New issue

podman run fails with operation not permitted - podman running in docker container #8190

Closed

longwuyuan opened on Oct 30, 2020 · edited by longwuyuan

Edits ▾ •••

Is this a BUG REPORT or FEATURE REQUEST? (leave only one on its own line)

/kind bug

Description

- If there is a "pip install" command in a Dockerfile, then Podman build fails with error "operation not permitted"
- Podman build creates docker image, if Dockerfile does not have "pip install" command

Steps to reproduce the issue:

1.Install or get a kubernetes cluster. Minikube also works

2.Install Jenkins in Kubernetes via helm chart https://github.com/jenkinsci/helm-charts

3.Create a pipeline project in jenkins using the Jenkinsfile and repo at https://github.com/longwuyuan/jenkins-kubernetes-podman

4. Build the project

5. Running a

Describe the results you received:

error running container: error creating new mount namespace for [/bin/sh -c pip install -r requirements.txt]: operation not permitted time="2020-10-29T19:14:31Z" level=error msg="unable to write build event: "write unixgram @75e5c->/run/systemd/journal/socket: sendmsg: no such file or directory""

Describe the results you expected:

Image is built

Additional information you deem important (e.g. issue happens only occasionally):

Only happening when there is a pip install command in the Dockerfile

** podman info

```
+ podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins info
time="2020-10-29T19:14:08Z" level=error msg="unable to write system event: \"write unixgram @75e4b->/run/systemd/journal/socket: sendmsg: no such
file or directory\""
host:
  arch: amd64
  buildahVersion: 1.16.1
  cgroupManager: systemd
  cgroupVersion: v1
  conmon:
    package: 'conmon: /usr/libexec/podman/conmon'
    path: /usr/libexec/podman/conmon
    version: 'conmon version 2.0.20, commit: '
  cpus: 8
  distribution:
    distribution: ubuntu
    version: "20.04"
  eventLogger: journald
  hostname: test0-6-p73zw-jcz29-cgm38
  idMappings:
    gidmap: null
    uidmap: null
  kernel: 5.4.0-48-generic
  linkmode: dynamic
  memFree: 23314305024
  memTotal: 33676963840
  ociRuntime:
    name: runc
    package: 'runc: /usr/sbin/runc'
    path: /usr/sbin/runc
    version: 'runc version spec: 1.0.1-dev'
  os: linux
  remoteSocket:
    path: /run/podman/podman.sock
  rootless: false
  slirp4netns:
    executable: ""
    package: ""
    version: ""
  swapFree: 0
  swapTotal: 0
  uptime: 657h 36m 47.56s (Approximately 27.38 days)
registries:
  search:
  - docker.io
  - quay.io
store:
  configFile: /etc/containers/storage.conf
  containerStore:
    number: 0
    paused: 0
    running: 0
    stopped: 0
  graphDriverName: vfs
  graphOptions: {}
  graphRoot: /home/jenkins
  graphStatus: {}
  imageStore:
    number: 0
  runRoot: /home/jenkins
  volumePath: /home/jenkins/volumes
version:
  APIVersion: 2.0.0
  Built: 0
  BuiltTime: Thu Jan  1 00:00:00 1970
  GitCommit: ""
  GoVersion: go1.14
```

```
    OsArch: linux/amd64
    Version: 2.1.1
```

Have you tested with the latest version of Podman and have you checked the Podman Troubleshooting Guide?

Yes

Additional environment details (AWS, VirtualBox, physical, etc.):

