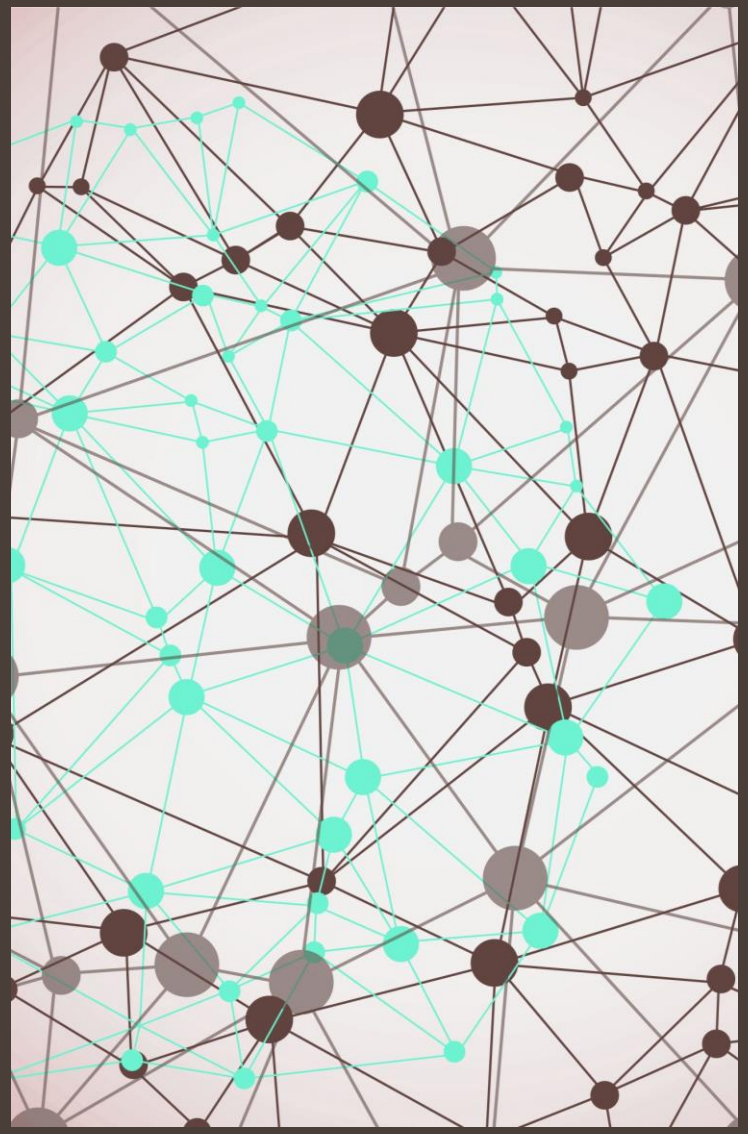
Hard questions of
Windows server monitoring

