

# Morning Talks - Zabbix

## Open Source Monitoring

**Lukáš Malý, DiS**

*IT konzultant bezpečnost a monitoring*

email: [maly@datasys.cz](mailto:maly@datasys.cz)

- Drobný úvod do Zabbixu
- Vzdalený monitoring pomocí Zabbix proxy
- Automatizace monitoringu pomocí Low Level Discovery (LLD)
- Šifrování komunikace mezi všemi komponentami Zabbixu
- Zabbix API jako možnost integrace s jinými systémy
- Vizualizace - vizualizace architektury a real-time status
- Zabbix 4.0 nový dashboard s novými SVG grafy
- Značkování událostí, tagy napříč celým systémem
- JConsole - inteligentní Java monitoring pomocí JMX
- Orchestrator - VMWare monitoring
- Web tester - 24x7 testování uživatelských scénářů HTTP agent

- Nový směr v ukládání dat
- Podpora PostgreSQL s rozšířením TimescaleDB
- Nový LTS Zabbix 5.0

**ZABBIX**

+



**TIMESCALE**

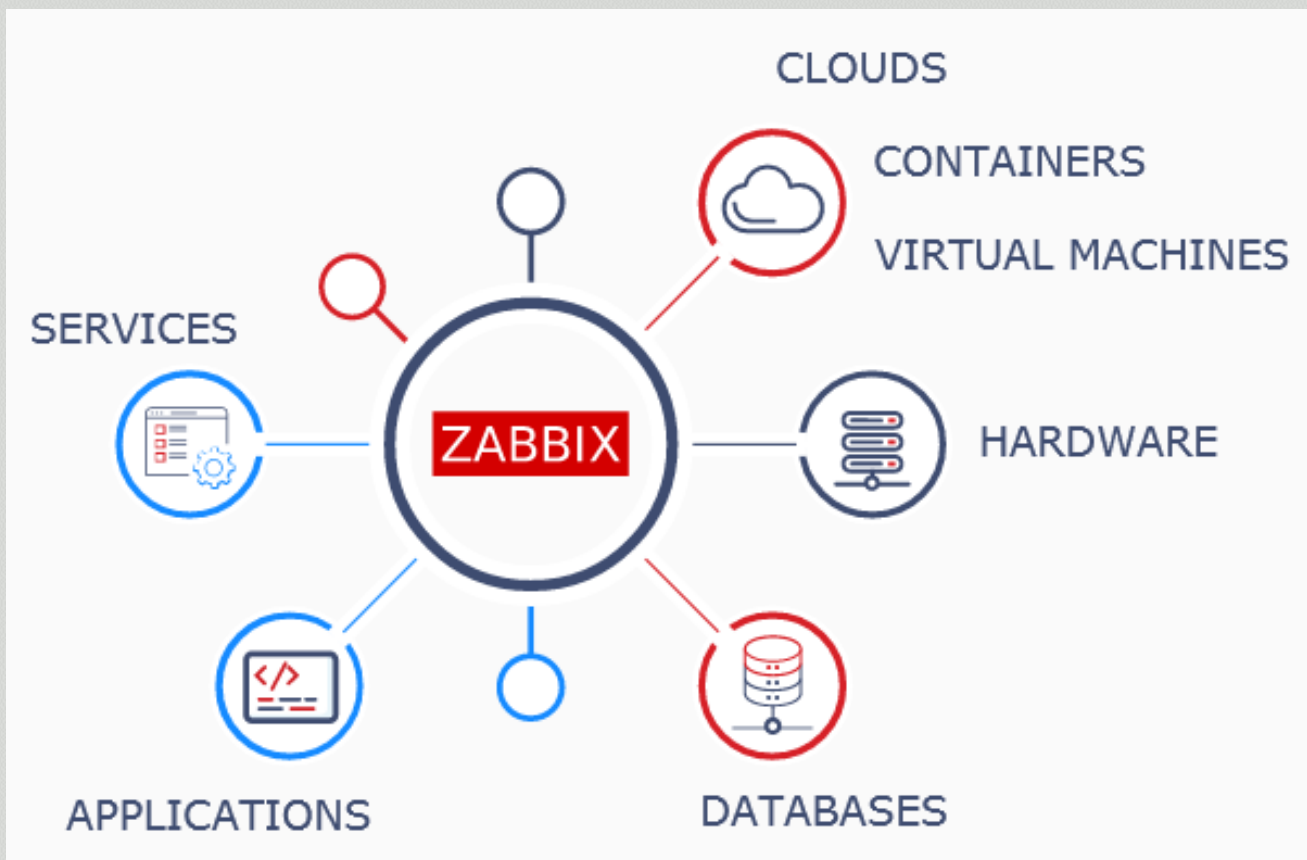
=



- **Zabbix je firemní monitorovací software**
  - Opravdu volný, bez omezení
  - Opravdu “enterprise”
    - Rozšiřitelný až
      - 100.000 monitorovaných zařízení
      - 1.000.000 monitorovaných veličin
      - Tisíce kontrol za sekundu
    - Distribuovaný monitoring
    - Popora mnoha platforem



