AdityaGupta 1 year, 2 months ago

Selected Answer: D

D is correct answer because

- Memcache backed by Persistent Disk SSD storage for customer session state data. - Persistent disk will ensure that Session data is preserv evern if not used for long time.

- Assorted local SSD-backed instances for VM boot/data volumes. Provides faster boot up for VMs. (There is no requirement for persistent storage)

- Cloud Storage for log archives and thumbnails. - For low cost and scalable solution.

upvoted 1 times

ductrinh 1 year, 2 months ago

d wrong because of local ssd cannot use for boot image. its temporary and will be cleared if vm was suspended >> so chose b

upvoted 2 times

A21325412 1 year, 1 month ago

A lot of folks keep saying D is wrong because of "local SSD". It never mentioned "local" in option D. It said "Persistent Disk SSD".

https://cloud.google.com/compute/docs/disks

I would definitely choose D.

upvoted 2 times

A21325412 1 year, 1 month ago

My bad, I was focusing on the memcache. I would choose C. The "assorted local ssd" for VM boot/data volumes can't work, as Local SSDs are ephemeral, meaning it's lost if the VM instance is stopped or deleted.

upvoted 1 times

A21325412 1 year, 1 month ago

I think I'm tired. I meant to write Option B as the correct answer.
Memcache backed by Cloud Datastore, etc.

upvoted 1 times

Murtuza 1 year, 3 months ago

Local SSD means Ephemeral (Temp Disk) so do not confused with PERSISTENT disk (Permanent Disk). The data that you store on a local S persists only until the instance is stopped or deleted.

upvoted 1 times

medi01 1 year, 8 months ago

Selected Answer: B

Local SSD cannot be used for neither boot nor data!!! This rules out B&C. Oh, and A too.

upvoted 1 times

Kamaly 1 year, 8 months ago

Selected Answer: B

Cloud Datastore is the right solution to store the session data

upvoted 1 times

feholen210 1 year, 9 months ago

Selected Answer: B

B Seems correct.

upvoted 1 times

ile02 1 year, 9 months ago

D. makes more sense

upvoted 1 times

WAENANY 1 year, 9 months ago

Selected Answer: D

d makes more sense

upvoted 1 times

Deb2293 1 year, 9 months ago

Selected Answer: D

ChatGPT says option D.

upvoted 1 times

Deb2293 1 year, 9 months ago

chatgpt has knowledge till Sept 2021. Don't rely on it bro

upvoted 3 times

kaleemahmad75 1 year, 11 months ago

Selected Answer: D

My answer is D

upvoted 1 times

Santanu_01 1 year, 11 months ago

I will go with Option D as it is best practice to keep similar data together and seprate OS, Volatile and permanent

upvoted 2 times

thamaster 1 year, 12 months ago

Selected Answer: D

i'll go D because i don't think Cloud storage can be used for booting a VM.

upvoted 2 times

Question #87 *Topic 1*

Your web application uses Google Kubernetes Engine to manage several workloads. One workload requires a consistent set of hostnames even after pod scaling and relaunches.

Which feature of Kubernetes should you use to accomplish this?

A. StatefulSets

B. Role-based access control

C. Container environment variables

D. Persistent Volumes

Eroc Highly Voted 3 years, 7 months ago

StatefulSets is a feature of Kubernetes, which the question asks about. Yes, Persistent volumes are required by StatefulSets (https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/). See the Google documentations for mentioning of hostnames (https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset)... Answer A

upvoted 57 times

tartar 2 years, 10 months ago

A is ok

upvoted 6 times

OrangeTiger 1 year, 5 months ago

thank you!

upvoted 1 times

kumarp6 2 years, 7 months ago

A is correct, statefulset

upvoted 2 times

nitinz 2 years, 3 months ago

It is A

upvoted 2 times

omermahgoub Highly Voted 6 months ago

A. StatefulSets

To ensure that a workload in Kubernetes has a consistent set of hostnames even after pod scaling and relaunches, you should use StatefulSe StatefulSets are a type of controller in Kubernetes that is used to manage stateful applications. They provide a number of features that are specifically designed to support stateful applications, including:

Stable, unique network identifiers for each pod in the set
Persistent storage that is automatically attached to pods
Ordered, graceful deployment and scaling of pods
Ordered, graceful deletion and termination of pods
By using StatefulSets, you can ensure that your workload has a consistent set of hostnames even if pods are scaled or relaunched, which car important for applications that rely on stable network identifiers.

upvoted 17 times

Tamirm 4 months, 1 week ago

You are the best.. thanks for all the hard work to explain

upvoted 2 times

Wangyu60 2 months, 2 weeks ago

obviously from chatGPT, but still good to share.

upvoted 1 times

kaleemahmad75 Most Recent 5 months ago

Selected Answer: A

A is the answer

upvoted 1 times

megumin 7 months, 1 week ago

Selected Answer: A

A is ok

upvoted 1 times

⊟ **Deepak31** 7 months, 2 weeks ago

A StatefulSet is the Kubernetes controller used to run the stateful application as containers (Pods) in the Kubernetes cluster. StatefulSets assi sticky identity—an ordinal number starting from zero—to each Pod instead of assigning random IDs for each replica Pod. A new Pod is create by cloning the previous Pod's data.

