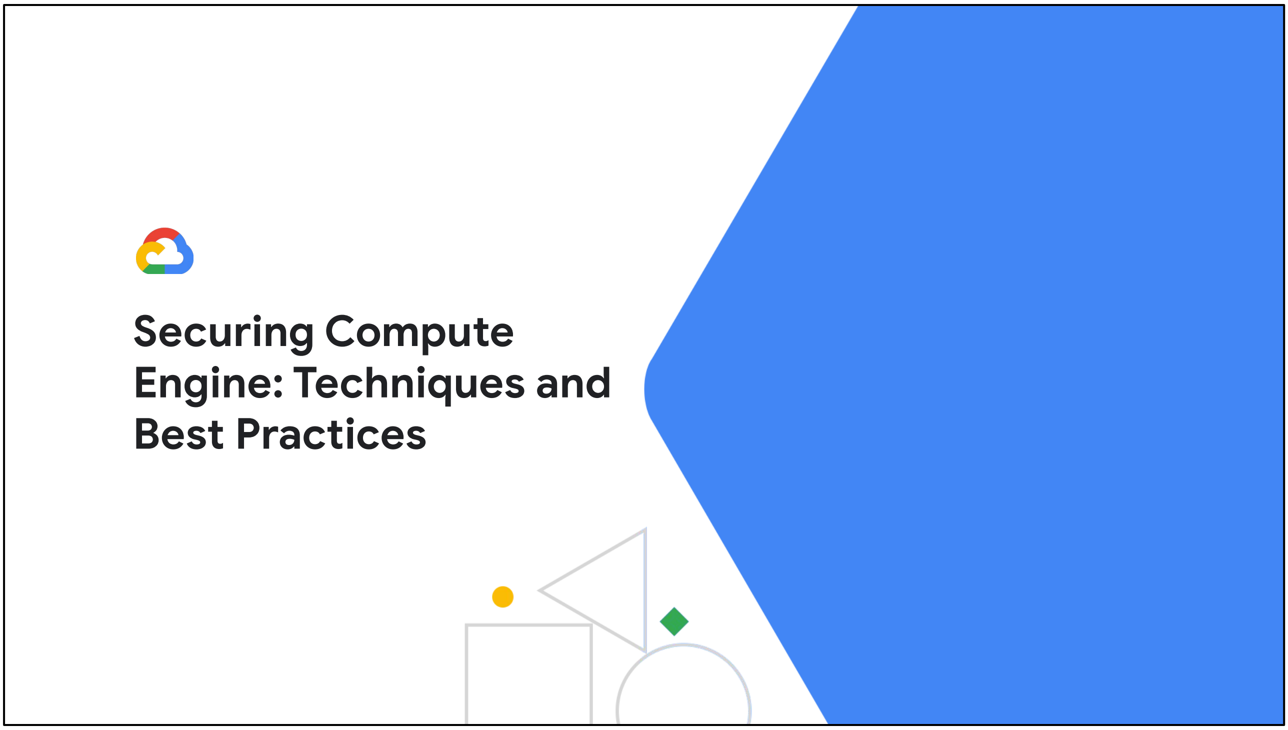
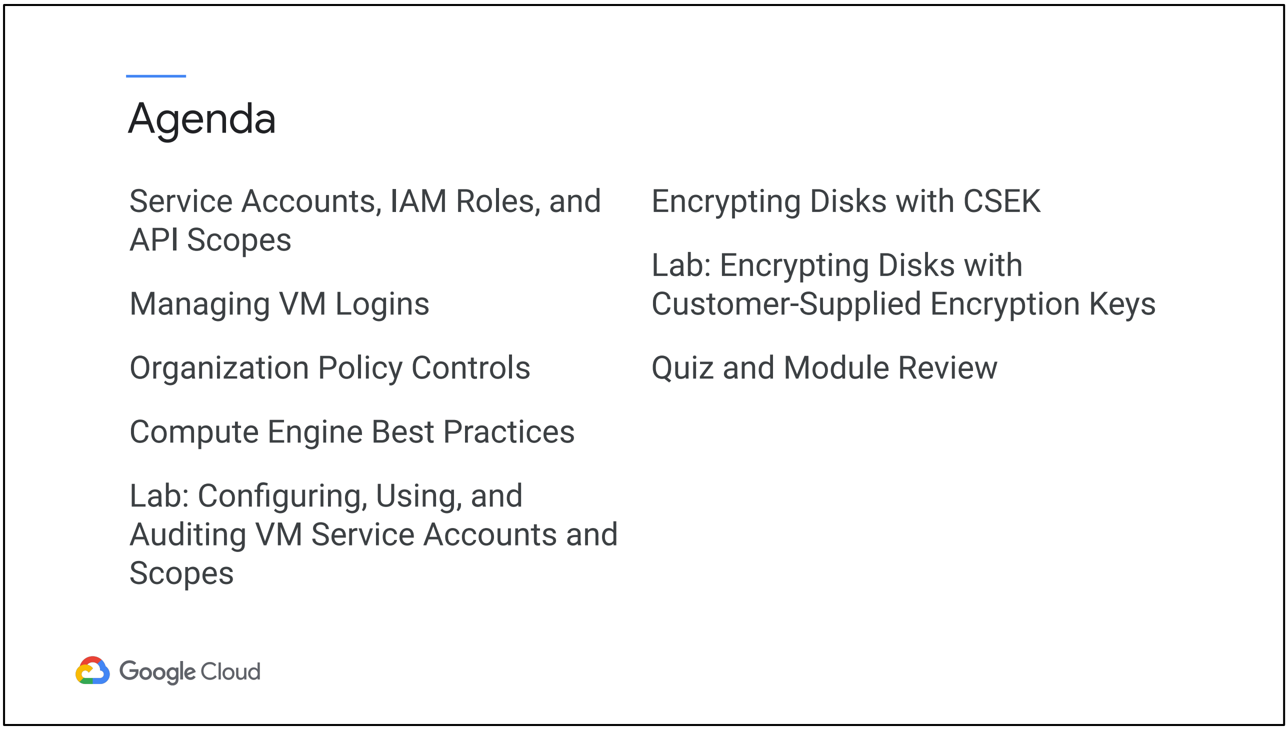


# Securing Compute Engine: Techniques and Best Practices

Welcome to Securing Compute Engine: Techniques and Best Practices module.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review

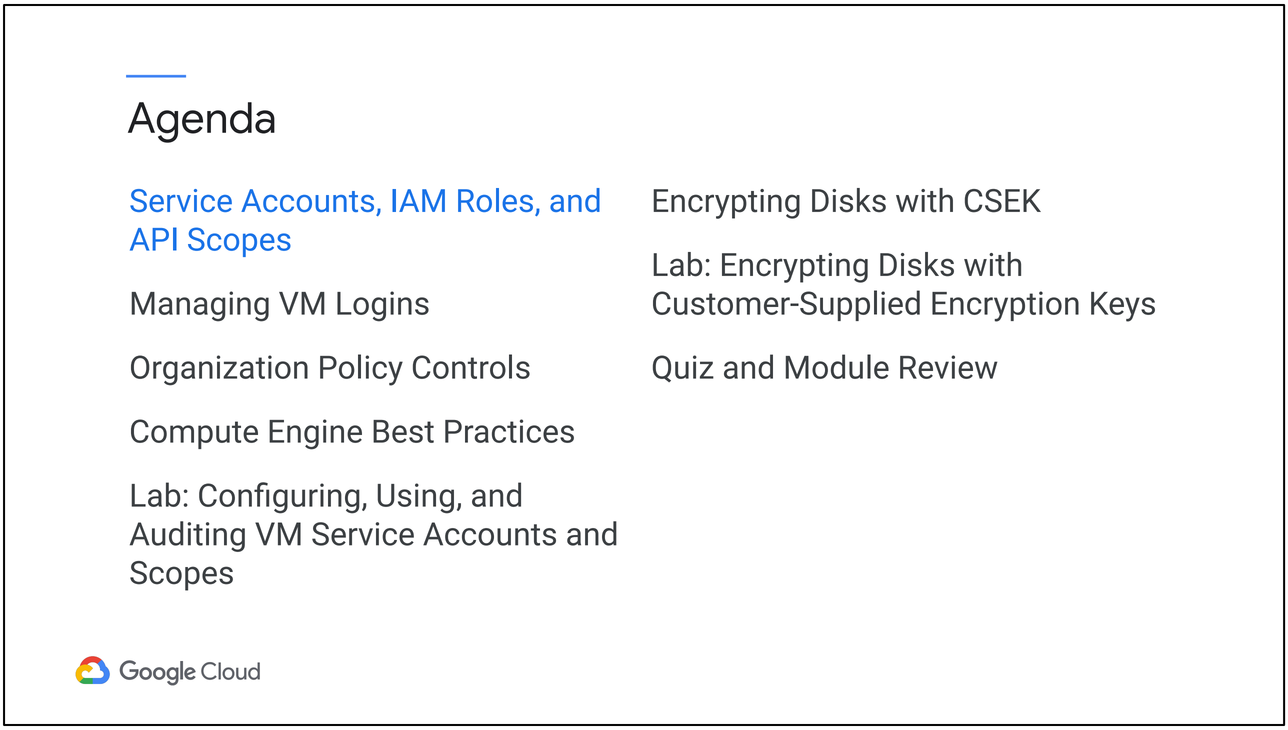
Compute Engine security encompasses many different topics.

In this module we will start with a discussion of service accounts, IAM roles and API scopes as they apply to compute engine.

We will also discuss managing VM logins and using shielded VMs, and how to use organization policies to set constraints that apply to all resources in your organization's hierarchy.

Next, we will review compute engine best practices to give you some tips for securing Compute Engine. You will also have an opportunity to configure and use service accounts as well as scopes in a lab.

Lastly, we will cover encrypting persistent disks with Customer Supplied Encryption keys and let you practice encrypting disks with a lab.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

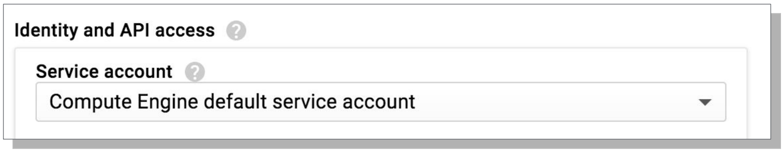
Quiz and Module Review

Google Cloud

OK, let’s get started with Service accounts, IAM roles and API scopes.

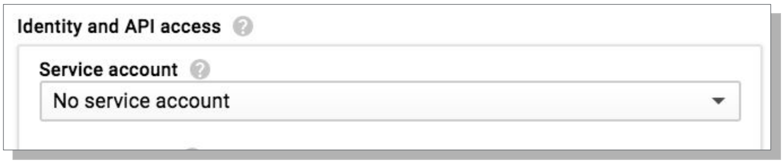
# Compute Engine Identity and API access

Compute Engine virtual machines can run under a particular service account - or not be assigned any service account.



Identity and API access

Service account: Compute Engine default service account



Identity and API access

Service account: No service account

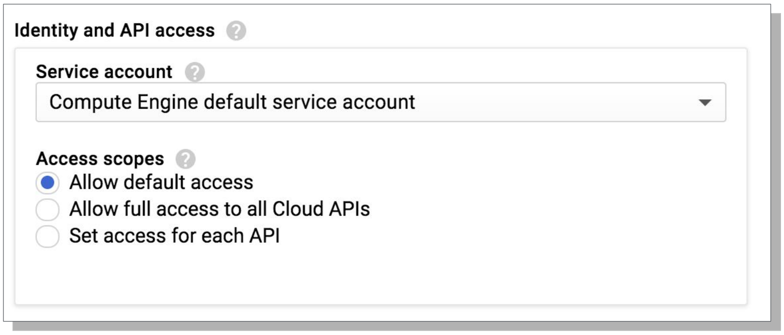
Google Cloud

A “service account” is an identity that a resource such as a VM instance can use to run API requests on your behalf. When launching a virtual machine in Compute Engine, a service account can be associated directly to that VM. When a service account is specified, the VM authenticates using the identity of that service account when making calls to the Google APIs.

It also possible to specify no service account association. In that case, API requests running on the VM will not assume the service account identity by default and would therefore need to be manually configured.

# Default service account

- Created automatically when the Compute Engine is enabled.
- Assigned the Project Editor role.
- Used by default when creating a VM.



**Identity and API access**

**Service account**

Compute Engine default service account

**Access scopes**

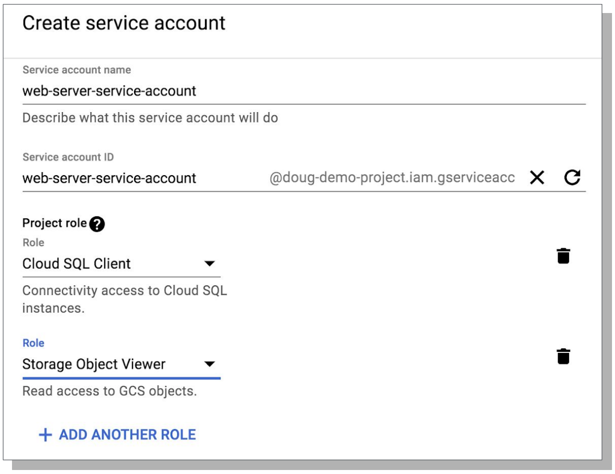
● Allow default access

○ Allow full access to all Cloud APIs

○ Set access for each API

Every project has a default service account that is automatically created when Compute Engine is first enabled for the project. In this instance the service account is assigned the role of project editor and is used by default when launching VMs.

# Create service accounts using Cloud IAM



Create service account

Service account name
web-server-service-account

Describe what this service account will do

Service account ID
web-server-service-account @doug-demo-project.iam.gserviceacc

Project role

Role
Cloud SQL Client

Connectivity access to Cloud SQL instances.

Role
Storage Object Viewer

Read access to GCS objects.

Google Cloud

You can also create and manage your own service accounts using Cloud Identity and Access Management. These user-managed service accounts are granted “necessary” permissions just like any member in Cloud IAM - by assigning roles.

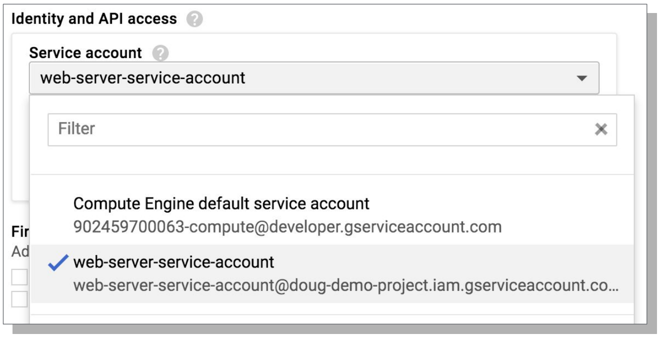
This gives you full control over exactly which permissions the service account will have.

If you do not grant any roles, the service account will not have any access to services.

# Assign custom service accounts to machines

Access to APIs controlled by the roles, not by scopes:

- Assign 1 or more roles to those service accounts.
- Scopes are only used by default service accounts.



Identity and API access

Service account: web-server-service-account

Filter

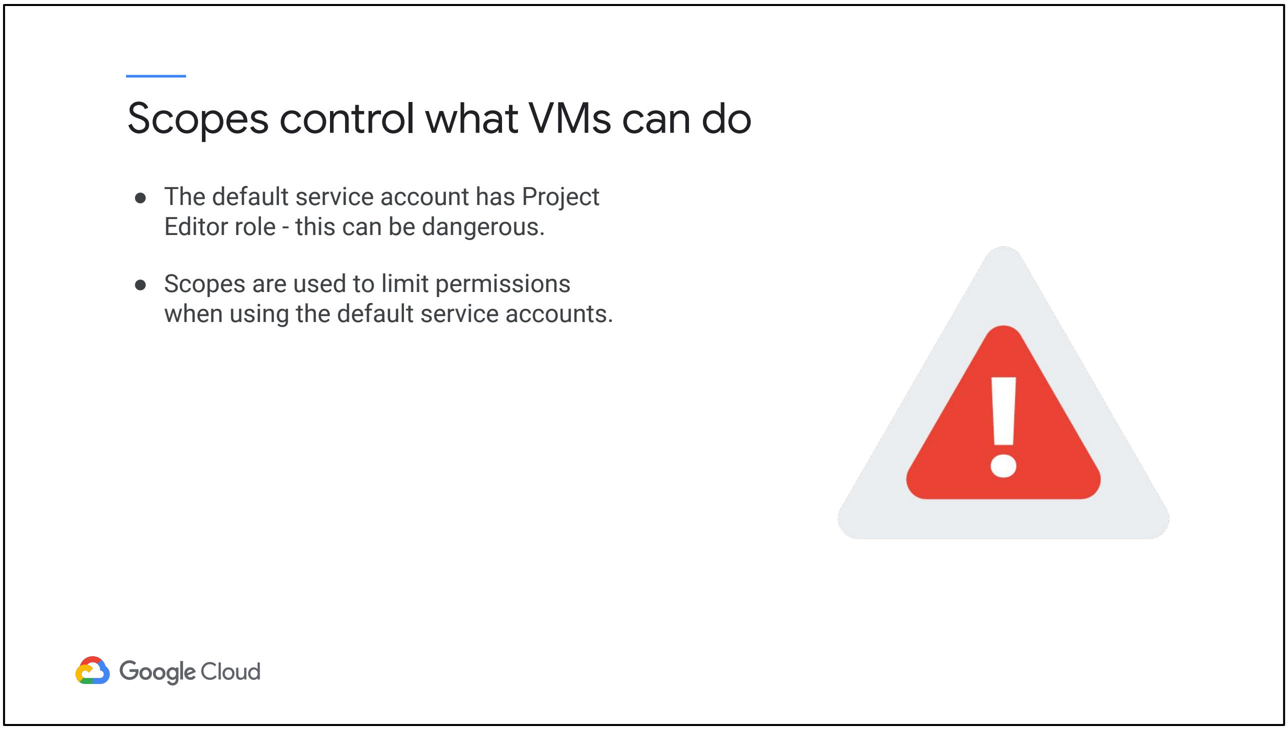
Compute Engine default service account
902459700063-compute@developer.gserviceaccount.com

✓ web-server-service-account
web-server-service-account@doug-demo-project.iam.gserviceaccount.co...

Google Cloud

When you create a new service account, it can be assigned to instances in exactly the same way as the default service account. The only difference is user-managed service accounts do not use the access scope concept.

Instead, permissions are controlled through the IAM roles assigned to the account. Applications running on instances associated with the service account can make authenticated requests to other Google APIs using the service account identity.



## Scopes control what VMs can do

- The default service account has Project Editor role - this can be dangerous.
- Scopes are used to limit permissions when using the default service accounts.

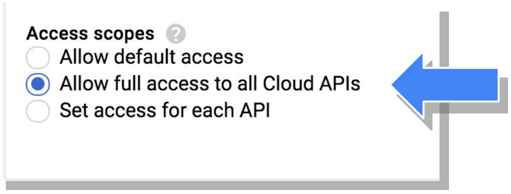
Google Cloud

The IAM Project Editor role contains permissions to create and delete resources for most Google Cloud services and can be dangerous to use as-is. Access scopes provide the ability to limit what permissions are allowed when using the default service account containing this role.

Before the existence of IAM roles, access scopes were the only mechanism for granting permissions to service accounts. Although they are not the primary way of granting permissions now, you must still configure access scopes when initiating an instance to run under the default service account.

It is important to remember that access scopes only apply on a per-instance basis. You set access scopes when creating an instance and the access scopes persists only for the life of the instance.

# Allow default access scope



Access scopes

○ Allow default access

● Allow full access to all Cloud APIs

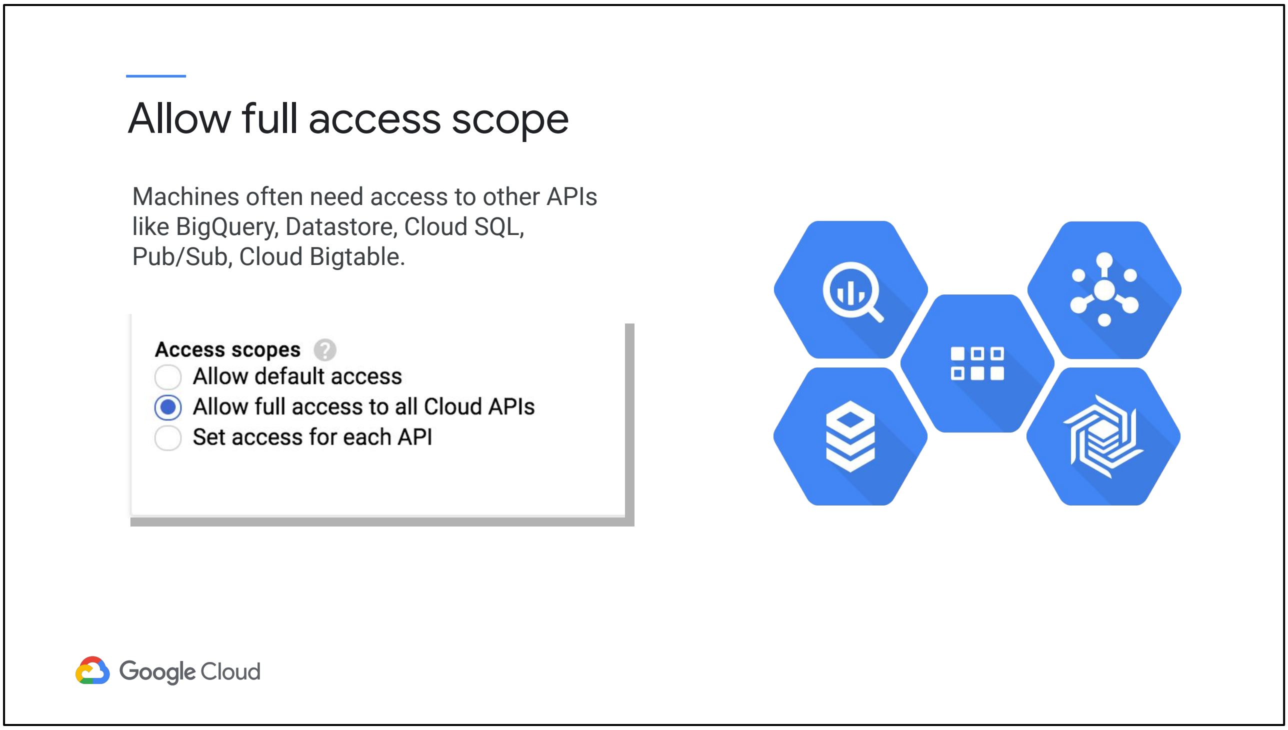
○ Set access for each API

The default access scope is very limited:

- Read-only access to storage
- Access to Cloud Logging and monitoring

Google Cloud

There are several options when setting access scopes. The first is called “Allow default access”. The default access scope is actually very narrow and allows read-only access to storage, as well as access to Cloud Logging and Monitoring. Other API access using the default service account will obviously be restricted.



