EuroCloud SLOVAKIA

Cloud Computing Guide

Meranie aplikačnej výkonnosti cloudových riešení

State and Future of Application Performance Measurement in today's complex Cloud environments

SLOVAKIA

Autor publikácie

Eurocloud Austria
Združenie pre podporu cloudových technológií

Museumstrassse 5/14
1070 Vienna, Austria
E-mail: info@eurocloud.at
Web: http://www.eurocloud.at

Copyright: EuroCloud Austria, 2014

Vydavateľ slovenskej verzie

Eurocloud Slovakia, o. z.

Konopná 52
821 05 Bratislava, Slovakia
E-mail: eurocloud@eurocloud.sk
Web: http://www.eurocloud.sk

Obsah

Úvod 5

1. Manažérske zhrnutie 6

2. Manažment aplikačnej výkonnosti (APM) v súčasnosti 7

3. Budúcnosť manažmentu aplikačnej výkonnosti (APM) 9
   - 3.1 V krátkodobom horizonte – kombinácie monitorovacích metód 9
   - 3.2 V dlhodobom horizonte – Koncepcia otvorených nástrojov pre analýzu aplikačnej výkonnosti 10

4. Súčasnosť a budúcnosť monitoringu cloudových riešení virtuálnych desktopov 12
   - 4.1 Aktívny monitoring 12
   - 4.2 Budúcnosť: Pasívny monitoring 14

5. Benchmarking, záťažový a stress test, regresné testy 21

6. Detailnejší pohľad na Desktop, ako službu (DaaS) 21
   - 6.1 VDI/DaaS v spolupráci s LAN klientom (najjednoduchší prípad) 24
   - 6.2 VDI/DaaS v spolupráci s virtualizovaným LAN klientom 25
   - 6.3 VDI/DaaS klient vo WAN sieti 26
   - 6.4 Použité výrazy a definície 27

7. Právne informácie 29
   - 7.1 Všeobecná informácia 29
   - 7.2 Obsah príručky 29
   - 7.3 Odkazy a linky 29
   - 7.4 Autorské práva 30
   - 7.5 Poplatky 30

8. Autor 31

Cloud Computing Guide
Meranie
aplikačnej výkonnosti
cloudových riešení

State and Future of Application
Performance Measurement
in today's complex
Cloud environments

Úvod



Vážený čitateľ. Cloud, mobilné technológie a sociálne siete sa stávajú extrémne komplexným IKT prostredím, ktoré nemá obdobu v žiadnych iných technológiách. Následkom toho mnohé komponenty dodávateľského reťazca aplikácií získavajú nie celkom jasné atribúty v dodávateľskej a vlastníckej štruktúre. Skutočná pozorovateľná výkonnosť a aktívna inteligencia systémov by sa mala stať najdôležitejším kritériom pre všetky organizácie vo vzrastajúcej zložitosti cloudových systémov a sústavne rastúcom objeme spracovávaných dát.

Táto skutočnosť je dôvodom, prečo sa Eurocloud rozhodol vydať túto Bielu knihu, ktorá sa zaoberá týmto špecifickým a technologicky veľmi náročným problémom. Cieľom Eurocloudu je podporiť vývoj a dosiahnuť zdravú rovnováhu medzi dodávateľmi cloudových služieb a zákazníkmi. Súčasťou našej snahy sú aj vecné riešenia, legislatívna podpora, bezproblémový prístup k cloudovým službám a ďalšie technické otázky, súvisiace s predmetným riešením.

Chceme podporovať užívateľov a dodávateľov cloudových služieb pri pochopení podstaty problému a rizík merania aplikačnej výkonnosti. Táto snaha vyústila do príručky, ktorá sa dostáva do Vašich rúk a ktorá je preložená do mnohých jazykov.

EuroCloud chce vysloviť úprimnú vďaku pánovi Reinhardtovi Trávničkovi, riaditeľovi spoločnosti X-tech a autorovi tejto príručky. Pán Trávniček je uznávaným odborníkom v oblasti virtuálneho desktopu a do príručky zahrnul informácie na základe vlastných skúseností a rozsiahlych poznatkov v predmetnej problematike.

Viedeň , September 2014

Dr. Tobias Höllwarth
Viceprezident EuroCloud Europe

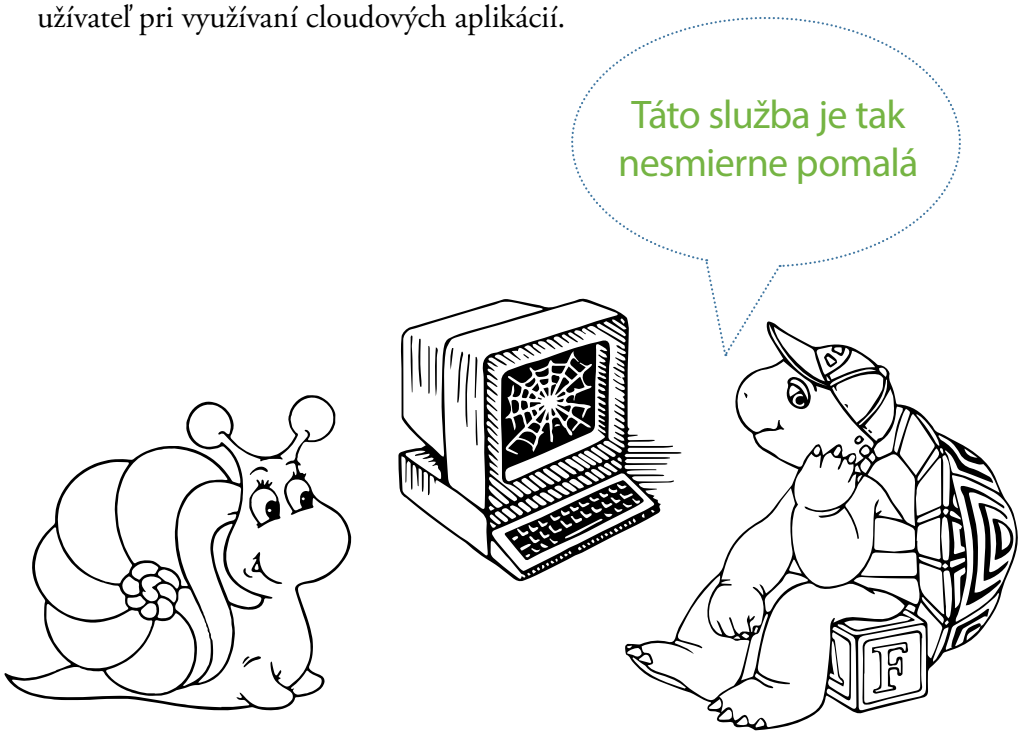
1. Manažérske zhrnutie

Mnohé štúdie preukazujú, že pre užívateľov, zákazníkov a CIO je kritická vysoká dostupnosť aplikácií. Zároveň viacnásobná závislosť aplikácií na podpornej a realizačnej infraštruktúre môže vplývať na degradáciu výkonnosti jednotlivých aplikácií. Organizácie si postupne uvedomujú potrebu a význam monitorovania užívateľskej dostupnosti kritických aplikácií ako aj skvalitňovania ich výkonnosti. Efektivita a realizácia týchto strategických snáh výrazne závisí na spôsobe overovania aplikačnej výkonnosti a spokojnosti koncových užívateľov. Úroveň a reálne skúsenosti koncových užívateľov sa pomerne ťažko exaktne kvantifikujú, ale aplikačná výkonnosť spracovania dát sa dá odmerať pomerne jednoducho. Súčasné riešenia na monitorovanie výkonnosti len veľmi obťažne zabezpečujú transformáciu týchto údajov do KPI a do SLA, tak aby sa zohľadnili požiadavky a skúsenosti koncových užívateľov .

Tento dokument prezentuje rozličné metódy premostenia problémov súčasných SLA zavedením presných, sieťovo a procesne zameraných podrobných informácií. Súčasne také informácie pomáhajú pri hľadaní problémov, súvisiacich s aplikačnou výkonnosťou, diagnostikou výkonnosti, diagnostikou základných príčin a zatriedením užívateľských skúseností v oblasti (VDI) infraštruktúry virtuálneho desktopu a DaaS (desktop ako služba). Úspech, alebo neúspech IT tímov sa najmarkantnejšie odráža od stavu aplikačnej výkonnosti a dostupnosti služby. Vysoké čísla dostupnosti služby predstavujú vysokú prioritu dodávateľov a nútia ich uplatňovať komplexné postupy manažmentu výkonnosti a analýz pre rozhodovanie. Využívanie best practices pri konzultáciách s užívateľskými spoločnosťami pomáha pri hľadaní najlepšieho využívania IT investícií. Umožňuje interpretovať následky spracovania miliárd transakcií a ich vplyv na prevádzku, bezpečnosť a správnosť spracovania a na konkurencieschopnosť. Help desk IT spoločností nemôže byť jediným miestom zberu informácií, ktoré ovplyvňujú prevádzkyschopnosť systému a dosahovanie maximálnych výsledkov.

