

Realizzazione e gestione di una nuova infrastruttura informatica al servizio della Pubblica Amministrazione denominata Polo Strategico Nazionale (“PSN”), di cui al comma 1 dell’articolo 33-septies del d.l. n. 179 del 2012

CUP: J51B21005710007

CIG: 9066973ECE

Manuale Utente

Secure Public Cloud su Cloud Provider Google

Data: 21/05/2025

PSN_Manuale Utente SPC Google

Ed. 1 - ver. 2.1

QUESTA PAGINA È LASCIATA
INTENZIONALMENTE BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
Manuale Utente Secure Public Cloud su Cloud Provider Google			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	28/03/2023	Prima versione
1	1.1	07/06/2023	Eliminati refusi Adeguate il layout
2	1.0	04/04/2025	Seconda versione
3	1.1	21/05/2025	Aggiornato capitolo "Guida alla fatturazione"

NUMERO TOTALE PAGINE:	76
-----------------------	----

AUTORE:	
Team di lavoro PSN	Unità operative Solution Development, Technology Hub e Sicurezza

REVISIONE:	
Referente del Servizio	Paolo Trevisan

APPROVAZIONE:	
Direttore del Servizio	Antonio Garelli

INDICE

1	Definizioni e Acronimi.....	7
1.1	DEFINIZIONI	7
1.2	ACRONIMI	7
2	Executive Summary.....	10
2.1	SCOPO DEL DOCUMENTO	10
2.2	PREMESSA ALL'UTILIZZO DELLA CONSOLE TECNICA	10
3	Security Governance.....	11
3.1	GESTIONE UTENTI PA	11
3.1.1	<i>Organization Unit.....</i>	<i>11</i>
3.1.2	<i>Utenze di emergenza.....</i>	<i>11</i>
3.1.3	<i>Utenze PA</i>	<i>11</i>
3.1.4	<i>User Group.....</i>	<i>12</i>
3.1.5	<i>Creazione nuovo user.....</i>	<i>13</i>
3.1.6	<i>Guide GCP.....</i>	<i>15</i>
3.1.7	<i>Autenticazione</i>	<i>15</i>
3.1.8	<i>GCP Org Policy.....</i>	<i>16</i>
3.1.9	<i>Security Command Center.....</i>	<i>19</i>
3.2	NETWORKING.....	20
3.2.1	<i>Soluzione con IDS.....</i>	<i>20</i>
3.2.2	<i>Soluzione con IPS.....</i>	<i>21</i>
3.2.3	<i>Gestione Shared VPC</i>	<i>22</i>
3.2.4	<i>Gestione DNS.....</i>	<i>24</i>
3.2.5	<i>Gestione Firewall.....</i>	<i>27</i>
3.2.6	<i>Cloud IDS.....</i>	<i>31</i>
3.2.7	<i>IAP</i>	<i>32</i>
3.2.8	<i>Cloud Armor.....</i>	<i>36</i>
3.2.9	<i>Esposizione Web server su Global Load Balancer (Gestito Da PSN)</i>	<i>37</i>
3.2.10	<i>Consultazione dei logs</i>	<i>45</i>
3.3	BACKUP PSN SCP	47
3.3.1	<i>Introduzione al servizio di backup PSN SPC.....</i>	<i>47</i>
3.3.2	<i>Struttura del Portale: Dashboard</i>	<i>49</i>
3.3.3	<i>Storage.....</i>	<i>51</i>

3.3.4	<i>Plan</i>	55
3.3.5	<i>VM Groups</i>	57
3.3.6	<i>Jobs</i>	60
3.3.7	<i>Manual Backup</i>	61
3.3.8	<i>Restore</i>	62
3.3.9	<i>Restore Confidential VM con CMEK</i>	63
3.3.10	<i>Manuali Commvault</i>	67
3.4	KMS	67
3.4.1	<i>Utilizzo Chiave esterna per una Virtual Machine</i>	69
3.4.2	<i>Rotazione chiave</i>	70
3.4.3	<i>Cancellazione chiave</i>	70
3.4.4	<i>Utilizzo nuova Chiave</i>	71
4	Guida alla fatturazione	76

LISTA DELLE FIGURE

Figura 1: HLD Commvault	48
Figura 2: Dettaglio Flussi	49

LISTA DELLE TABELLE

Tabella 1: Glossario Definizioni	7
Tabella 2: Glossario Acronimi	9

1 Definizioni e Acronimi

1.1 Definizioni

Definizione	Descrizione
PSN	È la nuova società che è stata costituita nell'ambito del progetto del Cloud Nazionale
TBC	Il tema è stato discusso ma è in attesa di conferma dalle parti coinvolte
TBD	Il tema non è ancora stato discusso

Tabella 1: Glossario Definizioni

1.2 Acronimi

Acronimo	Descrizione
AD	Active Directory
APT	Advanced Persistent Threat
API	Application Program Interface
AV	AntiVirus
BaaS	Backup as a Service
CaaS	Container as a Service
CLI	Command Line Interface
CSP	Cloud Service Provider
DBE	DataBase Encryption
DDC	Data Discovery and Classification
DDoS	Distributed DoS
DE	Data Encryption
DLP	Data Loss Prevention
DM	Data Masking
DMZ	DeMilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DWDM	Dense Wavelength Division Multiplexing
EDE	Endpoint Disk Encryption
EDR	Endpoint Detection and Response
FIM	File Integrity Monitoring
FW	FireWall
Gbps	Gigabits per second
GUI	Graphical User Interface
HA	High Availability
HSM	Hardware Security Module

Acronimo	Descrizione
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure
IaaS	Infrastructure as a Service
IAG	Identity and Access Governance
I&AM	vedi IAM
IAM	Identity and Access Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
iSCSI	Internet SCSI
ISO	International Organization for Standardization
KMS	Key Management System
L2	Layer 2 (della pila ISO/OSI)
L3	Layer 3 (della pila ISO/OSI)
L4	Layer 4 (della pila ISO/OSI)
LAG	Link Aggregation Group
LAN	Local Area Network
LM	Log Management
LOM	Lights Out Management
MAC	Media Access Control
MC-LAG	Multi Chassis LAG
MDM	Mobile Device Management
MFA	Multi Factor Authentication
MPLS	MultiProtocol Label Switching
NAC	Network Access Control
NGFW	Next Generation FW
NL-SAS	Near Line SAS
NPB	Network Packet Broker
NTP	Network Time Protocol
OOB	Out of band
OSI	Open Systems Interconnection
PaaS	Platform as a Service
PA	Pubblica Amministrazione
PAM	Privileged Access Management
PdL	Postazione di Lavoro
PSN	Polo Strategico Nazionale
rpm	Rotation per minute
SaaS	Software as a Service
SAN	Storage Area Network
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SEG	Security Email Gateway
SFP	Small Form-factor Pluggable
SFP+	Enhanced SFP
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response

Acronimo	Descrizione
SOC	Security Operation Center
SQL	Structured Query Language
SR	Short Reach
SWG	Secure Web Gateway
TB	TeraByte
TBC	To Be Confirmed
TBD	To Be Defined
TI	Threat Intelligence and Infosharing
ToR	Top of Rack
VBR	Veeam Backup & Replication
VDOM	Virtual DOMain (Contesto Virtuale)
VLAN	Virtual LAN
VM	Vulnerability Management
VPN	Virtual Private Network
WAF	Web Application Firewall
WAN	Wide Area Network
XSS	Cross-Site Scripting

Tabella 2: Glossario Acronimi

2 Executive Summary

2.1 *Scopo del documento*

Il documento ha lo scopo di fornire una guida all'utente finale delle funzionalità rilasciate nel Secure Public Cloud Google.

2.2 *Premessa all'utilizzo della console tecnica*

Con riferimento all'utilizzo della console di cui al presente capitolo, in ragione dell'oggetto del Contratto di Utenza e dei relativi allegati, incluso il Progetto dei Piani dei Fabbisogni ("PPDF") ("Contratto"), l'Amministrazione Utente deve attivare esclusivamente quegli elementi presenti nel Listino pubblicato nell'area del sito istituzionale di Polo Strategico Nazionale e che trovano una corrispondenza nell'ambito dei Servizi oggetto di Contratto.

Resta inteso che, nel caso di violazione di quanto sopra, PSN

- sarà legittimata, previa comunicazione all'Amministrazione Utente, alla disattivazione di quegli elementi indebitamente attivati, mettendosi a disposizione, per quanto possibile, per l'identificazione ed attivazione di soluzioni alternative;
- non sarà in alcun modo responsabile dell'utilizzo o del funzionamento di quegli elementi indebitamente attivati dall'Amministrazione Utente.

3 Security Governance

3.1 Gestione utenti PA

Relativamente alla gestione degli utenti della PA:

- sono indicate le utenze per la gestione di altre utenze (gruppi e grant ad essi associati)
- esempio di creazione e profilazione utenza
- link generici a guide GCP generiche

3.1.1 Organization Unit

Ogni Organizzazione GCP corrispondente ad un cliente Pubblica Amministrazione deve essere configurata con la predisposizione di due Organization Unit (OU):

- Una OU a livello root, gestita dal personale del PSN (di seguito definita OUPSN);
- Una OU gerarchicamente subordinata alla precedente a cui avrà accesso la PA per la gestione utente (di seguito definita OUPA).

La OUPSN avrà al suo interno le utenze di emergenza da utilizzare nei casi di necessità ad opera del PSN.

La OUPA avrà invece le utenze del cliente Pubblica Amministrazione.

3.1.2 Utenze di emergenza

All'interno della OUPSN sono definite due utenze di emergenza con ruolo di Super Admin.

Occorre conservare la password in una apposita cassaforte digitale che sia nella sola disponibilità del personale autorizzato del PSN.

Queste utenze andranno utilizzate solo in caso di emergenza per recuperare l'accesso alla ORG.

3.1.3 Utenze PA

Alla PA verranno date una o più utenze che avranno grant di profilazione di altri utenti, ovvero:

- Potranno creare utenze cloud native nella Organization Unit dedicata alla PA
- Potranno aggiungere tali utenze ai gruppi predefiniti (preconfigurati dal PSN) distribuendo così i permessi per l'ambiente console.

Le sole utenze PA con diritti di creazione e gestione utenti nella OU della PA saranno le sole ad avere accesso al pannello admin.google.com

Le altre, sempre utenze PA, avranno accesso a console.google.com

3.1.4 User Group

Il PSN configura nella Org della PA i gruppi di utenze a cui assegnare i ruoli di gestione delle risorse, fornendo in sede di setup una utenza con diritti di creazione e gestione utenti.

Di seguito la tabella dei gruppi con descrizione delle responsabilità, ruoli e scope di applicazione.

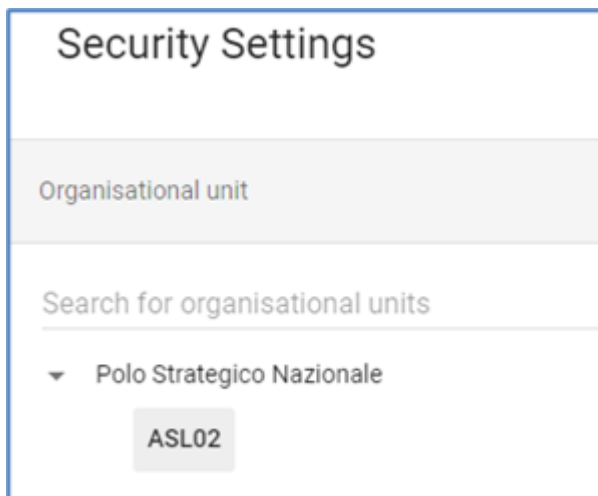
Group of work	Responsibilities	GCP Role	GCP Resource
PA Network Team	Custom Role to control the network aspects over the Network PA folder. - Create and associate subnets to service project - Create FR and Routes - Add subnet to Packet Mirroring Policy - Create and manage Internal Load Balancers	Network Admin, XPN Admin, Compute Security Admin	Network PA Folder
		Monitoring Admin, Logging Admin	Network Shared Prj
		XPN Admin	Teams Folder
PA Cloud Operator Team	Cloud Logging Admin (Creating LogSink, LogBucket and reading logs within the PA Folder), Compute Instance Admin, Container Admin, Cloud Storage Admin, Cloud Monitoring Admin, CI/CD Admin inside the Teams folder. It should also be able to access and change the SCC configuration for this folder. It shouldn't be able to: - Create/update OrgPolicies - Give itself additional permissions not needed (no IAM Admin)	Folder Admin, Project Creator	Teams Folder
		Network User	Network Shared Prj
		Custom role with delegation for KMS user (restriction on cloudkms.cryptoKeys.setIamPolicy)	Key Ring (inside Sec Folder)
PA Tech Support Team	This is optional, but makes using the console easier as it lets the user browse keyrings and keys from the UI.	Cloud KMS Viewer	sec-shared project (project containing the keyring)
		Tech support Editor	Teams Folder
PA Billing User	Associate new projects to existing Billing Account. Can't see billing information	Billing Account User	PA Billing Account

PA Cloud viewers	Can browse folders and projects under secure cloud. Useful to let the user navigate resources in the console, grant no permissions to see resources inside projects. Also, using the console is in some cases easier (e.g.: select a key when creating a VM).	Organization Viewer	PA Organization
		Folder Viewer, Browser	Secure Cloud folder
PA KMS Users	Can use KMS keys to create VMs and buckets	Custom role with delegation for KMS user (restriction on cloudkms.cryptoKeys.setIamPolicy)	Key Ring (inside sec-shared project)
PA SCC Admins	Can manage SCC in PA projects, see SCC in Shared PA project	Security Center Admin	Teams Folder
		Security Center Admin Viewer	Network Shared Prj
		Organization Viewer	PA Organization
PA IDS Viewers	Can see IDS threats	Cloud IDS Viewer Logs Viewer Compute Network Viewer	Network Shared Prj
		Organisation Viewer	PA Organization
PA IAM Admins	Can create projects and in Teams folder manage IAM on PA resources	Folder Admin, Project Creator	Teams Folder
		Organisation Viewer	PA Organization
		Folder Viewer, Browser	Secure Cloud folder

3.1.5 Creazione nuovo user

Per creare una nuova user occorre collegarsi al portale di admin: <https://admin.google.com> con le credenziali di admin.

Creare nella OUPA le utenze della PA, Selezionare la OUPA



Security Settings

Organisational unit

Search for organisational units

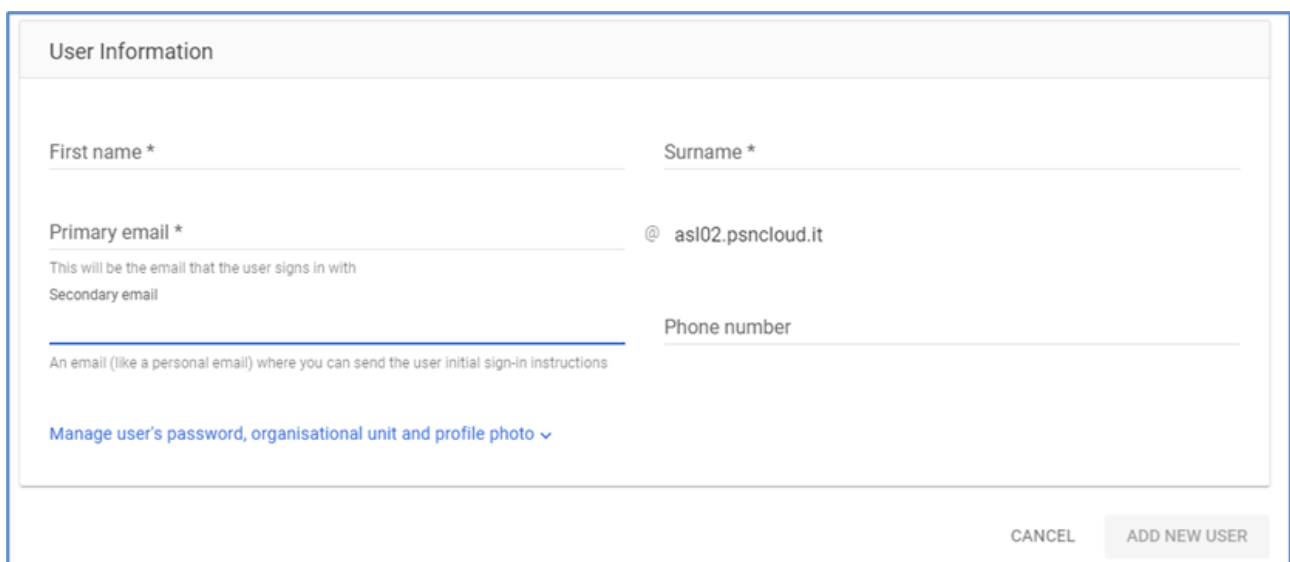
▼ Polo Strategico Nazionale

ASL02

Cliccare su “Add new user”

Inserire nella form i dati:

- First name: Nome
- Surname: Cognome
- Primary email: nome-cognome (in casi di omonimia aggiungere un integer incrementale)
- Secondary email: Email (fornita dalla PA, con dominio diverso da quello della Org)
- Phone number: Mobile



User Information

First name * _____ Surname * _____

Primary email * _____ @ asl02.psncloud.it
This will be the email that the user signs in with

Secondary email _____
An email (like a personal email) where you can send the user initial sign-in instructions

Phone number _____

[Manage user's password, organisational unit and profile photo ▼](#)

CANCEL ADD NEW USER

Salvare la password in una cassaforte digitale.

Dopo aver creato la user assegnare la user al corretto gruppo di riferimento.

Sempre dal menu Directory, Group selezionare “Add Members” sul gruppo richiesto (ad es. GCP-Support)

☐	Group name ↑	Email address	Members	Access type
☐	gcp-billing-admins	gcp-billing-admins@asl02.psncloud.it	1	Public
☐	gcp-devops	gcp-devops@asl02.psncloud.it	1	Public
☐	gcp-network-admins	gcp-network-admins@asl02.psncloud.it	1	Public
☐	gcp-organization-admins	gcp-organization-admins@asl02.psncloud.it	6	Public
☐	gcp-security-admins	gcp-security-admins@asl02.psncloud.it	2	Public
☐	gcp-support	gcp-support@asl02.psncloud.it	Add members Manage members	

Successivamente si dovranno inoltrare le informazioni per il login agli utenti per il primo accesso.

3.1.6 *Guide GCP*

Per ulteriori dettagli circa user, group e altri argomenti relativi al tema fare riferimento alla documentazione ufficiale Google:

- Add an account for a new user
- Add or update multiple users from a CSV file
- Delete or remove a user from your organization

3.1.7 *Autenticazione*

Le utenze dell'ambiente Google Cloud Platform sono di tipo “cloud native”. Ovvero sono identità digitali create direttamente nella Organizzazione del cliente finale.

