SOMONE
IT Monitoring & Event Management

ZABBIX WATCHES EVERYTHING, BUT WHO WATCHES ZABBIX?

Pascal de JESSEY

Senior Monitoring Consultant, Somone, France

pjessey@somone.fr

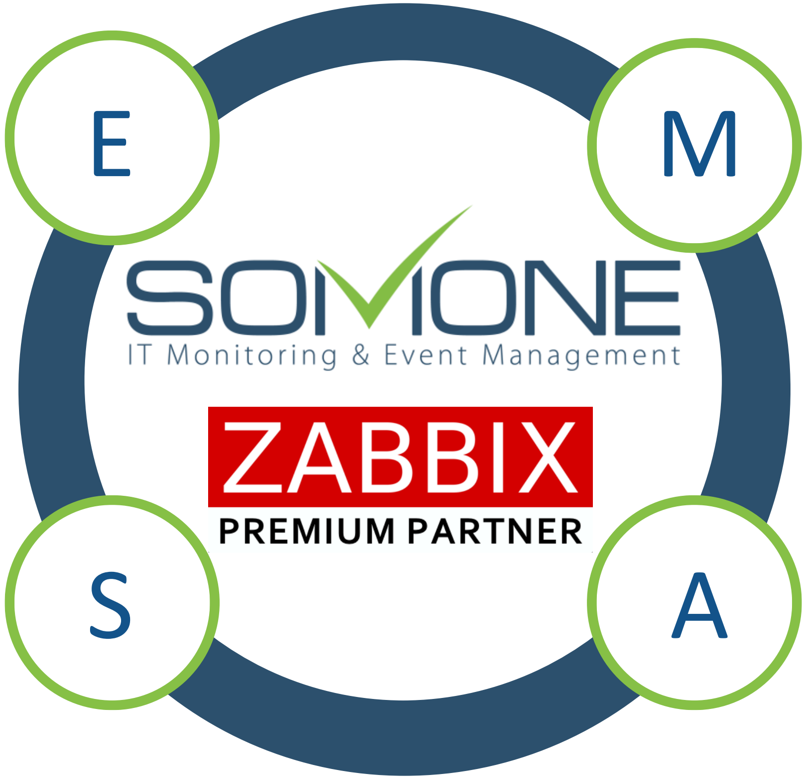
SOMONE in a nutshell

Consulting/Projects

- ✓ Audit, consulting
- ✓ Expertise on demand
- ✓ Migration, upgrade, turnkey projects, troubleshooting

Support

- ✓ Technical support and assistance services



Manage services

- ✓ Monitoring solution in managed mode
- ✓ Administration and operation of your monitoring system

Academy SOMONE ACADEMY

- ✓ Certified or custom-made training

ZABBIX
CERTIFIED TRAINER

Whoami

- my name is Pascal de JESSEY
- Zabbix user for many years ZABBIX
- Zabbix certified Trainer ZABBIX CERTIFIED TRAINER
- Linux and opensource user
- Loves to monitor the clouds ... from above

Agenda

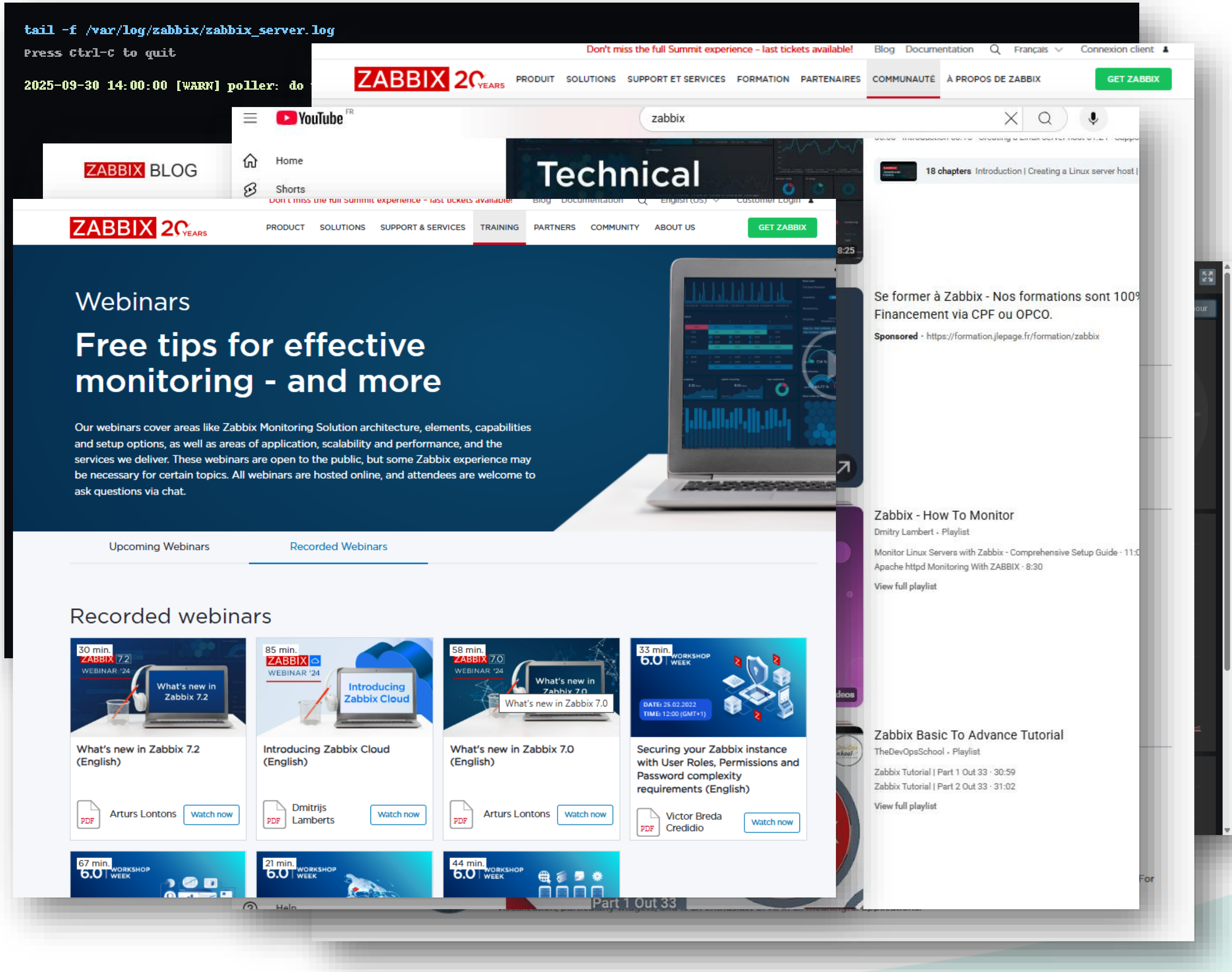
- Why this matters
- What already exists
- What we check
- Our response
- Use case & demo

