Ansible Policy as Code

Ein Blick in die (nahe) Zukunft

Computacenter

$ whoami

Tim Grützmacher

Senior Consultant

@ Computacenter since 2016

- started in Big Data - Hadoop
  - Big Data needs Automation
- 6+ years in DevOps & Automation
- Puppet, Terraform, but mostly Ansible
- Contributor to ansible-builder and multiple Ansible Collections

AAP gets bigger

IaC, CaC and now PaC

Press releases > Red Hat Introduces "Policy as Code" to Help Address ...

Red Hat Introduces "Policy as Code" to Help Address AI Complexities at Scale

As a capability of Red Hat Ansible Automation Platform, automated policy as code will aim to drive policy-specific automation across the hybrid cloud, bringing governance and greater consistency to the AI boom and traditional IT operations alike

DENVER – RED HAT SUMMIT 2024 - May 7, 2024 – Red Hat, Inc., th
open source solutions, today announced automated policy as code, a
future versions of Red Hat Ansible Automation Platform. The capabili
and compliance across hybrid cloud estates that increasingly include
number of AI applications. Another step in automation maturity, polic
possible to adhere to changing internal or external requirements and
sprawling infrastructure in support of scaling AI workloads.

IT Ops Times

SD Times | Features | Learning Center | Advertise | Podcast | Subscribe

AI OPS | AUTOMATION | CLOUD | CONTAINERS | DEVOPS | HARDWARE | ITSM | KUBERNETES

Red Hat to introduce 'policy-as-code' in Ansible Automation platform

Latest News Published: May 9th, 2024 - David Rubinstein

Red Hat is introducing 'policy-as-code' with its Ansible Automation platform to help enforce compliance within hybrid cloud environments that are leveraging an increasing number of applications powered by

nore rapidly, the need for AI to manage policies across
ncing the new capability, Red Hat wrote that "policy as
practices into automation code, so that internal
tes are built into every process."

