Google.Professional-Cloud-Security-Engineer-JPN.v2026-02-19.q142

試験コード：	Professional-Cloud-Security-Engineer-JPN
試験名称：	Google Cloud Certified - Professional Cloud Security Engineer Exam (Professional-Cloud-Security-Engineer日本語版)
認証ベンダー：	Google
無料問題の数：	142
バージョン：	v2026-02-19
ページの閲覧量：	103
問題集の閲覧量：	1452

https://www.jpnshiken.com/shiken/Google.Professional-Cloud-Security-Engineer-JPN.v2026-02-19.q142.html

質問: **1**
顧客は、モバイル ワーカーが Google Cloud Platform (GCP) でホストされている CRM Web インターフェイス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。顧客は、それ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。あなたのチームは、2 要素認証をサポートするアプリケーションの前に認証レイヤーを必要としています。これらの要件を満たすために、お客様はどの GCP プロダクトを実装する必要がありますか?
A. Cloud Identity-Aware Proxy
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
正解: **(**正解を表示します**)**
Cloud Identity-Aware Proxy (Cloud IAP) provides a way to control access to your web applications and resources running on Google Cloud. It works by verifying the identity of a user trying to access the application and supports multi-factor authentication (MFA). Cloud IAP can restrict access to users on the corporate network and also supports access over the internet securely.
Steps:
Enable Cloud IAP: In the Google Cloud Console, navigate to the IAP section and enable IAP for your web application.
Configure OAuth Consent Screen: Set up the OAuth consent screen to manage how users grant access.

Set Up Authentication: Use Google Identity Platform to manage users and enable two-factor authentication.
Add Users: Grant users access to the application by adding their identities in the IAP settings.
References:
Google Cloud: Identity-Aware Proxy
Setting up IAP

質問**: 2**
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、ML 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 アーキテクチャのセキュリティ、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する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. MLモデルに使用す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とCloud Storageからユーザーデータにアクセスするために使用する暗号鍵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、ポイズニング攻撃のリスクを軽減します。認証にはIAMを使用し、コードリポジトリとクラウドサービスには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出を実現します。
正解**: B (**コメントを発表する**)**
To enhance the security of your machine learning (ML) model supply chain within a serverless architecture, it's crucial to implement measures that protect both the development and deployment pipelines.
Option A: While limiting external dependencies and rotating encryption keys are good security practices, they do not directly address the risks associated with the ML model supply chain.
Option B: Implementing container image vulnerability scanning during development and pre-deployment helps identify and mitigate known vulnerabilities in your container images. Enforcing Binary Authorization ensures that only trusted and verified images are deployed in

your environment. This combination directly strengthens the security of the ML model supply chain by validating the integrity of container images before deployment.
Option C: Sanitizing training data and applying role-based access controls are important security practices but do not specifically safeguard the deployment pipeline against compromised container images.
Option D: While strict firewall rules and intrusion detection systems enhance network security, they do not specifically address vulnerabilities within the container images or the deployment process.
Therefore, Option B is the most effective approach, as it directly addresses the security of the development and deployment pipeline by ensuring that only vetted and secure container images are used in your environment.
References:
Container Scanning Overview
Binary Authorization Overview

質問**: 3**
あなたの会社のメッセージング アプリが FIPS 140-2 に準拠するために、GCP コンピューティング サービスとネットワーク 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 キャッシングにローカル SSD を使用し、インスタンス間の通信に UDP を使用します。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喜んで行います。要件を満たすためにどのオプションを推奨する必要がありますか?
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 が使用するインスタンス テンプレートのディスク暗号化をカスタマー マネージド 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 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 マネージド 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。
正解**: (**正解を表示します**)**
To comply with FIPS 140-2 for the messaging app, you need to ensure that both data at rest and data in transit are encrypted according to the standard. Using customer-managed encryption keys (CMEK) ensures that you have control over the encryption keys, and BoringSSL is a library that meets FIPS 140-2 standards for encrypting data in transit.
Steps:
* Encrypt Local SSDs: Modify the instance template for the Managed Instance Group (MIG) to use customer-managed encryption keys (CMEK) for encrypting Local SSDs.

* Enable BoringSSL: Update the application to use the BoringSSL library for all instance-to-instance communication to ensure that all data in transit is encrypted according to FIPS 140-2 standards.
References:
Google Cloud: Customer-managed encryption keys (CMEK)
BoringSSL documentation

質問**: 4**
顧客は、平文のシークレットをソース コード管理 (SCM) システムに保存する代わりの方法を必要としています。
お客様は、Google Cloud Platform を使用してこれをどのように達成する必要がありますか?
A. Cloud Source Repositories を使用し、シークレットを Cloud SQL に保存します。
B. シークレットを顧客管理の暗号鍵 (CMEK) で暗号化し、Cloud Storage に保存します。
C. Cloud Data Loss Prevention API を実行してシークレットをスキャンし、Cloud SQL に保存します。
D. ローカル SSD を使用して SCM を Compute Engine VM にデプロイし、プリエンプティブル VM を有効にします。
正解**: B (**コメントを発表する**)**
Storing secrets securely is crucial for maintaining the integrity and confidentiality of your applications. Here is how you can achieve this using Google Cloud Platform:
Encrypt the Secrets: Use Customer-Managed Encryption Keys (CMEK) to encrypt your secrets. CMEK allows you to have greater control over the encryption keys used to protect your data. This ensures that even if the storage medium is compromised, the secrets remain protected by strong encryption.
Store in Cloud Storage: Store the encrypted secrets in Google Cloud Storage. Cloud Storage is a secure and scalable object storage service. By using encrypted storage, you can ensure that the secrets are securely stored and can only be accessed by authorized entities.
This method provides a secure and managed way to store secrets, ensuring that they are not exposed in plain text within your source code management system.
References
Customer-Managed Encryption Keys (CMEK)
Google Cloud Storage Security

質問**: 5**
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。
正解**: (**正解を表示します**)**
The requirements are met by granting access at the highest point in the resource hierarchy that encompasses all the necessary resources, using the least privileged role required.
Least Privilege Role: The team needs to read data and not modify or delete it. The roles/bigquery.dataViewer role is the correct least privileged role for read-only access to data.
Minimize Operational Overhead: Granting the role at the Folder level ensures that the access is automatically inherited by all current and future projects within that folder, drastically reducing the operational overhead compared to granting the role per project (C) or per dataset (A).
Scope: The Folder scope (Data Warehouse folder) is the container for all BigQuery data in the projects within the folder, making it the ideal single point of granting access.
Extracts:
"IAM roles are inherited down the resource hierarchy... Granting a role at the folder level will grant the principal that role across all projects within that folder, including any projects created in the future." (Source
10.1)
"The BigQuery Data Viewer (roles/bigquery.dataViewer) role grants permission to read data in BigQuery tables and views... It does not grant permissions to modify or delete the data, adhering to the principle of least privilege for read-only tasks." (Source 10.2)

質問**: 6**
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。その企業は、イメージをスキャンして既知のセキュリティ問題がないか確認し、レポートを Google Cloud の外部に公開することなくセキュリティ チームと安全に共有したいと考えています。
あなたは何をするべきか？
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 にないすべてのクラスタを、可能な最新の GKE バージョンにアップグレードします。
* 3. Security Command Center からの結果の表示と共有
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 の一般にアクセスできるバケットにレポートをアップロードします。
* 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します
* 3. 自動スキャンのために画像を Artifact Registry にプッシュします。
* 4. Artifact Registry の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、自動スキャンのために GitHub に保存します。
* 3. GitHub からレポートをダウンロードし、セキュリティ チームと共有します
正解**: (**正解を表示します**)**
"The service evaluates all changes and remote access attempts to detect runtime attacks in near-real time." : https://cloud.google.com/security-command-center/docs/concepts-container-threat-detection-overview This has nothing to do with KNOWN security Vulns in images

質問**: 7**
Google Cloud に保存されている特定の BigQuery データを暗号化するには、Cloud External Key Manager を使用して暗号鍵を作成する必要があります。最初にどの手順を実行する必要がありますか?
A. 1. Google Cloud プロジェクトで一意の Uniform Resource Identifier (URI) を持つ既存のキーを作成または使用します。
2. Google Cloud プロジェクトに、サポートされている外部鍵管理パートナー システムへのアクセス権を付与します。
B. 1. Cloud Key Management Service (Cloud KMS) で一意の Uniform Resource Identifier (URI) を持つ既存の鍵を作成または使用します。
2. Cloud KMS で、キーを使用するためのアクセス権を Google Cloud プロジェクトに付与します。
C. 1. サポートされている外部キー管理パートナー システムで、一意の Uniform Resource Identifier (URI) を持つ既存のキーを作成または使用します。
2. 外部鍵管理パートナー システムで、この鍵に Google Cloud プロジェクトを使用するためのアクセス権を付与します。
D. 1. Cloud Key Management Service (Cloud KMS) で一意の Uniform Resource Identifier (URI) を使用して外部キーを作成します。
2. Cloud KMS で、キーを使用するためのアクセス権を Google Cloud プロジェクトに付与します。
正解**: (**正解を表示します**)**
https://cloud.google.com/kms/docs/ekm#how_it_works
- First, you create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.

- Next, you grant your Google Cloud project access to use the key, in the external key management partner system.
- In your Google Cloud project, you create a Cloud EKM key, using the URI or key path for the externally-managed key.

質問: **8**
顧客管理の暗号鍵（CMEK）で暗号化された新しい Cloud Storage バケットを環境内に設定しています。CMEK はクラウド キー管理サービス (KMS) に保存されます。プロジェクト「prj-a」内にあり、Cloud Storage バケットはプロジェクト「prj-b」を使用します。キーはクラウド ハードウェア セキュリティ モジュール (HSM) によってサポートされており、リージョン europe-west3 に存在します。ストレージ バケットはリージョン europe-west1 に配置されます。バケットを作成するときは、キーにアクセスできません。その理由をトラブルシューティングする必要があります。
アクセスの問題の原因は何ですか?
A. ファイアウォール ルールにより、キーへのアクセスが妨げられています。
B. Cloud HSM は Cloud Storage をサポートしていません
C. CMEK は Cloud Storage バケットとは異なるプロジェクトにあります
D. CMEK は Cloud Storage バケットとは異なるリージョンにあります。
正解: **D** (コメントを発表する)
When you use a customer-managed encryption key (CMEK) to secure a Cloud Storage bucket, the key and the bucket must be located in the same region. In this case, the key is in europe-west3 and the bucket is in europe-west1, which is why you're unable to access the key.

質問: **9**
組織では仮想マシン（VM）を Google Cloud に移行しています。プロジェクト全体で使用されるオペレーティング システム イメージが信頼できるものであり、セキュリティ要件を満たしていることを確認する必要があります。
何をすべきでしょうか?
A. 信頼できるイメージ プロジェクトから取得したイメージからのみブート ディスクを作成できるようにするための組織ポリシーを実装します。
B. 信頼できるイメージ リポジトリから新しい仮想マシンが作成された場合に自動的にトリガーされる Cloud Function を作成します。イメージが非推奨になっていないことを確認します。
C. すべてのプロジェクトで Shielded VM サービスを有効にして、信頼できるイメージ リポジトリの使用を強制する組織ポリシー制約を実装します。
D. 信頼できるイメージ リポジトリに一般的な脆弱性と露出 (CVE) が存在しないことを確認するセキュリティ スキャナーを自動化します。
正解: **A** (コメントを発表する)
Define Trusted Image Projects:

Identify the project or projects where your trusted operating system images are stored.
Ensure these images meet your organization's security requirements and are regularly updated to mitigate vulnerabilities.
Create an Organization Policy:
Navigate to the Organization Policies page in the Google Cloud Console.
Create a policy constraint that restricts the creation of boot disks to only those images stored in your trusted image project(s).
The policy constraint to use is constraints/compute.trustedImageProjects.
Apply the Policy:
Apply this organization policy at the appropriate level (organization, folder, or project) to enforce that all new VM instances use images from the trusted repository.
This ensures consistency in the security posture across all projects within the organization.
Monitor Compliance:
Regularly monitor the compliance with this policy using audit logs and other monitoring tools.
Update the trusted images as necessary to ensure they remain secure and compliant with your security standards.
References:
Organization Policy Service
Trusted Image Projects Constraint

質問**: 10**
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。
正解**: B (**コメントを発表する**)**

The most effective way to address VM sprawl while enforcing consistent security baselines at the VM creation stage (VM lifecycle management) is through the use of immutable, hardened images built via an automated pipeline.
Centralized Image Management and Hardening: A Cloud Build pipeline is the standard way to automate the creation of "golden images." The pipeline can install OS/packages, apply hardening scripts (e.g., CIS benchmarks), run vulnerability scans, and then store only the verified, secure images in a central registry. This centralizes control over the security baseline.
Enforcement: Instance Templates are the mechanism to standardize VM deployment. By configuring the templates to only point to the central registry of approved, hardened images, you ensure that every new VM spun up automatically adheres to the security baseline. This prevents teams from deploying unhardened or insecure images, solving the "VM sprawl" and "consistent security hardening" problem at its source.
Option A (SCC Posture Management) is a detective control that monitors after the VM is deployed; it does not prevent unhardened VMs from being created, which is the goal of lifecycle management.
Option D (VM Manager) is excellent for ongoing patching and updating of existing VMs, but it doesn't solve the initial problem of ensuring a secure, centralized, hardened image is used for creation (which is where the baseline is enforced).
Extracts:
"Golden images that are configured and used to create servers play a key role in allowing companies to scale securely." (Source 1.2)
"Using an automated tool eradicates this issue. When engineers use images produced by [automated tools], the evidence is clear, as everything needed is pre-baked into the image." (Source 1.2)
"An instance template is a convenient way to save a virtual machine (VM) instance's configuration that includes machine type, boot disk image... You can use an instance template to... Create individual VMs." (Source 3.3) The overall strategy described in Option B-automate hardening, scan, store, and enforce usage via templates-is the best practice for secure and compliant VM deployment at scale.

質問**: 11**
組織は、現在のオンプレミスの生産性向上ソフトウェア システムから G Suite に移行しています。以前のオンプレミス システムに対して、地域の規制機関によって義務付けられた、いくつかのネットワーク セキュリティ制御が実施されていました。組織のリスク チームは、ネットワーク セキュリティ制御が維持され、G Suite で有効であることを確認したいと考えています。この移行をサポートするセキュリティ アーキテクトは、組織と Google Cloud の間の新しい共有責任モデルの一部として、ネットワーク セキュリティ制御を確実に実施するよう求められました。
要件を満たすのに役立つソリューションはどれですか?

A. ファイアウォール ルールが必要な制御を満たすように設定されていることを確認します。
B. Cloud Armor をセットアップして、G Suite のネットワーク セキュリティ コントロールを確実に管理できるようにします。
C. ネットワーク セキュリティは組み込みソリューションであり、G Suite などの SaaS プロダクトに対する Google のクラウド責任です。
D. Virtual Private Cloud (VPC) ネットワークのアレイをセットアップして、関連する規制で義務付けられているネットワーク セキュリティを制御します。
正解**: (**正解を表示します**)**
https://gsuite.google.com/learn-more/security/security-whitepaper/page-1.html Shared responsibility "Security of the Cloud" - GCP is responsible for protecting the infrastructure that runs all of the services offered in the GCP Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run GCP Cloud services.

質問**: 12**
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。
正解**: (**正解を表示します**)**
Use the org policy constraint "Google Cloud Platform - Resource Location Restriction" on your Google Cloud organization node: This organizational policy constraint allows you to restrict the locations where your resources can be created. By setting this constraint to allow only Europe regions, you can ensure compliance with GDPR and other regional regulations. Implementation: To implement this, you need to configure the organization policy with the constraint constraints/gcp.resourceLocations. You can specify allowed regions such as europe-west1 and europe-west4 to ensure resources are only created in these locations.
References
Resource Location Restriction documentation
GDPR compliance on Google Cloud

質問**: 13**

大規模な金融機関は、ビッグデータ分析を Google Cloud Platform に移行しています。彼らは、BigQuery に保存されているデータの暗号化プロセスを最大限に制御したいと考えています。
機関はどのような手法を使用する必要がありますか?
A. Cloud Storage をフェデレーション データ ソースとして使用します。
B. クラウド ハードウェア セキュリティ モジュール (Cloud HSM) を使用します。
C. 顧客管理の暗号鍵 (CMEK)。
D. 顧客指定の暗号化キー (CSEK)。
正解: **C** (コメントを発表する)
If you want to manage the key encryption keys used for your data at rest, instead of having Google manage the keys, use Cloud Key Management Service to manage your keys. This scenario is known as customer- managed encryption keys (CMEK).
https://cloud.google.com/bigquery/docs/encryption-at-rest Reference:
https://cloud.google.com/bigquery/docs/encryption-at-rest

質問: **14**
組織のアプリケーションは、顧客の注文を処理するために顧客データへの読み取りアクセスを必要とするパートナーアプリケーションと統合されています。顧客データは、Cloud Storage バケットの 1 つに保存されています。複数のオプションを評価した結果、このアクティビティにはサービス アカウント キーの使用が必要であると判断しました。サービス アカウント キーの侵害によってデータが失われるリスクを最小限に抑える方法について、パートナーにアドバイスする必要があります。パートナーにはどのような対応をアドバイスすればよいでしょうか。
A. VPC Service Controls の境界を定義し、Cloud Storage API を制限します。境界に上り（内向き）ルールを追加して、境界外からサービスアカウントの Cloud Storage API にアクセスできるようにします。
B. 新しいデータが追加されたときに、機密データ保護を使用して Cloud Storage バケットをスキャンし、すべての顧客データを自動的にマスクします。
C. 関連するサービス アカウントを通じてアクセスされるアプリケーションのすべてのデータが、顧客管理の暗号鍵 (CMEK) を使用して保存時に暗号化されていることを確認します。
D. シークレット管理サービスを実装します。サービスアカウントキーを頻繁にローテーションするようにサービスを設定します。キーへの適切なアクセス制御を設定し、サービスアカウントキーを作成できるユーザーを制限します。
正解: (正解を表示します)
When integrating applications that require access to sensitive data stored in Cloud Storage, managing service account keys securely is crucial to prevent unauthorized access or data loss.
Option A: Defining a VPC Service Controls perimeter enhances security by restricting access to Google Cloud services. However, configuring ingress rules to allow external access for the

service account may introduce complexities and potential security gaps, especially if the partner's infrastructure is outside the defined perimeter.
Option B: Scanning and masking customer data addresses data sensitivity but does not mitigate risks associated with compromised service account keys. This approach focuses on data content rather than access control mechanisms.
Option C: Encrypting data at rest using customer-managed encryption keys (CMEK) ensures data confidentiality but does not directly address the security of service account keys or access controls.
Option D: Implementing a secret management service to handle service account keys is a best practice. By configuring the service to frequently rotate keys, you reduce the window of opportunity for malicious actors to exploit compromised keys. Additionally, enforcing strict access controls ensures that only authorized personnel can create or manage service account keys, minimizing the risk of unauthorized access. This approach directly addresses the security concerns related to service account key management.
Therefore, Option D is the most appropriate recommendation, as it focuses on securely managing service account keys through rotation and access controls, thereby minimizing the risk of data loss due to compromised keys.
References:
Best Practices for Managing Service Account Keys
Secret Manager Documentation

質問**: 15**
Google Cloud 上には多数のプライベート仮想マシンがあります。場合によっては、リモートの場所から Secure Socket Shell (SSH) を介してサーバーを管理する必要があります。セキュリティとコスト効率を最適化する方法でサーバーへのリモート アクセスを構成したいと考えています。
あなたは何をするべきか？
A. 企業ネットワークから Google Cloud へのサイト間 VPN を作成します。
B. パブリック IP アドレスを使用してサーバー インスタンスを構成する 企業 IP からのトラフィックのみを許可するファイアウォール ルールを作成します。
C. Identity-Aware Proxy (IAP) IP 範囲からのアクセスを許可するファイアウォール ルールを作成します。IAP で保護されたトンネル ユーザーの役割を管理者に付与します。
D. パブリック IP を使用してジャンプ ホスト インスタンスを作成します。ジャンプ ホスト経由で接続してインスタンスを管理します。
正解**: C (**コメントを発表する**)**
Using Identity-Aware Proxy (IAP) for managing SSH access to private VMs ensures secure access control and avoids the need for public IPs. IAP allows you to enforce identity-based access control policies.
Enable IAP: Ensure that IAP is enabled for your project. This can be done via the Google Cloud Console under "Security" -> "Identity-Aware Proxy".

Set Up Firewall Rule: Create a firewall rule to allow SSH traffic from the IAP IP ranges.
Navigate to "VPC network" -> "Firewall".
Create a new rule allowing ingress traffic on port 22 (SSH) from the IAP IP ranges.
Assign IAP-Secured Tunnel User Role: Grant the roles/iap.tunnelResourceAccessor role to the administrators who need SSH access.
Go to "IAM & Admin" -> "IAM".
Assign the IAP-Secured Tunnel User role to the relevant users or groups.
SSH Using IAP: Administrators can now use IAP to SSH into the instances. This can be done using the gcloud command:
gcloud compute ssh [INSTANCE_NAME] --tunnel-through-iap
References:
Using Identity-Aware Proxy for TCP forwarding
Google Cloud Firewall Rules

質問**: 16**
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。セキュリティ管理基準の一つでは、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. Security Health Analytics 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90日後にローテーションされていない場合、Security Command Center で検出結果が生成されます。
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. Cloud Logging を使用して、タイムリーな鍵更新を確認する指標を定義します。鍵が90日後にローテーションされない場合、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。
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 日後に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。
正解**: (**正解を表示します**)**

質問: **17**
PCI コンプライアンスについて GCP を評価したい。Google 固有のコントロールを特定する必要があります。
情報を見つけるためにどのドキュメントを確認する必要がありますか?
A. Google Cloud Platform: お客様の責任マトリックス
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
正解: **(**正解を表示します**)**
To evaluate Google Cloud Platform (GCP) for PCI compliance and identify Google's inherent controls, you should review the "Google Cloud Platform: Customer Responsibility Matrix". This document provides detailed information about the shared responsibility model, outlining the security controls managed by Google and those that are the responsibility of the customer.
Steps to access and use the document:
Access the Document:
Go to the Google Cloud compliance resource center.
Locate the "Customer Responsibility Matrix" for PCI DSS compliance.
Review Inherent Controls:
The document lists various controls and specifies whether they are managed by Google, the customer, or both.
It covers different aspects such as infrastructure security, data protection, and compliance requirements.
Analyze PCI Compliance:
Use the matrix to understand which PCI DSS requirements are inherently addressed by Google Cloud.
Identify the controls you need to implement and manage as a customer to ensure full compliance.
By reviewing this document, you can gain a comprehensive understanding of the inherent controls provided by Google Cloud and the responsibilities you must fulfill to achieve PCI compliance.
Google Cloud Compliance Documentation
PCI DSS Compliance on Google Cloud

質問: **18**

組織は、インフラストラクチャをオンプレミス環境から Google Cloud Platform (GCP) に移行し始めています。組織が実行したいと考えている最初のステップは、現在のデータ バックアップと障害復旧ソリューションを GCP に移行して、後で分析できるようにすることです。組織の本番環境は、無期限にオンプレミスのままになります。この組織は、スケーラブルで費用対効果の高いソリューションを望んでいます。
組織はどの GCP ソリューションを使用する必要がありますか?
A. 継続的な更新を伴うデータ パイプライン ジョブを使用する BigQuery
B. スケジュールされたタスクと gsutil を使用する Cloud Storage
C. 永続ディスクを使用する Compute Engine 仮想マシン
D. 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
正解**: (**正解を表示します**)**
To migrate the current data backup and disaster recovery solutions to GCP while keeping the production environment on-premises, the most scalable and cost-efficient solution is using Google Cloud Storage with scheduled tasks and the gsutil command.
Setup Cloud Storage: Create a Cloud Storage bucket to store the backups.
Go to the Cloud Console and navigate to Cloud Storage.
Click "Create bucket" and follow the prompts to configure the storage bucket.
Install gsutil: Ensure gsutil is installed on the on-premises servers.
gsutil is a command-line tool for interacting with Cloud Storage.
Follow the installation guide here.
Create Backup Script: Write a script to upload data to Cloud Storage using gsutil.
#!/bin/bash gsutil -m cp -r /path/to/local/backup gs://your-bucket-name Schedule Backup Task: Use a scheduling tool like cron on Linux to run the backup script at regular intervals.
Edit the crontab file with crontab -e and add an entry like:
Cloud Storage Documentation
gsutil Documentation

