

# Where does your Ansible code come from?

Fabio Alessandro "Fale" Locati  
Principal Specialist Solutions Architect, Red Hat

# TOC

- The automation supply chain
- Securing the automation supply chain
- Conclusions

## About me

- Working in IT since 2004, mostly in consulting roles
- Ansible user since 2013
- Author of 5 books, 4 of which on Ansible
- Principal Specialist Solution Architect @ Red Hat

## Some disclaimers

- This presentation wants to be a primer, not a full security course
- Everything discussed today is **open source**
- There will be many links in the slides
- A QR-Code to the slides is present at the end of the presentation

# Supply chain attack

A software supply chain attack refers to a malicious activity that targets the sourcing, development, distribution, or deployment of the code.

## Why care about supply chain attack?

- Can have a devastating impact on organizations
- Can be very difficult to detect
- Are difficult to defend against
- Can affect non-intended targets
- Are becoming increasingly common!

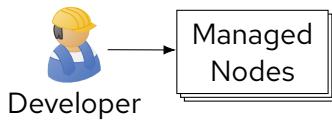
## Why should WE care about supply chain attack?

- Ansible code often runs with elevated privileges
- A lot of Ansible code supply chains are *not very secure*
- Often, the Ansible supply chains are *not even appropriately mapped*

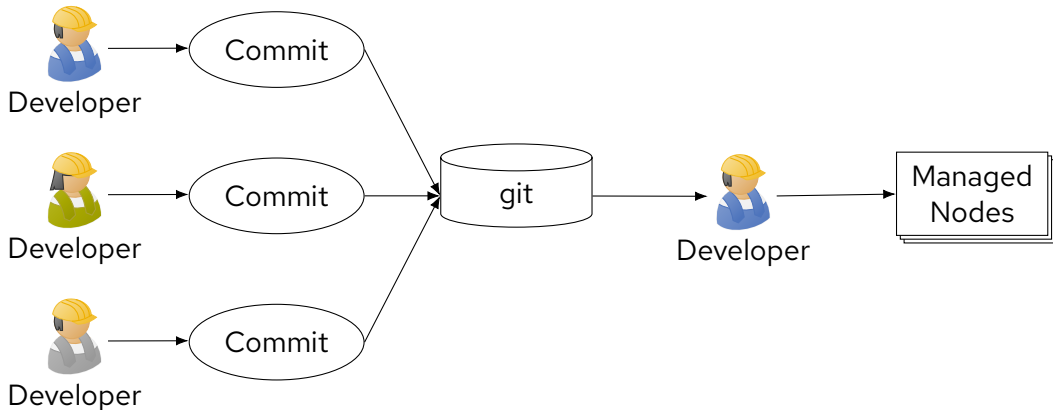
