

SECRET MANAGEMENT

GIT-CRYPT

- ▶ Encrypts whole files
- ▶ Based on PGP
- ▶ Git-Diff won't work at all

MOZILLA SOPS

- ▶ Encrypts only YAML Value
- ▶ Can use a multitude of credential providers and encryption methods (PGP, AGE, Vault, ...)
- ▶ Git-diff works (to some extent)

...dev/k8s/k8s-manifests

+

zsh kind-capi

cedi@mae

~/src/cedi/cedi.dev/k8s/k8s-manifests

main

-7

1

bat

kustomize/overlays/argocd/oauth-credentials.secret.yaml

File: kustomize/overlays/argocd/oauth-credentials.secret.yaml

1 apiVersion: v1

2 kind: Secret

3 type: Opaque

4 metadata:

5 name: argocd-secret

6 namespace: argocd

7 annotations:

8 kustomize.config.k8s.io/behavior: replace

9 stringData:

10 dex.oauth.github.clientID: ENC[AES256_GCM,data:wfBycZqV9Zu0lTLTH2E+qMEGOKI=,iv:cxpSJaIjffDS/MAC6fapLhH9BytuFXQIOfn0LB4rUiI=,tag:AwWq8V3dqghPiWYACM0j8A==,type:str]

11 dex.oauth.github.clientSecret: ENC[AES256_GCM,data:rjuLmezWZqhobtUKatu5FrFwmXqiw/x+HgE4zCDbgrO5NDcpa1R9wg==,iv:6qAdmmRo49tDnBH5JXStjBf6qeCkf2SXDwk55i/NaFM=,tag:JuMq2wXKhy4Gu09IeqE7SQ==,type:str]

12 sops:

13 kms: []

14 gcp_kms: []

15 azure_kv: []

16 hc_vault: []

17 age:

18 - recipient: age1r9chn8pl3d4msxktw457x3xz2l8p04pwuyd7pkgldkmmakras5ks7tfsyq

19 enc: |

20 -----BEGIN AGE ENCRYPTED FILE-----

21 YWdlLlVWYy3J5cHRpb24ub3JnL3YxCi0+IFgyNTUxOSBvZVVRMUZSaE5BbzI1dmJh

22 MEdkakZPUXZlLy9KUHJIckF0N2RZK1RDWUU0ClZPaWkzY3h0Zke3NXJLOUM3b1Nr

23 U05sZHV0L0w2SHgyeUNRdmRqcXA1dTQKLS0tIDZ2ZUxndnV2cXV3WLQweCtJYXJS

24 TXF0T1RH0XVpN1J4ZFBRT3VCUXFWcGMKoMy8xDck8Et14N3RGgh/6kerrz800+J9

25 oXKJEU0HUQ43p+xTAUvaklyZqp4WCktPnASxi5JEU+4tAm88i7yIrg==

26 -----END AGE ENCRYPTED FILE-----

27 - recipient: age10hzpv26wext204acftvf2n8r6hmnwxdpknzaysllpwynccjvjsjvhq4z

28 enc: |

29 -----BEGIN AGE ENCRYPTED FILE-----

30 YWdlLlVWYy3J5cHRpb24ub3JnL3YxCi0+IFgyNTUxOSBSZVB2RDBVUURGcjBMZmtY

31 T3p4b2lwMTV4Sk14UVR5RGdDZU5udStDY1V3CmV5cGJWSHIVbzJHaVo1Yk5LeE5w

32 MkdnQWNhNzBFYjBSWTd1aEVEVjJ5MFEKLS0tIHBTSTJtYzFXTTMxN24zRks1bUJp

33 OVkwTlxxQzZlbSsyTEZsVkweFM4bncKaJyu2l0Ie4+JC4EC4YPYlyvZPZ+Xp7SB

34 fN58qf4LrF3nKs1W1A5xAypACT0JZp/3fBuXfD+18QQy7aEE8D+CAA==

35 -----END AGE ENCRYPTED FILE-----

36 lastmodified: "2023-05-01T19:04:27Z"

37 mac: ENC[AES256_GCM,data:CXKh18u4vNCAQ20uA6PaHDSaJn3tHZVkJQ962KqLYDs37VSCxbwZxZ+RxYB7UlsLYVL+EI2kfwzEkWGXLmDLWCsssw4CxCB/rrQNj1tvb/xWa2l1g4sYx/uTUo/hfu4E2qdfz50etpf99DGnxMYj5hNwPFDbzkgCe2aNqFusfhsg=,iv:3Lew0xiu2hiyxkW/lqw47nzDJGvQFNtplfCqc3yUd9k=,tag:40GNMM+UsDBkQercWxA9Hw==,type:str]

38 pgp: []

39 encrypted_regex: ^(data|stringData|spec|bot_token|chat_id)\$

40 version: 3.7.2

cedi@mae

~/src/cedi/cedi.dev/k8s/k8s-manifests

main

-7

1

zsh kind-capi