質問**: 19**
あなたは、機密性の高い患者データの保存と処理のためにクラウドへの展開を進めている医療機関で働いています。a. 選択した Google Cloud 構成が、以下の厳格な規制要件を満たしていることを確認する必要があります。
データは特定の地理的領域内に保存される必要があります。
患者データに関する特定の管理アクションには、指定されたコンプライアンス担当者からの明示的な承認が必要です。
患者データへのアクセスは監査可能である必要があります。
何をすべきでしょうか?
A. 高可用性を実現するために、複数の標準 Google Cloud リージョンを選択します。患者データを含む個々のストレージ オブジェクトにアクセス制御リスト (ACL) を実装します。Cloud Audit Logs を有効にします。

B. 冗長性を確保するために、複数のリージョンに Assured Workloads 環境をデプロイします。きめ細かな権限設定が可能なカスタム IAM ロールを活用します。VPC Service Controls を使用して、ネットワークレベルのデータを分離します。
C. 承認されたリージョンに Assured Workloads 環境をデプロイします。患者データに対する機密性の高い操作に対してアクセス承認を設定します。Cloud Audit Logs とアクセスの透明性の両方を有効にします。
D. 標準の Google Cloud リージョンを選択します。Access Context Manager を使用して、ユーザーの所在地と職務に基づいて患者データへのアクセスを制限します。Cloud Audit Logging とアクセスの透明性の両方を有効にします。
正解**: (**正解を表示します**)**
To ensure compliance with strict regulatory requirements for storing and processing sensitive patient data in the cloud, the following measures should be implemented:
Assured Workloads: Deploying an Assured Workloads environment in an approved region ensures that data residency requirements are met by restricting data storage and processing to specific geographic locations.
Assured Workloads provide predefined controls and configurations tailored to meet regulatory compliance needs.
Access Approval: Configuring Access Approval ensures that certain administrative actions on patient data require explicit approval from designated compliance officers. This adds a layer of control over sensitive operations, aligning with the need for explicit approvals.
Cloud Audit Logs and Access Transparency: Enabling Cloud Audit Logs provides a detailed record of actions taken on your data, supporting the requirement for auditability. Access Transparency logs offer visibility into Google's administrative access to your content, enhancing transparency and compliance.
Therefore, Option C is the most appropriate choice, as it comprehensively addresses data residency, administrative control, and auditability requirements.
References:
Assured Workloads Overview
Access Approval Documentation
Cloud Audit Logs Overview
Access Transparency Overview

質問**: 20**
組織は、本番環境アプリケーションの脆弱性がセキュリティ侵害につながったという最近のニュース報道を懸念しています。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環境で実行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. Binary Authorization を有効にし、スキャンの証明書を作成します。
B. gcloud アーティファクト docker イメージを使用して、LOCATION-docker.pkg.dev/PROJECT_ID を記述します。

CI/CD パイプラインで /REPOSITORY/IMAGE_ID@sha256:HASH --show-package-vulnerability を実行し、重大な脆弱性に対してパイプラインの障害をトリガーします。
C. Kubernetesのロールベースアクセス制御（RBAC）をクラスタアクセスの信頼できる情報源として使用し、
「container clusters.get」を限定されたユーザーにのみ実行させます。これらのユーザーにGKEクラスタへの設定アクセスを含むkubeconfigファイルの生成を許可することで、デプロイメントへのアクセスを制限します。
D. 開発に Cloud Code の使用を強制することで、ユーザーはコードをチェックインする前に、脆弱なライブラリや依存関係に関するセキュリティ フィードバックをリアルタイムで受け取ることができます。
正解: **(**正解を表示します**)**
The core requirement is to ensure only scanned and verified containers can run in the environment, which is a deployment-time enforcement action.
Binary Authorization is the service designed for this purpose. It is a deployment-time security control that ensures only trusted container images are deployed on Google Kubernetes Engine (GKE) or other supported container platforms. The core mechanism it uses to verify that an image has completed required steps (like a vulnerability scan) is an attestation.
Extracts:
"GCP Binary Authorization is a security feature designed to prevent the deployment of unverified, unauthorized, or potentially malicious container images to Kubernetes clusters." (Source 1.1)
"Binary Authorization ensures that only images that are signed by trusted entities (such as a trusted attestation authority) are allowed to be deployed." (Source 1.1)
"Binary Authorization aims to reduce the risk of deploying defective, vulnerable, or unauthorized software in this type of environment. Using this service, you can prevent images from being deployed unless it satisfies a policy you define." (Source 1.2)
"The most common Binary Authorization use cases involve attestations. An attestation certifies that a specific image has completed a previous stage... Attestations signify that the associated image was built by successfully executing a specific, required process. For example, the attestation might indicate that the image has passed all required end-to-end functional testing in a staging environment." (Source 1.2, 1.4)
"After a container image is built, an attestation can be created to affirm that a required activity was performed on the image such as a regression test, vulnerability scan, or other test." (Source 1.5) Option A correctly identifies the two necessary components for this deployment-time enforcement: Binary Authorization for policy enforcement and attestations to certify that the vulnerability scan (or other required check) has been completed and verified.

質問**: 21**

集中型セキュリティ サービスが会社で実装されており、Google Cloud で実行されてい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。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ながら、開発者がプロジェクト内でファイアウォール ルールを構成できる高い自律性を確保する必要があります。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。中央のセキュリティ 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の接続を許可し、他のすべてのトラフィックを次のファイアウォールレベルに誘導することで、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 ルールを一元的に管理します。
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。ルールの変更権限を Terraform サービス アカウントのみに制限します。
正解**: (**正解を表示します**)**
The problem has two key requirements:
All applications must send data to a centralized security service.
Developers need high autonomy over firewall rules within their projects.
Prevent accidental blockage of access to the central security service.
This scenario requires a mechanism to enforce critical network policies at a higher level of the resource hierarchy while still allowing project-level flexibility.
Hierarchical Firewall Policies: Google Cloud's Hierarchical Firewall Policies (HFP) are designed precisely for this purpose. They allow administrators to define firewall rules at the organization or folder level, and these rules are inherited by all projects and VPC networks within that hierarchy. Crucially, HFP rules can be prioritized. Rules with higher priority (lower numerical value) are evaluated first. This means you can create high-priority "allow" rules for critical services that cannot be overridden or blocked by project-level firewall rules.Extract Reference: "Hierarchical firewall policies allow you to define and enforce consistent network security policies across your organization. Policies can be applied at the organization or folder level, and they are inherited by all projects and VPC networks within that hierarchy." and "Rules in a hierarchical firewall policy can take precedence over VPC network firewall rules based on priority. A rule with a lower priority value takes precedence over a rule with a higher priority value." (Google Cloud documentation: https://cloud.google.com/vpc/docs/firewall-policies-overview)
Preventing Accidental Blockage while Allowing Autonomy: By setting a high-priority "allow" rule for the central security service in a hierarchical firewall policy, you guarantee that this traffic will always be permitted, regardless of what project-level firewall rules developers

might configure. This ensures the critical connectivity while still allowing developers to manage other, less critical firewall rules within their projects with high autonomy.
Let's evaluate the other options:
A). Deploy a central Secure Web Proxy and connect it to all VPC networks. Create a Secure Web Proxy policy to allow traffic to the central security service. A Secure Web Proxy is for HTTP/S outbound traffic to external web services. The central security service might not be an external web service, and this solution is focused on application-layer proxies, not general network connectivity like sending data to an internal service. Also, it doesn't directly address the challenge of developers blocking access with project-level firewall rules.
C). Create a central project to manage Shared VPC networks which will be accessible to all other projects.
Administer all firewall rules centrally within this project. While Shared VPC centralizes network management, it means all firewall rules are administered centrally. This directly contradicts the requirement for developers to have "high autonomy to configure firewall rules within their projects." Shared VPC would centralize too much control for this specific scenario.
D). Use Terraform to automate the creation of the required firewall rule in all projects. Restrict rule change permissions solely to the Terraform service account. This approach automates the creation but doesn't prevent developers from creating conflicting or overriding rules in their projects (unless Terraform is used to manage all rules, again removing autonomy). It also relies on restricting IAM permissions for all firewall rules, which is against the "high autonomy" requirement for developers. Hierarchical firewall policies offer a more robust and native solution for overriding and enforcing specific rules.
Therefore, implementing a hierarchical firewall policy is the most effective solution, as it allows for the enforcement of critical security service connectivity at a higher level, while still granting developers the desired autonomy over their project-specific firewall rules.

質問**: 22**
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. ID 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
正解**: (**正解を表示します**)**
To enforce access control policies for applications and resources in Google Cloud, the recommended service is Identity-Aware Proxy (IAP).
Identity-Aware Proxy (IAP):
IAP allows you to control access to your applications and resources based on the identity of the user and the context of the request. It integrates with IAM to provide fine-grained access control, ensuring that only authorized users can access specific resources.

IAP helps enforce security policies at the application layer, providing an additional layer of protection beyond traditional network-based security measures.
References
Identity-Aware Proxy documentation

質問: **23**
Google Cloud 環境には、組織ノードが 1 つと、 Apps」という名前のフォルダが 1 つあり、そのフォルダ内に複数のプロジェクトがあります。組織ノードは、constraints/iam.allowedPolicyMemberDomains 組織ポリシーを適用し、terramearth.com 組織のメンバーを許可します。 Apps」フォルダは、constraints/iam.allowedPolicyMemberDomains 組織ポリシーを適用し、flowlogistic.com 組織のメンバーを許可します。また、inheritFromParent: false プロパティも設定されています。
ユーザー testuser@terramearth.com に、Apps フォルダー内のプロジェクトへのアクセスを許可しようとします。
あなたの行動の結果は何ですか、そしてその理由は何ですか?
A. 制約を一時的に非アクティブ化するには、現在のプロジェクトで constraints/iam.allowedPolicyMemberDomains 組織ポリシーを定義する必要があるため、アクションは失敗します。
B. 制約/iam.allowedPolicyMemberDomains 組織ポリシーが設定されており、flowlogistic.com 組織のメンバーのみが許可されているため、アクションは失敗します。
C. terramearth.com と flowlogistic.com の両方の組織のメンバーが Apps」フォルダ内のプロジェクトにアクセスできるため、アクションは成功します。
D. すべてのポリシーが基礎となるフォルダーとプロジェクトに継承されるため、アクションは成功し、新しいメンバーがプロジェクトの Identity and Access Management (1AM) ポリシーに正常に追加されます。
正解: **B (**コメントを発表する**)**
The action fails because a constraints/iam.allowedPolicyMemberDomains organization policy is in place and only members from the flowlogistic.com organization are allowed. The inheritFromParent: false property on the "Apps" folder means that it does not inherit the organization policy from the organization node. Therefore, only the policy set at the folder level applies, which allows only members from the flowlogistic.com organization. As a result, the attempt to grant access to the user testuser@terramearth.com fails because this user is not a member of the flowlogistic.com organization.

質問: **24**
Cloud Run でアプリケーションを実行しています。脆弱性スキャンのためにコンテナ分析を既に有効にしています。しかし、デプロイされた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。
正解: **(**正解を表示します**)**
To ensure that only trusted container images are deployed on Cloud Run, you can implement Binary Authorization, which is a deploy-time security control that ensures only trusted images are used.
* Set Up Binary Authorization:
* Navigate to the Google Cloud Console.
* Go to Security > Binary Authorization.
* Configure the policy to include attestors that verify your trusted images.
* Enable Binary Authorization on Cloud Run:
* Go to the Cloud Run service.
* Enable Binary Authorization on your existing Cloud Run services by selecting the appropriate Binary Authorization policy.
* Set Organization Policy:
* Go to the Organization Policies page in the Google Cloud Console.
* Add a constraint for constraints/run.allowedBinaryAuthorizationPolicies.
* Specify the list of allowed Binary Authorization policy names to enforce across your organization.
These steps ensure that any container image deployed on Cloud Run is validated against the specified Binary Authorization policies, preventing untrusted images from being deployed.
Binary Authorization Documentation
Enabling Binary Authorization on Cloud Run

質問: **25**
組織の記録データは Cloud Storage に存在します。すべての記録データは少なくとも 7 年間保持する必要があります。このポリシーは永続的である必要があります。
あなたは何をするべきか？
A. * 1 レコードデータが含まれるバケットを識別します

※2 保存ポリシーを適用し、7年間保存するように設定します。
* 3 ログベースのアラートを使用してバケットを監視し、保持ポリシーの変更が発生しないようにします。
B. * 1 レコードデータを持つバケットを識別します
※2 保存ポリシーを適用し、7年間保存するように設定します。
* 3 ストレージ バケットの更新権限を含む Identity and Access Management (IAM) ロールを削除します。
C. * 1 レコードデータを持つバケットを識別します
*2 データが確実に保持されるようにするためにのみバケット ポリシーを有効にします。
※3 バケットロックを有効にする
D. * 1 レコードデータを持つバケットを識別します
※2 保存ポリシーを適用し、7年間保存するように設定します。
※3 バケットロックを有効にする
正解**: (**正解を表示します**)**
To ensure that your organization's record data is retained for at least seven years in Cloud Storage, you need to apply a retention policy and enable bucket lock. This prevents the policy from being altered or the data from being deleted before the retention period ends.
* Identify Buckets: Determine which Cloud Storage buckets contain the record data that needs to be retained.
* Apply Retention Policy:
* Go to the Google Cloud Console and navigate to "Cloud Storage".
* Select the bucket you identified.
* Go to the "Retention" tab and set a retention policy to retain objects for seven years.
* Enable Bucket Lock:
* Once the retention policy is set, you need to lock the bucket to make the retention policy permanent.
* This is done by enabling the bucket lock. Go to the "Retention" tab and click "Lock".
* Confirm and Monitor:
* Confirm that the bucket lock is applied.
* Monitor the bucket using log-based alerts to ensure compliance.
References:
Cloud Storage Retention Policy
Cloud Storage Bucket Lock

質問**: 26**
あなたは、会社のGoogle Cloud組織におけるID管理を担当しています。従業員が組織の企業ドメイン名を使用して、管理対象外のGoogleアカウントを頻繁に作成しています。今後、従業員がこのような行為を行うことを防ぐための、実用的かつ効率的なソリューションを実装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 ID をスキャンし、管理されていないアカウントを無効にする自動プロセスを実装します。
B. 組織内のすべてのユーザーに対して Google Cloud ID を作成します。新しいユーザーが自動的に追加されるようにしてください。
C. Google Cloud リソース用の新しいドメインを登録します。既存のすべての ID とリソースをこのドメインに移動します。
D. Google Cloud ID と企業メールに同じドメインを使用しないように、企業メールシステムを別のドメインに切り替えます。
正解: **(**正解を表示します**)**
An unmanaged Google account is a personal account created by an individual using a corporate email address (e.g., john@company.com), which the organization cannot control. The root cause is that the organization has not claimed the identity for that email address.
Extracts:
"To prevent unmanaged Google account creation, you have two options: Create a user for every person who has an email address in your domain... If there are unmanaged accounts already created, you can use the Transfer Tool for unmanaged users to invite them to become managed users." (Source 5.1)
"If an admin creates a managed Google Account using the same account name as an existing unmanaged user account, this results in a conflicting account." (Source 5.3) By provisioning an account for every employee (via Google Workspace or Cloud Identity), you effectively claim that domain identity, making it a managed account under IT control and preventing the creation of a new, unmanaged consumer account with the same email address.
Option B describes the foundational, preventative step in identity management: provisioning managed identities for all users in the domain.

質問: **27**
セキュリティ チームがファイアウォール ルールなどのネットワーク リソースを制御できるようにする VPC を作成する必要があります。
ネットワーク リソースの職務を分離できるようにするには、ネットワークをどのように構成する必要がありますか?
A. 複数の VPC ネットワークをセットアップし、マルチ NIC 仮想アプライアンスをセットアップしてネットワークを接続します。
B. VPC ネットワーク ピアリングを設定し、開発者がネットワークを共有 VPC とピアリングできるようにします。
C. プロジェクトに VPC を設定します。Compute ネットワーク管理者の役割をセキュリティ チームに割り当て、Compute 管理者の役割を開発者に割り当てます。
D. セキュリティ チームがファイアウォール ルールを管理する共有 VPC を設定し、サービス プロジェクトを介して開発者とネットワークを共有します。
正解: **(**正解を表示します**)**

Setting up a Shared VPC allows you to create a centrally managed network that spans multiple projects.
Here's how you can achieve this while ensuring separation of duties:
Create a Host Project:
Create a project that will act as the host project for your Shared VPC.
Configure Shared VPC:
In the host project, enable the Shared VPC feature.
Create Service Projects:
Create separate service projects for different teams, such as developers and other stakeholders.
Assign Roles:
Security Team: Grant the Compute Network Admin role. This allows the security team to manage network resources, such as firewall rules, subnets, and routes.
Developers: Share the host project's network with the service projects. Assign roles like Compute Instance Admin to developers in the service projects, enabling them to create and manage VM instances without altering network configurations.
Firewall Management:
The security team will define and manage firewall rules within the host project, ensuring consistent and secure network policies.
Benefits:
Separation of Duties: Security teams handle networking, and developers focus on application deployment and management.
Centralized Control: Network policies are centrally managed, ensuring compliance and security.
Scalability: Easy to add new projects and teams without compromising the overall network security.
References
Google Cloud VPC Documentation
Managing Resources with Shared VPC

質問**: 28**
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) を有効にし、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。
正解: **C (**コメントを発表する**)**
By generating a key in your on-premises environment and storing it in an HSM that you manage, you're ensuring that the key material is fully under your control. Using the key as an external key in Cloud KMS allows you to use the key with Google Cloud services without having the key stored on Google Cloud.
Activating Key Access Justifications (KAJ) provides a reason every time the key is accessed, and you can configure the external key system to reject unauthorized access attempts.

質問: **29**
あなたの会社は、Spark と Hadoop のジョブに Cloud Dataproc を使用しています。Cloud Dataproc で使用される永続ディスクに使用される対称暗号鍵を作成、ローテーション、破棄できるようにしたいと考えています。キーはクラウドに保存できます。
あなたは何をするべきか？
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 を使用して鍵暗号鍵 (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。
正解: **(**正解を表示します**)**
This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.
https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption
https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0

質問: **30**

組織では Vertex AI Workbench インスタンスを使用しています。新しくデプロイされたインスタンスが自動的に最新の状態に保たれ、ユーザーが誤ってオペレーティング システムの設定を変更でき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. VM マネージャーを有効にし、対応する Google Compute Engine インスタンスが追加されていることを確認します。
B. 新しくデプロイされたインスタンスに対して、disableRootAccess および requireAutoUpgradeSchedule 組織ポリシーを適用します。
C. AI ワークベンチインスタンスのユーザーに AI Notebooks ランナーと AI Notebooks ビューアーのロールを割り当てます。
D. タグを使用して、対応する Google Compute Engine インスタンスへの Secure Shell アクセスを防止するファイアウォール ルールを実装します。
正解**: (**正解を表示します**)**
To ensure that Vertex AI Workbench Instances (formerly AI Platform Notebooks) are automatically updated and that users cannot modify operating system settings, it's crucial to implement organizational policies that enforce these requirements.
* disableRootAccess Organization Policy:This policy prevents users from obtaining root access on virtual machines. By enforcing this policy, you ensure that users cannot make unauthorized changes to the operating system settings, maintaining the integrity and security of the instances.
* requireAutoUpgradeSchedule Organization Policy:This policy mandates that virtual machines have an auto-upgrade schedule for their operating systems. By enforcing this policy, you ensure that instances are automatically kept up-to-date with the latest security patches and updates, reducing the risk of vulnerabilities.
Given the options:
* Option A: Enabling VM Manager helps in managing updates and configurations but does not inherently prevent users from altering OS settings.
* Option B: Enforcing the disableRootAccess and requireAutoUpgradeSchedule organization policies directly addresses both requirements: preventing unauthorized OS modifications and ensuring automatic updates.
* Option C: Assigning specific roles controls user permissions but does not enforce OS-level restrictions or automatic updates.
* Option D: Implementing firewall rules to prevent SSH access adds a layer of security but does not ensure automatic updates or prevent OS modifications through other means.
Therefore, Option B is the most effective approach, as it directly enforces the necessary policies to meet both requirements.
References:
Organization Policy Service
VM Manager Overview

質問**: 31**

あなたの組織は、CIS Google Cloud Computing Foundations Benchmark v1 3 0 (CIS Google Cloud Foundation 1 3) に対して継続的に評価されることを望んでいます。コントロールの中には組織に無関係なものもあり、評価では無視する必要があります。関連するコントロールのみが確実に評価されるように、自動化されたシステムまたはプロセスを作成する必要があります。
あなたは何をするべきか？
A. 無関係なすべてのセキュリティ検出結果をタグとセキュリティ例外を示す値でマークします。マークされた検出結果をすべて選択し、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 をアクティブにします。
B. Security Command Center (SCC) プレミアムを有効にする SCC 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) からすべての検出結果を CSV ファイルにダウンロードします。CIS Google Cloud Foundation 1 3 の一部である検出結果をファイル内でマークします。無関係で会社の範囲外のエントリは無視します。
D. 外部の監査会社に、必要な CIS ベンチマークを含む独立したレポートの提供を依頼します。監査の範囲内で、一部の管理は不要であり、無視する必要があることを明確にします。
正解: **B (**コメントを発表する**)**
Activate Security Command Center (SCC) Premium: Security Command Center (SCC) Premium provides advanced security analytics and best practice recommendations for your Google Cloud environment. It includes functionalities such as asset discovery, vulnerability scanning, and security findings.
Create a Custom Rule to Mute Irrelevant Security Findings:
Navigate to the Security Command Center (SCC) in the Google Cloud Console.
Go to the "Settings" tab and find the "Mute findings" section.
Create a new mute rule by specifying the conditions that match the irrelevant controls you want to disregard.
These conditions can be based on attributes such as resource type, finding type, and other metadata.
Apply this mute rule, which will ensure that the specified findings are not evaluated in your security posture assessments.
Ensure Continuous Compliance Monitoring:
The mute rules will automatically filter out the irrelevant findings, ensuring that only relevant controls from the CIS Google Cloud Computing Foundations Benchmark v1.3.0 are evaluated.
Regularly review and update the mute rules to adapt to any changes in your compliance requirements or security posture.
References:
Security Command Center Documentation
Creating and Managing Mute Rules

質問: **32**
セキュリティ チームは、多層防御アプローチを実装して、Cloud Storage バケットに保存されている機密データを保護したいと考えています。チームには次の要件があります。
* プロジェクト A の Cloud Storage バケットは、プロジェクト B からのみ読み取ることができます。
* プロジェクト A の Cloud Storage バケットは、ネットワークの外部からアクセスできません。
* Cloud Storage バケット内のデータを外部の Cloud Storage バケットにコピーすることはできません。
セキュリティ チームは何をすべきですか?
A. 組織のポリシーでドメイン制限共有を有効にし、Cloud Storage バケットで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、Cloud Storage API をサービス境界構成に含めます。
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。
正解: **B** (コメントを発表する)
VPC Peering is between organizations not between Projects in an organization. That is Shared VPC. In this case, both projects are in same organization so having VPC Service Controls around both projects with necessary rules should be fine.
https://cloud.google.com/vpc-service-controls/docs/overview

質問: **33**
セキュリティ チームは、ユーザーが管理するキーが誤って管理され、侵害されるリスクを軽減したいと考えています。これを実現するには、開発者が組織内のプロジェクトの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。これをどのように実施する必要がありますか？

A. サービス アカウント キーを管理するように Secret Manager を構成します。
B. 組織の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. 組織の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。
正解**: C (**コメントを発表する**)**
To prevent developers from creating user-managed service account keys and reduce the risk of key mismanagement, you should enable an organization policy that specifically prohibits the creation of these keys.
Enable an organization policy to prevent service account keys from being created (C):
Google Cloud provides the capability to enforce organizational policies that restrict various actions, including the creation of service account keys. By enabling this policy, you ensure that developers cannot create new user-managed service account keys, thus minimizing the risk of key mismanagement and potential security breaches.
References
Service Accounts documentation
Organization Policy Service documentation

質問**: 34**
あなたの組織は、サードパーティ企業の Compute Engine インスタンスで実行される金融サービス アプリケーションをホストしています。アプリケーションを使用するサードパーティ企業のサーバーも、別の Google Cloud 組織の Compute Engine 上で実行されます。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。次の要件があります。
* ネットワーク接続は暗号化する必要があります。
* サーバー間の通信は、プライベート IP アドレスを介して行う必要があります。
あなたは何をするべきか？
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との間に Cloud VPN 接続を構成します。
B. VPC ファイアウォール ルールによって制御される、組織の VPC ネットワークとサードパーティの VPC 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 インスタンスの周りに VPC Service Controls 境界を構成し、アクセス レベルを介してサードパーティへの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、サードパーティにのみアクセスを許可する TLS で暗号化される Apigee プロキシを構成します。
正解**: A (**コメントを発表する**)**
To meet the requirements of encrypted communication over private IP addresses between Compute Engine instances in different Google Cloud organizations, a Cloud VPN connection is appropriate:

Cloud VPN: Cloud VPN creates a secure, encrypted tunnel between your organization's VPC network and the third party's VPC network. This ensures that data transmitted over the network is encrypted and secure.
Private IP Communication: Cloud VPN allows communication over private IP addresses, which helps maintain security by keeping traffic within the Google Cloud network and not exposing it to the public internet.
Firewall Rules: VPC firewall rules can be configured to control the traffic that flows through the VPN, ensuring that only authorized traffic is allowed, further enhancing security.
By setting up a Cloud VPN connection, you can achieve secure, encrypted communication over private IP addresses between different Google Cloud organizations.
References
Cloud VPN Overview

質問**: 35**
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。
正解**: (**正解を表示します**)**
The core security and privacy requirement is to prevent personal data from being used in the training process, which necessitates de-identification. Cloud Data Loss Prevention (DLP), also referred to as Sensitive Data Protection (SDP), is the specific Google Cloud tool for this purpose. The secondary requirement, restricting access, is handled by IAM.
Extracts:

"Sensitive Data Protection (SDP)... De-identification enables you to transform your data to reduce data risk while retaining data utility." (Source 1.4)
"De-identification techniques like encryption, obfuscate raw sensitive identifiers in your data. These techniques let you preserve the utility of your data for joining or analytics, while reducing the risk of handling the data." (Source 1.1)
"DLP provides tools to classify and de-identify sensitive elements or unwanted content within your data...
Find and remove sensitive elements from your data before model training." (Source 1.4) IAM policies are the standard mechanism to satisfy the requirement to "restrict access to the dataset to an authorized subset of people only." Option B combines the precise technical solution for privacy (DLP De- identification) with the necessary access control (IAM).

