SAP.C_TS413_2020.v2023-11-27.q111

試験コード:	C_TS413_2020
試験名称:	SAP Certified Application Associate - SAP S/4HANA Asset Management
認定資格:	SAP
無料問題数:	111
バージョン:	v2023-11-27
アクセス数:	487
ページビュー数:	1110
https://www.jpnpdf.com/SAP.C_TS413_2020.v2023-11-27.q111-mondaishu.html	

最新問題: **1**
2 つの Cloud Router を設定して、1 台がアクティブなボーダー ゲートウェイ プロトコル (BGP) セッションを持ち、もう 1 台がスタンバイとして機能するようにしたいと考えています。
オンプレミスルーターではどの BGP 属性を使用する必要がありますか?
A. AS パス
B. コミュニティ
C. ローカル設定
D. 多重出口識別器
Answer: (解答を表示する**)**
https://cloud.google.com/router/docs/concepts/overview

最新問題: **2**
あなたのソフトウェア チームは、RFC 1918 アドレス空間を使用して GCP の Compute Engine インスタンスに直接接続する必要があるオンプレミス ウェブ アプリケーションを開発しています。次の仕様を考慮して、オンプレミス環境から GCP への接続ソリューションを選択したいと考えています。
ISP は Google Partner Interconnect プロバイダーです。
オンプレミス VPN デバイスのインターネットのアップリンクおよびダウンリンク速度は 10 Gbps です。
オンプレミス ゲートウェイと GCP 間のテスト VPN 接続は、パケット損失により最大 500 Mbps で実行されています。
データ転送のほとんどは、GCP からオンプレミス環境へ行われます。
アプリケーションは、インターコネクト経由のピーク転送中に最大 1.5 Gbps までバーストできます。
ソリューションのコストと複雑さは最小限に抑える必要があります。
接続ソリューションをどのようにプロビジョニングする必要がありますか?
A. ISP を通じて Partner Interconnect をプロビジョニングします。
B. VPN の代わりに専用相互接続をプロビジョニングします。
C. パケット損失を考慮して複数の VPN トンネルを作成し、ECMP を使用して帯域幅を増やします。
D. VPN 経由でネットワーク圧縮を使用して、VPN 経由で送信できるデータ量を増やします。
Answer: A (メーッセージを残す**)**

直接相互接続は高価すぎるため、この要件には過剰になります。パケット損失を考慮した複数のトンネルの管理も複雑です。一方、パートナー インターコネクトは、必要な帯域幅を提供するという要件に適合しますが、非常に高価ではなく、セットアップが完了すれば管理もそれほど複雑ではありません。

最新問題**: 3**
インスタンス グループを作成しているため、HTTP(s) ロード バランシング用の新しいヘルス チェックを作成する必要があります。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
A. gcloud コマンドライン ツールを使用して新しいヘルスチェックを作成します。
B. GCP Console の [VPC ネットワーク] セクションを使用して、新しいヘルスチェックを作成します。
C. GCP Console でロードバランサのバックエンド構成を完了したら、新しいヘルスチェックを作成するか、既存のヘルスチェックを選択します。
D. gcloud コマンドライン ツールを使用して、新しいレガシー ヘルスチェックを作成します。
E. GCP Console の [ヘルス チェック] セクションを使用して、新しいレガシー ヘルスチェックを作成します。
Answer: A,E (メーッセージを残す**)**
参照：
https://cloud.google.com/load-balancing/docs/health-checks

最新問題**: 4**
プロジェクト内のすべてのインスタンスは、カスタム メタデータのenable-oslogin 値が FALSE に設定され、プロジェクト全体の SSH キーをブロックするように構成されています。どのインスタンスにも SSH キーが設定されておらず、プロジェクト全体の SSH キーも設定されていません。ファイアウォール ルールは、任意の IP アドレス範囲からの SSH セッションを許可するように設定されています。1 つのインスタンスに SSH 接続したいとします。
あなたは何をするべきか？
A. 新しい SSH キー ペアを生成します。秘密キーの形式を確認し、インスタンスに追加します。Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
B. 新しい SSH キー ペアを生成します。公開キーの形式を確認し、プロジェクトに追加します。Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
C. gcloud compute ssh を使用してインスタンスへの Cloud Shell SSH を開きます。
D. カスタム メタデータのenable-oslogin を TRUE に設定し、Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
Answer: C (メーッセージを残す**)**

最新問題**: 5**
オンプレミス ネットワークに接続するように Google Cloud 環境を構成しています。構成では、プライベート Cloud Interconnect ネットワークを介して Cloud Storage API と Google Kubernetes Engine ノードにアクセスできる必要があります。相互接続 VLAN アタッチメントを使用して Cloud Router をすでに構成しています。次に、Cloud Router 上で適切なルーター アドバタイズメント構成を設定する必要があります。あなたは何をするべきか？
A. ルート アドバタイズメントをカスタム設定に構成し、プレフィックス 199.36.153.8/30 を手動でアドバタイズメントのリストに追加します。他のオプションはすべてデフォルト設定のままにしておきます。
B. ルート広告をカスタム設定に構成し、広告のリストにプレフィックス 199.36.153.8/30 を手動で追加します。表示されているすべてのサブネットを Cloud Router にアドバタイズします。
C. ルート広告をデフォルト設定にします。

D. オンプレミス ルーターで、Cloud Router のリンクローカル IP アドレスを指すストレージ API 仮想 IP アドレスの静的ルートを構成します。
Answer: (解答を表示する**)**

最新問題**: 6**
最近、デフォルトのルーティング構成を使用して、Virtual Private Cloud (VPC) 内のリージョン us-west1 と us-east1 に Compute Engine インスタンスをデプロイしました。会社のセキュリティ ポリシーでは、仮想マシン (VM) にパブリック IP アドレスを接続してはならないと規定しています。外部アクセスを防止しながら、インスタンスがインターネットから更新を取得できるようにする必要があります。あなたは何をするべきか？
A. 宛先 0.0.0.0/0 への送信を許可するファイアウォール ルールを作成します。
B. VPC 内に単一のグローバル Cloud NAT ゲートウェイとグローバル Cloud Router を作成します。
C. インスタンスのネットワーク インターフェイスの外部 IP アドレスを [なし] から [エフェメラル] に変更します。
D. us-west1 と us-east1 の両方に Cloud NAT ゲートウェイと Cloud Router を作成します。
Answer: D (メーッセージを残す**)**

最新問題**: 7**
組織には、複数の Virtual Private Cloud (VPC) を含む 1 つのプロジェクトがあります。企業のパブリック ネットワーク内のリソースからのみ API アクセスを許可することで、Cloud Storage バケットと BigQuery データセットへの API アクセスを保護する必要があります。あなたは何をするべきか？
A. 企業のパブリック ネットワークの IP 範囲を許可するアクセス コンテキスト ポリシーを使用して、VPC ごとに VPC Service Controls 境界を作成します。
B. ファイアウォール ルールを作成して、未承認のネットワークから Cloud Storage と BigQuery への API アクセスをブロックします。
C. 企業のパブリック ネットワークの IP 範囲を許可するアクセス コンテキスト ポリシーを使用して、プロジェクトの VPC Service Controls 境界を作成します。
D. VPC と企業のパブリック ネットワークの IP 範囲を許可するアクセス コンテキスト ポリシーを作成し、そのポリシーを Cloud Storage と BigQuery にアタッチします。
Answer: C (メーッセージを残す**)**

最新問題**: 8**
プロジェクト内のすべてのインスタンスは、カスタム メタデータのenable-oslogin 値が FALSE に設定され、プロジェクト全体の SSH キーをブロックするように構成されています。どのインスタンスにも SSH キーが設定されておらず、プロジェクト全体の SSH キーも設定されていません。ファイアウォール ルールは、任意の IP アドレス範囲からの SSH セッションを許可するように設定されています。1 つのインスタンスに SSH 接続したいとします。
あなたは何をするべきか？
A. gcloud compute ssh を使用してインスタンスに Cloud Shell SSH を開きます。
B. カスタム メタデータのenable-oslogin を TRUE に設定し、Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
C. 新しい SSH キー ペアを生成します。秘密キーの形式を確認し、インスタンスに追加します。
Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
D. 新しい SSH キー ペアを生成します。公開キーの形式を確認し、プロジェクトに追加します。
Putty や ssh などのサードパーティ ツールを使用してインスタンスに SSH 接続します。
Answer: B (メーッセージを残す**)**
https://cloud.google.com/compute/docs/storing-retrieving-metadata

最新問題: **9**
あなたは最近、組織の ID とアクセス管理の管理を任されました。いくつかのプロジェクトがあり、可能な限りスクリプトと自動化を使用したいと考えています。プロジェクト メンバーに編集者の役割を付与したいと考えています。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
A. [メンバーの追加] フィールドにメール アドレスを入力し、GCP Console のドロップダウン メニューから目的のロールを選択します。
B. REST API 経由の setIamPolicy()
C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername --role ロール/エディター
D. gcloud プロジェクト add-iam-policy-binding Sprojectname --member user:Susername --role ロール/エディター
E. REST API 経由の GetIamPolicy()
Answer: A,D (メーッセージを残す**)**

最新問題: **10**
あなたの会社は最近、EMEA ベースの事業を APAC に拡大しました。世界中に分散しているユーザーから、SMTP サービスと IMAP サービスが遅いと報告されています。あなたの会社ではエンドツーエンドの暗号化が必要ですが、SSL 証明書にアクセスできません。
どの Google Cloud ロードバランサを使用する必要がありますか?
A. HTTPS ロードバランサ
B. ネットワークロードバランサー
C. SSL プロキシ ロード バランサ
D. TCP プロキシ ロード バランサ
Answer: C (メーッセージを残す**)**

最新問題: **11**
オンプレミス データセンターには 2 つのルーターがあり、各ルーターの VPN を介して GCP に接続されています。すべてのアプリケーションは正しく動作しています。ただし、すべてのトラフィックは、必要に応じて 2 つの接続間で負荷分散されるのではなく、単一の VPN を通過します。
トラブルシューティング中に次のことがわかります。
* 各オンプレミス ルーターは同じ ASN で構成されます。
* 各オンプレミス ルーターは同じルートと優先度で構成されます。
* 両方のオンプレミス ルーターは、単一の Cloud Router に接続された VPN で構成されています。
* VPN 接続時の VPN ログには、提案が選択されていない行が表示されます。
* 1 台のオンプレミス ルーターと Cloud Router の間に BGP セッションが確立されていません。
この問題の最も考えられる原因は何ですか?
A. オンプレミス ルーターと Cloud Router の両方の間で BGP セッションが確立されていません。
B. VPN セッションの 1 つが正しく構成されていません。
C. ネットワーク トラフィックの負荷分散を行うロード バランサーがありません。
D. ファイアウォールが 2 番目の VPN 接続を介したトラフィックをブロックしています。
Answer: C (メーッセージを残す**)**

最新問題: **12**
オンプレミス ネットワーク ブロックと GCP の間でアドレス変換を実行するように NAT を構成したいと考えています。

どの NAT ソリューションを使用する必要がありますか?
A. クラウド NAT
B. IP 転送が有効になっているインスタンス
C. iptables DNAT ルールで構成されたインスタンス
D. iptables SNAT ルールで構成されたインスタンス
Answer: A (メーッセージを残す**)**
https://cloud.google.com/nat/docs/overview

最新問題**: 13**
あなたの会社では、同じ組織内で別々の GCP プロジェクトを担当する 2 つの部門 (コード開発とデータ開発) が、GCP 内のすべての仮想マシン間で完全な相互通信を許可する必要があります。各部門はプロジェクト内に 1 つの VPC を持ち、ネットワークを完全に制御したいと考えています。どちらの部門も、既存のコンピューティング リソースを再構築するつもりはありません。コストを最小限に抑えるソリューションを実装したいと考えています。
どの 2 つのステップを実行する必要がありますか? (2つお選びください。)
A. Cloud VPN を使用して両方のプロジェクトを接続します。
B. code-dev プロジェクトでプロジェクト data-dev の宛先プレフィックスへのルートを作成し、ネクストホップをデフォルト ゲートウェイとして使用します (その逆も同様)。
C. VPC ネットワーク ピアリングを使用して、プロジェクト code-dev と data-dev の VPC を接続します。
D. ファイアウォール ルールを有効にして、プロジェクト code-dev のすべてのサブネットからプロジェクト data-dev のすべてのインスタンスへのすべての受信トラフィック (またはその逆) を許可します。
E. 1 つのプロジェクト (例: code-dev) で共有 VPC を有効にし、2 番目のプロジェクト (例: data-dev) をサービス プロジェクトにします。
Answer: (解答を表示する**)**

最新問題**: 14**
gsutil ツールと Google への 10 Gbps ダイレクト ピアリング接続を使用して、オンプレミス サーバーから Cloud Storage バケットにファイルをアップロードしています。オンプレミス サーバーは、Google ピアリング ポイントから 100 ミリ秒離れています。アップロードでは、利用可能な 10 Gbps 帯域幅をすべて使用していないことがわかります。接続の帯域幅使用率を最適化したいと考えています。
オンプレミスのサーバーでは何をすべきでしょうか?
A. オンプレミス サーバーの TCP パラメーターを調整します。
B. tar などのユーティリティを使用してファイルを圧縮し、送信されるデータのサイズを削減します。
C. gsutil コマンドから -m フラグを削除して、シングルスレッド転送を有効にします。
D. gsutil コマンドで perfdiag パラメータを使用して、パフォーマンスを高速化します: gsutil perfdiag gs://[バケット名]。
Answer: A (メーッセージを残す**)**
https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid
https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid https://cloud.google.com/blog/products/gcp/5-steps-to -better-gcp-ネットワークパフォーマンス?hl=ml

最新問題**: 15**
セキュリティ チームは、GCP の本番環境仮想マシンへの外部 SSH アクセスを無効にしました。
運用チームは、VM およびその他のリソースをリモートで管理する必要があります。彼らに何ができるでしょうか？

A. 運用エンジニアがタスクを実行する必要がある場合に、クラウド VM への一時的な SSH アクセスを許可する新しいアクセス要求プロセスを開発します。
B. 運用チームに Google Cloud Shell を使用するためのアクセス権を付与します。
C. 開発チームに、運用チームがタスクを達成するために特定のリモート プロシージャ コールを実行できるようにする API サービスを構築してもらいます。
D. GCP への VPN 接続を構成して、クラウド VM への SSH アクセスを許可します。
Answer: B (メーッセージを残す)
運用チームに Google Cloud Shell を使用するためのアクセス権を付与します。
B (正解) - 運用エンジニアに Google Cloud Shell を使用するためのアクセス権を付与します。
エンジニアに求められたのは、SSH を使用するのと同じように VM にリモート アクセスすることだけです。そのため、マシンに外部 IP アドレスが残っている場合、エンジニアは Google Cloud Shell を使用して SSH 経由で VM にアクセスできます。
これは要件を満たす簡単で効果的な方法です。他のすべての答えは、ニーズに見合った価値以上に多くのセットアップが必要になる可能性があるオプションです。

