VMware Advanced Customer Engagements (ACE) Team

How-to Change User or Password for Tanzu Kubernetes Grid (TKG) on vSphere

July 2020

Table of Contents

Purpose

This document is a quick guide to change secrets in the TKG clusters in the below scenarios:

- The password of the vSphere user used to create the TKG clusters has changed
- A new user is setup and user needs to update in TKG clusters.

The document covers the following topics:

- Updating user password in vSphere
- Updating secrets in the management cluster
- Updating secrets in the workload clusters

Secrets and Credential information

When a TKG cluster is deployed, secrets are created in Kubernetes(K8s) that authenticates the cluster to the provider. There are three types of secrets that are created:

- capv-manager-bootstrap-credentials in the namespace capv-system (only in the management cluster)
- cloud-provider-vsphere-credentials in the kube-system namespace (in both the management and workload clusters)
- csi-vsphere-config in the kube-system namespace (in both the management and workload clusters)

The TKG cli uses the TKG config file to authenticate against the provider as well and requires to be updated apart from the secrets. The above secrets/credentials are described in the following sections.

Capv manager bootstrap

Cluster API bootstrap provider Kubeadm (CABPK) is a component of Cluster API that is responsible of generating a cloud-init script to turn a Machine into a Kubernetes Node; this implementation uses kubeadm for kubernetes bootstrap.

Cloud Provider vSphere Credentials

Kubernetes(K8s) Cloud Providers are an interface to integrate various node (i.e. hosts), load balancers and networking routes. This interface allows extending K8s to use various cloud and virtualization solutions as a base infrastructure to run on.

Kubernetes Cloud Providers provide the following interfaces to effectively integrate cloud platforms into Kubernetes:

- Instances - interface for virtual machine management
- Load Balancers - interface to integrate with load balancer provided by cloud platform
- Routes - interface to add new routing rules of cloud platform
- Zones - integrate with zones if implemented by cloud platform

CSI vSphere Config

Cloud Native Storage (CNS) provides comprehensive data management for stateful, containerized apps, enabling apps to survive restarts and outages. Stateful containers can use vSphere storage primitives such as standard volume, persistent volume, and dynamic provisioning, independent of VM and container lifecycle.

The vSphere Container Storage Interface (CSI) driver is what enables Kubernetes clusters running on vSphere to provision persistent volumes on vSphere storage. The CSI driver will utilize the secret in the kube-system namespace.

Assumptions

The following assumptions are made in this guide:

- TKG cluster, both management and workload clusters are created as user user@domain

Change User Password in vSphere

This section goes through an overview of updating the user password in vCenter for the user user@domain.

Permissions Required

The role that the user is assigned to requires the following permissions.

The required permission for the TKG Roles is:-

Datastore

- Allocate space
- Browse datastore
- Low level file operations

Network

- Assign network

Resource

- Assign virtual machine to resource pool

Sessions

- Message
- Validate session

Profile-driven storage

- Profile-driven storage view

vApp

- Import

Virtual machine

Configuration

- Change Configuration
- Add existing disk
- 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
- Create from existing
- Remove

