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 Azure

Data: 21/05/2025

PSN_Manuale Utente SPC Azure

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 Azure			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	23/06/2023	Prima versione
2	1.0	04/04/2025	Seconda versione
3	2.1	21/05/2025	Aggiornato capitolo “Guida alla fatturazione”

NUMERO TOTALE PAGINE:	64

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

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
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 Azure.

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 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 Microsoft Azure generiche

3.1.1 Management Group

Ogni tenant Azure corrispondente ad un cliente Pubblica Amministrazione deve essere configurata con la predisposizione dei seguenti Management Group (MG):

- "Management", gestito dal personale del PSN che contiene le risorse di logging, sicurezza, backup e KMS
- "Connectivity", gestito dal personale del PSN che contiene le risorse HUB Networking tra cui Firewall, Gateway, VNet Centralizzate
- "Landing Zone", gestito dalla PA che contiene tutte le risorse cloud necessarie alla gestione del workload applicativo del cliente

Il tenant 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, la prima con il ruolo di Global Admin, l'altra che ha ruolo di Managed HSM Administrator.
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 o il ripristino del Managed HSM ospitato su Azure.

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 nel tenant Azure 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 portal.azure.com

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.

Ruolo	Type	Responsabilità	Assegnazione (PSN | PA)	Assignment Scope
User Administrator	BuiltIn	Ruolo per la PA per poter creare e gestire nuove utenze.	PA	Azure Active Directory
[PSN] PA User - Spoke	Custom	Ruolo personalizzato per gli utenti della PA nelle sottoscrizioni Spoke di Workload. Permette l'accesso in lettura a tutte le risorse, ed in scrittura a tutte le risorse eccetto quelle di rete, per cui l'utente ha accesso in scrittura solo a Virtual Networks, Subnets, e Network Security Groups.	PA	Spokes
[PSN] PA User - Managed HSM	Custom	Ruolo per l'utente PA nello Spoke Management per il Managed HSM. Permette l'accesso in sola lettura al Managed HSM.	PA	Management
[PSN] PA User - Child FW Policy	Custom	Ruolo personalizzato per gli utenti della PA. Permette l'accesso in lettura all'oggetto Firewall Policy ed in scrittura solo a collezioni di regole, relativi gruppi e regole.	PA	Connectivity
Reader	BuiltIn	Ruolo da assegnare agli utenti della PA per avere accesso in lettura alle risorse del HUB.	PA	Connectivity
Contributor	Builtin	Ruolo da assegnare agli utenti del PSN per avere accesso alle risorse del HUB.	PSN	Connectivity
Contributor	Builtin	Ruolo da assegnare agli utenti del PSN per avere accesso alle risorse dello spoke di Management.	PSN	Management
Security Admin	Builtin	Alla figura apicale del SOC del PSN verrà assegnato in ambiente Azure il ruolo di Security Admin nella sottoscrizione che ospita l'istanza Sentinel deputata al controllo della security posture del PSN	PSN	Management

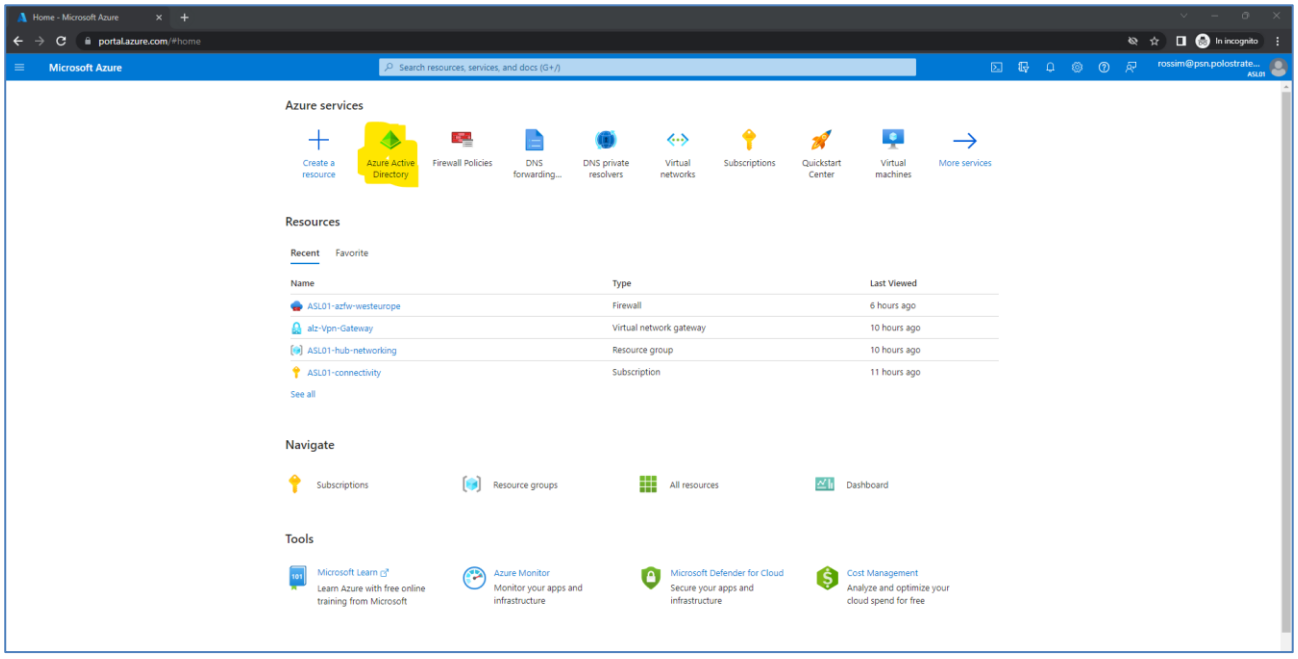
Microsoft Sentinel Contributor	Builtin	Ruolo da affidare agli operatori del SOC del PSN deputati al monitoraggio dei servizi Secure Public Cloud	PSN	Management

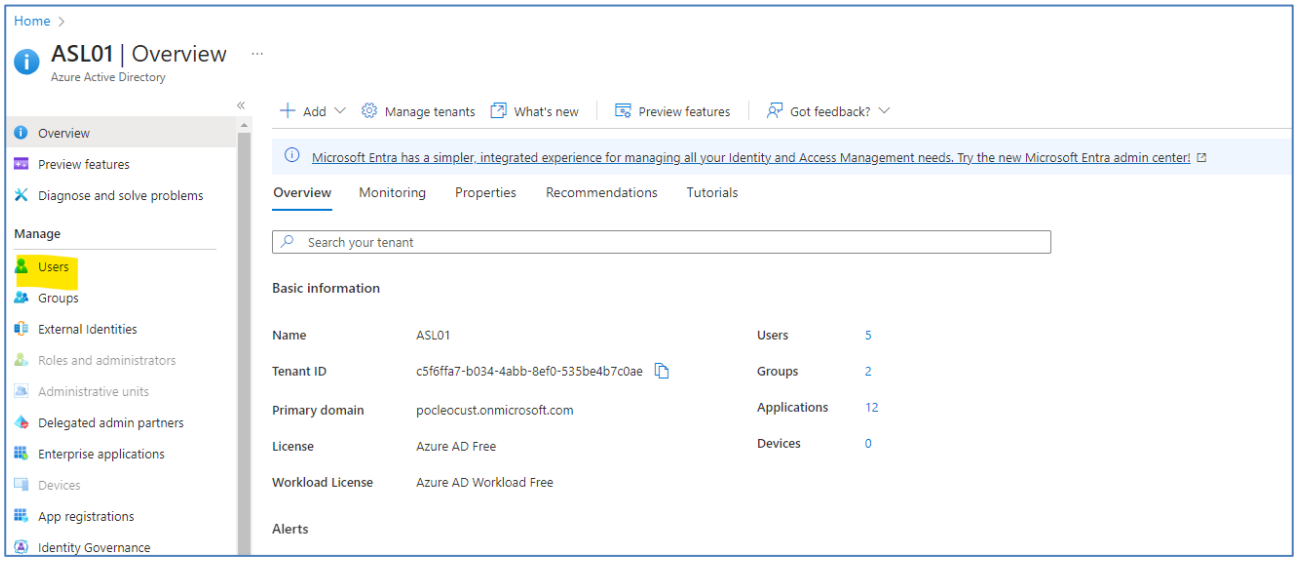
Tabella 3: Ruoli

3.1.5 *Creazione nuovo user*

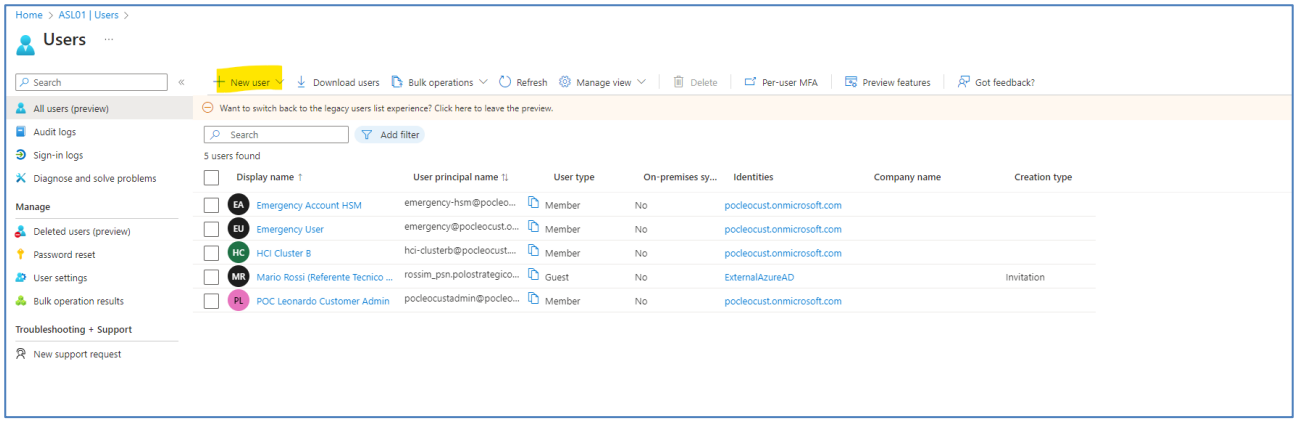
Per creare un nuovo user occorre collegarsi al portale di amministrazione di Azure Active Directory "portal.azure.com" con le credenziali di referente tecnico della PA:

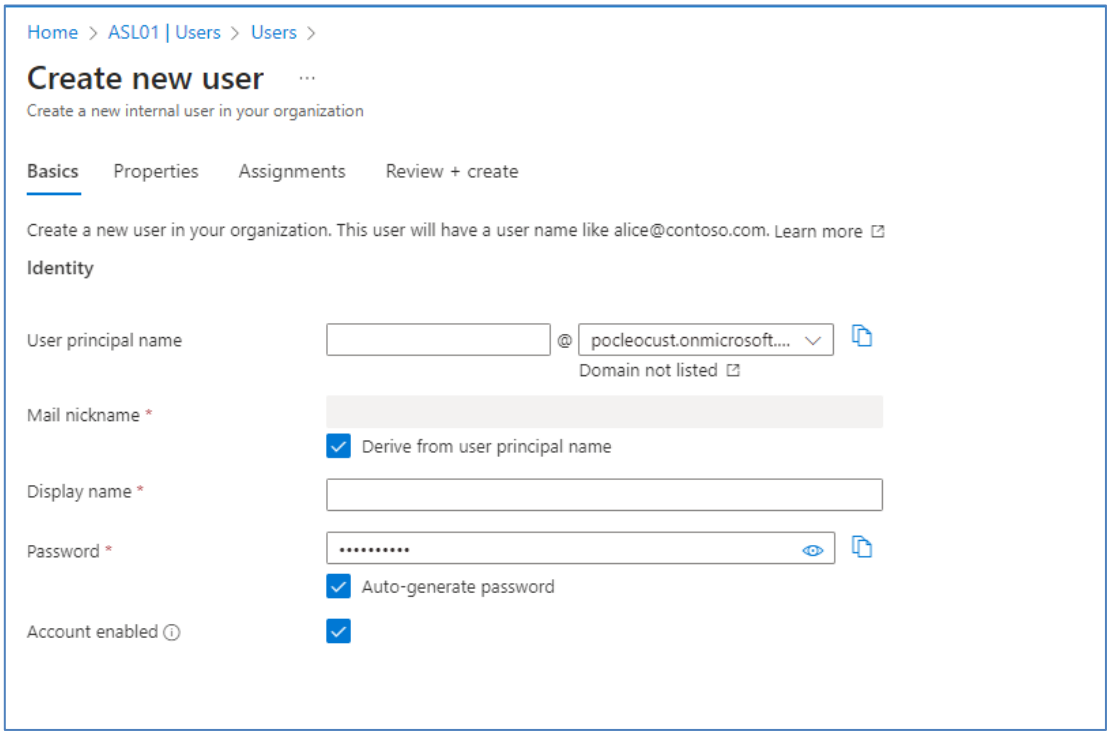
- Accedere al portale di Azure e selezione "Azure Active Directory"





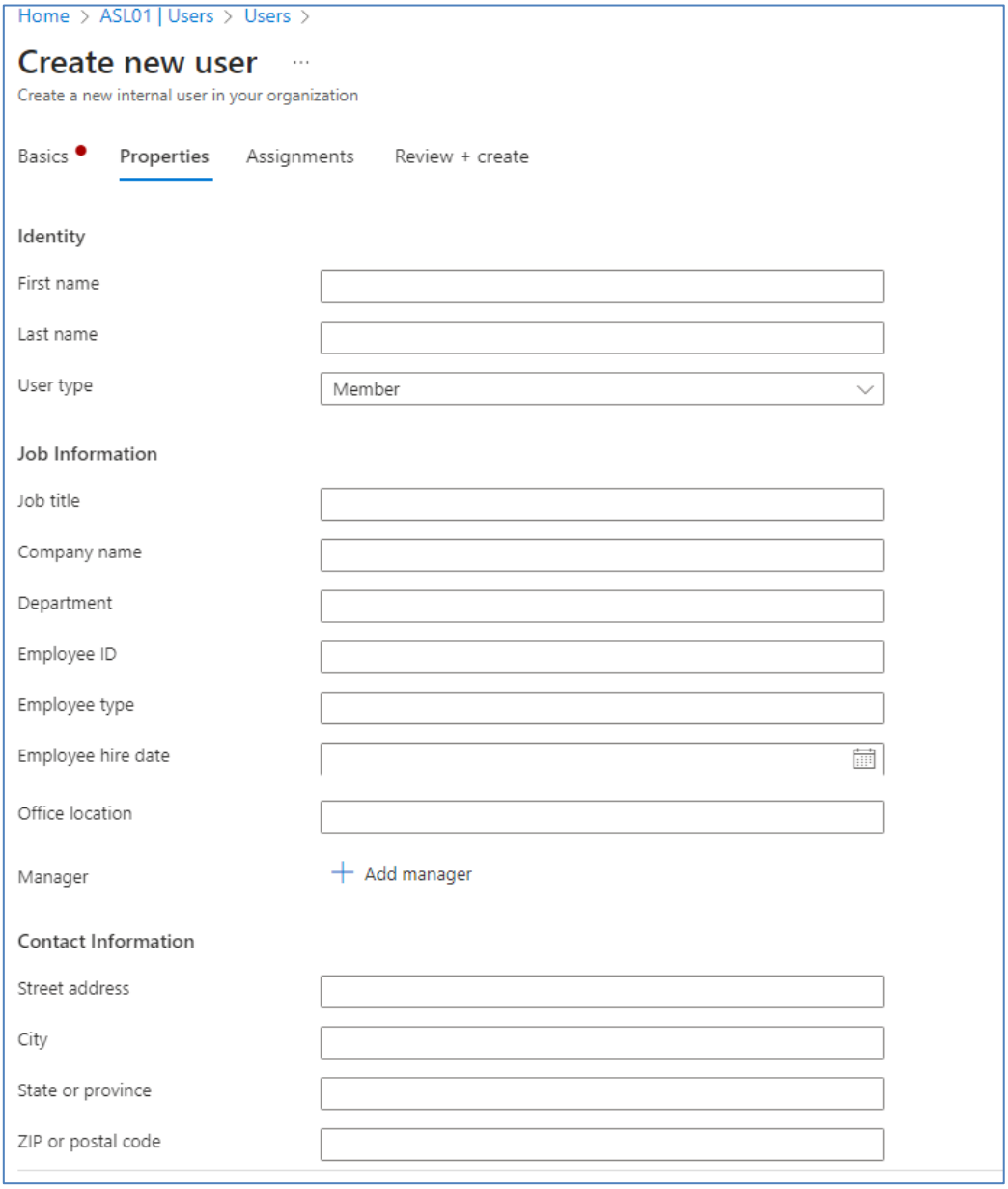
- Selezionare Users e successivamente cliccare su “+ New User”





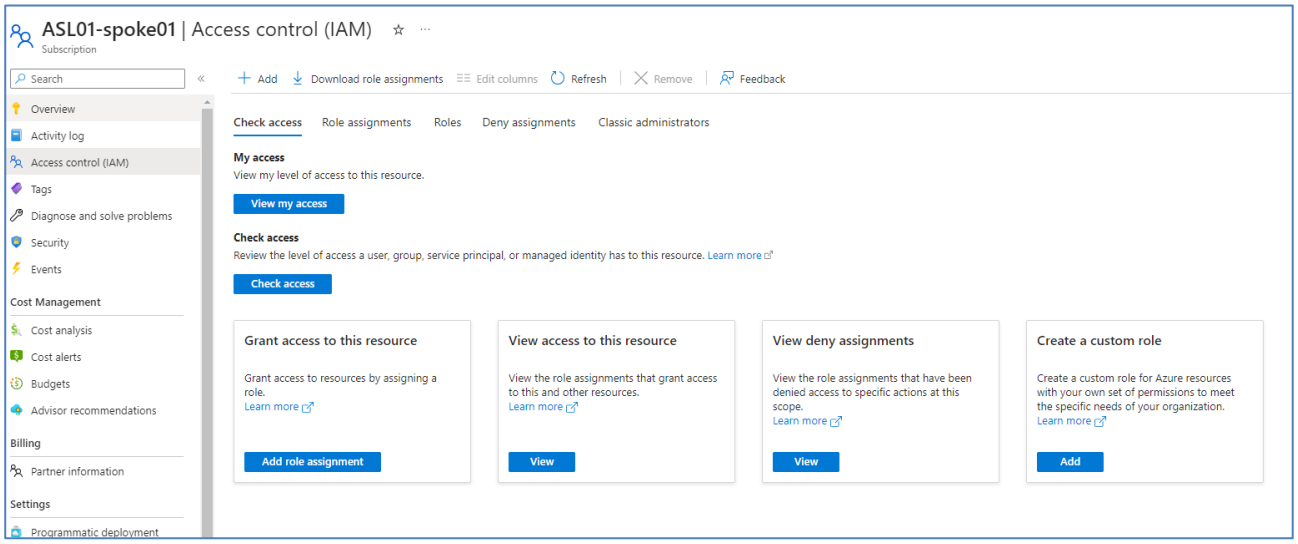
- Inserire nella form i dati:
    - User Principal Name
    - Display Name
    - Password
    - Account Enabled

- Le informazioni specifiche dell'utente sono da configurare all'interno del tab "Properties"

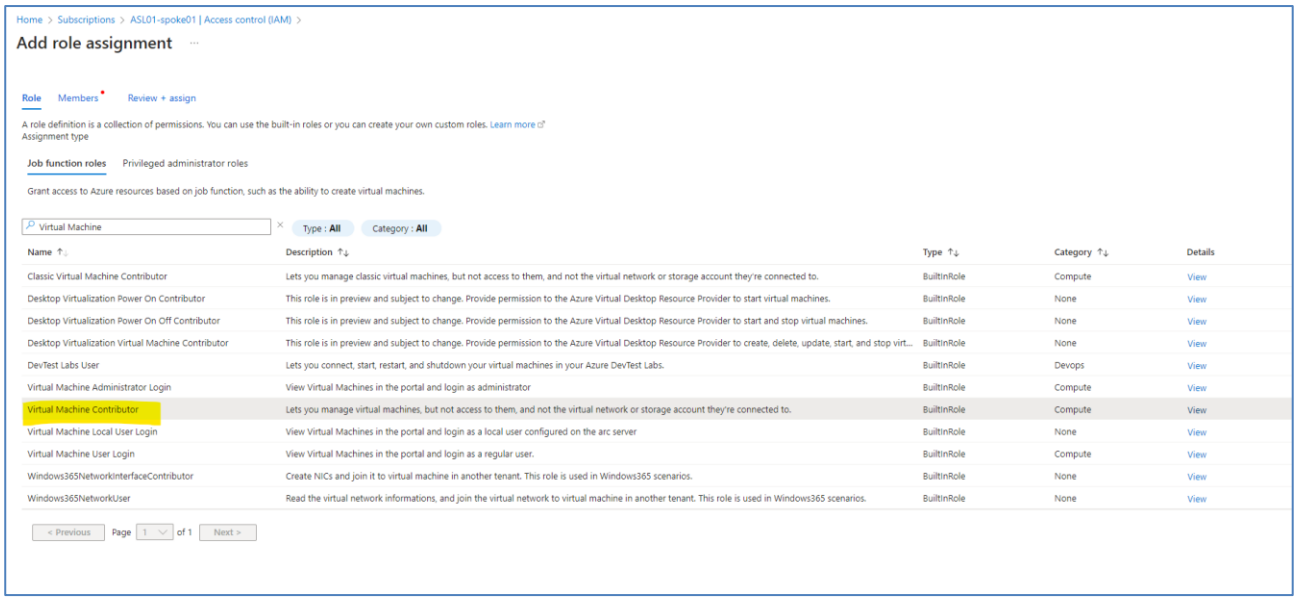


- Salvare la password in una cassaforte digitale.

