Windows Active Directory i Group Policy

Igor Hitrec, SRCE

Sadržaj:

- Windows Active Directory (AD)
- Windows Group Policy (GP)
- Zaključak

Windows Active Directory (AD)

- Zašto AD
- AD općenito
- AD - replikacija, servisi/protokoli
- AD - shema
- AD - Kerberos
- AD - NTLMv2
- AD - prava na objektima/ atributima
- AD - DNS, značajke
- AD - DNS, Unix BIND interoperabilnost
- AD - DNS, uloga SRV zapisa
- AD - DNS, malo o sigurnosti

Zašto AD

- “Dobitna kombinacija”:
  - (Ne)održavanje OSa i aplikacija
  - Prevelike ovlasti na sustavu (Administrator by default)
  - Nestručnost korisnika
- AD nudi jedini prihvatljivi način održavanja većega broja osobnih računala pod Windows OSom

Zašto AD

- Imate li vremena održavati više od 20 samostalnih računala?
  - briga o zakrpama
  - briga o virusnim definicijama
  - održavanje korisničkih aplikacija
  - briga o korisničkim problemima
  - sigurnosno spremanje podataka, pristup mrežnim pisačima…
  - Lakše definiranje zajedničkog mrežnog okruženja…

AD općenito

- Lokacija: \%Systemroot%\NTDS\ntds.dit
- Format: ESE (Extensible Storage Engine)
- Ograničenja: teoretski 17TB, praktično 4TB
- Veličina baze 1.4GB (defragmentirana) sadrži:
  - 100.000 korisničkih računa sa 30 atributa veličine po 10 byteova
  - 100.000 računalnih računa
  - 10.000 grupa koje sadrže po 25 korisnika
  - 10.000 mrežnih pisača sa 15 atributa veličine 10 byteova
  - Dodavanjem 1.3kB digitalnog certifikata za svaki korisnički račun baza raste za 1.1GB (ukupno 2.6GB)
  - Dodavanjem fotografije veličine 16kB svakome korisniku povećava bazu za dodatnih 2.6GB (ukupno 5.2GB)
  - Instalacijom MS Exchange 2000 baza raste za dodatnih 490 MB (dodavanje novih atributa objektima ADa) na ukupno 5.6GB

Preuzeto iz **Building Enterprise Active Directory Services: Notes from the Field, izdavač MS Press, stranica 120**

AD - replikacija, servisi/protokoli

- Za replikaciju ADa - KKC servis uz RPC i SMTP
- za SYSVOL replikaciju - NTFRS servis uz RPC

AD - replikacija, protokoli/portovi

- RPC - inicijalno TCP 135 a potom mijenja broj porta dinamički
  - Fiksno određivanje portova opisano u KB224196
- NTFRS - inicijalno TCP 135 a potom mijenja broj porta dinamički
  - Fiksno određivanje portova opisano u KB319553
- Problem firewallinga - KB154596
- Problem domain trustova - KB179442

AD - shema

- AD shemu mijenjajte PAŽLJIVO!
- regsvr32.exe schmmgmt.dll
- Schema Admins grupa neka bude prazna
- auditing/monitoring za “Shema Update Allowed”
- postupak Recoveryja/Restorea sheme je složen…

AD - Kerberos

- Defaultni autentifikacijski protokol, RFC 1510
- Brži od starog NTLMa (UDP vs. RPC)
- Koristi uzajamnu autentifikaciju
- pogodan za Smart Cards
- Korisnički “master key” napravljen je pomoću korisničke lozinke (sigurnija politika korištenih lozinki!)
- KerbCrack http://ntsecurity.nu/toolbox/kerbcrack

AD - NTLMv2

- kada se Kerberos ne može koristiti
- Forsirajte 128bitnu enkripciju i isključivo NTLMv2 protokol za RPC sesije - KB239869, KB147706
- Odgovarajući Group Policy objekt postoji za Windows 2003
- Ako se želite riješiti LM hasha - KB299656
- Pazite - Win9x klijenti neće moći mijenjati lozinku čak i uz instaliran ADCE, UNIX/Mac PAMovi neće ispravno raditi…

AD - prava na objektima/ atributima

- Svaka vrijednost/atribut svakoga objekta može imati svoja specifična prava pristupa
- Konflikt može nastati između eksplicitnih i nasljednih prava, eksplicitno pravo prevladat će naslijeđeno pravo
- Vidljivost raspoloživih prava na objektima i atributima definirana je unutar obične ASCII datoteke \%Systemroot%\System32\dssec.dat
  - “7” sakriva stavku
  - “6” apokazuje Read pravo
  - “5” pokazuje Write pravo
  - “0” ili prazno prikazat će sva prava

