

# Moderní monitoring IT infrastruktury

*Michal Švamberg*

Západočeská univerzita v Plzni  
Centrum informatizace a výpočetní techniky  
email: [svamberg@civ.zcu.cz](mailto:svamberg@civ.zcu.cz)

20. dubna 2018

## Abstrakt

Monitoring systémů je důležitý prvek při správě informačních technologií. Předkládaný projekt se zabývá možnostmi monitoringu, testováním a nasazením nového monitorovacího systému, který by zjednodušil a zpřehlednil jeho správu. Cílem je nasadit nové řešení s maximální možnou automatizací, které by respektovalo dnešní trendy v této oblasti.

## 1 Současný stav řešeného problému

Jako základ monitoringu používáme systém Nagios<sup>1</sup> ve verzi 3.5.1. K lednu 2018 monitorujeme přes 600 hostů a okolo 6500 služeb (testů). Skladba testů je různorodá, od standardních testů konektivity protokolem ICMP až po vlastní testy pro AFS servery.

Problém Nagiosu spatřujeme v několika rovinách. Je to relativně těžkopádný systém, který neumí dynamickou konfiguraci, například na základě vlastností hosta. Jen velmi špatně lze upravit uživatelské rozhraní bez nutnosti zásahu do zdrojových kódů. Nemá jednotné rozhraní pro přidávání dalších rozšíření.

Pro vzdálená volání testů používáme NRPE<sup>2</sup>. Bohužel v Debianu byla vypnuta možnost posílat argumenty jako reakce na bezpečnostní problém, proto je třeba udržovat vlastní balík. Druhý problém vidíme v přechodu na NRPEv3, kde jsme zjistili, že nelze uspokojivě přejít na novou verzi při zachování současného rozsahu používání. Řešením je přejít na jiný způsob vzdáleného spouštění testů.

Konfigurace NRPE je zcela oddělená od systému Nagios a je třeba ji samostatně udržovat. V tomto nám velmi pomáhá centrální systém pro správu operačního systému<sup>3</sup>. I tak je

---

<sup>1</sup><https://www.nagios.org/>

<sup>2</sup><https://github.com/NagiosEnterprises/nrpe>

<sup>3</sup>Používáme CFEngine3, viz <https://cfengine.com/>

při úpravě sondy (například rozšíření o další parametr) nutné změnit konfiguraci na všech dotčených hostech a službu restartovat. To si představujeme, že by měl monitoring řešit vlastními nástroji.

Protože do konfigurace monitoringu zasahuje více lidí, využíváme webové rozhraní NConf<sup>4</sup> pro konfiguraci Nagiosu. Správci systémů se tak nemusí učit syntaxi konfigurace, přitom mají možnost snadné úpravy jednotlivých testů. Dříve se správa Nagiosu prováděla ruční editací konfiguračních souborů, po zavedení webového rozhraní prudce narostl počet testů. To se odrazilo také na výkonu NConfu jehož webové rozhraní se stalo pomalým pro uživatele. Systém NConf navíc přestal být vyvíjen v roce 2013, což dále zhoršuje udržitelnost tohoto řešení.

Aktuálně používané nastavení téměř neumožňuje automatizaci, což je škoda, protože mnoho informací by šlo nastavit z centrální správy operačních systémů nebo jiných zdrojů dat (DNS, LDAP, ...). Chybí také jakékoliv API nebo jiný model pro zvýšení automatizace zakládání nových strojů nebo služeb či uživatelských účtů. Všechny změny je tedy nutné provádět ručně.

Systém NConf nerozlišuje žádná oprávnění. Buď uživatel má právo přístupu a pak může dělat cokoli nebo jej nemá. Uvítali bychom trochu větší granularitu pro správu, alespoň přidání možnosti pouhého čtení.

Výstup z Nagiosu byl použit v dřívějším projektu pro HelpDesk. V něm se kumulované testy pluginem `check_multi`<sup>5</sup> promítaly uživatelům ve srozumitelnější formě. Výslednou vizualizaci zajišťuje program NagVis<sup>6</sup>. Správa NagVisu a kumulovaných testů není úplně snadná. Navíc výsledky mají zpoždění dané tím, že se kumulace provádí jako další test volaný z Nagiosu.

Data získaná z jednotlivých testů se ukládají do RRD formátu a zobrazují se nástrojem Nagiosgraph<sup>7</sup>. To umožňuje sledovat vývoj infrastruktury v minulosti a odhadovat tak další vývoj. Vzhledem k akregaci ukládaných dat za účelem ušetření diskového prostoru nelze data využít jiným způsobem. Je možné pouze prohlížet. O rychlém generování grafů se zde také nedá hovořit.

