Secrets management
centraal beheer van gevoelige data

Rayen Nasra, Jan Delamper, Antonia Pierreux

Hogeschool Gent, Arbeidstraat 14, 9300 Aalst
rayen.nasra@student.hogent.be

Abstract

Secrets management is een belangrijk begrip dat vaak over het hoofd wordt gezien door bedrijven. Het is een sterk fundament om gevoelige gegevens te beheren in een bloeiend IT-ecosysteem. In dit onderzoek werd er benaderd wat secrets management concreet is en hoe dit gebruikt kan worden in een Continuous Integration / Continuous Deployment omgeving. Meer specifiek werd er gekeken hoe de workflow, met het gebruik van gevoelige gegevens, optimaal behouden kan worden.

Introductie

Bij het Wolters Kluwer Finance Risk & Reporting departement, bevinden zich alle back-end operaties waar via TeamCity, een Continuous Integration / Continuous Deployment tool, continu applicaties worden opgebouwd. Deze tool maakt gebruik van chronologische sets van taken waar soms gevoelige parameters worden opgegeven. Men geraakt makkelijk aan duizenden verschillende configuraties waar men geen overzicht meer heeft in welke locaties deze gevoelige gegevens aanwezig zijn.

Secrets management tracht dit probleem op te lossen door deze gevoelige gegevens, die men *secrets* noemt, centraal te beheren. In dit onderzoek werd een secrets management tool, on-premise opgezet en een cloud oplossing gebruikt die als Proof-of-Concept diende voor deze case.

Dit onderzoek werd volbracht in opdracht van Wolters Kluwer Financial Services. De Proof-Of-Concept werd verwezenlijkt met bijstand van Jan Delamper, Principal Product Software Engineer bij het Wolters Kluwer Finance Risk & Regulatory Reporting development team.

Onderzoek

Om concreet het nut van secrets management te verstaan, werd allereerst een uitgebreide literatuurstudie gevoerd. Hiermee is men op de hoogte hoe secrets management is ontstaan en welke problemen dit concept tracht op te lossen. Verder werd er ook uitgelegd wat cloud computing is met de belangrijkste onderdelen hiervan.

In een volgend hoofdstuk, de methodologie, werd aan de hand van de MoSCoW-methode een geschikte kandidaat gekozen voor de on-premise opstelling. Hiermee werd er ondervonden dat Hashicorp Vault een zeer geschikte tool is voor deze uitwerking. Voor de cloud oplossing werd Microsoft Azure Key Vault gebruikt omdat hier de voorkeur lag bij het bedrijf.

In het Proof-of-Concept gedeelte, werden beide opstellingen opgezet. Via de TeamCity production en development server, werden deze twee instanties getest met test configuraties die bij beide applicaties secrets zou ophalen om de build succesvol te laten verlopen. Ansible werd gebruikt om sommige processen te automatiseren omdat het gebruik hiervan aan het groeien is binnenin het bedrijf. Dit zou er dan voor zorgen dat later werk bespaard wordt indien er gekozen zou worden om bepaalde zaken te laten automatiseren.

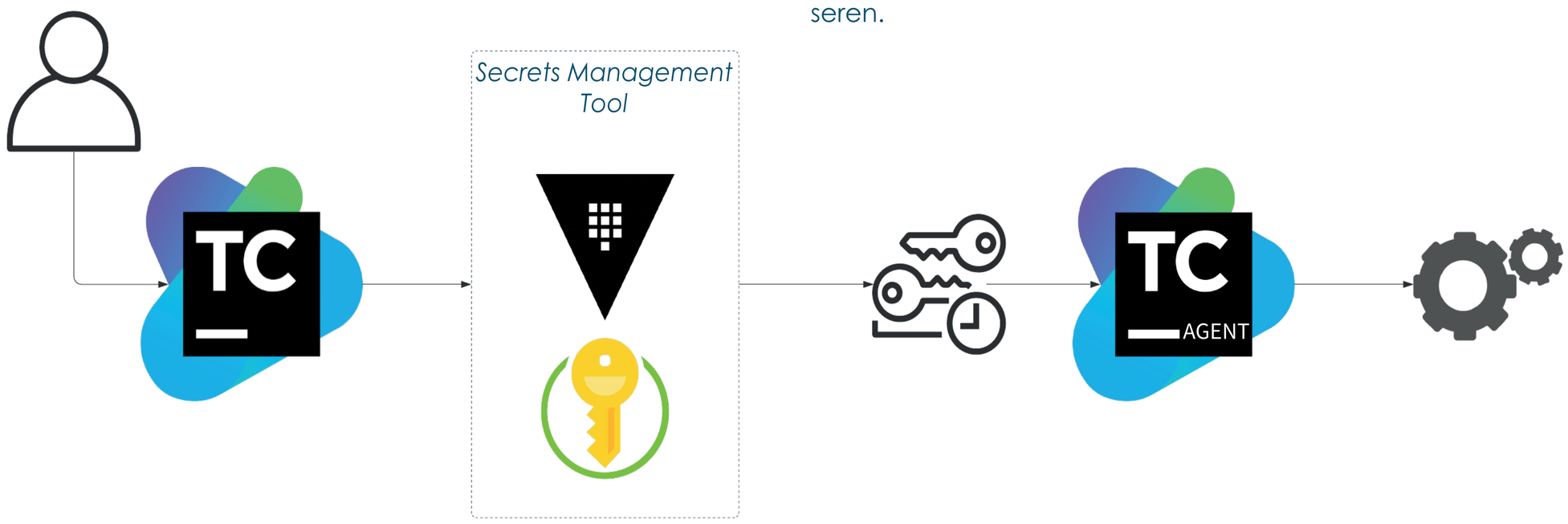

Figure 1: Werking van TeamCity wanneer secrets worden opgevraagd bij builds

Conclusies

Na de literatuurstudie werd er ondervonden dat er tegenwoordig voldoende applicaties bestaan die het concept van secrets management zo goed mogelijk benaderen. Ook stonden cloud providers gedurende de laatste jaren niet stil om hiervoor een service aan te bieden.

De integraties met Hashicorp Vault en Azure Key Vault zijn gelukt met de nodige voorwaarden. De werking werd enkel bewezen met Azure Key Vault. Hashicorp Vault kon geen secrets opvragen gedurende builds binnen de twee verschillende TeamCity omgevingen. Dit zou na enige troubleshooting opgelost kunnen worden. Bij Azure Key Vault werden er wel succesvol secrets opgehaald vanuit de aangemaakte key vault. Dit bewijst dat secrets centraal beheerd kunnen worden via een secrets management tool.

Toekomstig onderzoek

Secrets management systemen bevatten veel domeinen die in de Proof-of--Concept niet aan bod zijn gekomen. Door de functionaliteiten die ter beschikking gesteld zijn, kan het zeer interessant zijn om deze verder te configureren en integraties te voeren met andere applicaties. Verder kan het ook interessant zijn om deze functionaliteiten in de toekomst verder te onderzoeken.