

Implementação e Configuração do ambiente TKGm

O propósito da documentação é abordar o processo de implementação do VMware Tanzu Kubernetes Grid Management (TKGm) em infraestrutura VMware vSphere 8.

Requisitos Gerais para Implantação do Tanzu Kubernetes Grid

 Máquina de Bootstrap com os seguintes softwares instalados:

- **Sistema operacional:** Ubuntu 22.04 ou superior
- **Shell:** `bash`
- **Permissões:** Acesso como usuário com privilégios `sudo`
- **Internet:** Conexão ativa e funcional
- **Arquitetura suportada:** `amd64 (64-bit Intel/AMD)`

[!IMPORTANT]

Utilize o script [tkgm-bastion.sh](#) para instalação dos pacotes necessários.

Executando o Script

```
curl -fsSL  
https://raw.githubusercontent.com/sretriples/setups/refs/heads/main/tkgm-  
bastion.sh | bash
```

Consulte: [Instalação do Tanzu CLI](#)

- Utilizada para executar comandos `tanzu`, `kubectl` e outros.
- Pode ser uma máquina física local ou uma VM acessada via console ou shell remoto.

Ambiente Compatível

- vSphere 7 ou 8
- [Permissões Requeridas para Conta no vSphere](#)

Estrutura Requerida no vSphere

- Um host standalone ou um cluster com **mínimo de dois hosts**
- Recomenda-se **vSphere DRS habilitado** se usar cluster
- Recursos necessários:
 - Pool de recursos (opcional)
 - Pasta de VMs para organização
 - Datastore com espaço suficiente para control plane e nós workers

🛠️ Preparação do Ambiente vSphere

- Template de imagem base compatível com a versão do cluster
 - Conta vSphere com permissões apropriadas para o TKG
 - Se usar **Avi Load Balancer**, ele deve estar corretamente implantado
-

📡 Requisitos de Rede

- Rede vSphere com:
 - DHCP ou IPs estáticos disponíveis
 - Servidor DNS acessível
 - Servidor DHCP configurado com:
 - **Opção 3 (Gateway)**
 - **Opção 6 (DNS)**
 - IPs virtuais estáticos disponíveis para:
 - Todos os clusters (gerenciamento e workloads)
 - Configure o endpoint do control plane com **VSPHERE_CONTROL_PLANE_ENDPOINT**, ou deixe o Avi Load Balancer gerenciar
-

💡 Conectividade Necessária

- Comunicação permitida:
 - Entre clusters e **vCenter Server**
 - Da máquina bootstrap para **porta 6443** (API Kubernetes) nas VMs
 - Das VMs para o **vCenter Server na porta 443**
 - Máquina bootstrap para os repositórios de imagens (porta 443/TCP)
-

⌚ Configuração de sincronização de hora (NTP)

- Todos os hosts e a máquina bootstrap devem estar em UTC com **NTP ativo**
- Para verificar:

```
ssh [host]
date
esxcli system time set
```

Criação de usuário para o TKGm

<https://techdocs.broadcom.com/us/en/vmware-tanzu/standalone-components/tanzu-kubernetes-grid/2-5/tkg/mgmt-reqs-prep-vsphere.html#vsphere-permissions>

Permissões Requeridas para Conta vSphere

A conta **vCenter Single Sign-On (SSO)** fornecida ao Tanzu Kubernetes Grid durante a implantação do cluster de gerenciamento deve possuir as permissões adequadas para executar operações no vSphere.

Recomendação: Não utilize a conta de administrador do vSphere.

O ideal é criar uma **função (role)** com permissões específicas e um **usuário** dedicado, atribuindo essa função aos objetos necessários no vSphere.

Se pretende utilizar o **Velero** para backup e restauração de clusters de workload, adicione também as permissões descritas em:

- [Credenciais e Privilégios para Acesso a VMDK \(VMware Virtual Disk Development Kit Guide\)](#)

Criando a Função e o Usuário

Etapas Gerais

1. No **vSphere Client**, crie uma nova função (ex: **TKG**) com as permissões listadas abaixo.
2. Crie um novo usuário (ex: **tkg-user**) no domínio apropriado.
3. Atribua o usuário **tkg-user** à função **TKG** em todos os objetos vSphere que serão utilizados pela implantação do Tanzu Kubernetes Grid.

Permissões Necessárias por Objeto vSphere

Objeto vSphere	Permissões Requeridas
Cns	Searchable
Datastore	Allocate space
	Browse datastore
	Low level file operations
Global (se usar Velero)	Disable methods
	Enable methods
	Licenses
Network	Assign network
Profile-driven storage	Profile-driven storage view
Resource	Assign virtual machine to resource pool
Sessions	Message
	Validate session
Virtual Machine	Change Configuration > Add existing disk

Objeto vSphere	Permissões Requeridas
	Add new disk
	Add or remove device
	Advanced configuration
	Change CPU count
	Change Memory
	Change Settings
	Configure Raw device
	Extend virtual disk
	Modify device settings
	Remove disk
	Toggle disk change tracking *
	Edit Inventory > Create from existing
	Remove
	Interaction > Power On / Power Off
	Provisioning > Allow read-only disk access *
	Allow virtual machine download *
	Deploy template
	Snapshot Management > Create snapshot *
	Remove snapshot *
vApp	Import

⚠️ Permissões marcadas com * são necessárias apenas para habilitar o plugin do Velero. Elas podem ser adicionadas posteriormente, se desejado.

⌚ Atribuição da Função aos Objetos

Atribua a função TKG ao usuário tkg-user nos seguintes objetos:

💻 Hosts e Clusters

- Objeto raiz do vCenter Server
- Datacenter e todas as pastas de Hosts e Clusters (do Datacenter até o cluster de destino)
- Hosts e clusters alvo
- Pools de recursos alvo (com propagação para os filhos ativada)

💻 VMs e Templates

- Templates de imagem base do Tanzu Kubernetes Grid
- Pastas de VMs e Templates alvo (com propagação para os filhos ativada)

📁 Armazenamento

- Datastores e todas as pastas de armazenamento (do Datacenter até os datastores utilizados)

📡 Rede

- Redes ou grupos de portas distribuídas (Distributed Port Groups) atribuídas aos clusters
- Switches distribuídos (Distributed Switches), se aplicável

Para mais detalhes sobre como criar funções e usuários no vCenter Server, consulte:

[Utilização de Funções no vCenter Server para Atribuir Privilégios \(vSphere 8\)](#)

🚀 Implantação do Tanzu Kubernetes Grid Management

⌨️ Criação da chave SSH para acesso às VMs dos Clusters

```
ssh-keygen -t rsa -b 4096 -C "email@example.com"
```

⌨️ Adicione a chave no SSH Agent

```
ssh-add ~/.ssh/id_rsa
```

Instalação do Management Cluster

[!IMPORTANT]

A instalação do Management Cluster inicia pela execução do comando abaixo no BootStrap, habilitando a interface gráfica para geração do arquivo de instalação.

