

# • Dealing with more than 100 secrets on GitHub Actions using Mozilla SOPS and Azure Key Vault

• Thada Wangthammang

07 May 2022 at 11:30-12:00



Thailand Community Leaders

# Dealing with more than 100 secrets on GitHub Actions using Mozilla SOPS and Azure Key Vault

Join us for the Global Azure 2022 – Thailand

7 May 2022, 9 AM – 3 PM



May 5<sup>th</sup> - 7<sup>th</sup>, 2022

#GlobalAzure



# Speaker



Thada Wangthammang, (Mild)  
DevSecOps Engineer

- **Work at:**
  - T.T. Software Solution: [tt-ss.net](http://tt-ss.net)
  - WRM Software: [wrmsoftware.com](http://wrmsoftware.com)
- **Write Blog at:**
  - [thadaw.com](http://thadaw.com) since 2015
  - [medium.com/@thadaw](https://medium.com/@thadaw)
- **Admin group:**
  - [fb.com/groups/dotnetthailand](https://fb.com/groups/dotnetthailand) (8K Members)
  - [www.dotnetthailand.com](http://www.dotnetthailand.com)

# My Contribution

## Publication

*"A Software Cache Mechanism for Reducing the OpenTSDB Query Time,"*

## Source:

[github.com/mildronize/tscache](https://github.com/mildronize/tscache)

## Open Source Projects (Github)

- [dotnetthailand/dotnetthailand.github.io](https://dotnetthailand/dotnetthailand.github.io)
- [mildronize/mildronize.github.io](https://mildronize/mildronize.github.io)
- [mildronize/dotfiles](https://mildronize/dotfiles)
- [dotnetthailand/kata-workshop](https://dotnetthailand/kata-workshop)
- [dotnetthailand/azure-to-github](https://dotnetthailand/azure-to-github)



เกี่ยวกับ .NET Thailand

Contributors

เว็บไซต์พันธมิตร

รวมฟรีหนังสือ, วิดีโอ และแหล่งความรู้การ...

Suggested social network accounts for ...

Privacy Policy

? .NET FAQ

🔥 Web Frameworks

💾 storage

✓ Testing

Front and Web

Home .NET Thailand group Credit to our contributors

## Contributors

Edit on Github

### Give credit where credit's due

Thank you so much to these contributors. Without you, .NET Thailand would not have happened.



aaronamm



filipowm



mildronize



renovate-bot



praveenweb



dmakeroam



# Mild Thada

No subscribers

[Home](#)[Videos](#)[Playlists](#)[Channels](#)[About](#)

## Description

โปรแกรมเมอร์ที่จำโค้ดได้ แต่จำสูตรกับข้าวไม่ได้  
เอนจอย Productivity และอยากมี Healthy Life Style

# Agenda

- Introduction
- Why Mozilla SOPS?
- Using SOPS with Age Encryption
- Using SOPS with Azure Key Vault
- Demo

A complex, abstract network diagram is visible in the background, composed of numerous small white dots connected by thin lines, forming a dense web-like structure.

