A Ilica 242, HR-10000 Zagreb
T (01) 2222 182
E student@algebra.hr
www.algebra.hr

ALGEBRA

KATEDRA ZA OPERACIJSKE SUSTAVE

Operacijski sustavi

Lab 10 – Korisnici, grupe i dozvole pristupa

REV 1.0

Sadržaj

Korisnički račun

Kako bi se korisnik jednoznačno identificirao na računalu, mora imati korisnički račun (eng. *User Account*), koji omogućava dodjelu određenih prava i privilegija korištenja dijelova računalnog sustava. Važno je napomenuti da bi svaki korisnik računalnog sustava trebao imati svoj korisnički račun, odnosno da treba izbjegavati zajedničke korisničke račune.
Pri imenovanju, potrebno je pridržavati se sljedećih naputaka:

- Korisničko ime (eng. *Username*) mora biti jedinstveno. Ako je riječ o lokalnom korisničkom računu, ime mora biti jedinstveno na tom određenom računalu. Ako je pak riječ o domenskom korisničkom računu, ime tog korisničkog računa mora biti jedinstveno unutar domene.
- Ime korisničkog računa može sadržavati ukupno 20 velikih ili malih slova, osim specijalnih (npr. ; : / \ )
- Mogu se kombinirati specijalni i alfanumerički znakovi. Znak razmaka je dopušten, no ne preporučuje se za upotrebu.

Korisnički račun možete izraditi na dva načina: putem Computer Management konzole i putem linijske naredbe. Pokažimo izradu putem Computer Management konzole:

1. Pokrenite virtualno računalo **OS**. Prijavite se kao **admin**.
2. Kliknite **Start** -> Desni klik na **Computer** -> **Manage**.
3. Maksimizirajte **Computer Management** prozor radi preglednijeg rada.
4. Sa lijeve strane prozora iz kategorije **Local User and Groups** otvorite mapu **Users**.
5. Kliknite na izbornik **Action**->**New User**.
6. Popunite podatke za novog korisnika:
    a. **User name**: student01
    b. **Full name**: student
    c. **Description**: Probni račun
    d. **Password**: Pa$$w0rd
    e. **Confirm Password**: Pa$$w0rd
    f. Isključite opciju **User must change password at next logon**.
    g. Ostale opcije ostavite na predefiniranim vrijednostima i kliknite na gumb **Create**.
7. Gornjim postupkom izradite još jednog korisnika sa imenom **student02**. Ostale opcije su identične kao i kod student01 korisnika (korak 6).
8. Minimizirajte **Computer Management** konzolu.

Izradimo račun putem linijske naredbe:

1. Kliknite na **Start**->**All Programs**->**Accessories**->**Command Prompt**.
2. Upišite naredbu za kreiranje korisnika **profesor** sa lozinkom **Pa$$w0rd**:
   ```
   Net user profesor Pa$$w0rd /add /active:yes
   ```
3. Minimizirajte **Command Prompt**

U nastavku vježbe ćemo upoznati grupe korisnika.

Grupe korisnika

Korisnička grupa se sastoji od korisnika koji dijele zajednička obilježja. Grupe se koriste kako bi se olakšalo upravljanje korisnicima, njihovim ovlastima, mogućnostima, privilegijama i restrikcijama. Nakon što ovlasti dodijelite grupi, dodjeljuju se i svakom korisniku koji je član te grupe. Korisnik može biti član nekoliko grupa, a moguće je staviti grupu unutar druge grupe.
Lokalne grupe možete kreirati na računalima koja su članovi radne grupe (eng. *Workgroup*), te na računalima koja su članovi domene. Kao i kod korisničkih računa, lokalne grupe na računalima koja su članovi domene se ne mogu koristiti unutar cijele domene, već samo na računalu na kojem su kreirane.
Značajke lokalnih grupa su:

- Mogu se kreirati na svim računalima, osim na domenskom kontroleru.
- Pohranjene su u SAM bazi na svakom pojedinom računalu.
- Koriste se za dodjelu dozvola pristupa, ovlasti korištenja i privilegija samo na računalima na kojima su kreirane.

