**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Diplomová práce**

# Monitoring IT prostředí pomocí produktu Operations Manager

**Bc. Michal Toman**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ DIPLOMOVÉ PRÁCE

Michal Toman

Informatika

Název práce

**Monitoring IT prostředí pomocí produktu Operations Manager**

Název anglicky

**Monitoring of IT infrastructure using Operations Manager**

---

**Cíle práce**

Hlavním cílem práce je monitoring IT prostředí ve vybrané firmě pomocí produktu System Center Operations Manager.

Dílčí cíle:
Zpracovat přehled řešené problematiky s důrazem na Microsoft System Center 2012. Dále uvést definice jednotlivých modulů, možnosti a funkce prostředí Operations Manager
a porovnat s produkty jiných firem. V rámci vlastního řešení nakonfigurovat agenty na jednotlivých stanicích tak, aby zasílali požadované informace, nastavit monitoring síťových routerů a switchů a upravit operační konzoli, aby přehledně zobrazovala získané informace. Vyhodnotit vlastní práci a uvést závěry a doporučení.

**Metodika**

Práce se skládá ze dvou částí – z přehledu řešené problematiky a vlastního řešení. Předpokladem přehledu řešené problematiky je komparace vybraných zdrojů odborné literatury.

V přehledu řešené problematiky je nejprve představen nástroj Microsoft System Center 2012 jako celek a poté se práce věnuje představení nástroje Operations Manager. V závěru této kapitoly jsou srovnány i nástroje od jiných výrobců, které obsahují podobné funkce jako Operations Manager.

V rámci vlastního řešení je realizován postup konfigurace jednotlivých agentů, kteří mají na starosti sběr požadovaných informací a také nastavení monitoringu síťových routerů a switchů. V další kapitole jsou vyhodnoceny a zpracovány získané informace.

**Doporučený rozsah práce**

50- 60 stran

**Klíčová slova**

Operations Manager, System Center, monitoring služeb, monitoring zařízení, operační konzole

---

**Doporučené zdroje informací**

CORNELISSEN, Bob. Mastering System Center 2012 Operations Manager. Indianapolis: John Wiley & Sons, 2013, xxvi, 646 p.

HERMANS, Danny. Microsoft system center software update management field experience. pages cm. ISBN 9780735695825.

MEYLER, Kerrie, Cameron FULLER a John JOYNER. System center 2012 operations manager unleashed. Indianapolis, Ind.: Sams, c2013, xxxii, 1492 p. Unleashed. ISBN 0672335913.

WALLACE, George. Microsoft system center extending operations manager reporting. pages cm. ISBN 9780735695788.

---

**Předběžný termín obhajoby**

2015/16 LS – PEF

**Vedoucí práce**

Ing. Jiří Vaněk, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

**Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2015

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 21. 03. 2016

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Monitoring IT prostředí pomocí produktu Operations Manager" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 29. 3. 2016 _____

Poděkování

Rád bych touto cestou poděkoval panu Ing. Jiřímu Vaňkovi, Ph.D. za jeho cenné připomínky, podporu a odborné vedení, které mi poskytl při vypracování této diplomové práce.

Poděkování patří také Petrovi Krausovi a Václavu Štáfkovi za vytvoření vhodných podmínek ve vybrané firmě k tvorbě této práce. Děkuji i své přítelkyni a rodině za podporu, kterou mi po celou dobu poskytovali.

# Monitoring IT prostředí pomocí produktu Operations Manager

**Souhrn**

Tato diplomová práce se zabývá monitoringem IT prostředí za pomocí produktu Microsoft System Center Operations Manager, který patří mezi dohledové systémy.

V první části je práce zaměřena na jednotlivé kategorie dohledových systémů a na protokoly, které jsou pro monitoring používány. Vzhledem k tomu, že Operations Manager je součástí celé rodiny produktů nástroje System Center a dohromady tvoří silný nástroj pro IT oddělení, jsou zde představeny i ostatní produkty této rodiny. V závěru první části jsou představeny 3 konkurenční dohledové systémy, mezi kterými se firma rozhodovala a které patří mezi nejznámější dohledové systémy.

Druhá část práce obsahuje postup nasazení vybraného dohledového systému včetně jeho všech komponent a jeho následnou konfiguraci tak, aby reporty byly pro administrátory přehledné a snadno získatelné. Poslední část práce se věnuje vyhodnocení získaných informací a varování.

**Klíčová slova:** Operations Manager, System Center, monitoring, dohledové systémy, operační konzole

# Monitoring of IT infrastructure using Operations Manager

**Summary**

This thesis deals with monitoring of IT environments using Microsoft System Center Operations Manager, which belongs to surveillance systems.

The first part of the thesis focuses on individual categories of surveillance systems and protocols that are used for monitoring. Given that Operations Manager is part of a family of products System Center and together they form a powerful tool for IT departments, they are presented as well as other products in this family. At the end of first part there are presented the three competing surveillance systems, among which the company had to decide which to use and which are the best known surveillance systems.

The second part contains the procedure to deploy the selected monitoring system including all of its components and its subsequent configuration so that the reports were for administrators organized and easy to obtain. The last part deals with the evaluation of information and warnings.

**Keywords**: Operations Manager, System Center, monitoring, surveillance systems, operating console

# Obsah

# Seznam obrázků

# Seznam tabulek



# Seznam příloh

# 1. Úvod

Správa rozsáhlé IT infrastruktury ve velkých společnostech vyžaduje komplexní řešení, které nabídne administrátorům centrální správu prostředí, sofistikované zálohování celé infrastruktury, automatizaci úloh a také rozsáhlý monitoring IT služeb. V případě výpadku některého ze zařízení by mohlo dojít k nevyčíslitelným ztrátám nebo dokonce krachu celé firmy. Jedním z nástrojů pro komplexní správu IT prostředí je Microsoft System Center 2012 R2. Tento nástroj obsahuje celou řadu možností, které usnadňují administrátorům správu veškeré IT techniky. Jednotlivými nástroji jsou například Configuration Manager, Orchestrator, Service Manager a také Operations Manager.

Operations manager je takzvaný dohledový systém. Ten má za úkol detailně monitorovat IT prostředí a poskytovat informace o jeho zdraví. Funguje na principu periodického zjišťování dostupnosti a stavu jednotlivých uzlů a v případě, že se některý z uzlů nehlásí nebo je vyhodnocen jako problémový, tak upozorní administrátora sítě, který tak může na daný problém ihned zareagovat a vyřešit ho mnohdy ještě před tím, než uživatel zpozoruje, že se objevila chyba.

Mezi nejpoužívanější dohledové systémy patří System Center Operations Manager, který autor vybral v rámci diplomové práce pro monitoring IT prostředí, ale dále například Nagios XI, Cacti nebo Zabbix.

# 2. Cíl práce a metodika

## 2.1. Cíl práce

Hlavním cílem práce je monitoring IT prostředí ve vybrané firmě pomocí produktu System Center Operations Manager.

Dílčí cíle:

Zpracovat přehled řešené problematiky s důrazem na Microsoft System Center 2012. Dále uvést definice jednotlivých modulů, možnosti a funkce prostředí Operations Manager a porovnat s produkty jiných firem.

V rámci vlastního řešení nakonfigurovat agenty na jednotlivých stanicích tak, aby zasílali požadované informace, nastavit monitoring síťových routerů a switchů a upravit operační konzoli, aby přehledně zobrazovala získané informace. Vyhodnotit vlastní práci a uvést závěry a doporučení.

## 2.2. Metodika

Práce se skládá ze dvou částí – z přehledu řešené problematiky a vlastního řešení. Předpokladem přehledu řešené problematiky je komparace vybraných zdrojů odborné literatury.

V přehledu řešené problematiky je nejprve představen nástroj Microsoft System Center 2012 jako celek a poté se práce věnuje představení nástroje Operations Manager. V závěru této kapitoly jsou představeny i nástroje od jiných výrobců, které obsahují podobné funkce jako Operations Manager.

V rámci vlastního řešení je realizován postup konfigurace jednotlivých agentů, kteří mají na starosti sběr požadovaných informací a také nastavení monitoringu síťových routerů a switchů. V další kapitole jsou vyhodnoceny a zpracovány získané informace.

# 3. Přehled řešené problematiky

Bez monitoringu funkčnosti informačních technologií již v dnešní době není možné na IT oddělení větších společností fungovat. Výsledky monitoringu patří k základním údajům, které ke své práci potřebují IT administrátoři. Monitoring značně ušetří čas správců sítě a tím potažmo i náklady celé firmy. Autor nejprve představí jednotlivé kategorie dohledových systémů a protokoly pro jejich fungování.

## 3.1. Kategorie dohledových systémů

Dohledové systémy se dělí do jednotlivých kategorií podle jejich funkčnosti. U všech kategorií platí, že se v nich nenalézá pouze jeden typ nebo nástroj dohledového systému, ale navzájem se prolínají. Ty nejlepší systémy na monitoring zasahují do většiny zde uvedených kategorií.

### 3.1.1. Notifikační

Tato kategorie dohledových systémů primárně slouží pro upozornění administrátora, že vyvstal nějaký problém. Nejčastější metodou, jak administrátora kontaktovat, je využití SMS notifikace nebo zaslání emailu. Některé systémy umožňují zasílání upozornění i přes IM komunikátory nebo pomocí RSS kanálu. Další metody, které se dají použít pro zaznamenání chyb a kontaktování administrátora jsou log soubory nebo také webové rozhraní systému. Notifikační systémy existují jako samostatné systémy, které nasazený monitoring rozšiřují, ale fungují i bez něho nebo mohou být přímo součástí komplexnějších monitorovacích systémů. [1]

### 3.1.2. Application monitoring

Stav programů a měření kvality služeb poskytovaných informačními systémy v reálném čase dovoluje sledovat application monitoring. Nejzákladnější zjišťované informace jsou dostupnost interních i externích služeb, diagnostikování problémů aplikačních serverů a chování jednotlivých aplikací. Tento monitoring lze využít administrátory i pro sledování práce jednotlivých uživatelů. Umožňuje sledovat, jak často jsou daným uživatelem otevřeny konkrétní programy, jak dlouho s nimi uživatel pracuje

[1] PLESKOT, Vít. *Dohledové systémy pro počítačové sítě*, s.13.

nebo počet písmenek, která v daném programu napsal. Dají se využít i pro správu licencí, kde například u rozhlehlých společností se ztrácí přehled o instalovaných aplikacích na koncové počítače.[2]

### 3.1.3. Database monitoring

Database monitoring může být i součástí application monitoringu. Monitoruje ale pouze databázové servery. Pomocí aktivního databázového monitoringu můžou být odhaleny chyby ještě dříve, než se projeví u koncových uživatelů. Dochází také k optimalizaci struktury databáze a ulehčuje plánování využití databázových serverů. Mezi další funkce patří sledování propustnosti transakcí a aktivních spojení, umožňují agregovat často volané tabulky pro zlepšení rychlosti databáze nebo mohou obnovit poškozenou databázi do původního stavu.

### 3.1.4. Network monitoring

Bez internetu v dnešní době nemůžou firmy existovat, proto je velice důležité, aby veškeré síťové služby byly funkční. Network monitoring umožňuje kontrolovat propustnost sítě a dostupnost veškerých síťových prvků. Samozřejmostí je sledování propustnosti a latence celé infrastruktury, ale i síťového rozhraní serverů, routerů a switchů. Na základě získaných dat je vytvořena analýza vytížení sítě, pomocí které můžou být administrátorem nastavena různá pravidla pro optimalizace vytížení sítě. [3]

### 3.1.5. Security monitoring

Případný únik dat by mohl pro firmu znamenat její likvidaci. Kvůli tomu by měla být bezpečnost ve firmě nastavena na několika na sobě nezávislých úrovních. Pomocí security monitoringu mohou administrátoři sledovat stav a aktuálnost antivirových programů, nastavení firewallů, ale i dostupnost aktualizací pro operační systémy nebo sledují stav otevřených portů a síťového rozhraní.[4]

---

[2] Network Monitor Software and Windows Development Tools. *Monitortools.com* [online]. [cit. 2015-08-15]. Dostupné z: http://www.monitortools.com

[3] Zařízení v síti pod kontrolou. *Samuraj-cz* [online]. 2009 [cit. 2015-08-15]. Dostupné z: http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/

[4] PLESKOT, Vít. *Dohledové systémy pro počítačové sítě*, s. 18

### 3.1.6. Environment monitoring

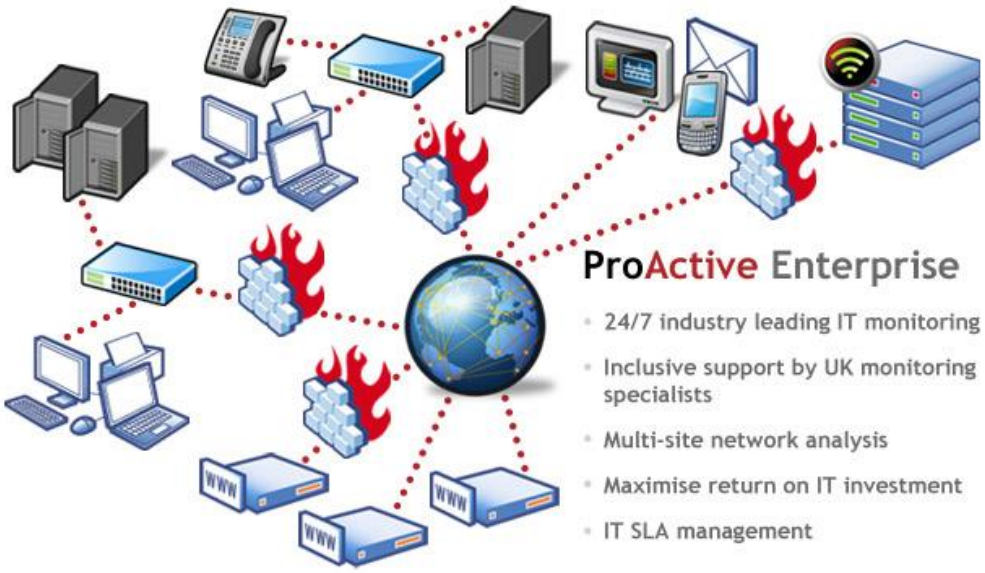
Dlouhodobý provoz IT zařízení v nesprávné teplotě zvyšuje nespolehlivost zařízení. Teplota okolního prostředí v serverové místnosti by měla být v intervalu od 20 do 25°C s vlhkostí ideálně 40 – 50% RH. Nikdy by se nemělo stát, aby teplota uvnitř místnosti přesáhla více jak 30° C. Pro udržování stálé teploty se využívá klimatizací, ale i to jsou pouze stroje a mohou se snadno rozbít. Environment monitoring se zakládá na HW čidlech uvnitř serverové místnosti, která měří teplotu v různých částech místnosti, vlhkost vzduchu, mohou detekovat kouř, vibrace, sledovat úroveň napětí nebo pohyb uvnitř místnosti. Všechna naměřená data jsou předána centrální jednotce, která vše vyhodnotí a v případě, že něco není v pořádku, upozorní administrátora.[5]

### 3.1.7. Enterprise monitoring

Pro velké společnosti je téměř nemožné nasazovat různé produkty pro sledování jednotlivých (zde uvedených) kategorií IT prostředí. Bylo by to složité jak na správu všech dohledových systémů, tak i finančně. Zároveň by docházelo k situacím, že není pro administrátory jasné, kde požadované informace z dohledových systémů naleznou. Z toho důvodu existují enterprise dohledové systémy, které obsahují vlastnosti všech ostatních kategorií monitoringu.

[5] Jak a proč měřit teplotu serverů. *NETguru* [online]. [cit. 2015-08-22]. Dostupné z: http://netguru.cz/network/jak-a-pro-mit-teplotu-server.html

*Obrázek 1 - Enterprise monitoring*




*Zdroj: ProActive Enterprise | Proactive Monitor. ProActive. [online]. [2014] [cit. 2015-11-30]. Dostupné z: http://www.proactivemonitor.co.uk/proactive-enterprise*

Sjednocení všech druhů monitoringu do jednoho nástroje umožňuje mnohem lepší přehled o stavu monitorovaného IT prostředí, ulehčuje administrátorům nastavení monitoringu a poskytuje ucelená data pro další analýzy a plány následného využívání sítě. Enterprise systémy jsou poskytovány převážně jako komerční produkty se svými výhodami i nevýhodami. Nevýhodou je vyšší cena, ale mezi výhody nesporně patří technická podpora při nasazování systému, odborná pomoc pro řešení problémů i neustálé vylepšování a aktualizace systémů.[6]

## 3.2. Protokoly pro monitorování

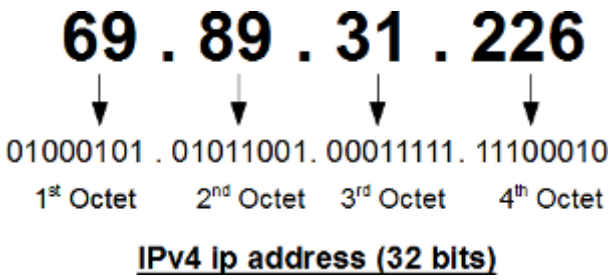
Aby dohledové systémy mohly správně fungovat a monitorovat prostředí, musí s prostředím nějak komunikovat. Pro zjišťování stavu IT prostředků využívají dohledové systémy celé řady síťových protokolů. V následující kapitole jsou představeny nejčastěji využívané protokoly.

