THALES

CTE for Kubernetes Signing Tool

REFERENCE GUIDE

CTE Kubernetes Signing Tool

- Introduction to the CTE Signing Tool
- Installing and Using the CTE Signing Tool

Introduction to the CTE Signing Tool

CTE for Kubernetes uses standard signature sets to test if a pod in the cluster has permission to use a CTE for Kubernetes Storage Group policy. Currently, CTE for Kubernetes is unable to pass signature sets to CipherTrust Manager like CipherTrust Transparent Encryption can. To alleviate this problem, Thales has created a utility that can populate CipherTrust Manager with signatures from other containers.

Specifically, the utility:

1. Calculates a list of binary paths.
2. Includes the URL and tag of a container from which to get the image.
3. Collects CipherTrust Manager authentication credentials.
4. Downloads the container image and collects signatures from it.
5. Calculates the SHA256 sum of all of the binary paths requested.
6. Requests authentication with CipherTrust Manager.
7. Pushes signatures collected from other containers to CipherTrust Manager.

Obtaining the Tool

This tool is available from the Thales Support Portal. Search for **CipherTrust Transparent Encryption for Kubernetes**. The file will be a tar file. Decompress it with `tar -xf`.

Installing and Using the CTE Signing Tool

To use this tool to gather signatures from other container images and then push them to CipherTrust Manager, complete the following steps:

1. Download a container image:
   a. From a **public** repository, type:

```
./cte-sign --cdi --image=<image name> --tag=<image version>
```

   b. From a **private** repository, type:

```
./cte-sign --cdi --image=<image name with url> --tag=<image version> --repo-user=<repo username> --repo-password=<repo password>
```

2. Get a list of signature set IDs from CipherTrust Manager, type:

```
./cte-sign --cm --signature-sets list --ip=<CM IP> --user=<CM username> --password=<CM password> --cm-domain=<CM Domain>
```

3. Create a signature set for the process set or Container Image Digest set, type:

```
./cte-sign --cm --signature-sets create --sigset-name=<signature-set-name> --sigset-type=<signature-set-type> --ip=<CM IP> --user=<CM username> --password=<CM password> --cm-domain=<CM Domain>
```

4. Send the signatures collected from the downloaded container image to CipherTrust Manager in a signature set ID, type:

```
./cte-sign --cm --signature-sets add-signatures --sigset-name=<signature-set-name> --path=<source-path> --ip=<CM IP> --user=<CM username> --password=<CM password> --cm-domain=<CM Domain>
```

5. Cleanup and remove the image directory, type:

```
./cte-sign --cleanup
```

6. Retrieve container image digests

   a. Retrieve digests for pod spec yaml file:

```
./cte-sign --digest --podspec=<pod spec file name> --kubeconfig=<kubeconfig file path>
```

   b. Retrieve digest for public image:

```
./cte-sign --digest --image=<image name> --tag=<image tag>
```

   c. Retrieve digest for private image:

```
./cte-sign --digest --image=<image name> --tag=<image tag> --repo-user=<repo username> --repo-password=<repo password>
```

7. Retrieve and push Container Image Digest to CipherTrust Manager

   a. Retrieve and push for public image:

```
./cte-sign --digest --push-to-cm --image=<image name> --tag=<image tag> --ip=<CM IP> --user=<CM username> --password=<CM password> --sigset-name=<signature-set-name> --cm-domain=<CM Domain>
```

   b. Retrieve and push for private image:

```
./cte-sign --digest --push-to-cm --image=<image name> --tag=<image tag> --repo-user=<repo username> --repo-password=<repo password> --ip=<CM IP> --user=<CM username> --password=<CM password> --sigset-name=<signature-set-name>--cm-domain=<CM Domain>
```

c. Retrieve and push for public/private images using pod spec yaml file:

```
./cte-sign --digest --push-to-cm --podspec=<pod spec file name> --ip=<CM IP> --user=<CM username> --password=<CM password> --sigset-name=<signature-set-name> --cm-domain=<CM Domain>
```

CLI Argument Definitions

Argument	Definition
--cleanup	Delete the container image files and directories.
--cm-domain	(**Optional**) Provide this option only if an operation belongs to a specific domain, other than the root domain.
--image	Container image name/URL.
--ip	CipherTrust Manager IP address.
--kubeconfig	`kubeconfig` file for retrieving pod digests.
--password	Password of CipherTrust Manager credential.
--path	The binary path from the downloaded container image, for the files that need to be pushed to CipherTrust Manager. ex: `/usr/bin`
--podspec	Pod specification yaml file.
--repo-password	Password/AccessToken for the private repository.
--repo-user	Username for private repository access.
--sigset-name	The signature set name where signatures will be contained.
--sigset-type	The signature set type. **Application**: for process signatures. **Container-Image** for container image signature.
--tag	Container image version.
--user	Username of CipherTrust Manager credential.

Support Contacts

If you encounter a problem while installing, registering, or operating the product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at Thales Customer Support, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

Tip

You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@Thales.com.