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

PSN

Manuale Utente

CaaS Licensed

Data:02/05/2023

PSN_Manuale_Utente_CaaS_Licensed

Ed. 1 - ver. 2.0

QUESTA PAGINA È LASCIATA INTENZIONALMENTE BIANCA

STATO DEL DOCUMENTO

TITOLO DEL DOCUMENTO			
PSN Manuale Utente CaaS Licensed			
EDIZ.	REV.	DATA	AGGIORNAMENTO
1	1.0	12/04/2023	Prima versione del documento del Manuale Utente
1	2.0	02/05/2023	Revisione Documento

NUMERO TOTALE PAGINE:	46

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

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Sviluppo della soluzione
- Funzione Technology Hub
- Funzione Sicurezza
- Referente Servizio
- Direttore Servizio

ESTERNA A:

Direttore dell'Esecuzione Contrattuale (DEC)	PSN ing. Fabrizio Marchese

INDICE

LISTA DELLE FIGURE

LISTA DELLE TABELLE

1 Definizioni e Acronimi

1.1 Definizioni

Definizione	Descrizione
PSN	È la nuova società (New Company) 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

Definizione	Descrizione
Cloud Portal IaaS VMware	Identifica il Portale di accesso alla Piattaforma offerta dal PSN
Console Tecnica IaaS	Identifica il Portale Tecnico di amministrazione del Servizio IaaS
Cloud IaaS VMware	Identifica il Servizio IaaS offerto dal PSN

Tabella 2. Nomenclatura

1.2 Acronimi

Acronimo	Descrizione
ALB	Application Load Balancer
CaaS	Container as a Service
CSE	Cluster e Container Service Extension
CSI	Container Storage Interface
DNAT	Traduzione degli indirizzi di rete Destinazione
FQDN	Fully Qualified Domain Name
HA	Alta Affidabilità
HLD	High Level Design
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
LCM	Gestione del ciclo di vita
PA	Pubblica Amministrazione
PSN	Polo Strategico Nazionale
RBAC	Controllo Degli Accessi Basato Sui Ruoli
SNAT	Traduzione degli indirizzi di rete Sorgente
TKG	Tanzu Kubernetes Grid
NAT	Traduzione degli indirizzi di rete
NSX	Network Security
UI	Interfaccia Utente
vCD	VMware Cloud Director
VDC	Virtual Datacenter
VIP	Virtual IP
VM	Macchina Virtuale

Tabella 3. Glossario Acronimi

2 Panoramica Generale

Il "*Containers as a Service*" è un modello di servizio basato su cloud computing che aiuta a gestire e distribuire applicazioni utilizzando l'astrazione basata su container. Il PSN offre la piattaforma di orchestrazione (Kubernetes) sulla quale i container vengono distribuiti e gestiti.
Tale servizio si rivela utile soprattutto per gli sviluppatori, ai quali consente di realizzare app containerizzate più sicure e scalabili semplificando la gestione infrastrutturale.

"*Container Service Extension*" è un plug-in per PSN Cloud Directory che aiuta gli utenti a realizzare e lavorare con i Cluster Kubernetes. Più in dettaglio, il CSE è un'estensione del Virtual Cloud che offre un server ed un'interfaccia grafica agli utenti per creare cluster *Tanzu Kubernetes Grid* nei propri data center virtuali insieme alle loro macchine virtuali e vApp. I Cluster Kubernetes utilizzano una rete esistente del proprio vCloud, consumano risorse di storage e sono vincolati dai limiti del vCloud del PSN Cloud Platform.

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

Questo capitolo descrive l'architettura del servizio *"Container as a Service"* integrato nella piattaforma Cloud offerta dal PSN.
Il servizio è basato sullo stack tecnologico che eroga i servizi IaaS (Cloud Director, NSX-T, NSX ALB, vSphere), con l'integrazione di ulteriori due tecnologie:

- **Tanzu Kubernetes Grid**
- **Cloud Director Container Service Extension (o CSE)**

Questo stack tecnologico, che definisce il servizio CaaS, è disponibile nei modelli di servizio:

- IaaS Private
- IaaS Shared

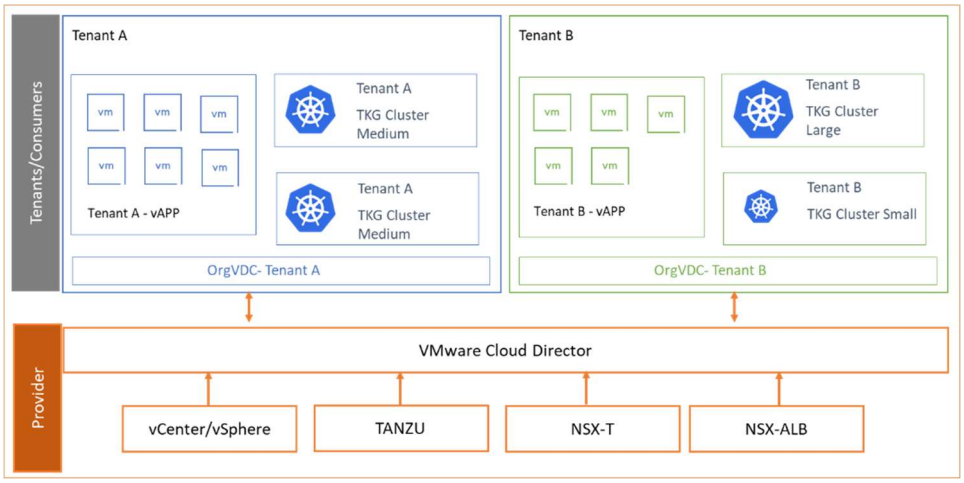

Figura 1-Schema del Servizio CaaS

4 Introduzione al servizio

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

4.1 Qual è lo scopo del servizio offerto nel CaaS?

VMware Tanzu Kubernetes Grid (TKG) è una **pacchettizzazione di soluzioni** open source firmate, testate e **supportate da VMware per ambienti Enterprise**, che facilitano la creazione e la successiva gestione dell'intero ciclo di vita (LCM) dei cluster Kubernetes "upstream" e "*fully conformant*" (come da specifiche CNCF).
Questo conferisce a TKG le caratteristiche di sostenibilità, conformità ed affidabilità che ne fanno una soluzione adatta all'impiego in un contesto Enterprise e critico come quello offerto dal PSN.

TKG supporta tre diverse versioni di Kubernetes, l'ultima e le precedenti due, per consentire ai clienti delle pubbliche amministrazioni (PA) della piattaforma PSN Cloud di scegliere una varietà di opzioni che consentono:

- Possibilità di gestione rapida
- Flessibilità nelle evoluzioni applicative

Tali componenti, costituenti il package TKG sono completamente integrati e predisposti per poter garantire ai clienti della PA un utilizzo immediato senza alcuna interazione diretta e/o attività di basso livello tipica della gestione interna al workload (Container/Applicazioni). Nella figura seguente alcuni dettagli sulle componenti presenti nell'architettura Tanzu VMware adottata dal servizio CaaS.

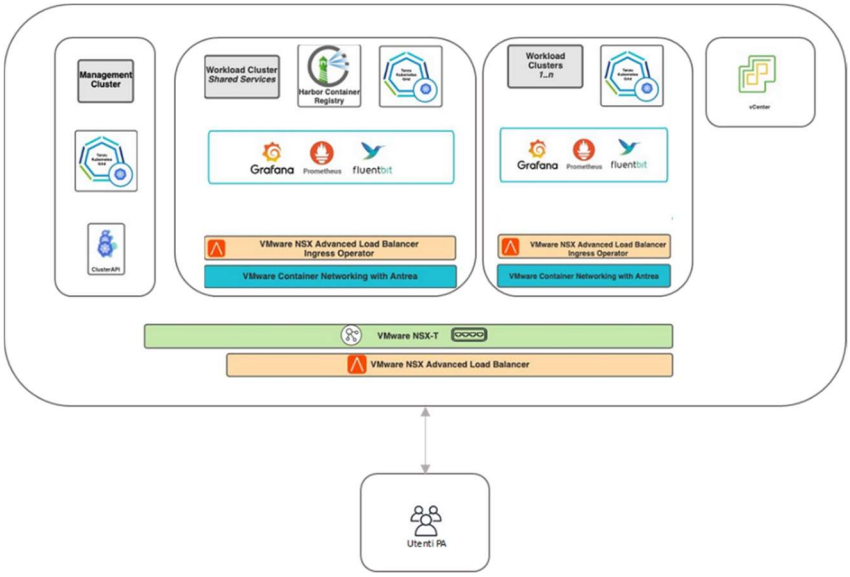

Figura 2-Componenti presenti nell'architettura Tanzu VMware

4.2 Chi può utilizzare il servizio CaaS

Tutte le PA che decidono di sottoscrivere il Servizio CaaS mediante il Piano dei Fabbisogni.

4.3 Come accedo al Servizio?

Il servizio è usufruibile mediante l'accesso alla "Console Tecnica IaaS", dalla quale le PA, che hanno sottoscritto la soluzione CaaS, facendone esplicita richiesta nel piano dei Fabbisogni. Dopo avere effettuato l'accesso alla "Console Tecnica IaaS", per visualizzare la Dashboard del CaaS, cliccare su "*More*" e selezionare "*Kubernetes Container Cluster*":

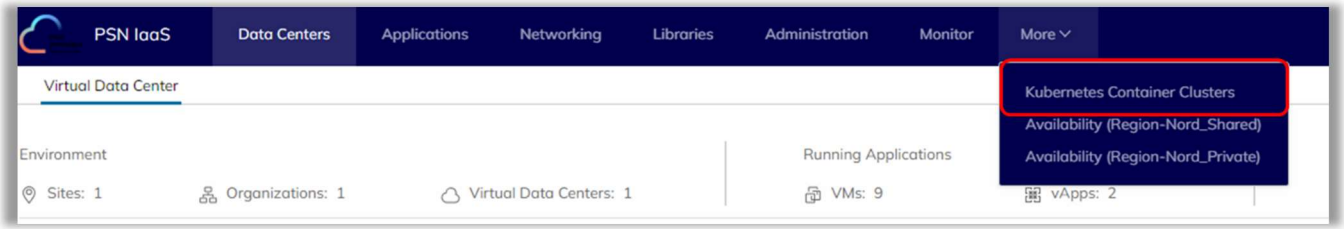

Figura 3- Accesso al Servizio CaaS

NOTA: Ricordiamo che la console tecnica IaaS è disponibile nel portale di accesso "Console Unica", raggiungibile dalla seguente URL:
https://console.polostrategiconazioneale.it

4.4 Quali Ruoli si possono assegnare alle PA che attivano il Servizio CaaS?

All'attivazione del Servizio CaaS all'utenza amministrativa della PA è assegnato il ruolo "*Kubernetes Cluster Author*".

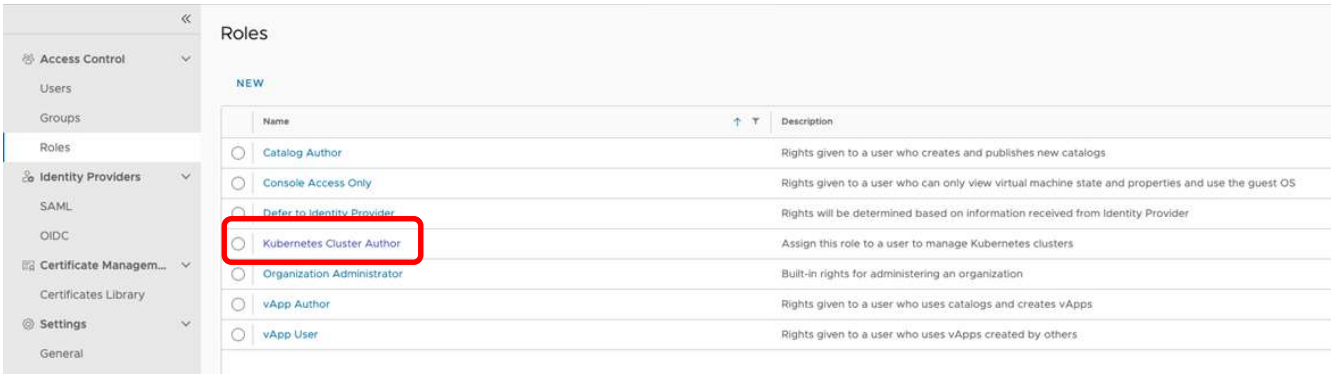

Figura 4- Ruolo Kubernetes Cluster Author

Qualora sia richiesto estendere il ruolo “Kubernetes Cluster Author” ad altre utenze della PA è necessario effettuare specifica richiesta al PSN, mediante esplicita indicazione nel Piano dei Fabbisogni o con successiva richiesta tramite i canali definiti nel documento di Gestione Operativa, che provvederà a generare le utenze richieste mediante i sistemi di gestione Unificate delle Utenze (IAM). La piattaforma CSE utilizza un modello di accesso basato su ruoli (RBAC) che permette la separazione dei ruoli tra gli amministratori IT del PSN e i referenti tecnici della PA. Il modello di accesso garantisce privilegi commisurati alla funzione svolta e consente pertanto di implementare il modello del minimo privilegio necessario.

