Projekt OPEN ORION

Centrum informatizace a výpočetní techniky,
Laboratoř počítačových systémů,
Západočeská univerzita v Plzni

Pracovní verze ze dne 12. února 2001 12:04

Abstrakt

Projekt OPEN ORION je vyjádřením jedné ze snah o rozvoj výpočetního prostředí Západočeské Univerzity v Plzni (projekt ORION) s ohledem na současnou situaci a potřeby. Jeho hlavní myšlenkou je využití vývoje v okolním světě, kde dochází k stále silnější akceptaci technologií, jež jsou klíčovými stavebními kameny projektu ORION, pro výrazné vylepšení dosud stagnující oblasti – podpory uživatelů s vlastní stanicí (pod vlastní správou) snadno aplikovatelnou formou (zjednodušeně řečeno ORION klientem pro jejich OS). Vzhledem k tomu, že tato snaha, podpořená navíc mnoha dalšími projekty zásadního rázu (např. technologie tenkého klienta), otevírá řadu obecnějších otázek, je součástí tohoto koncepčního materiálu i návrh aktualizace koncepce ORIONu jako celku. Tato část tohoto materiálu je tedy zamýšlena (minimálně v první fázi) jako podklad pro diskuzi nad střednědobou koncepcí rozvoje výpočetního prostředí ZČU.

Tento dokument je pracovní verze a slouží pro interní použití, především jako podklad k diskuzím na naznačená témata.

1 Projekt OPEN ORION

1.1 Motivace a vazby

1.1.1 Projekt ORION

Projekt ORION je distribuované výpočetní prostředí Západočeské univerzity v Plzni. Toto výpočetní prostředí, které je v celouniverzitním produkčním provozu od roku 1996, je založeno na otevřených principech a technologiích. Cílem projektu OPEN ORION není tedy přechod na takovéto principy či technologie, ale jejich zdůraznění v souladu se současnými podmínkami a to zejména s ohledem na aktuální posun v míře adobce technologií použitých v projektu ORION v obecném světě otevřených systémů.

Projekt ORION je distribuované výpočetní prostředí založené na několika základních komponentách:

- centrální autentizační mechanismus (Kerberos),
- distribuovaný souborový systém (AFS),
- koncepce centrální údržby systémového a aplikačního SW,

- systém pro management výpočetního prostředí (Moira).

1.1.2 Vývoj v okolním světě

Lze říci, že v uplynulé době došlo k posunu v akceptaci autentizačního mechanismu Kerberos v prostředí výpočetních systémů. Kerberos 5 se stal standardně podporovaným autentizačním protokolem například v jedné z hlavních distribucí Unixového operačního systému Linux – RedHat a základem autentizačního subsystému nového výpočetního prostředí firmy Microsoft – Windows 2000.

Mnohé naděje jsou vkládány do událostí posledních několika měsíců souvisejících s distribuovaným souborovým systémem AFS. Aktivita firmy IBM, která je aktuálním vlastníkem této technologie – projekt Open AFS – dává naději, že se AFS, posíleno úsilím mnoha schopných lidí v rámci hnutí open software, stane standardním modulem, resp. SW balíkem základních Linuxových distribucí a bude se nadále aktivně vyvíjet[1]. Znamená to samozřejmě také to, že nyní již je k dispozici na většinu platforem AFS technologie zcela zdarma.

1.1.3 Strukturované nasazení projektu ORION

Projekt ORION je postaven tak, aby umožňoval několik variant nasazení své funkcionality na systémech jednotlivých uživatelů. Pro zjednodušení problematiky stanovme následující základní možnosti/kombinace:

a) Plné nasazení

   Systém využívá veškeré funkcionality projektu ORION. Jeho použití a možnosti zcela určuje koncepce a aktuální stav projektu ORION. Centrálně instalovaný SW, konkrétní fixní distribuce operačního systému, transparentní přístup k datům a jednotnému uživatelskému rozhraní ze všech systémů. Mechanismy údržby systému vhodné především pro veřejné laboratoře a centrální přístupové servery.

b) Systém ve vlastní správě

   Lokální systém se samostatnou správou, který umožňuje transparentní přístup k datům výpočetního prostředí. Systémový a aplikační SW je udržován lokálně dle potřeb a možností uživatele, systém využívá centrální autentizační službu a souborový systém.

c) Systém s odpovídajícími přístupovými prostředky

   Zcela lokální a nezávislý systém. Část instalovaného SW dovoluje bezpečný a plnohodnotný vzdálený přístup k systémům výše uvedených typů.