[6] PLESKOT, Vít. *Dohledové systémy pro počítačové sítě*, s. 15

### 3.2.1. IP

Tento protokol byl vydán už v roce 1981, ale i přes to, že se jedná o jeden z nejstarších protokolů, tak patří mezi základní protokoly pro komunikaci v počítačových sítích. Základní službou, kterou protokol IP poskytuje, je přenos paketů mezi dvěma uzly. Protokol ale negarantuje pořadí, ve kterém pakety mezi uzly dorazí, ani to, že pakety budou doručeny. Pro realizaci přenosu paketů jsou využity unikátní identifikátory pro každý síťový uzel (IP adresa).

*Obrázek 2 - IPv4*

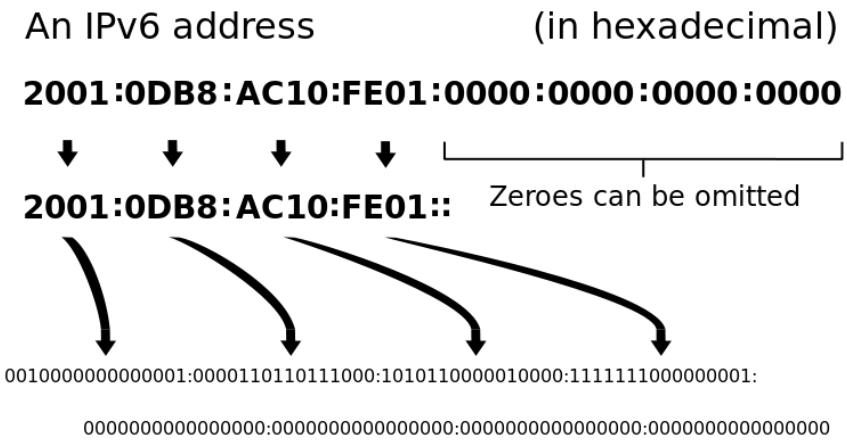



*Zdroj: ip-address-fundamentals. The Geek Stuff. [online]. 15.1.2012 [cit. 2015-11-30]. Dostupné z: http://www.thegeekstuff.com/2012/01/ip-address-fundamentals/*

Původní a doposud používaný protokol nese označení IPv4. S rozvíjejícím se internetem ale došlo k vyčerpání adresního prostoru protokolu IPv4. Z toho důvodu došlo k vytvoření protokolu IPv6, který řeší nedostatky předcházející verze. Způsob adresování byl změněn na 128 bitové adresy, což umožňuje přidat unikátní IP adresu pro $3{,}4\times10^{38}$ síťových zařízení. [7]

[7] IP - Internet Protocol. *EArchiv.cz: Archiv článků a přednášek Jiřího Peterky* [online]. [cit. 2015-08-22]. Dostupné z: http://www.earchiv.cz/anovinky/ai1843.php3

*Obrázek 3 - IPv6*

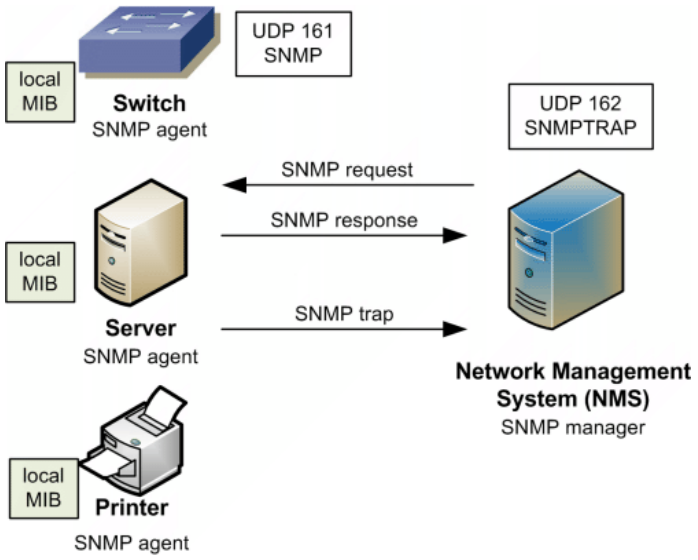



*Zdroj: The IP Address. Vista Networking Solutions. [online]. 10.3.2013 [cit. 2015-11-30]. Dostupné z: http://blog.vnssystems.com/*

### 3.2.2. SNMP

Pro správu a dohled síťových zařízení byl konkrétně vytvořen protokol SNMP. Nachází se na aplikační vrstvě. Na sledovacím zařízení je spuštěn SNMP agent, který přijímá SNMP požadavky od SNMP serveru. Tyto požadavky mají nastavený identifikátor typu SNP zprávy, který nabývá hodnot GetRequest, GetNextRequest, SetRequest, GetResponse, GetBulk, Inform a SetRequest. SNMP agent získá ze správy jednoznačný identifikátor SNMP hodnoty (OID) a podle typu požadavku ji nastaví nebo zašle zpět získaná data.

*Obrázek 4 - Komunikace prostřednictvím protokolu SNMP*




*Zdroj: Zařízení v síti pod kontrolou. Samuraj-CZ. [online]. 21.9.2009 [cit. 2015-11-30]. Dostupné z: http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/*

Protokol SNMP byl postupně rozvíjen. První verze využívala pro ověřování, jestli je zdroj požadavku autorizovaný, pouze jednoduchý textový řetězec, který nebyl zašifrovaný. Posun v oblasti výkonu přinesla verze 2. Ta sice nezlepšila zabezpečení protokolu, ale alespoň umožnila získávání velkého množství dat. K zabezpečení došlo v poslední verzi, která je označována jako SNMP v3. Tato nová verze zavádí ověřování pomocí jména a hesla a také přináší šifrování celé komunikace. [8]

### 3.2.3. TCP

Další protokol využívaný dohledovými systémy se nazývá TCP. Jedná se o základní protokol, který je spojově orientovaný a pracuje na transportní vrstvě ISO/OSI modelu. Tento protokol slouží k zajištění potvrzení doručování paketů a k jejich seřazení ve správném pořadí. Nevýhodou protokolu je to, že značně zpomaluje proces doručení dat, jelikož provádí ověřování správného seřazení paketů. Protokol TCP spolu s protokolem IP tvoří základní komunikační sadu protokolů pro přenos dat v rámci internetu. [9]

### 3.2.4. ICMP

Servisní protokol nese označení ICMP. Primárně neslouží k přenosu aplikačních dat, ale je využíván k hlášení chyb a pro šíření informací napříč sítí. Jeho zprávy se generují při výskytu chybových událostí, mezi které patří například nedostupnost příjemce, přesměrování nebo vypršení TTL. ICMP zprávy jsou po síti posílány zabalené v jednom IP datagramu, takže je komunikace jednoduchá a rychlá. Tento protokol využívá např. příkaz traceroute, pomocí kterého jsou zasílány zprávy echo request. Pomocí odpovědí TTL je sestavena síťová cesta ke sledovanému cíli.[10]

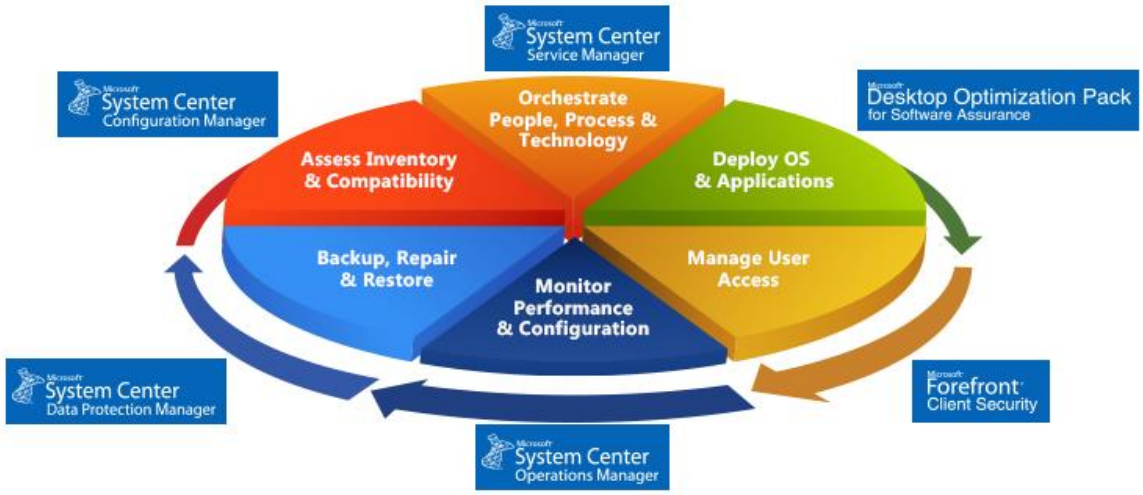
## 3.3. Microsoft System Center 2012 R2

Produkt System Center 2012 R2, jehož vydavatelem je Microsoft, je oblíbená technologie pro výstavbu privátních, hybridních, ale i veřejných cloudů a poskytuje

[8] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*, s. 94
[9] Tamtéž, s. 446
[10] Protocol Registries. *IANA: Internet Assigned Numbers Authority* [online]. [cit. 2015-08-24]. Dostupné z: http://www.iana.org/protocols

administrátorům jednotnou správu IT infrastruktury. [11] Tento produkt obsahuje řadu komponent, které dohromady vytvářejí velmi silný nástroj obsahující veškeré potřebné funkce. Mezi komponenty patří Operations Manager, Configuration Manager, Orchestrator, Data Protection Manager, Service Manager, Client Security.[12]

*Obrázek 5 - komponenty System Center*




*Zdroj: Products | Microsoft System Center*. Cased dimensions. *[online]. [2014] [cit. 2015-08-10]. Dostupné z:* http://www.caseddimensions.com/microsoft_system_center/

### 3.3.1. Configuration Manager

Pomocí tohoto nástroje lze zvýšit efektivitu i produktivitu IT snížením počtu ručních úloh. Configuration Manager umožňuje zajistit bezpečné a škálovatelné nasazení softwaru, správu nastavení a komplexní správu prostředků jak pro servery, tak i pro koncové zařízení. [13]

### 3.3.2. Orchestrator

Tento nástroj má za úkol automatizovat tvorbu a provádět nasazení prostředků v podniku. Umožňuje vytvářet vizuální kompilace a integruje úlohy pro různé platformy. [14]

[11] Přehled nástroje System Center 2012 R2 | Microsoft. *System Center 2012 R2.* [online]. [2015] [cit. 2015-08-10]. Dostupné z: *http://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Overview.aspx*

[12] Microsoft System Center. *Dimensions* [online]. [cit. 2015-08-05]. Dostupné z: http://www.caseddimensions.com/microsoft_system_center/

[13] System Center 2012 R2. *Microsoft* [online]. [cit. 2015-11-15]. Dostupné z: https://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Components.aspx

[14] Tamtéž

### 3.3.3. Service Manager

Jedná se o integrovanou platformu pro automatizaci a adaptaci osvědčených postupů správy IT služeb v organizaci. Nabízí integrované postupy pro řešení incidentů a problémů, řízení změn a správu životního cyklu aktiv.[15]

### 3.3.4. Data Protection Manager

Data Protection Manager je podnikový zálohovací systém, pomocí kterého se můžou zálohovat data ze zdrojového umístění do sekundárního cílového umístění. V případě, že dojde ke ztrátě původních dat, dají se ze zálohy obnovit. [16]

### 3.3.5. Client Security

Client Security nebo také Endpoint Protection je malwarová ochrana na koncových zařízeních, která malware nejen identifikuje, ale i odstraní. [17]

*Obrázek 6 - logo Microsoft System Center 2012*


*Zdroj:* blogs.technet.com. The System Center Team Blog. [online]. 2.8.2011 [cit. 2015-08-19]. Dostupné z: http://blogs.technet.com/b/systemcenter/archive/2011/08/02/system-center-monitoring-pack-for-microsoft-dynamics-ax-2012.aspx

## 3.4. System Center Operations Manager

Vzhledem k tomu, že se jedná o produkt z rodiny System Center, je Operations manager někdy označován jako SCOM (System Center Operations Manager). Pomocí tohoto systému lze monitorovat celé IT prostředí ve společnosti. Jedná se o proaktivní

[15] System Center 2012 R2. *Microsoft* [online]. [cit. 2015-11-15]. Dostupné z: https://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Components.aspx
[16] Tamtéž
[17] Tamtéž

dohledový systém, který ukládá získaná data z monitorování do databáze a umožňuje reportování problémů administrátorům.

### 3.4.1. Historie

Dohledový systém Operations Manager vznikl jako systém pro správu sítě s názvem Sentry ELM, který byl vyvinut britskou společností Serverware Group plc. V roce 1998 byly práva na tento systém koupeny společností Mission Critical Software, inc která přejmenovala tento systém na nový název Enterprise Event Manager. Tato společnost se ujala kompletního přepsání programu a na konci této změny vznikl program OnePoint Operations Manager (OOM). V roce 2000 došlo k prodání licence na tento systém společnosti Microsoft, která systém vlastní a vyvíjí doposud a která systém opět přejmenovala, tentokráte na Microsoft Operations Manager (MOM). [18]

Od chvíle, co licenci na tento dohledový systém vlastní Microsoft, byly vydány tři verze. První nesla název Microsoft Operations Manager 2005. Další verze již byla součástí rodiny produktů System Center a celý její název byl System Center Operations Manager 2007. Od této verze došlo opět k přepsání celého kódu, a i když se verze 2007 podobá předešlé verzi, tak se nejedná o upgrade, ale o zcela novou verzi.

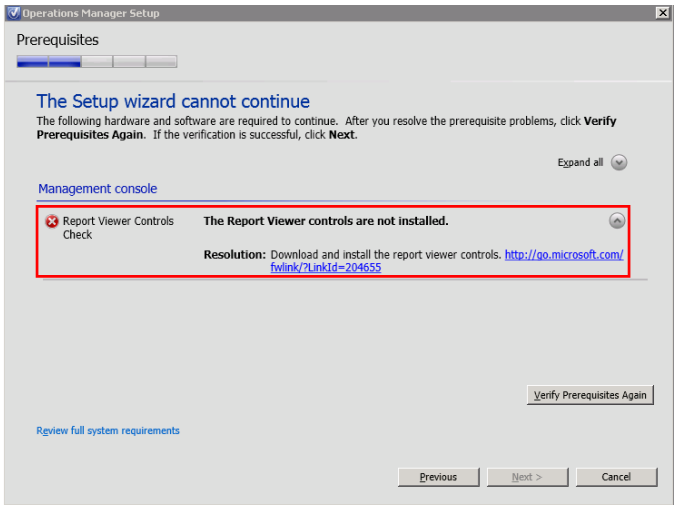
Poslední verze tohoto dohledového systému nese název System Center Operations Manager 2012 a touto verzí se zabývá i tato diplomová práce.

### 3.4.2. Současnost

Nejnovější systém se nazývá System Center Operations Manager 2012 R2. Během jeho instalace se uživatelům zobrazí nový průvodce instalací, který je znám ze systému System Center Essentials 2010. Průvodce uživatele pohodlně provede celým instalačním procesem a v případě, že je na serveru něco špatně nakonfigurováno nebo něco schází, tak průvodce nedovolí pokračovat dál v instalaci.

[18] MEYLER, Kerrie, Cameron FULLER a John JOYNER. *System center 2012 operations manager unleashed*. S. 59

*Obrázek 7 - nemožnost pokračovat v instalaci*




*Zdroj - První pohled na System Center Operations Manager 2012. Optimalizované IT [online]. 13.12.2011 [cit. 2016-01-20]. Dostupné z: [http://www.optimalizovane-it.cz/sprava-it-prostredi/strana-2.html](http://www.optimalizovane-it.cz/sprava-it-prostredi/strana-2.html)*

Další novinkou současné verze je, že jsou všechny Management Servery považovány za rovnocenné a není nutno mít roli Root Management Server. Zátěž je rozdělena mezi všechny Management Servery a je zajištěna bez nutnosti clusteru vysoká dostupnost.

*Obrázek 8 - Role Roor Management Serveru*


*Zdroj : První pohled na System Center Operations Manager 2012. Optimalizované IT [online]. 2011 [cit. 2016-01-20]. Dostupné z: http://www.optimalizovane-it.cz/sprava-it-prostredi/strana-2.html*

K několika drobným změnám došlo i v operační konzoli. Došlo zde k přejmenování několika panelů a doplnění oddílu Navigation, který administrátorům zajistí snazší otevírání pohledů při práci s objekty.

Výraznou změnou je i změna licenční politiky. Zatím co dříve měl každý produkt rodiny System Center své vlastní licenční podmínky, s představením verze 2012 došlo k značnému zjednodušení. Nyní se již prodávají pouze licence pro správu (management license) dostupná ve dvou verzích (Standard a Datacenter). Po zakoupení kterékoli z těchto licencí jsou zpřístupněny všechny produkty System Center. [19]

- Licence ML Standard pokrývá dva fyzické procesory nebo dvě spravovaná OSE (Operating System Environment)
- Licence ML Datacenter pokrývá dva fyzické procesory a umožňuje správu neomezeného množství OSE

### 3.4.3. **Vlastnosti**

Základní instalace SCOM zahrnuje 4 komponenty:

- Management server
- Operations console
- Web console
- Reporting server

Komponenta Management server umožňuje centralizovanou komunikaci mezi agenty a databází. Nemůže být nainstalována na tom samém počítači nebo serveru, kde je již nainstalovaný agent pro sběr údajů.