Dopo aver creato lo user è possibile assegnare lo user al corretto ruolo di riferimento sulle sottoscrizioni / resource group degli Spoke tramite la funzionalità di IAM di Azure:



Ad esempio, è possibile assegnare un ruolo “builtin” come “Virtual Machine Contributor”, al fine di assegnare il ruolo di gestore delle macchine virtuali all’utente appena creato:



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

3.1.6 Guide Azure RBAC Roles

Si rimanda alla documentazione ufficiale di Azure considerando la vastità di ruoli disponibili per personalizzare l’accesso degli utenti:

https://learn.microsoft.com/en-us/azure/role-based-access-control/built-in-roles

Nome	Descrizione	Valore	Livello di applicazione	Eccezioni
[PSN POLICY] Allowed PSN locations	Restringe il deploy delle risorse cloud nella region del PSN.	Deny	Root Management Group	-
[PSN POLICY] Enforce Data Classification Tag and SKU - Critical	Tag obbligatorio da settare alle VM per definire la Data Classification “Critical”	Deny	Root Management Group	-
[PSN POLICY] Enforce data classification Tag and SKU - Ordinary	Tag obbligatorio da settare alle VM per definire la Data Classification “Ordinary	Dent	Root Management Group	-
[PSN POLICY] Not allowed resource types	Non è possibile creare di risorse cloud di questo tipo: ["microsoft.network/publicipaddresses","microsoft.network/publicipprefixes","microsoft.network/internalpublicipaddresses","microsoft.network/azurefirewalls","microsoft.network/applicationgateways","microsoft.network/expressroutegateways","microsoft.classicnetwork/expressroutecrossconnections","microsoft.network/expressroutecircuits","microsoft.network/applicationgatewayavailablewafrulesets","microsoft.network/bastionhosts","microsoft.network/routetables"]	Deny	Root Management Group	
[PSN POLICY] Network interfaces should not have public Ips	Le interfacce di rete non devono avere un IP pubblico associato.	Audit	Root Management Group	-

[PSN POLICY] All Internet traffic should be routed via your deployed Azure Firewall	Tutto il traffico da e per internet deve passare per Azure Firewall	AuditIfNotExists	Root Management Group	-
[PSN POLICY] Web Application Firewall (WAF) should use the specified mode for Application Gateway	Application Gateway ha la funzionalità Web Application Firewall attiva	Audit	Connectivity	-
[PSN POLICY] Subscription should configure the Azure Firewall Premium to provide additional layer of protection	Utilizzo del livello Premium (Next Generation Firewall) per Azure Firewall	AuditIfNotExists	Connectivity	-
[PSN POLICY] Firewall Policy Premium should enable the Intrusion Detection and Prevention System (IDPS)	Abilitazione dell'IDPS sul firewall	Audit	Connectivity	
[PSN POLICY] Firewall Policy Premium should enable all IDPS signature rules to monitor all traffic flows	Abilitazione delle Signature IDPS sul firewall per monitorare il flusso di rete	Audit	Connectivity	-

[PSN POLICY] Deploy - Configure diagnostic settings for Azure Key Vault to Log Analytics workspace	Abilitazione dei diagnostic setting per Azure Key Vault	Audit	Platform	-
[PSN POLICY] Configure diagnostic settings for Storage Accounts to Log Analytics workspace	Configurazione dei diagnostic setting per gli storage account	Audit	Platform	-
[PSN POLICY] Bypass list of Intrusion Detection and Prevention System (IDPS) should be empty in Firewall Policy Premium	La lista di bypass di IPS/IDS deve essere vuota.	Audit	Connectivity	
[PSN POLICY] Deploy log diagnostic setting	Deploy dei diagnostic Setting per la parte di log di audit sulle componenti dell'HUB		Management & Connectivity	
[PSN POLICY] Deploy metrics diagnostic settings	Deploy dei diagnostic Setting per la parte di log di metrics sulle componenti dell'HUB		Management & Connectivity	
[PSN POLICY] Audit log diagnostic settings	Audit della presenza dei diagnostic Setting per la parte di log di audit sulle componenti dell'HUB	Audit	Management & Connectivity	

[PSN POLICY] Subnets must have PSN Route Table	Previene operazioni (creazione e modifica) che definiscono le subnets senza la Route Table predefinita dal PSN.	Deny		
[PSN POLICY] OS and data disks should be encrypted with a customer-managed key	Nega la creazione di dischi per VM che non usano le chiavi gestite dal cliente.	Deny		
[PSN POLICY] Both OS and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys	Nega la creazione di dischi per cluster Kubernetes che non usano le chiavi gestite dal cliente.	Deny		

3.1.7 Autenticazione

Le utenze dell'ambiente Azure 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.
Di seguito si riporta il link del pannello di controllo per la gestione dell'SPC:

Portal.azure.com

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

3.1.8 Azure Policy

L'ambiente Secure Public Cloud in Azure 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 il link alla pagina Azure della documentazione relativa al servizio:

https://learn.microsoft.com/en-us/azure/governance/policy/overview

In caso di esigenze specifiche relative ad attivazione, disattivazione o diversa configurazione di Policy sul tenant 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 Azure Sentinel

La componente Azure Sentinel, nel mondo Microsoft Azure, è la soluzione che si occupa di implementare le funzionalità di SIEM (Security information and event management) e SOAR (Security Orchestration, Automation and Response). All'interno dell'architettura proposta, questa componente si occupa di analizzare i log di sicurezza provenienti dalle risorse cloud, monitorare la postura di sicurezza definita dal PSN Provider ed eseguire automazioni nel caso in cui vengono rilevati degli incident di sicurezza all'interno del tenant Azure SPC.

Per Maggiori informazioni sulle funzionalità di Azure Sentinel si prega di far riferimento alla guida ufficiale fornita dal cloud provider Microsoft:

https://azure.microsoft.com/it-it/products/microsoft-sentinel

Nell'ambito del servizio Secure Public Cloud su Azure, viene configurato un Sentinel di default dal PSN che è utilizzato per garantire la postura di sicurezza dell'infrastruttura di base. Viene preconfigurato con una serie di regole di Alert che saranno inviati al SIEM del PSN, regole utili a garantire che la postura di sicurezza di base dell'infrastruttura.

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.

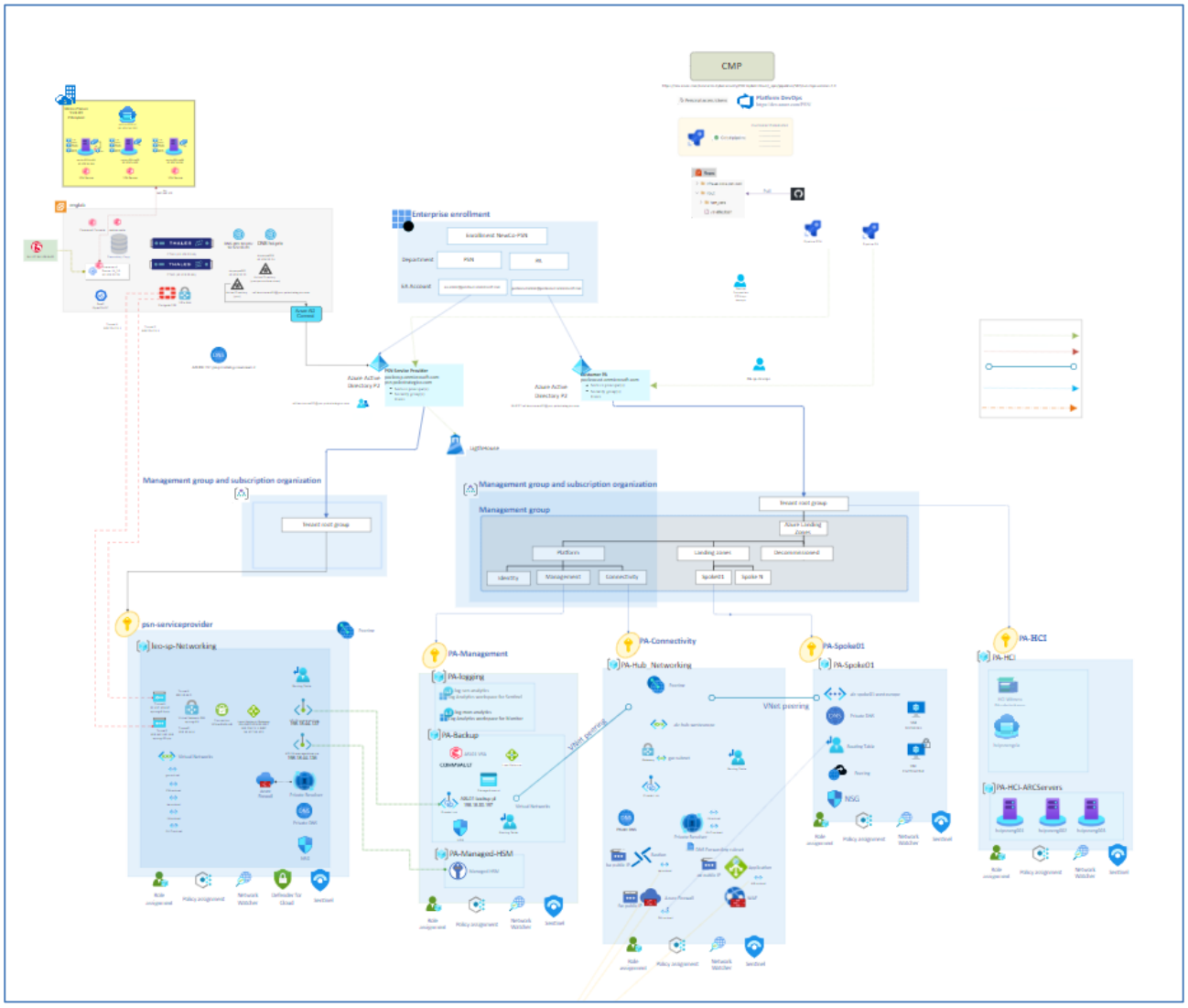


Figura 1: Design di rete

In questo modello la vnet presente nell'HUB è in peering con le vnet presenti negli Spoke.

Sia nell'HUB che nello Spoke sono presenti delle Tabelle di Routing dette UDR(User Defined Route) che fanno sì che tutto il traffico dagli Spoke, sia verso Internet, che tra Spoke e Hub, venga forzato verso il Firewall che risiede sulla vnet dell'HUB.

Il Firewall ha anche funzione di Sonda IDS che di Proxy DNS verso il servizio di DNS Private Resolver per la risoluzione di tutti gli FQDN richiesti.

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

3.2.1 Gestione vnet

Nel caso in cui la PA ha la necessità di attivare un nuovo Spoke per ospitare una nuova vnet, 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;
- Creare il peering con la vnet dell'HUB;
- Aggiornare la UDR dell'HUB;
- Creare la UDR da associare alle subnet della vnet.

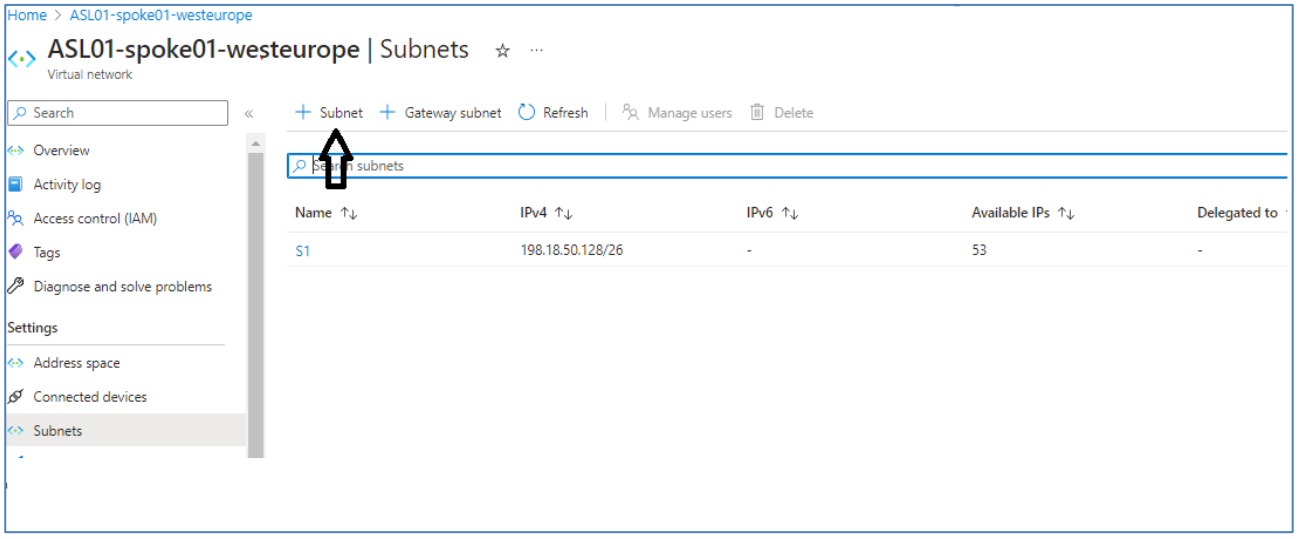
Tutte le subnet all'interno della vnet creata si vedono tra di loro, al netto di specifici NSG (Network Security Group) configurati ad hoc per impedirne la visibilità.

3.2.2 Gestione subnet

La PA può gestire le subnet all'interno della vnet dello Spoke.

Per aggiungere una nuova subnet all'interno di una vnet occorre prima di tutto verificare se esiste ancora disponibilità di Reti IP libere nello spazio di indirizzamento messo a disposizione per la vnet.

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



Configurare Nome, IP, e impostare la Route Table:

3.2.3 *Gestione DNS*

Il Servizio di DNS è fornito dal DNS Proxy presente nel Firewall.
Tutte le vnet sono configurare per fornire alle Vm che sono agganciate alle subnet della vnet, l'IP del Firewall come DNS server.

La PA può creare e gestire Zone DNS private create dentro le sottoscrizioni degli Spoke.

Per far sì che i record inseriti nella nuova zona DNS Privata siano risolvibili dalle Vm della PA occorre aprire un ticket al PSN che provvederà a:

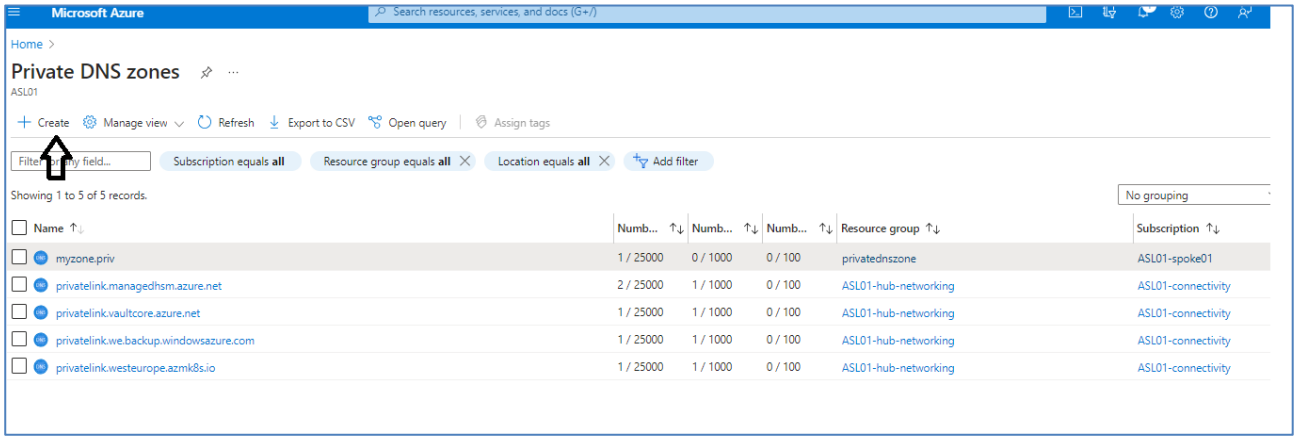
- Creare il link alla vnet di Connectivity all'interno della zona DNS privata per consentirne la risoluzione.

Per aggiungere una zona DNS privata con risoluzione On Prem occorre aggiungere una nuova rule all'interno della "DNS forwarding ruleset", in questo caso la PA dovrà aprire un ticket al PSN che provvederà a:

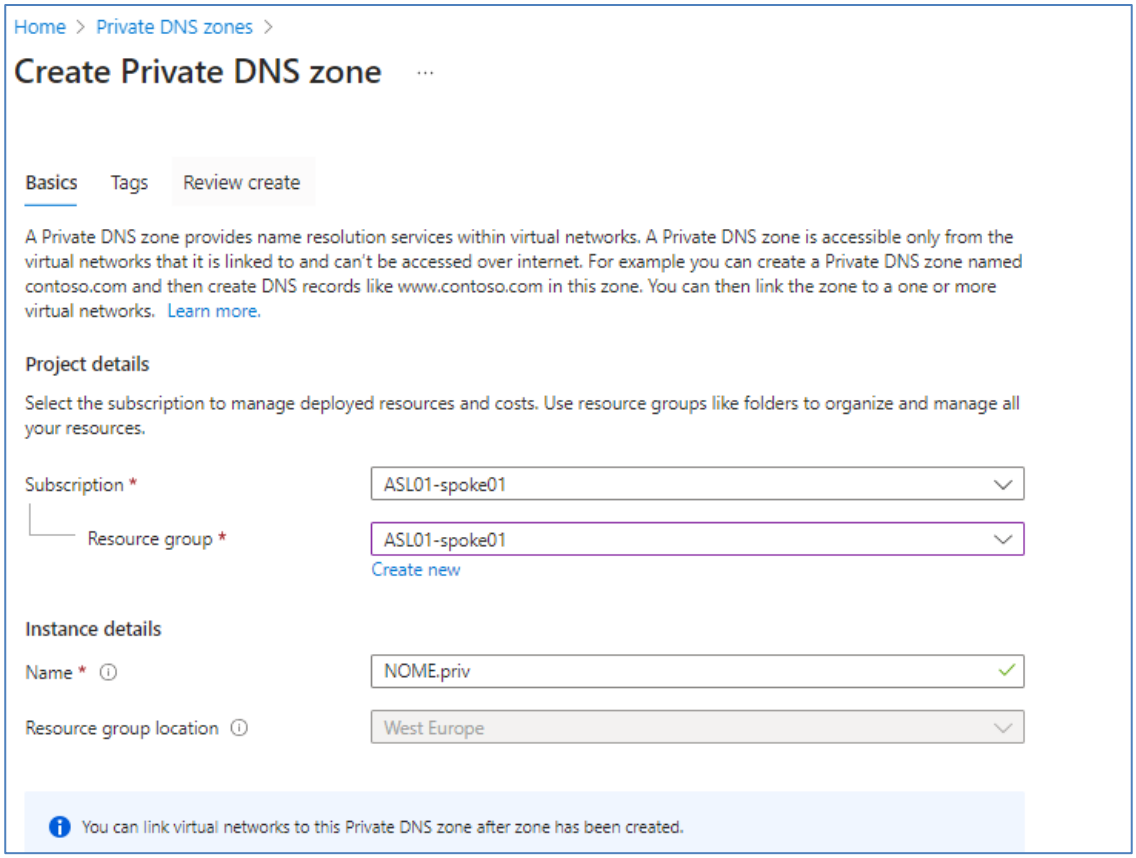
- DNS forwarding ruleset (se non presente);
- Creare la DNS rule.

Di seguito viene indicata la procedura per creare una Zona DNS Privata dall'utente della PA:

Andare sotto Private DNS Zones e cliccare su Create



Fornire:
Subscription, Resource Group e Nome:

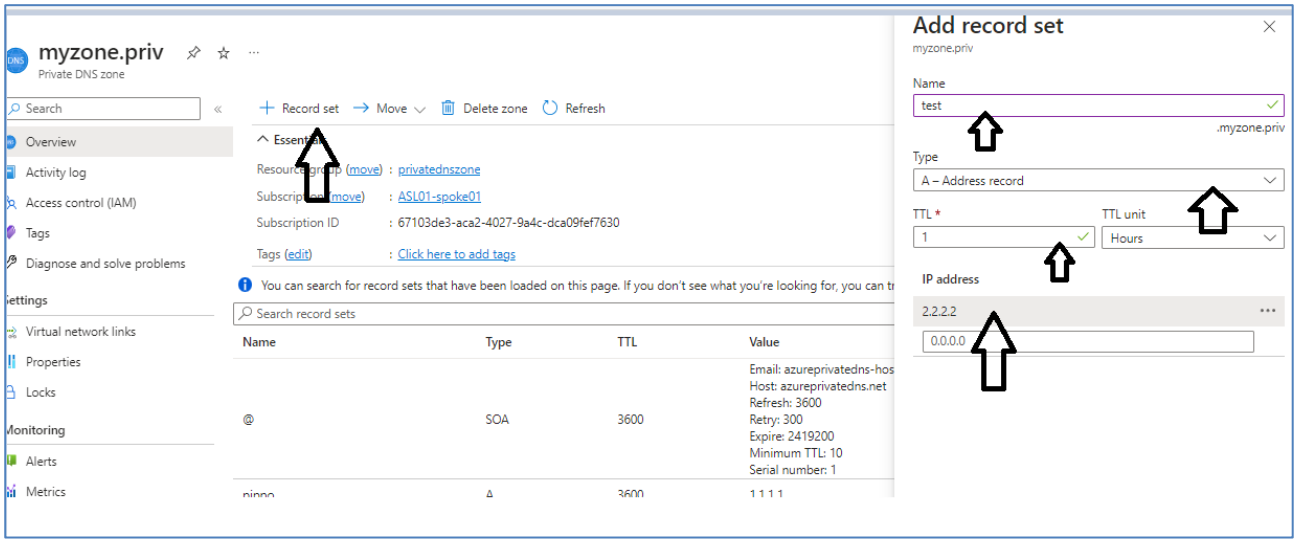


Gestione Record nella DNS Private Zone.

