



ANDREWS
IT ENGINEERING

Átlátni az átláthatatlant

Hálózati forgalomelemzés egyszerűen

Trendek:

- növekvő hálózati adatmennyiség
- növekvő kiberfenyegetettség
- bonyolultabb hálózatok
- hálózati vakfoltok
- a nyilvános szolgáltatásoknál egyre magasabb SLA-t várnak el

A láthatóság a hálózaton is fontossá vált!



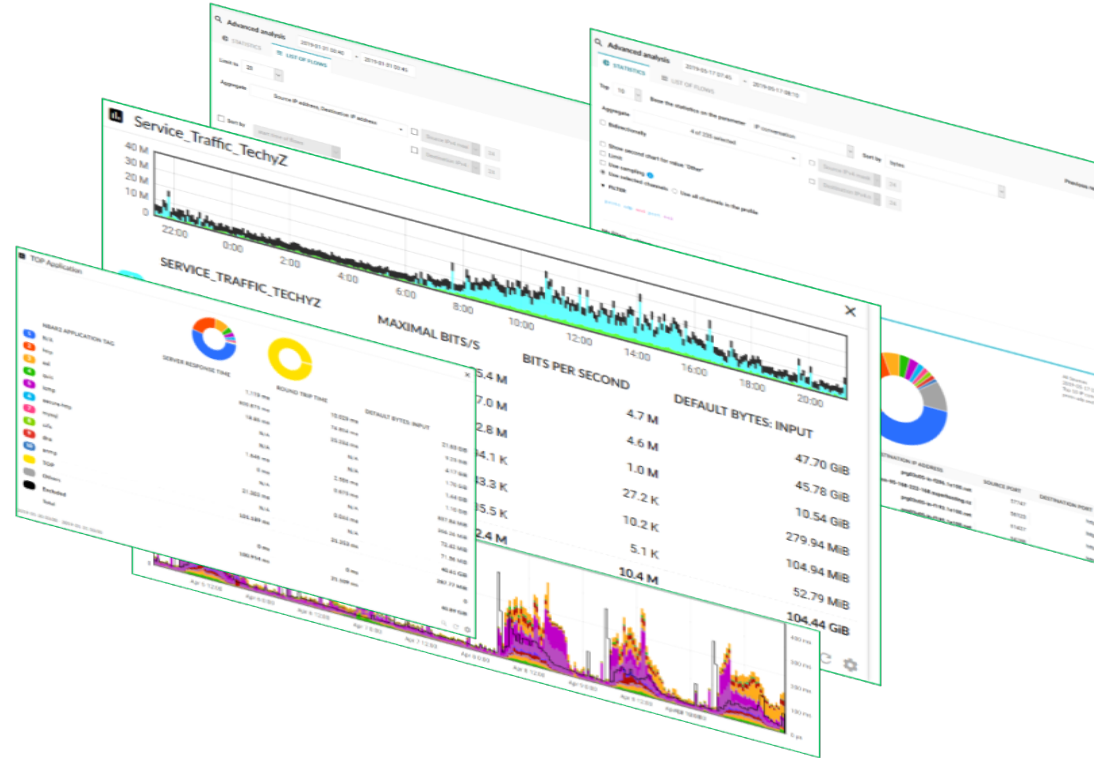
Adott egy alkalmazás probléma/lassulás:

- alkalmazás csoport vs. dba-k vs. infra team vs. hálózatosok vs. storage adminok → tcpdump
- egy órával korábbi forgalmat kellene nézni → history?
- óránként 160 ezer tranzakció → mit is nézzünk?
- mindehova agent-ek?