Items and Alerts tweaking and

Zabbix historical improvements

by GIORS GEKS



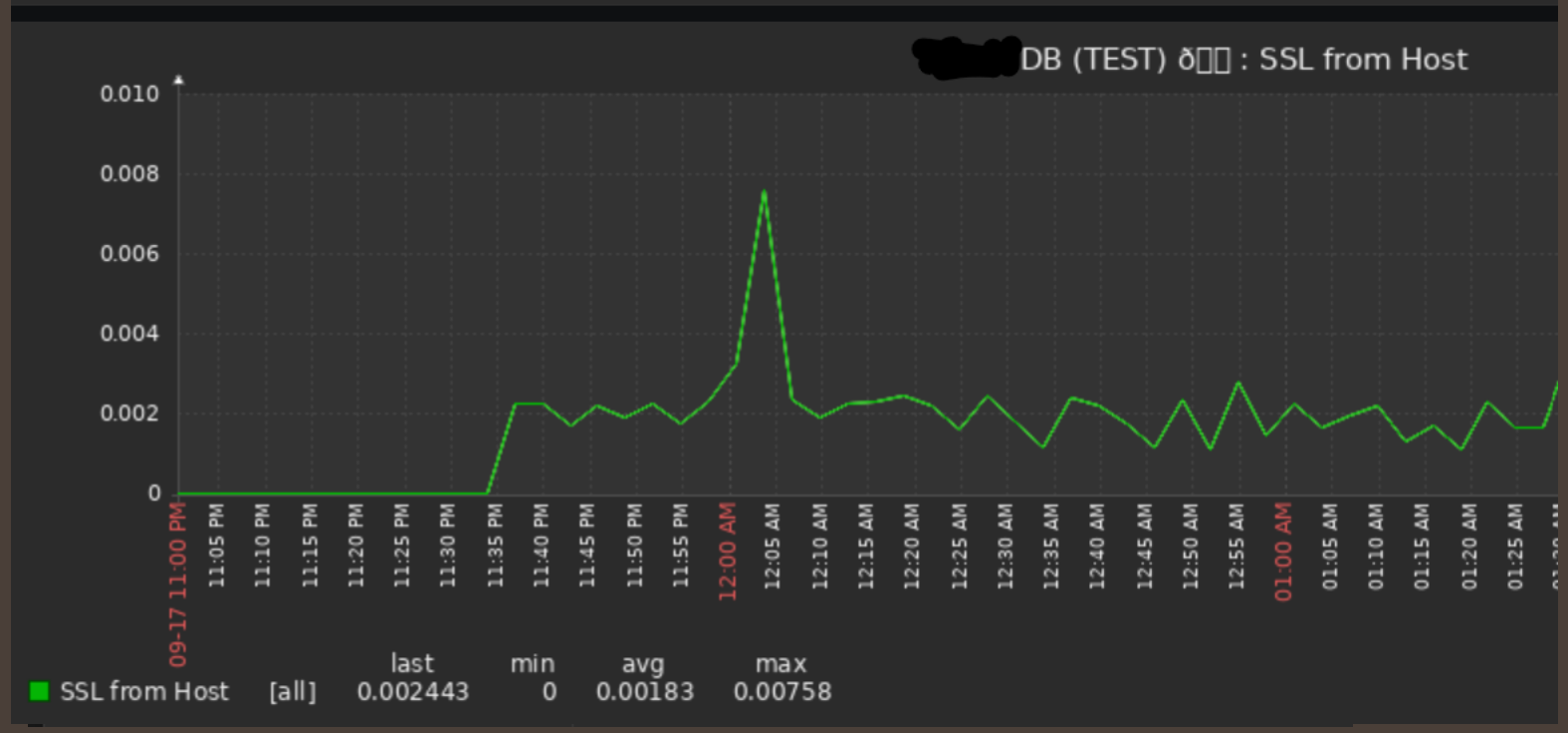
Zabbix improvements during time

- Availability monitoring by DNS name
- EXE monitoring
- HDD monitoring
- Timeleft

How to measure availability?

Remote monitoring Monitor host>host:port availability 2012-2023

Host	Name ▲	Last check	Last value	Last check	Last value
PYTHON-DB	SSH from Host	1m 23s	0	1m 23s	0
PYTHON-WEB	SSH from Host	22s	0	22s	0
✕ IT -ADMIN	SSH from Host	2s	0.005206	2s	0.005206



https://www.zabbix.com/documentation/4.0/en/manual/config/items/itemtypes/simple_checks

UserParameter=CheckDnsAndPort,powershell.exe -NoProfile -ExecutionPolicy bypass Test-NetConnection PYTHON-WEB.CFLA.GOV.LV -Port 443 -InformationLevel Quiet

DNS:PORT MONITORING

using POWERSHELL

Host	Name ▲	Last check	Last value
PYTHON -WEB	SQL Server Available	2m 32s	True
PYTHON -WEB	WEB server available	2m 33s	True

*C:\Program Files\Zabbix Agent 2\zabbix_agent2.conf - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

zabbix_agent2.conf

```
### Option: UserParameter
#   User-defined parameter to monitor. There can be several user-defined parameters.
#   Format: UserParameter=<key>,<shell command>
#   See 'zabbix_agentd' directory for examples.
#
# Mandatory: no
# Default:
# UserParameter=
UserParameter=CheckSqlByDns,powershell.exe -NoProfile -ExecutionPolicy bypass Test-NetConnection PYTHON-SQL.CFLA.GOV.LV -Port 1433 -InformationLevel Quiet
UserParameter=CheckDnsAndPort,powershell.exe -NoProfile -ExecutionPolicy bypass Test-NetConnection PYTHON-WEB.CFLA.GOV.LV -Port 443 -InformationLevel Quiet
```