#SopsWithKeyVault

# 1. Introduction



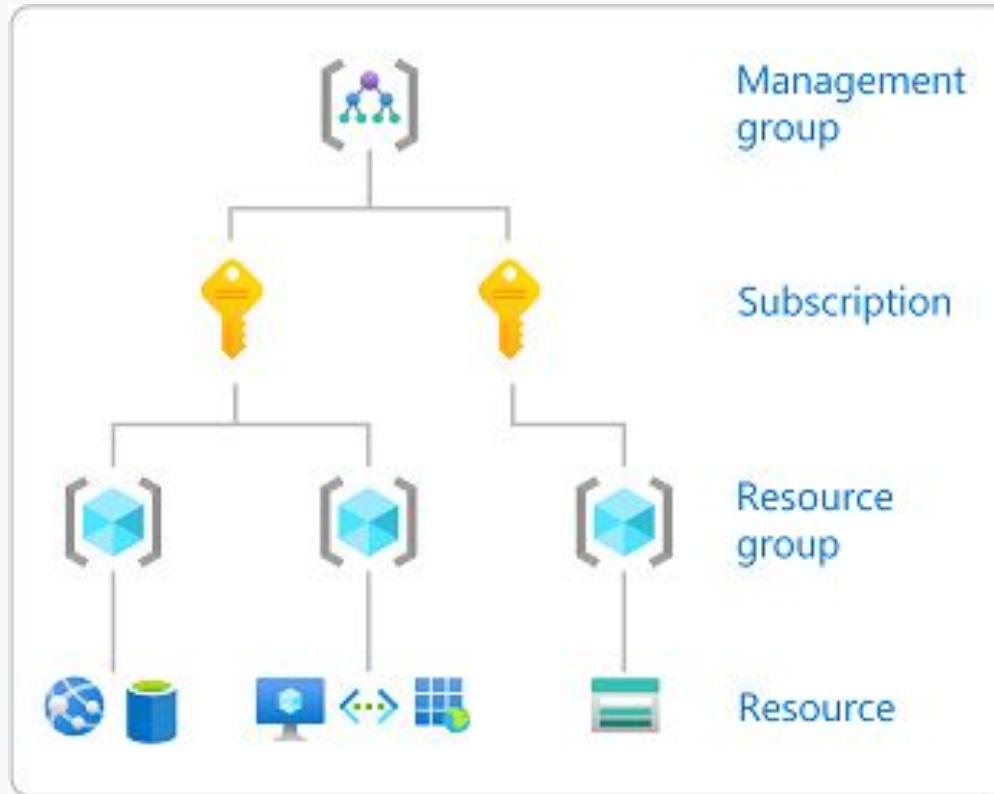
#GlobalAzure

# Possible Solution

## Introduction

1. ย้ายไปสร้างที่ Organization แทน มันไลส์ได้ 1,000 ตัว เพราะว่า secret จะไปเห็นที่ repo อื่นๆ ด้วย
2. สร้าง Service Principal ของแต่ละ resource group และ ตอน deploy ให้ไป download publish profile ทุกรรัง แทน เพื่อลดจำนวน secrets
3. เราจะเก็บ Decryption Key ใน Github secrets โดยแยกแต่ละ Environment หรือ group ที่เรากำหนดไว้ เวลาจะใช้ ก็ decrypt ออกมา ซึ่งไฟล์ encrypted secrets อยู่ใน Private Repo แทน ว่านาเพิ่ม

# Understand scope for Azure RBAC



# Our Solution

## Introduction

เราเลือกที่จะไปทางข้อ Solution ข้อที่ 3 โดยเราเลือกใช้ Mozilla SOPS ซึ่งเป็น Tools ที่เป็นที่นิยมมากๆ ในการจัดการ secrets โดยใช้วิธีการ symmetric encryption ไฟล์ Yaml

- เพื่อที่จะ encrypt secrets ต่างๆ โดย SOPS support การ Encrypt จาก Cloud ไม่ว่าจะเป็น Azure, AWS, หรือ GCP รวมถึง HashiCorp Vault ด้วย และยังสามารถใช้ Local Encrypt จาก Age และ PGP ได้อีกด้วย



#SopsWithKeyVault

## 2. Why Mozilla SOPS?



#GlobalAzure

# Why Mozilla SOPS?

เราไม่สามารถเก็บ secrets ทั้งหมดได้ใน GitHub Secrets เพราะจำนวน secrets ที่  
เยอะ จึงไม่สามารถเก็บใน 1 Github Secrets ที่มีขนาดไม่เกิน 64 KB

แต่ SOPS เองก็มีประเด็นต้องพิจารณาเพิ่มเติมด้วย

1. เราจะเก็บ Cipher text (Encrypted data) ไว้ที่ไหนก็จะปลอดภัย
2. เรื่องของ Key Rotation อาจจะต้องการจัดเอง

# Why Mozilla SOPS? (cont.)

ดังนั้น ถ้าเราเก็บ SOPS Encrypted Secrets ตรงๆ ใน GitHub Secrets ไม่ได้เนื่องจาก  
ขนาดเกิน การเก็บ Encrypted Secrets ใน Git Repo ก็ทางเลือกหนึ่งที่พอรับได้ แต่สิ่งที่  
ต้องเผชิญต่อไปคือ Internal Threat

