Red Hat Summit

Connect

You Shall Not Pass!

Schutz von Ansible-Inhalten

Red Hat

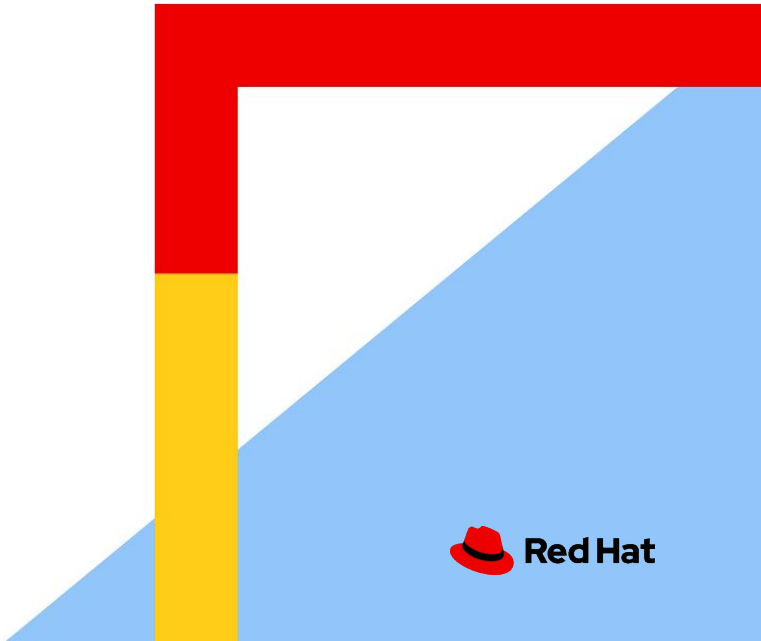
Dr. Jason Breitweg

Senior Ansible Technical Account Manager
Red Hat

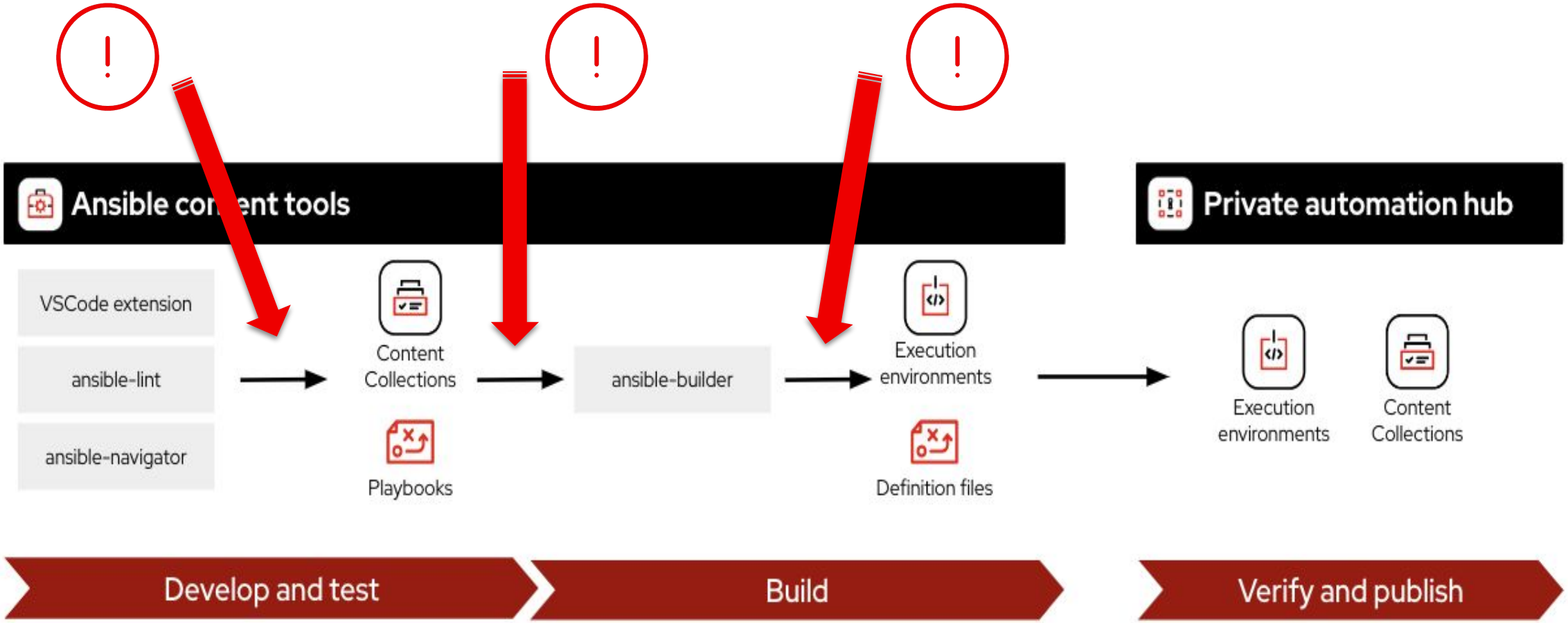
Red Hat

What we'll discuss today

- Supply chain attack vectors
- Deeper look into Ansible Content signing
- Ansible Content Collection signing
- Execution Environment signing
- Project signing and verification

