

Leveraging the Little Known Features of Artifact Hub

Matt Farina



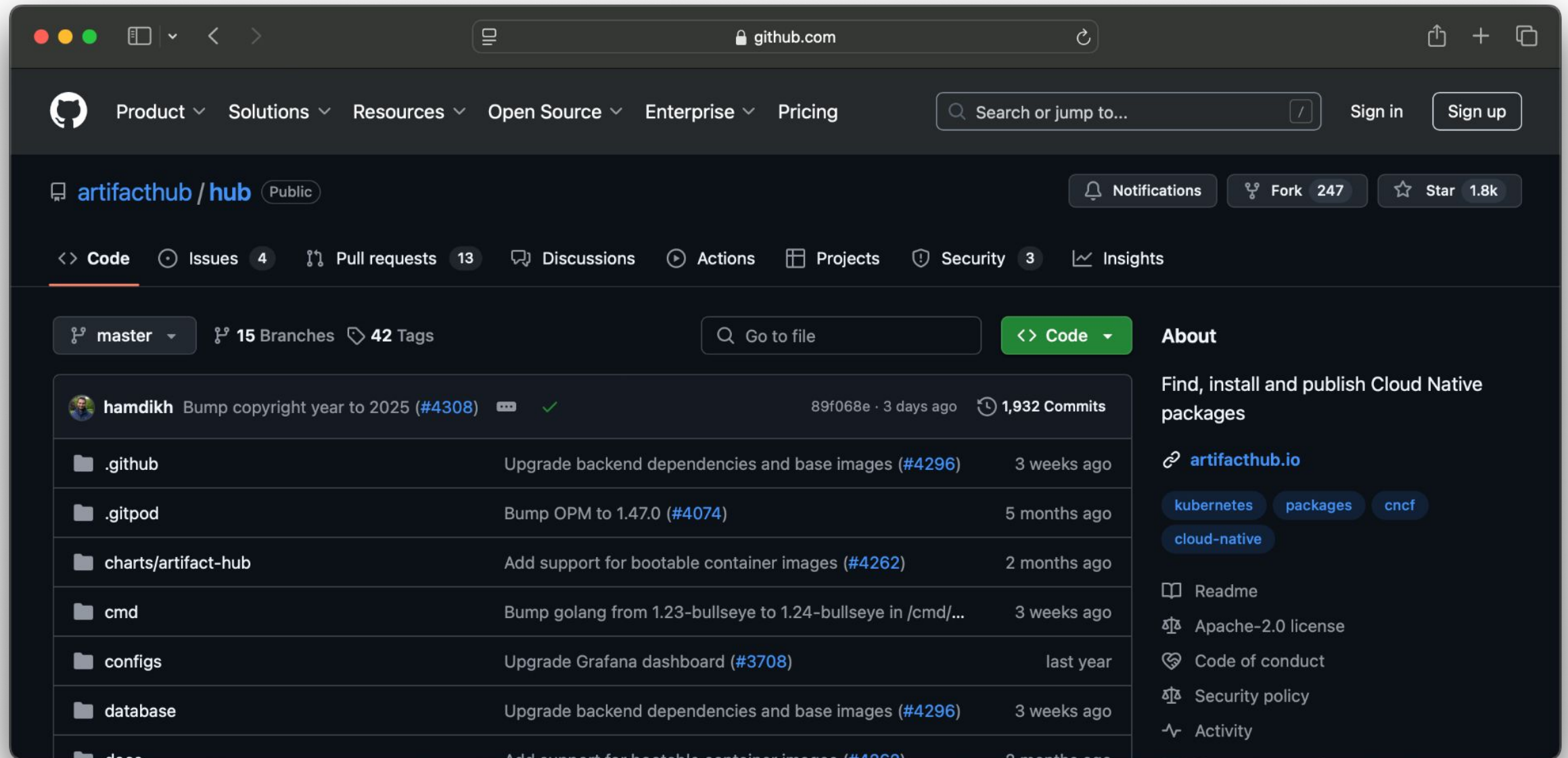
KubeCon



CloudNativeCon

Europe 2025





The screenshot shows the GitHub repository page for `artifacthub/hub`. The repository is public and has 15 branches and 42 tags. The main branch is `master`. The repository has 1,932 commits and 247 forks. The repository is described as "Find, install and publish Cloud Native packages". The repository includes a README, Apache-2.0 license, Code of conduct, Security policy, and Activity.

artifacthub / hub Public

Notifications Fork 247 Star 1.8k

<> Code Issues 4 Pull requests 13 Discussions Actions Projects Security 3 Insights

master 15 Branches 42 Tags Go to file <> Code

hamdikh Bump copyright year to 2025 (#4308) 89f068e · 3 days ago 1,932 Commits

.github	Upgrade backend dependencies and base images (#4296)	3 weeks ago
.gitpod	Bump OPM to 1.47.0 (#4074)	5 months ago
charts/artifact-hub	Add support for bootable container images (#4262)	2 months ago
cmd	Bump golang from 1.23-bullseye to 1.24-bullseye in /cmd/...	3 weeks ago
configs	Upgrade Grafana dashboard (#3708)	last year
database	Upgrade backend dependencies and base images (#4296)	3 weeks ago
docs	Add support for bootable container images (#4262)	2 months ago

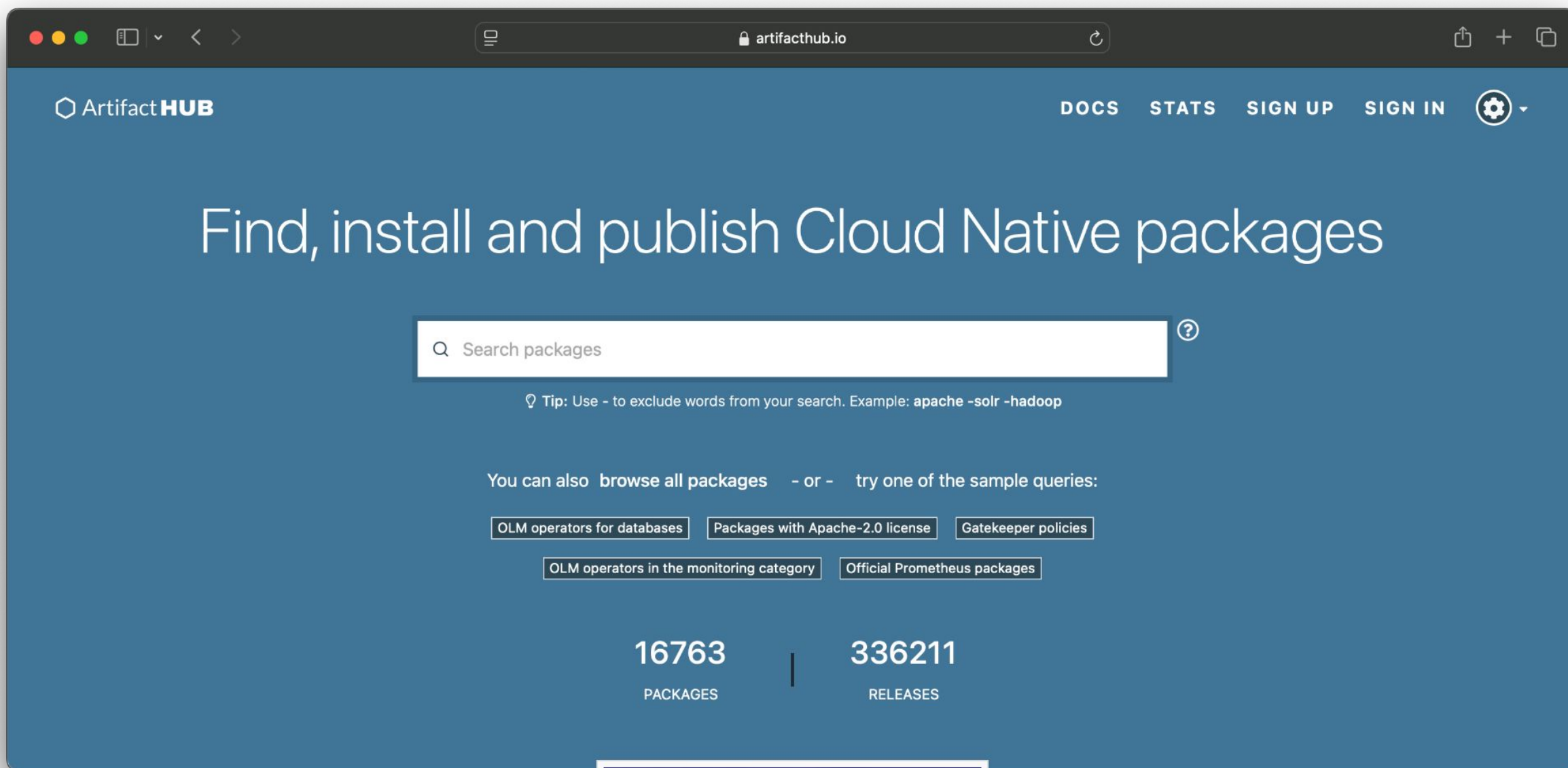
About

Find, install and publish Cloud Native packages

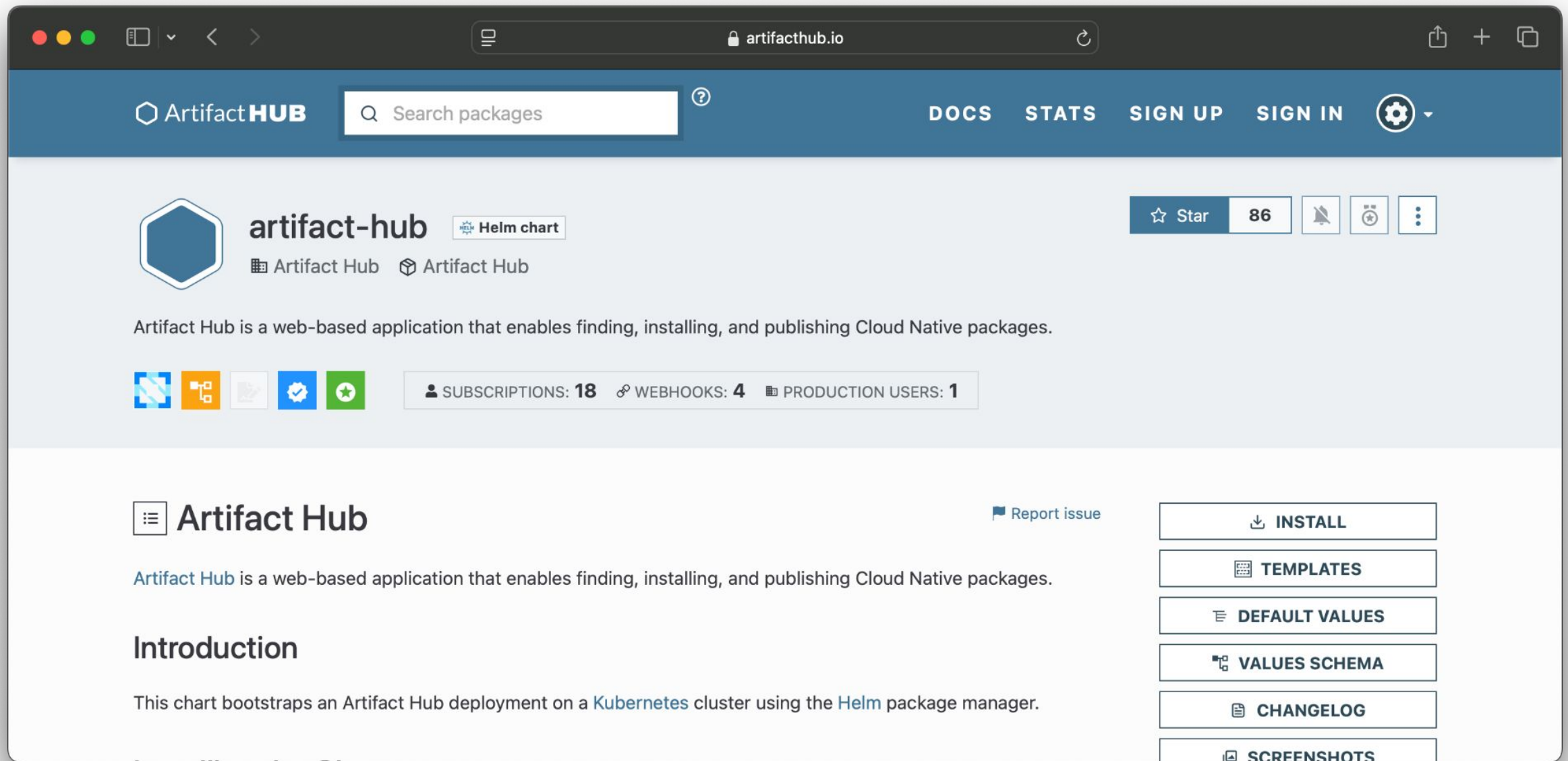
artifacthub.io

kubernetes packages cncf cloud-native

Readme Apache-2.0 license Code of conduct Security policy Activity



Artifact Hub on artifacthub.io



The screenshot shows the artifacthub.io website. The top navigation bar includes the Artifact HUB logo, a search bar, and links for DOCS, STATS, SIGN UP, and SIGN IN. The main content area features the artifact-hub Helm chart, which includes a description, a list of production users, and a sidebar with links to INSTALL, TEMPLATES, DEFAULT VALUES, VALUES SCHEMA, CHANGELOG, and SCREENSHOTS.

artifacthub.io

Artifact HUB

Search packages

DOCS STATS SIGN UP SIGN IN

artifact-hub

Helm chart

Star 86

Artifact Hub

Artifact Hub

Artifact Hub is a web-based application that enables finding, installing, and publishing Cloud Native packages.

SUBSCRIPTIONS: 18 WEBHOOKS: 4 PRODUCTION USERS: 1

Artifact Hub

Report issue

INSTALL

TEMPLATES

DEFAULT VALUES

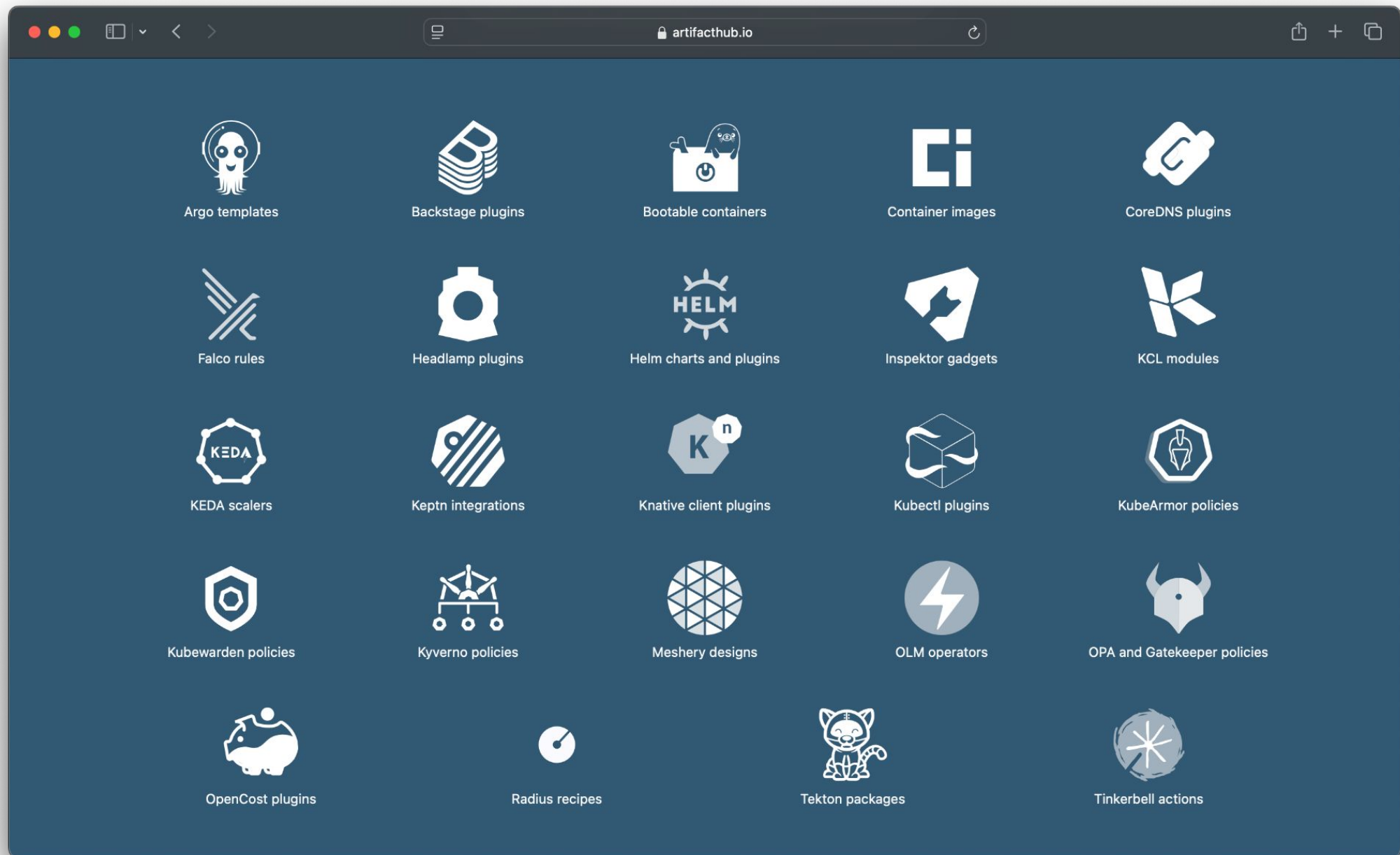
VALUES SCHEMA

CHANGELOG

SCREENSHOTS

Introduction

This chart bootstraps an Artifact Hub deployment on a [Kubernetes](#) cluster using the [Helm](#) package manager.



Argo templates



Backstage plugins



Bootable containers



Container images



CoreDNS plugins



Falco rules



Headlamp plugins



Helm charts and plugins



Inspektor gadgets



KCL modules



KEDA scalars



Keptn integrations



Knative client plugins



Kubectl plugins



KubeArmor policies



Kubewarden policies



Kyverno policies



Meshery designs



OLM operators



OPA and Gatekeeper policies



OpenCost plugins



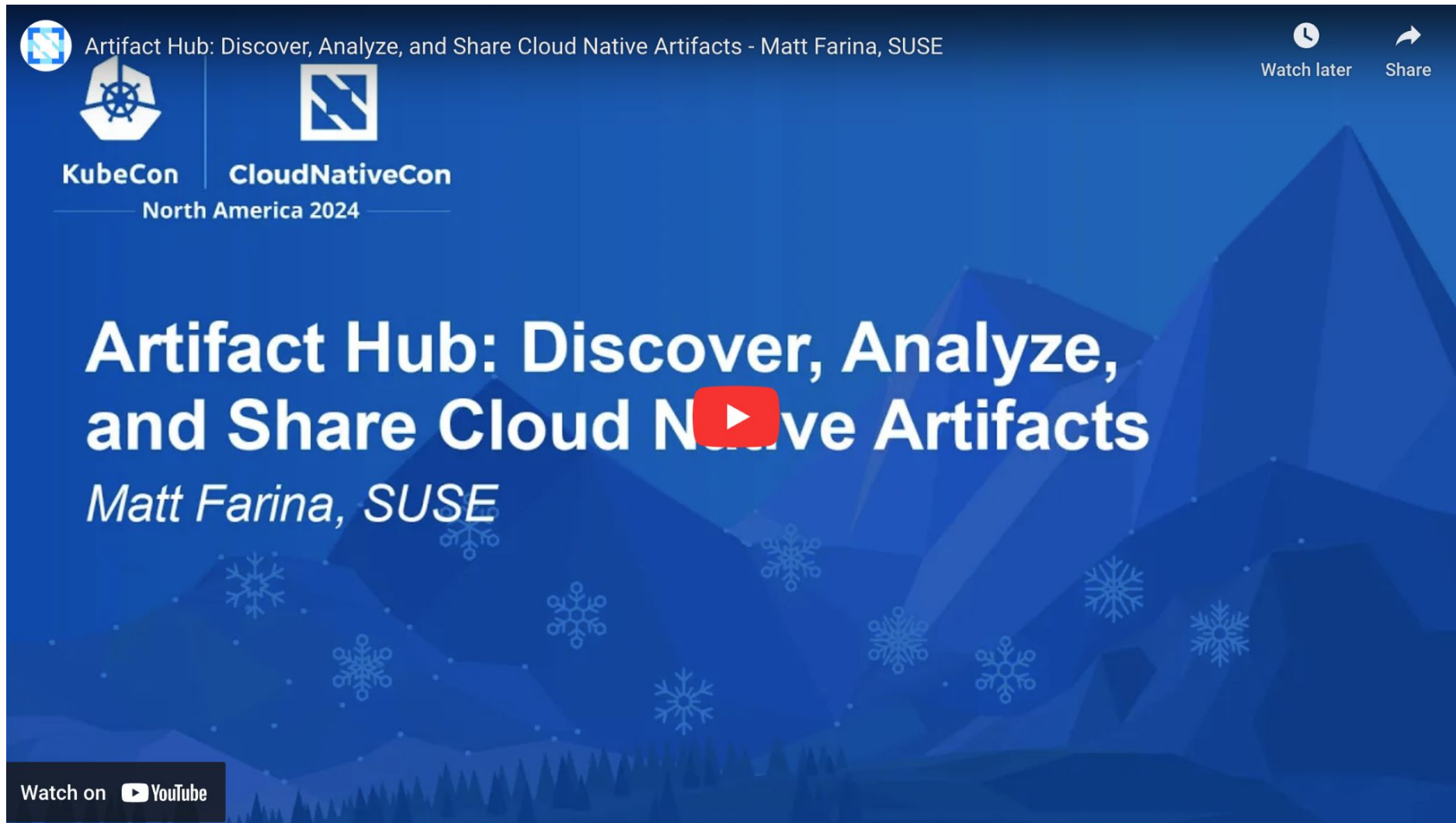
Radius recipes



Tekton packages



Tinkerbell actions



<https://sched.co/1howN>

Who Is This Guy?