⌨️ Comando para habilitar a UI

```
tanzu management-cluster create --ui --bind 10.5.1.141:8080 --browser none -v 9
```

Exemplo da URL de acesso a UI

<http://10.5.1.141:8080/#/ui>

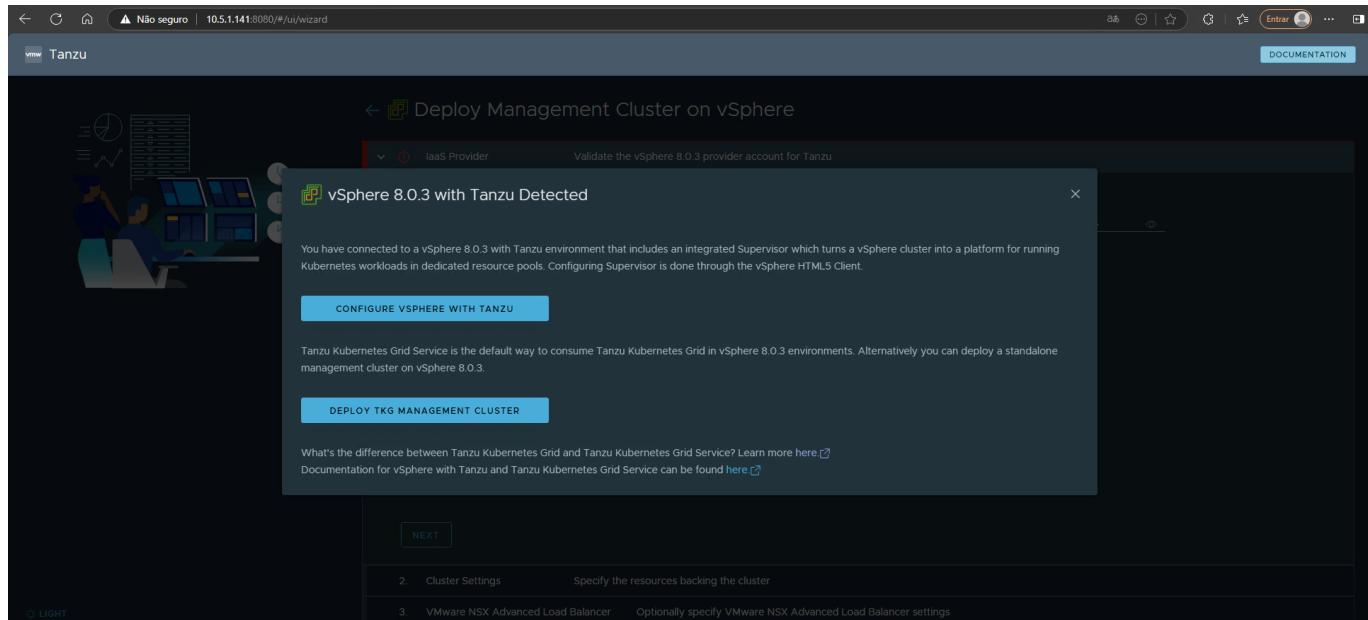
1 - Clique em DEPLOY

The screenshot shows the 'Welcome to the VMware Tanzu Kubernetes Grid Installer' page. It features a central illustration of two people working at a computer, surrounded by icons related to cloud, databases, and infrastructure. To the right, there is descriptive text about Tanzu Kubernetes Grid and a 'Deploy the management cluster' button. Below this, a specific section for 'VMware vSphere' is shown with a 'DEPLOY' button.

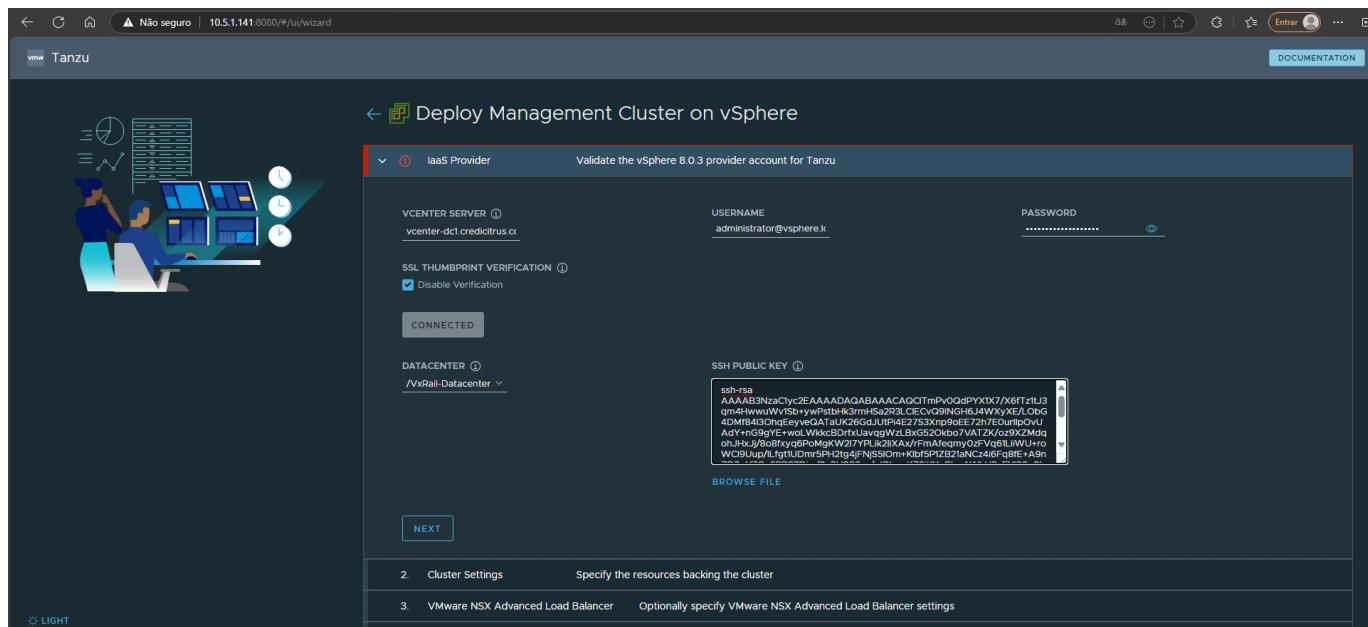
2 - Adicione as informações de acesso ao vSphere e clique em CONNECT

The screenshot shows the 'Deploy Management Cluster on vSphere' wizard, step 1: IaaS Provider. It asks to validate the vSphere provider account for Tanzu. It includes fields for 'VCENTER SERVER' (vcenter-dc1.credictrus.br), 'USERNAME' (administrator@vsphere.br), and 'PASSWORD'. There is also an 'SSL THUMBPRINT VERIFICATION' section with a checked 'Disable Verification' option and a 'CONNECT' button. Step 2, 'Cluster Settings', is visible at the bottom.

