Enhancing Ansible Content within open-source projects

Nejc Slabe
DevRel at XLAB Steampunk
nejc.slabe@xlab.si

Anže Luzar
DevSecOps Engineer at XLAB Steampunk
anje.luzar@xlab.si
IT automation specialists. Ansible ninjas.
Problem

Lots of open-source projects are using Ansible.

- Most of that Ansible content is not up to date or fully compatible with target Ansible version.
- QA and SAST is often not present, without any testing/linting in the project.
- Linting in the projects is more about formatting the code then linting it.
Advanced tools can fix that and offer trustable automation for all.

This brings benefits that if we fix the public repos, we influence a lot of people:

• To start writing Ansible content of better quality.
• Be safer with the Ansible content on the web.
Problems in Ansible Content

- Best practices.
- Validation (of AI generated code).
- Upgrade and Security, Ansible is getting old and for new users it can be confusing.
Bad playbook example

playbook.yml

```yaml
---
- name: Bad playbook
  hosts: localhost
  tasks:
    - name: Change ownership, group and permissions for file
      ansible.builtin.file:
        path: /etc/file.txt
        owner: user
        group: user
        mode: "644"
        follow: true
      with_items: [ 1, 2, 3, 4 ]
```

Good playbook example

playbook.yml

```yaml
---
- name: Good playbook
  hosts: localhost
  tasks:
    - name: Change ownership, group and permissions for file
      ansible.builtin.file:
        path: /etc/file.txt
        owner: user
        group: user
        mode: "644"
        follow: true
      with_items: [ 1, 2, 3, 4 ]
```

Steampunk
Ansible scanning tools

- Ansible Lint
- Ansible Later
- Ansible Navigator
- Ansible Molecule
- KICS – Keeping Infrastructure as Code Secure
- Deepsource
- Steampunk Spotter
Steampunk Spotter

Trustable Automation

Ansible Playbook Scanning Tool that analyzes and offers recommendations for your playbooks.

steampunk.si/spotter
The Power of Spotter
Use case

Easily upgrade to a specific Ansible version
Features

Quickly apply fixes to playbooks

```yaml
cat playbook.yml
---
name: Sample playbook
hosts: localhost
tasks:
  - name: Ensure that the server certificate belongs to the specified private key
    openssl_certificate:
      path: "{{ config_path }}/certificates/server.crt"
      privatekey_path: "{{ config_path }}/certificates/server.key"
      provider: assertonly

# Spotter scan --rewrite playbook.yml
playbook.yml:7: ERROR: Use a fully-qualified name, such as community.crypto.x509_certificate instead of openssl_certificate.
View docs at https://docs.ansible.com/ansible/latest/plugins/macros/community.crypto.html
playbook.yml:5:7: HINT: Required collection community.crypto is missing from requirements.yml or requirements.yml is missing.
---
cat playbook.yml
---
name: Sample playbook
hosts: localhost
tasks:
  - name: Ensure that the server certificate belongs to the specified private key
    community.crypto.x509_certificate:
      path: "{{ config_path }}/certificates/server.crt"
      privatekey_path: "{{ config_path }}/certificates/server.key"
      provider: assertonly
```

XLAB Steampunk
Features

Save time with convenience features
Enhancing open-source projects
Selecting and scanning projects

Ansible Lockdown, RedHat COP, etc.
Selecting and scanning projects

- Ansible Lockdown, RedHat COP, etc.
- Scanning projects from Ansible Lockdown (with Steampunk Spotter):
  - RHEL7-CIS, UBUNTU-22-CIS, AMAZON2023-CIS, Windows2016-CIS, etc.
  - Used Spotter CLI and Spotter App
  - FQCNs, invalid/deprecated module parameters, inline values, etc.
Selecting and scanning projects

Spotter took 2.144 s to scan your input.
It resulted in 9 error(s), 151 warning(s) and 122 hint(s).
Overall status: ERROR
Selecting and scanning projects

- Ansible Lockdown, RedHat COP, etc.
- Scanning projects from Ansible Lockdown (with Steampunk Spotter):
  - RHEL7-CIS, UBUNTU-22-CIS, AMAZON2023-CIS, Windows2016-CIS, etc.
  - Used Spotter CLI and Spotter App
  - FQCNs, invalid/deprecated module parameters, inline values, etc.

DEMO: [https://spotter.steampunk.si](https://spotter.steampunk.si)
Fixing errors

Fixing errors in projects from Ansible Lockdown (with Steampunk Spotter):

- [https://github.com/ansible-lockdown/RHEL7-CIS/pull/321](https://github.com/ansible-lockdown/RHEL7-CIS/pull/321)
- [https://github.com/ansible-lockdown/UBUNTU22-CIS/pull/72](https://github.com/ansible-lockdown/UBUNTU22-CIS/pull/72)
- [https://github.com/ansible-lockdown/Windows-2016-CIS/pull/37](https://github.com/ansible-lockdown/Windows-2016-CIS/pull/37)
- [https://github.com/ansible-lockdown/RHEL7-STIG/pull/437](https://github.com/ansible-lockdown/RHEL7-STIG/pull/437)
- [https://github.com/ansible-lockdown/AMAZON2023-CIS/pull/8](https://github.com/ansible-lockdown/AMAZON2023-CIS/pull/8)
Ensuring trustable automation

How can we establish QA on public open-source projects?

- DEMO: https://github.com/anzoman/RHEL7-CIS
Ensuring trustable automation

How can we establish QA on public open-source projects:

- Choosing the right Ansible version (e.g., 2.12)
- Local scanning (with CLIs, in IDEs, development scripts, pre-commit hooks)
Ensuring trustable automation

How can we establish QA on public open-source projects:

- Choosing the right Ansible version (e.g., 2.12)
- Local scanning (with CLIs, in IDEs, development scripts, pre-commit hooks)
- Establish CI/CD (e.g., Lint + Spotter)
Ensuring trustable automation

How can we establish QA on public open-source projects:

- Choosing the right Ansible version (e.g., 2.12)
- Local scanning (with CLIs, in IDEs, development scripts, pre-commit hooks)
- Establish CI/CD (e.g., Lint + Spotter)
- Improving the content on the fly
Ensuring trustable automation

How can we establish QA on public open-source projects:

- Choosing the right Ansible version (e.g., 2.12)
- Local scanning (with CLIs, in IDEs, development scripts, pre-commit hooks)
- Establish CI/CD (e.g., Lint + Spotter)
- Improving the content on the fly
- Extra: rewriting and Spotter GitOps
Ensuring trustable automation

tasks/section_6/main.yml:3:3: HINT: [H1001] Inline passing of parameters is not good practice.

Spotter took 2.066 s to scan your input.
It resulted in 0 error(s), 0 warning(s) and 181 hint(s).
Overall status: HINT

spotter scan --ansible-version 2.12 --display-level hint --rewrite .


Spotter took 2.083 s to scan your input.
It resulted in 0 error(s), 0 warning(s) and 129 hint(s).
Overall status: HINT
Ensuring trustable automation
Ensuring trustable automation

How can we establish QA on public open-source projects:

▪ Choosing the right Ansible version (e.g., 2.12)
▪ Local scanning (with CLIs, in IDEs, development scripts, pre-commit hooks)
▪ Establish CI/CD (e.g., Lint + Spotter)
▪ Improving the content on the fly
▪ Extra: rewriting and Spotter GitOps
▪ DEMO: https://github.com/anzoman/RHEL7-CIS
Conclusion and key takeaway

Benefits:
- Improving Ansible content
- Spreading the knowledge about common flaws
- Improving the tools themselves

Process (gathering ecosystem of tools)

Spread the word!

Ansible Challenge: https://steampunk.si/ansible-challenge/
Steampunk Spotter

Visit our page
steampunk.si/spotter

Talk to us
Nejc Slabe
nejc.slabe@xlab.si

Anže Luzar
anje.luzar@xlab.si

Join the Ansible Challenge
steampunk.si/ansible-challenge

Follow us