Why does this matter?

- Zabbix, as a central monitoring point, becomes a single point of failure
- Misconfigurations, bottlenecks, blind spots
- We should proactively validate Zabbix health

What do we see and what already exists?

- Built-in logs
- Built-in health templates
- Advice from many different sources
  - summit
  - blogs
  - youtube
  - webinars



```
tail -f /var/log/zabbix/zabbix_server.log
Press ctrl-c to quit

2025-09-30 14:00:00 [WARN] poller: do
```

Don't miss the full Summit experience – last tickets available!

18 chapters Introduction | Creating a Linux server host |

Se former à Zabbix - Nos formations sont 100% Financement via CPF ou OPCO.

Sponsored · https://formation.jlepage.fr/formation/zabbix

Zabbix - How To Monitor
Dmitry Lambert · Playlist
Monitor Linux Servers with Zabbix - Comprehensive Setup Guide · 11:0
Apache httpd Monitoring With ZABBIX · 8:30
View full playlist

Zabbix Basic To Advance Tutorial
TheDevOpsSchool · Playlist
Zabbix Tutorial | Part 1 Out 33 · 30:59
Zabbix Tutorial | Part 2 Out 33 · 31:02
View full playlist

Webinars

Free tips for effective monitoring - and more

Our webinars cover areas like Zabbix Monitoring Solution architecture, elements, capabilities and setup options, as well as areas of application, scalability and performance, and the services we deliver. These webinars are open to the public, but some Zabbix experience may be necessary for certain topics. All webinars are hosted online, and attendees are welcome to ask questions via chat.

Upcoming Webinars | Recorded Webinars

Recorded webinars

30 min. – What's new in Zabbix 7.2 (English) – Arturs Lontons – Watch now

85 min. – Introducing Zabbix Cloud (English) – Dmitrijs Lambert – Watch now

58 min. – What's new in Zabbix 7.0 (English) – Arturs Lontons – Watch now

33 min. – Securing your Zabbix instance with User Roles, Permissions and Password complexity requirements (English) – Victor Breda Credidio – Watch now

67 min. · 21 min. · 44 min.

When do we need this?

