

Podman Astra Linux

-

- Astra Linux Special Edition .10015-01 (1.7) c 2022-0819SE17 (1.7.2) ;
- Astra Linux Special Edition .10015-10 c 2022-0819SE17 (1.7.2) ;
- Astra Linux Special Edition .10015-17 .
- Astra Linux Special Edition .10015-37 (7.7) c 2022-0819SE17 (1.7.2) ;
- Astra Linux Special Edition .10152-02 (4.7 2022-0926SE47 (4.7.2)

!

Astra Linux, [Astra Linux Special Edition](#).

() [7.2 1]. Docker- rootless-, () [7.2.1] [7.2.7] .

Podman — , , . podman **docker**, (.. , container orchestration) (root).


```
podman      crun. Astra Linux      runc, ..   Astra Linux      podman --runtime=runc --cgroup-manager=cgroupfs.
```

⋮

- , .local/share/containers;
- ;

Podman [Open Container Initiative \(OCI\)](#), docker.

podman docker, . Docker Astra Linux 1.7.

$$\vdots$$

- (pod) — , . : Pods;
- (registry) — , ;
- (repository) — ;
- (tag) — - , .

podman podman. . synaptic :

```
sudo apt install podman
```

```
()
```

```
:
```

```
podman <> <podman->
```

```
:
```

- — ;
- podman — . , docker pod create.

```
podman docker. :
```

```
podman --help
```

```
:
```

Manage pods, containers and images

Usage:

```
podman [options] [command]
```

Available Commands:

attach	Attach to a running container
auto-update	Auto update containers according to their auto-update policy
build	Build an image using instructions from Containerfiles
commit	Create new image based on the changed container
container	Manage containers
cp	Copy files/folders between a container and the local filesystem
create	Create but do not start a container
diff	Display the changes to the object's file system
events	Show podman events
exec	Run a process in a running container
export	Export container's filesystem contents as a tar archive
generate	Generate structured data based on containers, pods or volumes
healthcheck	Manage health checks on containers
help	Help about any command
history	Show history of a specified image
image	Manage images
images	List images in local storage
import	Import a tarball to create a filesystem image
info	Display podman system information
init	Initialize one or more containers
inspect	Display the configuration of object denoted by ID
kill	Kill one or more running containers with a specific signal
kube	Play containers, pods or volumes from a structured file
load	Load image(s) from a tar archive
login	Login to a container registry
logout	Logout of a container registry
logs	Fetch the logs of one or more containers
machine	Manage a virtual machine
manifest	Manipulate manifest lists and image indexes
mount	Mount a working container's root filesystem
network	Manage networks
pause	Pause all the processes in one or more containers
pod	Manage pods
port	List port mappings or a specific mapping for the container
ps	List containers
pull	Pull an image from a registry
push	Push an image to a specified destination
rename	Rename an existing container
restart	Restart one or more containers
rm	Remove one or more containers

rm	Removes one or more images from local storage
run	Run a command in a new container
save	Save image(s) to an archive
search	Search registry for image
secret	Manage secrets
start	Start one or more containers
stats	Display a live stream of container resource usage statistics
stop	Stop one or more containers
system	Manage podman
tag	Add an additional name to a local image
top	Display the running processes of a container
umount	Unmounts working container's root filesystem
unpause	Unpause the processes in one or more containers
unshare	Run a command in a modified user namespace
untag	Remove a name from a local image
update	update an existing container
version	Display the Podman version information
volume	Manage volumes
wait	Block on one or more containers

Options:

--cgroup-manager string	Cgroup manager to use ("cgroupfs" "systemd") (default "systemd")
--common string	Path of the common binary
-c, --connection string	Connection to use for remote Podman service
--events-backend string	Events backend to use ("file" "journald" "none") (default "file")
--help	Help for podman
--hooks-dir strings	Set the OCI hooks directory path (may be set multiple times) (default [/usr/share/containers/oci/hooks.d])
--identity string	path to SSH identity file, (CONTAINER_SSHKEY)
--log-level string	Log messages above specified level (trace, debug, info, warn, warning, error, fatal, panic) (default "warn")
--namespace string	Set the libpod namespace, used to create separate views of the containers and pods on the system
--network-cmd-path string	Path to the command for configuring the network
--network-config-dir string	Path of the configuration directory for networks
--noout	do not output to stdout
-r, --remote	Access remote Podman service
--root string	Path to the root directory in which data, including images, is stored
--runroot string	Path to the 'run directory' where all state information is stored
--runtime string	Path to the OCI-compatible binary used to run containers. (default "runc")
--runtime-flag stringArray	add global flags for the container runtime
--ssh string	define the ssh mode (default "golang")
--storage-driver string	Select which storage driver is used to manage storage of images and containers
--storage-opt stringArray	Used to pass an option to the storage driver
--syslog	Output logging information to syslog as well as the console (default false)
--tmpdir string	Path to the tmp directory for libpod state content.
Note: use the environment variable 'TMPDIR' to change the temporary storage location for container images, '/var/tmp'.	
--url string	URL to access Podman service (CONTAINER_HOST) (default "unix:/run/user /1000/podman/podman.sock")
-v, --version	version for podman
--volumepath string	Path to the volume directory in which volume data is stored