Item Tags Preprocessing

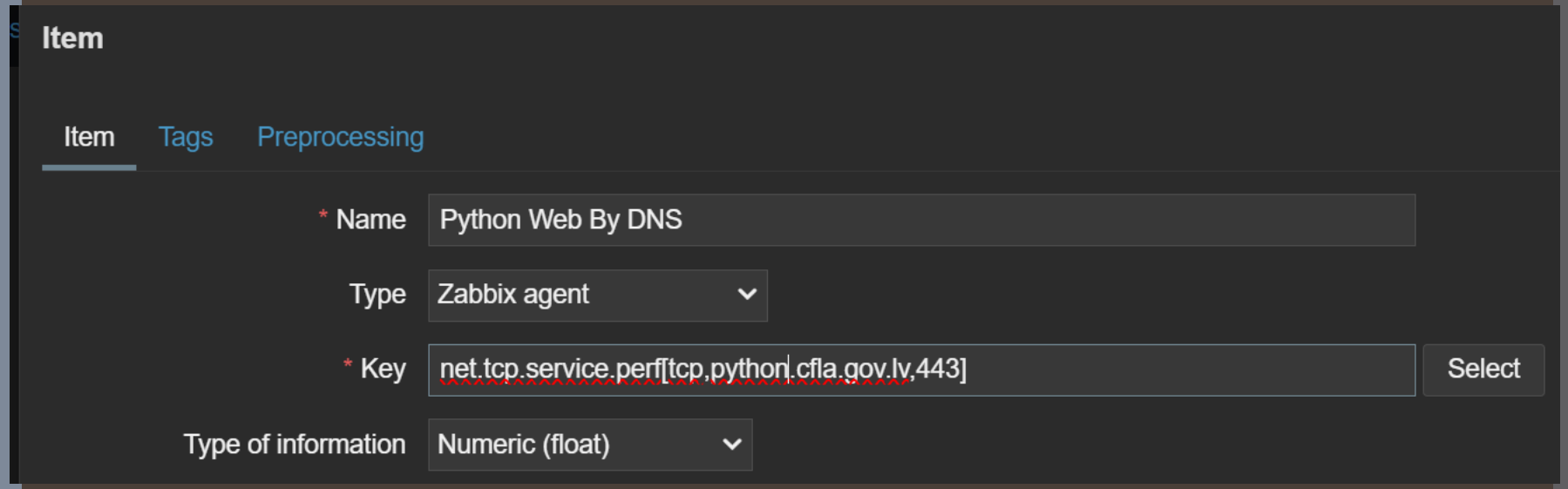
* Name	WEB server available
Type	Zabbix agent
* Key	CheckDnsAndPort Select
Type of information	Text
* Update interval	5m

https://learn.microsoft.com/en-us/powershell/module/nettcpip/test-netconnection?view=windowsserver2022-ps&viewFallbackFrom=win10-ps

Net.Tcp.Service.perf[tcp,python.cfla.gov.lv,443]

Net.Tcp.Service can check by DNS NAME

out of the box



Host	Name ▲	Last check	Last value
PYTHON- DB (TEST)	Python Web By DNS	3s	0.007222
PYTHON- WEB (TEST)	Python Web By DNS	1m 59s	0
ITN-ADMIN	Python Web By DNS	1m 41s	0.01201

Zabbix does what?

RAM used by EXE

* Name	sqlserv.exeDLX
Type	Zabbix agent
* Key	proc_info[sqlservr.exe,wkset,sum] Select
Type of information	Numeric (float)
* Host interface	192.168.7.7:10050
Units	B
* Update interval	1m
Custom intervals	Type: Flexible Scheduling; Interval: 50s; Period: 1-7,00:00-24:00; Action: Remove; Add
* History storage period	Do not keep history / Storage period 90d
* Trend storage period	Do not keep trends / Storage period 365d

