XLAB Steampunk

Enhancing Ansible Content

within open-source projects

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

Anže Luzar
DevSecOps Engineer at XLAB Steampunk
anze.luzar@xlab.si

XLAB
Steampunk

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.

Solution

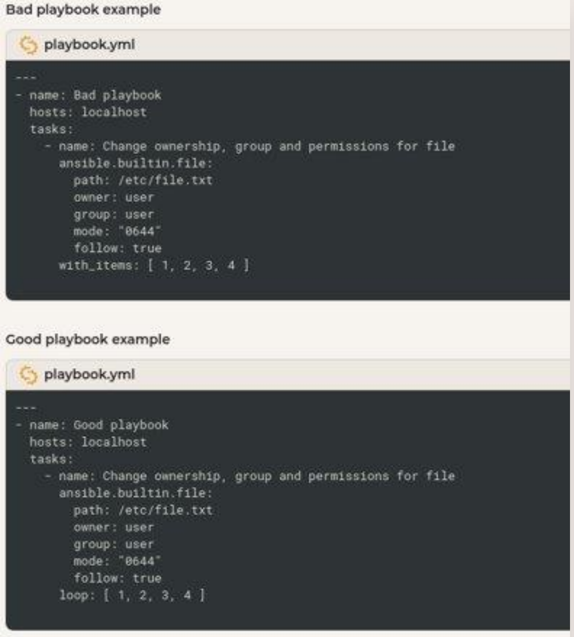
Advanced tools can fix that and offer trustable automation for all.

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

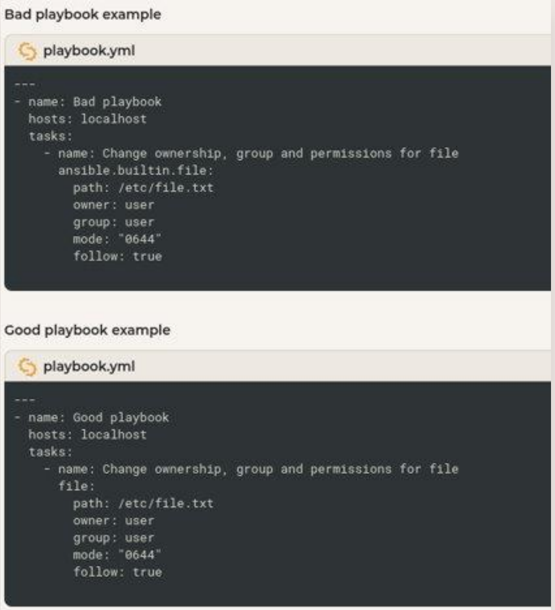
playbook.yml

```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: "0644"
        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: "0644"
        follow: true
      loop: [ 1, 2, 3, 4 ]
```



Bad playbook example

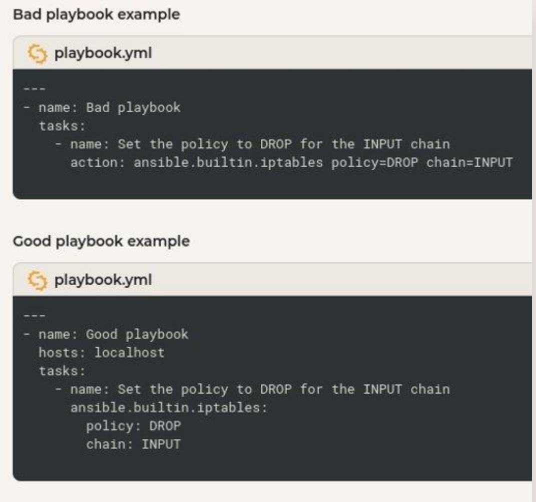
playbook.yml

```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: "0644"
        follow: true
```

Good playbook example

playbook.yml

```yaml
---
- name: Good playbook
  hosts: localhost
  tasks:
    - name: Change ownership, group and permissions for file
      file:
        path: /etc/file.txt
        owner: user
        group: user
        mode: "0644"
        follow: true
```



Bad playbook example

playbook.yml

```yaml
---
- name: Bad playbook
  tasks:
    - name: Set the policy to DROP for the INPUT chain
      action: ansible.builtin.iptables policy=DROP chain=INPUT
```

Good playbook example

playbook.yml

```yaml
---
- name: Good playbook
  hosts: localhost
  tasks:
    - name: Set the policy to DROP for the INPUT chain
      ansible.builtin.iptables:
        policy: DROP
        chain: INPUT
```

Ansible scanning tools

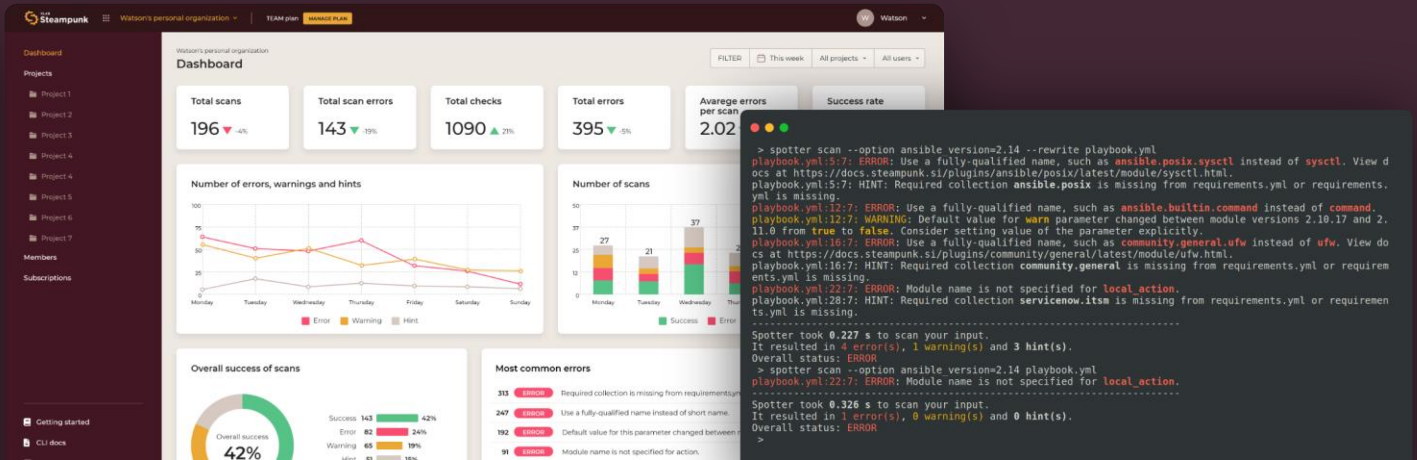
- Ansible Lint
- Ansible Later
- Ansible Navigator
- Ansible Molecule
- KICS – Keeping Infrastructure as Code Secure
- Deepsource
- Steampunk Spotter