JENKINS BUILD LOG

```
Started by user admin
Obtained Jenkinsfile from git https://github.com/longwuyuan/jenkins-kubernetes-podman.git
Running in Durability level: MAX_SURVIVABILITY
[Pipeline] Start of Pipeline
[Pipeline] podTemplate
[Pipeline] {
[Pipeline] node
Created Pod: jenkins/test0-6-p73zw-jcz29-cgm38
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Scheduled] Successfully assigned jenkins/test0-6-p73zw-jcz29-cgm38 to ssdnodes0.devopsdragon.com
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Pulling] Pulling image "longwuyuan/podman"
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Pulled] Successfully pulled image "longwuyuan/podman" in 916.856378ms
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Created] Created container podman
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Started] Started container podman
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Pulled] Container image "jenkins/inbound-agent:4.3-4" already present on machine
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Created] Created container jnlp
[Normal][jenkins/test0-6-p73zw-jcz29-cgm38][Started] Started container jnlp
Still waiting to schedule task
Waiting for next available executor on ‘test0-6-p73zw-jcz29-cgm38’
Agent test0-6-p73zw-jcz29-cgm38 is provisioned from template test0_6-p73zw-jcz29
---
apiVersion: "v1"
kind: "Pod"
metadata:
  annotations:
    buildUrl: "http://jenkins-release-0:8080/job/test0/6/"
    runUrl: "job/test0/6/"
  labels:
    jenkins/label-digest: "9688aaccd7c4e3102bb5d181c613e2857ece7967"
    jenkins/jenkins-release-0-jenkins-slave: "true"
    jenkins/label: "test0_6-p73zw"
  name: "test0-6-p73zw-jcz29-cgm38"
spec:
  containers:
  - args:
    - "infinity"
    command:
    - "sleep"
    image: "longwuyuan/podman"
    name: "podman"
    volumeMounts:
    - mountPath: "/home/jenkins/agent"
      name: "workspace-volume"
      readOnly: false
  - env:
    - name: "JENKINS_SECRET"
      value: "********"
    - name: "JENKINS_TUNNEL"
      value: "jenkins-release-0-agent:50000"
    - name: "JENKINS_AGENT_NAME"
      value: "test0-6-p73zw-jcz29-cgm38"
    - name: "JENKINS_NAME"
      value: "test0-6-p73zw-jcz29-cgm38"
    - name: "JENKINS_AGENT_WORKDIR"
      value: "/home/jenkins/agent"
    - name: "JENKINS_URL"
      value: "http://jenkins-release-0:8080/"
    image: "jenkins/inbound-agent:4.3-4"
    name: "jnlp"
    resources:
      requests:
        cpu: "100m"
        memory: "256Mi"
    volumeMounts:
    - mountPath: "/home/jenkins/agent"
      name: "workspace-volume"
      readOnly: false
  nodeSelector:
    kubernetes.io/os: "linux"
  restartPolicy: "Never"
  volumes:
  - emptyDir:
      medium: ""
    name: "workspace-volume"
```

```
Running on test0-6-p73zw-jcz29-cgm38 in /home/jenkins/agent/workspace/test0
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Declarative: Checkout SCM)
[Pipeline] checkout
Selected Git installation does not exist. Using Default
The recommended git tool is: NONE
No credentials specified
Cloning the remote Git repository
Avoid second fetch
Checking out Revision c3fc096c832d7d2dc9b401716636fd11f80e3136 (refs/remotes/origin/master)
Cloning repository https://github.com/longwuyuan/jenkins-kubernetes-podman.git
 > git init /home/jenkins/agent/workspace/test0 # timeout=10
Fetching upstream changes from https://github.com/longwuyuan/jenkins-kubernetes-podman.git
 > git --version # timeout=10
 > git --version # 'git version 2.20.1'
 > git fetch --tags --force --progress -- https://github.com/longwuyuan/jenkins-kubernetes-podman.git +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git config remote.origin.url https://github.com/longwuyuan/jenkins-kubernetes-podman.git # timeout=10
 > git config --add remote.origin.fetch +refs/heads/*:refs/remotes/origin/* # timeout=10
 > git rev-parse refs/remotes/origin/master^{commit} # timeout=10
 > git config core.sparsecheckout # timeout=10
 > git checkout -f c3fc096c832d7d2dc9b401716636fd11f80e3136 # timeout=10
Commit message: "added text in requirements.txt and added pip install command back again"
 > git rev-list --no-walk 8d45f06ff2fc4a71c95fbb214da34f0e65ac9358 # timeout=10
[Checks API] No suitable checks publisher found.
[Pipeline] }
[Pipeline] // stage
[Pipeline] withEnv
[Pipeline] {
[Pipeline] container
[Pipeline] {
[Pipeline] stage
[Pipeline] { (Main)
[Pipeline] sh
+ hostname
test0-6-p73zw-jcz29-cgm38
+ grep -i namespace
+ sysctl -A
sysctl: reading key "kernel.unprivileged_userns_apparmor_policy"
user.max_cgroup_namespaces = 128125
user.max_ipc_namespaces = 128125
user.max_mnt_namespaces = 128125
user.max_net_namespaces = 128125
user.max_pid_namespaces = 128125
user.max_user_namespaces = 128125
user.max_uts_namespaces = 128125
+ ls -l /
total 48
lrwxrwxrwx   1 root root    7 Oct  8 01:31 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Apr 15  2020 boot
drwxr-xr-x   5 root root  360 Oct 29 19:13 dev
drwxr-xr-x   1 root root 4096 Oct 29 19:13 etc
drwxr-xr-x   1 root root 4096 Oct 29 19:13 home
lrwxrwxrwx   1 root root    7 Oct  8 01:31 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Oct  8 01:31 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 Oct  8 01:31 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 Oct  8 01:31 libx32 -> usr/libx32
-rw-r--r--   1 root root    0 Oct 29 10:31 long-booyah
drwxr-xr-x   2 root root 4096 Oct  8 01:31 media
drwxr-xr-x   2 root root 4096 Oct  8 01:31 mnt
drwxr-xr-x   1 root root 4096 Oct 29 10:31 opt
dr-xr-xr-x 396 root root    0 Oct 29 19:13 proc
drwx------   2 root root 4096 Oct  8 01:34 root
drwxr-xr-x   1 root root 4096 Oct 29 19:13 run
lrwxrwxrwx   1 root root    8 Oct  8 01:31 sbin -> usr/sbin
drwxr-xr-x   2 root root 4096 Oct  8 01:31 srv
dr-xr-xr-x  13 root root    0 Oct 29 19:13 sys
drwxrwxrwt   1 root root 4096 Oct 29 10:31 tmp
drwxr-xr-x   1 root root 4096 Oct 29 10:31 usr
drwxr-xr-x   1 root root 4096 Oct  8 01:34 var
+ whoami
root
+ pwd
/home/jenkins/agent/workspace/test0
+ ls -alth
total 44K
drwxr-xr-x 4 1000 1000 4.0K Oct 29 19:14 ..
drwxr-xr-x 8 1000 1000 4.0K Oct 29 19:14 .git
drwxr-xr-x 3 1000 1000 4.0K Oct 29 19:14 .
-rw-r--r-- 1 1000 1000   25 Oct 29 19:14 .dockerignore
-rw-r--r-- 1 1000 1000   14 Oct 29 19:14 .gitignore
-rw-r--r-- 1 1000 1000  245 Oct 29 19:14 Dockerfile
-rw-r--r-- 1 1000 1000   37 Oct 29 19:14 Dockerfile.testbuild
-rw-r--r-- 1 1000 1000 1.9K Oct 29 19:14 Jenkinsfile