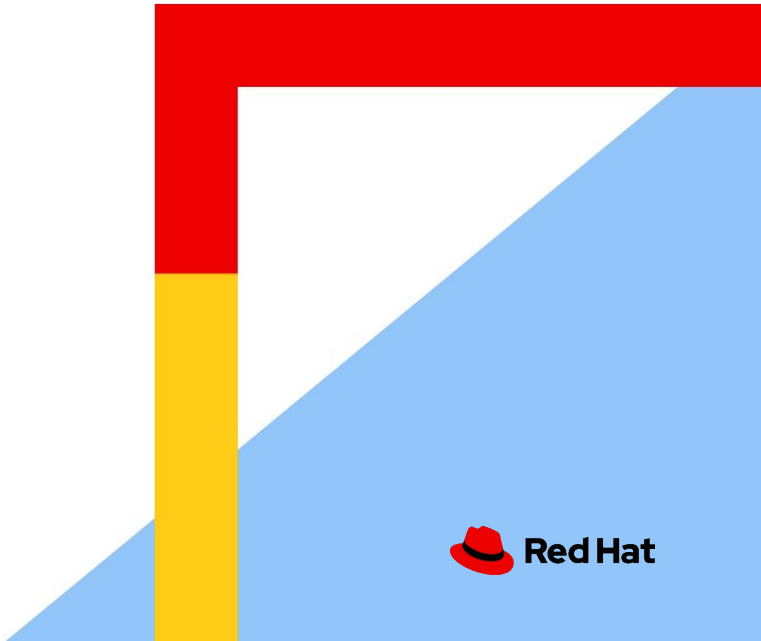


Possible supply chain attack vectors for automation



Red Hat

A deeper look into Ansible content signing



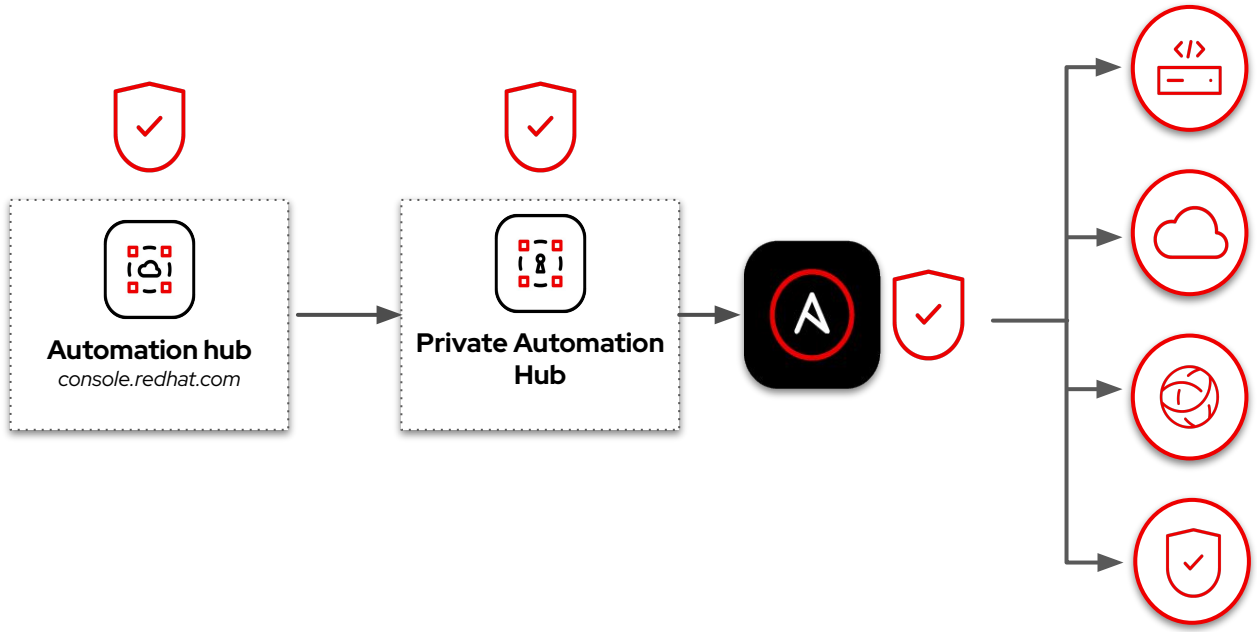
Chain of custody features

Automation hub and Red Hat Ansible Certified Content

Red Hat Ansible Certified Content is digitally signed to ensure data integrity and verify content ownership

