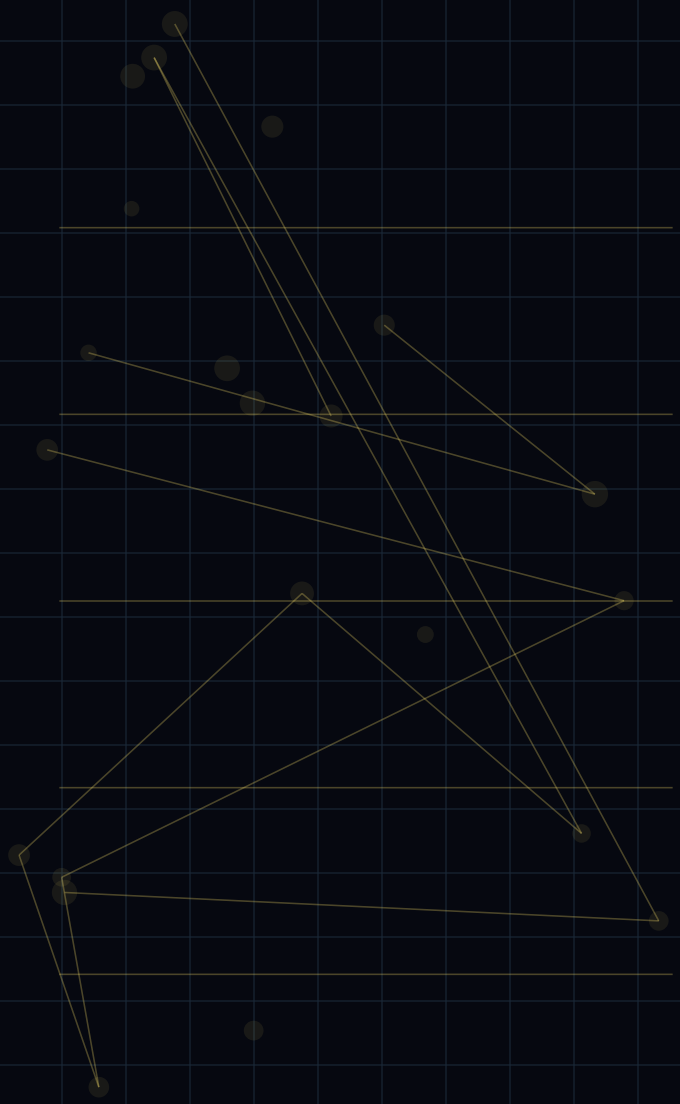
COMPARATIVE EVALUATION / EVIDENCE REFRESH

CMP-008

Configuration Management

Fleet configuration, convergence and orchestration platforms



CURRENT EVIDENCE SNAPSHOT

Official product sources refreshed through 2026-09-17

Controlled Mythos laboratory rerun: NOT ASSERTED

BENCHMARK DOCTRINE

Gates before scores. Evidence before certainty. Profile fit before universal ranking.

VERSION 1.2.0-candidate

CANDIDATE COMPARATIVE EVALUATION / PUBLIC

Configuration Management

Fleet configuration, convergence and orchestration platforms

DOCUMENT ID
CMP-008
VERSION
1.2.0-candidate
STATUS
Candidate Comparative Evaluation
PUBLICATION DATE
2026-09-17
SCHEDULED REVIEW
2026-12-16
CANONICAL ROUTE
/library/evaluations/cmp-008/

4
CANDIDATES

18
ATOMIC CRITERIA

9
MANDATORY GATES

3
WORKLOAD PROFILES

E2
CURRENT MAX EVIDENCE

CURRENT DECISION BOUNDARY

Ansible remains a strong July documentation baseline, but that is not a universal selection. Puppet lifecycle changes, Chef 19 migration, and Salt runtime evolution make current lab evidence mandatory. Prove drift, content trust, secrets, fleet scale, rollback, recovery, and upgrade behavior.

NO CURRENT UNIVERSAL WINNER IS PUBLISHED FROM THIS REFRESH.

July 24 baseline scores are preserved as lineage and sensitivity evidence, not silently reissued as September laboratory results.

Red Hat Ansible Automation P

AAP 2.6 patch / 2026-08-04

REFRESH TRIGGER

Current 2.6 patch line includes security fixes and updates across controller, hub, Event-Driven Ansible, and Receptor.

Puppet Enterprise

PE 2025.11.3 / 2026-09-10

REFRESH TRIGGER

Puppet is transitioning support lifecycle models while updating certificate, patching, PostgreSQL, security, and platform support.