質問**: 36**
あなたは、組織の Google Cloud 環境用に Security Command Center を構成する任務を負っています。セキュリティ チームは、組織のコンピューティング環境における仮想通貨マイニングの可能性に関するアラートと、セキュリティに影響を与える一般的な Google Cloud の構成ミスに関するアラートを受け取る必要があります。これらのアラートを構成するには、Security Command Center のどの機能を使用する必要がありますか? 2つ選んでください。）
A. イベント脅威検出
B. コンテナ脅威検出
C. セキュリティ状況分析
D. クラウド データ損失防止
E. Google クラウド アーマー
正解**: A,C (**コメントを発表する**)**
Security Command Center (SCC) in Google Cloud provides several features to help organizations detect and respond to security threats and misconfigurations.
Event Threat Detection: This feature continuously monitors and analyzes system logs to detect potential threats such as crypto mining. It uses machine learning and threat intelligence to identify suspicious activities and generate alerts.
Security Health Analytics: This feature helps identify common misconfigurations and compliance violations that could impact security. It provides visibility into security posture and helps remediate issues related to misconfigurations in your Google Cloud environment.
By using both Event Threat Detection and Security Health Analytics, you can effectively monitor for crypto mining activities and detect common misconfigurations that could compromise security.
References
Security Command Center Documentation
Event Threat Detection
Security Health Analytics

質問**: 37**
脆弱性に対するパッチがリリースされ、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 チームはこれをどのように達成する必要がありますか?
A. Puppet または Chef を使用して、実行中のコンテナー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。その場合、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、新しいイメージをビルドして再デプロイします。
D. Container Registry で基本イメージが使用可能になったときにコンテナーを自動的にアップグレードするように構成します。
正解**: (**正解を表示します**)**
When a vulnerability patch is released for a running container in Google Kubernetes Engine (GKE), the recommended approach is to update the application code or apply the patch directly to the codebase. Then, a new container image should be built incorporating these changes. After building the new image, it should be deployed to replace the running containers. This method ensures that the containers run the updated, secure code.
Steps:
Update Application Code: Modify the application code or dependencies to incorporate the vulnerability patch.
Build New Image: Use a tool like Docker to build a new container image with the updated code.
Push New Image: Push the new container image to the Container Registry.
Update Deployments: Update the Kubernetes deployment to use the new image. This can be done by modifying the image tag in the deployment YAML file.
Redeploy Containers: Apply the updated deployment configuration using kubectl apply -f <deployment-file>.
yaml, which will redeploy the containers with the new image.
References:
Google Cloud: Container security
Kubernetes: Updating an application

質問**: 38**
あなたの組織は機密性の高い健康情報を処理しています。仮想マシン (VM) による使用中にデータが確実に暗号化されるようにしたいと考えています。組織全体に適用されるポリシーを作成する必要があります。
あなたは何をするべきか？
A. 組織全体で作成されたすべての VM リソースが顧客管理の暗号化キー (CMEK) 保護を使用することを保証する組織ポリシーを実装します。

B. 組織全体で作成されるすべての 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 リソースがクラウド外部キー マネージャー (EKM) 保護を使用することを保証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。
正解**: (**正解を表示します**)**
To ensure that data is encrypted while in use by the virtual machines (VMs) and enforce this policy across your organization, you should use Confidential VM instances. Here are the steps:
Enable Confidential VM:
Ensure that Confidential VMs are available in your selected regions and enabled for your project.
Set Organization Policy:
Implement an organization policy to enforce the use of Confidential VM instances for all VMs across your organization.
Use the Google Cloud Console or the gcloud command-line tool to set this policy. Example command:
gcloud resource-manager org-policies set-policy my_policy.yaml
Example my_policy.yaml:
name: organizations/1234567890/policies/compute.requireConfidentialCompute spec: rules: - enforce: true Verify and Monitor:
Ensure that all newly created VMs across your organization are Confidential VMs.
Regularly monitor compliance through the Google Cloud Console and set up alerts if non-compliant VMs are created.
Benefits:
Data Encryption in Use: Confidential VMs ensure that data is encrypted not just at rest and in transit but also while in use.
Policy Enforcement: Organization policies provide a way to enforce security configurations across all projects under your organization.
References
Confidential Computing Documentation
Creating and Managing Organization Policies

質問**: 39**
あなたの会社では、Google Cloud 上に 3 層ウェブ アプリケーション(ウェブ、アプリケーション、データベース)をデプロイしています。
攻撃対象領域を最小限に抑えるには、層間のネットワーク分離を構成する必要があります。Web層はパブリックインターネットからアクセス可能で、アプリケーション層はWeb層からのみアクセス可能、データベース層はアプリケーション層からのみアクセス可能である

必要があります。ソリューションはGoogleが推奨するプラクティスに従う必要があります。どうすればよいでしょうか？
A. 各層に1つずつ、3つの独立したVPCネットワークを作成します。ウェブVPCとアプリケーションVPC間、およびアプリケーションVPCとデータベースVPC間にVPCネットワークピアリングを設定します。ファイアウォールルールを使用してトラフィックを制御します。
B. すべての層に単一のサブネットを作成します。同じサブネット内のインスタンス間のすべてのトラフィックを許可するファイアウォールルールを作成します。アプリケーションレベルのセキュリティを使用して、不正アクセスを防止します。
C. VPC 内に各層に 1 つずつ、合計 3 つのサブネットを作成します。各サブネットの特定のポートへのトラフィックを許可するファイアウォール ルールを作成します。ファイアウォール ルールを適用するには、VM のネットワーク タグまたはサービス アカウントを使用します。
D. VPC 内に各層に 1 つずつ、合計 3 つのサブネットを作成します。各サブネットでプライベート Google アクセスを有効にします。サブネット間のすべてのトラフィックを許可するファイアウォール ルールを 1 つ作成します。
正解**: (**正解を表示します**)**
In Google Cloud, the best practice for micro-segmentation and tier isolation is to use a single VPC with multiple subnets and apply firewall rules using Service Accounts or Network Tags. Using Service Accounts is generally preferred over tags because they are identity-based and more secure.
According to the Google Cloud Security Foundations Guide:
"Segment your VPC networks into subnets to provide logical isolation. Use firewall rules to control traffic between tiers. Instead of relying on IP addresses, use service accounts to define source and destination for firewall rules. This ensures that even if an IP changes, the security policy remains enforced based on the identity of the workload." Implementation Details:
* Web Tier: Use a firewall rule allowing 0.0.0.0/0 (Internet) to the Service Account associated with the web VMs on port 80/443.
* App Tier: Use a firewall rule allowing traffic ONLY from the Web Tier Service Account to the App Tier Service Account.
* DB Tier: Use a firewall rule allowing traffic ONLY from the App Tier Service Account to the DB Tier Service Account.
Reference:
Google Cloud Documentation: "Best practices for VPC design - Use service accounts to restrict traffic" (https://cloud.google.com/vpc/docs/using-firewalls#service-account-vs-tag).
Professional Cloud Security Engineer Study Guide: Section on "Configuring Network Security - Micro- segmentation."

質問**: 40**

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 2 つあります。
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。
正解**: D (**コメントを発表する**)**
To ensure least-privilege access and provide necessary permissions to the DevOps team only during a deployment issue, follow these steps:
Create a Service Account:
In your Google Cloud project, create a new service account specifically for the DevOps team.
Assign Limited Permissions:
Grant the service account permissions with only the necessary list/view roles. For instance, you can create a custom IAM role with compute.instances.list and compute.instances.get permissions.
Grant Service Account User Role:
Assign the Service Account User role to the DevOps team members for the created service account. This allows them to act as the service account and use its permissions.
Access Control During Incidents:
During a deployment issue, the DevOps team can temporarily use the service account to access the resources.
This ensures they have the least-privilege access required to investigate and resolve the issue.
Automation and Monitoring:
Implement automation to enable and disable the service account access as needed and monitor the usage to ensure compliance with the least-privilege principle.
Benefits:
Security: Limits access to only what is necessary, reducing the risk of unauthorized changes.
Flexibility: Provides necessary access during incidents without granting permanent elevated permissions.

References
Creating and Managing Service Accounts
Service Account User Role

質問: **41**
組織の一般的なネットワークとセキュリティのレビューは、アプリケーションの通過経路、要求処理、およびファイアウォール ルールの分析で構成されます。彼らは、開発者チームがこの完全なレビューのオーバーヘッドなしで新しいアプリケーションを展開できるようにしたいと考えています。
この組織にどのようにアドバイスする必要がありますか?
A. Forseti とファイアウォール フィルターを使用して、本番環境で不要な構成をキャッチします。
B. コードとしてのインフラストラクチャの使用を義務付け、ポリシーを適用するために CI/CD パイプラインで静的分析を提供します。
C. すべての VPC トラフィックをお客様が管理するルーター経由でルーティングして、本番環境で悪意のあるパターンを検出します。
D. すべての運用アプリケーションはオンプレミスで実行されます。開発者が GCP を開発および QA プラットフォームとして自由に使用できるようにします。
正解: **(正解を表示します)**
To enable developer teams to deploy new applications without the extensive overhead of network and security reviews, it's recommended to mandate the use of infrastructure as code (IaC) and enforce policies through static analysis in CI/CD pipelines. This approach ensures that security and compliance policies are checked automatically during the development process.
Step-by-Step:
* Adopt IaC: Use tools like Terraform or Google Cloud Deployment Manager to manage infrastructure as code.
* CI/CD Pipeline Integration: Integrate static analysis tools such as TFLint or Checkov in the CI/CD pipeline to enforce security policies.
* Policy Definition: Define security policies and best practices that need to be adhered to in the code.
* Automated Checks: Configure automated checks in the CI/CD pipeline to review code against these policies before deployment.
* Monitor and Audit: Continuously monitor and audit deployed applications to ensure ongoing compliance.
Infrastructure as Code on Google Cloud
Static Analysis for Terraform
Checkov for IaC

質問: **42**

組織が受信するフィッシング メールの数が増加しています。
この状況で従業員の資格情報を保護するには、どの方法を使用する必要がありますか?
A. 多要素認証
B. 厳格なパスワード ポリシー
C. ログインページのキャプチャ
D. 暗号化されたメール
正解**: (**正解を表示します**)**
https://cloud.google.com/blog/products/g-suite/7-ways-admins-can-help-secure-accounts-against-phishing-g- suite
https://www.duocircle.com/content/email-security-services/email-security-in-cryptography#:~:text=Customer%20Login-,Email%20Security%20In%20Cryptography%20Is%20One%20Of%20The%20Most,Measures%20To%20Prevent%20Phishing%20Attempts&text=Cybercriminals%20love%20emails%20the%20most,networks%20all%20over%20the%20world.

質問**: 43**
あなたの組織は新しいワークロードを取得しました。ウェブ サーバーとアプリケーション (アプリ) サーバーは、新しく作成されたカスタム VPC 内の Compute Engine で実行されます。次の要件を満たす安全なネットワーク通信ソリューションを構成する責任があります。
Web 層とアプリケーション層の間の通信のみを許可します。
Web 層とアプリ層を自動スケーリングする際に、一貫したネットワーク セキュリティを適用します。
Compute Engine インスタンス管理者がネットワーク トラフィックを変更できないようにします。
あなたは何をするべきか？
A. 1. 実行中のすべての Web サーバーとアプリケーション サーバーをそれぞれのネットワーク タグで構成します。
2. それぞれのネットワーク タグでターゲット/ソースを指定する VPC ファイアウォール ルールを許可するを作成します。
B. 1. 実行中のすべての Web サーバーとアプリケーション サーバーをそれぞれのサービス アカウントで構成します。
2. それぞれのサービス アカウントでターゲット/ソースを指定する許可 VPC ファイアウォール ルールを作成します。
C. 1. それぞれのネットワーク タグで構成されたインスタンス テンプレートを使用して、Web サーバーとアプリ サーバーを再展開します。
2. それぞれのネットワーク タグでターゲット/ソースを指定する VPC ファイアウォール ルールを許可するを作成します。
D. 1. それぞれのサービス アカウントで構成されたインスタンス テンプレートを使用して、Web サーバーとアプリ サーバーを再展開します。

2. それぞれのサービス アカウントでターゲット/ソースを指定する許可 VPC ファイアウォール ルールを作成します。
正解: (正解を表示します)
https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags
https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags
A service account represents an identity associated with an instance. Only one service account can be associated with an instance. You control access to the service account by controlling the grant of the Service Account User role for other IAM principals. For an IAM principal to start an instance by using a service account, that principal must have the Service Account User role to at least use that service account and appropriate permissions to create instances (for example, having the Compute Engine Instance Admin role to the project).

質問: **44**
あなたは会社のセキュリティ管理者として、Google Cloud におけるアクセス制御（識別 認証、認可）の管理を担当しています。認証と認可を構成する際に従うべき Google 推奨のベスト プラクティスはどれですか 2 つ選択してください）。
A. Google のデフォルトの暗号化を使用します。
B. ユーザーを Google Cloud に手動で追加します。
C. Google の Identity and Access Management (1AM) サービスを使用して、ユーザーに基本ロールをプロビジョニングします。
D. ユーザー認証とユーザー ライフサイクル管理には、Cloud Identity との SSO/SAML 統合を使用します。
E. 事前定義されたロールを使用してきめ細かなアクセスを提供します。
正解: (正解を表示します)
* SSO/SAML Integration: Implement SSO (Single Sign-On) with SAML integration through Cloud Identity to streamline user authentication and lifecycle management. This ensures centralized management of user identities and access.
* Predefined Roles: Use predefined roles to provide granular access control. These roles are designed to follow the principle of least privilege, ensuring that users have the minimum necessary permissions to perform their tasks.
* User Management: By leveraging SSO/SAML, user provisioning and de-provisioning become more efficient and secure. This integration helps maintain consistent access policies across your organization.
* Access Control: Predefined roles reduce the risk of over-permission by offering well-defined access levels, enhancing security and compliance. References:
* Google Cloud - SSO with SAML
* Google Cloud - IAM Best Practices

質問: **45**

エンタープライズ 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る必要がありますか?
A. Titan セキュリティ キー
B. Google プロンプト
C. Google 認証アプリ
D. クラウド HSM キー
正解**: (**正解を表示します**)**
Titan Security Keys are a physical form of two-step verification (2SV) that provide the highest level of account security by using cryptographic signatures to verify the user and the URL of the login page.
Cryptographic Security: Titan Security Keys use a hardware-based cryptographic method to authenticate users, which is resistant to phishing attacks. This ensures that the authentication process is secure and not susceptible to being intercepted or spoofed.
URL Verification: Titan Security Keys verify the URL of the login page during the authentication process, providing an additional layer of security against phishing attempts that may try to redirect users to malicious websites.
Ease of Use: These keys are easy to use and integrate with Google's 2SV process, providing a seamless and highly secure authentication method for users.
References
Titan Security Keys

質問**: 46**
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用いて既知の脆弱性がないか確認します。GrafeasとKritisを使用することで、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できます。
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て、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。
正解**: D (**コメントを発表する**)**

To secure a container supply chain, you need two things: Visibility (Scanning) and Enforcement (Policy).
Google Cloud provides Artifact Analysis (integrated with Artifact Registry) and Binary Authorization to solve this.
According to Google Cloud Documentation (Software Supply Chain Security):
"To secure your supply chain, use Artifact Registry with automatic vulnerability scanning to identify risks in your images. Then, use Binary Authorization to define a policy that requires images to be signed by trusted authorities (attestors) before they can be deployed to GKE or Cloud Run. This ensures that only images that have passed your security checks (like vulnerability scans) are allowed to run." How it works:
* Scanning: Every time an image is pushed to Artifact Registry, it is automatically scanned for CVEs.
* Attestation: A successful scan (e.g., no 'Critical' vulnerabilities) triggers a CI/CD step to "Sign" the image (create an attestation).
* Enforcement: The GKE admission controller (Binary Authorization) checks for this signature. If it's missing or invalid, the deployment is blocked.
Why other options are incorrect:
* A is incorrect: Container Threat Detection is for runtime (after it's already running). Supply chain security is about pre-deployment prevention.
* B is incorrect: While Grafeas/Kritis are the open-source foundations, Option D represents the managed Google Cloud services which "minimize management overhead."
* C is incorrect: Firewalls inspect network traffic, not the integrity or vulnerability status of the container image itself.
Reference:
Google Cloud Documentation: "Binary Authorization overview" (https://cloud.google.com/binary- authorization/docs/overview).
Google Cloud Documentation: "Vulnerability scanning in Artifact Registry" (https://cloud.google.com /artifact-registry/docs/analysis).

質問: **47**
あなたは金融会社のセキュリティエンジニアです。あなたの組織は Google Cloud にデータを保存することを計画していますが、経営陣は機密性の高いデータのセキュリティについて懸念しています。具体的には、あなたの会社は、Google の内部従業員が Google Cloud 上の会社のデータにアクセスする能力について懸念しています。どのようなソリューションを提案する必要がありますか?
A. 顧客管理の暗号化キーを使用します。
B. Google の Identity and Access Management (IAM) サービスを使用して、Google Cloud でアクセス制御を管理します。
C. 管理アクティビティ ログを有効にして、リソースへのアクセスを監視します。
D. Google 従業員のアクセス承認リクエストでアクセスの透明性ログを有効にします。
正解: **(**正解を表示します**)**
https://cloud.google.com/access-transparency Access approval Explicitly approve access to your data or configurations on Google Cloud. Access Approval requests, when combined with Access Transparency logs, can be used to audit an end-to-end chain from support ticket to access request to approval, to eventual access.

質問: **48**
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. 特定の外部ウェブ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を設定し、ウェブ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 パターンをチェックし、攻撃パターンを検出して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
正解: **(**正解を表示します**)**
The problem states that Google Cloud applications need to access external web services and requires the ability to monitor, control, and log this access.
Monitoring, Controlling, and Logging external web access: This specifically points to a proxy solution, which can intercept, inspect, and log HTTP/S traffic.
Secure Web Proxy (SWP): Google Cloud's Secure Web Proxy is designed for exactly this use case. It acts as an explicit forward proxy for HTTP(S) traffic, allowing organizations to implement granular access controls, inspect traffic for security threats, and log all outbound web requests from their Google Cloud environment.
Extract Reference: "Secure Web Proxy is a managed service that lets you deploy and manage an explicit forward proxy to protect your organization's internal resources from web-based threats and to control access to external web applications." and "With Secure Web

Proxy, you can: Enforce granular access policies based on different attributes, Log all HTTP(S) requests that are handled by the proxy, and Monitor web traffic for threats." (Google Cloud documentation: https://cloud.google.com/secure-web-proxy) Let's evaluate the other options:
A). Configure VPC firewall rules to allow the services to access the IP addresses of required external web services: VPC firewall rules operate at Layer 4 (TCP/UDP) and Layer 3 (IP). While they can allow or deny traffic to specific IP addresses and ports, they cannot monitor, control, or log HTTP/S requests at the application layer. They don't provide granular control over which web services are accessed or inspect the content of the requests.
C). Configure Google Cloud Armor to monitor and protect your applications by checking incoming traffic patterns for attack patterns: Google Cloud Armor is primarily a Distributed Denial of Service (DDoS) protection and Web Application Firewall (WAF) service. It focuses on protecting applications from incoming threats (ingress traffic), not controlling and logging outgoing access to external web services.
D). Set up a Cloud NAT instance to allow egress traffic from your VPC: Cloud NAT allows instances without external IP addresses to connect to the internet. While it enables egress, it does not provide monitoring, control, or logging capabilities for specific web services at the application layer. It's a network address translation service, not an application-layer proxy.
Therefore, setting up a Secure Web Proxy is the most appropriate solution to meet the requirements of monitoring, controlling, and logging access to external web services from Google Cloud applications.

質問**: 49**
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。これらの画像は、専用のプロジェクトに保存されます。
あなたは何をするべきか？
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、信頼できる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。信頼できるプロジェクトを拒否操作の例外としてリストします。
C. Resource Manager で、信頼済みプロジェクトのプロジェクト パーミッションを編集します。Compute Image User というロールを持つメンバーとして組織を追加します。
D. Resource Manager で、組織のアクセス許可を編集します。役割を持つメンバーとしてプロジェクト ID を追加します: Compute Image User。
正解**: A (**コメントを発表する**)**
Objective: You want to limit the images that can be used as the source for boot disks to a set of images stored in a dedicated project.
Solution: Use the Organization Policy Service.
Steps:
Step 1: Open the Google Cloud Console.

Step 2: Navigate to the Organization Policies page.
Step 3: Create a new policy by clicking on "Create Policy".
Step 4: Select the constraint compute.trustedimageProjects.
Step 5: Set the policy to ALLOW and specify the project ID where the trusted images are stored in the whitelist.
Step 6: Save and apply the policy.
By creating a compute.trustedimageProjects constraint at the organization level and specifying the trusted project in the allow list, you ensure that only images from this project can be used for boot disks across the organization.
References:
GCP Organization Policy Service Documentation
Compute Trusted Image Projects Constraint

質問**: 50**
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る必要がありますか?
A. バケットのアクセス制御モデルを変更します
B. 正しいバケットの宛先でシンクを更新します。
C. roles/logging.logWriter Identity and Access Management (IAM) ロールをログ シンク ID のバケットに追加します。
D. roles/logging.bucketWriter Identity and Access Management (IAM) ロールをログ シンク ID のバケットに追加します。
正解**: (**正解を表示します**)**
https://cloud.google.com/logging/docs/export/troubleshoot#errors_exporting_to_cloud_storage
https://cloud.google.com/logging/docs/export/troubleshoot
Unable to grant correct permissions to the destination: Even if the sink was successfully created with the correct service account permissions, this error message displays if the access control model for the Cloud Storage bucket was set to uniform access when the bucket was created. For existing Cloud Storage buckets, you can change the access control model for the first 90 days after bucket creation by using the Permissions tab. For new buckets, select the Fine-grained access control model during bucket creation. For details, see Creating Cloud Storage buckets.

質問**: 51**
顧客は、クラウド コンピューティングの伸縮自在な性質を利用するアプリケーションを Compute Engine にデプロイしました。
インフラストラクチャ オペレーション エンジニアとどのように連携して、Windows Compute Engine VM がすべての最新 OS パッチで最新の状態であることを確認するにはどうすればよいですか?