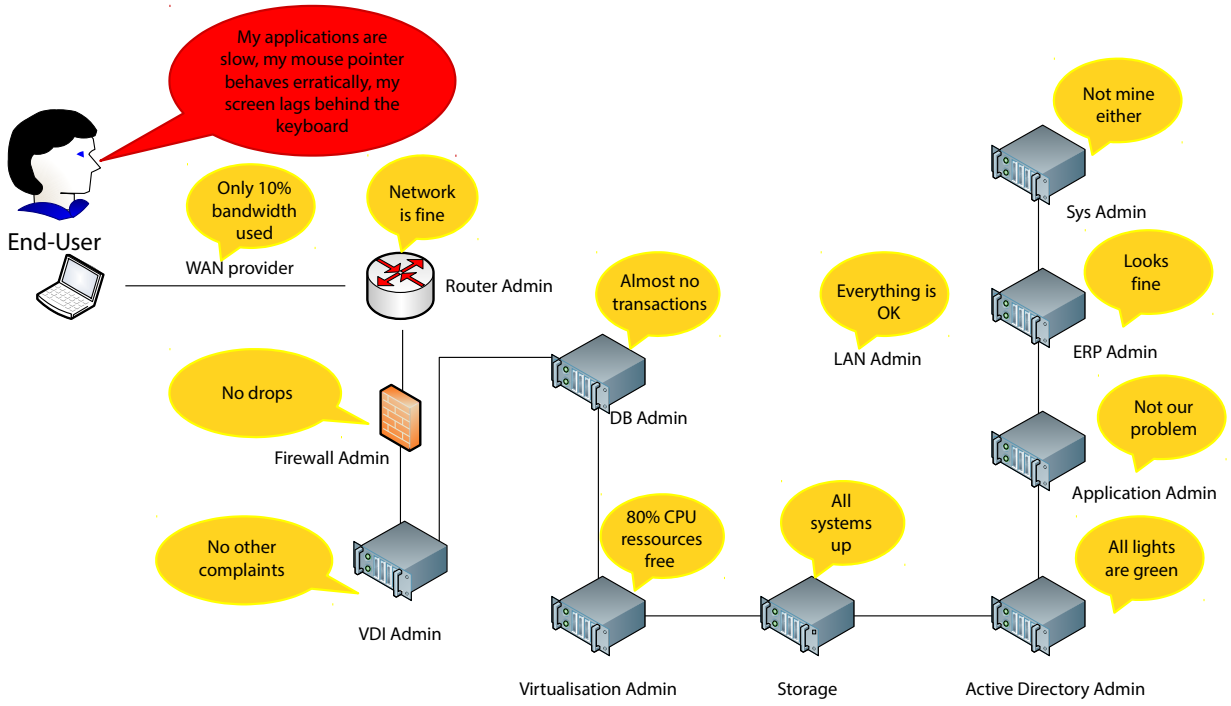
2. Manažment aplikačnej výkonnosti (APM) v súčasnosti

Každý chápe, že moderné IT prostredie prepája obrovský počet zariadení a takisto veľký počet internetových prepojení. Kombinovaný vplyv latencie, opozdenia prenosu každého z prepojení týchto zariadení, i samotných zariadení pri prenose a spracovaní signálu musí ovplyvňovať prácu a dynamiku spracovania, ktorú pozoruje koncový užívateľ pri využívaní cloudových aplikácií.



Jednou zo základných príčin, prečo koncový užívateľ má náskok v spozorovaní degradáciu aplikačnej výkonnosti pred IT poskytovateľom tkvie v tom, že IT organizácie analyzujú obrovské objemy dát súvisiacich s manažmentom procesov a komunikácie. Tieto dáta prichádzajú zo stále rastúceho počtu spracovávaných transakcií, ďalej zo zložitej, distribuovanej sieťovej a aplikačnej infraštruktúry. Rast objemu dát spôsobujú aj ďalší extenzívni využívatelia cloudovej infraštruktúry.

Následkom veľkého počtu zariadení, ktoré sa podieľajú na prenose a spracovaní transakcií, bude sťažnosť koncového užívateľa na nedostatočné aplikačné výkonnosť riešená približne tak, ako to zobrazuje schéma:



Mnohé IT spoločnosti si ešte stále zaobstarávajú diskrétne SW nástroje, ktoré spracovávajú problémy vybraných HW elementov infraštruktúry, siete alebo aplikácií. Často také riešenie vedie k SW skladačkám s rôznymi doplnkami, úpravami, ktoré nespolupracujú dostatočne dobre s monitorovacím SW. Následkom toho dochádza k situácii, že aj keď určitý segment infraštruktúry vykazuje dobré parametre výkonnosti, v rámci dohodnutej normy, problém pretrváva a koncový užívateľ deklaruje nespokojnosť s výkonnosťou.

Obrázok ilustruje aj situáciu, že manažér dodávateľa, resp. koncový užívateľ sa nevie zorientovať a dohodnúť s veľkým počtom externých a interných dodávateľov služieb. Nevedia vyhodnotiť a pochopiť veľké množstvo rôznych vzťahov a závislostí medzi elementami infraštruktúry. Objednávateľa IT služieb, zákazníka, nezaujíma, ako je vytvorená a riadená obslužná infraštruktúry služby. Predmetom záujmu sú úžitkové parametre tejto služby pre zákazníka.

3. Budúcnosť manažmentu aplikačnej výkonnosti (APM)

3.1 V krátkodobom horizonte – kombinácie monitorovacích metód

Kombinácia aktívneho a pasívneho monitoringu (v kapitole 6.4 uvádzame podrobnejšiu analýzu monitorovacích metód) umožňuje operátorovi (dodávateľovi služby) lepší a komplexnejší náhľad na stav riadeného systému a na spôsob, ako definovať KPI a SLA pre jeho zákazníkov. Aktívne komponenty monitorovacieho systému zabezpečia presné hodnoty pre KPI, ako dostupnosť služby, presný termín štartu aplikácie a pod. a pasívne prvky monitorovacieho systému zabezpečia štatistické dáta pre stanovenie hraníc možných požiadaviek koncových zákazníkov. V ďalšej fáze, v strednom časovom horizonte, sa dá predpokladať rozšírený pasívny monitoring prepojený s BDM – analýzou Big Data.

Intenzívny nárast virtualizácie serverov a nástrojov, potrebných k monitoringu a manažmentu virtualizovanej dynamickej infraštruktúry a výrazne distribuovaných aplikácií bude znásobovať zdroje dát a súvislosti prvkov systémov, ktoré bude potrebné analyzovať.

Následkom toho sa často prehliadne kľúčová informácia, ktorá spôsobí, že administrátor neobjaví utajené šablóny správania sa siete, súvislosti a závislosti javov a prvkov siete. Naviac, zber dát nie je normalizovaný, alebo časovo synchronizovaný a to znemožňuje následnú analýzu a rýchle riešenie vzniknutých problémov. Násobenie zberu dát, sledovaných zastaranými analytickými nástrojmi, len prehlbuje popísaný problém. Je nutné hľadať nové riešenia monitorovania aplikačnej výkonnosti.

Výzva na spracovanie obrovských objemov dát analýzou vedie jednoznačne k pojmu Big Data. Tento pojem sa používa v tom prípade, ak máme spracovať tak veľký a komplexný objem dát, že je veľmi obťažné, až priam nemysliteľné ich spracovávať tradičnými postupmi a technológiami. IT spoločnosti z oblasti výskumu vyvíjajú širokú škálu riešení pre spracovanie veľkých dátových objemov. Tieto aktivity vedú k riešeniam na báze nástrojov pre analýzu Big Data. Ich nasadenie na

riešenia otázok manažmentu aplikačnej výkonnosti zodpovedá metódam analýzy správania sa aplikácií.

Monitorovací nástroj pre analýzu správania sa aplikácií sa bude automaticky učiť z reálnych dát, ktoré reprezentujú normálne správanie sa systému. V nástroji implementované sofistikované štatistické postupy budú identifikovať situácie, ktoré sa odchyľujú od štandardného správania sa systému a budú identifikovať zdroje odchýlok. Implementácia nástrojov pre analýzu správania sa aplikácií umožní IT organizáciám zlepšiť proaktívny, aj krízový manažment riadenia aplikačnej výkonnosti. Analýza Big Data na výkonných počítačoch bude poskytovať IT organizáciám detailnú analýzu v reálnom čase a umožní business manažérom získať presvedčenie, že ich kritické procesy prebiehajú s plánovanou dynamikou a spoľahlivosťou. Predpokladáme, že na trhu sa objavia nástroje pre manažment aplikačnej výkonnosti na báze metód Big Data Manažment už v priebehu roka 2015.