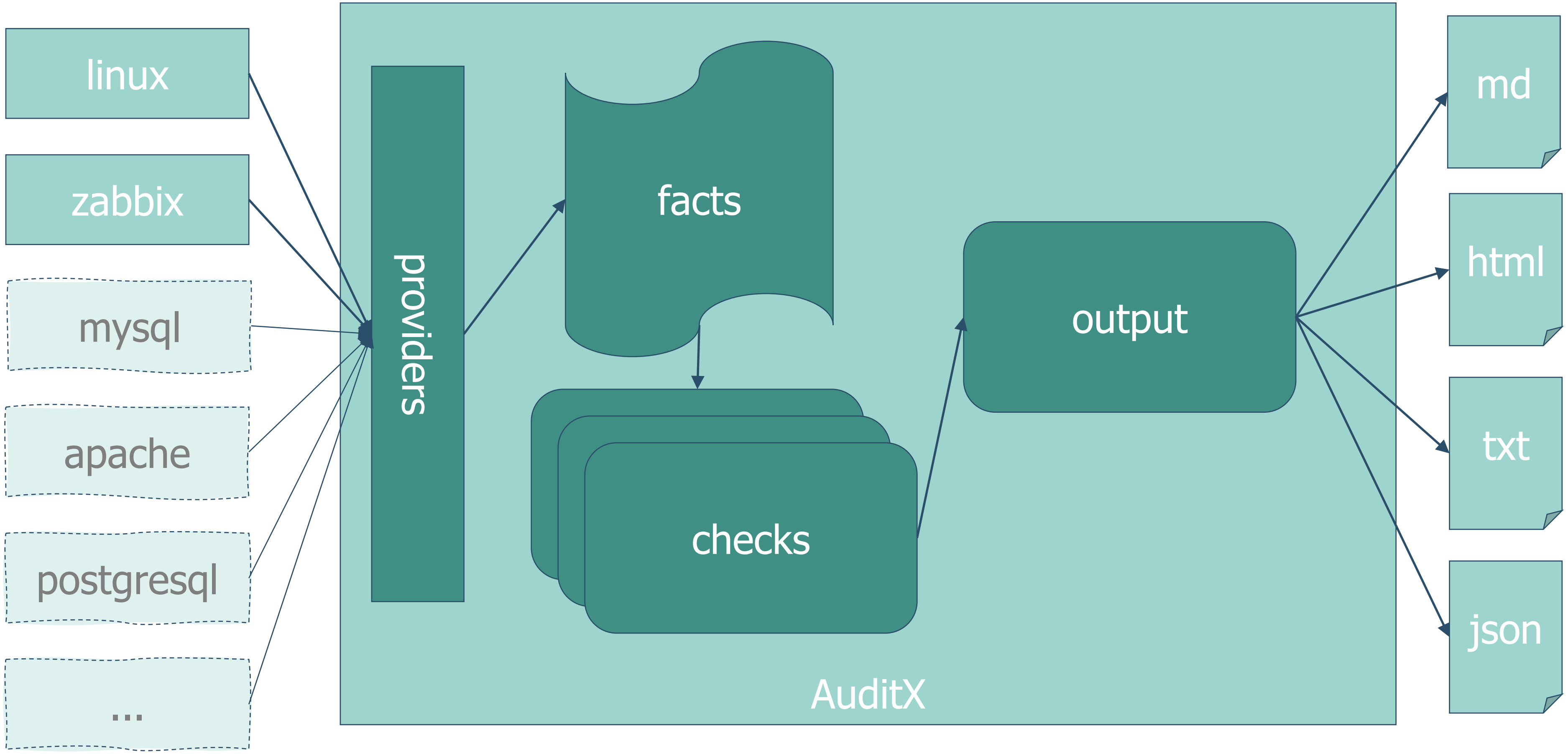
- When we switch from one Zabbix installation to another
- When we arrive on a new context without any clues about how the Zabbix installation was done
- When we have to check a Zabbix installation after weeks of administration by another person or team

Our response

We built an **audit framework** with the following philosophy:

- Lightweight & modular
- Python + Zabbix API + needed libs
- One rule = one simple check
- Easily extensible, version-controlled, shareable
- List rules (ready-to-use knowledge base)
- Schedulable or on-demand

Our response – *Architecture overview*



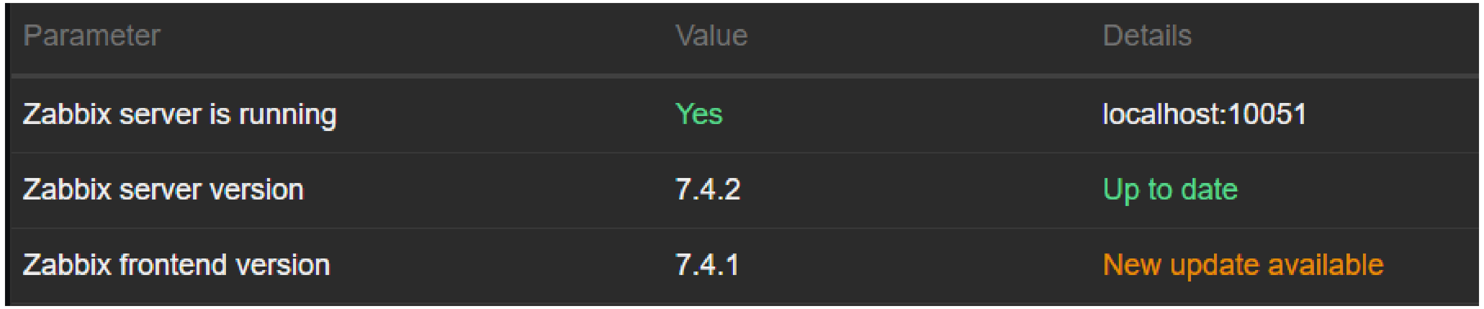
What do we check?

- 🛠️ System configuration
- 📋 Monitoring configuration
- 📈 Performance
- 🔐 Security

🛠 Outdated Zabbix version

- Problem spotted
  - Outdated zabbix version
- Risks
  - Lack of support
  - Miss new features
  - No security or debug patches

- Fix
  - Upgrade to newer version

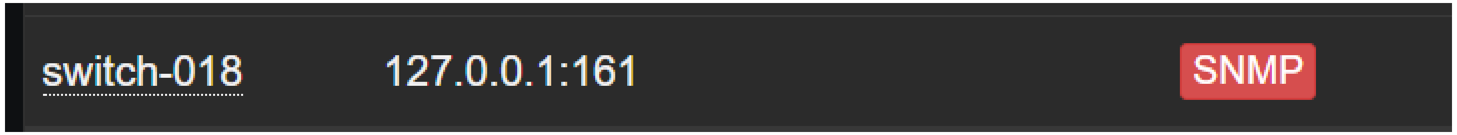


Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Zabbix server version	7.4.2	Up to date
Zabbix frontend version	7.4.1	New update available