A. パッチが利用可能になったら新しい基本イメージを構築し、CI/CD パイプラインを使用して VM を再構築し、段階的に展開します。
B. ドメイン コントローラを Compute Engine にフェデレートし、グループ ポリシー オブジェクトを介して毎週パッチをロールアウトします。
C. Deployment Manager を使用して、更新された VM を新しいインスタンス グループ (IG) にプロビジョニングします。
D. 毎週のメンテナンス期間中にすべての VM を再起動し、スタートアップ スクリプトがインターネットから最新のパッチをダウンロードできるようにします。
正解: **(**正解を表示します**)**
Compute Engine doesn't automatically update the OS or the software on your deployed instances. You will need to patch or update your deployed Compute Engine instances when necessary. However, in the cloud it is not recommended that you patch or update individual running instances. Instead it is best to patch the image that was used to launch the instance and then replace each affected instance with a new copy.

質問: **52**
組織のセキュリティ オペレーション センター (SOC) を管理します。現在、ネットワーク ログに基づいて、VPC のネットワーク トラフィックの異常を監視および検出しています。ただし、ネットワーク ペイロードとヘッダーを使用して環境を調査する必要があります。どの Google Cloud プロダクトを使用する必要がありますか?
A. クラウド IDS
B. VPC Service Controls のログ
C. VPC フロー ログ
D. Google クラウド アーマー
E. パケット ミラーリング
正解: **(**正解を表示します**)**
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

質問: **53**
大規模な組織で勤務しており、最近、Google Cloud とオンプレミスのエッジルーター間に 100GB の Cloud Interconnect 接続を導入しました。定期的に接続を確認していたところ、接続は正常に動作しているものの、MACsec が動作停止していることを示すエラーメッセージが表示されていることに気付きました。このエラーを解決する必要があります。どうすればよいでしょうか？
A. MACsec 用に作成されたアクティブな事前共有キーが、オンプレミスと Google エッジルーターの両方で期限切れになっていないことを確認します。

B. アクティブな事前共有キーがオンプレミスと Google エッジルーターの両方で一致していることを確認します。
C. Cloud Interconnect 接続が MACsec をサポートしていることを確認します。
D. オンプレミスのルーターがダウンしていないことを確認します。
正解**: B (**コメントを発表する**)**
MACsec (Media Access Control Security) relies on a shared secret (a pre-shared key, made up of a Connectivity Key Name, CKN, and Connectivity Association Key, CAK) to establish a secure session between the two endpoints. If the session is "operationally down," it indicates a cryptographic mismatch.
Extracts:
"MACsec is operationally down on my Cloud Interconnect connection... The issue could be caused by one of the following: The active keys on your on-premises router and Google's edge routers don't match." (Source
3.1)
The troubleshooting guide further specifies checking that the "active CKN, CAK, and start times on your on- premises router match the values that MACsec for Cloud Interconnect displays." (Source 3.1) Therefore, the primary and most common step to resolve a "MACsec is operationally down" status is to verify that the cryptographic keys (the pre-shared key) are correctly configured and match on both the on-premises and Google Cloud routers.

質問**: 54**
マネージャーは、コストを最小限に抑えながら、2 年間のセキュリティ イベント ログの保持を開始したいと考えています。適切なログ エントリを選択するフィルタを記述します。
ログはどこにエクスポートする必要がありますか?
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
正解**: B (**コメントを発表する**)**
To retain security event logs for 2 years while minimizing costs, exporting the logs to Cloud Storage buckets is the most cost-effective solution. Cloud Storage provides scalable and durable storage at a lower cost compared to BigQuery, which is more suited for analytics and querying, or Cloud Pub/Sub, which is designed for messaging and stream processing.
Steps:
Create a Cloud Storage Bucket: Set up a new Cloud Storage bucket configured with appropriate retention policies.
Set Up Log Export: Use the Google Cloud Console or gcloud command-line tool to create a sink that exports the selected log entries to the Cloud Storage bucket.
Configure Retention Policy: Set the retention policy on the Cloud Storage bucket to ensure that logs are retained for the required period of 2 years.

References:
Google Cloud: Exporting logs
Google Cloud Storage pricing

質問: **55**
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のプロジェクト レベルで Identity and Access Management (IAM) ロールを使用します。
ストレージ チームに、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付与します。
正解: **(**正解を表示します**)**
The key requirement is restricting access based on the client device (i.e., "corporate computers"). Context- Aware Access (CAA) is the specific Google Cloud tool designed to enforce access based on contextual factors, including the device security status or IP address.
Context Restriction: Context-Aware Access allows you to define an Access Level based on attributes like device policy compliance, operating system, or IP address range-this addresses the "corporate computers" requirement.
Isolation and Control: The Access Level is then enforced via an Organization Policy applied at the Project Level (or the folder/organization level), which fulfills the requirement to isolate access to Cloud Storage for this project and restrict the access to specific resources (Cloud Storage).
VPC Service Controls (VPC SC) (Option B) are great for isolating projects and preventing data exfiltration, but its primary access restriction mechanisms are based on IP range, not fine-grained device security posture and user identity together, making CAA the more precise tool for device-specific enforcement. Also, applying VPC SC ingress/egress based on IP addresses for end-user access can be complex and less flexible than CAA.

IAM (Option D) only controls who (identity) can access a resource, not where or how (context) they are accessing it from.
Extracts:
"Context-Aware Access (CAA) integrates with Google Workspace or Cloud Identity to enforce granular access to Google Cloud resources based on a user's context, such as their location, device security status, and IP address." (Source 7.1)
"To enforce CAA for Google Cloud resources like Cloud Storage, you create an Access Level that defines the required context (e.g., only corporate-managed devices) and apply it via an Organization Policy constraint (e.
g., iam.allowedServices) at the project level." (Source 7.2)
"CAA allows you to restrict access based on the device security posture, a key requirement for enforcing
'corporate computer' access." (Source 7.3)

質問: **56**
組織のセキュリティ オペレーション センター (SOC) を管理します。現在、パケット ヘッダー情報に基づいて、Google Cloud VPC のネットワーク トラフィックの異常をモニタリングおよび検出しています。ただし、調査を支援するために、ネットワーク フローとそのペイロードを調査する機能が必要です。どの Google Cloud プロダクトを使用する必要がありますか?
A. マーケットプレイス IDS
B. VPC フロー ログ
C. VPC Service Controls のログ
D. パケット ミラーリング
E. Google Cloud Armor ディープ パケット インスペクション
正解: **D (**コメントを発表する**)**
Reference: https://aws.amazon.com/blogs/aws/new-vpc-traffic-mirroring/
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers. https://cloud.google.com/vpc/docs/packet-mirroring

質問: **57**
顧客がアプリケーションを App Engine にデプロイし、Open Web Application Security Project (OWASP) の脆弱性を確認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る必要がありますか?
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. Forseti セキュリティ
正解: **(**正解を表示します**)**

Reference: https://cloud.google.com/security-scanner/
Web Security Scanner supports categories in the OWASP Top Ten, a document that ranks and provides remediation guidance for the top 10 most critical web application security risks, as determined by the Open Web Application Security Project (OWASP).
https://cloud.google.com/security-command-center/docs
/concepts-web-security-scanner-overview#detectors_and_compliance

質問: **58**
データベース管理者は、Cloud SQL インスタンス内での悪意のあるアクティビティに気付きました。データベース管理者は、リソースの構成またはメタデータを読み取る API 呼び出しを監視したいと考えています。データベース管理者はどのログを確認する必要がありますか?
A. 管理者の活動
B. システムイベント
C. アクセスの透明性
D. データアクセス
正解: **A** (コメントを発表する)
Review Admin Activity logs:
Admin Activity logs contain entries for API calls that modify or read the configuration or metadata of resources.
These logs are useful for monitoring and auditing administrative actions, including those that could indicate malicious activity on a Cloud SQL instance.
References:
Audit Logs: Admin Activity

質問: **59**
顧客は、攻撃者がドメイン/IP をハイジャックし、中間者攻撃によってユーザーを悪意のあるサイトにリダイレクトするのを防ぐ必要があります。
このお客様はどのソリューションを使用する必要がありますか?
A. VPC フロー ログ
B. クラウドアーマー
C. DNS セキュリティ拡張機能
D. Cloud Identity-Aware Proxy
正解: **C** (コメントを発表する)
DNSSEC - use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof. Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block

of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites. https://cloud.google.com/blog /products/gcp/dnssec-now-available-in-cloud-dns

質問: **60**
VPC ネットワークで定義されている暗黙のファイアウォール ルールを 2 つ選択してください。2つ選んでください。）
A. すべてのアウトバウンド接続を許可するルール
B. すべてのインバウンド接続を拒否するルール
C. すべての受信ポート 25 接続をブロックするルール
D. すべてのアウトバウンド接続をブロックするルール
E. すべての受信ポート 80 接続を許可するルール
正解: **(**正解を表示します**)**
Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them.
https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules

質問: **61**
ユーザーに代わってユーザーの Google ドライブにアクセスする必要がある内部 App Engine アプリケーションを作成しています。あなたの会社は、現在のユーザーの資格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。
あなたは何をするべきか？
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 ユーザーの役割を与えます。
C. 専用の G Suite 管理者アカウントを使用し、これらの G Suite 資格情報で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、それに 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れを使用して、ユーザーを偽装します。
正解: **D (**コメントを発表する**)**

To access a user's Google Drive on their behalf without relying on the user's credentials and following Google- recommended practices, you should use a service account with domain-wide delegation.
* Create a Service Account:
* Go to the Cloud Console, navigate to IAM & Admin > Service Accounts.
* Click "Create Service Account" and provide necessary details.
* Grant Domain-Wide Delegation:
* Edit the service account to enable "G Suite Domain-wide Delegation".
* Download the JSON key file.
* Configure API Access in G Suite:
* Go to the Google Admin Console.
* Navigate to Security > API Controls > Domain-wide Delegation.
* Add a new API client and use the client ID from the service account.
* Authorize the necessary API scopes (e.g., https://www.googleapis.com/auth/drive).
* Implement in Application:
* Use the Google API Client Library for the desired language.
* Load the service account credentials and perform user impersonation to access Google Drive.
Domain-wide Delegation of Authority
Using OAuth 2.0 for Server to Server Applications

質問: **62**
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。
正解: **(**正解を表示します**)**
* Use Cloud External Key Management (EKM) that integrates with an external Hardware Security Module (HSM) system from supported vendors: Cloud EKM allows you to use encryption keys that are managed externally to Google Cloud. This means you can generate and store your keys in an on- premises HSM or another supported external HSM service, and integrate these keys with various Google Cloud services.
* Integration with Google Services: Cloud EKM integrates seamlessly with many Google Cloud services, including BigQuery, Cloud Storage, Compute Engine, and more. This provides you with full control over your encryption keys while still taking advantage of Google Cloud's powerful services.
References
* Cloud External Key Management (EKM) documentation
* External Key Management overview

質問: **63**
社内のネットワークエンジニアと協力し、BigQuery ベースの大規模なデータ分析アプリケーションの拡張に取り組んでいます。現在、このアプリケーションのデータはすべて、オンプレミスのアプリケーションから 20Gbps の Dedicated Interconnect 接続経由で取り込まれています。Microsoft Azure 上にデータ ソースをオンボードする必要があり、毎日約 250TB のデータを取り込む必要があります。データが安全かつ効率的に転送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. Microsoft Azure と Google Cloud 間のクロスクラウド相互接続を確立します。
データを転送するには、この接続を介してネットワーク ルートを構成します。
B. ソースアプリケーションが実行されているMicrosoft Azureサブスクリプションとの VPN 接続を確立します。VPN接続を介してデータを転送します。
C. オンプレミス ネットワーク経由で既存の Dedicated Interconnect 接続を使用し、Microsoft Azure への接続を確立します。
D. Google Cloud プロジェクトの VM 上で動作するパブリック IP アドレスを持つ SFTP サーバーを設定します。Microsoft Azure からこのサーバーに接続します。
正解: **A (**コメントを発表する**)**
For massive daily data transfers (250 TB) between cloud providers, traditional VPNs or routing through on- premises "hairpinning" are inefficient and costly. Cross-Cloud

Interconnect is the architecturally correct solution for high-bandwidth, low-latency, and secure cloud-to-cloud connectivity.
According to Google Cloud Documentation (Cross-Cloud Interconnect Overview): "Cross-Cloud Interconnect helps you establish high-bandwidth dedicated connectivity between Google Cloud and another cloud service provider (CSP) such as Microsoft Azure... It simplifies multi-cloud setup by providing a direct physical connection between Google's network and the other CSP's network." Calculation of Requirement:
* Data Volume: 250 TB per day.
* Time: 86,400 seconds (1 day).
* Required Bandwidth: $250 \times 10^{12} \text{ bytes} \times 8 \text{ bits/byte} / 86,400 \text{ seconds} \approx 23.1 \text{ Gbps}$.
* A standard VPN (Option B) typically caps out at 3 Gbps per tunnel, making it insufficient.
* The existing 20Gbps Interconnect (Option C) is already used for on-premises data and would be overwhelmed by an additional 23.1 Gbps requirement, not to mention the latency of routing Azure traffic through an on-premises data center.
Why other options are incorrect:
* B is incorrect: VPN throughput is insufficient for 250 TB/day and lacks the reliability of a dedicated circuit.
* C is incorrect: Routing through on-premises (hairpinning) introduces unnecessary latency and would exceed the 20Gbps capacity of the existing Interconnect.
* D is incorrect: SFTP over the public internet is neither efficient for petabyte-scale data nor as secure as a private interconnect.
Reference: * Google Cloud Documentation: "Cross-Cloud Interconnect overview" (https://cloud.google.com /network-connectivity/docs/interconnect/concepts/cross-cloud-overview).

質問**: 64**
あなたは、Identity and Access Management (IAM) 管理者として所有および管理するプロジェクトで実行される、規制されたワークロードのプロジェクト オーナーです。今後の監査のために、アクセス レビューの証拠を提供する必要があります。
どのツールを使用する必要がありますか?
A. ポリシーに関するトラブルシューティング
B. ポリシー アナライザー
C. IAM レコメンダー
D. ポリシー シミュレーター
正解**: (**正解を表示します**)**
Objective: Provide evidence of access reviews for an upcoming audit.
Solution: Use Policy Analyzer to review and report on IAM policies.
Steps:
Step 1: Open the Google Cloud Console.
Step 2: Navigate to the Policy Analyzer tool.

Step 3: Select the project for which you need to review access policies.
Step 4: Use the tool to generate reports on IAM roles and permissions.
Step 5: Export the reports as evidence for the audit.
Policy Analyzer provides detailed insights into IAM policies, helping you to review access configurations and generate necessary reports for compliance and auditing purposes.
References:
Policy Analyzer Documentation

質問**: 65**
組織では、Compute Engine VM 上で実行されるすべてのワークロードを保護し、インスタンスがブートレベルまたはカーネルレベルのマルウェアによって侵害されていないことを保証したいと考えています。また、ハードウェアベースのソリューションを使用して、VM で使用されているデータが基盤となるホストシステムによって読み取られ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. * 1 セキュアブート仮想トラステッドプラットフォームモジュール（vTPM）と整合性モニタリングを含むGoogle Shielded VMを使用する
* 2 VM設定をチェックし、指標を生成し、定期的に関数を実行するためのCloud Run関数を作成する
B. * 1 セキュリティコマンドセンター（SCCプレミアム）で仮想マシン脅威検出を有効にする
* 2 SCCで調査結果を監視する
C. * 1 セキュアブート仮想トラステッドプラットフォームモジュール（vTPM）と整合性モニタリングを含むGoogle Shielded VMを使用する
* 2 機密コンピューティングを有効にする
* 3 組織のポリシーを使用してこれらのアクションを実施する
D. * 1 Google Cloud Marketplace の安全に強化されたイメージを使用する
* 2 イメージを展開する際に、機密コンピューティングオプションを有効にします
* 3 組織のポリシーを使用して、正しい画像と機密コンピューティングの使用を強制する
正解**: (**正解を表示します**)**
Use Google Shielded VM including secure boot Virtual Trusted Platform Module (vTPM) and integrity monitoring: Shielded VMs provide verifiable integrity of the VM by ensuring that it was not tampered with or compromised at the boot level. They use features like Secure Boot, vTPM, and integrity monitoring to detect and prevent malicious changes to the VM's operating system and firmware.
Activate Confidential Computing: Confidential Computing provides a secure environment for processing sensitive data. It uses hardware-based enclaves to protect data in use by ensuring it cannot be accessed by the underlying host or any other unauthorized entity. By leveraging Intel SGX or AMD SEV, it ensures that data remains encrypted even when it is being processed.

Enforce these actions by using organization policies: Organization policies can enforce the use of Shielded VMs and Confidential Computing across your organization. This ensures that all VMs comply with these security measures without requiring manual configuration for each VM.
References
Shielded VMs documentation
Confidential Computing documentation
Organization Policies documentation

質問: **66**
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 外部キー マネージャーを構成して、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。
正解: **(**正解を表示します**)**
https://cloud.google.com/confidential-computing/confidential-vm/docs/creating-cvm-instance#considerations Confidential VM does not support live migration. You can only enable Confidential Computing on a VM when you first create the instance.
https://cloud.google.com/confidential-computing/confidential-vm/docs /creating-cvm-instance

質問: **67**

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を設定します。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。

正解**: D (**コメントを発表する**)**

Workforce Identity Federation is the modern, Google-recommended way to grant external partners access to Google Cloud resources using their own identity provider (IdP). This avoids the "Identity Lifecycle Management" burden of creating guest accounts in your own directory.

According to Google Cloud Documentation (Workforce Identity Federation Overview): "Workforce Identity Federation lets you use an external identity provider (IdP) to authenticate and authorize a workforce-a group of users, such as employees, partners, and contractors-so that the users can access Google Cloud services. With Workforce Identity Federation, you don't need to synchronize user identities from your existing IdP to Google Cloud identities."

Advantages of this approach:

* Syncless: You don't create or manage partner accounts in your Cloud Identity/Workspace (eliminating Option C).
* Security: If a partner employee leaves their company, their access to your Google Cloud database is automatically revoked when their home IdP account is disabled.
* Scoped Access: You grant IAM roles (like roles/cloudsql.client) specifically to the Workforce Pool or specific groups within that pool, ensuring they can't touch other resources.

Why other options are incorrect:

* A is incorrect: Public IPs are a major security risk and don't provide centralized identity governance.
* B is incorrect: You cannot "grant access" to accounts in another organization's Cloud Identity directly in a secure, manageable way for production databases without federation.

Reference:

Google Cloud Documentation: "Workforce Identity Federation" (https://cloud.google.com/iam/docs/workforce-identity-federation).
Google Cloud Security Engineer Study Guide: Section on "Advanced Identity Management - Federation."

質問: **68**
組織では、外部IPアドレスを持つCompute Engine VMインスタンスの使用を無効にするカスタム組織ポリシーを適用しています。1 しかし、規制対象となる事業部門では、サードパーティの監査プロセスのために一時的に外部IPを使用するという例外措置が必要です。規制対象となる業務ワークロードは、最小権限の原則に準拠し、ポリシーの逸脱を最小限に抑える必要があります。安全なポリシー管理と適切な処理を確保する必要があります。どうすればよいでしょうか？
A. 組織レベルで制限的な組織ポリシーを適用します。組織ポリシーをバイパスする権限を持つIAMカスタムロールを作成します。カスタムロールを、特定のプロジェクトの規制対象ビジネスチームに割り当てます。
B. 組織レベルでカスタム組織ポリシーを変更し、すべてのプロジェクトで外部 IP を許可します。
規制されたビジネス ワークロードを除く出力トラフィックを制限するように VPC ファイアウォール ルールを構成します。
C. 組織レベルでカスタム組織ポリシーを適用し、外部IPを制限します。規制対象のビジネスワークロードを別のフォルダに移動します。そのフォルダレベルでポリシーをオーバーライドします。
D. フォルダを作成します。フォルダ内の規制対象外の業務ワークロードには、制限的な組織ポリシーを適用します。規制対象の業務ワークロードは、そのフォルダに配置します。
正解: **(**正解を表示します**)**
The Google Cloud Resource Hierarchy is designed to allow inheritance with the ability to override policies at lower levels (Folders or Projects).2 This is the standard way to handle exceptions for specific business units without weakening the security posture of the entire organization.
According to Google Cloud Documentation (Understanding Hierarchy Evaluation):
"By default, organization policies are inherited by the descendants of the resource on which the policy is enforced. However, you can explicitly override a policy on a child resource (Folder or Project) by setting a new policy that either adds to or replaces the inherited values.3 This allows for granular control and exception handling." Why this is the correct approach:
* Isolation: By moving the workload to a specific folder, you isolate the exception.
* Least Privilege: Only the resources within that folder gain the exception; the rest of the organization remains protected by the constraints/compute.vmExternalIpAccess constraint.

* No "Bypass" Role: There is no standard IAM role that allows a user to "bypass" an Org Policy (Option A). Policies are enforced at the API level regardless of user roles.
* Auditability: Having a specific folder with an override makes it easy for auditors to see exactly where and why an exception exists.
Reference:
Google Cloud Documentation: "Creating and managing organization policies" (https://cloud.google.com/resource-manager/docs/organization-policy/creating-managing-policies).
Google Cloud Security Engineer Study Guide: Chapter 2 - Resource Management.

質問: **69**
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
正解: **(**正解を表示します**)**
Customer-Managed Encryption Keys (CMEK):
CMEK allows you to manage encryption keys using Cloud Key Management Service (KMS). This gives you control over the lifecycle of the keys, including rotation, destruction, and auditing.
Set up a Cloud KMS key ring and create encryption keys that will be used to protect your data in BigQuery, Cloud SQL, and Cloud Storage.
Configure the services to use CMEK for encrypting data at rest, ensuring compliance with your organization's security policies.
Cloud External Key Manager (EKM):
Cloud EKM allows you to use keys managed by an external key management provider to encrypt data in Google Cloud services.
Integrate your external key management system with Google Cloud using supported protocols and APIs.
Configure your data warehouse services to use the external keys for encryption, ensuring that key management is handled outside of the Google Cloud environment.
Key Access Justifications:

Enable Key Access Justifications to provide visibility into why encryption keys are being accessed. This helps in monitoring and auditing key usage to ensure compliance and security.
Set up policies and logging to capture and review key access requests, providing insights into how and why keys are used.
Access Transparency and Approval:
Implement Access Transparency to gain visibility into Google's access to your data and encryption keys.
Configure Access Approval to require explicit approval for Google support or engineering access to your data, adding an additional layer of security and control.
References:
Customer-Managed Encryption Keys (CMEK)
Cloud External Key Manager (EKM)
Key Access Justifications
Access Transparency
Access Approval

質問**: 70**
会社の検出および対応チームには、セキュリティ調査の際に Google Cloud 組織への緊急アクセスが必要です。毎日の終わりに、すべてのセキュリティ グループのメンバーシップが削除されます。Cloud Identity セキュリティ グループへのユーザー プロビジョニングを自動化する必要があります。グループ メンバーシップをプロビジョニングするためのサービス アカウントを作成しました。ソリューションは、Google が推奨するプラクティスに従い、最小権限の原則に準拠する必要があります。何をすればよいですか?
A. Google Workspace で、ドメイン全体の委任を使用して、サービス アカウント クライアント ID にスコープ https://wwwgoogleapiscom/auth/admindirectorygroup へのアクセスを許可し、サービス アカウント キーを使用します。
B. Google Workspace で、ドメイン全体の委任を使用して、サービス アカウントのクライアント ID にスコープ https://wwwgoogleapiscom/auth/admindirectorygroup へのアクセスを許可します。リソースが接続されたサービス アカウントでアプリケーションのデフォルト認証情報を使用します。
C. Google Workspace で、サービス アカウントにグループ編集者のロールを付与します。Cloud Identity API を有効にします。サービス アカウント キーを使用します。
D. Google Workspace で、サービス アカウントにグループ編集者のロールを付与し、Cloud Identity API を有効にして、リソースが接続されたサービス アカウントでアプリケーションのデフォルト認証情報を使用します。
正解**: (**正解を表示します**)**
The problem requires automating user provisioning to a Cloud Identity security group using a service account, adhering to Google-recommended practices and the principle of least privilege.