Ai fini dell'autenticazione basterà visitare uno dei link ai pannelli di controllo dedicati e verrà richiesto l'inserimento di nome utente e password dell'identità digitale selezionata.

Di seguito si riportano i link ai pannelli di controllo disponibili:

- [Google Cloud Platform Admin Console](#);
- [Google Cloud Platform Console](#).

Si noti che tutte le identità digitali della Organizzazione richiedono autenticazione a due fattori.

3.1.8 GCP Org Policy

L'ambiente Secure Public Cloud in GCP è sottoposto a restrizioni e monitoraggi tramite l'implementazione di un set di policy.

Tali policy sono gestite direttamente dai servizi del PSN che si occupa di:

- Definire quali attivare in funzione dei requisiti di ambiente;
- Configurare le opzioni necessarie al corretto funzionamento;
- Monitorare gli allarmi generati dalle policy (ove applicabile)
- Monitorare la consistenza della configurazione delle policy

Di seguito si riporta la configurazione delle policy attive per Project GCP.

Nome	Descrizione	Valore	Livello di applicazione	Eccezioni
Disable public IPs (VM)	Le VM non possono essere create con un indirizzo IP pubblico connesso alla scheda di rete della macchina.	Deny All	ORG Root	-
Disallow external load balancers	Consente la creazione di bilanciatori di traffico solo per il perimetro network interno.	in:INTERN AL	Org Root	-
Disable public IPs (SQL)	Impedisce la creazione di una istanza SQL GCP con IP pubblico associato.	enforced = true	Org Root	-
Disable service account key creation	Disabilita la creazione di chiavi esterne agli account di servizio.	enforced = true	Org Root	project: prj-sec-shared Tali attività sono tuttavia consentite nel progetto che include i servizi di KMS dell'ambiente.

Disable Service Account Key Upload	Disabilita la possibilità di caricamento di una chiave esterna per gli account di servizio.	enforced = true	Org Root	-
Google Cloud Platform - Resource Location Restriction	Restringe la possibilità di rilascio delle risorse GCP alle sole region presenti su territorio nazionale.	allow: europe-west8	Org Root	-
Google Cloud Platform - Detailed Audit Logging Mode	Configura il livello di logging da applicare all'ambiente.	enforced = true	Org Root	-
Enforce Public Access Prevention	Disabilita, ove previsto, l'accesso pubblico alle risorse GCP.	enforced = true	Org Root	-
Sets the internal DNS setting for new projects to Zonal DNS Only	Configura il DNS interno come default per i progetti in ambiente GCP.	enforced = true	Org Root	project: prj-net-landing Policy disabilitata.

Skip default network creation	Disabilita la creazione automatica di nuove network alla creazione di risorse GCP.	enforced = true	Org Root	-
Disable Audit Logging exemption	Disabilita le eccezioni alle attività di Audit Logging	enforced = true	Org Root	-
Require OS Login	Abilita il login a livello di Sistema Operativo per ogni VM creata nell'ambiente.	enforced = true	Org Root	-
[CMEK] Restrict which projects may supply KMS CryptoKeys for CMEK	Configura e restringe i progetti autorizzati alla fornitura di chiavi di crittografia da parte dei servizi KMS.	allow = id-prj-sec-shared	Org Root	-
[CMEK] Restrict which KMS CryptoKey types may be created	Definisce quali tipologie di chiavi possono essere generate ed utilizzate in ambiente GCP.	allow = HSM	Org Root	-

Restrict VPC peering usage	Limita i network VPC che possono accettare definizioni di peering.	under:folders/ID_folder_Network_PA Allow List: Google Network and Landing VPC	Org Root	-
Restrict Shared VPC Host Projects	Limita i progetti che possono essere connessi ad altri all'interno di una Shared VPC.	under:folders/TEAM S Allow List: Shared VPC	Org Root	-

Di seguito si riporta il link alla pagina Google della documentazione relativa al servizio [Criteri dell'Organizzazione](#).

In caso di esigenze specifiche relative ad attivazione, disattivazione o diversa configurazione di Org Policy è richiesta l'apertura di una Service Request che motivi l'esigenza. Tale richiesta sarà approvata solo nel caso in cui questa non implichi un incremento del livello di rischio dell'ambiente.

3.1.9 Security Command Center

Il Security Command Center (di seguito SCC) è il servizio di segnalazione vulnerabilità e minacce dell'ambiente GCP. Ha lo scopo di individuare e guidare l'utente alla eradicazione o mitigazione di rischi e minacce legate prevalentemente alla configurazione e struttura dell'ambiente cloud.

Esistono due modalità di attivazione di SCC:

- Standard: con l'attivazione del modulo "Security Health Analytics";
- Premium: con l'attivazione opzionale di diversi moduli di SCC.

Per maggiori informazioni sulle versioni e funzionalità di GCP SCC si prega di far riferimento alla guida ufficiale fornita dal cloud provider Google: [Panoramica di Security Command Center](#).

Nell'ambito del servizio Secure Public Cloud su GCP, l'utente finale ha la responsabilità di gestione e consultazione dell'istanza SCC attivata sui progetti inclusi dentro la folder "Teams".

Il Polo Strategico Nazionale, per policy, attiva il componente SCC nei progetti dell'utente finale in modalità "Standard". A discrezione dell'utente finale l'eventuale attivazione a livello Premium e la gestione dei moduli aggiuntivi da attivare.

[Link documentazione GCP](#)

3.2 *Networking*

Il design di rete è basato sul modello Hub&Spoke questo layout permette al PSN di erogare, alle PA, un'infrastruttura di sicurezza preconfezionata e standardizzata per garantire il corretto livello di protezione per i workload che le PA porteranno nei CSP.

La soluzione Hub&Spoke ha, a sua volta, due declinazioni:

- Soluzione con IDS Intrusion Detection System;
- Soluzione con IPS Intrusion Prevention System;

Le due soluzioni si differenziano dal punto di vista del networking per il modello di routing e di interconnessione fra Hub e Spoke.

3.2.1 *Soluzione con IDS*

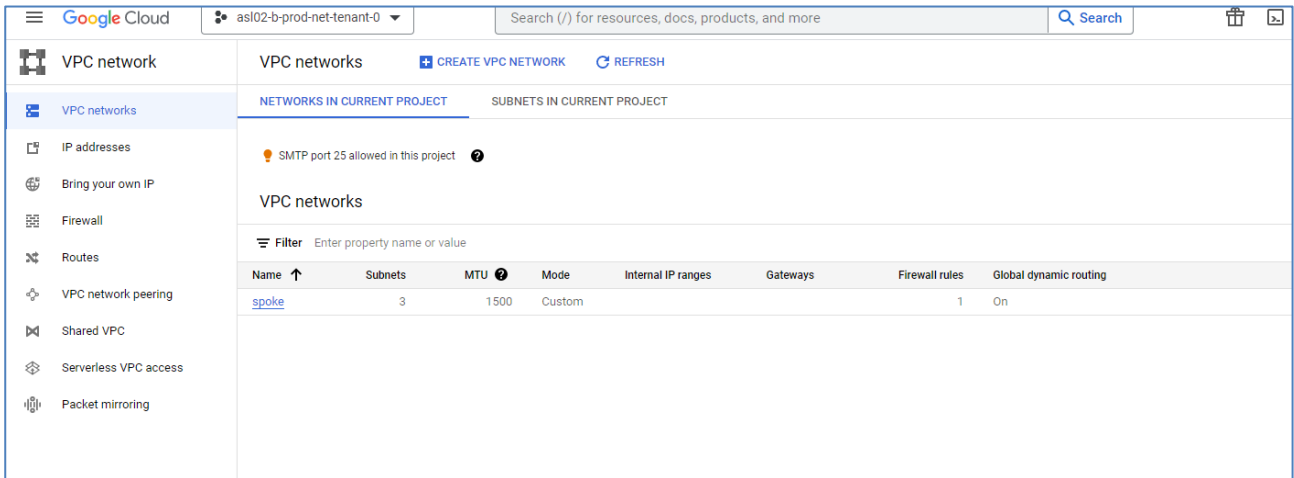
Nella Architettura di Rete con IDS la VPC dell'Hub e la Shared-VPC dello Spoke sono in Peering, ciò significa che esiste un routing tra le reti IP presenti nell'Hub e le reti IP presenti nello Spoke. A sua volta sullo Spoke è presente il Peering verso il Servizio di IDS – Cloud IDS.

Nell'architettura di Rete con IPS, viene introdotta una nuova VPN di Transit nell'HUB. Tra la VPN di Hub e la VPN di Transit viene inserito un Cluster di appliance che monta a bordo la soluzione IPS. Il Peering con la Shared-VPC dello Spoke è realizzato con la VPN di Transit, ciò significa che esiste un routing tra le reti presenti nello Spoke e la rete di Transit. Le Appliance IPS gestiscono il routing tra la rete di Transit e la VPN di Hub. In questo modello la gestione del routing avviene come di seguito indicato:

- Sebbene il traffico tra Spoke e Hub possa essere controllato dall'IPS, nella parte di Spoke è presente un Peering verso il Servizio di IDS Cloud IDS che permette di analizzare il traffico east-west.

Panoramica VPC

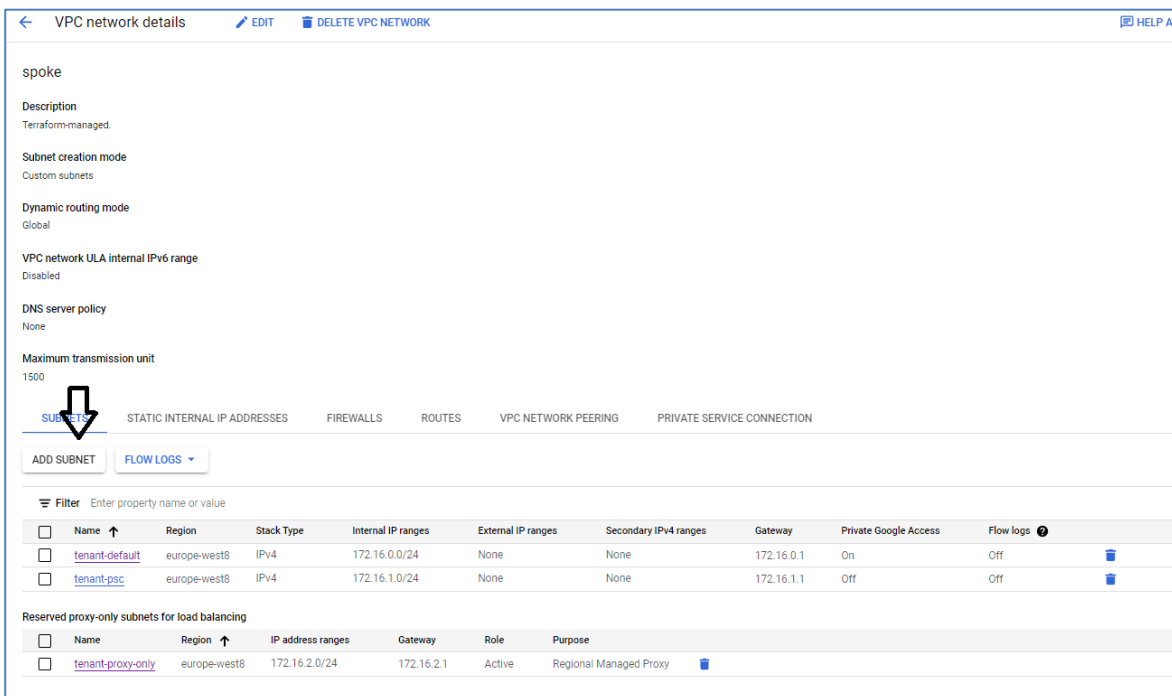
La Shared VPC è la zona di rete dedicata ad ospitare i workload della PA, l'utente dopo avere impostato il Project di Spoke (area dedicata ad ospitare un workload), può vedere la sua Shared VPC andando sulla Sezione “VPC Network” di Google Console:



The screenshot shows the Google Cloud console interface for VPC networks. The left sidebar contains a navigation menu with options like IP addresses, Bring your own IP, Firewall, Routes, VPC network peering, Shared VPC, Serverless VPC access, and Packet mirroring. The main content area is titled 'VPC networks' and includes a search bar and a 'CREATE VPC NETWORK' button. Below this, there's a section for 'NETWORKS IN CURRENT PROJECT' and 'SUBNETS IN CURRENT PROJECT'. A table lists the VPC networks, with one network named 'spoke' having 3 subnets, an MTU of 1500, and custom mode.

Tutte le subnet all'interno della Shared VPN si vedono tra di loro come routing.

All'interno dello Spoke l'utente potrà creare nuove subnet utilizzando il menu Shared VPC selezionando Add subnet:



The screenshot shows the 'VPC network details' page for a network named 'spoke'. The page includes a description, subnet creation mode (Custom subnets), dynamic routing mode (Global), and VPC network ULA internal IPv6 range (Disabled). A section for 'SUBNETS' is highlighted with a black arrow, showing a table of subnets. Below this, there's an 'ADD SUBNET' button and a 'FLOW LOGS' dropdown. The subnets table lists three subnets: 'tenant-default', 'tenant-psc', and 'tenant-proxy-only'.

Name	Region	Stack Type	Internal IP ranges	External IP ranges	Secondary IPv4 ranges	Gateway	Private Google Access	Flow logs
tenant-default	europe-west8	IPv4	172.16.0.0/24	None	None	172.16.0.1	On	Off
tenant-psc	europe-west8	IPv4	172.16.1.0/24	None	None	172.16.1.1	Off	Off

I punti di attenzione durante la creazione della nuova subnet sono:

- Piano di indirizzamento coerente ai piani presenti nel Secure Public Cloud e con il piano di indirizzamento del cliente on prem, se questi ultimi sono raggiunti direttamente attraverso una visibilità di rete diretta;
- Se siano nella configurazione con IPS fare attenzione che il piano di indirizzamento delle subnet sia coerente con il routing Nord/Sub definito nella landing zone dell'HUB.

- Inserire la Region italiana di riferimento;
- Abilitare l'accesso al Private Service Connect PSC senza indirizzo IP pubblico.

Add a subnet

Name *

Lowercase letters, numbers, hyphens allowed

Description

VPC Network

Region *

Purpose
☐ Regional Managed Proxy
☐ Private Service Connect
☒ None

IP stack type
☒ IPv4 (single-stack)
☐ IPv4 and IPv6 (dual-stack)

IPv4 range *

E.g. 10.0.0.0/24

CREATE SECONDARY IPV4 RANGE

Private Google Access
☒ On
☐ Off

Flow logs
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Logging. [Learn more](#)
☐ On
☒ Off



CANCEL ADD

3.2.4 Gestione DNS

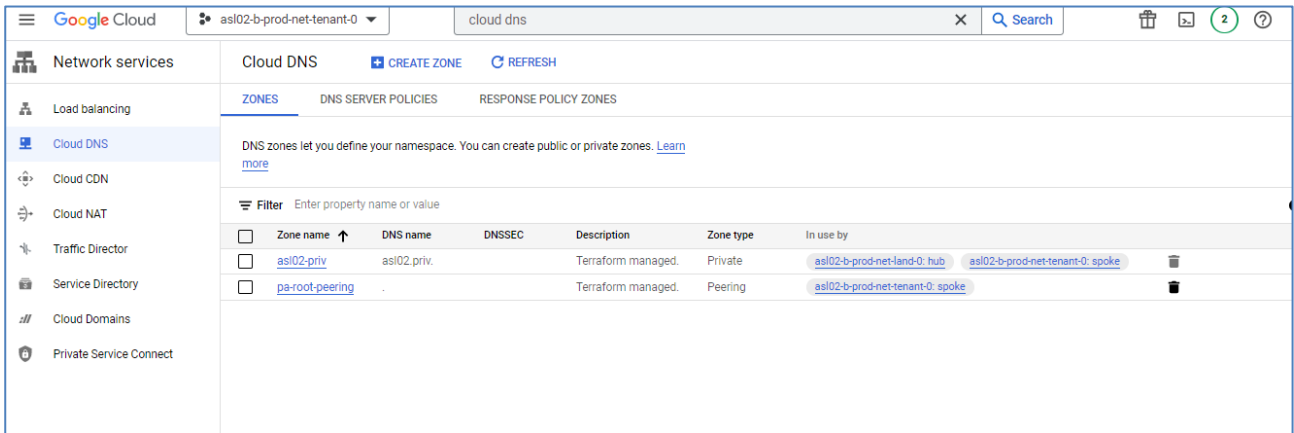
La gestione del DNS nel Secure Public Cloud prevede due Cloud DNS così definiti:

- Dispatcher DNS posizionato all'interno della Landing Zone HUB ;
- Local DNS posizionato all'interno della zona Spoke.

Il Dispatcher DNS è in grado di risolvere tutte le zone internet, di essere configurato in peering con zone terze e se necessario può risolvere in forwarding le zone on prem della PA.

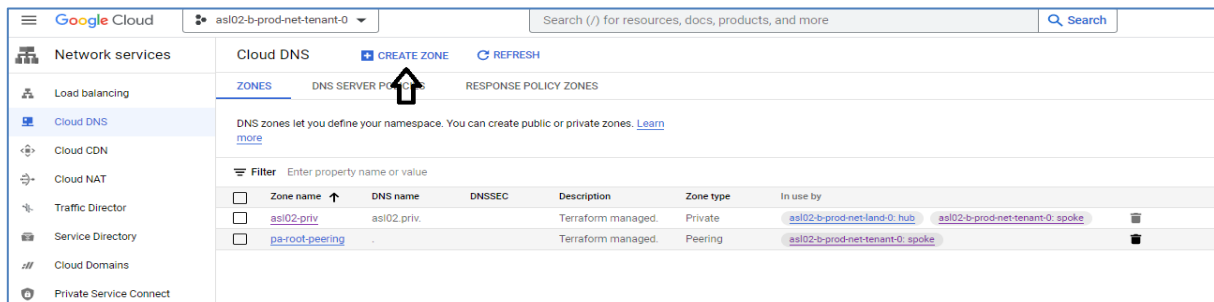
Il Local DNS risolve le zone interne degli spoke e ha una configurazione in peering con il Dispatcher per tutte le zone che non conosce.

Per gestire il DNS posizionarsi nel progetto di riferimento e selezionare "Cloud DNS":



Qui l'utente può gestire i record in una zona già presente o creare delle nuove Zone DNS private.
Nell'ipotesi di creare una nuova Zone DNS privata “test-zone” test.zone:

1. Selezionare Create Zone:



2. inserire i dati obbligatori: Nome, zona, tipo (Private) e Shared VPN (Spoke):

Zone type ?

☒ Private ←

☐ Public

Zone name * test-zone ?
Example: example-zone-name

DNS name * test.zone ← ?
Example: myzone.example.com

Description

Options * Default (private) ?