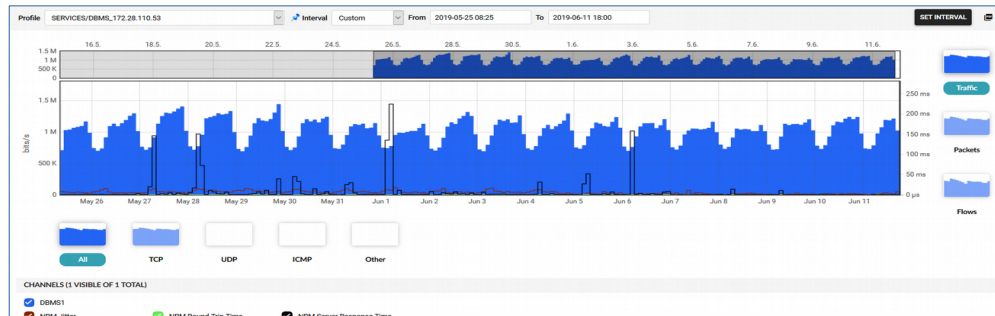
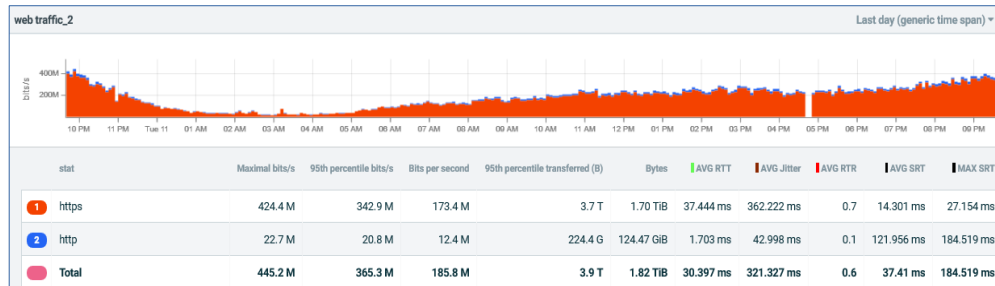


Netflow

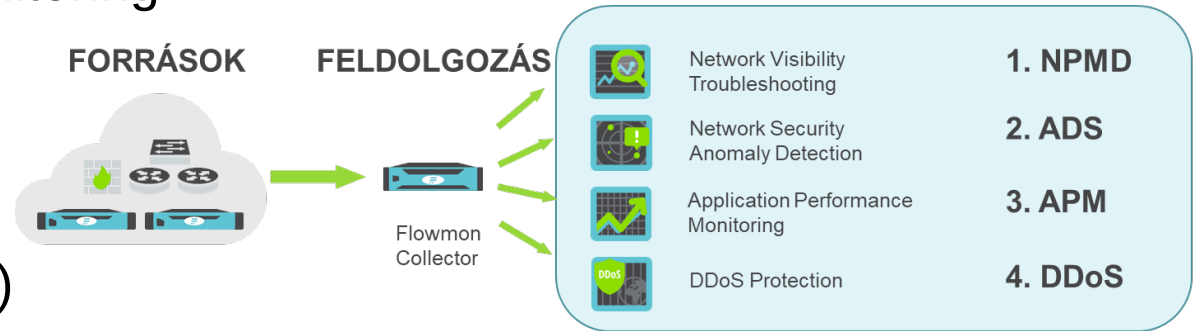
- 1996-ban jelent meg
- V5 infók:
 - forrás és cél címek, portok, protokoll.
- v9 infók:
 - + pl. VLAN címkék, ipv6, stb.
- A forgalom méretének átlagosan úgy 500-ad része, tehát:
 - menthető, kezelhető adatról van szó,
 - hetes, hónapos historyval is.



- Mi lenne ha lementenénk még egy kis plusz információt?
 - http header-ek,
 - SQL select-ek
 - round trip time (RTT)
 - server response time (SRT)
 - data transfer time (DTT)
 - stb...
- v10, vagyis inkább IPFIX:
 - + Layer 7 információ, illetve bármi, amit csak bele akarunk tenni.