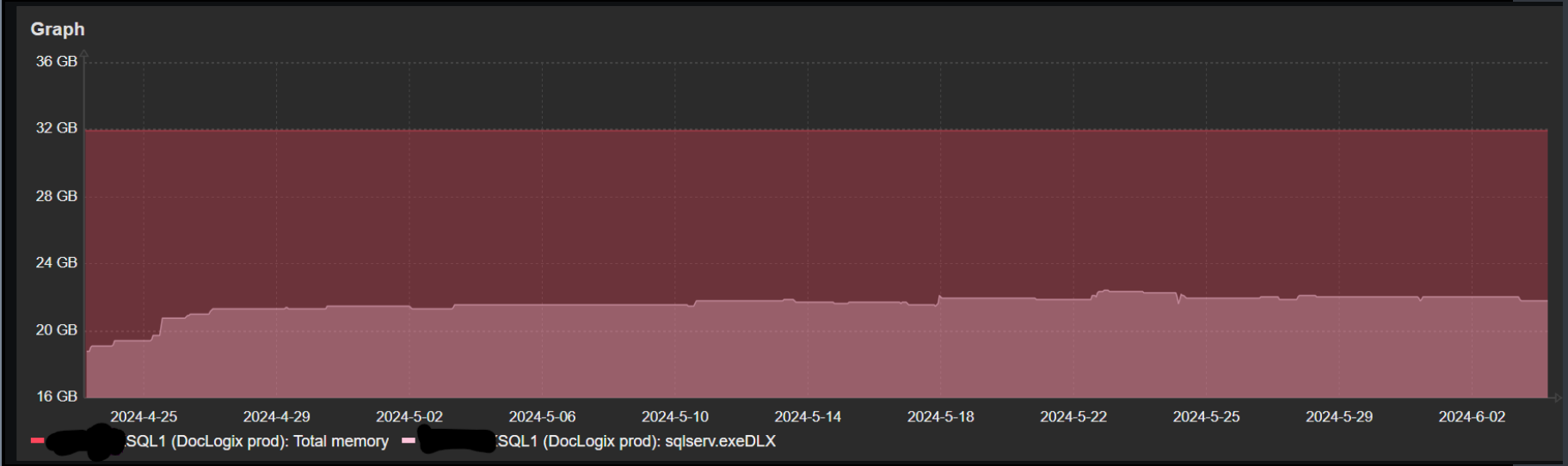
Item | Tags | Preprocessing 1

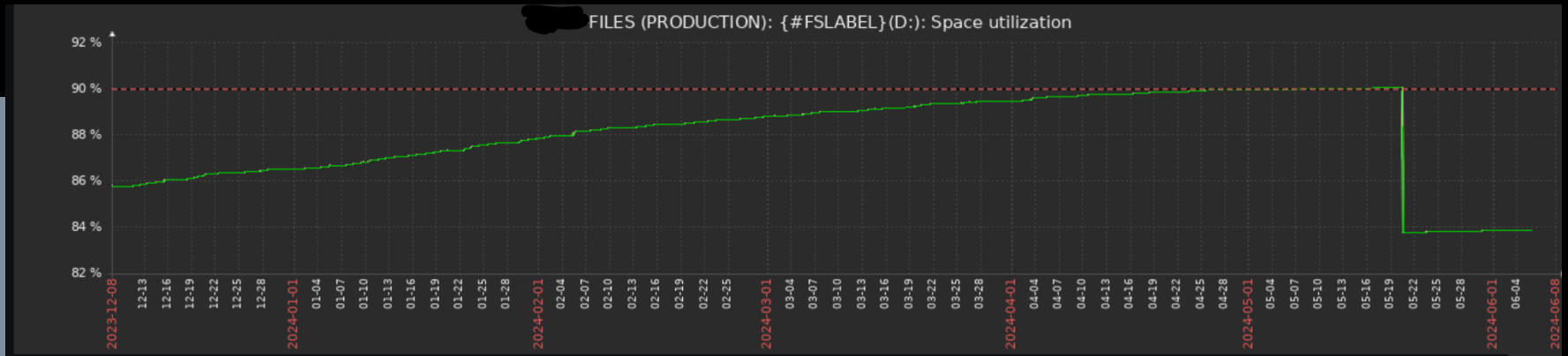
Preprocessing steps	Name	Parameters
1:	Custom multiplier	1024

