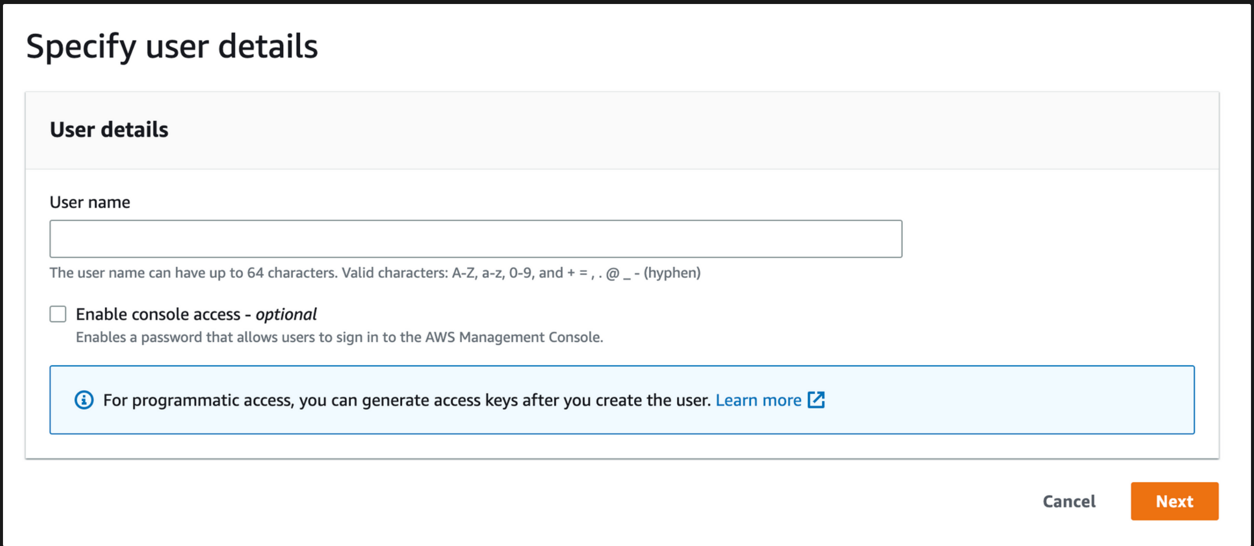
Steps to implement Hands-on Project - Mission 1

Amazon Web Services

- Access AWS console and go to IAM service
- Under Access management, Click in "Users", then "Add users". Insert the User name **terraform-en-1** and click in **Next** to create a programmatic user.



Specify user details

User details

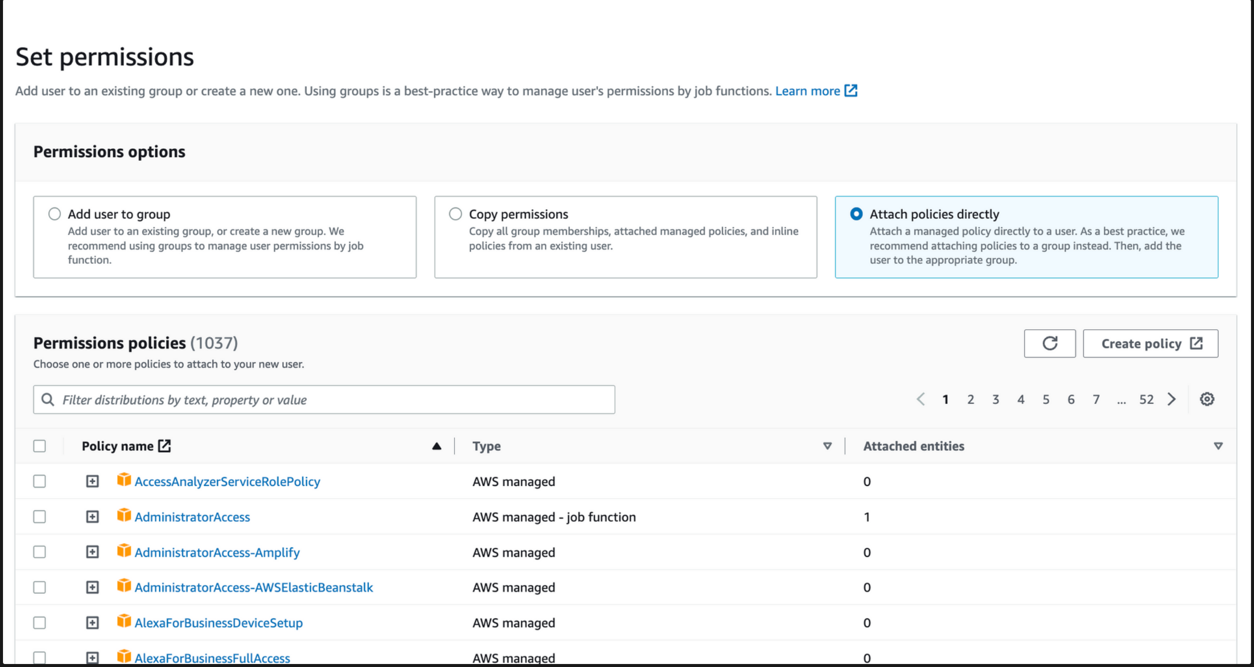
User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ Enable console access - *optional*
Enables a password that allows users to sign in to the AWS Management Console.