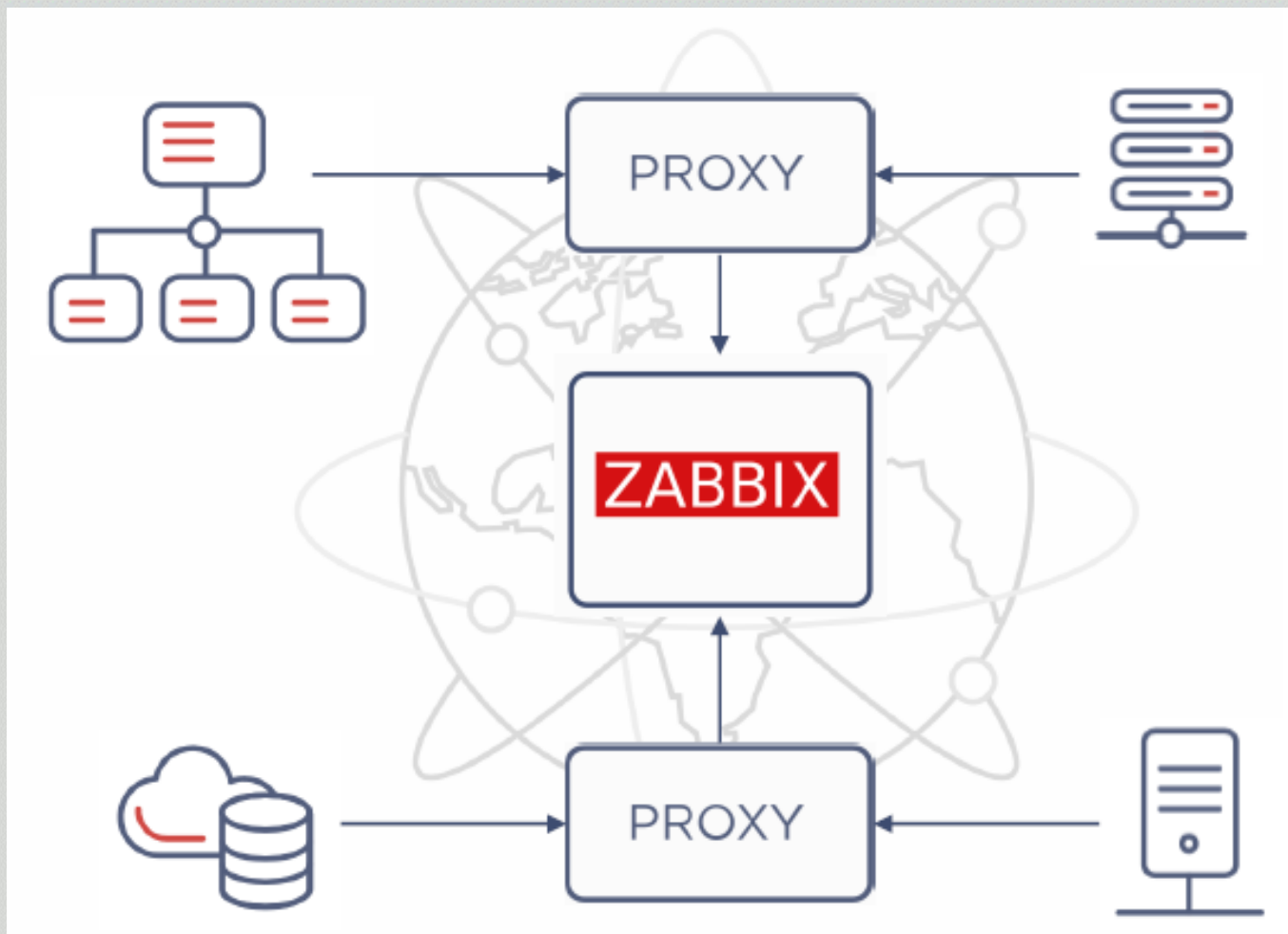
- **Základní architektura**



- **Idea: potřeba lepšího monitorovacího nástroje**

- Kdy?