Operations console poskytuje rozhraní pro provádění monitorování, správu, ověřování a správu reportingu.

Web console dovoluje administrátorovi přistupovat, kontrolovat a plánovat aktivity pro monitoring přes webovou stránku.

Poslední komponenta – reporting server – poskytuje administrátorovi možnost vytvořit a prohlédnout reporty v konzoli Operations Manager na základě dotazování z úložiště Operations Manager. [20]

---

[19] Novinky v System Center 2012 R2. *Daquas* [online]. [cit. 2015-08-13]. Dostupné z: http://www.daquas.cz/articles/622-novinky-v-system-center-2012-r2

[20] WALLACE, George. *Microsoft system center extending operations manager reporting*. S. 1

Management server uživatelům nabízí:

- Management pro správu a zpracování základní administrativy a zprostředkování připojení k databázím
- Provozní databázi poskytující SQL databázi pro aktuální reporting
- Dlouhodobou SQL databázi pro zaznamenání dlouhodobých reportů

Operations manager pomocí agentů nainstalovaných na sledovaných zařízeních sleduje výkon systému a sbírá data, která posílá zpět systému. S její pomocí je sledováno správné fungování fyzické, virtuální i cloudové infrastruktury. Vestavěná funkce pro zjišťování síťové topologie umožňuje monitorovat stav síťových zařízení a virtuální sítě.

Bezproblémová integrace mezi komponentami nabízí možnost podrobného monitorování prostředků infrastruktury privátního cloudu. SCOM také optimalizuje výkon úložiště pro klíčové úlohy.

Nástroj Operations Manager umožňuje monitorovat služby, zařízení a provoz mnoha počítačů na jediné konzoli. Administrátoři získávají rychlý přehled o stavu IT prostředí a IT služeb spuštěných napříč různými systémy.

•Monitorování a vydávání výstrah týkajících se infrastruktury a aplikací

•Monitorování úloh společnosti Microsoft a třetích stran

•Monitorování cloudu, včetně platformy Azure

•Informace o stavu, zdraví a výkonu systému[21]

### 3.4.4. **Nasazení**

Při nasazení platí, že pro provozování základních rolí (MS, DB, RS, DW) Operations Manager 2012 Management Group na jednom serveru pro dohled IT prostředí o cca 100 serverech, 50 síťových zařízeních a vytvoření několika vlastních syntetických transakcí nebo distribuovaných aplikací, jsou minimální HW požadavky 8 GB RAM, procesor QUAD Core CPU (Xeon) s rychlými disky o celkové kapacitě alespoň 200 GB.

[21] Preparing your environment for System Center 2012 R2 Operations Manager. *TechNet* [online]. 2015 [cit. 2015-07-20]. Dostupné z: https://technet.microsoft.com/en-us/library/dn249696.aspx

**Minimální doporučené požadavky na hardware:** [22]

- Architektura AMD64
- RAM 4 GB a více (nelze nainstalovat s méně než 2 GB)
- HDD 200 GB a více
- Procesor QUAD Core, 2,8 GHz a více

**Minimální doporučené požadavky na software:** [23]

- OS Windows Server 2008 R2
- SQL Server 2008 SP1, R2 a vyšší (SQL Server collation na SQL_Latin1_General_CP1_CI_AS)
- .NET Framework 3.5 Service Pack 1 (SP1)
- .NET Framework 4
- Microsoft Core XML Services version 6.0
- Authorization Manager hotfix (KB975332)
- Windows PowerShell version 2.0
- Windows Remote Management
- Microsoft Report Viewer 2008 SP1 Redistributable Package (Operační konzole)
- Internet Information Services (IIS) v7.5 a vyšší (Web Console)

[22] CORNELISSEN, Bob. *Mastering System Center 2012 Operations Manager*. S. 25
[23] Tamtéž

*Tabulka 1 - Doporučené počty objektů v rámci infrastruktury Operations Manager 2012*

| Monitored item | Recommended limit |
|---|---|
| Simultaneous Operations consoles | 50 |
| Agent-monitored computers reporting to a management server | 3000 |
| Agent-monitored computers reporting to a gateway server | 2000 |
| Agentless Exception Monitored (AEM)-computers per dedicated management server | 25000 |
| Agentless Exception Monitored (AEM)-computers per management group | 100000 |
| Collective client monitored computers per management server | 2500 |
| Management servers per agent for multihoming | 4 |
| Agentless-managed computers per management server | 10 |
| Agentless-managed computers per management group | 60 |
| Agent-managed and UNIX or Linux computers per management group | 6000 (with 50 open consoles)<br>10000 (with 25 open consoles) |
| UNIX or Linux computers per dedicated management server | 500 |
| UNIX or Linux computers monitored per dedicated gateway server | 100 |
| Network devices managed by a resource pool with three or more management servers | 1000 |
| Network devices managed by two resource pools | 2000 |
| Agents for Application Platform Monitoring (APM) | 700 |
| Applications for Application Platform Monitoring (APM) | 400 |
| URLs monitored per dedicated management server | 3000 |
| URLs monitored per dedicated management group | 12000 |
| URLs monitored per agent | 50 |

*Zdroj:* Jak na instalaci System Center Operations Manager 2012. Pavel Řepa – IT management [online]. [cit. 2015-11-21]. Dostupné z: https://pavelrepa.wordpress.com/2011/11/28/jak-na-instalaci-system-center-operations-manager-2012/

### 3.4.5. Správa

Potřebná nastavení lze vytvořit několika způsoby. Prvním z nich je využít Operatins Manager, kde se v záložce Administration nachází srozumitelně roztříděné možnosti k nastavení. Administrátor zde má velkou skupinu device management, ve které má možnost zobrazit a nastavit zařízení, na kterých jsou nainstalovaní agenti, na kterých nejsou agenti, UNIX/Linux počítače a management serverů. Další záložka Nerwork management umožňuje monitorovat síťové připojení a jeho zdraví. Samozřejmostí je nastavení notifikací a zabezpečení.

Druhou možností, jak provést potřebná nastavení, je využít nainstalovaného nástroje Operations Shell Manager. Po zadání příkazu „get-command –module

operationsmanager“ se administrátorovi zobrazí veškeré příkazy, které může použít pro nastavení SCOM. [24]

## 3.5. Produkty jiných firem

Není to pouze Microsoft, který vyvíjí svůj vlastní dohledový systém. Existuje celá řada dalších nástrojů. Mezi nejznámější z nich patří Cacti, Zabbix a Nagios XI.

### 3.5.1. Cacti

Systém Cacti byl dříve vyvíjen pod názvem HotSaNIC (HTML overview to System and Network Information Center). HotSaNIC byl nástroj pro tvorbu grafů o činnosti serveru, který umožňoval sledovat traffic na síťových kartách, vytížení procesorů, počet procesů, stav paměti, počet přihlášených uživatelů, kapacity pevných disků a další zajímavé údaje. Další rozvoj systému ale přinesl přejmenování na Cacti.

Systém je postaven na RRDtools, pomocí kterých jsou ukládány a načítány všechny potřebné informace pro vytváření grafů z MySQL databáze. Je to open source systém a kompletně je napsán v jazyce PHP.

Cacti umožňuje vytvoření uživatelských účtů s vazbou na odlišné grafy. Toho může být využito například v případě, kdy každý administrátor má na starosti jinou oblast. Jeden administrátor tak může sledovat například vytížení serverů a druhý má zpřístupněno sledování dostupnosti a vytíženosti sítě i jejích prvků.

Dohledový systém Cacti primárně sbírá a analyzuje data a oproti ostatním dohledovým systémům je u něj sledování infrastruktury v reálném čase až druhořadé. V případě výpadku některé ze služeb je administrátor upozorněn až po několika minutách, což může být u některých společností problém. Cacti nemá ani žádnou placenou variantu a tak je vývoj a přizpůsobení záležitostí čistě na uživateli či komunitě, která se tímto systémem zabývá. Veškeré nastavení a administrace se provádí prostřednictvím webového rozhraní a systém je možno rozšířit o celou řadu doplňků. Pro nasazení pluginů je nejprve nutné nainstalovat plugin Architecture. Instalace pluginů už je potom jen otázkou

[24] CORNELISSEN, Bob. *Mastering System Center 2012 Operations Manager*, s. 231

nakopírování patřičných souborů na správné místo a zapsání názvu pluginu do konfiguračního souboru. Pluginy jsou ke stažení na adrese cactiusers.org. [25]

Cacti podporuje protokoly ICMP, TCP, UDP a SNMP, ale celkově je systém stavěný spíše pro centralizovaný dohled.

.

### 3.5.2. **Zabbix**

Od roku 1998 existuje dohledový systém s názvem Zabbix. Jeho autorem je Alexei Vladishev a primárně byl tento systém tvořený pro banku. Slouží k monitorování aktivních síťových prvků za využití různých metod. Lze nastavit nejzákladnější kontrolu pomocí protokolu ICMP (ping) na základě které zjistí, zda dotazované zařízení odpovídá. Více informací získá zpět pomocí využití složitějších protokolů (SNMP a IPMI). [26]

Dle dokumentace je tento systém schopný monitorovat robustní sít s až 100 000 zařízeními, je ale závislý na systémových zdrojích serveru, na kterém je Zabbix nainstalovaný. Velkou výhodou tohoto monitoringu je jeho webové rozhraní, pomocí něhož může být systém spravován a které slouží i pro vyhodnocování dat. Systém funguje pod licencí GPL a má intuitivní ovládání.

Celý systém se skládá z unixového serveru, agenta a webového rozhraní. Server řídí sběr a vyhodnocení dat a řídí celou logiku systému. Agent je proces, který je spuštěný na hostitelských zařízeních. Sbírá průběžně informace a zasílá je zpět serveru. Pomocí webového prostředí je systém spravován a vyhodnocován administrátorem.

Celý systém splňuje parametry proaktivního monitoringu. Sbírá ve stanoveném časovém úseku data a po vyhodnocení může na základě nastavených scénářů provádět automatické řešení problému.

Za poplatek lze získat podporu systému a také přizpůsobení na míru, ale základní systém je kompletně zdarma. [27]

---

[25] Cacti: vše důležité v jednom monitoru. *ROOT.CZ* [online]. 2009 [cit. 2016-01-28]. Dostupné z: http://www.root.cz/clanky/cacti-vse-dulezite-v-jednom-monitoru/

[26] What is Zabbix. *Zabbix* [online]. [cit. 2015-08-20]. Dostupné z: http://www.zabbix.com/product.php

[27] Dohledový systém Zabbix - představení I. *Linuxsoft.cz* [online]. 2013 [cit. 2015-08-15]. Dostupné z: http://www.linuxsoft.cz/article.php?id_article=1963

### 3.5.3. Nagios

Tento dohledový systém je znám od roku 1999 a řadí se mezi velice populární dohledové systémy. Pod označením Nagios se vyskytuje až od roku 2002, kdy byl přejmenován z původního Netsaint. Jedná se o open source systém, který automaticky sleduje stav počítačových sítí. Největší výhodou tohoto systému je jeho cena – základní systém je k dispozici zdarma. Toto řešení však vyžaduje, aby ten, kdo systém nasazuje, s ním již měl bohaté zkušenosti. Systém se konfiguruje pomocí příkazů v příkazovém řádku a jeho konfigurace je složitá. Mezi další výhody se řadí i možnost přizpůsobení, díky open source řešení, pro jakékoliv požadavky firem. Primárně byl Nagios vyvíjen pro Linux, ale lze jej nasadit i na ostatních unixových systémech. Mezi hlavní nevýhody patří, že pro jeho nasazení je zapotřebí serveru s velkým množstvím paměti.

Existuje i placená verze, která se nazývá Nagios XI. Obsahuje ucelený balík nástrojů pro monitoring sítě a pro tuto verzi je k dispozici technická podpora. [28]

[28] KAPLAN, Věroslav. *Nagios - the monitoring system*. S. 27.

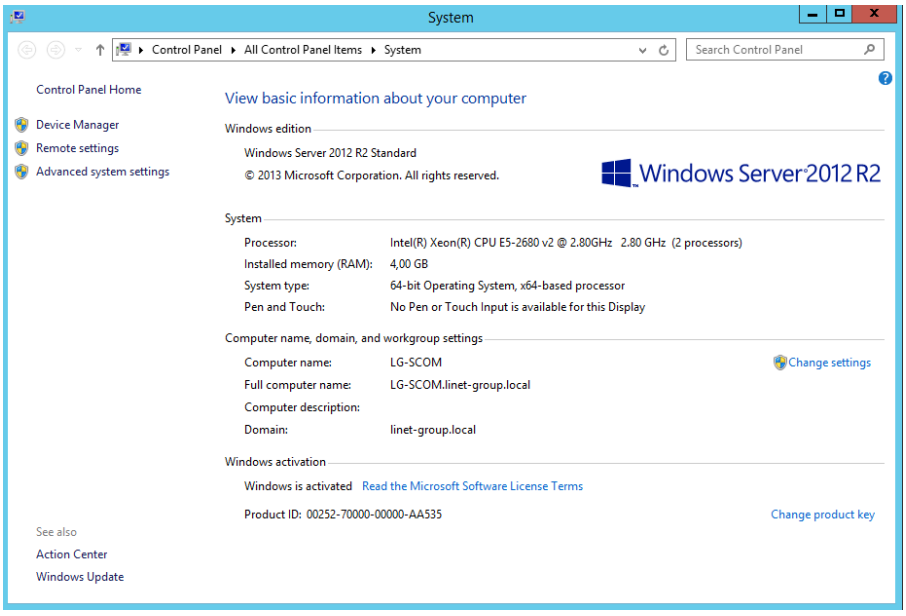
# 4. Praktická část

## 4.1. Příprava serveru

Vzhledem k tomu, že má vybraná firma virtualizované prostředí pomocí VMware nástrojů, byl pro SCOM vytvořen zcela nový virtuální server. Fyzicky se celý tento server skládá ze sedmi ESX serverů. Všechny tyto servery obsahují management kartu a je k nim možno přistupovat pomocí iDRAC [29]. Na serveru určeném pro instalaci SCOM je operační systém Windows Server 2012 R2 64-bit a bylo mu alokováno 40 GB místa na disku, 4 GB paměti a procesor Intel Xeon CPU E5-2680 s 2,80 GHz. Server nese název LG-SCOM a je členem domény „linet-group.local“.

Všechny minimální HW požadavky pro instalaci SCOM (až na velikost disku, která ale díky tomu, že se jedná o virtuální stroj, jde v případě potřeby kdykoliv rozšířit) byly splněny.

*Obrázek 9 - Základní informace o serveru*




*Zdroj: vlastní zpracování*

Dalším krokem bylo stažení image SCOM. Celý ISO soubor má velikost 694 MB a vzhledem k tomu, že již společnost úspěšně používá produkt System Center Configuration Manager a má zakoupenu licenci, nebylo potřeba řešit nákup další licence.

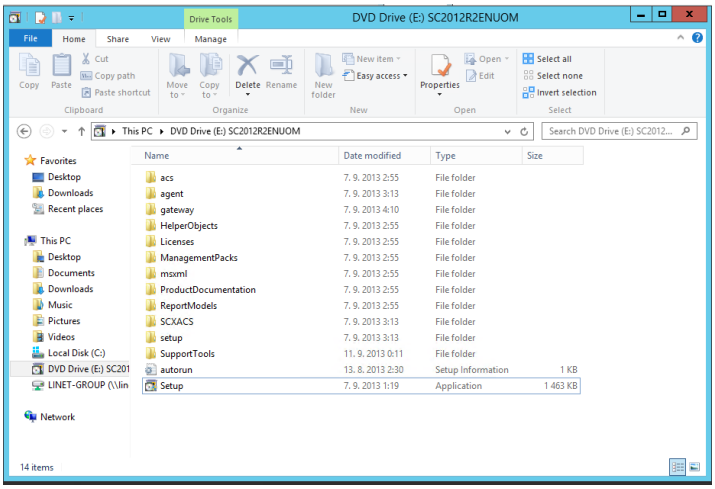
[29] Integrated Dell Remote Access Controller

Aby byly splněny i minimální softwarové požadavky, bylo nutné doinstalovat SQL server. Bylo rozhodnuto, že celá instalace SCOM bude řešena pouze v rámci lg-scom serveru. Z tohoto důvodu nešlo propojit SCOM s již existujícími SQL servery, ale bylo nutné SQL nainstalovat přímo na tento server. První snahou bylo nainstalovat SQL Server Express 2014. Po úspěšné instalaci ale bylo zjištěno, že tento SQL server není aplikací Operations Manager podporován. Došlo tedy ke stažení a instalaci SQL Server 2012 SP2 evaluation verze, která je k vyzkoušení na 90 dnů zdarma. Při její instalaci je velice důležité si dát pozor na SQL Server collation. V případě, že nebude nastavena na SQL_Latin1_General_CP1_CI_AS, tak nebude uživateli umožněno SCOM nainstalovat.

