Polo Strategico Nazionale

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 AWS

Data: 21/05/2025

PSN_Manuale Utente SPC AWS

Ed. 1 - ver. 2.1

Polo Strategico Nazionale

QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
Manuale Utente Secure Public Cloud su Cloud Provider AWS			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	23/10/2024	Prima versione
2	2.0	04/04/2025	Seconda versione
3	2.1	21/05/2025	Aggiornato capitolo “Guida alla fatturazione”

NUMERO TOTALE PAGINE:	83

AUTORE:	
Team di lavoro PSN	Unità operativa Technology & Information

REVISIONE:	
Referente del Servizio	Paolo Trevisan

APPROVAZIONE:	
Direttore del Servizio	Antonio Garelli

INDICE

LISTA DELLE FIGURE

LISTA DELLE TABELLE

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
HTTP	HyperText Transfer Protocol

Acronimo	Descrizione
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
SOC	Security Operation Center

Acronimo	Descrizione
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
VPC	Virtual Private Cloud
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 AWS.

2.2 Premessa all'utilizzo della console tecnica

Con riferimento all'utilizzo della consolle 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 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 AWS generiche

3.1.1 *Organizaton Unit*

Ogni Organization AWS corrispondente ad un cliente Pubblica Amministrazione deve essere configurata con la predisposizione dei seguenti Account contenuti in diverse Organization Unit.

- Unità Organizzativa "Root":
  - È l'unità organizzativa di livello superiore nella gerarchia di un'organizzazione AWS e contiene tutte le altre unità organizzative;
- Unità Organizzativa "Share":
  - È concepita per ospitare account che gestiscono risorse e servizi condivisi tra diversi reparti o team all'interno dell'organizzazione; questo approccio centralizza servizi comuni come: directory, strumenti di gestione delle identità o archivi dati, rendendoli accessibili a più unità senza la necessità di duplicazione. La centralizzazione delle risorse non solo migliora l'efficienza operativa, ma riduce anche i costi associati alla gestione di servizi duplicati. Inoltre, facilita la standardizzazione e il controllo delle risorse condivise, garantendo che tutti i reparti aderiscano alle stesse politiche di sicurezza e conformità.
  - È presente l'HUB centrale dell'intero tenant PA: è l'account centrale dove vengono sviluppati tutti i servizi utili alla landing zone.
- Unità Organizzativa "Security":
  - È dedicata agli account che gestiscono funzioni di sicurezza e conformità all'interno dell'organizzazione; questo può includere account che eseguono il monitoraggio della sicurezza, la gestione dei log di sicurezza e la risposta agli incidenti. Centralizzando queste funzioni, la Security OU assicura che le pratiche di sicurezza siano applicate in modo uniforme in tutta l'organizzazione. Inoltre, la gestione centralizzata delle funzioni di sicurezza facilita l'implementazione e il monitoraggio delle policy di sicurezza, migliorando la capacità dell'organizzazione di rispondere rapidamente a minacce e incidenti di sicurezza.
    Sono presenti due account diversi:
    - Audit Account: dedicato alla raccolta e archiviazione centralizzata di tutti i log di attività e sicurezza provenienti dagli account dell'organizzazione; questo approccio garantisce che i dati dei log siano conservati in modo sicuro e immutabile, facilitando il monitoraggio e l'analisi per la conformità e la sicurezza;
    - Log Archive Account: progettato per eseguire attività di monitoraggio e verifica della conformità all'interno dell'organizzazione AWS; questo

account ha accesso in sola lettura ai log e alle configurazioni delle risorse, permettendo agli auditor di esaminare le attività senza rischiare di alterare i dati o le configurazioni esistenti.

- Unità Organizzativa "Spoke":
  - È dedicata agli Spoke ed è utilizzata per gestire e isolare account che supportano carichi di lavoro specifici o progetti individuali all'interno di un'organizzazione; questi account sono configurati per ospitare applicazioni, servizi o ambienti di sviluppo e produzione distinti, separati dalle risorse comuni e dalle funzionalità di sicurezza centralizzate.

L'organization della PA avrà al suo interno, oltre le utenze nominali assegnate ai referenti, anche le utenze di emergenza da utilizzare nei casi di necessità ad opera del PSN.

3.1.2 Utenze di emergenza

All'interno del tenant della PA sono definite due utenze di emergenza. Occorre conservare la password di entrambe le utenze 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 al tenant PA.

3.1.3 Utenze PA

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

- potranno creare utenze cloud native nel tenant AWS dedicata alla PA;
- potranno aggiungere tali utenze ai gruppi predefiniti (pre-configurati dal PSN) distribuendo così i permessi per l'ambiente console.

Tutte le utenze della PA avranno accesso alla console AWS.

3.1.4 User Group

Il PSN configura nel tenant 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 ruoli con descrizione delle responsabilità, assegnazione e scope di applicazione.

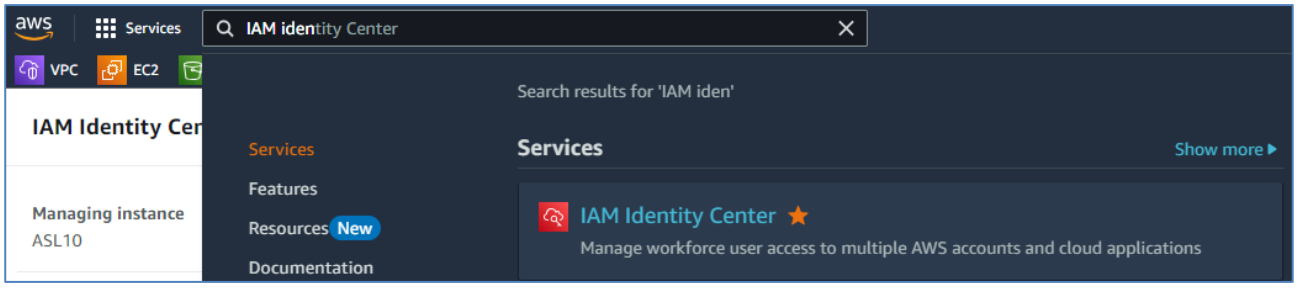
Appartenenza	Nome Gruppo	Descrizione Gruppo
PA	PA-Administrator	Creazione utenze cloud (IAM Identity Center) Assegnazione utenze in specifici gruppi
PA	NetworkGroup	Esposizione Servizi Esposizione WAF Policy Firewall Lettura LOG Firewall
PA	SystemGroup	Creazione risorse in SPOKE Account Lettura di ARN KMS su HUB Account
LDO	PSN-Administrator	Tutto su tutti gli account
PA	SOC-RTSM	Gestione degli allarmi (Audit Account, Security Hub, Cloudwatch)
PA	SOC-SDM	Gestione amministrativa Accesso AWS Config Gestisce WAF Gestisce FIREWALL

Tabella 3: Gruppi - Ruoli

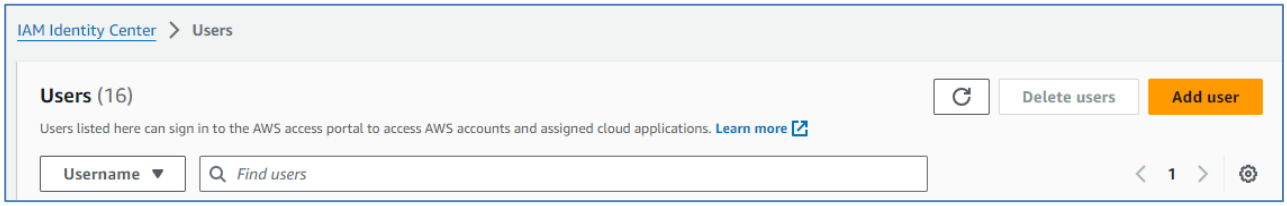
3.1.5 *Creazione nuovo user*

Per creare un nuovo user occorre collegarsi al portale di amministrazione di AWS con le credenziali di referente tecnico della PA:

- Accedere al portale di AWS e selezionare la voce “IAM Identity Center”

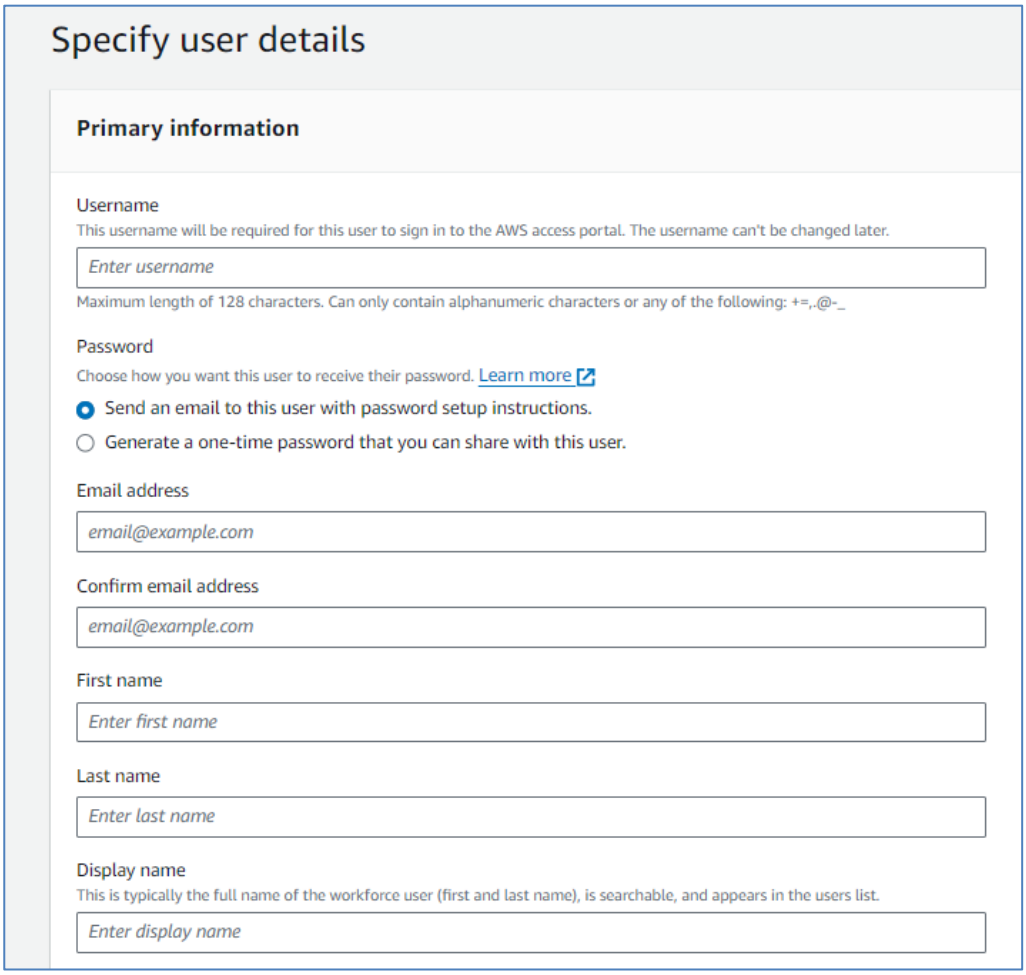


- Selezionare Users e successivamente cliccare su “Add user”



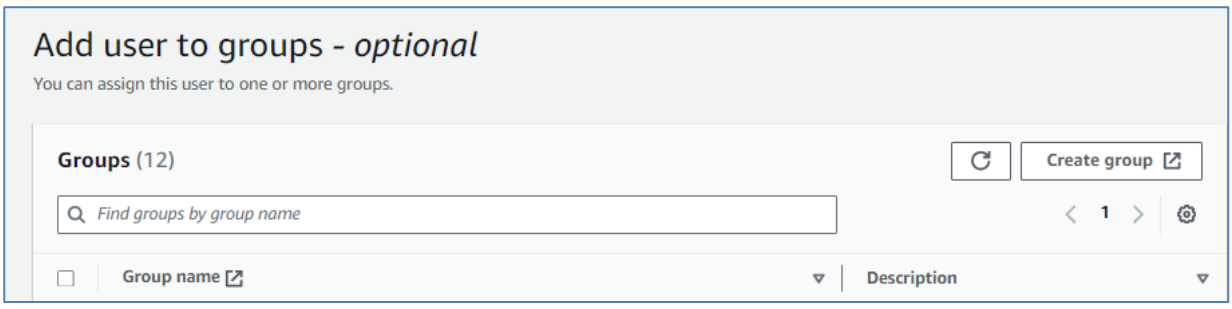
- Compilare il form con i dati indicati:

- Username
- Email Address
- First and Second Name
- Display Name

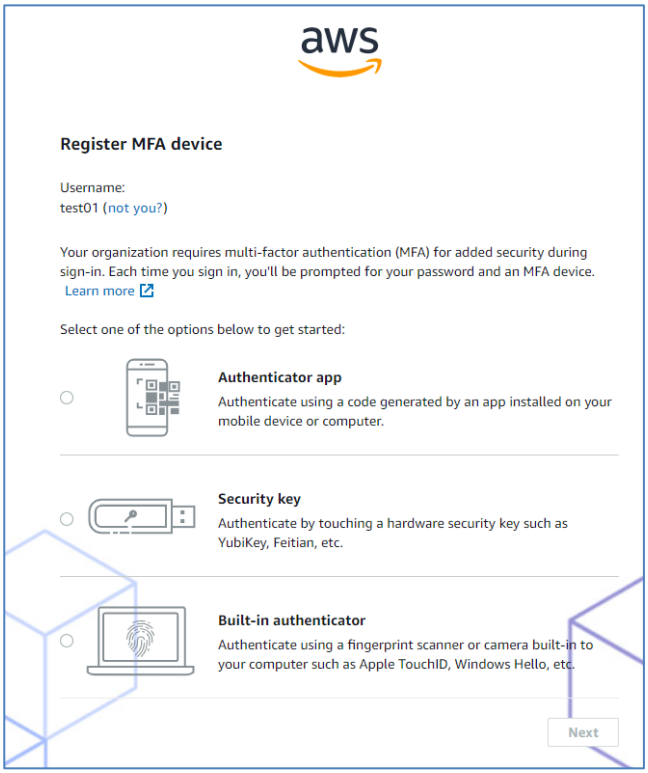


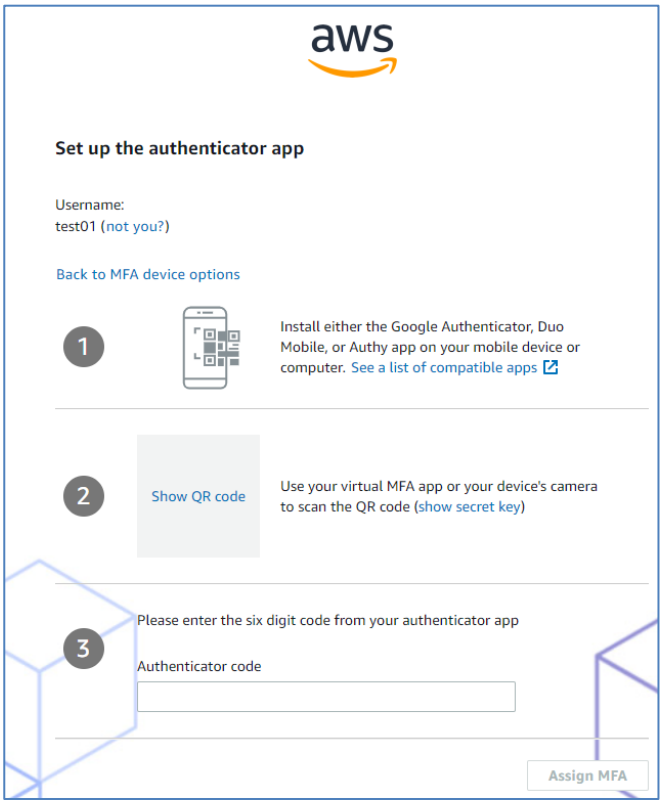
La password può essere inserita subito oppure inviata via email.

- Assegnare la user ad uno dei gruppi PA indicati nel capitolo precedente



- All'utente al primo login verrà richiesta la configurazione del dispositivo MFA





3.1.6 Policy e GuardRails

Di seguito vengono mostrati i controlli abilitati sulla Landing Zone AWS per SPC.
Le policy possono avere due effetti diversi:

- Proactive: impedisce il provisioning della risorsa all'atto della creazione
- Detective: permette il provisioning della risorsa ma notifica (attraverso log di postura di sicurezza) la non conformità

Nome	Descrizione	Effetto
CT.AUTOSCALING.PR.11	Richiedere che solo i tipi di istanza AWS Nitro che supportano la crittografia del traffico di rete tra le istanze siano aggiunti a un gruppo Amazon EC2 Auto Scaling, quando si sovrascrive un modello di lancio.	Proactive
SH.RDS.27	I cluster RDS DB devono essere crittografati a riposo	Detective
SH.RDS.3	Le istanze DB RDS devono avere la crittografia a riposo abilitata.	Detective
CT.EC2.PR.19	Richiedere che un'istanza EC2 utilizzi un tipo di istanza AWS Nitro che supporti la crittografia nel passaggio tra le istanze quando viene creata utilizzando il tipo di risorsa AWS::EC2::Instance	Proactive
CT.S3.PR.10	Richiedere che un bucket Amazon S3 abbia una crittografia lato server configurata utilizzando una chiave AWS KMS.	Proactive
SH.S3.17	I bucket S3 devono essere crittografati a riposo con le chiavi AWS KMS.	Detective
CT.EC2.PR.9	Richiedere che qualsiasi modello di lancio di Amazon EC2 non assegni automaticamente indirizzi IP pubblici alle interfacce di rete.	Proactive
SH.EC2.15	Le sottoreti EC2 non devono assegnare automaticamente indirizzi IP pubblici.	Detective
SH.EC2.3	I volumi EBS collegati devono essere crittografati at rest	Detective
SH.EC2.7	La crittografia predefinita di EBS deve essere abilitata	Detective
SH.EC2.9	Le istanze EC2 non devono avere un indirizzo IPv4 pubblico.	Detective
CT.EC2.PV.2	Richiedere che un volume Amazon EBS collegato sia configurato per crittografare i dati at rest	Preventive
AWS-GR_EC2_INSTANCE_NO_PUBLIC_IP	Rilevare se un'istanza Amazon EC2 ha un indirizzo IPv4 pubblico associato	Detective
AWS-GR_NO_UNRESTRICTED_ROUTE_TO_IGW	Rilevare se nella tabella delle rotte di un Internet Gateway (IGW) sono presenti rotte pubbliche	Detective
AWS-GR_SUBNET_AUTO_ASSIGN_PUBLIC_IP_DISABLED	Rilevare se alle sottoreti di Amazon VPC è assegnato un indirizzo IP pubblico	Detective

CT.EC2.PR.15	Richiedere che un'istanza Amazon EC2 utilizzi un tipo di istanza AWS Nitro quando viene creata dal tipo di risorsa "AWS::EC2::LaunchTemplate"	Proactive
AWS-GR_RDS_INSTANCE_PUBLIC_ACCESS_CHECK	Rilevare se è abilitato l'accesso pubblico alle istanze di database Amazon RDS	Detective
CT.RDS.PR.16	Richiedere che un cluster di database Amazon RDS abbia la crittografia a riposo configurata	Proactive
CT.RDS.PR.24	Richiedere che un'istanza di database Amazon RDS abbia la crittografia a riposo configurata	Proactive
SH.RDS.18	Le istanze RDS devono essere distribuite in un VPC	Detective
SH.RDS.27	I cluster di database RDS devono essere crittografati a riposo	Detective
CUSTOM	Tutte le nuove subnet create devono essere obbligate a transitare verso HUB ACCOUNT (con GTW attachment)	
SH.ECS.2	I servizi ECS non devono avere indirizzi IP pubblici assegnati automaticamente	Detective
AWS-GR_EKS_ENDPOINT_NO_PUBLIC_ACCESS	Rilevare se un endpoint Amazon EKS è bloccato dall'accesso pubblico	Detective
CT.EKS.PR.2	Richiedere che un cluster Amazon EKS sia configurato con la crittografia crittografia segreta utilizzando le chiavi del servizio di gestione delle chiavi (KMS) di AWS	Proactive
SH.EKS.1	Gli endpoint del cluster EKS non devono essere accessibili al pubblico	Detective
CT.WAFV2.PR.1	Richiedere che una ACL web AWS WAFV2 non sia vuota	Proactive
CT.WAFV2.PR.2	Richiedere che un gruppo di regole AWS WAFV2 sia non vuoto	Proactive
CUSTOM	Imporre ad ALB che abbia un profilo WAF (anche su HUB Account)	Proactive
CUSTOM	Imporre al NLB di avere un public ip agganciato (quindi i NLB devono essere solo interni)	Proactive
CUSTOM	Imporre ad ALB se è internet facing deve essere solo sulla igress	Proactive
CUSTOM	Nell'HUB la PA può solo modificare le regole FW (non la baseline definita dal PSN). Ma non puo' modificare e cancellare nessuna altra risorsa	Proactive
CUSTOM	Imporre Internet Gateway solo su Igress e Egress	Proactive
CUSTOM	Imporre Nat Gateway solo su e Egress	Proactive
CUSTOM	Tutte le utenze cloud native in ambiente cloud devono avere la MFA abilitata	Proactive
CUSTOM	Tutte le risorse in ambiente cloud devono essere localizzate nella region di Milano (Italia)	Proactive
CUSTOM	Tutto il traffico in uscita ed entrata per i servizi del PSN deve essere gestito tramite un hub dedicato, istanziato in ambito Public Cloud. Modello network HUB and SPOKE	Proactive

CUSTOM	Il PSN invia alert via email alla PA in caso di fault, anche parziale e di manutenzione programmata dei servizi cloud. Deve essere direttamente il CSP ad inviare gli alert, per quello che riguarda le proprie risorse	Detective

3.1.7 Autenticazione

Le utenze dell'ambiente AWS Cloud sono di tipo "cloud native", ovvero sono identità digitali create direttamente nel tenant del cliente finale, ad eccezione dell'utenza del referente tecnico che è un'utenza che proviene dall'On-Premise.

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.

Si noti che tutte le identità digitali del tenant AWS richiedono autenticazione a due fattori.

4 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.

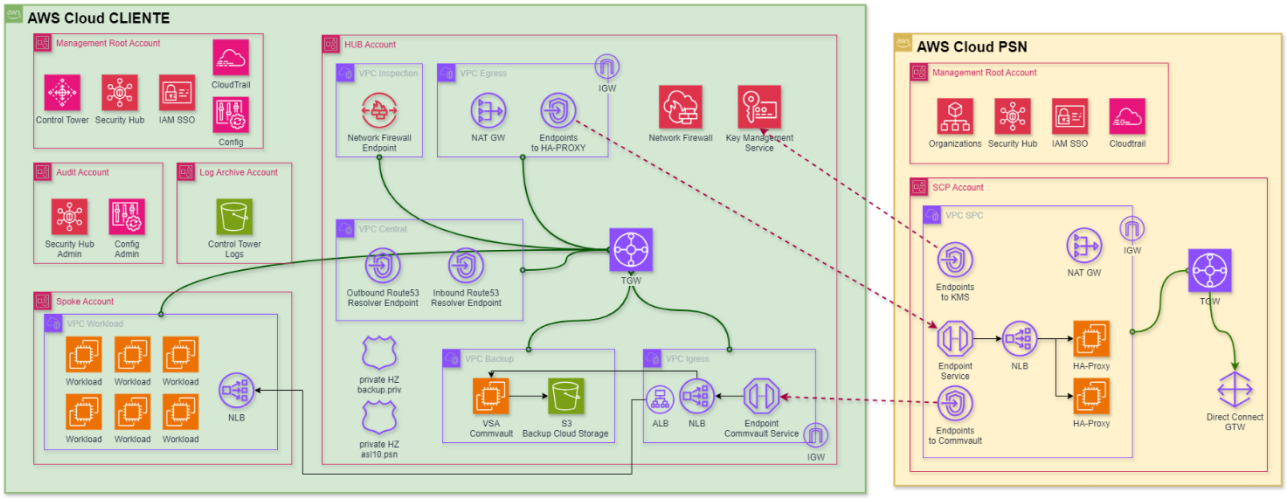


Figura 1: Design di Rete

In questo modello il Transit Gateway presente nell'HUB è l'elemento che mette in comunicazione tutte le VPC presenti nell'HUB e in ciascuno Spoke, compreso le eventuali VPN S2S.

Le Tabella di routing Spoke del Transit Gateway nell'HUB è associata in automatico a tutte le VPC, e che fa sì che tutto il traffico dagli Spoke, sia verso Internet, che tra Spoke e Hub, venga forzato verso il Firewall che risiede sulla VPC Inspection dell'HUB.

Il Firewall ha anche la funzione di Sonda IDS/IPS che sarà abilitato puntualmente dove necessario.

Nell'HUB è presente un DNS Profile per la risoluzione di tutti gli FQDN richiesti.

Di seguito vengono riportati i manuali per la gestione operativa riguardante il Network.

4.1.1 Gestione VPC

Per gestire le VPC occorre andare nella sezione VPC del HUB account.

Nel caso in cui la PA ha la necessità di attivare un nuovo Spoke per ospitare una nuova VPC, la PA dovrà seguire la procedura per la creazione delle risorse attraverso l'apertura di un ticket al PSN il quale provvederà ad espletare le seguenti attività:

- concordare un piano di indirizzamento per il nuovo Spoke;

- verificare il collegamento della VPC con il Transit Gateway dell'HUB;
- verificare la UDR da associare alle subnet della VPC;
- verificare che la tabella di routing del FW Transit Gateway dell'HUB contenda la rotta per lo Spoke;

Tutte le subnet all'interno della VPC creata si vedono tra di loro, al netto di specifici Network ACL e/o Security Group.

4.1.2 Gestione Subnet

Per gestire le VPC subnet occorre andare nella sezione VPC.

La PA può gestire le Subnet all'interno della VPC dello Spoke.

Per aggiungere una nuova subnet all'interno di una VPC occorre prima di tutto verificare se esiste ancora disponibilità di Reti IP libere nello spazio di indirizzamento messo a disposizione per la VPC.
Si raccomanda di creare sempre una subnet su ogni zona della Region; le zone a disposizione sono tre: a, b, c; quindi per ogni subnet, ne verranno create tre.
Si raccomanda di creare sempre le subnet su ciascuna zona denominandole -a, -b, -c, al fine distinguerle.

N.B: Alle subnet appena create viene associata per default la Network ACL di Default, che non consente tutto il traffico In/Out; per controllare il traffico locale sulle Subnet o sulle Istanze, fare riferimento alla Sezione "Gestione Security Groups e Network ACL".

Per creare una nuova subnet occorre andare nella VPC dello Spoke, posizionarsi nella sezione subnet e creare una nuova subnet:

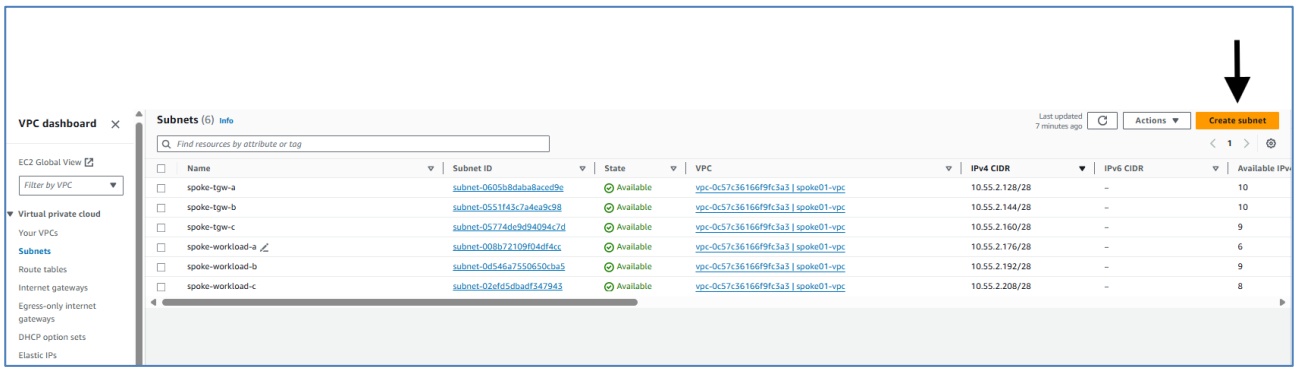


Figura 2: Creazione Subnet 1

Possono essere create tutte le subnet in un unico form.
Configurare VPC ID, Nome, Availability Zone e IP come indicato di seguito:

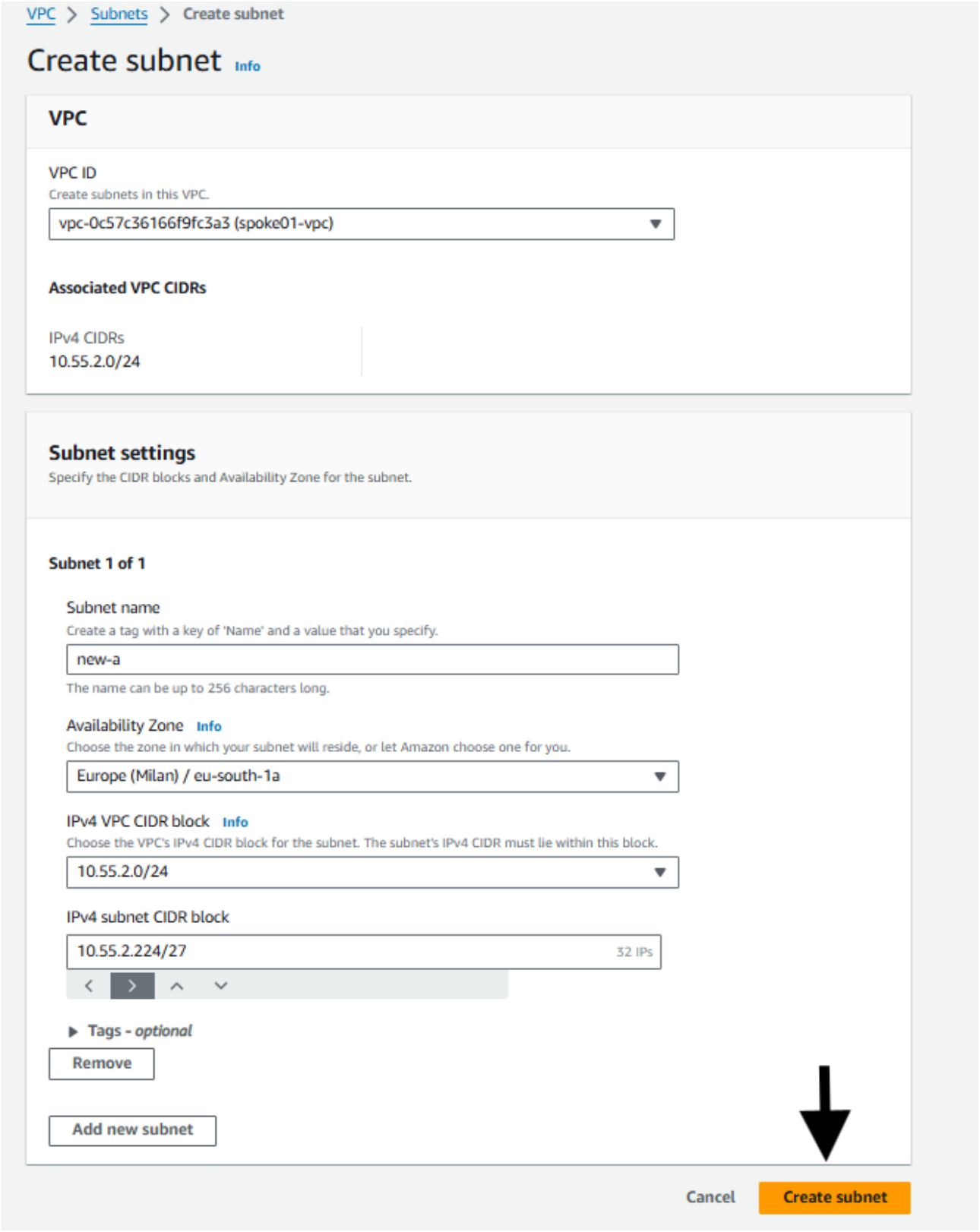


Figura 3: Creazione Subnet 2

Per consentire alle subnet appena create di usare l'infrastruttura di rete, occorre associare loro la tabella di routing esistente sullo Spoke alle subnet appena create.