- |              |               |
|--------------|---------------|
| • Zabbix 1.0 | Březen 2004   |
| • Zabbix 1.8 | Prosinec 2009 |
| • Zabbix 2.0 | Květen 2012   |
| • Zabbix 2.2 | Listopad 2013 |
| • Zabbix 2.4 | Červenec 2014 |
| • Zabbix 3.0 | Leden 2016    |
| • Zabbix 3.2 | Září 2016     |
| • Zabbix 3.4 | Srpen 2017    |
| • Zabbix 4.0 | Říjen 2018    |
| • Zabbix 4.2 | Duben 2019    |
| • Zabbix 4.4 | Říjen 2019    |

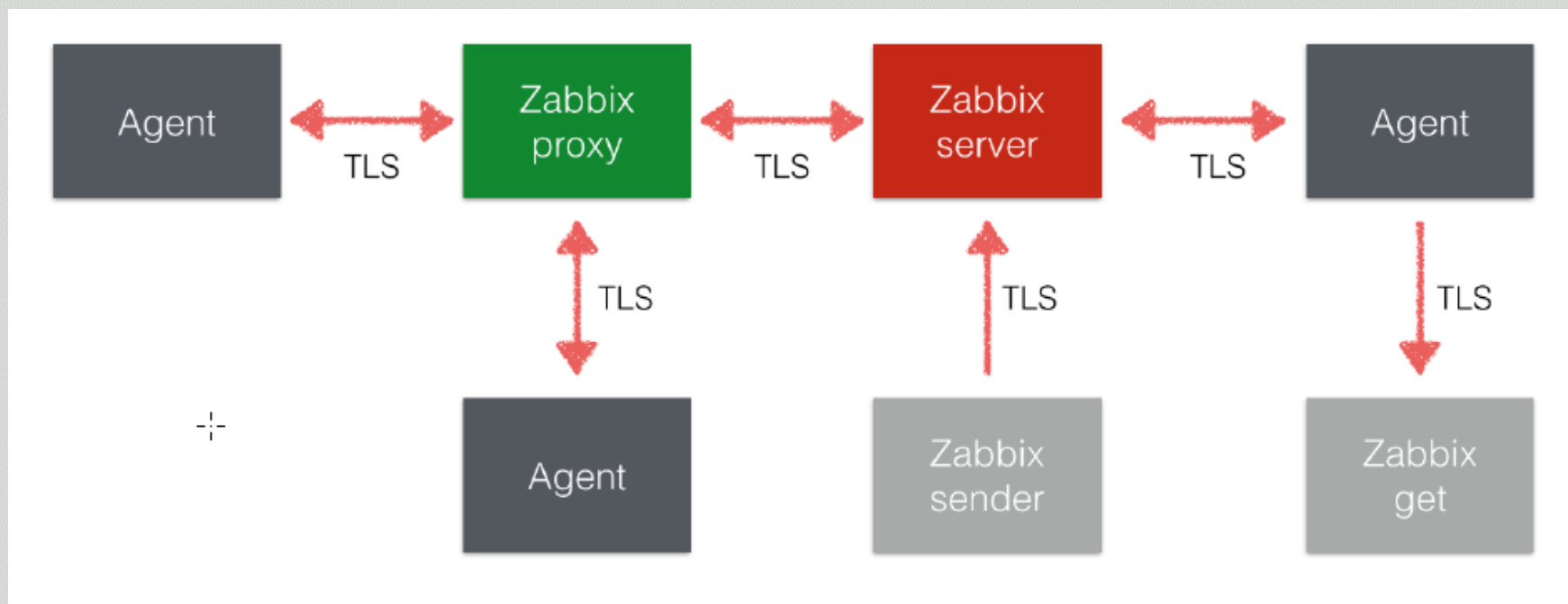


- **LLD je způsob automatického vytváření itemů, triggerů, a grafů pro prvky objevené na zařízení**
  - Vytváření objektů je řízeno prototypy
  - Filtry na objevované prvky
  - Zabbix podporuje 8 typů LLD objevování
  - Dále je možné psát vlastní scripty