3.2 V dlhodobom horizonte – Koncepcia otvorených nástrojov pre analýzu aplikačnej výkonnosti

Sme presvedčení, že v súčasnosti prebieha vývoj nástrojov na báze Open source platformy, zameraných na manažment aplikačnej výkonnosti, ktoré by mohli byt k dispozícii koncom roka 2016. Táto skutočnosť by mala byť výzvou pre ďalších dodávateľov riešení na tejto platforme, aby využili túto otvorenú architektúru na to, aby ponúkli svoje špecifické dáta pre analýzu Big Data s cieľom získať operačnú BI pri spracovaní týchto sprístupnených údajov.

Cieľom týchto snáh je:

- Zvýšiť pridanú hodnotu ponúkaných produktov presmerovaním vývojárskych tímov a ich úsilia zameraného na získavanie testovacích údajov
- Vzájomnú výmenu a zdieľanie údajov jednotlivých výrobcov pre krížovú analýzu a zmiešanú analýzu hlavných príčin problémov
- každý dodávateľ sa stáva súčasťou oveľa väčšieho ekosystému, čo je dôveryhodnou náhradou za individuálne vlastníctvo koncepcie manažmentu

» Dátový sklad bude open source a bude tolerantne licencovaný, čím bude chrániť vývojárov a dodávateľov od uzatvorenia sa, alebo iného nepriaznivého dôsledku

Navrhovaná platforma reprezentuje ucelenejší prístup k adaptívnemu, proaktívnemu a predvídavému operatívnemu manažmentu dát a k analýze. Platforma má potenciál prepojiť pokrokové manažmenty aplikačnej výkonnosti a technológie Big Data manažmentu tak, aby umožnili získať hlboký náhľad v reálnom čase do aplikačnej výkonnosti, získať inteligenciu pre predvídanie zmien. Riešenie umožní monitorovať virtuálne a mobilné systémy s rastúcou zložitosťou v celom dodávateľskom reťazci aplikácií.

Tieto nové analytické technológie merania výkonnosti musia spoločnostiam ponúknuť riešenie v týchto troch oblastiach:

» Veľké spoločnosti musia pochopiť, aká je požadovaná úroveň výkonnosti (napríklad rýchlosť, dostupnosť) ich cloudových a mobilných aplikácií k tomu, aby mohli dodávať spoľahlivé, ich zákazníkov upokojujúce riešenia, spĺňajúce požiadavky koncových užívateľov. Pre lepšie pochopenie vlastností jednotlivých komponentov a ich miesto v celkovej štruktúre dodávania aplikácie klientom je potrebná vyššia úroveň stanovenia vzájomných vzťahov týchto komponentov. Komplexná analýza aplikačnej výkonnosti umožní zviditeľnenie celého dodávateľského reťazca aplikácie – od firewallu až po Web, včítane cloudových dodávateľov tretích strán.
» Bod dodania, teda miesto, kde užívateľ má prístup k zloženej aplikácii je jediným sledovateľným miestom, kde sa môžu definovať užívateľské požiadavky. Utilizácia infraštruktúry nie tým najrelevantnejším parametrom, na ktorý sa majú sústrediť IT organizácie. Tým parametrom je práve hranica utilizácie, pri ktorej sa začínajú degradovať užívateľské parametre služby. Veľké spoločnosti musia zvládnuť meranie sústavy indikátorov najdôležitejších segmentov koncových zákazníkov, vrátane vzdialených a mobilných.
» Nakoniec je potrebné umožniť komerčným užívateľom získať prehľad a know-how, súvisiace s analýzou a manažmentom aplikačnej výkonnosti.

4. Súčasnosť a budúcnosť monitoringu cloudových riešení virtuálnych desktopov

Technológie monitorovania sa spravidla delia na dve oddelené kategórie:

- Riešenia pre aktívny monitoring (syntetický monitoring)
- Riešenia pre pasívny monitoring (skúsenosti reálneho užívateľa)

Obidve uvedené metódy majú svoje výhody a pomáhajú organizáciám merať aplikačnú výkonnosť. Nástroje aktívneho monitoringu, kombinované so zberom vybraných systémových údajov tvoria základ väčšiny monitorovacích riešení, ktorú sú v súčasnosti implementované.

4.1 Aktívny monitoring

Technológie aktívneho monitoringu užívateľskej skúsenosti sa založené na generovaní simulovaných transakcií a na meraní aplikačnej a transakčnej odozvy. Monitorovací agent pravidelne vysiela požiadavky cez celú sieť a odozvy aplikačného servera a sieťovej infraštruktúry sa logujú a vyhodnocujú.

Tento syntetický monitorovací prístup je veľmi efektívny a zodpovedá primárnemu cieľu manažmentu aplikačnej výkonnosti, ktorým je prevencia výkonnostných problémov ešte predtým, než ich vplyv spozoruje koncový užívateľ. Y toho dôvodu organizácie testujú vybrané časti svojej infraštruktúry, aby mohli identifikovať potenciálne úzke hrdlá sietí ešte predtým, než spôsobia narušenie business procesov.

Syntetický monitoring nedáva náhľad na skúsenosť a pozorovania koncového užívateľa, ak ten užíva virtuálny desktop interface (VDI) alebo desktop ako službu (DaaS) od svojho cloudového prevádzkovateľa služieb.

Na rozdiel od klasickej klient-server architektúry, VDI/DaaS prostredie využíva prezentačnú vrstvu, ktorá zabezpečuje grafické zobrazenie SW aplikácie, ktorá je prevádzkovaná v cloude na užívateľskom klientskom zariadení. To sa dá porovnať s TV prenosom, kde obrazovka TV prístroja len zobrazuje niečo, čo sa technologicky spracúva v štúdiu.

Základom riešení pre aktívny monitoring je evidencia okien eventov, udalostí (vytvorenie, pop-up, uzatvorenie) a z toho dôvodu musí byť kompletne prepracované pre VDI/DaaS prostredie tak, aby bolo schopné registrovať zobrazované schémy, obrazy.

Registrácia zobrazovaných schém, obrazov je časovo náročná a náchylná k chybám, následkom prekrývania okien. To spôsobuje nízku spoľahlivosť tejto metódy, ak sa používa v prostredí VDI/DaaS. To znamená, že monitorovací agent môže byť inštalovaný len v malej množine operačných systémov, v ktorých umožňuje predvídať výkonnosť a užívateľské reakcie na mobilných zariadeniach, alebo na inštaláciách s tenkým klientom.

4.1.1 Prínosy aktívneho monitoringu pre VDI/DaaS prostredie

Reálne prínosy aktívneho monitoringu:

- Monitoring sa robí na presne určených bodoch siete
- Výstupom z merania sú presné numerické hodnoty
- Veľký poet meraní podporu trendovú analýzu
- Je možné ľahko kvantifikovať KPI
- Umožňuje overiť vplyv ladenia parametrov na výkonnosť
- Zobrazuje vplyv zmien, alebo úprav, ako napr. inštalácia servisných balíkov, alebo bezpečnostných opravných modulov

4.1.2 Nevýhody aktívneho monitoringu v VDI/DaaS prostredí

Medzi nevýhody aktívneho monitoringu zaraďujeme:

- Agent spotrebúva viac CPU výkonu pre identifikáciu zmien šablón
- Agenta nie je možné inštalovať na server do prezentačnej vrstvy, lebo tam nie sú identifikovateľné šablóny
- Ak SW neodpovie presne nastavenou predpokladanou šablónou, meranie zlyhá

- Agent pravdepodobne používa syntetického užívateľa
- Nastavenie monitoringu nezodpovedá podmienkam reálnej prevádzky, lebo syntetický užívateľ využíva veľmi statické prostredie pre meranie
- Aktívny monitoring nepokrýva celý rozsah aktivít skutočného koncového užívateľa, lebo nepokrýva meraním:
  - Degradáciu audio prenosu
  - Zmeny asynchrónneho audio/video prenosu
  - Nepravidelný pohyb kurzora myšky
  - Oneskorenie zobrazovania klávesnicových vstupov
  - Spomalený prenos jednotlivých video snímkov (trhaný pohyb)
  - Problém scrolovania obrazovky
  - Monitoring v podstate neumožňuje vyvodiť závery, súvisiace so skutočnými príčinami níženia aplikačnej výkonnosti

V súčasnosti používané aktívne nástroje na monitorovanie sa často kombinujú s nástrojmi ktoré reportujú metriku procesných úrovní, ako napr. CPU, pamäť a vstupno-výstupné zariadenia. Táto metrika, sústava parametrov umožňuje IT oddeleniam meranie dostupnosti business služieb, ktoré sú sprístupnené koncovým užívateľom, ale neumožňuje im meranie aktuálnej kvality IT služby, tak ako sú vnímané koncovými užívateľmi.