Networks spoke ← ?
Your private zone will be visible to the selected networks

After creating your zone, you can add resource record sets and modify the networks your zone is visible on.

CREATE CANCEL

- Inserire un record A di test: localhost.test.zone = 127.0.0.01

← **Zone details** EDIT ADD NETWORKS DELETE ZONE

test-zone

DNS name test.zone.

Type Private

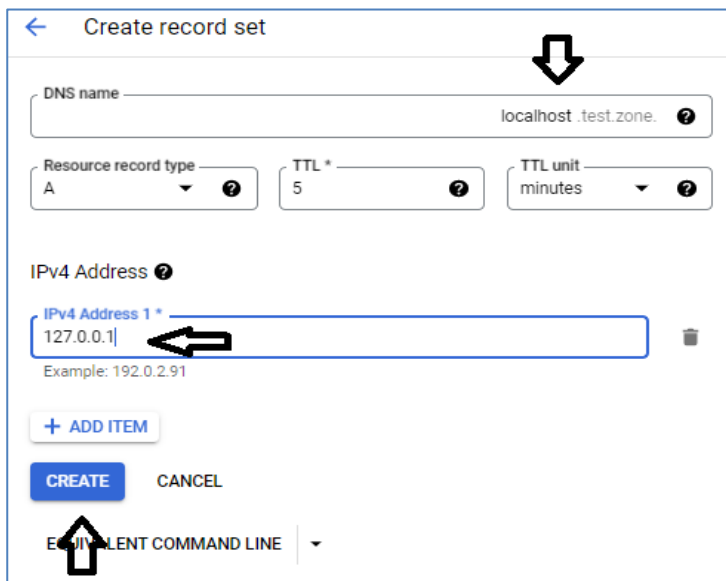
RECORD SETS IN USE BY

+ ADD STANDARD + ADD WITH ROUTING POLICY DELETE RECORD SETS REFRESH

Filter Filter record sets

	DNS name ↑	Type	TTL (seconds)	Routing policy
☐	test.zone.	SOA	21600	Default
☐	test.zone.	NS	21600	Default

EQUIVALENT REST



← Create record set

DNS name

Resource record type TTL * TTL unit

IPv4 Address

+ ADD ITEM

CREATE CANCEL

EQUIVALENT COMMAND LINE

4. Risultato atteso:

test-zone

DNS name

test.zone.

Type

Private

RECORD SETS

IN USE BY

+ ADD STANDARD

+ ADD WITH ROUTING POLICY

DELETE RECORD SETS

REFRESH

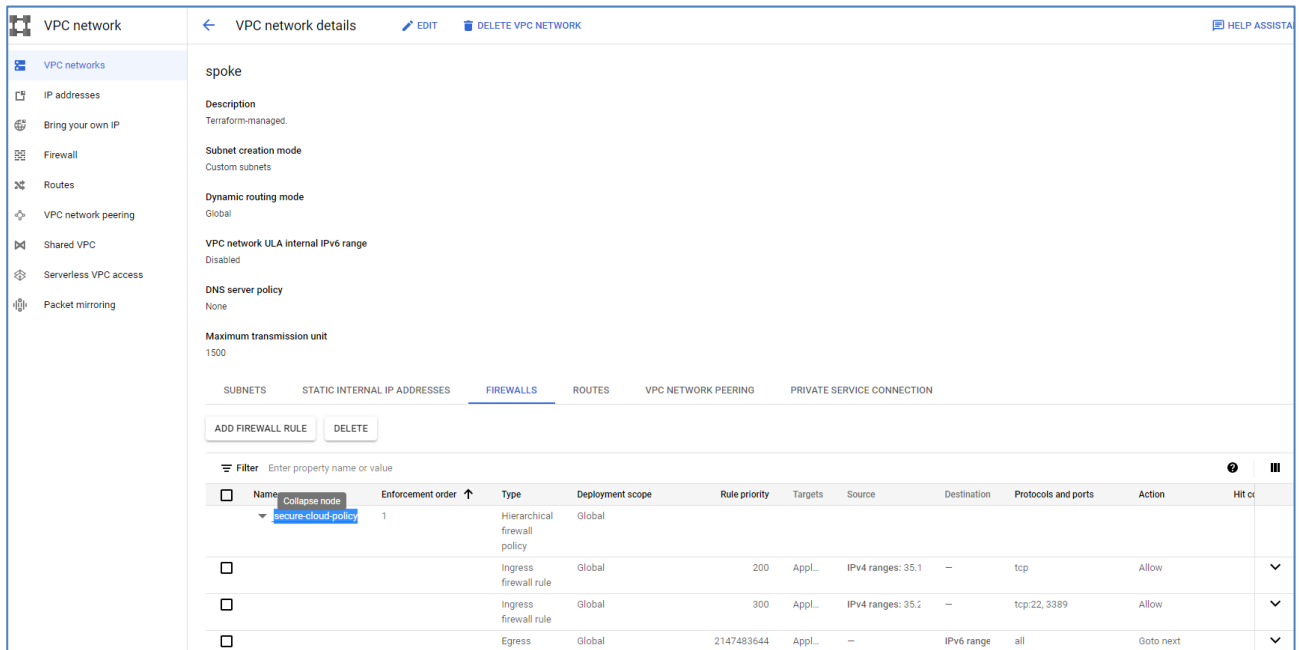
Filter

Filter record sets

☐	DNS name ↑	Type	TTL (seconds)	Routing policy		
☐	localhost.test.zone.	A	300	Default	▼	✎
☐	...	...	...	...	▼	✎

3.2.5 Gestione Firewall

La shared VPC è soggetta alle Hierarchicals Firewall Policy gestite dal PSN. Queste policy possono essere consultate tramite la GIU Google Console nella sezione “VPC Network”, selezionando nella Shared VPC Spoke per poi esplorare il TAB FIREWALLS aprendo le “secure-cloud-policy”:



Tutte le policy firewall si applicano esclusivamente ai workload (as ed: Vm).

L'utente ha la facoltà di creare nuove firewall policy, tenendo presente che per Default tutto il traffico in uscita da una vm è permesso e tutto il traffico in ingresso è negato.

Ad esempio, se si vuole instaurare una comunicazione fra due Vm occorre creare una policy che permetta alla VM di destinazione di ricevere traffico proveniente dalla VM sorgente per la specifica porta.

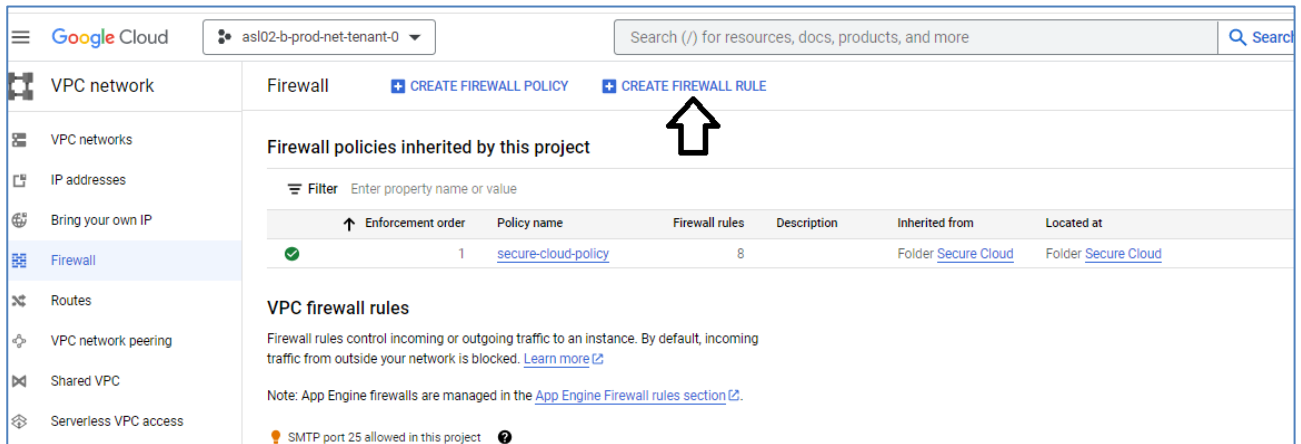
I target delle Policy possono essere:

1. Tutta la rete
2. Solo alcuni Computer Account (ad ogni Vm è associato un Computer Account)
3. Associazione a Network-tag (ad ogni Vm possono essere associato dei Network-Tag)

Nelle Firewall Policy è possibile creare singole Regole Firewall o gruppi di Regole Firewall, la priorità delle policy riflette l'ordine di esecuzione delle stesse.

Ad esempio, se volessimo consentire il traffico SSH in ingresso dall'IP 1.1.1.1 a tutte le Vm che abbiamo il Network-Tag "ssh" tra le proprietà, si procede come segue:

1. Selezionare "VPC Network" e aprire il menu "Firewall":



The screenshot shows the Google Cloud Firewall console for project 'asl02-b-prod-net-tenant-0'. The left sidebar lists VPC network resources, with 'Firewall' selected. The main panel shows 'Firewall policies inherited by this project' with a table containing one policy: 'secure-cloud-policy' with enforcement order 1 and 8 firewall rules. A black arrow points to the 'CREATE FIREWALL RULE' button at the top right of the panel.

Enforcement order	Policy name	Firewall rules	Description	Inherited from	Located at
1	secure-cloud-policy	8		Folder Secure Cloud	Folder Secure Cloud

2. Selezionare Create Firewall Rule, inserendo i seguenti parametri:

Nome: allow-ssh

Network: spoke

Direction Of Traffic: Ingress

Specified Targets Tags: ssh

IPv4 Ranges: 1.1.1.1

Action On Match: Allow

Specified Protocols and Ports: TCP: 22

←

Create a firewall rule

traffic from outside your network is blocked. [Learn more](#)

Name *

allow-ssh

?

Lowercase letters, numbers, hyphens allowed

Description

Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Logging. [Learn more](#)

☐ On
 ☒ Off

Network *

spoke

▼

?

Priority *

1000

CHECK PRIORITY OF OTHER FIREWALL RULES

?

Priority can be 0 - 65535

Direction of traffic ?

☒ Ingress
 ☐ Egress

Action on match ?

☒ Allow
 ☐ Deny

Targets

Specified target tags

▼

?

Target tags *

ssh

✕

Source filter

IPv4 ranges

▼

?

Source IPv4 ranges *

1.1.1.1

✕

?

Second source filter

None

▼

?

Protocols and ports ?

☐ Allow all
 ☒ Specified protocols and ports

☒ TCP

Ports

22

E.g. 20, 50-60

3.2.6 Cloud IDS

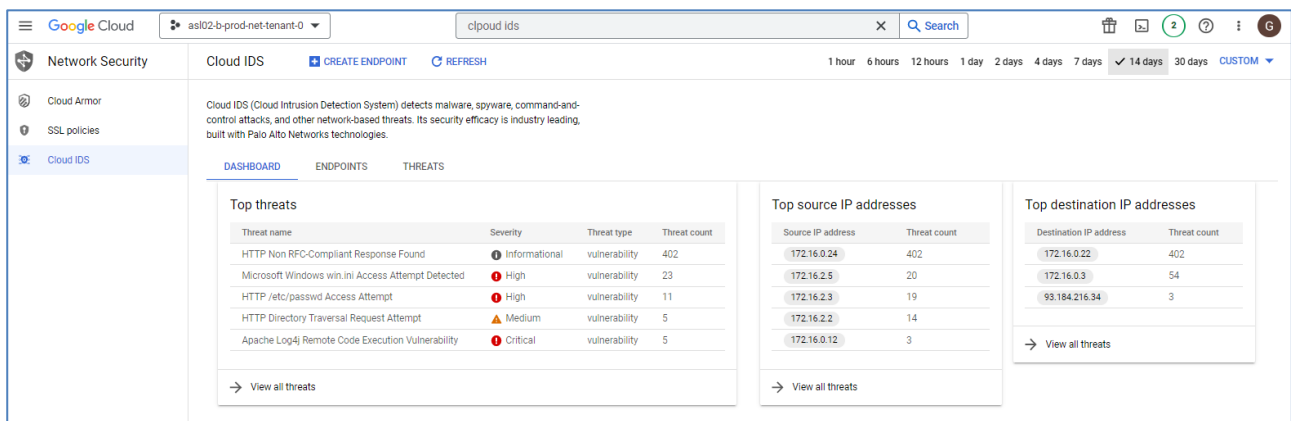
Il servizio di cloud IDS è fornito in collaborazione Palo Alto. e la documentazione è consultabile al seguente link:

<https://cloud.google.com/intrusion-detection-system/docs/overview>

Per attivare il servizio Cloud IDS si utilizza un Peering tra la Shared VPC spoke e gli Appliance Palo al Network a cui viene inviato il traffico in mirror che gira sulla rete Shared VPC.

Il peering viene fatto utilizzando un rete di classe B staccata dalla supernet riservata agli Internet providers: 100.64. 0.0/10; in questo esempio: 100.127.0.0/16

Gli eventi cloud IS sono consultabili posizionandosi sul Progetto di Tenant e selezionando “Network Security” e poi “Cloud IDS” e poi “Dashboard”:



The screenshot shows the Google Cloud Cloud IDS dashboard. The left sidebar contains 'Network Security' with sub-items 'Cloud Armor', 'SSL policies', and 'Cloud IDS'. The main content area is titled 'Cloud IDS' and includes a description: 'Cloud IDS (Cloud Intrusion Detection System) detects malware, spyware, command-and-control attacks, and other network-based threats. Its security efficacy is industry leading, built with Palo Alto Networks technologies.' Below this are tabs for 'DASHBOARD', 'ENDPOINTS', and 'THREATS'. The 'DASHBOARD' tab is active, displaying three tables:

Threat name	Severity	Threat type	Threat count
HTTP Non RFC-Compliant Response Found	Informational	vulnerability	402
Microsoft Windows win.ini Access Attempt Detected	High	vulnerability	23
HTTP /etc/passwd Access Attempt	High	vulnerability	11
HTTP Directory Traversal Request Attempt	Medium	vulnerability	5
Apache Log4j Remote Code Execution Vulnerability	Critical	vulnerability	5

Source IP address	Threat count
172.16.0.24	402
172.16.2.5	20
172.16.2.3	19
172.16.2.2	14
172.16.0.12	3

Destination IP address	Threat count
172.16.0.22	402
172.16.0.3	54
93.184.216.34	3

Ogni volta che viene creata una nuova Subnet nella Shared VPC su cui siano state deployate delle Vm, essa va aggiunta al Cloud IDS Mirror, altrimenti non potrà essere monitorata da Cloud IDS.

Quindi occorre andare nella sezione VPC Network e poi “Packet Mirroring” e modificare la policy di mirror in essere:

 **VPC network**

- VPC networks
- IP addresses
- Bring your own IP
- Firewall
- Routes
- VPC network peering
- Shared VPC
- Serverless VPC access
- Packet mirroring**

Edit policy details

✓

Define policy overview

✓

Select VPC network

3

Select mirrored source

Specify the source that will be mirrored. Packet mirroring captures all the ingress and egress traffic of mirrored instances.

Mirrored source

Select at least one mirrored source

☒ Select one or more subnetworks

Instances in these subnetworks are mirrored

Select subnet *

new-subnet, tenant-default, tenant-proxy-only, and tenant-psc

☐ Select with network tag

Instances with matching tags are mirrored

☐ Select individual instances

Selected instances are mirrored

CONTINUE

4

Select collector destination

5

Select mirrored traffic

SUBMIT

CANCEL

3.2.7 IAP

L'accesso amministrativo alle VM presenti nei progetti è garantito dalla soluzione attraverso l'utilizzo della applicazione IAP.

Inoltre, per le sole Vm linux è possibile effettuare l'accesso SSH direttamente da Gui Google Console.

L'applicazione IAP è scaricabile al seguente link:

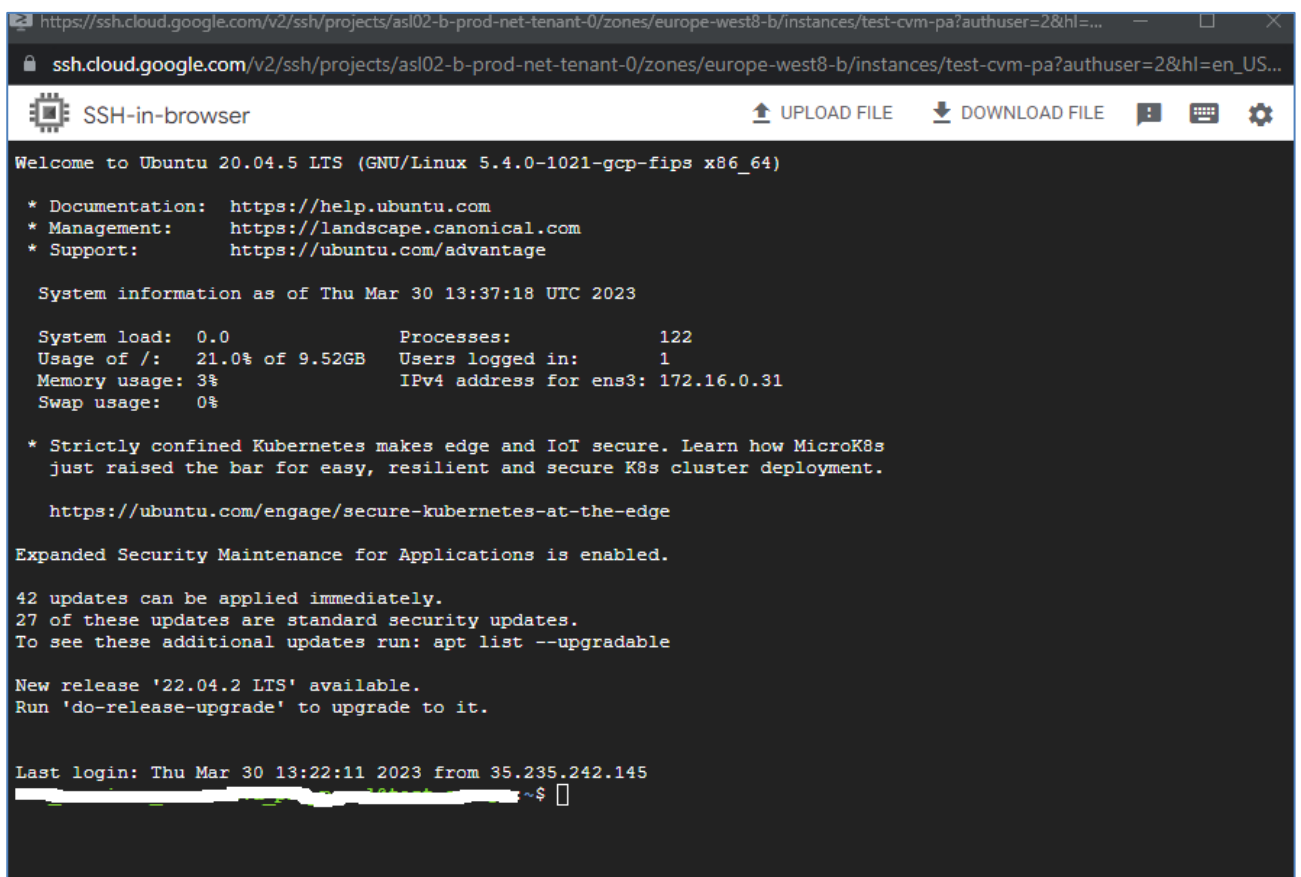
<https://github.com/GoogleCloudPlatform/iap-desktop>

