Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Teze bakalářské práce

Monitoring počítačové sítě

Autor: Lukáš Dvořák

Monitoring počítačové sítě

Computer network monitoring

Souhrn

Práce se zaměřuje na zhodnocení dostupných řešení pro monitoring počítačové sítě a postupy při jejich provozu. V první části se zaměřuje na teoretické uvedení do problematiky sítí a možnosti jejich sledování. Pokračuje s uvedením příkladů nástrojů, které se k tomuto sledování používají, a jejich krátkým představením. V další části se věnuje podrobným rozpracováním možnosti práce s vybranými nástroji vhodnými pro zvolenou síť. Ukazují se zde postupy instalace i práce na konkrétních typech úloh. V závěrečné části dochází ke zhodnocení zvolených nástrojů ve scénářích, které mohou v síti nastat. Je zde uvedena reakce nástrojů na vybrané situace. Na závěr je uvedeno zhodnocení přínosu zvolených nástrojů pro síť.

Klíčová slova: počítačová síť, monitoring, DWDM, Nagios, Node Manager, Open View, Icinga, CTC

1 Cíl a metodika práce

1.1 Cíl práce

Cílem práce je detailní zhodnocení komerčních i nekomerčních řešení pro monitoring počítačové sítě. Dílčím cílem je ukázat důležitost takových systémů a jejich neodmyslitelnou přítomnost u každého poskytovatele síťového připojení nebo serverových služeb. To je provedeno výčtem možných situací, které mohou nastat, a tím, jak je nástroje zachytí.

Dalším cílem práce je nastínit práci s vybranými programy pro monitoring sítě. Ukázat jejich uživatelské prostředí a udělat doporučení pro jejich efektivní provoz.

Na základě všech poznatků je na závěr doporučena nejlepší kombinace dostupných řešení.

1.2 Metodika práce

Teoretická část představuje jednotlivé programy pro monitoring počítačové sítě. Jak komerční, tak nekomerční. Je zde vzpomenuta důležitost těchto systémů pro co nejvíce bezproblémový chod počítačové sítě.

Uvedené informace čerpá autor z dostupných zdrojů a zejména pak z řešení, která jsou provozována ve firmě CESNET, z. s. p. o., Na základě získaných informací je navrhnuto optimální řešení pro střední až velkou počítačovou síť. V poslední části jsou formulovány závěry a doporučení.

2 Teoretická východiska

Teoretická část je rozdělena na čtyři hlavní kapitoly. První z nich stručně popisuje historii počítačové sítě a období jejího největšího rozmachu. Dále pokračuje popisem, co to počítačová síť vlastně je.

Další kapitola se věnuje vysvětlení pojmu monitoring počítačové sítě. Jsou zde vyjmenovány jednotlivé druhy upozornění a výhody tohoto sledování.

Práce pokračuje další částí, která je věnovaná kategoriím monitorovacích nástrojů. Nejdříve je popsána možnost upozorňování na vyvstalé problémy, a to tak, že je ukázána důležitost a praktičnost těchto upozornění a jakými způsoby je možno zabezpečit. Dále se práce zabývá způsoby, jak můžeme sledování provádět. Například monitorováním logu událostí, monitorováním provozu sítě a také se věnuje protokolu SNMP. Je zde uveden jeho princip a výhody jeho použití. Toho je využito v další části, která se věnuje všemu, co a jakým způsobem můžeme sledovat.

Poslední kapitola se věnuje rozdělení nástrojů pro monitoring sítě na komerční a nekomerční. Jsou zde uvedeni hlavní zástupci obou kategorií a popsán jejich princip.

3 Vlastní zpracování

Tato část práce se podrobněji zabývá zvolenými nástroji, které jsou zvoleny pro síť o daných parametrech. Jedná se o nástroje HP Network Node Manager, Icinga a Cisco Transport Controller. Tyto nástroje jsou detailněji rozebrány z pohledu způsobu používání a instalace. Jsou zde uvedeny výhody a nevýhody jednotlivých módů zobrazení, které jsou doplněny snímky obrazovek z reálného provozu.

4 Zhodnocení výsledků

Za pomocí předchozích poznatků autor zpracoval ideální rozvržení tří vybraných nástrojů, a to HP Network Node Manager, Icinga a Cisco Transport Controller pro co nejefektivnější sledování počítačové sítě.