KubeCon



CloudNativeCon

Europe 2025



Matt Farina

mattfarina.com

@mattfarina



The Developers



Sergio and **Cintia** are the main developers

Tell Artifact Hub More About Your Artifacts



KubeCon



CloudNativeCon

Europe 2025



Auto Detection

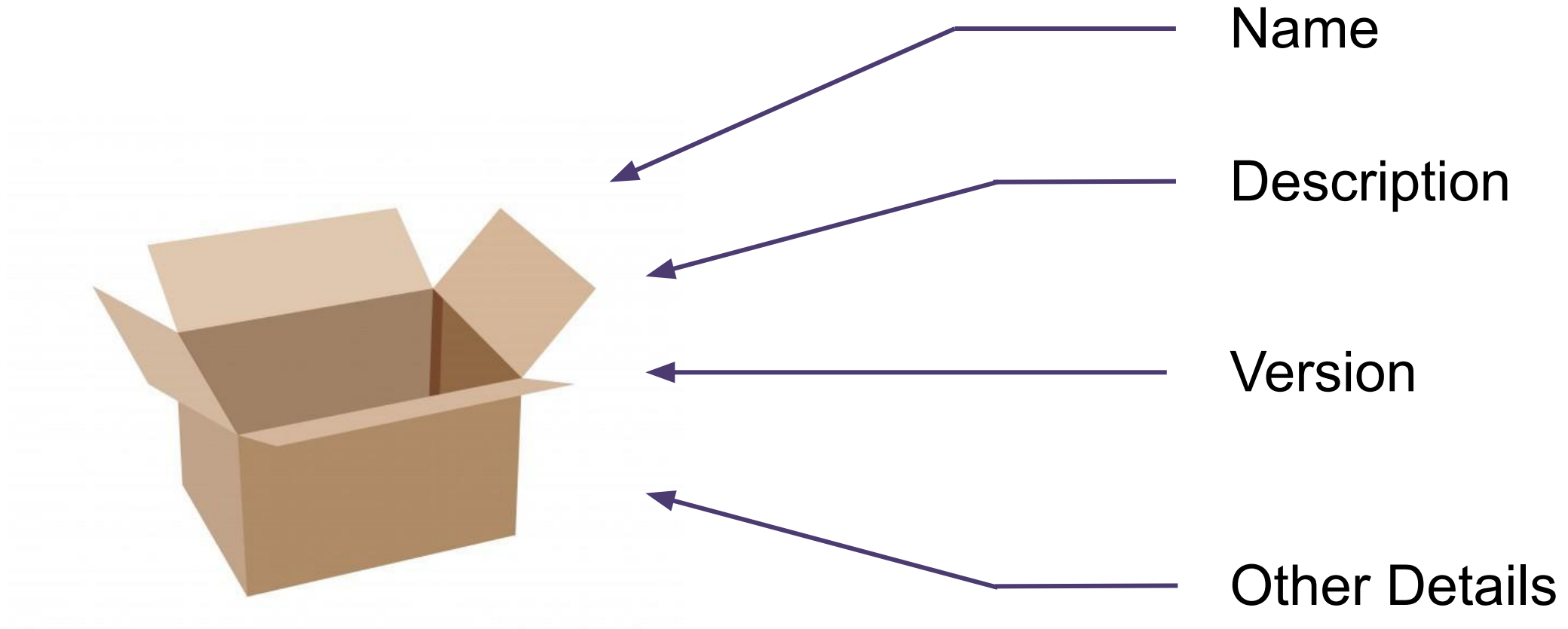


KubeCon



CloudNativeCon

Europe 2025



You Might Want To

- Control the name
- Provide a category or keywords
- Recommend other artifacts
- Share the name of the person or company that produced the artifact
- Set the install instructions
- Even more...

YAML Files



```
version: A SemVer 2 version (required)
name: The name of the package (only alphanum, no spaces, dashes allowed) (required)
alternativeName: Alternative name of the package (optional)
category: Category of the package (optional)
displayName: The name of the package nicely formatted (required)
createdAt: The date this package was created (RFC3339 layout) (required)
description: A short description of the package (required)
license: SPDX identifier of the package license (https://spdx.org/licenses/) (optional)
homeURL: The URL of the project home page (optional)
keywords: # (optional)
  - A list of keywords about this package
  - Using one or more categories names as keywords will improve package visibility
changes: # (optional)
  - kind: added # Supported kinds are: added, changed, deprecated, removed, fixed and security
    description: cool feature
    links:
      - name: GitHub Issue
        url: https://github.com/issue-url
      - name: GitHub PR
        url: https://github.com/pr-url
```

artifacthub-pkg.yml:



```
name: postgresql  
alternativeName: postgres
```

Manifest annotation:



```
annotations:  
  artifacthub.io/alternativeName: postgres
```

Note, the alternative name must be a substring of the name, or the name must be a substring of the alternative name.

artifacthub-pkg.yml:

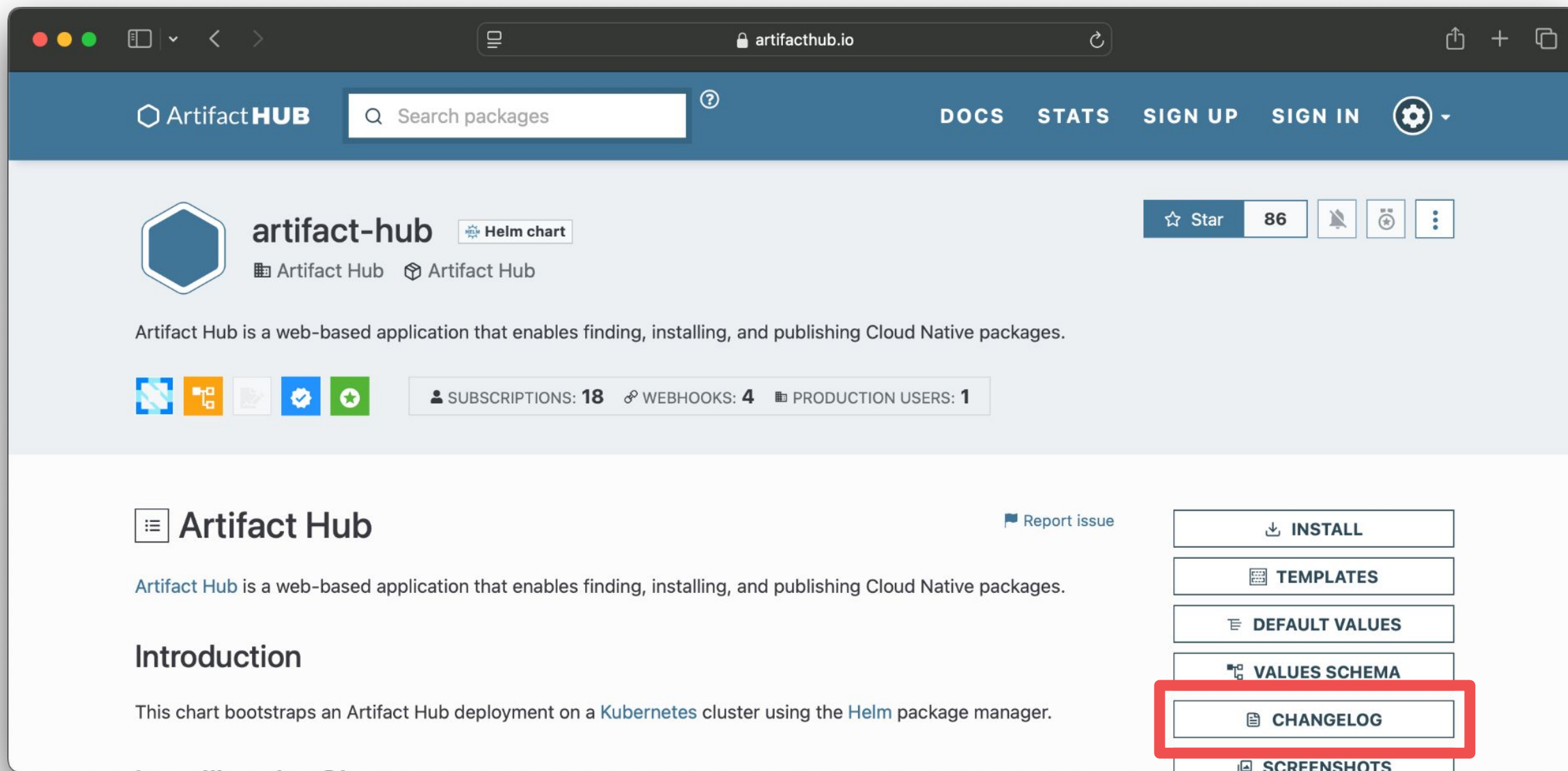


```
changes:
  - kind: added
    description: cool feature
    links:
      - name: GitHub Issue
        url: https://github.com/issue-url
      - name: GitHub PR
        url: https://github.com/pr-url
```

Manifest annotation:



```
annotations:
  artifacthub.io/changes:
    - kind: added
      description: cool feature
      links:
        - name: GitHub Issue
          url: https://github.com/issue-url
        - name: GitHub PR
          url: https://github.com/pr-url
```



The screenshot shows the Artifact Hub web interface in a browser. The URL is artifacthub.io. The page features a search bar, navigation links (DOCS, STATS, SIGN UP, SIGN IN), and a user profile icon. The main content area displays the 'artifact-hub' Helm chart, including its icon, name, and a brief description: 'Artifact Hub is a web-based application that enables finding, installing, and publishing Cloud Native packages.' Below this, there are icons for various integrations and statistics: SUBSCRIPTIONS: 18, WEBHOOKS: 4, and PRODUCTION USERS: 1. On the right side, there are buttons for 'Star' (86), 'Report issue', and a list of actions: INSTALL, TEMPLATES, DEFAULT VALUES, VALUES SCHEMA, CHANGELOG, and SCREENSHOTS. The 'CHANGELOG' button is highlighted with a red rectangle.

Artifact HUB

Search packages

DOCS STATS SIGN UP SIGN IN

artifact-hub Helm chart

Artifact Hub Artifact Hub

Artifact Hub is a web-based application that enables finding, installing, and publishing Cloud Native packages.

SUBSCRIPTIONS: 18 WEBHOOKS: 4 PRODUCTION USERS: 1

Artifact Hub

Report issue

INSTALL

TEMPLATES

DEFAULT VALUES

VALUES SCHEMA

CHANGELOG

SCREENSHOTS

artifacthub.io

< Back to "artifact hub" results

Changelog

1.20.0 11 Oct, 2024

1.19.0 27 Jun, 2024

1.18.0 18 Apr, 2024

1.17.0 15 Jan, 2024

1.20.0 [Contains security updates](#) Released 5 months ago

- + ADDED Support for Radius recipes
- + ADDED Display signed badge for Inspektor Gadget artifacts
- + ADDED Populate chart labels for all resources
- + ADDED Allow adding extra containers to the hub pod from the chart
- ◇ CHANGED Update db migration script to support pg_partman 5
- ◇ CHANGED Banner frame style

GET MARKDOWN

CLOSE

INSTALL

TEMPLATES

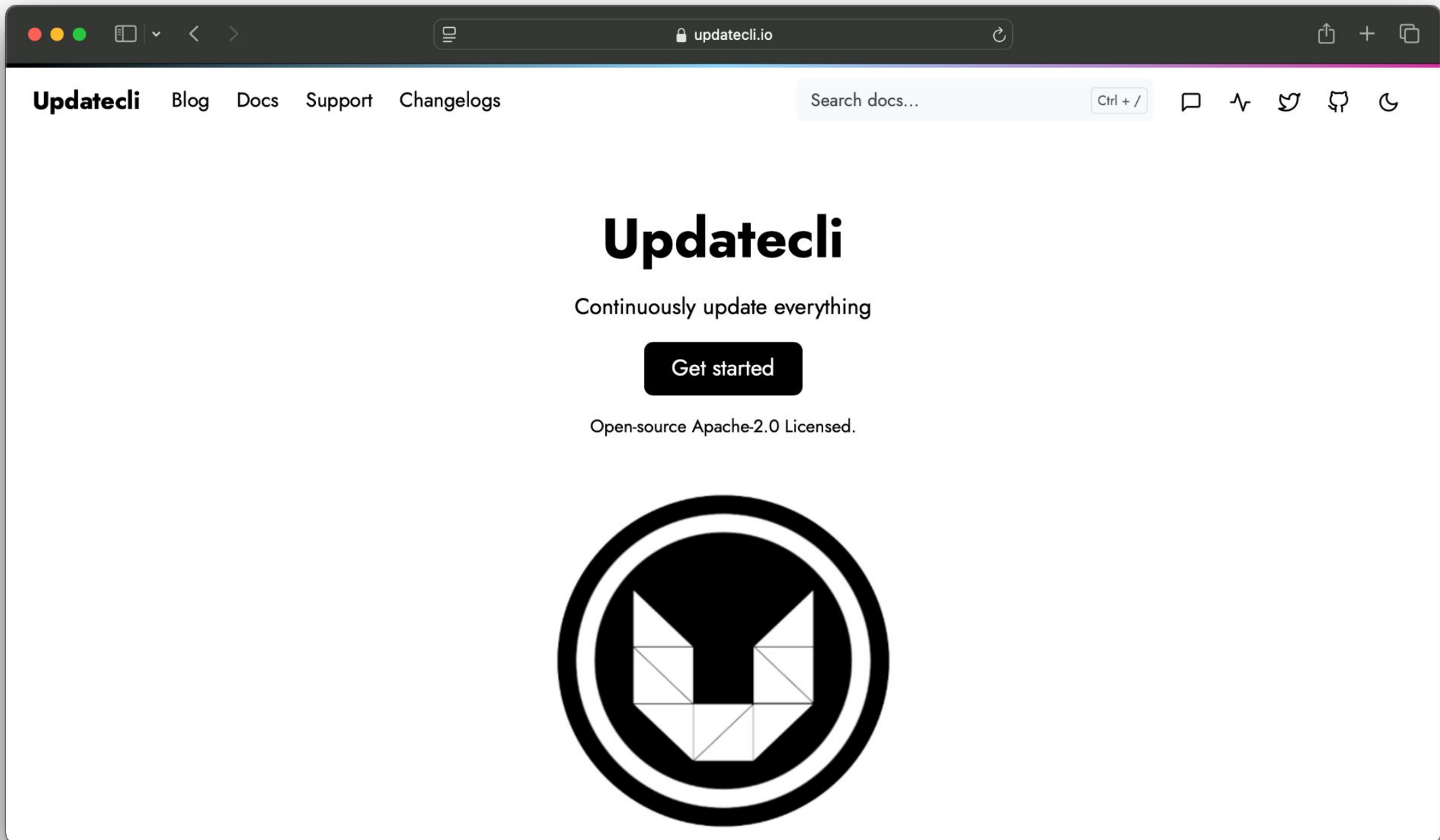
FAULT VALUES

VALUES SCHEMA

CHANGELOG

SCREENSHOTS

This chart bootstraps an Artifact Hub deployment on a [Kubernetes](#) cluster using the [Helm](#) package manager.



artifacthub-pkg.yml:



```
install: |
```

```
The policy can be obtained using [kwctl](https://github.com/kubewarden/kwctl):
```

```
```console
```

```
kwctl pull ghcr.io/kubewarden/policies/cel-policy:v1.2.2
```

```
```
```

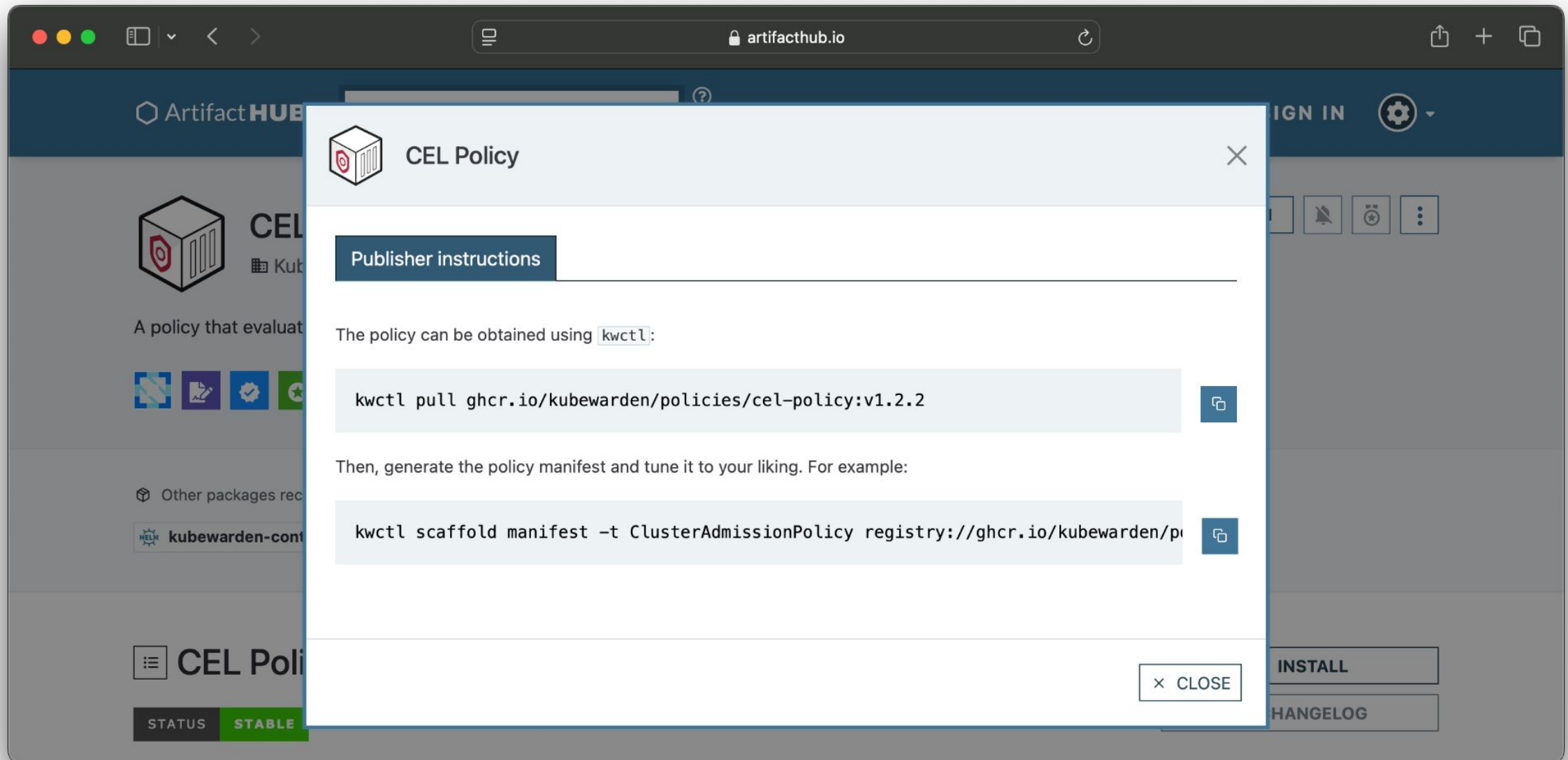
```
Then, generate the policy manifest and tune it to your liking. For example:
```

```
```console
```

```
kwctl scaffold manifest -t ClusterAdmissionPolicy registry://ghcr.io/kubewarden/policies/cel-policy:v1.2.2
```

```
```
```

Custom Install Directions



The screenshot shows the Artifact Hub web interface. A modal window titled "CEL Policy" is open, displaying the "Publisher instructions" tab. The instructions state that the policy can be obtained using `kwctl` and provide two example commands. The background page shows the "CEL Policy" package details, including its status as "STABLE".

CEL Policy

Publisher instructions

The policy can be obtained using `kwctl`:

```
kwctl pull ghcr.io/kubewarden/policies/cel-policy:v1.2.2
```

Then, generate the policy manifest and tune it to your liking. For example:

```
kwctl scaffold manifest -t ClusterAdmissionPolicy registry://ghcr.io/kubewarden/p
```

CEL Policy

STATUS **STABLE**

INSTALL

CHANGELOG

artifacthub-pkg.yml:



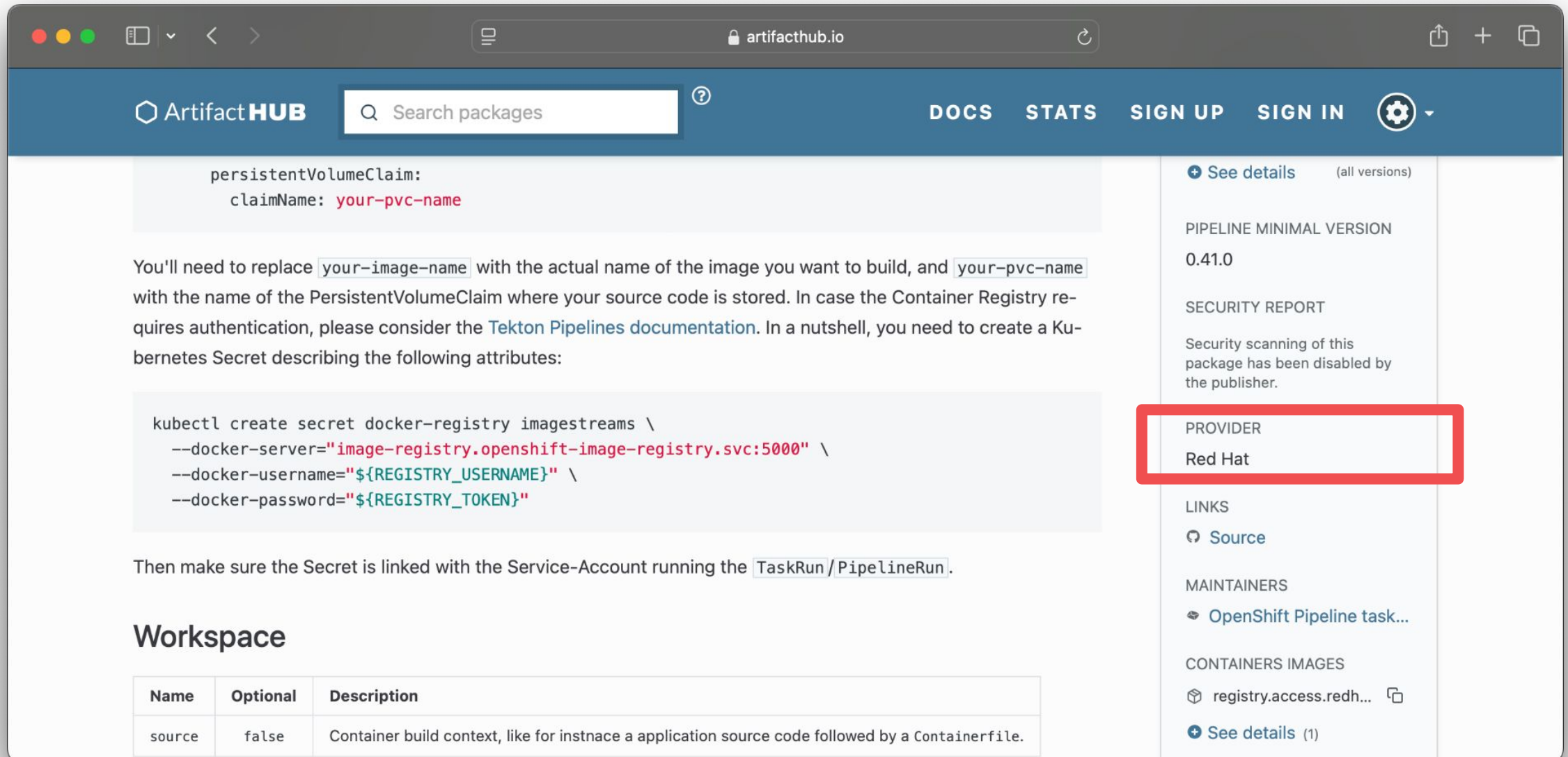
```
provider:  
  name: kubewarden
```

Manifest annotation:



```
annotations:  
  artifacthub.io/provider: Eclipse Foundation
```

Providers Name



The screenshot shows the Artifact Hub website interface. The top navigation bar includes the Artifact HUB logo, a search bar, and links for DOCS, STATS, SIGN UP, and SIGN IN. The main content area displays the details of a pipeline package. On the left, there is a code block for a Kubernetes secret and a paragraph explaining the need to replace placeholders. On the right, there is a sidebar with various sections: See details, PIPELINE MINIMAL VERSION (0.41.0), SECURITY REPORT, PROVIDER (Red Hat, highlighted with a red box), LINKS (Source), MAINTAINERS (OpenShift Pipeline task...), and CONTAINERS IMAGES (registry.access.redh...). The PROVIDER section is highlighted with a red box.

persistentVolumeClaim:
claimName: **your-pvc-name**

You'll need to replace `your-image-name` with the actual name of the image you want to build, and `your-pvc-name` with the name of the PersistentVolumeClaim where your source code is stored. In case the Container Registry requires authentication, please consider the [Tekton Pipelines documentation](#). In a nutshell, you need to create a Kubernetes Secret describing the following attributes:

```
kubectl create secret docker-registry imagestreams \
  --docker-server="image-registry.openshift-image-registry.svc:5000" \
  --docker-username="${REGISTRY_USERNAME}" \
  --docker-password="${REGISTRY_TOKEN}"
```

Then make sure the Secret is linked with the Service-Account running the `TaskRun/PipelineRun`.