```

```
-rw-r--r-- 1 1000 1000 1.1K Oct 29 19:14 README.md
-rw-r--r-- 1 1000 1000   62 Oct 29 19:14 main.py
-rw-r--r-- 1 1000 1000    7 Oct 29 19:14 requirements.txt
+ echo WORKSPACE=/home/jenkins/agent/workspace/test0
WORKSPACE=/home/jenkins/agent/workspace/test0
[Pipeline] git
Selected Git installation does not exist. Using Default
The recommended git tool is: NONE
No credentials specified
Warning: JENKINS-30600: special launcher org.csanchez.jenkins.plugins.kubernetes.pipeline.ContainerExecDecorator$1@73388762; decorates
RemoteLauncher[hudson.remoting.Channel@240dcd14:JNLP4-connect connection from 192.168.132.200/192.168.132.200:51222] will be ignored (a typical
symptom is the Git executable not being run inside a designated container)
Fetching changes from the remote Git repository
Checking out Revision c3fc096c832d7d2dc9b401716636fd11f80e3136 (refs/remotes/origin/master)
Commit message: "added text in requirements.txt and added pip install command back again"
[Checks API] No suitable checks publisher found.
[Pipeline] sh
+ echo Testing if podman build works
Testing if podman build works
 > git rev-parse --is-inside-work-tree # timeout=10
 > git config remote.origin.url https://github.com/longwuyuan/jenkins-kubernetes-podman.git # timeout=10
Fetching upstream changes from https://github.com/longwuyuan/jenkins-kubernetes-podman.git
 > git --version # timeout=10
 > git --version # 'git version 2.20.1'
 > git fetch --tags --force --progress -- https://github.com/longwuyuan/jenkins-kubernetes-podman.git +refs/heads/*:refs/remotes/origin/* #
timeout=10
 > git rev-parse refs/remotes/origin/master^{commit} # timeout=10
 > git config core.sparsecheckout # timeout=10
 > git checkout -f c3fc096c832d7d2dc9b401716636fd11f80e3136 # timeout=10
 > git branch -a -v --no-abbrev # timeout=10
 > git checkout -b master c3fc096c832d7d2dc9b401716636fd11f80e3136 # timeout=10
[Pipeline] sh
+ podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins info
time="2020-10-29T19:14:08Z" level=error msg="unable to write system event: \"write unixgram @75e4b->/run/systemd/journal/socket: sendmsg: no such
file or directory\""
host:
  arch: amd64
  buildahVersion: 1.16.1
  cgroupManager: systemd
  cgroupVersion: v1
  conmon:
    package: 'conmon: /usr/libexec/podman/conmon'
    path: /usr/libexec/podman/conmon
    version: 'conmon version 2.0.20, commit: '
  cpus: 8
  distribution:
    distribution: ubuntu
    version: "20.04"
  eventLogger: journald
  hostname: test0-6-p73zw-jcz29-cgm38
  idMappings:
    gidmap: null
    uidmap: null
  kernel: 5.4.0-48-generic
  linkmode: dynamic
  memFree: 23314305024
  memTotal: 33676963840
  ociRuntime:
    name: runc
    package: 'runc: /usr/sbin/runc'
    path: /usr/sbin/runc
    version: 'runc version spec: 1.0.1-dev'
  os: linux
  remoteSocket:
    path: /run/podman/podman.sock
  rootless: false
  slirp4netns:
    executable: ""
    package: ""
    version: ""
  swapFree: 0
  swapTotal: 0
  uptime: 657h 36m 47.56s (Approximately 27.38 days)
registries:
  search:
  - docker.io
  - quay.io
store:
  configFile: /etc/containers/storage.conf
  containerStore:
    number: 0
    paused: 0
    running: 0
    stopped: 0
  graphDriverName: vfs
  graphOptions: {}
```

```
    graphRoot: /home/jenkins
    graphStatus: {}
    imageStore:
      number: 0
    runRoot: /home/jenkins
    volumePath: /home/jenkins/volumes
  version:
    APIVersion: 2.0.0
    Built: 0
    BuiltTime: Thu Jan  1 00:00:00 1970
    GitCommit: ""
    GoVersion: go1.14
    OsArch: linux/amd64
    Version: 2.1.1

  [Pipeline] sh
  + podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins images
  REPOSITORY  TAG     IMAGE ID  CREATED  SIZE
  [Pipeline] sh
  + podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins build -t test-podman-build -f Dockerfile.testbuild .
  STEP 1: FROM alpine
  Getting image source signatures
  Copying blob sha256:188c0c94c7c576fff0792aca7ec73d67a2f7f4cb3a6e53a84559337260b36964
  Copying config sha256:d6e46aa2470df1d32034c6707c8041158b652f38d2a9ae3d7ad7e7532d22ebe0
  Writing manifest to image destination
  Storing signatures
  STEP 2: COPY requirements.txt /
  STEP 3: COMMIT test-podman-build
  --> bad7bb73738
  bad7bb737383958fcf78236bf2461d47a5c4444b311c5a85413ffbc2124e9ce0
  time="2020-10-29T19:14:15Z" level=error msg="unable to write build event: \"write unixgram @75e4f->/run/systemd/journal/socket: sendmsg: no such
  file or directory\""
  [Pipeline] sh
  + podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins images
  REPOSITORY                   TAG     IMAGE ID      CREATED        SIZE
  localhost/test-podman-build  latest  bad7bb737383  2 seconds ago  5.85 MB
  docker.io/library/alpine     latest  d6e46aa2470d  7 days ago     5.85 MB
  [Pipeline] sh
  + podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins build --pid=host -t jenkins-kubernetes-podman .
  STEP 1: FROM python:alpine
  Getting image source signatures
  Copying blob sha256:188c0c94c7c576fff0792aca7ec73d67a2f7f4cb3a6e53a84559337260b36964
  Copying blob sha256:55578f60cda7613da5791c7c3424aaad36a95084141f2f0b9fa8f715044ce672
```

```
Copying blob sha256:692da2fcb614a9721c13d58683f1ae3069df423c6f756f983d83d247c0b33f4e
Copying blob sha256:4b3bf1abad55b794662aa1c408df460c088897b7e29bed8c22cd0a9cc88dad9e
Copying blob sha256:599e2857d4f0d5abc1c8c6d62cbe0ab7a3ec2e866ec4a61e1df9f494ac193d57
Copying config sha256:dc68588b180130138228e65308cfd4334d28423e37d93ece6768c49a92b3c836
Writing manifest to image destination
Storing signatures
STEP 2: COPY requirements.txt /
--> d2a3e8a40fe
STEP 3: COPY main.py ./main.py
--> 01090ad5ebb
STEP 4: RUN pip install -r requirements.txt
error running container: error creating new mount namespace for [/bin/sh -c pip install -r requirements.txt]: operation not permitted
time="2020-10-29T19:14:31Z" level=error msg="unable to write build event: \"write unixgram @75e5c->/run/systemd/journal/socket: sendmsg: no such file or directory\""
Error: error building at STEP "RUN pip install -r requirements.txt": error while running runtime: exit status 1
[Pipeline] }
[Pipeline] // stage
[Pipeline] }
[Pipeline] // container
[Pipeline] }
[Pipeline] // withEnv
[Pipeline] }
[Pipeline] // node
[Pipeline] }
[Pipeline] // podTemplate
[Pipeline] End of Pipeline
[Checks API] No suitable checks publisher found.
ERROR: script returned exit code 125
Finished: FAILURE
```