Dále autor na vybraných scénářích, které zachycují většinu situací, které mohou nastat, vypracoval přehled, jak budou jednotlivé nástroje reagovat. Díky tomuto srovnání je jasně vidět, že ani jeden z nástrojů nezajistí správný a úplný monitoring sítě samotný. Vždy musí jít o kombinaci vhodně nakonfigurovaných nástrojů.

HP Network Node Manager zajišťuje sledování aktivních prvků, jejich portů a uzlů. V tom je velmi podobný nástroji Icinga, ten je ale více specializovaný na služby jednotlivých serverů. Nástroj Cisco Transport Controller je velice specifický a velmi se od předchozích dvou odlišuje. Specifičnost tohoto nástroje spočívá v tom, že je určen pro optické propoje uzlů a k jejich konfiguraci. Zajistí tak upozornění na incidenty, které se nedají sledovat v HP Network Node Manageru ani v Icinze.

5 Závěr

Tato práce se zabývala přehledem a představením práce s různými nástroji pro monitoring sítě. Ukázala důležitost těchto nástrojů u každého většího poskytovatele síťových služeb. Jako příklad byla vybrána firma CESNET, z. s. p. o., ve které jsou tyto nástroje používané v běžné praxi. Autor v této firmě čerpal zkušenosti s prací s nástroji pro sledování sítě a zhodnotil jejich význam v konkrétních situacích. Doporučil také, jak tyto nástroje používat v praxi. Vyzdvihl ideální způsob použití pro co nejefektivnější sledování konkrétního stavu sítě. V práci je dále uvedeno praktické rozložení uživatelského rozhraní nástrojů. Pro každý nástroj totiž existuje více možností, jak informace o síti zobrazit. Některé zbytečně zahlcují operátora, nebo mu naopak nedávají pravdivý přehled o síti.

Všemi těmito postřehy autor ukázal na důležitost stálé služby, který tyto nástroje kontroluje a ovládá. U menších sítí postačují automatické zprávy, které nástroje generují. U větších sítí je již však doporučeno zřídit stálou službu, která bude vykonávat nepřetržitý dohled nad těmito nástroji. Může tak zareagovat okamžitě po nastalé události, která může vést k omezení provozu sítě nebo k výpadkům serveru.

6 Bibliografie

1. Začínáme s monitoringem sítě. *Samuraj-cz.com.* [Online] http://www.samuraj-cz.com/clanek/zaciname-s-monitoringem-site/.

2. Příhoda, Petr. [Online] http://phoenix.inf.upol.cz/esf/ucebni/poc_site.pdf.

3. *Network monitor software and windows development tools.* [Online] http://www.monitortools.com/.

4. Cloud monitoring. [Online] http://forpsicloud.cz/cloud-monitoring/vlastnosti.

5. Network diagnostic utilities. *ManageEngine.* [Online] http://www.manageengine.com/products/oputils/help/diagnostics/diagnostics_tools.html.

6. Bruey, Douglas. SNMP: Simple? Network Management Protocol. [Online] http://www.rane.com/note161.html.

7. Bouška, Petr. SNMP - Simple Network Management Protocol. [Online] http://www.samuraj-cz.com/clanek/snmp-simple-network-management-protocol/.

8. VILEMAITIS, Marius. *HP Network Node Manager 9: getting started.* Birmingham, U.K. : Packt Enterprise, 2011. 9781849680851.

9. Alwayn, Vivek. *Optical Network Design and Implementation.* místo neznámé : Cisco Press, 2009. 1587141507.

10. Jamrich, Marián. Nagios: monitorovanie počítačovej siete. *Root.* [Online] 15. 12 2010. http://www.root.cz/clanky/nagios-monitorovanie-pocitacovej-siete/.

11. Štrauch, Adam. Icinga: monitorování sítí a serverů. *Root.cz.* [Online] 13. 05 2011. [Citace: 06. 06 2014.] http://www.root.cz/clanky/icinga-monitorovani-siti-a-serveru/.

12. What does Icinga have that Nagios doesn't? *Icinga.org.* [Online] [Citace: 06. 06 2014.] https://www.icinga.org/about/nagios/feature-comparison/.

13. Mehta, Viranch. *Icinga network monitoring monitor complex and large environments across dispersed locations with Icinga.* Birmingham, UK : Packt Pub, 2013.

14. Cisco Systems, Inc. *Cisco ONS 15454 Reference Manual* . San Jose : Cisco Systems, Inc., 2008.