Cloud Identity Groups and Google Workspace: Cloud Identity groups are managed as part of Google Workspace. To programmatically manage Google Workspace resources (like groups), you typically use the Admin SDK APIs.
Domain-Wide Delegation: Service accounts cannot directly authenticate to Google Workspace APIs using IAM roles. Instead, they require "domain-wide delegation" to impersonate a user with the necessary administrative privileges within Google Workspace. This allows a service account to access user data or perform administrative tasks across the domain. The correct scope for managing groups is https://www.googleapis.com/auth/admin.directory.group.Extract Reference: "To allow a service account to access user data on behalf of users in a Google Workspace domain, you must delegate domain-wide authority to your service account." (Google Cloud documentation: https://developers.google.com/identity/protocols/oauth2/service-account#delegating)
Extract Reference (Admin SDK Scopes): The https://www.googleapis.com/auth/admin.directory.group scope is explicitly listed for "View and manage all groups on the domain." (Google Workspace Admin SDK documentation: https://developers.google.com/admin-sdk/directory/v1/scopes) Application Default Credentials (ADC) with Resource-Attached Service Account: Google-recommended practices strongly advise against using service account keys directly for authentication when running on Google Cloud infrastructure. Instead, it's recommended to use Application Default Credentials (ADC) with a service account attached to the resource (e.g., a Compute Engine VM, Cloud Run service, or Cloud Functions). This method manages credentials automatically and securely, reducing the risk associated with managing and rotating keys.Extract Reference: "For most Google Cloud services, Application Default Credentials (ADC) is the recommended way to authenticate." and "When running code in a Google Cloud environment, such as Compute Engine, Cloud Run, or Cloud Functions, use the built-in service account to authenticate automatically with ADC. This is the most secure approach, as you don't need to manually create or manage service account keys." (Google Cloud documentation: https://cloud.google.com/docs/authentication/production)
Options C and D are incorrect because granting an IAM role like "Groups Editor" in Google Cloud does not enable a service account to manage Google Workspace (Cloud Identity) group memberships; domain-wide delegation is required for that. Option A uses a service account key, which is less secure than ADC with a resource-attached service account according to Google's recommendations.
Therefore, option B is the most aligned with Google's recommended practices for securely automating group provisioning using a service account and domain-wide delegation.

質問: 71
あなたのチームは、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。

あなたのチームは、AD グループ メンバーシップによってアクセス許可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、あなたのチームは何をすべきですか?
A. Cloud Directory Sync をセットアップしてグループを同期し、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) をセットアップし、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。
正解**: (**正解を表示します**)**
"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP. Once the identities have been replicated then it's possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider.
This way you effectively delegate the authentication from Google to something that is under your control."

質問**: 72**
あなたのチームは、ユーザーが組織内でプロジェクトを作成できないようにする必要があります。DevOps チームのみが、要求者に代わってプロジェクトを作成できるようにする必要があります。
この要求を処理するためにチームが実行する必要がある 2 つのタスクはどれですか? 2つ選んでください。)
A. 組織レベルでプロジェクト作成者の役割からすべてのユーザーを削除します。
B. 組織ポリシーの制約を作成し、組織レベルで適用します。
C. 組織レベルでのプロジェクト編集者の役割を、指定されたユーザー グループに付与します。
D. 指定されたユーザー グループを、組織レベルでプロジェクト作成者の役割に追加します。
E. 請求先アカウントの作成者の役割を、指定された DevOps チームに付与します。
正解**: (**正解を表示します**)**
* Objective: Prevent users from creating projects while allowing only the DevOps team to create projects.
* Solution: Modify IAM roles and permissions.
* Steps:
* Step 1: Open the Google Cloud Console.
* Step 2: Navigate to the IAM & Admin page.

* Step 3: At the organizational level, find and remove all users from the Project Creator role.
* Step 4: Create or identify a group for the DevOps team.
* Step 5: Assign the Project Creator role to the DevOps team group at the organizational level.
By removing all users from the Project Creator role and granting it only to the DevOps team, you ensure that only the designated team can create projects.
References:
GCP IAM Documentation
Project Creator Role

質問**: 73**
Google Cloud 上で実行される自社アプリケーションの運用は、あなたに責任があります。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権を付与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、自社ネットワーク内の他のリソースには拡張できません。ソリューションは、Google が推奨するプラクティスに従う必要があります。何をすべきでしょうか?
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. 企業の ID プロバイダでパートナー チームのアカウントを作成し、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。
C. 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、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。
D. パートナーの Workforce Identity Federation を構成する ID プール プロバイダをパートナーの ID プロバイダに接続する Workforce プール リソースにデータベースへのアクセスを許可する
正解**: D (**コメントを発表する**)**
The problem requires granting an external partner team access solely to a database, without extending to other network resources, and following Google-recommended practices.
Workforce Identity Federation: This Google Cloud IAM feature is specifically designed for scenarios where an organization needs to grant Google Cloud access to external identities (like partners, contractors, or customers) who are managed by their own identity provider (IdP). It allows these external users to authenticate using their existing credentials and then gain access to specified Google Cloud resources.
Extract Reference: "Workforce Identity Federation lets you use an external identity provider (IdP) to authenticate and authorize a workforce-a group of users, such as employees, partners, and contractors- using IAM, so that the users can access Google Cloud services." (Google Cloud Documentation: "Workforce Identity Federation | IAM

Documentation" - https://cloud.google.com/iam/docs/workforce-identity-federation) Extract Reference: "Secure access for partners and vendors. Workforce Identity Federation can enable enterprises to selectively federate users from partner or vendor IdPs without requiring IT teams to sync or create a separate identity store to use Google Cloud resources." (Google Cloud Documentation: "Introducing Workforce Identity Federation..." - https://www.azalio.io/introducing-workforce-identity-federation-to-easily- manage-workforce-access-to-google-cloud/) Least Privilege and Isolation: With Workforce Identity Federation, you create an identity pool and a provider that trusts the partner's IdP. You then grant IAM roles only to the workforce pool (or specific identities within it) on the specific database resource. This ensures fine-grained access control and prevents access to other resources in your network, directly addressing the least privilege and isolation requirements. The partner's identities are never synced into your internal Cloud Identity directory.
Let's evaluate the other options:
A). Add a public IP address... Securely distribute credentials: Adding a public IP address exposes the database to the internet, which is a major security risk and contradicts "restricted solely to the database and can not extend to any other resources within your company's network" as it allows any external network to potentially reach it. Distributing credentials manually is also not a Google-recommended secure practice.
B). Create accounts for the partner team in your corporate identity provider. Synchronize these accounts with Google Cloud Identity: This means you become responsible for managing the partner's identities within your own corporate IdP and syncing them. This is an unnecessary operational burden and blurs the lines of identity management. It also may inadvertently grant them broader network access if your corporate IdP is connected to your internal network resources.
C). Ask the partner team to set up Cloud Identity accounts within their own corporate environment and identity provider. Grant the partner's Cloud Identity accounts access: While better than B, this implies the partner managing Cloud Identity accounts themselves and you directly granting IAM roles to their Cloud Identity users. Workforce Identity Federation is a more robust and scalable solution for federating any external IdP with Google Cloud IAM, rather than requiring partners to adopt Cloud Identity directly. Workforce Identity Federation is the explicit pattern for cross-organization access using existing external IdPs.
Therefore, Workforce Identity Federation is the most secure, scalable, and Google-recommended solution for granting restricted access to external partner teams.

質問**: 74**
あなたの組織は最近、Google Kubernetes Engine に新しいアプリケーションをデプロイしました。アプリケーションを保護するソリューションをデプロイする必要があります。このソリューションには次の要件があります。
スキャンは少なくとも 1 週間に 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る必要がありますか?
A. Google クラウド アーマー
B. Web セキュリティ スキャナー
C. セキュリティ状況分析
D. コンテナ脅威検出
正解**: (**正解を表示します**)**
Web Security Scanner is designed to scan your web applications deployed on Google Cloud for common vulnerabilities, including cross-site scripting (XSS). It can authenticate using Google accounts and can be scheduled to run scans regularly.
Steps:
Enable Web Security Scanner: In the Google Cloud Console, enable Web Security Scanner for your project.
Configure Scan: Set up the scan configuration, specifying the target URLs, authentication details (Google accounts), and scan frequency (at least once per week).
Run and Monitor Scans: Run the scans and monitor the results for vulnerabilities, addressing any issues found.
References:
Web Security Scanner documentation

質問**: 75**
標準ネットワーク層を使用している間、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. SSL プロキシ
B. TCP プロキシ
C. 内部 TCP/UDP
D. TCP/UDP ネットワーク
正解**: D (**コメントを発表する**)**
* Use the TCP/UDP Network Load Balancer:
* TCP/UDP Network Load Balancer maintains the client IP address by default when forwarding traffic to backends.
* Configure a TCP/UDP Network Load Balancer with appropriate backend services and health checks.
* Ensure that the load balancer is using the standard network tier to comply with the requirements.
References:
TCP/UDP Network Load Balancing
Network Service Tiers

質問**: 76**

Compute Engine でホストされているウェブ アプリケーションをデプロイしています。ビジネス要件では、アプリケーション ログを 12 年間保存し、データをヨーロッパの境界内に保持す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。あなたは何をするべきか？
A. EUROPE-WEST1 リージョンにログを保存する Cloud Storage バケットを作成します。効率を高めるために、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、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 12 年間のカスタム保持期間で送信するように、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 リージョンにある Google Cloud のオペレーション スイートのログバケットで、12 年のカスタム保持ポリシーを構成します。
正解: **(**正解を表示します**)**
To fulfill the requirements of preserving logs for 12 years and ensuring data residency within European boundaries, the best approach is to use Google Cloud's operations suite (formerly Stackdriver) with a custom log bucket configured in the desired region.
* Configure Cloud Logging Agent:
* Install and configure the Cloud Logging agent on your Compute Engine instances. This agent collects logs from your application and system and sends them to Google Cloud's operations suite.
* Create a Custom Log Bucket:
* In the Cloud Logging interface, create a custom log bucket in the EUROPE-WEST1 region. This bucket will store your logs and can be configured with a custom retention period.
* Set Custom Retention Policy:
* Configure the retention policy for the custom log bucket to 12 years. This ensures that all logs are preserved for the required duration.
* Ship Logs to the Custom Log Bucket:
* Modify the logging configuration to direct logs from the Cloud Logging agent to the custom log bucket. This can be done through the logging configuration settings in the Cloud Console or by updating the agent configuration files.
This solution minimizes overhead by using managed services and ensures cost-effectiveness by leveraging Cloud Logging's built-in capabilities for log storage and retention management.
References
* Cloud Logging Documentation
* Creating and Managing Logs Buckets

質問: **77**
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、適切なテーブルの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。
正解: **C** (コメントを発表する)
"To support common use cases like setting a Time to Live (TTL) for objects, retaining noncurrent versions of objects, or "downgrading" storage classes of objects to help manage costs, Cloud Storage offers the Object Lifecycle Management feature. This page describes the feature as well as the options available when using it.
To learn how to enable Object Lifecycle Management, and for examples of lifecycle policies, see Managing Lifecycles." https://cloud.google.com/storage/docs/lifecycle

質問: **78**
Compute Engine で実行されるバッチジョブには、Cloud Storage バケットへの一時的な書き込みアクセス権が必要です。バッチジョブには、タスクを完了するために必要な最小限の権限のみを使用させたいと考えています。どうすればよいでしょうか？
A. Cloud Storage 管理者の完全な権限を持つサービス アカウントを作成します。このサービス アカウントを Compute Engine インスタンスに割り当てます。
B. 事前定義された storage.objectcreator ロールを Compute Engine インスタンスのデフォルトのサービス アカウントに付与します。
C. サービス アカウントを作成し、書き込み権限が指定された長期有効のサービス アカウント キー ファイルをバッチ ジョブ スクリプトに直接埋め込みます。

D. ストレージの .objectcreator ロールを持つサービスアカウントを作成します。バッチジョブのコードでサービスアカウントの偽装を使用します。
正解**: (**正解を表示します**)**
To provide temporary write access to a Cloud Storage bucket with the minimum permissions necessary, you should:
* Identify the Compute Engine instance's default service account: Each Compute Engine instance has a default service account that is used to interact with other Google Cloud services.
* Assign the storage.objectCreator role: This predefined IAM role grants permissions to create objects in a Cloud Storage bucket, which is sufficient for temporary write access. It does not grant permissions to read or delete objects, thus adhering to the principle of least privilege.
* Avoid using full permissions or long-lived keys: Options A and C suggest using broader permissions than necessary or embedding long-lived keys, which could pose a security risk if compromised.
* Service account impersonation (Option D) is not necessary for this task and would be more appropriate for scenarios where you need to assume a different identity with different permissions.
References:
Google Cloud documentation on IAM roles for Cloud Storage, which lists the storage.objectCreator role as providing permissions to create objects without granting full administrative access to the bucket1.
Best practices for access control in Cloud Storage recommend using the least privilege necessary and avoiding the use of long-lived service account keys2.

質問**: 79**
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。オンプレミスPKIへの影響は、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設定します (IaC)。
B. 証明書マネージャを使用して、オンプレミスPKIから発行された証明書とフロントエンド用の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。
C. オンプレミスの 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。

正解: **(**正解を表示します**)**
This approach allows you to leverage your existing on-premises PKI infrastructure while minimizing its impact and manual processes. By creating a subordinate CA in Google's Certificate Authority Service, you can automate the process of issuing certificates for your HTTP load balancer frontends. This solution scales well as the number of load balancers increases.

質問: **80**
あなたは会社の開発チームに所属しています。GKE のステージングでホストされているウェブ アプリケーションは、入力されたデータを最初に適切に検証せずに、ウェブページにユーザー データを動的に含めることに気付きました。これにより、攻撃者は意味不明なコマンドを実行し、実稼働環境で被害者のユーザーのブラウザに任意のコンテンツを表示する可能性があります。
この脆弱性をどのように防止および修正する必要がありますか?
A. IP アドレスまたはエンドユーザーのデバイス属性に基づいて Cloud IAP を使用して、脆弱性を防止および修正します。
B. HTTPS ロード バランサーをセットアップし、本番環境に Cloud Armor を使用して潜在的な XSS 攻撃を防ぎます。
C. Web Security Scanner を使用して、コード内の古いライブラリの使用を検証し、含まれているライブラリのセキュリティで保護されたバージョンを使用します。
D. ステージングで Web Security Scanner を使用して XSS インジェクション攻撃をシミュレートし、コンテキストの自動エスケープをサポートするテンプレート システムを使用します。
正解: **(**正解を表示します**)**
There is mention about simulating in Web Security Scanner. "Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions."
https://cloud.google.com/security-command-center/docs
/how-to-remediate-web-security-scanner-findings#xss
Reference: https://cloud.google.com/security-scanner/docs/remediate-findings

質問: **81**
組織のオンプレミス ネットワークを、Production と Non-Production という名前の 2 つのサブネットを持つ 1 つの共有 VPC を含む既存の GCP 環境に接続する必要があります。次のことを行う必要があります。
プライベート トランスポート リンクを使用します。
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 APIs 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。
あなたは何をするべきか？

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、制限付きの 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 の間にダイレクト ピアリング 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 アクセスを設定します。
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。
正解**: (**正解を表示します**)**
Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud:
Dedicated Interconnect provides a direct physical connection between your on-premises network and Google's network, which is ideal for high-throughput, low-latency connections.
Request a Dedicated Interconnect from the Google Cloud Console, specifying the required bandwidth and location.
Once provisioned, set up the connection on your on-premises router and configure the BGP sessions to exchange routes with Google Cloud.
Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations:
Configure your on-premises DNS server to resolve Google APIs to restricted.googleapis.com. This ensures that the traffic stays within the Google network and is not exposed to the public internet.
Update your DNS settings to use restricted.googleapis.com for the necessary API endpoints.
This setup ensures that all Google Cloud API traffic is routed through the private link and subject to VPC Service Controls for additional security and compliance.
References:
Dedicated Interconnect Overview
Configuring DNS to use restricted.googleapis.com

質問**: 82**
組織は、特定の IT ワークロードに対する Google Cloud Platform (GCP) の使用を評価しています。十分に確立されたディレクトリ サービスを使用して、ユーザー ID とライフサイクル管理を管理します。このディレクトリ サービスは、組織が ID の "信頼できるソース" ディレクトリとして使用するために継続する必要があります。
組織の要件を満たすソリューションはどれですか?

A. Google Cloud Directory Sync (GCDS)
B. クラウド ID
C. セキュリティ アサーション マークアップ言語 (SAML)
D. パブ/サブ
正解**: A (**コメントを発表する**)**
With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.
https://support.google.com/a/answer/106368?hl=en

質問**: 83**
あなたは、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セキュリティ チームの一員です。
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、Cloud Storage バケットにコピーしたりできないようにする必要があります。
あなたは何をするべきか？
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付き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. プロジェクト A と B のネットワークでプライベート アクセスを有効にし、厳格なファイアウォール ルールを使用して、ネットワーク間の通信を許可します。
D. プロジェクト A と B のネットワーク間で VPC ピアリングを有効にし、厳格なファイアウォール ルールを使用してネットワーク間の通信を許可します。
正解**: A (**コメントを発表する**)**
Objective: Ensure that a Cloud Storage bucket in Project A can only be readable from Project B and prevent data access or copying to Cloud Storage buckets outside the network, even with correct credentials.
Solution: Use VPC Service Controls to create a security perimeter.
Steps:
Step 1: Open the Google Cloud Console.
Step 2: Navigate to the VPC Service Controls page.
Step 3: Create a new service perimeter.
Step 4: Add Project A and Project B to the service perimeter.
Step 5: Include Cloud Storage service in the perimeter configuration.
Step 6: Define access levels to ensure that only resources within the perimeter can access the Cloud Storage bucket.

By setting up a VPC Service Controls perimeter, you can enforce security boundaries that restrict data access and movement to within defined projects, providing an extra layer of protection beyond IAM permissions.
References:
VPC Service Controls Overview
Configuring VPC Service Controls

質問: **84**
あなたの組織は、最近いくつかの DDoS 攻撃を受けました。ドメイン名検索への応答を認証する必要があります。どの Google Cloud サービスを使用する必要がありますか?
A. Generalization
B. Redaction
C. CryptoHashConfig
D. CryptoReplaceFfxFpeConfig
正解: **A (**コメントを発表する**)**
Cloud DNS with DNSSEC (Domain Name System Security Extensions) provides authentication for DNS responses, ensuring that they are legitimate and have not been tampered with. DNSSEC helps protect against DNS spoofing and cache poisoning attacks, which are common techniques used in DDoS attacks.
Steps:
* Enable DNSSEC: In the Google Cloud Console, navigate to Cloud DNS and enable DNSSEC for your managed zones.
* Configure Key Signing: Set up key signing keys (KSK) and zone signing keys (ZSK) to sign your DNS records.
* Monitor DNSSEC Status: Regularly monitor the DNSSEC status and logs to ensure it is functioning correctly.
References:
Cloud DNS documentation

質問: **85**
あなたは新しいユーザーを Cloud Identity にオンボーディングしていて、一部のユーザーが企業のドメイン名を使用してコンシューマー ユーザー アカウントを作成していることに気付きました。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る必要がありますか?
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. コンシューマ ユーザー アカウントごとに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 アカウントの転送ツールを使用します。
D. お客様のサードパーティ 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。

正解: (正解を表示します)
To manage consumer user accounts created using the corporate domain name, you can use the transfer tool for unmanaged user accounts provided by Google Cloud Identity. Here's how you can proceed:
* Identify Unmanaged Accounts:
* Use the Cloud Identity interface to identify consumer (unmanaged) accounts that exist with your corporate domain.
* Initiate Transfer Process:
* Use the transfer tool for unmanaged user accounts to initiate the transfer. This tool helps in converting unmanaged accounts (consumer accounts) into managed accounts.
* User Notification:
* Users with unmanaged accounts will receive an email notification prompting them to accept the transfer to the organization's managed account system.
* Accept Transfer:
* Users need to follow the instructions in the email to accept the transfer. Once accepted, their accounts will be managed under your organization's Cloud Identity setup.
* Benefits:
* Centralized Management: All user accounts under your corporate domain are managed centrally, ensuring compliance and security.
* Enhanced Security: Managed accounts provide better control over security policies and access management.
References
* Transfer tool for unmanaged users
* Cloud Identity Documentation

質問: **86**
Google Cloud 内にデータベースサーバー用の安全な内部ネットワークを構築したいと考えています。サーバーはパブリックインターネットと直接通信してはなりません。どうすればよいでしょうか？
A. 各データベースサーバーに静的パブリックIPアドレスを割り当てます。ファイアウォールルールを使用して外部アクセスを制限します。
B. プライベートサブネットを持つVPCを作成します。各データベースサーバーにプライベートIPアドレスを割り当てます。
C. 各データベース サーバーにプライベート IP アドレスとパブリック IP アドレスの両方を割り当てます。
D. 各データベースサーバーにプライベートIPアドレスを割り当てます。NATゲートウェイを使用して、データベースサーバーへのインターネット接続を提供します。
正解: (正解を表示します)
To ensure servers do not have any direct communication with the public internet, they must be configured without a public IP address.

VPC and Private Subnet: A Virtual Private Cloud (VPC) network provides the isolated, internal network structure. A subnet is the logical partition within the VPC.
Private IP Address: Assigning only a private IP address to the database servers ensures they can only communicate internally within the VPC (or connected on-premises networks) and cannot directly connect to or be connected from the public internet.
Extracts:
"Resources in a VPC network can be assigned two types of IP addresses: internal (private) and external (public). If a VM is not assigned an external IP address, it can only communicate internally with other resources in the VPC network..." (Source 6.1) Option A and C involve assigning a public IP address, which violates the "no direct communication with the public internet" rule. Option D uses NAT to provide outbound internet connectivity, which also violates the requirement.

質問: **87**
管理アプリケーションは、Virtual Private Cloud（VPC）インスタンス内のマネージドグループ内の仮想マシン（VM）のポート5601で実行されていますが、現在インターネットにアクセスできません。ポート5601のウェブインターフェースをユーザーに公開し、Google認証情報による認証と承認を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. デフォルトのルート ポイントをデフォルトのインターネット ゲートウェイに設定して VPC ルーティングを変更します。VPC ファイアウォール ルールを変更して、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。
B. OS ログインを有効にして要塞ホストを構成し、VPC ファイアウォールでポート 5601 への接続を許可します。ブラウザの SSH を使用して Google Cloud コンソールから要塞ホストにログインし、次にウェブ アプリケーションにログインします。
C. Google 認証情報を使用して、Identity-Aware Proxy (IAP) 保護を備えたマネージド グループを指す HTTP ロード バランシング インスタンスを構成します。VPC ファイアウォールを変更して、IAP ネットワーク範囲からのアクセスを許可します。
D. パブリックネットワークにセキュアシェルアクセス（SSH）の要塞ホストを設定し、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。
正解: **(**正解を表示します**)**
This approach allows you to expose the web interface securely by using Identity-Aware Proxy (IAP), which provides authentication and authorization with Google credentials. The HTTP Load Balancer can distribute traffic to the VMs in the managed group, and the VPC firewall rule ensures that access is allowed from the IAP network range.

質問: **88**

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できるようにします。顧客は、コメントやレビューが公開される前に、テキストに機密データ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 Service を使用する必要がありますか?
A. クラウド鍵管理サービス
B. Cloud Data Loss Prevention API
C. BigQuery
D. クラウド セキュリティ スキャナー
正解**: (**正解を表示します**)**
To ensure user-uploaded comments and product reviews do not include sensitive data before publication, use the Cloud Data Loss Prevention (DLP) API.
Enable DLP API:
Go to the Cloud Console and navigate to APIs & Services > Library.
Search for "Data Loss Prevention API" and enable it.
Configure DLP API:
Create an inspection template specifying the types of sensitive data to detect.
Set up de-identification templates if you want to redact or mask sensitive data.
Implement DLP in Application:
Use the Google Cloud DLP Client Library for the desired programming language.
Send the text data to the DLP API for inspection before saving or publishing.
from google.cloud import dlp_v2 dlp_client = dlp_v2.DlpServiceClient() parent = f"projects/{project_id}" item = {"value": "User comment text here"} inspect_config = {"info_types": [{"name": "PERSON_NAME"},
{"name": "CREDIT_CARD_NUMBER"}]} response = dlp_client.inspect_content(parent=parent, inspect_config=inspect_config, item=item) Cloud Data Loss Prevention API Documentation DLP API Client Libraries

質問**: 89**
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 プラクティスに従って、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、ドメイン制限共有組織ポリシーを実装しました。エンジニアリング チームは現在、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報告しています。記載されているベスト プラクティスに従いながら、パートナーのドメインの例外をどのように作成する必要がありますか?
A. ドメイン制限共有の組織ポリシーをオフにします。ポリシー値を 「すべて許可」に設定します。
B. ドメイン制限共有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 グループを組織のポリシーの例外として追加してから、ポリシーを再び有効にします。
D. ドメイン制限共有組織ポリシーをオフにします。ポリシー値を「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 のお客様 ID を組織ポリシーの例外として追加してから、ポリシーをオンに戻します。
正解**: (**正解を表示します**)**
https://cloud.google.com/resource-manager/docs/organization-policy/restricting-domains#setting_the_organization_policy The domain restriction constraint is a type of list constraint. Google Workspace customer IDs can be added and removed from the allowed_values list of a domain restriction constraint. The domain restriction constraint does not support denying values, and an organization policy can't be saved with IDs in the denied_values list.
All domains associated with a Google Workspace account listed in the allowed_values will be allowed by the organization policy. All other domains will be denied by the organization policy.