AD - DNS, značajke

- SRV zapisi
- Inkrementalni zone transfer
- Objava promjena unutar zona
- AD integrirane zone (sastavni dio AD baze)
- AD prava nad objektima DNS zona
- AD sigurnost pri dinamičkom osvježavanju zapisa u zoni
- Podrška tzv. Conditional Forewarding - npr. upiti na .hr domenu idu na jedan DNS server a ostali na drugi server

AD - DNS, Unix BIND interoperabilnost

- Tijekom instalacije ADa u \%Systemroot\System32\Config nastaje datoteka netlogon.dns koja sadrži potrebne SRV rekorde - datoteku importirajte u Unix BIND
- MSov AD primarni, Unix BIND sekundarni i ostale kombinacije
- AD sigurnost dinamičkog osvježavanja zapisa ipak je karakteristika samo AD integriranog DNSa (a AD WINS?)

AD - DNS, uloga SRV zapisa

- Omogućuju pronalaženje potrebnih servisa, definiraju protokol i broj porta, osiguravaju load-balancing

_service._protokol.imedomene SRV prioritet# težina# port# FQDN

- Podaci o LDAPu(_ldap), Kerberos poslužitelju (_kerberos), Global katalogu (_gc), mijenjanja Kerberos lozinke (_kpasswd).
- SRV zapis može sadržavati i GUID broj poslužitelja što je korisno kada ga klijenti znaju ali je on prebačen u novu DNS domenu

AD - DNS, malo o sigurnosti

- Čuvajte se “gotovine” (Cache) - “Secure cache against pollution”opcija
- Svakako ugasite zone transfer, (AD DNS samo za internu uporabu)
- DIG (http://www.isc.org/products/BIND)
- DNSCMD (unutar Win2000 resource kita)
- DNSLINT za testiranje DNS funkcionalnosti - KB321045
- DNSDIAG (samo za Windows 2003)
- Zapamtite: AD DNS služi ADu i dio je INTERNE infrastrukture

Windows Group Policy (GP)

- GP - općenito
- GP - predlošci (templates)
- GP - rad sa predlošcima - SCA
- GP - rad sa predlošcima - SECEDIT
- GP - praktična primjena
- GP - alati za testiranje i rješavanje problema
- GP - kako to radi?
- GP - Computer Configuration/User Configuration
- GP - GP ostaju…
- GP - poredak primjene
- GP - Kada su Internet veze spore…

Windows Group Policy (GP)

- GP - loopback mod, zamjena umjesto spajanja
- GP - Podešavanje intervala osvježavanja
- GP - primjena GPa asinkrono
- GP - Group Policy Management konzola
- GP - Group Policy sigurnosne postavke
- GP - nametanje kompleksnih lozinki
- GP - inzistirajte na dugim lozinkama
- GP - Ograničenje pristupa “Anonymous” korisniku
- GP - Primjer NULL sesije
- GP - Rješenje problema NULL sesije

GP - općenito

- Osnovna funkcija GPa - osiguravanje poslužitelja i radnih stanica kroz infrastrukturu ADa
- Koristite tzv. sigurnosne predloške pohranjene na SYSVOL shareu svakoga domain kontrolera
- Prepravite registry vrijednosti ili dodajte nove
- Upravljajte pravilima za korisničke račune, članstvima u grupama
- Mijenjajte izgled radne okoline
- Upravljajte odlaznim i dolaznim prometom na računalima

GP - predlošci (templates)

- Obični ASCII tekst, .INF ekstenzija
- Svakim Service Packom obično se povećavaju opcije upravljive GPjem
- mmc - Security Template - Generic
- GP predloške možete skinuti sa mreže (Microsoft, NSA, CIS)

GP - rad sa predlošcima - SCA

- Poseban MMC - Security Configuration & Analysis (SCA)
- Definiranje predloška, njegova primjena i provjera promjene postavki prije same primjene, uvoz i izvoz postojećih postavki
- Ovim alatom se ne mogu mijenjati postavke udaljene radne stanice, zato postoji komandnolinijski alat SECEDIT

GP - rad sa predlošcima - SECEDIT

- Pokrenite “SECEDIT /?” za ispis svih opcija
- Koristite mogućnost “SECEDIT /GENERATEROLLBACK”
  - omogućuje stvaranje sigurnosne kopije postojećega stanja
  - samo kod XP/2003 sustava