Interaction >

- Power off
- Power on

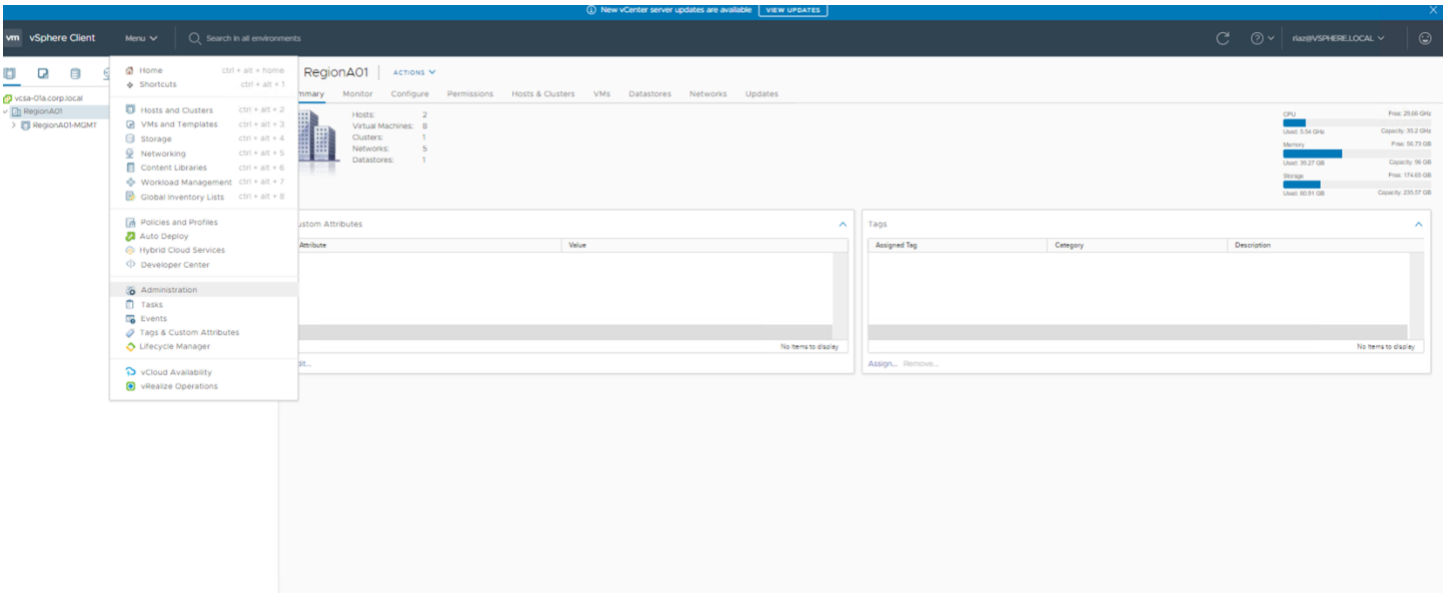
Provisioning >

- Deploy template

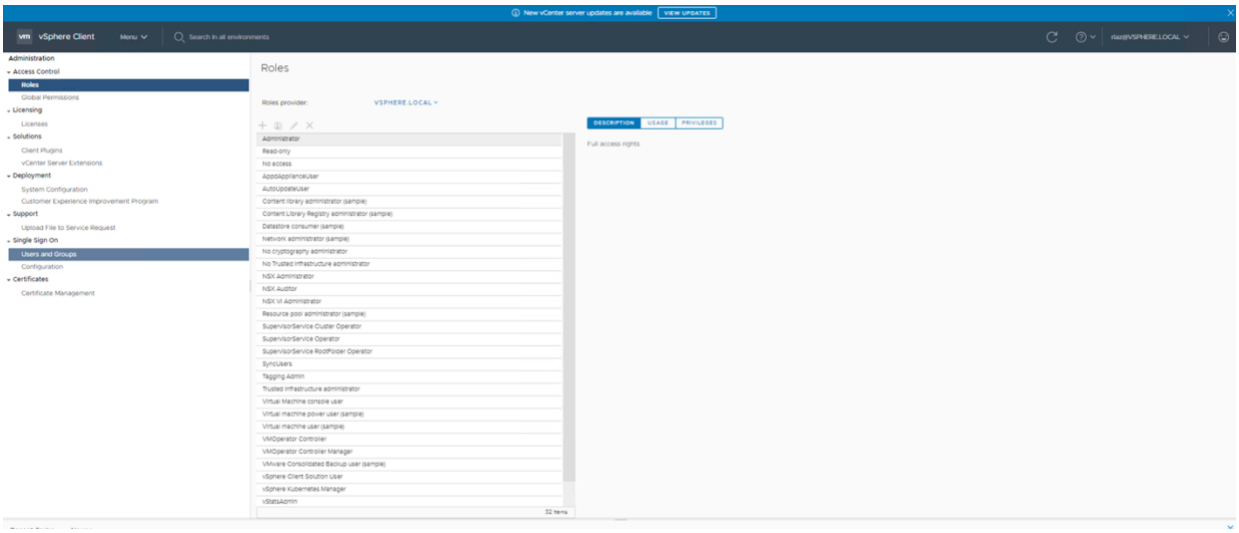
The objects that we need to assign the user with the TKG role are:

- The deployed TKG OVF templates
- The vCenter
- Datacenters or datacenter folders
- Datastores or datastore folders
- Hosts and clusters
- TKG resource pools (With Propagate to children)
- Networks to which clusters will be assigned >>> In my case it was the "DSwitch-Management" Distributed Port Group.
- The Distributed Switch
- The TKG VM and Template folders (With Propagate to children)

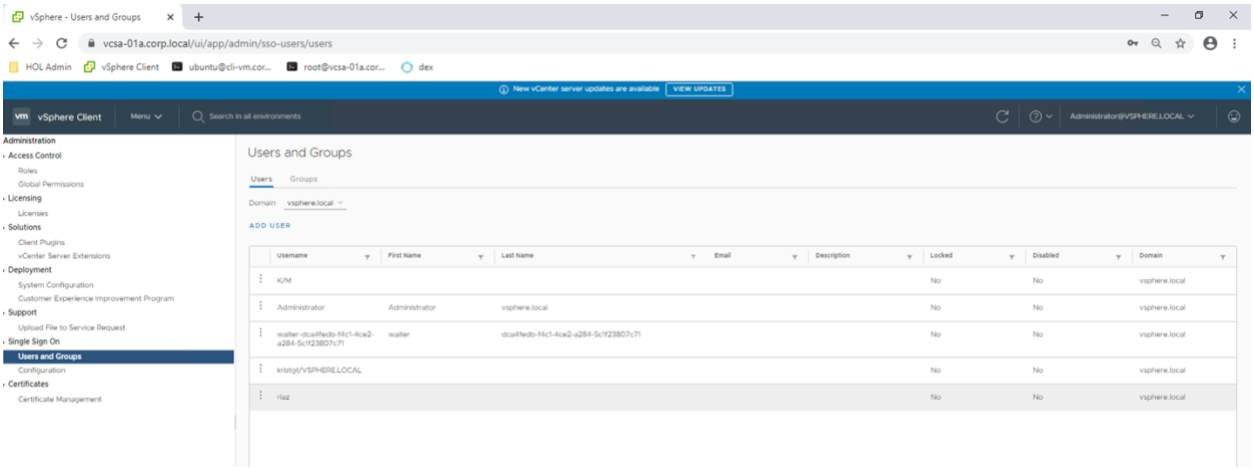
Step 1: Login to vCenter and from the menu select Administration