Grupe u domenskom okruženju kreirate na domenskom kontroleru te omogućavaju dodjeljivanje resursima na svim računalima koja su članovi domene.
Značajke domenskih grupa su:

- Grupe su pohranjene na domenskom kontroleru te njima (unutar Windows okruženja) upravlja servis Active Directory.
- Koriste se za dodjelu dozvola pristupa, ovlasti korištenja i privilegija na svim računalima koja su članovi domene.
- Članovi domenskih grupa mogu biti korisnički računi, računala ili druge grupe (uz određena ograničenja).

Izradimo grupu putem **Computer Management** konzole:

1. Prikažite **Computer Management** konzolu.
2. Sa lijeve strane **Computer Management** prozora iz kategorije **Local User and Groups** otvorite mapu **Groups**.
3. Kliknite na izbornik **Action**->**New Group**
4. Upišite podatke o grupi:
    a. **Group name**: Studenti
    b. **Description**: Studenti prve godine
    c. Kliknite na gumb **Add** kako bi dodali članove grupi:
        i. Kliknite na gumb **Advanced**
        ii. Kliknite na gumb **Find Now**
        iii. Sa **Search results** popisa označite korisnike **student01** i **student02** i kliknite gumb **OK**.
5. Kliknite gumb **OK** i zatim kliknite gumb **Create**.

Grupu možemo izraditi putem linijske naredbe:

1. Prikažite **Command Prompt**.
2. Upišite naredbu za kreiranje grupe profesori:
   ```
   Net localgroup profesori /add
   ```
3. Dodat ćemo račun profesor u grupu Profesori pomoću naredbe:
   ```
   Net localgroup profesori profesor /add
   ```
4. Ne zatvarajte **Command Prompt**.

Naredbe u Windows Command Promptu možemo izvršavati sekvencijalno, ako ih upišemo u datoteku s .bat ekstenzijom. Takva datoteka postaje **skriptna datoteka**. Pokažimo na primjeru s novom grupom korisnika:

1. Upišite naredbu **notepad** u **Command Promptu**.
2. Otvara se prozor **Notepada**. Njega ćemo koristiti za pisanje skripte.
3. Redom u Notepad upisujte naredbe (svaka naredba u svoj red):
   ```
   Net user asistent01 Pa$$w0rd /add /active:yes
   Net user asistent02 Pa$$w0rd /add /active:yes
   Net user asistent03 Pa$$w0rd /add /active:yes
   Net user asistent04 Pa$$w0rd /add /active:yes
   Net localgroup Asistenti-1 /add
   Net localgroup Asistenti-2 /add
   Net localgroup Asistenti-1 asistent01 asistent02 asistent03 /add
   Net localgroup Asistenti-2  asistent03 asistent04 /add
   ```
4. Kliknite na **File**->**Save As**
5. Kao lokaciju snimanja postavite korijensku mapu diska **C** (eng. *Root*)
6. Opciju **Save as type** postavite na **All Files**
7. Kao ime datoteke unesite **skripta.bat**
8. Kliknite na gumb **Save** i zatvorite **Notepad**.

Skriptu ćemo izvršiti pokretanjem bat datoteke:

1. Prikažite **Command Prompt**
2. Upišite naredbu **cd**
3. Upišite naredbu **skripta.bat**
4. Skripta se izvršava i izrađuje korisnike i grupe. Ukoliko se javi greška provjerite tipfelere u naredbama.
5. Minimizirajte **Command Prompt**.