Cliccare su edit subnet association:

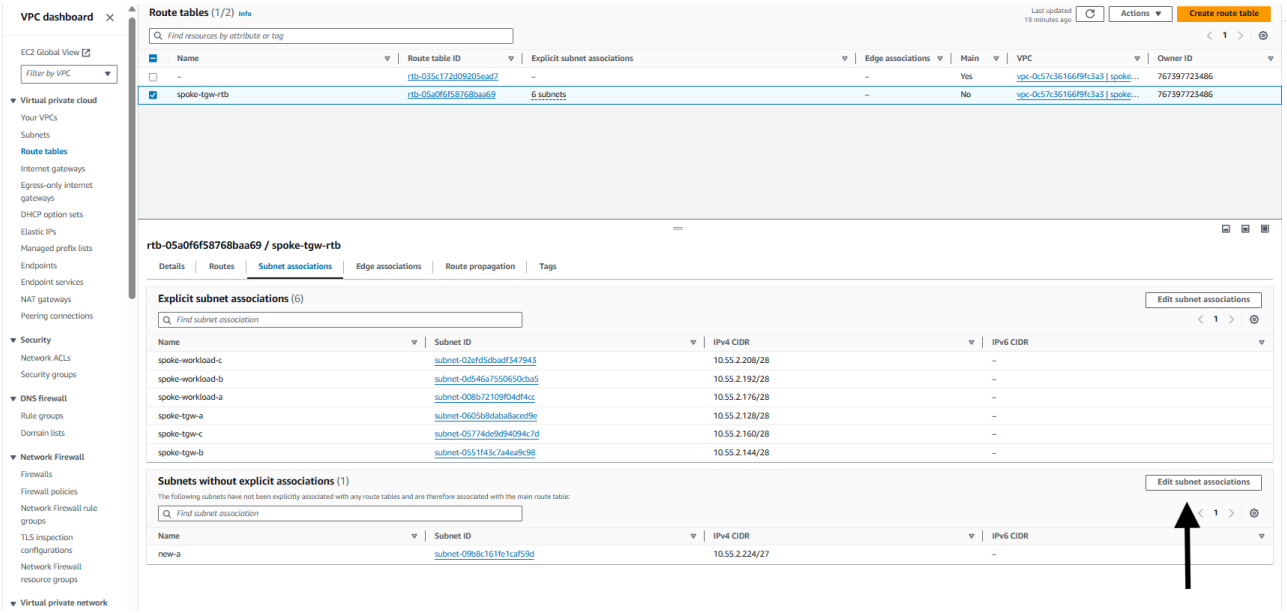


Figura 4: Associazione Subnet 1

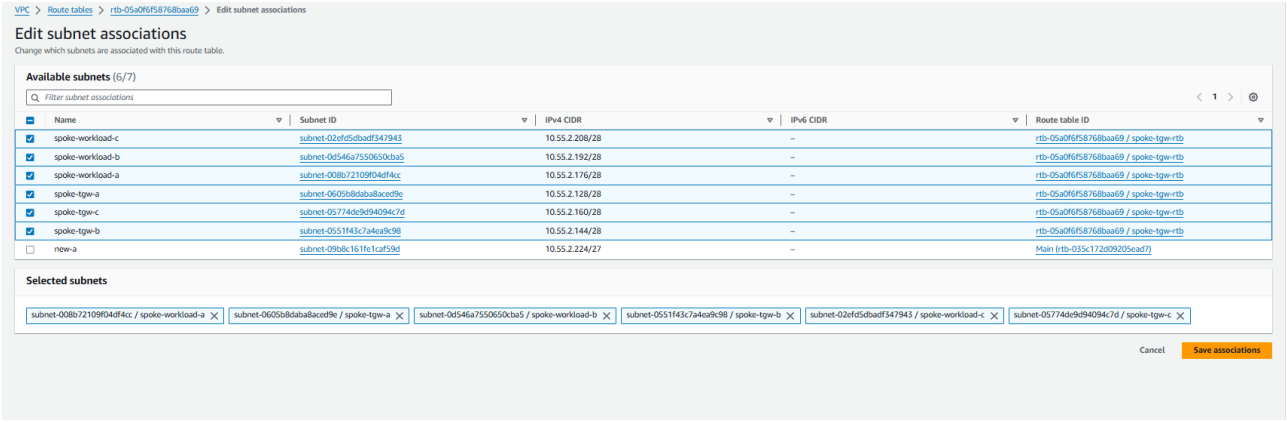


Figura 5: Associazione Subnet 2

Selezionare le Nuove Subnet:

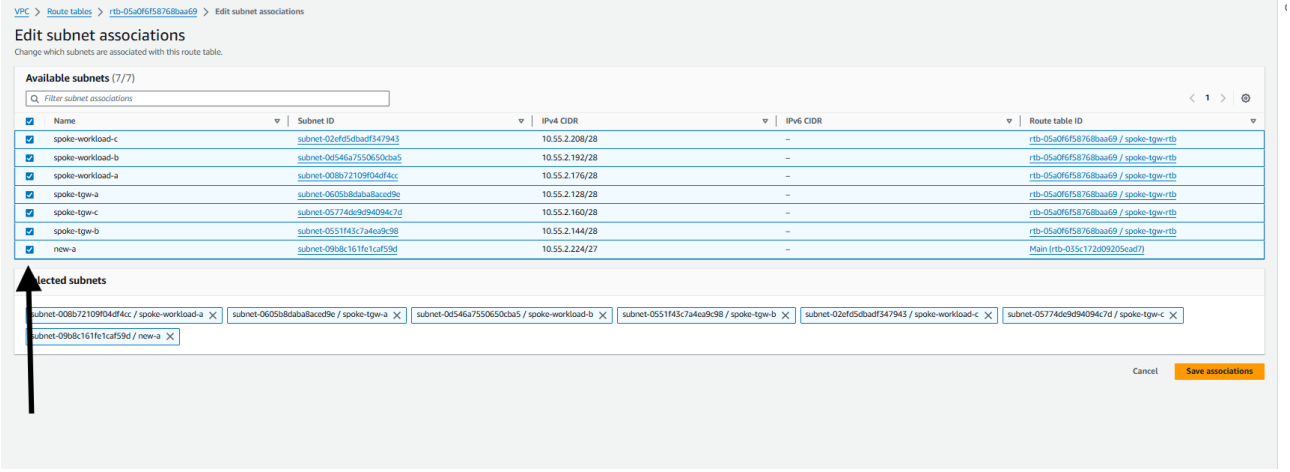


Figura 6: Associazione Subnet 3

Salvare:

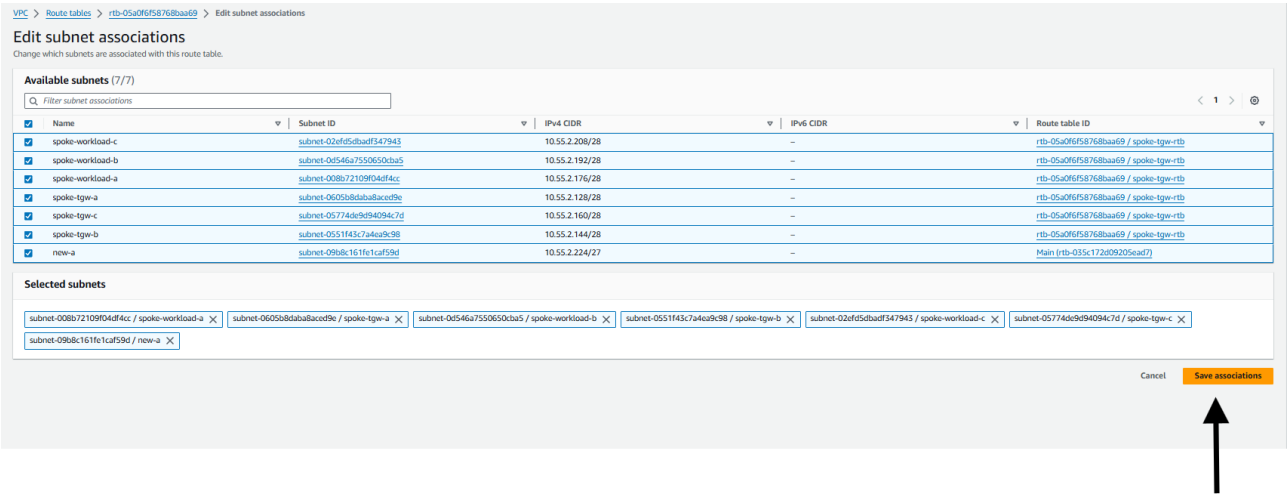


Figura 7: Associazione Subnet 4

La documentazione ufficiale delle VPC si trova al seguente link:
[Amazon Virtual Private Cloud Documentation]

4.1.3 Gestione Security Groups e Network ACL

Per gestire Security Group e Network ACL occorre andare nella sezione VPC.

È possibile controllare il traffico di una risorsa associata al Security Group usando solo i Security Group. Si può associare anche una Network ACL per un ulteriore livello di controllo, ma considerate il fatto che esiste sempre già una Network ACL di Default associata alla Subnet che consente tutto il traffico In/Out e che le Network ACL non sono stateful.

I Security Groups possono contenere solo Regole che aggiungono permessi, e per le risorse che lo consentono, possono essere più di uno associato alla risorsa, sommandosi l'uno all'altro.

Di seguito una tabella riassuntiva di comparazione:

Security group	Network ACL
Opera a livello di Istanza	Opera a livello di Subnet
E applicato alla sola Istanza o alla risorsa associata	E applicato a tutta la Subnet
Supporta solo Regole di Allow	Supporta sia Regole di Allow che di Deny
Controlla tutte le Regole prima di decidere se far passare il Traffico	Prende in considerazione le Regole sulla base dell'ordine
È Stateful quindi non è necessario specificare gli Allow per il traffico di ritorno	È Stateless quindi devono essere presenti anche gli Allow per il traffico di ritorno

Tabella 4: Tabella Comparativa SG e NACL

La gestione su Security Groups e Network ACL si trova nella Sezione VPC.

Le network ACL possono essere associate alle varie Subnet.
I Security Groups possono essere associati ad esempio alle Istanze.

Di seguito un esempio di Network ACL:

- Dettagli:

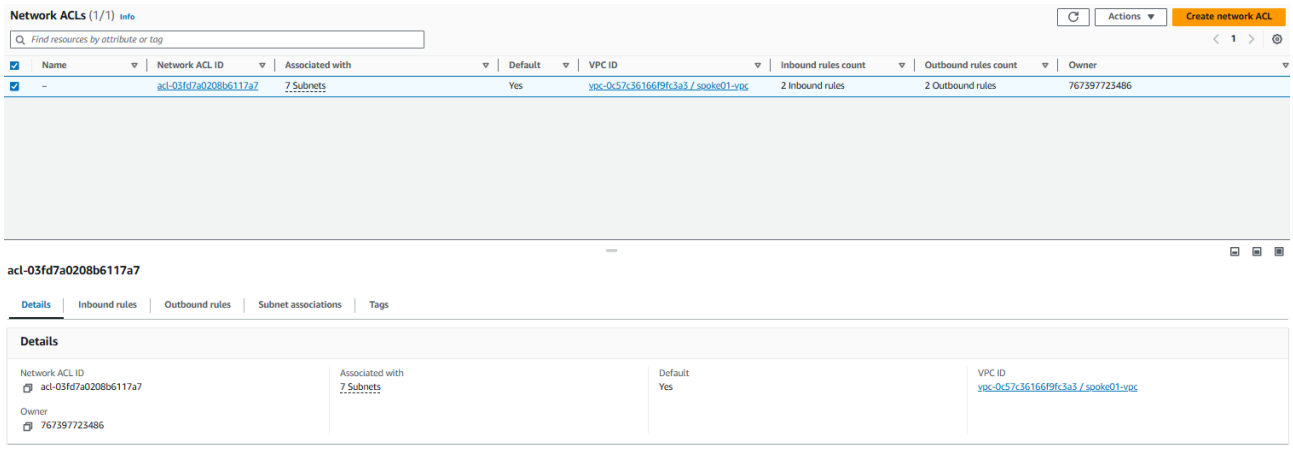


Figura 8: Network ACL

- Inbound rules:

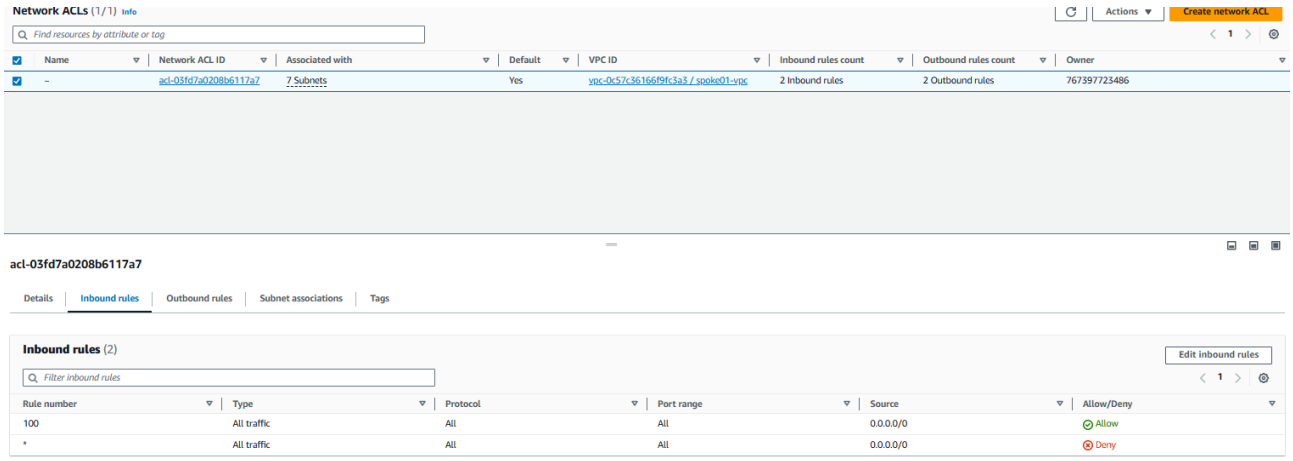


Figura 9: Network ACL Inbound

- Outbound rules:

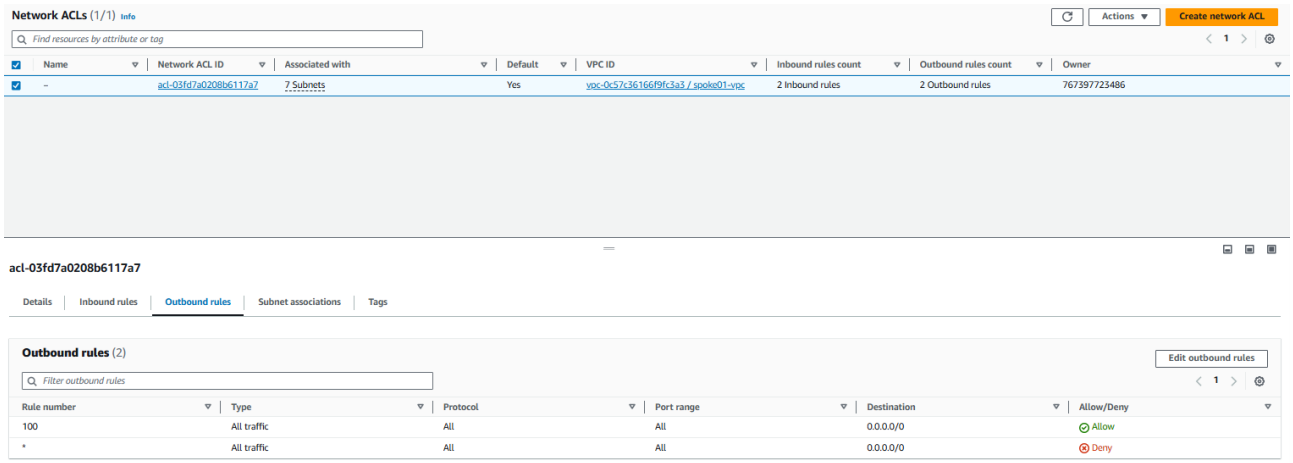


Figura 10: Network ACL Outbound

- Associazione Subnet:

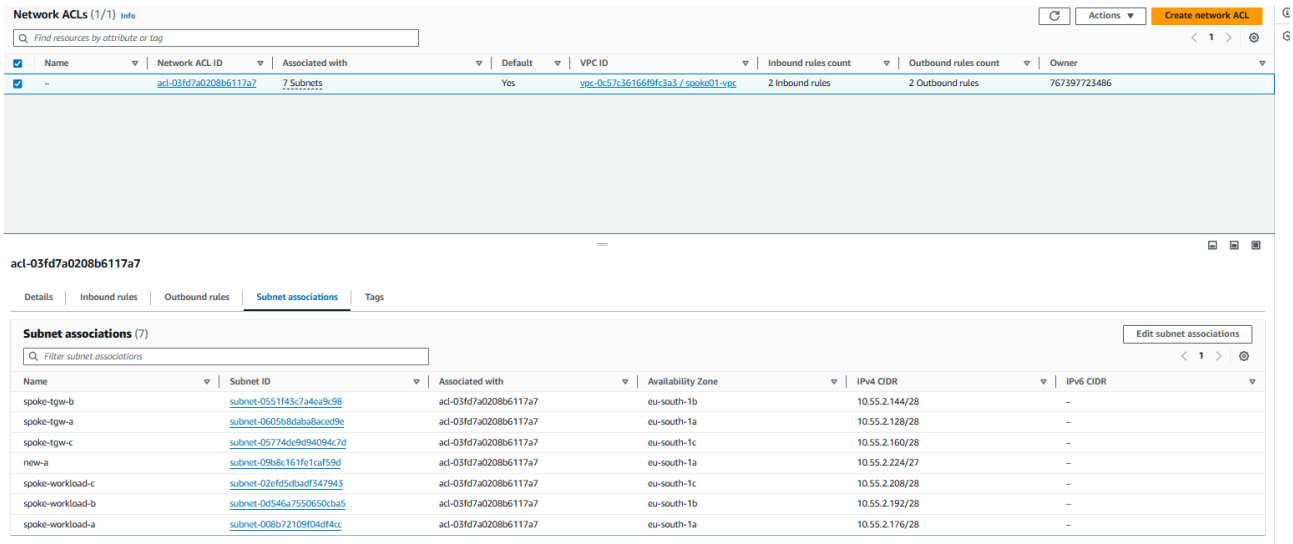


Figura 11: Network ACL Associazione Subnet

Di seguito un esempio di Security Groups:

- Dettaglio:

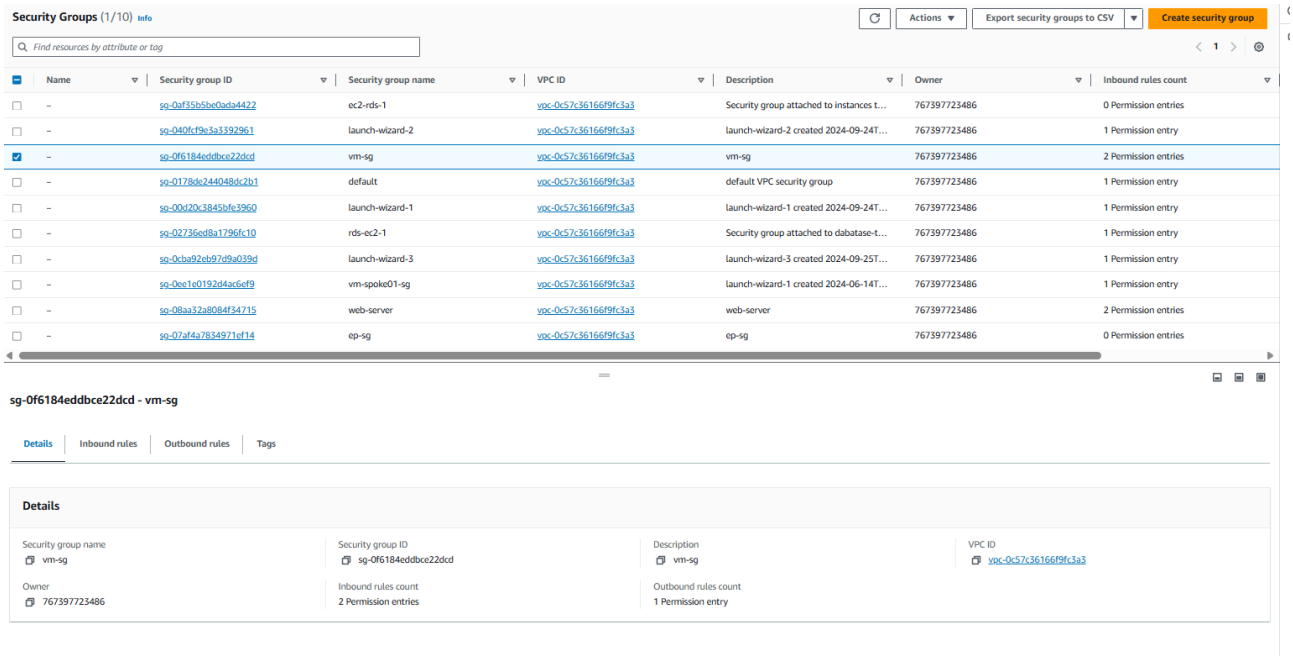


Figura 12: Security Groups

- Inbound Rules:

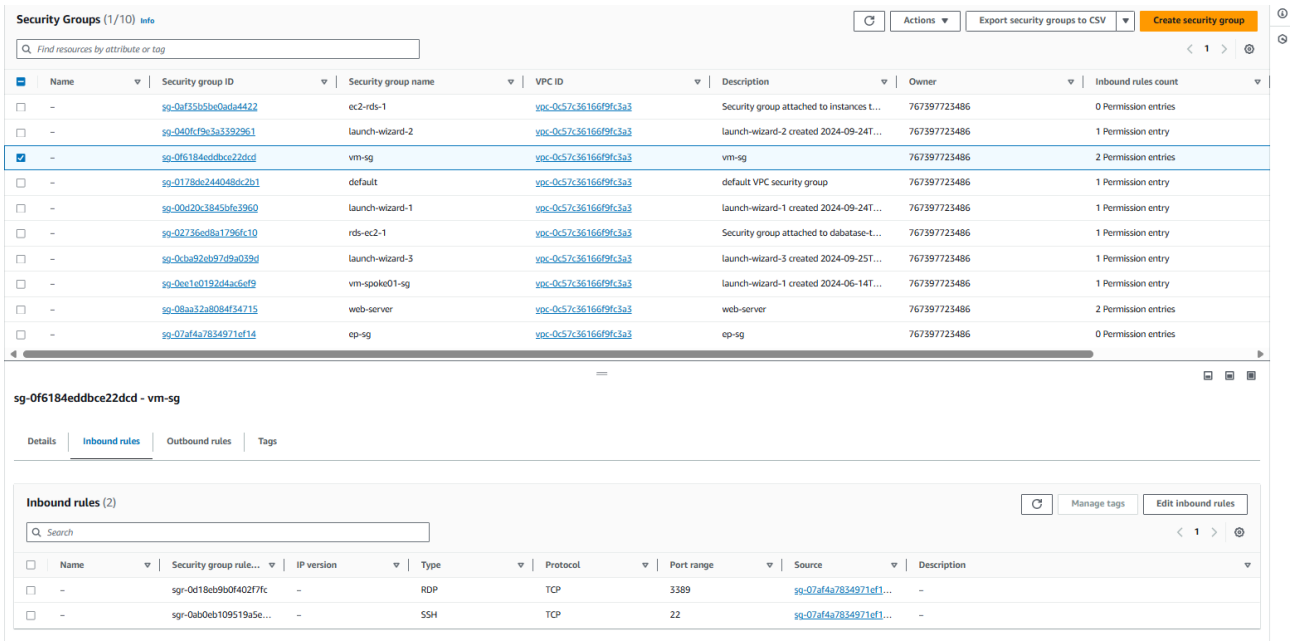


Figura 13: Security Groups Inbound

- Outbound Rules:

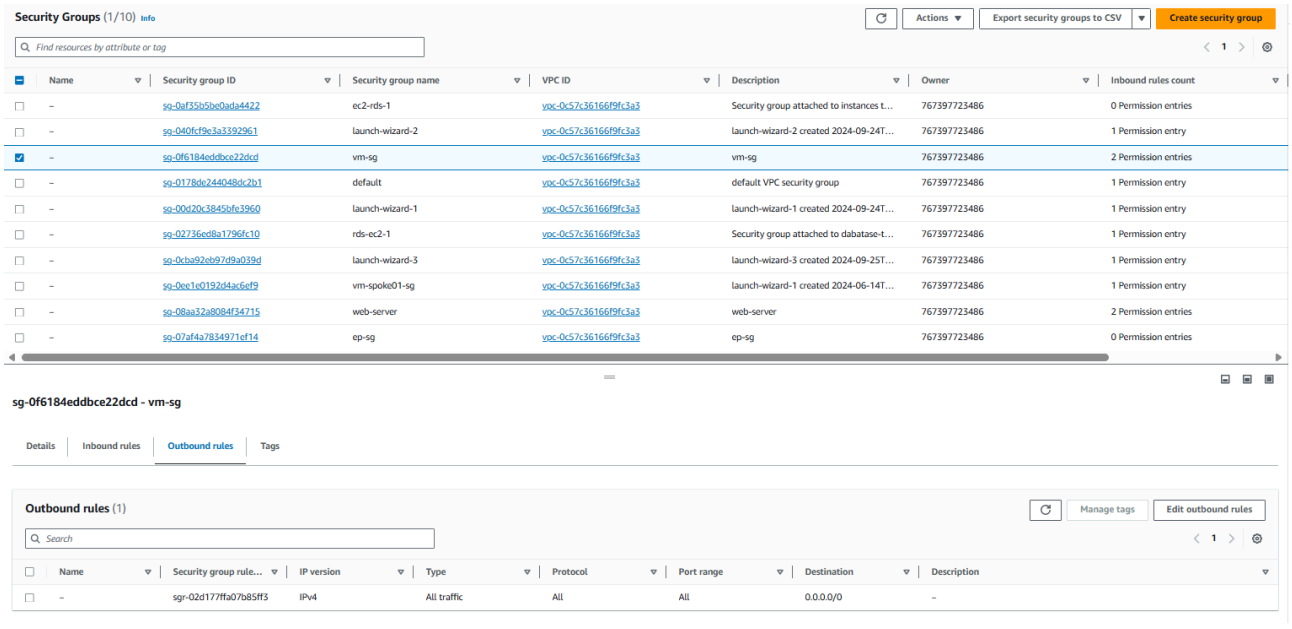


Figura 14: Security Groups Outbound

Per create una Network ACL:

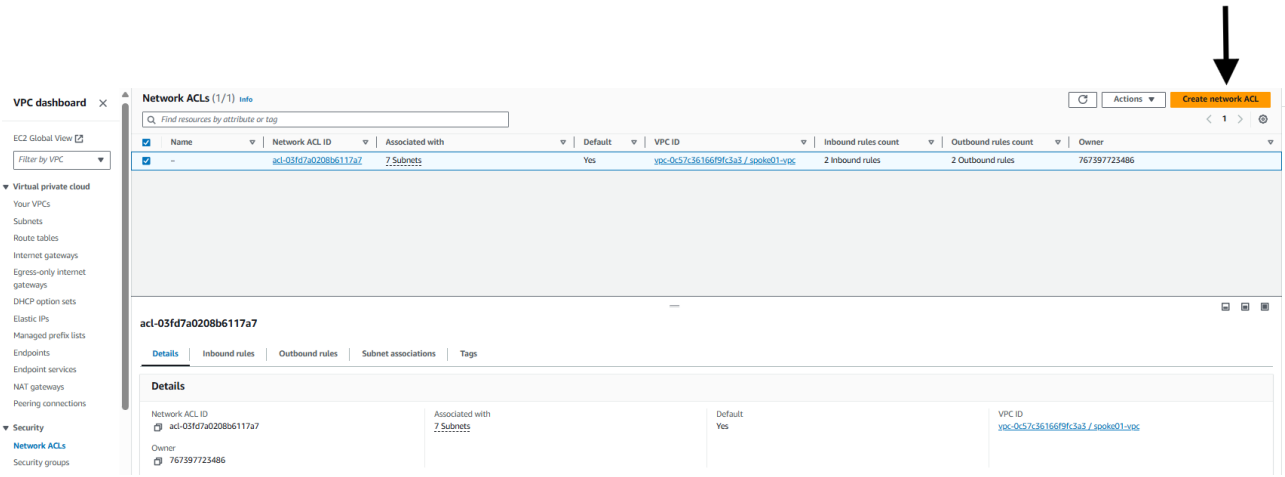


Figura 15: Creazione Network ACL 1

- Specificare VPC, Nome:

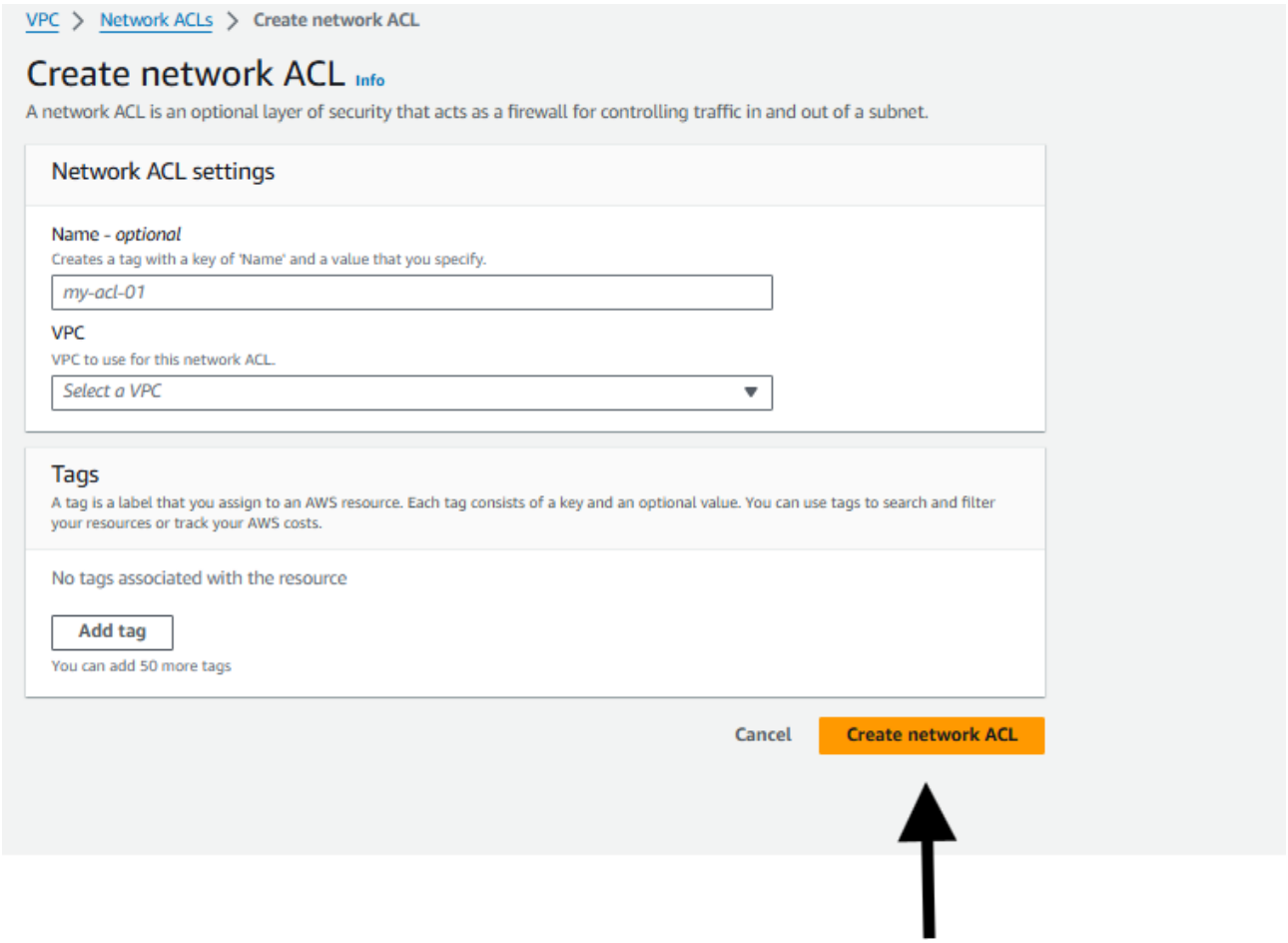


Figura 16: Creazione Network ACL 2

- Editare Inbound e Outbound rules:

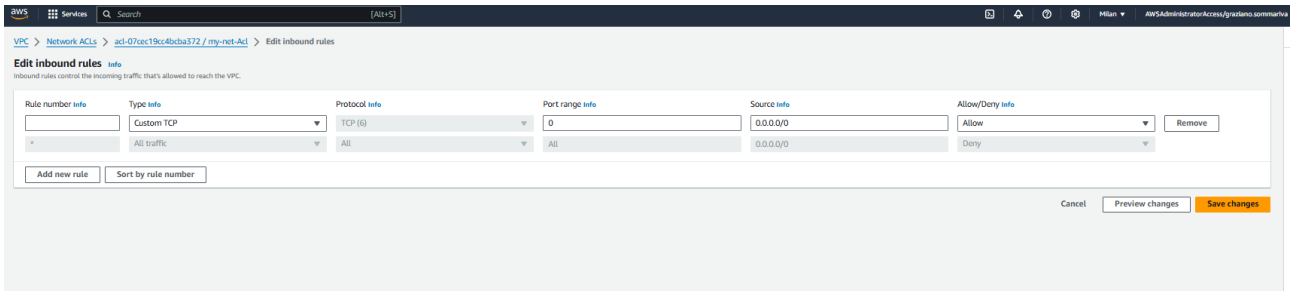


Figura 17: Creazione Network ACL 2

Per creare un Security Group:

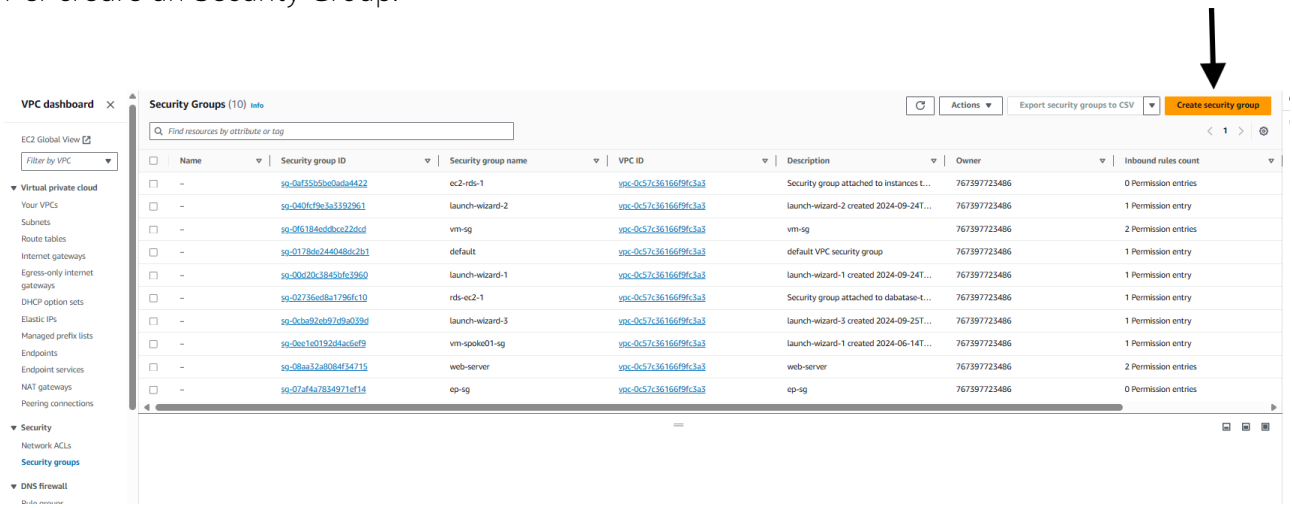


Figura 18: Creazione Security Group 1

- Specificare Nome, VPC, Regole di Inbound e Outbound:

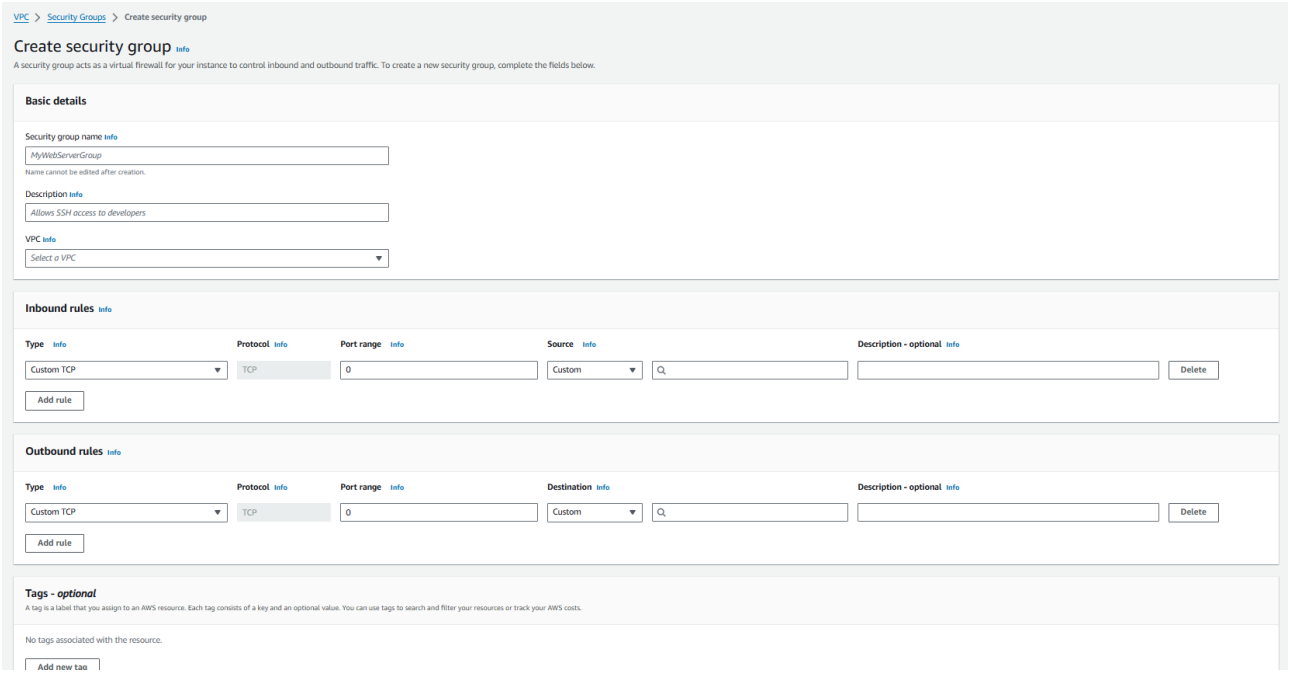


Figura 19: Creazione Security Group 2

4.1.4 Gestione DNS

Per gestire il DNS occorre andare nella sezione Route 53.

Il Servizio di DNS è fornito dal DNS Profile, che risiede nell'HUB e che è condiviso con la Organization Unit che comprende gli Spoke.

Tutte le VPC sono configurate per fornire alle VM un DNS Server, locale alla VPC, che è in grado di usufruire dei Servizi del PNS Profile.

Per gestire il DNS si usa la Sezione Route 53.

Nella Sezione Route 53 troviamo i DNS Endpoint di Outbound e Inbound(opzionale) attestati sulla VPC Central.
Il DNS Endpoint di Outbound serve per risolvere le richieste DNS in uscita.
Il DNS Endpoint di Inbound serve per risolvere le richieste DNS in entrata.

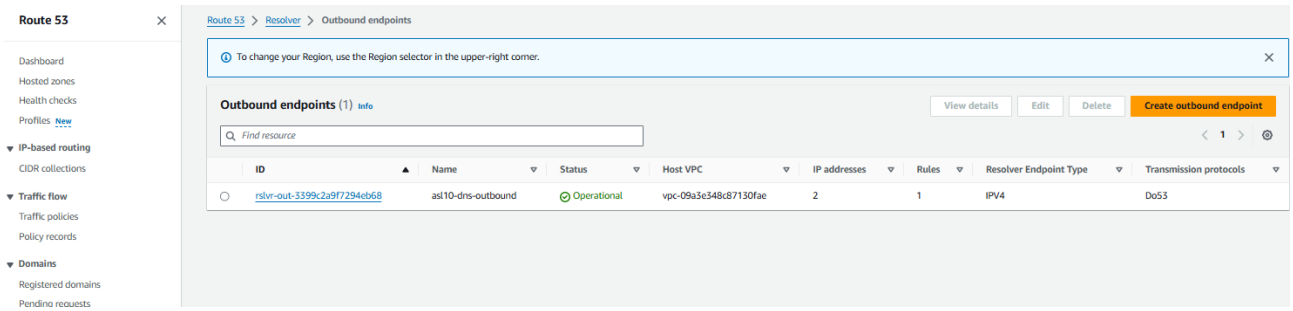


Figura 20: Route 53 Outbound Endpoint

Nella Sezione Route 53 possiamo trovare DNS Rules per consentire la risoluzione di Zone DNS gestire su altri DNS Server usando il DNS Endpoint di Outbound.

Esiste sempre la Rule Internet Resolver, più eventuali DNS rules custom:

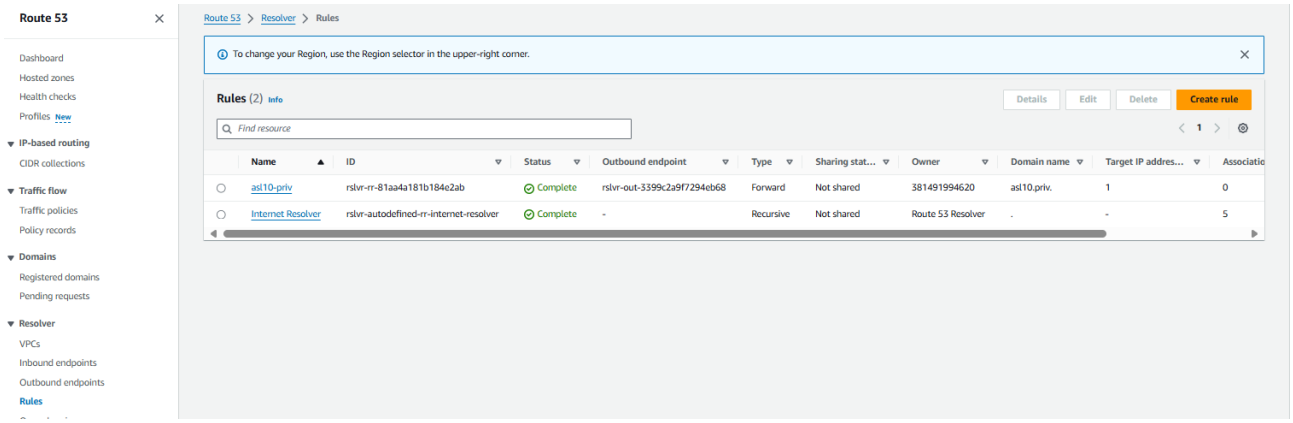


Figura 21: Route 53 Rules

Si possono creare nuove DNS Rule:

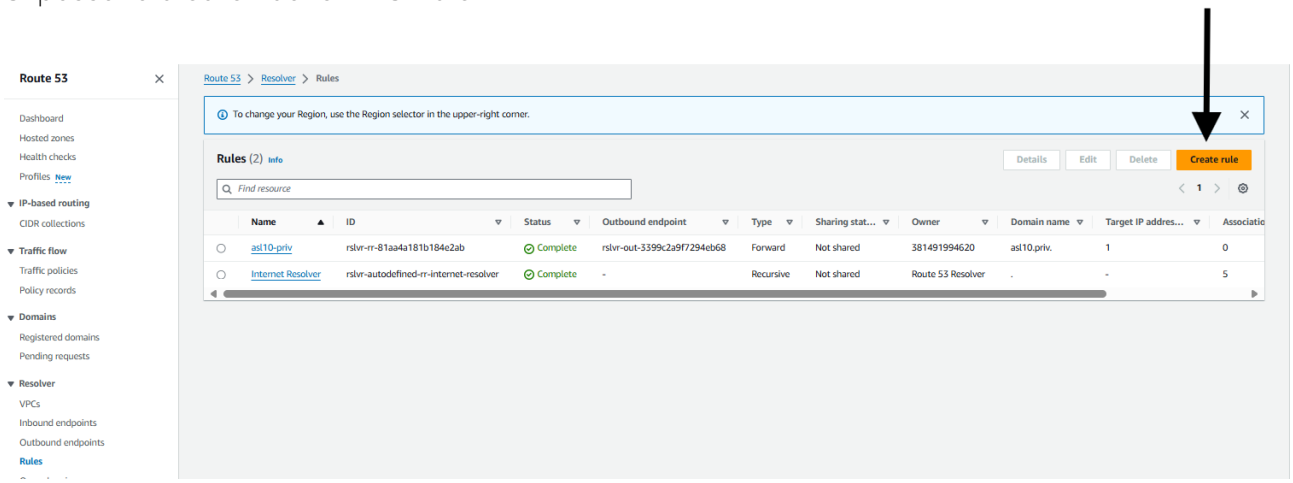


Figura 22: Route 53 Creazione Rules 1

Specificando Nome, Zona DNS, VPC associata (Central), DNS Outbound Endpoint, Target DNS Ips:

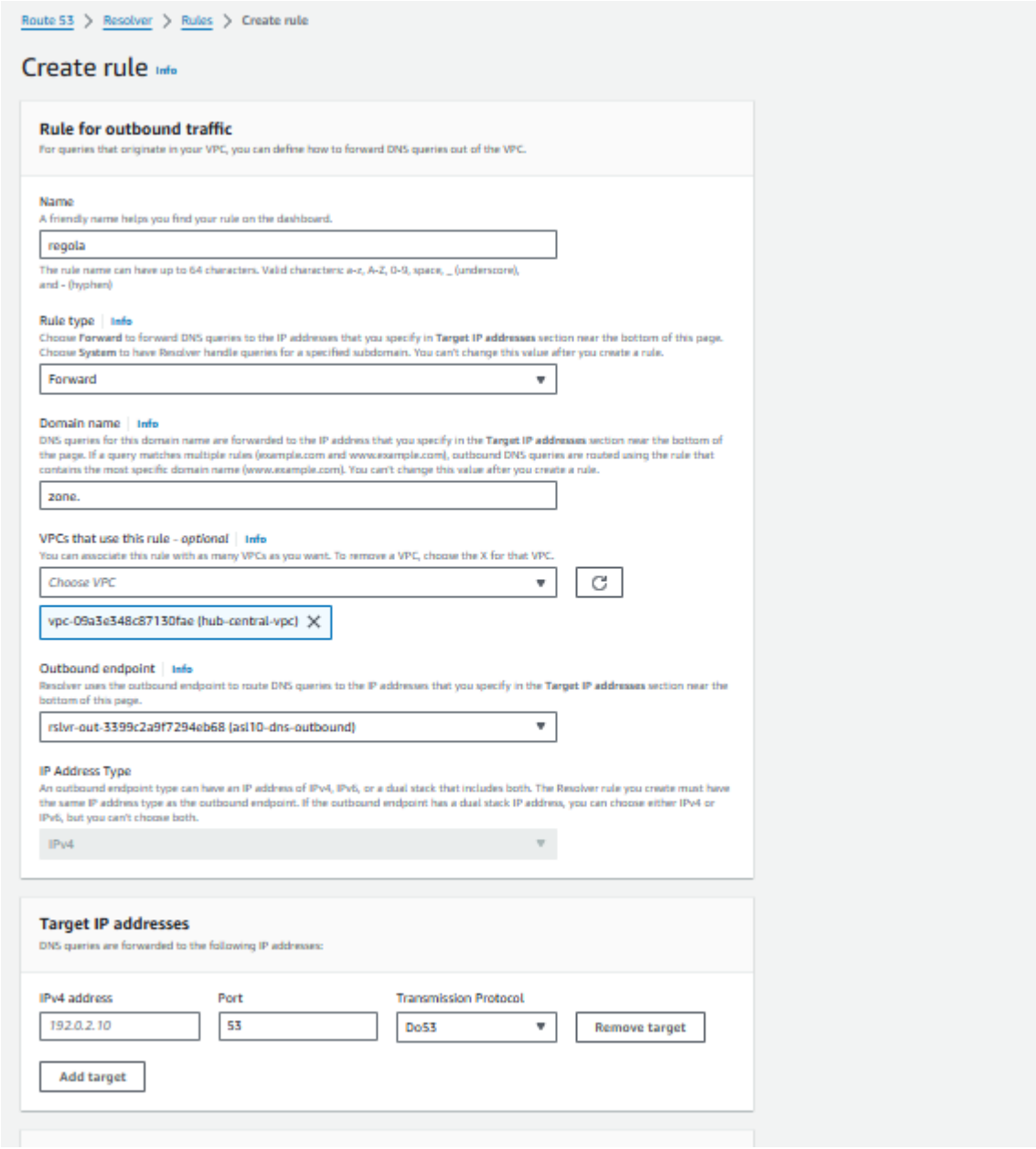


Figura 23: Route 53 Creazione Rules 2

N.B: Per usare le DNS rule occorre associarle al DNS Profile.

Nella Sezione Route 53 si possono trovare anche le Zone DNS private (Hosted Zones). Come Hosted Zones è presente almeno la zona DNS backup.priv con il record della VSA:

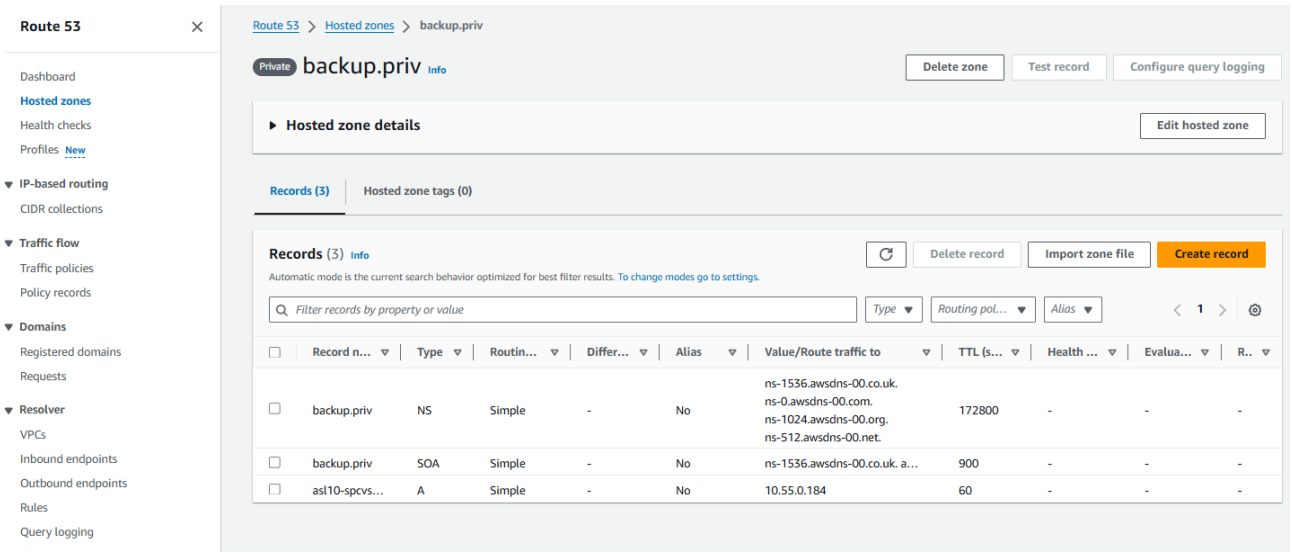


Figura 24: Route 53 Hosted Zones

Si possono creare nuove Hosted zones usando:

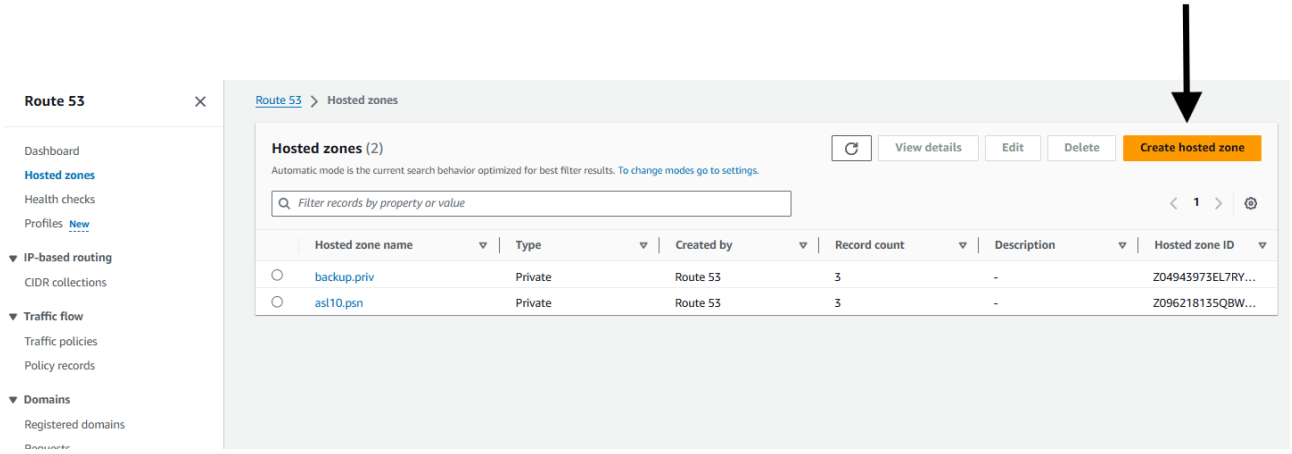


Figura 25: Route 53 Creazione Zones 1

Specificando DNS Zone Name, Tipo (private), Regione (Europe-Milan) VPC-ID della VPC Central:

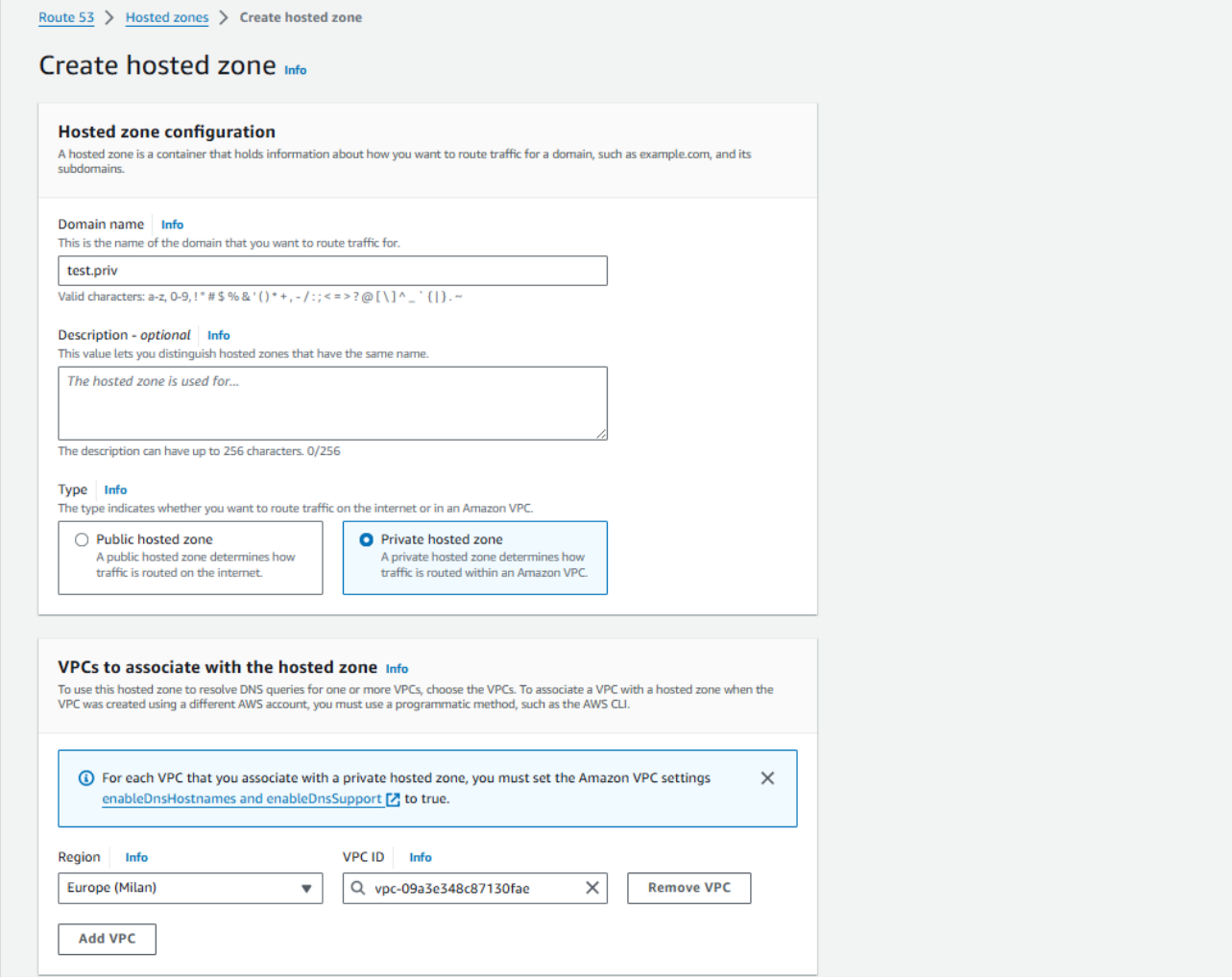


Figura 26: Route 53 Creazione Zones 2

N.B: Per consentire la risoluzione delle zone private occorre associarle al DNS Profile.

Per accedere al DNS Profile nell'HUB andare nella sezione Route 53:

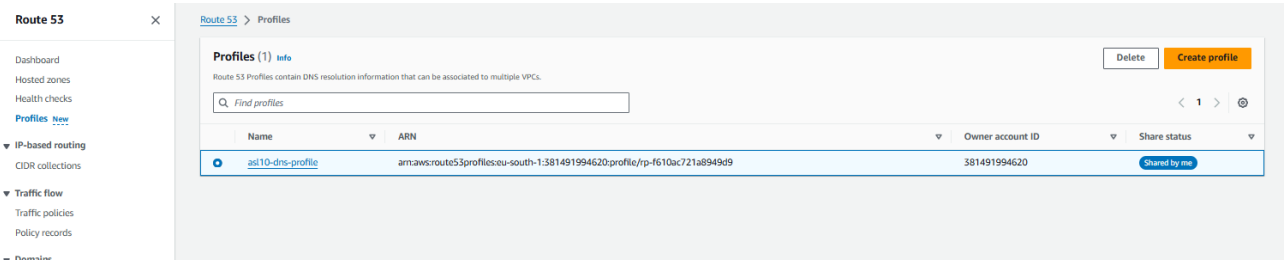


Figura 27: Route 53 DNS Profile 1

Tipicamente Il DNS può comprendere.