質問**: 90**
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動したいと考えています。ジョブはバースト性があり、迅速に完了する必要があります。暗号化キーを管理およびローテーションできる必要があります。
この顧客の要件を満たすには、クラスタ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. 顧客指定の暗号化キー (CSEK)
B. Cloud Key Management Service (KMS) を使用した顧客管理の暗号鍵 (CMEK)
C. デフォルトでの暗号化
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
正解**: (**正解を表示します**)**
For managing and rotating encryption keys in a Compute Engine-based cluster using Managed Instance Groups (MIGs), Customer-Managed Encryption Keys (CMEK) with Cloud KMS is the appropriate solution.
Set Up Cloud KMS:
Go to the Cloud Console and navigate to Security > Cryptographic Keys.
Create a keyring and a key.
Create and Use CMEK:
While creating or updating a Compute Engine instance, specify the CMEK key.
Example command:
gcloud compute instances create example-instance \ --image-family=debian-9 \ --image-project=debian-cloud

\ --boot-disk-kms-key=projects/[PROJECT_ID]/locations/global/keyRings/[KEY_RING]/cryptoKeys/[KEY] Rotate Keys:
Rotate keys periodically using Cloud KMS by creating new key versions and updating the instances to use the new key versions.
Customer-Managed Encryption Keys (CMEK)
Using Customer-Managed Encryption Keys

質問**: 91**
チームは、Compute Engine インスタンスがインターネットや Google API や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ために無効のままにしておく必要がある 2 つの設定はどれですか? （2 つ選んでください。）
A. パブリック IP
B. IP フォワーディング
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
正解**: A,C (**コメントを発表する**)**
To ensure that a Compute Engine instance does not have access to the internet or to any Google APIs or services, you need to disable the following settings:
Public IP: Disabling the public IP address ensures that the instance does not have a direct connection to the internet. Without a public IP address, the instance cannot be accessed from or communicate with the internet directly.
Private Google Access: Disabling Private Google Access ensures that the instance does not have access to Google APIs and services through the internal Google network. Private Google Access allows instances without a public IP to reach Google APIs and services using private IP addresses, but disabling it will block this path.
Disabling these settings will effectively isolate the instance from both the public internet and Google's internal API services.
References
Google Cloud VPC Documentation - Overview
Configuring Private Google Access
Compute Engine Network Overview

質問: **92**
多国籍企業のビジネス ユニットが GCP にサインアップし、GCP へのワークロードの移動を開始します。ビジネス ユニットは、数百のプロジェクトを持つ組織リソースを使用して Cloud Identity ドメインを作成します。
あなたのチームはこれに気づき、権限の管理とドメイン リソースの監査を引き継ぐことを望んでいます。
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権を付与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
正解: **(**正解を表示します**)**
Here are the permissions available to organizationRoleAdmin
iam.roles.create
iam.roles.delete
iam.roles.undelete
iam.roles.get
iam.roles.list
iam.roles.update
resourcemanager.projects.get
resourcemanager.projects.getIamPolicy
resourcemanager.projects.list
resourcemanager.organizations.get
resourcemanager.organizations.getIamPolicy
There are sufficient as per least privilege policy. You can do user management as well as auditing.
https://cloud.google.com/iam/docs/understanding-custom-roles

質問: **93**
Google Cloud 組織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 を操作できるようにするため、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. 毎日実行される Cloud Functions をトリガーして、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 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。
正解**: (**正解を表示します**)**
* Organization Policy: Use the constraints/compute.skipDefaultNetworkCreation organization policy constraint to disable the creation of default networks in new projects.
* Policy Application: Apply this constraint at the organization level to ensure it affects all projects within your organization, preventing the creation of default networks.
* Best Practices Compliance: Following this best practice helps maintain a clean and secure network configuration by avoiding the use of default networks, which may not be properly segmented or secured.
* Verification: Verify the policy application by creating new projects and ensuring that default networks are not created. References:
* Google Cloud - Organization Policy Constraints
* Google Cloud - Best Practices for Enterprise Organizations

質問**: 94**
チームは、SIEM 内のすべての開発クラウド プロジェクトの統合ログ ビューを取得する必要があります。開発プロジェクトは、NONPROD 組織フォルダーの下にあり、テスト プロジェクトと本番前のプロジェクトがあります。
開発プロジェクトは、ABC-BILLING 請求先アカウントを組織の他のメンバーと共有します。
要件を満たすには、どのロギング エクスポート戦略を使用する必要がありますか?
A. 1. 専用の SIEM プロジェクトで、folders/NONPROD 親および includeChildren プロパティを True に設定して、Cloud Pub/Sub トピックにログをエクスポートします。
2.SIEM をトピックにサブスクライブします。
B. 1. 専用の SIEM プロジェクトで、billingAccounts/ABC-BILLING 親と includeChildren プロパティを False に設定して Cloud Storage シンクを作成します。
2.SIEM で Cloud Storage オブジェクトを処理します。
C. 1. 各開発プロジェクトのログを専用の SIEM プロジェクトの Cloud Pub/Sub トピックにエクスポートします。
2.SIEM をトピックにサブスクライブします。
D. 1. 各プロジェクトで、パブリックに共有された Cloud Storage バケットを使用して Cloud Storage シンクを作成します。
2.SIEM で Cloud Storage オブジェクトを処理します。
正解**: (**正解を表示します**)**

"Your team needs to obtain a unified log view of all development cloud projects in your SIEM" - This means we are ONLY interested in development projects. "The development projects are under the NONPROD organization folder with the test and pre-production projects" - We will need to filter out development from others i.e test and pre-prod. "The development projects share the ABC-BILLING billing account with the rest of the organization." - This is unnecessary information.

質問: **95**
組織は、いくつかのミッション クリティカルなアプリケーションをオンプレミスで維持しながら、アプリケーションを Google Cloud に移行しています。組織は、少なくとも 50 Gbps の帯域幅でデータを転送する必要があります。サイト間の安全な継続的な接続を確保するために、何を使用する必要がありますか?
A. 専用インターコネクト
B. クラウド ルーター
C. クラウド VPN
D. パートナー インターコネクト
正解: **A (**コメントを発表する**)**
Dedicated Interconnect provides a high-bandwidth (up to 80 Gbps per connection) and secure connection between your on-premises network and Google Cloud. It ensures reliable and high-speed data transfer, meeting the requirement of at least 50 Gbps bandwidth.
Steps:
* Set Up Dedicated Interconnect: Order a Dedicated Interconnect connection through the Google Cloud Console.
* Configure VLAN Attachments: Set up VLAN attachments to segment traffic between your on-premises network and Google Cloud.
* Establish BGP Sessions: Configure BGP sessions for dynamic routing and failover.
References:
Dedicated Interconnect documentation

質問: **96**
会社の中核プロジェクトに人工知能モデルを導入しました。このモデルには機密性の高い知的財産が多く含まれており、インターネットから厳重に隔離する必要があります。モデルのエンドポイントは、組織内の特定のプロジェクトにのみ公開する必要があります。どうすればよいでしょうか？
A. モデルプロジェクト内に、モデルエンドポイントを指す外部アプリケーションロードバランサを作成します。IPアドレスをGoogle Cloudに制限するCloud Armorポリシーを作成します。B. モデルプロジェクト内に、モデルエンドポイントを指す内部アプリケーションロードバランサを作成します。このロードバランサをPrivate Service Connectを使用して、構成済みのプロジェクトリストに公開します。

B. モデルプロジェクトと、モデルに接続する必要がある各プロジェクトの両方で、プライベート Google アクセスを有効にします。プライベート Google アクセス アドレスへの接続を許可するファイアウォール ポリシーを作成します。
C. 他のすべてのプロジェクトに提供される共有VPCネットワークをホスト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、モデルへのアクセスを許可します。
正解**: (**正解を表示します**)**
The requirements necessitate a private, cross-project service-to-service connection with explicit authorization-a capability perfectly addressed by Private Service Connect (PSC).
Internal Load Balancer: Ensures the service is isolated from the internet (Layer 7 Load Balancer for HTTP/S ML endpoint).
Private Service Connect (PSC): Allows a service (the model endpoint, exposed via the internal load balancer) in one VPC/project (producer) to be securely consumed by other VPCs/projects (consumers) using an internal IP address.
Defined List of Projects: PSC enables Explicit authorization, allowing the producer to define the allowed list of consumers that can establish a connection, directly meeting the granular restriction requirement.
Extracts:
"Private Service Connect provides... Explicit authorization. Private Service Connect provides an authorization model that gives consumers and producers granular control." (Source 2.4)
"Private Service Connect backends let Google Cloud load balancers send traffic through Private Service Connect to reach published services... Placing a load balancer in front of a managed service provides the consumer with more visibility and control..." (Source 2.4)
"Publish services by using Private Service Connect... Select the internal load balancer that hosts the service that you want to publish." (Source 2.3)

質問**: 97**
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。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
正解**: (**正解を表示します**)**
Enable the compute.restrictXpnProjectLienRemoval organization-level policy constraint:
This constraint prevents users from removing liens from Shared VPC host projects.
By enabling this constraint, you ensure that the Shared VPC host project cannot be accidentally deleted, as liens prevent deletion without proper authorization.
Apply this constraint via the Google Cloud Console or using the gcloud command-line tool.
References:

Organization Policy Constraints
Shared VPC

質問: **98**
既存の VPC Service Controls 境界を新しいアクセス レベルで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を壊さないようにし、オーバーヘッドを最小限に抑えながら、ユーザーへの影響を最小限に抑える必要があります。あなたは何をするべきか？
A. 既存の境界の正確なレプリカを作成します。新しいアクセス レベルをレプリカに追加します。アクセス レベルが精査された後、元の境界を更新します。
B. 決して一致しない新しいアクセス レベルで境界を更新します。新しいアクセス レベルを更新して、必要な状態に 1 つずつ一致させ、過度に寛大にならないようにします。
C. 境界で予行演習モードを有効にします。新しいアクセス レベルを境界構成に追加します。アクセス レベルが精査された後、境界構成を更新します。
D. 境界で予行演習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構成に追加します。アクセス レベルが精査された後、境界構成を更新します。
正解: **(**正解を表示します**)**
Enable Dry Run Mode: Start by enabling the dry run mode for your VPC Service Controls perimeter. This mode allows you to test changes without actually enforcing them, thus preventing any disruption to your current setup.
Add Access Level: Add your new access level to the dry run configuration. This way, you can monitor how the new access level would behave and interact with your existing setup without any real impact.
Vetting Process: Carefully vet the new access level by analyzing logs and monitoring the behavior in the dry run mode. Ensure that the new configuration meets your security and operational requirements.
Update Perimeter: Once you are confident that the new access level will not disrupt existing services and meets all requirements, update the actual perimeter configuration with the new access level. This approach minimizes risk by allowing you to test changes before they take effect, ensuring seamless updates with minimal disruption. References:
Google Cloud - Configuring VPC Service Controls
Google Cloud - Using Dry Run Mode

質問: **99**
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。
正解**: (**正解を表示します**)**
The goal is to deploy 2SV with a phased rollout to control the number of individuals affected at once, minimizing disruption, and keeping management simple.
While OU structure can be used, managing policy exceptions based on Configuration Groups is the recommended and less complex way to handle phased rollouts of security settings like 2SV in Google's Admin console.
Extracts:
"When rolling out 2SV, it is highly recommended to use a phased deployment approach to manage the impact on user access and support resources." (Source 2.1)
"You can use configuration groups to select a subset of users within an OU structure and apply specific settings, such as 2SV enforcement, to them. This allows for a gradual, controlled rollout without needing to alter your primary organizational unit structure." (Source 2.2) Groups allow you to easily add/remove users from the enforcement scope without moving their identity within the OU hierarchy (Option A), which keeps management complexity low. Options C and D do not allow for the necessary phased control of enforcement.

質問**: 100**
Cloud Key Management Service （KMS）によって管理される鍵を使用して、Compute Engine ディスク上のデータを保存時に暗号化する必要があります。これらのキーに対する Cloud Identity and Access Management (IAM) のアクセス許可は、グループ化された方法で管理する必要があります。これは、アクセス許可がすべてのキーに対して同じである必要があるためです。
あなたは何をするべきか？
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。KeyRing レベルで IAM 権限を管理します。
C. 永続ディスクごとに KeyRing を作成します。各 KeyRing には単一のキーが含まれます。キー レベルで IAM 権限を管理します。
D. 永続ディスクごとに KeyRing を作成します。各 KeyRing には 1 つのキーが含まれます。KeyRing レベルで IAM 権限を管理します。
正解**: (**正解を表示します**)**

Managing IAM permissions at the KeyRing level is more efficient and scalable compared to managing them at the individual Key level. By creating a single KeyRing and placing all encryption keys within it, you can apply uniform IAM permissions to the entire KeyRing, simplifying the management of permissions.
Steps:
Create a KeyRing: Set up a single KeyRing in Cloud KMS for all the encryption keys required for the persistent disks.
Create Encryption Keys: Generate the necessary encryption keys within this KeyRing.
Set IAM Permissions: Assign IAM roles and permissions to the KeyRing to manage access control at this level, ensuring that all keys within the KeyRing inherit these permissions.
References:
Google Cloud: Cloud Key Management Service (KMS)
Managing access to resources

質問**: 101**
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 consrraints/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. 管理されていないインスタンス 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。
正解**: (**正解を表示します**)**
Provision a Cloud NAT Instance:
Cloud NAT (Network Address Translation) allows instances without external IP addresses to access the internet securely.

In the Google Cloud Console, navigate to the VPC Network section and select Cloud NAT.
Create a new Cloud NAT configuration, specifying the VPC and region where your Compute Engine VMs are deployed.
Configure Cloud NAT:
Ensure that the Cloud NAT instance is configured to provide outbound internet connectivity for the VMs in your specified subnet.
This setup allows the VMs to access the internet for package updates and external installations without requiring public IP addresses.
Enable Private Google Access:
Private Google Access allows VMs in a subnet to reach Google APIs and services using internal IP addresses.
In the Google Cloud Console, navigate to the VPC Network section and select Subnets.
Edit the subnet used by your Compute Engine VMs and enable Private Google Access.
Update DevOps Scripts:
Ensure that your DevOps scripts are updated to work with the new network configuration.
Test the build process to confirm that the VMs can access necessary resources and complete the build pipeline successfully.
References:
Cloud NAT Documentation
Private Google Access

質問**: 102**
顧客のアーキテクチャでセキュリティ評価を実行し、複数の VM にパブリック IP アドレスがあることを発見しました。パブリック IP アドレスを削除することを推奨した後、これらの VM は、顧客の通常の操作の一部として外部サイトと通信する必要があると言われます。顧客の VM でパブリック IP アドレスの必要性を減らすために、何をお勧めしますか?
A. Google クラウド アーマー
B. クラウド NAT
C. クラウド ルーター
D. クラウド VPN
正解**: (**正解を表示します**)**
Cloud NAT (Network Address Translation) enables instances in a private network to connect to external services while not exposing their internal IP addresses to the public internet. This solution helps in situations where VMs need to initiate outbound connections without having a public IP address:
* Cloud NAT Setup: Configure Cloud NAT for the subnet where your VMs are located. This allows these VMs to use the NAT gateway to communicate with external services securely.
* Network Security: By using Cloud NAT, the internal IP addresses of VMs remain private, reducing the attack surface and enhancing security.

* Operational Continuity: VMs can continue to communicate with external sites as needed for operations without requiring public IP addresses, meeting both security and functional requirements.
References
* Cloud NAT Documentation

質問: **103**
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 compuce.imageUser ロールを付与します。
B. ユーザーに OS イメージ プロジェクトでの compuce.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、自分と自分のチームのみが VM インスタンスを作成できるようにします。
正解: **(**正解を表示します**)**
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints - constraints
/compute.trustedImageProjects
This list constraint defines the set of projects that can be used for image storage and disk instantiation for Compute Engine. If this constraint is active, only images from trusted projects will be allowed as the source for boot disks for new instances.

質問: **104**
グローバルな防衛関連企業である貴社は、極秘の機密データをBigQueryとCloud Storageに移行しています。国家安全保障規制により、マスター暗号鍵の素材は認定されたオンプレミスの暗号ハードウェアから外部に持ち出すことが禁じられています。クラウドプロバイダに依存しない、データアクセスを一方的に取り消す権限を維持する必要があります。どうすればよいでしょうか？
A. Cloud Storage と BigQuery での各データ操作で独自の暗号化キーを提供することにより、顧客指定の暗号化キー （CSEK）を使用します。
B. BigQuery データセットと Cloud Storage バケットには、顧客管理の暗号鍵 （CMEK）を使用します。鍵は Cloud Key Management Service （Cloud KMS）に保存します。
C. 既存のオンプレミスのマスター暗号化鍵を Cloud Key Management Service （Cloud KMS）にインポートします。インポートした鍵は、BigQuery と Cloud Storage の暗号化に使用します。

D. BigQuery データセットと Cloud Storage バケット用に Cloud External Key Manager（Cloud EKM）を構成します。EKM を既存のオンプレミス ハードウェア セキュリティ モジュール（HSM）と統合します。
正解: **(**正解を表示します**)**
The requirement to ensure the master encryption key material never leaves the on-premises hardware (HSM) and retaining the unilateral ability to revoke access are the defining features of Cloud External Key Manager (Cloud EKM).
Key Residency: Cloud EKM allows you to use encryption keys stored and managed in a supported external key management system, such as an on-premises HSM, for encrypting data in Google Cloud services like BigQuery and Cloud Storage. This ensures the key material remains in your accredited hardware.
Unilateral Control: Since Google Cloud must request the key from the external system for every encryption
/decryption operation, revoking access (by disabling the key or revoking Google's access) in the external system immediately renders the data in Google Cloud inaccessible, granting the customer unilateral control.
Extracts:
"Cloud External Key Manager (Cloud EKM) is a cloud service that lets you encrypt data in Google Cloud with keys you manage outside of Google Cloud." (Source 6.1)
"The key material is stored on an external system, such as a Cloud EKM partner or an on-premises HSM, and never leaves that system." (Source 6.1)
"The customer can unilaterally revoke access to the key at the EKM system, making the encrypted data in Google Cloud inaccessible, which is a key requirement for highly regulated industries." (Source 6.2)

質問: **105**
クラウド サービスの提供と使用に適用される情報セキュリティ管理のガイドラインを提供する国際コンプライアンス標準はどれですか?
A. ISO27001
B. ISO27002
C. ISO 27017
D. ISO 27018
正解: **(**正解を表示します**)**
Create a new Service Account that should be able to list the Compute Engine instances in the project. You want to follow Google-recommended practices.
https://cloud.google.com/security/compliance/iso-27017

質問: **106**
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. 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。
D. 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。
正解: **(**正解を表示します**)**
To handle significant traffic spikes and potentially malicious IPs, you can use Google Cloud Armor to configure rate-based bans. This approach allows you to automatically ban clients that exceed a predefined request rate, protecting your application from potential denial-of-service attacks.
Access Google Cloud Console: Log in to your Google Cloud Console.
Navigate to Google Cloud Armor: Go to the "Security" section and select "Google Cloud Armor".
Create Security Policy: Create a new security policy or edit an existing one. Add a new rule to the policy.
Configure Rate-Based Ban: Set the action to rate_based_ban. Define the rate limit (e.g., requests per second) and set the ban_duration_sec parameter to the desired time interval.
Apply the Policy: Apply the security policy to your backend service or load balancer.
Monitor and Adjust: Monitor the traffic patterns and adjust the rate limits and ban durations as necessary to balance security and availability.
References:
Google Cloud Armor Documentation
Rate Limiting with Cloud Armor

質問: **107**
ある企業は、アナリストと管理者の両方が共有する 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必要があります。PII を含むログ ファイルは、管理者だけ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。
あなたは何をするべきか？
A. Cloud Pub/Sub と Cloud Functions を使用して、ファイルが共有バケットに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 PII が検出された場合は、管理者のみがアクセスできる Cloud Storage バケットに関数を移動します。
B. 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ログを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。PII を含む共有バケットからすべてのファイルを削除するようにトリガーを構成します。
C. アナリストと管理者の両方が共有するバケットで、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が共有するバケットで、PII データがアップロードされたときにのみトリガーされる Cloud Storage トリガーを構成します。Cloud Functions を使用してトリガーをキャプチャし、そのようなファイルを削除します。
正解: **(**正解を表示します**)**
To ensure that PII data is separated from non-PII data, using Cloud Pub/Sub and Cloud Functions to trigger a scan by the Data Loss Prevention (DLP) API is an effective approach. This method allows for automated detection and handling of PII.
Steps:
* Set Up Cloud Pub/Sub: Configure a Cloud Pub/Sub topic to receive notifications whenever a file is uploaded to the shared Cloud Storage bucket.
* Deploy Cloud Functions: Create a Cloud Function that is triggered by the Pub/Sub topic. This function will invoke the DLP API to scan the uploaded file for PII.
* Move Detected PII Files: If the scan detects PII, the Cloud Function will move the file to a secure Cloud Storage bucket accessible only by the administrator.
* Set Permissions: Ensure that appropriate permissions are set on the Cloud Storage buckets to restrict access to files containing PII.
References:
Google Cloud: Data Loss Prevention
Cloud Functions documentation

質問: **108**

Compute Engine でホストされている 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。資格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。あなたは何をするべきか？
A. クラスター専用の Cloud Identity ユーザー アカウントを作成します。ユーザーの一時的な資格情報を保存するには、強力な自己ホスト型のコンテナー ソリューションを使用します。
B. クラスター専用の 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 アカウントを作成する 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 アカウントを作成する 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。
正解: **(**正解を表示します**)**
Disable service account key creation You can use the iam.disableServiceAccountKeyCreation boolean constraint to disable the creation of new external service account keys. This allows you to control the use of unmanaged long-term credentials for service accounts. When this constraint is set, user-managed credentials cannot be created for service accounts in projects affected by the constraint.
https://cloud.google.com /resource-manager/docs/organization-policy/restricting-service-accounts#example_policy_boolean_constraint

質問: **109**
あなたは、Google Cloud コンソールのログイン アクティビティ イベントと、Google Cloud リソースの構成を変更する API 呼び出しのセキュリティ ログをエクスポートして監査する任務を負っています。エクスポートは次の要件を満たす必要があります。
Google Cloud 組織内のすべてのプロジェクトの関連ログをエクスポートします。
ログをほぼリアルタイムで外部 SIEM にエクスポートします。
あなたは何をするべきか？ 2つ選んでください。）
A. Pub/Sub 宛先を使用して、組織レベルでログ シンクを作成します。
B. includeChildren パラメータを使用して組織レベルでログ シンクを作成し、送信先を Pub/Sub トピックに設定します。
C. 組織レベルでデータ アクセス監査ログを有効にして、すべてのプロジェクトに適用します。
D. 管理コンソールで Google Workspace 監査ログを Google Cloud と共有できるようにします。
E. SIEM が監査ログ エントリの AuthenticationInfo フィールドを処理して ID 情報を収集することを確認します。
正解: **(**正解を表示します**)**

To meet the requirements for exporting and auditing security logs in near real-time for login activity events and API calls:
Organization-Level Log Sink with Pub/Sub: Create a log sink at the organization level to ensure logs from all projects are captured. Use the includeChildren parameter to include logs from all child resources (projects).
Set the destination to a Pub/Sub topic to facilitate near real-time log export to an external SIEM.
Enable Data Access Audit Logs: Enable Data Access audit logs at the organization level to capture and export detailed information about API calls that modify configurations of Google Cloud resources across all projects.
These steps ensure comprehensive logging and real-time export capabilities, which are crucial for security auditing and monitoring.
References
Audit Logs Overview
Exporting with Sinks

質問**: 110**
2 つのネットワーク セグメントを設定する必要があります。1 つは信頼されていないサブネットで、もう 1 つは信頼されているサブネットです。
次世代ファイアウォール (NGFW) などの仮想アプライアンスを構成して、2 つのネットワーク セグメント間のすべてのトラフィックを検査したいと考えています。トラフィックを検査するには、ネットワークをどのように設計する必要がありますか?
A. 1. 1 つの VPC に 2 つのサブネット (信頼できるサブネットと信頼できないサブネット) を設定します。
2. 仮想アプライアンスを指すすべてのトラフィック (0.0.0.0/0) のカスタム ルートを構成します。
B. 1. 1 つの VPC に 2 つのサブネット (信頼できるサブネットと信頼できないサブネット) を設定します。
2. 仮想アプライアンスを指すすべての RFC1918 サブネットのカスタム ルートを構成します。
C. 1. 信頼できるネットワークと信頼できないネットワークの 2 つの VPC ネットワークを設定し、それらをピアリングします。
2. 仮想アプライアンスを指す各ネットワークでカスタム ルートを構成します。
D. 1. 信頼できるネットワークと信頼できないネットワークの 2 つの VPC ネットワークをセットアップします。
2. 複数のネットワーク インターフェースを使用して仮想アプライアンスを構成し、各インターフェースを VPC ネットワークの 1 つに接続します。
正解**: D (**コメントを発表する**)**
Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to

one of the VPC networks. Internet and on-premises connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.
https://cloud.google.com/architecture/best-practices-vpc-design#l7
This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

質問**: 111**
あなたの組織では、Model Gardenを使用して、複数のモデルを一元管理し、異なる種類のモデルを一貫した方法でデプロイしています。ユーザーが承認されたモデルのみにアクセスでき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. 特定のモデルへのアクセスを制限するために、個々の Model Garden に対して IAM 権限を設定します。
B. Vertex AI のユーザー アクティビティ ログを定期的に監査し、承認されていないモデルへのアクセスを識別して取り消します。
C. Vertex AI プロジェクト内でカスタム モデルをトレーニングし、これらのモデルへのユーザー アクセスを制限します。
D. vertexai.allowedModels 制約を制限する組織ポリシーを実装します。
正解**: (**正解を表示します**)**
To centrally govern and restrict which AI models (from the Model Garden) can be used within an organization, Google Cloud provides a specific Organization Policy Constraint.9
According to Google Cloud Documentation (Vertex AI Organization Policy Constraints):
"The constraints/vertexai.allowedModels constraint allows you to define a list of allowed models that can be deployed or used within your organization. This includes Google first-party models, open-source models, and third-party models available in the Model Garden.10
By using this policy, you can prevent users from using unvetted or non-compliant models even if they have IAM permissions to use Vertex AI." How it works:
* You define an "Allowlist" of model IDs.
* When a user attempts to deploy a model or call an API for a model not on the list, the request is blocked.
* This is the most scalable and compliant way to manage AI governance.
Why other options are incorrect:
* A is incorrect: Model Garden is a catalog; you cannot apply granular IAM permissions to individual entries within the public catalog itself in the same way you can restrict API usage via Org Policy.