DevOps.com
POWERED BY Techstrong Group

LATEST | VIDEOS/PODCASTS | WEBINARS | LIBRARY | EVENTS | SPONSORED CONTENT | RELATED SITES | MEDIA KIT

AI | CLOUD | CI/CD | CONTINUOUS TESTING | DATAOPS | DEVSECOPS | DEVOPS ONRAMP | PLATFORM ENGINEERING | LOW-CODE

Red Hat Plans to Add Policy-as-Code Tools to Ansible Platform

Red Hat Plans to Add Policy-as-Code Tools to Ansible Platform

BY: MIKE VIZARD ON MAY 13, 2024

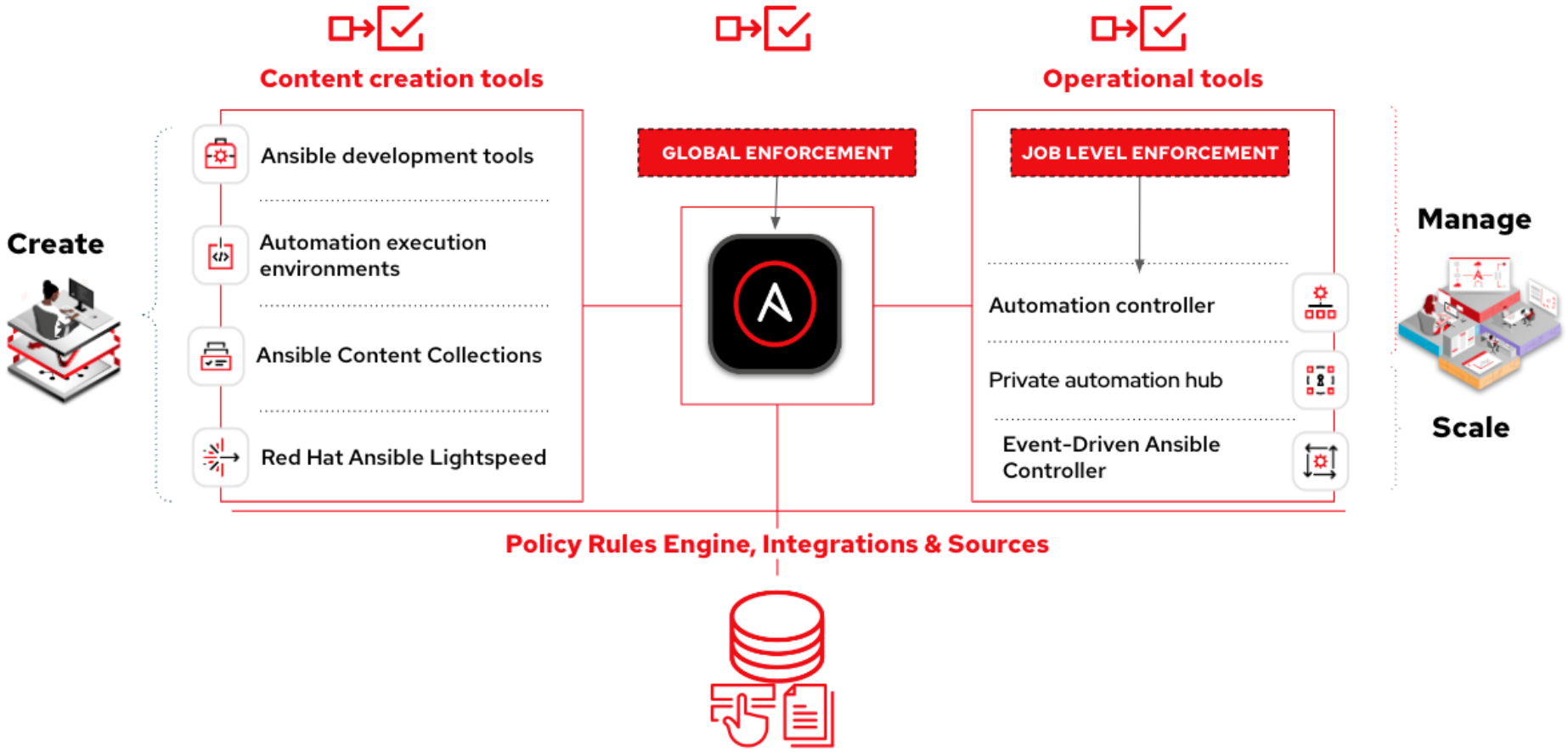
Red Hat is previewing a policy-as-code capability for the Ansible Automation Platform that promises to make it simpler to apply and enforce governance and compliance policies.

Demonstrated at the Red Hat Summit and AnsibleFest 2024 conference, Matthew Jones, chief architect for Red Hat Ansible Automation Platform, told conference attendees this capability would, for example, make it possible to enforce policies that prevent artificial intelligence (AI) models from initiating actions beyond the scope of a set of policies defined as code.

Scheduled to be added to the Red Hat Ansible Automation Platform in the coming months, Red Hat is in effect providing a declarative approach to implementing policy-as-code, in a way that eliminates the need to deploy and master a separate programming framework.

