POVEZIVANJE LINUXA S ACTIVE DIRECTORY SUSTAVOM

verzija 1.2

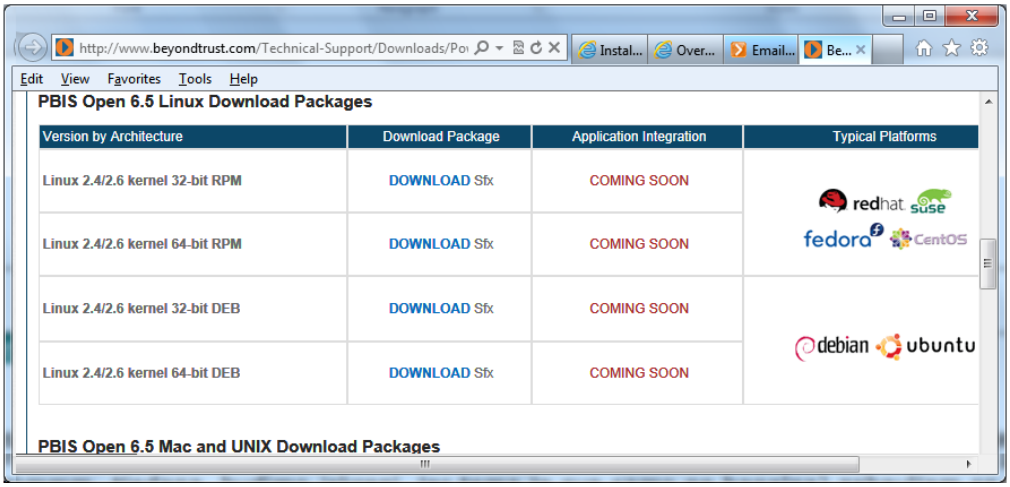
Ratko Žižek, MCSE-MCITP

Rasprave tipa "Linux-je-bolji-bljak-bolji-je-Windows-fuj" uglavnom smatram prelijevanjem iz šupljeg u prazno. S druge strane, odavno me zainteresirala problematika interoperabilnosti ovih dvaju dobrano zavađenih OS-ova pa pomalo njuškam sveze & glede toga. Zadnjih par dana (hmmm, tjedana, budimo iskreni, jer tema je sve samo ne banalna) zabavljam se sa učlanjenjem Linuxa - u mom slučaju Ubuntua - u Active Directory sustav.

Povezivanje Linux računala (OS-a i aplikacija) s Active Directory servisom kao središnjim sustavom autentikacije, autorizacije i auditinga od prvorazrednog je značenja za sve poslovne subjekte koji su već implementirali ovaj cijenjen i dokazano pouzdan imenički sustav (taj je, prisjetimo se, ujedno i moćan alat za managiranje Windows računala). Out-of-the-box interoperabilnost Linux i Windows OS-ova niske je razine, za enterprise sredine nedostatne, pa se kontinuirano razvijaju svakojaka (ne)komercijalna medijatorska rješenja. Od tih igrača koji nastoje nagovoriti razne Linux distribucije da se ipak uklope u Active Directory, naposljetku sam odabrao besplatnu (tj. licenciranu po GPL/LGPL v2 modelu) PowerBroker Identity Services Open Edition. PBISOE je oslabljena verzija komercijalnog PBIS produkta iliti, po naški, navlakuša. Srećom, i takva je vrlo upotrebljiva.

PBISOE agent se skine sa linka http://www.beyondtrust.com/Products/PowerBroker-Identity-Services-Open-Edition/Evaluation/ za odgovarajući OS, kernel i CPU arhitekturu. Sve značajke besplatne verzije, i kako ju optimalno iskoristiti, nalaze se u dokumentu **PBISO Installation and Administration Guide**, također objavljenog na BeyondTrust siteu.

Trebamo skinuti paket za Linux distro koju želimo učlaniti u Active Directory.