## Allow full access scope

Machines often need access to other APIs like BigQuery, Datastore, Cloud SQL, Pub/Sub, Cloud Bigtable.

Access scopes

○ Allow default access

● Allow full access to all Cloud APIs

○ Set access for each API

Google Cloud

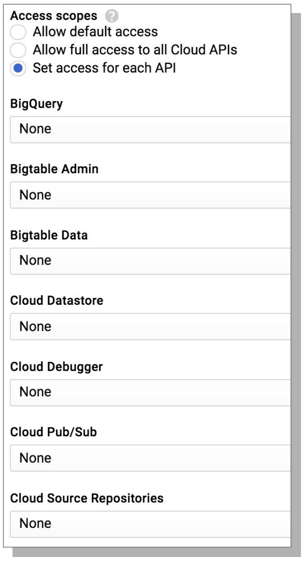
Consider the situation where your VMs need access to other APIs, such as BigQuery, Datastore, Cloud SQL, Pub/Sub, or Cloud Bigtable?  The default access scope does not include these APIs and would cause a security error when accessing these, or other, APIs not included in scope.

The next access scope option is to “allow full access”. This grants full access to all Cloud APIs. Choosing this option would violate the Principle of Least Privilege, and therefore is definitely NOT best practice!

# Set access for each API with scopes

Can grant access to only to the APIs required by the programs running on the machine:

- Choose only the scopes required
- by your application.
- Better practice than granting full access.



Access scopes

○ Allow default access
○ Allow full access to all Cloud APIs
● Set access for each API

BigQuery: None

Bigtable Admin: None

Bigtable Data: None

Cloud Datastore: None

Cloud Debugger: None

Cloud Pub/Sub: None

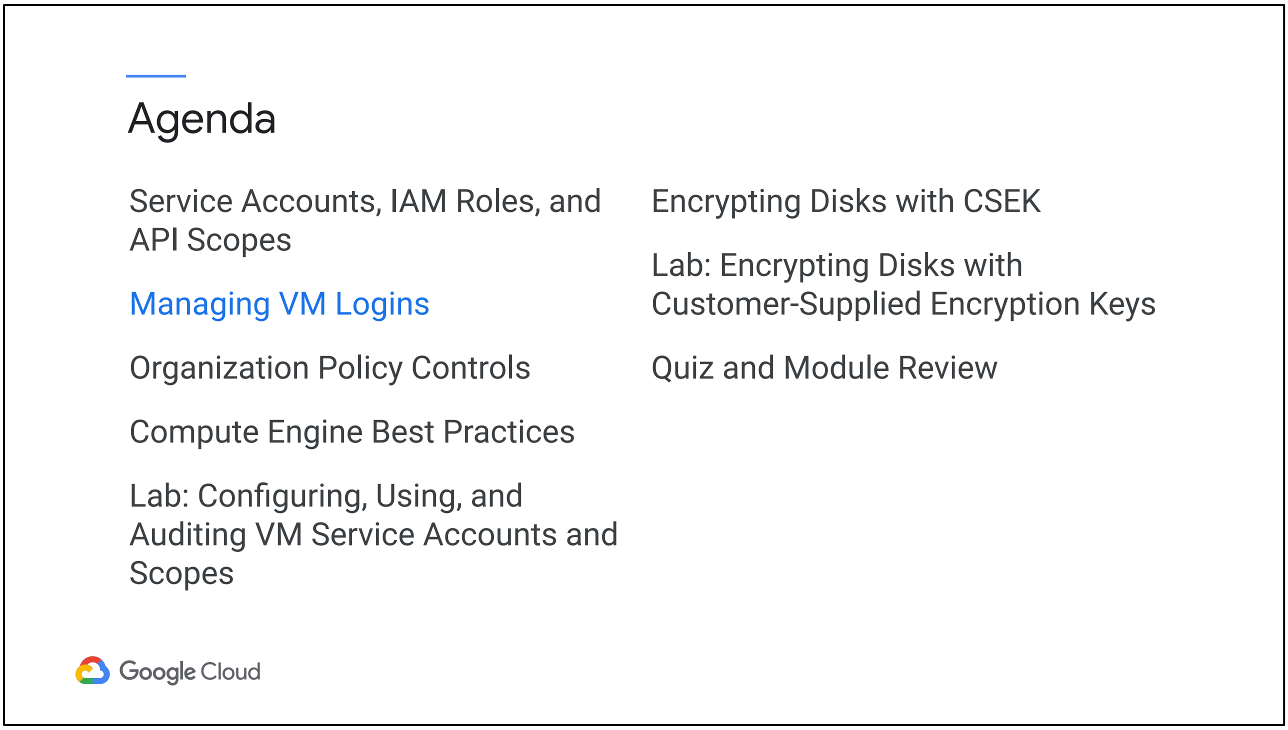
Cloud Source Repositories: None

Google Cloud

There is another option, and that is to set the each API access required individually. This will allow you to grant access to only the APIs required by the programs running on the VM.

You can choose only the scopes required by your application.

If you are using the default service account, then this is a much better practice than granting full API access.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

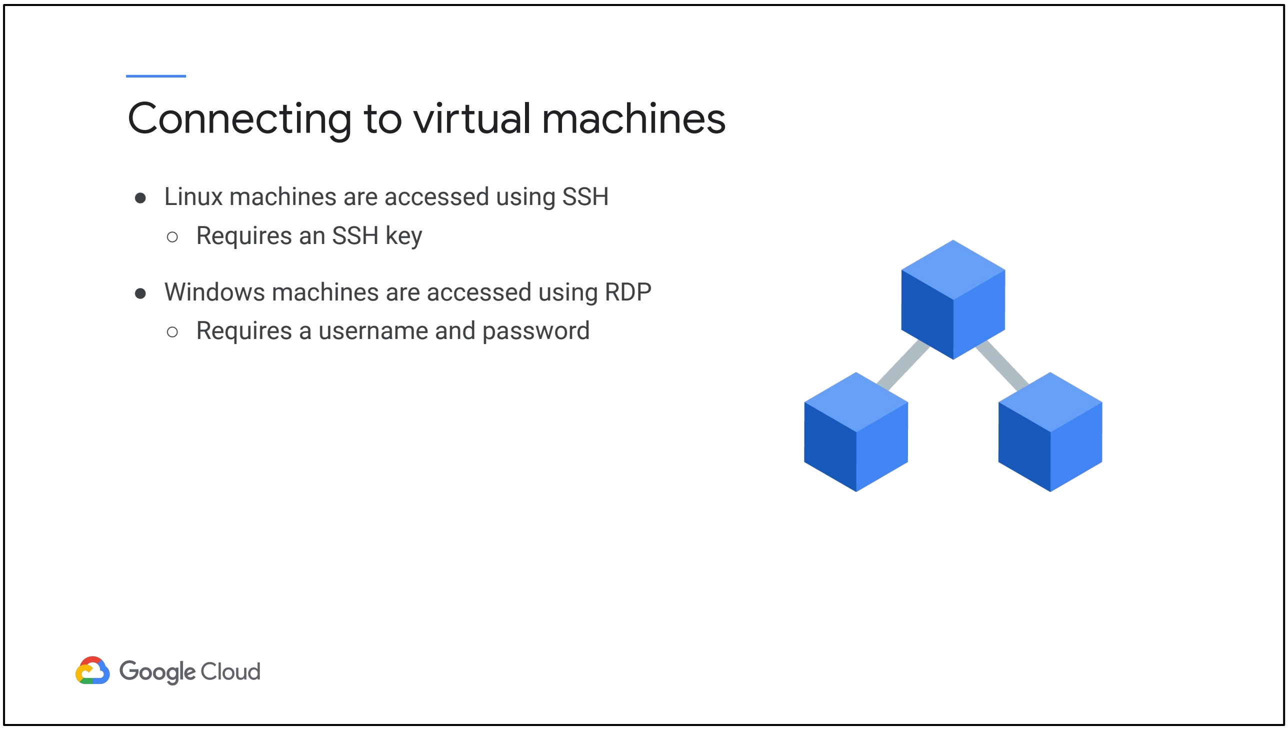
Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review

Google Cloud

In this section, we will discuss various options for logging into and securing VMs.



## Connecting to virtual machines

- Linux machines are accessed using SSH
    - Requires an SSH key
- Windows machines are accessed using RDP
    - Requires a username and password

Connecting to virtual machines in the cloud is generally very easy.

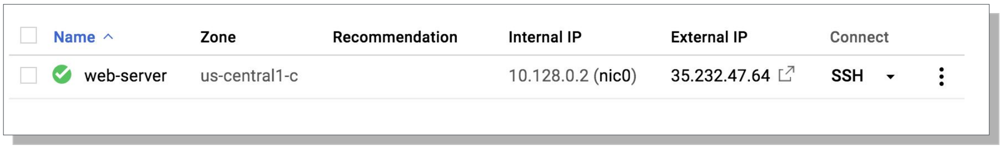
By default, Linux instances on Google Cloud are accessed with Secure Shell (i.e SSH) and require a username and an SSH key for authentication. Password authentication is disabled by default.

Window instances are accessed with Remote Desktop Protocol (i.e., RDP) and require a username and password to authenticate.

# SSH from the Cloud Console

Click the SSH control:

- Keys are automatically generated.
- SSH terminal session opens in a new browser tab.
- Requires the VM to have an external IP.

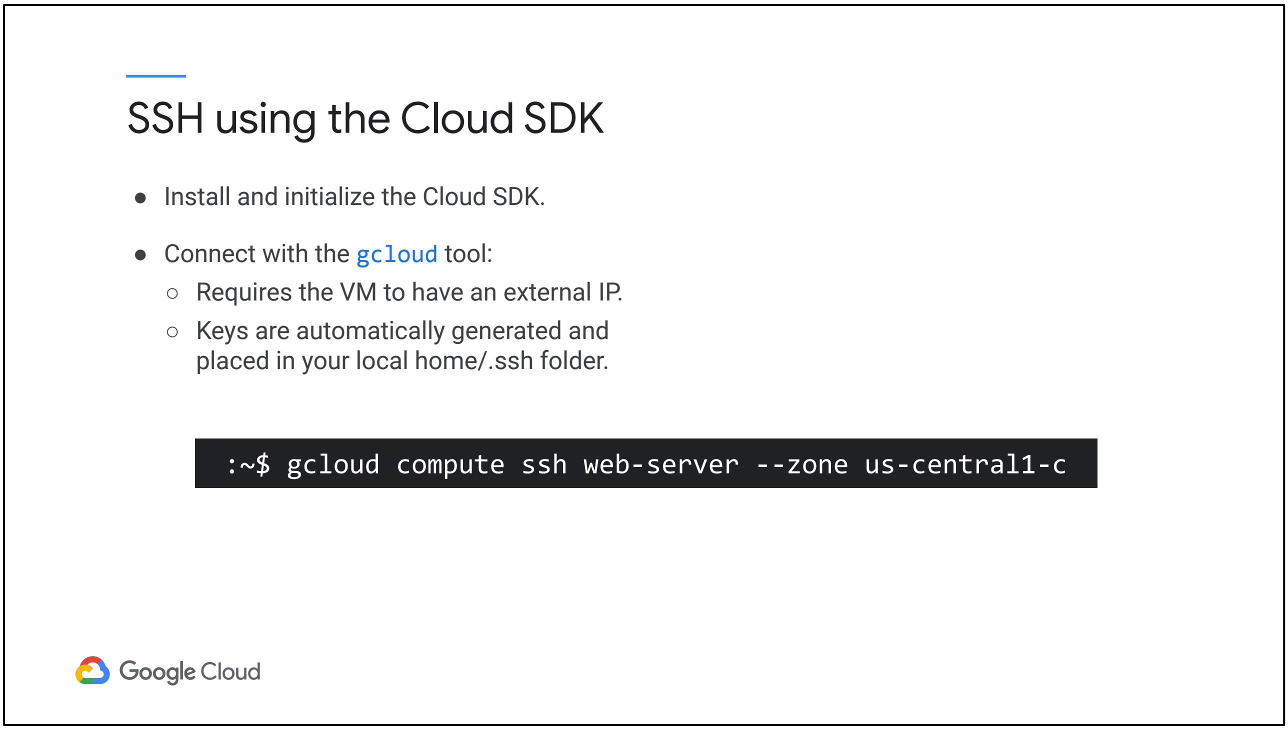


| □ | Name ^ | Zone | Recommendation | Internal IP | External IP | Connect | |
|---|---|---|---|---|---|---|---|
| □ | ✓ web-server | us-central1-c | | 10.128.0.2 (nic0) | 35.232.47.64 | SSH ▾ | ⋮ |

When connecting to Linux instances, the Cloud Console provides a built-in SSH access mechanism. To connect to an instance, simply click the SSH button in the console and a SSH terminal session will open in a new browser window.

As part of the connection process, the browser window performs an HTTPS connection to a Google Web server, which in turn creates an SSH connection to the instance. SSH keys are automatically generated and propagated to the instance during this process.

For this to work, the VM must have a public IP address and a firewall rule to allow TCP port 22 traffic from Google's servers.



## SSH using the Cloud SDK

- Install and initialize the Cloud SDK.
- Connect with the `gcloud` tool:
  - Requires the VM to have an external IP.
  - Keys are automatically generated and placed in your local home/.ssh folder.

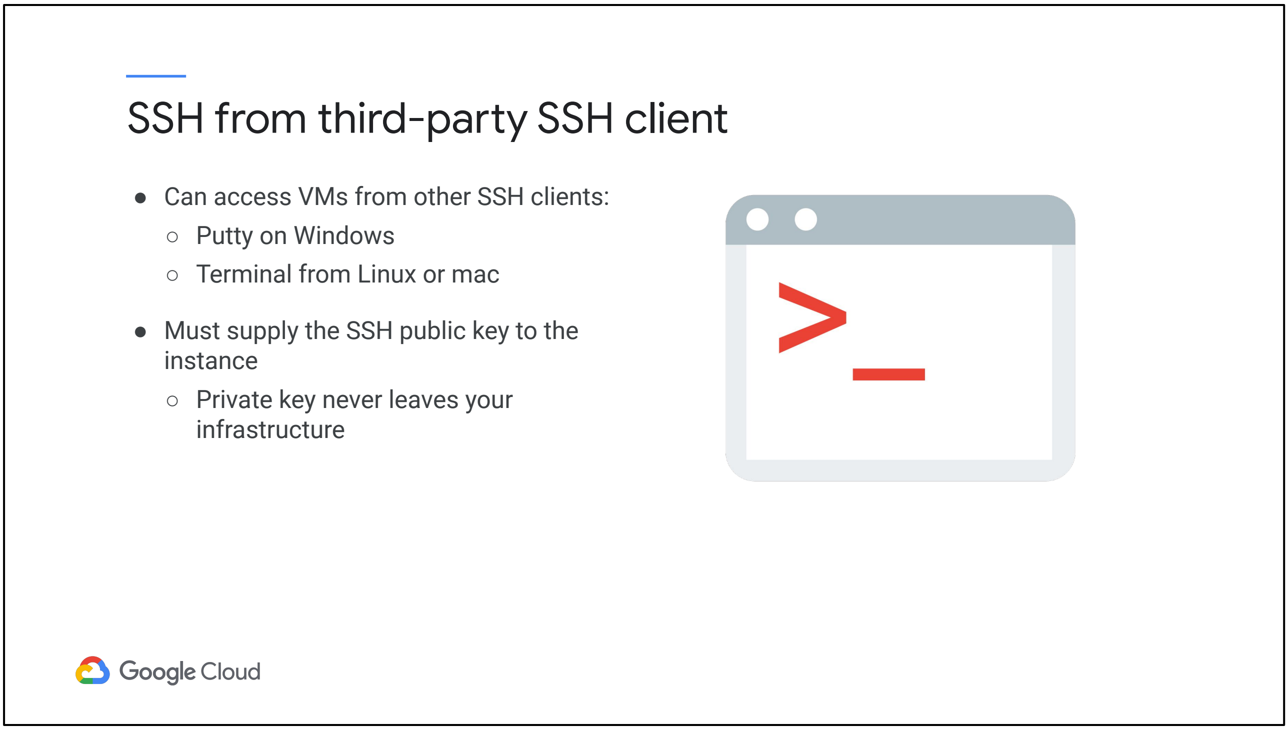
```
:~$ gcloud compute ssh web-server --zone us-central1-c
```

It is also possible to connect to a Linux instance via SSH using the gcloud SDK. Once you have the Cloud SDK installed and configured, simply connect with the command `gcloud compute ssh` , passing in the <instance-name> and the <zone-name>.

In this command, the <instance-name> is the name given to the instance when it was launched. Notice you do not need to connect to, or even know, the VMs IP address.

However, it is required for the VM to have a public IP address**.** The public IP address is used by gcloud as it is running outside of project and therefore does not have access to internal compute engine IPs.

The <zone-name> is the name of the zone where the instance is running. Running this command will automatically generate SSH keys and place a copy of them in your local home/.ssh folder.



## SSH from third-party SSH client

- Can access VMs from other SSH clients:
  - Putty on Windows
  - Terminal from Linux or mac
- Must supply the SSH public key to the instance
  - Private key never leaves your infrastructure

But what if you just want to SSH into the instance and do not have access to either the console or gcloud credentials? Don't worry, there are further options available.

It is possible to connect from alternative SSH clients such as PuTTY on Windows or similar applications on Linux or Mac operating systems. To connect remember you just need to SSH to the public IP address of the instance and provide a valid username and SSH private key to authenticate.

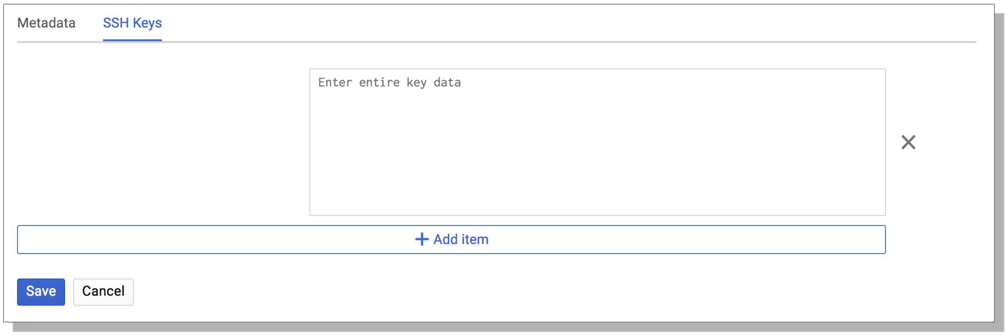
The firewall rule for the instance still requires TCP port 22 to be allowed for the IP address range of your SSH client. Note the SSH keys to use in this case are managed outside of Google Cloud. You can manually create your own SSH key pairs, using tools like PuTTYgen or ssh-keygen.

The public key must be provided to the instance that you wish to authenticate against, but your private key never leaves your infrastructure.

# Adding SSH keys to projects

Can add SSH keys as project metadata:

- Provide only the public key.
- Automatically added to all VMs by default.



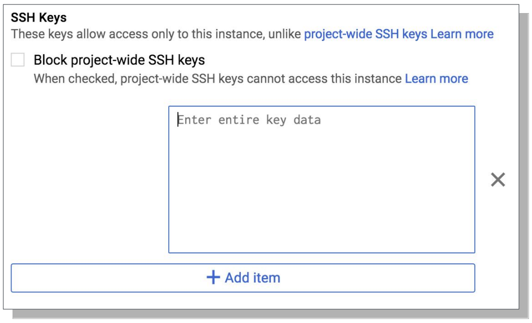
Google Cloud

The public key is provided to the instance using the project metadata. The project metadata can be accessed in the Cloud Console from the Compute Engine dashboard. Simply select the “add item” option and upload your public key.

Note: by default, all keys added to the project metadata are available to ALL VMs in the project.

## Adding SSH keys to instances

- Can configure instances to NOT use project-wide keys:
  - Can specify public key for individual instances.
- Add SSH keys to instance metadata when creating a VM:
  - Provide access to only this machine.



SSH Keys

These keys allow access only to this instance, unlike project-wide SSH keys Learn more

□ Block project-wide SSH keys

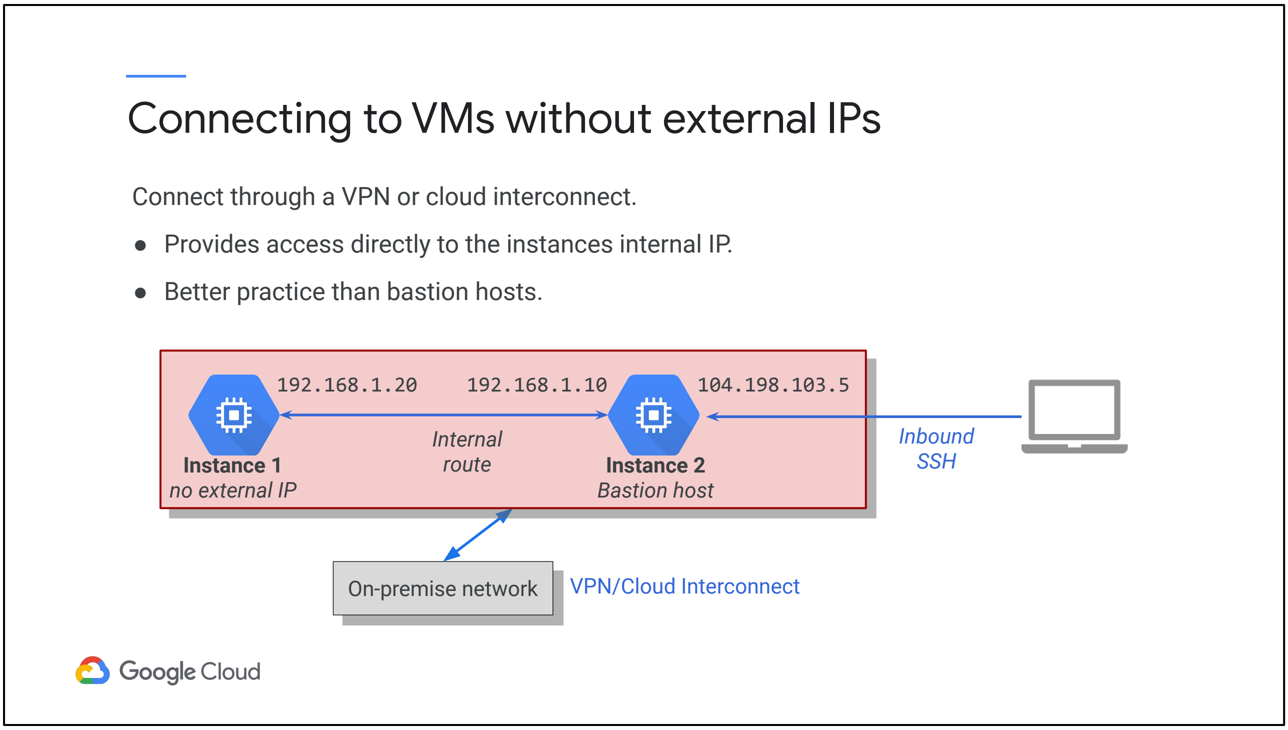
When checked, project-wide SSH keys cannot access this instance Learn more

Google Cloud

However if you do not want keys to the available to all VMs in the project, you can configure individual VMs to not use project-wide keys.

