

Postupná migrace firemní infrastruktury a aplikací do cloudu s sebou přináší zcela nové výzvy na monitorování a diagnostiku výkonu sítě i aplikací. Současné nástroje (NPMD/APM) nejsou schopny zajistit komplexní monitorování často hybridního cloudového prostředí. Odpovědní pracovníci, kteří se starají o provozování a správu cloudových aplikací, musejí zvážit nové metody monitorování založené na cloudových technologiích, které dokážou zajistit potřebnou viditelnost.

PAVEL MINAŘÍK

Cloud se již stal běžnou součástí podnikového **IT** a v nějaké formě jej využívá většina firem. Umožňuje jim lépe škálovat výpočetní prostředky a nabízí také lepší rozložení finančních nákladů v čase.

Otázka, která však aktuálně trápí síťové administrátory a bezpečnostní **IT** specialisty, zní:

„Jak můžeme monitorovat a analyzovat provoz napříč fyzickou, virtuální a cloudovou infrastrukturou? Jak zajistit stejnou míru kontroly při využívání hybridní infrastruktury, kdy jedna její část leží v on premise datovém centru, další je umístěna v private cloudu a jiná zase využívá public cloud? V konečném důsledku je veškeré **IT** a jeho fungování naše odpovědnost.“

Tyto otázky dnes nejvýrazněji rezonují ve Spojených státech, kde je potřeba konsolidovaného monitoringu a poptávka po řešeních založených na nových paradigmatech nejhlasitější.

Jako jeden z mála dodavatelů je na hybridní monitoring již dnes připravena společnost Flowmon Networks se svým pokročilým řešením Flowmon.

Kde jsou moje pakety?

Důvodem, proč selhávají tradiční přístupy k monitoringu, jsou zřejmé. Hlavním problémem je chybějící přístup k informacím ze síťové vrstvy L2. V prostředí public cloudu se k nim jednoduše nelze dostat. Nefungují ani tradiční neinvazivní přístupy s využitím například SPAN portu. Výrobci proto hledají cestu, jak tato slepá místa ve virtuální síti odstranit a umožnit analýzu kritických dat, která řeší bezpečnostní hrozby a problémy s výkonem v cloudu. Tam, kde dříve postačoval export Flow dat z aktivní ho síťového prvku, dnes kvůli komunikaci virtualizačních platformem jako takových (VxLAN) již nelze monitorovat síťovou komunikaci na příslušné úrovni a detailu. Řešení Flowmon jako jedno z mála nabízí centrální pohled na všechna konsolidovaná data napříč infrastrukturou, a to díky flexibilním síťovým sondám, které umožňují různé způsoby nasazení napříč prostředními typu on premise, private cloud nebo public cloud, a zároveň poskytují identická data z těchto rozdílných prostředí. Stejně tak sondy Flowmon rozpoznají různé typy enkapsulace (tunelování), jež odstraní a změní skutečně přenášená data. Jak na monitoring v public cloudu I. Virtual tapping – agentní řešení instalované na monitorované servery. Zachytává komunikaci mezi virtuálními stroji (VM) na příslušných síťových rozhraních a doručuje pakety monitorovacím nástrojům třetích stran. Nejznámější řešení založené na virtual tappingu nabízí IXIA nebo Gigamon. Flowmon podporuje řešení obou společností.

II. ERSPAN/GRE – zrcadlení portu na úrovni L3 a doručení kopie síťového provozu monitorovacím nástrojům prostřednictvím tzv. GRE tunelu. Funkce je dostupná nejen ve virtuálních platformách a public cloudu (například VMWare VDS switch, Cisco CSR 1000V), ale umožňuje konsolidaci monitoringu v on premise prostředí s využitím vlastností pokročilých podnikových prepínačů. Řešení Flowmon umí na rozdíl od běžných monitorovacích nástrojů zakončit ERSPAN/GRE tunel, a nepotřebuje tak žádnou mezivrstvu.

III. Podpora FlowLogs – export nativních Flow dat přímo z prostředí public cloudu (například z Amazon AWS nebo Microsoft Azure) do monitorovacích nástrojů. Zde jde o poměrně novou technologii, která zatím ve srovnání s tradičním NetFlow nabízí velmi omezený set informací. Ve společnosti Flowmon Networks nyní sledují vývoj v této oblasti a připravují podporu pro FlowLogs v řešení Flowmon. Dodejme, že získaná Flow data nejsou přímo kompatibilní s NetFlow technologií a je potřeba je konvertovat.