- sensor/probe → collector
- NetFlow + layer 7 infó (probe)
→ IPFIX
- hálózat teljesítmény monitoring (NPM)
- alkalmazás teljesítmény monitoring (APM)
- anomália detekció (ADS)
- traffic recorder
- riasztások



last 1 hour



06/11/2019 14:23 — 06/11/2019 15:23

Information

Transaction count	41 967
Total amount of data	161.75 MB
Avg. app. response time	0.07 s
Median of app. response time	0.049 s
95% application response time	0.122 s
99% application response time	0.521 s

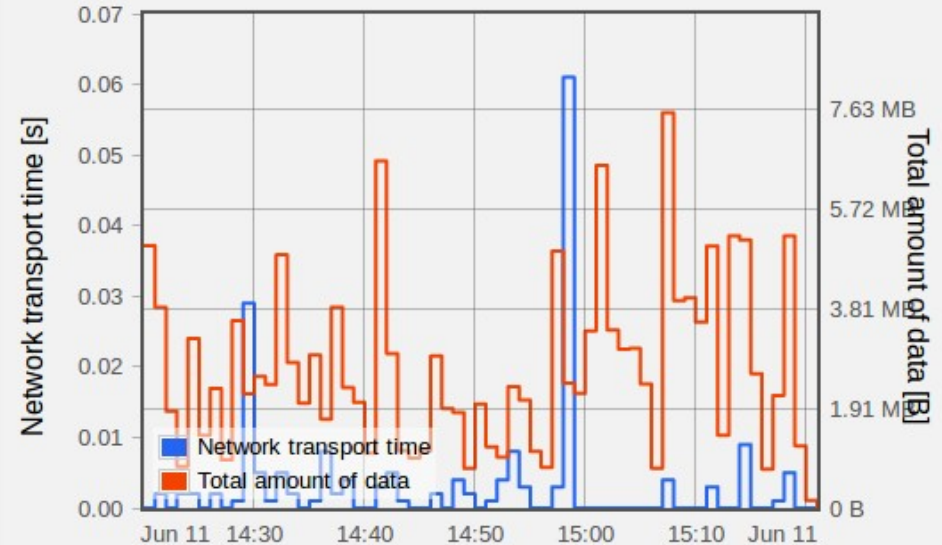


Five slowest transactions

#	Transactions	Count	APM index	Avg. app. respon...
1	POST//...insert	38	100.00	0.605
2	POST//...upload	391	100.00	0.460
3	GET//...mapByCity	35	100.00	0.312
4	POST//...account/login	1 455	97.92	0.260
5	POST//...delete	38	100.00	0.236