1.2 Cíle projektu OPEN ORION

Cílem projektu OPEN ORION je shromáždit a systematicky uržovat informace potřebné pro nasazení dle varianty b) a c). Jedná se zejména o informace na úrovni konkrétních technických popisů pro jednotlivé operační systémy, které v současnosti dovolují relativně přímočaře dosáhnout požadovaného výsledku bez nutnosti hlubších znalostí a zásahů.

Základní cílovou oblastí projektu OPEN ORION jsou uživatelé výpočetní techniky z řad studentů a zaměstnanců ZČU, kteří chtějí přistupovat k základní funkcionalitě univerzitního výpočetního prostředí ze svých pracovních stanic za výše naznačených podmínek.

[1] Open AFS je k dispozici i na další platformy včetně MS Windows.

1.3 OPEN ORION – pohled uživatele

Uživatelem výsledků projektu OPEN ORION je každý, kdo je schopen a ochoten základní systémové správy nějakého (podporovaného) operačního systému (platformy). Vize projektu OPEN ORION je taková, že každý takový člověk musí dostat k dispozici z jeho pohledu jednoduchý a srozumitelný mechanismus pro provedení kroků, jež z jeho OS zpřístupní základní služby poskytované v rámci výpočetního prostředí ZČU. V závislosti na technických okolnostech a platformě může nastat jedna z následujících situací:

- Pro zvolený cíl je k dispozici konkrétní návod, popisující konfiguraci zvolené platformy s použitím běžně dostupného systémového a aplikačního SW. Tento SW může být bud' udržován přímo v rámci distribuce OS, nebo třetí stranou (např. Open Source projekt). Návod je udržován lokálně dle specifik výpočetního prostředí ZČU (tj. také náležitě průběžně přizpůsobován změnám).

- Kromě návodu je k dispozici také příslušná SW komponenta realizující majoritu lokálních konfiguračních a jiných přizpůsobení. Smyslem této komponenty je zjednodušení (automatizace) konfiguračních kroků. Podle technických možností může jít o samostatný SW balík realizující konfiguraci a náležité „slepení“ standardních SW balíků[2], nebo také o „lokalizované“ SW balíky (standardní balíky s jinými implicitními konfiguracemi, či vhodnými základními doplňky pro bezstarostnou integraci do výpočetního prostředí ZČU).

- V některých případech musí být poskytováno i specifické SW vybavení. Může jít o komponenty, které nejsou dosud pro danou platformu standardně k dispozici, nebo o nestandardní komponenty, specifické pro výpočetní prostředí ZČU (příklady viz kap. 1.6). Zde se může situace průběžně měnit dle vývoje s akceptací technologií jednotlivými platformami. V lokální režii musí být udržovány všechny potřebné komponenty aktuální a to i vzhledem k vývoji (hostitelských) OS.

Tento model lze v podstatě chápat jako poskytnutí klientského SW pro projekt ORION, podobně jako mluvíme např. o klientu Novellu (poslední z výše uvedených variant) nebo o klientu Win NT (podobně jako první dvě varianty – kde vlastně o žádný SW nejde, neboť je součástí (hostitelského) OS).

Uživatel (zde systémový správce lokálního OS) je plně zodpovědný za funkčnost systému a všechny jeho komponenty. Může mu být poskytována technická podpora na úrovni konfigurace a řešení problémů s výše naznačenými SW balíky (například formou služby HELPS podobně jako u jiných klientů).

1.4 OPEN ORION technicky

1.4.1 Poskytované služby

- Autentizace

  Centrální autentizační služba pro ověřování uživatelů (při přihlášení na stanici). Je zajištěna funkcionalita SSO (Single Sign On), tj. další přístup uživatele k centrálním

[2] Příkladem mohou být balíky využívající mechanismy pro správu SW balíků jednotlivých distribucí OS Linux, viz např. projekt Boxed Penguin pro Debian Linux.

službám a prostředkům je realizován s možností transparentního předání prokázané identity.

Realizace: Kerberos 5 (varianta MIT)

- Souborový systém

  Přístup k centrálnímu souborovému systému. Z hlediska projektu OPEN ORION poskytuje zejména přístup k centrálně spravovanému uživatelskému diskovému prostoru, který je sdílený, zálohovaný a slouží také k prezentaci dat. Jedná se o uživatelské domovské adresáře a projektové adresáře.