upvoted 2 times

⊟ **AzureDP900** 8 months ago

this is straight forward question if you know kubernetes concepts. A is right

upvoted 1 times

⊟ **zr79** 8 months ago

I do not know Kubernetes

upvoted 2 times

⊟ **DrishaS4** 10 months, 2 weeks ago

Selected Answer: A

https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/

upvoted 3 times

⊟ **mv2000** 11 months, 2 weeks ago

06/30/2022 Exam

upvoted 3 times

⊟ **haroldbenites** 1 year, 6 months ago

Go for A.
https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/

upvoted 2 times

⊟ **vincy2202** 1 year, 6 months ago

Selected Answer: A

A is the correct answer

upvoted 2 times

⊟ **MaxNRG** 1 year, 7 months ago

A – StatefulSets
StatefulSets are suitable for deploying Kafka, MySQL, Redis, ZooKeeper, and other applications needing unique, persistent identities and stal hostnames. Read more about StatefulSets. https://cloud.google.com/kubernetes-engine/docs/concepts/statefulset

C – Container Env Variable, are good if you need to init containers with some static content. E.g. Pod passes to containers its HOSTNAME (where containers are running), namespace and user defined vars. So, env vars is a way for Pod to init containers at start up. But, stable hostnames must be preserved at Pod level via StatefulSets.
Defining Env Vars for Container: https://kubernetes.io/docs/tasks/inject-data-application/define-environment-variable-container/

upvoted 6 times

⊟ **Arjun1983** 1 year, 7 months ago

StatefulSets are designed to deploy stateful applications and clustered applications that save data to persistent storage, such as Compute Engine persistent disks. StatefulSets are suitable for deploying Kafka, MySQL, Redis, ZooKeeper, and other applications needing unique, persistent identities and "stable hostnames". Answer is A

upvoted 2 times

⊟ **victory108** 2 years, 1 month ago

A. StatefulSets

upvoted 3 times

⊟ **un** 2 years, 1 month ago

A is correct

upvoted 1 times

⊟ **Ausias18** 2 years, 2 months ago

Answer is A

upvoted 1 times

BhupalS 2 years, 6 months ago

A is the Ans
https://kubernetes.io/docs/concepts/workloads/controllers/statefulset/

upvoted 1 times

Chulbul_Pandey 2 years, 6 months ago

StatefulSets for sequencing..
A is correct

upvoted 1 times

Question #88 *Topic 1*

You are using Cloud CDN to deliver static HTTP(S) website content hosted on a Compute Engine instance group. You want to improve the cache hit ratio.
What should you do?

A. Customize the cache keys to omit the protocol from the key.

B. Shorten the expiration time of the cached objects.

C. Make sure the HTTP(S) header ג€Cache-Regionג€ points to the closest region of your users.

D. Replicate the static content in a Cloud Storage bucket. Point CloudCDN toward a load balancer on that bucket.

shandy Highly Voted 5 years ago

Option A is Correct.
https://cloud.google.com/cdn/docs/caching#cache-keys

upvoted 23 times

tartar 4 years, 4 months ago

A is ok

upvoted 7 times

kumarp6 4 years, 1 month ago

Yes, A is correct

upvoted 2 times

nitinz 3 years, 9 months ago

A, both http and https will use same key.

upvoted 3 times

MestreCholas 1 year, 9 months ago

https://cloud.google.com/cdn/docs/best-practices#cache-hit-ratio

upvoted 6 times

gfhbox0083 Highly Voted 4 years, 6 months ago

A, for sure.
By default, Cloud CDN uses the complete request URL to build the cache key. For performance and scalability, it’s important to optimize cach
hit ratio. To help optimize your cache hit ratio, you can use custom cache keys .....

upvoted 9 times

⊟ **Ekramy_Elnaggar** Most Recent 4 weeks, 1 day ago

Selected Answer: A

Cache Keys and Protocols: Cloud CDN uses cache keys to identify and store content in its cache. By default, the protocol (HTTP or HTTPS) i included in the cache key. This means that the same content served over HTTP and HTTPS will be cached separately, reducing the cache hit ratio.

Omitting the Protocol: Customizing the cache keys to omit the protocol allows Cloud CDN to treat HTTP and HTTPS requests for the same content as identical. This increases the chance of a cache hit, as the CDN can serve the cached content regardless of the protocol used in the request.

Improved Cache Hit Ratio: By consolidating the cache entries for HTTP and HTTPS versions of the content, you effectively increase the cache ratio. This leads to better performance, reduced latency, and lower costs.

upvoted 1 times

⊟ **nareshthumma** 1 month, 3 weeks ago

Answer is D

upvoted 1 times

⊟ **Prajjwal199831** 9 months, 4 weeks ago

Selected Answer: A

A is right

upvoted 2 times

⊟ **JB28** 10 months ago

option D

upvoted 2 times

⊟ **Pime13** 10 months, 2 weeks ago

Selected Answer: A

https://cloud.google.com/cdn/docs/best-practices#cache-hit-ratio

upvoted 1 times

⊟ **bargou** 10 months, 3 weeks ago

Selected Answer: D

i'm with D Option

upvoted 2 times

⊟ **AdityaGupta** 1 year, 2 months ago

Selected Answer: A

https://cloud.google.com/cdn/docs/best-practices#using_custom_cache_keys_to_improve_cache_hit_ratio