3 - Clique em DEPLOY TKG MANAGEMENT CLUSTER

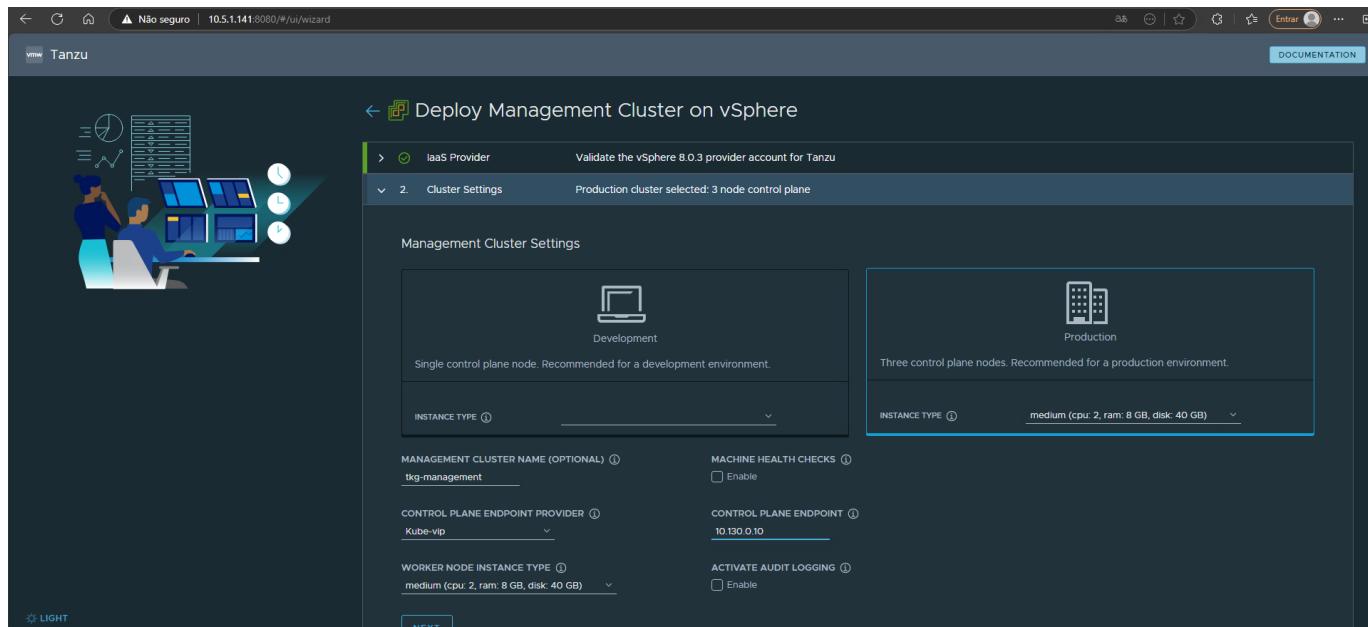


4 - Adicione em **SSH PUBLIC KEY** a chave SSH gerada e clique em **NEXT**

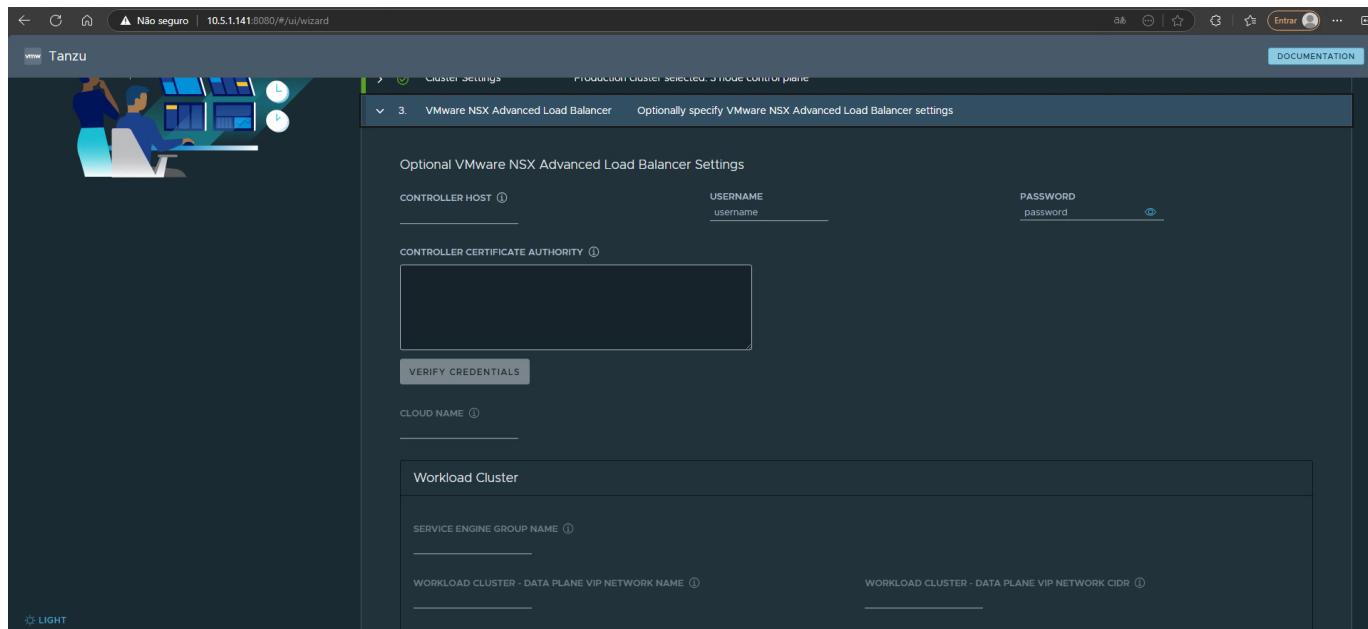


5 - Selecione a configuração **Production** e a capacidade das VMs e clique em **NEXT**.

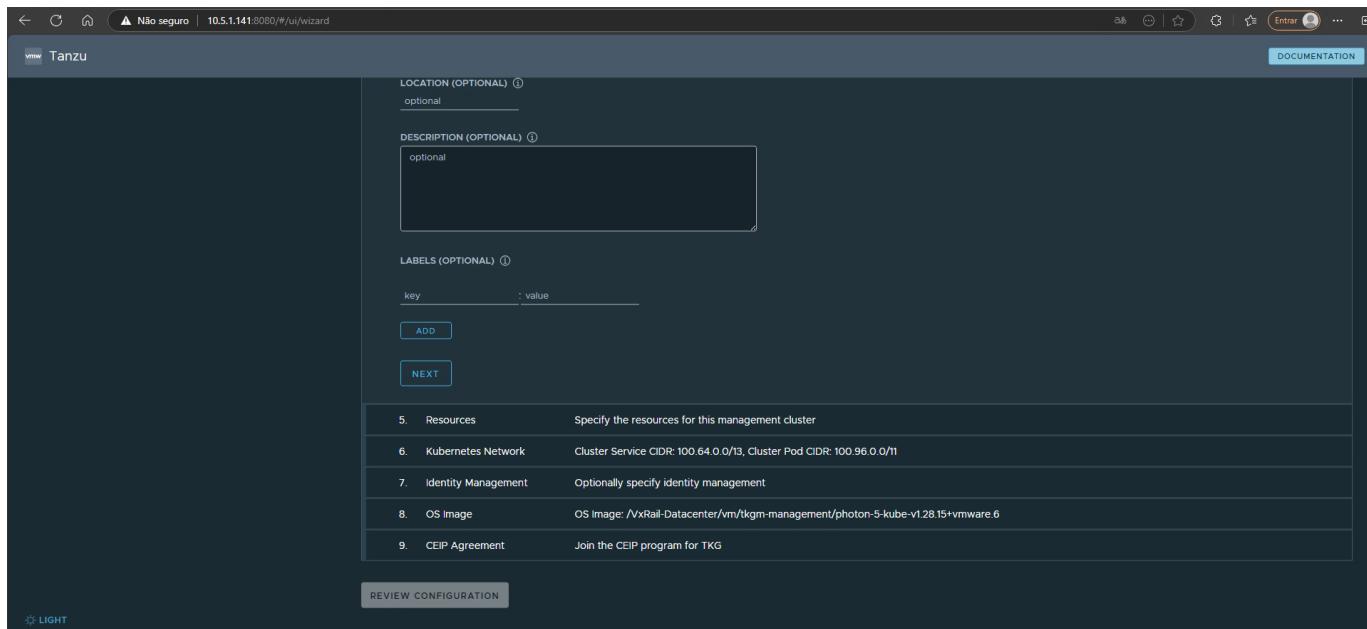
Ex.: medium (cpu 2, ram 8 GB, disk 40 GB)