Workspace

| Name | Optional | Description |
|--------|----------|---|
| source | false | Container build context, like for instance a application source code followed by a Containerfile. |

[+ See details](#) (all versions)

PIPELINE MINIMAL VERSION
0.41.0

SECURITY REPORT
Security scanning of this package has been disabled by the publisher.

PROVIDER
Red Hat

LINKS
[Source](#)

MAINTAINERS
[OpenShift Pipeline task...](#)

CONTAINERS IMAGES
[registry.access.redh...](#)

[+ See details](#) (1)

artifacthub-pkg.yml:



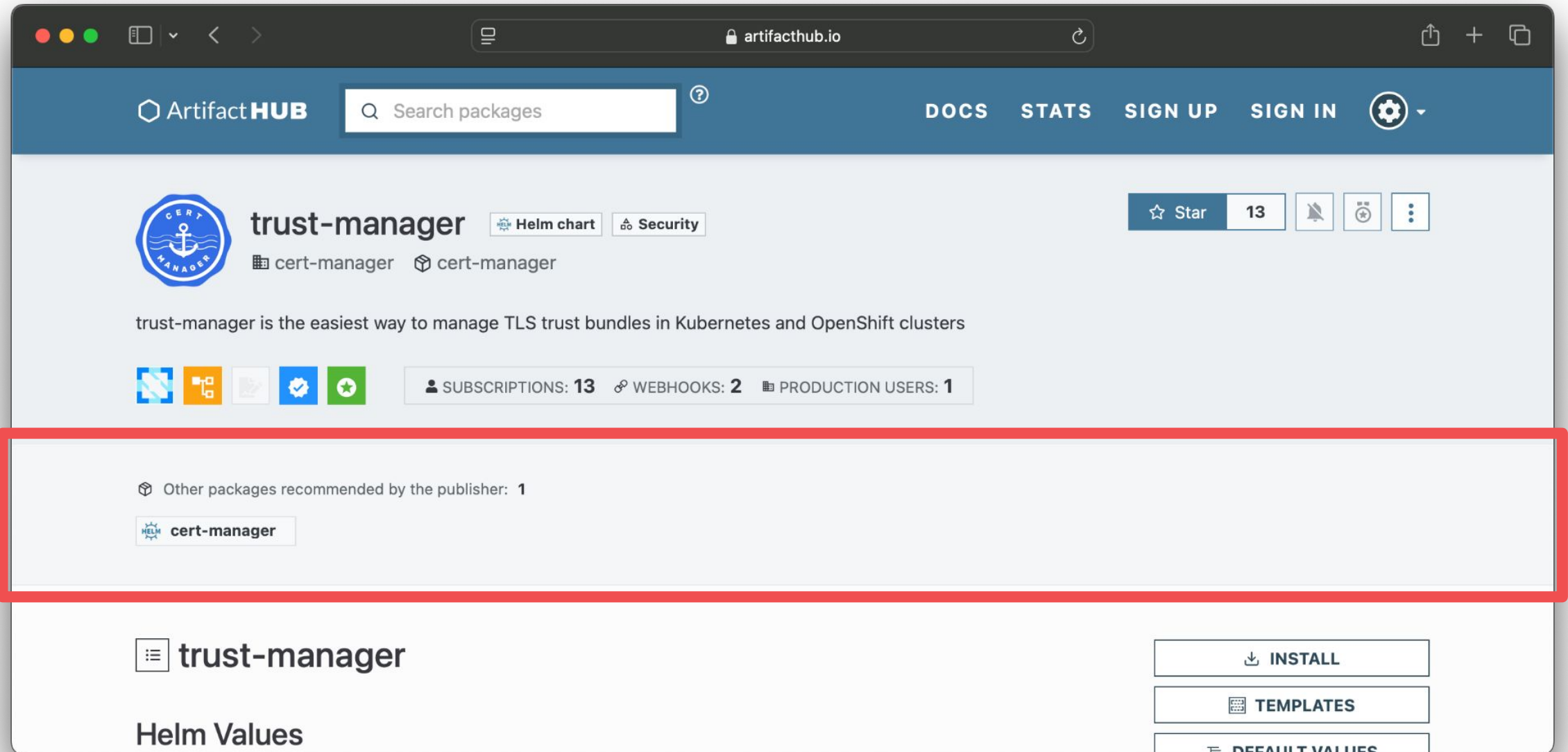
```
recommendations:  
  - url: https://artifacthub.io/packages/helm/cert-manager/cert-manager
```

Manifest annotation:



```
annotations:  
  artifacthub.io/recommendations: |  
    - url: https://artifacthub.io/packages/helm/cert-manager/cert-manager
```

Recommendations



The screenshot shows the Artifact Hub interface for the **trust-manager** package. The page includes a search bar, navigation links (DOCS, STATS, SIGN UP, SIGN IN), and a star count of 13. The main description states: "trust-manager is the easiest way to manage TLS trust bundles in Kubernetes and OpenShift clusters". Below this, statistics are shown: SUBSCRIPTIONS: 13, WEBHOOKS: 2, and PRODUCTION USERS: 1. A red box highlights the "Other packages recommended by the publisher: 1" section, which lists **cert-manager**. At the bottom, there are links for "trust-manager", "Helm Values", and buttons for "INSTALL", "TEMPLATES", and "DEFAULT VALUES".

Artifact **HUB** Search packages

DOCS STATS SIGN UP SIGN IN

 **trust-manager** Helm chart Security

cert-manager cert-manager

trust-manager is the easiest way to manage TLS trust bundles in Kubernetes and OpenShift clusters

SUBSCRIPTIONS: 13 WEBHOOKS: 2 PRODUCTION USERS: 1

Other packages recommended by the publisher: 1

 **cert-manager**

 **trust-manager**

Helm Values

INSTALL

TEMPLATES

DEFAULT VALUES

Signing Artifacts



KubeCon



CloudNativeCon

Europe 2025

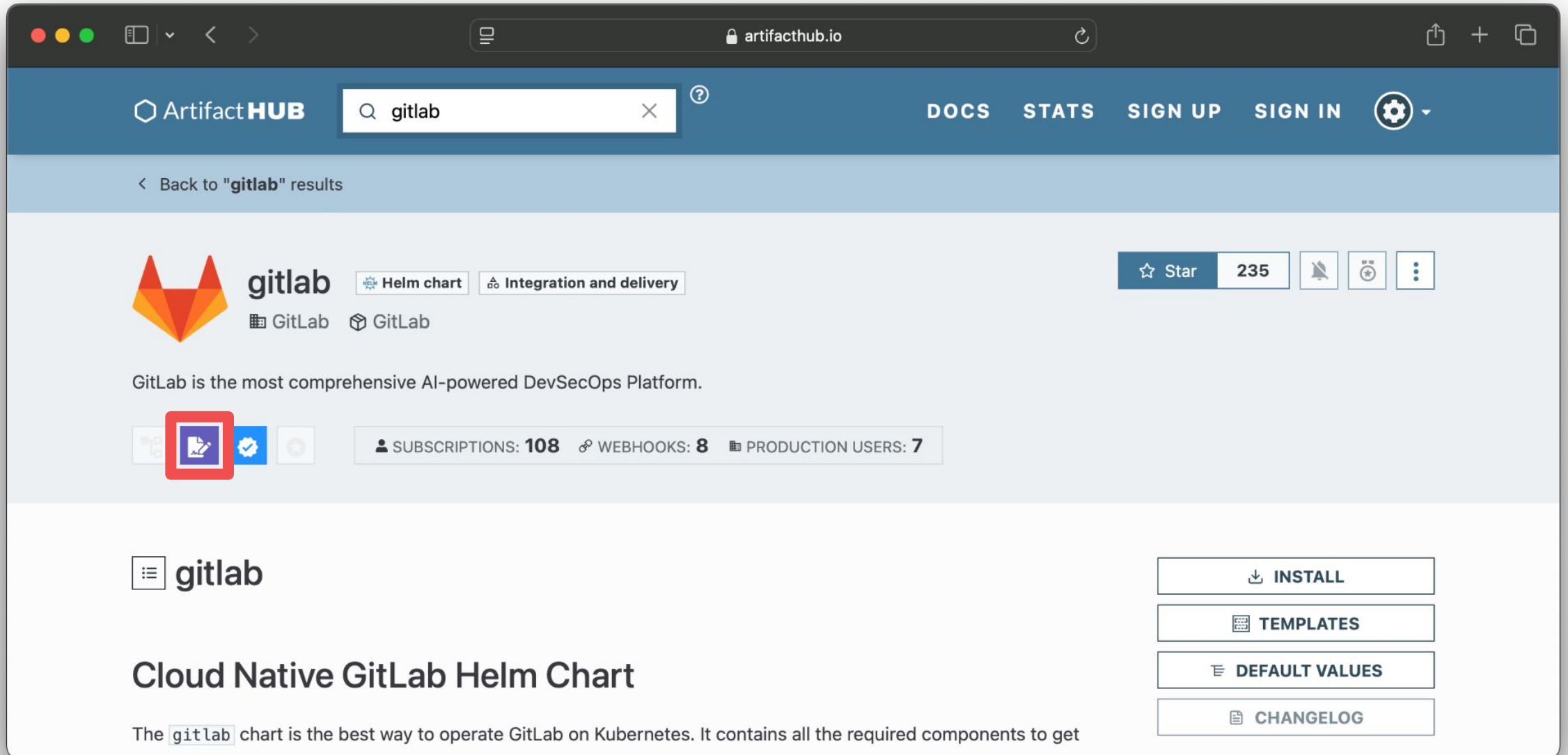


“ Software provenance refers to the origin and history of a piece of software.

It's the **documented record** of where software came from, **how it was built**, and who was involved in its creation. Essentially, it's about establishing **trust** and transparency in the software supply chain.

– Gemini (AI)

Authenticity and Integrity



The screenshot shows a web browser window at `artifacthub.io`. The page displays the search results for "gitlab". At the top, there's a navigation bar with the Artifact HUB logo, a search bar containing "gitlab", and links for DOCS, STATS, SIGN UP, and SIGN IN. Below the navigation bar, a blue banner indicates the search results for "gitlab". The main content area features the GitLab logo, the name "gitlab", and tags for "Helm chart" and "Integration and delivery". To the right, there's a "Star" button showing 235 stars, along with notification and settings icons. Below this, a description states: "GitLab is the most comprehensive AI-powered DevSecOps Platform." A row of icons follows, with the first icon (a document with a pencil) highlighted by a red square. To the right of the icons, statistics are shown: "SUBSCRIPTIONS: 108", "WEBHOOKS: 8", and "PRODUCTION USERS: 7". At the bottom, the title "Cloud Native GitLab Helm Chart" is displayed, followed by a brief description: "The `gitlab` chart is the best way to operate GitLab on Kubernetes. It contains all the required components to get". On the right side of the page, there are four buttons: "INSTALL", "TEMPLATES", "DEFAULT VALUES", and "CHANGELOG".

Artifact HUB

gitlab

DOCS STATS SIGN UP SIGN IN

< Back to "gitlab" results

 **gitlab**  Helm chart  Integration and delivery

Star 235

GitLab is the most comprehensive AI-powered DevSecOps Platform.

SUBSCRIPTIONS: 108 WEBHOOKS: 8 PRODUCTION USERS: 7

 **gitlab**

Cloud Native GitLab Helm Chart

The `gitlab` chart is the best way to operate GitLab on Kubernetes. It contains all the required components to get

INSTALL

TEMPLATES

DEFAULT VALUES

CHANGELOG

Signing

Artifact **HUB**

gitlab

DOCS STATS SIGN UP SIGN IN

[Back to "gitlab" results](#)



gitlab

GitLab GitLab

Helm chart Integration and delivery

Star 235

GitLab is the most comprehensive AI-powered DevSecOps Platform.

SUBSCRIPTIONS: 108 WEBHOOKS: 8 PRODUCTION USERS: 7

Signed

This package has been **signed**.

Signature: chart provenance file

INSTALL

TEMPLATES

DEFAULT VALUES

CHANGELOG

Cloud Native GitLab Helm Chart

The `gitlab` chart is the best way to operate GitLab on Kubernetes. It contains all the required components to get

Signing

Artifact **HUB**

Search packages

DOCS

STATS

SIGN UP

SIGN IN



Verify Image Signatures

Kubewarden policy Security

Star 2

Kubewarden Developers

Verify Image Signatures

A Kubewarden Policy that verifies all the signatures of the container images referenced by a Pod



Signed

This package has been **signed**.

Signature: `cosign`



Verify Image Signatures

STATUS

STABLE

INSTALL

CHANGELOG

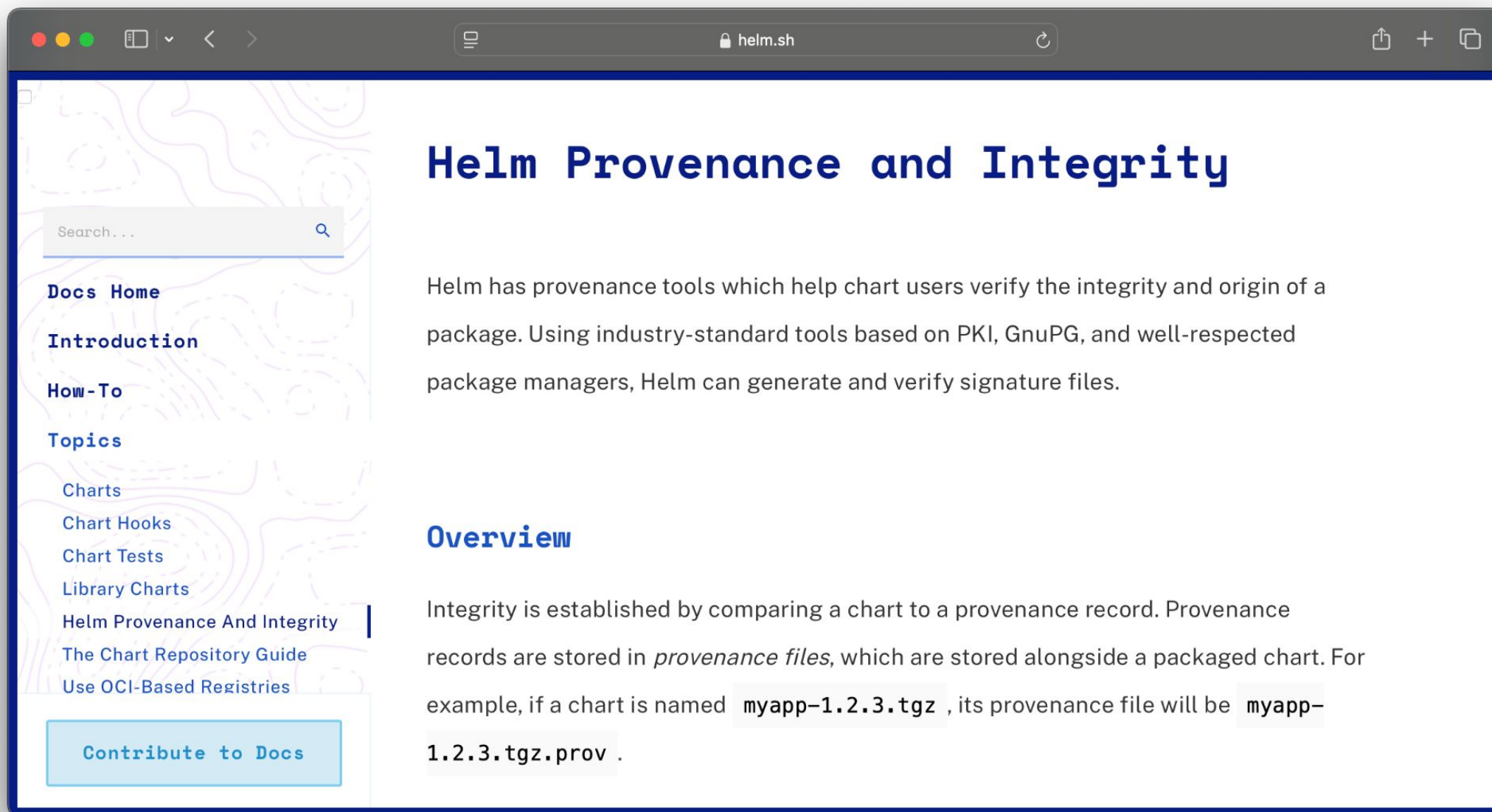
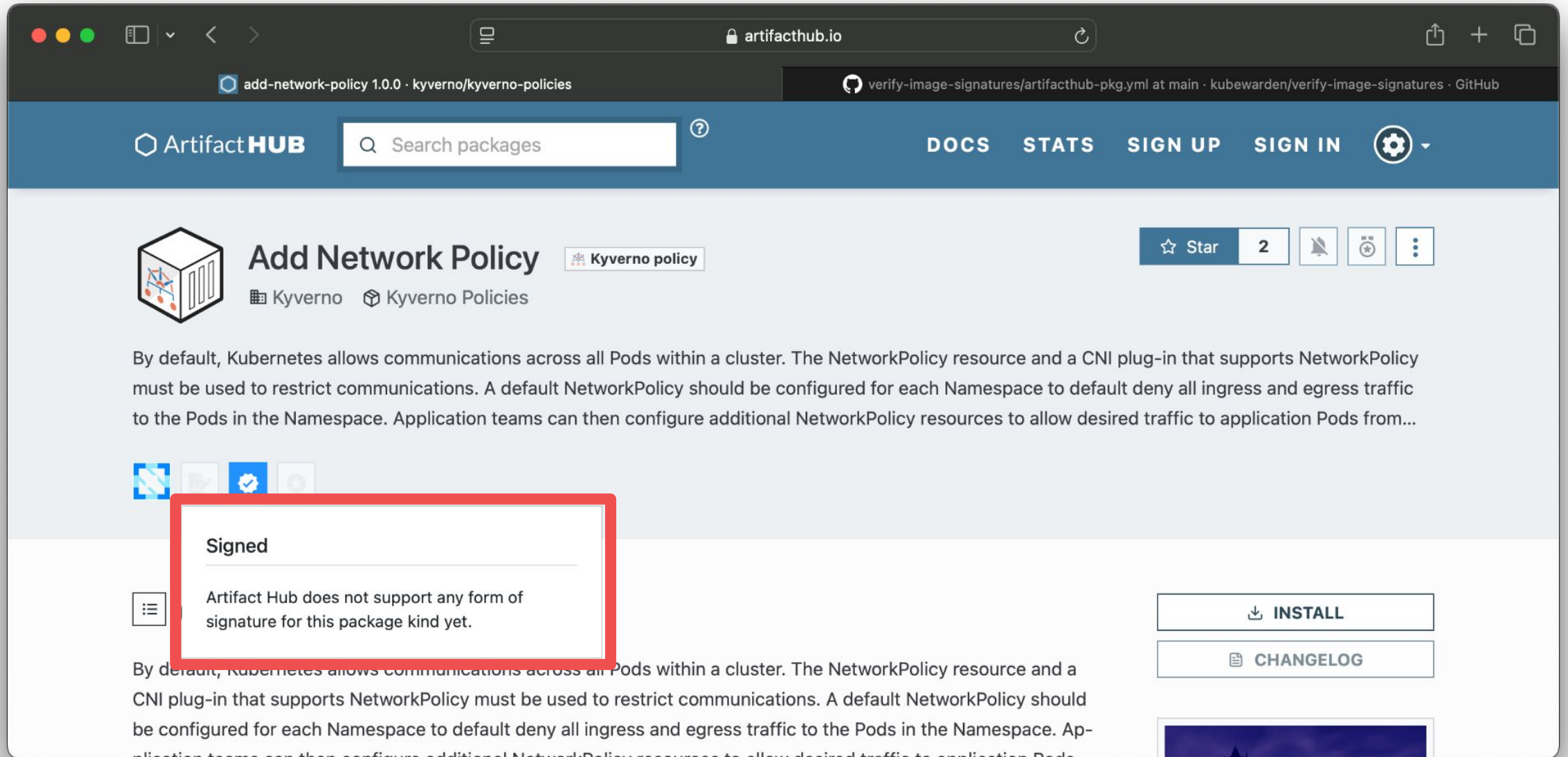


Chart.yaml



```
annotations:  
  artifacthub.io/signKey: |  
    fingerprint: C874011F0AB405110D02105534365D9472D7468F  
    url: https://keybase.io/hashicorp/pgp_keys.asc
```

Not Everything Supports Signing



The screenshot shows the Artifact Hub interface for the package 'add-network-policy 1.0.0' by 'kyverno/kyverno-policies'. The page includes a search bar, navigation links (DOCS, STATS, SIGN UP, SIGN IN), and a star count of 2. A red box highlights a 'Signed' warning message that states: 'Artifact Hub does not support any form of signature for this package kind yet.' Below the warning, the package description is partially visible, and buttons for 'INSTALL' and 'CHANGELOG' are present on the right.

add-network-policy 1.0.0 · kyverno/kyverno-policies

verify-image-signatures/artifacthub-pkg.yml at main · kubewarden/verify-image-signatures · GitHub

Artifact HUB Search packages

DOCS STATS SIGN UP SIGN IN

 **Add Network Policy** Kyverno policy

Kyverno Kyverno Policies

By default, Kubernetes allows communications across all Pods within a cluster. The NetworkPolicy resource and a CNI plug-in that supports NetworkPolicy must be used to restrict communications. A default NetworkPolicy should be configured for each Namespace to default deny all ingress and egress traffic to the Pods in the Namespace. Application teams can then configure additional NetworkPolicy resources to allow desired traffic to application Pods from...

Signed

Artifact Hub does not support any form of signature for this package kind yet.

By default, Kubernetes allows communications across all Pods within a cluster. The NetworkPolicy resource and a CNI plug-in that supports NetworkPolicy must be used to restrict communications. A default NetworkPolicy should be configured for each Namespace to default deny all ingress and egress traffic to the Pods in the Namespace. Application teams can then configure additional NetworkPolicy resources to allow desired traffic to application Pods from...