A is correct option, use custom keys.

upvoted 2 times

⊟ **Gregwaw** 1 year, 2 months ago

Selected Answer: D

A and D could be OK but there is no information in the question that both http and https protocols are used (it is in fact not probable to use bo protocols). Anwer A would be only valid when both http and https are in use.

upvoted 1 times

⊟ **MikeH20** 1 year ago

Incorrect, respectfully. "HTTP(S)" (the parenthesis) implies that HTTP requests can be made using *either* HTTP or HTTPS, especially if TL not mandatory. If a site returns a 200 OK for http://www.example.com/picture/of/a/cat.jpg and httpS://www.example.come/picture/of/a/cat.jpg, then you should exclude the protocol in the cache key to increase the cache-hit ratio. If y don't, the CDN will treat both URLs as different objects.

upvoted 2 times

⊟ **heretolearnazure** 1 year, 3 months ago

A sounds correct

upvoted 1 times

daidaidai 1 year, 4 months ago

Replicating static content in a Cloud Storage bucket and pointing CloudCDN toward a load balancer on that bucket may improve the distribut of content but is not directly related to improving the cache hit ratio based on the customizing of cache keys.

upvoted 1 times

VarunGo 1 year, 7 months ago

Selected Answer: D

D

This option is the best because Cloud Storage has built-in caching and can serve content faster than Compute Engine instances. It also allow for better scalability and availability. By pointing Cloud CDN towards a load balancer on the Cloud Storage bucket, the cache hit ratio can be improved as the content will be served directly from the cache without needing to access the Compute Engine instances.

Option A (Customize the cache keys to omit the protocol from the key) may not be effective in improving the cache hit ratio as it only removes protocol from the cache key and does not address the underlying issue of slow content delivery.

upvoted 2 times

Deb2293 1 year, 9 months ago

Selected Answer: D

Customizing the cache keys by omitting the protocol from the key (option A) can be a valid approach to improve the cache hit ratio for CDN delivered Compute Engine, but it may not be the most effective solution for all cases.

Customizing the cache keys can improve the cache hit ratio by reducing the number of cache misses caused by variations in the request URL headers, and parameters. However, customizing the cache keys requires careful consideration of the caching policies, traffic patterns, and content types

upvoted 1 times

omermahgoub 1 year, 12 months ago

A. Customize the cache keys to omit the protocol from the key.

To improve the cache hit ratio with Cloud CDN, you should customize the cache keys to omit the protocol (e.g. HTTP or HTTPS) from the key. This will allow Cloud CDN to cache the same content under both HTTP and HTTPS, which can help to improve the hit ratio by allowing Cloud CDN to serve content from cache more frequently.

To customize the cache keys, you can use the --key-include-protocol flag when enabling Cloud CDN for your Compute Engine instance group load balancer. Setting this flag to false will cause Cloud CDN to omit the protocol from the cache key.

Other options, such as shortening the expiration time of cached objects or replicating content in Cloud Storage, may also help to improve the cache hit ratio, but customizing the cache keys to omit the protocol is likely to have the greatest impact.

upvoted 8 times

AzureDP900 2 years, 2 months ago

https://cloud.google.com/cdn/docs/best-practices#cache-hit-ratio. A is right

upvoted 3 times

AzureDP900 2 years, 2 months ago

Each cache entry in a Cloud CDN cache is identified by a cache key. When a request comes into the cache, the cache converts the URI of request into a cache key, and then compares it with keys of cached entries. If it finds a match, the cache returns the object associated witl that key.

upvoted 2 times

aut0pil0t 2 years, 3 months ago

Selected Answer: A

Use case:
"A logo needs to be cached whether displayed through HTTP or HTTPS. When you customize the cache keys for the backend service that ho the logo, clear the Protocol checkbox so that requests through HTTP and HTTPS count as matches for the logo's cache entry."

https://cloud.google.com/cdn/docs/best-practices#using_custom_cache_keys_to_improve_cache_hit_ratio

upvoted 2 times

Question #89 *Topic 1*

Your architecture calls for the centralized collection of all admin activity and VM system logs within your project.

How should you collect these logs from both VMs and services?

A. All admin and VM system logs are automatically collected by Stackdriver.

B. Stackdriver automatically collects admin activity logs for most services. The Stackdriver Logging agent must be installed on each instance to collect system logs.

C. Launch a custom syslogd compute instance and configure your GCP project and VMs to forward all logs to it.

D. Install the Stackdriver Logging agent on a single compute instance and let it collect all audit and access logs for your environment.

