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 Operativo

# PSN Cloud Platform

# IaaS Industry Standard

Data: 16/11/2023

PSN_UserGuide_IaaS_Industry_Standard

Ed. 1 - ver. 3.0.3

# QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

# STATO DEL DOCUMENTO

| TITOLO DEL DOCUMENTO | | | |
|---|---|---|---|
| **vCloud User Guide** | | | |
| EDIZ. | REV. | DATA | AGGIORNAMENTO |
| 1 | 1.0 | 29/11/2022 | Prima versione del documento finalizzata alla realizzazione di un manuale utente |
| 1 | 1.01 | 15/12/2022 | Modifica dei titoli |
| 1 | 1.02 | 02/03/2023 | Modifica delle immagini e revisione del doc |
| 1 | 2.0 | 20/03/2023 | Adeguamento formale |
| 1 | 3.0 | 21/03/2023 | Revisione del documento |
| 1 | 3.0.1 | 13/04/2023 | Revisione del documento |
| 1 | 3.0.2 | 26/04/2023 | Revisione del documento |
| 1 | 3.0.3 | 16/11/2023 | Revisione del documento |

| | |
|---|---|
| NUMERO TOTALE PAGINE: | 8581 |

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

| **REVISIONE:** | |
|---|---|

| | |
|---|---|
| Referente del Servizio | Paolo Trevisan |

| **APPROVAZIONE:** | |
|---|---|
| Direttore del Servizio | Giovanni Santocchia |

# INDICE

# LISTA DELLE FIGURE

# LISTA DELLE TABELLE

# 1 Definizioni e Acronimi

## 1.1 Definizioni

| Definizione | Descrizione |
|---|---|
| PSN | Polo Strategico Nazionale S.p.A. 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 |
| da definire | Il tema non è ancora stato discusso |

Tabella 1. Glossario Definizioni

| Definizione | Descrizione |
|---|---|
| PSN Cloud Platform | Identifica tutte le componenti della piattaforma Cloud offerta dal PSN |
| Console Tecnica IaaS | Identifica il Portale Tecnico di amministrazione del Servizio IaaS |
| Cloud Industry Standard IaaS | Identifica il Servizio IaaS offerto dal PSN |

Tabella 2. Nomenclatura

## 1.2 Acronimi

| Acronimo | Descrizione |
|---|---|
| API | Application Program Interface |
| BaaS | Backup as a Service |
| DHCP | Dynamic Host Configuration Protocol |
| DNAT | Destination Network Address Translation |
| DNS | Domain Name System |
| FAQ | Domande Frequenti Poste Dagli Utilizzatori Del Servizio |
| HA | High Availability (Alta Affidabilità) |
| HTML | Hypertext Markup Language |
| HTTP | HyperText Transfer Protocol |
| HTTPS | HTTP Secure |
| IaaS | Infrastructure as a Service |
| IaC | Meccanismi di rilascio automatico |
| IAM | Identity and Access Management |
| IP | Internet Protocol |
| IPSEC | Internet Protocol Security |
| ISO | International Organization for Standardization |
| LAN | Local Area Network |
| MPLS | MultiProtocol Label Switching |
| NAS | Storage Collegato Alla Rete |
| NAT | Network Address Translation(Traduzione Degli Indirizzi Di Rete) |
| NIC | Network Interface Card |
| OS | Sistema Operativo |
| OVF | Open Virtualization Format |
| PaaS | Platform as a Service |
| PA | Pubblica Amministrazione |
| PSN | Polo Strategico Nazionale |
| pVDC | Provider Virtual Data Center |

| Acronimo | Descrizione |
|---|---|
| SaaS | Software as a Service |
| SNAT | Source Network Address Translation |
| SSO | Single Sign On (autenticazione unica) |
| TB | TeraByte |
| vApp | Raggruppamento Logico VM |
| vCPU | Virtual Central Processing Unit |
| VDC | Virtual Data Center |
| VLAN | Virtual LAN |
| VM | Macchina Virtuale |
| VMRC | VMware Remote Console |
| vNet | Rete Virtuale |
| VPN | Virtual Private Network |
| vRAM | Virtual Random Access Memory |

Tabella 3. Glossario Acronimi

# 2 Panoramica Generale

Il presente documento fornisce le linee di utilizzo e una panoramica di dettaglio e della soluzione di "***Cloud Industry Standard IaaS***" (di seguito identificato anche come IaaS) prevista tra le architetture tecnologiche necessarie all'erogazione dei servizi di cui all'art. 5, comma 1 della Convenzione, redatto e presentato dal concessionario PSN S.p.A. (di seguito identificato anche come "**PSN**") secondo quanto stabilito dal Capitolato Tecnico per la componente Industry Standard.

La soluzione IaaS, mediante la Console Tecnica IaaS offre un "***Virtual Data Center***" (VDC) alla PA permettendo di istanziare server virtuali, aggiungendo o diminuendo capacità elaborativa e storage in base alla sottoscrizione al fine di erogare le proprie applicazioni sulla piattaforma PSN Cloud Platform. Il servizio è accessibile mediante interfaccia web.

## *2.1 Scopo del documento*

Questo documento rappresenta un manuale con le linee guida di utilizzo della soluzione oltre a contenere una raccolta delle domande più comuni sul servizio e le relative risposte. Il manuale e le FAQ saranno integrati nel tempo in base ad eventuali altri argomenti che si riveleranno di interesse comune.

# 3 Descrizione del Servizio

Il servizio permette di fornire alla PA contesti di sicurezza e rete isolate associando a ciascuno di essi risorse condivise in termini di risorse computazionali, storage e network con la possibilità di abilitare diverse modalità di allocazione e livelli di servizio. Nei prossimi paragrafi sono descritte le caratteristiche e le funzionalità del servizio Virtual Data Center messe a disposizione nella Console Tecnica IaaS.

# 4 Introduzione al Servizio

In questa sezione sono riportate alcune definizioni dei costrutti logici utilizzati all'interno del servizio Virtual Data Center. Tali principi consentiranno una migliore comprensione dei successivi capitoli del manuale che si focalizzeranno su alcune aree 'verticali' di gestione del servizio.

## *4.1 Come si accede al Servizio?*

Il servizio è usufruibile mediante il portale "***Console Unica***", raggiungibile dalla seguente URL: **https://console.polostrategiconazioneale.it**

L'accesso all'interfaccia applicativa del portale viene effettuato tramite browser e, dopo aver inserito username e password nella pagina di Login, mediante il processo di autenticazione SSO, l'utente, accedendo alla "***Console Tecnica***", visualizzerà la dashboard di accesso ai servizi contrattualizzati.

Il dettaglio del tipo di servizi è illustrato nel paragrafo 4.3

## *4.2 Come utilizzo il Servizio?*

Come anticipato, il servizio è utilizzabile mediante interfacce WEB della "Console Unica" e "Console Tecnica".

La Console Tecnica fornisce un ulteriore metodo di gestione mediante API di prodotto, per la creazione di Infrastrutture e Macchine all'interno della propria Sottoscrizione con i meccanismi di rilascio automatico di Infrastructure as Code (IaC).

La documentazione delle API viene resa disponibile sul sito del Vendor al seguente link:

https://developer.vmware.com/apis/1507/vmware-cloud-director#api

**NOTA:** La versione di riferimento delle API è la 37.1 relativa al Prodotto vCloud Director 10.4.1

## 4.3 Che cosa è un Token di accesso API?

Un token di accesso è un elemento che le applicazioni client utilizzano per effettuare richieste API.

## 4.4 Come si genera un Token di accesso API?

Di seguito, la procedura di generazione di un Token di accesso API:

1. Cliccare il nome utente, nell'angolo superiore della barra di navigazione, e selezionare "*User Preferences*\ *Preferenze Utente*"
2. Posizionarsi nella sezione "Access Tokens\Token di Accesso" e cliccare "New\Nuovo"; Vedi Figura 1


**Figura 1** - Creazione Token di Accesso

3. Inserire il nome in "Create General Token\ Crea Token Generale" e cliccare su "Create\Crea"

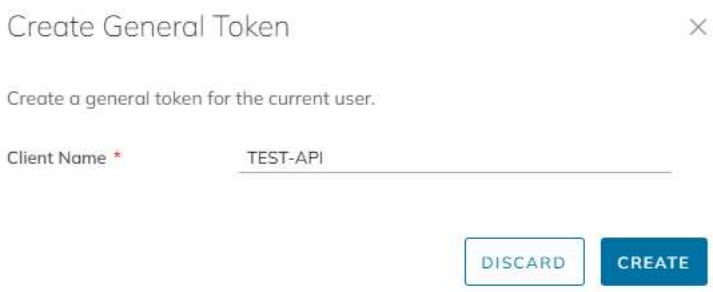


**Figura 2-** Creazione Token di Accesso, Definizione del Client Name

4. Viene visualizzato il token API generato. È necessario copiare il token perché viene visualizzato una sola volta

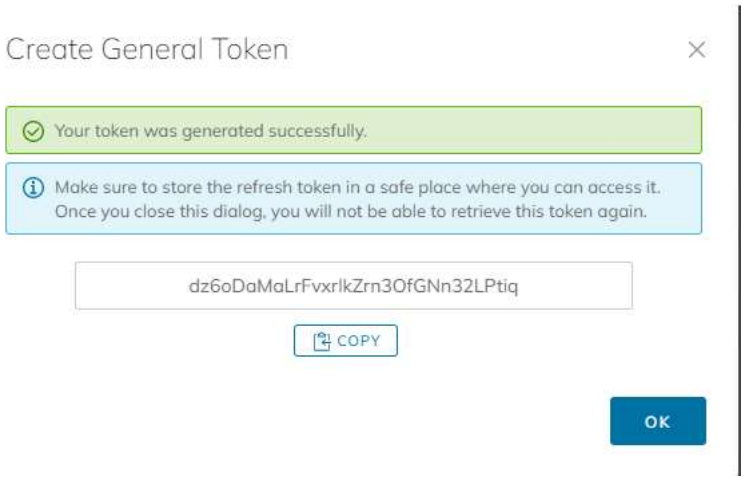


**Figura 3-** Creazione Token di Accesso, Token generato

**NOTA:** Dopo aver cliccato "*OK*", non sarà più possibile recuperare questo token, ma si potrà solo revocarlo.

## *4.5 Come utilizzo un Token di accesso API?*

Mediante strumenti di chiamate API è necessario effettuare una richiesta conforme a *OAuth 2.0* per l'endpoint dell'API, come ad esempio:

*"https://site.cloud.example.com/oauth/tenant/tenant_name/token"*

Nella seguente tabella, le chiavi necessarie per effettuare la richiesta:

| Chiave | Valore |
|---|---|
| **grant_type** | refresh_token |
| **refresh_token** | Generated_refresh_token |

**Tabella 4.** Chiavi necessarie per effettuare una richiesta conforme a OAuth 2.0

La richiesta restituisce un token di accesso che le applicazioni possono utilizzare per eseguire attività nella Console Tecnica IaaS. Il token è valido anche dopo la disconnessione della PA.

Di seguito è riportato un esempio di chiamata tramite Token con richiesta e risposta.

- ***Esempio di Richiesta tramite Token***

| | |
|---|---|
| *POST* | *https://host_name/oauth/tenant/tenant_name/token* |
| *Accept:* | *application/json* |
| *Content-Type:* | *application/x-www-form-urlencoded* |
| *Content-Length: 71* | |
| *grant_type=refresh_token&refresh_token=Generated_API_Token* | |

- ***Esempio di Risposta tramite Token***

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "access_token":"Generated_Access_Token",
  "token_type":"Bearer",
  "expires_in":2592000,
  "refresh_token":null
}
```

- ***Esempio di configurazione con Provider Terraform***

