Входящие trap / syslog

SNMP trap и syslog (входящие)

Не отдельная страница. Приём — на **узле** (шаблон + IP); лента — вкладка **Входящие сообщения** в панели метрик (только если есть trap/syslog items); аварии по триггерам — в **Событиях** / воркфлоу (и краткий блок «Последние события» в сайдбаре).

Как настроить

1. **Админ** → Настройки → Мониторинг → **Приём trap / syslog**:
   - SNMP trap: вкл (default), порт **162**.
   - Syslog: вкл **явно** (default выкл), порт **514**.
   - **Принимать с loopback**: для Docker Desktop lab обычно вкл; в проде часто выкл.
   - После смены — **перезапуск backend**. Linux unit: `CAP_NET_BIND_SERVICE` (wisla-backend.service).
2. Узел → Шаблоны → **Принимать SNMP traps** / **Принимать syslog**.
3. IP интерфейса = peer, как его видит backend (на Docker Desktop часто `127.0.0.1`).
4. На устройстве: destination = IP wiSLA, порт из настроек.
5. Обзор узла → вкладка **Входящие сообщения**. Поиск, период (1ч–7д / свой диапазон), выпадающие фильтры типа и критичности, чипы как на «Последних событиях», **свернуть повторы**, пагинация. Проблемы — триггеры по `{$... PROBLEM.REGEXP}` или воркфлоу.

Триггеры по умолчанию

Шаблон	Макрос	Смысл
`SNMP traps`	`{$SNMPTRAP.PROBLEM.REGEXP}`	`find(...iregexp...)=1` → WARNING
`Syslog`	`{$SYSLOG.PROBLEM.REGEXP}`	то же для syslog

Макросы правятся на узле (Настроить / Параметры). Пустой или слишком широкий regexp = шум в Событиях.

Техдетали

	Trap	Syslog
Listener		`SyslogListener`

	Trap	Syslog
	`SnmpTrapListener` (SNMP4J v1/v2c/v3 + inform ack)	
Type / collector	`SNMP_TRAP` / `server:snmptrap`	`SYSLOG` / `server:syslog`
Key	`snmptrap.fallback`, `snmptrap[oid]` (linkDown/linkUp/…)	`syslog.fallback`, `syslog[err]`…
Парсинг	SNMP4J PDU ⟶ trap OID + varbinds	PRI ⟶ facility/severity labels
Peer	`IncomingPeerMatcher` + `monitoring.incoming_accept_loopback`	то же

- API: `GET …/incoming/capable`, `GET …/metrics/recent` (PG ring + ClickHouse fallback).
- Smoke: incoming-trap-syslog-smoke.md.
- ADR / matrix: ADR-002, zabbix-template-runtime.

Не в scope (пока)

TCP/TLS syslog, отдельная страница Incoming, auto-fallback на порт 1162, полный trap catalog на все enterprise MIB.