** I will do as advised or commented on

openshift-ci-robot added kind/bug on Oct 30, 2020

rhatdan on Oct 30, 2020 Member ···

Have you tried running rootfull podman build outside of Kubernetes? Does it still fail?
Have you tried running rooless podman build outside of Kubernetes? Does it fail?

mheon on Oct 30, 2020 Member

EPERM on making the mount namespace makes me wonder if this isn't seccomp. I'm not really familiar with the Kube + Jenkins setup, but can you disable Seccomp (if enabled) on the container in question?

Adding all capabilities would also be instructive.

longwuyuan on Oct 30, 2020 Author

@rhatdan
rootfull --> I seem to be unable to pip install even outside kubernetes (on my linux laptop) ;

```
__$ sudo docker run --name jenkinsagent -ti jenkinsagent bash
root@348265431e35:/# podman
Error: missing command 'podman COMMAND'
Try 'podman --help' for more information.
root@348265431e35:/# ls -l
total 60
-rw-rw-r--   1 root root  245 Oct 30 10:00 Dockerfile
lrwxrwxrwx   1 root root    7 Oct  8 07:01 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Apr 15  2020 boot
drwxr-xr-x   5 root root  360 Oct 30 10:06 dev
drwxr-xr-x   1 root root 4096 Oct 30 10:06 etc
drwxr-xr-x   2 root root 4096 Apr 15  2020 home
lrwxrwxrwx   1 root root    7 Oct  8 07:01 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Oct  8 07:01 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 Oct  8 07:01 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 Oct  8 07:01 libx32 -> usr/libx32
-rw-r--r--   1 root root    0 Oct 30 09:50 long-booyah
-rw-rw-r--   1 root root   62 Oct 30 09:59 main.py
drwxr-xr-x   2 root root 4096 Oct  8 07:01 media
drwxr-xr-x   2 root root 4096 Oct  8 07:01 mnt
drwxr-xr-x   1 root root 4096 Oct 30 09:50 opt
dr-xr-xr-x 263 root root    0 Oct 30 10:06 proc
```

```
-rw-rw-r--   1 root root    7 Oct 30 09:59 requirements.txt
drwx------   2 root root 4096 Oct  8 07:04 root
drwxr-xr-x   1 root root 4096 Oct 23 23:02 run
lrwxrwxrwx   1 root root    8 Oct  8 07:01 sbin -> usr/sbin
drwxr-xr-x   2 root root 4096 Oct  8 07:01 srv
dr-xr-xr-x  13 root root    0 Oct 30 10:06 sys
drwxrwxrwt   1 root root 4096 Oct 30 09:50 tmp
drwxr-xr-x   1 root root 4096 Oct 30 09:50 usr
drwxr-xr-x   1 root root 4096 Oct  8 07:04 var
root@348265431e35:/# ls
root@348265431e35:/# cat Dockerfile
FROM python:alpine

# Add source code in the container
COPY requirements.txt /
COPY main.py ./main.py
RUN pip install -r requirements.txt

# Define container entry point (could also work with CMD python main.py)
ENTRYPOINT ["python", "main.py"]
root@348265431e35:/# podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins build --pid=host -t jenkins-kubernetes-podman .
ERRO[0000] unable to write system event: "write unixgram @000f0->/run/systemd/journal/socket: sendmsg: no such file or directory"
STEP 1: FROM python:alpine
Getting image source signatures
Copying blob 692da2fcb614 done
Copying blob 188c0c94c7c5 done
Copying blob 599e2857d4f0 done
Copying blob 55578f60cda7 done
Copying blob 4b3bf1abad55 done
Copying config dc68588b18 done
Writing manifest to image destination
Storing signatures
STEP 2: COPY requirements.txt /
--> aa040299ff4
STEP 3: COPY main.py ./main.py
--> 8448b2303d1
STEP 4: RUN pip install -r requirements.txt
error running container: error creating new mount namespace for [/bin/sh -c pip install -r requirements.txt]: operation not permitted
ERRO[0036] unable to write build event: "write unixgram @000f0->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: error building at STEP "RUN pip install -r requirements.txt": error while running runtime: exit status 1
root@348265431e35:/# vi requirements.txt
bash: vi: command not found
root@348265431e35:/# cat requirements.txt
```

```
awscli
root@348265431e35:/# podman info
Error: mount /var/lib/containers/storage/aufs:/var/lib/containers/storage/aufs, flags: 0x1000: operation not permitted
root@348265431e35:/# alias p="podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins"
root@348265431e35:/# p info
host:
  arch: amd64
  buildahVersion: 1.16.1
  cgroupManager: systemd
  cgroupVersion: v1
  conmon:
    package: 'conmon: /usr/libexec/podman/conmon'
    path: /usr/libexec/podman/conmon
    version: 'conmon version 2.0.20, commit: '
  cpus: 2
  distribution:
    distribution: ubuntu
    version: "20.04"
  eventLogger: journald
  hostname: "348265431e35"
  idMappings:
    gidmap: null
    uidmap: null
  kernel: 5.4.0-52-generic
  linkmode: dynamic
  memFree: 9199898624
  memTotal: 16186175488
  ociRuntime:
    name: runc
    package: 'runc: /usr/sbin/runc'
    path: /usr/sbin/runc
    version: 'runc version spec: 1.0.1-dev'
  os: linux
  remoteSocket:
    path: /run/podman/podman.sock
  rootless: false
  slirp4netns:
    executable: ""
    package: ""
    version: ""
  swapFree: 1017688064
  swapTotal: 1023406080
  uptime: 95h 4m 40.31s (Approximately 3.96 days)
```

```
registries:
  search:
  - docker.io
  - quay.io
store:
  configFile: /etc/containers/storage.conf
  containerStore:
    number: 0
    paused: 0
    running: 0
    stopped: 0
  graphDriverName: vfs
  graphOptions: {}
  graphRoot: /home/jenkins
  graphStatus: {}
  imageStore:
    number: 3
  runRoot: /home/jenkins
  volumePath: /home/jenkins/volumes
version:
  APIVersion: 2.0.0
  Built: 0
  BuiltTime: Thu Jan  1 05:30:00 1970
  GitCommit: ""
  GoVersion: go1.14
  OsArch: linux/amd64
  Version: 2.1.1

root@348265431e35:/# p images
REPOSITORY                TAG     IMAGE ID      CREATED             SIZE
<none>                    <none>  8448b2303d14  About a minute ago  46.4 MB
docker.io/library/python  alpine  dc68588b1801  8 days ago          46.4 MB
root@348265431e35:/# p run --name python python:alpine pip