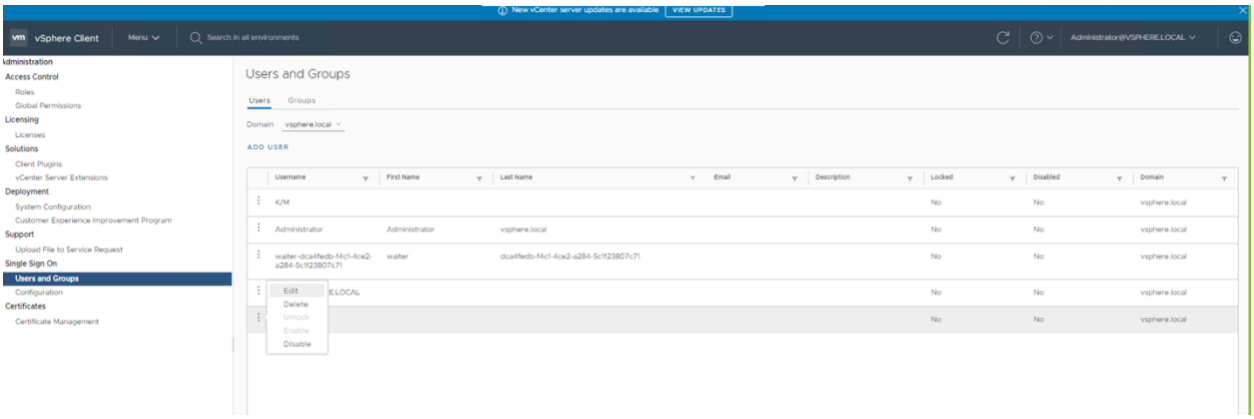
Step 2: Select Users and Groups



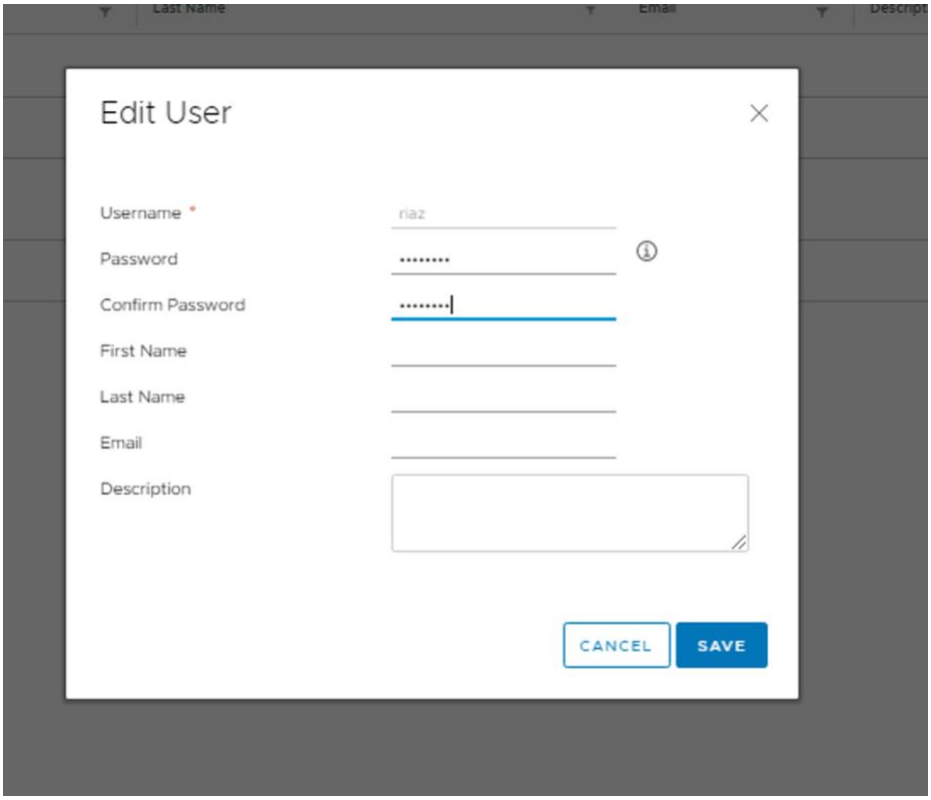
Step 3: Select the domain



Step 4: Click on the 3 dots and click on edit

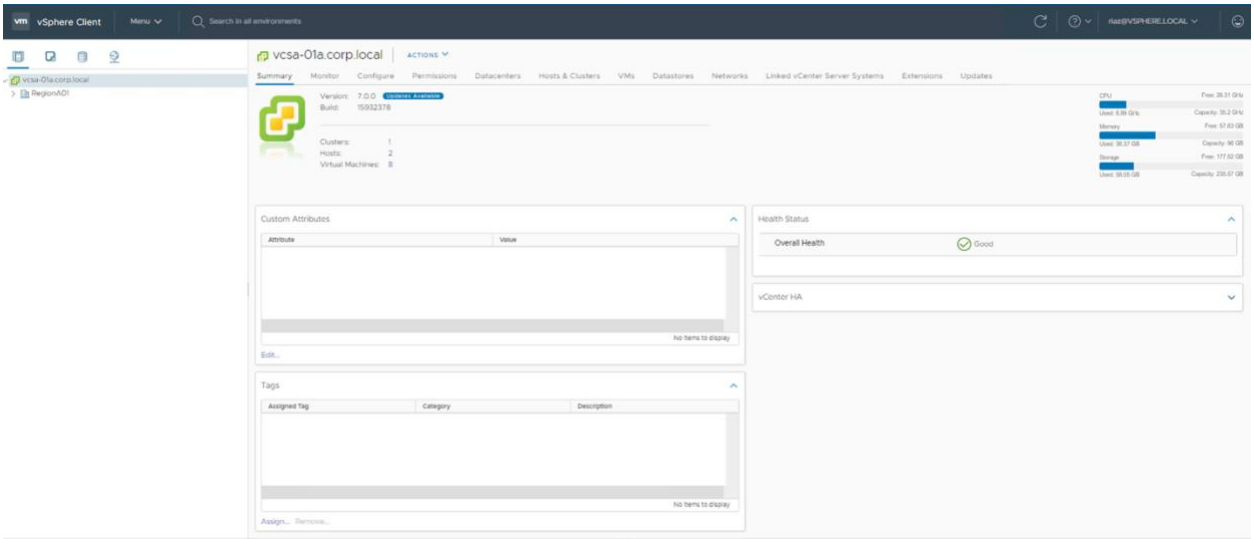


Step 5: Change the password E.g. VMware4!



Step 6: Log out and login to the vCenter as the user and the new password

Step 7: Make sure the login works as expected



Step 8: Verify that the user has the roles defined above.

Update TKG clusters

This section goes through the steps to update the credentials on the TKG clusters.

TKG Config

Step 1: Encode the new password to base64

https://www.base64encode.org/

E.g. VMware4! translates to Vk13YXJlNCE=

Step 2 : Change the password in the tkg config file

cd ~/.tkg

Open the config.yaml file and change the value of the VSPHERE_PASSWORD with the new password from above.

If the user needs to be changed VSPHERE_USERNAME and the corresponding password needs to be edited.

```
VSPHERE_USERNAME: riaz@vsphere.local
VSPHERE_FOLDER: /RegionA01/vm/TKG
VSPHERE_NUM_CPUS: "1"
SERVICE_CIDR: 100.64.0.0/13
VSPHERE_SERVER: vcsa-01a.corp.local
VSPHERE_DATACENTER: /RegionA01
VSPHERE_DATASTORE: /RegionA01/datastore/map-vol
VSPHERE_RESOURCE_POOL: /RegionA01/host/RegionA01-MGMT/Resources/TKG-Pool
VSPHERE_MEM_MIB: "2028"
