

Optimalizace správy konfigurace na ZČU

Michal Švamberg
Západočeská univerzita v Plzni
Centrum informatizace a výpočetní techniky
email: svamberg@civ.zcu.cz

13. května 2008

Abstrakt

Předkládaný projekt se zabývá nalezením, ověřením a implementací nástroje pro optimalizaci správy konfigurací ve výpočetním prostředí Západočeské univerzity s ohledem na zvýšení celkové bezpečnosti.

V projektu bude provedeno srovnání a výběr softwarového nástroje, který bude nasazen pro správu konfigurace v heterogenním výpočetním prostředí. Nástroj bude implementován do současné infrastruktury s důrazem na napojení na instalační mechanismus FAI.

1 Současný stav řešeného problému

K dnešnímu dni není uspokojivě vyřešena centrální správa konfigurací pro stroje připojené do sítě. Nyní existuje několik způsobů jak takovou konfiguraci provádět, avšak žádnou z nich nelze považovat za vhodnou do tak rozsáhlého prostředí jako je univerzitní síť.

Jedno z úložných míst pro konfiguraci strojů je instalační mechanismus FAI¹, ten se používá při instalaci a je nemyslitelné provádět reinstalaci při každé změně. Druhé úložné místo konfigurací je AFS, to ovšem slouží jen pro vybrané služby (DHCP, DNS, Kerberos, ...) a na klientech musí být implementovány skripty, které zajišťují jejich pravidelnou obnovu a restarty příslušných služeb.

Protože tento stav nebyl dlouhodobě udržitelný, byla vypsána bakalářská práce, jejímž výsledkem je skript, který spolupracuje s informacemi z doby instalace stroje a je tak částečně navázán na FAI. Tento skript je nasazen od loňského léta a velmi zlepšil možnosti změn konfigurací. Jeho velkou nevýhodou je bezpečnost a problémy se syntaktickými chybami při přípravě změn v konfiguracích.

Morálně zastaralá Moira a projekt Athena pro management konfigurací nelze v dnešních systémech rozumně používat. Proti jejímu používání stojí obzvláště problémová administrace a zastaralé možnosti pro napojení na okolní systémy.

¹<http://www.informatik.uni-koeln.de/fai/>

Nejčastěji používaný způsob konfigurace je vzdálený přístup. Ten je preferovaný pro samostatné zásahy na serverech, nikoliv ovšem pro hromadné změny na stovkách strojů². Z bezpečnostních důvodů je na stanicích uživatelů zakázán vzdálený přístup, což významně omezuje možnost změn v konfiguraci.

2 Cíle řešení

Výsledkem projektu bude implementace nejvhodnějšího nástroje do výpočetního prostředí. Tento nástroj bude sloužit k hromadné konfiguraci a správě operačních systémů v síti. Tímto krokem si slibujeme snazší a přehlednější správu, kde bude vidět historie úprav. Nezanedbatelný bude také bezpečnostní přínos.

Kritéria pro výběr nástroje vychází ze současného stavu a potřeb. Bude požadována návaznost nástroje na informace z instalační procedury, tak aby jednotlivé úpravy na stroji prováděl podle služeb, které jsou na stroji provozovány. Důležitým bodem bude možnost navázání na některé z existujících úložišť konfigurací. Taktéž budeme požadovat, aby existovalo nějaké řešení pro uchování historie změn. Jako samozřejmost bude požadována zpětná vazba v případě chyby.

Součástí projektu bude ověření vlastností v praxi a jeho použitelnost zvláště při hromadných změnách konfigurací. To je důležité z pohledu bezpečnosti, kde velkou roli hraje čas. Například v případě ohlášení bezpečnostní chyby je většinou mezi prvními řešeními rekonfigurace systému. Například přenastavení firewallu tak, aby dotčená služba nemohla být napadnuta. Právě toto je typický případ, kdy se vybraný nástroj pro správu konfigurací osvědčí nejvíce. Přestože se v této žádosti mluví o správě strojů, je zde míněna (a tento zjednodušený příklad to potvrzuje) optimalizace poskytování a správa služeb, jež jsou na daných strojích provozovány.

