

PKS Enterprise and Pure Storage Deployment Guide

Jon Owings
Principal Solutions Architect
Pure Storage



Summary

Getting Started and Architectural Guide to using PKS Enterprise with Pure Storage. PKS provides an Enterprise Platform as a Service for deploying and managing Kubernetes Clusters at scale for Private and Public Cloud Solutions. This paper will walk through the configuration of PKS Enterprise on VMware vSphere using multiple Availability Zones and Highly Available Pure Storage FlashArray for Persistent Storage.

Introduction

Deploying Platform as a Service - PaaS enables developers to deliver applications to the business with consistency in the underlying Infrastructure and Platform. PKS Enterprise is delivering orchestration for containers using Kubernetes delivered with the familiar Enterprise PaaS tools used for Pivotal Cloud Foundry, allowing applications to now scale and be managed by Kubernetes. This enables them to run along side CF and enhance workflows and applications with Deployments, Stateful Sets, Daemon Sets and beyond. In most Enterprises, Pivotal will leverage VMware vSphere as the underlying Infrastructure as a Service - IaaS. In this reference guide, we will deploy Pivotal Ops Manager connected to VMware vCenter. There are other options to manage other Private and Public Clouds. Using Ops Manager we will deploy PKS Enterprise.

PKS Enterprise and Pure Storage

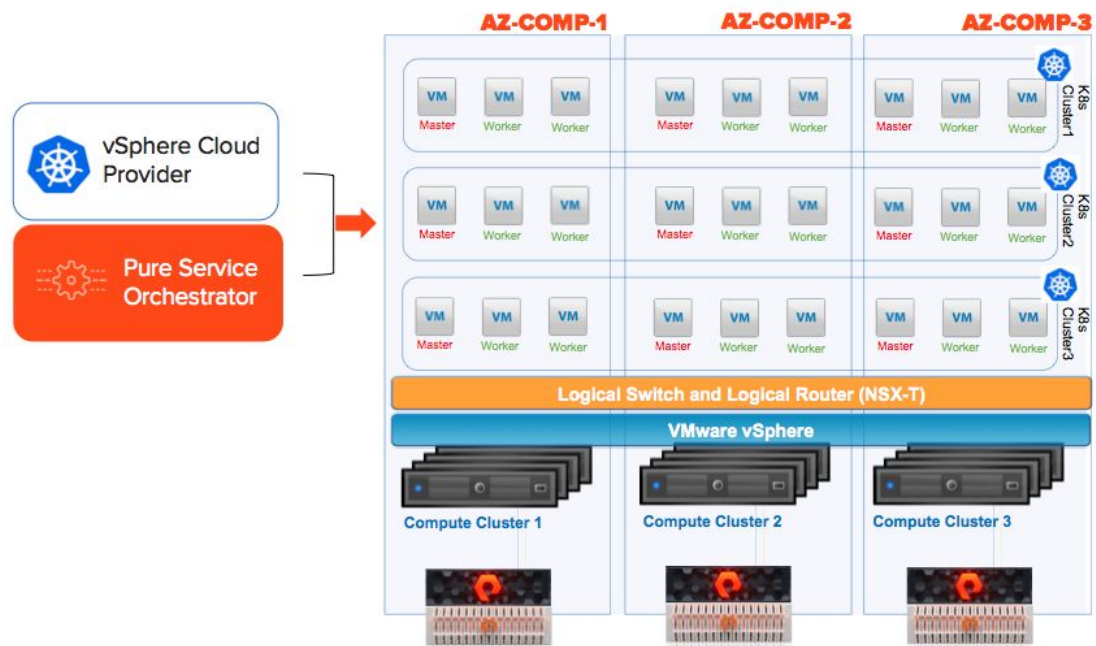
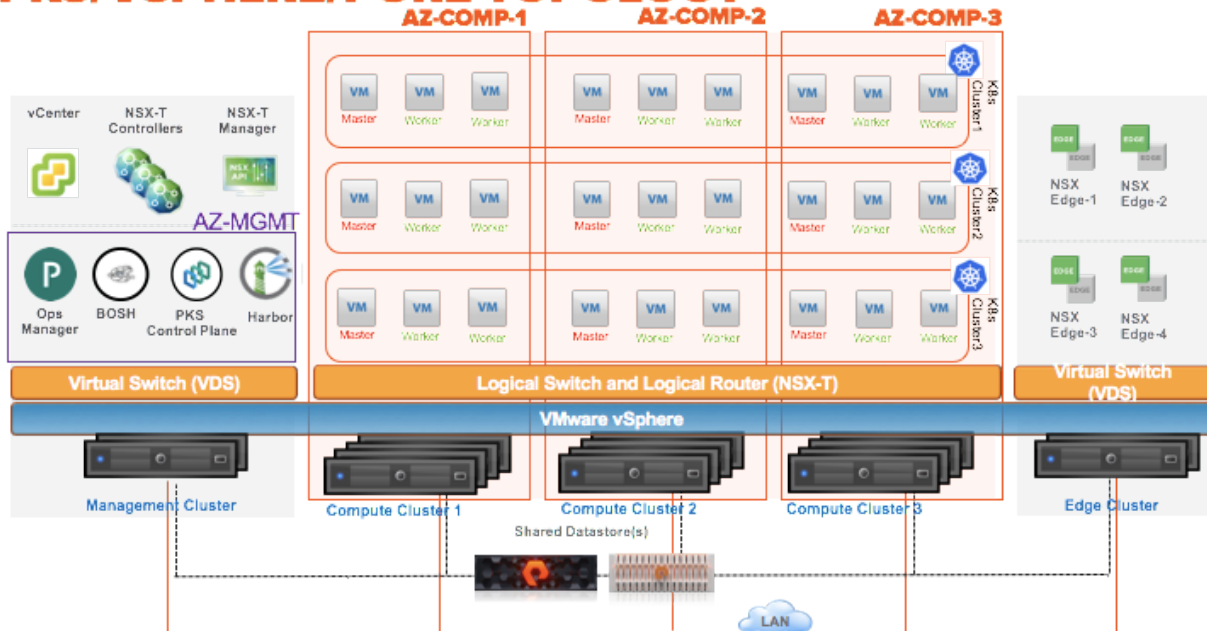
The benefit of running PKS and Pure Storage is customers can use existing vSphere environments or deploy a converged stack that is able to support both legacy VM workloads or new applications developed for the cloud to use PKS. Top reasons include:

1. Disaggregated Scale. Scale Compute, Network and Storage independently the same way modern Cloud and SaaS providers.
2. Better overall TCO. Stateless compute, storage and Applications allow that allow for a cloud consumption model that is never EOL, has zero tech refresh cycles. Highest levels of flexibility and the lowest operating costs.
3. Manage a single domain. Do not build siloed environments.