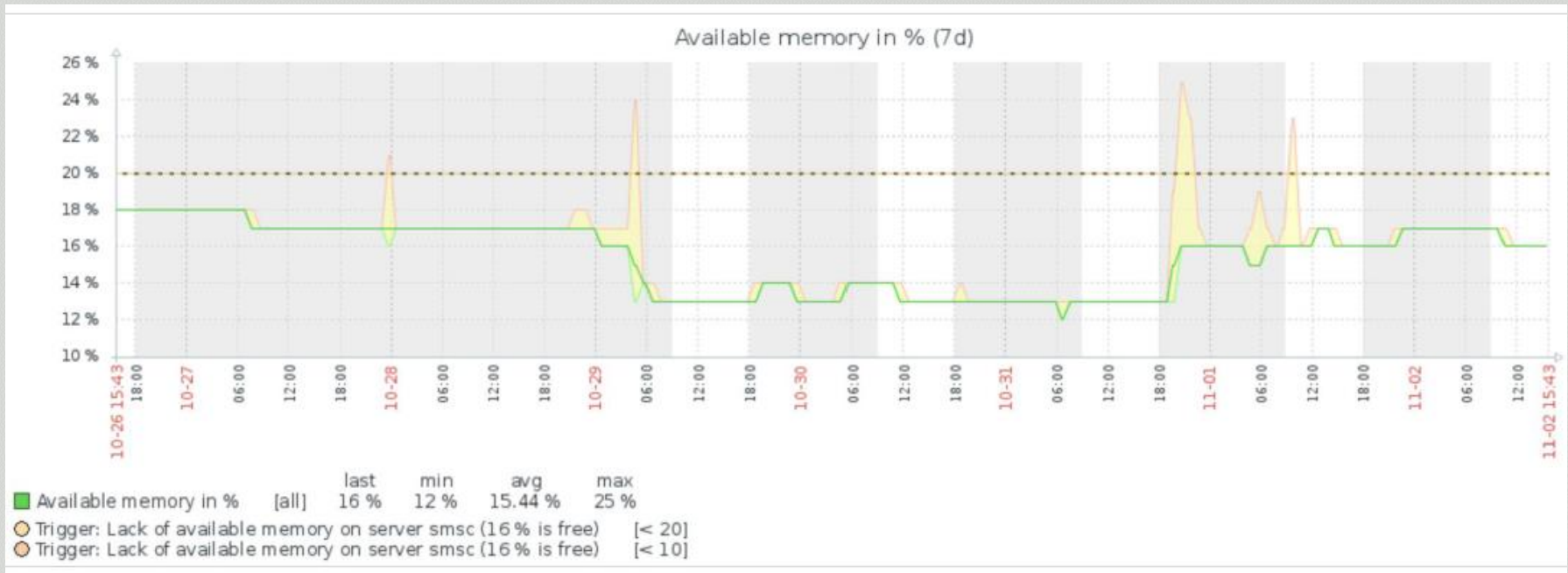
- **LLD je způsob automatického vytváření itemů, triggerů, a grafů pro prvky objevené na zařízení**
  - Objevování file systémů
  - Objevování síťových rozhraní
  - Objevování CPU a CPU core
  - Objevování SNMP OID
  - Objevování JMX objects
  - Objevování ODBC SQL dotazů
  - Objevování Windows services
  - Objevování host interfaces v Zabbix

- Použití Certifikátů
- Použití Pre-shared keys



- Zabbix disponuje možností API
  - Zabbix API umožňuje programově načíst a měnit konfiguraci
  - Poskytuje přístup k historickým datům
  - Umožňuje integraci Zabbix se softwarem třetích stran (např. mobilní aplikace)
  - Automatizujte rutinní úlohy
- Zabbix API je realizováno pomocí Zabbix Frontend
  - Používá protokol JSON-RPC 2.0
  - API se skládá ze souboru samostatných metod
  - Požadavky a odpovědi mezi klientem a rozhraním API jsou zakódovány ve formátu JSON
  - Plány na přepracování do Zabbix server