  Realizace: AFS

- Jednotná báze uživatelských kont

  Centrální služba, která distribuuje informaci o uživatelských kontech ve výpočetním prostředí. Dovoluje namísto lokální údržby uživatelských kont využít managementu distribuovaného výpočetního prostředí.

  Spolu s vlastní informací o existujících uživatelských kontech je k dispozici také informace o příslušnosti jednotlivých kont do skupin uživatelů. Tyto skupiny mají význam definovaný a zaručený centrálním managementem (např. student, zaměstnanec, apod.), resp. mohou být uživatelsky definovatelné. S využitím příslušných SW modulů (např. PAM) je možno tyto informace využívat k řízení přístupu nebo jiným autorizačním účelům.

  Realizace: LDAP (NSS_LDAP, resp. RFC 2307)

- Pošta

  Centrální služba zajišťující distribuci pošty, poštovní schránky uživatelů a přístup k nim ze standardních klientů.

  Realizace: IMAP4 (POP3 pro kompatibilitu), zabezpečení SSL, možnost kerberos autentizace uživatele

- Další

  Další centrální služby, např. tisky, nebo samozřejmě takové služby, které přímo nesouvisejí s koncepcí koncové stanice, ale jsou k dispozici každému uživateli ORIONu (WWW prezentace, virtuální WWW servery, ...).

1.5 Software

Hlavní SW komponenty, kterými je třeba se zabývat jsou odvozeny z potřebných služeb popsaných výše. Jsou to:

- Kerberos 5

  Klientský SW sloužící pro explicitní získání, vypsání a zrušení Kerberos identity, knihovny a „kerberizované“ verze klientských programů (ftp, telnet, ssh, IMAP klient, atd.). Patří sem také podpora integrace se systémem, zejména login a xlogin (XDM) s transparentní autentizací vůči Kerberovi a získání pověření (na Linuxu realizováno PAM modulem pam_krb). Mohou sem patřit i základní (kerberizované) SW pro poskytování služeb, především přístupový SW typu sshd či ftpd.

- OpenAFS

  Poměrně samostatný SW balík zpřístupňující AFS – globální souborový systém. S tím souvisí také SW pro získávání pověření pro službu AFS (token) z primární Kerberos identity a integrace tohoto procesu do jednoho transparentního mechanismu získání identity.

- NSS LDAP

  Knihovna resp. modul zajišťující transparentní přístup k informacím distribuovaným přes LDAP (RFC 2307). Funguje podobně jako NIS, používá se pro distribuci položek /etc/passwd a /etc/group.

1.6 Podporované platformy

Předpokládáme podporu následujících platforem (hostitelských OS):

- Linux

  Linux je základní platformou projektu OPEN ORION zejména vzhledem k relativně bezproblémové a mnohdy zcela standardní a obecně akceptované integraci všech potřebných technologií. Zde je třeba vyzdvihnout RedHat Linux 7.0, který je první ze stabilních distribucí obsahujících potřebné komponenty. Debian Linux, standardní podporovaná Linux platforma (distribuce) ORIONu, je v tomto směru v závěsu (potřebné komponenty jsou již ve vývojové verzi).

  Jsou zde k dispozici všechny výše uvedené a naznačené balíky a mechanismy (PAM, NSS_LDAP, kerberizovaný SW, OpenAFS, možnost tvorby „konfiguračních“ balíků, atd.). Vzhledem k razantnímu vývoji Linuxových distribucí a obrovskému množství standardně dostupných SW balíků (tj. také extrémnímu množství možných instalací, resp. konfigurací) je koncepce OPEN ORIONu ponechávající většinu věcí na udržovateli distribuce Linuxu a správci stanice zvláště výhodná. Je-li navíc správce stanice zároveň jediným uživatelem, což je u Linuxu běžné, poskytuje taková koncepce možnost potřebné svobody při zachování přístupu k základním službám.

  Předpokládá se, že tuto koncepci je možné použít i pro údržbu učeben, či jiných jednotně spravovaných skupin strojů a to v kombinaci se standardními nástroji pro automatizovanou instalaci a konfiguraci (dle šablony) strojů, které jsou k dispozici v rámci dané distribuce Linuxu.

  Je možné počítat s doplněním zajištění kritických nebo z technických důvodu (platforma) nedostupných aplikací pomocí služeb založených na technologii tenkého klienta (Orion TC). Dá se zde mluvit o možnosti zavedení nové komplexní služby, poskytující klasickému uživateli Unixového prostředí aplikace ze světa MS platforem a to velmi transparentním způsobem (přístup ke sdíleným datům).

