DemandFlow Network Discovery and Audit

DEMANDFLOW®

Read the live network, compare it with the record, and change the record only through review

DATA SHEET

Every network inventory drifts. Devices are swapped, interfaces re-cabled, versions upgraded and adjacencies formed that the record never hears about, until a change built on the documented network fails against the real one. The usual answer is a discovery tool that overwrites the inventory with whatever it saw last, so the documented design disappears and the audit trail with it.

DemandFlow® keeps the documented network and the observed network side by side. A collector or an existing source reads what is live, reconciliation matches it to the records one to one, and the differences become proposals that a reviewer approves into a single network change. The record is never overwritten by a run, and every command the collector sends is logged.

What it is

A discovery, reconciliation and audit layer for the telco and data centre estate: scheduled or on-demand discovery from the DemandFlow collector, IP Fabric, NetBox, file upload or AWS, Azure and GCP; snapshots stored as tables and browsed in the platform; drift between documented and observed for devices, interfaces, links and peerings; a drift-to-proposal-to-change workflow; snapshot diffs before and after a change; running configuration capture with secrets scrubbed; CVE correlation against device operating systems; intent rules that run on every snapshot; and a command-level audit trail of everything the collector did.

It sits inside DemandFlow, so a drift item becomes a network change with work order lines, a new vulnerability lands on the device that carries the services, and a silent collector raises a SIEM alert like any other source.

What an operator gets

- **Read only, outbound only.** The collector runs as a container or OVA inside your network, makes outbound HTTPS calls only and never listens; devices are read by SNMP, gNMI and SSH with credentials held locally or fetched into memory at run time.
- **The record is never overwritten.** Documented records are annotated with what was last seen; the only automatic write is ports for new interfaces on matched devices. Devices are never created by a run.
- **Drift you can see.** A drift map with links in both, documented but not observed, observed but not documented and wrong adjacency, with matched, new, missing and changed counts per snapshot.
- **Change through review.** Tick drift items, raise proposals, approve or reject with a reason, and the approved set becomes one network change with the decision history kept.
- **Before and after proof.** Pre-change and post-change snapshots taken on change status moves, with a diff and a green, amber or red verification.
- **Vulnerabilities on the device.** Device OS versions correlated daily against the NVD and CISA KEV, with triage that survives re-runs.
- **An audit trail per command.** Every device command, credential fetch, enrolment attempt and proposal decision recorded; silence raises an alert.
- **Configs with secrets scrubbed.** Running configurations captured over SSH, scrubbed on the collector and again on store, with a side-by-side diff.

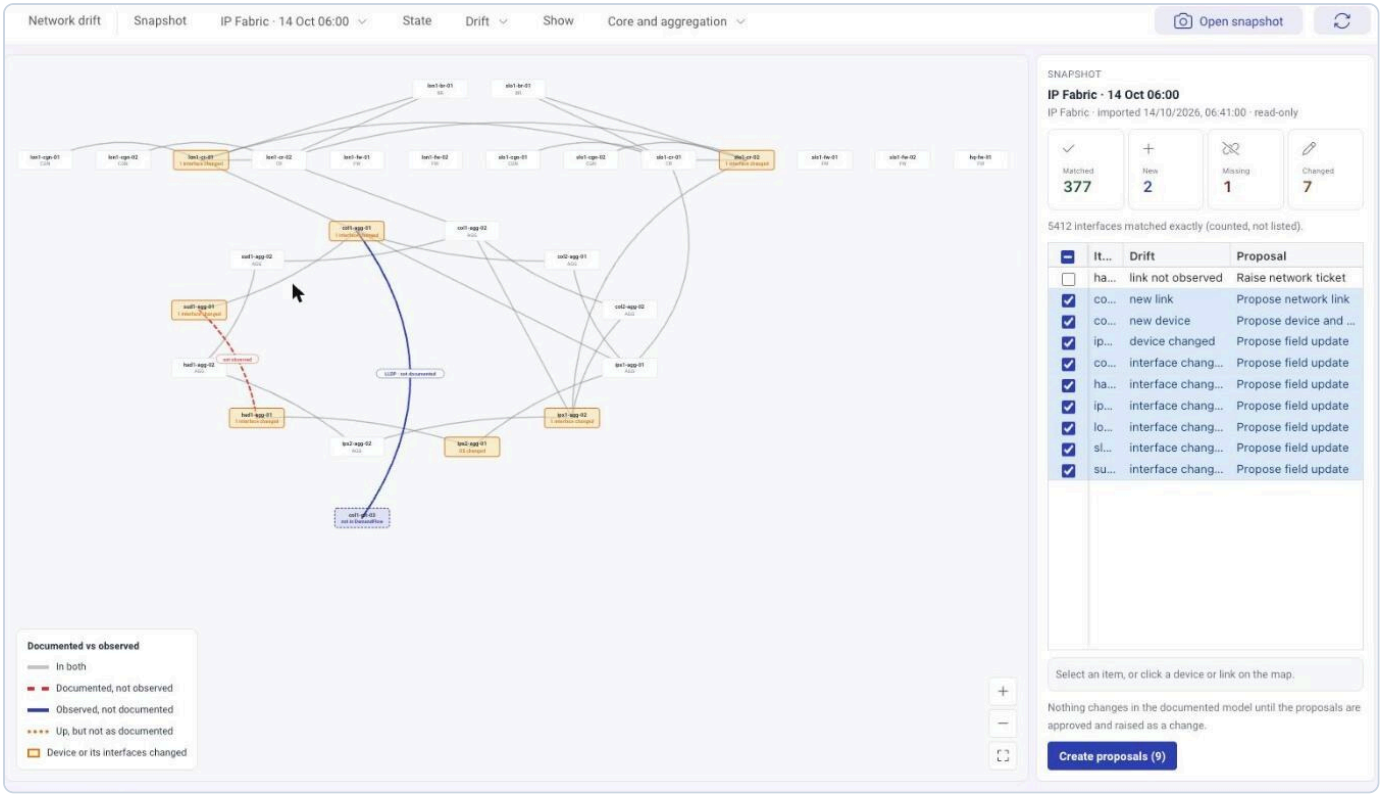

FIGURE 1. NETWORK DRIFT FOR AN IP FABRIC SNAPSHOT OF 145 DEVICES: 377 MATCHED, 2 NEW, 1 MISSING AND 7 CHANGED, WITH THE DRIFT DRAWN ON THE DOCUMENTED TOPOLOGY AND EACH ITEM CARRYING ITS PROPOSAL

Sources and the collector

The DemandFlow collector ships as an OCI container for amd64 and arm64 or as an OVA, installs in under thirty minutes and needs 1 vCPU and 1 GB as a container or 2 vCPU, 4 GB and 20 GB as an appliance. It enrols with a one-time activation key, receives its own collector key, and from then on polls for jobs over outbound HTTPS. It runs as an unprivileged user on a read-only root filesystem, and upgrades are signed with SHA-256 and ECDSA P-256 with rollback on the OVA.

Drivers: SNMP v2c and v3 (IF-MIB, ENTITY-MIB, LLDP-MIB, ARP and MAC tables, with an LLDP crawl), gNMI OpenConfig (devices, interfaces, LLDP, BGP, IS-IS, routes, ARP and MPLS LSPs, with crawl), SSH CLI for running configurations and state on Cisco IOS XE, NX-OS and IOS XR, Arista EOS, Juniper Junos and Nokia SR OS, and read-only hypervisor inventory from vSphere, libvirt and Proxmox. A crawl follows neighbours to 2,000 devices and 16 hops; eight devices are read in parallel; a failed device never stops a run, which completes as partial. Interface counters are read every five minutes and rolled up hourly onto ports and links.

Source	What it reads
DemandFlow collector	SNMP, gNMI, SSH CLI and hypervisors inside your network; optional address sweep, off by default, whose finds become proposals only
IP Fabric	Technology tables in pages of 1,000: devices, interfaces, neighbours, ARP, MAC, routes, BGP, IS-IS, OSPF
NetBox	Preview first, then one-way sync into a snapshot
File upload	Device and interface tables from a file
AWS, Azure, GCP	Networks, subnets, routes, gateways and peerings, read only through an assumed role and Describe calls

Jobs run manually, daily or weekly at a chosen UTC time, or on demand with Run now. Scope is a set of sites, a collector and include or exclude prefixes, and the

documented side of a reconciliation is limited to the same scope. One run per job at a time; a run with fifteen minutes of silence is marked failed.

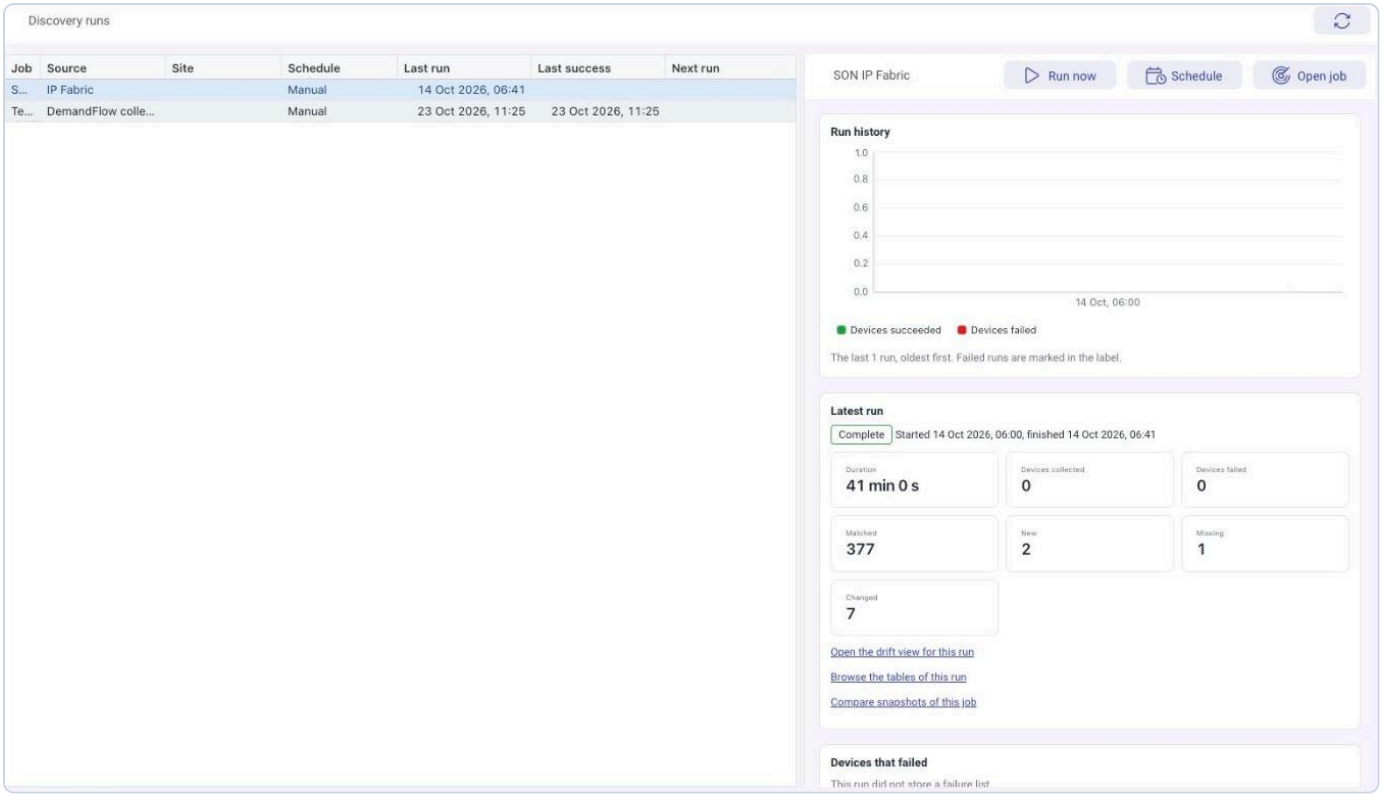

FIGURE 2. DISCOVERY RUNS: JOBS WITH THEIR SCHEDULE, LAST RUN AND LAST SUCCESS, AND THE LATEST RUN'S DURATION, COUNTS AND LINKS TO THE DRIFT VIEW, THE STORED TABLES AND THE SNAPSHOT COMPARISON

Snapshots and reconciliation

Each run produces a snapshot with a status (running, complete, partial, failed or expired), a role (scheduled, on demand, pre-change or post-change) and counts of devices, interfaces, neighbours, ARP and MAC entries, routes, BGP sessions and IS-IS and OSPF adjacencies, with devices collected and failed. The tables are stored as Parquet and browsed in grids inside the platform. Snapshots are retained for ninety days.

Reconciliation matches observed devices to documented ones by serial, then hostname, then management IP, one to one; interfaces by canonical name; links from LLDP and CDP, IGP adjacencies and /31 and /30 pairs. Each item is matched, new, missing or changed, and changed fields are listed: OS version, serial, hostname, management IP and model on a device; admin and operational status, speed and MAC on an interface. Matched records are annotated with last seen, match status and the observed values, never overwritten. BGP and IS-IS sessions become peerings; hypervisor inventory becomes clusters, hosts, VMs, virtual switches and port groups.

From drift to change. On the drift screen, tick the items to act on and raise proposals. A reviewer approves or rejects each with a reason, and the approved proposals become one network change: logical items applied, physical items as work order lines. A Decided view shows who decided what and why, with acceptance-rate tiles over thirty days.

Snapshot diff. Compare any two snapshots of a job, or a snapshot with the documented network. Moving a change to its implementation window takes a pre-change snapshot; closing it takes a post-change one; the diff verifies the change green, amber or red.

Topology states. The topology viewer draws the documented network, the latest observed network or the drift between them, with link styles for in both, documented not observed, observed not documented and wrong adjacency.

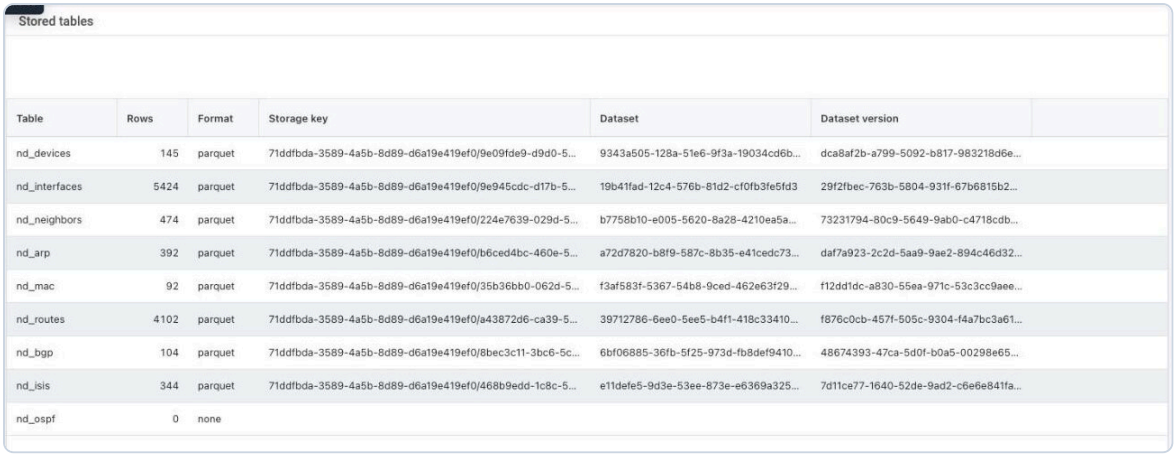
Stored tables

Table	Rows	Format	Storage key	Dataset	Dataset version
nd_devices	145	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/9e09fde9-d9d0-5...	9343a505-128a-51e6-9f3a-19034cd6b...	dca8af2b-a799-5092-b817-983218d6e...
nd_interfaces	5424	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/9e945cdc-d17b-5...	19b41fad-12c4-576b-81d2-cf0fb3fe5fd3	29f2fbec-763b-5804-931f-67b6815b2...
nd_neighbors	474	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/224e7639-029d-5...	b7758b10-e005-5620-8a28-4210ea5a...	73231794-80c9-5649-9ab0-c4718cdb...
nd_arp	392	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/b6ced4bc-460e-5...	a72d7820-b8f9-587c-8b35-e41cedc73...	daf7a923-2c2d-5aa9-9ae2-894c46d32...
nd_mac	92	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/35b36bb0-062d-5...	f3af583f-5367-54b8-9ced-462e63f29...	f12dd1dc-a830-55ea-971c-53c3cc9aee...
nd_routes	4102	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/a43872d6-ca39-5...	39712786-6ee0-5ee5-b4f1-418c33410...	f876c0cb-457f-505c-9304-f4a7bc3a61...
nd_bgp	104	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/8bec3c11-3bc6-5c...	6bf06885-36fb-5f25-973d-fb8def9410...	48674393-47ca-5d0f-b0a5-00298e65...
nd_isis	344	parquet	71ddfbda-3589-4a5b-8d89-d6a19e419ef0/468b9edd-1c8c-5...	e11defe5-9d3e-53ee-873e-e6369a325...	7d11ce77-1640-52de-9ad2-c6e6e841fa...
nd_ospf	0	none			

FIGURE 3. A SNAPSHOT'S STORED TABLES: DEVICES, INTERFACES, NEIGHBOURS, ARP, MAC, ROUTES, BGP AND IS-IS HELD AS PARQUET WITH THEIR DATASET VERSIONS

Configurations, vulnerabilities and intent

Configurations. Running configurations are captured over SSH, scrubbed of secrets on the collector and checked again on store, which refuses any body still holding one. Each configuration record carries a hash, line count, masked flag and whether it changed since the previous capture; the Config panel shows a side-by-side diff that ignores volatile lines.

Vulnerabilities. A shared corpus of the NVD 2.0 feed and the CISA Known Exploited Vulnerabilities list is refreshed daily at 03:00 UTC. Each device's OS version maps to a network OS record with its CPE, which is matched against the corpus to produce one vulnerability per device and CVE with severity, CVSS score, KEV flag, fixed-in version and triage state (open, investigating, fixed, risk accepted, false positive). Re-runs keep triage and flip non-matching items to fixed; a change of OS version re-correlates that device.

Intent rules. Rules run on every snapshot and raise findings: two built in (every access link has a diverse backup; no VRF leaks) and customer rules written as SQL against the snapshot tables in a sandboxed engine. Field evidence records the source, date and confidence of each device field, and data quality and service completeness screens score the estate.

Audit trail. Every command the collector issues is one audit line with the command and its result, never the output or the credentials, uploaded in batches of up to 500 at least hourly as SIEM log rows under a per-collector source. Every credential fetch is logged by name and job, never value. Enrolment attempts are immutable, proposal decisions record who, when and why, and a silent collector raises an absence alert; collector health is swept every five minutes.

Two estates. The telco and data centre estate and the IT estate are separate entity sets with separate collectors and keys, never one data set with a filter.

Security of collection

Device credentials are held on the collector in a file that must not be readable by other users, or fetched from the DemandFlow vault at run time into memory only; the cloud side releases only the secrets that the collector's own jobs name, encrypted under KMS with the tenant as context. Activation and collector keys are stored as SHA-256 hashes; activation keys carry an expiry, a maximum number of enrolments and an IP allow list, and re-enrolling a collector revokes its old key. NETCONF and device REST APIs are not used. Nothing is pushed to a device.

Summary of specifications

Item	Detail
Collector	OCI container (amd64, arm64) or OVA; outbound HTTPS only; container 1 vCPU, 1 GB, 1 GB; OVA 2 vCPU, 4 GB, 20 GB; unprivileged user, read-only root; signed upgrades (SHA-256, ECDSA P-256) with OVA rollback; heartbeat 300 s

Item	Detail
Drivers	SNMP v2c/v3 (GET, GETBULK; IF-MIB, ENTITY-MIB, LLDP-MIB, ARP, MAC); gNMI OpenConfig; SSH CLI on Cisco IOS XE, NX-OS, IOS XR, Arista EOS, Juniper Junos, Nokia SR OS; vSphere, libvirt, Proxmox read only
Run limits	Crawl 2,000 devices, depth 16; 8 parallel workers; 3,600 s deadline; partial on device failure; sweep up to 4,096 addresses at 100 probes/s, off by default
Other sources	IP Fabric (pages of 1,000), NetBox (preview then sync), file upload, AWS/Azure/GCP read only
Scheduling	Manual, daily or weekly at HH:MM UTC (default 02:00), Run now; one run per job; failed after 15 min silence; scope by sites, collector, include and exclude prefixes
Snapshots	Devices, interfaces, neighbours, ARP, MAC, routes, BGP, IS-IS, OSPF as Parquet; status and role; 90-day retention; browse and compare in the platform
Reconciliation	Serial, then hostname, then management IP, one to one; links from LLDP/CDP, IGP and /31, /30 pairs; matched, new, missing, changed; annotate only; ports for new interfaces on matched devices (cap 2,000); never creates devices
Change	Drift items to proposals to one network change; approve or reject with reason; Decided view with 30-day acceptance; pre and post snapshots on change status; diff verification
Configurations	SSH only; scrubbed twice; hash, line count, changed flag; side-by-side diff ignoring volatile lines
CVE	NVD 2.0 and CISA KEV refreshed daily; OS version to CPE to vulnerability; severity, CVSS, KEV, fixed-in, triage kept across runs
Audit	One line per device command (no output, no credentials), batches of 500 at least hourly, 90-day retention; credential fetches, enrolments and decisions logged; absence alert; health sweep 5 min
API	120 requests per minute per key

www.demandflow.com

Book a demo: www.demandflow.com/telco-network-management/

DemandFlow® is a registered trademark of TOCLOCO LTD. Registered in England No. 09950859. 71-75 Shelton St, London, WC2H 9JQ. © TOCLOCO LTD. All rights reserved.