L'utente della PA può gestire i record presenti nella Zona DNS privata.

Ad esempio per inserire un nuovo Record A all'interno di una zona DNS privata occorre fornire:

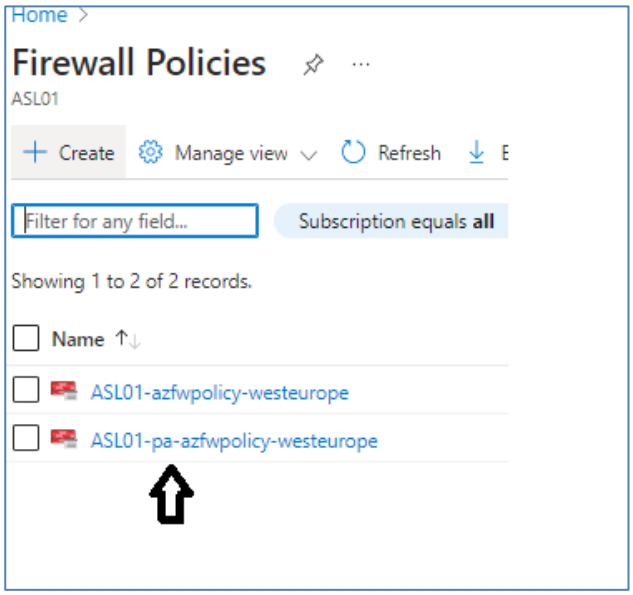
nome, tipo, TTL, IP:



3.2.4 *Gestione Firewall*

Il Firewall Azure che risiede nell'HUB viene controllato dalle Firewall Policy che la PA inserirà per le visibilità che la stessa vorrà inserire per i suoi workload. Queste policy sono gerarchicamente figlie delle Firewall policy in carico al PSN. Pertanto le policy impostate dal PSN non sono modificabili dalla PA e precedono le policy che la pubblica amministrazione, in modo da garantire il livello minimo di sicurezza preimpostato in fase di creazione del tenant.

Le due Firewall Policy possono essere distinte in base al nome, così da facilitarne la lettura ed il riconoscimento. Per ottenere questo risultato sarà sufficiente impostare un prefisso "pa", come nell'esempio qui di seguito:



Il Firewall Dell'HUB supporta due tipi di Policy:

- Network Rules
- Application Rules

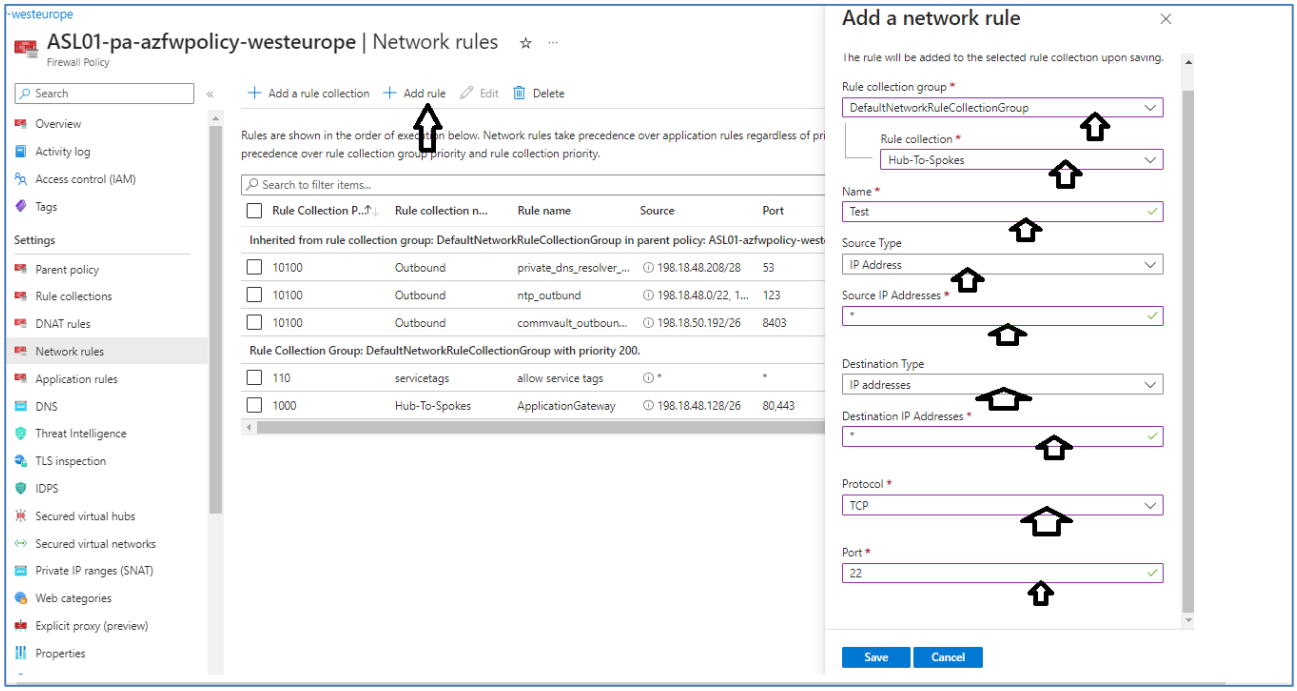
Le Network rules sono regole che lavorano a livello 4 e supportano policy basate su destinazione IP, Service Tags, IP Group e FQDN.
Le Network Policy supportano protocolli TCP, UDP, ICMP o Any.

Una Network Policy va inserita all'interno di una Rule Collection Group di Tipo Network Rule e dentro una Rule Collection.
Se la rule Collection esiste già, può essere aggiunta una Regola alla rule Collection.

Per Inserire una nuova Rule occorre fornire:

- Rule Collection Group
  - Rule Collection
- Name
- Source Type
  - Source
- Destination Type
  - Destination
- Protocol
- Port

Ecco un esempio di una Network policy che consente la porta TCT/22 da qualsiasi IP verso qualsiasi IP



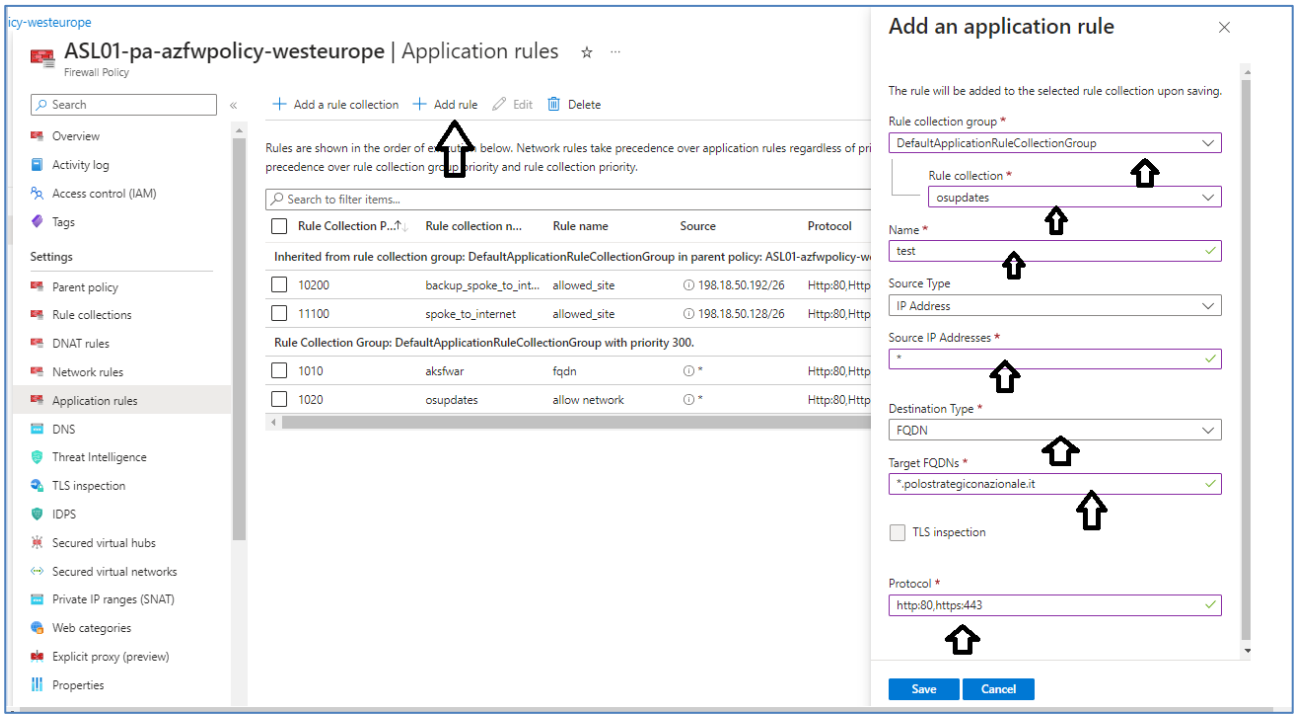
Le Application rules solo regole che lavorano a livello 7 su HTTP e HTTPS e supportano policy basate su destinazione IP, FQDN, FQDN Tags, Web Categories, URL

Una Application rule va inserita all'interno di una Rule Collection Group di Tipo Application Rule e dentro una Rule Collection.
Se la rule Collection esiste già, può essere aggiunta una Regola alla rule Collection

Per Inserire una nuova Rule occorre fornire:

- Rule Collection Group
  - Rule Collection
- Name
- Source Type
  - Source
- Destination Type
  - Destination
- Protocol

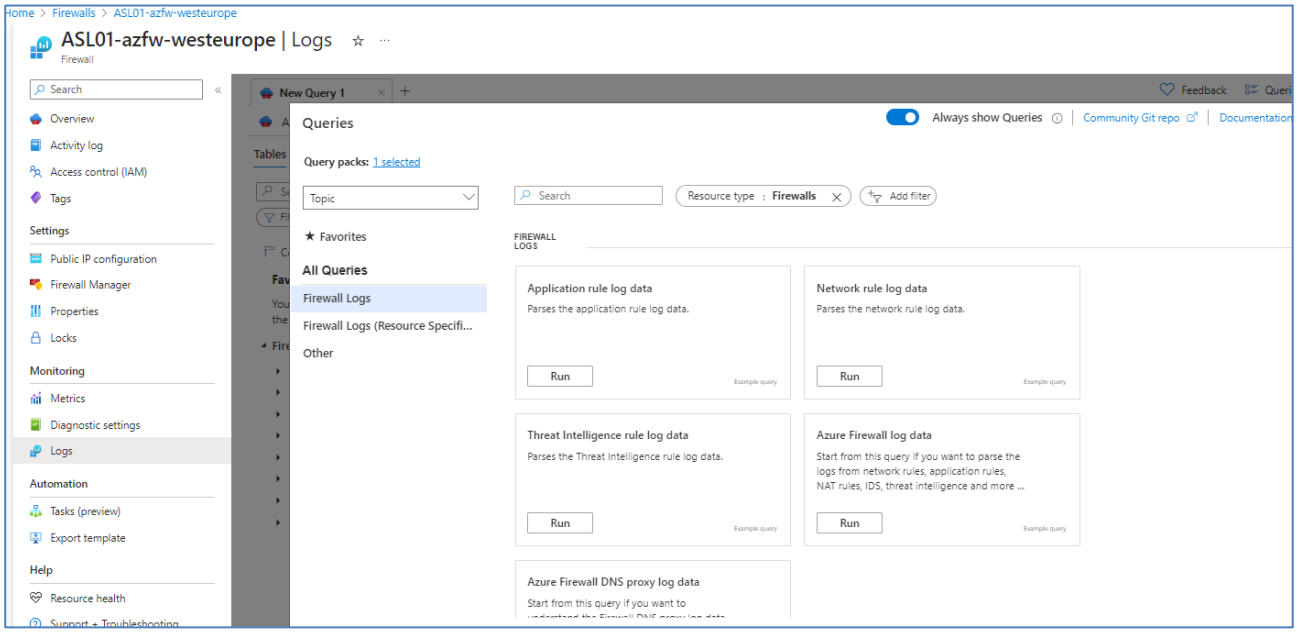
Di seguito un esempio di una application policy che consente HTTP:80 e HTTPS:443 verso *.polostrategiconazionele.it :



Nel firewall è presente anche una sonda IDS.

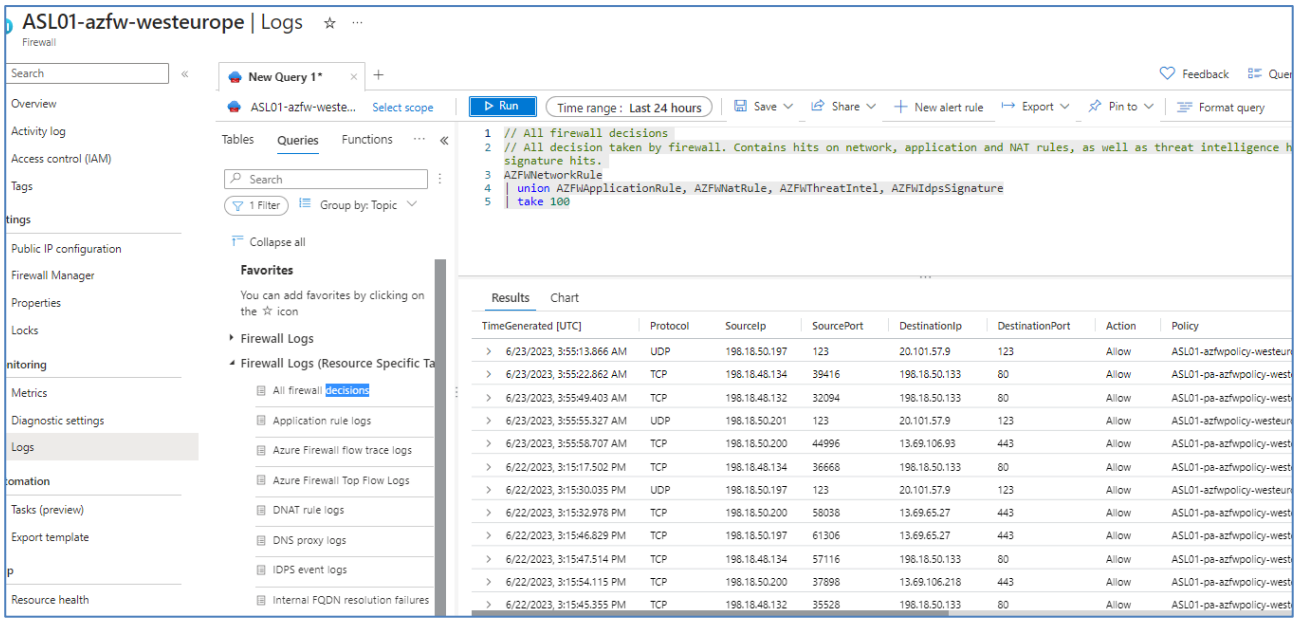
Consultazione dei log del Firewall

Per consultare i log del Firewall andare sul firewall e selezione logs;

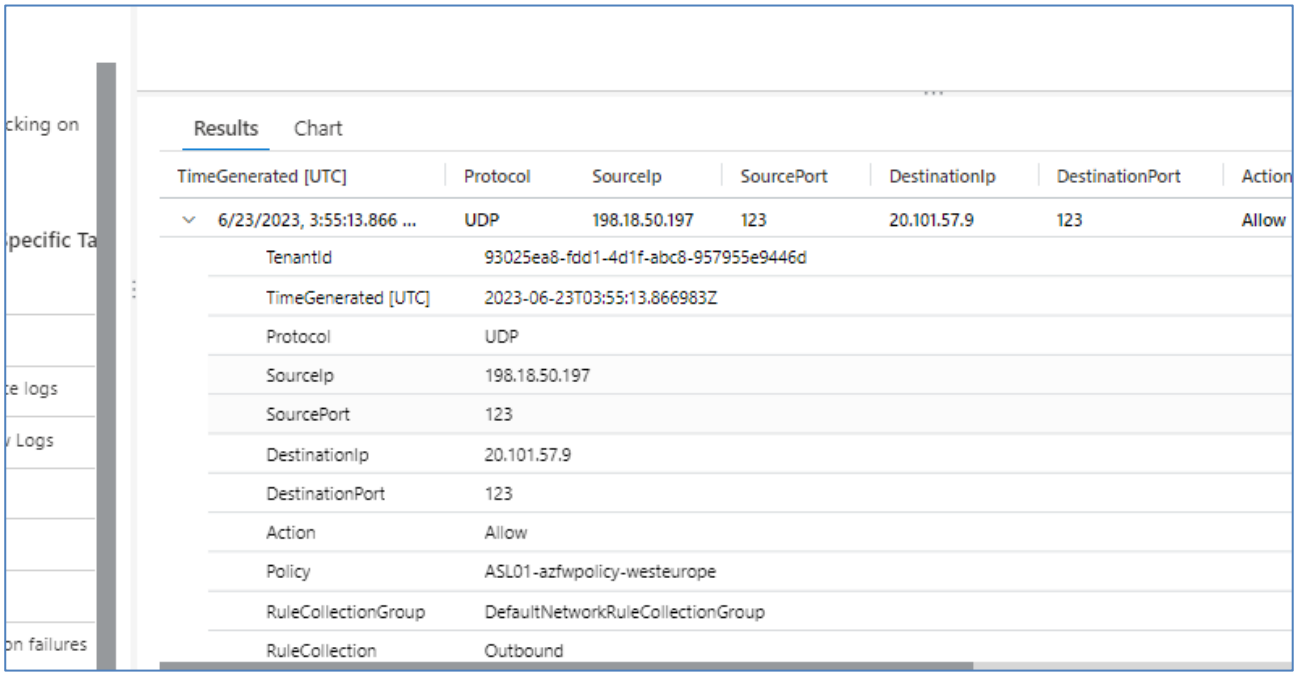


L'utente può consultare i logs attraverso query precostituite o tramite query custom.

Di seguito un estratto della query precostituita "All Firewall Decisions":



di cui il dettaglio:



La documentazione ufficiale di Azure Firewall e consultabile a questo link:

[What is Azure Firewall? | Microsoft Learn]

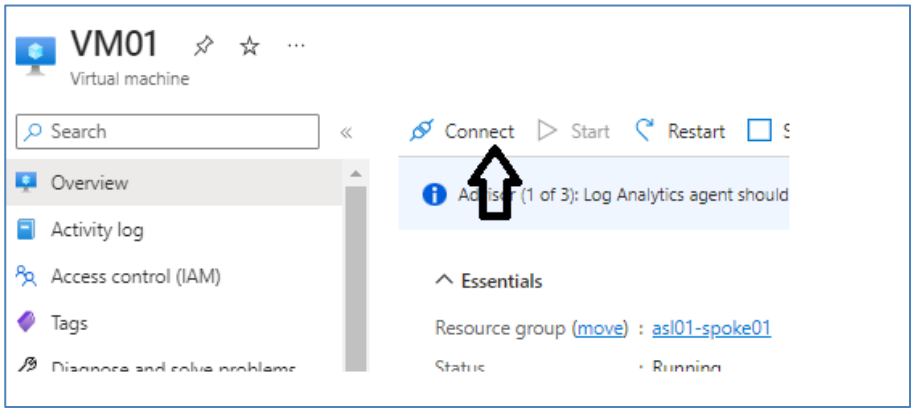
3.2.5 Bastion

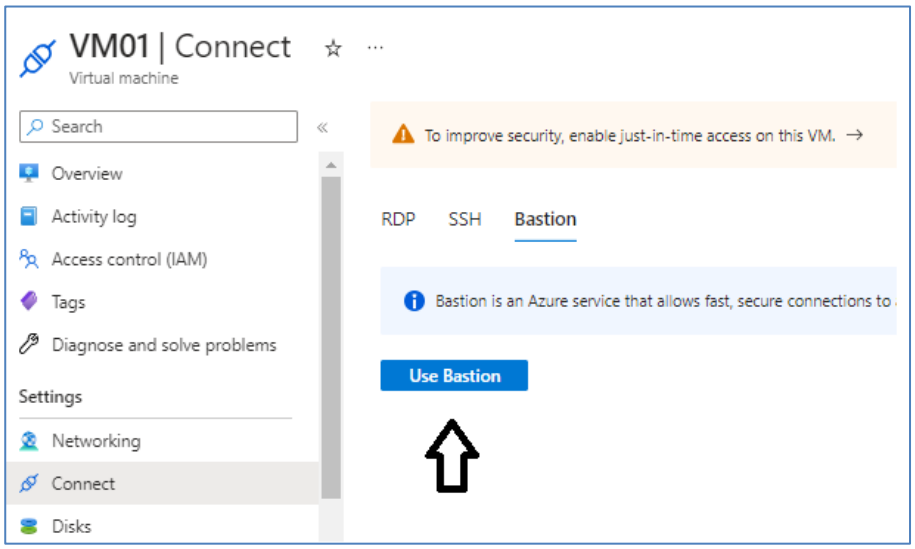
L'accesso amministrativo alle VM presenti negli Spoke è garantito dalla soluzione attraverso l'utilizzo di Bastion.