Steampunk Spotter

Trustable Automation

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

steampunk.si/spotter



Total scans 196 ▼ -4%

Total scan errors 143 ▼ -19%

Total checks 1090 ▲ 21%

Total errors 395 ▼ -5%

Avarege errors per scan 2.02

Success rate

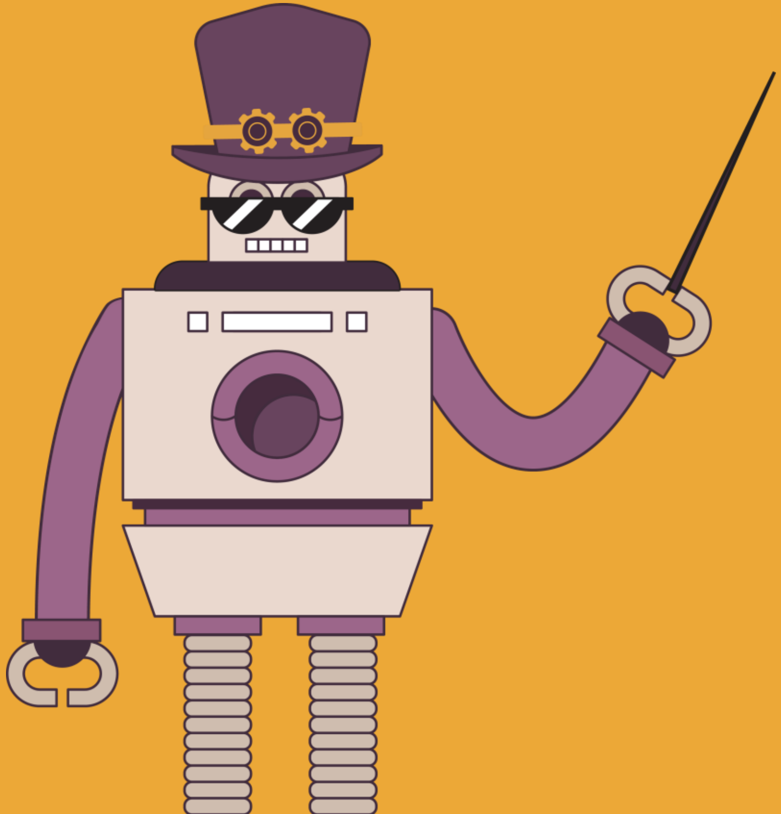
Success	143	🟩	42%
Error	82	🟥	24%
Warning	65	🟨	19%
Hint	51	▨	15%

Most common errors

313	ERROR	Required collection is missing from requirements.yml
247	ERROR	Use a fully-qualified name instead of short name.
192	ERROR	Default value for this parameter changed between
91	ERROR	Module name is not specified for action.

```
 > spotter scan --option ansible version=2.14 --rewrite playbook.yml
playbook.yml:5:7: ERROR: Use a fully-qualified name, such as ansible.posix.sysctl instead of sysctl. View d
ocs at https://docs.steampunk.si/plugins/ansible/posix/latest/module/sysctl.html.
playbook.yml:5:7: HINT: Required collection ansible.posix is missing from requirements.yml or requirements.
yml is missing.
playbook.yml:12:7: ERROR: Use a fully-qualified name, such as ansible.builtin.command instead of command.
playbook.yml:12:7: WARNING: Default value for warn parameter changed between module versions 2.10.17 and 2.
11.0 from true to false. Consider setting value of the parameter explicitly.
playbook.yml:16:7: ERROR: Use a fully-qualified name, such as community.general.ufw instead of ufw. View do
cs at https://docs.steampunk.si/plugins/community/general/latest/module/ufw.html.
playbook.yml:16:7: HINT: Required collection community.general is missing from requirements.yml or requirem
ents.yml is missing.
playbook.yml:22:7: ERROR: Module name is not specified for local_action.
playbook.yml:28:7: HINT: Required collection servicenow.itsm is missing from requirements.yml or requiremen
ts.yml is missing.
--------------------------------------------------------------------------
Spotter took 0.227 s to scan your input.
It resulted in 4 error(s), 1 warning(s) and 3 hint(s).
Overall status: ERROR
 > spotter scan --option ansible_version=2.14 playbook.yml
playbook.yml:22:7: ERROR: Module name is not specified for local_action.
--------------------------------------------------------------------------
Spotter took 0.326 s to scan your input.
It resulted in 1 error(s), 0 warning(s) and 0 hint(s).
Overall status: ERROR
 >
```

