

Discover unmanaged secrets in Secrets Hub

This topic describes how to discover AWS unmanaged secrets by running a script.

Overview

Discover secrets that are not managed in your AWS account by running a python script.

This enables you to identify secrets that should be managed, according to your organization's security policy, and then onboard them to Secrets Hub.

What does the script do?

The script scans each of the regions on your AWS account and lists the managed and unmanaged secrets in it.

Region that were unsuccessfully scanned, are listed as part of script summary.

Once the script is run, you get the following information:

- Total number of secrets
- Total number of unmanaged secrets by CyberArk or AWS*
- Total number of secrets managed by CyberArk
- Total number of secrets managed by AWS*
- Percentage of managed secrets and percentage of managed secrets by CyberArk

* Managed by AWS means that the secret has a rotation policy assigned to it

Generated report

The script generates a report named `SecretsHub_discovery_report.csv`, which includes information on managed and unmanaged secrets by both CyberArk and AWS.

**Note:**

- Empty reports are not generated
- The script overrides existing reports with the new ones, if generated.

Prerequisites

- python version 3.7 or higher: <https://www.python.org/>
- pip: <https://packaging.python.org/en/latest/tutorials/installing-packages/>
- AWS SSO method: <https://docs.aws.amazon.com/cli/latest/userguide/cli-configure-ssso.html>
- The user with which you are connecting to the AWS account must have **secretsmanager:ListSecrets** on the regions you want to scan.

Run the script

If you are running the script for the first time, do the first 2 steps. For all subsequent runs, begin on step 3.

Step 1: Install boto3



```
pip install boto3
```

**Note:**

If you are using newer python versions, for example 3.11, use `pip3 install boto3`.

Step 2: Mark the file as executable



```
chmod +x aws_discovery_script.py
```

Step 3: Open an AWS session

Make sure that you have the relevant permissions mentioned in [Prerequisites](#).

If SSO is supported, you can log on using the following command:



```
aws sso login
```

Step 4: (Optional) check the AWS account and user details

Validate your connection.



```
aws sts get-caller-identity
```

Step 5: Run the script

Run script and save report to current folder:



```
./aws_discovery_script.py
```

Run script and save report to a specific folder (using the relative path)



```
./aws_discovery_script.py --output=./output
```

For more options, see [Script parameters](#)

Script parameters

Show help:



```
./aws_discovery_script.py -h
```

Usage: aws_discovery_script.py [-h] [-o OUTPUT] [--show-errors [SHOW_ERRORS]]

optional arguments:

-h, --help show this help message and exit

--folder_path FOLDER_PATH

The folder path for csv file

--show-errors [SHOW_ERRORS]

Show error messages
