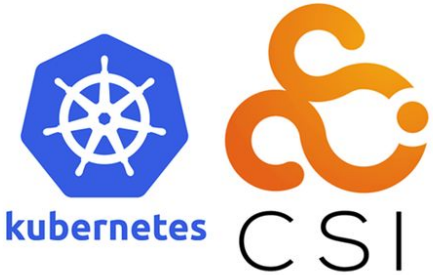
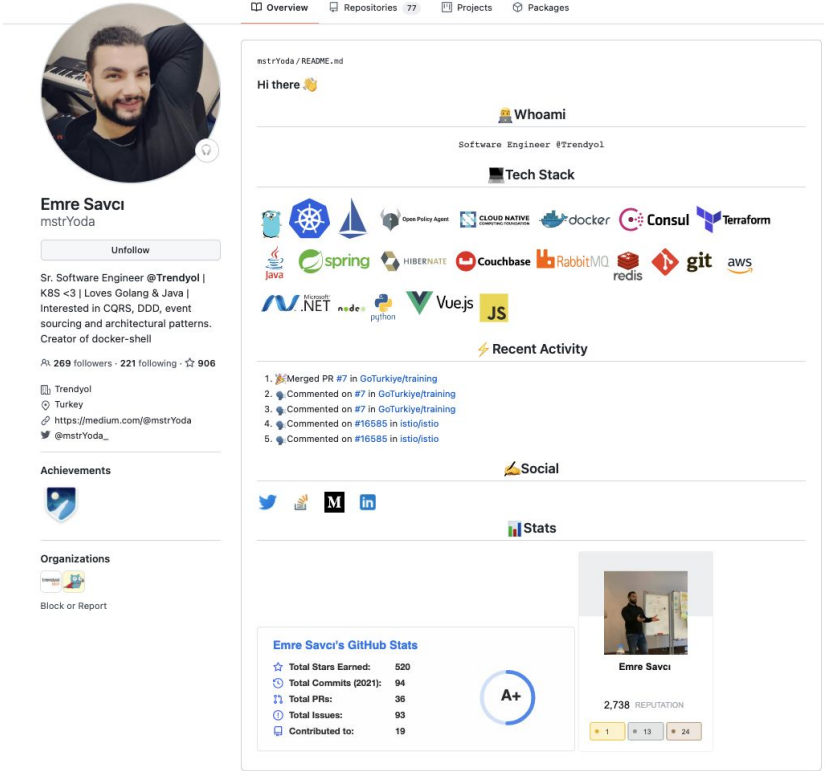


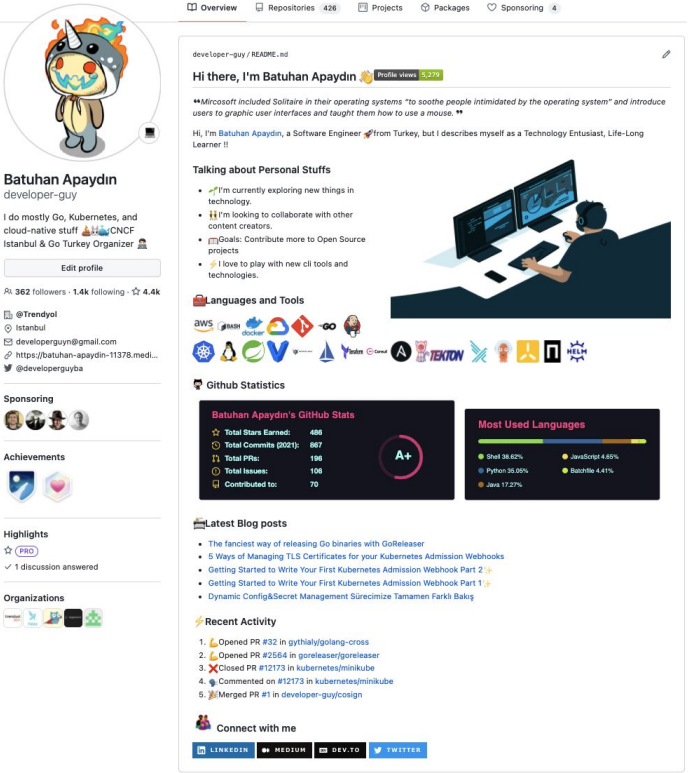
The power of Kubernetes Extensibility

Secrets Store CSI Driver

🤫🔐

Who we are?


