



A MITEL
PRODUCT
GUIDE

OpenScape Business V3

Google Cloud Platform (GCP) Deployment

Release Number 10/2024

Contents

- 1 Upload OpenScape Business to GCP4**
- 2 Create a VM on GCP8**
- 3 Access via VPN 11**
 - 3.1 IPSEC IKEv2 for VPN access 11
 - 3.2 GCP's firewall 13
 - 3.3 Office configuration 14
 - 3.3.1 Firewall 14
 - 3.3.2 Phones configuration 14
- 4 Tests executed 16**

History of Changes

Date	Issue	Summary
20.12.2022	1.0	initial version
11.10.2024	1.1	editorial changes

Note: The basis for this document is the current OpenScape Business at the time of certification. Since OpenScape Business is constantly developed, input masks and interfaces as well as requirements may change in the future. The settings and entries described here then apply accordingly.

Comments and corrections are welcome, please contact: osbiz-certification@mitel.com

Disclaimer

Google Cloud Platform (GCP) Branding, Pictures and Icons in this document might be under copyright of Google Inc..

This document is intended for trained OpenScape Business and Google Cloud Platform technicians or trained OpenScape Business technicians with the support of Google Cloud Platform experts, such as an Administrator or System Integrator.

The configuration example within this document shows a basic network setup of the OpenScape Business S image in a Google Cloud Platform (GCP) environment with mandatory requirements, such as the need of activating Google VPN for a secure operation.

Depends on the used Google Cloud Platform version and individual customer needs, especially in regards of security aspects or advanced network settings, further configuration (Google Firewall, etc.) steps might be needed. Availability and technical specifications are subject to change without notice.


Mitel doesn't deliver any administration services, training, or cost information (for e.g. required Google Cloud packages, modules or licenses, etc.) for the Google Cloud Platform. This is up to the responsibility of the Google Cloud Operator, the Administrator or System Integrator.

Furthermore, the operator of the Google Cloud Platform is responsible for any security and/or configuration issues might lead in a malfunction or a security leak.

The following description refers to OpenScape Business V3R2 and above.

1 Upload OpenScape Business to GCP

Step1: Login to Google Cloud Platform <https://console.cloud.google.com/>



Anmeldung

Weiter zur Google Cloud Platform

E-Mail oder Telefonnummer

[E-Mail-Adresse vergessen?](#)

Nicht Ihr Computer? Dann können Sie den Gastmodus verwenden, um sich privat anzumelden.
[Weitere Informationen](#)

[Konto erstellen](#)