最新問題: **16**
次のファイアウォール ルールセットが Virtual Private Cloud (VPC) 内のすべてのインスタンスに適用されています。
ファイアウォール ルールを更新して、次のルールをルールセットに追加する必要があります。
新しいユーザー アカウントを使用しています。ファイアウォール ルールを更新する前に、適切な ID およびアクセス管理 (IAM) ユーザー ロールをこの新しいユーザー アカウントに割り当てる必要があります。新しいユーザー アカウントは、アップデートを適用し、ファイアウォール ログを表示できる必要があります。あなたは何をするべきか？
A. compute.orgSecurityPolicyAdmin およびlogging.viewer ロールを新しいユーザー アカウントに割り当てます。優先度 50 の新しいファイアウォール ルールを適用します。
B. compute.securityAdmin およびlogging.viewer ルールを新しいユーザー アカウントに割り当てます。優先度 50 の新しいファイアウォール ルールを適用します。
C. 新しいユーザー アカウントに compute.securityAdmin ロールとlogging.bucketWriter ロールを割り当てます。優先度 150 の新しいファイアウォール ルールを適用します。
D. 新しいユーザー アカウントに compute.orgSecurityPolicyAdmin ロールとlogging.bucketWriter ロールを割り当てます。優先度 150 の新しいファイアウォール ルールを適用します。
Answer: B (メーッセージを残す)

最新問題: **17**

最近、us-central1 に 2 つのネットワーク仮想アプライアンスをデプロイしました。ネットワーク アプライアンスは、オンプレミス ネットワーク 10.0.0.0/8 への接続を提供します。Virtual Private Cloud (VPC) のルーティングを構成する必要があります。設計は次の要件を満たす必要があります。
オンプレミス ネットワークへのすべてのアクセスは、ネットワーク仮想アプライアンスを経由する必要があります。
単一のネットワーク仮想アプライアンスに障害が発生した場合に、オンプレミスへのアクセスを許可します。
両方のネットワーク仮想アプライアンスを同時に使用する必要があります。
これを実現するにはどの方法を使用する必要がありますか?
A. 2 つのネットワーク仮想アプライアンスのネットワーク ロード バランサーを構成します。ネットワーク ロード バランサーをネクスト ホップとして使用して、10.0.0.0/8 のルートを構成します。
B. 2 つのネットワーク仮想アプライアンスをバックエンドとして使用して内部 HTTP(S) ロード バランサーを構成します。内部 HTTP(S) ロード バランサーをネクスト ホップとして使用して、10.0.0.0/8 のルートを構成します。
C. 異なる優先順位を持つ 10.0.0.0/8 の 2 つのルートを構成し、それぞれが別のネットワーク仮想アプライアンスを指します。
D. 2 つのネットワーク仮想アプライアンスをバックエンドとして使用して内部 TCP/UDP ロード バランサーを構成します。内部ロード バランサーをネクスト ホップとして使用して、10.0.0.0/8 のルートを構成します。
Answer: B (メーッセージを残す**)**

最新問題**: 18**
VPC 内の 1 つのインスタンスは、プライベート IP アドレスのみで実行されるように構成されています。このインスタンスが削除された場合でも、現在のプライベート IP アドレスが別のインスタンスに自動的に割り当てられないようにしたいと考えています。
GCP Console では何をすればよいでしょうか?
A. インスタンスの現在の内部 IP アドレスを静的アドレスに変更します。
B. 新しい予約済み内部 IP アドレスをインスタンスに割り当てます。
C. インスタンスにパブリック IP アドレスを割り当てます。
D. キーの内部アドレスと予約された値を使用して、カスタム メタデータをインスタンスに追加します。
Answer: (解答を表示する)

最新問題**: 19**
あなたはハイブリッド クラウド環境を設計しています。Google Cloud 環境は、中央のトランジット ハブ VPC 内の HA VPN と Cloud Router を使用してオンプレミス ネットワークと相互接続されます。Cloud Router はデフォルト設定で構成されています。オンプレミスの DNS サーバーは 192.168.20.88 にあります。複数のスポーク VPC 内の Compute Engine リソースが、ドメイン corp.altostrat.com を使用してオンプレミスのプライベート ホスト名を解決できると同時に、Google Cloud のホスト名も解決できることを確認する必要があります。Google が推奨する慣行に従いたいと考えています。あなたは何をするべきか？
A. Cloud DNS に、192.168.20.88 を指す、corp-altostrat-com という「corp.altostrat.com」のプライベート転送ゾーンを作成します。ゾーンをハブ VPC に関連付けます。
ハブ VPC をターゲットとして、スポーク VPC に関連付けられた corp-altostrat-com という名前の「corp.altostrat.com」用のプライベート ピアリング ゾーンを Cloud DNS に作成します。
Cloud Router に 35.199.192.0/19 のカスタム ルート アドバタイズメントを設定します。
スポーク VPC で VPC ピアリングを構成し、ハブ VPC とピアリングします。
B. Cloud DNS に、192.168.20.88 を指す、corp-altostrat-com という「corp.altostrat.com」のプライベート転送ゾーンを作成します。ゾーンをハブ VPC に関連付けます。

ハブ VPC をターゲットとして、スポーク VPC に関連付けられた corp-altostrat-com という名前の「corp.altostrat.com」用のプライベート ピアリング ゾーンを Cloud DNS に作成します。
Cloud Router に 35.199.192.0/19 のカスタム ルート アドバタイズメントを設定します。
各スポーク VPC にハブアンドスポーク VPN デプロイメントを作成して、オンプレミス ネットワークに直接接続し直します。
C. Cloud DNS に、192.168.20.88 を指す、corp-altostrat-com という「corp.altostrat.com」のプライベート転送ゾーンを作成します。
ゾーンをハブ VPC に関連付けます。ハブ VPC をターゲットとして、スポーク PC に関連付けられた corp-altostrat-com という名前の「corp.altostrat.com」用のプライベート ピアリング ゾーンを Cloud DNS に作成します。
Cloud Router に 35.199.192.0/19 のカスタム ルート アドバタイズメントを設定します。
D. 「corp altostrat.com」の Cloud DNS に、192.168.20.88 を指す corp-altostrat-com という名前のプライベート転送ゾーンを作成します。ゾーンをハブ VPC に関連付けます。
ハブ VPC をターゲットとして、スポーク VPC に関連付けられた corp-altostrat-com という名前の「corp.altostrat.com」用のプライベート ピアリング ゾーンを Cloud DNS に作成します。
Cloud Router 上で 35.199.192.0/19 のカスタム ルート アドバタイズメントを実行しました。
各スポーク VPC にハブ アンド スポーク VPN デプロイメントを作成し、ハブ VPC に接続し直します。
Answer: A (メーッセージを残す**)**

最新問題**: 20**
Partner Interconnect 接続をプロビジョニングして、オンプレミス データセンターから Google Cloud への接続を拡張しました。Cloud Router を構成し、VPC 内のリソースに接続するための VLAN アタッチメントを作成する必要があります。関連する Cloud Router で使用する自律システム番号（ASN）を構成し、VLAN アタッチメントを作成する必要があります。
あなたは何をするべきか？
A. 2 バイトのプライベート ASN 64512-65535 を使用します。
B. 公開されている Google ASN 15169 を使用します。
C. パブリック Google ASN 16550 を使用します。
D. 4 バイトのプライベート ASN 4200000000-4294967294 を使用します。
Answer: (解答を表示する**)**

最新問題**: 21**
Virtual Private Cloud (VPC) とオンプレミス ネットワークの間に HA VPN 接続を構成しています。VPN ゲートウェイの名前は VPN_GATEWAY_1 です。プロジェクトで作成された VPN トンネルがオンプレミス VPN パブリック IP アドレス 203.0.113.1/32 にのみ接続するように制限する必要があります。あなたは何をするべきか？
A. 203.0.113.1/32 を除くすべてのトラフィックを拒否するようにピア VPN ゲートウェイでアクセス コントロール リストを構成し、それをプライマリ外部インターフェイスに接続します。
B. 203.0.113.1/32 アドレスのみで構成されるallowList を使用するように、リソース マネージャーの制約constraints/compute.restrictVpnPeerIPsを構成します。
C. 203.0.113.1/32 を受け入れるファイアウォール ルールを構成し、ターゲット タグを VPN_GATEWAY_1 に設定します。
D. Google Cloud Armor セキュリティ ポリシーを構成し、203.0.113.1/32 を許可するポリシー ルールを作成します。
Answer: B (メーッセージを残す**)**

最新問題: **22**
Google Kubernetes Engine (GKE) にデプロイされたアプリケーションに新しい Cloud Armor ポリシーを適用したいと考えています。Cloud Armor ポリシーにどのターゲットを使用するかを調べたいと考えています。
どの GKE リソースを使用する必要がありますか?
A. GKE ノード
B. GKE ポッド
C. GKE クラスタ
D. GKE Ingress
Answer: B (メーッセージを残す**)**
説明/参照: https://cloud.google.com/kubernetes-engine/docs/how-to/cloud-armor-backendconfig

最新問題: **23**
オンプレミス データセンターには 2 台のルーターがあり、各ルーターの VPN を介して Google Cloud 環境に接続されています。すべてのアプリケーションは正しく動作しています。ただし、すべてのトラフィックは、必要に応じて 2 つの接続間で負荷分散されるのではなく、単一の VPN を通過します。
トラブルシューティング中に次のことがわかります。
* 各オンプレミス ルーターは一意の ASN で構成されます。
* 各オンプレミス ルーターは同じルートと優先度で構成されます。
* 両方のオンプレミス ルーターは、単一の Cloud Router に接続された VPN で構成されています。
* BGP セッションは、オンプレミス ルーターと Cloud Router の両方の間で確立されます。
* オンプレミス ルーターのルートは 1 つだけルーティング テーブルに追加されます。
この問題の最も考えられる原因は何ですか?
A. オンプレミス ルーターは同じルートで構成されています。
B. オンプレミス ルーターで使用されている ASN が異なります。
C. ファイアウォールが 2 番目の VPN 接続を介したトラフィックをブロックしています。
D. ネットワーク トラフィックの負荷分散を行うロード バランサーがありません。
Answer: (解答を表示する**)**

最新問題: **24**
次のオブジェクトを含むストレージ バケットがあります。
- フォルダーa/画像a-1.jpg
- フォルダーa/画像a-2.jpg
- フォルダ-b画像-b-1. jpg
- フォルダ-b画像-b-2. jpg
Cloud CDN はストレージ バケットで有効になっており、4 つのオブジェクトはすべて正常にキャッシュされています。最小限のコマンドを使用して、接頭辞がfolder-aであるすべてのオブジェクトのキャッシュされたコピーを削除したいと考えています。
あなたは何をするべきか？
A. ストレージ バケットに適切なライフサイクル ルールを追加します。
B. ストレージ バケットで Cloud CDN を無効にします。90秒待ちます。ストレージ バケットで Cloud CDN を再度有効にします。
C. プレフィックスフォルダー a を持つすべてのオブジェクトがパブリックに共有されていないことを確認してください。

D. パターン /folder-a/* でキャッシュ無効化コマンドを発行します。
Answer: (解答を表示する**)**

最新問題**: 25**
あなたは、Google Cloud への移行を進めている大学で働いています。
クラウドの要件は次のとおりです。
10 Gbps のオンプレミス接続
クラウドへの最小遅延アクセス
集中ネットワーク管理チーム
新しい部門は、プロジェクトへのオンプレミス接続を求めています。キャンパスを Google Cloud に接続するために、最もコスト効率の高い相互接続ソリューションをデプロイしたいと考えています。
あなたは何をするべきか？
A. スタンドアロン プロジェクトを使用し、個々のプロジェクトのそれぞれに VLAN アタッチメントと専用インターコネクトを展開します。
B. 共有 VPC を使用し、VLAN アタッチメントと Dended Interconnect をホスト プロジェクトにデプロイします。
C. スタンドアロン プロジェクトを使用し、個々のプロジェクトに VLAN アタッチメントを展開します。VLAN アタッチメントをスタンドアロン プロジェクトの専用インターコネクトに接続します。
D. 共有 VPC を使用し、サービス プロジェクトに VLAN アタッチメントをデプロイします。VLAN アタッチメントを共有 VPC のホスト プロジェクトに接続します。
Answer: B (メーッセージを残す**)**

最新問題**: 26**
あなたの会社には、Cloud Interconnect を使用してオンプレミス ネットワークからアクセスできる、Google Cloud にデプロイされた単一の Virtual Private Cloud (VPC) ネットワークがあります。サービス レベル アグリーメント (SLA) が適用されたハイブリッド接続を介して、VPC Service Controls によってサポートされる Google API およびサービスへのアクセスのみを構成する必要があります。あなたは何をするべきか？
A. デフォルト ルートをアドバタイズするように既存の Cloud Router を構成し、Cloud NAT を使用してオンプレミス ネットワークからのトラフィックを変換します。
B. ダイレクト ピアリング リンクを追加し、パブリック仮想 IP アドレスを使用する Google API への接続に使用します。
C. 限定公開の Google アクセスを、restricted.googleapis.com 仮想 IP アドレスを持つオンプレミス ホストに使用します。
D. Google API のパブリック仮想 IP アドレスをアドバタイズするように既存の Cloud Router を構成します。
Answer: C (メーッセージを残す**)**

最新問題**: 27**
会社のセキュリティ チームは、可能な限りマネージド サービスを使用する傾向があります。運用上のオーバーヘッドを増加させることなく、構成されたファイアウォール ルールに対して発生する拒否ヒットの数を表示するダッシュボードを構築する必要があります。あなたは何をするべきか？
A. Google Cloud Marketplace からファイアウォール アプライアンスを構成します。すべてのトラフィックをこのアプライアンス経由でルーティングし、この層でファイアウォール ルールを適用します。ファイアウォール アプライアンスを使用してヒット数を表示します。
B. ファイアウォール ルールのログを構成します。Firewall Insights を使用してヒット数を表示します。
C. VPC でパケット ミラーリングを構成します。拒否されたファイアウォール ルールの IP アドレス リストを使用してフィルターを適用します。侵入検知システム (IDS) アプライアンスを受信機として構成し、ヒット数を表示します。

D. ファイアウォール ルールのログを構成します。Cloud Logging でログを表示し、Cloud Monitoring でカスタム ダッシュボードを作成してヒット数を表示します。
Answer: (解答を表示する**)**

最新問題**: 28**
オンプレミスからアクセスできる既存の VPC に GKE クラスタを作成する必要があります。次の要件を満たす必要があります。
* ポッドとサービスの IP 範囲は可能な限り小さくする必要があります。
* ノードとマスターはインターネットからアクセスできない必要があります。
* クラスターを管理するには、オンプレミスのサブネットから kubectl コマンドを使用できる必要があります。
GKE クラスタはどのように作成すればよいですか?
A. * VPC アドバンスト ルートを使用するプライベート クラスターを作成します。
* ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
B. * GKE が管理する IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* ポッド IP 範囲を /21 に設定し、サービス IP 範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
C. * ユーザー管理の IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* GKE クラスタ ネットワーク ポリシーを有効にし、ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
* マスター承認ネットワークを有効にします。
D. * ユーザー管理の IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* クラスターマスターで privateEndpoint を有効にします。
* ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
* マスター承認ネットワークを有効にします。
Answer: C (メーッセージを残す**)**
説明/参照: https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips

最新問題**: 29**
現在、us-central1 リージョンでホストされている Web アプリケーションがあります。ユーザーはアジアを旅行する際に高い遅延を経験します。ネットワーク ロード バランサーを構成しましたが、ユーザーはパフォーマンスの向上を経験していません。レイテンシを短縮したいと考えています。
あなたは何をするべきか？
A. ポリシーベースのルート ルールを設定して、トラフィックに優先順位を付けます。
B. HTTP ロード バランサーを構成し、トラフィックをそこに送信します。
C. アプリケーションをホストするサブネットの動的ルーティングを構成します。
D. DNS ゾーンの TTL を構成して、更新間の時間を短縮します。
Answer: (解答を表示する**)**
説明/参考: https://cloud.google.com/load-balancing/docs/tutorials/optimize-app-latency

最新問題: **30**
あなたの会社には、Cloud Interconnect 接続を使用してオンプレミスの場所からアクセスできる、Google Cloud にデプロイされた単一の Virtual Private Cloud (VPC) ネットワークがあります。会社は、公共のインターネット経由で他の Google API やサービスにアクセスしながら、相互接続リンク経由でのみ Cloud Storage にトラフィックを送信できる必要があります。あなたは何をするべきか？
A. 限定公開の Google アクセスを使用し、Cloud Storage には制限付き.googleapis.com 仮想 IP アドレスを使用し、他のすべての Google API とサービスには private.googleapis.com を使用します。
B. すべての Google API とサービスにデフォルトのパブリック ドメインを使用します。
C. Private Service Connect を使用して Cloud Storage にアクセスし、他のすべての Google API とサービスにはデフォルトのパブリック ドメインを使用します。
D. プライベート Google アクセスを使用します。Cloud Storage には private.googleapis.com 仮想 IP アドレスを使用し、他のすべての Google API およびサービスには制限付き.googleapis.com 仮想 IP アドレスを使用します。
Answer: C (メーッセージを残す**)**

最新問題: **31**
あなたは最近、組織の ID とアクセス管理の管理を任されました。いくつかのプロジェクトがあり、可能な限りスクリプトと自動化を使用したいと考えています。プロジェクト メンバーに編集者の役割を付与したいと考えています。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
A. REST API 経由の GetIamPolicy()
B. REST API 経由の setIamPolicy()
C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername -- role ロール/エディター
D. gcloud プロジェクト add-iam-policy-binding Sprojectname --member user:Susername --role ロール/エディター
E. [メンバーの追加] フィールドにメール アドレスを入力し、GCP Console のドロップダウン メニューから目的のロールを選択します。
Answer: D,E (メーッセージを残す**)**
https://cloud.google.com/iam/docs/granting-changing-revoking-access

最新問題: **32**
あなたのソフトウェア チームは、RFC 1918 アドレス空間を使用して GCP の Compute Engine インスタンスに直接接続する必要があるオンプレミス ウェブ アプリケーションを開発しています。次の仕様を考慮して、オンプレミス環境から GCP への接続ソリューションを選択したいと考えています。
* ご利用の ISP は Google Partner Interconnect プロバイダーです。
* オンプレミス VPN デバイスのインターネット アップリンクおよびダウンリンク速度は 10 Gbps です。
* オンプレミス ゲートウェイと GCP 間のテスト VPN 接続は、最大速度で実行されています。
パケットロスにより500Mbps。
* ほとんどのデータ転送は GCP からオンプレミス環境へ行われます。

* アプリケーションは、インターコネクト上のピーク転送中に最大 1.5 Gbps までバーストできます。
* ソリューションのコストと複雑さは最小限である必要があります。
接続ソリューションをどのようにプロビジョニングする必要がありますか?
A. ISP を通じて Partner Interconnect をプロビジョニングします。
B. VPN の代わりに専用相互接続をプロビジョニングします。
C. パケット損失を考慮して複数の VPN トンネルを作成し、ECMP を使用して帯域幅を増やします。
D. VPN 経由でネットワーク圧縮を使用して、VPN 経由で送信できるデータ量を増やします。
Answer: C (メーッセージを残す)

最新問題: **33**
オンプレミスからアクセスできる既存の VPC に GKE クラスタを作成する必要があります。次の要件を満たす必要があります。
* ポッドとサービスの IP 範囲は可能な限り小さくする必要があります。
* ノードとマスターはインターネットからアクセスできない必要があります。
* クラスターを管理するには、オンプレミスのサブネットから kubectl コマンドを使用できる必要があります。
GKE クラスタはどのように作成すればよいですか?
A. * VPC アドバンスト ルートを使用するプライベート クラスターを作成します。
* ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
B. * GKE が管理する IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* ポッド IP 範囲を /21 に設定し、サービス IP 範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
C. * ユーザー管理の IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* GKE クラスタ ネットワーク ポリシーを有効にし、ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
* マスター承認ネットワークを有効にします。
D. * ユーザー管理の IP 範囲を使用して VPC ネイティブ GKE クラスタを作成します。
* クラスターマスターで privateEndpoint を有効にします。
* ポッドとサービス範囲を /24 に設定します。
* マスターにアクセスするためにネットワーク プロキシを設定します。
* マスター承認ネットワークを有効にします。
Answer: C (メーッセージを残す)
参照：
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips

最新問題: **34**
Google Cloud のコンピューティング エンジンのポート 8085 に Apache Tomcat 8.X をインストールし、同じマシンのカスタム ポートに Jenkins もインストールしました。ポート 8085 へのトラフィックを許可するファイアウォール ルールを作成しました。XXXX:8085 を参照すると Apache Tomcat ページがロードされますが、XXXX:custom port を参照すると Jenkins ページがロードされません。考えられる解決策は何でしょうか? 正しい選択肢を選択してください。

A. ファイアウォール ルールを作成します。正しいネットワークを選択し、ネットワーク内のすべてのインスタンスとしてターゲットを選択し、カスタム ポートとプロトコルを指定します。
B. ファイアウォール ルールを作成します。正しいネットワークを選択し、ターゲット タグを作成してそのタグをコンピューティング エンジン インスタンスにアタッチし、Jenkins でマッピングされたカスタム ポートへのトラフィックを許可します。
C. ファイアウォール ルールを作成します。コンピューティング エンジンを備えた正しいサブネットを選択し、すべてのプロトコルとポートを許可します。
D. ファイアウォール ルールを作成します。正しいサブネットを選択し、ターゲット タグを作成してコンピューティング エンジン インスタンスにアタッチし、すべてのプロトコルとポートを許可します。
Answer: B (メーッセージを残す**)**
タグを作成してコンピューティング エンジン インスタンスにアタッチし、カスタム ポートへのトラフィックを許可することは許容度が低いため、オプション B が正しい選択です。
選択肢 A は不正解です。ネットワーク内のすべてのインスタンスとしてターゲットを選択すると、すべてのインスタンスへのトラフィックが許可されます。
選択肢 C は不正解です。すべてのプロトコルとポートを許可することはセキュリティ上の問題であり、常に最小許容度の原則に従うためです。
選択肢 D は不正解です。すべてのプロトコルとポートを許可すると、セキュリティ上の災害につながる可能性があり、常に最小許容度の原則に従うためです。

最新問題**: 35**
あなたは、GCP への移行を進めている多国籍企業に勤めています。
クラウドの要件は次のとおりです。
* 米国のオレゴン州とニューヨークにあるオンプレミス データ センターで、クラウド リージョン us-west1 (プライマリ本社) と us-east4 (バックアップ) に接続された専用インターコネクトを備えています。
* ヨーロッパとアジア太平洋に複数の支社を設置
* europe-west1 および australia-southeast1 では地域データ処理が必要です
* 集中ネットワーク管理チーム
セキュリティおよびコンプライアンス チームは、URL フィルタリングの L7 インスペクションを実行するために仮想インライン セキュリティ アプライアンスを必要としています。アプライアンスを us-west1 にデプロイしたいと考えています。
あなたは何をするべきか？
A. * 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。* ホスト プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。* ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
B. * 共有 VPC ホスト プロジェクトに 1 つの VPC を作成します。* ホスト プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの us-west1 サブネットに NIC0 を接続します。* NIC1 を接続します。ホスト プロジェクトの us-west1 サブネットに* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
C. * 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。* サービス プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。* ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。

D. * 共有 VPC サービス プロジェクトに 1 つの VPC を作成します。* サービス プロジェクトのゾーン us-west1-a に 2 枚の NIC インスタンスを構成します。* サービス プロジェクトの us-west1 サブネットに NIC0 を接続します。* NIC1 を接続します。サービス プロジェクトの us-west1 サブネットに* インスタンスをデプロイします。* インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
Answer: A (メーッセージを残す)

最新問題**: 36**
あなたは、組織の Google Cloud 環境で Cloud Router の新しいインスタンスを構成し、新しい Dended Interconnect を介してデータセンターに接続できるようにしています。営業、マーケティング、IT のそれぞれが、組織のホスト プロジェクトに接続されているサービス プロジェクトを持っています。
Cloud Router インスタンスはどこに作成する必要がありますか?
A. すべてのプロジェクトの VPC ネットワーク
B. IT プロジェクトの VPC ネットワーク
C. ホスト プロジェクトの VPC ネットワーク
D. セールス、マーケティング、IT プロジェクトの VPC ネットワーク
Answer: C (メーッセージを残す)
参照：
https://cloud.google.com/interconnect/docs/how-to/d dedicated/using-interconnects-other-projects

最新問題**: 37**
Compute Engine 上で実行されているアプリケーションがあり、BigQuery を使用して結果を生成し、Cloud Storage に保存しています。どのアプリケーション インスタンスも外部 IP アドレスを持たないようにしたいと考えています。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
A. VPC と BigQuery の間にネットワーク ピアリングを作成します。
B. VPC でプライベート サービス アクセスを有効にします。
C. VPC でプライベート Google アクセスを有効にします。
D. すべてのサブネットで限定公開の Google アクセスを有効にします。
E. クラウド NAT を作成し、NAT ゲートウェイ経由でアプリケーション トラフィックをルーティングします。
Answer: C,E (メーッセージを残す)

最新問題**: 38**
Cloud NAT を設定することにしました。構成を完了すると、インスタンスの 1 つがアウトバウンド NAT に Cloud NAT を使用していないことがわかります。
この問題の最も考えられる原因は何ですか?
A. 外部 IP アドレスがインスタンスに構成されています。
B. インスタンスはロード バランサーの外部 IP アドレスによってアクセスできます。
C. RFC1918 範囲を使用する静的ルートを作成しました。
D. インスタンスは複数のインターフェースで構成されています。
Answer: A (メーッセージを残す)

最新問題**: 39**
Partner Interconnect を使用してオンプレミス ネットワークを VPC に接続したいと考えています。すでに相互接続パートナーがいます。

まず何をすべきでしょうか？
A. パートナーのポータルにログインし、そこで VLAN アタッチメントを要求します。
B. Interconnect パートナーに、Google への物理接続をプロビジョニングするよう依頼します。
C. GCP Console で Partner Interconnect タイプの VLAN アタッチメントを作成し、ペアリング キーを取得します。
D. gcloud compute interconnectattachments Partner update <attachment> / --region <region> --admin-enabled を実行します。
Answer: B (メーッセージを残す**)**
参照：
https://cloudplatform.googleblog.com/2018/06/Partner-Interconnect-now-generally-available.html

最新問題**: 40**
Cloud DNS が管理するゾーンの 1 つで DNSSEC を無効にしています。ゾーン ファイルから DS レコードを削除し、キャッシュから期限切れになるのを待って、ゾーンの DNSSEC を無効にしました。DNSSEC 検証解決がゾーン内の名前を解決できないというレポートを受け取ります。
あなたは何をするべきか？
A. ゾーンの TTL を更新します。
B. ゾーンを TRANSFER 状態に設定します。
C. ドメイン レジストラで DNSSEC を無効にします。
D. ドメインの所有権を新しい登録者に譲渡します。
Answer: (解答を表示する**)**
使用するマネージド ゾーンの DNSSEC を無効にする前に、ドメイン レジストラーで DNSSEC を無効にして、DNSSEC 検証リゾルバーが引き続きゾーン内の名前を解決できることを確認する必要があります。

最新問題**: 41**
トラフィックを検査するためにサードパーティの次世代ファイアウォールを使用しています。送信トラフィックをファイアウォールにルーティングするカスタム ルート 0.0.0.0/0 を作成しました。パブリック IP アドレスを持たない VPC インスタンスが、ファイアウォールを介してトラフィックを送信せずに BigQuery および Cloud Pub/Sub API にアクセスできるようにしたいと考えています。
どの 2 つのアクションを取る必要がありますか? (2つお選びください。)
A. サブネット レベルで限定公開の Google アクセスをオンにします。
B. VPC レベルで限定公開の Google アクセスを有効にします。
C. VPC レベルでプライベート サービス アクセスをオンにします。
D. デフォルトのインターネット ゲートウェイ経由で Google API およびサービスの外部 IP アドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
E. デフォルトのインターネット ゲートウェイ経由で Google API およびサービスの内部 IP アドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
Answer: (解答を表示する**)**
説明/参照: https://cloud.google.com/vpc/docs/private-access-options

最新問題**: 42**
サービス アカウントを使用して認証する作業オートメーションにステップを追加しています。Cloud Storage バケットからファイルを取得する機能の自動化を推進する必要があります。組織では、可能な限り最小限の権限を使用する必要があります。
あなたは何をするべきか？

A. ユーザー アカウントに compute.instanceAdmin を付与します。
B. iam.serviceAccountUser をユーザー アカウントに付与します。
C. Cloud Storage バケットのサービス アカウントに読み取り専用権限を付与します。
D. Cloud Storage バケットのサービス アカウントにクラウド プラットフォーム権限を付与します。
Answer: (解答を表示する**)**
説明/参照: https://cloud.google.com/compute/docs/access/iam

最新問題**: 43**
ストレージ バケット内のすべてのオブジェクトに対して Cloud CDN を有効にする必要があります。ストレージ バケット内のすべてのオブジェクトが CDN によって提供されることを確認したいと考えています。
GCP Console では何をすればよいでしょうか?
A. 新しい TCP ロードバランサを作成し、ストレージ バケットをバックエンドとして選択して、バックエンドで Cloud CDN を有効にします。
B. 新しい HTTP ロードバランサを作成し、バックエンドとしてストレージ バケットを選択し、バックエンドで Cloud CDN を有効にして、ストレージ バケット内の各オブジェクトがパブリックに共有されていることを確認します。
C. 新しいクラウド ストレージ バケットを作成し、そのバケット上で Cloud CDN を有効にします。
D. 新しい SSL プロキシ ロードバランサを作成し、ストレージ バケットをバックエンドとして選択して、バックエンドで Cloud CDN を有効にします。
Answer: C (メーッセージを残す**)**

最新問題**: 44**
次のルーティング設計があります。asia-southeast1 リージョンの Subnet-2 にある Compute Engine インスタンスがオンプレミスのコンピューティング リソースと通信できないことがわかりました。あなたは何をするべきか？
A. asia-southeast1 リージョンで IP 転送を有効にします。
B. 2 番目のボーダー ゲートウェイ プロトコル (BGP) セッションを Cloud Router に追加します。
C. Cloud Router でカスタム ルート アドバタイズメントを構成します。
D. VPC 動的ルーティング モードをグローバルに変更します。
Answer: (解答を表示する**)**