- Windows NT

  Windows NT jsou v krátkodobém výhledu základní platformou, kterou chceme nabídnout (doporučit a podporovat) koncovým uživatelům na jejich stroje. Linux lze bohužel chápat jako platformu pro specifickou skupinu uživatelů (zpravidla technicky zdatnější, kteří si váží výhod Linuxu a nejsou zásadně vázáni na MS platformy), Win

95/98/ME nepodporujeme a nedoporučujeme a Win 2000 jsou v tuhle chvíli stále nastupující (HW náročnou) novou platformou.

V rámci projektu OPEN ORION chceme dosáhnout podobné funkcionality, jaká byla popsána výše a to většinou v kontextu Linuxu. Přiměřeně technicky zdatný uživatel (schopný základní instalace a správy Win NT, což je v dnešní době snadno dostupná kvalifikace, v našem prostředí navíc práce oddělení uživatelské podpory (a HELPS)) dostane k dispozici SW balík (balíky), který nainstaluje obvyklým způsobem na svůj stroj a získá tím výše uvedenou funkcionalitu. Aplikace instaluje a spravuje lokálně. Předpokládá se, že:

  - Součástí nainstalovaného balíku je klient AFS s příslušnou konfigurací.
  - Součástí je také autentizační modul (GINA), který realizuje ověření uživatele dle Kerbera (dovolí přihlášení lokálního uživatele, ale přidá navíc i možnost přihlášení libovolného centrálně definovaného uživatele). Tento modul navíc volitelně umožní řízení přístupu na stanici jen pro některé centrálně definované uživatele.
  - V tomto balíku by měly být i základní utility pro manipulaci s Kerberos identitou.

  I zde se předpokládá potenciální možnost zajištění kritických a centrálně podporovaných aplikací přes terminálové služby. Je možno předpokládat i to, že technologií tenkého klienta lze (dočasně a omezeně?) distribuovat na takovéto stanice případné aplikace vyžadující vyšší OS (Win 2000).

- Windows 2000

  Windows 2000 jsou pravděpodobným nástupcem Win NT jakožto základní doporučované klientské platformy, musí být tedy podporovanou platformou Open ORIONu. Jejich návrh a vlastnosti jsou z hlediska koncepce OPEN ORIONu slibné a to zdaleka nejvíc z dosud existujících OS firmy Microsoft.

  Zrejmě je zde možné poměrně přímočaře použít výše popsanou technologii z Win NT (navíc ji máme jako součást první generace ORION TC serveru). Strategií do budoucna je však jednoznačně příklon k využívání standardních prostředků, které jsou ve Win 2000 k dispozici nativně, zejména Kerberos, pravděpodobně i Active Directory.

1.7 Variabilita nasazení projektu OPEN ORION

Projekt OPEN ORION ze své podstaty nabízí značnou variabilitu nasazení, kterou si může správce lokálního systému volit. Většina těchto variant je patrná z předchozích odstavců, je však třeba najít správnou míru nabízení možných variant běžnému uživateli (at' už formou doporučených konfigurací, nebo formou voleb při instalaci OPEN ORION SW balíků).

2 Koncepce projektu ORION – aktualizace

Uvedení projektu OPEN ORION je vhodným okamžikem k aktualizaci koncepce projektu ORION jakožto jádra provozního výpočetního prostředí ZČU. Sám projekt OPEN ORION plně navazuje na koncepci projektu ORION, jednou z jeho motivací je však také změna vnějších podmínek, která za dobu od vzniku projektu ORION nastala. Chápejme tedy následující text, aktualizaci koncepce projektu ORION, jako rámcový koncepční materiál k dalšímu vývoji jádra systému, který není podmíněn ani nepodmiňuje vlastní OPEN ORION.

2.1 Projekt ORION a jeho rozvojové projekty

Popišme nejprve současný stav projektu ORION vzhledem k jeho hlavním rozvojovým projektům. Základní přehled (do nějž samozřejmě patří ještě navrhovaný projekt OPEN ORION):

- Jádro projektu ORION

  Základní poskytované služby, „ORIONizované" distribuce podporovaných Unixových OS včetně nástrojů pro jejich instalaci (v rámci koncepce dataless stanice), centrální báze softwarových balíků s jednotnou konfigurací pro všechny podporované OS, management distribuovaného prostředí, pošta, atd.