4.5 Quali versioni sono Disponibili?

Il PSN mette a disposizione delle PA, mediante un Catalogo Pubblico le seguenti Versioni di Kubernetes:

- 1.22.9
- 1.21.11
- 1.20.15

Verranno introdotte nuove versioni, coerentemente con le evoluzioni del prodotto CaaS/Kubernetes.

4.6 Quali profili di VM sono disponibili per i Cluster Kubernetes?

Il catalogo definisce il dimensionamento delle Macchine Virtuali che compongono un Cluster Kubernetes.
Il PSN mette a disposizione della PA i seguenti dimensionamenti:

Sizing	Valori
small	2 CPU, 4 GB di memoria
medium	2 CPU, 8 GB di memoria

Sizing	Valori
large	4 CPU, 16 GB di memoria
extra large	8 CPU, 32 GB di memoria

Tabella 4. Sizing Policy

4.7 Dopo aver creato un Cluster Kubernetes, la PA può modificarlo?

Si, a seguito della creazione di un cluster, la PA, tramite UI, può modificare il numero dei nodi incrementandoli o diminuendoli ma non può effettuare un ridimensionamento verticale. Nel caso in cui una PA abbia la necessità di modificare il dimensionamento di un nodo, può farlo solamente creando un nuovo nodo con un profilo di dimensionamento differente, eliminando il vecchio nodo e facendo ripartire le applicazioni su quello con il nuovo profilo.

4.8 Il CaaS supporta cluster eterogenei?

Si; il CaaS supporta cluster eterogenei, ovvero cluster con profili/dimensioni dei nodi diverse/personalizzate per creare cluster in grado di ospitare Containers Applicativi a uso intensivo di memoria o di calcolo.

4.9 Esistono dei prerequisiti per creare un Cluster Kubernetes?

Si, per creare un Cluster Kubernetes è necessario soddisfare i seguenti prerequisiti **Network**:

- Creazione di un "**Logical Segment**" abilitato alla navigazione Internet, mediante opportune regole di:
  - ***SNAT*** *(*che permetta al cluster l'accesso ad Internet)
  - ***Firewalling*** (che consenta l'utilizzo della porta 6443 sul protocollo TCP)

  al fine di garantire la raggiungibilità degli Endpoint dei *Repository Kubernetes*
- Verificare la presenza di **IP Pubblici disponibili**, nella sezione "*IP Allocation*"; Ogni volta che un cluster viene creato si genera automaticamente anche un Load Balancer che necessita di un IP Pubblico senza il quale la procedura va in errore

4.10 Ci sono elementi specifici da indicare nella creazione di un Cluster?

Si, in fase di creazione di un Cluster vanno indicati i seguenti parametri:

1. Nome Cluster Kubernetes
2. Scelta del Servizio IaaS sul quale Creare il Cluster Kubernetes

3. Versione Kubernetes desiderata (tra quelle messe a disposizione dal PSN)
4. "*Logical Segment"* sul quale attestare il Cluster Kubernetes
5. Dimensionamento dei nodi di gestione del Cluster Kubernetes ("*control-plane")*
6. Dimensionamento dei nodi che ospiteranno i container applicativi ("*worker"*)
7. *Opzionale*: specificare un indirizzo IP da assegnare al VIP del "*control-plane kubernetes*"; omettendo l'indirizzo IP ne verrà scelto uno automaticamente dal sistema
8. *Opzionale*: definire un indirizzamento alternativo di una External Network secondaria che verrà utilizza per esporre le applicazioni del cluster; omettendo l'indirizzo IP ne verrà scelto uno automaticamente dal sistema
9. Storage da utilizzare per la creazione e gestione di volumi persistenti utilizzati dai container(s)

Nel Dettaglio, la procedura di creazione di un Cluster Kubernetes è descritta nel paragrafo 4.11.

4.11 Come creo un Cluster Kubernetes?

Un **Cluster Kubernetes** può essere creato dalla Console Tecnica IaaS nell'apposita sezione, **Kubernetes Container Cluster**, cliccando su *"New/Nuovo*" e seguendo la seguente procedura guidata:

1. Nella sezione "Kubernetes Provider", scegliere il *"Kubernetes runtime"* per il Cluster

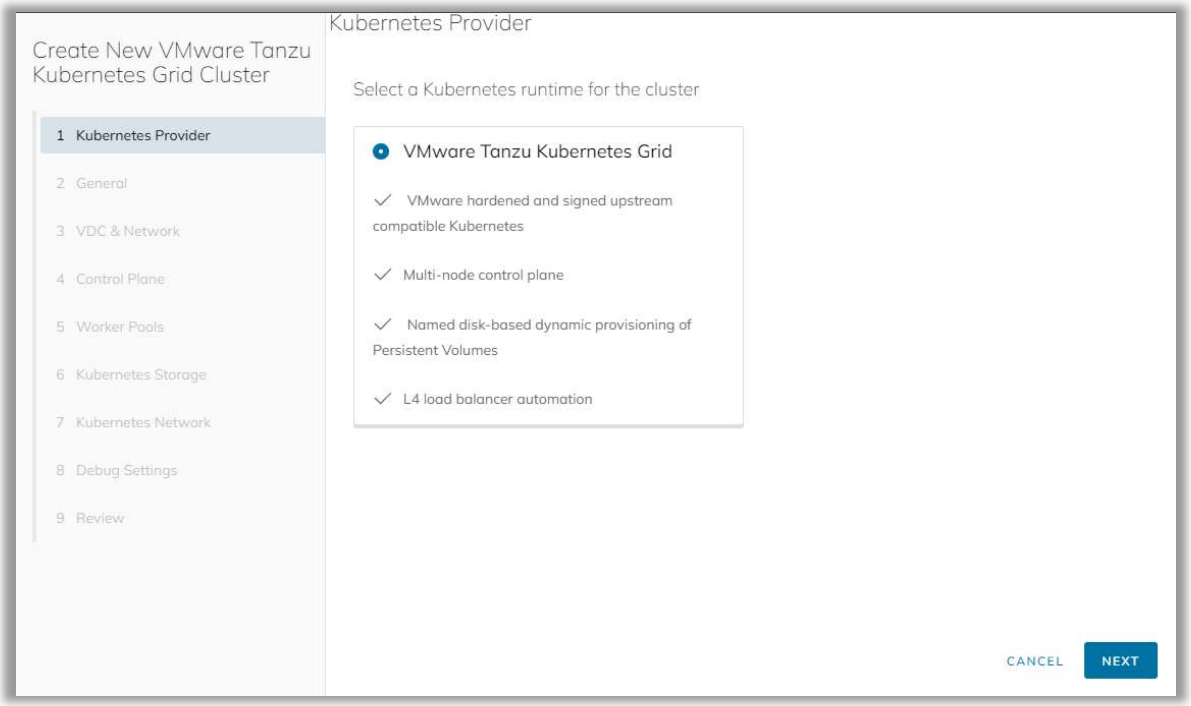

Figura 5-Creazione Cluster, Sezione Kubernetes Provider

2. Nella a sezione "*General*", inserire il Nome del Cluster Kubernetes e selezionare la versione Kubernetes desiderata (tra quelle messe a disposizione dal PSN)

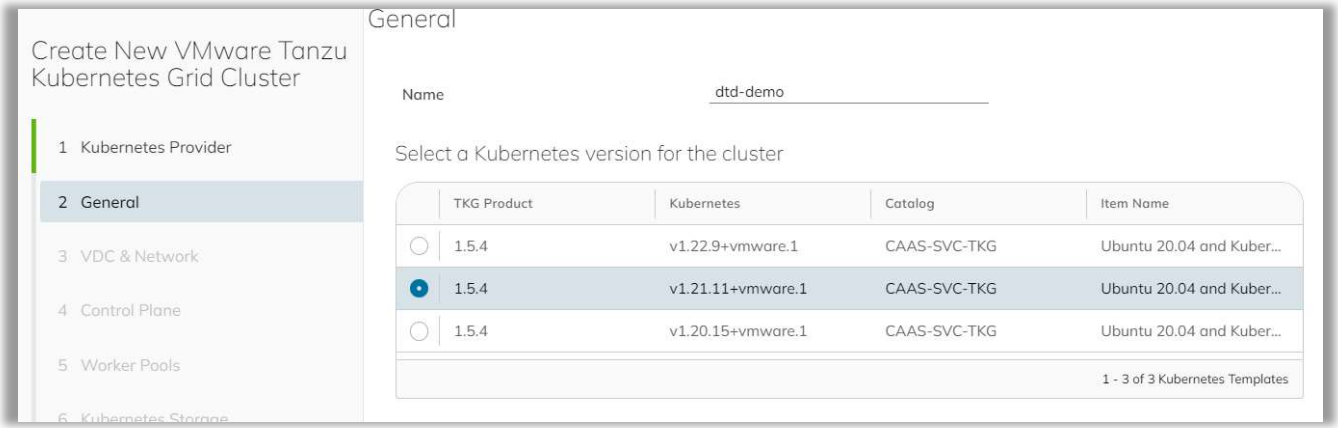

Figura 6- Creazione Cluster, Sezione General

3. In "*VDC & Network*", selezionare la Rete sulla quale attestare il cluster Kubernetes e il VDC

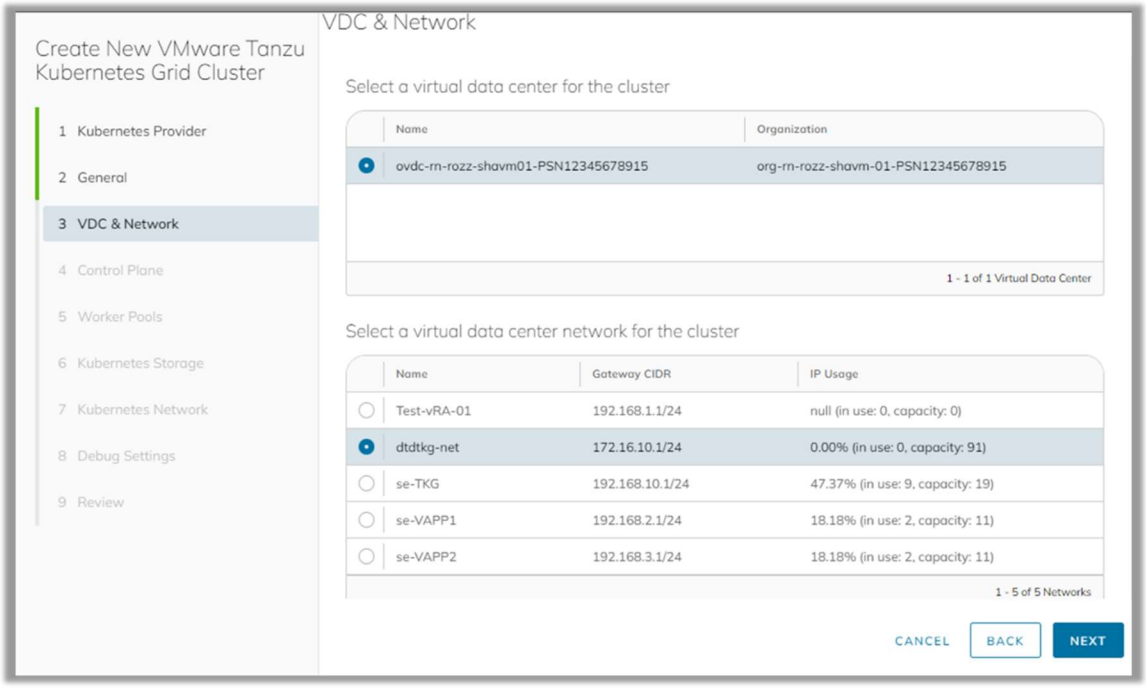

Figura 7-Creazione Cluster, Sezione VDC & Network

4. Nella sezione "*Control Plane*", inserire il numero di nodi, la dimensione del disco, la Sizing Policy e lo Storage Profile