# The automation supply chain



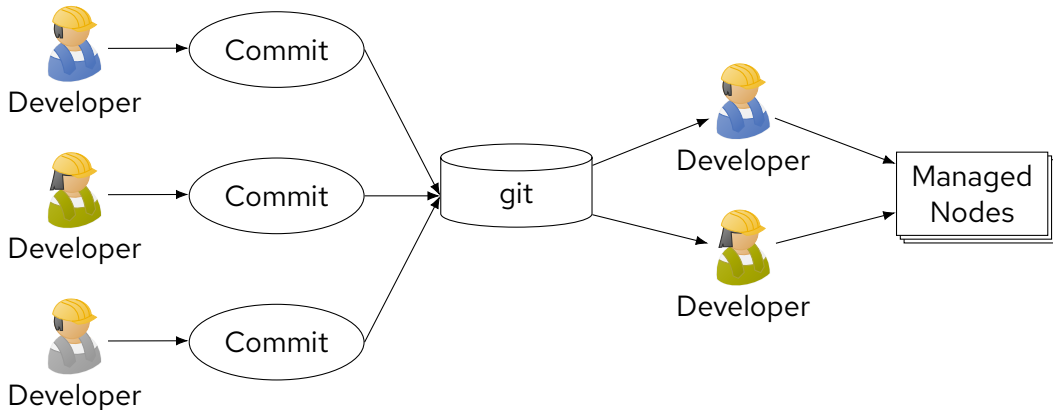
## The initial automation workflow



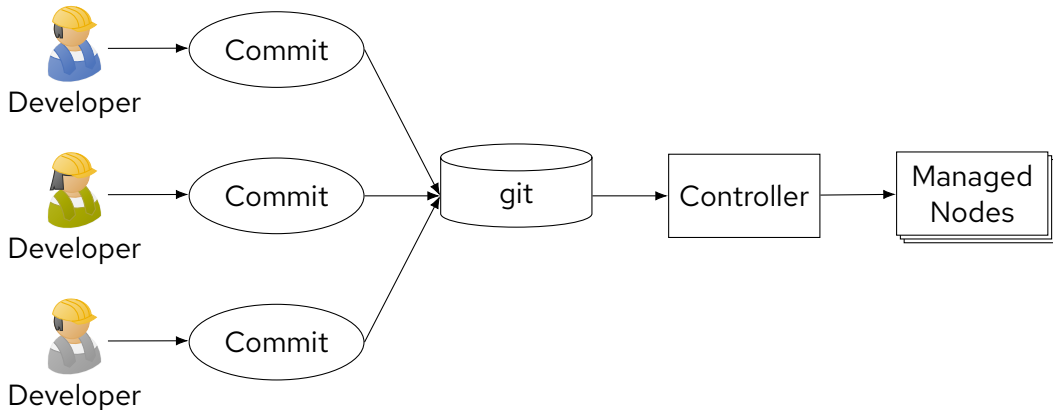
## A more scalable automation workflow



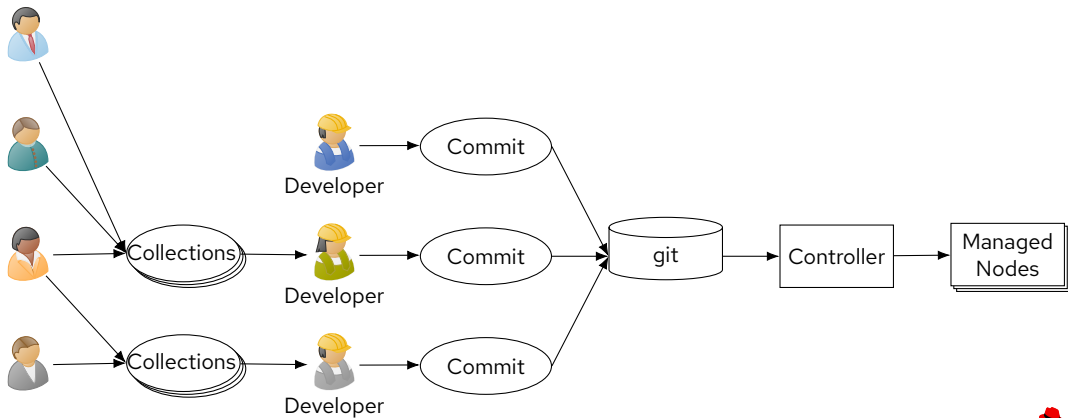
## A more scalable automation workflow



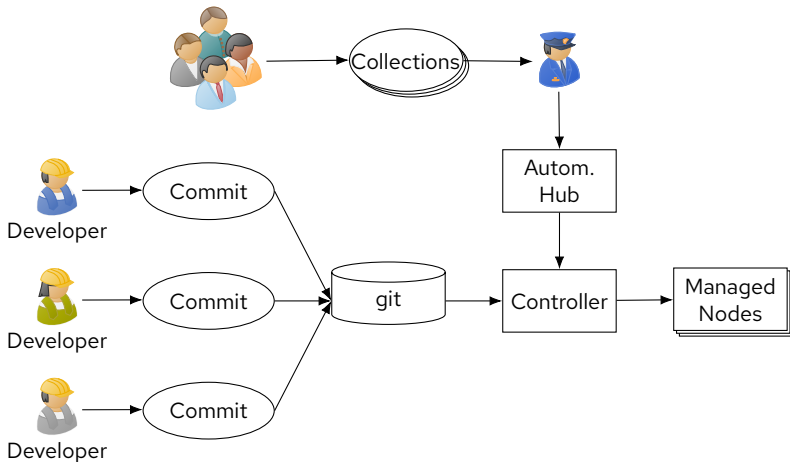
## A more scalable automation workflow



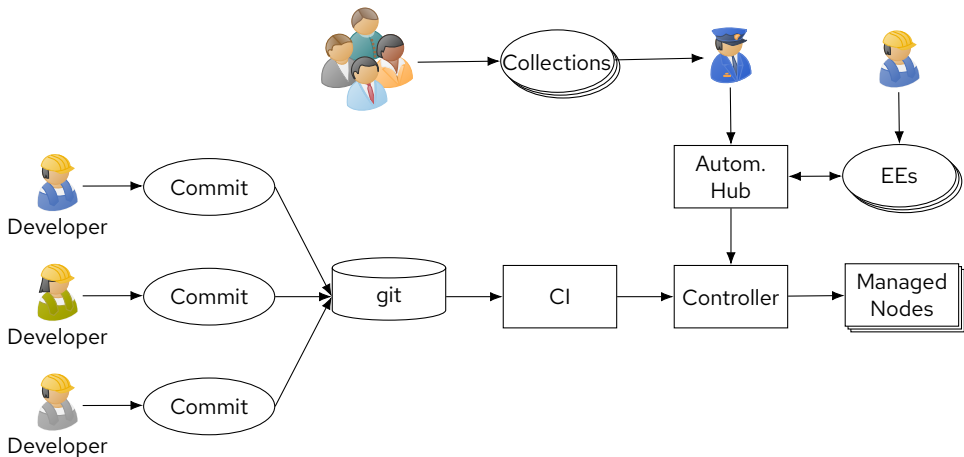
## A more scalable automation workflow



## A better structured workflow



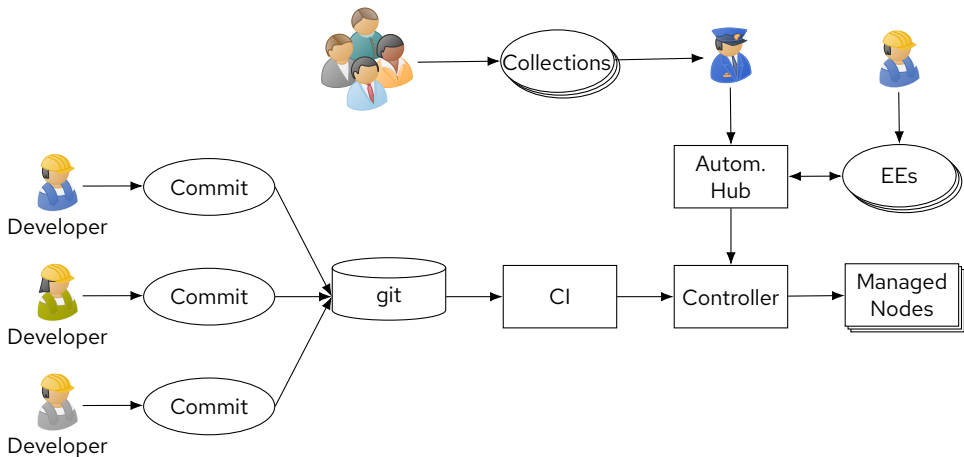
## A better structured workflow



# Securing the automation supply chain



## Our automation workflow



## Sign git commits

- `git commit -S -m "YOUR COMMIT MESSAGE"`

More details at:

- <https://git-scm.com/book/en/v2/Git-Tools-Signing-Your-Work>

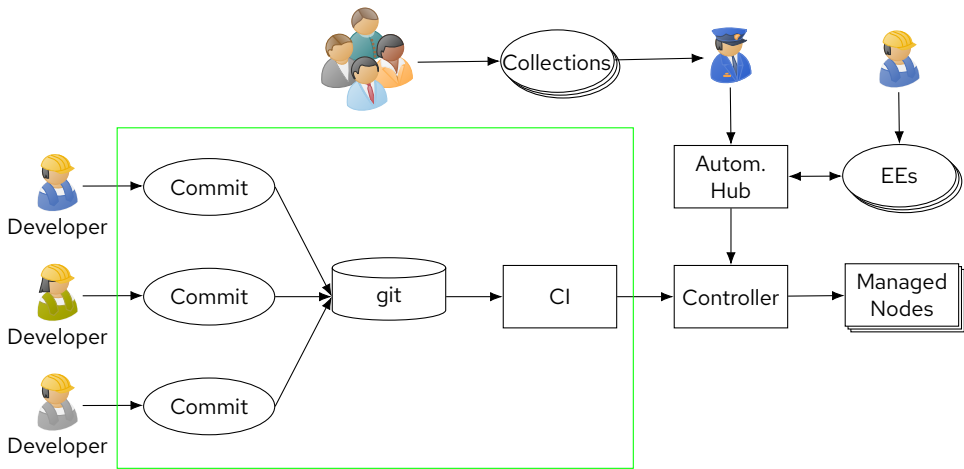
# Validate signed git commits

- `git verify-commit <commit>`

More details at:

- <https://git-scm.com/docs/git-verify-commit>

## Our automation workflow



# Ansible project signature

- `ansible-sign project gpg-sign .`

More details at:

- <https://docs.ansible.com/automation-controller/latest/html/userguide/project-sign.html>

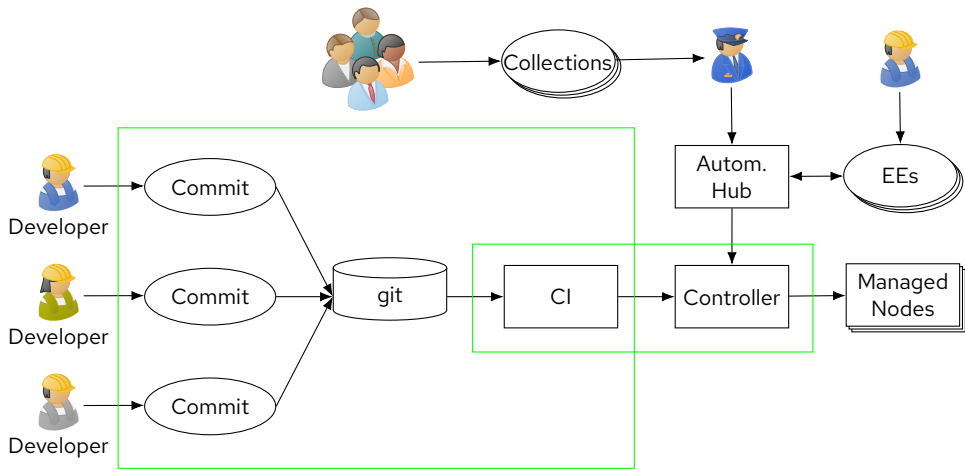
# Ansible project validation

- Manually
  - `ansible-sign project gpg-verify .`
- Via AWX/AAC UI

More details at:

- <https://docs.ansible.com/automation-controller/latest/html/userguide/project-sign.html>

## Our automation workflow



## Ansible collections signature

- Manually

- `gpg --quiet --batch --pinentry-mode loopback --yes --detach-sign --default-key KEY_ID --armor --output MANIFEST.json.asc MANIFEST.json`

- (Manually) via GalaxyNG/PAH UI

- (Automatically) via GalaxyNG/PAH at collection approval stage

- Import previous signature via GalaxyNG/PAH

More details at:

- [https://ansible.readthedocs.io/projects/galaxy-ng/en/latest/config/collection\\_signing/](https://ansible.readthedocs.io/projects/galaxy-ng/en/latest/config/collection_signing/)



