A webinar by IT-Conductor™

Autonomous Patching Without Downtime



REGISTER NOW

Wednesday, August 12th, 2026

8:30 AM PDT | 11:30 AM EDT | 5:30 CEST

Hosted by Linh Nguyen,
CEO, and Co-Founder of IT-Conductor

PART OF A SERIES

Building toward one idea, one session at a time

SESSION 1

Why existing SAP security approaches leave a remediation gap

SESSION 2

Why SAP needs its own cyber operations platform

SESSION 3

Anatomy of an SAP cyber attack

SESSION 4

The Four Pillars of SAP Autonomous Cyber Operations

SESSION 5 · TODAY

Autonomous Patching Without Downtime

THE OPERATIONAL REALITY

Patching is essential. It’s also operationally brutal.

Kernel updates, HANA revisions, Host Agent updates, SAP Security Notes, Security HotNews — all essential, all demanding: careful planning, multiple approvals, maintenance windows, extensive validation.

This session lands the day after SAP Patch Day — we’ll also walk through this month’s most significant Security Notes and how to prioritize them.

The goal isn’t zero downtime everywhere. It’s eliminating unnecessary downtime through design.

REFRAMING THE GOAL

Three categories, one objective

1

True Zero-Downtime

Patch occurs with no application interruption.

2

Minimal Downtime

Brief failover or restart — seconds to a few minutes.

3

Maintenance Window Required

Outage or rolling maintenance can’t fully eliminate interruption.

The objective of SACO isn’t “zero downtime everywhere.” It’s eliminating unnecessary downtime through architectural design and orchestration.

THE DOWNTIME MATRIX

Most of the SAP stack can patch without downtime

COMPONENT	CAN PATCH LIVE?	REQUIREMENT
SAP Host Agent	Yes	Restart Host Agent only
SAP Web Dispatcher	Yes	Active/Standby or load balanced
SAP Cloud Connector	Yes	HA pair
SAP Router	Yes	Two routers / network failover
ABAP Application Servers	Yes	Drain users, then restart
SAP Kernel	Minimal	Rolling across app servers
Central Services (ASCS/ERS)	Minimal	ENSA2 + HA
HANA Primary Database	Minimal	Takeover required
SAP Gateway / ICM	Minimal	Multiple app servers, rolling

THE EXCEPTIONS

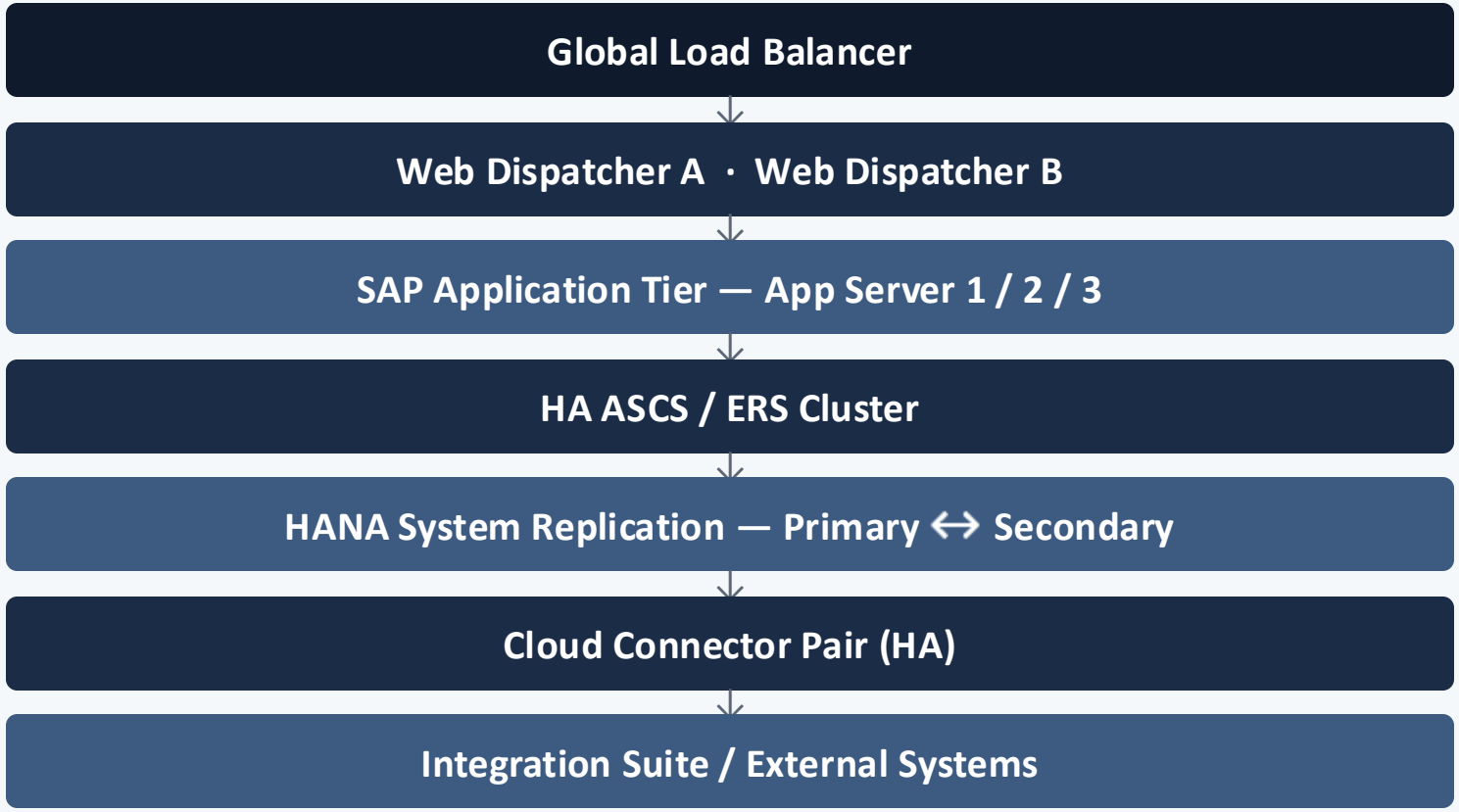
Some components are generally impossible to patch live

- Major SAP kernel upgrades
- HANA revision upgrades on standalone systems
- OS kernel updates without live patching
- Firmware
- BIOS
- SAN firmware
- Hypervisor upgrades
- Single-instance ABAP / standalone ASCS without clustering

These become minimal-downtime only through infrastructure design — not through the patch itself.

DESIGNING FOR RESILIENCE

The architecture that makes it possible



KEY PRINCIPLES

- No single points of failure
- Every SAP service has redundant capacity
- Patch one component while traffic shifts elsewhere
- Automatic health checks before failover

HOW SACO ORCHESTRATES IT

Intelligence. Dependency Mapping. Autonomous Orchestration.

1

Intelligence

Collect Security Notes, CVEs, and patch data; correlate with what's actually installed and exposed.

2

Dependency Graph

Map prerequisites, incompatible revisions, sequencing, and rollback points before touching anything.

3

Autonomous Orchestration

Execute component-specific, tested playbooks with health validation and rollback built in.

PHASE 1 OF 3

Intelligence — every Patch Tuesday

COLLECT

- SAP Security Notes
- HANA revisions
- Kernel patches
- Host Agent updates
- Cloud Connector updates
- OS CVEs
- Hypervisor patches
- Firmware advisories

CORRELATE WITH

- Installed versions
- Running kernel
- Component inventory
- Exposure
- Internet accessibility
- Business criticality

PHASE 2 OF 3

Dependency graph — nothing patches in isolation

Kernel

- Host Agent
- Database Client
- Enqueue, Message Servers
- JVM
- Application Servers

Database Revision

- Kernel Compatibility
- ABAP Compatibility
- Backup Validation
- System Replication

SACO determines: prerequisite patches · incompatible revisions · sequencing · rollback points

PHASE 3 OF 3

Autonomous orchestration — component by component

COMPONENT	SEQUENCE	DOWNTIME
Host Agent	Drain → Install → Restart → Health Check → Resume	None
Cloud Connector	Fail to Secondary → Patch Primary → Validate → Fail back → Patch Secondary	None
Web Dispatcher	Remove from LB → Patch → Restart → Health Check → Return to LB	None
Application Server	Disable logon → Drain → Restart → Kernel update → Health Check → Enable logon	None for users
HANA	Patch Secondary → Replication catch-up → Takeover → Patch former Primary → Re-establish	30–90 sec
ASCS	Failover → Patch inactive node → Switch → Patch second node	Seconds

BEFORE ADVANCING

Every step is validated automatically

INFRASTRUCTURE

- CPU
- Memory
- Disk
- Network

SAP

- disp+work
- Message Server
- Gateway
- ICM
- RFC
- Background Jobs
- Lock Table

DATABASE

- Replication
- Log shipping
- Backups
- Alerts

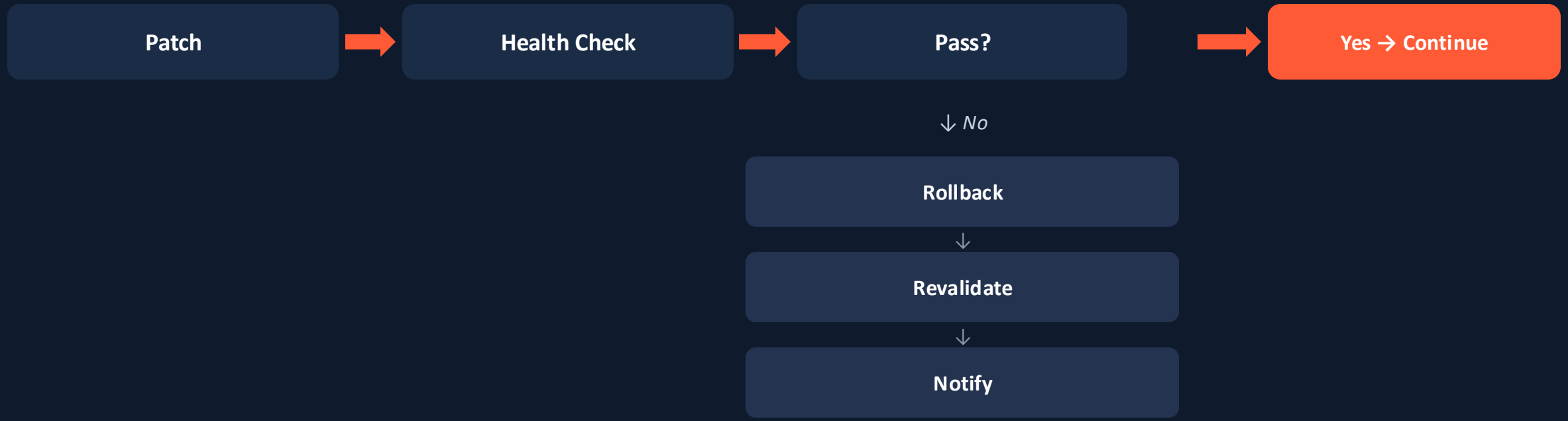
BUSINESS

- Login
- Business transactions like VA01, ME23N, etc.
- Reports
- Fiori launchpad
- RFC ping
- IDoc
- OData

Only proceed when all validations pass.

WHEN SOMETHING DOESN'T PASS

Every patch has a deterministic rollback



Deterministic, well-suited to automation — not a judgment call under pressure.

WHERE DOES YOUR ORGANIZATION STAND?

The SACO Autonomous Patching Maturity Model

LEVEL	CAPABILITY	DOWNTIME
Level 1	Manual patching	Hours
Level 2	Automated installation	30–60 min
Level 3	Rolling application servers	5–15 min
Level 4	HANA replication with automated takeover	< 2 min
Level 5	Full autonomous patch orchestration, health validation, and rollback across the SAP landscape	Seconds to ~2 min

PUTTING IT ALL TOGETHER

The SACO reference architecture

1 Discovery

Inventory SAP Kernel, ABAP, HANA, Host Agent, Cloud Connector, Web Dispatcher, JVM, OS, and infrastructure versions.

2 Risk Correlation

Map SAP Security Notes and CVEs to deployed components; identify exploitable exposure.

3 Change Planning

Build dependency-aware patch plans with sequencing, compatibility validation, and rollback checkpoints.

4 Resilient Execution

Use rolling restarts, clustered services, load balancers, and HANA System Replication to minimize impact.

5 Autonomous Validation

Execute technical and business health checks after each patch before advancing.

6 Continuous Assurance

Record evidence, update baselines, and recalculate cyber risk posture after remediation.

THE TAKEAWAY

“Most of the SAP stack can be patched with no user-visible outage. The rest can be reduced to controlled, automated failovers measured in seconds.”

This turns patching from a periodic scramble into a continuous cyber resilience capability — maximizing availability while accelerating the deployment of critical security fixes.

COMING UP

This is session 5 of the series

SAP AUTONOMOUS CYBER OPERATIONS

More sessions are on the way

We’re continuing to build out SAP Autonomous Cyber Operations as a series — stay registered for details on what’s next.

Watch your inbox for the next session announcement.

TAKE THE NEXT STEP

Begin your SAP Autonomous Cyber Operations journey

Start with an assessment to identify:

- Operational gaps
- Remediation bottlenecks
- Automation opportunities

Request a SAP Security Operations Assessment

Questions?