EXAM PROFESSIONAL MACHINE LEARNING ENGINEER TOPIC 1 QUESTION 181 DISCUSSI...

Actual exam question from Google's Professional Machine Learning Engineer
Question #: 181
Topic #: 1
[All Professional Machine Learning Engineer Questions]

You work for a bank with strict data governance requirements. You recently implemented a custom model to detect fraudulent transactions. You want your training code to download internal data by using an API endpoint hosted in your project's network. You need the data to be accessed in the most secure way, while mitigating the risk of data exfiltration. What should you do?

A. Enable VPC Service Controls for peerings, and add Vertex AI to a service perimeter.

B. Create a Cloud Run endpoint as a proxy to the data. Use Identity and Access Management (IAM) authentication to secure access to the endpoint from the training job.

C. Configure VPC Peering with Vertex AI, and specify the network of the training job.

D. Download the data to a Cloud Storage bucket before calling the training job.

Show Suggested Answer

by pikachu007 at *Jan. 11, 2024, 11:50 a.m.*

Comments

Type your comment...

Submit

tardigradum 2 months, 1 week ago

Selected Answer: A

VPC Service Controls: This feature allows you to define network boundaries (service perimeters) and control the flow of data between services. By adding Vertex AI to a service perimeter, you can restrict its access to only the necessary resources, including the API endpoint.

With peerings you can enable secure communication between your VPC and the VPC where Vertex AI is running, ensuring data stays within your network boundary.

upvoted 1 times

dija123 3 months, 4 weeks ago

Selected Answer: A

A is correct

upvoted 1 times

peppenapo7 6 months ago

Selected Answer: A

It's literally written in the description of this service: avoid data exfiltration.

upvoted 3 times

fitri001 6 months ago

Selected Answer: B

Security: Cloud Run offers a secure environment to run your proxy code. IAM authentication ensures only authorized training jobs have access to the data endpoint.
Data Minimization: The proxy can potentially filter or transform data before sending it to the training code, reducing the amount of sensitive information exposed.
Network Isolation: The proxy acts as an additional layer of isolation between the training code and the internal data source.

upvoted 2 times

fitri001 6 months ago

A. VPC Service Controls: While VPC Service Controls offer network segmentation, they wouldn't directly address data exfiltration risk from the training code itself.
C. VPC Peering: VPC Peering allows communication between networks but doesn't provide access control mechanisms like IAM.
D. Downloading to Cloud Storage: This approach creates an unnecessary data transfer step and doesn't address the risk of the training code potentially leaking data after download.

upvoted 1 times

pinimichele01 6 months ago

https://cloud.google.com/vpc-service-controls/docs/overview#how-vpc-service-controls-works

upvoted 1 times

pinimichele01 6 months, 1 week ago

Selected Answer: A

To mitigate data exfiltration risks, your organization might also want to ensure secure data exchange across organizational boundaries with fine-grained controls. As an administrator, you might want to ensure the following:

Clients with privileged access don't also have access to partner resources.
Clients with access to sensitive data can only read public data sets but not write to them

upvoted 1 times

Sunny_M 8 months ago

It should be A, VPC service controls can reduce data exfiltration risks.
https://cloud.google.com/vpc-service-controls/docs/overview

upvoted 2 times

guilhermebutzke 8 months, 1 week ago

Selected Answer: B

My Answer B:
Creating a Cloud Run endpoint as a proxy to the data allows you to control access to the internal data through an API endpoint. By using IAM authentication, you can enforce strict access controls, ensuring that only authorized entities (such as your training job) can access the data. This approach helps mitigate the risk of data exfiltration by providing a secure and controlled access point to the internal data.
- Option A: may help control access within Google Cloud Platform services, but it does not directly address securing access to the internal data through an API endpoint.
- Option C: is more about network configurations and does not provide a solution for securely accessing the internal data through an API endpoint.
- Option D: transferring the data to a Cloud Storage bucket, which might introduce additional security risks during the data transfer process.

upvoted 3 times

guilhermebutzke 8 months, 1 week ago

My Answer B:
Creating a Cloud Run endpoint as a proxy to the data allows you to control access to the internal data through an API endpoint. By using Identity and Access Management (IAM) authentication, you can enforce strict access controls, ensuring that only authorized entities (such as your training job) can access the data. This approach helps mitigate the risk of data exfiltration by providing a secure and controlled access point to the internal data.

- Option A: may help control access within Google Cloud Platform services, but it does not directly address securing access to the internal data through an API endpoint.
- Option C: is more about network configurations and does not provide a solution for securely accessing the internal data through an API endpoint.
- Option D: involves transferring the data to a Cloud Storage bucket, which might introduce additional security risks during the data transfer process.

upvoted 3 times

ddogg 8 months, 3 weeks ago

Selected Answer: A

A. https://cloud.google.com/security/vpc-service-controls?hl=en
The first benefit on the official google cloud site is "Mitigate data exfiltration risks"
Here's why:

VPC Service Controls: This powerful tool allows you to restrict the network connectivity of resources within your VPC network. By enabling it for peerings, you can control which services within your project can access specific internal resources.

Service perimeter: Adding Vertex AI to a service perimeter further restricts its access to only approved internal resources, including the API endpoint for your bank's data. This creates a secure zone where your model training can happen without jeopardizing sensitive data.

upvoted 1 times

daidai75 8 months, 3 weeks ago

Selected Answer: A

I will go with A.

upvoted 1 times

pikachu007 9 months, 2 weeks ago

Selected Answer: B

It provides a controlled and secure way to allow the training job to access the necessary data while adhering to strict data governance requirements.

upvoted 1 times

Facebook , Twitter
YouTube , Reddit
Pinterest

We are the biggest and most updated IT certification exam material website.
Using our own resources, we strive to strengthen the IT professionals community for free.