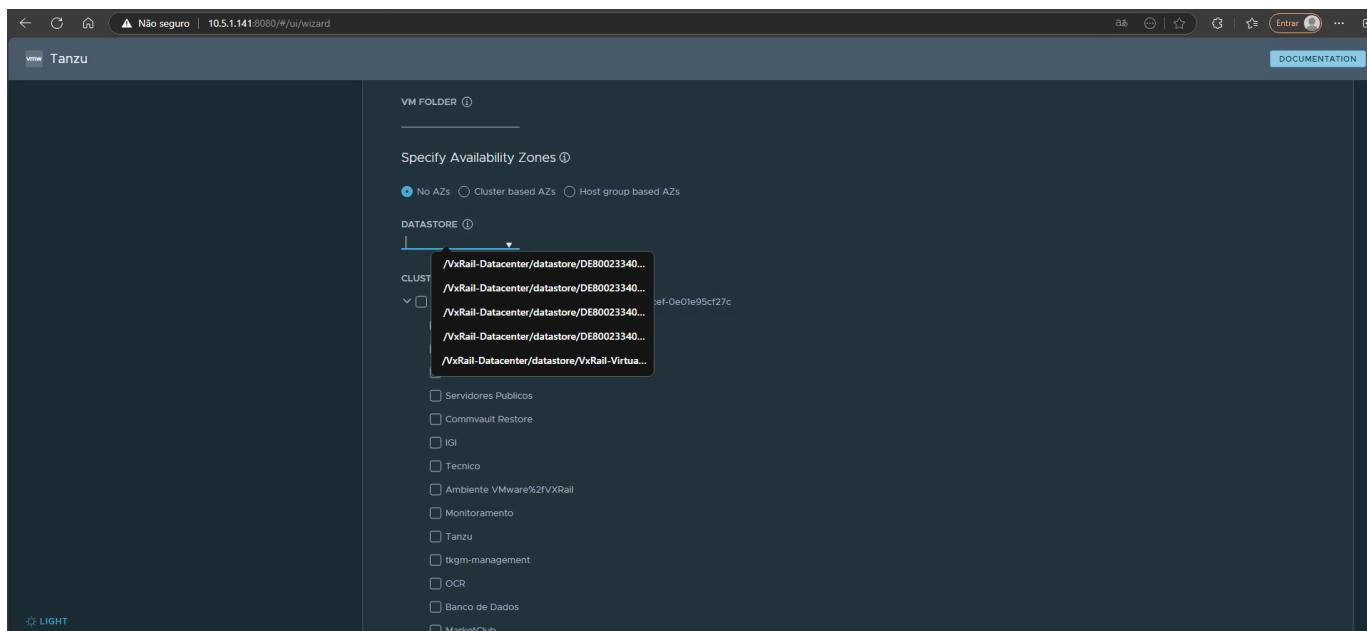
6 - No item 3 Clique em **NEXT** pois a solução adotada foi o Kube-VIP



