SYMBEEO

PUBLIC

REFERENCE ARCHITECTURE

Infrastructure automation for a multi-vendor estate: source of truth, pipeline, event-driven operations

CAPABILITY	DOCUMENT	VERSION	DATE
Automation	SRA-AUT-001	1.3	Nov 4, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SRA-AUT-001	Version	1.3
Issued	Nov 4, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.2, Oct 10, 2026
Capability	Automation	Author	Mark Winston
Role	Principal Network Architect		
Credentials	CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026 (version 1.2). Version 1.3 issued by Symbeeo, Nov 4, 2026.		
Sign-off	"The practice lead signs this document before any build proceeds under it."		

Contents

1 · Scope 3
2 · Requirements register 3
3 · Architecture overview 5
4 · Component design 5
5 · Options and platform choices 6
6 · Failure conditions 8
7 · Validation 8
8 · Operations and lessons learned 8
9 · Appendix 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] read on Sep 24, 2026 from the standard, the project's release page or the vendor's own documentation (URLs in §9) · [A] design assumption for a typical buyer, to be confirmed by the signing engineer. No figure comes from any prior engagement. No product is chosen here: products are options in §5, chosen by the comparison. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 27, 2026	1.0	First issue.
Oct 7, 2026	1.1	Two rules removed from the §9.1 table of industry rules.
Oct 10, 2026	1.2	Approval line now reads: approved by the Founder, issued by Symbeeo. Mark Winston remains the author.
Nov 4, 2026	1.3	Wording correction: how the comparison is described.

1 · Scope

Who it is for. The head of infrastructure whose network, security and cloud estate is still changed by hand, device by device, and who needs every change reviewed, tested, reversible and auditable — without adding headcount and without binding the estate to one vendor's controller.

Typical buyer [A]. The estate of SRA-NET-001's typical buyer: head office, three branches, two data centers, two hyperscaler accounts; about 350 managed devices from at least three vendors; a change team of six; an ITSM tool already holding change records.

What is in. Source of truth; repository and pipeline; configuration and infrastructure-as-code execution; telemetry and drift; event-driven remediation; the boundary for AI-assisted operations; secrets, identity and audit; break-glass. **What is out.** The designs being automated (SRA-NET-001, SRA-DC-001); zero-trust policy content (SRA-SEC-001 — its changes flow through this pipeline); the ITSM product.

Assumptions. Most devices expose a model-driven interface; the rest take templated CLI [A]. The out-of-band network of SRA-NET-001 §4.6 exists and is the break-glass path.

Related documents. Standards and releases listed with URLs in §9. Comparable published designs: Juniper JVD AI DC (Terraform-automation chapter), Arista DCI guide (failure chapter), Nutanix NVD-2031 (automation chapter).

2 · Requirements register

Each requirement is an outcome the build passes or fails, naming no product.

Table 2. Requirements register

#	Requirement	Value	Source
R1	Managed estate	6 sites · ≈ 350 devices · 3+ vendors · 2 cloud accounts	[A] input

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R2	Every managed device, interface, prefix and VLAN has one authoritative record from which its intended configuration is generated	100 %; zero unrecorded devices found by discovery	[A]
R3	Every change to intended configuration is committed to version control with author, independent reviewer and change reference	100 %; author ≠ reviewer	[A]
R4	Every proposed change is checked against a model of the whole network and blocked on any failed check	100 % of changes	[S] model-based analysis (Batfish class)
R5	A change set is applied to a device as one transaction or not at all	≥ 90 % of devices [A]; the rest by CLI with pre/post checks	[S] RFC 6241; gNMI Set is atomic
R6	Any automated change set can be returned to its prior state	≤ 15 min [A]	[A]
R7	A difference between intended and running configuration is reported	≤ 15 min after it occurs [A]	[A]
R8	Operational state is collected by subscription	on-change for state; ≤ 30 s sample for counters [A]	[S] gNMI Subscribe; RFC 8641
R9	A pre-approved event class starts its runbook without a human	≤ 60 s event to start [A]	[A]
R10	Any change outside the standard-change catalog has a named human approval recorded before execution	100 %	[A]
R11	An AI agent is read-only by default and cannot write without R10 approval	zero unapproved writes	[S] MCP Jul 28, 2026; NIST AI RMF
R12	No long-lived credential is stored in automation code or job definitions	lifetime ≤ job + 15 min [A]	[S] short-lived job tokens (AAP 2.7, tech preview)
R13	Every automated action is logged — actor, target, time, change, result — in a store the actor cannot alter	100 %; 13 months [A]	[A]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R14	Every automation artifact is built from version control with recorded provenance	SLSA Build L2 minimum [A]	[S] SLSA v1.2; NIST SP 800-218
R15	Every new template or runbook runs on a virtual replica of the affected topology before production	100 %; re-run on each OS baseline change	[S] containerlab class