VSPHERE_HAPROXY_TEMPLATE: /RegionA01/vm/TKG/photon-3-haproxy-v1.2.4+vmware.1
# VSPHERE_TEMPLATE will be autodetected based on the kubernetes version. Please use VSPHERE_TEMPLATE only to override this behavior
VSPHERE_TEMPLATE: /RegionA01/vm/TKG/photon-3-kube-v1.17.3+vmware.2
CLUSTER_CIDR: 100.96.0.0/11
VSPHERE_PASSWORD: <encoded:Vk13YXJlNCE=>
VSPHERE_NETWORK: DSwitch-Management
VSPHERE_DISK_GIB: "20"
VSPHERE_SSH_AUTHORIZED_KEY: ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCVuwsAoJmYBtGbGalvm2AYTo/MQfAN0J5DbNtilZ4dh+iwq6shYC91T7DsXaIR1Bssf844iSc
ljrS0viiUcUrOO8ZPd5Z9+xo/Ch19FxVBX+XiJ15P0I7bSrlJEdSZu8IS5o3Nkhv/aIe6dASH3HfP8JP9mR+yyvrko+cDnUfJ7q6H5eye28sf5W5YGOYz/0Wk7YnWkwH8DJQQ7Gz1PN
alN9yYhW3KOvSn/1lvYwA62o4VyZZGyfzRMCcGbcP4YOHL5iSIy6GzDh6aMFmJ3miDa//N4XfidtJXjEFlXAgokTCxVbv5M9woYYZBtFUHLEuEeD3vUjGaW3YRvSzO/Lsgr8YwG3x0c
SZ5HZJ7wb4T8oIk+wKrUOTPE/6oIS63UnfpGtgSb7fzDTeUjfMnZzlFpNECtF+CPZr/8eB4077Mpmy2C35REnsadt9EWH8F1OBm+ES+4wQqibWPMmZfKuwoygT0mXgNL+I/I3zDutuI
iLk0AsLZJCM+5w==
tkg:
    regions:
      - name: tkg-mgmt-vsphere-20200721110152
        context: tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152
        file: /home/ubuntu/.kube/config
    current-region-context: tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152
cert-manager-timeout: 30m0s
NODE_STARTUP_TIMEOUT: 20m
release:
    version: v1.1.2
BASTION_HOST_ENABLED: "true"
```