- Projekt ORIONT

  Klientská platforma Orionu založená na Win NT 4.0 se stejnou koncepcí. Centrální údržba příslušného SW, automatická instalace. Orientace na veřejné učebny.

- Projekt ORIONT–IS

  Klienská platforma vycházející z ORIONT s koncepcí modifikovanou pro specifické potřeby vysoce produkčního prostředí informačního systému univerzity. Vysoké nároky na spolehlivost a podporu koncových stanic a uživatelů. Specifické mechanismy instalace, správy SW i údržby.

- Projekt ORION TC

  Doplňková služba založená na technologii tenkého klienta. Poskytování vybraných aplikací na koncové stanice u nichž jsou výše uvedené koncepce neefektivní či jinak nevyhovující.

2.2 Cílové domény

Základní cílové domény (oblasti použití), které projekt ORION pokrývá, nebo by pokrývat měl lze specifikovat takto:

- Centrální unixové systémy

  Víceuživatelské unixové systémy pro vzdálený přístup. Uživatelé zde pracují terminálovým způsobem a to včetně X-Windows. Jádro ORIONu, všechny služby a standardní mechanismy. Několik málo strojů umístěných centrálně.

- Veřejné učebny – PC

  Poměrně homogenní skupiny PC stanic. Režim veřejných učeben vyžaduje bezúdržbovou koncepci. Podpora Win NT a Linux. V současnosti pokrývají projekty ORIONT a Orion Linux. 100 až 200 PC v asi 10 učebnách v několika objektech.

- Veřejné učebny specializované, převážně Unix Workstations

  Součást jádra ORIONu, platformy IRIX a Tru64. Dvě až tři učebny po deseti strojích.

- Informační systém univerzity

  Specifické potřeby i koncepce. Nutnost poskytnutí podpory na nejvyšší možné úrovni

a z toho plynoucí potřeba centrální kontroly nad HW i SW konfigurací. Vysoké nároky na provozní spolehlivost musí být odraženy i v návrhu systému, který musí počítat s výpadky komunikační infrastruktury. Přes 300 pracovišť po celé univerzitě včetně jinak oddělených vzdálených pracovišť (Cheb).

- Osobní stroje zaměstnanců, katedrální učebny

  Potenciálně všechny stroje, které nejsou přímo centrálně spravovány. V současnosti jsou řešeny velmi omezeně projektem Orion Linux či ORIONT, případně využívají služeb Novellu nebo Dají se předpokládat řádově stovky kusů po celé univerzitě.

- Superpočítače

  Speciální režim, měl by zapadat do koncepce ORIONu i MetaCentra. Poskytuje specifické služby. Několik málo kusů centrálně umístěných.

- Služební systémy

  Převážně systémy poskytující služby včetně služeb přímo nesouvijících s jádrem ORIONu (např. databáze). Zvláštní kapitolou jsou servery založené na Windows, zejména servery ORION TC. Maximálně desítky strojů, převážně centrálně, ale i v jednotlivých lokalitách.

2.3 Architektura projektu ORION

Předpokládejme nyní pro jednoduchost základní představu o současné architektuře projektu ORION. Zaměřme se nejprve na jednotlivé subsystémy, resp. služby a koncepci jejich poskytování. Koncepce pro jednotlivé cílové domény, resp. řešení konkrétních dílčích potřeb oddělme a ponechme zvlášť.

2.3.1 Služby a jejich poskytování

- Kerberos

  Základní a relativně samostatná služba, infrastruktura MIT Kerberos KDC.

- AFS

  Jednotný souborový systém. Infrastruktura serverů s příslušnými diskovými kapacitami. Zajišťuje zejména: domovské adresáře uživatelů, projektové adresáře a depozitář software.

- Centrální depozitář software

  Centrální depozitář software poskytuje podporovaný aplikační a částečně systémový software jednotnou formou a v jednotné konfiguraci pro všechny podporované platformy. Rozhranní pro uživatele zajišťuje software pro manipulaci se SW balíky „modules“. Základní informace o existujících balících jsou udržovány v centrálním management systému.

  Údržba centrálního depozitáře software je náročná na zdroje. Poskytuje jednotnou základnu software pro všechny podporované (Unixové) platformy a to v lokálně přizpůsobených a ověřených konfiguracích. Nevýhodou je, že takový depozitář nutně

zaostává za nejnovějšími trendy (verzemi SW) a v některých případech zanaší jistou nestandardnost a duplikuje práci vzhlede k SW základně udržované v rámci příslušné distribuce OS (zejména Linux).