MeasService Highly Voted 4 years, 8 months ago

Does not agree with D. B is the nearest answer I feel !

upvoted 43 times

KouShikyou 4 years, 8 months ago

Agree.

upvoted 9 times

tartar 3 years, 10 months ago

B is ok

upvoted 12 times

nitinz 3 years, 3 months ago

It is B, all rest are BS

upvoted 2 times

kumarp6 3 years, 7 months ago

B is correct, D is SPOF ...

upvoted 2 times

shandy Highly Voted 4 years, 6 months ago

Admin and event logs are configured by default. VM System logs require a logging agent to be configured. So A is not valid. Answer is B

upvoted 20 times

JaimeMS Most Recent 2 weeks, 2 days ago

Selected Answer: B

Admin and event logs are configured by default. VM System logs require a logging agent to be configured. Answer is B

upvoted 1 times

hitmax87 1 month ago

Selected Answer: A

Stackdriver Logging agent doesn't need for audit logs

upvoted 1 times

convers39 5 months, 2 weeks ago

Selected Answer: B

B is correct
Now it is recommended to use OpsAgent as a replacement. Although you can create a VM instance with OpsAgent automatically enabled, wh
makes it look like 'the logging is automatically enabled', under the hood you need to install the agent on the instance.
https://cloud.google.com/stackdriver/docs/solutions/agents/ops-agent/install-agent-vm-creation

upvoted 2 times

stefanop 6 months, 1 week ago

Selected Answer: A

A: Stackdriver already collects admin logs and GCE logs.

upvoted 2 times

spuyol 6 months, 1 week ago

Answer is A
you don't need to install the Stackdriver Logging agent or any other agents in order to collect admin or system logs from compute engine instances (VM):
https://cloud.google.com/compute/docs/logging/activity-logs
https://cloud.google.com/compute/docs/logging/audit-logging

upvoted 2 times

squishy_fishy 7 months, 1 week ago

Answer is B, but it would be more accurate if the answer mentioned install the Ops Agent on the VMs.
https://cloud.google.com/logging/docs/agent/ops-agent

upvoted 1 times

jlambdan 1 year, 2 months ago

Selected Answer: B

answer is B as per this tutorial step: https://cloud.google.com/logging/docs/logging-gce-quickstart#install-agent

upvoted 1 times

omermahgoub 1 year, 6 months ago

Stackdriver does not require the Stackdriver Logging agent to be installed in order to collect system logs.
Stackdriver is a cloud monitoring and logging platform that is integrated with Google Cloud Platform (GCP) and is designed to collect, monito and troubleshoot logs from your GCP resources. By default, Stackdriver automatically collects admin activity logs for most GCP services, as as VM system logs. This means that you don't need to install the Stackdriver Logging agent or any other agents in order to collect these logs they are automatically collected and centralized by Stackdriver.

However, if you want to collect logs from other sources that are not automatically collected by Stackdriver (e.g. logs from applications running your VMs, logs from on-premises systems, etc.), you can use the Stackdriver Logging agent to forward these logs to Stackdriver. The agent is lightweight daemon that runs on your VMs or other hosts, and it can be used to collect logs from various sources and forward them to Stackdriver for centralized storage and analysis.

upvoted 6 times

omermahgoub 1 year, 6 months ago

Answer is A

In Google Cloud Platform (GCP), you can use Stackdriver to collect and centralize all admin activity and VM system logs within your projec Stackdriver is a powerful cloud monitoring and logging platform that is integrated with GCP, and it provides a number of features that are specifically designed to help you collect, monitor, and troubleshoot logs from your GCP resources.

One of the key features of Stackdriver is that it automatically collects admin activity logs for most GCP services, as well as VM system logs This means that you don't need to install any agents or configure any additional components to collect these logs - they are automatically collected and centralized by Stackdriver.

To view and analyze your logs in Stackdriver, you can use the Stackdriver Logs Viewer, which provides a powerful interface for searching, filtering, and aggregating your logs. You can also use the Stackdriver Logs API to programmatically access your logs, or use the Stackdrive Logging agent to forward your logs to other log management or analysis tools.

upvoted 6 times

megumin 1 year, 7 months ago

Selected Answer: B

B is ok

upvoted 1 times

DrishaS4 1 year, 10 months ago

Selected Answer: B

https://cloud.google.com/logging/docs/agent/logging/installation#before_you_begin

upvoted 5 times

AzureDP900 1 year, 8 months ago

Thank you for sharing the link, B is right

upvoted 1 times

panqueca 2 years ago

Selected Answer: B

it's B

upvoted 2 times

haroldbenites 2 years, 6 months ago

Go for B.

upvoted 2 times

vincy2202 2 years, 6 months ago

B is the correct answer.

upvoted 2 times

MaxNRG 2 years, 7 months ago

B – stackdriver automatically collects admin activity logs for most services. Stackdriver Logging Agenct must be installed on each instance to collect system logs.
Read more about Logging Agent. https://cloud.google.com/logging/docs/agent/
Logging agent streams logs from 3rd party apps and systems SW (syslog on Linux) to Logging. It is best practice to run the Logging agent on your VM instances. It runs on Linux and Windows.
Cloud Audit Logs says that Admin Activity audit logs are always enabled.

upvoted 3 times

unnikrisb 2 years, 8 months ago

Agree with B

upvoted 1 times

Question #90 *Topic 1*

You have an App Engine application that needs to be updated. You want to test the update with production traffic before replacing the current application version.
What should you do?

A. Deploy the update using the Instance Group Updater to create a partial rollout, which allows for canary testing.

B. Deploy the update as a new version in the App Engine application, and split traffic between the new and current versions.

C. Deploy the update in a new VPC, and use Google's global HTTP load balancing to split traffic between the update and current applications.

D. Deploy the update as a new App Engine application, and use Google's global HTTP load balancing to split traffic between the new and current applications.