Chef Infra

Client 19.3.15 LTS / 2026-05-22

REFRESH TRIGGER

Client 19 LTS moves to Habitat-based packaging; migration and platform compatibility are first-class selection risks.

Salt

3008.2 line / current docs

REFRESH TRIGGER

Current 3008 line includes packaging/runtime changes while 3006.x remains an important long-lived branch.

FINAL BENCHMARK SYSTEM / DECISION ARCHITECTURE

01 SCOPE

Freeze decision, candidates, versions and exclusions.

02 GATES

Test non-compensable trust, state, recovery, change and exit.

03 SCORES

Measure atomic capability with approved profile weights.

04 CONFIDENCE

Discount by source grade, freshness, repeatability and relevance.

05 PROOF

Run normal, failure, migration, recovery and operator scenarios.

06 DECISION

Record conditional fit, residual risk, owner and revalidation trigger.

EVIDENCE CONFIDENCE / MODIFIERS

E0	E1	E2	E3	E4	E5
0.00	0.38	0.64	0.78	0.91	1.00
UNSUPPORTED	VENDOR ASSERTION	OFFICIAL SOURCE	MYTHOS LAB	PRODUCTION	INDEPENDENT

THIS EDITION

Current official product and release sources have been refreshed to E2. No E3 controlled Mythos lab rerun is claimed. Therefore current profile rankings remain intentionally unissued until the proof plan is executed.

What changed since the July benchmark snapshot

Changes below are sourced from current official release documentation. They identify revalidation triggers; they are not translated into new numeric scores without controlled proof.

Red Hat Ansible Automation Platfor

AAP 2.6 patch / 2026-08-04

MATERIAL DELTA

Current 2.6 patch line includes security fixes and updates across controller, hub, Event-Driven Ansible, and Receptor.

CRITERIA TOUCHED

C02 / C05 / C07 / C09 / C14

MODERATE REVALIDATION

Puppet Enterprise

PE 2025.11.3 / 2026-09-10

MATERIAL DELTA

Puppet is transitioning support lifecycle models while updating certificate, patching, PostgreSQL, security, and platform support.

CRITERIA TOUCHED

C02 / C04 / C09 / C14 / C17

HIGH REVALIDATION

Chef Infra

Client 19.3.15 LTS / 2026-05-22

MATERIAL DELTA

Client 19 LTS moves to Habitat-based packaging; migration and platform compatibility are first-class selection risks.

CRITERIA TOUCHED

C04 / C09 / C11 / C14 / C16 / C17

HIGH REVALIDATION

Salt

3008.2 line / current docs

MATERIAL DELTA

Current 3008 line includes packaging/runtime changes while 3006.x remains an important long-lived branch.

CRITERIA TOUCHED

C04 / C08 / C09 / C14 / C17

MODERATE REVALIDATION

Mandatory gates remain non-compensable

No current release is marked PASS solely from documentation. E2 means the official source supports the capability path; LAB and RETEST identify proof still required. HOLD blocks a current decision.

MANDATORY GATE	RED HAT ANSIBLE	PUPPET ENTERPRI	CHEF INFRA	SALT
C01 Functional coverage	E2	E2	E2	E2
C02 Security / trust	RETEST	RETEST	E2	E2
C03 Governance / approval	E2	E2	E2	E2
C04 State integrity	E2	RETEST	RETEST	RETEST
C07 Observability / evidence	RETEST	E2	E2	E2
C09 Resilience / continuity	RETEST	RETEST	RETEST	RETEST
C11 Change safety / rollback	LAB	LAB	RETEST	LAB
C16 Portability / exit	LAB	LAB	RETEST	LAB
C18 Assurance confidence	HOLD	HOLD	HOLD	HOLD

LEGEND

E2 official-source support only

LAB controlled proof required

RETEST release delta touches this gate

HOLD decision gate remains closed

Historical profile sensitivity - preserved, not reissued

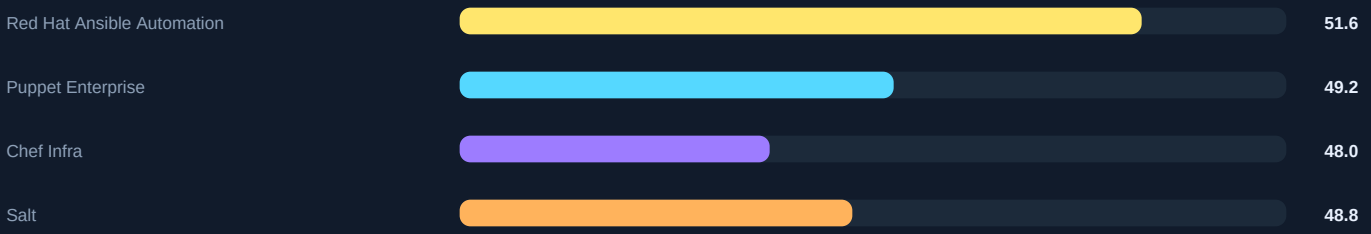
Values below are the 2026-07-24 evidence-adjusted baseline. They show sensitivity to operating-model weights. The September refresh does not recompute rank because E3 lab proof has not been reproduced.