When launching a VM, the “Block project-wide SSH keys” option can be selected to enable this restriction.

SSH keys can also be added to instance-specific metadata and will only be available to that instance.



## Connecting to VMs without external IPs

Connect through a VPN or cloud interconnect.

- Provides access directly to the instances internal IP.
- Better practice than bastion hosts.

192.168.1.20

192.168.1.10

104.198.103.5

*Internal route*

**Instance 1**
*no external IP*

**Instance 2**
*Bastion host*

*Inbound SSH*

On-premise network

VPN/Cloud Interconnect

Google Cloud

So far, all of the SSH connection options discussed require the VM instance to have a public IP address. This raises the obvious question: what if the instance does not have a public IP address?

One solution to this type of situation is to use a bastion host.

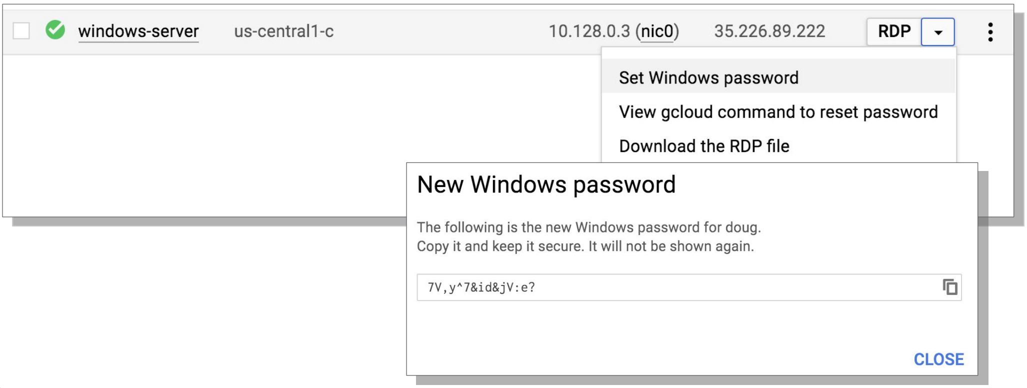
To implement this solution, create a second VM with a Public IP address in the same network as the instance you want to connect to. Then, connect to the bastion host and from there SSH to the private VM.

Be sure to harden the bastion host and ensure the firewall rules limit the source IPs able to connect to the Bastion, and then only allow SSH traffic to private instances from the bastion.

An even better practice would be to use a VPN or some other more secure form of connection, such as Cloud Interconnect, for ordinary activities. Only use SSH with the bastion host as the maintenance avenue of last resort.

## Connecting to Windows with RDP

- Set the username and password using the Console or gcloud.
- Can download an RDP file.



New Windows password

The following is the new Windows password for doug.
Copy it and keep it secure. It will not be shown again.

```
7V,y^7&id&jV:e?
```

Google Cloud

For Windows VMs, connect using RDP and login in with a username and password.

The username and password can be set from the Admin Console or using gcloud.

From the console, click the down arrow next to the RDP button and select Set WIndows password.

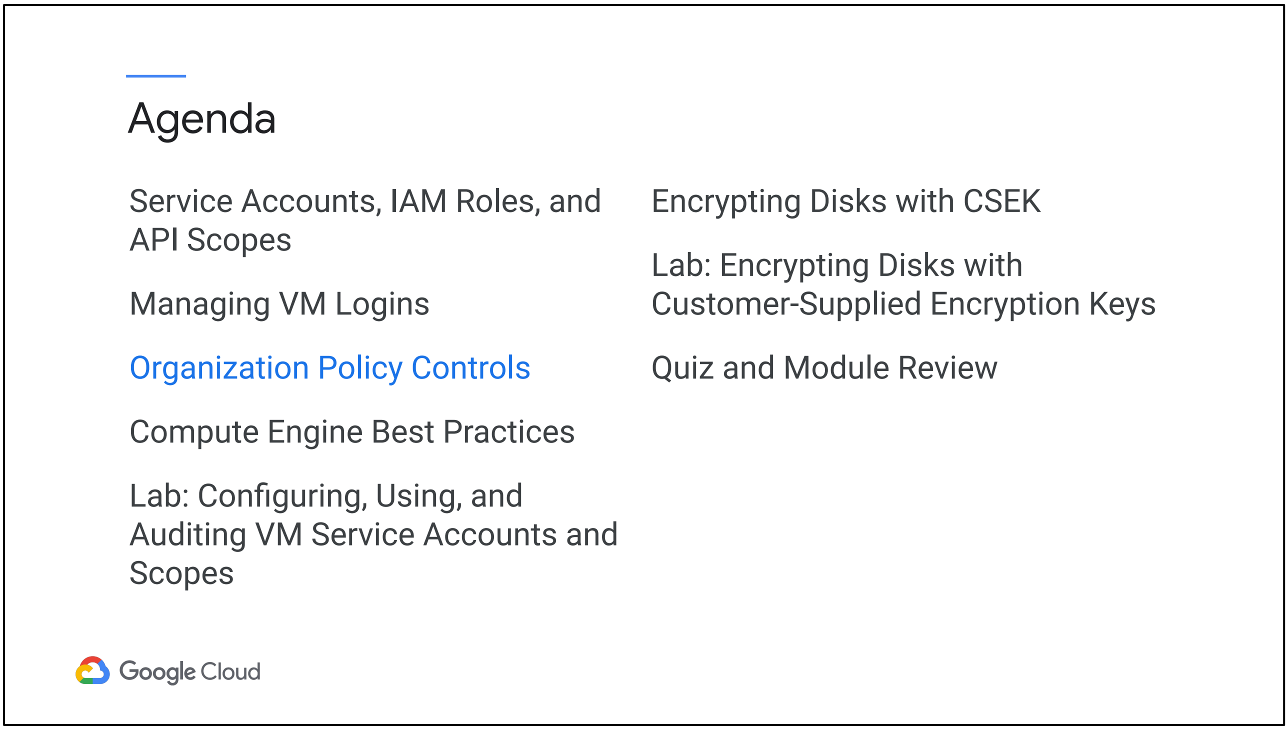
From `gcloud`, the command is:

```
gcloud compute reset-windows-password instance-name
```

and then specify the username (i.e. **`--user=`**) whose password will be reset.

To connect, simply use an RDP client and connect to the external address of the instance. You can optionally download an RDP file if you wish.

Compute Engine will automatically generate a random password for your Windows instance. Once you connect, you should change this to a custom password.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

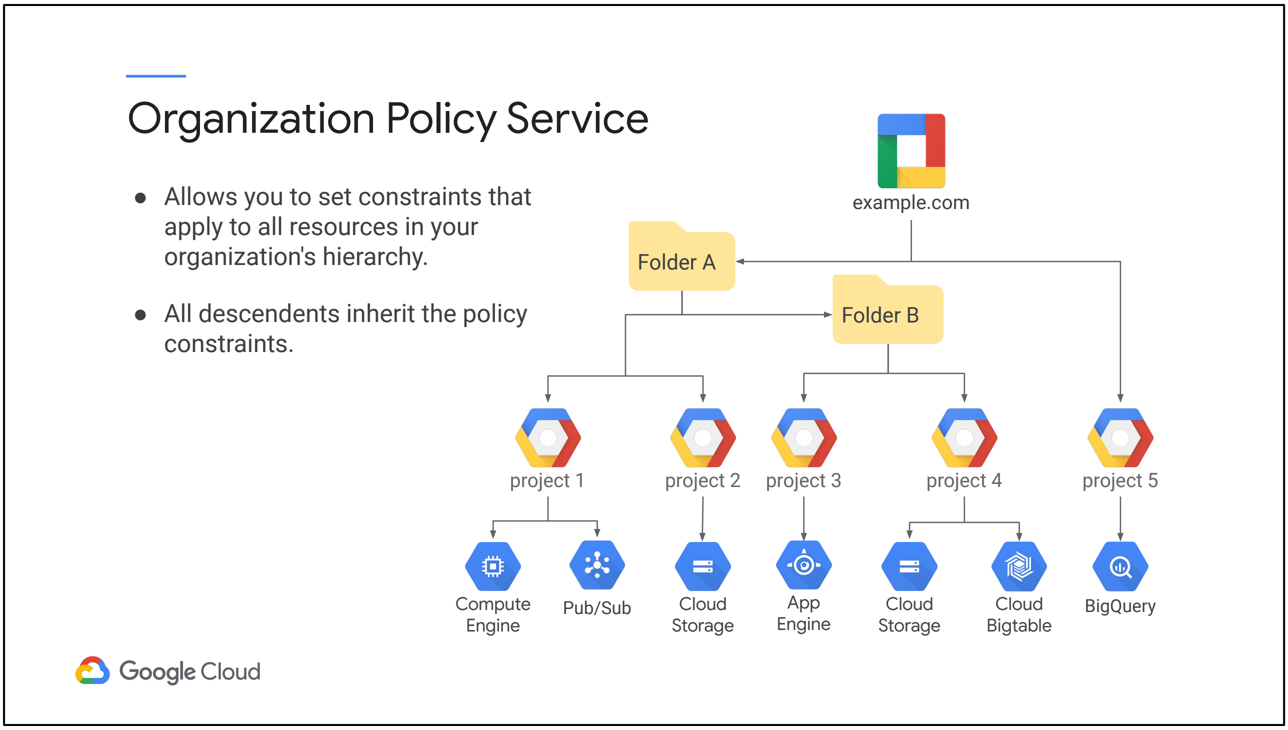
Quiz and Module Review

Google Cloud

We are now going to talk about Organization policy controls.

Ok, by now you know that Cloud Identity and Access Management focuses on the “who”: that is who can take action on specific resources based on permissions.

Organization Policy focuses on the “what”, and lets the administrator set restrictions on specific resources to determine how they can eventually be configured.



## Organization Policy Service

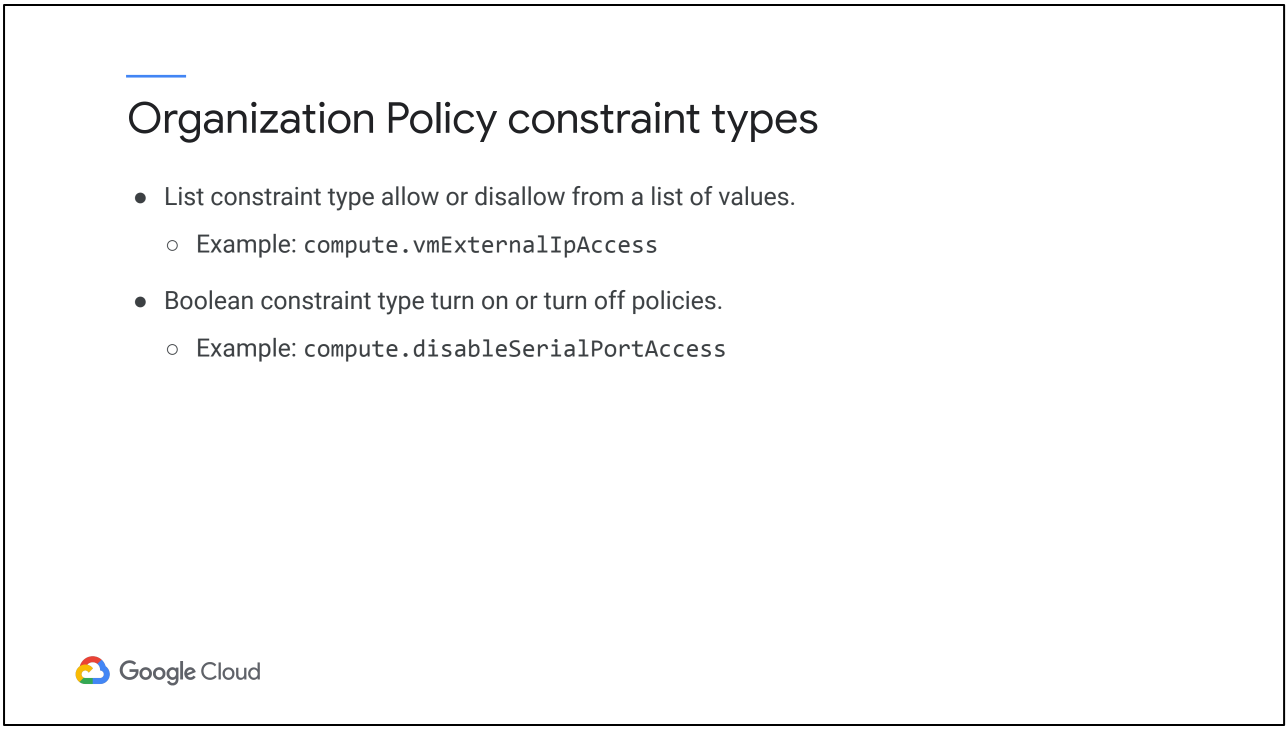
- Allows you to set constraints that apply to all resources in your organization's hierarchy.
- All descendents inherit the policy constraints.

As you can see, the Organization Policy Service gives you both centralized and programmatic control over your organization's cloud resources.  An organization policy administrator can configure restrictions across your entire resource hierarchy. A few benefits are:

- Centralize control to configure restrictions on how your organization’s resources can be used.
- Define and establish guardrails for your development teams to stay within compliance boundaries.
- Assist project owners and their teams move quickly without worry of breaking compliance.

To define an organization policy, you choose a constraint, which is a particular type of restriction against either a Google Cloud service or a group of Google Cloud services. You then configure that constraint with your desired restrictions.

Note that descendants of the targeted resource inherit the organization policy. For example, applying an organization policy to the root organization node, effectively drives enforcement of that organization policy and its configuration of restrictions across your organizations hierarchy.



## Organization Policy constraint types

- List constraint type allow or disallow from a list of values.
  - Example: `compute.vmExternalIpAccess`
- Boolean constraint type turn on or turn off policies.
  - Example: `compute.disableSerialPortAccess`

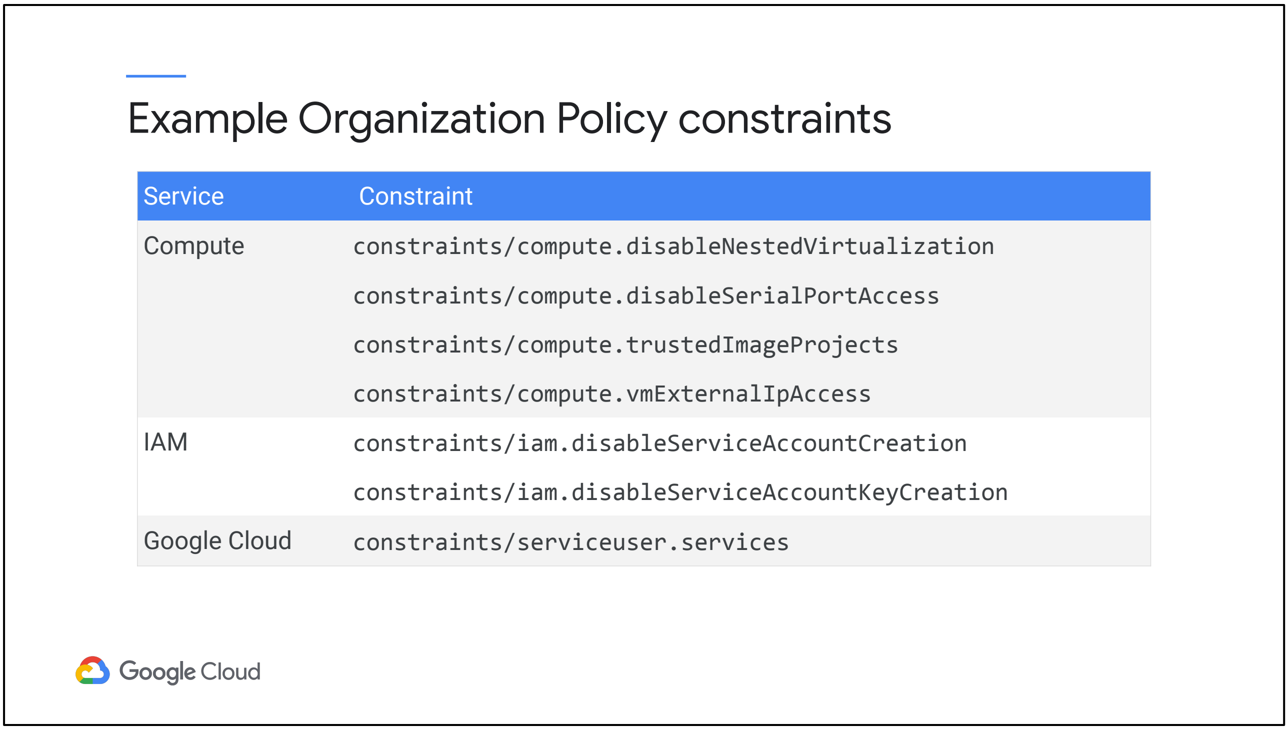
Google Cloud

Earlier you learned that a constraint is a particular type of restriction against a Google Cloud service or group of services. Think of a constraint as a blueprint that defines what behaviors are controlled. The enforcing service will evaluate the constraint type and value to determine the restriction.

There are 2 main constraint types: list and boolean.

The list constraint type allows or disallows values within a list. An example is the “compute.vmExternalIpAccess” list constraint. This constraints defines the set of Compute Engine VM instances that are allowed to use external IP addresses. Remembe thatr by default, all Compute  Engine instances are allowed to use external IP addresses.

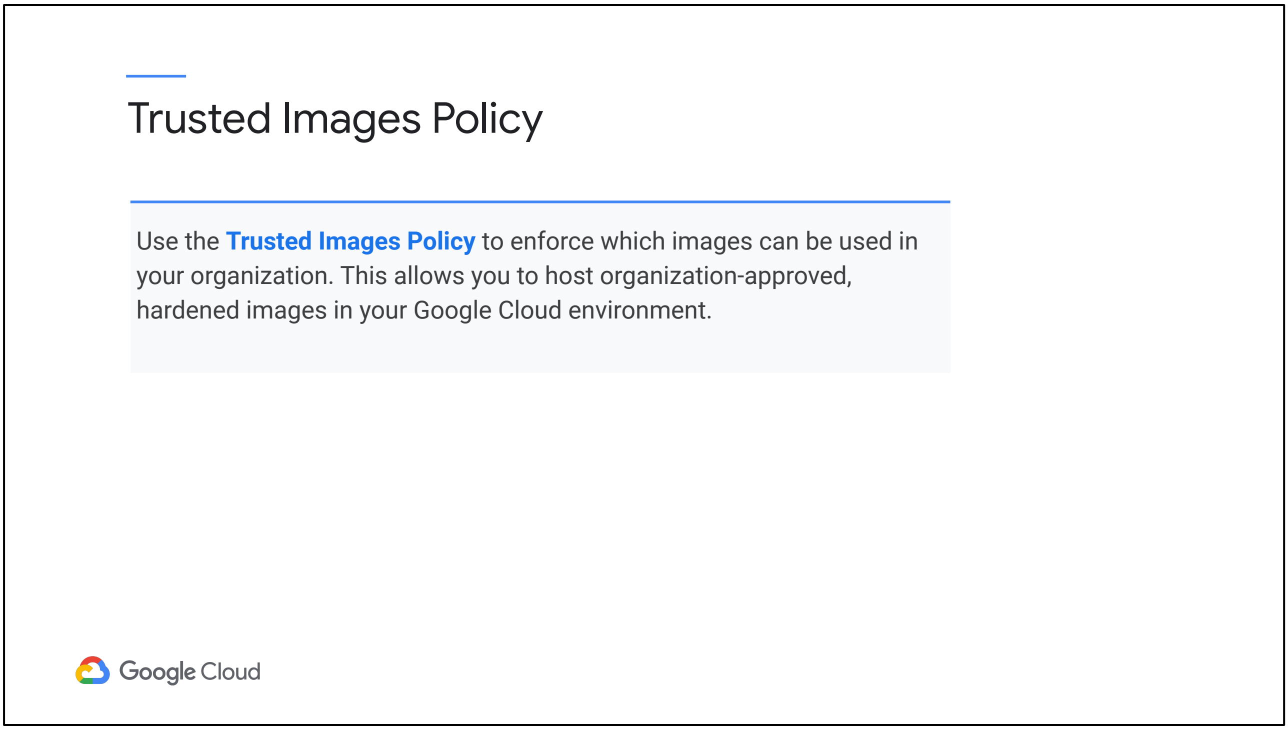
Boolean constraint types turn policies on or off. and an example of this constraint type would be the “compute.disableSerialPortAccess” constraint.



## Example Organization Policy constraints

| Service | Constraint |
|---|---|
| Compute | `constraints/compute.disableNestedVirtualization` |
| | `constraints/compute.disableSerialPortAccess` |
| | `constraints/compute.trustedImageProjects` |
| | `constraints/compute.vmExternalIpAccess` |
| IAM | `constraints/iam.disableServiceAccountCreation` |
| | `constraints/iam.disableServiceAccountKeyCreation` |
| Google Cloud | `constraints/serviceuser.services` |

Of course, there are many different constraints for different Google Cloud services. This slide shows a few more constraints that are available for some other services.