Připravme se na další výzvy

Přechod do cloudu nepředstavuje pro oblast monitoringu a detekce anomálií jedinou komplikaci. Další výzvou je trend virtualizace na bázi kontejnerů v čele s řešením Docker, případně orchestrační platformou Kubernetes. Nejenže má Docker dnes už podporu u všech velkých hráčů nabízejících svá cloudová prostředí, ale využívá ho stále více firem, služeb a aplikací. Z pohledu monitoringu ale představuje obdobnou komplikaci jako jiná cloudová prostředí. Ve Flowmon Networks jsme již ověřili, že je možné statistiky o provozu virtuální sítě v prostředí Docker generovat a zpracovat v prostředí Flowmon kolektoru.

Hybridní cloud, příležitost pro univerzitní výzkum a vývoj

Viditelnost v hybridním cloudovém prostředí bude do budoucna představovat stále významnější téma. Již dnes je poptávka po jednom centrálním řešení nad celou hybridní infrastrukturou velkým tématem v USA a je zřejmé, že zanedlouho bude také u nás v Evropě. I proto se této oblasti věnují ve Flowmon Networks s patřičnou intenzitou. Interní vývoj doplňuje spolupráce s předními českými technickými univerzitami. Například ve spolupráci s Masarykovou univerzitou v Brně startuje v lednu 2019 projekt „Inteligentní senzory pro měření a analýzu cloudového prostředí“ podpořený v programu TAČR Delta. Cílem projektu je vytvořit inteligentní senzory pro měření a analýzu síťového provozu právě v cloudovém prostředí. Budou zkoumány nové způsoby měření s důrazem na optimalizaci používaných výpočetních zdrojů, autonomní chování senzorů a vytváření provozních telemetrických informací o chování celého systému. Výstupy projektu umožní návrh nových aplikací a služeb. Dílčí výsledky budou obratem aplikovány do produktů společnosti Flowmon Networks, aby mohly být co nejdříve uvedeny na trhu cloudových monitorovacích řešení.

\*\*\*

RNDr. Pavel Minařík, PhD.

Pavel Minařík se zabývá oblastí kybernetické bezpečnosti od roku 2006. Účastnil se řady výzkumných projektů v oblasti analýzy provozu datových sítí a detekce pokročilých hrozeb jako výzkumný pracovník Ústavu výpočetní techniky Masarykovy univerzity. V současné době pracuje jako technologický ředitel ve společnosti Flowmon Networks, kde je zodpovědný za návrh a vývoj produktů společnosti.

vTAP – elegantní řešení pro veřejný cloud

Virtuální TAP je softwarový nástroj umožňující dostat se skrze adresovanou výzvu k síťovému provozu v cloudu, a zajistit tak plnou viditelnost i ve virtuálním prostředí veřejného cloudu. Zachytává kopii datového provozu mezi virtuálními stroji včetně komunikace uvnitř VM (tzv. east-west traffic) a nepřetržitě zrcadlí tento provoz z virtuální sítě do cílového virtuálního kolektoru. Virtuální TAP odstraňuje slepá místa ve virtuální síti a umožňuje analyzovat důležitá data vztahující se k bezpečnostním a výkonnostním problémům.

Flowmon a MS Azure vTAP

Společnost Microsoft vybrala Flowmon jako vůbec jedno z prvních řešení, kterému umožnila nativně monitorovat své cloudové prostředí AZURE. Flowmon kolektor, nasazený v cloudu Azure, poskytuje síťovým administrátorům a bezpečnostním technikům dokonalý přehled o tom, co se děje v jejich cloudovém nebo hybridním prostředí. Pomáhá rychle řešit provozní incidenty, zlepšuje výkonnost klíčových aplikací a umožňuje vypořádat se s moderními bezpečnostními hrozbami. Microsoft Azure vTAP je zde plně využit k zrcadlení datového provozu na monitorovací porty Flowmon kolektoru.

Výhody řešení Flowmon + vTAP

\* Rychlé zprovoznění monitoringu \* Centrální řízení a monitoring \* Plná viditelnost bez vlivu na výkon systému \* Snadná škálovatelnost \* Snižuje provozní náklady

Foto popis|