AGENTLESS ENTERPRISE AUTOMATION

BASELINE SPREAD 4.0 PTS

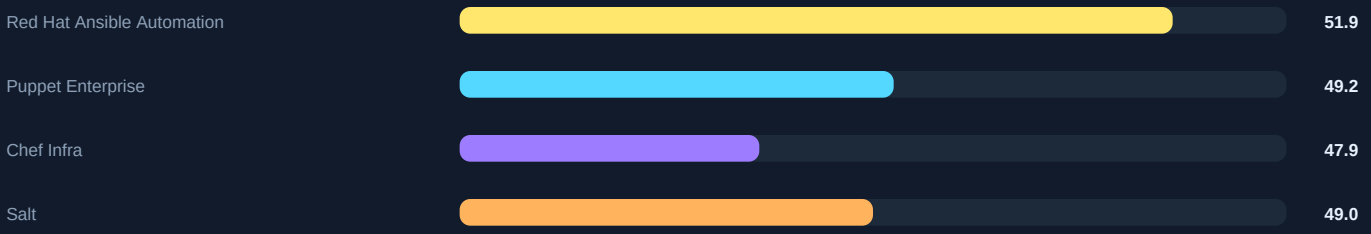
CONTINUOUS DESIRED-STATE ENFORCEMENT

BASELINE SPREAD 3.6 PTS



EVENT-DRIVEN OPERATIONS FABRIC

BASELINE SPREAD 4.0 PTS



CURRENT RANK STATUS: WITHHELD PENDING CONTROLLED PROOF.

Evidence confidence is separate from capability

E5 — Independent repeatable validation
confidence modifier 1.00

E4 — Production evidence in adopting environment
confidence modifier 0.91

E3 — Controlled Mythos laboratory result
confidence modifier 0.78

E2 — Official documentation / release / source
confidence modifier 0.64

E1 — Vendor assertion or marketing
confidence modifier 0.38

E0 — Unsupported or unverified
confidence modifier 0.00

CURRENT EVIDENCE STATE

Red Hat Ansible Automation P	E2 REFRESHED
Historical adjusted confidence: 58.2%	
E3 LAB: NOT REPRODUCED	
Puppet Enterprise	E2 REFRESHED
Historical adjusted confidence: 58.2%	
E3 LAB: NOT REPRODUCED	
Chef Infra	E2 REFRESHED
Historical adjusted confidence: 58.2%	
E3 LAB: NOT REPRODUCED	
Salt	E2 REFRESHED
Historical adjusted confidence: 58.2%	
E3 LAB: NOT REPRODUCED	

ASSURANCE RULE

A current release note can change capability context, but it cannot raise assurance beyond E2. Current recommendation strength is therefore bounded until the test plan produces reproducible artifacts.

Lifecycle risk is evaluated independently of features

The benchmark models migration, upgrade, compatibility, support, staffing, data/state export, downtime and exit. Current release changes below are explicit proof triggers.

Red Hat Ansible Automation Platform

MODERATE REVALIDATION

Current 2.6 patch line includes security fixes and updates across controller, hub, Event-Driven Ansible, and Receptor.

RETEST: C02 / C05 / C07 / C09 / C14

Puppet Enterprise

HIGH REVALIDATION

Puppet is transitioning support lifecycle models while updating certificate, patching, PostgreSQL, security, and platform support.

RETEST: C02 / C04 / C09 / C14 / C17

Chef Infra

HIGH REVALIDATION

Client 19 LTS moves to Habitat-based packaging; migration and platform compatibility are first-class selection risks.

RETEST: C04 / C09 / C11 / C14 / C16 / C17

Salt

MODERATE REVALIDATION

Current 3008 line includes packaging/runtime changes while 3006.x remains an important long-lived branch.

RETEST: C04 / C08 / C09 / C14 / C17

IRREVERSIBLE COMMITMENT GATE

Before migration or procurement lock-in, prove rollback, state portability, operational reconstruction, and supplier-exit assumptions.

Controlled proof is the next decision-producing step

REPRODUCTION STATE / NOT EXECUTED IN THIS EVIDENCE-REFRESH RELEASE

01

CONTROLLED SCENARIO

Manage representative Linux, Windows, network, cloud, middleware, and application targets.