Monitorovanie bezporuchovej prevádzkyschopnosti aplikácií už nestačí ako kľúčový parameter dodávky business služby. Nástroje aktívneho monitoringu nezabezpečujú dodŕžanie užívateľských parametrov koncových užívateľov v prostredí DaaS

4.2 Budúcnosť: Pasívny monitoring

Pasívny monitoring bude zabezpečovať pre operátora IT služieb monitoring aplikačnej výkonnosti a výkonnosti virtuálneho desktopu v súlade s užívateľovou produktivitou využívania služby. Na základe týchto údajov, operátor služieb môže dynamicky preveriť reklamácie užívateľa súvisiace s nedostatočnou aplikačnou výkonnosťou, určiť rozsah ovplyvnených užívateľov a determinovať primárnu príčinu

problému ešte skôr, než ovplyvní produktivitu práce pripojených užívateľov. IT organizácie zvýšia požiadavky na zber informácií, akými sú aplikačná a transakčná odozva a indexy spokojnosti koncových užívateľov, čo im umožní monitorovať aktuálnu rýchlosť aplikácií a ohodnocovať kvalitu uspokojovania požiadaviek koncových užívateľov. Pri budovaní pasívnych monitorovacích systémov bude možné využívať množstvo ušetrených zdrojov a výkonu CPU, ušetrenej sieťovej priepustnosti, cenovo prístupných dátových úložných priestorov a analýzu Big Data, ktorá dokáže spracovať enormné objemy dát, získaných z inštalovaných monitorovacích senzorov.

4.2.1 Funkčné požiadavky

Monitoring musí zodpovedať nasledujúcim kritériám:

- Úplná viditeľnosť prenosu dát: Všetky transakcie medzi aplikáciou a službou a každý prvok infraštruktúry musia byť monitorované. Riešenie musí byť nezávislé na aplikácii, operačnom systéme, programovaní, virtualizácii a infraštruktúre
- Štrukturálna viditeľnosť: Monitorovaní nástroj musí byť schopný vytvoriť topologickú mapu siete od jedného konca po druhý, musí zabezpečiť viditeľnosť infraštruktúry od druhej po siedmu vrstvu OSI modelu, sieť a úložiská musia byť zobrazené.
- Viditeľnosť celej trasy: agenti na oboch koncoch trasy, na strane servera a klienta, SNMP a WMI monitory musia umožniť vyobrazenie aplikačnej výkonnosti a výkonnosti podporných služieb tak, ako ich vníma koncový užívateľ. Kompletný získaný dátový set je potrebné odoslať na serverového klienta pre následnú koreláciu udalostí, analýzu základných príčin a odporúčanie riešenia problému
- Zisťovanie topológie. Tak, ako aplikácie a služby štartujú vzájomné interakcie a budujú workflow, monitorovacia aplikácia má začať budovať obraz topológie a trasu priebehu transakcie po jednotlivých krokoch ,medzi uzlami topológie a vybudovať virtuálnu a fyzickú mapu interakcie aplikácie so sieťovou infraštruktúrou
- Analýza základných príčin. Na základe tisícov uložených prípadov a pravidiel, ktoré sa kontinuálne rozširujú o prírastky na báze autolearningu, sa v monitoringu vytvára analýza základných príčin incidentu na základe deterministického princípu.

4.2.2 Architektúra

Monitorovací systém bude s veľkou pravdepodobnosťou pozostávať z riadiaceho systému (master), databázy, s manažmentského grafického interface (GUI). Musí obsahovať detailnú signalizačnú službu porúch a varovaní a dôsledný reportovací nástroj. Moderné monitorovacie systémy ponúkajú administrátorovi pomoc pri stanovení východzej základnej konfigurácie topológie transakcie. Je vhodné, ak monitorovací systém obsahuje súčasné moduly a prvky, ktoré predstavujú vývojové trendy v oblasti monitorovania. Dáta budú získavané prostredníctvom senzorov a SW agentov, ktoré sa dajú inštalovať na monitorovaný komponent infraštruktúry, alebo sa využije spolupráca vzdialených monitorovacích prvkov, akými sú SNMP senzory alebo WMI dopyty, ak budú prevádzkované v rámci základného riadiaceho systému monitoringu.

Je potrebné, aby celá komunikácia medzi agentmi a riadiacim systémom monitoringu bola bezpečná a kryptovaná. Komunikačná cesta by mala používať štandardný port 443 a štandardný https protokol, aby agenti mohli komunikovať cez proxy a firewally, chrániace prevádzkové prostredie.

4.2.3 Umiestňovanie agentov a výber dát VDI klienta, spracované senzorom

VDI klientske moduly, využívané v komplexných multitaskových operačných systémoch, môžu spôsobovať problémy aplikačnej výkonnosti a degradáciu užívateľských parametrov už sami o sebe. Jednoduchšie klientske operačné systémy, ako napríklad iOS alebo Android s jedným procesom v popredí sú menej náchylné k problémom, ktoré spôsobuje prevádzka klientskej aplikácie. NA druhej strane komplexné operačné systémy a prostredia vytvárajú priestor pre zložitejšie koncepty monitorovacích agentov.

Bez pochyby je potrebná inštalácia monitorovacieho agenta na VDI klienta, ktorý minimálne aspoň sleduje sieťové prepojenia, latenciu a transakčné správanie sa. V prostredí multitaskového operačného systému monitorovací agent môže ďalej prispievať k riešeniu problémov zaznamenaním a nahlasovaním systémových stavov (CPU, pamäť, diskové vstupno-výstupné rozhrania a prebiehajúce procesy)

» Merania nábehu VDI monitorovacieho SW klienta

Aj keď počas nábehu monitorovacieho SW klienta sa nezískavajú dôležité hodnoty, dávajúce náhľad na aplikačnú výkonnosť systému, tento proces je prvým viditeľným detailom pre koncového užívateľa. Ak je to možné, tak tento nábehový čas VDI monitorovacieho SW klienta, v ktorom prebieha autentifikácia klienta a jeho reprezentácia v monitorovacom SW by mal byť meraný. Ak klient zvolí aplikáciu a vzdialený desktop, tak sa realizuje relácia a inicializácia klientskeho obsahu a na prezentačnej vrstve musí začať vlastné meranie.

» Inicializácia obsahu VDI monitorovacieho SW klienta

Pri inicializácii relácie sa ošetrujú klientske zariadenia (Tlačiarne, drivery a pod.), čo môže spôsobovať značené zdržanie. Monitorovací agent by mal mať schopnosť zistiť tieto zdržania a reportovať ich späť riadiacej jednotke.

Senzor na riadiacej jednotke

Ak sa naštartuje desktop, alebo aplikácia VDI/SaaS infraštruktúry, vyvolá sa relácia (session) na riadiacej jednotke. Riadiaca jednotka realizuje program (programy), ktoré sú nakonfigurované na desktope alebo sú vyvolané definíciou vzdialenej aplikácie. To je dôvod, prečo je nutné umiestniť monitorovací SW klient aj na riadiacu jednotku.

» Meranie inicializácie relácie

Vytvorenie relácie (kontext) vyžaduje úplný „login“ proces. Počas login procesu sa realizujú skupinové politiky, Logon skripty, vytvára sa spojenie s rôznymi presmerovanými zariadeniami (tlačiarne, lokálne zariadenia, USB kľúče a pod.), ktoré ovplyvňuje nábeh desktopu, resp. aplikácií. Tento nábeh registruje, vníma koncový užívateľ. Čo je potrebné poznať k tomu, aby sme pochopili vnímanie a skúsenosť koncového užívateľa?

Potrebujem poznať fázy logon procesu, aké aktivity sa vykonávajú a čo spôsobuje, že nábeh relácie je pomalý:

- Dochádza k prenosu dát smerom na Active directory (RFS – resource facing service)
- Aktivuje sa komunikácia s Fileserverom (CFS – customer facing service) pre prenos logon skriptu a skupinových politík

- Nastáva výrazný prenos CFS k zdieľaným voľným profilom
- Určitý prenos je smerovaný k užívateľskému základnému directory (Homeshare)
- Určitý čas trvá spracovanie skupinových politík
- Určitý čas trvá spracovanie logon skriptu
- Samozrejme určitý čas spotrebuje aj CPU na vybudovanie obsahu relácie na riadiacej jednotke

Technicky to znamená, že je len jedno prepojenie medzi VDI klientom a riadiacou jednotkou, ale existuje mnoho prepojení z riadiacej jednotky smerom k backendovým službám (a to CFS, ako aj RFS). To je dôvod, prečo potrebujeme monitorovací agent/senzor aj na riadiacej jednotke a ak je to možné, tak aj na backendových službách.