INSTALL

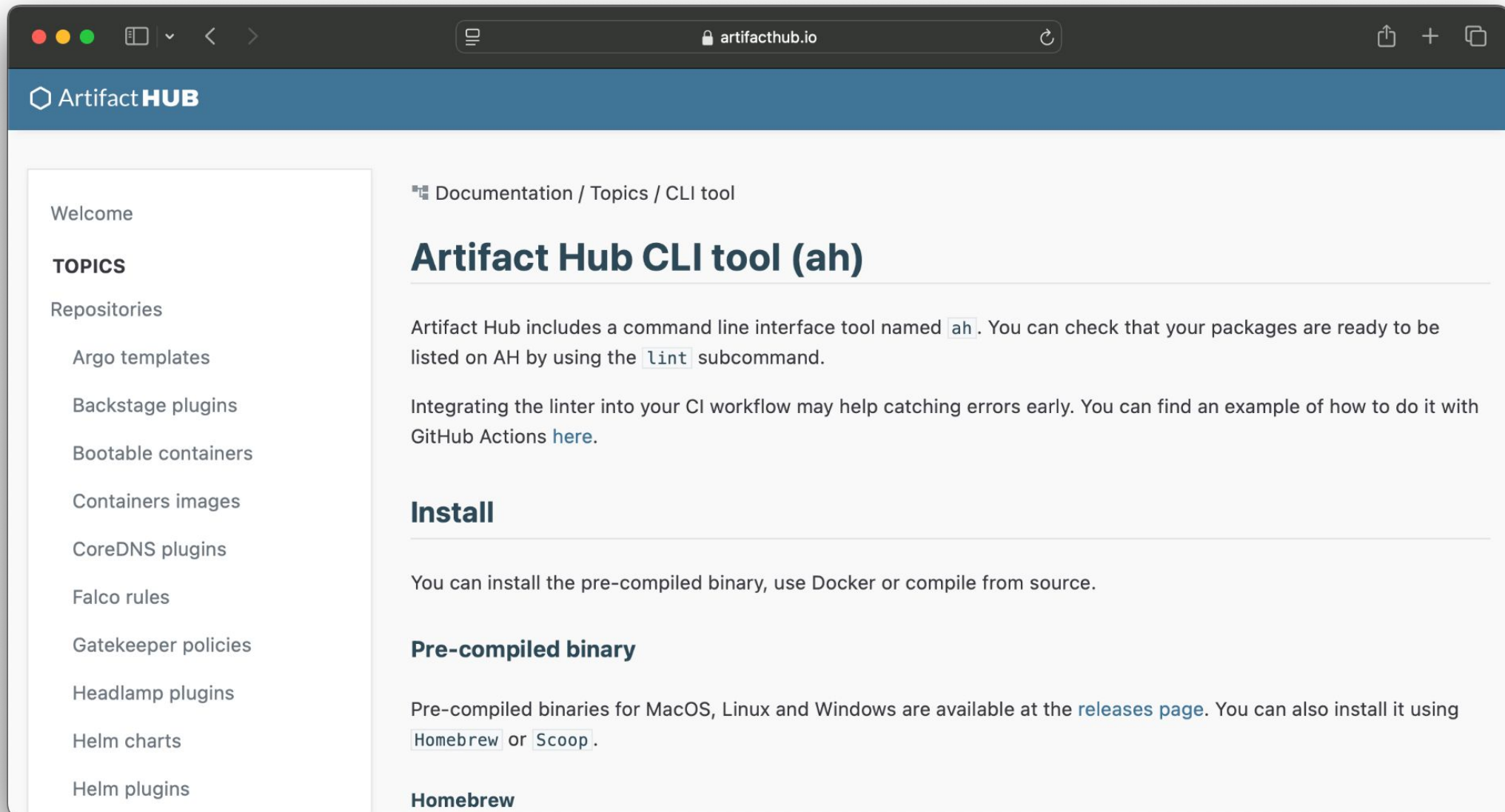
CHANGELOG

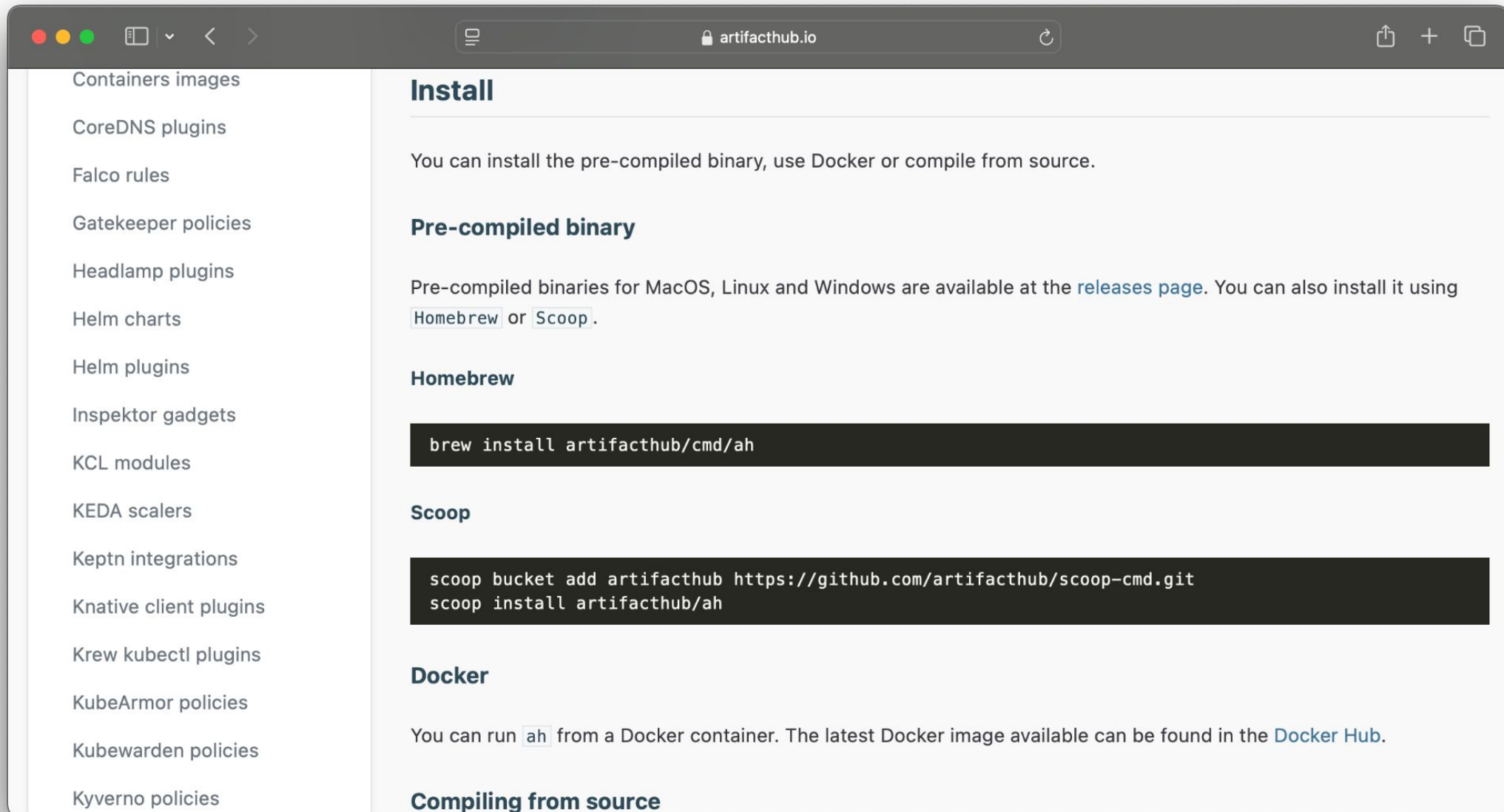
Linting & Learning



Europe 2025







The screenshot shows a web browser window with the address bar displaying 'artifacthub.io'. The left sidebar contains a list of categories: Containers images, CoreDNS plugins, Falco rules, Gatekeeper policies, Headlamp plugins, Helm charts, Helm plugins, Inspektor gadgets, KCL modules, KEDA scalars, Keptn integrations, Knative client plugins, Krew kubectl plugins, KubeArmor policies, Kubewarden policies, and Kyverno policies. The main content area is titled 'Install' and provides instructions on how to install the CLI. It mentions that pre-compiled binaries are available for MacOS, Linux, and Windows, and can be installed using Homebrew or Scoop. It also mentions that the latest Docker image can be found in the Docker Hub. The 'Compiling from source' section is partially visible at the bottom.

Install

You can install the pre-compiled binary, use Docker or compile from source.

Pre-compiled binary

Pre-compiled binaries for MacOS, Linux and Windows are available at the [releases page](#). You can also install it using [Homebrew](#) or [Scoop](#).

Homebrew

```
brew install artifacthub/cmd/ah
```

Scoop

```
scoop bucket add artifacthub https://github.com/artifacthub/scoop-cmd.git  
scoop install artifacthub/ah
```

Docker

You can run [ah](#) from a Docker container. The latest Docker image available can be found in the [Docker Hub](#).

Compiling from source



```
$ ah
```

```
Artifact Hub command line tool
```

```
Usage:
```

```
ah [command]
```

```
Available Commands:
```

```
help          Help about any command
```

```
lint          Check the repository's packages are ready for Artifact Hub
```

```
version       Print version information
```

```
Flags:
```

```
-h, --help    help for ah
```

```
Use "ah [command] --help" for more information about a command.
```



```
$ helm create ah-demo  
Creating ah-demo
```

```
$ ah lint --kind helm --path ah-demo
```

```
✓ ah-demo 0.1.0 (ah-demo)
```

```
Package lint SUCCEEDED!
```

```
✓ Name: ah-demo
```

```
! Display name: *** NOT PROVIDED ***
```

```
✓ Version: 0.1.0
```

```
✓ App version: 1.16.0
```

```
✓ Description: A Helm chart for Kubernetes
```

```
! License: *** NOT PROVIDED ***
```

```
! Logo URL: *** NOT PROVIDED ***
```

```
! Home URL: *** NOT PROVIDED ***
```

```
✓ Deprecated: false
```

```
✓ Pre-release: false
```

```
✓ Contains security updates: false
```

```
! Provider: *** NOT PROVIDED ***
```

```
! Readme: *** NOT PROVIDED ***
```

```
! Keywords: *** NOT PROVIDED ***
```

```
! Links: *** NOT PROVIDED ***
```

```
! Maintainers: *** NOT PROVIDED ***
```

```
✓ Containers images:
```

```
  - Name: | Image: nginx:1.16.0
```

```
! Changes: *** NOT PROVIDED ***
```

```
! Recommendations: *** NOT PROVIDED ***
```

```
! Screenshots: *** NOT PROVIDED ***
```

```
✓ Operator: false
```

```
! Sign key: *** NOT PROVIDED ***
```

```
! Values schema: *** NOT PROVIDED ***
```

```
1 package(s) found, 0 package(s) with errors
```



```
$ ah lint --kind kubewarden
```

```
✓ cel-policy 1.2.2 (.)
```

```
Package lint SUCCEEDED!
```

```
✓ Name: cel-policy
✓ Display name: CEL Policy
✓ Version: 1.2.2
! App version: *** NOT PROVIDED ***
✓ Description: A policy that evaluates CEL expressions
✓ License: Apache-2.0
! Logo URL: *** NOT PROVIDED ***
✓ Home URL: https://github.com/kubewarden/cel-policy
✓ Deprecated: false
✓ Pre-release: false
✓ Contains security updates: false
✓ Provider: kubewarden
✓ Readme: PROVIDED
✓ Keywords:
  - compliance
  - CEL
  - ValidatingAdmissionPolicy
  - Common Expression Language
✓ Links:
  - Name: policy | URL: https://github.com/kubewarden/cel-policy/releases/download/v1.2.2/policy.wasm
  - Name: source | URL: https://github.com/kubewarden/cel-policy
✓ Maintainers:
  - Name: Kubewarden developers | Email: cncf-kubewarden-maintainers@lists.cncf.io
✓ Containers images:
  - Name: policy | Image: ghcr.io/kubewarden/policies/cel-policy:v1.2.2
! Changes: *** NOT PROVIDED ***
✓ Recommendations:
  - https://artifacthub.io/packages/helm/kubewarden/kubewarden-controller
! Screenshots: *** NOT PROVIDED ***
✓ Operator: false
✓ Install: PROVIDED
```

```
1 package(s) found, 0 package(s) with errors
```

Embedding



KubeCon

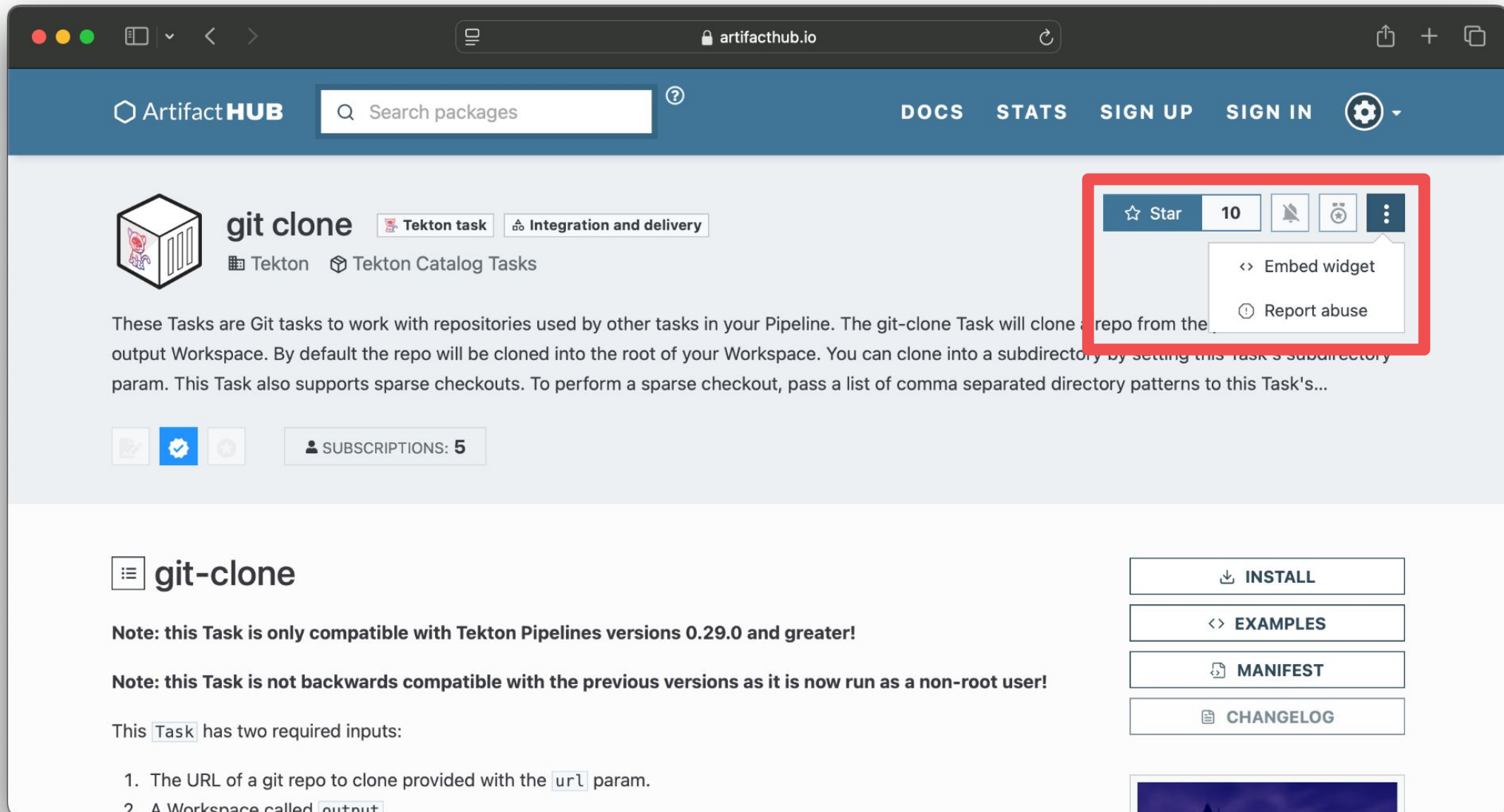


CloudNativeCon

Europe 2025



Embedding



The screenshot shows the Artifact Hub interface for the 'git clone' task. The top navigation bar includes the Artifact HUB logo, a search bar, and links for DOCS, STATS, SIGN UP, and SIGN IN. The main content area features the 'git clone' task card, which includes a cube icon, the task name, and labels for 'Tekton task' and 'Integration and delivery'. A red box highlights the interaction area on the right side of the task card, which includes a 'Star' button (10 stars), a notification bell, a clock icon, and a three-dot menu. The menu is open, showing options for 'Embed widget' and 'Report abuse'. Below the task card, there is a description of the task, a 'SUBSCRIPTIONS: 5' button, and a section for 'git-clone' with a list of inputs. On the right side, there are buttons for 'INSTALL', 'EXAMPLES', 'MANIFEST', and 'CHANGELOG'.

Artifact HUB Search packages

DOCS STATS SIGN UP SIGN IN

 **git clone** Tekton task Integration and delivery

Tekton Tekton Catalog Tasks

These Tasks are Git tasks to work with repositories used by other tasks in your Pipeline. The git-clone Task will clone a repo from the output Workspace. By default the repo will be cloned into the root of your Workspace. You can clone into a subdirectory by setting this task's subdirectory param. This Task also supports sparse checkouts. To perform a sparse checkout, pass a list of comma separated directory patterns to this Task's...

   SUBSCRIPTIONS: 5

 **git-clone**

Note: this Task is only compatible with Tekton Pipelines versions 0.29.0 and greater!

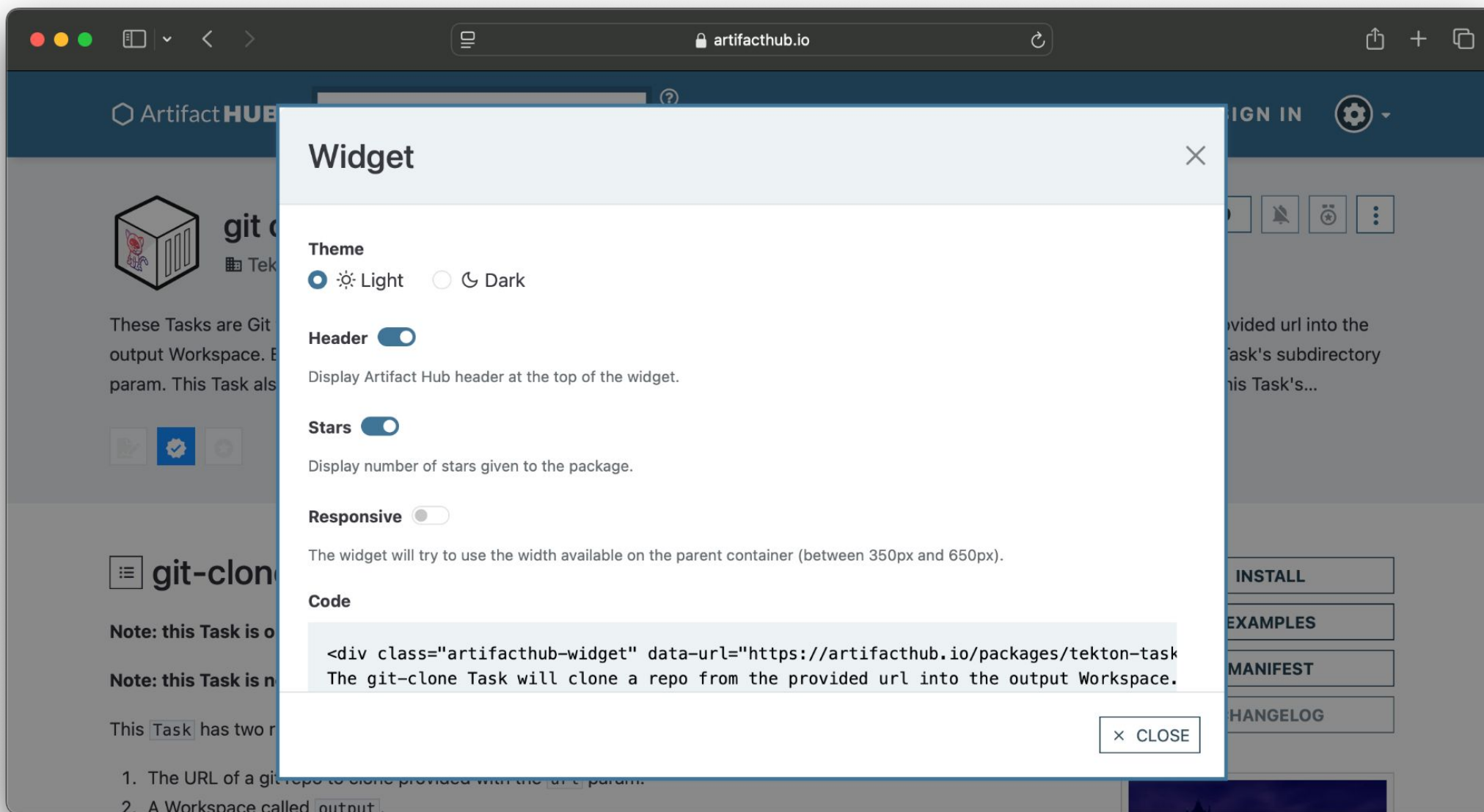
Note: this Task is not backwards compatible with the previous versions as it is now run as a non-root user!

This Task has two required inputs:

1. The URL of a git repo to clone provided with the `url` param.
2. A Workspace called `output`.

INSTALL EXAMPLES MANIFEST CHANGELOG

Embedding



The screenshot shows the Artifact Hub website interface. A modal window titled "Widget" is open, allowing users to generate an embed code for a specific task. The modal includes the following settings:

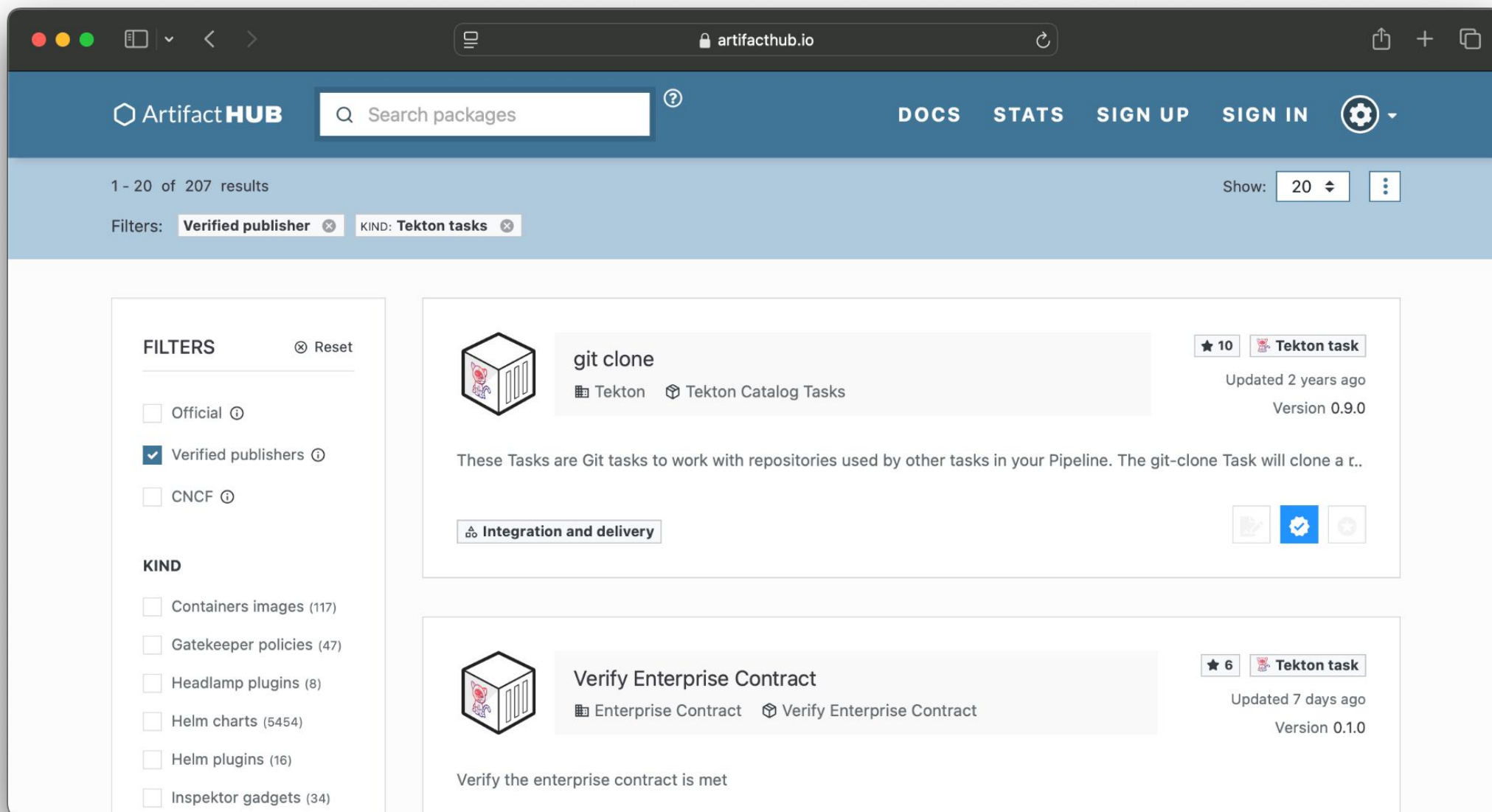
- Theme:** Radio buttons for "Light" (selected) and "Dark".
- Header:** A toggle switch that is turned on. Description: "Display Artifact Hub header at the top of the widget."
- Stars:** A toggle switch that is turned on. Description: "Display number of stars given to the package."
- Responsive:** A toggle switch that is turned off. Description: "The widget will try to use the width available on the parent container (between 350px and 650px)."
- Code:** A text area containing the generated embed code.