XLAB Steampunk

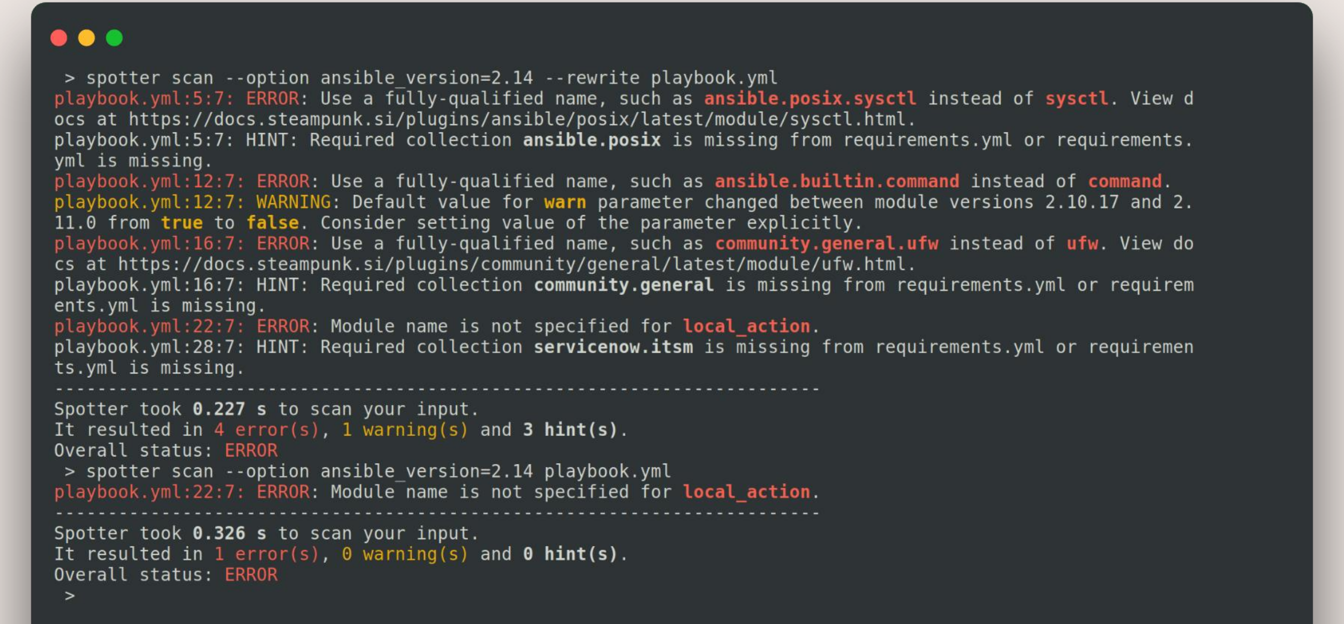


The Power of Spotter

XLAB Steampunk

Use case

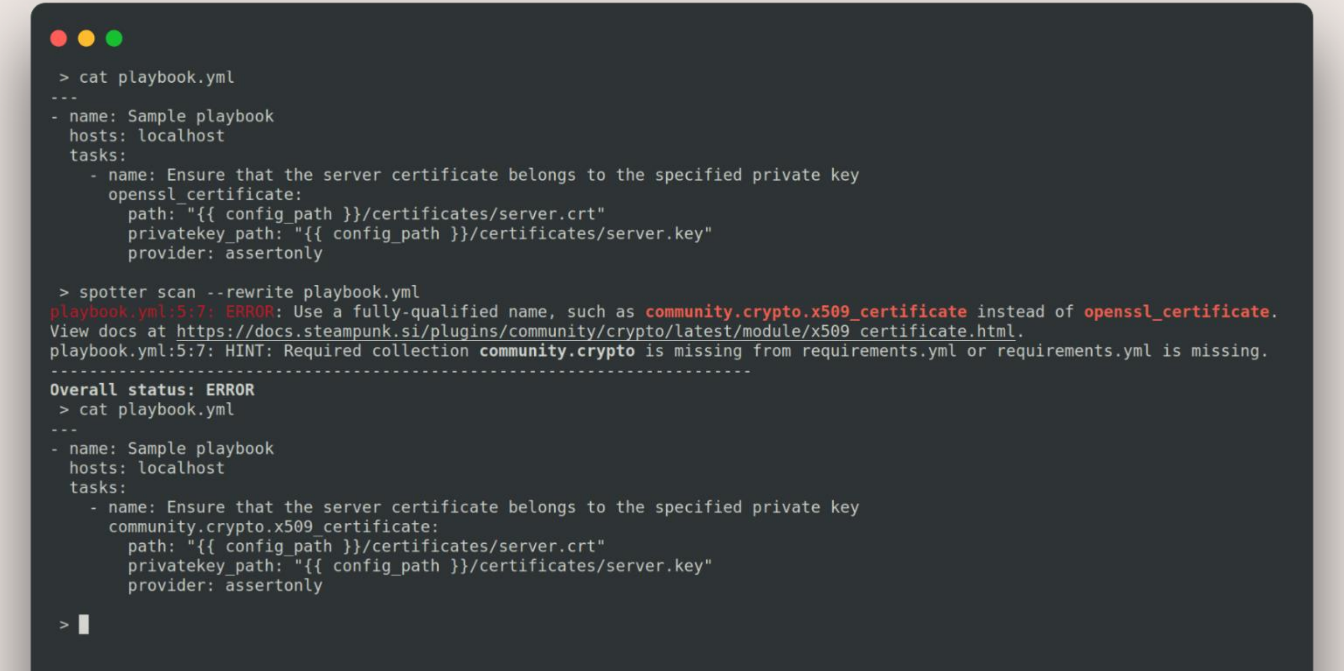
Easily upgrade to a specific Ansible version



```
 > spotter scan --option ansible_version=2.14 --rewrite playbook.yml
playbook.yml:5:7: ERROR: Use a fully-qualified name, such as ansible.posix.sysctl instead of sysctl. View d
ocs at https://docs.steampunk.si/plugins/ansible/posix/latest/module/sysctl.html.
playbook.yml:5:7: HINT: Required collection ansible.posix is missing from requirements.yml or requirements.
yml is missing.
playbook.yml:12:7: ERROR: Use a fully-qualified name, such as ansible.builtin.command instead of command.
playbook.yml:12:7: WARNING: Default value for warn parameter changed between module versions 2.10.17 and 2.
11.0 from true to false. Consider setting value of the parameter explicitly.
playbook.yml:16:7: ERROR: Use a fully-qualified name, such as community.general.ufw instead of ufw. View do
cs at https://docs.steampunk.si/plugins/community/general/latest/module/ufw.html.
playbook.yml:16:7: HINT: Required collection community.general is missing from requirements.yml or requirem
ents.yml is missing.
playbook.yml:22:7: ERROR: Module name is not specified for local_action.
playbook.yml:28:7: HINT: Required collection servicenow.itsm is missing from requirements.yml or requiremen
ts.yml is missing.
-------------------------------------------------------------------------
Spotter took 0.227 s to scan your input.
It resulted in 4 error(s), 1 warning(s) and 3 hint(s).
Overall status: ERROR
 > spotter scan --option ansible_version=2.14 playbook.yml
playbook.yml:22:7: ERROR: Module name is not specified for local_action.
-------------------------------------------------------------------------
Spotter took 0.326 s to scan your input.
It resulted in 1 error(s), 0 warning(s) and 0 hint(s).
Overall status: ERROR
 >
```

