Talk to Prometheus

This is a simple demo of CrewAI flow for converting user query to PromQL.

Ask to prometheus:

analyze network packets for last 10 minutes for all devices use node_network_receive_packets_total and node_network_transmit_packets_total

Ask AI

visualize flow

AI Analysis

Key Insights:

- Only `eth0` shows network activity (2926 total received packets over 10 minutes), while all other interfaces (`erspan0` , `lo` , `gre0` , etc.) recorded **zero packets**, indicating inactive or unused network devices.
- Traffic on `eth0` grew linearly at **30 packets per minute** (0.5 packets/sec), suggesting stable, low-volume inbound traffic with no spikes or anomalies.
- Cumulative packet count increased by **300 packets** (from 2626 to 2926) over the 10-minute window, reflecting consistent but minimal usage.

Actionable Recommendations:

- Investigate why non- `eth0` interfaces (e.g., `tunl0` , `sit0`) show zero activity—confirm if they are intentionally disabled or misconfigured.
- Monitor `eth0` for deviations from the baseline (0.5 pps); sudden increases could indicate scanning or unexpected traffic.
- Validate network policies to ensure critical services relying on inactive interfaces (e.g., tunnels like `ip6_vti0`) are functioning as intended.
- Consider alerting on sustained zero traffic for mission-critical interfaces to detect unplanned outages.


```
{
  "id" : "c1763698-37c5-4225-911d-d90c1d58da77"
  "original_query" :
  "analyze network packets for last 10 minutes for all devices use
  node_network_receive_packets_total and node_network_transmit_packets_total. current epoch is
  1757183082"
  "promql_plan" : {
    "query" : "node_network_receive_packets_total or node_network_transmit_packets_total"
    "query_type" : "query_range"
    "parameters" : {...}
  }
  "validation_result" : true
```


Select chart type

line

View Graph

```
"validation_feedback" : "Query executed successfully."
"final_prometheus_result" : {
  "status" : "success"
  "data" : {
    "resultType" : "matrix"
    "result" : [
      0 : {
        "metric" : {
          "__name__" : "node_network_receive_packets_total"
          "device" : "erspan0"
          "instance" : "node-exporter:9100"
          "job" : "node-exporter"
        }
        "values" : [...]
      }
      1 : {...}
      2 : {...}
      3 : {...}
      4 : {...}
      5 : {...}
      6 : {...}
      6 : {...}
      7 : {...}
      8 : {...}
      9 : {...}
      10 : {
        "metric" : {
          "__name__" : "node_network_receive_packets_total"
          "device" : "tunl0"
          "instance" : "node-exporter:9100"
          "job" : "node-exporter"
        }
        "values" : [
          0 : [
            0 : 1757182482
            1 : "0"
          ]
          1 : [...]
          2 : [...]
          3 : [...]
          4 : [...]
```

```
                5 : [...]
                6 : [...]
                7 : [...]
                8 : [...]
                9 : [...]
                10 : [...]
              ]
            }
          ]
        }
      }
"final_answer" :
"**Key Insights**:
- Only `eth0` shows network activity (2926 total received packets over 10 minutes), while all other interfaces (`erspan0`, `lo`, `gre0`, etc.) recorded **zero packets**, indicating inactive or unused network devices.
- Traffic on `eth0` grew linearly at **30 packets per minute** (0.5 packets/sec), suggesting stable, low-volume inbound traffic with no spikes or anomalies.
- Cumulative packet count increased by **300 packets** (from 2626 to 2926) over the 10-minute window, reflecting consistent but minimal usage.

**Actionable Recommendations**:
- Investigate why non-`eth0` interfaces (e.g., `tunl0`, `sit0`) show zero activity—confirm if they are intentionally disabled or misconfigured.
- Monitor `eth0` for deviations from the baseline (0.5 pps); sudden increases could indicate scanning or unexpected traffic.
- Validate network policies to ensure critical services relying on inactive interfaces (e.g., tunnels like `ip6_vti0`) are functioning as intended.
- Consider alerting on sustained zero traffic for mission-critical interfaces to detect unplanned outages."
"retry_count" : 1
"next_task" : NULL
}
```