Network state audit

Evaluate captured operational command results against defined rules and retain findings for review.

The business requirement

Configuration policy and actual operating behavior answer different questions. A device can retain an approved configuration while an interface or protocol state violates an operational requirement. Gluware's audit capability can evaluate captured operational evidence through Config Drift & Audit, alongside configuration checks.



HOW THE CAPABILITY WORKS

Define operational capture scope

Use standard or vendor/OS-scoped custom operational command sets in Config Drift & Audit. Select the supported command outputs that contain the evidence required by the operational control.

Express the required conditions

Build audit rules that evaluate the captured output for required or forbidden conditions. Use regular expressions and the appropriate scope to identify the evidence the policy needs.

Run and inspect the audit

Capture results and run the policy on demand, scheduled with email notification, through a syslog-triggered process, or through Network RPA. Inspect findings, integrated logs, and detailed audit reports.

Coordinate follow-up and evidence

Use Network RPA to route failures to investigation or supported corrective tasks. Re-capture and reassess the specified condition. Data Explorer can summarize stored data; optional Git integration preserves audit-policy history.

Network state audit

Connect the operating process to defined component responsibilities.

COMPONENTS DELIVERING THE CAPABILITY

Config Drift & Audit	Owns operational command capture, audit policy, evaluation, logs, and results.
Device Manager	Supplies device and fleet context.
Network RPA	Coordinates capture, audit, investigation, and follow-up.
Data Explorer	Builds reusable reports from stored data.
Version Control	Synchronizes supported audit policies to Git for backup/restore.

OPERATING SCOPE

Config Drift & Audit: captured command results

Capture configuration and operational command results, compare snapshots to identify drift, and evaluate audit policies for required or forbidden conditions. Installed modeling Concept Items can scope the audit inputs.

Config Model Editor: separate state assessments

Run CLI/API state assessments on demand, as pre/post checks while provisioning, or through a Network RPA task.

Network RPA: process coordination

Connect targets, tasks, variables, conditions, scheduling, triggers, and notifications across Gluware applications and external systems. Each task uses its supported application or execution mechanism.

Business value and measurement

Measure the operational controls covered, failed conditions, recurring exceptions, and time to a verified result. This capability evaluates captured operating evidence. Config Model Editor's CLI/API state assessments provide a separate on-demand and pre/post-change check path.

Technical documentation | Request a demo

Audit and operational control background