Private automation hub

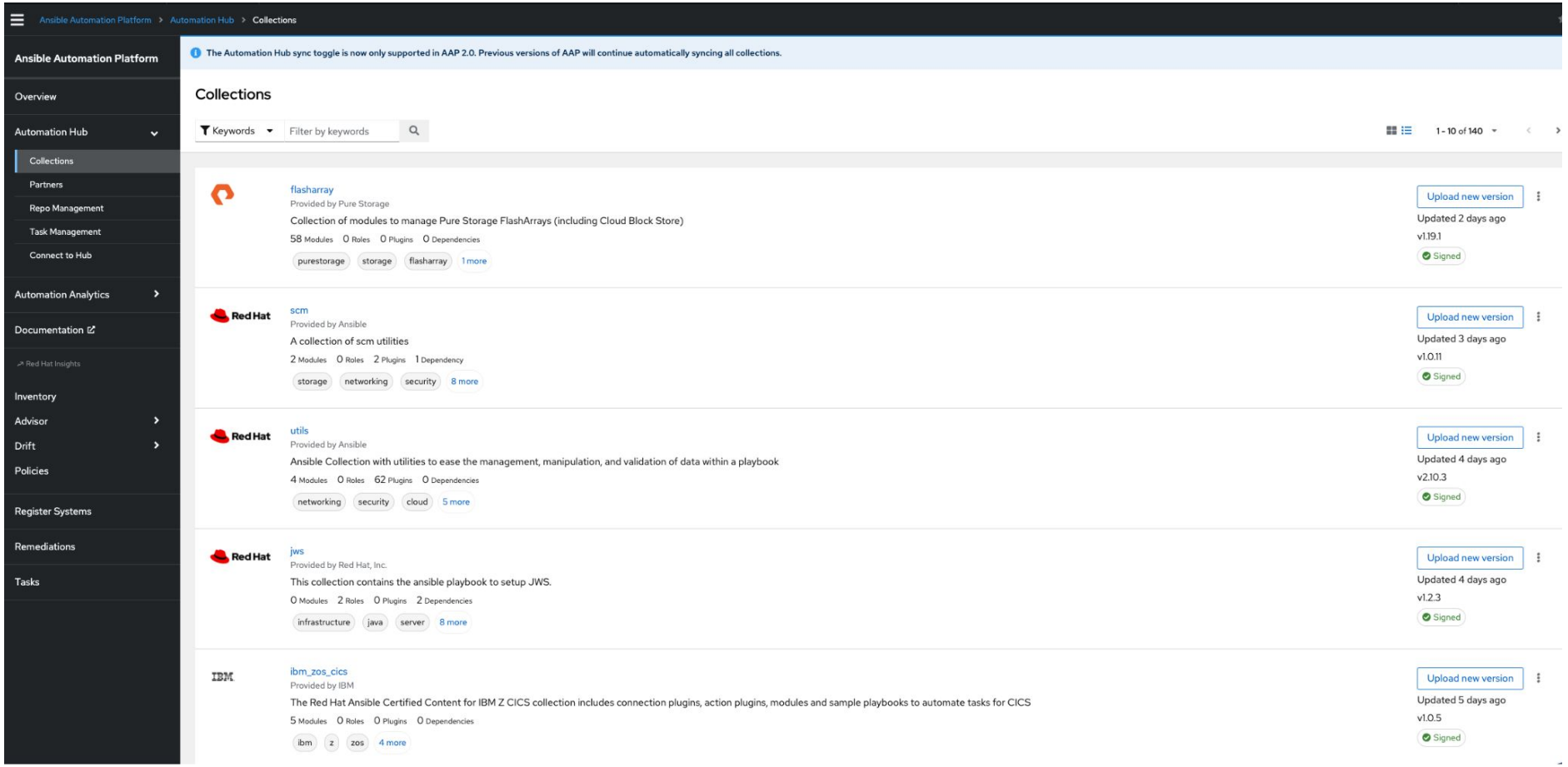
Sign user-built or third-party Ansible Content Collections when publishing to your private automation hub instance



Red Hat

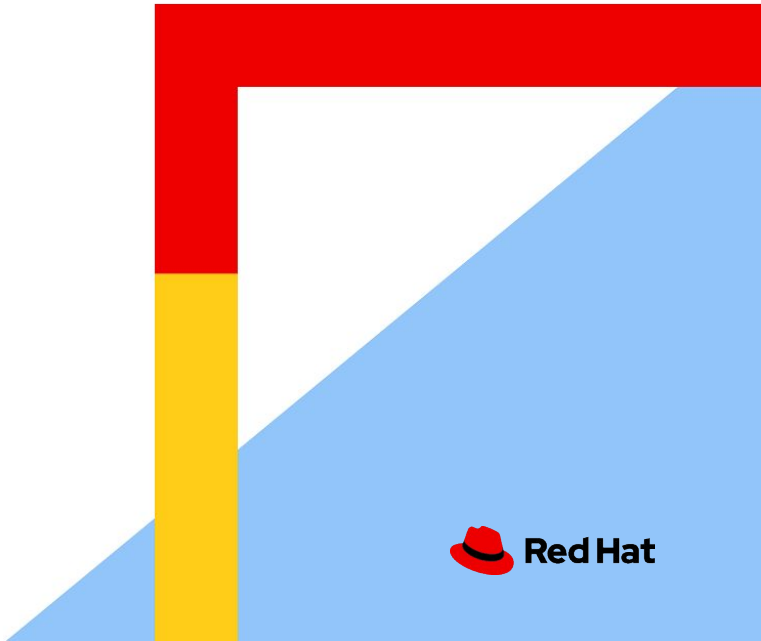
Signed and certified Ansible Content Collections

