gruve Red Hat

SOLUTION BRIEF

Ansible Automation Platform Autonomous AIOps

A three-mode operational model for task-driven, event-driven, and AI-driven operations

01

Business problem

Most enterprises do not have an automation problem — they have an automation maturity problem. They already have playbooks, runbooks, monitoring tools, and ticketing systems, but operations are still manual, reactive, and dependent on people knowing what to run, when to run it, and why.

The symptoms are compounding. Infrastructure provisioning consumes days of ticket queues. Monitoring tools fire alerts constantly, but humans still triage, gather facts, decide what to run, and execute which yields to slow MTTR and operational overhead. Configuration drift is discovered after the fact, not prevented automatically.

Organizations that attempt to consolidate on Red Hat Ansible Automation Platform without a structured approach face predictable failure modes: playbook sprawl, disconnected event handling, and automation that cannot scale to modern IT operations or AI-assisted remediation.

CURRENT STATE

Automation exists, but it is not yet operating as a system.

$300K–$800K
hidden annual costs

6–12 mo
compliance remediation

9–18 mo
to build expertise

CORE CHALLENGES

- Scattered automation, no governed execution layer
- Alerts fire but humans still triage and respond manually
- Siloed teams, automation knowledge leaves with engineers
- Playbook sprawl replaces, not solves, the problem

UNDERLYING BARRIERS

- No trusted foundation for event or AI-driven invocation
- RBAC & credential management as afterthoughts
- No governed execution environments or content signing
- Configuration drift with no automated enforcement

AI agents have moved from future vision to operational reality. Complexity is increasing, business expectations are rising, security and compliance demands are growing, and staffing constraints remain real. At the same time, AI has changed the economics of operations.

Who will be accountable for AI?

Managing costs

AI has reduced the cost of generating code to zero, but it has dramatically increased the volume of code to manage, the complexity implications across the stack, and token costs. Why spend tokens and GPU to do basic deterministic infrastructure tasks?

Taming complexity

AI agents introduce execution at a scale and speed that humans cannot manually review in real time. Without a governed foundation, the blast radius of an AI mistake may be unknowable. Mission-critical infrastructure cannot be an experiment.

Securing operations

Governance cannot be retrofitted. It must be foundational — established before the agents arrive. The governance you build with Ansible Automation Platform through task-driven and event-driven operations is a massive head start.

02

The governance imperative

Governance cannot be retrofitted. It must be foundational — established before the agents arrive.

A library of approved actions
Tested and certified playbooks, roles, and workflows. Every automation asset in your estate is a pre-approved action AI can safely invoke. Governed, auditable, trusted.

Execution boundaries defined before it runs
Not after it breaks. Policy-based access controls, RBAC scope, and approval workflows established in advance. The guardrails are built into the execution layer, not bolted on afterwards.

An audit trail proving what happened
When it ran, who authorized it, and why. Full activity stream across every automated action — from task execution to event-driven response to agent-invoked workflows.

The compounding returns of a governed foundation

EVERY PLAYBOOK

Grows your approved actions footprint

Every automation asset you add increases the library of approved, tested actions that AI agents can safely invoke. These aren't one-time wins — they accumulate.

EVERY POLICY

Creates a governance boundary

Every access control, RBAC scope, and approval rule you define in AAP creates the governance boundaries that guard against unwanted or unvetted AI execution. Set once, always enforced.

EVERY USE CASE

Builds the audit trail

Every domain you automate creates a comprehensive audit record across the entire stack. These returns compound, and they become the evidence your organization needs as AI scales.

03

The automation maturity model

Most customers already have some level of automation. The challenge is that it is not yet operating as a system. Gruve provides a practical path from task-driven automation to Autonomous AIOps.