Další koncepci a případné řešení je třeba zvážit.

- Management a informační služby

  Současný management ORIONu je v technicky nevyhovujícím stavu. Je třeba oživit a posílit úsilí směřující ke tvorbě nového systému. Jeho funkce i koncepční zásady jeho návrhu jsou tématem samostatného dokumentu. Mezi základní patří:

  - Vazba na existující datové báze

    Všechny informace by měli mít jednoho a jasně definovaného gestora (toho, kdo je za ně zodpovědný). Každá aplikace by měla sloužit k údržbě těch dat, za která jsou logicky odpovědní její uživatelé a ostatní data by měla pouze využívat. Zde lze považovat za zásadní přímou vazbu na studijní agendu a (nově vytvořený) registr osob.
  - Jednotné rozhraní informačních služeb

    Management systém by měl poskytovat většinu informací potřebných pro provoz výpočetního prostředí formou jednotného rozhraní. V oblasti informačních služeb je zřetelná koncepce jednotného rozhraní založeného na adresářových službách.

- „Distribuce“ jednotlivých platforem a mechanismy jejich instalace

  Tato problematika se týká zejména veřejných PC učeben, specializovaných (Unix) učeben a centrálních serverů. Zde všude se využívá jednotných distribucí podporovaných platforem ORIONu. Je třeba zvážit další postup v této oblasti.

- Zálohování

  Koncepce zálohování vychází z existence centrální zálohovací služby, kterou využívají jednotlivý klienti (v tomto případě systémy s lokálně uloženými daty, zejména služební stroje). Z technických důvodů je oddělen mechanismus pro zálohování centrálního souborového systému (AFS). Z organizačně technických důvodů a z důvodů zajištění jiné třídy spolehlivosti a bezpečnosti záloh jsou samostatně zálohovány agendy informačního systému (zejména databáze Oracle).

  Je potřeba dořešit řadu věcí, zejména:

  - kapacitu centrální zálohovací služby – technicky zaostává za nárůstem diskových kapacit,
  - provozní zajištění – provoz služby musí odpovídat jejímu produkčnímu a rutinnímu charakteru;

- Pošta

  Poštovní subsystém je řešen relativně autonomně. Pošta je poskytována standardními protokoly (IMAP, POP), její uložení a realizace poštovního subsystému je pro uživatele transparentní. Poskytované doplňkové služby jsou zejména třídění a přesměrování

pošty. Přístup ke všem službám je řešen v rámci jednotného autentizačního prostředí, přístup k poště navíc podporuje (s příslušným klientem) SSO funkcionalitu.

Jinými slovy současná koncepce předpokládá, že vystačíme se zcela standardní a lokální imlementací (tj. také zcela centralizovanou, nedistribuovanou), přičemž doporučované použití je takové, že služba nerealizuje jen doručování pošty, ale i uložení veškeré uživatelské pošty (foldery). Koncové systémy zaručují pouze běh uživatelova poštovního klienta, tj. přístup k poště je pro uživatele transaparentní z libovolného místa.

- Tiskové služby

  V oblasti tiskových služeb je prostor pro návrh zcela nového moderního a potřebám vyhovujícího řešení. Stávající podporované rozhraní LPR je zřejmě vyhovující a je potřeba v blízké době navrhnout a realizovat odpovídající mechanismus poskytování této služby. Zřejmě je zde nutnost hledání cest pro implementaci řízení přístupu uživatelů k této službě (a accountingu, včetně počítání stránek u poskriptových tiskáren). V této oblasti je samozřejmě počítáno s využitím jednotného AAA (autentizace, autorizace, accounting) rámce.

- Autorizační služby a jednotný rámec pro tvorbu aplikací (autentizace, autorizace)

  Pro systémové i uživatelské aplikace je nutné nabídnout nejen základní a jednotnou autentizační službu, ale i další věci. Zejména se jedná o autorizační službu, resp. rámec pro zacházení s autorizačními informacemi. Tyto potřeby je zřejmě rozumné pokrýt jednotným rámcem zastřešujícím AAA (autentizace, autorizace, accounting) služby a poskytujícím vhodné rozhraní a metodiku pro vývojáře aplikací.

  Řešení musí, a to v neposlední řadě, pokrývat problematiku aplikací s WWW uživatelským rozhraním. Mělo by také zajistit, nebo napomoci k zajištění zastřešujících vazeb mezi v současnosti existujícími mechanismy prokázání identity (aplikace, Oracle, JIS).