## 4.2. Instalace SCOM

Po připojení ISO souboru k systému se uživateli zobrazí veškerý jeho obsah. Nejzásadnějším souborem je v tuto chvíli SETUP.EXE jehož spuštěním se otevře instalační manager.

*Obrázek 10 - Obsah ISO souboru*




*Zdro: vlastní zpracování*

Při spuštění setup.exe je uživateli nabídnuto, jaké všechny komponenty SCOM se mají nainstalovat:

- Management server
- Operations console
- Web console
- Reporting server

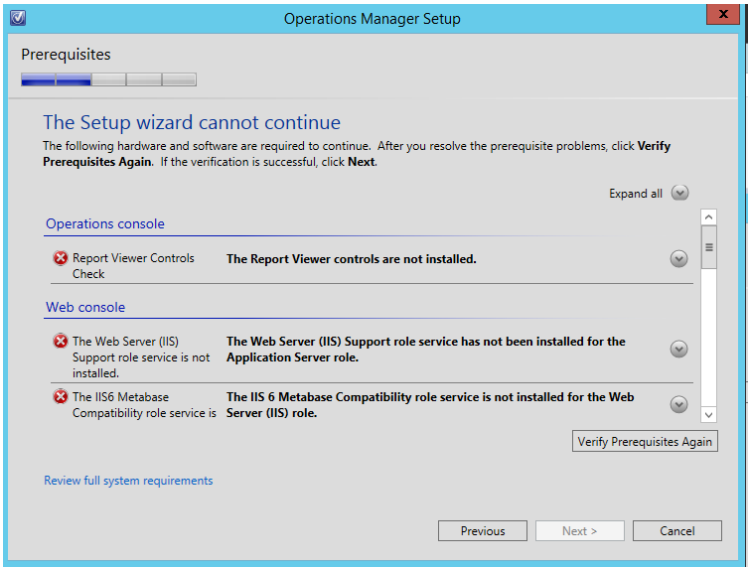
V dalším kroku si zvolí, kam chce aplikaci nainstalovat. Po kliknutí na tlačítko „další“ dojde k ověření instalace a v případě, že na serveru něco schází, je zde detailně napsáno, co a jak je potřeba doinstalovat.

### 4.2.1. Instalace Management serveru a Operations console

Prvotní snahou bylo nainstalovat všechny 4 komponenty SCOM najednou a po jejich instalaci se starat již pouze o jejich správnou konfiguraci a správu. Během instalace ale instalační průvodce zjistil aktuální nastavení serveru a vyžadoval jeho značné úpravy a doinstalování dalších doplňků. Z tohoto důvodu se proto autor rozhodl ze začátku nainstalovat pouze Operations console a Management server a zbylé dvě komponenty vyřešit později.

V případě instalace Operations console bylo dle instalačního manageru potřeba doinstalovat aplikaci Report Viewer Controls, která je na internetu volně ke stažení.

*Obrázek 11 - Požadavky k doinstalování / nastavení*



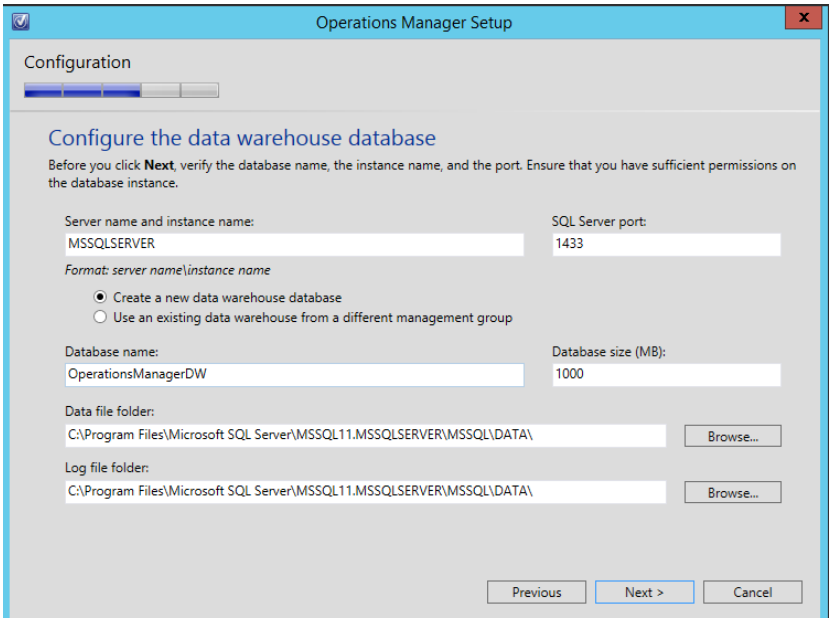

*Zdroj: vlastní zpracování*

Po stáhnutí nejnovější verze Report Viewer Controls došlo k její instalaci, ale ta napoprvé neskončila úspěšně. Pro tuto aplikaci bylo potřeba doinstalovat ASP.Net 2.0 Framework. Vzhledem k tomu, že se jedná o server, tak nebylo možné nainstalovat ASP.Net pomocí klasického instalačního balíčku, ale pomocí Server Manageru. Poté, co byly aplikace ASP.Net 2.0 a následně Report Viewer Controls nainstalovány, mohl autor pokračovat

v samotné instalaci aplikace Operations Manager, respektive v instalaci jeho dvou komponent.

Aby byla instalace dokončena, bylo ještě potřeba nastavit jméno pro Management server, odsouhlasit licenční podmínky a nastavit údaje o SQL databázi, kam budou ukládána veškerá získaná data. Instalační průvodce otestoval připojení k databázi a vytvořil v ní potřebné tabulky. V případě úspěšného testovacího připojení k databázi je konfigurace instalace téměř u konce.

*Obrázek 12 - Nastavení přístupu k databázi*




*Zdroj: vlastní zpracování*

Posledním krokem instalace bylo stanovení účtů pro správu. Celkem bylo zapotřebí vyplnit doménu, uživatelské jméno a heslo pro čtyři úrovně správy SCOM, přičemž není zakázáno použít jeden doménový účet pro všechny čtyři úrovně.

Od této chvíle nebylo potřeba, aby uživatel nastavoval další údaje. Instalační průvodce pouze zobrazil souhrn důležitých údajů o instalaci a následně po kliknutí na tlačítko „Install“ se během 10 minut SCOM na server nainstaloval.

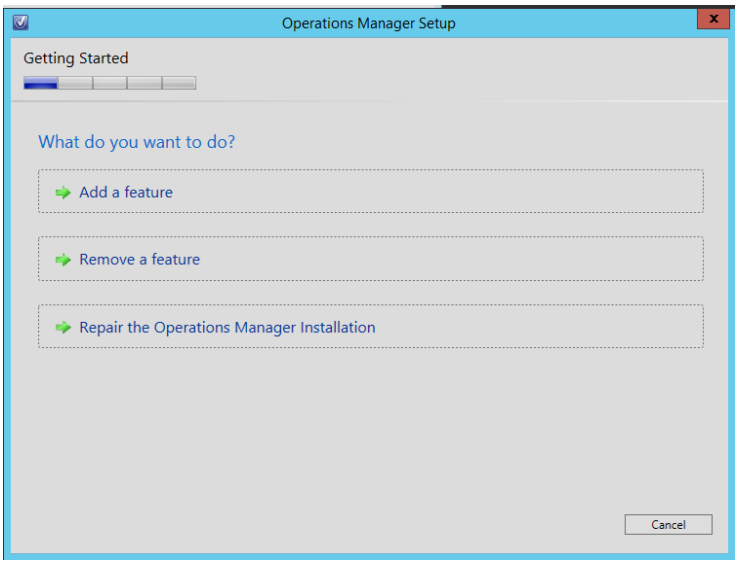
### 4.2.2. Instalace Web Console

Po úspěšné instalaci předešlých dvou komponent přišla na řadu instalace Web Console, která byla ze začátku z důvodu velkého počtu nutných změn přeskočena. Vzhledem

k tomu, že část SCOM již byla na serveru nainstalována, tak instalační průvodce vypadal po spuštění jinak. Jeho nabídka obsahovala možnosti:

- Přidání další komponenty
- Odebrání nainstalované komponenty
- Opravu instalace SCOM

*Obrázek 13 - Změněný instalační manager*

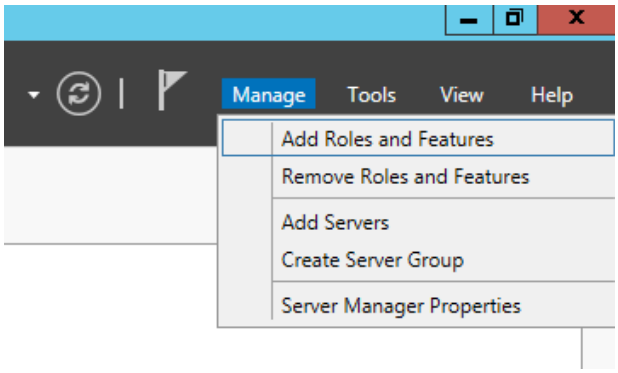



*Zdroj: vlastní zpracování*

Po zvolení možnosti „Add a feature“ vypadal instalační manager tak, jak již bylo prezentováno. Jedinou změnou bylo, že některé údaje nebylo potřeba vyplňovat, jelikož byly nakonfigurovány pomocí instalace prvních dvou komponent.

I v případě instalace Web console došlo automaticky ke kontrole, zda server splňuje všechny požadavky. Nejzásadnější úpravou bylo nastavit serveru roli IIS (Internet Information Services), která vytvoří softwarový webový server a zajistí podporu protokolů HTTP, HTTPS, FTP, aj. Role serveru se přidává přes Server manager.

*Obrázek 14 - Přidání rolí přes Server manager*

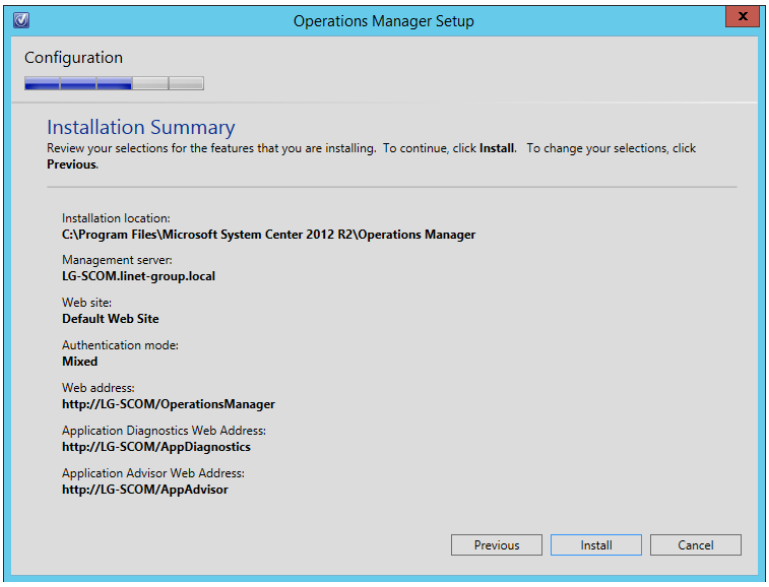



*Zdroj: vlastní zpracování*

Jakmile byla serveru přidána role IIS, bylo potřeba ještě zvolit funkce, které mají být doinstalovány. Seznam všech potřebných funkcí byl zobrazen v instalačním manageru. Po zvolení těch správných funkcí mohl uživatel kliknout na tlačítko „Verify Prerequisites Again“, které zajistilo opětovnou kontrolu požadavků SCOM na server. V případě, že ještě nějaká role scházela, instalační manager uvedl přesný postup, jak tuto chybějící roli přidat.

V dalších krocích bylo potřeba definovat internetovou adresu, ze které bude web console přístupná. Předdefinovaná adresa se skládá z názvu serveru a textu „operationsManager“. Na konci instalace jsou opět shrnuty všechny nejzásadnější informace o instalaci.

*Obrázek 15 - Web console - souhrn informací*




*Zdroj: vlastní zpracování*

Po úspěšné instalaci se autor pokusil otevřít webovou adresu http://LG-SCOM/operationsManager, na které je dostupná webová console, ale kvůli aplikaci Microsoft Silverlight mu to nebylo umožněno. Při přihlašování se zobrazila chybová hláška, že tato aplikace není nainstalovaná, ač nainstalovaná byla. Reinstalace Microsoft Silverlight nepomohla, proto bylo nutné najít chybu jinde.

Aby aplikace Silverlight mohla být na serveru spuštěna, bylo jí potřeba správně nakonfigurovat pro IIS. Pro konfiguraci bylo využito příkazu „inetmgr“ a následně byla vybrána ikona MIME Types, kde bylo zkontrolováno, zda jsou asociovány správné koncovky. Jednalo se o koncovky .svc, .xaml, .xap a .xbap.

Po nastavení koncovek bylo potřeba nastavit ASP.NET a povolit službu pro IIS. K tomu slouží v příkazovém řádku příkaz „aspnet_regiis /i“. V příkazovém řádku bylo dále potřeba provést příkaz „ServiceModelReg.exe /i“ ve složce c:\Windows\Microsoft.NET\Framework\v3.0\Windows Communication Foundation. Tento příkaz doinstaluje několik protokolů a definitivně povolí pro IIS publikovat a spouštět aplikaci Silverlight.

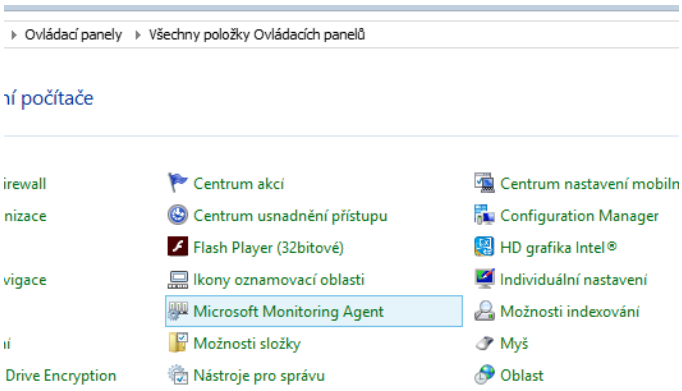
### 4.2.3. Instalace Agenta na koncových zařízeních

Existují dva způsoby, jak nainstalovat agenta pro sběr informací na koncových zařízeních. Jedním způsobem je ruční instalace na konkrétních zařízeních, druhá možnost je, že se agent nainstaluje na všechna zařízení, která se definují přímo v managementu SCOM.

Jelikož má společnost, ve které se SCOM zavádí, přes 600 zařízení po celém světě, tak autor zvolil v průběhu zkušebního provozu ruční instalaci na několika vybraných zařízeních. Instalační soubory jsou součástí ISO souboru s instalací celého SCOM, které stačí zkopírovat a spustit instalaci. V průběhu instalace bylo potřeba správně zadat údaje s názvem serveru pro správu, název skupiny pro správu a port serveru pro správu, kterým se k managementu má agent připojit. Dále bylo vyžadováno uvedení uživatelského účtu, který bude používat agent při provádění akcí požadovaných serverem pro správu. Zde bylo na výběr, aby se použil místní systémový účet nebo doménový účet.

Poté, co je agent nainstalovaný, tak ho uživatelé nenajdou, stejně jako ostatní nainstalované programy, v programech a funkcích, ale jeho zástupce je přímo v ovládacích panelech počítače pod názvem Microsoft Monitoring Agent.

*Obrázek 16 - nainstalovaný agent na počítači*




*Zdroj: vlastní zpracování*

## 4.3. První spuštění a konfigurace SCOM

Při prvním spuštění se zobrazí přehledný overview, který znázorňuje kroky, které jsou potřeba splnit pro správné fungování monitoringu, akce, které může administrátor vyvolat a také stručný přehled počtu zdravých monitorovaných zařízení, zařízení s kritickou chybou, neznámým stavem nebo s upozorněním. Dále jsou dostupné odkazy na návody a online zdroje.

Po prvním spuštění bylo pro správnou funkčnost SCOM potřeba:

- Nakonfigurovat počítače a zařízení pro monitoring
- Importovat management packs
- Povolit a nastavit notifikační kanál
- Upgradovat na plnou verzi

### 4.3.1. Import management packs

Po prvním spuštění bylo potřeba, aby byly importovány management packs, které slouží k specifikaci všech instrukcí pro SCOM agenta. Tento soubor se může importovat jako prosté XML nebo jako zabezpečený balíček. Výhodou XML souboru je, že v něm může administrátor provést změny a ovlivnit tak chování management pack. Management pack zpravidla obsahuje:

- Definici tříd
- Definici monitorů
- Definici úkolů
- Definici pravidel

- Reporty
- Definici pohledů
- Znalostní databázi, která se vztahuje k monitorům a pravidlům[30]

V nainstalovaném SCOM autor importoval management packs z katalogu, který SCOM nabízí. Celý proces stažení jednotlivých balíčků, ověření a instalace trval více než hodinu.

Jednotlivé MP jsou vytvářeny přímo i výrobci zařízení, takže lze stáhnout a importovat MP pro hardware, který je ve firmě nasazen. Další možností je, nechat si vyrobit MP na míru.

### 4.3.2. Přidání monitorovaného zařízení

Aby SCOM měl přístup na všechna zařízení, bylo potřeba povolit určité porty, jejichž seznam je uveden v tabulce 1.