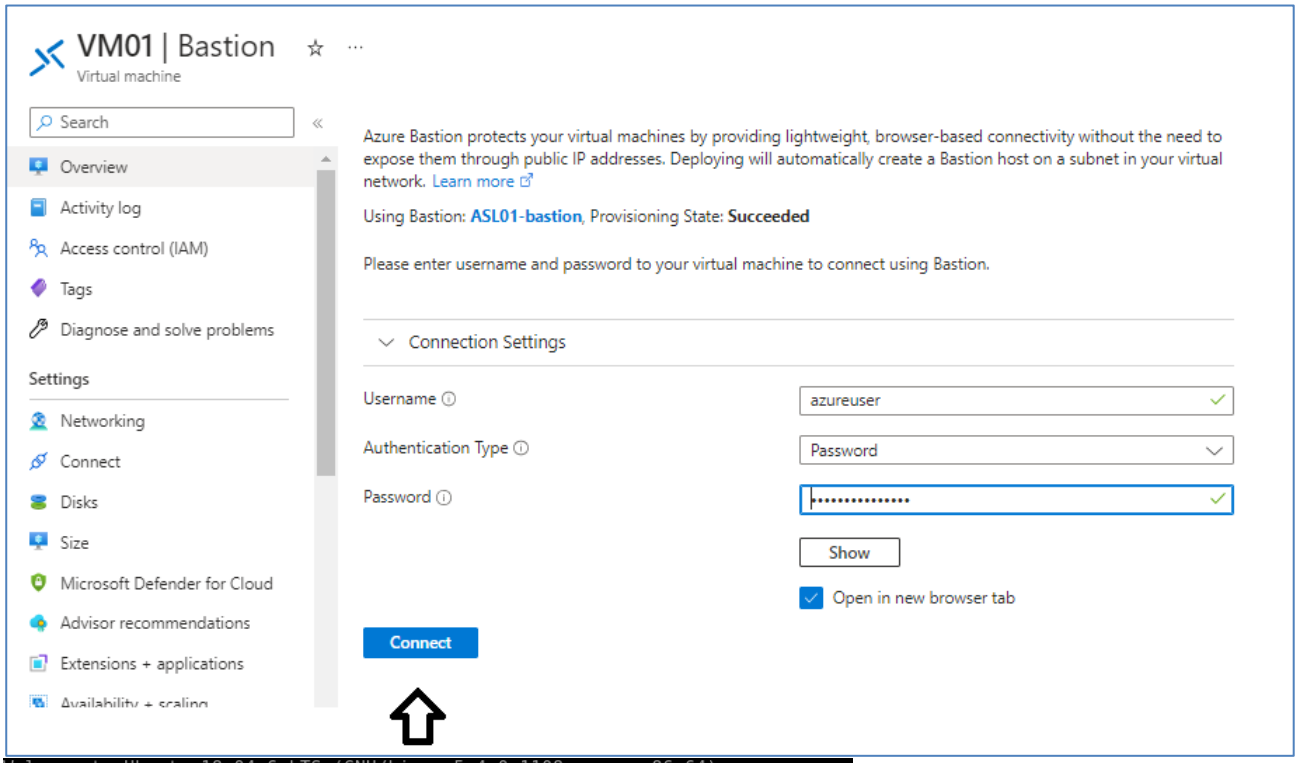
Per utilizzare il Bastion occorre selezione la VM desiderata, cliccare su Connect e poi su "Use Bastion" e fornire le credenziali per l'accesso.

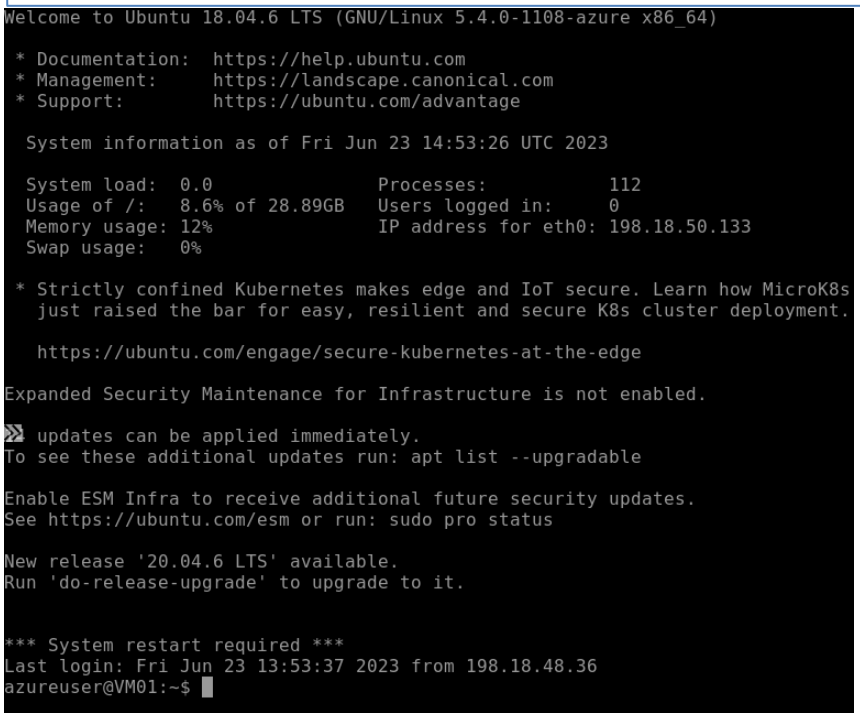
Si aprirà una nuova finestra con l'accesso alla VM

di seguito un esempio:


VM01
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Connect
Start
Restart
Essentials
Resource group (move) : asl01-spoke01


VM01 | Connect
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Disks
To improve security, enable just-in-time access on this VM.
RDP
SSH
Bastion
Bastion is an Azure service that allows fast, secure connections to
Use Bastion





La documentazione ufficiale di Azure Bastion e consultabile a questo link:

[About Azure Bastion | Microsoft Learn]

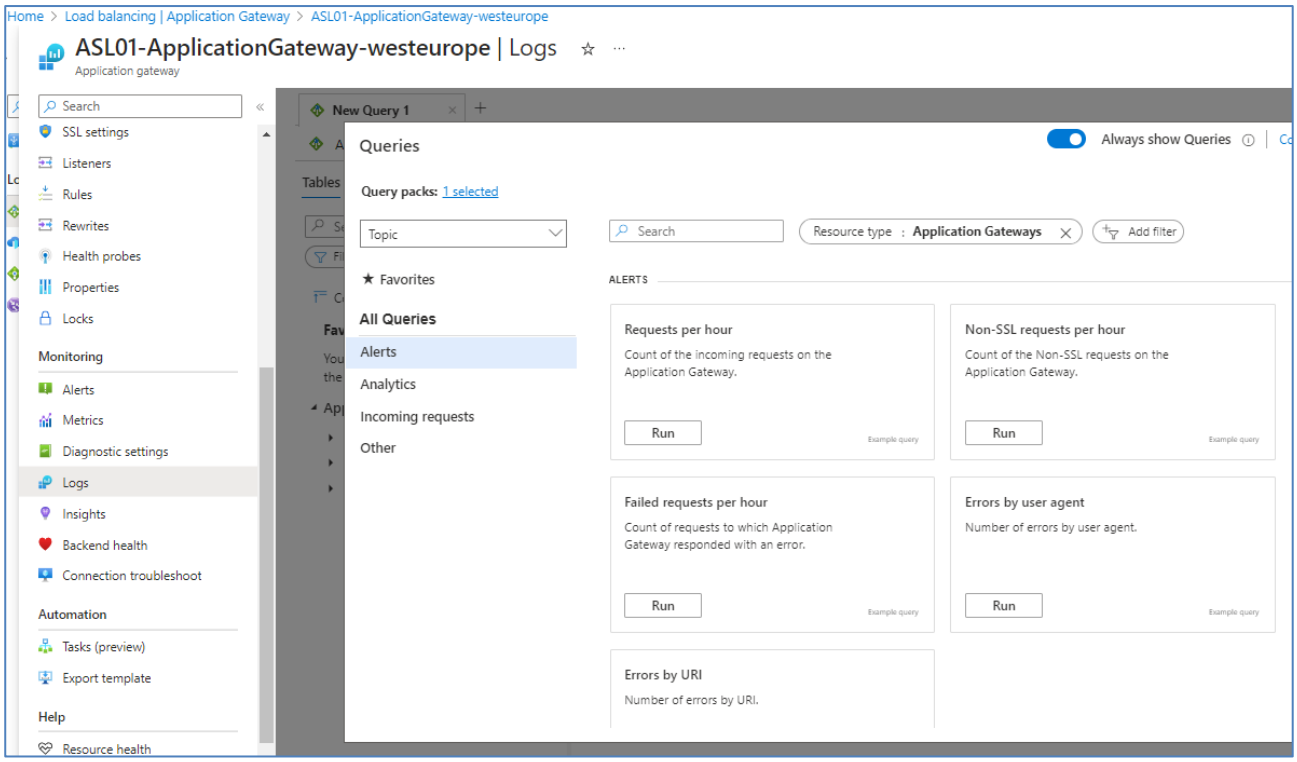
3.2.6 Esposizione Web server con WAF

I servizi Web della PA sono esposti tramite Sull'Application Gateway che si avvale del WAF (Web Application Firewall) per controllare la bontà degli accessi effettuati.

La configurazione dell'Application Gateway e del WAF è competenza del PSN; la PA ha la facoltà di accedere ai Log.

Ogni richiesta di modifica della configurazione dell'Application Gateway o del WAF sarà fatta via opportuna Service Request al PSN.

Per consultare i log dell'Application Gateway andare sull'Application Gateway e selezione logs:



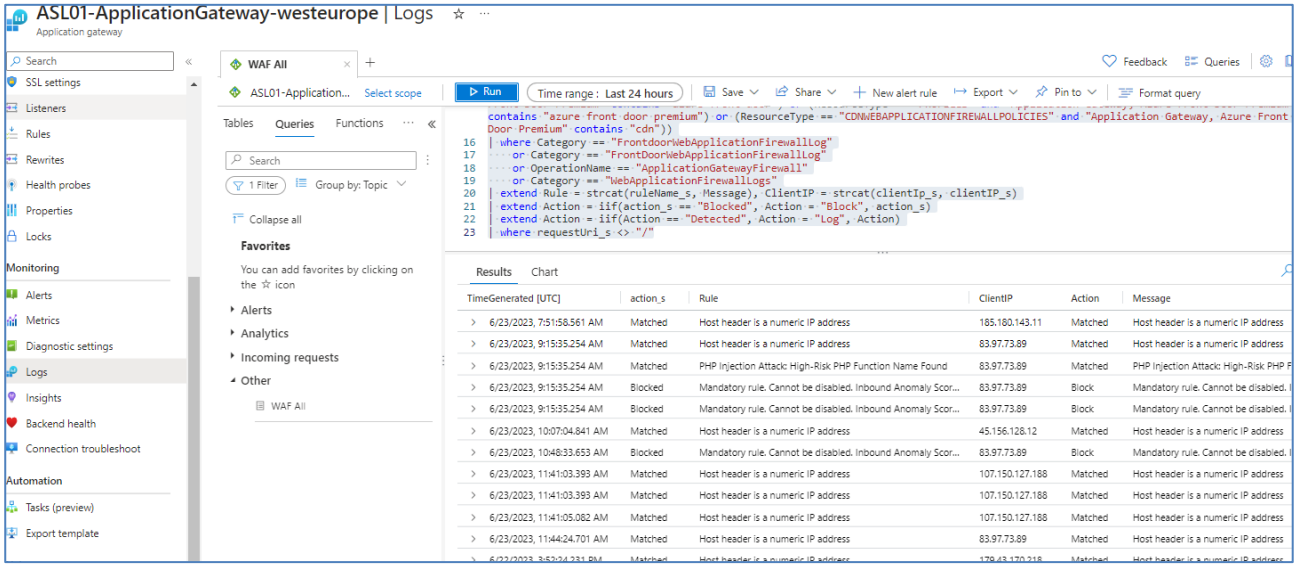
L'utente può consultare i logs attraverso query precostituite o tramite query custom.

Ad esempio per consultare i log del WAF usare la query:

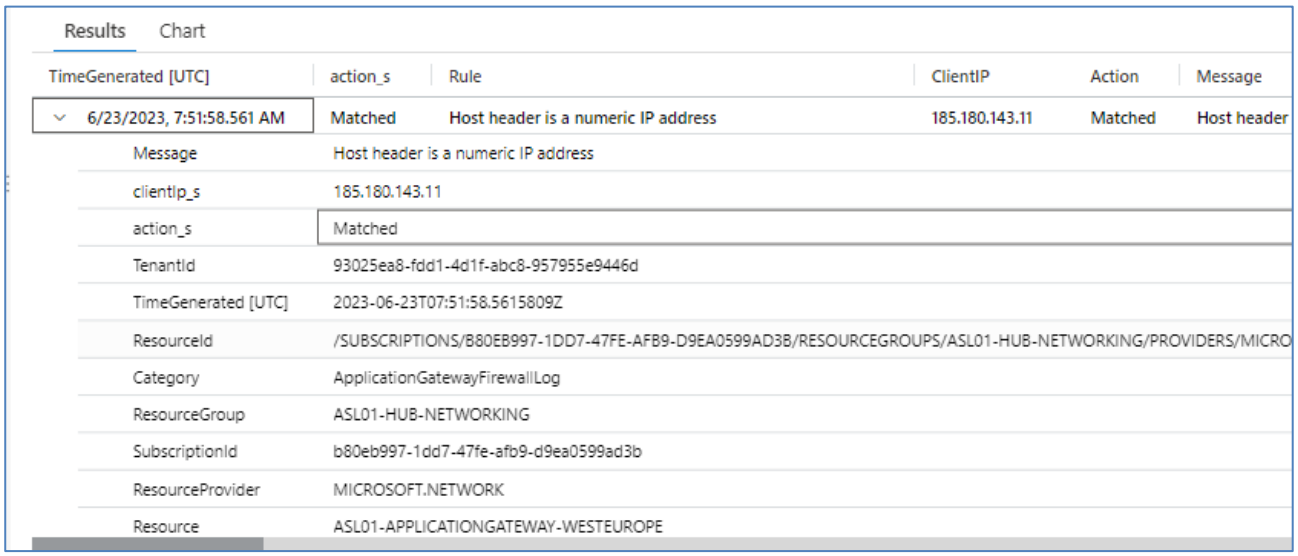
```
let FakeData = (datatable (
    Message: string,
    ruleName_s: string,
    clientIp_s: string,
    clientIP_s: string,
    action_s: string,
```

```
    transactionId_s: string,

    trackingReference_s: string

) [

    "", "", "", "", "", "", ""

]);

FakeData

| union AzureDiagnostics

| where (ResourceType == "APPLICATIONGATEWAYS" or ResourceType == "FRONTDOORS" or ResourceType == "PROFILES" or ResourceType == "CDNWEBAPPLICATIONFIREWALLPOLICIES")

    and ("Application Gateway, Azure Front Door Premium" == "All" or (ResourceType == "APPLICATIONGATEWAYS" and "Application Gateway, Azure Front Door Premium" contains "application gateway") or (ResourceType == "FRONTDOORS" and "Application Gateway, Azure Front Door Premium" contains "azure front door") or (ResourceType == "PROFILES" and "Application Gateway, Azure Front Door Premium" contains "azure front door premium") or (ResourceType == "CDNWEBAPPLICATIONFIREWALLPOLICIES" and "Application Gateway, Azure Front Door Premium" contains "cdn"))

| where Category == "FrontdoorWebApplicationFirewallLog"

    or Category == "FrontDoorWebApplicationFirewallLog"

    or OperationName == "ApplicationGatewayFirewall"

    or Category == "WebApplicationFirewallLogs"

| extend Rule = strcat(ruleName_s, Message), ClientIP = strcat(clientIp_s, clientIP_s)

| extend Action = iif(action_s == "Blocked", Action = "Block", action_s)

| extend Action = iif(Action == "Detected", Action = "Log", Action)

| where requestUri_s <> "/"
```

Di seguito un esempio di log:



di cui un dettaglio:



La documentazione ufficiale di Azure Application Gateway e consultabile a questo link:

[What is Azure Application Gateway | Microsoft Learn]

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.

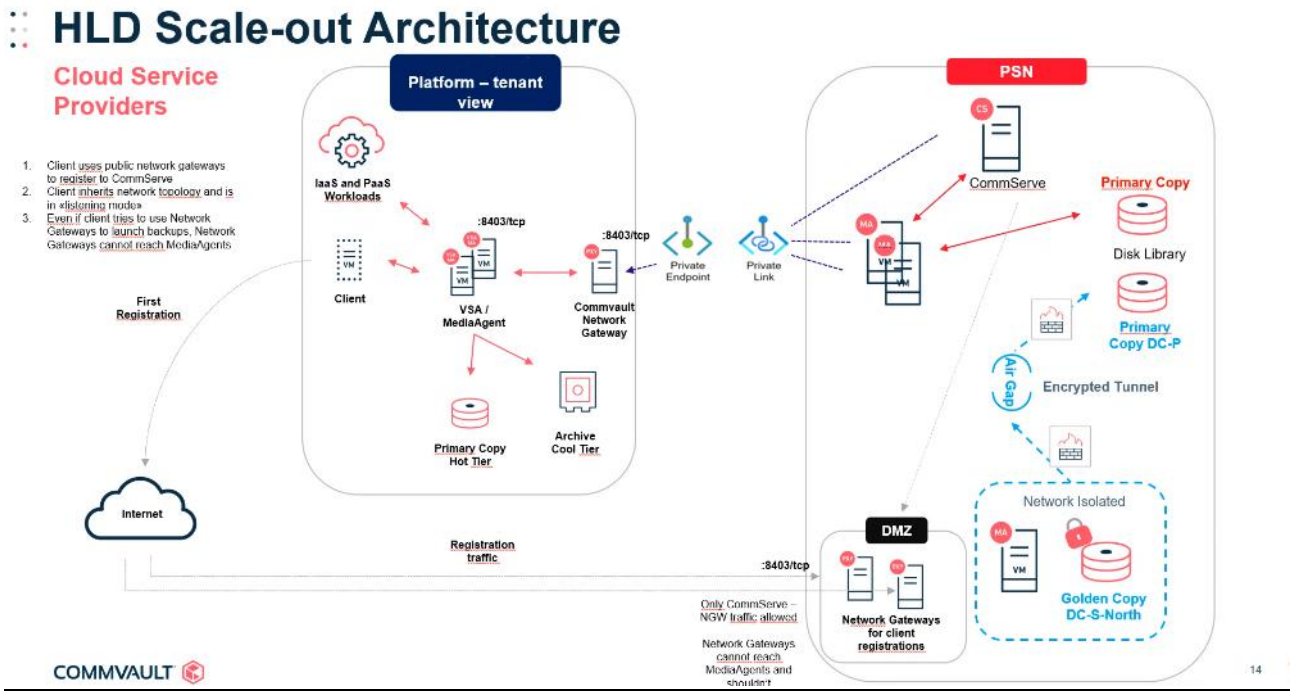


Figura 2: HLD Commvault

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 Azure 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 Azure avviene sfruttando la tecnologia Private Service Connect.

Nel dettaglio, l'infrastruttura on-premises del PSN raggiunge la PSN ORG su Azure attraverso una VPN.
Da questa 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 Azure. Grazie alla soluzione Azure di Private Link / Private EndPoint il CommServe può comunicare con il Network Gateway all'intenro delle PA.
Nell'esempio, per comodità, i ruoli di NG, MA e AN sono eseguiti da una singola VM.

