Praktikum 4

FAILISÜSTEEMIDE JUURDEPÄÄSUÕIGUSED

NTFS failisüsteemi juurdepääsuõigused

Põhimõtted:

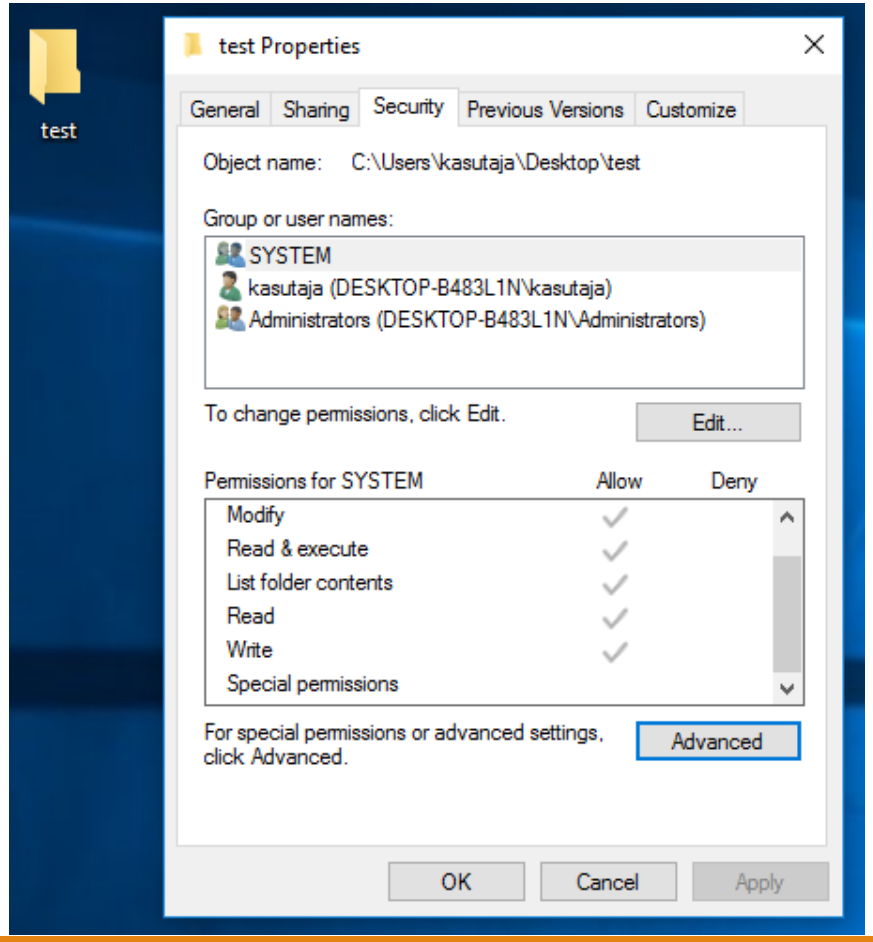
- Juurdepääsuõigused on **kasutajakonto ja/või kasutajagrupi põhised**.
- Iga failisüsteemi objekt omab **juurdepääsuõiguste nimekirja** ja/või pärib selle ülemobjektilt.
- Igal failisüsteemi objektil on **omanik**, kellel on alati õigus juurdepääsuõiguseid muuta.
- Vaikimisi on juurdepääsuõigused **hierarhiliselt päritavad**.
- Juurdepääsuõigused on **kumulatiivsed**.
- Juurdepääsuõiguste nimekirja kirje võib olla **lubav (allow)** või **keelav (deny):**
  - Objektile **määratud deny** on tähtsam kui:
    - Objektile **määratud allow** on tähtsam kui:
      - Ülemobjektilt **päritud deny** on tähtsam kui:
        - Ülemobjektilt **päritud allow**.

NTFS juurdepääsuõiguste grupid

NTFS õigus	***Kirjeldus***
Read	Kasutaja või grupp saab vaadata faili sisu, näha selle omanikku, atribuute ja õigusi
Write	Kasutaja või grupp võib muuta faili sisu ja atribuute. Lisaks veel näha selle omanikku ja õigusi.
Read&Execute	Sama, mis Read aga lisaks tohib kasutaja või grupp programmifaili käivitada
Modify	Kasutaja või grupp tohib faili muuta ja kustutada ning lisaks on neil kõik õigused, mille annavad Read, Write ja Read&Execute
Full Controll	Kõik ülaltoodud õigused ja lisaks veel õigus muuta faili õigusi ja faili omanikku.

