This document outlines the kube yaml fields that are currently supported by the **podman kube play** command. The notes were cross referenced with the Kubernetes Docs, particularly the <u>Greppable Reference</u>, where printable view make Ctrl-F go vroom

Not Supported ₹ Not Documented ₹ Supported ₹ Only with multiple nodes ✓

1. Pod Fields

<u>PodSpec</u>

Field	Field
containers	💢 os.name
initContainers	💢 volumes
💢 imagePullSecrets	
💢 enableServiceLinks	

1.1. Scheduling

KubeSchedulerConfiguration: has many profiles, each identified by a schedulerName. See also section on Scheduling Profiles.

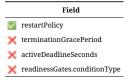
Field	Field	Field
☑ nodeSelector	💢 priority	<pre>preemptionPolicy</pre>
☑ nodeName	💢 priorityClassName	? overhead
☑ schedulerName	💢 runtimeClassName	

- PriorityClass
- RuntimeClass

1.1.1. Affinity, Tolerations, Taints, Topology Spread Constraints

	affinity.*		tolerations.*		topologySpreadConstraints.*
✓	nodeAffinity		key	Z	maxSkew
✓	podAffinity	✓	operator		topologyKey
	podAntiAffinity		effect	7	whenUnsatisfiable
			toleration Seconds	7	labelSelector
		☑			minDomains

1.1.2. Lifecycle



1.2. DNS

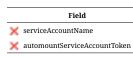
Field		hostAliases.*		dnsConfig.*
M hostname	V	hostAliases.hostnames	V	nameservers
💢 setHostnameAsFQDN	V	hostAliases.ip	V	options.name
💢 subdomain			V	options.value
💢 dnsPolicy			V	searches

hostAliases

only valid for non-hostNetwork pods.

1.3. Security

Service Accounts



1.4. Namespaces, sysctl and seccomp profiles

Emacs also supports seccomp profiles, if you're paranoid and for some reason compiling BPF programs isn't an undue time investment.

Field	securityContext.*
hostNetwork	💢 seccompProfile.type
MostPID	💢 seccompProfile.localhostProfile
MostIPC hostIPC	💢 sysctls.name
shareProcessNamespace	🔀 sysctls.value

1.5. Volume/Process Ownership and SELinux

Other securityContext.* fields for PodSpec

S	ecurityContext.*		securityContext.*
☑ ru	nAsUser	V	seLinuxOptions.level
💢 ru	nAsNonRoot	V	seLinuxOptions.role
🔽 ru	nAsGroup	V	seLinuxOptions.type
🗾 suj	pplementalGroups	V	seLinuxOptions.user
💢 fsC	Froup	Х	windowsOptions.gmsaCredentialSpec
💢 fsC	GroupChangePolicy	Х	windowsOptions.hostProcess
		×	windows Options. run As User Name

fsGroup/ChangePolicy

these pertain to whether a pod can change the ownership of volumes before "being exposed inside Pod." The former is a Group ID and setgid will be set, changing ownership of files created. The latter can only be set to OnRootMismatch or Always. Not entirely sure, but I wouldn't want to have to fix whatever this solves.

2. Container Fields

Name/Image		Entry Point		Ports		Debugging
name	V	command	V	ports.containerPort	Х	stdin
image	V	args	V	ports.hostIP	×	stdinOnce
imagePullPolicy	V	workingDir	V	ports.hostPort	Х	tty
			V	ports.name		
			V	ports.protocol		

2.1. Env References

Either set env.value or supply a reference source with env.valueFrom, which needs a corresponding envFrom.* source

env.*	env.valueFrom.*	env.valueFrom.*	env.valueFrom.*
🔽 name 🔽	fieldRef	configMapKeyRef.key	secretKeyRef.key
📝 value 📝	resource Field Ref	configMapKeyRef.name	secretKeyRef.name
		configMapKeyRef.optional	secretKeyRef.optional

env.valueFrom.fieldRef

- Composed of fieldPath & apiVersion (ObjectFieldSelector)
- Selects a field of the pod
- Only annotations, labels, name and namespace are supported.

env.valueFrom.resourceFieldRef

- Composed of resource, containerName, divisor (ResourceFieldSelector)
- Selects a resource of the container
- $\bullet \ \, \text{Only resources limits and requests (limits.cpu, limits.memory, requests.cpu and requests.memory) are currently supported. } \\$

2.2. Env Sources

envFrom.*	envFrom.*	env.*
💢 prefix	configMapRef.name	secretRef.name
	configMapRef.optional	secretRef.optional

2.3. Volumes, Devices and Resources

	volumeMounts.*		volumeMounts.*		volumeMounts.*		volumeDevices.*		resources.*
V	name	V	mountPath	X	subPath	X	devicePath	V	limits
V	readOnly	Х	mountPropagation	Х	subPathExpr	Х	name	V	requests

2.4. Lifecycle, Termination and Probes

LifecycleHandler	TerminationMessage		<u>Probe</u>
X lifecycle.postStart	X terminationMessagePath	V	livenessProbe
💢 lifecycle.preStop	💢 terminationMessagePolicy	×	readinessProbe
		×	startupProbe

For the termination message, the **path** is the mounted file to which the container's termination message will be written and the **policy** indicates how the termination message should be populated.

securityContext.*		securityContext.*
securityContext.runAsUser	V	securityContext.readOnlyRootFilesystem
💢 securityContext.runAsNonRoot	X	securityContext.procMount
securityContext.runAsGroup	V	securityContext.privileged
	V	security Context. allow Privilege Escalation

2.4.1. Capabilities and Seccomp

securityContext.*

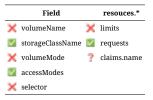
	sc.capabilities.*		sc.seccompProfile.*
V	add	X	type
V	drop	×	localhostProfile

2.4.2. SELinux and Windows

securityContext.*

	sc.seLinuxOptions.*		sc.windowsOptions.*
V	level	Х	gmsaCredentialSpec
V	role	X	hostProcess
V	type	×	runAsUserName
V	user		

3. PersistentVolumeClaim Fields



4. ConfigMap Fields

	Field		
V	binaryData		
V	data		
×	immutable		

5. Deployment Fields

Field		Field	
replicas	X	minReadySeconds	
selector	×	progressDeadlineSeconds	
template	×	strategy.type	
💢 revisionHistoryLimit	×	strategy.rollingUpdate.maxSurge	
💢 paused	×	strategy. rolling Update. max Unavailable	

^{• (}Podman) For replicas the actual replica count is ignored and set to 1

Created: 2023-07-14 Fri 05:26 Validate