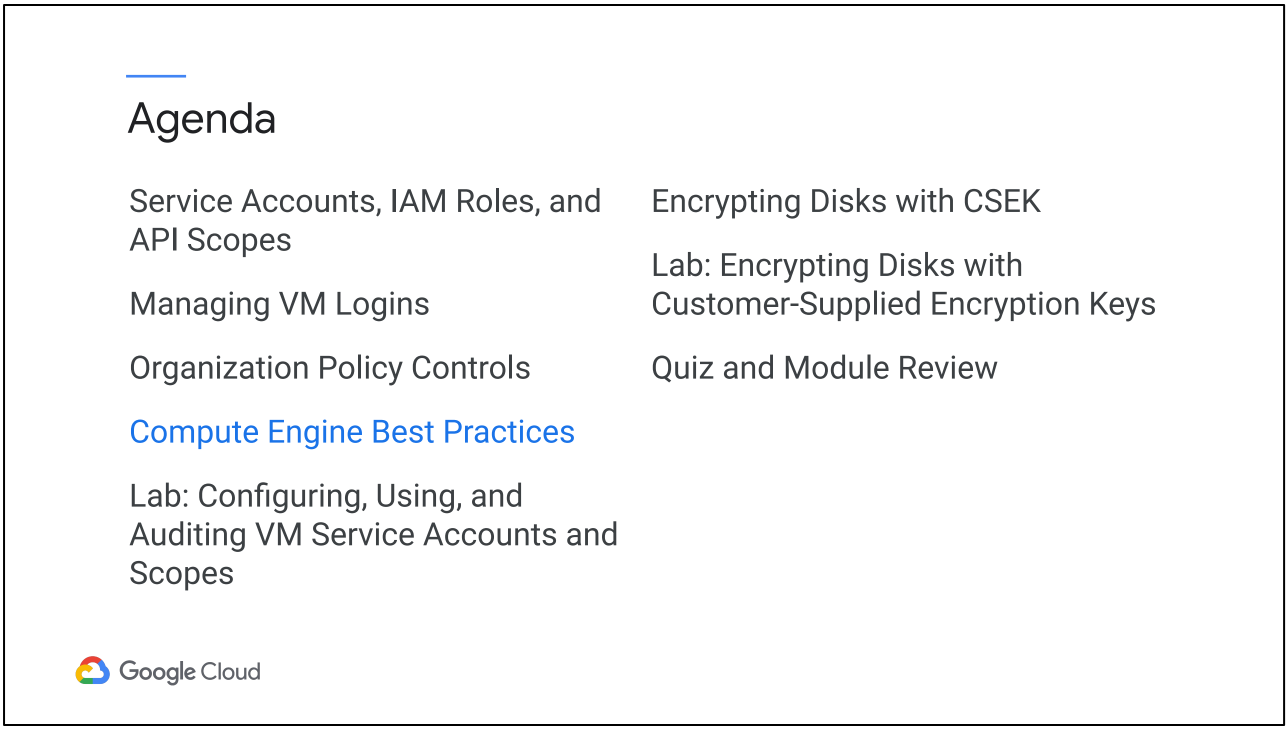
## Trusted Images Policy

Use the **Trusted Images Policy** to enforce which images can be used in your organization. This allows you to host organization-approved, hardened images in your Google Cloud environment.

The compute.trustedImageProjects constraint has an interesting use case.

By default, project users can create persistent disks or copy images using either public images and any other images that project members can access through IAM roles. However, you may want to restrict your projects to only use images that contain approved software to create boot disks that meets your policy or security requirements.

The Trusted Images Policy can be used to enforce which images can be used in your organization. This allows you to host organization-approved, hardened images in your Google Cloud environment.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

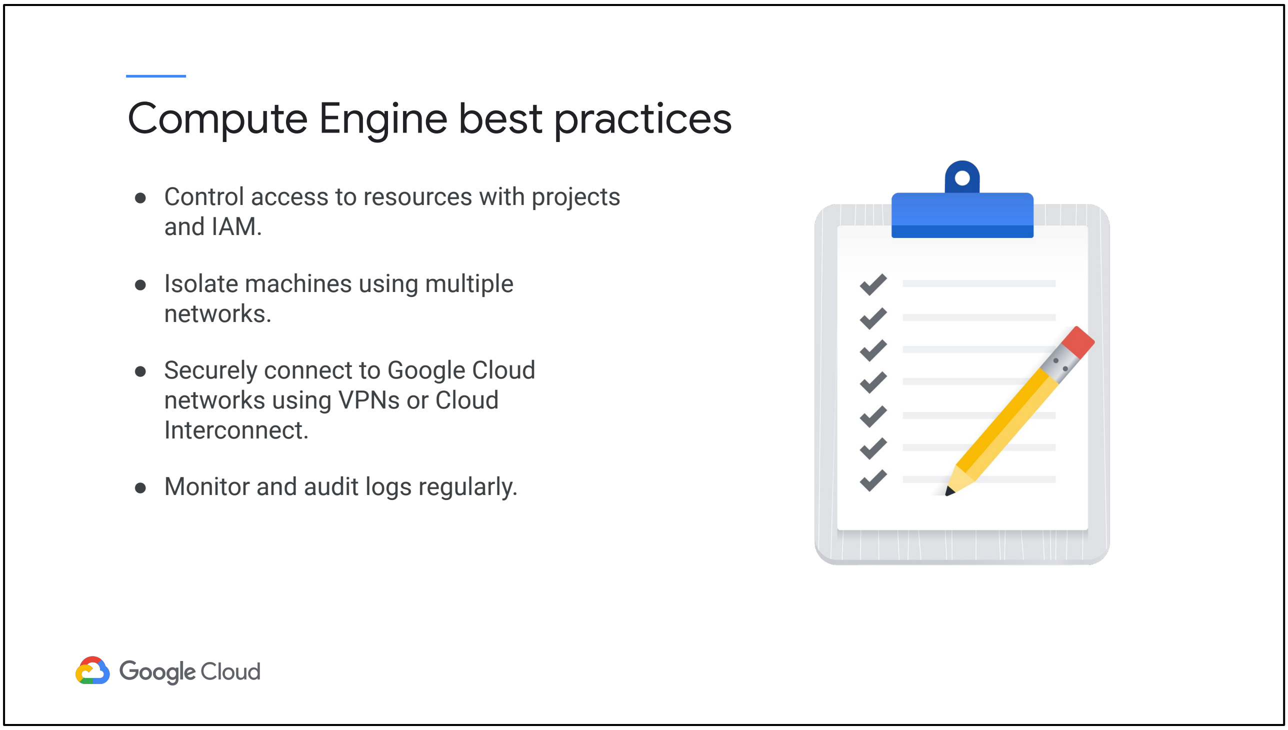
Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review

Now let’s discuss Compute Engine best practices.



## Compute Engine best practices

- Control access to resources with projects and IAM.
- Isolate machines using multiple networks.
- Securely connect to Google Cloud networks using VPNs or Cloud Interconnect.
- Monitor and audit logs regularly.

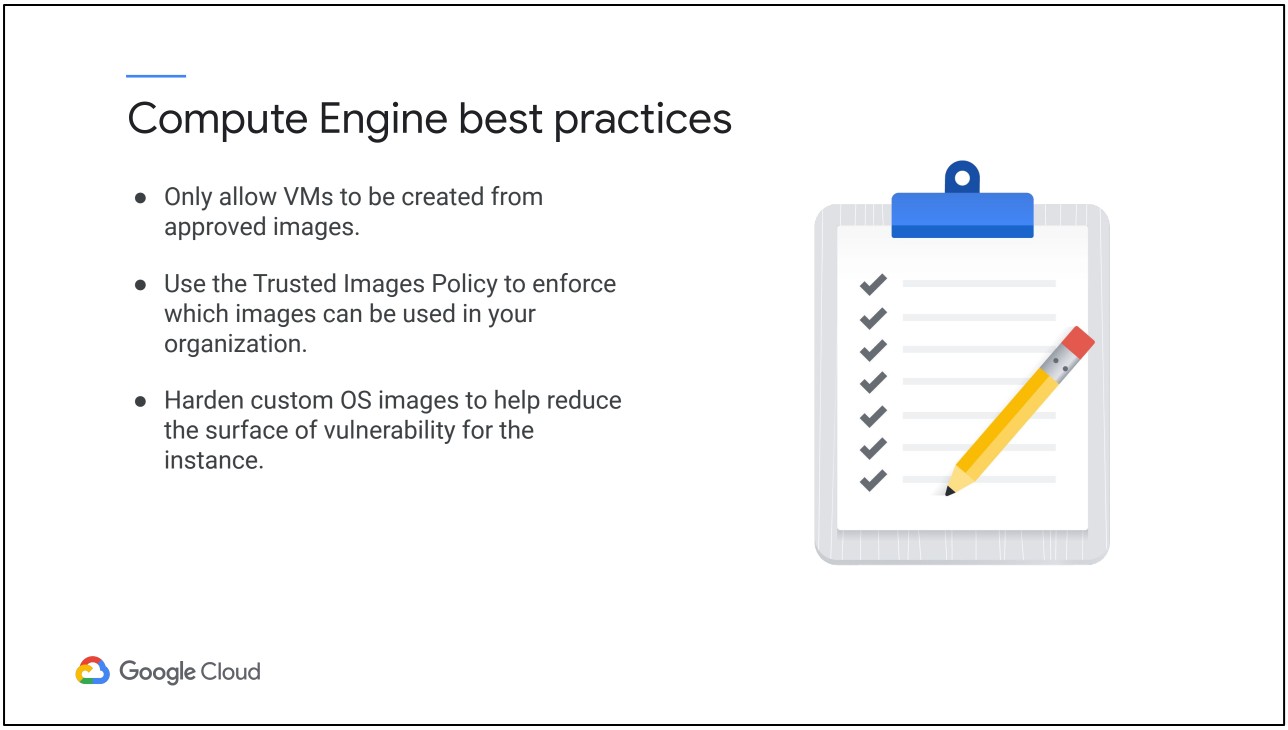
Google Cloud

First of all, always ensure the proper permissions are given to control access to resources. Projects form the basis for creating, enabling, and using all Google Cloud services, including managing resource permissions. Build for success, and utilize projects and IAM roles to control access.

Host Compute Engine resources on the same VPC network where they require network based communication . If the resources aren’t related and don’t require network communication among themselves, consider hosting them on different VPC networks.

Secure connections to public cloud providers are a concern for all organizations. You can securely extend your data center network into projects with Cloud Interconnect or Cloud VPN.

Use Cloud Audit Logging to generate logs for API operations performed in Google Compute Engine. Audit logs help you determine “who did what”, “where”, and “when”. Specifically, audit logs track how Compute Engine resources are modified and accessed within projects for auditing purposes.



## Compute Engine best practices

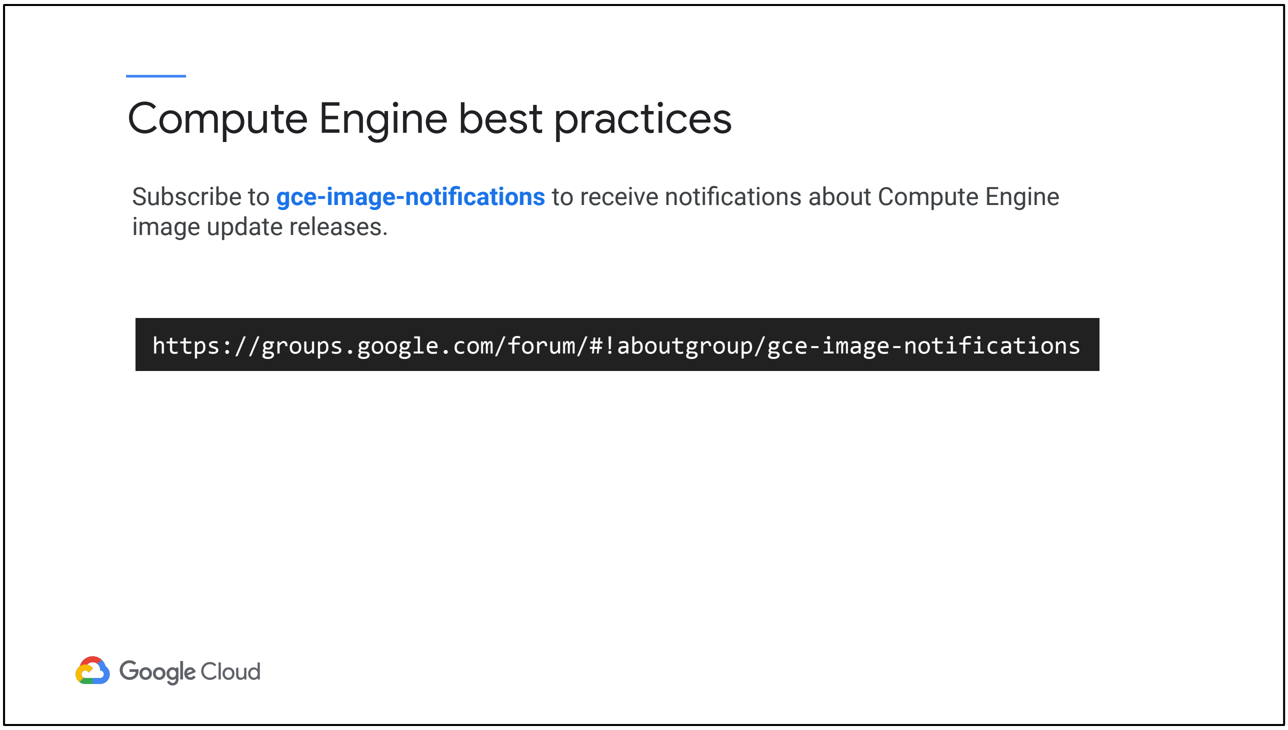
- Only allow VMs to be created from approved images.
- Use the Trusted Images Policy to enforce which images can be used in your organization.
- Harden custom OS images to help reduce the surface of vulnerability for the instance.

Google Cloud

By default, users in a project can create persistent disks or copy images using any of the public images and any images that your project members can access through IAM roles. You may want to restrict your project members so that they can create boot disks only from images that contain approved software that meets your policy or security requirements. You can define an organization policy that only allow compute engine VMs to be created from approved images.

This can be done by using the trusted Images Policy to enforce which images can be used in your organization.This allows you to host organization-approved, hardened images in your Google Cloud environment.

Hardening a custom OS image will help reduce the attack surface for the instance. Making hardened images available in your organization can help reduce your organization's overall risk profile. However, if you create a custom image, formulate a plan for how to maintain the image with security patches and other updates.



## Compute Engine best practices

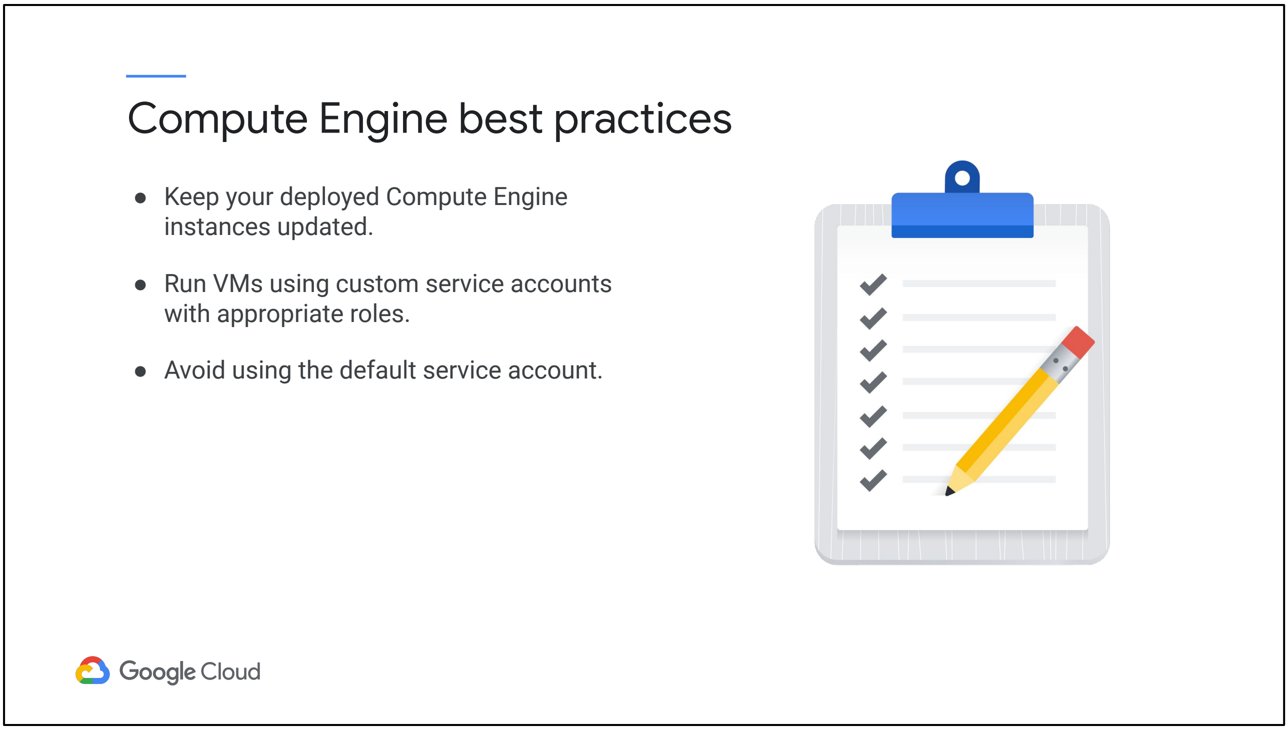
Subscribe to **gce-image-notifications** to receive notifications about Compute Engine image update releases.

```
https://groups.google.com/forum/#!aboutgroup/gce-image-notifications
```

Google Cloud

Subscribe to “gce-image-notifications” announcements to receive release notes and other updates regarding public Compute Engine images.

This will be of interest to anyone looking to keep up with the latest information about Compute Engine Images, feel free to subscribe.



## Compute Engine best practices

- Keep your deployed Compute Engine instances updated.
- Run VMs using custom service accounts with appropriate roles.
- Avoid using the default service account.

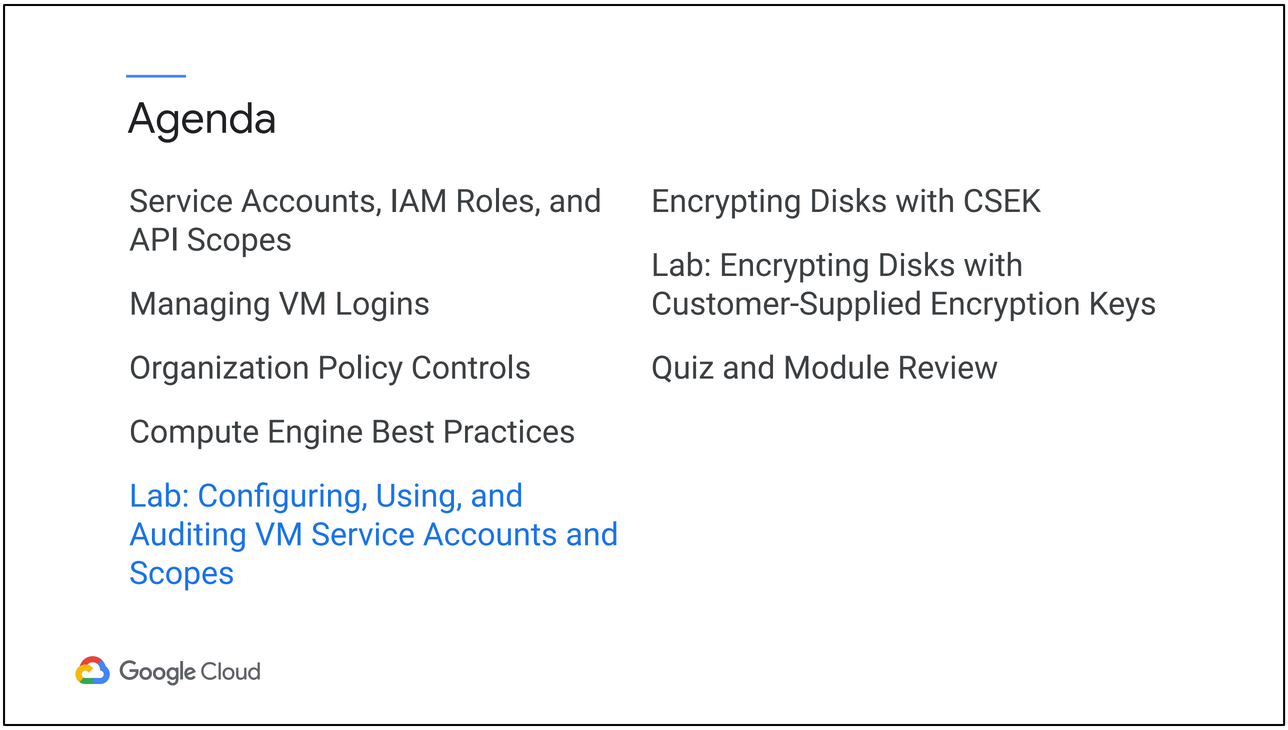
Google Cloud

Compute Engine doesn't automatically update the OS or the software on your deployed instances. You will need to patch or update your deployed Compute Engine instances when necessary. However, it is not recommended that you patch or update individual running instances.

This could end up being a lot of work and risks a chance that something could be missed in the process. Instead, it is best to patch the image that was used to launch the instance and then replace each affected instance with a new copy.