Pivotal Container Services (PKS)

High-Level Design

PKS/VSPHERE/PURE TOPOLOGY



Software	Version
Ops Manager	2.6.9
VMware vSphere ESXi	6.7 (13006603)
VMware vSphere vCenter	6.7 (13639324)
Pivotal Container Services (PKS)	1.4.1-build.4*+
Purity//FA	5.1.10
Purity//FB	2.4.1
Pivotal Stemcell	Ubuntu-xenial 250.63
Bosh Director for vSphere	2.5.7-build.208*
VMware Harbor Registry	1.8.2-build.6
Pks cli	1.5.0-build.291
Bosh cli	6.0.0-5240e8aa-2019-08-05T22:16:39Z
NSX-T	2.4.2

VMware vSphere Configuration

The configuration of vSphere and NSX-T should follow the guidelines listed in the PKS Enterprise documentation.

Networking and NSX-T

NSX-T provides the virtual network constructs to allow PKS Enterprise to scale. The key benefits of PKS + NSX-T is the ability to provide customers a packaged turnkey solution that includes advanced container networking, micro-segmentation, ingress controller, load balancing, and security policy. Make sure it is configured by the instructions from Pivotal for your

version of PKS. Make sure to enable networking pathing for iSCSI FlashArray and/or NFS for FlashBlade.

<https://docs.pivotal.io/pks/1-4/vsphere-nsxt-requirements.html>

Additionally, this blog from VMware covers the network topologies and their interaction from NSX-T and PKS.

<https://blogs.vmware.com/networkvirtualization/2019/06/kubernetes-and-vmware-enterprise-pks-networking-security-operations-with-nsx-t-data-center.html/>

DRS/HA Clusters

This architecture uses a single HA/DRS Cluster and Resource Pool for each Availability Zone.

Create a cluster in your vSphere environment. Configured according to the PKS Enterprise Documentation.

Create the PKS Management Plane

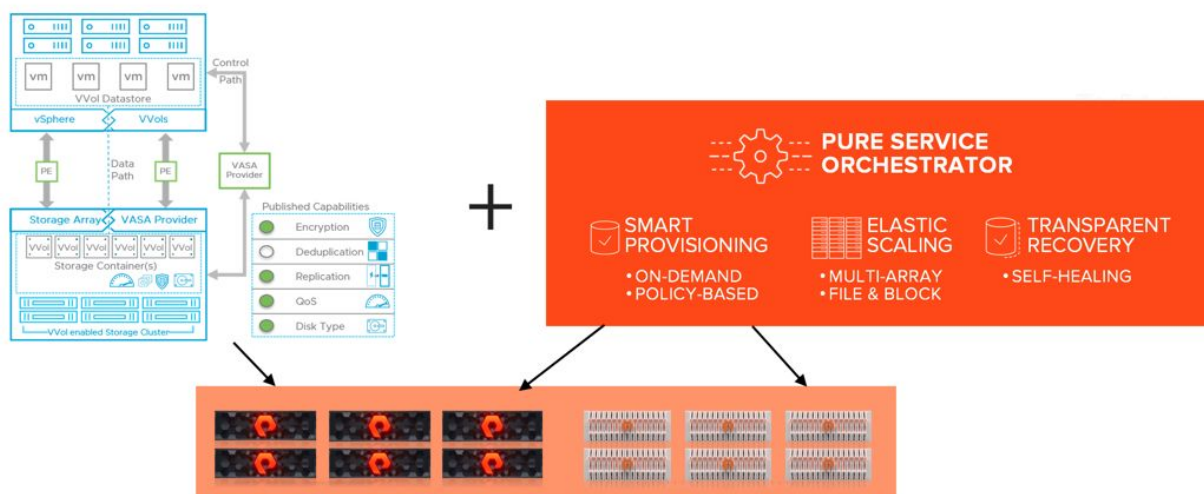
<https://docs.pivotal.io/pks/1-4/nsxt-prepare-mgmt-plane.html>

Create the PKS Compute Plane

<https://docs.pivotal.io/pks/1-4/nsxt-prepare-compute-plane.html>

Shared Storage

Shared storage using Storage Policy Based Management and Pure Service Orchestrator allows for workloads requiring Persistent Data to be accessible on all compute nodes in all availability zones.



A FlashArray and Flashblade will provide the resiliency and performance required for applications to scale for production workloads with no additional management trade-offs or overhead.

Using the vSphere Cloud Provider for Cloud Native Storage with Pure Storage FlashArray vVOs enables data mobility from Virtual Machines to Containers and to the Public Cloud. It allows for instant movement from 'other' container platforms and even cloning data between PKS Clusters. PKS clusters are no longer an island of persistent data enabling software developers to quickly and easily move applications from test environments to production and have consistent underlying persistent data.

Client Configuration

The management and configuration of PKS requires a few CLI tools. These tools are available for Linux, Mac OS and Windows.

Great article explaining all of the options. We will need the Bosh, Kubectl, UAAC Client, OM CLI and PKS CLI for this guide. The following website is a great collection and explanation of each.