* B is incorrect: Auditing is reactive. The requirement is to ensure users can only access approved models (prevention).
Reference:
Google Cloud Documentation: "Vertex AI organization policy constraints" (https://cloud.google.com/vertex-ai/docs/general/org-policies).

質問**: 112**
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. 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ます。
C. 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。
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。
正解**: (**正解を表示します**)**
To remove personally identifiable information (PII) from files older than 12 months and archive the anonymized files for retention purposes, you can use Google Cloud Data Loss Prevention (DLP).
Create a Cloud DLP Inspection Job:
Go to the Cloud DLP section in the Google Cloud Console.
Create an inspection job that scans files in your Cloud Storage bucket for PII.
Configure the job to only target files that are older than 12 months.
Configure De-identification:
In the inspection job settings, configure de-identification actions to remove or obfuscate PII in the files.
Specify the transformation techniques appropriate for your data, such as masking or tokenization.
Archive Anonymized Files:
Set up the job to move the de-identified files to another Cloud Storage bucket designated for archival.
Ensure this bucket has the appropriate retention policies and access controls in place.

Delete Original Files:
After de-identification and archiving, configure the job to delete the original files from the source bucket.
This approach ensures that PII is effectively removed from old files and that the anonymized data is securely archived, maintaining compliance with data retention and privacy policies.
Cloud Data Loss Prevention Documentation
Setting Up DLP Jobs
Cloud Storage Documentation

質問**: 113**
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ごとに、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、サード パーティの ID 管理プロバイダーでユーザー ID を維持し、シングル サインオンを利用する必要があります。かなりの数のユーザーが会社のドメインのメール アドレスを個人の Google アカウントに使用していることがわかったので、Google の推奨される方法に従って、既存の管理対象外ユーザーを管理対象アカウントに変換する必要があります。
どの 2 つのアクションを実行する必要がありますか? 2つ選んでください。）
A. Google Cloud Directory Sync を使用して、ローカル ID 管理システムを Cloud Identity に同期します。
B. Google 管理コンソールを使用して、再設定用メールに個人アカウントを使用している管理対象ユーザーを表示します。
C. 管理対象の Google アカウントにユーザーを追加し、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ユーザーに強制します。
D. 管理対象外ユーザー用移行ツール (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. すべての従業員に電子メールを送信し、会社の電子メール アドレスを持つユーザーに個人の Google アカウントをすぐに削除するよう依頼します。
正解**: (**正解を表示します**)**
To manage user accounts and ensure they comply with corporate policies, using Google Cloud Directory Sync (GCDS) allows synchronization between your local identity system and Cloud Identity. The Transfer Tool for Unmanaged Users (TTUU) helps identify and manage conflicting accounts by allowing users to transfer their personal accounts to managed accounts.
Steps:
* Synchronize Identities: Use GCDS to sync users from your local identity management system to Cloud Identity, ensuring that all corporate user accounts are managed.
* Identify Conflicting Accounts: Use TTUU to find users who have personal Google accounts using corporate email addresses.
* Manage Conflicting Accounts: Request users to transfer their personal accounts to managed accounts using TTUU, ensuring all accounts are under corporate control.

References:
Google Cloud Directory Sync
Transfer Tool for Unmanaged Users

質問: **114**
アプリケーションは多くの場合、ビルド時または実行時に機密データの小さな断片である「シークレット」へのアクセスを必要とします。GCP でこれらのシークレットを管理する管理者は、「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。GCP プロジェクト内。
管理者が探している情報を提供する 2 つのログ ストリームはどれですか? 2つ選んでください。）
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
正解: **(**正解を表示します**)**
To keep track of "who did what, where, and when?" within GCP projects, the administrator should focus on Admin Activity logs and Data Access logs. Here's a detailed explanation of why these two log streams are essential:
* Admin Activity Logs:
* These logs capture administrative actions performed in your Google Cloud resources. This includes actions like creating, modifying, or deleting resources.
* Admin Activity logs provide detailed information about the user who performed the action, the resource that was affected, the action performed, and the timestamp.
* Data Access Logs:
* These logs capture read and write operations on data within your Google Cloud services. This includes actions like accessing or modifying data stored in databases, storage buckets, etc.
* Data Access logs help track the access patterns of users and services to sensitive data, providing insights into who accessed which data and when.
Steps to Enable and Access Logs:
* Navigate to the Google Cloud Console.
* Go to Logging in the left-hand menu.
* Enable Admin Activity and Data Access logs if not already enabled.
* Use Logs Explorer to filter and view specific logs based on your requirements.
By monitoring both Admin Activity and Data Access logs, administrators can gain comprehensive visibility into the actions performed on their GCP resources and data, ensuring robust security and compliance tracking.
Google Cloud Logging Documentation

Audit Logs Overview

質問**: 115**
あなたは、Google Cloud 上のパブリック アプリケーションに対する一般的なウェブ 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。これらのポリシーの変更を適用する前に検証する必要があります。どのサービスを使用する必要がありますか?
A. プレビュー モードでの Google Cloud Armor の事前構成済みルール
B. 監視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) 固有の保護機能
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
正解**: (**正解を表示します**)**
* Objective: Implement external web application protection and validate policy changes before enforcement.
* Solution: Use Google Cloud Armor's preconfigured rules in preview mode.
* Steps:
* Step 1: Open the Google Cloud Console.
* Step 2: Navigate to the Google Cloud Armor section.
* Step 3: Create or select a security policy.
* Step 4: Apply preconfigured rules to the policy.
* Step 5: Enable preview mode to simulate the effects of the rules without enforcing them.
* Step 6: Monitor the logs to validate the policy changes.
Google Cloud Armor's preview mode allows you to test and validate the impact of security policies on your application traffic before applying them, ensuring that they work as intended without disrupting the service.
References:
Google Cloud Armor Documentation
Using Preview Mode

質問**: 116**
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。データの流出を防ぐため、BigQueryテーブルへのクエリは、承認された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。
正解: **(**正解を表示します**)**
Enable VPC Service Controls:
VPC Service Controls help mitigate the risk of data exfiltration by allowing you to define a security perimeter around GCP resources.
Set up a service perimeter around your BigQuery project to restrict data access to within the defined perimeter.
Create Access Levels:
In the Google Cloud Console, navigate to the Access Context Manager.
Define access levels based on IP address conditions, specifying the authorized source IP addresses that are allowed to access your BigQuery resources.
These access levels are used to enforce policies that restrict who can access your sensitive data based on their IP addresses.
Apply Service Perimeter with Access Levels:
Apply the created access levels to the service perimeter to ensure that only requests originating from the specified IP addresses are able to access BigQuery tables.
This setup ensures that the sensitive PII data is not accessible from unauthorized IP addresses, reducing the risk of data exfiltration.
References:
VPC Service Controls
Access Context Manager
Defining Access Levels

質問: **117**
組織ではGoogle Workspace、Google Cloud、サードパーティのSIEMを使用しています。ユーザーログイン、ログイン成功、ログイン失敗などのイベントをSIEMにエクスポートする必要があります。ログはリアルタイムまたはほぼリアルタイムで取り込む必要があります。どうすればよいでしょうか？
A. Cloud Logging シンクを作成し、関連する認証ログを SIEM サブスクリプションの Pub/Sub トピックにエクスポートします。
B. gcloud ログ読み取りツールを使用して、Cloud Logging で認証イベントをポーリングします。イベントを SIEM に転送します。
C. サードパーティ SIEM の API エンドポイントにログを直接送信するように Google Workspace を構成します。
D. すべてのログのシンクとして Cloud Storage バケットを作成します。SIEM を設定して、バケット内の新しいログファイルを定期的にスキャンします。
正解: **A (**コメントを発表する**)**

The most efficient and recommended way to achieve real-time/near real-time ingestion of logs (including Google Workspace Audit Logs, which feed into Cloud Logging) to a third-party system is by using a Cloud Logging sink to a Pub/Sub topic.
Cloud Logging Sink: Creates a stream of logs filtered by type (e.g., authentication events).
Pub/Sub Topic: A messaging service that acts as a reliable, real-time message queue.
SIEM Subscription: The SIEM system can subscribe directly to the Pub/Sub topic, receiving log events as soon as they are published, meeting the real-time requirement.
Extracts:
"Cloud Logging sinks let you route logs to destinations like Cloud Storage, BigQuery, or Pub/Sub... Routing logs to Pub/Sub enables real-time streaming of log data for consumption by external services or applications, such as a third-party SIEM." (Source 7.1) Option B (polling) and Option D (Cloud Storage bucket) are batch-oriented methods, which do not meet the real-time/near real-time requirement.

質問**: 118**
臨床試験を実施している会社で、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。
正解**: (**正解を表示します**)**
"Date shifting techniques randomly shift a set of dates but preserve the sequence and duration of a period of time. Shifting dates is usually done in context to an individual or an entity. That is, each individual's dates are shifted by an amount of time that is unique to that individual."

質問**: 119**
組織のインフラストラクチャを GCP に移行する際、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、ユーザーを管理するための十分に確立された方法を既に持っており、既存の SSO パスワードと共に既存の Active Directory または LDAP サーバーを引き続き使用したいと考えています。
あなたは何をするべきか？
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 準拠の ID プロバイダーからの認証情報を使用して、GCP コンソール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 Console にログインします。
正解**: B (**コメントを発表する**)**
To allow a large number of users to access the GCP Console while keeping the existing Active Directory or LDAP server for identity management, use Google Cloud Directory Sync (GCDS).
Install GCDS:
Download and install Google Cloud Directory Sync from here.
Configure GCDS:
Set up the synchronization by specifying the LDAP server details and the Google domain.
Map the LDAP attributes to Google attributes to ensure user data is synchronized correctly.
Run Synchronization:
Perform an initial synchronization to populate the Google domain with existing users from the LDAP server.
Schedule regular synchronizations to keep the data up-to-date.
Benefits:
Automated Sync: Ensures that user data is consistently updated without manual intervention.
Secure Access: Users can log in to the GCP Console using their existing credentials, enhancing security and user experience.
Google Cloud Directory Sync Documentation
GCDS Administration Guide

質問**: 120**
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。
正解**: D (**コメントを発表する**)**

The immediate goal is to improve password security and enforce the change due to a recent event. This is done through the Google Workspace Admin console, which controls the identity provider for Google Cloud users.
Improve Password Security: The most effective control is to Enforce strong password policy, which requires users to use long, complex, and unguessable passwords, addressing the core security weakness.
Immediate Enforcement: Checking the option to Enforce password policy at the next sign-in ensures that all current users are immediately prompted to change their weak passwords to ones that meet the new strong policy requirements.
Option C is based on the outdated security practice of frequent password expiration, which often leads to users choosing weaker, predictable passwords (e.g., Spring2025 -> Summer2025). The modern recommendation is strong passwords and multi-factor authentication, not frequent expiration.
Option A is a detective control, not a preventative measure to improve password strength.
Extracts:
"In the Google Workspace Admin console, you can require users to use passwords that meet a strong password policy. A strong password must meet minimum complexity requirements, such as a minimum length and a mix of characters." (Source 6.1)
"After changing the password policy, you can select the option to Require all users to change their password at the next sign-in. This is the fastest way to enforce the new policy immediately across the organization." (Source 6.2)
"Google Cloud's recommended security best practice for identity is to prioritize strong passwords and Multi- Factor Authentication (MFA) over frequent password expiry." (Source 6.3)

質問**: 121**
Compute Engine でホストされている公開アプリケーションの停止について、ユーザーから報告を受けています。ファイアウォール ルールに対する最近の変更が原因であると思われます。ファイアウォール ルールが正しく機能しているかどうかをテストする必要があります。あなたは何をするべきか？
A. 変更された最新のルールでファイアウォール ルール ログを有効にします。ログ エクスプローラを使用して、ルールが正しく機能しているかどうかを分析します。
B. VPC の踏み台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. 運用前環境では、すべてのファイアウォール ルールを個別に無効にして、ユーザー トラフィックをブロックしているルールを特定します。
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。
正解**: (**正解を表示します**)**

Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly:
Enable Firewall Rules Logging for the specific firewall rules in question through the Google Cloud Console.
Once logging is enabled, use Logs Explorer to filter and review the firewall logs.
Analyze the logs to determine if the rules are allowing or blocking traffic as intended, identifying any misconfigurations or issues.
References:
Firewall Rules Logging
Using Logs Explorer

質問: **122**
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 Google Cloud 組織に適用する必要があります。現在、組織にはバケットがありません。運用上のオーバーヘッドを最小限に抑えてこの目標を達成するには、どのソリューションを事前に実装する必要がありますか?
A. 1 時間ごとの cron ジョブを作成して、パブリック バケットを見つけてプライベートにする Cloud Function を実行します。
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で 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境界に追加します。
正解: **(正解を表示します)**
https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public. If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

質問: **123**
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。
正解: **(正解を表示します)**
Google Cloud Logging supports Field-level access control, which allows you to hide specific sensitive fields within a log entry from certain users while still allowing them to see the rest of the log entry.5 This is achieved using Log Views and IAM.
According to Google Cloud Documentation (Configuring field-level access):
"Field-level access control allows you to restrict access to specific fields of LogEntry objects. You can define which fields are sensitive (such as principalEmail) and then grant the logging.fieldAccessor role to specific users or groups.6 Users without this role will see the log entry, but the sensitive fields will be redacted or omitted from their view." Key Implementation Steps:
* Identify Fields: Determine which paths in the JSON payload are sensitive.
* Define Access: Use a Log View to define the scope of logs and apply field-level restrictions.7
* Grant Permissions: Grant the standard logging.viewer role for general access and the logging.
fieldAccessor role ONLY to the security team for the specific sensitive fields.
Why other options are incorrect:
* B is incorrect: IAM conditions cannot natively parse and redact specific JSON fields within a log entry at the platform level; they are typically used for resource-level access.

* C is incorrect: While excluding fields via a sink works, it is "all or nothing." If you exclude it at the sink, no one (including the security team) will see that data in the destination.
* D is incorrect: This is a workaround that only works if the team uses BigQuery for logs. It doesn't solve the problem within the Cloud Logging Logs Explorer itself.
Reference:
Google Cloud Documentation: "Configure field-level access" (https://cloud.google.com/logging/docs/access- control#field-level-access).

質問**: 124**
金融サービス企業は、厳格なプライバシー規制を遵守しながら、顧客の個人識別情報（PII）を分析のために処理する必要があります。個人のプライバシーを保護するために、このデータを変換し、分析の整合性を確保するために、元の形式と一貫性を維持する必要があります。また、ソリューションでは、完全に元に戻せない削除を回避する必要があります。どうすればよいでしょうか？
A. フォーマット保持暗号化 (FPE) を使用して PII を匿名化するように機密データ保護 (SDP) を構成します。
B. Cloud Key Management Service (Cloud KMS) を使用して、顧客管理の暗号鍵 (CMEK) でデータセット全体を暗号化します。
C. JavaScript を使用してすべての機密フィールドをハッシュし、分析テーブルにロードする前に、カスタム BigQuery ユーザー定義関数 (UDF) を実装します。
D. BigQuery プロジェクトに VPC Service Controls を設定します。行レベルの暗号化を実装します。
正解**: (**正解を表示します**)**
The critical requirements are:
De-identify PII (protect individual privacy).
Retain original format and consistency (analytical integrity).
Avoid full irreversible deletion (the process must be reversible/re-identifiable).
Sensitive Data Protection (SDP), also known as Cloud DLP, is Google Cloud's specialized service for discovering, classifying, and de-identifying sensitive data. The specific de-identification technique that meets the need to retain the original format and consistency is Format-Preserving Encryption (FPE).
Extracts:
"Sensitive Data Protection supports several types of tokenization, including transformations that can be reversed, or 're-identified.'" (Source 5.3)
"Pseudonymization by replacing with cryptographic format preserving token (CryptoReplaceFfxFpeConfig)...
Preserves format... Reversible transformations can be reversed to re-identify the sensitive data using the content.reidentify method." (Source 5.3)
"Format Preserving Encryption (FPE) is an encryption algorithm that preserves the format of the original data set, but it replaces it with tokens that have no inherent meaning or value...

FPE ensures the ciphertext maintains the same format (length, number of hyphens, etc.) as the original plaintext." (Source 5.1) FPE is necessary for analytical integrity when the structure/format (e.g., 9-digit SSN, 16-digit credit card number) is required for processing in downstream systems.

質問**: 125**
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。
正解**: (**正解を表示します**)**
Physical Token for MFA: Implement multi-factor authentication (MFA) using physical tokens (such as security keys) for super admin accounts. This adds an extra layer of security to the highest privilege accounts.
Non-Privileged Identities: Provide super admins with separate non-privileged accounts for daily activities.
This practice minimizes the risk associated with using highly privileged accounts for routine tasks.
Account Management: Ensure that super admin accounts are only used for tasks requiring elevated privileges, reducing exposure to potential security threats. These measures enhance the security of super admin accounts, protecting your Google Cloud organization from unauthorized access. References:
Google Cloud - Best Practices for Securing Cloud Identity
Google Cloud - Using Security Keys

質問**: 126**
あなたは、規制が厳しく、積極的なコンプライアンスが求められる業界の金融機関で働いています。コンプライアンス要件を満たすには、特定の設定、データレジデンシー、組織ポリシー、そして人事データへのアクセス制御を継続的に維持する必要があります。どうすればよいでしょうか？
A. 定義された制御と要件を適用するために必要なコンプライアンス プログラム用の Assured Workloads フォルダーを作成します。

B. 必要なセキュリティコンプライアンス態勢を記述したposture.yamlファイルを作成します。Security Command Center Premiumで、gcloud sec postures create POSTURE_NAME --posture-from-file=posture.yamlコマンドを使用して、この態勢を適用します。
C. 組織レベルで組織ポリシー制約を適用して、新しいリソースが作成される場所を制限します。
D. Security Command Center のコンプライアンス ページに移動し、必要なコンプライアンス基準に対するステータスのレポートを表示します。定期的に違反をトリアージし、コンプライアンスを維持してください。
正解**: A (**コメントを発表する**)**
The key requirements are maintaining a specific set of controls, including data residency and personnel data access controls, specifically to meet a highly regulated industry's compliance program.
Assured Workloads is the specific Google Cloud service designed to help customers meet these stringent regulatory and compliance requirements (e.g., FINRA, FedRAMP, HIPAA, etc.) by enforcing a specific control bundle.
Extracts:
"Assured Workloads helps organizations run their sensitive workloads securely and in a compliant manner...
by providing continuous compliance monitoring for specific compliance programs." (Source 4.1)
"When you create an Assured Workloads folder, the platform automatically enforces compliance controls...
including: Data residency and location controls... Personnel access controls... Organizational policies..." (Source 4.2) This service creates a dedicated, compliant environment in a folder, ensuring the necessary configurations and personnel controls are applied automatically and continuously maintained, which is a more complete solution than the posture management in option B (which focuses only on configuration monitoring) or the singular organizational policy in option C.

質問**: 127**
ある企業が Google Kubernetes Engine でウェブショップを運営しており、BigQuery で顧客のトランザクションを分析したいと考えています。クレジット カード番号が BigQuery に保存されないようにする必要があります。
A. クレジット カード番号に一致する正規表現を使用して BigQuery ビューを作成し、影響を受ける行をクエリして削除します。
B. データが BigQuery に取り込まれる前に、Cloud Data Loss Prevention API を使用して、関連する infoType を秘匿化します。
C. Security Command Center を利用して、BigQuery でクレジット カード番号タイプのアセットをスキャンします。

D. Cloud Identity-Aware Proxy を有効にして、ログを BigQuery に保存する前にクレジットカード番号を除外します。
正解**: (**正解を表示します**)**
https://cloud.google.com/bigquery/docs/scan-with-dlp
Cloud Data Loss Prevention API allows to detect and redact or remove sensitive data before the comments or reviews are published. Cloud DLP will read information from BigQuery, Cloud Storage or Datastore and scan it for sensitive data.

質問**: 128**
社内には複数のチームがあり、それぞれ異なるプロジェクトのために、様々なGoogle Cloud データサービスにまたがる特定のデータセットにアクセスする必要があります。チームメンバーが各自のプロジェクトに関連するデータにのみアクセスできるようにし、BigQuery、Cloud Storage、Cloud SQL内の機密情報への不正アクセスを防止する必要があります。どうすればよいでしょうか？
A. 特定の Cloud IAM ロールを使用して、プロジェクトレベルのグループ権限を付与します。BigQuery の承認済みビューを使用します。Cloud Storage の均一なバケットレベルのアクセスと Cloud SQL データベース ロールを使用します。
B. これらのデータサービスを管理するユーザーの Google Cloud コンソールへのアクセスを制御するためのアクセスレベルを設定します。すべてのアクセス試行に対して多要素認証を必須にします。
C. VPC Service Controls を使用して、BigQuery、Cloud Storage、Cloud SQL サービスのプロジェクトの周囲にセキュリティ境界を作成し、リクエストのネットワーク オリジンに基づいてアクセスを制限します。
D. BigQuery、Cloud Storage、Cloud SQL のプロジェクトレベルのデータアクセス ログを有効にします。ログシンクを構成してこれらのログを Security Command Center にエクスポートし、不正なアクセス試行を特定します。
正解**: A (**コメントを発表する**)**
This question requires implementing fine-grained data access control across multiple services based on the Principle of Least Privilege.
Project/Service Access (IAM): Granting project-level group permissions with specific Cloud IAM roles (e.g., BigQuery Data Viewer) is the primary way to control who has access to which project's resources.
Data Isolation (Service-Specific): To ensure only relevant data is accessed and to protect sensitive information within the datasets, you must use the most granular control mechanism available for each service:
BigQuery: Authorized Views allow access to specific query results (subsets of data) without granting access to the underlying table.
Cloud Storage: Uniform bucket-level access simplifies and tightens security by forcing all access to be controlled by IAM, preventing accidental object-level exposure.