Weiter

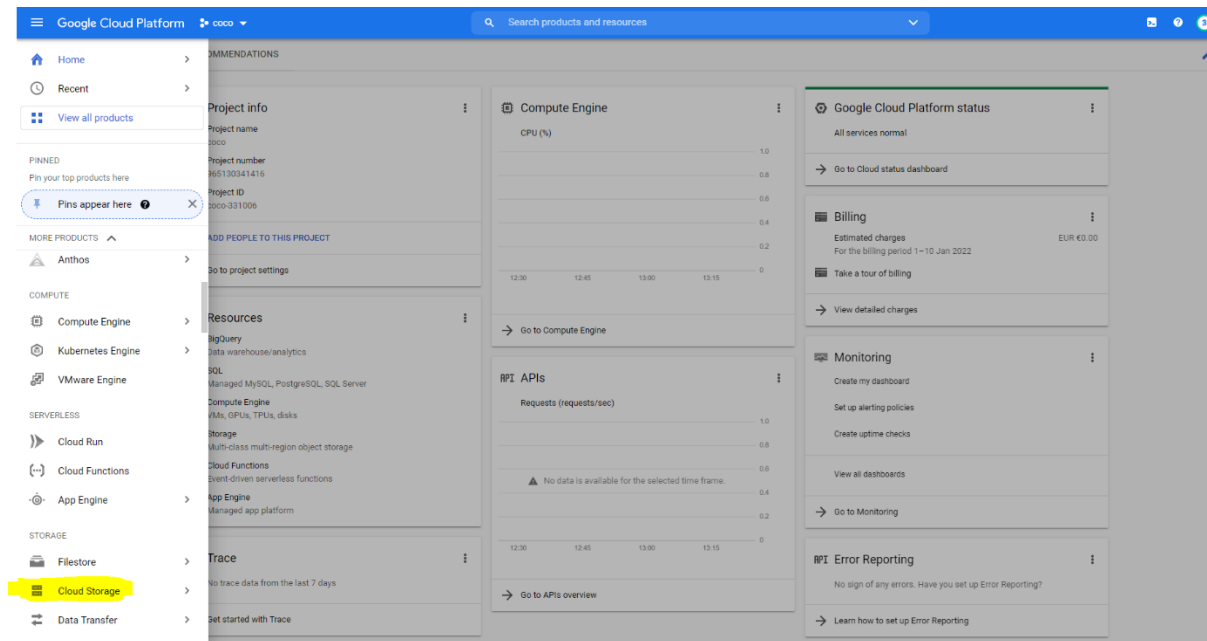
Deutsch ▼

Hilfe

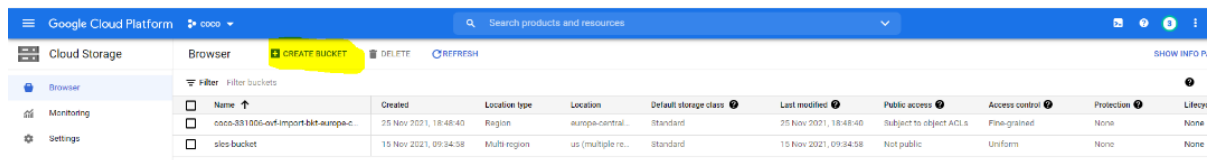
Datenschutz

Nutzungsbedingungen

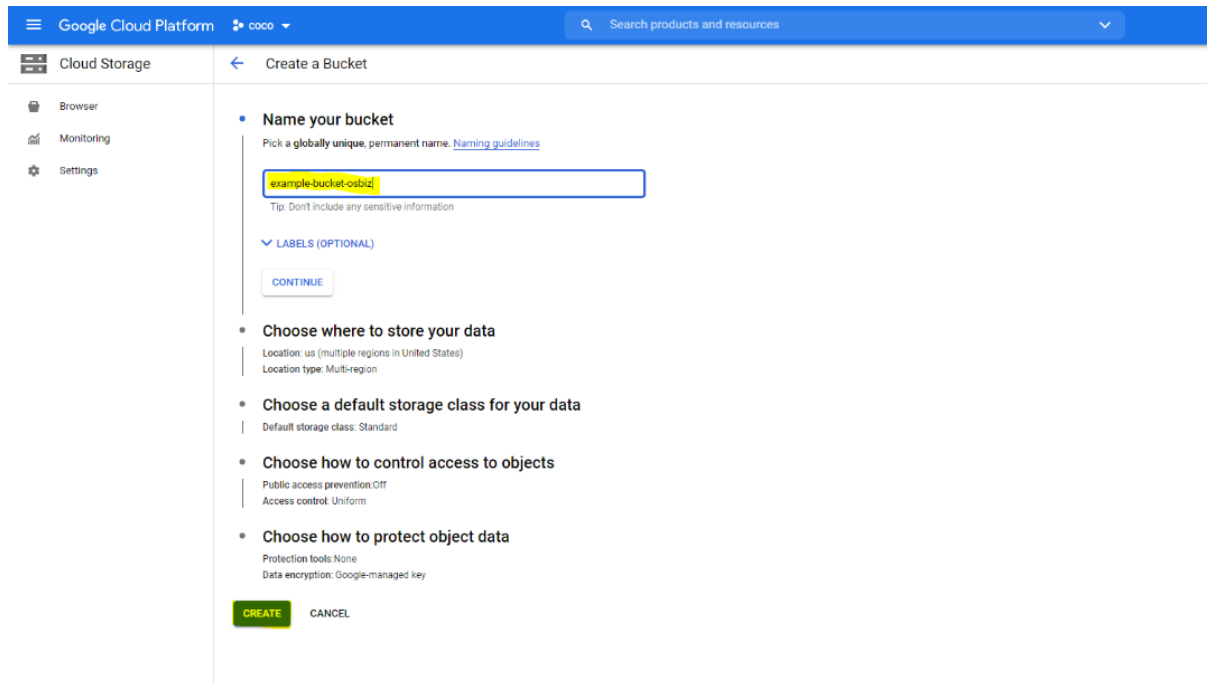
Step2: Navigate to the *Cloud Storage* menu