console.redhat.com/ansible/automation-hub



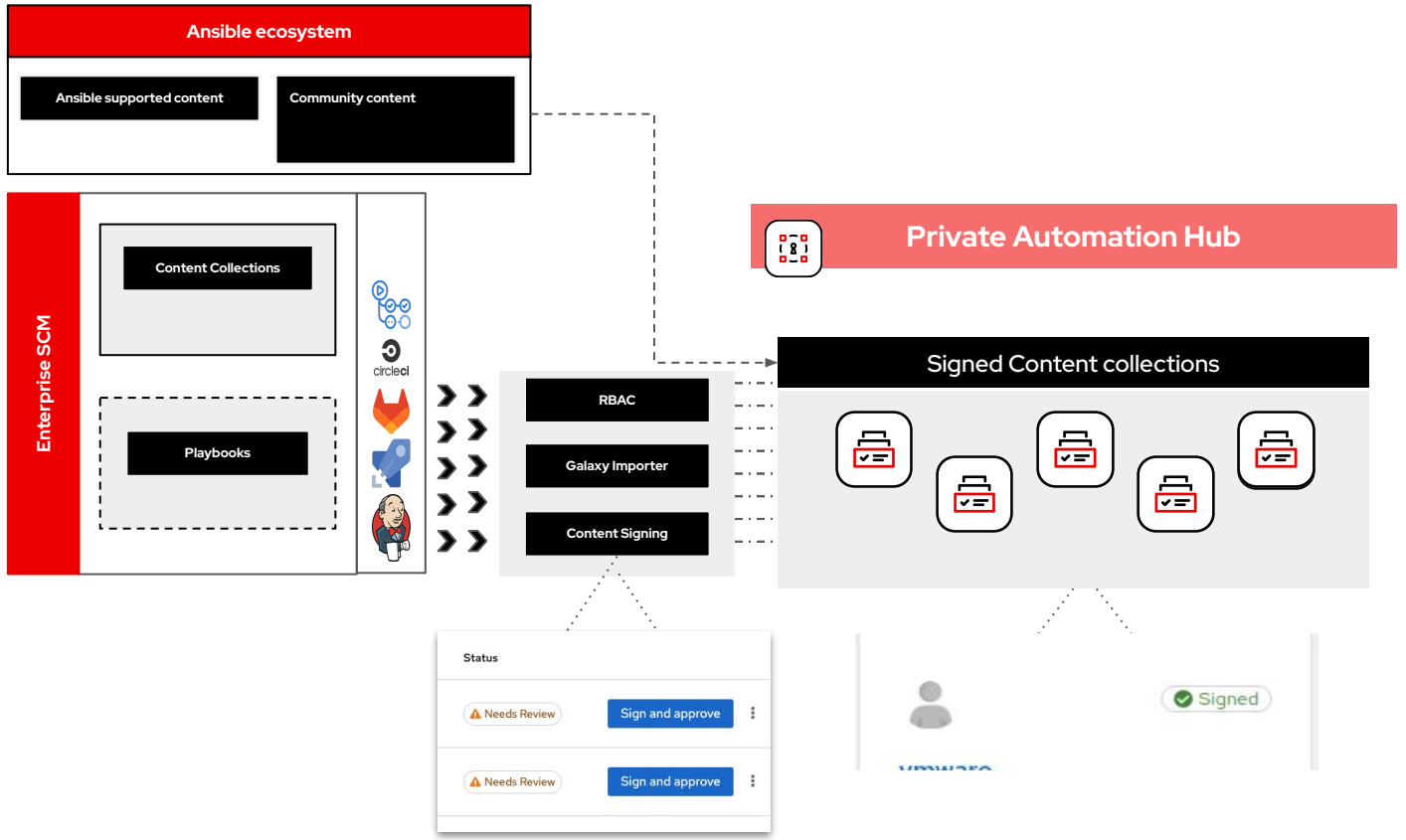
Red Hat

Ansible Content Collection signing



Signing Ansible Content Collections

- Private Automation Hub is the library of content for your organization
- It can be enabled to sign collections on upload through a signing service
- Upload Ansible Content Collections to Private Automation Hub using GUI or ansible-galaxy CLI



Red Hat

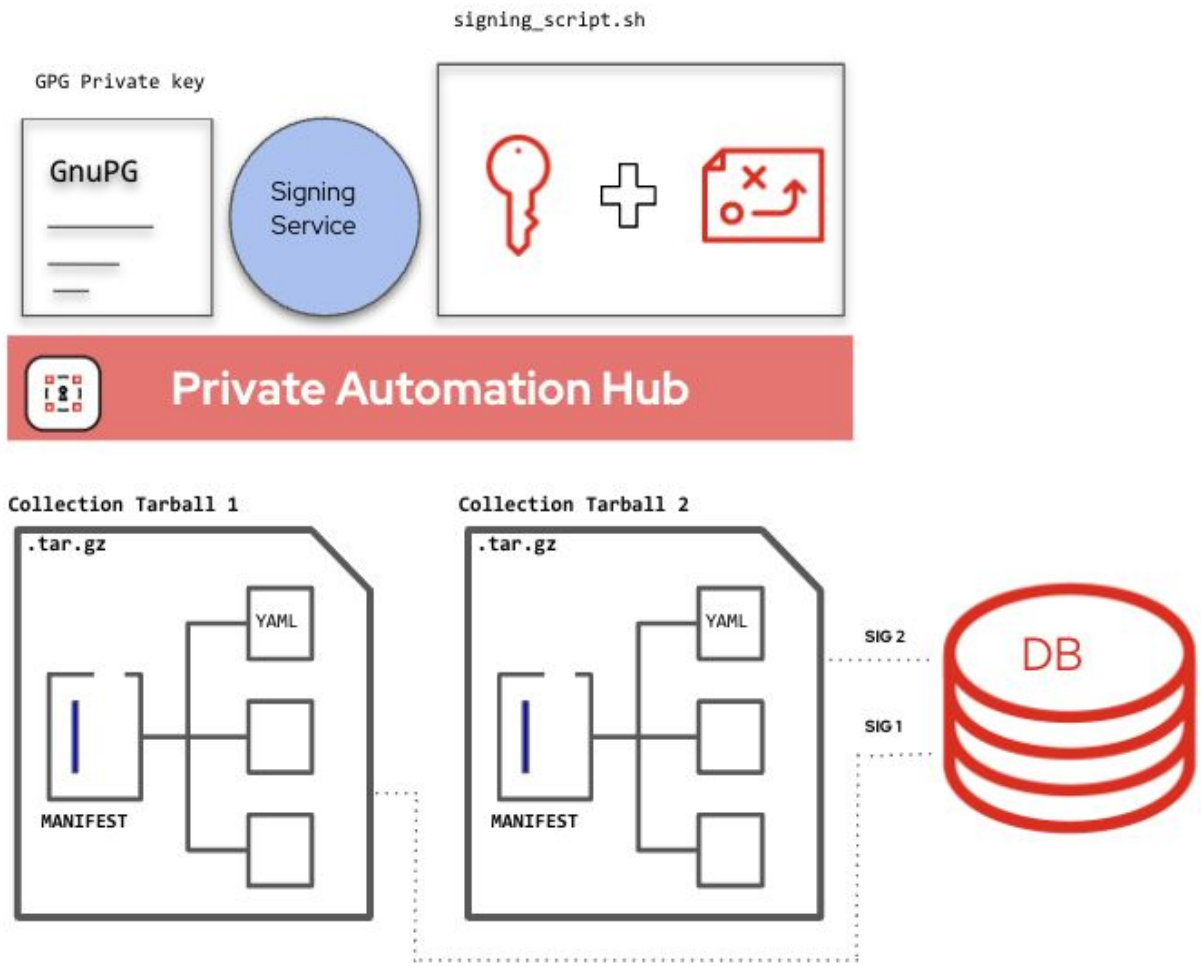
Install Ansible Automation Hub with signing enabled