Management Cluster

The management cluster contains three secrets that needs to be updated with the new password:

- capv-manager-bootstrap-credentials in the namespace capv-system
- cloud-provider-vsphere-credentials in the kube-system namespace
- csi-vsphere-config in the kube-system namespace

Step 1: Get all tkg clusters

```
tkg get cluster --include-management-cluster
```

```
ubuntu@cli-vm:~/tkgpwd$ tkg get cluster --include-management-cluster
 NAME                            NAMESPACE   STATUS   CONTROLPLANE  WORKERS  KUBERNETES
 riaz-workload                   default     running  1/1           1/1      v1.17.3+vmware.2
 tkg-mgmt-vsphere-20200721110152 tkg-system  running  1/1           1/1      v1.17.3+vmware.2
```

NOTE: The versions of k8 is v1.17.3

Step 2: Get the management cluster

tkg get mc

```
ubuntu@cli-vm:~$ tkg get mc
 MANAGEMENT-CLUSTER-NAME          CONTEXT-NAME
 tkg-mgmt-vsphere-20200721110152 *  tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152
```

Step 3: Set the management context

tkg set mc <management-cluster-name>

E.g. tkg set mc tkg-mgmt-vsphere-20200721110152

```
ubuntu@cli-vm:~$ tkg set mc tkg-mgmt-vsphere-20200721110152
The current management cluster context is switched to tkg-mgmt-vsphere-20200721110152
```

Step 3: Use the kubectl context to the management cluser

kubectl config get-contexts

```
ubuntu@cli-vm:~$ kubectl config get-contexts
CURRENT   NAME                                                    CLUSTER                     AUTHINFO                          NAMESPACE
*         riaz-workload-admin@riaz-workload                       riaz-workload               riaz-workload-admin
          tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152   tkg-mgmt-vsphere-20200721110152   tkg-mgmt-vsphere-20200721110152-admin
```

kubectl config use-context tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152

```
ubuntu@cli-vm:~$ kubectl config set-context tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152
Context "tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152" modified.
ubuntu@cli-vm:~$ kubectl config use-context tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152
Switched to context "tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152".
```

Step 4: Check for namespaces in the management cluster

kubectl get ns

```
ubuntu@cli-vm:~$ kubectl get ns
NAME                                STATUS   AGE
capi-kubeadm-bootstrap-system       Active   86m
capi-kubeadm-control-plane-system   Active   86m
capi-system                         Active   86m
capi-webhook-system                 Active   87m
capv-system                         Active   86m
cert-manager                        Active   94m
default                             Active   95m
kube-node-lease                     Active   95m
kube-public                         Active   95m
kube-system                         Active   95m
tkg-system                          Active   86m
```

NOTE: The management cluster contains the capi* and the cap* namespaces

Bootstrap

Step 5: The capv-system namespace contains the capv-manager-bootstrap-credentials secret which is used to bootstrap the workload clusters

kubectl get secrets -n capv-system

```
ubuntu@cli-vm:~$ kubectl get secrets -n capv-system
NAME                                  TYPE                                  DATA   AGE
capv-manager-bootstrap-credentials    Opaque                                1      87m
default-token-jc9zg                   kubernetes.io/service-account-token   3      87m
```

kubectl describe secret capv-manager-bootstrap-credentials -n capv-system

```
ubuntu@cli-vm:~$ kubectl describe secret capv-manager-bootstrap-credentials -n capv-system
Name:         capv-manager-bootstrap-credentials
Namespace:    capv-system
Labels:       cluster.x-k8s.io/provider=infrastructure-vsphere
              clusterctl.cluster.x-k8s.io=
Annotations:  <none>

Type:  Opaque

Data
====
credentials.yaml:  53 bytes
```

