することはできません。
したがって、ソース IP / アクセスレベルに基づいて適切に構成された上りポリシーを備えた VPC Service Controls は、地理的な場所と環境によって Google Cloud API への管理者アクセスを制限するための推奨される最も効果的な方法です。

最新問題: **139**
オンプレミス環境からBigQueryデータセットへの日々のETLプロセスにおいて、機密性の高い個人情報（PII）がGoogle Cloud環境に取り込まれていることが判明しました。このデータを秘匿化してPIIを難読化する一方で、データ分析のために再識別する必要があります。ソリューションではどのコンポーネントを使用すべきですか（2つ選択してください）。
A. AES-SIV を使用した確定的暗号化によるクラウド データ損失防止
B. クラウドキー管理サービス

C. シークレットマネージャー
D. 暗号化ハッシュを使用したクラウドデータ損失防止
E. 自動テキスト編集機能を備えたクラウドデータ損失防止
Answer: A,E (メーッセージを残す)

最新問題**: 140**
機密データを保護し、非機密データの鍵管理の複雑さを軽減する保存時暗号化戦略を実装する必要があります。ソリューションには以下の要件があります。
* 機密データのキーのローテーションをスケジュールします。
* 機密データの暗号化キーがどの領域に保存されるかを制御します。
* 機密データと非機密データの両方の暗号化キーにアクセスするための遅延を最小限に抑えます。
何をすべきでしょうか?
A. Cloud External Key Manager を使用して、非機密データと機密データを暗号化します。
B. Cloud Key Management Service を使用して、非機密データと機密データを暗号化します。
C. 機密性が低いデータは Google のデフォルトの暗号化で暗号化し、機密データは Cloud External Key Manager で暗号化します。
D. 機密性が低いデータは Google のデフォルトの暗号化で暗号化し、機密データは Cloud Key Management Service で暗号化します。
Answer: D (メーッセージを残す)
説明
Googleは、FIPS 140-2レベル1認定モジュールであるBoringCryptoを組み込んだ共通暗号ライブラリTinkを使用して、ほぼすべてのGoogle Cloudプロダクトで一貫した暗号化を実現しています。鍵の保管場所とローテーションスケジュールを柔軟に管理するため、非機密データにはGoogle提供の鍵を使用し、機密データはCloud Key Management Serviceで暗号化します。

最新問題**: 141**
2 つの VPC ネットワークを接続するための VPC ピアリングの使用に関連する 2 つのセキュリティ特性はどれですか。
（2つ選択してください。）
A. ピアリングされたネットワークのルート、ファイアウォール、VPN の集中管理
B. 非推移的なピアリングネットワーク。直接ピアリングされたネットワークのみが通信できる。
C. 異なる Google Cloud Platform 組織に属するネットワークをピアリングする機能
D. ピアリングされたネットワークから別のピアリングされたネットワークへのタグを使用して作成できるファイアウォール ルール
E. ピアネットワーク間で特定のサブネットを共有する機能
Answer: B,C (メーッセージを残す)
* 目標: VPC ピアリングのセキュリティ特性を理解する。
* セキュリティ特性:

* 非推移的ピアリング :VPC ピアリング接続は非推移的です。つまり、ピアリングは 2 つの VPC ネットワーク間のみで行われます。VPC A が VPC B とピアリングされ、VPC B が VPC C とピアリングされている場合、直接ピアリング接続が確立されない限り、VPC A は VPC C と通信できません。
* 組織間ピアリング: VPC ピアリングを使用すると、異なる Google Cloud Platform 組織間で VPC ネットワークを接続し、異なる組織単位間でのプライベート通信を容易にすることができます。
これらの特性により、意図しないデータの公開を防ぎながら、VPC ネットワーク間の制御された安全な接続が保証されます。
参考文献:
* GCP VPC ピアリングのドキュメント
* VPC ネットワーク ピアリングの概要

最新問題**: 142**
エンジニアリングチームが、インターネット上で公開するウェブアプリケーションをリリースしようとしています。このウェブアプリケーションは複数のGCPリージョンでホストされており、URLリクエストに基づいてそれぞれのバックエンドにリダイレクトされます。
あなたのチームは、アプリケーションがインターネット上に直接公開されることを避け、悪意のある IP アドレスの特定のリストからのトラフィックを拒否したいと考えています。これらの要件を満たすには、どのソリューションを実装する必要がありますか?
A. クラウドアーマー
B. ネットワーク負荷分散
C. SSLプロキシ負荷分散
D. NATゲートウェイ
Answer: A (メーッセージを残す**)**
説明/参考資料: https://cloud.google.com/armor/docs/security-policy-concepts

最新問題**: 143**
組織ではActive Directoryを使用しており、Security Assertion Markup Language （SAML）の設定を希望しています。すべてのユーザーに対してシングルサインオン （SSO）を設定し、適用する必要があります。
何をすべきでしょうか?
A. 1. SAML プロファイルの割り当てを管理します。
* 2. Active Directory (AD) テナントで OpenID Connect (OIDC) を有効にします。
* 3. ドメインを検証します。
B. 1. 新しい SAML プロファイルを作成します。
* 2. X.509証明書をアップロードします。
* 3. パスワード変更URLを有効にします。
* 4. IdP でエンティティ ID と ACS URL を設定します。
C. 1- 新しい SAML プロファイルを作成します。
* 2. サインイン ページとサインアウト ページの URL を入力します。
* 3. X.509証明書をアップロードします。
* 4. IdPでエンティティIDとACS URLを設定する

D. 1. Active Directory (AD) テナントで OpenID Connect (OIDC) の前提条件を構成する
* 2. ADドメインを確認します。
* 3. SAML を使用するユーザーを決定します。
* 4. 事前設定されたプロファイルを、選択した組織単位 (OU) とグループに割り当てます。
Answer: (解答を表示する**)**
説明
Active Directory を使用している組織で SAML ベースのシングル サインオン (SSO) を構成する場合の一般的な手順としては、SAML プロファイルの設定、サインインおよびサインアウト プロセスに必要な URL の指定、安全な通信のための X.509 証明書のアップロード、アイデンティティ プロバイダー (この場合は Active Directory) でのエンティティ ID とアサーション コンシューマー サービス (ACS) URL の設定などがあります。

最新問題**: 144**
現在の保守契約の期限が切れる前に、社内データセンターからGCPへレガシーアプリケーションを移行する責任を負っています。アプリケーションがどのポートを使用しているかは不明で、確認できるドキュメントもありません。環境をリスクにさらすことなく移行を完了したいと考えています。
何をすべきでしょうか?
A. 『リフト＆シフト」アプローチを用いて、アプリケーションを独立したプロジェクトに移行します。VPCファイアウォールルールを使用して、すべての内部TCPトラフィックを有効にします。VPCフローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
B. カスタム ネットワークで 『リフト アンド シフト」アプローチを使用して、アプリケーションを分離されたプロジェクトに移行します。
VPC 内のすべてのトラフィックを無効にし、ファイアウォール ログを確認して、アプリケーションが適切に動作するために許可する必要があるトラフィックを判断します。
C. アプリケーションをGKEクラスタ内のマイクロサービスアーキテクチャにリファクタリングします。ファイアウォールルールを使用して、クラスタ外からのすべてのトラフィックを無効にします。VPCフローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
D. アプリケーションを、分離されたプロジェクト内の Cloud Functions でホストされるマイクロサービス アーキテクチャにリファクタリングします。
ファイアウォールルールを使用して、プロジェクト外からのすべてのトラフィックを無効にします。VPCフローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
Answer: A (メーッセージを残す**)**
説明
『リフト＆シフト」アプローチを用いて、アプリケーションを独立したプロジェクトに移行します。VPCファイアウォールルールを使用して、すべての内部TCPトラフィックを有効にします。VPCフローログを使用して、アプリケーションが適切に動作するために許可する必要があるトラフィックを特定します。

最新問題**: 145**

PCI DSS 要件を満たすために、顧客はすべての送信トラフィックが承認されていることを保証したいと考えています。
追加の補償制御なしでこの要件を満たす 2 つのクラウド オファリングはどれですか?
（2つ選択してください。）
A. App Engine
B. クラウド関数
C. コンピューティングエンジン
D. Google Kubernetes Engine
E. クラウドストレージ
Answer: C,D (メーッセージを残す**)**
App Engine の上り（内向き）ファイアウォール ルールは利用可能ですが、下り（外向き）ルールは現在利用できません。要件 1.2.1 および 1.3.4 に基づき、すべての送信トラフィックが承認されていることを確認する必要があります。SAQ A-EP および SAQ D タイプの加盟店は、代替制御を提供するか、別の Google Cloud プロダクトを使用する必要があります。Compute Engine と GKE が推奨される代替手段です。
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

最新問題**: 146**
会社ではGKEに新しいアプリケーションをデプロイしています。このアプリケーションは顧客の機密データを扱い、厳格なデータ レジデンシー要件が適用されます。データがeurope-west4リージョン内にのみ保存されるようにする必要があります。どうすればよいでしょうか？
A. europe-west4 に GKE クラスターを作成します。ネットワークポリシーを設定して、他のリージョンとの間のトラフィックをすべてブロックします。Kubernetes のロールベースアクセス制御 (RBAC) を使用して、クラスターへのアクセスを制限します。
B. 開発チームにデータ レジデンシー要件についてトレーニングを行い、コード レビューを使用してすべてのリソースが europe-west4 にデプロイされていることを確認します。
C. 組織ポリシーを使用して、GKE クラスタを含むプロジェクトのリソースの場所を europe-west4 に制限します。
D. europe-west4 に GKE クラスターを作成します。GKE のカスタムアドミッションコントローラを使用して、デプロイされたすべてのリソースのリージョンを事前定義された許可リストと照合します。
Answer: (解答を表示する**)**
プラットフォーム レベルでデータ所在地を適用するために、Google Cloud はリソース ロケーション組織ポリシー（constraints/gcp.resourceLocations）を提供しています。6 これは、リソース（GKE クラスタ、永続ディスク、Cloud Storage バケットなど）が特定のリージョン外で作成されるのを防ぐための正式な方法です。
Google Cloud ドキュメント (組織ポリシー - リソースの場所) によると、次のようになります。
リソース ロケーションの制約を使用すると、サポートされているすべての Google Cloud サービスに対して許可されるロケーション（リージョンまたはマルチリージョン）を定義できます。7 このポリシーをプロジェクト レベルまたはフォルダ レベルで設定すると、IAM 権限に関係なく、指定されたリージョン以外のリージョン（例 ローカル リージョン）にユーザーがリソースを作成できないようになります。
例 :ヨーロッパ西部4）。

これが最善の解決策である理由:
* 予防的: ユーザーが他の場所にデプロイしようとすると、API 呼び出し自体がブロックされます。
* 効率的: カスタム コード (オプション D など) や手動レビュー (オプション B) を必要とせず、プロジェクト内のすべてのサービスに適用されます。
* コンプライアンス重視: コンプライアンス担当者に明確な監査証跡と確実な保証を提供します。
参照：
Google Cloud ドキュメント：『リソース ロケーションの組織ポリシー」（https://cloud.google.com/resource-manager/docs/organization-policy/defining-locations）。

最新問題**: 147**
あるお客様は、マネージドインスタンスグループ（MIG）を使用して、機密性の高いワークロードをCompute Engineベースのクラスタに移行したいと考えています。ジョブはバースト的に発生するため、迅速に完了させる必要があります。また、暗号鍵の管理とローテーションも必要となります。
この顧客の要件を満たすには、クラスター上でどのブート ディスク暗号化ソリューションを使用する必要がありますか?
A. 顧客提供の暗号化キー (CSEK)
B. Cloud Key Management Service (KMS) を使用した顧客管理の暗号鍵 (CMEK)
C. デフォルトで暗号化
D. 分析のために Google Cloud Platform (GCP) に転送する前にファイルを事前に暗号化する
Answer: B (メーッセージを残す**)**
マネージド インスタンス グループ (MIG) を使用して Compute Engine ベースのクラスタで暗号鍵を管理およびローテーションするには、Cloud KMS を使用した顧客管理の暗号鍵 (CMEK) が適切なソリューションです。
Cloud KMS を設定する:
Cloud Console に移動し、[セキュリティ] > [暗号化キー] に移動します。
キーリングとキーを作成します。
CMEK を作成して使用する:
Compute Engine インスタンスを作成または更新するときに、CMEK キーを指定します。
コマンド例:
gcloud コンピューティングインスタンスは、example-instance \ --image-family=debian-9 \ --image-project=debian-cloud を作成します。
\ --boot-disk-kms-key=projects/[PROJECT_ID]/locations/global/keyRings/[KEY_RING]/cryptoKeys/[KEY] キーのローテーション:
新しいキー バージョンを作成し、新しいキー バージョンを使用するようにインスタンスを更新することで、Cloud KMS を使用して定期的にキーをローテーションします。
顧客管理暗号化キー（CMEK）
顧客管理暗号化キーの使用

最新問題**: 148**
顧客は別の企業と協力して Compute Engine 上にアプリケーションを構築しています。

お客様は自社のGCP組織内にアプリケーション層を構築し、相手企業は別のGCP組織内にストレージ層を構築しています。これは3層ウェブアプリケーションです。
アプリケーションの各部分間の通信は、いかなる手段によってもパブリック インターネットを通過してはなりません。
どの接続オプションを実装する必要がありますか?
A. クラウド相互接続
B. 共有VPC
C. VPCピアリング
D. クラウドVPN
Answer: D (メーッセージを残す**)**

最新問題**: 149**
組織には、Google Cloud API にアクセスする必要があるオンプレミス ホストがあります。これらのホスト間にプライベート接続を適用して、コストを最小限に抑え、運用効率を最適化する必要があります。何をすべきでしょうか?
A. すべてのオンプレミス トラフィックを、プライベート Google アクセスが有効になっている VPC への IPsec VPN トンネル経由で Google Cloud にルーティングします。
B. オンプレミスのホストと VPC 間の VPC ピアリングをインターネット経由で設定します。
C. すべてのアプリケーションに Cloud Key Management を使用してデータを暗号化することを義務付けるセキュリティ ポリシーを適用します。
ネットワーク経由で送信する前に、サービス (KMS) キーを確認してください。
D. すべてのオンプレミス トラフィックを、専用またはパートナー相互接続を介して、プライベート Google アクセスが有効になっている VPC に Google Cloud にルーティングします。
Answer: (解答を表示する**)**
オンプレミスホストとGoogle Cloud API間のプライベート接続を、コストと運用効率を最適化しながら確保するには、専用またはパートナー相互接続の使用が最適なソリューションです。この設定により、プライベートIPアドレスによる信頼性の高い高帯域幅の接続が確保されます。
* 相互接続タイプを選択: 帯域幅のニーズと Google Cloud のロケーションへの近さに基づいて、Dedicated Interconnect と Partner Interconnect のどちらかを選択します。
* 相互接続の設定:
* Dedicated Interconnect の場合は、Google Cloud Console から回線を注文します。
* パートナー相互接続の場合は、サポートされているサービス プロバイダーを選択し、そのプロバイダーを通じて接続を注文します。
* VPC とプライベート Google アクセスを構成する:
* VPC でプライベート Google アクセスを有効にして、オンプレミス ホストが Google API にプライベートにアクセスできるようにします。
* 「VPC ネットワーク」-> 「プライベート Google アクセス」に移動し、サブネットに対して有効にします。
* 接続を確立する: ネットワーク チームおよび (該当する場合) パートナー相互接続プロバイダーと協力して、物理接続と論理接続を設定します。

* 接続テスト: オンプレミス ホストがプライベート IP アドレスを使用して Google Cloud サービスにアクセスできることを確認します。
参考文献:
* Google Cloud Interconnect の概要
* プライベートGoogleアクセスの設定

最新問題: **150**
DevOpsチームは、Google Kubernetes Engine上で実行する新しいコンテナを作成します。アプリケーションはインターネットに接続するため、コンテナの攻撃対象領域を最小限に抑えたいと考えています。
彼らは何をすべきでしょうか?
A. Cloud Build を使用してコンテナ イメージをビルドします。
B. 小さなベースイメージを使用して小さなコンテナを構築します。
C. コンテナ レジストリから使用されていないバージョンを削除します。
D. 継続的デリバリー ツールを使用してアプリケーションをデプロイします。
Answer: B (メーッセージを残す**)**
通常、小さなコンテナは、大きなベースイメージを使用するコンテナと比較して、攻撃対象領域が小さくなります。
https://cloud.google.com/blog/products/gcp/kubernetes-best-practices-how-and-why-to-build- 小さなコンテナイメージ

最新問題: **151**
ある組織のセキュリティおよびリスク管理チームは、Google Cloud Platform（GCP）で実行している特定の本番環境ワークロードに対する責任の所在と、Googleの責任の所在について懸念を抱いています。彼らは主にApp EngineをはじめとするGoogle CloudのPlatform-as-a-Service（PaaS）サービスを使用してワークロードを実行しています。
App Engine を使用する際に、テクノロジー スタック内のどの領域に主な責任として重点を置く必要がありますか。
A. 保存されているすべてのデータを暗号化する
B. XSSおよびSQLi攻撃からの防御
C. ゲストOSの最新のアップデートとセキュリティパッチを管理します
D. VPC フローログの設定と監視
Answer: A (メーッセージを残す**)**

最新問題: **152**

Data Warehouse」というフォルダに含まれる一連のGoogle Cloudプロジェクトを管理しています。新しいデータ分析チームが、Data Warehouseフォルダ内のプロジェクトに含まれるすべてのBigQueryデータのデータ分析を実行することが承認されました。このチームはデータの読み取り権限のみを持ち、変更や削除の権限は持たないようにする必要があります。最小権限の原則を遵守しながら、アクセス権限のプロビジョニングに伴う運用上のオーバーヘッドを削減したいと考えています。どうすればよいでしょうか？

A. データ ウェアハウス フォルダ内の各プロジェクト内の各 BigQuery データセットに対して、データセット レベルで BigQuery データ閲覧者ロールを付与します。

B. データ ウェアハウス フォルダで BigQuery データ閲覧者ロールを付与します。

C. データ ウェアハウス フォルダ内の各プロジェクトに対して、プロジェクト レベルで BigQuery データ閲覧者ロールを付与します。

D. データ ウェアハウス フォルダで BigQuery メタデータ閲覧者ロールを付与します。

Answer: B (メーッセージを残す)

正確な抜粋からの包括的かつ詳細な説明：

要件は、必要な最小限の権限のロールを使用して、必要なすべてのリソースを含むリソース階層の最上位でアクセスを許可することによって満たされます。

最小権限ロール :チームはデータを読み取る権限を持ち、変更や削除は行いません。roles/bigquery.dataViewer ロールは、データへの読み取り専用アクセスに必要な最小権限ロールです。

運用オーバーヘッドを最小限に抑える: フォルダー レベルでロールを付与すると、そのフォルダー内のすべての現在および将来のプロジェクトにアクセス権が自動的に継承されるため、プロジェクト (C) またはデータセット (A) ごとにロールを付与する場合と比較して、運用オーバーヘッドが大幅に削減されます。

スコープ: フォルダ スコープ (データ ウェアハウス フォルダ) は、フォルダ内のプロジェクトにあるすべての BigQuery データのコンテナであり、アクセスを許可する理想的な単一ポイントになります。

抜粋:

「IAM ロールはリソース階層に継承されます。フォルダレベルでロールを付与すると、そのフォルダ内のすべてのプロジェクト（将来作成されるプロジェクトを含む）でプリンシパルにそのロールが付与されます。」(出典 10.1)

BigQueryデータ閲覧者（roles/bigquery.dataViewer）ロールは、BigQueryのテーブルとビュー内のデータを読み取る権限を付与します。読み取り専用タスクに対する最小権限の原則に従い、データの変更または削除の権限は付与しません。（出典10.2）

最新問題: **153**

HTTPS リソースにアクセスするために、Identity and Access Management (IAM) ユーザーに付与する必要がある Identity-Aware Proxy ロールはどれですか?

A. IAP保護トンネルユーザー

B. セキュリティレビュー担当者

C. サービスブローカーオペレーター
D. IAP で保護された Web アプリ ユーザー
Answer: (解答を表示する**)**

最新問題**: 154**
顧客の社内セキュリティ チームは、Cloud Storage 上のデータを暗号化するために独自の暗号化キーを管理する必要があり、顧客指定の暗号化キー (CSEK) を使用することを決定しました。
チームはこのタスクをどのように完了する必要がありますか?
A. 暗号化キーを Cloud Storage バケットにアップロードし、オブジェクトを同じバケットにアップロードします。
B. gsutil コマンドライン ツールを使用してオブジェクトを Cloud Storage にアップロードし、暗号化キーの場所を指定します。
C. Google Cloud Platform Console で暗号化キーを生成し、指定されたキーを使用してオブジェクトを Cloud Storage にアップロードします。
D. オブジェクトを暗号化し、gsutil コマンドライン ツールまたは Google Cloud Platform Console を使用してオブジェクトを Cloud Storage にアップロードします。
Answer: B (メーッセージを残す**)**
説明
https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#gsutil

最新問題**: 155**
貴社は、CIS Google Cloud Computing Foundations Benchmark v1 3 0 (CIS Google Cloud Foundation 1 3)に基づく継続的な評価を希望しています。一部のコントロールは貴社とは無関係であり、評価において除外する必要があります。関連するコントロールのみが評価されるように、自動化されたシステムまたはプロセスを構築する必要があります。
何をすべきでしょうか?
A. 外部監査会社に、必要なCISベンチマークを含む独立したレポートの提出を依頼してください。監査の範囲において、一部のコントロールは不要であり、無視する必要があることを明確にしてください。
B. Security Command Center (SCC) Premium をアクティブ化します。SCC でのセキュリティ検出結果をミュートして評価されないようにするルールを作成します。
C. Security Command Center (SCC) からのすべての検出結果を CSV ファイルにダウンロードします。ファイル内の CIS Google Cloud Foundation 1 3 の一部である検出結果をマークします。会社にとって無関係で範囲外のエントリは無視します。
D. 無関係なすべてのセキュリティ検出結果を、セキュリティ例外を示すタグと値でマークします。マークされたすべての検出結果を選択し、表示されるたびにコンソールでミュートします。Security Command Center (SCC) Premium をアクティブ化します。
Answer: B (メーッセージを残す**)**

最新問題**: 156**

ある組織が、オンプレミス環境からGoogle Cloud Platform（GCP）へのインフラストラクチャ移行を開始しています。組織が最初に取り組むべきステップは、現在使用しているデータバックアップおよび災害復旧ソリューションをGCPに移行することです。組織のオンプレミスの本番環境は、GCPへの移行に向けた次の段階となります。オンプレミス環境とGCP間の安定したネットワーク接続も実装中です。
組織はどの GCP ソリューションを使用すべきでしょうか?
A. Cloud VPN 経由で継続的に更新されるデータ パイプライン ジョブを使用する BigQuery
B. Cloud Interconnect 経由でスケジュールされたタスクと gsutil を使用する Cloud Storage
C. Cloud Interconnect 経由で永続ディスクを使用する Compute Engine 仮想マシン
D. Cloud VPN 経由で定期的にスケジュールされたバッチアップロード ジョブを使用する Cloud Datastore
Answer: B (メーッセージを残す**)**
* 目標: 進行中のデータ バックアップおよび災害復旧ソリューションを GCP に移行します。
* 解決策: スケジュールされたタスクと gsutil を使用して Cloud Storage を使用します。
* 手順:
* ステップ 1: オンプレミス環境と GCP 間の安定したネットワーク接続を確保するために、Cloud Interconnect を設定します。
* ステップ 2: バックアップを保存するための Cloud Storage バケットを作成します。
* ステップ 3: Cloud Storage のコマンドライン ツールである gsutil を使用して、データ転送用のスクリプトを作成します。
* ステップ 4: cron ジョブまたは別のスケジュール ツールを使用してこれらのスクリプトをスケジュールし、バックアップ プロセスを自動化します。
スケジュールされたタスクと gsutil を備えた Cloud Storage を使用すると、Cloud Interconnect によって提供される安定した接続を活用しながら、効率的で信頼性の高いバックアップと障害復旧を実現できます。
参考文献:
* クラウドストレージのドキュメント
* gsutil ツールのドキュメント
* クラウド相互接続ドキュメント

最新問題**: 157**
あなたの会社ではGoogle Cloudを利用しており、ネットワーク資産を公開しています。ソフトウェアツールを使用して、これらの資産を検出し、セキュリティ監査を最短時間で実施したいと考えています。
何をすべきでしょうか?
A. 組織内のすべてのインスタンスでプラットフォーム セキュリティ スキャナーを実行します。
B. 保留中の監査について Google に通知し、確認を待ってからスキャンを実行します。
C. 監査を実行するには、Google 認定のセキュリティ ベンダーに問い合わせてください。
D. Cloud Asset Inventory を使用してすべての外部資産を識別し、それらに対してネットワーク セキュリティ スキャナーを実行します。
Answer: D (メーッセージを残す**)**
説明
Cloud Asset Inventory :Cloud Asset Inventoryを使用すると、Google Cloud環境内のすべての外部アセットとリソースを迅速に特定できます。これには、プロジェクト、インスタンス、ストレージバケットなどの情報が含ま

れます。このステップは、監査の範囲を把握するために非常に重要です。ネットワーク セキュリティ スキャナ：
外部資産を特定したら、ネットワークセキュリティスキャナーを実行して、これらの資産のセキュリティを評価できます。ネットワークセキュリティスキャナーは、脆弱性や潜在的なセキュリティリスクを迅速に特定するのに役立ちます。

最新問題: **158**
組織のインフラストラクチャをGCPに移行する際には、多数のユーザーがGCP Consoleにアクセスする必要があります。Identity Managementチームは既にユーザー管理のための確立された方法を確立しており、既存のActive DirectoryまたはLDAPサーバーと既存のSSOパスワードを引き続き使用したいと考えています。
何をすべきでしょうか?
A. Google ドメインのデータを既存の Active Directory または LDAP サーバーと手動で同期します。
B. Google Cloud Directory Sync を使用して、Google ドメイン内のデータを既存の Active Directory または LDAP サーバーと同期します。
C. ユーザーは、オンプレミスの Kerberos 準拠 ID プロバイダの認証情報を使用して、GCP Console に直接サインインします。
D. ユーザーは OpenID (OIDC) 互換の IdP を使用してサインインし、認証トークンを受け取り、そのトークンを使用して GCP コンソールにログインします。
Answer: (解答を表示する**)**
説明
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-configuring-single-sign-on

最新問題: **159**
臨床試験を実施している会社では、BigQuery に保存されている最近の研究結果を分析する必要があります。薬剤が投与された期間には、開始日と終了日が含まれています。期間データは分析にとって重要ですが、特定の日付によって特定のバッチが特定され、バイアスが生じる可能性があります。各行の開始日と終了日を難読化し、期間データを保持する必要があります。
何をすべきでしょうか?
A. バケット化を使用して、初期値に基づいて値を事前に決定された日付にシフトします。
B. TimePartConfigを使用して各日付フィールドから日付を抽出し、ランダムな月と年を追加します。
C. コンテキストをテスト対象の一意のIDに設定して日付シフトを使用します。
D. フォーマット保持暗号化(FPE)のFFXモードを使用し、データの一貫性を維持します。
Answer: A (メーッセージを残す**)**
説明
日付シフト技術は、一連の日付をランダムにシフトしますが、期間の順序と期間は維持されます。日付シフトは通常、個人または団体の文脈に基づいて行われます。つまり、各個人の日付は、その個人に固有の時間量だけシフトされます。

最新問題: **160**

ある企業は、さまざまな Google Cloud Platform リージョンに冗長メール サーバーを保有しており、場所に基づいて顧客を最も近いメール サーバーにルーティングしたいと考えています。
企業はどのようにこれを達成すべきでしょうか?
A. TCP プロキシ負荷分散を、ポート 995 でリッスンするグローバル負荷分散サービスとして構成します。
B. 場所に基づいてトラフィックを転送する転送ルールを使用して、TCP ポート 995 をリッスンする Network Load Balancer を作成します。
C. HTTP(S) ロードバランサによるクロスリージョン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ルーティングします。
D. Cloud CDN を使用して、クライアント IP アドレスに基づいてメール トラフィックを最も近い元のメール サーバーにルーティングします。
Answer: A (メーッセージを残す**)**
説明
https://cloud.google.com/load-balancing/docs/tcp
TCP プロキシ ロードバランシングは、グローバルに分散された GFE に実装されています。ネットワーク サービス ティアのプレミアム ティアを選択した場合、TCP プロキシ ロードバランサはグローバルになります。プレミアム ティアでは、バックエンドを複数のリージョンにデプロイでき、ロードバランサはユーザー トラフィックを、キャパシティのある最も近いリージョンに自動的にリダイレクトします。スタンダード ティアを選択した場合、TCP プロキシ ロードバランサは単一リージョン内のバックエンド間でのみトラフィックをリダイレクトできます。
https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing

最新問題**: 161**
IPパケットデータに無効なコンテンツや悪意のあるコンテンツが含まれていないか検査する任務を負っています。どうすればよいでしょうか？
A. パケットミラーリングを使用して、特定のVMインスタンスとの間のトラフィックをミラーリングします。ミラーリングされたトラフィックを分析するセキュリティソフトウェアを使用して検査を実行します。
B. VPC 内のすべてのサブネットに対して VPC フローログを有効にします。Cloud Logging を使用してフローログデータの検査を実行します。
C. VPC 内の各 VM インスタンスに Fluentd エージェントを設定します。Cloud Logging を使用してログデータの検査を実行します。
D. ログデータの検査を実行するように Google Cloud Armor アクセス ログを構成します。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/vpc/docs/パケットミラーリング
パケットミラーリングは、Virtual Private Cloud (VPC) ネットワーク内の指定されたインスタンスのトラフィックを複製し、検査のために転送します。パケットミラーリングは、ペイロードやヘッダーを含むすべてのトラフィックとパケットデータをキャプチャします。

最新問題**: 162**
本番環境プロジェクトのすべての Google Cloud リソースを監査しています。ファイアウォール ルールを変更できるすべてのプリンシパルを特定したいと考えています。

何をすべきでしょうか?
A. Policy Analyzer を使用して、compute、firewalls、compute の作成、firewalls、compute の作成、firewalls の削除の権限を照会します。
B. セキュリティ コマンド センターの 『セキュリティ ヘルス分析 - ファイアウォールの脆弱性の検出』を参照します。
C. Policy Analyzer を使用して、compute、firewalls、list の compute、firewalls、get の権限を照会します。
D. ファイアウォール インサイトを使用して、ファイアウォール ルールの使用パターンを把握します。
Answer: A (メーッセージを残す)
ファイアウォール ルールを変更できるすべてのプリンシパルを特定するには、Google Cloud プロジェクト内のファイアウォール ルールを変更する権限を持つユーザーまたはサービス アカウントを特定する必要があります。適切な権限は、compute.firewalls.create と compute.firewalls.delete です。これらの権限により、ユーザーはそれぞれファイアウォール ルールを作成および削除できます。
Google Cloud の Policy Analyzer ツールを使用すると、IAM ポリシーをクエリして分析し、特定の権限を持つプリンシパルを特定できます。Policy Analyzer を使用すると、compute.firewalls.create および compute.firewalls.delete 権限を持つすべてのプリンシパルを効果的に特定できます。
* ポリシー アナライザーを開く: Google Cloud Console にアクセスし、[IAM と管理] に移動して、[ポリシー アナライザー] を選択します。
* クエリの設定: compute.firewalls.create および compute の権限を指定して新しいクエリを作成します。ファイアウォールを削除します。
* クエリの実行: クエリを実行して、これらの権限を持つプリンシパルのリストを取得します。
* 結果の確認: 結果を分析して、ファイアウォール ルールを変更する権限を持つすべてのユーザーとサービス アカウントを特定します。
この方法により、ファイアウォール ルールを変更できるすべてのプリンシパルの包括的なリストが得られるため、監査とセキュリティ体制が強化されます。
参考文献:
* Google Cloud Policy Analyzer のドキュメント
* Google Cloud IAM ドキュメント

最新問題**: 163**
あなたはセキュリティ チームの一員であり、プロジェクト A の Cloud Storage バケットがプロジェクト B からのみ読み取り可能であることを保証したいと考えています。また、ユーザーが正しい認証情報を持っている場合でも、ネットワーク外部の Cloud Storage バケットから Cloud Storage バケット内のデータにアクセスしたり、そのバケットにデータをコピーしたりできないようにしたいと考えています。
何をすべきでしょうか?
A. VPC Service Controls を有効にし、プロジェクト A と B で境界を作成し、Cloud Storage サービスを含めます。
B. Cloud Storage バケットでドメイン制限共有組織ポリシーとバケット ポリシーのみを有効にします。
C. 厳格なファイアウォール ルールを使用してプロジェクト A および B のネットワークでプライベート アクセスを有効にし、ネットワーク間の通信を許可します。

D. 厳格なファイアウォール ルールを使用してプロジェクト A と B のネットワーク間の VPC ピアリングを有効にし、ネットワーク間の通信を許可します。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/vpc-service-controls/docs/overview#isolate

最新問題**: 164**
チームは、本番環境プロジェクトで実行されている Compute Engine インスタンスにパブリック IP アドレスが付与されていないことを確認したいと考えています。フロントエンド アプリケーションの Compute Engine インスタンスにはパブリック IP が必要です。プロダクト エンジニアには、リソースを変更するための編集者ロールが付与されています。チームはこの要件を強制したいと考えています。
あなたのチームはこれらの要件をどのように満たすべきでしょうか?
A. 本番環境プロジェクトの VPC ネットワークでプライベート アクセスを有効にします。
B. エディター ロールを削除し、エンジニアに Compute Admin IAM ロールを付与します。
C. フロントエンド Compute Engine インスタンスに対してパブリック IP のみを許可するように組織ポリシーを設定します。
D. パブリック IP を持つサブネットとパブリック IP を持たないサブネットの 2 つを持つ VPC ネットワークを設定します。
Answer: (解答を表示する**)**
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints#constraints-for-specific-services

最新問題**: 165**
あなたは会社のために新しい Google Cloud 組織を作成する責任を負っています。特権管理者アカウントを作成する際に実行する必要がある 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. Google 管理コンソールでアクセス レベルを作成し、スーパー管理者が Google Cloud にログインできないようにします。
B. Google Cloud Console の組織レベルで、特権管理者の Identity and Access Management (IAM) ロールを無効にします。
C. 物理トークンを使用して、多要素認証 (MFA) でスーパー管理者の資格情報を保護します。
D. 資格情報がインターネット経由で送信されないように、プライベート接続を使用してスーパー管理者アカウントを作成します。
E. スーパー管理者ユーザーに、日常業務のために非特権 ID を提供します。
Answer: C,E (メーッセージを残す**)**
説明
https://cloud.google.com/resource-manager/docs/super-admin-best-practices#discourage_super_admin_account_
- セキュリティキーまたはその他の物理的な認証デバイスを使用して2段階認証を強制する - スーパー管理者に別のログインを必要とする別のアカウントを与える

最新問題**: 166**

あなたの会社では最近、サービス アカウント キーの使用を最小限に抑えるためのセキュリティ ポリシーを公開しました。
オンプレミスの Windows ベース アプリケーションは Google Cloud API と連携しています。オンプレミスの ID プロバイダとの Workload Identity Federation (WIF) を実装する必要があります。
何をすべきでしょうか?
A. 名前マシン上で OpenID Connect (OIDC) サービスを使用してワークロード ID プールを設定し、プール内のプリンシパルが Google Cloud サービス アカウントになりすますことができるように arule を構成します。
B. 企業の Active Directory フェデレーション サービス (ADFS) を使用してワークロード ID プールを設定し、プール内のすべてのプリンシパルが Google Cloud サービス アカウントになりすますことを許可します。
C. 企業の Active Directory フェデレーション サービス (ADFS) を使用してワークロード ID プールを設定し、プール内のプリンシパルが Google Cloud サービス アカウントになりすますことができるようにルールを構成します。
D. 同じマシン上に OpenID Connect (OIDC) サービスを使用してワークロード ID プールを設定し、プール内のすべてのプリンシパルが Google Cloud サービス アカウントになりすますことを許可します。
Answer: C (メーッセージを残す**)**

最新問題**: 167**
組織には、外部ウェブ サービスへのアクセスを必要とする Google Cloud アプリケーションがあります。これらのサービスへのアクセスを監視、制御、およびログに記録する必要があります。何をすればよいですか?
A. VPC ファイアウォール ルールを設定して、サービスが必要な外部 Web サービスの IP アドレスにアクセスできるようにします。
B. 特定の外部Webサービスへのアクセスを許可するセキュアWebプロキシを設定し、Webサービスリクエストにプロキシを使用するようにアプリケーションを構成します。
C. Google Cloud Armor を構成して、着信トラフィック パターンで攻撃パターンをチェックし、アプリケーションを監視および保護します。
D. VPC からの出力トラフィックを許可するように Cloud NAT インスタンスを設定します
Answer: B (メーッセージを残す**)**
問題は、Google Cloud アプリケーションが外部ウェブサービスにアクセスする必要があり、このアクセスを監視、制御、およびログに記録する機能が必要であることを示しています。外部ウェブアクセスの監視、制御、ログ記録: これは具体的には、HTTP/S トラフィックを傍受、検査、ログに記録できるプロキシ ソリューションを指します。セキュア ウェブ プロキシ (SWP): Google Cloud のセキュア ウェブ プロキシは、まさにこのユース

ケース向けに設計されています。HTTP(S) トラフィックの明示的なフォワード プロキシとして機能し、組織がきめ細かなアクセス制御を実装し、トラフィックをセキュリティ脅威から検査し、Google Cloud 環境からのすべての送信ウェブ リクエストをログに記録できるようにします。抜粋参照: 「セキュア ウェブ プロキシは、明示的なフォワード プロキシをデプロイおよび管理して、組織の内部リソースをウェブベースの脅威から保護し、外部ウェブ アプリケーションへのアクセスを制御できるマネージド サービスです」および 「セキュア ウェブ プロキシを使用すると、さまざまな属性に基づいてきめ細かなアクセス ポリシーを適用し、プロキシによって処理されるすべての HTTP(S) リクエストをログに記録し、ウェブ トラフィックの脅威を監視できます」(Google Cloud ドキュメント: https://cloudgooglecom/secure-web-proxy) 他の点を評価してみましょう。オプション:
A サービスが必要な外部ウェブサービスの IP アドレスにアクセスできるように VPC ファイアウォール ルールを構成します。VPC ファイアウォール ルールはレイヤ 4（TCP/UDP）とレイヤ 3（IP）で動作します。特定の IP アドレスとポートへのトラフィックを許可または拒否できますが、アプリケーション レイヤで HTTP/S リクエストをモニタリング、制御、またはログに記録することはできません。アクセスされるウェブサービスに対するきめ細かな制御や、リクエストのコンテンツの検査は提供されません。C Google Cloud Armor を構成して、受信トラフィック パターンで攻撃パターンをチェックすることで、アプリケーションをモニタリングおよび保護します。Google Cloud Armor は主に分散型サービス拒否（DDoS）対策およびウェブ アプリケーション ファイアウォール（WAF）サービスです。外部ウェブサービスへの送信アクセスを制御およびログに記録するのではなく、受信脅威（上り トラフィック）からアプリケーションを保護することに重点を置いています。D VPC からの下りトラフィックを許可するように Cloud NAT インスタンスを設定します。Cloud NAT を使用すると、外部 IP アドレスを持たないインスタンスでもインターネットに接続できます。下りは有効ですが、アプリケーション レイヤで特定のウェブサービスをモニタリング、制御、またはログに記録する機能は提供されません。これはネットワーク アドレス変換サービスであり、アプリケーション層プロキシしたがって、セキュア ウェブ プロキシを設定することは、Google Cloud アプリケーションから外部ウェブ サービスへのアクセスを監視、制御、およびログに記録するという要件を満たす最も適切なソリューションです。

最新問題: **168**
DevOpsチームは、Google Kubernetes Engine上で実行する新しいコンテナを作成します。アプリケーションはインターネットに接続するため、コンテナの攻撃対象領域を最小限に抑えたいと考えています。
彼らは何をすべきでしょうか?
A. Cloud Build を使用してコンテナ イメージをビルドします。
B. 小さなベースイメージを使用して小さなコンテナを構築します。
C. コンテナ レジストリから使用されていないバージョンを削除します。
D. 継続的デリバリー ツールを使用してアプリケーションをデプロイします。
Answer: B (メーッセージを残す**)**
Google Kubernetes Engine（GKE）上で実行されるインターネット向けアプリケーションのコンテナの攻撃対象領域を最小限に抑えるには、小さなベースイメージを使用して小さなコンテナを構築するのがベストプラクティスです。このアプローチは、次のような点で役立ちます。
脆弱性の削減: ベースイメージが小さいほど、パッケージと依存関係が少なくなり、攻撃者が悪用する可能性のある潜在的な脆弱性が最小限に抑えられます。

セキュリティの強化: distroless や Alpine Linux などの最小限のベース イメージを使用すると、必要なコンポーネントのみが含まれ、攻撃対象領域が大幅に削減されます。
メンテナンスが容易: コンテナが小さいとメンテナンスや更新が容易になり、不要なコンポーネントを扱うことなくセキュリティ パッチを迅速に適用できます。
実装手順:
最小限のベースイメージを選択します。
gcr.io/distroless/base や alpine などのベースイメージを使用します。
gcr.io/distroless/base から myapp /myapp にコピー CMD ["/myapp"]
コンテナイメージを最適化:
不要なツールとライブラリを削除します。
最終イメージを小さく保つために、マルチステージビルドを使用します。
ベースイメージを定期的に更新する:
最新のセキュリティ パッチを適用してベース イメージを最新の状態に保ちます。
参照：
Distroless イメージ
コンテナ構築のベストプラクティス

最新問題**: 169**
ある企業がデータセンター全体をGoogle Cloud Platformに移行しました。複数のプロジェクトにまたがり、複数の部門が管理する数千ものインスタンスが稼働しています。Google Cloud Platformでどの時点で何が実行されていたか、履歴記録を残しておきたいと考えています。
何をすべきでしょうか?
A. 組織レベルでリソース マネージャーを使用します。
B. Forseti Security を使用してインベントリ スナップショットを自動化します。
C. Stackdriver を使用して、すべてのプロジェクトにわたるダッシュボードを作成します。
D. Security Command Center を使用して、組織全体のすべての資産を表示します。
Answer: B (メーッセージを残す**)**
Google Cloud Platform で実行されていたあらゆる時点の履歴記録を維持するには、Forseti Security を使用してインベントリ スナップショットを自動化する必要があります。Forseti Security は、GCP リソースのインベントリ スナップショットを取得することで、GCP のセキュリティとコンプライアンスを自動化するオープンソース ツールキットです。
ステップバイステップ:
* Forseti Securityをインストールします。
* インストール ガイドに従って、Forseti Security を GCP 環境にデプロイします。
* インベントリを構成する:
* Forseti でインベントリ モジュールを設定し、GCP リソースのスナップショットをキャプチャして保存します。
* スナップショットのスケジュール:
* Forseti の設定を使用して、定期的なインベントリ スナップショットをスケジュールします。
* 履歴データにアクセス:

* Forseti のダッシュボードまたは Forseti データベースを照会して、履歴レコードを確認してアクセスします。
* コンプライアンスと監視: Forseti を使用してコンプライアンスを確保し、時間の経過に伴う変化を監視します。
Forseti セキュリティの概要
在庫モジュール

最新問題: **170**
ブートディスクのソースとして使用できるイメージを制限したい場合、これらのイメージは専用のプロジェクトに保存されます。
何をすべきでしょうか?
A. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。信頼済みプロジェクトを拒否操作の例外としてリストします。
B. リソースマネージャーで、信頼されたプロジェクトのプロジェクト権限を編集します。組織を ロンピューティングイメージユーザー」ロールのメンバーとして追加します。
C. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。許可操作で、信頼されたプロジェクトをホワイトリストとしてリストします。
D. リソースマネージャーで組織の権限を編集します。プロジェクトIDを ロンピューティングイメージユーザー」ロールのメンバーとして追加します。
Answer: A (メーッセージを残す**)**

最新問題: **171**
あなたは、厳格なデータ保護要件を持つ規制業界の組織で働いています。組織はデータをクラウドにバックアップしています。データプライバシー規制を遵守するため、このデータは一定期間のみ保存され、一定期間経過後は削除する必要があります。
ストレージコストを最小限に抑えながら、この規制へのコンプライアンスを自動化したいと考えています。どうすればよいでしょうか？
A. データを永続ディスクに保存し、有効期限が切れたらディスクを削除します。
B. データを Cloud Bigtable テーブルに保存し、列ファミリーに有効期限を設定します。
C. データを BigQuery テーブルに保存し、テーブルの有効期限を設定します。
D. データを Cloud Storage バケットに保存し、バケットのオブジェクト ライフサイクル管理機能を構成します。
Answer: (解答を表示する**)**
Google Cloud Storage は、データの保持と削除のプロセスを自動化し、データ プライバシー規制への準拠を確保しながらストレージ コストを最小限に抑えるオブジェクト ライフサイクル管理機能を提供します。
* ライフサイクル管理 :オブジェクトライフサイクル管理では、一定期間後にオブジェクトを自動的に削除するルールを定義できます。これにより、データは必要な期間のみ保持され、有効期限が切れると削除されます。
* 設定 :ライフサイクルルールを設定することで、オブジェクトの保存期間、作成日、カスタムメタデータなどの条件に基づいてオブジェクトを削除できます。これにより、データの保持期間を正確に制御できます。

* コスト効率: ライフサイクル ポリシーを使用してデータを自動的に削除すると、アクティブに使用するストレージに対してのみ料金を支払うことになるため、ストレージ コストを削減できます。
参考文献
* クラウドストレージオブジェクトのライフサイクル管理

最新問題: **172**
Compute Engine でホストされるウェブアプリケーションをデプロイしています。ビジネス要件により、アプリケーションログは12年間保存され、データは欧州域内に保管されることが義務付けられています。オーバーヘッドを最小限に抑え、費用対効果の高いストレージソリューションを実装したいと考えています。どうすればよいでしょうか？
A. EUROPE-WEST1 リージョンの Google Cloud オペレーション スイートのログバケットに 12 年間のカスタム保持ポリシーを構成します。
B. Pub/Sub トピックを使用して、アプリケーション ログを EUROPE-WEST1 リージョンの Cloud Storage バケットに転送します。
C. EUROPE-WEST1 リージョンにログを保存するための Cloud Storage バケットを作成します。アプリケーションコードを変更して、ログをバケットに直接送信し、効率性を高めます。
D. Google Cloud のオペレーション スイートの Cloud Logging エージェントを使用して、カスタム保持期間を 12 年に設定し、アプリケーション ログを EUROPE-WEST1 リージョンのカスタム ログバケットに送信するように Compute Engine インスタンスを構成します。
Answer: D (メーッセージを残す**)**

最新問題: **173**
あるマネージャーは、コストを最小限に抑えながら、セキュリティイベントログを2年間保存したいと考えています。適切なログエントリを選択するためのフィルターを作成します。
ログはどこにエクスポートすればよいですか?
A. BigQueryデータセット
B. Cloud Storage バケット
C. StackDriver のログ
D. Cloud Pub/Sub トピック
Answer: C (メーッセージを残す**)**
説明/参考資料: https://cloud.google.com/logging/docs/exclusions

最新問題: **174**
あなたは会社のセキュリティ管理者です。Google が推奨するベスト プラクティスに従い、ドメイン制限付き共有の組織ポリシーを実装し、必要なドメインのみがプロジェクトにアクセスできるようにしました。ところが、エンジニアリング チームから、組織ドメイン外の外部パートナーのユーザーにプロジェクト内のリソースへのアクセスを許可できないという報告を受けました。規定のベスト プラクティスに従いながら、パートナーのドメインに対して例外を設定するにはどうすればよいでしょうか。
A. ドメイン制限共有組織ポリシーを無効にします。ポリシー値を すべて許可」に設定します。

B. ドメイン制限共有の組織ポリシーをオフにします。Google の Identity and Access Management（IAM）サービスを使用して、外部パートナーに必要な権限を付与します。
C. ドメイン制限共有の組織ポリシーをオフにします。各パートナーの Google Workspace 顧客 ID を Google グループに追加し、その Google グループを組織ポリシーの例外として追加してから、ポリシーを再度オンにします。
D. ドメイン制限共有の組織ポリシーをオフにします。ポリシーの値を「カスタム」に設定します。各外部パートナーの Cloud Identity または Google Workspace の顧客 ID を組織ポリシーの例外として追加し、ポリシーを再度オンにします。
Answer: D (メーッセージを残す**)**
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy ドメイン制限制約はリスト制約の一種です。Google Workspace のお客様 ID は、ドメイン制限制約の allowed_values リストに追加したり、リストから削除したりできます。ドメイン制限制約では拒否値はサポートされておらず、deny_values リストに ID が含まれている状態で組織ポリシーを保存することはできません。allowed_values にリストされている Google Workspace アカウントに関連付けられているすべてのドメインは、組織ポリシーによって許可されます。それ以外のドメインは、組織ポリシーによって拒否されます。

最新問題**: 175**
貴社の顧客は、契約書と運転免許証をスキャンし、クラウドストレージ内のウェブポータルにアップロードする必要があります。12か月以上経過したファイルから、すべての個人識別情報（PII）を削除してください。また、匿名化されたファイルは保管のためにアーカイブする必要があります。
何をすべきでしょうか?
A. Cloud Storage バケット内のファイルの有効期間 (TTL) を 12 か月に設定し、PII を削除してファイルをアーカイブ ストレージ クラスに移動します。
B. PII を含む Cloud Storage ファイルの暗号化キーの 12 か月の Cloud Key Management Service (KMS) ローテーション期間をスケジュールして、ファイルを匿名化し、元のキーを削除します。
C. 12か月以上前に作成されたファイル内のPIIを匿名化し、別のCloud Storageバケットにアーカイブする Cloud Data Loss Prevention（DLP）検査ジョブを作成します。元のファイルは削除してください。
D. Cloud Storage バケットの Autoclass 機能を設定して PII を匿名化し、12 か月以上経過したファイルをアーカイブし、元のファイルを削除します。
Answer: (解答を表示する**)**

最新問題**: 176**
企業のユーザーアカウントでフィッシング攻撃が増加していることに気付きました。暗号署名を使用してユーザーを認証し、ログインページのURLを検証するGoogle 2段階認証（2SV）オプションを導入したいと考えています。どのGoogle 2SVオプションを使用すべきでしょうか？
A. Titan セキュリティ キー
B. Google プロンプト
C. Google 認証システムアプリ

D. クラウドHSMキー
Answer: A (メーッセージを残す**)**
説明
https://cloud.google.com/titan-security-key
セキュリティ キーは公開キー暗号化を使用してユーザーの ID とログイン ページの URL を検証し、たとえユーザー名とパスワードを入力するよう誘導されたとしても攻撃者がアカウントにアクセスできないようにします。

最新問題**: 177**
組織では最近、Google Kubernetes Engine に新しいアプリケーションをデプロイしました。このアプリケーションを保護するためのソリューションをデプロイする必要があります。ソリューションの要件は次のとおりです。
スキャンは少なくとも週に1回実行する必要があります
クロスサイトスクリプティングの脆弱性を検出できる必要がある
Googleアカウントを使用して認証できる必要があります
どのソリューションを使用すべきでしょうか?
A. Google クラウド アーマー
B. Webセキュリティスキャナー
C. セキュリティヘルス分析
D. コンテナ脅威検出
Answer: B (メーッセージを残す**)**
Web Security Scanner は、Google Cloud にデプロイされたウェブアプリケーションをスキャンし、クロスサイトスクリプティング（XSS）などの一般的な脆弱性を検出するように設計されています。Google アカウントによる認証が可能で、定期的なスキャン実行をスケジュール設定できます。
手順:
* Web セキュリティ スキャナを有効にする: Google Cloud Console で、プロジェクトに対して Web セキュリティ スキャナを有効にします。
* スキャンの構成: スキャン構成を設定し、ターゲット URL、認証の詳細 (Google アカウント)、およびスキャン頻度 (少なくとも週に 1 回) を指定します。
* スキャンの実行と監視: スキャンを実行し、脆弱性の結果を監視して、見つかった問題に対処します。
参考文献:
* Webセキュリティスキャナのドキュメント

最新問題**: 178**
社内で Cloud Data Loss Prevention (DLP) API の導入が進むにつれ、コスト削減のために利用を最適化する必要があります。DLP 対象データは Cloud Storage と BigQuery に保存されます。場所とリージョンはリソース名のサフィックスとして識別されます。
どのようなコスト削減オプションを推奨すべきでしょうか?
A. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットに適切な bytesLimitPerFile 値を設定します。

B. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットの変換単位を最小限に抑えます。
C. rowsLimit と bytesLimitPerFile を使用してデータをサンプリングし、CloudStorageRegexFileSet を使用してスキャンを制限します。
D. FindingLimits と TimespanContfig を使用してデータをサンプリングし、変換単位を最小限に抑えます。
Answer: (解答を表示する**)**
https://cloud.google.com/dlp/docs/inspecting-storage#sampling
https://cloud.google.com/dlp/docs/best-practices-
コスト#関連ファイルのみにファイルのスキャンを制限する

最新問題**: 179**
お客様が社内アプリケーションをGoogle Cloud Platformに移行しています。セキュリティチームは、組織内のすべてのリソースの詳細な可視性を求めています。Resource Managerを使用して、自身を組織管理者として設定します。セキュリティチームには、どのようなCloud Identity and Access Management (Cloud IAM) ロールを付与すべきでしょうか？
A. 組織閲覧者、プロジェクトオーナー
B. 組織閲覧者、プロジェクト閲覧者
C. 組織管理者、プロジェクトブラウザ
D. プロジェクトオーナー、ネットワーク管理者
Answer: B (メーッセージを残す**)**
A は不正解です。プロジェクトオーナーの権限が広すぎるためです。セキュリティチームがプロジェクトに変更を加える必要はありません。
B が正解です。理由は次のとおりです。
- 組織閲覧者は、セキュリティ チームに組織の表示名を表示する権限を付与します。
- プロジェクト閲覧者は、セキュリティ チームにプロジェクト内のリソースを表示する権限を付与します。
C は不正解です。組織管理者の権限が広すぎるためです。セキュリティチームが組織に変更を加える権限は必要ありません。
D は不正解です。プロジェクトオーナーの権限が広すぎるためです。セキュリティチームがプロジェクトに変更を加える必要はありません。
https://cloud.google.com/resource-manager/docs/access-control-org#定義済みロールの使用

最新問題**: 180**
会社の新CEOが最近、2つの部門を売却しました。ディレクターから、これらの部門に関連するGoogle Cloudプロジェクトを新しい組織ノードに移行するよう依頼されました。この移行を行う前に、どのような準備手順が必要ですか (2つ選択してください)。
A. プロジェクト レベルのカスタム Identity and Access Management (1AM) ロールをすべて削除します。
B. 組織ポリシーの継承を禁止します。
C. 移行するプロジェクトで継承された Identity and Access Management (1AM) ロールを識別します。
D. 移行するすべてのプロジェクト用の新しいフォルダーを作成します。

E. 特定の移行プロジェクトを VPC Service Controls の境界とブリッジから削除します。
Answer: C,E (メーッセージを残す**)**
Google Cloud プロジェクトを新しい組織ノードに移行する準備をするには、プロジェクトの現在の構成と依存関係が適切に管理されていることを確認することが重要です。必要な準備手順は次の 2 つです。
* 移行するプロジェクトで継承された Identity and Access Management (IAM) ロールを特定します (C):
* プロジェクトは親リソースからIAMロールを継承します。これらのロールを特定することは、ユーザーがプロジェクトに対して持つ権限とアクセスレベルを把握するために不可欠です。これにより、移行後に適切なロールと権限が正しく適用されることを保証できます。
* VPC Service Controls の境界とブリッジから特定の移行プロジェクトを削除します (E):
* VPC Service Controls は、Google Cloud リソースの周囲にセキュリティ境界を設定し、データ漏洩のリスクを軽減します。プロジェクトを移行する前に、アクセスやネットワーク通信の中断を防ぐため、既存の VPC Service Controls の境界およびブリッジからプロジェクトを削除する必要があります。移行後、プロジェクトを必要な境界に再度追加できます。
参考文献
* Google Cloud IAM ドキュメント
* VPC サービスコントロールのドキュメント

