

# Summary

Exit

Question 1:

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

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

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

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

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

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 2:

Your company is using Google Cloud. You have two folders under the Organization: Finance and Shopping. The members of the development team are in a Google Group. The development team group has been assigned the Project Owner role on the Organization. You want to prevent the development team from creating resources in projects in the Finance folder. What should you do?

A. Assign the development team group the Project Viewer role on the Finance folder, and assign the development team group the Project Owner role on the Shopping folder.

B. Assign the development team group only the Project Viewer role on the Finance folder.

C. Assign the development team group the Project Owner role on the Shopping folder, and remove the development team group Project Owner role from the Organization.

D. Assign the development team group only the Project Owner role on the Shopping folder.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 3:

Your company wants to start using Google Cloud resources but wants to retain their on-premises Active Directory domain controller for identity management.What should you do?

A. Use the Admin Directory API to authenticate against the Active Directory domain controller.

B. Use Google Cloud Directory Sync to synchronize Active Directory usernames with cloud identities and configure SAML SSO.

C. Use Cloud Identity-Aware Proxy configured to use the on-premises Active Directory domain controller as an identity provider.

D. Use Compute Engine to create an Active Directory (AD) domain controller that is a replica of the on-premises AD domain controller using Google Cloud Directory Sync.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 4:

Your organization has decided to restrict the use of external IP addresses on instances to only approved instances. You want to enforce this requirement across all of your Virtual Private Clouds (VPCs). What should you do?

A. Remove the default route on all VPCs. Move all approved instances into a new subnet that has a default route to an internet gateway.

B. Create a new VPC in custom mode. Create a new subnet for the approved instances, and set a default route to the internet gateway on this new subnet.

C. Implement a Cloud NAT solution to remove the need for external IP addresses entirely.

D. Set an Organization Policy with a constraint on constraints/compute.vmExternallpAccess. List the approved instances in the allowedValues list.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 5:

You are designing a Data Warehouse on Google Cloud and want to store sensitive data in BigQuery. Your company requires you to generate encryption keys outside of Google Cloud. You need to implement a solution. What should you do?

A. Generate a new key in Cloud Key Management Service (Cloud KMS). Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a BigQuery dataset.

B. Generate a new key in Cloud Key Management Service (Cloud KMS). Create a dataset in BigQuery using the customer-managed key option and select the created key

C. Import a key in Cloud KMS. Store all data in Cloud Storage using the customer-managed key option and select the created key. Set up a Dataflow pipeline to decrypt the data and to store it in a new BigQuery dataset.

D. Import a key in Cloud KMS. Create a dataset in BigQuery using the customer-supplied key option and select the created key.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 6:

Your company has a support ticketing solution that uses App Engine Standard. The project that contains the App Engine application already has a Virtual Private Cloud(VPC) network fully connected to the company's on-premises environment through a Cloud VPN tunnel. You want to enable App Engine application to communicate with a database that is running in the company's on-premises environment. What should you do?

A. Configure private services access

B. Configure private Google access for on-premises hosts only

C. Configure serverless VPC access

D. Configure private Google access

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 7:

You have deployed several instances on Compute Engine. As a security requirement, instances cannot have a public IP address. There is no VPN connection between Google Cloud and your office, and you need to connect via SSH into a specific machine without violating the security requirements. What should you do?

A. Configure Cloud NAT on the subnet where the instance is hosted. Create an SSH connection to the Cloud NAT IP address to reach the instance.

B. Add all instances to an unmanaged instance group. Configure TCP Proxy Load Balancing with the instance group as a backend. Connect to the instance using the TCP Proxy IP.

C. Configure Identity-Aware Proxy (IAP) for the instance and ensure that you have the role of IAP-secured Tunnel User. Use the gcloud command line tool to ssh into the instance.

D. Create a bastion host in the network to SSH into the bastion host from your office location. From the bastion host, SSH into the desired instance.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Question 8:

Your company has sensitive data in Cloud Storage buckets. Data analysts have Identity Access Management (IAM) permissions to read the buckets. You want to prevent data analysts from retrieving the data in the buckets from outside the office network. What should you do?

A. 1. Create a VPC Service Controls perimeter that includes the projects with the buckets. 2. Create an access level with the CIDR of the office network.

B. 1. Create a firewall rule for all instances in the Virtual Private Cloud (VPC) network for source range. 2. Use the Classless Inter-domain Routing (CIDR) of the office network.

C. 1. Create a Cloud Function to remove IAM permissions from the buckets, and another Cloud Function to add IAM permissions to the buckets.2. Schedule the Cloud Functions with Cloud Scheduler to add permissions at the start of business and remove permissions at the end of business.

D. 1. Create a Cloud VPN to the office network. 2. Configure Private Google Access for on-premises hosts.

Type : SINGLE SELECTION

Answered By

1

Correct Answers Given By

1

Percentage

100 %

A

B

C

D

Home

Features


Pricing


Blogs


Contact Us

Privacy Policy

Follow us







Copyright © 2017 - 2021 TapOn Tech Solutions Pvt Ltd - All rights reserved