<https://www.virtuallyghetto.com/2018/03/getting-started-with-vmware-pivotal-container-service-pks-part-2-pks-client.html>

Configuration of OpsManager and BOSH Director

Deploy OVA for Ops Manager in MGT Cluster or Resource Pool. This requires importing the Operations Manager OVA downloaded from

<https://network.pivotal.io>

Choose your Auth method. Using Internal for Setup Guide as LDAP or OAUTH outside this scope.

Once logged into your Ops Manager Instance you should see the following screen.



IMPORT A PRODUCT

Installation Dashboard

vmware®

BOSH Director
for vSphere

v2.5.2-build.172



Configure the BOSH director tile.

First setup the vCenter that Managers your PKS Enterprise Cluster. The Datacenter name is required and case sensitive.

BOSH Director for vSphere

Settings | Status | Credentials

vCenter Config

☐ vCenter Config

☐ Director Config

☐ Create Availability Zones

☐ Create Networks

☐ Assign AZs and Networks

☒ Security

☒ BOSH DNS Config

☒ Syslog

☒ Resource Config

vCenter Config

Name*

vCenter Host*

vCenter Username*

vCenter Password*
 The password

Datacenter Name*

Virtual Disk Type*

Additionally, add a datastore for your Persistent and Ephemeral Data.

Datacenter Name*

Virtual Disk Type*

Virtual Disk Type to provision for all VMs.

Ephemeral Datastore Names (comma delimited)*

NOTE: Removing an Ephemeral Datastore after an initial deploy can result in a system outage and/or data loss.

Persistent Datastore Names (comma delimited)*

NOTE: Removing a Persistent Datastore after an initial deploy can result in a system outage and/or data loss.

Last supply the details for your NSX environment. Be sure the networking and certificates are setup to match the PKS Enterprise for NSX-T documentation.

NOTE: Removing a Persistent Datastore after an initial deploy can result in a system outage and/or data loss.

☒ Standard vCenter Networking
☐ NSX Networking

NSX Mode*

☐ NSX-V
☒ NSX-T

NSX Address*

10.21.142.30

NSX Username*

admin

NSX Password*

[Change](#)

NSX CA Cert

```
-----BEGIN CERTIFICATE-----
MIIDSDCAJCgAwIBAgIJAPJ04pY48q+fMA0GCSqGSIb3DQEBCwUAMFlixCzAJBgNV
BAYTAiVMTMRawDgYDVQQIDAdHZW9yZ2lhmQswCQYDVQQHDAJHQTEmMAoGA1UECgw
D
TINYMRYwFAYDVQQDDA0xMC4yMS4xNDMuMTQxMB4XDTE5MTAyMTAzMTkyMVoXDTEw
MTAyMTAzMTkyMBoKCFMAAGCAUUECDkMCBAUMFCDAGDw44BDAAMQDQ44k3JmXUEwCg
I=
```

Set the NTP and other settings as needed. For PKS not much needs to be

changed.

The screenshot shows the 'BOSH Director for vSphere' interface. At the top, there are three tabs: 'Settings' (selected), 'Status', and 'Credentials'. Below the tabs is a list of configuration sections, each with a green checkmark icon: 'vCenter Config', 'Director Config' (highlighted with a grey arrow), 'Create Availability Zones', 'Create Networks', 'Assign AZs and Networks', 'Security', 'BOSH DNS Config', 'Syslog', and 'Resource Config'. The 'Director Config' section is expanded, showing the following fields and options:

- Director Config**
- NTP Servers (comma delimited)***: A text input field containing '10.21.230.6'. To the right, a note says 'One or more NTP server addresses for consistent and valid time'.
- JMX Provider IP Address**: An empty text input field.
- Bosh HM Forwarder IP Address**: An empty text input field.
- ☐ Enable VM Resurrecter Plugin
- ☒ Enable Post Deploy Scripts
- ☐ Recreate All VMs

PKS requires clicking Enable Post Deploy Scripts. The PKS documentation also recommends enabling the VM Resurrecter Plugin and Clicking the Recreate All VMs checkbox.

Note about the Director VM:

Additionally, If you are using NSX-T in NAT mode. You will most likely need to access the director VM via bosh for troubleshooting if anything ever goes wrong. You should set the Director Hostname to the DNS record for the NAT routable IP in your Network.

Director Workers

5

Max Threads

Director Hostname

Custom SSH Banner

Don't do this unless you are the admin

A login banner displayed when SSHing to the BOSH Director

Identification Tags

Save

If you do not do this, the SSL certificate will be issued to the internal IP and connecting to the hostname on the outside network will fail.

Optional: Blob Store

You are able to use an S3 bucket on FlashBlade to house the Bosh Blobstore. The endpoint, bucket name and keys are required to configure the blobstore.