- Jednoduchý Graf – Latest Data
- Graf
- Screen, Mapa, Dashboard



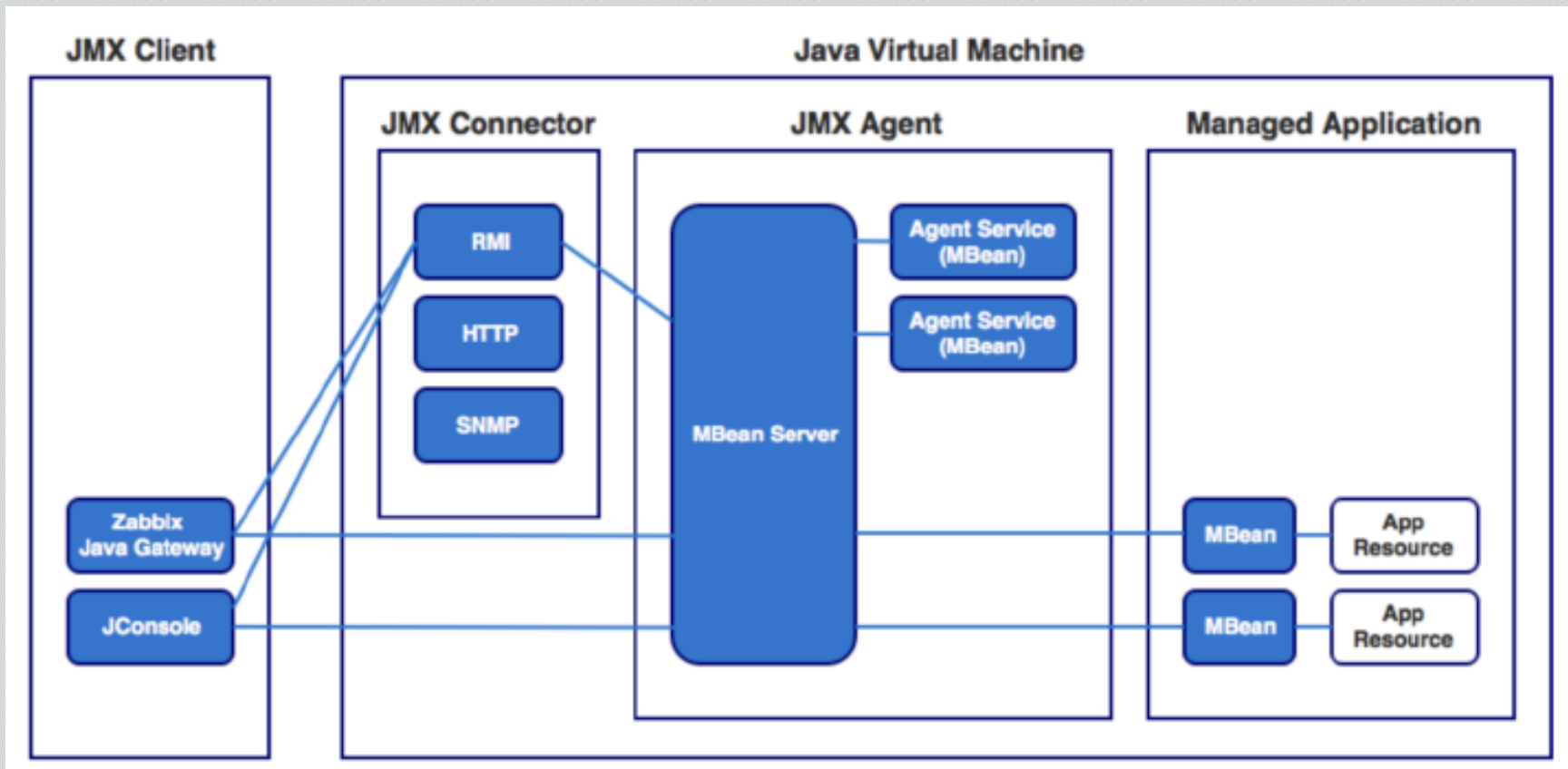
# Zabbix 4.0 LTS a 4.4

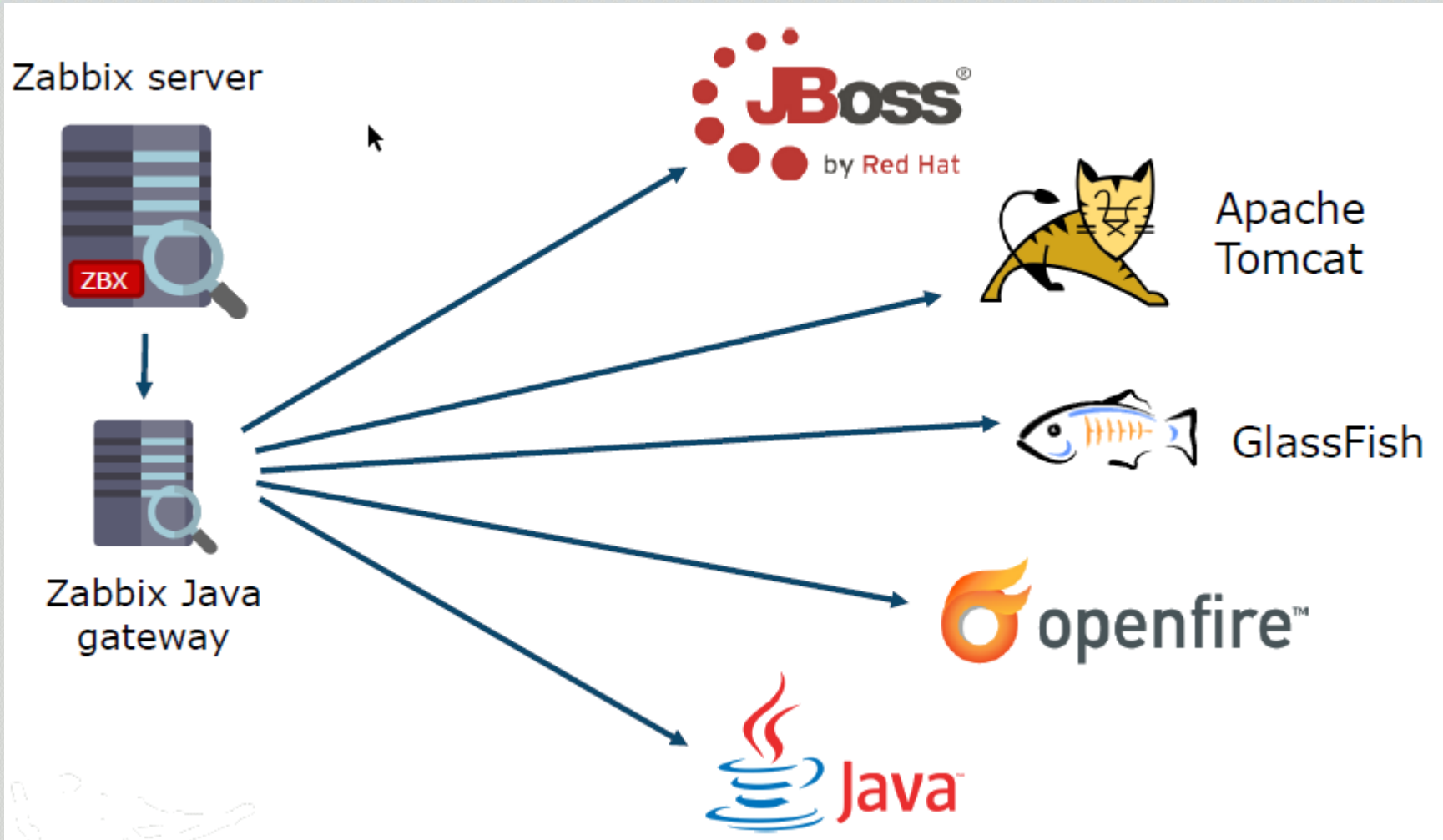
---

- Co je nového v poslední LTS verzi
  - Podívejme se na nový Zabbix 4.0 LTS
  - <https://www.root.cz/clanky/novy-zabbix-4-0-lts-mnoho-uprav-vzhledu-i-funkcnosti/>
- Co je nového v poslední vývojové verzi
  - Podívejme se na nový vývojový Zabbix 4.4
  - <https://www.root.cz/clanky/zabbix-4-4-prichazi-s-druhou-generaci-agenta-v-jazyce-go/>

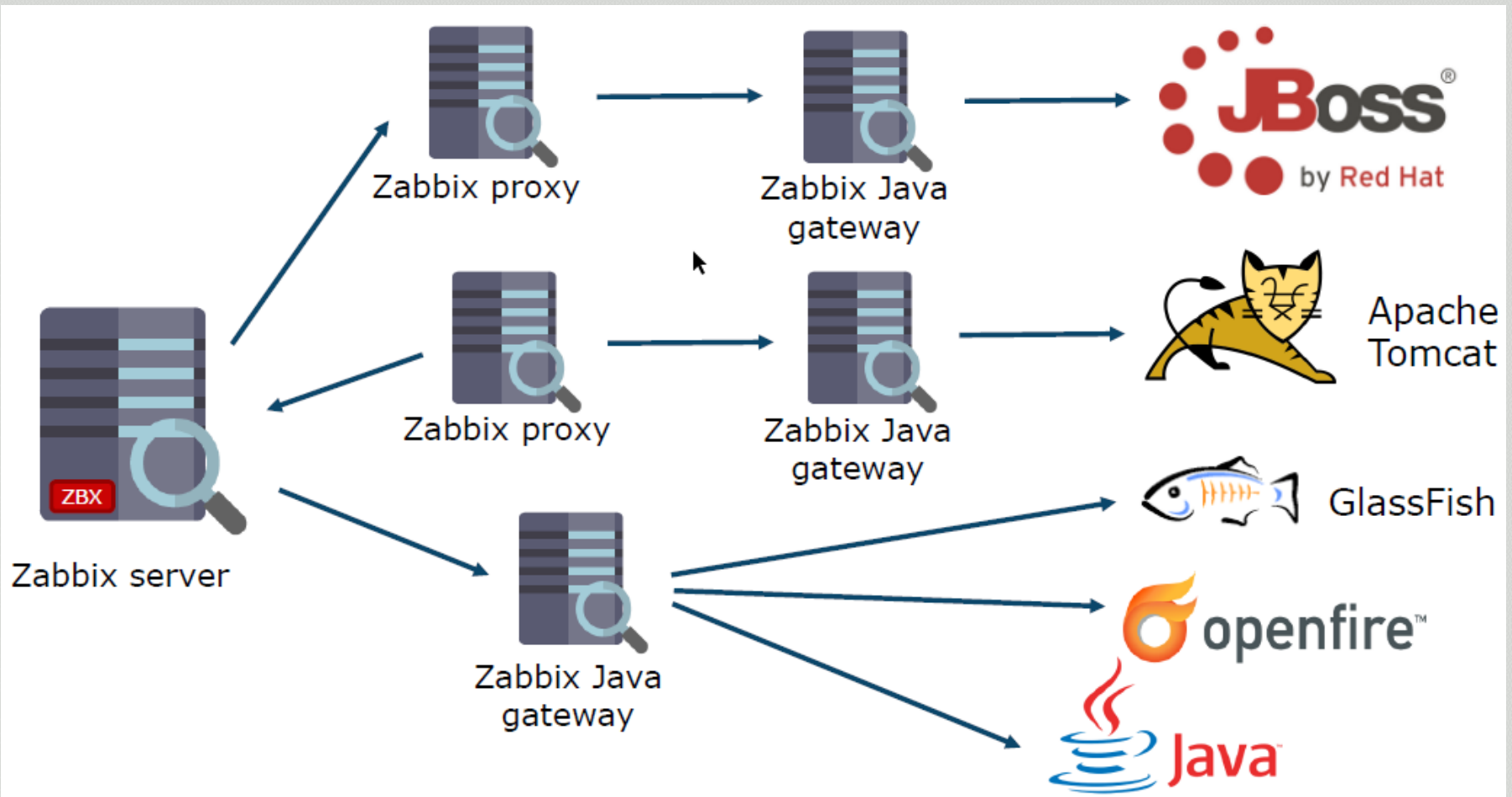
- Značkování je nový mechanismus v Zabbix 4.0
- V Zabbix 4.4 je podpora tagu na úrovni hosta
  - Tag neboli značka se nastavuje v Triggeru
  - Jedná se o doplňující informaci k události
  - Hodnota může být statická ale je možné použít i makra
- Tag : Value, Service : MySQL, Location : Prague atd.
- Tagy je možné následně využít při vyhledávání a filtrování
- Tagy je možné použít u oprávnění - Host Group atd.

[https://www.zabbix.com/documentation/4.0/manual/config/event\\_correlation/trigger/event\\_tags](https://www.zabbix.com/documentation/4.0/manual/config/event_correlation/trigger/event_tags)

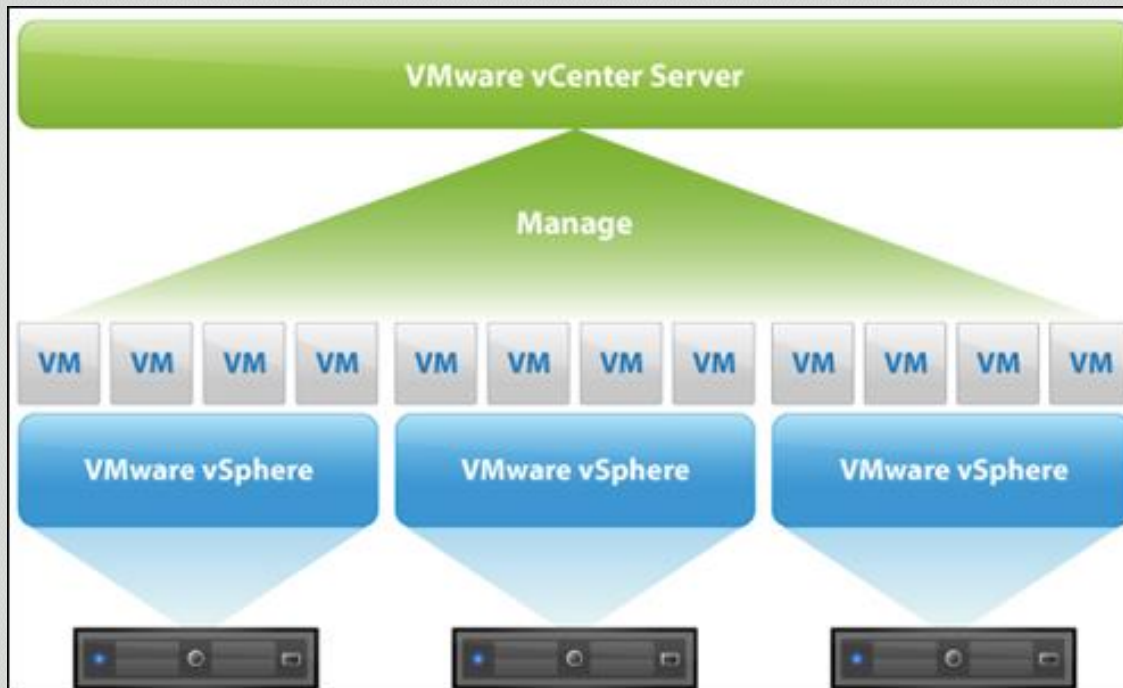








- Zabbix 4.0 LTS podporuje monitoring VMware
  - Využívá nativní VMware API
  - V minulosti se hojně používalo Perl SDK API pro scripty



## – Mnoho podporovaných items (typu “Simple check”)

[https://www.zabbix.com/documentation/4.0/manual/config/items/itemtypes/simple\\_checks/vmware\\_keys](https://www.zabbix.com/documentation/4.0/manual/config/items/itemtypes/simple_checks/vmware_keys)

| Description   | Key   |  |
|---|---|--|
|   | Return value  | Parameters   |
| <b>vmware.cluster.discovery[&lt;url&gt;]</b>                    |   |  |
| Discovery of VMware clusters.                                   | JSON object   | <b>url</b> - VMware service <a href="#">URL</a>  |
| <b>vmware.cluster.status[&lt;url&gt;, &lt;name&gt;]</b>         |   |  |
| VMware cluster status.  | Integer:<br>0 - gray;<br>1 - green;<br>2 - yellow;<br>3 - red | <b>url</b> - VMware service <a href="#">URL</a><br><b>name</b> - VMware cluster name         |
| <b>vmware.eventlog[&lt;url&gt;]</b>                             |   |  |
| VMware event log.   | Log   | <b>url</b> - VMware service <a href="#">URL</a>  |
| <b>vmware.fullname[&lt;url&gt;]</b>                             |   |  |
| VMware service full name.                                       | String  | <b>url</b> - VMware service <a href="#">URL</a>  |
| <b>vmware.hv.cluster.name[&lt;url&gt;, &lt;uuid&gt;]</b>        |   |  |
| VMware hypervisor cluster name.                                 | String  | <b>url</b> - VMware service <a href="#">URL</a><br><b>uuid</b> - VMware hypervisor host name |
| <b>vmware.hv.cpu.usage[&lt;url&gt;, &lt;uuid&gt;]</b>           |   |  |
| VMware hypervisor processor usage (Hz).                         | Integer   | <b>url</b> - VMware service <a href="#">URL</a><br><b>uuid</b> - VMware hypervisor host name |
| <b>vmware.hv.datastore.discovery[&lt;url&gt;, &lt;uuid&gt;]</b> |   |  |
| Discovery of VMware hypervisor datastores.                      | JSON object   | <b>url</b> - VMware service <a href="#">URL</a><br><b>uuid</b> - VMware hypervisor host name |

|   |
|---|
| <b>CPU (5 Items)</b>                              |
| CPU cores   |
| CPU frequency                                     |
| CPU model   |
| CPU threads                                       |
| CPU usage   |
| <b>Datastore (2 Items)</b>                        |
| Average read latency of the datastore datastore1  |
| Average write latency of the datastore datastore1 |
| <b>General (6 Items)</b>                          |
| <b>Hardware (8 Items)</b>                         |
| <b>Memory (3 Items)</b>                           |
| Ballooned memory                                  |
| Total memory                                      |
| Used memory                                       |
| <b>Network (2 Items)</b>                          |
| Number of bytes received                          |
| Number of bytes transmitted                       |

# Kontroly dostupnosti Web



- Co je TimescaleDB (TSDB)?
- Je to komerční extenze relační databáze PostgreSQL vydané jako Open Source - <https://www.timescale.com/>
  - Od verze Zabbix 4.4 je pro TSDB oficiální podpora
- <https://www.zabbix.com/documentation/current/manual/appendix/install/timescaledb>
- Jedná se částečně o obdobu - PostgreSQL Partitions
- <https://blog.zabbix.com/zabbix-time-series-data-and-timescaledb/6642/>
- Podrobnosti o fungování TSDB
- <https://blog.timescale.com/blog/time-series-data-postgresql-10-vs-timescaledb-816ee808bac5/>

- Sledujte Roadmap
- <https://www.zabbix.com/roadmap>
- Vydání je oznámeno na Březen 2020
- Co je nového
- <https://www.zabbix.com/documentation/5.0/manual/introduction/whatsnew500>



Dotazy?