TASK-DRIVEN

01. Automation foundation & governance

Gruve delivers

- Automation readiness assessment
- AAP architecture & implementation
- Execution environments & private hub
- Git repo structure & playbook standards
- RBAC, credential governance & team enablement

Business outcomes

Standardized, governed, reusable automation estate

Ansible Automation Platform

EVENT-DRIVEN

02. Event-driven automation & closed-loop response

Gruve delivers

- EDA rulebook design & activation
- Splunk, Prometheus, SolarWinds ingestion
- Alert enrichment & normalization
- Approved remediation playbook execution
- Escalation workflows with human approval

Business outcomes

Faster MTTR, consistent operations, signals trigger approved automation

Event-Driven Ansible

AI-DRIVEN

03. AI-driven AIOps with Ansible execution

Gruve delivers

- AI reasoning layer & MCP server integration
- AAP API integration & tool registry
- Context enrichment & incident classification
- Human-in-the-loop approval workflows
- ServiceNow/Jira updates & full audit logging

Business outcomes

Intelligent operations with governed, auditable Ansible execution

AAP + AI Agent

04

Solution overview

Gruve's Autonomous AIOps service helps customers build a governed automation control plane that becomes the execution layer for modern IT operations and AI-driven AIOps. We standardize trusted playbooks and execution environments, connect those workflows to real-time events, then add AI reasoning on top — with Red Hat Ansible Automation Platform remaining the governed execution layer throughout.

Red Hat Ansible Automation Platform

The agent reasons, and Ansible executes. Gruve builds the governed workflow between them.

Gruve's solution components

Solution component	Description
TRACK 1 Task-driven automation foundation	Build the trusted execution layer: automation readiness assessment, AAP architecture, controller setup, private hub, execution environments, Git repo structure, playbook & role standards, RBAC, credential governance, content migration, team enablement.
TRACK 2 Event-driven automation & closed-loop response	Connect operational signals to approved automation: EDA rulebooks, event ingestion from Splunk, Prometheus, SolarWinds, Dynatrace, alert enrichment, rule-based decision logic, ticket creation, approved remediation execution, escalation workflows.
TRACK 3 AI-driven AIOps with Ansible execution	Add intelligence over a governed control plane: AI reasoning layer, MCP server integration, AAP API integration, tool registry mapped to approved job templates, context enrichment, incident classification, human-in-the-loop approval, audit logging.
ALL Platform architecture & design	Design multi-mode platform topology: Git-backed projects, automation mesh, private hub, execution environment strategy, Event-Driven Ansible, and AI agent API interfaces. Each layer builds trust that enables the next.
ALL CI/CD & ITSM integration	Integrate with Jenkins, GitLab CI, GitHub Actions, ServiceNow, and Jira to embed task, event, and AI-driven automation into delivery pipelines and IT service management.
ALL Team enablement & governance	Role-based training for administrators, automation developers, and operations teams; governance frameworks; content approval workflows; center-of-excellence operating models.

05

Benefits of Gruve's solution

TRACK 1 — FOUNDATION

Accelerated automation ROI

Reduce infrastructure provisioning time by 70–80% and eliminate manual configuration toil. Organizations typically recover implementation investment within 6–9 months through engineer productivity gains and reduced change-window failures.

70–80%
provisioning time reduction

TRACK 1 — FOUNDATION

Eliminated automation debt

Replace brittle scripts and tribal knowledge with governed, version-controlled automation in private automation hub. Reduce maintenance burden by 50% through standardized roles, signed execution environments, and documented workflows.

50%
maintenance burden reduction

TRACK 2 — EVENT-DRIVEN

Closed-loop operational response

A playbook sitting in a repository does not reduce MTTR. A playbook triggered by the right signal at the right time does. EDA enables automated remediation in under 60 seconds — consistent, governed, and auditable every time.

40–65%
MTTR reduction

TRACK 3 — AI-DRIVEN

Governed AI operations with auditability

AI agents reason over context and invoke only pre-approved Ansible job templates through controlled interfaces, with full RBAC, human oversight, and audit trails. AI without governance is risk — Gruve builds the guardrails.

90 days
to platform independence

ALL TRACKS

Strengthened security & compliance

Every automated action is RBAC-scoped, logged, and auditable. Automate continuous enforcement of security baselines across the entire infrastructure estate, reducing audit preparation time by 60% and eliminating configuration drift.

