Rocky Enterprise Linux 9.2 Manual Pages on command 'podman-image-trust.1'

$ man podman-image-trust.1

podman-image-trust(1)() podman-image-trust(1)()

NAME

podman-image-trust - Manage container registry image trust policy

SYNOPSIS

podman image trust set|show [options] registry[/repository]

DESCRIPTION

Manages which registries you trust as a source of container images based on its location.

(This option is not available with the remote Podman client)

The location is determined by the transport and the registry host of the image. Using this container image docker://docker.io/library/busybox as an example, docker is the transport and docker.io is the registry host.

Trust is defined in /etc/containers/policy.json and is enforced when a user attempts to pull a remote image from a registry. The trust policy in policy.json describes a registry scope (registry and/or repository) for the trust. This trust can use public keys for signed images.

The scope of the trust is evaluated from most specific to the least specific. In other words, a policy may be defined for an entire registry. Or it could be defined for a par?ticular repository in that registry. Or it could be defined down to a specific signed im?age inside of the registry.

For example, the following list includes valid scope values that could be used in pol?icy.json from most specific to the least specific:

docker.io/library/busybox:notlatest docker.io/library/busybox docker.io/library docker.io

If no configuration is found for any of these scopes, the default value (specified by us?

ing "default" instead of REGISTRY[/REPOSITORY]) is used.

Trust type provides a way to:

Allowlist ("accept") or Denylist ("reject") registries or Require signature (?signedBy?).

Trust may be updated using the command podman image trust set for an existing trust scope.

OPTIONS

--help, -h

Print usage statement.

--pubkeysfile=KEY1, -f

A path to an exported public key on the local system. Key paths will be referenced in policy.json. Any path to a file may be used but locating the file in /etc/pki/containers is recommended. Options may be used multiple times to require an image be signed by multiple keys. The --pubkeysfile option is required for the signedBy type.

--type=value, -t

The trust type for this policy entry.

Accepted values:

signedBy (default): Require signatures with corresponding list of
public keys

accept: do not require any signatures for this
registry scope

reject: do not accept images for this registry scope

show OPTIONS

--raw

Output trust policy file as raw JSON

--json, -j

Output trust as JSON for machine parsing

EXAMPLES

Accept all unsigned images from a registry

```
sudo podman image trust set --type accept docker.io
```

Modify default trust policy

```
sudo podman image trust set -t reject default
```

Display system trust policy

```
sudo podman image trust show
```

Display trust policy file

```
sudo podman image trust show --raw
```

Display trust as JSON

```
sudo podman image trust show --json
```

SEE ALSO

containers-policy.json(5)

HISTORY

January 2019, updated by Tom Sweeney (tsweeney at redhat dot com) December 2018, origi? nally compiled by Qi Wang (qiwan at redhat dot com)