Cílem projektu není nasazení nástroje přes všechny spravované stroje, ale jeho nalezení, příprava nastavení, ověření provozu, možností a zhodnocení. Tento projekt má nastartovat a připravit nový způsob správy konfigurace v síti ZČU, jenž se bude po ukončení projektu dále rozšiřovat o další spravované stroje.

Jako již v dřívějších grantech 154R1/2005 a 192R1/2006, bychom rádi umožnili přístup k tomuto rozvojovému projektu také studentům. Centrum informatizace a výpočetní techniky (CIV) již řadu let umožňuje studentům podílet se na správě výpočetního prostředí, za což dostávají přiměřenou odměnu ve formě stipendia. Zapojením studenta do projektu se předpokládá zvýšení jeho kvalifikace a umožnění nahlédnutí do procesu správy rozsáhlejší výpočetní infrastruktury.

V projektu se počítá s navštívením zahraniční konference, která se orientuje na administraci systémů a sítí. Zde bychom rádi získali kontakty a informace od ostatních institucí ve světě, jak dotčený problém řeší. Zároveň chceme získat informace o nových způsobech správy, nástrojích a jejich využití v praxi. Od konference si slibujeme získání informací ohledně správy systémů s ohledem na zlepšení celkové bezpečnosti.

²Předpokládá se správa více než 150 serverů a cca 300 uživatelských stanic.

3 Způsob řešení

Projekt se bude řešit ve dvou fázích. V první fázi bude výběr z vhodných kandidátů a srovnání jejich vlastností. Na základě získaných informací bude následovat seznámení se s nástrojem a experimentální nasazení na serveru. V této fázi bude vybraný nástroj nastaven tak, aby co nejvíce vyhovoval existující infrastruktuře. Pokud nastanou nepřekonatelné obtíže, vyzkouší se pro experimentální nasazení nástroj, který se umístil jako další v pořadí. Zde je třeba zdůraznit, že nebudou prováděny žádné úpravy v kódu nástroje a budeme se snažit navázat na výpočetnímu prostředí provést formou změny konfigurace.

Po ukončení přípravné fáze se začne ověřovací provoz. Napřed nasazením na menší skupinu spravovaných strojů, která se postupně bude rozšiřovat. Tuto úvodní skupinu budou tvořit vývojové servery a několik stanic z veřejných učeben. Na základě získaných zkušeností z ověřovacího provozu budou provedeny případné úpravy a rozhodnuto o dalším rozšíření nástroje.

Na projektu se bude podílet alespoň jeden student, jemuž pod vedením řešitelů bude umožněn přístup a možnost podílet se na přípravě a provozu nově zaváděné technologie do heterogenního prostředí ZČU. Tento přístup se nám velmi dobře osvědčil již v předchozích projektech a rádi bychom v něm pokračovali.

Cestovné a konferenční bude využito pro účast dvou osob na mezinárodní zahraniční konferenci, která bude zaměřena na problematiku správy služeb, jejich optimalizaci a poskytování. Jako typickou konferenci co do rozsahu a zaměření lze předpokládat SANE³, jejíž konání organizátoři předpokládají v roce 2009. Lze ovšem předpokládat účast na jiné konferenci s obdobným zaměřením, která by lépe časově vyhovovala projektu, tak aby získané informace mohly být uplatněny co nejdříve.

4 Prezentace výsledků

Odborné materiály, získané poznatky, použitá řešení a výsledky související s řešením projektu budou zájemcům dostupné v elektronické formě prostřednictvím WWW stránek CIV, ZČU v Plzni.

Klíčové výstupy budou prezentovány formou semináře nebo konference. Ke stěžejní prezentaci výsledků bude patřit přednáška pro odbornou veřejnost na některé z národních konferencích zabývající se tematikou správy systémů. Lze předpokládat prezentaci na konferenci se zaměřením jako jsou EurOpen.CZ nebo LinuxAlt.

Za neméně důležitý bude seminář pro zaměstnance CIV. Zde bude prezentace výsledků a seznámení se s novou technologií pro správce, která může zasahovat do oblastí, které sami spravují.