  Tato problematika je tématem samostatného koncepčního materiálu.

- Další služby

  Služby, které nepatří do základního poskytovaného jádra, nicméně prakticky či historicky se staly součástí funkce distribuovaného výpočetního prostředí. Řada z nich úzce souvisí, nebo by se dala považovat za součást managementu distribuovaného výpočetního prostředí. Některé jsou také zásadní pro zajištění provozu.

  Jedná se zejména o následující služby:

  - Rozvrh aneb rezervace učeben
  - Tresty
  - Monitorování provozu (provozní spolehlivost a údržba)
  - Bezpečnostní monitorování

  Technické zajištění některých (doplňkových) služeb může být realizováno singulárně, dle poměru cena/výkon, přičemž cenou je myšlen souhrn lidských a finančních kapacit nutných pro vytvoření/převedení služby a pro provozní zajištění této služby. Jedná se zejména o to, že některé služby monou být poskytovány na „legacy“ systémech

(Novell), některé na lokálních, touto koncepcí k poskytování služeb nedoporučovaných OS (Win NT), další na běžně nepodporovaných lokálních variantách Linuxu apod.

2.4 Jednotlivé dílčí koncepce

Tato kapitola popisuje architekturu projektu ORION z pohledu jednotlivých cílových domén.

2.4.1 Zajištění provozu IS

Základ pokryt projektem ORIONT–IS, předpoklad využití ORION TC jako doplňkové služby pro řešení některých zásadních problémů (podpora zásadních aplikací i na stanicích, které nepodléhají přísné produkční politice a podpora produkčních aplikací jejichž charakter vyžaduje časté změny).

Aplikace podléhající změnám Ze základu (lokální stanice) lze vyjmout aplikace, které vyžadují časté změny. Tento krok by měl přispět ke zvýšení stability celého ORIONT–IS a ke snížení nároků na jeho údržbu. Celý systém se tím také dostane blíže své původní koncepci (velmi produkční, neměnné prostředí).

ORION TC musí podporovat tyto aplikace a tyto musí být uživateli ORIONT–IS přístupné transparentně ikonou na ploše (pokud možno uživatel nepozná, že už to neběží lokálně)

Podpora agend na libovolné stanici Jednou z hlavních výhod technologie tenkého klienta je to, že dovoluje vyhovět základnímu požadavku jisté skupiny uživatelů, tj. produkční podpory několika aplikací při zachování možnosti prakticky libovolných zásahů do konfigurace OS uživatelské stanice. Tento požadavek může být také motivován snahou o zachování lokální stanice na jiném než podporovaném OS a to z různých důvodů, přičemž mezi zásadní patří HW výkonnost.

Předpokládá se tedy poskytování zasádních agend IS formou typického ASP (Application Service Provider) v rámci projektu ORION TC.

Zajišťování dočasných aplikací Další problém, který lze elegantně řešit na základě technologie tenkého klienta je nutnost zajišťování dočasných aplikací (např. „dotazníky“ pro ministerstvo).

Tuto funkcionalitu bude zajišťovat samostatný NT server, se základními službami (Krb autentizace, mechanismus řízení přístupu pro vybrané uživatele, lokální disk pro SW) a Citrix TC serverem. Jeho správa bude plně pod kontrolou správce zajišťovaných aplikací.

2.4.2 Osobní stroje zaměstnanců

Koncepce projektu OPEN ORION. Z něj vyplývají i podporované platformy. Lze v omezeném rozsahu nabídnout i služby projektu ORION TC, zejména pro stanice s nevyhovujícím HW sloužící pro základní aplikace (poskytnutí celého desktopu se základním aplikačním vybavením typu poštovního klienta). Omezení vyplývá zejména z finančních nároků na zajištění ORION TC služeb.

V souladu s koncepcí projektu OPEN ORION lze pro učebny či skupiny strojů počítat s možností tvorby a využití prostředků pro automatizovanou instalaci strojů (mělo by být

možné přímočaře pro Linux a pravděpodoblě lze najít i standardní a přitom v kontextu OPEN ORIONu vyhovující řešení pro Windows NT či 2000).

2.4.3 Veřejné učebny PC

Současná koncepce bezdatové stanice instalované z centrálně udržovaného prototypu (na lokálním disku nejsou ani aplikace) je vyhovující z funkčního hlediska. Otázkou je kapacita pro údržbu těchto prototypů (distribucí) vzhledem k potřebné kvalitě a aktuálnosti.