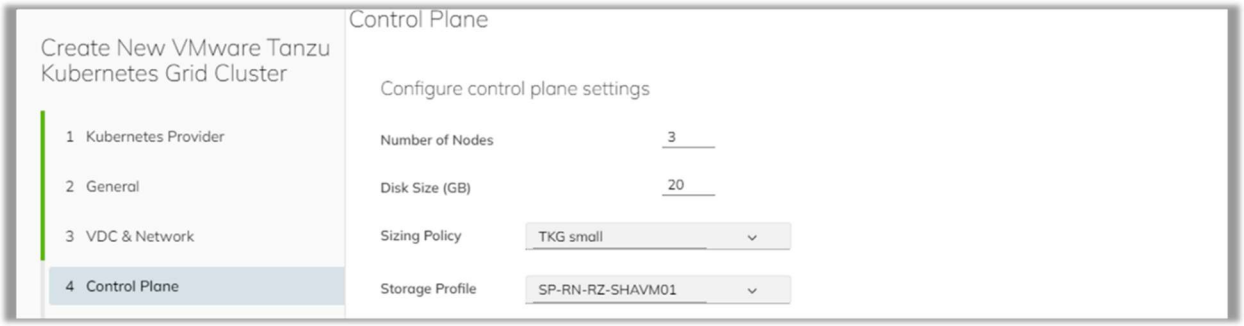

Figura 8-Creazione Cluster, Sezione Control Plane

5. Nella sezione "*Worker Pools*", creare e dimensionare uno o più "*worker node pool";* per creare un secondo *Worker Pool* cliccare su *"Create new worker pool"*, cerchiato in rosso in Figura 9

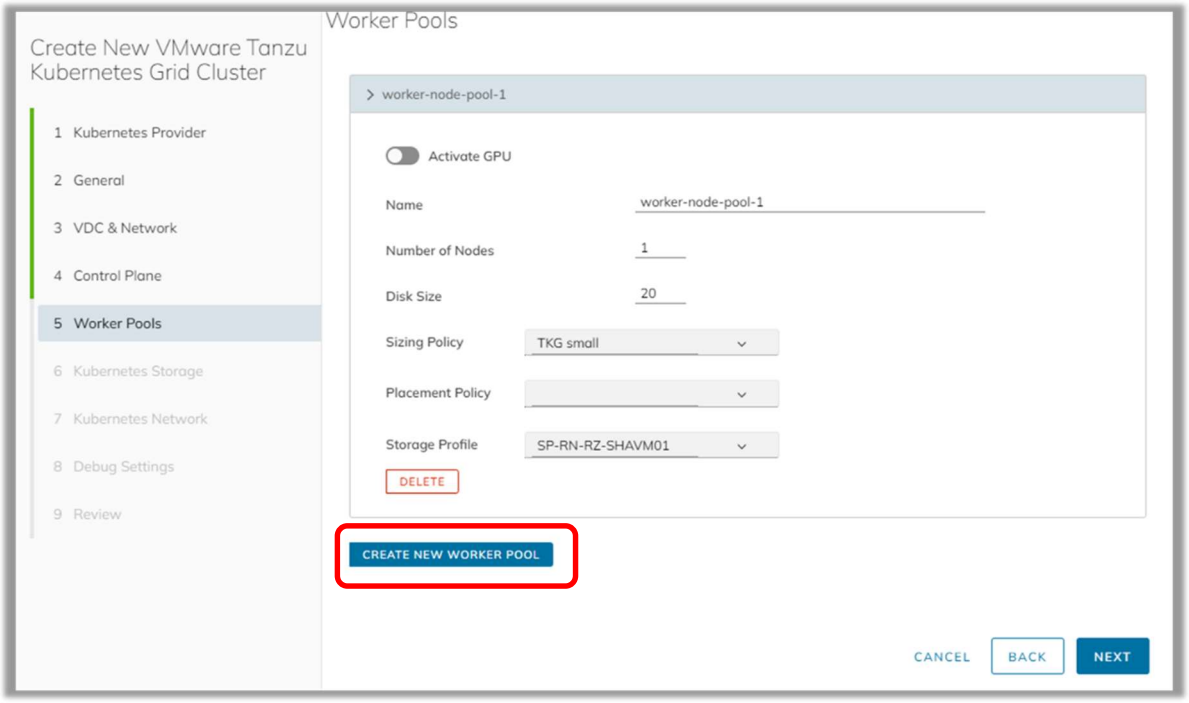

Figura 9- Creazione Cluster, Sezione Worker Pools 1

6. In "*Kubernetes Storage*", selezionare lo "*Storage Profile*" da utilizzare per la creazione e gestione dei volumi sui container

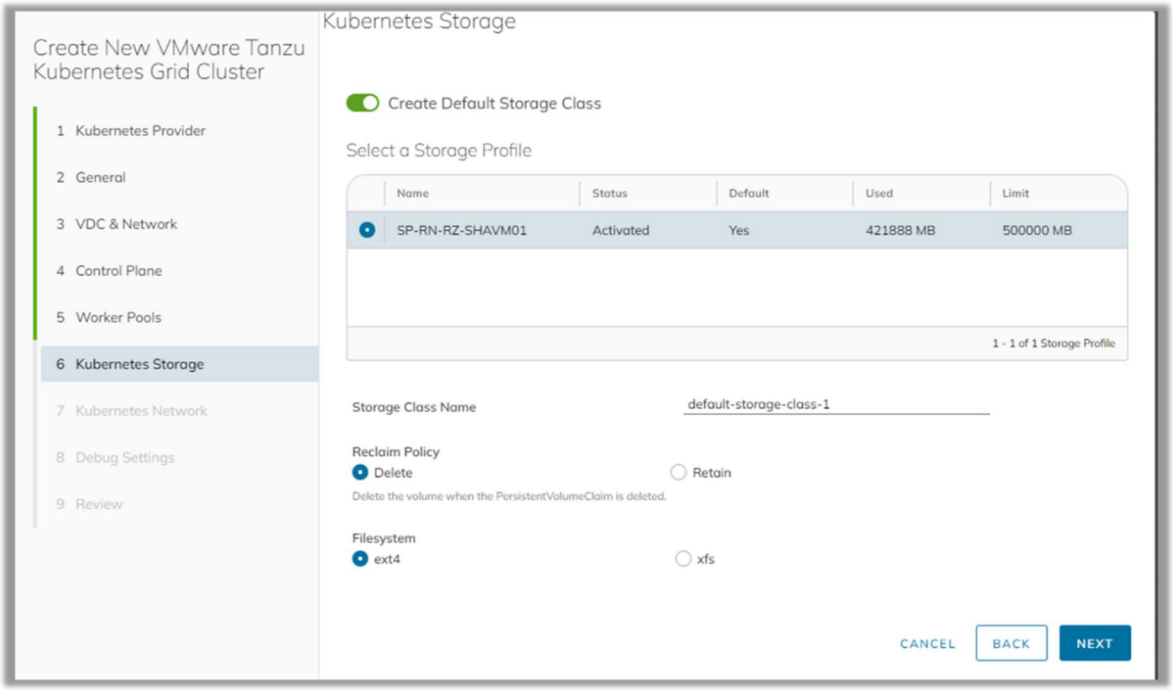

Figura 10- Creazione Cluster, Sezione Kubernetes Storage

7. In "*Kubernetes Network*", inserire la rete del *"Kubernetes **Pods**[1]"* e del *"Kubernetes Services[2]";* è possibile specificare anche un indirizzo IP da assegnare al VIP del *"control-plane kubernetes";* omettendo l'indirizzo IP ne verrà scelto uno automaticamente dal Sistema

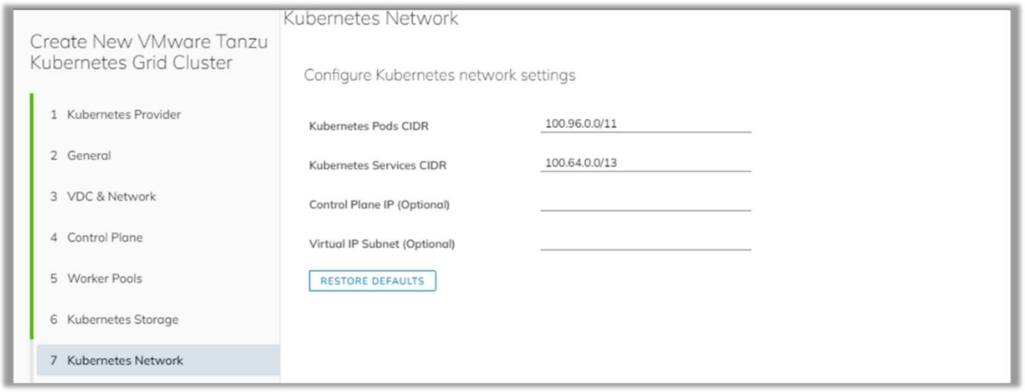

Figura 11- Creazione Cluster, Sezione Kubernetes Network

[1] I ***Pod*** sono le più piccole unità di calcolo distribuibili che si possono creare e gestire in Kubernetes.
[2] Un ***Services*** in Kubernetes è un metodo per esporre un'applicazione di rete in esecuzione come uno o più ***Pod*** nel cluster. Inoltre, i **Pod** e i **Services** non possono essere mai uguali.