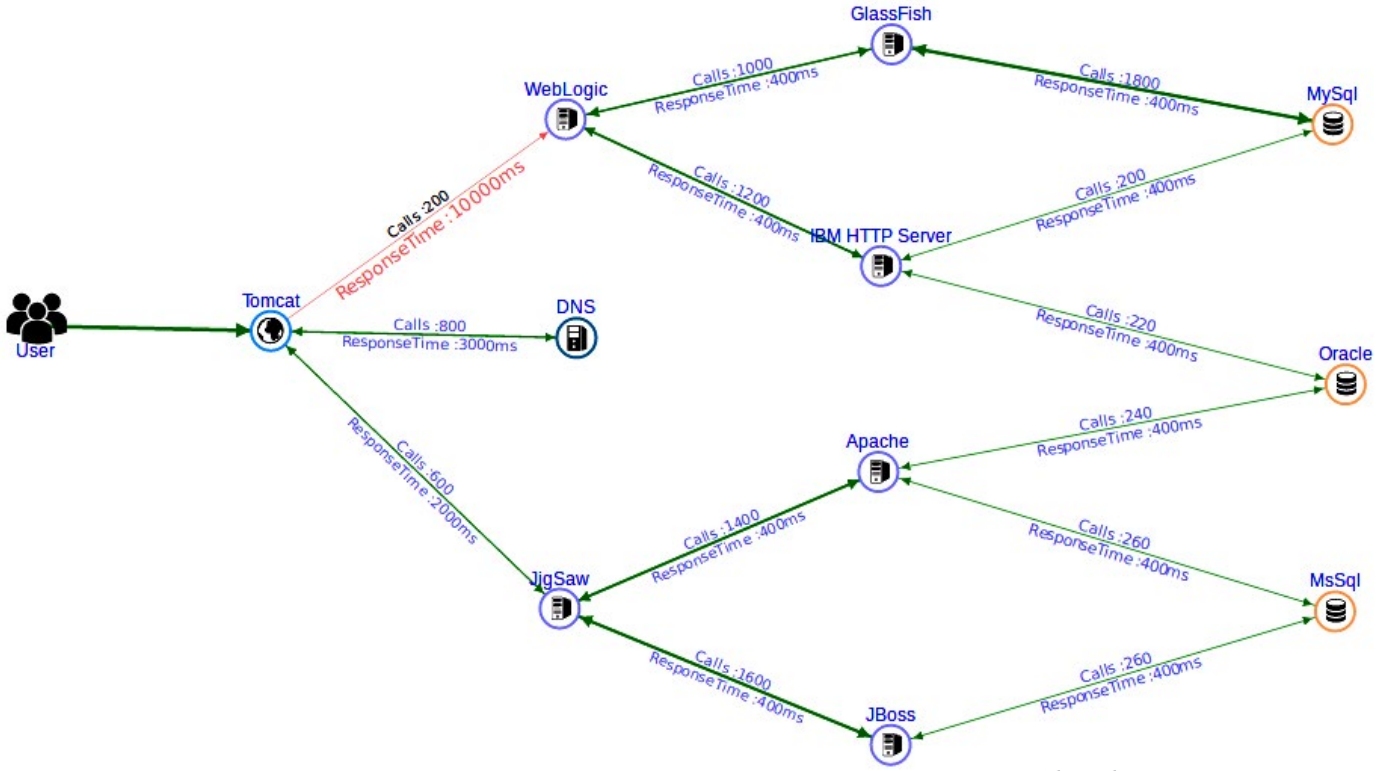
Od momentu, keď relácia na riadiacej jednotke môže byť priradená ku koncovému užívateľovi, môže byť pridaná k celkovému obrazu, ak monitorovací agent zaznamená túto informáciu spojenú s riadiacou jednotkou. Je vysoko pravdepodobné, že koncový užívateľ nebude reklamovať pomalosť publikovaného desktopu, ale bude poskytovať popis problému koncipovaný ako napr. „Moja ERP aplikácia nefunguje", alebo „moje video z WEB je pomalé", alebo „Moje Office aplikácie sú pomalé, keď loadujú dáta".

Aplikačná výkonnosť

Výkonnosť aplikácií, ktoré sú prevádzkované na riadiacej jednotke v rámci relačného obsahu, je závislá na viacerých faktoroch :

- CPU takt na riadiacej jednotke
- Obsiahnuteľná RAM na riadiacej jednotke, pretože stránkovanie pamäte spôsobuje oneskorenie
- Šírka prenosového pásma siete od riadiacej jednotky k backendovým infraštruktúram
- Transakčné spomalenie backendových služieb (CFS a RFS)
- Úzke výkonnostné hrdlo hypervizora (monitora virtuálneho servera)
- Úzke výkonnostné hrdlo dátového úložiska pripojeného k hypervizoru

Záverom, pre monitorovanie výkonnosti čo i jedinej aplikácie je potrebné korelovať údaje z rôznych monitorovacích agentov/snímačov. A v tomto bode nastáva kľúčová príležitosť pre Big Data analýzu. Monitorovací systém musí pochopiť topológiu aplikácie. Tú to znalosť, závislosti je možné zadať ručne do monitorovacieho systému, ale lepšie monitorovacie systémy zabezpečia automatické rozpoznanie a znázornenie topológie.



Obrázok 1
Aplikačná topológia

Snímače backendových systémov

Zobrazenie aplikačnej topológie dokumentuje, že je dôležité inštalovať monitorovacích SW agentov aj priamo na backendové systémy. Mnohé zákaznícky orientované služby (CFS), ako napr. file service sú závislé na zdrojoch pripojených na systémoch (AD pre autorizáciu, DNS, a pod.) a preto analýza základných príčin a problémov je možná len vtedy, ak všetky transakčné údaje takýchto služieb sú zaznamenávané a uložené v master databáze riadiacej jednotky.

4.2.4 Funkcia prídavných snímačov (agentov) – informácia koncovému užívateľovi

Autor je presvedčený, že posielanie stavových informácií koncovému užívateľovi je kľúčovou aktivitou monitoringu a z toho dôvodu implementované riešenie musí zabezpečiť spätnú väzbu systémového stavu pre užívateľa, zákazníka.

Proaktívna informácia koncového užívateľa je cestou, ako znížiť počet hlásení porúch na service desk. V prípade degradácie výkonnosti systému monitorovací agent GUI na klientskom zariadení má byť využitý na notifikáciu pre koncového užívateľa. Pre sieťové prepojenie je to možné realizovať vyznačením opozdenia číslom a farebnou indikáciou (červenou, jantárovo žltou, zelenou farbou) a pre backendové zariadenia je možné využiť pop up balónikový odkaz, ktorý poskytne stav merania a odhad zdržania procesu, takže užívateľ nemusí v takom prípade volať help desk a žiadať informáciu o dôvode zdržania a môže si podľa statusových informácií naplánovať práce s aplikáciou s vedomím aktuálnej latencie.

4.2.5 Prínosy pasívneho monitoringu v VDI / DaaS prostredí

Pasívny monitoring má viacero prínosov:

- Zabezpečuje údaje z reálneho prostredia a práce užívateľov
- Sníma údaje od každého užívateľa
- Sníma a spracúva údaje od veľkého množstva agentov a snímačov
- Vyhodnocuje transakčné dáta súvisiace s výkonnosťou a umožňuje koncovému užívateľovi predvídať správanie a výkonnosť aplikácií
- Zjednodušuje analýzu hlavných príčin problémov
- Umožňuje stanoviť trendy pre všetky zapojené systémy

4.2.6 Negatíva aktívneho monitoringu v VDI / DaaS prostredí

K negatívam aktívneho monitoringu je možné zaradiť:

- Nie je možné merať parametre typu „trvanie Logon“
- Nie je zabezpečená opakovateľnosť merania identickej aplikačnej interakcie
- Nie je možné okamžité varovanie, ak aplikácia spadne

5. Benchmarking, záťažový a stress test, regresné testy

V súčasnosti sa benchmarkové testy, záťažové testy a regresné testy zabezpečujú aktívnymi monitoringovými systémami. Záťažové a stresové testy dodávajú jasnú a presvedčivú odpoveď na nasledujúce otázky:

- Zhavaruje sa moja aplikácia pod záťažou ?
- Zabezpečím preddefinovanú výkonnosť systému ?
- Koľko súčasných (simultánnych) užívateľov zvládne moja stránka ?