Per l'accesso diretto in SSH da Gui Google Console alle Vm Linux seguire i seguenti passi:

1. Accedere a Google Console con il proprio account (<https://console.cloud.google.com>):
2. Selezionare la sezione "Computer Engine" e "Vm Instances"
3. Selezionare SSH della Vm a cui si vuole accedere:

INSTANCES									
OBSERVABILITY									
INSTANCE SCHEDULES									
VM instances									
Filter Enter property name or value									
☐	Status	Name ↑	Zone	Recommendations	In use by	Internal IP	External IP	Network tags	Connect
☐	✓	test-cvm-pa	europe-west8-b			172.16.0.31 (nic0)		ssh	SSH ↓
☐	✓	test-vm-pa-rhel-9	europe-west8-b			172.16.0.30 (nic0)		ssh	SSH ↓
☐	✓	test-vm-pa-windows-2022	europe-west8-b			172.16.0.14 (nic0)		ssh	RDP ↓
Related actions									

4. Nel Pop-Up del browser si aprirà la console del terminale, l'autenticazione con scambio di Chiavi sarà trasparente per l'utente.



```

https://ssh.cloud.google.com/v2/ssh/projects/asl02-b-prod-net-tenant-0/zones/europe-west8-b/instances/test-cvm-pa?authuser=2&hl=en_US...
SSH-in-browser
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-1021-gcp-fips x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:       https://ubuntu.com/advantage

System information as of Thu Mar 30 13:37:18 UTC 2023

System load:  0.0          Processes:            122
Usage of /:   21.0% of 9.52GB   Users logged in:     1
Memory usage: 3%          IPv4 address for ens3: 172.16.0.31
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
  just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is enabled.

42 updates can be applied immediately.
27 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

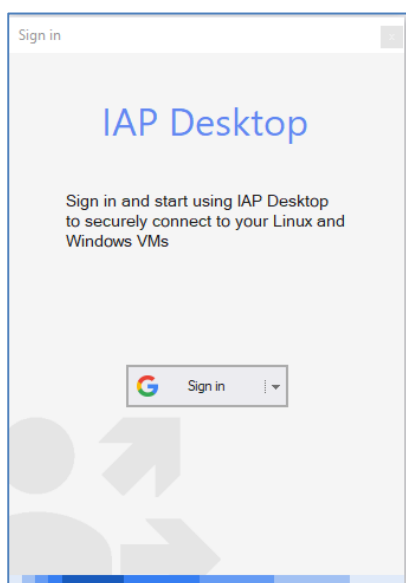
New release '22.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Mar 30 13:22:11 2023 from 35.235.242.145
~$

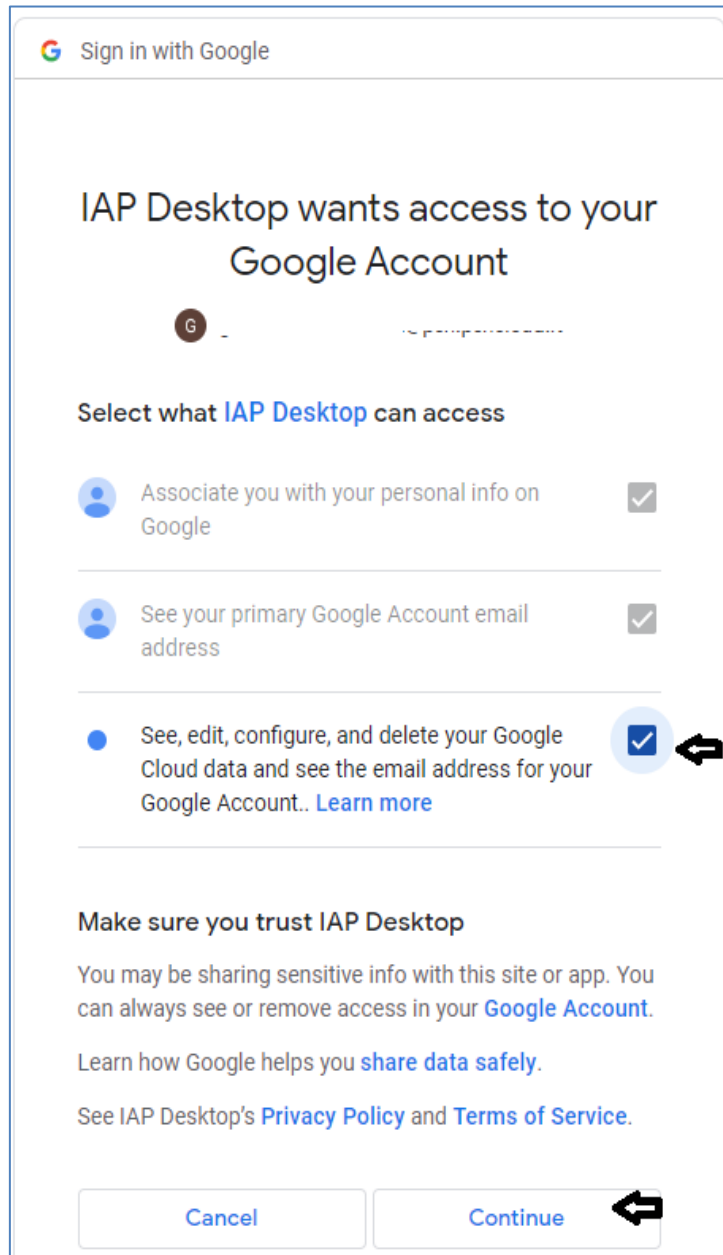
```

In caso di utilizzo della versione applicazione dello IAP Desktop seguire i seguenti passi:

1. Installare IAP Desktop
2. Attivare IAP Desktop fare Sign In:



Al termine dell'operazione di Sign cliccare sull'ultima punta e confermare con "Continue".



Sign in with Google

IAP Desktop wants access to your Google Account

Select what IAP Desktop can access

- ☒ Associate you with your personal info on Google
- ☒ See your primary Google Account email address
- ☒ See, edit, configure, and delete your Google Cloud data and see the email address for your Google Account.. [Learn more](#)

Make sure you trust IAP Desktop

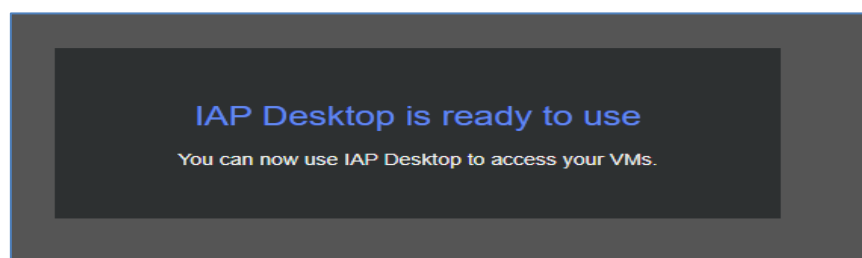
You may be sharing sensitive info with this site or app. You can always see or remove access in your [Google Account](#).

Learn how Google helps you [share data safely](#).

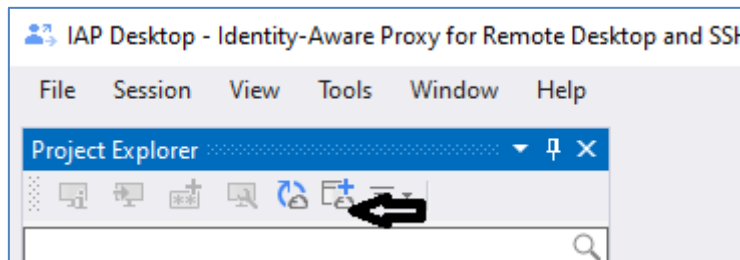
See IAP Desktop's [Privacy Policy](#) and [Terms of Service](#).

[Cancel](#) [Continue](#)

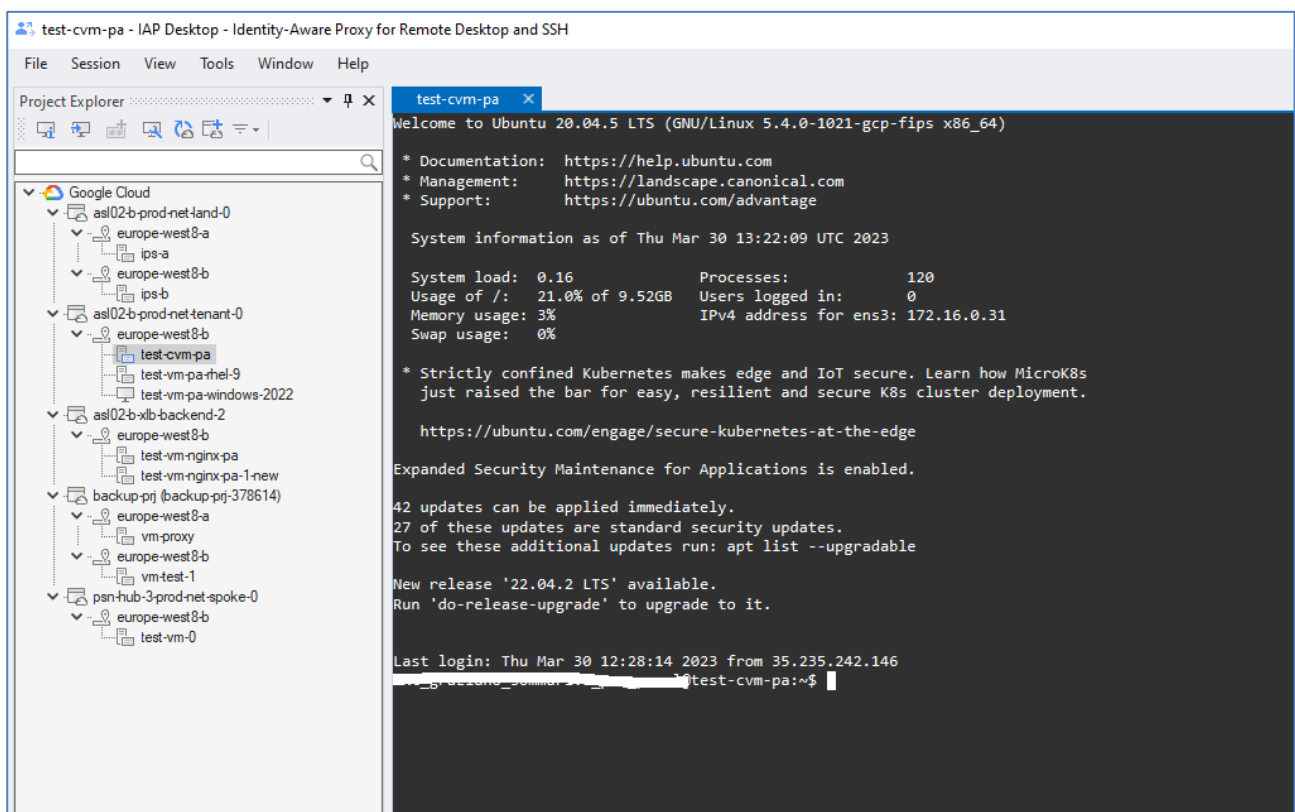
A questo punto IAP Desktop è pronto:



3. Attivare IAP Desktop e aggiungere il progetto desiderato cliccando Add Project:



4. Selezione il Progetto da aggiungere:
5. Cliccare sul sistema per connettersi
6. Il prompt si presenta come segue:



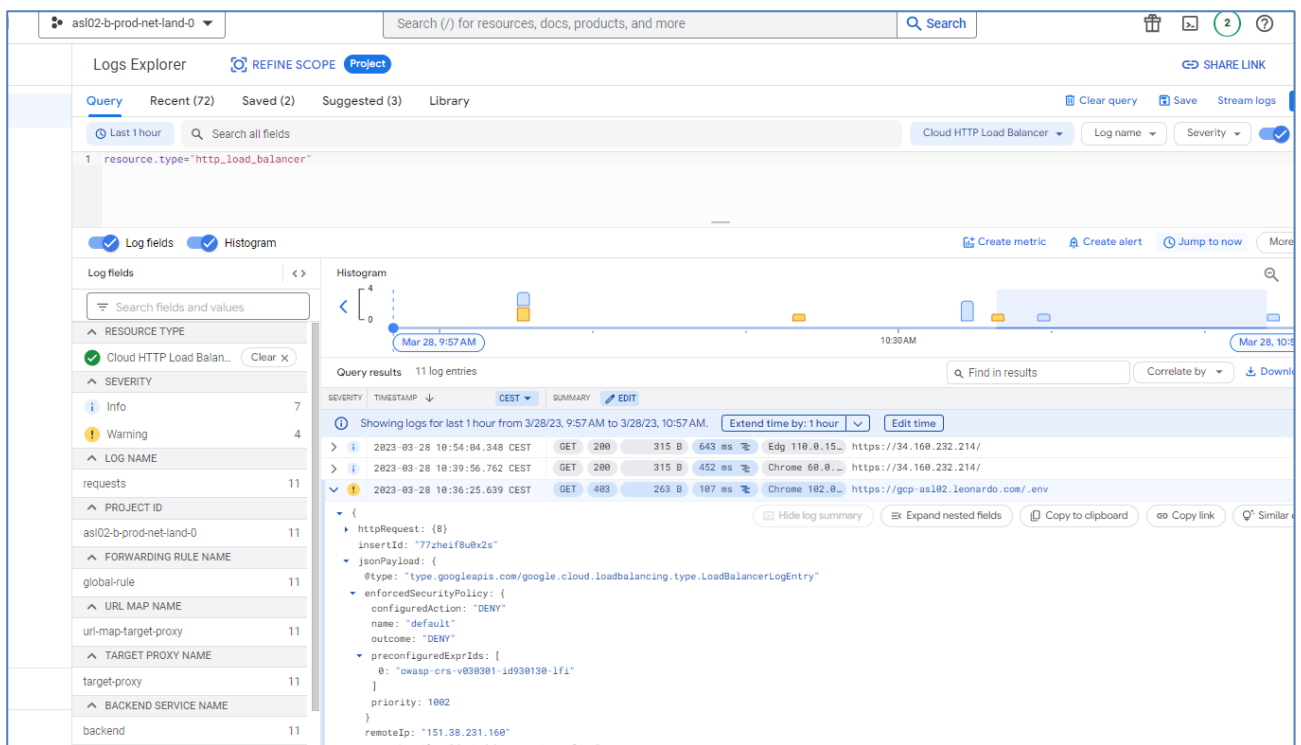
3.2.8 Cloud Armor

Il PSN attiva Cloud Armor come WAF per l'esposizione dei servizi HTTP della PA, configurando e attivando le policy relative alla "OWASP Top 10".

La configurazione di Cloud Armor è competenza del PSN, la PA ha la facoltà di accedere ai Log di cloud Armor.

I log di cloud Armor sono accessibili posizionandosi nel project di landing HUB e nella sezione "Logging"

In calce un esempio di Log su cloud Armor:



Ogni richiesta di modifica della configurazione di Cloud Armor sarà fatta via opportuna Service Request al PSN.

La documentazione ufficiale di GCP di Cloud Armor è consultabile a questo link: <https://cloud.google.com/armor/docs/cloud-armor-overview>

3.2.9 Esposizione Web server su Global Load Balancer (Gestito Da PSN)

Al fine di esporre un servizio Web della PA su Internet, nella Landing zone della PA è presente un Global Load-Balancer, che espone un servizio in HTTP e HTTPS protetto da Cloud Armor che fornisce la funzionalità di Web Application Firewall.

La Gestione Il Global Load-Balancer e del Cloud Armor sono in carico al PSN.

Global Load-Balancer è configurato per inoltrare le richieste HTTPS ad un Internal Load Balancer presente sul Project della PA, il quale inoltra le richieste ai workload presenti nel Project di xlb-backend della PA stessa.

Nella configurazione attuale il servizio esposto dal Global Load-Balancer fa riferimento ad un server Web della PA istanziato su una macchina Linux del Project xlb-backend .

La URL esposta è la seguente: <https://asl02.polostrategiconazionale.it> la cui risoluzione DNS restituisce l'indirizzo l'IP 34.160.232.214.

Per agevolare l'accesso al sito Web, Il Global Load-Balancer espone anche la porta HTTP(porta TCP/80); a fronte di una richiesta HTTP, il Global Load-Balancer invia una richiesta di "redirect" da HTTP a HTTPS al Browser del client.

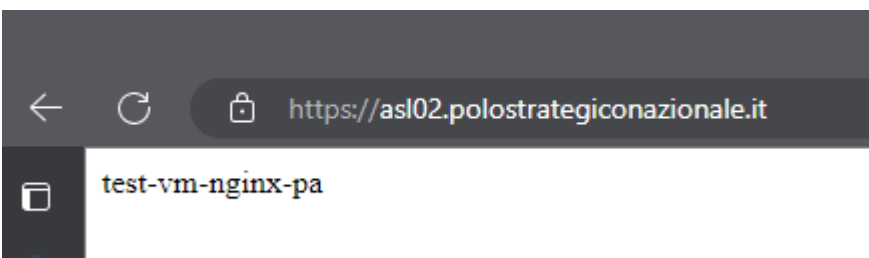
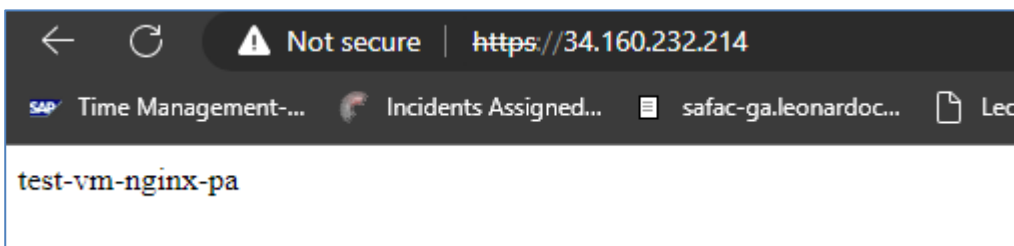
In questo modo, sia che si acceda a <http://asl02.polostrategiconazionale.it>, che a <http://34.160.232.214>, si viene rediretti sulla corrispettiva URL HTTPS.

