

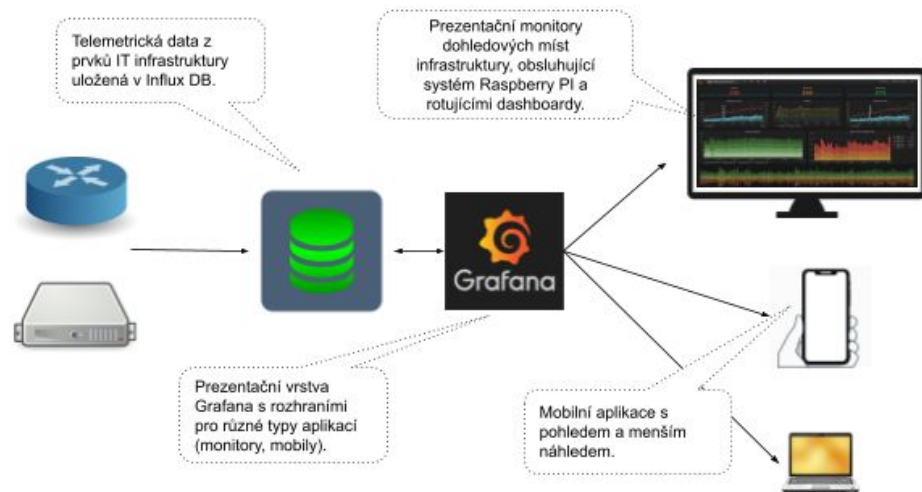
Telemetrie IT infrastruktury na VŠB-TU Ostrava

Jakub Kalnik

FRC 646/2019

Co si pod telemetrií představit

- Sběr telemetrických dat z různých zdrojů - Telegraf (VMware, telemetrie OS, vlastní skripty, SNMP), ELK stack (parsování logů, Netflow).
- Telemetrická data se ukládají do InfluxDB, Elasticsearch.
- Telemetrii zobrazujeme v Grafaně.



Proč jsme to vůbec dělali

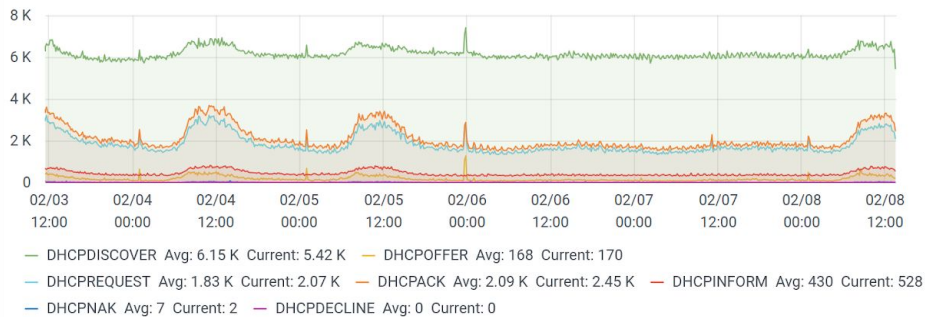
- Nagios/Icinga stavy vzorkuje v určené periodě (většinou v příliš dlouhé).
- Nagios/Icinga umí jen ok,warning,error stavy.
- Vzorkujeme s malou periodou (typicky 1s).
- Rozlišení až na μs (v případě parsovaných logů).
- Zobrazení dat a statistické operace můžeme dělat dodatečně.