☒ Enable TLS

☒ S3 Compatible Blobstore

S3 Endpoint*

Bucket Name*

Access Key*

Secret Key*

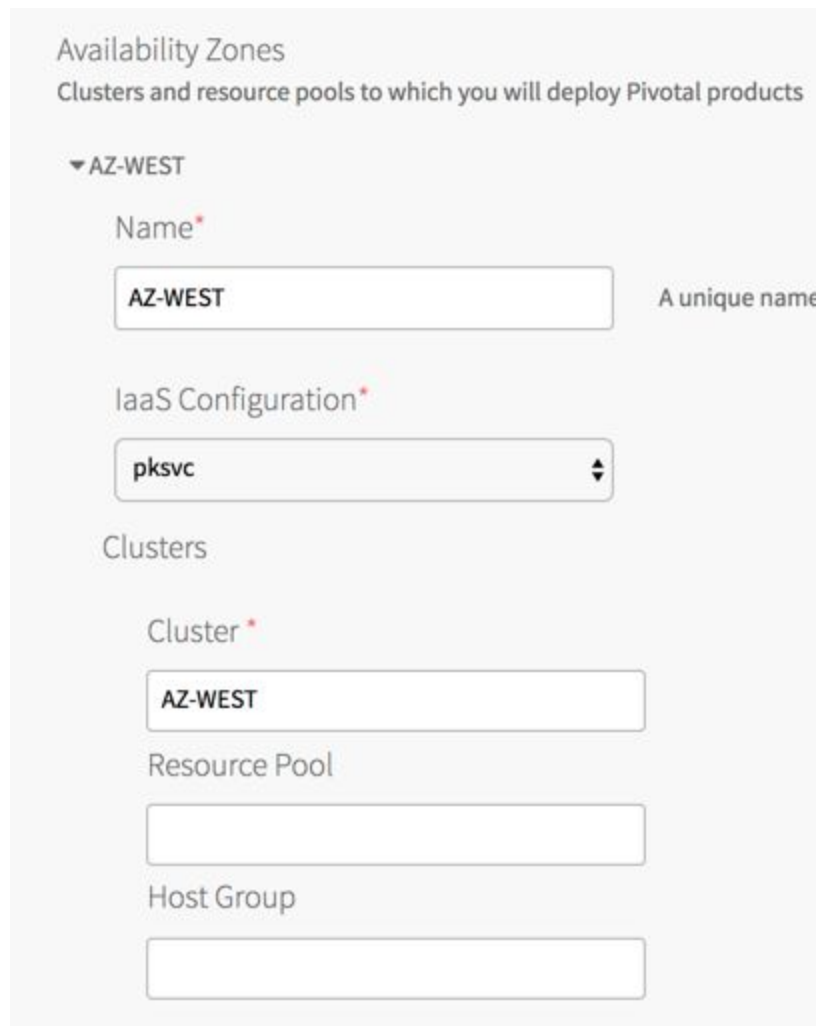
☒ V2 Signature

☐ V4 Signature

Create Availability Zones

Set the Availability Zones Create 1 for each vSphere Cluster or resource pool depending on your vSphere Setup.

Our example uses 3 Compute zones and 1 Management Zone.



The screenshot shows a configuration page titled "Availability Zones" with the subtitle "Clusters and resource pools to which you will deploy Pivotal products". A dropdown menu is set to "AZ-WEST". Below this, there are three main sections: "Name", "IaaS Configuration", and "Clusters". The "Name" section has a text input field containing "AZ-WEST" and a note "A unique name". The "IaaS Configuration" section has a dropdown menu set to "pksvc". The "Clusters" section contains three stacked text input fields: the first is labeled "Cluster" and contains "AZ-WEST", the second is labeled "Resource Pool" and is empty, and the third is labeled "Host Group" and is empty.

Availability Zones
Clusters and resource pools to which you will deploy Pivotal products

▼ AZ-WEST

Name*

AZ-WEST A unique name

IaaS Configuration*

pksvc

Clusters

Cluster *

AZ-WEST

Resource Pool

Host Group

Setup your networks as necessary. Please visit [Pivotal documentation](#) for NSX-T setup .

One or many IP ranges upon which your products will be deployed

▼ pks-net1

Name*

pks-net1

Subnets*

vSphere Network Name*

VM

The name of the network is the name of the vSphere network, the name of the network folder, or the name of the network switch.

CIDR*

10.21.230.0/24

Reserved IP Ranges*

10.21.230.1-10.21.230.130,10.21.230.210-10.21.230.254

DNS*

10.21.230.6,10.21.230.7

Gateway*

10.21.230.1

Assign where the Bosh Director will be deployed. In the Management zone.

Assign AZs and Networks

The BOSH Director is a single instance.

Choose the availability zone in which to place that instance. It is high

Singleton Availability Zone

MGT

Network

pks-net1

Save

Optional: Increase the VM size for the Bosh VM's as needed. My settings:

Resource Config

JOB	INSTANCES	PERSISTENT DISK TYPE	VM TYPE
BOSH Director	Automatic: 1	Automatic: 50 GB	xlarge.disk (cpu: 4, ram: 16 GB, disk: 128 GB)
Master Compilation Job	Automatic: 4	None	xlarge.cpu (cpu: 8, ram: 8 GB, disk: 32 GB)

Save

1. Initiate the setup of BOSH Director by going to:
 - a. Click the **Installation Dashboard** link to return to the Installation Dashboard.
 - b. Review Pending Changes

☒ Select All Products

☒

BOSH Director
Version 2.5.7-build.208

Staged
[SEE CHANGES](#)

Depends on
No Dependencies

APPLY CHANGES

- c. Apply Changes

Enterprise PKS Setup (PKS)

PKS Enterprise Configuration

Upload the PKS Package Downloaded from Pivotal and Install PKS

1. Import **Pivotal-container-service-1.4.1-build.4.pivotal**
2. Import the stemcell - **Ubuntu-Xenial 250.63** (current version as of writing this, make sure you use the stem required by your PKS Enterprise version) **Update:** the required stem is now included in the PKS package from step 1. If you don't see the stemcell you can manually import one. This can be downloaded from Pivotal's download website.
3. API Endpoint.
 - a. Click Generate Certificate then enter in your wildcard domain (*.newstack.local and *.app.newstack.local) hit Generate. For more on PKS and certificates please see the PKS Documentation. Use your Certificate Authority to sign the Certificate, this should be default practice for production.
 - b. Enter the FQDN of you PKS API endpoint.
(pks.app.newstack.local)
4. Plan 1-n.

No matter how many plans you may require. We will spread the load across the Availability Zones we Created with our vSphere Clusters. Plan 1, maybe a lightweight dev cluster 1 master and 3 workers. Set the Worker and Master Type VM's to fit your requirements.

Master Persistent Disk Type*

Automatic: 10 GB

Master/ETCD Availability Zones *

☒ AZ-WEST *

☒ AZ-EAST *

☒ AZ-SOUTH *

☐ MGT *

Maximum number of workers on a cluster (min: 1) *

50

Worker Node Instances (min: 1) *

3

Worker VM Type*

Automatic: medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB)

Worker Persistent Disk Type*

Automatic: 50 GB

Worker Availability Zones *

☒ AZ-WEST *

☒ AZ-EAST *

☒ AZ-SOUTH *

☐ MGT *

Specify the availability zones you want your worker nodes spread across equally.

