

Encrypting Ansible secrets with SOPS

Felix Fontein

September 12th, 2023

Roadmap

- 1 Unrelated things
- 2 What is SOPS?
- 3 How does it compare to Ansible Vault?
- 4 Using SOPS with community.sops

Who am I?

Felix Fontein ('fe:liks 'fontain)

✉ felix@fontein.de

🔗 @felixfontein

felixfontein (Libera.Chat)

felixfontein:matrix.org (Matrix)

Ansible contributor

- (co-)maintainer of several community collections
 - among them community.sops
- co-maintainer of antsibull tools
- member of Ansible Community Steering Committee

SOPS contributor

co-maintainer of SOPS (for 3 weeks by now)



Ansible Forum

Officially available since September 11th:

forum.ansible.com

≡

ANSIBLE
COMMUNITY

[Sign Up](#) [Log In](#)  

Topics

Groups

More

Categories

News & Announcements

Get Help

Project Discussions

Events

Social Space

International Communities

Forum Guide & Feedback

All categories


Tags


documentation

All tags

Welcome to the Ansible Community! This is the place to discuss anything related to Ansible - the language, the tools, the collections, the wider ecosystem, meetups, events - anything Ansible that's on your mind!

Here are some things you can do to get started:

 **Introduce yourself** by adding your picture and information about yourself and your interests to [your profile](#). What is one thing you'd like to be asked about? Also, come say hi in the [Introduce yourself!](#) topic!

 **Get to know the community** by [browsing discussions](#) that are already happening here. When you find a post interesting, informative, or

all categories ▾

all tags ▾

Categories


Latest

Top

Category


Topics


Latest


 **News & Announcements**


7 / month

All the latest activity in the Ansible Community.

 Newsletter


 Ecosystem Releases


 Blog

 **Get Help**



17 / month

Need help? This is the place! Get started with Ansible, debug your playbooks, set up your tooling ... whatever your question, ask it here!


 Guides, FAQs & Howtos


 **Project Discussions**

14 / month


 **Welcome to the Ansible Community!** 



4
Jul 21


 News & Announcements

 **Host bulk deletion**



0
7h

 Project Discussions

 feedback-wanted  awx

 **DjangoCon.us 2023 (Durham, USA)**

0
1d

 Events  conference

This website uses cookies to function. The compliance people asked us to tell you. [More information.](#)

Fine.

SOPS: Secrets OPerationS (1/3)

- Secret handling tool

`https://github.com/getsops/sops`

SOPS: Secrets OPerationS (1/3)

- Secret handling tool

`https://github.com/getsops/sops`

- Handles **structured data**: YAML, JSON, INI, ...
 - ... but also binary files (Base64);
 - keys are not encrypted;
 - values and comments are encrypted.

SOPS: Secrets OPerationS (1/3)

- **Secret handling tool**
<https://github.com/getsops/sops>
- Handles **structured data**: YAML, JSON, INI, ...
 - ... but also binary files (Base64);
 - keys are not encrypted;
 - values and comments are encrypted.
- **Multiple identities** can have access
 - GPG, Age, AWS KMS, Google Cloud KMS, Azure Key Vault, Hashicorp Vault
 - supports **Shamir's Secret Sharing** (need access to multiple identities to decrypt)

SOPS: Secrets OPerationS (2/3)

- Written and originally maintained by (ex-)Mozilla employees
- Effectively unmaintained since June 2022
 - A lot of community PRs, but no way to get them merged...
 - Or get a new release with some already merged bugfixes out...

SOPS: Secrets OPerationS (2/3)

- Written and originally maintained by (ex-)Mozilla employees
- Effectively unmaintained since June 2022
 - A lot of community PRs, but no way to get them merged...
 - Or get a new release with some already merged bugfixes out...
- February 2023: SOPS has applied to be adopted into the CNCF sandbox
- May 2023: **CNCF sandbox application accepted!**

SOPS: Secrets OPerationS (2/3)

- Written and originally maintained by (ex-)Mozilla employees
- Effectively unmaintained since June 2022
 - A lot of community PRs, but no way to get them merged...
 - Or get a new release with some already merged bugfixes out...
- February 2023: SOPS has applied to be adopted into the CNCF sandbox
- May 2023: **CNCF sandbox application accepted!**
- August 25th: 3.8.0-rc.1 pre-release

SOPS: Secrets OPerationS (3/3)

- Quick demo!
- Contents:
 - `.sops.yaml` config
 - `example.sops.yaml` file

SOPS vs. Ansible Vault

SOPS

- asymmetric crypto

Ansible Vault

- symmetric crypto

Other service (via plugin)

- "trust by contract"

HashiVault, BitWarden,
OnePassword, ... →

SOPS vs. Ansible Vault

SOPS

- ⦿ asymmetric crypto
- ⊕ multiple identities per file

Ansible Vault

- ⦿ symmetric crypto
- ⊖ one passphrase per file

Other service (via plugin)

- ⦿ "trust by contract"
- ⊕ access management

HashiVault, BitWarden, →
OnePassword, ...