Jistým řešením by mohl být rozvoj koncepce naznačené v rámci projektu Open ORION pro katedrální učebny. Zejména v Linuxovém světě si lze představit, že by stačilo udržovat depozitář balíků OPEN ORIONu (pro příslušnou distribuci Linuxu včetně jejích aktualizací) a použít prostředky pro automatizovanou instalaci a konfiguraci, které jsou součástí příslušné distribuce (udržovat lokální konfiguraci a zajistit vhodný přístup k instalační proceduře, např. z BootROM). Toto řešení má nepochybně řadu nevýhod i výhod ke zvážení.

Ve veřejných učebnách je třeba také zvážit nasazení tenkého klienta. Jeho výhody jsou opět zřejmé – přístup k pracovnímu prostředí pro běžné aplikace (čtení pošty, kancelářské balíky) ze stanic, které HW nevyhovují podporovaným platformám. Je možné také zvážit nasazení bezúdržbových stanic – terminálů TC (viz dále).

2.4.4 Koncepce bezúdržbových koncových stanic – terminálů

Tato koncepce vychází ze starých dobrých principů znakových terminálů, X-terminálů a moderní technologie tenkého klienta. Základní výhodou této koncepce je razantní zlepšení a zjednodušení v oblasti podpory koncové stanice.

Principem této koncepce je nasazení specializovaného HW zařízení jako koncové stanice. Toto zařízení je jednoúčelové a z hlediska uživatele nabízí pouze naprosto základní konfiguraci. V našem prostředí jsou výhodná zařízení, která zvládají technologii tenkého klienta a X-terminálu. Uživatel takového zařízení má přístup ke službám ORION TC, tj. základnímu aplikačnímu vybavení na bázi platformy Windows a ke kompletnímu Unixovému prostředí centrálních serverů projektu ORION.

Údržba zařízení spočívá v podstatě pouze v HW údržbě. Díky naprosté nezávislosti uživatele na koncovém terminálu lze bez problémů tuto údržbu provést okamžitou záměnou terminálu. Navíc transparentnost přístupu ke službám z libovolného terminálu plně vyhovuje celkové koncepci projektu ORION.

Nasazení této varianty koncové stanice lze považovat za vhodné jednak v oblastech s vysokými nároky na provozní spolehlivost a podporu (IS) a jednak v oblastech, kde jednoduchost a jednoúčelovost na straně klienta může přinést úsporu času a zjednodušení provozu (veřejné terminály, některé veřejné učebny).

2.4.5 Centrální servery, Unix učebny, služební systémy a superpočítače

Tato oblast se dá považovat za skutečné jádro ORIONu. S vyjímkou služebních serverů určených pro zajišťování specifických služeb (Oracle) se jedná o plné využití lehce upravené základní koncepce ORIONu (lokální systémový software pro zlepšení spolehlivostních parametrů, apod.). Za zásadní lze považovat plaftormy Tru 64, Linux a IRIX. Je potřeba zvážit do jaké míry a v jakých oblastech je rozumné tuto koncepci dále upravit tak, aby odpovídala současným možnostem a potřebám. Zejména se jedná o vazbu na možné využití výsledků

projektu OPEN ORION na některých platformách (Linux?) a tudíž postoj k jednotnému depozitáři SW.

2.4.6 Systémy zajišťující služby založené na Windows

Jedná se zejména o ORION TC. Předpokládanou nosnou platformou jsou Windows 2000. Koncepcí je maximální využití standardních prostředků (nativních MS prostředím), s důrazem na výběr těch (dostupných ve Windows 2000), které jsou blízko koncepci ORIONu (Kerberos 5, adresářové služby). Z pohledu MS nestandardní technologie nasazovat pouze v klíčových případech (AFS) a omezeným způsobem (v souladu s filozofií OPEN ORIONu, tj. pouze pro přístup k centrálnímu úložišti uživatelských dat, nikoli SW). Pro instalaci SW a správu distribuce pro jednotnou údržbu clusteru serverů zvolit z našeho pohledu nejvhodnější z technologií běžně akceptovaných ve světě MS Windows (pravděpodobně součásti Win 2000). Zásadní prací je návrh využití jádra Win 2000 managementu (Active Directory – adresářových a autorizačních služeb) tak, aby to bylo co nejstandardnější a přitom co nejlépe zapadalo do jednotné koncepce ORIONu.