Amount of data and network transport time

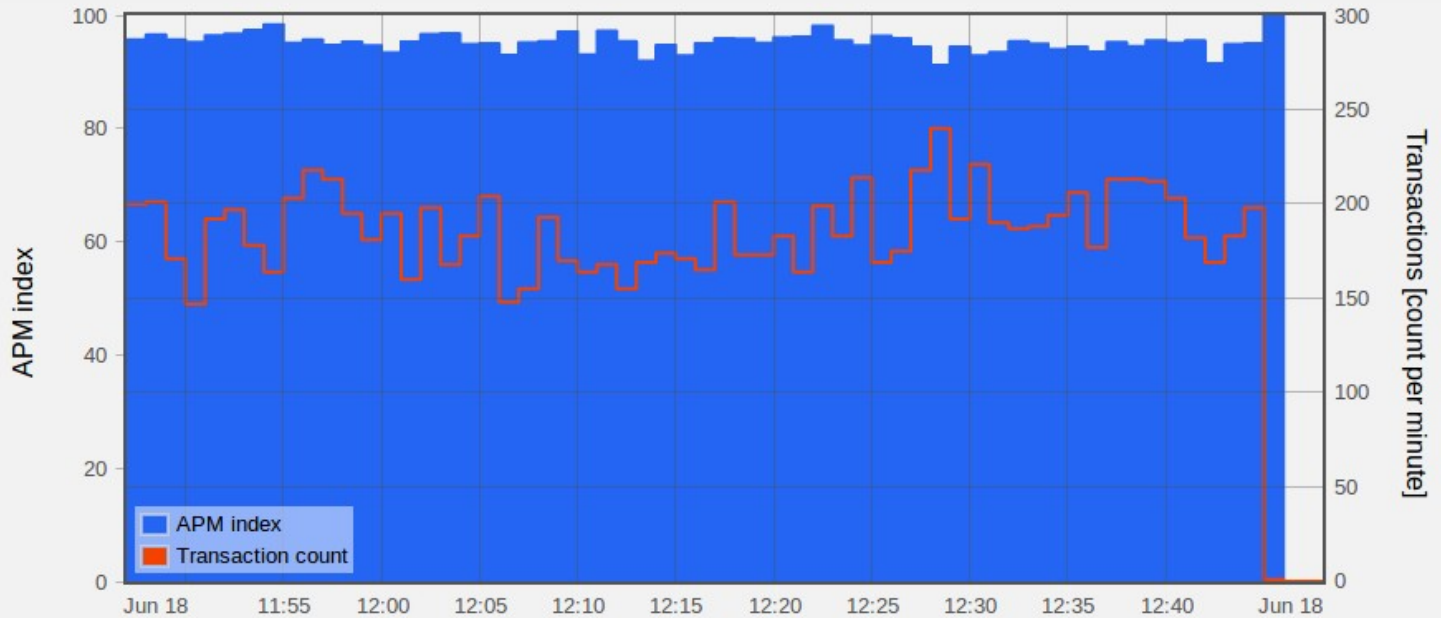