*Tabulka 2 - seznam potřebných portů*

| Feature | Exception | Port and protocol |
|---|---|---|
| Management server | • System Center Management service<br>• System Center Data Access service<br>• Operations Manager Connector Framework<br>• Operations Manager Customer Experience Improvement<br>• Operations Manager Application Error Monitoring | 5723/TCP<br>5724/TCP<br>51905/TCP<br>51907/TCP<br>51906/TCP |
| Web console | Operations Manager web console | Selected web site port/TCP |
| Web console, http | World Wide Web Services, http | 80/TCP |
| Web console, https | Secure World Wide Web Service, https | 443/TCP |
| Operational database | • SQL Server database server | 1433/TCP<br>1434/UDP |

[30] Dohled HW pomocí SCOM 2012 a MP třetích stran. *TechNet* [online]. [cit. 2016-01-15]. Dostupné z: https://blogs.technet.microsoft.com/technetczsk/2015/09/07/dohled-hw-pomoc-scom-2012-a-mp-tetch-stran-dell-hp-emc/

| | | |
|---|---|---|
| | • If using a named instance, add. | |
| Operations Manager data warehouse database | • SQL Server database server<br>• If using a named instance, add. | 1433/TCP<br><br>1434/UDP |
| Operations Manager Reporting | SQL Server Reporting Services | 80/TCP |
| Agent, manual installation of MOMAgent.msi | System Center Management service | 5723/TCP |
| Agent, push installation | • System Center Management service<br>• File and Print Sharing<br>• Remote Administration | 5723/TCP<br><br>137/UDP, 138/UDP, 139/TCP, 445/TCP<br><br>135/TCP, 445/TCP |
| Agent, pending repair | • System Center Management service<br>• File and Print Sharing<br>• Remote Administration | 5723/TCP<br><br>137/UPD, 138/UPD, 139/TCP, 445/TCP<br><br>135/TCP, 445/TCP |
| Agent, pending upgrade | • System Center Management service<br>• File and Print Sharing<br>• Remote Administration | 5723/TCP<br><br>137/UDP, 138/UDP, 139/TCP, 445/TCP<br><br>135/TCP, 445/TCP |
| Gateway | System Center Management service | 5723/TCP |
| Operations Manager Audit Collection Services database | • SQL Server<br>• If using a named instance, add. | 1433/TCP<br><br>1434/UDP |
| Operations Manager Audit Collection Services Collector | ACS Collector Service | 51909/TCP |

*Zdroj: Preparing your environment for System Center 2012 R2 Operations Manager. Microsoft System Center. [online]. 11.5.2015 [cit. 2016-01-18]. Dostupné z: https://technet.microsoft.com/en-us/library/dn249696.aspx*

Zařízení, která se mají monitorovat, se přidávají pomocí průvodce, který lze spustit v menu Administration – Discovery Wizard. Po jeho spuštění je nutné, aby administrátor určil, zda se mají monitorovat počítače s operačním systémem Windows, Unix/Linux nebo síťová zařízení. Po zvolení požadované možnosti bylo potřeba nastavit, zda se mají vyhledávat počítače v rámci domény automaticky nebo administrátor musí ve druhém kroku

definovat, zda vyhledávat počítače a servery nebo pouze počítače či pouze servery. V případě vyhledávání zařízení pomocí této rozšířené metody lze specifikovat doménu, ve které se zařízení mají vyhledávat a dále je možno konfigurovat konkrétní OU v rámci Active Directory.

V dalším kroku je potřeba zadat kredence k administrátorskému účtu, pomocí kterého budou nainstalováni agenti v počítačích, kde nebyli nainstalováni ručně. Daný účet musí mít administrátorská oprávnění na všech počítačích, na kterých se má agent nainstalovat.

Poté, co průvodce provede vyhledávání, zobrazí seznam, ve kterém je zobrazeno jméno počítače a jeho doména. U každého počítače je checkbox, který může administrátor zaškrtnout a tím přidat daný počítač do monitoringu. Pokud byly vybrány všechny požadované počítače, kliknutím na tlačítko Next dojde k nainstalování agenta na vybraných počítačích a následné přidání počítače do monitoringu.

Vyhledávací průvodce je možno spustit kdykoliv je potřeba.

### 4.3.3. Nastavení notifikací

Užitečný dohledový systém musí být schopný zaslat v případě výskytu upozornění nebo chyby notifikaci administrátorům. SCOM umožňuje zasílat notifikace prostřednictvím SMS zprávy, emailu, IM a příkazové řádky.

Nastavení se provádí v několika krocích v administraci SCOM. Pod záložkou Notifications jsou zde tři úrovně nastavení: kanál, příjemce a akce která vyvolá notifikaci.

Jednotlivé formy kontaktování se nastavují v první možnosti – kanálech. Nastavují se zde informace, které mají být prostřednictvím daného kanálu (SMS, email, IM a příkazová řádka) zaslány. Dále se nastavují informace k připojení na SMTP, SIP nebo ke spuštění příkazové řádky. Notifikační kanály lze libovolně pojmenovat.

Druhým krokem je nastavení příjemců. Příjemci se nastavují v záložce Subscribers, kde se pro každého příjemce definují časy, ve kterých mu budou notifikace zasílány. Standardně je předvoleno, že se upozornění zasílají 24 hodin denně, ale toto lze změnit a nastavit, aby se zprávy zasílaly:

- V intervalu podle kalendáře (např. od 1. 12. 2015 do 31. 8. 2016)
- Každý den v určeném časovém intervalu (od 6:00 do 18:00 mimo 11:30 – 12:00)

- V konkrétní dny (a také nastavit konkrétní hodiny v konkrétních dnech)

Uvedené nastavení lze použít například v případě, kdy IT oddělení zajišťuje podporu pro dceřiné společnosti rozmístěné po světě a kvůli časovému posunu drží vždy některý z administrátorů pohotovost. Snadno tak lze nastavit, že budou notifikace zasílány pouze administrátorovi, který má službu a nebudou rušit ty, kteří mají dovolenou nebo mají po pracovní době.

Poslední akce, kterou je potřeba pro správné zasílání notifikací udělat, je provést nastavení v záložce subscriptions. Zde se v prvním kroku nastaví podmínka, která musí být splněna, aby byla notifikace zaslána. Při nastavení je možno zvolit více podmínek a zadat u nich kritéria, která vedou k odeslání notifikace. V dalším kroku se zvolí příjemci.

Vzhledem k tomu, že mohou být pro každou akci zvolení různí příjemci, můžou být notifikace zaslány vždy pouze tomu, kdo se o sledované zařízení stará a ví, co a jak má opravit. Předejde se tak zbytečnému zdržení při hledání správného řešitele problému.

V dalším kroku je ještě nutné zvolit kanály, kterými má být administrátor upozorněn. Může být vybráno i více kanálů (např. SMS a email). Po potvrzení nastavení začal fungovat notifikační kanál a v případě objevení kritických událostí se zasílá administrátorům notifikace.

*Tabulka 3 - výchozí nastavení informací v notifikacích*

| **Typ upozornění** | **Defaultní formát** |
|---|---|
| E-mail | Subject:<br>Alert: *název události*<br>Resolution state: *new* nebo *closed*<br>Alert:<br>Source:<br>Path:<br>Last modified by:<br>Last modified time:<br>Alert description: |

| | |
|---|---|
| | Alert view link:<br>Notification subscription ID generating this message: |
| Instant Message | Alert: *název události*<br>Path: odkaz na událost<br>Resolution state: *new* nebo *closed*<br>Last modified by: |
| SMS | Alert: *název události*<br>Resolution state: *new* nebo *closed* |

*Zdroj: How to Customize Message Content for Notifications.* Microsoft TechNet *[online]. [cit. 2016-01-13]. Dostupné z: https://technet.microsoft.com/en-gb/library/hh212698.aspx*

### 4.3.4. Nastavení SMS notifikací

Aby mohly být SMS zprávy zasílány, je potřeba, aby byl nastaven GSM modem a aby byla do něj vložena SIM karta. Nákup nového modemu řešen být nemusel, protože SMS notifikace již firma používá standardně i pro jiné systémy.

Na serveru SCOM byl nainstalován program pro zasílání SMS zpráv. Na základě dobrých zkušeností z minulosti byl nainstalován program Microsoft SMS Sender. Tento program zprostředkuje předání notifikace ze systému SCOM do GSM modemu, který zašle potřebná upozornění.

## 4.4. Web console

Rozložení web console je totožné s celým SCOM manažerem, ale není zde umožněno provádět jakákoliv nastavení. Celá konzole slouží výhradně k sledování zdraví IT infrastruktury. Při prvním spuštění se zobrazí hláška, že musí být SilverLight nastaven. Během instalace byl do počítače nahrán i EXE soubor, který se po potvrzení této hlášky spustí a provede nastavení v registrech, aby mohla být konzole korektně spuštěna.

Ve výchozím nastavení bylo nastaveno, že aktivní session vyprší po 30 minutách a administrátor se bude muset znovu přihlásit. Chtěným stavem ale bylo, aby měli administrátoři konzoli spuštěnou v jedné ze záložek internetového prohlížeče a kdykoliv v případě potřeby se do ní mohli podívat.

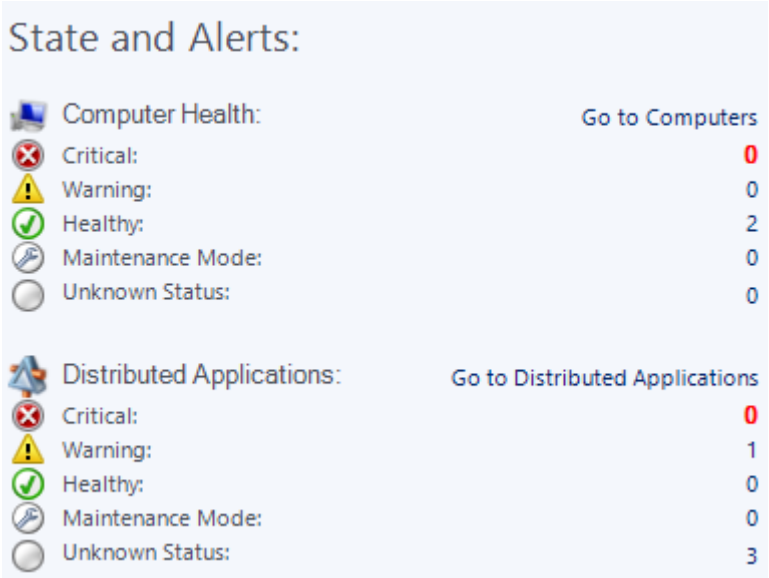
Pomocí souboru web.confg, který je dostupný v umístění „Program Files\System Center Operations Manager 2012\WebConsole\WebHost" lze toto nastavení změnit. V tomto souboru je limit nastaven pomocí příkazu <connection autoSignIn="true" autoSignOutInterval="30">. Aby bylo automatické odhlášení disablováno, byla změněna hodnota z 30 na 0, což vypne automatické odhlášení z web concole.

Ve výchozím stavu byla webová stránka http://lg-scom/OperationsManager přístupná pouze ze serveru, na kterém je SCOM nainstalován. Došlo tedy k publikování stránky pro celou síť firmy, aby byla dostupná z jakéhokoliv počítače v rámci firmy.

## 4.5. Dohled zařízení

Přehled o monitorovaných zařízeních je možný ze záložky Monitoring a je přístupný jak přes webovou consoli, tak i přes management SCOM. V úvodním dashboardu je přehled stavů a upozornění všech zařízení, která jsou pomocí SCOM monitorovány.

*Obrázek 17 - Dashboard*




*Zdroj: vlastní zpracování*

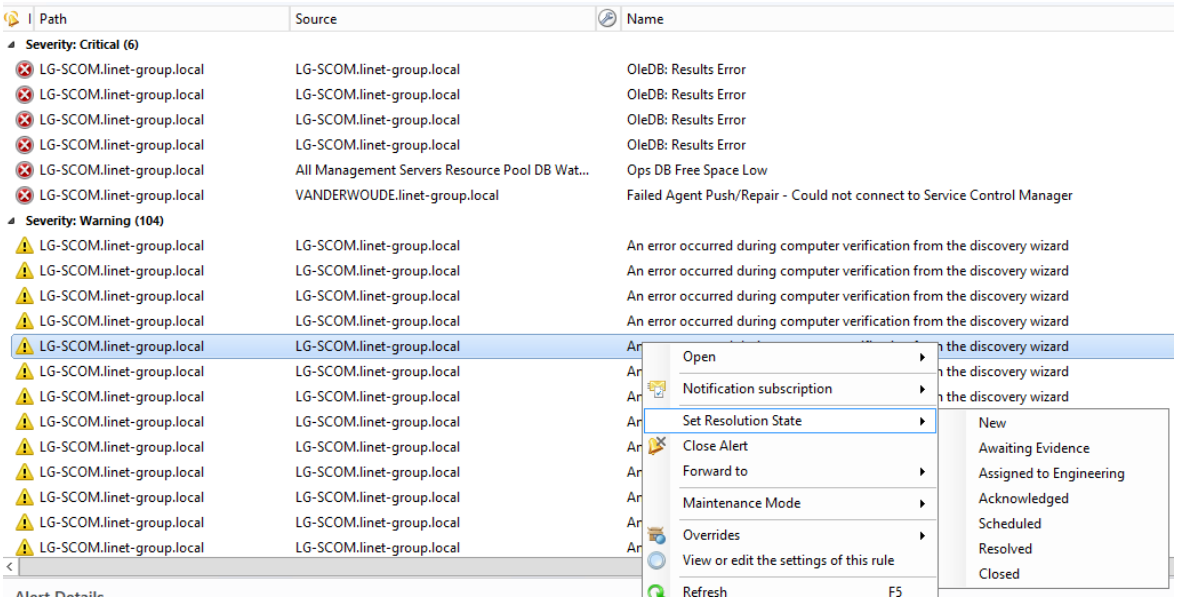
Detailnější výpis je k dispozici při kliknutí na tlačítko „Go to Computers" ohledně monitorovaných počítačů a serverů a „Go to Distributed Applications" ohledně monitorování stavu aplikací. V autorově případě mezi neznámé zařízení patřil ConfigMgr, Service Manager a Microsoft AD RMS Service. Uvedené varování se týkalo Operations

Manager Management Group. Po přechodu k detailnějšímu výpisu těchto aplikací bylo možno zobrazit alert view, diagram view, event. view a performance view.

### 4.5.1. Alert View

V tomto zobrazení byl uveden seznam veškerých alertů, které vyvstaly během činnosti dohledového systému. Jsou přehledně seřazeny podle závažnosti – kritické a varování. Po zvolení libovolného záznamu byl ve spodní části obrazovky zobrazen podrobný detail dané chyby nebo upozornění. Ve sloupcích byly uvedeny informace o zdroji chyby, názvu chyby, stavu řešení tohoto upozornění a jak je upozornění staré. Administrátor měl možnost upozornění ručně přejmenovat, změnit stav řešení z New na: awaiting evidence, assigned to engineering, acknowledged, sheduled, resolved a closed, což usnadňuje orientaci při řešení problémů a mimo další mohl také upravit pravidlo pro sledování daného chování.

*Obrázek 18 - Alert View*



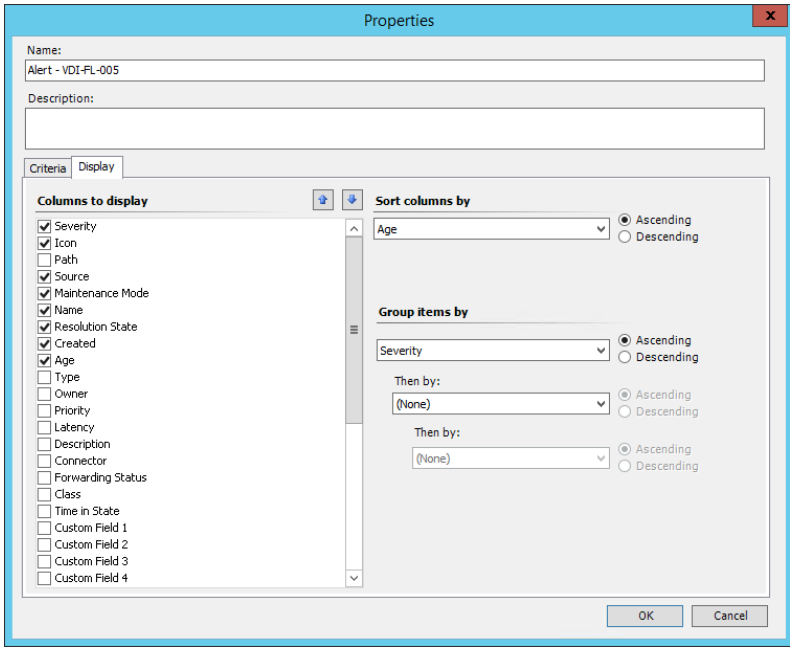

*Zdroj: vlastní zpracování*

Pro administrátora bylo k dispozici také přepnutí do maintenance mode. Při této volbě bylo nutné zvolit, zda se má do tohoto módu přepnout pouze zvolený objekt nebo i objekt se všemi dalšími objekty, které obsahuje. Bylo možno přidat komentář a naplánovat, jak dlouho bude objekt v tomto módu. Přepnutí do maintenance mode způsobilo, že byly dočasně pozastaveny pravidla pro sledování, notifikace, alerty, změny stavů a automatické odpovědi.