Je zde vidět, že současný stav monitoringu prošel dlouhým vývojem, kdy se na něj postupně nabalovaly další potřebné součásti. Každá tato část se ovšem spravuje jinak, jejich provázání není nejlepší, což ve výsledku působí potíže a brzdí další rozvoj a využití. Cítíme, že potenciál monitorovacích služeb je daleko větší, než současný stav a to včetně rychlejšího a lepšího informování zodpovědných lidí.

## 2 Cíle řešení

Projekt má za cíl připravit nový monitoring s co možná největší automatizací, přehledným a jednotným rozhraním. Důležité je zachovat všechny používané funkce monitoringu.

---

<sup>4</sup><http://www.nconf.org>

<sup>5</sup>[http://my-plugin.de/wiki/projects/check\\_multi/start](http://my-plugin.de/wiki/projects/check_multi/start)

<sup>6</sup><http://www.nagvis.org/>

<sup>7</sup><http://nagiosgraph.sourceforge.net/>

Na základě požadavků vybereme vhodné řešení pro změnu monitoringu. Budeme vybírat ze zavedených projektů, které mají potenciál dlouho vydržet a jsou dostatečně otevřené.

Při výběru budeme klást důraz na dobrou integraci jednotlivých částí monitoringu jako jsou grafy, webový management, napojení vzdálených testů či kompatibilita se různými operačními systémy.

Nový monitorovací nástroj by měl nejen přinést přehlednější a rychlejší rozhraní, ale hlavně odstranit systémové neduhy současného řešení za které považujeme zejména:

- lepší reakce na uživatelské požadavky (recheck testu),
- dynamické testy na základě vlastností hosta,
- vyšší granularita oprávnění při správě monitoringu i jeho managementu,
- automatizace správy hostů, služeb, uživatelů, ...
- lepší využití sbíraných dat ze sond, možnosti filtrování, zpracování, ...
- rychlejší synchronizace konfigurace vzdálených testů se snadnou možností změn parametrů,
- uživatelský přívětivější a rychlejší zobrazování grafů,
- uchování dat pro grafy s nepovinnou agregací a po delší dobu než jeden rok,
- lepší odezva u kumulovaných testů pokud nastane změna,
- bezpečné a snadno konfigurovatelné vzdálené spouštění testů,
- přístup k datům i na mobilních zařízeních.

Projekt bude završen nasazením nového monitoringu do provozu. Tím ale vlastní práce nekončí, protože bude nutné reagovat a ladit výsledky dle potřeb.

Dalším cílem je zlepšit přehled správců o aktuálním stavu výpočetní infrastruktury. Nyní správce může získat informaci o nefunkční službě z emailu, webu nebo telefonicky od uživatelů. Toho si ale často nemusí administrátor hned všimnout nebo uživatel nepovažuje problém za závažný. Cílem je tedy zvýšit počet kanálů, jak dostat informaci o závadě ke správci.

Předpokládáme, že nové moderní rozhraní, lepší přehlednost zobrazovaných dat i větší konfigurovatelnost významnělepší sledování IT prostředí. Velké zjednodušení si slibujeme od automatizace.

Dále bychom chtěli zlepšit informování administrátorů, dnes sice administrátorům přijde email nebo SMS s varováním, ale ne vždy mohou dopad problému odhadnout. Navíc se často stává, že varování je nasměrováno jen na malý okruh lidí, kteří si hned nevšimnou problému ani jeho rozsahu. Proto bychom chtěli zavést přehledové obrazovky také pro administrátory, které by byly umístěny ve společných prostorách. Tím by nenásilnou formou

byli informováni všichni o aktuálním stavu služeb. Inspiraci pro toto rozšíření jsme získali na stáži ve firmě Puppet<sup>8</sup>.

Výsledkem projektu by nemělo být jen ucelený nový monitoring, ale také přínos pro další informační prostředí v podobě náhledu jak postavit monitoring s novými technologiemi. Případně jako inspirace pro další rozvoj jejich vlastního monitorovacího systému.

### 3 Způsob řešení

Pro projekt předpokládáme nákup jednoho serveru, na kterém bude připraven nový monitoring. Ačkoliv očekáváme, že nový systém by měl běžet bez problémů i na virtuálním stroji, požadujeme fyzický samostatný stroj. Důvodem je důležitost monitoringu, protože se jedná o prakticky jediný rychlý pohled na stav infrastruktury a proto by měl být co nejvíce nezávislý na monitorované infrastruktuře

Jako jádro monitorovacího systému předpokládáme nasazení některého ze známých projektů. Mezi ně patří Icinga<sup>9</sup>, Centreon<sup>10</sup> či Zabbix<sup>11</sup>. Tím nejsou vyloučeny ani ostatní projekty pokud se ukáže jejich použitelnost.