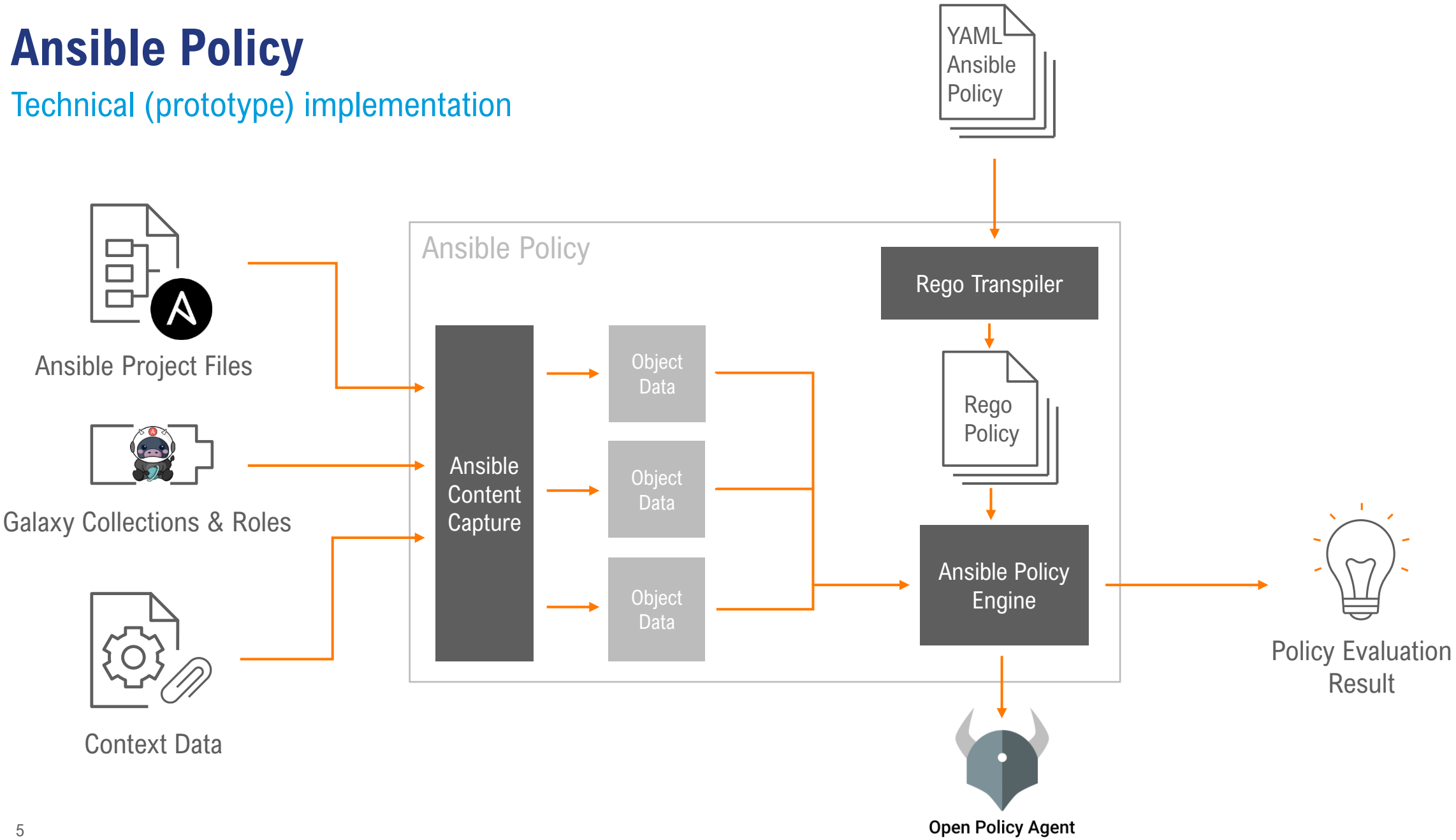
Trusted Automation Supply Chain

Step 1: Policy Enforcement at content creation



Ansible Policy

Technical (prototype) implementation



Policybook

New type next to playbooks and rulebooks

Different types of Ansible content

- **Playbooks -** Ansible Core
  - How to automate stuff
- **Rulebooks -** Event-Driven Ansible
  - Trigger automation when certain conditions occur
- **Policybooks -** Ansible Policy as Code
  - What is allowed in automation

- Policybooks contain a list of policysets
  - Looks very similar to playbooks, policies key instead of tasks or roles
- Policies decide to run actions by evaluating the condition(s)
  - Targets `play`, `roles` or `task`
  - Conditions support many (but not all/and additional) well-known operators
  - Action can be `deny`, `allow`, `info`, `warn` or `ignore`
- **Only minimal (and incomplete) documentation available**
  - It is tech-preview and will improve over time

```
---
- name: Compliance policies for Ansible automation
  hosts: localhost
  vars:
     allowed_users:
       - ansible
       - postgres
       - ec2-user
  policies:
    - name: Check for using become in play
      target: play
      condition: input.become == true
      actions:
        - deny:
            msg: Use become at task-level only!
      tags:
        - compliance

    - name: Check for using become in task
      target: task
      condition:
        any:
          - input.become == true and input.become_user not in allowed_users
          - input.become == true and input lacks key become_user
      actions:
        - deny:
            msg: Allowed users for are one of {{ allowed_users }}
      tags:
        - compliance
```

Demo

Ansible Policy Walkthrough:
Check playbook against a set of policies

https://github.com/TimGrt/anwendertreffen-03-2025-demo

Danke