最新問題**: 181**
アプリケーションは、グローバル外部HTTP(S)ロードバランサの背後に、高可用性のクロスリージョンソリューションとしてデプロイされています。複数のIPアドレスからのトラフィックが急増していることに気づきましたが、それらのIPアドレスが悪意のあるものかどうかは不明です。アプリケーションの可用性が懸念されます。これらのクライアントからのトラフィックを、指定した時間間隔で制限したいと考えています。
何をすべきでしょうか?
A. Google Cloud Armor を使用して rate_based_ban アクションを設定し、ban_duration_sec パラメータを指定された時間間隔に設定します。
B. Google Cloud Armor を使用して拒否アクションを構成し、指定された時間間隔内に過剰なリクエストを発行したクライアントを拒否します。
C. 識別された IP アドレスからのトラフィックを制限するために、VPC でファイアウォール ルールを設定します。
D. Google Cloud Armor を使用してスロットル アクションを構成し、指定された時間間隔におけるクライアントあたりのリクエスト数を制限します。
Answer: (解答を表示する**)**

最新問題: **182**
チームは、Compute Engine インスタンスがインターネットや Google API またはサービスにアクセスできないようにする必要があります。
これらの要件を満たすには、どの 2 つの設定を無効のままにしておく必要がありますか? (2 つ選択してください。)
A. パブリックIP
B. IP転送
C. プライベート Google アクセス
D. 静的ルート
E. IAM ネットワーク ユーザー ロール
Answer: C,D (メーッセージを残す)
https://cloud.google.com/vpc/docs/configure-private-google-access

最新問題: **183**
チームは、特定の Compute Engine 仮想マシンインスタンスから指定された Cloud Storage バケットへのデータ転送を認証するためにサービスアカウントを使用しています。エンジニアが誤ってサービスアカウントを削除してしまい、アプリケーションの機能が停止してしまいました。セキュリティを損なうことなく、できるだけ早くアプリケーションを復旧したいと考えています。
何をすべきでしょうか?
A. Cloud Storage バケットの認証を一時的に無効にします。
B. undelete コマンドを使用して、削除されたサービス アカウントを回復します。
C. 削除されたサービス アカウントと同じ名前で新しいサービス アカウントを作成します。
D. 別の既存のサービス アカウントの権限を更新し、その資格情報をアプリケーションに提供します。
Answer: B (メーッセージを残す)
目的: データ転送に使用された削除されたサービス アカウントをすばやく回復します。
解決策: gcloud コマンドライン ツールで使用可能な undelete コマンドを使用して、サービス アカウントを回復します。
手順:
ステップ 1: Google Cloud Console で Cloud Shell を開きます。
手順 2: 削除されたサービス アカウントを一覧表示するには、次のコマンドを実行します。
gcloud iam サービスアカウントリスト --filter="削除済み: true"
ステップ 3: 削除されたサービス アカウントの名前と ID を特定します。
ステップ 4: undelete コマンドを使用してサービス アカウントを回復します。
gcloud iam service-accounts undelete [SERVICE_ACCOUNT_ID]
ステップ 5: サービス アカウントが復元されたことを確認し、必要な権限を再割り当てします。
undelete コマンドを使用すると、セキュリティを損なうことなく、サービス アカウントをすばやく復元し、アプリケーションの機能を再開できます。

参照：
削除されたサービスアカウントの復元
gcloud iam サービスアカウントの削除解除

最新問題: **184**
会社のアプリケーションは、ユーザーが管理するサービス アカウント キーを使用してデプロイされています。Google が推奨するプラクティスに従ってキーをローテーションしたいと考えています。
何をすべきでしょうか?
A. Cloud Shell を開き、gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT を実行します。
B. Cloud Shell を開き、gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT --key=NEW_KEY を実行します。
C. 新しいキーを作成し、アプリケーションで新しいキーを使用します。サービスアカウントから古いキーを削除します。
D. 新しいキーを作成し、アプリケーションで使用します。古いキーはバックアップキーとしてシステムに保存します。
Answer: C (メーッセージを残す**)**
ユーザーが管理するサービスアカウントキーのローテーションには、新しいキーを作成し、新しいキーを使用するようにアプリケーションを更新し、セキュリティを維持するために古いキーを削除するという手順が含まれます。具体的な手順は以下のとおりです。
* 新しい鍵の作成: Google Cloud Console または gcloud コマンドライン ツールを使用して、サービス アカウントの新しい鍵を作成します。これにより、新しい鍵ペアが生成され、秘密鍵が提供されます。
gcloud iam サービスアカウント キー 作成 新しいキーファイル.json --iam-アカウント=YOUR_SERVICE_ACCOUNT_EMAIL
* アプリケーションの更新: 新しいキーを使用するようにアプリケーション構成を更新します。これには、古いキーファイルを新しいキーファイルに置き換えるか、キーファイルを参照する環境変数または構成を更新することが含まれる場合があります。
* 古いキーを削除する: アプリケーションが新しいキーで正常に動作することを確認したら、サービス アカウントから古いキーを削除して、不正アクセスに使用されないようにします。
gcloud iam サービスアカウント キー削除 OLD_KEY_ID --iam-アカウント=YOUR_SERVICE_ACCOUNT_EMAIL
このプロセスにより、サービス アカウント キーが定期的にローテーションされ、キーが侵害されるリスクが軽減されます。
参考文献
* サービスアカウントキーの管理
* サービスアカウントキーのローテーション

最新問題: **185**
組織のセキュリティ基準に従って強化された OS イメージを作成し、セキュリティチームが管理するプロジェクトに保存しています。Google Cloud 管理者として、運用オーバーヘッドを最小限に抑えながら、Google

Cloud 組織内のすべての VM がその特定の OS イメージのみを使用できるようにする必要があります。どのような対応をすべきでしょうか 2 つ選択してください)。
A. ユーザーに自分のプロジェクトで compute.imageUser ロールを付与します。
B. ユーザーに OS イメージ プロジェクト内の compute.imageUser ロールを付与します。
C. 組織内で起動されるすべてのプロジェクトにイメージを保存します。
D. イメージ アクセス組織ポリシー制約を設定し、セキュリティ チームが管理するプロジェクトをプロジェクトの許可リストにリストします。
E. プロジェクトのユーザーから VM インスタンスの作成権限を削除し、自分とチームのみが VM インスタンスを作成できるようにします。
Answer: B,D (メーッセージを残す)
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints
- 制約/compute.trustedImageProjects
このリスト制約は、Compute Engine のイメージ ストレージとディスクのインスタンス化に使用できるプロジェクトのセットを定義します。
この制約が有効な場合、新しいインスタンスのブート ディスクのソースとして、信頼できるプロジェクトのイメージのみが許可されます。

最新問題**: 186**
Google Cloud 上の公開アプリケーションに対して、一般的なウェブアプリケーション攻撃に対する外部ウェブアプリケーション保護を実装する任務を負っています。これらのポリシー変更を適用する前に検証したいと考えています。どのサービスを使用すべきでしょうか？
A. プレビュー モードでの Google Cloud Armor の事前構成済みルール
B. モニターモードで事前設定された VPC ファイアウォール ルール
C. Google Front End (GFE) の固有の保護
D. Cloud Load Balancing ファイアウォール ルール
E. ドライランモードの VPC Service Controls
Answer: (解答を表示する)
目的: 外部 Web アプリケーション保護を実装し、適用前にポリシーの変更を検証します。
解決策: プレビュー モードで Google Cloud Armor の事前構成済みルールを使用します。
手順:
ステップ 1: Google Cloud Console を開きます。
ステップ 2: Google Cloud Armor セクションに移動します。
ステップ 3: セキュリティ ポリシーを作成または選択します。
ステップ 4: 事前構成されたルールをポリシーに適用します。
ステップ 5: プレビュー モードを有効にして、ルールを適用せずにその効果をシミュレートします。
ステップ 6: ログを監視してポリシーの変更を検証します。
Google Cloud Armor のプレビュー モードを使用すると、セキュリティ ポリシーを適用する前に、アプリケーション トラフィックに対するセキュリティ ポリシーの影響をテストおよび検証できるため、サービスを中断することなく、ポリシーが意図したとおりに機能することを確認できます。

参照：
Google Cloud Armor ドキュメント
プレビューモードの使用

最新問題: **187**
ユーザーが共有 VPC ホスト プロジェクトを誤って削除するのを防ぎたい場合、どの組織レベルのポリシー制約を有効にする必要がありますか？
A. compute.restrictSharedVpcHostProjects
B. compute.restrictXpnProjectLienRemoval
C. compute.restrictSharedVpcSubnetworks
D. compute.sharedReservationsOwnerProjects
Answer: B (メーッセージを残す**)**
compute.restrictXpnProjectLienRemoval 組織レベルのポリシー制約を有効にします。
この制約により、ユーザーは共有 VPC ホスト プロジェクトからリーエンを削除できなくなります。
この制約を有効にすると、適切な承認なしでの削除がリーエンによって防止されるため、共有 VPC ホスト プロジェクトが誤って削除されることがなくなります。
この制約は、Google Cloud Console または gcloud コマンドライン ツールを使用して適用します。
参照：
組織ポリシーの制約
共有VPC

最新問題: **188**
チームは、本番環境プロジェクトで実行されている Compute Engine インスタンスにパブリック IP アドレスが付与されていないことを確認したいと考えています。フロントエンド アプリケーションの Compute Engine インスタンスにはパブリック IP が必要です。プロダクト エンジニアには、リソースを変更するための編集者ロールが付与されています。チームはこの要件を強制したいと考えています。
あなたのチームはこれらの要件をどのように満たすべきでしょうか?
A. 本番環境プロジェクトの VPC ネットワークでプライベート アクセスを有効にします。
B. エディター ロールを削除し、エンジニアに Compute Admin IAM ロールを付与します。
C. フロントエンド Compute Engine インスタンスに対してパブリック IP のみを許可するように組織ポリシーを設定します。
D. パブリック IP を持つサブネットとパブリック IP を持たないサブネットの 2 つを持つ VPC ネットワークを設定します。
Answer: C (メーッセージを残す**)**
参照：
https://cloud.google.com/compute/docs/ip-addresses/reserve-static-external-ip-address

最新問題: **189**

Compute Engine ディスク上のデータを、Cloud Key Management Service（KMS）で管理される鍵を使用して保存時に暗号化する必要があります。これらの鍵に対する Cloud Identity and Access Management（IAM）権限は、すべての鍵に対して同じ権限を持つ必要があるため、グループ化して管理する必要があります。
何をすべきでしょうか?
A. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーレベルで管理します。
B. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。キーレベルでIAM権限を管理します。
C. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。IAM権限はキーリングレベルで管理します。
D. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーリングレベルで管理します。
Answer: A (メーッセージを残す**)**

最新問題**: 190**
プロジェクト内の Compute Engine インスタンスを一覧表示できる新しいサービス アカウントを作成します。Google が推奨するプラクティスに従ってください。
何をすべきでしょうか?
A. インスタンス テンプレートを作成し、Compute Engine アクセス スコープに対してサービス アカウントの読み取り専用アクセスを許可します。
B. compute.instances.list 権限を持つカスタム ロールを作成し、サービス アカウントにこのロールを付与します。
C. サービス アカウントにコンピューティング閲覧者の役割を付与し、すべてのインスタンスに新しいサービス アカウントを使用します。
D. サービス アカウントにプロジェクト閲覧者の役割を付与し、すべてのインスタンスに新しいサービス アカウントを使用します。
Answer: B (メーッセージを残す**)**
https://cloud.google.com/compute/docs/access/iam

最新問題**: 191**
組織では機密性の高い医療情報を扱っています。仮想マシン（VM）での使用中はデータが暗号化されていることを確認する必要があります。そのためには、組織全体に適用するポリシーを作成する必要があります。
何をすべきでしょうか?
A. 組織全体で作成されたすべての VM リソースが Confidential VM インスタンスであることを保証する組織ポリシーを実装します。
B. Google はデフォルトで使用中のデータを暗号化するため、アクションは必要ありません。
C. 組織全体で作成されたすべての VM リソースで顧客管理の暗号化キー (CMEK) 保護が使用されるようにする組織ポリシーを実装します。
D. 組織全体で作成されたすべての VM リソースが Cloud 外部キー マネージャー (EKM) 保護を使用するようにする組織ポリシーを実装します。

Answer: C (メーッセージを残す)

最新問題**: 192**
GDPRの要件に準拠し、設計段階からデータ保護を実装しています。設計レビューの一環として、Compute Engine、Google Kubernetes Engine、Cloud Storage、BigQuery、Pub/Subのワークロードを含むソリューションの暗号鍵を管理する必要があると指示されました。この実装ではどのオプションを選択すべきでしょうか？
A. クラウド外部キーマネージャー
B. 顧客管理の暗号化キー
C. 顧客提供の暗号化キー
D. Google のデフォルトの暗号化
Answer: B (メーッセージを残す)
GDPR の要件に準拠し、複数の Google Cloud サービスにわたるワークロードの暗号鍵を管理するには、顧客管理の暗号鍵（CMEK）が適切なソリューションとなります。
顧客管理暗号化キー（B）：
CMEK を使用すると、Google Cloud Key Management Service（KMS）を使用して暗号鍵を作成および管理できます。鍵のローテーションや破棄など、鍵のライフサイクルを完全に制御できます。
CMEK は、Compute Engine、Google Kubernetes Engine、Cloud Storage、BigQuery、Pub/Sub などのさまざまな Google Cloud サービスで使用でき、環境全体で一貫性のあるコンプライアンス準拠の暗号化を保証します。
CMEK を使用すると、暗号化キーが適切に管理され、保護されることで、GDPR 要件に準拠した設計によるデータ保護を実装できます。
参照：
顧客管理暗号化キーのドキュメント
Google Cloud における保存時の暗号化

最新問題**: 193**
ある多国籍企業の事業部門がGCPにサインアップし、ワークロードのGCPへの移行を開始しました。この事業部門は、数百のプロジェクトを含む組織リソースを使用してCloud Identityドメインを作成しました。
チームはこれを認識し、権限の管理とドメイン リソースの監査を引き継ぎたいと考えています。
この要件を満たすために、チームはどのタイプのアクセスを許可する必要がありますか?
A. 組織管理者
B. セキュリティレビュー担当者
C. 組織ロール管理者
D. 組織ポリシー管理者
Answer: D (メーッセージを残す)
https://cloud.google.com/resource-manager/docs/access-control-org

最新問題**: 194**
ある企業は、アナリストと管理者が共有する Cloud Storage バケットにアプリケーションログをバックアップしています。アナリストは、個人を特定できる情報（PII）を含まないログにのみアクセスできるようにする必要

があります。PII を含むログファイルは、管理者のみがアクセスできる別のバケットに保存する必要があります。
何をすべきでしょうか?
A. Cloud Pub/Sub と Cloud Functions を使用して、共有バケットにファイルがアップロードされるたびにデータ損失防止スキャンをトリガーします。スキャンで個人情報（PII）が検出された場合は、関数を管理者のみがアクセスできる Cloud Storage バケットに移動します。
B. ログを共有バケットと管理者のみがアクセスできるバケットの両方にアップロードします。Cloud Data Loss Prevention API を使用してジョブトリガーを作成します。共有バケットから個人情報（PII）を含むファイルを削除するようにトリガーを設定します。
C. アナリストと管理者の両方で共有されるバケットで、PII を含むオブジェクトを削除するようにオブジェクト ライフサイクル管理を構成します。
D. アナリストと管理者の両方で共有するバケットに、PII データがアップロードされた場合にのみトリガーされる Cloud Storage トリガーを設定します。Cloud Functions を使用してトリガーをキャプチャし、該当するファイルを削除します。
Answer: (解答を表示する**)**
説明
https://codelabs.developers.google.com/codelabs/cloud-storage-dlp-functions#0https://www.youtube.com/watch

最新問題**: 195**
顧客がエンジニアを解雇し、エンジニアの Google アカウントが自動的にプロビジョニング解除されていることを確認する必要があります。
顧客は何をすべきでしょうか?
A. ディレクトリ サービスで Cloud SDK を使用して、Cloud Identity の IAM 権限を削除します。
B. Cloud SDK をディレクトリ サービスと併用して、Cloud Identity からユーザーをプロビジョニングおよびプロビジョニング解除します。
C. Cloud Directory Sync をディレクトリ サービスと構成して、Cloud Identity からユーザーをプロビジョニングおよびプロビジョニング解除します。
D. ディレクトリ サービスで Cloud Directory Sync を構成して、Cloud Identity の IAM 権限を削除します。
Answer: (解答を表示する**)**
説明
https://cloud.google.com/identity/solutions/automate-user-provisioning#cloud_identity_automated_provisioning
「Cloud Identity には、Cloud Identity とサードパーティのクラウド アプリ間の橋渡しとして機能する自動プロビジョニング コネクタのカタログがあります。」

最新問題**: 196**
GCP リソースに直接アクセスする必要がある開発者と運用スタッフそれぞれに、Google Cloud で企業ユーザーアカウントを提供する必要があります。企業ポリシーでは、ユーザー ID をサードパーティの ID 管理プロバイダで管理し、シングル サインオンを活用することが義務付けられています。多くのユーザーが企業ドメイ

ンのメールアドレスを個人の Google アカウントに使用していることが判明したため、Google の推奨プラクティスに従って、既存の管理対象外ユーザーを管理対象アカウントに変更する必要があります。
取るべき行動は 2 つありますか? (2 つ選択してください。)
A. Google Cloud Directory Sync を使用して、ローカル ID 管理システムを Cloud Identity と同期します。
B. Google 管理コンソールを使用して、再設定用のメールアドレスに個人アカウントを使用している管理対象ユーザーを確認します。
C. 管理対象の Google アカウントにユーザーを追加し、ユーザーに個人アカウントに関連付けられているメール アドレスを変更するよう強制します。
D. 管理対象外ユーザー向け移行ツール (TTUU) を使用して、競合するアカウントを持つユーザーを見つけ、個人の Google アカウントを移行するよう依頼します。
E. 従業員全員にメールを送信し、個人の Google アカウントに会社のメール アドレスを使用しているユーザーに、個人アカウントを直ちに削除するよう依頼します。
Answer: A,D (メーッセージを残す**)**
ユーザーアカウントを管理し、企業ポリシーへの準拠を確保するには、Google Cloud Directory Sync（GCDS）を使用することで、ローカルの ID システムと Cloud Identity を同期できます。管理対象外ユーザー向け転送ツール（TTUU）を使用すると、ユーザーが個人アカウントを管理対象アカウントに移行できるため、競合するアカウントを特定して管理しやすくなります。
手順:
ID の同期: GCDS を使用して、ローカル ID 管理システムから Cloud Identity にユーザーを同期し、すべての企業ユーザー アカウントが管理されるようにします。
競合するアカウントを特定する: TTUU を使用して、企業のメールアドレスを使用して個人の Google アカウントを持つユーザーを見つけます。
競合するアカウントの管理: TTUU を使用して個人アカウントを管理対象アカウントに移行するようユーザーに要求し、すべてのアカウントが企業の管理下にあることを確認します。
参照：
Google Cloud ディレクトリ同期
管理対象外ユーザー向け転送ツール

最新問題**: 197**
組織の Google Cloud VM は、外部ユーザー向けのウェブサービスをホストするために、パブリック IP アドレスが設定されたインスタンス テンプレートを使用してデプロイされています。VM は、VM 用のカスタム共有

VPC を 1 つ含むホスト (VPC) プロジェクトに接続されたサービス プロジェクトに配置されています。外部ユーザーへのサービス提供を継続しながら、VM のインターネットへの公開範囲を縮小するよう求められています。マネージド インスタンス グループ (MIG) を起動するために、パブリック IP アドレスを設定せずにインスタンス テンプレートを既に再作成済みです。どうすればよいでしょうか？
A. MIG のサービス プロジェクトに Cloud NAT ゲートウェイをデプロイします。
B. MIG のホスト (VPC) プロジェクトに Cloud NAT ゲートウェイをデプロイします。
C. MIG をバックエンドとして使用して、サービス プロジェクトに外部 HTTP(S) ロードバランサをデプロイします。
D. MIG をバックエンドとして使用して、ホスト (VPC) プロジェクトに外部 HTTP(S) ロードバランサをデプロイします。
Answer: D (メーッセージを残す**)**
https://cloud.google.com/load-balancing/docs/https#shared-vpc
すべての負荷分散コンポーネントとバックエンドを共有 VPC ホスト プロジェクトで作成できますが、このモデルではネットワーク管理とサービス開発の責任が分離されません。

最新問題**: 198**
組織ではGoogle Cloudプロジェクトで職務分離を実施しています。開発者グループは新しいコードをデプロイする必要がありますが、ネットワークファイアウォールルールを変更する権限がありません。
何をすべきでしょうか?
A. すべての開発者にネットワーク管理者のIAMロールを割り当てます。開発者にはファイアウォール設定を変更しないように指示します。
B. 開発者グループに編集者のIAMロールを付与します。IAM拒否ポリシーを使用して、ファイアウォールの変更権限を明示的に無効にします。
C. Access Context Manager を使用して、IP アドレスやデバイスのセキュリティ ポスチャなどの属性に基づいて、承認された管理者のみがファイアウォール ルールを変更できる条件を作成します。
D. 2つのカスタムIAMロールを作成して割り当てます。デプロイヤロールを割り当てて、Compute Engineとデプロイメント関連の権限を制御します。ネットワーク管理者ロールを割り当てて、ファイアウォールの権限を管理します。
Answer: D (メーッセージを残す**)**

最新問題**: 199**
会社のアプリケーションは、ユーザーが管理するサービス アカウント キーを使用してデプロイされています。Google が推奨する手順に従ってキーをローテーションしたいと考えています。
何をすべきでしょうか?
A. Cloud Shell を開き、gcloud iam service-accounts enable-auto-rotate --iam- account=IAM_ACCOUNT を実行します。
B. Cloud Shell を開き、gcloud iam service-accounts keys rotate --iam- account=IAM_ACCOUNT --key=NEW_KEY を実行します。

C. 新しいキーを作成し、アプリケーションで新しいキーを使用します。サービスアカウントから古いキーを削除します。
D. 新しいキーを作成し、アプリケーションで使用します。古いキーはバックアップキーとしてシステムに保存します。
Answer: C (メーッセージを残す**)**
鍵をローテーションするには、新しい鍵を作成し、新しい鍵を使用するようにアプリケーションを更新し、古い鍵を削除します。serviceAccount.keys.create() メソッドと serviceAccount.keys.delete() メソッドを併用することで、ローテーションを自動化できます。
https://cloud.google.com/iam/docs/creating-managing-service-account-
キー#サービスアカウントキーの削除

最新問題**: 200**
セキュリティ運用チームは、組織内のすべてのプロジェクトのセキュリティ関連ログにアクセスする必要があります。そのためには、以下の要件を満たす必要があります。
- ログへの表示アクセスのみを許可することで、最小権限モデルに従います。
- 管理者アクティビティ ログにアクセスできます。
- データ アクセス ログにアクセスできます。
- アクセスの透明性ログにアクセスできます。
セキュリティ運用チームに付与する必要がある Identity and Access Management (IAM) ロールはどれですか?
A. ロール/ロギング.プライベートログビューア
B. ロール/ログ記録.管理者
C. ロール/閲覧者
D. ロール/ログ記録ビューア
Answer: (解答を表示する**)**
roles/logging.privateLogViewer (プライベート ログ ビューア) には、roles/logging.viewer に含まれるすべての権限に加えて、_Default バケット内のデータ アクセス監査ログを読み取る機能が含まれます。
https://cloud.google.com/logging/docs/アクセス制御

最新問題**: 201**
セキュリティチームは、過去2か月の間に、貴社の元従業員がサービスアカウントキーを使用してGoogle Cloudリソースに不正アクセスしたと考えています。不正アクセスを確認し、ユーザーのアクティビティを特定する必要があります。どうすればよいですか？
A. セキュリティ ヘルス分析を使用してユーザー アクティビティを判断します。
B. Cloud Monitoring コンソールを使用して、監査ログをユーザー別にフィルタリングします。
C. Cloud Data Loss Prevention API を使用して、Cloud Storage 内のログをクエリします。
D. ログ エクスプローラーを使用してユーザー アクティビティを検索します。
Answer: D (メーッセージを残す**)**
説明

監査ログを使用して、サービス アカウントを検索し、過去 2 か月間のアクティビティを確認します。(ユーザーは SA ID を使用しているため、ユーザー ID は表示されませんが、IP アドレス、勤務時間などに基づいて相関関係を作成できます。)

最新問題**: 202**
小売顧客は、ユーザーがコメントや製品レビューをアップロードすることを許可しています。コメントやレビューを公開する前に、顧客はテキストに機密情報が含まれていないことを確認する必要があります。
これを実現するにはどの Google Cloud サービスを使用すればよいですか?
A. クラウド キー管理サービス
B. クラウドデータ損失防止 API
C. ビッグクエリ
D. クラウドセキュリティスキャナー
Answer: B (メーッセージを残す**)**
ユーザーがアップロードしたコメントや製品レビューに公開前に機密データが含まれていないことを確認するには、Cloud Data Loss Prevention (DLP) API を使用します。
* DLP API を有効にする:
* Cloud Console にアクセスし、[API とサービス] > [ライブラリ] に移動します。
* Data Loss Prevention API」を検索して有効にします。
* DLP API を構成する:
* 検出する機密データの種類を指定する検査テンプレートを作成します。
* 機密データを編集またはマスクする場合は、匿名化テンプレートを設定します。
* アプリケーションにDLPを実装する:
* 希望するプログラミング言語の Google Cloud DLP クライアント ライブラリを使用します。
* 保存または公開する前に、テキスト データを DLP API に送信して検査します。
google.cloud から dlp_v2 をインポートします。dlp_client = dlp_v2.DlpServiceClient() parent = f"projects/{project_id}" item = {"value": "ユーザーコメントのテキストをここに入力してください"} inspect_config = {"info_types": [{"name": "PERSON_NAME"},
{"name": "CREDIT_CARD_NUMBER"}]} response = dlp_client.inspect_content(parent=parent, inspect_config=inspect_config, item=item) 参照:
* クラウドデータ損失防止 API ドキュメント
* DLP API クライアント ライブラリ

最新問題**: 203**
セキュリティ運用チームは、組織内のすべてのプロジェクトのセキュリティ関連ログにアクセスできる必要があります。
次のような要件があります。
ログへの表示アクセスのみを許可して、最小権限モデルに従います。
管理者アクティビティ ログにアクセスできます。
データ アクセス ログにアクセスできます。
アクセスの透明性ログにアクセスできます。

セキュリティ運用チームに付与する必要がある Identity and Access Management (IAM) ロールはどれですか?
A. ロール/ロギング.プライベートログビューア
B. ロール/ログ記録.管理者
C. ロール/閲覧者
D. ロール/ログ記録ビューア
Answer: (解答を表示する**)**
説明
https://cloud.google.com/logging/docs/access-control#considerations roles/logging.privateLogViewer (プライベート ログ ビューア) には、roles/logging.viewer に含まれるすべての権限に加えて、_Default バケット内のデータアクセス監査ログを読み取る機能が含まれています。

最新問題**: 204**
ブートディスクのソースとして使用できるイメージを制限したい場合、これらのイメージは専用のプロジェクトに保存されます。
何をすべきでしょうか?
A. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。許可操作で、信頼されたプロジェクトをホワイトリストとしてリストします。
B. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。信頼済みプロジェクトを拒否操作の例外としてリストします。
C. リソースマネージャーで、信頼されたプロジェクトのプロジェクト権限を編集します。組織を 「コンピューティングイメージユーザー」ロールのメンバーとして追加します。
D. リソースマネージャーで組織の権限を編集します。プロジェクトIDを 「コンピューティングイメージユーザー」ロールのメンバーとして追加します。
Answer: (解答を表示する**)**
https://cloud.google.com/compute/docs/images/restricting-image-access#trusted_images