KouShikyou Highly Voted 3 years, 8 months ago

I think B is correct. Because GAE supports service version control and A/B test.
Is my understanding correct?

upvoted 60 times

kumarp6 2 years, 7 months ago

Yes, B is correct

upvoted 5 times

nitinz 2 years, 3 months ago

Only B works.

upvoted 4 times

ADVIT Highly Voted 3 years, 4 months ago

Only one App Engine application can be created per Project.
So it's B.

upvoted 15 times

omermahgoub Most Recent 6 months ago

B. Deploy the update as a new version in the App Engine application, and split traffic between the new and current versions.

To test an update to an App Engine application with production traffic before replacing the current version, you can deploy the update as a ne version in the App Engine application and split traffic between the new and current versions. This is known as a "blue-green" deployment, anc allows you to test the new version with a portion of production traffic while the current version is still serving the remainder of traffic.

To split traffic between the new and current versions, you can use the App Engine traffic splitting feature. This feature allows you to specify th percentage of traffic that should be sent to each version, and it can be used to gradually ramp up traffic to the new version over time. This allo you to test the new version with a small portion of traffic initially, and gradually increase the traffic as you become more confident in the updat

upvoted 11 times

omermahgoub 6 months ago

Other options, such as deploying the update in a new VPC or as a new App Engine application, are not recommended for testing updates production traffic, as they can be more complex and may require additional steps to set up.

upvoted 3 times

TonytheTiger 6 months, 2 weeks ago

Answer B : You can use traffic splitting to specify a percentage distribution of traffic across two or more of the versions within a service. Splitt traffic allows you to conduct A/B testing between your versions and provides control over the pace when rolling out features.
Traffic splitting is applied to URLs that do not explicitly target a version. For example, the following URLs split traffic because they target all th available versions within the specified service:
https://cloud.google.com/appengine/docs/standard/splitting-traffic

upvoted 3 times

megumin 7 months, 1 week ago

Selected Answer: B

B is ok

upvoted 2 times

AzureDP900 8 months ago

B is right , Option D is just to confuse you.
Deploy the update as a new version in the App Engine application, and split traffic between the new and current versions.

upvoted 2 times

DrishaS4 10 months, 2 weeks ago

Selected Answer: B

Versioning is supported in App Engine.

upvoted 2 times

ghadxx 1 year, 4 months ago

Selected Answer: B

Versioning is supported in App Engine.

upvoted 2 times

haroldbenites 1 year, 6 months ago

Go for D,
The option B don´t say with wich service will split the traffic.
The option D gives more datail and makes sense.

upvoted 1 times

ale_brd_111 7 months ago

No mate, only one app engine per project can be deployed, you can have multiple version on the same app tho. D is to confuse you. B is t only feasible answer in here.

upvoted 4 times

vincy2202 1 year, 6 months ago

B is the correct answer

upvoted 1 times

robotgeek 1 year, 7 months ago

A is not because "Instance Group Updater " is only for Computer Engine MIG

upvoted 1 times

MaxNRG 1 year, 7 months ago

B – Deploy the update as a new version in AppEngine app, and split traffic between the new and current versions.
Traffic Splitting is feature of AppEngine for A/B testing.
https://cloud.google.com/appengine/docs/standard/python/splitting-traffic

upvoted 6 times

[Removed] 1 year, 8 months ago

B is correct. App Engine supports versioning.

upvoted 1 times

unnikrisb 1 year, 8 months ago

B is correct... Canary Testing -> Traffic Splitting

upvoted 1 times

victory108 2 years, 1 month ago

B. Deploy the update as a new version in the App Engine application, and split traffic between the new and current versions

upvoted 3 times

un 2 years, 1 month ago

B is the answer

upvoted 1 times

getzsagar 2 years, 2 months ago

Answer - B
Configure how much traffic the version that you just deployed should receive.

By default, the initial version that you deploy to your App Engine application is automatically configured to receive 100% of traffic. However, a
subsequent versions that you deploy to that same App Engine application must be manually configured, otherwise they receive no traffic.

For details about how to configure traffic for your versions, see Migrating and Splitting Traffic.
https://cloud.google.com/appengine/docs/admin-api/migrating-splitting-traffic

upvoted 3 times

Question #91 *Topic 1*

All Compute Engine instances in your VPC should be able to connect to an Active Directory server on specific ports. Any other traffic emerging from your instances is not allowed. You want to enforce this using VPC firewall rules.
How should you configure the firewall rules?

A. Create an egress rule with priority 1000 to deny all traffic for all instances. Create another egress rule with priority 100 to allow the Active Directory traffic for all instances.

B. Create an egress rule with priority 100 to deny all traffic for all instances. Create another egress rule with priority 1000 to allow the Active Directory traffic for all instances.

C. Create an egress rule with priority 1000 to allow the Active Directory traffic. Rely on the implied deny egress rule with priority 100 to block all traffic for all instances.

D. Create an egress rule with priority 100 to allow the Active Directory traffic. Rely on the implied deny egress rule with priority 1000 to block all traffic for all instances.

wk Highly Voted 4 years, 8 months ago

Should be A, there is no implied deny egress but only implied allow egress

https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules

Every VPC network has two implied firewall rules. These rules exist, but are not shown in the Cloud Console:

The implied allow egress rule: An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by GCP. Outbound access may be restricted by a higher priority firewall rule Internet access is allowed if no other firewall rules deny outbound traffic and if the instance has an external IP address or uses a NAT instance Refer to Internet access requirements for more details.