02

CONTROLLED SCENARIO

Execute configuration, patch, compliance, orchestration, secret, and remediation workflows.

03

CONTROLLED SCENARIO

Test dry-run, check or noop mode, canary, concurrency, failure, retry, rollback, and recovery.

04

CONTROLLED SCENARIO

Inject controller loss, certificate expiry, repository outage, partial fleet reachability, and conflicting state.

05

CONTROLLED SCENARIO

Measure convergence time, drift detection, job throughput, operator effort, and evidence completeness.

06

CONTROLLED SCENARIO

Rebuild the control plane and representative nodes from versioned content and backups.

EVIDENCE PACKAGE

Preserve exact versions, architecture, configuration, scenario, expected result, instrumentation, raw output, timing, failures, operator actions, deviations, acceptance state, owner, and artifact hashes.

Current decision posture

Ansible remains a strong July documentation baseline, but that is not a universal selection. Puppet lifecycle changes, Chef 19 migration, and Salt runtime evolution make current lab evidence mandatory. Prove drift, content trust, secrets, fleet scale, rollback, recovery, and upgrade behavior.

CURRENT RANKING: NOT REISSUED / CONTROLLED LAB REQUIRED

CURRENT OFFICIAL-SOURCE REGISTER / CHECKED 2026-09-17

Red Hat Ansible Automation P	E2 / OFFICIAL	
Red Hat AAP 2.6 Aug 4 release		docs.redhat.com
Puppet Enterprise	E2 / OFFICIAL	
Puppet Enterprise release notes		help.puppet.com
Chef Infra	E2 / OFFICIAL	
Chef Infra Client release notes		docs.chef.io
Salt	E2 / OFFICIAL	
Salt 3008.2 release notes		docs.saltproject.io

REVISION LINEAGE

1.2.0-candidate / 2026-09-17 - current-source evidence refresh; no lab rescore issued.

1.1.0-candidate / 2026-07-24 - baseline benchmark using the final comparative evaluation system.

Trigger earlier review after major release, acquisition, licensing change, critical vulnerability, material outage, failed PoC, or workload change.

BASELINE ANALYTIC RECORD CONTINUES ON PAGE 11 FOR TRACEABILITY.

ATOMIC CRITERIA MODEL

WEIGHTED CAPABILITY WITH EXPLICIT MINIMUM EVIDENCE

ID	CRITERION	WEIGHT	GATE	MINIMUM EVIDENCE
C01	Configuration, patch, compliance, orchestration, and remediation coverage	5	YES	Feature documentation, APIs, configuration exports, and scenario demonstration.
C02	Controller, agent, credential, content, and execution trust architecture	5	YES	Threat model, identity flows, RBAC tests, audit records, and security configuration.
C03	Governance and approval controls	5	YES	Approval workflow, policy controls, separation-of-duties tests, and decision records.
C04	Desired-state, inventory, content, report, and run-state integrity	5	YES	Backup, restore, rollback, drift, and corruption-recovery evidence.
C05	Automation and API quality	4	NO	API specifications, authentication tests, rate limits, event samples, and automation runs.
C06	Integration ecosystem	4	NO	Supported integrations, connector tests, failure behavior, and lifecycle ownership.
C07	Observability and evidence	4	YES	Logs, traces, metrics, reports, export tests, and evidence-retention controls.
C08	Node, job, event, content, and controller scale	4	NO	Controlled load tests, topology scale, saturation behavior, and capacity model.
C09	Resilience and continuity	5	YES	Failure injection, HA tests, recovery timing, degraded-mode operation, and runbooks.
C10	Usability and operator cognition	3	NO	Task observation, error-rate measures, navigation tests, and operator interviews.
C11	Dry-run, change window, canary, rollback, and recovery safety	5	YES	Plan or preview output, canary tests, rollback execution, and post-change verification.
C12	Extensibility and programmability	3	NO	Plugin, module, provider, workflow, or code-extension tests and upgrade impact analysis.
C13	Deployment and sovereignty options	3	NO	Deployment architecture, data-flow mapping, residency evidence, and offline tests.
C14	Lifecycle and upgrade discipline	4	NO	Release notes, upgrade test, compatibility matrix, support policy, and migration plan.
C15	Economics and cost predictability	3	NO	Bill-of-materials, licensing model, staffing estimates, metering, and sensitivity analysis.
C16	Portability and exit	4	YES	Export tests, format analysis, replacement workflow, and decommission evidence.
C17	Vendor and ecosystem risk	3	NO	License analysis, roadmap evidence, bus-factor indicators, and dependency inventory.
C18	Assurance confidence	5	YES	Source provenance, lab artifacts, production evidence, independent replication, and review date.