```
provider "vcd" {
 user     = "none"
 password  = "none"
 auth_type = "api_token"
 api_token = "**********************"
 org      = "org-rn-rozz-flex-01-12345678912"
 url      = "https://it-nord-1.testcloud.psncloud.it/api"
}
```

## 4.6 Che cosa è una Organization?

L'Organization è l'unità di amministrazione costituita da un raggruppamento logico di utenti, gruppi e risorse. Costituisce inoltre un confine di sicurezza entro il quale gli utenti possono attivare ed utilizzare i propri workload domain.

L'entità Organization viene configurata dal PSN in fase di creazione del Servizio ed eventualmente modificata e gestita durante il ciclo di vita del contratto.

## 4.7 Che cosa è un Provider Virtual Data Center?

Il Provider Virtual Data Center (pVDC) è l'insieme di risorse (Resource Group) fornite da PSN. I Provider VDC sono classificati nei seguenti piani di servizio:

- **IaaS Private** – Servizio con risorse computazionali storage e network dedicate, definite nel piano di acquisto del servizio.
- **IaaS Shared Pool** – Servizio con risorse computazionali storage e network su infrastruttura condivisa.
- **IaaS Shared VM** – Servizio con risorse VM pre-allocate da PSN con le caratteristiche concordate in fase di attivazione del Servizio

Anche in questo caso la creazione dell'oggetto Provider Virtual Data Center viene effettuata dal PSN che, in fase di attivazione della soluzione, predispone le risorse necessarie all'erogazione del servizio.

Naturalmente ogni modifica necessaria (ad esempio, a fronte dell'estensione del numero di risorse) deve essere veicolata e gestita dal PSN stesso sulla base delle richieste della PA.

## 4.8 Che cosa è un virtual Data Center?

Il Virtual Data Center (successivamente anche nominato VDC) è l'allocazione di un sotto-insieme di risorse fornite da un "Provider Virtual Data Center" che sono assegnate ad un'Organization. L'allocazione della capacità a livello computazionale, di network e di storage in questo caso viene effettuata secondo il modello "Allocation Pool" che assicura alla PA una quantità predefinita di risorse.

Come nel caso precedente, il Virtual Data Center viene dimensionato e predisposto dal PSN sulla base di quanto contrattualizzato (a livello di Ghz, GB di RAM e GB di spazio disco in base ai profili di storage acquistati). Naturalmente, a fronte di qualsiasi variazione del perimetro di risorse contrattualizzate, sarà compito del PSN allineare il dimensionamento della relativa infrastruttura "VDC".

## 4.9 Che cosa è una vApp?

Una vApp (virtual Appliance) è un contenitore di una o più Virtual Machine. Il concetto di vApp può essere associato a quello di servizio applicativo o infrastrutturale (è una aggregazione di più VM). Pertanto, una vApp può essere costituita da una sola VM o da una complessa applicazione di business distribuita su più livelli architetturali. Per rendere più evidente il concetto di vApp, pensiamo, ad esempio, ad un'applicazione web ospitata da una macchina virtuale.

L'applicazione necessiterà ad esempio di un database, di un "application server" e di un "web server" ospitati in diverse macchine virtuali. Da un punto di vista del servizio, tutte le machine virtuali che contribuiscono alla realizzazione dell'applicazione possono essere raggruppate all'interno di una stessa entità che, negli ambienti, è rappresentata proprio dalle vApp. All'interno dell'offerta Virtual Data Center, le vApp sono gestite dalla PA che può procedere in autonomia alla creazione di vApp e modelli di vAPP da caricare all'interno del catalogo della propria organization (si veda poi la definizione di Catalogo).

## 4.10 Che cosa è un Catalogo?

Un catalogo è un contenitore di modelli di vApp e media file (ISO) a disposizione dell'Organization.

Da vApp template è possibile eseguire il deployment di vApp. La vApp risultante costituirà un clone del template con la possibilità di eseguire alcune personalizzazioni per definire l'identità delle singole VM. I file ***.iso*** (media files) possono essere connessi a VM esistenti per eseguire, ad esempio, installazioni software o installazioni di sistemi operativi su nuove VM.

Possono esistere due tipologie di cataloghi: Pubblico o relativo all'Organization. Nel primo, PSN predispone le immagini .iso per l'installazione di sistemi operativi su nuove VM. Nel secondo, ogni Organization (PA) puo' creare e salvare i propri template di vApp o VM in modo da poter ricreare i diversi oggetti a partire da configurazioni prestabilite e personalizzate.

## 4.11 Che cosa è una vApp Network?

Una vApp Network è una rete virtuale contenuta all'interno di una vApp che facilita la connettività tra le macchine virtuali della vApp stessa.

Una vApp Network consente di stabilire il modo in cui le macchine virtuali di una vApp possono comunicare.

La configurazione della vApp Network avviene durante la creazione della vApp. È poi possibile modificarla utilizzando le apposite funzionalità del prodotto vCloud Director (si veda Par. Gestione delle vApp).

## 4.12 Che cosa è una Organization Network?

Una Organization Network viene utilizzata per il traffico interno alla Organizzazione e consente la comunicazione tra tutte le vApp. L'amministratore dell'organizzazione può gestire le proprie reti, inclusi i relativi servizi di rete.

## 4.13 Che cosa è una External Network?

Se l'Organization (e le vApp) devono disporre di connettività con il mondo esterno (Internet pubblica o rete aziendale delle sedi remote), è necessario disporre di una External Network. Si tratta di una rete gestita dall'esterno del pool di risorse elaborative ed è fornita/gestita dal PSN. Può essere un collegamento Internet o MPLS.

## 4.14 Che cosa è una Internal Network?

Una rete isolata interna all'Organization senza avere connettività con il mondo esterno.

## 4.15 Quale tipologia di accesso devo contrattualizzare su Virtual Data Center?

Nessuna. L'accesso e l'erogazione del servizio avviene di default mediante connettività EXTERNAL su banda condivisa.

## 4.16 Se con il profilo di servizio attivo "Allocation Pool" viene chiesta una variazione (es. aggiunta di un pool) è necessario fermare il servizio per ampliare il precedente pool contrattualizzato?

No, l'upgrade di un pool di risorse non richiede necessariamente il fermo del servizio. Le modifiche alle singole VM potrebbe invece richiedere un fermo della macchina.

## 4.17 Organizzazione del Portale PSN Cloud Platform e principali sezioni

Di seguito si riportano alcuni esempi di schermate o modelli di sintesi utili ad illustrare il funzionamento del Portale PSN Cloud Platform e delle relative funzionalità descritte nelle precedenti risposte.

In **Figura 4** si riporta una sintesi dell'organizzazione 'gerarchica' relativa agli elementi descritti ai punti precedenti.

Naturalmente le indicazioni riportate (anche nel seguito del manuale) si riferiscono alla soluzione '***un-managed***' del servizio Virtual Data Center, dove la PA utilizza il Portale per organizzare le risorse e configurare in autonomia il proprio ambiente di lavoro a livello di componenti infrastrutturali.

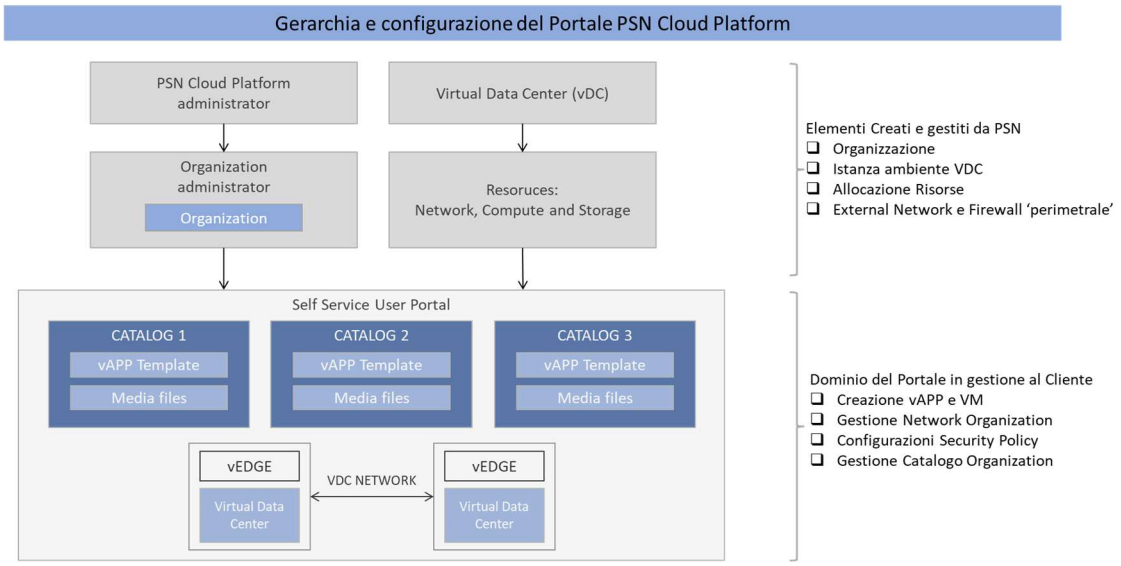


