



Connect

El futuro de Ansible en un entorno de IA basado en agentes: Automation Orchestrator

Ricardo Carrillo Cruz
Principal Software Engineer

César Francisco San Nicolás Martínez
Senior Software Engineer

Ricardo Carrillo Cruz

Principal Software Engineer
Red Hat

César Francisco San Nicolás Martínez

Senior Software Engineer
Red Hat



Visual Workflow Automation with Human Oversight

Automation Orchestrator is a visual workflow platform combining AI agents, action steps, and human oversight.

- **No-Code Canvas:** Easily connect triggers, task agents, action steps, logic, and approval gates.
- **Flexible Deployment:** Runs standalone or alongside Ansible Automation Platform (AAP).
- **Multimode Automation:** Matches the right execution type (event-driven, task-driven, AI-reasoned) to each step under one shared governance model.
- **AI Meets Reliability:** Extends AAP with AI capabilities and cross-system orchestration. AI reasons and decides, while AAP's job templates provide the deterministic, tested, and repeatable execution layer.



Core Workflow Concepts and Execution Patterns

The platform relies on foundational building blocks including triggers, steps (nodes), and edges (connections) defined in exportable, version-controllable YAML.

- **Triggers:** Initiate workflows via manual input, webhooks, schedules, or Event-Driven Ansible.
- **Execution Patterns:** Supports sequential, parallel, conditional, switch, loop, and converge flows.
- **Reliability:** State is preserved across runs with configurable 'on failure' behavior per step (continue vs. stop).
- **Data Flow:** Variable mapping seamlessly passes data between steps, making trigger, loop, and workflow context available in expressions.



Enhancing Automation with AI Task Agents

Task Agent steps introduce LLM reasoning for complex tasks that cannot be encoded as static rules, such as log analysis, incident classification, and remediation recommendations.

▶ **Execution Modes:**

- **Standard:** Free-form text response.
 - **Structured Output:** Constrained to a specific JSON schema.
 - **Post-Tool Extraction:** Tool use combined with a structured final answer.
- ▶ **Model-Agnostic Flexibility:** Bring your own LLM provider using any OpenAI-compatible endpoint.
- ▶ **Granular Control:** Optimize for cost, latency, or capability with per-step model selection.



Secure Tool Integration and Strict Governance

The Model Context Protocol (MCP) securely connects AI agents to external tools, such as querying AAP inventory, job status, or host variables, using an All, Selected, or None tool selection strategy.

Governance Controls

Human Oversight

- Approval steps for mandatory human review.

Access Control

- Restricted tool access and prompt guardrails.

Security

- Credential isolation ensures agents never see decrypted secrets.

Reliability

- Structured output enforcement guarantees expected data formats.

Auditing

- A full audit trail logs every AI decision alongside existing AAP RBAC and approval records.



Combining AI Judgment with Deterministic Execution

AI agents decide, and AAP executes deterministically.

► Dynamic Selection

Task Agent output dynamically selects which tested AAP Job Execution template to run via expressions, replacing hardcoded logic.

► Safety Guardrails

- An approval gate sits directly between the AI recommendation and execution.
- Structured output (JSON schema) ensures the agent only returns valid, expected values.
- Credentials are referenced by ID and never exposed to the LLM.

► Result

Non-deterministic reasoning safely drives deterministic, auditable automation.



Orchestrator Enhances AAP Without Disruption

Automation Orchestrator adds a new layer without replacing your existing infrastructure. No migration or disruption is required.

- **Seamless Continuity:** Existing playbooks, workflow templates, and scheduled jobs continue running unchanged in automation controller.
- **Instant Reusability:** Every production-ready job template, role, and collection immediately becomes a reusable workflow node.
- **Inherited Governance:** Workflows automatically inherit existing AAP Role-based access control (RBAC), approval gates, and audit trails.
- **Governed AI:** Every AI decision is recorded in the audit log, making AI a governed participant rather than a separate, siloed system.



Intuitive Workflow Builder Interface

The Automation Orchestrator provides a comprehensive UI for designing, managing, and monitoring automation workflows.

Workflows Page

Browse, filter, and import/export saved workflows.

Workflow Runs

View detailed execution history and real-time status updates.

Workflow Builder Canvas

Design workflows using an intuitive drag-and-drop interface.

Approvals

Centrally manage pending human decision points and gates.

Details Panel

Configure Input, Parameters, and Output for each selected step.



Developer Preview: Custom Script Steps

Script steps allow the inclusion of custom Python or Bash code directly within a workflow, useful for data transformation, validation, or command-line tool invocation.

- ▶ **Current Status:** Developer Preview.
- ▶ **Security Note:** Execution is currently disabled as it runs inside the worker process without isolation, presenting a security risk.
- ▶ **Functionality:** You can add and save script steps in the builder, but they will intentionally fail upon execution until isolation is addressed.



RECOMMENDATION

Do not use for production or business-critical workloads at this time.