Statistiky - logy DHCP a RADIUS serverů

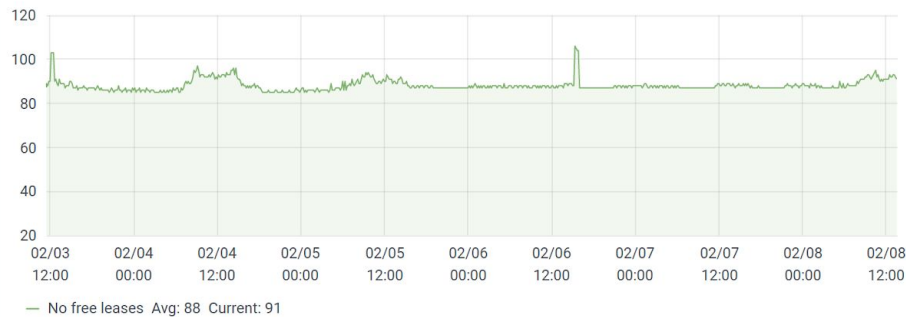
TV / NOC - TV ☆ 🔗

📊 📄 ⚙️ 🖨️ < 2021-02-03 11:29:37 to 2021-02-08 13:38:28 > 🔍 ↺ ↻

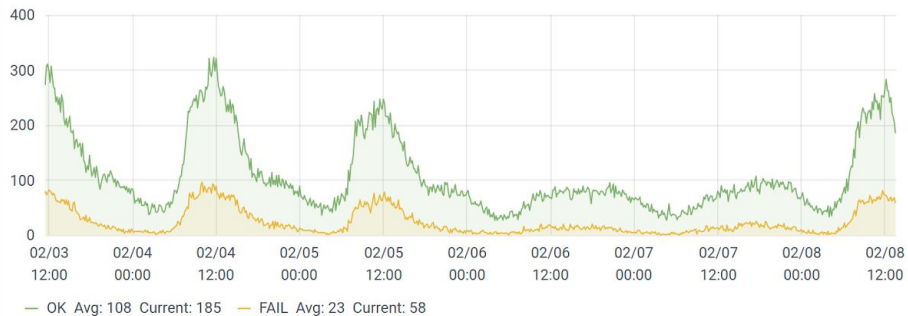
DHCP traffic



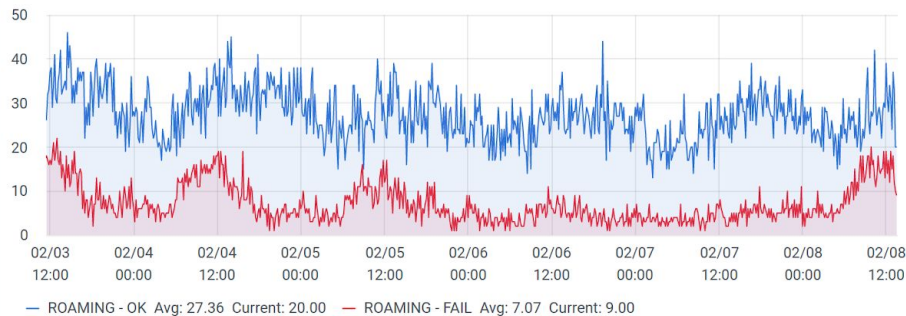
DHCP - No free leases - unique count



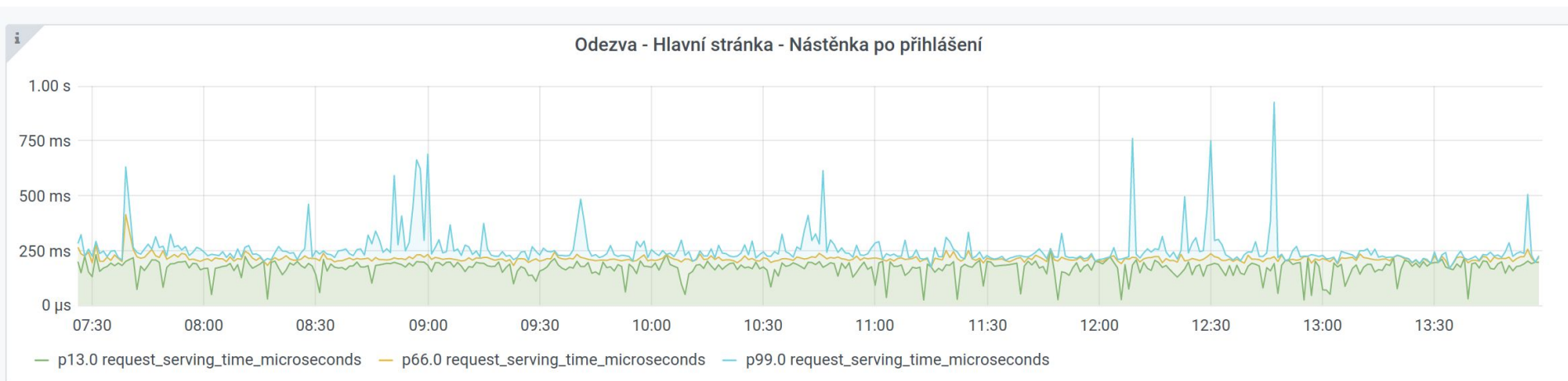
Radiator - vsb users auth - unique count