**Figura 4 -** Organizzazione logica dei principali elementi di servizio della soluzione Virtual Data Center

A livello logico (e gerarchico) le varie componenti del servizio sono organizzate come in **Figura 5.**

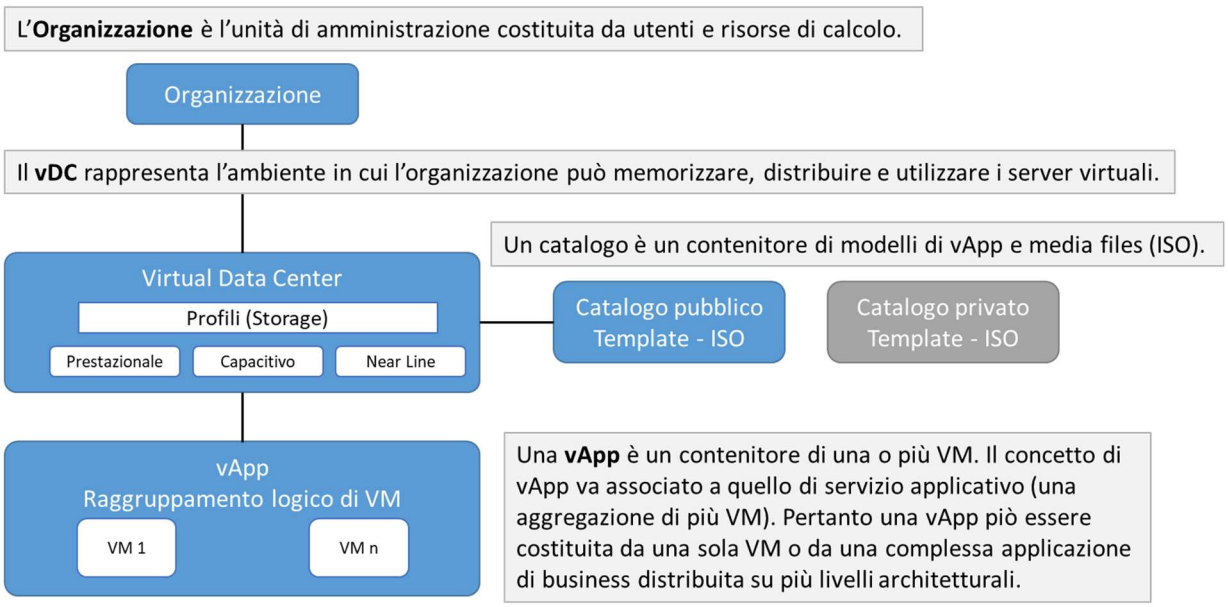


**Figura 5 -** Organizzazione logica delle componenti di servizio

Per avere evidenza delle risorse complessive assegnate al Virtual Data Center (ed al relativo stato di allocazione) è possibile accedere alla sezione Administration (area Monitor) del Portale PSN Cloud Platform, in base alle indicazioni di accesso al portale descritto nel **paragrafo 4.1**. (Si veda anche **Figura 6).**

Come anticipato, dal tab **Virtual Datacenters** (sezione **Monitor**) è possibile verificare anche lo stato di utilizzo delle risorse computazionali, storage e networking per ogni Virtual Data Center dell'organizzazione.

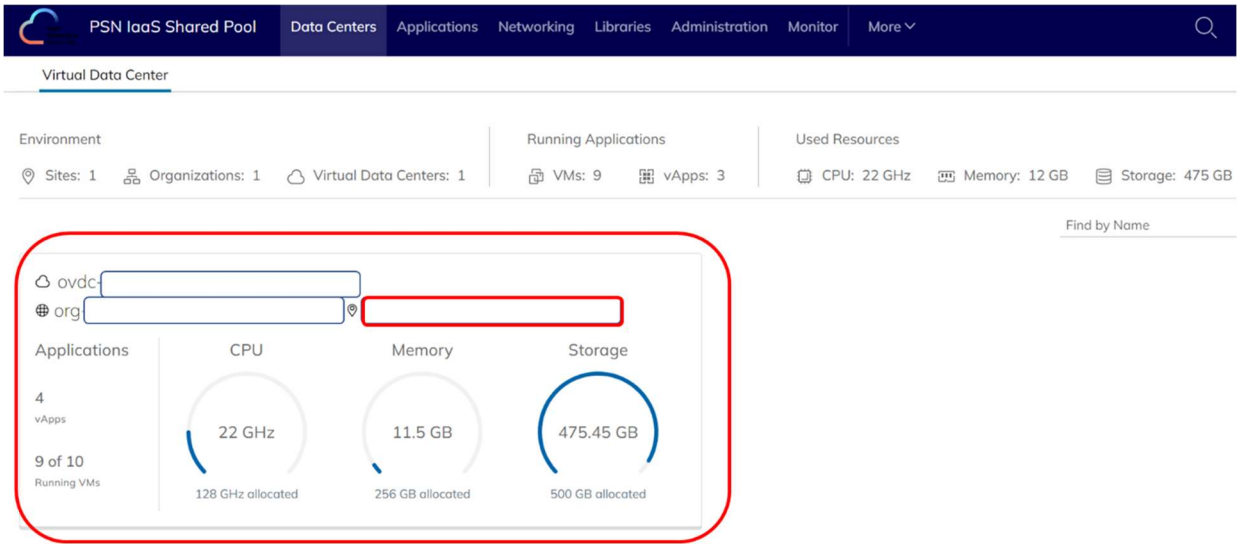


**Figura 6 -** Dashboard riepilogativa dell'ambiente Virtual Data Center

La rappresentazione delle risorse viene indicata in GHz per le CPU e in GB/TB per RAM e Storage.

I Valori della CPU sono riconducibili ad una formula di conversione di **GHz= vCPU** come indicato in tabella:

| Valore di riferimento GHz | vCPU |
|---|---|
| **2** | **1** |

**Tabella 5**. Valori di rifermento, conversioni vCPU

A titolo esemplificativo, nella Figura 6 evidenziamo che sono disponibili 128 GHz corrispondenti a 64 vCPU.

Cliccando sulla dashboard del proprio **Virtual Data Center** (riquadro rosso **Figura 6**), si eccederà alla sezione operativa, dove compariranno tutte le VM e vApp presenti nel "VDC" (**Figura 7 e 8).**

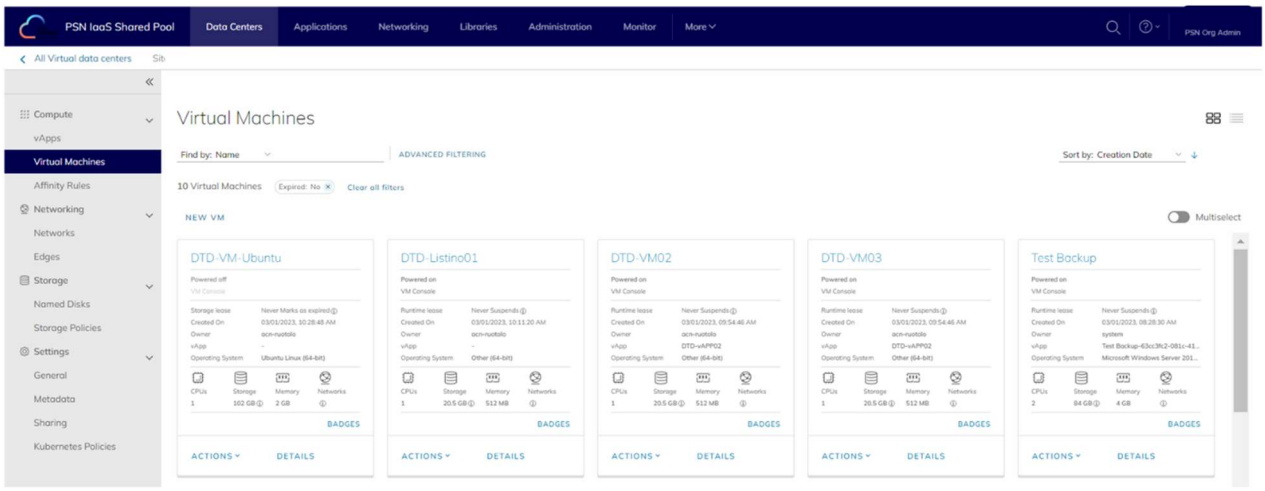


**Figura 7 -** Schermata riepilogativa delle Virtual Machine presenti nel Virtual Data Center

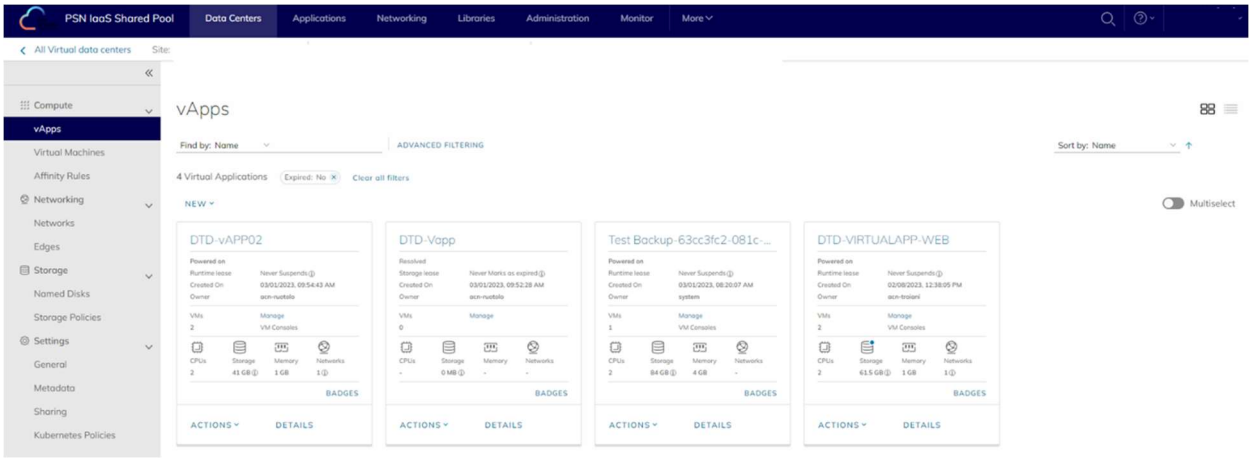


**Figura 8 -** Schermata riepilogativa delle vAPP presenti nel VDC

Nelle sezioni vApps e Virtual Machines si avrà l'accesso alle principali funzionalità di gestione dando all'utente la possibilità di accedere ai dettagli non solo delle vApp, ma anche delle singole VM. Da qui sarà inoltre possibile accedere alle aree di gestione e configurazione di Networking e Storage ed i relativi menu contestuali.

# 5 Gestione delle vApp

Nella gestione delle soluzioni erogati dalla PSN Cloud Platform, uno degli aspetti centrali riguarda la configurazione e l'aggregazione delle virtual machine all'interno di appositi 'contenitori' logici (***vApp***) che, oltre ad organizzare l'architettura su base servizi/applicazioni, assumono un ruolo fondamentale anche nel definire gli schemi di rete e le funzionalità di networking del Virtual Data Center.

Nei prossimi paragrafi si illustreranno le modalità di creazione e gestione delle "*vApp*" anticipando alcune tematiche legate a Cataloghi ed elementi di Networking che verranno affrontati nei capitoli successivi.

## *5.1 Quali versioni di sistema operativo è possibile installare nell'ambiente Virtual Data Center?*

È possibile installare tutte le versioni di sistema operative con un supporto attivo

| Versione S.O. | Descrizione |
|---|---|
| Windows 2019 Std. | Windows Server 2019 Standard Edition |
| Windows 2022 Std. | Windows Server 2022 |
| RedHat 8 Enterprise | Linux OS Red Hat |
| RedHat 9.1 | Linux OS Red Hat |
| Centos 8 | Linux OS Open |
| Ubuntu 22.04 ITS | Linux OS Open |

**Tabella 6.** Sistemi Operativi Installabili

E' previsto un processo di aggiornamento dei Template semestrale per le major version e trimestrale per i Security update o in via eccezionale a fronte di segnalazioni di security.

Relativamente alla gestione del *patching* dei sistemi rilasciati nelle OrgVDC della PA il processo è carico della PA stessa. L'aggiornamento dei Tepmplate non è retroattivo.

## 5.2 Come si configura e attiva una vApp?

La configurazione di vApp è realizzabile dal pannello **Home**. Di seguito come pura linea guida verrà descritto il processo di creazione di vApp tramite le funzionalità disponibili nel pannello **Home** (gli stessi strumenti possono essere richiamati anche dalla schermata **Home**).

Le modalità di creazione delle vApp sono di tre tipi:

1) partendo da un template presente nei cataloghi (pubblico o 'privato') già disponibile nell'ambiente vCloud Director di riferimento
2) importando un'immagine OVF da una fonte esterna (per tale attività è richiesta l'installazione di un plugin VMware)
3) creando una vApp vuota, a cui sarà possibile associare le VM in un secondo momento

**NOTA:** prima di procedere alla configurazione delle vApp si consiglia di aver creato almeno una rete relativa all'Organization. La vApp, infatti, dovrà essere agganciata da una Organization Network per poter comunicare con altre vApp o verso l'esterno.

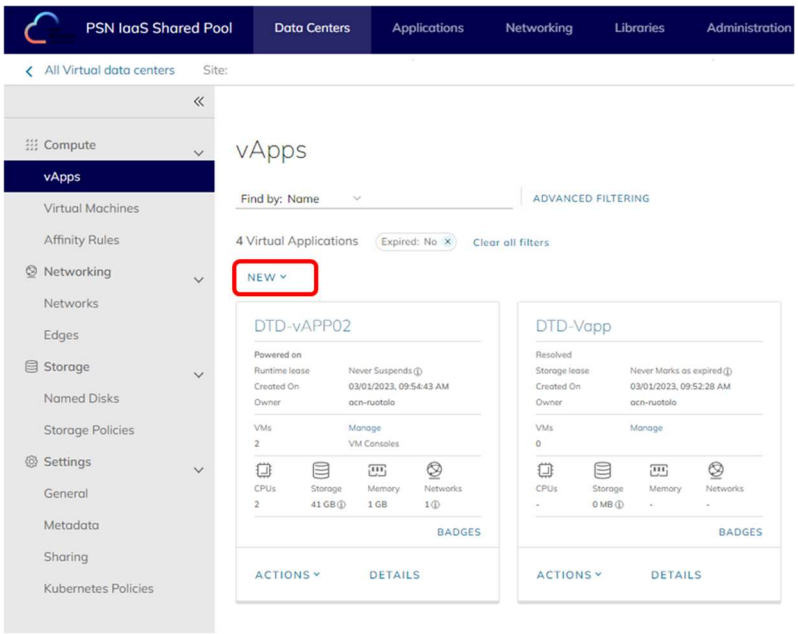


**Figura 9 -** Menu per la creazione di vApp

## 5.3 Creazione di vAPP contenente una VM da Catalogo

Di seguito la procedura da seguire per la creazione di una vApp che conterrà al suo interno una VM a partire da un template precaricato o reso disponibile dalla Piattaforma PSN (si veda anche **Figura 6**).

a Per avviare la procedura cliccare su *"New"*

b Selezionare *"**Add vApp** From **Catalog**"* (**Figura 10**)

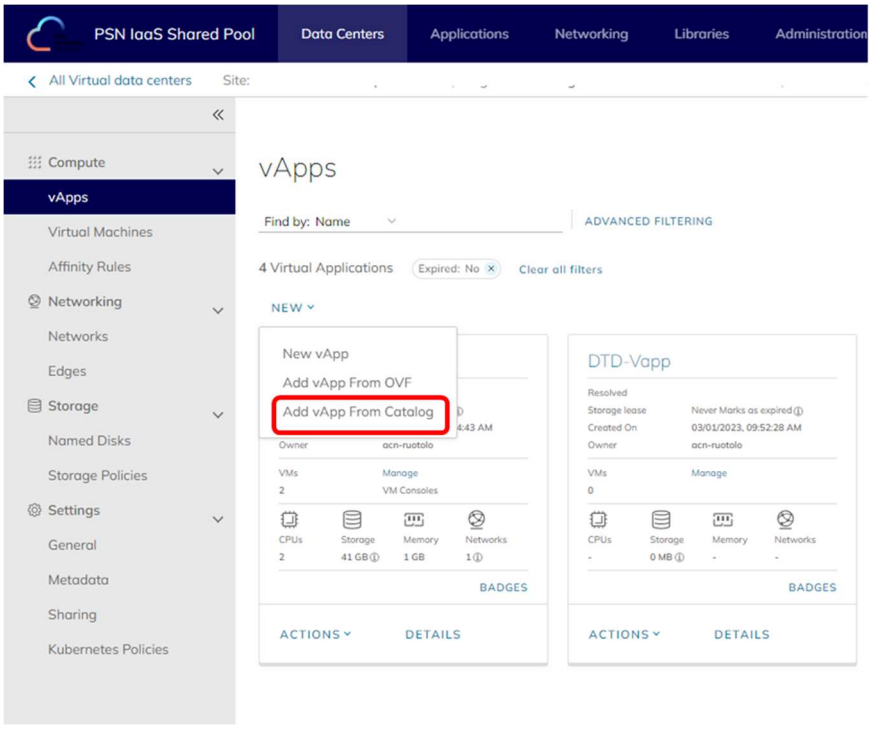


**Figura 10 –** Menu di creazione di una nuova vApp

c Nel Wizard di creazione della vApp selezionare l'immagine template su cui si baserà la VM contenuta nella vAPP quindi fare ***"Next"***

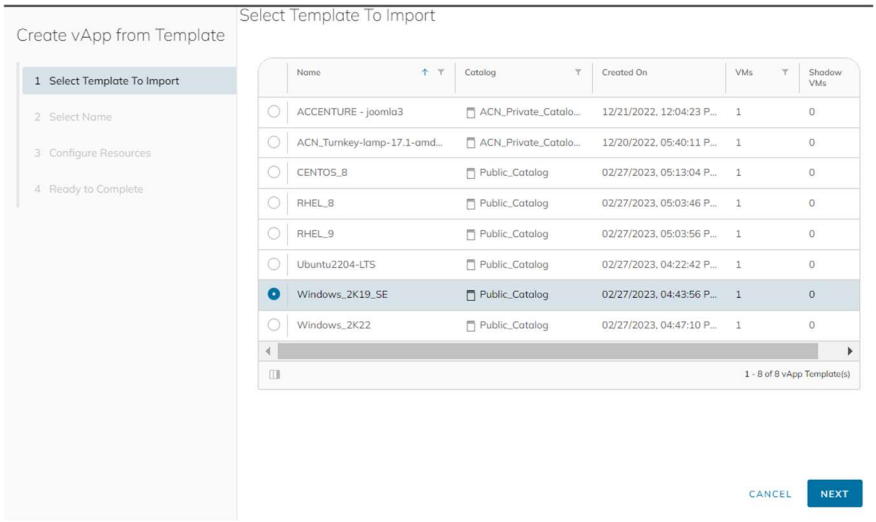


**Figura 11 -** Wizard creazione VM da Template

d Inserire il nome da dare alle vApp, ed eventualmente impostare un limite di tempo di funzionamento (**Runtime lease** e **Storage lease**), fare ***"Next"***

e Scegliere il **profilo di stogare** su cui salvare la VM e la vApp relativa, quindi fare ***"Next"***

f Scegliere la quantità di risorse **vCPU** e **vRam** da assegnare alla VM, quindi fare ***"Next"***

g Indicare la dimensione del disco primario della VM, quindi fare ***"Next"***

h Scegliere dal menu a tendina, su quale rete (**Network**) si vuole agganciare la VM, quindi fare ***"Next"***

i Verificare le impostazioni scelte nella schermata **Ready to Complete** e quindi fare *"**FINISH**"* per avviare la creazione della VM

## 5.4 Creazione di vAPP da OVF

In questo caso è possibile caricare importare un template OVF/OVA di vApp partendo da una fonte esterna che dovrà essere specificata nel wizard di creazione della vApp.

a. Seleziona *"New"* per avviare la procedura di creazione

b. Selezionare "**Add vApp from OVF"** (**Figura 12**)

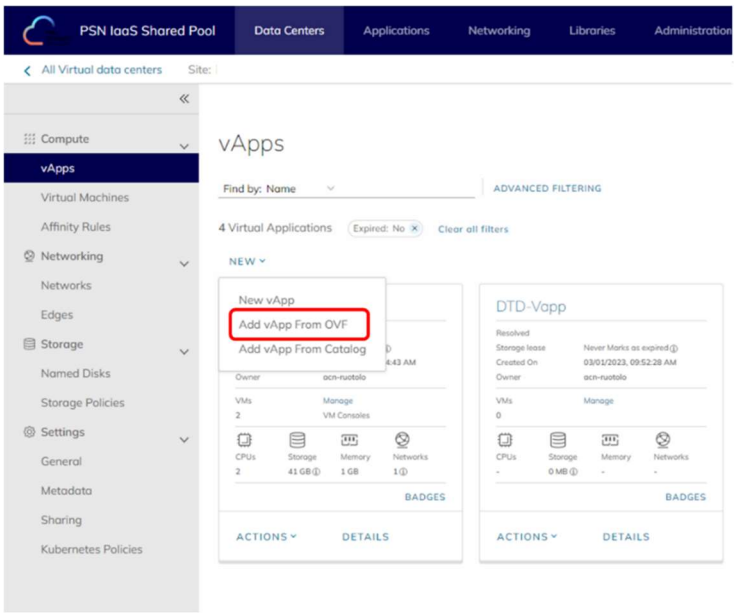


**Figura 12 –** Menu di creazione vApp da immagine OVF

c. Il wizard di creazione della vApp ci chiederà quindi di selezionare, dal nostro computer locale, l'immagine sorgente (tipi di file: ISO, OVA, OVF, etc..) sfogliando le cartelle locali del nostro computer.

**NOTA**: questa sarà caricata all'interno del catalogo privato della nostra organizzazione

d. Terminato il caricamento dell'immagine potremo proseguire con il wizard, selezionando ***"Next"***

e. Completare i passaggi proposti dal wizard, indicando:

- Nome della vApp
- Profilo di storage (Storage Policy)
- Impostazioni di rete

- Parametri computazionali

