CLOUTRIX

PRODUCT DATASHEET

VERSION 2.8.0

Visibility into traffic. Control over infrastructure.

Centralized bandwidth monitoring for cloud infrastructure, datacenters and baremetal servers. Turn network counters into history, comparisons and actionable operational metrics.

5 s
Collection interval

15 s
Dashboard refresh

120 days
Aggregate retention

Default operating intervals. Detailed measurements are retained for 48 hours.

From host to datacenter.

A consistent view of network usage and capacity.

History and P95

Explore 1 h, 12 h, 24 h, 30 and 60 days. Track inbound and outbound traffic, volume and P95 across complete five-minute windows.

Totals and comparisons

Aggregate authorized traffic by datacenter and compare up to eight host or datacenter selections on the same chart.

Default NIC per server

Detect uplinks using the default route or select interfaces manually. Inspect other NICs without changing datacenter totals.

Internal, external and combined

Classify IP traffic on Linux hosts using eBPF and datacenter-specific IPv4/IPv6 blocks, without requiring switch NetFlow export.

Resource-based access

Administrator and restricted read roles with datacenter or host authorization. Provider information is visible only to administrators.

Dashboard operations

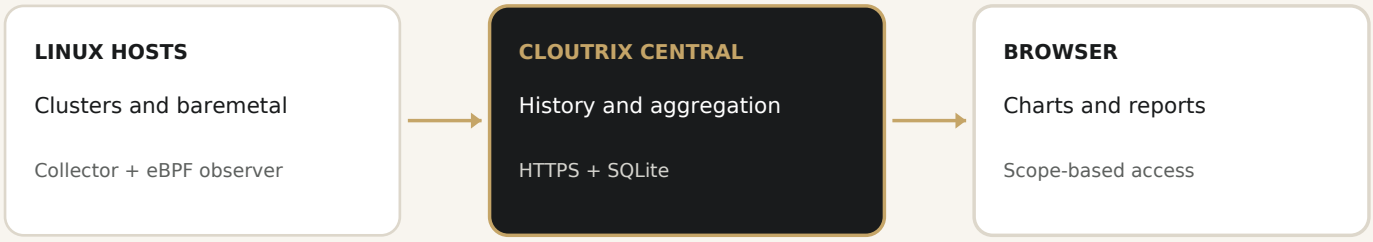
Manage hosts, users and passwords. Export CSV and explore role-filtered help. Portuguese and English interface, with light and dark modes.

FOR CLOUD PROVIDERS, MSPs AND INFRASTRUCTURE TEAMS

A clearer view of usage, traffic variations and capacity planning.

Architecture and specifications.

Collect on hosts. Store and aggregate centrally. Explore in the browser.



Technical characteristics

Collection and display	Measurements every 5 s; dashboard refresh every 15 s. Hosts send measurements to the central server over HTTPS.
History and retention	Query windows from 1 h to 60 days; details for 48 h and aggregates for 120 days. Export chart series as CSV.
Metrics and calculation	RX/TX in Mbps, volumes in decimal GB and P95 across complete five-minute windows. Aggregation sums simultaneous measurements.
Resource organization	Provider, datacenter, cluster, host and interface. Baremetal servers do not require cluster membership.
Traffic classification	Internal, external, combined and a separate Non-IP category. Policies use IPv4/IPv6 blocks and datacenter membership.
Security and users	HTTPS with TLS 1.2 or later; individual tokens; hashed passwords; host/datacenter access scopes and temporary password changes.
Deployment	Linux Debian/Ubuntu central server with Python 3, OpenSSL, systemd and local SQLite. Configurable HTTPS port; default TCP 9088.
Traffic observer	Compatible Linux kernel and eBPF/TC privileges; install as root. Tools include clang/LLVM, libbpf, iproute2 and bpftool.

Measurement scope

- Capture covers traffic crossing monitored interfaces. VM-to-VM traffic outside those interfaces is not observed; aggregating hosts does not deduplicate packets.
- Internal/external classification requires an active observer and is not retroactive. Traffic across datacenters is external. Combined sums internal and external traffic, excluding Non-IP.
- Collection failures and missing periods appear as gaps, not zero. Coverage indicates the availability of complete measurement windows for P95.

Deployed in the operator's infrastructure, with data and access managed on its own central server.