SCORE SCALE

0 absent; 1 materially deficient; 2 partial; 3 adequate with limits; 4 strong; 5 leading for the defined profile. Scores remain provisional until the required evidence grade is achieved.

RAW CAPABILITY SCORECARD

DOCUMENTED CAPABILITY BEFORE EVIDENCE DISCOUNT

CRITERION	ANSIBLE AAP	PUPPET	CHEF	SALT
C01 Configuration, patch, compliance, orchestration, and remediation coverage	4.8	4.4	4.3	4.5
C02 Controller, agent, credential, content, and execution trust architecture	4.4	4.4	4.3	4.2
C03 Governance and approval controls	4.4	4.2	4.1	4.0
C04 Desired-state, inventory, content, report, and run-state integrity	4.2	4.5	4.4	4.3
C05 Automation and API quality	4.8	4.1	4.0	4.6
C06 Integration ecosystem	4.7	4.2	4.1	4.2
C07 Observability and evidence	4.5	4.4	4.3	4.2
C08 Node, job, event, content, and controller scale	4.6	4.6	4.4	4.6
C09 Resilience and continuity	4.3	4.4	4.2	4.1
C10 Usability and operator cognition	4.5	4.0	3.9	4.0
C11 Dry-run, change window, canary, rollback, and recovery safety	4.5	4.2	4.1	4.2
C12 Extensibility and programmability	4.8	4.3	4.4	4.6
C13 Deployment and sovereignty options	4.4	4.3	4.2	4.4
C14 Lifecycle and upgrade discipline	4.3	4.1	3.9	3.8
C15 Economics and cost predictability	3.8	3.7	3.6	4.0
C16 Portability and exit	4.4	4.0	3.9	4.2
C17 Vendor and ecosystem risk	4.1	3.7	3.5	3.6
C18 Assurance confidence	3.7	3.5	3.4	3.4

WEIGHTED BASELINE / 100

Ansible AAP	Puppet	Chef	Salt
88.0	**83.7**	**81.4**	**83.2**

EVIDENCE-ADJUSTED SCORECARD

CAPABILITY DISCOUNTED BY CURRENT EVIDENCE CONFIDENCE

CANDIDATE	RAW	EVIDENCE CONFIDENCE	ADJUSTED	CURRENT STATE
Ansible AAP	88.0	58.2%	51.8	CONTROLLED LAB PENDING
Puppet	83.7	58.2%	49.2	CONTROLLED LAB PENDING
Chef	81.4	58.2%	47.9	CONTROLLED LAB PENDING
Salt	83.2	58.2%	48.9	CONTROLLED LAB PENDING

EVIDENCE SCALE

E0 / 0.00
Unsupported or unverified

E1 / 0.38
Vendor assertion or marketing statement

E2 / 0.64
Official documentation, release notes, or source repository

E3 / 0.78
Controlled Mythos laboratory result

E4 / 0.91
Production evidence from the adopting environment

E5 / 1.00
Independent repeatable validation

CURRENT CONFIDENCE BOUNDARY

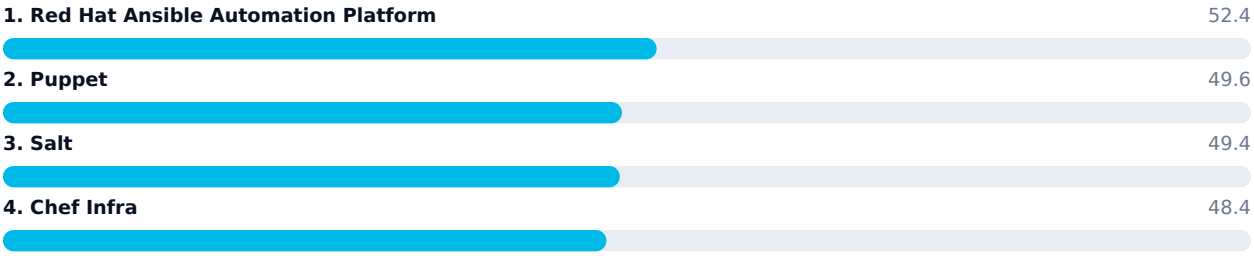
Most candidate criteria are supported at E2: official documentation or source evidence. Environment-specific laboratory, production, and independent evidence remain future gates.