- Provide the path to the GnuPG private key
- Provide the path to the signing script
- Enable signing related options

Red Hat

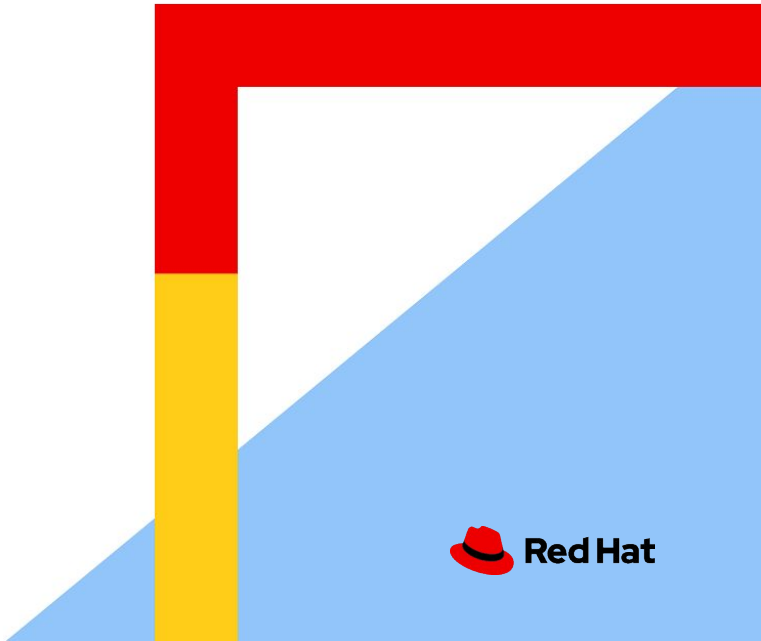
Collection signing service

- Signing in Automation Hub is based on GPG
- Signing service holds the GPG key and the signing script
- Signing service performs signing on collection manifest and stores the signatures in the Automation Hub database for each collection