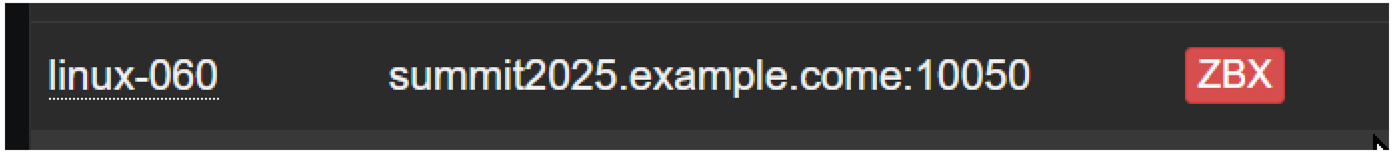
Long-unavailable hosts

- Problem spotted
  - Unavailable hosts don’t collect data.
- Risks
  - No data collected

- Fix
  - Correct errors making hosts unavailable



switch-018 127.0.0.1:161 SNMP

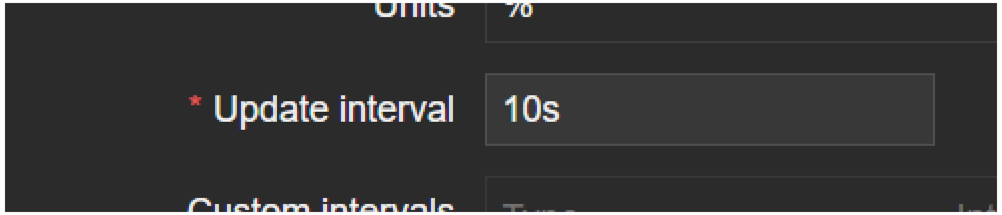


linux-060 summit2025.example.come:10050 ZBX

Overfrequent item updates

- Problem spotted
  - The item interval is too short
- Risks
  - Overloading the server

- Fix
  - Increase update interval



Units %

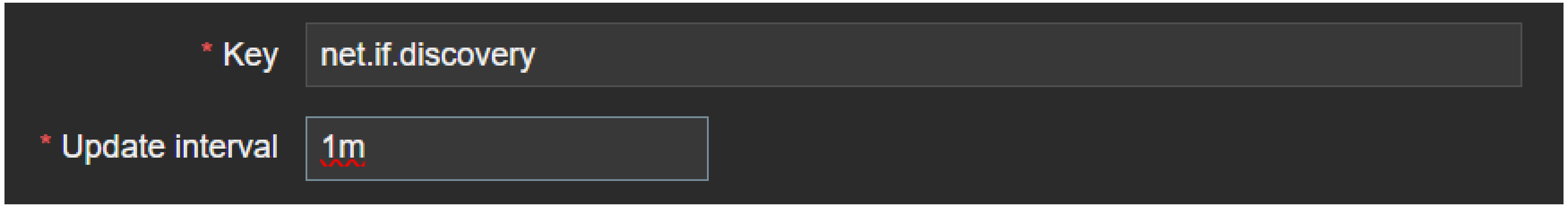
* Update interval 10s

Custom intervals Type

📋 High-frequency low level discovery

- Problem spotted
  - The LLD interval is too short
- Risks
  - Overloading the server

- Fix
  - Increase LLD interval

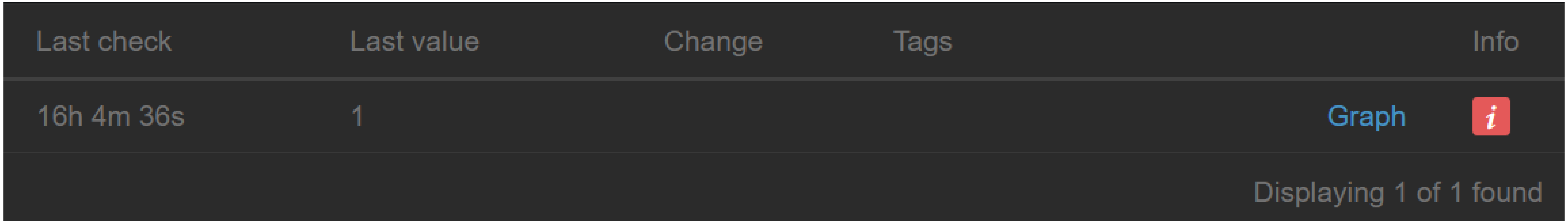


* Key	net.if.discovery
* Update interval	1m

Items unsupported for a long time

- Problem spotted
  - Unsupported item for a long time
- Risks
  - No data collected for this item
  - No trigger execution

- Fix
  - Correct item definition
  - “Check for not supported value" preprocessing if possible



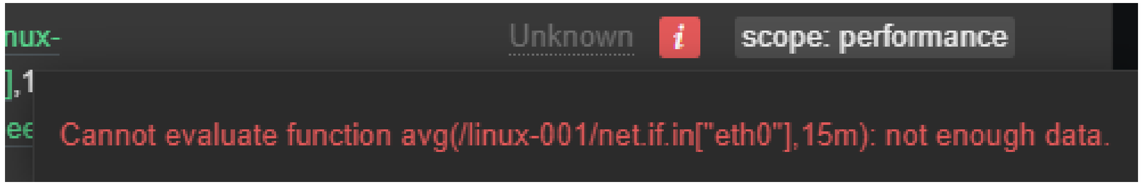
Last check	Last value	Change	Tags		Info
16h 4m 36s	1			Graph	i