In general, Google recommends that each instance that needs to call a Google API should run as a service account with the minimum permissions necessary for that instance to do its job. In practice, this means you should configure service accounts for your instances like this:

- Create a new service account rather than using the Compute Engine default service account.
- Grant IAM roles to that service account for only the resources that it needs.
- Configure the instance to run as that service account.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

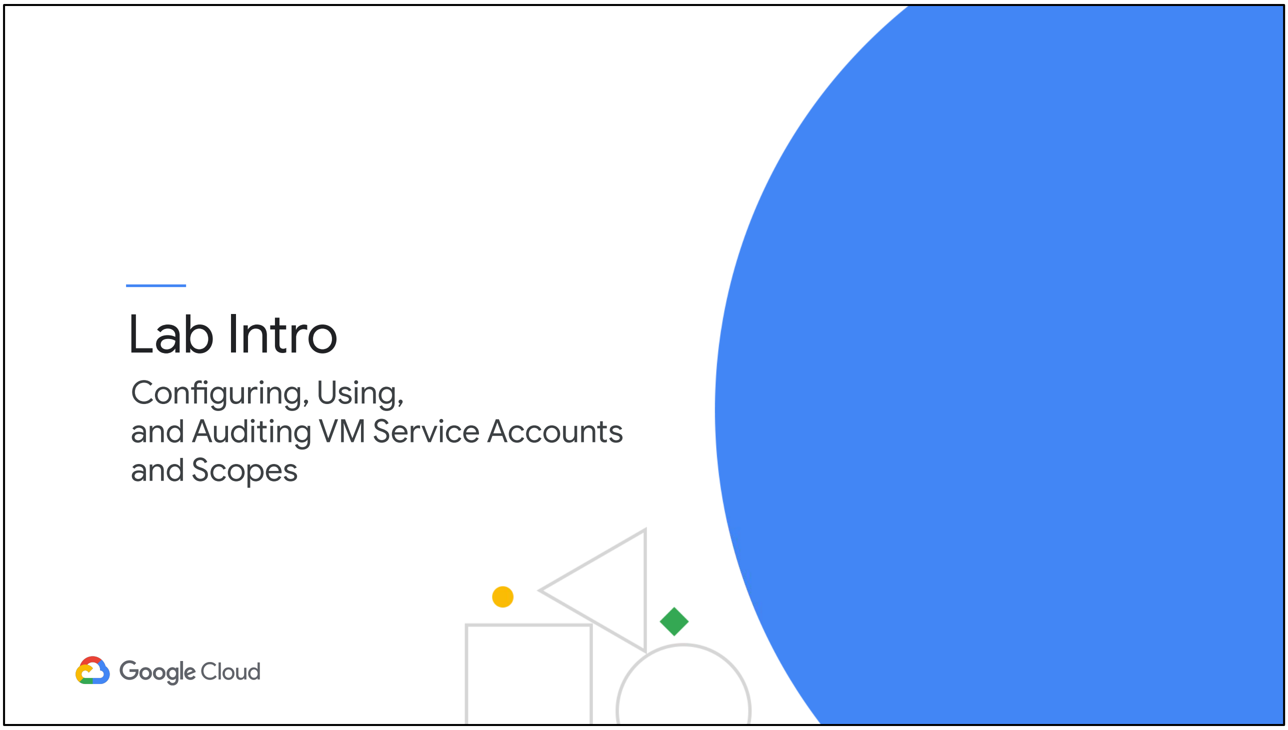
Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review



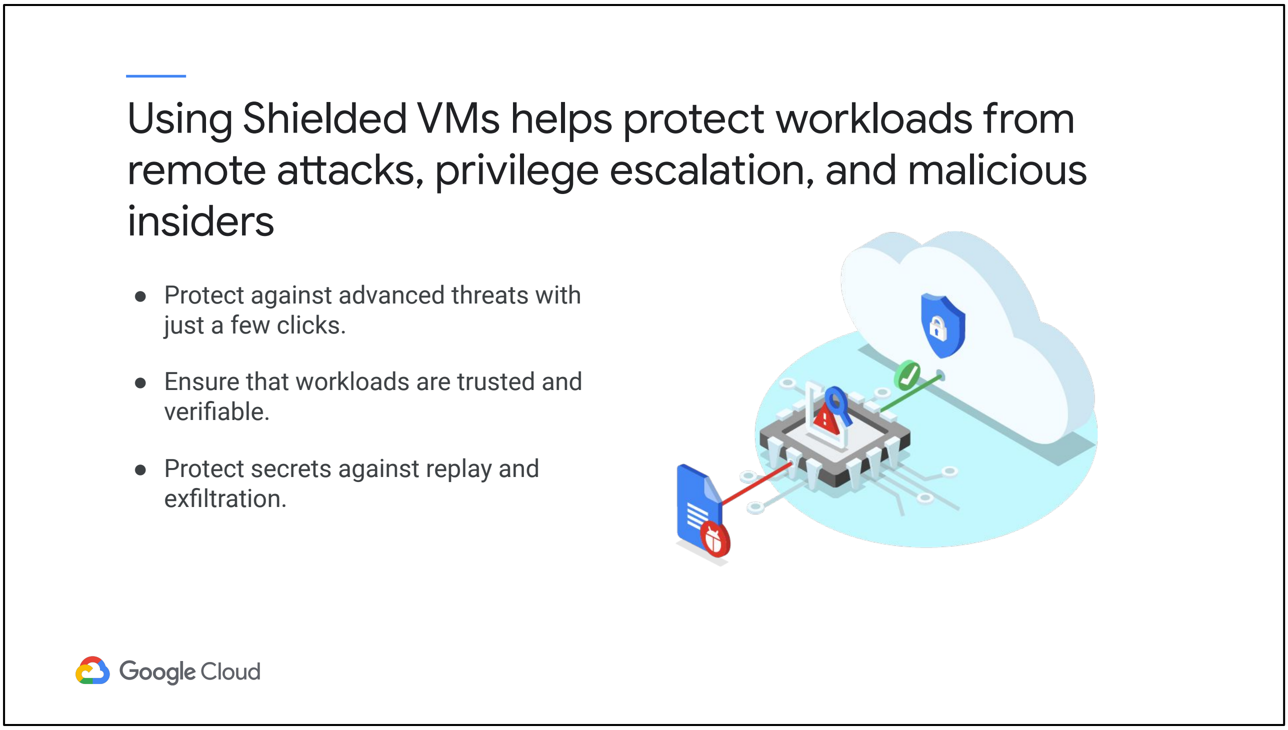
# Lab Intro

Configuring, Using,
and Auditing VM Service Accounts
and Scopes

Google Cloud

OK, now you will get a chance to configure and use service accounts and scopes. In this lab, you will learn how to:

- Create and manage service accounts.
- Create a virtual machine and associate it with a service account.
- Use client libraries to access BigQuery from a service account.
- Run a query on a BigQuery public dataset from a Compute Engine instance.

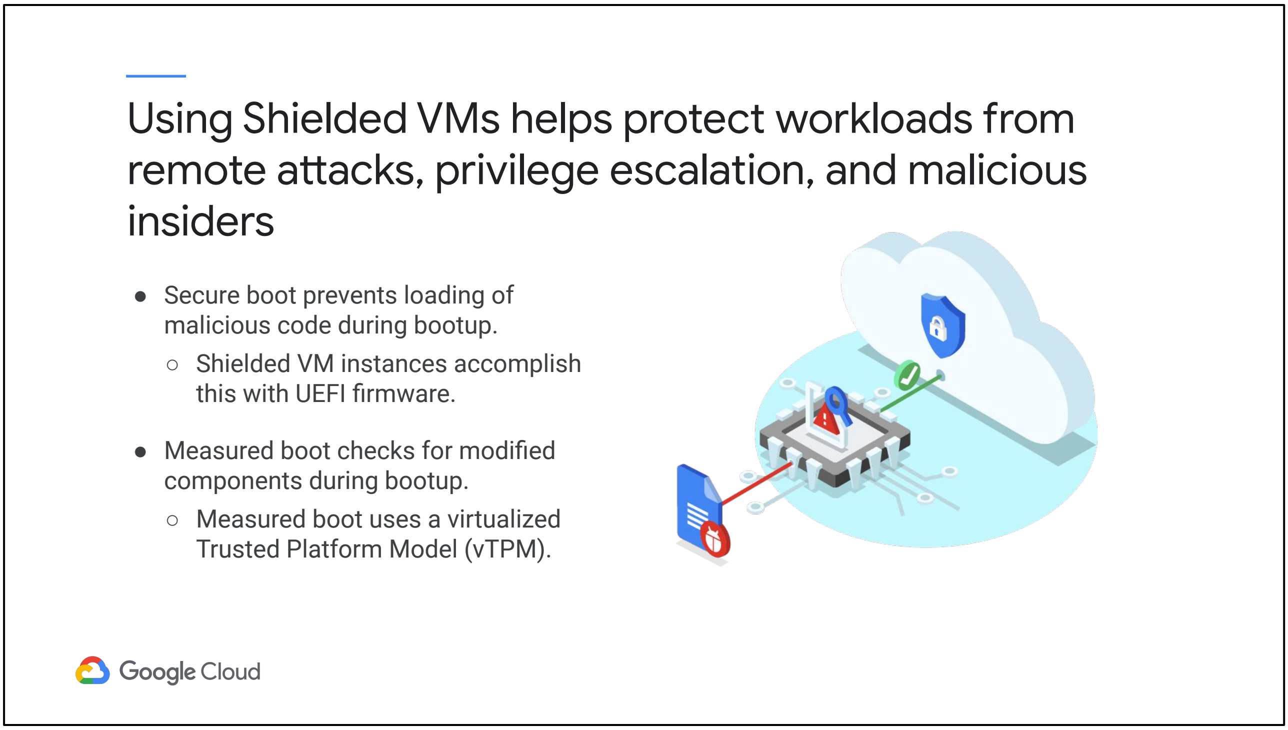


## Using Shielded VMs helps protect workloads from remote attacks, privilege escalation, and malicious insiders

- Protect against advanced threats with just a few clicks.
- Ensure that workloads are trusted and verifiable.
- Protect secrets against replay and exfiltration.

Protecting your hardware and firmware and host and guest operating systems is an important part of securing your workloads and data from malicious use and attacks. Unfortunately, some types of malware attacks can remain undetected on your virtual machines for long periods of time.

Shielded VM offers **verifiable integrity** of your Compute Engine VM instances, so you can be confident that your instances haven't been compromised by boot-level or kernel-level malware or rootkits, or that your secrets exposed and used by others.



## Using Shielded VMs helps protect workloads from remote attacks, privilege escalation, and malicious insiders

- Secure boot prevents loading of malicious code during bootup.
  - Shielded VM instances accomplish this with UEFI firmware.
- Measured boot checks for modified components during bootup.
  - Measured boot uses a virtualized Trusted Platform Model (vTPM).

Google Cloud

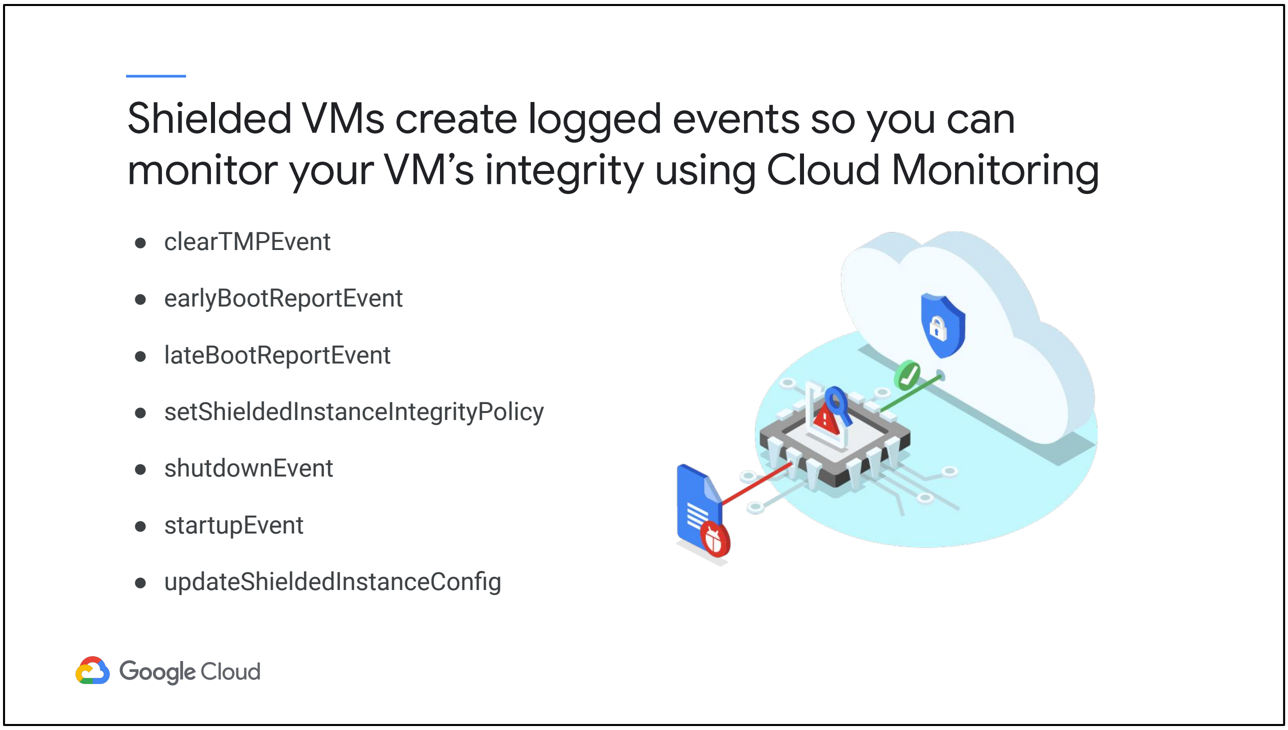
Each time your VM starts up, secure boot makes certain that the software it is loading is authentic and unmodified by verifying that the firmware has been digitally signed with Google’s Certificate Authority.

Shielded VM instances use Unified Extensible Firmware Interface (UEFI) firmware, which securely manages the certificates that contain the keys used by the software manufacturers to sign the system firmware, the system boot loader, and any binaries loaded. UEFI firmware verifies the digital signature of each boot component in turn against its secure store of approved keys, and if that component isn't properly signed (or isn't signed at all), it isn't allowed to run. This verification ensures that the instance's firmware is unmodified and establishes the “root of trust” for Secure Boot.

Measured boot creates a hash of each component as it loads, concatenates that hash with other components that have already been loaded, and then rehashes it. This allows measured boot to record the number of components loaded on boot-up and their sequence.

The first time your Shielded VM is booted, this initial hash is securely stored and used as the baseline for verification of that VM during subsequent boots. This is called “integrity monitoring,” and it helps ensure that your VM’s boot components and boot sequence have not been altered.

Shielded VMs use a virtual Trusted Platform Model, which is the “virtualized” version of a specialized computer chip you can use to protect objects, like keys and certificates, that are used to provide authenticated access to your system. This vTPM allows Measured Boot to perform the measurements needed to create a known good boot baseline, called the integrity policy baseline, upon the first bootup of your Shielded VM.



## Shielded VMs create logged events so you can monitor your VM’s integrity using Cloud Monitoring

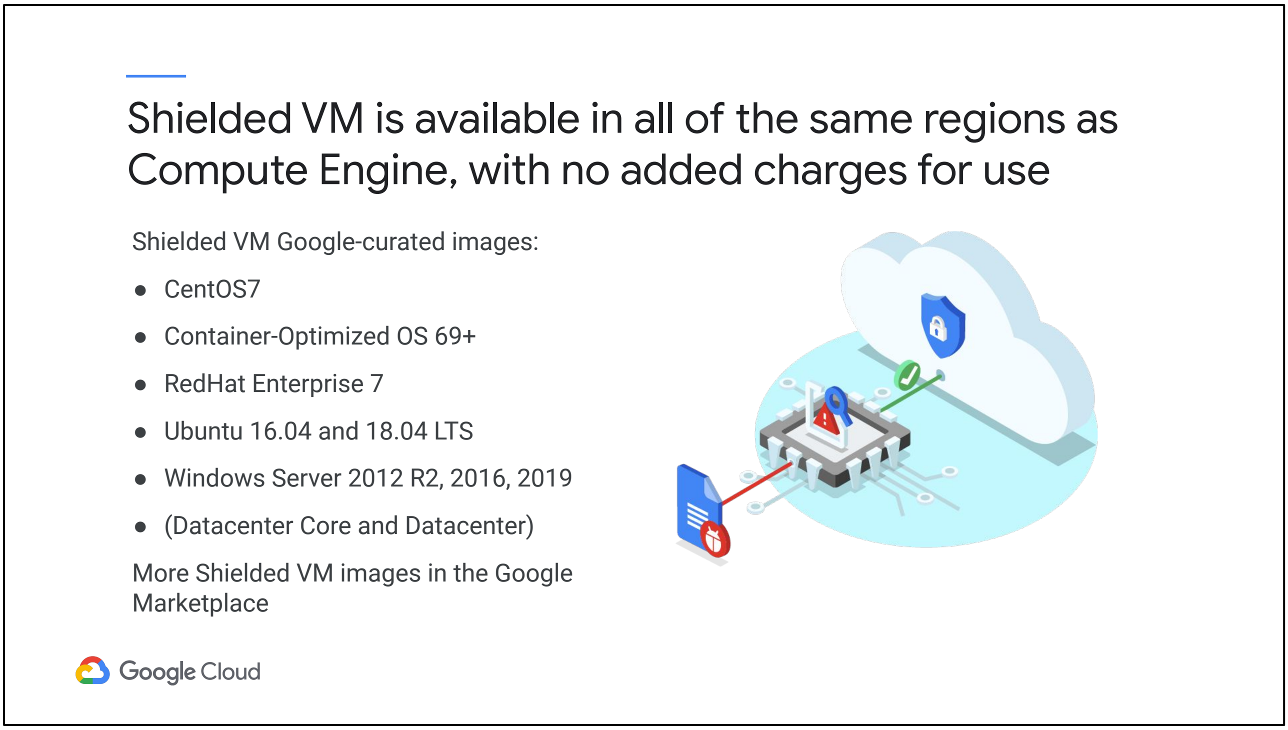
- clearTMPEvent
- earlyBootReportEvent
- lateBootReportEvent
- setShieldedInstanceIntegrityPolicy
- shutdownEvent
- startupEvent
- updateShieldedInstanceConfig

Google Cloud

Shielded VM creates log entries for the following types of events:

- clearTPMEvent: Identifies whether the vTPM has been cleared, which deletes any secrets stored in it.
- earlyBootReportEvent: Identifies whether the early boot sequence integrity check passed.
- lateBootReportEvent: Identifies whether the late boot sequence integrity check passed.
- setShieldedInstanceIntegrityPolicy: Logged each time you update the integrity policy baseline.
- shutdownEvent: Logged each time the VM instance is stopped.
- startupEvent: Logged each time the VM instance is started. Keeps a bootCounter value, which shows how many times this particular instance has been restarted.
- updateShieldedInstanceConfig: Logged each time you enable or disable one of the Shielded VM options.

The typical event progression seen in the logs is startupEvent, earlyBootReportEvent, lateBootReportEvent, and eventually shutdownEvent. These all have the same bootCounter value to identify them as describing the same VM instance boot sequence.



## Shielded VM is available in all of the same regions as Compute Engine, with no added charges for use

Shielded VM Google-curated images:

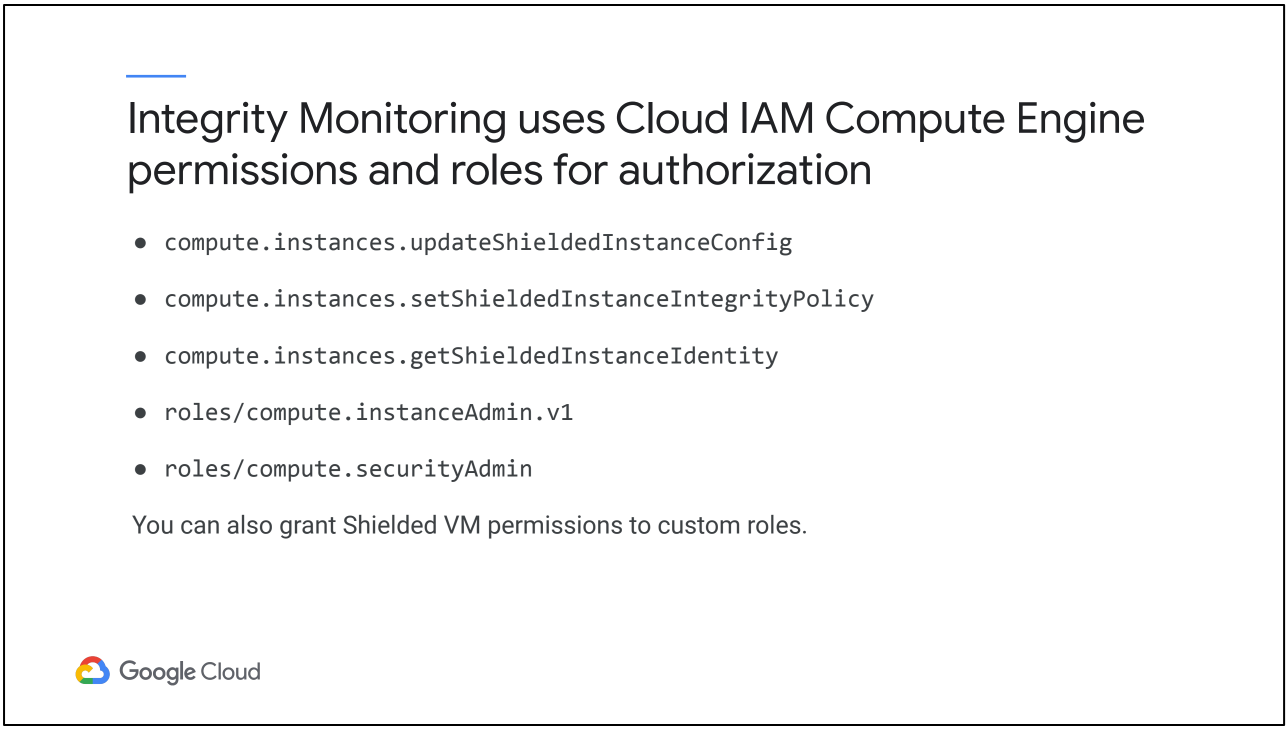
- CentOS7
- Container-Optimized OS 69+
- RedHat Enterprise 7
- Ubuntu 16.04 and 18.04 LTS
- Windows Server 2012 R2, 2016, 2019
- (Datacenter Core and Datacenter)

More Shielded VM images in the Google Marketplace

Google Cloud

When creating a Shielded VM, there are a wide range of image options. This slide shows a list of currently available Google-curated images. You can find even more shielded VM images the Google Cloud Marketplace.

In addition, if your organization relies on custom images, you can now transform an existing VM into a Shielded VM that runs on Google Cloud.