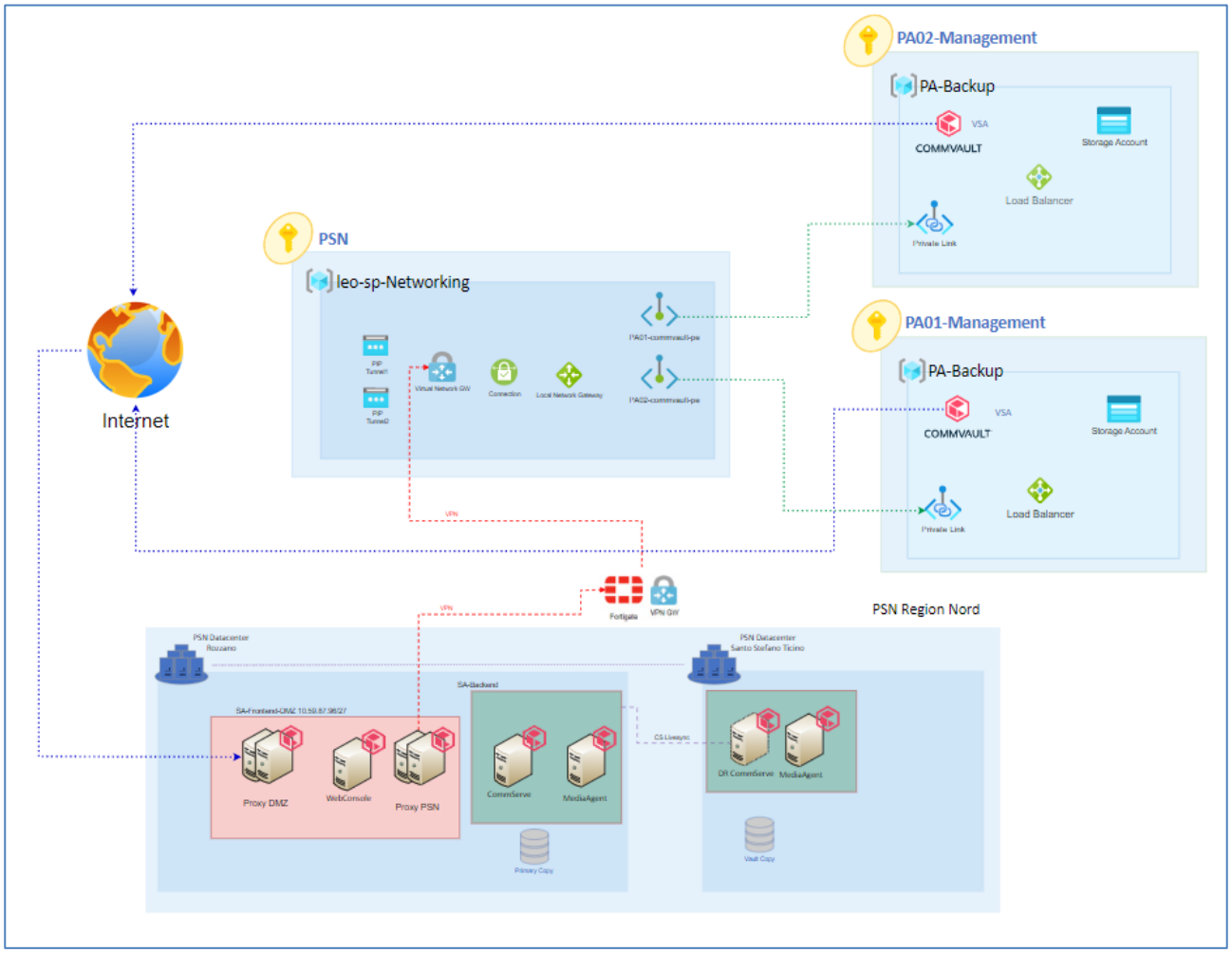


Figura 3: Dettaglio Flussi

Il flusso Private Link / Private Endpoint è unidirezionale. Parte dal CommServe on-prem e arriva alla VSA su Azure.
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 Private Link / Private Endpoint .

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.

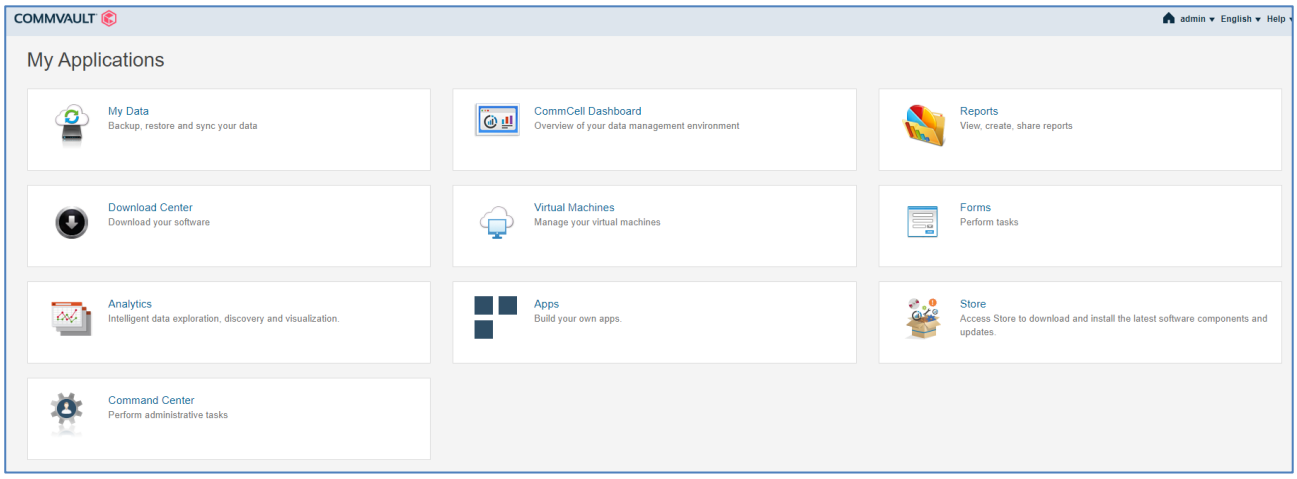
3.3.2 *Struttura del Portale: Dashboard*

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

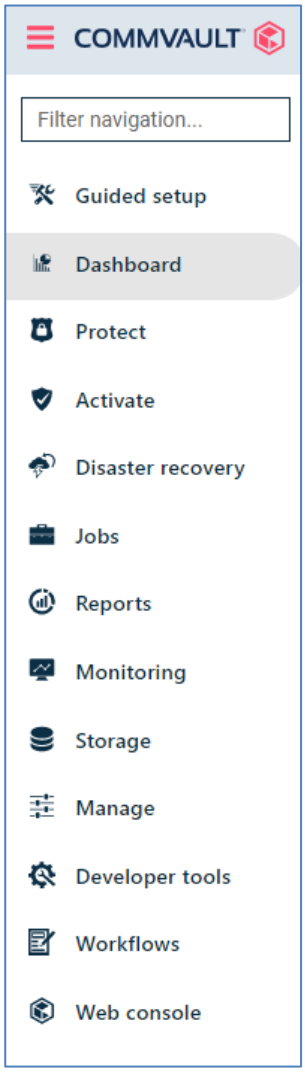
https://baas-nord.console.polostrategiconazionale.it

La login 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"
Il command Center è il portale da cui si eseguiranno tutte le configurazioni.
Di seguito il menu di navigazione

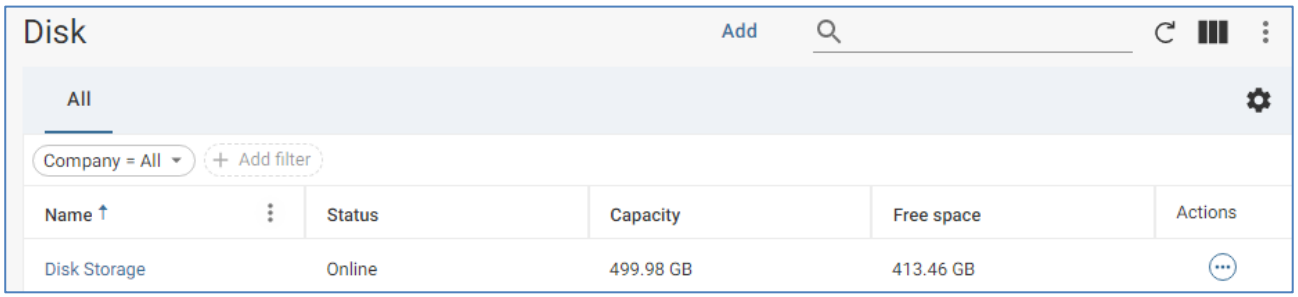


Ogni voce del menu attiva funzionalità o sottomenu aggiuntivi. Nei capitoli seguenti sono indicati i dettagli dei menu.
Per alcune risorse sono preconfigurati oggetti in fase di onboarding mentre su altre la PA avrà la possibilità di definirne di nuove.

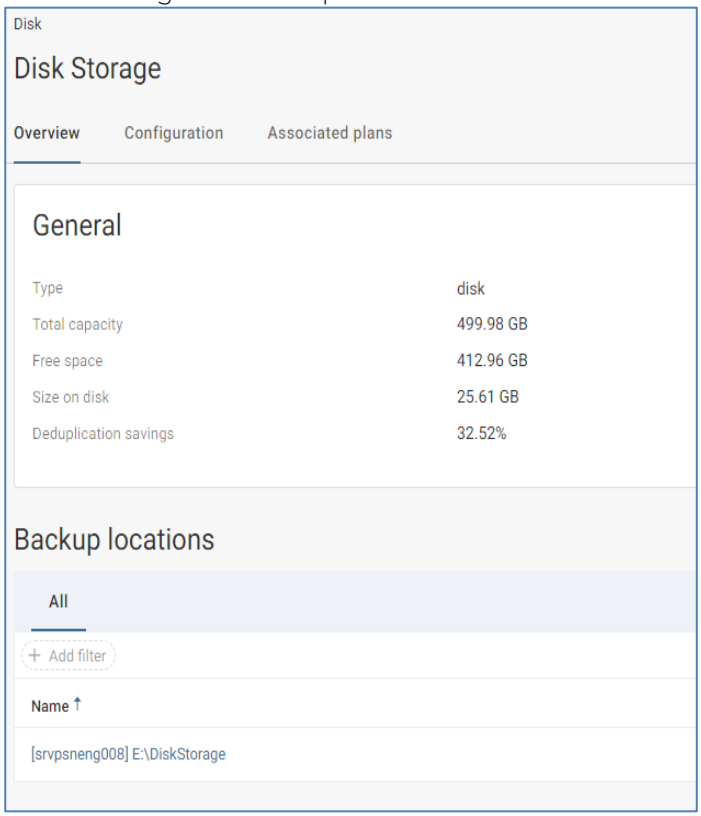
3.3.3 *Storage*

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.

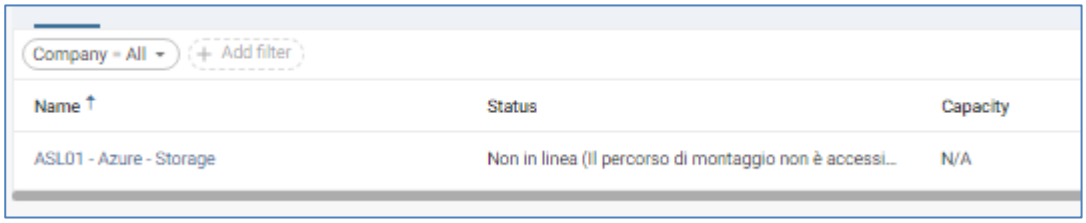
Lo storage di tipo Disk indica lo spazio disco On Premesis presso il datacenter PSN. Verrà poi utilizzato dai Plan che prevedono la replica del dato.



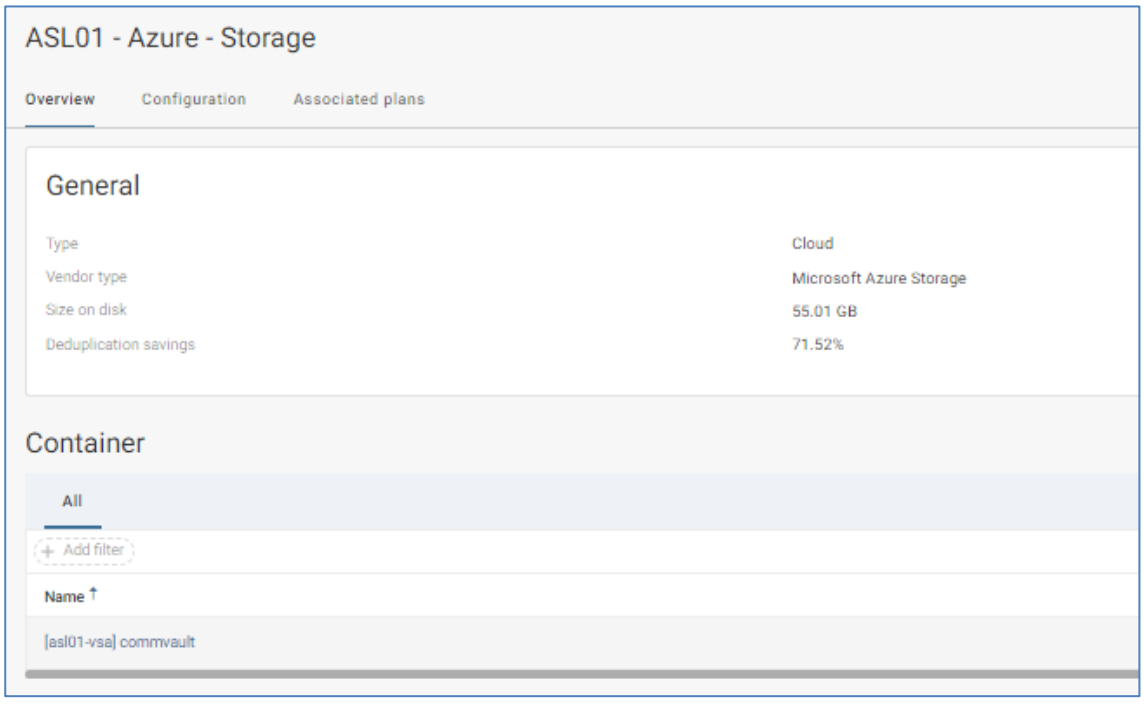
Il disk storage è situato presso il DC di PSN e risiede su uno storage di backend.



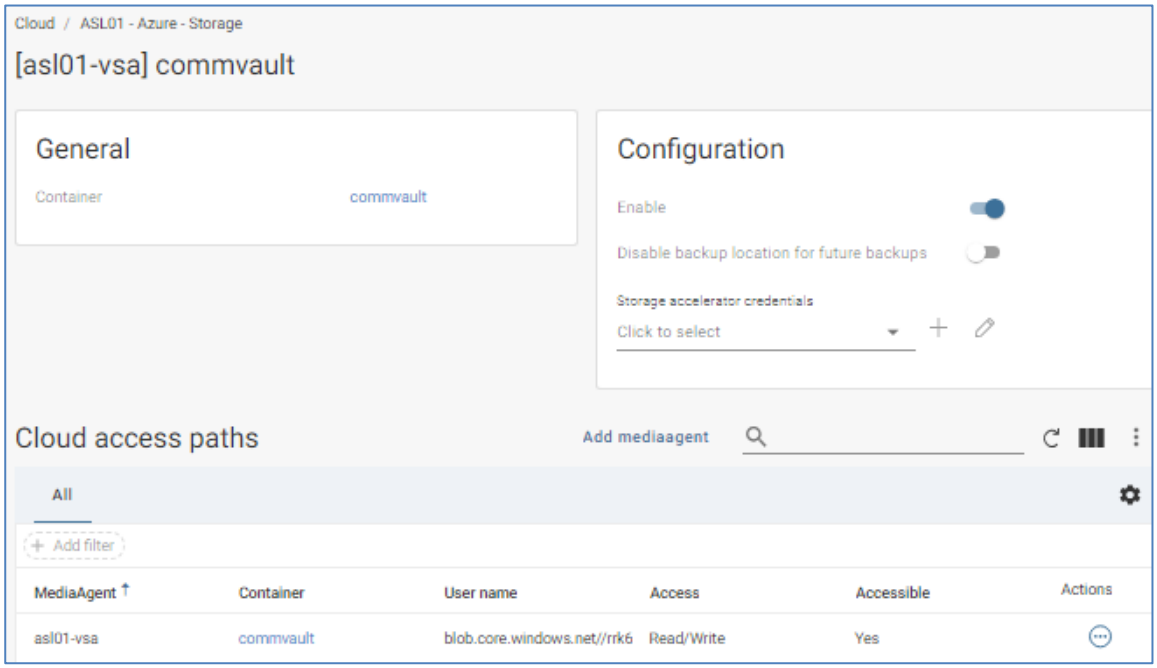
Lo storage di tipo cloud è uno Azure Storage Account definito sul tenant della PA all'interno del resource group dedicato al backup



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



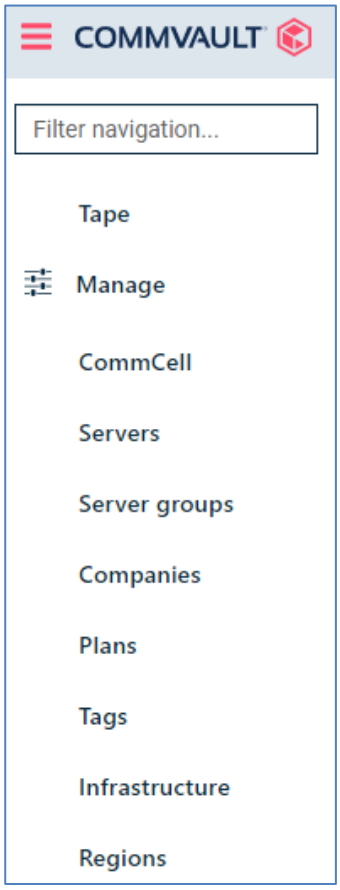
Su Azure Storage Account viene definito un Container gestito dal VSA

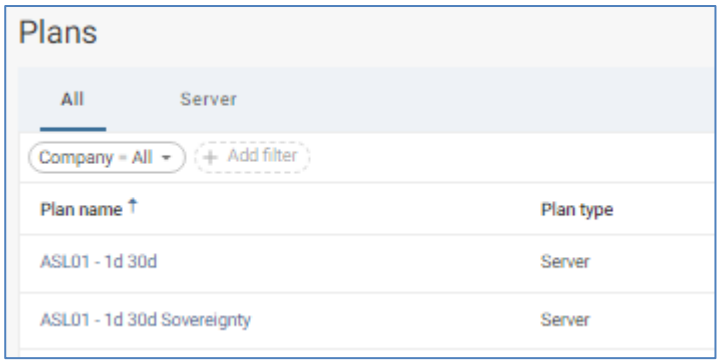


Il VSA utilizzerà le Azure API per accedere al Container per memorizzare i backup.
Per la parte storage la PA non dovrà eseguire modifiche.

3.3.4 Plan

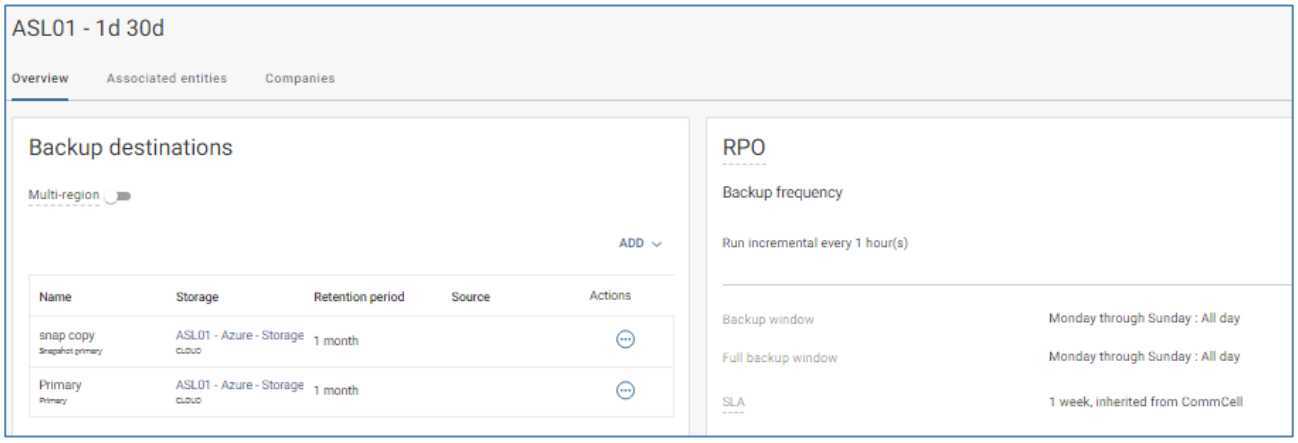
I Plan sono preconfigurati con due tipologie di default ma la PA può crearne di nuovi secondo le sue necessità.
Dal menu Manage => Plans sono visibili i plan configurati



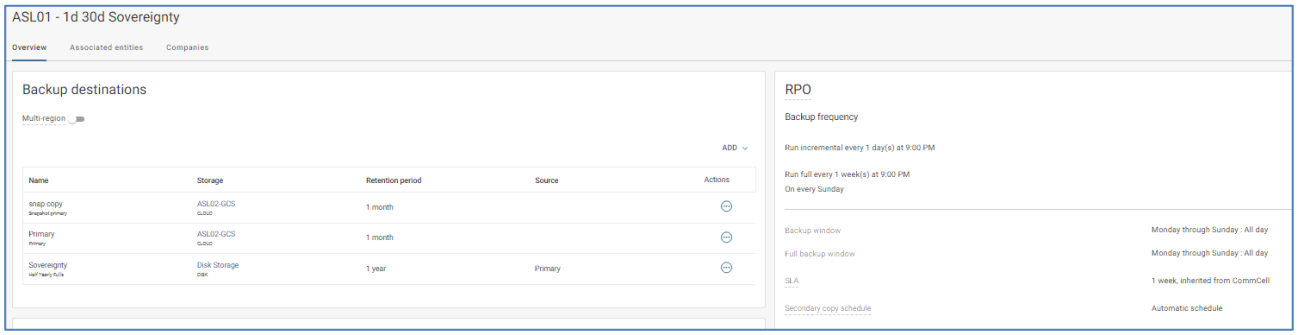


Vengono preconfigurati due Plan.