ⓘ For programmatic access, you can generate access keys after you create the user. Learn more

- On Set permissions, Permissions options, click in "Attach policies directly" button.



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

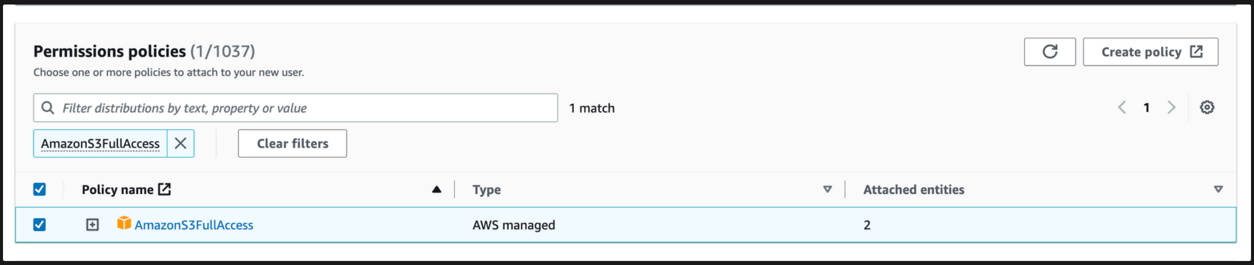
Permissions policies (1037)

Choose one or more policies to attach to your new user.

□	Policy name	Type	Attached entities
□	AccessAnalyzerServiceRolePolicy	AWS managed	0
□	AdministratorAccess	AWS managed - job function	1
□	AdministratorAccess-Amplify	AWS managed	0
□	AdministratorAccess-AWSElasticBeanstalk	AWS managed	0
□	AlexaForBusinessDeviceSetup	AWS managed	0
□	AlexaForBusinessFullAccess	AWS managed	0

- Type **AmazonS3FullAccess** in **Filter distributions by text, property or value**, press Enter.

- Select AmazonS3FullAccess



Permissions policies (1/1037)

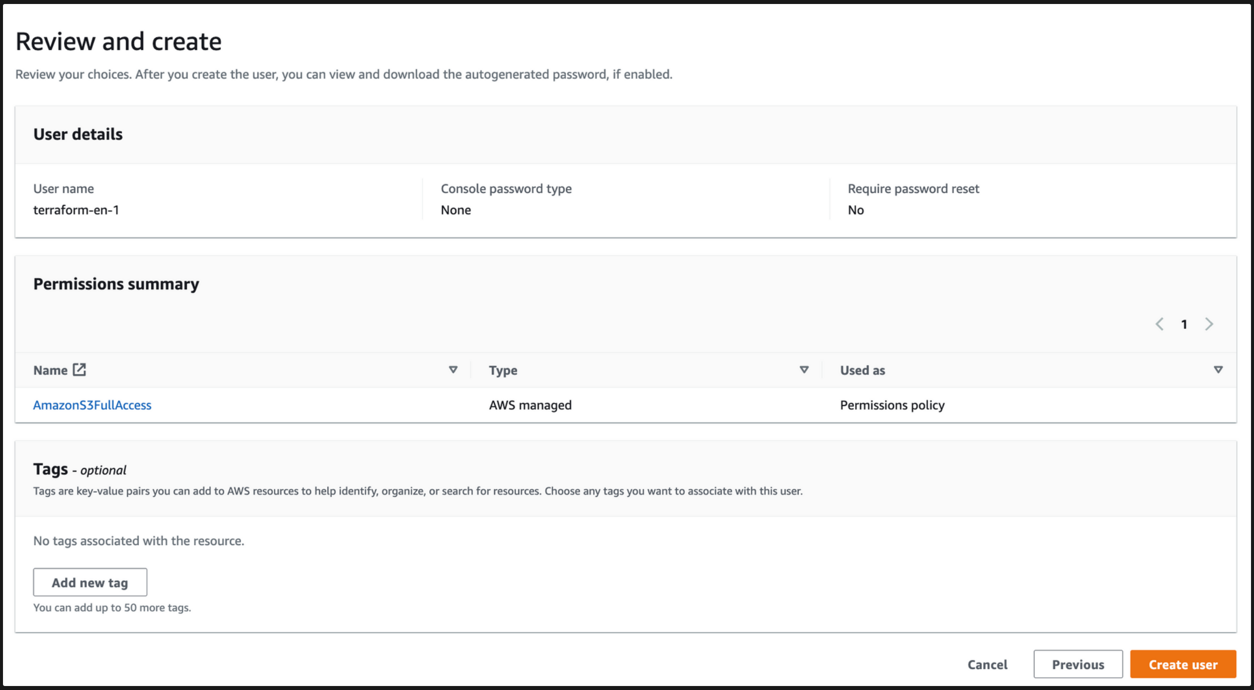
Choose one or more policies to attach to your new user.