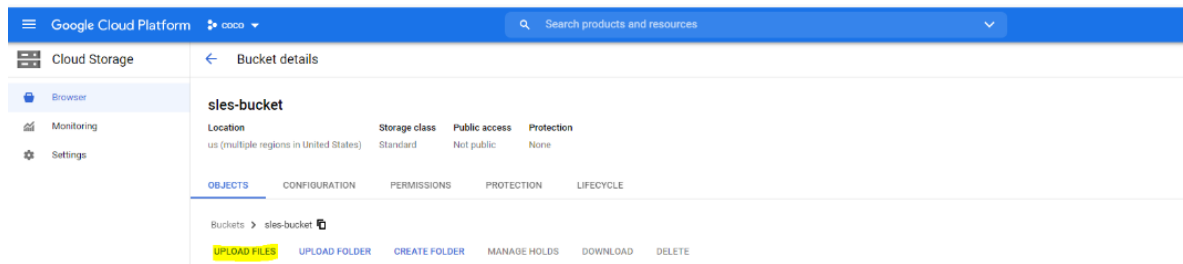
Step3: Hit the [Create Bucket] button or use an existing button



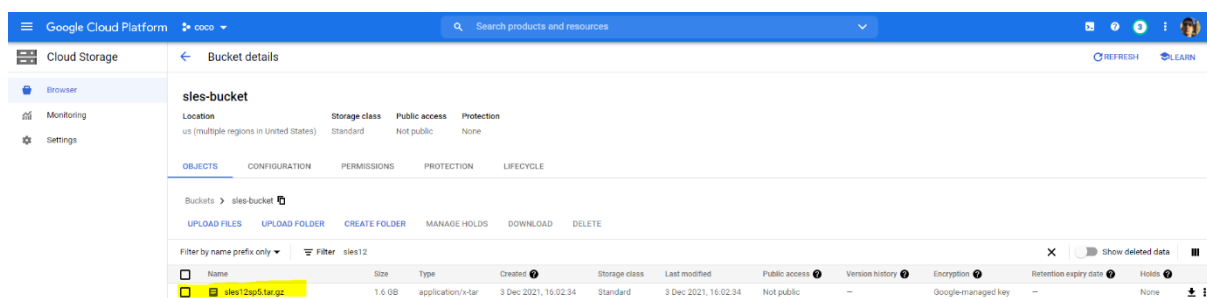
Step4: Select a name and hit [Create]



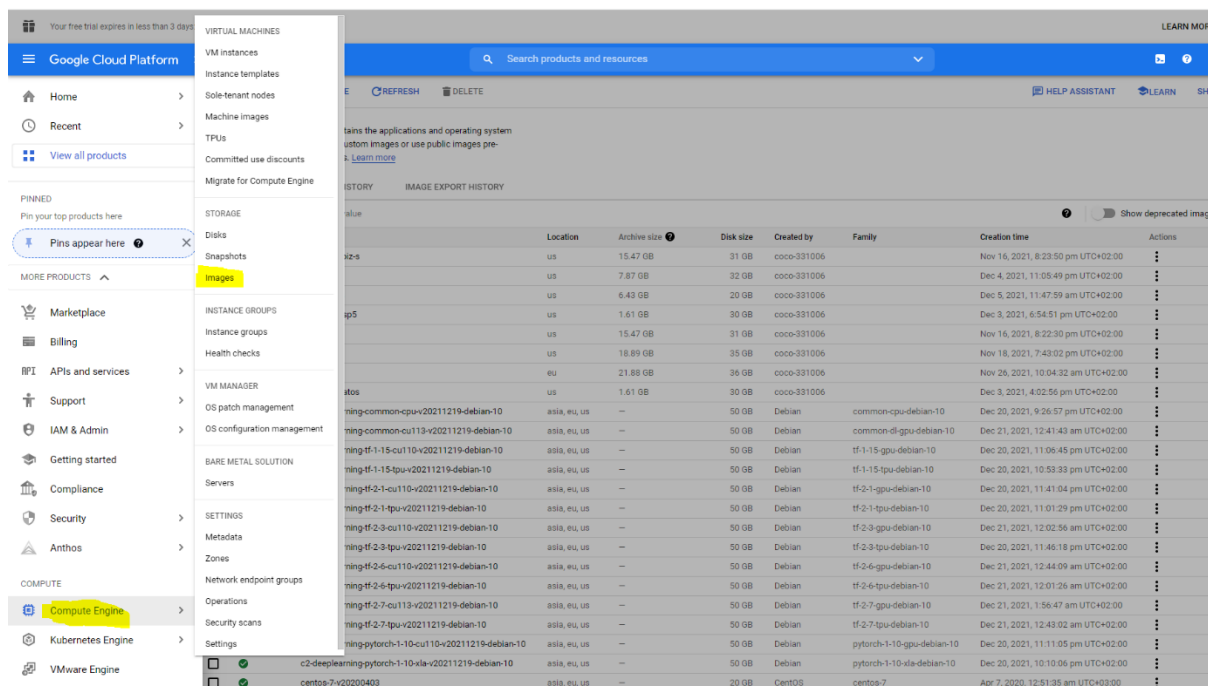
Step5: Navigate to the newly created bucket and hit [*Upload Files*] to select the **image-name.tar.gz** that was generated in the previous section



Step6: When the upload is completed you will be able to see the new image-name.tar.gz file inside the bucket.