Radiator - roaming users auth - unique count



Percentily odezvy webového serveru

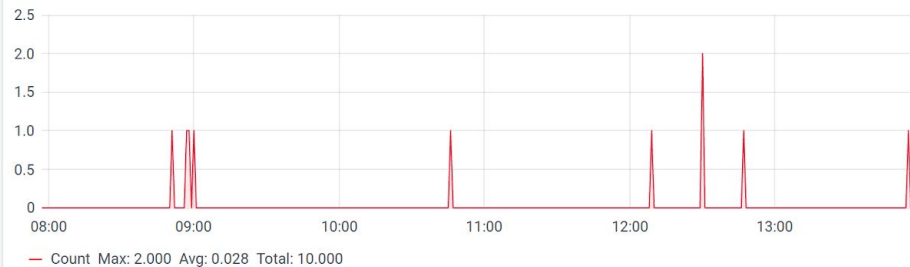


Statistiky webového serveru

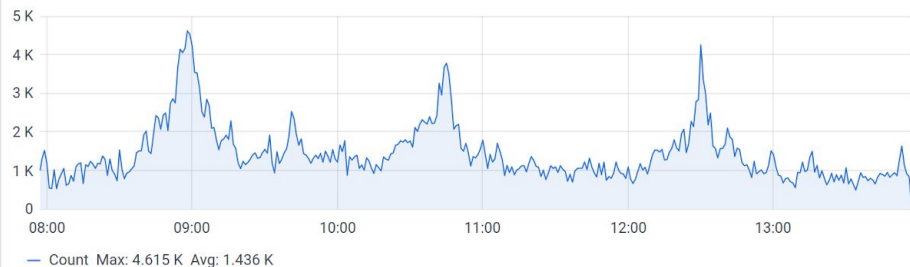
Počty unikátních přihlášení do LMS (nová přihlášení za minutu)



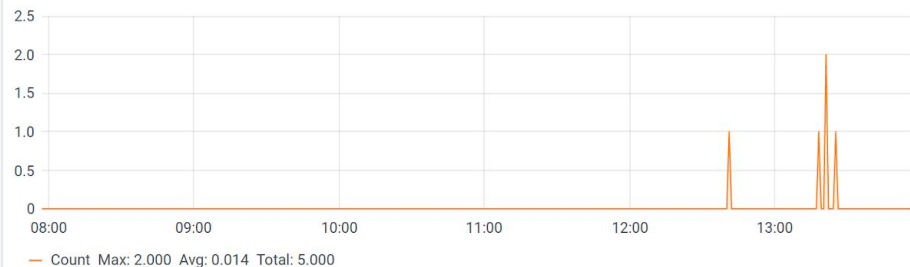
Počty přihlašovacíh požadavků, které se odbavovaly déle než 0.5 sekundy



