SYMBEEO

PUBLIC

DESIGN STUDY

Event-driven store operations for 450 retail stores, standard changes without a ticket queue

Complete design on current platforms

CAPABILITY	INDUSTRY	SETTING
Automation	Retail	Home-improvement retailer
DOCUMENT	**VERSION**	**DATE**
AUT-004	1.1	Oct 10, 2026

WRITTEN BY

Mark Winston, Principal Network Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	AUT-004	Version	1.1
Issued	Oct 10, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.0, Sep 27, 2026
Capability	Automation	Industry	Retail
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. Issued by Symbeeo, Oct 10, 2026. Design study: every figure is vendor-published, a design target or a marked assumption.		
Sign-off	"An engagement under this design is signed by the practice lead before any build proceeds."		

Contents

1 · Scope 3
1c · Public implementations this design follows 4
2 · Requirements register 4
3 · Architecture overview 5
4 · Design by subsystem 6
5 · Failure behavior 7
6 · Limits 7
7 · Lessons learned 7
8 · The author 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] figure read from the vendor's or project's own current page on Sep 24, 2026 · [S*] figure from the page's published summary where the page itself could not be opened · [A] design assumption, to be confirmed by the signing engineer · [T] design target: the record's outcome figure and anything derived from it. No figure comes from any engagement, file or asset. 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 10, 2026	1.1	Approval line now reads: approved by the Founder, issued by Symbeeo. Mark Winston remains the author.

1 · Scope

Who it is for. The head of IT operations at a retailer whose store network changes wait in a ticket queue for a central engineer, whose store openings need a technician on site for a day, and whose overnight alerts are read in the morning.

Typical buyer [A]. A home-improvement retailer with 450 stores in three countries. Per store: one Fortinet FortiGate firewall and three HPE Aruba Networking CX access switches — 450 firewalls and 1,350 switches, 1,800 devices in all. Stores connect over two broadband circuits. An IT operations team of twelve; about 25 store openings a year; an ITSM tool with a self-service catalog already used by store managers.

What is in. The source of truth for store devices; the standard-change catalog and its runbooks; store turn-up from data; event-driven remediation with throttling; per-job credentials; the audit trail. **What is out.** Store Wi-Fi; SD-WAN and firewall policy design (SEC practice); point-of-sale systems; the ITSM product; the WAN circuits.

Assumptions. Red Hat Ansible Automation Platform is the automation platform [A]. Each FortiGate and CX switch is reachable from the data center over the store's management tunnel [A]. Store devices send syslog and alerts to two central collectors [A]. The client's secrets broker can issue credentials to automation jobs [A].

Related documents, read Sep 24, 2026.

- SRA-AUT-001, Symbeeo reference architecture for infrastructure automation (the pattern this design applies)
- What's new in Red Hat Ansible Automation Platform 2.7 — https://developers.redhat.com/articles/2026/06/10/whats-new-red-hat-ansible-automation-platform-2-7
- ansible-rulebook, conditions and throttling — https://docs.ansible.com/projects/rulebook/en/latest/conditions.html
- ansible.eda collection, event sources — https://github.com/ansible/event-driven-ansible/tree/main/extensions/eda/plugins/event_source
- fortinet.fortios collection on Ansible Galaxy — https://galaxy.ansible.com/ui/repo/published/fortinet/fortios/
- arubanetworks.aoscx collection on Ansible Galaxy — https://galaxy.ansible.com/ui/repo/published/arubanetworks/aoscx/
- containerlab kinds (FortiGate, Aruba CX) — https://github.com/srl-labs/containerlab/tree/main/docs/manual/kinds
- Red Hat, European grocery retail group case study — https://www.redhat.com/en/resources/schwarz-group-case-study

© 2026 Symbeeo. All rights reserved. · Public

1c · Public implementations this design follows

Each row is labeled. **Public deployment**: a named operator's real deployment, published and dated by the operator, its vendor or a partner, used where one exists. **Our own design**: the dated vendor or standards documentation this design was built from, where no public deployment of the design exists. Labels and dates checked Sep 27, 2026.