Features

Quickly apply fixes to playbooks

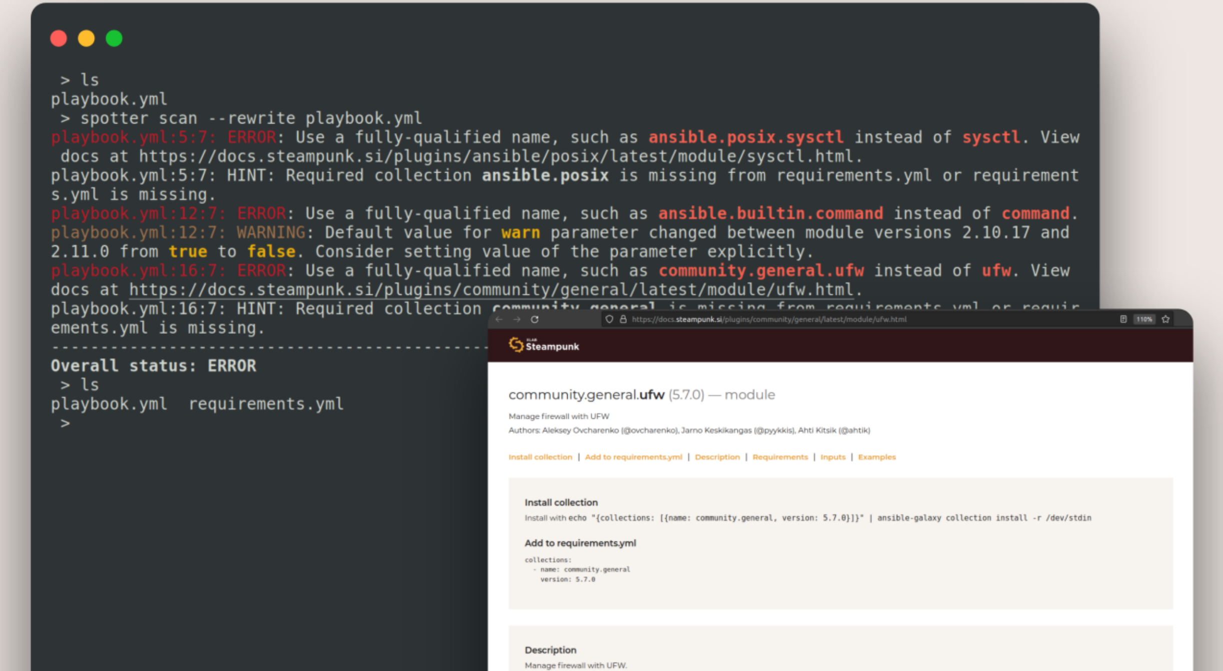


```
 > cat playbook.yml
---
- name: Sample playbook
  hosts: localhost
  tasks:
    - name: Ensure that the server certificate belongs to the specified private key
      openssl_certificate:
        path: "{{ config_path }}/certificates/server.crt"
        privatekey_path: "{{ config_path }}/certificates/server.key"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

 > spotter scan --rewrite playbook.yml
playbook.yml:5:7: ERROR: Use a fully-qualified name, such as community.crypto.x509_certificate instead of openssl_certificate.
View docs at https://docs.steampunk.si/plugins/community/crypto/latest/module/x509_certificate.html.
playbook.yml:5:7: HINT: Required collection community.crypto is missing from requirements.yml or requirements.yml is missing.
------------------------------------------------------------------------
Overall status: ERROR
 > 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



```
 > ls
playbook.yml
 > spotter scan --rewrite playbook.yml
playbook.yml:5:7: ERROR: Use a fully-qualified name, such as ansible.posix.sysctl instead of sysctl. View
 docs at https://docs.steampunk.si/plugins/ansible/posix/latest/module/sysctl.html.
playbook.yml:5:7: HINT: Required collection ansible.posix is missing from requirements.yml or requirement
s.yml is missing.
playbook.yml:12:7: ERROR: Use a fully-qualified name, such as ansible.builtin.command instead of command.
playbook.yml:12:7: WARNING: Default value for warn parameter changed between module versions 2.10.17 and
2.11.0 from true to false. Consider setting value of the parameter explicitly.
playbook.yml:16:7: ERROR: Use a fully-qualified name, such as community.general.ufw instead of ufw. View
docs at https://docs.steampunk.si/plugins/community/general/latest/module/ufw.html.
playbook.yml:16:7: HINT: Required collection community.general is missing from requirements.yml or requir
ements.yml is missing.
-----------------------------------------
Overall status: ERROR
 > ls
playbook.yml  requirements.yml
 >
```

https://docs.steampunk.si/plugins/community/general/latest/module/ufw.html

community.general.**ufw** (5.7.0) — module

Manage firewall with UFW

Authors: Aleksey Ovcharenko (@ovcharenko), Jarno Keskikangas (@pyykkis), Ahti Kitsik (@ahtik)

Install collection | Add to requirements.yml | Description | Requirements | Inputs | Examples

Install collection

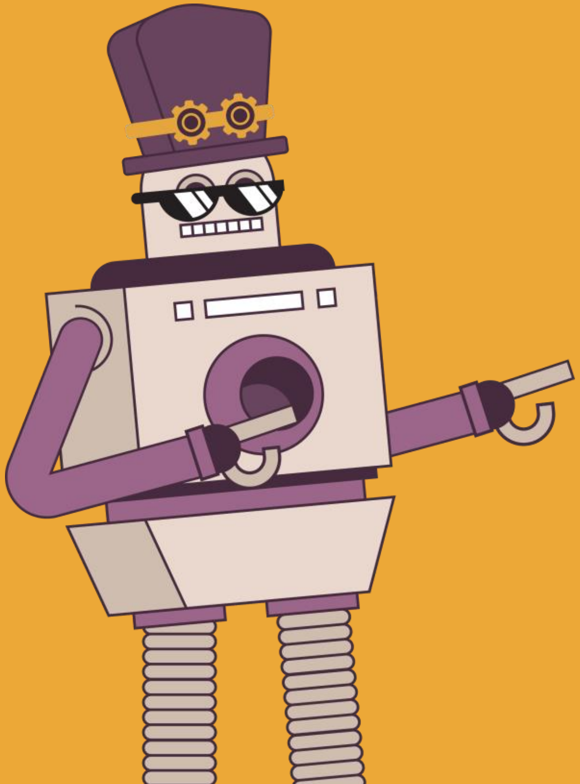
Install with `echo "{collections: [{name: community.general, version: 5.7.0}]}" | ansible-galaxy collection install -r /dev/stdin`

Add to requirements.yml