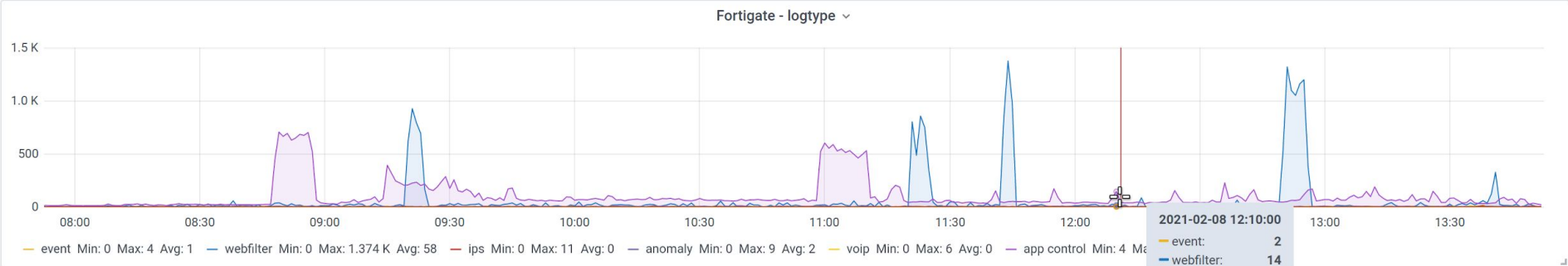
Celkový počet úspěšně zpracovaných požadavků serverem LMS (http kódy 20x, 30x)



Celkový počet neúspěšně zpracovaných požadavků serverem LMS (http kódy 50x)



Statistiky - logy IPS Fortigate



Fortigate - Events detail

@timestamp	action	hostname	msg	src	subtype
2021-02-08 13:52:20	dropped	codedexchange.com	URL blocked by malicious-url-list	158.196. [REDACTED]	ips
2021-02-08 13:52:17	dropped	codedexchange.com	URL blocked by malicious-url-list	158.196. [REDACTED]	ips
2021-02-08 13:38:30	dropped	down.dd799aa.com	URL blocked by malicious-url-list	2001:718:1001 [REDACTED]	ips
2021-02-08 13:38:30	dropped	down.dd799aa.com	URL blocked by malicious-url-list	2001:718:1001: [REDACTED]	ips
2021-02-08 13:38:26	dropped	xpltm.mea5ms.com	URL blocked by malicious-url-list	158.196. [REDACTED]	ips