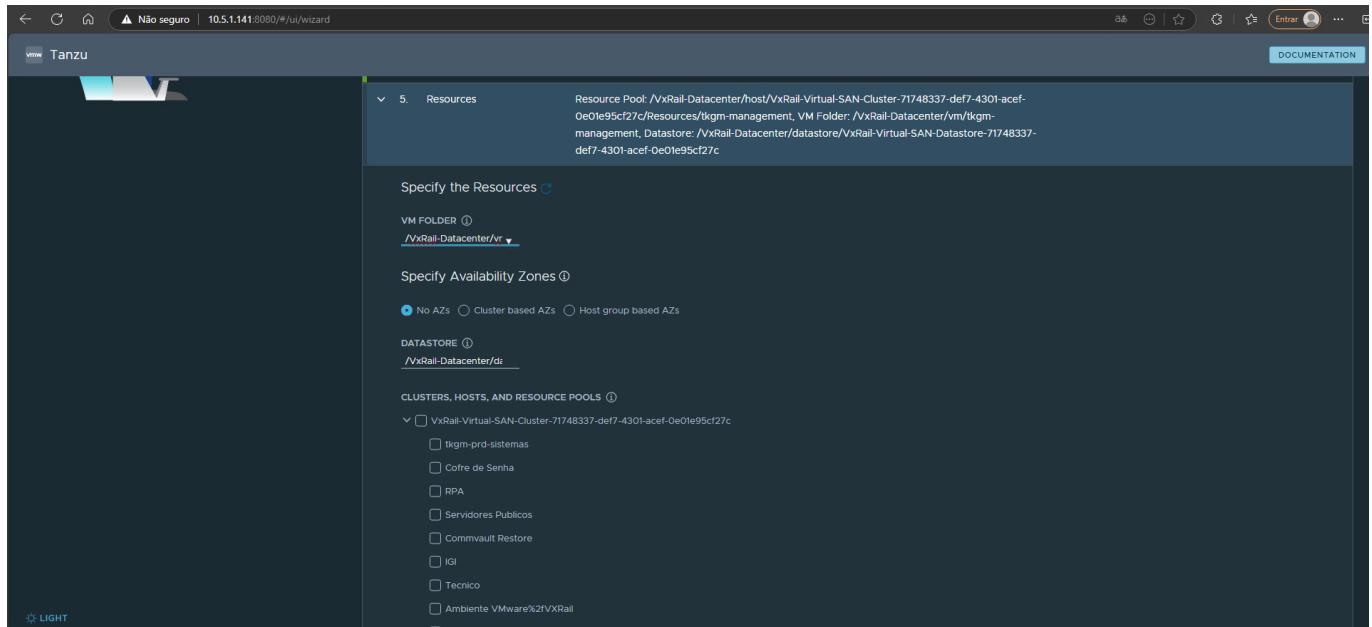
7 - No item 4 Clique em **NEXT**



8 - Selecione o Datastore em DATASTORE

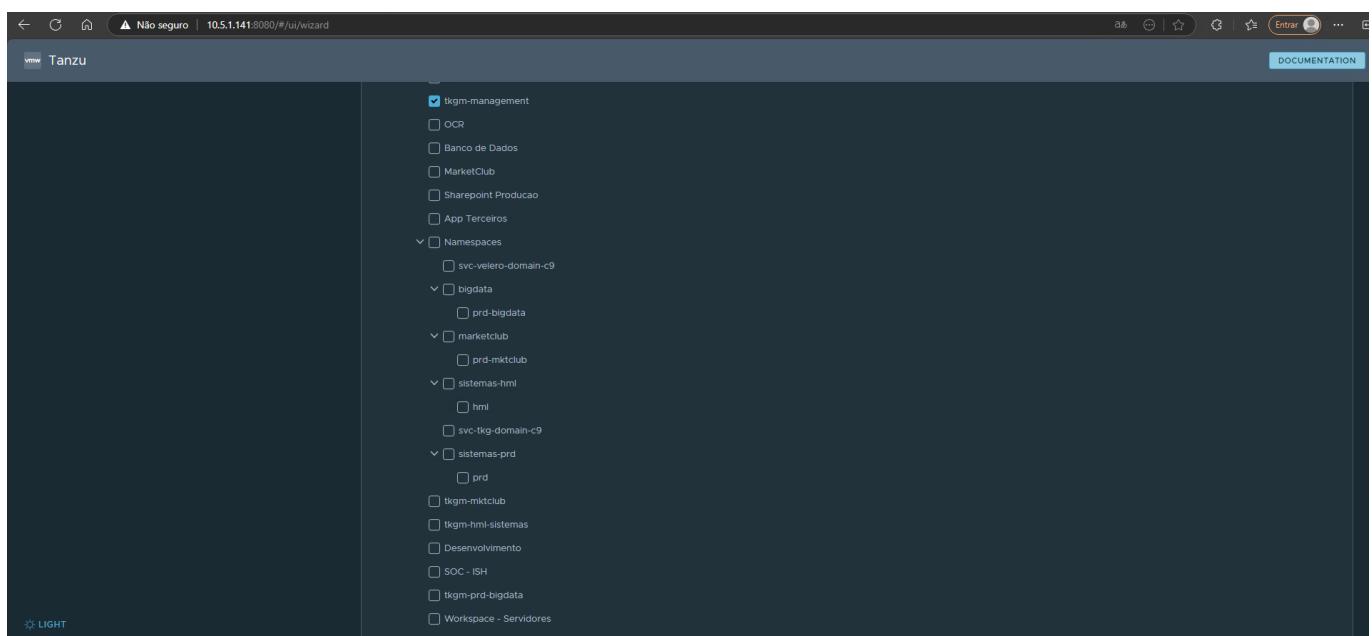


9 - Selecione o VM folder e mantenha selecionada a opção No AZs



10 - Selecione a opção de folder definida para o Management Cluster e clique em **NEXT**

Ex.: tkgn-management



11 - Selecione a rede que será utilizada em **NETWORK NAME** e clique em **NEXT**

Ex.: [.../tkgm-workload](#)

12 - Habilite a opção **ACTIVE INDENTITY MANAGEMENT SETTINGS** e clique em **NEXT**

13 - Em **Identity Management** selecione a opção **LDAPS**, insira as opções pertinentes ao ambiente Active Directory, adicione o conteúdo do certificado da Entidade Certificadora Interna (AD-CS) em **ROOT CA** e clique em **NEXT**

Não seguro | 10.5.1.141:8080/#/ui/wizard

vmw Tanzu DOCUMENTATION

Identity Management LDAP configured: credicitrus.com.br:636

Optionally Specify Identity Management with OIDC or LDAPS

ACTIVATE IDENTITY MANAGEMENT SETTINGS

OIDC LDAPS

LDAPS Identity Management Source

LDAPS ENDPOINT ⓘ
credicitrus.com.br:636

BIND DN (OPTIONAL) ⓘ
CN=srv_tkgn,OU=Conta

BIND PASSWORD (OPTIONAL) ⓘ
.....

User Search Attributes

BASE DN (OPTIONAL) ⓘ
DC=credicitrus,DC=com.br

FILTER ⓘ
(&(objectClass=person))

USERNAME ⓘ
dn

Group Search Attributes

BASE DN (OPTIONAL) ⓘ
DC=credicitrus,DC=com.br

FILTER ⓘ
(&(objectClass=group))

NAME ATTRIBUTE (OPTIONAL) ⓘ
cn

USER ATTRIBUTE (OPTIONAL) ⓘ
sAMAccountName

GROUP ATTRIBUTE (OPTIONAL) ⓘ
sAMAccountName

ROOT CA (OPTIONAL) ⓘ

VERIFY LDAP CONFIGURATION (OPTIONAL) ⓘ

VERIFY LDAP CONFIGURATION ⓘ

The screenshot shows the Tanzu VMWARE Cloud Director configuration wizard. The top bar displays the URL as 10.5.1.141:8080/#/ui/wizard. The main area is titled "User Search Attributes" and "Group Search Attributes". Under "User Search Attributes", the "BASE DN (OPTIONAL)" field contains "DC=credicitrus,DC=com," and the "FILTER (OPTIONAL)" field contains "(&(objectClass=person))". The "USERNAME (OPTIONAL)" section has a "dn" input field. Under "Group Search Attributes", the "BASE DN (OPTIONAL)" field contains "DC=credicitrus,DC=com," and the "FILTER (OPTIONAL)" field contains "(&(objectClass=group))". The "NAME ATTRIBUTE (OPTIONAL)" section has a "cn" input field. Below these sections, there is a large text box containing a long string of characters, likely a password or token. At the bottom, there are two "NEXT" buttons, one for each search attribute section. The footer includes a "REVIEW CONFIGURATION" button and a "LIGHT" mode switch.

14 - Selecione a imagem que será utilizada em OS IMAGE e clique em NEXT



Não seguro | 10.5.1.141:8080/#/ui/wizard

Cluster Settings Production cluster selected: 3 node control plane

VMware NSX Advanced Load Balancer Optionally specify VMware NSX Advanced Load Balancer settings

Metadata Specify metadata for the management cluster

Resources Resource Pool: /VxRail-Datacenter/host/VxRail-Virtual-SAN-Cluster-71748337-def7-4301-acef-0e0te95cf27c/Resources/tkgm-management. VM Folder: /VxRail-Datacenter/vm/tkgm-management. Datastore: /VxRail-Datacenter/datastore/VxRail-Virtual-SAN-Datastore-71748337-def7-4301-acef-0e0te95cf27c

Kubernetes Network Network: /VxRail-Datacenter/network/tkgm-workload, Cluster Service CIDR: 100.64.0.0/13. Cluster Pod CIDR: 100.96.0.0/11