The implied deny ingress rule: An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming traffic to them. Incoming access may be allowed by a higher priority rule. Note that the default network includ some additional rules that override this one, allowing certain types of incoming traffic.

upvoted 92 times

nitinz 3 years, 3 months ago

It is A, rest all do not make sense. If you think of any other option then go back and read about firewalls. Seriously you are not ready for thi exam.

upvoted 2 times

zr79 1 year, 8 months ago

thank you

upvoted 1 times

kumarp6 3 years, 7 months ago

B is correct...

upvoted 2 times

p4 3 years, 7 months ago

from a book:
"Firewall rules control network traffic by blocking or allowing traffic into (ingress) or out of (egress) a network. Two implied firewall rules are defined with VPCs: one blocks all incoming traffic, and the other allows all outgoing traffic. You can change this behavior
Virtual Private Clouds 115
116 Chapter 6 ■ Designing Networks
by defining firewall rules with higher priority. Firewall rules have a priority specified by an integer from 0 to 65535, with 0 being the highest priority and 65535 being the lowest."

so this confirms A

upvoted 13 times

SSS987 5 months ago

Good summary. To the point!

upvoted 1 times

MeasService Highly Voted 4 years, 8 months ago

Agree Correct is A. There is no implied deny egress only deny ingress rule

upvoted 10 times

MyPractice 4 years, 5 months ago

Agree with A . only Implied allow egress rule (or) Implied deny ingress rule.
There is No "Implied deny egress rule" which rules out C & D

upvoted 3 times

ManishKS Most Recent 10 months, 3 weeks ago

B. Create an egress rule with priority 100 to deny all traffic for all instances. Create another egress rule with priority 1000 to allow the Active Directory traffic for all instances.

This option creates a deny all rule with a lower priority and an allow rule with a higher priority.

This option will work as intended, as the Active Directory traffic will be allowed and all other outbound traffic will be blocked.

upvoted 2 times

Emmarof 1 year, 3 months ago

The answer to this question is A.

Explanation:
To enforce the requirement that all Compute Engine instances in your VPC should be able to connect to an Active Directory server on specific ports while blocking any other traffic emerging from instances, the following two egress rules should be created:

Create an egress rule with priority 1000 to deny all traffic for all instances.
Create another egress rule with priority 100 to allow the Active Directory traffic for all instances.
In this configuration, the rule that allows the AD traffic has a lower priority number than the rule that denies all other traffic. Therefore, this rule should be evaluated first.

upvoted 2 times

Deb2293 1 year, 3 months ago

Selected Answer: A

It should be A.
It cannot be D as The Implied allow egress rule, with its action of "allow", allows all traffic out to the 0.0. 0.0/0 destination, which basically me everywhere. The priority of the implied allow egress rule is the lowest possible, 65535. The implied deny ingress rule, with an action of "deny" blocks all incoming connections.

upvoted 1 times

8d31d36 1 year, 4 months ago

The correct answer is B.

To enforce that all Compute Engine instances in a VPC can connect to an Active Directory server on specific ports while blocking any other traffic, you should create an egress rule with a high priority (lower numerical value) to deny all traffic from all instances, and another egress rul with a lower priority (higher numerical value) to allow traffic to the Active Directory server on the specific ports.

Option B creates the necessary egress rules in the correct order: a deny-all rule with a high priority (100), followed by an allow rule for the Acti Directory traffic with a lower priority (1000). This way, traffic to the Active Directory server is allowed, but all other traffic is denied.

upvoted 1 times

megumin 1 year, 7 months ago

Selected Answer: A

A is ok

upvoted 1 times

AzureDP900 1 year, 8 months ago

It is pretty straight forward question, It this case priority low should be allow and high priority rules deny all requests. A is right

upvoted 2 times

DrishaS4 1 year, 10 months ago

Selected Answer: A

https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

upvoted 1 times

mv2000 1 year, 11 months ago

06/30/2022 Exam question.

upvoted 6 times

> **moiradavis** 1 year, 11 months ago
>
> Oh, really? I got this question on my exam 2 years ago, I did not expect to repeat this kind of questions in the current exam.
>
> upvoted 1 times

Baumster 2 years, 3 months ago

OT: why is there no way to mark questions for review/repeat later on?

upvoted 1 times

haroldbenites 2 years, 6 months ago

Go for A.
While the priority is higher, the egress rule is more restricted.
While the priority is higher, the ingress rule is more free.

upvoted 1 times

vincy2202 2 years, 6 months ago

Selected Answer: A

A is correct answer

upvoted 1 times

vchrist 2 years, 6 months ago

Selected Answer: A

to understand rules priority:
https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

upvoted 1 times

nqthien041292 2 years, 6 months ago

Selected Answer: A

Vote A

upvoted 1 times

MaxNRG 2 years, 7 months ago

A – create an egress rule with priority 1000 to deny all traffic for all instances. Create another egress rule with priority 100 to allow the Active Directory traffic for all instances.
Default Firewall rules (aka implied rules) are following:
1) Egress traffic is allowed to all IP/ports.
2) Ingress traffic is disabled completely.
Both these rules have lowest priority (65535) and cannot be removed.
https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules

upvoted 2 times

victory108 3 years, 1 month ago

A. Create an egress rule with priority 1000 to deny all traffic for all instances. Create another egress rule with priority 100 to allow the Active

Question #92 *Topic 1*

Your customer runs a web service used by e-commerce sites to offer product recommendations to users. The company has begun experimenting with a machine learning model on Google Cloud Platform to improve the quality of results.
What should the customer do to improve their model's results over time?

