Active Directory - podaci "na pladnju" - glava "na panju"

pon, 2018-05-28 13:19 - Ratko Žižek

Prisjetimo se višestruke uloge Active Directory (dalje: AD) sustava: posredstvom Group Policy i pratećih upravljačkih alata omogućuje nam efikasno administriranje Windows (može i Linux) računala određene ustanove; ujedno je, budući da mu je osnovica LDAP servis, baza raznovrsnih podataka o korisnicima, računalima i servisima te ustanove. Zahvaljujući spomenutim ulogama, Active Directory omogućuje autentikaciju i autorizaciju na IT resurse. Dakle, s obzirom na rečeno, da kojim slučajem obnašam časnu ulogu administratora AD-a, ne bih baš bio sretan s ovime što slijedi....

Pretpostavimo ovu situaciju:

* imamo jednodomenski AD sustav - to je preporučeni, u Hrvatskoj i najzastupljeniji arhitekturalni model;

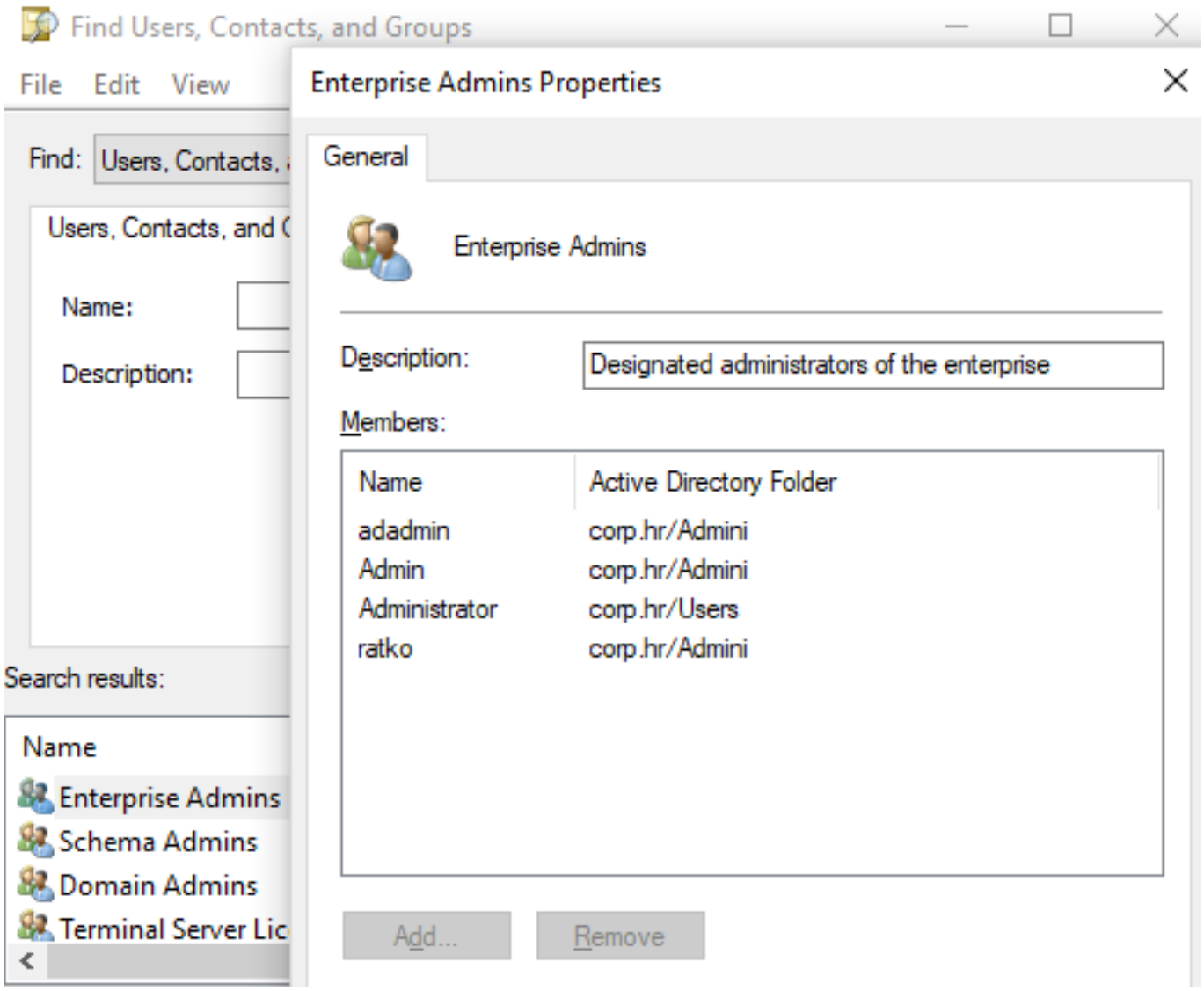
* Domain Controlleri, bazirani na Windows Server 2016, nalaze se u zasebnom mrežnom segmentu - opet, u skladu s *best practices*;