Slijedi sažet pregled mojih iskustava glede učlanjenja Ubuntu Servera 11.10 u Win 2008 R2 forest te Ubuntu Desktopa 11.04 u Win 2003 forest. Ubuntu server je, kako mu i dolikuje, bez X-a; Ubuntu stanica, kako njoj dolikuje, s X-om; Active Directory instance rade u njihovim najnaprednijim modovima, na GUI edicijama windoza.

a. produkt je odlično dokumentiran; dovoljno je pratiti naputke iz priručnika da bi priprema Ubuntu boxa, potom i povezivanje s forestom, prošli sasvim ležerno i glatko. Važno je samo da oni koji s Linuxom nisu baš na „ti", krenu od poglavlja Configuring clients before PBIS agent installation.

b. PBISOE setup pored nekolicine servisa instalira i 30-ak admin alata – uglavnom su u /opt/pbis/bin - što za administriranje tog servisa što za dijagnostiku/tshooting relacije Linux računalo <=> AD;

c. PBISOE ne zahtjeva bilo kakve zahvate na Domain Controllerima ili, poput Sambe ako ju želimo postaviti u ADS režimu rada, opsežna dokonfiguriranja Linux boxa koja se mjestimice pretvaraju u prave improvizacije (a što će se kasnije, poučava nas praksa, pretvoriti u barijeru upgradeima Linux računala ili AD sustava);

d. učlanjenjem u domenu, Ubuntu računalo:

- postaje svjesno AD siteova (site affiliation)
- postaje svjesno forest trustova i svih domain controllera matičnog foresta te, zaista dojmljivo, svih Domain Controllera foresta s kojime postoji trust
- dopušta ulogiravanje – interaktivno ili SSH konekcijom - uporabom accounta matične domene i svake domene s kojom postoji odgovarajući trust (znači, account može biti iz drugog foresta); na istom računalu moguće je rabiti lokalne i domenske accounte, k tomu istovremeno
- dopušta ugnježđivanje domenskih accounta ili grupa u lokalne admin ili user grupe
- tijekom etape autentikacije i autorizacije rabi Kerberos/LDAP protokole uskladive s domenskim
- ima svoj objekt u AD-u s par info o OS-u (domenske GPO na taj objekt **ne** djeluju, za to je potrebna Enterprise edicija PBIS-a)
- promjenu passworda uredno replicira na Domain Controller s kojime trenutno komunicira – razumljivo, rečeno važi za domenski account, ne za lokalni

* Uočite prikriveni benefit točke **d.**: Single-Sign-On na domenske resurse, pri čemu podjednako ciljamo na Windows i Linux dijeljene resurse. Informatički osvješteni djelatnici znaju to cijeniti!

PuTTY, vsftpd, WinSCP, SSH, Samba F&P sharing... spadaju u aplikacije koje bez ikakvih prilagodbi mogu rabiti domenske accounte (za višenamjensku Sambu PBISOE ima zaseban konfiguracijski alat samba-interop-install); načelno, tako će raditi sve aplikacije koje se za autentikaciju/autorizaciju oslanjaju na NSS i PAM module. Postfix je primjer aplikacije koja **ne** spada u tu kategoriju jer mail klijente autenticira primijenjeni LDA/MDA a PBISOE se ne povezuje s njime. Glede Postfixa, valja ipak reći da on i nakon učlanjenja Ubuntu servera u domenu normalno odrađuje svoje poslove, samo s lokalnim accountima; nadalje, moguće ga je dokonfigurirati za uporabu domenskih accounta ali to je već sasvim nepovezano s temom...

Slijedi izvješće s Ubuntu Servera 11.10, „friško" učlanjenog u testni Win 2008 R2 forest. Dobro će vam doći kao referenca ako odlučite isprobati ovako nešto jer pokazuje da je sve OK.

*

corecar@ubusrv10-2:/opt/pbis/bin#**./get-status**
LSA Server Status:

Compiled daemon version: 6.5.561.63589
Packaged product version: 6.5.561.63589
Uptime: 0 days 0 hours 21 minutes 0 seconds

[Authentication provider: lsa-activedirectory-provider]

Status: Online
Mode: Un-provisioned
Domain: WINUX.CORECAR.HR
Domain SID: S-1-5-21-2382663490-1430662848-3673307170
Forest: winux.corecar.hr
Site: ZAGREB
Online check interval: 300 seconds
[Trusted Domains: 1]