A. Export Cloud Machine Learning Engine performance metrics from Stackdriver to BigQuery, to be used to analyze the efficiency of the model.

B. Build a roadmap to move the machine learning model training from Cloud GPUs to Cloud TPUs, which offer better results.

C. Monitor Compute Engine announcements for availability of newer CPU architectures, and deploy the model to them as soon as they are available for additional performance.

D. Save a history of recommendations and results of the recommendations in BigQuery, to be used as training data.

ghadxx Highly Voted 👍 1 year, 4 months ago

Selected Answer: D

Model performance is generally based on the volume of its training data input. The more the data, the better the model.

upvoted 19 times

AzureDP900 8 months ago

I agree with you, D is right

upvoted 1 times

Sur_Nikki 1 month, 1 week ago

Yes, correctly said..This is actually a question for Data Engineer role

upvoted 1 times

sgofficial Highly Voted 👍 10 months, 3 weeks ago

Selected Answer: D

A,B,C is defining about the performance of ML but not the result....only the training data will give good ML result/predictions

upvoted 6 times

Deb2293 Most Recent ⏲ 3 months, 2 weeks ago

Selected Answer: D

Best answer is D. Other 3 makes no sense

upvoted 1 times

PST21 4 months ago

Need to improve the model results and not performance .. hence D

upvoted 1 times

surajkrishnamurthy 6 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

DrishaS4 10 months, 2 weeks ago

Selected Answer: D

Model performance is generally based on the volume of its training data input. The more the data, the better the model.

upvoted 3 times

sivre 1 year, 2 months ago

The following insights and recommendations can be exported (to bigquery):
IAM recommender
VM machine type recommender
Managed instance group machine type recommender
Idle PD recommender
Idle VM recommender
Cloud SQL overprovisioned instance recommender
Cloud SQL idle instance recommender
Unattended project recommender
Cloud Run Service Identity recommender
https://cloud.google.com/recommender/docs/bq-export/export-recommendations-to-bq

None of this is correlated with Machine Learning, how can be D? looks more A the answer

upvoted 2 times

kimharsh 1 year, 2 months ago

what we will do with metrics , it won't improve our Machine learning model , D is the closest answer , also it didn't say export it said Save which could be manually moving the data to BQ

upvoted 2 times

Pime13 1 year, 4 months ago

Selected Answer: D

i vote D

upvoted 3 times

victory108 1 year, 5 months ago

D. Save a history of recommendations and results of the recommendations in BigQuery, to be used as training data.

upvoted 2 times

LoveT 1 year, 5 months ago

"training data" is the key in option "D" and that's the answer

upvoted 4 times

vincy2202 1 year, 5 months ago

Selected Answer: D

D seems to be the correct answer

upvoted 1 times

Question #93 *Topic 1*

A development team at your company has created a dockerized HTTPS web application. You need to deploy the application on Google Kubernetes Engine (GKE) and make sure that the application scales automatically.

How should you deploy to GKE?

A. Use the Horizontal Pod Autoscaler and enable cluster autoscaling. Use an Ingress resource to load-balance the HTTPS traffic.

B. Use the Horizontal Pod Autoscaler and enable cluster autoscaling on the Kubernetes cluster. Use a Service resource of type LoadBalancer to load-balance the HTTPS traffic.

C. Enable autoscaling on the Compute Engine instance group. Use an Ingress resource to load-balance the HTTPS traffic.

D. Enable autoscaling on the Compute Engine instance group. Use a Service resource of type LoadBalancer to load-balance the HTTPS traffic.

crypt0 Highly Voted 👍 5 years, 1 month ago

Why not using Ingress? (A)

upvoted 28 times

techalik 4 years ago

I think A is OK:

upvoted 2 times

nitinz 3 years, 9 months ago

It is A, K8s best way to LB is Ingress.

upvoted 5 times

Smart 4 years, 9 months ago

"Ingress is a Kubernetes resource that encapsulates a collection of rules and configuration for routing external HTTP(S) traffic to internal services.

On GKE, Ingress is implemented using Cloud Load Balancing. When you create an Ingress in your cluster, GKE creates an HTTP(S) load balancer and configures it to route traffic to your application."

Are you exposing multiple services through single IP address? Hence, do you need routing your traffic?

Correct answer is B.

upvoted 42 times

Smart 4 years, 9 months ago

My bad, as stated by other, Service doesn't support L7 load balancing. Hence, need to setup ingress resource. Correct answer is A.

upvoted 46 times

tartar 4 years, 4 months ago

B is ok.
https://cloud.google.com/kubernetes-engine/docs/tutorials/hello-app

upvoted 9 times

GopiSivanathan 4 years, 2 months ago

service resource does a NLB using IP address, however, Ingress does HTTP(S) Load balancer. A should be an answer.

upvoted 8 times

jcmoranp Highly Voted 5 years, 1 month ago

Name is service resource, it's B:

https://cloud.google.com/kubernetes-engine/docs/concepts/service?hl=es-419

upvoted 13 times

nareshthumma Most Recent 1 month, 3 weeks ago

Answer A

upvoted 1 times

mstaicu 5 months, 2 weeks ago

Selected Answer: A

A and B both create under the hood a Service of type LoadBalancer with external IP address. However, when it comes to http(s) traffic an ingr is the way to go because of ssl termination and for the routing options.

upvoted 2 times

huuthanhdlv 6 months, 4 weeks ago

Selected Answer: A

C & D is clearly incorrect.