ERRO[0000] unable to write pod event: "write unixgram @00104->/run/systemd/journal/socket: sendmsg: no such file or directory"
ERRO[0000] Error preparing container fe12790a5e8643d582ea70481b8df5e68fb574818fa5f1798a98cc5b0daa881f: error creating network namespace for
container fe12790a5e8643d582ea70481b8df5e68fb574818fa5f1798a98cc
5b0daa881f: mount --make-rshared /var/run/netns failed: "operation not permitted"
Error: failed to mount shm tmpfs "/home/jenkins/vfs-containers/fe12790a5e8643d582ea70481b8df5e68fb574818fa5f1798a98cc5b0daa881f/userdata/shm":
operation not permitted
root@348265431e35:/# p --pid=host run --name python python:alpine pip
Error: unknown flag: --pid
root@348265431e35:/# p run --pid=host  --name python python:alpine pip
Error: error creating container storage: the container name "python" is already in use by
```

```
"fe12790a5e8643d582ea70481b8df5e68fb574818fa5f1798a98cc5b0daa881f". You have to remove that container to be able t
o reuse that name.: that name is already in use
root@348265431e35:/# p rm python
ERRO[0000] unable to write pod event: "write unixgram @00107->/run/systemd/journal/socket: sendmsg: no such file or directory"
fe12790a5e8643d582ea70481b8df5e68fb574818fa5f1798a98cc5b0daa881f
root@348265431e35:/# p ps
CONTAINER ID  IMAGE   COMMAND  CREATED  STATUS  PORTS   NAMES
root@348265431e35:/# p ps -a
CONTAINER ID  IMAGE   COMMAND  CREATED  STATUS  PORTS   NAMES
root@348265431e35:/# p rm python
Error: no container with name or ID python found: no such container
root@348265431e35:/# p run --pid=host  --name python python:alpine pip
ERRO[0000] unable to write pod event: "write unixgram @0010b->/run/systemd/journal/socket: sendmsg: no such file or directory"
ERRO[0000] Error preparing container bf4b5f99e7021659aa547c060ac1727294351133fc5a6c877a0d5a7ea2d2ad9b: error creating network namespace for
container bf4b5f99e7021659aa547c060ac1727294351133fc5a6c877a0d5a
7ea2d2ad9b: mount --make-rshared /var/run/netns failed: "operation not permitted"
Error: failed to mount shm tmpfs "/home/jenkins/vfs-containers/bf4b5f99e7021659aa547c060ac1727294351133fc5a6c877a0d5a7ea2d2ad9b/userdata/shm":
operation not permitted
root@348265431e35:/# netns
bash: netns: command not found
root@348265431e35:/# man netns
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, including manpages, you can run the 'unminimize'
command. You will still need to ensure the 'man-db' package is installed.
root@348265431e35:/# p run --pid=host --net=host --name python python:alpine pip
Error: error creating container storage: the container name "python" is already in use by
"bf4b5f99e7021659aa547c060ac1727294351133fc5a6c877a0d5a7ea2d2ad9b". You have to remove that container to be able t
o reuse that name.: that name is already in use
root@348265431e35:/# p rm python
ERRO[0000] unable to write pod event: "write unixgram @0010d->/run/systemd/journal/socket: sendmsg: no such file or directory"
bf4b5f99e7021659aa547c060ac1727294351133fc5a6c877a0d5a7ea2d2ad9b
root@348265431e35:/# p run --pid=host --net=host --name python python:alpine pip
ERRO[0000] unable to write pod event: "write unixgram @0010e->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: failed to mount shm tmpfs "/home/jenkins/vfs-containers/515859c5e4080dce7301696fd99c4dad5d8dd04209f4002d2bac9ad497ce2627/userdata/shm":
operation not permitted
root@348265431e35:/# p rm python
ERRO[0000] unable to write pod event: "write unixgram @0010f->/run/systemd/journal/socket: sendmsg: no such file or directory"
515859c5e4080dce7301696fd99c4dad5d8dd04209f4002d2bac9ad497ce2627
root@348265431e35:/# p run --pid=host --net=host --ipc=host --name python python:alpine pip
ERRO[0000] unable to write pod event: "write unixgram @00110->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: systemd cgroup flag passed, but systemd support for managing cgroups is not available: OCI runtime error
```

```
root@348265431e35:/# p rm python
ERRO[0000] unable to write pod event: "write unixgram @00112->/run/systemd/journal/socket: sendmsg: no such file or directory"
c7ea2c14e9f65a5172d397a8f1c0fd7c287a4e36c8aa5a76ce030231e9eaa30d
root@348265431e35:/# p rm python
Error: no container with name or ID python found: no such container
root@348265431e35:/# p run --pid=host --net=host --ipc=host --cgroupns=host --name python python:alpine pip
ERRO[0000] unable to write pod event: "write unixgram @00114->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: systemd cgroup flag passed, but systemd support for managing cgroups is not available: OCI runtime error
root@348265431e35:/# p rm python
ERRO[0000] unable to write pod event: "write unixgram @00116->/run/systemd/journal/socket: sendmsg: no such file or directory"
4ca3ad4dba97eea6f921bb831b50b2d9e7d5e2adf39816c9737101137e344f10
root@348265431e35:/# p run --pid=host --net=host --ipc=host --cgroups=disabled --name python python:alpine pip
Error: containers not creating CGroups must create a private PID namespace: invalid argument
root@348265431e35:/# p run --pid=host --net=host --ipc=host --cgroups=disabled --cgroupns=host --name python python:alp
ine pip
Error: containers not creating CGroups must create a private PID namespace: invalid argument
root@348265431e35:/# p run --pid=host --net=host --ipc=host --cgroups=noconmon --cgroupns=host --name python python:alp
ine pip
Error: error running container create option: Invalid cgroup mode "noconmon": invalid argument
root@348265431e35:/# p run --pid=host --net=host --ipc=host --cgroups=no-conmon --cgroupns=host --name python python:al
pine pip
ERRO[0000] unable to write pod event: "write unixgram @0011a->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: systemd cgroup flag passed, but systemd support for managing cgroups is not available: OCI runtime error
root@348265431e35:/# exit
```