Displaying 1 of 1 found

📋 Triggers stuck in UNKNOWN state

- Problem spotted
  - Trigger in UNKNOWN state
- Risks
  - The trigger is not evaluated, incidents won't be detected

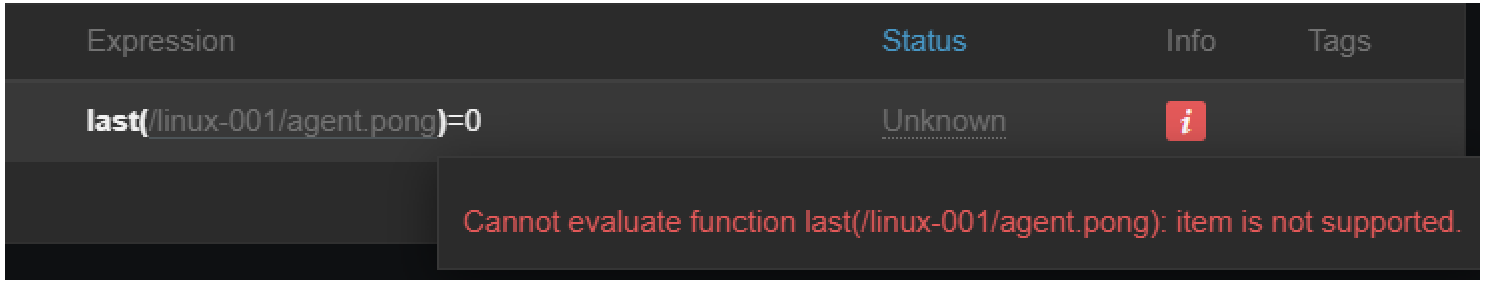
- Fix
  - Inspect and correct trigger
  - Can be temporary


nux- Unknown i scope: performance

],1

ee

Cannot evaluate function avg(/linux-001/net.if.in["eth0"],15m): not enough data.


Expression | Status | Info | Tags

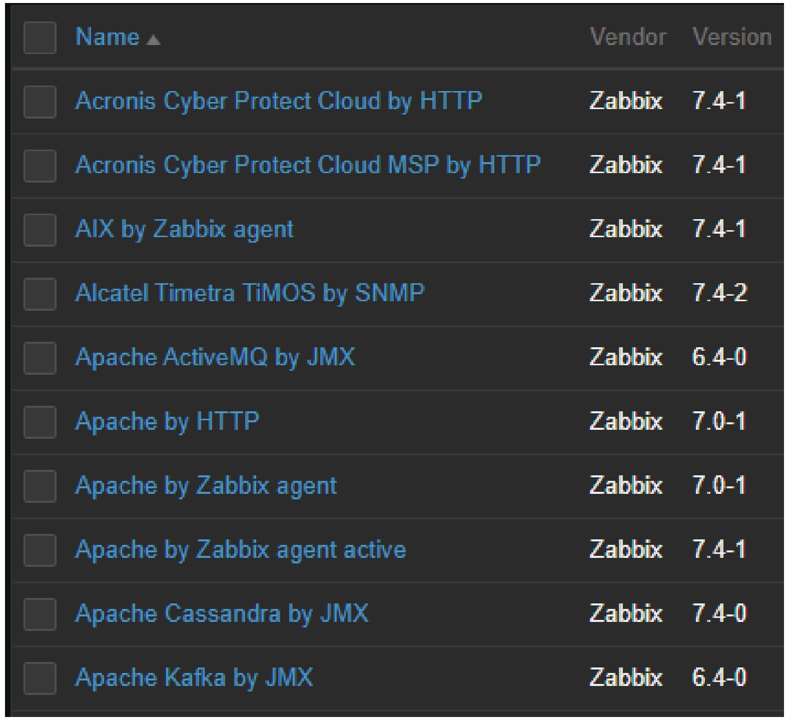
last(/linux-001/agent.pong)=0 | Unknown | i |

Cannot evaluate function last(/linux-001/agent.pong): item is not supported.

Outdated templates

- Problem spotted
  - Zabbix server has been updated but old template versions remains
- Risks
  - Old templates miss all fixes of the new template. New features are not present in the template (especially true for Health templates)

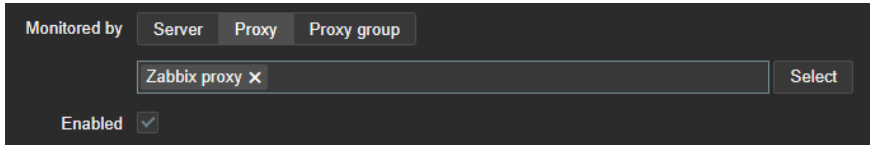
- Fix
  - Install newer templates (Zabbix GIT, Zabbix integrations page)



