

How to write better playbooks: a “quick” deep dive

Sean Cavanaugh

Senior Principal Technical Marketing

Manager

Red Hat Ansible

@IPvSean



Agenda

- Separate connection vars from hostvars
- Avoid conditionals!
- Treat role tasks files like ACLs
- Avoid Blocks unless you are using rescues
- Use ansible-lint!
 - Force you to use name field
 - Force you to breakup long blocks of text



1 Separate connection vars from hostvars

```
1 ---
2 # Define host-specific variables for the switch
3 hostvars:
4   - cisco_switch:
5     - # General device information
6     - hostname: "Switch01"
7     - ios_version: "15.2(2)E5"
8     - management_ip: "192.168.1.1"
9     - domain_name: "example.com"
10    - timezone: "UTC"
11
12    - # Login credentials (make sure to use vault or encrypted values for production)
13    - ansible_user: "admin"
14    - ansible_password: "admin_password"
15    - ansible_become: yes
16    - ansible_become_method: enable
17    - ansible_become_password: "enable_password"
18
19    - # Interface configurations
20    - interfaces:
21      - - name: "GigabitEthernet0/1"
22        - description: "Uplink to Core Switch"
23        - ip_address: "10.0.0.1"
24        - subnet_mask: "255.255.255.0"
25        - speed: "1000"
26        - duplex: "full"
27
28      - - name: "GigabitEthernet0/2"
29        - description: "Server Connection"
30        - ip_address: "10.0.1.1"
31        - subnet_mask: "255.255.255.0"
32        - speed: "1000"
33        - duplex: "full"
34
35    - # VLAN configurations
36    - vlans:
37      - - id: 10
38        - name: "Management"
```

Vars can be:

1) How do I connect to the network device
e.g. SSH, netconf, yang, httpapi (e.g. nx-api)

2) What do I configure?
e.g. OSPF config, VLANs, ACLs

3) Info about the switch
e.g. software version, operational state,
hardware status



1 Separate connection vars from hostvars

```
[cisco]
rtr1 ansible_host=18.220.156.59
rtr2 ansible_host=18.221.53.11
rtr4 ansible_host=3.16.82.231
rtr3 ansible_host=13.59.242.237
```

Host variables apply to the host
and override group vars

```
[cisco:vars]
ansible_user=andriusb
ansible_network_os=ios
ansible_connection=network_cli
```

Group variables apply for all devices in that
group



2

Avoid conditionals!

```
- name: Ensure VLANs are configured for Cisco IOS
  cisco.ios.ios_vlans:
    config: "{{vlan_config}}"
    when: ansible_network_os == 'cisco.ios'

- name: Ensure VLANs are configured for Cisco NXOS
  cisco.nxos.nxos_vlans:
    config: "{{vlan_config}}"
    when: ansible_network_os == 'cisco.nxos'

- name: Ensure VLANs are configured for Cisco IOS-XR
  cisco.iosxr.iosxr_vlans:
    config: "{{vlan_config}}"
    when: ansible_network_os == 'cisco.iosxr'
```



2 Avoid conditionals!

Ansible Tasks Schema - Ansible tasks file (ansible.json)

```
- name: Configure VLANs
  ansible.builtin.include_tasks: "{{ ansible_network_os }}.yaml"
```

```
▼ tasks
  ! ios.yml
  ! iosxr.yml
  ! main.yml
  ! nxos.yml
```



3

Treat role tasks files like ACLs

```
tasks
  > ami_find
  > instances
  > inventory
  > resources
  > security_includes
  ! attendance.yml
  ! automation_hub.yml
  ! check_prebuild_hub.yml
  ! check_prebuild.yml
  ! cluster_instances.yml
  ! cockpit_machines.yml
  ! create_inventory.yml
  ! main.yml
  ! provision.yml
  ! teardown.yml
```

```
control_node
  > defaults
  > files
  > meta
  tasks
    ! 10_aap_setup.yml
    ! 12_controller.yml
    ! 15_package_dependencies.yml
    ! 20_all_workshop.yml
    ! main.yml
```