SOPS vs. Ansible Vault

SOPS

- ⦿ asymmetric crypto
- ⊕ multiple identities per file
- ⊕ no service needed

Ansible Vault

- ⦿ symmetric crypto
- ⊖ one passphrase per file
- ⊕ no service needed


Other service (via plugin)

- ⦿ "trust by contract"
- ⊕ access management
- ⊖ needs service

HashiVault, BitWarden, →
OnePassword, ...


SOPS vs. Ansible Vault

SOPS


- ⦿ asymmetric crypto
- ⊕ multiple identities per file
- ⊕ no service needed
- ⊖ no native  support

HashiVault, BitWarden,
OnePassword, ... →

Ansible Vault

- ⦿ symmetric crypto
- ⊖ one passphrase per file
- ⊕ no service needed
- ⊕ native  support

Other service (via plugin)

- ⦿ "trust by contract"
- ⊕ access management
- ⊖ needs service
- ⊖ no native  support

Ansible community.sops collection: roles and playbooks

Roles

- `community.sops.install`

Playbooks

- `community.sops.install`
- `community.sops.install_localhost`
 - Useful for setting up Execution Environments


Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- Vars plugin: `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- Lookup: `community.sops.sops`
- Filter: `community.sops.decrypt`
- Module: `community.sops.sops_encrypt`

Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- **Vars plugin:** `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- Lookup: `community.sops.sops`
- Filter: `community.sops.decrypt`
- Module: `community.sops.sops_encrypt`


Vars plugin `community.sops.sops`

Load encrypted files directly from `host_vars` and `group_vars` as  variables.

Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- Vars plugin: `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- Lookup: `community.sops.sops`
- Filter: `community.sops.decrypt`
- Module: `community.sops.sops_encrypt`

Action plugin `community.sops.load_vars`

Load encrypted file similar to
`ansible.builtin.include_vars` as  facts.

Caveat: interpolation must be done at load time.

Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- Vars plugin: `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- **Lookup: `community.sops.sops`**
- Filter: `community.sops.decrypt`
- Module: `community.sops.sops_encrypt`

Lookup `community.sops.sops`

Load encrypted file from disk:

```
lookup('community.sops.sops', '/path/to/file').
```

Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- Vars plugin: `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- Lookup: `community.sops.sops`
- Filter: `community.sops.decrypt`
- Module: `community.sops.sops_encrypt`

Filter `community.sops.decrypt`

Decrypt data in Jinja2 expressions:

```
encrypted_data | community.sops.decrypt.
```

Ansible community.sops collection: plugins

- Documentation on docs.ansible.com
- Vars plugin: `community.sops.sops`
- Action plugin: `community.sops.load_vars`
- Lookup: `community.sops.sops`
- Filter: `community.sops.decrypt`
- **Module: `community.sops.sops_encrypt`**

Module `community.sops.sops_encrypt`

Encrypt data with SOPS, for example output of another task:
`community.crypto.openssl_privatekey_pipe` →
`community.sops.sops_encrypt`

Load encrypted data files as variables

```
1 - hosts: webserver
2   vars_files:
3     - data/letsencrypt.yml
4   pre_tasks:
5     - name: Load encrypted credentials
6       community.sops.load_vars:
7         file: keys/credentials.sops.yml
8         expressions: ignore # or: evaluate-on-load
9         tags: always
10        no_log: true
11  roles:
12    - ...
```

Note

Expressions must be evaluated on load time (\neq include_vars).

Create or update SOPS encrypted private key

```
1  - block:
2    - community.crypto.openssl_privatekey_pipe:
3      content: "{{lookup('community.sops.sops',
4        'keys/private_key.pem.sops',
5        empty_on_not_exist=true)|default(omit,true)}}"
6      no_log: true
7      register: private_key_temp
8
9    - community.sops.sops_encrypt:
10     path: keys/private_key.pem.sops
11     content_text: "{{private_key_temp.privatekey}}"
12     when: private_key_temp.changed
13
14  always:
15    - ansible.builtin.set_fact:
16      private_key_temp: ''
```


Thank You for your attention!

Questions? Comments?

[Link to demo repository](#)