PROFILE-SPECIFIC RANKINGS

EVIDENCE-ADJUSTED SENSITIVITY ANALYSIS

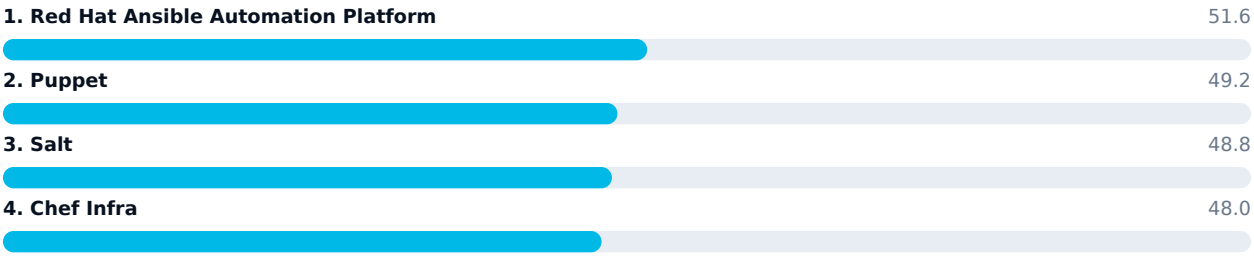
AGENTLESS ENTERPRISE AUTOMATION

Prioritizes broad automation, workflows, execution portability, network and cloud coverage, and low endpoint footprint.



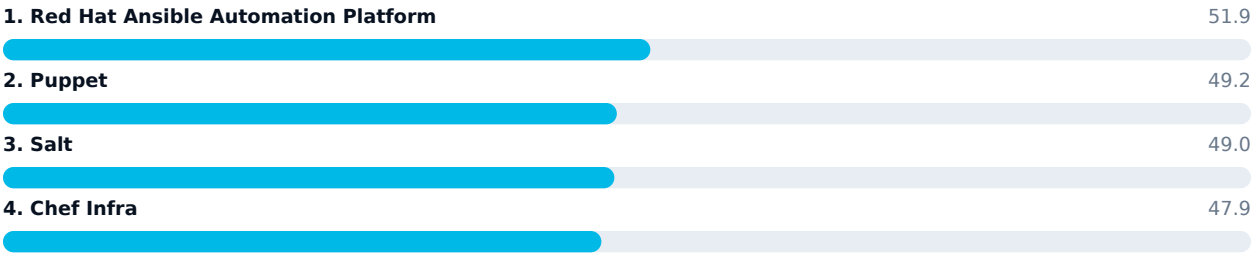
CONTINUOUS DESIRED-STATE ENFORCEMENT

Prioritizes periodic convergence, drift correction, reporting, fleet scale, and stable server configuration.



EVENT-DRIVEN OPERATIONS FABRIC

Prioritizes high-speed remote execution, event reactions, targeting, scale, extensibility, and operational control.



RANK SENSITIVITY

Small score differences are not decision certainty. Treat near-ties as a requirement for deeper PoC, commercial, migration, and operating-model evidence.

CANDIDATE DEEP DIVE / 01

RED HAT ANSIBLE AUTOMATION PLATFORM

OPERATING MODEL

Agentless automation platform using playbooks, inventories, collections, execution environments, controller, API, and event-driven capabilities.

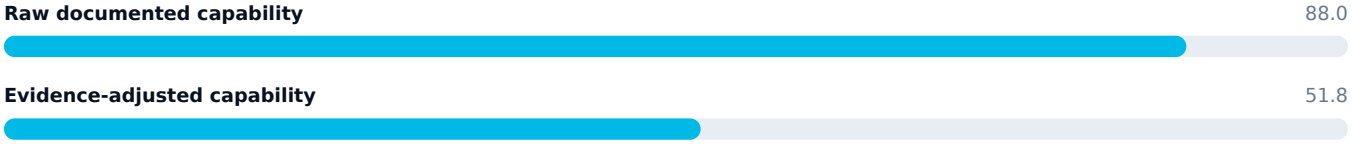
DOCUMENTED STRENGTHS

- Broad automation ecosystem and strong network, cloud, server, and application coverage.
- Agentless SSH and API execution reduces endpoint footprint.
- Execution environments improve reproducibility.
- Controller, RBAC, workflow, and API support enterprise operations.

CAUTIONS AND PROOF OBLIGATIONS

- Idempotence and rollback depend on module and playbook engineering.
- Push execution can miss drift between runs without additional controls.
- Content sprawl and inventory quality require governance.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - agentless enterprise automation | CONDITIONAL - content quality and drift architecture

CANDIDATE DEEP DIVE / 02

PUPPET

OPERATING MODEL

Agent-server desired-state configuration management using catalogs, facts, modules, reports, and periodic enforcement.

DOCUMENTED STRENGTHS

- Strong desired-state convergence and drift correction.
- Mature agent-server architecture and reporting.
- Rich module and policy ecosystem.
- Suitable for large persistent server fleets.