2021-02-08 12:10:00

- event: 2
- webfilter: 14
- ips: 0
- anomaly: 9
- voip: 0
- app control: 143

Netflow - statistiky

TV / Netflow - TV ☆ 🔗



now-90m to now-30m ▾



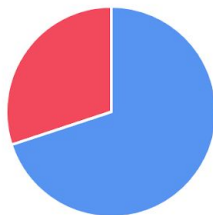
IP protocols



total percentage

TCP	280 GB	76.7%
UDP	84.8 GB	23.3%
Others	85.4 MB	0.0%

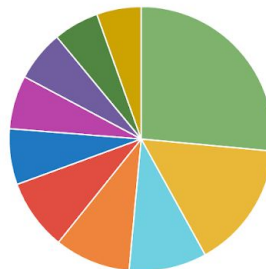
IPv4 vs IPv6



total percentage

IPv4	255 GB	69.9%
IPv6	109.6 GB	30.1%

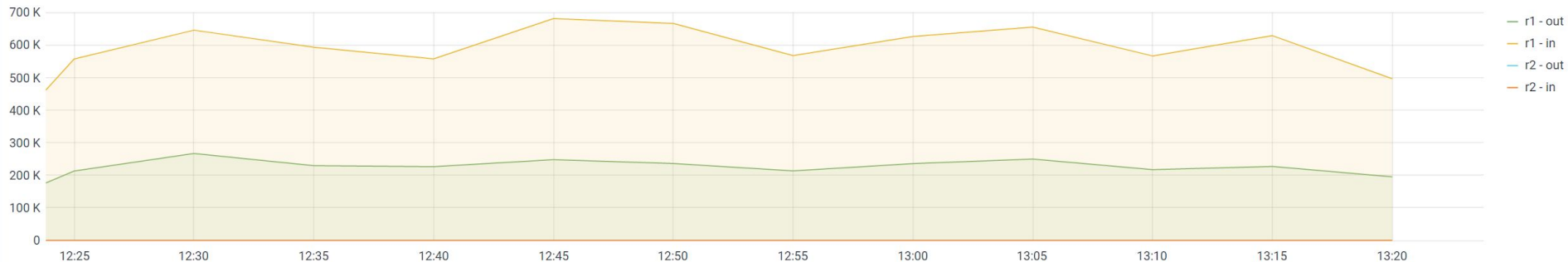
TOP 10 destination ports



total percentage

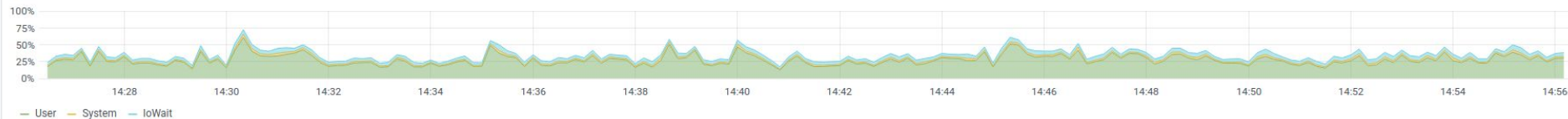
https (TCP/443)	11.99 GB	26.5%
ipsec-nat-t (UDP/4500)	7.01 GB	15.5%
plethora (UDP/3480)	4.31 GB	9.5%
TCP/59547	4.21 GB	9.3%
TCP/63038	3.92 GB	8.7%
TCP/50628	3.09 GB	6.8%
cleanerliverc (UDP/3481)	2.958 GB	6.5%
TCP/57456	2.817 GB	6.2%
search-agent (UDP/1234)	2.517 GB	5.6%
openvpn (UDP/1194)	2.470 GB	5.5%

Border routers - number of sessions

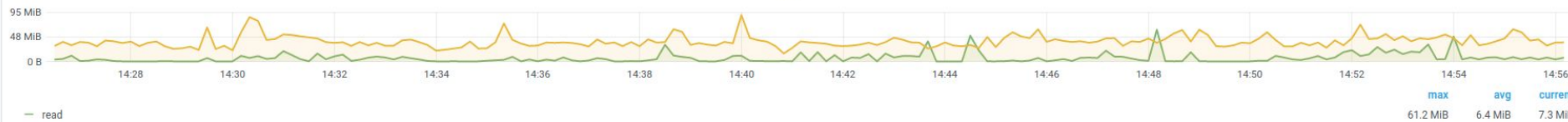


Telemetrie OS

CPU (%)