Poté, co administrátor otevřel okno Alert Properties, měl zde k dispozici na první záložce podrobné shrnutí problému, kde může přiřadit oproti AD i řešitele problému. Toto okno ale obsahovalo další záložky, které velice usnadňují řešení daných problémů. Mezi tyto záložky patří Product knowledge, Company knowledge a history. V první z těchto záložek jsou shrnuty informace k zobrazené chybě. Company knowledge je ale ve formě textového pole a administrátor tak může uvést veškeré kroky, které vedou k vyřešení problému. V praxi to znamená, že pokud je to náročnější problém, tak nad jeho řešením pracovníci můžou strávit i několik hodin. Poté ale, co tento problém vyřeší, tak ho podrobně popíší v této záložce a ve chvíli, kdy se problém objeví znovu, tak pomocí tohoto popisu problém vyřeší podstatně rychleji.

Vytvoření vlastního alert view provedl autor v záložce My Workspace, kde kliknutím pravého tlačítka v poli My Workspace zvolil vytvořit nový alert view. Prvním krokem bylo pojmenovat tento view. Autor zvolil, že veškeré vlastní monitoringy pojmenuje ve formě „typ monitoringu – název monitorovaného objektu“ V tomto případě chtěl vytvořit alert view pro virtuální stroj s názvem VDI FL 005, název tohoto monitoringu tedy zvolil jako „alert – VDI-FL-005“.

*Obrázek 19 - možnosti zobrazení Alert View*



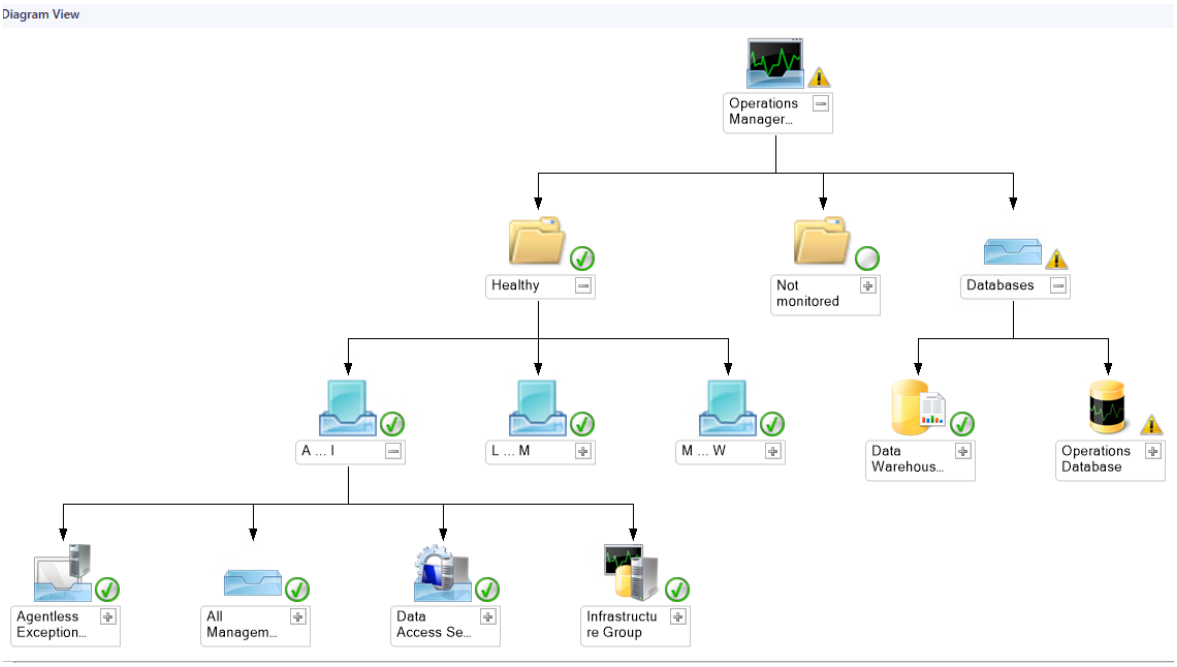

*Zdroj: vlastní zpracování*

Volitelný popis nebyl vyplněn, ale v záložce criteria bylo zvoleno, aby byly zobrazeny veškeré upozornění pro výše zmíněný virtuální počítač. Tyto kritéria lze kdykoliv v budoucnu upravit, přidat nová kritéria nebo zvolit, aby se upozornění vyhledávaly např. pro počítače s operačním systémem Windows 7. Druhá záložka Display slouží k úpravě zobrazovaných informací a k nastavení výchozího řazení výsledků. Vzhledem k tomu, že monitorovaný stroj nehlásí žádný problém, byl alert view po vytvoření prázdný.

### 4.5.2. Diagram View

Tento pohled znázorňuje strukturu prostředí v grafické formě. Celá struktura je zobrazena pomocí stromu, kde na vrchu je samotný Operations manager a postupným rozbalováním větví jsou zobrazeny až koncové monitorované stanice.

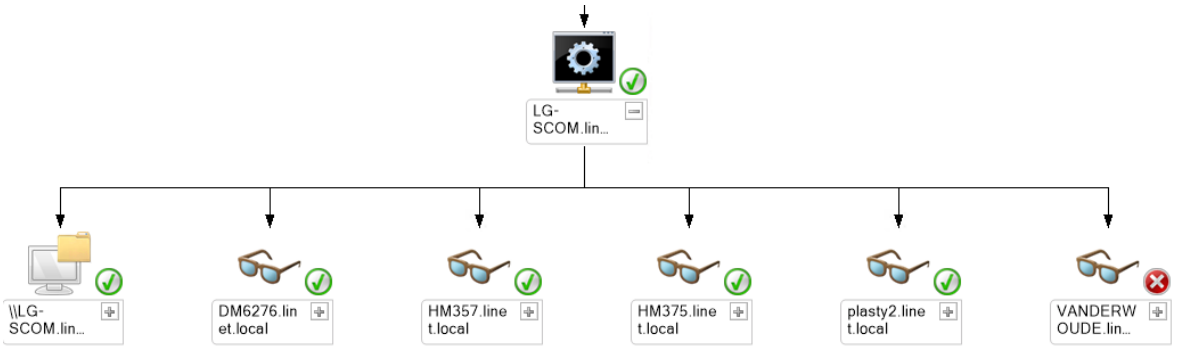
*Obrázek 20 - Diagram view*




*Zdroj: vlastní zpracování*

U každého uzlu je ikonka stavu monitorování objektu. Zelená fajfka značí, že objekt je v pořádku. Červený křížek sděluje, že objekt obsahuje nějakou vážnou chybu, žlutý vykřičník značí upozornění (například, že dochází místo na disku, ale objekt je jinak zdravý) a zelené kolečko, že objekt není monitorován.

*Obrázek 21 - Koncové stanice zobrazené pomocí Diagram View*




*Zdroj: vlastní zpracování*

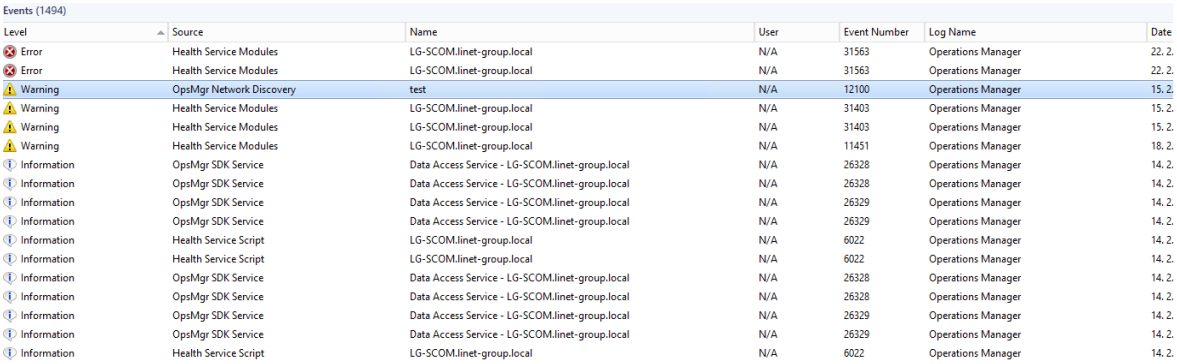
Vlastní diagram view autor vytvořil v záložce My Workspace, kde klikl pravým tlačítkem a zvolil nový diagram view. V dalším kroku bylo potřeba tento diagram view pojmenovat a volitelně doplnit popis. Dále bylo potřeba vybrat správný monitorovaný objekt pomocí tlačítka Browse u pole Choose Target. Vzhledem k tomu, že template ještě nebyl žádný definovaný, bylo potřeba template definovat. To znamená, že bylo potřeba zvolit, kolik úrovní monitorovaného objektu má být zobrazováno, jak má být graf orientován (odkud kam). V záložce line properties mohla být upravena barva, styl a tloušťka čar znázorňujících v grafu vztahy mezi objekty a mimo jiné bylo možné definovat virtuální skupinu.

Toto nastavení lze kdykoliv měnit a graf si tak uzpůsobit pro získání požadovaných výsledků.

### 4.5.3. Event View

V překladu se jedná o protokol událostí, který je dostupný i na běžných počítačích. Celý výpis je, stejně jako u alert view, přehledně rozdělený do několika sloupců. První sloupec obsahuje informaci o tom, zda se jedná o informaci, varování nebo chybu. V dalších sloupcích je uveden zdroj, název, číslo události a datum vytvoření události.

*Obrázek 22 - Event View*



Events (1494)

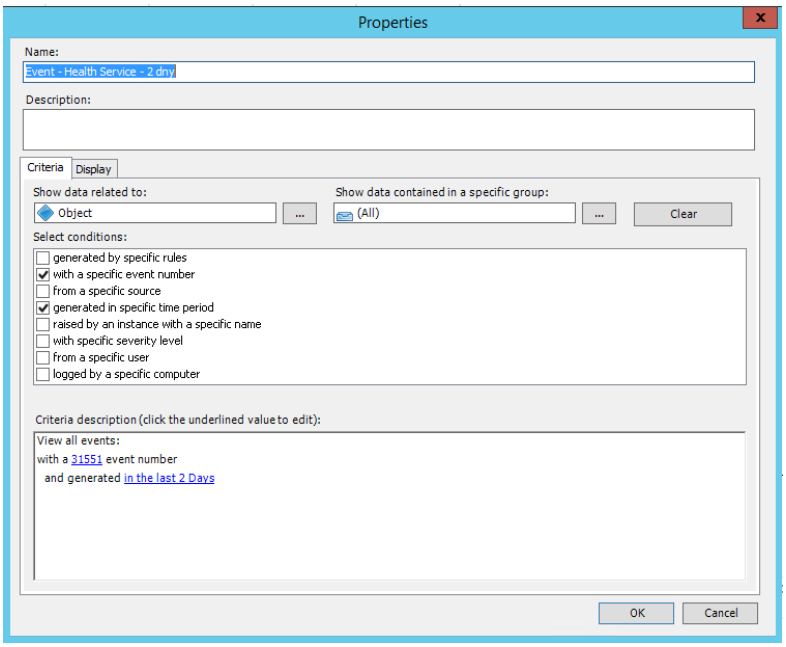
| Level | Source | Name | User | Event Number | Log Name | Date |
|---|---|---|---|---|---|---|
| Error | Health Service Modules | LG-SCOM.linet-group.local | N/A | 31563 | Operations Manager | 22. 2. |
| Error | Health Service Modules | LG-SCOM.linet-group.local | N/A | 31563 | Operations Manager | 22. 2. |
| Warning | OpsMgr Network Discovery | test | N/A | 12100 | Operations Manager | 15. 2. |
| Warning | Health Service Modules | LG-SCOM.linet-group.local | N/A | 31403 | Operations Manager | 15. 2. |
| Warning | Health Service Modules | LG-SCOM.linet-group.local | N/A | 31403 | Operations Manager | 15. 2. |
| Warning | Health Service Modules | LG-SCOM.linet-group.local | N/A | 11451 | Operations Manager | 18. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26328 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26328 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26329 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26329 | Operations Manager | 14. 2. |
| Information | Health Service Script | LG-SCOM.linet-group.local | N/A | 6022 | Operations Manager | 14. 2. |
| Information | Health Service Script | LG-SCOM.linet-group.local | N/A | 6022 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26328 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26328 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26329 | Operations Manager | 14. 2. |
| Information | OpsMgr SDK Service | Data Access Service - LG-SCOM.linet-group.local | N/A | 26329 | Operations Manager | 14. 2. |
| Information | Health Service Script | LG-SCOM.linet-group.local | N/A | 6022 | Operations Manager | 14. 2. |

*Zdroj: vlastní zpracování*

Poté, co je libovolná událost označena, zobrazí se v dolní části obrazovky její detailní popis. Vzhledem k tomu, že se jedná o výpis událostí a ne o alert, není zde možnost jednotlivé události přiřazovat řešitelům nebo měnit jejich stavy. Administrátorovi je u událostí umožněno spustit a prohlížet veřejnou i firemní znalostní databázi a případně pozastavit nebo změnit pravidla události.

Vytvoření vlastního protokolu událostí se opět provádí v záložce My Workspace. Vzhledem k tomu, že autor při prohlížení celého Event logu zjistil, že dochází k chybě v modulu Health Service, rozhodl se, že vlastní Event View bude obsahovat výpis právě těchto chyb za poslední 2 dny.

*Obrázek 23 - Event View Gealth Service*




*Zdroj: vlastní zpracování*

Parametry tedy zvolil tak, že jsou sledovány všechny události s ID 31551 a výběr je omezen na poslední 2 dny. ID události bylo zjištěno v úplném výpisu událostí, kde je pro každou událost v detailním popisu zobrazeno. Po uložení vlastního zobrazení protokolu událostí byly zobrazeny celkově 4 chyby.

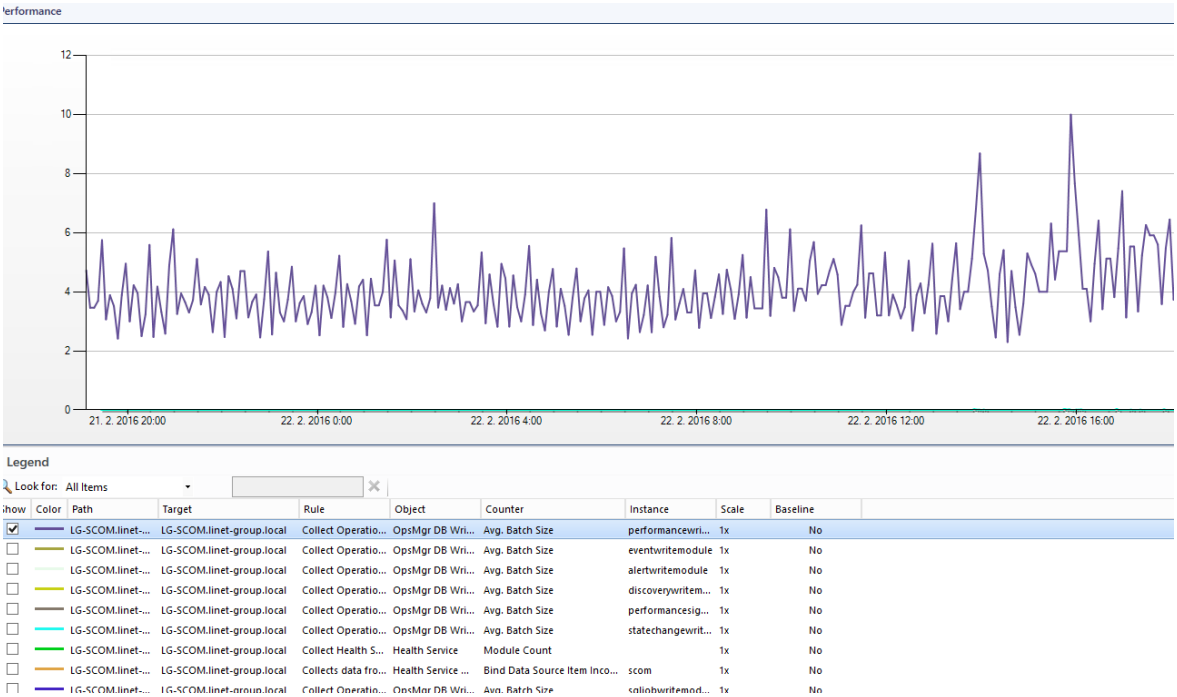
### 4.5.4. Performance View

Přehled výkonu jednotlivých počítačů a serverů znázorňuje Performance view. Správci zde mohou zobrazovat aktuální i uložená historická data. V legendě pod grafem je možnost vybrat, co bude na grafu zobrazeno. Správci sítě tak mohou porovnávat několik pohledů mezi sebou. V legendě jsou informace o barvě, zdroji, sledovaném pravidle, objektu, počítadle atd.

Mimo jiné lze u jednotlivých řádků měnit barvu a měřítko pro daný zdroj. Pomocí tohoto nastavení si mohou IT zaměstnanci zpřehlednit graf.

Výsledný graf lze jednoduše exportovat nebo uložit a může být použit na různých poradách jako podkladový materiál pro řešení eventuálních problémů.

