



**Full credit is given to the above companies including the Operating System (OS) that this PDF file was generated!**

### ***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 transports from containers-transport(5) (see examples below). If no transport is specified, the input is subject to short-name resolution (see containers-registries.conf(5)) and the docker (i.e., container registry) 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 `${XDG_RUNTIME_DIR}/containers/auth.json`. If `XDG_RUNTIME_DIR` is not set, the default is `/run/containers/$UID/auth.json`. This file is created using `buildah login`.

If the authorization state is not found there, `$HOME/.docker/config.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 REGISTRY_AUTH_FILE=path`

`--cert-dir path`

Use certificates at path (`*.crt`, `*.cert`, `*.key`) to connect to the registry. 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 entered 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.

`--quiet, -q`

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

`--os="OS"`

Set the OS of the image to be pulled instead of using the current operating 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`). If `--platform` is set, then the values of the `--arch`, `--os`, and `--variant` options will be overridden.

OS/ARCH pairs are those used by the Go Programming Language. In several 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`.

`--policy=always|missing|never`

Pull image policy. The default is missing.

? missing: attempt to pull the latest image from the registries listed in `registries.conf` if a local image does not exist. Raise an error if the image is not in any listed registry and is not present locally.

? always: Pull the image from the first registry it is found in as listed in `registries.conf`. Raise an error if not found in the registries, even if the image is present locally.

? never: do not pull the image from the registry, use only the local version. Raise an error if the image is not present locally.

`--remove-signatures`

Don't copy signatures when pulling images.

`--tls-verify bool-value`

Require HTTPS and verification of certificates when talking to container 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:imagetag
```

```
buildah pull --creds=myusername:mypassword --cert-dir /auth myregistry/myrepository/imagename:imagetag
```

```
buildah pull --authfile=/tmp/auths/myauths.json myregistry/myrepository/imagename:imagetag
```

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

```
buildah pull --arch=arm --variant=v7 myregistry/myrepository/imagename:imagetag
```

## ENVIRONMENT

`BUILD_REGISTRY_SOURCES`

`BUILD_REGISTRY_SOURCES`, if set, is treated as a JSON object which contains lists of registries.

istry 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 container 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 images. 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)`, `containers-policy.json(5)`, `containers-registries.conf(5)`, `containers-transport(5)`

`buildah`

July 2018

`buildah-pull(1)`