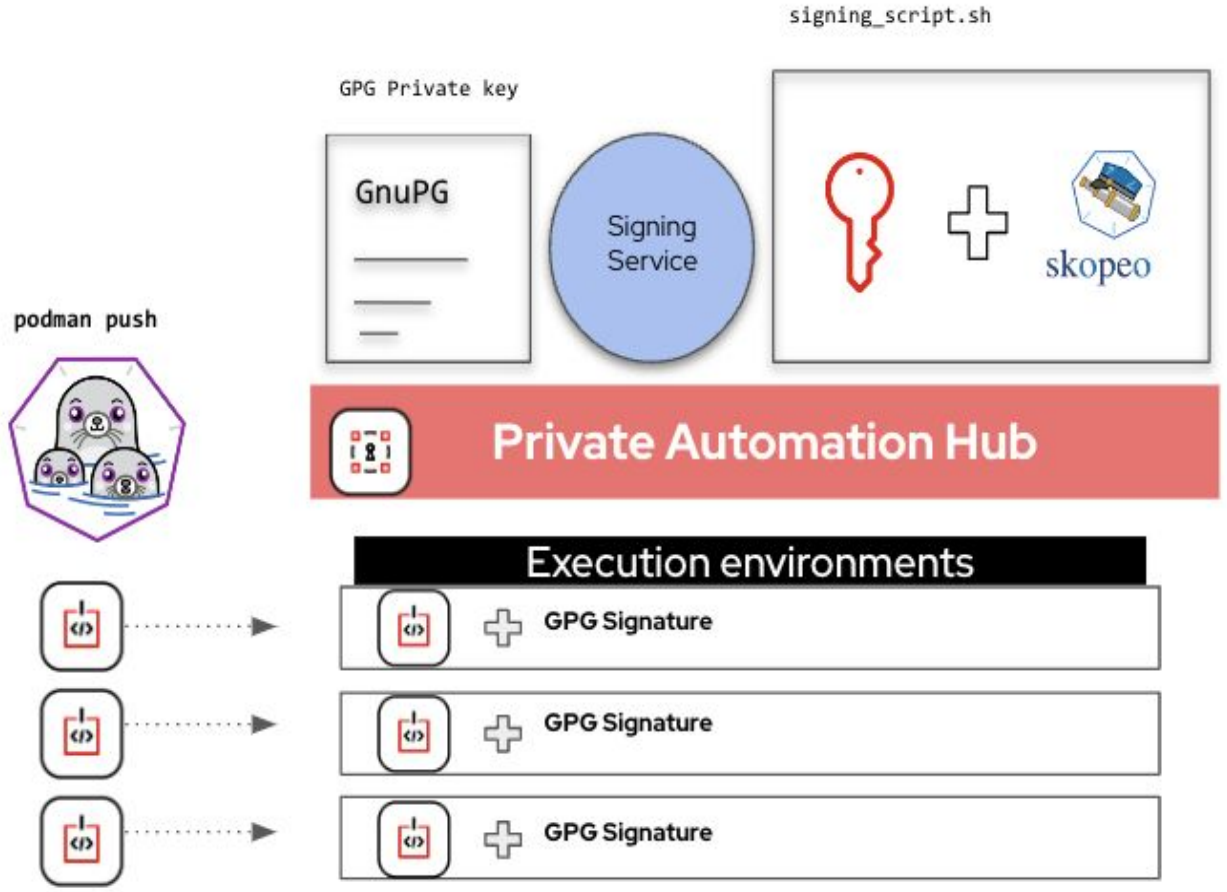
Red Hat

Execution Environment signing



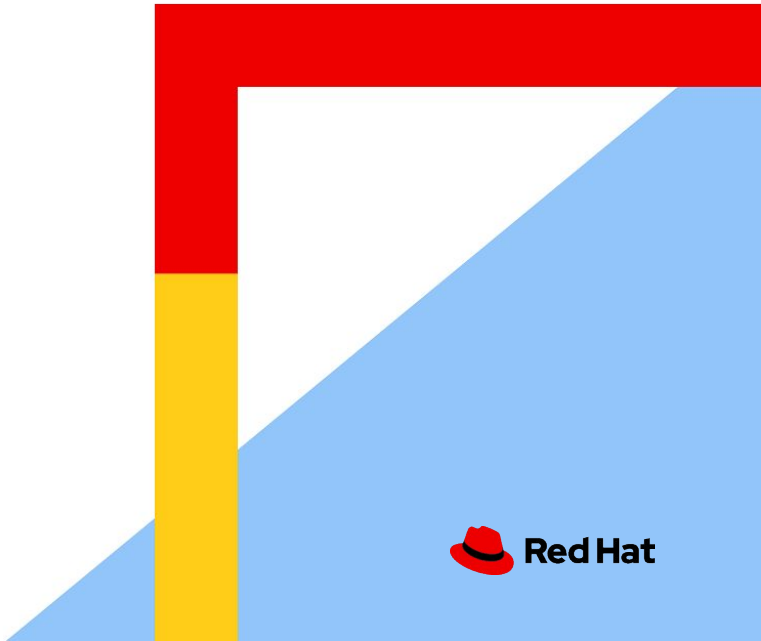
Execution Environment signing service

- Signing in Automation Hub is based on GPG
- Signing service holds the GPG key and the signing script
- Signing service performs signing on execution environment/container image and adds the signature to the image itself