Building an AI-Driven Workflow

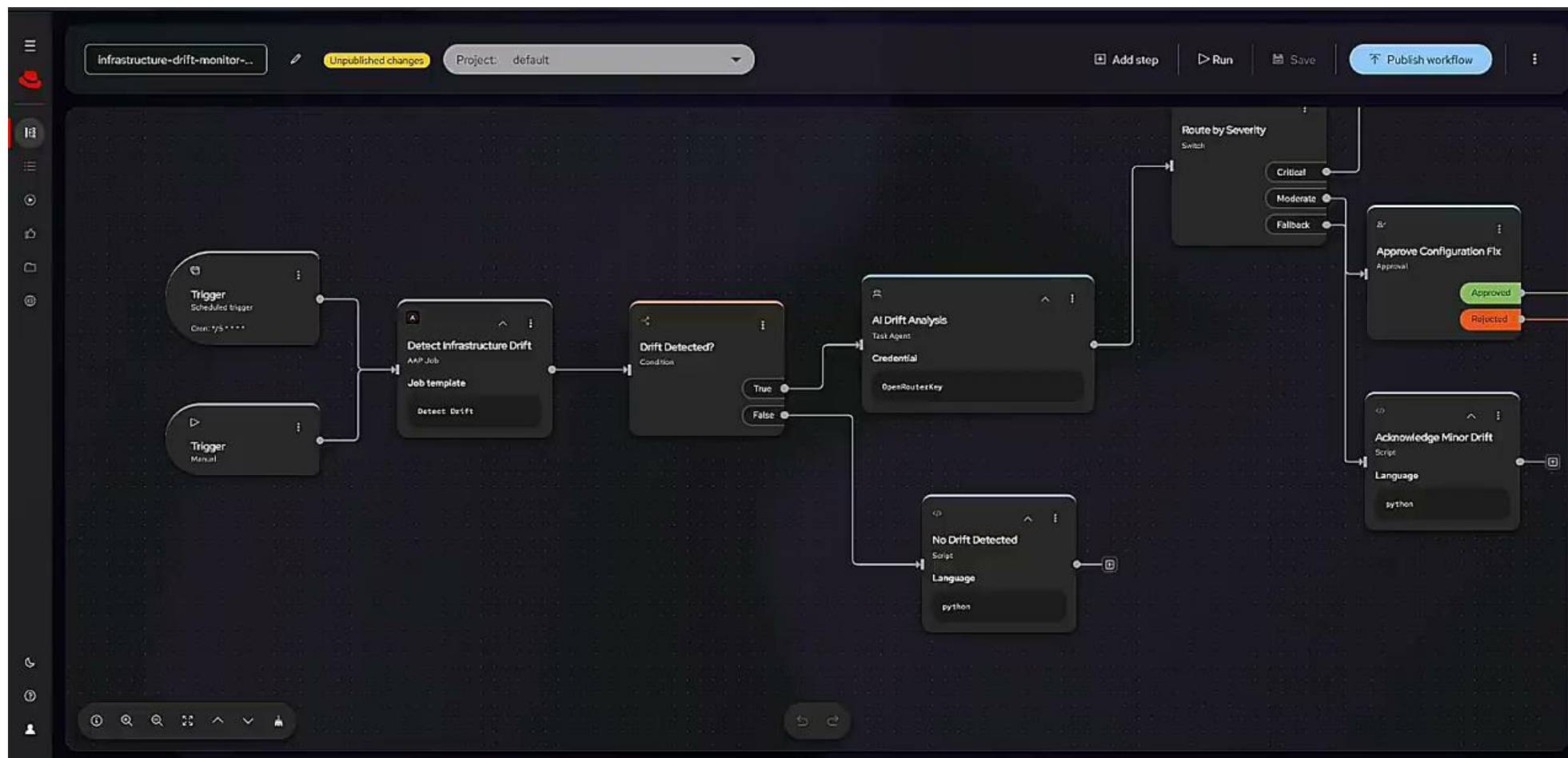
We will now build an example workflow demonstrating:



- 01** **Configure a Task Agent step**, defining the model, prompt, tools, and JSON response schema.
- 02** **Add an Approval step**, assigning approvers and a timeout duration.
- 03** **Add an AAP Job Execution step**, demonstrating the agent's structured output (job_template_name) feeding directly into template selection.
- 04** **Connect the steps**, save, and execute the workflow.
- 05** **Walk through the execution viewer** to observe step status, the approval decision, and deterministic AAP execution.



Demo!



Tech Journey demos: Red Hat Security



Webinar

[Desplegando una fortaleza digital: no confíes, siempre verifica y encripta tus datos](#)

23 de octubre de 2026, 10:00 a.m.



Webinar

[Automatización y seguridad: estrategia de remediación integral con Red Hat](#)

13 de noviembre de 2026, 10:00 a.m.





Hands-on Workshop Week • November 30, to December 4, 2026

Red Hat Tech Journey workshop week

One week. Four areas shaping enterprise IT. Hands-on experience.



Discover how to apply open source technologies to build secure platforms, automate operations, and run modern applications across hybrid environments.



Connect

Thank you



linkedin.com/company/red-hat



facebook.com/redhatinc



youtube.com/user/RedHatVideos



x.com/RedHat

