amxexam 3 years, 3 months ago

Let's go with option elimination
A. Create a VPC and connect it to your on-premises data centre using Dedicated Interconnect.
>> Is the only remaining best option after elimination. As per the document, its partner interconnects with VPN. Interconnect is between GCP on-prem. URL1

B. Create a VPC and connect it to your on-premises data centre using a single Cloud VPN.
>> max 3 gigabits per second (Gbps) eliminate the option.

C. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises data centre using Dedicated Interconnect.
>> CDN is for egress traffic or static content hosting hence eliminate the option URL2

D. Create a Cloud Content Delivery Network (Cloud CDN) and connect it to your on-premises datacenter using a single Cloud VPN.
>> CDN is for egress traffic or static content hosting hence eliminate the option URL2

Hence A

URL1 https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview
URL2 https://cloud.google.com/network-connectivity/docs/cdn-interconnect

upvoted 3 times

MamthaSJ 3 years, 5 months ago

Answer is A

upvoted 1 times

aviratna 3 years, 5 months ago

A is correct. Dedicated Interconnect supports upto 80 GBPS

upvoted 1 times

victory108 3 years, 7 months ago

A. Create a VPC and connect it to your on-premises data center using Dedicated Interconnect.

upvoted 2 times

Question #44 *Topic 1*

You are analyzing and defining business processes to support your startup's trial usage of GCP, and you don't yet know what consumer demand for your product will be. Your manager requires you to minimize GCP service costs and adhere to Google best practices. What should you do?

A. Utilize free tier and sustained use discounts. Provision a staff position for service cost management.

B. Utilize free tier and sustained use discounts. Provide training to the team about service cost management.

C. Utilize free tier and committed use discounts. Provision a staff position for service cost management.

D. Utilize free tier and committed use discounts. Provide training to the team about service cost management.

ehgm Highly Voted 2 years, 11 months ago

Sustained are automatic discounts for running specific GCE a significant portion of the billing month:
https://cloud.google.com/compute/docs/sustained-use-discounts

Committed is for workloads with predictable resource needs between 1 year or 3 year, discount is up to 57% for most resources:
https://cloud.google.com/compute/docs/instances/signing-up-committed-use-discounts

upvoted 43 times

ashishdwi007 11 months ago

Adding to it.
Provide training to the team about service cost management: Because we are still using free tier, and no need a separate position even if tl need arises. Its startup Company any way, and they are trained to work beyond hours :-)

upvoted 2 times

squishy_fishy 2 years, 10 months ago

Best answer!

upvoted 5 times

crypt0 Highly Voted 5 years, 1 month ago

I would choose "B"

upvoted 40 times

tartar 4 years, 4 months ago

B is ok

upvoted 11 times

nitinz 3 years, 9 months ago

B reason minimize GCP service costs

upvoted 3 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: B

1. Free Tier: Google Cloud's Free Tier allows you to use certain services for free, up to specified limits. This is ideal for a startup testing the platform and controlling costs during the trial phase.

2. Sustained Use Discounts: These discounts are automatically applied to your bill when you use eligible services for a significant portion of tl billing month. This is beneficial for a startup that might have unpredictable usage patterns during the trial phase, as it doesn't require any upfr commitment.

3. Training for cost management: Educating your team about cost management best practices empowers them to make cost-effective decisic from the start. This includes understanding pricing models, monitoring resource usage, and optimizing configurations.

upvoted 1 times

omermahgoub 1 year, 12 months ago

The recommended approach for minimizing GCP service costs and adhering to Google best practices are:
- Free tier: Google Cloud offers a free tier of services that allows you to try out many of its products for free, up to certain usage limits. Utilizin the free tier can help you minimize your GCP service costs while you are in the trial usage phase.

- Committed use discounts: Committed use discounts are a type of discount that you can apply to certain GCP products by committing to a certain level of usage over a one- or three-year period. Committed use discounts can help you save on your GCP service costs, but they requ you to commit to a certain level of usage, which may not be suitable if you are unsure of your future demand.

- Providing training to the team about service cost management: It is important that your team is aware of the different options available for minimizing GCP service costs and understands how to manage and monitor their usage of GCP services. Providing training on service cost management can help your team make informed decisions about how to use GCP services in the most cost-effective way.

upvoted 8 times

omermahgoub 1 year, 12 months ago

The recommended approach for minimizing GCP service costs and adhering to Google best practices while your startup is in the trial usag phase and you don't yet know what consumer demand for your product will be is option D: Utilize free tier and committed use discounts. Provide training to the team about service cost management.

upvoted 1 times

omermahgoub 1 year, 12 months ago

Sustained use discounts are based on your usage of GCP services over a certain period, and are not available for all GCP products.

Provisioning a staff position for service cost management may not be necessary if you provide training to the team about service cost management.

upvoted 1 times

SureshbabuK 2 years ago

Selected Answer: B

Sustained use discounts - Compute Engine - Google Cloudhttps://cloud.google.com › ... › Documentation
Compute Engine offers sustained use discounts on resources that are used for more than 25% of a billing month - There trial could be more t
7 or 8 days , at this point commitment of use can not be provided due to trails stage of gcp use

upvoted 1 times

vranjan 2 years, 1 month ago

The answer is B, because Sustained use discount can give up to 30% and requires no commitment.