*Obrázek 24 - Performance View*




*Zdroj: vlastní zpracování*

## 4.6. Monitoring switche

SCOM umožňuje monitoring nejen koncových stanic, ale i fyzických síťových routerů a switchů. V případě monitoringu switche sleduje zdraví připojení, VLAN, HSRP a i jednotlivé porty. Pro monitorování switche bylo potřeba spustit průvodce pro vyhledání zařízení, ve kterém se zvolila možnost „Síťová zařízení".

Dále bylo nutné nastavit název a určit management server, ze kterého bude monitoring spuštěn. V tomto případě to byl server SCOM.linet-group.local a dále bylo nutné vybrat management pool. Pool může obsahovat jeden nebo více serverů pro správu a v případě selhání služeb jednoho z těchto serverů, jsou pomocí SCOM serveru přesměrovány na jiný pool.

V dalším kroku průvodce bylo nutné nastavit typ vyhledávání. Bylo zde na výběr explicitní vyhledávání a rekurzivní vyhledávání.

- Explicitní vyhledávání: zjišťuje pouze ta zařízení, u kterých je specifikována IP adresa nebo úplný název domény. Pomocí tohoto pravidla probíhá monitoring přes SNMP nebo ICMP.
- Rekurzivní vyhledávání: vyhledává zařízení specifikovaná v průvodci podle IP adresy, ale i další síťová zařízení, která jsou připojena na zadanou SNMP.

V autorově případě byla zvolena explicitní metoda. V případě, že by bylo zvoleno rekurzivní vyhledávání, bylo by potřeba ještě nastavit filtry, zda vyhledávat všechna připojená zařízení v rámci zvoleného IP rozsahu nebo zda vynechat zařízení s konkrétním jménem nebo IP adresou.

Výchozí účet autor vytvořil nový, který byl typu Spustit jako. Poté se průvodce přepnul do okna, ve kterém bylo nutno specifikovat IP adresu nebo název zařízení. V rámci struktury firmy bylo nutné povolit na Fortigate pro SCOM komunikaci prostřednictvím SNMP, který autor zvolil pro monitoring síťových zařízení. Tímto byl nastaven monitoring switche.

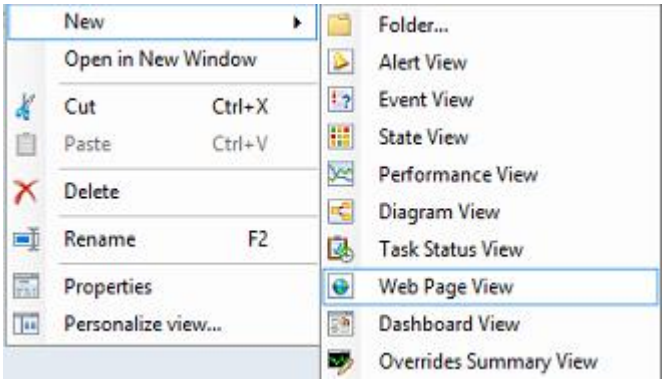
## 4.7. Úprava konzole

Celá úprava slouží k tomu, aby zobrazované informace byly snadno dohledatelné a aby byly zobrazeny vždy ty správné. Každému může vyhovovat něco jiného, ale v záložce My Workspace si může každý uživatel nástroje SCOM upravit vše, co se mu bude zobrazovat.

V této práci bylo popsáno vytvoření vlastních pohledů. Všechny tyto pohledy jsou automaticky přidány do levého panelu v záložce My Workspace. Pro přehlednost lze vytvořit nové složky a jednotlivé reporty do nich roztřídit.

Mimo již představené pohledy typu Alert view, Event View a tak dále, lze vytvořit State View, Task Status View, Web Page View, Dashboard View a Overrides Summary View.

*Obrázek 25 - možnosti přidání pohledů do My Workspace*




*Zdroj: vlastní zpracování*

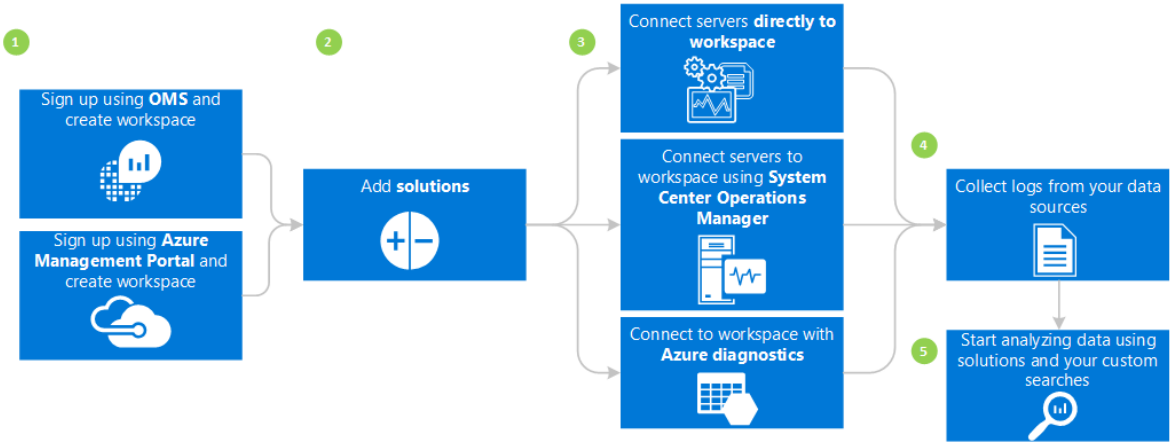
V záložce My Workspace lze také uložit různá hledání pro budoucí použití. Při nastavování vyhledávání lze specifikovat, zda se mají vyhledávat objekty typů Alerts, Events, Rules, atd.

### 4.7.1. OMS Mobile Apps

Správci sítě ve vybrané firmě mají k dispozici služební mobily, takže bylo požadováno, aby měli přístup k monitoringu i prostřednictvím tohoto zařízení. Microsoft bohužel vlastní mobilní aplikaci pro nástroj SCOM nemá, ale umožňuje propojit monitoring se svou jinou aplikací Microsoft OMS.

Tato aplikace je dostupná uživatelům, kteří používají zařízení Android a iOS. Po nainstalování do mobilu se bylo potřeba registrovat nebo přihlásit pomocí Microsoft účtu.

*Obrázek 26 - proces spojení aplikace s SCOM*




*Zdroj: Onboard in minutes. TechNet [online]. 2015 [cit. 2016-01-07]. Dostupné z: https://technet.microsoft.com/library/mt484118.aspx*

Poté, co se uživatel registruje, je potřeba aplikaci propojit přímo s SCOM. Propojení lze nastavit přímo v SCOM, kde je možnost Register to Operational Insights. Poté byly přidány skupiny monitorovaných objektů a tím byla aplikace propojena s SCOM.

V rámci aplikace byly nastaveny některé dashboardy, pomocí kterých byly zobrazeny informace o monitorovaných zařízeních. Aplikace dále umožňuje pomocí příkazů libovolnou úpravu toho, co má být zobrazeno.

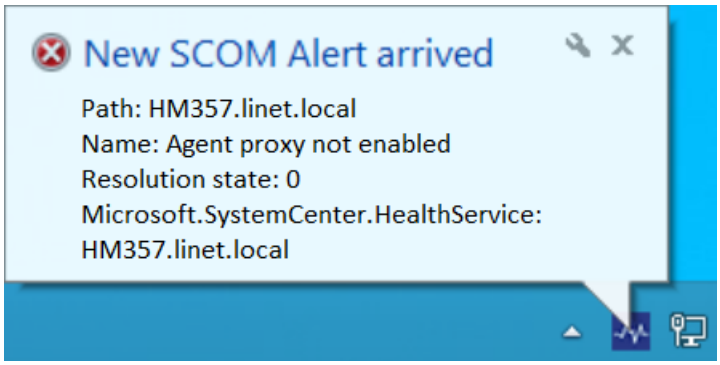
### 4.7.2. SCOM Tray Notification Tool

Dalším vylepšením a usnadněním práce administrátorům byl notifikační nástroj v dolní liště počítače s názvem SCOM Tray Notification Tool - TNT. Jedná se o mini aplikaci, která byla nainstalována na počítače administrátorů a která zobrazovala každé upozornění z SCOM.

Během konfigurace byla zvolena správná Management skupina, a co vše má být zobrazeno (nové kritické události). Po otevření tohoto nástroje je administrátorům dostupná i historie upozornění.

Ve chvíli, kdy došlo k nějaké kritické chybě, správci sítě byli upozorněni nejen pomocí SMS zprávy a emailu, ale i pomocí zobrazené informace přímo z lišty svého vlastního počítače.

*Obrázek 27 - Tray Notification Tool*




*Zdroj: vlastní zpracování*

Aby byly notifikace zobrazovány, musí být počítač připojen do sítě uvnitř firmy nebo případně, pokud je mimo firmu, tak musí být připojen přes VPN.

# 5. Výsledky a diskuse

Společnost, ve které byl SCOM nasazen, má po celém světě 16 dceřiných společností, ale IT oddělení pouze v České republice, odkud se IT administrátoři starají o celou IT strukturu v rámci holdingu. V každé dceřiné společnosti je umístěn fortigate a server, ale většina databází, terminálových serverů a ostatních klíčových serverů je umístěna pouze v mateřské společnosti v České republice.

Doposud tato společnost používala pro monitoring svého prostředí několik navzájem nepropojených aplikací (auditpro, PRTG, Veem One a OCS), ale postupem času se začalo hledat řešení pro efektivní monitoring prostřednictvím jediné aplikace. Jako nejvhodnější (nejen z hlediska monitoringu, ale i usnadnění práce při instalacích počítačů a dalších hlediscích, které nabízejí produkty z rodiny produktů System Center) se jevilo a managementem bylo odsouhlaseno pořízení licence pro rodinu produktů System Center. Tato rodina obsahuje App Controller, Configuration Manager, Data Protection Manager, Endpoint Protection, Operations Manager, Orchestrator, Service Manager a Virtual Machine Manager. Pořízení této licence stálo cca 35 000,- Kč na 2 roky. Po zakoupení licence byl jako první nasazen produkt System Center Configuration Manager, který od samého začátku začal ulehčovat administrátorům práci při instalacích počítačů.

Po jeho nasazení byl jako další na řadě System Center Operations Manager, který by měl být využit pro efektivní monitoring celého prostředí. Od jeho nasazení si společnost slibuje zrychlení řešení výpadků IT zařízení a také předcházení těchto výpadků. V případě zastavení výroby se škoda pohybuje řádově v milionech korun za den. Z tohoto důvodu je snahou předcházet jakýmkoliv výpadkům a mít IT prostředí funkční.

V rámci této diplomové práce byl nainstalován produkt SCOM 2012 a do jeho monitoringu přidáno několik desítek testovacích koncových počítačů a notebooků uživatelů, kteří s tím byli seznámeni, 10 virtuálních serverů a 2 switche. Po celou dobu psaní této diplomové práce probíhal sběr informací prostřednictvím SCOM a v případě uměle i samovolně vytvořených kritických událostí na monitorovaných zařízeních byla zaslána notifikace nastavenému administrátorovi prostřednictvím SMS a emailu.

Do monitoringu nebylo zapojeno více zařízení z důvodu, že se jedná o celosvětovou firmu s téměř 900 zaměstnanci a 600 koncovými stanicemi a v případě, že by došlo k nějakému problému během tohoto testování, mohl by zastavit výrobu a způsobit vysoké škody. Až po důsledném otestování veškerých možností aplikace a jistotě, že se tento scénář

nevyplní, bude SCOM překlopen do ostrého provozu a do monitoringu budou přidány veškeré koncové stanice zaměstnanců, servery a switche.

Na základě získaných dat z PRTG monitoringu, který obsahuje časové údaje o zjištěném problému a jeho následném vyřešení, se reakceschopnost administrátorů po nasazení SCOM průměrně zrychlila o 20 minut v případě problémů se switchem, o 7 minut v případě problémů se serverem a při problémech s koncovými stanicemi uživatelů byla nezměněna. Výsledky musejí ale být brány s rezervou, jelikož po delším používání SCOM dojde k nasbírání většího počtu pozorování a po roce používání budou mít výsledky daleko větší váhu, než po 3 měsících testovacího provozu, kdy běžel monitoring jen na vybraných serverech a ostatních zařízeních.

## 5.1. Problémy, které byly řešeny pomocí SCOM

K nejzásadnějšímu problému, který nastal během testování, došlo jednou. Jednalo se o vytvoření smyčky u switche, kdy uživatelka omylem zapojila LAN kabel opět do zásuvky místo do notebooku. Vzhledem k tomu, že takto propojila dva různé switche, došlo k jejich zacyklení a ochranné mechanismy nezafungovaly korektně. Pomocí SCOM bylo zjištěno, o který switch se jedná a na kterém konkrétním portu je problém. Po fyzické kontrole pak došlo k odhalení příčiny a během 9 minut již opět vše fungovalo správně.

K podobnému problému došlo několikrát i před nasazením SCOM. Jakmile se objevil tento problém vůbec poprvé, znamenalo to, že administrátoři museli postupně odpojovat jednotlivé switche a takto neefektivně zjišťovat, kde vzniká problém. Celé řešení trvalo přibližně 45 minut. Po této zkušenosti bylo vytvořeno nápravné opatření a byl vytvořen monitoring těchto zařízení za pomocí PRTG.

Jakmile se objevil daný problém znovu, měli již administrátoři informace o tom, kde mají chybu hledat. Nebylo ale možné zjistit konkrétní port a tak řešení pouze za pomocí PRTG monitoringu trvalo 30 minut.

Monitoring jednotlivých portů switche pomocí System Center Operations Manager není nastaven automaticky, ale administrátor musí provést nastavení pro každé zařízení zvlášť.

SCOM odhalil také problémy na terminálovém serveru, na kterém došlo k nečekanému zastavení služeb, a uživatelé se nemohli připojit do informačního systému. Vzhledem k správnému nastavení monitoringu a notifikací věděli o tomto problému administrátoři ještě před tím, než začali uživatelé volat a psát na podporu, že se nemohou přihlásit do informačního systému.

Čas řešení problémů na koncových stanicích se nezměnil. V konkrétním případě bylo dohledovým systémem hlášeno, že uživateli dochází místo na disku. Do tohoto problému nebylo administrátory zasahováno a uživatel si disk pročistil sám. I agenti nainstalovaní na koncových počítačích ale mají smysl. Ve firmě byla aktuální otázka reinstalace zbývajících počítačů s Windows XP na podstatně novější Windows 7 nebo Windows 8.1 (záleží na počítači a dostupných ovladačích pro konkrétní systémy). Pomocí SCOM byl vytvořen report o počítačích, na kterých je nainstalovaný tento starý systém a dále se řešila jejich reinstalace nebo obměna.

Podobný report byl vytvořen i pro počítače, které obsahují starší Office, než je verze 2013. Zde však nedocházelo k ruční reinstalaci, ale bylo využito System Center Configurations Manager a do počítačů se starší verzí Office byl zaslán instalační balíček pro Microsoft Office 2013 a upgrade proběhl zcela automaticky při restartování počítače.

Po uvedení SCOM do ostrého provozu by měly být postupně převedeny veškeré monitorované služby a stavy z ostatních běžících monitorovacích systémů do SCOM a ostatní v současné chvíli běžící monitorovací systémy by následně měly být ukončeny. Zde však autor doporučuje, aby po dobu minimálně 6 měsíců fungovaly všechny dohledové systémy zároveň a až po vyhodnocení, zda během této doby SCOM zaznamenal stejné události, jako ostatní systémy, tak poté teprve ostatní dohledové systémy ukončit. Ničemu nevadí, když budou po omezenou dobu fungovat všechny dohledové systémy najednou, ale ve chvíli, kdy by ostatní systémy byly ukončeny předčasně a až poté se zjistilo, že pomocí SCOM nebyly zjištěny některé kritické události, mohlo by být už pozdě.

Po uplynutí přechodné doby dojde k sjednocení monitoringu do jednoho systému. Tato změna ulehčí práci administrátorům, jelikož nebudou muset přemýšlet, kde jaké informace najdou, ale tyto informace budou mít přístupné vždy v rámci jedné monitorovací aplikace – System Center Operations Manager.

Při dalším rozvíjení SCOM je nutné přidat společně s externím konzultantem do monitoringu také napájení záložních napájecích zdrojů. Firma má velice dobře vyřešené zálohování napájení, jelikož v minulosti zakoupila diesel agregát, který se v případě výpadku elektrického proudu spustí a napájí všechny servery, switche a další systémy. Spuštění agregátu trvá ale přibližně 1 minutu a po tuto dobu musí být napájeny servery a switche pomocí UPS. Monitoring by tedy měl obsahovat i informace o jednotlivých UPS, zda jsou schopné po tuto dobu bezpečně napájet tato síťová zařízení.

Poté, co bude mít firma vyřešen monitoring veškerých klíčových zařízení, mohou být do monitoringu přidány i projektory v zasedacích místnostech. Pomocí tohoto monitoringu se administrátoři dozvědí ihned, že se v projektoru rozbila lampa nebo že projektor nebyl vypnut a zbytečně je spuštěn přes noc a další zařízení.