Fifteen rows, every one with a number; seven cite a standard or project source for the mechanism, seven rest on typical-buyer assumptions, and R1 is an input, not a testable requirement.

3 · Architecture overview

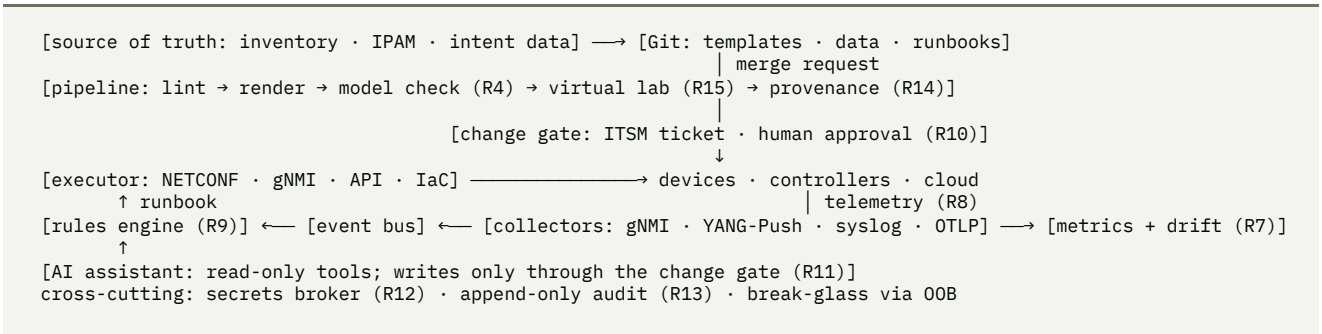


Figure 1. Automation loop

One loop: intent is data, data renders configuration, configuration is proven before it moves, and the network reports back so drift and events close the loop — RFC 9315's intent pattern [S] on standard interfaces.

4 · Component design

4.1 Source of truth.

One database for inventory, cabling, IPAM, VLANs, circuits and site variables (R2); configuration is rendered from it. Nightly discovery raises any unknown device [A]. Rejected: a vendor controller as source of truth — it records only its own devices.

4.2 Repository and pipeline.

Templates, data, rulebooks and IaC modules in Git; every change a reviewed merge request (R3). The pipeline lints, renders every affected configuration, runs §4.3, and signs the artifact with provenance at SLSA Build L2 (R14) [S]. Rejected: scripts run from laptops — no review, no provenance.

4.3 Validation and virtual lab.

Rendered configurations load into a network model that answers reachability, ACL and routing questions before anything moves (R4); Batfish v2026.08.27 is one open-source model [S]. New artifacts then run on a container-based

© 2026 Symbeeo. All rights reserved. · Public

replica (R15); containerlab v0.79.0 is one tool [S].

4.4 Execution.

NETCONF (RFC 6241) with candidate datastore and confirmed commit, or gNMI Set, which applies a request wholly or rolls it back [S] (R5, R6). Other devices take templated CLI with a stored rollback file. OS install, reboot and certificate rotation use gNOI where supported [S]. Fabric controllers and SD-WAN managers are driven through their APIs as targets, never bypassed.

4.5 Cloud infrastructure-as-code.

Cloud network constructs declared as code, remote encrypted state, plan reviewed in the merge request; open-source and source-available engines both meet R3–R6 (§5).