Identity Management LDAP configured: credicitrus.com.br:636

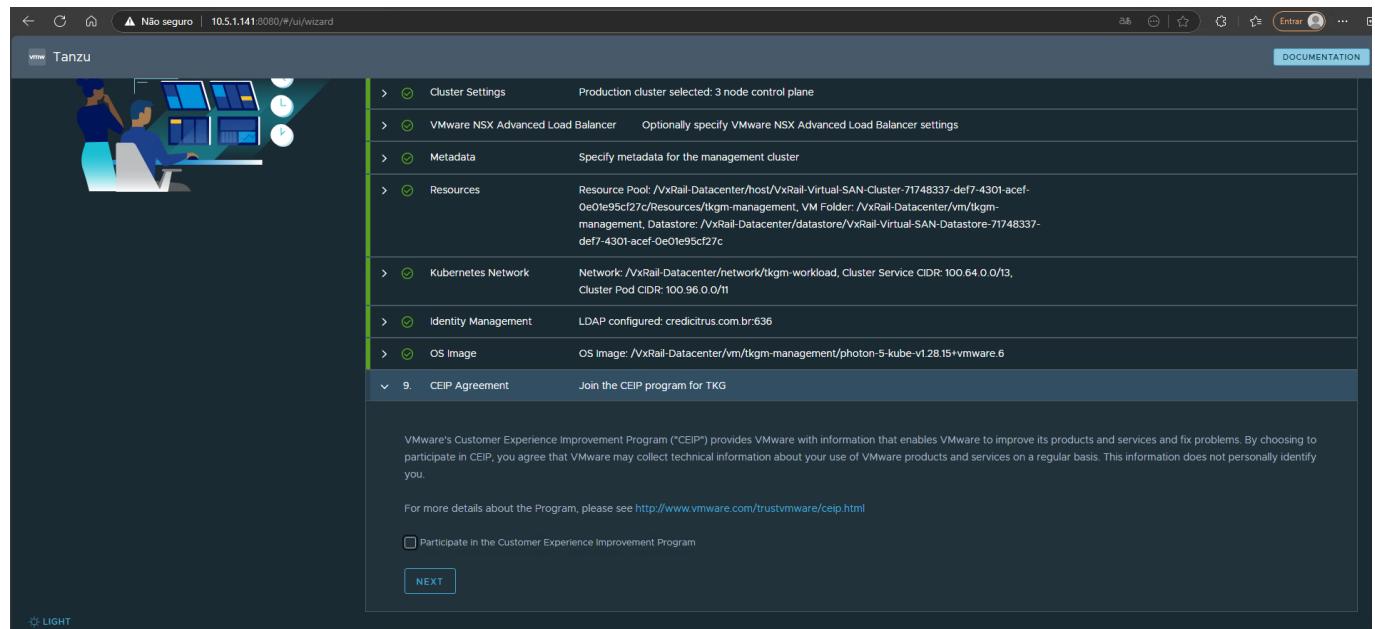
OS Image OS Image: /VxRail-Datacenter/vm/tkgm-management/photon-5-kube-v1.28.15+vmware-6

OS Image with Kubernetes v1.28.15+vmware-6-tkg.1

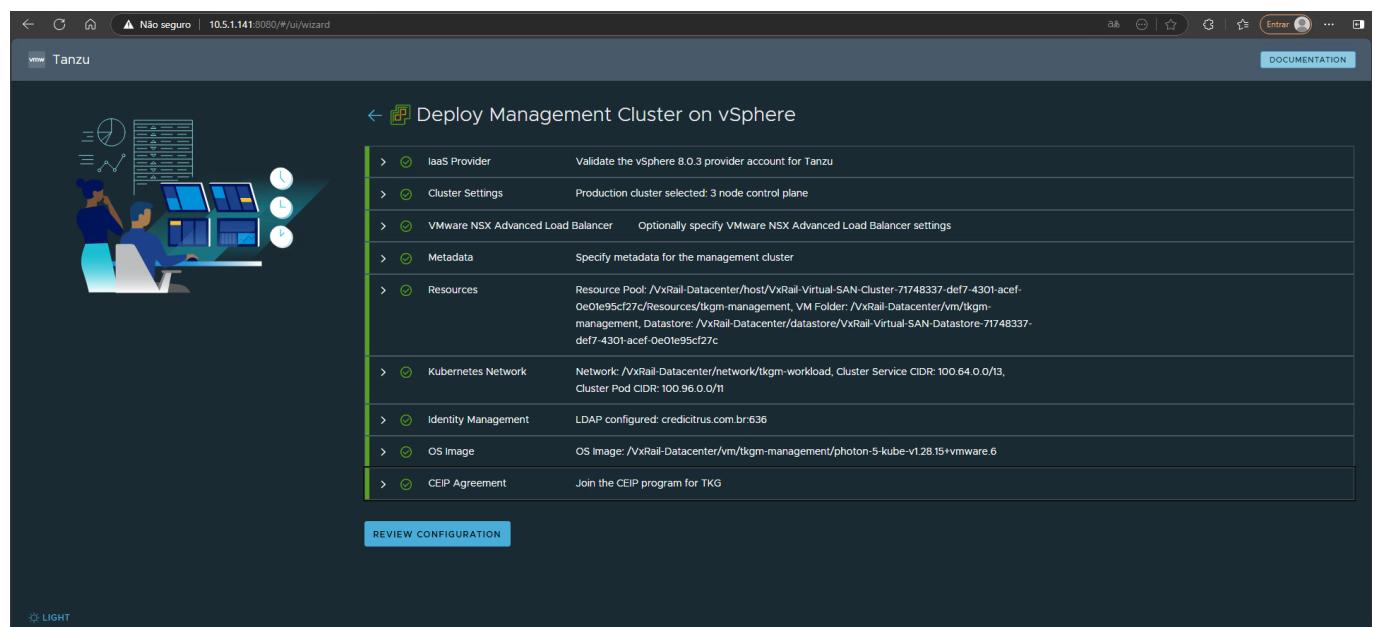
OS IMAGE ⓘ
/VxRail-Datacenter/vm/tkgm-management/photon-5-kube-

CEIP Agreement Join the CEIP program for TKG

15 - Em CEIP Agreement mantenha marcado caso queira participar de forma voluntária para prover informações técnicas para a Broadcom, ou, caso não queira, desmarque a opção e clique em **NEXT**



16 - Clique em **REVIEW CONFIGURATION** para revisar as configurações realizadas nos intenc anteriores



Não seguro | 10.5.1.141:8080/#/ui/wizard

[Entrar](#)

Tanzu

DOCUMENTATION

VMware NSX Advanced Load Balancer

VMware NSX Advanced Load Balancer	Optionally specify VMware NSX Advanced Load Balancer settings
CLUSTER LABELS (OPTIONAL)	
Metadata	
Metadata	Specify metadata for the management cluster
LABELS (OPTIONAL)	
Resources	
Resources	Resource Pool: /VxRail-Datacenter/host/VxRail-Virtual-SAN-Cluster-71748337-def7-4301-acef-0e01e95cf27c/Resources/tkgm-management, VM Folder: /VxRail-Datacenter/vm/tkgm-management, Datastore: /VxRail-Datacenter/datastore/VxRail-Virtual-SAN-Datastore-71748337-def7-4301-acef-0e01e95cf27c
VM FOLDER	/VxRail-Datacenter/vm/tkgm-management
DATASTORE	/VxRail-Datacenter/datastore/VxRail-Virtual-SAN-Datastore-71748337-def7-4301-acef-0e01e95cf27c
CLUSTERS, HOSTS, AND RESOURCE POOLS	/VxRail-Datacenter/host/VxRail-Virtual-SAN-Cluster-71748337-def7-4301-acef-0e01e95cf27c/Resources/tkgm-management
Kubernetes Network	
Kubernetes Network	Network: /VxRail-Datacenter/network/tkgm-workload, Cluster Service CIDR: 100.64.0.0/13, Cluster Pod CIDR: 100.96.0.0/11
NETWORK NAME	/VxRail-Datacenter/network/tkgm-workload
CNI PROVIDER	antrea
CLUSTER SERVICE CIDR	100.64.0.0/13
CLUSTER POD CIDR	100.96.0.0/11
ACTIVATE PROXY SETTINGS	no
USE SAME CONFIGURATION FOR HTTPS PROXY	yes

[!IMPORTANT]

Após revisão clique em **EXPORT CONFIGURATION** pois o arquivo **config.yaml** será utilizado para criação do Management Cluster

The screenshot shows the Tanzu UI wizard interface. At the top, there's a navigation bar with a back arrow, forward arrow, and a link to '10.5.1.141:8080/#/ui/wizard'. Below the navigation is a search bar with placeholder text 'Não seguro'.