**NOTA**: a seconda dell'immagine che verrà utilizzate potrebbero essere richieste altre impostazioni necessarie per la creazione della vApp (rivolgersi quindi al fornitore dell'immagine).

## 5.5 Creazione di una nuova vAPP vuota

Per creare una vApp vuota a cui assegnare una o più VM, in seguito, basterà selezionare la voce **"New vApp"** nel menu **"*New*"** all'interno delle vApps. (**Figura 13** e **14**)

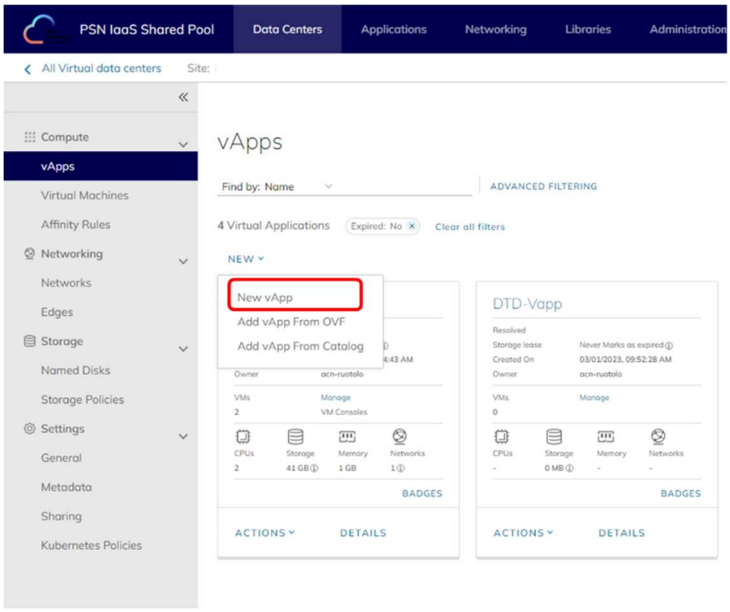


**Figura 13 -** Menu per la creazione di vApp

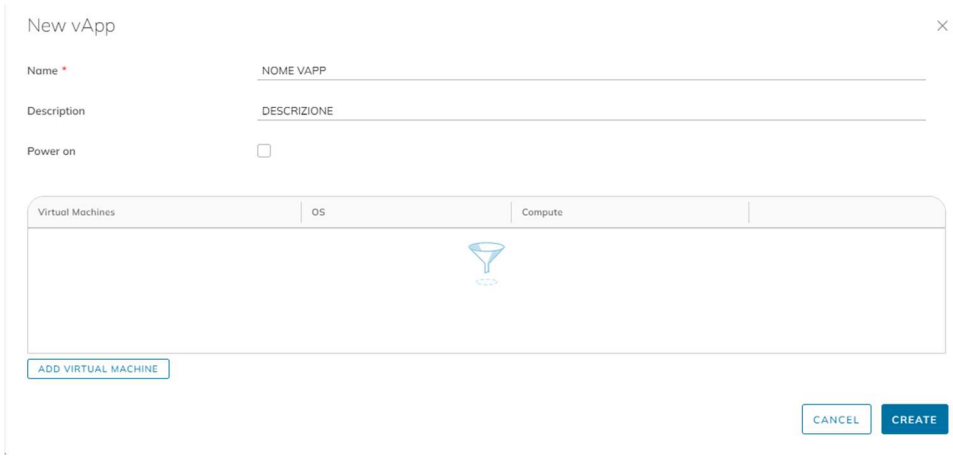


**Figura 14 -** Wizard di creazione di una nuova vApp

## 5.6 Come è possibile controllare e gestire la configurazione delle vApp?

È possibile consultare la configurazione di una singola vApp dal Menu Compute – vApps, selezionando la voce *"Details"* nel contesto della vApp stessa (**Figura 15**).

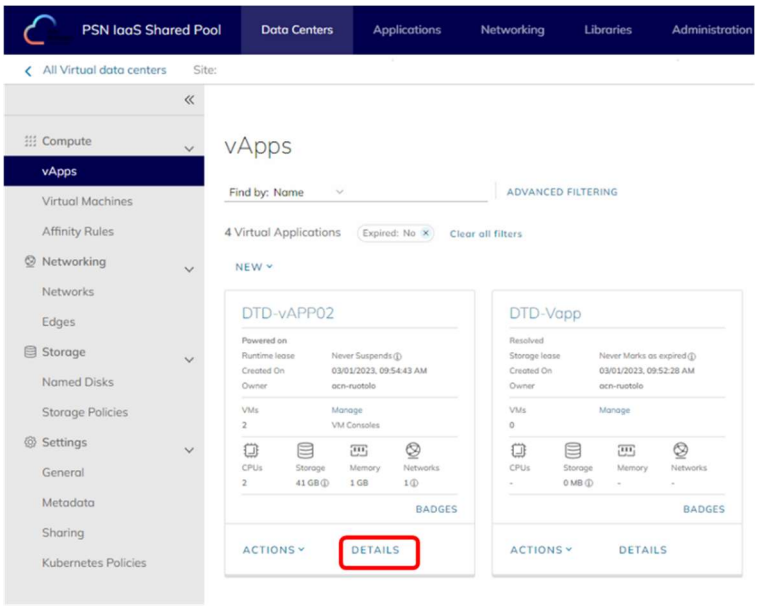


**Figura 15 -** Menu per la visualizzazione dettagli di una vApp

Dal menu *"Details"* è quindi possibile visualizzare:

a Visualizzare il dettaglio delle singole VM che la compongono (**VMs**). Da questa schermata è anche possibile controllare la sequenza di avvio delle VM contenute nella vApp (**Start and Stop Order**) ed impostare la condivisione di accesso con gli utenti dell'organizzazione (**Sharing**) (**Figura 16**).

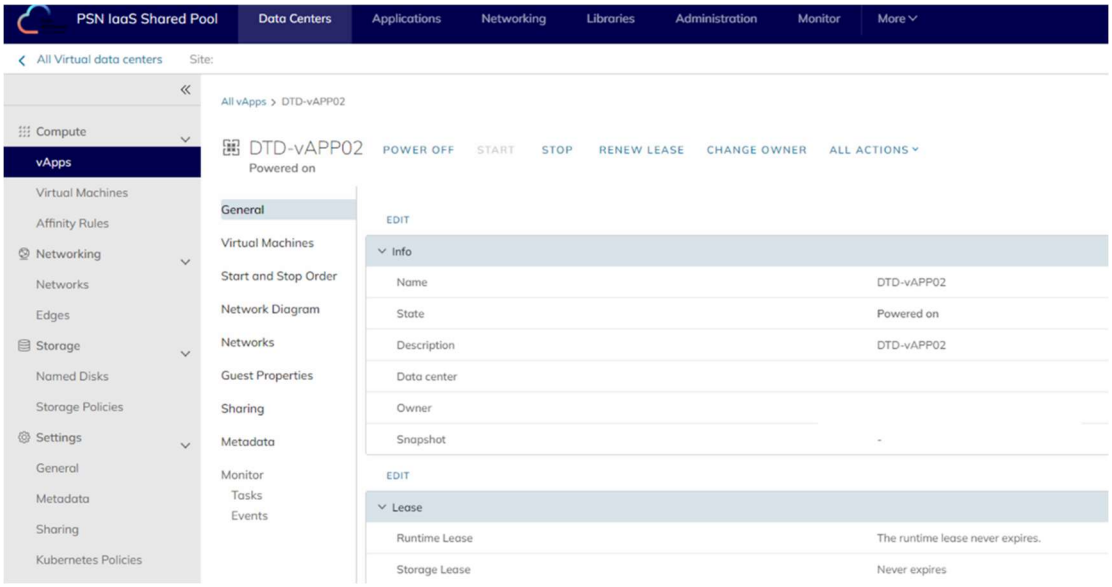


**Figura 16 -** Menu di dettaglio della vApp

b Visualizzare il **Network Diagram** della **vApp** (Figura 17)

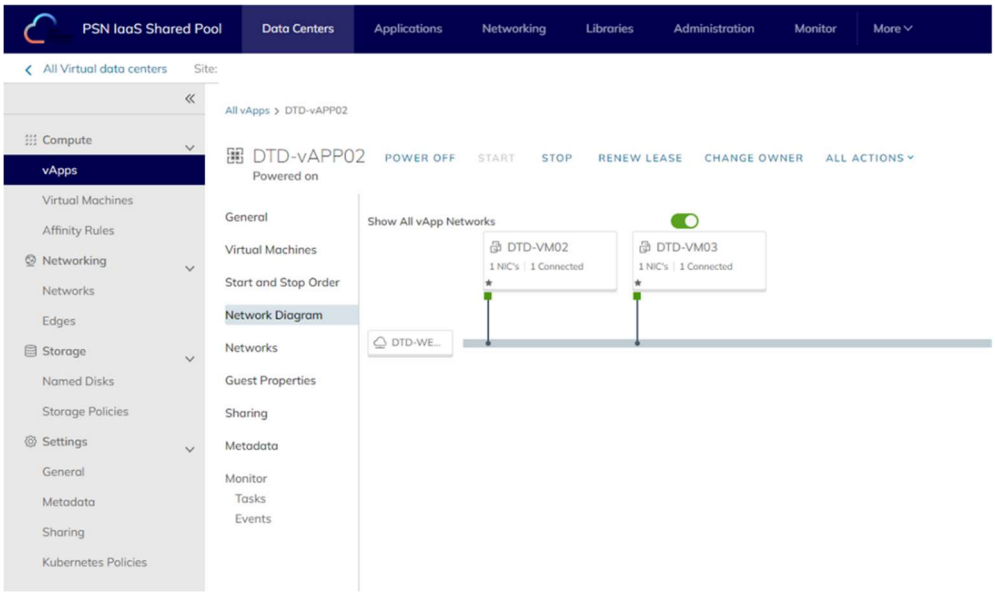


**Figura 17 -** Esempio di diagramma di rete di una vApp

c Analizzare la configurazione delle reti associate alla vApp tramite il tab Networks. I dettagli della configurazione saranno trattati nella sezione dedicata al Network

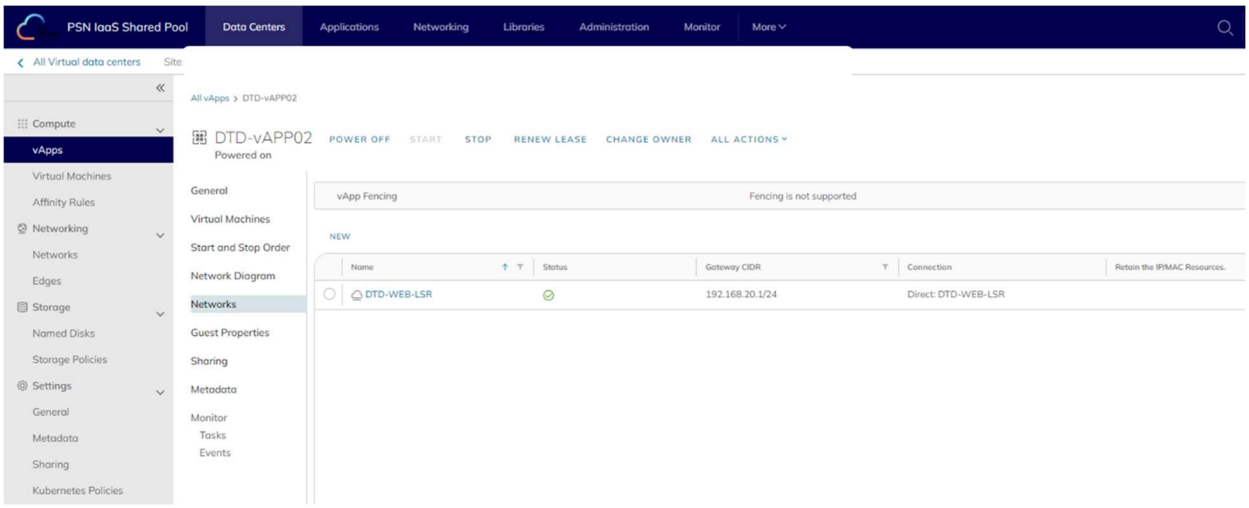


**Figura 18 -** Dettaglio della componente Networking associata ad una vApp

Dal menu Actions è invece possibile (**Figura 19**):

a Sospendere (**Suspend**), Spegnere (**Power Off e Stop**), Avviare (**Start**) e riavviare (**Reset**) l'esecuzione di una vApp e delle VM al suo interno

b Creare e gestire snapshot (**Create Snapshot**), riportare lo stato di una vApp al momento della creazione (**Revert Snapshot**) e rimuovere i punti creati (**Remove Snapshot**)

c Spostare (**Move to…**) e copiare (**Copy to…**) una VM su un profilo storage differente

d Aggiungere una VM ad un catalog personale (**Add to Catalog…)**

e Aggiungere una VM nuova nella vApp (**Add VM…**)

f Aggiungere una rete alla vApp (**Add Network…**)

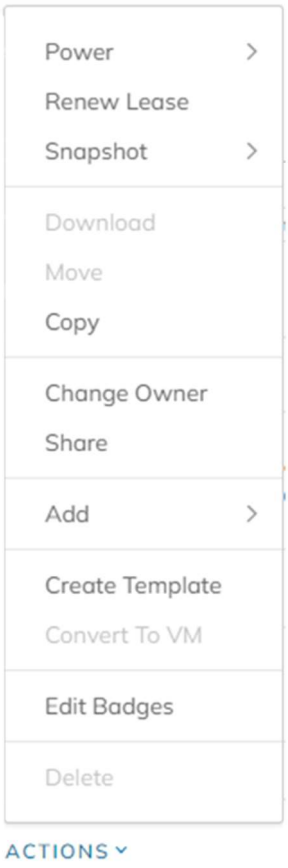


**Figura 19 -** Menu Action delle vApp

## 5.7 Come si configura e attiva una VM?

La configurazione e predisposizione di una **VM** si fa direttamente dal menu principale del nostro VDC dalla sezione **Virtual Machine**, di seguito sono descritti i metodi ed i passaggi principali come indicazione per la creazione di VM.

Le modalità di creazione di una VM sono 2:

1. Partendo da un'immagine presente nel catalogo (privato o pubblico PSN)
2. Configurando una VM dall'inizio ed installando il sistema operativo in modalità classica

## 5.8 Creazione di una VM da Catalogo

Di seguito sarà' descritta la procedura per la creazione di una VM partendo da un'immagine (template) già presente nel catalogo

1. Dalla sezione Virtual Machine, selezionare *"New VM"*, per far partire il wizard (**Figura 20**)

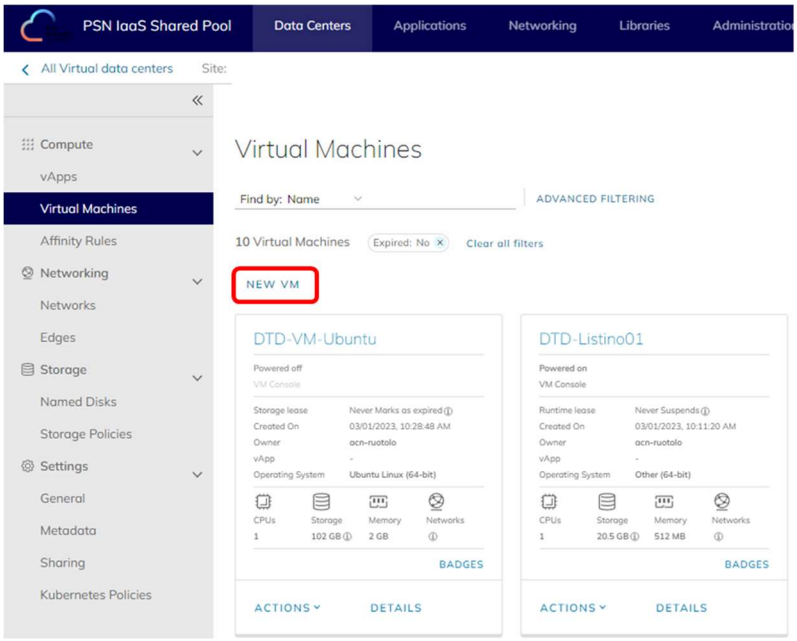


**Figura 20 -** Menu per la creazione di una VM

2. Nel wizard (**Figura 21**) indicare il Nome della VM e la descrizione (opzionale)
3. Selezionare *"From Template"*, per far comparire il catalogo messo a disposizione da PSN
4. Selezionare l'immagine da cui si desidera partire

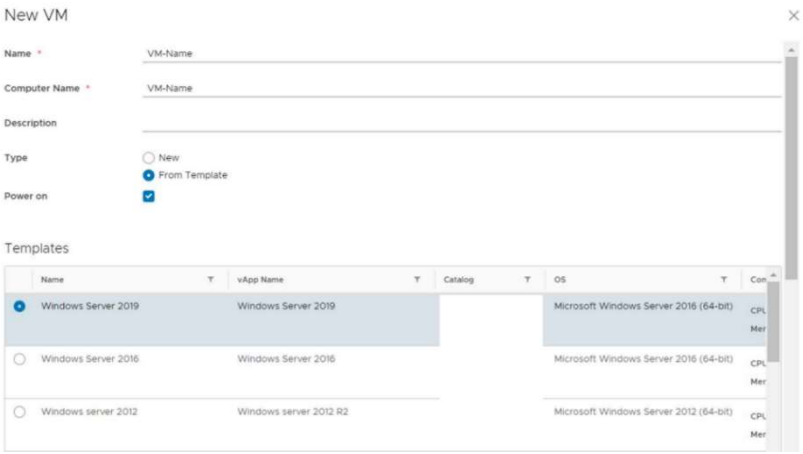


**Figura 21 -** Wizard di creazione di una VM da Template

## 5.9 Creazione di una VM da zero

Di seguito sara' descritta la procedura per la creazione di una VM da zero

a Dalla sezione Virtual Machine, selezionare **"New VM"**, per far partire il wizard (**Figura 22**)

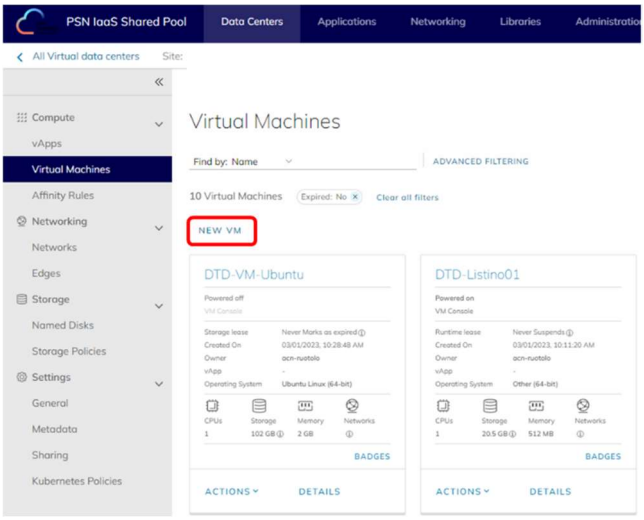


**Figura 22 -** Menu per la creazione di una VM

b Nel wizard (**Figura 23**) indicare il Nome della VM e la descrizione (opzionale)

c Come Type selezionare **"New"**

d Quindi indicare la famiglia (Family), la versione (Operating System) e l'immagine di installazione (Boot Image) del sistema operativo che vogliamo installare all'interno della VM (**Figura 23**)

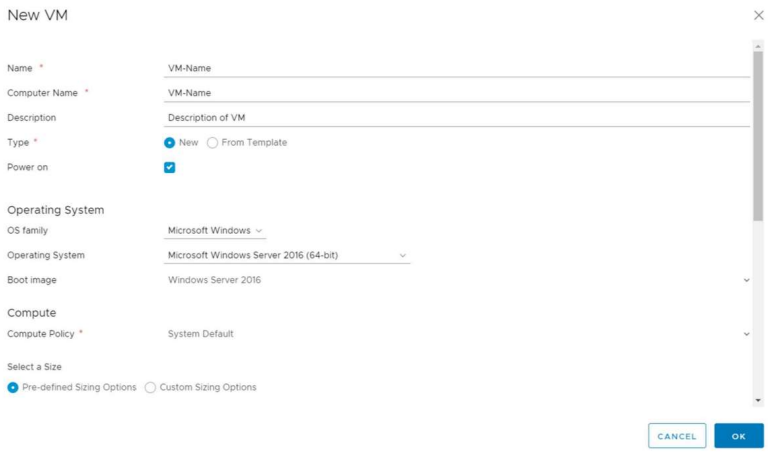


**Figura 23 –** Menu per la creazione di una VM

e Inserire nella sezione Compute i valori personalizzati di CPU, RAM e Memory (**Custom Sizing Options**). (**Figura 24**)


**Figura 24 –** Sezione Compute del wizard di creazione di una VM

f Selezionare il profilo di default e inserire le dimensioni del disco[1] delle VM. Da qui è anche possibile aggiungere ulteriori dischi dati già in fase di creazione, cliccando su "**Add"** (**Figura 25**)

[1] La Piattaforma PSN Cloud impone un limite di dimensione di ogni singolo *vDisk* a 1TB. Nel caso in cui la PA abbia necessità di volumi logici con spazio superiore al limite imposto dal *Service Provider*, dovrà configurare più *vDisk* e gestirli via *Volume Manager*.

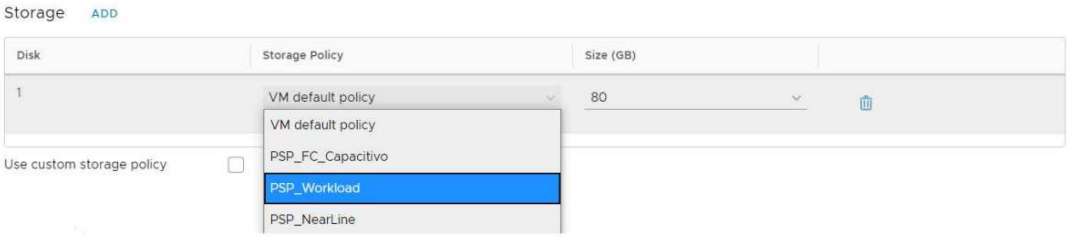


**Figura 25 -** Menu di selezione delle dimensioni dello storage

g Selezione e configurazione della scheda di rete associata alla VM, bisognerà quindi indicare su quale rete, presente nel VDC, associare la VM, quale tipologia di scheda utilizzare (si consiglia VMXNET3), e la tipologia di assegnazione dell'IP. Maggiori dettagli riguardo a queste configurazioni saranno riportati nella sezione dedicata Network. (**Figura 26**)

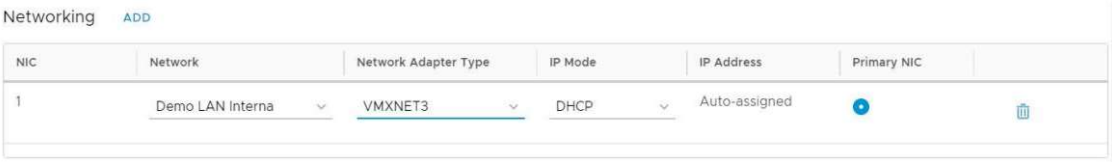


**Figura 26 -** Menu di selezione della rete di una VM

- ***Cloud-init***

Il cloud-init è uno strumento integrato nativamente con i sistemi operativi più diffusi e permette la personalizzazione delle VM automaticamente durante la fase di accensione, basandosi su un file di configurazione. Questo strumento può essere utilizzato nella customizzazione dei private template per la standardizzazione degli stessi.

Il cloud-init può essere configurato, in base alle proprie esigenze, secondo le linee guida di documentazione ufficiale (cloud-init 23.2 documentation (cloudinit.readthedocs.io); ad esempio, può essere utilizzato per effettuare le seguenti personalizzazioni di base:

- Disabilitare l'accesso in ssh all'utenza di root
- impostazione della time-zone
- impostazione layout tastiera italiano
- creazione di utenze di servizio

Ogni PA può eseguire in maniera autonoma la customizzazione del cloud-init o, in alternativa, rivolgersi ai servizi professionali per poter implementare i propri template in un Private Catalog.

## 5.10 Come è possibile controllare e gestire la configurazione delle VM?

Accedendo alla sezione principale del VDC e andando nel menu Virtual Machine, avremo la rappresentazione a blocchi o ad elenco delle VM (**Figura 27**).

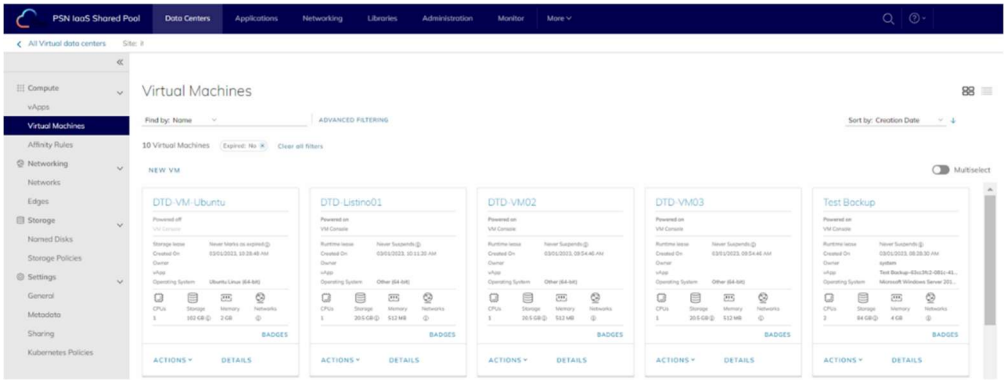


**Figura 27 -** Menu Virtual Machine del VDC

Per ogni VM avremo la possibilità di verificare i dettagli (**Details**) della configurazione di una VM, poter eventualmente modificare alcune impostazioni come le risorse (CPU, RAM, Disco e Rete) assegnate alla VM dalla sezione **"Hardware"** (**Figura 28**).