The generated code is:

```
<div class="artifacthub-widget" data-url="https://artifacthub.io/packages/tekton-task-git-clone">
  The git-clone Task will clone a repo from the provided url into the output Workspace.
</div>
```

A "CLOSE" button is located at the bottom right of the modal.

Embedding



The screenshot shows the Artifact Hub website interface. The header includes the Artifact HUB logo, a search bar, and navigation links for DOCS, STATS, SIGN UP, and SIGN IN. The main content area displays search results for Tekton tasks, filtered by 'Verified publisher' and 'KIND: Tekton tasks'. Two task cards are visible: 'git clone' and 'Verify Enterprise Contract'.

Artifact HUB Search packages

1 - 20 of 207 results

Filters: **Verified publisher** **KIND: Tekton tasks**

Show: 20

FILTERS [Reset](#)

- ☐ Official
- ☒ Verified publishers
- ☐ CNCF

KIND

- ☐ Containers images (117)
- ☐ Gatekeeper policies (47)
- ☐ Headlamp plugins (8)
- ☐ Helm charts (5454)
- ☐ Helm plugins (16)
- ☐ Inspektor gadgets (34)

git clone ★ 10 **Tekton task**

Updated 2 years ago
Version 0.9.0

These Tasks are Git tasks to work with repositories used by other tasks in your Pipeline. The git-clone Task will clone a r..

Integration and delivery

Verify Enterprise Contract ★ 6 **Tekton task**

Updated 7 days ago
Version 0.1.0

Verify the enterprise contract is met

Embedding

The screenshot shows the Artifact Hub website interface. At the top, there's a navigation bar with the Artifact HUB logo, a search bar, and links for DOCS, STATS, SIGN UP, and SIGN IN. Below the navigation bar, the search results are displayed. On the left, there's a sidebar with filters. The main content area shows a list of search results. A red box highlights the 'Embed results' button in the top right corner of the results area.

Artifact HUB

Search packages

DOCS STATS SIGN UP SIGN IN

1 - 20 of 207 results

Filters: Verified publisher x KIND: Tekton tasks x

Show: 20 > < > Embed results

FILTERS x Reset

☐ Official ⓘ

☒ Verified publishers ⓘ

☐ CNCF ⓘ

KIND

☐ Containers images (117)

☐ Gatekeeper policies (47)

☐ Headlamp plugins (8)

☐ Helm charts (5454)

☐ Helm plugins (16)

☐ Inspektor gadgets (34)

git clone

Tekton Tekton Catalog Tasks

★ 10 Tekton task

Updated 2 years ago

Version 0.9.0

These Tasks are Git tasks to work with repositories used by other tasks in your Pipeline. The git-clone Task will clone a r..

Integration and delivery

Verify Enterprise Contract

Enterprise Contract Verify Enterprise Contract

★ 6 Tekton task

Updated 7 days ago

Version 0.1.0

Verify the enterprise contract is met

Embedding

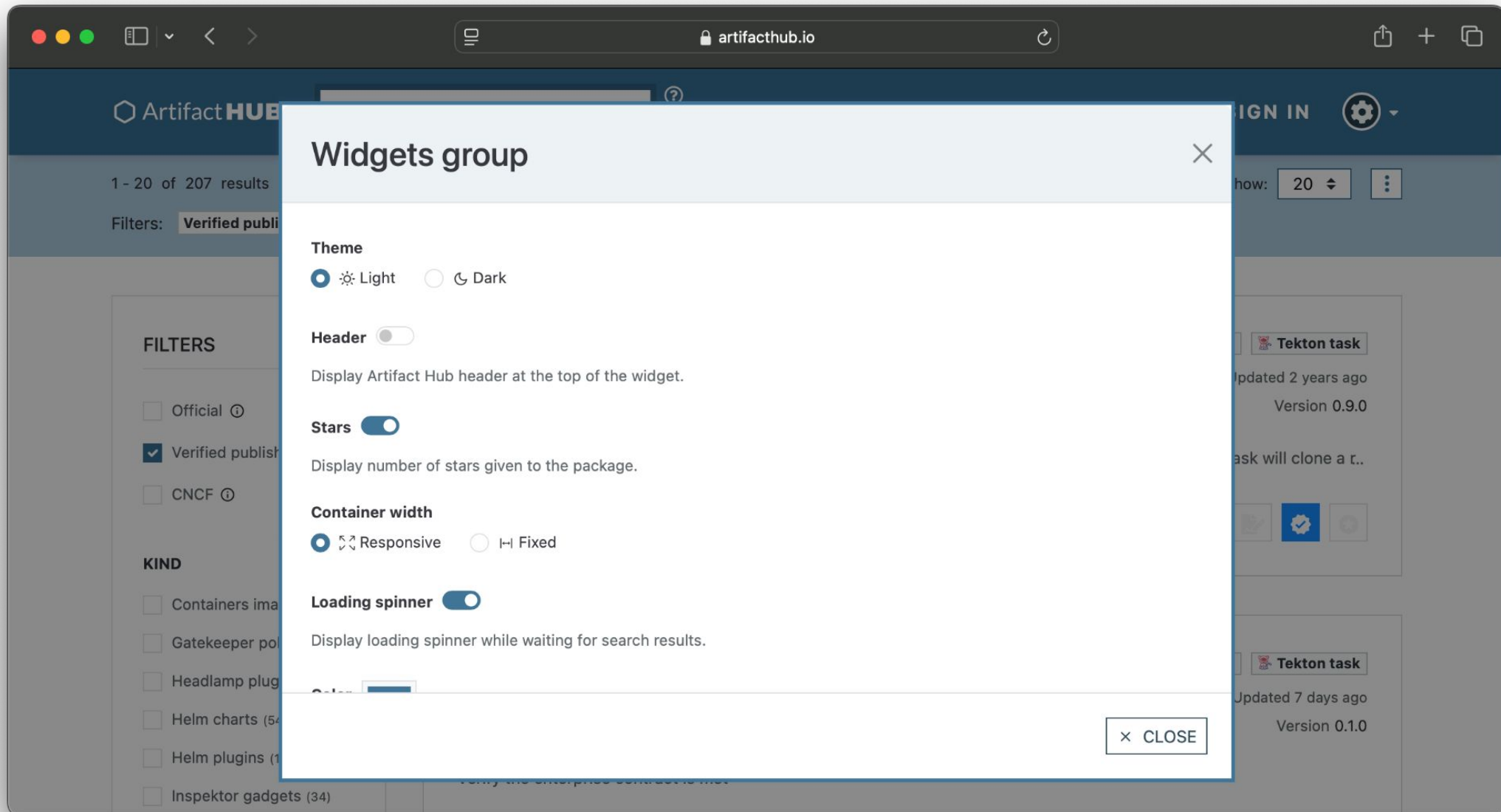


KubeCon



CloudNativeCon

Europe 2025



Webhooks



KubeCon



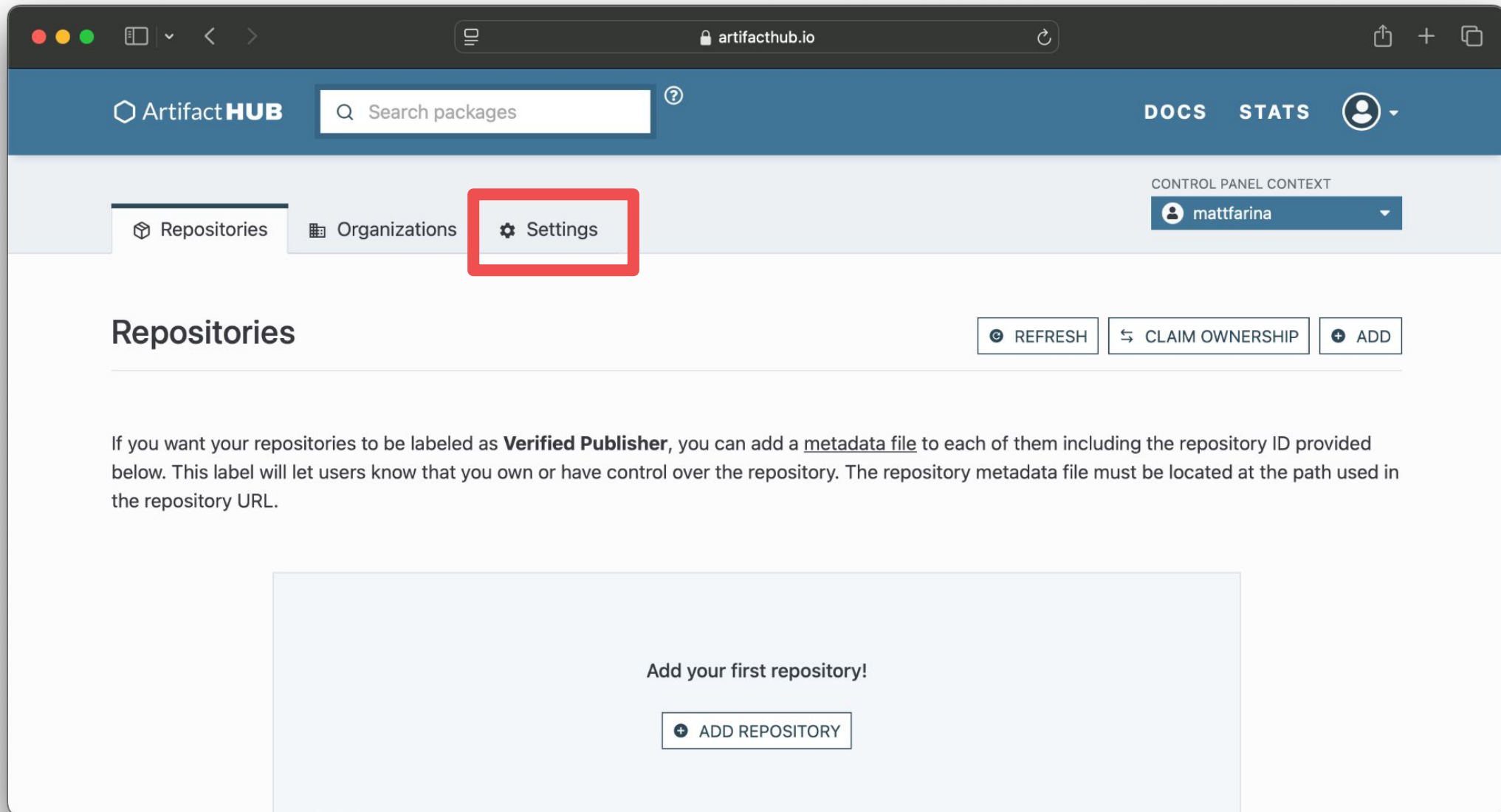
CloudNativeCon

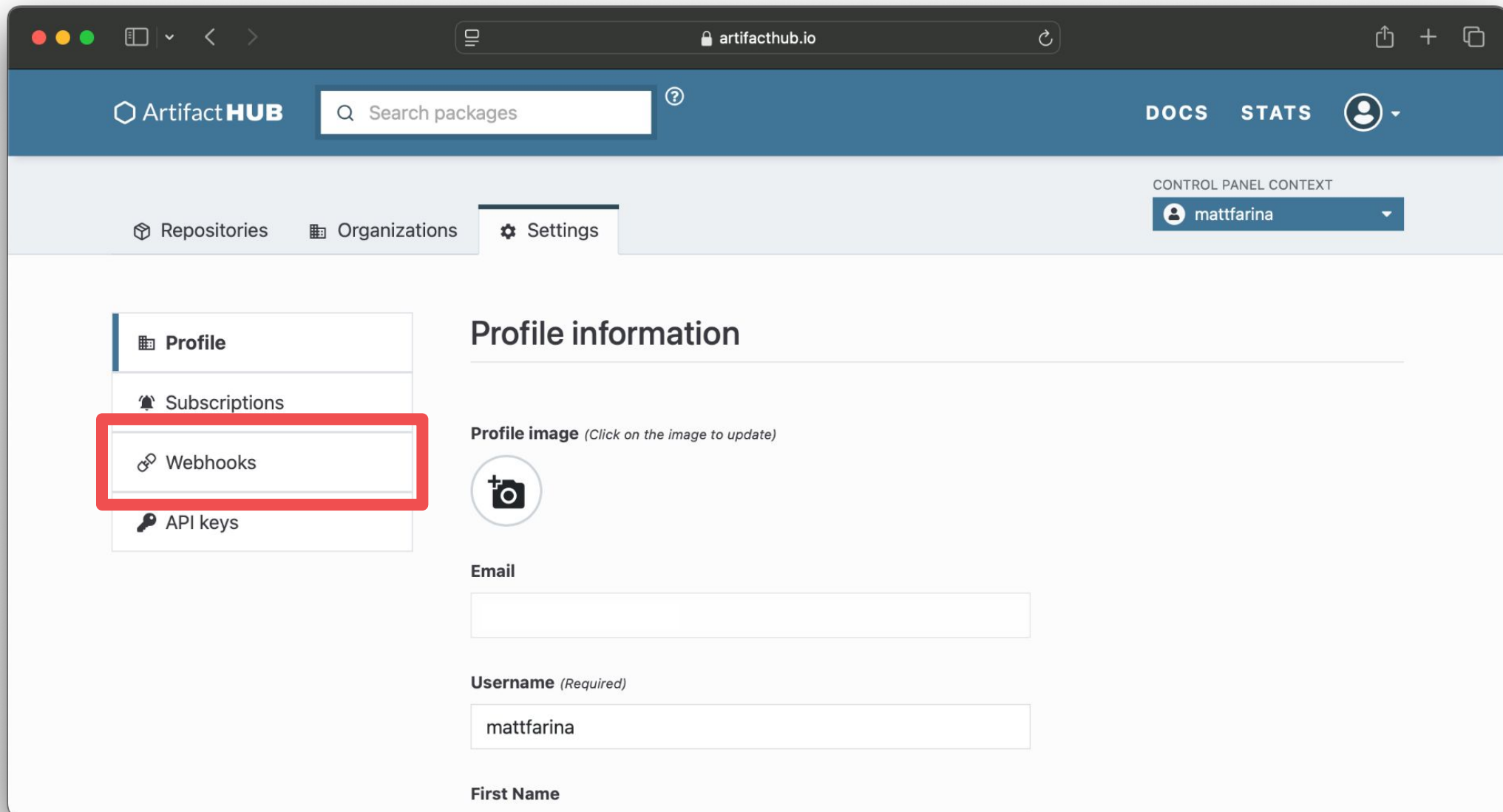
Europe 2025



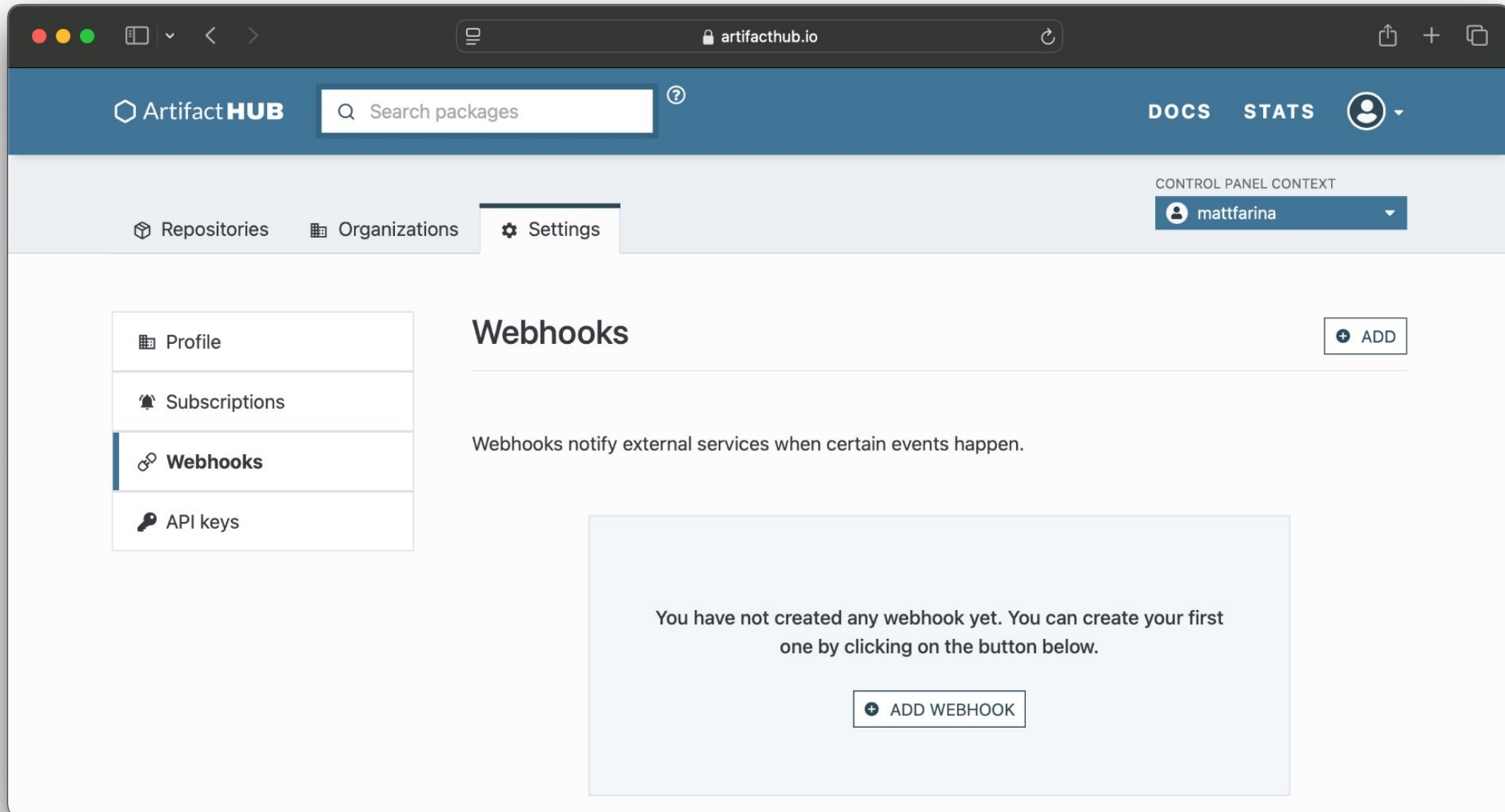
The screenshot shows the Artifact Hub website interface. The main heading reads "Find, install and publish Cloud Native packages". Below this is a search bar with the placeholder text "Search packages". A tip below the search bar states: "Tip: Use - to exclude words from your search. Example: apache -solr -hadoop". Further down, there are buttons for "Tekton tasks and pipelines", "Helm Charts in the storage category", "Falco rules for CVE", "Keptn integrations", and "Official Prometheus packages". At the bottom, two large numbers are displayed: "16793" and "337298".

In the top right corner, there is a user menu. The menu is open, showing the user is signed in as "mattfarina". The menu options are: "THEME" (with sub-options: Automatic, Light, Dark), "★ Starred packages", "⚙️ Control Panel" (highlighted with a red rectangle), and "➡️ Sign out".





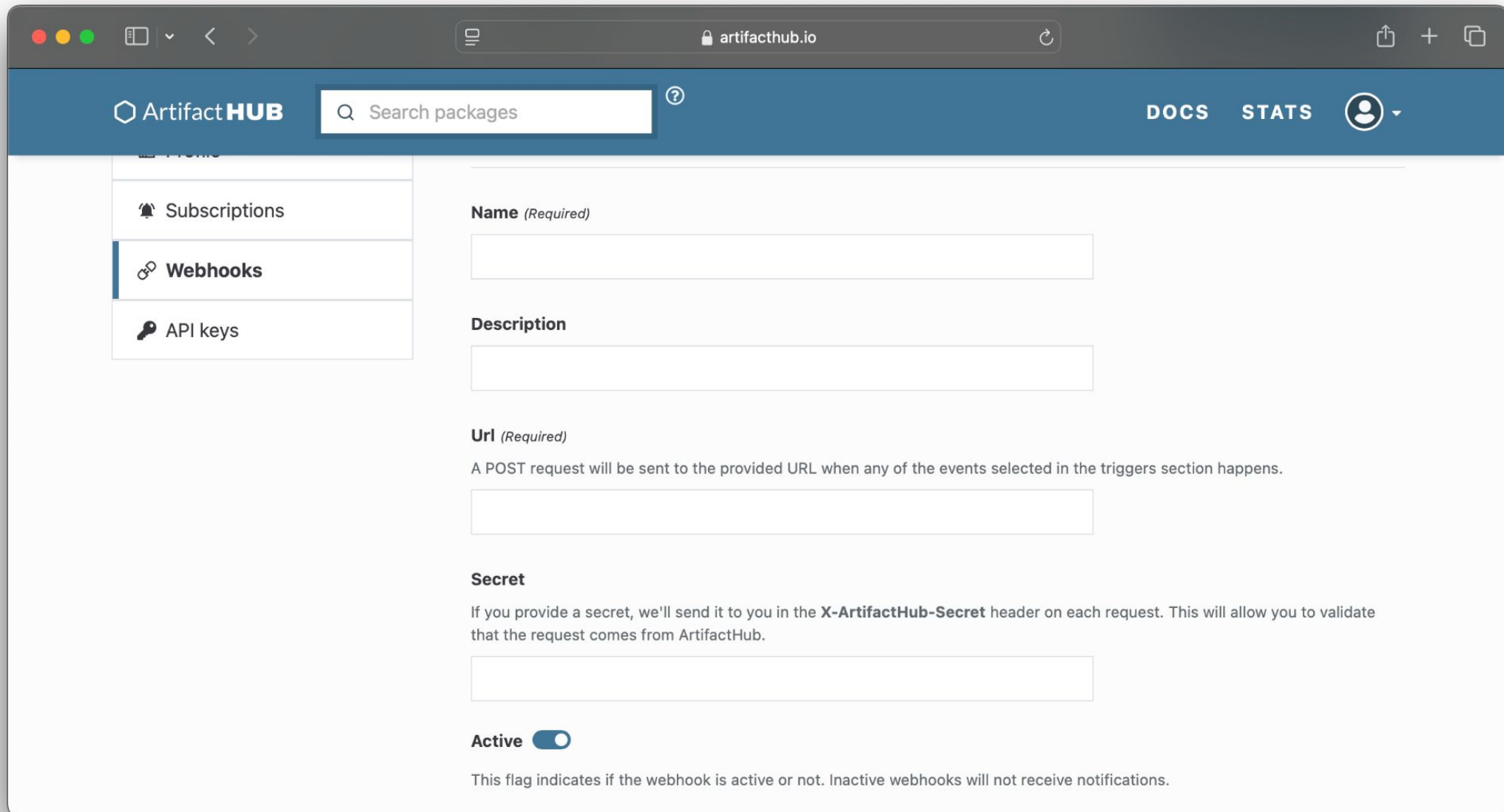
Webhooks



The screenshot shows the Artifact Hub web interface. At the top, there's a navigation bar with the Artifact HUB logo, a search bar labeled "Search packages", and links for "DOCS" and "STATS". Below this is a secondary navigation bar with tabs for "Repositories", "Organizations", and "Settings" (which is active). On the right of this bar, it says "CONTROL PANEL CONTEXT" with a dropdown menu showing the user "mattfarina".

On the left side, there's a sidebar menu with options: "Profile", "Subscriptions", "Webhooks" (which is highlighted with a blue bar), and "API keys".