Filter distributions by text, property or value — 1 match

AmazonS3FullAccess ✕ | Clear filters

☑	Policy name	Type	Attached entities
☑	AmazonS3FullAccess	AWS managed	2

- Click in Next
- Review all details



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
terraform-en-1	None	No

Permissions summary

Name	Type	Used as
AmazonS3FullAccess	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

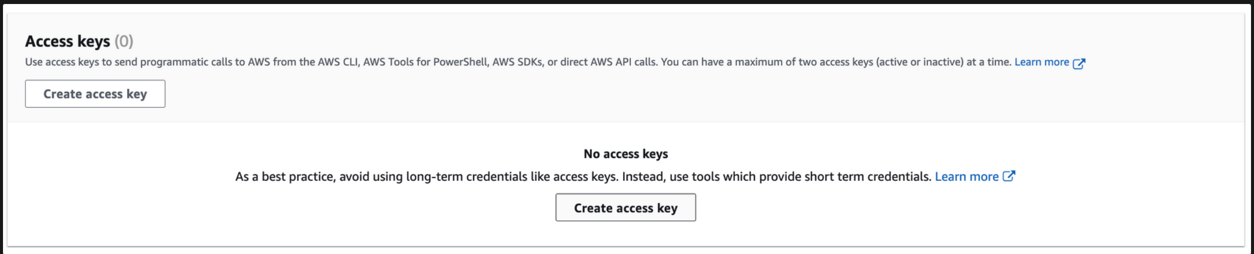
Add new tag

You can add up to 50 more tags.

- Click in Create user

[NEW] AWS has recently changed the way to download the key. Follow the new steps:

- Click on the user you have created.
- Click on Security credentials.
- Scroll down and go to Access keys section.
- Click on Create access key



Access keys (0)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

Create access key

No access keys

As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. Learn more

Create access key

- Select **Command Line Interface (CLI)** and **I understand the above recommendation and want to proceed to create an access key** checkbox.
- Click Next
- Click on Create access key

- Click on Download .csv file

▼ [TIP] Access key best practices

  - Never store your access key in plain text, in a code repository, or in code.
  - Disable or delete access key when no longer needed.
  - Enable least-privilege permissions.
  - Rotate access keys regularly.

- After download, click Done.
- Now, rename .csv file downloaded to accessKeys.csv

Google Cloud Platform (GCP)

- CLICK HERE to download the hands-on files.
- Access GCP Console and open Cloud Shell
- Upload accessKeys.csv and .zip hands-on file to GCP Cloud Shell
- Hands-on files preparation

```
mkdir mission1_en mv mission1.zip mission1_en cd mission1_en unzip
mission1.zip mv ~/accessKeys.csv mission1/en cd mission1/en chmod +x *.sh
```

- Run the following commands to prepare AWS and GCP environment. Authorize when asked.

```
./aws_set_credentials.sh accessKeys.csv gcloud config set project
<project_id>
```

- Execute the command below

```
./gcp_set_project.sh
```

- Enable the Container Registry API, Kubernetes Engine API and the Cloud SQL API

```
gcloud services enable containerregistry.googleapis.com gcloud services
enable container.googleapis.com gcloud services enable
sqladmin.googleapis.com
```