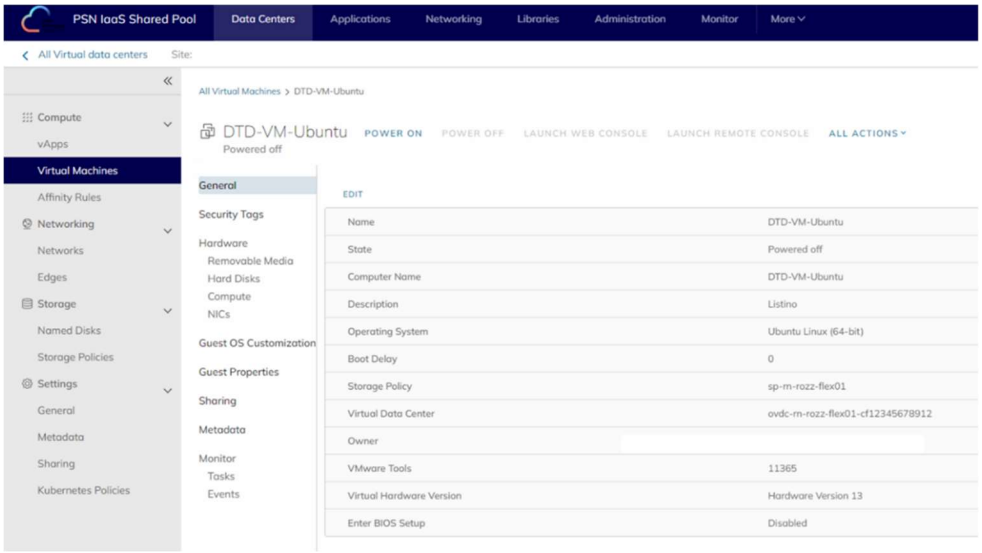


**Figura 28 -** Menu Details di una VM

Dalla sezione Vitrual Machine, sarà inoltre possibile eseguire alcune operazioni tramite il menu "**Actions"** sulla VM stessa come (**Figura 29**):

a Gestire lo stato di esecuzione di una VM (**Suspend, Shutdown Guest OS, Power Off, Power On, Reset**)

b Installare i tool di gestione e integrazione con l'hypervisor (**Install VMware Tools**)

c Gestire file media (emulazione di CD e DVD) (**Inser Media, Eject Media**)

d Creare e gestire snapshot (Create Snapshot), riportare lo stato di una VM al momento della creazione (Revert Snapshot) e rimuovere i punti creati (**Remove Snapshot**)

e Eseguire la console di una VM per poter gestire i servizi al suo interno (**Launch Web Console, Launch Remote Console, Download VMRC**)

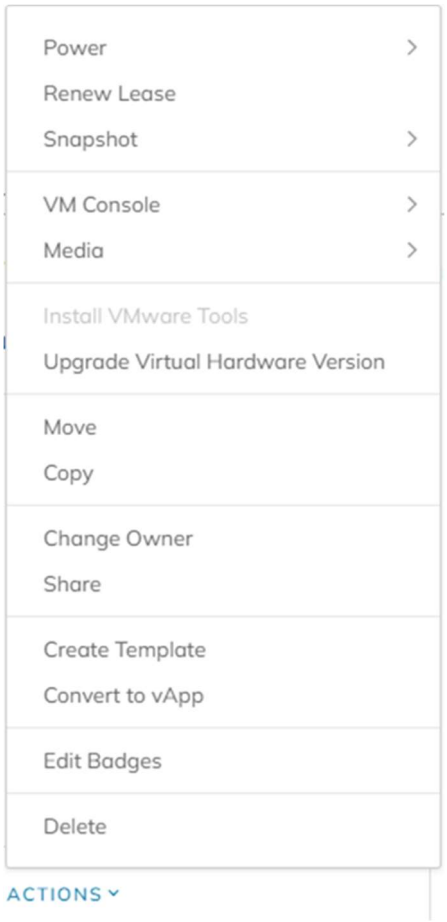


**Figura 29** -Menu Action delle VM

## 5.11 Come accedo ad una VM creata?

Di seguito la procedura per poter accedere ad una VM, ed interagire con il Sistema operativo:

- Dal menu "*Actions*" della VM Stessa

Selezionare la modalità di accesso desiderato:

- Lunch WEB Console (sessione Interattiva HTML)
- Lunch VM Remote Console (necessario il tool VMRC)

## 5.12 Con quali credenziali accedo al Sistema Operativo?

Nella fase di creazione di una VM, il processo di provisioning esegue la generazione randomica di una "Password" temporanea che dovrà essere necessariamente aggiornata al primo accesso sul Sistema Operativo.

Di seguito la procedura per effettuare il recupero delle credenziali ed eseguire le operazioni di Update della Password:

1. Selezionare la VM relativa nel menu "Macchine Virtuali" / "Virtual Machine"
2. Selezionare "*Dettagli*" /Details", in questo modo si accede al dettaglio della VM
3. Nel menu di dettaglio, selezionare *"Personalizzazione di sistema operativo guest"*
4. Selezionare "*Modifica*"
5. Recuperare la Password (one-time Password) selezionare la password nel Campo "*Specifica Password*" eseguire la Copia con il tasto destro del Mouse e salvare la Password in un File testo di Appoggio)
6. Chiudere la Schermata di dettaglio (con X o con il tasto "Ignora")
7. Eseguire il Logon al Sistema Operativo con Utenza1 e la Password (one-time Password), precedentemente copiata, dalla Web Console o dalla Remote Console
8. Inserire una nuova Password relativa all'account Locale del Sistema

[1] Di seguito la tabella relativa degli account di default dei sistemi Operativi:

| Sistema Operativo | Amministratore di Default |
|---|---|
| Windows OS (2016/2019/2022) | Administrator |
| Linux OS | root |

**Tabella 7.** Elenco Account di Default

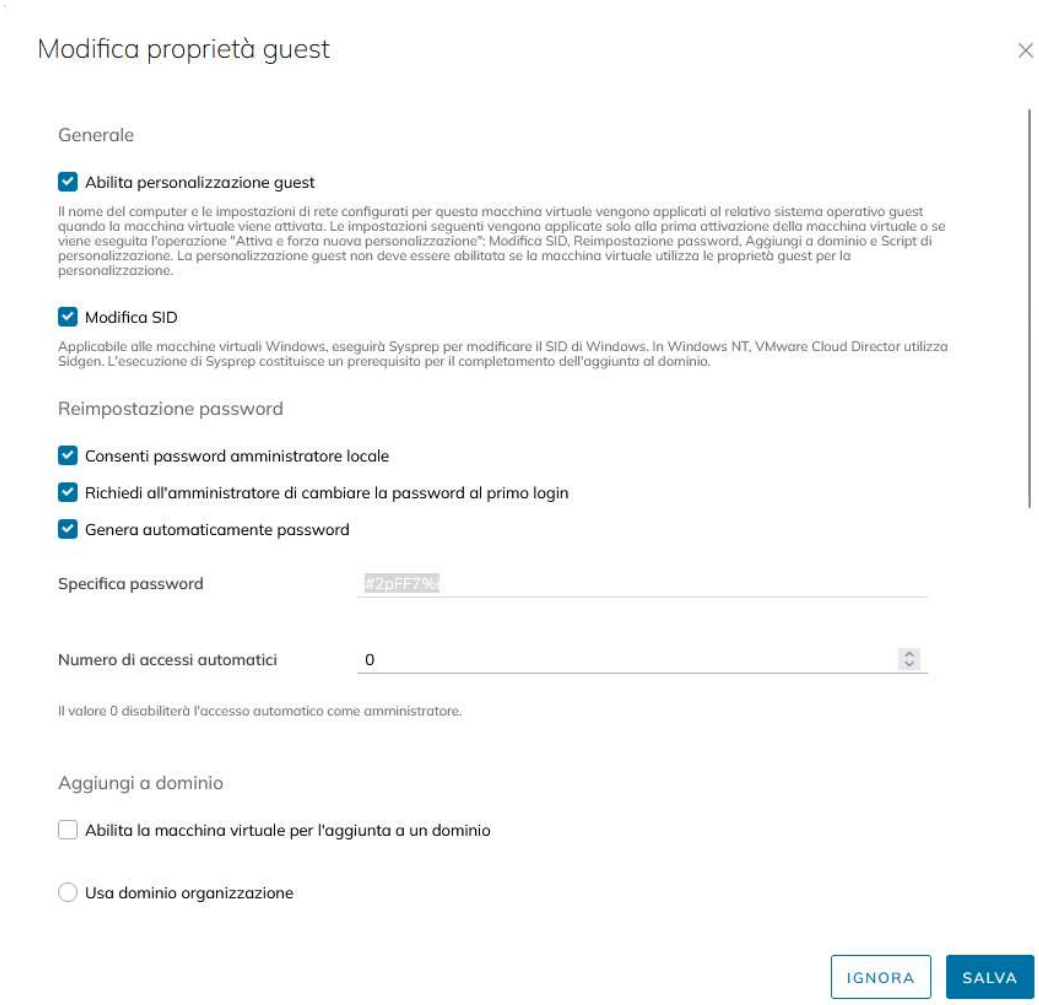


**Figura 30-** Step 5 della Procedura di Recupero delle Credenziali

## 5.13 Quali sono le configurazioni massime per ogni vApp?

Una Organization può contenere al massimo 5000 vApp.

Una vApp può contenere al massimo **128 Virtual Machine**. Per ogni Virtual Machine valgono i seguenti limiti massimi:

- **Virtual CPUs** per Virtual Machine (Virtual SMP): **128**
- **RAM** per Virtual Machine: **6 TB**
- **Virtual NICs** per Virtual Machine: **10**

## 5.14 È possibile effettuare modifiche "a caldo" sulle VM (Core, RAM e Storage)?

Per poter apportare modifiche (in incremento) su una VM in termini di CPU e RAM è necessario che siano stati precedentemente impostati appositi flag **di Virtual CPU hot add e Memory hot add** nella sezione **Details/Hardware/Compute** della Virtual Machine e che il sistema operativo supporti tale funzionalità (**Figure 31 e 32**).

La modifica a caldo è quindi possibile. Dipende però dalla compatibilità del sistema operativo utilizzato con tale modalità di aggiornamento della VM.

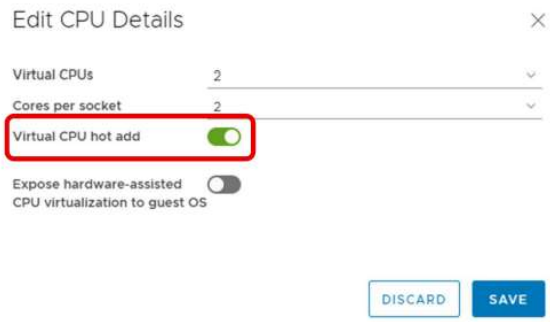


**Figura 31 -** Schermata configurazione vCPU


**Figura 32 -** Schermata configurazione vRAM

In caso contrario, le modifiche alle configurazioni delle VM possono essere fatte a macchina spenta, pertanto è necessario prima spegnere la macchina e poi è possibile apportare le modifiche.

## 5.15 È previsto un accesso NAS allo storage?

Si, è un servizio aggiuntivo da richiedere su una separata offerta.

## 5.16 Posso ampliare un disco precedentemente allocato ad una VM?

Si, è possibile eseguire la funzione di ampliamento della dimensione di un virtual disk (se vi sono risorse disponibili a livello di VDC, in caso contrario è necessario quotare un'estensione delle risorse storage associate al servizio Virtual Data Center).

Non è invece possibile eseguire una riduzione.

**NOTA**: una volta eseguito l'espansione del disco a livello di VM, sarà necessario espandere il volume a livello di sistema operativo, perché' questo possa essere utilizzato

## 5.17 Posso agganciare uno storage condiviso tra più nodi?

No, un disco può essere visto solo da una VM.

## 5.18 La PA ha la possibilità di eseguire degli snapshots delle VM?

Si, è possibile effettuare lo snapshot di una intera vApp oppure delle singole VM (con il vincolo di poter gestire al più uno snapshot per ogni VM). Lo snapshot viene eseguita sui Data Store che ospitano i dischi storage della VM (non è possibile selezionare altri volumi).

## 5.19 Quali sono le feature di High Availability disponibili?

Sulla piattaforma PSN sono attivi strumenti ed algoritmi per garantire l'alta disponibilità (per cui se un host che ospita la nostra app o VM diventa indisponibile le macchine su di esso vengono riavviate su altri host disponibili)

## 5.20 È possibile impostare regole di affinità / anti-affinità' tra le VM?

Si, se vi è la necessità di avere 2 o più VM operative sullo stesso host fisico oppure viceversa, per maggiori garanzie operative, avere la certezza che 2 o più VM non stiano sullo stesso host fisico, è possibile impostare le Affinity Rules, direttamente dal menu principale del VDC (**Figura 33**).

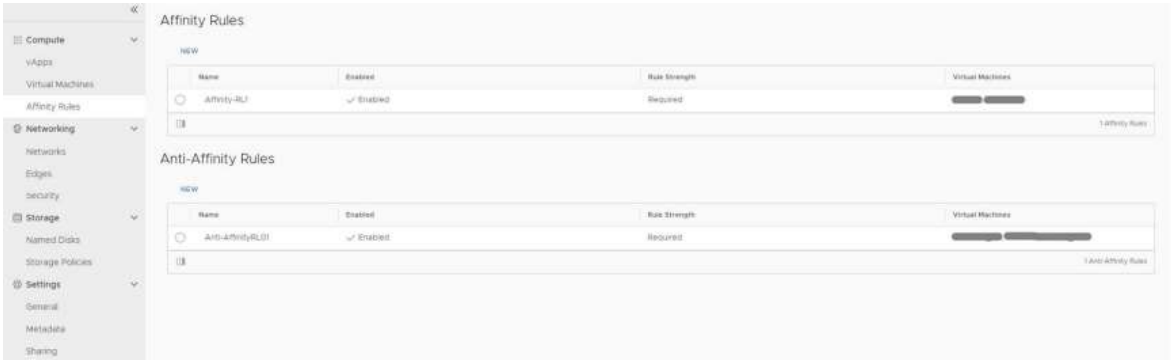


**Figura 33 -** Schermata di gestione delle Affinity Rules

## 5.21 Una PA che ha due organization può spostare/copiare in autonomia una vApp da una organization a un'altra?

Non è possibile copiare/spostare una vApp mediante singolo comando tra una organization ed un'altra, né tantomeno è possibile condividere un catalogo privato tra Organization diverse.

In alternativa, è possibile effettuare l'export dei template relativi alle vApp della prima Organization e poi procedere all'import del template sulla seconda Organizzazione.

# 6 Cataloghi

## 6.1 Come posso creare un Organization Catalog?

È possibile creare dei cataloghi privati della singola Organization importando dei template da fonti esterne. Tali template potranno poi essere utilizzati per creare in maniera più veloce e semplice vApp e singole VM all'interno dell'ambiente Virtual Data Center

a Accedere alla sezione **"Libraries"** del portale

b Dal menu di Sinistra andare in **"Catalogs"**

c Fare quindi click su **"New"**

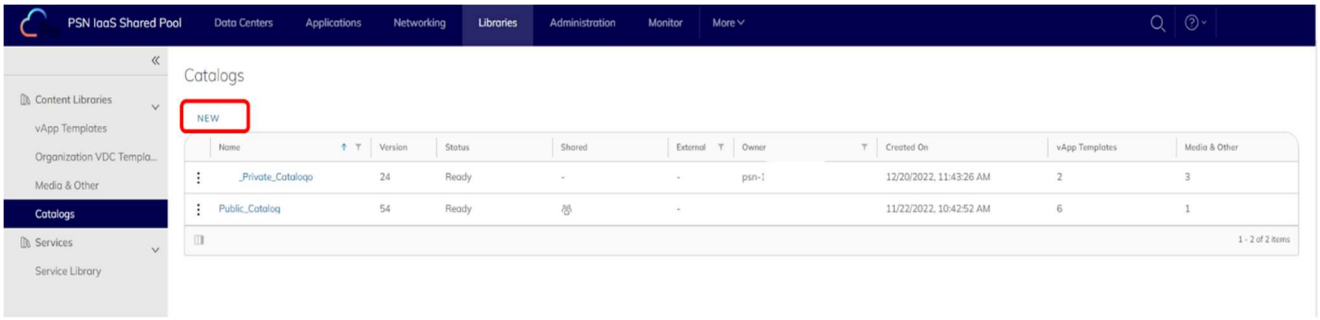


**Figura 34 -** Schermata menu Libraries per la gestione dei Cataloghi

d indicare il nome da assegnare al catalogo

e Opzionale: è possibile anche indicare uno storage profile dove sarà distribuita l'applicazione ogni volta che sarà predisposta, selezionando **"Pre-provisioning on specific storage policy"**