³<http://www.sane.nl/>

5 Charakteristika řešitelského týmu

Řešitelský tým je složen ze zkušených pracovníků Laboratoře počítačových systémů Centra informatizace a výpočetní techniky na Západočeské univerzitě v Plzni. Řešitelský kolektiv má zkušenosti z oblasti správy operačních systémů a jejich implementace do infrastruktury distribuovaného výpočetního prostředí. Do řešitelského týmu bude také vybrán student⁴, který bude mít zájem na projektu spolupracovat.

Řešitelský kolektiv tvoří:

Ing. Michal Švamberg (hlavní řešitel) je absolventem Fakulty Aplikovaných věd Západočeské univerzity v Plzni v oboru Distribuované systémy. Od roku 2002 pracuje v Laboratoři počítačových systémů, Centra informatizace a výpočetní techniky, kde se účastnil návrhu a budování kolejních sítí Západočeské univerzity. Dále se zabývá správou operačního systému Linux a jeho integrací do distribuovaného výpočetního prostředí Orion. Spravuje také FibreChannel infrastrukturu, distribuovaný souborový systém AFS. Na ZČU působí jako instruktor v certifikačních programech CCNA a CCNP⁵.

Ing. Oldřich Balák (spoluřešitel) Ing. Oldřich Balák (spoluřešitel) je absolventem Vysoké školy strojní a elektrotechnické v Plzni. V letech 1986 až 2003 pracoval v několika státních i soukromých organizacích jako programátor nebo správce systémů. Od roku 2003 pracuje v Laboratoři počítačových systémů Centra informatizace a výpočetní techniky Západočeské univerzity v Plzni. Jako člen Oddělení distribuovaných systémů se zabývá správou operačních systémů Solaris a Linux, dále zálohováním a tiskovými službami. Kromě toho se podílí na vývoji software pro Český národní registr dárců kostní dřeně.

6 Navrhovaná doba trvání projektu

Navrhovaná doba trvání projektu je plánována na 12 měsíců.

7 Finanční rozvaha

Pro projekt jsou požadovány jen náklady spojené s řešením grantu, které činí 292 000,- Kč včetně DPH. Z prostředků fondu rozvoje budou čerpány prostředky ve výši 182 000,- Kč, zbylou částku 110 000,- Kč (tj. 37,6%) včetně dalších nákladů spojených s projektem hradí řešitelská organizace.

Celkem odhadované náklady na pokrytí projektu včetně DPH byly stanoveny následovně:

⁴Předpokládá se, že bude vybrán jeden student ze skupiny HELPs. Tato skupina studentů pomáhá řešit běžné uživatelské problémy na stanicích jež provozuje CIV.

⁵Jedná se o kurzy z Cisco Networking Academy Program, více viz <http://www.netacad.cz/>

položka	hodnota v Kč	z prostředků
server	70 000	FR-CESNET
mzdy	107 000	FR-CESNET
tuzemské cestovné, konferenčné	5 000	FR-CESNET
zahraniční cestovné, ubytování	40 000	ZČU
zahraniční konferenčné	40 000	ZČU
odměny studentských řešitelů formou stipendia	30 000	ZČU
celkem	292 000	

Náklady na zahraniční cestovné, ubytování a konferenčné jsou odhadovány na základě informací z již konaných zahraničních konferencí a aktuálních cen za dopravu resp. ubytování.

Tuzemské cestovné a konferenčné pokrývá náklady odhadované na prezentaci výsledků projektu na některé z národních konferencí zabývajících se administrací systémů.

Cena serveru, konfigurace a dodavatel (viz příloha) vychází z interního výběrového řízení ZČU pro rok 2008 na dodávku serverů. Předpokládaná životnost serveru je minimálně 5 let, čemuž odpovídá záruční podmínka a hardwarová konfigurace.

Mzda pro řešitele byla odvozena od 0,15 úvazku na jednu osobu a její rozpočítání je uvedeno v následující tabulce:

měsíční mzda při úvazku 1.0	22 000
měsíční mzda při úvazku 0.15	3 300
roční mzda při úvazku 0.15	39 600
sociální a zdravotní pojištění (35%)	13 860
mzda + sociální a zdravotní pojištění	53 460
celkem náklady na mzdu pro 2 osoby	106 920
zaokrouhlení na tisíce	107 000

Výše úvazku zohledňuje objem činností, které se na projektu předpokládají.