8. Nella sezione *"Debug Settings",* è possibile abilitare l'*"Auto Repair"*

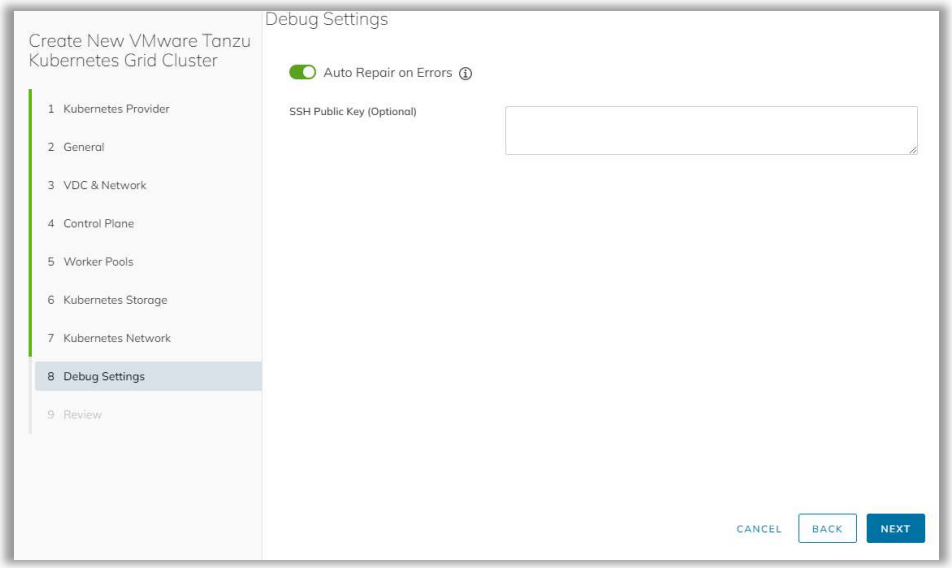

Figura 12- Creazione Cluster, Sezione Debug Settings

9. In "Review", verificare che tutte le informazioni inserite siano corrette

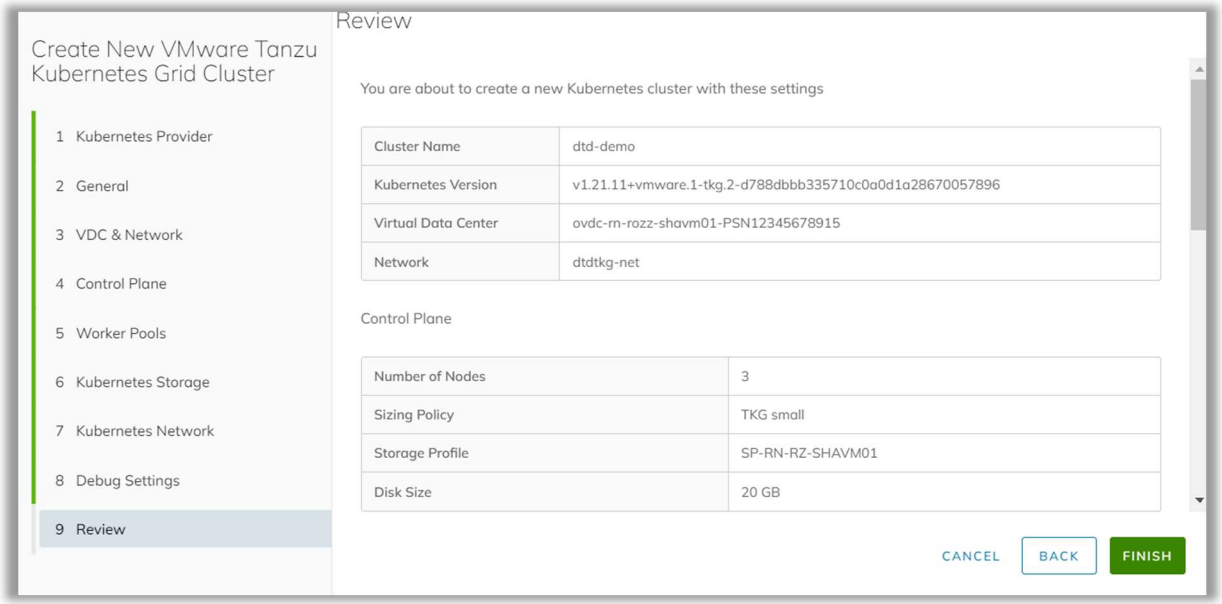

Figura 13- Creazione Cluster, Sezione Review

10. Infine, cliccare su *Finish* e attendere che il cluster passi dallo stato "*pending*" a "*avaible*"

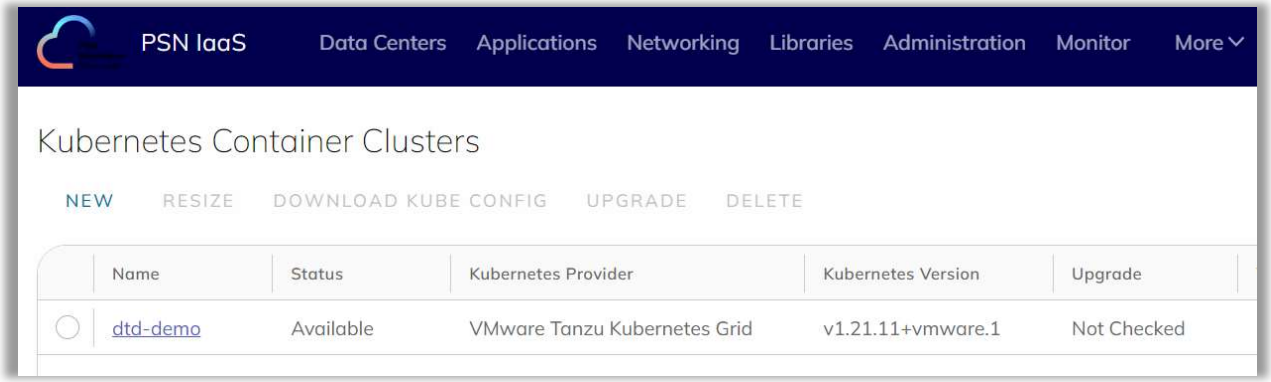

Figura 14- Dashboard Kubernetes Container Clusters

4.12 Quanti Cluster Kubernetes posso istanziare?

Non ci sono limiti, dipende dalla disponibilità di VM e dallo spazio acquisito nel modello di servizio IaaS.

4.13 Esistono dei prerequisiti per accedere e gestire un Cluster Kubernetes?

Si, per poter accedere e gestire un cluster è necessario installare sul proprio client i seguenti software:

- *"Kubernetes CLI"*
- *"Tanzu CLI" & "Tanzu CLI Plugins"*
- *"Cerverl Tools"*
- *"Yq v4.5 o inferiori"*

4.13.1 Come installo "Kubernetes CLI"?

Di seguito viene descritta la procedura di installazione del software "**Kubernetes CLI**"; il file di installazione è disponibile accedendo al link:

- "*https://customerconnect.vmware.com/en/downloads/info/slug/infrastructure_operations_management/vmware_tanzu_kubernetes_grid/2_x*"

Nella sezione "Product Downloads", posizionarsi nella riga *"VMware Tanzu Kubernetes Grid"*, cliccare su *"Go to Downloads"* e scaricare il file di installazione, al momento la versione disponibile è "**kubectl cli v1.24.10 for Windows**".
NOTA: I "*Costumer connect"* sono scaricabili solo via login (effettuare la registrazione se non si ha un account).
Dopo aver scaricato e scompattato la ***CLI di Kubernetes*** sul proprio client, procedere con i seguenti step:

- Creare una nuova cartella "*Program Files\tanzu"*[3]
- Copiare il file "*kubectl-windows-v1.24.10+vmware.1.exe*" nella Folder appena creata
- Rinominare "*kubectl-windows-v1.24.10+vmware.1.exe*" in "*kubectl.exe*"
- Fare clic con il tasto destro del mouse sulla cartella "*kubectl*", selezionare "*Properties> Security*" e assicurarsi che l'account che si sta utilizzando abbia l'autorizzazione di "*Full Control*"

Inoltre, per semplicità si suggerisce di settare il *Path di exe di kubectl* come variabile di ambiente:

- Utilizzare *"Windows Search"* per cercare "*env*"
- Selezionare "*Edit the System Environment Variables*" e cliccare su " *Environment Variables*"
- Selezionare la riga "*Path*" in Variabili di sistema e fare clic su "Edit"
- Fare clic su "*New*"[*C:\Program Files\tanzu*] per aggiungere una nuova riga e inserire il percorso della CLI di kubectl
- Aprire un nuovo terminale in "*command line*" e verificare la versione del client appena installato: *"kubectl version"*

NOTA: Una volta installato "*kubectl*", è necessario creare una cartella nascosta denominata "**kube**" nel seguente Path "*C:\Users\[nome.utente]\.kube*". In questa cartella andrà copiato il file "***kubeconfig***" del cluster al quale si vuole accedere. La procedura per scaricare il file kubeconfig è indicata nel paragrafo "*Come accedo ad un Cluster Kubernetes?*".

4.13.2 Come installo "Tanzu CLI" & "Tanzu CLI Plugins"?

Di seguito viene descritta la procedura di installazione del software "***Tanzu CLI***"; il file di installazione è disponibile accedendo al link:

- *"https://customerconnect.vmware.com/en/downloads/info/slug/infrastructure_operations_management/vmware_tanzu_kubernetes_grid/2_x"*

Nella sezione "*Product Downloads*", posizionarsi nella riga "*VMware Tanzu Kubernetes Grid*", cliccare su "*Go to Downloads*" e scaricare il file di installazione, al momento la versione disponibile è **"VMware Tanzu CLI for Windows"**.
Dopo aver scaricato e scompattato la ***CLI di Tanzu*** sul proprio client, procedere con i seguenti step:

- Creare, se non esiste, una nuova cartella "*Program Files\tanzu"*[4]
- Copiare il file " *core\v0.11.6\tanzu-core-windows_amd64.exe*" nella Folder sopracitata
- Rinominare " *tanzu-core-windows_amd64.exe* " in "*tanzu.exe*"

[3] Verificare di avere i permessi di Amministratore sul Path indicato. Nel non fosse possibile, scegliere un Path dove si possono avere tali permessi.
[4] La creazione della Folder *"Program File\tanzu"* è stata indicata nel paragrafo 4.13.1 e, per semplicità, conterrà tutti gli eseguibili dei Software necessari per l'accesso e la gestione dei Cluster Kubernetes.

- Assicurarsi che nella cartella “tanzu” l’account che si sta utilizzando abbia l'autorizzazione di "*Full Control*"
- Inizializzare la “*Tanzu CLI*” aprendo una nuova CLI sul proprio terminale ed eseguire il comando “*tanzu init*”
- Visualizzare la versione del client con il comando “*tanzu version*”
- Installare le estensioni della “*Tanzu CLI*” tramite il comando “*tanzu plugin sync*”
- Infine, visualizzare la lista dei Plugin eseguendo “*tanzu plugin list*”

A valle dell’installazione della “*Tanzu CLI*” è possibile eseguire il comando ***“tanzu login”*** e collegarsi al Cluster Kubernetes in due diverse modalità:

- *Kubeconfig*
- *Endpoint*

Per semplicità in Tabella 5 viene descritto l’accesso tramite *Kubeconfig*:

Richieste da CLI	Dati da inserire
Select Login type	Selezionare *“Local kubeconfig”*
Enter path to kubeconfig	Inserire il Path dove è presente il kubeconfig del cluster in esame (ad es. “C:\User\[utente]\.kube\kubeconfig-[nomecluster].txt”)
Enter context to use	Inserire il campo *“current-context”* preso dal file *kubeconfig* (nell’esempio in Figura 15 “dtd-demo-admin@dtd-demo”)
Give the server a name	Inserire il campo nome preso dal file *kubeconfig* (nell’esempio in Figura 15 *“dtd-demo”*)

Tabella 5. Accesso al Cluster Kubernetes tramite il file Kubeconfig

In Figura 15, un esempio di accesso in CLI al Cluster Kubernetes con la modalità appena descritta:

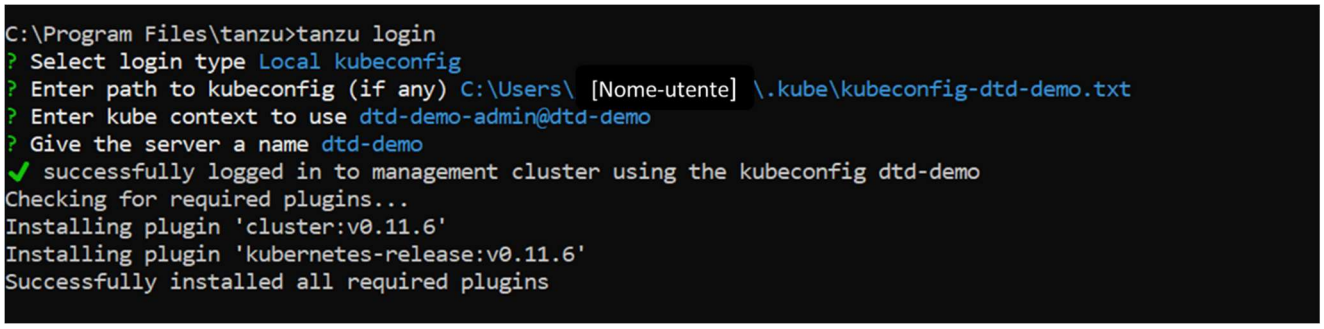

Figura 15- Esempio di Accesso in CLI al Cluster Kubernetes tramite file Kubeconfig

4.13.3 Come installo "Carvel Tools"?

Carvel fornisce un insieme di strumenti affidabili, monouso e componibili che aiutano a creare, configurare e distribuire applicazioni Kubernetes.
Tanzu Kubernetes Grid utilizza i seguenti strumenti del progetto open-source Carvel:

- **ytt** - uno strumento a riga di comando per la creazione di modelli e la modifica di file *Yaml*. È anche possibile utilizzare ytt per raccogliere frammenti e pile di *Yaml* in pezzi modulari per un facile riutilizzo
- **kapp -** la CLI di distribuzione delle applicazioni per Kubernetes. Consente di installare, aggiornare e cancellare più risorse Kubernetes come un'unica applicazione
- **kbld -** strumento per la creazione e la risoluzione di immagini
- **imgpkg** - uno strumento che consente a Kubernetes di memorizzare le configurazioni e le immagini dei contenitori associati come immagini OCI e di trasferire queste immagini

Per installare i *"Carvel Tools",* posizionarsi nella cartella "*tanzu-cli-bundle-windows-amd64\cli"* (estratta nella sezione 4.13.2), copiare e rinominare i file nel percorso "*C:\Program Files\tanzu*" come segue:

File di Origine (Folder cli)	File Rinominato (Folder tanzu)
ytt-windows-amd64-v0.37.0+vmware.1.gz	ytt.exe
kapp-windows-amd64-v0.42.0+vmware.2.gz	kapp.exe
kbld-windows-amd64-v0.31.0+vmware.1.gz	kbld.exe
imgpkg-windows-amd64-v0.22.0+vmware.1.gz	imgkg.exe

Tabella 6. Installazione Carvel Tools

4.13.4 Come installo "Yq"?

Per installare *"Yq v4.5 o inferiori*", collegarsi al seguente link:

- "*https://github.com/mikefarah/yq/releases*"

Posizionarsi nella sezione "*Assets*", cliccare su "*Show all XX assets*" e scaricare il file **"yq_windows_amd64.exe".**
Spostare il file appena scaricato nel Path "*C:\Program Files\tanzu*" e rinominarlo in "*yq.exe*".