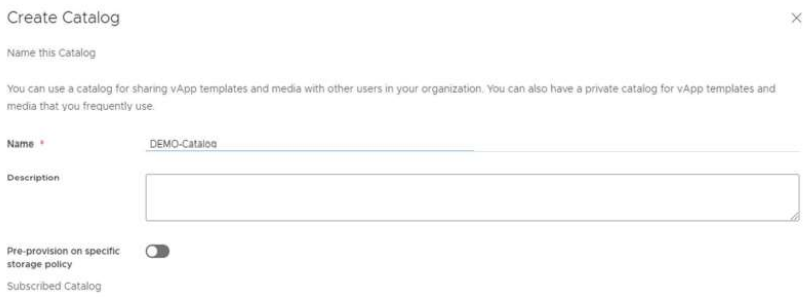


**Figura 35 -** Wizard di creazione di un nuovo catalogo

## 6.2 Come posso caricare nuovi template all'interno del catalogo privato dell'Organization?

Una volta disponibile il catalogo 'privato', è possibile importare dei template di VM.

Per procedere nell'import del template seguire i seguenti passaggi:

a Cliccare su **"Libraries"**

b Spostarsi nella scheda **"Media & Other"**

c Cliccare su **"Add"**

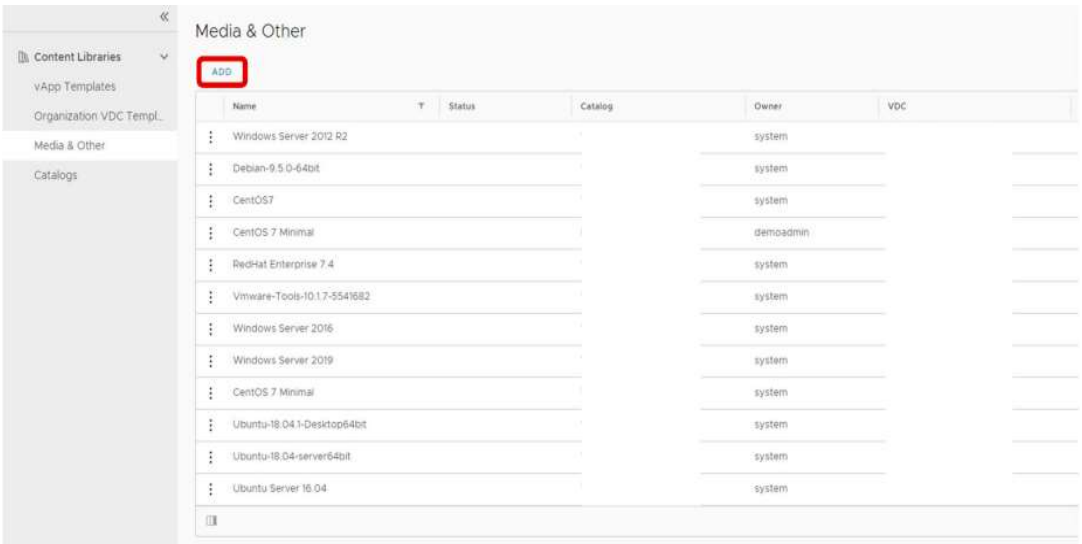


**Figura 36 -** Upload template VM

d indicare il nome dell'immagine che si sta caricando

e Selezionare la funzione per il caricamento del file immagine da caricare

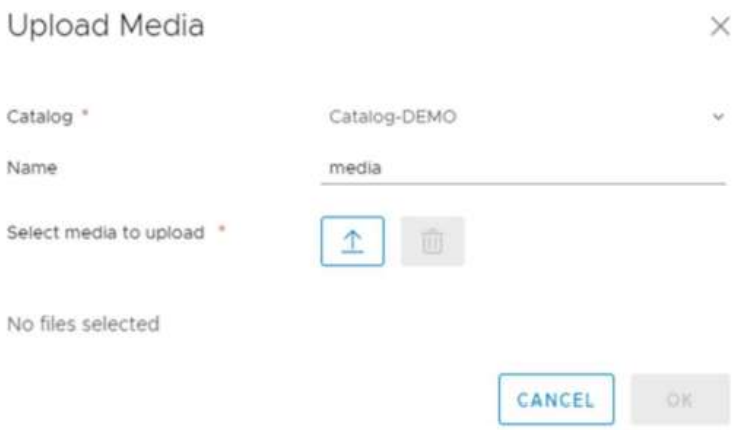


**Figura 37 -** Upload template VM

**Nota**: è fondamentale inserire anche l'estensione (es. .iso) altrimenti il prodotto potrebbe non riconoscere correttamente l'immagine.

# 7 Network

Nel servizio di PSN Cloud Platform esistono diverse tipologie di reti. Le principali tipologie di network che condizionano l'utilizzo dello strumento sono le seguenti:

- **External network** (o anche **Edge Gateway**). Tali reti sono gestite e configurate da PSN sulla base delle indicazioni fornite dai Clienti o in base a quanto acquistato in fase di accesso al servizio (**si precisa che il servizio prevede un acquisto di default di un piano d'indirizzamento pubblico /29**).

  Ad integrazione per maggior dettaglio si forniscono le due subnet pubbliche (External Network) associate alle Region e dalle quali verranno estrapolate le Subnet IP dedicate poi ad una PA e al suo workload, come indicato in tabella:

| Region | Public Subnet |
|---|---|
| **Cloud Region Nord** | 81.126.64.0/21 |
| **Cloud Region Sud** | 81.126.72.0/21 |

**Tabella 8.** Mapping Region-Public Subnet

- **Organization Network**. Si tratta di reti interne al Virtual Data Center tramite le quali le vApp possono comunicare tra di loro e/o raggiungere le reti pubbliche (tramite l'Edge Gateway)
- **vApp Network.** Sono reti interne alle vApp che possono essere collegate alle Organization Network e consentono di mettere in comunicazione le VM tra di loro (all'interno della vApp) e verso il resto dell'Organization

Nell'Organization possono esistere anche reti 'isolate' all'interno del VDC (ovvero non connesse con l'External Network). Tali reti sono le **Internal Network**. Si vedrà un esempio nella prossima sezione.

Di seguito si riporta un ulteriore sintesi e approfondimento legato alle varie tipologie di reti.


**Figura 38 -** Tipologie di reti previste dalle soluzioni PSN Cloud Platform

Se l'Organization (e le vApp) devono avere connettività con il mondo esterno è necessario disporre di una **Rete Esterna**. Si tratta di una rete gestita da PSN Cloud Platform dall'esterno del pool di risorse elaborative (può essere ad esempio un collegamento Internet o MPLS).

La Rete di organizzazione viene utilizzata per il traffico interno alla organizzazione e consente la comunicazione tra tutte le vApp. L'amministratore dell'organizzazione può gestire le proprie reti, inclusi i relativi servizi di rete.

Una Rete di vApp consente di stabilire il modo in cui le macchine virtuali di una vApp possono comunicare. Le vApp possono essere:

- **ruotate** (attraverso l'Edge Gateway) verso l'External network
- isolate dalle altre vApp dell'organizzazione

Si veda anche **Figura 39**.

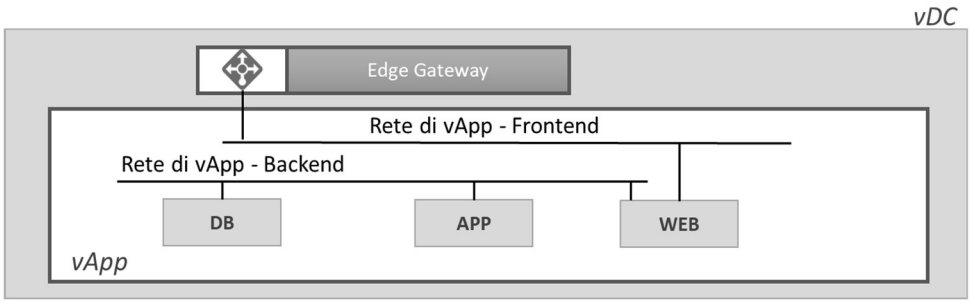


**Figura 39 -** Diagramma di un possibile scenario di rete per il servizio VDC

## 7.1 Come posso gestire e creare le Organization Network?

Per configurare le **Organization Network** è necessario accedere al proprio **Virtual Datacenter** e spostarsi nella sezione **"Networking – Networks"**, da qui potremo gestire, aggiungere ed eventualmente rimuovere le nostre reti.

La creazione delle Network con la funzionalità di distribuite firewall attiva (Firewall Est-Ovest) deve essere eseguita selezionando lo *Scope* **Data Center Group** come indicato in Figura 41.

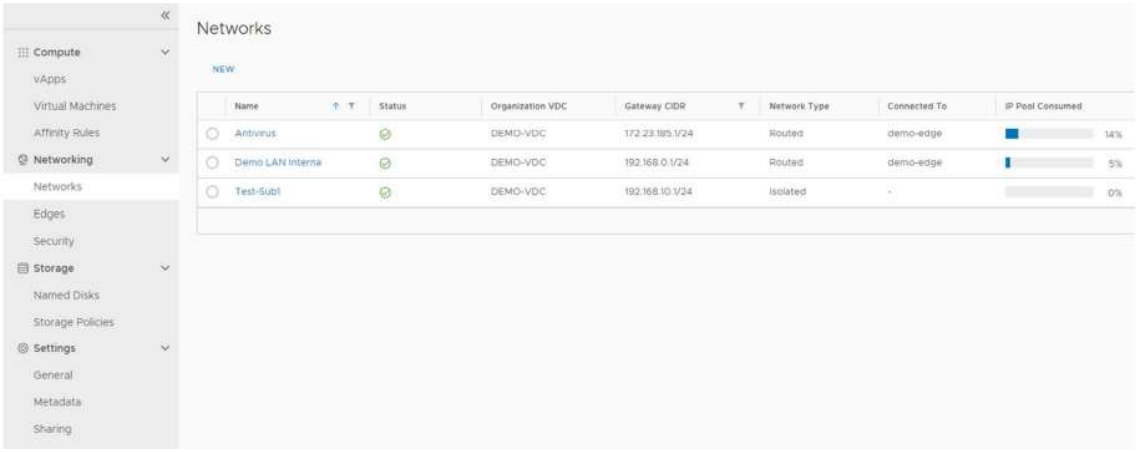


**Figura 40 -** Schermata amministrativa della sezione Network

Da tale sezione è possibile modificare le reti già create o istanziarne di nuove, cliccando su **"New"** e selezionando *Data Center Group,* nella sezione *Scope:*

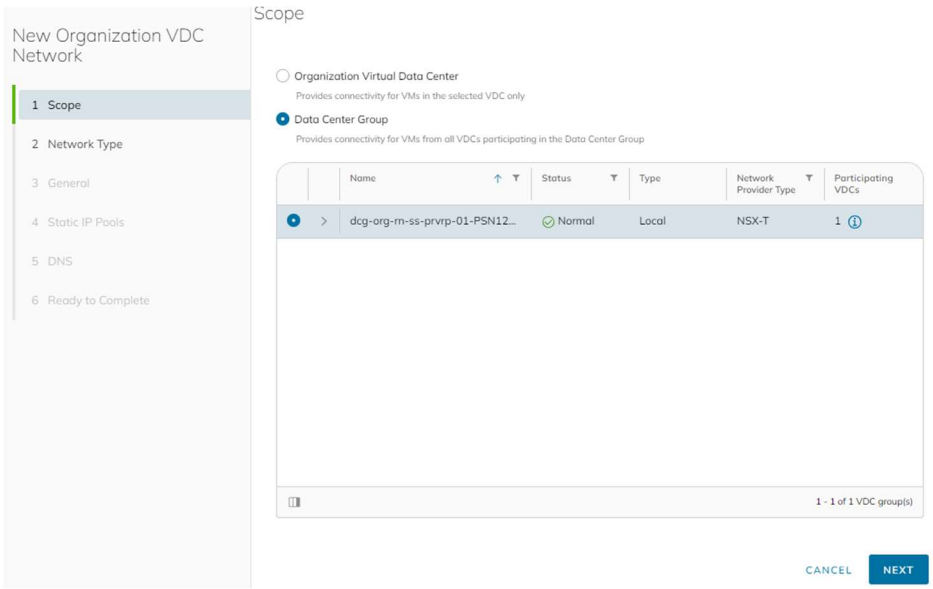


**Figura 41** - Creazione Network, selezione Scope

È possibile creare una rete isolata all'interno del Virtual Data Center oppure collegata all'Edge Gateway (quindi alle reti pubbliche esterne).

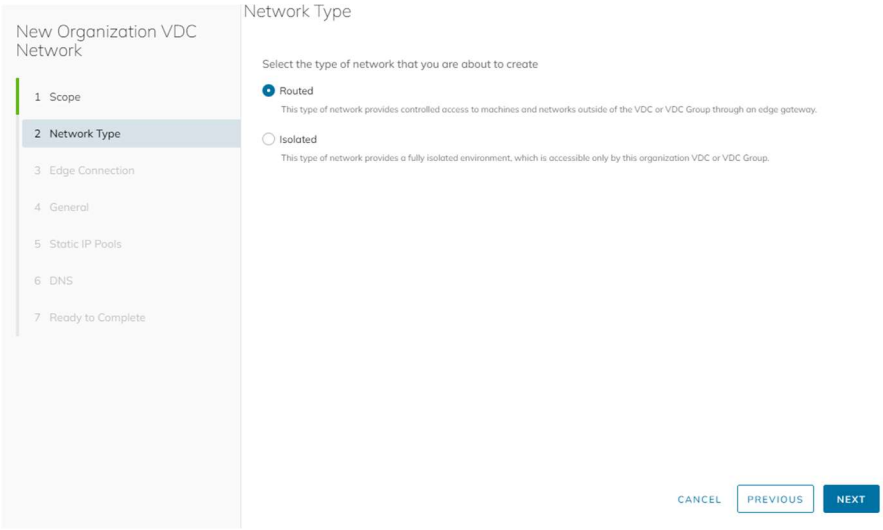


**Figura 42 -** Selezione tipologia di rete

Nel wizard di configurazione della rete ti verranno richieste alcune informazioni obbligatorie come

Nome della rete e indirizzo IP del gateway della rete (Gateway CIDR).

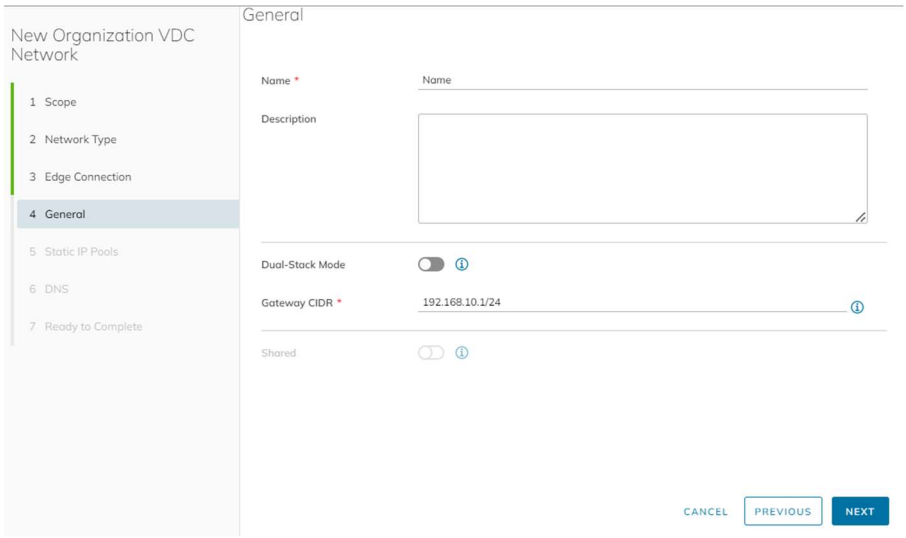


**Figura 43 -** Wizard di configurazione di una rete

Successivamente avrai la possibilità di completare le impostazioni, facoltative, della rete stessa come un gruppo di IP statici (**Static IP Pool**) e le configurazioni **DNS** da impostare automaticamente alle VM agganciate alla vnet.

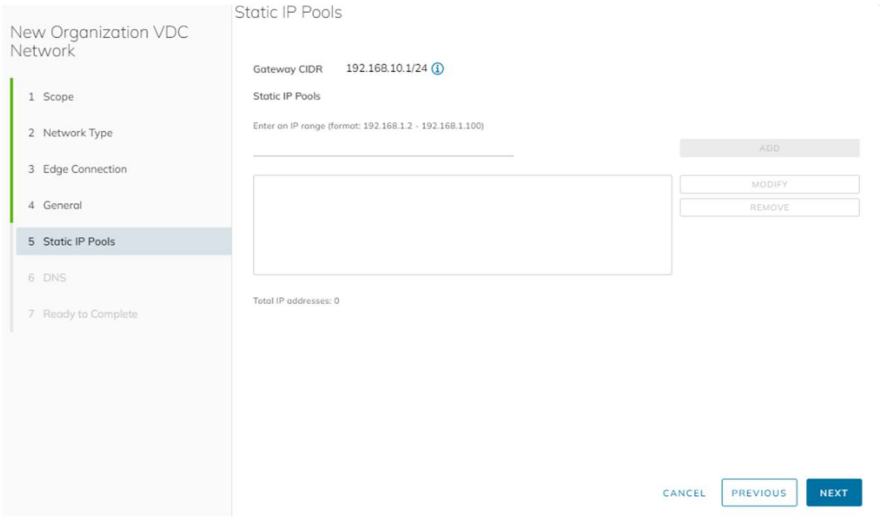


**Figura 44 -** Wizard di configurazione di una rete

## 7.2 Come posso creare e gestire le reti interne alle vApp?

Ogni vApp può essere associata ad una o più Organization VDC Network.

È poi possibile creare una rete interna alla singola vApp agendo dal pannello di configurazione della vApp stessa.

Ad esempio, partendo dalla singola vApp, selezionando **"Details"** si può accedere al tab **"Networks"** e:

a visualizzare le reti già associate alla vApp

b oppure, creare una nuova rete vApp o associare una rete di tipo Organization già esistente (**Figura 45**)

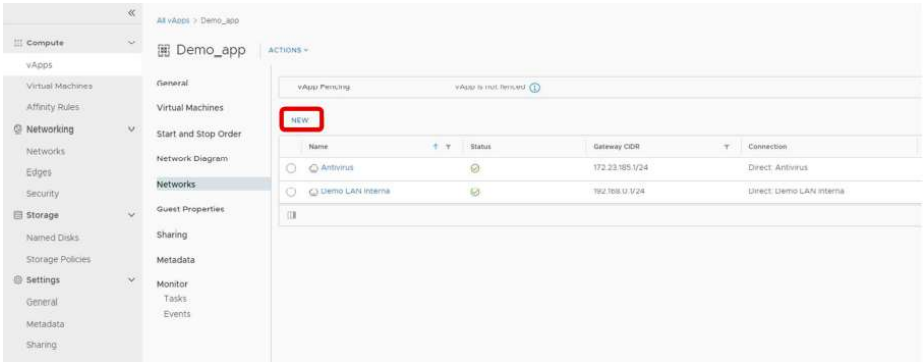


**Figura 45 -** Vista delle reti associate alla vApp di riferimento

## 7.3 Posso annunciare le reti private all'interno del backbone PSN?

Si. Mediante la funzionalità BGP, posizionandosi nella sezione Edge Gateways, gestione degli annunci (Route *Advertisement*) è possibile annunciare la *private network* cliccando su *Edit*.

Questa funzionalità abilita il colloquio con elementi di servizio esterni alla Piattaforma PSN Cloud.

## 7.4 Posso utilizzare il DHCP in autonomia?

L'amministratore dell'organizzazione può (durante la creazione della VM o della vApp – si vedano

sezioni precedenti) abilitare il servizio DHCP per una rete di organizzazione, connettendo una scheda NIC sulla macchina virtuale dell'organizzazione a tale rete e selezionando DHCP come modalità IP della scheda.

Il sistema assegna un indirizzo IP DHCP alla macchina virtuale quando questa viene attivata.

## 7.5 Dove trovo gli indirizzi IP Pubblici associati al mio Virtual Data Center?

Nel caso di Virtual Data Center con connettività diretta[1], è possibile visualizzare gli indirizzi IP Pubblici associati accedendo alla sezione **"Networking – Edges"** del Virtual Data Center. Selezionare il **"gateway edge"** relativo alla propria organizzazione e spostarsi nel menu "**IP Allocations"**, saranno mostrati gli IP pubblici a disposizione con la relativa subnet (**Figure 46 e 47**).