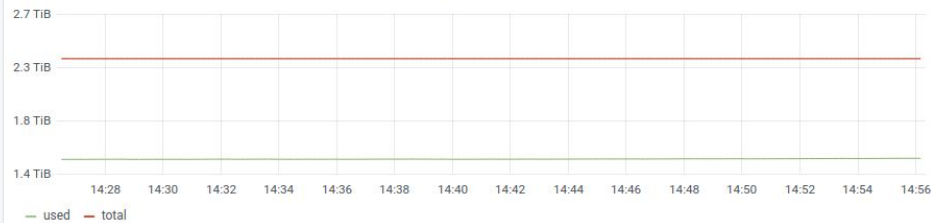
Disk IO



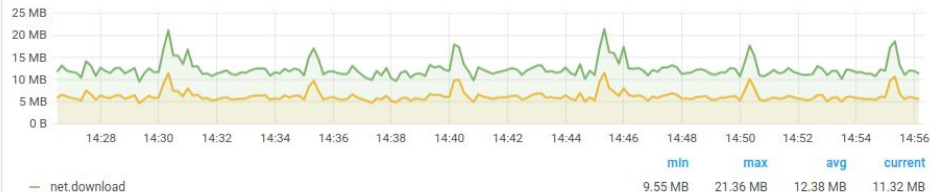
MEM



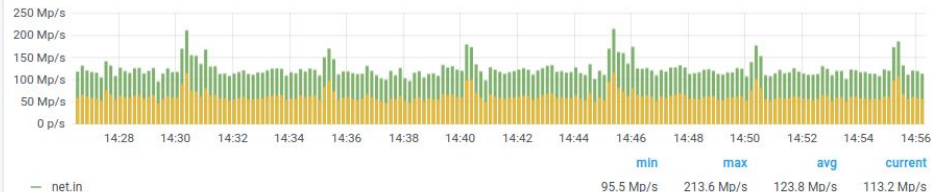
/data Size



Network Usage - ens192



Network Packets - ens192



VMware - přehled - cluster

CPU Usage

100 GHz

CPU Total

446 GHz

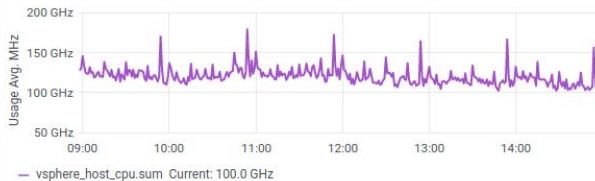
RAM Usage

2.121 TB

RAM Total

3.171 TB

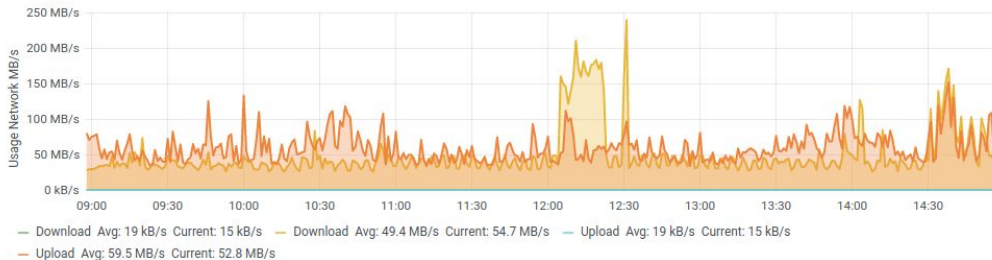
Cluster CPU usage



Cluster RAM usage



Cluster Network Usage



TOP 10 - VMs by CPU usage

vmname

CPU usage ▾

6 GHz

5 GHz

4 GHz

3 GHz

3 GHz

3 GHz

3 GHz

Ping na routery VŠB

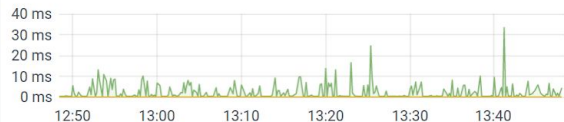
TV / Ping - LAN - TV New ☆ 🔗

📊 📄 ⚙️ 🖨️ ⌚ Last 1 hour 🔍 ↺️ ↻️

vsb_routers

All ▾

██████.vsb.cz



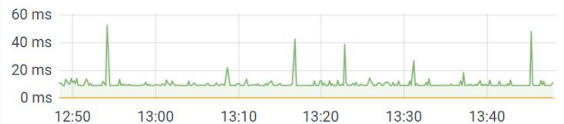
	min	max	current
IPv4	0.3 ms	33.4 ms	4.4 ms
IPv6	0 ms	0 ms	0 ms

██████.vsb.cz



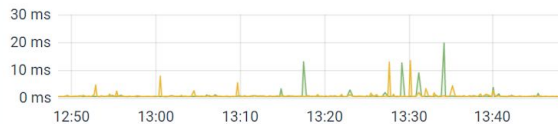
	min	max	current
IPv4	8.4 ms	85.0 ms	8.5 ms
IPv6	8.4 ms	12.5 ms	8.4 ms