Note: The data references the credentials.yaml file

Step 6: View contents of the credentials.yaml file

kubectl -n capv-system get secret capv-manager-bootstrap-credentials -o jsonpath="{.data.credentials\.yaml}" | base64 -d

```
ubuntu@cli-vm:~$ kubectl -n capv-system get secret capv-manager-bootstrap-credentials -o jsonpath="{.data.credentials\.yaml}" | base64 -d
username: 'riaz@vsphere.local'
password: 'VMware123!'ubuntu@cli-vm:~$
```

Step 7: Copy the contents to a file locally and name its credentials.yaml

kubectl -n capv-system get secret capv-manager-bootstrap-credentials -o jsonpath="{.data.credentials\.yaml}" | base64 -d > credentials.yaml

Note the ' on the values

Step 8: Change the password to the updated password

username: 'riaz@vsphere.local'

password: 'VMware4!'

NOTE: If the user needs to be changed update the file with the username and the corresponding password

Step 9: Delete the capv-manager-bootstrap-credentials secret

kubectl delete secret capv-manager-bootstrap-credentials -n capv-system

```
ubuntu@cli-vm:~/tkgpwd$ kubectl delete secret capv-manager-bootstrap-credentials -n capv-system
secret "capv-manager-bootstrap-credentials" deleted
```

Step 10: Create the capv-manager-bootstrap-credentials secret with the updated credentials file

kubectl -n capv-system create secret generic capv-manager-bootstrap-credentials --from-file=credentials.yaml

Step 11: Verify that the newly created secret contains the right credentials

kubectl -n capv-system get secret capv-manager-bootstrap-credentials -o jsonpath="{.data.credentials\.yaml}" | base64 -d

```
ubuntu@cli-vm:~/tkgpwd$ kubectl -n capv-system get secret capv-manager-bootstrap-credentials -o jsonpath="{.data.credentials\.yaml}" | base64 -d
username: 'riaz@vsphere.local'
password: 'VMware4!'ubuntu@cli-vm:~/tkgpwd$
```

NOTE: The password field reflects the correct password

Cloud Provider

Step 12: The kube-system namespace contains the cloud provider secret, which is used to authenticate against vCenter

kubectl get secret cloud-provider-vsphere-credentials -o yaml -n kube-system

```
ubuntu@cli-vm:~/tkgpwd$ kubectl get secret cloud-provider-vsphere-credentials -o yaml -n kube-system
apiVersion: v1
data:
  vcsa-01a.corp.local.password: Vk13YXJlMTIzIQ==
  vcsa-01a.corp.local.username: cmlhekB2c3BoZXJlLmxvY2Fs
kind: Secret
metadata:
  creationTimestamp: "2020-07-21T18:20:15Z"
  name: cloud-provider-vsphere-credentials
  namespace: kube-system
  resourceVersion: "162"
  selfLink: /api/v1/namespaces/kube-system/secrets/cloud-provider-vsphere-credentials
  uid: be2c8ca6-fe2a-4503-892e-2ebef54f0eb2
type: Opaque
```

NOTE: The password is base 64 encoded

To decode the password in unix use the command echo <password> | base64 -d

Step 13: Encode the new password to base64

https://www.base64encode.org/

E.g. VMware4! translates to Vk13YXJlNCE=

NOTE: If the user needs to be changed the username needs to be encoded along with the corresponding password.

Step 14: Update the password for the cloud provider secret

```
kubectl edit secret cloud-provider-vsphere-credentials -n kube-system
```

Update the password to the one generated in the step above

NOTE: If the user needs to be changed the username needs to be update the username as well.