60%
audit preparation time saved

06

Service offerings

One umbrella offering, three service tracks. Start where you are and grow at your own pace.

Gruve Autonomous AIOps with Red Hat Ansible Automation Platform

Task-driven automation foundation

Build the trusted execution layer
Customers with scripts, manual runbooks, or early Ansible usage

- ✓ Automation readiness assessment
- ✓ AAP architecture & implementation
- ✓ Execution environments & private hub
- ✓ Git repo structure & playbook standards
- ✓ RBAC, credential governance
- ✓ Content migration from scripts/ runbooks
- × EDA rulebooks
- × AI agent integration

Red Hat Ansible Automation Platform

→ Governed automation estate

8–12 weeks

Event-driven operations

Connect signals to approved automation
Customers with monitoring tools and recurring incidents

- ✓ Requires Track 1 foundation
- ✓ EDA rulebook design & activation
- ✓ Splunk, Prometheus, SolarWinds ingestion
- ✓ Alert enrichment & normalization
- ✓ Approved remediation playbook execution
- ✓ Escalation & approval workflows
- × AI agent integration
- × MCP server integration

Red Hat
Event-Driven Ansible

→ Signals trigger approved automation

8–16 weeks

AI-driven AIOps

Add intelligence over a governed control plane
Customers ready to add AI reasoning over operations

- ✓ Requires Tracks 1 & 2
- ✓ AI reasoning layer design
- ✓ MCP server & AAP API integration
- ✓ Tool registry for approved job templates
- ✓ Context enrichment & classification
- ✓ Human-in-the-loop approval
- ✓ ServiceNow/Jira ticket updates
- ✓ Full audit logging & governance

Red Hat
AAP + AI Agent

→ AI-assisted closed-loop operations

12–20 weeks

07

Use case: Before & after

BEFORE GRUVE

- Manual NOC: scripts scattered across teams, no event-driven response, no governed execution layer.
- Monitoring fires alerts constantly. NOC teams manually triage, gather facts, decide what to run, and execute. Slow MTTR.
- AI initiatives explored but running outside Ansible. Ad-hoc actions bypass RBAC, audit trails, and governance controls.
- Compliance audits require weeks of manual evidence collection. Configuration drift is discovered in retrospect, not prevented.

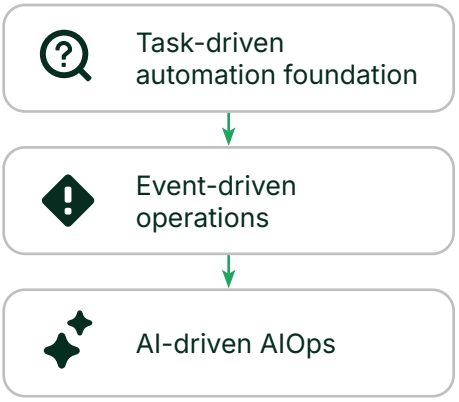
AFTER GRUVE

- Governed automation control plane: versioned Git repos, signed execution environments, private hub, RBAC. Reusable, auditable, approved patterns events and AI can safely invoke.
- Splunk alerts trigger EDA rulebooks invoking approved job templates in under 60 seconds — disk cleanup, service restarts, certificate rotation, incident enrichment — consistent every time.
- AI agent reasons over context, selects the appropriate approved Ansible job template, and launches through MCP/API controls. Every action is RBAC-scoped, logged, and auditable.
- Event-Driven Ansible continuously enforces configuration baselines. Compliance evidence is generated automatically — no manual collection, no retrospective discovery.

08

Start your autonomous AI journey

“Most customers already have some level of automation. The challenge is that it is not yet operating as a system. Gruve helps customers mature from task-driven automation — where playbooks are standardized and governed — to event-driven operations, where alerts trigger approved workflows, and then to AI-driven operations, where agents reason over context and invoke trusted Ansible automation through guardrails. This gives customers a practical path to Autonomous AIOps without giving up control, auditability, or human oversight.”



Engagements typically begin within 2 weeks of initial assessment completion.

www.gruve.ai | **info@gruve.ai**