- Zone DNS private

Nel DNS Profile è presente almeno l'associazione la zona DNS Privata backup.priv con dentro il record DNS che fa riferimento alla VSA:

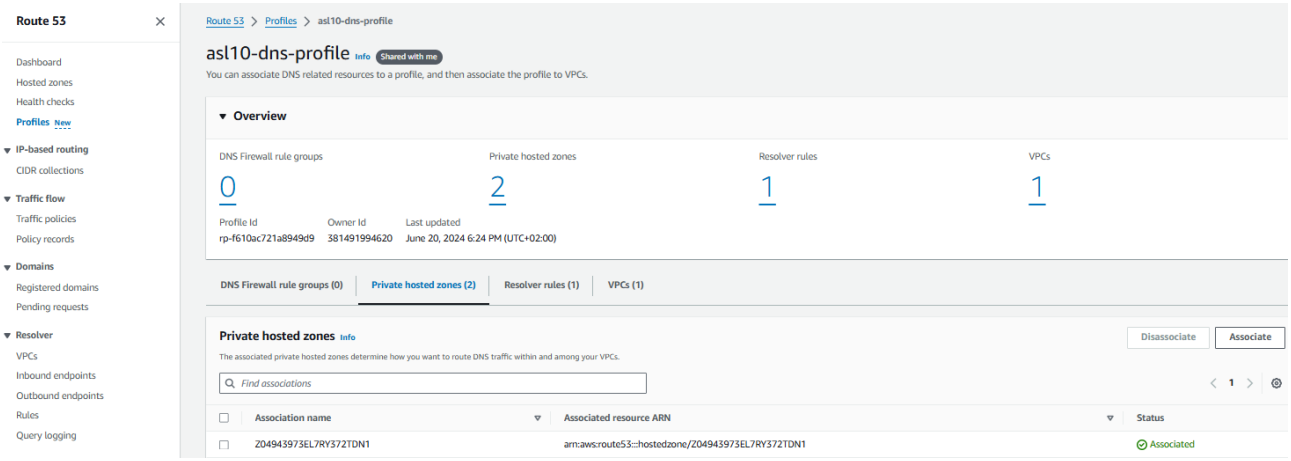


Figura 28: Route 53 DNS Profile 2

- Regole di Risoluzione DNS verso Zone DNS Esterne

Tutte le eventuali DNS Rule che si aggiungono devono essere associate:

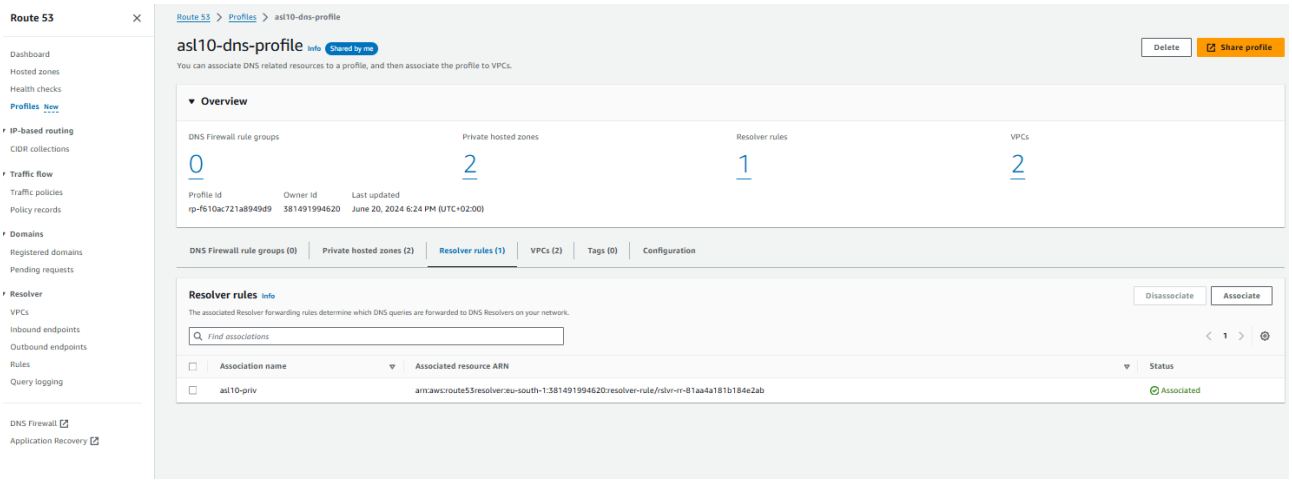


Figura 29: Route 53 DNS Profile 3

Il DNS Profile è associato alle VPC che ne possono usufruire:

- Vista da HUB:

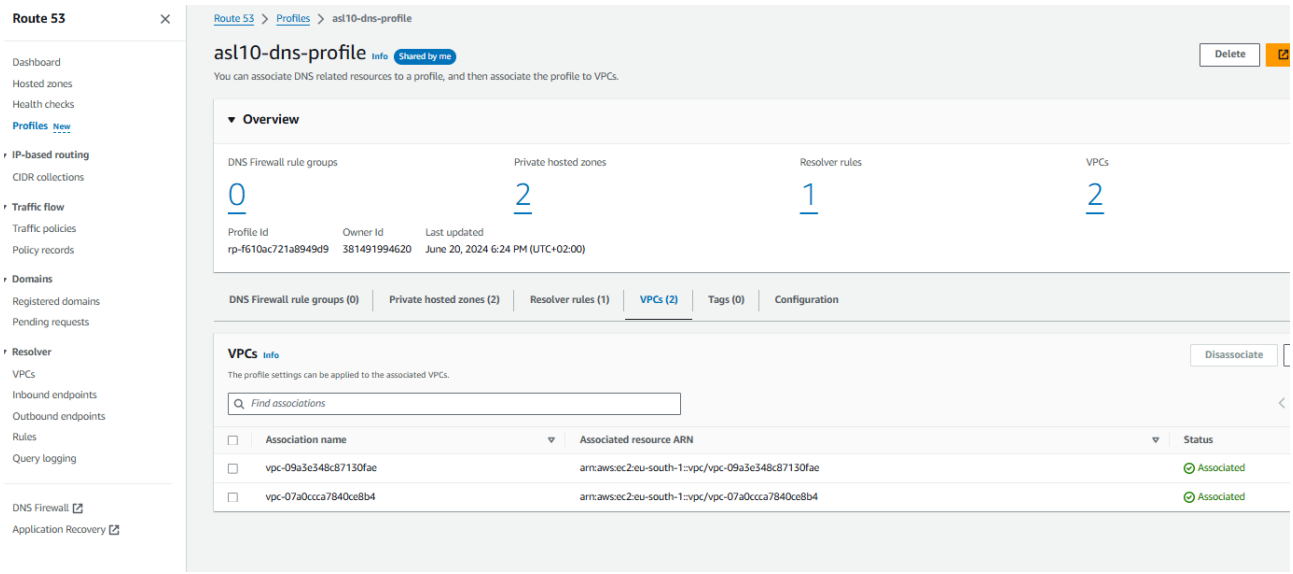


Figura 30: Route 53 DNS Profile 4

- Vista da Spoke:

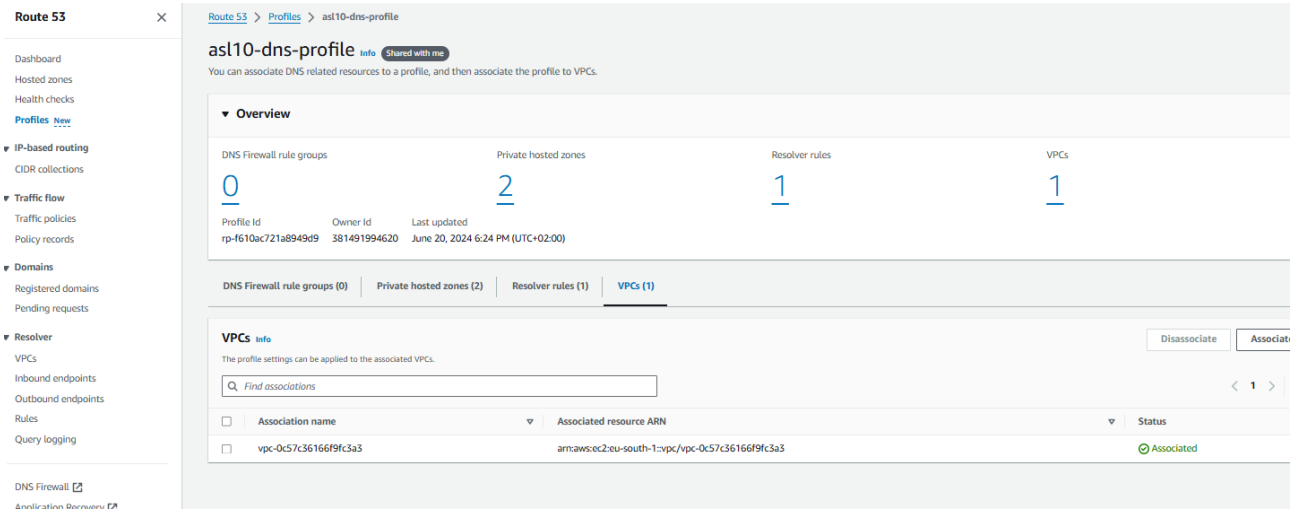


Figura 31: Route 53 DNS Profile 5

La documentazione ufficiale della gestione di Route 53 si trova al seguente link:
[What is Amazon Route 53? - Amazon Route 53]

4.1.5 Gestione Target Groups

Per gestire i Target Groups occorre andare nella sezione EC2.

I Target Groups sono gruppi di risorse che possono essere associate ai Load Balancer.
In fase di creazione di un Load Balancer serve avere il Target Group di riferimento.

Ci sono diversi tipi di Target Group, quelli più in uso sono Target Group verso IP address e verso Instance ec2.

Ogni Target Group lavora con un protocollo e una porta, ed usa un health-check per capire se il Target è disponibile.

L'utilizzo peculiare di un Target Group che punta ad IP è quando un bilanciatore deve bilanciare Instance EC2 che non si trovano sul suo stesso Account, mentre si usa il Target Group che punta ad Instance EC2 quando i Target sono sullo stesso Account.

4.1.6 Gestione Load Balancers

Per gestire i Load Balancer occorre andare nella sezione EC2.

I Load Balancers servono per bilanciare delle risorse.
I Load Balancer possono essere di vari tipi; possono lavorare a livello 4 o 7, e possono essere fatti per essere usati internamente (Internal) o avere accesso verso Internet (Internet-Facing).
I load Balancer di livello 7 possono essere associati ad una policy di WAF.

Tipicamente si potranno usare solo Load Balancer di tipo Internal; solo gli Application Load Balancer per esposizione verso Internet potranno essere di tipo Internet-Facing e con WAF.

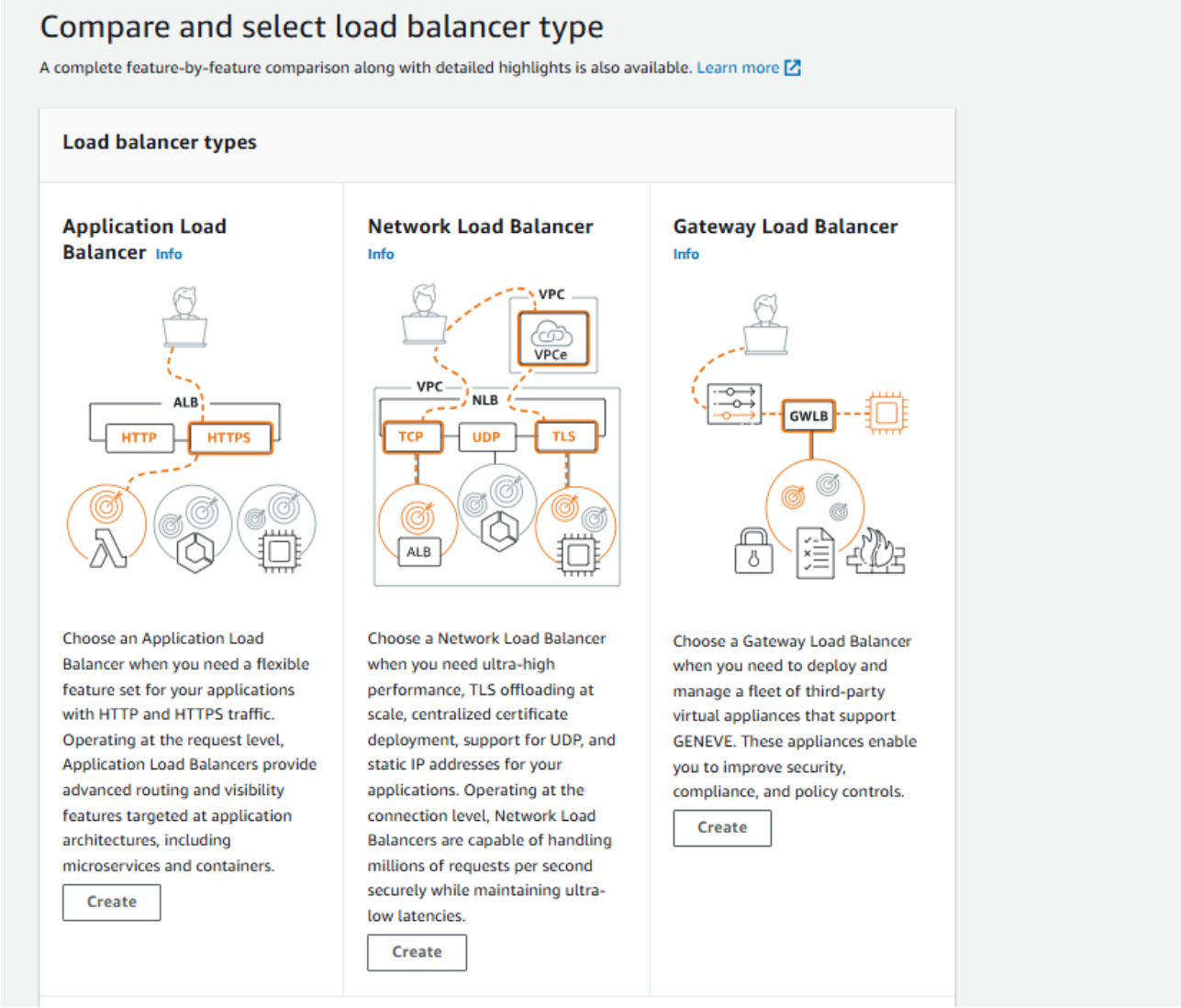


Figura 32: Tipi di Load Balancer

La documentazione ufficiale della gestione dei Load Balancer si trova al seguente link:
[Network Traffic Distribution – Elastic Load Balancing – Amazon Web Services]

4.1.7 Gestione WAF

Per gestire il WAF occorre andare nella sezione WAF & Shield.

Qui possono essere create e gestite le Web ACL che devono essere associate agli Application Load Balancers.

Una Web ACL è un insieme di gruppi di signature verticali sul protocollo HTTP.

È possibile associare diversi gruppi di signature preconfigurati, oppure creare delle proprie signature.
È possibile modificare l'action sulle signature preconfigurate, per esempio, per reagire a casi di falsi positivi.

Ogni Web-ACL potrà avere al massimo 5000 signature; quindi occorre stare attenti al numero di signature dei gruppi che si scegli di inserire.

Di seguito un esempio di creazione di una Web ACL fornendo il Nome:

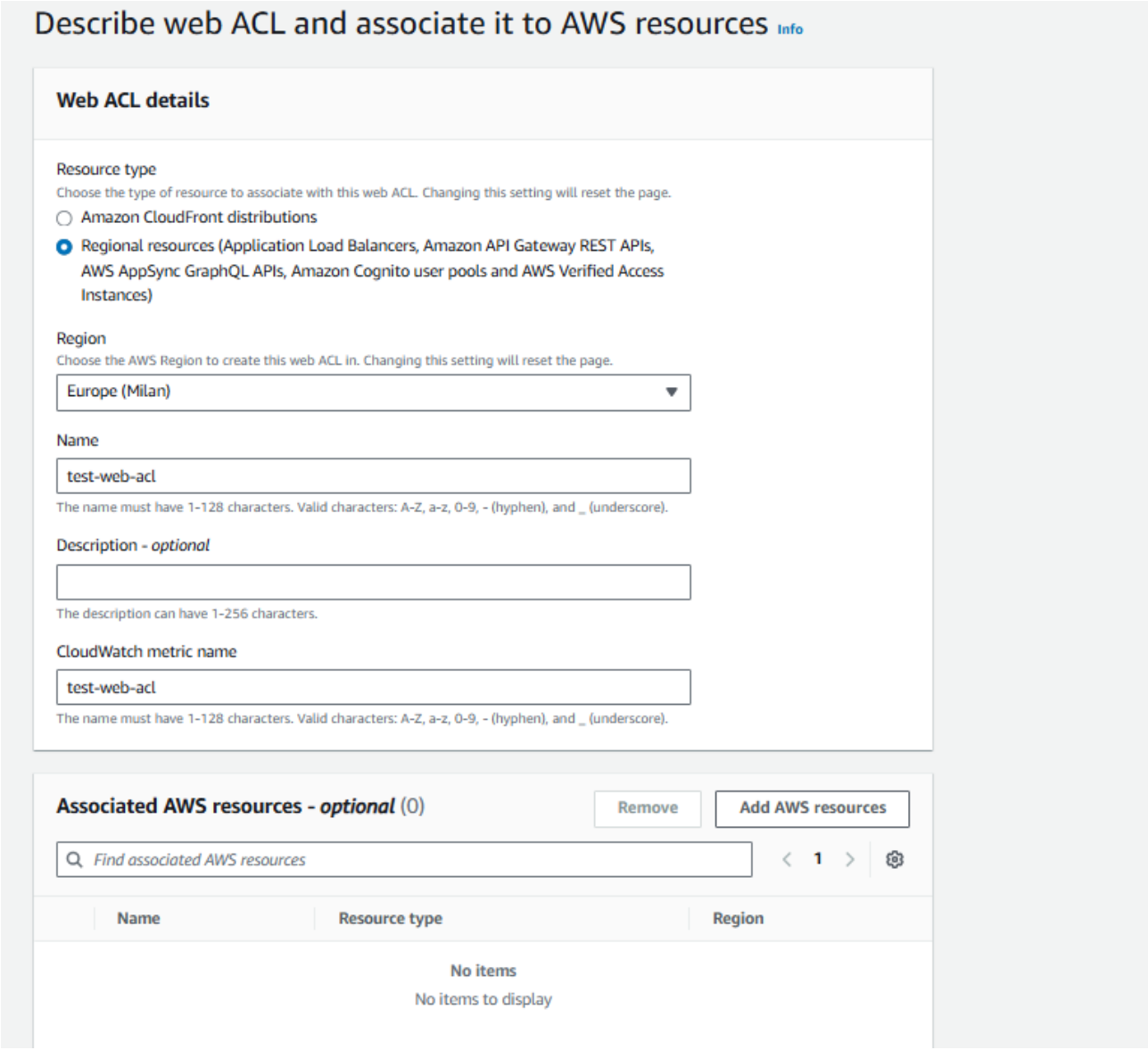


Figura 33: Creazione Web ACL 1

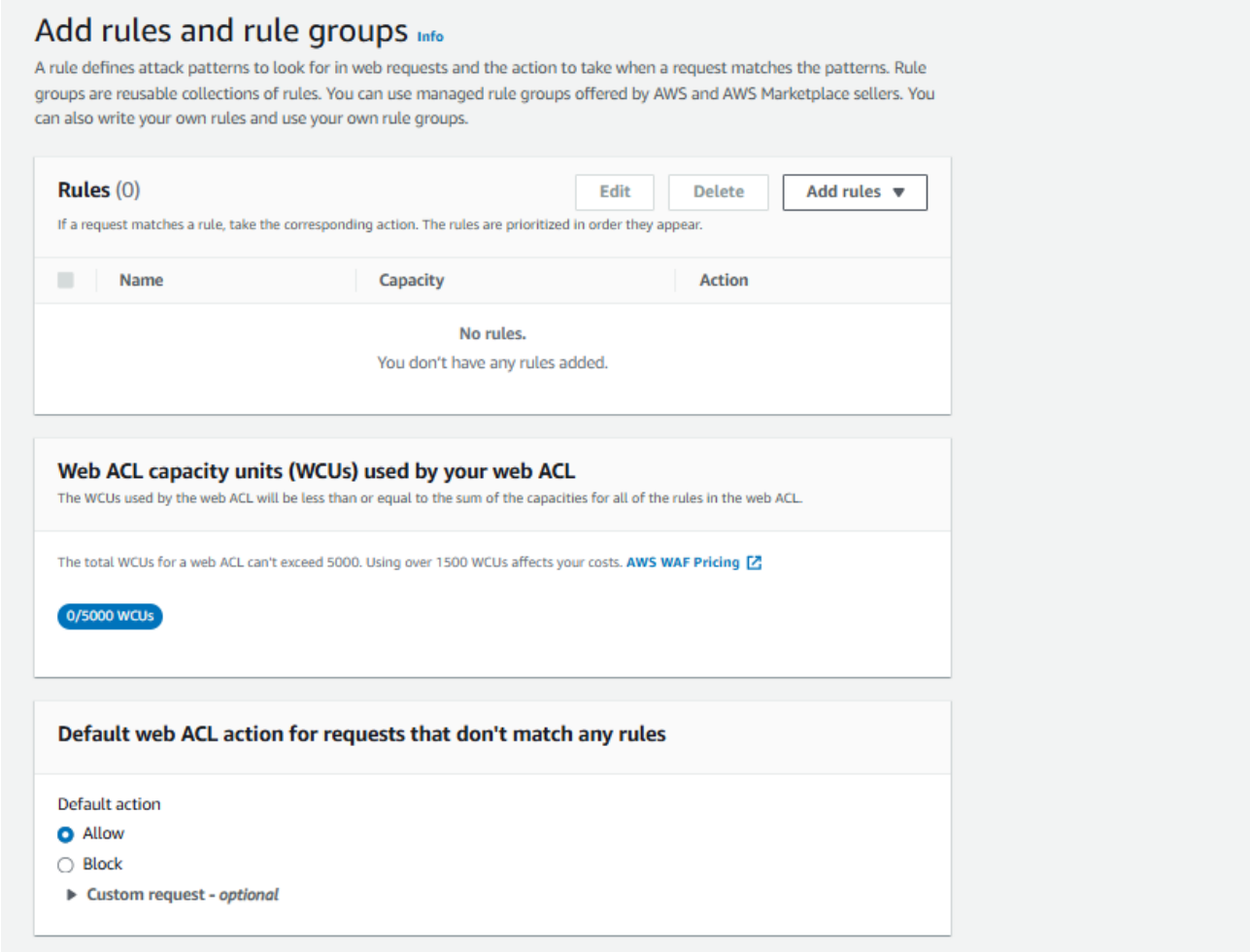


Figura 34: Creazione Web ACL 2

Inserire almeno il gruppo AWS Managed Core Rule set che contiene le OSWAP:

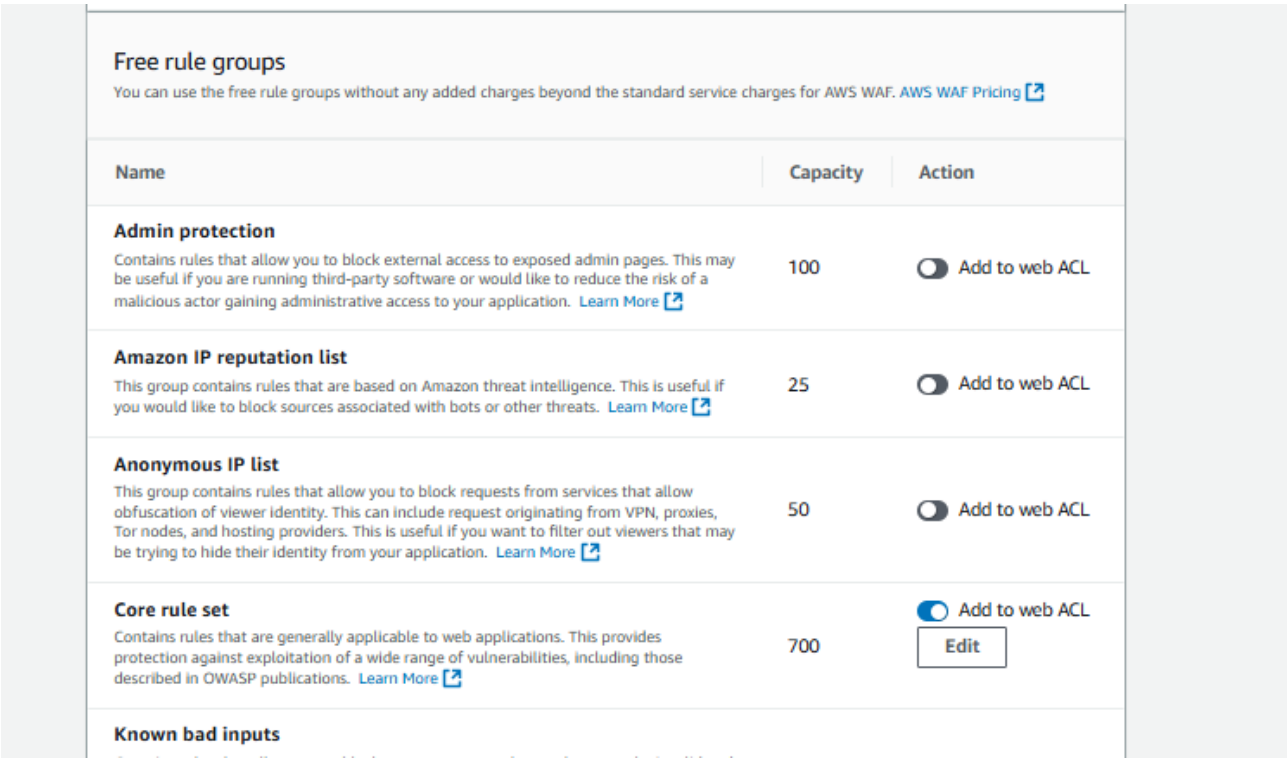


Figura 35: Creazione Web ACL 3

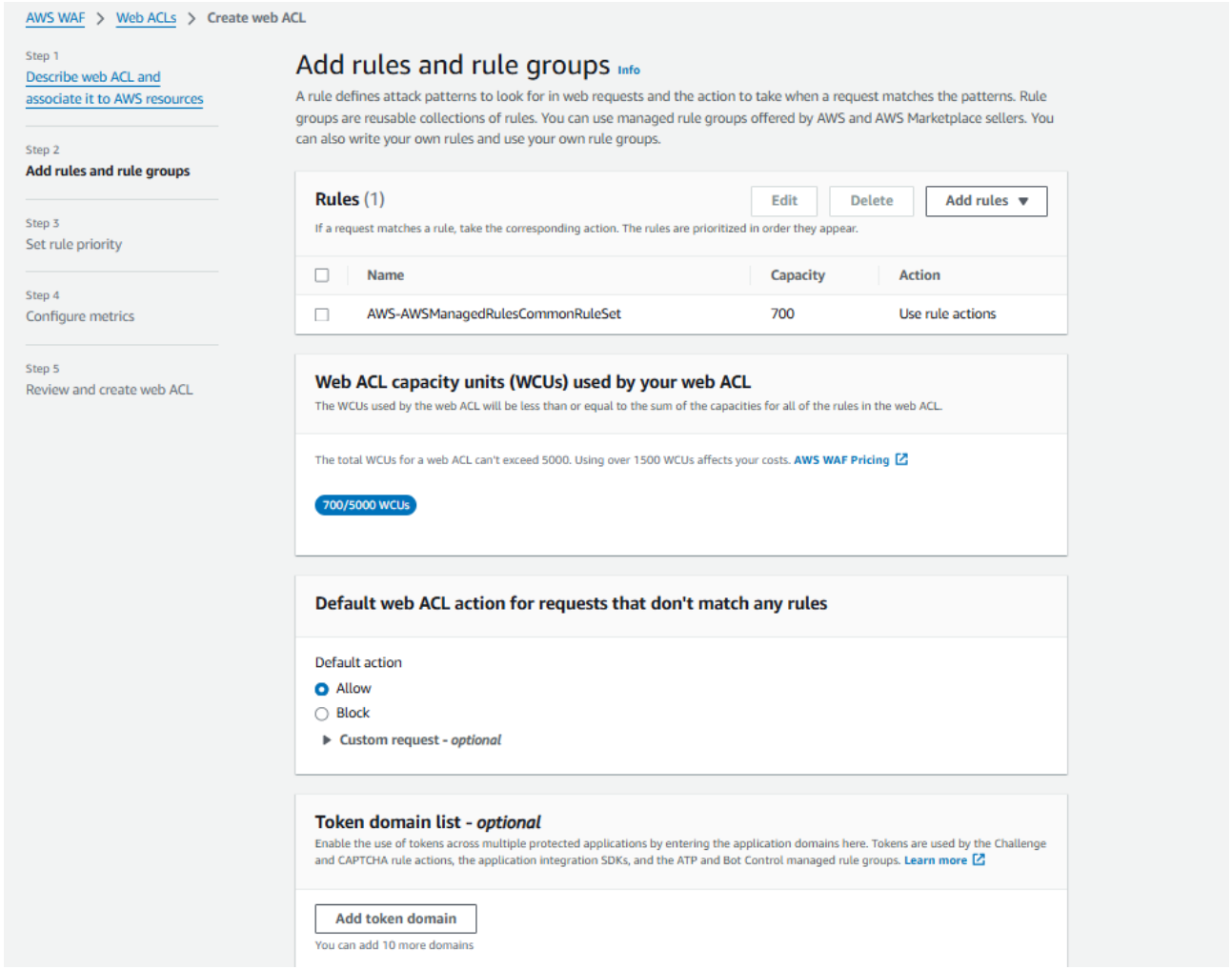


Figura 36: Creazione Web ACL 4

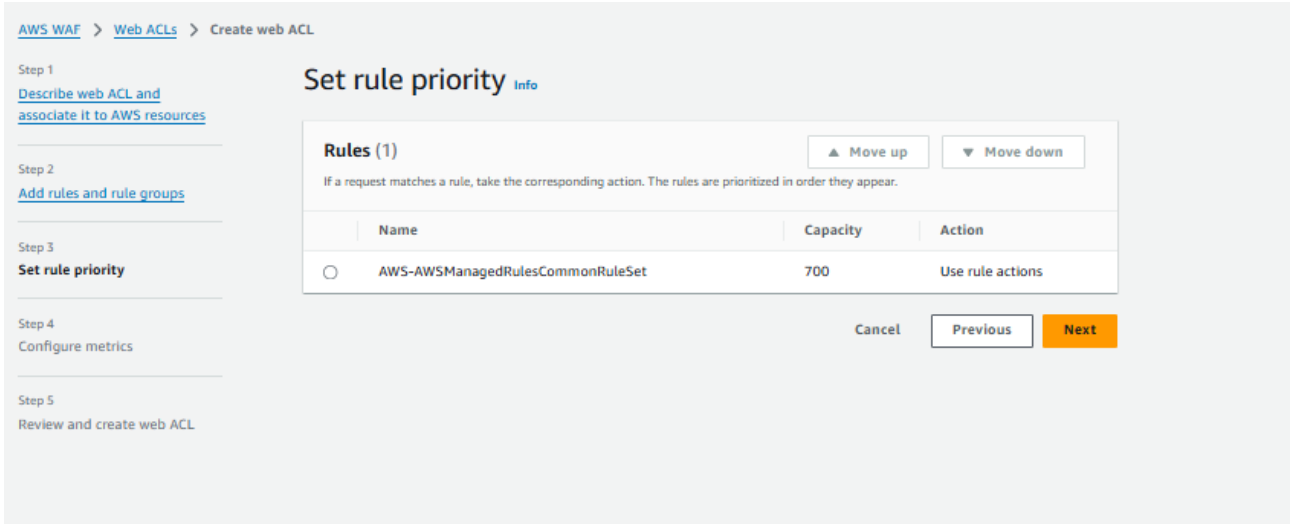


Figura 37: Creazione Web ACL 5

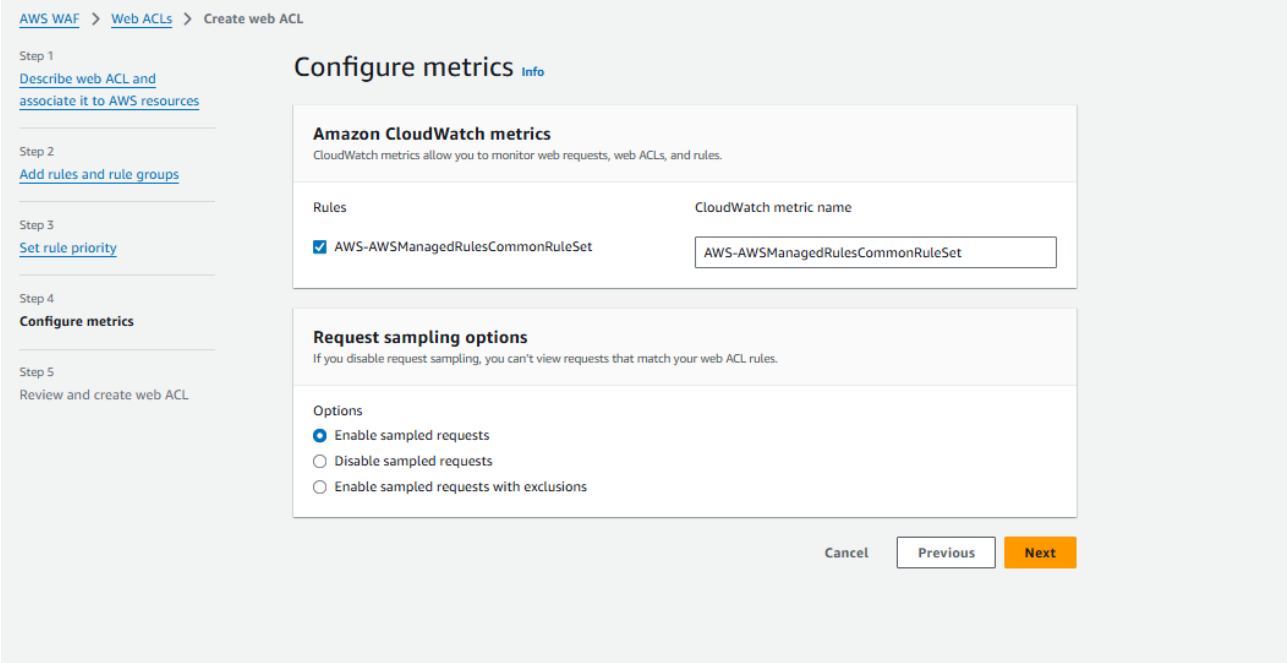


Figura 38: Creazione Web ACL 6

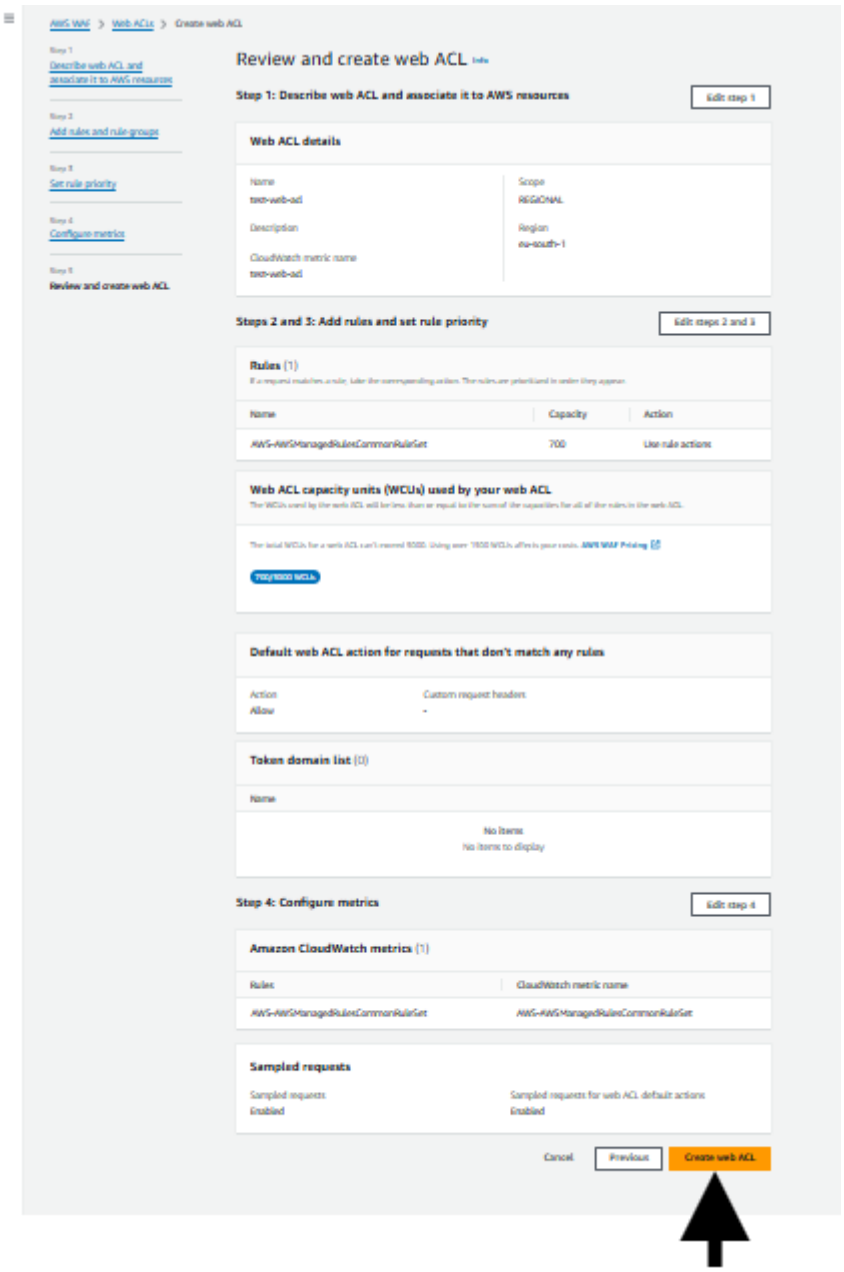


Figura 39: Creazione Web ACL 7

La documentazione ufficiale della gestione delle Web ACL si trova al seguente link: [How AWS WAF works - AWS WAF, AWS Firewall Manager, and AWS Shield Advanced (amazon.com)]

4.1.8 *Gestione Firewall*

Per gestire il Firewall occorre andare nella sezione VPC.