* shodno gornjem, Windows 10 računala su u tzv. klijentskom ogranku korporativne mreže;

* Na Windows 10 stanicu, članicu Windows domene (AD-a), ulogirani smo s domenskim računom koji je, glede prava, i na stanici i u AD-u običan korisnik (*standard user*).

Kakve sve podatke o djelatnicima i računalima svoje ustanove može takav "obespravljeni" korisnik iščitati iz AD-a? Odgovor je kratak i uznemirujuć: teško za opisati!

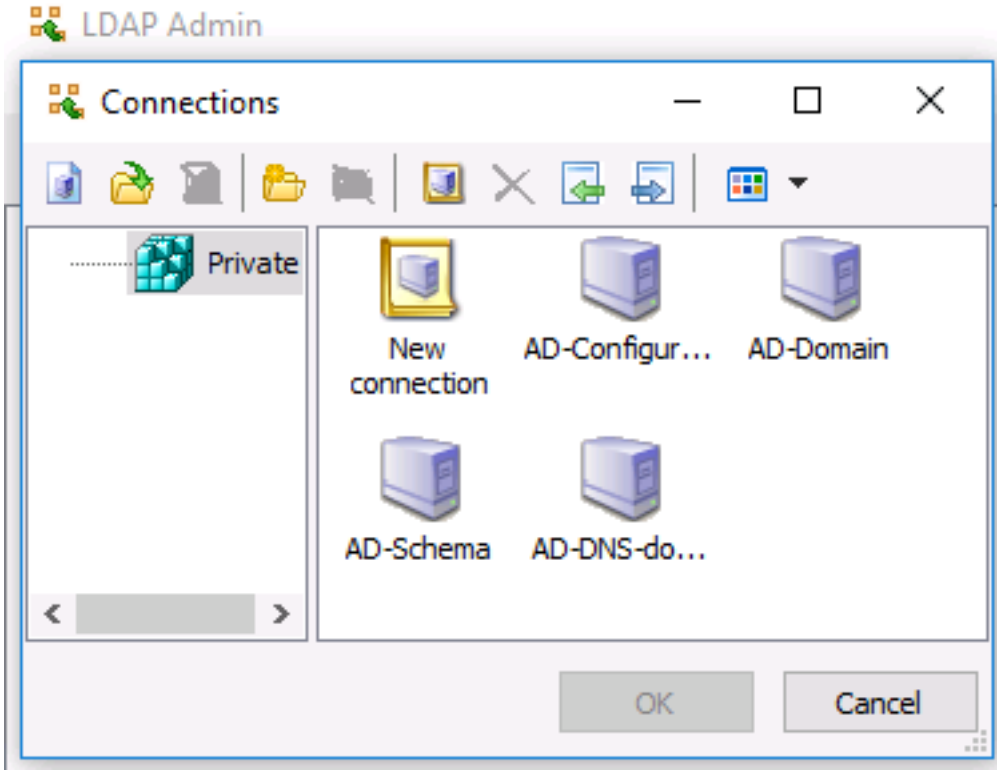
Naš znatiželjni korisnik ne mora se zamarati s rebusima poput **"%windir%\System32\rundll32.exe" dsquery.dll,OpenQueryWindow** - s time nek se pate nadobudni informatičari, jel'te - jer isti alat za pretraživanje AD-a može elegantno pokrenuti iz Windows Explorera klikom na naredbi Search Active Directory. Potom će u hipu, s par samorazumljivih operacija, saznati koji su sve korisnici, računala i grupe u AD-u. Na nižoj slici vidimo kako pregledava članstvo sigurnosno senzitivnih AD grupa Domain, Enterprise i Schema Admins.