Kataloogi puhul on lisaks neile õigustele veel ka List Folder Contents – see lubab kasutajal või grupil näha kataloogis olevaid faile ja alamkataloge.

NTFS juurdepääsuõiguste vaatamine



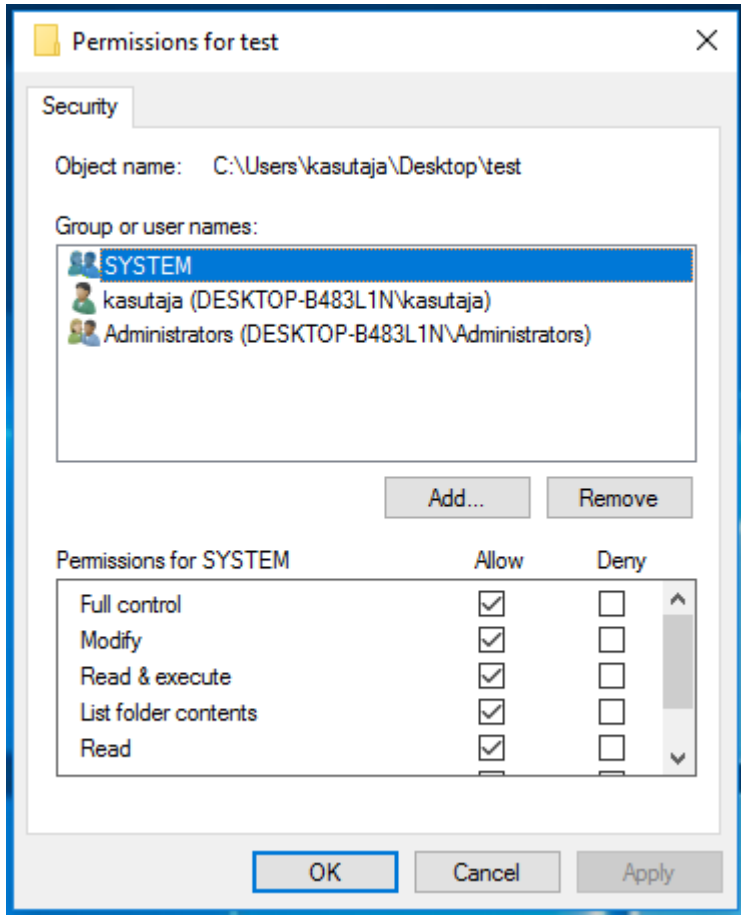
Üldine info: Properties – Security

Täpsem info: Properties – Security – Advanced

Käsurealt: icacls [objekti nimi]