Pro zlepšení informovanosti nakoupíme dvě televizní obrazovky na které budeme promítat stav monitoringu přizpůsobený správcům. Obrazovky budou umístěny do druhého (správci databází a služeb) a třetího patra (správci sítí a operačních systémů) budovy CIV a bude na ně promítán přehledový stav o službách za které dané patro zodpovídá. Tento model jsme si úspěšně odzkoušeli na operátorském stanovišti v projektu FR CESNET 371R1/2010. Tyto obrazovky se budou lišit svým obsahem, proto potřebujeme nový a snadněji ovladatelný nástroj pro jejich nastavování. Součástí nákupu bude také řešení promítání webu do televizních obrazovek, pravděpodobně jednoduchý HDMI dongle se síťovým rozhraním, například chromecast.

Největší objem prací bude věnován přechodu ze současného řešení na nové. Jedná se o převod testů, ale hlavně rozmyšlení automatizace a to zejména přidávání nových hostů a jejich aktualizace.

Asi nejvíce viditelnou částí pak bude nutnost přizpůsobení výstupu pro jednotlivé cílové skupiny (uživatelé, operátoři, správci, ...) včetně nastavení upozornění.

Plánujeme ještě v průběhu projektu nasadit výsledky do provozního stavu. Předtím je nutné seznámit uživatele s novinkami a připravit je na přechod.

### 4 Presentace výsledků

Za nejzajímavější část práce považujeme automatizaci. Proto bychom chtěli prezentovat toto řešení na některém semináři nebo konferenci určené odborné veřejnosti. Plánujeme

---

<sup>8</sup>Toto řešení jsme viděli i v jiných firmách, <https://puppet.com/> ji však měl nejvíce proracovanou.

<sup>9</sup><https://www.icinga.com/>

<sup>10</sup><https://www.centreon.com/en/>

<sup>11</sup><https://www.zabbix.com/>

přihlásit přednášku na známé české konference jako jsou OpenAlt<sup>12</sup> nebo EurOpen<sup>13</sup>.

Plánujeme několik seminářů na kterých nové vlastnosti a používání nového monitoringu vysvětlíme uživatelům ještě před jeho nasazením do provozu.

Všechny výsledky projektu budou k dispozici členům sdružení CESNET a veřejně dostupné na webu.

## 5 Charakteristika řešitelského týmu

Řešitelský tým je složen ze zkušených pracovníků Laboratoře počítačových systémů Centra informatizace a výpočetní techniky na Západočeské univerzitě v Plzni. Řešitelský kolektiv má zkušenosti z oblasti správy operačních systémů a jejich implementace do infrastruktury distribuovaného výpočetního prostředí.

Řešitelský kolektiv tvoří:

*Ing. Michal Švamberg (hlavní řešitel)* vystudoval obor distribuované systémy na Fakultě aplikovaných věd na Západočeské univerzitě v Plzni. Od roku 2002 pracuje v Laboratoři počítačových systémů, Centra informatizace a výpočetní techniky, kde se účastnil návrhu a budování kolejních sítí Západočeské univerzity. Dále se zabývá správou operačního systému Linux a jeho integrací do distribuovaného výpočetního prostředí *Orion*. Spravuje diskovou FibreChannel infrastrukturu, souborový systém AFS, systém virtualizace serverů založených na technologii XEN a mnoho dalších. Na ZČU působí jako instruktor v certifikačních programech CCNA a CCNP. Podílí se na správě národní gridové infrastruktury MetaCentrum.

*Bc. Milan Ševčík (spoluřešitel)* je absolventem Fakulty aplikovaných věd Západočeské univerzity v Plzni v oboru Výpočetní technika. Od roku 2014 pracuje v Laboratoři počítačových systémů Centra informatizace a výpočetní techniky, kde spravuje především Javové aplikační servery. Dále se zabývá správou operačního systému Linux a některých webových aplikací nasazených v prostředí univerzity. Dále je členem projektové části cloudové skupiny MetaCentra.

## 6 Navrhovaná doba trvání projektu

Navrhovaná doba trvání projektu je plánována na 12 měsíců. Tuto dobu předpokládáme jako minimální pro úspěšné dokončení projektu.

---

<sup>12</sup><http://www.openalt.cz/>

<sup>13</sup><http://www.europen.cz/>

## 7 Finanční rozvaha

Pro projekt jsou požadovány jen náklady spojené s řešením grantu, které činí 388 000,- Kč (409 000,-Kč s DPH). Z prostředků Fondu rozvoje budou čerpáno ve výši 164 000,- Kč (170 000,- Kč s DPH), zbylou částku 224 000,- Kč (239 000,- Kč s DPH) včetně dalších nákladů spojených s projektem hradí řešitelská organizace. Spoluúčasť Západočeské univerzity je v poměru 57,7% k celkovým nákladům projektu.

Náklady na pokrytí projektu byly stanoveny v tisících Kč následovně:

položka	bez DPH	s DPH	zdroj financování
server	70	85	ZČU
2x televize s příslušenstvím	30	36	CESNET
mzdy	100	100	CESNET
odměny řešitelům	60	60	ZČU
povinné odvody ze mzdy a odměn (34%)	34	34	CESNET
povinné odvody ze mzdy a odměn (34%)	20	20	ZČU
tuzemské cestovné, konferenční	20	20	ZČU
režie (15% z NIV)	54	54	ZČU
celkem	388	409	

Tuzemské cestovné a konferenční pokrývá náklady odhadované na prezentaci výsledků projektu na některé z konferencí zabývající se otevřenými systémy nebo vývojem a správou systémů, případně jiným příbuzným tématem.

Cena serveru je odhadnuta z výběrového řízení ZČU proběhlé na podzim 2017, kdy byl v ceně 63 100,- Kč bez DPH vysoutěžen obdobný stroj, který bychom pro nasazení předpokládali. Rozdíl je pouze v počtu a velikosti disků. Výsledky výběrového řízení jsou veřejně k dispozici na profilu zadavatele<sup>14</sup>.

Předpokládaná životnost serveru je minimálně 5 let, čemuž odpovídají záruční podmínky a hardwarová konfigurace, kterou pro použití zamýšlíme:

- 1x CPU
- 64GB RAM, 1600MHz
- 4x 1TB HDD v HW RAID
- 2x 1Gbps síťové rohraní
- redundantní zdroj napájení
- vzdálený management

Televizní obrazovky předpokládáme v dostatečném rozlišení, minimálně Full HD o velikosti úhlopříčky 55 palců. Cena obrazovek včetně příslušenství (HDMI dongle + držák)

<sup>14</sup>[https://zakazky.zcu.cz/contract\\_display\\_2398.html](https://zakazky.zcu.cz/contract_display_2398.html)

byla odhadnuta na základě průzkumu cen internetových obchodů. Nákup bude proveden veřejnou soutěží dle zákonných podmínek.

Předpokládaný rozpis prací na projektu je uveden v tabulce číslo 1 v pracovních dnech na plný úvazek (tzv. člověkodny). Jsou zde uvedeny nejdůležitější práce, které na projektu předpokládáme provést. Cenu za jeden pracovní den jsme stanovili na 2500,- Kč včetně odvodů.

Popis předpokládané práce	Pracovních dnů
Analýza možných monitorovacích systémů a výběr kandidáta	5
Instalace serveru a napojení do infrastruktury	1
Instalace a základní nastavení jádra monitorovacího systému	2
Základní nastavení a zabezpečení webového rozhraní	1
Konfigurace administrátorského a uživatelského rozhraní	3
Instalace vzdálených sond a jejich připojení	2
Vzdálený monitoring linux serverů novým způsobem	4
Napojení vzdáleného monitoringu pro "legacy" systémy	2
Konfigurace vzdáleného monitoringu pro OS Windows	4
Monitoring síťových prvků	1
Převod používaných testů ze starého systému	17
Zpracování performance dat a prezentace grafů	4
Automatizace konfigurace	5
Nastavení notifikací	2
Uživatelské pohledy	4
Nasazení do provozu	2
Úprava vlastních sond,	6
Přidání nových testů	4
Napojení na konfigurační management serverů	4
Monitoring uzavřených sítí a prvků v nich, např. koleje	3
Výběr vhodného mobilního klienta, zabezpečení, nastavení	4
<b>Celkem</b>	<b>80</b>

Tabulka 1: Tabulka rozpisu prací rozpočtena na pracovní dny

Celková částka na mzdy přesahuje limitní hodnotu 100 000,- Kč určenou Radou Fondu Rozvoje CESNET ze dne 11.4.2018. Rozsah prací však zůstává zachován z důvodu dokončení celého projektu jako funkčního celku. Považujeme tento projekt za důležitý pro další vývoj IT prostředí univerzity. Proto se náklady na tyto práce ve výši 100 000,- Kč rozhodla uhradit Západočeská univerzita bez nároku na navýšení vlastní spoluúčasti (vlastní mzdy nelze do projektu započítat).