4.6 Telemetry and drift.

gNMI Subscribe (ON_CHANGE for state, SAMPLE for counters) or YANG-Push (RFC 8641) (R8) [S]; syslog and OTLP for the rest. Drift: rendered intent against running configuration after each change and every 15 minutes (R7) [A].

4.7 Event-driven operations.

Collectors publish to an event bus; a rules engine maps event classes to runbooks (R9). Only catalog runbooks run unattended; any other match opens a change (R10). A circuit breaker stops a runbook after three runs on one target in an hour [A].

4.8 AI-assisted operations.

An assistant may read the source of truth, telemetry, the model and job history. Any write it proposes becomes a merge request or a change awaiting a named human (R11). MCP Jul 28, 2026's multi-round-trip request, returning `input_required` when a tool needs confirmation, is the protocol stop [S]; NIST AI RMF 1.0 with profile AI 600-1 is the governance frame [S]. Rejected: autonomous write access.

4.9 Secrets, identity, audit.

Credentials issued per job and expiring with it (R12); per-RPC and per-path authorization through gNSI authz and pathz where supported [S]; every action to an append-only log outside the platform's own administration (R13).

4.10 Break-glass and lifecycle.

Named engineers keep console access over OOB when the platform is down; such changes are reconciled into the source of truth within one business day [A]. Platform components share the devices' software-baseline review.

5 · Options and platform choices

Patterns are chosen here; products are shortlisted for the comparison. One row per decision; every option considered is kept under its decision. [CMP] = decided by the comparison, not by this document.

© 2026 Symbeeo. All rights reserved. · Public

Table 3. Options and platform choices

ID	Decision	Requirement	Alternatives considered	Decision taken	Rationale
D1	How changes reach the estate	R2–R15	(a) source of truth + Git + pipeline + executor — meets §2; (b) one vendor's controller for the whole estate — fails R2; (c) scripts run from laptops — fails R3, R13, R14	(a)	(a) meets R2–R15 on standard interfaces [S]; (b) records only its own devices; (c) has no review, no provenance, no audit. Cost band: (a) mid · (b) mid–high · (c) low
D2	Source-of-truth product	R2	NetBox 4.7 (Sep 2, 2026) [S]; Nautobot 3.2 (3.2.5, Sep 15, 2026) [S] — both meet §2	[CMP]	Both open source sources of truth [S]; neither fails a requirement, so price and fit to the client's data decide. Cost band low–mid for both
D3	Executor and orchestration product	R5, R6, R9	ansible-core 2.21 / Ansible Automation Platform 2.7 (GA Jun 10, 2026) [S]; Cisco Crosswork NSO 6.7 [S] — both meet §2	[CMP]	Ansible: Event-Driven Ansible; MCP server in tech preview [S]; cost band low (core) / mid (platform). NSO: transactional multi-vendor orchestration [S]; cost band high
D4	Fabric-domain controllers	R5, R6	Nokia EDA 26.x · Apstra Data Center Director 6.x · Arista AVD 6.x [S] — each meets §2 within its own domain only	Driven as §4.4 targets, never bypassed; product [CMP] per domain	Fabric intent within one domain [S]; none can be the estate-wide source of truth (D1 b). Cost band mid
D5	Cloud infrastructure-as-code engine	R3–R6	OpenTofu 1.12 (MPL 2.0, CNCF sandbox) [S]; Terraform 1.16 (source-available) [S] — both meet §2	[CMP]	OpenTofu: client-side state encryption [S], cost band low. Terraform: widest provider ecosystem [S], cost band low–mid
D6	Event transport	R9	Apache Kafka 4.x (4.3.1, Jun 25, 2026) [S] — meets §2; NATS with JetStream (nats-server 2.15.0, Sep 17, 2026; CNCF incubating; Apache 2.0) [S] — meets §2 as a transport, but needs a source plugin the buyer writes, because the ansible.eda collection (2.13.0, Jul 7, 2026) ships a Kafka event source and no NATS source [S] (alternative added and read Sep 27, 2026)	[CMP]	Kafka: KRaft only since 4.0 [S]; a shipped rules-engine source; cost band low–mid. NATS: lighter to run [A]; the custom source is code the buyer maintains [A]; cost band low. Neither fails a requirement, so the comparison decides
D7	Metrics and drift store	R7, R8	Prometheus 3.x (3.15.0, Sep 25, 2026; Apache 2.0) [S] — meets §2; VictoriaMetrics (1.152.0, Sep 14, 2026; Apache 2.0) [S] — meets §2; Grafana Mimir (3.2.1, Sep 10, 2026; AGPL-3.0) [S] — meets §2 (alternatives added and read Sep 27, 2026)	[CMP]	All three accept OTLP metrics: Prometheus through its native receiver, off by default and switched on by a flag; VictoriaMetrics and Mimir at their own OTLP endpoints [S]. Mimir's AGPL-3.0 license must pass the buyer's licensing policy [S]. Cost band low (Prometheus, VictoriaMetrics) · low–mid (Mimir) [A]
D8	Write authority of the AI assistant	R10, R11	(a) read-only, writes only through the change gate; (b) autonomous write — fails R10, R11	(a)	MCP Jul 28, 2026 `input_required` is the protocol stop [S]; NIST AI RMF 1.0 with AI 600-1 is the governance frame [S]; (b) rejected (§4.8)