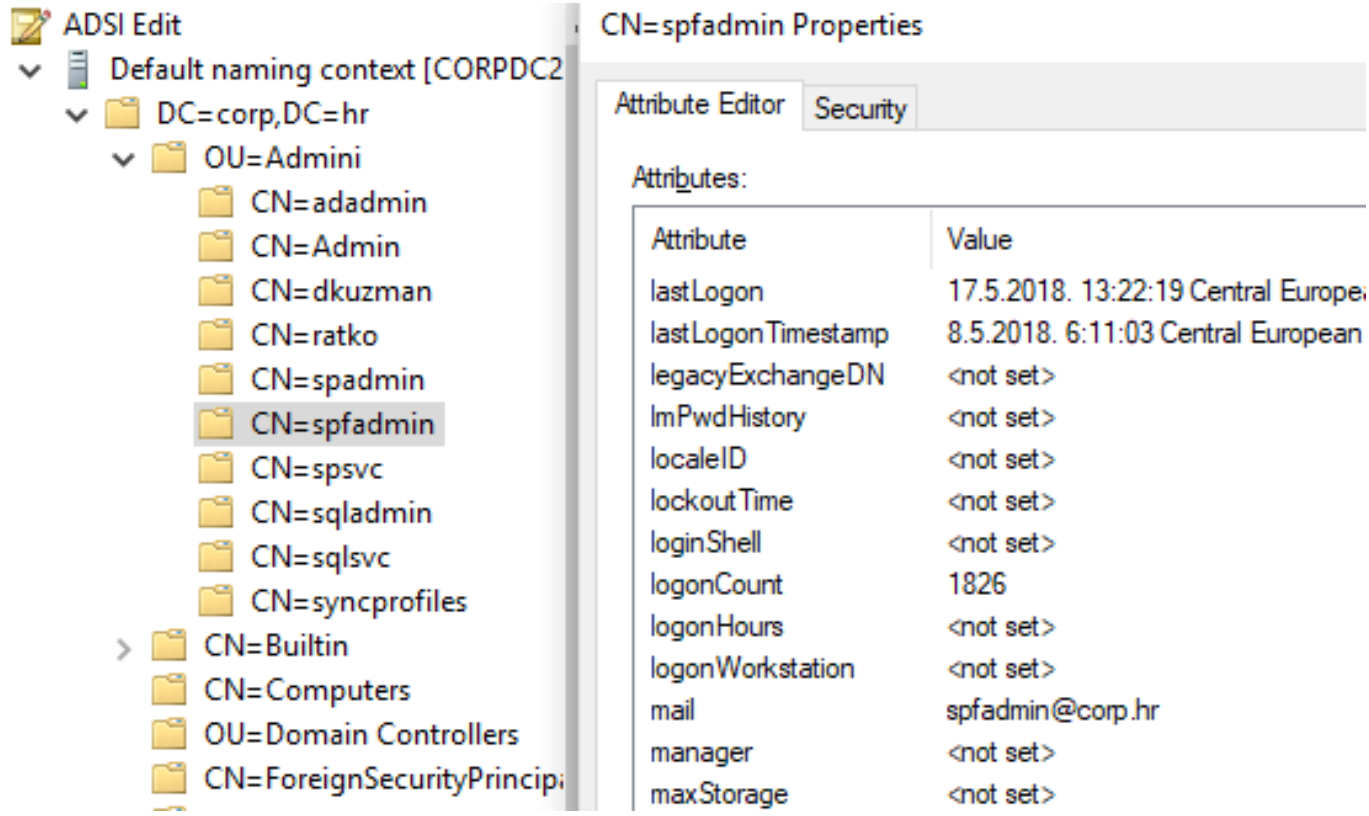
Običan korisnik računala može pokrenuti CMD naredbe poput **gpresult** i **nltest** pa kombiniranjem njihovih opcija prikupiti svakojake *low-level* informacije o AD-u. Na nižoj slici korisnik ispituje značajke Domain Controllera koji ga je autenticirao. Popis aktivnih DC-eva i njihov razmještaj po AD siteovima - uočite, riječ je o topologiji AD servisa - prikazati će opcija **/dclist:**.

```
C:\Users\boss1>nltest /dsgetdc:corp.hr
           DC: \\CORPDC2.corp.hr
      Address: \\10.1.147.55
     Dom Guid: b3d39dfb-0bd2-4d5e-9dd3-1eca0d913654
     Dom Name: corp.hr
  Forest Name: corp.hr
 Dc Site Name: Centar
Our Site Name: Centar
        Flags: PDC GC DS LDAP KDC TIMESERV GTIMESERV WRITABLE DNS_DC
 DNS_DOMAIN DNS_FOREST CLOSE_SITE FULL_SECRET WS DS_8 DS_9 DS_10
The command completed successfully
```