Step7: Navigate to Computer *Engine* → *Images*



Step8: Hit [Create Image]

An image is a replica of a disk that contains the applications and operating system needed to start a VM. You can create custom images or use public images pre-configured with Linux or Windows OSes. [Learn more](#)

IMAGES IMAGE IMPORT HISTORY IMAGE EXPORT HISTORY

Filter Enter property name or value

<input type="checkbox"/>	Status	Name	Location	Archive size	Disk size	Created by	Family	Creation time	Actions
<input type="checkbox"/>	✓	custom-osbiz-s	us	15.47 GB	31 GB	coco-331006		Nov 16, 2021, 8:23:50 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	final-demo	us	7.87 GB	32 GB	coco-331006		Dec 4, 2021, 11:05:49 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	final-osbiz	us	6.43 GB	20 GB	coco-331006		Dec 5, 2021, 11:47:59 am UTC+02:00	⋮
<input type="checkbox"/>	✓	gce-sles12sp5	us	1.61 GB	30 GB	coco-331006		Dec 9, 2021, 6:54:51 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	image-1	us	15.47 GB	31 GB	coco-331006		Nov 16, 2021, 8:22:30 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	image-2	us	18.89 GB	35 GB	coco-331006		Nov 18, 2021, 7:43:02 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	sles-2611	eu	21.88 GB	36 GB	coco-331006		Nov 26, 2021, 10:04:32 am UTC+02:00	⋮
<input type="checkbox"/>	✓	sles12sp5-afos	us	1.61 GB	30 GB	coco-331006		Dec 3, 2021, 4:02:56 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	cd-deeplearning-common-cpu-v20211219-debian-10	asia, eu, us	—	50 GB	Debian	common-cpu-debian-10	Dec 20, 2021, 9:26:57 pm UTC+02:00	⋮
<input type="checkbox"/>	✓	cd-deeplearning-common-cu113-v20211219-debian-10	asia, eu, us	—	50 GB	Debian	common-gpu-debian-10	Dec 21, 2021, 12:41:43 am UTC+02:00	⋮

Step9: Enter the Name, as Source enter Cloud Storage file and then hit [Browse] and select the recently uploaded image.

Create an image

Name * Your free trial credit will be used for this image. [GCP Free Tier](#)

Source *

Cloud Storage file *

Location ☐ Multi-regional ☐ Regional

Select location

Family

Labels

Encryption ☒ Google-managed encryption key ☐ Customer-managed encryption key (CMEK) ☐ Customer-supplied encryption key (CSEK)

Step10: Select Location and hit [Create]

Create an image

Name is permanent Your free trial credit will be used for this image. [GCP Free Tier](#)