Step 15: Make sure that the password reflects the new base 64 encoded format

```
kubectl get secret cloud-provider-vsphere-credentials -n kube-system -o yaml
```

Storage Interface

Step 16: The kube-system namespace contains the storage interface secret, which is used to authenticate against vCenter to provision storage for PV's

kubectl -n kube-system describe secret csi-vsphere-config

```
ubuntu@cli-vm:~/tkgpwd$ kubectl -n kube-system get secret csi-vsphere-config
NAME                  TYPE     DATA   AGE
csi-vsphere-config    Opaque   1      5h22m
ubuntu@cli-vm:~/tkgpwd$ kubectl -n kube-system describe secret csi-vsphere-config
Name:         csi-vsphere-config
Namespace:    kube-system
Labels:       <none>
Annotations:  <none>

Type:  Opaque

Data
====
csi-vsphere.conf:  254 bytes
```

NOTE: The secret references csi-vsphere.conf

Step 16: The kube-system namespace contains the storage interface secret, which is used to authenticate against vCenter to provision storage for PV's.

kubectl -n kube-system get secret csi-vsphere-config -o jsonpath="{.data.csi-vsphere\.conf}" | base64 -d

```
ubuntu@cli-vm:~/tkgpwd$ kubectl -n kube-system get secret csi-vsphere-config -o jsonpath="{.data.csi-vsphere\.conf}" | base64 -d
[Global]
insecure-flag = true
cluster-id = tkg-system/tkg-mgmt-vsphere-20200721110152

[VirtualCenter "vcsa-01a.corp.local"]
user = riaz@vsphere.local
password = VMware123!
datacenters = /RegionA01

[Network]
public-network = DSwitch-Management
```

Step 17: Save the contents of the file to csi-vsphere.conf

kubectl -n kube-system get secret csi-vsphere-config -o jsonpath="{.data.csi-vsphere\.conf}" | base64 -d > csi-vsphere.conf

Step 17: Edit the contents of csi-vsphere.conf and change the password to the new password

e.g.

[Global]

insecure-flag = true

cluster-id = "tkg-system/tkg-mgmt-vsphere-20200721110152"

[VirtualCenter "vcsa-01a.corp.local"]

user = "riaz@vsphere.local"

password = "VMware4!"

datacenters = "/RegionA01"

[Network]

public-network = "DSwitch-Management"

NOTE: If the user needs to be changed the username needs to be updated along with the corresponding password

Step 18: Delete the existing csi-vsphere-config secret

```
kubectl delete secret csi-vsphere-config -n kube-system
```

```
ubuntu@cli-vm:~/tkgpwd$ kubectl delete secret csi-vsphere-config -n kube-system
secret "csi-vsphere-config" deleted
```

Step 19: Create the csi-vsphere-config in the kube-system namespace from the updated csi-vsphere.conf file

kubectl -n kube-system create secret generic csi-vsphere-config --from-file=csi-vsphere.conf

```
ubuntu@cli-vm:~/tkgpwd$ kubectl -n kube-system create secret generic csi-vsphere-config --from-file=csi-vsphere.conf
secret/csi-vsphere-config created
```

Workload Cluster

The workload cluster contains two secrets that needs to be updated with the new password:

- cloud-provider-vsphere-credentials in the kube-system namespace
- csi-vsphere-config in the kube-system namespace

Step 1: Change the context to reference the workload cluster

kubectl config get-contexts

```
ubuntu@cli-vm:~/tkgpwd$ kubectl config get-contexts
CURRENT   NAME                                                    CLUSTER                     AUTHINFO                                  NAMESPACE
          riaz-workload-admin@riaz-workload                       riaz-workload               riaz-workload-admin
*         tkg-mgmt-vsphere-20200721110152-admin@tkg-mgmt-vsphere-20200721110152   tkg-mgmt-vsphere-20200721110152   tkg-mgmt-vsphere-20200721110152-admin
```

kubectl config use-context riaz-workload-admin@riaz-workload

```
ubuntu@cli-vm:~/tkgpwd$ kubectl config use-context  riaz-workload-admin@riaz-workload
Switched to context "riaz-workload-admin@riaz-workload".
```

kubectl get ns

```
ubuntu@cli-vm:~/tkgpwd$ kubectl get ns
NAME              STATUS   AGE
default           Active   91m
kube-node-lease   Active   91m
kube-public       Active   91m
kube-system       Active   91m
```

NOTE: cap* namespaces do not exist

Step 2: Follow steps 12 to 19 from the Management Cluster steps

Conclusion

We hope this document was useful. As you try these configuration steps, please provide any feedback or questions in the comments section for this document on code.vmware.com. Also, do let us know if you have any suggestions or if you would like to see guidance on other topics.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.