GP - praktična primjena

- Promjena/dodavanje registry vrijednosti
- Instalacija aplikacija (.MSI i .ZAP paketi)
- Izvršavanje skripti (logon/logoff, startup/shutdown)
- Instalacija i upravljanje IPSec podrškom
- Instalacija i upravljanje PKI unutar ADa
- Blokiranje neželjenog softvera
- Upravljanje Internet Explorerom
- RIS
- Preusmjeravanje korisničkih mapa…

GP - alati za testiranje i rješavanje problema

- GPTOOL - unutar Resource kita, provjerava konzistenciju i broj inačice
- SECEDIT- za rješavanje raznih problema (pročitajte KB227302 i KB227448)
- GPRESULT -detaljan prikaz djelovanja GPa - KB258595 i KB250842
- ADDIAG -troubleshooting primjene .MSI paketa
- GPOLMIG - alat za migraciju NT 4.0 System Policy sustava u GP
- GPUPDATE - XP/2003 verzija SECEDITa, podržava i obavezni reboot ili logoff
- DCGPOFIX - ako pokvarite tzv. Default Domain /Controller policy postavke ☺

GP - kako to radi?

- “Linka” se na cijelu domenu/site/OU
- Učitava pri pokretanju računala (Boot Up), prijavi korisnika (Logon) i u zadanim vremenskim intervalima
- Pri pokretanju računala šalje LDAP upit koje policyje treba učitati i kojim redoslijedom LDAP://cn=Policies,cn=System,dc=imedomene
- GP može upućuje računalo ili korisnika da preuzme i pokrene odgovarajuće skripte ili datoteke sa SYSVOL mape
- Policy spremljen na putanju \\imeposlužitelja\SYSVOL\imedomene\Policies unutar mape imena GUID broja samog policyja

GP - Computer Configuration/User Configuration

- “Computer Configuration” sadrži postavke koje će se primijeniti na računalu bez obzira tko radi za njime, prevladavaju nad “User Configuration” postavkama
- “User Configuration” postavke
  - prilikom prijave određenog korisnika
  - gube se prijavom drugoga korisnika

GP - GP ostaju…

- …unutar ADa iako trenutno nisu nigdje u funkciji - “linkanjem” su opet tu…
- Napravite nekoliko GPova za hitna stanja ali vežite samo kada je hitno

GP - poredak primjene

- Pravilo u slučaju konflikta jest da prevlada ono koji se primjeni kasnije
- Za iznimke koristite “Block Inheritance” i “No Override”
- LSD-OU (Lokalni, Site, Domenski, OU)

GP - loopback mod, zamjena umjesto spajanja

- Želimo forsirati primjenu “User” postavki GPa na računalu - Internet kiosci, javna računala
- Computer Configuration\Administrative Templates\System\Group Policy “User Group Policy Loopback Processing Mode”
- “Replace” - zanemari postojeće “user” postavke
- “Merge” - primijeni obje postavke, konflikt forsira loopback postavke
- ZAPAMTITE: “Loopback” nadvadava “No Override” GPove

GP - Kada su Internet veze spore…

- Mogućnost detekcije spore Internet veze - Zadana vrijednost je 500Kbps
- .MSI/.ZAP paketi se ne instaliraju
- Nema posebne postavke Internet
- Nema diskovnih kvotama i redirekcija korisničkih mapa
- Sigurnosne postavke, EFS i registry postavke te IPSec primjenjuju se uvijek

GP - Podešavanje intervala osvježavanja

- svakih 90 minuta uz slučajnu vrijednost plus/minus 0 - 30 minuta (osim DCova)
- interval 0 - 64800 minuta daje praktičan okvir od svakih nekoliko sekundi do svakih 45 dana
- Najviša slučajna vrijednost jest 1440 minuta odnosno jedan dan
- Uključivanjem opcije “Turn Off background Refresh of Group Policy” (“Computer” Conf.)
  - učitavat će se samo odjavom korisnika
  - isključeno učitavanje GPova kod prijave korisnika

GP - primjena GPa asinkrono

- GPovi vezani na računalni AD korisnički račun (Computer account) učitavaju se do pojave poruke “Press Ctrl-Alt-Delete to Logon”
- GPovi vezani na korisnički račun (User account) učitavaju se do pojave cijele Desktop okoline
- Kako ovaj proces može potrajati postoji mogućnost tzv. asinkrone primjene GPova