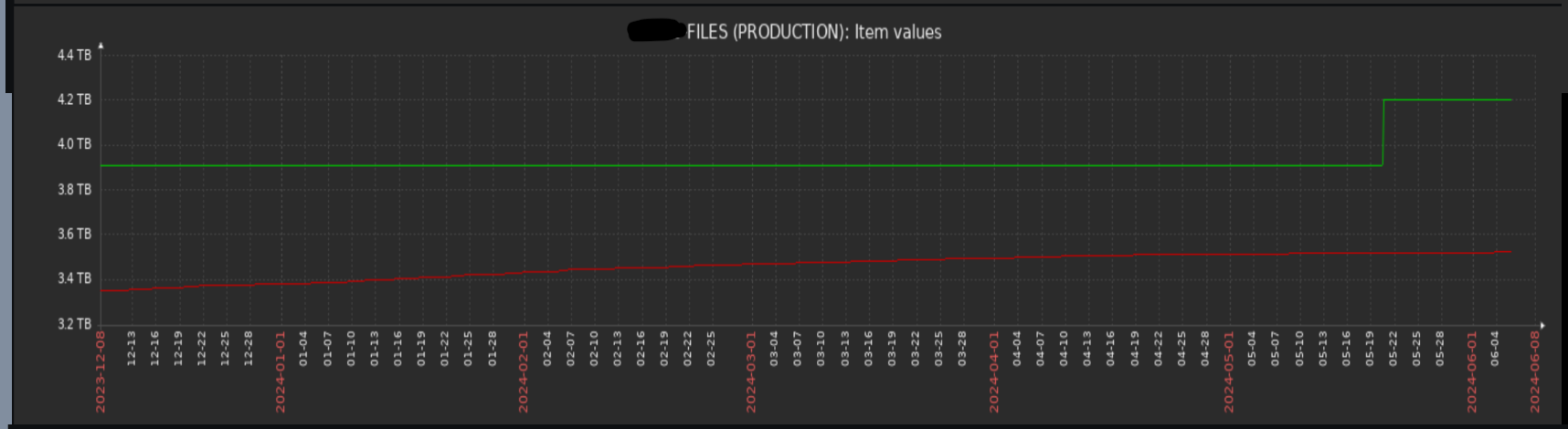
Add

True or false?

- MicroSoft SQL eats all RAM?







Proper HDD monitoring

300GB*12months*7years/2

Local ~300€

Azure ~ 1470$

Amazon ~ 1008 $

Host	Name ▲	Last check	Last value	Change
[redacted] FILES (PRODUC…	KPFDTimeleft2	9m 5s	13y 2M 3d	-2M 2d 6h
[redacted] FILES (PRODUC…	KPFilesTimeleftCalc	3h 9m 21s	7y 8M 26d	-2M 29d 17h

https://azure.microsoft.com/en-us/pricing/details/managed-disks/

https://aws.amazon.com/ebs/pricing/

Forecasting Trigger Functions

Host	Name ▲	Last check	Last value	Change
PYTHON-WEB	FDriveTimeleftFPUsed	33m 11s	8y 1M 19d	-22d 21h 37m
PYTHON-WEB	FDriveTimeleftFPUsed	33m 11s	8y 1M 19d	-22d 21h 37m
FILES (PROD)	KPFDTimeleft2	4h 33m 5s	9y 6M 28d	+5M 4d 16h
FILES (PROD)	KPFilesTimeleftCalc	4h 33m 21s	9y 6M 22d	+8M 9d 13h
Redmine D)	RedmineTimeleftdaysroot	33m 3s	12y 7M 19d	+5d 19h 26m
Zabbix server	ROOTtimeleft90	33m 10s	2M 28d 7h	+1h 26m 20s

Table 4: Exact formulas used in calculations

		linear	polynomial N	exponential	logarithmic	power
`forecast()`	value	$f^\star(t_r)$	$f^\star(t_r)$	$f^\star(t_r)$	$f^\star(t_r)$	$f^\star(t_r)$
	max	$\max\{f^\star(t_l), f^\star(t_r)\}$	*	$\max\{f^\star(t_l), f^\star(t_r)\}$	$\max\{f^\star(t_l), f^\star(t_r)\}$	$\max\{f^\star(t_l), f^\star(t_r)\}$
	min	$\min\{f^\star(t_l), f^\star(t_r)\}$	*	$\min\{f^\star(t_l), f^\star(t_r)\}$	$\min\{f^\star(t_l), f^\star(t_r)\}$	$\min\{f^\star(t_l), f^\star(t_r)\}$
	delta	$\lvert f^\star(t_l) - f^\star(t_r)\rvert$	*	$\lvert f^\star(t_l) - f^\star(t_r)\rvert$	$\lvert f^\star(t_l) - f^\star(t_r)\rvert$	$\lvert f^\star(t_l) - f^\star(t_r)\rvert$
	avg	$\frac{f^\star(t_l)+f^\star(t_r)}{2}$	$\frac{F(t_r)-F(t_l)}{t_r-t_l}$	$\frac{f^\star(t_r)-f^\star(t_l)}{(t_r-t_l)a_1}$	$f^\star(t_r)+a_1\left(\log\left(1+\frac{t_r-t_l}{t_l}\right)\frac{t_l}{t_r-t_l}-1\right)$	$\begin{cases}\frac{(f^\star(t_r)t_r-f^\star(t_l)t_l)}{(t_r-t_l)(a_1+1)}, & \text{if } a_1 \neq -1\\ \frac{\exp(a_0)\log\left(1+\frac{t_r-t_l}{t_l}\right)}{t_r-t_l}, & \text{if } a_1 = -1\end{cases}$
`timeleft()`		$\frac{x_{\text{th}}-a_0}{a_1}-t_l$	**	$\frac{\log(x_{\text{th}})-a_0}{a_1}-t_l$	$\exp\left(\frac{x_{\text{th}}-a_0}{a_1}\right)-t_l$	$\exp\left(\frac{\log(x_{\text{th}})-a_0}{a_1}\right)-t_l$