rootless --> I have not tried. I guess I need to add "USER " in dockerfile and rebuild podman image or maybe there is a flag to run rootless. I will check but kindly advise accordingly and I will try rootless and update.

@mheon

- Now that I seem to be unable to do pip install even outside kubernetes, would you advise I still try disabling seccomp. I use a default k8s config so I will have to read and check what is the default for seccomp on k8s pod containers.
- I assume you mean --cap-add=all so I tried this

```
root@4a76cb278870:/# alias p="podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins"
root@4a76cb278870:/# p run --cap-add=all --name python python:alpine pip
ERRO[0000] unable to write system event: "write unixgram @0011c->/run/systemd/journal/socket: sendmsg: no such file or directory"
Trying to pull docker.io/library/python:alpine...
```

```
Getting image source signatures
Copying blob 55578f60cda7 done
Copying blob 692da2fcb614 done
Copying blob 188c0c94c7c5 done
Copying blob 599e2857d4f0 done
Copying blob 4b3bf1abad55 done
Copying config dc68588b18 done
Writing manifest to image destination
Storing signatures
ERRO[0028] unable to write pod event: "write unixgram @0011c->/run/systemd/journal/socket: sendmsg: no such file or directory"
ERRO[0028] Error preparing container 066877f41fb03dcdc9912d6a091ababf24ca2bd9bb8e6508b094a6e3b0c9acfa: error creating network namespace for
container 066877f41fb03dcdc9912d6a091ababf24ca2bd9bb8e6508b094a6e3b0c9acfa: mount --make-rshared /var/run/netns failed: "operation not permitted"
Error: failed to mount shm tmpfs "/home/jenkins/vfs-containers/066877f41fb03dcdc9912d6a091ababf24ca2bd9bb8e6508b094a6e3b0c9acfa/userdata/shm":
operation not permitted
root@4a76cb278870:/#
[0] 0:sudo*Z
```

This is my podman image's Dockerfile ;

```
__$ cat Dockerfile
FROM ubuntu
RUN  apt-get update -qq && \
     export DEBIAN_FRONTEND=noninteractive && \
    ln -fs /usr/share/zoneinfo/Asia/Kolkata /etc/localtime && \
    apt-get install -y tzdata && \
    dpkg-reconfigure --frontend noninteractive tzdata && \
    apt install -y -qq gnupg curl git
RUN echo 'deb https://download.opensuse.org/repositories/devel:/kubic:/libcontainers:/stable/Debian_10/ /' >
/etc/apt/sources.list.d/devel:kubic:libcontainers:stable.list && \
    curl -L https://download.opensuse.org/repositories/devel:/kubic:/libcontainers:/stable/Debian_10/Release.key | apt-key add - && \
    apt-get update -qq && \
    apt-get -qq -y install slirp4netns fuse-overlayfs podman && \
    touch /long-booyah
```

longwuyuan changed the title ~~error running container: error creating new mount namespace - operation not permitted~~ podman run fails with operation not permitted - podman running in docker container on Oct 30, 2020

mheon on Oct 30, 2020 Member ···

@longwuyuan I meant adding capabilities to the Kubernetes container Podman is running in, not to Podman itself - sorry if I was unclear. That is also where I'd recommend disabling Seccomp, if it's enabled. The outer container seems to be too restrictive for us to run Podman.

longwuyuan on Oct 30, 2020 Author ···

@mheon thank you very much. Its my fault as I am a first time user of podman.

My current thought is that, if i can reproduce the problem without kubernetes.