# 6. Závěr

Pokud se rozhodne řešit otázku komplexního monitoringu velká společnost, je SCOM výbornou volbou. Nasazení a hlavně správné nastavení SCOM zabere oproti Zabbix, Cacti nebo Nagios monitoringu mnohem více času a pro efektivní nastavení je zapotřebí absolvovat různá školení nebo si zaplatit externí firmu, která toto provede za poplatek. Ve chvíli, kdy ale SCOM funguje jak má, dokáže ušetřit spoustu času při řešení problémů.

Autor si zvolil toto téma z důvodu aktuálnosti zavádění tohoto systému ve firmě, kde pracuje. Za cíl měl, aby po dopsání této diplomové práce probíhal monitoring celého prostředí vybrané firmy. To se bohužel nepovedlo, protože i přes to, že je monitoring nasazen a aktivně sbírá z vybraných zařízení údaje o jejich stavu. Pro rozšíření sledovaných zařízení a nastavení více uživatelských pohledů v konzoli je potřeba, aby si firma zajistila externího konzultanta, který vytvoří další balíčky s MP pro zařízení, která se ve firmě používají a také nastaví monitoring, aby sledoval změny v monitorovaných zařízeních mnohem podrobněji.

Práce byla ale i přes to pro autora přínosem, neboť si mnohonásobně rozšířil vědomosti o dohledových systémech a získal osobní zkušenosti s rodinou produktů System Center, hlavně s Operations Manager.

Dílčí cíle byly splněny a v rámci teoretické části byl zpracován přehled několika dohledových systémů, byly definovány jednotlivé kategorie dohledových systémů a protokoly, pomocí kterých monitoring probíhá.

Na vybraných stanicích byli nainstalováni agenti ručně i systémově pomocí SCOM a aktivně sbírají informace o nainstalovaných programech, verzi operačního systému, využití procesoru a místě na disku. Po stáhnutí management pack z webových stránek DELL a jeho importování do SCOM byl nastaven monitoring pro 2 switche od firmy DELL včetně sledování jednotlivých portů.

Dohled byl nastaven i pro 10 virtuálních serverů, na kterých SCOM sleduje, zda nedošlo k zastavení služeb, monitoruje jejich vytížení a celkové zdraví.

SCOM splňuje náležitosti i notifikačního dohledového systému, takže byly vytvořeny cesty prostřednictvím SMS a emailu a nastaveny časy, které určují, komu mají být v daný čas zaslány notifikace. Zároveň byla upravena i konzole, aby zobrazovala pouze ty informace, které jsou pro administrátory potřebné a se kterými pracují a naopak aby se jim nezobrazovaly ty, o kterých nic nevědí. Tyto úpravy lze kdykoliv změnit,

nebo přidat další pohledy, takže až se SCOM začne používat úplně, budou zde muset být doplněny a upraveny zobrazované informace i z nově monitorovaných zařízení.

Na trhu existují podstatně jednodušší dohledové systémy, SCOM patří mezi ty složité na nakonfigurování, ale poté je schopný monitorovat téměř celou IT infrastrukturu. Pokud existuje nějaké zařízení, které SCOM neumí monitorovat, stačí nahrát nový MP (nebo pokud neexistuje, tak MP ručně vytvořit). Z těchto důvodů není zcela vhodný pro malé firmy, které disponují jen několika počítači a jedním serverem. Pro tyto účely jsou vhodnější dohledové systémy typu Zabbix nebo Cacti.

Pro velké firmy, které disponují rozsáhlou IT infrastrukturou je ale SCOM výborným řešením a lze jej jedině doporučit.

# 7. Seznam použitých zdrojů


WALLACE, George. *Microsoft system center extending operations manager reporting*. Redmond, WA: Microsoft Press, 2014. ISBN 978-073-5695-788.

SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Vyd. 1. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7

MEYLER, Kerrie, Cameron FULLER a John JOYNER. *System center 2012 operations manager unleashed*. Indianapolis, Ind.: Sams, c2013. Unleashed. ISBN 06-723-3591-3.

HERMANS, Danny. Microsoft system center software update management field experience. pages cm. ISBN 9780735695825

CORNELISSEN, Bob. *Mastering System Center 2012 Operations Manager*. Indianapolis: John Wiley, 2013. ISBN 978-1-118-12899-2.

KAPLAN, Věroslav. *Nagios - the monitoring system*. Brno: Konvoj, 2004. ISBN 8073020688.

PLESKOT, Vít. *Dohledové systémy pro počítačové sítě*. Pardubice, 2012. Bakalářská práce. UNIVERZITA PARDUBICE. Vedoucí práce Mgr. Josef Horálek.

Network Monitor Software and Windows Development Tools. *Monitortools.com* [online]. [cit. 2015-08-15]. Dostupné z: http://www.monitortools.com

Zařízení v síti pod kontrolou. *Samuraj-cz* [online]. 2009 [cit. 2015-08-15]. Dostupné z: http://www.samuraj-cz.com/clanek/zarizeni-v-siti-pod-kontrolou/

Jak a proč měřit teplotu serverů. *NETguru* [online]. [cit. 2015-08-22]. Dostupné z: http://netguru.cz/network/jak-a-pro-mit-teplotu-server.html

ProActive Enterprise | Proactive Monitor. ProActive. [online]. [2014] [cit. 2015-11-30]. Dostupné z: http://www.proactivemonitor.co.uk/proactive-enterprise

ip-address-fundamentals. The Geek Stuff. [online]. 15.1.2012 [cit. 2015-11-30]. Dostupné z: http://www.thegeekstuff.com/2012/01/ip-address-fundamentals/

IP - Internet Protocol. *EArchiv.cz: Archiv článků a přednášek Jiřího Peterky* [online]. [cit. 2015-08-22]. Dostupné z: http://www.earchiv.cz/anovinky/ai1843.php3

The IP Address. Vista Networking Solutions. [online]. 10.3.2013 [cit. 2015-11-30]. Dostupné z: http://blog.vnssystems.com/

Protocol Registries. *IANA: Internet Assigned Numbers Authority* [online]. [cit. 2015-08-24]. Dostupné z: http://www.iana.org/protocols

Products | Microsoft System Center. Cased dimensions. [online]. [2014] [cit. 2015-08-10]. Dostupné z: http://www.caseddimensions.com/microsoft_system_center/

Přehled nástroje System Center 2012 R2 | Microsoft. *System Center 2012 R2*. [online]. [2015] [cit. 2015-08-10]. Dostupné z: *http://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Overview.aspx*

Microsoft System Center. *Dimensions* [online]. [cit. 2015-08-05]. Dostupné z: http://www.caseddimensions.com/microsoft_system_center/

System Center 2012 R2. *Microsoft* [online]. [cit. 2015-11-15]. Dostupné z: https://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Components.aspx

blogs.technet.com. The System Center Team Blog. [online]. 2.8.2011 [cit. 2015-08-19]. Dostupné z: http://blogs.technet.com/b/systemcenter/archive/2011/08/02/system-center-monitoring-pack-for-microsoft-dynamics-ax-2012.aspx

System Center 2012 R2. *Microsoft* [online]. [cit. 2015-11-15]. Dostupné z: https://www.microsoft.com/cs-cz/server-cloud/products/system-center-2012-r2/Components.aspx

První pohled na System Center Operations Manager 2012. Optimalizované IT [online]. 13.12.2011 [cit. 2016-01-20]. Dostupné z: http://www.optimalizovane-it.cz/sprava-it-prostredi/strana-2.html

Novinky v System Center 2012 R2. *Daquas* [online]. [cit. 2015-08-13]. Dostupné z: http://www.daquas.cz/articles/622-novinky-v-system-center-2012-r2

Preparing your environment for System Center 2012 R2 Operations Manager. *TechNet* [online]. 2015 [cit. 2015-07-20]. Dostupné z: https://technet.microsoft.com/en-us/library/dn249696.aspx

Jak na instalaci System Center Operations Manager 2012. Pavel Řepa – IT management [online]. [cit. 2015-11-21]. Dostupné z: https://pavelrepa.wordpress.com/2011/11/28/jak-na-instalaci-system-center-operations-manager-2012/

Cacti: vše důležité v jednom monitoru. *ROOT.CZ* [online]. 2009 [cit. 2016-01-28]. Dostupné z: http://www.root.cz/clanky/cacti-vse-dulezite-v-jednom-monitoru

What is Zabbix. *Zabbix* [online]. [cit. 2015-08-20]. Dostupné z: http://www.zabbix.com/product.php

Dohledový systém Zabbix - představení I. *Linuxsoft.cz* [online]. 2013 [cit. 2015-08-15]. Dostupné z: http://www.linuxsoft.cz/article.php?id_article=1963

Preparing your environment for System Center 2012 R2 Operations Manager. Microsoft System Center. [online]. 11.5.2015 [cit. 2016-01-18]. Dostupné z: https://technet.microsoft.com/en-us/library/dn249696.aspx

How to Customize Message Content for Notifications. *Microsoft TechNet* [online]. [cit. 2016-01-13]. Dostupné z: https://technet.microsoft.com/en-gb/library/hh212698.aspx
Onboard in minutes. TechNet [online]. 2015 [cit. 2016-01-07]. Dostupné z: https://technet.microsoft.com/library/mt484118.aspx

# 8. Seznam použitých zkratek a symbolů

| Zkratka | Anglický význam | Překlad |
|---|---|---|
| **GPL** | General Public License | Volně použitelná licence |
| **ICMP** | Internet Control Message Protocol | Protokol řídících zpráv Internetu |
| **IIS** | Internet Information Server | Informační server pro internet |
| **IM** | Instant message | Rychlá zpráva - chat |
| **IP** | internet protocol | Protokol Internetu |
| **ISO** | Image | Soubor obsahující digitální kopii dat |
| **IT** | Information Technology | informační technologie |
| **ML** | Multi language | Více jazyčný |
| **MP** | Management pack | Balíček s informacemi jak daná zařízení sledovat |
| **OID** | Object Identifiers | Identifikátory objektu |
| **OSE** | operating system environment | Prostředí operačního systému |
| **PHP** | **Hypertext Preprocessor** | Skriptovací jazyk na straně serveru |
| **RH** | relative humidity | relativní vlhkost |
| **SCOM** | Software Center Operations Manager | Software Center Operations Manager |
| **SNMP** | Simple Network Management Protocol | Jednoduchý protokol správy sítě |
| **SQL** | Structured Query Language | Strukturovaný dotazovací jazyk |
| **TCP** | Transmission Control Protocol | Přenosový řídící protokol |
| **TTL** | Time To Live | Nastavená maximální doba životností datagramu v sítí |
| **VPN** | Virtual Private Network | Virtuální privátní sítě |

# 9. Přílohy

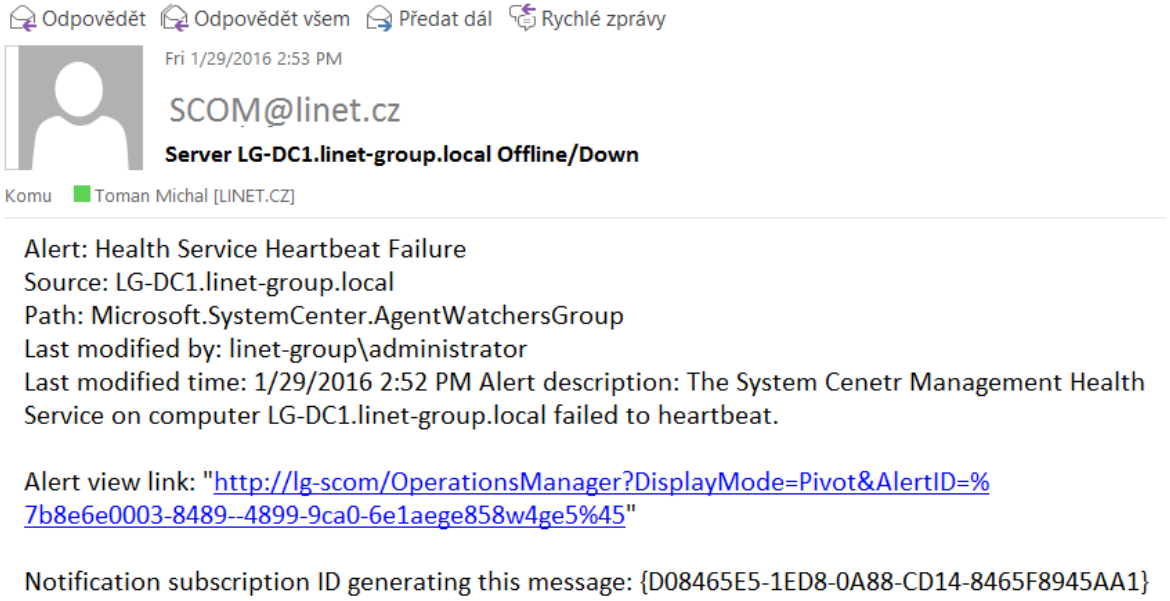
### Příloha 1: Management Pack pro DELL zařízení

Stránky, odkud lze stáhnout Management Pack pro zařízení od firmy Dell:

http://www.dell.com/support/home/us/en/19/Drivers/DriversDetails?driverId=DFGM2

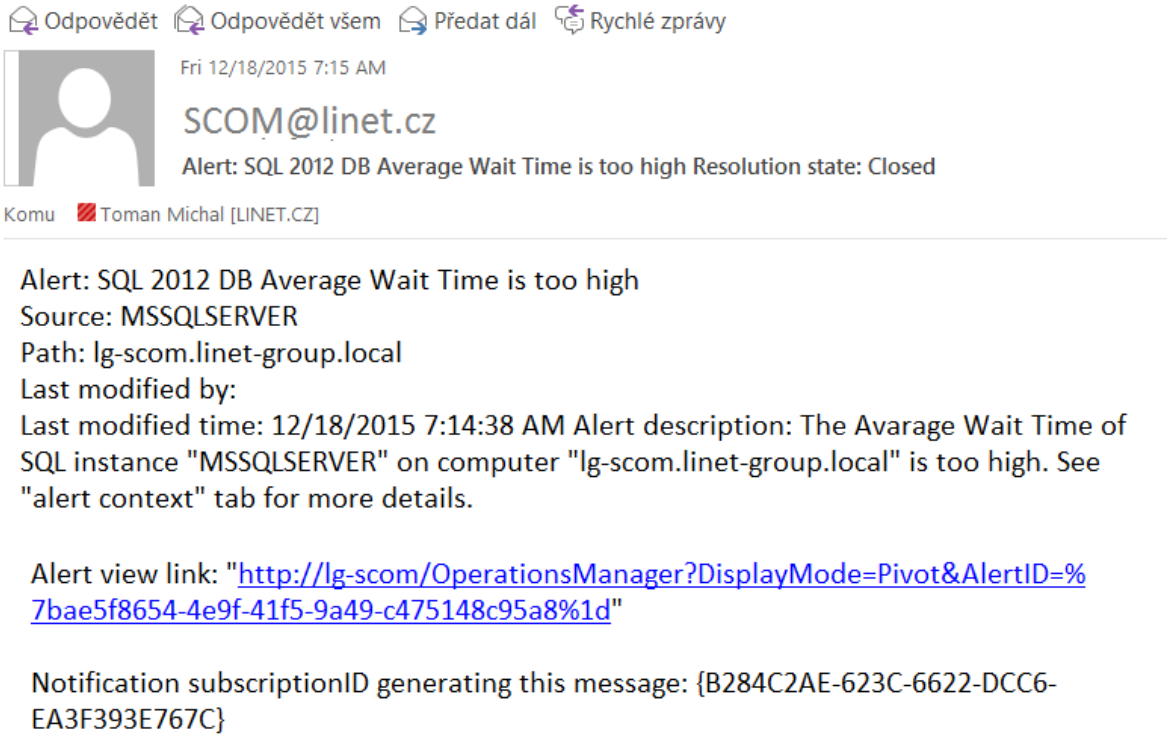
### Příloha 2: Alert pomocí E-mailu

Zaslaná notifikace na email o tom, že je server LG-DC1 nedostupný:



### Příloha 3: Alert typu closed

Další notifikace administrátorům, že doba přístupu k databázi byla příliš vysoká. Tato notifikace je typu closed, takže problém byl vyřešen.




### Příloha 4: Parametrsy pro instalaci SCOM

Instalaci jednotlivých Operations Manager 2012 rolí lze provést také pomocí příkazové řádky. K tomu slouží následující parametry:

```
setup.exe /silent /install
/components:OMServer,OMConsole,OMWebConsole,OMReporting
/ManagementGroupName: "<ManagementGroupName>"
/SqlServerInstance: <server\instance>
/DatabaseName: <OperationalDatabaseName>
/DWSqlServerInstance: <server\instance>
/DWDatabaseName: <DWDatabaseName>
/UseLocalSystemActionAccount /UseLocalSystemDASAccount
/DatareaderUser: <domain\username>
/DatareaderPassword: <password>
/DataWriterUser: <domain\username>
/DataWriterPassword: <password>
/WebSiteName: "<WebSiteName>" [/WebConsoleUseSSL]
```

*/WebConsoleAuthorizationMode: [Mixed|Network]*
*/SRSInstance: <server\instance>*
*/SendODRReports: [0|1]*
*/EnableErrorReporting: [Never|Queued|Always]*
*/SendCEIPReports: [0|1]*
*/UseMicrosoftUpdate: [0|1] Více na:*