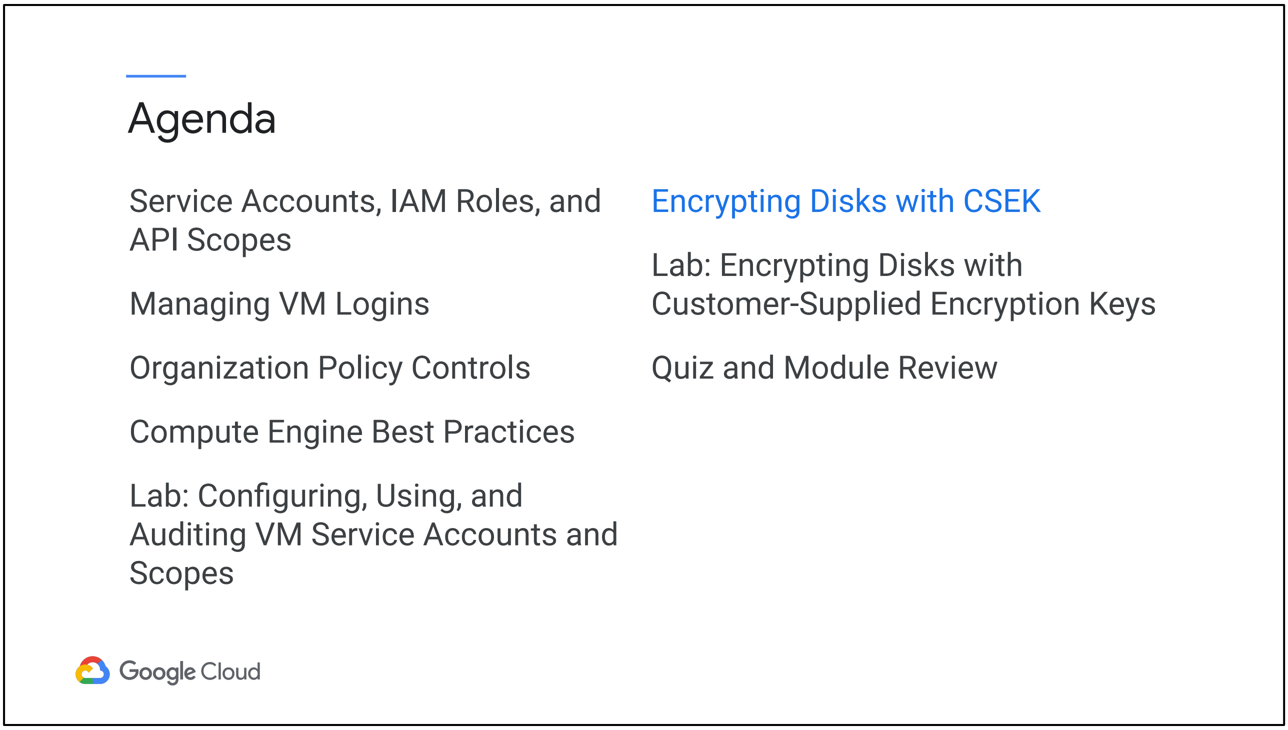


## Integrity Monitoring uses Cloud IAM Compute Engine permissions and roles for authorization

- `compute.instances.updateShieldedInstanceConfig`
- `compute.instances.setShieldedInstanceIntegrityPolicy`
- `compute.instances.getShieldedInstanceIdentity`
- `roles/compute.instanceAdmin.v1`
- `roles/compute.securityAdmin`

You can also grant Shielded VM permissions to custom roles.

In order to administer and use the integrity modeling features of the Shielded VM, you will need to assign these Cloud IAM Compute Engine permissions and roles to the appropriate accounts. If your organization uses custom roles, you can also assign any or all of these permissions to the appropriate custom role. If you want all of the VMs in your organization to be Shielded VM instances, you can also set the constraints/compute.requireShieldedVm organization policy constraint to True.



## Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

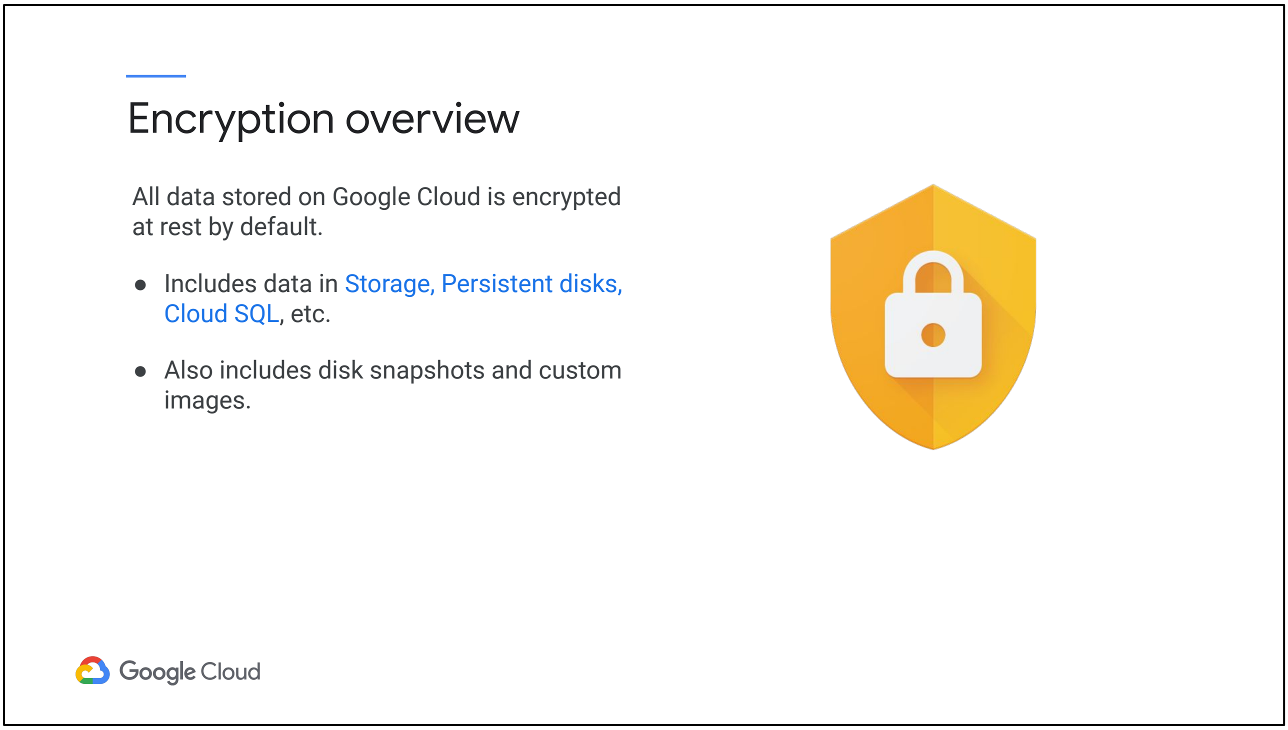
Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review

Google Cloud

Some people wonder “How do I protect my data when it is stored in Google Cloud?”.

In this section, we will discuss how data is stored and “encrypted at rest” in Google Compute Engine.



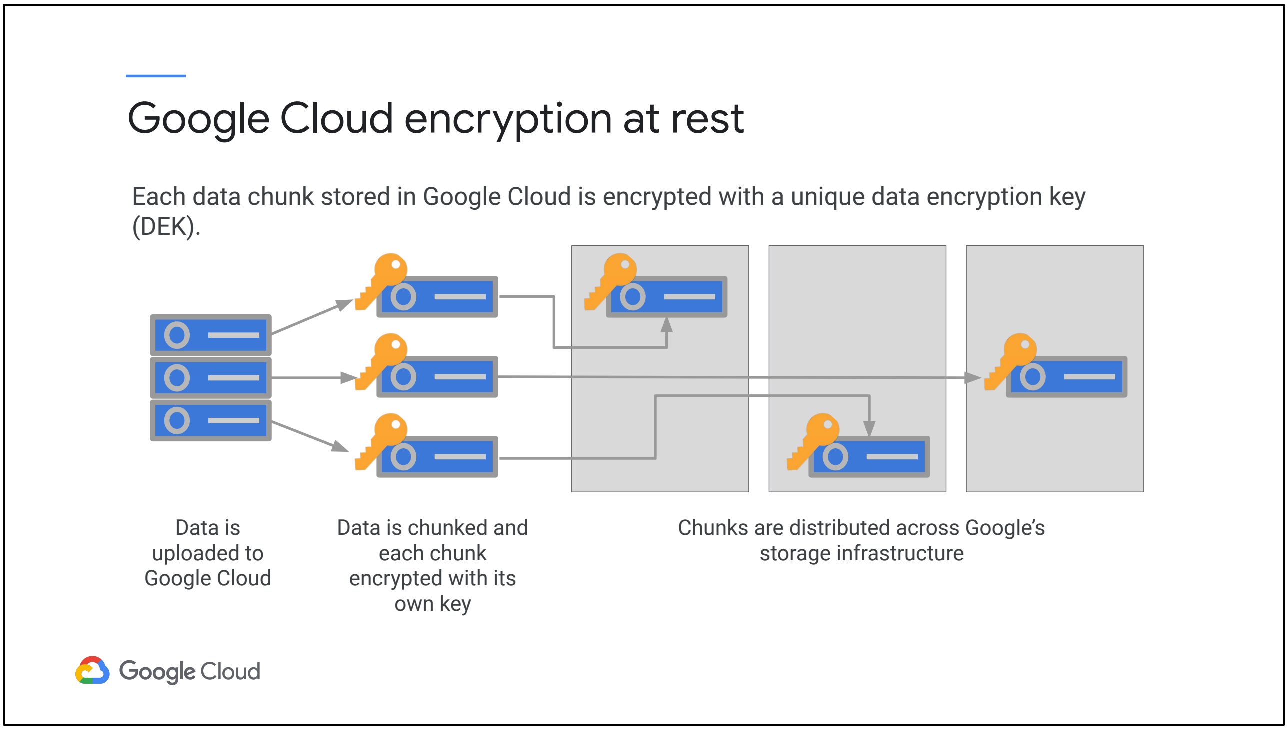
## Encryption overview

All data stored on Google Cloud is encrypted at rest by default.

- Includes data in Storage, Persistent disks, Cloud SQL, etc.
- Also includes disk snapshots and custom images.

Google Cloud

Google Cloud encrypts all customer data stored at rest, without any action required from you, the customer. A common cryptographic library is used to implement encryption consistently across almost all Google Cloud products. This includes data stored in Cloud Storage, Compute Engine persistent disks, Cloud SQL databases - virtually everything! Even disk snapshots and custom Compute Engine virtual machine images are encrypted.



# Google Cloud encryption at rest

Each data chunk stored in Google Cloud is encrypted with a unique data encryption key (DEK).

Data is uploaded to Google Cloud

Data is chunked and each chunk encrypted with its own key

Chunks are distributed across Google's storage infrastructure

Google Cloud

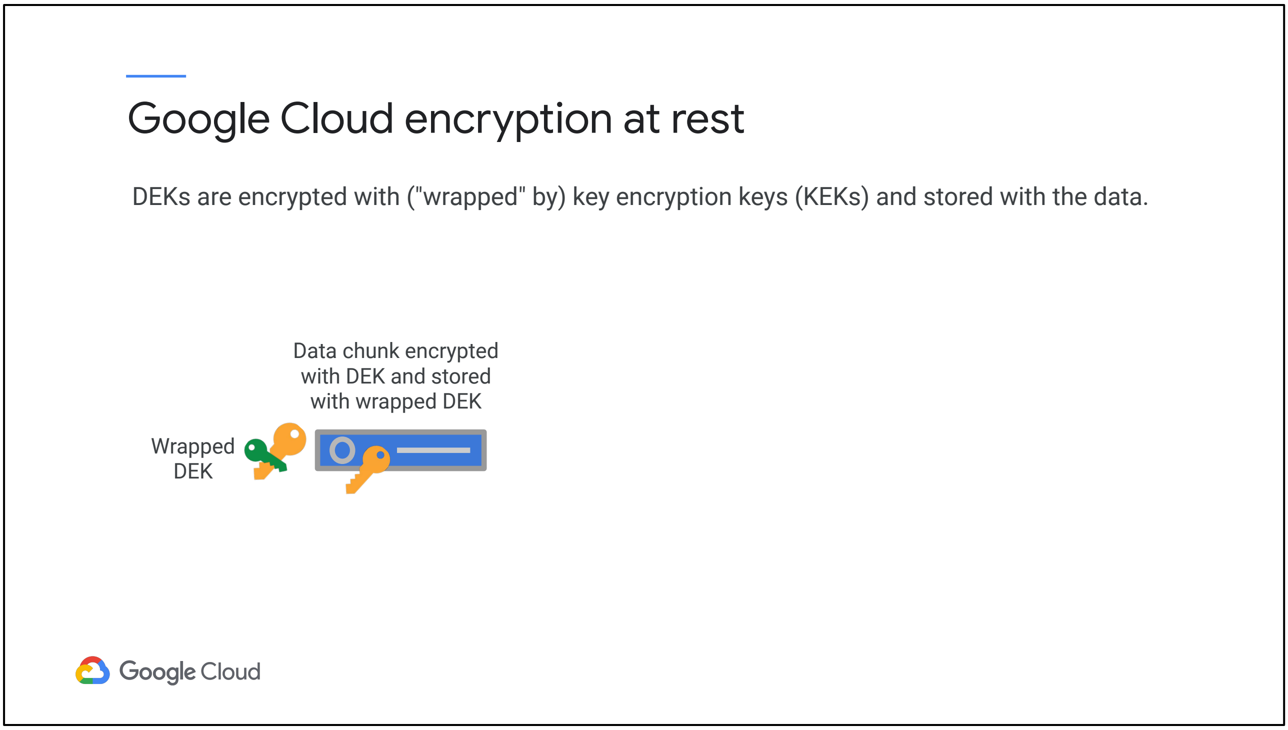
Let's have a closer look at how Google Cloud encrypts data at rest.

All data stored in Google Cloud is encrypted with a unique data encryption key or DEK.

More specifically, data is then broken into sub file chunks for storage; each chunk can be up to several gigabytes (GB) in size.

Each chunk of data is then encrypted at the storage level with a unique key. Note that two chunks will not have the same encryption key, even if they are part of the same Cloud Storage object, owned by the same customer, or stored on the same machine.

The encrypted data chunks are then distributed across Google's storage infrastructure. This partition of data, each using a different key, means the "blast radius" of a potential data encryption key compromise is limited to only that data chunk.



## Google Cloud encryption at rest

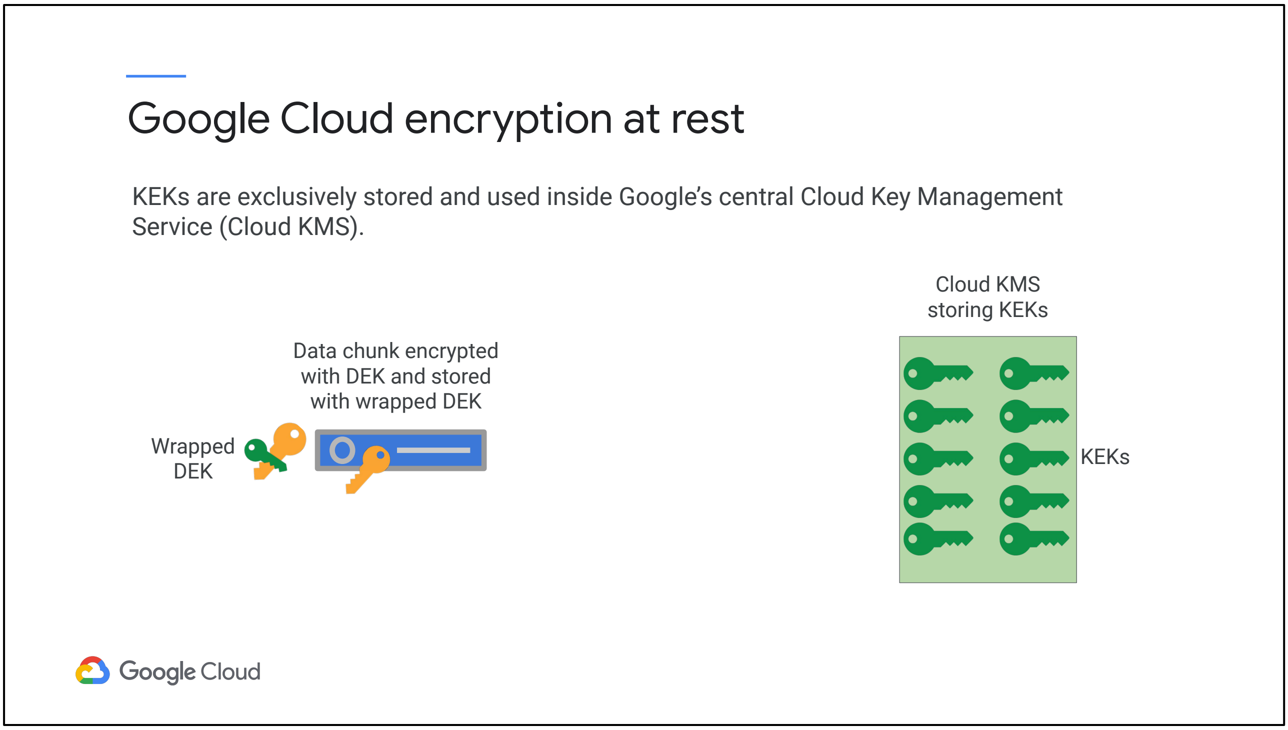
DEKs are encrypted with ("wrapped" by) key encryption keys (KEKs) and stored with the data.

Data chunk encrypted with DEK and stored with wrapped DEK

Wrapped DEK

Google Cloud

The data encryption keys are encrypted with (or “wrapped” by) key encryption keys, or KEKs. The wrapped data encryption keys are then stored with the data.



# Google Cloud encryption at rest

KEKs are exclusively stored and used inside Google’s central Cloud Key Management Service (Cloud KMS).

Data chunk encrypted with DEK and stored with wrapped DEK

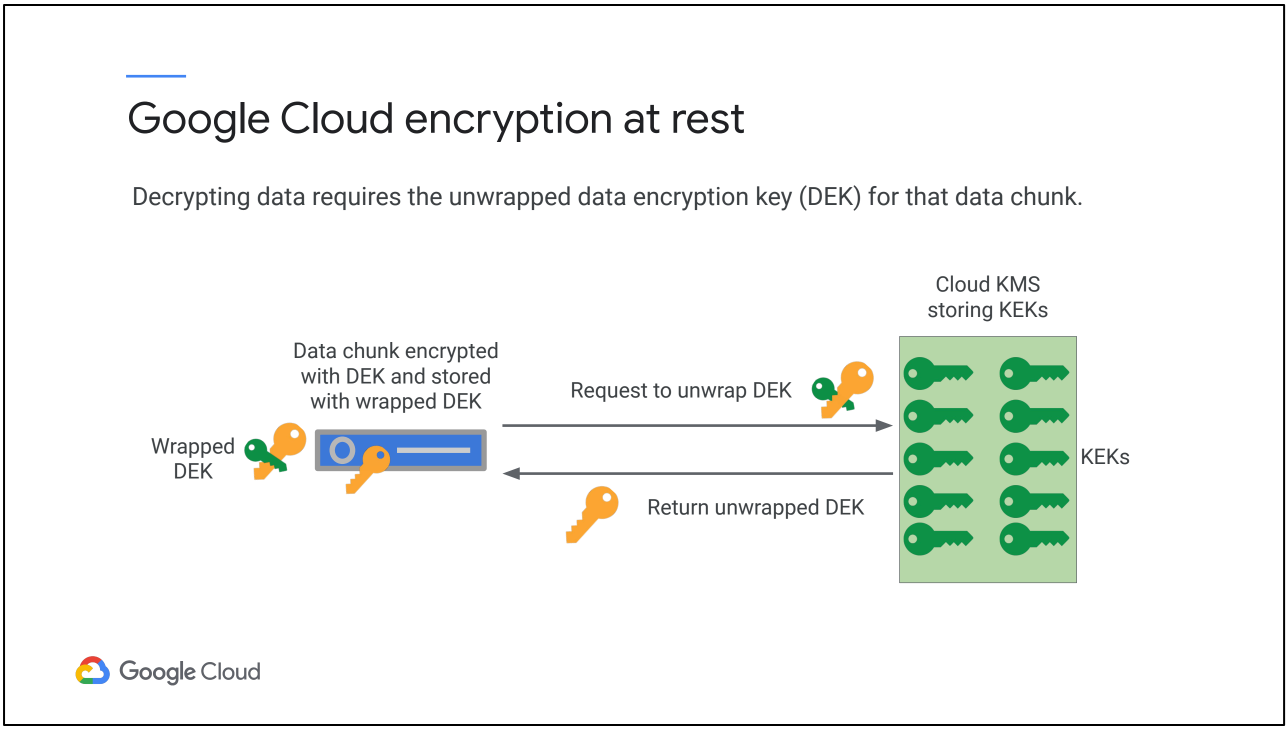
Wrapped DEK

Cloud KMS storing KEKs

KEKs

Google Cloud

The key encryption keys are exclusively stored and used inside Google’s central Cloud Key Management Service (or Cloud KMS). Cloud KMS-held keys are also backed up for disaster recovery purposes, and are indefinitely recoverable.



## Google Cloud encryption at rest

Decrypting data requires the unwrapped data encryption key (DEK) for that data chunk.

Cloud KMS storing KEKs

Data chunk encrypted with DEK and stored with wrapped DEK

Request to unwrap DEK

Wrapped DEK

KEKs

Return unwrapped DEK

Google Cloud

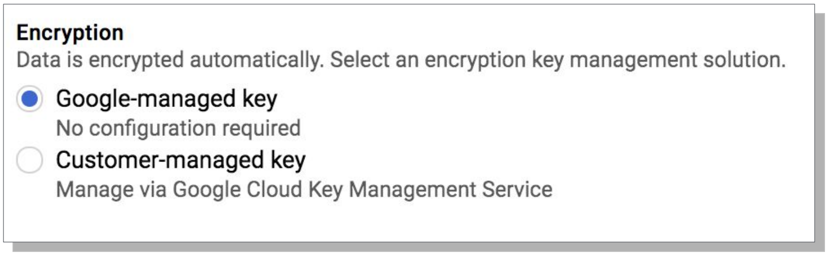
Decrypting data requires the unwrapped data encryption key (DEK) for that data chunk.

When a Google Cloud service accesses an encrypted chunk of data, here's what happens:

- For each chunk, the storage system pulls the wrapped DEK stored with that chunk, and calls Cloud KMS to retrieve the unwrapped data encryption key for that data chunk.
- Cloud KMS passes the unwrapped DEK back to the storage system, which then is able to decrypt the data chunk.

# Google Cloud encryption by default

- By default, KEKs are fully managed by Google.
- There is nothing to enable or configure.



