Hochschule Worms
Fachbereich Informatik
Studiengang Angewandte Informatik - dual (M.Sc)

Projektbericht
Deep Dive

Entwicklung einer Lösung zur Berechtigungsverwaltung von Secrets zwischen Entwicklerinnen und Entwicklern

In der Arbeitsumgebung des Partnerunternehmens Medienagenten oHG

Version 1.0

Vorgelegt von

Leon Etienne, 676838
inf4437@hs-worms.de
Im Wintersemester 2024/25

bei Professor Dr. Heinemann
heinemann@hs-worms.de

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Schriften entnommen wurden, sind als solche kenntlich gemacht. Die Arbeit ist noch nicht in gleicher oder ähnlicher Form oder auszugsweise im Rahmen einer anderen Prüfung vorgelegt worden.

Ludwigshafen am Rhein, 21. Februar 2025

Leon Etienne _____

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

1P 1Password

Glossar

Docker

Eine arrivierte Container-Engine für Anwendungsentwicklung.

Ansible-Playbook/s

Ansible-Playbooks sind Skripte, mit dem Ziel einen deklarierten Zustand herzustellen.

1 Einleitung

1.1 Problemstellung

In der Arbeitsumgebung des Partnerunternehmens besteht zum Zeitpunkt der Themenfindung der hier beleuchteten Arbeit kein Management für Secrets und Logindaten zwischen Entwicklern. Logindaten zu den Projekten des Unternehmens liegen schlicht in einem 1Password (1P)-Vault. 1P ist der vom Unternehmen verwendete Passwortmanager. Auf diesen Vault haben sämtliche interne Entwickler Zugriff, jedoch keine externen Entwickler. Das ist so, weil anderenfalls dem externen Entwickler Lesezugriff auf sämtliche Einträge dieses Vaults gegeben werden müssten. 1P unterstützt keine Freigaben einzelner Einträge an andere Nutzer, ohne diese Einträge in einen eigenen Vault zu kopieren. Würden diese manuell in einen eigenen Vault kopiert werden, müssten diese Einträge fortan redundant gepflegt werden. Das ist eine Fehlerquelle, die zu asynchronen Einträgen führt. Außerdem ist das ein großer Arbeitsaufwand. All das gestaltet das Einbinden von externen Entwicklern, wie z.B. Freelancern, schwer.

Ein weiteres Problem ist, dass Secrets in Konfigurationsdateien, die firmeninternen Ansible-Scripten beilegen, unverschlüsselt einsichtig sind. Das macht es zu einem großen Sicherheitsrisiko und somit impraktikabel externen Entwicklern Zugriff auf dieses Ansible-Repository zu gewähren. Dieses Ansible-Repository ist jedoch zwingend erforderlich, um eine Entwicklungsungebung für Firmenprojekte auf dem lokalen Rechner zu schaffen. Auch hier sind Lösungen für externe Entwickler zumeist unschöne Workarounds.

1.2 Zielsetzung

Ziel ist es, eine Umgebung zu schaffen, in der beliebigen Entwicklern bestimmte 1P-Einträge zugewiesen werden können. Der Pflegeaufwand sollte hierbei überschaubar bleiben. Das heisst, dass z.B. ganze Gruppen von Einträgen Entwicklern zugewiesen werden können. Wenn z.B. einem Projekt viele Einträge zugeordnet sind, sollten diese idealerweise mit einer einzigen Configzeile einem Entwickler zugeordnet werden können. Außerdem sollte eine Möglichkeit ausgearbeitet werden, um 1P-Einträge in Ansible auszulesen, damit keine Secrets mehr in den beiliegenden Konfigurationsdateien stehen, die das Freigeben dieser zu einem Sicherheitsproblem machen.

1.3 Methodische Vorgehensweise

Einige Anforderungen sind bereits im Voraus definiert. Weiterführende Anforderungen werden im Rahmen einer Anforderungserfassung ermittelt. Anschließend werden verschiedene Lösungsansätze betrachtet und auf Tauglichkeit geprüft. Nachdem ein akzeptabler Lösungsweg gefunden ist, wird dieser umgesetzt. Abschließend wird der Erfolg des Unterfanges evaluiert und mögliche, auf dieses Projekt aufbauende Arbeiten in Ausblick gestellt.

2 Grundlagen

2.1 Die Arbeitsumgebung

Die Arbeitsumgebung des Partnerunternehmens besteht für diese Themenstellug nennenswert aus:

- Cloudbasierten Web- und Datenbankservern
- Git-Repositories bei Bitbucket
- Der lokalen, Docker-basierten Arbeitsumgebung
- Ein Ansible-Playbook, das ein Projekt mit Daten aus der Cloudumgebung und Code aus Bitbucket in der lokalen Entwicklungsumgebung bereitstellt.

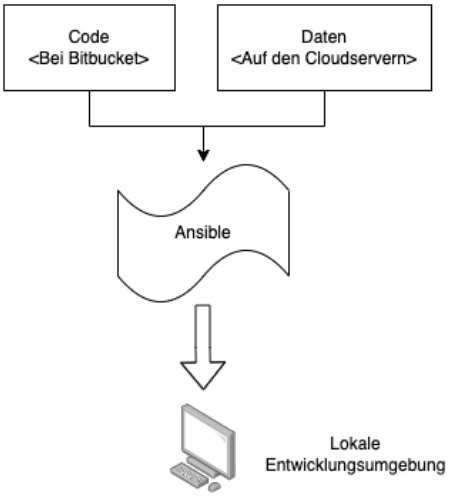

Abbildung 1: Relationsdiagramm: Aufsen von Projekten des Partnerunternehmens in einer Entwicklungsumgebung

Quelle: Eigene Darstellung

2.2 1Password

2.3 Ansible

3 Anforderungen

3.1 Methodik und Planung

3.2 Ergebnisse

4 Technische Umsetzung

4.1 Berechtigungsverwaltung

4.2 Integration in Ansible

5 Evaluation

6 Fazit

6.1 Ausblick

6.2 Offene Problemstellungen

Literaturverzeichnis

[Google Inc., 2023] Google Inc. (2023). Legal frameworks for data transfers . `https://policies.google.com/privacy/frameworks`. Zugriff: Mai 2024.

[Maral et al., 1991] Maral, G., de Ridder, J.-J., Evans, B. G., und Richharia, M. (1991). Low earth orbit satellite systems for communications. *International Journal of Satellite Communications*, 9(4):209–225.

[TYPO3 Association, 2024] TYPO3 Association (2024). TYPO3 — the Professional, Flexible Content Management System . `https://typo3.org/`. Zugriff: Mai 2024.

Anhang