Where $f^\star$ is expression from Table 1 with "best fit" coefficients, $t_l = t_{\text{"now"}}$, $t_r = t_{\text{"now"}} + t_{\text{"time"}}$, $F(t) = \sum_{n=1}^{N+1}\frac{a_{n-1}t^n}{n} + C$ is polynomial antiderivative, x_{th} is "threshold", a_i means i-th element of a from Table 2.

* We solve $\frac{df^\star(t)}{dt} = 0$ using ** (with $N' = N-1$) and search for maximum and minimum among t_l, t_r and roots lying in between; $\frac{df^\star(t)}{dt} = \sum_{n=0}^{N-1}(n+1)\,a_{n+1}t^n$.

** Exact formulas for $N = 1$ (see linear case) and $N = 2$, (Weierstrass—)Durand—Kerner method for $3 \leq N \leq 6$.

https://www.zabbix.com/documentation/5.0/assets/en/manual/config/triggers/prediction_docs.pdf

Templates

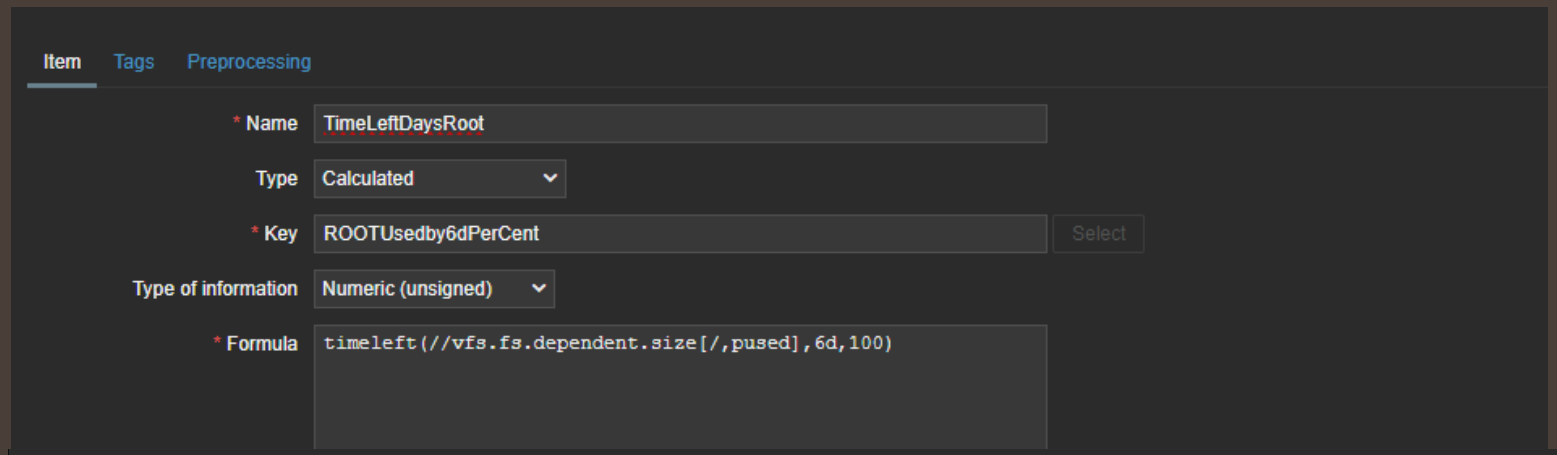
- Article with detailed explanations with
  - Windows template to monitor EXE, Timeleft and Availability
  - Linux template to monitor Timeleft