- I create this dockerfile ;

```
FROM ubuntu
RUN  apt-get update -qq && \
     export DEBIAN_FRONTEND=noninteractive && \
    ln -fs /usr/share/zoneinfo/Asia/Kolkata /etc/localtime && \
    apt-get install -y tzdata && \
    dpkg-reconfigure --frontend noninteractive tzdata && \
    apt install -y -qq gnupg curl git
RUN echo 'deb https://download.opensuse.org/repositories/devel:/kubic:/libcontainers:/stable/Debian_10/ /' >
/etc/apt/sources.list.d/devel:kubic:libcontainers:stable.list && \
    curl -L https://download.opensuse.org/repositories/devel:/kubic:/libcontainers:/stable/Debian_10/Release.key | apt-key add - && \
    apt-get update -qq && \
    apt-get -qq -y install slirp4netns fuse-overlayfs podman && \
    touch /long-booyah_
```

- Then I create a image from above dockerfile

```
$ docker build -t podman .
```

- Then on a ubuntu20 laptop, i just create a container using above mentioned podman image as baseimage ;

```
__$ cat dockerfile.jenkinsagent
FROM podman
```

```
COPY main.py /
COPY requirements.txt /
COPY Dockerfile /

__$ cat main.py


if __name__ == '__main__':
    print('Hello Docker world!')
__me@mypad ~/Documents/github/longwuyuan/jenkins-kubernetes-podman/tmp _master*_
__$ cat requirements.txt
awscli

__$ cat Dockerfile
FROM python:alpine

# Add source code in the container
COPY requirements.txt /
COPY main.py ./main.py
RUN pip install -r requirements.txt

# Define container entry point (could also work with CMD python main.py)
ENTRYPOINT ["python", "main.py"]
__$

$ docker build -t jenkinsagent -f dockerfile.jenkinsagent .
```

- So I get a ubuntu20 based container with podman installed as per docs

```
__$ docker run --name jenkinsagent -ti jenkinsagent bash
root@6bebc8fc41b1:/# ls -l
total 60
-rw-rw-r--   1 root root  245 Oct 30 10:00 Dockerfile
lrwxrwxrwx   1 root root    7 Oct  8 07:01 bin -> usr/bin
drwxr-xr-x   2 root root 4096 Apr 15  2020 boot
drwxr-xr-x   5 root root  360 Oct 30 19:41 dev
drwxr-xr-x   1 root root 4096 Oct 30 19:41 etc
drwxr-xr-x   2 root root 4096 Apr 15  2020 home
lrwxrwxrwx   1 root root    7 Oct  8 07:01 lib -> usr/lib
lrwxrwxrwx   1 root root    9 Oct  8 07:01 lib32 -> usr/lib32
lrwxrwxrwx   1 root root    9 Oct  8 07:01 lib64 -> usr/lib64
lrwxrwxrwx   1 root root   10 Oct  8 07:01 libx32 -> usr/libx32
-rw-r--r--   1 root root    0 Oct 30 09:50 long-booyah
-rw-rw-r--   1 root root   62 Oct 30 09:59 main.py
drwxr-xr-x   2 root root 4096 Oct  8 07:01 media
drwxr-xr-x   2 root root 4096 Oct  8 07:01 mnt
drwxr-xr-x   1 root root 4096 Oct 30 09:50 opt
dr-xr-xr-x 285 root root    0 Oct 30 19:41 proc
-rw-rw-r--   1 root root    7 Oct 30 09:59 requirements.txt
drwx------   2 root root 4096 Oct  8 07:04 root
drwxr-xr-x   1 root root 4096 Oct 23 23:02 run
lrwxrwxrwx   1 root root    8 Oct  8 07:01 sbin -> usr/sbin
drwxr-xr-x   2 root root 4096 Oct  8 07:01 srv
dr-xr-xr-x  13 root root    0 Oct 30 19:41 sys
drwxrwxrwt   1 root root 4096 Oct 30 09:50 tmp
drwxr-xr-x   1 root root 4096 Oct 30 09:50 usr
drwxr-xr-x   1 root root 4096 Oct  8 07:04 var
root@6bebc8fc41b1:/#
root@6bebc8fc41b1:/# which podman
/usr/bin/podman
root@6bebc8fc41b1:/# podman info
Error: mount /var/lib/containers/storage/aufs:/var/lib/containers/storage/aufs, flags: 0x1000: operation not permitted
root@6bebc8fc41b1:/#
root@6bebc8fc41b1:/# mkdir /home/jenkins
root@6bebc8fc41b1:/# alias p="podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins
> ^C
root@6bebc8fc41b1:/# alias p="podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins"
root@6bebc8fc41b1:/# p info
ERRO[0000] unable to write system event: "write unixgram @00123->/run/systemd/journal/socket: sendmsg: no such file or directory"
host:
  arch: amd64
  buildahVersion: 1.16.1
  cgroupManager: systemd
  cgroupVersion: v1
  conmon:
    package: 'conmon: /usr/libexec/podman/conmon'
    path: /usr/libexec/podman/conmon
    version: 'conmon version 2.0.20, commit: '
  cpus: 2
  distribution:
    distribution: ubuntu
    version: "20.04"
  eventLogger: journald
  hostname: 6bebc8fc41b1
  idMappings:
    gidmap: null
    uidmap: null
  kernel: 5.4.0-52-generic
  linkmode: dynamic
  memFree: 8926265344
  memTotal: 16186175488
  ociRuntime:
    name: runc
    package: 'runc: /usr/sbin/runc'
    path: /usr/sbin/runc
    version: 'runc version spec: 1.0.1-dev'
  os: linux
  remoteSocket:
    path: /run/podman/podman.sock
  rootless: false
  slirp4netns:
    executable: ""
    package: ""
    version: ""
  swapFree: 1017712640
  swapTotal: 1023406080
  uptime: 104h 40m 38.37s (Approximately 4.33 days)
registries:
  search:
  - docker.io
  - quay.io
store:
  configFile: /etc/containers/storage.conf
  containerStore:
    number: 0
    paused: 0
    running: 0
    stopped: 0
  graphDriverName: vfs
  graphOptions: {}
  graphRoot: /home/jenkins
  graphStatus: {}
  imageStore:
    number: 0
  runRoot: /home/jenkins
  volumePath: /home/jenkins/volumes
version:
  APIVersion: 2.0.0
  Built: 0
  BuiltTime: Thu Jan  1 05:30:00 1970
  GitCommit: ""
  GoVersion: go1.14
  OsArch: linux/amd64
  Version: 2.1.1

root@6bebc8fc41b1:/#
```