□	Name ▲	Vendor	Version
□	Acronis Cyber Protect Cloud by HTTP	Zabbix	7.4-1
□	Acronis Cyber Protect Cloud MSP by HTTP	Zabbix	7.4-1
□	AIX by Zabbix agent	Zabbix	7.4-1
□	Alcatel Timetra TiMOS by SNMP	Zabbix	7.4-2
□	Apache ActiveMQ by JMX	Zabbix	6.4-0
□	Apache by HTTP	Zabbix	7.0-1
□	Apache by Zabbix agent	Zabbix	7.0-1
□	Apache by Zabbix agent active	Zabbix	7.4-1
□	Apache Cassandra by JMX	Zabbix	7.4-0
□	Apache Kafka by JMX	Zabbix	6.4-0

Excess direct monitoring (no proxy)

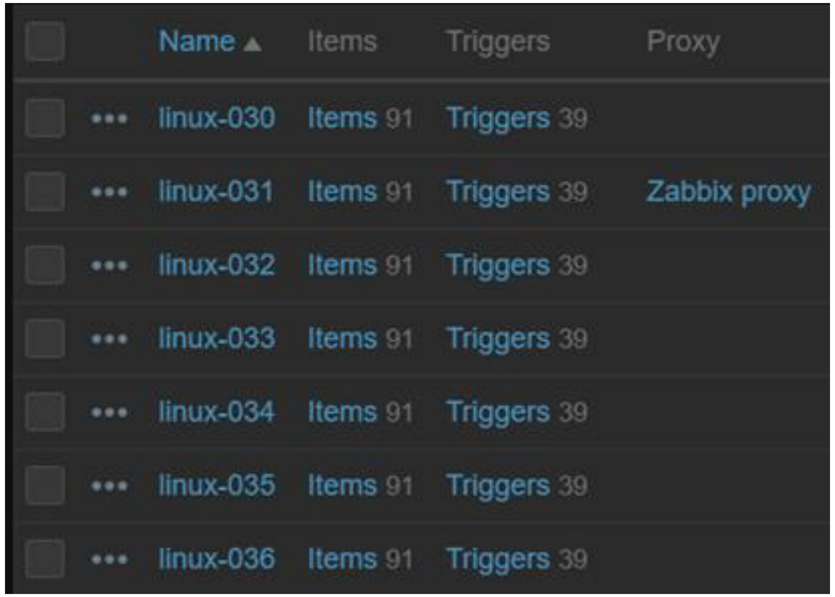
- Problem spotted
  - A lot of hosts are monitored directly by the server and not on a proxy
- Risks
  - Overload the server
- Fix
  - All hosts should go through a proxy



Monitored by: Server | Proxy | Proxy group

Zabbix proxy ✕ Select

Enabled ☑

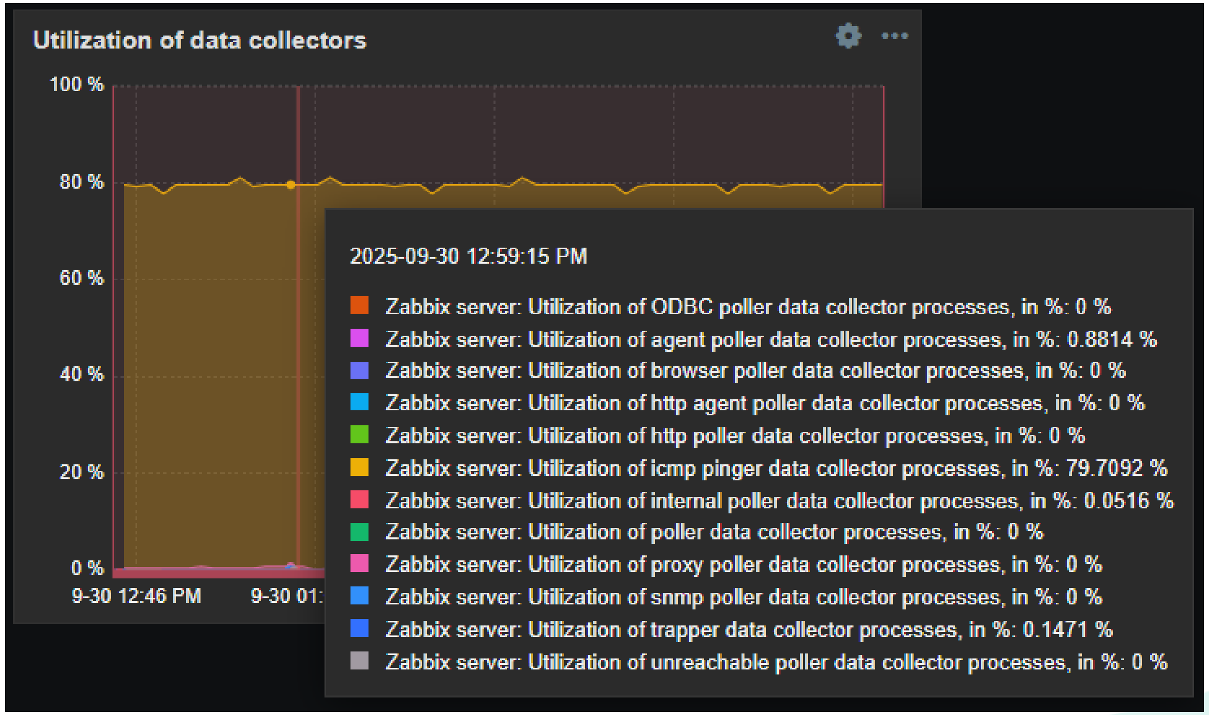


□		Name ▲	Items	Triggers	Proxy
□	•••	linux-030	Items 91	Triggers 39	
□	•••	linux-031	Items 91	Triggers 39	Zabbix proxy
□	•••	linux-032	Items 91	Triggers 39	
□	•••	linux-033	Items 91	Triggers 39	
□	•••	linux-034	Items 91	Triggers 39	
□	•••	linux-035	Items 91	Triggers 39	
□	•••	linux-036	Items 91	Triggers 39	

