Accessing static secrets in Multi Service Environments

No draft as of today

Andrew McCormick
Arndt Schwenkschuster

WIMSE and Static Secret Credentials

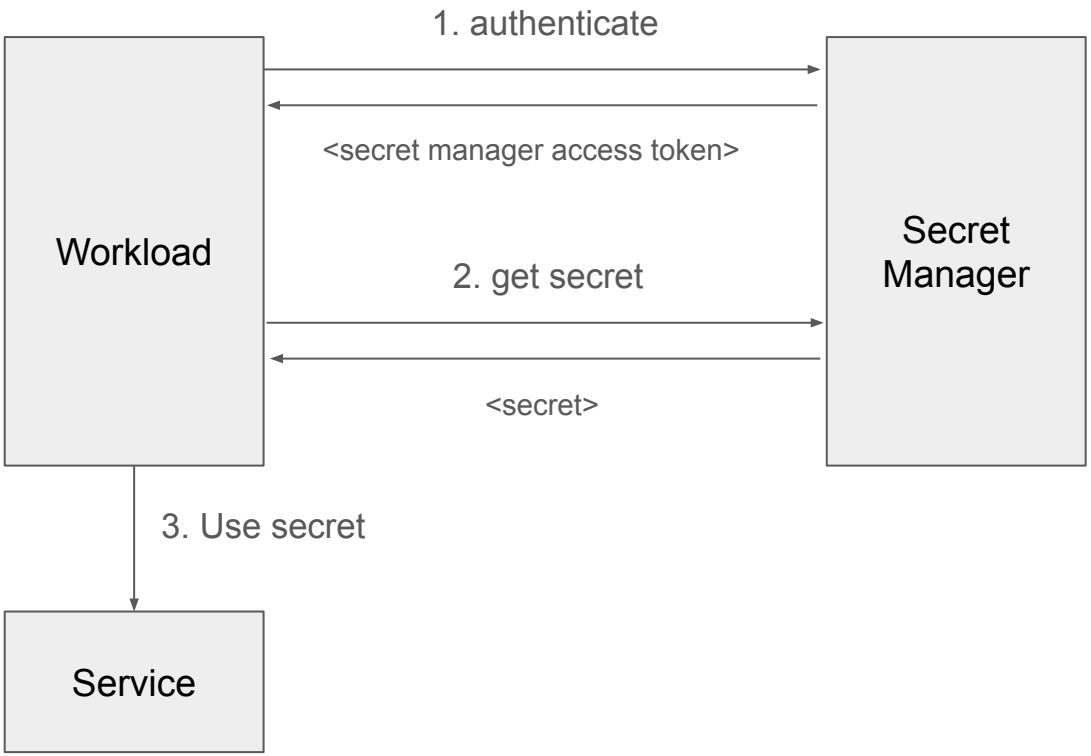
- Most services still use static secrets like API keys and passwords instead of standards-based authentication for workloads
- Lifecycle management for these secrets varies significantly across services
- These secrets are generally stored in Secrets Managers
  - Still requires some form of authentication, causing “Secret Zero” problem for many environments
  - Some support standards-based authentication for workloads, most don’t
  - Operational burden of managing these static secrets and least-privilege access to them at scale is huge
  - Shortcuts cause breaches (credentials in code, weak authentication to secrets manager, etc)

Market overview

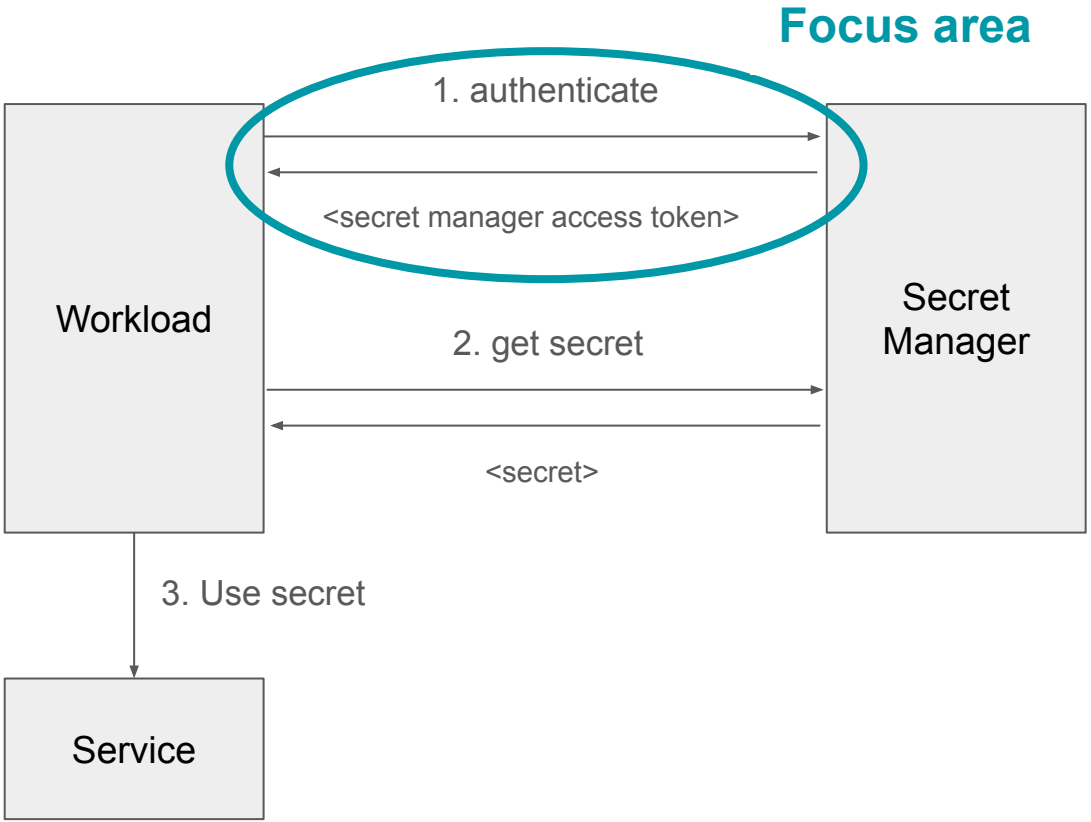
- Out of **36** Secret Managers, only **9** support authentication without a client secret
- Out of the 9 that do support it, **5** are cloud providers
- The majority of the 27 that do not support it **use Bearer credentials**
- The 9 that do support it use **different APIs for authentication**

Source: https://external-secrets.io/latest/

Secret Manager Authentication Flow



Secret Manager Authentication Flow



Questions to the working group

Do you have experience with this problem? Is there precedence/ prior-art?

Should the WG work in this area?