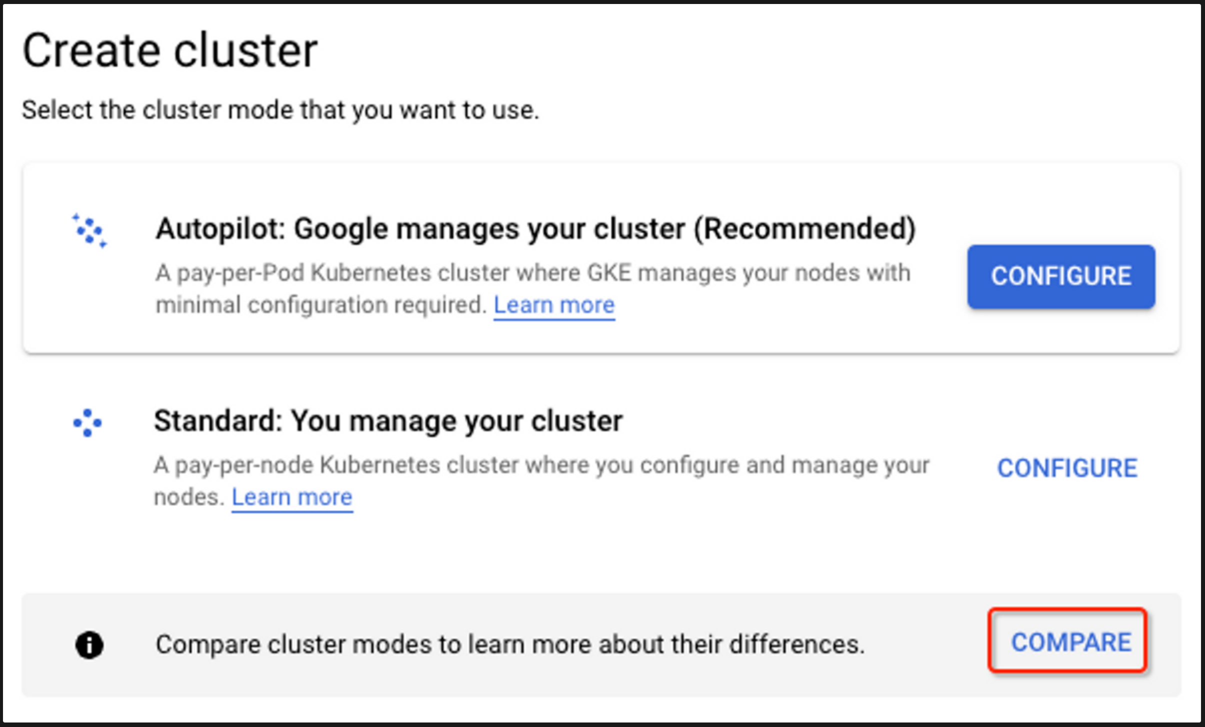
IMPORTANT (DO NOT SKIP):

- **Before executing the Terraform commands, open the Google Editor and update the file tcb_aws_storage.tf replacing the bucket name with an unique name (AWS requires unique bucket names).**
  - Open the tcb_aws_storage.tf using Google Editor
  - On line 4 of the file tcb_aws_storage.tf:
    - Replace xxxx with your name initials plus two random numbers: Example: luxxy-covid-testing-system-pdf-en-jr29

- Run the following commands to finish provision infrastructure steps

```
cd ~/mission1_en/mission1/en/terraform/ terraform init terraform plan
terraform apply Type Yes and go ahead.
```

💡 After access the GKE Service to create a cluster, click on the **Compare** button to “**Compare cluster modes to learn more about their differences**”.



Create cluster

Select the cluster mode that you want to use.