The main form contains several input fields:

- USERNAME:** ceditricitrus
- BASE DN (OPTIONAL):** DC=cedriticitrus,DC=com,DC=br
- FILTER:** (&(objectClass=group)(member.1.2.84.1.13566.1.4.1941={}))
- NAME ATTRIBUTE (OPTIONAL):** cn
- USER ATTRIBUTE (OPTIONAL):** sAMAccountName
- GROUP ATTRIBUTE (OPTIONAL):** sAMAccountName
- ROOT CA (OPTIONAL):** A large text area containing a base64 encoded certificate.

To the right of the form, a 'Downloads' sidebar is open, showing two files:

- config (4).yaml
- config (3).yaml

Below the sidebar is a 'DOCUMENTATION' button.

At the bottom of the page are three buttons: 'DEPLOY MANAGEMENT CLUSTER', 'EDIT CONFIGURATION', and 'EXPORT CONFIGURATION'.

🛡️ Valide o arquivo de configuração:

```

● ● ●
1 AVI_CA_DATA_B64: ""
2 AVI_CLOUD_NAME: ""
3 AVI_CONTROL_PLANE_HA_PROVIDER: "false"
4 AVI_CONTROL_PLANE_NETWORK: ""
5 AVI_CONTROL_PLANE_NETWORK_CIDR: ""
6 AVI_CONTROLLER: ""
7 AVI_DATA_NETWORK: ""
8 AVI_DATA_NETWORK_CIDR: ""
9 AVI_ENABLE: "false"
10 AVI_LABELS: ""
11 AVI_MANAGEMENT_CLUSTER_CONTROL_PLANE_VIP_NETWORK_CIDR: ""
12 AVI_MANAGEMENT_CLUSTER_CONTROL_PLANE_VIP_NETWORK_NAME: ""
13 AVI_MANAGEMENT_CLUSTER_SERVICE_ENGINE_GROUP: ""
14 AVI_MANAGEMENT_CLUSTER_VIP_NETWORK_CIDR: ""
15 AVI_MANAGEMENT_CLUSTER_VIP_NETWORK_NAME: ""
16 AVI_PASSWORD: ""
17 AVI_SERVICE_ENGINE_GROUP: ""
18 AVI_USERNAME: ""
19 CLUSTER_ANNOTATIONS: description:,location:tkg-management-dc1
20 CLUSTER_CIDR: 100.96.0.0/11
21 CLUSTER_NAME: tkg-management
22 CLUSTER_PLAN: prod
23 MANAGEMENT_NODE_IPAM_IP_POOL_GATEWAY: "10.130.1.254"
24 MANAGEMENT_NODE_IPAM_IP_POOL_ADDRESSES: "10.130.0.11-10.130.0.20"
25 MANAGEMENT_NODE_IPAM_IP_POOL_SUBNET_PREFIX: "23"
26 CONTROL_PLANE_NODE_NAMESERVERS: "10.5.0.80,10.5.0.163"
27 WORKER_NODE_NAMESERVERS: "10.5.0.80,10.5.0.163"
28 ENABLE_AUDIT_LOGGING: "false"
29 ENABLE_MHC: "true"
30 ENABLE_CEIP_PARTICIPATION: false
31 IDENTITY_MANAGEMENT_TYPE: ldap
32 INFRASTRUCTURE_PROVIDER: vsphere
33 LDAP_BIND_DN: "CN=srv_tkgm,OU=Contas de Serviço,OU=Usuários de Manutenção,DC=credicitrus,DC=com,DC=br"
34 LDAP_BIND_PASSWORD: "<encoded>SENHASEGURABASE64"
35 LDAP_GROUP_SEARCH_BASE_DN: "DC=credicitrus,DC=com,DC=br"
36 LDAP_GROUP_SEARCH_FILTER: "(&(objectClass=group)(member:1.2.840.113556.1.4.1941:={}))"
37 LDAP_GROUP_SEARCH_NAME_ATTRIBUTE: cn
38 LDAP_GROUP_SEARCH_USER_ATTRIBUTE: sAMAccountName
39 LDAP_HOST: "credicitrus.com.br:636"
40 LDAP_ROOT_CA_DATA_B64: "LS0tLS1CRUJTiBDRVJUS..."
41 LDAP_USER_SEARCH_BASE_DN: "DC=credicitrus,DC=com,DC=br"
42 LDAP_USER_SEARCH_FILTER: "(&(objectClass=(!computer))(!showInAdvancedViewOnly=TRUE))(|(sAMAccountName={})(mail={})(userPrincipalName={}))({sAMAccountType=805306368})"
43 LDAP_USER_SEARCH_NAME_ATTRIBUTE: dn
44 LDAP_USER_SEARCH_USERNAME: sAMAccountName
45 OS_ARCH: amd64
46 OS_NAME: photon
47 OS_VERSION: "5"
48 SERVICE_CIDR: 100.64.0.0/13
49 TKG_HTTP_PROXY_ENABLED: "false"
50 VSphere_CONTROL_PLANE_DISK_GIB: "40"
51 VSphere_CONTROL_PLANE_ENDPOINT: 10.130.0.10
52 VSphere_CONTROL_PLANE_MEM_MIB: "8192"
53 VSphere_CONTROL_PLANE_NUM_CPUS: "2"
54 VSphere_DATACENTER: /VxRail-Datacenter
55 VSphere_DATASTORE: /VxRail-Datacenter/datastore/VxRail-Virtual-SAN-Datastore-71748337-def7-4301-acef-0e01e95cf27c
56 VSphere_FOLDER: /VxRail-Datacenter/vm/tkgm-management
57 VSphere_INSECURE: "true"
58 VSphere_NETWORK: /VxRail-Datacenter/network/tkgm-workload
59 VSphere_PASSWORD: <encoded>SENHASEGURABASE64
60 VSphere_RESOURCE_POOL: /VxRail-Datacenter/host/VxRail-Virtual-SAN-Cluster-71748337-def7-4301-acef-0e01e95cf27c/Resources/tkgm-management
61 VSphere_SERVER: vcenter-dc1.credicitrus.com.br
62 VSphere_SSH_AUTHORIZED_KEY: ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQACQC...service@credicitrus.com.br
63 VSphere_TLS_THUMPREPRINT: ""
64 VSphere_USERNAME: adminuser@vsphere.local
65 VSphere_WORKER_DISK_GIB: "40"
66 VSphere_WORKER_MEM_MIB: "8192"
67 VSphere_WORKER_NUM_CPUS: "2"
68 WORKER_ROLLOUT_STRATEGY: ""
69

```

█ Após validação, execute o comando abaixo:

```
tanzu management-cluster create tkg-management --dry-run -f config.yaml > tkg-management.yaml
```

█ Execute o comando abaixo para criação do Management Cluster:

```
tanzu management-cluster create tkg-management --file tkg-management.yaml -v 9
```

█ Execute o comando abaixo para exportar o kubeconfig do Management Cluster

```
tanzu management-cluster kubeconfig get --admin --export-file /TKGm/dc01/management/kube-config-tkg-management
```

- Execute o comando abaixo para renomear o contexto

```
kubectl config rename-context tkg-management@tkg-management tkg-management
```