Source *

Cloud Storage file *

Location ☒ Multi-regional ☐ Regional

Select location

Family

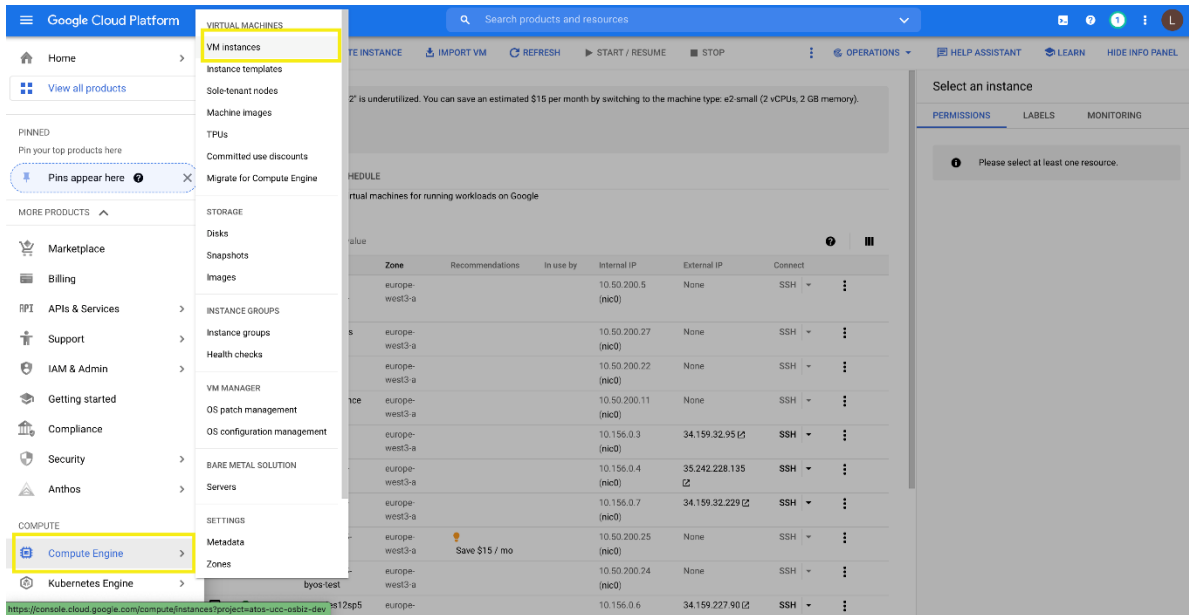
Labels

Encryption ☒ Google-managed encryption key ☐ Customer-managed encryption key (CMEK) ☐ Customer-supplied encryption key (CSEK)

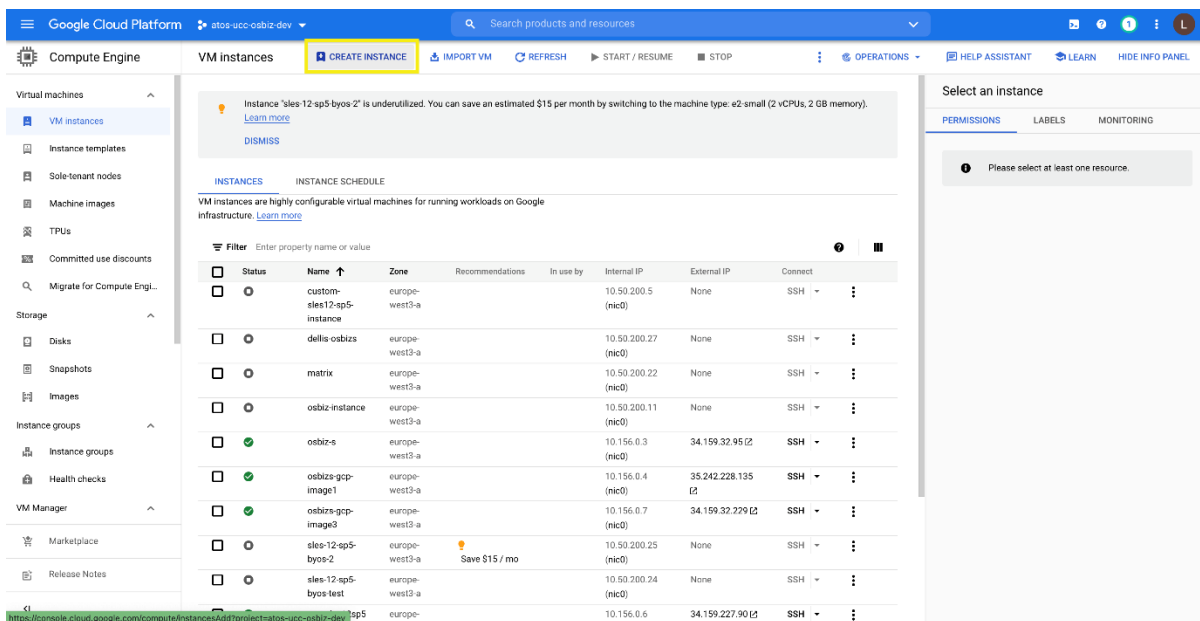
✓ image has been uploaded successfully to GCP! ✓

2 Create a VM on GCP

Step1: In the Google Cloud Console, hit the three lines on the top left corner, go to the **Compute Engine**, and hit the [VM instances] page.



Step2: Hit [Create Instance]



Step3: Specify a **Name** for your VM. For more information, see Resource naming convention.

Google Cloud Platform | atos-ucc-osbiz-dev | Search products and resources

Create an instance

To create a VM instance, select one of the options:

- New VM instance (Create a single VM instance from scratch)
- New VM instance from template (Create a single VM instance from an existing template)
- New VM instance from machine image (Create a single VM instance from an existing machine image)
- Marketplace (Deploy a ready-to-go solution onto a VM instance)

Labels

+ ADD LABELS

Region * europe-west3 (Frankfurt) Zone * europe-west3-a

Region is permanent Zone is permanent

Machine configuration

Machine family

GENERAL-PURPOSE COMPUTE-OPTIMIZED MEMORY-OPTIMIZED

Machine types for common workloads, optimized for cost and flexibility

Series E2

CPU platform selection based on availability

Machine type e2-medium (2 vCPU, 4 GB memory)

vCPU 1 shared core Memory 4 GB

CPU PLATFORM AND GPU

Display device

Enable to use screen capturing and recording tools.