CAUTIONS AND PROOF OBLIGATIONS

- Agent and server lifecycle add operational responsibility.
- General orchestration and network/cloud breadth may require complementary tools.
- Language, module, certificate, and upgrade governance are specialized.

BASELINE SCORE PROFILE

Raw documented capability 83.7

Evidence-adjusted capability 49.2

GATE DISPOSITION

PASS - continuous desired-state server fleet | CONDITIONAL - agent and platform lifecycle

CANDIDATE DEEP DIVE / 03

CHEF INFRA

OPERATING MODEL

Agent-based configuration management using recipes, cookbooks, Policyfiles, Chef Infra Server, and client convergence.

DOCUMENTED STRENGTHS

- Powerful code-driven configuration model.
- Policyfiles support versioned dependency and run-list control.
- Mature convergence architecture and ecosystem.
- Strong fit for organizations with existing Chef engineering capability.

CAUTIONS AND PROOF OBLIGATIONS

- Ruby and cookbook engineering skill are required.
- Platform and product transitions must be evaluated.
- Agent, server, policy, and content lifecycle add complexity.

BASELINE SCORE PROFILE

Raw documented capability 81.4

Evidence-adjusted capability 47.9

GATE DISPOSITION

PASS - code-driven convergence for established Chef estates | CONDITIONAL - skills and product trajectory

CANDIDATE DEEP DIVE / 04

SALT

OPERATING MODEL

Event-driven remote execution and configuration-management platform using master/minion, states, pillars, reactors, and execution modules.

DOCUMENTED STRENGTHS

- Fast remote execution and event-driven operations.
- Flexible states, modules, targeting, and orchestration.
- Strong fit for large-scale operational control and reactive automation.
- Extensible Python-based architecture.

CAUTIONS AND PROOF OBLIGATIONS

- Master, key, event, and minion architecture require strong security and operations.
- Content and state complexity can become difficult to govern.
- Enterprise support, packaging, and lifecycle expectations need validation.

BASELINE SCORE PROFILE

Raw documented capability 83.2

Evidence-adjusted capability 48.9

GATE DISPOSITION

PASS - event-driven operations fabric | CONDITIONAL - security, content, and support model

ARCHITECTURE AND INTEGRATION FIT

THE PRODUCT IS ONLY ONE PART OF THE OPERATING SYSTEM

REFERENCE OPERATING LAYERS

01 Inventory, facts, targeting, and desired-state authority

02 Controller, server, master, agent, or execution environment

03 Content, modules, cookbooks, states, playbooks, policy, and secrets

04 Execution, convergence, orchestration, events, and remediation

05 Reports, evidence, recovery, content supply chain, and lifecycle

INTEGRATION BOUNDARIES

- Identity, secrets, PKI, SSH, and privilege management
- Git, artifact, collection, module, cookbook, and package registries
- CMDB, source of truth, ITSM, CI/CD, and policy
- Cloud, network, operating system, application, and endpoint platforms
- Observability, compliance, vulnerability, and security operations

ARCHITECTURE GATE

Every external dependency requires an owner, identity boundary, failure mode, evidence path, version policy, recovery procedure, and exit strategy.

SECURITY, OPERATIONS, LIFECYCLE, ECONOMICS, AND EXIT

CROSS-DOMAIN DECISION RECORD

SECURITY AND AUTHORITY

Identity, credentials, secrets, roles, privileged actions, signing, approvals, isolation, audit, and incident response must be tested as an integrated system.

RELIABILITY AND RECOVERY

Control-plane, data-plane, dependency, region, database, queue, network, and operator failures require defined degraded modes and recovery objectives.

CHANGE AND LIFECYCLE

Version, compatibility, migration, canary, rollback, content, plugin, provider, firmware, and decommission procedures are part of product fitness.

ECONOMICS AND CAPACITY

Licenses, metering, data, compute, hardware, storage, support, staffing, training, integration, migration, and opportunity cost require sensitivity analysis.

SOVEREIGNTY AND PRIVACY

Data location, support access, telemetry, subprocessors, encryption, key control, disconnected operation, and legal obligations must align with policy.

PORTABILITY AND EXIT

Configuration, policy, data, state, evidence, workflows, identities, and operational knowledge must be exportable and reconstructable.

DECISION OWNERSHIP

Architecture, security, operations, finance, procurement, legal, data, and service owners jointly accept the final profile, evidence, residual risk, and exit obligations.