4 Avoid Blocks unless you are using rescues

```
! Create_inventory.yml ! - name: attempt to download specified AAP from specified URL if we don't already have it
- name: attempt to download specified AAP from specified URL if we don't already have it
  when:
    - aap_download_url is defined
    - stat_var.stat.checksum | default("") != provided_sha_value
  block:
    - name: Do something here
      example.fake.task:
        dosomething: true
    - name: Do something second
      example.fake.task:
        dosomething: true
    - name: Do something Third
      example.fake.task:
        dosomething: true
```

```
- name: attempt to download specified AAP from specified URL if we don't already have it
  when:
    - aap_download_url is defined
    - stat_var.stat.checksum | default("") != provided_sha_value
  block:
    - name: Do something here
      example.fake.task:
        dosomething: true
    - name: Do something second
      example.fake.task:
        dosomething: true
    - name: Do something Third
      example.fake.task:
        dosomething: true
- name: attempt to download specified AAP from specified URL if we don't already have it
  when:
    - aap_download_url is defined
    - stat_var.stat.checksum | default("") != provided_sha_value
  block:
    - name: Do something here
      example.fake.task:
        dosomething: true
    - name: Do something second
      example.fake.task:
        dosomething: true
    - name: Do something Third
      example.fake.task:
        dosomething: true
- name: attempt to download specified AAP from specified URL if we don't already have it
  when:
    - aap_download_url is defined
    - stat_var.stat.checksum | default("") != provided_sha_value
  block:
    - name: Do something here
      example.fake.task:
        dosomething: true
    - name: Do something second
      example.fake.task:
        dosomething: true
```



4

Avoid Blocks unless you are using rescues

✓ - `name: attempt to download specified AAP from specified URL if we don't already have it`

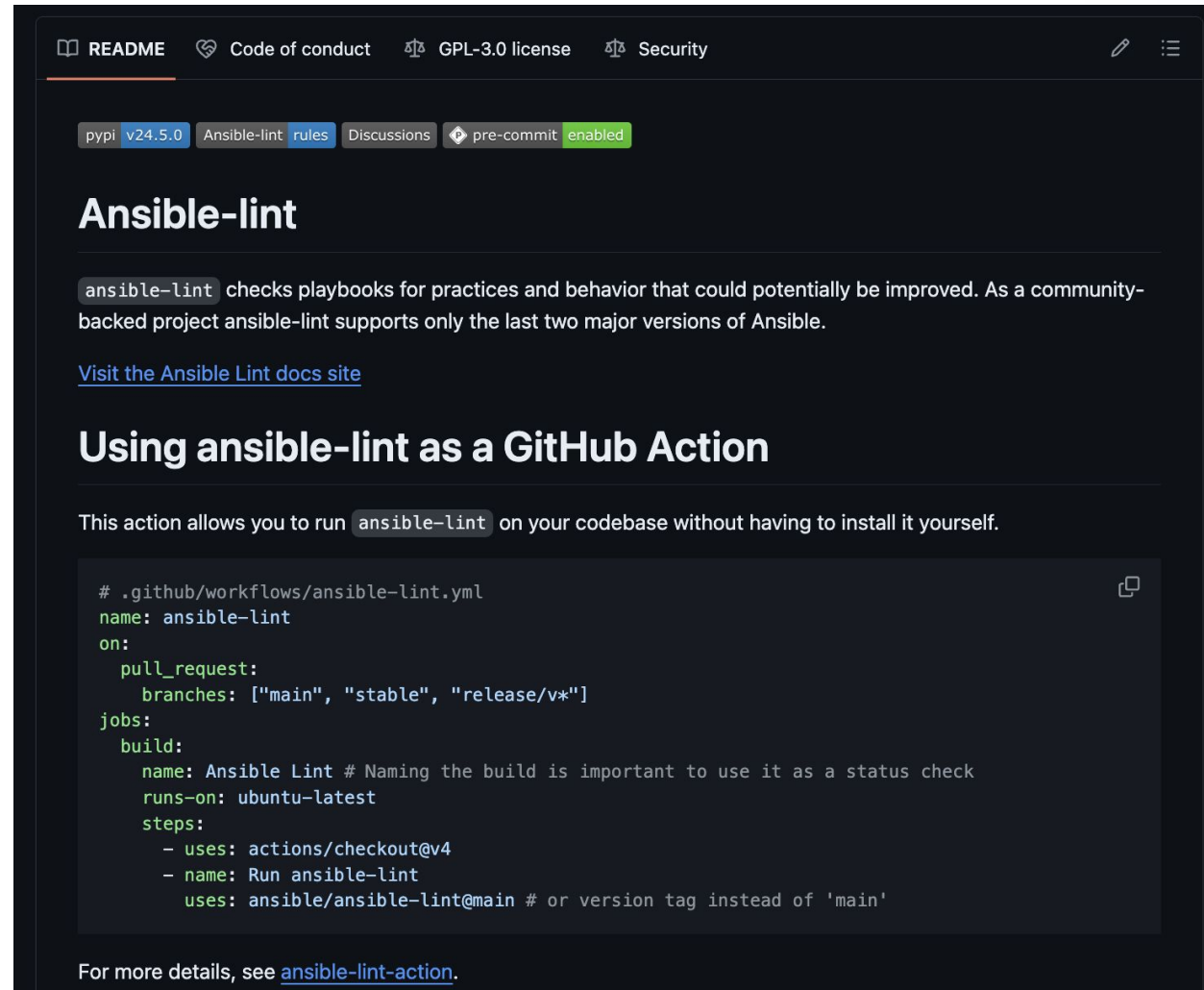
Click to collapse the range.

```
    - aap_download_url is defined
    - stat_var.stat.checksum | default("") != provided_sha_value
  include_tasks: 09_download_url.yml
```