- Execute o comando abaixo para definir o contexto corrente

```
kubectl config use-context tkg-management
```

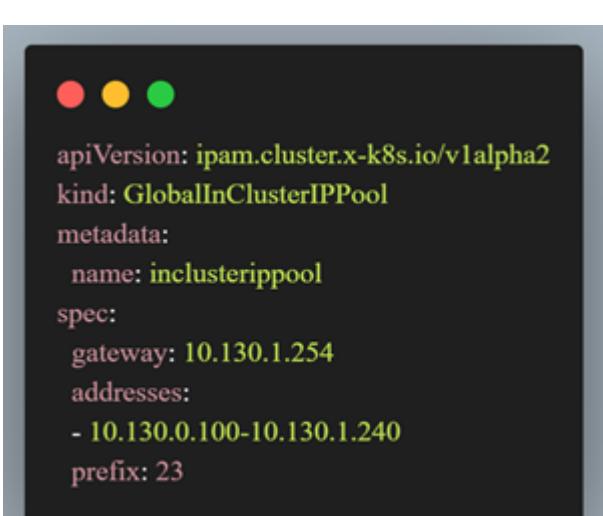
[!IMPORTANT]

Implementação do TKG Management utilizando a solução Kube-VIP Load Balancer (L4 Load Balancer) é necessário configurar o Node IPAM. Recurso útil em ambientes onde o uso de DHCP não é viável ou desejável, permitindo a alocação e gerenciamento de endereços IP com previsibilidade.

- Execute o comando abaixo para para criar o objeto **GlobalInClusterIPPool**

```
kubectl create -f GlobalInClusterIPPool.yaml
```

- Manifesto GlobalInClusterIPPool.yaml



```
apiVersion: ipam.cluster.x-k8s.io/v1alpha2
kind: GlobalInClusterIPPool
metadata:
  name: inclusterippool
spec:
  gateway: 10.130.1.254
  addresses:
  - 10.130.0.100-10.130.1.240
  prefix: 23
```

-
- Criacao do Workload Cluster

```
kubectl config use-context <MANAGEMENT_CLUSTER_CONTEXT>
```

- Criação do Namespace onde o Workload Cluster será criado

```
kubectl create ns <tkgm-ambiente-cluster>
```

💻 Preparação do manifesto yaml baseado no template

```
tanzu cluster create tkgm-prd-bigdata --dry-run --file tkgm-prd-bigdata.yaml > tkgm-prd-bigdata-legacy.yaml
```

💻 Criação do cluster

```
tanzu cluster create -f tkgm-prd-bigdata-legacy.yaml -v 9 --tkr v1.28.15---vmware.6-tkg.1
```

Exportação do kubeconfig

👤 Perfil Admin

```
tanzu cluster kubeconfig get tkgm-prd-bigdata -n tkgm-prd-bigdata --admin --export-file tkgm-prd-bigdata-config
```

👤 Perfil LDAP

```
tanzu cluster kubeconfig get tkgm-prd-bigdata -n tkgm-prd-bigdata --export-file /tmp/tkgm-prd-bigdata-config
```

[!IMPORTANT]

Para realizar o acesso LDAP via Pinniped será necessário configurar algumas variáveis para obter sucesso

```
export KUBECONFIG=/TKGm/management/tkgm-prd-bigdata-config  
export TANZU_CLI_PINNIPED_AUTH_LOGIN_SKIP_BROWSER=true  
export PINNIPED_UPSTREAM_IDENTITY_PROVIDER_FLOW=cli_password  
export PINNIPED_USERNAME=login  
export PINNIPED_PASSWORD="SENHA"
```

[!TIP] Atividade executada para o Victor realizar a cópia via WinSCP

```
chown "bt.vjose:domain users" /tmp/tkgm-prd-bigdata-config
```

🔧 Configuração do arquivo config `~/.kube/config`. Vide shellscript `join.sh`

📄 Conteúdo do script

```
#!/bin/bash
unset KUBECONFIG
export KUBECONFIG=~/ kube/config:/TKGm/tkg/prd-sistemas/tkgm-prd-sistemas-config
kubectl config view --flatten > /tmp/config-merged.yaml && mv /tmp/config-
merged.yaml ~/ kube/config
unset KUBECONFIG
```

💻 Selecionar o contexto do Workload Cluster

```
kubectl config use-context <CLUSTER_CONTEXT>
```

📦 Instalação do MetalLB

💻 Configuração do ConfigMap kube-proxy para instalação do MetalLB

```
kubectl edit configmap -n kube-system kube-proxy
```

Atributo:

```
apiVersion: kubeproxy.config.k8s.io/v1alpha1
kind: KubeProxyConfiguration
mode: "ipvs"
ipvs:
  strictARP: true
```

💻 Instalação dos operadores MetalLB

```
kubectl apply -f
https://raw.githubusercontent.com/metallb/metallb/v0.14.9/config/manifests/metallb-
-native.yaml
```

💻 Criação do IPAddressPool

```
kubectl create -f IPAddressPool.yaml
```

💻 Criação do L2Advertisement

```
kubectl create -f L2Advertisement.yaml
```

- 🔗 DaemonSet para criação do arquivo de certificado da CA interna `/etc/ssl/certs/harbor-ca.crt`, adição do hostname, fqdn e ip da VM harbor no arquivo `/etc/hosts` dos Worker Nodes. E criação do ConfigMap com o conteúdo do certificado.

```
kubectl create -f harbor-ca.yaml
```

- ⌚ Criação dos clusterrolebinding com base na definição de papéis informados pelo cliente. Vide shellscript `add-roles.sh`.

📄 Conteúdo do script

```
#!/bin/bash

# Script para criar ClusterRoleBindings no Kubernetes

# Lista de usuários e seus respectivos ClusterRoles
declare -A users_roles=(
    ["asilva_ext"]="cluster-admin"
    ["dmsilveira"]="cluster-admin"
    ["mprado"]="cluster-admin"
    ["vjose"]="cluster-admin"
    ["loliveira"]="view"
    ["smazolla"]="view"
)

# Criando os ClusterRoleBindings
for user in "${!users_roles[@]}"; do
    role="${users_roles[$user]}"
    binding_name="${role}-${user}"

    echo "Criando ClusterRoleBinding: $binding_name"
    kubectl create clusterrolebinding "$binding_name" --clusterrole="$role" --
    user="$user"
done
```

🔗 Referências

- 🔗 [Tanzu Kubernetes Grid 2.5](#)
- 🔗 [Install the Tanzu CLI and Kubernetes CLI](#)
- 🔗 [Prepare to Deploy Management Clusters to vSphere](#)

-  Deploying Standalone Management Clusters
 -  Managing Your Management Clusters
 -  Identity and Access Management
 -  Active Directory Configuration
 -  Tanzu Kubernetes Grid Networking
 -  Kube-VIP Load Balancer
 -  Managing Resource Pools with vSphere
 -  Deploy Management Clusters from a Configuration File
 -  Node IPAM
-

 Equipe responsável pela Documentação:

Autor(es)/Revisor(es)	Atividade(s)
Anderson Silva	Criação da Documentação / Revisão da Documentação
Carlos Papalardo	Criação da Documentação / Revisão da Documentação
Delson Lopes	Criação da Documentação / Revisão da Documentação