最新問題**: 45**
開発チーム用に新しい VPC を作成しました。SSH 経由のみでこの VPC 内のリソースへのアクセスを許可したいと考えています。
ファイアウォール ルールをどのように構成すればよいでしょうか?
A. 2 つのファイアウォール ルールを作成します。1 つは優先度 0 ですべてのトラフィックをブロックし、もう 1 つは優先度でポート 22 を許可します。1000。
B. 2 つのファイアウォール ルールを作成します。1 つは優先度 65536 のすべてのトラフィックをブロックし、もう 1 つは優先度 1000 のポート 3389 を許可します。
C. 優先度 1000 のポート 22 を許可する単一のファイアウォール ルールを作成します。
D. 優先度 1000 のポート 3389 を許可する単一のファイアウォール ルールを作成します。
Answer: C (メーッセージを残す**)**
説明/参照: https://geekflare.com/gcp-firewall-configuration/

最新問題**: 46**

Cloud DNS が管理するゾーンの 1 つで DNSSEC を無効にしています。ゾーン ファイルから DS レコードを削除し、キャッシュから期限切れになるのを待って、ゾーンの DNSSEC を無効にしました。DNSSEC 検証解決がゾーン内の名前を解決できないというレポートを受け取ります。
あなたは何をするべきか？
A. ゾーンの TTL を更新します。
B. ゾーンを TRANSFER 状態に設定します。
C. ドメイン レジストラーで DNSSEC を無効にします。
D. ドメインの所有権を新しいレジストラに譲渡します。
Answer: C (メーッセージを残す)
使用するマネージド ゾーンの DNSSEC を無効にする前に、ドメイン レジストラーで DNSSEC を無効にして、DNSSEC 検証リゾルバーが引き続きゾーン内の名前を解決できることを確認する必要があります。
参考: https://cloud.google.com/dns/docs/dnssec-config

最新問題**: 47**
あなたは GCP への移行計画の初期段階にいます。本番環境への実装を開始する前に、ハイブリッド クラウド設計の機能をテストしたいと考えています。この設計には、プライベート IP アドレスを使用してオンプレミス サーバーと通信する必要がある Compute Engine 仮想マシン インスタンス上で実行されるサービスが含まれています。オンプレミス サーバーはインターネットに接続できますが、Cloud Interconnect 接続はまだ確立されていません。インスタンスとオンプレミス サーバー間の接続を有効にする最も低コストの方法を選択し、テストを 24 時間以内に完了したいと考えています。
どの接続方法を選択する必要がありますか?
A. クラウド VPN
B. 50 Mbps パートナー VLAN アタッチメント
C. 単一の VLAN アタッチメントを備えた専用インターコネクト
D. 専用相互接続ですが、VLAN アタッチメントをプロビジョニングしません
Answer: A (メーッセージを残す)

最新問題**: 48**
あなたのソフトウェア チームは、RFC 1918 アドレス空間を使用して GCP の Compute Engine インスタンスに直接接続する必要があるオンプレミス ウェブ アプリケーションを開発しています。次の仕様を考慮して、オンプレミス環境から GCP への接続ソリューションを選択したいと考えています。
* ご利用の ISP は Google Partner Interconnect プロバイダーです。
* オンプレミス VPN デバイスのインターネット アップリンクおよびダウンリンク速度は 10 Gbps です。
* オンプレミス ゲートウェイと GCP 間のテスト VPN 接続は、パケット損失により最大 500 Mbps で実行されます。
* ほとんどのデータ転送は GCP からオンプレミス環境へ行われます。
* アプリケーションは、インターコネクト上のピーク転送中に最大 1.5 Gbps までバーストできます。
* ソリューションのコストと複雑さは最小限である必要があります。

接続ソリューションをどのようにプロビジョニングする必要がありますか?
A. VPN 経由でネットワーク圧縮を使用して、VPN 経由で送信できるデータ量を増やします。
B. ISP を通じて Partner Interconnect をプロビジョニングします。
C. VPN の代わりに専用相互接続をプロビジョニングします。
D. パケット損失を考慮して複数の VPN トンネルを作成し、ECMP を使用して帯域幅を増やします。
Answer: (解答を表示する**)**

最新問題**: 49**
Google Kubernetes Engine (GKE) にデプロイされたアプリケーションに新しい Cloud Armor ポリシーを適用したいと考えています。Cloud Armor ポリシーにどのターゲットを使用するかを調べたいと考えています。
どの GKE リソースを使用する必要がありますか?
A. GKE クラスタ
B. GKE ポッド
C. GKE Ingress
D. GKE ノード
Answer: (解答を表示する**)**

最新問題**: 50**
あなたは、3 層アプリケーション アーキテクチャをオンプレミスから Google Cloud に移行しています。移行の最初のステップとして、外部 HTTP(S) ロード バランサを使用して新しい Virtual Private Cloud (VPC) を作成します。このロード バランサーは、プレゼンテーション層を実行するオンプレミスのコンピューティング リソースにトラフィックを転送します。悪意のあるトラフィックが VPC に入り、エッジでリソースを消費するのを阻止する必要があるため、IP アドレスをフィルタリングし、クロスサイト スクリプティング (XSS) 攻撃を阻止するようにこのポリシーを構成する必要があります。あなたは何をするべきか？
A. 階層型ファイアウォール ルールセットを作成し、VPC の親組織リソース ノードに適用します。
B. Google Cloud Armor ポリシーを作成し、インターネット ネットワーク エンドポイント グループ (NEG) バックエンドを使用するバックエンド サービスに適用します。
C. Google Cloud Armor ポリシーを作成し、アンマネージド インスタンス グループ バックエンドを使用するバックエンド サービスに適用します。
D. VPC ファイアウォール ルールセットを作成し、それを非マネージド インスタンス グループ内のすべてのインスタンスに適用します。
Answer: B (メーッセージを残す**)**

最新問題**: 51**
あなたの会社では、営業部門と財務部門の 2 つの部門が単一リージョンに個別の Virtual Private Cloud (VPC) ネットワークを持っています。営業部門の VPC ネットワークはすでに HA VPN を使用してオンプレミスの場所に接続されており、サブネット範囲が重複していないことを確認しました。Cloud NAT を介して Google Cloud ワークロードにインターネット接続を提供しながら、両方の VPC ネットワークをピアリングしてオンプレミス接続に同じ HA トンネルを使用することを計画しています。オンプレミスの場所からのインターネット アクセスは、Google Cloud を経由しないでください。財務部門とオンプレミスの場所の間のすべてのルートを伝播する必要があります。あなたは何をするべきか？
A. 2 つの VPC をピアリングします。Sales からカスタム ルートをエクスポートし、Finance の VPC ネットワークにカスタム ルートをインポートするように VPC ネットワーク ピアリングを構成します。Cloud Router のカスタム ルート アドバタイズメントを使用して、ピアリングされた VPC ネットワーク範囲をオンプレミスの場所にアナウンスします。

B. 2 つの VPC をピアリングします。Sales からカスタム ルートをエクスポートし、Finance の VPC ネットワークにカスタム ルートをインポートするように VPC ネットワーク ピアリングを構成します。Cloud Router のカスタム ルート アドバタイズメントを使用して、オンプレミスのロケーションへのデフォルト ルートをアナウンスします。
C. 2 つの VPC をピアリングし、Cloud Router のデフォルト構成を使用します。
D. 2 つの VPC をピアリングし、Cloud Router のカスタム ルート アドバタイズメントを使用して、ピアリングされた VPC ネットワーク範囲をオンプレミスの場所にアナウンスします。
Answer: C (メーッセージを残す**)**

最新問題**: 52**
あなたの組織は、Virtual Private Cloud (VPC) 内の重要な Compute Engine インスタンスでハブアンドスポーク アーキテクチャを使用しています。あなたは、Google Cloud の Cloud DNS の設計を担当します。オンプレミスのデータセンターから Cloud DNS プライベート ゾーンを解決し、ハブアンドスポーク VPC 設計からオンプレミスの名前解決を有効にできる必要があります。あなたは何をするべきか？
A. ハブ VPC でプライベート DNS ゾーンを構成し、オンプレミス サーバーへの DNS 転送を構成します。
スポーク VPC からハブ VPC への DNS ピアリングを構成します。
B. スポーク VPC で DNS ポリシーを構成し、オンプレミス DNS を代替 DNS サーバーとして構成します。
プライベート ゾーンを使用してハブ VPC を構成し、各スポーク VPC への DNS ピアリングを設定します。
C. ハブ VPC で DNS ポリシーを構成し、オンプレミス DNS を代替 DNS サーバーとして構成します。
プライベート ゾーンを使用してスポーク VPC を構成し、ハブ VPC への DNS ピアリングを設定します。
D. ハブ VPC で DNS ポリシーを構成し、スポーク VPC からの受信クエリの転送を許可します。
プライベート ゾーンを使用してスポーク VPC を構成し、ハブ VPC への DNS ピアリングを設定します。
Answer: (解答を表示する)

最新問題**: 53**
あなたの組織は、仮想マシン (VM) 間のフローを制御するためにファイアウォール ルールを適用する方法を制御する新しいセキュリティ ポリシーを実装しています。Google が推奨する方法を使用して、VM A と VM B の間のトラフィックを厳密に制御するファイアウォール ルールを設定する必要があります。
通信は VPC 内の VM A から VM B にのみ流れ、他の通信パスは許可されないことを確認する必要があります。VPC には他のファイアウォール ルールは存在しません。この通信パスのみを許可するには、どのファイアウォール ルールを設定する必要がありますか?
A. ファイアウォール ルールの方向: 入力
アクション: 許可する
ターゲット: VM A サービス アカウント
ソース範囲: VM B サービス アカウントと VM B ソース IP アドレス
優先度: 100
B. ファイアウォール ルールの方向: 入力
アクション: 許可する
ターゲット: 特定の VM B タグ
ソース範囲: VM A タグおよび VM A ソース IP アドレス
優先度: 1000
C. ファイアウォール ルールの方向: イングレス
アクション: 許可する

ターゲット: VM B サービス アカウント
ソース範囲: VM A サービス アカウント
優先度: 1000
D. ファイアウォール ルールの方向: 入力
アクション: 許可する
ターゲット: 特定の VM A タグ
ソース範囲: VM B タグおよび VM B ソース IP アドレス
優先度: 100
Answer: (解答を表示する**)**

最新問題**: 54**
単一の Compute Engine ゾーンにインスタンスを手動で配置して、概念実証アプリケーションをデプロイしました。これからアプリケーションを実稼働環境に移行するため、アプリケーションの可用性を高め、自動スケーリングできるようにする必要があります。
インスタンスをどのようにプロビジョニングする必要がありますか?
A. 単一のマネージド インスタンス グループを作成し、目的のリージョンを指定して、その場所として [複数のゾーン] を選択します。
B. リージョンごとにマネージド インスタンス グループを作成し、その場所で [単一ゾーン] を選択し、そのリージョン内のゾーン全体にインスタンスを手動で分散します。
C. 単一ゾーンにアンマネージド インスタンス グループを作成し、そのインスタンス グループの HTTP ロード バランサを作成します。
D. ゾーンごとに非マネージド インスタンス グループを作成し、目的のゾーン全体にインスタンスを手動で分散します。
Answer: (解答を表示する**)**
https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances

最新問題**: 55**
ユーザーが 3 つの VPC すべてのリソースにアクセスできるように、3 つの Virtual Private Cloud ネットワーク (Sales、Marketing、および Finance) 間のネットワーク接続を確立する必要があります。Sales VPC と Finance VPC の間に VPC ピアリングを構成します。また、Marketing VPC と Finance VPC 間の VPC ピアリングも構成します。構成を完了すると、一部のユーザーは Sales VPC および Marketing VPC のリソースに接続できなくなります。あなたは問題を解決したいと考えています。
あなたは何をするべきか？
A. フルメッシュで VPC ピアリングを構成します。
B. ネットワーク タグを作成して、3 つすべての VPC 間の接続を許可します。
C. ルーティング テーブルを変更して、非対称ルートを解決します。
D. レガシー ネットワークを削除し、推移的なピアリングを可能にするために再作成します。
Answer: A (メーッセージを残す**)**

最新問題**: 56**
TFTP サーバーとして使用する複数の Compute Engine 仮想マシン インスタンスを作成します。
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. HTTP(S) ロードバランサ
B. SSL プロキシ ロード バランサ
C. TCP プロキシ ロード バランサ

D. ネットワークロードバランサー
Answer: D (メーッセージを残す)
TFTP は UDP ベースのプロトコルです。サーバーは、TFTP セッションを確立するために最初のクライアントからサーバーへのパケットをポート 69 でリッスンし、その後、そのセッション中のすべてのパケットに対して 1023 より上のポートを使用します。クライアントは 1023 より上のポートを使用します。」https ://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_02.htm また、Google Cloud の外部 TCP/UDP ネットワーク負荷分散（以降 ネットワーク負荷分散と呼びます）は、リージョンの非プロキシ ロード バランサです。ネットワーク負荷分散は、Virtual Private Cloud (VPC) ネットワーク内の同じリージョン内の仮想マシン (VM) インスタンス間でトラフィックを分散します。

最新問題: **57**
gcloud コマンド ライン ツールを使用して、事前定義されたロールをコピーして、プロジェクトに新しいカスタム ロールを作成しています。次のエラー メッセージが表示されます。
INVALID_ARGUMENT: 権限 resourcemanager.projects.list が無効です。
A. resourcemanager.projects.getpermission を追加して、再試行します。
B. 新しい名前と同じ権限を持つ別のロールで再試行します。
C. resourcemanager.projects.list 権限を削除して、再試行します。
D. resourcemanager.projects.setIamPolicypermission を追加して、再試行します。
Answer: C (メーッセージを残す)
説明/参照: https://cloud.google.com/iam/docs/ Understanding-custom-roles

最新問題: **58**
アプリケーションの HTTP(S) 負荷分散が有効になっていますが、HTTP(S) リクエストが Compute Engine 仮想マシン インスタンスに正しく分散されていないとアプリケーション開発者から報告されました。リクエストがどのように分散されているかに関するデータを見つけたいと考えています。
これを達成できる 2 つの方法はどれですか? (2つお選びください。)
A. Stackdriver Error Reporting で、Cloud Load Balancer サービスの未確認のエラーを探します。
B. Stackdriver Monitoring で、[リソース] > [Google Cloud ロードバランサ] を選択し、ダッシュボードの主要指標グラフを確認します。
C. Stackdriver Monitoring で、[リソース] > [指標エクスプローラー] を選択し、https/request_bytes_count 指標を検索します。
D. GCP Console のロード バランサの詳細ページで、[モニタリング] タブをクリックし、バックエンド サービスを選択してグラフを確認します。
E. Stackdriver Monitoring で、新しいダッシュボードを作成し、ロードバランサの https/backend_request_count 指標を追跡します。
Answer: B,D (メーッセージを残す)

最新問題: **59**
Google Kubernetes Engine プライベート クラスターを作成し、kubectl を使用してポッドのステータスを取得したいと考えています。インスタンスの 1 つで、クラスターが稼働しているにもかかわらず、マスターが応答していないことに気づきました。
問題を解決するには何をすべきでしょうか?
A. VPC に適切なファイアウォール ポリシーを作成し、マスター ノードの IP アドレスからインスタンスへのトラフィックを許可します。
B. デフォルトのインターネット ゲートウェイを指す、マスターに到達するルートを作成します。
C. 適切なマスター承認済みネットワーク エントリを作成して、インスタンスがマスターと通信できるようにします。
D. インスタンスにパブリック IP アドレスを割り当てます。
Answer: A (メーッセージを残す)