4.14 Come accedo ad un Cluster Kubernetes?

Una volta creato un Cluster Kubernetes, è possibile accedere al cluster stesso scaricando il file di accesso, "*kubeconfig",* direttamente dalla Console Tecnica IaaS. Tale file contiene i certificati e gli IP necessari per accedere ed effettuare l'autenticazione al cluster Kubernetes ed eseguire le necessarie attività operative all'interno del cluster. Per scaricare il "*kubeconfig",* posizionarsi sul cluster di interesse e cliccare su *"DOWNLOAD KUBE CONFIG":*

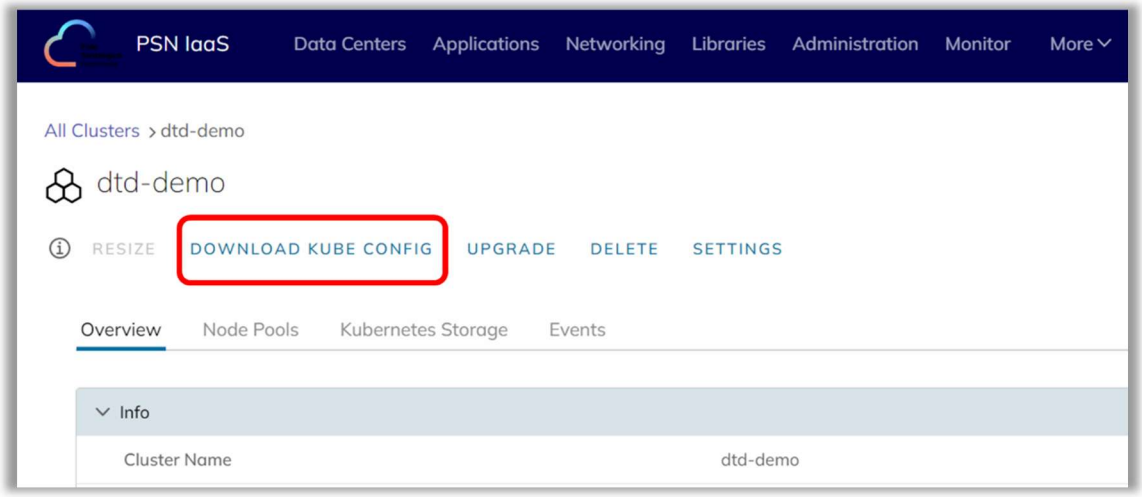

Figura 16- Accesso al Cluster Kubernetes

Copiare il "*kubeconfig*" nella cartella "*.kube*" e aprire una "*command line*" per eseguire l'accesso al cluster.
NOTA: Si consiglia di settare il file "*kubeconfig*" come variabile di ambiente, lanciando il seguente comando da *Powershell*:

[Environment]::SetEnvironmentVariable("KUBECONFIG", $HOME + "\.kube\[nome file kubeconfig]",

[EnvironmentVariableTarget]::Machine)

4.15 Che aspetti network posso gestire?

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 7. 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 17 - 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 16.

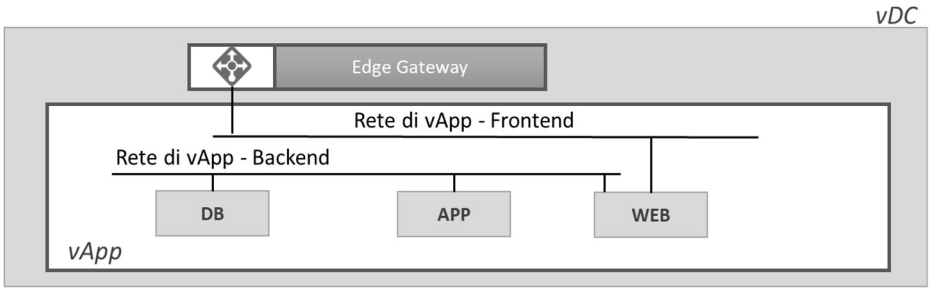

Figura 18 - Diagramma di un possibile scenario di rete per il servizio VDC

Per ulteriori informazioni, si faccia riferimento alla sezione "*Gestione Network*" del documento *"PSN_Manuale_Utente_IaaS_Shared_Private".*

4.16 Ci sono componenti Open Source già installate nei Cluster Kubernetes?

Si, i Cluster Kubernetes, istanziati dal servizio CaaS, sono dotati di componenti open source già installate di default e pronte all'uso, così come riportato nella tabella sottostante:

Pacchetto	Descrizione dei pacchetti
antrea	Abilita il networking dei POD e applica le politiche di rete per i cluster Kubernetes. Questo pacchetto è installato in ogni cluster.
Coredns	Fornisce il servizio DNS, installato in ogni cluster
vcd-cpi	Fornisce l'interfaccia del provider cloud VMware. Questo pacchetto è installato in ogni cluster.
vcd-csi	Fornisce la Cloud Storage Interface (CSI) di VMware Cloud Provider. Questo pacchetto è installato in ogni cluster.
Cert-manager	Fornisce una soluzione integrata per il ciclo di vita completo dei certificati.

Tabella 8.Componenti Kubernetes aggiuntive installate di default

4.17 È possibile installare componenti aggiuntive del Cluster Kubernetes?

Si.

4.18 Quali componenti aggiuntive del Cluster Kubernetes posso installare?

Al completamento dell'installazione del Cluster Kubernetes, è possibile installare ulteriori componenti *open source*, già validate per operare con il Servizio CaaS, per estendere le funzionalità di gestione.
Tali componenti sono disponibili dal sito del *Vendor* e scaricabili direttamente dalla piattaforma Kubernetes, di seguito alcuni esempi:

Nome del pacchetto	Funzione	Dipendenza
Contour	Ingress	Richiesto da Harbour, Grafana
Harbor Registry	Container registry	n / a
Prometheus	Time series DB utilizzato per raccogliere le metriche dalle applicazioni cloud native	Potrebbe richiedere Contour
Grafana	Applicazione che legge le informazioni da Prometheus e permette di creare e visualizzare dashboard.	Richiede Prometheus

Nome del pacchetto	Funzione	Dipendenza
Fluent-bit	Inoltro dei log dei container ad un sistema di logging esterno	n / a

Tabella 9.Componenti Kubernetes opzionali validate per operare con Servizio CaaS

4.19 È possibile integrare il servizio CaaS con soluzioni di Alta affidabilità (HA) e funzionalità di Recovery (DR)?

Si.

4.20 I cluster Kubernetes su due Region differenti possono comunicare tra loro?

Si. I Cluster Kubernetes creati su Region differenti dovranno necessariamente utilizzare connettività Internet per comunicazioni bidirezionali di tipo applicativo/funzionali.

5 Procedure di amministrazione dei Cluster Kubernetes

In questo paragrafo si descrivono le operazioni di Gestione dei Cluster Kubernetes e i dettagli tecnici della soluzione.Tutte le operazioni di creazione e cancellazione del cluster viene vengono gestite in modo trasparente per la PA grazie alle integrazioni tecnologiche previste dalla PSN Cloud Platform.

5.1 Come si effettua un upgrade di un Cluster Kubernetes?

Dalla Console Tecnica IaaS è possibile attivare la procedura di upgrade, con le ultime due versioni rese disponibili dal PSN nel catalogo condiviso. Tale procedura è automatizzata; eventuali *downtime* sono dipendenti dal funzionamento dell'applicazione e non sono conoscibili apriori.[5]

Per effettuare un "Upgrade" di un Cluster Kubernetes, posizionarsi sul Cluster in esame cliccare su "*Upgrade*":

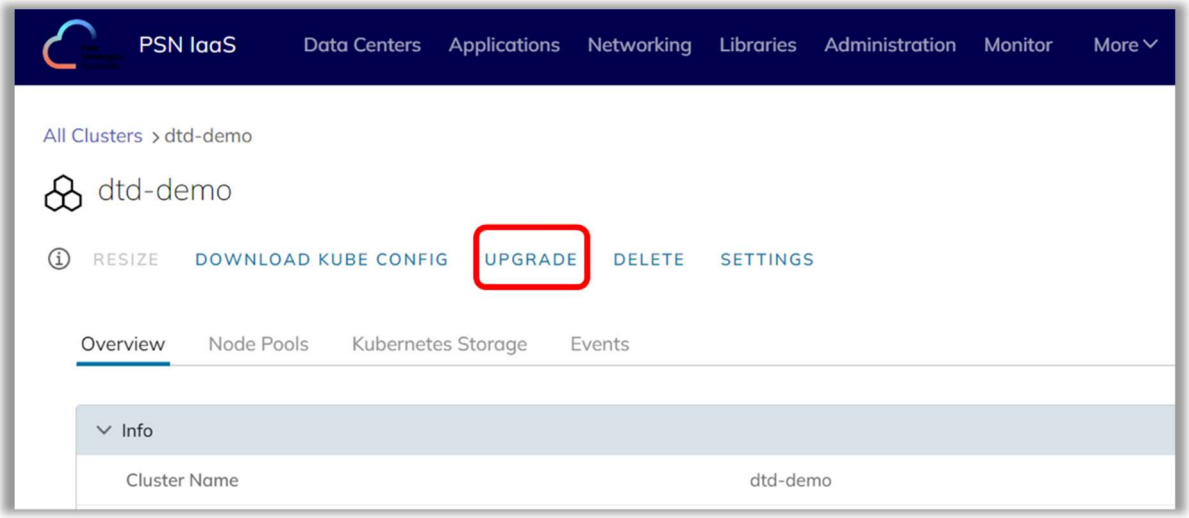

Figura 19-Upgrade del Cluster Kubernetes

Selezionare la versione desiderata, tra quelle messe a disposizione dal PSN e cliccare su "*Upgrade*".

[5] Per il ***Control-Plane***, se è in HA, non ci sono impatti operativi, ogni componente di K8s interagisce costantemente con il Control-Plane.Per i ***worker*** invece, dipende dall'applicazione.

Bisogna tenere a mente che, tendenzialmente, in fase di upgrade viene aggiunto un "*worker node*" nuovo ed effettuato il *drain* del vecchio. A questo punto i **pods** vengono ricreati sul nodo nuovo ed il vecchio viene rimosso.