5

Use ansible-lint!



The screenshot shows the GitHub repository page for `ansible-lint`. At the top, there are links for `README`, `Code of conduct`, `GPL-3.0 license`, and `Security`. Below these are tags for `pypi`, `v24.5.0`, `Ansible-lint`, `rules`, `Discussions`, `pre-commit`, and `enabled`. The main heading is `Ansible-lint`. The description states that `ansible-lint` checks playbooks for practices and behavior that could potentially be improved. It also mentions that as a community-backed project, it supports only the last two major versions of Ansible. A link to the `Ansible Lint docs site` is provided. The section `Using ansible-lint as a GitHub Action` explains that this action allows running `ansible-lint` on the codebase without manual installation. A code block shows a GitHub Actions workflow configuration for `ansible-lint`. The workflow is named `ansible-lint` and is triggered on pull requests to the `main`, `stable`, or `release/v*` branches. The job is named `build` and runs on `ubuntu-latest`. The steps include checking out the code and running `ansible-lint`.

`ansible-lint` checks playbooks for practices and behavior that could potentially be improved. As a community-backed project `ansible-lint` supports only the last two major versions of Ansible.

[Visit the Ansible Lint docs site](#)

Using ansible-lint as a GitHub Action

This action allows you to run `ansible-lint` on your codebase without having to install it yourself.

```
# .github/workflows/ansible-lint.yml
name: ansible-lint
on:
  pull_request:
    branches: ["main", "stable", "release/v*"]
jobs:
  build:
    name: Ansible Lint # Naming the build is important to use it as a status check
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - name: Run ansible-lint
        uses: ansible/ansible-lint@main # or version tag instead of 'main'
```

For more details, see [ansible-lint-action](#).



5a

Catching Non-Idempotent Tasks

```
... - name: Restart nginx
... | shell: systemctl restart nginx

... - name: Restart nginx service
... | service:
... |   name: nginx
... |   state: restarted
```



5b

Force you to breakup long blocks of text

```
---
- name: Configure banner on Cisco IOS switch with a super long line
  hosts: cisco_ios_switch
  gather_facts: no
  tasks:
    - name: Configure banner
      cisco.ios.ios_banner:
        banner: motd
        text: "Unauthorized access to this device is prohibited. All activities performed on this device are logged and monitored. Disconnect immediately if you are not an authorized user."
```

```
---
- name: Configure banner on Cisco IOS switch with broken up lines
  hosts: cisco_ios_switch
  gather_facts: no
  tasks:
    - name: Configure banner
      cisco.ios.ios_banner:
        banner: motd
        text: |
          Unauthorized access to this device is prohibited.
          All activities performed on this device are logged and monitored.
          Disconnect immediately if you are not an authorized user.
```





Q & A



Thank you!



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



x.com/RedHat