```
collections:
  - name: community.general
    version: 5.7.0
```

Description

Manage firewall with UFW.

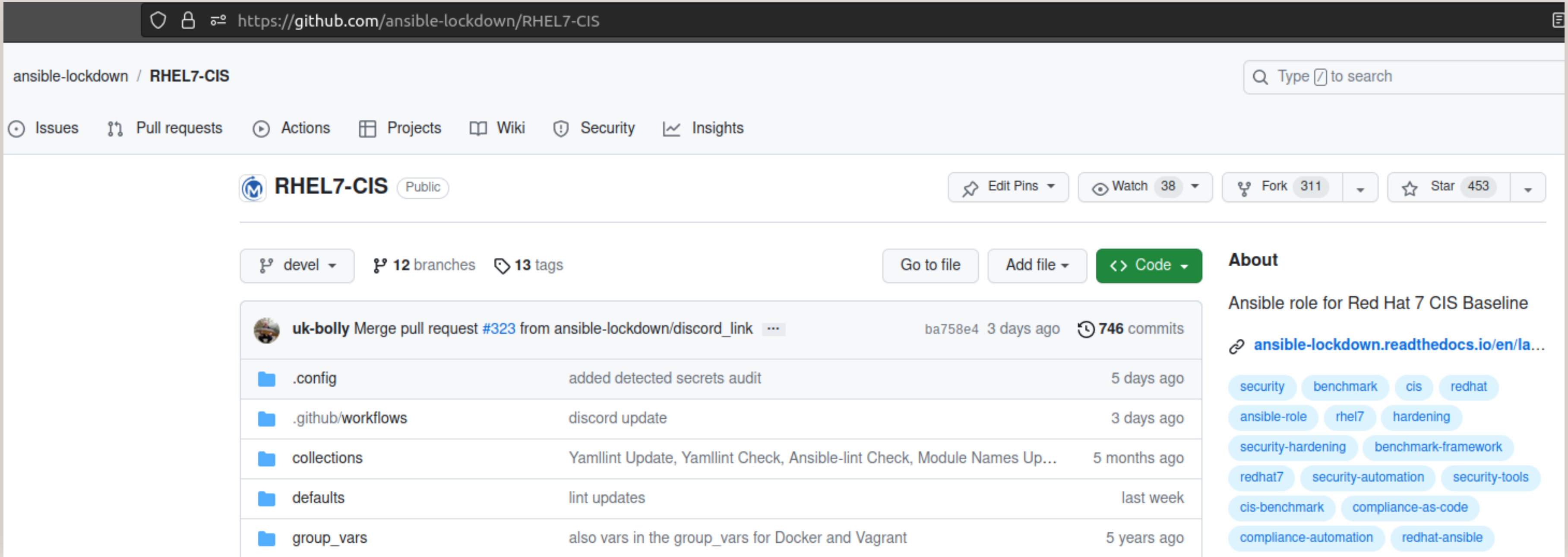


DEMO

Enhancing open-source projects

Selecting and scanning projects

Ansible Lockdown, RedHat COP, etc.



https://github.com/ansible-lockdown/RHEL7-CIS

ansible-lockdown / RHEL7-CIS

RHEL7-CIS Public

uk-bolly Merge pull request #323 from ansible-lockdown/discord_link ··· ba758e4 3 days ago 746 commits

.config	added detected secrets audit	5 days ago
.github/workflows	discord update	3 days ago
collections	Yamllint Update, Yamllint Check, Ansible-lint Check, Module Names Up…	5 months ago
defaults	lint updates	last week
group_vars	also vars in the group_vars for Docker and Vagrant	5 years ago

About

Ansible role for Red Hat 7 CIS Baseline

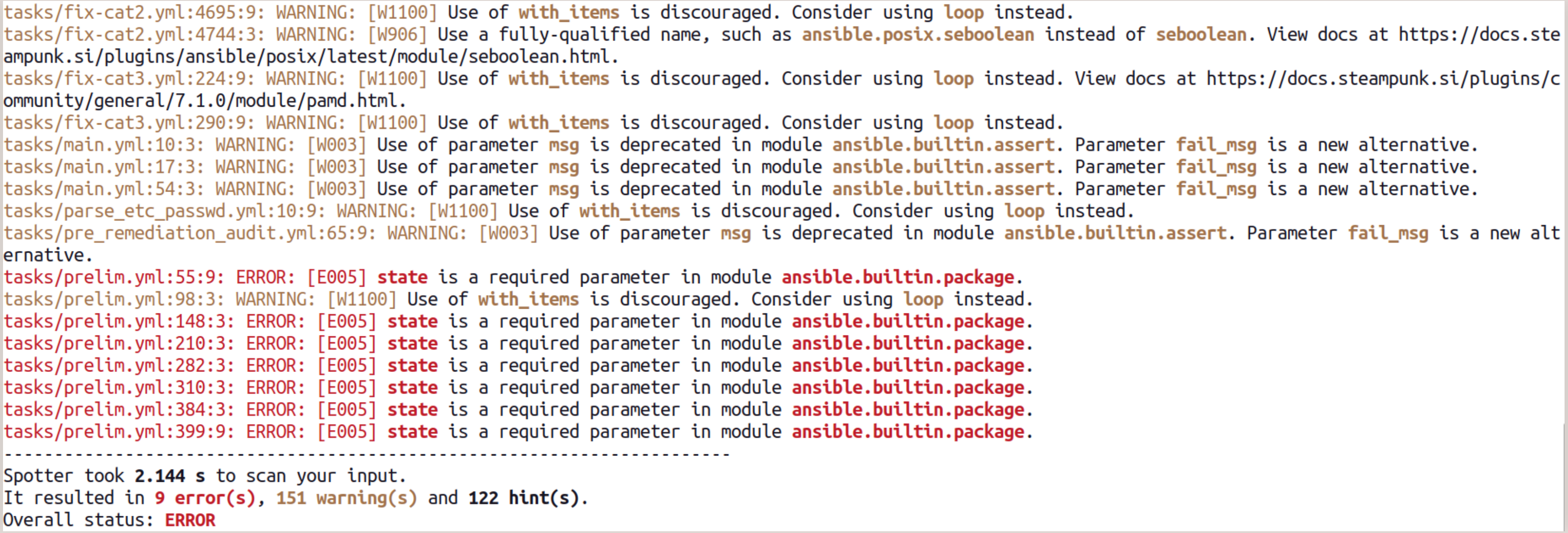
ansible-lockdown.readthedocs.io/en/la…

security benchmark cis redhat ansible-role rhel7 hardening security-hardening benchmark-framework redhat7 security-automation security-tools cis-benchmark compliance-as-code compliance-automation redhat-ansible

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



```
tasks/fix-cat2.yml:4695:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/fix-cat2.yml:4744:3: WARNING: [W906] Use a fully-qualified name, such as ansible.posix.seboolean instead of seboolean. View docs at https://docs.ste
ampunk.si/plugins/ansible/posix/latest/module/seboolean.html.
tasks/fix-cat3.yml:224:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead. View docs at https://docs.steampunk.si/plugins/c
ommunity/general/7.1.0/module/pamd.html.
tasks/fix-cat3.yml:290:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/main.yml:10:3: WARNING: [W003] Use of parameter msg is deprecated in module ansible.builtin.assert. Parameter fail_msg is a new alternative.
tasks/main.yml:17:3: WARNING: [W003] Use of parameter msg is deprecated in module ansible.builtin.assert. Parameter fail_msg is a new alternative.
tasks/main.yml:54:3: WARNING: [W003] Use of parameter msg is deprecated in module ansible.builtin.assert. Parameter fail_msg is a new alternative.
tasks/parse_etc_passwd.yml:10:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/pre_remediation_audit.yml:65:9: WARNING: [W003] Use of parameter msg is deprecated in module ansible.builtin.assert. Parameter fail_msg is a new alt
ernative.
tasks/prelim.yml:55:9: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:98:3: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/prelim.yml:148:3: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:210:3: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:282:3: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:310:3: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:384:3: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
tasks/prelim.yml:399:9: ERROR: [E005] state is a required parameter in module ansible.builtin.package.
------------------------------------------------------------------------
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