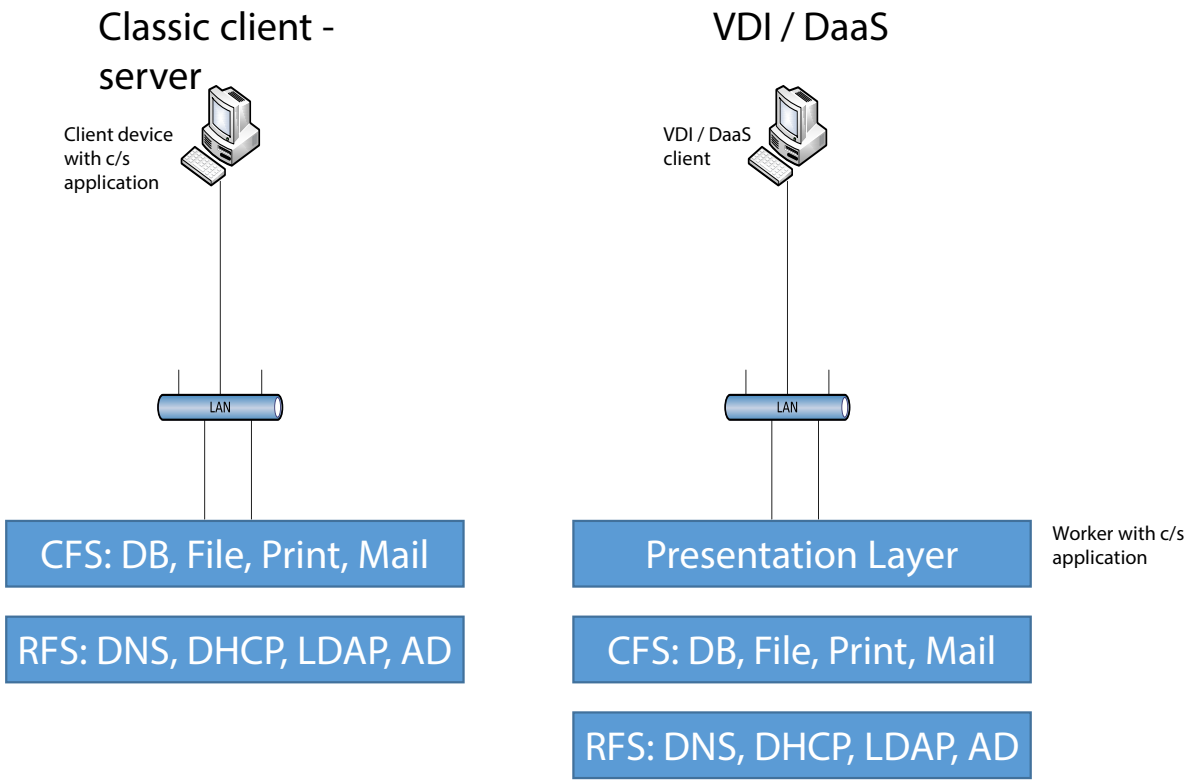
Ako bolo uvedené v negatívach aktívnych monitorovacích systémov, obsah užívateľskej relácie a simulované jedinečné zaťaženie koncového užívateľa sú syntetické, monitoringom získané dáta sú vhodné len na porovnanie s inými systémami a pre trendovú analýzu. Odpoveď na otázku, či sa systém preťaží je možná, ale test nie je zameraný na hlavnú príčinu preťaženia systému.

Je možné realizovať regresné testy, ktoré overia tieto vplyvy:

- Vplyv nového nastavenia tuningových parametrov (doladenia systému)
- Zmeny vplyvom update, napríklad servisných balíčkov, alebo bezpečnostných zlepšení
- Zmeny architektúry
- Zmeny CFS a RFS
- Hardwarové zmeny

6. Detailnejší pohľad na Desktop, ako službu (DaaS)

Nové riešenia distribuovanej výpočtovej architektúry a metódy agilných, dynamických aplikácií vytvorili podmienky, že výpočtové riešenia sú podstatne viac škálovateľné a dynamickejšie, ako kedykoľvek predtým. VDI/DaaS prostredia so všetkými komponentami (okrem klientskeho zariadenia) sú veľmi zložité.



Obrázok 2
Klient server architektúra v porovnaní s VDI riešením

V porovnaní s klasickým klient server prostredím, VDI/DaaS potrebuje ďalšiu prezentačnú vrstvu. Pre manažérsky team, zodpovedný za monitoring je nie najvhodnejšou skutočnosť, že typické VDI/DaaS riešenie je súčasťou WAN, resp. korporátneho WAN prostredia, ktoré pridáva ďalšie komponenty do komunikačnej cesty medzi klientom a prezentačnou vrstvou.

Diskusie s VDI/DaaS zákazníkmi poukazujú na nedostatky typických SLA kontraktov:

- Neschopnosť adekvátne definovať ponúkanú službu
- Neschopnosť definovať spôsob merateľnosti ponúkanej služby
- Výluky počas plánovaných servisných zásahov bez toho, aby bola definovaná frekvencia servisných aktivít, notifikácie a výpadky z dôvodu servisu
- Neschopnosť rozlišovať čiastočné výpadky (ako napríklad spomalenie, obmedzenie kapacít, nespôsobilosť odštartovať novú desktop reláciu) od úplných výpadkov služby, vrátane straty celej rozpracovanej práce

- Výpadky funkcionality zariadení, ktoré sú dedikované jednotlivým zákazníkom, ale nad ktorými zákazník nemá priamu kontrolu
- Exkluzívne priradenie zodpovednosti za monitorovacie služby na zákazníka
- Neschopnosť vykázať chyby, spôsobené dodávateľom služby
- Neschopnosť vykázať zlyhanie SW infraštruktúry
- Neschopnosť vykázať zlyhanie konektivity k dátovému centru
- Neschopnosť dokumentovať kompenzačnú úroveň vyvolanú nedodržaním SLA podmienok

Množstvo a rozsah slabých stránok SLA je náznakom toho, že podstatná časť dodávateľov VDI/DaaS (či už interných, alebo externých) musí ešte popracovať na plnom pochopení podstaty služby, ktorú ponúkajú.

DaaS musí byť taká istá služba, ako iné utility, tak ako užívateľ nemusí ovládať otázky zložitosti elektrickej siete na to, aby používal elektrickú energiu na kúrenie, alebo osvetlenie svojej domácnosti, tak isto DaaS užívateľ nemusí rozumieť a pochopiť technológiu, ktorá je využívaná na to, aby mu bola služba sprístupnená.

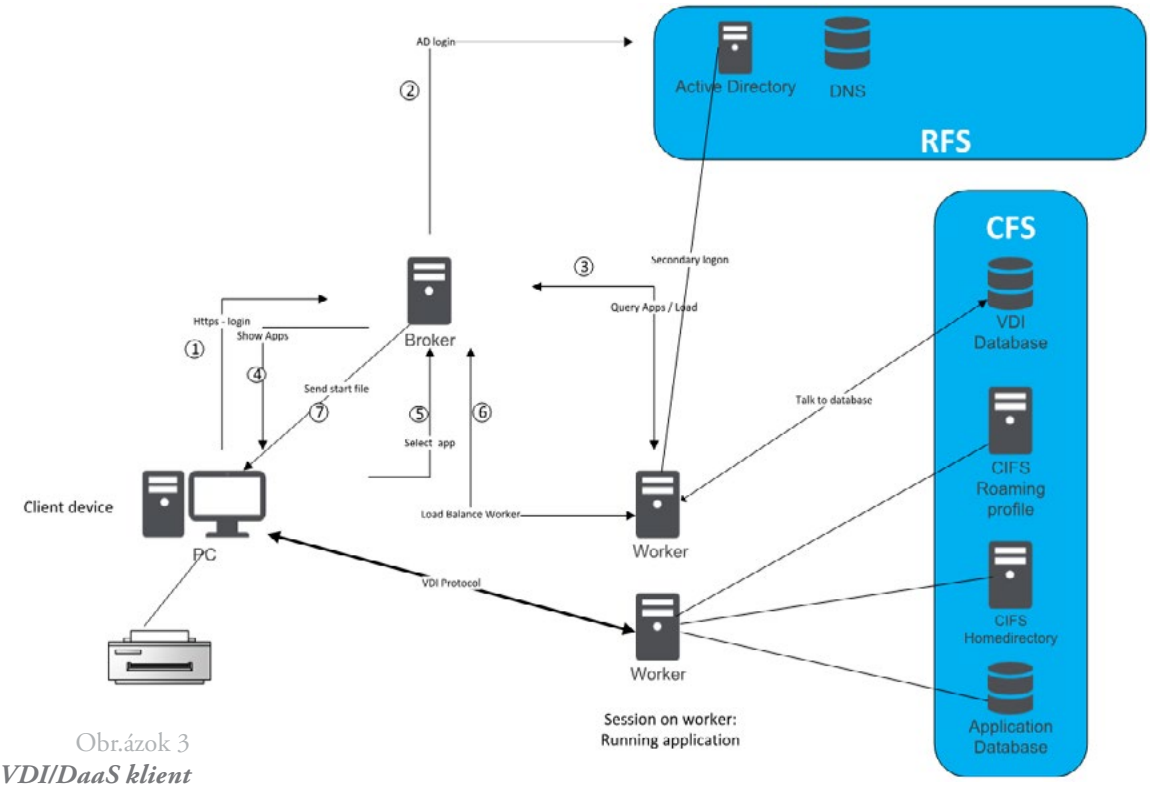
Pozícia, poloha klientskych zariadení v sieti (LAN/WAN) a využívanie virtualizácie (servery, sieť, úložiská) a integrácia hybridných cloudov definuje zložitosť prostredia. Napriek tomu, sťažnosti podávané koncovými užívateľmi (spravidla spôsobené problémami koncových užívateľov) sú si veľmi podobné.

Na čo si môže sťažovať užívateľ?