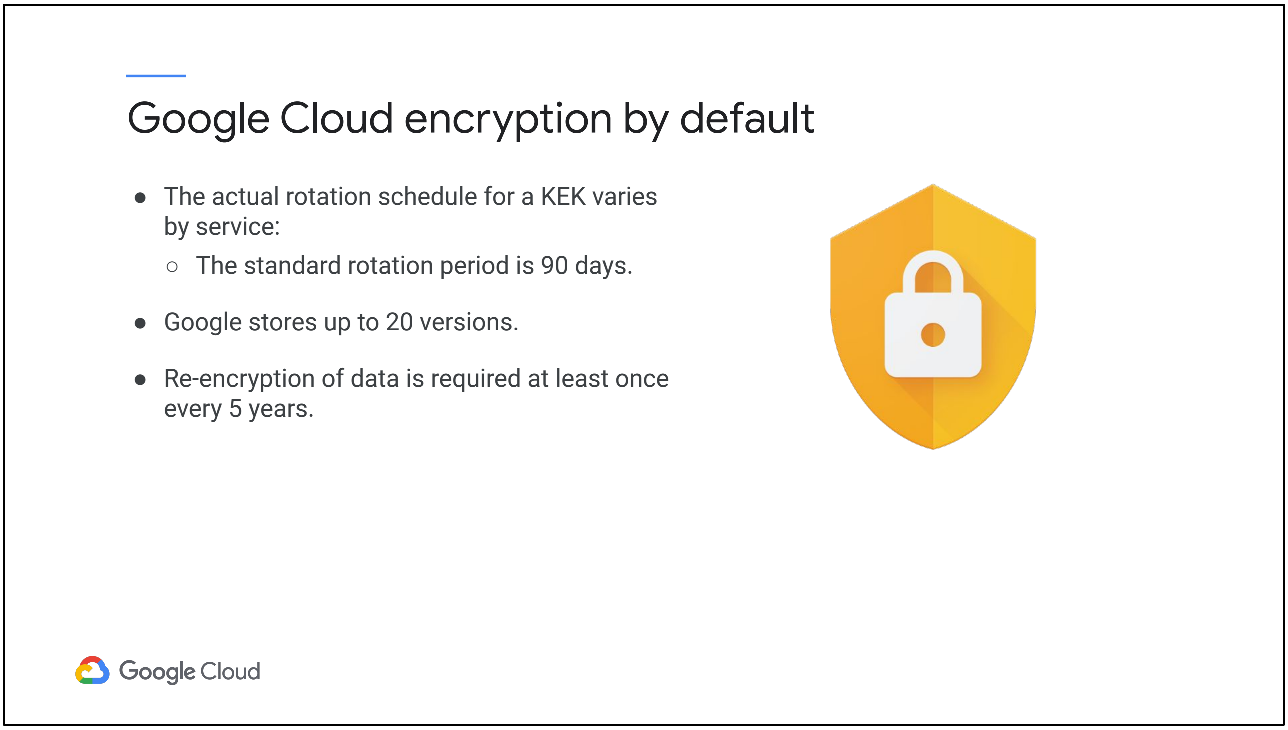
**Encryption**

Data is encrypted automatically. Select an encryption key management solution.

● Google-managed key
No configuration required

○ Customer-managed key
Manage via Google Cloud Key Management Service

By default, this entire process is enabled by default and is fully managed by Google - including the key encryption keys. There is absolutely nothing to enable or configure.



## Google Cloud encryption by default

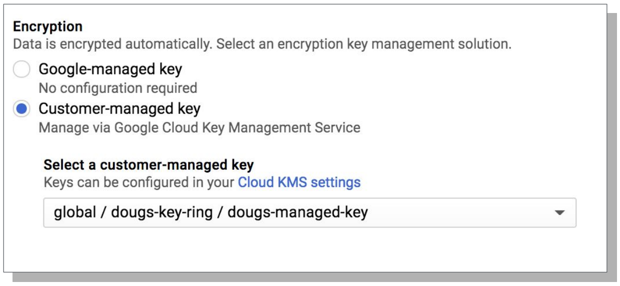
- The actual rotation schedule for a KEK varies by service:
  - The standard rotation period is 90 days.
- Google stores up to 20 versions.
- Re-encryption of data is required at least once every 5 years.

Google also manages the key rotation schedule. This schedule varies slightly depending on the service, but the standard rotation period for KEKs is every 90 days.

For example, Google Cloud Storage specifically rotates its KEKs every 90 days, and can store up to 20 versions, requiring re-encryption of data at least once every 5 years - though in practice, data re-encryption is much more frequent.

# Customer-managed keys

- Allows you to manage the KEKs:
  - Generate keys
  - Rotation periods
  - Expire keys
- KEKs still stored on Cloud KMS.



**Encryption**
Data is encrypted automatically. Select an encryption key management solution.

○ Google-managed key
No configuration required

● Customer-managed key
Manage via Google Cloud Key Management Service

**Select a customer-managed key**
Keys can be configured in your Cloud KMS settings

global / dougs-key-ring / dougs-managed-key ▾

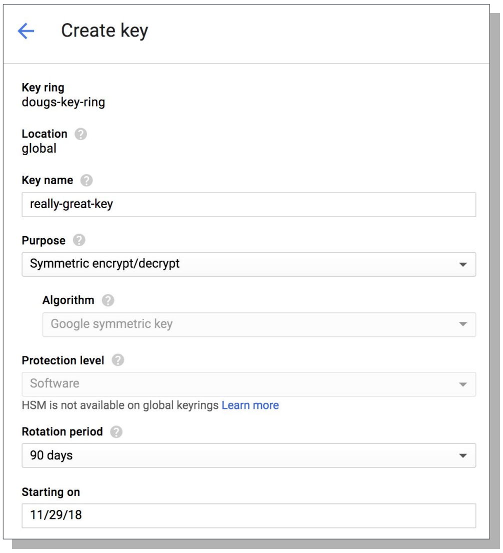
Google Cloud

You can control the generation of the keys, the rotation periods, and when to expire keys.

Customer managed keys are still stored in Cloud KMS, but you control of the keys' lifecycle.

# Creating keys with Cloud KMS

1. Create a key ring
2. Add a key
3. Specify type of key (symmetric, asymmetric, etc.)
4. Define rotation period



Create key

Key ring
dougs-key-ring

Location
global

Key name
really-great-key

Purpose
Symmetric encrypt/decrypt

Algorithm
Google symmetric key

Protection level
Software
HSM is not available on global keyrings Learn more

Rotation period
90 days

Starting on
11/29/18

Google Cloud

Cloud KMS uses an object hierarchy: a key belongs to a key ring, and a key ring resides in a particular location.

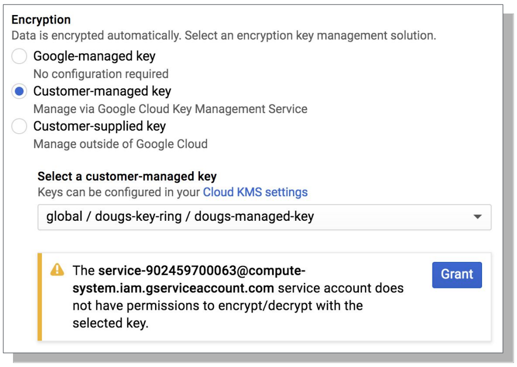
When creating keys, you must first create a key ring and specify its location, which can be regional, multi-regional, or global. A key can then be created and added to the key ring.

Note that Cloud KMS supports both symmetric and asymmetric key types.

The keys rotation period can also be defined to meet your requirements.

# Using customer-managed encryption keys

- Choose your managed key when creating VMs, disks, images, storage buckets, etc.
- Grant permissions to the service account to use your key.



**Encryption**

Data is encrypted automatically. Select an encryption key management solution.

○ Google-managed key
No configuration required

● Customer-managed key
Manage via Google Cloud Key Management Service

○ Customer-supplied key
Manage outside of Google Cloud

**Select a customer-managed key**

Keys can be configured in your Cloud KMS settings

global / dougs-key-ring / dougs-managed-key

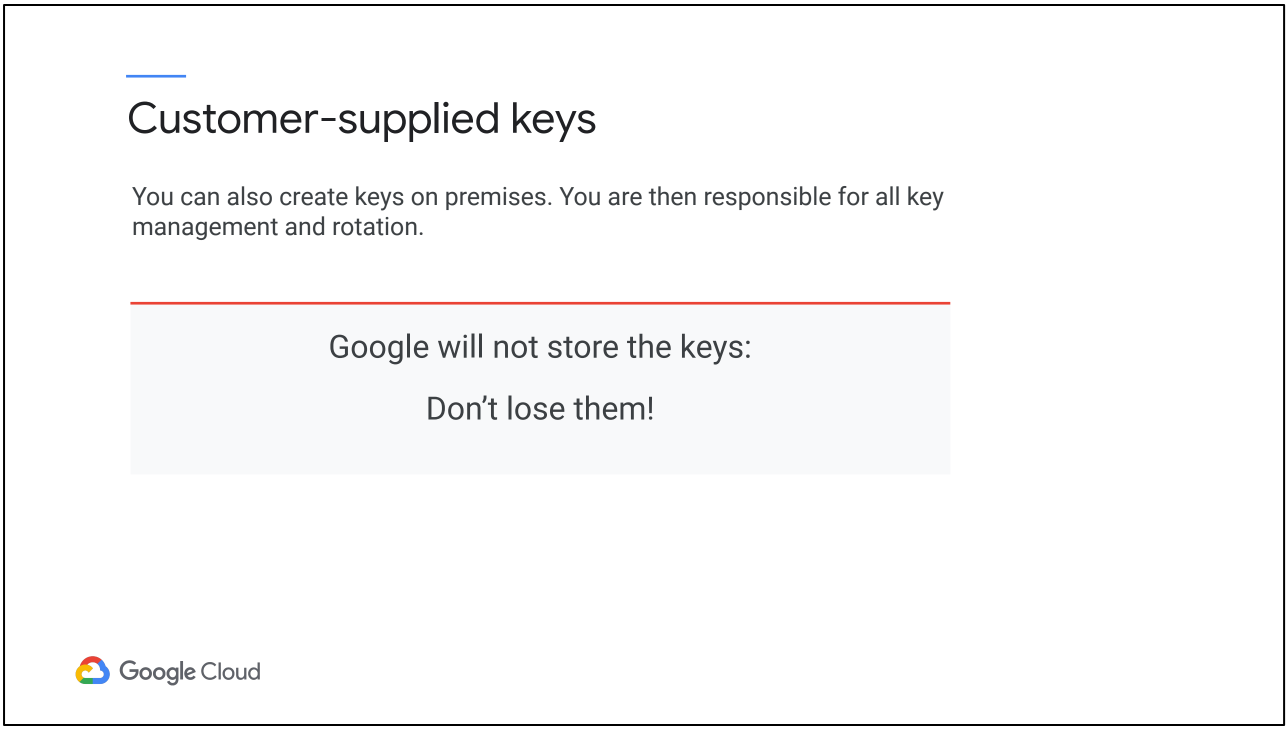
⚠ The **service-902459700063@compute-system.iam.gserviceaccount.com** service account does not have permissions to encrypt/decrypt with the selected key.

Google Cloud

Using customer-managed keys is as simple as choosing the key when creating VMs, disks, images, or storage buckets.

You also need to grant permissions to the service account to be able to use your key.

The general process is the same as when using the default Google managed keys.



## Customer-supplied keys

You can also create keys on premises. You are then responsible for all key management and rotation.

Google will not store the keys:

Don’t lose them!

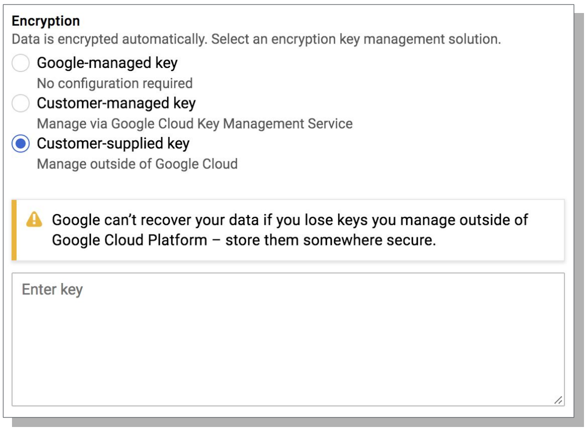
Another available option for encryption is customer-supplied keys. This allows you to create your keys yourself outside of Google Cloud, on your premises.

Remember, Google will not store these keys. You are responsible for ALL key management and rotation.

Be sure to not lose these keys. If you lose them, there will be no way to decrypt your data.

# Using customer-supplied encryption keys

You must provide the key when creating or using the storage resource.



**Encryption**

Data is encrypted automatically. Select an encryption key management solution.

○ Google-managed key
No configuration required

○ Customer-managed key
Manage via Google Cloud Key Management Service

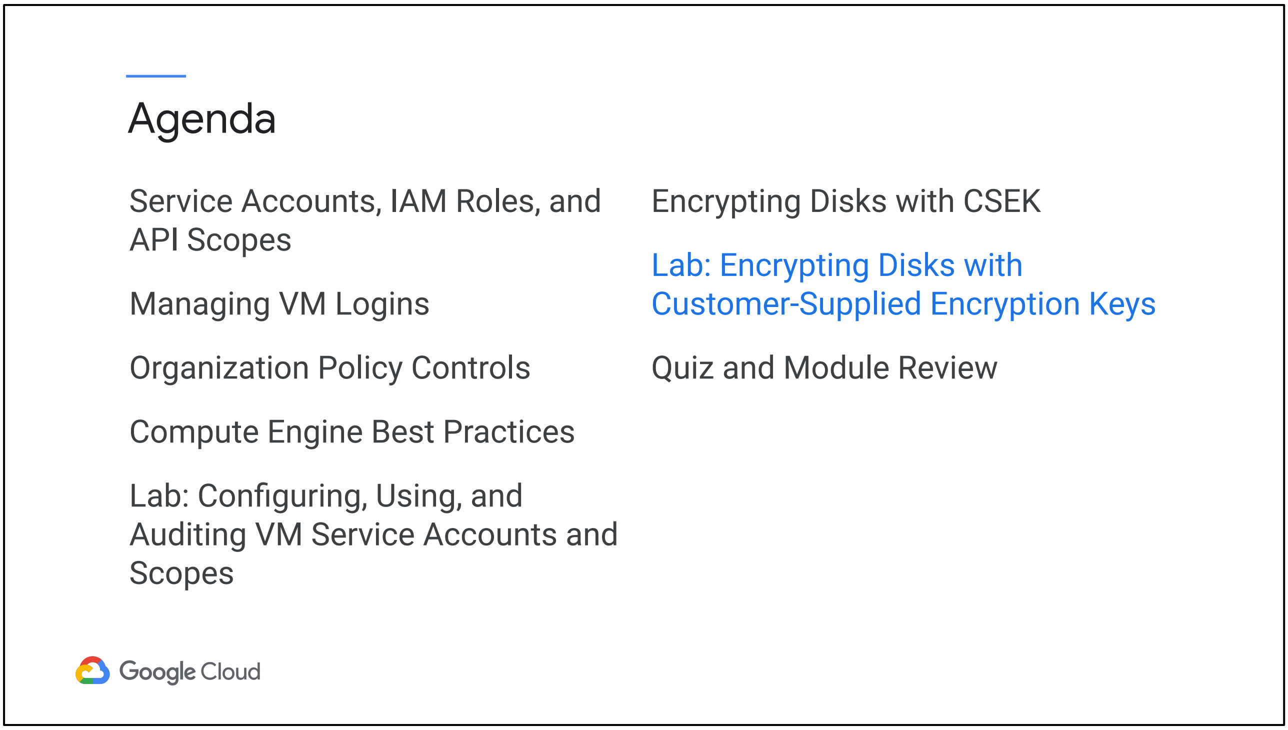
● Customer-supplied key
Manage outside of Google Cloud

⚠ Google can't recover your data if you lose keys you manage outside of Google Cloud Platform – store them somewhere secure.

Enter key

Google Cloud

When using customer-supplied encryption, since Google never stores the keys, you must provide the appropriate key whenever creating or using the storage resource. For example, if a persistent disk is created with a customer-supplied encryption key, that key must be specified each time the disk is attached to an instance.



# Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

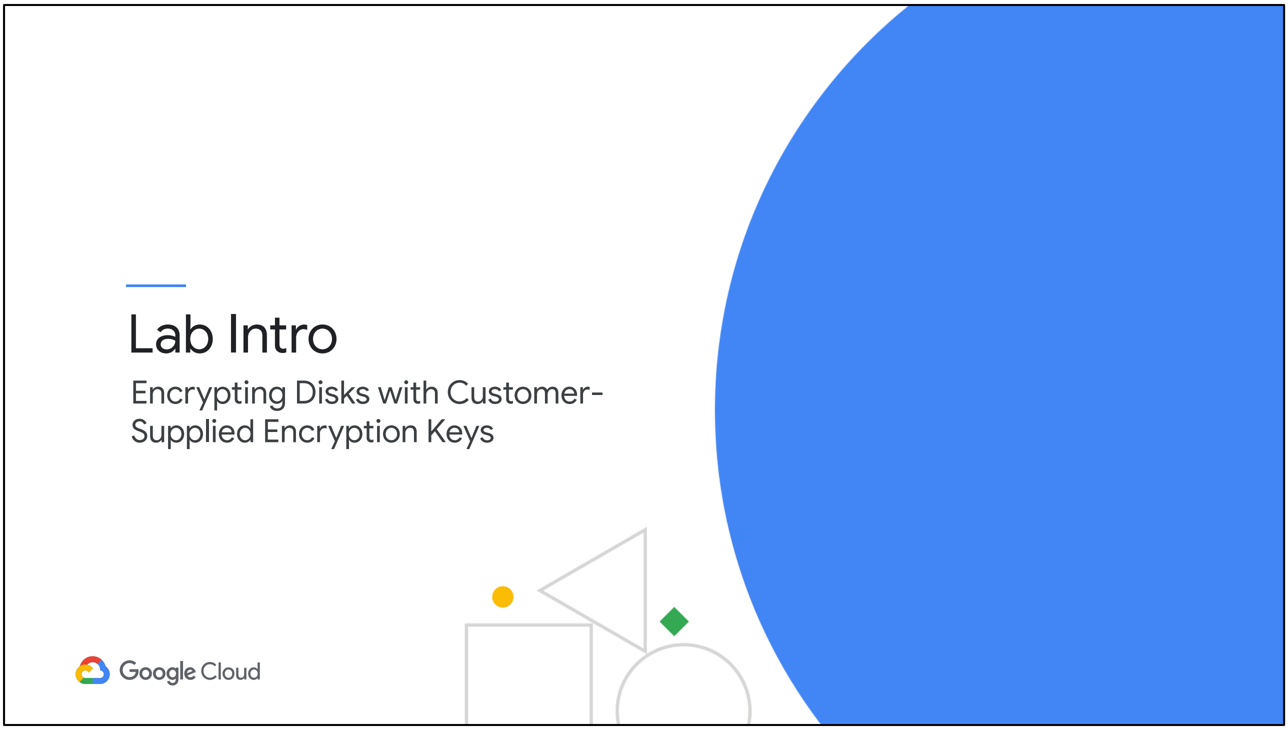
Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review



## Lab Intro

Encrypting Disks with Customer-Supplied Encryption Keys

Google Cloud

OK, now you will get a chance to practice encrypting disks with customer-supplied encryption keys.

In this lab, you learn how to perform the following tasks:

- Create an encryption key and wrap it with the “Google Compute Engine” RSA public key certificate
- Encrypt a new persistent disk with your own key
- Attach the disk to an compute engine instance
- Create a snapshot from an encrypted disk

# Agenda

Service Accounts, IAM Roles, and API Scopes

Managing VM Logins

Organization Policy Controls

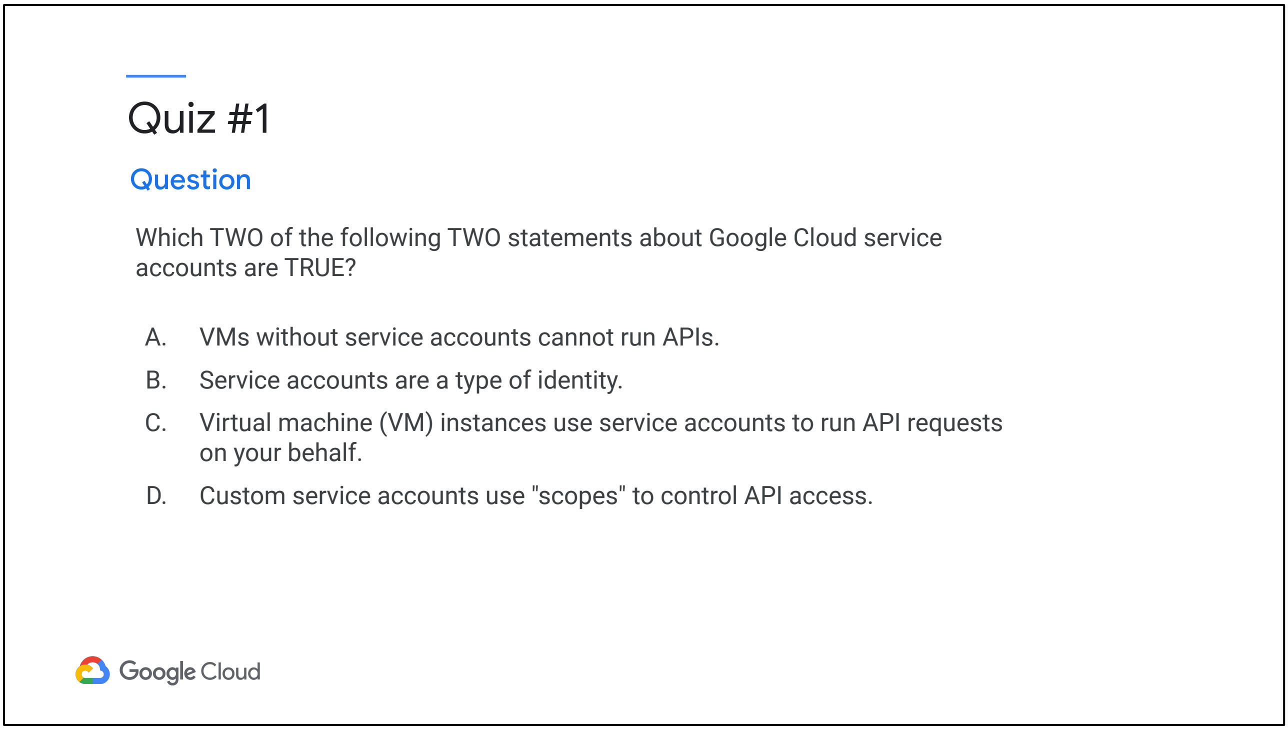
Compute Engine Best Practices

Lab: Configuring, Using, and Auditing VM Service Accounts and Scopes

Encrypting Disks with CSEK

Lab: Encrypting Disks with Customer-Supplied Encryption Keys

Quiz and Module Review



# Quiz #1

## Question

Which TWO of the following TWO statements about Google Cloud service accounts are TRUE?