GP - Group Policy Management konzola

- Prvo smo je upoznali kod SBS 2003, kasnije raspoloživa za donwload za XP/2003, zatim unutar Windows 2003 Sp1

  http://www.microsoft.com/windowsserver2003/gpmc/default.mspx

- Nova osobina jest jednostavna mogućnost backupa/restorea GPova

GP - Group Policy sigurnosne postavke

- Forsiranje pojedinih sigurnosnih postavki lozinke
- Najmanja dužina, kompleksnost, pamćenje korištenih lozinki, uvjeti blokiranja korisničkoga računa
- Učite korisnike da koriste dugačke i za njih lako pamtljive lozinke (passphrase vs. password)

GP - nametanje kompleksnih lozinki

- Za domenu uključite opciju
  Computer Configuration\Windows Settings\Account Policies\Password Policy\Password Must Meet Complexity Requirements
- Korisnik ne može koristi svoje ime kao lozinku
- Lozinka mora imati minimalno 6 znakova
- Obavezno korištenje najmanje tri od četiri kategorije (velika slova, mala slova, posebni simboli i brojevi)
- Kompleksnost je dobra no bolja je dužina…

GP - inzistirajte na dugim lozinkama

- Duže ali smislene i pamtljive lozinke su bolje, npr:
- Vozim plavoga volva s40 - 23 znakova
- W4(#5mrak - 9 znakova
- Obje lozinke dovoljno su kompleksne no prva je otpornija na “brute force” napad

GP - Ograničenje pristupa “Anonymous” korisniku

- Poznati “null user session” problem
- Napadač dobije listu svih korisničkih računa u domeni
- Username i password su null znakovi
- Boljka aplikacija koje koriste SMB protokol
- korisnik Null sesije dobiva unaprijed zadani SID S-1-5-7, zadani SIDovi - KB243330

GP - Primjer NULL sesije

D:\WINNT>net view \\pc-korisnik
System error 5 has occured.
Access is denied.

D:\WINNT>net use \\pc-korisnik\ipc$ “” /user:””
The command completed succesfully.

D:\WINNT>net view \\pc-korisnik
Shared resources at \\pc-korisnik

Share name Type Used as Comment

InterChk Disk
wininstall Disk
The command completed successfully.

GP - Rješenje problema NULL sesije

- GP stavke (XP/2003) Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

- 1. Network access: Do not allow anonymous enumeration of SAM accounts - **omogućeno**
- 2. Network access: Do not allow anonymous enumeration of SAM accounts and shares - **omogućeno**
- 3. Network access: Let Everyone permissions apply to anonymous users - **onemogućeno**
- 4. Network access: Named pipes that can be accessed anonymously - **testirajte zbog mogućih problema sa pojedinim aplikacijama**

GP - Rješenje problema NULL sesije

- 5.Network access: Remotely accessible registry paths and subpaths - **testirajte zbog mogućih problema sa pojedinim aplikacijama**
- 6. Network access: Restrict anonymous access to Named Pipes and Shares -**omogućeno**
- 7. Network access: Shares that can be accessed anonymously - **testirajte zbog mogućih problema sa pojedinim aplikacijama**
- 8. Network access: Allow anonymous SID/Name translation - ako je ova opcija omogućena imati ćete problema sa napadima korištenjem poznatih SIDova

Zaključak

- AD & GP - preporuke
- AD & GP - Dobra praksa…

AD & GP - preporuke

- Barem dva domain kontrolera po domeni
- Pazite na slobodni prostor na disku
- Odvojite AD bazu i AD log datoteke na dva različita diska
- Redoviti backup - backup stariji od 60 dana ne prolazi (zadana tombstone vrijednost)
- Izvježbajte AD Restore proceduru

AD & GP - Dobra praksa…

- Uvijek započeti za kompletno zakrpanim računalom
- Ugasiti servise koji se ne koriste
- Odvojiti sistemske od korisničkih podataka
- koristiti slipstream instalaciju SPova i zakrpi
- npr. Windows 2003 SP1

1. C:\Win2003SP1\WindowsServer2003-KB889101-SP1-x86-ENU.exe /x
2. C:\Win2003SP1\i386\Update\Update.exe -s:g:\Win2003install

AD & GP - Dobra praksa…

- Odvojite korisničko od administratorskog okruženja
- Korisnika obučiti da koristi kompleksniju lozinku (Passphrase umjesto Passworda)
- Onemogućiti NTLM, koristiti NTLM v2
- Koristiti RunAS komandu ili RunAs skriptu
- Centralizirana antivirusna nadogradnja
- Centralizirana nadogradnja zakrpama