- Pomalý nábeh VDI klientskeho komponentu
- Pomalý nábeh aplikácie
- Nedostatočná výkonnosť aplikácie
- Nepravidelné odozvy pohybu kurzora a klávesnicových vstupov
- Pomalý a nepresný scrolling v aplikáciách, ako MS Excel
- Asynchrónne správanie sa videa a audia
- Nekvalitný zvuk, audio

6.1 VDI/DaaS v spolupráci s LAN klientom (najjednoduchší prípad)

V tomto čistom LAN prostredí je pozorovateľná celá komunikácia medzi klientskym zariadením a riadiacou jednotkou, nie je zapojený hypervisor alebo úložný subsystém.



Obr.ázok 3
VDI/DaaS klient v LAN prostredí

6.1.1 Príčiny výkonnostných problémov pre tento scenár

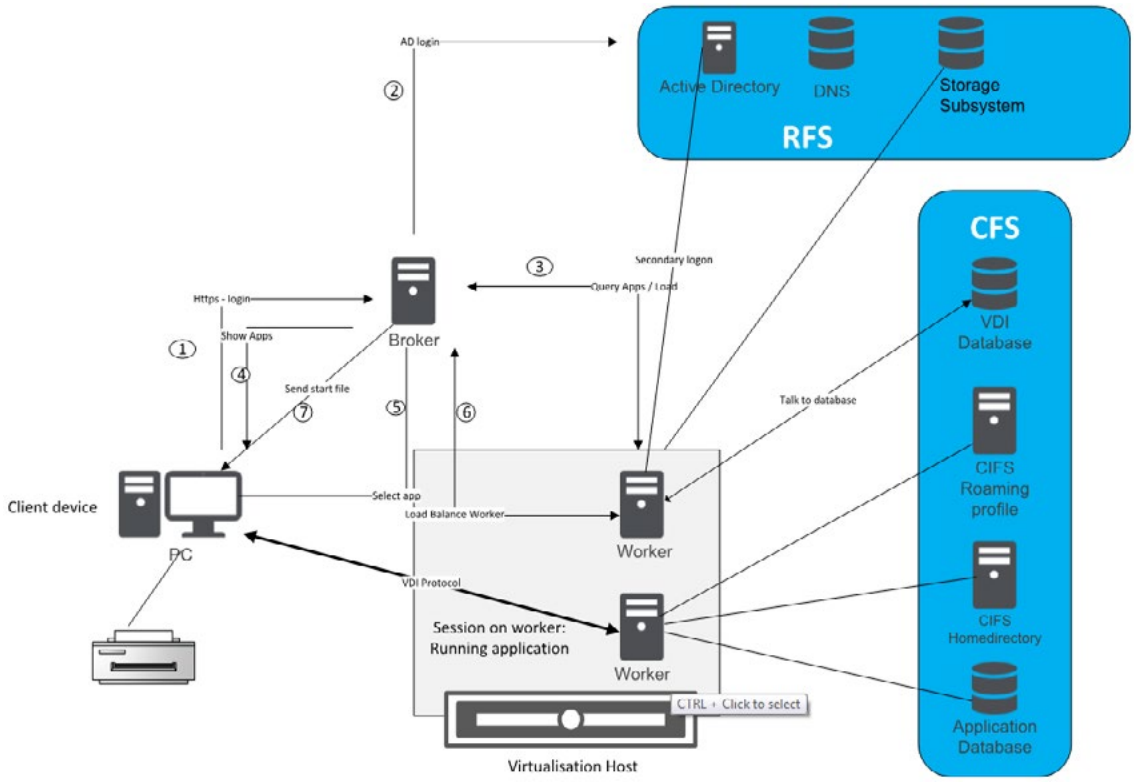
- Ak login je pomalý, pravdepodobnou príčinou je, že Broker server je preťažený a preto je základnou príčinou problému výkonnosti. Ľahko môže nastať interakcia active directory (AS) a XML query (dopytov) a následkom AD a XML chýb konfiguračného servera môže dôjsť k výraznému (až 30 sec) zdržaniu (timeout) počas nábehu VDI klienta.
- Aplikačný nábeh vyžaduje kompletný login proces (minimálne to platí pre prvú aplikáciu, štartujúcu na riadiacej jednotke pre konkrétneho užívateľa). Login proces je zložitý a zaťažuje riadiacu

jednotku. Sieťové interakcie s CFIS, zdieľajúcim roamingový profil, sú vysoké.

- Ak aplikácia nedosahuje požadovanú výkonnosť, môže to byť problém nedostatočných zdrojov (CPU, RAM) alebo sieť spôsobuje oneskorenia na pozadí procesov. RAM môže spôsobovať problém kvôli stránkovaniu, ak užívateľ využíva svoj hard disk pre stránkovanie, tak sa môže zmeniť užívateľská skúsenosť s aplikáciou.
- Sťažnosti súvisiace s myšou, alebo klávesnicou sa nemajú prečo objavovať v LAN limitovaných inštaláciách, pretože predstavujú veľmi malé paktety a prepojenie je spravidla s priepustnosťou rádovo v Gigabitoch/s
- Pomalé, resp. nepresné scrolovanie je tiež najčastejšie pozorované v WAN aplikáciách, ale môže nastať aj v LAN prostredí, aj je používaný veľmi poddimenzovaný HW klientskeho zariadenia

6.2 VDI/DaaS v spolupráci s virtualizovaným LAN klientom

Obrázok 4
Virtualizovaný VDI/DaaS klient v LAN prostredí

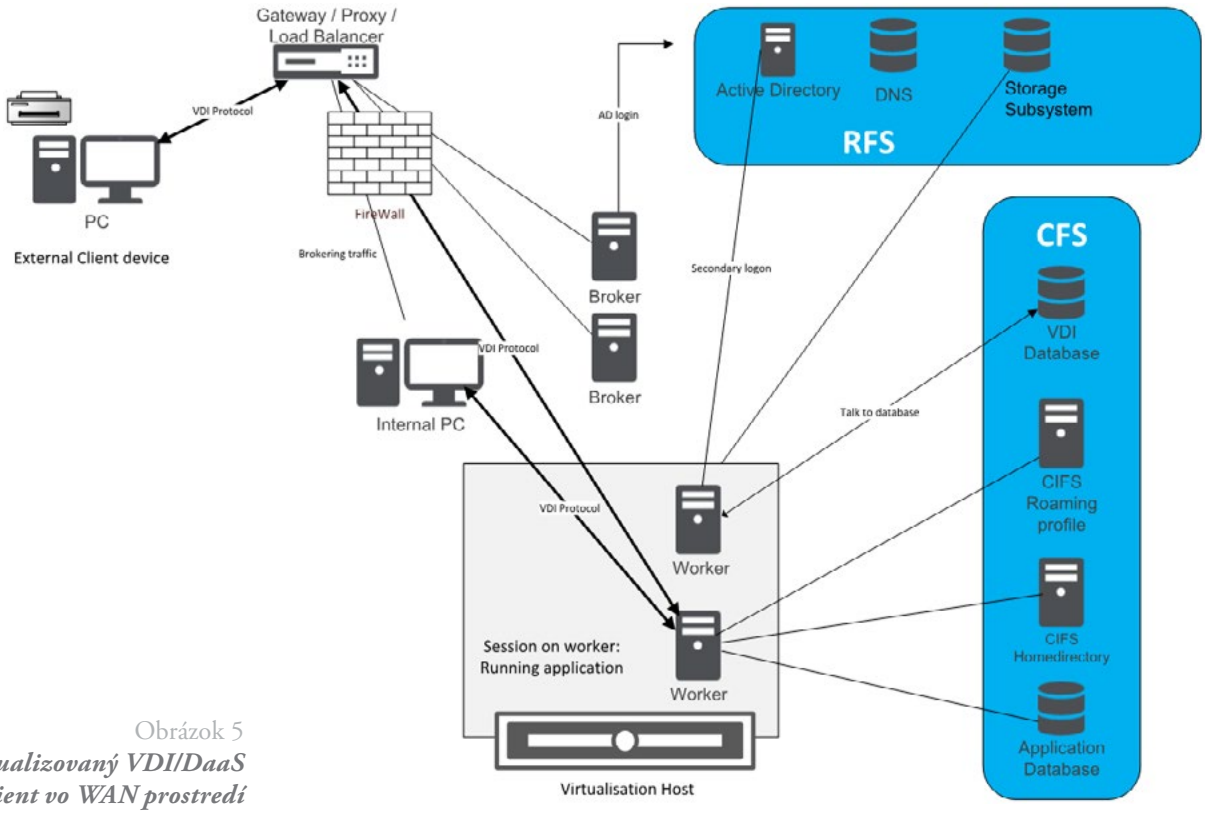


V tomto čistom LAN prostredí je pozorovateľná celá komunikácia medzi klientskym zariadením a riadiacou jednotkou, ale pribudla virtualizačná vrstva (hypervisor) a úložný subsystém.