Fixing errors

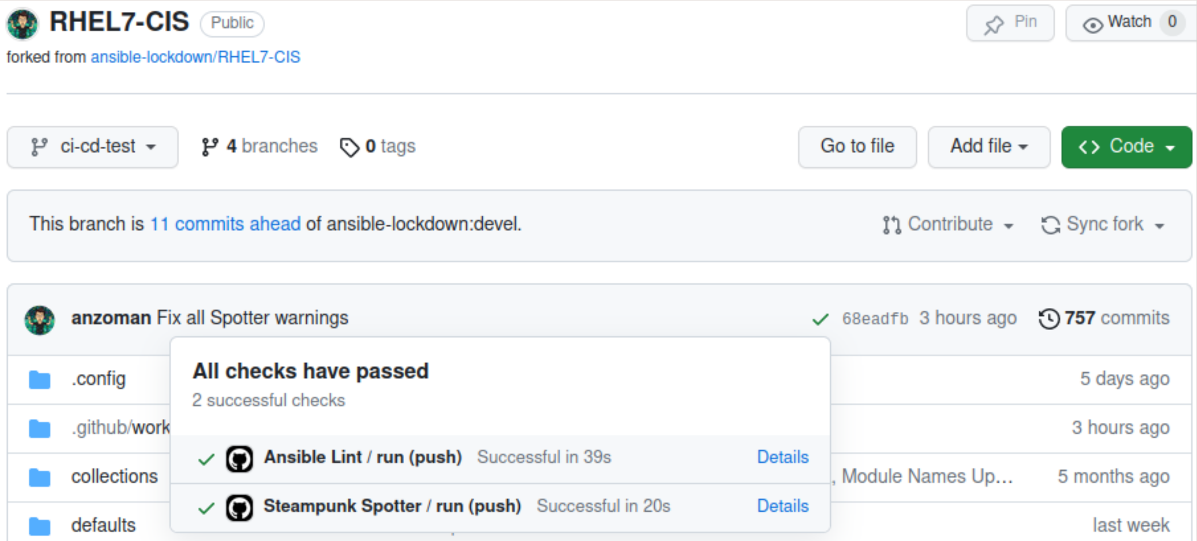
Fixing errors in projects from Ansible Lockdown (with Steampunk Spotter):

- https://github.com/ansible-lockdown/RHEL7-CIS/pull/321
- https://github.com/ansible-lockdown/UBUNTU22-CIS/pull/72
- https://github.com/ansible-lockdown/Windows-2016-CIS/pull/37
- https://github.com/ansible-lockdown/RHEL7-STIG/pull/437
- 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



RHEL7-CIS Public

forked from ansible-lockdown/RHEL7-CIS

This branch is 11 commits ahead of ansible-lockdown:devel.

anzoman Fix all Spotter warnings ✓ 68eadfb 3 hours ago 757 commits

.config		5 days ago
.github/work		3 hours ago
collections	, Module Names Up...	5 months ago
defaults		last week

All checks have passed

2 successful checks

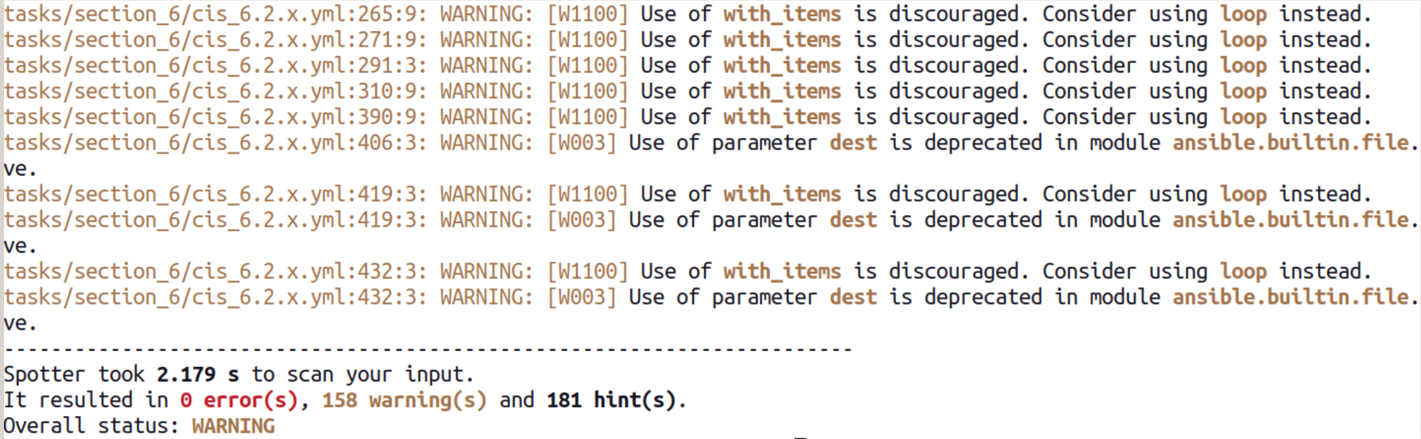
✓ **Ansible Lint / run (push)**	Successful in 39s	Details
✓ **Steampunk Spotter / run (push)**	Successful in 20s	Details

XLAB Steampunk

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)**

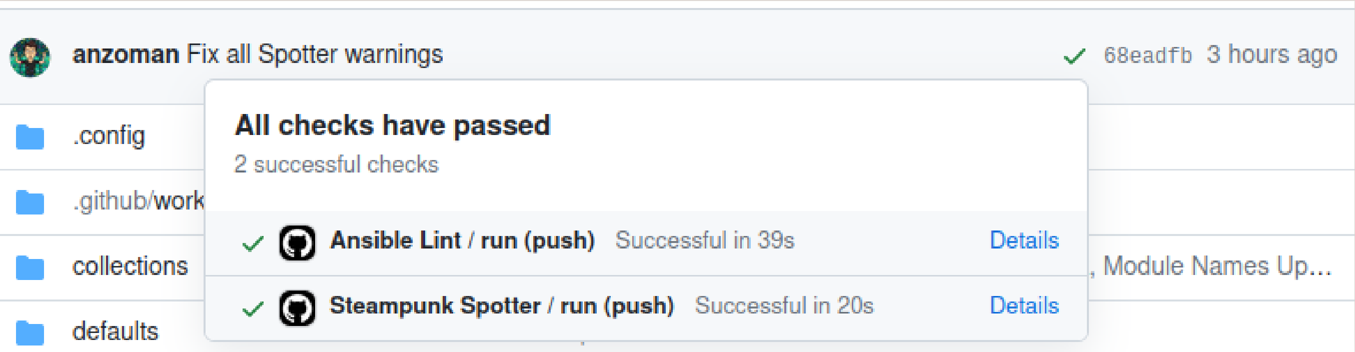


```
tasks/section_6/cis_6.2.x.yml:265:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:271:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:291:3: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:310:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:390:9: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:406:3: WARNING: [W003] Use of parameter dest is deprecated in module ansible.builtin.file.
ve.
tasks/section_6/cis_6.2.x.yml:419:3: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:419:3: WARNING: [W003] Use of parameter dest is deprecated in module ansible.builtin.file.
ve.
tasks/section_6/cis_6.2.x.yml:432:3: WARNING: [W1100] Use of with_items is discouraged. Consider using loop instead.
tasks/section_6/cis_6.2.x.yml:432:3: WARNING: [W003] Use of parameter dest is deprecated in module ansible.builtin.file.
ve.
------------------------------------------------------------------------
Spotter took 2.179 s to scan your input.
It resulted in 0 error(s), 158 warning(s) and 181 hint(s).
Overall status: WARNING
```

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)**



anzoman Fix all Spotter warnings ✓ 68eadfb 3 hours ago

.config

.github/work

collections

defaults

, Module Names Up...

All checks have passed

2 successful checks

✓ **Ansible Lint / run (push)** Successful in 39s Details

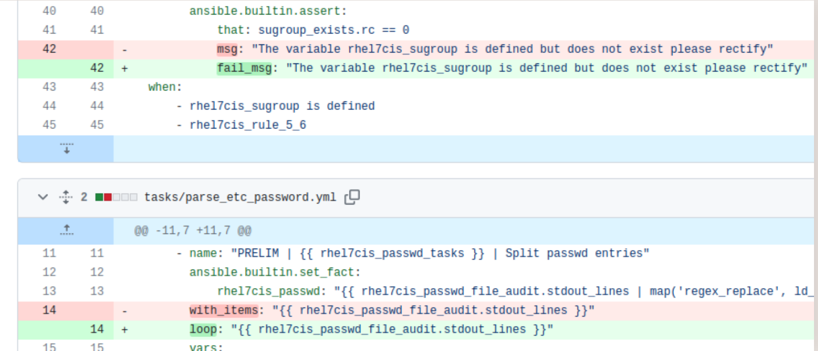
✓ **Steampunk Spotter / run (push)** Successful in 20s Details

XLAB Steampunk

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**



```
            ansible.builtin.assert:
              that: sugroup_exists.rc == 0
-             msg: "The variable rhel7cis_sugroup is defined but does not exist please rectify"
+             fail_msg: "The variable rhel7cis_sugroup is defined but does not exist please rectify"
        when:
          - rhel7cis_sugroup is defined
          - rhel7cis_rule_5_6
```

2 tasks/parse_etc_password.yml

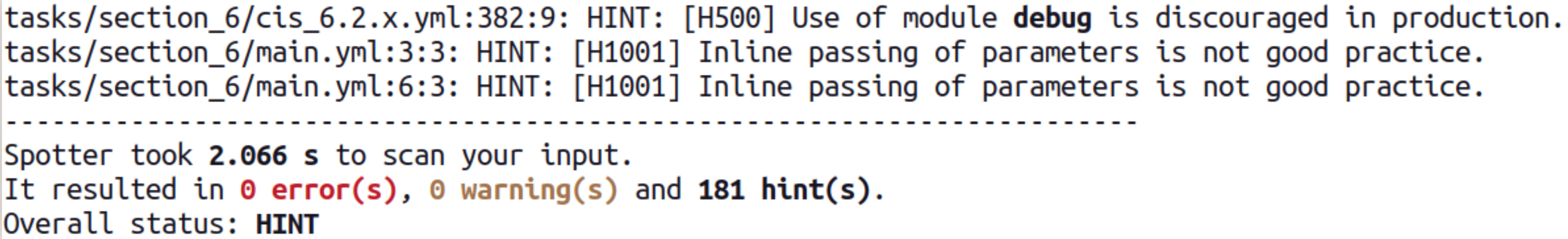
```
@@ -11,7 +11,7 @@
          - name: "PRELIM | {{ rhel7cis_passwd_tasks }} | Split passwd entries"
            ansible.builtin.set_fact:
              rhel7cis_passwd: "{{ rhel7cis_passwd_file_audit.stdout_lines | map('regex_replace', ld_
-           with_items: "{{ rhel7cis_passwd_file_audit.stdout_lines }}"
+           loop: "{{ rhel7cis_passwd_file_audit.stdout_lines }}"
            vars:
```

Ensuring trustable automation

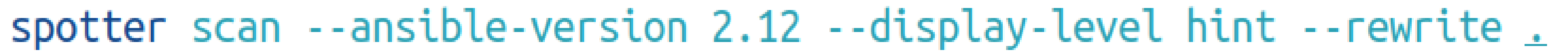
How can we establish QA on public open-source projects:

- 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**

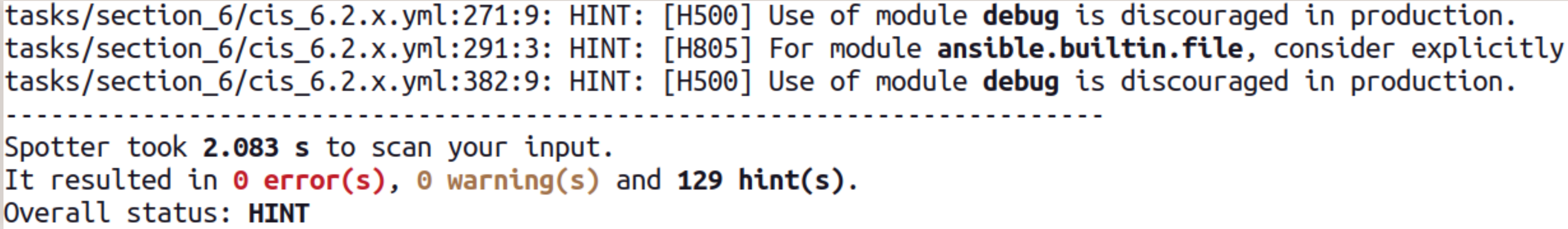
Ensuring trustable automation



```
tasks/section_6/cis_6.2.x.yml:382:9: HINT: [H500] Use of module debug is discouraged in production.
tasks/section_6/main.yml:3:3: HINT: [H1001] Inline passing of parameters is not good practice.
tasks/section_6/main.yml:6:3: 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
```