# Our Final Decision

ถ้าการใช้ SOPS อาจจะยังไม่ตอบโจทย์เรื่องความปลอดภัยเพียงพอ เราอาจจะต้องใช้ External Secret Management Tool เช่น HashiCorp Vault

แต่สิ่งที่พิจารณาเพิ่มเติมคือ เรื่อง External Threat แทนที่จะเป็นเรื่องของ Internal Threat เวลาใช้ SOPS เก็บ secrets ใน Git Repo

เนื่องจากข้อจำกัดทางด้านเวลา และทรัพยากรที่เรามี เราจึงเลือกที่เก็บ SOPS encrypted secrets ใน Git Repo แทน จึงทำให้เราต้องมาพิจารณาเรื่อง internal threat แทน และขอไม่รับ External Threat มาเพิ่ม

#SopsWithKeyVault

# 3. Using SOPS with Age Encryption



#GlobalAzure

# Age Encryption

ใน Docs ของ SOPS ไม่แนะนำให้ใช้ PGP แล้ว ให้เปลี่ยนมาใช้ Age Encryption แทน โดย Age Encryption ใช้เป็น X25519 is an elliptic curve **Diffie-Hellman key exchange** using **Curve25519**.

# Age Encryption

```
$ brew install age
# Generate Age Key
$ age-keygen -o key.txt
# The contain in file key.txt :

# created: 2022-04-11T15:36:32+07:00
# public key: age1js5y137ghup68pzf8f2kutf6xtuwc4m6lpha01lgmcup93q3sp9qtfwvr8
AGE-SECRET-KEY-15YXVYTPWNT4UF3KY05K27LZN2SAT83SJKX7UH4MXQEQAWRWPFNYSDHK860

# Encrypt SOPS with Age
$ sops --encrypt --age
age1js5y137ghup68pzf8f2kutf6xtuwc4m6lpha01lgmcup93q3sp9qtfwvr8 examples/data.yaml >
examples/data.age-enc.yaml
```

# Encrypted SOPS

The image shows two side-by-side code editors. The left editor displays a file named `data.age-enc.yaml`, and the right editor displays a file named `data.yaml`. Both files contain YAML configuration with encrypted secret values.

**data.age-enc.yaml Content:**

```
examples > data.age-enc.yaml > {} sops > [ ] age
1 scope_a:
2   app_service:
3     app1: ENC[AES256_GCM,data:Z2y
+1hh5mNjyopGZioDgjeYsTs=,iv:U/U8ux1Su3M5HGDnz7H/
+X5SY1Bo83+OZ1uWdw/N8+Q=,tag:GwIPm/
LFKTdU4kpjL5VdDg==,type:str]
4 sops:
5   kms: []
6   gcp_kms: []
7   azure_kv: []
8   hc_vault: []
9   age:
10    - recipient:
11      age1js5y137ghup68pzf8f2kutf6xtuwc4m6lpha0llgmcup93q
12        3sp9qtfwvr8
13          enc: |
14            -----BEGIN AGE ENCRYPTED FILE-----
15            YWdlLWVuY3J5cHRpb24ub3JnL3YxCi0
16            +IFgyNTUxOSBST3JxRFhvNkxxaWI5a0p1
17            TGozNXBQRG9mdWJhRWNtSnJ2cnpxVWhTWXpjCld3bWZtMVB
18            10GpZS1JZcWhJZjh
19            U0IzRGRiWCtVcm5JQWtzcG9NRDVtWjAKLS0tIDh4aHpUMGZ
20            4TnFoaVZqT0VDc3ZG
21            UEErWjNGR3ZQQWJ5WGYwVlpVOGtCN0UK0ONX0/
22            1UCvLyA3kCL0qS0jk04reZjBK5
23            yoePNXJmpNGgqPMN3qQLYeV3f9gCDZiPo8Cu2NyeZrwqDXn
```

**data.yaml Content:**

```
examples > data.yaml > {} scope_a > {} app_service > app1
1 scope_a:
2   app_service:
3     app1: This is Super secret
```

Both files are displayed in a dark-themed code editor with syntax highlighting. The encrypted secret in the `data.age-enc.yaml` file is highlighted with a red box, and the decrypted value in the `data.yaml` file is also highlighted with a red box. The status bar at the bottom of the editor provides information about the file paths, commit history, and current settings.