Il Global Load-Balancer espone su HTTPS un Certificato di test che deve essere accettato dal Browser del client.

Provando ad accedere alle seguenti URL:

- <http://34.160.232.214>
- [http:// asl02.polostrategiconazionale.it](http://asl02.polostrategiconazionale.it)

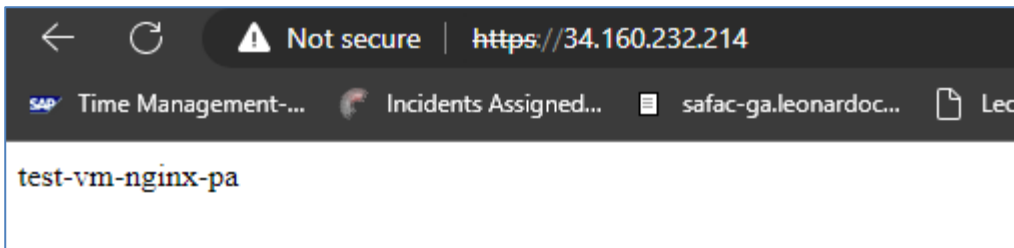
si arriva sulla pagina HTTPS esposta dal server della PA il cui testo è "test-vm-nginx-pa":



L'utente della PA può creare nuovi workload ed esporli attraverso il Global Load Balancer.

Lo “Use Case” che segue ha lo scopo di illustrare come la PA possa esporre un nuovo Workload aggiungendo un nuovo Web Server, modificando la URL-Map creando una nuova “Routing Rule” per puntare anche al nuovo servizio.

Al termine della configurazione la URL <http://34.160.232.214> continua a mostrare la pagina originale:



Se invece si punta alla URL <http://asl02.polostrategiconazionale.it>, si arriva sul nuovo Workload.

Per raggiungere lo scopo, occorre prima creare una Vm nel progetto di Backend analoga a quella che esiste già:

Name: test-vm-nginx-pa-1-new

Zone: europe-west8-b

Machine type: e2-standard-2

Network: Tenant-default

Network tags lb-http lb-https

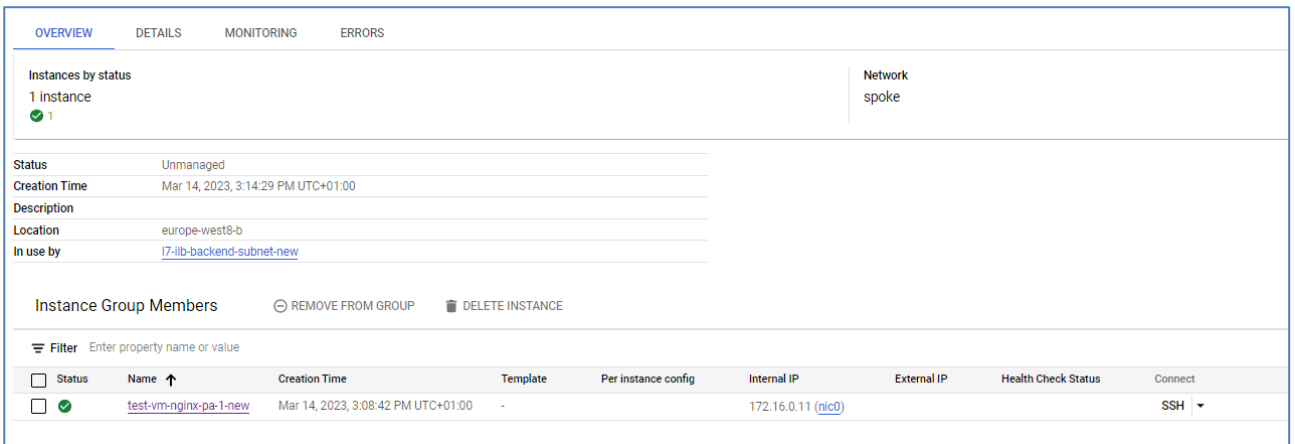
Occorre installare nginx come web server, e configurare la pagina web in modo da poterla distinguere da quella in essere:

1. Collegarsi al sistema in ssh con IAP
2. Dare i seguenti comandi apt update
3. “apt update”
4. “apt install iputils-ping bind9-dnsutils nginx-light”
5. “cd /var/www/html/”
6. “vi index.nginx-debian.html” e modificare come:

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
  body {
    width: 35em;
    margin: 0 auto;
    font-family: Tahoma, Verdana, Arial, sans-serif;
  }
</style>
</head>
<body>
<h1>NUOVO HTTP</h1>
</body>
</html>
~
~
~
```

di seguito vengono indicati i passaggi della configurazione dei Load Balancer:

1. Si ricorda che l'Internal Load Balancer è in grado di puntare solo a "Instance-Group" e non direttamente una Vm;
Dopo essersi posizionati nel Project "xlb-backend", creare un Instance-Group di tipo UNMANAGED inserendo la Vm appena creata:



Instances by status
1 instance

Status Unmanaged
Creation Time Mar 14, 2023, 3:14:29 PM UTC+01:00
Description
Location europe-west8-b
In use by [l7-ilb-backend-subnet-new](#)

Instance Group Members [REMOVE FROM GROUP](#) [DELETE INSTANCE](#)

Filter Enter property name or value

Status	Name	Creation Time	Template	Per instance config	Internal IP	External IP	Health Check Status	Connect
☒	test-vm-nginx-pa-1-new	Mar 14, 2023, 3:08:42 PM UTC+01:00	-		172.16.0.11 (nic0)			SSH

2. Sempre restando nel Project "xlb-backend", bisogna spostarci nella Sezione "Load Balancing":

Google Cloud

asl02-b-ilib-backend-2

load bala

Navigation menu

balancing

+ CREATE REGIONAL BACKEND SERVICE

REFRESH

DELETE

PERMISSIONS

LOAD BALANCERS

BACKENDS

FRONTENDS

Filter

Enter property name or value

☐	Name ↑	Backend type	Scope	Protocol	IP stack type	Load balancer
☐	i7-ilib-backend-subnet	Backend service (Internal)	Regional (europe-west8)	HTTP (Internal)	IPv4	

- o l'Instance-Group appena creato va abbinato ad un nuovo BACKEND del servizio Bilanciatore di Carico Regionale;
- o Il BACKEND deve essere di tipo "INTERNAL MANAGED", e istanziato nella stessa zona del nuovo Instance-Group.

Il nuovo BACKEND può usare l'Health Check già presente che punta alla porta dove risponde il server HTTP nell'Instance-Group:

Lo "Use Case" prevede l'utilizzo di:
Nuovo BACKEND: i7-ilib-backend-subnet-new

I7-ilb-backend-subnet-new

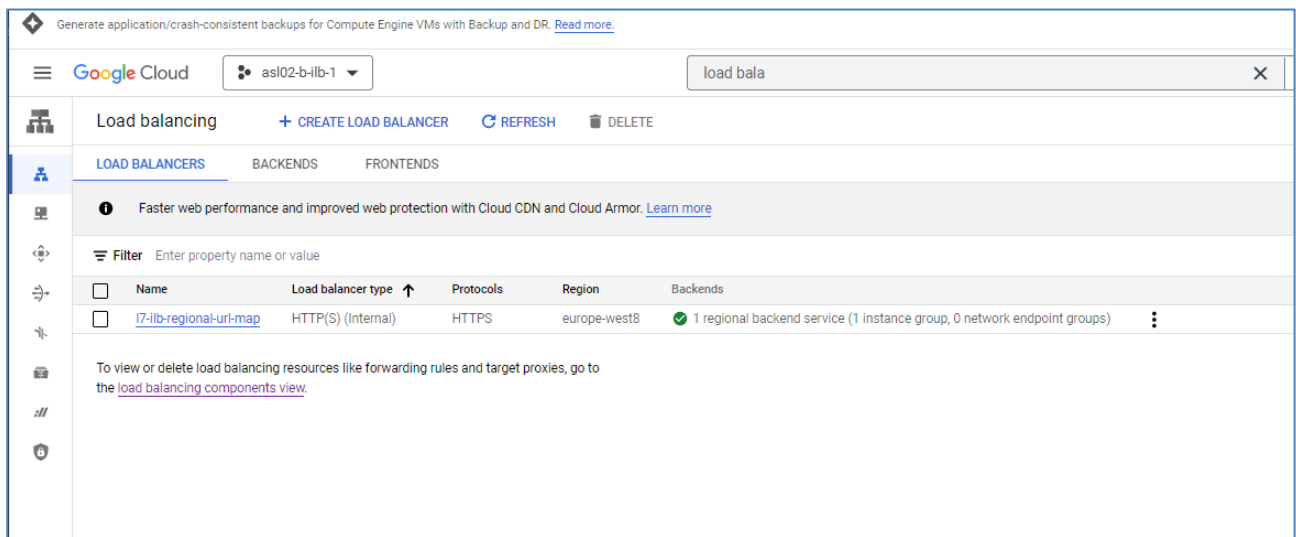
General properties

Region	europe-west8
Load balancer type	Regional Internal HTTP(S) Load Balancing (INTERNAL_MANAGED)
Endpoint protocol	HTTP
In use by	Not used
Timeout	30 seconds
Health check	I7-ilb-hc VIEW HEALTH CHECK DETAILS
Session affinity	None
Connection draining timeout	300 seconds

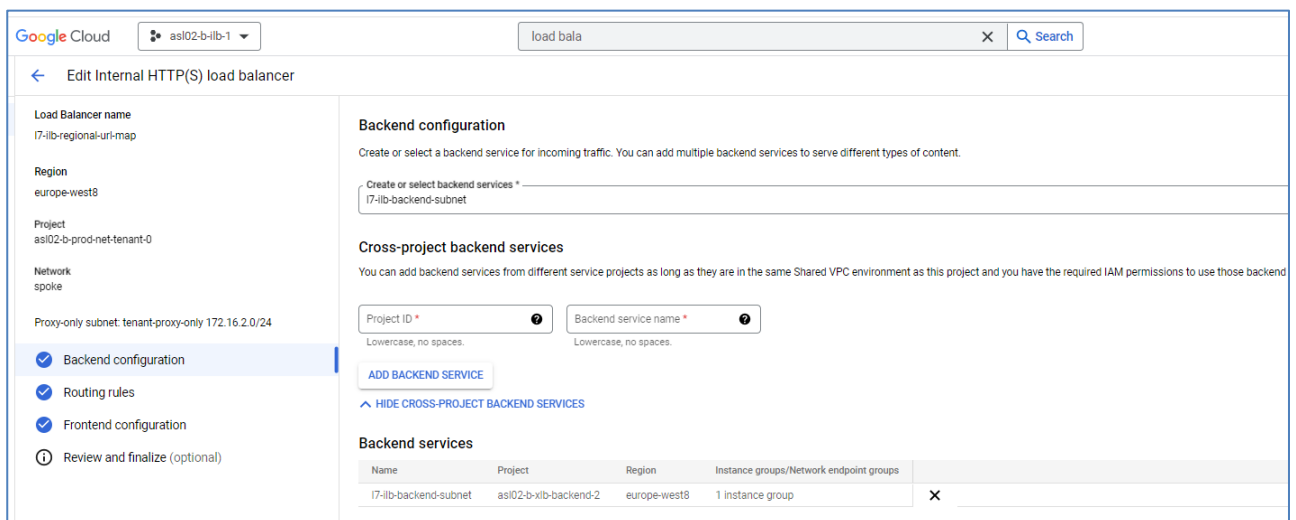
Backends

Name	Type	Scope	Healthy	Autoscaling	Balancing mode	Selected ports	Capacity
test-vm-nginx-pa-new	Instance group	europe-west8-b	1 of 1	No configuration	Max backend utilization: 80%	80	100%

- La modifica della URL-MAP prevede di spostarsi nel project "ilib".
Dopo essersi posizionati nel project Project "ilib", utilizzare la funzionalità di "Load Balancing" dove è presente l'Internal LOAD BALANCER



4. Modificare l'Internal LOAD BALANCER (l7-ilb-regional-url-map) aggiungendo un Cross Backend Services impostando correttamente il "Project ID" e il nuovo "Backend-Service Name" creato al punto "2".
Fare "Edit" su l7-ilb-regional-url-map e modificare la parte Backend configuration:



Lo "Use Case" prevede l'utilizzo di:
Project id: asl02-b-xlb-backend-2
Backend service name: l7-ilb-backend-subnet-new

Backend configuration

Create or select a backend service for incoming traffic. You can add multiple backend services to serve different types of content.

Create or select backend services *

I7-ilb-backend-subnet

Cross-project backend services

You can add backend services from different service projects as long as they are in the same Shared VPC environment as this project a

Project ID *

asl02-b-xlb-backend-2

Lowercase, no spaces.

Backend service name *

I7-ilb-backend-subnet-new

Lowercase, no spaces.

ADD BACKEND SERVICE

↩

^ HIDE CROSS-PROJECT BACKEND SERVICES

- Il passo successivo prevede l'aggiunta di una "Routing Rules" con FQDN e PATH che punti al Backend-Service.

Lo "Use Case" prevede l'utilizzo di:
 Host: asl02.polostrategiconazionale.it
 Path: /
 Backend: I7-ilb-backend-subnet-new

Routing rules

Routing rules determine how your traffic will be directed. You can direct traffic to a backend service or a kubernetes service. Any traffic not explicitly matched with a host and path matcher will be sent to the default service.

Mode

☒ Simple host and path rule

☐ Advanced host and path rule

Host and path rules

Host 1	Path 1	Backend 1 *
Host 2 *	Path 2 *	Backend 2 *
gcp-asl02.leonardo.com	/	I7-ilb-backend-subnet
Example: web.example.com	Example: /images/*	I7-ilb-backend-subnet-new

+ ADD HOST AND PATH RULE

- Fare Update per finalizzare la configurazione

Load Balancer name
l7-ilb-regional-uri-map

Region
europe-west8

Project
asl02-b-prod-net-tenant-0

Network
spoke

Proxy-only subnet: tenant-proxy-only 172.16.2.0/24

- Backend configuration
- Routing rules**
- Frontend configuration
- Review and finalize (optional)

Routing rules

Routing rules determine how your traffic will be directed. You can dire

Mode

☒ Simple host and path rule
☐ Advanced host and path rule

Host and path rules

Host 1

Host 2 *

gcp-asl02.leonardo.com

Example: web.example.com

+ ADD HOST AND PATH RULE

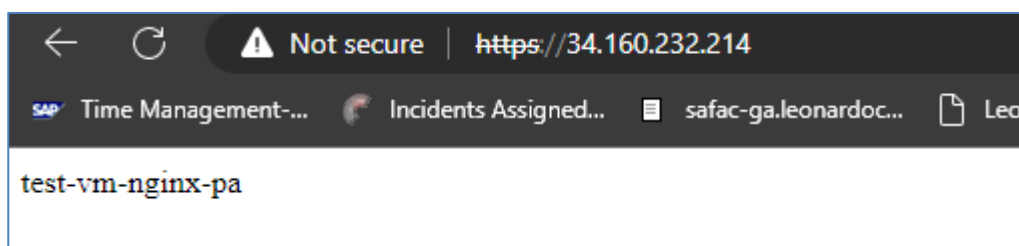
↓

UPDATE CANCEL EQUIVALENT CODE PREVIEW

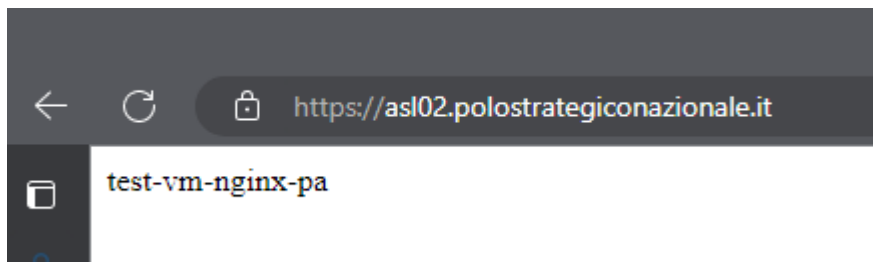
Now viewing project "as

7. Testare la configurazione del Load balancer.

Accedere a <http://34.160.232.214> e verificare che la pagina di risposta non è cambiata:

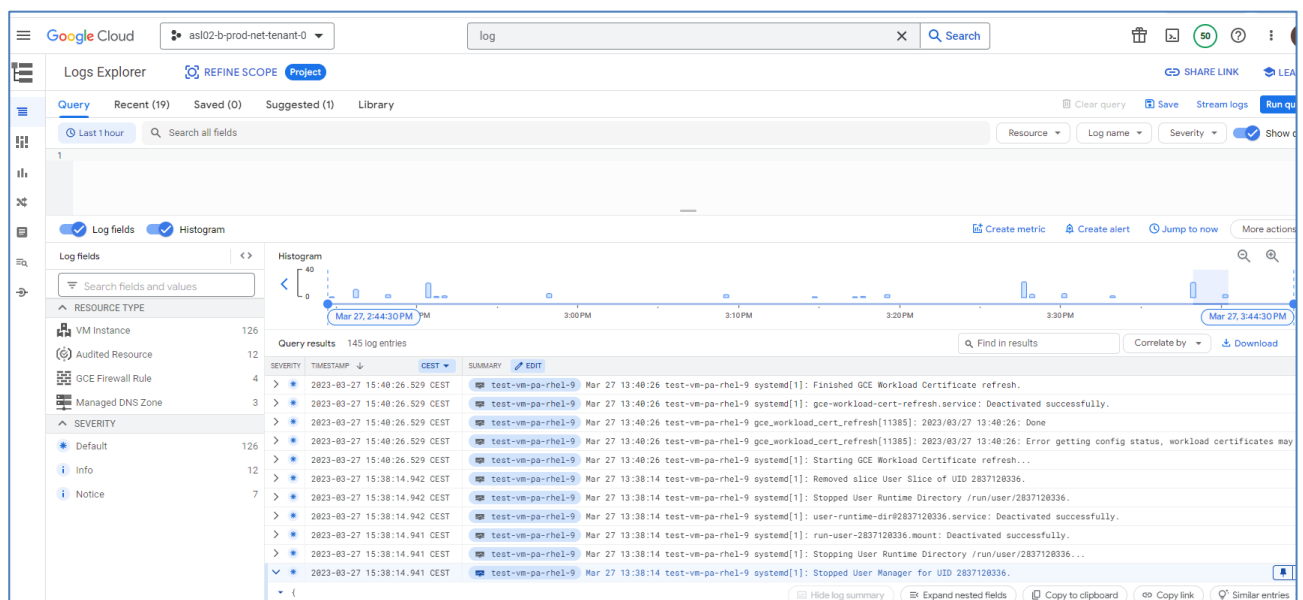


Accedere a <https://asl02.polostrategiconazionale.it> e verificare che si ottenga la pagina del nuovo web server:

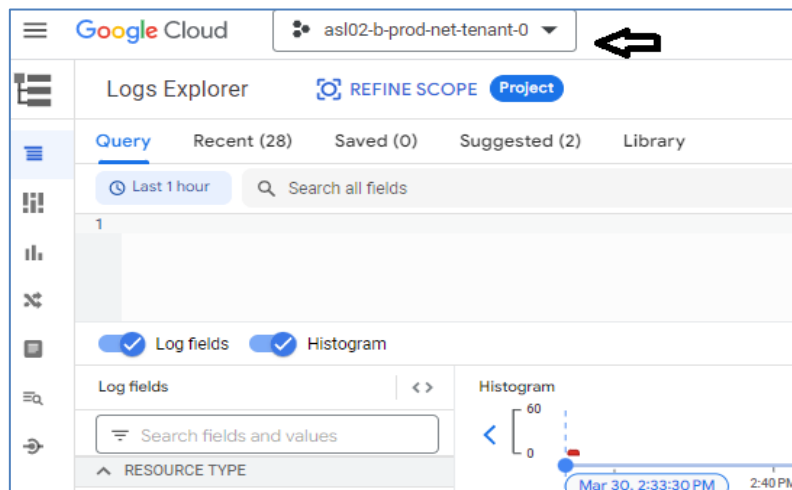


3.2.10 Consultazione dei logs

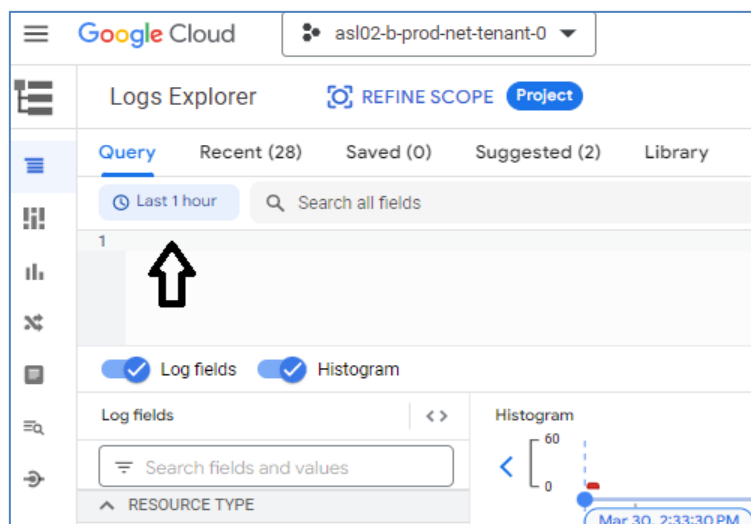
I logs generati dagli asset presenti nei project sono consultabili nella Google Console all'interno del servizio Logs Explorer.



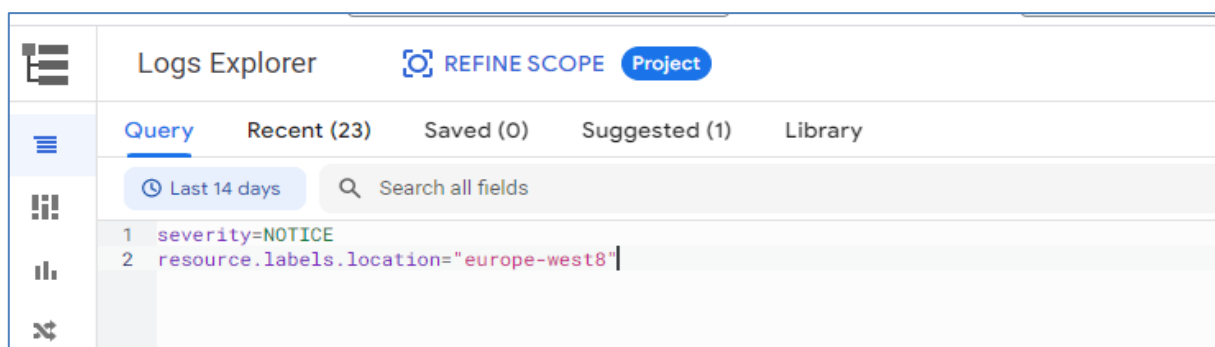
Una volta entrati nel menù Logs Explorer l'utente seleziona il project di suo interesse.



Per una consultazione più mirata l'utente può visionare i logs scegliendo una finestra temporale specifica selezionando il menù disponibile in alto a sinistra.



Inoltre ai log possono essere applicati ulteriori filtri per restringere il risultato su log più puntuali, ad esempio per visualizzare solo i log con severity NOTICE provenienti da una specifica Location "europe-west8", occorre impostare nel filtro quanto segue:



3.3 Backup PSN SCP

3.3.1 Introduzione al servizio di backup PSN SPC

Il Polo Strategico Nazionale prevede una infrastruttura di backup ibrida cloud – on-premises. È prevista una componente sul data center del PSN e una componente in Cloud in relazione alla sottoscrizione del cliente del Public Secure Cloud.

Il servizio di backup risponde a due distinti requisiti.

Il primo requisito è legato alla sovranità del dato, nel perimetro fisico del PSN deve essere disponibile e fruibile una copia dei workload erogati presenti sul Cloud Service Provider.

Per soddisfare il requisito della sovranità del dato, la replica del dato su storage del PSN ha frequenza mensile e ne viene mantenuta solo una versione. La replica avviene attraverso il circuito di rete protetto tra il Cloud Provider Pubblico e il data center del PSN.

Il secondo requisito che tale soluzione deve garantire è la protezione del dato. In questo scenario i dati per la restore sono salvati su storage del cloud provider. Il repository di backup in cloud è ottimizzato per garantire la migliore efficienza di archiviazione.

La piattaforma di backup è mantenuta dai managed services da parte del PSN.

La soluzione prevede la presenza di un portale per garantire al cliente accesso alle operazioni in modalità self-service per le operazioni di Backup/Restore delle risorse e dei dati in Cloud. Dallo stesso portale, il cliente può verificare lo stato delle repliche del dato a garanzia della sovranità.

I dati sottoposti a backup tramite la modalità backup sovrano, utilizzando la console tecnica del servizio BaaS, dovranno essere esclusivamente quelli di cui è già stato effettuato il backup sul CSP attraverso il servizio Secure Public Cloud.

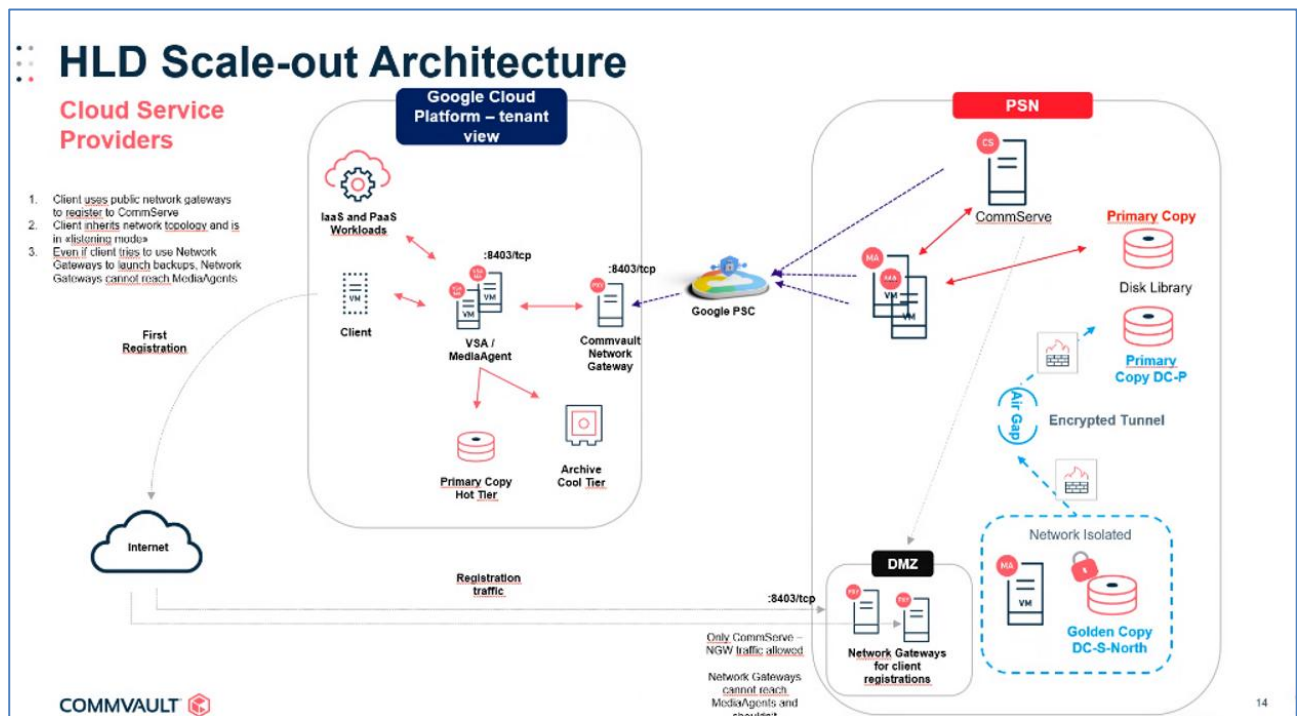


Figura 1: HLD Commvault

L'infrastruttura di backup Commvault è modulare e presenta diversi oggetti installati.

CommServe (CS)

È il server che gestisce tutte le componenti e le funzionalità. Comunica con i Media Agent e con i Network Gateway remoti. Gestisce la schedulazione dei backup e tutte le configurazioni. Attiva i servizi per la CommServe Console Java di amministrazione ma anche la Console Web per le attività operative che sono demandata alle PA in modalità Self-service. Per il collaudo è stato ipotizzato un ambiente con un singolo CS.

Media Agent (MA)

I server con ruolo di media Agent si occupano di gestire il flusso dei dati verso le disk library che proviene dagli access node, Network Gateway o altri Media Agent.

Access Node (AN)

Hanno il ruolo di comunicare con gli hypervisor. Nel caso di GCP utilizzando un Service Account possono inviare istruzioni per preparare i sistemi al backup. Come, ad esempio, creare snapshot dei dischi, mappare dischi al VSA o creare un VM in caso di restore.

Network Gateway (NG)

Mettono in comunicazione i MA in topologie più complesse come quella configurata per il PSN SPC dove abbiamo una distribuzione di servizi tra sistemi on-premises e cloud. Vengono anche installati due NG in DMZ con la funzione di “prima registrazione” di un VSA in cloud.

Dal punto di vista di infrastruttura network la comunicazione tra la parte on-premises e il GCP avviene sfruttando la tecnologia Private Service Connect.

Nel dettaglio, l'infrastruttura on-premises del PSN raggiunge la PSN ORG su GCP attraverso una VPN.

Da questa Organization vengono creati tanti flussi PSC quante sono le Org delle PA.

I flussi PSC sono interni al backend di GCP. Grazie al PSC il server CommServe può comunicare con il Network Gateway.

Nell'esempio, per comodità, i ruoli di NG, MA e AN sono eseguiti da una singola VM.

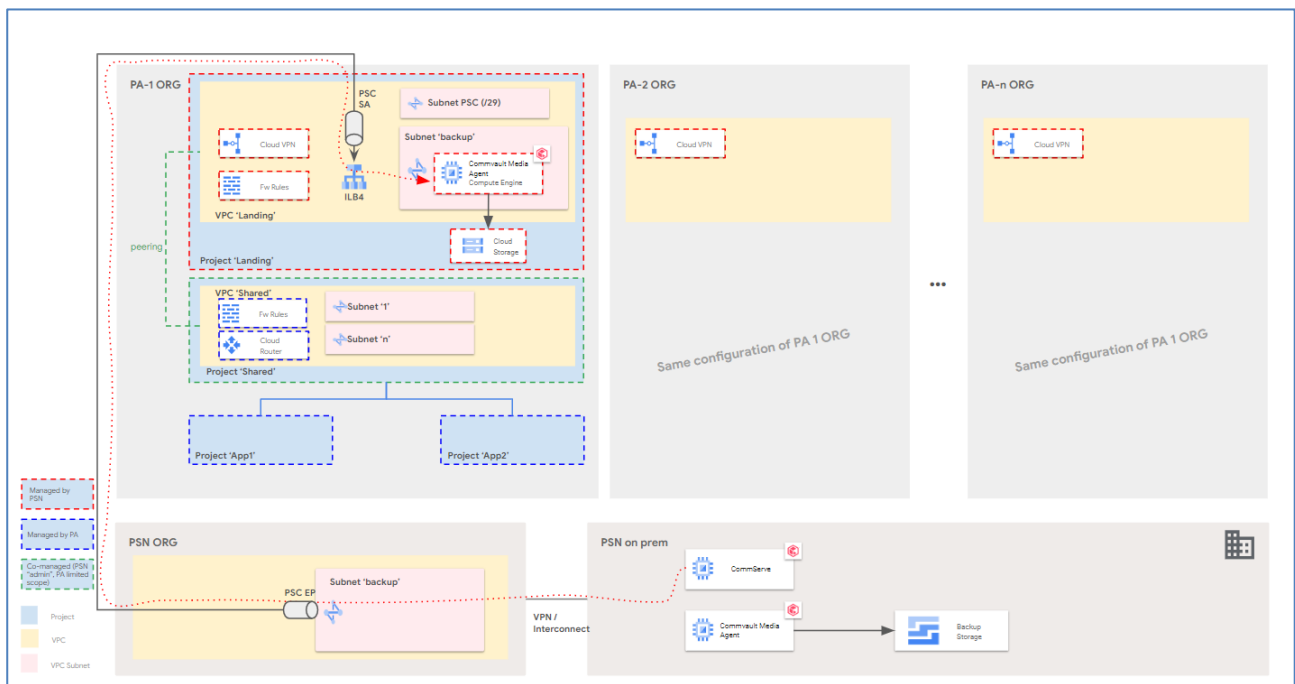


Figura 2: Dettaglio Flussi

Il flusso PSC è unidirezionale. Parte dal CommServe on-prem e arriva alla VSA su GCP.

Esiste solo una comunicazione inversa, ovvero dalla VSA verso il CommServe.

Si tratta del flusso attivo durante la fase di registrazione della VSA. In fase di onboarding viene installata la VSA sulla Org della PA. In questa fase la VSA deve contattare via TCP sulla porta 8403 il CommServe.

Una volta registrato questo link non verrà più utilizzato. La VSA andrà configurata in passive mode e il flusso dei dati transiterà solo attraverso il PSC.

Il server CommServe ha anche il ruolo di Commvault Web Console. Un portale web console dove le PA possono fare, in modalità self-service, tutte le operazioni necessarie come backup, restore.

3.3.2 Struttura del Portale: Dashboard

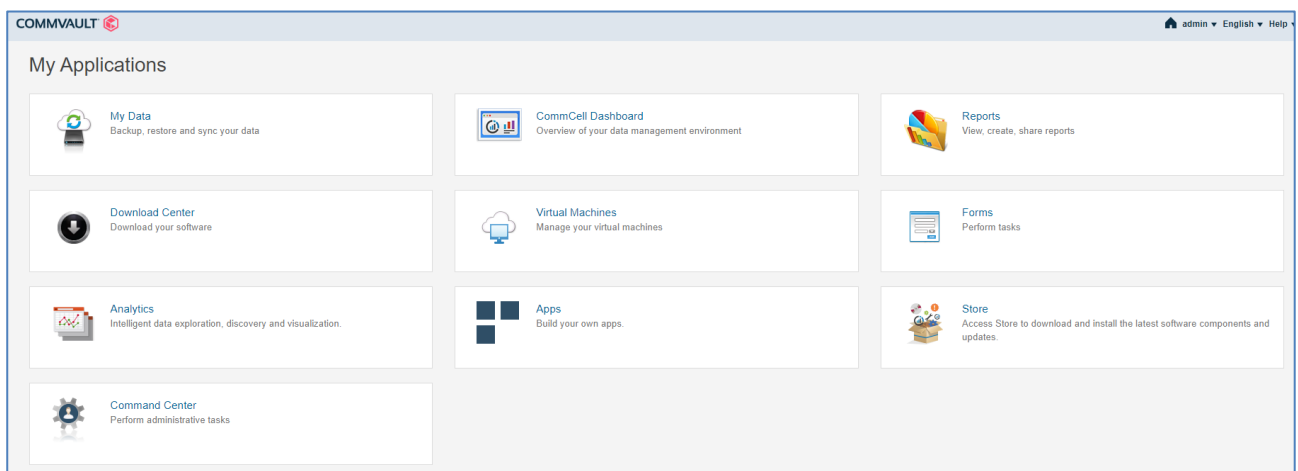
La PA si collega al portale di gestione del backup Commvault attraverso l'URL di accesso a disposizione delle PA.

<https://baas-nord.console.polostrategiconazionale.it>

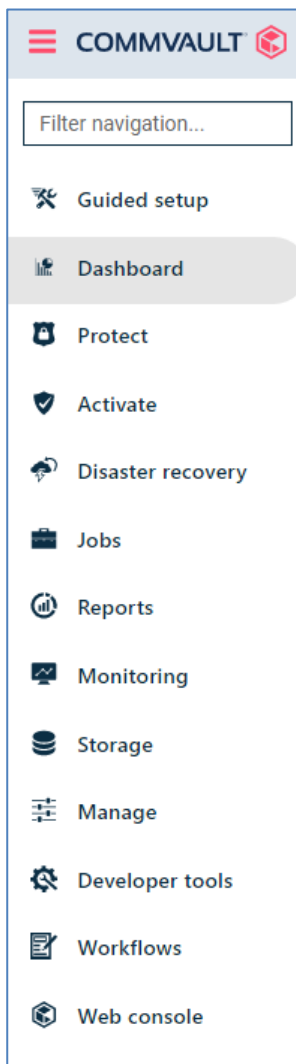


La login dovrà avvenire con l'utenza fornita alla PA al momento dell'attivazione del servizio.

La dashboard visualizzerà solo gli item di backup appartenenti alla stessa PA
Dopo la login vengono visualizzate tutte le applicazioni disponibili all'utente.



Per eseguire le configurazioni di base occorre entrare nella sezione "Command Center"
Il command Center è il portale da cui si eseguiranno tutte le configurazioni.
Di seguito il menu di navigazione



Ogni voce del menu attiva funzionalità o sottomenu aggiuntivi. Nei capitoli seguenti sono indicati i dettagli dei menu.

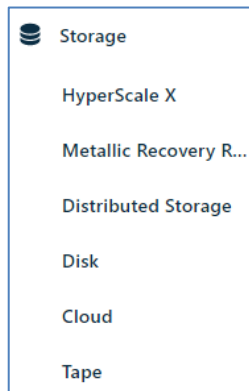
Per alcune risorse sono preconfigurati oggetti in fase di onboarding mentre su altre la PA avrà la possibilità di definirne di nuove.

3.3.3 *Storage*

La configurazione di backup viene preconfigurata con due storage utilizzabili come target dei backup.

Uno storage di tipo Disk e uno di tipo Cloud

Per visualizzarli occorre entrare nel menù storage come da immagine.



Lo storage di tipo Disk indica lo spazio disco On Premesis presso il datacenter PSN. Verrà poi utilizzato dai Plan che prevedono la replica del dato.

Disk Add Q ↺ ☰ ⋮					
All ⚙️					
Company = All + Add filter					
Name ↑ ⋮	Status	Capacity	Free space	Actions	
Disk Storage	Online	499.98 GB	413.46 GB	⋮	

Il disk storage è situato presso il DC di PSN e risiede su uno storage di backend.

Disk

Disk Storage

Overview
Configuration
Associated plans

General

Type	disk
Total capacity	499.98 GB
Free space	412.96 GB
Size on disk	25.61 GB
Deduplication savings	32.52%

Backup locations

All

+ Add filter

Name ↑
[srvpsneng008] E:\DiskStorage

Lo storage di tipo cloud è il Google Cloud Storage definito sulla Organization della PA all'interno del Project dedicato al backup

Cloud
Add

All

Company = All
+ Add filter

Name ↑	Status	Capacity	Free space	Actions
ASL02-GCS	Online	N/A	N/A	...

Il target GCS viene usato per i backup standard che non necessitano di replica On Premises.

ASL02-GCS

Overview Configuration Associated plans

General

Type	Cloud
Vendor type	Google Cloud Storage
Size on disk	181 MB
Deduplication savings	0%

Bucket

Add ↻ ☰ ⋮

All ⚙️

+ Add filter

Name ↑	Status	Actions
[asl02-b-prod-vsa] asl02-b-prodbackup-bucket	Ready	⋮

Sul GCS viene definito un bucket gestito dal VSA

Cloud / ASL02-GCS

[asl02-b-prod-vsa] asl02-b-prodbackup-bucket

General

Bucket [asl02-b-prodbackup-bucket](#)

Configuration

Enable ☒

Disable backup location for future backups ☐

Storage accelerator credentials

Click to select ▼ + ✎

Cloud access paths

Add mediaagent ↻ ☰ ⋮

All ⚙️

+ Add filter

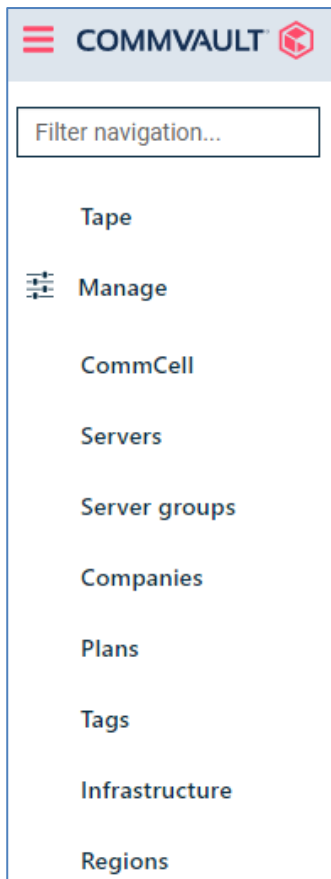
MediaAgent ↑	Bucket	User name	Access	Accessible	Actions
asl02-b-prod-vsa	asl02-b-prodbackup-bucki	storage.googleapis.com//	Read/Write	Yes	⋮

Il VSA utilizzerà le googleapis per accedere al bucket per memorizzare i backup.
Per la parte storage la PA non dovrà eseguire modifiche.

3.3.4 Plan

I Plan sono preconfigurati con due tipologie di default ma la PA può crearne di nuovi secondo le sue necessità.

Dal menu Manage => Plans sono visibili i plan configurati



Plans							Plan rules	Create plan ▾	Q	↺	⌵
All Server											
Company = All ▾ + Add filter											
Plan name ↑	Plan type	Associated e...	RPO	Number of c...	Status	Tags					
1d 30d	Server	1	1 day	2	Enabled	No tags					
1d 30d GoldenCopy	Server	0	1 day	3	Enabled	No tags					

Vengono preconfigurati due Plan.

Il primo plan “1d 30d” è configurato con la backup destination sullo storage Cloud GCS con retention di 30 giorni.

Il RPO è impostato a 24 ore attraverso un backup giornaliero alle 21.00

1d 30d

Overview

Associated entities

Companies

Backup destinations

Multi-region ☐

ADD

Name	Storage	Retention period	Source	Actions
snap copy Snapshot primary	ASL02-GCS CLOUD	1 month		
Primary Primary	ASL02-GCS CLOUD	1 month		

RPO

Backup frequency

Run incremental every 1 day(s) at 9:00 PM

Backup window

Full backup window

SLA

Il secondo Plan “1d 30d Sovereignty” viene usato per avere repliche sul DC On Premises.

Sono configurati due storage di destinazione, la copia primaria viene salvata sul GCS con la retention di 30 giorni. La secondaria invece viene replicata sul datacenter PSN con policy “Half Yearly Fulls” e retention di 1 anno.

Quindi verrà eseguito un backup ogni sei mesi con retention di un anno, ovvero sempre 2 versioni per mantenere la richiesta di sovranità del dato.

Plans

1d 30d Sovereignty

Overview

Associated entities

Companies

Backup destinations

Multi-region ☐

ADD

Name	Storage	Retention period	Source	Actions
snap copy Snapshot primary	ASL02-GCS CLOUD	1 month		
Primary Primary	ASL02-GCS CLOUD	1 month		
Sovereignty Half Yearly Fulls	Disk Storage DSK	1 year	Primary	

RPO

Backup frequency

Run incremental every 1 day(s) at 9:00 PM

Run full every 1 week(s) at 9:00 PM

On every Sunday

Backup window

Monday through Sunday : All day

Full backup window

Monday through Sunday : All day

SLA

1 week, inherited from CommCell

Secondary copy schedule

Automatic schedule

Inoltre per garantire alla PA una schedulazione alternativa, la PA stessa potrà creare nuovi Plan dal menu Manage/Plan seguendo il wizard indicato dalla figura

Plans

Create Server Backup Plan

1 General

2 Backup Destinations

3 RPO

4 Options

General

☒ **Create a new plan**
New backup plan from scratch

☐ **Use existing base plan**
Create plan by inheriting setting from base plan

Plan name *

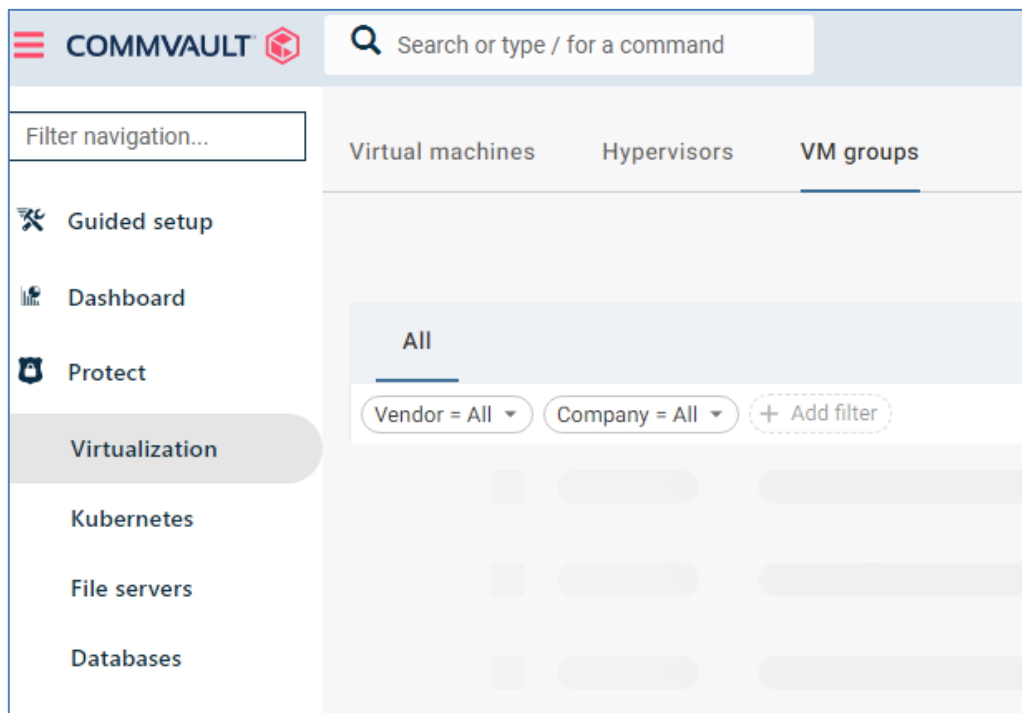
CANCEL NEXT

I campi da compilare sono: nome, destinazione e RPO.

3.3.5 VM Groups

I VM Groups sono in gestione della PA. I VM Groups associamo le entità dell'hypervisor GCP (quindi le VM) a un Plan.

Dal menu Protect/Virtualization/VM Groups



Selezionare add VM Groups e inserire nel Wizards l'hypervisor GCP, il Plan e le VM

Add VM Group

1 Select Hypervisor

2 Plan

3 Add VM Group

Select Hypervisor

Hypervisor *
ASL02-GCP

CANCEL

NEXT

Add VM Group

✓ Select Hypervisor

2 Plan

3 Add VM Group

Select Plan

Search plans by plan name
+ ↺

1d 30d

RPO	1 day	Primary storage type	Cloud
Copies	2	Entities	0

1d 30d GoldenCopy

RPO	1 day	Primary storage type	Cloud
Copies	3	Entities	0

Add VM Group

- Select Hypervisor
- Plan
- 3 Add VM Group**

Add VM Group

Name *

Vm Groups PA

Content Delete Add Q

Type ↑	Rule	Actions
No content	Content	yet

Snap configuration

IntelliSnap ☐

EQUIVALENT API

PREVIEW

CANCEL
PREVIOUS
SUBMIT

Le VM possono essere inserite in modalità statica selezionandole dai Project, oppure utilizzando Rules dinamiche.

Particolarmente consigliate sono le Rules basate su la Label associate alla VM GCP.

Add rule

Match rule ☒ all ☐ any

Label ▼

Key

Equals ▼ 30gg

Value

Equals ▼ backup

ADD

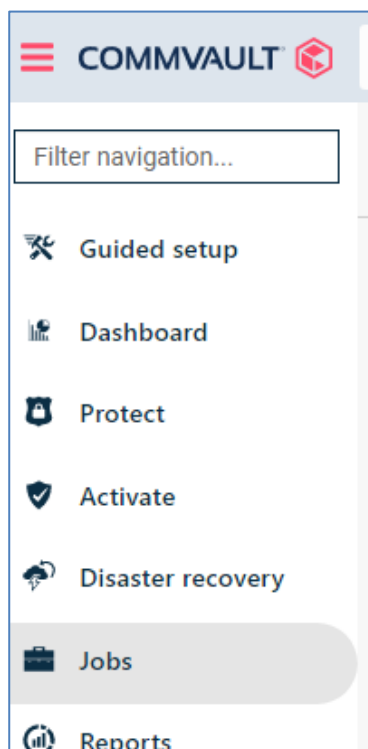
CANCEL SAVE

In questo esempio vengono selezionate dal VM Groups tutte le VM con Label 30gg

Basic information	
Name	test-vm-pa-rhel-9
Instance Id	1140380018551297872
Description	Managed by the compute-vm Terraform module.
Type	Instance
Status	Running
Creation time	Mar 21, 2023, 1:57:36 PM UTC+01:00
Zone	europa-west8-b
Instance template	None
In use by	None
Reservations	Automatically choose (default)
Labels	backup : 30gg
Tags	—
Deletion protection	Disabled
Confidential VM service	Disabled
Preserved state size	0 GB

3.3.6 Jobs

I JOB in esecuzione o quelli terminati possono essere monitorati nella loro esecuzione sotto il menu JOBS:



I JOB possono essere analizzati nel dettaglio selezionando con il mouse il numero di job

COMMVAULT								
Search or type / for a command								
Filter navigation...	Active Jobs Job history							
Guided setup	Job history View Last 24 hours							
Dashboard	Search Show admin jobs							
Protect	Job id	Operation	Server	Agent type	Subclient	Size	End	Elapsed
Activate	166	Snap Backup	test-vm-nginx-pa	Virtual Server	default	10 GB	Mar 24, 2023 2:40:45 PM	2 min 16 sec
Disaster recovery	165	VM Admin Job(Snap Backup)	ASL02-GCP	Virtual Server	asl02 1h 7d GoldenCopy	10 GB	Mar 24, 2023 2:40:45 PM	14 min 47 sec
Jobs	163	VM Admin Job(Snap Backup)	ASL02-GCP	Virtual Server	asl02 1h 7d GoldenCopy	10 GB	Mar 24, 2023 2:24:30 PM	14 min 28 sec
Reports	164	Snap Backup	test-vm-nginx-pa	Virtual Server	default	10 GB	Mar 24, 2023 2:24:29 PM	1 min 54 sec
	162	Snap Backup	test-vm-nginx-pa	Virtual Server	default	10 GB	Mar 24, 2023 2:09:27 PM	1 min 58 sec
	161	VM Admin Job(Snap Backup)	ASL02-GCP	Virtual Server	asl02 1h 7d GoldenCopy	10 GB	Mar 24, 2023 2:09:27 PM	14 min 29 sec

3.3.7 Manual Backup

I backup sono schedulati secondo la RPO del Plan. Per eseguire backup manuali occorre andare nel menu Protect/Virtualization/Virtual Machine.

COMMVAULT								
Search or type / for a command								
Filter navigation...	Virtual machines Hypervisors VM groups Add hypervisor Add VM group							
Guided setup	All							
Dashboard	Vendor = All VM status = All Company = All Add filter							
Protect	Name	Hypervis...	VM group	VM status	Last bac...	Applicati...	Plan	SLA stat...
Virtualization	asl0...	Not Appl...	Not Appl...	Not con...	Never ba...	0 B	Not assi...	Excluded
Kubernetes	test...	ASL02-G...	asl02 1d...	Protected	23 mar, ...	10 GB	Not assi...	Met
File servers								

Selezionare la VM ed eseguire il backup.

All								
Vendor = All VM status = All Company = All Add filter								
Name	Hypervis...	VM group	VM status	Last bac...	Applicati...	Plan	SLA stat...	Tags
asl0...	Not Appl...	Not Appl...	Not con...	Never ba...	0 B	Not assi...	Excluded	Restore
test...	ASL02-G...	asl02 1d...	Protected	23 mar, ...	10 GB	Not assi...	Met	Back up
test...	ASL02-G...	asl02 1h...	Protected	24 mar, ...	10 GB	1h 7d Go...	Met	Manage plan
test...	ASL02-G...	asl02 1d...	Protected	23 mar, ...	80 GB	Not assi...	Met	View jobs
test...	ASL02-G...	asl02 1d...	Protected	23 mar, ...	50 GB	Not assi...	Met	Do not back up

Seguire l'esecuzione del backup dal menu JOB.

Restore options

Type ☒ In place ☐ Out of place

Access node Automatic

test-cvm-pa Instance display name test-cvm-pa

☐ Power on VMs after restore

☐ Unconditionally overwrite if it already exists

☐ When the job completes, notify me via email

Equivalent API Cancel Submit

Restore options

Type ☐ In place ☒ Out of place

Destination ASL02-GCP

Access node Automatic

test-cvm-pa Instance display name test-cvm-pa

Zone asl02-b-prod-net-tenant-0\europa-west8-b Browse

Machine type n2d-standard-2 (2 core(s) 8192 MB 128 disks)

Network settings >

Sole-tenant nodes >

Custom metadata ⓘ >

☐ Power on VMs after restore

☐ Unconditionally overwrite if it already exists

3.3.9 Restore Confidential VM con CMEK

Per la restore delle VM in modalità confidential VMs con chiave CMEK occorre seguire una particolare procedura.

Le VM create in modalità confidential con chiave CMEK hanno il disco criptato con chiave customer esterna come indicato nelle proprietà del disco.

Encryption	
Type	Customer-managed
Key ID	projects/asl02-b-prj-sec-shared/locations/europe-west8/keyRings/asl02-keyring/cryptoKeys/asl02-01-key01/cryptoKeyVersions/1
Key name	asl02-01-key01

La chiave è quella depositata all'interno del keyring sul progetto shared e in sync con l'infrastruttura Thales on premises.

Dopo il processo di restore con Commvault la CVM ripristinata avrà una chiave differente da quella Thales come indicato in precedenza.

Questo avviene per un bug del prodotto Commvault relativo alle restore di VMs con chiave esterna CMEK su progetti separati rispetto tra VMs a Keyring.

Il vendor ha garantito un bug fix nella prossima release.

✓ test-cvm-pa	
DETAILS	MONITORING
Properties	
Type	Balanced persistent disk
Size ?	10 GB
Architecture	—
Zone	europe-west8-b
Labels	None
In use by	test-cvm-pa
Snapshot schedule	None
Source snapshot	gx-restore-1045-6798006279973738935-1679304566
Encryption	
Type	Customer-managed
Key ID	projects/asl02-b-prod-net-tenant-0/locations/europe-west8/keyRings/asl02-keyring/cryptoKeys/asl02-01-key01/cryptoKeyVersions/1
Key name	asl02-01-key01

Come si vede dall'immagine la VM ripristinata ha una chiave differente, in particolare si vede come venga creato un nuovo keyring sul progetto della VM.

Per risolvere il bug, e utilizzare nuovamente la key di Thales sulla VM ripristinata, è stato implementato il seguente workaround.

Come primo step occorre individuare il disco con la chiave CMEK non corretta ed eseguirne lo snapshot in modalità regional. La snapshot così creata è protetta dalla stessa chiave del disco ripristinato.

← Create a snapshot

Snapshots are backups of persistent disks. They're commonly used to recover, transfer, or make data accessible to other resources in your project. [Learn more](#)

Name *

test-cvm-pa-snapshots

Name is permanent

Description

Source disk *

test-cvm-pa-restore

Type

☒ Snapshot

Best for long-term backup and disaster recovery

☐ Archive snapshot

Best for cost-efficient data retention

Location ?

There may be a network transfer fee if you choose to store this snapshot in a location different than the source disk. [Learn more](#)

☐ Multi-regional

☒ Regional

Select location

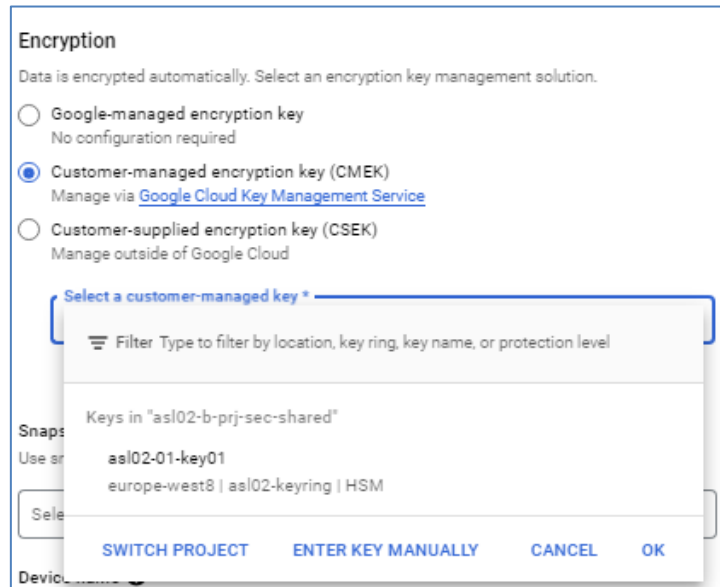
europa-west8 (Milan)

Utilizzare lo snapshot per creare una nuova istanza VM utilizzando la chiave di cifratura CMEK.

Manuale Utente Secure Public Cloud su Cloud Provider
Google
Ed. 1 - ver. 1.1

65

Data: 07/06/2023



La chiave sarà quella del keyring del progetto prj-sec-shared.
La VM creata avrà ora la key corretta di Thales così come era la VM originale.

DETAILS

MONITORING

Properties

Type	Balanced persistent disk
Size ?	10 GB
Architecture	—
Zone	europe-west8-a
Labels	None
In use by	instance-1
Snapshot schedule	None
Source snapshot	test-cvm-pa-snapshots

Encryption

Type	Customer-managed
Key ID	projects/asl02-b-prj-sec-shared/locations/europe-west8/keyRings/asl02-keyring/cryptoKeys/asl02-01-key01/cryptoKeyVersions/1
Key name	asl02-01-key01

3.3.10 Manuali Commvault

Per tutte le procedure operative di backup, restore e configurazione non indicate in questo manuale fare riferimento alla documentazione ufficiale Commvault:

[Backups for Google Cloud Platform](#)

[Restores for Google Cloud Platform](#)

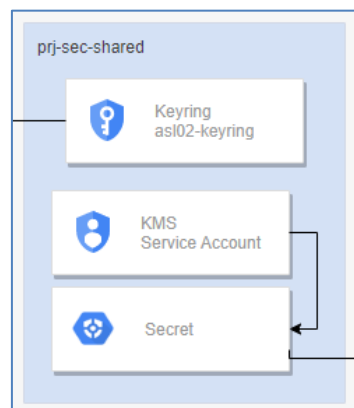
[Adding a VM Group for Google Cloud Platform](#)

3.4 KMS

La gestione delle chiavi prevede una modalità definita come BYOK. Le chiavi di cifratura vengono create e gestite dall'infrastruttura Thales presente on-premises nei datacenter del PSN, escludendo così, dalla gestione delle chiavi di cifratura, il CSP.

Nell'alberatura della Organization della PA sono presenti vari progetti out-of-the-box, che costituiscono la foundation della Organization.

Fra questi c'è un progetto: prj-sec-shared, che è riservato alla gestione delle chiavi.



All'interno del progetto è configurato il Keyring che ospita le chiavi generate dalla piattaforma Thales. Su richiesta della PA gli operatori del PSN creano sulla piattaforma Thales on prem la nuova chiave richiesta dal cliente. Una volta generata la chiave questa viene poi copiata nel Keyring e messa a disposizione dell'ambiente Secure Public Cloud.

Chiavi per il keyring "KeyRing-EU8"

Una chiave di crittografia è una risorsa che viene utilizzata per criptare e decryptare i dati o per generare e verificare le firme digitali. Per eseguire operazioni sui dati con una chiave, utilizza l'API Cloud KMS. [Ulteriori informazioni](#)

Filtro Inserisci il nome o il valore della proprietà

☐	Nome ↑	Stato ?	Livello di protezione ?
☐	keyhsmbackup01	✓ Disponibile	HSM
☐	keytest3	✗ Non disponibile	Software
☐	keytestbackup01	Non applicabile	HSM
☐	MWtest01	Non applicabile	HSM
☐	MWTest02	✗ Non disponibile	HSM

In fase di onboarding del servizio, sono preconfigurate delle chiavi di crittografia, generate sugli apparati KMS/HSM del PSN e sincronizzate sui device HSM in cloud. Completata la fase di rilascio il cliente ha a disposizione le chiavi nel suo HSM di riferimento.

Nello specifico sono create chiavi per le principali tipologie di risorse da poter utilizzabili per la cifratura del layer applicativo (produzione, sviluppo e test), esempio:

- Standard VM;
- Confidential VM;
- servizi PaaS SQL;

È comunque possibile per la PA richiedere, tramite il servizio di ticketing dedicato del PSN, chiavi aggiuntive per specifici workload applicativi, indicando le caratteristiche della chiave da generare (nome, algoritmo di encryption, size, durata), nonché la destinazione d'uso.

Il servizio base non prevede impostazioni di rotazione chiavi by design, ma deve essere espressamente richiesto dalla PA, con contestuale specifica dell'intervallo di rotazione ed il perimetro di chiavi impattato.

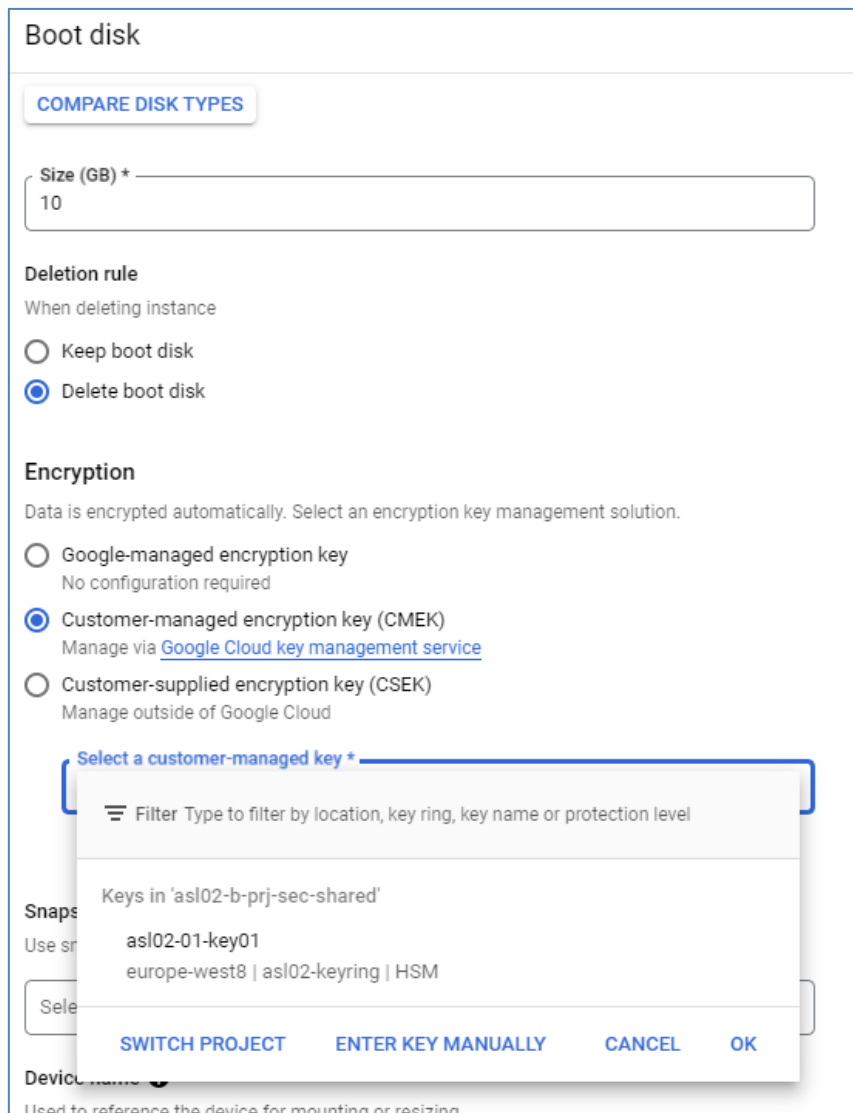
La PA rimane responsabile del corretto utilizzo delle chiavi di crittografia messe a disposizione dal PSN, in particolare si definisce il seguente dettaglio:

- Impiego delle chiavi specifiche a seconda della tipologia di workload applicativo e della classificazione del dato trattato (ordinario e critico);
- Richiedere la disabilitazione o revoca di una chiave, accertandosi preventivamente che non sia ancora applicata alle proprie risorse;
- In contesti di rotazione chiavi, esecuzione degli interventi tecnici necessari volti ad applicare le nuove release delle chiavi per l'encryption delle proprie risorse.

Il project che contiene il keyring è visibile da tutta la Organization della PA, mettendo a disposizione le chiavi per i differenti workload.

3.4.1 Utilizzo Chiave esterna per una Virtual Machine

La figura seguente mostra un esempio di utilizzo di una chiave, denominata “asl02-01-key01”, presente nel keyring “asl02-keyring”, nel project “asl02-b-prj-sec-shared”.



Boot disk

[COMPARE DISK TYPES](#)

Size (GB) *
10

Deletion rule
When deleting instance

☐ Keep boot disk
☒ Delete boot disk

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

☐ Google-managed encryption key
No configuration required

☒ Customer-managed encryption key (CMEK)
Manage via [Google Cloud key management service](#)

☐ Customer-supplied encryption key (CSEK)
Manage outside of Google Cloud

Select a customer-managed key *

Filter Type to filter by location, key ring, key name or protection level

Keys in 'asl02-b-prj-sec-shared'

asl02-01-key01
europe-west8 | asl02-keyring | HSM

[SWITCH PROJECT](#) [ENTER KEY MANUALLY](#) [CANCEL](#) [OK](#)

Tale chiave è utilizzata, nel caso specifico dell'esempio, per criptare il disco di boot di una Confidential Virtual Machine.

Tutte le attività sulle chiavi rotazione, devono essere effettuate sull'infrastruttura del PSN di gestione chiavi, cioè sulla piattaforma Thales, non è possibile operare rotazioni o cancellazioni di chiavi direttamente dalla console GCP.

3.4.2 Rotazione chiave

Come già detto in precedenza, tutte le operazioni sulle chiavi sono effettuate tramite l'infrastruttura Thales ospitata nei datacenter del PSN e gestita da personale PSN.

Durante la fase di generazione della nuova chiave destinata alla rotazione, il personale PSN, crea la nuova key utilizzando il Cipher Trust Manager di Thales sincronizzando quest'ultima nel Keyring in cloud.

☐	↓ Versione	Stato ?	Algoritmo ?
☐	2	Abilitata e primaria	Chiave Simmetrica Google
☐	1	Abilitata	Chiave Simmetrica Google

La vecchia chiave continua ad esser valida e a poter essere utilizzata fino a quando non viene disabilitata, per questo motivo una Virtual Machine criptata con la vecchia versione continua a funzionare regolarmente. Per completare il ciclo di rotazione con la disabilitazione della chiave da dismettere, su tutte le VM deve essere obbligatoriamente sostituita la chiave stessa, così da poter procedere alla disabilitazione della chiave senza generare disservizi.

Quando una chiave viene disabilitata lato Thales, lo stato della chiave si riflette anche sulla sua copia nel Keyring:

☐	↓ Versione	Stato ?	Algoritmo ?
☐	2	Disabilitata e primaria	Chiave Simme
☐	1	Disabilitata	Chiave Simme

Nessuna versione selezionata

Non sarà possibile abilitare/disabilitare delle chiavi dal KeyRing Google.

Nel caso venga disabilitata una chiave, lato Thales, utilizzata da una VM, la VM non sarà più accessibile.

3.4.3 Cancellazione chiave

Se una chiave viene cancellata lato Thales, dopo 24 ore, la chiave sarà rimossa e, sul KeyRing di GCP, la chiave diventa "non disponibile".

☐	MWTest02	✖ Non disponibile	HSM
☐	MWTest03	✖ Non disponibile	HSM

Lo status diventerà "cancellata" e la sarà mostrata la data di cancellazione.

Filtro Inserisci il nome o il valore della proprietà			
☐	↓ Versione	Stato ?	Al
☐	1	Eliminata il giorno 16/02/23, 14:38	Ch

Nota: Se la chiave è associata ad una VM, la VM non sarà più accessibile dopo il riavvio.

3.4.4 Utilizzo nuova Chiave

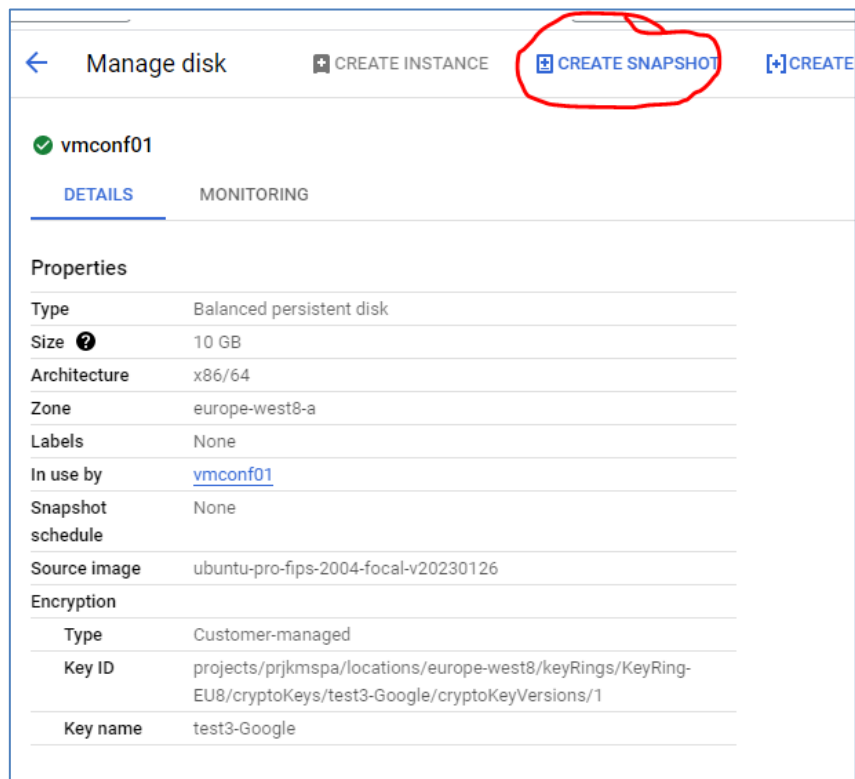
Per utilizzare la versione nuova di una chiave, o una chiave differente su una Virtual Machine, sia essa Confidential o no, è necessaria una procedura manuale di rotazione.

La procedura è identica alla procedura descritta nel 3.3.9 Restore Confidential VM con CMEK.

I passi consistono nel:

- effettuare uno snapshot del disco
- creare un nuovo disco dallo snapshot
- associare il disco alla nuova versione della chiave
- creare una nuova VM che utilizza il disco nuovo

Nell'esempio in figura:



La VM utilizza la chiave:

projects/prjkm spa/locations/europe-west8/keyRings/KeyRing-EU8/cryptoKeys/test3-Google/cryptoKeyVersions/1

[←](#) **Create a snapshot**

Snapshots are backups of persistent disks. They're commonly used to recover, transfer or make data accessible to other resources in your project. [Learn more](#)

Name *
snapshot4newkey
Name is permanent

Description

Source disk *
vmconf01

Type
☒ **Snapshot**
Best for long-term backup and disaster recovery
☐ **Archive snapshot**
Best for cost-efficient data retention

Location ?
There may be a network transfer fee if you choose to store this snapshot in a location other than the source disk. [Learn more](#)
☐ Multi-regional
☒ **Regional**
Select location
europe-west8 (Milan)

Labels ?
[+ ADD LABEL](#)

Lo snapshot, come indicato anche dalla Console sarà comunque criptato ancora con la stessa chiave.

Labels ?
[+ ADD LABEL](#)

Encryption

i This snapshot will use the same encryption type as the disk. [Learn more](#)

Encryption

Type	Customer-managed
Key ID	projects/prjkmspa/locations/europe-west8/keyRings/KeyRing-EU8/cryptoKeys/test3-Google/cryptoKeyVersions/1
Key name	test3-Google

Application consistency

An application-consistent snapshot is taken while a disk is in use, so there's no need to shut down the VM or take the disk offline. With application consistency, pending writes are completed (using guest flush or VSS) before the snapshot is taken. [Learn more](#)

Questo snapshot può essere utilizzato per creare una Virtual Machine.
A questo punto si può creare una nuova Virtual machine, anche Confidential, che utilizza come sorgente per un disco, lo snapshot generato in precedenza.
La particolarità è che in questa modalità, si può indicare la chiave con cui criptare il disco generato da questo snapshot:

Boot disk

Select an image or snapshot to create a boot disk, or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

PUBLIC IMAGES

CUSTOM IMAGES

SNAPSHOTS

ARCHIVE SNAPSHOTS

Snapshot

snapshot4newkey

x86_64, Created on 27 Mar 2023, 21:19:03, vmconf01

Boot disk type *

Balanced persistent disk

COMPARE DISK TYPES

Size (GB) *

10

Deletion rule

When deleting instance

☐ Keep boot disk

☒ Delete boot disk

Encryption

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

☐ Google-managed encryption key

No configuration required

☒ Customer-managed encryption key (CMEK)

Manage via [Google Cloud key management service](#)

☐ Customer-supplied encryption key (CSEK)

Manage outside of Google Cloud

Select a customer-managed key *

MWTest07

Don't see your key? Check permissions. [Learn more](#)

Il risultato è una nuova Confidential Machine, identica alla precedente, ma criptata con una nuova versione della chiave o, come nel caso dell'esempio, con una nuova chiave.

4 Guida alla fatturazione

I servizi Public Cloud PSN managed e Secure Public Cloud verranno fatturati secondo i termini previsti in convenzione a livello di “Famiglia di servizio” che è il risultato del campo “Macrotipologia” e “Tipo 1” del listino ufficiale pubblicato sul sito istituzionale di Polo Strategico Nazionale nell’area [“Tutti i documenti per aderire a Polo Strategico Nazionale”](#).

Le risorse attivate dal cliente tramite la console CSP verranno contabilizzate secondo il modello a consumo, sulla base dell’effettivo utilizzo.

Per l’attivazione di risorse riservate o committate per 1 anno o 3 anni, in caso di recesso anticipato dal contratto o alla scadenza del contratto di utenza, al cliente verrà addebitata una fattura di consuntivo relativa agli importi non usufruiti per il periodo residuo di reservation/commitment.