██████.vsb.cz



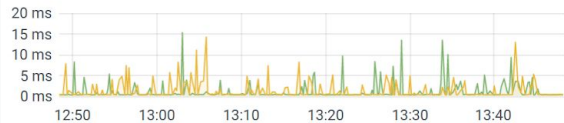
	min	max	current
IPv4	8.7 ms	52.2 ms	11.0 ms
IPv6	0 ms	0 ms	0 ms

██████.vsb.cz



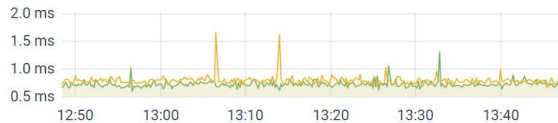
	min	max	current
IPv4	0.4 ms	19.7 ms	0.6 ms
IPv6	0.4 ms	13.3 ms	0.5 ms

██████.vsb.cz



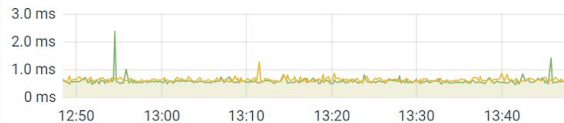
	min	max	current
IPv4	0.3 ms	15.3 ms	0.4 ms
IPv6	0.3 ms	14.2 ms	0.4 ms

██████.vsb.cz



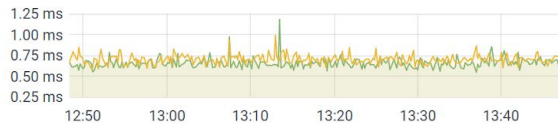
	min	max	current
IPv4	0.6 ms	1.3 ms	0.7 ms
IPv6	0.7 ms	1.7 ms	0.8 ms

██████.vsb.cz



	min	max	current
IPv4	0.4 ms	2.4 ms	0.5 ms
IPv6	0.5 ms	1.3 ms	0.6 ms

██████.vsb.cz



	min	max	current
IPv4	0.5 ms	1.2 ms	0.7 ms
IPv6	0.6 ms	1.0 ms	0.7 ms

Odběr sálů v datovém centru

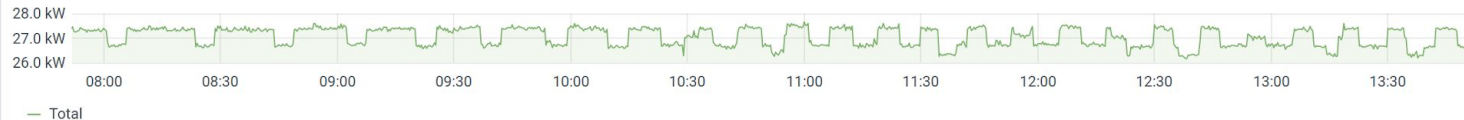
TV / TV - Electricity readout - Nová aula 1/2 ☆ 🔊



⌚ Last 6 hours ▾



Příkon - Celkem - Nová Aula (bez NA101e)



Příkon - Celkem - Nová Aula (bez NA101e)



Příkon - (NA101a)



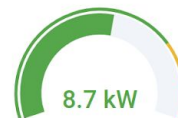
Příkon - (NA101a)



Příkon - Datacentrum (NA101b)



Příkon - Datacentrum (NA101b)



Příkon - CESNET (NA101c)



Příkon - CESNET (NA101c)



Přínosy

- Výrazné zvýšení povědomí o stavu IT infrastruktury.
- Využití v bezpečnosti, zajištění provozuschopnosti infrastruktury, detekování anomálií.
- Zvýšení kompetencí helpdeskového pracoviště - ví, že se stala porucha.

Děkuji za pozornost

Jakub Kalník