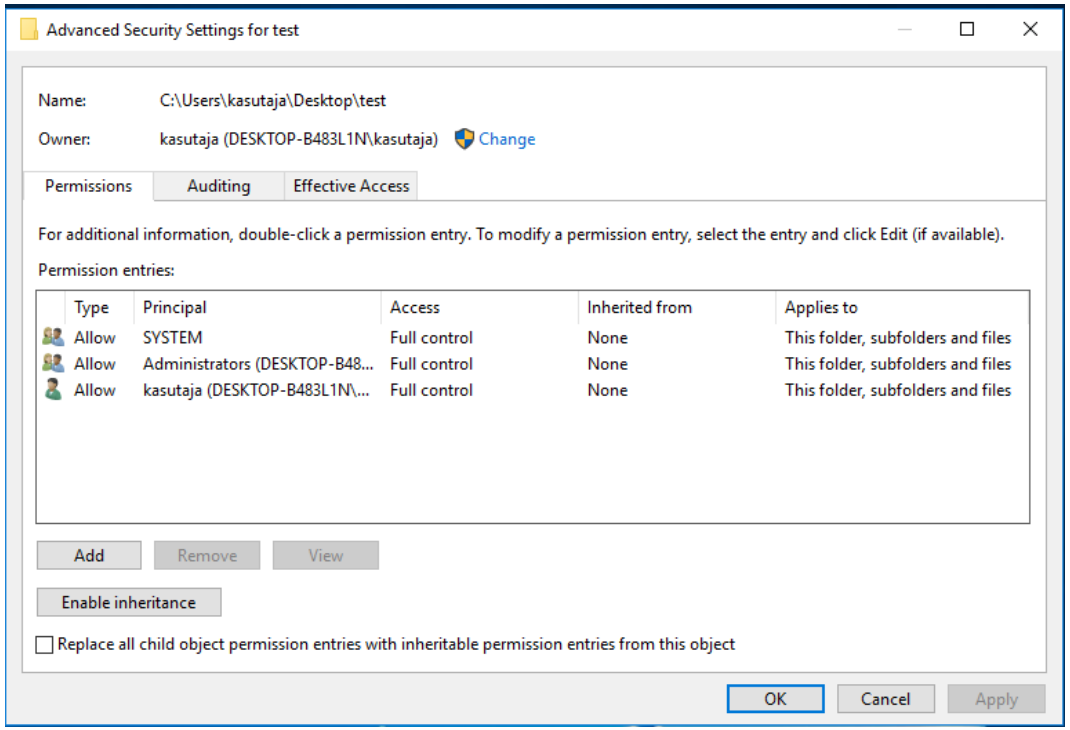
Näiteks: icacls c:\users\kasutaja\Desktop\test

NTFS juurdepääsuõiguste muutmine



Üldine muudatus: Properties – Security - Edit

Täpsem muudatus: Properties – Security – Advanced



Harjutus

1. Looge 2 uut kasutajagruppi nimedega „grupp1“ ja „grupp2“
2. Looge 3 uut kasutajat nimedega „kasutaja1“, „kasutaja2“, „kasutaja3“
3. Tee nii, et kasutaja „kasutaja2“ oleks administraatori õigustega; „kasutaja1“ kuuluks gruppidesse „grupp1“ ja „grupp2“ ning „kasutaja3“ kuuluks gruppi „grupp1“
4. Tehke C: kettale kataloog „peremees“ ja selle sisse alamkataloogid „sulane1“ ja „sulane2“
5. tekitage igasse kataloogi tühjad tekstifailid „tekst1.txt“ ja „tekst2.txt“ (kokku 6 faili)
6. tehke nii, et „kasutaja1“ omaks kõiki õigusi kataloogis „sulane2“ olevatele failidele
7. tehke nii, et „grupp1“ omaks kirjutamisõigust kataloogidele „sulane1“ ja „sulane2“
8. tehke nii, et „kasutaja1“ ei omaks kindlasti kirjutamisõigust alamkataloogis „sulane1“ failile tekst1.txt
9. tehke nii, et „grupp2“ omaks lugemis ja käivitamisõigusi kataloogile „peremees“
10. tehke nii, et alamkataloogis „sulane1“ olevad failid ei päriks kataloogi „peremees“ õigusi.

UNIXi klassikalised juurdepääsuõigused (1)

Põhimõtted:

- Eraldi juurdepääsuõigused määratakse kolmele klassile: **kasutaja (user)**, **grupp (group)** ja **teised (others)**
- Igal failisüsteemi objektil on omanik. Objekti omanik kuulub klassi **kasutaja (user)**.
- Igal failisüsteemi objektil on grupp. Gruppi võivad kuuluda mitmed kasutajakontod sh. omanik.
- Kasutajakonto, kes pole omanik ega kuulu gruppi, kuulub klassi **teised (others)**
- Kehtivaid kasutajaõiguseid kontrollitakse järjekorras: **omanik – grupp – teised**
- Juurdepääsuõigusi saab muuta ainult **root** kasutaja ja **objekti omanik**

UNIXi klassikalised juurdepääsuõigused (2)

Juurdepääsuõigused:

Read – õigus lugeda faili sisu. Kataloogi puhul õigus lugeda kataloogis olevate objektide nimesid (aga mitte teisi metaandmeid).

Write – õigus faili sisu muuta. Kataloogi puhul õigus muuta kataloogi objektide sisu (kustutada, muuta, nimetada ümber).

