輕鬆搞定 DevOps 帳密憑證控管！

ONE IDENTITY by Quest × WT 威雲科技 WeiCloudTech

什麼是 Vault？

在企業級應用開發過程中，團隊每時每刻都需要管理各種各樣的機密資訊，從個人的登入密碼到生產環境的 SSH Key，以及資料庫登錄帳密、API 認證帳密等。常見的做法是將這些機密資訊保存在某個文件中，並放置到 git 之類的程式碼控管工具中。個人和應用程式可以透過 Pull Request(PR) 來存取這些訊息，但這種方式弊端很多，比如跨團隊分享存在安全隱患、文件格式難以維護、機密資訊難以回收等。

尤其是微服務大行其道的今天，如何讓開發者添加機密資訊、應用程式能輕鬆的獲取機密資訊、採用不同策略更新機密資訊、適時回收機密資訊等變得越來越關鍵，所以企業需要一套統一的接口來處理機密資訊的各種層面，而 Vault 就是這樣的一款工具。Vault 作為集中化的機密資訊管理工具，具有以下特點：

● 儲存機密資訊：所有存放的資訊都是加密的。任何動態生成的機密資訊都有租期，並且到期會自動回收。

● 自動更新金鑰：用戶可以隨時更新存放的機密資訊。Vault 提供了加密即服務 (encryption-as-a-service) 的功能，可以隨時將密鑰滾動到新的密鑰版本，同時保留對使用過去密鑰版本加密的值進行解密的能力。

● 稽核日誌：保管庫儲存所有經過身分驗證的客戶端交互的詳細審核日誌 (如：身分驗證、Token 建立、機密資訊存取 / 撤銷等)。

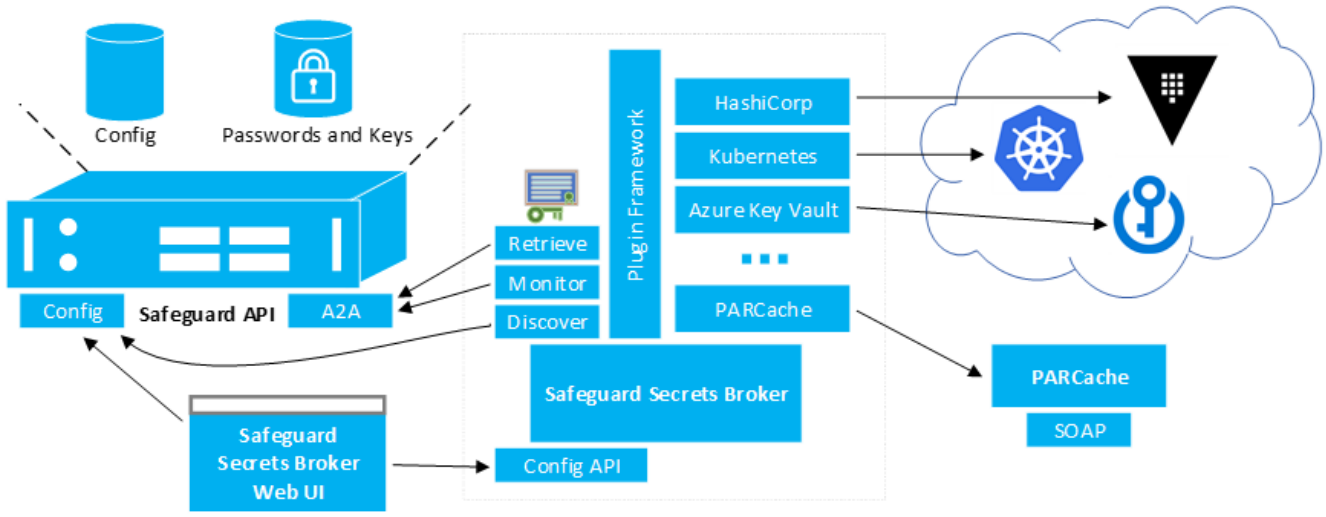
One Identity Safeguard 整合 Vault

One Identity 為了使 DevOps 上的安全性管理更便捷，發展了 "DevOps 上機密訊息推播技術 "，此技術有以下益處：

● 微服務開發人員不需修改目前的開發模組，採用原生與 Vault 整合的方式

● 中央化機密資訊控管 ，一致的機密管控政策

● 減少 PAM 受惡意攻擊



系統架構

在此解決方案中，其元件組成說明如下：

● **Safeguard API**：使用 A2A (Application to Application) REST API 以及 Core REST API ，以設定 A2A 及其他 Safeguard 服務

● **Safeguard Secrets Broker for DevOps**：此服務包含了與 DevOps 後端整合的套件，主要用來進行私密資訊同步使用

● **Safeguard Secrets Broker for DevOps Config Utility**：使用網頁化的設定工具來設定 Safeguard Secrets Broker for DevOps 與 Safeguard 之間的溝通

運作流程 (請參考影片 https://youtu.be/QFNlllpQxQ8)

1. 當私密資訊到達變更的時間點時， Safeguard 進行私密資訊變更
2. Safeguard Secrets Broker for DevOps 偵測到私密資訊變更，啟動已設定告知的套件
3. 套件與後端 DevOps 技術溝通，傳遞私密資訊至後端
4. DevOps 上的應用程式使用原 DevOps 技術，由 Vault 取得私密資訊