bitwarden | Hilfezentrum Artikel

SECRETS MANAGER > INTEGRATIONEN

GitHub-Aktionen

Ansicht im Hilfezentrum:
https://bitwarden.com/help/github-actions-integration/

GitHub-Aktionen

Bitwarden bietet eine Integration mit GitHub Actions, um Geheimnisse aus dem Secrets Manager abzurufen und sie in GitHub Actions-Workflows einzufügen. Die Integration wird abgerufene Geheimnisse als maskierte Umgebungsvariablen innerhalb einer Aktion einfügen. Um die Integration einzurichten:

Speichern Sie ein Zugriffs-Token

In diesem Schritt werden wir ein Zugriffs-Token als ein GitHub verschlüsseltes Geheimnis speichern. Verschlüsselte Geheimnisse können für eine Organisation, ein Repository oder eine Repository-Umgebung erstellt werden und stehen zur Verwendung in GitHub Actions-Workflows zur Verfügung:

1. In GitHub navigieren Sie zu Ihrem Repository und wählen Sie das **Einstellungen** Tab.
2. Im Sicherheitsbereich der linken Navigation wählen Sie **Geheimnisse und Variablen → Aktionen.**
3. Öffnen Sie den **Geheimnisse** Tab und wählen Sie den **Neues Repository-Geheimnis** Button.
4. Öffnen Sie in einem anderen Tab den Secrets Manager Web-Tresor und erstellen Sie ein Zugriffs-Token.
5. Zurück in GitHub, geben Sie Ihrem Geheimnis einen **Namen** wie `BW_ACCESS_TOKEN` und fügen Sie den Zugriffs-Token-Wert aus Schritt 4 in das **Geheimnis**-Eingabefeld ein.
6. Wählen Sie die Schaltfläche **Geheimnis hinzufügen**.

Fügen Sie Ihrer Workflow-Datei hinzu

Als nächstes werden wir einige Schritte zu Ihrer GitHub Actions Workflow-Datei hinzufügen.

Geheimnisse bekommen

Um Geheimnisse in Ihren Arbeitsablauf zu bekommen, fügen Sie einen Schritt mit den folgenden Informationen zu Ihrer Arbeitsablauf-YAML-Datei hinzu:

```bash
- name: Get Secrets
  uses: bitwarden/sm-action@v2
  with:
    access_token: ${{ secrets.BW_ACCESS_TOKEN }}
    base_url: https://vault.bitwarden.com
    secrets: |
      fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff > SECRET_NAME_1
      bdbb16bc-0b9b-472e-99fa-af4101309076 > SECRET_NAME_2
```

Wo:

- `${{ secrets.BW_ACCESS_TOKEN }}` bezieht sich auf Ihr zuvor gespeichertes Repository-Geheimnis. Ändern Sie entsprechend, wenn Sie das Geheimnis nicht `BW_ACCESS_TOKEN` genannt haben.

- `fc3a93f4-2a16-445b-b0c4-aeaf0102f0ff` und `bdbb16bc-0b9b-472e-99fa-af4101309076` sind Referenzkennungen für Geheimnisse, die im Secrets Manager gespeichert sind. Das Service-Konto, zu dem Ihr Zugriffs-Token gehört, **muss in der Lage sein, auf diese spezifischen Geheimnisse zuzugreifen**.

- `GEHEIM_NAME_1` und `GEHEIM_NAME_2` sind die Namen, die Sie verwenden werden, um auf die injizierten geheimen Werte im nächsten Schritt zu verweisen.

Verwende Geheimnisse

Schließlich können Sie den Pfad vervollständigen, indem Sie die angegebenen geheimen Namen (`SECRET_NAME_1` und `SECRET_NAME_2`) als Parameter in einer nachfolgenden Aktion verwenden, zum Beispiel:

```bash
- name: Use Secret
  run: SQLCMD -S MYSQLSERVER -U "$SECRET_NAME_1" -P "$SECRET_NAME_2"
```