The main content area is titled "Webhooks" and includes an "ADD" button. Below the title, a text block states: "Webhooks notify external services when certain events happen." Below this, a light blue box contains the message: "You have not created any webhook yet. You can create your first one by clicking on the button below." At the bottom of this box is an "ADD WEBHOOK" button.



The screenshot shows a web browser window at artifacthub.io. The page has a dark blue header with the ArtifactHUB logo, a search bar, and links for DOCS, STATS, and a user profile. A left sidebar contains links for Subscriptions, Webhooks (which is highlighted), and API keys. The main content area is for configuring a new webhook. It includes fields for Name (Required), Description, and Url (Required). Below the Url field is a paragraph explaining that a POST request will be sent to the provided URL when any of the events selected in the triggers section happens. There is also a Secret section with a paragraph explaining that if a secret is provided, it will be sent in the X-ArtifactHub-Secret header on each request to allow for validation. At the bottom, there is an Active toggle switch, which is currently turned on, and a paragraph explaining that this flag indicates if the webhook is active or not.

ArtifactHUB

Search packages

DOCS STATS

Subscriptions

Webhooks

API keys

Name *(Required)*

Description

Url *(Required)*

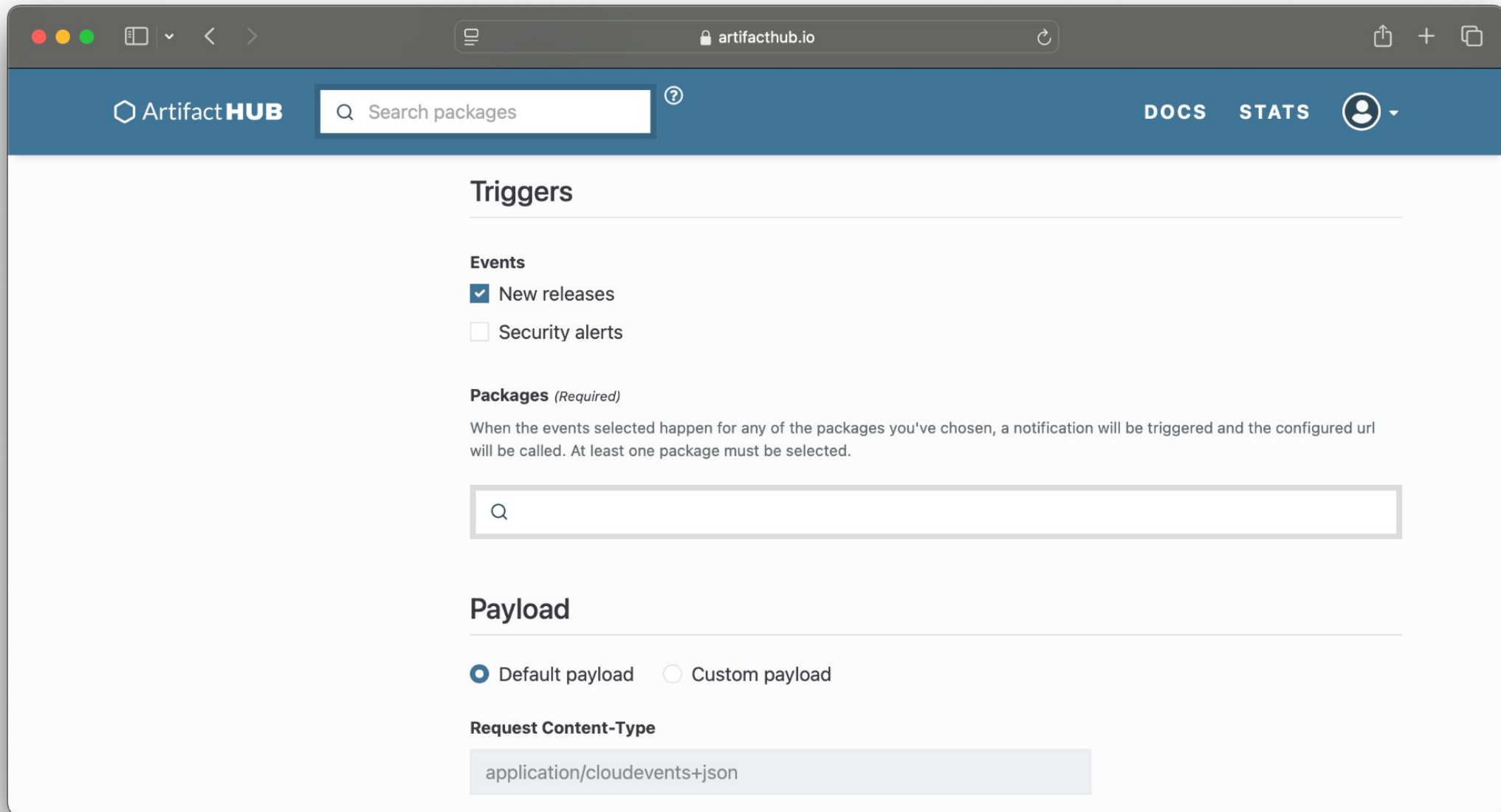
A POST request will be sent to the provided URL when any of the events selected in the triggers section happens.

Secret

If you provide a secret, we'll send it to you in the **X-ArtifactHub-Secret** header on each request. This will allow you to validate that the request comes from ArtifactHub.

Active ☒

This flag indicates if the webhook is active or not. Inactive webhooks will not receive notifications.



The screenshot shows a web browser window with the URL `artifacthub.io`. The page header includes the Artifact HUB logo, a search bar with the placeholder text "Search packages", and links for "DOCS" and "STATS". The main content area is titled "Triggers" and contains two sections: "Events" and "Packages (Required)". In the "Events" section, the "New releases" checkbox is checked, and the "Security alerts" checkbox is unchecked. The "Packages (Required)" section includes a text box for selecting packages. Below this, the "Payload" section has two radio buttons: "Default payload" (selected) and "Custom payload". The "Request Content-Type" section has a text box containing the value `application/cloudevents+json`.

Triggers

Events

☒ New releases

☐ Security alerts

Packages *(Required)*

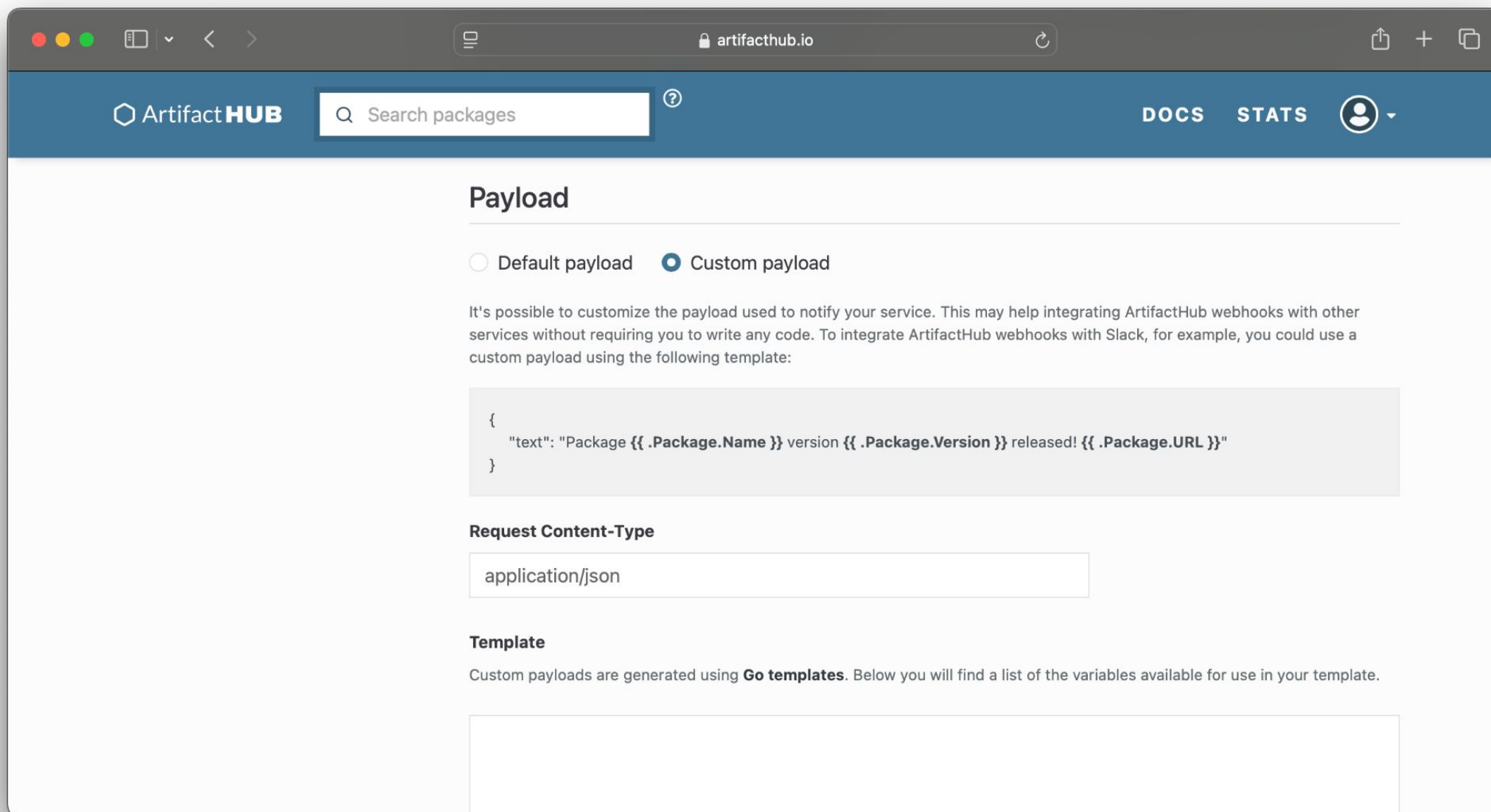
When the events selected happen for any of the packages you've chosen, a notification will be triggered and the configured url will be called. At least one package must be selected.

Payload

☒ Default payload ☐ Custom payload

Request Content-Type

`application/cloudevents+json`



The screenshot shows a web browser window with the URL `artifacthub.io`. The page header includes the ArtifactHUB logo, a search bar with the placeholder text "Search packages", and links for "DOCS" and "STATS". A user profile icon is also visible.

Payload

☐ Default payload ☒ Custom payload

It's possible to customize the payload used to notify your service. This may help integrating ArtifactHub webhooks with other services without requiring you to write any code. To integrate ArtifactHub webhooks with Slack, for example, you could use a custom payload using the following template:

```
{
  "text": "Package {{ .Package.Name }} version {{ .Package.Version }} released! {{ .Package.URL }}"
}
```

Request Content-Type

Template

Custom payloads are generated using **Go templates**. Below you will find a list of the variables available for use in your template.



Europe 2025

Subscriptions



Subscriptions

 Artifact HUB

[DOCS](#) [STATS](#) 

[< Back to search results](#)



sigstore

 Helm plugin

 sigstore  sigstore

This plugin integrates Helm into the Sigstore ecosystem.



helm-sigstore

Artifact Hub

 helm-sigstore

 SLSA level 3

Plugin for [Helm](#) to integrate the [sigstore](#) ecosystem. Search, upload and verify signed Helm Charts in the [Rekor](#) Transparency Log.

Info

 **INSTALL**



Subscriptions

 Artifact HUB

[DOCS](#) [STATS](#) 

[< Back to search results](#)



sigstore

 Helm plugin

 sigstore  sigstore

This plugin integrates Helm into the Sigstore ecosystem.

 Star

3

 **New releases**

☐ Receive a notification when a new version of this package is released.

 **Security alerts**

☐ Receive a notification when important security vulnerabilities are found in the latest version of this package.

 **INSTALL**

 **helm-sigstore**

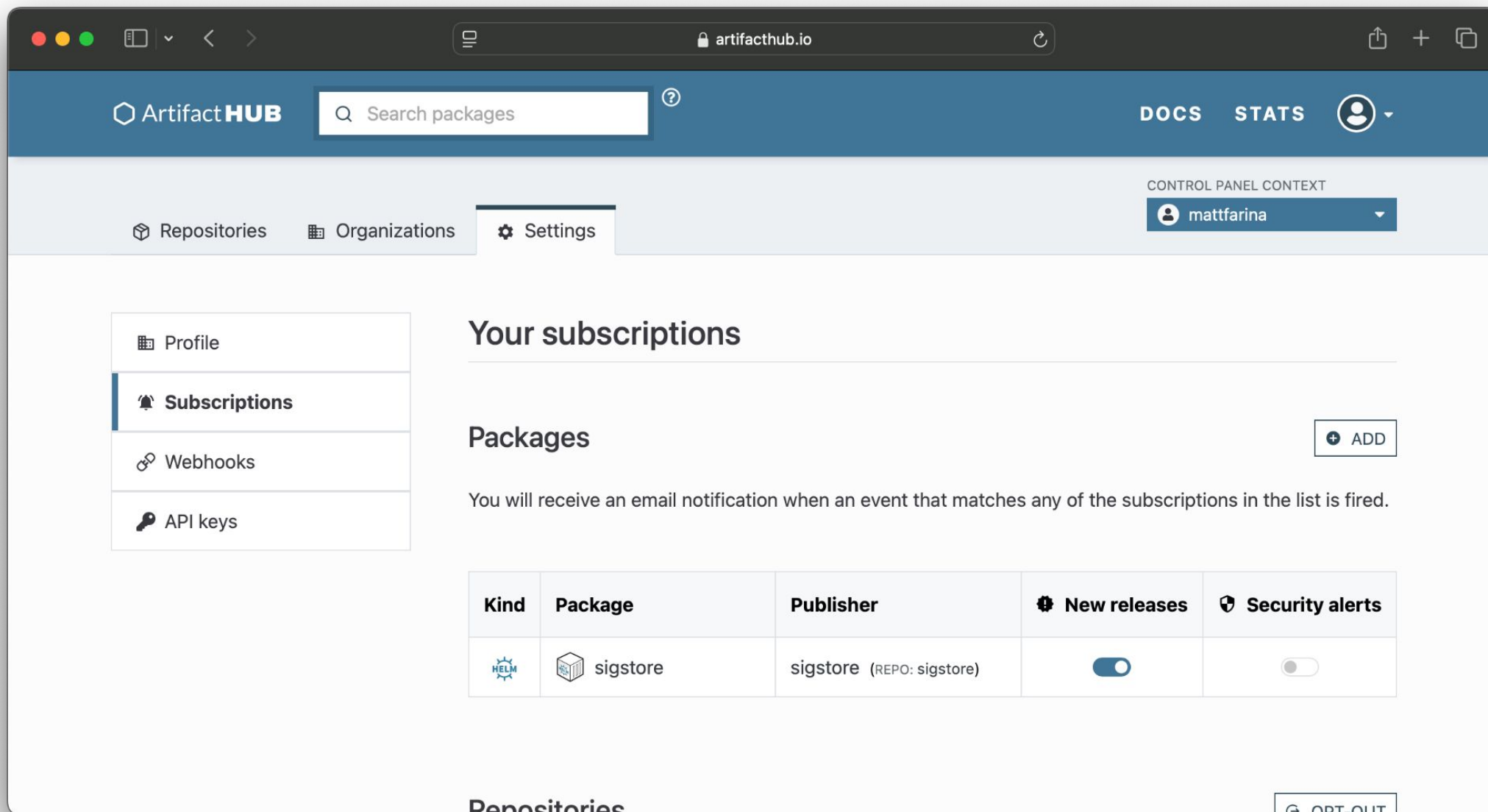
 Artifact Hub  helm-sigstore  SLSA  level 3

Plugin for [Helm](#) to integrate the [sigstore](#) ecosystem. Search, upload and verify signed Helm Charts in the [Rekor](#) Transparency Log.

Info



Subscriptions



Artifact HUB

Search packages

DOCS STATS

CONTROL PANEL CONTEXT

mattfarina

Repositories Organizations Settings

Profile

Subscriptions

Webhooks

API keys

Your subscriptions

Packages

+ ADD

You will receive an email notification when an event that matches any of the subscriptions in the list is fired.

Kind	Package	Publisher	New releases	Security alerts
	 sigstore	sigstore (REPO: sigstore)	☒	☐

Repositories

OPT-OUT

The API



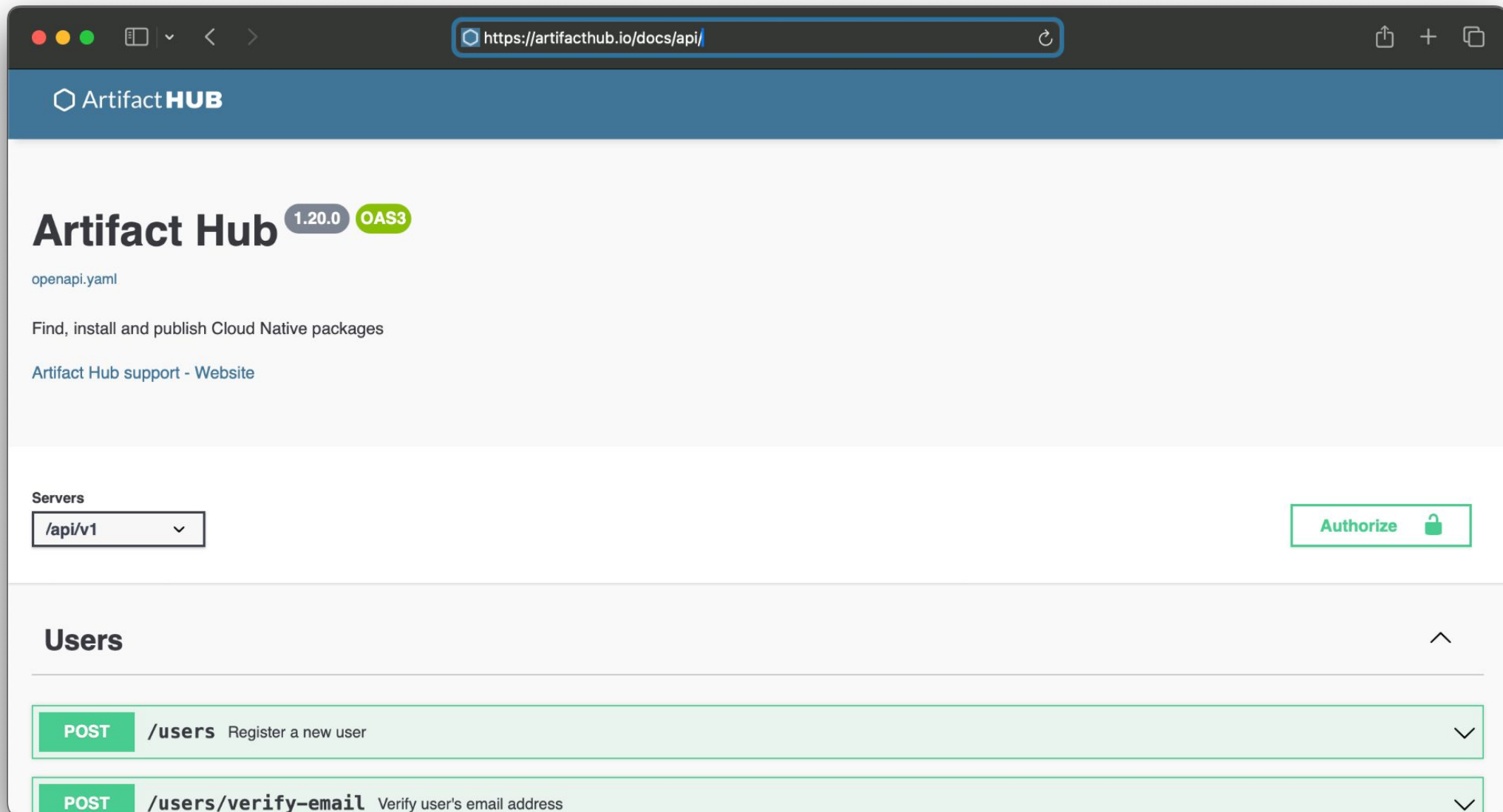
KubeCon



CloudNativeCon

Europe 2025





The screenshot shows a web browser window with the URL `https://artifacthub.io/docs/api/`. The page header features the "Artifact HUB" logo. The main content area displays "Artifact Hub" with version "1.20.0" and "OAS3" tags, followed by the text "openapi.yaml" and "Find, install and publish Cloud Native packages". A link "Artifact Hub support - Website" is also present. Below this, a "Servers" section contains a dropdown menu showing "/api/v1" and an "Authorize" button with a lock icon. A "Users" section is partially visible, showing two API endpoints: "POST /users" (Register a new user) and "POST /users/verify-email" (Verify user's email address).

Artifact HUB

Artifact Hub 1.20.0 OAS3

openapi.yaml

Find, install and publish Cloud Native packages

[Artifact Hub support - Website](#)

Servers

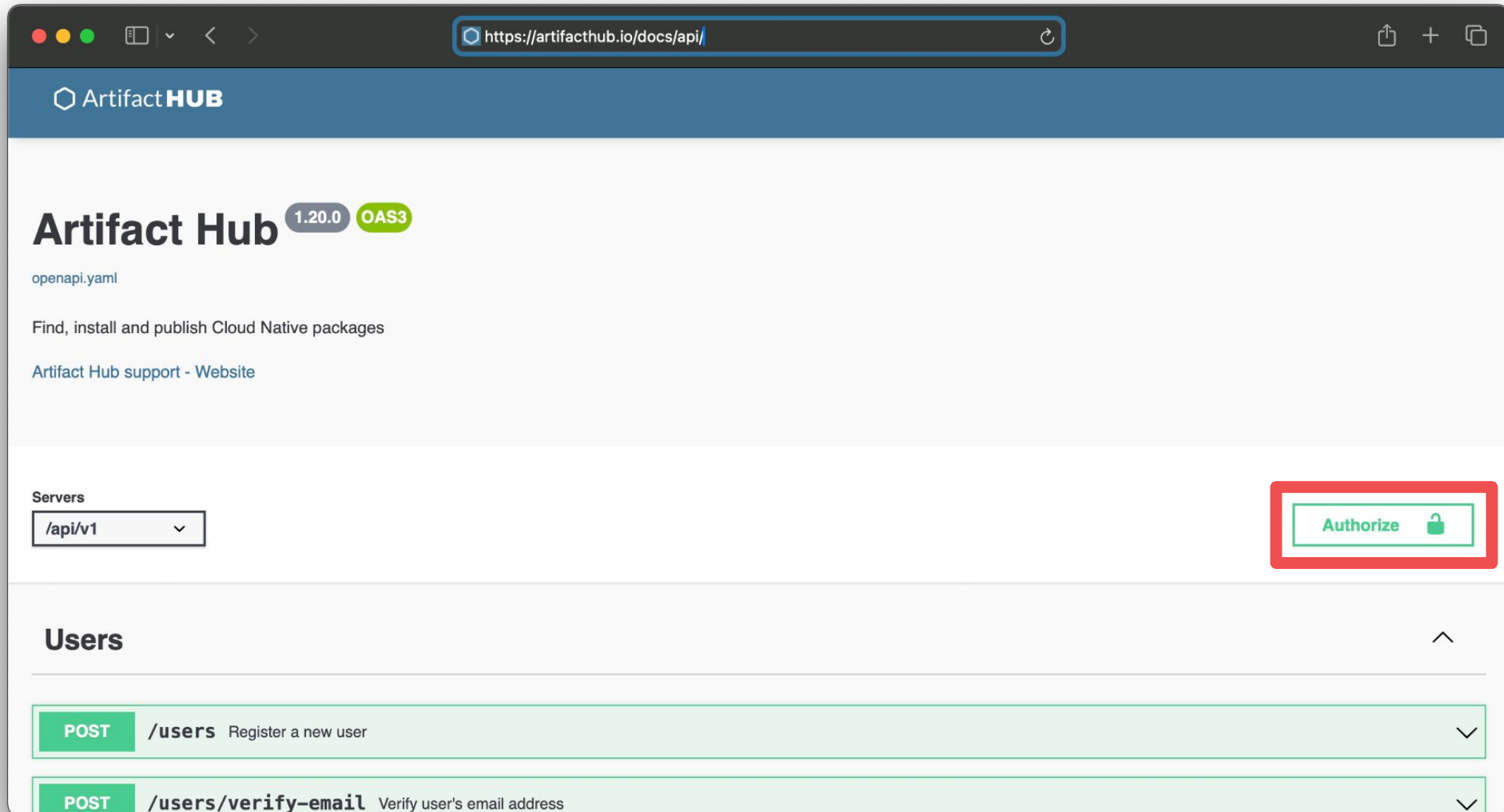
/api/v1

Authorize

Users

POST /users Register a new user

POST /users/verify-email Verify user's email address



The screenshot shows a web browser window with the URL `https://artifacthub.io/docs/api/` in the address bar. The page header features the "Artifact HUB" logo. The main content area displays "Artifact Hub" with version tags "1.20.0" and "OAS3", followed by the text "openapi.yaml" and "Find, install and publish Cloud Native packages". A link "Artifact Hub support - Website" is also present. On the left, a "Servers" section contains a dropdown menu showing "/api/v1". On the right, an "Authorize" button with a lock icon is highlighted by a red rectangle. Below this, a "Users" section is visible, containing two API endpoint entries: "POST /users Register a new user" and "POST /users/verify-email Verify user's email address".