Znamo da običan korisnik računala ne može instalirati aplikacije bez podrške administratora stanice, znači, nedostupna mu je suita alata poznata kao Remote Server Administrative Tools (RSAT), s konzolama za administriranje AD-a, ds*.exe naredbama i Powershell ADDS modulom. Niti alate tzv. treće strane neće moći instalirati. Ali, ako je imalo dosjetljiv, potražiti će alat kojega niti ne treba instalirati, poput LDAP Admina. Dakle, skine taj kompaktni LDAP preglednik s Interneta, pokrene ga, spoji se sa svojim računom na *root* AD particija, od domene preko konfiguracijske... sve do DNS-a ako je ovaj integriran s AD-om (vidi nižu sliku) i - EUREKA - zamalo pa nema tog zakutka AD-a u kojega naš znatiželjni korisnik ne može gurnuti nos! Da se admini AD-a ne bi zapitali zašto je tako dugo konektiran na DC, svo to podatkovno blago spremiti će na disk i baviti se njime kad mu se prohtije.



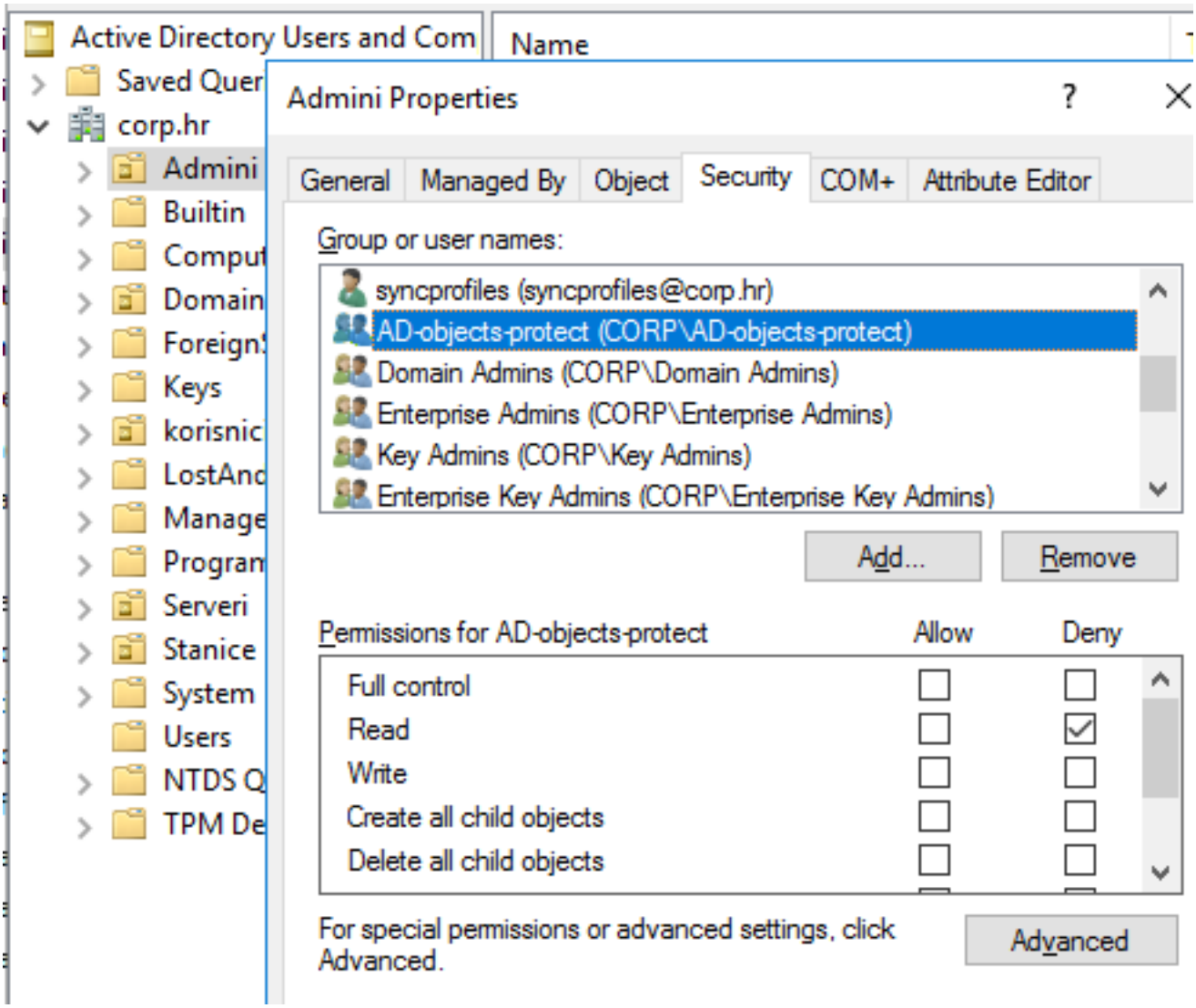
Dolazimo tako do paradoksalne situacije da običan korisnik Windows računala ne može uključiti Network Discovery i File and Print Sharing funkcionalnosti na svojoj stanici, ali može usnimiti maltene cijeli AD sustav! Po logici stvari, korisnik s administratorskim ovlastima na stanicu ima širi manevarski prostor, može si instalirati svakojake alate, tipično, RSAT pa konzolama poput AD Users and Computers, Sites and Services, ADSIEdit... odn. PowerShell modulom za AD pregledavati objekte i njihove atribute. Na slici vidimo kako u ADSIEdit čita značajke računa s raznim admin dozvolama na AD. Pokrene li Group Policy Management, ne samo da može pregledavati svaku politiku nego odabrane, poput onih za DC-eve, može lokalno spremiti u HTML formatu i na miru proučavati.



