Rocky Enterprise Linux 9.2 Manual Pages on command 'buildah-pull.1'

$ man buildah-pull.1

buildah-pull(1)   General Commands Manual   buildah-pull(1)

NAME

    buildah-pull - Pull an image from a registry.

SYNOPSIS

    buildah pull [options] image

DESCRIPTION

    Pulls an image based upon the specified input. It supports all trans?

    ports from containers-transports(5) (see examples below). If no trans?

    port is specified, the input is subject to short-name resolution (see

    containers-registries.conf(5)) and the docker (i.e., container reg?

    istry) transport is used.

  DEPENDENCIES

    Buildah resolves the path to the registry to pull from by using the

    /etc/containers/registries.conf file,   containers-registries.conf(5).

    If the buildah pull command fails with an "image not known" error,

    first verify that the registries.conf file is installed and configured

    appropriately.

RETURN VALUE

The image ID of the image that was pulled. On error 1 is returned.

OPTIONS

--all-tags, -a

All tagged images in the repository will be pulled.

--arch="ARCH"

Set the ARCH of the image to be pulled to the provided value instead of

using the architecture of the host. (Examples: arm, arm64, 386, amd64,

ppc64le, s390x)

--authfile path

Path of the authentication file. Default is ${XDG_\RUNTIME_DIR}/con?

tainers/auth.json. If XDG_RUNTIME_DIR is not set, the default is

/run/containers/$UID/auth.json. This file is created using buildah lo?

gin.

If the authorization state is not found there, $HOME/.docker/con?

fig.json is checked, which is set using docker login.

Note: You can also override the default path of the authentication file

by setting the REGISTRY_AUTH_FILE environment variable. export REG?

ISTRY_AUTH_FILE=path

--cert-dir path

Use certificates at path (*.crt, *.cert, *.key) to connect to the reg?

istry. The default certificates directory is /etc/containers/certs.d.

--creds creds

The [username[:password]] to use to authenticate with the registry if

required. If one or both values are not supplied, a command line

prompt will appear and the value can be entered. The password is en?

tered without echo.

--decryption-key key[:passphrase]

The [key[:passphrase]] to be used for decryption of images. Key can

point to keys and/or certificates. Decryption will be tried with all

keys. If the key is protected by a passphrase, it is required to be

passed in the argument and omitted otherwise.

--os="OS"

Set the OS of the image to be pulled instead of using the current oper?

ating system of the host.

--platform="OS/ARCH[/VARIANT]"

Set the OS/ARCH of the image to be pulled to the provided value instead

of using the current operating system and architecture of the host (for

example linux/arm).

OS/ARCH pairs are those used by the Go Programming Language. In sev?

eral cases the ARCH value for a platform differs from one produced by

other tools such as the arch command. Valid OS and architecture name

combinations are listed as values for $GOOS   and $GOARCH   at

https://golang.org/doc/install/source#environment,   and can also be

found by running go tool dist list.

NOTE: The --platform option may not be used in combination with the

--arch, --os, or --variant options.

--policy=always|missing|never|newer

Pull image policy. The default is missing.

     ? always: Always pull the image and throw an error if the pull

       fails.

     ? missing: Pull the image only if it could not be found in the

       local containers storage. Throw an error if no image could be

       found and the pull fails.

     ? never: Never pull the image but use the one from the local

       containers storage.   Throw an error if no image could be

       found.

     ? newer: Pull if the image on the registry is newer than the one

       in the local containers storage. An image is considered to be

       newer when the digests are different.   Comparing the time

       stamps is prone to errors. Pull errors are suppressed if a

       local image was found.

--quiet, -q

If an image needs to be pulled from the registry, suppress progress

output.

--remove-signatures

Don't copy signatures when pulling images.

--retry attempts

Number of times to retry in case of failure when performing pull of im?

ages from registry.

Defaults to 3.

--retry-delay duration

Duration of delay between retry attempts in case of failure when per?

forming pull of images from registry.

Defaults to 2s.

--tls-verify bool-value

Require HTTPS and verification of certificates when talking to con?

tainer registries (defaults to true). TLS verification cannot be used

when talking to an insecure registry.

--variant=""

Set the architecture variant of the image to be pulled.

EXAMPLE

buildah pull imagename

buildah pull docker://myregistry.example.com/imagename

buildah pull docker-daemon:imagename:imagetag

buildah pull docker-archive:filename

buildah pull oci-archive:filename

buildah pull dir:directoryname

buildah pull --tls-verify=false myregistry/myrepository/imagename:im?

agetag

buildah pull --creds=myusername:mypassword --cert-dir ~/auth myreg?

istry/myrepository/imagename:imagetag

buildah pull --authfile=/tmp/auths/myauths.json myregistry/myreposi?

tory/imagename:imagetag

buildah pull --arch=aarch64 myregistry/myrepository/imagename:imagetag

buildah pull --arch=arm --variant=v7 myregistry/myrepository/image?

name:imagetag

ENVIRONMENT

BUILD_REGISTRY_SOURCES

BUILD_REGISTRY_SOURCES, if set, is treated as a JSON object which con?

tains lists of registry names under the keys insecureRegistries, blockedRegistries, and allowedRegistries.

When pulling an image from a registry, if the name of the registry matches any of the items in the blockedRegistries list, the image pull attempt is denied. If there are registries in the allowedRegistries list, and the registry's name is not in the list, the pull attempt is denied.

TMPDIR The TMPDIR environment variable allows the user to specify where temporary files are stored while pulling and pushing images. Defaults to '/var/tmp'.

FILES

registries.conf (/etc/containers/registries.conf)

registries.conf is the configuration file which specifies which con‐ tainer registries should be consulted when completing image names which do not include a registry or domain portion.

policy.json (/etc/containers/policy.json)

Signature policy file. This defines the trust policy for container im‐ ages. Controls which container registries can be used for image, and whether or not the tool should trust the images.

SEE ALSO

buildah(1), buildah-from(1), buildah-login(1), docker-login(1), con‐ tainers-policy.json(5), containers-registries.conf(5), containers-transports(5)