最新問題**: 205**
会社のGoogle Cloud組織にCloud Identityを設定しています。ユーザーアカウントはMicrosoft Entra IDからDirectory Sync経由でプロビジョニングされ、Entra IDを介したシングルサインオンが利用可能になります。組織の特権管理者アカウントを保護する必要があります。ソリューションは最小権限の原則に従い、強力な認証を実装する必要があります。どうすればよいでしょうか？
A. スーパー管理者専用のアカウントを作成します。Entra IDのスーパー管理者アカウントには2段階認証が強制されていることを確認してください。
B. 特権管理者専用のアカウントを作成します。特権管理者アカウントにはGoogleの2段階認証プロセスを適用します。
C. 組織管理者とスーパー管理者の権限を組み合わせたアカウントを作成します。
Entra ID のスーパー管理者アカウントに対して 2 段階認証が実施されていることを確認します。
D. 組織管理者とスーパー管理者の権限を組み合わせたアカウントを作成します。スーパー管理者アカウントに Google の 2 段階認証プロセスを適用します。

Answer: B (メッセージを残す)
Google の特権管理者のセキュリティに関するベスト プラクティスでは、特にサードパーティの SSO（Entra ID など）を使用する場合、これらのアカウントは標準のユーザー アカウントとは異なる方法で処理する必要があることが強調されています。
Google Cloud の管理者アカウントに関するベスト プラクティスによると、次のようになります。
標準のSSO（シングルサインオン）フローに含まれない特権管理者アカウントを少なくとも2つ維持する必要があります。これらのアカウントは「クラウド専用」アカウントである必要があります。これにより、外部 IdP（Entra ID）がダウンしたり、設定ミスが発生しても、Google Cloudにログインできるようになります。さらに、IdPに依存しない最高レベルの保護を提供するために、これらのアカウントにはGoogle 2段階認証（2SV）（理想的にはハードウェアセキュリティキーを使用）を直接適用する必要があります。重要なベストプラクティス：
* 専用アカウント: 日常業務 (メール/ドキュメント) と管理タスクに同じアカウントを使用しないでください。
* 管理者の SSO を避ける: Entra ID に問題がある場合、Google 組織からロックアウトされる可能性があります。クラウドのみのアカウントでこの問題を解決できます。
* 強力な 2SV: これらの高度な権限を持つ ID をフィッシングや認証情報の盗難から保護するには、Google のネイティブ 2SV が必要です。
参照：
Google Cloud ドキュメント: 「特権管理者アカウントのベスト プラクティス」(https://cloud.google.com)(/resource-manager/docs/super-admin-best-practices)。
Google Workspace 管理者ヘルプ: 「管理者アカウントのセキュリティに関するおすすめの方法」(https://support.google.com/a/answer/9011373)。

最新問題**: 206**
ある雇用主は、従業員の外れ値を特定し、収入格差を是正するために、ボーナス報酬の経時的な変化を追跡したいと考えています。この作業は、個人の報酬に関する機密データを公開することなく実行でき、外れ値を特定するために元に戻すことができる必要があります。
これを実現するには、どの Cloud Data Loss Prevention API テクニックを使用する必要がありますか?
A. 一般化
B. 編集
C. 暗号ハッシュ設定
D. 暗号置換FfxFpeConfig
Answer: D (メッセージを残す)
機密データの匿名化
Cloud Data Loss Prevention（DLP）は、テーブルなどのコンテナ構造に格納されたテキストを含む、テキストコンテンツ内の機密データを匿名化できます。匿名化とは、データから識別情報を削除するプロセスです。APIは個人識別情報（PII）などの機密データを検出し、匿名化変換を用いてデータをマスク、削除、またはその他の方法で難読化します。例えば、匿名化技術には以下が含まれます。

文字をアスタリスク (*) やハッシュ (#) などの記号に部分的または完全に置き換えることで機密データをマスクします。
機密データの各インスタンスをトークンまたはサロゲート文字列に置き換えます。
ランダムに生成されたキーまたは事前に決定されたキーを使用して機密データを暗号化および置き換えます。
CryptoReplaceFfxFpeConfig または CryptoDeterministicConfig infoType 変換を使用してデータを匿名化する場合、元々データを匿名化するために使用された CryptoKey がある限り、そのデータを再識別できます。
https://cloud.google.com/dlp/docs/機密データの識別を解除

最新問題**: 207**
あなたの組織では、BigQuery と Cloud Storage に保存されたライブユーザーアクティビティデータを処理する ML モデルを使用して、リアルタイムのレコメンデーションエンジンを構築しています。開発された新しいモデルはすべて Artifact Registry に保存されます。
この新しいシステムは、モデルをGoogle Kubernetes Engineにデプロイし、メッセージキューにはPub/Subを使用します。最近の業界ニュースでは、機械学習モデルのサプライチェーンを悪用した攻撃が報告されています。このサーバーレスアーキテクチャでは、特に開発およびデプロイメントパイプラインへのリスクに対して、セキュリティを強化する必要があります。
何をすべきでしょうか?
A. ML モデルに使用される外部ライブラリと依存関係を可能な限り制限します。
BigQuery および Cloud Storage からユーザーデータにアクセスするために使用される暗号化キーを継続的にローテーションします。
B. 開発中およびデプロイ前のコンテナイメージの脆弱性スキャンを有効にします。Artifact Registry から継続的インテグレーションおよび継続的デプロイ (CI/CD) パイプラインにデプロイされたイメージに Binary Authorization を適用します。
C. モデル開発の前にすべてのトレーニング データを徹底的にサニタイズして、ポイズニング攻撃のリスクを軽減します。
承認には IAM を使用し、コード リポジトリとクラウド サービスにロールベースの制限を適用します。
D. Cloud Run インスタンスへの外部トラフィックを制限するための厳格なファイアウォール ルールを作成します。侵入検知システム (IDS) を統合して、Pub/Sub メッセージフローにおけるリアルタイムの異常検知を実現します。
Answer: (解答を表示する**)**
サーバーレス アーキテクチャ内で機械学習 (ML) モデルのサプライ チェーンのセキュリティを強化するには、開発パイプラインとデプロイメント パイプラインの両方を保護する対策を実装することが重要です。
* オプション A: 外部依存関係を制限し、暗号化キーをローテーションすることはセキュリティ上は良い方法ですが、ML モデルのサプライ チェーンに関連するリスクに直接対処するものではありません。
* オプションB：開発中およびデプロイ前の段階でコンテナイメージの脆弱性スキャンを実施することで、コンテナイメージ内の既知の脆弱性を特定し、軽減することができます。Binary Authorization を適用することで、信頼され検証済みのイメージのみが環境にデプロイされることが保証されます。この組み合わせにより、デプロイ前にコンテナイメージの整合性を検証することで、MLモデルのサプライチェーンのセキュリティが直接的に強化されます。

* オプション C: トレーニング データをサニタイズし、ロールベースのアクセス制御を適用することは重要なセキュリティ プラクティスですが、侵害されたコンテナ イメージに対してデプロイメント パイプラインを具体的に保護するものではありません。
* オプション D: 厳格なファイアウォール ルールと侵入検知システムはネットワーク セキュリティを強化しますが、コンテナ イメージまたは展開プロセス内の脆弱性には具体的に対処しません。
したがって、オプション B は、検証済みの安全なコンテナ イメージのみが環境内で使用されるようにすることで、開発およびデプロイメント パイプラインのセキュリティに直接対処するため、最も効果的なアプローチです。
参考文献:
* コンテナスキャンの概要
* バイナリ認証の概要

最新問題: **208**
会社の最高情報セキュリティ責任者（CISO）は、会社のグローバル展開計画に影響を与える規制要件に基づき、ビジネスデータを特定の場所に保存することを要求しています。この要件を実現するための計画を策定した後、以下の点を決定します。
対象範囲のサービスは、Google Cloud のデータ所在地要件に含まれています。
ビジネス データは同じ組織の特定の場所に保存されます。
フォルダー構造には複数のデータ保存場所を含めることができます。
プロジェクトは特定の場所に合わせて配置されます。
リソースの場所制限という組織ポリシー制約を非常にきめ細かく制御するために使用する予定です。この制約は階層のどのレベルで設定すればよいですか？
A. 組織
B. リソース
C. プロジェクト
D. フォルダ
Answer: D (メーッセージを残す**)**
フォルダー レベルでリソースの場所の制限組織ポリシー制約を設定します。
フォルダー レベルで制約を設定すると、データ保存要件を非常に細かく制御できます。
各フォルダーは特定の地理的な場所を表すことができ、それらのフォルダー内のプロジェクトは場所の制約を継承し、規制要件への準拠を保証します。
このアプローチにより、同じ組織内の異なるリージョンにわたるデータの保存場所を柔軟に管理できるようになります。
参照：
組織ポリシー サービス: リソースの場所の制限

最新問題: **209**
ある組織のセキュリティおよびリスク管理チームは、Google Cloud Platform（GCP）で実行している特定の本番環境ワークロードに対する責任の所在と、Googleの責任の所在について懸念を抱いています。彼らは主に

App EngineをはじめとするGoogle CloudのPlatform-as-a-Service（PaaS）サービスを使用してワークロードを実行しています。
App Engine を使用する際に、テクノロジー スタック内のどの領域に主な責任として重点を置く必要がありますか。
A. VPC フローログの設定と監視
B. XSSおよびSQLi攻撃からの防御
C. ゲスト OS の最新のアップデートとセキュリティ パッチを管理します
D. 保存されているすべてのデータを暗号化する
Answer: (解答を表示する**)**
App Engine などの Google Cloud の Platform-as-a-Service (PaaS) サービスを使用する場合、基盤となる OS、ランタイム、スケーリングなどのインフラストラクチャは Google が管理します。ただし、クロスサイト スクリプティング (XSS) や SQL インジェクション (SQLi) 攻撃の防御など、アプリケーション コード自体のセキュリティ確保はユーザーの責任となります。これには、安全なコーディング プラクティスの実装、入力の検証、アプリケーション内での適切なセキュリティ対策の導入が含まれます。
参照：
Google Cloud: 責任共有モデル
App Engine のセキュリティ

最新問題**: 210**
組織では、Google Cloud にインフラストラクチャとアプリケーションをデプロイするための新しい継続的インテグレーションとデリバリー（CI/CD）プロセスを展開しています。多くのチームが独自の CI/CD ワークフロー インスタンスを使用します。これは Google Kubernetes Engine（GKE）上で実行されます。CI/CD パイプラインは、Google Cloud API に安全にアクセスできるように設計する必要があります。どうすればよいですか?
A. * 1 CI/CD パイプライン専用のサービス アカウントを作成する* 2 GKE クラスタ内の専用ノード プールでデプロイメント パイプラインを実行する* 3 プール内のノードの ID として作成したサービス アカウントを使用して、Google Cloud API に認証する
B. * 1 各デプロイメントパイプラインのサービスアカウントを作成する* 2 サービスアカウントの秘密鍵を生成する* 3 特定のデプロイメントパイプラインを実行するポッドのみがアクセスできるKubernetesシークレットとして秘密鍵を安全に保存する
C. * 1 個別のサービス アカウント (または各デプロイメント パイプライン) を作成する* 2 サービス アカウントの命名規則でパイプラインの識別子を追加する* 3 各パイプラインが専用のポッドで実行されることを確認する* 4 ワークロード ID を使用してデプロイメント パイプライン ポッドをサービス アカウントにマッピングする
D. * 1 インフラストラクチャ用とアプリケーションデプロイメント用の 2 つのサービス アカウントを作成します。* 2 ワークロード ID を使用して、ポッドが 2 つのパイプラインを実行し、サービス アカウントで認証できるようにします。* 3 インフラストラクチャ パイプラインとアプリケーション パイプラインを別々の名前空間で実行します。
Answer: C (メーッセージを残す**)**

Google Kubernetes Engine（GKE）で実行されている CI/CD パイプラインから Google Cloud API に安全にアクセスするには、次の手順に従います。
* サービス アカウントを作成します:
* 各CI/CDパイプラインごとに個別のサービスアカウントを作成します。これにより、パイプラインの分離と最小限の権限が確保されます。
* pipeline-a-sa、pipeline-b-sa など、各パイプラインの識別子を含む命名規則を使用します。
* Kubernetes サービス アカウントを構成する:
* 各 CI/CD パイプライン ポッドに Kubernetes サービス アカウントを作成します。
* Kubernetes サービス アカウントを Google サービス アカウントにマッピングします。
* Workload Identity を使用して、Kubernetes サービス アカウントを対応する Google サービス アカウントに関連付けます。これにより、ポッドは Google Cloud API に対して安全に認証できるようになります。
* Kubernetes サービス アカウントを Google サービス アカウントにバインドするコマンドの例:
gcloud iam サービスアカウント add-iam-policy-binding \ --role roles/iam.workloadIdentityUser \ --member "serviceAccount:<プロジェクトID>.svc.id.goog[<名前空間>/<KSA名>]" \
<GSA_NAME>@<プロジェクトID>.iam.gserviceaccount.com
* CI/CD パイプラインをデプロイする:
* 各パイプラインが、以前に構成された特定の Kubernetes サービス アカウントを使用する専用のポッドで実行されることを確認します。
* この設定により、最小権限の原則に従って、各パイプラインに Google Cloud API と安全にやり取りするために必要な権限が付与されます。
参考文献
* ワークロード ID の使用
* サービスアカウントの管理

最新問題**: 211**
コンプライアンス上の理由から、組織はPCI Kubernetesの対象となるポッドが 「対象となる」ノードにのみ配置されていることを確認する必要があります。これらのノードには、 「対象となる」ポッドのみを配置できます。組織はこの目的をどのように達成すべきでしょうか?
A. inscope: true というラベルの付いたノードのみを使用するように、ポッド構成に nodeSelector フィールドを追加します。
B. ラベル inscope: true を持つノード プールと、そのラベルを持つノードでのみポッドの実行を許可するポッド セキュリティ ポリシーを作成します。
C. ラベル inscope: true、効果 NoSchedule、および Pod 構成に一致する toleration を使用して、ノードに taint を配置します。
D. 名前空間 「in-scope-pci」内のすべてのスコープ内ポッドを実行します。
Answer: A (メーッセージを残す**)**
説明

nodeSelectorは、ノード選択制約の最もシンプルな推奨形式です。Pod仕様にnodeSelectorフィールドを追加し、ターゲットノードに付与するノードラベルを指定できます。Kubernetesは、指定されたラベルを持つノードにのみPodをスケジュールします。=>
https://kubernetes.io/docs/concepts/scheduling-eviction/assign-pod-node/#nodeselector ポッドには許容範囲が適用されます。許容範囲により、スケジューラは一致するテイントを持つポッドをスケジュールできます。許容範囲はスケジュールを可能にしますが、スケジュールを保証するものではありません。スケジューラは機能の一部として他のパラメータも評価します。
=>https://kubernetes.io/docs/concepts/scheduling-eviction/taint-and-toleration/

最新問題**: 212**
ある企業は、専用サーバールームでワークロードを実行しています。これらのワークロードへのアクセスは、社内のプライベートネットワーク内からのみ行う必要があります。これらのワークロードには、Google Cloud Platform プロジェクト内の Compute Engine インスタンスから接続する必要があります。
要件を満たすために、どの 2 つのアプローチを取ることができますか? (2 つ選択してください。)
A. Cloud Interconnect を使用してプロジェクトを構成します。
B. VPC ピアリングを使用してプロジェクトを構成します。
C. Cloud VPN を使用してプロジェクトを構成します。
D. 共有 VPC を使用してプロジェクトを構成します。
E. すべての Compute Engine インスタンスをプライベート アクセスで構成します。
Answer: A,C (メーッセージを残す**)**

最新問題**: 213**
現在の保守契約の期限が切れる前に、社内データセンターからGCPへレガシーアプリケーションを移行する責任を負っています。アプリケーションがどのポートを使用しているかは不明で、確認できるドキュメントもありません。環境をリスクにさらすことなく移行を完了したいと考えています。
何をすべきでしょうか?
A. アプリケーションを、独立したプロジェクト内の Cloud Functions でホストされるマイクロサービス アーキテクチャにリファクタリングします。ファイアウォール ルールを使用して、プロジェクト外からのすべてのトラフィックを無効にします。VPC フローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。

B. 『リフト＆シフト」アプローチを用いて、アプリケーションを独立したプロジェクトに移行します。VPCファイアウォールルールを使用して、すべての内部TCPトラフィックを有効にします。VPCフローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
C. アプリケーションをGKEクラスタ内のマイクロサービスアーキテクチャにリファクタリングします。ファイアウォールルールを使用して、クラスタ外からのすべてのトラフィックを無効にします。VPCフローログを使用して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
D. カスタムネットワーク内で 『リフト＆シフト」アプローチを使用して、アプリケーションを独立したプロジェクトに移行します。VPC内のすべてのトラフィックを無効にし、ファイアウォールのログを確認して、アプリケーションが正常に動作するために許可する必要があるトラフィックを特定します。
Answer: C (メーッセージを残す**)**

最新問題**: 214**
組織における典型的なネットワークおよびセキュリティレビューは、アプリケーションのトランジットルート、リクエスト処理、ファイアウォールルールの分析で構成されます。組織は、開発チームがこのような包括的なレビューにかかるオーバーヘッドなしに、新しいアプリケーションをデプロイできるようにしたいと考えています。
この組織にはどのようにアドバイスすればよいでしょうか?
A. ファイアウォール フィルターを備えた Forseti を使用して、運用環境で不要な構成をキャッチします。
B. インフラストラクチャをコードとして使用することを義務付け、CI/CD パイプラインで静的分析を提供してポリシーを適用します。
C. すべての VPC トラフィックを顧客管理ルーター経由でルーティングし、本番環境で悪意のあるパターンを検出します。
D. すべての本番アプリケーションはオンプレミスで実行されます。開発者は開発およびQAプラットフォームとしてGCPを自由に利用できます。
Answer: (解答を表示する**)**
開発チームがネットワークやセキュリティレビューの膨大なオーバーヘッドなしに新しいアプリケーションをデプロイできるようにするには、インフラストラクチャ ･アズ ･コード (IaC) の使用を義務付け、CI/CDパイプラインにおける静的解析を通じてポリシーを適用することをお勧めします。このアプローチにより、開発プロセス中にセキュリティとコンプライアンスのポリシーが自動的にチェックされます。
ステップバイステップ:
* IaC を採用: Terraform や Google Cloud Deployment Manager などのツールを使用して、インフラストラクチャをコードとして管理します。
* CI/CD パイプラインの統合: TFLint や Checkov などの静的分析ツールを CI/CD パイプラインに統合して、セキュリティ ポリシーを適用します。
* ポリシー定義: コード内で遵守する必要があるセキュリティ ポリシーとベスト プラクティスを定義します。
* 自動チェック: CI/CD パイプラインで自動チェックを構成して、デプロイ前にこれらのポリシーに照らしてコードを確認します。
* 監視と監査: 展開されたアプリケーションを継続的に監視および監査して、継続的なコンプライアンスを確保します。

参考文献:
* Google Cloud 上の Infrastructure as Code
* Terraformの静的解析
* IaC の Checkov

最新問題**: 215**
貴社は、IT インフラストラクチャの大部分を Google Cloud に移行する予定です。既存のオンプレミス Active Directory を Google Cloud の ID プロバイダとして活用したいと考えています。貴社のオンプレミス Active Directory を Google Cloud と統合し、アクセス管理を構成するには、どの 2 つの手順を実行する必要がありますか (2 つ選択してください)。
A. Identity Platform を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
B. Cloud Identity SAML 統合を使用して、ユーザーとグループを Google Cloud にプロビジョニングします。
C. Google Cloud Directory Sync をインストールし、Active Directory と Cloud Identity に接続します。
D. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (IAM) ロールを作成します。
E. 各 Active Directory グループに対応する権限を持つ Identity and Access Management (IAM) グループを作成します。
Answer: (解答を表示する**)**
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing- user-accounts?hl=en
https://cloud.google.com/architecture/identity/federating-gcp-with-active-directory-synchronizing- user-accounts?hl=en#deciding_where_to_deploy_gcds

最新問題**: 216**
組織ではActive Directoryを使用しており、Security Assertion Markup Language (SAML)の設定を希望しています。すべてのユーザーに対してシングルサインオン (SSO)を設定し、適用する必要があります。
何をすべきでしょうか?
A. 1. SAML プロファイルの割り当てを管理します。
* 2. Active Directory (AD) テナントで OpenID Connect (OIDC) を有効にします。
* 3. ドメインを検証します。
B. 1. 新しい SAML プロファイルを作成します。
* 2. X.509証明書をアップロードします。
* 3. パスワード変更URLを有効にします。
* 4. IdP でエンティティ ID と ACS URL を設定します。
C. 1- 新しい SAML プロファイルを作成します。
* 2. サインイン ページとサインアウト ページの URL を入力します。
* 3. X.509証明書をアップロードします。
* 4. IdPでエンティティIDとACS URLを設定する
D. 1. Active Directory (AD) テナントで OpenID Connect (OIDC) の前提条件を構成する
* 2. ADドメインを確認します。

* 3. SAML を使用するユーザーを決定します。
* 4. 事前設定されたプロファイルを、選択した組織単位 (OU) とグループに割り当てます。
Answer: C (メッセージを残す)
Active Directory を使用している組織で SAML ベースのシングル サインオン (SSO) を構成する場合の一般的な手順としては、SAML プロファイルの設定、サインインおよびサインアウト プロセスに必要な URL の指定、安全な通信のための X.509 証明書のアップロード、アイデンティティ プロバイダー (この場合は Active Directory) でのエンティティ ID とアサーション コンシューマー サービス (ACS) URL の設定などがあります。

最新問題**: 217**
組織では、Cloud Run 上にサーバーレス ウェブ アプリケーションをデプロイしており、HTTPS 経由で一般公開する必要があります。セキュリティ要件を満たすには、エッジで TLS を終端し、脅威の緩和策を適用し、地域ベースのアクセス制限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. allUsers アクセスを有効にして、Cloud Run サービスを公開します。認証と IP ベースのアクセス制御のために、Identity-Aware Proxy (IAP) を構成します。HTTPS にはカスタム SSL 証明書を使用します。
B. Cloud Run サービスにカスタムドメインを割り当てます。HTTPS を有効にします。IAM を設定して、allUsers がサービスを呼び出せるようにします。ファイアウォールルールと VPC Service Controls を使用して、地域ベースの制限とトラフィックフィルタリングを行います。
C. Cloud Run サービスを指すサーバーレス NEG を使用して外部 HTTP(S) ロードバランサをデプロイします。
TLS 終端には Google マネージド証明書を使用します。地理ベースのアクセス制御を備えた Cloud Armor ポリシーを構成します。
D. Cloud Run URL 用の Cloud DNS パブリックゾーンを作成します。サービスに静的 IP をバインドします。VPC ファイアウォール ルールを使用して、IP 範囲と脅威シグネチャに基づいて受信トラフィックを制限します。
Answer: C (メッセージを残す)
この問題に対処するには、HTTPS、エッジでの TLS 終了、脅威の緩和、地理ベースのアクセス制限を備えた、一般公開されている Cloud Run サービスが必要です。
外部 HTTP(S) ロードバランサ: これは、一般公開されているウェブ アプリケーションを公開するための標準の Google Cloud コンポーネントであり、単一のグローバル IP アドレス、グローバル ロード バランシング、そして重要な点として、Google ネットワークのエッジでの TLS 終端を提供します。
サーバーレス ネットワーク エンドポイント グループ (NEG): サーバーレス NEG は、HTTP(S) ロードバランサを Cloud Run サービス (または Cloud Functions や App Engine などの他のサーバーレス バックエンド) に接続し、ロードバランサがトラフィックをサーバーレス アプリケーションにルーティングできるようにします。抜粋参照: 「サーバーレス ネットワーク エンドポイント グループ (NEG) で外部 HTTP(S) ロードバランサを使用すると、Cloud Run サービスを Cloud CDN、Google Cloud Armor、Cloud Identity-Aware Proxy などの高度な負荷分散機能と統合できます。」(Google Cloud ドキュメント: 「Cloud Run サービスを HTTP(S) ロードバランサに接続する | Cloud Run ドキュメント」- https://cloud.google.com/run/docs/integrating/load-balancers)
TLS 終端用の Google マネージド証明書: Google マネージド SSL 証明書を使用すると、証明書のプロビジョ

ニング、更新、デプロイが Google によって処理されるため、HTTPS の管理が簡素化されます。外部 HTTP(S) ロードバランサは、これらの証明書を使用して TLS を終了します。抜粋参照: 「Google マネージド SSL 証明書を使用すると、Google Cloud のグローバルに分散されたインフラストラクチャを使用して、証明書を自動的にプロビジョニングおよび更新できます。」(Google Cloud ドキュメント: 「Google マネージド SSL 証明書の概要 | ロード バランシング」 - https://cloud.google.com/load-balancing/docs/ssl-certificates/google-managed-certs)
脅威の軽減と地理ベースのアクセス制御のための Cloud Armor: Cloud Armor は、HTTP(S) ロードバランサと統合されるウェブ アプリケーション ファイアウォール (WAF) サービスです。DDoS 保護を提供し、脅威（SQL インジェクション、XSS など）を軽減するためのカスタムルールを許可し、ソースの地理的地域に基づいてトラフィックを許可または拒否する地理ベースのアクセス制御ルールをサポートします。抜粋参照: 「Google Cloud Armor は、分散型サービス拒否（DDoS）攻撃や、クロスサイト スクリプティング（XSS）や SQL インジェクション（SQLi）などのアプリケーション攻撃など、さまざまな脅威から Google Cloud デプロイメントを保護します。」および 「Google Cloud Armor は地理ベースのアクセス制御をサポートしており、地理的地域に基づいてリクエストをフィルタリングできます。」 (Google Cloud ドキュメント: 「Google Cloud Armor の概要」 - https://cloud.google.com/armor/docs
/概要）
他のオプションを評価してみましょう。
A) 認証とIPベースのアクセス制御のためのIAP + カスタムSSL証明書 :IAPは主にユーザー/IDの認証レイヤーであり、認証が行われる前に公開サービスに対する脅威軽減やジオブロックを行うWAFではありません。IPベースのアクセス制御を適用することもできますが、通常は認証後の制御を目的としています。
B). カスタムドメインを割り当て、HTTPS、allUsers IAM、ファイアウォールルール、VPC SC を有効化: Cloud Run はカスタムドメインと HTTPS をサポートし、allUsers はこれを公開しますが、直接の Cloud Run サービスは、パブリック Ingress に従来の VPC ファイアウォールルールを活用しません。VPC Service Controls は API アクセスとデータ流出を目的としており、WAF やパブリック Web トラフィックのジオブロッキングには利用できません。
D）Cloud DNS パブリックゾーン、静的 IP、VPC ファイアウォール ルール、脅威シグネチャ :Cloud Run サービスはマネージド型であり、通常、パブリック トラフィックの VPC ファイアウォール ルールに直接関連付けられる静的 IP アドレスを公開しません。VPC ファイアウォール ルールは、VPC 内の VM に適用され、Cloud Run のパブリック エンドポイントのマネージド グローバル インフラストラクチャには適用されません。
したがって、サーバーレス NEG を使用して外部 HTTP(S) ロードバランサをデプロイし、それを Google マネージド証明書および Cloud Armor と統合することは、一般公開されている Cloud Run アプリケーションに指定されたすべてのセキュリティ要件を満たすための最も包括的で Google が推奨するソリューションです。

最新問題**: 218**
組織のインフラストラクチャをGCPに移行する際には、多数のユーザーがGCP Consoleにアクセスする必要があります。Identity Managementチームは既にユーザー管理のための確立された方法を確立しており、既存のActive DirectoryまたはLDAPサーバーと既存のSSOパスワードを引き続き使用したいと考えています。
何をすべきでしょうか?
A. Google ドメインのデータを既存の Active Directory または LDAP サーバーと手動で同期します。