If you plan to use Helm and Pure Service Orchestrator with your cluster you will want to enable the “Allow Privileged” setting near the bottom and click save.

(Optional) Add-ons - Use with caution

☒ Allow Privileged ⚠ Allows containers to run in privileged mode. Sets --allow-privileg

Admission Plugins

☐ PodSecurityPolicy

☐ DenyEscalatingExec

☐ SecurityContextDeny

Save

For a more prodction or permanent cluster, Master nodes need to be HA and increase the Mem and CPU. Make sure to spread the master nodes across your AZ's and place Workers in different AZ's as necessary.

Master/ETCD Node Instances (min: 1, max: 5) *

Master/ETCD VM Type*

large (cpu: 2, ram: 8 GB, disk: 16 GB) ▾

Master Persistent Disk Type*

Automatic: 10 GB ▾

Master/ETCD Availability Zones *

☐ AZ-WEST *

☐ AZ-EAST *

☐ AZ-SOUTH *

☐ MGT *

Maximum number of workers on a cluster (min: 1) *

Worker Node Instances (min: 1) *


Worker VM Type*

xlarge (cpu: 4, ram: 16 GB, disk: 32 GB) ▾

Worker Persistent Disk Type*

Automatic: 50 GB ▾

The K8s worker persistent disk type



Don't forget to click "Allow Privileged" if you need it later.

- a. Create as many plans as you need. I would suggest creating at least 3 for now.

5. Kubernetes Cloud Provider Configuration

Fill in your vSphere information, The Stored VM Folder must match what you put into the Ops Manager Director earlier in the config.

Additionally, Pure Storage recommends using vVOLS for the Persistent Datastore. This allows the use of Storage Policy Based Management (SPBM) and disaggregated scaling of Compute and Capacity to provide flexibility as you grow your Kubernetes footprint.

Choose your IaaS*

☐ GCP

☒ vSphere

vCenter Master Credentials *

administrator@pksvc.local

vCenter Host *

pksvc.newstack.local

Datacenter Name *

pkdemo

Datastore Name *

m50-vvols, m70r2-vvols

Stored VM Folder *

pcf-vms

☐ AWS

☐ Azure

Click Save.

6. Under Monitoring Enable syslog and vRealize Log Insight Integration if you required.
7. Agree or Disagree with the Usage Data Portion.

- Click "Installation Dashboard" Once you have green checks next to every config category. Click Review Pending Changes, then Apply Changes. This will take several minutes to complete.

The screenshot shows the BOSH installation progress on the left and the terminal output on the right.

Progress List:

- Installing BOSH
- Uploading runtime config releases to the director
- Uploading syslog release
- Updating BOSH director with 2.0 cloud config
- Updating CPI configs
- Updating Internal UAA Configuration
- Putting Tile Credentials into CredHub
- Updating runtime configs for pivotal-container-service
- Uploading stemcell for Enterprise PKS
- Uploading releases for Enterprise PKS
- Migrating credentials to director CredHub
- Installing Enterprise PKS
- Running errand Upgrade all clusters errand for Enterprise PKS
- Cleaning up BOSH director

Terminal Output:

```
===== 2019-05-14 11:56:22 UTC Running "/usr/local/bin/bosh --no-color --non-interactive /default/deployments/bosh.yml"
Deployment manifest: '/var/tempest/workspaces/default/deployments/bosh.yml'
Deployment state: '/var/tempest/workspaces/default/deployments/bosh-state.json'

Started validating
Validating release 'bosh'... Finished (00:00:01)
Validating release 'bosh-vsphere-cpi'... Finished (00:00:00)
Validating release 'uaa'... Finished (00:00:02)
Validating release 'credhub'... Finished (00:00:00)
Validating release 'bosh-system-metrics-server'... Finished (00:00:02)
Validating release 'os-conf'... Finished (00:00:00)
Validating release 'backup-and-restore-sdk'... Finished (00:00:03)
Validating release 'bpm'... Finished (00:00:01)
Validating cpi release... Finished (00:00:00)
Validating deployment manifest... Finished (00:00:00)
Validating stemcell... Finished (00:00:05)
Finished validating (00:00:18)

Started installing CPI
Compiling package 'ruby-2.4-r4/0cdc60ed7fdb326e605479e9275346200af30a25'... Finished
Compiling package 'iso9660wrap/2e7db549be4f20243d9e3b835df265e1a23d0ebb'... Finished
Compiling package 'vsphere_cpi/7556c6c966f3efcd1660cf2dc010e6c28a58182d'... Finished
Installing packages... Finished (00:00:01)
```

DNS Configuration

After the BOSH setup is completed and successful. Make sure to enter in your DNS records for the pks api endpoint. In this configuration example pks.app.newstack.local must map to the IP given to the VM during the rollout of PKS Enterprise. Trying to access the PKS endpoint or cluster managers by IP will result in the request failing. The certificates generated are tied to the host names or endpoint names. So working DNS servers are required.

Select the Enterprise PKS tile in Ops Manager and Click the Status tab.

The screenshot shows the "Enterprise PKS" status page with tabs for Settings, Status, Credentials, and Logs. The Status tab is active, displaying a table with the following data:

JOB	INDEX	IPS	AZ	CID
Pivotal Container Service	0	10.21.230.132	MGT	vm-daf2d603-a6a7-4f72-8896-b2cfbc828fb7