- So I can run podman info with flags as seen above
- And in this container I try to create a image that needs to do pip install

```
root@6bebc8fc41b1:/home/jenkins# pwd
/home/jenkins
root@6bebc8fc41b1:/home/jenkins# alias | grep podman
alias p='podman --storage-driver vfs --runroot /home/jenkins/ --root /home/jenkins'
root@6bebc8fc41b1:/home/jenkins# ls
Dockerfile  libpod  main.py  mounts  requirements.txt  storage.lock  tmp  userns.lock  vfs  vfs-containers  vfs-images  vfs-layers  vfs-locks
root@6bebc8fc41b1:/home/jenkins# cat Dockerfile
FROM python:alpine

# Add source code in the container
COPY requirements.txt /
COPY main.py ./main.py
RUN pip install -r requirements.txt

# Define container entry point (could also work with CMD python main.py)
ENTRYPOINT ["python", "main.py"]
root@6bebc8fc41b1:/home/jenkins# p build -t pythonhelloworld .
STEP 1: FROM python:alpine
Getting image source signatures
Copying blob 599e2857d4f0 done
Copying blob 4b3bf1abad55 done
Copying blob 188c0c94c7c5 done
Copying blob 692da2fcb614 done
Copying blob 55578f60cda7 done
Copying config dc68588b18 done
Writing manifest to image destination
Storing signatures
STEP 2: COPY requirements.txt /
```

```
--> b8018e9bf37
STEP 3: COPY main.py ./main.py
--> 3e923f3cfbd
STEP 4: RUN pip install -r requirements.txt
error running container: error creating new mount namespace for [/bin/sh -c pip install -r requirements.txt]: operation not permitted
ERRO[0042] unable to write build event: "write unixgram @00124->/run/systemd/journal/socket: sendmsg: no such file or directory"
Error: error building at STEP "RUN pip install -r requirements.txt": error while running runtime: exit status 1
root@6bebc8fc41b1:/home/jenkins#
```

- Now I try to build a image that does not do `pip install`

```
root@6bebc8fc41b1:/home/jenkins# cat dockerfile.simple
FROM python:alpine

# Add source code in the container
COPY requirements.txt /
COPY main.py ./main.py

# Define container entry point (could also work with CMD python main.py)
ENTRYPOINT ["python", "main.py"]
root@6bebc8fc41b1:/home/jenkins# p build -t pthonhelloworld-simple -f dockerfile.simple .
STEP 1: FROM python:alpine
STEP 2: COPY requirements.txt /
--> Using cache b8018e9bf37b452d2efb9db1eefd8186e683a0d02f0f0b5cfc57eb05f7fc8673
--> b8018e9bf37
STEP 3: COPY main.py ./main.py
--> Using cache 3e923f3cfbd02d845ba196ba9293f1e699dfb75177d85a0adb95f9c16e3ff80c
--> 3e923f3cfbd
STEP 4: ENTRYPOINT ["python", "main.py"]
STEP 5: COMMIT pthonhelloworld-simple
--> 5fda857bea9
5fda857bea985081a485ae3348d2452121a6bef7f16512b23d758907caedb05e
ERRO[0001] unable to write build event: "write unixgram @00139->/run/systemd/journal/socket: sendmsg: no such file or directory"
root@6bebc8fc41b1:/home/jenkins# p images
REPOSITORY                        TAG     IMAGE ID      CREATED        SIZE
localhost/pthonhelloworld-simple  latest  5fda857bea98  7 seconds ago  46.4 MB
docker.io/library/python          alpine  dc68588b1801  8 days ago     46.4 MB
root@6bebc8fc41b1:/home/jenkins#
```

- As you can see now, the image got built
- There is also a systemd error I don't understand
- But at least the image got built and the only difference was that I removed the `pip install` step in the docckerfil.simple

rhatdan on Oct 30, 2020 Member ···

@longwuyuan I just want to make sure that running podman on the host, not in a Docker container or Kubernetes container works.

Docker has known issues with what it blocks in it's seccomp rules.

longwuyuan on Oct 30, 2020 Author ···

@rhatdan ah ok

- I don't have podman installed on my laptop and the problem I am trying to solve is building docker/podman images inside the jenkins agents that are launched as kubernetes pods, when jenkins master itself is running as a pod.
- I am informed that running DIND with privileged containers mounting the host docker daemon socket is a solution.
- I started exploring podman, so I can build images without privileged containers
- Is there a document/link you can point me at that shows how to use podman in a unprivileged docker container (taking care of seccomp etc)
- If this is not supported, I am sorry for troubling you all but request advise/confirmation if it is even possible to use podman in a unprivilged docker container

rhatdan on Oct 31, 2020 Member ···

Well don't use podman, use Buildah. quay.io/buildah/stable Which has support for Dockerfile
`buildah bud`

longwuyuan on Oct 31, 2020 Author ···

understood. thank you very much

rhatdan closed this as completed on Oct 31, 2020

longwuyuan mentioned this on Nov 1, 2020

✓ Jenkins is unable to execute podman mgoltzsche/jenkins-jnlp-slave#1

github-actions added **locked - please file ...** on Sep 23, 2023

github-actions locked as resolved and limited conversation to collaborators on Sep 23, 2023

Sign up for free **to join this conversation on GitHub.** Already have an account? Sign in to comment

Assignees

No one assigned

Labels

kind/bug **locked - please file new issue/PR**

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development

Code with agent mode ▾

No branches or pull requests

Participants