最新問題: **60**
あなたの会社では、各部門の親フォルダーとサブフォルダーを含むリソース階層を定義しています。各部門は、割り当てられたフォルダ内でそれぞれのプロジェクトと VPC を定義し、Google Cloud ファイアウォール ルールを作成するための適切な権限を持っています。VPC 間でトラフィックが流れることを許可してはなりません。他の VPC を含むあらゆる送信元からのすべてのトラフィックをブロックし、VPC 内のファイアウォール ルールのみをそれぞれの部門に委任する必要があります。あなたは何をするべきか？
A. 各 VPC に VPC ファイアウォール ルールを作成し、優先度 1000 であらゆる送信元からのトラフィックをブロックします。
B. 部門のフォルダーごとに 2 つの階層型ファイアウォール ポリシーを作成し、それぞれに 2 つのルールを作成します。1 つはそれぞれの VPC に割り当てられたプライベート CIDR からのトラフィックと一致し、アクションを許可するように設定する優先度の高いルール、もう 1 つはブロックする優先度の低いルールです。他のソースからのトラフィック。
C. 各 VPC に VPC ファイアウォール ルールを作成し、優先度 0 で任意の送信元からのトラフィックをブロックします。
D. 部門のフォルダーごとに 2 つの階層型ファイアウォール ポリシーを作成し、それぞれに 2 つのルールを作成します。1 つはそれぞれの VPC に割り当てられたプライベート CIDR からのトラフィックと一致し、アクションを goto_next に設定する優先度の高いルール、もう 1 つはブロックする優先度の低いルールです。他のソースからのトラフィック。
Answer: A (メーッセージを残す**)**

最新問題: **61**
プロジェクト my-project には、Virtual Private Cloud (VPC) 内に 2 つのサブネットがあります。IP 範囲 10.128.0.0/20 の subnet-a と IP 範囲 172.16.0.0/24 の subnet-b です。データベース サーバーをサブネットに展開する必要があります。また、アプリケーション サーバーと Web サーバーを subnet-b に展開します。アプリケーション サーバーからデータベース サーバーへのデータベース トラフィックのみを許可するファイアウォール ルールを構成したいと考えています。あなたは何をするべきか？
A. サービス アカウント sa-app@my-project.iam.gserviceaccount.com および sa-db@my-project.iam.gserviceaccount.com を作成します。サービス アカウント sa-app をアプリケーション サーバーに関連付け、サービス アカウント sa-db をデータベース サーバーに関連付けます。次のコマンドを実行します。
gcloud compute firewall-rules create app-db-firewall-ru
--TCP を許可:3306 \
--source-service-accounts sa-app@democloud-idp-
デモ.iam.gserviceaccount.com \
--target-service-accounts sa-db@my-
project.iam.gserviceaccount.com
B. ネットワーク タグ app-server とサービス アカウント sa-db@my-project.iam.gserviceaccount.com を作成します。タグをアプリケーション サーバーに追加し、サービス アカウントをデータベース サーバーに関連付けます。次のコマンドを実行します。
gcloud compute firewall-rules create app-db-firewall-rule \
--アクション許可\
--方向入力 \
--ルールトップ:3306 \
--source-tags アプリサーバー \
--target-service-accounts sa-db@my-
project.iam.gserviceaccount.com

C. サービス アカウント sa-app@my-project.iam.gserviceaccount.com および sa-db@my-project.iam.gserviceaccount.com を作成します。サービス アカウント sa-app をアプリケーション サーバーに関連付け、サービス アカウント sa-db をデータベース サーバーに関連付けます。次のコマンドを実行します。
gcloud compute firewall-rules create app-db-firewall-ru
--TCP を許可:3306 \
--source-ranges 10.128.0.0/20 \
--source-service-accounts sa-app@my-
project.iam.gserviceaccount.com \
--target-service-accounts sa-db@my-
project.iam.gserviceaccount.com
D. ネットワーク タグ app-server および db-server を作成します。app-server タグをアプリケーション サーバーに追加し、db-server タグをデータベース サーバーに追加します。次のコマンドを実行します。
gcloud compute firewall-rules create app-db-firewall-rule \
--アクション許可\
--方向入力 \
--rules tcp:3306 \
--source-ranges 10.128.0.0/20 \
--source-tags アプリサーバー \
--target-tags データベースサーバー
Answer: (解答を表示する**)**

最新問題: **62**
あなたは最近、Google Cloud プロジェクトでネットワーク使用量が毎日繰り返し急増していることに気づきました。必要なコストと管理オーバーヘッドを最小限に抑えながら、トラフィック使用率の急増の原因となっている仮想マシン (VM) インスタンスとトラフィックの種類を特定する必要があります。あなたは何をするべきか？
A. すべてのトラフィックを VM に送信するようにパケット ミラーリングを構成します。VM 上で Wireshark を使用して、VPC 内の各 VM のトラフィック使用率を特定します。
B. 許可されたすべてのトラフィックに対してファイアウォール ルール ロギングを有効にし、分析のために出力を BigQuery に送信します。
C. VPC フロー ログを有効にし、分析のために出力を BigQuery に送信します。
D. サードパーティのネットワーク アプライアンスを展開し、デフォルト ゲートウェイとして構成します。サードパーティのネットワーク アプライアンスを使用して、ネットワーク トラフィックが多いユーザーを特定します。
Answer: A (メーッセージを残す**)**

最新問題: **63**
オンプレミスと GCP の間で Cloud VPN の使用量が増加しており、単一のトンネルで処理できるより多くのトラフィックをサポートしたいと考えています。Cloud VPN を使用して利用可能な帯域幅を増やしたいと考えています。
あなたは何をするべきか？
A. 別のパブリック IP アドレスを持つ 2 番目のオンプレミス VPN ゲートウェイを追加します。既存の Cloud VPN ゲートウェイ上に 2 番目のトンネルを作成します。このトンネルは同じ IP 範囲を転送しますが、新しいオンプレミス ゲートウェイ IP をポイントします。
B. オンプレミス VPN ゲートウェイの MTU を 1460 バイトから 2920 バイトに 2 倍にします。
C. 既存の VPN ゲートウェイとは異なるリージョンに 2 番目の Cloud VPN ゲートウェイを追加します。2 番目の Cloud VPN ゲートウェイ上に、同じ IP 範囲を転送するが、既存のオンプレミス VPN ゲートウェイの IP アドレスを指す新しいトンネルを作成します。
D. 同じ Cloud VPN ゲートウェイ上に、同じ宛先 VPN ゲートウェイ IP アドレスを指す 2 つの VPN トンネルを作成します。
Answer: D (メーッセージを残す**)**

最新問題: **64**
あなたは GCP に移行中の大学で働いています。
クラウドの要件は次のとおりです。
* 10 Gbps のオンプレミス接続
* クラウドへのアクセスのレイテンシが最も低い
* 集中ネットワーク管理チーム
新しい部門は、プロジェクトへのオンプレミス接続を求めています。キャンパスを Google Cloud に接続するために、最もコスト効率の高い相互接続ソリューションをデプロイしたいと考えています。
あなたは何をするべきか？
A. 共有 VPC を使用し、ホスト プロジェクトに VLAN アタッチメントと相互接続をデプロイします。
B. 共有 VPC を使用し、サービス プロジェクトに VLAN アタッチメントをデプロイします。VLAN アタッチメントを共有 VPC のホスト プロジェクトに接続します。
C. スタンドアロン プロジェクトを使用し、個々のプロジェクトに VLAN アタッチメントを展開します。VLAN アタッチメントをスタンドアロン プロジェクトの相互接続に接続します。
D. スタンドアロン プロジェクトを使用し、個々のプロジェクトのそれぞれに VLAN アタッチメントとインターコネクトを展開します。
Answer: (解答を表示する**)**
https://cloud.google.com/interconnect/docs/how-to/dicate/using-interconnects-other-projects 共有 VPC での Cloud Interconnect の使用 共有 VPC を使用して、プロジェクト内の VLAN アタッチメントを他の VPC ネットワークと共有できます。多数のプロジェクトを作成する必要があり、個々のプロジェクト所有者がオンプレミス ネットワークへの接続を管理できないようにしたい場合は、共有 VPC を選択することをお勧めします。このシナリオでは、ホスト プロジェクトには、サービス プロジェクトの VM で使用できる共通の共有 VPC ネットワークが含まれています。サービス プロジェクト内の VM はこのネットワークを使用するため、サービス プロジェクト管理者はサービス プロジェクト内に他の VLAN アタッチメントや Cloud Router を作成する必要はありません。このシナリオでは、共有 VPC ホスト プロジェクトでのみ Cloud Interconnect 接続用の VLAN アタッチメントと Cloud Router を作成する必要があります。VLAN アタッチメントとそれに関連付けられた Cloud Router の組み合わせは、特定の共有 VPC ネットワークに固有です。https://cloud.google.com/network-connectivity/docs/interconnect/how-to/enabling-multiple-networks-access-same-attachment#using_with
https://cloud.google.com/vpc/docs/shared-vpc

最新問題: **65**

あなたの組織には、デフォルトの VPC 構成を使用する us-east1、us-west4、europe-west4 のサブネットを持つ Google Cloud Virtual Private Cloud (VPC) があります。ヨーロッパの支社の従業員は、HA VPN を使用して VPC 内のリソースにアクセスする必要があります。europe-west4 にデプロイされた Cloud Router を使用して、組織の Google Cloud VPC に関連付けられた HA VPN を構成しました。ブランチ オフィスのユーザーが VPC 内のすべてのリソースに迅速かつ簡単にアクセスできるようにする必要があります。あなたは何をするべきか？
A. Cloud Router のアドバタイズされたルートをグローバルに設定します。
B. サブネットごとにカスタムのアドバタイズされたルートを作成します。
C. VPC 動的ルーティング モードをグローバルに設定します。
D. Cloud VPN を使用してブランチ オフィスに接続するように各サブネットの VPN 接続を構成します。
Answer: C (メーッセージを残す)

最新問題**: 66**
2 つのオブジェクトを含むストレージ バケットがあります。バケットでは Cloud CDN が有効になっており、両方のオブジェクトが正常にキャッシュされました。次に、2 つのオブジェクトのうちの 1 つがもうキャッシュされず、常にオリジンから直接インターネットに提供されるようにする必要があります。
あなたは何をするべきか？
A. キャッシュしたくないオブジェクトがパブリックに共有されていないことを確認してください。
B. 新しいストレージ バケットを作成し、チェックしたくないオブジェクトをその中に移動します。次に、バケット設定を編集し、プライベート属性を有効にします。
C. 2 つのオブジェクトを含むストレージ バケットに適切なライフサイクル ルールを追加します。
D. キャッシュしたくないオブジェクトのメタデータに値がプライベートの Cache-Control エントリを追加します。以前にキャッシュされたすべてのコピーを無効にします。
Answer: (解答を表示する)
https://cloud.google.com/cdn/docs/invalidating-cached-content

最新問題**: 67**
Cloud NAT を設定することにしました。構成を完了すると、インスタンスの 1 つがアウトバウンド NAT に Cloud NAT を使用していないことがわかります。
この問題の最も考えられる原因は何ですか?
A. インスタンスは複数のインターフェースで構成されています。
B. 外部 IP アドレスがインスタンスに構成されています。
C. RFC1918 範囲を使用する静的ルートを作成しました。
D. インスタンスはロード バランサーの外部 IP アドレスによってアクセスできます。
Answer: B (メーッセージを残す)
https://www.sovereignsolutionscorp.com/google-cloud-nat/

最新問題**: 68**
オンプレミス ホストに HTTP サービスと TFTP サービスを提供する新しい内部アプリケーションをデプロイしました。トラフィックを複数の Compute Engine インスタンスに分散できるようにしたいと考えていますが、クライアントが両方のサービスにわたって特定のインスタンスに固定されるようにする必要があります。
どのセッション アフィニティを選択する必要がありますか?

A. クライアント IP とプロトコル
B. クライアント IP、ポート、プロトコル
C. クライアントIP
D. なし
Answer: C (メーッセージを残す)

最新問題: **69**
HTTP、HTTPS、および SSH ポート経由のトラフィックのみを許可するルールを使用してファイアウォールを作成しました。テスト中は、具体的には複数のポートとプロトコルを介してサーバーにアクセスしようとします。ただし、ファイアウォール ログには拒否された接続は表示されません。あなたは問題を解決したいと考えています。
あなたは何をするべきか？
A. トラフィックを受信する VM インスタンスでのログ記録を有効にします。
B. 明示的な拒否ルールを作成し、新しいルールでのログ記録を有効にします。
C. デフォルトの 「拒否」ファイアウォール ルールでログを有効にします。
D. フィルターなしですべてのファイアウォール ログを転送するログ シンクを作成します。
Answer: A (メーッセージを残す)

最新問題: **70**
あなたの組織は、3 つの異なる部門に 1 つのプロジェクトを展開しています。これらの部門のうち 2 つは相互にネットワーク接続を必要としますが、3 番目の部門は分離したままにする必要があります。設計では、これらの部門間に個別のネットワーク管理ドメインを作成する必要があります。運用上のオーバーヘッドを最小限に抑えたい。
トポロジーはどのように設計すればよいでしょうか?
A. 共有 VPC ホスト プロジェクトと、3 つの個別の部門ごとにそれぞれのサービス プロジェクトを作成します。
B. 3 つの個別の VPC を作成し、Cloud VPN を使用して 2 つの適切な VPC 間の接続を確立します。
C. 3 つの個別の VPC を作成し、VPC ピアリングを使用して 2 つの適切な VPC 間の接続を確立します。
D. 単一のプロジェクトを作成し、特定のファイアウォール ルールを展開します。ネットワーク タグを使用して、部門間のアクセスを分離します。
Answer: (解答を表示する)
共有 VPC を使用して、共通の VPC ネットワークに接続します。これらのプロジェクト内のリソースは、内部 IP を使用してプロジェクトの境界を越えて安全かつ効率的に相互に通信できます。サブネット、ルート、ファイアウォールなどの共有ネットワーク リソースを中央のホスト プロジェクトから管理できるため、プロジェクト全体に一貫したネットワーク ポリシーを適用して強制できます。
共有 VPC と IAM コントロールを使用すると、ネットワーク管理をプロジェクト管理から分離できます。この分離は、最小特権の原則を実装するのに役立ちます。たとえば、集中ネットワーク チームは、参加プロジェクトへの権限がなくてもネットワークを管理できます。同様に、プロジェクト管理者は、共有ネットワークを操作する権限がなくても、プロジェクト リソースを管理できます。

最新問題: **71**
あなたは共有 VPC アーキテクチャを設計しています。ネットワークおよびセキュリティ チームは、部門間でどのルートが公開されるかを厳密に制御しています。制作部門とステージング部門は相互に通信できますが、特定のネットワーク経由でのみ通信できます。Google が推奨する慣行に従いたいと考えています。
このトポロジをどのように設計すればよいでしょうか?