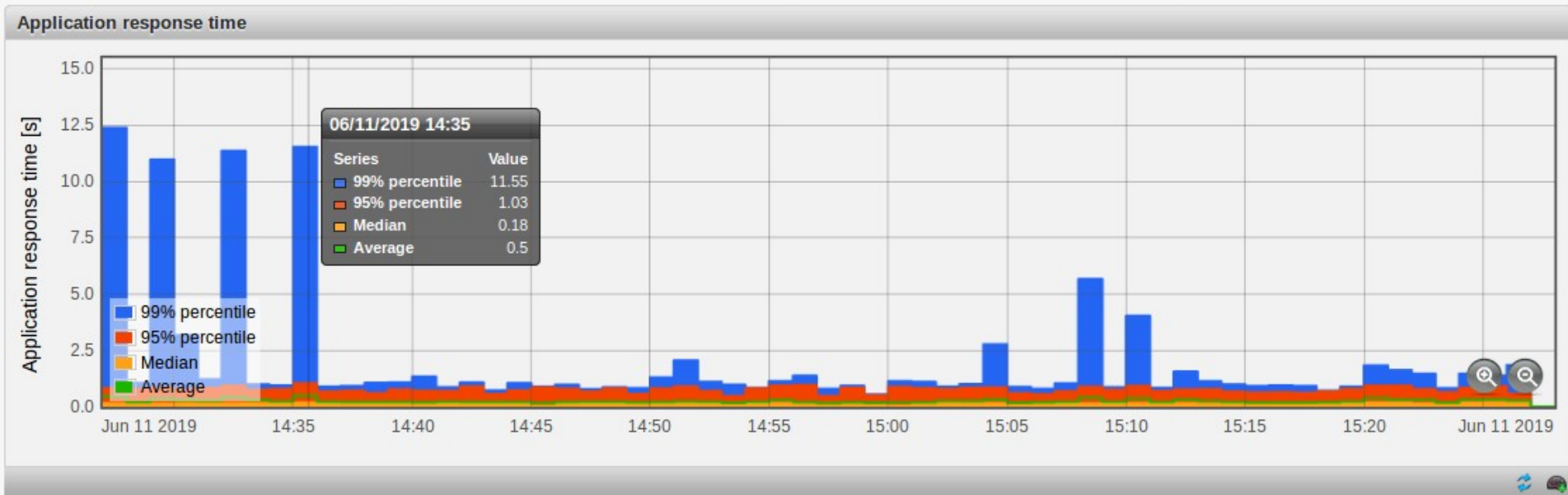
Application: WEBAPP_172.28.110.21

APM index

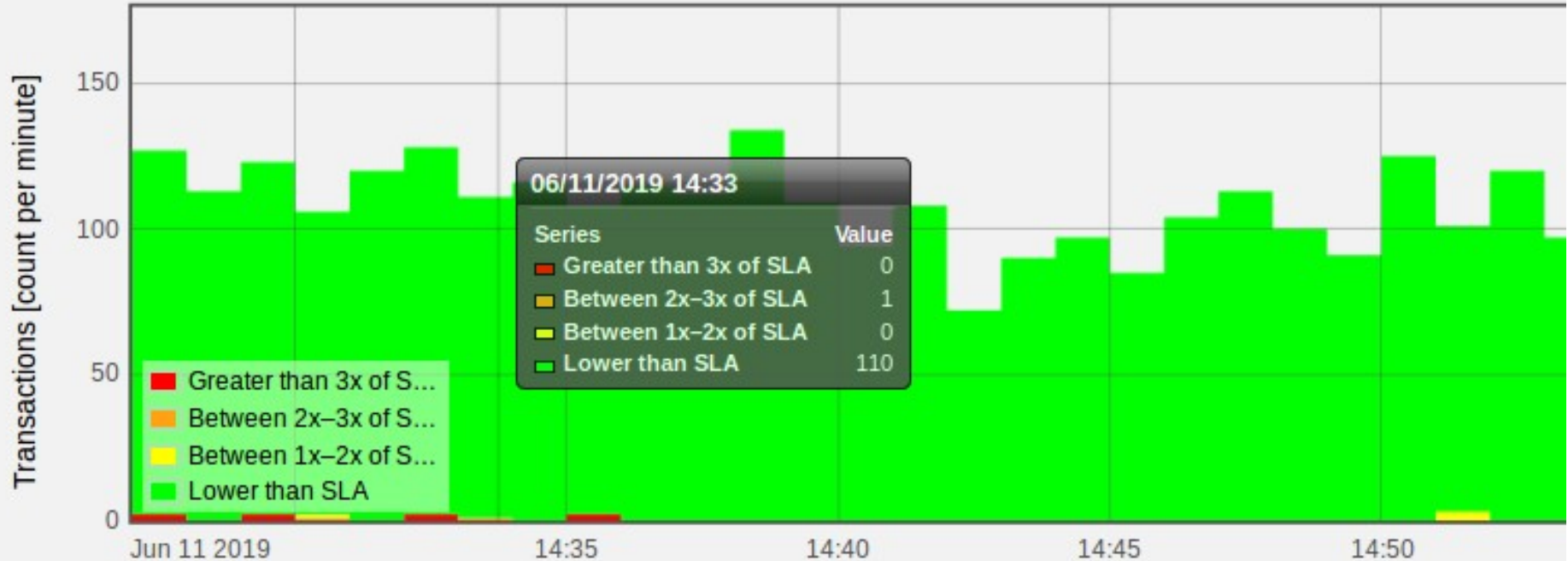