Overview
Repositories 77
Projects
Packages
Emre Savcı
mstrYoda
Unfollow
Sr. Software Engineer @Trendyol | K8S <3 | Loves Golang & Java | Interested in CQRS, DDD, event sourcing and architectural patterns. Creator of docker-shell
269 followers · 221 following · ☆ 906
Trendyol
Turkey
https://medium.com/@mstrYoda
@mstrYoda_
Achievements
Organizations
Block or Report
mstrYoda / README.md
Hi there 👋
Whoami
Software Engineer @Trendyol
Tech Stack
Recent Activity
1. 🎉Merged PR #7 in GoTurkiye/training
2. 🗣Commented on #7 in GoTurkiye/training
3. 🗣Commented on #7 in GoTurkiye/training
4. 🗣Commented on #16585 in istio/istio
5. 🗣Commented on #16585 in istio/istio
Social
Stats
Emre Savcı's GitHub Stats
Total Stars Earned: 520
Total Commits (2021): 94
Total PRs: 36
Total Issues: 93
Contributed to: 19
A+
Emre Savcı
2,738 REPUTATION


Overview
Repositories 426
Projects
Packages
Sponsoring 4
Batuhan Apaydın
developer-guy
I do mostly Go, Kubernetes, and cloud-native stuff ☸️🚢CNCF Istanbul & Go Turkey Organizer 🏯
Edit profile
362 followers · 1.4k following · ☆ 4.4k
@Trendyol
Istanbul
developerguyn@gmail.com
https://batuhan-apaydin-11378.medi...
@developerguyba
Sponsoring
Achievements
Highlights
PRO
1 discussion answered
Organizations
developer-guy / README.md
Hi there, I'm Batuhan Apaydın 👋
Profile views 5,279
Mircosoft included Solitaire in their operating systems "to soothe people intimidated by the operating system" and introduce users to graphic user interfaces and taught them how to use a mouse.
Hi, I'm Batuhan Apaydin, a Software Engineer 🚀from Turkey, but I describes myself as a Technology Entusiast, Life-Long Learner !!
Talking about Personal Stuffs
I'm currently exploring new things in technology.
I'm looking to collaborate with other content creators.
Goals: Contribute more to Open Source projects
I love to play with new cli tools and technologies.
Languages and Tools
Github Statistics
Batuhan Apaydin's GitHub Stats
Total Stars Earned: 486
Total Commits (2021): 867
Total PRs: 196
Total Issues: 106
Contributed to: 70
A+
Most Used Languages
Shell 38.62%
JavaScript 4.65%
Python 36.95%
Batchfile 4.41%
Java 17.27%
Latest Blog posts
The fanciest way of releasing Go binaries with GoReleaser
5 Ways of Managing TLS Certificates for your Kubernetes Admission Webhooks
Getting Started to Write Your First Kubernetes Admission Webhook Part 2
Getting Started to Write Your First Kubernetes Admission Webhook Part 1
Dynamic Config&Secret Management Sürecimize Tamamen Farklı Bakış
Recent Activity
1. 💪Opened PR #32 in gythialy/golang-cross
2. 💪Opened PR #2564 in goreleaser/goreleaser
3. ❌Closed PR #12173 in kubernetes/minikube
4. 🗣Commented on #12173 in kubernetes/minikube
5. 🎉Merged PR #1 in developer-guy/cosign
Connect with me
LINKEDIN
MEDIUM
DEV.TO
TWITTER