A. 共有 VPC サービス プロジェクト内に 2 つの共有 VPC を作成し、それらの間にクラウド VPN/クラウド ルーターを作成します。フレキシブル ルート アドバタイズメント (FRA) を使用して、特定のネットワーク間のアクセスをフィルタリングします。
B. 共有 VPC ホスト プロジェクト内に 2 つの共有 VPC を作成し、それらの間にクラウド VPN/クラウド ルーターを作成します。フレキシブル ルート アドバタイズメント (FRA) を使用して、特定のネットワーク間のアクセスをフィルタリングします。
C. 共有 VPC ホスト プロジェクト内に 1 つの VPC を作成し、個々のサブネットをサービス プロジェクトと共有して、特定のネットワーク間のアクセスをフィルターします。
D. 共有 VPC ホスト プロジェクト内に 2 つの共有 VPC を作成し、それらの間の VPC ピアリングを有効にします。ファイアウォール ルールを使用して、特定のネットワーク間のアクセスをフィルタリングします。
Answer: (解答を表示する**)**

最新問題**: 72**
あなたの会社はパートナーと協力して顧客にソリューションを提供しています。あなたの会社とパートナー組織は両方とも GCP を使用しています。パートナーのネットワークには、会社の VPC 内の一部のリソースにアクセスする必要があるアプリケーションがあります。VPC 間に CIDR の重複はありません。
セキュリティを損なうことなく望ましい結果を達成するには、どの 2 つのソリューションを実装できますか?
(2つお選びください。)
A. VPC ピアリング
B. 共有 VPC
C. クラウドVPN
D. 専用インターコネクト
E. クラウド NAT
Answer: (解答を表示する**)**
説明 参考 :https://cloud.google.com/vpc/docs/vpc

最新問題**: 73**
共有 VPC をセットアップし、3 つのプロジェクトを作成しました。ホスト プロジェクト、サービス プロジェクト-1、およびサービス プロジェクト-2。us-west1 の subnet-1 と subnet-2 の 2 つのサブネットを作成しました。
ホスト プロジェクトの us-central1 に 2。サービス プロジェクト -1 と共有されているのはサブネット 1 のみですが、サービス プロジェクト 1 の VPC ネットワークに移動すると、サービス プロジェクト 1 と共有されていないサブネット 2 も表示されます。サブネット 2 がサービス プロジェクト 1 で利用できる理由を以下から正しいオプションを選択してください。注 ホスト プロジェクトは共有 VPC のホスト プロジェクトであり、サービス プロジェクト-1とサービス プロジェクト-2は共有 VPC のサービス プロジェクトです。
A. 現在のユーザーは共有 VPC 管理者ロールを持っており、共有 VPC 管理者ロールがあれば、すべてのネットワークが利用可能になります。
B. これは Google Cloud のバグです。報告してください。
C. デフォルトでは、すべてのサブネットが使用可能です。
D. 現在のユーザーから共有ネットワーク管理者の役割を削除します。
Answer: A (メーッセージを残す**)**
現在のユーザーが共有 VPC 管理者ロールを持っている場合、サービス プロジェクトとのサブネット レベルの共有権限に関係なく、ユーザーは共有 VPC 内のすべてのネットワークを利用できるため、オプション A が正しい選択です。
選択肢 B はバグではないため、不正解です。

オプション C は不正解です。現在のユーザーが共有管理者の役割を持っている場合、すべてのサブネットが使用可能になります。
オプション D は不正解です。共有ネットワーク管理者の役割が存在しません。

最新問題: **74**
ストレージ バケット内のすべてのオブジェクトに対して Cloud CDN を有効にする必要があります。ストレージ バケット内のすべてのオブジェクトが CDN によって提供されることを確認したいと考えています。
GCP Console では何をすればよいでしょうか?
A. 新しい SSL プロキシ ロードバランサを作成し、バックエンドとしてストレージ バケットを選択して、バックエンドで Cloud CDN を有効にします。
B. 新しい TCP ロードバランサを作成し、ストレージ バケットをバックエンドとして選択して、バックエンドで Cloud CDN を有効にします。
C. 新しいクラウド ストレージ バケットを作成し、そのバケット上で Cloud CDN を有効にします。
D. 新しい HTTP ロードバランサを作成し、バックエンドとしてストレージ バケットを選択し、バックエンドで Cloud CDN を有効にして、ストレージ バケット内の各オブジェクトがパブリックに共有されていることを確認します。
Answer: (解答を表示する**)**

最新問題: **75**
トラフィックを検査するためにサードパーティの次世代ファイアウォールを使用しています。送信トラフィックをファイアウォールにルーティングするカスタム ルート 0.0.0.0/0 を作成しました。パブリック IP アドレスを持たない VPC インスタンスが、ファイアウォールを介してトラフィックを送信せずに BigQuery および Cloud Pub/Sub API にアクセスできるようにしたいと考えています。
どの 2 つのアクションを取る必要がありますか? (2つお選びください。)
A. サブネット レベルで限定公開の Google アクセスをオンにします。
B. VPC レベルでプライベート サービス アクセスをオンにします。
C. デフォルトのインターネット ゲートウェイ経由で Google API およびサービスの内部 IP アドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
D. VPC レベルで限定公開の Google アクセスを有効にします。
E. デフォルトのインターネット ゲートウェイ経由で Google API およびサービスの外部 IP アドレスにトラフィックを送信するためのカスタム静的ルートのセットを作成します。
Answer: (解答を表示する**)**

最新問題: **76**
Cloud DNS が管理するゾーンの 1 つで DNSSEC を無効にしています。ゾーン ファイルから DS レコードを削除し、キャッシュから期限切れになるのを待って、ゾーンの DNSSEC を無効にしました。DNSSEC 検証解決がゾーン内の名前を解決できないというレポートを受け取ります。
あなたは何をするべきか？
A. ドメイン レジストラで DNSSEC を無効にします。
B. ゾーンの TTL を更新します。
C. ドメインの所有権を新しいレジストラに譲渡します。
使用するマネージド ゾーンの DNSSEC を無効にする前に、ドメイン レジストラーで DNSSEC を無効にして、DNSSEC 検証リゾルバーが引き続きゾーン内の名前を解決できることを確認する必要があります。
D. ゾーンを TRANSFER 状態に設定します。
Answer: A (メーッセージを残す**)**

最新問題: **77**
Retail という名前の VPC ネットワークを自動モードで作成しました。Distribution という名前の VPC ネットワークを作成し、Retail VPC とピアリングしたいと考えています。
ディストリビューション VPC はどのように構成すればよいですか?
A. デフォルト VPC の名前を Distribution」に変更し、ネットワーク ピアリング経由でピアします。
B. 自動モードでディストリビューション VPC を作成します。ネットワーク ピアリングを介して両方の VPC をピアリングします。
C. カスタム モードでディストリビューション VPC を作成します。CIDR 範囲 10.0.0.0/9 を使用します。必要なサブネットを作成し、ネットワーク ピアリング経由でピアリングします。
D. カスタム モードでディストリビューション VPC を作成します。CIDR 範囲 10.128.0.0/9 を使用します。必要なサブネットを作成し、ネットワーク ピアリング経由でピアリングします。
Answer: C (メーッセージを残す**)**

最新問題: **78**
HTTP(S) 負荷分散サービスが作成されました。バックエンド インスタンスが適切に応答していることを確認する必要があります。
ヘルスチェックをどのように設定すればよいでしょうか?
A. request-path をヘルスチェックに使用する特定の URL に設定し、proxy-header を PROXY_V1 に設定します。
B. request-path をヘルス チェックに使用される特定の URL に設定し、host を設定してヘルス チェックを識別するカスタム ホスト ヘッダーを含めます。
C. request-path をヘルスチェックに使用する特定の URL に設定し、response をバックエンド サービスが応答本文で常に返す文字列に設定します。
D. プロキシ ヘッダーをデフォルト値に設定し、ヘルス チェックを識別するカスタム ホスト ヘッダーを含めるようにホストを設定します。
Answer: B (メーッセージを残す**)**
https://cloud.google.com/load-balancing/docs/health-checks

最新問題: **79**
あなたの会社のウェブサーバー管理者は、アプリケーションのオンプレミスのバックエンド サーバーを GCP に移行しています。ライブラリと構成は、これらのバックエンド サーバー間で大きく異なります。
GCP への移行はリフトアンドシフトで行われ、サーバーへのすべてのリクエストは単一のネットワーク ロード バランサー フロントエンドによって処理されます。可能であれば、GCP ネイティブ ソリューションを使用したいと考えています。
このサービスを GCP にどのようにデプロイする必要がありますか?
A. オンプレミス サーバーのイメージの 1 つからマネージド インスタンス グループを作成し、このインスタンス グループをロード バランサーの背後にあるターゲット プールにリンクします。
B. ターゲット プールを作成し、すべてのバックエンド インスタンスをこのターゲット プールに追加し、ロード バランサの背後にターゲット プールをデプロイします。

C. これらのバックエンド サーバー間の大きな違いに対応できるように、サードパーティの仮想アプライアンスをフロントエンドとしてこれらのサーバーにデプロイします。
D. GCP の ECMP 機能を使用して、バックエンド サーバーに複数の等しい優先順位の静的ルートをインストールすることで、バックエンド サーバーへのトラフィックの負荷を分散します。
Answer: B (メーッセージを残す)
https://cloud.google.com/compute/docs/instance-groups/adding-an-instance-group-to-a-load-balancer

最新問題**: 80**
あなたの会社は最近、EMEA ベースの事業を APAC に拡大しました。世界中に分散しているユーザーから、SMTP サービスと IMAP サービスが遅いと報告されています。あなたの会社ではエンドツーエンドの暗号化が必要ですが、SSL 証明書にアクセスできません。
どの Google Cloud ロードバランサを使用する必要がありますか?
A. SSL プロキシ ロード バランサ
B. ネットワークロードバランサー
C. HTTPS ロードバランサ
D. TCP プロキシ ロード バランサ
Answer: D (メーッセージを残す)
https://cloud.google.com/security/encryption-in-transit/ GFE とバックエンド間の自動暗号化 次のロードバランサ タイプの場合、Google は Google フロント エンド（GFE）と Google Cloud 内にあるバックエンド間のトラフィックを自動的に暗号化します。VPC ネットワーク: HTTP(S) ロード バランシング TCP プロキシ ロード バランシング SSL プロキシ ロード バランシング

最新問題**: 81**
会社のオンプレミス ネットワークは、Cloud VPN トンネルを使用して VPC に接続されています。VPC で定義されたネクストホップとして VPN トンネルを持つ 0.0.0.0/0 の静的ルートがあります。現在、インターネットに向かうすべてのトラフィックはオンプレミス ネットワークを通過します。1 つのリージョン内の Compute Engine インスタンスのプライマリ IP アドレスを変換するように Cloud NAT を構成しました。これらのインスタンスからのトラフィックは、オンプレミス ネットワークからではなく、VPC から直接インターネットに到達するようになります。仮想マシン (VM) からのトラフィックが予想どおりにアドレスを変換しません。あなたは何をするべきか？
A. NAT ゲートウェイの TCP 確立接続アイドル タイムアウトを短くします。
B. クラウド NAT ゲートウェイのデフォルトの min-ports-per-vm 設定を増やします。
C. 外部 NAT IP アドレスの上り下りを許可し、Compute Engine インスタンス上にターゲット タグがあり、VPN ゲートウェイへのデフォルト ルートの優先度値よりも高い優先度値を持つファイアウォール ルールを追加します。
D. ネクストホップとしてデフォルトのインターネット ゲートウェイ、Compute Engine インスタンスに関連付けられたネットワーク タグ、および VPN トンネルへのデフォルト ルートの優先度よりも高い優先度を使用して、デフォルトの静的ルートを VPC に追加します。
Answer: A (メーッセージを残す)

最新問題**: 82**
パブリック IP アドレス経由で Cloud SQL にアクセスでき、サードパーティのサービス プロバイダを必要としない、Google への専用接続を確立したいと考えています。
どの接続タイプを選択する必要がありますか?
A. キャリアピアリング
B. ダイレクトピアリング

C. 専用インターコネクト
D. パートナー相互接続
Answer: B (メーッセージを残す**)**
参照：
https://cloud.google.com/interconnect/docs/how-to/direct-peering

最新問題**: 83**
あなたの組織では、今後の法的手続きでの分析に備えて、すべてのアプリケーションからのメトリクスを 5 年間保持することが求められています。どのアプローチを使用する必要がありますか?
A. すべてのプロジェクトに対して Stackdriver Monitoring を構成し、BigQuery にエクスポートします。
B. デフォルトの保持ポリシーを使用して、すべてのプロジェクトの Stackdriver Monitoring を構成します。
C. すべてのプロジェクトに対して Stackdriver Monitoring を構成し、Google Cloud Storage にエクスポートします。
D. セキュリティ チームに各プロジェクトのログへのアクセスを許可します。
Answer: C (メーッセージを残す**)**
B と D は、いずれも要件に対する適切な解決策ではないため、すぐに除外できます。
5年間保有」
A と C の違いは、BigQuery と Cloud Storage のどちらに保存するかです。主な関心事は保存期間の延長であるため、C (正解) がより適切な答えであり、たとえば Coldline ストレージ クラスを使用するなど、 将来の分析のために 5 年間保存される」という条件がさらに適格となります。
BigQuery に関しては、低コストのストレージでもありますが、主な目的は分析です。
また、Cloud Storage のログは、必要に応じていつでも簡単に BigQuery に転送できます。

最新問題**: 84**
エンド ユーザーは us-east1 と europe-west1 のすぐ近くにいます。それらのワークロードは相互に通信する必要があります。コストを最小限に抑え、ネットワーク効率を向上させたいと考えています。
このトポロジをどのように設計すればよいでしょうか?
A. それぞれ独自のリージョンと個別のサブネットを持つ 2 つの VPC を作成します。2 つの VPN ゲートウェイを作成して、これらのリージョン間の接続を確立します。
B. それぞれ独自のリージョンと個別のサブネットを持つ 2 つの VPC を作成します。インスタンスの外部 IP アドレスを使用して、これらのリージョン間の接続を確立します。
C. 2 つのリージョン サブネットを持つ 1 つの VPC を作成します。グローバル ロード バランサーを作成して、リージョン間の接続を確立します。
D. 2 つのリージョン サブネットを持つ 1 つの VPC を作成します。これらのサブネットにワークロードをデプロイし、プライベート RFC1918 IP アドレスを使用して通信させます。
Answer: D (メーッセージを残す**)**
VPC ネットワーク ピアリングを使用すると、VPC ネットワークをピアリングできるため、異なる VPC ネットワーク内のワークロードがプライベート RFC 1918 スペースで通信できるようになります。トラフィックは Google のネットワーク内に留まり、公共のインターネットを通過しません。

最新問題**: 85**
HTTP(s) ロードバランサをデプロイしましたが、Compute Engine 仮想マシン インスタンスのポート 80 へのヘルスチェックが失敗し、インスタンスにトラフィックが送信されません。あなたは問題を解決したいと考えています。どのコマンドを実行すればよいでしょうか?