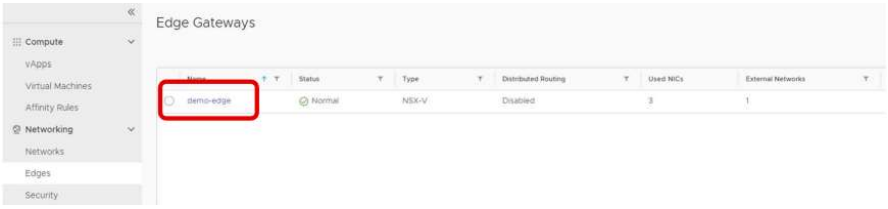


**Figura 46 -** Elenco dei Gateway Edge

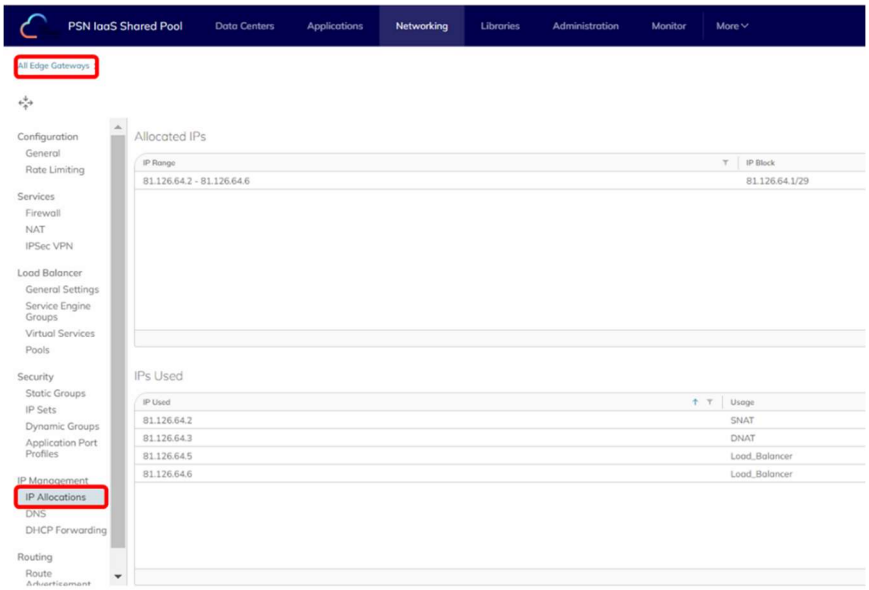


**Figura 47 -** Schermata IP Allocations del Gateway Edge

**[1]Per connettività diretta si intende una connettività intermediata da firewall esterni**

## 7.6 Come posso configurare le regole di firewalling e natting?

Per configurare le regole di firewalling e natting è necessario accedere alla sezione **“Networking – Edges”**, selezionare il **“gateway edge”** della propria organizzazione e successivamente Services (**Figura 47**)

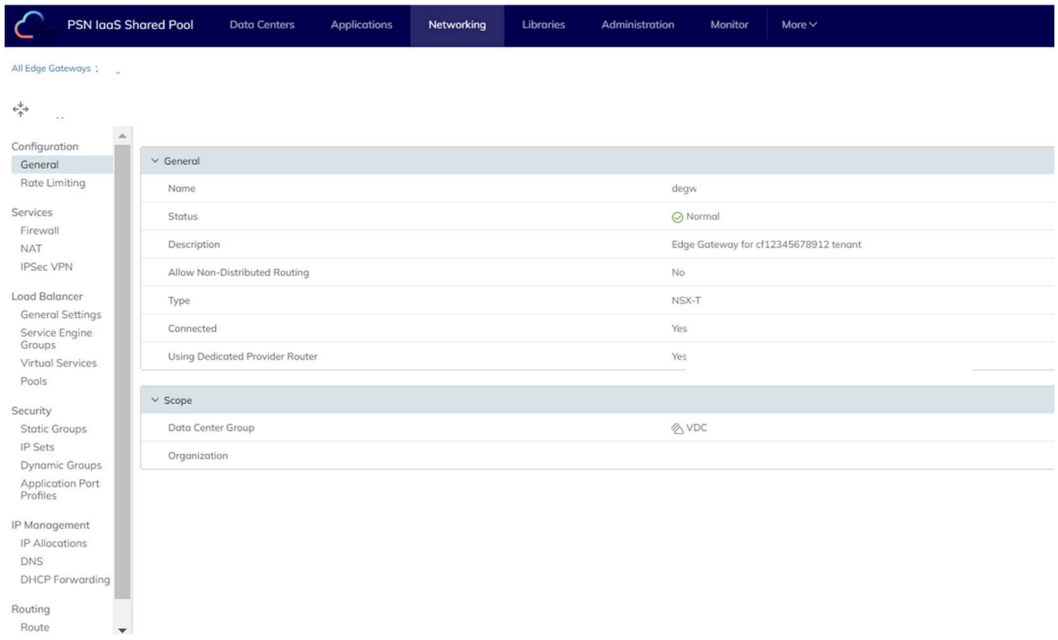


**Figura 48 -** Schermata riepilogativa del Gateway Edge

Nella schermata che apparirà è possibile configurare tutti i servizi disponibili sull’Edge: Firewall, DHCP, NET, Rounting, Bilanciamento di carico, VPN, ecc.

Per creare una nuova regola firewall selezionare il Tab **“Firewall”** e poi cliccare sul tasto + per aggiungere una nuova regola. Una volta aggiunta la regola potrà essere personalizzata andando a specificare:

- Nome
- Origine
- Destinazione
- Servizio

- Azione (Nega o Accetta)

Per i campi Origine e Destinazione è possibile aggiungere Oggetti Network già esistenti (es. una intera LAN) cliccando sul tasto +, oppure definire puntualmente il singolo indirizzo IP cliccando sul tasto IP. È possibile anche l'ordine di applicazione delle regole Firewall ordinandole tramite i tasti SU e GIU. Una volta completate le modifiche è necessario cliccare sulla voce in alto a destra "Salva modifiche" per applicare le regole all'Edge.

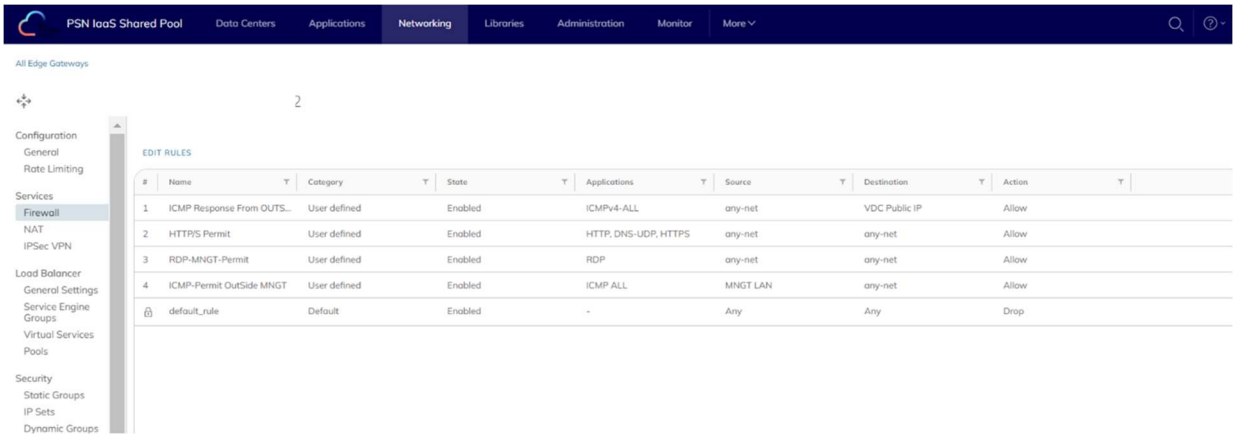


**Figura 49 -** Menu di gestione del Edge Gateway

Allo stesso modo è possibile definire regole di NAT selezionando il Tab NAT.

Nel caso in cui si ha la necessità di Firewall distribuiti (Est-Ovest) vanno prima creati i gruppi di applicazione nella sezione IP Set e poi va configurata la regola Firewall come descritto precedentemente.

È possibile aggiungere regole di Static NAT cliccando sul pulsante + **Regola SNAT** o Dinamic NAT cliccando sul pulsante + **Regola DNAT**.

In funzione della tipologia di regola scelta è possibile definire:

- L'interfaccia di rete su cui applicare la regola
- L'intervallo di indirizzi IP origine da convertire

- L’intervallo di indirizzi IP in cui convertirli
- Solo nel caso di regole DNAT, anche un protocollo e porta da convertire

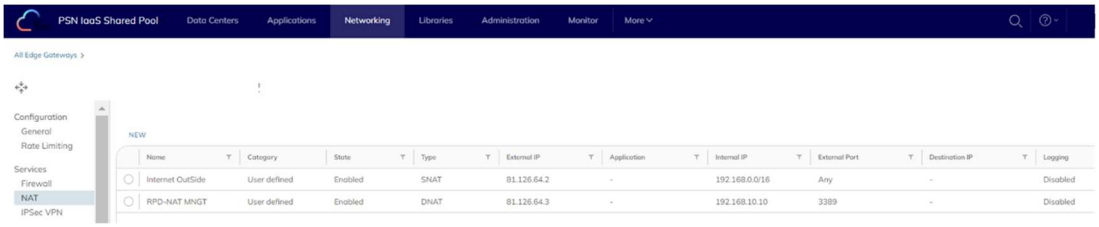


**Figura 50 -** Menu di configurazione delle NAT all’interno del Edge Gateway

Una volta completate le modifiche è necessario cliccare sulla voce in alto a destra “**Salva modifiche**” per applicare le regole all’Edge.

## *7.7 Quali tipologie di VPN sono implementabili?*

Nel servizio Virtual Data Center possono essere configurate due tipologie di VPN:

- VPN Lan-to-Lan (tunnel IPSec) – T1[2]
- VPN Client -to-Lan /SSL VPN)[3]

[2] In questa modalità la VPN è terminata sul EDGE GATEWAY Firewall di servizio mediante le funzionalità native offerte nel servizio PSN Cloud Platform.

[3] Questa modalità di VPN è configurabile in autonomia da parte della PA prevedendo ed installando sulla propria organizzazione le componenti (ad es. una VM con un’immagine di virtual firewall) necessarie al funzionamento.

## 7.8 È possibile configurare più subnet all'interno di un tunnel VPN?

Si.

## 7.9 È possibile accedere alle VM in modalità VPN client?

La VPN nativamente supportata è del tipo VPN IPSec LAN-TO-LAN e sono configurate a livello di EDGE Gateway Firewall.

Eventualmente la PA può:

- creare all'interno della propria Organization una VM Windows o Linux configurata come server VPN (VPN concentrator)

## 7.10 È possibile terminare più sessioni VPN IPSec differenziate verso l'Organization?

Si.

## 7.11 Ci sono vincoli a fornire contemporaneamente accesso internet e MPLS alla piattaforma?

No.

## 7.12 Quanti IP pubblici possono essere richiesti?

Gli IP pubblici vengono resi disponibili in pool definiti in Subnet IP (da un size minimo di /29), la PA ha la facoltà di richiedere ulteriori Subnet IP.

## 7.13 Gli IP pubblici vengono usati come nat o assegnati direttamente alle macchine?

Gli IP pubblici vengono associati alla External Network sul EDGE GATEWAY (T1).

La configurazione dei NAT verso le External Network viene gestita a partire dal pannello **Org VDC Networks** del Virtual Data Center (opzione Configure Services).

## 7.14 È possibile creare all'interno della stessa organization "external network" diverse che fanno riferimento ad altrettanti collegamenti MPLS?

Si.

## 7.15 Ci sono dei vincoli o dei limiti nell'impiego dei firewall virtuali che possono essere istanziati nelle vApp Network tramite le funzionalità native della piattaforma?

Il firewalling è previsto nella piattaforma ed è vincolato alle funzionalità messe a disposizione dai moduli PSN Cloud Platform.

## 7.16 Quali sono i passi da seguire per pubblicare una VM su un IP pubblico dell'organizzazione?

La pubblicazione delle VM su IP Pubblici richiede essenzialmente i seguenti passaggi:

- Selezione dell'IP Privato della macchina da esporre su IP Pubblico tramite il tab *Virtual Machines* del *virtual host* in questione
- Verifica degli IP Pubblici assegnati all'External Network e di quelli ancora utilizzabili.
- Impostazione delle regole di firewalling sull'External Network
- Configurazione delle regole di NAT per mappare l'IP Pubblico con l'indirizzamento privato della VM

Gli ultimi due passaggi sono gestiti da PSN e quindi devono essere richiesti tramite *service request*.

Naturalmente la PA deve aver verificato che anche il *routing* del traffico tra VM (quindi vApp network), la rete dell'Organizzazione e la relativa External Network sia stato correttamente impostato nelle fasi di configurazione della vApp e della VM stessa.

## 7.17 Come è possibile accedere alla console delle singole VM?

Per poter accedere alla console di una VM, è necessario accedere al portale vCloud Director, da qui spostandosi all'interno del proprio Virtual Datacenter nella sezione *"Virtual Machines"*. Qui compare' l'elenco di tutte le VM a catalogo, basterà posizionarsi sulla VM di interesse e quindi cliccare *"Actions"* e selezionare la VM Console desiderata (**Figura 50).**

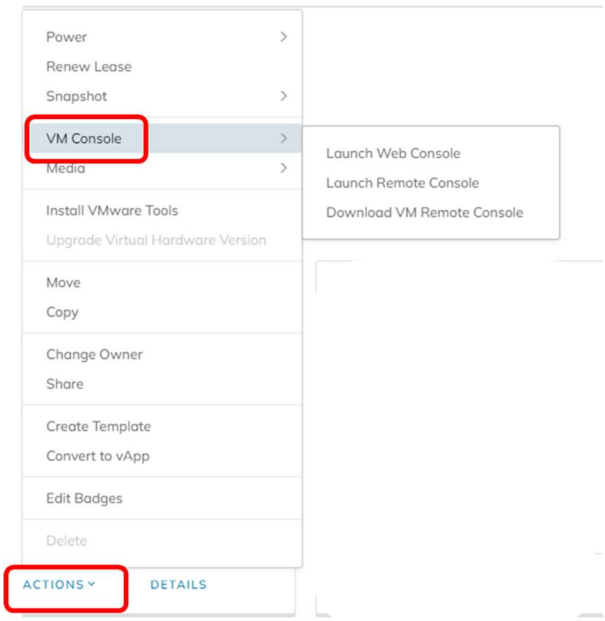


**Figura 51 -** Menu Virtual Machine, riquadro per l'accesso alla console di una VM

Diversamente è possibile impostare accessi diretti alla VM come:

- in RDP su VM Windows da configurare opportunamente sulla *virtual machine*
- nei casi di VM Linux, tramite protocollo SSH da configurare opportunamente sulla *virtual machine*

**Nota**: qualora, per la creazione della VM, fosse stato utilizzato un template presente nel Catalogo Pubblico PSN, per accedere alla macchina a livello di Sistema Operativo va eseguita la procedura di recupero password descritta del paragrafo "*Con quali credenziali accedo al Sistema Operativo?*".

## *7.18 Come è possibile trasferire dei file da una macchina locale ad una VM presente all'interno del Virtual Data Center?*

Per abilitare in maniera semplice il trasferimento di file da una macchina locale ad una VM in PSN Cloud Platform è opportuno configurare una VPN IPSEC Lan to Lan. In questo modo sara' possibile