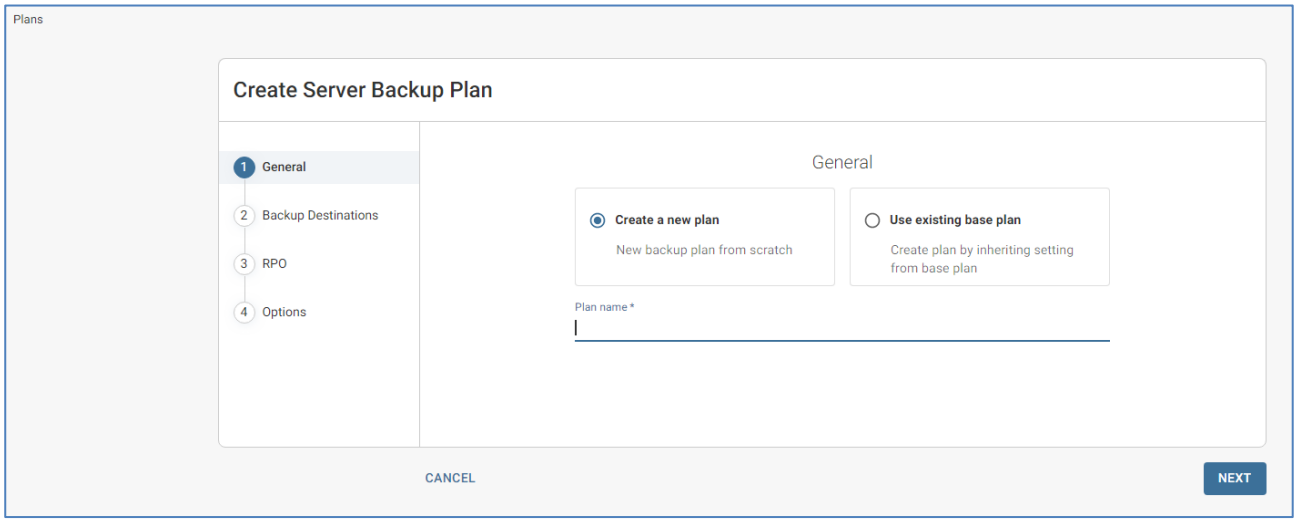
Il primo plan “ASL01 - 1d 30d” è configurato con la backup destination sullo storage Cloud Azure Storage Account con retention di 30 giorni.
Il RPO è impostato a 24 ore attraverso un backup giornaliero alle 21.00



Il secondo Plan “ASL01 - 1d 30d Sovereignty” viene usato per avere repliche sul DC On Premises. Sono configurati due storage di destinazione, la copia primaria viene salvata sul Container 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.



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

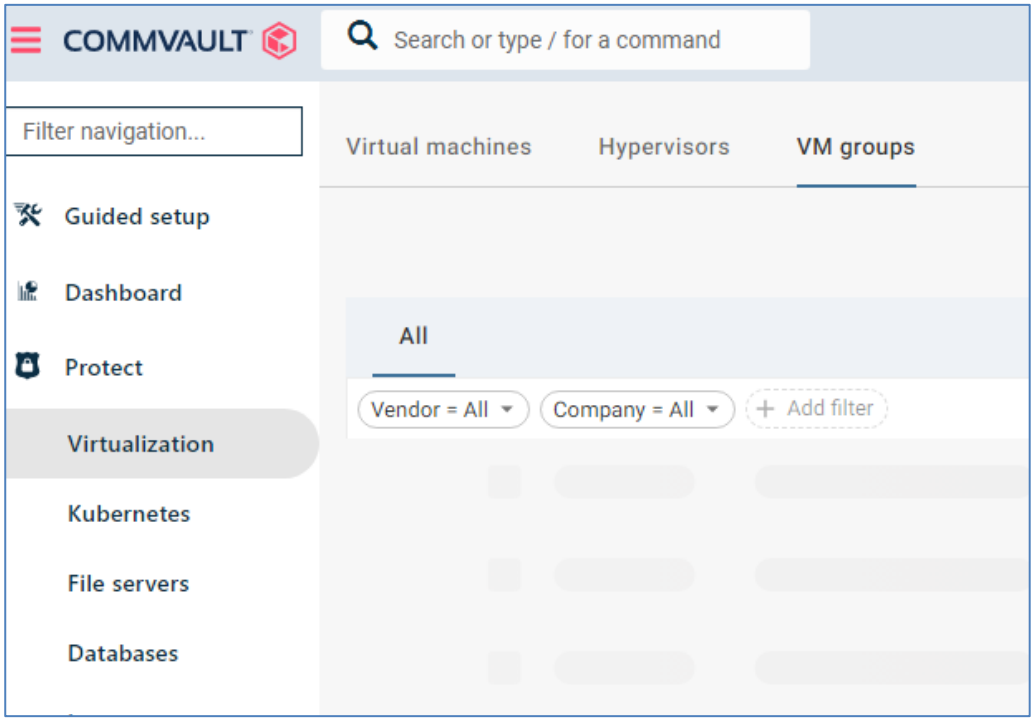


I campi da compilare sono: nome, destinazione e RPO.

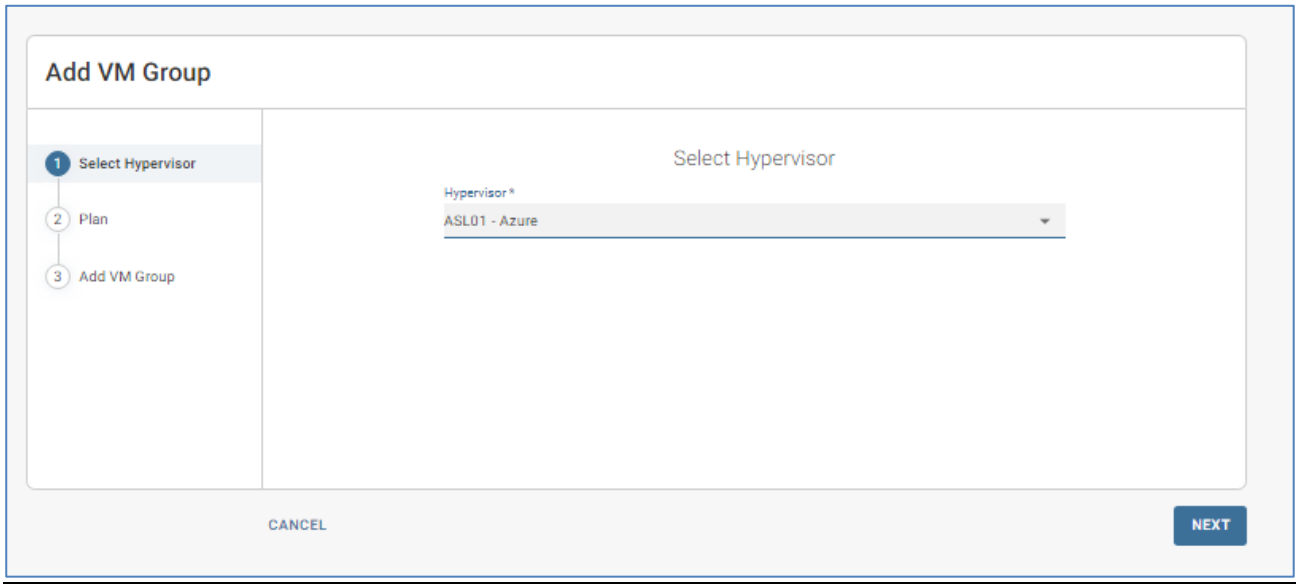
3.3.5 *VM Groups*

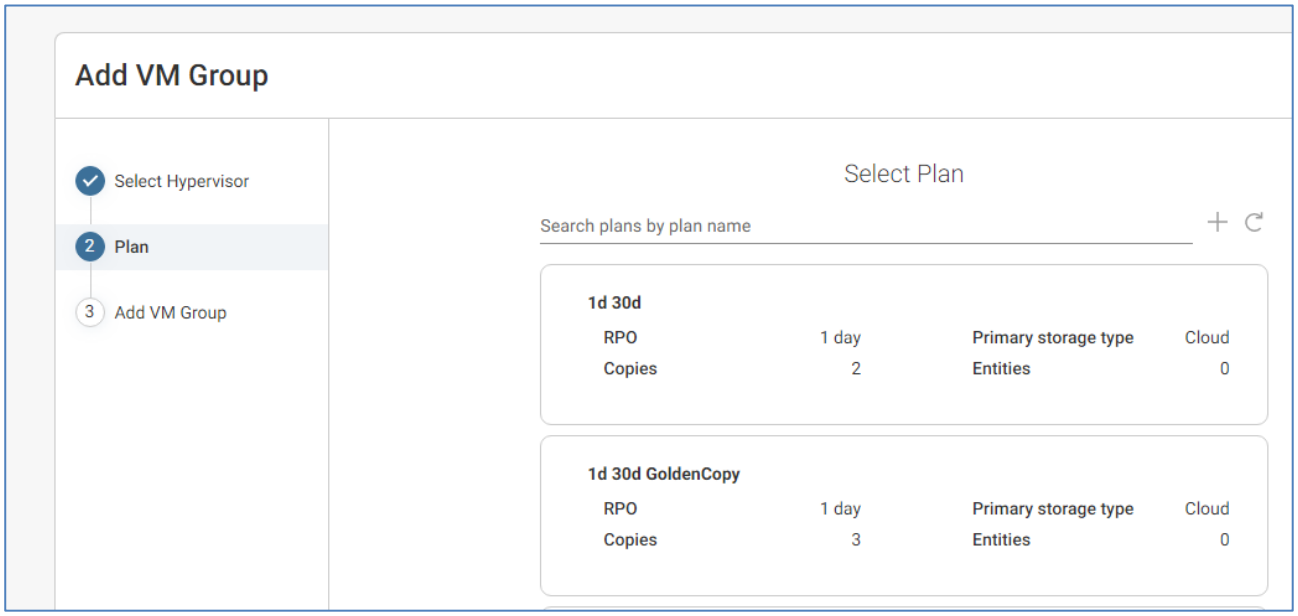
I VM Groups sono in gestione della PA. I VM Groups associamo le entità dell'hypervisor Azure (quindi le VM) a un Plan.

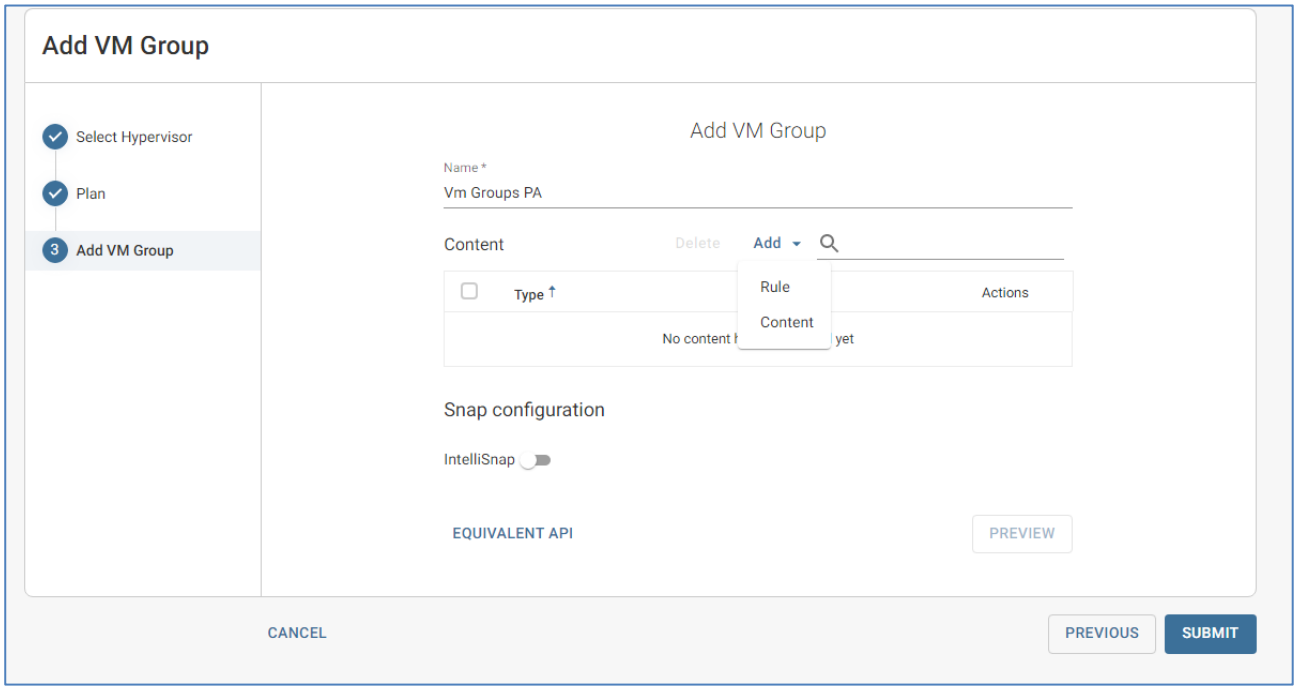
Dal menu Protect/Virtualization/VM Groups



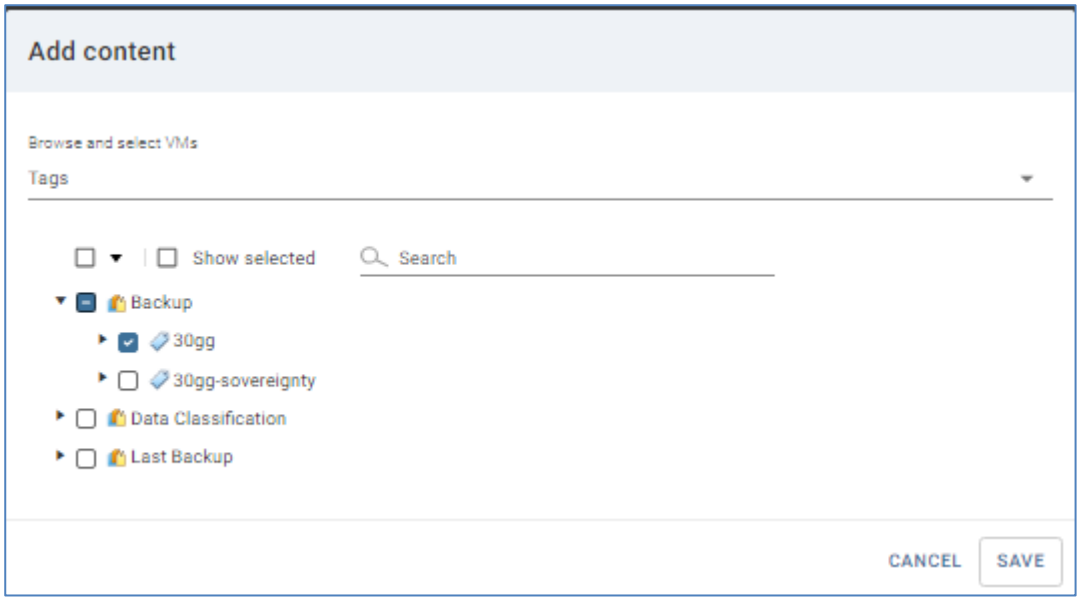
Selezionare add VM Groups e inserire nel Wizards l'hypervisor Azure , il Plan e le VM


Add VM Group
1 Select Hypervisor
2 Plan
3 Add VM Group
Select Hypervisor
Hypervisor *
ASL01 - Azure
CANCEL
NEXT

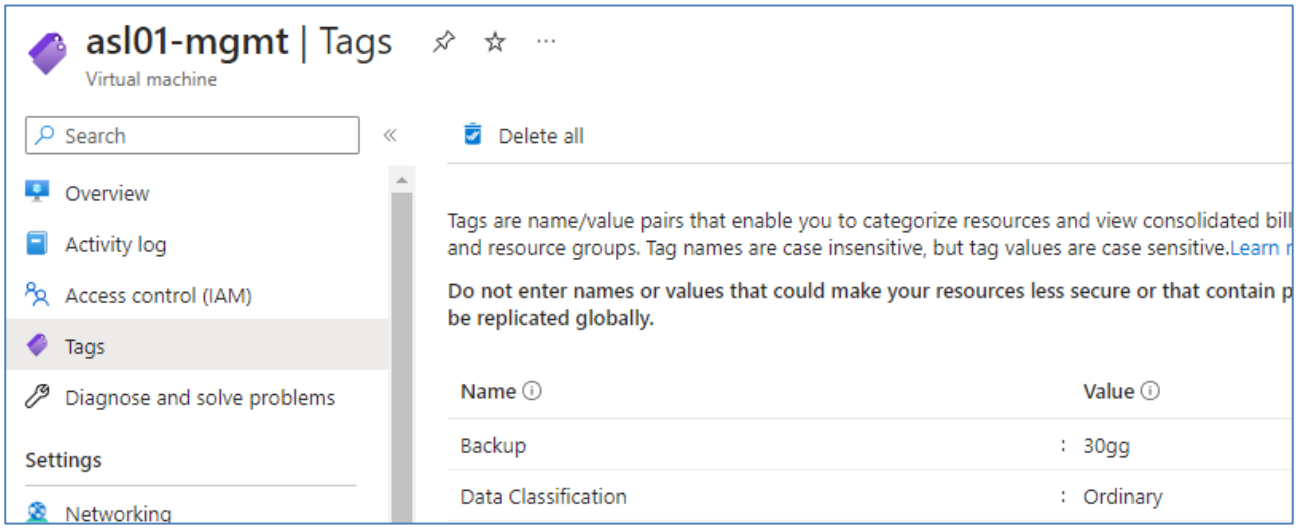

Add VM Group
Select Hypervisor
2 Plan
3 Add VM Group
Select Plan
Search plans by plan name
1d 30d
RPO 1 day
Primary storage type Cloud
Copies 2
Entities 0
1d 30d GoldenCopy
RPO 1 day
Primary storage type Cloud
Copies 3
Entities 0



Le VM possono essere inserite in modalità statica selezionandole dai Project, oppure utilizzando Rules dinamiche.
Particolarmente consigliate sono le Rules basate su la TAG associate alla VM Azure.

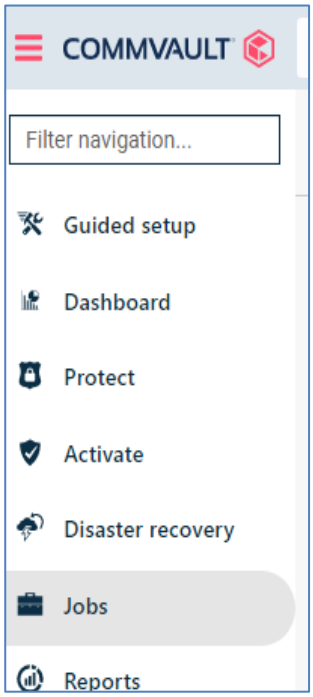


In questo esempio vengono selezionate dal VM Groups tutte le VM con il tag 30gg

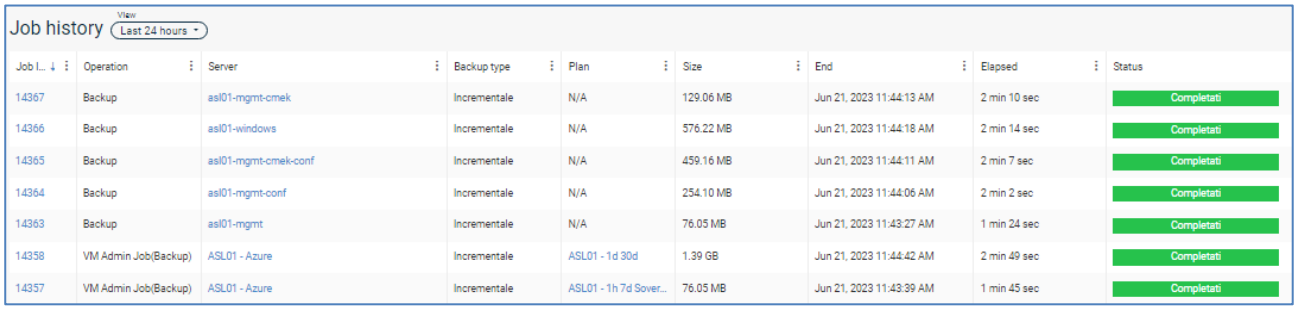


3.3.6 *Jobs*

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

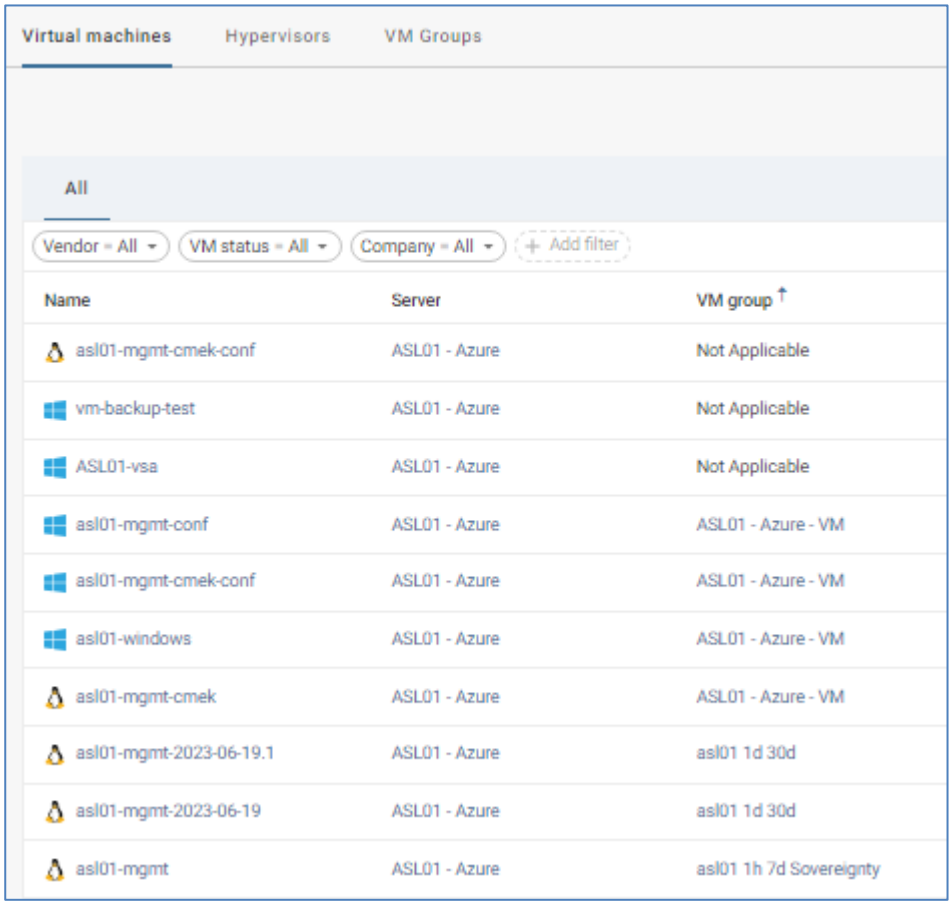


I JOB possono essere analizzati nel dettaglio selezionando con il mouse il numero di job