B. Google Cloud Directory Sync を使用して、Google ドメイン内のデータを既存の Active Directory または LDAP サーバーと同期します。
C. ユーザーは、オンプレミスの Kerberos 準拠 ID プロバイダの認証情報を使用して、GCP Console に直接サインインします。
D. ユーザーは OpenID (OIDC) 互換の IdP を使用してサインインし、認証トークンを受け取り、そのトークンを使用して GCP コンソールにログインします。
Answer: (解答を表示する**)**
ID 管理用の既存の Active Directory または LDAP サーバーを維持しながら、多数のユーザーが GCP Console にアクセスできるようにするには、Google Cloud Directory Sync（GCDS）を使用します。
* GCDS をインストールします。
* ここから Google Cloud Directory Sync をダウンロードしてインストールします。
* GCDS を設定します。
* LDAP サーバーの詳細と Google ドメインを指定して同期を設定します。
* ユーザーデータが正しく同期されるように、LDAP 属性を Google 属性にマッピングします。
* 同期を実行:
* 初期同期を実行して、LDAP サーバーの既存のユーザーを Google ドメインに追加します。
* データを最新の状態に保つために定期的な同期をスケジュールします。
利点：
* 自動同期: 手動による介入なしにユーザー データが一貫して更新されることを保証します。
* 安全なアクセス: ユーザーは既存の認証情報を使用して GCP コンソールにログインできるため、セキュリティとユーザー エクスペリエンスが向上します。
参考文献:
* Google Cloud Directory Sync ドキュメント
* GCDS 管理ガイド

最新問題**: 219**
会社で承認されたコンピューティング イメージを、イメージ リポジトリとして使用される単一の Google Cloud プロジェクトに保存しています。このプロジェクトは VPC Service Controls で保護されており、組織内の他のプロジェクトとともに境界内に存在します。これにより、他のプロジェクトはイメージ リポジトリ プロジェクトからイメージをデプロイできます。
チームでは、外部の Google Cloud 組織に保存されているサードパーティのディスク イメージをデプロイする必要があります。
境界内に展開できるように、ディスク イメージへの読み取りアクセスを許可する必要があります。
何をすべきでしょうか?
A. * 1 境界を更新する
* 2 egressTo フィールドを構成して、ID タイプを any_identity に設定します。
* 3 許可されたリソースとして外部 Google Cloud プロジェクト番号を含めるように egressFrom フィールドを設定し、serviceName を compute. googleapis. com に設定します。
B. * 組織ポリシーを使用して外部プロジェクトを許可する

制約/compute.trustedImageProjects。
C. * 1 境界を更新する
* 2 egressTo フィールドを設定して、許可されたリソースとして外部の Google Cloud プロジェクト番号を含め、serviceName を compute. googleapis. com に設定します。
* 3 egressFrom フィールドを構成して、ID タイプを any_idestity に設定します。
D. * 1 境界を更新する
* 2 ingressFrcm フィールドを設定して、identityType を an-y_identity に設定します。
* 3 ingressTo フィールドを設定して、許可されたリソースとして外部の Google Cloud プロジェクト番号を含め、serviceName を compute.googleapis -com に設定します。
Answer: A (メーッセージを残す**)**
外部の Google Cloud 組織に保存されているサードパーティのディスク イメージへの読み取りアクセス権を付与して、VPC Service Controls 境界にデプロイできるようにするには、プロジェクトから外部プロジェクトへの下り（外向き）トラフィックを許可するようにサービス境界を更新する必要があります。
* サービス境界を更新します。
* Google Cloud Console にアクセスし、[セキュリティ] > [VPC Service Controls] に移動します。
* イメージ リポジトリ プロジェクトを含む適切なサービス境界を選択します。
* 出力ポリシーを構成する:
* 境界設定内で、外部プロジェクトへのトラフィックを許可するように egressTo フィールドを構成します。
* この特定の出力ルールの外部プロジェクトへのアクセスをすべてのプリンシパルに許可するには、identityType を ANY_IDENTITY に設定します。
* 外部プロジェクトとサービスを指定します:
* egressFrom フィールドに、許可されたリソースとして外部の Google Cloud プロジェクト番号を含めます。
* 外部プロジェクト内の Compute Engine サービスへのアクセスを明示的に許可するには、serviceName を compute.googleapis.com に設定します。
この構成により、サービス境界によって確立されたセキュリティ境界を維持しながら、内部プロジェクトが外部プロジェクトからディスク イメージを読み取ることができるようになります。
参考文献:
* VPC サービスコントロールのドキュメント
* サービス境界の構成

最新問題**: 220**
顧客は、インターネット アクセスを制限する必要がある Compute Engine 上で分析ワークロードを実行しています。
チームは、インターネットへのすべてのトラフィックを拒否する (優先度 1000) 出力ファイアウォール ルールを作成しました。
Compute Engine インスタンスは、セキュリティアップデートを取得するために公開リポジトリにアクセスする必要があります。チームとして何をすべきでしょうか？
A. 優先度が 1000 を超えるリポジトリの CIDR 範囲へのトラフィックを許可する出力ファイアウォール ルールを作成します。

B. 優先度が 1000 未満のリポジトリの CIDR 範囲へのトラフィックを許可する出力ファイアウォール ルールを作成します。
C. 優先度が 1000 を超えるリポジトリのホスト名へのトラフィックを許可する出力ファイアウォール ルールを作成します。
D. 優先度が 1000 未満のリポジトリのホスト名へのトラフィックを許可する出力ファイアウォール ルールを作成します。
Answer: B (メーッセージを残す**)**
すべてのインターネットトラフィックを拒否する下りファイアウォールルールを適用しながら、Compute Engineインスタンスがセキュリティアップデート用の公開リポジトリにアクセスできるようにするには、リポジトリのCIDR範囲へのトラフィックを許可する、より具体的な下りルールを作成する必要があります。このルールの優先度は、拒否ルールよりも低く（つまり、優先度番号を大きく）する必要があります。
手順:
CIDR 範囲を特定する: セキュリティ更新を取得するパブリック リポジトリの CIDR 範囲を決定します。
出力ファイアウォール ルールの作成: 優先度が 1000 未満の、特定された CIDR 範囲へのトラフィックを許可する新しい出力ファイアウォール ルールを作成します。
ファイアウォール ルールを適用する: Google Cloud Console または gcloud コマンドライン ツールを使用して、新しいファイアウォール ルールを適用します。
参照：
Google Cloud: ファイアウォール ルール
ファイアウォールルールの作成

最新問題**: 221**
あなたは会社のセキュリティ管理者です。Cloud Storage バケットには 3,000 個のオブジェクトがあります。各オブジェクトへのアクセスを個別に管理したくありません。また、オブジェクトのアップロード者に常にオブジェクトのフルコントロール権限を与えることも望んでいません。しかし、バケットへのアクセス管理には Cloud Audit Logs を使用したいと考えています。
何をすべきでしょうか?
A. allUsers のスコープに OWNER 権限を持つ ACL を設定します。
B. allUsers のスコープに READER 権限を持つ ACL を設定します。
C. デフォルトのバケット ACL を設定し、IAM を使用してユーザーのアクセスを管理します。
D. Cloud Storage バケットに均一なバケットレベルのアクセスを設定し、IAM を使用してユーザーのアクセスを管理します。
Answer: D (メーッセージを残す**)**
https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled

最新問題**: 222**
ある企業がデータセンター全体をGoogle Cloud Platformに移行しました。複数のプロジェクトにまたがり、複数の部門が管理する数千ものインスタンスが稼働しています。Google Cloud Platformでどの時点で何が実行されていたか、履歴記録を残しておきたいと考えています。
何をすべきでしょうか?

A. 組織レベルでリソース マネージャーを使用します。
B. Forseti Security を使用してインベントリ スナップショットを自動化します。
C. Stackdriver を使用して、すべてのプロジェクトにわたるダッシュボードを作成します。
D. Security Command Center を使用して、組織全体のすべての資産を表示します。
Answer: B (メーッセージを残す)
説明
Forseti セキュリティのみが、リソースの 過去」と 現在」つまり、履歴）の両方の記録を保持できます。
https://forsetisecurity.org/about/

最新問題**: 223**
コンテナイメージ内のパッケージのCVE情報を収集 分析し、既知のセキュリティ問題のあるイメージがGoogle Kubernetes Engine環境で実行されないようにしたいと考えています。コンテナビルドパイプラインに含めることをGoogleが推奨するセキュリティ機能は2つあります。
A. デプロイメントポリシー
B. パスワードポリシー
C. 脆弱性スキャン
D. ネットワーク分離
Answer: (解答を表示する)
A は正解です。Binary Authorization で定義されたデプロイメントポリシーにより、Google Kubernetes Engine クラスタには信頼できるイメージのみがデプロイされます。Binary Authorization は Container Analysis と統合でき、Container Registry に保存されているコンテナイメージの脆弱性をスキャンし、認可プロセスで使用される信頼できるメタデータを保存します。
B はユースケースに対応していないため不正解です。
C が正解です。Container Analysis によって脆弱性スキャンを実行し、コンテナ ベース イメージ内のパッケージの脆弱性情報を検出し、それぞれの Linux ディストリビューションから CVE データを取得できるためです。
D はユースケースに対応していないため不正解です。
https://cloud.google.com/binary-authorization/docs/概要
https://cloud.google.com/container-registry/docs/container-analysis

最新問題**: 224**
あなたの会社は、顧客の年齢層に応じて信用スコアの向上を支援するために、どのような商品を開発できるかを検討したいと考えています。そのためには、会社の銀行アプリのユーザー情報と、サードパーティから取得した顧客の信用スコアデータを統合する必要があります。この生データを使用することでこのタスクは完了しますが、機密データが露出し、新しいシステムに伝播される可能性があります。
このリスクに対処するには、データベース全体の参照整合性を維持しながら、Cloud Data Loss Prevention による匿名化とトークン化を行う必要があります。これらの要件を満たすには、どの暗号トークン形式を使用すべきでしょうか？
A. 決定論的暗号化
B. 安全なキーベースのハッシュ
C. フォーマット保持暗号化

D. 暗号ハッシュ
Answer: (解答を表示する**)**
この暗号化方法は可逆的であるため、データベース全体の参照整合性を維持するのに役立ち、文字セットの制限もありません。
https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how- tokenization-makes-data-usable-without-sacrificing-privacy

最新問題**: 225**
オンプレミスのデータウェアハウスをBigQuery Cloud SQLとCloud Storageに移行しています。データウェアハウスでセキュリティサービスを構成する必要があります。会社のコンプライアンスポリシーでは、データウェアハウスに対して以下の要件が定められています。
* 暗号化キーの完全なライフサイクル管理により保存データを保護
* データ管理とは別のキー管理プロバイダを実装する
* すべての暗号化キー要求を可視化する
データ ウェアハウスの実装にはどのようなサービスを含める必要がありますか?
2つの回答を選択してください
A. クラウド外部キーマネージャー
B. 顧客管理の暗号化キー
C. アクセスの透明性と承認
D. キーアクセスの正当化
E. 顧客提供の暗号化キー
Answer: A,D (メーッセージを残す**)**

最新問題**: 226**
あなたの会社は、Google Cloud Platform 上に個人情報（PII）を保存するウェブサイトを運営しています。データプライバシー規制を遵守するため、このデータは一定期間のみ保存され、一定期間経過後は完全に削除する必要があります。保存期間が経過していないデータは削除すべきではありません。この規制への準拠プロセスを自動化したいと考えています。
何をすべきでしょうか?
A. データを単一の永続ディスクに保存し、有効期限が切れるとディスクを削除します。
B. データを単一の BigQuery テーブルに保存し、適切なテーブル有効期限を設定します。
C. データを Cloud Storage バケットに保存し、バケットのオブジェクト ライフサイクル管理機能を構成します。
D. データを単一の BigTable テーブルに保存し、列ファミリーに有効期限を設定します。
Answer: (解答を表示する**)**
オブジェクトの有効期限（TTL）の設定、オブジェクトの非最新バージョンの保持、コスト管理のためのオブジェクトのストレージ クラスの「ダウングレード」といった一般的なユースケースをサポートするため、Cloud Storage ではオブジェクトのライフサイクル管理機能を提供しています。このページでは、この機能と、使用時に利用できるオプションについて説明します。

オブジェクトのライフサイクル管理を有効にする方法とライフサイクル ポリシーの例については、「ライフサイクルの管理」をご覧ください。https://cloud.google.com/storage/docs/lifecycle

最新問題: **227**
チームは、組織レベルで管理者権限を持つユーザーを制限したいと考えています。チームが制限する必要がある 2 つのロールはどれですか? (2 つ選択してください。)
A. 組織管理者
B. スーパー管理者
C. NGO クラスター管理者
D. コンピューティング管理者
E. 組織ロール閲覧者
Answer: A,B (メーッセージを残す**)**
説明/参考資料: https://cloud.google.com/resource-manager/docs/creating-managing-organization

最新問題: **228**
Compute Engine でホストされるウェブアプリケーションをデプロイしています。ビジネス要件により、アプリケーションログは12年間保存され、データは欧州域内に保管されることが義務付けられています。オーバーヘッドを最小限に抑え、費用対効果の高いストレージソリューションを実装したいと考えています。どうすればよいでしょうか？
A. EUROPE-WEST1 リージョンにログを保存するための Cloud Storage バケットを作成します。アプリケーションコードを変更して、ログをバケットに直接送信し、効率性を高めます。
B. Google Cloud のオペレーション スイートの Cloud Logging エージェントを使用して、12 年間のカスタム保持期間でアプリケーション ログを EUROPE-WEST1 リージョンのカスタム ログバケットに送信するように Compute Engine インスタンスを構成します。
C. Pub/Sub トピックを使用して、アプリケーション ログを EUROPE-WEST1 リージョンの Cloud Storage バケットに転送します。
D. EUROPE-WEST1 リージョンの Google Cloud オペレーション スイートのログバケットに 12 年間のカスタム保持ポリシーを構成します。
Answer: B (メーッセージを残す**)**

ログを 12 年間保存し、ヨーロッパの境界内でデータの保存場所を確保するという要件を満たすには、目的のリージョンで構成されたカスタム ログバケットを備えた Google Cloud のオペレーション スイート（旧称 Stackdriver）を使用するのが最適です。
Cloud Logging エージェントを構成します。
Compute Engine インスタンスに Cloud Logging エージェントをインストールして設定します。このエージェントは、アプリケーションとシステムからログを収集し、Google Cloud のオペレーション スイートに送信します。
カスタム ログ バケットを作成します。
Cloud Logging インターフェースで、EUROPE-WEST1 リージョンにカスタム ログバケットを作成します。このバケットにログが保存され、カスタム保持期間を設定できます。
カスタム保持ポリシーを設定する:
カスタムログバケットの保持ポリシーを12年に設定します。これにより、すべてのログが必要な期間保持されます。
ログをカスタム ログ バケットに送信します。
Cloud Logging エージェントからのログをカスタムログバケットに送信するように、ログ設定を変更してください。これは、Cloud Console のログ設定から、またはエージェント設定ファイルを更新することで実行できます。
このソリューションは、マネージド サービスを使用することでオーバーヘッドを最小限に抑え、ログの保存と保持管理のための Cloud Logging の組み込み機能を活用してコスト効率を確保します。
参照：
Cloud Logging ドキュメント
ログバケットの作成と管理

最新問題**: 229**
組織では、Compute Engine の仮想マシン（VM）に大きく依存しています。チームの成長とリソース需要の増加により、VM の無秩序な増加が問題となっています。一貫したセキュリティ強化とタイムリーなパッケージ更新の維持は、ますます困難になっています。VM イメージ管理を一元化し、仮想マシンのライフサイクル全体にわたってセキュリティ ベースラインの適用を自動化する必要があります。どうすればよいでしょうか？
A. Security Command Center Enterprise を有効化します。VM 検出およびポスチャ管理機能を使用して、強化状態を監視し、問題が検出されると自動レスポンスをトリガーします。B. Cloud Build トリガーを作成し、強化された VM イメージを生成するパイプラインを構築します。パイプラインで脆弱性スキャンを実行し、スキャンに合格したイメージをレジストリに保存します。このレジストリを指すインスタンス テンプレートを使用します。
B. すべてのプロジェクトに対して Compute Engine の単一テナンシー機能を設定します。Policy Controller でカスタム組織ポリシーを設定し、チームが使用できるオペレーティング システムとイメージ ソースを制限します。
C. VM Manager を使用すると、プロジェクト全体の VM にパッチを自動的に配布および適用できます。VM Manager を、中央リポジトリに保存されている強化された組織標準の VM イメージと統合できます。
Answer: B (メーッセージを残す**)**

VM 作成段階 (VM ライフサイクル管理) で一貫したセキュリティ ベースラインを適用しながら VM の拡散に対処する最も効果的な方法は、自動化されたパイプラインを介して構築された不変の強化されたイメージを使用することです。
一元的なイメージ管理と強化 :Cloud Build パイプラインは、「ゴールデンイメージ」の作成を自動化する標準的な方法です。このパイプラインでは、OS やパッケージのインストール、強化スクリプト（CIS ベンチマークなど）の適用、脆弱性スキャンの実行が可能で、検証済みの安全なイメージのみを中央レジストリに保存できます。これにより、セキュリティ ベースラインを一元的に管理できます。
適用 :インスタンステンプレートは、VMのデプロイを標準化するメカニズムです。テンプレートを、承認済みの強化されたイメージの中央レジストリのみを参照するように設定することで、新たに起動されるすべてのVMがセキュリティベースラインに自動的に準拠することを保証できます。これにより、強化されていないイメージや安全でないイメージのデプロイを防ぎ、「VMのスプロール化」と「一貫したセキュリティ強化」の問題を根本から解決できます。
オプション A (SCC ポスチャ管理) は、VM の展開後に監視する検出制御です。ライフサイクル管理の目的である、強化されていない VM の作成を防ぐことはできません。
オプション D (VM マネージャー) は、既存の VM の継続的なパッチ適用と更新には最適ですが、安全で集中管理された強化されたイメージが作成に使用されることを保証するという初期の問題は解決されません (ここでベースラインが適用されます)。
抜粋:
「サーバーを作成するために構成され使用されるゴールデンイメージは、企業が安全に拡張できるようにする上で重要な役割を果たします。」（出典1.2）
自動化ツールを使用すれば、この問題は解消されます。エンジニアが[自動化ツール]で生成された画像を使用する場合、必要なものがすべて画像にあらかじめ組み込まれているため、証拠は明確です。(出典1.2)
「インスタンス テンプレートは、マシンタイプ、ブートディスク イメージなどを含む仮想マシン (VM) インスタンスの構成を保存する便利な方法です。インスタンス テンプレートを使用すると、個別の VM を作成できます。」(出典 3.3) オプション B で説明されている全体的な戦略 (テンプレートによる強化、スキャン、保存、使用の強制の自動化) は、大規模で安全かつコンプライアンスに準拠した VM の展開のためのベスト プラクティスです。

最新問題**: 230**
サポートセンターのエージェントとオンラインチャットでやり取りする際、顧客が個人情報（PII）を含む書類の写真を共有することがよくあります。サポートセンターを運営する組織は、社内または社外のアナリストによる顧客サービスの傾向分析のために定期的に保存しているチャットログにPIIが含まれ、データベースに保存されることを懸念しています。
データの有用性を維持しながら顧客のこの懸念を解決するために、組織はどの Google Cloud ソリューションを使用すべきでしょうか。
A. 顧客が共有する PII データを分析用に保存する前に、Cloud Key Management Service (KMS) を使用して暗号化します。
B. オブジェクトライフサイクル管理を使用して、PII が含まれるすべてのチャット記録が破棄され、分析用に保存されないようにします。

C. DLP API の画像検査および編集アクションを使用して、分析用に保存する前に画像から PII を編集します。
D. DLP API ソリューションの一般化およびバケット化アクションを使用して、分析用に保存する前にテキストから PII を編集します。
Answer: D (メーッセージを残す**)**
参考: https://cloud.google.com/dlp/docs/deidentify-sensitive-data

最新問題**: 231**
ある企業は、さまざまな Google Cloud Platform リージョンに冗長メール サーバーを保有しており、場所に基づいて顧客を最も近いメール サーバーにルーティングしたいと考えています。
企業はどのようにこれを達成すべきでしょうか?
A. TCP プロキシ負荷分散を、ポート 995 でリッスンするグローバル負荷分散サービスとして構成します。
B. 場所に基づいてトラフィックを転送する転送ルールを使用して、TCP ポート 995 をリッスンする Network Load Balancer を作成します。
C. HTTP(S) ロードバランサによるクロスリージョン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ルーティングします。
D. Cloud CDN を使用して、クライアント IP アドレスに基づいてメール トラフィックを最も近い元のメール サーバーにルーティングします。
Answer: (解答を表示する**)**
https://cloud.google.com/load-balancing/docs/tcp

最新問題**: 232**
あなたは規制の厳しい業界の企業に勤務し、クラウド環境の継続的なセキュリティ確保に責任を負っています。特定のコンプライアンスポリシーに基づき、特定のフォルダにおける設定ミスを防止 検出する必要があります。業界固有のコンプライアンスポリシーと社内ポリシーを遵守する必要があります。どうすればよいでしょうか？
A. 業界の規制に適した特定のコントロール バンドルを使用して、フォルダー レベルで Assured Workloads を有効にします。
B. Workload Manager とカスタム Rego ポリシーを使用して、フォルダレベルで環境の誤構成を継続的にスキャンします。C. カスタムおよび定義済みの SHA または組織ポリシーを使用してポスチャファイルを作成します。フォルダレベルでポスチャを適用します。
C. 特定のビジネス要件に沿ったカスタム組織ポリシーを作成します。ポリシーはフォルダレベルで適用します。
Answer: C (メーッセージを残す**)**
正確な抜粋からの包括的かつ詳細な説明：
要件は、フォルダレベルで適用される予防的制御と検出的制御（構成ミスの防止と検出）の組み合わせであり、業界固有の（事前定義された標準）ポリシーと社内／カスタムポリシーの両方を満たす必要があります。このための専用のGoogle Cloud機能は、Security Command Center（SCC）のセキュリティ態勢管理です。

態勢と適用 :セキュリティ態勢は、SCC Premium/Enterpriseの機能であり、クラウド資産のセキュリティ状態を定義、展開、監視できます。組織、フォルダ、またはプロジェクトレベルで態勢を展開し、標準を適用できます。
カスタム ポリシーと定義済みポリシー: ポスチャは次の両方を組み合わせます。
定義済みポリシー: セキュリティヘルスアナリティクス（SHA）検出器とマッピングされた標準（CIS、ISOなど）を使用する
27001、PCI DSS は、業界固有のコンプライアンス要件 (検出) をカバーしています。
カスタム ポリシー: カスタム組織ポリシー制約とカスタム SHA モジュールを使用すると、社内ポリシー (防止と検出) を適用および検出できます。
抜粋:
Google Cloud では、Security Command Center のセキュリティ ポスチャ サービスを使用して、セキュリティ ポスチャを定義および展開し、Google Cloud リソースのセキュリティ ステータスを監視できます...」（出典 2.3）
「ポスチャは組織レベル、フォルダレベル、またはプロジェクトレベルで展開できます。」(ソース 2.3)
セキュリティ ポスチャ サービスには、次のコンポーネントが含まれます: ポスチャ。組織がセキュリティ標準を満たすために必要な予防的制御と検出的制御を実施する 1 つ以上のポリシー セット...
サポートされているポリシーは次のとおりです: 組織ポリシー制約（カスタム制約を含む）
[予防的]。カスタムモジュールを含むセキュリティヘルスアナリティクス検出器[検出的]。(出典2.3、8.2) オプションCは、必要な範囲(フォルダ)で適用されるカスタムポリシーと定義済みポリシーをサポートするポスチャファイルを使用して、予防と検出の両方を実現する包括的なソリューションを正しく識別します。

最新問題**: 233**
ある会社では、全従業員にGoogle Cloud Platformの利用を許可しています。各部門にはGoogleグループがあり、部門メンバー全員がグループメンバーとして参加しています。ある部門メンバーが新しいプロジェクトを作成すると、その部門のメンバー全員が、すべての新規プロジェクトリソースへの読み取り専用アクセス権を自動的に付与する必要があります。他の部門のメンバーは、そのプロジェクトにアクセスできません。この動作を設定する必要があります。
これらの要件を満たすにはどうすればよいでしょうか?
A. 組織の下に部門ごとにフォルダを作成します。各部門のフォルダに対して、その部門に関連するGoogleグループにプロジェクト閲覧者ロールを割り当てます。
B. 組織の下に部門ごとにフォルダを作成します。各部門のフォルダに対して、その部門に関連するGoogleグループにプロジェクト閲覧者ロールを割り当てます。
C. 組織の下に部門ごとにプロジェクトを作成します。各部門のプロジェクトについて、その部門に関連するGoogleグループにプロジェクト閲覧者ロールを割り当てます。
D. 組織の下に部門ごとにプロジェクトを作成します。各部門のプロジェクトごとに、その部門に関連するGoogleグループにプロジェクト閲覧者ロールを割り当てます。
Answer: A (メーッセージを残す**)**

各部門メンバーが、任意の部門メンバーが作成したすべての新しいプロジェクトリソースに対して自動的に読み取り専用アクセス権を持つように動作を設定するには、Google Cloud のフォルダ構造と IAM ロールを効果的に使用する必要があります。手順は以下のとおりです。
部門別フォルダの作成：組織内に各部門のフォルダを作成します。フォルダはリソースを整理し、ポリシーと権限を適用するための階層構造を構築するのに役立ちます。
Google グループに IAM ロールを割り当てる：各部門に関連付けられた Google グループに、フォルダレベルでプロジェクト閲覧者ロールを割り当てます。これにより、グループのすべてのメンバーに必要な権限が付与されます。
継承された権限：部門メンバーが所属する部門のフォルダ内に新しいプロジェクトを作成すると、そのフォルダに割り当てられた権限が新しいプロジェクトに継承されます。そのため、部門メンバー全員が自動的にプロジェクトのリソースへの読み取り専用アクセス権を持つことになります。
GCP コンソールで [IAM と管理] に移動します。
左側のメニューから「フォルダー」を選択します。
部門ごとに、組織の下に新しいフォルダーを作成します。
新しく作成したフォルダを選択し、「権限」タブに移動します。
新しいロールを割り当てるには、「追加」をクリックします。
部門の Google グループのメール アドレスを入力します。
グループに「プロジェクト閲覧者」ロールを割り当てます。
アクセス制限：権限はフォルダレベルで適用されるため、特定の部門のGoogleグループのメンバーのみが、そのフォルダ内に作成されたプロジェクトへの読み取り専用アクセス権限を持ちます。他の部門は、明示的に許可されない限りアクセスできません。
これらの手順に従うことで、新しいプロジェクトごとに手動で構成することなく、部門メンバーがそれぞれのプロジェクトに必要なアクセス権を持つことができるようになります。
Google Cloud IAM ドキュメント
Google Cloud Resource Manager のドキュメント

最新問題: **234**
組織には、Google Cloud API にアクセスする必要があるオンプレミス ホストがあります。これらのホスト間にプライベート接続を適用して、コストを最小限に抑え、運用効率を最適化する必要があります。何をすべきでしょうか?
A. すべてのオンプレミス トラフィックを、プライベート Google アクセスが有効になっている VPC への IPsec VPN トンネル経由で Google Cloud にルーティングします。
B. オンプレミスのホストと VPC 間の VPC ピアリングをインターネット経由で設定します。
C. すべてのアプリケーションでデータをネットワーク経由で送信する前に、Cloud Key Management Service (KMS) キーを使用してデータを暗号化することを義務付けるセキュリティ ポリシーを適用します。
D. すべてのオンプレミス トラフィックを、専用またはパートナー相互接続を介して、プライベート Google アクセスが有効になっている VPC に Google Cloud にルーティングします。
Answer: (解答を表示する**)**

オンプレミスホストとGoogle Cloud API間のプライベート接続を、コストと運用効率を最適化しながら確保するには、専用またはパートナー相互接続の使用が最適なソリューションです。この設定により、プライベートIPアドレスによる信頼性の高い高帯域幅の接続が確保されます。
相互接続タイプを選択: 帯域幅のニーズと Google Cloud のロケーションへの近さに基づいて、Dedicated Interconnect と Partner Interconnect のどちらかを選択します。
相互接続の設定:
Dedicated Interconnect の場合は、Google Cloud Console から回線を注文します。
パートナー相互接続の場合は、サポートされているサービス プロバイダーを選択し、そのプロバイダーを通じて接続を注文します。
VPC とプライベート Google アクセスを構成します。
VPC でプライベート Google アクセスを有効にして、オンプレミス ホストが Google API にプライベートにアクセスできるようにします。
「VPC ネットワーク」-> 「プライベート Google アクセス」に移動し、サブネットに対して有効にします。
接続を確立する: ネットワーク チームおよび (該当する場合) パートナー相互接続プロバイダーと協力して、物理接続と論理接続を設定します。
接続のテスト: オンプレミス ホストがプライベート IP アドレスを使用して Google Cloud サービスにアクセスできることを確認します。
参照：
Google Cloud Interconnect の概要
プライベートGoogleアクセスの設定