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: B

ok for B

upvoted 1 times

zr79 2 years, 2 months ago

committed use discounts are for long-run discounts which in the case of startup they're trying GCP. So options C and D are out
B is the correct answer

upvoted 1 times

AzureDP900 2 years, 2 months ago

I will choose B, D is only long term commitment

upvoted 1 times

minmin2020 2 years, 2 months ago

Selected Answer: B

B. Utilize free tier and sustained use discounts. Provide training to the team about service cost management.

upvoted 2 times

BiddlyBdoyng 2 years, 2 months ago

Sustained use discount makes sense over committed as not enough info to know what to comit to. Provide staff training on how to keep thin
cheap gonna further keep cost down.

upvoted 1 times

cmamiusa 2 years, 8 months ago

Selected Answer: B

B is the correct option

upvoted 1 times

gcmrjbr 2 years, 10 months ago

free tier (monthly discounts) does not make sense combined with committed use discounts - anual base, dont't you think so?

upvoted 2 times

vincy2202 2 years, 11 months ago

B is the correct answer

upvoted 1 times

Israel 3 years, 3 months ago

Answer is B

upvoted 1 times

VishalB 3 years, 4 months ago

Answer B
Sustained use discounts are applied on incremental use after you reach certain usage thresholds. This means that you pay only for the numbe
minutes that you use an instance, and Compute Engine automatically gives you the best price. There's no reason to run an instance for longe
than you need it.
- https://cloud.google.com/compute/docs/sustained-use-discounts
Committed use discounts are ideal for workloads with predictable resource needs. When you purchase a committed use contract, you purcha
compute resource (vCPUs, memory, GPUs, and local SSDs) at a discounted price in return for committing to paying for those resources for 1
year or 3 years. The discount is up to 57% for most resources like machine types or GPUs. The discount is up to 70% for memory-optimized
machine types. For committed use prices for different machine types, see VM instances pricing.
- https://cloud.google.com/compute/docs/instances/signing-up-committed-use-discounts

upvoted 5 times

MamthaSJ 3 years, 5 months ago

Answer is B

upvoted 1 times

Question #45 *Topic 1*

You are building a continuous deployment pipeline for a project stored in a Git source repository and want to ensure that code changes can be verified before deploying to production. What should you do?

A. Use Spinnaker to deploy builds to production using the red/black deployment strategy so that changes can easily be rolled back.

B. Use Spinnaker to deploy builds to production and run tests on production deployments.

C. Use Jenkins to build the staging branches and the master branch. Build and deploy changes to production for 10% of users before doing a complete rollout.

D. Use Jenkins to monitor tags in the repository. Deploy staging tags to a staging environment for testing. After testing, tag the repository for production and deploy that to the production environment.

Googler2 Highly Voted 4 years, 8 months ago

I believe the best answer is D, because the tagging is a best practice that is recommended on Jenkins/Spinnaker to deploy the right code anc prevent accidentally (or intentionally) push of wrong code to production environments. See https://stackify.com/continuous-delivery-git-jenkin

upvoted 59 times

Ziegler 4 years, 6 months ago

Agreed with D as the right answer. The url provided explains it better

upvoted 10 times

AzureDP900 2 years, 2 months ago

yes, D is correct

upvoted 1 times

zr79 2 years, 2 months ago

How can I join Google

upvoted 6 times

Anish17 Highly Voted 4 years, 3 months ago

I got this question in real exam. This question states "before deploying to production" environment. So i picked D . I passed the exam.

upvoted 53 times

bnlcnd 3 years, 10 months ago

that resolved the puzzle :)

upvoted 6 times

GunaGCP123 3 years, 1 month ago

congrats for passing the exam. practising all 255 questions is sufficient for passing the exam? how much percentage of questions you got from here roughly?

upvoted 2 times

zr79 2 years, 2 months ago

He won't answer, he already passed the exam

upvoted 10 times

Rzla 3 years, 3 months ago

Agree, its the only answer that meets the requirement of "before deploying to production"

upvoted 2 times

winset 3 years, 10 months ago

not only 1 Q passed! C is beeter

upvoted 2 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: D

1. Clear separation of environments: Using separate staging and production environments ensures that code changes are thoroughly tested before they reach your users. This minimizes the risk of introducing bugs or regressions into production.

2. Controlled deployments: Tagging the repository for different stages (staging, production) provides a clear and auditable way to track which code versions are deployed in each environment. This makes it easier to roll back to a previous version if necessary.

3. Jenkins for automation: Jenkins is a powerful automation server that can monitor your Git repository for new tags, automatically build and deploy the code to the appropriate environment, and even trigger automated tests.

4. Comprehensive testing: A staging environment allows you to perform comprehensive testing, including integration testing, user acceptance testing (UAT), and performance testing, before deploying to production.

upvoted 1 times

sim7243 1 month, 1 week ago

Selected Answer: D

D is the best choice.

upvoted 1 times

bkovari 10 months ago

ABC is about to deploy to production without prior testing. Hence D is the only reasonable choice.

upvoted 1 times

ashishdwi007 11 months ago

A B and C are very risky options and irrelevant as involving production. Whereas question is to test before rolling out to production. Hence D

upvoted 1 times

blackhawk86 1 year, 3 months ago

Selected Answer: D

No discussion here.