Artifact HUB

Artifact Hub 1.20.0 OAS3

openapi.yaml

Find, install and publish Cloud Native packages

[Artifact Hub support - Website](#)

Servers

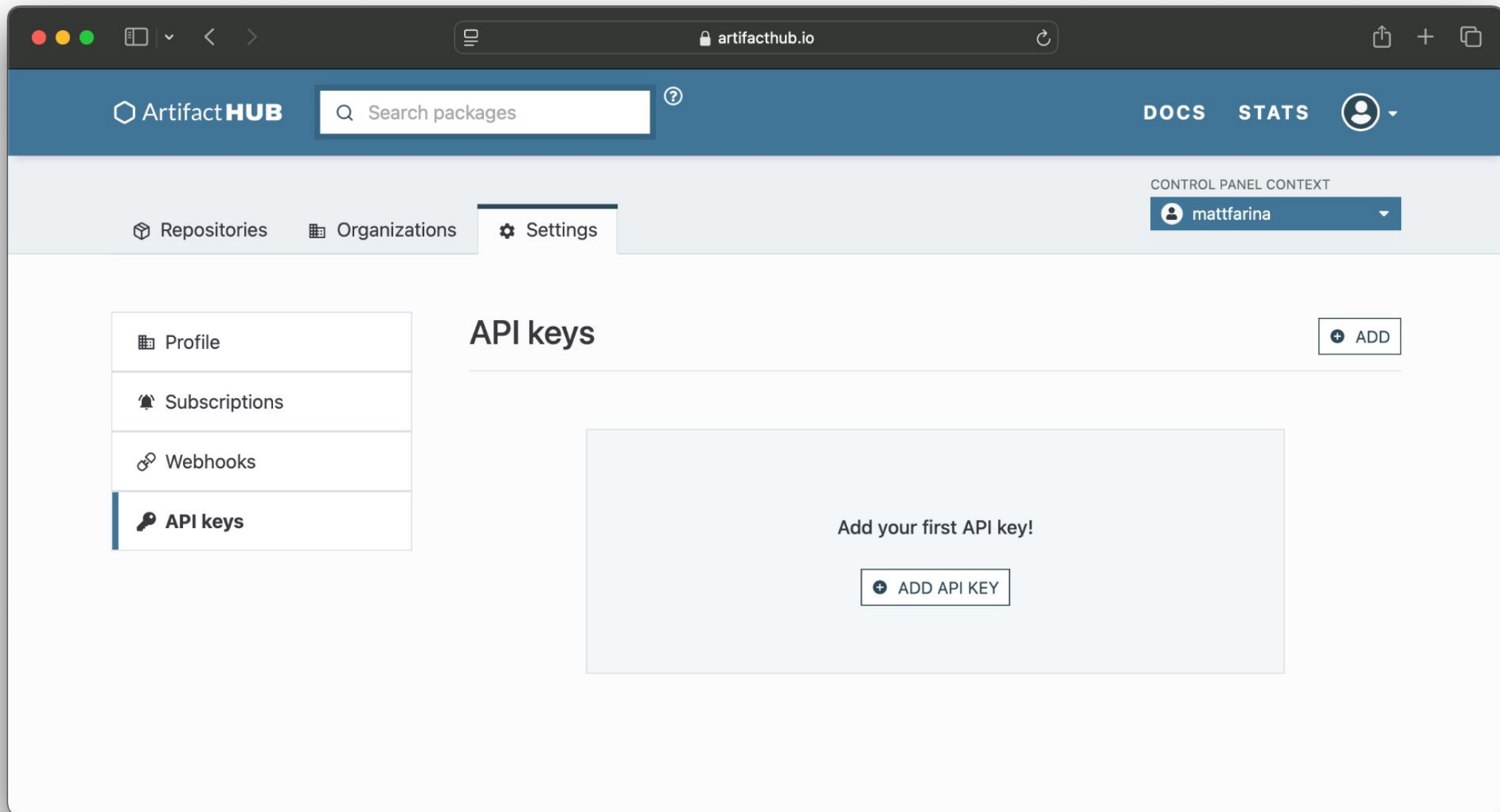
/api/v1

Authorize

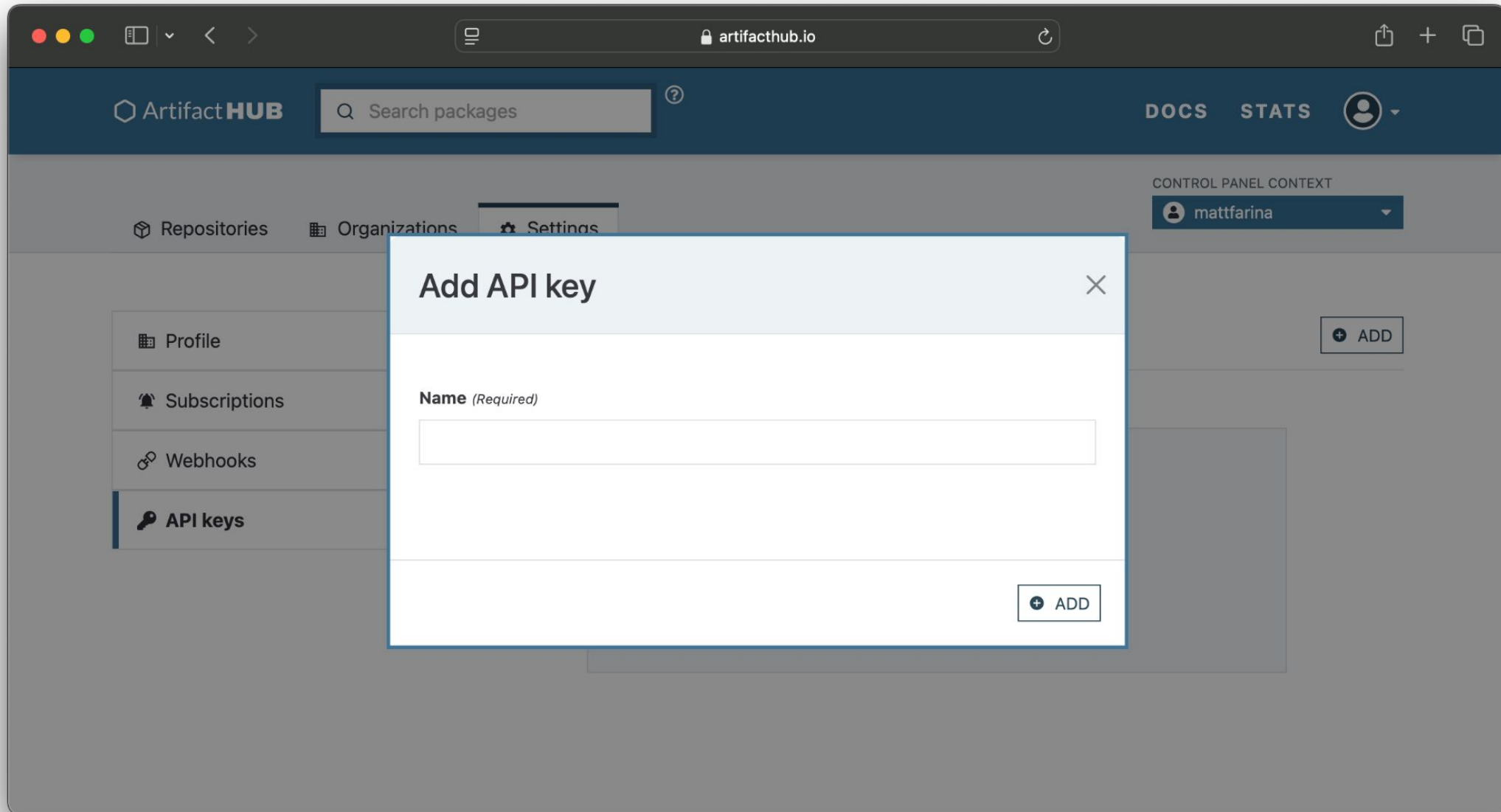
Users

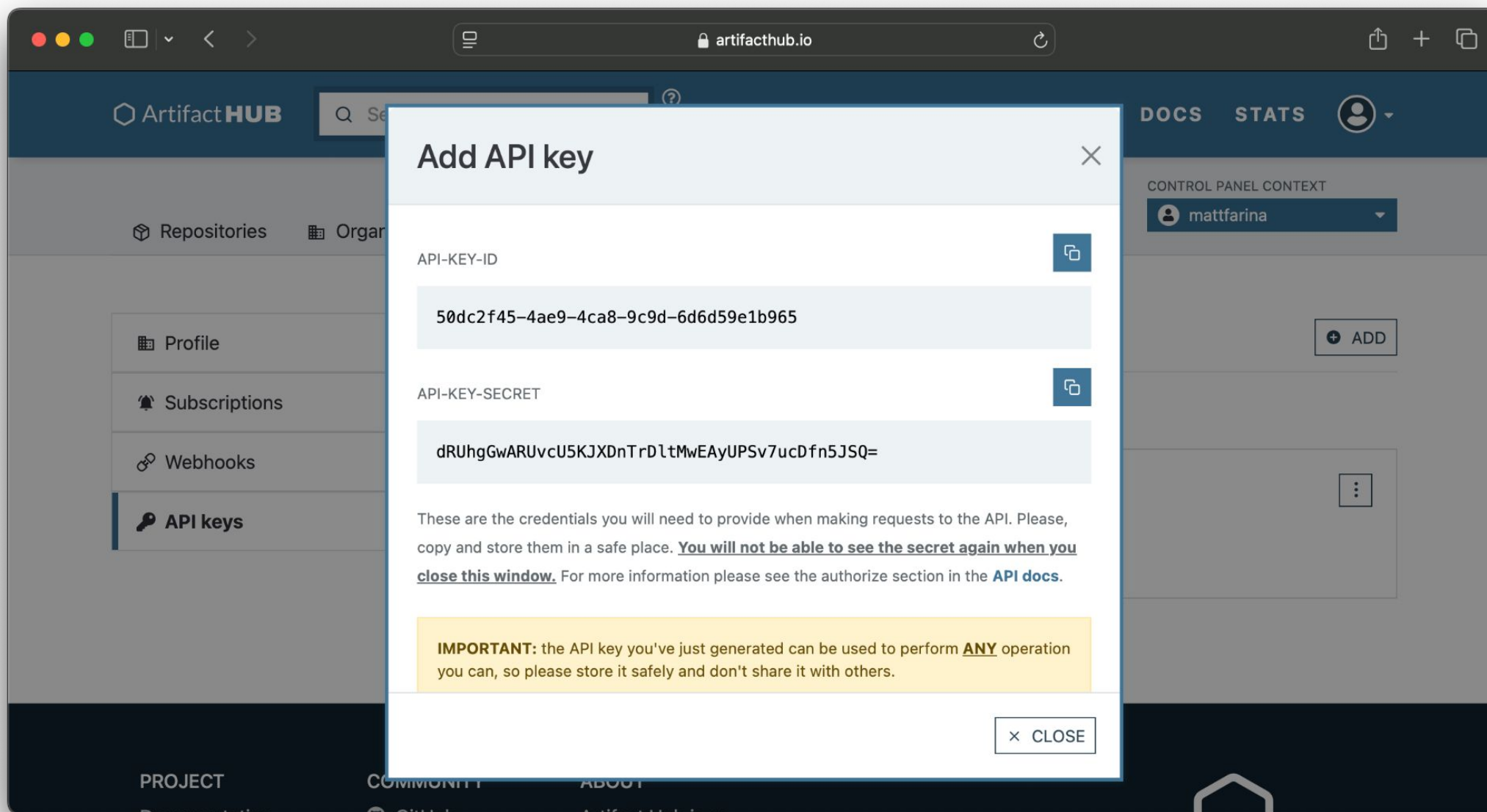
POST /users Register a new user

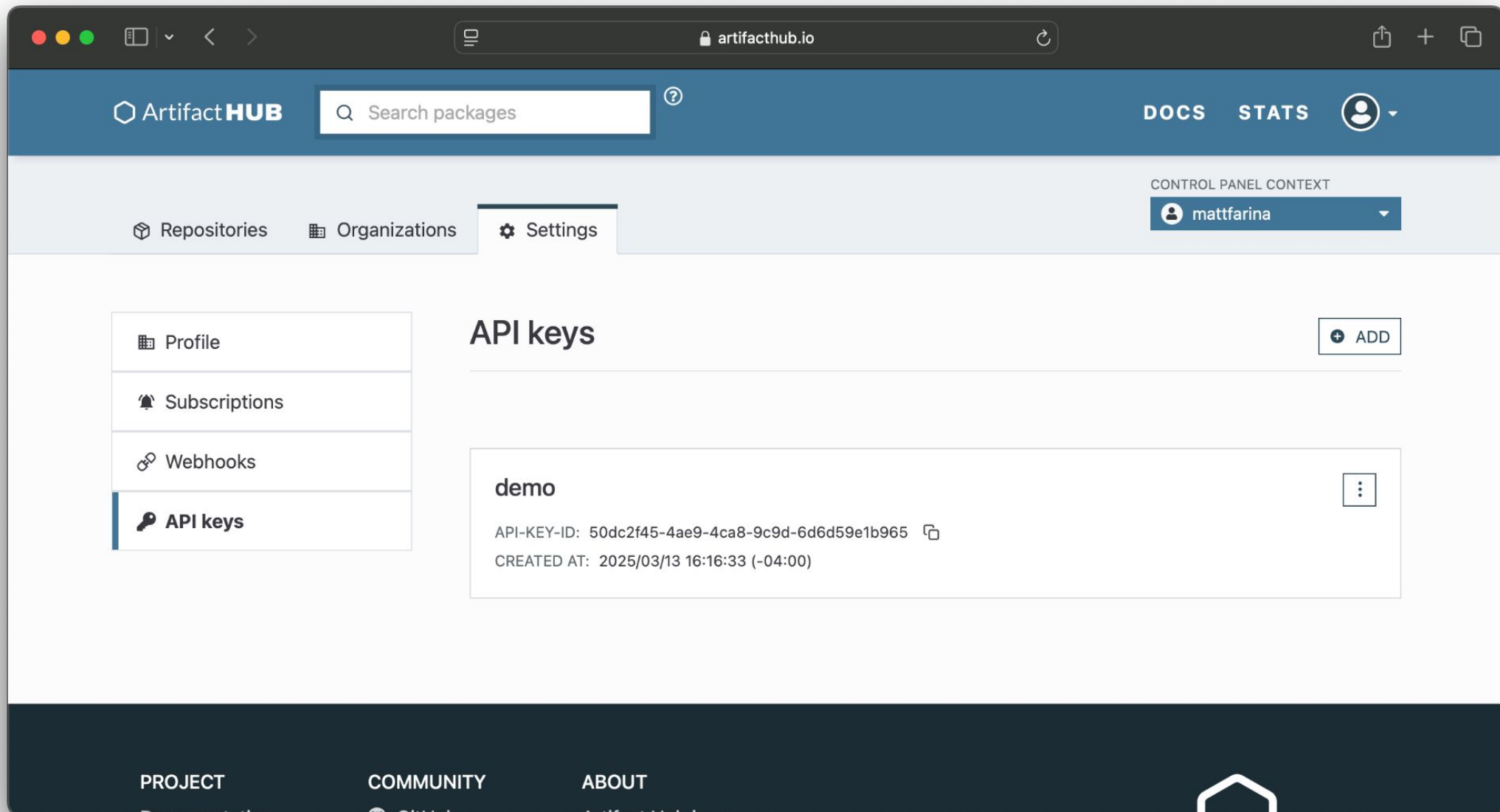
POST /users/verify-email Verify user's email address

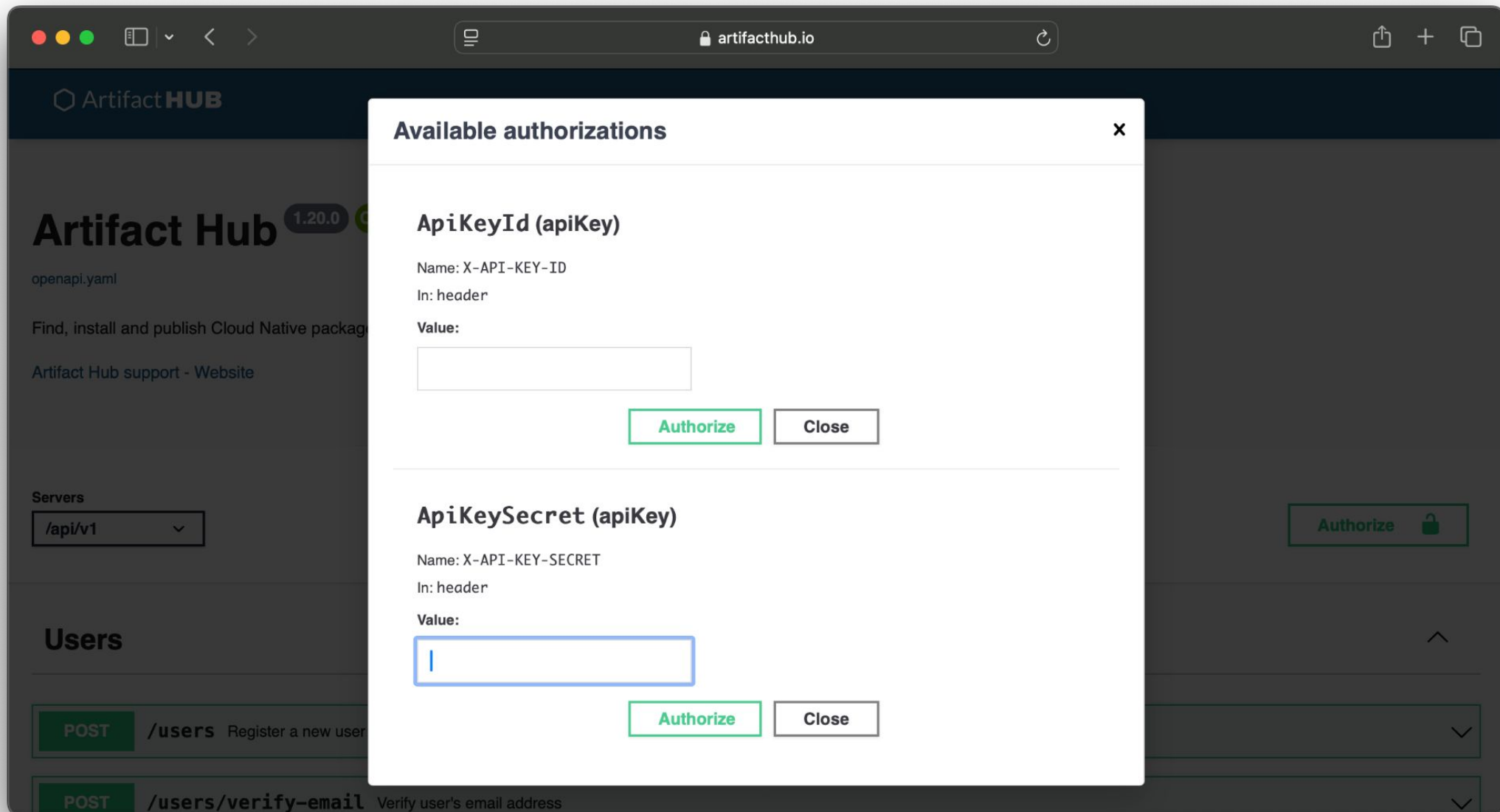


APIs









The screenshot shows the Artifact Hub website interface. The main header includes the 'Artifact HUB' logo and a version indicator '1.20.0'. The main content area displays 'Artifect Hub' (note the typo in the image), 'openapi.yaml', and a description: 'Find, install and publish Cloud Native packages'. Below this is a link to 'Artifact Hub support - Website'. A 'Servers' dropdown menu is set to '/api/v1'. The 'Users' section shows two endpoints: 'POST /users Register a new user' and 'POST /users/verify-email Verify user's email address'. An 'Available authorizations' modal is open in the center, showing two authorization options: 'ApiKeyId (apiKey)' and 'ApiKeySecret (apiKey)'. Each option has a 'Name', 'In' (header), and a 'Value' input field. Both modal entries have 'Authorize' and 'Close' buttons. The background website is dimmed.