# Age Decryption

```
$ cat key.txt

# created: 2022-04-11T15:36:32+07:00
# public key: age1js5y137ghup68pzf8f2kutf6xtuwc4m6lpha01lgmcup93q3sp9qtfwvr8
AGE-SECRET-KEY-15YXVYTPWNT4UF3KY05K27LZN2SAT83SJKX7UH4MXQEQAWRWPFNYSDHK860

# Decrypt SOPS with Age
$ export
SOPS_AGE_KEY="AGE-SECRET-KEY-15YXVYTPWNT4UF3KY05K27LZN2SAT83SJKX7UH4MXQEQAWRWPFNYSDH
K860"
$ sops --decrypt examples/data.age-enc.yaml > examples/data.yaml

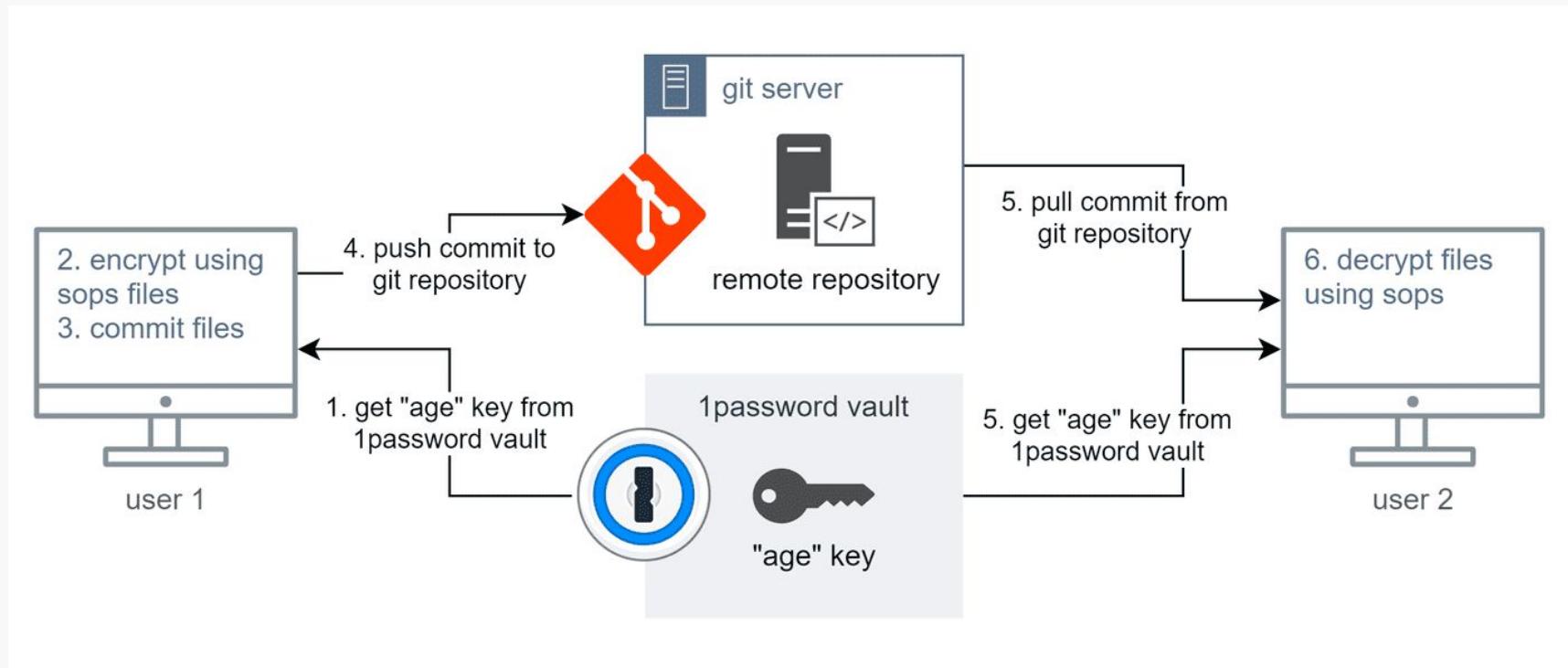
# SOPS also provide built-in editor using VIM
$ sops
```

# Discussion

แต่ปัญหา ก็คือ ....