Execute – õigus faili käivitada (kui on käivitatav fail või skript). Kataloogi puhul õigus näha kataloogid olevate objektide metaandmeid ja sisu (eeldusel, et objektide nimi on teada). Samas kataloogi sisu nimekrirja näidatakse ainult siis, kui on olemas ka read õigus.

UNIXi juurdepääsuõigusi modifitseerivad atribuudid

setuid (set user ID) – kui failile on määratud setuid bit, siis faili käivitamisel tekib uus protsess faili omaniku õigustes (mitte selle kasutaja õigustes, kes faili käivitas.)

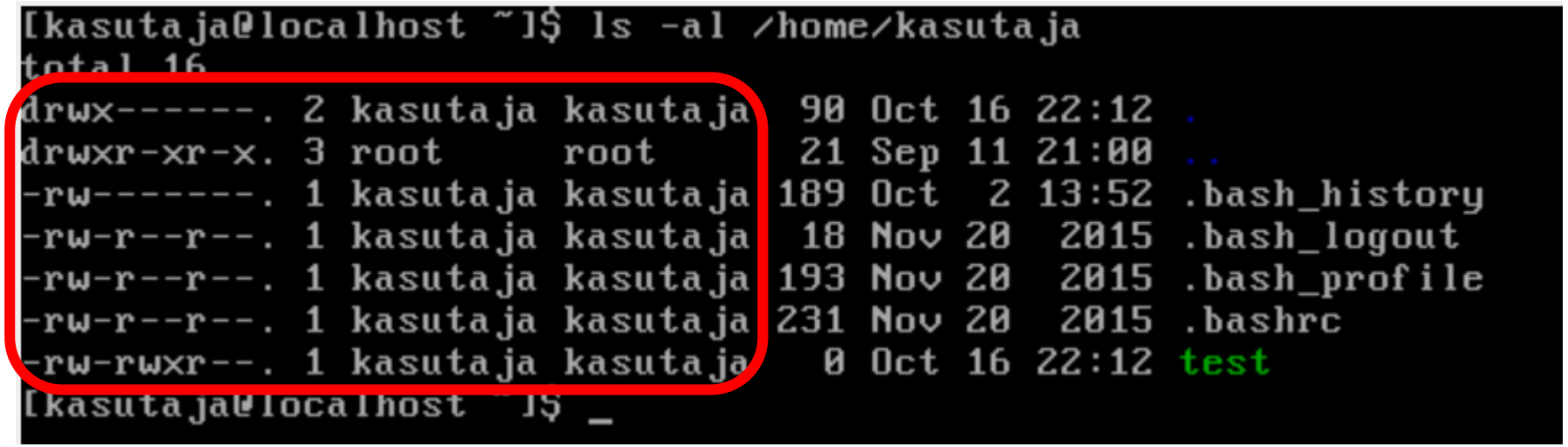
setgid (set group ID) – kui failile on määratud setgid bit, siis faili käivitamisel tekib uus protsess faili grupi õigustes. Kui kataloogile on määratud setgid bit, siis sellesse kataloogi loodavad uued failid ja kataloogid pärivad peakataloogi grupi (ilma setgid bit-ita määratakse grupiks aktiivse kasutaja esimene grupp).

sticky bit – kui kataloogile on määratud sticky bit, siis kasutajad ei saa kustutada ega ümbernimetada alamkatalooge ja faile, mis ei kuulu neile (isegi siis kui neil on peakataloogile kirjutamisõigus). Sticky bit ei kehti root kasutajale ja selle kataloogi, millele on sticky bit määratud, omanikule.

UNIXi juurdepääsuõiguste vaatamine

ls –al [objekt]

Näiteks: ls –al /home/kasutaja



Sümbolite tähendus

Tähised:

- õigus puudub

r lugemisõigus

w kirjutamisõigus

x käivitamisõigus

s setuid/setgid JA käivitamisõigus

S setuid/setgid ilma käivitamisõiguseta

t sticky JA käivitamisõigus

T sticky ilma käivitamisõiguseta

Tähiste grupid:

Gruppeerimine: 1-3-3-3-1 sümbolit

1 grupp - objekti tüüp

2 grupp - omaniku õigused

3 grupp – grupi õigused

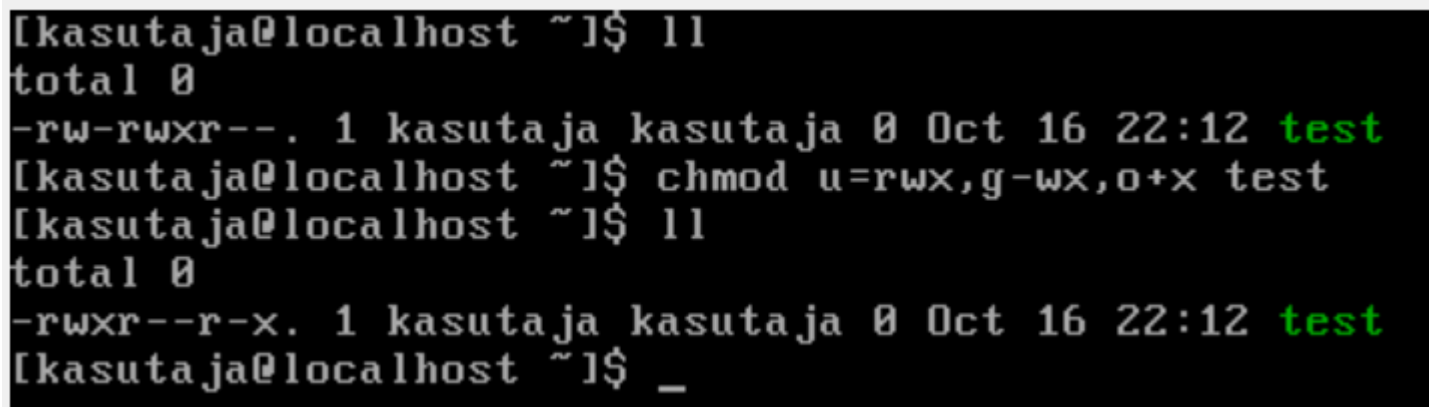
4 grupp – teiste õigused

5 grupp – lisainfo

Õiguste muutmine

Käsk: chmod

Kasutamine vaata: https://en.wikipedia.org/wiki/Chmod



Harjutus

1. Loo kaks uut kasutajat “kasutaja1” ja “kasutaja2”
2. Loo kaks uut gruppi nimega “grupp1” ja “grupp2”
3. Tee nii, et kasutaja „kasutaja1“ kuuluks gruppi “grupp1”
4. Tee nii, et kasutaja ”kasutaja2” primaarne grupp oleks ”grupp2”
5. Tekita kataloog “/test1” ja sinna sisse fail “proov.txt”
6. Määra kataloogi “/test1” ja faili “proov.txt” omanikuks “kasutaja1” ja grupiks “grupp2”
7. Tee nii, et kasutaja 2 saaks faili ”proov.txt” sisu muuta, kuid faili ennast mitte kustutada.
8. Tee nii, et kõik teised ei omaks failile “proov.txt” mitte mingeid õigusi.

Iseseisev ülesanne nr. 2

NTFS failisüsteemis on vaja salvestada projektiga seotud andmeid.

Projektiga töötab 7 töötajat (kasutajad: worker1 – worker7).

Projekti käigus tekib 3 tüüpi dokumente: avalikud, privaatsed ja täiesti salajased.

• Töötajad 1 ja 2 peavad saama vaadata, luua ja muuta kõiki dokumente.

• Töötajad 3 ja 4 peavad saama vaadata, luua ja muuta avalikke ja privaatseid dokumente.

• Töötajad 5 ja 6 peavad saama vaadata, luua ja muuta avalikke dokumente ja vaadata täiesti salajasi dokumente.

• Töötaja 7 peab saama vaadata kõiki dokumente.

• Avalikud dokumendid peavad olema loetavad kõigile.

• Lihtsuse huvides võivad kõik kataloogid kuuluda ühele administraatorõigustes kasutajale

Milline on ülesande lahendamiseks vajalik kataloogistruktuur?

Millised on ülesande lahendamiseks vajalikud kasutajagrupid?

Millised on kasutajate grupikuuluvused ning millised on gruppidele määratud õigused iga kataloogi juures?

Põhjenda oma valikuid.