Cloud SQL: Database Roles are the native, most granular way to control access within the database itself (e.
g., read-only access to specific tables).
Extracts (Conceptual Basis):
"The principle of least privilege dictates that users should only have the permissions necessary to perform their jobs. Granular access is enforced using a combination of IAM roles and service-native access controls." (Source 5.1)
"For BigQuery, using authorized views is the standard way to limit data exposure to users who should only see a subset of data." (Source 5.2)

質問**: 129**
貴社では最近、機密性の高い顧客データを Cloud Storage バケットに移行しました。コンプライアンス上の理由から、Google 担当者によるベンダーデータへのアクセスと管理アクセスはすべてログに記録される必要があります。
何をすべきでしょうか?
A. Cloud Storage バケットをホストしているプロジェクトで、Cloud Storage のデータアクセス監査ログを構成します。
B. 組織のアクセスの透明性を有効にします。
C. 組織レベルで Cloud Storage のデータアクセス監査ログを構成します。
D. Cloud Storage バケットをホストしているプロジェクトのアクセスの透明性を有効にします。
正解**: (**正解を表示します**)**
The requirement to log access by Google personnel (e.g., Google administrators or support) is the specific function of Access Transparency.
Access Transparency logs provide records of actions taken by Google staff when they interact with your content, which is a requirement for many regulated industries. It is typically enabled at the Organization level to ensure consistent coverage, though it can be configured lower.
Extracts:
"Access Transparency logs provide records of actions taken by Google employees when accessing your data or configuration... Access Transparency allows you to monitor compliance with vendor access rules, including those for security and privacy." (Source 9.1)
"Access Transparency is enabled for all supported Google Cloud services across your organization when enabled at the organization level." (Source 9.2) Option A and C (Data Access logs) record customer/user access to data, but do not record actions taken by Google personnel.

質問**: 130**
組織では、最上位フォルダを使用してアプリケーション環境（本番環境と開発環境）を分離しています。開発者はすべてのアプリケーション開発監査ログを確認する必要がありますが、

本番環境のログを確認する権限はありません。セキュリティチームは、本番環境と開発環境のすべてのログを確認できます。開発者とセキュリティチームには、最小限の権限を確保しながら、適切なリソースレベルでIdentity and Access Management（IAM）ロールを付与する必要があります。
何をすべきでしょうか?
A. * 1 組織のリソース レベルでセキュリティ チームにログ記録および閲覧権限を付与します。
* 2 すべての開発プロジェクトを含むフォルダー リソース レベルで、開発チームにログ記録およびビューアの権限を付与します。
B. * 1 組織のリソース レベルでセキュリティ チームにログ記録権限を付与します。
* 2 組織リソース レベルで開発チームにログ記録管理者の役割を付与します。
C. * 1 組織リソース レベルでセキュリティ チームに logging.admin ロールを付与します。
* 2 すべての開発プロジェクトを含むフォルダー リソース レベルで、開発チームにログ記録とビューアのログ権限を付与します。
D. * 1 組織リソース レベルでセキュリティ チームに logging.admin ロールを付与します。
* 2 組織リソース レベルで開発チームに logging.admin ロールを付与します。
正解**: C (**コメントを発表する**)**
To ensure that the developers can view audit logs for the development environment and the security team can review all logs, you should grant IAM roles at the appropriate resource levels:
Grant logging.admin Role to the Security Team:
Assign the logging.admin role to the security team at the organization resource level.
This grants the security team full access to all logging data across the organization, including both production and development environments.
Grant logging.viewer Role to the Developer Team:
Assign the logging.viewer role to the developer team at the folder resource level that contains all the development projects.
This restricts the developers' access to only view logs in the development environment, ensuring they do not have access to production logs.
By using these roles and assigning them at the appropriate levels, you ensure that each team has the access they need while adhering to the principle of least privilege.
IAM Roles for Cloud Logging
Resource Hierarchy in Google Cloud

質問**: 131**
お客様のデータ サイエンス グループは、分析ワークロードに Google Cloud Platform (GCP) を使用したいと考えています。
会社のポリシーでは、すべてのデータは会社所有でなければならず、すべてのユーザー認証は独自の Security Assertion Markup Language (SAML) 2.0 ID プロバイダー (IdP) を経由する必要があると規定されています。インフラストラクチャ オペレーション システム エンジ

ニアは、お客様のために Cloud Identity を設定しようとしていたところ、お客様のドメインがすでに G Suite で使用されていることに気付きました。
混乱を最小限に抑えて作業を進めるには、システム エンジニアにどのようにアドバイスすればよいですか?
A. Google サポートに連絡し、ドメイン競合プロセスを開始して、新しい Cloud Identity ドメインでドメイン名を使用してください。
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. お客様の経営陣に、Google マネージド サービスの他の用途を発見するよう依頼し、既存のスーパー管理者と協力します。
正解**: (**正解を表示します**)**
Since the domain is already being used by G Suite, the best course of action is to minimize disruption by discovering any existing uses of Google-managed services. Collaborate with the existing Super Administrator to align the setup with the company's requirements.
Step-by-Step:
Identify Existing Usage: Have the customer's management identify all current uses of the domain within Google-managed services.
Collaboration: Work closely with the existing Super Administrator of the domain.
Provision Required Accounts: Ask the Super Administrator to provision necessary accounts and permissions for the data science manager or other relevant personnel.
Integrate SAML IdP: Ensure that the existing domain integrates with the company's SAML 2.0 IdP for user authentication.
Set Up Cloud Identity: Configure Cloud Identity under the guidance of the Super Administrator without disrupting current services.
Google Cloud Identity Administration
Google Support for Domain Issues

質問**: 132**
組織では、機密性の高い構造化データセットを処理するためにBigQueryを使用しています。「Need to Know」の原則に従い、これらのユーザーのニーズを満たすIdentity and Access Management（IAM）設計を作成する必要があります。
* ビジネス ユーザーは、キュレーションされたレポートにアクセスする必要があります。
* データ エンジニア: プラットフォーム内のデータ ライフサイクルを管理する必要があります。
* セキュリティ オペレーター: データ プラットフォーム上のユーザー アクティビティを確認する必要があります。
何をすべきでしょうか?
A. BigQuery サービスのデータ アクセス ログを構成し、セキュリティ オペレーターにプロジェクト閲覧者ロールを付与します。

B. ビジネス ユーザーのニーズに基づいて CSV データ ファイルを生成し、そのデータを電子メール アドレスに送信します。
C. 別のデータセットにキュレートされたテーブルを作成し、ロールに role/bigquery.dataViewer を割り当てます。
D. 「地域」列に基づいて行ベースのアクセス制御を設定し、データ エンジニア向けに米国からのレコードをフィルターします。
正解: **(**正解を表示します**)**
This option directly addresses the needs of the business user who must access curated reports. By creating curated tables in a separate dataset, you can control access to specific data. Assigning the roles/bigquery.
dataViewer role allows the business user to view the data in BigQuery.

質問: **133**
貴社では、個人情報(PII)を含む顧客データベースをGoogle Cloudに移行しています。偶発的な漏洩を防ぐため、このデータは保存時に保護する必要があります。あらゆる分析を行う前に、すべてのPIIが自動的に検出され、編集(または仮名化)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. Cloud Armor を実装してデータベースを外部の脅威から保護し、ファイアウォール ルールを構成してネットワーク アクセスを許可された内部 IP アドレスのみに制限します。
B. 定義済みおよびカスタムの infoType の両方を使用してデータベースをスキャンし、機密データをマスクするように機密データ保護を構成します。8
C. Cloud KMS を使用して、顧客管理の暗号鍵 (CMEK) で保存中のデータベースを暗号化します。
VPC サービス コントロールを実装します。
D. オブジェクトのバージョニングを有効にしたCloud Storageバケットを作成し、IAMポリシーを使用してデータへのアクセスを制限します。バケットに対してデータ損失防止 API(DLP API)を使用して機密データをスキャンし、検出アラートを生成します。9
正解: **(**正解を表示します**)**
For "automatic discovery, redaction, or pseudonymization" of sensitive data, the specific product is Sensitive Data Protection (formerly known as Cloud Data Loss Prevention - DLP).10 According to Google Cloud Documentation (Sensitive Data Protection Overview): "Sensitive Data Protection provides visibility into where PII exists in your organization. It allows you to automatically discover and classify data using over 150 predefined infoTypes (like SSN, Credit Card, etc.).
Beyond discovery, it can redact (remove), mask (cover), or pseudonymize (replace with a token) the data so that it can be used for analysis without exposing the raw PII." Why other options are incorrect:
* A is incorrect: Cloud Armor is a WAF; it doesn't scan data contents inside a database for PII.

* C is incorrect: Encryption (KMS) protects the data from unauthorized disk access, but once an authorized user opens the database, the PII is still visible. It doesn't perform "redaction" or
"pseudonymization."
* D is incorrect: While the DLP API is mentioned, this option focuses on Cloud Storage and alerts rather than the "redaction/pseudonymization" for analysis requested in the prompt. Option B is the comprehensive managed service approach.
Reference:
Google Cloud Documentation: "Sensitive Data Protection - De-identification" (https://cloud.google.com
/sensitive-data-protection/docs/de-identification).

質問**: 134**
大規模な電子小売業者は、e コマース ウェブサイトを Google Cloud Platform に移行しています。同社は、顧客がオンラインでチェックアウトするときに、顧客のブラウザと GCP の間で支払い情報が確実に暗号化されるようにしたいと考えています。
彼らは何をすべきですか？
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 で受信トラフィックを許可し、他のすべての受信トラフィックをブロックするようにファイアウォールを構成します。
D. ポート 443 でアウトバウンド トラフィックを許可し、他のすべてのアウトバウンド トラフィックをブロックするようにファイアウォールを構成します。
正解**: (**正解を表示します**)**
To ensure that payment information is encrypted between the customer's browser and Google Cloud Platform during checkout, the company should configure an SSL certificate on an L7 (Layer 7) Load Balancer. Here's why this is the best solution:
* SSL/TLS Termination: An L7 Load Balancer can handle SSL/TLS termination, which means it can decrypt HTTPS traffic, offloading the work from the backend servers. This is essential for handling encrypted connections securely.
* HTTPS Configuration: By configuring an SSL certificate, the load balancer ensures that all traffic between the customer's browser and the application is encrypted using HTTPS.
* Security Best Practices: Using an L7 Load Balancer with an SSL certificate aligns with best practices for securing web applications, particularly for e-commerce sites handling sensitive payment information.
* Managed Certificates: Google Cloud offers managed SSL certificates, which simplifies the process of obtaining, deploying, and renewing SSL certificates.
Implementation Steps:
* Obtain an SSL certificate.
* Configure the L7 Load Balancer in the GCP Console.

* Associate the SSL certificate with the load balancer.
* Ensure that the backend services are configured to handle HTTPS traffic.
Google Cloud Load Balancing Documentation
Setting up HTTPS Load Balancing

質問**: 135**
会社では最近、組織レベルで Security Command Center を有効化しました。本番環境フォルダ内のプロジェクト内のコンテナで実行されているアプリケーションに対して、ランタイム脅威検出を実装する必要があります。具体的には、実行中のコンテナ内で追加のライブラリがロードされたり、悪意のあるスクリプトが実行されたりした場合に通知を受け取る必要があります。この要件を満たすように Security Command Center を設定し、検出結果を Security Command Center 内で確実に表示でき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. 本番フォルダー内のコンテナーが、Container-Optimized OS を使用しているホスト上で実行されていることを確認します。
B. 本番環境フォルダ内のプロジェクトに対して、Security Command Center プレミアム レベルでコンテナ脅威検出を有効にします。
C. Security Command Center 内で Security Health Analytics を構成して、プロダクション フォルダー内のコンテナ ランタイムの脆弱性を監視します。
D. 本番環境フォルダ内の疑わしいコンテナ アクティビティについて、Cloud Logging と Cloud Monitoring でログベースの指標とアラートを作成します。
正解**: B (**コメントを発表する**)**
The requirements are runtime threat detection for containers that specifically detects activities like loading additional libraries or executing malicious scripts, with findings visible in Security Command Center (SCC).
Container Threat Detection (CTD) is the specific SCC service component designed to monitor container runtimes for suspicious events like reverse shells, suspicious library loading, and execution of malicious scripts. It is available only with the Security Command Center Premium tier.
Extracts:
"Container Threat Detection (CTD) is a Security Command Center Premium service that provides runtime threat detection for Google Kubernetes Engine (GKE) and Kubernetes clusters." (Source 4.1)
"CTD detects specific runtime events, such as: Execution of malicious scripts... Loading of suspicious libraries... CTD creates high-fidelity Security Command Center findings for these threats." (Source 4.2)
"Security Health Analytics (Option C) identifies misconfigurations and compliance violations, such as overly permissive IAM roles or open firewall ports, but it does not perform runtime threat detection." (Source 4.3) While using log-based metrics (Option D) is possible, enabling

CTD (Option B) is the specific, managed, and authoritative way to generate verified runtime threat findings directly within Security Command Center as required by the prompt.

質問: **136**
Google Cloud 環境内のフォルダのネットワーク トラフィックを制御しています。フォルダには複数のプロジェクトと Virtual Private Cloud (VPC) ネットワークが含まれています。フォルダレベルで、下り（外向き）接続を IP 範囲 10.58.5.0/24 に制限し、VPC ネットワーク dev-vpc からのみ接続できるようにしたいと考えています。実装とメンテナンスの労力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. * 1. スコープ内の VM に外部 IP アドレスを接続します。
* 2. このネットワーク内のすべての送信元アドレスに対して IP 範囲 10.58.5.0/24 への出力接続を許可する VPC ファイアウォール ルールを「dev-vpc」に設定します。
B. * 1. スコープ内の VM に外部 IP アドレスを接続します。
* 2. フォルダー レベルで階層型ファイアウォール ポリシーを定義および適用し、すべての出力接続を拒否し、ネットワーク dev-vpc から IP 範囲 10 58.5.0/24 への出力を許可します。
C. * 1. スコープ内の VM のネットワーク構成は変更しません。
* 2. 新しい VPC ネットワーク「new-vpc」を含む新しいプロジェクトを作成します。
* 3 「new-vpc」にネットワーク アプライアンスを展開して、アクセス要求をフィルタリングし、「dev-vpc」から 10.58.5.0/24 への出力接続のみを許可します。
D. * 1 スコープ内のVMのネットワーク構成を変更しない
* 2 「dev-vpc に対して Cloud NAT を有効にします」を選択し、Cloud NAT のターゲット範囲を 10.58.5 0/24 に制限します。
正解: **(**正解を表示します**)**
This approach allows you to control network traffic at the folder level. By attaching external IP addresses to the VMs in scope, you can ensure that the VMs have a unique, routable IP address for outbound connections.
Then, by defining and applying a hierarchical firewall policy at the folder level, you can enforce that egress connections are limited to the specified IP range and only from the specified VPC network.

質問: **137**
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。
正解: **(正解を表示します)**
This question combines two powerful security features: VPC Service Controls (VPC SC) for data exfiltration prevention and Context-Aware Access (CAA) for fine-grained user access based on context.
Contextual Requirement: Requiring a "company-managed device," "specific location," etc., is the function of Context-Aware Access (CAA), implemented via an Access Level.
Combining VPC SC and CAA: CAA policies can be integrated with VPC SC perimeters to enforce the context for access into the perimeter.
Evaluating Impact: To evaluate changes without blocking access, the entire VPC SC perimeter (including the new CAA rule) should be configured in dry run mode.
Extracts:
"Context-Aware Access (CAA) allows you to define and enforce granular access to Google Cloud resources based on user attributes like device security status, IP address (location), and identity." (Source 3.1)
"When implementing a new security policy... it is best practice to initially configure the VPC Service Controls perimeter (including any associated Access Levels/Context-Aware Access) in dry run mode. Dry run mode allows you to test the perimeter's effect on services without blocking any access." (Source 3.2)
"You can use an Access Level (the core component of CAA) to define the conditions for accessing resources protected by a Service Perimeter." (Source 3.3)

質問: **138**

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。
正解: **C,E (**コメントを発表する**)**
Google Cloud Directory Sync (GCDS): Install and configure GCDS to synchronize your on-premises Active Directory with Google Cloud Identity. This tool helps in maintaining consistency between your local directory and Google Cloud.
IAM Groups: Create IAM groups in Google Cloud with permissions that correspond to your Active Directory groups. This mapping ensures that users inherit the appropriate permissions based on their AD group membership.
Synchronization: Set up regular synchronization schedules to keep the user and group information up-to-date between your on-premises AD and Google Cloud.
Access Management: Use these IAM groups to manage access to Google Cloud resources, ensuring that permissions are applied consistently and securely. This approach leverages existing AD infrastructure for identity management, providing a seamless integration with Google Cloud. References:
Google Cloud - Google Cloud Directory Sync
Google Cloud - IAM Groups

質問: **139**
組織では Vertex AI Workbench インスタンスを使用しています。新しくデプロイされたインスタンスが自動的に最新の状態に保たれ、ユーザーが誤ってオペレーティング システムの設定を変更でき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. VM マネージャーを有効にし、対応する Google Compute Engine インスタンスが追加されていることを確認します。
B. 新しくデプロイされたインスタンスに対して、disableRootAccess および requireAutoUpgradeSchedule 組織ポリシーを適用します。
C. AI ワークベンチインスタンスのユーザーに AI Notebooks ランナーと AI Notebooks ビューアーのロールを割り当てます。

D. タグを使用して、対応する Google Compute Engine インスタンスへの Secure Shell アクセスを防止するファイアウォール ルールを実装します。
正解**: (**正解を表示します**)**
To ensure that Vertex AI Workbench Instances are automatically kept up-to-date and that users cannot alter operating system settings, implementing specific organization policies is essential.
* Option A: Enabling VM Manager and adding Compute Engine instances assists in managing and monitoring VM instances but does not enforce automatic updates or restrict user modifications to the operating system.
* Option B: Enforcing the disableRootAccess organization policy prevents users from gaining root access, thereby restricting unauthorized changes to the operating system. Additionally, the requireAutoUpgradeSchedule policy ensures that instances are automatically updated according to a defined schedule. Together, these policies maintain system integrity and compliance with update requirements.
* Option C: Assigning AI Notebooks Runner and AI Notebooks Viewer roles controls user permissions related to running and viewing notebooks but does not directly influence operating system settings or update mechanisms.
* Option D: Implementing firewall rules to prevent SSH access limits direct access to instances but does not ensure automatic updates or prevent alterations through other means.
Therefore, Option B is the most appropriate action, as it directly addresses both the enforcement of automatic updates and the prevention of unauthorized operating system modifications.
References:
Organization Policy Constraints
VM Manager Overview

質問**: 140**
CI/CD パイプラインを設定して、コンテナ化されたアプリケーションを Google Kubernetes Engine (GKE) の本番環境クラスタにデプロイしています。既知の脆弱性を持つコンテナーがデプロイされないようにする必要があります。ソリューションには次の要件があります。
クラウドネイティブである必要があります
費用対効果が高い必要があります
運用上の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る必要がありますか？ 2つ選んでください。）
A. Cloud Source Repositories リポジトリ内のコンテナ テンプレートへの変更をモニタリングする Cloud Build パイプラインを作成します。ビルドの続行を許可する前に、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 Function を使用して、Container Registry 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、既知の脆弱性について既存のリポジトリをスキャンし、準拠していないコンテナ イメージが見つかった場合にアラートを生成します。
D. GKE に Jenkins をデプロイし、CI/CD パイプラインを構成してコンテナを Container Registry にデプロイします。コンテナーをクラスターにデプロイする前に、コンテナー 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、脆弱性が見つからない場合は、コンテナー イメージに証明書を追加します。Binary Authorization ポリシーを使用して、クラスター内の構成証明のないコンテナーのデプロイをブロックします。
正解**: (**正解を表示します**)**
A). Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue:
Use Cloud Build to automate your CI/CD pipeline.
Integrate Container Analysis to scan container images for vulnerabilities during the build process.
If vulnerabilities are found, configure the build to fail, preventing deployment of insecure containers.
E). In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster:
Use Binary Authorization to enforce deploy-time security policies.
Configure your CI/CD pipeline to generate attestations for container images that pass vulnerability scans.
Binary Authorization will then block deployments of any containers without valid attestations, ensuring only secure images are deployed.
References:
Cloud Build Overview
Container Analysis
Binary Authorization

質問**: 141**
セキュリティ監査により、プロジェクトの Identity and Access Management (IAM) 構成にいくつかの不整合が見つかりました。一部のサービス アカウントに過度に許可されたロールがあり、少数の外部共同作業者には必要以上のアクセス権が与えられています。IAM ポリシー、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に対する変更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. OS Config Management エージェントを VM に導入します。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。

B. 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。
C. Cloud Audit Logs を使用するログ 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。
D. IAM ポリシーの変更によってトリガーされるように Google Cloud Functions を構成する。ポリシー シミュレータを使用して変更を分析し、リスクのある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する。
正解**: (**正解を表示します**)**
The problem requires gaining "detailed visibility into changes to IAM policies, user activity, service account behavior, and access to sensitive projects" due to security inconsistencies.
Cloud Audit Logs: Cloud Audit Logs records administrative activities, data access, and system events across Google Cloud. These logs are the primary source of truth for tracking "who did what, where, and when" in your Google Cloud environment.
Extract Reference: "Cloud Audit Logs maintains the following audit logs for each project, folder, and organization: Admin Activity audit logs, Data Access audit logs, System Event audit logs, Policy Denied audit logs." Extract Reference: "Admin Activity audit logs contain log entries for API calls or other actions that modify the configuration or metadata of resources. Data Access audit logs record API calls that read the configuration or metadata of resources, as well as user-provided data." (Google Cloud Documentation: "Cloud Audit Logs overview" - https://cloud.google.com/logging/docs/audit) These logs directly capture:Changes to IAM policies: Recorded in Admin Activity logs.
User activity: Recorded in Admin Activity and Data Access logs.
Service account behavior: Actions performed by service accounts are logged in the same way as user actions.
Access to sensitive projects: Data Access logs, especially for sensitive data services, record access events.
Log Export Sinks: To gain "detailed visibility" and enable "correlation with other event sources," these audit logs should be exported to a centralized Security Information and Event Management (SIEM) solution. Log sinks allow you to route logs from Cloud Logging to various destinations, including BigQuery, Cloud Storage, or Pub/Sub (which can then feed into a SIEM).
Extract Reference: "You can use sinks to route some or all of your logs to supported destinations." and "Many security information and event management (SIEM) systems can ingest logs through Cloud Pub/Sub." (Google Cloud Documentation: "Routing and storage overview | Cloud Logging" - https://cloud.google.com /logging/docs/routing-overview)
Let's evaluate the other options:

A). OS Config Management agent: This service manages operating system configurations, patching, and inventory on VMs. It is not designed to monitor or log IAM policy changes, user activity, or service account behavior within Google Cloud's IAM system.
B). Metrics Explorer in Cloud Monitoring: While Cloud Monitoring can provide some metrics related to service account authentication, it focuses on time-series data and operational health metrics. It does not provide the detailed, event-level audit records necessary for forensic analysis of IAM policy changes, specific user actions, or granular access events to sensitive data that Cloud Audit Logs offer.
D). Cloud Functions triggered by IAM policy changes + Policy Simulator: This describes a reactive automation pattern for some IAM changes. While useful for immediate alerting on risky modifications, it's a custom solution for a subset of the requirements. It doesn't inherently provide "detailed visibility" into all user activity or comprehensive service account behavior across all projects, nor does it replace the robust logging and correlation capabilities of a SIEM solution ingesting raw audit logs. Cloud Audit Logs are the fundamental data source this approach would rely on.
Therefore, leveraging Cloud Audit Logs and exporting them to a SIEM is the most comprehensive and recommended approach for gaining detailed visibility into IAM-related changes and activities across your Google Cloud organization.

質問**: 142**
Compute Engine インスタンスで実行されているアプリケーションは、Cloud Storage バケットからデータを読み取る必要があります。あなたのチームは、Cloud Storage バケットをグローバルに読み取り可能にすることを許可しておらず、最小権限の原則を確保したいと考えています。
あなたのチームの要件を満たすオプションはどれですか?
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資格情報なしでバケットから読み取ることを許可する Cloud Storage ACL を作成します。
B. Cloud Storage バケットへの読み取り専用アクセス権を持つサービス アカウントを使用し、Compute Engine インスタンスのアプリケーションの構成にあるサービス アカウントへの認証情報を保存します。
C. Cloud Storage バケットへの読み取り専用アクセス権を持つサービス アカウントを使用して、インスタンス メタデータから認証情報を取得します。
D. Cloud KMS を使用して Cloud Storage バケット内のデータを暗号化し、アプリケーションが KMS 鍵を使用してデータを復号できるようにします。
正解**: C (**コメントを発表する**)**
If the environment variable GOOGLE_APPLICATION_CREDENTIALS is set, ADC uses the service account key or configuration file that the variable points to. If the environment variable GOOGLE_APPLICATION_CREDENTIALS isn't set, ADC uses the service account

that is attached to the resource that is running your code.
https://cloud.google.com/docs/authentication
/production#passing_the_path_to_the_service_account_key_in_code