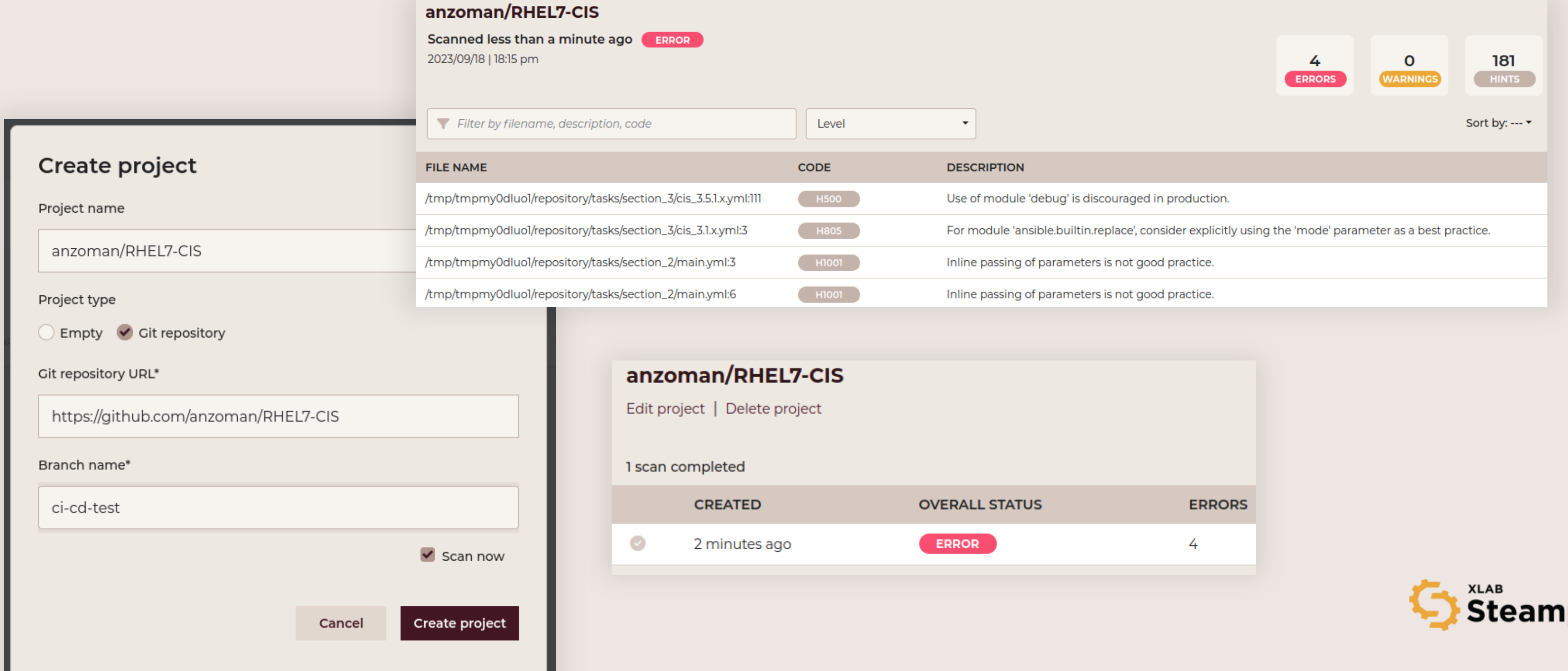


```
spotter scan --ansible-version 2.12 --display-level hint --rewrite .
```



```
tasks/section_6/cis_6.2.x.yml:271:9: HINT: [H500] Use of module debug is discouraged in production.
tasks/section_6/cis_6.2.x.yml:291:3: HINT: [H805] For module ansible.builtin.file, consider explicitly
tasks/section_6/cis_6.2.x.yml:382:9: HINT: [H500] Use of module debug is discouraged in production.
----------------------------------------------------------------------
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



Create project

Project name

anzoman/RHEL7-CIS

Project type

○ Empty ● Git repository

Git repository URL*

https://github.com/anzoman/RHEL7-CIS

Branch name*

ci-cd-test

☑ Scan now

anzoman/RHEL7-CIS

Scanned less than a minute ago ERROR

2023/09/18 | 18:15 pm

4 ERRORS | 0 WARNINGS | 181 HINTS

FILE NAME	CODE	DESCRIPTION
/tmp/tmpmy0dluo1/repository/tasks/section_3/cis_3.5.1.x.yml:111	H500	Use of module 'debug' is discouraged in production.
/tmp/tmpmy0dluo1/repository/tasks/section_3/cis_3.1.x.yml:3	H805	For module 'ansible.builtin.replace', consider explicitly using the 'mode' parameter as a best practice.
/tmp/tmpmy0dluo1/repository/tasks/section_2/main.yml:3	H1001	Inline passing of parameters is not good practice.
/tmp/tmpmy0dluo1/repository/tasks/section_2/main.yml:6	H1001	Inline passing of parameters is not good practice.

anzoman/RHEL7-CIS

1 scan completed

	CREATED	OVERALL STATUS	ERRORS
✓	2 minutes ago	ERROR	4

XLAB Steampunk

Ensuring trustable automation

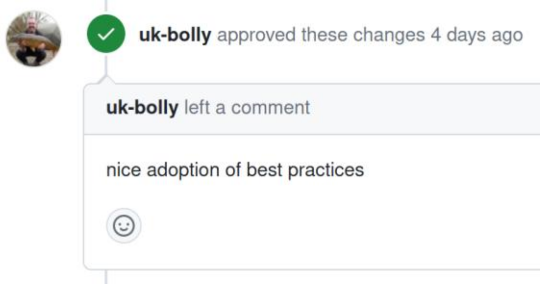
How can we establish QA on public open-source projects:

- 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



uk-bolly approved these changes 4 days ago

uk-bolly left a comment

nice adoption of best practices

Process (gathering ecosystem of tools)

Spread the word!

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

XLAB Steampunk

Steampunk Spotter

Visit our page

steampunk.si/spotter

Join the Ansible Challenge

steampunk.si/ansible-challenge

Talk to us

Nejc Slabe
nejc.slabe@xlab.si

Anže Luzar
anze.luzar@xlab.si

Follow us