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: D

ok for D

upvoted 1 times

BiddlyBdoyng 2 years, 2 months ago

Given the question D is the only answer. Everything else pushes to production immediately.

upvoted 1 times

[Removed] 2 years, 8 months ago

I don't think it was a good idea when new edtion be created and directly deploy to the production ENV without any testing stage even using Canary deployment.

upvoted 1 times

> **[Removed]** 2 years, 8 months ago
>
> D is better.
>
> upvoted 1 times

Davidik79 2 years, 9 months ago

Selected Answer: D

The question states: "... code changes can be verified BEFORE deploying to production", it eliminates option C.
The approach of tagging is the correct practise that DevOps use

upvoted 2 times

[Removed] 2 years, 11 months ago

Selected Answer: D

Correct answer is D. Question talks about 'before deploying to production'. C talks about after deploying to production.

upvoted 4 times

hantanbl 2 years, 11 months ago

C is the closest answer
If question is asking 'what's Jenkin best practise' then D is the answer

upvoted 1 times

> **Davidik79** 2 years, 9 months ago
>
> C involves deploying into production. the question specifies: "BEFORE deploying to production"
>
> upvoted 2 times

> **blackhawk86** 1 year, 3 months ago
>
> Incorrect. D is the correct answer. 1. It should test BEFORE deploy to production. 2. It's a DevOps practice
>
> upvoted 1 times

lxgywil 2 years, 11 months ago

I choose D as we want to ensure that code changes can be verified BEFORE deploying to production. Option C suggests that we build and deploy changes to production for 10% of users.

upvoted 1 times

OrangeTiger 2 years, 11 months ago

Selected Answer: D

Vote D.
C is canary deploy.
But the sentence in question has no word to mean "tested by a small number of users"

upvoted 3 times

OrangeTiger 2 years, 11 months ago

The revelal solution on this site is wrong, isn't it? I'm getting anxious.

upvoted 1 times

vincy2202 2 years, 11 months ago

D is the correct answer

upvoted 1 times

ABO_Doma 3 years ago

Selected Answer: D

clearly

upvoted 2 times

Question #46 *Topic 1*

You have an outage in your Compute Engine managed instance group: all instances keep restarting after 5 seconds. You have a health check configured, but autoscaling is disabled. Your colleague, who is a Linux expert, offered to look into the issue. You need to make sure that he can access the VMs. What should you do?

A. Grant your colleague the IAM role of project Viewer

B. Perform a rolling restart on the instance group

C. Disable the health check for the instance group. Add his SSH key to the project-wide SSH Keys

D. Disable autoscaling for the instance group. Add his SSH key to the project-wide SSH Keys

Narinder Highly Voted 2 years, 11 months ago

C, is the correct answer. As per the requirement linux expert would need access to VM to troubleshoot the issue. With health check enabled,
VM will be terminated as soon as health-check fails for the VM and new VM will be auto-created. So, this situation will prevent linux expert to
troubleshoot the issue. Had it been the case that stack-drover logging is enabled and the expert just want to view the logs from the Cloud-log
than role to project-viewer could help. But it is specifically mentioned that expert will login into VM to troubleshoot the issue and not looking a
the cloud Logs. So, Option-C is the correct answer.

upvoted 93 times

twistyfries 2 years, 9 months ago

great answer

upvoted 2 times

AmitAr 2 years, 7 months ago

This looks best justification between A and C.. So, C should be correct answer.

upvoted 2 times

devjuliusoh 2 years, 4 months ago

Good explanation

upvoted 2 times

ashishdwi007 11 months ago

The key element in C is "Disable the Health check.", so that server wont restart automatically.
But before that the actual troubleshooting step is to check Cloud console -> Instance template -> Metadata-> and see if any startup script there, if yes review it and possibly remove it. [Consider the case, a script is causing restarting the VM, (possibly in Metadata).]

upvoted 1 times

KouShikyou Highly Voted 5 years, 1 month ago

C should be correct answer.

upvoted 39 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: C

1. Access for troubleshooting: Disabling the health check prevents the VMs from constantly restarting, allowing the expert to log in and investigate the root cause.

2. SSH access: Adding the expert's SSH key grants them the necessary access to the VMs.

3. Temporary measure: This is a temporary measure for troubleshooting. Once the issue is resolved, the health check should be re-enabled.

upvoted 1 times

wilson1005 9 months ago

Selected Answer: C

C is correct!

upvoted 1 times

heretolearnazure 1 year, 3 months ago

I like C

upvoted 1 times

JC0926 1 year, 9 months ago

Selected Answer: C

To allow your colleague, who is a Linux expert, to access the VMs and troubleshoot the issue, you should disable the health check for the instance group. This will prevent the instance group from automatically removing and replacing unhealthy instances.

You should also add your colleague's SSH key to the project-wide SSH Keys to allow him to SSH into the instances and perform troubleshoo
This can be done through the Google Cloud Console or the gcloud command-line tool.

upvoted 3 times

MestreCholas 1 year, 9 months ago

Selected Answer: C

C. Disable the health check for the instance group. Add his SSH key to the project-wide SSH Keys.

Granting the IAM role of project Viewer (Option A) would allow your colleague to view the project resources but not necessarily give them acc
to the specific VM instances. Performing a rolling restart on the instance group (Option B) would not resolve the issue, as the instances keep restarting after 5 seconds. Disabling autoscaling for the instance group (Option D) is not relevant since autoscaling is already disabled.

Disabling the health check for the instance group will prevent the managed instance group from automatically recreating the instances. Addin
your colleague's SSH key to the project-wide SSH Keys will allow them to access the VMs and troubleshoot the issue. Once the issue is resolved, you can re-enable the health check for the instance group.

upvoted 5 times

urssiva 1 year, 10 months ago

Selected Answer: C

C is the answer

upvoted 1 times

roaming_panda 1 year, 11 months ago

C as the machines will keep restarting if hc is not disabled , and then our expert can look around for RCA

upvoted 1 times

omermahgoub 1 year, 12 months ago

To allow your colleague access the instances in MIG you should do option D: Disable autoscaling for the instance group. Add his SSH key to project-wide SSH Keys.

Disabling autoscaling for the instance group will prevent new instances from being created or terminated while your colleague is trying to troubleshoot the issue. This will give him a stable environment to work in and will ensure that he can access the instances that are currently in instance group.

Adding his SSH key to the project-wide SSH Keys will allow him to connect to the instances using Secure Shell (SSH) without requiring a password. This is a convenient way to give him access to the instances and can help him troubleshoot the issue more efficiently.

upvoted 2 times

n_nana 1 year, 11 months ago

autoscaling is already disabled. Answer D is not make sense here. i voted it wrongly instead of reply.

upvoted 1 times

omermahgoub 1 year, 12 months ago

Option A: Granting your colleague the IAM role of project Viewer will not allow him to access the instances in the managed instance group. The project Viewer role does not include any permissions to access Compute Engine resources.

Option B: Performing a rolling restart on the instance group will not solve the issue and may even make it worse if the instances are not ab to start up properly.

Option C: Disabling the health check for the instance group will not solve the issue and may even make it worse if the instances are not ab to start up properly. Adding his SSH key to the project-wide SSH Keys will allow him to access the instances, but it is not a sufficient solut on its own.

upvoted 2 times

surajkrishnamurthy 2 years ago

Selected Answer: C

C is the correct answer

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: C

ok for C

upvoted 1 times

minmin2020 2 years, 2 months ago

C. Disable the health check for the instance group. Add his SSH key to the project-wide SSH Keys. This will allow the engineer to logon to the VM's and check the logs. Disabling health checks will prevent rebooting of the VM's.

upvoted 2 times

holerina 2 years, 2 months ago

C should be the correct answer

upvoted 1 times

abirroy 2 years, 3 months ago

Selected Answer: C

Disable the health check for the instance group. Add his SSH key to the project-wide SSH Keys

upvoted 1 times

backhand 2 years, 4 months ago

vote C
what can project viewer do without access vm by linux expert?

upvoted 1 times

tricky_learner 2 years, 5 months ago

Selected Answer: C

I believe that answer C is correct.

upvoted 1 times

Question #47 *Topic 1*

Your company is migrating its on-premises data center into the cloud. As part of the migration, you want to integrate Google Kubernetes Engine (GKE) for workload orchestration. Parts of your architecture must also be PCI DSS-compliant. Which of the following is most accurate?

A. App Engine is the only compute platform on GCP that is certified for PCI DSS hosting.

B. GKE cannot be used under PCI DSS because it is considered shared hosting.

C. GKE and GCP provide the tools you need to build a PCI DSS-compliant environment.

D. All Google Cloud services are usable because Google Cloud Platform is certified PCI-compliant.

rishab86 Highly Voted 3 years, 6 months ago

Link : https://cloud.google.com/security/compliance/pci-dss
Clearly mention GKE as PCI DSS-Compliant but not all GCP service are PCI DSS-Compliant so answer is definitely C.

upvoted 46 times

Mikado211 2 years, 4 months ago

In 2022, GCP is now fully PCI-DSS compliant, so technically D is perfectly true.
But you still have to check that your application is PCI-DSS compliant.

so C is still the best answer.

upvoted 7 times

MaxNRG 3 years, 1 month ago

C – Kubernetes Engine provides tools you need to build to PCI-DSS compliant environment.

upvoted 1 times

haroldbenites 3 years ago

But, The paragraph 3 says that all products of google are certified by PCI.

upvoted 2 times

aviratna Highly Voted 3 years, 5 months ago

C: GKE & Compute Engine is PCI DSS compliant while Cloud Function, App Engine are not PC compliant

upvoted 5 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: C

1. GKE and PCI DSS: While GKE itself isn't inherently PCI DSS compliant, it provides the infrastructure and tools you need to build a complia
environment. You'll need to configure it correctly, implement security measures, and follow best practices.

2. Shared Responsibility Model: Google Cloud Platform operates under a shared responsibility model. Google is responsible for securing the underlying infrastructure, while you are responsible for securing your applications and data within that environment.

3. Flexibility for Compliance: GKE offers features like private clusters, network policies, and integration with security tools that help you meet
DSS requirements.

upvoted 1 times

eka_nostra 1 year, 4 months ago

Selected Answer: C

We still have to configure our env to comply with PCI/DSS. https://cloud.google.com/architecture/pci-dss-compliance-in-gcp#kubernetes_en

upvoted 1 times

omermahgoub 1 year, 12 months ago

The most accurate statement is option C: GKE and GCP provide the tools you need to build a PCI DSS-compliant environment.

Google Kubernetes Engine (GKE) is a fully managed service that allows you to deploy and manage containerized applications on Google Clou is not specifically certified for PCI DSS hosting, but it can be used as part of a PCI DSS-compliant environment if the necessary controls and safeguards are in place.

Google Cloud Platform (GCP) provides a range of tools and services that can be used to build a PCI DSS-compliant environment, including Cloud Identity and Access Management (IAM) for controlling access to resources, Cloud Key Management Service (KMS) for managing encryption keys, and Cloud Security Command Center for monitoring and detecting security threats.

upvoted 3 times

omermahgoub 1 year, 12 months ago

Option A: App Engine is a fully managed platform for building and deploying web and mobile applications, but it is not the only compute platform on GCP that is certified for PCI DSS hosting. Other compute platforms such as Compute Engine and Google Kubernetes Engine also be used as part of a PCI DSS-compliant environment.

Option B: GKE is not considered shared hosting and can be used as part of a PCI DSS-compliant environment if the necessary controls ar safeguards are in place.

Option D: While Google Cloud Platform is certified PCI-compliant, not all of its services are automatically usable in a PCI DSS-compliant environment. It is up to the user to ensure that they are using the appropriate controls and safeguards to meet the requirements of the PCI DSS.

upvoted 2 times

abirroy 2 years, 3 months ago

Selected Answer: C

C is the right answer

upvoted 1 times

[Removed] 2 years, 10 months ago

Selected Answer: C

I got similar question on my exam.

upvoted 3 times

vincy2202 2 years, 11 months ago

Selected Answer: C

C is the correct answer

upvoted 1 times

haroldbenites 3 years ago

Go for C.

upvoted 1 times

SHOURYA_SOOD 3 years ago

Selected Answer: C

C- All of them: GKE, GCE, and GAE ate PCI-DSS-Compliant but A & B says it's only GAE and GCE respectively so cancel them out.
D says all of GCP is PCI DSS-Compliant but it's not true.
So, C seems to be the right answer.

upvoted 1 times

imranmani 3 years, 2 months ago

C is the right answer

upvoted 1 times

MamthaSJ 3 years, 5 months ago

Answer is C

upvoted 3 times

victory108 3 years, 5 months ago

C. GKE and GCP provide the tools you need to build a PCI DSS-compliant environment.

upvoted 1 times

Question #48 *Topic 1*

Your company has multiple on-premises systems that serve as sources for reporting. The data has not been maintained well and has become degraded over time.

You want to use Google-recommended practices to detect anomalies in your company data. What should you do?

A. Upload your files into Cloud Storage. Use Cloud Datalab to explore and clean your data.

B. Upload your files into Cloud Storage. Use Cloud Dataprep to explore and clean your data.

C. Connect Cloud Datalab to your on-premises systems. Use Cloud Datalab to explore and clean your data.

D. Connect Cloud Dataprep to your on-premises systems. Use Cloud Dataprep to explore and clean your data.

JohnWick2020 Highly Voted 👍 3 years, 8 months ago

Answer is B:

Keynotes from question:
1- On-premise data sources
2- Unfit data; not well maintained and degraded
3- Google-recommended best practice to "detect anomalies" <<-Very important.

Explanation:
A & C - incorrect; Datalab does not provide anomaly detection OOTB. It is used more for data science scenarios like interactive data analysis build ML models.
B - CORRECT; DataPrep OOTB provides for fast exploration and anomaly detection and lists cloud storage as an ingestion medium. Refer to pipeline architecture here = https://cloud.google.com/dataprep
D - incorrect; At this time DataPrep cannot connect to SaaS or on-premise source. Not to be confused for DataFlow which can!

upvoted 59 times

Eroc Highly Voted 5 years, 1 month ago

Both B and D work, because the question says "Google's Best Practices" uploading the files first would keep the original copies Google encrypted and stored.

upvoted 12 times

skywalker 4 years, 7 months ago

Both of them works....

upvoted 1 times

Musk 4 years, 4 months ago

You can't connect DataPrep to your on-prem systems. You simply upload a file, but that is not connecting it to your systems. Because that, I'd discard D and stay with B.

upvoted 9 times

tartar 4 years, 4 months ago

B is ok

upvoted 9 times

nitinz 3 years, 9 months ago

B, dataprep = visually explore, clean, and prepare data for analysis

upvoted 7 times

AzureDP900 2 years, 2 months ago

B is better choice

upvoted 1 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: B

Why Cloud Storage is important ?
1. Centralized repository: Cloud Storage provides a secure and scalable place to store your data. This makes it accessible to various GCP services.
2. Data lake concept: This aligns with the idea of a data lake, where you bring raw data into a central location before processing and refining i

Why Cloud Dataprep is a good fit ?
1. Visual data exploration: Dataprep excels at helping you quickly understand your data through visualizations and profiling. This is crucial for identifying anomalies.
2. Data cleaning and transformation: Dataprep makes it easy to clean and standardize your data, which is essential before anomaly detection. Inconsistent formats, missing values, and errors can skew your analysis.
3. Built-in anomaly detection: Dataprep has features specifically designed to help you find anomalies. It can highlight unusual values, outliers, patterns.

upvoted 1 times

snehaso 4 months, 1 week ago

Datalab was shutdown. Its replacement is vertex AI. Read question accordingly

upvoted 1 times

thewalker 1 year, 1 month ago

Cloud Datalab is a powerful interactive tool created to explore, analyze, transform, and visualize data and build machine learning models on Google Cloud Platform.
Dataprep by Trifacta is an intelligent data service for visually exploring, cleaning, and preparing structured and unstructured data for analysis, reporting, and machine learning.
Dataprep do not have an integration for on-prem: https://console.cloud.google.com/marketplace/product/endpoints/cloud-dataprep-editions-project=fast-art-401415

So, clearly, the only option left is B.

upvoted 3 times

heretolearnazure 1 year, 3 months ago

B is correct.

upvoted 1 times

n_nana 1 year, 9 months ago

Today, data ingestion to DataPrep can be Application, file upload, database.
so B is also now valid

upvoted 1 times

omermahgoub 1 year, 12 months ago

The recommended approach for detecting anomalies in your company data using Google-recommended practices is option B: Upload your fi into Cloud Storage. Use Cloud Dataprep to explore and clean your data.

Cloud Storage is a highly scalable, durable, and secure object storage service that can be used to store and retrieve data from anywhere on tl web. You can use Cloud Storage to store your company data files and make them available for analysis.

Cloud Dataprep is a fully managed data preparation service that allows you to quickly and easily explore, clean, and transform your data for analysis. It can help you detect anomalies in your data by providing features such as data profiling, data cleansing, and data transformation.

upvoted 2 times

omermahgoub 1 year, 12 months ago

Option A: Using Cloud Datalab to explore and clean your data is not a recommended approach, as Cloud Datalab is a collaborative data exploration and visualization platform that is not specifically designed for data preparation tasks such as cleansing and transformation.

Option C: Connecting Cloud Datalab to your on-premises systems is not a recommended approach, as Cloud Datalab is a collaborative da exploration and visualization platform and is not designed for data preparation tasks such as cleansing and transformation.

Option D: Connecting Cloud Dataprep to your on-premises systems is not necessary, as you can use Cloud Dataprep to explore and clear data stored in Cloud Storage.

upvoted 1 times

allen_y_q_huang 2 years ago

ok for B & D, but B is suitable to gcp

upvoted 1 times

Smaks 2 years ago

Selected Answer: B

Datalab is deprecated : https://cloud.google.com/datalab/docs
New Cloud Dataprep options will give connectivity to relational databases, business applications and extend our integrations across Google Cloud with Google Sheets: https://www.trifacta.com/blog/cloud-dataprep-trifacta/

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: B

ok for B

upvoted 1 times

Cloudexplorer 2 years, 4 months ago

Could anyone provide a link where it explicitly says that Datprep does not connect to on-premises data sources.

In the ingestion layer on the diagram at https://cloud.google.com/dataprep it shows databases as a source.
I can't see anywhere that there is a limitation connecting to on-premises. Would be great if someone could share that.

upvoted 3 times

BigSteveO 2 years, 5 months ago

Selected Answer: B

It's gotta be B.

upvoted 1 times

Dhiraj03 2 years, 6 months ago

Keyword : Anamolies Data prep is the only product ... So options A and C is eliminated ... Cost effective is storing the data in GCS Cloud stor ... So option is B

upvoted 1 times

nkit 2 years, 8 months ago

Selected Answer: B

Dataprep to detect anomalies in Data is the right choice.

upvoted 1 times

GMats 2 years, 11 months ago

B...It supports only CloudStorage and Bigquery..."So you can start transforming datasets, you hereby instruct Google to allow Trifacta, who provides the service Dataprep in collaboration with Google, to view and modify project data in Cloud Storage and BigQuery, run Dataflow jobs and use all project service accounts."

upvoted 1 times

haroldbenites 3 years ago
Go for B.
upvoted 1 times

haroldbenites 3 years ago
The question says “best practice”. In GCP , a best practice for many use cases is load to cloud storage and then processing data.
upvoted 1 times

Question #49 *Topic 1*

Google Cloud Platform resources are managed hierarchically using organization, folders, and projects. When Cloud Identity and Access Management (IAM) policies exist at these different levels, what is the effective policy at a particular node of the hierarchy?

A. The effective policy is determined only by the policy set at the node

B. The effective policy is the policy set at the node and restricted by the policies of its ancestors

C. The effective policy is the union of the policy set at the node and policies inherited from its ancestors

D. The effective policy is the intersection of the policy set at the node and policies inherited from its ancestors

passnow Highly Voted 5 years ago
The effective policy for a resource is the union of the policy set at that resource and the policy inherited from its parent.https://cloud.google.com/iam/docs/resource-hierarchy-access-control
upvoted 31 times

ghadxx Highly Voted 2 years, 10 months ago
You can set IAM policies at the level of the node, in addition to policies inherited from its parent. Hence, it is a union.
upvoted 13 times

Ekramy_Elnaggar Most Recent 1 month ago
Selected Answer: C
Here's how IAM policies work in GCP's hierarchical structure:
1. Hierarchy: GCP resources are organized in a hierarchy:
- Organization: The root node representing your company.
- Folders: Used to organize projects within the organization.
- Projects: Containers for your resources (VMs, databases, etc.).
2. Inheritance: IAM policies are inherited down the hierarchy. This means a policy set at the Organization level applies to all folders and projec
within it.
3. Union of Policies: When you have policies at different levels, the effective policy at a particular node (e.g., a project) is the combination (unic
of:
- The policy set directly at that node.
- All the policies inherited from its parent folder and the organization.

Example: If a user has "Viewer" access at the Organization level and "Editor" access at the Project level, their effective permission on that pro
is "Editor" (the higher permission).
upvoted 1 times

Di4sa 1 year, 4 months ago

Selected Answer: C

From google doc: Google Cloud resources are organized hierarchically, where the organization node is the root node in the hierarchy, the proj are the children of the organization, and the other resources are descendants of projects. You can set allow policies at different levels of the resource hierarchy. Resources inherit the allow policies of the parent resource. The effective allow policy for a resource is the union of the allo policy set at that resource and the allow policy inherited from its parent.

upvoted 3 times

omermahgoub 1 year, 12 months ago

The effective policy at a particular node in the resource hierarchy in GCP is determined by the intersection of the policy set at the node and policies inherited from its ancestors, as described in option D

Cloud IAM policies in GCP are hierarchical, meaning that policies set at higher levels of the resource hierarchy can be inherited by lower level When a user or service account attempts to access a resource, the effective policy at that resource is determined by evaluating the policies s the resource itself and all of its ancestors in the hierarchy. If any of the policies deny access, the user or service account will be denied acces

For example, consider the following resource hierarchy:
Organization => Folder => Project => Compute Engine instance
If an IAM policy is set at the organization level that allows read access to all Compute Engine instances, and a policy is set at the project level that denies read access to a specific Compute Engine instance, the effective policy for that instance will be the intersection of the two policie which will be to deny read access to the instance.

upvoted 1 times

omermahgoub 1 year, 12 months ago

Option A: The effective policy is not determined only by the policy set at the node, as policies set at higher levels in the hierarchy can also have an impact on the effective policy.

Option B: The effective policy is not restricted by the policies of its ancestors, as the policies of its ancestors can also be included in the effective policy if they allow access.

Option C: The effective policy is not the union of the policy set at the node and policies inherited from its ancestors, as the intersection of t policies is used to determine the effective policy.

upvoted 1 times

habros 2 years ago

Selected Answer: C

C. Is a skewed wording question. Cannot be comprehended right away.

upvoted 2 times

megumin 2 years, 1 month ago

Selected Answer: C

ok for C

upvoted 1 times

Mahmoud_E 2 years, 1 month ago

Selected Answer: C

C is correct answer

upvoted 1 times

zr79 2 years, 2 months ago

English as a second language will struggle here. Good luck to us

upvoted 5 times

BiddlyBdoyng 2 years, 2 months ago

A: Would mean polcies set at the project or higher meant nothing, this is obviously wrong
B: would mean you could not grant a permissions to a single VM, it would need to be at project or above (you restrict by not giving the permission)
C : The permission is the sum of all the permissions you are given through the hierarchy, this is correct, you cannot restrict once it is given at higher level.
D: Would mean you would need the permission set at ancestor and the node, this would mean to get access to a single VM you would need t be given access to all VMs at the project level.

upvoted 3 times

⊟ **holerina** 2 years, 2 months ago

C is correct answer as it inheritance is the basic model of IAM

upvoted 2 times

⊟ **avinashvidyarthi** 2 years, 7 months ago

Selected Answer: C

C is correct

upvoted 1 times

⊟ **Atnafu** 2 years, 11 months ago

C

Google Cloud resources are organized hierarchically, where the organization node is the root node in the hierarchy, the projects are the childre the organization, and the other resources are descendants of projects. You can set Identity and Access Management (IAM) policies at differen levels of the resource hierarchy. Resources inherit the policies of the parent resource. The effective policy for a resource is the union of the po set at that resource and the policy inherited from its parent.

upvoted 3 times

⊟ **vincy2202** 2 years, 11 months ago

C is the correct answer

upvoted 2 times

⊟ **haroldbenites** 3 years ago

Go for C.

upvoted 1 times

⊟ **MamthaSJ** 3 years, 5 months ago

Answer is C

upvoted 3 times

⊟ **victory108** 3 years, 7 months ago

C. The effective policy is the union of the policy set at the node and policies inherited from its ancestors

upvoted 2 times

Question #50 *Topic 1*

You are migrating your on-premises solution to Google Cloud in several phases. You will use Cloud VPN to maintain a connection between your on-premises systems and Google Cloud until the migration is completed. You want to make sure all your on-premise systems remain reachable during this period. How should you organize your networking in Google Cloud?

A. Use the same IP range on Google Cloud as you use on-premises

B. Use the same IP range on Google Cloud as you use on-premises for your primary IP range and use a secondary range that does not overlap with the range you use on-premises

C. Use an IP range on Google Cloud that does not overlap with the range you use on-premises

D. Use an IP range on Google Cloud that does not overlap with the range you use on-premises for your primary IP range and use a secondary range with the same IP range as you use on-premises

⊟ **newbie2020** Highly Voted 👍 4 years, 10 months ago

Ans is C,
https://cloud.google.com/vpc/docs/using-vpc

"Primary and secondary ranges can't conflict with on-premises IP ranges if you have connected your VPC network to another network with C VPN, Dedicated Interconnect, or Partner Interconnect."

upvoted 131 times

Smart 4 years, 10 months ago

Agreed!

upvoted 2 times

AD2AD4 4 years, 6 months ago

Perfect.. Exact find in link.

upvoted 2 times

elaineshi 2 years, 6 months ago

agree, any ip range, shall use filewall rule to communicate, instead of setting same IP range, which is a mess to control.

upvoted 2 times

Sundeepk 4 years, 6 months ago

from the above link - it clearly states - "Primary and secondary ranges for subnets cannot overlap with any allocated range, any primary or secondary range of another subnet in the same network, or any IP ranges of subnets in peered networks." once we create a VPN, they all part of the same network . Hence option C is correct

upvoted 13 times

KouShikyou Highly Voted 5 years, 1 month ago

I think C is correct.