podman- man. podman-<>[<->]., attach :

man podman-attach

podman create — :

man podman-pod-create

podman- docker : <https://github.com/containers/podman/blob/main/transfer.md>.

--log-level . ():

- trace;
- debug;
- info;
- warn ();
- warning;
- error;
- fatal;
- panic.

(stderr). debug:

```
podman --log-level debug ps -a
```

. () podman- login:

```
podman login <_>[:<_>]
```

:

```
podman login repo:5000
```

, , .

:

```
podman logout <_>[:<_>]
```

(registry). podman- pull:

```
podman pull <_>
```

(), , Astra Linux Special Edition 1.7.4 registry.astralinux.ru: registry.astralinux.ru/library/alse:1.7.4.

docker, (podman- run). , Astra Linux Special Edition 1.7.4 registry.astralinux.ru:

```
podman --runtime=runc --cgroup-manager=cgroupfs run -it --rm registry.astralinux.ru/library/alse:1.7.4 /bin/bash
```

:

- registry.fedoraproject.org;
- registry.redhat.io;
- docker.io.

:

```
podman info -f "{{.Registries}}"
```

:

```
map[search:[registry.redhat.io docker.io]]
```

podman search, , , Astra Linux (registry.astralinux.ru):

```
podman search --list-tags registry.astralinux.ru/alse
```

:

NAME	TAG
registry.astralinux.ru/alse	1.7
registry.astralinux.ru/alse	1.7.0
registry.astralinux.ru/alse	1.7.0-mg9.0.0
registry.astralinux.ru/alse	1.7.1
registry.astralinux.ru/alse	1.7.1-mg9.0.0
registry.astralinux.ru/alse	1.7.2
registry.astralinux.ru/alse	1.7.2-mg9.0.0
registry.astralinux.ru/alse	1.7.3
registry.astralinux.ru/alse	1.7.3-mg8.2.1
registry.astralinux.ru/alse	1.7.3-mg9.0.0
registry.astralinux.ru/alse	1.7.3uu1
registry.astralinux.ru/alse	1.7.3uu1-mg9.1.1
registry.astralinux.ru/alse	1.7.3uu1-mg9.1.2
registry.astralinux.ru/alse	1.7.3uu2
registry.astralinux.ru/alse	1.7.3uu2-mg9.2.0
registry.astralinux.ru/alse	1.7.4
registry.astralinux.ru/alse	1.7.4-mg11.2.0
registry.astralinux.ru/alse	1.7.4-mg11.3.0
registry.astralinux.ru/alse	1.7.4uu1
registry.astralinux.ru/alse	1.7.4uu1-mg11.3.0
registry.astralinux.ru/alse	latest

, /etc/containers/registries.conf :



unqualified-search-registries , .. ,
' ().

```
unqualified-search-registries = [ 'registry.redhat.io', 'docker.io' ]
```

, .

. unqualified-search-registries. , [docker-registry](#) :

```
[[registry]]  
location="registry:5000"  
insecure=true
```

:

- registry — (IP-). IP- ;
- 5000 — IP- (docker-registry);
- insecure=true — HTTP (docker-registry).