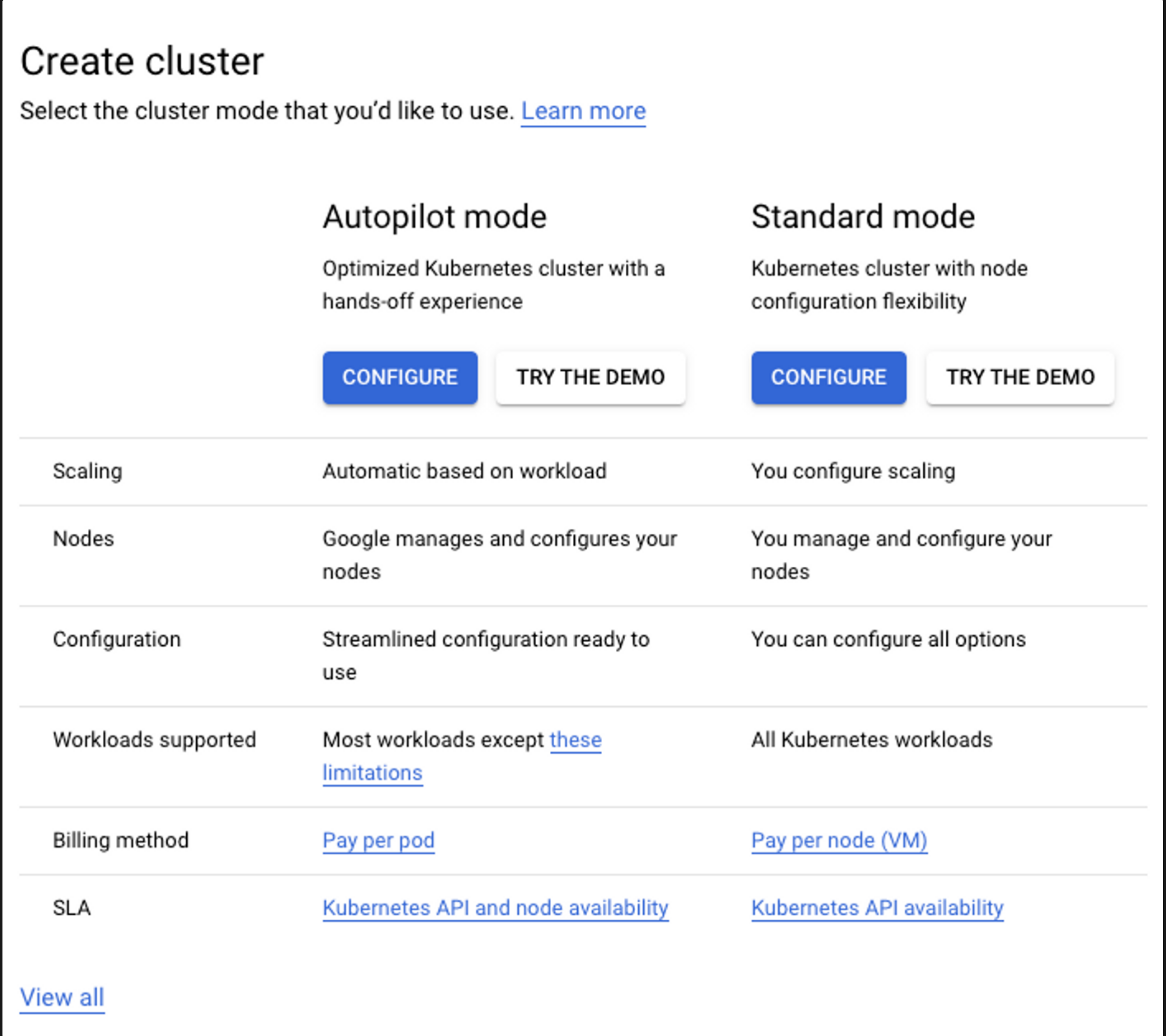
Autopilot: Google manages your cluster (Recommended)

A pay-per-Pod Kubernetes cluster where GKE manages your nodes with minimal configuration required. Learn more

Standard: You manage your cluster

A pay-per-node Kubernetes cluster where you configure and manage your nodes. Learn more

Compare cluster modes to learn more about their differences.