最新問題**: 235**
ある顧客が、Compute Engine でホストされている ERP システムに Cloud Identity-Aware Proxy を実装しています。セキュリティチームは、ERP システムが Cloud Identity-Aware Proxy からのトラフィックのみを受け入れるようにセキュリティ レイヤーを追加したいと考えています。
これらの要件を満たすために顧客は何をすべきでしょうか?
A. ERP システムが HTTP リクエスト内のユーザーの一意の識別子ヘッダーを検証できることを確認します。
B. ERP システムが HTTP リクエスト内の ID ヘッダーを検証できることを確認します。
C. ERP システムが HTTP リクエスト内の x-forwarded-for ヘッダーを検証できることを確認します。
D. ERP システムが HTTP リクエスト内の JWT アサーションを検証できることを確認します。
Answer: D (メーッセージを残す**)**

最新問題**: 236**
お客様の会社には複数の事業部門があります。各事業部門は独立して運営されており、それぞれにエンジニアリンググループがあります。お客様のチームは、社内で作成されたすべてのプロジェクトを可視化し、Google Cloud Platform（GCP）プロジェクトを事業部門ごとに整理したいと考えています。また、各事業部門には個別のIAM権限セットが必要です。
これらのニーズを満たすには、どのような戦略を採用すべきでしょうか?
A. 組織ノードを作成し、各ビジネス ユニットにフォルダーを割り当てます。

B. gmail.com アカウントを使用して、各ビジネス ユニットのスタンドアロン プロジェクトを確立します。
C. プロジェクト内の GCP リソースを割り当て、どのビジネス ユニットがリソースを所有しているかを識別するラベルを付けます。
D. 各ビジネス ユニットの VPC 内の GCP リソースを割り当てて、ネットワーク アクセスを分離します。
Answer: (解答を表示する**)**
GCPプロジェクトを異なる事業部門に基づいて整理し、IAM権限を管理するには、組織ノードを作成し、各事業部門にフォルダを割り当てる必要があります。このアプローチにより、プロジェクトをフォルダ内で論理的に分離し、フォルダレベルでIAMポリシーを適用できます。
ステップバイステップ:
組織ノードの作成: GCP アカウントが組織にリンクされていることを確認します。
ビジネスユニットのフォルダーを作成します。
GCP コンソール > IAM と管理 > リソース マネージャーに移動します。
組織ノードの下に各ビジネス ユニットのフォルダーを作成します。
プロジェクトをフォルダーに移動する:
既存のプロジェクトをビジネス ユニットに応じてそれぞれのフォルダーに移動します。
IAM ポリシーを設定する:
フォルダー レベルで IAM ロールと権限を割り当てて、各ビジネス ユニットのアクセスを個別に管理します。
監視と管理: Cloud Audit Logs やその他の GCP ツールを使用してアクティビティを監視し、組織のポリシーに準拠していることを確認します。
参照：
フォルダーの作成と管理
IAMポリシーの管理

最新問題**: 237**
金融サービス会社が業務を Google Cloud に移行しています。厳格な規制コンプライアンス要件を満たすため、集中ログ戦略を実装しています。会社の Google Cloud 組織には、すべての本番環境プロジェクト専用のフォルダがあります。この本番環境フォルダ内の現在および将来のすべてのプロジェクトのデータアクセスログを含むすべての監査ログは、長期保存と分析のために、中央の BigQuery データセットに安全に収集および保存する必要があります。ログの重複保存を防ぎ、集中管理を強化するには、これらの監査ログのプロジェクトレベルのログシンクを傍受してオーバーライドするロギング ソリューションを実装し、ログが誤って他の場所にルーティングされないようにする必要があります。どうすればよいでしょうか？
A. 本番環境フォルダレベルで集約ログシンクを作成し、中央のBigQueryデータセットを出力先として設定します。すべての監査ログとデータアクセスログの包含フィルタを設定します。本番環境フォルダのシンクのサービスアカウントにログバケット書き込みロールを付与します。
B. 各本番環境プロジェクトにログシンクを作成し、監査ログを中央のBigQueryデータセットにルーティングします。各シンクのwriter_identityフィールドに、中央データセットに対するBigQueryデータ編集者権限を持つサービスアカウントを設定します。
C. 組織レベルで集約ログシンクを作成し、BigQueryの中央データセットを出力先として、すべての監査ログをフィルタリングします。--include-children フラグを使用し、productionフォルダのログビューを設定します。

D. 本番環境フォルダレベルで、中央のBigQueryデータセットを宛先とするインターセプト集約ログシンクを作成します。必要な監査ログの包含フィルタを設定します。シンクのwriter_identityに、BigQueryデータセットに対する適切なIAM権限を付与します。

Answer: (解答を表示する**)**

この問題の重要な要件は、すべての監査ログ（データ アクセス ログを含む）を本番環境フォルダから中央の BigQuery データセットに一元的に収集し、長期保存することです。そして最も重要なのは、重複した保存や誤ったルーティングを防ぐために、プロジェクト レベルのログ シンクを傍受してオーバーライドできることです。

フォルダレベルでの集約ログシンク：現在および将来のすべてのプロジェクトからのログをフォルダ内に一元管理します。

「プロダクションフォルダ」の場合、フォルダレベルで集約シンクを設定するのが正しいアプローチです。子プロジェクトで生成されたログはフォルダレベルまで流れ、このシンクによって照合されます。

抜粋参照: 「集約エクスポートを使用すると、複数の Google Cloud プロジェクト、フォルダ、または組織全体からログをエクスポートできます。集約エクスポートには、含まれるすべてのリソースのすべてのログを含めることも、クエリを使用して特定のログのみを含めることもできます。」(Google Cloud ドキュメント: 「サポートされている出力先にログをルーティングする | Cloud Logging」 - https://cloud.google.com/logging/docs/export/aggregated_exports) インターセプトシンク (--intercept-logs / overrideDestinations): これは、「インターセプトとオーバーライド」の要件を満たすための重要な機能です。集約シンクが「インターセプト」シンクとして構成されている場合、そのフィルタに一致するログエントリはすべて直ちにその出力先にルーティングされ、下位レベルのシンク (例:

これにより、ログが誤って他の場所にルーティングされることがなくなり、重複したストレージが防止されます。

抜粋参照: 「インターセプトシンクは集約シンクであり、overrideDestinationsフィールドがtrueに設定されている場合、一致したログエントリがCloud Loggingリソース階層内の下位レベルのシンクに伝播されるのを停止します。」(Google Cloudドキュメント: 「サポートされている宛先へのログのルーティング | Cloud Logging」 - https://cloud.google.com/logging/docs/export/aggregated_exports)

BigQuery の保存先と IAM 権限: 長期保存の保存先として BigQuery が指定されています。

シンクの writer_identity（シンク用に自動的に作成されるサービス アカウント）には、ログを書き込むために、対象の BigQuery データセットに対する適切な IAM 権限（BigQuery データ編集者や BigQuery ユーザーなど）が必要です。

監査ログの包含フィルタ: データ アクセス ログ (logName: "cloudaudit.googleapis.com" または logName: "data_access") を含む必要な監査ログのみがルーティングされるようにするには、包含フィルタが必要です。

他のオプションを評価してみましょう。

A) 標準集約ログシンク… ログバケット書き込み: 標準集約シンクは、下位レベルのシンクをインターセプトしたりオーバーライドしたりしません。また、ログバケット書き込みロールは Cloud Logging バケット用であり、BigQuery 用ではありません。正しいロールは BigQuery 用です。

B). 各本番プロジェクトにおけるログシンク :これは集中管理型のソリューションではなく、プロジェクトごとに手動で設定を行う必要があるため、「現在および将来のすべてのプロジェクト」において非効率的でエラーが発生しやすくなります。また、オーバーライドメカニズムも提供されていません。

C). 組織レベルの集約ログシンク…ログビューの設定：組織レベルのシンクは広範な一元管理を提供しますが、要件が組織全体ではなく本番フォルダに限定されている場合は、フォルダレベルのインターセプトシンクの方が対象を絞り込むことができます。ログビューはログを表示するためのものであり、ルーティングやオーバーライドのためのものではありません。集約シンクでは --include-children フラグが暗黙的に指定されますが、インターセプト動作は提供されません。
したがって、監査ログを BigQuery に送信するように構成された、本番環境フォルダ レベルでインターセプト集約ログシンクを作成することは、すべての規定要件、特に重要な「インターセプトとオーバーライド」条件を満たす正確なソリューションです。

最新問題**: 238**
社内で Cloud Data Loss Prevention (DLP) API の導入が進むにつれ、コスト削減のために利用を最適化する必要があります。DLP 対象データは Cloud Storage と BigQuery に保存されます。場所とリージョンはリソース名のサフィックスとして識別されます。
どのようなコスト削減オプションを推奨すべきでしょうか?
A. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットに適切な bytesLimitPerFile 値を設定します。
B. rowsLimit と bytesLimitPerFile を使用してデータをサンプリングし、CloudStorageRegexFileSet を使用してスキャンを制限します。
C. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットの変換単位を最小限に抑えます。
D. FindingLimits と TimespanContfig を使用してデータをサンプリングし、変換単位を最小限に抑えます。
Answer: B (メーッセージを残す**)**

最新問題**: 239**
2 つの VPC ネットワークを接続するために VPC ピアリングを使用することに関連するセキュリティ特性はどれですか (2 つ選択してください)。
A. ピアリングされたネットワークのルート、ファイアウォール、VPN の集中管理
B. 非推移的なピアリングネットワーク。直接ピアリングされたネットワークのみが通信できる。
C. 異なる Google Cloud Platform 組織に属するネットワークをピアリングする機能
D. ピアリングされたネットワークから別のピアリングされたネットワークへのタグを使用して作成できるファイアウォール ルール
E. ピアネットワーク間で特定のサブネットを共有する機能
Answer: (解答を表示する**)**
目標: VPC ピアリングのセキュリティ特性を理解する。
セキュリティ特性:
非推移的ピアリング :VPCピアリング接続は非推移的です。つまり、ピアリングは2つのVPCネットワーク間のみで行われます。VPC AがVPC Bとピアリングされ、VPC BがVPC Cとピアリングされている場合、直接ピアリング接続が確立されない限り、VPC AはVPC Cと通信できません。

組織間ピアリング: VPC ピアリングを使用すると、異なる Google Cloud Platform 組織間で VPC ネットワークを接続し、異なる組織単位間でのプライベート通信を容易にすることができます。
これらの特性により、意図しないデータの公開を防ぎながら、VPC ネットワーク間の制御された安全な接続が保証されます。
参照：
GCP VPC ピアリングのドキュメント
VPC ネットワーク ピアリングの概要

最新問題**: 240**
ある企業がCompute Engine上でアプリケーションを実行していました。アプリケーションのバグにより、悪意のあるユーザーがスクリプトを繰り返し実行し、Compute Engineインスタンスをクラッシュさせる可能性がありました。バグは修正されましたが、このハッキングが再発した場合に備えて通知を受け取りたいと考えています。
何をすべきでしょうか?
A. Stackdriver で Process Health 条件を使用してアラートポリシーを作成し、スクリプトの実行回数が所定のしきい値を下回っていることを確認します。通知を有効にします。
B. Stackdriver で CPU 使用率指標を使用したアラートポリシーを作成します。しきい値を 80% に設定すると、CPU 使用率がこの 80% を超えた場合に通知が送信されます。
C. スクリプトのすべての実行をStackdriver Loggingに記録します。Stackdriver Loggingでログにユーザー定義のメトリックを作成し、そのメトリックを表示するStackdriverダッシュボードを作成します。
D. スクリプトのすべての実行をStackdriver Loggingに記録します。BigQueryをログシンクとして設定し、特定の期間内の実行回数をカウントするBigQueryのスケジュールクエリを作成します。
Answer: (解答を表示する**)**
説明/参考資料: https://cloud.google.com/logging/docs/logs-based-metrics/

最新問題**: 241**
あなたは、複数の Google Cloud リージョンに顧客の機密データを保存している e コマース企業で働いています。開発チームは注文処理用の新しい 3 層アプリケーションを構築し、本番環境に統合する必要があります。新しいアプリケーションのための強固なセキュリティ境界と分離を確保し、認定サードパーティベンダーによる安全なリモートメンテナンスを容易にし、最小権限の原則に従うように、ネットワークアーキテクチャを設計する必要があります。どうすればよいでしょうか？
A. 各層ごとに個別のVPCネットワークを作成します。アプリケーション層とその他の必要なVPC間ではVPCピアリングを使用します。ベンダーには、メンテナンス目的でVPC内のインスタンスへのSSHキーとルートアクセスのみを提供します。
B. 単一のVPCネットワークを作成し、各層に異なるサブネットを作成します。サードパーティベンダー専用の新しいGoogleプロジェクトを作成し、ベンダーにネットワーク管理者のロールを付与します。
VPN アプライアンスを導入し、ベンダーの構成を利用してサードパーティのアクセスを保護します。

C. 各層に個別のVPCネットワークを作成します。アプリケーション層とその他の必要なVPC間ではVPCピアリングを使用します。管理リソースへのリモートアクセスにはIdentity-Aware Proxy (IAP)を有効にし、アクセスを承認されたベンダーに制限します。
D. 単一のVPCネットワークを作成し、各層に異なるサブネットを作成します。サードパーティベンダー専用の新しいGoogleプロジェクトを作成します。ベンダーにそのプロジェクトの所有権と、共有VPC構成を変更する権限を付与します。
Answer: C (メーッセージを残す)
このアプローチにより、アプリケーションの各層が独自のVPC内で分離され、セキュリティが強化されます。VPCピアリングにより、分離を維持しながら層間の必要な通信が可能になります。
リモート アクセスに Identity-Aware Proxy (IAP) を使用すると、最小権限の原則に従って、承認されたベンダーのみが管理リソースにアクセスできるようになります。

最新問題**: 242**
Cloud Security Scanner を使用して、App Engine アプリの脆弱性スキャンを実行する必要があります。スキャン完了後、レポートに期待した数のウェブページが表示されません。マウスオーバーメニューのあるアプリ内のページがレポートに表示されません。スキャンを完了し、メニューを確実にキャプチャするには、どのような操作を行う必要がありますか？
A. 除外された URL を確認します。
B. 新しい結果を返すようにスキャン スケジュールを変更します。
C. 追加の開始 URL を含めるようにスキャンを変更します。
D. スキャンを実行している Google アカウントを調整します。
Answer: C (メーッセージを残す)
A は不正解です。マウスオーバー メニューに表示されない Web ページはスキャンされることが予想されるため、明示的に除外される可能性は低いからです。
B は不正解です。スキャンスケジュールを変更しても、スキャンされる Web ページが増えることはありません。
C は正解です。Cloud Security Scanner は、マウスオーバーで操作する多階層メニューなどの複雑な JavaScript を操作できない可能性があります。このシナリオでは、追加の開始 URL を指定することでスキャン範囲を拡大できます。
D は不正解です。Google アカウントを変更しても、スキャンされるウェブページが増えることはありません。
https://cloud.google.com/security-scanner/docs/scanning

最新問題: **243**
会社のアプリケーションは、ユーザーが管理するサービス アカウント キーを使用してデプロイされています。Google が推奨する手順に従ってキーをローテーションしたいと考えています。
何をすべきでしょうか?
A. Cloud Shell を開き、gcloud iam service-accounts enable-auto-rotate --iam-account=IAM_ACCOUNT を実行します。
B. 新しいキーを作成し、アプリケーションで使用します。古いキーはバックアップキーとしてシステムに保存します。
C. 新しいキーを作成し、アプリケーションで新しいキーを使用します。サービスアカウントから古いキーを削除します。
D. Cloud Shell を開き、gcloud iam service-accounts keys rotate --iam-account=IAM_ACCOUNT --key=NEW_KEY を実行します。
Answer: C (メーッセージを残す**)**

最新問題: **244**
Compute Engine ディスク上のデータを、Cloud Key Management Service（KMS）で管理される鍵を使用して保存時に暗号化する必要があります。これらの鍵に対する Cloud Identity and Access Management（IAM）権限は、すべての鍵に対して同じ権限を持つ必要があるため、グループ化して管理する必要があります。
何をすべきでしょうか?
A. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。キーレベルでIAM権限を管理します。
B. すべての永続ディスクと、このキーリング内のすべてのキーに対して単一のキーリングを作成します。IAM権限はキーリングレベルで管理します。
C. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーレベルで管理します。
D. 永続ディスクごとにキーリングを作成し、各キーリングに1つのキーを含めます。IAM権限はキーリングレベルで管理します。
Answer: (解答を表示する**)**
IAM権限をキーリングレベルで管理する方が、個々のキーレベルで管理するよりも効率的でスケーラブルです。単一のキーリングを作成し、その中にすべての暗号化キーを配置することで、キーリング全体に統一されたIAM権限を適用でき、権限管理が簡素化されます。
手順:
KeyRing を作成する: 永続ディスクに必要なすべての暗号化キーに対して、Cloud KMS に単一の KeyRing を設定します。
暗号化キーの作成: このキーリング内に必要な暗号化キーを生成します。
IAM 権限の設定: KeyRing に IAM ロールと権限を割り当てて、このレベルでのアクセス制御を管理し、KeyRing 内のすべてのキーがこれらの権限を継承するようにします。
参照：

Google Cloud: クラウド キー管理サービス (KMS)
リソースへのアクセスの管理

最新問題: **245**
組織ではゼロトラスト・セキュリティ・モデルを導入し、Chrome Enterprise Premium を使用しています。Cloud Storage に保存されている機密データへのアクセス管理に関心があります。ネットワーク上の場所に関係なく、管理対象デバイス上の承認されたユーザーのみがこのデータにアクセスできるよう、アクセス制御を設定する必要があります。アクセスはデバイスのセキュリティ体制に基づいて制限する必要があります。そのためには、最新のオペレーティング・システム・パッチとウイルス対策ソフトウェアが必要です。どうすればよいでしょうか？
A. Cloud Firewall ルールを使用して、送信元 IP アドレスに基づいて Cloud Storage バケットへのアクセスを制限します。ユーザーに多要素認証方式による認証を要求します。
B. Access Context Manager で、デバイスポリシーを必要とするアクセスレベルを作成します。このアクセスレベルを使用して、コンテキストアウェアアクセスポリシーを作成します。このポリシーを、Cloud Storage バケットを含む VPC Service Controls 境界に適用します。
C. IPアドレス範囲に基づいてIAM条件を設定します。ユーザーにVPN経由の接続を要求します。
基本的なコンプライアンスを確認するために、ユーザー デバイスにエンドポイント検証ソフトウェアを実装します。
D. 特定のユーザーに VPC Service Controls へのアクセスを許可し、Cloud Storage バケットへのアクセス境界を作成します。Identity-Aware Proxy (IAP) を設定して、ユーザーがデータにアクセスする前に認証を行います。1
Answer: (解答を表示する**)**
Cloud Storage 内のデータへのアクセスにおけるデバイスのポスチャ（OS バージョン、暗号化など）を評価するゼロトラスト アーキテクチャを実装するには、コンテキストアウェア アクセス（CAA）を使用する必要があります。CAA は、Access Context Manager を使用して「アクセスレベル」を定義し、VPC Service Controls（VPC-SC）を使用して Cloud Storage などのマネージド サービスにそれらのレベルを適用します。
Google Cloud ドキュメント (VPC Service Controls を使用したコンテキストアウェア アクセス) によると、次のようになります。
VPC Service Controls は、Access Context Manager のアクセスレベルを使用して、ユーザー ID、デバイスのセキュリティステータス（デバイスポリシー）、IP アドレスなど、さまざまな属性に基づいてアクセスを制限できます。2 サービス境界にアクセスレベルを適用することで、特定のコンテキスト要件を満たすリクエストのみがその境界内のリソースにアクセスできるようにすることができます。実装手順：
* アクセス コンテキスト マネージャー: デバイス管理ステータス、最小 OS バージョン、その他のポスチャ要件 (Chrome Enterprise /エンドポイント検証エージェントによって検証) をチェックするアクセス レベルを作成します。
* VPC Service Controls: Cloud Storage バケットを含むプロジェクトの周囲にサービス境界を作成します。
* ポリシーバインディング :アクセスレベルをVPC-SC境界に関連付けます。デバイスポリシー（例：古OS）に適合しないリクエストは、ユーザーが適切なIAMロールを持っていても、APIレイヤーでブロックされます。
参照：

Google Cloud ドキュメント: 「VPC Service Controls - コンテキストアウェア アクセス」
(https://cloud.google.com)
/vpc-service-controls/docs/context-aware-access)。
Google Cloud ドキュメント: 「アクセス コンテキスト マネージャー - デバイス ポリシー属性」
(https://cloud.google.
com/access-context-manager/docs/device-policy を参照してください。

最新問題: **246**
組織では、継続的インテグレーションおよびデリバリー (CI/CD) プラットフォームとして GitHub Actions を使用しています。CI/CD パイプラインから Google Cloud リソースへのアクセスを、最も安全な方法で有効にする必要があります。
何をすべきでしょうか?
A. GitHub を ID プール プロバイダーとして使用するようにワークロード ID フェデレーションを構成します。
B. サービス アカウント キーを作成し、GitHub リポジトリ コンテンツに追加します。
C. Workload Identity を使用して GitHub に認証情報を提供する Google Kubernetes Engine クラスタを構成します。
D. サービス アカウント キーを作成し、GitHub パイプライン構成ファイルに追加します。
Answer: A (メーッセージを残す**)**

最新問題: **247**
顧客の社内セキュリティ チームは、Cloud Storage 上のデータを暗号化するために独自の暗号化キーを管理する必要があり、顧客指定の暗号化キー (CSEK) を使用することを決定しました。
チームはこのタスクをどのように完了する必要がありますか?
A. 暗号化キーを Cloud Storage バケットにアップロードし、オブジェクトを同じバケットにアップロードします。
B. gsutil コマンドライン ツールを使用してオブジェクトを Cloud Storage にアップロードし、暗号化キーの場所を指定します。
C. Google Cloud Platform Console で暗号化キーを生成し、指定されたキーを使用してオブジェクトを Cloud Storage にアップロードします。
D. オブジェクトを暗号化し、gsutil コマンドライン ツールまたは Google Cloud Platform Console を使用してオブジェクトを Cloud Storage にアップロードします。
Answer: D (メーッセージを残す**)**
参照：
https://cloud.google.com/storage/docs/encryption/顧客提供キー

最新問題: **248**
アプリケーションをクラウドに移行しています。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。地域の規制要件により、暗号化に使用する鍵マテリアルを完全に管理する必要があり、鍵マテリアルにアクセスするための正当な理由が必要です。
何をすべきでしょうか?

A. Cloud ハードウェア セキュリティ モジュール (HSM) を基盤とする顧客管理の暗号鍵を使用して、Cloud Storage バケット内のデータを暗号化します。データアクセス ログを有効にします。
B. オンプレミス環境でキーを生成し、オンプレミスで管理されているハードウェア セキュリティ モジュール (HSM) に保存します。このキーを Cloud Key Management Service (KMS) の外部キーとして使用します。Key Access Justifications (KAJ) を有効化し、外部キーシステムを設定して不正アクセスを拒否します。
C. 顧客管理の暗号鍵を使用して、Cloud Storage バケット内のデータを暗号化します。
権限のないグループに対して IAM 拒否ポリシーを設定します。
D. データを Cloud Storage バケットにアップロードする前に、オンプレミス環境でデータを暗号化するための鍵を生成し、Cloud Key Management Service (KMS) にアップロードします。
Key Access Justifications (KAJ) を有効にして、外部キー システムが不正アクセスを拒否するようにします。
Answer: B (メーッセージを残す)

最新問題**: 249**
標準ネットワーク層を使用しながら、デフォルトでクライアント IP を維持するには、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
B. TCP/UDP ネットワーク
C. 内部TCP/UDP
D. SSLプロキシ
Answer: C (メーッセージを残す)

最新問題**: 250**
あなたのチームは、BigQuery内に1PBの機密データを保管しており、その中には個人を特定できる情報 (PII) が含まれています。分析のため、組織内の別のチームにこのデータセットへのアクセスを提供する必要があります。PIIを保護しながら、BigQueryデータセットを他のチームと共有する必要があります。どうすればよいでしょうか？
A. BigQuery の行レベルのアクセス ポリシーを利用して、他のチームのユーザー ID に基づいて PII 列をマスクします。
B. BigQuery データセットを Cloud Storage にエクスポートします。VPC Service Controls 境界を作成し、バケットへのアクセスをチームのプロジェクトのみに許可します。
C. データの仮名化技術を実装して、PII フィールドを識別できない値に置き換えます。
他のチームに仮名化されたデータセットへのアクセス権を付与します。
D. データセットのフィルタリングされたコピーを作成し、機密データを別のプロジェクト内のハッシュ値に置き換えます。他のチームにこの新しいプロジェクトへのアクセス権を付与します。
Answer: (解答を表示する)
https://cloud.google.com/bigquery/docs/行レベルセキュリティ-intro?hl=es-419#地域に基づく行データフィルター

最新問題**: 251**

貴社ではGSuiteを利用しており、Google App Engine上で社内利用向けのアプリケーションを開発しました。従業員のパスワードが漏洩した場合でも、外部ユーザーがアプリケーションにアクセスできないようにする必要があります。
何をすべきでしょうか?
A. すべてのユーザーに対して GSuite の 2 要素認証を強制します。
B. App Engine アプリケーション用に Cloud Identity-Aware Proxy を構成します。
C. GSuite パスワード同期を使用してユーザー パスワードをプロビジョニングします。
D. プライベート ネットワークと GCP の間に Cloud VPN を構成します。
Answer: B (メーッセージを残す)
従業員のパスワードが侵害された場合でも、外部ユーザーが Google App Engine 上の内部アプリケーションにアクセスできないようにするには、Cloud Identity-Aware Proxy（IAP）を構成します。
* IAP を有効にする:
* Cloud Console にアクセスし、App Engine アプリケーションに移動して、「dentity-Aware Proxy」を選択します。
* アプリケーションで IAP を有効にします。
* アクセスポリシーを構成する:
* アクセス ポリシーを設定して、アプリケーションにアクセスできるユーザーを制限します。
* IAM ロールを使用して、特定のユーザーまたはグループにのみアクセスを許可します。
* 認証を強制する:
* IAP は Google 認証を強制し、ユーザーが GSuite の資格情報を使用してログインする必要があるようにします。
* 多要素認証 (MFA) を有効にする:
* すべての GSuite ユーザーに 2FA を適用して、セキュリティをさらに強化します。
利点:
* 資格情報の侵害に対する保護: パスワードが侵害された場合でも、攻撃者は IAP 認証を通過しなければアプリケーションにアクセスできません。
* 集中アクセス管理: IAM および IAP ポリシーを通じてアクセスを簡単に管理および監視できます。
参考文献:
* アイデンティティ認識プロキシの概要
* IAPの設定

最新問題**: 252**
組織内のすべてのログは、分析と長期保存のために、一元化された Google Cloud ロギング プロジェクトに集約されています。4 ログデータの大部分は運用チームが閲覧できますが、特定の機密フィールド（protoPayload.authenticationinfo.principalEmail など）には、セキュリティ チームのみに制限する必要がある識別可能な情報が含まれています。一元化されたロギング プロジェクトで、各チームがそれぞれのアプリケーション ログを閲覧できるソリューションを実装する必要があります。また、これらのログ内の特定の機密フィールドへのアクセスを、指定されたセキュリティ グループのみに制限する必要があります。ソリューショ