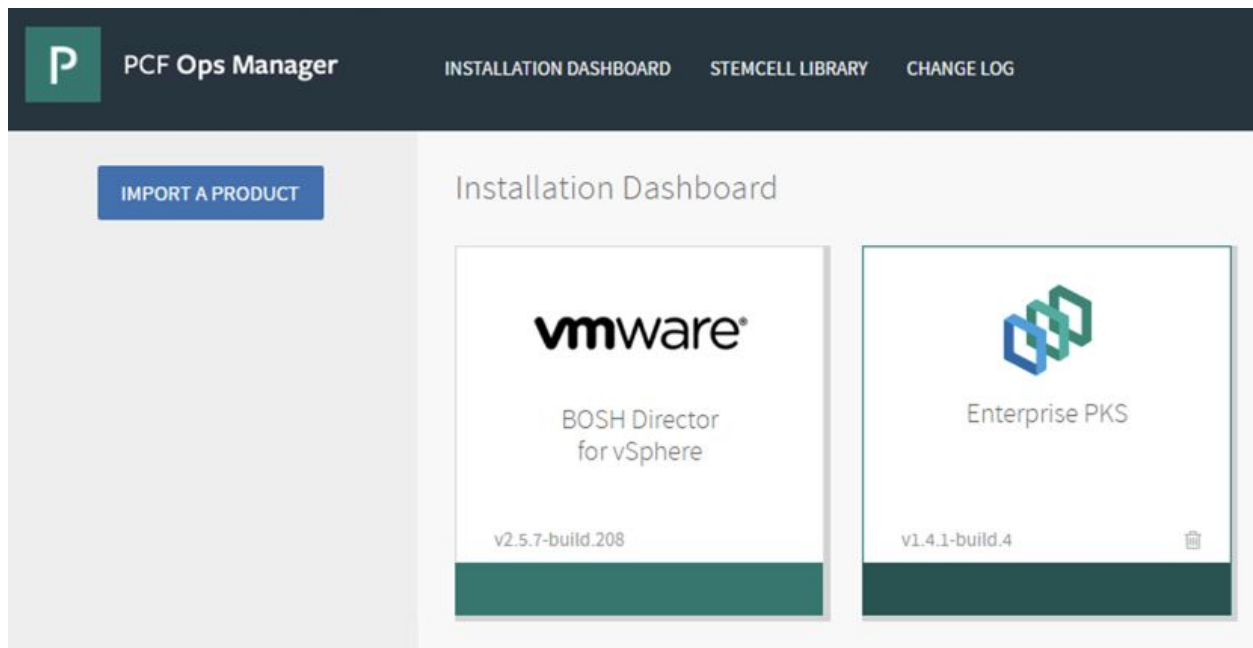
Setup Access to Ops Manager and PKS CLI

Create a PKS User


Set your UAAC target to the PKS API endpoint. (gem install cf-uaac). If you get an error installing on ubuntu make sure to install ruby.

```
uaac target https://pks.newstack.local:8443  
--skip-ssl-validation
```

Go to the PKS Enterprise tile:



Go to Credentials Tab and get the **PKS Uaa Management Admin Client key** by clicking “Link to Credential. **Copy the key without the “ marks.**


PCF Ops Manager
INSTALLATION DASHBOARD
STEMCELL LIBRARY
CHANGE LOG

Enterprise PKS

Settings
Status
Credentials
Logs

NAME	CREDENTIALS
Cf Mysql Mysql Admin Password	Link to Credential
Cf Mysql Mysql Cluster Health Password	Link to Credential
Cf Mysql Mysql Galera Healthcheck Endpoint Password	Link to Credential
Cf Mysql Mysql Galera Healthcheck Db Password	Link to Credential
Cf Mysql Pks Db Password	Link to Credential
Cf Mysql Uaa Db Password	Link to Credential
Cf Mysql Telemetry Db Password	Link to Credential
Cf Mysql Billing Db Password	Link to Credential
Pks Api Uaa Client	Link to Credential
Pks Uaa Management Admin Client	Link to Credential
Pks Services Admin Uaa Client	Link to Credential
Uaa Admin Password	Link to Credential
Uaa Encryption Passphrase	Link to Credential
UAA Client Credentials	Link to Credential

JOB	NAME	CREDENTIALS
Pivotal Container Service	VM Credentials	Link to Credential
	Pks Tls	Link to Credential

```
uaac token client get admin -s <paste key here>
```

Create your PKS user

```
uaac user add jowings --emails jowings@newstack.local -p <create a password>
```

Make your user cluster admin

```
uaac member add pks.clusters.admin jowings
```

Login to the PKS API server.

```
pks login -a pks.newstack.local -u jowings -k
```

Use the -k if your SSL is self-signed. Use your password created in the above step.

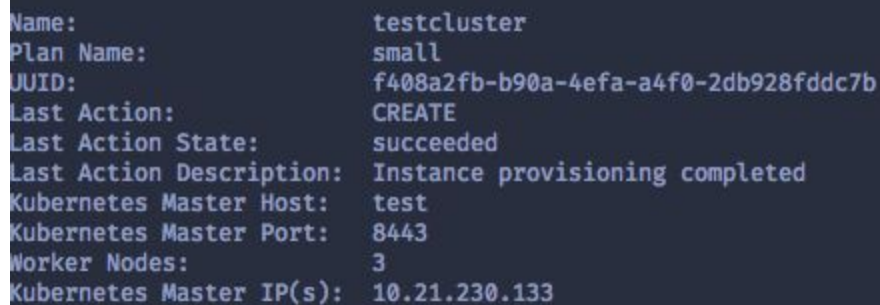
Test Cluster Creation

```
pks create-cluster testcluster --external-hostname test  
--plan small
```

Use PKS Cli to Check your cluster status

```
pks cluster testcluster
```

When provisioning is finished output will look like this:



```
Name:                testcluster  
Plan Name:           small  
UUID:               f408a2fb-b90a-4efa-a4f0-2db928fddc7b  
Last Action:         CREATE  
Last Action State:   succeeded  
Last Action Description: Instance provisioning completed  
Kubernetes Master Host: test  
Kubernetes Master Port: 8443  
Worker Nodes:        3  
Kubernetes Master IP(s): 10.21.230.133
```

Now run:

```
pks get-credentials testcluster
```

Add a DNS record for the Master Host name to the IP.

With this example, we will create a host 'test' pointing to the IP 10.21.230.133

If you get a timeout or error the DNS record may not be ready. Make sure your client can resolve the IP.