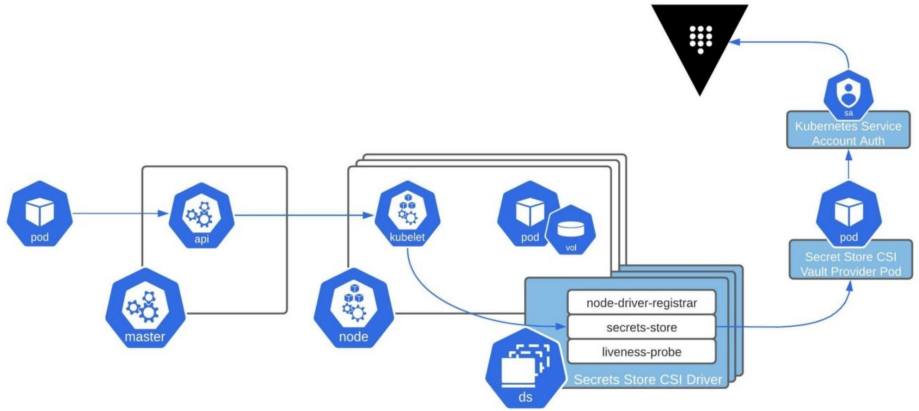
🔮 Agenda

- 🤨 What is wrong with Kubernetes Secrets?
- 🧐 Brief introduction to CSI (Container Storage Interface) & Secret Store CSI Driver
- 💡 Use-cases and Alternatives: Vault CSI Provider & Sidecar Injection
- 👩‍💻 Hands On
  - ⏱️ $ make create-cluster
  - 🔐 $ make setup-vault
  - 🪜 $ make setup-secrets-store-csi-driver
  - 💉 $ make test

🤨 What is wrong with Kubernetes Secrets?

- Kubernetes secrets are the native resources for **storing and managing sensitive data, like passwords, cloud access keys, or authentication tokens.**
- It's critical to ensure that **only authorized entities—users, services, or workloads**—are able to access it.
- Placing sensitive info into a secret object **does not automatically make it secure**. **By default**, data in Kubernetes secrets is **stored in Base64 encoding, which is practically the same as plaintext.**
- As the ultimate location where secrets are stored, etcd must be encrypted and well protected. You should enable data encryption and limit access to the etcd clusters.

🧐 Brief introduction to CSI & Secret Store CSI Driver



- [The Container Storage Interface](), or CSI, **is a standard specification for exposing storage systems to containerized workloads**.
- Using CSI third-party storage providers **can write and deploy plugins exposing new storage systems in Kubernetes without ever having to touch the core Kubernetes code.**
- This specification **enables storage providers to write standard plugins to integrate their storage systems into container orchestration systems**, like Kubernetes.
  - Automatically create storage when required.
  - Make storage available to containers wherever they're scheduled.
  - Automatically delete the storage when no longer needed.
- The Kubernetes project maintains a [list of supported CSI drivers.]()
- The Secrets Store CSI driver is one of them. secrets-store.csi.k8s.io allows Kubernetes to **mount multiple secrets, keys, and certs stored in enterprise-grade external secrets stores into their pods as a volume**. Once the Volume is attached, the data in it is mounted into the container's file system.

💡 Use-cases and Alternatives: Vault CSI Provider & Sidecar Injection

- Using Kubernetes CSI and the Vault CSI provider is **an alternative to sidecar injector method** (Vault Agent Injector)
- The sidecar method **requires init and/or sidecar containers** to retrieve secrets.
  - This is done either **by adding pod annotations or using configuration maps defining the Vault role and the path to the secret.**
  - This **increases the total number of containers** running in your cluster
  - An important difference is that the sidecar injector method **cannot facilitate syncing of secrets to environment variables.**
- The CSI method simplifies this architecture since it **does not require any sidecar containers.**
  - Vault provider is **deployed as a DaemonSet and renders secrets before the pod starts.**
  - It also **provides a method to sync secrets into environment variables and Kubernetes secrets.**
  - **If your security requirements require you to disable hostPath volumes, you should be aware that this method uses hostPath volumes to communicate with the CSI driver.**

Hands On

https://git.io/JwFMq