95.0

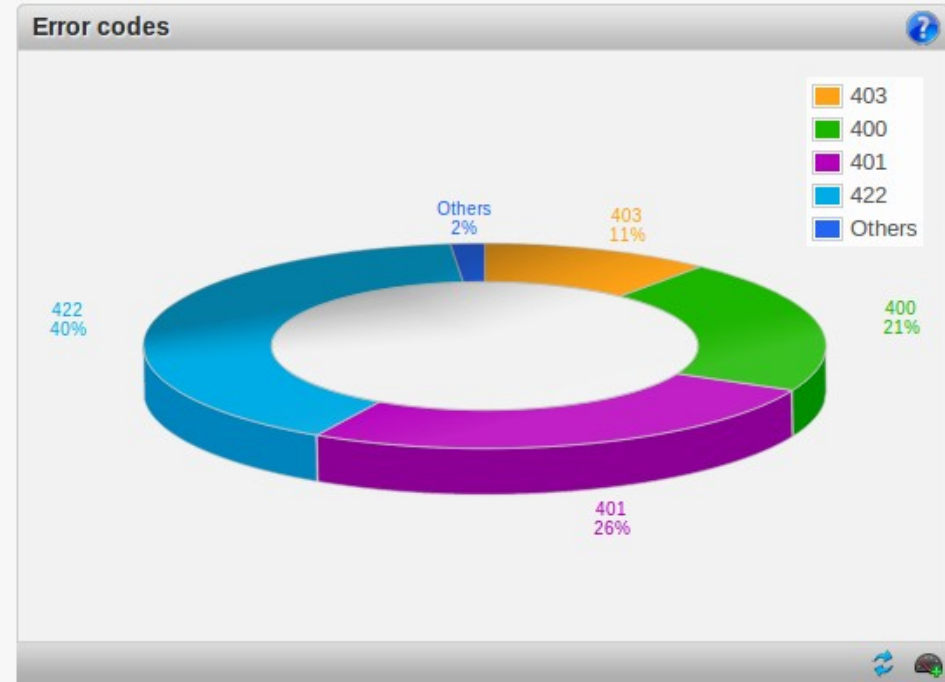
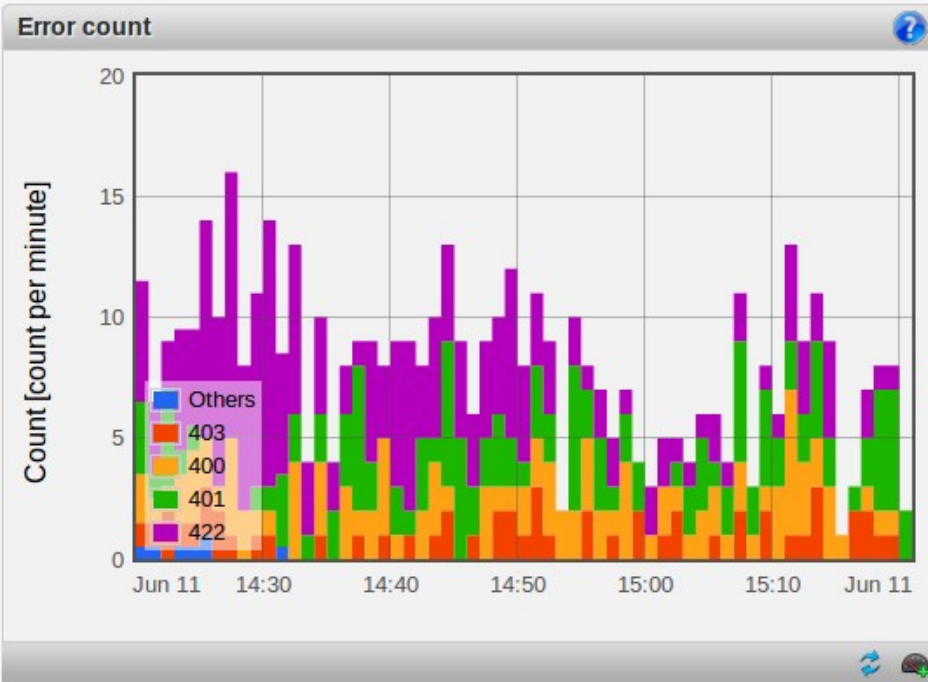
APM index