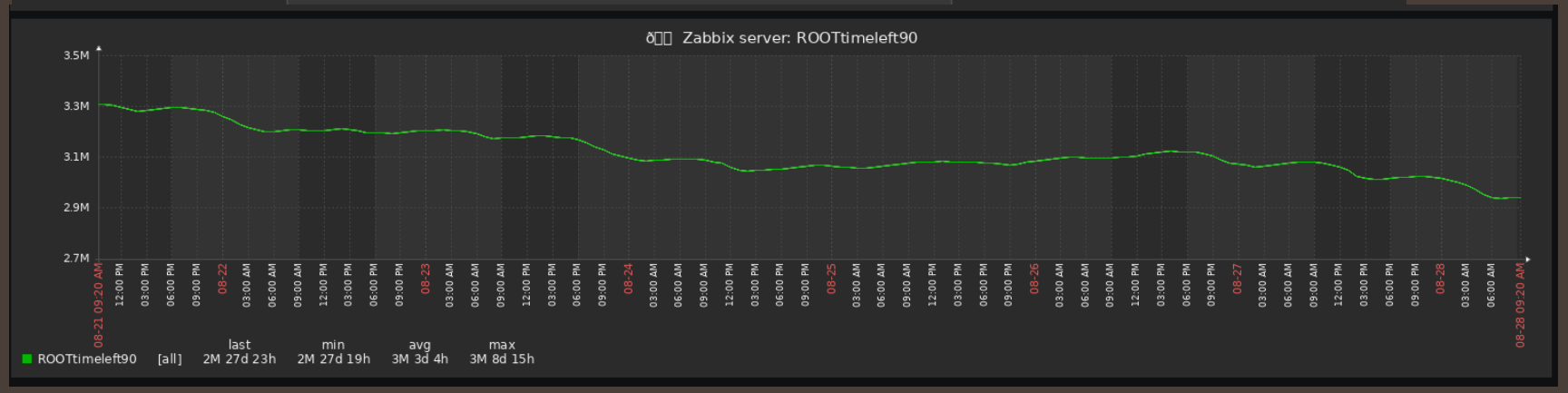
https://faqwiki.blogspot.com/2024/08/zabbix-templates-to-monitor-timeleft.html

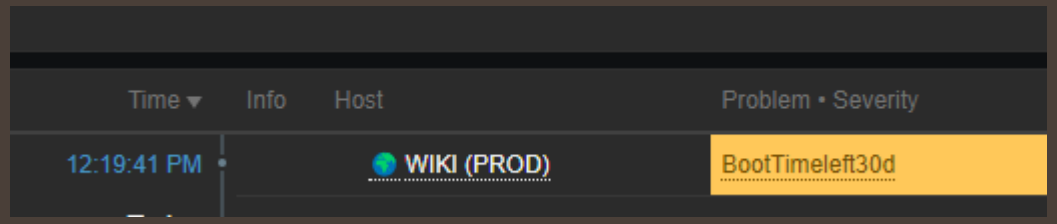
Predictive functions

Timeleft function

Forecast function







https://www.zabbix.com/documentation/current/en/manual/appendix/functions/prediction

Small step to mankind,
Big step to Admin sleep well

Message template

Message type: Problem

Subject: Problem: {EVENT.NAME}

Message:
Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {EVENT.NAME}
Host: {HOST.NAME}

Message template

Message type: Problem

Subject: {HOST.NAME}Problem: {EVENT.NAME}

Message:
Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {EVENT.NAME}
Host: {HOST.NAME}
Severity: {EVENT.SEVERITY}
Operational data: {EVENT.OPDATA}
Original problem ID: {EVENT.ID}
{TRIGGER.URL}

Update | Cancel

Conclusion

- Lot of good features are not well documented
- Use newest Zabbix7 with new functions
- Usage of experts pays back - tcp.service timeleft proc_info etc.
- Change default templates by making alerts dependent and more readable
- Use concatenated graphs in Dashboards
- Timeleft function is more useful than alert “90% disk full”

- Contact me GIORS.GEKS@GMAIL.COM