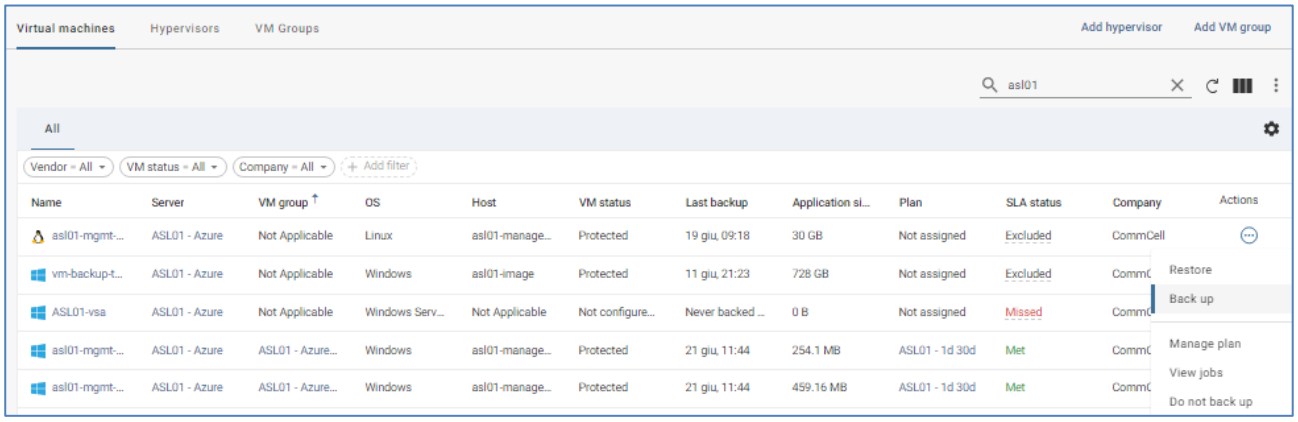


3.3.7 *Manual Backup*

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



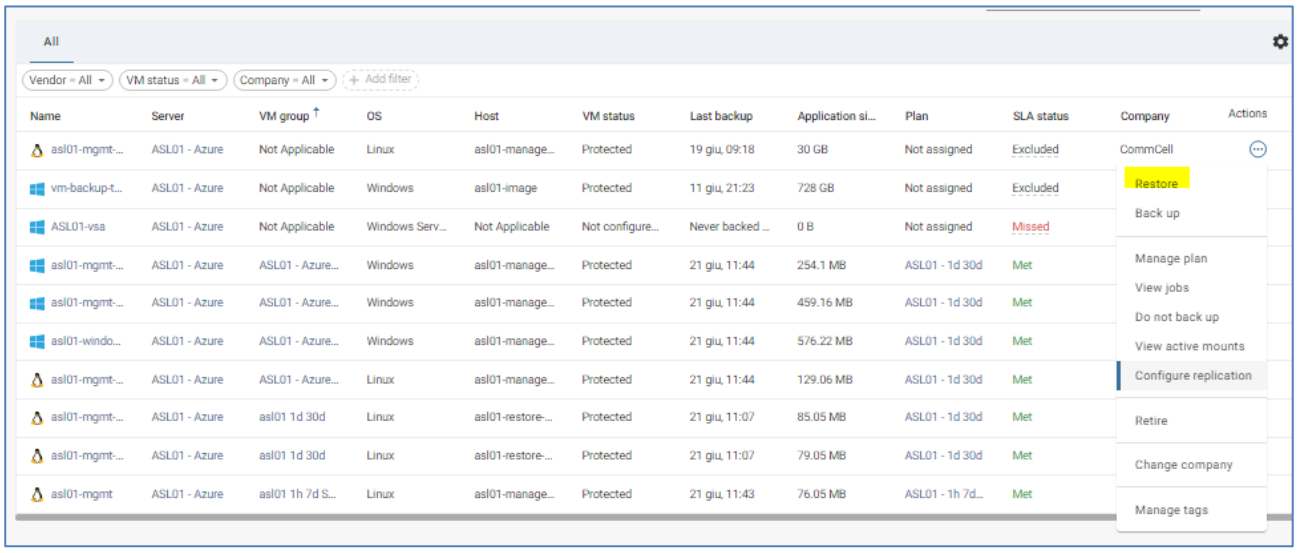
Selezionare la VM ed eseguire il backup.



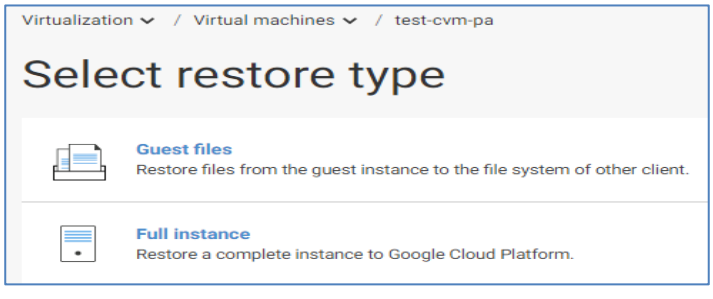
Seguire l'esecuzione del backup dal menu JOB.

3.3.8 *Restore*

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



Scegliere il tipo di restore

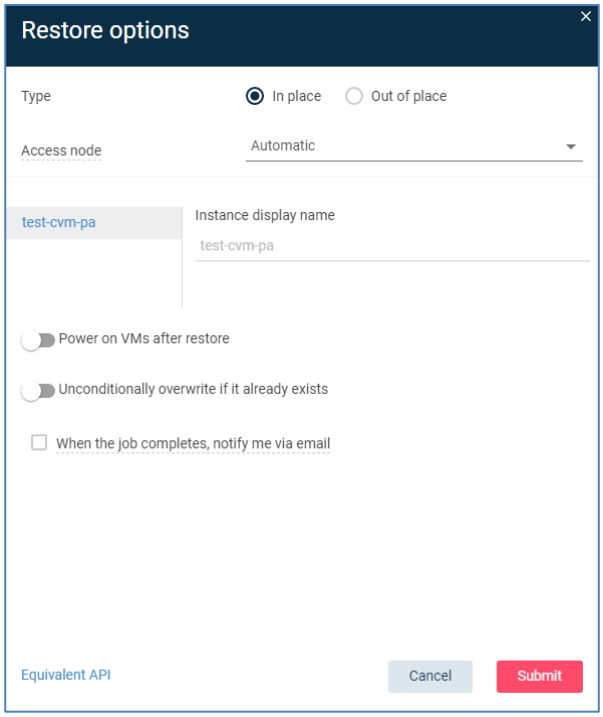


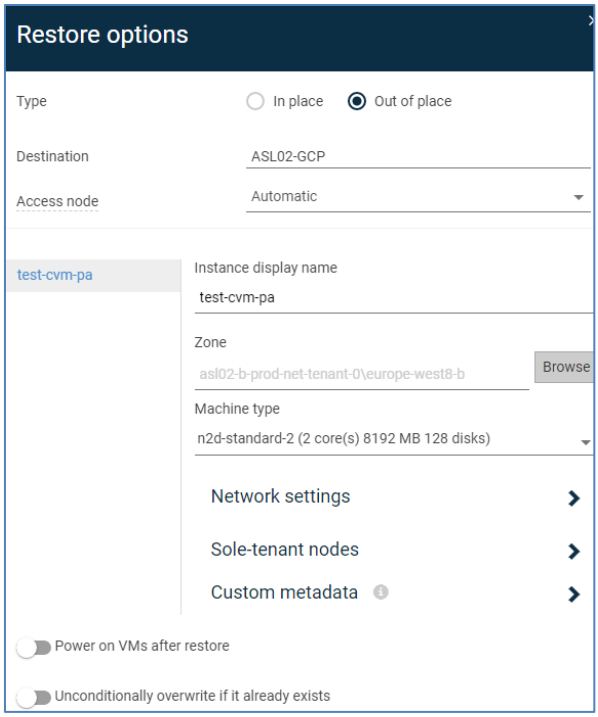
E procedere seguendo il wizard.

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.





3.3.9 *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 Azure VMs

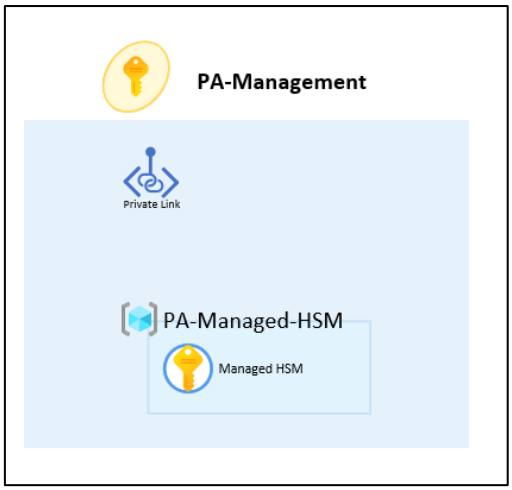
Cloud Feature Support for Azure

Protecting Azure VMs with Commvault

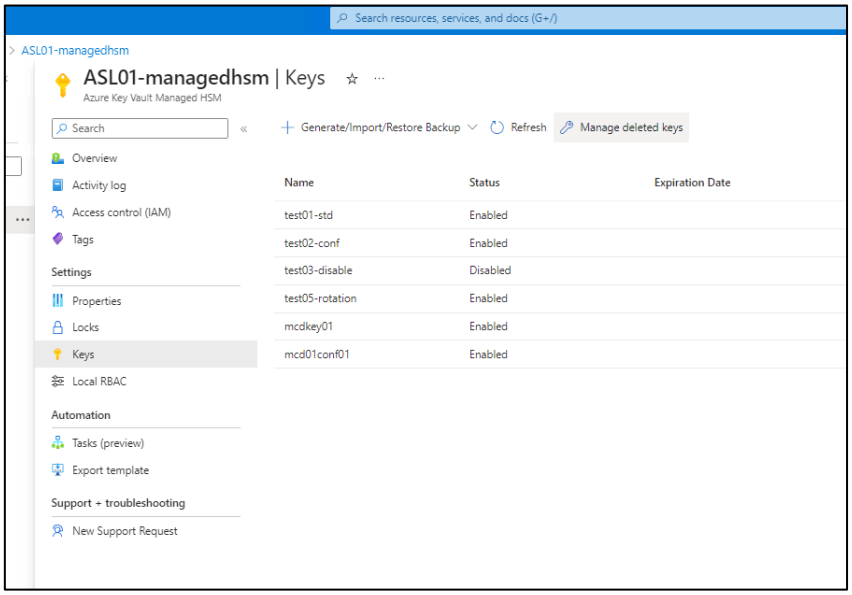
3.4 KMS

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-premises nei datacenter del PSN, escludendo così, dalla gestione delle chiavi di cifratura, il CSP.

Nell'alberatura delle risorse che costituiscono il tenant della PA, all'interno della Subscription "Management", è presente il Resource Group "Managed-HSM" riservato alla gestione delle chiavi.



Al suo interno viene istanziata la risorsa Managed HSM 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 Managed-HSM 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 utilizzabili per la cifratura del layer applicativo (produzione, sviluppo e test), esempio:

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

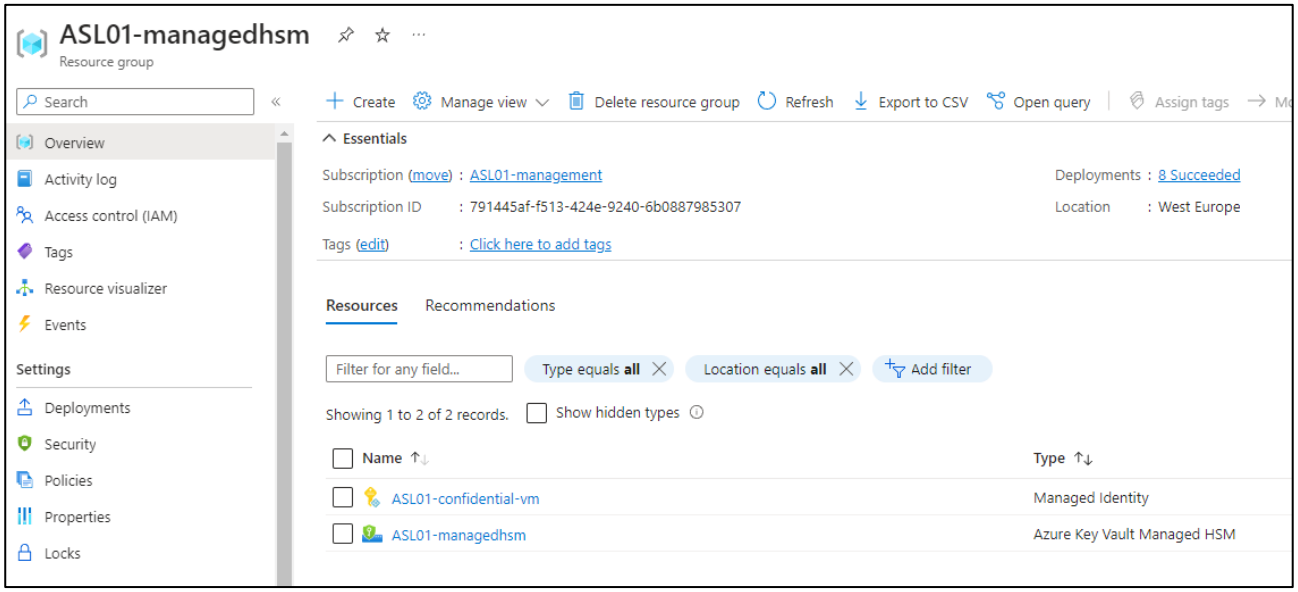
È comunque possibile per la PA richiedere, tramite il servizio di ticketing dedicato del PSN, chiavi aggiuntive per specifici workload applicativi, indicando le caratteristiche della chiave da generare (nome, algoritmo di encryption, size, durata), nonché la destinazione d'uso.

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.

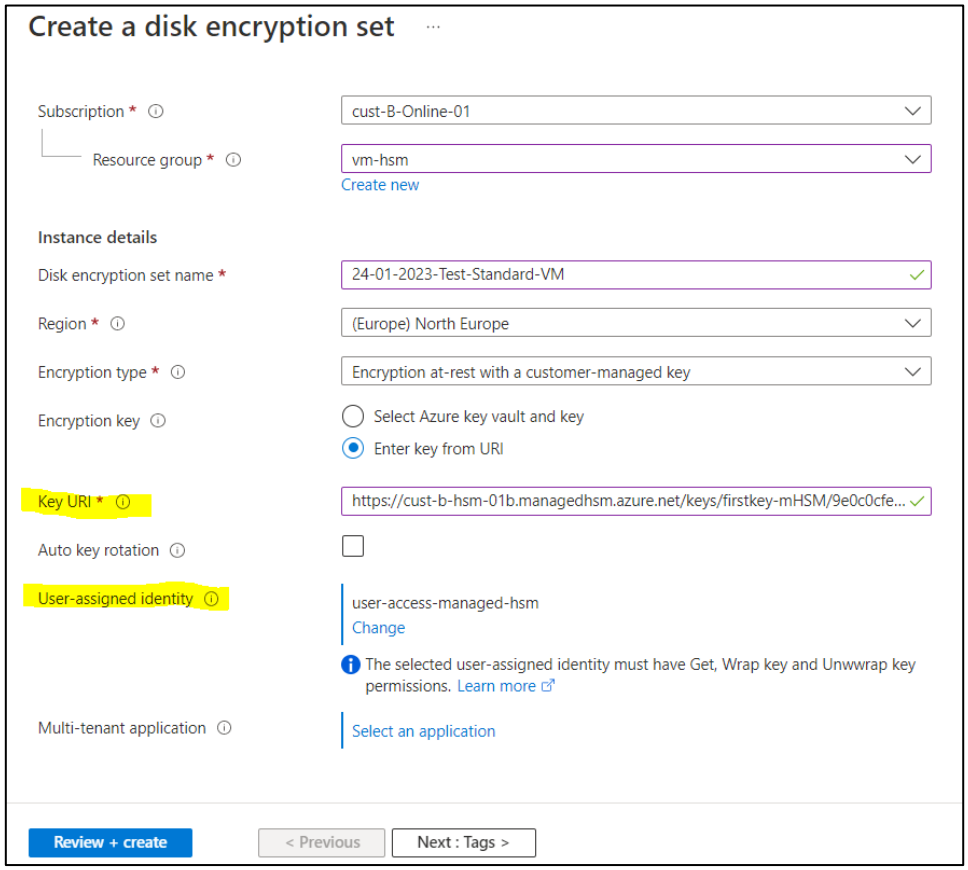
Il Managed-HSM contenente le chiavi di cifratura della PA è visibile da tutto il tenant, attraverso un'Azure Managed Identity appositamente creata, istanziata all'interno del Resource Group "Managed-HSM", consentendo l'accesso alle chiavi per i differenti workload.

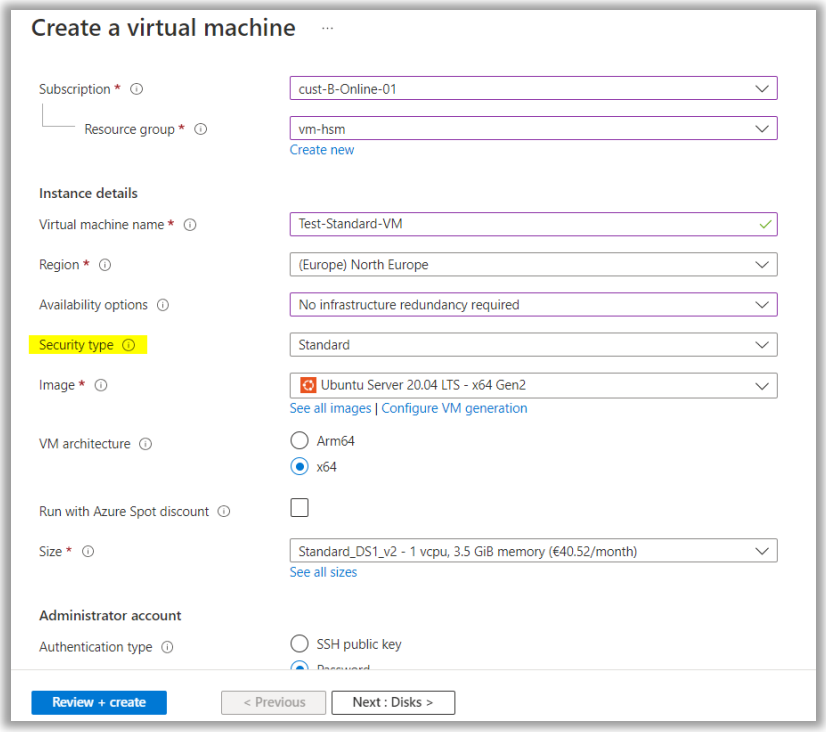


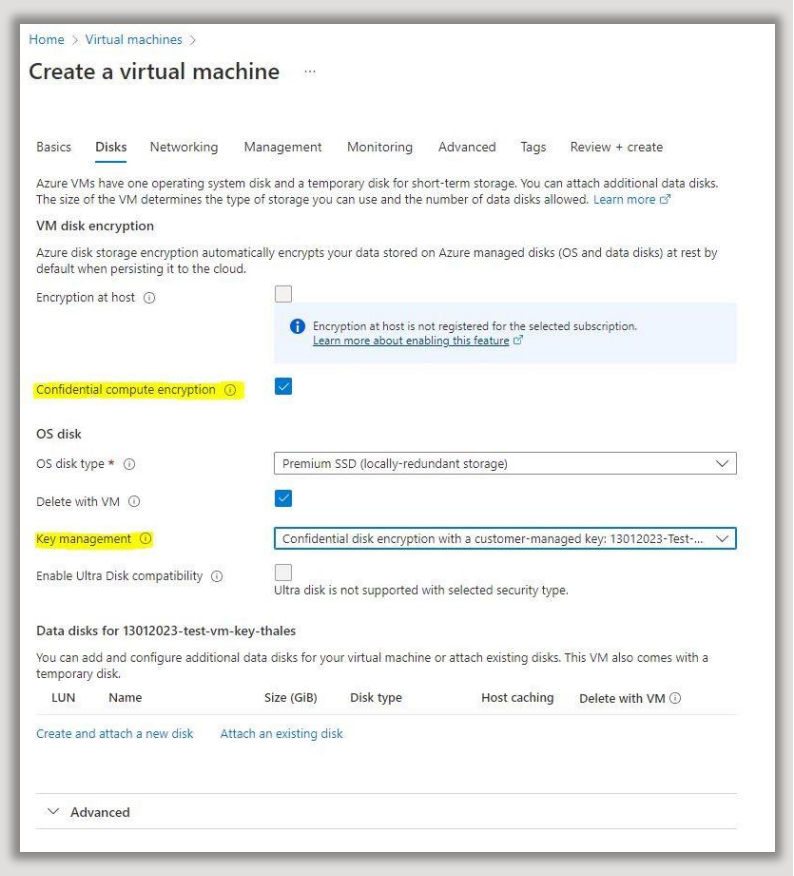
3.4.1 *Utilizzo Chiave esterna per una Virtual Machine*

Le chiavi di cifratura mantenute all'interno del Managed-HSM sono gestite attraverso la risorsa Azure Disk Encryption Set, che ne consente l'utilizzo per eseguire l'encryption di Standard HDD, Standard SSD e Premium SSD. Le figure seguenti mostrano i parametri di configurazione per la creazione del Disk Encryption Set "24-01-2023-Test-Standard-VM", dove viene utilizzata la chiave "firstkey-mHSM" e la creazione della standard virtual machine "Test-Standard-VM".