Da, od samih je početaka AD sustav zamišljen kao repozitorij podataka o djelatnicima i računalima neke ustanove, pretraživ od strane najšireg auditorija, sve kako bi se olakšala komunikacija i suradnja djelatnika te ustanove. Nažalost, to pravo čitanja je bilo i ostalo neselektivno pa svaka osoba s domenskim akreditivima može, kako smo vidjeli, iščitati podatke o telefonu i radnoj prostoriji kolege, što ima puno opravdanje, ali - za ovo je teško naći pokriće - s jednakom lakoćom će prikupiti podatke o kontrolerima i serverima domene, članstvu administrativnih grupa, topologiji i particijama AD-a... puno-i-previše toga za bilo koga osim administratora AD-a! Podsjetimo da je naš radoznali korisnik iz gornjeg dijela ovog članka njuškao po najnovijoj inkarnaciji AD-a, onoj koju donosi Windows Server 2016. Što pokazuje da je Microsoft, usprkos tucetu vrijednih unaprijeđenja ovog sustava i brojnih dokumenata na temu njegove zaštite, opet propustio učiniti ono najkorisnije adminima AD-a - ugraditi u sustav instrumentarij za efikasno maskiranje svih senzitivnih podataka od onih individua - djelatnika, partnera, uljeza - koji ih ili ne trebaju ili ne smiju vidjeti. Rečeno dobija na težini kad se prisjetimo da danas, u ozračju implementacije GDPR uredbe, među senzitivne podatke više ne spadaju samo poslovni nego i osobni podaci. Tako da za AD admine pravi izazov trenutno nije upravljanje računalima nego podacima u LDAP-u AD-a jer ih maltene "svaka šuša" može vidjeti. I zlorabiti. A tada na red dolazi pitanje odgovornosti...