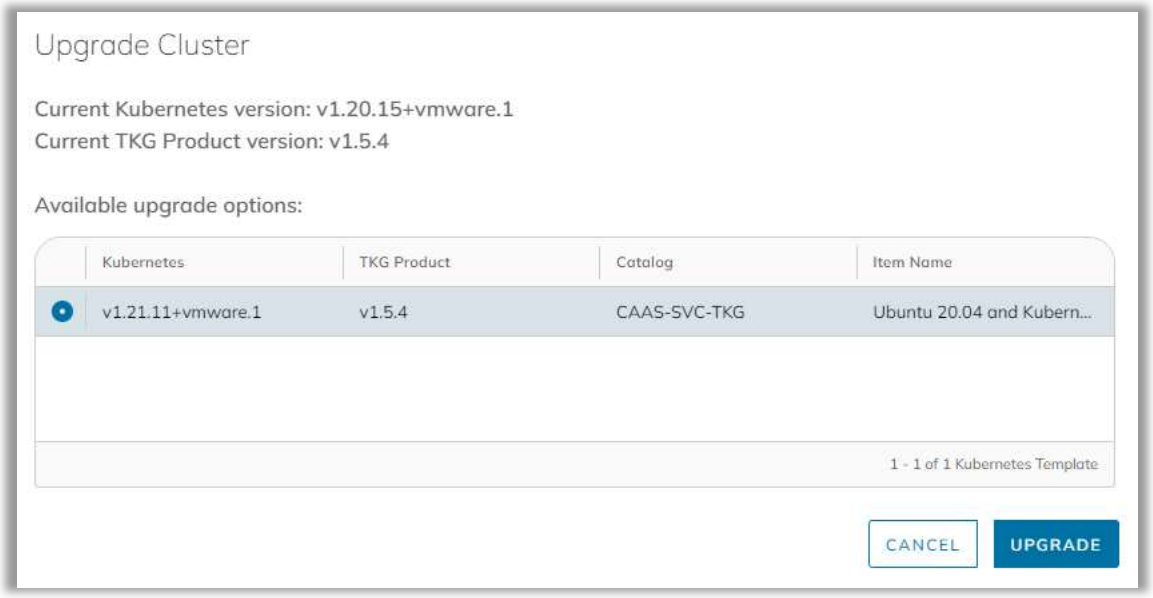

Figura 20-Upgrade del Cluster Kubernetes, selezionare la versione desiderata

Attendere la fine dell'upgrade e verificare che la versione sia quella selezionata in Figura 20.

5.2 Come si effettua un ridimensionamento di un Cluster Kubernetes?

In base alle necessità, è possibile effettuare un ridimensionamento di un Cluster Kubernetes (aggiungere o rimuovere nodi); tale processo è gestito dal cluster senza causare disservizi alle applicazioni già in esecuzione sul cluster stesso. Per aggiungere un "*Worker Node Pools*" al Cluster Kubernetes in esame, posizionarsi nella sezione "*Node Pools*" del cluster e cliccare su *"Create New Worker Node Pools"*, vedi in rosso nella Figura seguente*:*

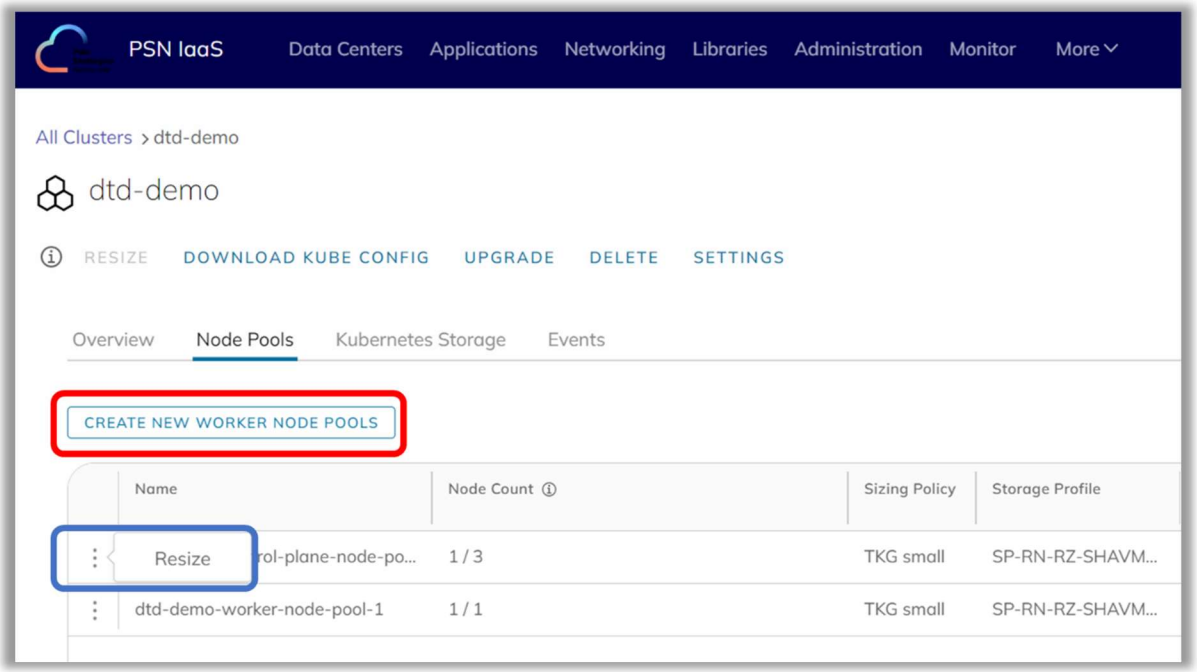

Figura 21- Creazione Nuovi Worker Node Pools

Compilare i seguenti campi, come si può osservare in Figura 22, e cliccare si "*Create*":

- Nome
- Numero di Nodi
- Dimensioni Disco
- Sizing Policy
- Placement Policy
- Storage Profile

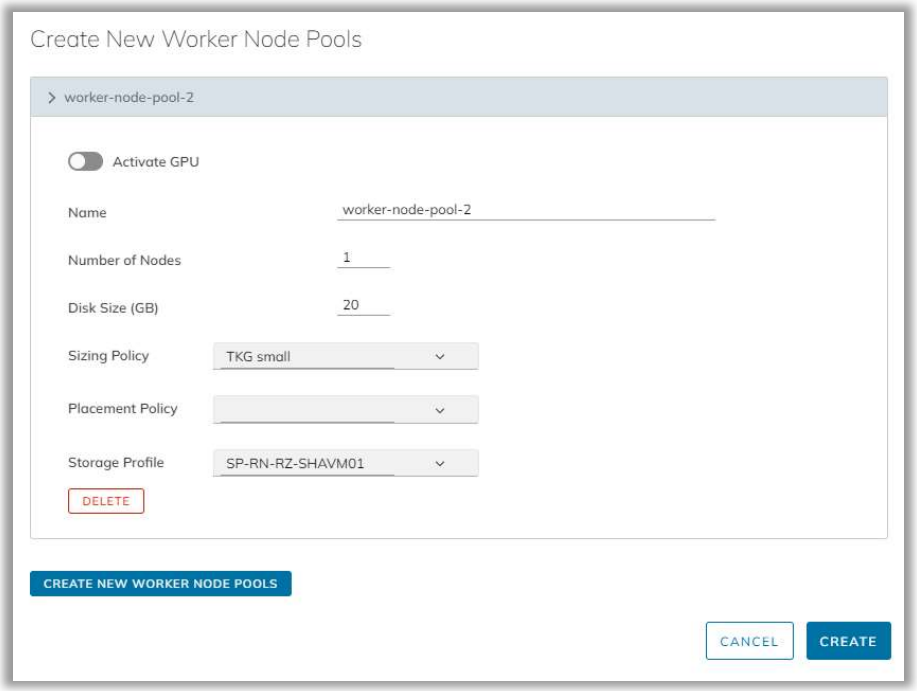

Figura 22- Dettaglio creazione di un nuovo Worker node Pools

Per editare *un "Worker Node Pools",* cliccare sui tre puntini e poi il tasto "*Resize*"; vedi selezione in Blu in Figura 21. A questo punto, come si può osservare in Figura 23, è possibile modificare il numero di nodi:

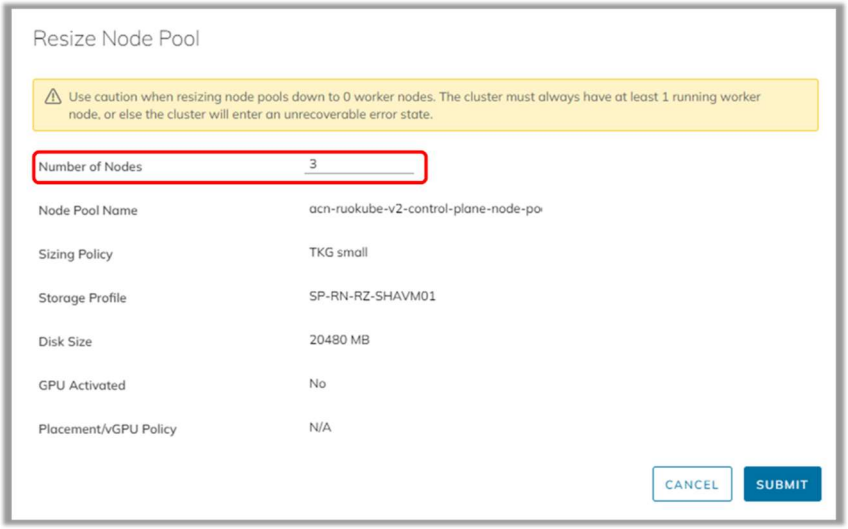

Figura 23- Ridimensionamento Nodi

NOTA: la riduzione ad un numero pari a 0 dei Worker Node compromette in modo irreversibile la funzionalità del Cluster Kubernetes e sarà necessario procedere alla sua cancellazione.

5.3 Come si effettua l'eliminazione di un Cluster Kubernetes?

La cancellazione di un Cluster è un'operazione definitiva e non c'è possibilità di effettuare un *rollback* dell'azione. Per cancellare un Cluster Kubernetes posizionarsi sul cluster in esame e cliccare su *"Delete\Elimina",* cerchiato in rosso in Figura, e confermare:

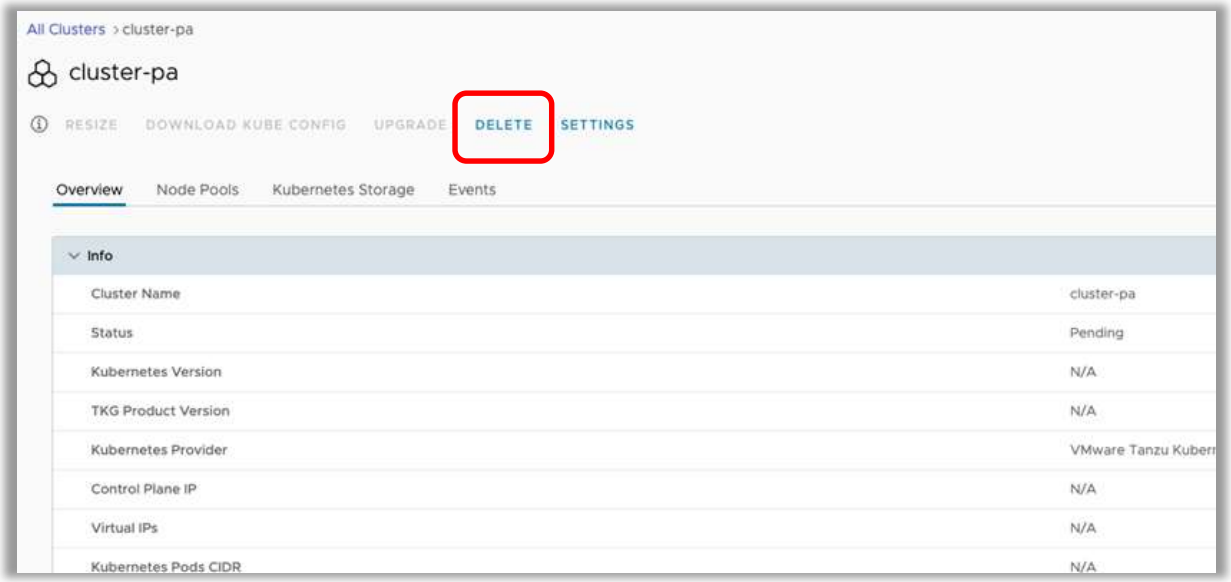

Figura 24- Eliminazione di un Cluster Kubernetes

Una richiesta di cancellazione di Cluster Kubernetes prevede la completa eliminazione del cluster e i relativi dati.