Sequence to create and use a PKS Cluster

```
pks create-cluster <cluster name> --external-hostname <host
name> --plan <plan name>
pks cluster <cluster name>
pks get-credentials <cluster name>
```

Create DNS record match <host name> to the output IP from the successful cluster creation.

Creating the SPBM Storage Class for the vSphere Cloud Provider

The following page describes the SPBM options available to the VCP:

<https://github.com/vmware/vsphere-storage-for-kubernetes/blob/master/documentation/storageclass.md>

Right now this issue is blocking this from working:

<https://github.com/kubernetes/kubernetes/issues/75040>

Just tested (6/25/19) PKS Enterprise version 1.4.1-build.4 not working.

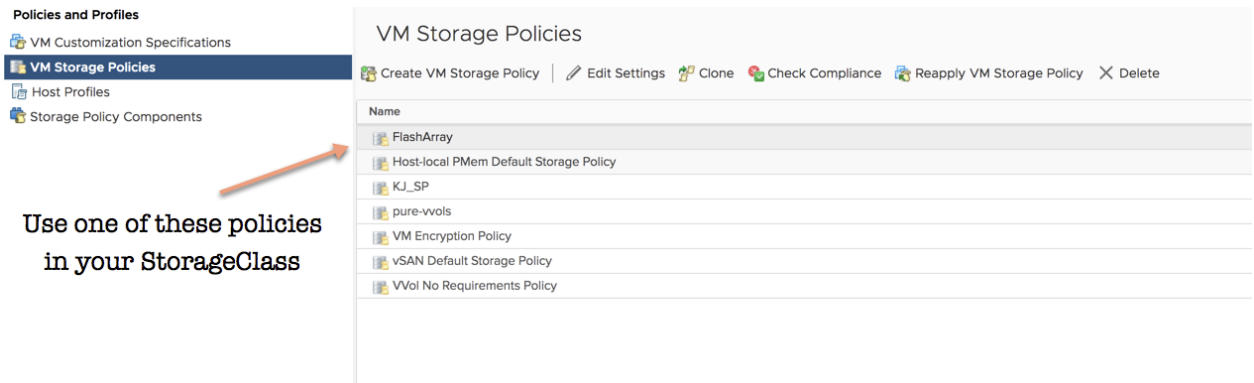
1. Create a StorageClass file. For example pure-vvols.yaml

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: pure-vvols
provisioner: kubernetes.io/vsphere-volume
parameters:
  diskformat: zeroedthick
  storagePolicyName: FlashArray
```

Alternative is to create a Storage Class tied directly to the datastore
Example

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: pure-ds
```

```
provisioner: kubernetes.io/vsphere-volume
parameters:
  datastore: m70-vvols-datastore
```



2. Apply the storage class
Kubectl apply
3. Run a test application

More Information on configuring the vSphere Cloud Provider

<https://vmware.github.io/vsphere-storage-for-kubernetes/documentation/overview.html>

<https://vmware.github.io/vsphere-storage-for-kubernetes/documentation/policy-based-mgmt.html>

Setting Up Bosh

Bosh CLI will be needed to create releases and is also helpful when troubleshooting and other tasks in the PKS Clusters.

Note: you have to install the om tool first: <https://github.com/pivotal-cf/om>

1. Output the CA into a file to be used when connecting to your Bosh Director.

```
om --target https://opsman.newstack.local -u admin -p <Ops Manager PW you created at the very beginning> -k curl -p /api/v0/certificate_authorities -s | jq -r '.certificate_authorities | select(map(.active == true))[0] | .cert_pem' > ~/opsmanager.pem
```
2. Output your credentials

```
om --target https://opsman.newstack.local -u jowings -p <Ops
```

Manager PW you created at the very beginning> -k curl -p
/api/v0/deployed/director/credentials/bosh2_commandline_credentials
-s | jq -r '.credential'

Output from last command

```
BOSH_CLIENT=ops_manager  
BOSH_CLIENT_SECRET=anXl0m55LdLNNLAib1i_5HP-Je5jToYn  
BOSH_CA_CERT=/var/tempest/workspaces/default/root_ca_certificate  
BOSH_ENVIRONMENT=10.21.230.32 bosh
```

3. Format as follows for .bashrc notice just the IP for the BOSH_ENVIRONMENT and the CA_CERT it pointing to the file we dumped the cert into earlier.

```
export BOSH_CLIENT=ops_manager  
export BOSH_CLIENT_SECRET=anXl0m55LdLNNLAib1i_5HP-Je5jToYn  
export BOSH_CA_CERT=~/.opsmanager.pem  
export BOSH_ENVIRONMENT=10.21.230.32
```

4. Test BOSH from the CLI
bosh releases

Output should look like this:

```
[jowings@pwkdev ~ (prod01:default)]$ bosh releases  
Using environment '10.21.230.131' as client 'ops_manager'
```

Name	Version	Commit Hash
backup-and-restore-sdk	1.8.0*	8b305df
bosh-dns	1.10.0*	7c6515f
bpm	1.0.4*	420dc51
cf-mysql	36.14.0.1*	2400c66a
cfcr-etcd	1.10.0*	3f69d31
docker	35.1.0*	fb29f63
kubo	0.31.0*	43bee79
kubo-service-adapter	1.4.0-build.194*	7b57641e
nsx-cf-cni	2.4.0.12511604*	37923f7+
on-demand-service-broker	0.26.0*	d074e07
pks-api	1.4.0-build.194*	5f3e572f
pks-nsx-t	1.25.1*	286dfefc
pks-telemetry	2.0.0-build.175*	7f937fe
pks-vrli	0.9.0*	566ba95
pks-vrops	0.13.0*	bd256c3
pxc	0.14.0*	c19b825
sink-resources-release	0.1.27*	2df5885+
syslog	11.4.0*	feedfa7
uaa	71.0*	6bbc04b