ンでは、同じログエントリ内の他のフィールドが、他の承認済みグループに引き続き表示されるようにする必要があります。どうすればよいでしょうか？
A. 機密フィールドと承認されたプリンシパルを指定するデータ アクセス ポリシーを定義して、Cloud Logging でフィールドレベルのアクセスを構成します。
B. logging.privateLogEntries.list に対する特定の権限を持つ Cloud IAM カスタムロールを使用します。カスタムロールの条件内でフィールドレベルのアクセスを定義します。
C. ログが集中ログ プロジェクトに送信される前に、機密フィールドを除外するログ シンクを実装します。機密データ
用に個別のシンクを作成します。
D. エクスポートされたログシンクに BigQuery 承認済みビューを作成し、ユーザー グループに基づいて機密フィールドを除外します。
Answer: (解答を表示する**)**
Google Cloud Logging はフィールドレベルのアクセス制御をサポートしており、ログエントリ内の特定の機密フィールドを特定のユーザーに対して非表示にしながら、ログエントリの残りの部分は引き続き表示できます。5 これは、ログビューと IAM を使用して実現されます。
Google Cloud ドキュメント (フィールドレベルのアクセスの構成) によると、次のようになります。
フィールドレベルのアクセス制御により、LogEntryオブジェクトの特定のフィールドへのアクセスを制限できます。機密性の高いフィールド（例principalEmail）を定義し、特定のユーザーまたはグループにlogging.fieldAccessorロールを付与できます。6 このロールを持たないユーザーにもログエントリは表示されますが、機密性の高いフィールドは編集または非表示になります。主な実装手順：
* フィールドを識別する: JSON ペイロード内のどのパスが機密であるかを判断します。
* アクセスの定義: ログ ビューを使用してログの範囲を定義し、フィールド レベルの制限を適用します。7
* 権限の付与: 一般的なアクセスとログ記録のために標準の logging.viewer ロールを付与します。
特定の機密フィールドのセキュリティ チームにのみ fieldAccessor ロールを付与します。
他のオプションが間違っている理由:
* B は不正解です。IAM 条件は、プラットフォーム レベルでログ エントリ内の特定の JSON フィールドをネイティブに解析および編集することはできません。通常は、リソース レベルのアクセスに使用されます。
* C は誤りです。シンク経由でフィールドを除外することは可能ですが、「すべてかゼロか」です。シンクで除外した場合、誰も（セキュリティチームを含め）宛先でそのデータを見ることができません。
* D は不正解です。これは、チームがログに BigQuery を使用している場合にのみ有効な回避策です。Cloud Logging ログ エクスプローラ自体の問題を解決するものではありません。
参照：
Google Cloud ドキュメント: 「フィールドレベルのアクセスを構成する」
(https://cloud.google.com/logging/docs/access- control#field-level-access)。

最新問題**: 253**
Google Cloud における会社の ID 管理を担当しています。会社では全ユーザーに 2 段階認証プロセス（2SV）を適用しています。ユーザーのアクセスをリセットする必要があるのですが、そのユーザーは 2SV の 2 つ目の要素を失ってしまいました。リスクを最小限に抑えたいと考えています。どうすればよいでしょうか？

A. Google 管理コンソールで適切なユーザー アカウントを選択し、ユーザーがログインできるようにバックアップ コードを生成します。ユーザーに 2 番目の要素を更新するよう依頼します。
B. Google 管理コンソールで、全ユーザーに対して 2 段階認証の要件を一時的に無効にします。ユーザーにログインして、新しい 2 段階認証要素をアカウントに追加するよう依頼します。その後、全ユーザーに対して 2 段階認証の要件を再度有効にします。
C. Google 管理コンソールで適切なユーザーアカウントを選択し、このアカウントの 2 段階認証を一時的に無効にします。ユーザーに 2 段階認証要素の更新を依頼し、その後、このアカウントの 2 段階認証を再度有効にします。
D. Google 管理コンソールで、特権管理者アカウントを使用してユーザーアカウントの認証情報をリセットします。ユーザーに初回ログイン後に認証情報を更新するよう依頼してください。
Answer: A (メッセージを残す**)**
https://support.google.com/a/answer/9176734
アカウント回復にはバックアップコードを使用する
アカウントを復旧する必要がある場合は、バックアップコードをご利用ください。アカウントは引き続き2段階認証によって保護されており、バックアップコードは簡単に生成できます。

最新問題**: 254**
御社のメッセージングアプリをFIPS 140-2に準拠させるため、GCPのコンピューティングおよびネットワークサービスを使用することが決定されました。メッセージングアプリのアーキテクチャには、Compute Engineインスタンスのクラスタを制御するマネージドインスタンスグループ（MIG）が含まれています。インスタンスは、データキャッシュにローカルSSDを使用し、インスタンス間通信にUDPを使用しています。アプリ開発チームは、標準に準拠するために必要な変更をすべて行う用意があります。要件を満たすために、どのようなオプションを推奨しますか？
A. BoringCrypto モジュールを使用して、すべてのキャッシュ ストレージと VM 間通信を暗号化します。
B. MIG で使用されるインスタンス テンプレートのディスク暗号化を顧客管理キーに設定し、インスタンス間のすべてのデータ転送に BoringSSL を使用します。
C. アプリのインスタンス間の通信を UDP から TCP に変更し、クライアントの TLS 接続で BoringSSL を有効にします。
D. MIG で使用されるインスタンス テンプレートのディスク暗号化を Google 管理のキーに設定し、すべてのインスタンス間通信で BoringSSL ライブラリを使用します。
Answer: B (メッセージを残す**)**
メッセージングアプリでFIPS 140-2に準拠するには、保存データと転送データの両方が標準に従って暗号化されていることを確認する必要があります。顧客管理暗号鍵（CMEK）を使用することで、暗号鍵を制御できるようになります。BoringSSLは、転送データの暗号化に関するFIPS 140-2標準に準拠したライブラリです。
手順:
ローカル SSD の暗号化: マネージド インスタンス グループ (MIG) のインスタンスのテンプレートを変更して、ローカル SSD の暗号化に顧客管理の暗号化キー (CMEK) を使用します。
BoringSSL を有効にする: すべてのインスタンス間通信に BoringSSL ライブラリを使用するようにアプリケーションを更新し、転送中のすべてのデータが FIPS 140-2 標準に従って暗号化されるようにします。

参照：
Google Cloud: 顧客管理の暗号鍵（CMEK）
BoringSSL ドキュメント

最新問題**: 255**
あなたはある組織のセキュリティチームのメンバーです。チームには、クレジットカード決済処理システム、ウェブアプリケーション、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、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。
何をすべきでしょうか?
A. Web アプリケーションへの管理者アクセスには多要素認証を使用します。
B. PA-DSS に準拠していることが認定されたアプリケーションのみを使用します。
C. カード所有者データ環境を別の 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: D (メーッセージを残す**)**
参照：
https://cloud.google.com/solutions/pci-dss-compliance-in-gcp

最新問題**: 256**
社内で Cloud Data Loss Prevention (DLP) API の導入が進むにつれ、コスト削減のために利用を最適化する必要があります。DLP 対象データは Cloud Storage と BigQuery に保存されます。場所とリージョンはリソース名のサフィックスとして識別されます。
どのようなコスト削減オプションを推奨すべきでしょうか?
A. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットに適切な bytesLimitPerFile 値を設定します。
B. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットの変換単位を最小限に抑えます。
C. rowsLimit と bytesLimitPerFile を使用してデータをサンプリングし、CloudStorageRegexFileSet を使用してスキャンを制限します。
D. FindingLimits と TimespanContfig を使用してデータをサンプリングし、変換単位を最小限に抑えます。
Answer: C (メーッセージを残す**)**
* 目標: Cloud Data Loss Prevention (DLP) API の使用を最適化してコストを削減します。
* 解決：
* rowsLimit と bytesLimitPerFile: これらのパラメーターは、データセット全体をスキャンするのではなくデータをサンプリングするのに役立ち、処理されるデータの量を削減します。
* CloudStorageRegexFileSet: この機能を使用すると、正規表現を使用してスキャンするファイルのサブセットを指定し、スキャンされるデータの範囲と量を制限できます。
手順:
* ステップ 1: テーブル全体をスキャンするのではなく、行をサンプリングするために、BigQuery データ スキャンに適切な rowsLimit 値を設定します。

* ステップ 2: Cloud Storage バケットの bytesLimitPerFile 値を設定し、ファイルごとにスキャンされるバイト数を制限します。
* ステップ 3: CloudStorageRegexFileSet を使用して、ファイル名に一致するパターンに基づいてスキャンするファイルのサブセットを指定します。
これらの戦略を組み合わせることで、DLP API によって処理されるデータの範囲と量を効果的に削減し、コストを削減できます。
参考文献:
* DLP API のベストプラクティス
* 検索制限の設定

最新問題**: 257**
セキュリティ脆弱性評価を実施した結果、クラウド管理者がGoogle Cloud CLIセッションを数日間開いたままにしていることがわかりました。これらのセッションの継続時間を最小限に設定することで、攻撃者がこれらのセッションを悪用するリスクを軽減する必要があります。
何をすべきでしょうか?
A. Google セッション コントロールのセッション期間を 1 時間に設定します。
B. 再認証頻度 または Google Cloud セッション コントロール）を 1 時間に設定します。
C. 組織ポリシーの制約constraintconstraints/iam.allowServiceAccountCredentialLifetimeExtension を 1 時間に設定します。
D. 組織ポリシー制約のconstraints/iam. serviceAccountKeyExpiryHoursをonehourに設定し、inheritFromParentをfalseに設定します。
Answer: B (メーッセージを残す**)**
Google Cloud CLI セッションの長時間実行によって生じるリスクを軽減するには、再認証頻度を強制することが不可欠です。これにより、ユーザーは定期的に再認証を強いられるため、攻撃者がオープンセッションを悪用する機会が減少します。再認証頻度を 1 時間に設定すると、この期間が経過するとユーザーは再認証を強制され、攻撃者が侵害されたセッションを利用できる期間が制限されます。
* Google Cloud Console にアクセスします。管理者の認証情報を使用して Google Cloud Console にログインします。
* セキュリティ設定に移動します。Cloud Console の 「セキュリティ」セクションに移動します。
* セッション制御の設定 :セッション管理設定の 「再認証頻度」設定で、ユーザーが再認証しなければならない頻度を制御します。

* 再認証頻度の設定：再認証頻度を「1時間」に設定します。この設定により、ユーザーは1時間ごとに再認証を要求され、各セッションの持続時間が制限されます。
* 変更を保存: 変更を確認して保存します。この設定はすべてのユーザーに適用され、開いているセッションの継続時間が1時間に短縮されます。
参考文献:
Google Cloud IAM ドキュメント
Google Cloud セキュリティのベストプラクティス

最新問題**: 258**
組織では、VPC Service Controls の境界内に機密性の高いプロジェクトを構築しました。この境界内のリソースへのアクセスを、会社管理デバイス、特定の場所、有効なユーザー ID など、特定のコンテキスト要件を満たすユーザーのみに限定する必要があります。正当なアクセスをブロックすることなく、この変更の影響を評価したいと考えています。どうすればよいでしょうか？
A. VPC Service Controls 境界をドライランモードで設定し、ファイアウォールルールを使用して厳密なネットワークセグメンテーションを適用します。ユーザー認証には多要素認証 (MFA) を使用します。
B. Cloud Audit Logs を使用して、プロジェクト リソースへのユーザー アクセスを監視します。インシデント後の分析を使用して、不正なアクセス試行を特定します。
C. 必要なコンテキスト属性を指定するコンテキスト認識アクセス ポリシーを確立し、そのポリシーをドライラン モードで VPC Service Controls 境界に関連付けます。
D. VPC サービス コントロール違反ダッシュボードを使用して、サービス境界によるアクセス拒否の詳細の影響を特定します。
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
この質問は、データの流出を防ぐための VPC Service Controls (VPC SC) と、コンテキストに基づいたきめ細かなユーザー アクセスを実現する Context-Aware Access (CAA) という 2 つの強力なセキュリティ機能を組み合わせたものです。
コンテキスト要件: 「企業が管理するデバイス」、「特定の場所」などを要求することは、アクセス レベルを介して実装されるコンテキスト認識アクセス (CAA) の機能です。
VPC SC と CAA の組み合わせ: CAA ポリシーを VPC SC 境界と統合して、境界へのアクセスのコンテキストを適用できます。
影響の評価: アクセスをブロックせずに変更を評価するには、VPC SC 境界全体 (新しい CAA ルールを含む) をドライ ラン モードで構成する必要があります。
抜粋:
「コンテキストアウェア アクセス (CAA) を使用すると、デバイスのセキュリティ ステータス、IP アドレス（場所）、ID などのユーザー属性に基づいて、Google Cloud リソースへのきめ細かなアクセスを定義および適用できます。」（出典 3.1）
新しいセキュリティポリシーを実装する際は、VPC Service Controls の境界（関連するアクセスレベル/コンテキストアウェアアクセスを含む）を最初にドライランモードで構成することがベストプラクティスです。ドラ

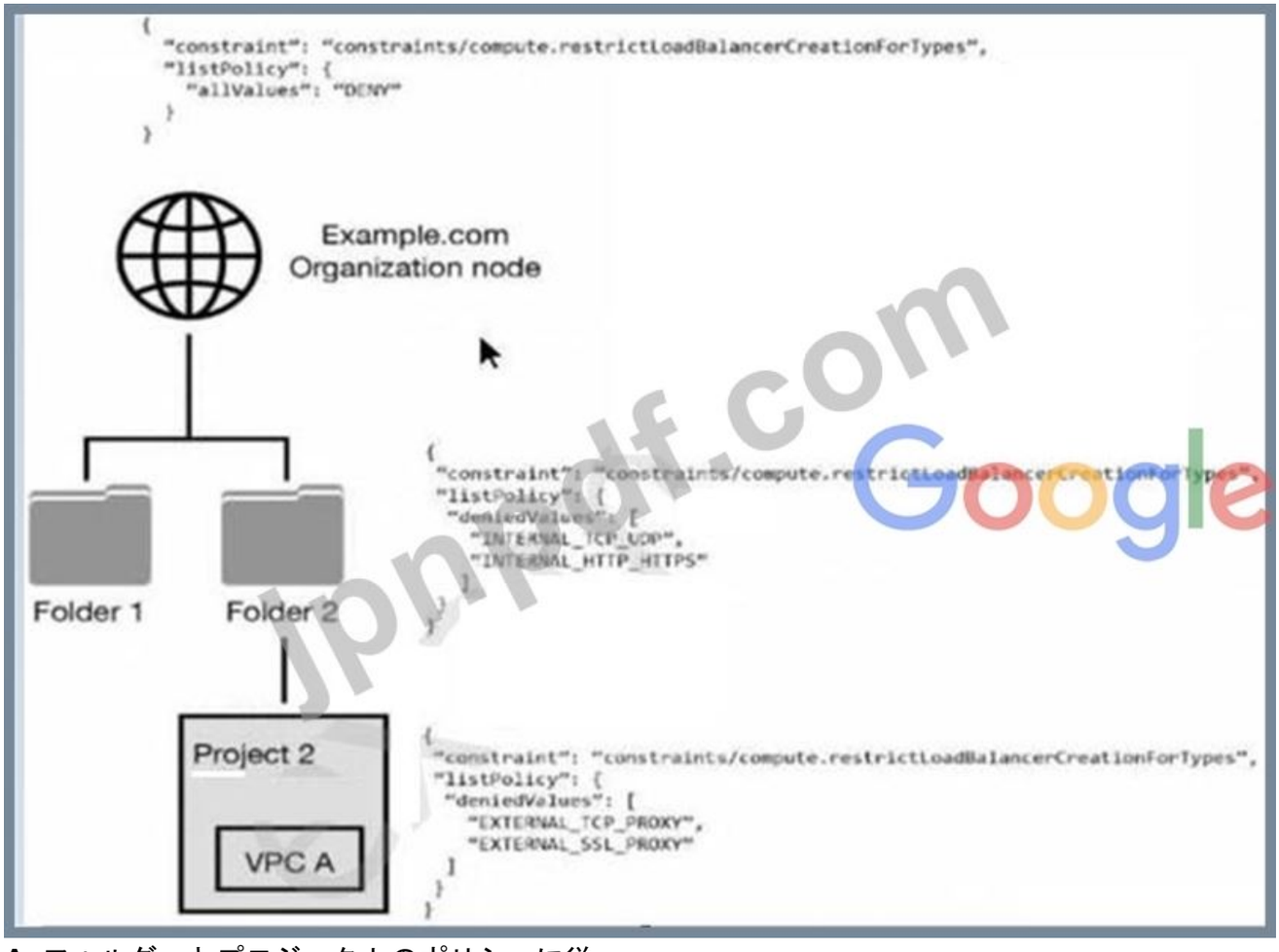
イランモードを使用すると、アクセスをブロックすることなく、境界がサービスに与える影響をテストできます。（出典3.2）
「アクセス レベル（CAA の中核コンポーネント）を使用して、サービス境界によって保護されているリソースにアクセスするための条件を定義できます。」（出典3.3）

最新問題: **259**
あなたは会社のセキュリティチームのメンバーです。Linux Bastion ホストの外部攻撃対象領域を縮小するため、パブリック IP アドレスをすべて削除するよう指示を受けました。サイト信頼性エンジニア (SRE) は、オフサイトから社内 VPC にアクセスできるように、パブリックの場所から Bastion ホストにアクセスする必要があります。このアクセスを有効にするにはどうすればよいでしょうか？
A. 要塞ホストが存在するリージョンに Cloud VPN を実装します。
B. 要塞ホストに 2 段階認証による OS ログインを実装します。
C. 要塞ホストに対して Identity-Aware Proxy TCP 転送を実装します。
D. 要塞ホストの前に Google Cloud Armor を実装します。
Answer: C (メーッセージを残す**)**
参照：
https://cloud.google.com/architecture/building-internet-connectivity-for-private-vms#configuring_iap_tunnels_for_interacting_with_instances

最新問題: **260**
あなたの会社は2段階認証（2SV）を導入したいと考えています。会社の組織単位（OU）は、人事、財務、エンジニアリング、マーケティングの4つの部門に分かれています。
複数のアクセス問題が同時に発生するのを防ぐ必要があります。ソリューションでは、管理と設定の複雑さを最小限に抑える必要があります。どうすればよいでしょうか？
A. 特定のユーザーに対して 2SV の適用を設定し、他のユーザーに対しては適用しないようにする新しい OU を 1 つ作成します。
B. 構成グループを作成し、段階的な移行を有効にして、2SV を適用するユーザーの数を制御します。
C. 管理コンソールで、各 OU に対して、ユーザーが 2 段階認証プロセスを有効にできるようにするチェックボックスをオンにし、適用をオフに設定します。
D. 管理コンソールで、各組織部門の「ユーザーが2段階認証プロセスを有効にできるようにする」チェックボックスをオフにし、「適用」を「オン」に設定します。
Answer: (解答を表示する**)**
正確な抜粋からの包括的かつ詳細な説明：
目標は、段階的に展開して 2SV を展開し、一度に影響を受けるユーザーの数を制御し、混乱を最小限に抑え、管理をシンプルに保つことです。
OU 構造を使用することもできますが、Google 管理コンソールで 2SV などのセキュリティ設定を段階的に展開するには、設定グループに基づいてポリシー例外を管理することが推奨され、複雑さも軽減されます。
抜粋:

2SV を導入する際は、ユーザーアクセスとサポートリソースへの影響を管理するために、段階的な導入アプローチを採用することを強くお勧めします。」（出典2.1）
設定グループを使用すると、OU構造内のユーザーのサブセットを選択し、2SV適用などの特定の設定を適用できます。これにより、主要な組織単位構造を変更することなく、段階的かつ制御された展開が可能になります。（出典2.2）グループを使用すると、OU階層内でユーザーのIDを移動することなく、適用範囲にユーザーを簡単に追加/削除できるため（オプションA）、管理の複雑さを軽減できます。オプションCとDでは、段階的な適用制御は実現できません。

最新問題: **261**
次のようなリソース階層があります。階層内の各ノードには、図に示すように組織ポリシーが適用されます。VPC A ではどのタイプのロードバランサーが拒否されていますか？



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. INTERNAL_TCP_UDP、INTERNAL_HTTP_HTTPS はフォルダーのポリシーに従って拒否されます。
C. 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。
D. EXTERNAL_TCP_PROXY、EXTERNAL_SSL_PROXY はプロジェクトのポリシーに従って拒否されます。
Answer: A (メーッセージを残す**)**

最新問題**: 262**
組織内で多数の仮想マシン (VM) を管理しています。多くのVMでパッチ適用が不十分な問題が発生しています。VMへの定期的なパッチ適用を自動化し、複数のプロジェクトにまたがるパッチ管理データを把握する必要があります。
何をすべきでしょうか?
2つの回答を選択してください
A. OSパッチ管理を使用してVMマネージャーでパッチを展開する
B. OS パッチ管理を使用して、VM マネージャーでパッチ管理データを表示します。
C. Rapid Vulnerability Detection を使用して、Security Command Center でパッチを展開します。
D. Security Command Center ダッシュボードでパッチ管理データを表示します。
E. Artifact Registry でパッチ管理データを表示します。
Answer: A,B (メーッセージを残す**)**
https://cloud.google.com/compute/docs/os-patch-management

最新問題**: 263**
あなたの組織では、BigQuery と Cloud Storage に保存されたライブユーザーアクティビティデータを処理する ML モデルを使用して、リアルタイムのレコメンデーションエンジンを構築しています。開発された新しいモデルはすべて Artifact Registry に保存されます。
この新しいシステムは、モデルをGoogle Kubernetes Engineにデプロイし、メッセージキューにはPub/Subを使用します。最近の業界ニュースでは、機械学習モデルのサプライチェーンを悪用した攻撃が報告されています。このサーバーレスアーキテクチャでは、特に開発およびデプロイメントパイプラインへのリスクに対して、セキュリティを強化する必要があります。
何をすべきでしょうか?
A. ML モデルに使用される外部ライブラリと依存関係を可能な限り制限します。
BigQuery および Cloud Storage からユーザーデータにアクセスするために使用される暗号化キーを継続的にローテーションします。
B. 開発中およびデプロイ前のコンテナイメージの脆弱性スキャンを有効にします。Artifact Registry から継続的インテグレーションおよび継続的デプロイ (CI/CD) パイプラインにデプロイされたイメージに Binary Authorization を適用します。
C. モデル開発の前にすべてのトレーニング データを徹底的にサニタイズして、ポイズニング攻撃のリスクを軽減します。
承認には IAM を使用し、コード リポジトリとクラウド サービスにロールベースの制限を適用します。
D. Cloud Run インスタンスへの外部トラフィックを制限するための厳格なファイアウォール ルールを作成します。侵入検知システム (IDS) を統合して、Pub/Sub メッセージフローにおけるリアルタイムの異常検知を実現します。
Answer: (解答を表示する**)**
サーバーレス アーキテクチャ内で機械学習 (ML) モデルのサプライ チェーンのセキュリティを強化するには、開発パイプラインとデプロイメント パイプラインの両方を保護する対策を実装することが重要です。

* オプション A: 外部依存関係を制限し、暗号化キーをローテーションすることはセキュリティ上は良い方法ですが、ML モデルのサプライ チェーンに関連するリスクに直接対処するものではありません。
* オプションB：開発中およびデプロイ前の段階でコンテナイメージの脆弱性スキャンを実施することで、コンテナイメージ内の既知の脆弱性を特定し、軽減することができます。Binary Authorizationを適用することで、信頼され検証済みのイメージのみが環境にデプロイされることが保証されます。
この組み合わせにより、展開前にコンテナ イメージの整合性を検証することで、ML モデル サプライ チェーンのセキュリティが直接強化されます。
* オプション C: トレーニング データをサニタイズし、ロールベースのアクセス制御を適用することは重要なセキュリティ プラクティスですが、侵害されたコンテナ イメージに対してデプロイメント パイプラインを具体的に保護するものではありません。
* オプション D: 厳格なファイアウォール ルールと侵入検知システムはネットワーク セキュリティを強化しますが、コンテナ イメージまたは展開プロセス内の脆弱性には具体的に対処しません。
したがって、オプション B は、検証済みの安全なコンテナ イメージのみが環境内で使用されるようにすることで、開発およびデプロイメント パイプラインのセキュリティに直接対処するため、最も効果的なアプローチです。
参考文献:
コンテナスキャンの概要
バイナリ認証の概要

最新問題**: 264**
ブートディスクのソースとして使用できるイメージを制限したい場合、これらのイメージは専用のプロジェクトに保存されます。
何をすべきでしょうか?
A. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。許可操作で、信頼されたプロジェクトをホワイトリストとしてリストします。
B. 組織ポリシーサービスを使用して、組織レベルで compute.trustedimageProjects 制約を作成します。信頼済みプロジェクトを拒否操作の例外としてリストします。
C. リソースマネージャーで、信頼されたプロジェクトのプロジェクト権限を編集します。組織を 「コンピューティングイメージユーザー」ロールのメンバーとして追加します。
D. リソースマネージャーで組織の権限を編集します。プロジェクトIDをロールを持つメンバーとして追加します。
コンピューティングイメージユーザー。
Answer: (解答を表示する**)**
* 目的: ブート ディスクのソースとして使用できるイメージを、専用のプロジェクトに保存されているイメージのセットに制限します。
* 解決策: 組織ポリシー サービスを使用します。
* 手順:
* ステップ 1: Google Cloud Console を開きます。
* ステップ 2: 組織ポリシー ページに移動します。

* ステップ 3: 「ポリシーの作成」をクリックして新しいポリシーを作成します。
* ステップ 4: 制約 compute.trustedimageProjects を選択します。
* ステップ 5: ポリシーを ALLOW に設定し、信頼できるイメージがホワイトリストに保存されているプロジェクト ID を指定します。
* ステップ 6: ポリシーを保存して適用します。
組織レベルで compute.trustedimageProjects 制約を作成し、許可リストに信頼できるプロジェクトを指定することにより、このプロジェクトのイメージのみが組織全体のブートディスクに使用されるようになります。
参考文献:
GCP 組織ポリシー サービス ドキュメント
信頼できるイメージプロジェクトの制約を計算する

最新問題**: 265**
Compute Engine でホストされる CI/CD クラスタを使用してクラウド インフラストラクチャをデプロイする予定です。認証情報が第三者に盗まれるリスクを最小限に抑えたいと考えています。どうすればよいでしょうか？
A. クラスタ専用の Cloud Identity ユーザーアカウントを作成します。強力なセルフホスト型ボールトソリューションを使用して、ユーザーの一時的な認証情報を保存します。
B. クラスタ専用の Cloud Identity ユーザーアカウントを作成します。プロジェクトレベルで、constraints/iam.disableServiceAccountCreation 組織ポリシーを有効にします。
C. クラスターのカスタム サービス アカウントを作成し、プロジェクト レベルで constraints/iam.disableServiceAccountKeyCreation 組織ポリシーを有効にします。
D. クラスターのカスタム サービス アカウントを作成し、プロジェクト レベルで constraints/iam.allowServiceAccountCredentialLifetimeExtension 組織ポリシーを有効にします。
Answer: (解答を表示する**)**
サービスアカウントキーの作成を無効化します。iam.disableServiceAccountKeyCreationブール制約を使用すると、新しい外部サービスアカウントキーの作成を無効化できます。これにより、サービスアカウントの管理対象外の長期認証情報の使用を制御できます。この制約が設定されている場合、制約の影響を受けるプロジェクト内のサービスアカウントに対して、ユーザーが管理する認証情報を作成できなくなります。https://cloud.google.com/resource-manager/docs/organization-policy/restricting-service-accounts#example_policy_boolean_constraint

最新問題**: 266**
Google Cloud 組織内に数百のエフェメラル プロジェクトをデプロイし、ユーザーが Google Cloud を利用できるようにするための新しいインフラストラクチャ CI/CD パイプラインを作成しています。Google が推奨するベスト プラクティスに従いながら、組織内のデフォルト ネットワークの使用を制限したいと考えています。どうすればよいでしょうか？
A. 組織レベルで、constraints/compute.skipDefaultNetworkCreation 組織ポリシー制約を有効にします。
B. 各プロジェクトのすべてのデフォルト ネットワークを自動的に削除する毎日の Cloud Functions をトリガーする cron ジョブを作成します。