Il Firewall risiede nell'HUB, associato alla VPC Inspection, ed è associato ad un firewall policy.

Il Firewall ha associata una Firewall Policy, che a sua volta è composta da una serie di Rule Groups.

I Rule Groups possono essere Stateless e Stateful. Si sconsiglia l'uso di Rule Group Stateful.

La Firewall Policy per i Rule Groups Stateless deve prevedere il forward verso I Rule Group Stateful.

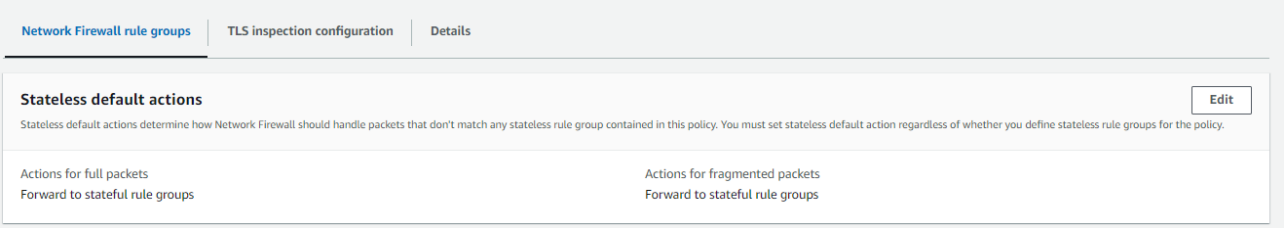


Figura 40: Firewall Policy Stateless

La Firewall Policy per i Rule Groups Stateful, di tipo Strict order e che il default Action è Drop Estabilished.

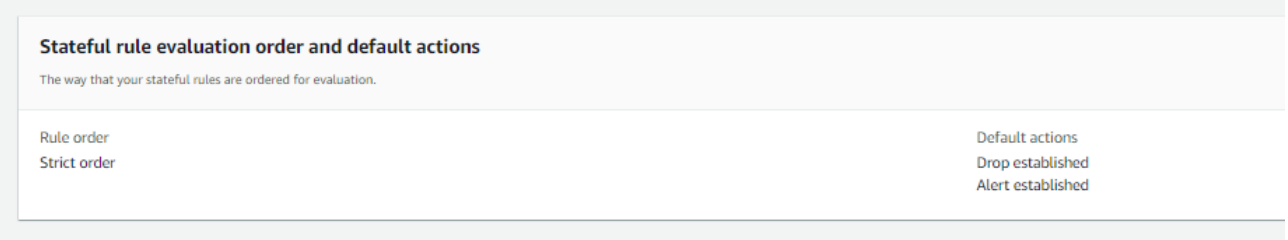


Figura 41: Firewall Policy Stateful

Questo garantisce che per i Rule Group Stateful.:

- la Firewall Policy segua le priorità stabilita dai stateful Rule Groups;
- a priori, le connessioni vengono sempre lasciate passare per riuscire a controllare le connessioni a livello 7; poi vengono droppate se non esiste una policy che le lasci passare.

Alcune osservazioni sulle aperture che si possono fare sugli Stateful rule Groups:

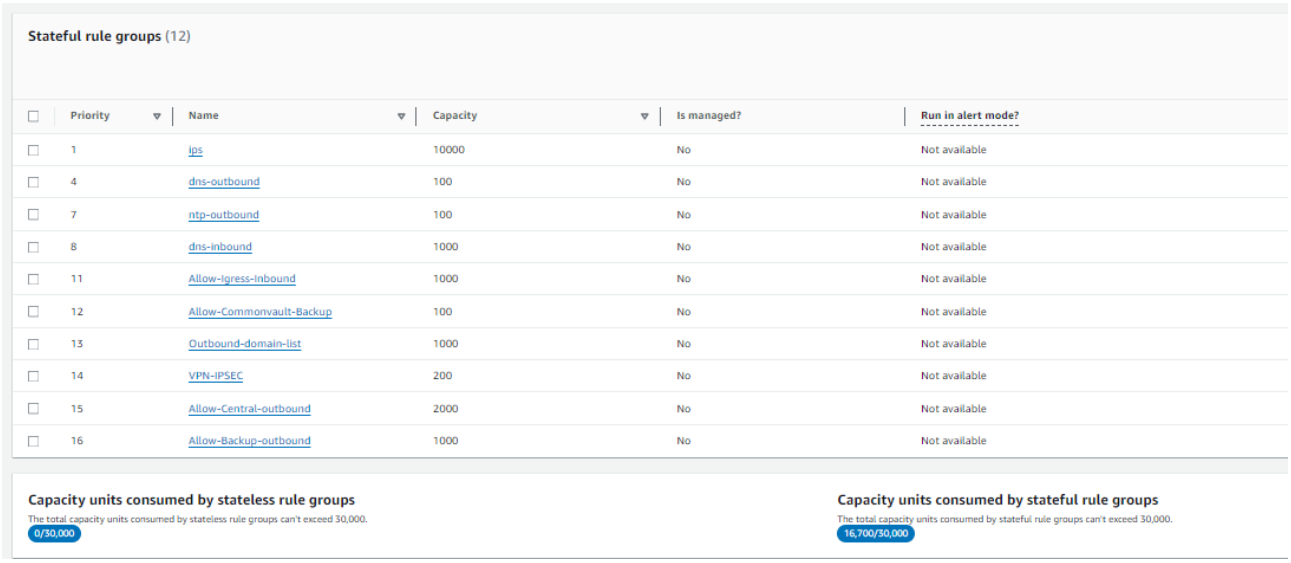
- occorre cercare sempre di usare il tipo di connessione più specifico: ad esempio TLS in luogo di TCP-PORT-443 per permettere l'analisi a livello 7;
- nonostante ci siano le priorità' sulla Stateful Rule Groups, se esistono delle State Rule Groups con Policy a livello 3: ad esempio: Allow, Source-IP 192.168.1.0/24, Destination-IP 192.1682.0/24, Protocollo IP, queste policy vengono comunque eseguite prima delle policy a livello più alto (importante perché potrebbero invalidare policy più specifiche).

Ci possono essere diversi tipo di Stateful Rule Groups: managed e un managed.
Le AWS managed Stateful Rule Groups sono gestite da AWS e possono essere aggiunte alla Firewall Policy.

Per quando riguarda le Unmanaged Stateful Rule Gruops esistono vari tipi:

- Standard – Usate per le regole IP
- Domain List – Per elencare domini FQDN
- Suricata compatible rule list – Per definire regole IDS/IPS

In fase di creazione di ogni Rule Gruops viene chiesto quante regole al massimo potrà contenere (da 1 a 30000).
Da notare che il numero di regole massimo di ciascun Unmanaged Rule Gruops non può essere cambiato, e che la Firewall Policy può avere una capacità massima potenziale di 30000 policy Stateful e 30000 Stateless.



Stateful rule groups (12)

Priority	Name	Capacity	Is managed?	Run in alert mode?
1	ips	10000	No	Not available
4	dns-outbound	100	No	Not available
7	ntp-outbound	100	No	Not available
8	dns-inbound	1000	No	Not available
11	Allow-Igress-Inbound	1000	No	Not available
12	Allow-Commonvault-Backup	100	No	Not available
13	Outbound-domain-list	1000	No	Not available
14	VPN-IPSEC	200	No	Not available
15	Allow-Central-outbound	2000	No	Not available
16	Allow-Backup-outbound	1000	No	Not available

Capacity units consumed by stateless rule groups
The total capacity units consumed by stateless rule groups can't exceed 30,000.
0/30,000

Capacity units consumed by stateful rule groups
The total capacity units consumed by stateful rule groups can't exceed 30,000.
16,700/30,000

Figura 42: Firewall Policy Capacity

Di seguito un esempio di Stateful Rule Gruops Standard:

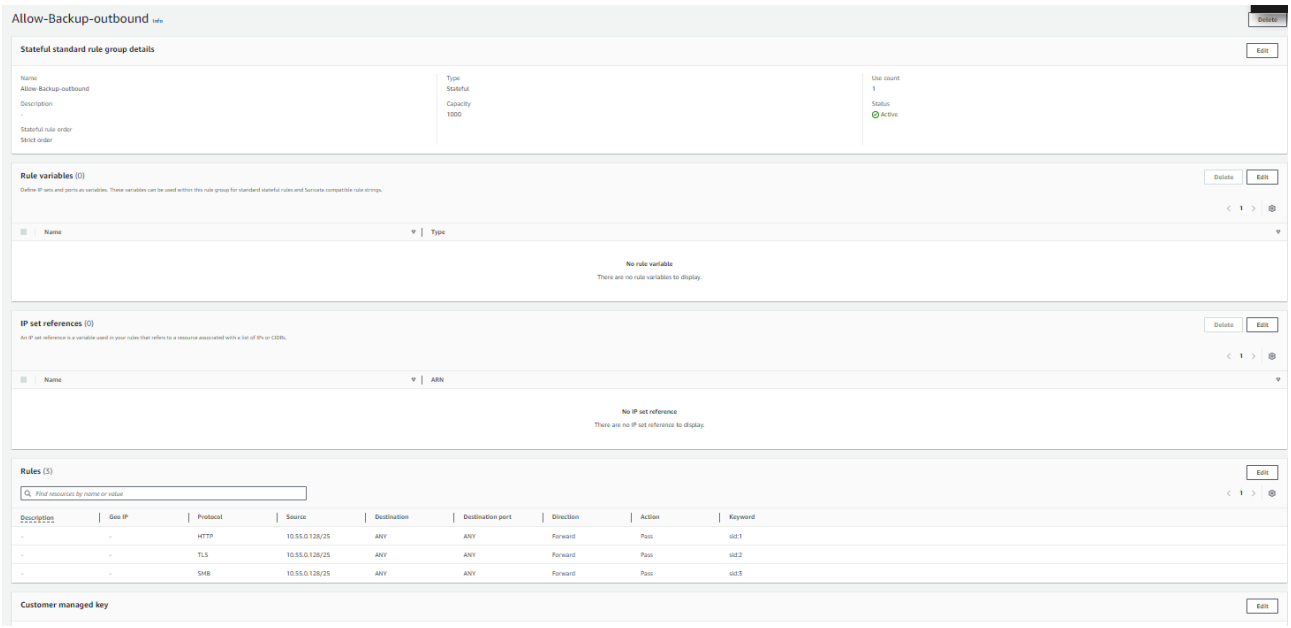


Figura 43: Stateful Standard Rule Group

Di seguito un esempio Di Stateful Rule Gruops Domain list:

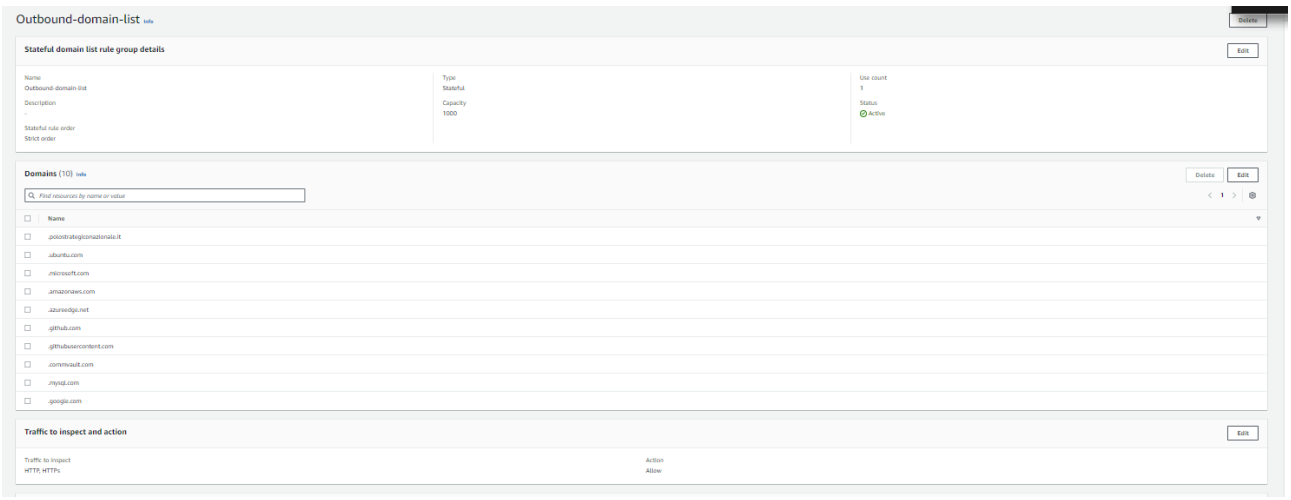


Figura 44: Stateful Domain List Rule Group

Di seguito un esempio Suricata compatible rule list:

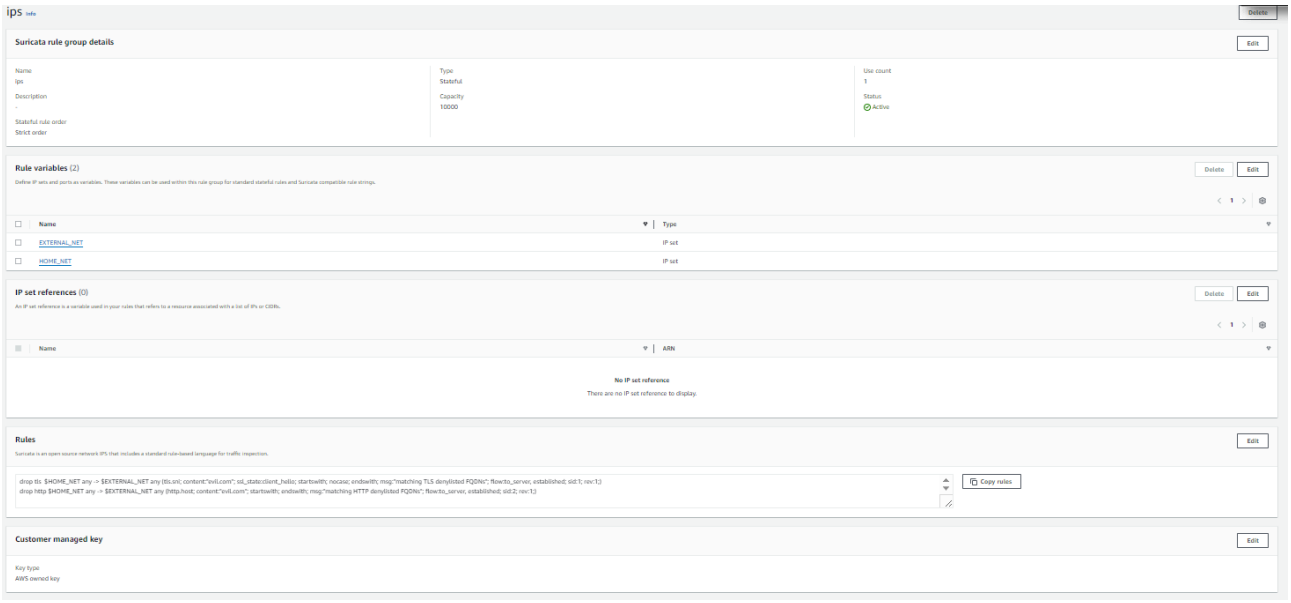


Figura 45: Stateful Suricata Rule Group

La documentazione ufficiale della gestione Firewall si trova al seguente link:
[Firewalls in AWS Network Firewall - AWS Network Firewall (amazon.com)]

4.1.9 Session Manager

L'accesso amministrativo alle VM presenti negli Spoke è garantito dalla soluzione attraverso l'utilizzo di Session Manager.

Per usufruire del Servizio di Session Manager la VM deve avere uno specifico ruolo agganciato:

- Si aprirà una nuova finestra con l'accesso alla VM
- di seguito un esempio: all'interno di uno Spoke account, selezionare il servizio EC2

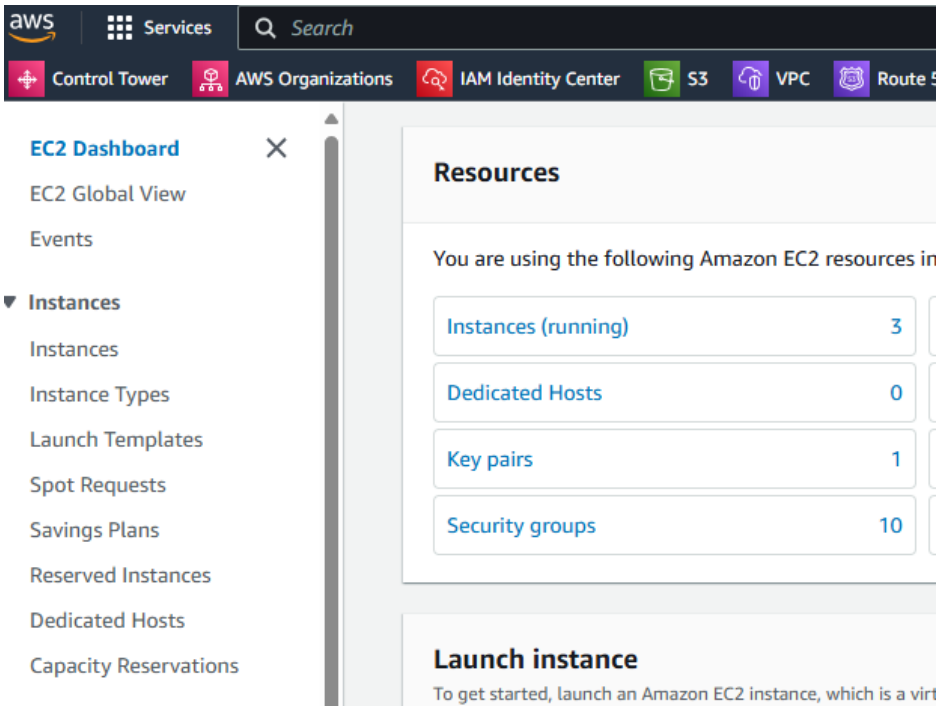


Figura 46: Session Manager 1

- Selezionare Instances (running) è una lista delle istanze attualmente in esecuzione:
- Selezionare una macchina specifica e premere sul bottone in alto a destra “Connect”

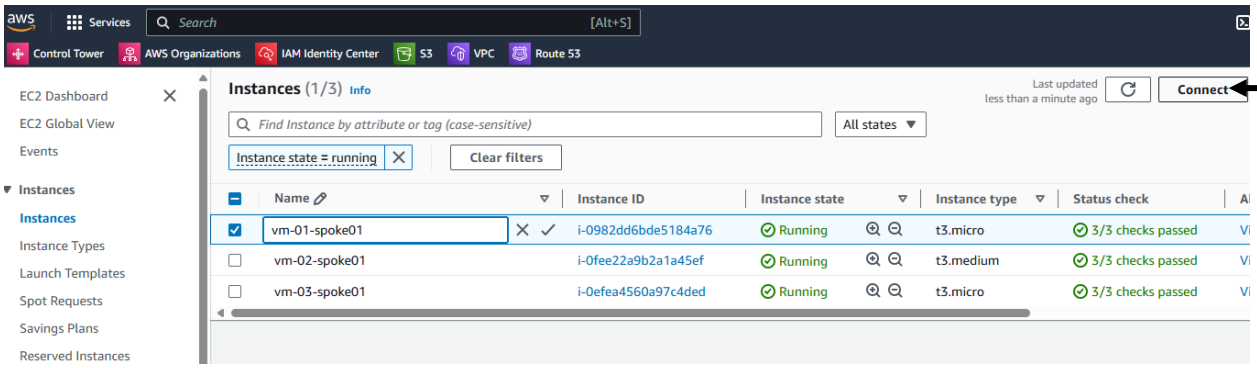


Figura 47: Session Manager 2

- Selezionare Session Manager e premere su connect:

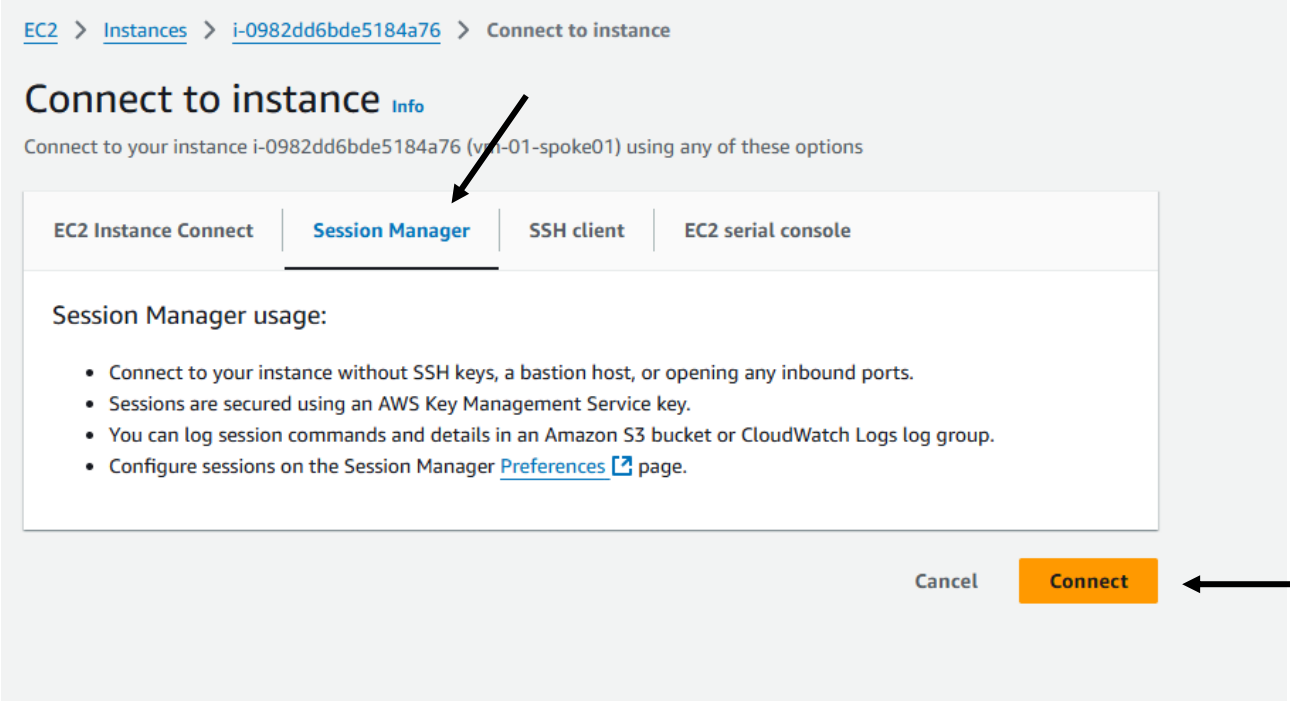


Figura 48: Session Manager 3

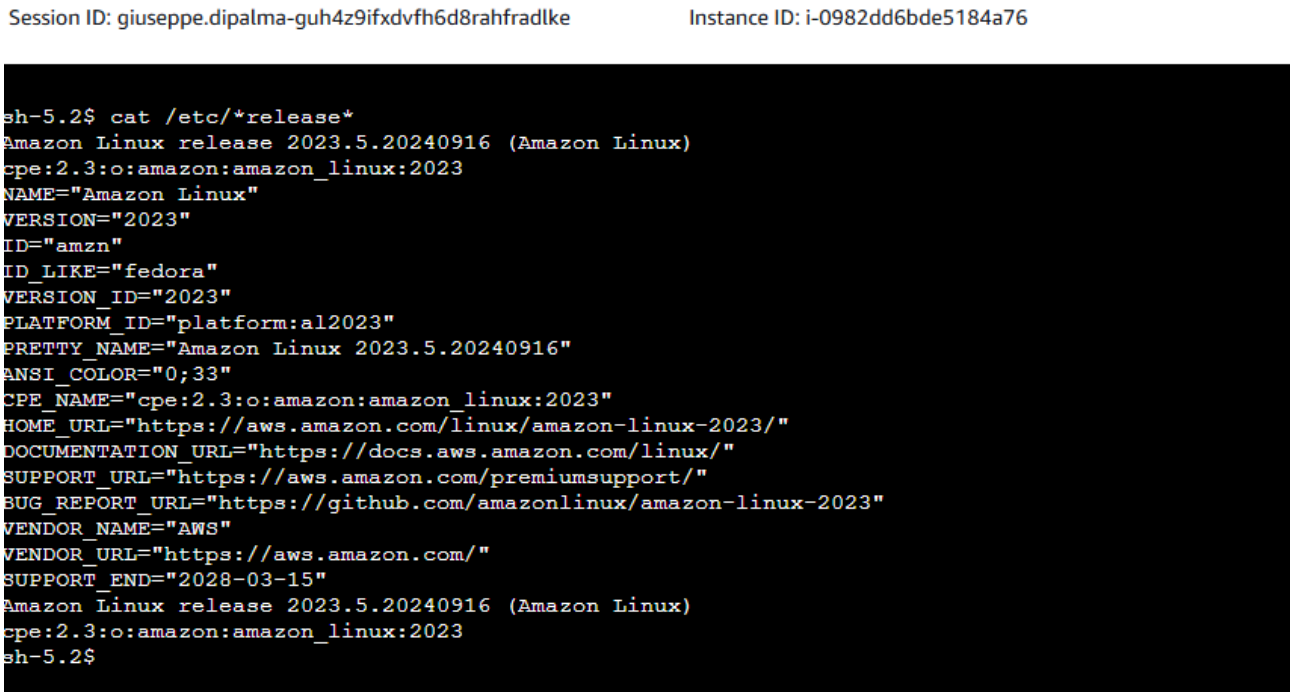


Figura 49: Session Manager 4

Per le macchine Windows Server invece, il session manager è sempre disponibile, permettendo l'accesso (con gli stessi step indicati in precedenza) alla console di gestione a riga di comando:

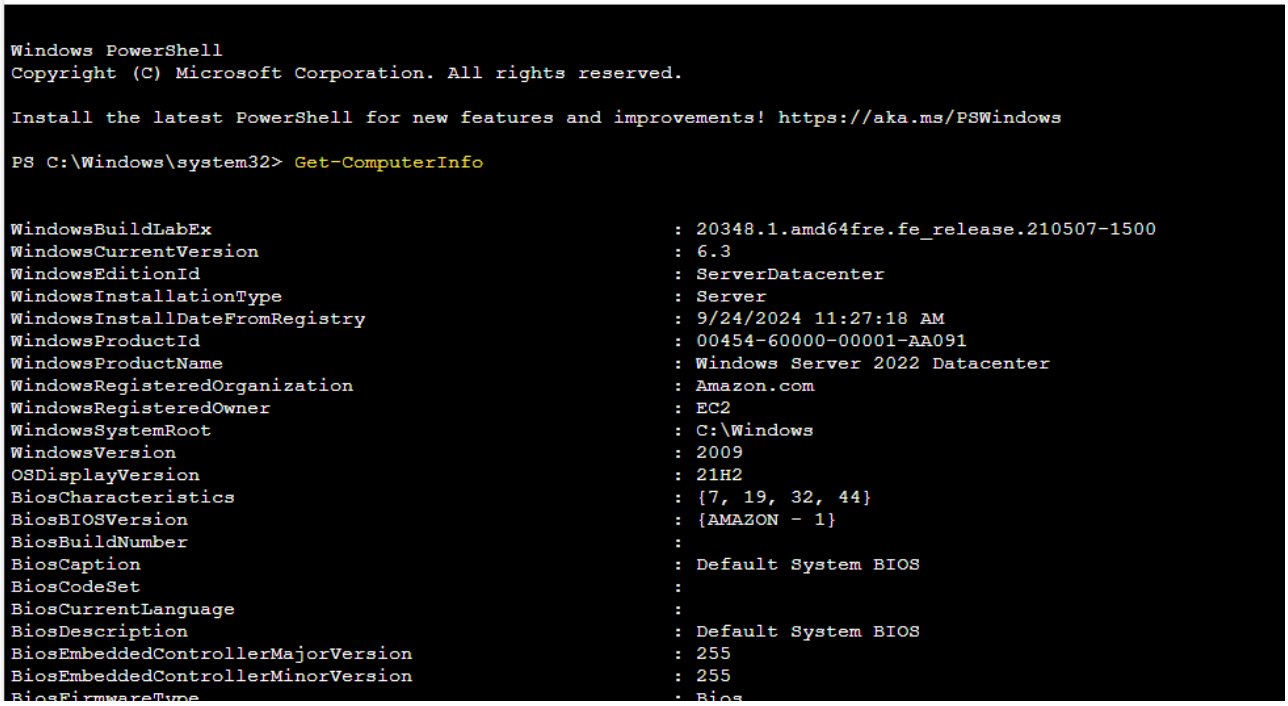


Figura 50: Session Manager 5

Oppure in alternativa per visualizzare la GUI di Windows:

Si usano features di AWS System Manager, denominate fleet manager:

- Selezionare l'istanza dalla lista delle istanze
- Premere il tasto in alto a destra "connect"
- Selezionare RDP client e successivamente "Fleet Manager Remote Desktop"

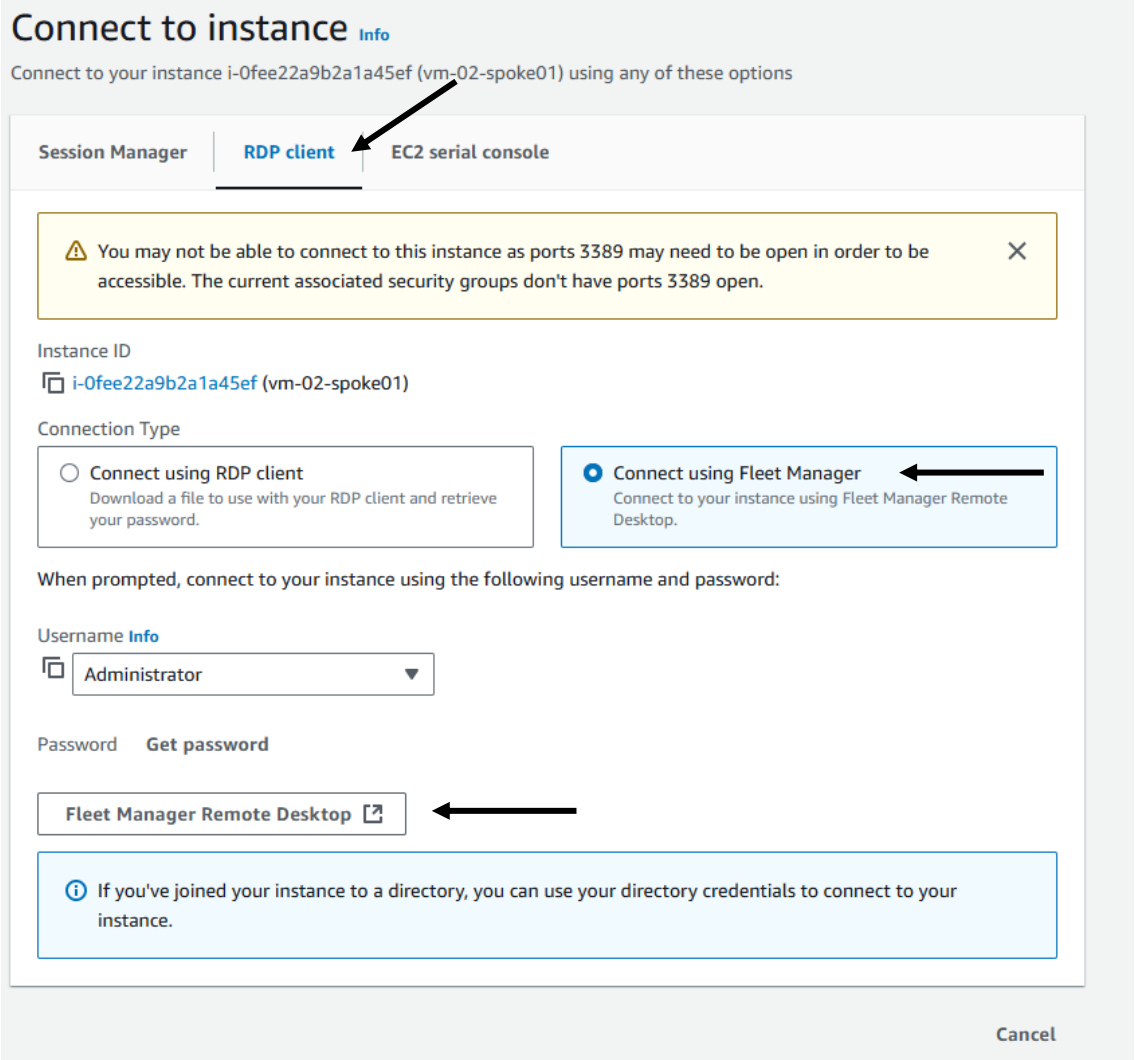


Figura 51: Session Manager 6

Scegliere il metodo di autenticazione adeguato:

- User Credentials: sono le credenziali disponibili per le utenze sul Sistema Operativo o di un eventuale dominio configurato; può essere anche l'utenza di "Administrator". Per la password di utenza di Administrator è possibile fare il retrive utilizzando la chiave pem associata alla macchina;
- Key Pair: è la chiave scelta e scaricata (o configurata) in fase di provisioning della macchina;
- Single Sign-On: sono credenziali della sessione AWS; in pratica sono le credenziali usate per accedere alla console AWS: se queste ultime hanno sufficienti privilegi sarà permesso l'accesso.

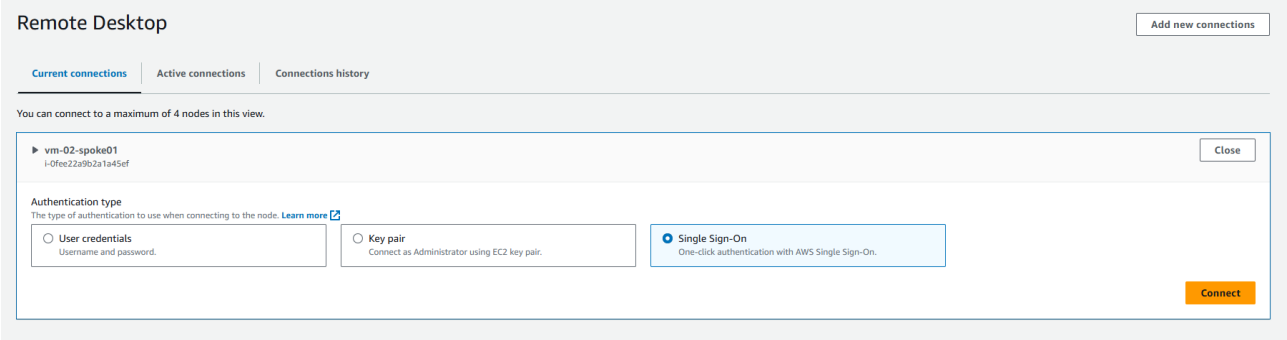


Figura 52: Session Manager 7

Di seguito la visualizzazione finale:

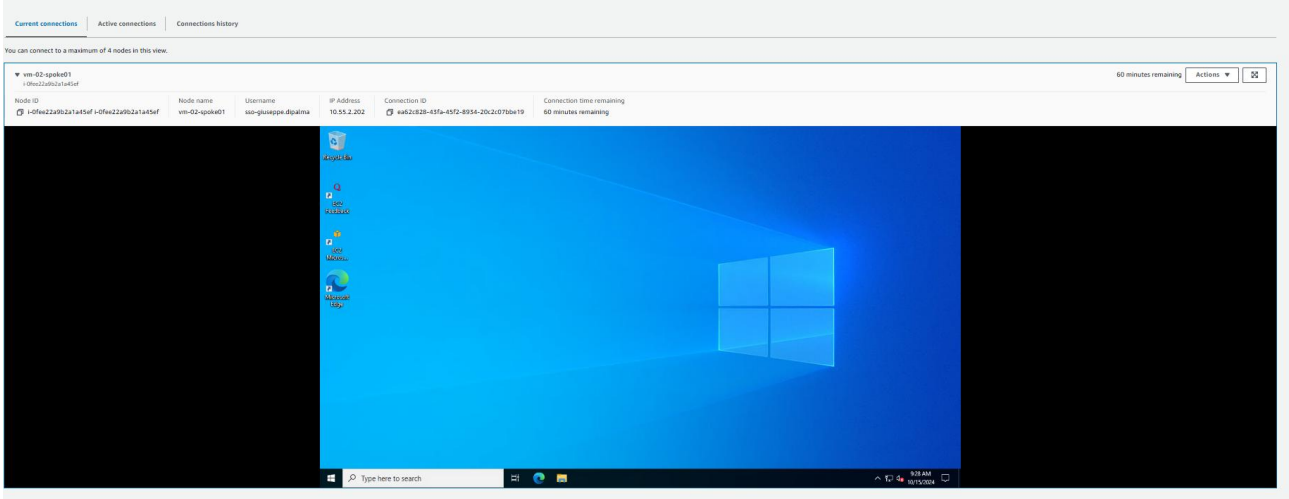


Figura 53: Session Manager 8

Per la documentazione relativa al servizio AWS Session Manager:
[AWS Systems Manager Session Manager - AWS Systems Manager (amazon.com)]

4.1.10 *Esposizione Web server con WAF*

Per esporre un Web Server su Internet servono:

- almeno un Web Server sulla VPC dello Spoke;
- un Network Load Balancer di tipo Internal sulla VPN dello Spoke che punti ai Web Server, con relativo Target Group di tipo EC2;
- Application Load Balancer ti tipo Internet Facing sulla VPC Igress, sulle Subnet Public, che punti agli IP esposti dal Network Load Balancer dello Spoke, Target Group di tipo IP;
- un Security Group da associare all'Application Load Balancer;
- una Web Acl da associare al Application Load Balancer;
- un Certificato SSL da associare al Listener HTTPS;

- policy sul Firewall che consenta il traffico, dalle Subnet Public della VPC Igress, verso gli IP esposti dal Network Load Balancer dello Spoke.

L'utilizzo del Network Load Balancer di tipo Internal sulla VPN dello Spoke che punti ai Web Server si rende necessario, perché gli IP address del Web server potrebbero variare in certe condizioni, mentre non è così per gli IP address esposti dal Network Load Balancer.

Nello schema qui riportato si rappresenta un esempio di traffico di esposizione:

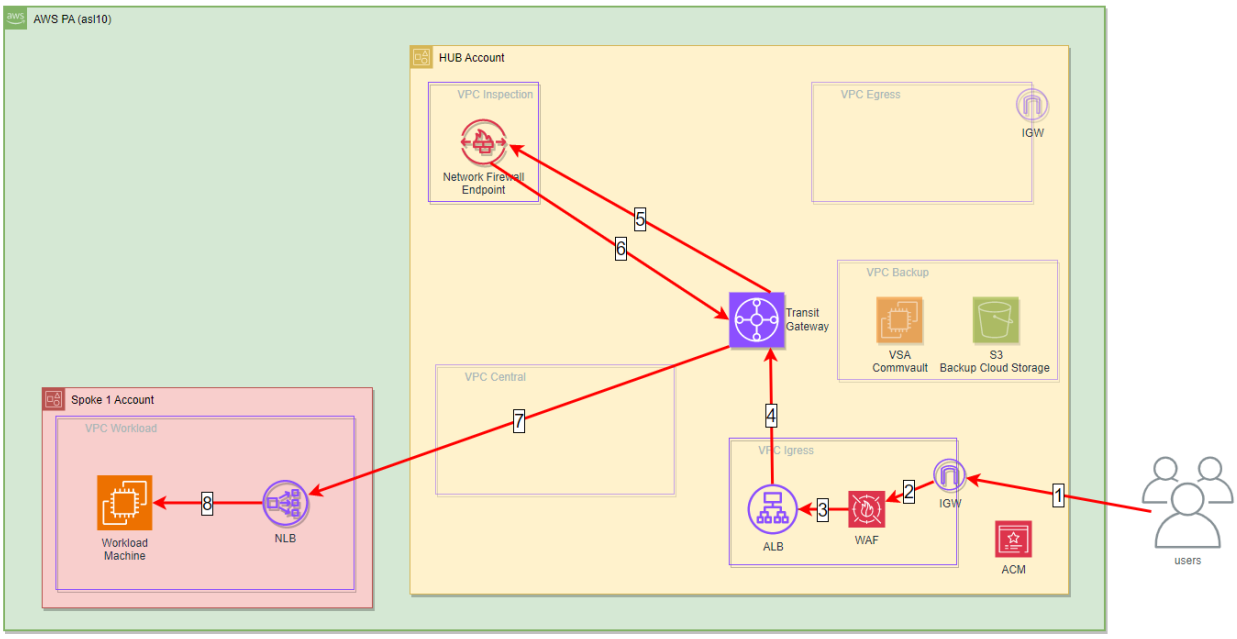


Figura 54: Esposizione Web Server 1

Di seguito un esempio di creazione di un Application Load Balancer per l'esposizione.
Perla creazione di un Application Load Balancer ci si deve portare nella Sezione EC2.

Per creare un Application Load Balancer per l'esposizione occorre specificare almeno quanto indicato in calce:

- Nome
- Tipo Internet Facing
- Tipo di IP Address: IPv4, IPv6 o entrambi
- VPC: Igress
- Network Mapping: scegliere tutte le zone disponibili e la Subnet Public
- Security Group: che consenta l'accesso alle porte esposte da qualunque IP
- Listener HTTP, HTTPS
  Associare porta e Target Group
- Certificato SSL per il Listener HTTPS
- Aggiungere la Network Integration AWS Web Application Firewall (WAF)

Una volta creato l'Application Load Balancer andare a modificare la Regola di Esposizione HTTP, se presente, per fare il Redirect su HTTPS:

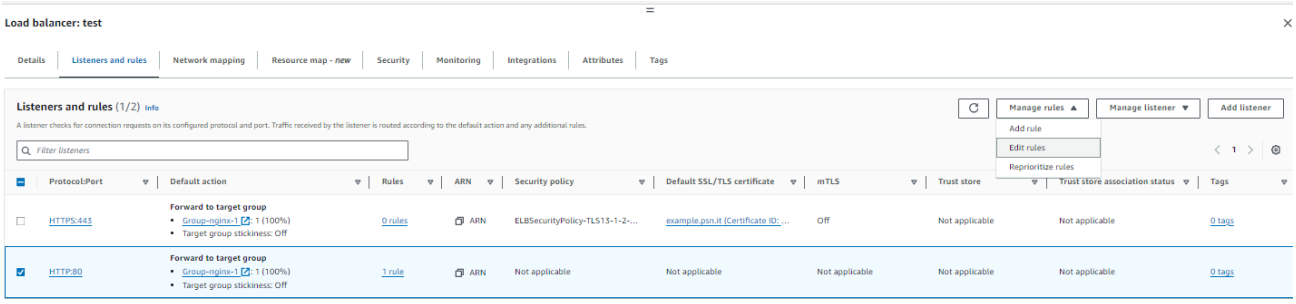


Figura 55: Esposizione Web Server 2

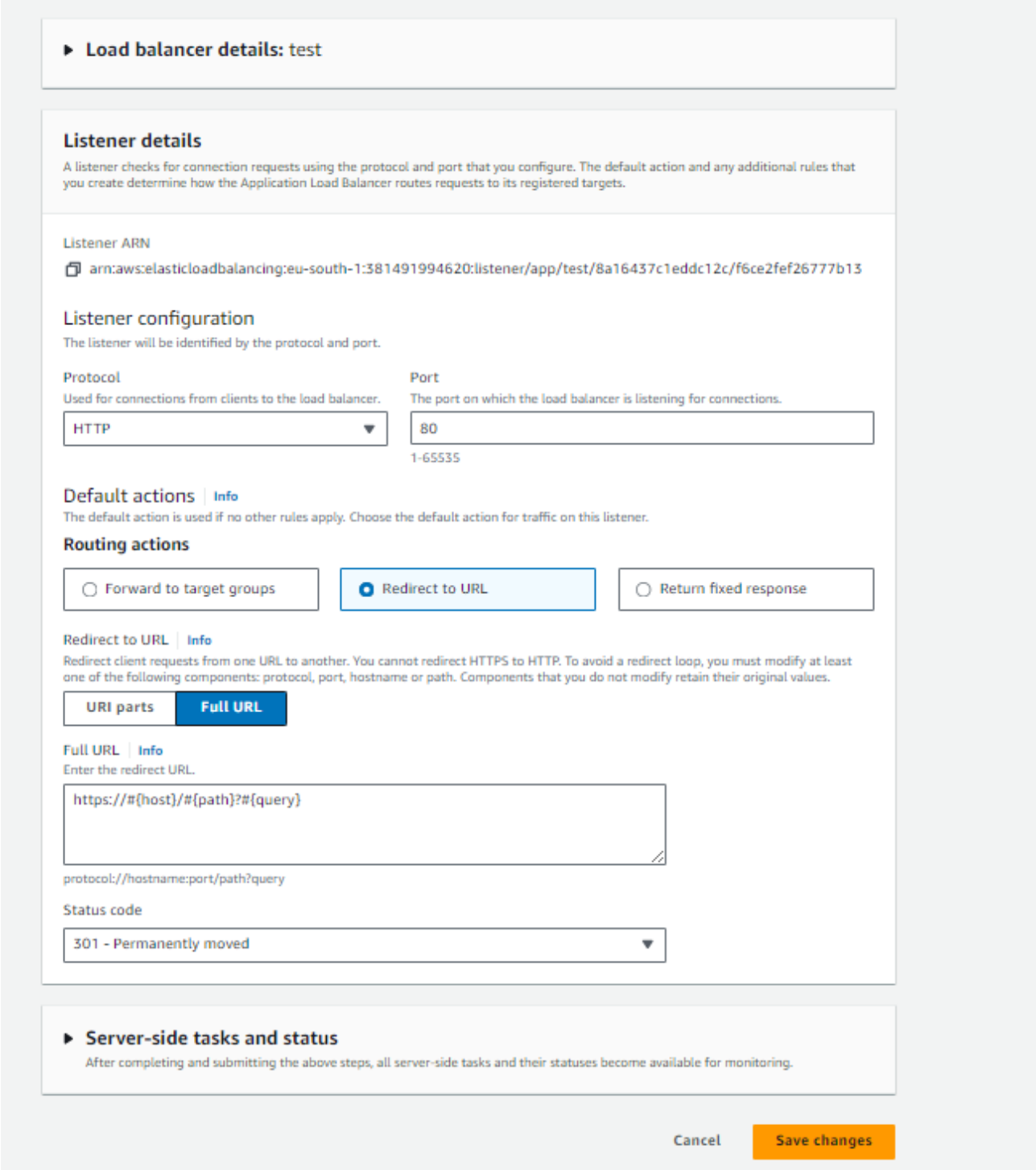


Figura 56: Esposizione Web Server 3

Di seguito il risultato atteso:

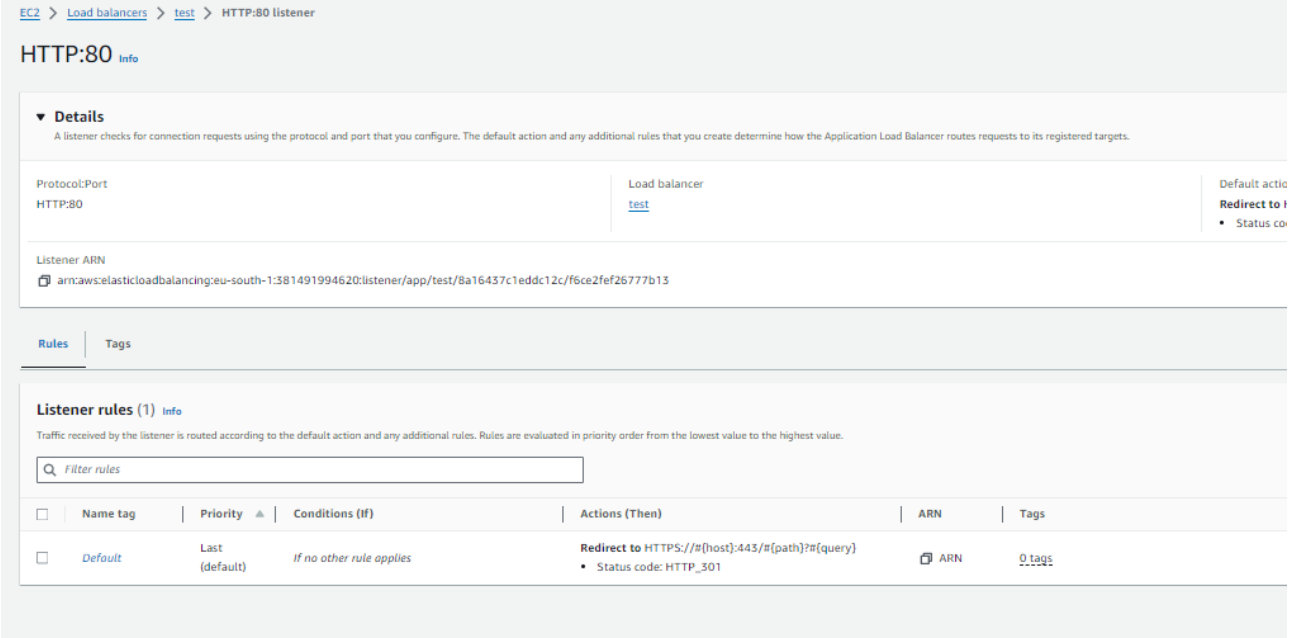


Figura 57: Esposizione Web Server 4

Il Load Balancer pubblica anche un FQDN dal quale si possono dedurre gli IP pubblici che sono stati creati:

Figura 58: Esposizione Web Server 5

C:\Users> nslookup test-1593571687.eu-south-1.elb.amazonaws.com 8.8.8.8
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: test-1593571687.eu-south-1.elb.amazonaws.com
Addresses: 15.161.202.197
          18.102.179.150

4.1.11 Consultazione Log

I log sono consultabili nella Sezione CloudWatch.

All'interno di Log Group si trovano i log:

- fw-log con i log del Firewall di traffico
- ips-log con i log del Firewall di IPD/IPS
- aws-waf-logs-PA con i log del WAF

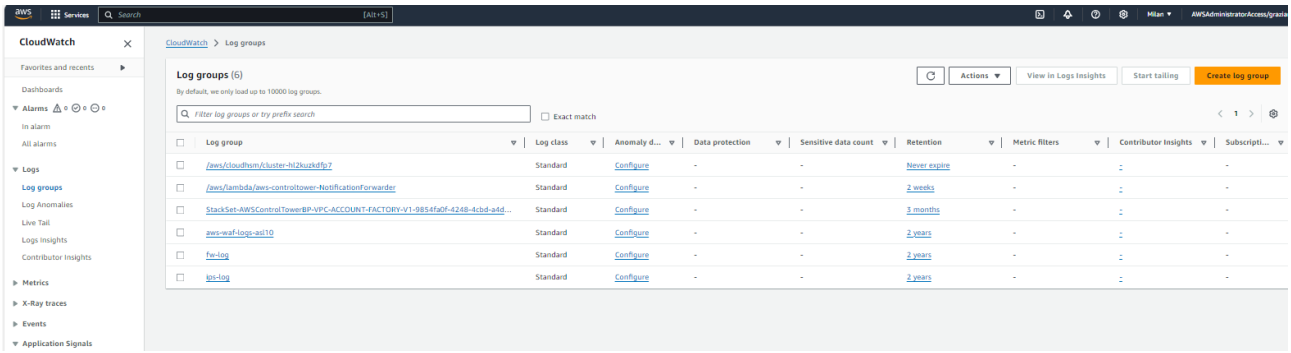


Figura 59: Log Group

5 Backup PSN SPC

5.1.1 *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 Secure Public 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 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.

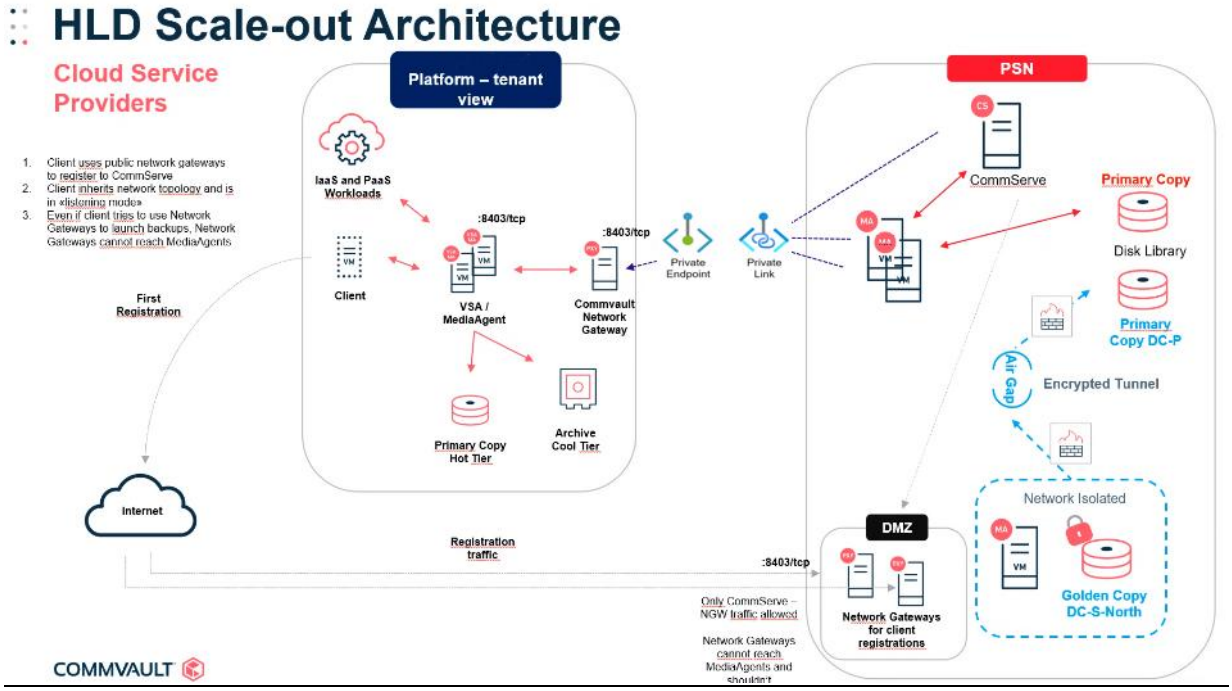


Figura 60: HLD Commvault

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.

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 AWS 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 AWS avviene sfruttando la tecnologia Private Service Connect.

Nel dettaglio, l'infrastruttura on-premises del PSN raggiunge la PSN ORG su AWS attraverso una VPN.
Da questo tenant vengono creati tanti flussi Private Link – Private EndPoint quante sono le Org delle PA.
I flussi Private Endpoint e Private Link sono interni al backend di AWS. Con la soluzione AWS di Private Link / Private EndPoint il CommServe può comunicare con il Network Gateway all'interno delle PA.
Nell'esempio, per comodità, i ruoli di NG, MA e AN sono eseguiti da una singola VM.

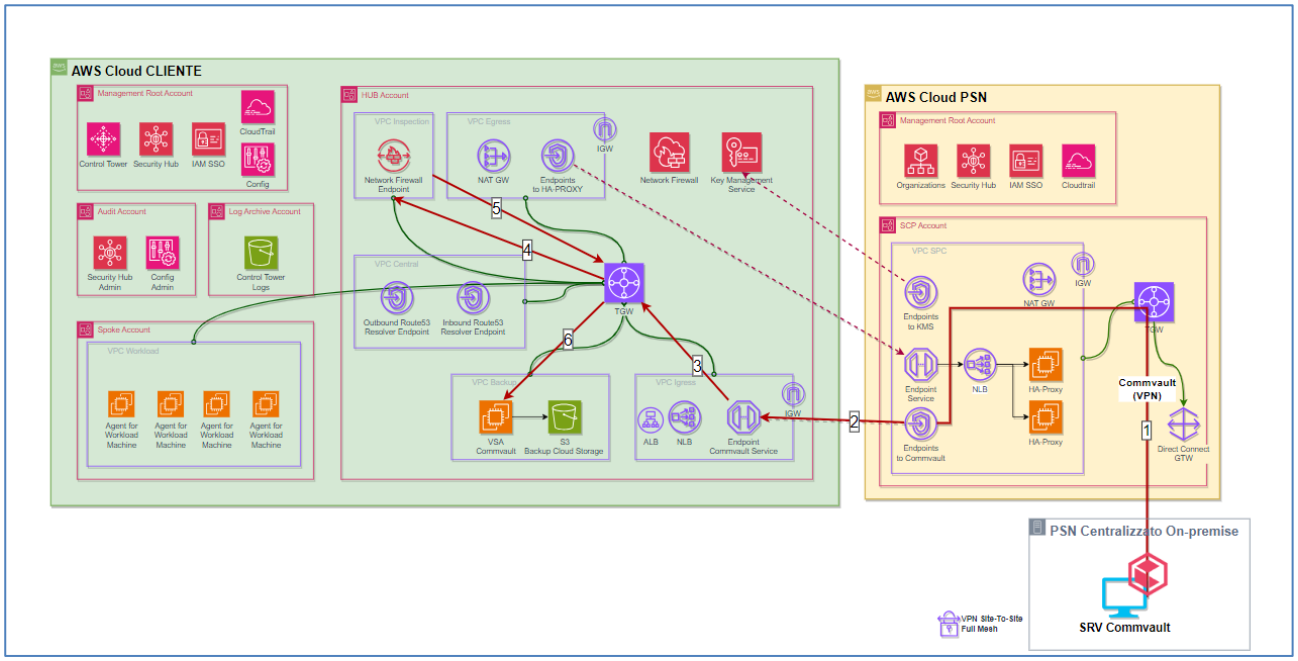


Figura 61: Dettaglio Flussi

Il flusso Private Link / Private Endpoint è unidirezionale: parte dal CommServe on-prem e arriva alla VSA su AWS.
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 sul tenant 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 flusso Endpoint / EndPoint Service.

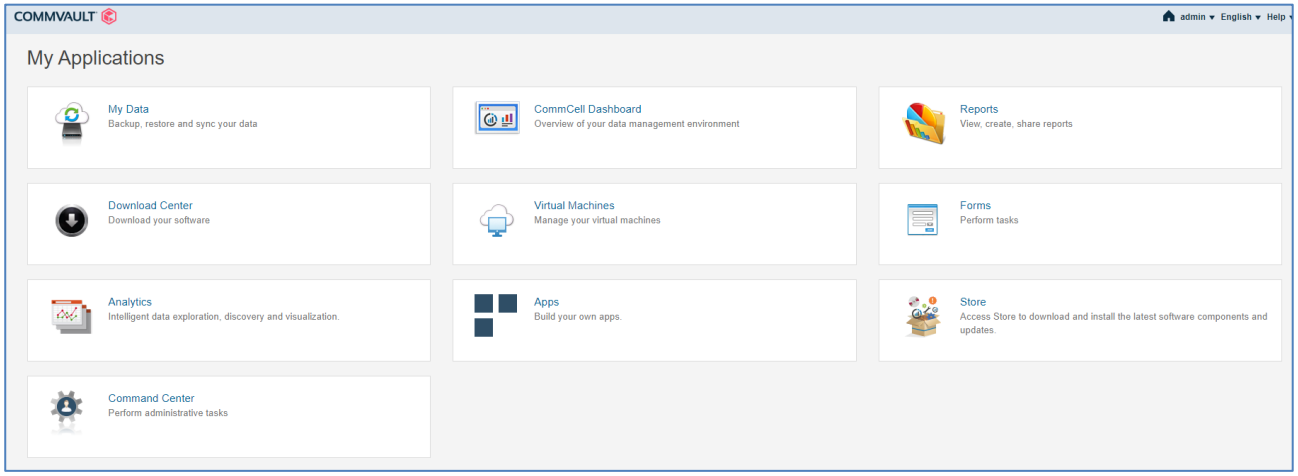
Il server CommServe ha anche il ruolo di Commvault Web Console: un portale web console dove le PA possono fare, in modalità self-service, tutte le operazioni necessarie come backup, restore.