6.2.1 Príčiny ďalších výkonnostných problémov pre tento scenár

Dôvody sťažností sú podobné, ako v prvom popísanom scenári. Monitorovaná zložitosť narástla, pretože pribudol hypervisor a úložný priestor. Hypervisor a úložný priestor môžu prispieť k latencii prenosov v systéme. Aj keď end to end transakčný čas vybranej aplikácie je výborný, môže dôjsť k situácii, že nižšia úroveň je pomalá, stagnujúca, napríklad následkom nedostatočnej výkonovej rezervy CPU, pridelenej pamäte alebo následkom iného backgroundového procesu, ktorého zdroje sa zacyklia a tak vnímanie koncového zákazníka bude jednoznačne nespokojnosť.

6.3 VDI/DaaS klient vo WAN sieti



Obrázok 5
Virtualizovaný VDI/DaaS klient vo WAN prostredí

V tomto scenári je zakomponovaný vzdialený prístup cez gateway/proxy server, takže celá komunikácia medzi externým klientskym zariadením a riadiacou jednotkou nie je „viditeľná“. Nájdeme tu hypervisor s priradeným úložným priestorom a Broker server, ktorý je redundantný s Load (záťažové vyrovnanie) balancingom na g/w. Spravidla g/w (gateway)/proxy server sú umiestnené v demilitarizovanej zóne (DMZ), takže celá komunikácia musí prechádzať cez f/w (firewall).

6.3.1 Príčiny prídavných výkonnostných problémov pre tento scenár

Dôvody sťažností sú podobné, ale komunikácia medzi externým klientom a riadiacou stanicou musí prechádzať dvomi firewallmi a potom je oprávnená na prístup k g/w. Gateway sa využíva pre autentifikáciu a autorizáciu užívateľa, čím vzniká prídavná potreby monitorovať sieť a jej výkonnosť smerom k a od active directory (AD).

Ak sa užívatelia sťažujú na reakcie myši a klávesnice, hlavná príčina spravidla spočíva v oneskorení (latency) siete medzi klientskym zariadením a g/w. Pomalé a nepresné scrolovanie je pozorovateľné v prípade, ak nie je dostatočná priepustnosť siete medzi klientskym zariadením a g/w, ktorý zabezpečuje prístup klienta.

6.4 Použité výrazy a definície

Vzhľadom k skutočnosti, že niektoré výrazy sa používajú v rôznych IT kontextoch, je potrebné definovať ich význam, aby umožnili správne pochopenie tejto Bielej knihy.

» Klientské zariadenie

Klientské zariadenie je zariadenie koncového užívateľa, ktoré sprostredkuje prístup k zdrojom, publikovaným prostredníctvom poskytovateľa VDI/DaaS

» Klientsky SW VDI

Klientský SW VDI je komponent, ktorý je zodpovedný za komunikáciu z klientskeho zariadenia k VDI/DaaS infraštruktúre

» Klientské zdroje

Klientské zdroje sú tlačiarne, pevné disky, CD ROM, audio, USB a pod. Všetky tieto zdroje sú lokálne z pohľadu klientskeho zariadenia.

» Gateway (g/w)

Gateway je bezpečný proxy server pre údaje, ktoré sú transportované do WAN z a do vzdialeného klientskeho zariadenia. S veľkou pravdepodobnosťou gateway bude zabezpečovať autentifikáciu a autorizáciu koncového užívateľa.

» Riadiaca jednotka

Riadiaca jednotka môže byť vzdialený host (napríklad terminálový ktorý server), ktorý ponúka relácie, alebo Windows - klientský operačný systém, kontrolovaný prostredníctvom VDI/DaaS SW.

» Relácia

Je obsahom riadiacej jednotky, kontextom. V rámci relácie sa naštartuje aplikácia. Relácia (kontext) sa uskutoční po kompletnom Login procese k danej riadiacej jednotke a závisí na systéme. Relácia buď zdieľa riadiacu jednotku s niekým iným (vzdialený desktop host) alebo riadiaca jednotka je dedikovaná pre reláciu (OS pracovnej stanice)

» Web GUI

Web GUI – grafický užívateľský interface zabezpečuje pre koncového užívateľa grafickú prezentáciu VDI/DaaS dostupných zdrojov.

» Broker

Broker poskytuje informácie od dostupných zdrojoch, nezaťažených riadiacich jednotkách a pod. Vo väčšine VDI/DaaS prostrediach je broker zodpovedný za vyváženie zaťaženia a prepojenie existujúcich, alebo rozpojených relácií.

» Užívateľsky orientované služby (CFS)[1]

Užívateľsky orientované služby sú služby vyššej úrovne, ako napr. Súbor-, Print-, Databázová služba-, CRM aplikačný host a i.

» Zdrojovo orientované služby (RFS)[2]

Zdrojovo orientované služby sú backendové procesy ako napr. Active directory, DHCP, DNS, LDAP a pod.

» Fyzické alebo virtuálne infraštrukturálne komponenty

Infraštrukturálne komponenty sú servery, alebo hypervisory, ktoré sú prevádzkované na riadiacich jednotkách, dátových úložiskách, sietiach, smerovačoch (routeroch) , firewalloch a pod.

[1] Customer Facing Service (NGOSS): http://tinyurl.com/k65xzn2
[2] Resource Facing Service (NGOSS): http://preview.tinyurl.com/k65xzn2

7. Právne informácie

7.1 Všeobecná informácia

Informácie, ktoré sú obsiahnuté v tejto Bielej knihe slúžia k ilustrácii vybraných a všeobecných právnych aspektov v súvislosti s cloudovými technológiami. Ich účelom nie sú relevantné vecné právne informácie alebo náhrada právneho poradenstva, lebo takéto aktivity vždy vyžadujú poznanie individuálnej situácie a faktorov pre konkrétne riešenia.

7.2 Obsah príručky

Autor a vydavateľ tejto Bielej knihy nepreberá zodpovednosť za úplnosť, presnosť a platnosť poskytnutých informácií. To sa zvlášť vzťahuje na otázky aktuálneho vývoja a jeho odrazu v právnych otázkach. Reklamácie škody voči autorom a vydavateľom, súvisiace s vecnými a nevecnými škodami, spôsobenými využívaním, alebo nevyužívaním informácií z tejto Bielej knihy, alebo následkom nekorektných, alebo neúplných informácií z príručky sú neopodstatnené.

7.3 Odkazy a linky

Na margo priamych a nepriamych odkazov na externý obsah (napr. linky a hyperlinky) mimo sféry zodpovednosti autora a vydavateľstva, zákonná zodpovednosť sa dá uplatniť len v prípade, ak autor a vydavateľ boli informovaní o obsahu odkazov a bolo technicky možné a uskutočniteľné zabrániť využívania nelegálneho obsahu. Autor a vydavateľ týmto jasne deklarujú, že v čase umiestnenia odvolávky a odkazu v texte nebol identifikovaný žiadny ilegálny obsah v odkázaných zdrojoch a na Web stránkach. Autor a vydavateľ nemajú žiadny vplyv a dosah na súčasný design, obsah a vlastníctvo linkovaných stránok. Autor i vydavateľ sa jednoznačne dištancujú od zmeny obsahu ktorejkoľvek z Web stránok, ktorá nastala po zapracovaní linky a odkazu do tejto Bielej knihy. Autori a vydavateľ nenesú žiadnu zodpovednosť

za nelegálny, chybný a nesprávny, respektíve neúplný obsah a žiadna škoda, spôsobená z využívania, resp., nevyužívania týchto ponúknutých informácií zostáva výhradne v pôsobnosti poskytovateľa referovanej Web stránky a nie na strane autora, ktorý uviedol odkazy a linky vo svojej publikácii.

7.4 Autorské práva

Obsah Bielej knihy, jej texty, grafické vyobrazenia a obrázky sú autorsky chránené podľa rakúskeho právneho poriadku a autorského zákona. Použitie a využitie, ktoré nie je v súlade s autorským zákonom, vyžaduje vopred získaný písomný súhlas vydavateľa. Príspevky tretích strán sú vyznačené a citované. Uvedené sa vzťahuje na reprodukcie, úpravy, umiestňovanie obsahu do databáz, alebo iných elektronických médií. Neautorizované reprodukcie, alebo zverejnenie príručky, alebo jej častí, je explicitne zakázané. Individuálne a súkromné používanie je výnimkou z uvedeného, ale súkromné využívanie príručky nezahrňuje práva jej zverejňovania tretím stranám. To isté sa vzťahuje na publikovanie príručky, alebo iné práce súvisiace s ňou.

7.5 Poplatky

Táto Biela kniha je pre odberateľov a prijímateľov bez poplatkov.

8. Autor



Reinhard Travniček

Technology X-tech obchodná spoločnosť
Riaditeľ

Haupstrasse 157
2231 Strasshof, Rakúsko
T: +43 2287 3928-23
M: +43 699 13928 023
Reinhard.travnicek@x-tech.at

Foto: autorské práva: Michael Fristscher
X-tech je sponzorujúcim partnerom Eurocloud Austria

Eurocloud Slovakia, o. z.

Konopná 52
821 05 Bratislava

E-mail: eurocloud@eurocloud.sk
Web: http://www.eurocloud.sk