GEHEIMEN MANAGER > INTEGRATIES

Ansible

Ansible

Bitwarden biedt een integratie met Ansible om geheimen op te halen uit Secrets Manager en ze in je Ansible playbook te injecteren. De lookup plugin injecteert opgehaalde geheimen als gemaskeerde omgevingsvariabelen in een Ansible playbook. De collectie instellen:

Vereisten

- We raden aan Python-pakketten te installeren in een virtuele Python-omgeving.
- Huidige versie van Ansible geïnstalleerd op uw systeem.
- Bitwarden Secrets Manager met een actief serviceaccount.

Voordat je de Ansible verzameling instelt, raden we je aan om ook Secrets Manager te openen om toegang te krijgen tot je toegangstoken en eventuele geheimen die je wilt opnemen in de opstelling.

Installeer de Bitwarden Ansible-verzameling

De volgende handleiding is een installatievoorbeeld voor de Bitwarden collectie op een Linux machine.

1. Installeer de Bitwarden SDK:

```Bash
pip install bitwarden-sdk
```

2. Installeer de verzameling bitwarden.secrets:

```Bash
ansible-galaxy collection install bitwarden.secrets
```

Nu de Ansible-verzameling is geïnstalleerd, kunnen we beginnen met het aanroepen van Bitwarden-geheimen vanuit een Ansible-afspeelboek met `bitwarden.secrets.lookup`. In de volgende paragraaf worden voorbeelden gegeven om dit proces te demonstreren.

> **Note**
>
> macOS gebruikers moeten mogelijk de volgende omgevingsvariabele instellen in shell om stroomopwaartse problemen met Ansible te voorkomen.
>
> - `export OBJC_DISABLE_INITIALIZE_FORK_SAFETY=YES`

Bitwarden geheimen ophalen

Om geheimen op te halen uit Secrets Manager in je playbook, zijn er twee methodes:

Sla het toegangstoken op als omgevingsvariabele.

Met de Secrets Manager kunnen we ons toegangstoken veilig instellen als omgevingsvariabele in de shell en het playbook gebruiken om het geheim op te halen. Om het toegangstoken te verifiëren:

1. Voer in de shell het volgende commando uit om de omgevingsvariabele voor het toegangstoken in te stellen:

```Bash
export BWS_ACCESS_TOKEN=<ACCESS_TOKEN_VALUE>
```

2. Nu de omgevingsvariabele is ingesteld, kunnen we de lookup plugin gebruiken om variabelen in ons playbook in te vullen. Bijvoorbeeld:

```Bash
  vars:
        database_password: "{{ lookup('bitwarden.secrets.lookup', '<SECRET_ID>') }}"
```

> **Note**
> Door `BWS_ACCESS_TOKEN` als omgevingsvariabele in te stellen, kan naar het toegangstoken verwezen worden zonder de ruwe toegangstokenwaarde in het playbook op te nemen.

Toegangstoken leveren in playbook

Naar het toegangstoken van Secrets Manager kan ook worden verwezen in het playbook zelf. Bij deze methode hoeft u de omgevingsvariabele `BWS_ACCESS_TOKEN` niet te gebruiken in uw shell, de waarde van het toegangstoken wordt echter opgeslagen in het playbook zelf.

1. Toegangstokens kunnen worden opgenomen in het playbook met het volgende voorbeeld:

```Bash
vars:
    password_with_a_different_access_token: "{{ lookup('bitwarden.secrets.lookup', '<SECRET_ID_V
ALUE>',
access_token='<ACCESS_TOKEN_VALUE>') }}"
```

Met deze methode kan in een enkel playbook naar meerdere toegangstokens worden verwezen.

Geheim ophalen van andere server

Bitwarden zelf gehoste gebruikers kunnen geheimen ophalen van hun Bitwarden server door de `base_url`, `api_url` en `identity_url` op te nemen:

```
Bash

vars:
    secret_from_other_server: "{{ lookup('bitwarden.secrets.lookup', '<SECRET_ID>', base_url='http
s://bitwarden.example.com' ) }}"
    secret_advanced: >-
      {{ lookup('bitwarden.secrets.lookup', '<SECRET_ID>',
        api_url='https://bitwarden.example.com/api',
        identity_url='https://bitwarden.example.com/identity' ) }}
```

Voorbeeld draaiboek

Het volgende is een voorbeeld van een playbookbestand met verschillende configuratieopties.

```
Bash

---
- name: Using secrets from Bitwarden

  vars:
    bws_access_token: "{{ lookup('env', 'CUSTOM_ACCESS_TOKEN_VAR') }}"
    state_file_dir: "{{ '~/.config/bitwarden-sm' | expanduser }}"
    secret_id: "9165d7a8-2c22-476e-8add-b0d50162c5cc"

    secret: "{{ lookup('bitwarden.secrets.lookup', secret_id) }}"
    secret_with_field: "{{ lookup('bitwarden.secrets.lookup', secret_id, field='note' ) }}"
    secret_with_access_token: "{{ lookup('bitwarden.secrets.lookup', secret_id, access_token=bws_ac
cess_token ) }}"
    secret_with_state_file: "{{ lookup('bitwarden.secrets.lookup', secret_id, state_file_dir=state_
file_dir ) }}"

  tasks:
    - name: Use the secret in a task
      include_tasks: tasks/add_db_user.yml # reference the secrets with "{{ secret }}", "{{ secret_
with_field }}", etc.
```

> **Note**
> In het bovenstaande voorbeeld laat de `CUSTOM_ACCESS_TOKEN_VAR` zien dat je meerdere, verschillende toegangstokens kunt opnemen. Deze hoeven niet op een harde kaart te staan en kunnen veilig bij je draaiboek worden geleverd.

Variabele	Aanvullende informatie
`bws_toegang_kenmerk`	Toegangstoken `env-variabele` opzoeken.
`staat_bestand_dir`	Een map waar je authenticatiestatus kan worden opgeslagen.
`geheim_id`	ID van het geheim dat je wilt opzoeken.
`geheim`	Zoek een geheime waarde op en sla deze op als een variabele met de naam `"secret".`
`geheim_met_veld`	Een geheim opzoeken met extra velduitvoer. In dit voorbeeld zal de lookup de `'noot'` waarde van de secret teruggeven.
`geheim_met_toegang_token`	Zoek een geheim op met de toegangstokenwaarde in het verzoek.
`geheim_met_staat_bestand`	Zoek een geheim op met het vooraf geconfigureerde statusbestand in het verzoek.

Extra verzoeken en velden

Naast de `secret_id` kunnen verschillende velden worden opgenomen in de `bitwarden.secrets.lookup`. A Het volgende JSON object bevat alle velden waarnaar verwezen kan worden in de playbook lookup:

```Bash
{
  "id": "be8e0ad8-d545-4017-a55a-b02f014d4158",
  "organizationId": "10e8cbfa-7bd2-4361-bd6f-b02e013f9c41",
  "projectId": "e325ea69-a3ab-4dff-836f-b02e013fe530",
  "key": "SES_KEY",
  "value": "0.982492bc-7f37-4475-9e60",
  "note": "",
  "creationDate": "2023-06-28T20:13:20.643567Z",
  "revisionDate": "2023-06-28T20:13:20.643567Z"
}
```

Om extra velden zoals `"notitie"` op te halen, kan het volgende commando aan het playbook worden toegevoegd:

```Bash
  vars:
        database_password: "{{ lookup('bitwarden.secrets.lookup', '0037ed90-efbb-4d59-a798-b1030124
87a0', field='note') }}"
```