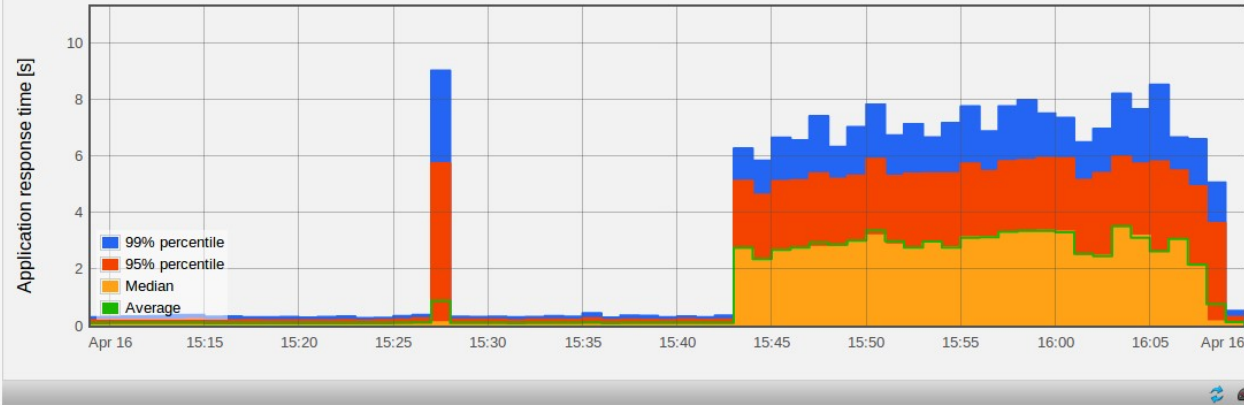


Transaction count based on SLA

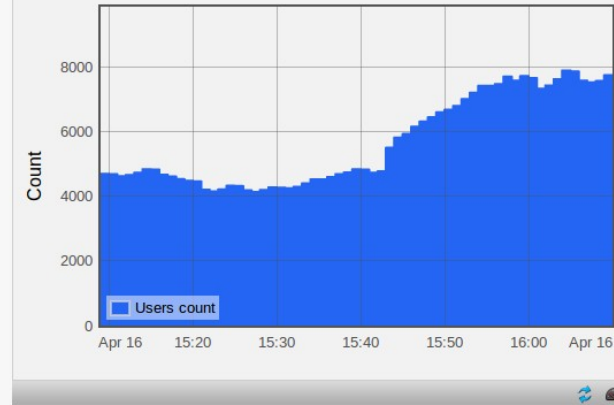




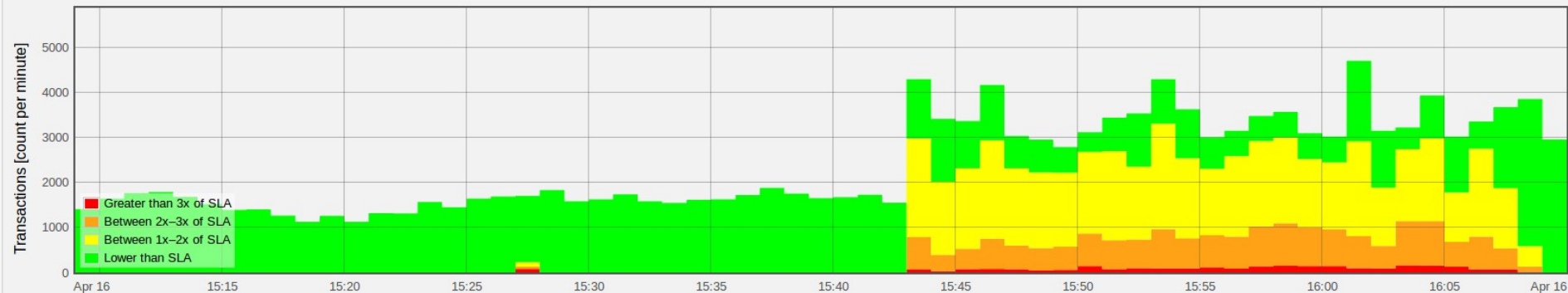
Application response time



Parallel users count



Transaction count based on SLA



Instances of transactions (SQL)

 Set filter
  Select filter
  Save filter
  Export a CSV

Show/hide columns

	SQL query	Start	Application respons...	Network transport time	Size	Client IP	Request size	Response size
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:05...	0.004	0.011	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:25...	0.001	0.005	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:50...	0.003	0.008	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:00...	0.001	0.009	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:15...	0.001	0.012	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:20...	0.001	0.011	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:44...	0.001	0.014	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:04...	0.001	0.008	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:09...	0.003	0.012	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:55...	0.002	0.006	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:39...	0.001	0.011	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:10...	0.003	0.007	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:34...	0.004	0.013	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:19...	0.003	0.008	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:15:14...	0.002	0.008	337.81 KB	172.28.110.21 	42 B	337.77 KB
	SELECT key, value, modified_at FROM ...	06/11/2019 21:16:30...	0.003	0.009	337.81 KB	172.28.110.21 	42 B	337.77 KB

Number of records: 231 157

>

Detail

Application: DBMS

06/11/2019

Transactions: SELECT FROM [REDACTED]

21:49:57,555 — 21:50:01,771

General

Transactions SELECT FROM [REDACTED] ...
 Start 06/11/2019 21:49:57,555
 End 06/11/2019 21:50:01,771
 Application response ... 4.215 s
 Network transport time 0.000 s
 SLA 0.100 s
 Size 510 B
 Session 172.28.110.21
 Username trans