Objekte važne nama IT-evcima, poput servisnih i administrativnih računa i grupa, lako ćemo sakriti od znatiželjnih očiju, načelno to ide ovako:

- kreirati organizacijsku jedinicu (OU) i u nju premjestiti predmetne objekte - voditi računa da se DC-evi i neke domenske grupe ne smiju micati iz svojih matičnih OU-ova, srećom, smijemo u taj novi OU utrpati grupe DNS Admins, Domain Admins, Enterprise Admins, Schema Admins, Domain Users i Domain Computers;
- u tom OU kreirati globalnu grupu, npr. protected-objects i u nju učlaniti sve korisnike (njihove objekte, dakako) koje želimo spriječiti u čitanju senzitivnih podataka;
- u pregledu dozvola za tu grupu postaviti Read na Deny.



Desi li se da nam nadređeni, potaknuti sve izraženijom potrebom zaštite poslovnih i osobnih podataka, dadu nalog da primijenimo model po kojem različite grupe korisnika mogu vidjeti različite objekte AD-a, imat ćemo jako puno posla. Radi se o tome da određene tipove podataka moraju moći pročitati ne samo ljudi nego i aplikacije i računala da bi ispravno funkcionirali, također, ne možemo primijeniti jednostavni Deny Read kriterij kako smo maloprije učinili. Iako je zaštita podataka od čitanja izvediva, zbog nedostatka ugrađenih kontrola te namjene riječ je o zahtjevnom poslu: treba se dobro pripremiti, oblikovati i testirati moguća rješenja, vjerojatno će se morati i restrukturirati AD. Jednoznačnih uputa, koliko vidim, nema - javite ODMAH ako ih otkrijete :o) - pa kao neku dobru polaznu točku mogu preporučiti http://www.itprotoday.com/management-mobility/hiding-data-active-directory-part-3-enabling-list-object-mode-forest [1]. Na kraju treba reći i ovo: ako nam je zaista stalo do zaštite podataka u AD-u, zaštita skrivanjem (nevidljivošću) je samo jedna od brojnih mjera koje moramo poduzeti, prioritet je *hardening* Domain Controllera, potom na red dolaze i brojne druge mjere obrađene u dokumentima
poput https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory [2].

Vijesti: Windows [3]
Kuharice: Windows [4]
Kategorije: Mrežna sigurnost [5]
Vote: 5

Vaša ocjena: Nema Average: 5 (3 votes)

story_tag: active directory [6]
windows [7]
zaštita [8]
vidljivost [9]
skrivanje [10]

Source URL: https://sysportal.carnet.hr./node/1810

Links
[1] http://www.itprotoday.com/management-mobility/hiding-data-active-directory-part-3-enabling-list-object-mode-forest
[2] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
[3] https://sysportal.carnet.hr./taxonomy/term/12
[4] https://sysportal.carnet.hr./taxonomy/term/18
[5] https://sysportal.carnet.hr./taxonomy/term/33
[6] https://sysportal.carnet.hr./taxonomy/term/154
[7] https://sysportal.carnet.hr./taxonomy/term/76
[8] https://sysportal.carnet.hr./taxonomy/term/204
[9] https://sysportal.carnet.hr./taxonomy/term/242
[10] https://sysportal.carnet.hr./taxonomy/term/243