A. gcloud compute firewall-rules createallow-lb --network load-balancer --allow tcp --destination-ranges 130.211.0.0/22,35.191.0.0/16 --direction EGRESS
B. gcloud compute firewall-rules createallow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS
C. gcloud compute インスタンス add-access-config インスタンス-1
D. gcloud compute health-checks update http health-check --unhealthy-threshold 10
Answer: C (メーッセージを残す**)**

最新問題**: 86**
自動モードの VPC ネットワークをカスタム モードに変換しました。変換後、Cloud Deployment Manager テンプレートの一部は機能しなくなりました。あなたは問題を解決したいと考えています。
あなたは何をするべきか？
A. 追加の IAM ロールを Google API のサービス アカウントに適用して、カスタム モード ネットワークを許可します。
B. VPC ファイアウォールを更新して、Cloud Deployment Manager がカスタム モード ネットワークにアクセスできるようにします。
C. Cloud Armor ホワイトリストでカスタム モード ネットワークを明示的に参照します。
D. Deployment Manager テンプレートでカスタム モード ネットワークを明示的に参照します。
Answer: D (メーッセージを残す**)**

最新問題**: 87**
あなたは最近、組織の ID とアクセス管理の管理を任されました。いくつかのプロジェクトがあり、可能な限りスクリプトと自動化を使用したいと考えています。プロジェクト メンバーに編集者の役割を付与したいと考えています。
これを実現するには、どの 2 つの方法を使用できますか? (2つお選びください。)
REST API 経由の GetIamPolicy()
A. REST API 経由の setIamPolicy()
B. gcloud pubsub add-iam-policy-binding $projectname --member user:$username --
C. 役割 役割/編集者
gcloud プロジェクト add-iam-policy-binding $projectname --member user:$username --
D. 役割 役割/編集者
E. [メンバーの追加] フィールドにメール アドレスを入力し、GCP Console のドロップダウン メニューから目的のロールを選択します。
Answer: D,E (メーッセージを残す**)**
説明/参照: https://cloud.google.com/iam/docs/granting-changing-revoking-access

最新問題**: 88**
個人の SSH キーがプロジェクト内のすべてのインスタンスで機能することを確認する必要があります。これをできるだけ効率的に達成したいと考えています。
あなたは何をするべきか？
A. 公開 SSH キーをプロジェクトのメタデータにアップロードします。
B. 公開 SSH キーを各インスタンスのメタデータにアップロードします。
C. 公開 ssh キーが埋め込まれたカスタム Google Compute Engine イメージを作成します。
D. gcloud compute ssh を使用して、公開 SSH キーをインスタンスに自動的にコピーします。
Answer: A (メーッセージを残す**)**

概要 SSH キーを作成および管理することにより、ユーザーがサードパーティ ツールを介して Linux インスタンスにアクセスできるようになります。SSH キーは次のファイルで構成されます。インスタンス レベルのメタデータまたはプロジェクト全体のメタデータに適用される公開 SSH キー ファイル。ユーザーがローカル デバイスに保存する秘密 SSH キー ファイル。ユーザーが秘密 SSH 鍵を提示すると、Google Cloud プロジェクトのメンバーでなくても、サードパーティ ツールを使用して、一致する公開 SSH 鍵ファイルで構成されているインスタンスに接続できます。したがって、1 つ以上のインスタンスの公開 SSH キー メタデータを変更することで、ユーザーがアクセスできるインスタンスを制御できます。https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey

最新問題: **89**
あなたの会社のウェブサーバー管理者は、アプリケーションのオンプレミスのバックエンド サーバーを GCP に移行しています。ライブラリと構成は、これらのバックエンド サーバー間で大きく異なります。GCP への移行はリフトアンドシフトで行われ、サーバーへのすべてのリクエストは単一のネットワーク ロード バランサー フロントエンドによって処理されます。可能であれば、GCP ネイティブ ソリューションを使用したいと考えています。
このサービスを GCP にどのようにデプロイする必要がありますか?
A. オンプレミス サーバーのイメージの 1 つからマネージド インスタンス グループを作成し、このインスタンス グループをロード バランサーの背後にあるターゲット プールにリンクします。
B. GCP の ECMP 機能を使用して、バックエンド サーバーに複数の同じ優先順位の静的ルートをインストールすることで、バックエンド サーバーへのトラフィックの負荷を分散します。
C. ターゲット プールを作成し、すべてのバックエンド インスタンスをこのターゲット プールに追加し、ロード バランサの背後にターゲット プールをデプロイします。
D. これらのバックエンド サーバー間の大きな違いに対応できるように、サードパーティの仮想アプライアンスをフロントエンドとしてこれらのサーバーにデプロイします。
Answer: C (メーッセージを残す)

最新問題: **90**
新しいアプリケーションを作成していて、パブリック IP アドレスなしで VPC インスタンスから Cloud SQL にアクセスする必要があるとします。
どの 2 つのアクションを取る必要がありますか? (2つお選びください。)
A. プロジェクトでサービス ネットワーキング API をアクティブ化します。
B. プロジェクトで Cloud Datastore API をアクティブ化します。
C. サービス プロデューサーへのプライベート接続を作成します。
D. トラフィックが Cloud SQL API に到達できるようにするカスタム静的ルートを作成します。
E. プライベート Google アクセスを有効にします。
Answer: A,C (メーッセージを残す)
参照：
https://cloud.google.com/sql/docs/mysql/private-ip

最新問題: **91**
ネットワーク運用チームの各メンバーに、Cloud Interconnect VLAN アタッチメントを作成、変更、削除するための最小限の権限アクセスを付与する必要があります。
あなたは何をするべきか？
A. 各ユーザーに編集者の役割を割り当てます。

B. 各ユーザーに compute.networkAdmin ロールを割り当てます。
C. 各ユーザーに compute.interconnectAttachments.create、compute.interconnectAttachments.get の権限のみを与えます。
D. 各ユーザーに次の権限のみを与えます:
compute.interconnectAttachments.create、compute.interconnectAttachments.get、compute.routers.create、compute.routers.get、compute.routers.update。
Answer: C (メーッセージを残す**)**
説明/参照:

最新問題: **92**
あなたは組織のネットワーク アーキテクチャを設計しています。あなたの組織には、Web、アプリ、データベースの 3 つの開発者チームがあります。すべての開発者チームは、重要なタスクを実行するために Compute Engine インスタンスにアクセスする必要があります。あなたは、開発者にネットワーク アクセスを提供する必要がある小規模なネットワークおよびセキュリティ チームの一員です。サブネット、ルート、ファイアウォールなどのネットワーク リソースに対する集中制御を維持する必要があります。運用上のオーバーヘッドを最小限に抑えたい。このトポロジをどのように設計すればよいでしょうか?
A. Web 用に 1 つの VPC、アプリ用に 1 つの VPC、データベース用に 1 つの VPC を構成します。VPC ネットワーク ピアリングを使用して、すべての VPC をフルメッシュで接続します。
B. Web 用に 1 つの VPC、アプリ用に 1 つの VPC、データベース用に 1 つの VPC を構成します。各 VPC 間に HA VPN を構成します。
C. 共有 VPC を使用してホスト プロジェクトを構成します。Web、アプリ、データベースのサービス プロジェクトを作成します。
D. 3 つの共有 VPC ホスト プロジェクトを構成し、それぞれにサービス プロジェクトを設定します (Web 用に 1 つ、アプリ用に 1 つ、データベース用に 1 つ)。
Answer: D (メーッセージを残す**)**

最新問題: **93**
リード エンジニアは、レガシー データ センターに仮想マシンを展開するカスタム ツールを作成しました。彼はカスタム ツールを新しいクラウド環境に移行したいと考えています。あなたは、Google Cloud Deployment Manager の導入を提唱したいと考えています。Cloud Deployment Manager への移行による 2 つのビジネス リスクは何ですか? 2 つの答えを選択してください
A. Cloud Deployment Manager は Python を使用します。
B. Cloud Deployment Manager は、Google Cloud リソースの自動化のみをサポートします。
C. Cloud Deployment Manager を使用して、クラウド リソースを完全に削除できます。
D. Cloud Deployment Manager API は将来廃止される可能性があります。
E. Cloud Deployment Manager を実行するには、Google API サービス アカウントが必要です。
F. Cloud Deployment Manager は、会社のエンジニアにとって馴染みのないものです。
Answer: (解答を表示する**)**

最新問題: **94**
アプリケーション開発チームは、現在のログ ツールでは新しいクラウドベース製品のニーズを満たせないと考えています。彼らは、エラーを捕捉し、履歴ログ データの分析に役立つ、より優れたツールを求めています。彼らのニーズを満たすソリューションを見つけられるように支援したいと考えています。どうすればよいでしょうか?
A. ログのベスト プラクティスに関するオンライン リソースのリストを送信します。
B. 要件を定義し、実行可能なログ ツールを評価できるように支援します。
C. 新しい機能を利用できるように、現在のツールをアップグレードできるように支援します。
D. Google StackDriver ロギング エージェントをダウンロードしてインストールするように指示します。
Answer: B (メーッセージを残す**)**
A と D は、一般的な IT の優れた実践方法ではないため、除外できます。彼らは単に製品を販売したり、説明なしに混雑したリソースを案内したりするだけではなく、あなたの助けを必要としています。
B (正解) - 要件を定義し、実行可能なロギング ツールを評価できるように支援します。彼らは要件と既存のツールの問題を知っています。StackDriver Logging と Error Reporting がすべての要件を満たしているのは事実ですが、新しいツール、特にエラーをキャプチャして履歴ログ データの分析に役立つロギング ツールを評価するための専門知識を提供していただく必要がありますか?
C - 新しい機能を利用できるように、現在のツールをアップグレードできるように支援します。彼らはすでにそれらのツールを使用しており、その欠点を知っています。より良いものを見つけるためにあなたの助けが必要です。新機能のためにアップグレードを支援するだけでは十分ではなく、問題を解決できない可能性があります。

最新問題: **95**
あなたには、組織のエンタープライズ ネットワークが Google Workspace にアクセスして使用するための新しい接続ソリューションを設計する責任があります。us-west1 に Compute Engine インスタンスを含む既存の共有 VPC があります。現在、サービス プロバイダのインターネット アクセスを介して Google Workspace にアクセスしています。ネットワークと Google の間に直接接続を設定したいと考えています。あなたは何をするべきか？
A. 同じ大都市圏でキャリア ピアリング接続を注文します。Google とルーターの間にボーダー ゲートウェイ プロトコル (BGP) セッションを構成します。
B. 同じ大都市圏でダイレクト ピアリング接続を注文します。Google とルーターの間にボーダー ゲートウェイ プロトコル (BGP) セッションを構成します。
C. 同じ大都市圏で Ddedicate Interconnect 接続を注文します。VLAN アタッチメント、us-west1 の Cloud Router、および Cloud Router とルーター間のボーダー ゲートウェイ プロトコル (BGP) セッションを作成します。
D. us-west1 で HA VPN を構成します。Cloud Router とオンプレミス データセンターの間にボーダー ゲートウェイ プロトコル (BGP) セッションを構成します。
Answer: (解答を表示する**)**

最新問題: **96**
エンド ユーザーは us-east1 と europe-west1 のすぐ近くにいます。それらのワークロードは相互に通信する必要があります。コストを最小限に抑え、ネットワーク効率を向上させたいと考えています。
このトポロジをどのように設計すればよいでしょうか?
A. それぞれ独自のリージョンと個別のサブネットを持つ 2 つの VPC を作成します。2 つの VPN ゲートウェイを作成して、これらのリージョン間の接続を確立します。

B. それぞれ独自のリージョンと個別のサブネットを持つ 2 つの VPC を作成します。インスタンスの外部 IP アドレスを使用して、これらのリージョン間の接続を確立します。
C. 2 つのリージョン サブネットを持つ 1 つの VPC を作成します。グローバル ロード バランサーを作成して、リージョン間の接続を確立します。
D. 2 つのリージョン サブネットを持つ 1 つの VPC を作成します。これらのサブネットにワークロードをデプロイし、プライベート RFC1918 IP アドレスを使用して通信させます。
Answer: (解答を表示する**)**
VPC ネットワーク ピアリングを使用すると、VPC ネットワークをピアリングできるため、異なる VPC ネットワーク内のワークロードがプライベート RFC 1918 スペースで通信できるようになります。トラフィックは Google のネットワーク内に留まり、公共のインターネットを通過しません。
参考: https://cloud.google.com/vpc/docs/vpc-peering

最新問題**: 97**
単一の Dended Interconnect が正常にプロビジョニングされました。物理接続は、us-west2 に最も近いコロケーション施設にあります。ワークロードの 75% は us-east4 にあり、ワークロードの残りの 25% は us-central1 にあります。すべてのワークロードは同じネットワーク トラフィック プロファイルを持ちます。VLAN アタッチメントを展開するときは、データ転送コスト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. us-east4 に最も近いコロケーション施設用に新しい専用インターコネクトを注文し、VPC グローバル ルーティングを使用して us-central1 のワークロードにアクセスします。
B. us-central1 に最も近いコロケーション施設用に新しい専用インターコネクトを注文し、VPC グローバル ルーティングを使用して us-east4 のワークロードにアクセスします。
C. 既存の専用インターコネクトを維持します。VLAN アタッチメントを us-east4 の Cloud Router にデプロイし、別の VLAN アタッチメントを us-central1 の Cloud Router にデプロイします。
D. 既存の専用インターコネクトを維持します。VLAN アタッチメントを us-west2 の Cloud Router にデプロイし、VPC グローバル ルーティングを使用して us-east4 と us-central1 のワークロードにアクセスします。
Answer: A (メーッセージを残す**)**

最新問題**: 98**
HTTP(S) 負荷分散サービスが作成されました。バックエンド インスタンスが適切に応答していることを確認する必要があります。
ヘルスチェックをどのように設定すればよいでしょうか?
A. request-path をヘルスチェックに使用する特定の URL に設定し、response をバックエンド サービスが応答本文で常に返す文字列に設定します。
B. ヘルスチェックに使用される特定の URL に request-path を設定し、ヘルスチェックを識別するカスタム ホスト ヘッダーを含むように host を設定します。
C. プロキシ ヘッダーをデフォルト値に設定し、ヘルス チェックを識別するカスタム ホスト ヘッダーを含めるようにホストを設定します。
D. request-path をヘルスチェックに使用する特定の URL に設定し、proxy-header を PROXY_V1 に設定します。
Answer: B (メーッセージを残す**)**

最新問題**: 99**
開発チーム用に新しい VPC を作成しました。SSH 経由のみでこの VPC 内のリソースへのアクセスを許可したいと考えています。
ファイアウォール ルールをどのように構成すればよいでしょうか?
A. 2 つのファイアウォール ルールを作成します。1 つは優先度 0 のすべてのトラフィックをブロックし、もう 1 つは優先度 1000 でポート 22 を許可します。

B. 2 つのファイアウォール ルールを作成します。1 つは優先度 65536 のすべてのトラフィックをブロックし、もう 1 つは優先度 1000 のポート 3389 を許可します。
C. 優先度 1000 のポート 22 を許可する単一のファイアウォール ルールを作成します。
D. 優先度 1000 のポート 3389 を許可する単一のファイアウォール ルールを作成します。
Answer: (解答を表示する**)**
参照：
https://geekflare.com/gcp-firewall-configuration/