/etc/containers/registries.conf man:

```
man containers-registries.conf
```

podman- images:

```
podman images
```

:

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
registry.astralinux.ru/library/alse	1.7.4	557b8fe356eb	7 weeks ago	98.4 MB

podman- run, :

```
podman run -it --rm registry.astralinux.ru/library/alse:1.7.4 /bin/bash
```

podman- -d:

```
podman run -d <_>
```

-. --mount, :

```
podman run --mount type=bind,source=<_>,target=<_> <_>
```

() docker- ps:

```
podman ps
```

() -a:

```
podman ps -a
```

:

CONTAINER ID	IMAGE	PORTS	NAMES	COMMAND	CREATED
STATUS					
0468d9f62e2d	registry.astralinux.ru/library/alse:1.7.4			/bin/bash	12 seconds ago
ago	priceless_hertz				Exited (0) 5 seconds ago

(CONTAINER ID) (NAMES).

podman- start, :

```
podman start <_>
```

podman- stop:

```
podman stop <_>
```



Podman

:

```
podman rm <_>
```

, ,

:

```
podman inspect <_>
```

, --format, :

```
podman inspect <_> --format '{{.NetworkSettings.IPAddress}}'
```

podman- logs:

```
podman logs <_>
```

podman- stats:

```
podman stats
```

, (-- 5). --no-stream:

```
podman stats --no-stream
```



Podman

:

```
podman rmi <_>
```

1. dockerfile , (registry.astralinux.ru/library/alse:1.7.4) (mkdir /testdir echo test > /testdir/testfile):

```
echo -e "FROM registry.astralinux.ru/library/alse:1.7.4\nRUN mkdir /testdir\nRUN echo test > /testdir/testfile" > Dockerfile
```

2. :

```
podman --runtime=runc --cgroup-manager=cgroupfs build -t testbuild .
```

Docker- Astra Linux, docker podman:



debootstrap:

```
sudo apt install debootstrap
```

:

- REPO —, debootstrap (— <https://dl.astralinux.ru/astra/stable/orel/repository>);
- IMAGE — (- astra_linux_ce_2.12);
- ROOTFS_IMAGE — (- <_>-rootfs);
- CODENAME — (- orel).

:

```
#!/bin/sh
if [ -z $REPO ]; then
    REPO="https://dl.astralinux.ru/astra/stable/orel/repository"
fi
set -e

IMAGE="${IMAGE:-astra_linux_ce_2.12}"
ROOTFS_IMAGE="$IMAGE-rootfs"
CODENAME="${CODENAME:-orel}"

TMPDIR=`mktemp -d`
cd $TMPDIR

cleanup() {
    cd $HOME
    # debootstrap leaves mounted /proc and /sys folders in chroot when terminated by Ctrl-C
    sudo umount $TMPDIR/proc $TMPDIR/sys 2>&1 >/dev/null || true
    # Delete temporary data at exit
    sudo rm -rf $TMPDIR
}
trap cleanup EXIT
sudo -E debootstrap --no-check-gpg --variant=minbase --include=apt-transport-https,ca-certificates \
--components=main,contrib,non-free "$CODENAME" ./chroot "$REPO"
trap - EXIT
echo "deb $REPO $CODENAME contrib main non-free" | sudo tee ./chroot/etc/apt/sources.list
podman rmi "$ROOTFS_IMAGE" || true
sudo tar -C chroot -c . | podman import - "$ROOTFS_IMAGE"
podman rmi "$IMAGE" || true
podman --runtime=runc --cgroup-manager=cgroupfs build --network=host --no-cache=true -t "$IMAGE" - <<EOF
FROM $ROOTFS_IMAGE
ENV TERM xterm-256color
ENV DEBIAN_FRONTEND noninteractive
RUN apt-get update
WORKDIR /
CMD bash
EOF

printf 'podman image `%s` has been generated\n' "$IMAGE"
exit 0
```

Astra Linux Special Edition 1.7 - (, build.sh):

```
REPO="https://dl.astralinux.ru/astra/stable/1.7_x86-64/repository-main"
IMAGE="alse1.7" CODENAME="1.7_x86-64" bash build.sh
```

:


```
podman image `alse1.7` has been generated
```

docker-registry

```
podman docker docker-registry, . . :
```

```
sudo apt install docker-registry
```

:

- docker-registry, ;
- (/var/lib/docker-registry/);
- /etc/docker/registry/config.yml :

```
version: 0.1
log:
  fields:
    service: registry
storage:
  cache:
    blobdescriptor: inmemory
  filesystem:
    rootdirectory: /var/lib/docker-registry
delete:
  enabled: true
http:
  addr: :5000
  headers:
    X-Content-Type-Options: [nosniff]
auth:
  htpasswd:
    realm: basic-realm
    path: /etc/docker/registry
health:
  storagedriver:
    enabled: true
    interval: 10s
    threshold: 3
```

() :

- IP-5000 ;
- HTTP;
- (.).