☐ Enable display device

Monthly estimate

\$32.71

That's about \$0.04 hourly

Pay for what you use: No upfront costs and per second billing

DETAILS

Step4: Scroll down and in the **Boot disk** section, click [Change],

Google Cloud Platform | atos-ucc-osbiz-dev | Search products and resources

Create an instance

To create a VM instance, select one of the options:

- New VM instance (Create a single VM instance from scratch)
- New VM instance from template (Create a single VM instance from an existing template)
- New VM instance from machine image (Create a single VM instance from an existing machine image)
- Marketplace (Deploy a ready-to-go solution onto a VM instance)

CPU PLATFORM AND GPU

Display device

Enable to use screen capturing and recording tools.

☐ Enable display device

Confidential VM service

☐ Enable the Confidential Computing service on this VM instance.

Container

Deploy a container image to this VM instance

DEPLOY CONTAINER

Boot disk

Name gcp-cloud

Type New balanced persistent disk

Size 10 GB

Image Debian GNU/Linux 10 (buster)

CHANGE

Identity and API access

Service accounts

Service account Compute Engine default service account

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. [Learn more](#)

Access scopes

☒ Allow default access

Monthly estimate

\$32.71

That's about \$0.04 hourly

Pay for what you use: No upfront costs and per second billing

DETAILS

and then do the following:

- a) Select the **Custom Images** tab.
- b) To select the image project, click [*Select a project*], and then do the following:
 - i. Select the project that contains the image you uploaded before.
 - ii. Click [*Open*].
- c) In the **Image** list, click the image that you want to import.
- d) Select the type and size of your boot disk.
- e) Optional: For advanced configuration options, click **Show advanced configuration**.
- f) To confirm your boot disk options, click [*Select*].

The screenshot shows the 'Create an instance' page in the Google Cloud Platform console. The 'Boot disk' section is expanded, showing the 'CUSTOM IMAGES' tab. The 'Image' dropdown is set to 'osbiza-gcp-image3'. The 'Boot disk type' is 'Balanced persistent disk' and the 'Size (GB)' is '32'. The 'SELECT' button is highlighted with a yellow box.

Step5: In the **Firewall** section, to permit HTTP or HTTPS traffic to the VM, select **Allow HTTP traffic** or **Allow HTTPS traffic**.

The Cloud Console adds a network tag to your VM and creates the corresponding ingress firewall rule that allows all incoming traffic on tcp:80 (HTTP) or tcp:443 (HTTPS). The network tag associates the firewall rule with the VM. For more information, see [Firewall rules overview](#) in the Virtual Private Cloud documentation.

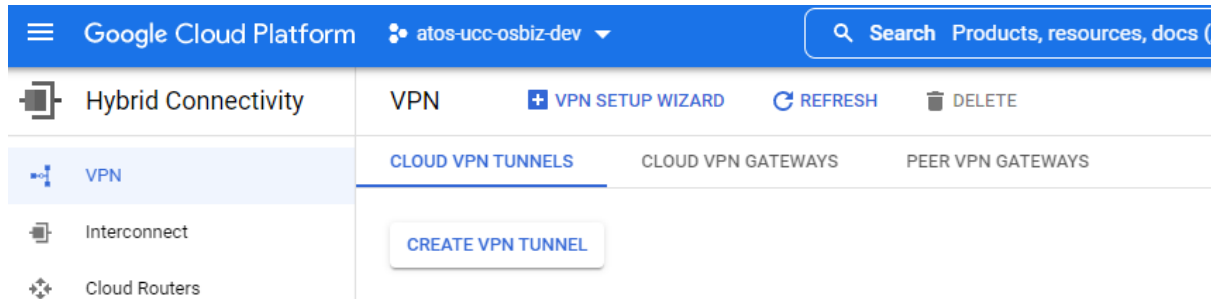
The screenshot shows the 'Create an instance' page in the Google Cloud Platform console. The 'Firewall' section is expanded, showing the 'Allow HTTP traffic' and 'Allow HTTPS traffic' options. The 'CREATE' button is highlighted with a yellow box.

Step6: To create and start the VM, click [*Create*].