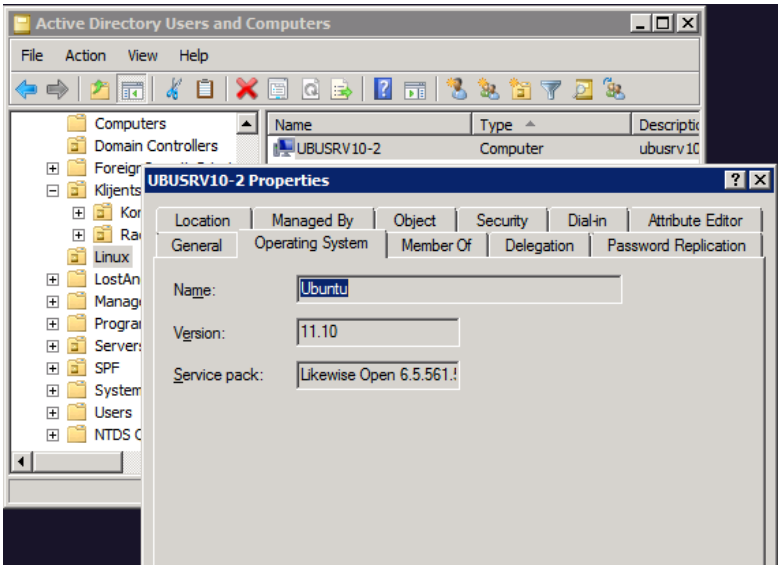
[Domain: WINUX]
DNS Domain: winux.corecar.hr

Netbios name: WINUX
Forest name: winux.corecar.hr
Trustee DNS name:
Client site name: ZAGREB
Domain SID: S-1-5-21-2382553490-1430662848-3573307170
Domain GUID: 4f758bf4-3528-654e-9850-9d2eb3fd4c82
Trust Flags: [0x001d]
[0x0001 - In forest]
[0x0004 - Tree root]
[0x0008 - Primary]
[0x0010 - Native]
Trust type: Up Level
Trust Attributes: [0x0000]
Trust Direction: Primary Domain
Trust Mode: In my forest Trust (MFT)
Domain flags: [0x0001]
[0x0001 - Primary]

[Domain Controller (DC) Information]
DC Name: DNS-DC1.winux.corecar.hr
DC Address: 10.10.110.112
DC Site: ZAGREB
DC Flags: [0x000031fd]
DC Is PDC: yes
DC is time server: yes
DC has writeable DS: yes
DC is Global Catalog: yes
DC is running KDC: yes

[Global Catalog (GC) Information]
GC Name: DNS-DC1.winux.corecar.hr
GC Address: 10.10.110.112
GC Site: ZAGREB
GC Flags: [0x000031fd]
GC Is PDC: yes
GC is time server: yes
GC has writeable DS: yes
GC is running KDC: yes

Slika skinuta s Domain Controllera pokazuje da ovaj posredno potvrđuje izvješće gore spomenute naredbe get-status: PBISOE je uspješno učlanio Ubuntu server u AD sustav.



*

Na kraju da pojasnim zašto sam se „zalijepio" baš za BeyondTrustov PowerBroker, jer postoje i drugi respektabilni igrači u ovom području: Microsoft, Centrify, Quest Software, Symark, Samba/Winbind.... BeyondTrust je sponzor poznatog Likewise Open projekta i na njemu gradi svoje PBIS rješenje. Likewise Open je, pak, široko prihvaćen od Linux zajednice, primjerice, Canonical je u svoju Ubuntu distribuciju dodao prilagođen Likewise Open za povezivanje Ubuntu boxa s AD-om, VMware oprema svoje ESX hostove Likewise agentom, i sl. Kalkuliram - rekao bi poznati detektiv Nik Praskaton - ja primijenim PBISOE i sve je super... ali jao!, BeyondTrust prestane razvijati besplatnu ediciju a meni se baš ne plaća komercijalna Enterprise edicija... heh, tada se lako preusmjerim na Likewise Open, bilo izvorni bilo customizirani. S druge strane, ako management uoči da Linux <–> Windows orkestracija donosi i poslovni benefit, pa je poželi unaprijediti, zasigurno će biti spreman izdvojiti određena sredstva za jaču, komercijalnu Enterprise PBIS ediciju.

Glede Microsoftovog servisa Identity Management for Unix, prisutnog u Windows 2008 R2 serverskoj distribuciji (podkomponenta je AD DS uloge): radi se o pomno razrađenom interoperability rješenju, ali specifične namjene – njime se Windows treba što bešavnije uklopiti u *ux okolinu već organiziranu u Network Information Service sustav, za dodatne info vidi http://technet.microsoft.com/en-us/library/cc731178.aspx.

<kraj>