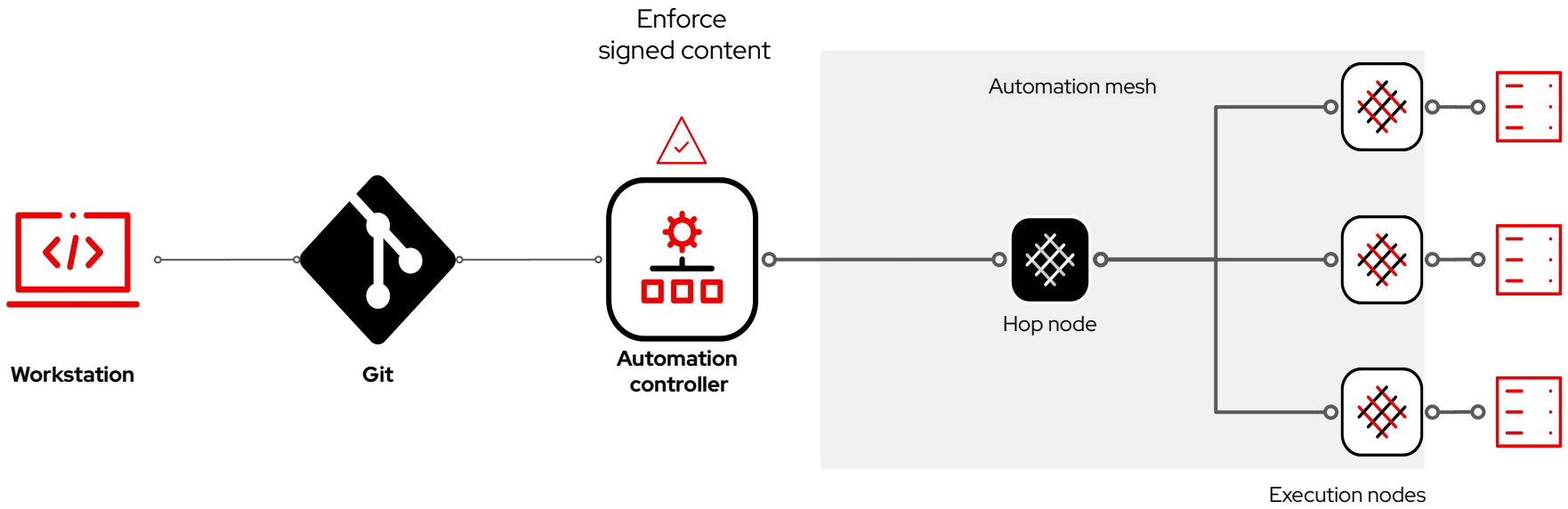


Red Hat

Project signing and verification in Automation Controller



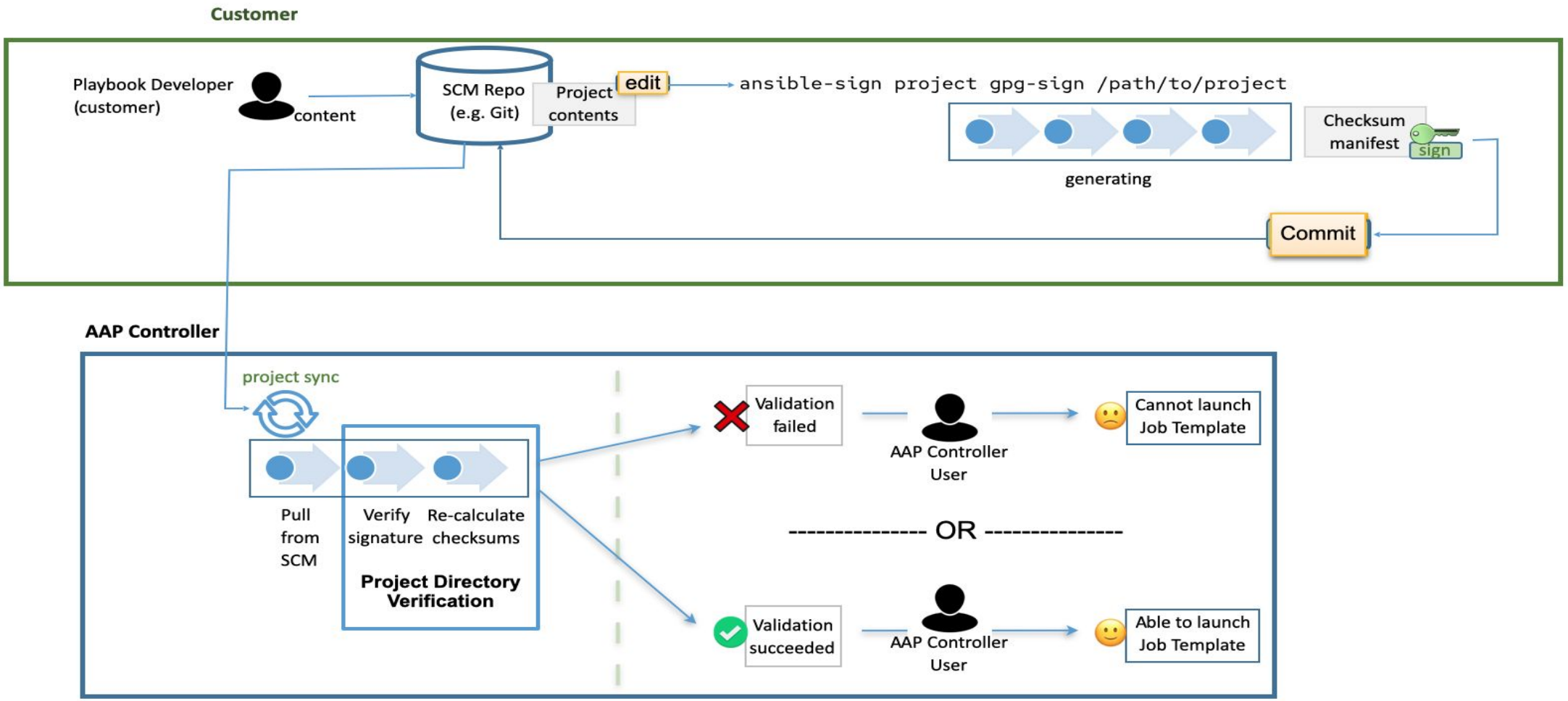
Project signing in six steps



1. Create GPG key pair
2. Create an ASC file (armored ASCII)
3. Create a MANIFEST.in for your Git project
4. Use `ansible-sign` utility to create signature for the project
5. Create a GPG credential in Automation Controller
6. Sync Project (will be enforced!)

