SECRETS MANAGER > VOS SECRETS

Décryptage Secret

Décryptage Secret

Secrets Manager peut utiliser des jetons d'accès, en plus des mots de passe principaux, pour déchiffrer, éditer et créer des secrets. Spécifiquement, cela est fait dans des scénarios d'injection de secrets comme les exemples ici.

Conceptuellement, les jetons d'accès se composent de deux éléments constitutifs :

- **Une clé API** , contenant un identifiant client et un secret pour l'authentification auprès des serveurs Bitwarden.
- Une **clé de chiffrement unique**, qui sera utilisée pour déchiffrer une charge utile cryptée contenant la clé de chiffrement symétrique de votre organisation.

Lorsqu'un jeton d'accès est utilisé, par exemple lors de l'authentification d'une commande CLI comme `bws get secret` :

1. Une demande est envoyée aux serveurs Bitwarden contenant l'identifiant du client et le secret du client de la clé API.
2. Les serveurs Bitwarden utilisent ces identifiants pour l'authentification de la session client, et envoyer une réponse contenant une charge utile cryptée. Cette charge utile cryptée contient la clé symétrique de l'organisation.
3. Une fois reçue, la clé symétrique de l'organisation est déchiffrée localement à l'aide de la clé de chiffrement unique du jeton d'accès.
4. Une demande ultérieure est envoyée aux API de Bitwarden pour la donnée appelée dans la commande `bws`, par exemple un secret.
5. Bitwarden détermine si la donnée demandée peut être fournie en fonction d'un identifiant de compte de service dans la demande. Si oui, une réponse est envoyée au client avec la donnée cryptée.
6. La donnée est déchiffrée localement à l'aide de la clé symétrique de l'organisation. Les valeurs pertinentes sont utilisées quelle que soit la manière dont vous utilisez Secrets Manager, par exemple en enregistrant une valeur déchiffrée `"clé": ""` dans une variable d'environnement.