

SECRETS MANAGER > INTEGRATIONEN

GitLab CI/CD

Ansicht im Hilfezentrum:
<https://bitwarden.com/help/gitlab-integration/>

GitLab CI/CD

Bitwarden bietet eine Möglichkeit, Geheimnisse in Ihre [GitLab CI/CD](#) Pipelines einzufügen, indem Sie die Bitwarden [Secrets Manager CLI](#) verwenden. Dies ermöglicht Ihnen das sichere Speichern und Verwenden von Geheimnissen in Ihren CI/CD-Workflows. Um zu beginnen:

Speichern Sie ein Zugriffs-Token

In diesem Schritt werden wir ein [Zugriffs-Token](#) als GitLab CI/CD-Variable speichern. Dieses Token wird verwendet, um sich bei der Bitwarden Secrets Manager API zu authentifizieren und [Geheimnisse](#) abzurufen.

1. In GitLab navigieren Sie zu der Seite Ihres Projekts **Einstellungen** > **CI/CD**.
2. Wählen Sie **Erweitern** im **Variablen** Bereich.
3. Wählen Sie **Variable hinzufügen**.
4. Überprüfen Sie die **Maskenvariable** Flagge.
5. Benennen Sie den Schlüssel **BWS_ACCESS_TOKEN**. Dies ist die Variable, nach der der Secrets Manager CLI sucht, um sich zu [authentifizieren](#). Alternativ, wenn Sie den Schlüssel anders benennen müssen, geben Sie **--access-token NAME_OF_VAR** in der späteren **bws secret get** Zeile an.
6. Öffnen Sie in einem anderen Tab die Secrets Manager Web-App und [erstellen Sie ein Zugriffstoken](#).
7. Zurück in GitLab, fügen Sie das neu erstellte Zugriffs-Token in das **Wert**-Feld ein.
8. Wählen Sie **Variable hinzufügen** um zu speichern.

The screenshot shows the Bitwarden CI/CD Settings page for a project named 'bws_secrets'. The left sidebar contains navigation options like Project, Manage, Plan, Code, Build, Secure, Deploy, Operate, Monitor, Analyze, and Settings. The main content area is divided into sections: Artifacts, Variables, and Pipeline trigger tokens. The 'Variables' section is active, showing a table for 'CI/CD Variables' with columns for Key, Value, and Environments. A modal titled 'Add variable' is open on the right, allowing the user to define a new variable. The modal includes fields for Type, Environments, and Flags, and a 'Key' field containing 'BWS_ACCESS_TOKEN'. The 'Value' field is currently empty and highlighted with a blue border. Buttons for 'Cancel' and 'Add variable' are at the bottom of the modal.

Fügen Sie eine Variable in GitLab hinzu

Fügen Sie Ihrer Workflow-Datei hinzu

Als nächstes werden wir einen rudimentären GitLab CI/CD Workflow schreiben. Erstellen Sie eine Datei namens `.gitlab-ci.yml` im Stammverzeichnis Ihres Repositorys mit folgendem Inhalt:

Bash

```
stages:
- default_runner

image: ubuntu

build:
  stage: default_runner
  script:
  - |
    # install bws
    apt-get update && apt-get install -y curl git jq unzip
    export BWS_VER="1.0.0"
    curl -LO \
      "https://github.com/bitwarden/sdk/releases/download/bws-v$BWS_VER/bws-x86_64-unknown-linux-gn
u-$BWS_VER.zip"
    unzip -o bws-x86_64-unknown-linux-gnu-$BWS_VER.zip -d /usr/local/bin

    # use the `bws run` command to inject secrets into your commands
  - bws run -- 'npm run start'
```

Wo:

- **BWS_VER** ist die Version des Bitwarden Secrets Manager CLI, die installiert werden soll. Hier erhalten wir automatisch die neueste Version. Sie können die zu installierende Version festlegen, indem Sie dies auf eine bestimmte Version ändern, zum Beispiel **BWS_VER="0.3.1"**.
- **534cc788-a143-4743-94f5-afdb00a40a41** und **9a0b500c-cb3a-42b2-aaa2-afdb00a41daa** sind Referenzidentifikatoren für Geheimnisse, die im Secrets Manager gespeichert sind. Das Dienstkonto, zu dem Ihr Zugriffstoken gehört, muss in der Lage sein, auf diese spezifischen Geheimnisse zuzugreifen.
- **npm run start** ist der Befehl, der die geheimen Werte erwartet, die von **bws** abgerufen werden. Ersetzen Sie dies durch die entsprechenden Befehle zum Ausführen Ihres Projekts.

Warning

Geheimnisse werden als Umgebungsvariablen gespeichert. Es ist wichtig, Befehle zu vermeiden, die diese Geheimnisse in die Protokolle ausgeben würden.

Führen Sie die CI/CD-Pipeline aus

Auf der linken Seite wählen Sie **Erstellen > Pipelines** und wählen Sie oben rechts im Tempo **Pipeline ausführen**. Wählen Sie **Pipeline ausführen** auf der Seite, um die neu erstellte Pipeline auszuführen.