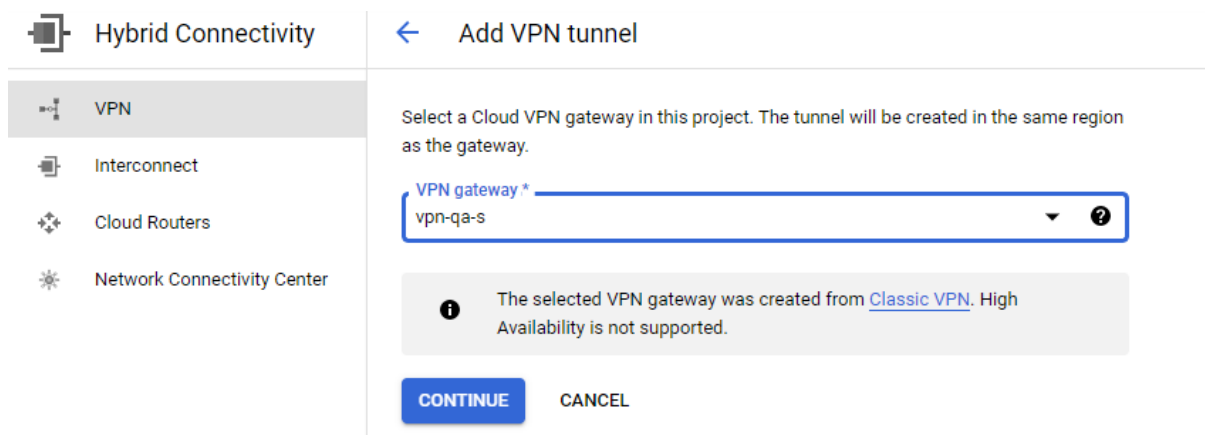
3 Access via VPN

3.1 IPSEC IKEv2 for VPN access

GCP supports IPSEC IKEv2 for VPN access. To configure it needs to click in **Cloud VPN Tunnels** the [Create VPN tunnel]



choose your gateway



and fill in the details:

← Create VPN tunnel

VPC network	osbiz-s-ova
Region	europa-west3
VPN gateway name	vpn-qa-s (Classic VPN gateway)
VPN gateway IP address	35.198.126.118


Name *
vpn-qa-s-tunnel5 ?
Lowercase letters, numbers, hyphens allowed

Description

Remote peer IP address *
62.38.100.120 ?

IKE version
IKEv2 ▼ ?

IKE pre-shared key *
daaOzCxibLloo4dbOWK2UuhNoe97xhq3 Generate and copy
Enter your own key or generate one automatically

 Make sure you record the pre-shared key in a secure location. The key can't be retrieved after this form is closed. [Learn more](#)

Routing options ?
☐ Dynamic (BGP)
☒ Route-based
☐ Policy-based

Remote network IP ranges *
192.168.1.0/24 ✕ for example: 192.168.0.0/24 10.16.0.0/12 ?
Enter multiple IP address ranges (in CIDR notation) by pressing Enter after each one

CREATE CANCEL

- your Office router's public IP. In the example it is 62.38.100.120
- IKE version, choose IKEv2, preferred
- generate a pre-shared key and keep it safe, as it will not be visible.
- Routing Options choose Route-based.
- Remote network IP ranges. Type the network ranges that the office router uses. In the attached example it is 192.168.1.0/24

3.2 GCP's firewall

We need to create the rules for the VPN access

Forwarding rules

Name	Protocol
vpn-qa-s-rule-esp	esp
vpn-qa-s-rule-udp4500	udp:4500
vpn-qa-s-rule-udp500	udp:500

3.3 Office configuration

In the office depending on the router used, it must support IKEv2. Needs to create an IPSEC IKEv2 tunnel from the router/firewall to GCP to route traffic from LAN to GCP, without public access.

3.3.1 Firewall

For the VPN to work it needs the following 3 ports allowed

The screenshot shows the 'Cloud VPN gateway details' page for a gateway named 'vpn-qa-s'. The left sidebar shows the navigation menu with 'VPN' selected. The main content area displays the gateway's configuration and forwarding rules.

vpn-qa-s
Classic Cloud VPN gateway

VPC network	osbiz-s-ova
Region	europa-west3
Description	vpn-qa-s
IP address	35.
High availability	No
Logs	View

Forwarding rules

Name	Protocol
vpn-qa-s-rule-esp	esp
vpn-qa-s-rule-udp4500	udp:4500
vpn-qa-s-rule-udp500	udp:500

VPN tunnels

[ADD VPN TUNNEL](#) [DELETE](#)

Filter Filter by VPN tunnel properties

<input type="checkbox"/>	VPN tunnel name	Peer gateway IP address	IP stack type	Routing type	Status
<input type="checkbox"/>	vpn-qa-s-tunnel4	7 .66	IPv4	Route-based	No incoming packets

3.3.2 Phones configuration

Since the phones are in the LAN (192.168.1.0/24) network, they have as default gateway the firewall IP (192.168.1.1/24) to be able to communicate with the GCP-OSBIZ (10.156.0.9) via VPN.