Request

Time of request 06/11/2019 21:49:57,555
 Network request trans... 0.000 s
 Request size 393 B
 SQL
 SQL query -- TEMPLPATH: templates/...
 SQL message type Sql
 Auth (empty)
 Database [REDACTED]
 Error code 0

Response

Time of response 06/11/2019 21:50:01,771
 Network response tra... 0.000 s
 Response size 117 B

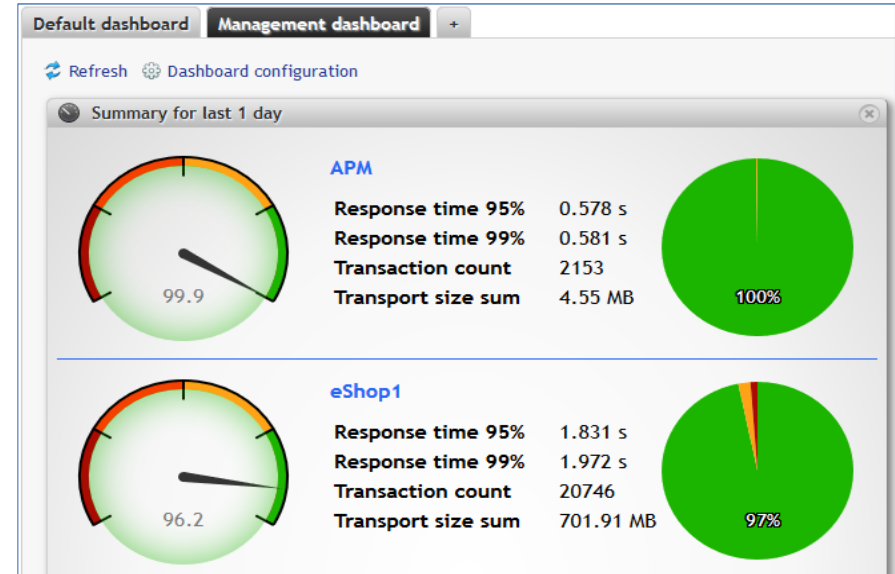
Connections

Client IP 172.28.110.21
 Client port 27719
 Server IP 172.28.110.53
 Server port 5432

SQL query

```
-- TEMPLPATH: templates/sql/[REDACTED].sql.tpl SELECT '[REDACTED]',
count(*), count(CASE WHEN [REDACTED] = 'locked' AND [REDACTED] until
>= CURRENT_TIMESTAMP THEN 1 ELSE NULL END) FROM [REDACTED] JOIN [REDACTED] using
(ad id, action id) WHERE [REDACTED] = '[REDACTED]' AND [REDACTED] IN
('[REDACTED]', 'locked');
```

- a felhasználó szemszögéből monitoroz
- agent nélkül, transzparensen
(switch port mirrorból táplálva)
- rámutat hogy hálózat, alkalmazás
vagy adatbázis probléma van-e
inkább
- kategorizál
- hibakódok
- SLA-t mér
- mindezt http/https és SQL
alkalmazásokon



- A szokásostól eltérő hálózati jelenségeket jelzi
- Network behaviour analysis (NBA)
 - user input
 - machine learning
 - feedback
- Példák:
 - 100-szor annyi levél ment ki, mint szokott,
 - elkezdtek páran másik DNS szervert használni,
 - 10-szer akkora a forgalom, mint az szokott lenni,
 - dictionary attack, stb...



- gyorsan üzembe helyezhető
- agentless
- transparens
- felhasználó szemszögéből is monitoroz
- minden modulja ugyanazon alapszik: IPFIX analitika
- a felhőszolgáltatók is adnak ki magunkból IPFIX jellegű információt, így a felhőben futó rendszerinket is be tudjuk alá vonni





ANDREWS
IT ENGINEERING

ANDREWS IT ENGINEERING KFT.

1138 Budapest, Tomori utca 34. \ 2. épület \ 1. emelet
+36 1 428 0600 \ www.andrews.hu