/usr/share/doc/docker-registry/ docker-registry.

, podman HTTP (HTTPS) "", /etc/containers/registries.conf insecure, :

```
[[registry]]
location = "localhost:5000"
insecure = true
```

():

1. :

```
auth:
  httpasswd:
    realm: basic-realm
    path: /etc/docker/registry
```

2. docker-registry:

```
sudo systemctl restart docker-registry
```

():

1. apache2-utils :

```
sudo apt install apache2-utils
```

2. ,, /etc/docker/registry-pass:

```
sudo touch /etc/docker/registry-pass
```

3. , docker-registry :

```
sudo chmod 640 /etc/docker/registry-pass
sudo setfacl -m u:docker-registry:r /etc/docker/registry-pass
```

4. /etc/docker/registry/config.yml (/etc/docker/registry-pass) auth:httpasswd:path:

```
auth:
  httpasswd:
    realm: basic-realm
    path: /etc/docker/registry-pass
```

5. docker-registry:

```
sudo systemctl restart docker-registry
```

6. ():

```
sudo htpasswd -B -b /etc/docker/registry-pass <> <>
```

-B (bcrypt).

-b , . , .

podman



(<https://thenewstack.io/tutorial-host-a-local-podman-image-registry/>).

, :

- docker-registry , ;
- IP- 5000;
- , ;
- localhost/else1.7.

:

1. , , :

```
podman tag alse1.7 localhost:5000/alse1.7
```

2. , :

```
podman images
```

REPOSITORY	TAG	IMAGE
ID	CREATED	SIZE
localhost/alse1.7	latest	8359adc98b69 2 hours ago 209 MB
localhost:5000/alse1.7	latest	8359adc98b69 2 hours ago 209 MB

3. "" :

```
podman push localhost:5000/alse1.7
```

```
Getting image source signatures
Copying blob e5a6e1aacdde done
Copying blob 39122d40d697 done
Copying config 8359adc98b done
Writing manifest to image destination
Storing signatures
```

4. , :

```
podman search localhost:5000/alse
```

NAME	DESCRIPTION
localhost:5000/alse1.7	

IP- (-10.107.0.227):

```
podman search 10.107.0.227:5000/alse
```

NAME	DESCRIPTION
10.107.0.227:5000/alse1.7	

()

:

```
podman --cgroup-manager cgroupfs pod create <_>
```

:

- ;
- ();
- (infra-), podman-pause. , . () .

-, ().

:

```
podman pod ps
```

:

POD ID	NAME	STATUS	CREATED	INFRA ID	# OF CONTAINERS
312fb1c5553f	testpod	Created	22 minutes ago	76972a488dbb	1

(POD ID, --no-trunc), (NAME), infra- (INFRA ID). (# OF CONTAINERS) — infra-. (STATUS) :

- Created — ;
- Running — ;
- Stopped — , ;
- Exited — .
- Dead — .

:

```
podman pod ps --ctr-names
```

:

POD ID	NAME	STATUS	CREATED	INFRA ID	NAMES
312fb1c5553f	testpod	Created	56 minutes ago	76972a488dbb	friendly_rhodes,312fb1c5553f-infra,brave_turing

NAMES .

podman- --pod=<_>, :

```
podman create --pod=testpod nginx
```

:

		Description
clone	podman-pod-clone(1)	.
create	podman-pod-create(1)	.
exists	podman-pod-exists(1)	, .
inspect	podman-pod-inspect(1)	.
kill	podman-pod-kill(1)	.
logs	podman-pod-logs(1)	.
pause	podman-pod-pause(1)	.
prune	podman-pod-prune(1)	.
ps	podman-pod-ps(1)	.
restart	podman-pod-restart(1)	.

rm	podman-pod-rm(1)	.
start	podman-pod-start(1)	.
stats	podman-pod-stats(1)	.
stop	podman-pod-stop(1)	.
top	podman-pod-top(1)	.
unpause	podman-pod-unpause(1)	.

Astra Linux Special Edition

podman

podman

podman :

```
sudo -u <_> -H -i podman <podman->
```

:

- -u <_> —, () ;
- -H —, HOME ;
- -i —, .

podman

pdp-exec:

```
sudo pdp-exec -u macuser -l "1:0:0:0" -- bash -c 'HOME=/home/.pdp/macuser/11i0c0x0t0x0 ; TMP=/var/private/tmp/11i0c0x0t0x0 ; cd $HOME ; podman images'
```