6 Come pubblico i servizi applicativi?

La pubblicazione dei servizi applicativi può avvenire in due modalità:

- **Base:** consiste nel creare un servizio di tipo ***Load Balancer*** per i pod dell'applicazione e far sì che la "Console Tecnica IaaS" fornisca l'infrastruttura necessaria per rendere raggiungibile l'applicazione; Questa modalità è totalmente automatizzata e supportata dalla PSN Cloud Platform. In questo scenario una PA può istanziare un massimo di 98 servizi applicativi in un OrgVDC
- **Avanzata:** prevede l'installazione e la configurazione di un "***Ingress Controller"***, ovvero un proxy che intercetta le richieste verso il cluster e mappa ogni servizio in base alla URL o il nome del dominio nella richiesta; in questo caso una PA non ha il limite sui servizi applicativi ma può creare un massimo di 98 cluster in un OrgVDC

6.1.1 Quale approccio utilizzare per la gestione dei Public IP?

Non ci sono vincoli di forma, ogni PA è libera di gestire come meglio crede la propria Infrastruttura Kubernetes. Dal punto di vista tecnico, suggeriamo di approcciare il seguente metodo:

- Pubblicazione metodo **Base** per tutti i moduli di gestione *Plugin* (*Access Layer, Registry, Observability*)

Ambito	Package
Access Layer	Ingress Controller (Contour)
Registry	Harbor
Observability	Log Forwarding
	Prometheus
	Grafana
	Dashboard

Tabella 10. Plugin dei moduli di Gestione di un Cluster Kubernetes

- Pubblicazione metodo **Avanzato** per tutte le applicazioni a disposizione dell'utilizzatore

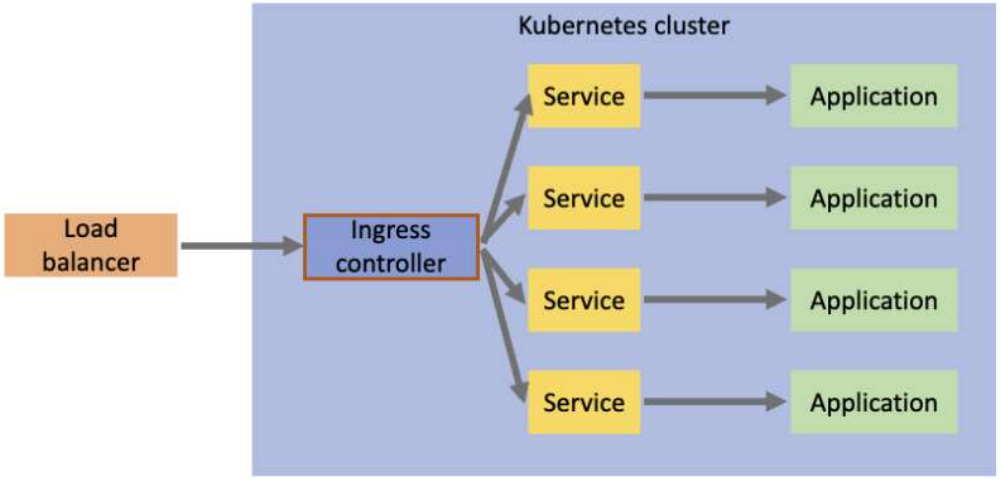

Figura 25- Pubblicazione dei servizi in modalità Avanzata con Ingress Controller

Con questa modalità di gestione, ogni singolo cluster necessita di 6 *Public IP* per la pubblicazione dei servizi di gestione.

6.2 Pubblicazione dei servizi in modalità Base

In questa sezione viene descritta la procedura di pubblicazione dei servizi Base; In Figura 26 si può osservare come in questa modalità ogni servizio applicativo rilasciato utilizza un nuovo IP di tipo Public, pertanto l'integrazione con le componenti ALB prevede un rapporto *Servizio:IP* di tipo *1:1*.

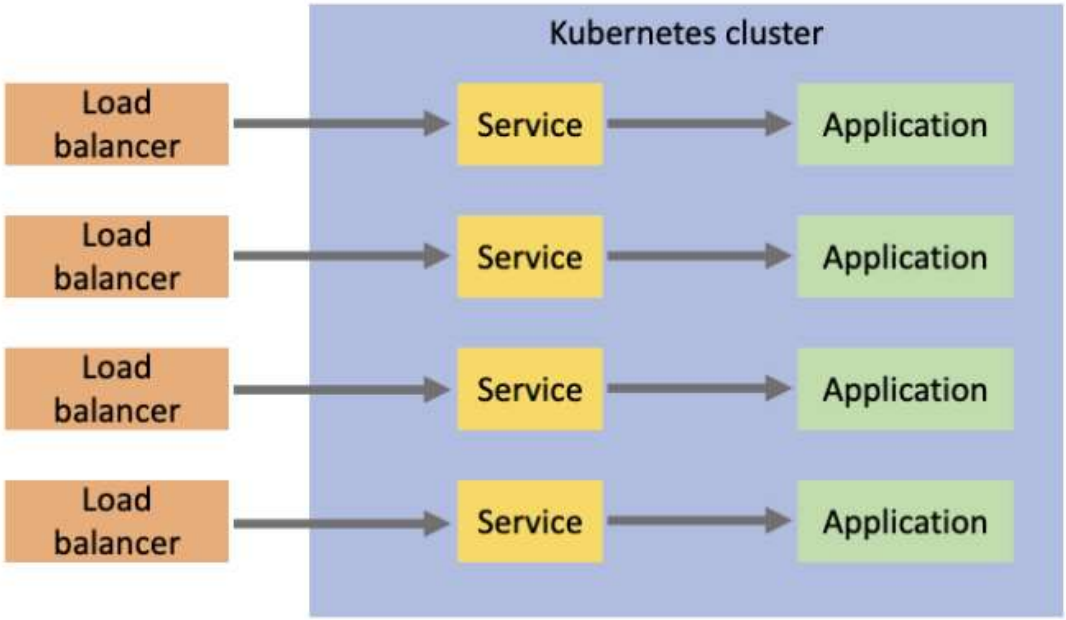

Figura 26- Pubblicazione dei servizi modalità Base

A valle del Deploy di un'applicazione, la piattaforma crea automaticamente una serie di oggetti:

- Regole di bilanciamento
- Associazione Public IP
- Regola di DNAT

Tuttavia, l'applicazione sarà raggiungibile solo dopo aver soddisfatto i seguenti requisiti funzionali:

- Creazione di oggetti di tipo *Security*, Gruppi di **IP SET**:
  - **SUB-SVCK8**: Network di SNIP (192.168.8.0/24)
  - **SUB-Public**: Spazio di indirizzamento associato (vedere in sezione "*IP Allocation*")
  - **SUB-InternetOUT**: Contiene le network che voglio abilitate alla navigazione internet per regola di SNAT
- Creazione di Regole di navigazione Internet: **Regola di SNAT**
- Verifica degli **IP disponibili** per ogni pubblicazione di Applicazione
- Creazione delle opportune **Regole Firewall**:
  - **Esposizione Applicazione**, come riportato in Tabella 11
  -

Nome Regola Firewall	Sorgente	Applicazione	Stato	Destinazione	Azione
from-internet-to-K8Ssvc	Any	«HTTP-Custom Port»	Enabled	SUB-SVCK8 (192.168.8.0/24)	Allow

Tabella 11. Regola Firewall esposizione Applicazione

Ad esempio, nel caso in cui si vuole pubblicare un'applicazione sulle porte 8080 e 80, va utilizzata la regola firewall di esposizione, precedentemente creata, aggiungendo protocolli dei nuovi servizi pubblicati:

Nome Regola Firewall	Sorgente	Applicazione	Stato	Destinazione	Azione
from-internet-to-K8Ssvc	Any	http (80), http (8080)	Enabled	SUB-SVCK8 (192.168.8.0/24)	Allow

Tabella 12. Regola Firewall, esempio esposizione applicazione

Nella soluzione del Cluster Kubernetes è necessario avere a disposizione un *Public IP* per ogni applicazione pubblicata. Di seguito un diagramma esemplificativo di HLD per comprendere come avviene la pubblicazione di due applicazioni:

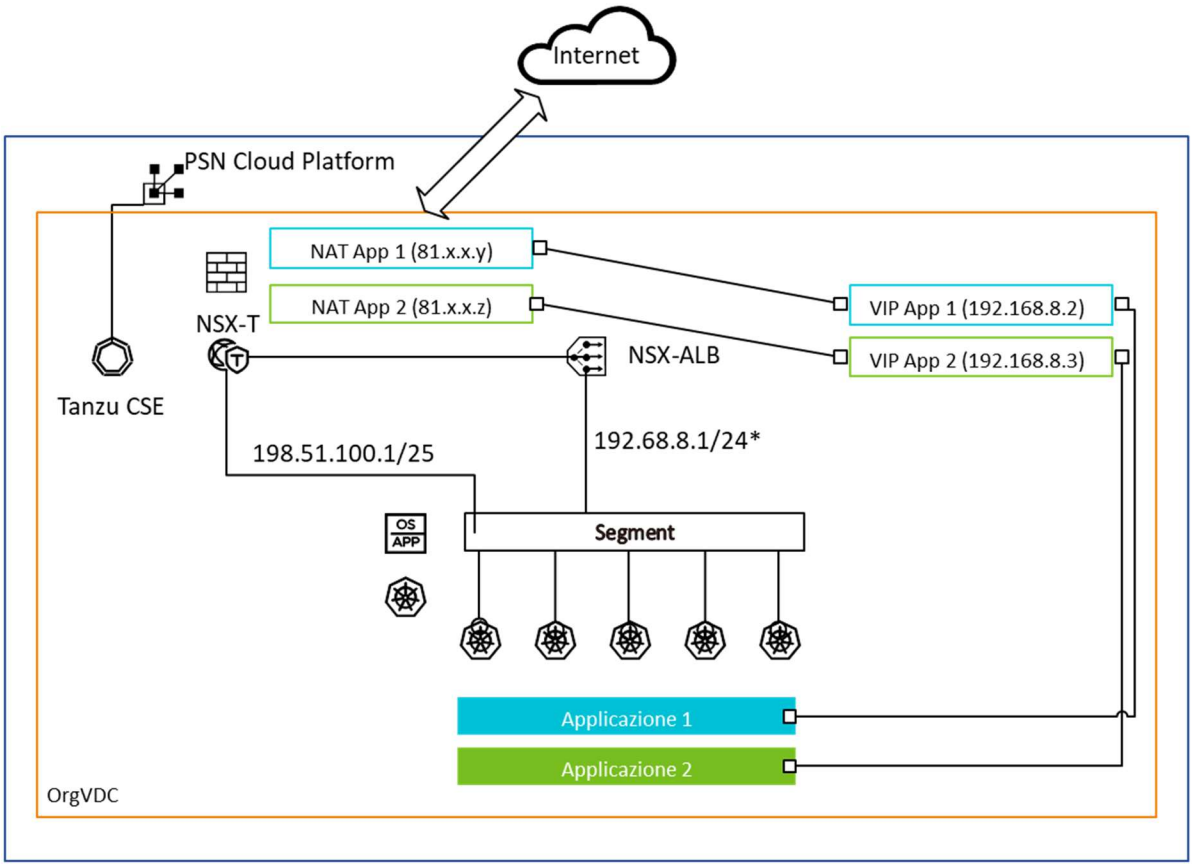

Figura 27- HLD esposizione dei Servizi

Si noti come la soluzione preveda una **network di servizio** (198.51.100.1/25) per le attività di configurazione e una **network di VIP**, utilizzata per realizzare i VIP dei servizi applicativi successivamente associati all'opportuna regola NAT generata automaticamente (DNAT). Dalla Figura 24, possiamo dedurre che per l'applicazione 1 il VIP è 192.168.8.2 è l'Internal IP della DNAT sopracitata mentre per l'applicazione 2 è il 192.168.8.3.