5.1.2 Struttura del Portale: Dashboard

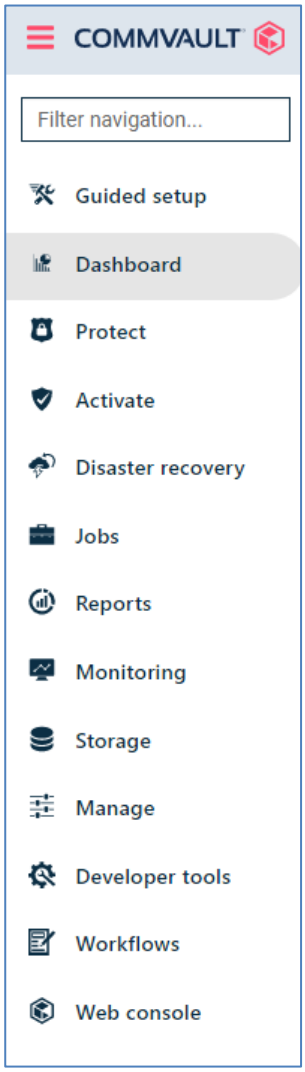
La PA si collega al portale di gestione del backup Commvault attraverso l'URL di accesso a disposizione delle PA:
https: //baas-nord.console.polostrategiconazionale.it

Il login avviene 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 il login vengono visualizzate tutte le applicazioni disponibili all'utente.



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

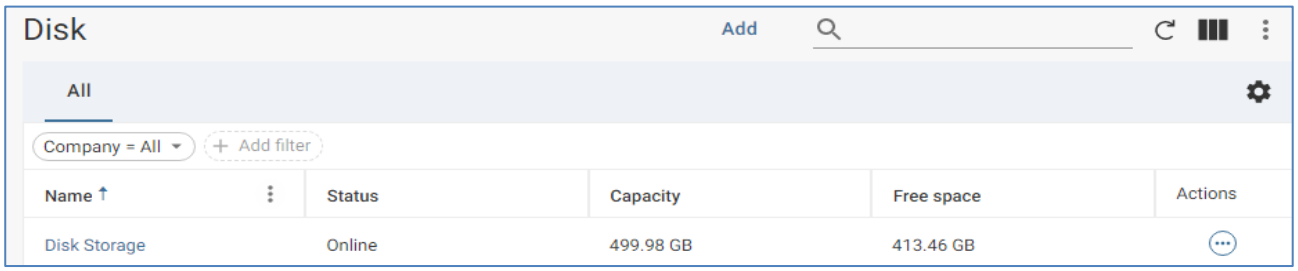


Ogni voce del menu attiva funzionalità o sottomenu aggiuntivi. Nei capitoli seguenti sono indicati i dettagli dei menu.
Per alcune risorse sono preconfigurati oggetti in fase di onboarding mentre su altre la PA avrà la possibilità di definirne di nuove.

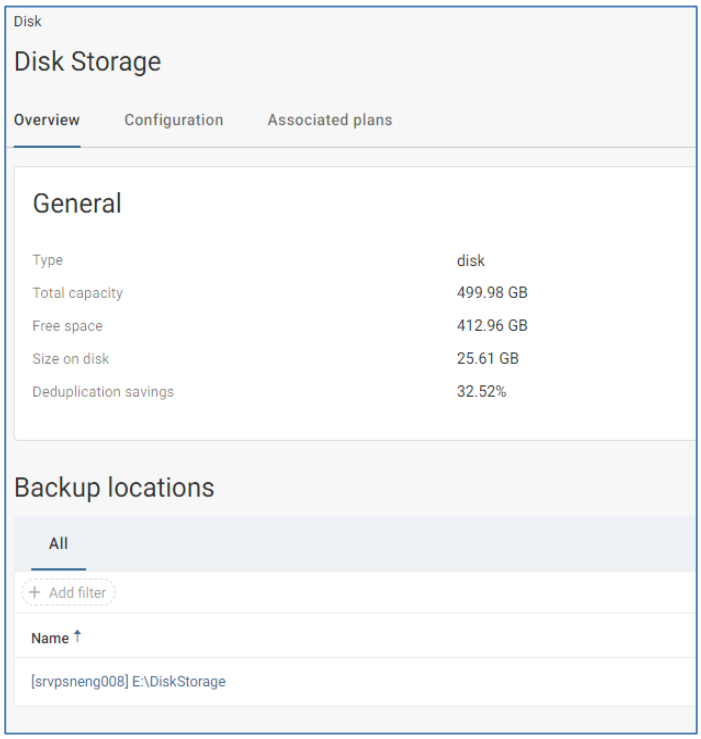
5.1.3 Storage

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.

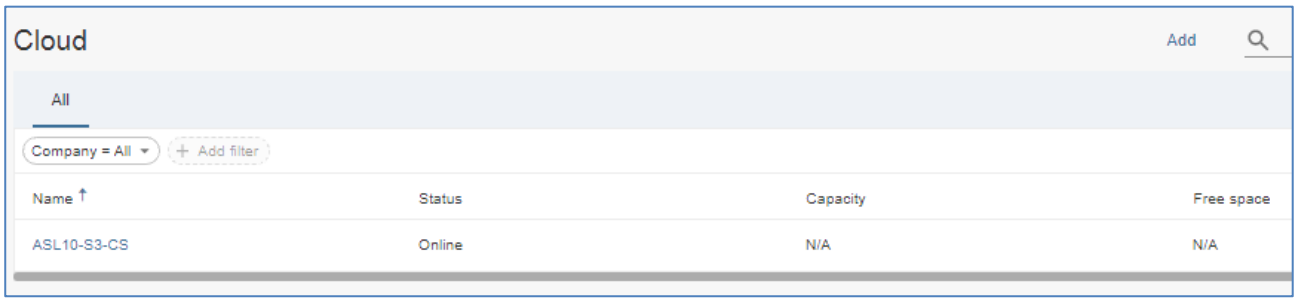
Lo storage di tipo Disk indica lo spazio disco On Premesis presso il datacenter PSN. Verrà poi utilizzato dai Plan che prevedono la replica del dato.



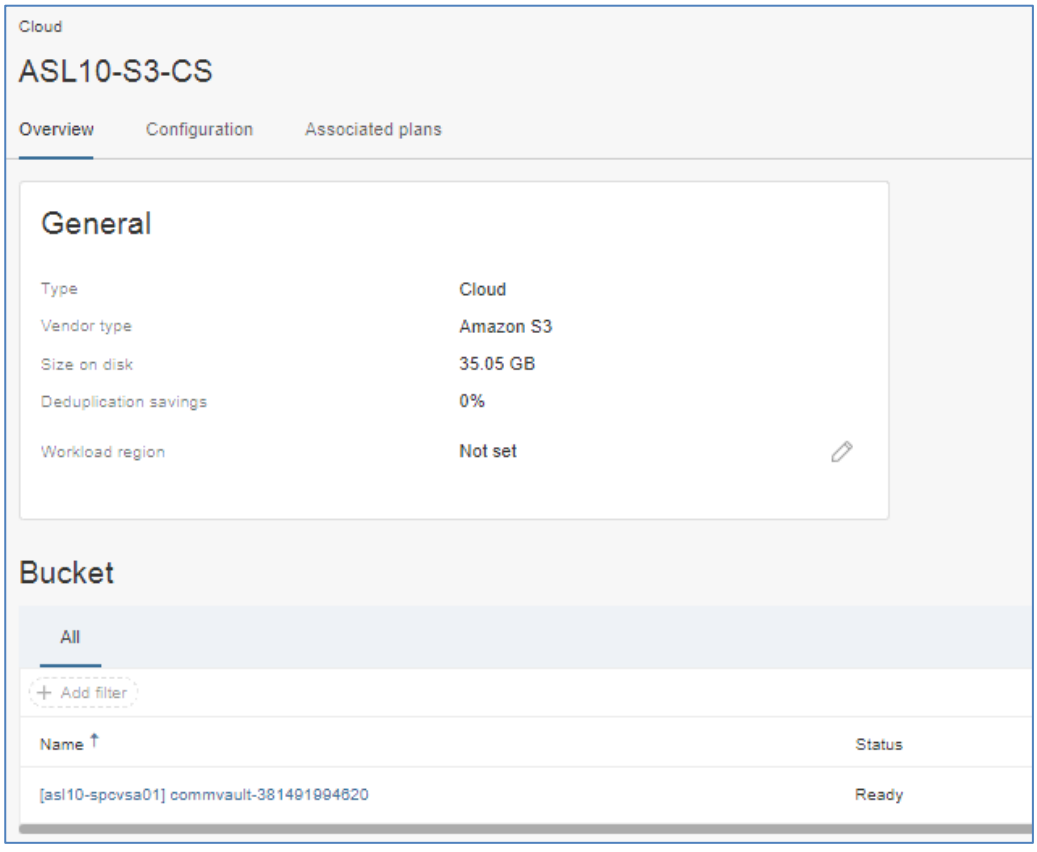
Il disk storage è situato presso il DC di PSN e risiede su uno storage di backend.



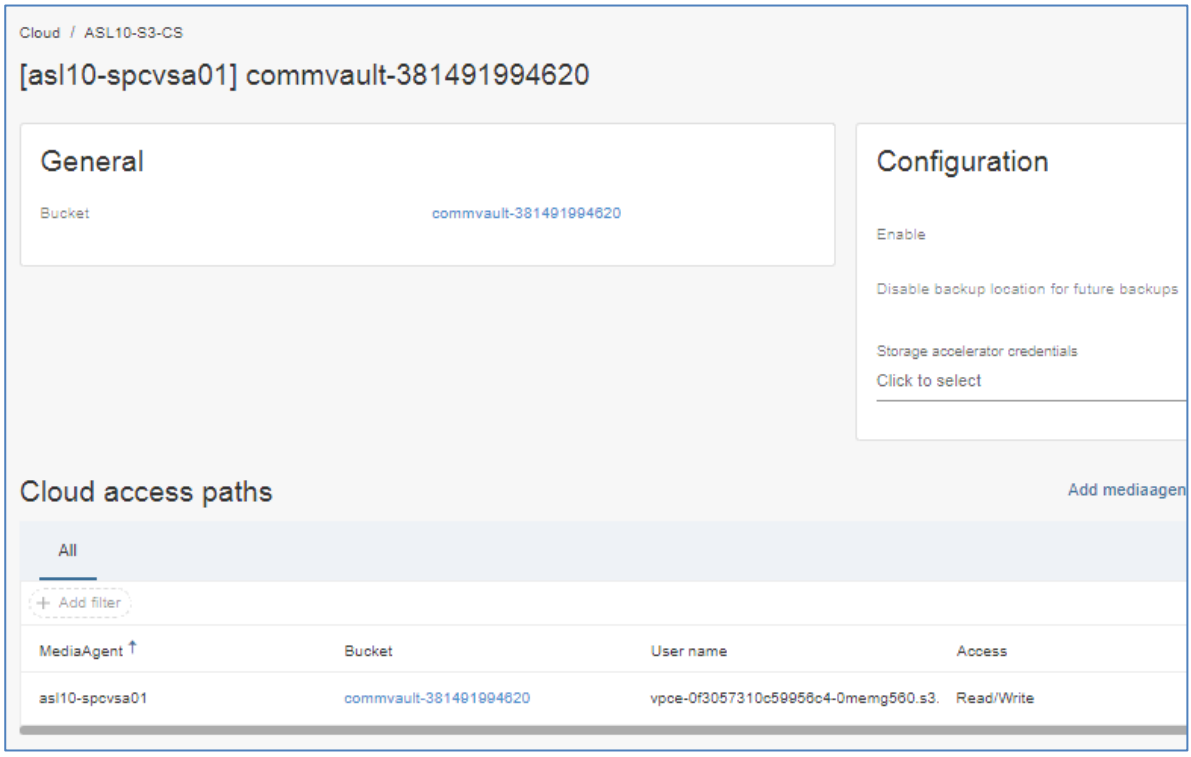
Lo storage di tipo cloud è un S3 AWS definito sul tenant della PA:



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



Su AWS S3 viene definito un Bucket gestito dal VSA.



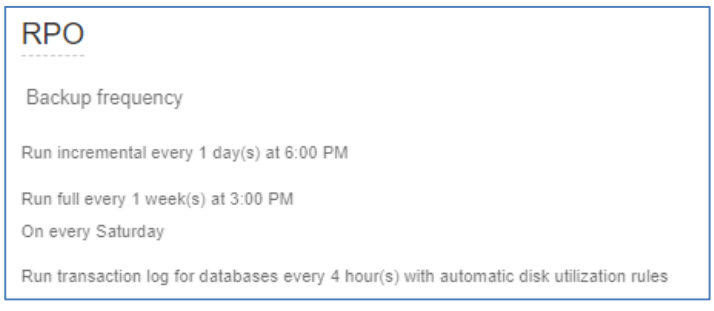
Il VSA utilizzerà le API AWS per accedere al bucket per memorizzare i backup.
Per la parte storage la PA non dovrà eseguire modifiche.

5.1.4 Plan

I Plan sono preconfigurati in 14 configurazioni con retention variabile tra 7 giorni e 10 anni. Per ogni retention disponibile è possibile indicare se si vuole attivare la sovranità del dato, portando una seconda copia su datacenter on-prem del PSN

In caso di necessità è possibile richiedere, attraverso il servizio di ticketing dedicato del PSN , ulteriori Plan.

Il RPO è impostato a 24 ore attraverso un backup incrementale giornaliero alle 18.00 con Full settimanale alle 15 del Sabato:



Anche in questo caso sono possibili modifiche attraverso apertura ticket del servizio di ticketing dedicato del PSN .

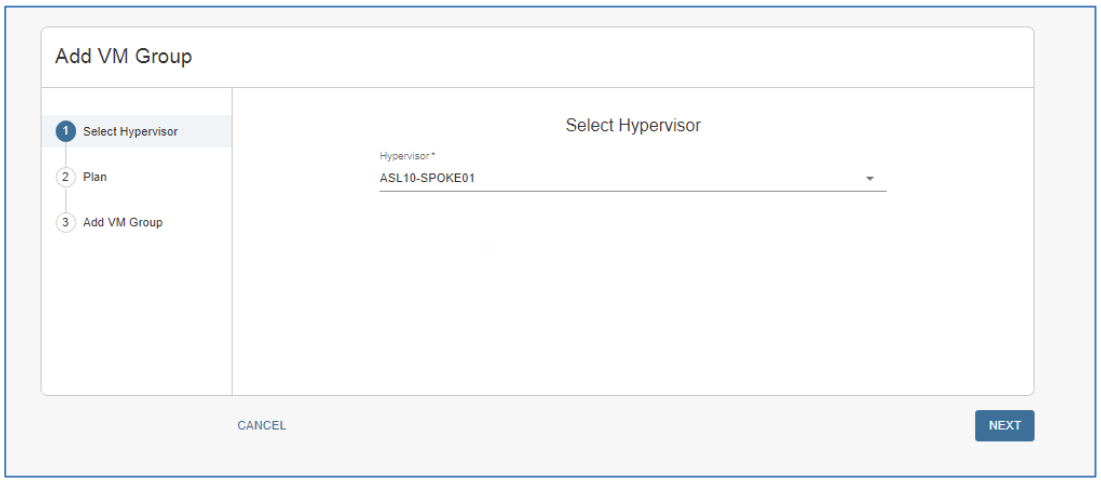
5.1.5 VM Groups

I VM Groups sono in gestione della PA. I VM Groups associano le entità dell'hypervisor AWS (e quindi le VM contenute) ad un Plan.

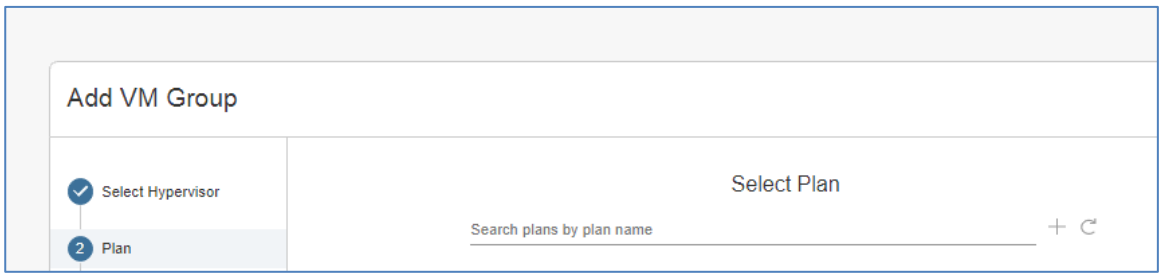
Al rilascio della Landing Zone viene definito un VM Group chiamato Default che protegge lo Spoke e in automatico tutte le VM che saranno create al suo interno.

In autonomia possono essere creati nuovi VM Group per sottoinsiemi di VM, oppure possono essere fatte esclusioni sui VM Group di Default.

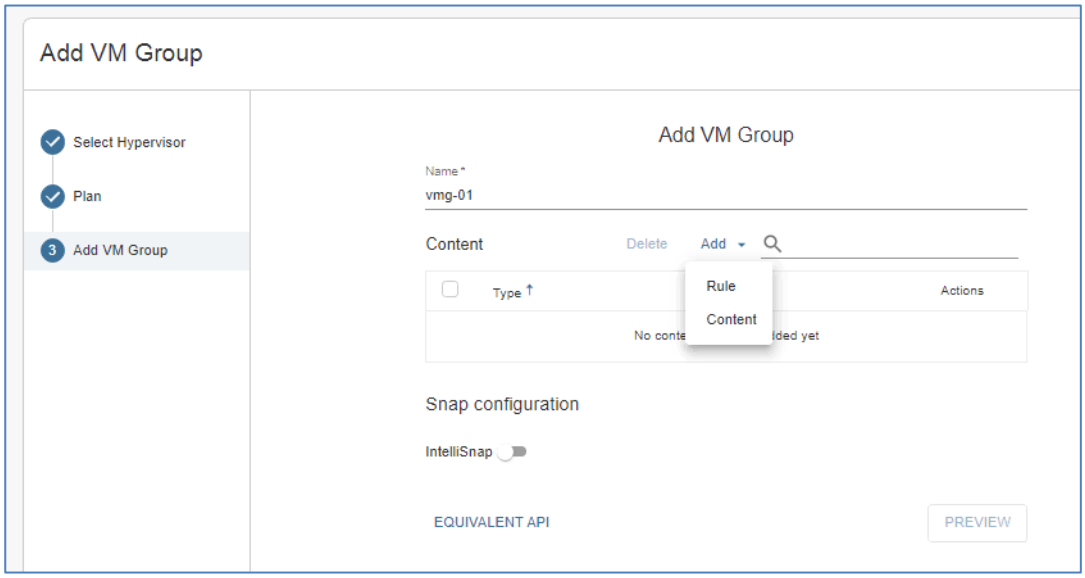
Creazione di un nuovo VM Group:



Selezionare il Plan:



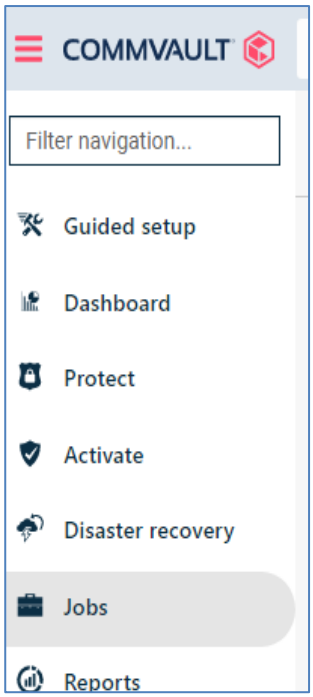
Definire il nome e il contenuto del VM Group:



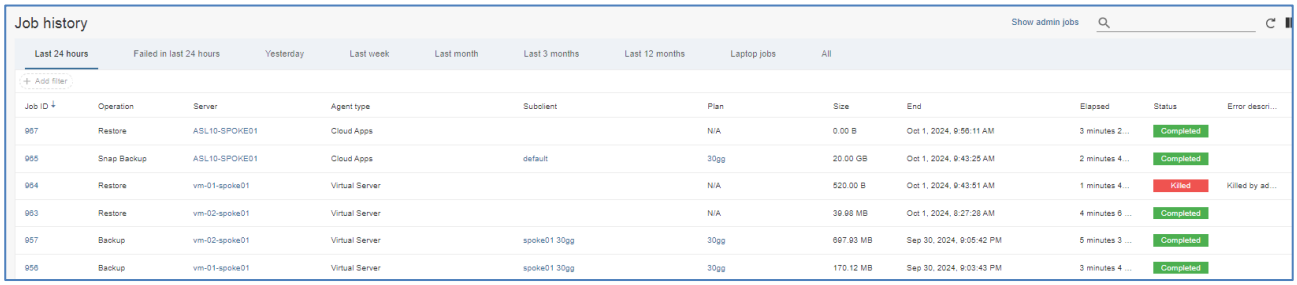
Il contenuto può essere configurato su regola (ad esempio con i TAG), oppure indicando le singole VM

5.1.6 Jobs

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



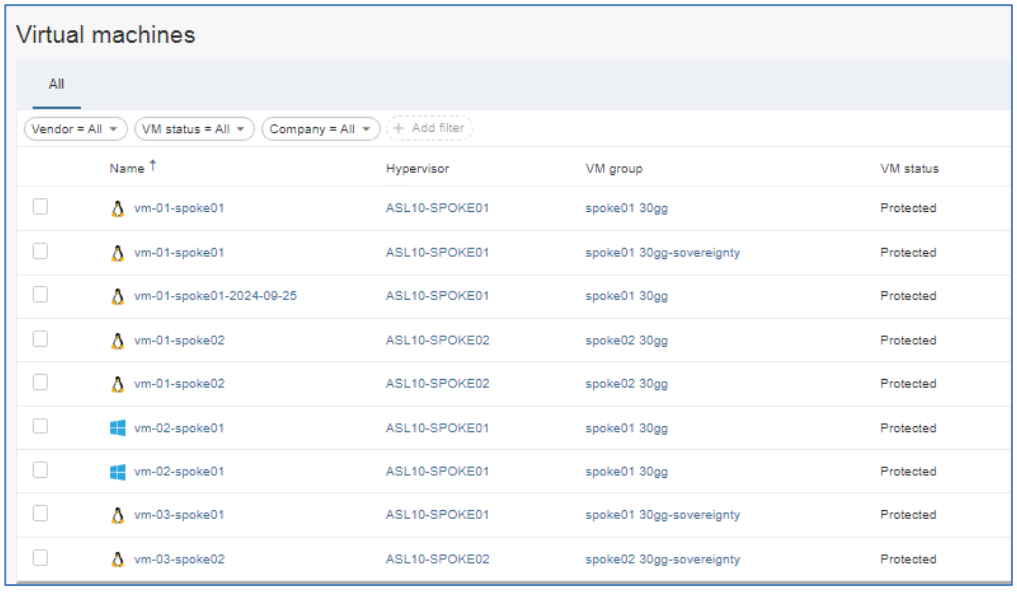
I JOB possono essere analizzati nel dettaglio selezionando con il mouse il numero di job:



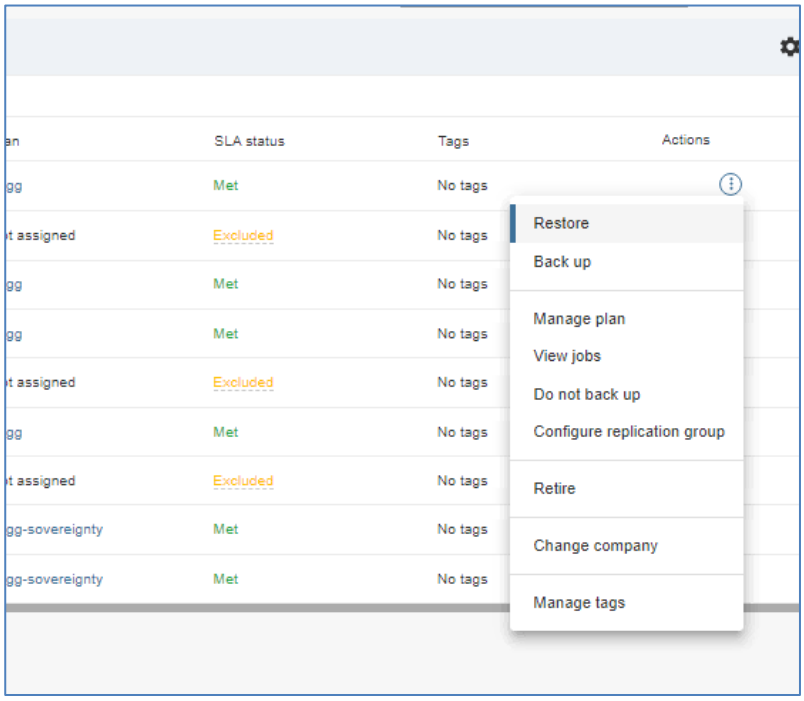
5.1.7 Manual Backup

I backup sono schedulati secondo la RPO del Plan.
Per eseguire backup manuali occorre:

- andare nel menu Protect/Virtualization/Virtual Machine:



- selezionare la VM ed eseguire il comando backup dal menu di action:

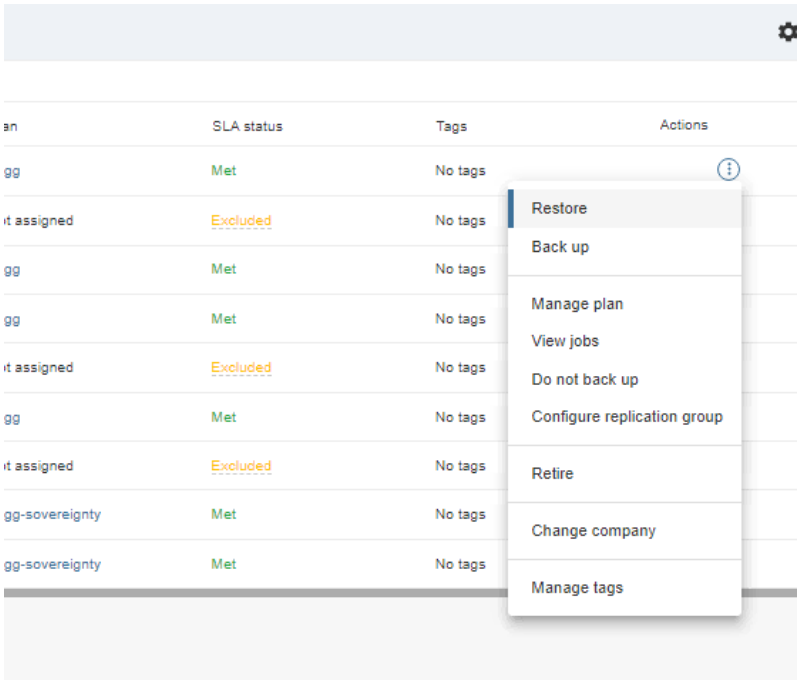


- Seguire l'esecuzione del backup dal menu JOB.

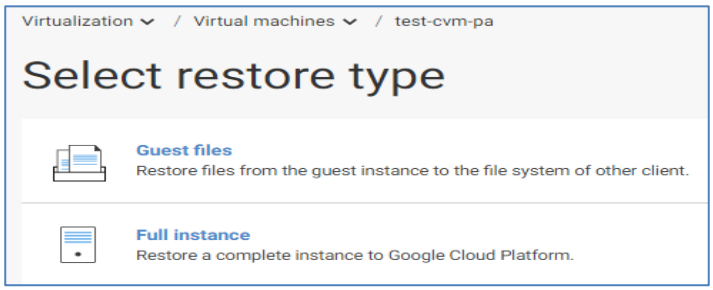
5.1.8 *Restore*

Per eseguire una restore occore:

- selezionare dal menu Protect/Virtualization/Virtual Machine la VM da restorare e selezionare restore dal menu Action:



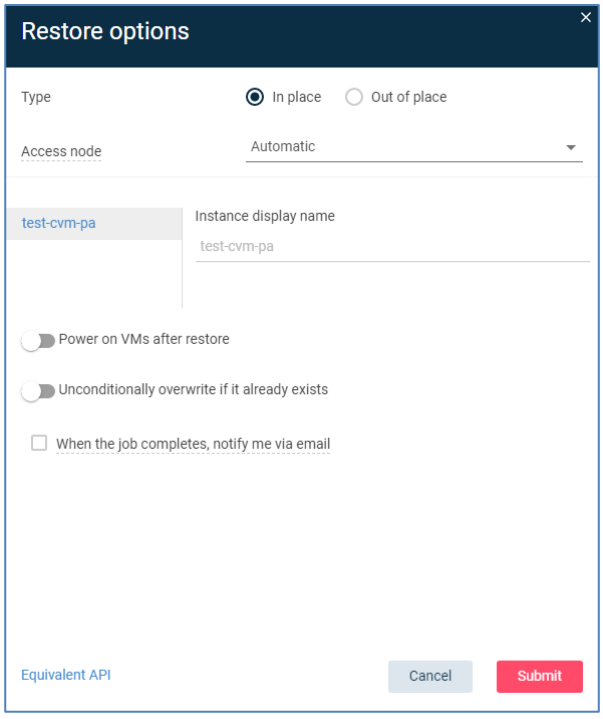
- scegliere il tipo di restore:

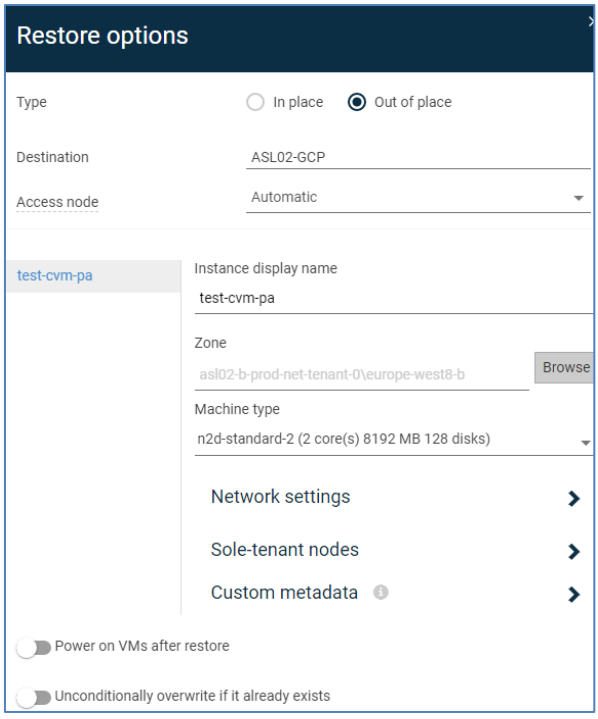


- procedere seguendo il wizard.

Dettagli sulla procedura sono reperibili sulla manualistica ufficiale di Commvault al seguente URL:
https: //documentation.commvault.com/commvault/index.html

La restore potrà essere eseguita “In Place”, sovrascrivendo la VM da restorare, oppure “Out of Place” per mantenere la VM originale.

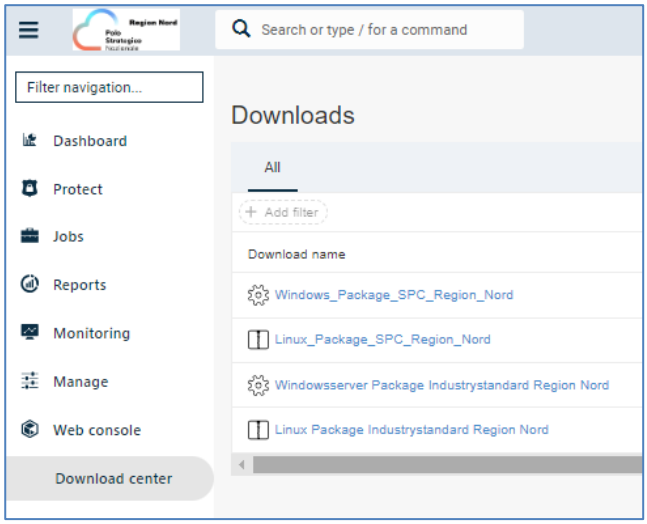




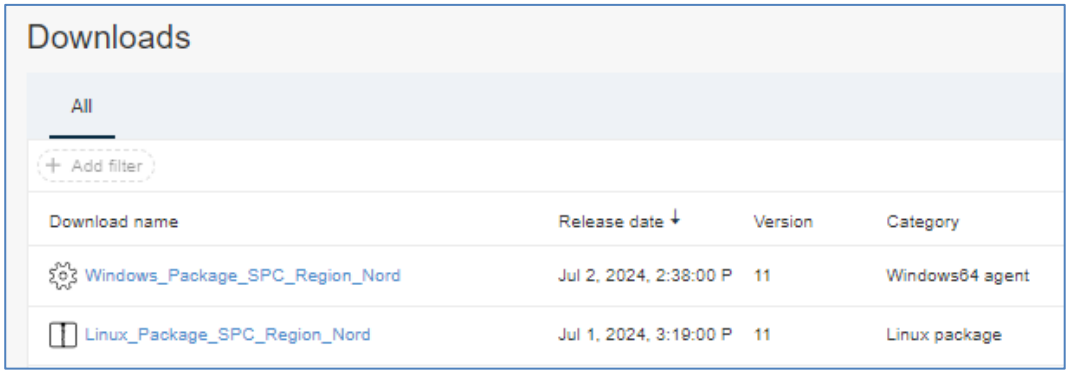
5.1.1 Backup con Agent

In caso di necessità di backup di workload differenti dalle virtual machine Ec2 occorre installare un agente Commvault sul sistema operativo della VM.
Lo scenario tipico è quello di database.

Il software necessario è scaricabile dal portale BaaS nel menu Web console => Download Center



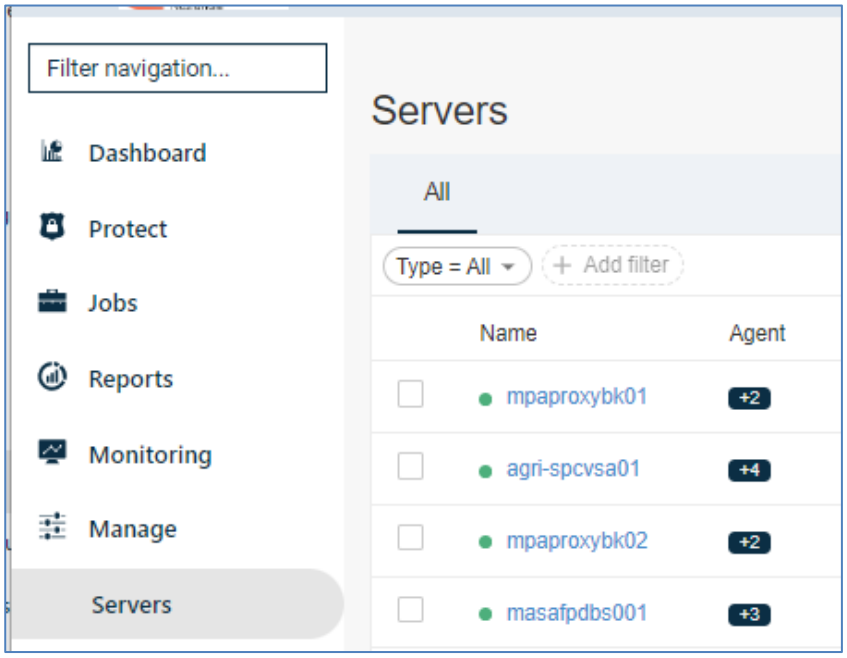
Sono disponibili due package per l'ambiente SPC.



Durante l'installazione occorre, se richiesto, indicare come server il DNS name della VSA.
Inoltre, occorre verificare che il client riesca a risolvere in modo corretto il DNS della VSA.
Lo standard di naming convention nomina le VSA come: XXXX-spcvsa01
Dove: XXXX è il codice prefisso della PA in ambiente SPC.

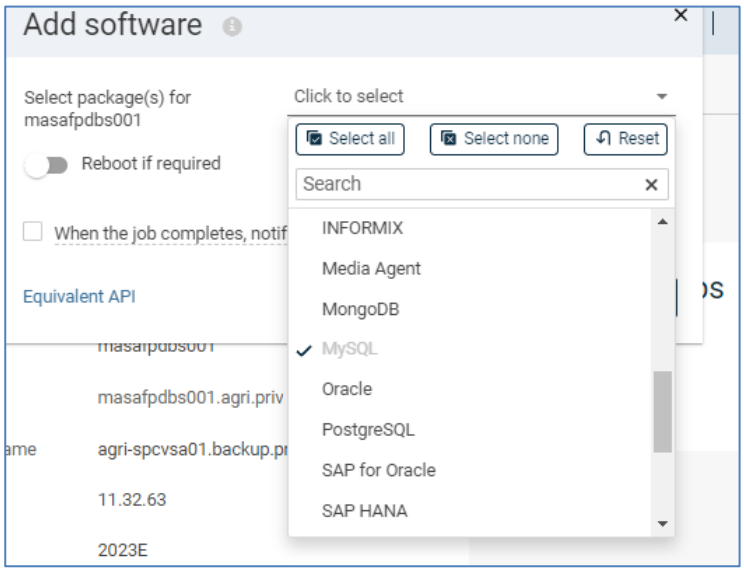
Oltre alla risoluzione del DNS name è essenziale l'apertura della porta 8403 del Firewall dal client verso la VSA.

Terminata l'installazione il client sarà visibile tra i server con una spia di colore verde.



Solo a questo punto sarà possibile installare sul client il software per la gestione dei backup del DB.

Ad esempio, se sul client è installato un MySQL, si seleziona il client e con il comando "Add Software" si aggiunge l'estensione relativa:



5.1.2 Manuali Commvault

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

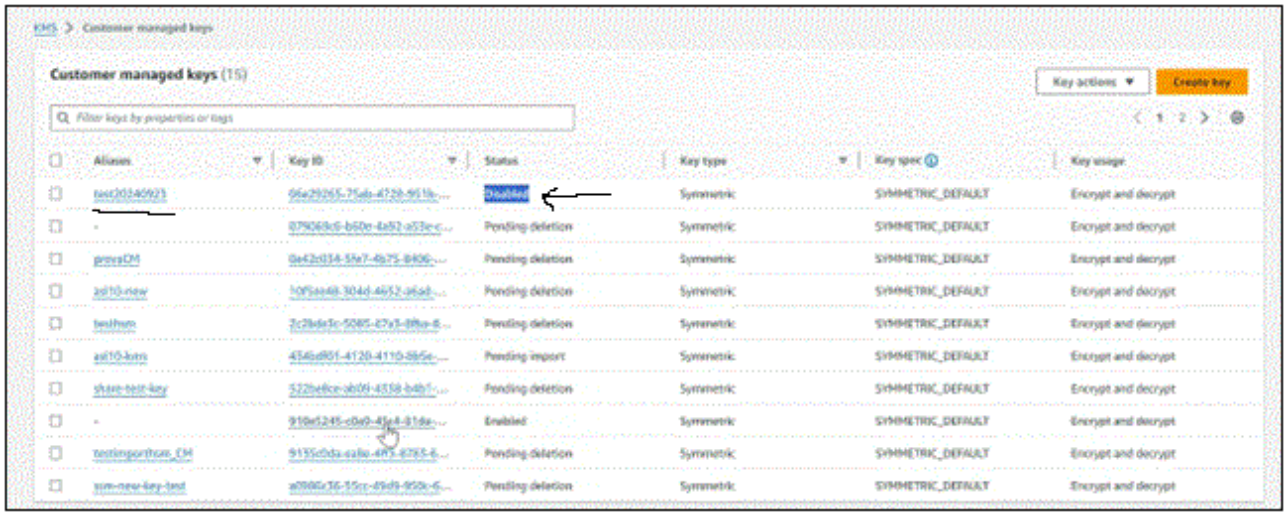
- Protecting Amazon EC2

- Amazon S3
- RDS Database
- AWS EKS
- Commvault Documentation

6 KMS

La gestione delle chiavi prevede l'utilizzo della modalità definita come Bring Your Own Key (BYOK). Le chiavi di cifratura vengono create e gestite dall'infrastruttura Thales presente on-premise nei datacenter del PSN, escludendo così il CSP dalla gestione delle chiavi di cifratura.

All'interno dell'Hub account viene istanziata la risorsa Key Management Service (KMS) 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 KMS e messa a disposizione dell'ambiente Secure Public Cloud.



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 utilizzare per la cifratura del layer applicativo (produzione, sviluppo e test), esempio:

- Amazon EC2
- Amazon EKS
- Amazon S3
- Amazon RDS

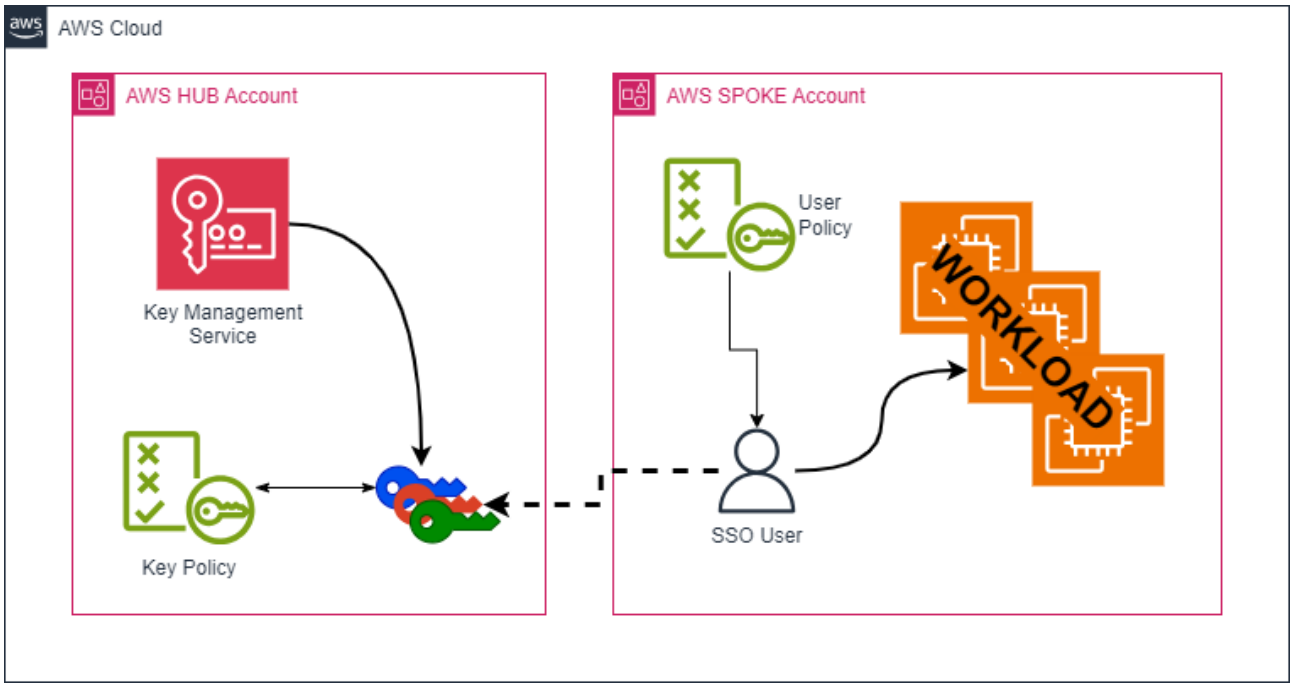
È comunque possibile per la PA richiedere, tramite il servizio di ticketing dedicato del PSN, chiavi aggiuntive per specifici workload applicativi, indicando le caratteristiche della chiave da generare (nome, algoritmo di encryption, size, durata), nonché la destinazione d'uso.

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.

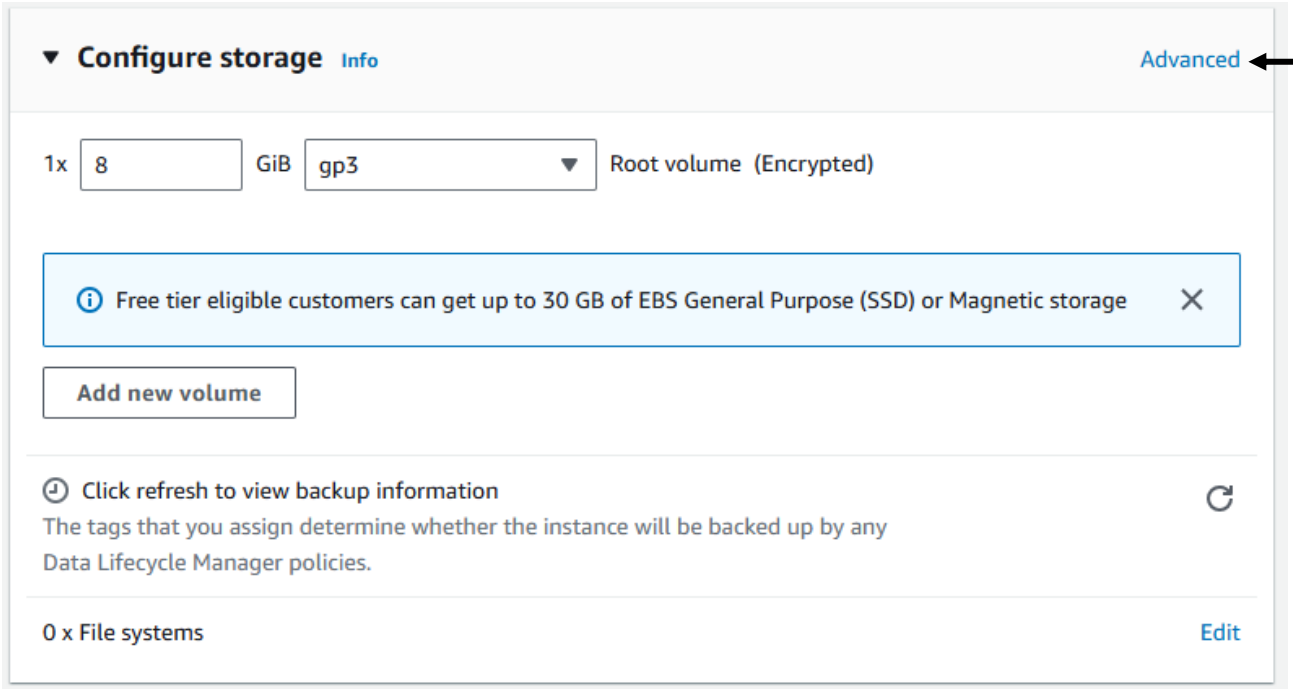
Il servizio AWS KMS contenente le chiavi di cifratura della PA è visibile dall'intero tenant PA, attraverso le policy assegnate alle chiavi e i privilegi concessi agli utenti PA utilizzatori, consentendo l'utilizzo delle chiavi per cifrare i differenti workload.



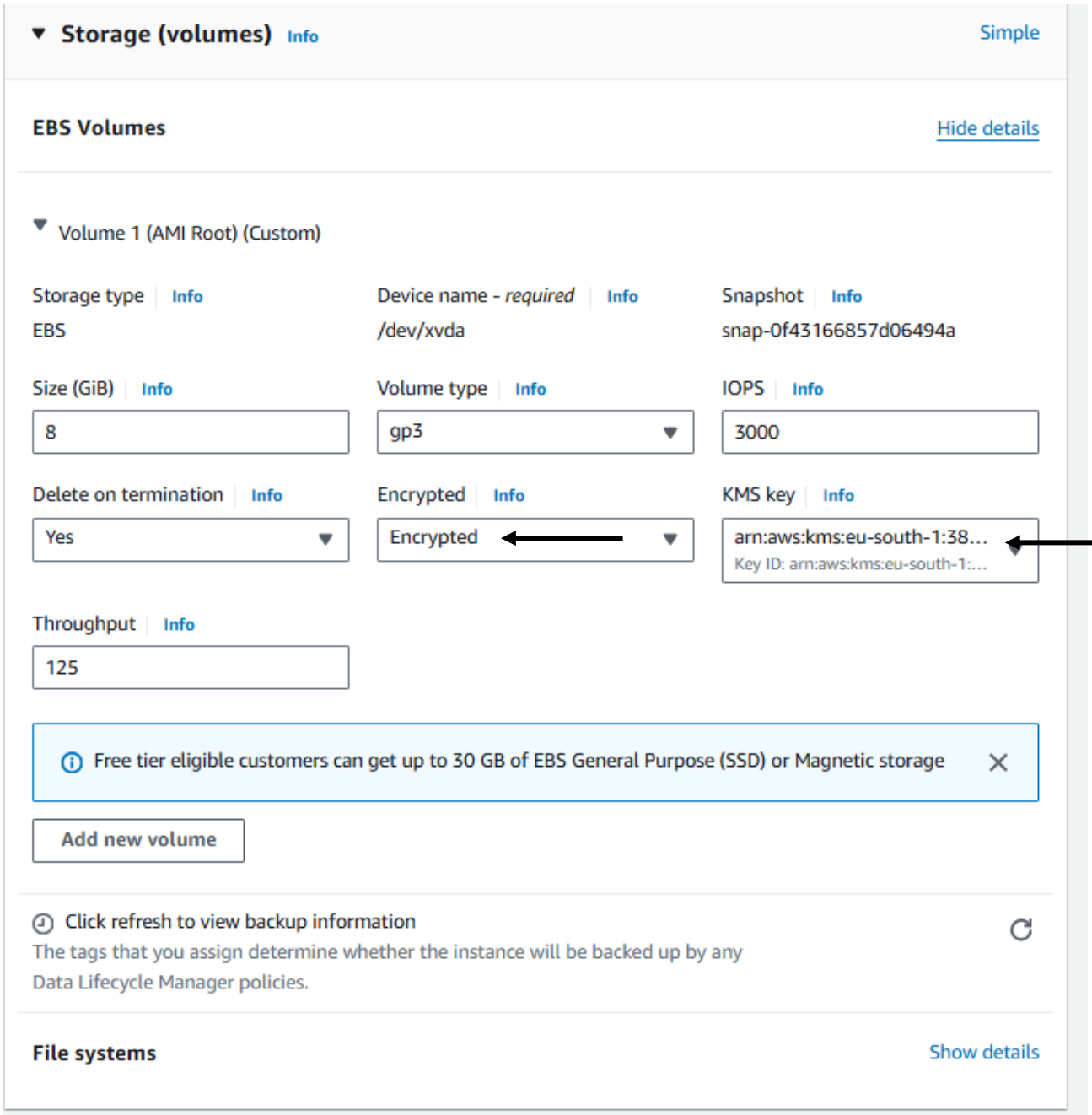
6.1.1 *Utilizzo Chiave esterna per una Virtual Machine*

Le chiavi di cifratura sono gestite attraverso il servizio AWS KMS, che ne consente l'utilizzo per eseguire l'encryption di EBS (dischi) di tipo HDD, SSD (gp2 e gp3) e IOPS. Il deploy di una standard virtual machine deve seguire il normale processo di provisioning di una EC2, ponendo attenzione alla scheda "Configure storage".

La scheda comparirà in questo modo:



Si dovrà premere sul tasto “Advanced” per mostrare l’apposito menù per la configurazione di una chiave di cifratura sul volume della macchina e scegliere dal menu a tendina Encrypted e, di conseguenza, “Specify a custom value”.



6.1.1 *Istanze Confidenziali*

In AWS non è necessario applicare ulteriori step per raggiungere la confidenzialità della parte compute.

Le macchine confidenziali in AWS offrono un livello avanzato di sicurezza, permettendo di proteggere i dati durante l'elaborazione, oltre che a riposo e in transito. Grazie al supporto integrato del Nitro System e alle tecnologie di crittografia hardware come AMD SEV e Intel SGX, i dati elaborati all'interno della macchina virtuale vengono crittografati automaticamente, garantendo che nemmeno l'hypervisor o gli amministratori del sistema possano accedervi.

Questa funzionalità è particolarmente importante per applicazioni che gestiscono informazioni sensibili o regolamentate, come i dati finanziari o sanitari. Un aspetto fondamentale è che AWS gestisce in modo trasparente l'abilitazione delle macchine confidenziali, senza la necessità di ulteriori sforzi da parte dell'utente per configurare o abilitare queste funzionalità di sicurezza. Di conseguenza, i clienti possono beneficiare di una protezione avanzata dei dati senza compromettere le prestazioni o la semplicità d'uso.

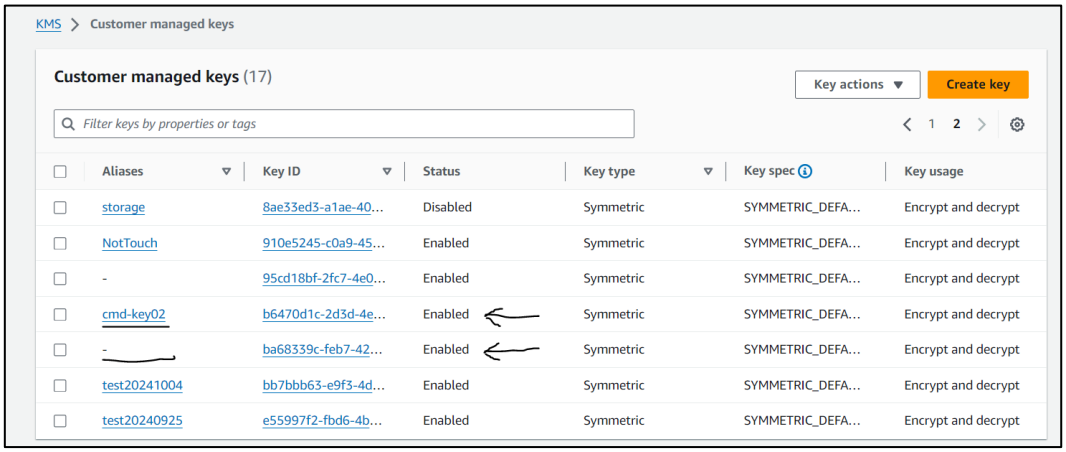
La documentazione di riferimento:
https://aws.amazon.com/blogs/compute/aws-nitro-system-gets-independent-affirmation-of-its-confidential-compute-capabilities/

6.1.2 Rotazione chiave

Tutte le attività inerenti il ciclo vita delle chiavi devono essere effettuate sull'infrastruttura Thales ospitata nei Datacenter del PSN e gestite da personale PSN; non è possibile quindi operare sulle chiavi direttamente dalla console Amazon.

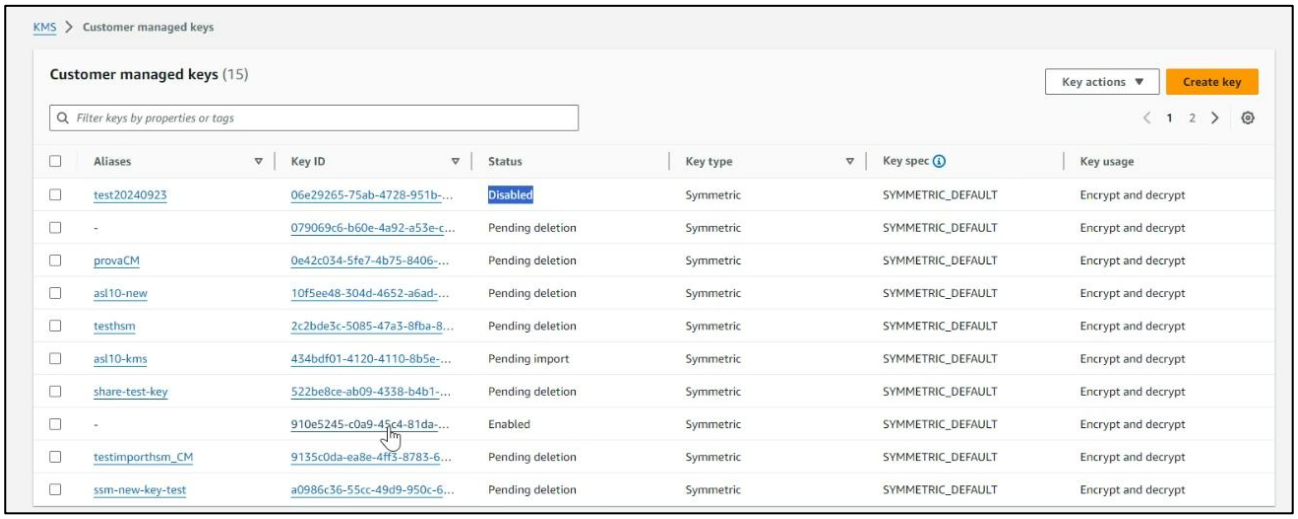
Durante la fase di generazione della nuova chiave destinata alla rotazione, il personale PSN crea la nuova key utilizzando il CipherTrust Manager di Thales, sincronizzando quest'ultima nel KMS in cloud.

Il nuovo materiale crittografico, con un nuovo codice ARN, sarà associato all'alias della chiave oggetto di rotazione; il codice ARN originario invece non avrà alcun alias associato.



In questa fase entrambe le versioni della chiave avranno validità e lo stato impostato su "Enabled", per consentire le operazioni di sostituzione della chiave sulle risorse AWS, al termine delle quali la vecchia versione della chiave (priva di alias) potrà essere disabilitata. Per completare il ciclo di rotazione con la disabilitazione della chiave da dismettere, la sostituzione della chiave dovrà essere obbligatoriamente eseguita su tutte le VM, per evitare di generare disservizi.

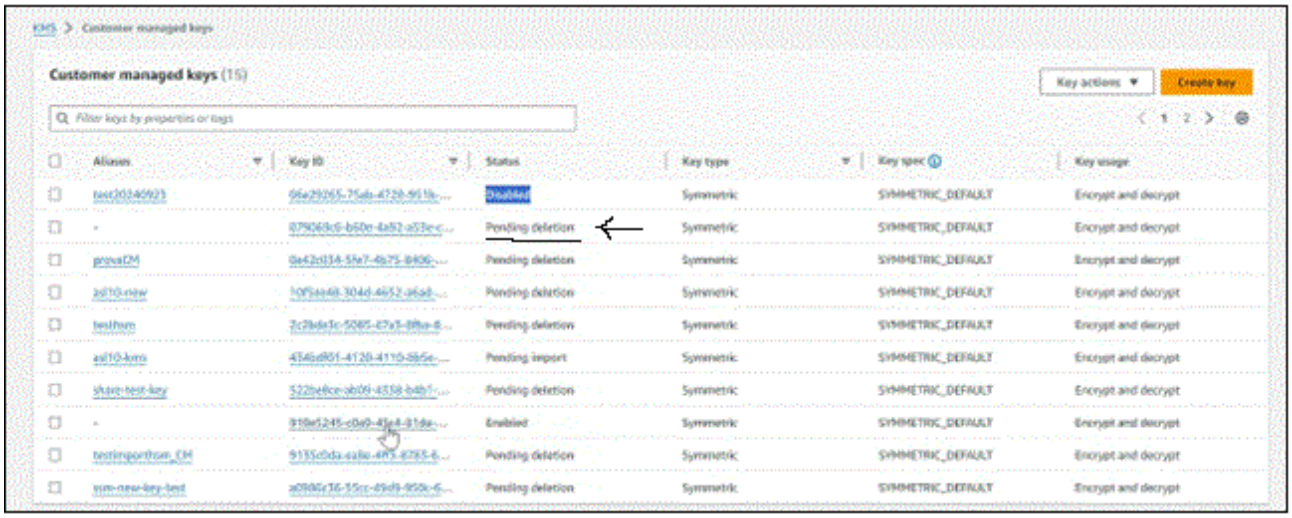
Quando una chiave viene disabilitata lato Thales, lo stato della stessa sul KMS risulterà come "disable" e al riavvio la VM non sarà più accessibile:



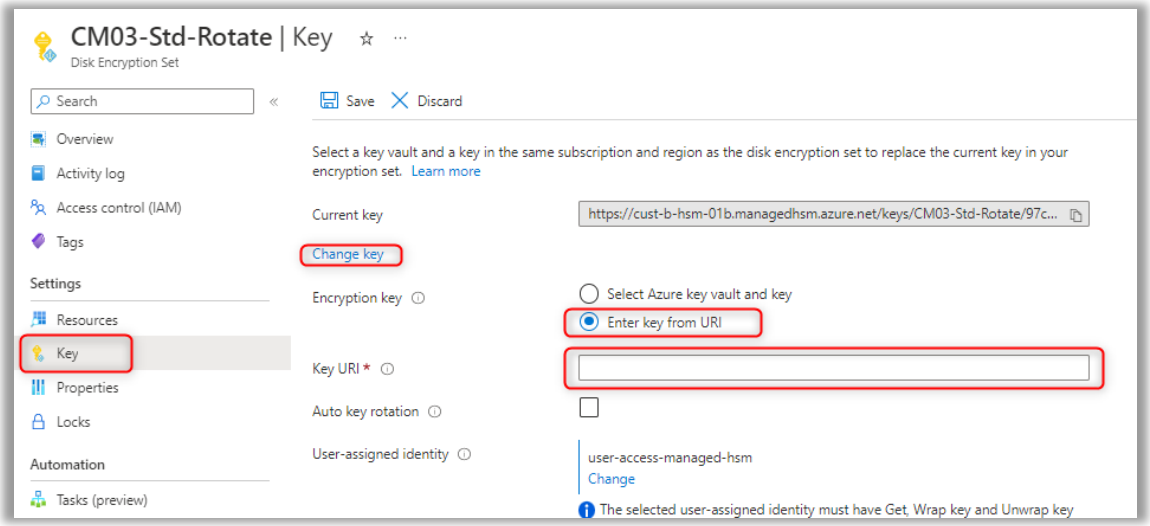
Non sarà possibile abilitare/disabilitare delle chiavi dall'Amazon KMS.

6.1.3 Cancellazione chiave

Se una chiave viene cancellata lato Thales, lo stato della stessa sull'AWS KMS risulterà come "Pending Deletion" e, al riavvio, la VM non sarà più accessibile; la chiave sarà cancellata definitivamente al termine del retention period. È altresì possibile annullare l'operazione di cancellazione chiave, intervenendo dalla console di gestione Thales: la chiave cambierà stato inizialmente su "Disabled" e dovrà essere nuovamente attivata per poter essere utilizzata.



Il retention-period che può essere impostato è compreso tra un minimo di 7 ed un massimo di 30 giorni.



7 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.