Artifact HUB

1.20.0

Artifect Hub

openapi.yaml

Find, install and publish Cloud Native packages

Artifact Hub support - Website

Servers

/api/v1

Users

POST /users Register a new user

POST /users/verify-email Verify user's email address

Available authorizations

ApiKeyId (apiKey)

Name: X-API-KEY-ID

In: header

Value:

Authorize Close

ApiKeySecret (apiKey)

Name: X-API-KEY-SECRET

In: header

Value:

Authorize Close

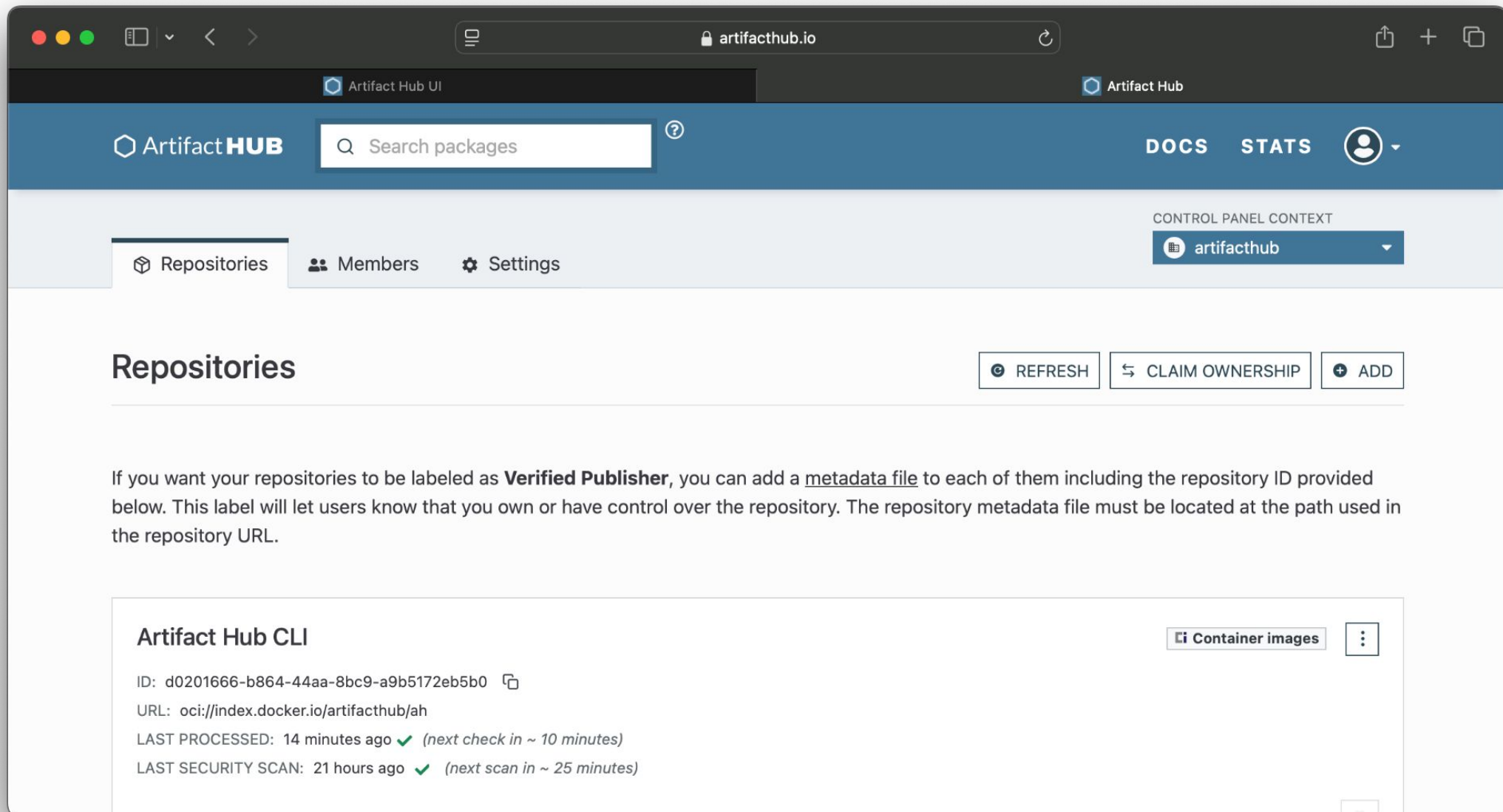


Europe 2025

Org Authorization



Authorization



The screenshot shows the Artifact Hub web interface. The browser address bar displays 'artifacthub.io'. The page header includes the 'Artifact HUB' logo, a search bar with the placeholder 'Search packages', and links for 'DOCS', 'STATS', and a user profile. Below the header, a navigation bar contains 'Repositories', 'Members', and 'Settings'. On the right, a 'CONTROL PANEL CONTEXT' dropdown is set to 'artifacthub'. The main content area is titled 'Repositories' and features three buttons: 'REFRESH', 'CLAIM OWNERSHIP', and 'ADD'. A text block explains that adding a 'metadata file' can label a repository as a 'Verified Publisher'. Below this, a card displays details for the 'Artifact Hub CLI' repository, including its ID, URL, and last processed/scan times with status indicators. A 'Container images' button is visible in the top right of the repository card.

artifacthub.io

Artifact Hub UI

Artifact Hub

Artifact HUB

Search packages

DOCS STATS

CONTROL PANEL CONTEXT

artifacthub

Repositories Members Settings

Repositories

REFRESH CLAIM OWNERSHIP ADD

If you want your repositories to be labeled as **Verified Publisher**, you can add a [metadata file](#) to each of them including the repository ID provided below. This label will let users know that you own or have control over the repository. The repository metadata file must be located at the path used in the repository URL.

Artifact Hub CLI

ID: d0201666-b864-44aa-8bc9-a9b5172eb5b0

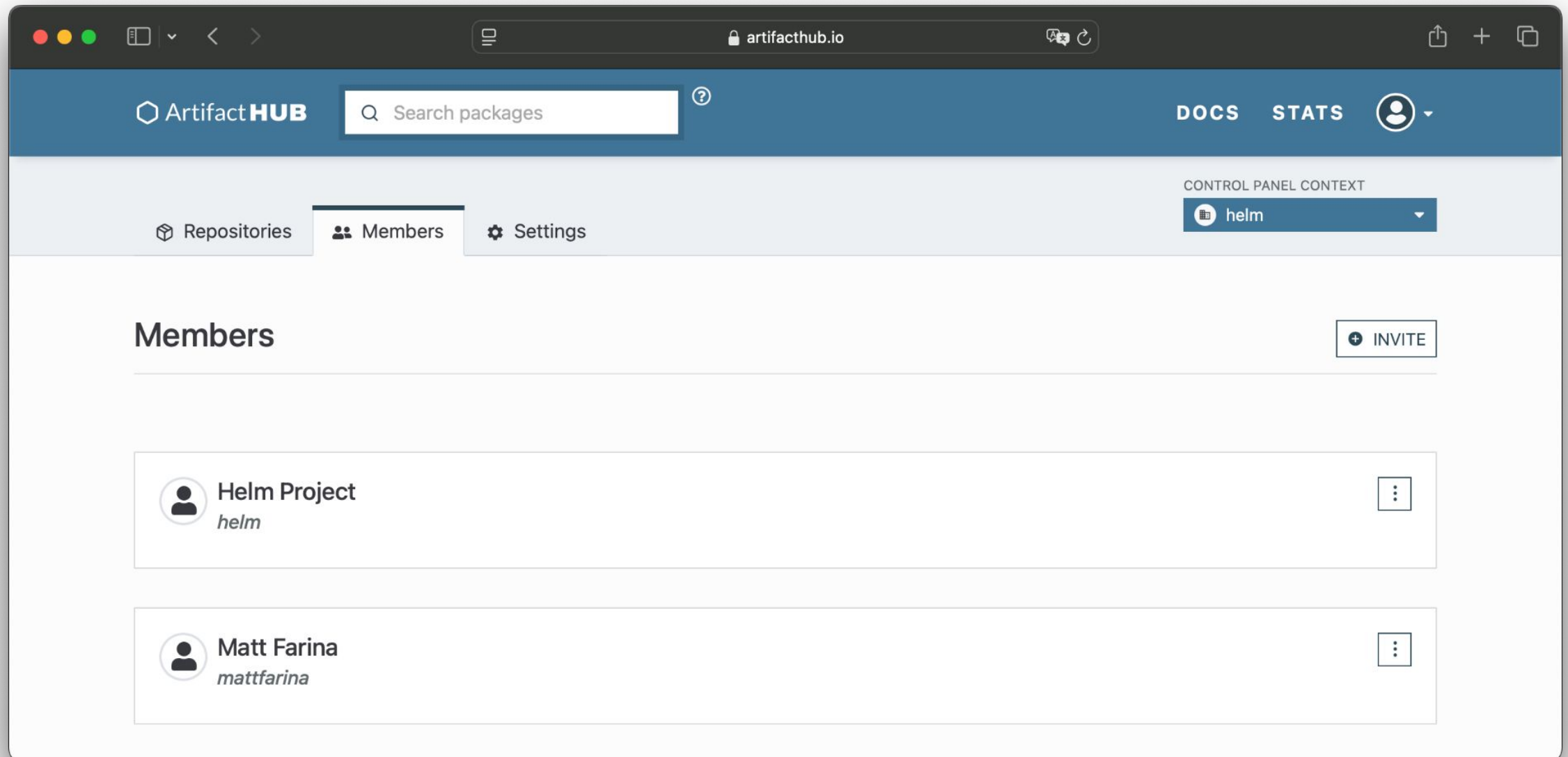
URL: oci://index.docker.io/artifacthub/ah

LAST PROCESSED: 14 minutes ago ✓ (next check in ~ 10 minutes)

LAST SECURITY SCAN: 21 hours ago ✓ (next scan in ~ 25 minutes)

Container images

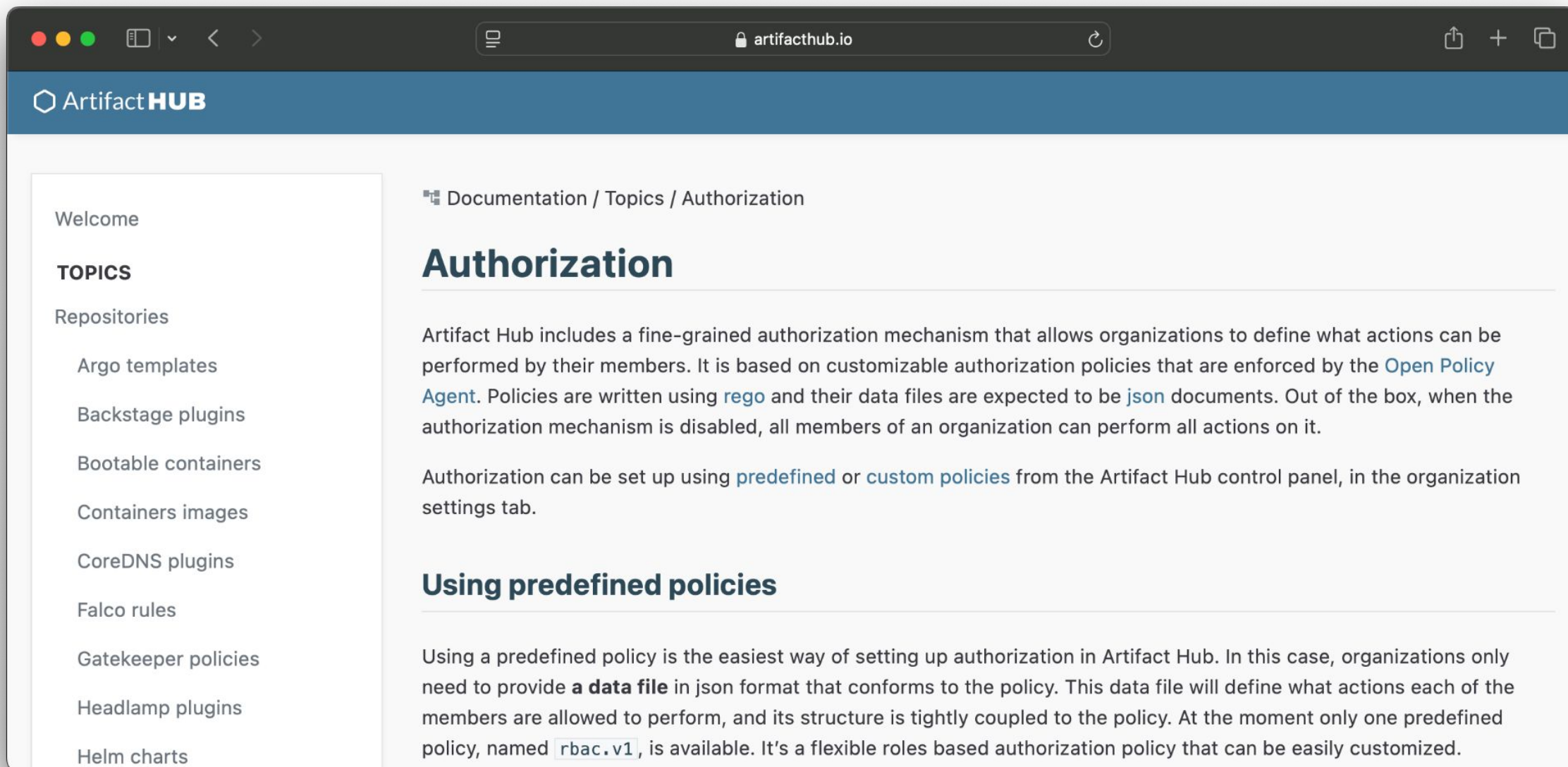
Authorization



The screenshot shows the Artifact Hub web interface. The browser address bar displays `artifacthub.io`. The top navigation bar includes the Artifact HUB logo, a search bar with the placeholder text "Search packages", and links for "DOCS" and "STATS". A user profile icon is visible in the top right corner. Below the navigation bar, there are tabs for "Repositories", "Members", and "Settings". The "Members" tab is currently selected. In the top right corner of the main content area, there is a "CONTROL PANEL CONTEXT" dropdown menu showing "helm". The main content area is titled "Members" and features an "+ INVITE" button. Below the title, there is a list of members:

- Helm Project**
helm
- Matt Farina**
mattfarina

Each member entry includes a user icon and a three-dot menu icon for additional actions.



The screenshot shows a web browser window with the URL `artifacthub.io`. The page is titled "Artifact HUB" and displays a sidebar with a "TOPICS" section. The main content area shows the "Authorization" documentation page, which includes a breadcrumb trail "Documentation / Topics / Authorization", a main heading "Authorization", and two sub-sections: "Using predefined policies" and "Using custom policies".

Welcome

TOPICS

Repositories

- Argo templates
- Backstage plugins
- Bootable containers
- Containers images
- CoreDNS plugins
- Falco rules
- Gatekeeper policies
- Headlamp plugins
- Helm charts

Documentation / Topics / Authorization

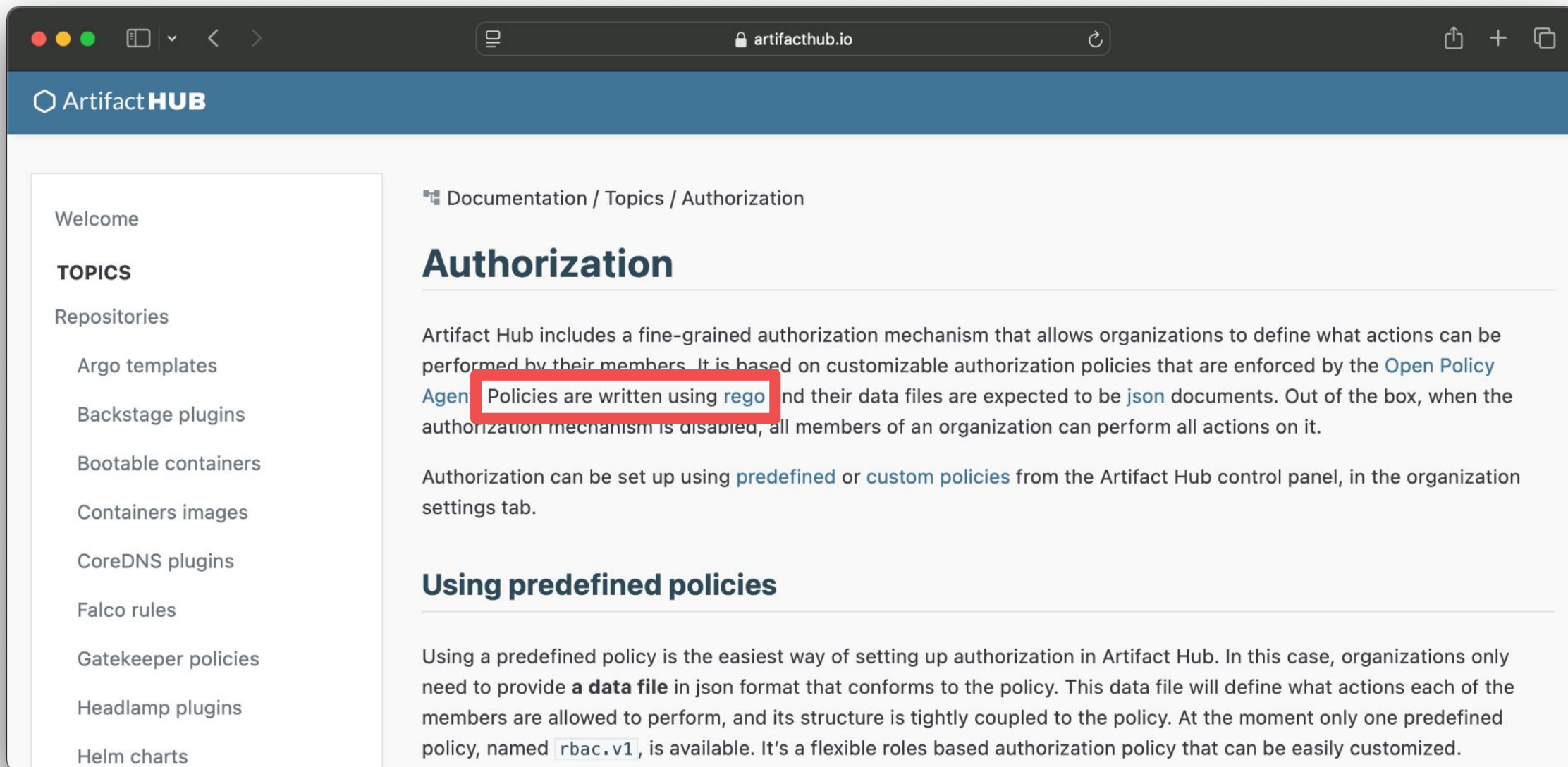
Authorization

Artifact Hub includes a fine-grained authorization mechanism that allows organizations to define what actions can be performed by their members. It is based on customizable authorization policies that are enforced by the [Open Policy Agent](#). Policies are written using [rego](#) and their data files are expected to be [json](#) documents. Out of the box, when the authorization mechanism is disabled, all members of an organization can perform all actions on it.

Authorization can be set up using [predefined](#) or [custom policies](#) from the Artifact Hub control panel, in the organization settings tab.

Using predefined policies

Using a predefined policy is the easiest way of setting up authorization in Artifact Hub. In this case, organizations only need to provide **a data file** in json format that conforms to the policy. This data file will define what actions each of the members are allowed to perform, and its structure is tightly coupled to the policy. At the moment only one predefined policy, named `rbac.v1`, is available. It's a flexible roles based authorization policy that can be easily customized.



The screenshot shows a web browser window with the URL `artifacthub.io`. The page is titled "Artifact HUB" and displays a sidebar with a "TOPICS" section. The main content area is titled "Authorization" and contains a paragraph explaining the authorization mechanism. A red box highlights the text "Policies are written using `rego`".

Welcome

TOPICS

Repositories

- Argo templates
- Backstage plugins
- Bootable containers
- Containers images
- CoreDNS plugins
- Falco rules
- Gatekeeper policies
- Headlamp plugins
- Helm charts

Documentation / Topics / Authorization

Authorization

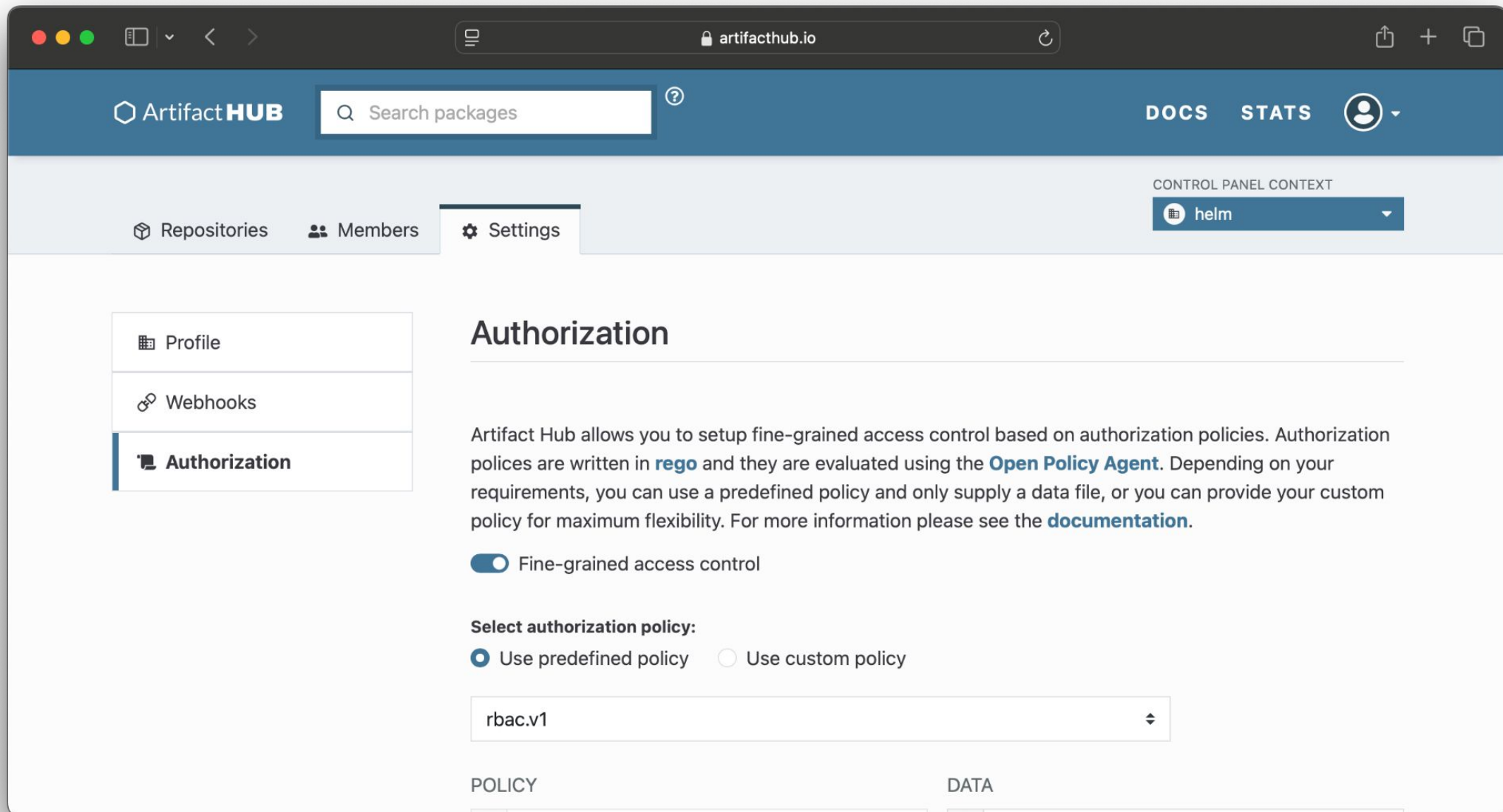
Artifact Hub includes a fine-grained authorization mechanism that allows organizations to define what actions can be performed by their members. It is based on customizable authorization policies that are enforced by the [Open Policy Agent](#). Policies are written using `rego` and their data files are expected to be `json` documents. Out of the box, when the authorization mechanism is disabled, all members of an organization can perform all actions on it.

Authorization can be set up using [predefined](#) or [custom policies](#) from the Artifact Hub control panel, in the organization settings tab.

Using predefined policies

Using a predefined policy is the easiest way of setting up authorization in Artifact Hub. In this case, organizations only need to provide **a data file** in `json` format that conforms to the policy. This data file will define what actions each of the members are allowed to perform, and its structure is tightly coupled to the policy. At the moment only one predefined policy, named `rbac.v1`, is available. It's a flexible roles based authorization policy that can be easily customized.

Authorization



The screenshot shows the Artifact Hub web interface in a browser window. The URL is artifacthub.io. The top navigation bar includes the Artifact HUB logo, a search bar with the placeholder "Search packages", and links for "DOCS" and "STATS". A user profile icon is on the right. Below the navigation bar, there are tabs for "Repositories", "Members", and "Settings". The "Settings" tab is active, and within it, the "Authorization" sub-tab is selected. On the left side of the "Authorization" page, there is a sidebar with links for "Profile", "Webhooks", and "Authorization". The main content area is titled "Authorization" and contains the following text: "Artifact Hub allows you to setup fine-grained access control based on authorization policies. Authorization polices are written in **rego** and they are evaluated using the **Open Policy Agent**. Depending on your requirements, you can use a predefined policy and only supply a data file, or you can provide your custom policy for maximum flexibility. For more information please see the **documentation**." Below this text, there is a toggle switch for "Fine-grained access control" which is turned on. Under the heading "Select authorization policy:", there are two radio buttons: "Use predefined policy" (which is selected) and "Use custom policy". Below the radio buttons, there is a dropdown menu showing "rbac.v1". At the bottom of the page, there are two tabs: "POLICY" and "DATA".

Q&A



KubeCon



CloudNativeCon

Europe 2025