- ใครเป็นคนเก็บ Age Secret Key?
- การแจกจ่าย key ให้คนอื่นใช้โดยไม่รู้ว่าใครเป็นคนใช้งาน ถือว่าเป็นปัญหาหนึ่งของ security

# Using 1Password as Key Store



# Conclusion

- การแจกจ่าย Key (Key Distribution) ให้คนอื่นใช้โดยไม่รู้ว่าใครเป็นคนใช้งาน อาจจะเกิดปัญหาเรื่อง Key หลุดแล้ว Track ไม่ได้ว่าเกิดอะไร
- ดังนั้นการใช้ 3rd Party Secret Management ช่วย
  - Azure Key Vault จะช่วยเก็บ Private Key

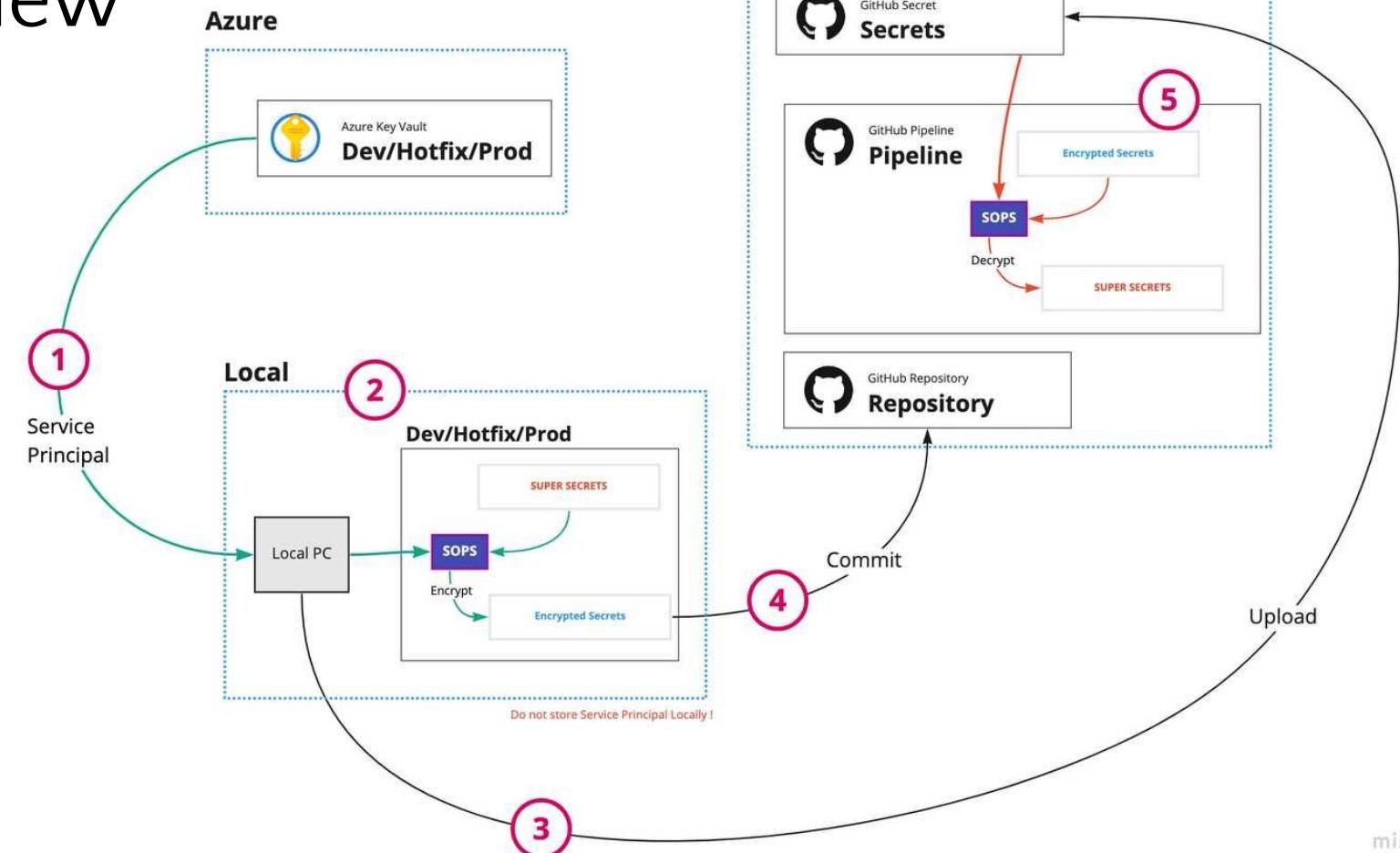
#SopsWithKeyVault

# 4. Using SOPS with Azure Key Vault



#GlobalAzure

# Overview



# SOPS with Azure Key Vault

The screenshot shows a code editor with two files open:

- data.azure-enc.yaml**: This file contains SOPS-encrypted secrets. A red box highlights the section where an app service's password is encrypted using AES256\_GCM. The encrypted string is: `ENC[AES256_GCM,data:H/H9Ed1R5kYga3mJJ5+NAVW35Ro=,iv:IbY1zZD0uE7E+z0Z5wSi6sstGog35mvroAtUaPrlsGQ=,tag:saSwkqt6T+scchd7oQm9Fw==,type:str]`. Another red box highlights the Azure Key Vault configuration, which includes the vault URL (`https://kv-github-action-sops.vault.azure.net`), key name (`sops-key`), key version (`cabcd0f57d0640a9ba91620f36c2a61b`), creation timestamp (`2022-04-11T08:40:33Z`), and the encrypted password itself.
- data.yaml**: This file contains a plain text secret for comparison: `app1: This is Super secret`.

Both files have a line of code at the bottom: `age: [] You, 3 days ago · github action: add test for azure key vault ...`

At the bottom of the editor, there are status indicators: `main`, `Git Graph`, `You, 3 days ago`, `Ln 14, Col 12`, `Spaces: 4`, `UTF-8`, `LF`, `YAML`, `No JSON Schema`, `✓ Prettier`, and icons for `Copy` and `Bell`.

# SOPS with GitHub Actions

```
steps:
  - uses: actions/checkout@v3
  - uses: mildronize/actions-get-secret-sops/azure@v1
    id: sops
    with:
      path: "azure.enc.yaml" # Encrypted SOPS yaml path
      property-path: ".scope_a.app_service.app1" # jq/yq expression syntax for
      decrypting-key: ${{ secrets.Azure_Credential }} # Azure Service Principle
      sops-version: '3.7.2'

  - run: echo "${{ steps.sops.outputs.secret }}"
```

ในการใช้งาน [mildronize/actions-get-secret-sops](#) จะต้องกำหนด `property-path` สำหรับเข้าถึง secret ที่เราต้องการผ่าน path ของ yaml ไฟล์ โดยใช้ syntax ของ `jq` หรือ `yq` ก็ได้



#SopsWithKeyVault

# 5. DEMO Time



#GlobalAzure

# Q&A

Thank you 

Follow me:

- [thadaw.com](https://thadaw.com) since 2015
- [medium.com/@thadaw](https://medium.com/@thadaw)

.NET Thailand:

- [fb.com/groups/dotnetthailand](https://fb.com/groups/dotnetthailand)
- [www.dotnetthailand.com](https://www.dotnetthailand.com)

## Article for this talk

<https://thadaw.com/s/suzlta6/>

## Main Repo

<https://github.com/mildronize/100-secrets-github-actions-sops-with-azure-key-vault>

## SOPS Secrets Template

<https://github.com/mildronize/sops-with-azure-keyvault-secrets>

## SOPS Actions for Azure Key Vault

<https://github.com/mildronize/actions-get-secret-sops>

SOPS with Key Vault

## **Previous Talks: Deploy Multiple Azure App Services using GitHub Actions Matrix**

<https://github.com/mildronize/deploy-multiple-azure-app-services-using-github-actions-matrix>

## **Azure Utility Tools**

<https://github.com/dotnetthailand/azure-tools>

May 5<sup>th</sup> - 7<sup>th</sup>, 2022

#GlobalAzure