Na razni računala moguće je definirati opcije lozinki. Primjerice, moguće je odrediti minimalni broj znakova u lozinci, forsirati kompleksne lozinke i sl. Te opcije se postavljaju putem Local Security Policy konzole:

1. Kliknite na **Start**->**All Programs**->**Accessories**->**Run**
2. Upišite **MMC** i kliknite na gumb **OK**.
3. Kliknite na izbornik **File**-> **Add/Remove Snap-In**
4. Označite **Group Policy Object Editor** i kliknite na gumb **Add**.
5. Kliknite na **Finish** i potom na **OK**
6. Proširite **Local Computer Policy**->**Computer Configuration**-> **Windows Settings**->**Security Settings**-> **Account Policy**
7. Dvostrukim klikom otvorite opciju **Minimum password lenght** i postavite ju na 7 znakova.
8. Dvostrukim klikom otvorite opciju **Maximum password age** i postavite ju na 30 dana.
9. Dvostrukim klikom otvorite opciju **Password must meet complexity requirements** i postavite ju na Enabled.
10. Primijetite da nigdje nema gumba OK, Apply i sl. Ove postavke se primjenjuju odmah po modifikaciji. U slučaju da se ipak ne primjene u Command Promptu bi upisali naredbu **gpupdate**.

Dozvole pristupa

Operacijski sustav Windows 7 je višekorisnički operacijski sustav i kao takav mora pružiti mogućnost ograničavanja pristupa datotekama i mapama. Datotečni sustavi koje Windowsi 7 podržavaju su FAT i NTFS. FAT je datotečni sustav nastao u doba jednokorisničkih operativnih sustava i nije nudio postavljanje dozvola pristupa datotekama i mapama. Za razliku od FAT-a, NTFS je nastao s višekorisničkim okružjem u vidu. Bez obzira na to što Windowsi 7 rade i na FAT datotečnom sustavu, odabirom NTFS-a korisniku su na raspolaganju brojne prednosti koje nudi ovaj datotečni sustav. Višekorisnički rad na računalu i pojam sigurnosti prvenstveno su vezani uz poslovna okruženja. Dok se u kućnim okruženjima još i može zamisliti nepostojanje sigurnosnog podsustava, u poslovnom okruženju takvi bi operacijski sustavi bili neupotrebljivi. Potencijalni problemi bili bi:

- gotovo nikakva tajnovitost podataka,
- mogućnost krađe podataka,
- mogućnost zlouporabe podataka,
- maliciozno postupanje prema korisničkim podacima drugih osoba.

Korištenjem poslovnog računala u privatne svrhe (što nikako nije dobro i strogo se ne preporučuje, ali je i realno očekivati ovakav način korištenja), NTFS sigurnost dodatno dobiva na snazi.
NTFS grupe dozvola sastoje se od 13 specifičnih NTFS dozvola koje su grupirane u šest glavnih grupa. Pomoću glavnih grupa moguće je na lak i jednostavan način dodjeljivati prava pristupa na NTFS objekte, a žele li se detaljnije i preciznije definirati prava pristupa, moraju se zasebno definirati specifična prava.
Windowsi 7 dijele NTFS dozvole u šest glavnih grupa:

- **Full Control** – pune ovlasti,
- **Modify** – modifikacija,
- **Read & Execute** – čitanje i izvršavanje,
- **List Folder Contents** – pregled sadržaja,
- **Read** – čitanje,
- **Write** – pisanje.

Ove grupe definiraju kombinaciju prava koje će korisnici imati nad NTFS objektom. U NTFS sigurnosnom sustavu moguće je da korisnici dobivaju više različitih prava zbog pripadnosti različitim grupama, nasljednih svojstava ili neuredne administracije. Zbog toga NTFS mora biti sposoban riješiti konačno pravo u slučaju više istovremenih dozvola. Za ove situacije postoje sljedeća pravila:

1. Deny opcija je uvijek jača od bilo koje Allow opcije. Ukoliko je korisnik član više grupa a u jedna grupa ima postavljen eksplicitni Deny, korisnik neće moći pristupiti mapi ili datoteci.
2. Dozvole dodijeljene izravno objektu jače su od naslijeđenih dozvola.