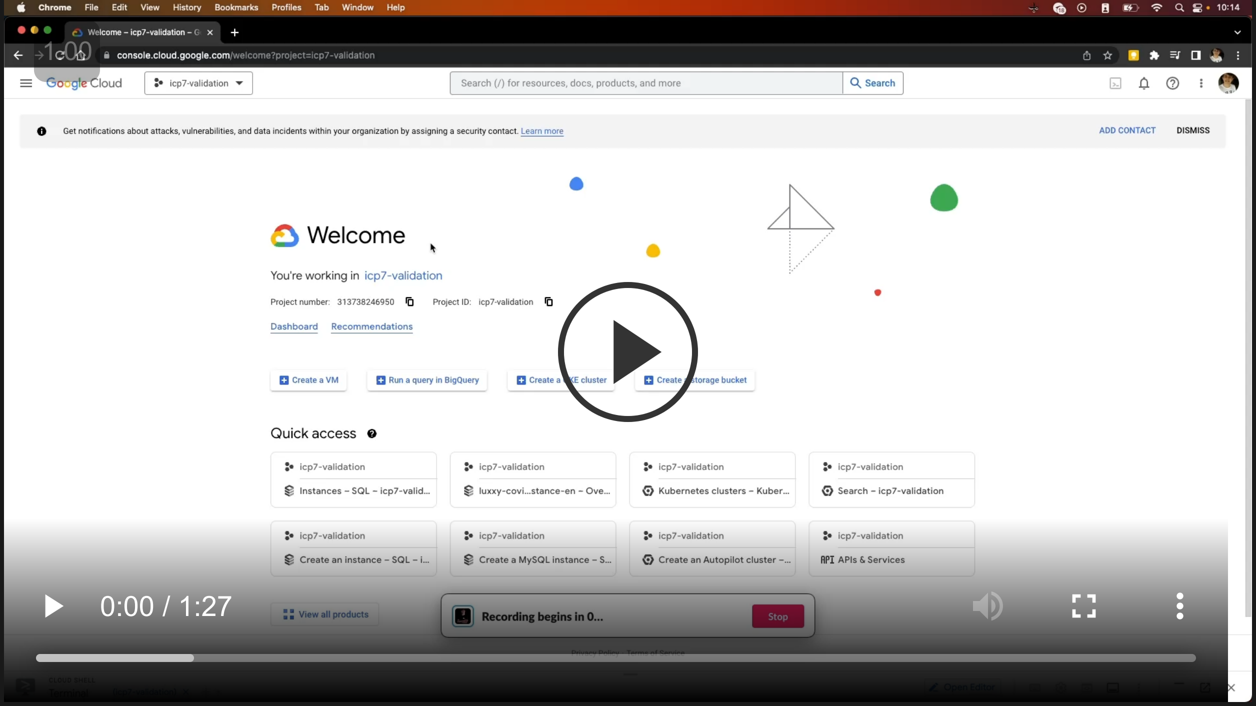
Create cluster

Select the cluster mode that you'd like to use. Learn more

	Autopilot mode	Standard mode
	Optimized Kubernetes cluster with a hands-off experience	Kubernetes cluster with node configuration flexibility
Scaling	Automatic based on workload	You configure scaling
Nodes	Google manages and configures your nodes	You manage and configure your nodes
Configuration	Streamlined configuration ready to use	You can configure all options
Workloads supported	Most workloads except these limitations	All Kubernetes workloads
Billing method	Pay per pod	Pay per node (VM)
SLA	Kubernetes API and node availability	Kubernetes API availability

💡 Download Visual Studio Code used by Jean during the Training HERE

SQL Network Configuration



Get notifications about attacks, vulnerabilities, and data incidents within your organization by assigning a security contact. Learn more

Welcome

You're working in icp7-validation

Project number: 313738246950 Project ID: icp7-validation

console.cloud.google.com/welcome?project=icp7-validation
Google Cloud
icp7-validation
Search (/) for resources, docs, products, and more
Search
ADD CONTACT
DISMISS
Dashboard
Recommendations
Create a VM
Run a query in BigQuery
Create a GKE cluster
Create a storage bucket
Quick access
Instances – SQL – icp7-valid...
luxxy-covi...stance-en – Ove...
Kubernetes clusters – Kuber...
Search – icp7-validation
Create an instance – SQL – i...
Create a MySQL instance – S...
Create an Autopilot cluster –...
APIs & Services
View all products
Recording begins in 0...
Stop
0:00 / 1:27

- Once the Cloud SQL instance is provisioned, access the Cloud SQL service
- Click on your Cloud SQL instance.
- On the left side, under Primary Instance, click on **Connections**.
- Under **Instance IP assignment**, enable Private IP.
  - Under **Associated networking**, select "Default"
  - Click **Set up Connection**
  - Enable Service Networking API (if asked)
  - Select **Use an automatically allocated IP range in your network**.
  - Click **Continue**
  - Click **Create Connection** and **wait a minutes.**
- Under **Authorized Networks**, click "Add Network".
- Under **New Network**, enter the following information:
  - **Name:** Public Access (For testing purposes only)
  - **Network**: 0.0.0.0/0
  - Click **Done**.
  - Click **Save** and wait to finish the update.

PS: For production environments, it is recommended to use only the Private Network for database access.

⚠️ Never grant public network access (0.0.0.0/0) to production databases.