6.2.1 Installazione altri package

In Tabella 13 sono riportati i link alla documentazione VmWare, contenenti le procedure di installazione di alcuni package consigliati per la gestione e il monitoraggio dei Cluster Kubernetes:

Package	Link alla documentazione
Log Forwarding	https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-packages-logging-fluentbit.html
Prometheus	https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-packages-prometheus.html
Grafana	https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-packages-grafana.html
Harbor	https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-packages-harbor-registry.html

Tabella 13. Installazione package, Link alla documentazione

6.2.2 Deploy Dashboard Kubernetes

In questo paragrafo viene spiegato come effettuare il *Deploy* della ***"Dashboard Kubernetes"*** su un Cluster Kubernetes.
La Dashboard è una UI web di Kubernetes ed è possibile utilizzarla per:

- Distribuire applicazioni containerizzate in un Cluster Kubernetes
- Risolvere i problemi delle applicazioni containerizzate
- Gestire le risorse del Cluster
- Ottenere una panoramica delle applicazioni in esecuzione sul cluster
- Creare o modificare singole risorse Kubernetes

La Dashboard fornisce anche informazioni sullo stato delle risorse Kubernetes nel cluster e su eventuali errori:

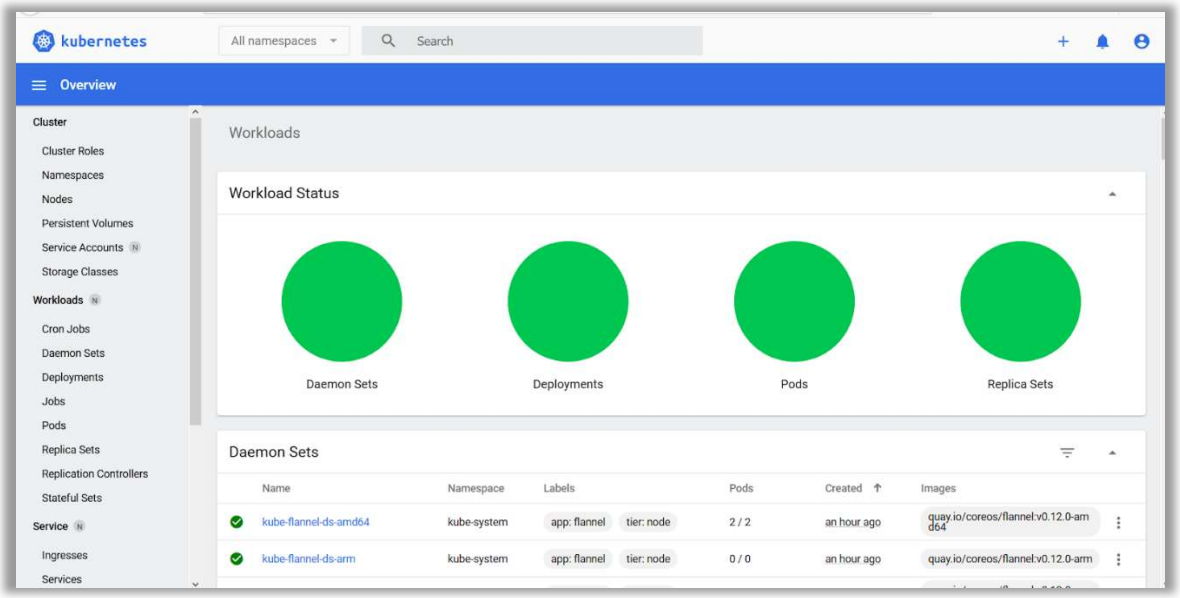

Figura 28- Dashboard Kubernetes

In Tabella 14 sono descritti gli step di installazione della Dashboard Kubernetes tramite Load Balancer:

Step	Spiegazione	Comandi CLI
1	Deploy del file yaml (verificare se la versione indicata è l'ultima scaricabile)	*kubectl apply -f https://raw.githubusercontent.com/kubernetes/dashboard/v2.7.0/aio/deploy/recommended.yaml*
2	Ottenere l'accesso completo al cluster per l'account *kubernetes-dashboard*	*kubectl create clusterrolebinding add-on-cluster-admin --clusterrole=cluster-admin --serviceaccount=kubernetes-dashboard:kubernetes-dashboard*
3	Esporre la Dashboard utilizzando la modalità Base	*kubectl expose deployment -n kubernetes-dashboard kubernetes-dashboard --type=LoadBalancer --name=kubernetes-dashboard-public*
4	Visualizzare i dettagli del servizio	kubectl get -n kubernetes-dashboard svc kubernetes-dashboard-public
5	Collegarsi alla URL della Dashboard	http:// VirtualIP:Port
6	Ottenere il Token da copiare e incollare nel browser per effettuare il login e accedere alla Dashboard	*kubectl describe -n kubernetes-dashboard secret kubernetes-dashboard-token*

Tabella 14. Deploy Dashboard Kubernetes

6.2.3 Prerequisiti Contour

I prerequisiti di installazione di *Contour* sono:

- Installazione dei prerequisiti client per gestione Cluster Kubernetes (vedi sezione 4.13)
- Login al cluster (vedi paragrafo 4.13.2) e installazione "*Cert-manager"*

Dopo aver effettuato il login al cluster, è possibile installare "*Cert-manager"* eseguendo da CLI i comandi:

- *"tanzu package available list -A"* per visualizzare i package disponibili nel cluster
- *"tanzu package available list cert-manager.tanzu.vmware.com -A"* per visualizzare le versioni del package disponibili
- *"tanzu package install cert-manager --package-name cert-manager.tanzu.vmware.com --namespace TARGET-NAMESPACE --version AVAILABLE-PACKAGE-VERSION --create-namespace"* per installare il Package
- "*tanzu package installed list -A"* per verificare che il package è stato installato

Se la procedura è andata a buon fine il package "*cert- manager*" è in stato "*Reconcile succeeded*" (vedi Figura 29).

6.2.4 Deploy Contour

Di seguito la procedura per installare Contour. Il primo step consiste nel creare un file **"contour-data-values.yaml"** del tipo:

```
infrastructure_provider: vsphere
namespace: tanzu-system-ingress
contour:
 configFileContents: {}
 useProxyProtocol: false
 replicas: 2
 pspNames: "vmware-system-restricted"
 logLevel: info
envoy:
 service:
  type: LoadBalancer
  annotations: {}
  nodePorts:
    http: null
    https: null
  externalTrafficPolicy: Cluster
  disableWait: false
 hostPorts:
  enable: true
  http: 80
  https: 443
 hostNetwork: false
 terminationGracePeriodSeconds: 300
 logLevel: info
 pspNames: null
certificates:
 duration: 8760h
 renewBefore: 360h
```

Dopo aver creato il file *Yaml*, eseguire il comando di installazione del package:

- *"tanzu package install contour –package-name contour.tanzu.vmware.com –version 1.18.2+vmware.1-tkg.1 –namespace tanzu-cli-managed-packages –values-file contour-data-values.yaml"*

Per verificare che il package sia installato e in stato "*Reconcile succeeded*" (vedere Figura 29) eseguire il comando:

- *"tanzu package installed list -A"*

```
tanzu package installed list -A
- Retrieving installed packages...
  NAME            PACKAGE-NAME                    PACKAGE-VERSION                STATUS               NAMESPACE
  cert-manager    cert-manager.tanzu.vmware.com   1.1.0+vmware.1-tkg.2           Reconcile succeeded  my-packages
  contour         contour.tanzu.vmware.com        1.17.1+vmware.1-tkg.1          Reconcile succeeded  my-packages
  antrea          antrea.tanzu.vmware.com                                        Reconcile succeeded  tkg-system
  [...]
```

Figura 29- Check sullo stato dei package installati

6.3 Pubblicazione dei servizi in modalità Avanzata

Nella modalità Avanzata è prevista l'installazione e la configurazione di un "***Ingress Controller"***, che semplifica il traffico in ingresso al cluster Kubernetes e fornisce funzionalità e vantaggi per scenari di rete più sofisticati. Una volta aggiunto un "*Ingress Controller"* al cluster, il flusso di traffico è quello mostrato in Figura 30:

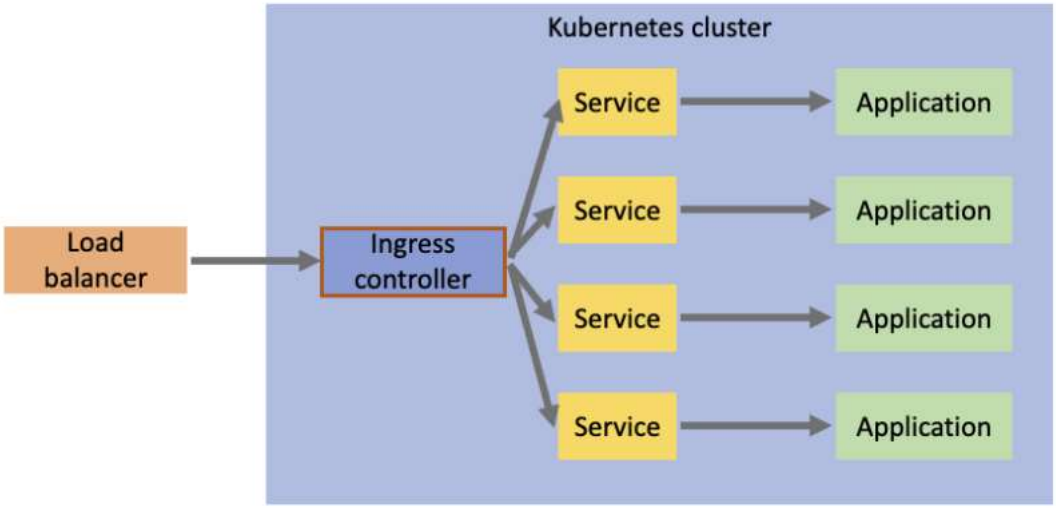

Figura 30-Pubblicazione dei servizi in modalità Avanzata con Ingress Controller

A differenza del caso precedente, ora il traffico esterno fluirà attraverso un singolo *Load Balancer* verso l'"*Ingress Controller***"** che prenderà la configurazione di ingresso per determinare a quale servizio inoltrare il traffico.

In questa sezione è illustrato il *Deploy* di un'applicazione di esempio "*Hello World*" in modalità Avanzata.
Dopo aver installato *Contour* (vedere paragrafo 6.2.4), il primo step prevede la creazione di un file *Yaml* contenente le configurazioni dell'applicazione e la sezione "*HTTPProxy"* deve essere del tipo:

```
kind: HTTPProxy

apiVersion: projectcontour.io/v1
metadata:
 name: hello-world
 namespace: default
spec:
 routes:
  - services:
    - name: hello-world
      port: 80
---
kind: HTTPProxy
apiVersion: projectcontour.io/v1
metadata:
 name: main
 namespace: default
spec:
 virtualhost:
  fqdn: myapps
 includes:
  - name: hello-world
    namespace: default
    conditions:
     - prefix: /hello-world
  - name: dashboard
    namespace: kubernetes-dashboard
    conditions:
     - prefix: /
```

Dopo aver creato il file *Yaml*, con il comando:

- *"kubeconfig apply – f [nomefile].yaml"*

È possibile effettuare il *Deploy* e l'esposizione dell'applicazione "*Hello World";* Per verificare che lo stato dell'"*HTTPProxy"* sia *"Valid"* eseguire il comando:

- *"kubectl get Proxy -A"*

L'applicazione sarà quindi raggiungibile collegandosi via web all'indirizzo:

- *"http://myapps/hello-world"*

NOTA: si ricorda che l'FQDN, in questo caso specifico "*myapps"*, deve essere registrato all'interno del DNS Pubblico con riferimento al Public IP assegnato all'"Ingress Controller".