Inefficient poller allocation

- Problem spotted
  - Pollers are over/under utilized
- Risks
  - Under utilization: waste server resources
  - Over utilization: delay checks

- Fix
  - Adapt poller in server configuration (`StartXxx=`)



Utilization of data collectors

2025-09-30 12:59:15 PM

- 🟧 Zabbix server: Utilization of ODBC poller data collector processes, in %: 0 %
- 🟪 Zabbix server: Utilization of agent poller data collector processes, in %: 0.8814 %
- 🟦 Zabbix server: Utilization of browser poller data collector processes, in %: 0 %
- 🟦 Zabbix server: Utilization of http agent poller data collector processes, in %: 0 %
- 🟩 Zabbix server: Utilization of http poller data collector processes, in %: 0 %
- 🟨 Zabbix server: Utilization of icmp pinger data collector processes, in %: 79.7092 %
- 🟥 Zabbix server: Utilization of internal poller data collector processes, in %: 0.0516 %
- 🟩 Zabbix server: Utilization of poller data collector processes, in %: 0 %
- 🟪 Zabbix server: Utilization of proxy poller data collector processes, in %: 0 %
- 🟦 Zabbix server: Utilization of snmp poller data collector processes, in %: 0 %
- 🟦 Zabbix server: Utilization of trapper data collector processes, in %: 0.1471 %
- ⬜ Zabbix server: Utilization of unreachable poller data collector processes, in %: 0 %

Inefficient cache allocation

- Problem spotted
  - Caches are over/under utilized
- Risks
  - Under utilization: waste server resources
  - Over utilization: could lead to server crash if reaching 100%

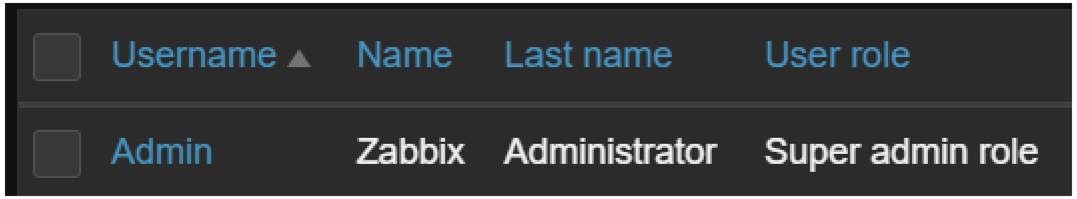
- Fix
  - Adapt cache sizes in server configuration (`XxxxCacheSize=`)

/var/log/zabbix/zabbix_server.log

```
[file:dbconfig.c,line:247] __zbx_shmem_malloc(): out of memory (requested 64 bytes)
[file:dbconfig.c,line:247] __zbx_shmem_malloc(): please increase CacheSize configuration parameter
482977:20250930:095604.611 One child process died (PID:482980,exitcode/signal:1). Exiting ...
```

🔐 Unchanged admin credentials

- Problem spotted
  - Default admin user is present with default password
- Risks
  - The default ‘Admin/zabbix’ is widely known.
  - Anyone can log in with super-admin rights.
- Fix
  - Change Admin Username
  - Change password

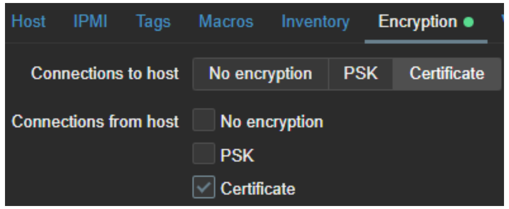


□	Username ▲	Name	Last name	User role
□	Admin	Zabbix	Administrator	Super admin role

Unencrypted hosts

- Problem spotted
  - No encryption between server/proxy/agent
- Risks
  - Plain text traffic between server/proxy and agent

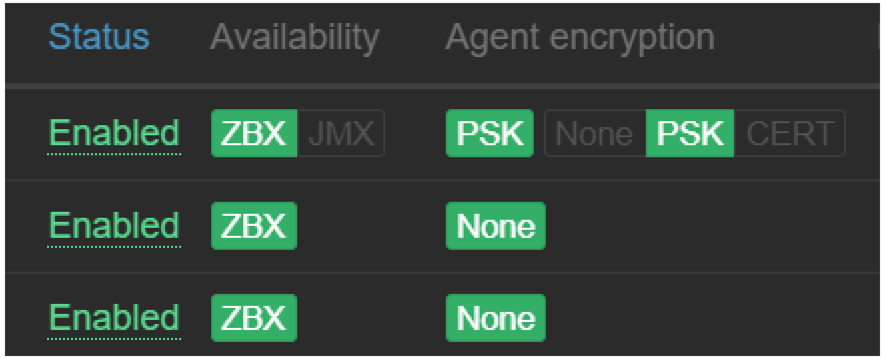
- Fix
  - Activate encryption on agents (either PSK or CERT based)