B is incorrect because of this:
"service of type LoadBalancer to load-balance the HTTPS traffic."
GKE Service Load Balancer is L4 Network or Internal Load Balancer, does not support HTTPS traffic.

Thus only A is correct.

upvoted 3 times

hitmax87 7 months ago

Selected Answer: A

The clue is HTTPS traffic. You need L7 stack. It can be achieved only through ingress controller.

upvoted 3 times

nanasenishino 7 months, 1 week ago

B

A. Ingress resource: While Ingress can be used for external load balancing, it often requires additional configuration for HTTPS termination (offloading SSL from your application containers). Additionally, LoadBalancer services typically offer a simpler setup for basic external load balancing without HTTPS termination concerns.
C & D. Compute Engine Instance Group Autoscaling: GKE manages its own nodes separate from Compute Engine instances. Autoscaling on Compute Engine instance group wouldn't manage the Kubernetes pods or nodes effectively in this scenario.

upvoted 1 times

Pime13 10 months, 2 weeks ago

Selected Answer: A

service loadBalancer: https://cloud.google.com/kubernetes-engine/docs/concepts/service-load-balancer
This page provides a general overview of how Google Kubernetes Engine (GKE) creates and manages Google Cloud load balancers when you apply a Kubernetes LoadBalancer Services manifest. It describes the different types of load balancers and how settings like the externalTrafficPolicy and GKE subsetting for L4 internal load balancers determine how the load balancers are configured. -> l4 tcp/udp not ht
Ingress: https://cloud.google.com/kubernetes-engine/docs/concepts/ingress This page provides a general overview of what Ingress for exter Application Load Balancers is and how it works. Google Kubernetes Engine (GKE) provides a built-in and managed Ingress controller called G Ingress. This controller implements Ingress resources as Google Cloud load balancers for HTTP(S) workloads in GKE. -S http(s)

upvoted 3 times

gun123 11 months, 2 weeks ago

Selected Answer: B

B is correct

upvoted 1 times

bandegg 11 months, 2 weeks ago

Selected Answer: A

I'm assuming B is the suggested answer because a the question doesn't state that the application should be available externally. Services all exposing resources internally and to load balancers.

However, it should be A, as the assumption would be a an external web application.

https://cloud.google.com/kubernetes-engine/docs/concepts/service

upvoted 2 times

MahAli 1 year ago

Selected Answer: B

Most if the labs in Google boost skills discuss how to expose the deployment using a load balancer.

upvoted 2 times

AwsSuperTrooper 1 year ago

Selected Answer: A

https://cloud.google.com/kubernetes-engine/docs/concepts/ingress
"This page provides a general overview of what Ingress for external Application Load Balancers is and how it works. Google Kubernetes Engi (GKE) provides a built-in and managed Ingress controller called GKE Ingress. This controller implements Ingress resources as Google Cloud l balancers for HTTP(S) workloads in GKE."

upvoted 2 times

thewalker 1 year, 1 month ago

https://cloud.google.com/kubernetes-engine/docs/concepts/ingress
As there is no mention about the type of the traffic, Internal or external - Going with A - Ingress.

upvoted 1 times

Arun_m_123 1 year, 2 months ago

Selected Answer: B

Option-C and D are straightforwardly wrong

Between A and B : B is the correct answer, because it makes use of loadbalancing the ingress in K8S native style. That is the reason why clus scaling is also done.

This is how it should
External Load Balancing Ingress --> K8S Service of type LoadBalancer --> pods that can autoscale

Directly allowing external loadbalcing ingress to autoscaled Pod, doesn't makes sense to use GKE

upvoted 1 times

someone2011 1 year, 2 months ago

Ingress is Https while Service is TCP/UDP.
https://cloud.google.com/load-balancing/docs/choosing-load-balancer
https://cloud.google.com/kubernetes-engine/docs/concepts/service-networking

upvoted 2 times

heretolearnazure 1 year, 3 months ago

B is correct

upvoted 2 times

willyf1 1 year, 4 months ago

Selected Answer: A

A Is the best choice

upvoted 1 times

Question #94 *Topic 1*

You need to design a solution for global load balancing based on the URL path being requested. You need to ensure operations reliability and end-to-end in- transit encryption based on Google best practices.
What should you do?

A. Create a cross-region load balancer with URL Maps.

B. Create an HTTPS load balancer with URL Maps.

C. Create appropriate instance groups and instances. Configure SSL proxy load balancing.

D. Create a global forwarding rule. Configure SSL proxy load balancing.

victory108 Highly Voted 2 years, 1 month ago

B. Create an HTTPS load balancer with URL maps.

upvoted 14 times

betiy Highly Voted 3 years, 5 months ago

URL paths supported only in HTTP(S) Load balancing
https://cloud.google.com/load-balancing/docs/ssl/#FAQ

upvoted 10 times