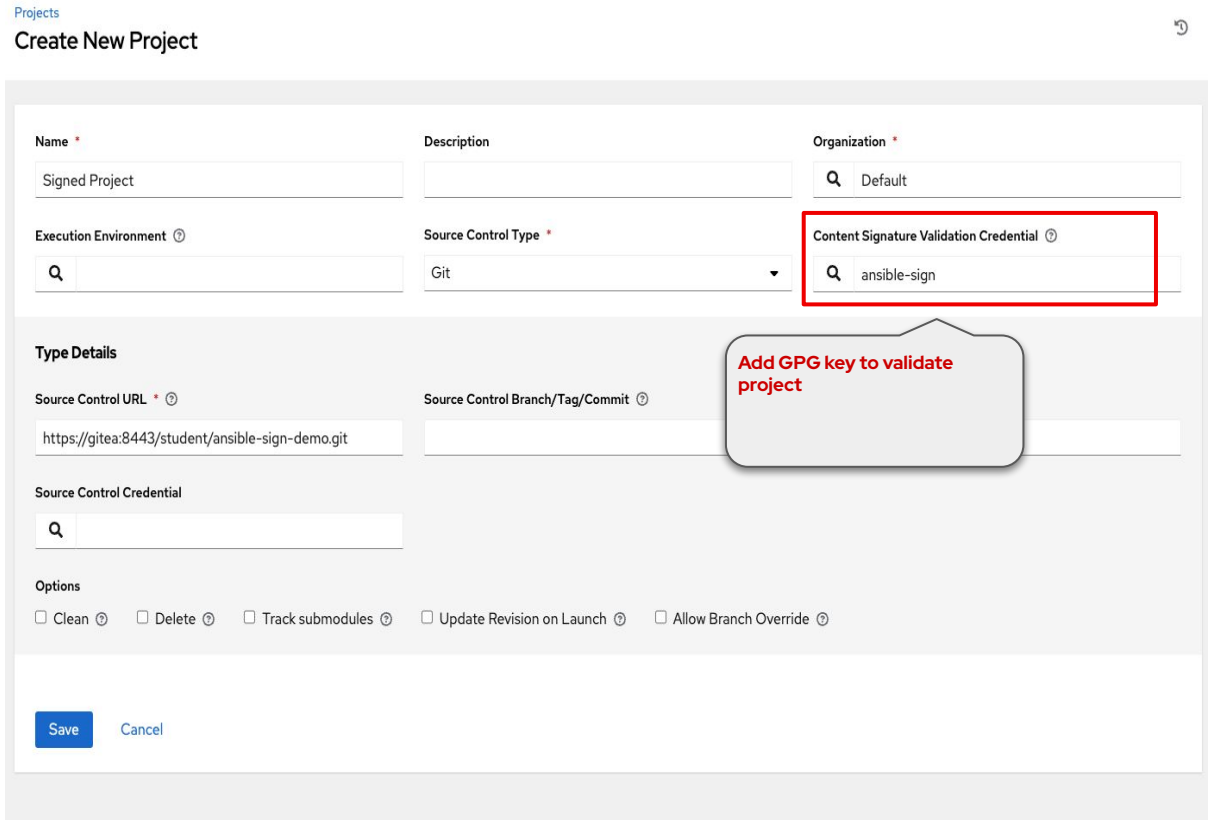
Red Hat

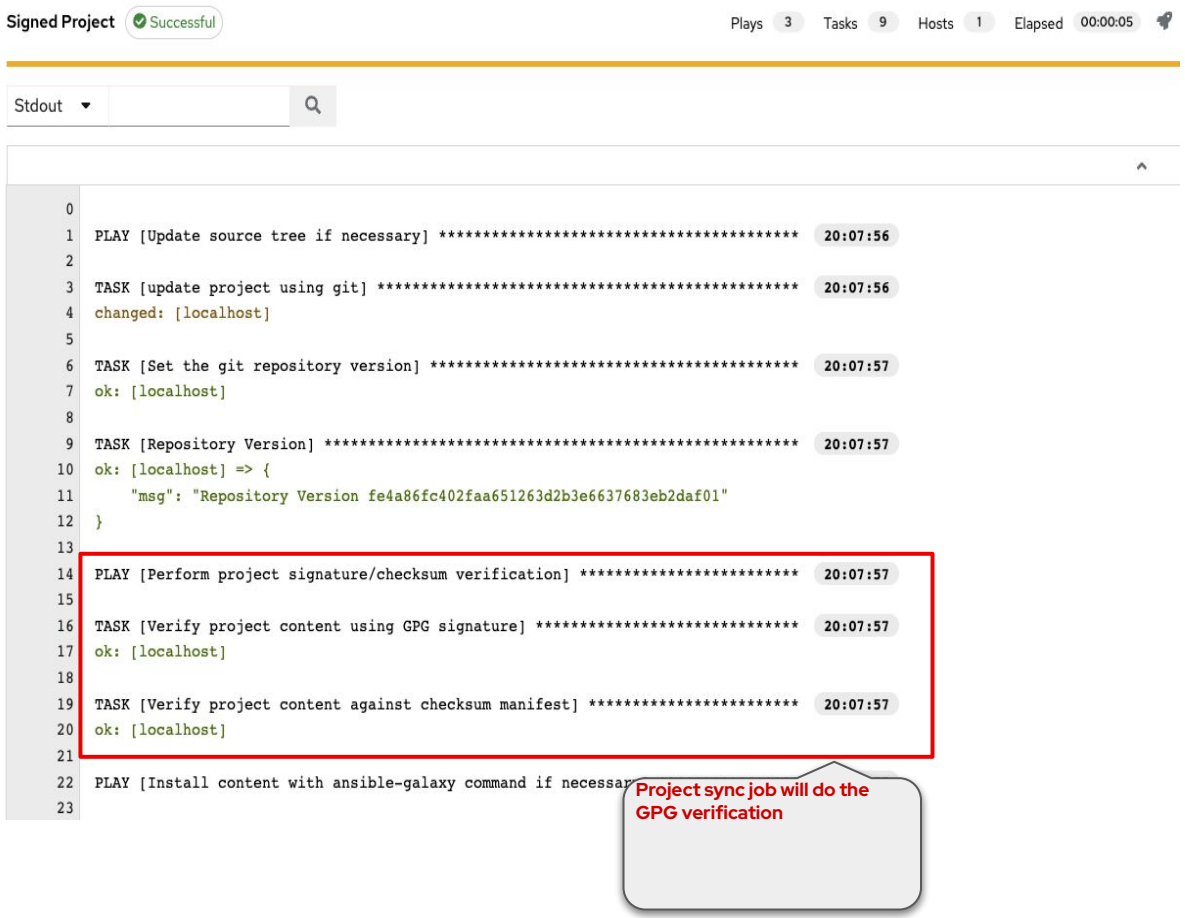
Project signing workflow



Red Hat

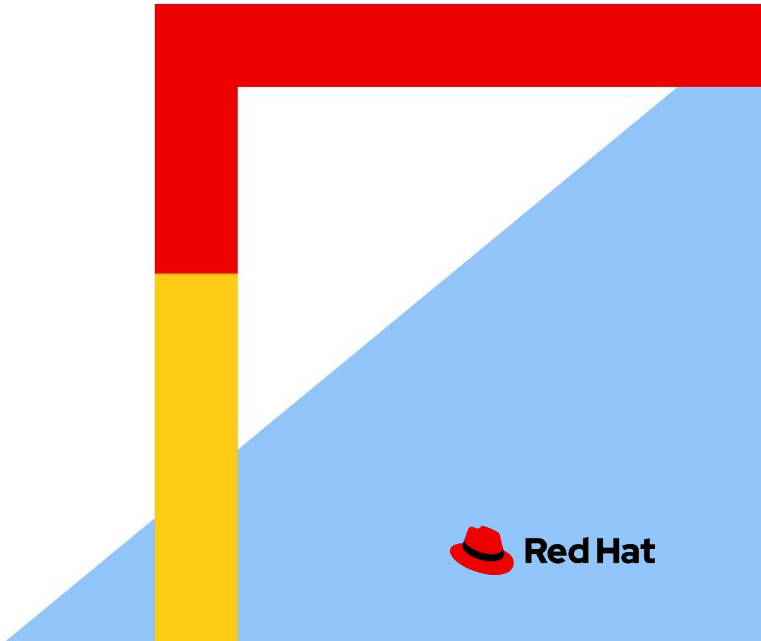
Project signing in Automation Controller





Red Hat

Resources



- **Self-paced Labs**
  - Signing in Private Automation Hub
  - Project signing in automation controller

- **Blogs**
  - Digitally signing Ansible Content Collections using private automation hub
  - Project signing and verification

- **Documentation**
  - Collections and content signing in private automation hub
  - Project Signing and Verification
  - Image Signature Verification

Session: 17:25 - 17:55

Jetzt Session bewerten!

Einfach QR-Code scannen, Session wählen und bewerten.
Vielen Dank!

red.ht/rhsc24-de-s8

Red Hat

Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat