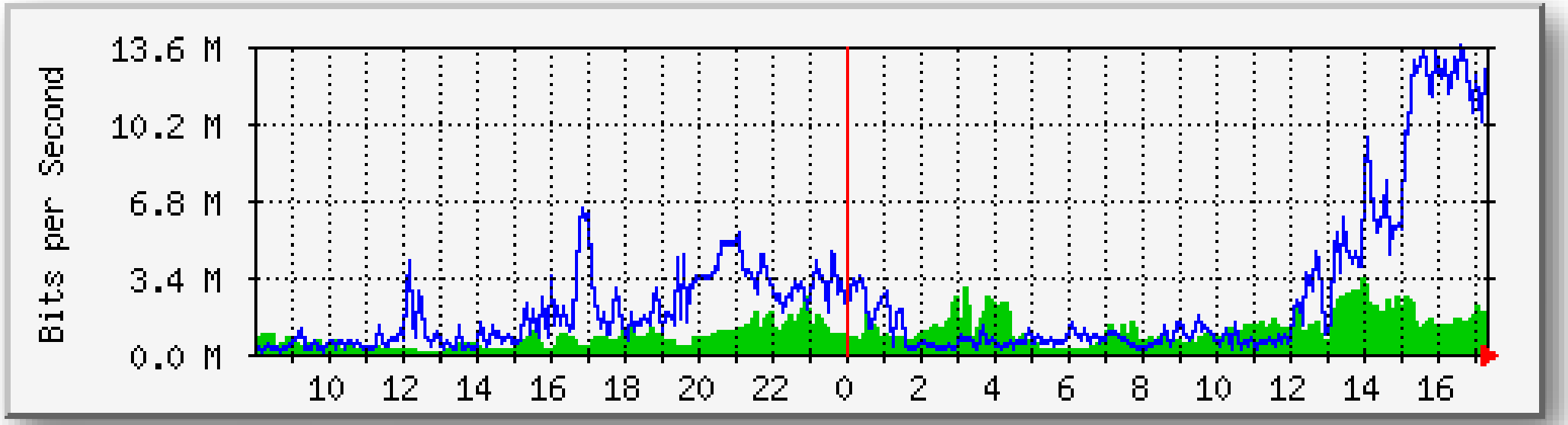
Timeseries Troubles: How (not) to calculate statistics

Marian Rychtecký

22.01.2025

NIX·CZ

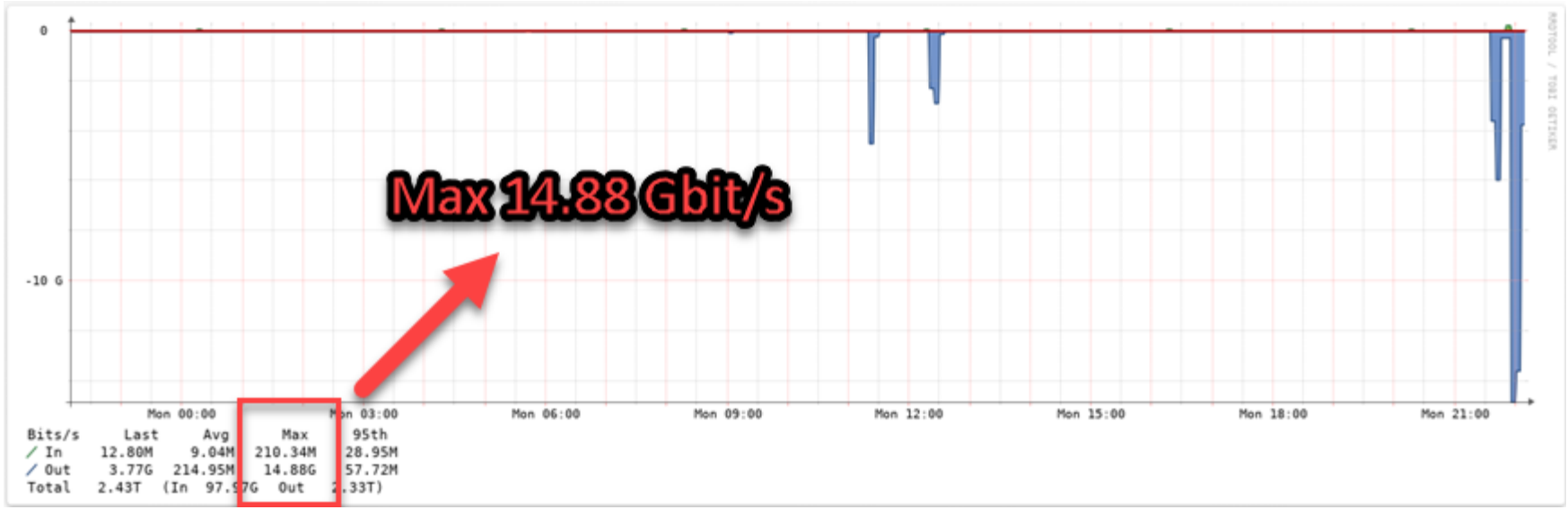
Zpět do roku 1995 – MRTG 1.0 released



(Ne)výhody

- 5/10 min. sběr dat
- Není možné měnit interval po založení souboru
- Závislost na SNMP
- Jednoduchost
- Předgenerované obrázky

Ukrývání skutečnosti



Je toto rozhraní přetížené?

NIX·CZ

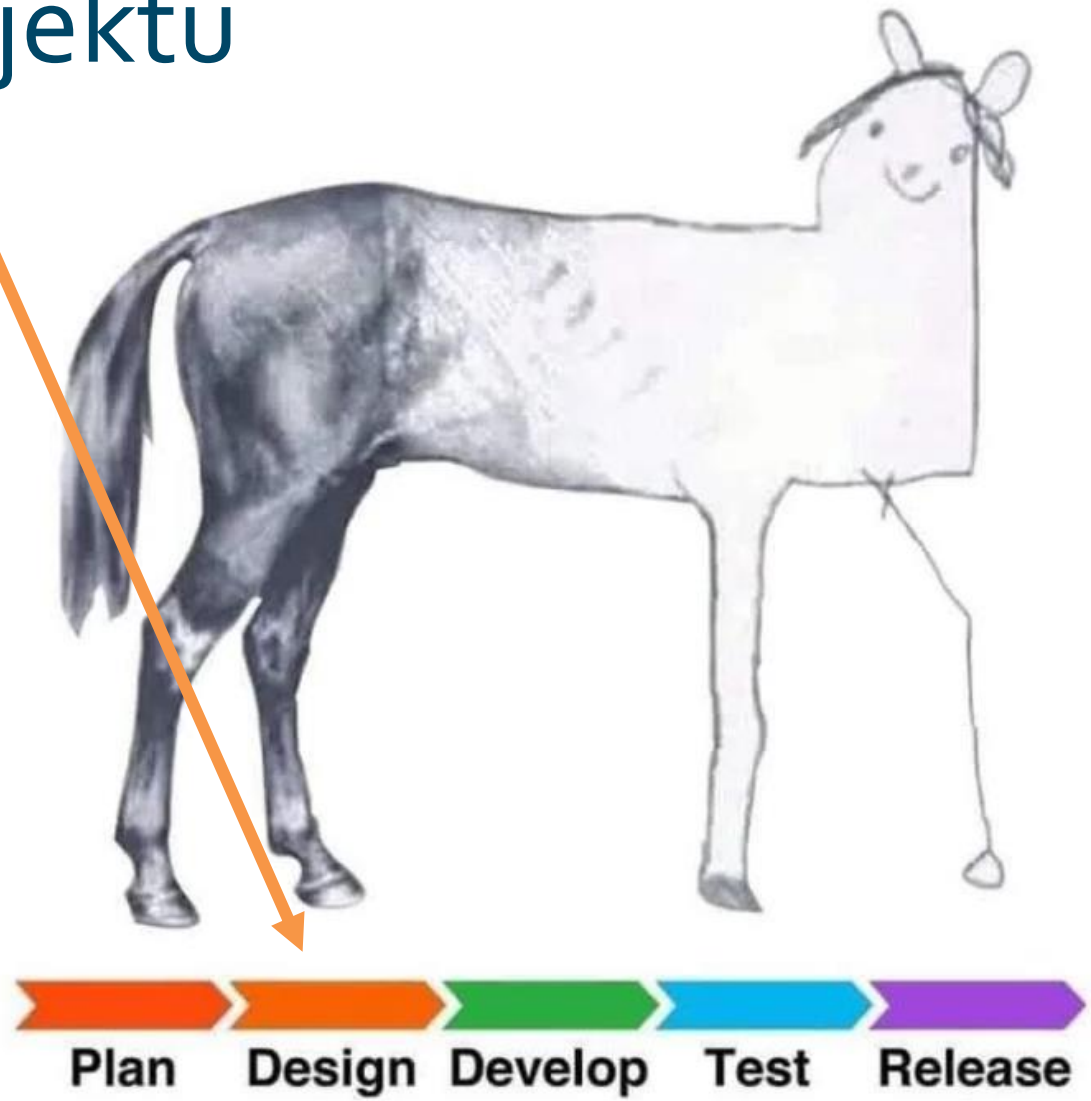
Jaké máme možnosti (2021)

- ~~SNMP MIB~~
- ~~Rich SNMP (Prometheus, Telegraf…)~~
- ~~Streaming Telemetry~~
- Vlastní řešení
- ~~Netconf (….a jeho klony)~~

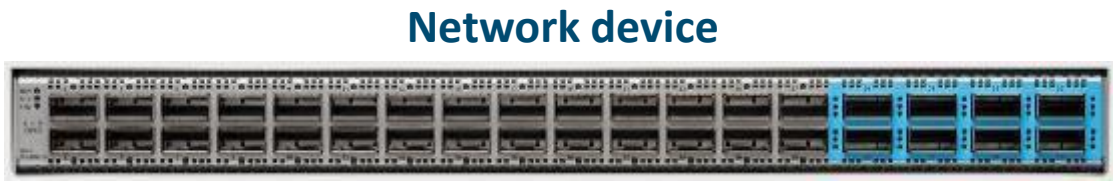
Výhoda vlastního řešení – příprava dat

- Nápad!
  - vezmene data ze sítě a provedeme „přípravu“
    - kalkulace hodnot
    - obohacení pro lepší (rychlejší?) seskupení
  - vložíme do databáze před připravené
  - budeme si užívat výhod TSDB

Fáze projektu



Network statistics



API

Netbox

API

Python code

Influx API

flux™

Traffic weather map

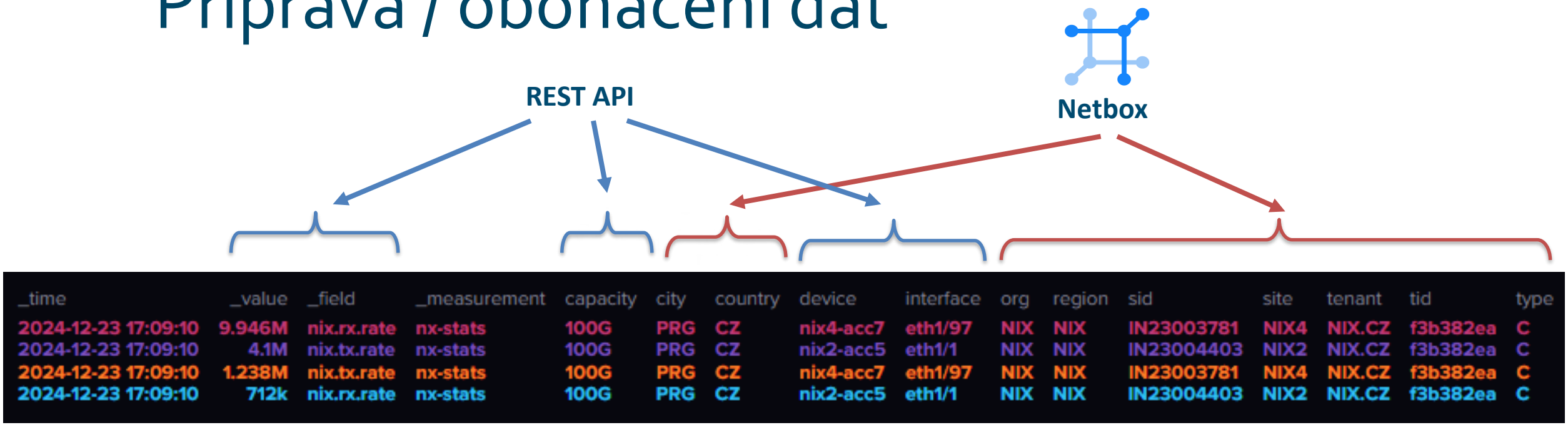
External Graphs

Internal Graphs

influxdb open source™

NIX·CZ

Příprava / obohacení dat



_time	_value	_field	_measurement	capacity	city	country	device	interface	org	region	sid	site	tenant	tid	type
2024-12-23 17:09:10	9.946M	nix.rx.rate	nx-stats	100G	PRG	CZ	nix4-acc7	eth1/97	NIX	NIX	IN23003781	NIX4	NIX.CZ	f3b382ea	C
2024-12-23 17:09:10	4.1M	nix.tx.rate	nx-stats	100G	PRG	CZ	nix2-acc5	eth1/1	NIX	NIX	IN23004403	NIX2	NIX.CZ	f3b382ea	C
2024-12-23 17:09:10	1.238M	nix.tx.rate	nx-stats	100G	PRG	CZ	nix4-acc7	eth1/97	NIX	NIX	IN23003781	NIX4	NIX.CZ	f3b382ea	C
2024-12-23 17:09:10	712k	nix.rx.rate	nx-stats	100G	PRG	CZ	nix2-acc5	eth1/1	NIX	NIX	IN23004403	NIX2	NIX.CZ	f3b382ea	C

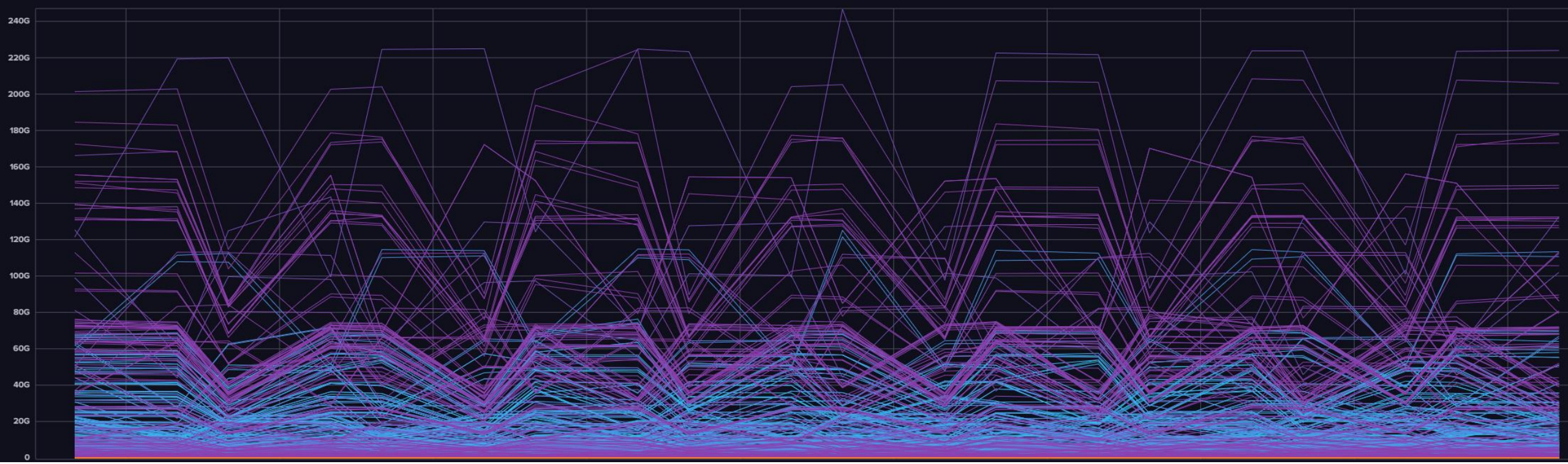
Ukládání dat

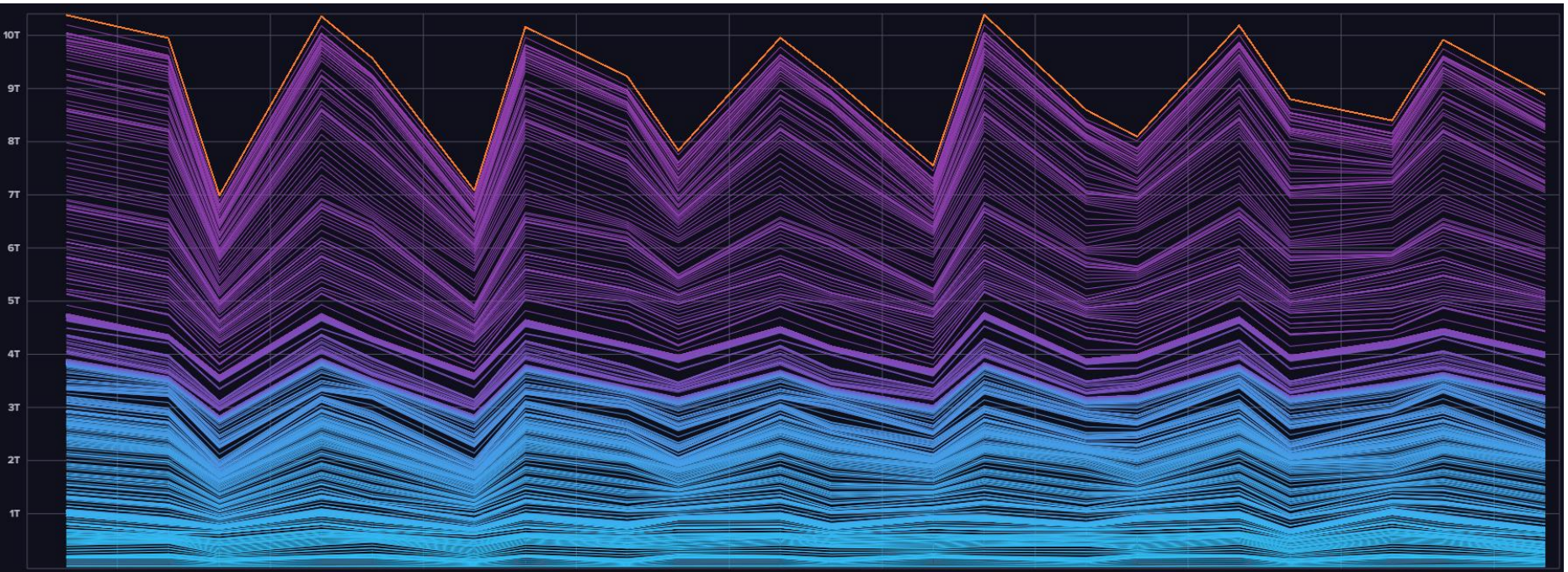
"main" bucket
~4GB / month

Down-sizing tasks

daily bucket 5 minutes MIN, MEAN, MAX	48 hodin
weekly bucket 30 minutes MIN,MEAN,MAX	10 dnů
monthly bucket 2 hours MIN, MEAN, MAX	40 dnů
yearly bucket 1 day MIN, MEAN, MAX	bez retence

NIX·CZ



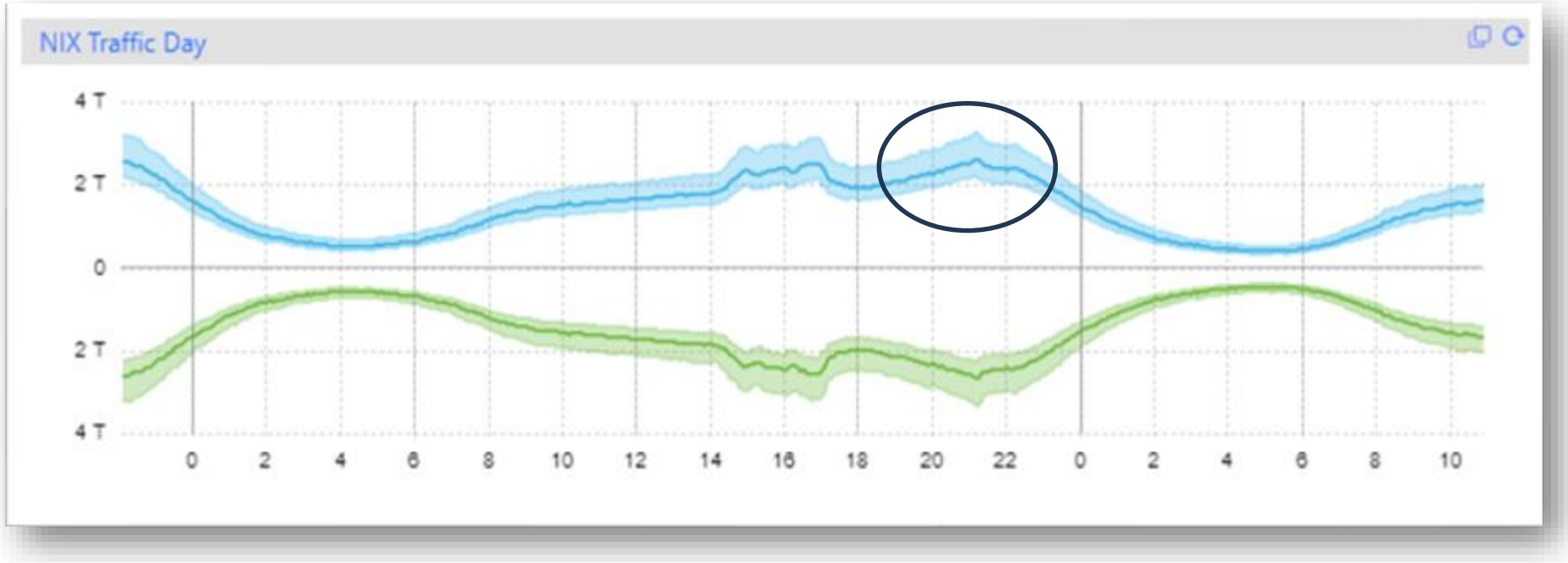


Surová data

NIX·CZ

Statistika

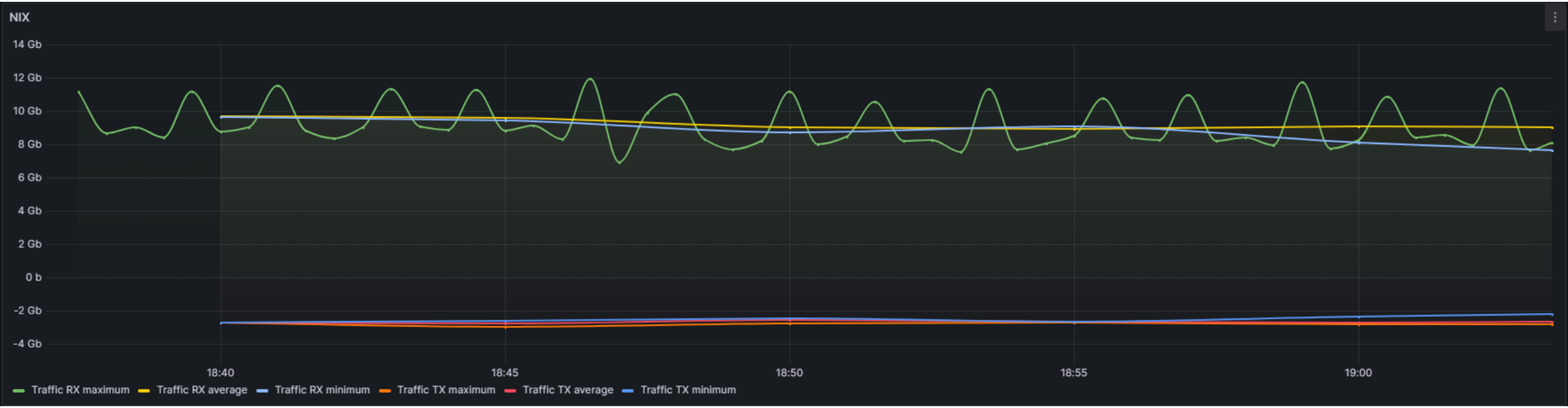
(nevěř žádné, kterou sis sám nezfalšoval)



- „day bucket"
- 5 min okno
  - 3 řady
    min,mean,max

```
from(bucket: "statistics")
  |> aggregateWindow(every: 300s, fn:min|max|mean)
```

NIX·CZ



⬆ Surová data ze switche

Průměr 3 hodnot jako max ⬇

Statistika

- surový vzorek á 30s
- 5 min okno (min,mean,max)

```
from(bucket: "statistics")
  |> aggregateWindow(every:
300s, fn:min|max|mean)
```

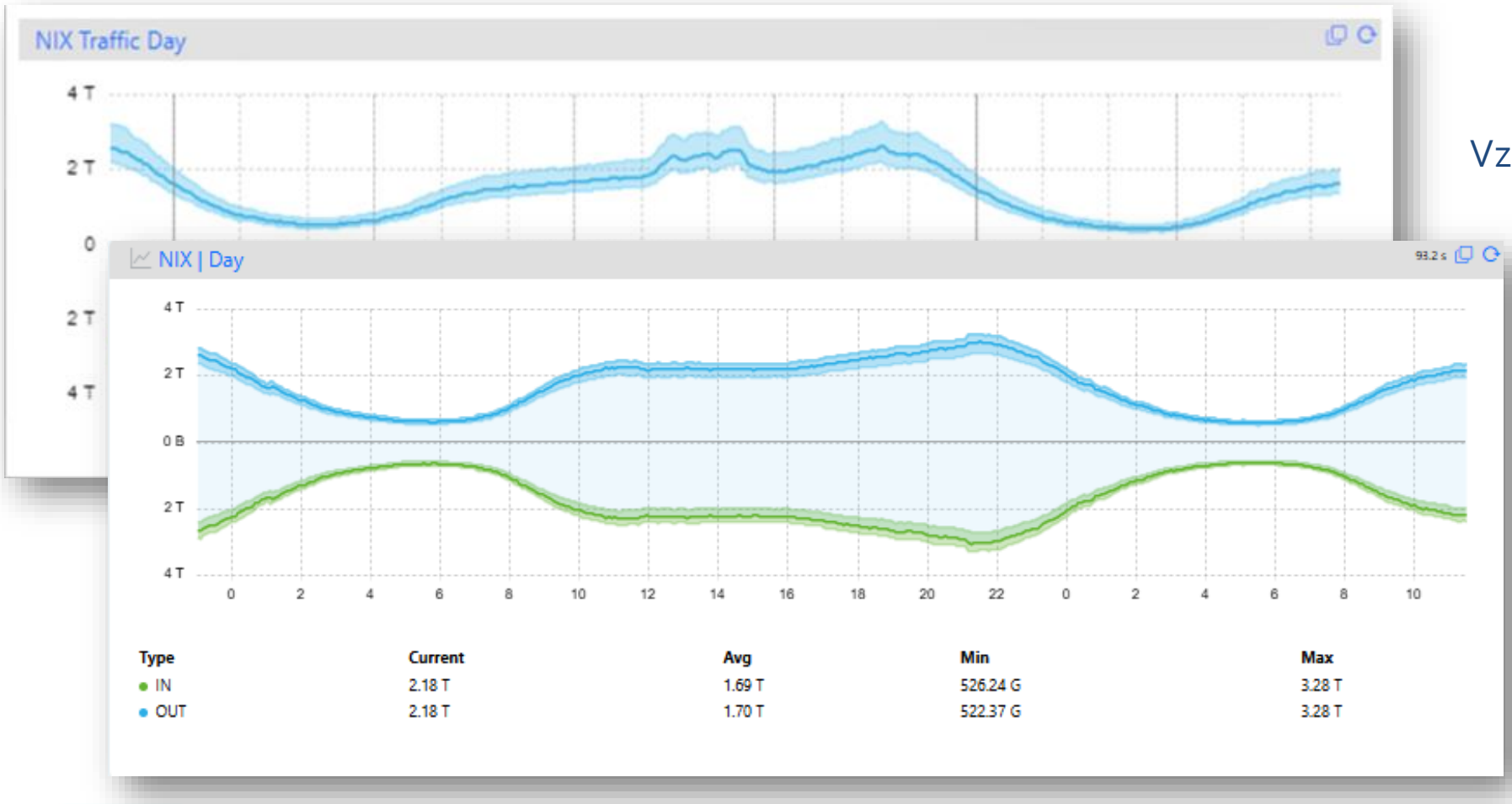
Tohle máme

- surový vzorek alespoň 20s (potřebujeme alespoň 3 vzorky za minutu)
- 1 min. okno min,mean,max (spočítáme průměrné hodnoty abychom dostali reálný provoz za 1 min.)
- 5 min. okno (5 hodnot po 1 minutě)
  - najdeme maximum z hodnot průměrů maxim
  - najdeme minimum z hodnot průměrů minim
  - spočítáme průměr z hodnot průměrů

```
from(bucket: "statistics")
  |> aggregateWindow(every: 60s, fn:mean)
  |> aggregateWindow(every: 300s, fn:max)
```

Tohle potřebujeme

NIX·CZ



Vzorky 30s (2 za minutu)

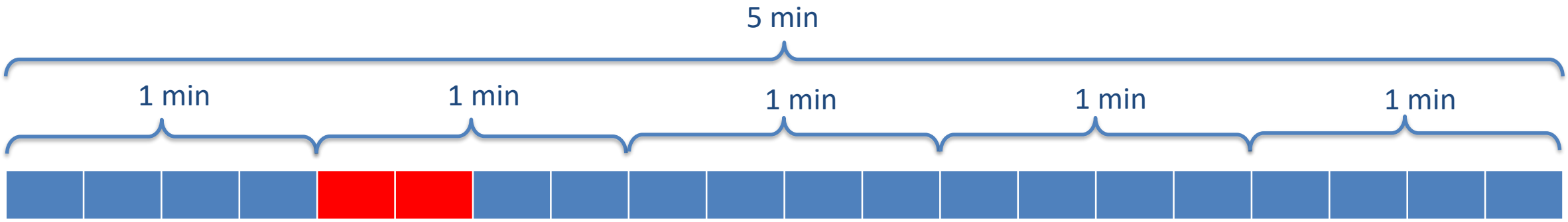
Vzorky 15s (4 za minutu)

NIX·CZ

Stavová data a časové intervaly

- Port UP / DOWN
  - problém s interpretací v GUI
  - nutné přepočítávání v časových oknech
  - jak ukládat do DB

Stavová data a časové intervaly



Výsledkem je port up 90% času z 5 minut
Do DB uložíme

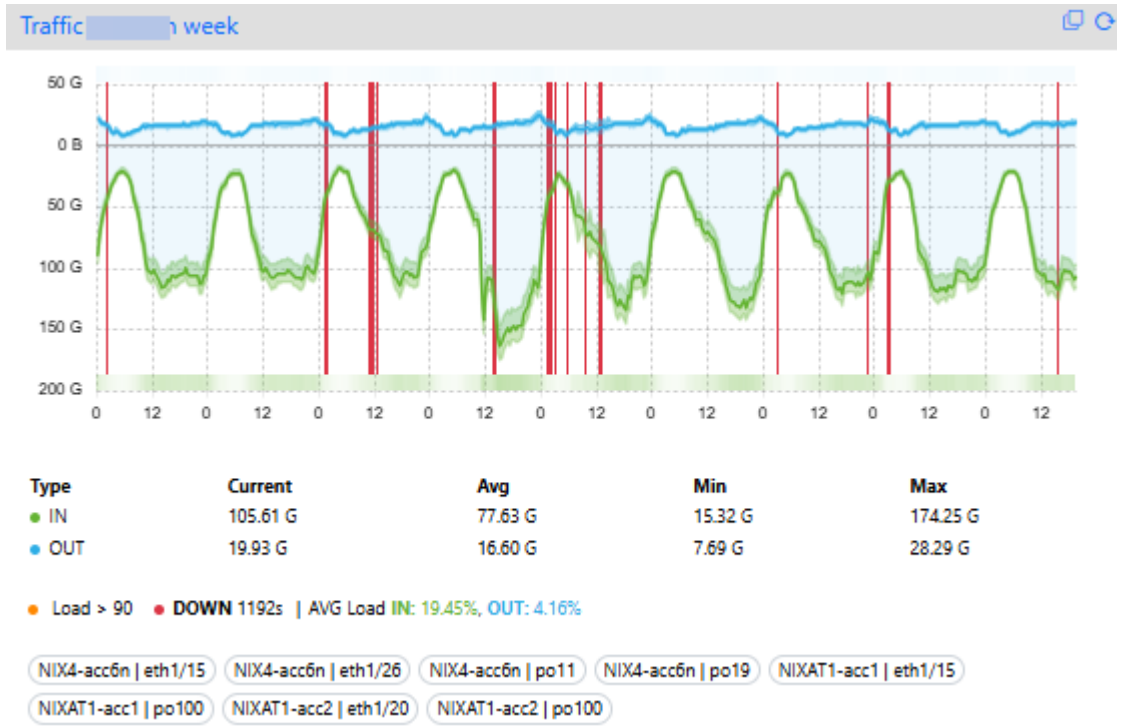
- pro tento 5 min interval hodnotu 0.9 (1-(2/20))
- pro 30 min interval hodnotu 0.98 (1-(2/120))
- pro 2h interval hodnotu 0.99 (1-(2/480))

NIX·CZ

```
|> aggregateWindow(
    every: 5m,
    fn: (column, tables=<-) =>
        tables
            |> reduce(
                fn: (r, accumulator) =>
                    ({
                        itemsTotal: accumulator.itemsTotal + 1,
                        itemsActive:
                            accumulator.itemsActive + (if r._value == true then 1 else 0),
                    }),
                identity: {itemsTotal: 0, itemsActive: 0},
            )
            |> map(
                fn: (r) =>
                    ({r with _value:
                            if r.itemsTotal > 0 then
                                float(v: r.itemsActive) / float(v: r.itemsTotal)
                            else
                                float(v: 0),
                    }),
            )
            |> drop(columns: ["itemsActive", "itemsTotal"]),
```

NIX·CZ

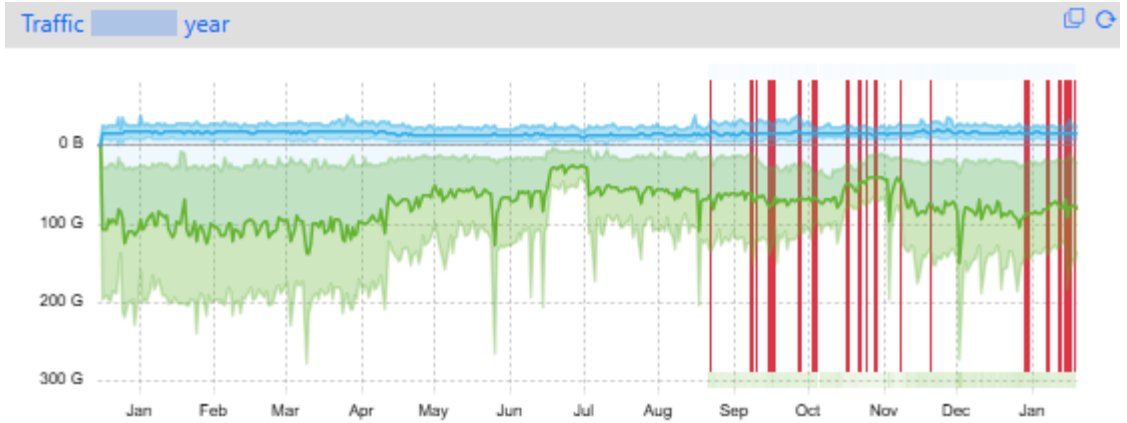
Stavová data v GUI



Type	Current	Avg	Min	Max
IN	105.61 G	77.63 G	15.32 G	174.25 G
OUT	19.93 G	16.60 G	7.69 G	28.29 G

Load > 90 **DOWN** 1192s | AVG Load IN: 19.45%, OUT: 4.16%

NIX4-acc6n | eth1/15 NIX4-acc6n | eth1/26 NIX4-acc6n | po11 NIX4-acc6n | po19 NIXAT1-acc1 | eth1/15
NIXAT1-acc1 | po100 NIXAT1-acc2 | eth1/20 NIXAT1-acc2 | po100



Type	Current	Avg	Min	Max
IN	81.43 G	75.63 G	0.00 B	277.89 G
OUT	16.82 G	16.23 G	0.00 B	39.54 G

Load > 90 **DOWN** 35744s | AVG Load IN: 6.69%, OUT: 1.58%

NIX4-acc6n | eth1/15 NIX4-acc6n | eth1/26 NIX4-acc6n | po11 NIX4-acc6n | po19 NIXAT1-acc1 | eth1/15
NIXAT1-acc1 | po100 NIXAT1-acc2 | eth1/20 NIXAT1-acc2 | po100

NIX·CZ

Kaskáda je lepší!

“main” bucket
~4GB / month

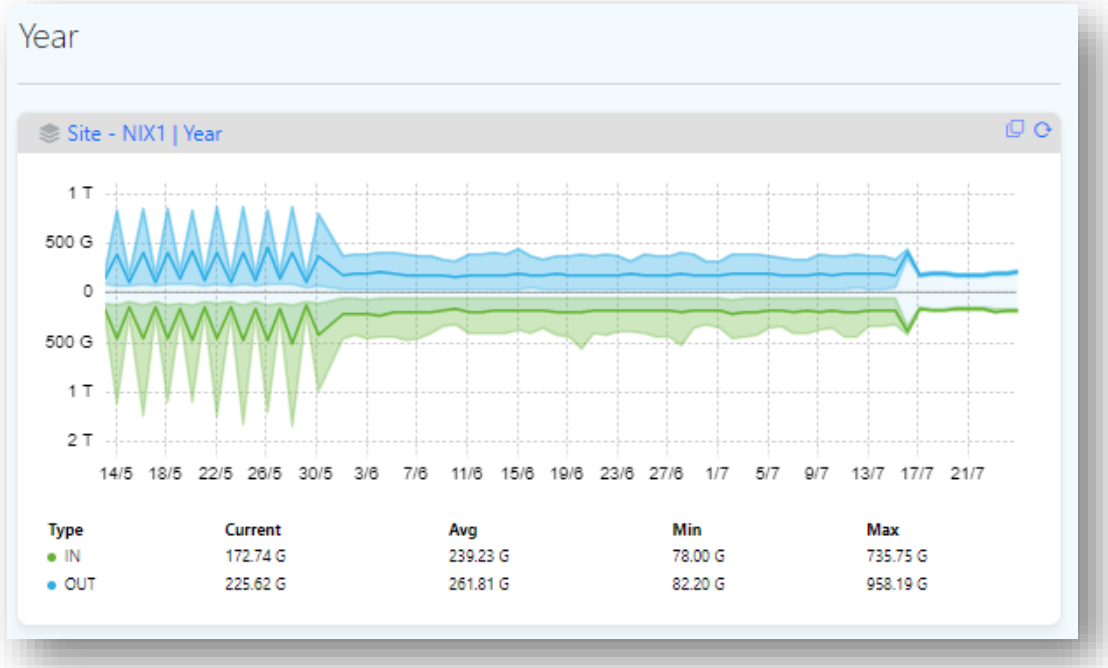
Down-sizing tasks

daily bucket
5 minutes MIN, MEAN, MAX

weekly bucket
30 minutes MIN,MEAN,MAX

monthly bucket
2 hours MIN, MEAN, MAX

yearly bucket
1 day MIN, MEAN, MAX



NIX·CZ

Město, moře, kuře....

daily bucket
5 minutes MIN, MEAN, MAX

Load data → Remap data → Save data

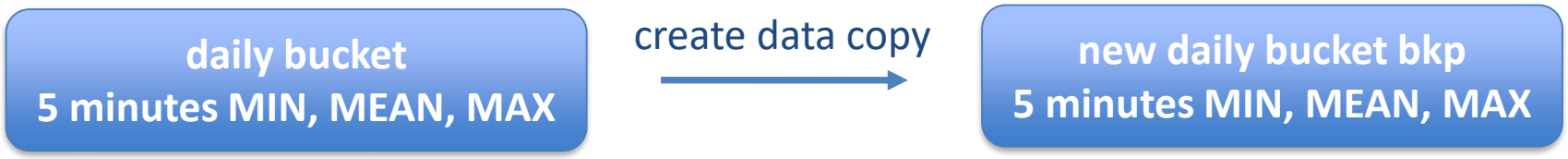
- NIX
  - AT
    - VIE
  - CZ
    - PRG
  - DE
    - FRA
  - SK
    - BLA

new daily bucket
5 minutes MIN, MEAN, MAX

NIX·CZ

Přetagování ~100k záznamů

Step 1) Vytvořit backup




```
from(bucket: "statistics-day")
    |> range(start, stop)
    |> to(bucket: "statistics-day_bkp")
```

NIX·CZ

Přetagování ~100k záznamů

Krok 2) Vyčistit původní bucket

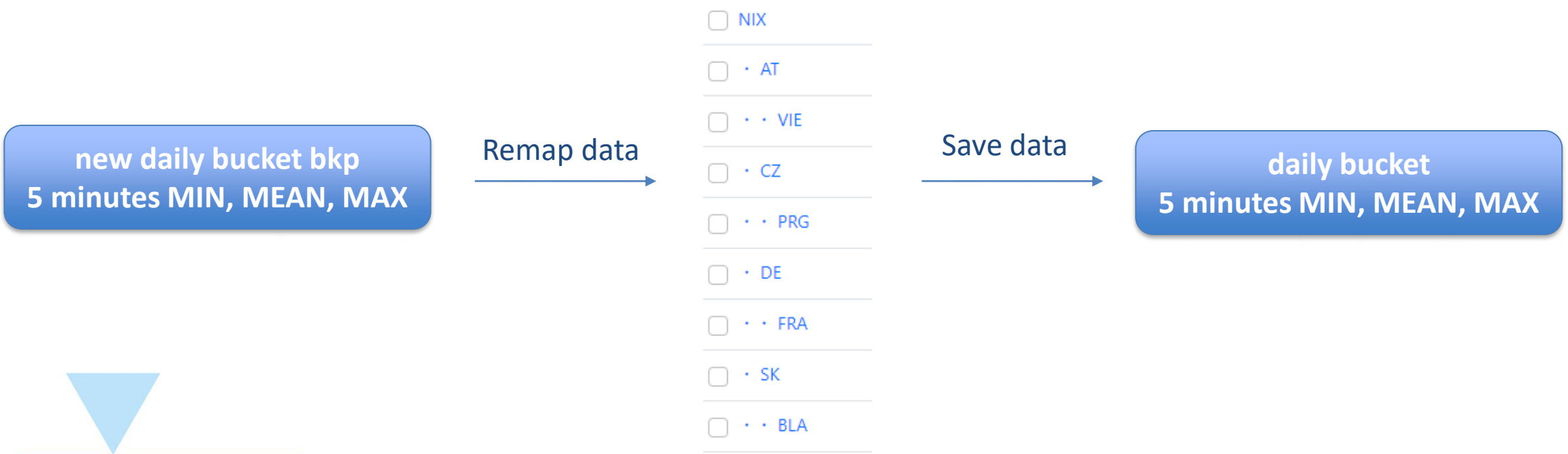
daily bucket
5 minutes MIN, MEAN, MAX

influx delete --bucket "statistics-month" --start "" --stop ""

NIX·CZ

Přetagování ~100k záznamů

Krok 2) Naplnit původní bucket modifikovanými daty



NIX·CZ

Přetagování ~100k záznamů

daily bucket
5 minutes MIN, MEAN, MAX

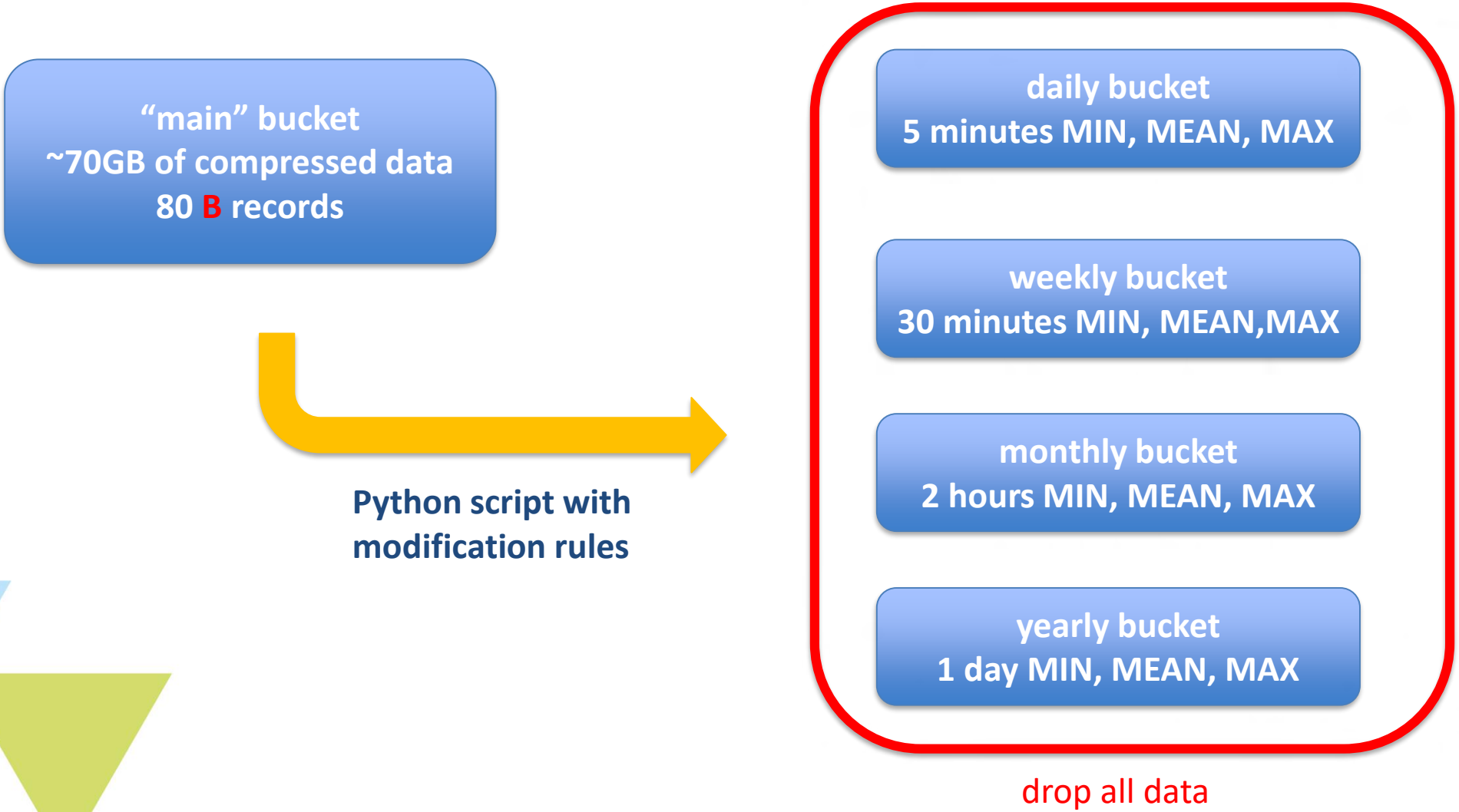
Výsledek: chybí cca 15% záznamů

Funkce >to() nezkopíruje vše !

(v GUI)

NIX·CZ

Přetagování 80 miliard RAW záznamů



NIX·CZ

Přetagování 80 miliard RAW záznamů

- Načítání, modifikace a uložení dat po dnech za 1 rok zpětně
- Přegenerování denních statistik cca 2h
- Celkem cca 4h

Přetagování 80 miliard RAW záznamů

- Po přegenerování velmi pomalé načítání dat
  - Před cca 500ms
  - Po cca 5s

Přetagování 80 miliard RAW záznamů

- Analýza problému
- Řešením je úprava „shard-groups“
- Jediná možnost je smazat buckety, založit nové s upravenými parametry a znovu je naplnit (*)

*) Mnohem později jsme zjistili, že je možné tuto operaci provést i bez mazání

Přetagování 80 miliard RAW záznamů

- Export dat v line-protocol formátu
- Smazat bucket v GUI
- Úprava parametrů

```
user@influx-db:~$ influx bucket update --id
<id> --retention 960h --shard-group-
duration 480h
```

- Nahrání dat zpět z line-protocolu

NIX·CZ

Jak RFC8950

```
Channel ipv6
  State:          UP
  Import state:   UP
  Export state:   READY
  Table:          T6_6881x2
  Preference:     100
  Input filter:   bgp6_in_AS6881x2
  Output filter:  bgp_peer_export6
  Import limit:   20
    Action:       block
  Routes:         8 imported, 0 filtered, 0 exported, 8 preferred
  Route change stats:     received   rejected   filtered    ignored   RX limit   IN limit   accepted
    Import updates:            600          0          0        592          0          0          8
    Import withdraws:            0          0        ---          0        ---          0
    Export updates:              0          8       1938        ---          0          0
    Export withdraws:            0        ---        ---        ---        ---          0
  BGP Next hop:   2001:7f8:14::100 fe80::e03a:53ff:fe30:3a80
  Pending 0 attribute sets with total 0 prefixes to send
Channel ipv4
  State:          UP
  Import state:   UP
  Export state:   READY
  Table:          T64_6881x2
  Preference:     100
  Input filter:   bgp6_in_AS6881x2
  Output filter:  bgp_peer_export4
  Import limit:   5000
    Action:       block
  Routes:         10 imported, 0 exported, 10 preferred
  Route change stats:     received   rejected   filtered    ignored   RX limit   IN limit   accepted
    Import updates:             10          0          0          0          0          0         10
    Import withdraws:            0          0        ---          0        ---          0
    Export updates:              0         10         74        ---          0          0
    Export withdraws:            0        ---        ---        ---        ---          0
  BGP Next hop:   2001:7f8:14::100 fe80::e03a:53ff:fe30:3a80
  Pending 0 attribute sets with total 0 prefixes to send
```

Proč RFC8950?

```
bird> show route table master64
Table master64:
309.204.80.0/20      unicast [R6_50658x2 2025-01-20 22:08:29] * (100)
        via 2001:9f8:114::81:2 on ens20
                     unicast [R6_50658x1 2025-01-20 22:08:29] (100)
        via 2001:9f8:114::81:1 on ens20
```

NIX·CZ

Děkuji za pozornost

mr@nix.cz

@marianrychtecky

NIX·CZ