RISK AND FAILURE REGISTER

SCENARIOS THAT CAN INVALIDATE A FEATURE-BASED SELECTION

ID	SEVERITY	FAILURE SCENARIO	REQUIRED TREATMENT
R-01	CRITICAL	Automation changes systems successfully but cannot prove intended service outcome.	PREVENT / DETECT / RECOVER / EVIDENCE
R-02	HIGH	Agent or controller compromise enables fleet-wide execution.	PREVENT / DETECT / RECOVER / EVIDENCE
R-03	HIGH	Content dependencies change without controlled locking or signing.	PREVENT / DETECT / RECOVER / EVIDENCE
R-04	HIGH	Dry-run behavior diverges from actual enforcement.	PREVENT / DETECT / RECOVER / EVIDENCE
R-05	MEDIUM	Desired-state engines fight manual incident recovery or application controllers.	PREVENT / DETECT / RECOVER / EVIDENCE
R-06	MEDIUM	Migration loses inventory semantics, encrypted data, schedules, reports, exceptions, and operator knowledge.	PREVENT / DETECT / RECOVER / EVIDENCE

RISK RULE

A candidate with an unresolved critical failure path cannot advance because optional capability, market position, or commercial discount cannot compensate for missing safety or recovery evidence.

CONTROLLED PROOF-OF-CAPABILITY PLAN

REPEATABLE SCENARIOS, INSTRUMENTATION, AND ACCEPTANCE

TEST 01

Manage representative Linux, Windows, network, cloud, middleware, and application targets.

TEST 02

Execute configuration, patch, compliance, orchestration, secret, and remediation workflows.

TEST 03

Test dry-run, check or noop mode, canary, concurrency, failure, retry, rollback, and recovery.

TEST 04

Inject controller loss, certificate expiry, repository outage, partial fleet reachability, and conflicting state.

TEST 05

Measure convergence time, drift detection, job throughput, operator effort, and evidence completeness.

TEST 06

Rebuild the control plane and representative nodes from versioned content and backups.

EVIDENCE PACKAGE

Preserve versions, architecture, configuration, data set, scenario, expected result, instrumentation, raw output, timing, failures, operator actions, deviations, acceptance state, owner, and artifact hashes.

CONDITIONAL RECOMMENDATION AND REVALIDATION

DECISION RECORD, ACCEPTANCE, AND NEXT EVIDENCE

RECOMMENDATION POSITION

- Select by enforcement model and target estate, not language preference alone.
- Require content-locking, secret, privilege, dry-run, and recovery evidence.
- Define which system owns each configuration domain.
- Revalidate quarterly and before major controller, agent, content, or packaging changes.

CANDIDATE	ADJ. SCORE	GATE POSITION	LAB STATE
Ansible AAP	51.8	PASS - agentless enterprise automation; CONDITIONAL - content quality and drift architecture	PENDING
Puppet	49.2	PASS - continuous desired-state server fleet; CONDITIONAL - agent and platform lifecycle	PENDING
Chef	47.9	PASS - code-driven convergence for established Chef estates; CONDITIONAL - skills and product trajectory	PENDING
Salt	48.9	PASS - event-driven operations fabric; CONDITIONAL - security, content, and support model	PENDING

REVALIDATION SCHEDULE

Review no later than 2026-10-24. Review earlier after a major release, commercial change, critical vulnerability, material outage, architecture transition, failed acceptance test, or change to the target workload profile.

SOURCE AUTHORITY AND REVISION

CURRENT EVIDENCE SNAPSHOT AND PUBLICATION HISTORY

SOURCE ID	PUBLISHER	TITLE	CHECKED
NIST-CSF-20	NIST	Cybersecurity Framework 2.0	2026-07-24
NIST-SP800-53	NIST	Security and Privacy Controls for Information Systems and Organizations	2026-07-24
CIS-CONTROLS	Center for Internet Security	CIS Critical Security Controls v8.1	2026-07-24
ANSIBLE-AAP	Ansible	Red Hat Ansible Automation Platform	2026-07-24
ANSIBLE-EE	Ansible	Ansible Execution Environments	2026-07-24
PUPPET	Perforce	Puppet Platform Components	2026-07-24
CHEF	Progress Chef	Chef Policyfiles	2026-07-24
SALT	Salt Project	Salt States	2026-07-24
SALT-TEST	Salt Project	Salt State Testing	2026-07-24

SOURCE POSITION

Official documentation and source repositories support the current capability model. Source records preserve publisher, title, URL, purpose, and review date in the machine-readable authority register. Commercial terms, performance, and environment-specific behavior remain unverified until controlled proof.

REVISION HISTORY

1.1.0-candidate / 2026-07-24 - permanent-publication rebuild using the final benchmark system, profile-specific rankings, evidence adjustment, mandatory gates, and controlled PoC requirements.