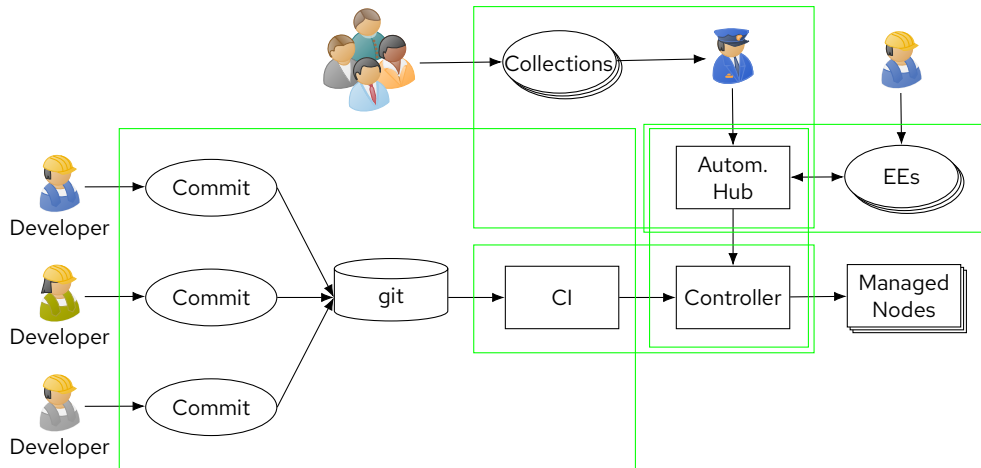
## Ansible collections validation

- Via ansible-galaxy
  - `ansible-galaxy collection verify <name>`
- Via ansible-build
  - `ansible-builder create --galaxy-keyring=<path to pubring>`
- (Automatically) via AWX/AAC

More details at:

- `https://docs.ansible.com/ansible/devel/collections_guide/collections_verifying.html`
- `https://www.ansible.com/blog/crank-up-your-automation-with-ansible-validated-content`

# Our automation workflow



## Ansible EE signature

- Manually via Skopeo
  - `skopeo standalone-sign <manifest-file> <image name> <fingerprint> --output <path>`
- Manually via Podman
  - `podman push --sign-by <email> <galaxy-ng host>`
- (Manually) via GalaxyNG/PAH UI
- (Automatically) via GalaxyNG/PAH when images are pushed

More details at:

- [https://ansible.readthedocs.io/projects/galaxy-ng/en/latest/config/container\\_signing/](https://ansible.readthedocs.io/projects/galaxy-ng/en/latest/config/container_signing/)
- <https://github.com/containers/skopeo/blob/main/docs/skopeo-standalone-sign.1.md>
- [https://github.com/containers/podman/blob/main/docs/tutorials/image\\_signing.md](https://github.com/containers/podman/blob/main/docs/tutorials/image_signing.md)
- [https://docs.pulpproject.org/pulp\\_container/workflows/sign-images.html](https://docs.pulpproject.org/pulp_container/workflows/sign-images.html)

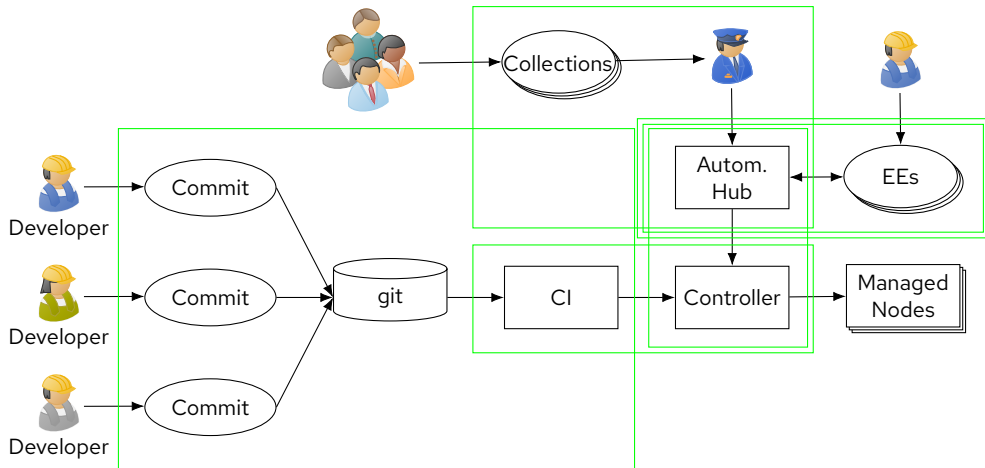
## Ansible EE validation

- Podman/Docker container policy

More details at:

- <https://github.com/containers/image/blob/main/docs/containers-policy.json.5.md>

## Our automation workflow



# Conclusions

## Wrapping up

- Automation can be a very interesting target for supply chain attacks
- Automation supply chains tend to be long and complex
- It is critical to map your automation supply chain
- There are many tools that can help you securing your supply chain!

# Questions?

**Email:** [fale@redhat.com](mailto:fale@redhat.com)  
**Fediverse:** [@fale@fale.io](https://fale.fale.io)





# Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.



[linkedin.com/company/red-hat](https://www.linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://www.youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://www.facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)