3. Dozvole naslijeđene od bliskijih mapa jače su od dozvola naslijeđenih od daljih mapa. Drugim riječima, dozvola naslijeđena od roditeljske mape jača je od dozvole naslijeđene od mape "djeda".
4. Dozvole dobivene od različitih grupa s iste razine su kumulativne.

Promotrimo na primjeru neke od gornjih pravila.

Korištenje NTFS dozvola

NTFS dozvole postavljamo direktno na objektu (mapa ili datoteka):

1. Otvorite u **Windows Exploreru** korijensku mapu diska C i napravite mapu **Dozvole**
2. Desnim gumbom miša kliknite na mapu **Dozvole** i odaberite opciju **Properties**
3. Kliknite na karticu **Security**
4. Kliknite gumb **Edit** i zatim gumb **Add**
5. U polje **Enter the object names to select** upišite **Asistenti-1; Asistenti-2** i kliknite gumb **OK**.
6. Označite grupu **Asistenti-1** dodijelite joj **Modify** dozvolu u stupcu **Allow**. Kliknite gumb **Apply**.
7. Označite grupu **Asistenti-2** dodijelite (tj. zabranite) joj **Full Control** dozvolu u stupcu **Deny**. Kliknite gumb **Apply**
8. Prikazuje se upozorenje o opasnostima eksplicitne zabrane. Kliknite gumb **Yes**.
9. Kliknite gumb **OK** pa zatim opet **OK**.
10. Na virtualno računalo se prijavite kao korisnik **Asistent03**
11. Pokušajte otvoriti mapu **Dozvole**.

Korištenje Share dozvola

Share (djeljene) dozvole postavljamo su dodatne dozvole koje definiramo za korisnike koji pristupaju putem mreže na dijeljene mape. Da bi korisnik mogao pristupiti mora uz NTFS dozvole imati i postavljena prava na pristup putem mreže.

1. Otvorite u **Windows Exploreru** korijensku mapu diska C
2. Desnim gumbom miša kliknite na mapu **Dozvole** i odaberite opciju **Properties**
3. Kliknite na karticu **Share**
4. Kliknite gumb **Advanced Sharing** i zatim dodajte kvačicu na **Share this folder**
5. U polje **Share name** možete upisati svoj naziv djeljene mape ili ostaviti predefinirani. (Taj naziv će korisnici vidjeti kada se spajaju na tu djeljenu mapu)
6. Kliknite na **Permissions**.
7. U novo otvorenom prozoru vidimo da je operacijski sustav u pristupnu listu (ACL) samostalno dodao jedan zapis u kojem grupi **Everyone** da je prava **Read**.
8. Ako ovo ostavimo ovako i preko mreže pristupimo mapi kao korisnik **Asistent01** nećemo moći mijenjati dokumente iako imamo NTFS prava da to napravimo.

Zadatak

Pronađite način kako možete s vašeg računala provjeriti tvrdnju iz točke 8.
Napravite neku testnu datoteku u **notepadu** i pospremite je u tu mapu.
Odjavite se sa sustava i prijaviti kao **Asistent01** te preko mreže pristupiti mapi.
Probajte napraviti promjenu na datoteci.
Korisnik **Asistent01** s članstvom u grupi **Asistenti-1** ima NTFS pravo **Modify**
Zašto ne može promijeniti datoteku?
Da li može promijeniti datoteku ako pristupi direktno na disku u mapu bez da koristi mrežni pristup?

Što treba znati nakon ove vježbe?

1. Objasniti razliku između lokalnih i domenskih korisničkih računa
2. Opisati NTFS dozvole
3. Objasniti pravila razrješavanja višestrukih NTFS dozvola
4. Objasniti opasnost eksplicitne zabrane
5. Objasniti određivanje efektivnih dozvola pristupa (kombinacija NTFS i Share).