© 2026 Symbeeo. All rights reserved. · Public

6 · Failure conditions

Table 4. Failure conditions

#	Condition	What the user sees	Recovers by itself	Needs a hand	Time
F1	Executor node down	none; jobs queue	surviving nodes take jobs	replace	< 5 min [A]
F2	Source of truth down	none; pipeline halts closed	no	restore	≤ 1 h [A]
F3	Git service down	none; no new changes	no	restore	≤ 1 h [A]
F4	Push fails part-way	none, or brief loss on affected devices	transaction / runbook rollback	review	≤ 15 min (R6)
F5	Bad change passes validation	degraded service	post-change check fails; auto-rollback	root cause	≤ 15 min [A]
F6	Telemetry collector down	none; drift and events blind	second collector; heartbeat alarm	replace	< 1 min [A]
F7	Event storm	none	dampening; circuit breaker	review	seconds
F8	Runbook fights intent (loop)	possible flap	circuit breaker after 3 runs / h	fix intent or runbook	≤ 1 h [A]
F9	Secrets broker down	none; jobs fail closed	no	break-glass via OOB	minutes
F10	AI assistant proposes a wrong action	none	blocked at change gate	reviewer rejects	0

7 · Validation

None yet. The acceptance test at first build — a change set end to end, a forced partial-push rollback, drift injection, an event runbook under the circuit breaker, a secrets-broker outage, an AI-proposed write stopped at the gate — timed against §2 and recorded here makes this a validated architecture.

8 · Operations and lessons learned

Day 2: monthly review of the standard-change catalog and every circuit-breaker trip; quarterly re-run of the virtual-lab suite; weekly source-of-truth accuracy as the share of devices with zero drift; platform, collections and providers on the devices' quarterly baseline. Lessons: to be written by the signing engineer after the first build under this document.

9 · Appendix

Component list, typical buyer [A]: source of truth (HA pair, database replica) · Git with 3 CI runners · validation service · virtual-lab host (64 cores, 512 GB) · executor cluster (3) · rules engine (2) · event bus (3 brokers) · collectors (2) · metrics store (HA pair) · secrets broker (3) · append-only log store · read-only AI tool connector. All on SRA-NET-001's management network.