最新問題**: 100**
サブネット レベルの分離を実現するには、あるサブネットのインスタンス A が、別のサブネットのインスタンス B と呼ばれるセキュリティ アプライアンスを経由するようにルーティングする必要があります。
あなたは何をするべきか？
A. システム生成のサブネット ルートよりも具体的なルートを作成し、ネクスト ホップをタグなしでインスタンス B に向けます。<B>: システム生成のサブネット ルートよりも具体的なルートを作成し、インスタンス A に適用されたタグを使用して
ネクスト ホップをインスタンス B に向けます。
B. システム生成のサブネット ルートを削除し、インスタンス A に適用されたタグを使用してインスタンス B への特定のルートを作成します。
C. インスタンス B を別の VPC に移動し、マルチ NIC を使用してインスタンス B のインターフェイスをインスタンス A のネットワークに接続します。トラフィックがインスタンス A に強制的に通過するように適切なルートを構成します。
Answer:
説明/参照:

最新問題**: 101**
あなたの組織は、3 つの異なる部門に 1 つのプロジェクトを展開しています。これらの部門のうち 2 つは相互にネットワーク接続を必要としますが、3 番目の部門は分離したままにする必要があります。設計では、これらの部門間に個別のネットワーク管理ドメインを作成する必要があります。運用上のオーバーヘッドを最小限に抑えたい。
トポロジーはどのように設計すればよいでしょうか?
A. 共有 VPC ホスト プロジェクトと、3 つの個別の部門ごとにそれぞれのサービス プロジェクトを作成します。
B. 3 つの個別の VPC を作成し、Cloud VPN を使用して 2 つの適切な VPC 間の接続を確立します。
C. 3 つの個別の VPC を作成し、VPC ピアリングを使用して 2 つの適切な VPC 間の接続を確立します。
D. 単一のプロジェクトを作成し、特定のファイアウォール ルールを展開します。ネットワーク タグを使用して、部門間のアクセスを分離します。
Answer: A (メーッセージを残す**)**
共有 VPC を使用して、共通の VPC ネットワークに接続します。これらのプロジェクト内のリソースは、内部 IP を使用してプロジェクトの境界を越えて安全かつ効率的に相互に通信できます。サブネット、ルート、ファイアウォールなどの共有ネットワーク リソースを中央のホスト プロジェクトから管理できるため、プロジェクト全体に一貫したネットワーク ポリシーを適用して強制できます。
共有 VPC と IAM コントロールを使用すると、ネットワーク管理をプロジェクト管理から分離できます。この分離は、最小特権の原則を実装するのに役立ちます。たとえば、集中ネットワーク チームは、参加プロジェクトへの権限がなくてもネットワークを管理できます。同様に、プロジェクト管理者は、共有ネットワークを操作する権限がなくても、プロジェクト リソースを管理できます。
参考: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

最新問題**: 102**

ストレージ バケット内のすべてのオブジェクトに対して Cloud CDN を有効にする必要があります。ストレージ バケット内のすべてのオブジェクトが CDN によって提供されることを確認したいと考えています。
GCP Console では何をすればよいでしょうか?
A. 新しいクラウド ストレージ バケットを作成し、そのバケット上で Cloud CDN を有効にします。
B. 新しい TCP ロードバランサを作成し、ストレージ バケットをバックエンドとして選択して、バックエンドで Cloud CDN を有効にします。
C. 新しい SSL プロキシ ロードバランサを作成し、バックエンドとしてストレージ バケットを選択して、バックエンドで Cloud CDN を有効にします。
D. 新しい HTTP ロードバランサを作成し、バックエンドとしてストレージ バケットを選択し、バックエンドで Cloud CDN を有効にして、ストレージ バケット内の各オブジェクトがパブリックに共有されていることを確認します。
Answer: D (メーッセージを残す**)**
https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers#using_cloud_cdn_with_cloud_storage_buckets Cloud CDN には HTTP(S) ロードバランサが必要で、Cloud Storage バケットは公開で共有する必要があります。https://cloud.google.com/cdn/docs/setting-up-cdn-with-bucket

最新問題: **103**
gsutil ツールと Google への 10 Gbps ダイレクト ピアリング接続を使用して、オンプレミス サーバーから Cloud Storage バケットにファイルをアップロードしています。オンプレミス サーバーは、Google ピアリング ポイントから 100 ミリ秒離れています。アップロードでは、利用可能な 10 Gbps 帯域幅をすべて使用していないことがわかります。接続の帯域幅使用率を最適化したいと考えています。
オンプレミスのサーバーでは何をすべきでしょうか?
A. gsutil コマンドから -m フラグを削除して、シングルスレッド転送を有効にします。
B. gsutil コマンドで perfdiag パラメータを使用して、パフォーマンスを高速化します: gsutil perfdiag gs://[バケット名]。
C. オンプレミス サーバーの TCP パラメーターを調整します。
D. tar などのユーティリティを使用してファイルを圧縮し、送信されるデータのサイズを削減します。
Answer: B (メーッセージを残す**)**

最新問題: **104**
あなたの会社はパートナーと協力して顧客にソリューションを提供しています。あなたの会社とパートナー組織は両方とも GCP を使用しています。
パートナーのネットワークには、会社の VPC 内の一部のリソースにアクセスする必要があるアプリケーションがあります。VPC 間に CIDR の重複はありません。
セキュリティを損なうことなく望ましい結果を達成するには、どの 2 つのソリューションを実装できますか? (2つお選びください。)
A. VPC ピアリング
B. 共有 VPC
C. クラウドVPN
D. 専用インターコネクト
E. クラウド NAT
Answer: A,C (メーッセージを残す**)**
Google Cloud VPC ネットワーク ピアリングを使用すると、同じプロジェクトまたは同じ組織に属しているかどうかに関係なく、2 つの Virtual Private Cloud (VPC) ネットワーク間で内部 IP アドレス接続が可能になります。

最新問題: **105**

あなたの会社は最近、オンプレミス データセンターと Google Cloud Virtual Private Cloud (VPC) の間に Cloud VPN トンネルを設置しました。オンプレミス サーバーの Cloud Functions API へのアクセスを構成する必要があります。構成は次の要件を満たす必要があります。
特定のデータは、それが保存されているプロジェクト内に保持し、他のプロジェクトに持ち出さないようにする必要があります。
RFC 1918 アドレスを持つデータセンター内のサーバーからのトラフィックは、インターネットを使用して Google Cloud API にアクセスしません。
すべての DNS 解決はオンプレミスで実行する必要があります。
このソリューションは、VPC Service Controls と互換性のある API へのアクセスのみを提供する必要があります。
あなたは何をするべきか？
A. 199.36.153.4/30 のアドレス範囲を使用して、restricted.googleapis.com の A レコードを作成します。
A レコードを指す *.googleapis.com の CNAME レコードを作成します。
A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。
Cloud VPN トンネルが終了する VPC からデフォルトのインターネット ゲートウェイを削除します。
B. 199.36.153.8/30 のアドレス範囲を使用して、private.googleapis.com の A レコードを作成します。
A レコードを指す *.googleapis.com の CNAME レコードを作成します。
A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。
Cloud VPN トンネルが終了する VPC からデフォルトのインターネット ゲートウェイを削除します。
C. 199.36.153.8/30 のアドレス範囲を使用して、private.googleapis.com の A レコードを作成します。
A レコードを指す *.googleapis.com の CNAME レコードを作成します。
A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。
private.googleapis.com アドレスへのトラフィックを許可するようにオンプレミスのファイアウォールを構成します。
D. 199.36.153.4/30 のアドレス範囲を使用して、restricted.googleapis.com の A レコードを作成します。
A レコードを指す *.googleapis.com の CNAME レコードを作成します。
A レコードで使用したアドレスのネクストホップとして Cloud VPN トンネルを使用するようにオンプレミス ルーターを構成します。
オンプレミスのファイアウォールを構成して、restricted.googleapis.com アドレスへのトラフィックを許可します。
Answer: (解答を表示する**)**

最新問題: **106**
Google Cloud 組織には、Dev と Prod という 2 つのフォルダがあります。最小限のコストですべての仮想マシン (VM) に次のファイアウォール ルールを適用する、スケーラブルで一貫した方法が必要です。
ポート 8080 は、Dev フォルダー内のプロジェクト内の VM に対して常に開いている必要があります。
ポート 8080 へのトラフィックは、Prod フォルダー内のプロジェクト内のすべての VM に対して拒否される必要があります。
あなたは何をするべきか？
A. Anthos Config Connector を使用して、開発 VM でポート 8080 を開き、本番 VM でポート 8080 へのトラフィックを拒否するセキュリティ ポリシーを適用します。
B. 開発プロジェクト用の共有 VPC と本番プロジェクト用の共有 VPC を作成します。開発用の共有 VPC でポート 8080 を開くための VPC ファイアウォール ルールを作成します。Prod 用の共有 VPC でポート 8080 へのトラフィックを拒否するファイアウォール ルールを作成します。これらの共有 VPC に VM をデプロイします。
C. 開発プロジェクトのすべての VPC で、ポート 8080 を開く VPC ファイアウォール ルールを作成します。本番プロジェクトのすべての VPC で、ポート 8080 へのトラフィックを拒否する VPC ファイアウォール ルールを作成します。

D. ファイアウォール ポリシーを作成し、ポート 8080 を開くルールを使用して Dev フォルダーに関連付けます。ファイアウォール ポリシーを作成し、ポート 8080 へのトラフィックを拒否するルールを使用して Prod フォルダーに関連付けます。
Answer: D (メーッセージを残す)

最新問題: **107**
GCP Console で D dedicated Interconnect を注文しました。物理接続を完了するには、認可状/接続機能割り当て (LOA-CFA) をクロスコネクト プロバイダーに渡す必要があります。
これを達成できる 2 つのアクションはどれですか? (2つお選びください。)
A. Cloud Interconnect カテゴリの下の Cloud Support チケットを開きます。
B. GCP Console の [ハイブリッド接続] セクションから LOA-CFA をダウンロードします。
C. gcloud compute interconnects description <interconnect> を実行します。
D. 注文プロセス中に指定した NOC 連絡先のアカウントの電子メールを確認します。
E. 相互接続プロバイダーに連絡し、Google が LOA/CFA を電子メールで自動的に送信したことを伝え、接続を完了します。
Answer: (解答を表示する)
https://cloud.google.com/network-connectivity/docs/interconnect/how-to/d dedicated/retrieving-loas

最新問題: **108**
あなたは、GCP への移行を進めている多国籍企業に勤めています。
クラウドの要件は次のとおりです。
- 米国のオレゴン州とニューヨークにあるオンプレミス データ センター。専用インターコネクトがクラウド リージョン us-west1 (プライマリ本社) と us-east4 (バックアップ) に接続されています。
- ヨーロッパとアジア太平洋地域に複数の支社を設置
- ヨーロッパ西部 1 とオーストラリアでは地域データ処理が必要です -
南東1
- 集中ネットワーク管理チーム
セキュリティおよびコンプライアンス チームは、URL フィルタリングの L7 インスペクションを実行するために仮想インライン セキュリティ アプライアンスを必要としています。アプライアンスを us-west1 にデプロイしたいと考えています。
あなたは何をするべきか？
A. 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。
ホスト プロジェクトのゾーン us-west1-a に 2 NIC インスタンスを構成します。
ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。
ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。
インスタンスをデプロイします。

インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
B. 共有 VPC サービス プロジェクトに 1 つの VPC を作成します。
サービス プロジェクトのゾーン us-west1-a に 2 NIC インスタンスを構成します。
サービス プロジェクトの us-west1 サブネットに NIC0 を接続します。
サービス プロジェクトの us-west1 サブネットに NIC1 を接続します。インスタンスをデプロイします。
インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
C. 共有 VPC ホスト プロジェクトに 1 つの VPC を作成します。
ホスト プロジェクトのゾーン us-west1-a に 2 NIC インスタンスを構成します。
ホスト プロジェクトの us-west1 サブネットに NIC0 を接続します。
ホスト プロジェクトの us-west1 サブネットに NIC1 を接続します。
インスタンスをデプロイします。
インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
D. 共有 VPC ホスト プロジェクトに 2 つの VPC を作成します。
サービス プロジェクトのゾーン us-west1-a に 2 NIC インスタンスを構成します。
ホスト プロジェクトの VPC #1 us-west1 サブネットに NIC0 を接続します。
ホスト プロジェクトの VPC #2 us-west1 サブネットに NIC1 を接続します。
インスタンスをデプロイします。
インスタンスを介してトラフィックを通過させるために必要なルートとファイアウォール ルールを構成します。
Answer: A (メーッセージを残す**)**

最新問題**: 109**
特定の IP アドレスのみが接続できるように、Google Cloud 負荷分散アプリケーションへのアクセスを制限する必要があります。
あなたは何をするべきか？
A. VPC Service Controls の Access Context Manager 機能を使用して安全な境界を作成し、許可されたクライアントのソース IP 範囲と Google ヘルスチェックの IP 範囲へのアクセスを制限します。
B. VPC Service Controls を使用して安全な境界を作成し、許可されたクライアントのソース IP 範囲と Google ヘルスチェックの IP 範囲に制限されたサービスとしてロード バランサーをマークします。
C. バックエンド インスタンスに 『アプリケーション」というタグを付け、ターゲット タグ 『アプリケーション」、許可されたクライアントのソース IP 範囲、および Google ヘルス チェックの IP 範囲を使用してファイアウォール ルールを作成します。
D. バックエンド インスタンスに 『アプリケーション」というラベルを付け、ターゲット ラベル 『アプリケーション」、許可されたクライアントのソース IP 範囲と Google ヘルス チェックの IP 範囲を使用してファイアウォール ルールを作成します。
Answer: (解答を表示する**)**
https://link.springer.com/chapter/10.1007/978-1-4842-1004-8_4

最新問題**: 110**
あなたの会社は、写真を Google クラウド ストレージ バケットにアップロードするモバイル アプリケーションを起動しました。アプリケーションは写真を Google クラウド ストレージ バケットに正常にアップロードしていましたが、最近このアプリケーションが人気になり、429 エラーが発生するようになりました。問題に対処する方法を提案してください。どれか 2 つお選びください。
A. クライアントのリクエストを抑制します

B. 切り捨てられた指数バックオフを使用します。
C. OAuth アクセス トークンの有効期限が切れているため、更新する必要があります。
D. /upload または /download URL では正しい動詞を使用します。
Answer: B (メーッセージを残す)
429 エラーはリクエストが多すぎるために発生するため、オプション A とオプション B が正しい選択です。アプリケーションが制限を超えて使用しようとすると、追加のリクエストは失敗します。クライアントのリクエストを抑制するか、切り捨てられた指数バックオフを使用します。
オプション C は間違った選択です。OAuth アクセス トークンの有効期限が切れるとエラーが発生します。
401(不正)
選択肢 D は不正解です。/upload または /download URL で間違った動詞を使用すると、
405 (メソッドが許可されていないエラー)。

最新問題: **111**
あなたの会社では、オンプレミスのデータセンターで重要なアプリケーションを実行するためのネットワーク容量が不足しています。
アプリケーションを GCP に移行したいと考えています。また、セキュリティ チームが Compute Engine インスタンスとの間のトラフィックを監視する能力を失わないようにする必要もあります。
ソリューションに組み込むべき 2 つの製品はどれですか? (2つお選びください。)
A. VPC フローログ
B. ファイアウォールのログ
C. クラウド監査ログ
D. Stackdriver トレース
E. Compute Engine インスタンスのシステム ログ
Answer: C,D (メーッセージを残す)
説明/参照: https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations