

🗨️ **omermahgoub** 1 year, 12 months ago

C. In a secret management system

It is important to store the credentials for your database back-end securely in order to protect them from unauthorized access. One way to do this is by using a secret management system, such as Google Cloud's Secret Manager. Secret Manager is a secure and convenient storage system for API keys, passwords, and other sensitive data that is designed to protect against unauthorized access. By storing the credentials in Secret Manager, you can ensure that they are kept secure and can be easily accessed by your microservices as needed.

Storing the credentials in the source code, an environment variable, or a config file that has restricted access through ACLs may not provide the same level of security as a dedicated secret management system. It is important to ensure that your credentials are stored in a secure and controlled manner to protect against unauthorized access.

upvoted 3 times

🗨️ **AniketD** 2 years, 1 month ago

**Selected Answer: C**

C is correct; If credential then always use secret manager.

upvoted 1 times

🗨️ **megumin** 2 years, 1 month ago

**Selected Answer: C**

C is ok

upvoted 1 times

🗨️ **zr79** 2 years, 2 months ago

secret manager is the answer

upvoted 1 times

🗨️ **AzureDP900** 2 years, 2 months ago

C is right

upvoted 1 times

🗨️ **Kubernetes** 2 years, 3 months ago

answer is C

upvoted 1 times

🗨️ **[Removed]** 2 years, 9 months ago

**Selected Answer: C**

Use Google Secret Manager

upvoted 1 times

🗨️ **rogerlovato** 2 years, 11 months ago

**Selected Answer: C**

C is correct

upvoted 1 times

🗨️ **haroldbenites** 3 years ago

Go for C

upvoted 1 times

🗨️ **vincy2202** 3 years ago

C is the right answer

upvoted 1 times

🗨️ **unnikrisb** 3 years, 2 months ago

Google Practice exam question with option C : In a key management system

C is correct because key management systems generate, use, rotate, encrypt, and destroy cryptographic keys and manage permissions to the keys.

<https://cloud.google.com/kms/>

Question #30

Topic 1

A lead engineer wrote a custom tool that deploys virtual machines in the legacy data center. He wants to migrate the custom tool to the new cloud environment.



You want to advocate for the adoption of Google Cloud Deployment Manager.

What are two business risks of migrating to Cloud Deployment Manager? (Choose two.)

- A. Cloud Deployment Manager uses Python
- B. Cloud Deployment Manager APIs could be deprecated in the future
- C. Cloud Deployment Manager is unfamiliar to the company's engineers
- D. Cloud Deployment Manager requires a Google APIs service account to run
- E. Cloud Deployment Manager can be used to permanently delete cloud resources
- F. Cloud Deployment Manager only supports automation of Google Cloud resources

  **victory108** Highly Voted 3 years, 5 months ago

E. Cloud Deployment Manager can be used to permanently delete cloud resources  
F. Cloud Deployment Manager only supports automation of Google Cloud resources  
upvoted 80 times

  **Gregwaw** 1 year, 2 months ago

F is not a risk, it is a limitation of solution. Risk is something that is not known for sure and is manageable (risk can be mitigated, avoided). cannot manage the limitation of solution. You can use it with this limitation or not and you know it in advance.  
upvoted 5 times

  **Terryhsieh** 11 months, 4 weeks ago

Advocating to adopt Google Cloud Deployment Manager will become a risk if the lead engineer or other business need ask for use other cloud platform.  
upvoted 3 times

  **poseidon24** 3 years, 4 months ago

Yup, E + F. In GCP documentation it states as a warning note that deletion made through Deployment Manager scripts cannot be undone, devs are not well trained a human errors can impact Business  
upvoted 13 times

  **AK2020** Highly Voted 3 years, 6 months ago

C and F- make sense to me  
upvoted 42 times

  **ssepiro** 3 years, 1 month ago

I think this is right. the key of the question is "business risks".  
upvoted 3 times

  **AzureDP900** 2 years, 2 months ago

yes, C and F right  
upvoted 3 times

  **[Removed]** 1 year, 8 months ago

C - Makes sense, because company engineer may take longer to develop, so more cost and more 'time-to-market'

Reg F:

Can I pls ask how does business care whether you are Google Cloud Resources or legacy data center tools, as long as it serves business requirement?

So I'm leaning towards E, as the engineers are still in the process of learning CDM and may accidentally delete VMs bringing down the application.

upvoted 5 times

  **[Removed]** 1 year, 8 months ago

Forgot to mention, once determined as "risks", the mitigation actions below can be followed:

C: Train the existing resources, Hire an experienced personnel

E: Peer Reviews, QA, thorough testing etc.

upvoted 2 times

  **drinkwater** Most Recent 3 weeks, 4 days ago

the right answers are C & E

C: because the engineers are dealing with legacy technologies

E: Cloud Deployment Manager has the ability to delete resources

upvoted 1 times

  **Ekramy\_Elnaggar** 1 month, 1 week ago

**Selected Answer: CF**

I guess everyone agree on C, the debate is between B and F.

Before I start, I need to stress on the word "Business" not "Technical" risks, we need to take this in our minds.

B: Cloud Deployment Manager APIs could be deprecated in the future >> this is not a risk at all as the APIs cannot be changed without an announcement and also there is a backward compatibility to prevent such issues, this is something that is tackled a decade ago in all cloud providers.

F: Cloud Deployment Manager only supports automation of Google Cloud >> Indeed this is a business risk, as the question didn't mention explicitly that the customer is using only GCP, they left it vague by saying "new cloud environment", so we have to assume that it is multi-cloud strategy including On-premise BTW ( Hybrid-Cloud as well ), so we need a tool that can handle deployments on all of those targets.

Based on all of that, I recommend ( C & F )


upvoted 4 times

  **beagle\_Masato** 1 month, 2 weeks ago

**Selected Answer: CF**


C and F right

upvoted 1 times

  **Shasha1** 2 months, 1 week ago

BF are correct


upvoted 1 times

  **Leo212003** 2 months, 3 weeks ago

**Selected Answer: EF**

E and F

upvoted 1 times



  **maxdanny** 3 months, 2 weeks ago

**Selected Answer: BC**

B. Cloud Deployment Manager APIs could be deprecated in the future: There's always a risk that APIs and tools can be deprecated or replaced with new versions. This could impact the long-term stability of your deployment process if the APIs used by Cloud Deployment Manager are deprecated and require migration to new APIs.

C. Cloud Deployment Manager is unfamiliar to the company's engineers: If the company's engineers are not familiar with Cloud Deployment Manager, there could be a learning curve and potential delays during the migration process. Training and adaptation time could affect productivity and introduce risks associated with potential mistakes or inefficiencies during the transition.

upvoted 3 times

  **Armne96X** 4 months ago

B. Cloud deployment manager is being deprecated.

F. Cloud Deployment Manager only supports automation of Google Cloud resources

The question is about business risks - it's not about technical risks

A C D E options are technical aspects of the Deployment manager

upvoted 2 times

  **vbondoo7** 4 months, 2 weeks ago

Should be B & C

upvoted 4 times

  **Choopaower** 5 months, 3 weeks ago

**Selected Answer: BC**

My answer is BC.

I think the correct answers should be related to the engineer's custom tool.


The choices should answer the question "Why should we migrate Lead Engineer's tool to the new cloud environment".

It's tried and tested Custom Tool versus the new Deployment Manager.

B, because it can be deprecated, custom tool has been used for a long time.



C, because their engineers don't know it yet.

upvoted 4 times

  **Sephethus** 6 months, 1 week ago

Chat GPT tells me B and C and it gets it right maybe 98% of the time so far. It seems nobody on this discussion can agree on an answer but i we're going to look at keywords of the questions and over-scrutinize them, then yes, risk is a key word and I don't see F as a risk. E is a risk b not even remotely unique to this situation. C is a mild risk but really the only one that makes sense in light of eliminating the others. B is defini a risk... but then it also isn't unique to this service so we're back at the same issue with E. This question is garbage.



upvoted 2 times

  **ccpmad** 6 months, 1 week ago

**Selected Answer: CF**

for me C and F

upvoted 2 times


  **de1001c** 6 months, 3 weeks ago

**Selected Answer: BF**

B: Cloud deployment manager is being deprecated.

F: Mentions on-premise resources and managing GCP which will make cloud deployment manager not the best tool for this.



upvoted 1 times

  **hitmax87** 7 months, 1 week ago

**Selected Answer: CF**

All solutions can be deprecated, even GCP. So we are talking about current business risks, so for me work C and F

upvoted 2 times

  **Gino17m** 7 months, 3 weeks ago

**Selected Answer: CE**

It's about business risk.

upvoted 1 times

  **Teckexam** 11 months ago

**Selected Answer: CF**

Since business risks are mentioned. C. Training resources will be a cost and untrained resources might cause unnecessary issues costing the business.

F. Since the current tool is developed in house and used on premise its not clear if its used for GCP only. GCP deployment manager is only fo GCP resources.

upvoted 2 times

## Question #31



## Topic 1

A development manager is building a new application. He asks you to review his requirements and identify what cloud technologies he can use to meet them. The application must:



1. Be based on open-source technology for cloud portability
2. Dynamically scale compute capacity based on demand
3. Support continuous software delivery
4. Run multiple segregated copies of the same application stack
5. Deploy application bundles using dynamic templates
6. Route network traffic to specific services based on URL



Which combination of technologies will meet all of his requirements?



- A. Google Kubernetes Engine, Jenkins, and Helm
- B. Google Kubernetes Engine and Cloud Load Balancing
- C. Google Kubernetes Engine and Cloud Deployment Manager
- D. Google Kubernetes Engine, Jenkins, and Cloud Load Balancing

  **rsamant** Highly Voted 3 years, 6 months ago  
it should be A .. helm is needed for "Deploy application bundles using dynamic templates"

Load Balancing should be part of GKE Already  
upvoted 66 times

  **raf2121** 3 years, 3 months ago  
Kubernetes Engine offers integrated support for two types of Cloud Load Balancing (Ingress and External Network Load Balancing) , hence Option A  
Reference : <https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer>  
upvoted 4 times

  **AzureDP900** 2 years, 2 months ago  
A should be fine  
upvoted 2 times

  **Prakzz** 1 year, 2 months ago  
Load balancing is not a part of GKE until it's created explicitly  
upvoted 2 times

 **poseidon24** 3 years, 4 months ago

Not for "based on URL", that is the difference.

upvoted 11 times

 **ashish\_t** 3 years, 2 months ago

[https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer#optional\\_serving\\_multiple\\_applications\\_on\\_a\\_load\\_balancer](https://cloud.google.com/kubernetes-engine/docs/tutorials/http-balancer#optional_serving_multiple_applications_on_a_load_balancer)

As per the above document and given example of "fanout-ingress.yaml" in above document and also in GKE sample repository below <https://github.com/GoogleCloudPlatform/kubernetes-engine-samples/tree/master/load-balancing>

it's clear that GKE LB can handle "6. Route network traffic to specific services based on URL"  
So NO need for Cloud Load balancing.

Helm satisfy "5. Deploy application bundles using dynamic templates"  
and no other option satisfies this point #5.

So correct answer should be:

A

upvoted 16 times

 **victory108** Highly Voted 3 years, 5 months ago

D. Google Kubernetes Engine, Jenkins, and Cloud Load Balancing

upvoted 42 times

 **MikeMike7** Most Recent 1 week, 6 days ago

**Selected Answer: D**

D: load balancing is needed for this requirement: 6. Route network traffic to specific services based on URL

upvoted 1 times

 **drinkwater** 3 weeks, 4 days ago

A & D are both right

Why D Might Still Be Preferred:

While A is a valid choice, D (Google Kubernetes Engine, Jenkins, and Cloud Load Balancing) might be preferred for the following reasons:

Cloud Load Balancing provides a more feature-rich, fully managed solution for routing traffic across multiple regions and services, including advanced load balancing, SSL termination, and support for more sophisticated network traffic management.

It integrates well with GKE and offers additional scalability and flexibility that might be important as your system grows

upvoted 1 times

 **Ekramy\_Elnaggar** 1 month, 1 week ago

**Selected Answer: A**

1. Open-source technology: Kubernetes Engine, Jenkins, and Helm.

2. Dynamically scale compute capacity: Kubernetes Engine provides autoscaling to adjust the number of nodes based on demand.

3. Support continuous software delivery: Jenkins enables CI/CD pipelines for automated building, testing, and deployment of applications.

4. Run multiple segregated copies: Kubernetes Engine allows deploying multiple instances of the application in isolated environments (namespaces) within the same cluster.

5. Deploy application bundles using dynamic templates: Helm uses charts (templates) to define, install, and upgrade Kubernetes applications

6. Route network traffic based on URL: Kubernetes Engine's service objects and ingress controllers can route traffic to specific services based on URLs and other criteria.

upvoted 5 times

 **VedaSW** 3 months, 2 weeks ago

**Selected Answer: A**


Based on: "Be based on open-source technology for cloud portability", I go for A, because it is more portable, as compare to D.

upvoted 2 times

 **Hungdv** 4 months, 1 week ago

Choose A

upvoted 2 times

 **desertlotus1211** 4 months, 2 weeks ago

Yes, Kubernetes can route network traffic to specific services based on URL using Ingress and Ingress controllers

Answer is A

upvoted 1 times

🗨️ 👤 **Chris\_21** 5 months, 3 weeks ago

**Selected Answer: D**

Load Balancer is required as per point 6.  
Jenkins satisfies point 3.  
D is correct  
upvoted 1 times

🗨️ 👤 **Ric350** 5 months ago

Helm is needed for the dynamic templates requirement. The question is vague in whether the application is internally or externally facing which would clarify things a lot more for us. However, in its ambiguity option A has the technologies needed to the requirements and thus deduce or infer that the application is internally facing and the ingress controllers will handle the routing of traffic. It's ambiguous on purpose which I hate in these exams. More of a test of how well we can read and interpret the questions vs our knowledge of material.  
upvoted 3 times

🗨️ 👤 **Rehamss** 9 months ago

**Selected Answer: D**

D is correct  
upvoted 1 times

🗨️ 👤 **kahinah** 9 months, 1 week ago

**Selected Answer: D**

Option A (GKE, Jenkins, Helm) meets most requirements except for explicit URL-based routing, though Kubernetes Ingress (which can be managed through Helm charts) implicitly covers this.

Option D (GKE, Jenkins, Cloud Load Balancing) directly meets every requirement, including URL-based routing without needing to infer capabilities or integrate additional tools beyond the scope of what's listed. Jenkins supports continuous delivery, GKE supports dynamic scaling segregated application stacks, and cloud portability. Cloud Load Balancing directly addresses the URL-based routing requirement.  
upvoted 4 times

🗨️ 👤 **Sephehus** 6 months, 1 week ago

Except none of that meets the needs for deployment templates.  
upvoted 1 times

🗨️ 👤 **Ric350** 5 months ago

My point exactly and my response to Chris\_21. By process of elimination, you need Helm for the dynamic templates and you need Jenkins. Thus, you have to assume the application is internally facing and the ingress controllers will handle the traffic just fine.  
upvoted 1 times

🗨️ 👤 **VidhyaBupesh** 10 months ago

**Selected Answer: D**

D is OK  
upvoted 1 times

🗨️ 👤 **ashishdwi007** 11 months ago

1. Be based on open-source technology for cloud portability: GKE
2. Dynamically scale compute capacity based on demand: GKE
3. Support continuous software delivery: Jenkins
4. Run multiple segregated copies of the same application stack: GKE
5. Deploy application bundles using dynamic templates -> Jenkins
6. Route network traffic to specific services based on URL -> Only HTTPs load balancer can meet this requirement: Next best is Cloud balance (that can be either Network or HTTPs),

So D makes sense to me.  
upvoted 5 times

🗨️ 👤 **kip21** 11 months, 1 week ago

D - Correct  
upvoted 1 times

  **MMuzammil** 11 months, 2 weeks ago



I thought that answer A was correct but after researching HELM I think now the option D is correct. Helm is not a cloud service on its own, and it is not built into Google Kubernetes Engine (GKE). Helm is an open-source package manager for Kubernetes that simplifies the deployment and management of applications on Kubernetes clusters.

Here's a brief overview:

Helm:



Helm allows you to define, install, and upgrade even the most complex Kubernetes applications using packages called charts. A Helm chart includes pre-configured Kubernetes resources that define the structure of an application. Helm provides a convenient way to package, version and deploy applications on Kubernetes.

upvoted 3 times

  **Sephehus** 6 months, 1 week ago

A is the real-world answer, D is the "Google (TM)" answer I think. It's obnoxious how bad these questions are.

upvoted 1 times

  **adoyt** 11 months, 4 weeks ago

**Selected Answer: A**

Kubernetes natively supports routing to different services based on URLs via the ingress gateway regardless of whether a LB is used...

upvoted 1 times

Question #32

Topic 1

You have created several pre-emptible Linux virtual machine instances using Google Compute Engine. You want to properly shut down your application before the virtual machines are preempted.

What should you do?

- A. Create a shutdown script named k99.shutdown in the /etc/rc.6.d/ directory
- B. Create a shutdown script registered as a xinetd service in Linux and configure a Stackdriver endpoint check to call the service
- C. Create a shutdown script and use it as the value for a new metadata entry with the key shutdown-script in the Cloud Platform Console when you create the new virtual machine instance
- D. Create a shutdown script, registered as a xinetd service in Linux, and use the gcloud compute instances add-metadata command to specify the service URL as the value for a new metadata entry with the key shutdown-script-url

  **Eroc**  5 years, 1 month ago

<https://cloud.google.com/compute/docs/shutdownscript> ... So C

upvoted 39 times

  **nitin** 3 years, 9 months ago

C, statup/shutdown script = metadata

upvoted 4 times

  **VishalB** 3 years, 4 months ago

Since the instance is already created Option C gets eliminated. "gcloud compute instances addmetadata" command can be used to add or update the metadata of a virtual machine instance"

upvoted 12 times



  **Gini** Highly Voted 4 years, 7 months ago

I have doubts with the answer C because the question states that "You have created the instances" so C works too but the solution cannot apply to the already created instances. D seems correct to me...

Reference:

[https://cloud.google.com/compute/docs/shutdownscript#apply\\_a\\_shutdown\\_script\\_to\\_running\\_instances](https://cloud.google.com/compute/docs/shutdownscript#apply_a_shutdown_script_to_running_instances)



upvoted 28 times

  **[Removed]** 12 months ago

I think C should be correct over D, because

[https://cloud.google.com/compute/docs/shutdownscript#apply\\_a\\_shutdown\\_script\\_to\\_running\\_instances](https://cloud.google.com/compute/docs/shutdownscript#apply_a_shutdown_script_to_running_instances)

upvoted 2 times

  **NG123** 2 years, 6 months ago

I also feel so because the virtual machines are already created.

upvoted 2 times

  **dsnaghxhinwtsvmip** 1 year, 8 months ago

xinetd. Xinet makes the D answer be nonsense

upvoted 5 times

  **pepYash** 4 years, 1 month ago


Yes. The correct answer should be D.

To add a shutdown script to a running instance, follow the instructions in the Applying a startup script to running instances documentation replace the metadata keys with one of the following keys:

shutdown-script: Supply the shutdown script contents directly with this key. Using the gcloud command-line tool, you can provide the path to a shutdown script file, using the --metadata-from-file flag and the shutdown-script metadata key.

shutdown-script-url: Supply a Cloud Storage URL to the shutdown script file with this key.

upvoted 4 times

  **pepYash** 4 years, 1 month ago

changed my mind. preemptible vms can be stopped and started anytime. with that flexibility, C is ok.

upvoted 6 times

  **RobertArnaud** Most Recent 6 days, 18 hours ago

**Selected Answer: C**

"when you create the new virtual machine instance" means it is too late, then C seems disqualified :( but the other choices are worse ?

upvoted 1 times



  **Ekramy\_Elnaggar** 1 month ago

**Selected Answer: C**

1. Preemptible instances and shutdown scripts: Google Cloud Platform's preemptible instances are cost-effective but can be terminated with short notice. To gracefully handle this, you need a shutdown script that runs before the instance is preempted.

2. Metadata and shutdown-script: Google Cloud allows you to add custom metadata to your instances. When you create a preemptible instance you can include a shutdown-script metadata entry. The value of this entry should be your script, which will be executed automatically before the instance is preempted.

upvoted 1 times

  **Barry123456** 2 months ago

**Selected Answer: D**

It's not C. C says "when you create the new virtual machine instance". But in the question, the instances have already been created. Thus, D. D, "service URL" obviously means cloud storage.

upvoted 1 times

  **snehaso** 4 months, 1 week ago

Among Option C & D, option D uses shutdown-script-url but shutdown-script-url should be a Cloud storage url and not a linux service URL.

That brings us to option C

upvoted 1 times

🗲️ 👤 **Hungdv** 4 months, 1 week ago

Choose C

upvoted 1 times

🗲️ 👤 **nicksb19** 5 months, 3 weeks ago

C is correct since xinetd does not make sense.

upvoted 1 times

🗲️ 👤 **lisabisa** 9 months, 4 weeks ago

**Selected Answer: C**

Every virtual machine instance in GCP has access to a metadata server, which provides information about the instance and allows you to configure various settings, including startup and shutdown scripts.

Startup and shutdown scripts are specified using special metadata keys in the metadata server.

shutdown-script specifies the shutdown script that should be executed when the instance is being shut down.

upvoted 2 times

🗲️ 👤 **ashishdwi007** 11 months ago

**Selected Answer: C**

All other options are related to play with Linux files or services. With Preemptible VMs, these operations are overhead. Hence it makes sense to Automate such tasks.

upvoted 1 times

🗲️ 👤 **Mo7y** 11 months, 1 week ago

**Selected Answer: C**

The answer is either C or D

I exclude D because shutdown-script-url only works with a shutdown script hosted on a cloud storage. Option D wants you to use shutdown-script-url for a locally hosted shutdown script, thus it's not the correct answer.

upvoted 2 times

🗲️ 👤 **kip21** 11 months, 1 week ago

C

<https://cloud.google.com/compute/docs/shutdownscript>

upvoted 1 times

🗲️ 👤 **Terryhsieh** 11 months, 4 weeks ago

The answer should be C. reference to [https://cloud.google.com/compute/docs/shutdownscript#apply\\_a\\_shutdown\\_script\\_to\\_running\\_instances](https://cloud.google.com/compute/docs/shutdownscript#apply_a_shutdown_script_to_running_instances)  
Regarding the answer D, it is not the option because no need to touch xinetd service inside Linux.

upvoted 2 times

🗲️ 👤 **RLsh** 1 year, 1 month ago

**Selected Answer: D**

I believe the answer should be D since the VMs are already created

upvoted 1 times

🗲️ 👤 **Arun\_m\_123** 1 year, 2 months ago

**Selected Answer: C**

C is the right answer. See, there is one tip. In GCP, things like these are given to the customers as a solution - like give a shutdown script. GCP won't trouble the users to know all those geeky linux stuffs. So the answer is simply C

upvoted 1 times

🗲️ 👤 **wukoon** 1 year, 2 months ago

Option D: Creating a shutdown script, registered as a xinetd service in Linux, and using the gcloud compute instances add-metadata command to specify the service URL as the value for a new metadata entry with the key shutdown-script-url is not as reliable as option C because it requires the gcloud command-line tool to be installed and configured on the virtual machine instance.

upvoted 1 times

🗲️ 👤 **vc1011** 1 year, 2 months ago

**Selected Answer: D**

Reference:

[https://cloud.google.com/compute/docs/shutdownscript#apply\\_a\\_shutdown\\_script\\_to\\_running\\_instances](https://cloud.google.com/compute/docs/shutdownscript#apply_a_shutdown_script_to_running_instances)

upvoted 1 times

## Question #33

## Topic 1

Your organization has a 3-tier web application deployed in the same network on Google Cloud Platform. Each tier (web, API, and database) scales independently of the others. Network traffic should flow through the web to the API tier and then on to the database tier. Traffic should not flow between the web and the database tier.

How should you configure the network?

- A. Add each tier to a different subnetwork
- B. Set up software based firewalls on individual VMs
- C. Add tags to each tier and set up routes to allow the desired traffic flow
- D. Add tags to each tier and set up firewall rules to allow the desired traffic flow

🗨️ 👤 **shandy** Highly Voted 👍 5 years ago

D. refer to target filtering. <https://cloud.google.com/solutions/best-practices-vpc-design>  
upvoted 36 times

🗨️ 👤 **tartar** 4 years, 4 months ago

D is ok  
upvoted 8 times

🗨️ 👤 **pepYash** 4 years, 1 month ago

Thank you for the link.  
Precisely:  
[https://cloud.google.com/solutions/best-practices-vpc-design#target\\_filtering](https://cloud.google.com/solutions/best-practices-vpc-design#target_filtering)  
upvoted 8 times

🗨️ 👤 **[Removed]** 1 year, 11 months ago

perfect! the example in that section is the exact question statement  
upvoted 2 times

🗨️ 👤 **nitinz** 3 years, 9 months ago

D, firewalls can be done on ip or network tags or service accounts in GCE.  
upvoted 4 times

🗨️ 👤 **AzureDP900** 2 years, 2 months ago

D is right  
upvoted 1 times

  **amxexam** Highly Voted 3 years, 3 months ago

Let's go with option elimination

A. Add each tier to a different subnetwork

>> Adding tiers to different subnets does not prevent or block them from accessing each other. Until specific firewall rules on VM or subnet allow access traffic on a specific port in the rule.

B. Set up software-based firewalls on individual VMs

>> Not a recommended practice will have to enable firewall anyway.

C. Add tags to each tier and set up routes to allow the desired traffic flow

>> Can be done but.

D. Add tags to each tier and set up firewall rules to allow the desired traffic flow

>> Recommended way

Hence D

upvoted 11 times

  **Ekramy\_Elnaggar** Most Recent 1 month ago

**Selected Answer: D**

1. Firewall rules for security: Firewall rules provide the most granular and robust control over network traffic. By using tags to identify instances each tier (web, API, database), you can create firewall rules that explicitly allow or deny traffic between these tiers.

2. Controlling traffic flow: You can create rules that:

- Allow traffic from the web tier to the API tier.
- Allow traffic from the API tier to the database tier.
- Explicitly deny traffic between the web and database tiers.



3. Scalability and Flexibility: This approach works well even when your tiers scale independently. As new instances are added, they inherit the tags and automatically adhere to the defined firewall rules.

upvoted 1 times

  **ddatta** 2 months ago

D is correct

upvoted 1 times

  **lisabisa** 9 months, 4 weeks ago

**Selected Answer: D**

Routes are typically used for directing traffic between networks rather than within the same network. While tags can be used for identifying resources, they are typically used in conjunction with firewall rules for controlling traffic flow.

upvoted 1 times

  **AdityaGupta** 1 year, 2 months ago

**Selected Answer: D**

Why to implement anything else when Firewall is built-in within VPC and works based on Tags associated with resources.

upvoted 1 times

  **heretolearnazure** 1 year, 3 months ago

separate vnet is ruled out as they are on same network.

upvoted 1 times

  **red\_panda** 1 year, 6 months ago

**Selected Answer: D**

For me most suitable answer is D

upvoted 1 times

  **omermahgoub** 1 year, 12 months ago

It's D

To configure the network so that traffic flows through the web to the API tier and then on to the database tier, but does not flow between the web and the database tier, you can add tags to each tier and set up firewall rules to allow the desired traffic flow. By adding tags to each tier, you can identify the VMs that belong to each tier and create firewall rules that allow traffic between the tiers as needed. For example, you can create a firewall rule that allows traffic from the web tier to the API tier, and another rule that allows traffic from the API tier to the database tier. This will ensure that traffic flows through the desired path and is not allowed between the web and database tiers.

Other options, such as adding each tier to a different subnetwork or setting up software-based firewalls on individual VMs, may not provide the necessary level of control over the traffic flow between the tiers. Setting up routes to allow the desired traffic flow may not be sufficient to prevent traffic between the web and database tiers.

upvoted 5 times

  **megumin** 2 years, 1 month ago

**Selected Answer: D**

D is ok

upvoted 1 times

  **Mahmoud\_E** 2 years, 1 month ago

**Selected Answer: D**

D is right answer



upvoted 1 times

  **minmin2020** 2 years, 2 months ago

**Selected Answer: D**

Having 3-tier web application deployed in the same network is wrong to begin with. However, even in different subnets you will need to apply firewall rules to prevent traffic between selected subnets. In this case they will probably be better off with D.

upvoted 1 times

  **zr79** 2 years, 2 months ago

Did this appear in the exam?

upvoted 1 times

  **holerina** 2 years, 2 months ago

use firewall rules

upvoted 1 times

  **amxexam** 2 years, 7 months ago

**Selected Answer: D**

A per my comment below .

upvoted 1 times

  **vincy2202** 2 years, 11 months ago


D is the correct answer

upvoted 3 times

  **haroldbenites** 3 years ago

Go for D

upvoted 2 times

  **unnikrisb** 3 years, 2 months ago

From Google practice exam question :

D is correct because as instances scale, they will all have the same tag to identify the tier. These tags can then be leveraged in firewall rules to allow and restrict traffic as required, because tags can be used for both the target and source.

<https://cloud.google.com/vpc/docs/using-vpc>

<https://cloud.google.com/vpc/docs/routes>

<https://cloud.google.com/vpc/docs/add-remove-network-tags>

upvoted 2 times

Question #34

Topic 1

Your development team has installed a new Linux kernel module on the batch servers in Google Compute Engine (GCE) virtual machines (VMs) to speed up the nightly batch process. Two days after the installation, 50% of the batch servers failed the nightly batch run. You want to collect details on the failure to pass back to the development team.

Which three actions should you take? (Choose three.)

- A. Use Stackdriver Logging to search for the module log entries
- B. Read the debug GCE Activity log using the API or Cloud Console
- C. Use gcloud or Cloud Console to connect to the serial console and observe the logs
- D. Identify whether a live migration event of the failed server occurred, using in the activity log
- E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics
- F. Export a debug VM into an image, and run the image on a local server where kernel log messages will be displayed on the native screen

  **rishab86** Highly Voted 3 years, 6 months ago

ACE

- A. Use Stackdriver Logging to search for the module log entries = Check logs
- C. Use gcloud or Cloud Console to connect to the serial console and observe the logs = Check grub messages, remember new kernel module was installed.
- E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics = Zoom into the time window when problem happened.

upvoted 45 times

  **Pokchok** 3 years, 6 months ago



But the assumption you made is that stack driver was already installed on the vms. What if it was not there? Would there be any scope to install later and retrieve the logs?

upvoted 3 times

  **[Removed]** 1 year, 11 months ago

But isn't it the same with B? it is talking about 'reading' the logs.

upvoted 1 times

  **AmitAr** 2 years, 7 months ago

A, B, E

C - doesn't look correct as it ends with "observe the logs" - question is on sharing the details to development team, not to look for cause

upvoted 1 times

  **tocsa** 6 months, 2 weeks ago

E observe the logs too. One of my problem is that several of the options go on and do some observation instead of just delivering.



upvoted 1 times

  **haroldbenites** Highly Voted 3 years ago

Go for A,B,E.

C is when the VM is running , but in this case the sentence says "recollect". It means that "error ever" already happened.

upvoted 11 times

  **pddddd** 2 years, 11 months ago

and how will activity log help?



upvoted 1 times

  **mahi\_h** Most Recent 1 day, 18 hours ago

**Selected Answer: ABE**

I chose B over C as both options trying to read/observe logs. But C looks like reading at the runtime. Give that, it's a nightly batch process, B seems to suitable post error occurrence.

upvoted 1 times

  **deep316** 1 week ago



**Selected Answer: ACD**

A. Use Stackdriver Logging to search for the module log entries: This will help you identify any errors or issues related to the new kernel module that were logged during the batch process.

C. Use gcloud or Cloud Console to connect to the serial console and observe the logs: The serial console logs can provide detailed information about the boot process and any kernel-related messages that might indicate why the batch servers failed.

D. Identify whether a live migration event of the failed server occurred, using the activity log: Live migration events can sometimes cause disruptions. Checking the activity log will help you determine if this was a factor in the failures.

upvoted 1 times

  **deep316** 1 week ago

**Selected Answer: ACE**

A. Use Stackdriver Logging to search for the module log entries: This will help you identify any errors or issues related to the new kernel module that were logged during the batch process.

C. Use gcloud or Cloud Console to connect to the serial console and observe the logs: The serial console logs can provide detailed information about the boot process and any kernel-related messages that might indicate why the batch servers failed.

D. Identify whether a live migration event of the failed server occurred, using the activity log: Live migration events can sometimes cause disruptions. Checking the activity log will help you determine if this was a factor in the failures.

upvoted 1 times

  **Ekramy\_Elnaggar** 1 month ago

**Selected Answer: ACE**

A. Use Stackdriver Logging to search for the module log entries: This is crucial. Stackdriver Logging aggregates logs from various sources, including your VMs. You can search for specific entries related to the new kernel module to identify errors, warnings, or unusual behavior that might explain the failures.

C. Use gcloud or Cloud Console to connect to the serial console and observe the logs: The serial console provides access to the VM's output even if the system is unresponsive. This can be invaluable for capturing kernel panic messages, boot errors, or other critical information that might not be available through standard logging channels.

E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics: Stackdriver Monitoring provides detailed performance metrics for your VMs. By aligning the timeline with the failures, you can analyze CPU usage, memory consumption, disk I/O, and network activity.

upvoted 1 times

  **SerGCP** 1 month, 1 week ago

**Selected Answer: ABE**

considering that logs from the serial console might not be useful after two days:

A. Use Stackdriver Logging to search for the module log entries: This will help you identify any errors or issues logged by the new kernel module.

B. Read the debug GCE Activity log using the API or Cloud Console: This can provide information on significant events like reboots or live migrations that might have affected the batch process.

E. Adjust the Google Stackdriver timeline to match the failure time, and observe the batch server metrics: This helps correlate the failure with anomalies in the server metrics, providing insights into what might have gone wrong.

upvoted 1 times

  **nareshthumma** 1 month, 3 weeks ago

Answer is ACE

upvoted 1 times

  **Hungdv** 4 months, 1 week ago

Vote ACE

upvoted 1 times

  **Gino17m** 7 months, 3 weeks ago

**Selected Answer: ABE**

I'm not sure but I vote for ABE

upvoted 2 times

ashishdwi007 11 months ago

ACE makes sense.

A and E dont have any doubts. Questions is that if it is B, C or F.

Whats' use of serial console if team does not use it for logging especially kernal related updates. that makes sense to choose C.

upvoted 1 times

CloudDom 1 year ago

**Selected Answer: ABE**

Most automated way, with C, collecting from VMs involves a lot of manual efforts

upvoted 3 times

pabloairat 1 year, 4 months ago

**Selected Answer: ABE**

ABE is correct

upvoted 2 times

Ozymandiox 1 year, 11 months ago

I'm really not sure here. A and E are just OK, and for me the final point is between B o C. many ppl is saying C, but, the question says that the VM's already failed and you're investigating what happened in the past.

Anyway, there are 2 ways to interpret this, from my point of view:

1) The failure happened and it's going to happen again. In this case ACE would be maybe the best option

BUt

2) The failure happened and you want to investigate this failure, which happened in the past. Therefore ABE would be the right one, as you are "splunking" in the logs of the past, not having a review of the logs as they happen.

from my personal interpretation I'd go with ABE

upvoted 8 times

omermahgoub 1 year, 12 months ago

ACE

To collect details on the failure of the batch servers in GCE VMs, you can take the following actions:

A: Stackdriver Logging can help you identify any issues related to the new Linux kernel module by searching for log entries related to the mod

C: Connecting to the serial console allows you to view the logs in real-time as the batch servers are running. This can help you identify any iss related to the new kernel module.

E: By adjusting the timeline in Stackdriver to match the failure time, you can view the batch server metrics during the time when the failures occurred. This can help you identify any issues related to the new kernel module.

Other options, such as reading the debug GCE Activity log using the API or Cloud Console, identifying whether a live migration event of the fa server occurred, or exporting a debug VM into an image and running the image on a local server, may not provide the necessary information t understand

upvoted 3 times

minmin2020 2 years, 2 months ago

**Selected Answer: ACE**

ACE by eliminating the incorrect answers

upvoted 2 times

holerina 2 years, 2 months ago

ADE seems correct

upvoted 1 times

Question #35

Topic 1

Your company wants to try out the cloud with low risk. They want to archive approximately 100 TB of their log data to the cloud and test the



analytics features available to them there, while also retaining that data as a long-term disaster recovery backup.

Which two steps should you take? (Choose two.)

- A. Load logs into Google BigQuery
- B. Load logs into Google Cloud SQL
- C. Import logs into Google Stackdriver
- D. Insert logs into Google Cloud Bigtable
- E. Upload log files into Google Cloud Storage

  **rishab86** Highly Voted 3 years, 6 months ago

Answer is A as they want to load logs for analytics and E for storing data in buckets for long term.

upvoted 33 times

  **omermahgoub** Highly Voted 1 year, 12 months ago

AE

To archive approximately 100 TB of log data to the cloud and test the analytics features available while also retaining the data as a long-term disaster recovery backup, you can take the following steps:

E: Upload log files into Google Cloud Storage: Google Cloud Storage is a scalable, durable, and fully-managed cloud storage service that can be used to store large amounts of data. You can upload your log files to Cloud Storage to archive them in the cloud.

A: Load logs into Google BigQuery: Google BigQuery is a fully-managed, cloud-native data warehouse that can be used to analyze large amounts of data quickly and efficiently. You can load your log data into BigQuery to perform analytics on it and test the available analytics features.

Other options, such as loading logs into Google Cloud SQL, importing logs into Google Stackdriver, or inserting logs into Google Cloud Bigtable may not provide the necessary functionality for archiving and analyzing the log data.

upvoted 11 times

  **Ekramy\_Elnaggar** Most Recent 1 month ago

Selected Answer: AE

A. Load logs into Google BigQuery: BigQuery is Google Cloud's serverless, highly scalable, and cost-effective multicloud data warehouse designed for data analytics. It's ideal for storing and analyzing large volumes of log data (100 TB in this case). You can use BigQuery's powerful SQL capabilities to run queries, generate reports, and gain insights from your logs.

E. Upload log files into Google Cloud Storage: Cloud Storage provides durable, scalable, and secure object storage. It's perfect for storing your log data as a long-term disaster recovery backup. Cloud Storage offers different storage classes to optimize costs based on your data access frequency and retention needs.


upvoted 1 times

  **ionescuandrei** 1 year, 8 months ago

Selected Answer: AE

This looks right.

upvoted 2 times

  **CMata** 2 years, 1 month ago

Selected Answer: AE

If you want to analyze those logs its recommended Big Query. For storing and backup Cloud Storage is your option, so AE

upvoted 3 times

  **AzureDP900** 2 years, 2 months ago

A and E can do the required task

upvoted 2 times

  **minmin2020** 2 years, 2 months ago

Selected Answer: AE

AE are the only options for analysis and archiving

upvoted 1 times

🗨️ 👤 **holerina** 2 years, 2 months ago

A load in Big query for analytics and E for cloud storage

upvoted 1 times

🗨️ 👤 **Ramheadhunter** 2 years, 4 months ago

**Selected Answer: AE**

The key word is 'Analytics' here the main reason for moving logs to GCP is to perform Analytics on the data. BigQuery is the best suite for it. I long term storage it would be GC

upvoted 1 times

🗨️ 👤 **raaj\_p** 2 years, 4 months ago

**Selected Answer: CE**

Answer is C and E

Key features

Real-time log management and analysis

Cloud Logging is a fully managed service that performs at scale and can ingest application and platform log data, as well as custom log data from GKE environments, VMs, and other services inside and outside of Google Cloud. Get advanced performance, troubleshooting, security, business insights with Log Analytics, integrating the power of BigQuery into Cloud Logging. - <https://cloud.google.com/products/operations>

upvoted 2 times

🗨️ 👤 **AMohanty** 2 years, 4 months ago

you don't do realtime log management on 10 TB data.

You only perform analytics on it.

So A for Analytics

E for storage.

upvoted 6 times

🗨️ 👤 **tocsa** 6 months, 2 weeks ago

Is it even possible to import 10TB of logs into StackDriver?

upvoted 1 times

🗨️ 👤 **Ramheadhunter** 2 years, 4 months ago

The key word is 'Analytics' here the main reason for moving logs to GCP is to perform Analytics on the data. BigQuery is the best suite for For long term storage it would be GCS

upvoted 1 times

🗨️ 👤 **faagee01** 2 years, 4 months ago

**Selected Answer: AE**

Big Query for analytics, Cloud Storage for long term archive

upvoted 3 times

🗨️ 👤 **Dhiraj03** 2 years, 6 months ago

For Storage GCS is the best option and for analyzing the data Blg Query makes sense

upvoted 1 times

🗨️ 👤 **Nirca** 2 years, 7 months ago

A E are ok

upvoted 2 times

🗨️ 👤 **vincy2202** 2 years, 11 months ago

AE are the correct answers

upvoted 3 times

  **andeu** 3 years ago

Answers: A is correct because BigQuery is the fully managed cloud data warehouse for analytics and supports the analytics requirement. E is correct because Cloud Storage provides the Coldline storage class to support long-term storage with infrequent access, which would support the long-term disaster recovery backup requirement.

<https://cloud.google.com/bigquery/>



<https://cloud.google.com/stackdriver/>

<https://cloud.google.com/storage/docs/storage-classes#coldline>

<https://cloud.google.com/sql/>

<https://cloud.google.com/bigtable/>

upvoted 4 times

  **MQQ** 2 years, 6 months ago

But BigQuery is for SQL DATA, the logs are nosql ?

Why not choose stackdriver?

upvoted 1 times

  **haroldbenites** 3 years ago

Go for A,E

upvoted 3 times

  **Bakili** 3 years ago

A and E

#### Question #36

Topic 1

You created a pipeline that can deploy your source code changes to your infrastructure in instance groups for self-healing. One of the changes negatively affects your key performance indicator. You are not sure how to fix it, and investigation could take up to a week. What should you do?

- A. Log in to a server, and iterate on the fix locally
- B. Revert the source code change, and rerun the deployment pipeline
- C. Log into the servers with the bad code change, and swap in the previous code
- D. Change the instance group template to the previous one, and delete all instances

  **amxexam** Highly Voted 3 years, 3 months ago

Let's go with option elimination

A. Log in to a server, and iterate on the fix locally

>> Long step, hence eliminate

B. Revert the source code change and rerun the deployment pipeline

>> This revert will be logged in the source repo. Will go with this way although D also is correct.

C. login to the servers with the bad code change, and swap in the previous code

>> C is manually doing what can be automatically done by B and C, hence eliminate.

D. Change the instance group template to the previous one and delete all instances

>> This is similar to B but why manually do something which is automated. Hence eliminate. But is also correct. But B is better from code lifecycle perspective.

Hence B

upvoted 75 times

  **ashishdwi007** 11 months ago

The question itself looks the madeup. Not a real scenario ... "You created a pipeline that can deploy your source code changes to your infrastructure in instance groups for self-healing. One of the changes negatively affects your key performance indicator. " How a self healing code is affecting KPI. What was KPI, we dont know. Was the self healing done? we dont know. Dont know who make this questions. Even we go whatever they try to ask, with options available, B is safest. However this option is just answer to any troubleshooting step. I m not convinced for the person who wrote this question

upvoted 3 times

  **ewredtrfygi** Highly Voted 4 years, 4 months ago

Too many responses saying B is the answer - I wonder if GCP pays people to provide the wrong answers on this website. It's clearly D, MIG templates support versioning, they were created to solve this exact problem. You simply select the previous template version, set that as the deployment, and it will roll back the KPI depriving deployment and roll out the previous working deployment. The only part of D I don't like is "terminate all instances" since you should engage in a rolling deployment, but if it's not a live website I suppose that would be fine.



<https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups>

upvoted 62 times

  **mexblood1** 4 years, 1 month ago



If you can deploy your source code changes to the infrastructure in instance group for self-healing, it means you're not using Managed Instance Groups. Otherwise you would be creating a new template with the code changes. Further more, you would not delete instances on a MIG, would be rolling out the previous template again in a controlled manner using maxsurge, maxunavailable, etc. For those reasons I'll choose

upvoted 21 times

  **AmitAr** 2 years, 6 months ago

B. keyword is "self-healing" not "auto-healing" - which means MIG not used. So correct answer is B

upvoted 2 times

  **Bill831231** 3 years, 2 months ago

seems with approach, there will be a mismatch in pipeline

upvoted 4 times

  **Meyucho** 2 years, 11 months ago

If you change manually the template.. why are using pipelines? B is the best answer because is automated!!! Why Google will be interested vote the wrong answers??? They want more professionals with GCP certifications!!!!

upvoted 7 times

  **Davidik79** 2 years, 9 months ago

"....One of the changes has impacted negatively your PKI". Why is the question about pipeline? It is about how to do investigations and keep your PKI at the proper SLA/SLO.

upvoted 1 times

  **Ekramy\_Elnaggar** Most Recent 1 month ago

**Selected Answer: B**

1. Quickest path to recovery: Reverting the code change that caused the performance degradation is the fastest way to restore your key performance indicator (KPI) to its previous level. Your pipeline is designed to automate deployments, so re-deploying the known good version should be straightforward.

2. Minimizes downtime: While investigating the issue is important, it can take time. Reverting first minimizes the duration of the negative impact on your KPI.

3. Clean and controlled: This approach avoids making ad-hoc changes directly on servers (options A and C), which can lead to inconsistencies and make it harder to track the problem's source.



4. Maintains instance group integrity: Option D involves deleting instances, which can disrupt services and lead to unnecessary re-creation of resources.

upvoted 1 times

  **sim7243** 1 month, 1 week ago

option B


upvoted 1 times

  **dija123** 8 months, 2 weeks ago

**Selected Answer: B**

Agree with B

upvoted 1 times

  **lisabisa** 9 months, 3 weeks ago

D is infrastructure change.

B is application change.

So B is correct.

upvoted 3 times