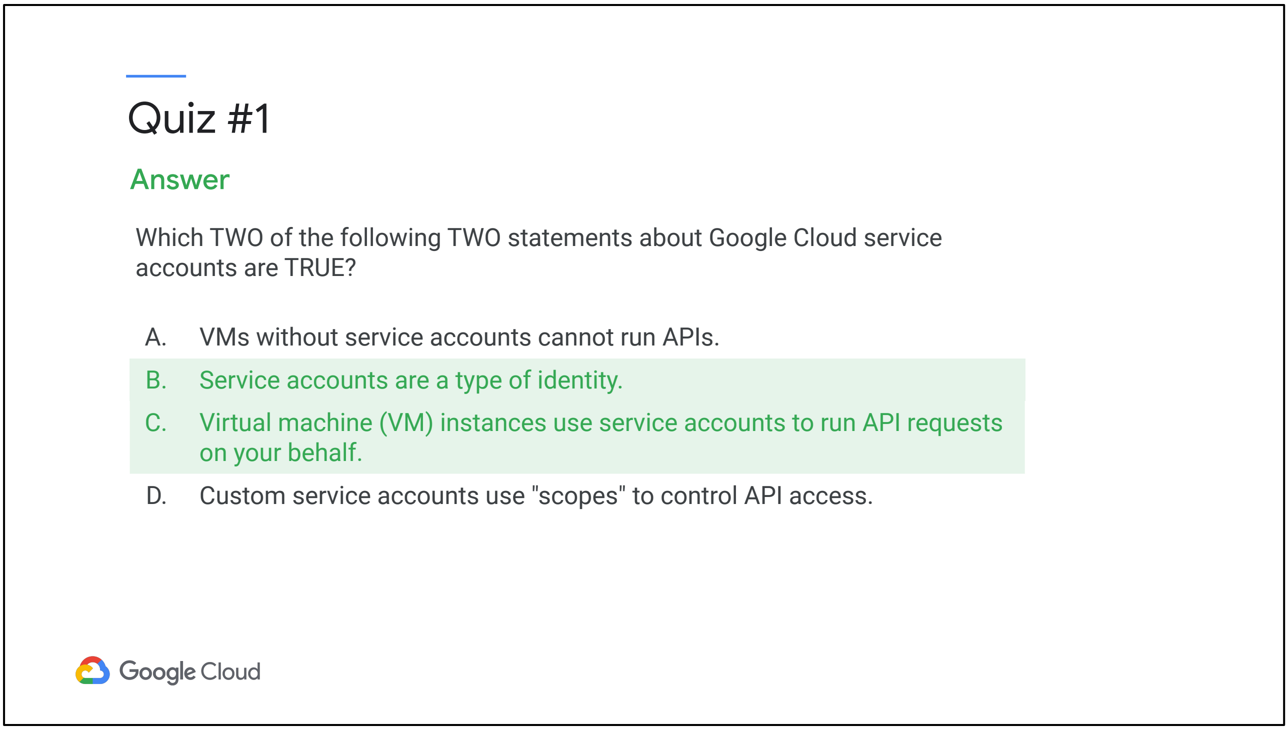
A. VMs without service accounts cannot run APIs.

B. Service accounts are a type of identity.

C. Virtual machine (VM) instances use service accounts to run API requests on your behalf.

D. Custom service accounts use "scopes" to control API access.

Google Cloud



## Quiz #1

### Answer

Which TWO of the following TWO statements about Google Cloud service accounts are TRUE?

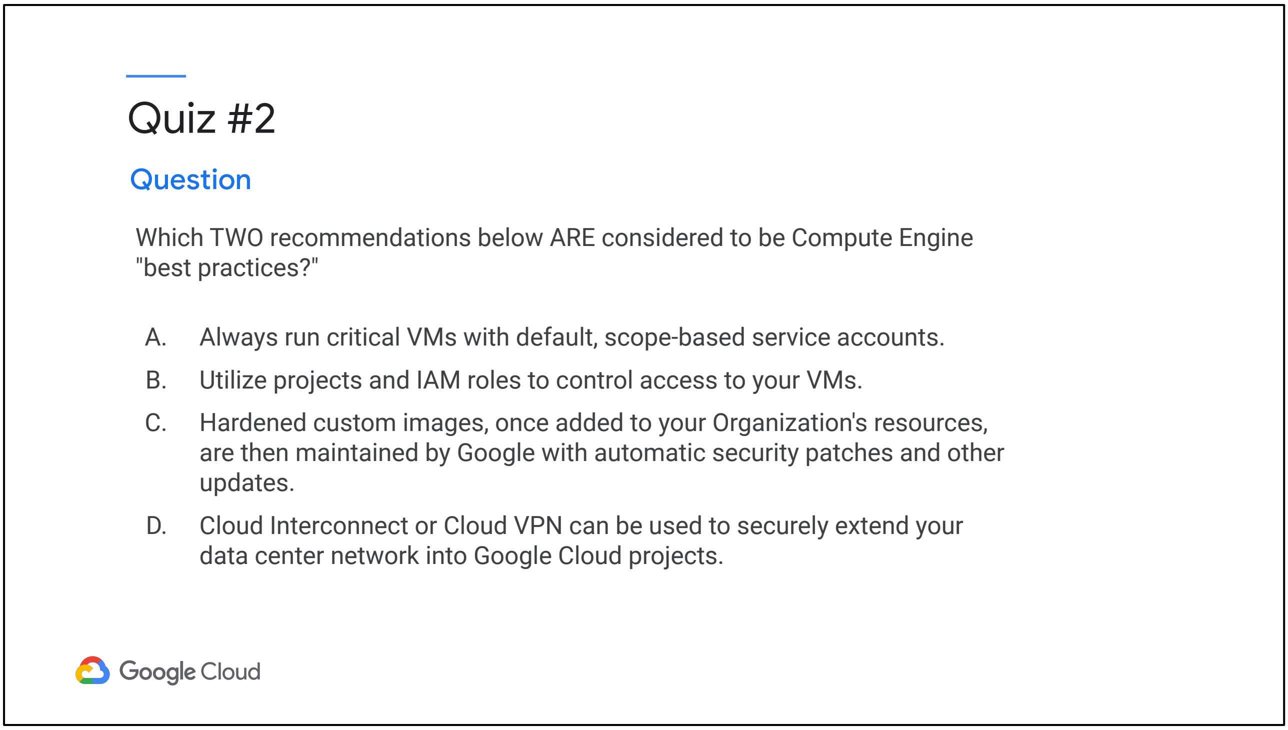
A. VMs without service accounts cannot run APIs.

B. Service accounts are a type of identity.

C. Virtual machine (VM) instances use service accounts to run API requests on your behalf.

D. Custom service accounts use "scopes" to control API access.

B. VMs authenticate using the identity of a service account when making calls to the Google APIs.
C. When launching a virtual machine in Compute Engine, a service account can be associated directly to that VM.



# Quiz #2

## Question

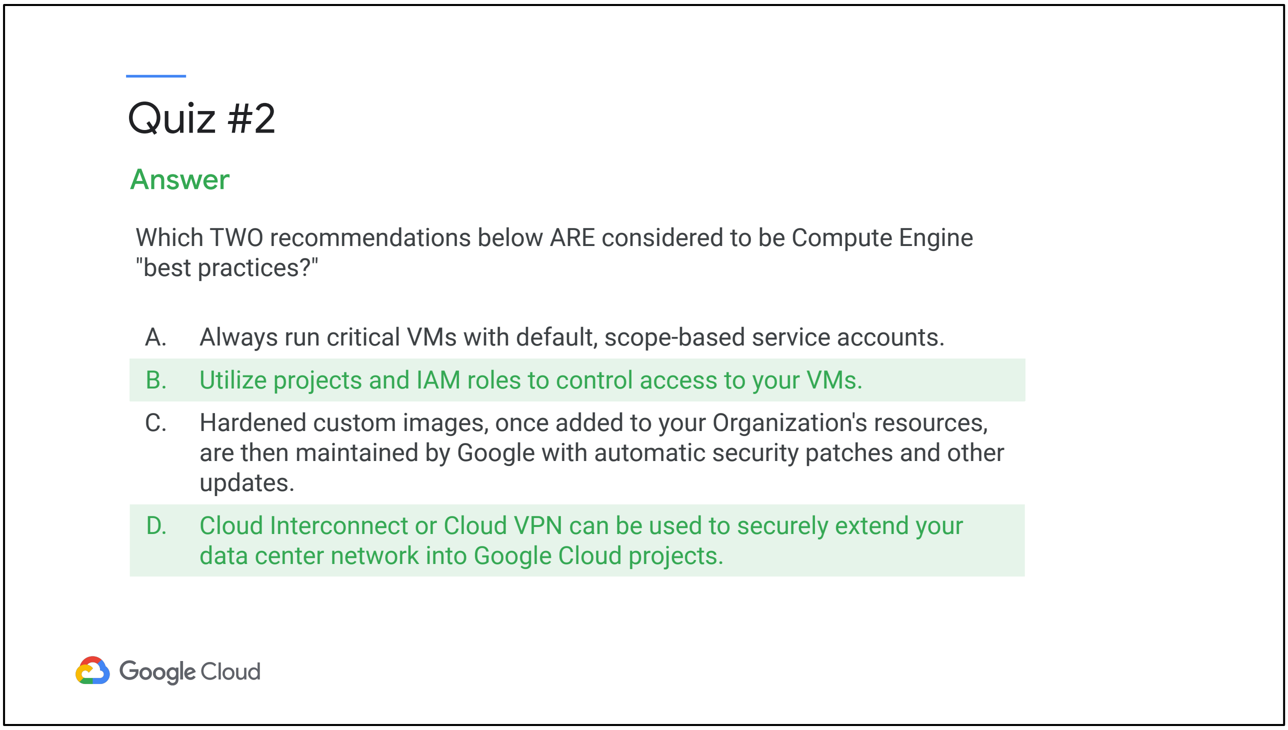
Which TWO recommendations below ARE considered to be Compute Engine "best practices?"

A. Always run critical VMs with default, scope-based service accounts.

B. Utilize projects and IAM roles to control access to your VMs.

C. Hardened custom images, once added to your Organization's resources, are then maintained by Google with automatic security patches and other updates.

D. Cloud Interconnect or Cloud VPN can be used to securely extend your data center network into Google Cloud projects.



## Quiz #2

### Answer

Which TWO recommendations below ARE considered to be Compute Engine "best practices?"

A. Always run critical VMs with default, scope-based service accounts.

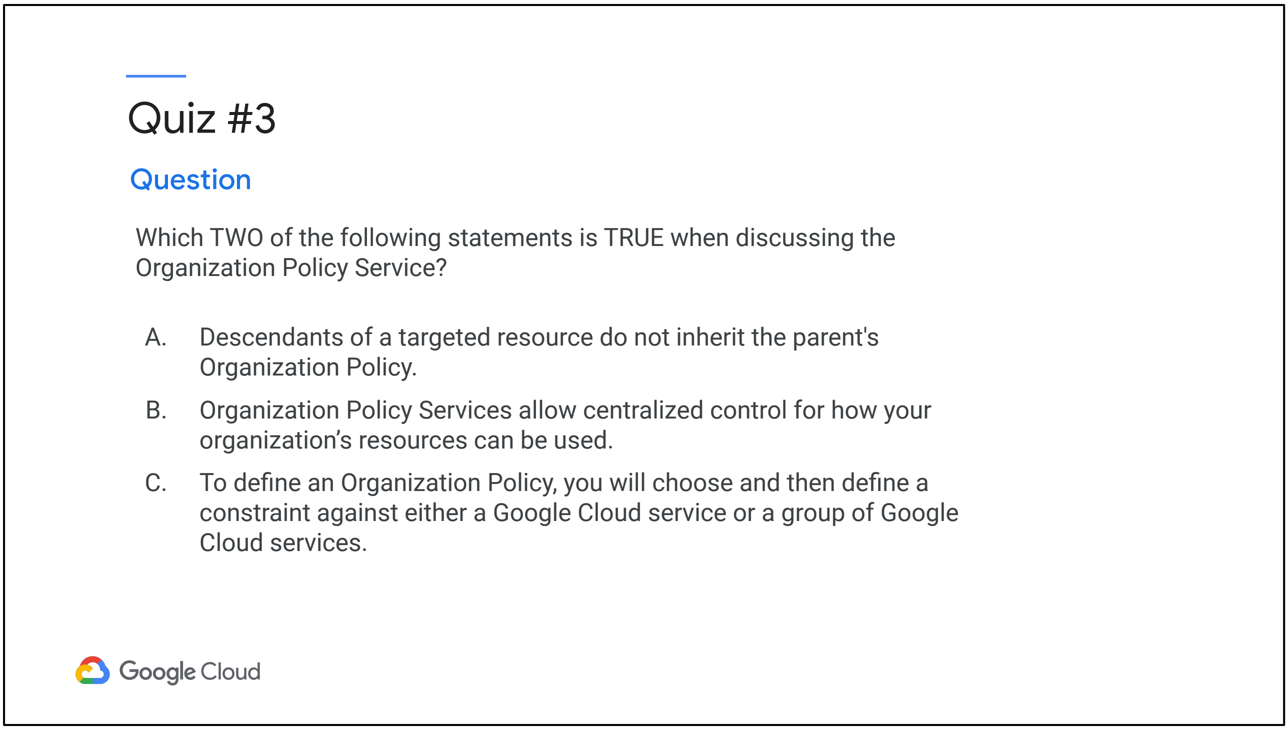
B. Utilize projects and IAM roles to control access to your VMs.

C. Hardened custom images, once added to your Organization's resources, are then maintained by Google with automatic security patches and other updates.

D. Cloud Interconnect or Cloud VPN can be used to securely extend your data center network into Google Cloud projects.

Google Cloud

B. Projects form the basis for creating, enabling, and using all Google Cloud services including managing permissions for Google Cloud resources.
D. Using these services to extend your on-prem resources into the cloud helps to make your hybrid network more secure and reliable.



# Quiz #3

## Question

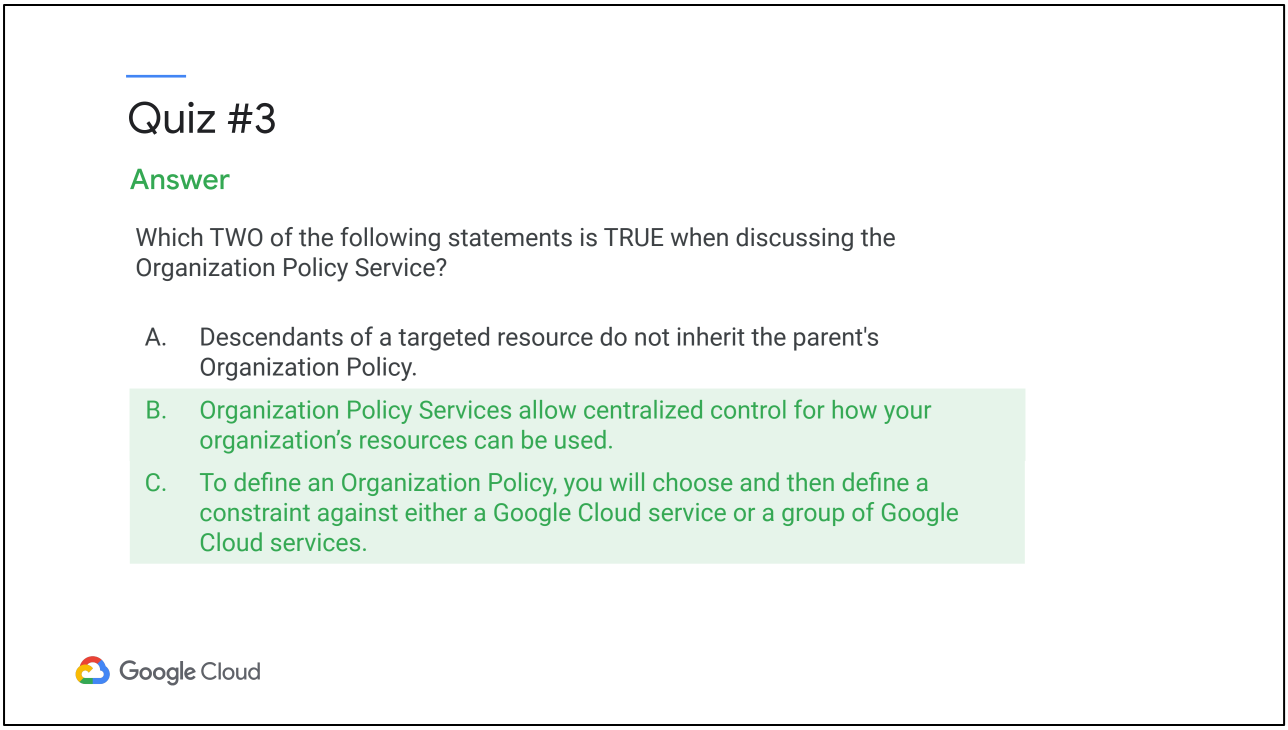
Which TWO of the following statements is TRUE when discussing the Organization Policy Service?

A. Descendants of a targeted resource do not inherit the parent's Organization Policy.

B. Organization Policy Services allow centralized control for how your organization’s resources can be used.

C. To define an Organization Policy, you will choose and then define a constraint against either a Google Cloud service or a group of Google Cloud services.

Google Cloud



## Quiz #3

Answer

Which TWO of the following statements is TRUE when discussing the Organization Policy Service?

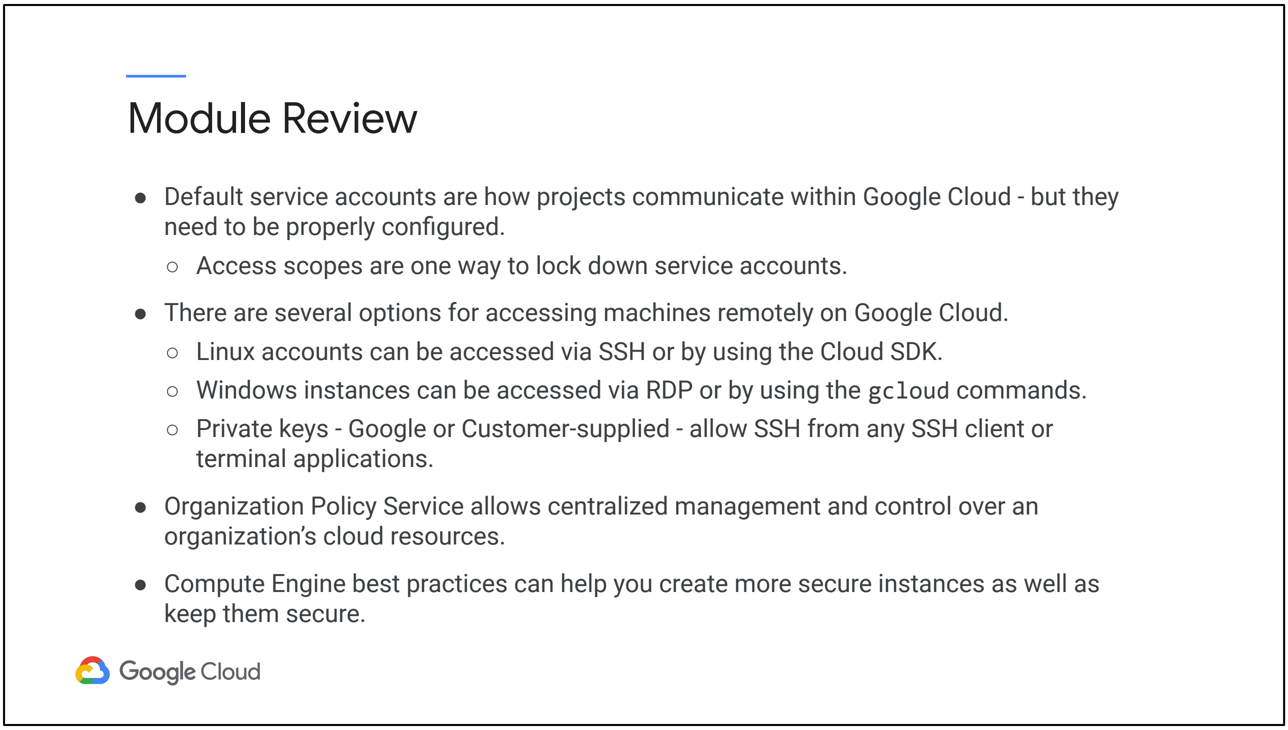
A. Descendants of a targeted resource do not inherit the parent's Organization Policy.

B. Organization Policy Services allow centralized control for how your organization’s resources can be used.

C. To define an Organization Policy, you will choose and then define a constraint against either a Google Cloud service or a group of Google Cloud services.

Google Cloud

B. Organization Policy Service gives you both centralized and programmatic control over your organization's cloud resources.
C. Organization Policy Service allows you to set constraints that apply to all resources in your organization's hierarchy.



## Module Review

- Default service accounts are how projects communicate within Google Cloud - but they need to be properly configured.
  - Access scopes are one way to lock down service accounts.
- There are several options for accessing machines remotely on Google Cloud.
  - Linux accounts can be accessed via SSH or by using the Cloud SDK.
  - Windows instances can be accessed via RDP or by using the `gcloud` commands.
  - Private keys - Google or Customer-supplied - allow SSH from any SSH client or terminal applications.
- Organization Policy Service allows centralized management and control over an organization's cloud resources.
- Compute Engine best practices can help you create more secure instances as well as keep them secure.

Google Cloud

Before we move to the next module, let's review some key concepts from this one.

**Default service accounts** are how projects communicate within Google Cloud - but they need to be properly configured

- Every Google Cloud project has a default service account that is automatically created when compute engine is first enabled for the project.
- This default service account is assigned the "**project editor role"** and is used by default when launching VMs.
- You can also create and manage your own service accounts using Google Identity and Access Management.

**Access scopes** provide the ability to limit what permissions are allowed when using the default service account with IAM Project Editor role permissions

- You set access scopes when creating an instance and the access scopes persists only for the life of that instance.
- Another option is to set the access for each API individually, which allows you to grant access to only to the APIs required by the programs running on the VM.

**There are several options for accessing machines remotely on Google Cloud**

- By default, Linux instances on Google Cloud are accessed with SSH and require a username and an SSH key for authentication. Password authentication is disabled by default.  It is also possible to connect to a Linux instance via SSH using the gcloud SDK.

- Window instances are accessed using RDP and require a username and password to authenticate. The username and password can be set from the Cloud Console or using gcloud.
- It is also possible to SSH from any SSH client such as PuTTY on Windows or ssh applications on Linux or Mac computer using the public IP address of the instance, a valid username and SSH private key. You can manually create your own SSH key pairs, using tools like PuTTYgen or ssh-keygen.

The **Organization Policy Service** gives you centralized and programmatic control over your organization's cloud resources.

- An organization policy administrator can configure restrictions across your entire resource hierarchy.
- A constraint is a particular type of restriction (List or Boolean) against a Google Cloud service or a list of Google Cloud services.

**Compute Engine best practices** can help you create more secure instances as well as keep them secure.
Compute Engine best practices include: control access, isolate machines, connect securely and regularly monitor and audit logs.
In addition, be sure to keep instances updated, and avoid using the default service account, especially if it is unmodified.

Ok, we are now ready to move on to the next module!

Google Cloud