C. 組織レベルでユーザーに 1AM オーナーロールを付与します。プロジェクトの周囲に VPC Service Controls 境界を作成し、compute.googleapis.com API へのアクセスを制限します。
D. ユーザーが、デフォルト ネットワークの作成をスキップするためにデプロイできる定義済みのインフラストラクチャ テンプレート セットのみを使用して CI/CD パイプラインを使用できるようにします。
Answer: A (メーッセージを残す**)**
* 組織ポリシー: 新しいプロジェクトでのデフォルト ネットワークの作成を無効にするには、constraints/compute.skipDefaultNetworkCreation 組織ポリシー制約を使用します。
* ポリシーの適用: この制約を組織レベルで適用して、組織内のすべてのプロジェクトに影響し、デフォルトネットワークの作成を防止します。
* ベスト プラクティスのコンプライアンス: このベスト プラクティスに従うことで、適切にセグメント化または保護されていない可能性のあるデフォルト ネットワークの使用を回避することができ、クリーンかつ安全なネットワーク構成を維持できます。
* 検証: 新しいプロジェクトを作成し、デフォルトネットワークが作成されていないことを確認して、ポリシーの適用を確認します。参考資料:
* Google Cloud - 組織ポリシーの制約
* Google Cloud - エンタープライズ組織向けのベストプラクティス

最新問題**: 267**
会社では、Google Cloud リソースへのアクセスを提供するために、Cloud Identity でユーザーを手動で作成してきました。環境の継続的な成長に伴い、Google Cloud Directory Sync（GCDS）インスタンスを承認し、オンプレミスの LDAP サーバーと統合して、数百人のユーザーをオンボーディングしたいと考えています。
以下のことが求められます:
オンプレミスの LDAP サーバーからユーザーとグループのライフサイクルの変更を Cloud Identity に複製します。
Cloud Identity で手動で作成されたユーザーを無効にします。
Google Cloud のスコープにユーザーとセキュリティ グループを含めるように、LDAP 検索属性をすでに設定しました。このソリューションを完了するには、次に何をすればよいですか？
A. 1. LDAP に見つからないドメイン ユーザーを停止するオプションを設定します。2. 定期的な GCDS タスクを設定します。
B. 1. LDAP に見つからないドメイン ユーザーを削除するオプションを設定します。2. ユーザーとグループのライフサイクルが変更された後に GCDS を実行します。
C. 1. LDAP 検索属性を設定して、LDAP に見つからない手動で作成された Cloud Identity ユーザーを除外します。2. 定期的な GCDS タスクを設定します。
D. 1. LDAP 検索属性を設定して、LDAP に見つからない手動で作成された Cloud Identity ユーザーを除外します。2. ユーザーとグループのライフサイクルが変更された後、GCDS を実行します。
Answer: A (メーッセージを残す**)**

最新問題**: 268**

アプリケーションとリソースにアクセス制御ポリシーを適用するには、どの Google Cloud サービスを使用する必要がありますか?
A. アイデンティティ認識プロキシ
B. クラウドNAT
C. Google クラウドアーマー
D. シールドされたVM
Answer: (解答を表示する**)**
Google Cloud 内のアプリケーションとリソースにアクセス制御ポリシーを適用するには、Identity-Aware Proxy (IAP) というサービスが推奨されます。
* アイデンティティ認識プロキシ (IAP):
* IAP を使用すると、ユーザーの ID とリクエストのコンテキストに基づいて、アプリケーションとリソースへのアクセスを制御できます。IAM と統合することできめ細かなアクセス制御が可能になり、承認されたユーザーのみが特定のリソースにアクセスできるようになります。
IAP は、アプリケーション層でセキュリティ ポリシーを適用し、従来のネットワークベースのセキュリティ対策を超えた追加の保護層を提供します。
参考文献
* アイデンティティ認識プロキシのドキュメント

最新問題**: 269**
組織ではGoogle Cloudを導入しており、機密性の高いリソースへのアクセスを社内オンプレミスネットワーク内のデバイスからのみに制限したいと考えています。この要件を適用するには、Access Context Managerを設定する必要があります。以下の点にご注意ください。
- 内部ネットワークは、IP 範囲 10.100.0.0/16 および 192.168.0.0/16 を使用します。
- 一部の従業員はリモートワークをしていますが、会社を通じて安全に接続しています-
マネージド仮想プライベートネットワーク (VPN)。VPNはIPアドレスプール172.16.0.0/20から動的にIPアドレスを割り当てます。
- アクセスは特定のGoogle Cloudプロジェクトに制限する必要があります
既存のサービス境界内に含まれます。
何をすべきでしょうか?
A. 「承認済みデバイス」というアクセスレベルを作成します。デバイスポリシー属性を使用して、企業管理デバイスの使用を必須にします。このアクセスレベルをGoogle Cloudプロジェクトに適用し、全従業員に組織の管理システムにデバイスを登録するよう指示します。
B. 「内部ネットワークのみ」というアクセスレベルを作成します。次の属性を持つ条件を追加します。
- IP サブネットワーク: 10.100.0.0/16、192.168.0.0/16
- デバイスポリシー :OS を Windows または macOS に設定する必要があります。このアクセスレベルを、機密性の高い Google Cloud プロジェクトに適用します。
C. 「Corporate Access」というアクセスレベルを作成します。IPサブネットワーク属性を含む条件を追加し、範囲を10.100.0.0/16、192.168.0.0/16、172.16.0.0/20とします。このアクセスレベルを、機密性の高いプロジェクトを含むサービス境界に割り当てます。

D. 「nternalAccess」という新しい IAM ロールを作成します。IP 範囲 10.100.0.0/16、192.16.0.0/16、172.16.0.0/20 を IAM 条件としてロールに追加します。このロールを、オンプレミス ユーザーと VPN ユーザーに対応する IAM グループに割り当てます。このロールに、この機密性の高い Google Cloud プロジェクト内のリソースに対する必要な権限を付与します。
Answer: (解答を表示する**)**
https://cloud.google.com/access-context-manager/docs/overview#ip-address

最新問題**: 270**
社内のユーザーはBigQueryテーブルのデータにアクセスします。ユーザーがデータにアクセスできるのは勤務時間中のみにすることを希望しています。
何をすべきでしょうか?
A. 指定された勤務時間にアクセスを制限する IAM 条件とともに、BigQuery データ閲覧者ロールを割り当てます。
B. BigQuery データ閲覧者のロールを割り当てる gsutil スクリプトを実行し、指定された営業時間内にのみそのロールを削除します。
C. 指定された営業時間中に毎日ユーザーを追加および削除するサービス アカウントに BigQuery データ閲覧者のロールを割り当てます。
D. 指定された勤務時間中に BigQuery の組織ポリシー制約を変更する Cloud Functions インスタンスをトリガーするように Cloud Scheduler を構成します。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/iam/docs/conditions-overview

最新問題**: 271**
Google Cloud 組織内に数百のエフェメラル プロジェクトをデプロイし、ユーザーが Google Cloud を利用できるようにするための新しいインフラストラクチャ CI/CD パイプラインを作成しています。Google が推奨するベスト プラクティスに従いながら、組織内のデフォルト ネットワークの使用を制限したいと考えています。どうすればよいでしょうか？
A. 組織レベルで、constraints/compute.skipDefaultNetworkCreation 組織ポリシー制約を有効にします。
B. 各プロジェクトのすべてのデフォルト ネットワークを自動的に削除する毎日の Cloud Functions をトリガーする cron ジョブを作成します。
C. 組織レベルでユーザーに 1AM オーナーロールを付与します。プロジェクトの周囲に VPC Service Controls 境界を作成し、compute.googleapis.com API へのアクセスを制限します。
D. ユーザーが、デフォルト ネットワークの作成をスキップするためにデプロイできる定義済みのインフラストラクチャ テンプレート セットのみを使用して CI/CD パイプラインを使用できるようにします。
Answer: A (メーッセージを残す**)**
組織ポリシー: 新しいプロジェクトでのデフォルト ネットワークの作成を無効にするには、constraints/compute.skipDefaultNetworkCreation 組織ポリシー制約を使用します。
ポリシーの適用: この制約を組織レベルで適用して、組織内のすべてのプロジェクトに影響し、デフォルト ネットワークの作成を防止します。

ベスト プラクティスのコンプライアンス: このベスト プラクティスに従うことで、適切にセグメント化または保護されていない可能性のあるデフォルトのネットワークの使用を回避することができ、クリーンかつ安全なネットワーク構成を維持できます。
検証: 新しいプロジェクトを作成し、デフォルトネットワークが作成されていないことを確認して、ポリシーの適用を確認します。参考:
Google Cloud - 組織ポリシーの制約
Google Cloud - エンタープライズ組織向けのベストプラクティス

最新問題**: 272**
チームは、Compute Engine インスタンスがインターネットや Google API またはサービスにアクセスできないようにする必要があります。
これらの要件を満たすには、どの 2 つの設定を無効のままにしておく必要がありますか? (2 つ選択してください。)
A. パブリックIP
B. IP転送
C. プライベート Google アクセス
D. 静的ルート
E. IAM ネットワーク ユーザー ロール
Answer: (解答を表示する**)**
オプション A: GCP ドキュメントによると、「インスタンスをプライベート IP アドレスのみで設定して、インターネット アクセスを防止する」ため、パブリック IP は使用されません。
オプションC：内部IPアドレスのみを持つ（外部IPアドレスを持たない）VMインスタンスは、プライベートGoogleアクセスを使用できるためです。これらのVMインスタンスは、Google APIおよびサービスの外部IPアドレスにアクセスできます。
https://cloud.google.com/vpc/docs/configure-private-google-access

最新問題**: 273**
あなたの会社は、顧客の年齢層に応じて信用スコアの向上を支援するために、どのような製品を開発できるかを検討したいと考えています。これを実現するには、会社の銀行アプリのユーザー情報と、サードパーティから取得した顧客の信用スコアデータを結合する必要があります。この生データを使用することでこのタスクを完了できますが、機密データが露出し、新しいシステムに伝播される可能性があります。

このリスクに対処するには、データベース全体の参照整合性を維持しながら、Cloud Data Loss Prevention による匿名化とトークン化を行う必要があります。これらの要件を満たすには、どの暗号トークン形式を使用すべきでしょうか？
A. 決定論的暗号化
B. 安全なキーベースのハッシュ
C. フォーマット保持暗号化
D. 暗号ハッシュ
Answer: (解答を表示する**)**
説明
この暗号化方法は可逆的であるため、データベース全体の参照整合性を維持するのに役立ち、文字セットの制限もありません。https://cloud.google.com/blog/products/identity-security/take-charge-of-your-data-how-tokenization
https://cloud.google.com/dlp/docs/仮名化
FPE は、AES-SIV などの他の確定的暗号化方式と比較して、セキュリティ保証が劣ります。そのため、Google は、セキュリティが重視されるすべてのユースケースにおいて、FPE ではなく AES-SIV による確定的暗号化を使用することを強く推奨します。AES-SIV を使用した確定的暗号化などの他の方式は、より強力なセキュリティ保証を提供するため、長さと文字セットの保持が厳格な要件である場合を除き たとえば、従来のデータシステムとの下位互換性が必要な場合など）、トークン化のユースケースでは推奨されます。

最新問題**: 274**
HTTPS リソースにアクセスするために、Identity and Access Management (IAM) ユーザーに付与する必要がある Identity-Aware Proxy ロールはどれですか?
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: (解答を表示する**)**
https://cloud.google.com/iap/docs/アクセス管理
「IAP で保護された Web アプリ ユーザー: IAP を使用するアプリおよびその他の HTTPS リソースへのアクセスを許可します。」

最新問題**: 275**
お客様は、Google Cloud Platform （GCP）でホストされているCRMウェブインターフェースに、モバイルワーカーが簡単にアクセスできるようにしたいと考えています。CRMには、企業ネットワーク上のユーザーのみがアクセスできます。お客様は、CRMをインターネット経由で利用できるようにしたいと考えています。あなたのチームでは、アプリケーションの前に2要素認証をサポートする認証レイヤーが必要です。これらの要件を満たすために、お客様はどのGCPプロダクトを導入すべきでしょうか？
A. クラウド ID 認識プロキシ
B. クラウドアーマー
C. クラウドエンドポイント

D. クラウドVPN
Answer: A (メーッセージを残す)
説明
Cloud IAP は、多要素認証を有効にできる Google サインインと統合されています。
https://cloud.google.com/iap/docs/concepts-overview

最新問題**: 276**
あなたは会社のセキュリティ管理者です。開発チームは、「implementation」フォルダ内に、開発、ステージング、本番環境のワークロードごとに複数のGCPプロジェクトを作成しています。セキュリティ境界を設定することで、悪意のある内部関係者や侵害されたコードによるデータの流出を防ぎたいと考えています。しかし、プロジェクト間の通信は制限したくありません。
何をすべきでしょうか?
A. 共有 VPC を使用してすべてのプロジェクト間の通信を可能にし、ファイアウォール ルールを使用してデータの流出を防ぎます。
B. データの流出を防ぐために Access Context Manager でアクセス レベルを作成し、プロジェクト間の通信に共有 VPC を使用します。
C. Infrastructure as Code ソフトウェアツールを使用して単一のサービス境界を設定し、Stackdriver と Cloud Pub/Sub を介して「implementation」フォルダを監視する Cloud Functions をデプロイします。この関数は、フォルダに新しいプロジェクトが追加されたことを認識すると、Terraform を実行して、関連する境界に新しいプロジェクトを追加します。
D. Infrastructure as Code ソフトウェアツールを使用して、開発、ステージング、本番の 3 つの異なるサービス境界を設定し、Stackdriver と Cloud Pub/Sub を介して「implementation」フォルダを監視する Cloud Functions をデプロイします。この関数は、フォルダに新しいプロジェクトが追加されたことを認識すると、Terraform を実行して、新しいプロジェクトをそれぞれの境界に追加します。
Answer: D (メーッセージを残す)
開発環境、ステージング環境、本番環境それぞれに個別のサービス境界を設定することで、よりきめ細かな制御と監視が可能になります。それぞれの境界への新規プロジェクトの追加を自動化することで、手動による介入なしに、すべてのプロジェクトを一貫して保護できます。
手順:
* サービス境界の設定: Access Context Manager を使用して、開発、ステージング、本番環境の 3 つの個別のサービス境界を定義および構成します。
* モニタリング関数のデプロイ: Stackdriver (Cloud Monitoring) と Cloud Pub/Sub を使用して、新しいプロジェクトの「implementation」フォルダをモニタリングする Cloud Function を作成します。
* 境界更新の自動化: 適切なサービス境界に新しいプロジェクトを自動的に追加する Terraform スクリプトを実行するように Cloud Functions を構成します。
参考文献:
* Google Cloud: アクセスコンテキストマネージャー
* サービス境界の自動化

最新問題: **277**
あなたの組織では、社内従業員との自動会話を実現する生成AIを搭載したチャットボットを構築しています。このチャットボットを通じて個人を特定できる情報（PII）を含むデータが送信されないようにする必要があります。どうすればよいでしょうか？
A. Cloud KMS を使用して、入力と出力の両方で保存データを暗号化し、暗号化キーに最小権限アクセスを適用します。
B. Cloud Data Loss Prevention (Cloud DLP) API を使用して、入力と出力の両方で PII データを検出し、変換します。
C. VPC-SC を使用してチャットボットの周囲に安全なスコープを作成し、PII データの流出を防止します。
D. Google Cloud Marketplace のデータ暗号化ツールを使用して、入力と出力の両方をスキャンします。
Answer: (解答を表示する**)**
https://cloud.google.com/blog/topics/developers-practitioners/how-keep-sensitive-data-out-your- チャットボット

最新問題: **278**
大手eコマース企業が、自社の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決済を行う際に、顧客のブラウザとGCPの間で決済情報が暗号化されることを保証したいと考えています。
彼らは何をすべきでしょうか?
A. 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。
B. ポート 443 の送信トラフィックを許可し、その他のすべての送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。
C. ポート 443 の受信トラフィックを許可し、その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. 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。
Answer: D (メッセージを残す**)**

最新問題: **279**
Cloud Identity に新規ユーザーをオンボーディングしている際に、一部のユーザーが企業ドメイン名を使用して一般ユーザーアカウントを作成していることがわかりました。これらの一般ユーザーアカウントを Cloud Identity でどのように管理すればよいでしょうか？
A. Google Cloud Directory Sync を使用して、管理対象外のユーザー アカウントを変換します。
B. 各コンシューマー ユーザー アカウントに対して新しい管理対象ユーザー アカウントを作成します。
C. 管理されていないユーザー アカウントには転送ツールを使用します。
D. 顧客のサードパーティ プロバイダーを使用してシングルサインオンを構成します。
Answer: C (メッセージを残す**)**
https://support.google.com/a/answer/6178640?hl=ja
転送ツールを使用すると、管理されていないユーザーが存在するかどうかを確認し、それらの管理されていないユーザーをドメインに招待できます。

最新問題: **280**
既存の VPC Service Controls 境界を新しいアクセスレベルに更新したいと考えています。この変更によって既存の境界が損なわれるのを防ぎ、ユーザーへの影響を最小限に抑えながらオーバーヘッドを最小限に抑える必要があります。どうすればよいでしょうか？
A. 既存の境界の完全なレプリカを作成します。レプリカに新しいアクセスレベルを追加します。アクセスレベルの検証が完了したら、元の境界を更新します。
B. 境界を、常に一致することのない新しいアクセスレベルに更新します。過度に許可されすぎないように、新しいアクセスレベルを、望ましい状態に一致するように一度に1つの条件ごとに更新します。
C. 境界でドライランモードを有効にします。新しいアクセスレベルを境界設定に追加します。
アクセス レベルが検証されたら、境界構成を更新します。
D. 境界でドライランモードを有効にします。新しいアクセスレベルを境界のドライラン設定に追加します。アクセスレベルの検証が完了したら、境界設定を更新します。
Answer: (解答を表示する**)**
ドライランモードを有効にする :まず、VPC Service Controls 境界でドライランモードを有効にします。このモードでは、変更を実際に適用することなくテストできるため、現在の設定に支障が生じることはありません。
アクセスレベルの追加：新しいアクセスレベルをドライラン設定に追加します。これにより、新しいアクセスレベルがどのように動作し、既存の設定とどのように連携するかを、実際の影響を与えることなく監視できます。
審査プロセス :ログを分析し、ドライランモードでの動作を監視することで、新しいアクセスレベルを慎重に審査します。新しい構成がセキュリティと運用の要件を満たしていることを確認します。
境界の更新：新しいアクセスレベルが既存のサービスに支障をきたさず、すべての要件を満たしていることが確認できたら、実際の境界構成を新しいアクセスレベルに更新します。このアプローチにより、変更内容が反映される前にテストできるため、リスクを最小限に抑え、中断を最小限に抑えながらシームレスな更新を実現できます。参考資料：
Google Cloud - VPC サービス コントロールの構成
Google Cloud - ドライランモードの使用

最新問題: **281**
ある組織は最近、顧客向けの新しいウェブアプリケーションの構築とホスティングにApp Engineを使い始めました。この組織は、既存のIAM設定を利用して、開発部門の従業員にリモートからアプリケーションへの昇格アクセスを許可したいと考えています。これにより、開発者はHTTPS接続を介してアプリケーションにアップデートや修正をプッシュできるようになります。開発者以外の従業員は、開発権限なしで本番環境バージョンのみにアクセスできるようにする必要があります。これらの要件を満たすには、どのGoogle Cloud Platformソリューションを使用すべきでしょうか？
A. Cloud Identity を使用して組織の Active Directory を同期し、従業員が Cloud VPN 経由でアクセスできるようにします。
B. アプリケーション アクセス制御リスト (ACL) から開発者以外の従業員の Google グループを削除して、開発者以外の従業員のアクセスを無効にします。

C. 従業員のアクセスの認証とさまざまな承認レベルを管理するために、Cloud Identity-Aware Proxy (Cloud IAP) を設定します。
D. 従業員のアクセスの認証とさまざまな承認レベルを管理するための仮想プライベート クラウド (VPC) ファイアウォール ルールを設定します。
Answer: (解答を表示する**)**
A は不正解です。ユーザーを Google Identity に同期しても、App Engine アプリケーションへの差別化されたアクセス権は付与されません。
B は不正解です。App Engine IAM ロールは、プロジェクト内の App Engine アプリケーションに対する異なるレベルの管理アクセスのみを指定します。
C は正解です。Cloud IAP を使用すると、組織は App Engine アプリのユーザー基準に基づいてさまざまなレベルのアクセスを確立できます。
D は不正解です。VPC ファイアウォール ルールでは、異なるレベルの承認は付与されず、トラフィックの許可/ブロックのみが行われるためです。
https://cloud.google.com/appengine/docs/standard/python/アクセス制御
https://cloud.google.com/iap/docs/concepts-overview

最新問題**: 282**
社内で Cloud Data Loss Prevention (DLP) API の導入が進むにつれ、コスト削減のために利用を最適化する必要があります。DLP 対象データは Cloud Storage と BigQuery に保存されます。場所とリージョンはリソース名のサフィックスとして識別されます。
どのようなコスト削減オプションを推奨すべきでしょうか?
A. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットに適切な bytesLimitPerFile 値を設定します。
B. 米国外でホストされている BigQuery データに適切な rowsLimit 値を設定し、マルチリージョンの Cloud Storage バケットの変換単位を最小限に抑えます。
C. rowsLimit と bytesLimitPerFile を使用してデータをサンプリングし、CloudStorageRegexFileSet を使用してスキャンを制限します。
D. FindingLimits と TimespanContfig を使用してデータをサンプリングし、変換単位を最小限に抑えます。
Answer: (解答を表示する**)**
説明
https://cloud.google.com/dlp/docs/inspecting-storage#sampling
https://cloud.google.com/dlp/docs/best-practices-costs#limit_scans_of_files_in_to_only_relevant_files

最新問題**: 283**
これまで、Google Cloud リソースへのアクセスを提供するために、Cloud Identity でユーザーを手動で作成してきました。環境の継続的な成長に伴い、Google Cloud Directory Sync（GCDS）インスタンスを承認し、オンプレミスの LDAP サーバーと統合して、数百人のユーザーをオンボーディングしたいと考えています。そのためには、以下の作業が必要です。
オンプレミスの LDAP サーバーからユーザーとグループのライフサイクルの変更を Cloud Identity に複製します。

Cloud Identity で手動で作成されたユーザーを無効にします。
Google Cloud のスコープにユーザーとセキュリティ グループを含めるように、LDAP 検索属性をすでに設定しました。このソリューションを完了するには、次に何をすればよいですか？
A. 1. LDAP に見つからないドメイン ユーザーを停止するオプションを設定します。
2. 定期的な GCDS タスクを設定します。
B. 1. LDAP に見つからないドメイン ユーザーを削除するオプションを設定します。
2. ユーザーとグループのライフサイクルが変更された後、GCDS を実行します。
C. 1. LDAP 検索属性を構成して、LDAP に見つからない手動で作成された Cloud Identity ユーザーを除外します。
2. 定期的な GCDS タスクを設定します。
D. 1. LDAP 検索属性を設定して、LDAP に見つからない手動で作成された Cloud Identity ユーザーを除外します。
2. ユーザーとグループのライフサイクルが変更された後、GCDS を実行します。
Answer: A (メッセージを残す**)**
「Cloud Identity で手動で作成されたユーザーを無効にする」という要件を満たすには、GCDS の LDAP ディレクトリにユーザー アカウントが見つからない場合、アカウントを削除するのではなく停止するように GCDS を設定します。参照: https://support.google.com/a/answer/7177267

最新問題**: 284**
組織では、Google Kubernetes Engine（GKE）上に多数のコンテナ化アプリケーションをデプロイしています。現在、ノードアップデートは手動で適用されています。監査結果によると、重要なパッチが通知の未達により適用されていないことが判明しました。より信頼性が高く、クラウドファーストでスケーラブルなノードアップデートプロセスを設計する必要があります。どうすればよいでしょうか？
A. パッチ適用プロセスをより細かく制御するために、クラスター インフラストラクチャを自己管理型の Kubernetes 環境に移行します。
B. パッチの可用性を継続的に確認し、パッチをダウンロードし、クラスターのすべてのコンポーネントにパッチを適用するカスタム スクリプトを開発します。
C. すべてのノードを自動的にアップグレードするために、毎日再起動をスケジュールします。
D. メンテナンス ウィンドウでノード プールのノードの自動アップグレードを構成します。
Answer: D (メッセージを残す**)**
GKE クラスタ内のノードを更新するための信頼性が高く、クラウド ネイティブでスケーラブルなプロセスを確立するには、指定されたメンテナンス ウィンドウ内でノードの自動アップグレードを構成するのが最も効果的なアプローチです。
オプションA :セルフマネージドKubernetes環境への移行は、パッチ適用やアップデートを含むインフラストラクチャ全体の管理を自社チームが担うことになるため、運用上のオーバーヘッドと複雑さが増大します。これはクラウドファースト戦略の導入という目標に反するものであり、本質的に信頼性の高いアップデートプロセスを実現するものではありません。

オプションB :パッチ管理用のカスタムスクリプトを開発すると、潜在的なリスクとメンテナンスの負担が生じます。このようなスクリプトの信頼性、セキュリティ、スケーラビリティを確保することは困難であり、このアプローチはGKE環境管理のベストプラクティスと一致しない可能性があります。
オプション C: 毎日の再起動をスケジュールしても、ノードに最新のパッチまたは更新が適用されることは保証されません。
更新を管理および適用するメカニズムがなければ、再起動だけではノードのセキュリティとコンプライアンスを維持するのに不十分です。
オプションD :ノードの自動アップグレードを設定すると、GKE がノードを最新の安定バージョンに自動的に更新し、重要なパッチの適用漏れのリスクを軽減します。メンテナンスの時間枠を設定することで、アップグレードのタイミングを制御し、ワークロードの中断を最小限に抑えることができます。このアプローチでは、GKE のマネージドサービスを活用して、セキュリティとコンプライアンスを効率的に維持します。
したがって、オプション D はクラウド ファースト戦略に適合し、GKE のネイティブ機能を活用してノードの更新を効果的に自動化およびスケジュールするため、最適なソリューションです。
参考文献:
ノードの自動アップグレード | Google Kubernetes Engine (GKE)
メンテナンスの時間枠と除外 | Google Kubernetes Engine

最新問題**: 285**
あなたは会社のセキュリティ管理者です。LDAPディレクトリのメールアドレスを持つすべてのセキュリティグループをCloud IAMで同期したいと考えています。
何をすべきでしょうか?
A. 一方向の同期を容易にするために、「ユーザーのメールアドレス」を属性として持つ LDAP 検索ルールを使用してセキュリティ グループを同期するように Google Cloud Directory Sync を構成します。
B. 双方向同期を容易にするために、「ユーザーのメールアドレス」を属性として持つ LDAP 検索ルールを使用してセキュリティ グループを同期するように Google Cloud Directory Sync を構成します。
C. 管理ツールを使用して、メールアドレス属性に基づいてサブセットを同期します。Google ドメインにグループを作成します。Google ドメインに作成されたグループには、明示的な Google Cloud Identity and Access Management (IAM) ロールが自動的に割り当てられます。
D. 管理ツールを使用して、グループオブジェクトクラス属性に基づいてサブセットを同期します。Google ドメインにグループを作成します。Google ドメインに作成されたグループには、明示的な Google Cloud Identity and Access Management (IAM) ロールが自動的に割り当てられます。
Answer: (解答を表示する**)**

最新問題**: 286**
IaaS のセキュリティ責任共有モデルでは、スタックのどの 2 つのレイヤーに対して顧客が責任を共有するのでしょうか (2 つ選択してください)。
A. ハードウェア
B. ネットワークセキュリティ
C. ストレージ暗号化

D. アクセスポリシー
E. ブート
Answer: B,D (メーッセージを残す**)**
目標: IaaS の共有セキュリティ責任モデルにおいて、顧客が責任を共有するスタックのレイヤーを特定します。
解決策: 共有責任モデルを理解する。
ネットワーク セキュリティ: ファイアウォールの設定、VPC の管理、安全なネットワーク トラフィックの確保など、ネットワーク セキュリティの構成はお客様の責任となります。
アクセス ポリシー: お客様は、承認されたユーザーのみがリソースにアクセスできるように、IAM ロールや権限などのアクセス ポリシーを管理する責任があります。
IaaS では、通常、クラウド プロバイダーが基盤となるインフラストラクチャを担当し、顧客はクラウド上のアプリケーションとデータのセキュリティ保護を担当します。
参考文献:
共有責任モデル
Google Cloud セキュリティの概要