sfruttare i meccanismi di trasferimento dei file tipici dei sistemi operativi in uso sulle VM.

## 7.19 È possibile aggiungere, rimuovere o associare nuove reti alle NIC di una VM?

Si, per i soli Servizi IaaS Private e Iaas Shared.

Per gestire la configurazione di rete ad una VM già operativa, dovremo accedere al menu *"Details"* della VM stessa, da spostarci nella sezione Hardware, dove comparirà la sottosezione NICs; da qui sarà possibile visualizzare l'attuale configurazione, aggiungere una nuova NIC associando una rete a questa interfaccia a VM accesa, così come modificare l'associazione di NIC già presenti sulla VM stessa. Terminata le modifiche ricordarsi di selezionare Save in fondo alla pagina

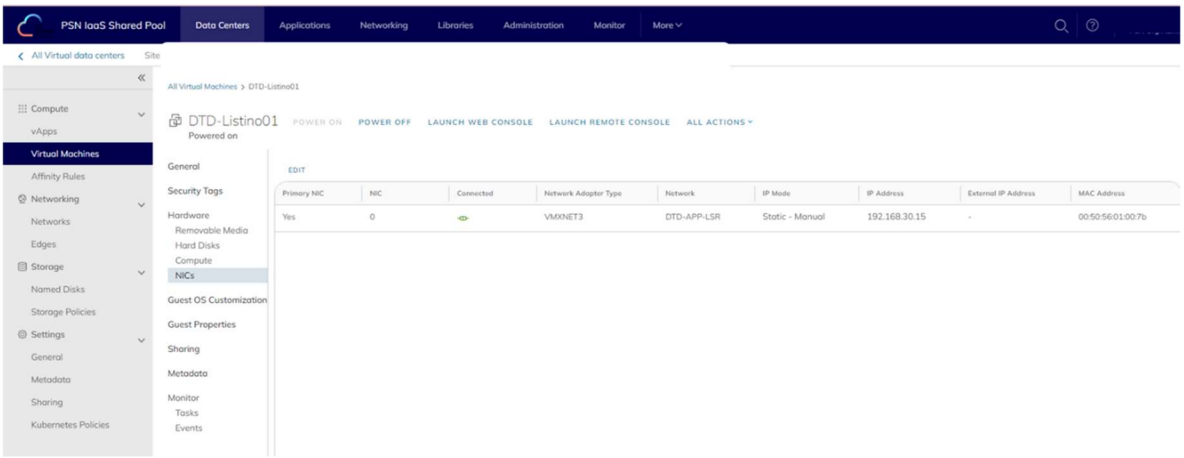


**Figura 52 -** Interfaccia di configurazione NIC della VM


Figura 53 - Interfaccia di configurazione NIC della VM

È anche possibile rimuovere NIC, previo spegnimento della vApp relativa alla VM

**Nota**: per raggiungere il pannello Hardware si veda risposta nel **paragrafo 5.3.**

## 7.20 Le vApp network sono proprie di una sola vApp e non utilizzabili da altre vApp?

La vApp Network è propria di una singola vApp e non può essere condivisa tra più vApp. Se si vuole far comunicare le vApp tra loro occorre agganciarle alla stessa Organization Network

## 7.21 È disponibile un servizio di load balancing tra le vApp?

Il servizio Virtual Data Center prevede delle funzionalità di Load balancing che possono essere gestite direttamente dal modulo Gateway Edge.

## 7.22 Che tipo di indirizzamento occorre indicare nelle regole DHCP, NAT e Firewall delle vApp?

È possibile indicare un IP individuale, un intervallo di IP o un Blocco CIDR. Le regole possono essere applicate selettivamente ad una determinata interfaccia del Gateway.

## 7.23 È utilizzabile il protocollo ICMP (Internet Control Message Protocol)?

Si.

# 8 Utenti e Gruppi

## 8.1 Come posso creare nuovi utenti per l'Organizzazione?

La creazione dell'utenza di Amministrazione dell'Organizzazione viene effettuata e comunicata alla PA da PSN.

## 8.2 Gli utenti dell'Organization possono essere importati da una directory LDAP?

No, la gestione IAM è in carico al gestore del servizio PSN Cloud Platform.

## 8.3 Come possono modificare il nome relativo all'Organization?

Non è possibile modificare il nome dell'Organization, tale compito spetta al gestore del servizio PSN Cloud Platform.

## 8.4 Come posso ricevere notifiche dal mio ambiente VDC?

PSN Cloud Platform richiede un server SMTP per inviare messaggi di notifica utente o avvisi di sistema. Un'organizzazione deve specificare le informazioni di configurazione dei propri servizi SMTP.

Di seguito la procedura per la relativa configurazione:

a Dalla pagina **"Administration"**, selezionare il sottomenu **"Email"**

b Da questa schermata è possibile configurare i parametri di configurazione SMTP per l'invio mail all'interno del VDC (**Figura 53**)

c Scegliere **Notification Settings** ed impostare il destinatario delle notifiche dalla sezione" **Send system notifications to"** e concludere cliccando con "**Save"** (**Figure 54)**

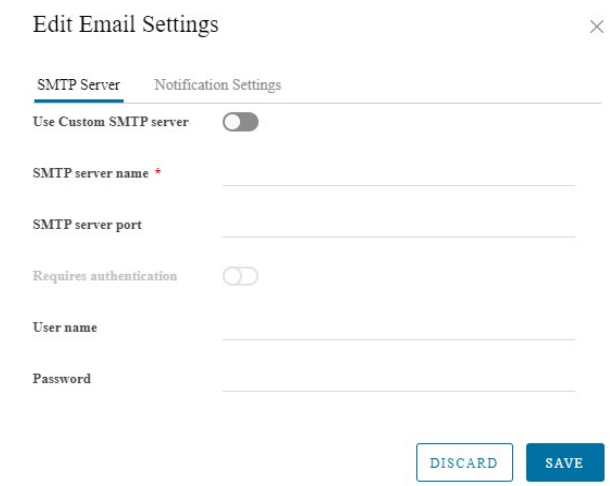


**Figura 54 –** Imput parametri SMTP

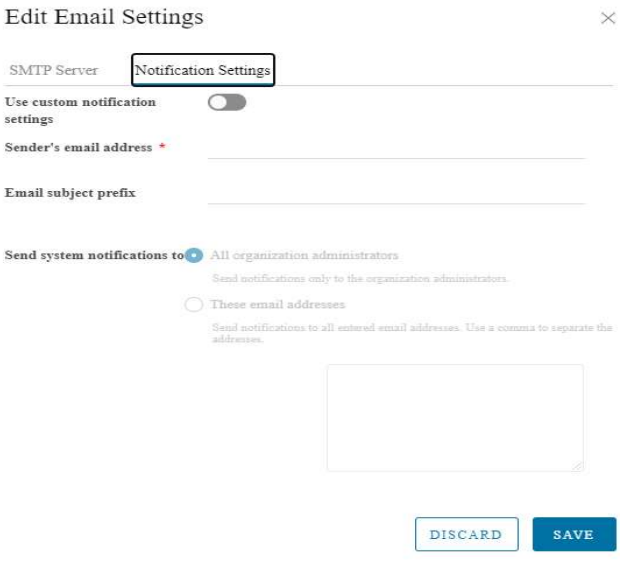


**Figura 55 –** Pannello di controllo destinatari

## 8.5 È prevista la raccolta e conservazione dei file di log?

Il sistema di Logging viene gestito centralmente dal Gestore del Servizio PSN.

# 9 Gestione Backup

Il Servizio BaaS (backup/restore delle VM) garantisce alle PA, attraverso una console centralizzata, totale autonomia per il salvataggio dei propri dati e naturalmente il recupero degli stessi, in caso di perdita dovuta a guasti hardware o malfunzionamenti del software. Il ripristino può avvenire ad una certa data in relazione alle copie di backup effettuate.

Il dettaglio delle istruzioni, per svolgere attività di data protection su PSN utilizzando il servizio BaaS, è descritto nel documento *"PSN_Backup_ManualeUtente".*

## 9.1 Come vengono gestite le funzionalità di Backup offerte in abbinamento al servizio di Virtual Data Center?

La gestione delle funzionalità di Backup viene effettuata mediante l'accesso alla Console Unica, dalla quale è possibile collegarsi al servizio BaaS tramite apposito link.

## 9.2 Come è possibile configurare il servizio di Backup?

Per la configurazione del Servizio di Backup fare riferimento alla sezione *"Configurazione dei client"* del documento *"PSN_Backup_ManualeUtente".*

## 9.3 Come si gestisce il restore delle VM?

Per le Operazioni di restore delle VM fare riferimento alla sezione *"Operazioni di restore"* del documento *"PSN_Backup_ManualeUtente".*

# 10 Installazione Antivirus

Per motivi di sicurezza, è fortemente consigliato installare un Antivirus sulle VM dedicate al servizio IaaS. Nei successi sottoparagrafi è descritta la procedura per l'installazione del BitDefender su macchine con sistema operativo Windows e Linux.

## 10.1 Quali sono i prerequisiti necessari per l'installazione del BitDefender?

I prerequisiti necessari per eseguire l'installazione dell'Agent BitDefender sono i seguenti:

- Disinstallare qualsiasi software *antimalware* o di sicurezza Internet esistente dai sistemi di destinazione
- Assicurarsi di avere i privilegi amministrativi e abilitare l'accesso ad Internet da parte dei sistemi verso gli endpoint BitDefender sulla porta 443/TCP

## 10.2 Come si installa il BitDefender su VM con sistema operativo Windows?

Di seguito sono descritti i principali step per l'installazione del BitDefender su macchine virtuali con sistema operativo Windows:

- Scaricare il pacchetto di installazione dall'endpoint fornito separatamente in riferimento a tecnologia Windows
- Eseguire il pacchetto di installazione sull'endpoint di destinazione e seguire le istruzioni presentate a schermo
- Quando l'Agent è stato installato su tutti i sistemi richiedere la verifica di corretta presa in carico aprendo ticket al COPS PSN e allegando elenco dei sistemi con i relativi indirizzi IP

**NOTA: In caso di anomalie o problemi di esecuzione del setup, aprire un ticket al COPS PSN.**

## 10.3 Come si installa il BitDefender su VM con sistema operativo Linux?

Di seguito sono descritti i principali step per l'installazione del BitDefender su macchine virtuali con sistema operativo Linux:

- Scaricare il pacchetto di installazione dall'endpoint fornito separatamente in riferimento a tecnologia Linux
- Dal sistema, oggetto di attività, ottenere i privilegi di root eseguendo il comando "*sudo su*"
- Modificare le autorizzazioni per il file di installazione in modo da poterlo eseguire mediante il comando *"chmod +x installer"*
- Avviare l'installazione del software BitDefender eseguendo il comando "./installer"
- Al termine dell'installazione, per verificare che l'Agent sia stato installato sul sistema, eseguire questo comando *"systemctl status bdsec*"*
- Quando l'Agent è stato installato su tutti i sistemi richiedere la verifica di corretta presa in carico aprendo ticket al COPS PSN e allegando elenco dei sistemi con i relativi indirizzi IP

**NOTA: In caso di anomalie o problemi di esecuzione del setup, aprire un ticket al COPS PSN.**