For the image update

The screenshot shows the 'Update service' configuration page in the OpenScape Business V3 web interface. The left sidebar shows the navigation menu with 'Update service' selected. The main content area displays the configuration options for the update service.

Update service
Select either DLS or DMS for use by providing an address, but only for one of them

Deployment service (DLS)

DLS address	10.156.0.9
Default mode port	18443
Revert to default security	<input type="checkbox"/>
Mode	Default
Security PIN	

Device management service (DMS)

DMS address	
Username	
Password	
Minimum update check (seconds)	300
Update check during working hours	<input checked="" type="checkbox"/>
Ignore software update from config file	<input type="checkbox"/>
Check for update	Now

For the registration of HFA

The screenshot shows the 'Administrator settings' page with a sidebar menu on the left and a top navigation bar. The sidebar menu includes 'Admin login', 'Network' (with sub-items: 'Common settings', 'Wired settings', 'IPv4 configuration', 'Update service', 'QoS', 'Port number configuration', 'PC port configuration'), 'System' (with sub-items: 'System identity', 'Gateway'), 'Features', 'Security', 'ICE', 'File transfer', 'Local functions', and 'Date and time'. The top navigation bar has 'User settings', 'Licences', and 'Logout'. The main content area is titled 'Gateway' and contains the following fields: 'System type' (dropdown menu showing 'Unknown'), 'IP address' (text box with '10.156.0.9'), 'Gateway ID' (text box with 'DEFAULTH323ID'), 'Subscriber number' (text box with '7000'), and 'Password' (text box). There are 'Submit' and 'Reset' buttons at the bottom.

as it can be seen from the picture above the registration takes place in a private IP, without password. It is like being in a LAN.

For the registration of SIP

The screenshot shows the 'Administrator settings' page with a sidebar menu on the left and a top navigation bar. The sidebar menu includes 'Admin login', 'Network' (with sub-items: 'Common settings', 'Wired settings', 'IPv4 configuration', 'Update service', 'QoS', 'Port number configuration', 'PC port configuration'), 'System' (with sub-items: 'System identity', 'SIP interface', 'Registration', 'SNMP'), 'Features', 'Security', 'ICE', 'File transfer', 'Local functions', and 'Date and time'. The top navigation bar has 'User settings', 'Licences', and 'Logout'. The main content area is titled 'Registration' and contains two sections: 'SIP addresses' and 'SIP session'. The 'SIP addresses' section has three text boxes: 'SIP server address' (10.156.0.9), 'SIP registrar address' (10.156.0.9), and 'SIP gateway address' (10.156.0.9). The 'SIP session' section has a 'Session timer enabled' checkbox (unchecked), 'Session duration (seconds)' (3600), 'Registration timer (seconds)' (3600), 'Subscription timer (seconds)' (3600), 'Refresh minimum (seconds)' (0), 'Server type' (dropdown menu showing 'Genesys'), 'Realm' (osbiz), 'User ID' (7005), and 'Password' (masked with dots).

4 Tests executed

The current setup is a VPN connection between GCP and a local router. **No calls via Public IP.** Phones and systems attached in the LAN and register to the local IP of the GCP. The tests are:

- Connect local HFA through VPN to GCP
- Connect local SIP through VPN to GCP
- Connect local myPortal@work through VPN to GCP
- Setup system via VPN, in UC Suite
- Enable ITSP
- Incoming calls from ITSP_A to local HFA/SIP/myPortal@work via VPN
- Outgoing calls from local HFA/SIP/myPortal@work via VPN to GCP ->ITSP_B -> ITSP_A -> recipient
- Conference between different phones in the LAN.
- Conference for an incoming call from ITSP with other internal members.
- Voicemail access via VPN
- myPortal for Desktop manage a phone, registered to GCP, via VPN.
- Auto-Attendant access via VPN
- Networking setup via VPN (GCP as Master node)
- Networking setup via VPN. An embedded system (V3 Mainboard Family) as slave node, via VPN.
- Networking calls between nodes