Table 2. Public implementations this design follows

Implementation	Who published it · date	What it settles for this design	URL
Public deployment. A European grocery retail group moved store-server management for 12,500+ stores from Puppet to Ansible Automation Platform; 5,000+ jobs a day; applications deployed to all stores in one step; country administrators deploy without root access	Red Hat case study · Mar 1, 2021	§4.2 and §4.3: a retailer running store operations from one automation platform, with delegated rights instead of shared administrator access, at about 28 times this design's store count	`https://www.redhat.com/en/resources/schwarz-group-case-study`
Our own design, built from published documentation. Ansible Automation Platform 2.7: short-lived JSON web tokens scoped to jobs, users and organizations; MCP server integration in Technology Preview	Red Hat Developer · Jun 10, 2026	R7 and §4.6: per-job credentials are a product feature on the release this design uses; the MCP server is preview and stays out of scope	`https://developers.redhat.com/articles/2026/06/10/whats-new-red-hat-ansible-automation-platform-2-7`
Our own design, built from published documentation. ansible-rulebook throttling: `once_within` acts on the first match and suppresses further action until the window expires	Ansible project documentation, page undated · ansible-rulebook 1.3.2 released Sep 25, 2026	R5: the circuit breaker in SRA-AUT-001 §4.7 is a rulebook feature, not custom code	`https://docs.ansible.com/projects/rulebook/en/latest/conditions.html`

The retail group's case covers store servers, not store network devices, so it settles the operating model only; no figure from it enters the register.

2 · Requirements register

Table 3. Requirements register

#	Requirement	Value	Source
R1	Estate	450 stores · 450 FortiGate · 1,350 Aruba CX · 3 countries	[A]
R2	Standard-change catalog	12 catalog items run without an engineer once the ITSM request is approved	[T]
R3	Store turn-up	firewall and switches configured from the source of truth ≤ 1 h after the devices come online	[T]
R4	Event to runbook start	≤ 60 s	[T]

© 2026 Symbeeo. All rights reserved. · Public

#	Requirement	Value	Source
R5	Runbook throttle	first match acts; further matches on the same target suppressed for 1 h	[S] ansible-rulebook `once_within`; [T] window
R6	New event rule	notify-only for 2 weeks before it acts	[T]
R7	Credentials	job-scoped short-lived tokens; no stored device password in any job	[S] AAP 2.7
R8	Device content	`fortinet.fortios` 2.6.0 · `arubanetworks.aoscx` 4.5.2	[S] Ansible Galaxy
R9	Event transport	Kafka and webhook event sources	[S] `ansible.eda` 2.13.0
R10	Rollback, one store	≤ 15 min	[T]
R11	Drift, store devices	reported ≤ 4 h	[T]
R12	Audit	every job and rulebook action logged with actor, target, time, result; 13 months	[A]

Twelve rows; four carry a vendor figure, two are design assumptions, six are design targets.

3 · Architecture overview

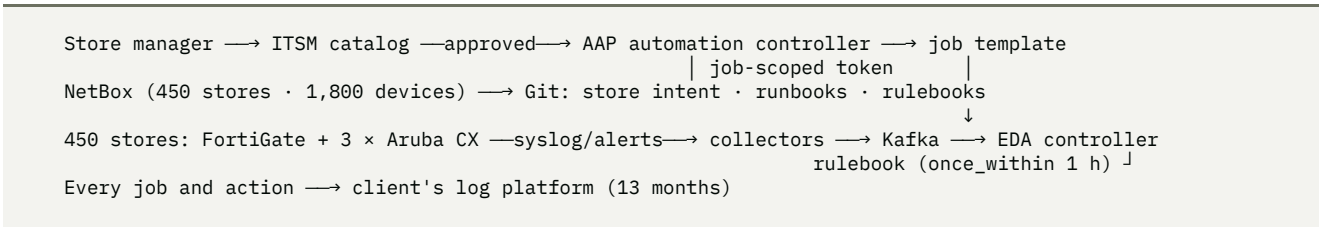


Figure 1. Store automation, catalog and event paths

Two ways into the same job templates: a store manager's catalog request, or an event from the store's own devices. Both run the same reviewed code with a credential that dies with the job, and both leave the same audit line.

Table 4. Architecture overview

Role	Product (exact version)	Qty	Capacity used	Why this unit
Automation controller	Red Hat Ansible Automation Platform 2.7 [S]	3 nodes [A]	1,800 devices, ≈ 40 catalog jobs a day [A]	job-scoped tokens [S]
Event-driven controller	Event-Driven Ansible, AAP 2.7 [S]	2 nodes [A]	10 rulebook activations [A]	rulebooks with throttling [S]
Firewall content	`fortinet.fortios` 2.6.0 [S]	1	450 FortiGate	Fortinet-published collection [S]
Switch content	`arubanetworks.aoscx` 4.5.2 [S]	1	1,350 CX	HPE Aruba Networking-published collection [S]
Source of truth	NetBox 4.7.1 [S]	HA pair [A]	450 sites [A]	store templates by site [A]

© 2026 Symbeeo. All rights reserved. · Public

Role	Product (exact version)	Qty	Capacity used	Why this unit
Event bus	Apache Kafka 4.x [S]	3 brokers [A]	1,800 devices' alerts [A]	`ansible.eda` Kafka source [S]
Replica	containerlab v0.79.0, FortiGate and Aruba CX kinds [S]	1 host	one model store, 4 nodes [A]	both store vendors in software [S]

4 · Design by subsystem

4.1 Source of truth and store template.

NetBox holds each store as a site with its four devices, prefixes, VLANs and circuits [A]. A store is rendered from one template plus its site variables, so 450 stores are 450 rows of data, not 450 configurations to edit [A]. Rejected: per-store configuration files — the first chain-wide change touches 1,800 files.

4.2 Standard-change catalog.

Twelve catalog items, each one job template: move a switch port to another VLAN; bounce PoE on a port; enable or disable a port; add a store-local printer reservation; point a store's devices at new NTP and syslog targets; open a temporary vendor access rule for 4 hours; and six more agreed with the change manager [A]. The ITSM request carries store and port; the job reads everything else from NetBox [A]. Anything outside the catalog opens a normal change (SRA-AUT-001 R10).

4.3 Store turn-up.

Devices arrive with a bootstrap configuration that calls home over the management tunnel [A]; the turn-up job renders the store's full configuration from NetBox and applies it, then runs post-checks (both WAN circuits up, uplinks up, VLANs present) [A]. The target is under an hour from power-on to configured (R3) [T]; the technician's day on site becomes racking and cabling.

4.4 Event-driven remediation.

Collectors publish store alerts to Kafka; Event-Driven Ansible consumes them through the `ansible.eda` Kafka source [S]. First rules: switch port flapping more than 5 times in 10 minutes — shut the port, open an incident; a WAN circuit down — collect diagnostics from the FortiGate, open an incident with them attached; a catalog field changed by hand — restore the intended value [A]. Each rule uses `once_within` of one hour per device **[S][T]**, so a storm acts once. Every new rule runs notify-only for two weeks first (R6) [T].

4.5 Test before stores.

A containerlab replica of one model store — a FortiGate and three Aruba CX nodes — runs every new job template and rulebook before production **[S][A]**. A new template then goes to 3 pilot stores, then 10 % of stores, then all, a day apart [A]. Rollback is the previous rendered configuration re-applied, ≤ 15 minutes per store (R10) [T].

4.6 Credentials, audit and AI.

Jobs authenticate to devices with credentials issued for the job; AAP 2.7 scopes short-lived tokens to jobs, users and organizations [S] (R7). Every job and rulebook action goes to the client's log platform (R12) [A]. AAP 2.7's MCP server is in Technology Preview [S] and is not enabled in this design [A].

© 2026 Symbeeo. All rights reserved. · Public

5 · Failure behavior

Table 5. Failure behavior

Failure	Behavior	Source
Store management tunnel down	jobs to that store fail and retry; the store keeps trading on its running configuration	[A]
Event storm from one store	first event acts; the rest suppressed for 1 h per device	[S] `once_within`; [T] window
Rule contradicts intent (port shut, then restored by drift rule)	second action suppressed by the same throttle; loop raises a ticket	[A]
Automation controller node down	jobs run on surviving nodes	[A]
Kafka broker down	two remaining brokers carry events	[A]
Secrets broker down	jobs fail closed; engineers use break-glass access over the store's out-of-band modem	[A]
Bad template reaches pilot stores	pilot stops the rollout; 3 stores rolled back ≤ 15 min each	[T]

6 · Limits

- The device counts, catalog size and job rate are assumptions; three months of store tickets set the real catalog.
- Drift is reported within 4 hours, not the reference architecture's 15 minutes, to keep polling off store broadband; a store change made by hand can stand for that long.
- The replica runs virtual FortiGate and Aruba CX images; PoE and hardware-specific behavior is proved only at the pilot stores.
- Collection versions move; the design pins the versions tested and upgrades them on the quarterly baseline.
- The retail group's case study is about store servers, not store networks; it shows the operating model at scale, not this design.

7 · Lessons learned

None yet — this is a design study; populated after the first build against it.

© 2026 Symbeeo. All rights reserved. · Public

8 · The author

WRITTEN BY

Mark Winston

Principal Network Architect

CCIE, CISSP, CCSP, CCISO, CISM, Adopting Zero Trust (Forrester)

Signed off by Edwin Ozer, Founder.

© 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.

AUT-004 · Version 1.1 · Oct 10, 2026