Optional: Pure Service Orchestrator for ISCSI

Pure Service Orchestrator provides Container Storage-as-a-Service with Direct access to FlashArray or FlashBlade resources. PSO requires additional packages when using the FlashArray that are not currently included in the Ubuntu Xenial Stemcell used by PKS. The NFS Client Packages required by PSO when using the FlashBlade are used by other Pivotal use cases and are therefore included. **If you are using FlashBlade only you only need to follow the directions for installing Helm and Pure Service Orchestrator. For FlashBlade follow the section 'Runtime Config for PSO'.**

1. Install Helm using the Pivotal Docs below.
 - a. <https://docs.pivotal.io/runtimes/pks/1-4/helm.html>
2. Setup the PSO Helm Repo
helm repo add pure <https://purestorage.github.io/helm-charts>
helm repo update
3. Create your values.yaml file
Use the latest full file from the Pure Storage helm repo.
<https://raw.githubusercontent.com/purestorage/helm-charts/master/pure-k8s-plugin/values.yaml>

Example Changes

namespace:

c pure: pks

arrays:

FlashBlades:

- MgmtEndPoint: "<FlashBlade MGT IP>"

NfsEndPoint: "<FlashBlade NFS IP>"

APIToken: "T-9f276a18-50ab-446e-8a0c-666a3529a1b6"

4. Install PSO
helm install -n pso pure/pure-k8s-plugin -f pksdemo-values.yaml
5. List the Storage Classes
kubectl get sc

- This example only used a single flashblade as we have not made runtime config changes needed for FlashArray.
- Deploy an app using the pure-file StorageClass.

<https://github.com/2vcps/pksapp>

```
git clone https://github.com/2vcps/pksapp.git
cd pksapp
kubectl apply -f . #notice the . in the cli
```

- Verify the demo app is running

Kubectl get pod

Kubectl get pvc

Output should look like this:

```
[jowings@pwkdev pksapp (testcluster:default)]$ kubectl get pod
NAME                                READY   STATUS    RESTARTS   AGE
frontend-74b4665db5-f7hc2          1/1     Running   0           12m
frontend-74b4665db5-m997n          1/1     Running   0           12m
frontend-74b4665db5-tj28f          1/1     Running   0           12m
frontend-74b4665db5-wf2mz          1/1     Running   0           12m
pure-flex-l98jm                     1/1     Running   0           15m
pure-flex-nxc5t                     1/1     Running   0           15m
pure-flex-wdfq6                     1/1     Running   0           15m
pure-provisioner-7444b7d54b-xkkgk   1/1     Running   0           15m
redis-master-54df6fb787-cqm5w       1/1     Running   0           12m
redis-slave-678676d9b7-hpt7b        1/1     Running   0           12m
[jowings@pwkdev pksapp (testcluster:default)]$ kubectl get pvc
NAME                                STATUS    VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
redis-master-claim                  Bound     pvc-d119f92f-764c-11e9-af05-005056a93580  2Gi        RWO             pure-file      12m
redis-slave-claim                   Bound     pvc-d11f2ee7-764c-11e9-af05-005056a93580  2Gi        RWO             pure-file      12m
[jowings@pwkdev pksapp (testcluster:default)]$
```

-

Runtime Config for PSO

Create a custom Bosh Release to add the *open-iscsi* and *multipath-tools* packages to your PKS environment. Perform the steps below to create a runtime config that will install these two packages in the stemcell. This is an included and supported feature of Pivotal and is used by other 3rd party vendors for storage plugins and monitoring.

- Go to the following git repo and clone to your client with the BOSH CLI tools.
https://github.com/2vcps/pso_prereqs
- Follow the README in the repo as it will have the most recent instructions for deployment.

Optional: Setup up Harbor

For Enterprise environments it is recommended to use an internal container repo. VMware provides Harbor with a tile to deply built into the Pivotal Platform.

<https://docs.pivotal.io/pks/1-5/harbor.html>

The deployment and use of Harbor requires the import CA Certificate from harbor to be used by your docker registry.

1. deploy tile following the documentation
2. download ca cert
3. copy ca.crt to /etc/docker/harbor.newstack.local/
4. You will have to login to push and pull from harbor

```
docker login harbor.newstack.local
jowings
password##
```

If you have images you need to push into the harbor repo you must tag them correctly prior to the docker push.

Mind the line wrapping in the document

```
docker tag gcr.io/google-samples/gb-frontend:v4
harbor.newstack.local/library/gb-frontend:v4
```

```
docker tag gcr.io/google_samples/gb-redisslave:v1
harbor.newstack.local/library/gb-redisslave:v1
```



```
docker tag gcr.io/google_containers/redis:e2e  
harbor.newstack.local/library/redis:e2e
```

```
docker push harbor.newstack.local/library/gb-frontend:v4  
docker push harbor.newstack.local/library/redis:e2e  
docker push harbor.newstack.local/library/gb-redisslave:v1
```

References:

Links I used to gather what I needed for install and configuration

<https://docs.pivotal.io/runtimes/pks/1-4/installing.html>

<https://www.virtuallyghetto.com/2018/03/getting-started-with-vmware-pivotal-container-service-pks-part-1-overview.html>

<https://www.virtuallyghetto.com/2018/03/getting-started-with-vmware-pivotal-container-service-pks-part-2-pks-client.html>

<https://www.virtuallyghetto.com/2018/03/getting-started-with-vmware-pivotal-container-service-pks-part-3-nsx-t.html>

<https://www.virtuallyghetto.com/2018/03/getting-started-with-vmware-pivotal-container-service-pks-part-4-ops-manager-bosh.html>

<https://www.virtuallyghetto.com/2018/04/getting-started-with-vmware-pivotal-container-service-pks-part-5-pks-control-plane.html>

<https://www.virtuallyghetto.com/2018/04/getting-started-with-vmware-pivotal-container-service-pks-part-6-kubernetes-go.html>

<https://www.virtuallyghetto.com/2018/04/getting-started-with-vmware-pivotal-container-service-pks-part-7-harbor.html>

Very Helpful

https://github.com/goharbor/harbor/blob/master/docs/use_notary.md