Host | IPMI | Tags | Macros | Inventory | Encryption ●

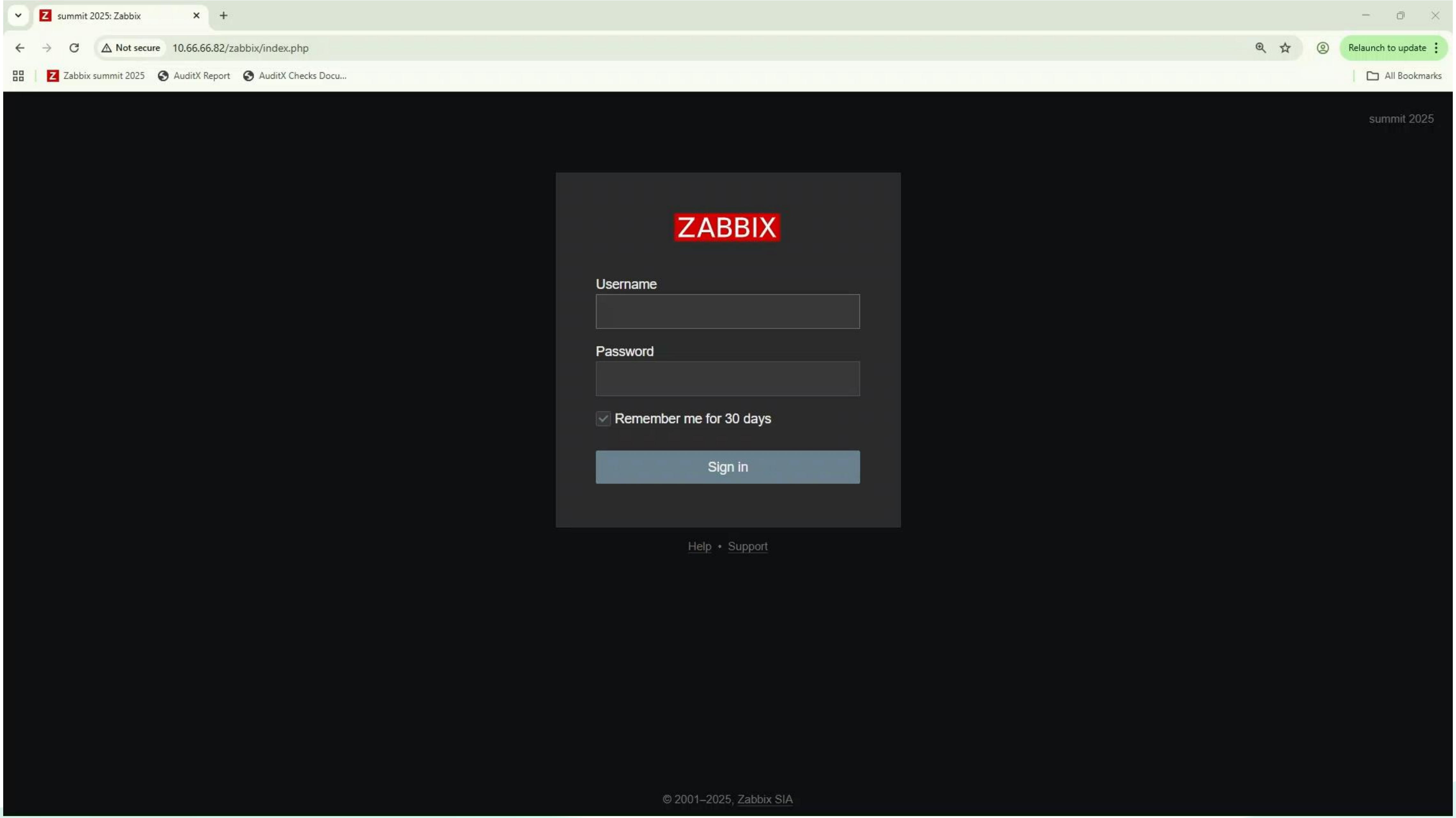
Connections to host: No encryption | PSK | [✓ Certificate]

Connections from host:
- □ No encryption
- □ PSK
- ☑ Certificate



Status	Availability	Agent encryption
Enabled	ZBX JMX	PSK None PSK CERT
Enabled	ZBX	None
Enabled	ZBX	None

DEMO



summit 2025: Zabbix
Not secure
10.66.66.82/zabbix/index.php
Relaunch to update
Zabbix summit 2025
AuditX Report
AuditX Checks Docu...
All Bookmarks
summit 2025
ZABBIX
Username
Password
☑ Remember me for 30 days
Sign in
Help • Support
© 2001–2025, Zabbix SIA

What's next?

- Want to add new check?
  - Create new check, using available facts from provider
  - if needed, adapt existing provider to gather new facts
  - Test the new check
- Want to add another tech
  - Create provider targeting this new tech
  - Create checks based on facts gathered by the provider
  - Test the new tech
- The next steps
  - Start small, build gradually
  - Adapt the framework to your infrastructure
  - Share rules and improve them collaboratively

Conclusion

- Zabbix is critical — it deserves to be monitored too
- Tool allows users to visualize potential problems at a glance in a single launch
- Self documentation
- “Zabbix takes care of our IT — now it’s time to take care of Zabbix”

Github Repository

https://github.com/SomoneIT/auditx

THANK YOU !