© 2026 Symbeeo. All rights reserved. · Public

References, read Sep 24, 2026: RFC 6241 · 7950 · 8040 · 8342 · 8639 · 8641, cited together in https://www.rfc-editor.org/rfc/rfc8641.html · RFC 9315 https://www.rfc-editor.org/rfc/rfc9315.html · gNMI 0.10.0 https://github.com/openconfig/reference/blob/master/rpc/gnmi/gnmi-specification.md · gNOI https://github.com/openconfig/gnoi · gNSI https://github.com/openconfig/gnsi · SLSA v1.2 https://slsa.dev/spec/ · SSDF (SP 800-218; r1 draft not final) https://www.nist.gov/news-events/news/2025/12/secure-software-development-framework-ssdf-version-12-available-public · NIST AI RMF https://www.nist.gov/itl/ai-risk-management-framework · MCP https://blog.modelcontextprotocol.io/posts/2026-07-28/ · Batfish https://github.com/batfish/batfish/releases · containerlab https://github.com/srl-labs/containerlab/releases · NetBox https://github.com/netbox-community/netbox/releases · Nautobot https://github.com/nautobot/nautobot/releases · ansible-core https://docs.ansible.com/ansible/latest/reference_appendices/release_and_maintenance.html · AAP 2.7 https://developers.redhat.com/articles/2026/06/10/whats-new-red-hat-ansible-automation-platform-2-7 · NSO https://nso-docs.cisco.com/releases · Nokia EDA https://documentation.nokia.com/eda/ · Apstra https://www.juniper.net/us/en/products/network-automation/apstra-data-center-director.html · AVD https://avd.arista.com/devel/docs/release-notes/6.x.x.html · OpenTofu https://opentofu.org/blog/opentofu-1-12-0/, https://www.cncf.io/projects/opentofu/ · Terraform https://github.com/hashicorp/terraform/releases · Kafka 4.0 https://kafka.apache.org/blog/2025/03/18/apache-kafka-4.0.0-release-announcement/ · Prometheus 3.0 https://prometheus.io/blog/2024/11/14/prometheus-3-0/.

References for D6 and D7 alternatives, read Sep 27, 2026: Kafka releases https://kafka.apache.org/community/downloads/ · nats-server 2.15.0 https://github.com/nats-io/nats-server/releases/tag/v2.15.0 · NATS at CNCF https://www.cncf.io/projects/nats/ · ansible.eda event sources https://github.com/ansible/event-driven-ansible/tree/main/extensions/eda/plugins/event_source · Prometheus releases https://github.com/prometheus/prometheus/releases and OTLP receiver https://prometheus.io/docs/guides/opentelemetry/ · VictoriaMetrics releases https://github.com/VictoriaMetrics/VictoriaMetrics/releases and OTLP ingestion https://docs.victoriametrics.com/victoriametrics/integrations/opentelemetry/ · Grafana Mimir releases https://github.com/grafana/mimir/releases and OTLP endpoint https://grafana.com/docs/mimir/latest/configure/configure-otel-collector/.

9.1 · Industry rules this architecture helps a buyer meet.

From Symbeeo's industry research of September 2026. Only rules that research links to this document's requirements are listed; rules it found this document does not address are left out.

Table 5. Industry rules this architecture helps a buyer meet

Rule	Jurisdiction	What it asks of infrastructure	Requirements here	Coverage
NERC CIP-010-4 (enforceable; CIP-010-5 from Jul 1, 2028)	US and Canada · Bulk Electric System entities	baseline configuration per asset, authorized and documented changes, baseline monitored at least every 35 days (high impact)	R3, R7, R13	partial
21 CFR Part 11 (electronic records; electronic signatures)	US · FDA-regulated records	secure, computer-generated, time-stamped audit trails	R13	partial
EU GMP Annex 11 Computerized Systems (2011 revision in force; the 2025 revision draft is not final)	EU · medicinal-product manufacturers	audit trail of changes to GMP data and systems	R13	partial

Naming a rule here is not a claim of compliance or certification: the buyer's assessor decides compliance, and Symbeeo holds no certification or authorization.

Sources for §9.1, read Sep 25, 2026: NERC CIP-010-4 [S] https://www.nerc.com/standards/reliability-standards/cip/cip-010-4 · 21 CFR Part 11 [S] https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 (text read on the

© 2026 Symbeeo. All rights reserved. · Public

eCFR) · EudraLex Volume 4, Annex 11 [S] https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en.

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SRA-AUT-001 · Version 1.3 · Nov 4, 2026