Nota: Per deployare una standard virtual machine, sul Disk Encryption Set dovrà essere selezionato il valore "Encryption at-rest with a customer managed key" e sul wizard di creazione della virtual machine il campo Security dovrà essere valorizzato come "Standard".

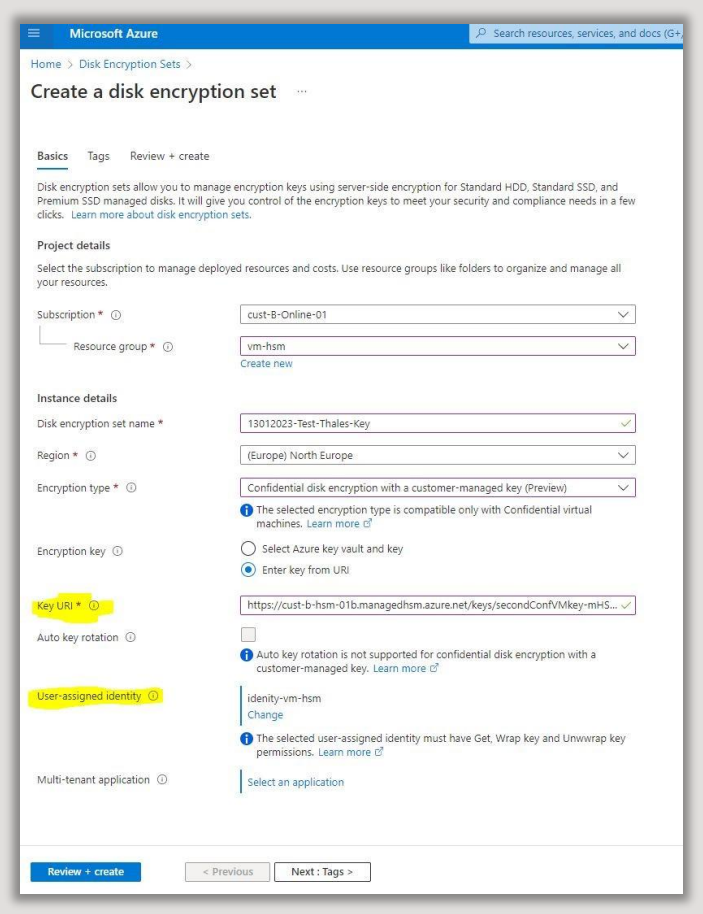

Create a disk encryption set
Subscription *
cust-B-Online-01
Resource group *
vm-hsm
Create new
Instance details
Disk encryption set name *
24-01-2023-Test-Standard-VM
Region *
(Europe) North Europe
Encryption type *
Encryption at-rest with a customer-managed key
Encryption key
Select Azure key vault and key
Enter key from URI
Key URI *
https://cust-b-hsm-01b.managedhsm.azure.net/keys/firstkey-mHSM/9e0c0cfe...
Auto key rotation
User-assigned identity
user-access-managed-hsm
Change
The selected user-assigned identity must have Get, Wrap key and Unwwrap key permissions. Learn more
Multi-tenant application
Select an application
Review + create
< Previous
Next : Tags >

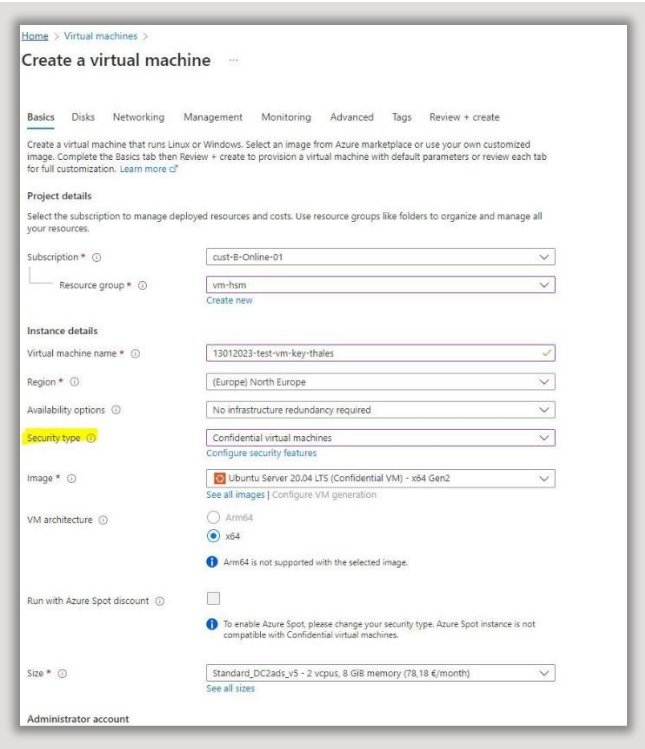

Create a virtual machine
Subscription *
cust-B-Online-01
Resource group *
vm-hsm
Create new
Instance details
Virtual machine name *
Test-Standard-VM
Region *
(Europe) North Europe
Availability options
No infrastructure redundancy required
Security type
Standard
Image *
Ubuntu Server 20.04 LTS - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Run with Azure Spot discount
Size *
Standard_DS1_v2 - 1 vcpu, 3.5 GiB memory (€40.52/month)
See all sizes
Administrator account
Authentication type
SSH public key
Review + create
< Previous
Next : Disks >

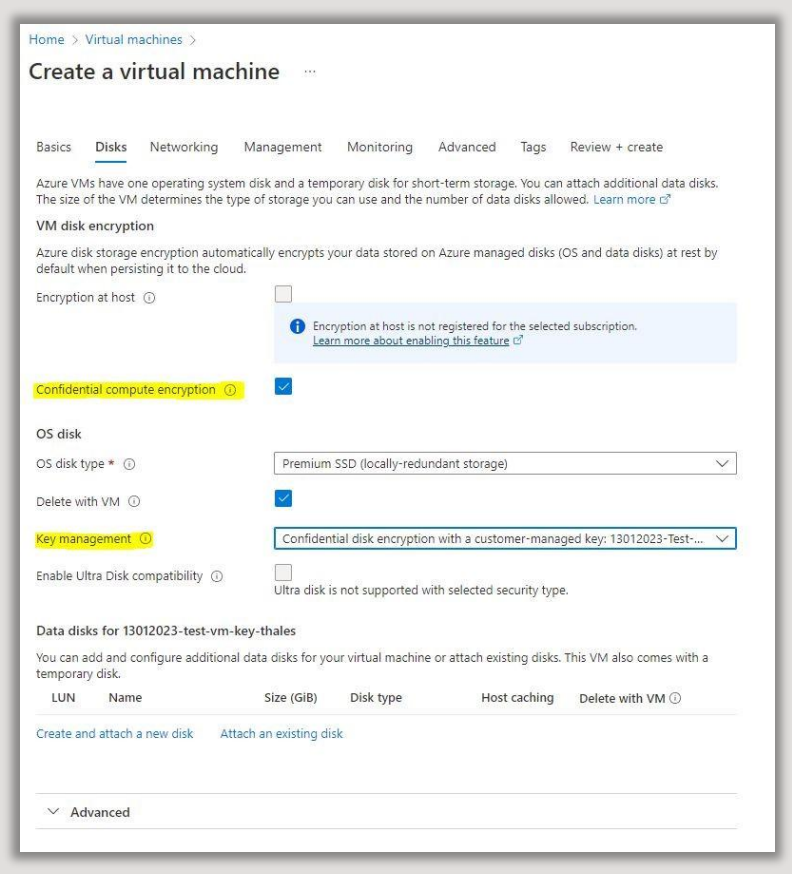


La medesima procedura dovrà essere utilizzata per la creazione di una Confidential virtual machine. Qui di seguito gli screenshot con i parametri di configurazione per la creazione del Disk Encryption Set "13012023-Test-Thales-Key", dove viene utilizzata la chiave "secondConfVMkey-mHSM" e la creazione della confidential virtual machine "13012023-test-vm-key-thales".

Nota: Per deployare una confidential virtual machine, sul Disk Encryption Set dovrà essere selezionato il valore "Confidential disk with a customer managed key", il campo Security dovrà essere valorizzato come "Confidential virtual machine" sul wizard di creazione della virtual machine e dovrà essere selezionata l'opzione "Confidential compute encryption" nella schermata relativa ai dischi della virtual machine. Dovrà inoltre essere utilizzata un'immagine di sistema operativo compatibile con questa tipologia di risorse.


Microsoft Azure
Search resources, services, and docs (G+/
Home > Disk Encryption Sets >
Create a disk encryption set
Basics
Tags
Review + create
Disk encryption sets allow you to manage encryption keys using server-side encryption for Standard HDD, Standard SSD, and Premium SSD managed disks. It will give you control of the encryption keys to meet your security and compliance needs in a few clicks. Learn more about disk encryption sets.
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
cust-B-Online-01
Resource group *
vm-hsm
Create new
Instance details
Disk encryption set name *
13012023-Test-Thales-Key
Region *
(Europe) North Europe
Encryption type *
Confidential disk encryption with a customer-managed key (Preview)
The selected encryption type is compatible only with Confidential virtual machines. Learn more
Encryption key
Select Azure key vault and key
Enter key from URI
Key URI *
https://cust-b-hsm-01b.managedhsm.azure.net/keys/secondConfVMkey-mHS...
Auto key rotation
Auto key rotation is not supported for confidential disk encryption with a customer-managed key. Learn more
User-assigned identity
idenity-vm-hsm
Change
The selected user-assigned identity must have Get, Wrap key and Unwwrap key permissions. Learn more
Multi-tenant application
Select an application
Review + create
< Previous
Next : Tags >

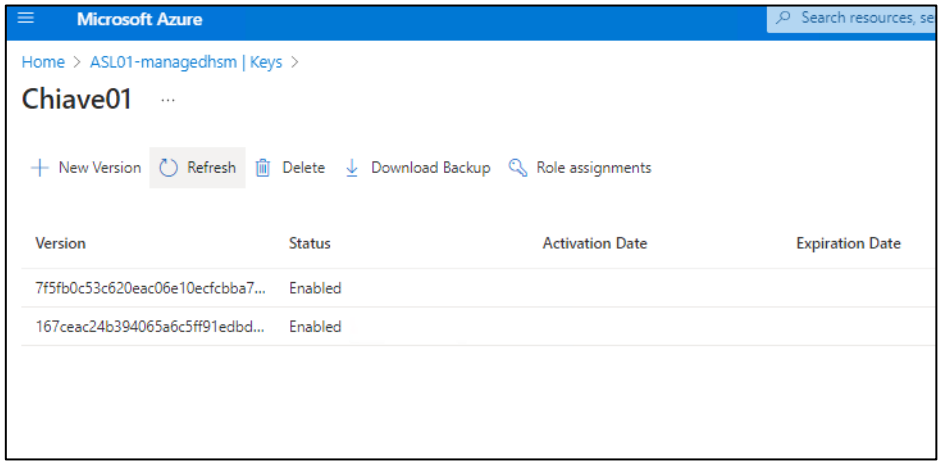

Home > Virtual machines >
Create a virtual machine
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create
Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more
Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.
Subscription *
cust-B-Online-01
Resource group *
vm-hsm
Create new
Instance details
Virtual machine name *
13012023-test-vm-key-thales
Region *
(Europe) North Europe
Availability options
No infrastructure redundancy required
Security type
Confidential virtual machines
Configure security features
Image *
Ubuntu Server 20.04 LTS (Confidential VM) - x64 Gen2
See all images | Configure VM generation
VM architecture
Arm64
x64
Arm64 is not supported with the selected image.
Run with Azure Spot discount
To enable Azure Spot, please change your security type. Azure Spot instance is not compatible with Confidential virtual machines.
Size *
Standard_DC2ads_v5 - 2 vcpus, 8 GiB memory (78,18 €/month)
See all sizes
Administrator account



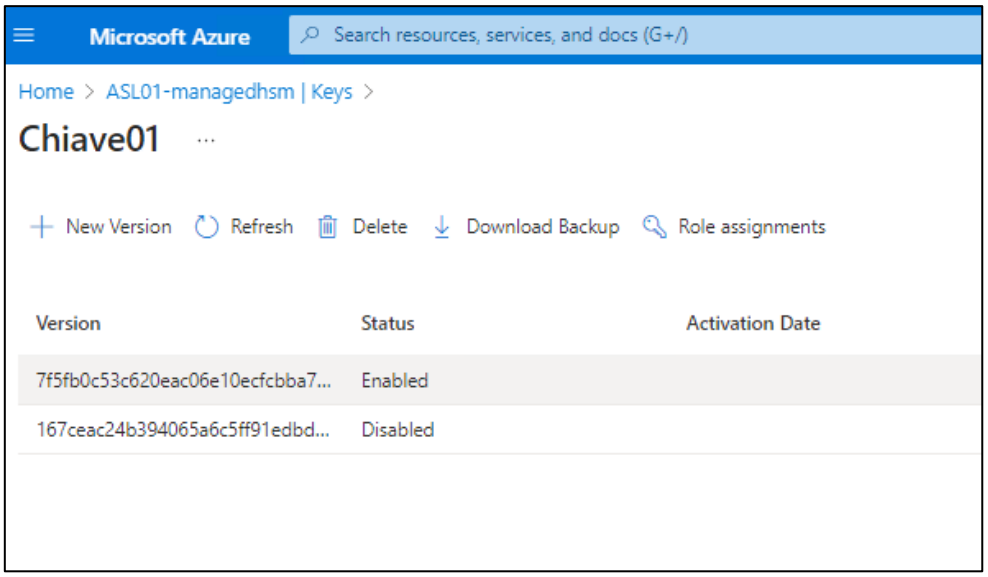
3.4.2 *Rotazione chiave*

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 Azure.

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 Managed-HSM in cloud.



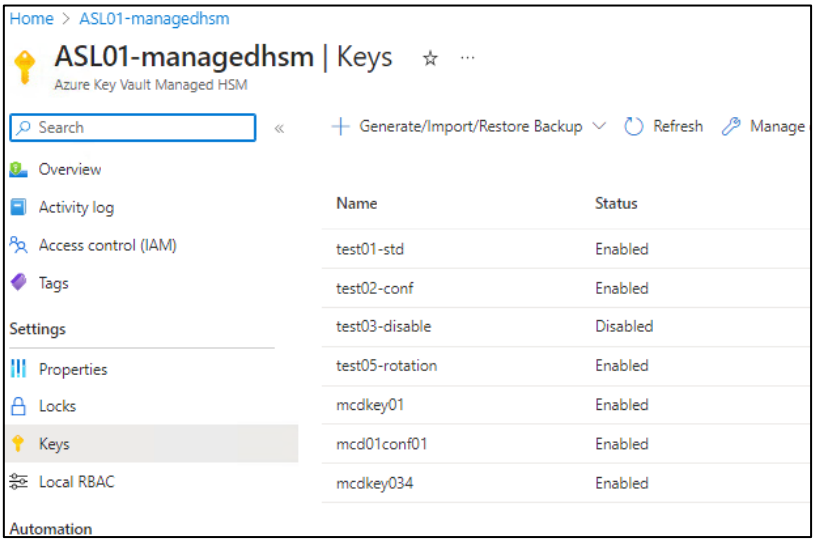
La vecchia chiave continua ad esser valida e a poter essere utilizzata fino a quando non viene disabilitata, per questo motivo una Virtual Machine criptata con la vecchia versione continua a funzionare regolarmente. Per completare il ciclo di rotazione con la disabilitazione della chiave da dismettere, 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 stessa sul Managed-HSM risulterà come "disable" e al riavvio la VM non sarà più accessibile:



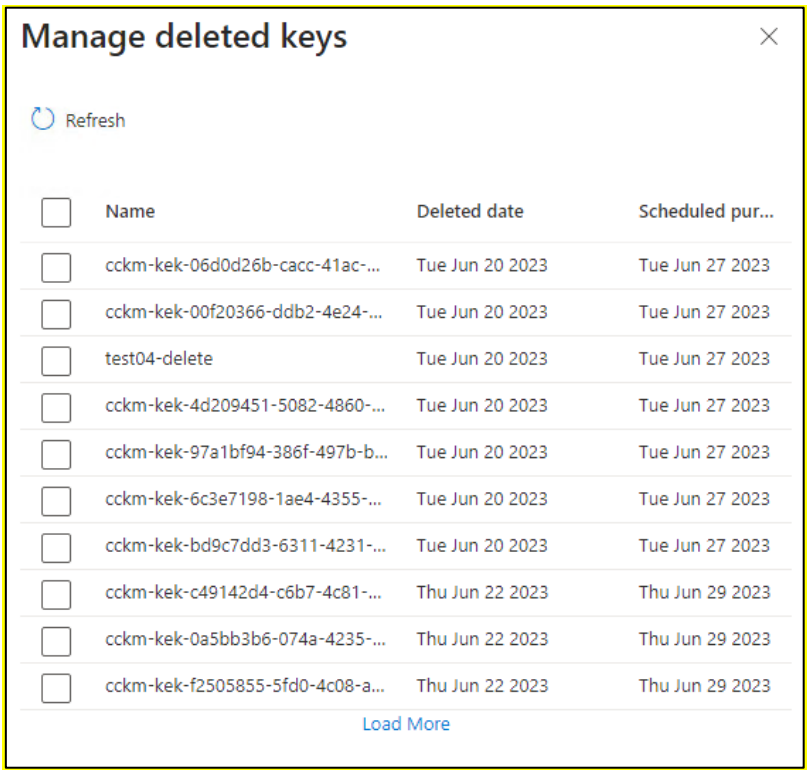
Non sarà possibile abilitare/disabilitare delle chiavi dall'Azure Managed-HSM.

3.4.3 *Cancellazione chiave*

Se una chiave viene cancellata lato Thales, la stessa non sarà più presente all'interno del Managed-HSM e la VM non sarà più accessibile.

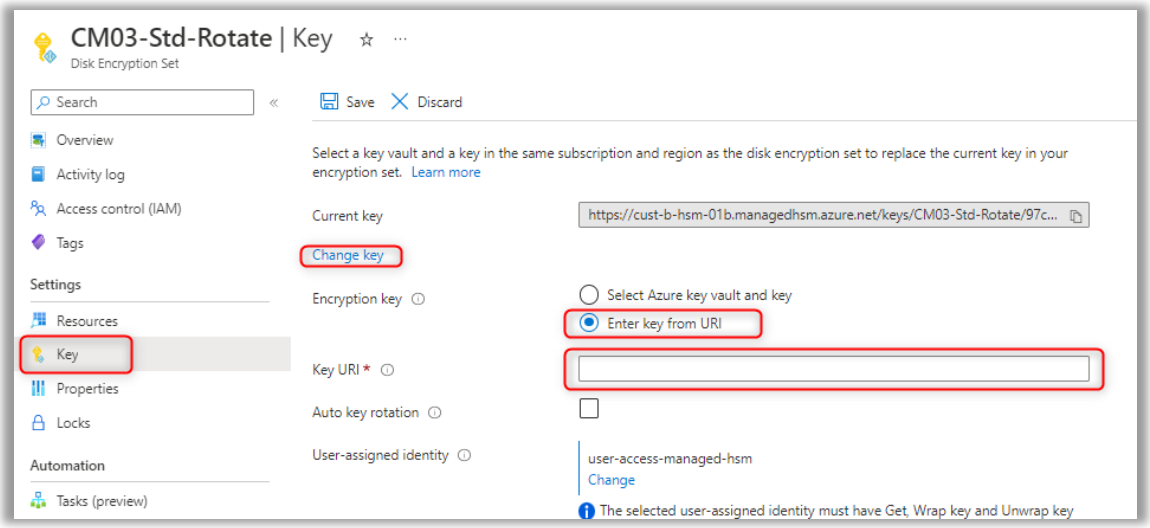


Partirà quindi un retention-period che consentirà l'eventuale ripristino della chiave, qualora necessario: la vera e propria cancellazione della chiave verrà eseguita allo scadere dell'intevallo impostato sul Managed-HSM in fase di onboarding del servizio (da 7 a 90 giorni). Le chiavi in stato retention sono visualizzabili da menù "Manage deleted keys"



3.4.4 Utilizzo nuova Chiave

Per utilizzare la versione nuova di una chiave, o una chiave differente su una Standard Virtual Machine, sia essa Confidential o no, è necessaria una procedura manuale di rotazione, impostando sul relativo Disk Encryption Set il puntamento al Key Uri della nuova chiave/versione:



Nota: Il cambio della chiave su una Confidential virtual machine deve essere eseguito a sistema operativo spento.

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.