upvoted 21 times

JoeShmoe 5 years, 1 month ago

Agree with C. Secondary IP range still can't overlap

upvoted 10 times

AWS56 4 years, 11 months ago

".... and Google Cloud until the migration is completed." Taking this as the key, the intention is to remove the connection b/w on-prem GCP once the migration is done. and then the secondary IPs will act as primary. So I will choose D

upvoted 3 times

tartar 4 years, 4 months ago

C is ok

upvoted 10 times

MaxNRG 3 years, 1 month ago

B, The key points here:
- migrating in several phases
- use Cloud VPN until the migration is completed
- all your on-premise systems remain reachable during this period

upvoted 2 times

zanfo 3 years, 3 months ago

how to manage the routing table in VPC if is present a subnet with the same network of vpn remote net? the correct answer is C

upvoted 1 times

kumarp6 4 years, 1 month ago

Yes C it is

upvoted 2 times

nitinz 3 years, 9 months ago

C, no brainer. You have on-prem <--> VPN <---> GCP only way this data flow to work in non-over lapping subnets. You can stretch subnet layer 7 but you wont be able to route it via VPN.

upvoted 4 times

Ekramy_Elnaggar Most Recent 1 month ago

Selected Answer: C

1. IP Address Conflicts: When you have overlapping IP ranges between your on-premises network and your Google Cloud network, you'll run routing conflicts. Devices won't know where to send traffic, leading to connectivity problems and unreachable systems.

2. Cloud VPN and Routing: Cloud VPN creates a secure tunnel between your on-premises network and your Google Cloud Virtual Private Clou (VPC). To ensure proper routing, each side of the connection needs to have distinct, non-overlapping IP address spaces.

3. Best Practice for Hybrid Networks: Using different IP ranges is a standard best practice for hybrid cloud setups. It prevents ambiguity and ensures that traffic flows correctly between your on-premises and cloud environments.

upvoted 1 times

gracjanborowiak 5 months, 1 week ago

Selected Answer: B

question is tricky. as network architect knowing gcp i have exp that you can use non-overlapping secondary ranges for vpn as well.

in many migrations it is not possible to make new addressing hence you need to make them overlapping. this is why 2nd ranges are so useful

B is better choice. more realistic and possible in gcp.

from overall perspective i agree to have non-overlapping but do not forget this is migration and you need to have full connectivity all the time. also not mentioning about what ips should be used

upvoted 1 times

desertlotus1211 4 months, 2 weeks ago

When migrating to the cloud, best practices for IP schema generally involve avoiding duplicate IP addresses and keeping cloud and on-premise IP ranges separate

upvoted 1 times

heretolearnazure 1 year, 3 months ago

C is correct

upvoted 1 times

JC0926 1 year, 9 months ago

Selected Answer: B

Using an IP range on Google Cloud that does not overlap with the range used on-premises (option C) is a good choice to avoid IP address conflicts. However, it is important to use the same IP range as the on-premises applications for the primary IP range to ensure that the on-premises systems remain accessible. Therefore, using the same IP range on Google Cloud as on-premises for the primary IP range and using secondary range that does not overlap with the range used on-premises can avoid IP address duplication and ensure that the on-premises systems remain accessible. Hence, option B is the better choice.

upvoted 3 times

omermahgoub 1 year, 12 months ago

The recommended approach for organizing your networking in Google Cloud to ensure that all your on-premises systems remain reachable during the migration is option C: Use an IP range on Google Cloud that does not overlap with the range you use on-premises.

When using Cloud VPN to establish a connection between your on-premises systems and Google Cloud, it is important to ensure that the IP ranges used in your on-premises systems and Google Cloud do not overlap. If the IP ranges overlap, it can cause conflicts and make it difficu route traffic between your on-premises systems and Google Cloud.

To avoid IP range conflicts, you should use an IP range on Google Cloud that is different from the range you use on-premises. This will ensure that all your on-premises systems remain reachable during the migration.

upvoted 2 times

omermahgoub 1 year, 12 months ago

Option A: Using the same IP range on Google Cloud as you use on-premises is not a recommended approach, as it can cause IP range conflicts and make it difficult to route traffic between your on-premises systems and Google Cloud.

Option B: Using the same IP range on Google Cloud as you use on-premises for your primary IP range and a secondary range that does n overlap with the range you use on-premises is not a recommended approach, as it can still cause IP range conflicts and make it difficult to route traffic between your on-premises systems and Google Cloud.

Option D: Using an IP range on Google Cloud that does not overlap with the range you use on-premises for your primary

upvoted 1 times

megumin 2 years, 1 month ago

Selected Answer: C

ok for C

upvoted 1 times

zr79 2 years, 2 months ago

no overlapping

upvoted 1 times

AzureDP900 2 years, 2 months ago

C. Use an IP range on Google Cloud that does not overlap with the range you use on-premises

upvoted 1 times

marksie1988 2 years, 3 months ago

Selected Answer: C

C, IP should never overlap if avoidable. double nat is nasty

upvoted 1 times

ZLT 2 years, 5 months ago

Selected Answer: C

The correct answer is C

upvoted 2 times

Barry123456 2 years, 6 months ago

Selected Answer: C

C

Why would you ever create an IP overlap?

upvoted 1 times

jonty4gcp 2 years, 8 months ago

Selected Answer: C

Answer is C

upvoted 1 times

Davidik79 2 years, 9 months ago

Selected Answer: C

From here: https://cloud.google.com/vpc/docs/create-modify-vpc-networks
"Primary and secondary ranges can't conflict with on-premises IP ranges if you have connected your VPC network to another network with C VPN, Dedicated Interconnect, or Partner Interconnect."

upvoted 1 times

[Removed] 2 years, 10 months ago

Selected Answer: C

I got similar question on my exam.

upvoted 3 times

Sreedharveluru 2 years, 11 months ago

ANS - C
Primary and secondary ranges for subnets cannot overlap with any allocated range, any primary or secondary range of another subnet in the same network, or any IPv4 ranges of subnets in peered networks.

upvoted 2 times