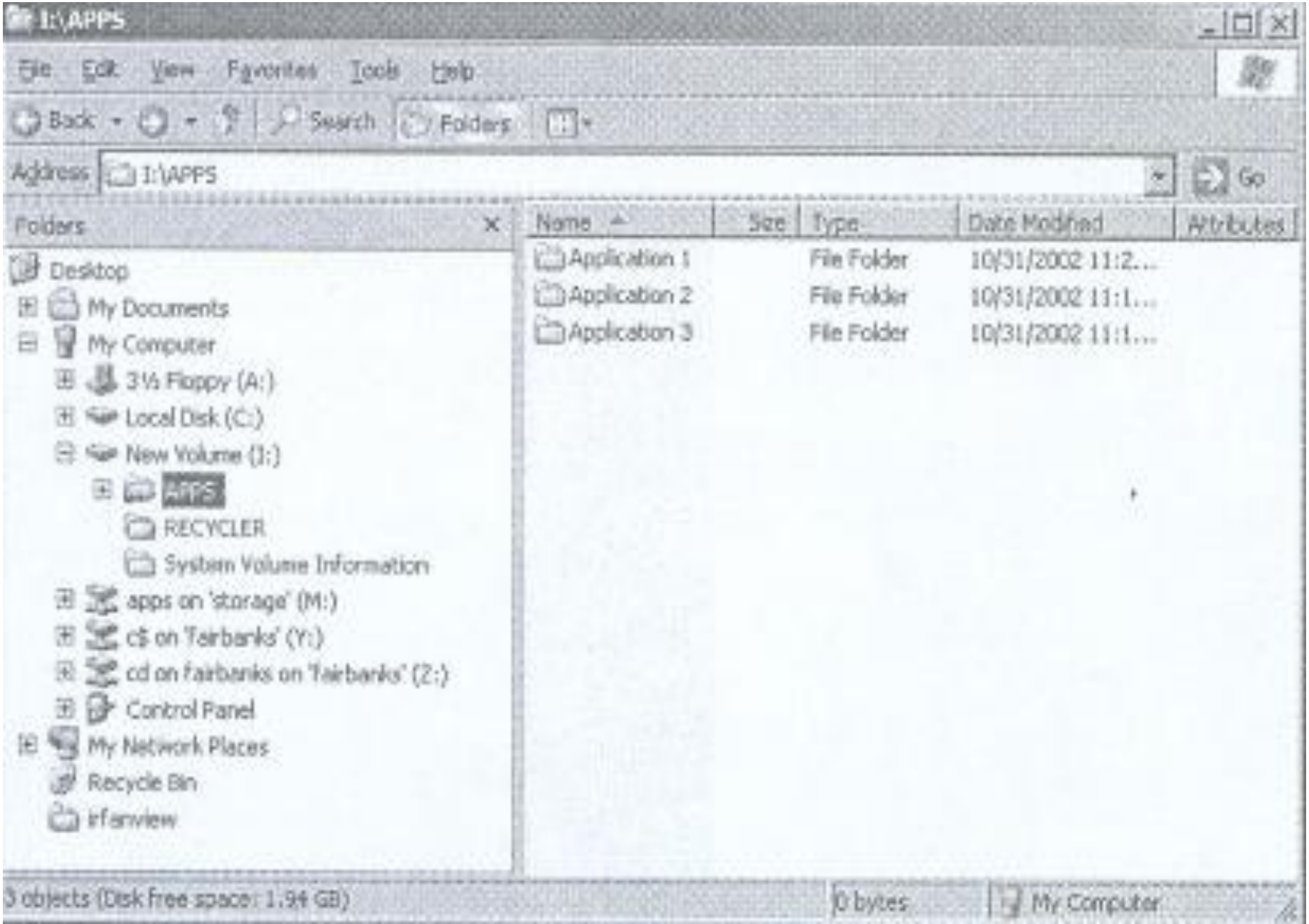
IX- Deljenje i bezbednost datoteka

S A D R Ž A J

9.1 Deljenje datoteka

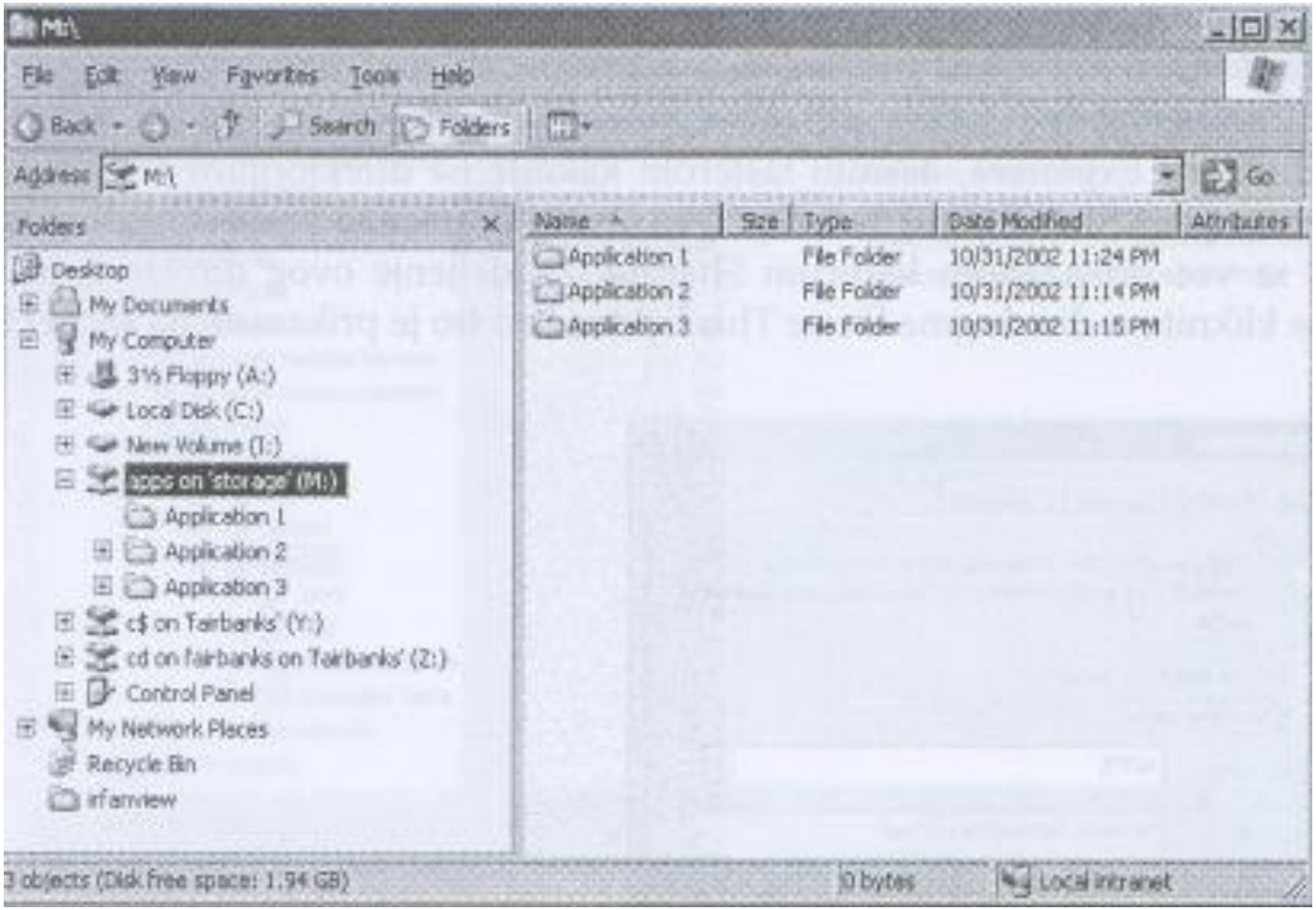
- Serverski OS u celoj Windows familiji, kontroliše mogućnost servera da deli fajlove i resurse za štampanje.
- Sama činjenica da imate podignut server ne znači da imate bilo šta raspoloživo za vaše korisnike.
- Microsoft je još u svom starom mrežnom OS, Windows 2000 Server, ubacio mnoge nove servise, karakteristike i funkcije čija je osnovna namena bila da se obezbedi dobar fajl server.
- Windows Server OS je preuzeo solidne mogućnosti za deljenje fajlova od Win.NT, proširio ih sa distribuiranim fajl sistemom (***D****istributed* ***F****ile* ***S****ystem*) i uveo dozvole i deljenje koje se lakše kontroliše
- Osnovna namena bilo kog mrežnog servera jeste da omogući nesmetano korišćenje resursa na mreži koju kontroliše.
- Da bi bilo ko od njih dobio pristup resursima servera, resurse morate da učinite deljivim (*shared*) tj. vidljivim za korisnike sa mreže.
- Kao primer poslužiće direktorijum na lokalnom drajvu I, pod nazivom APPS, sa 3 aplikacije u poddirektorijumima, kao na slici

9.1 Deljenje datoteka



9.1 Deljenje datoteka

- Kada direktorijum delimo preko mreže klijenti na svojim računarima mogu da mapiraju direktorijum **I:\APPS** sa novom oznakom drajva.



- Ako za deljenje direktorijuma **APPS** sa servera na klijentu koristite oznaku M: taj drajv M: identičan je direktorijumu na serveru **I:\APPS**

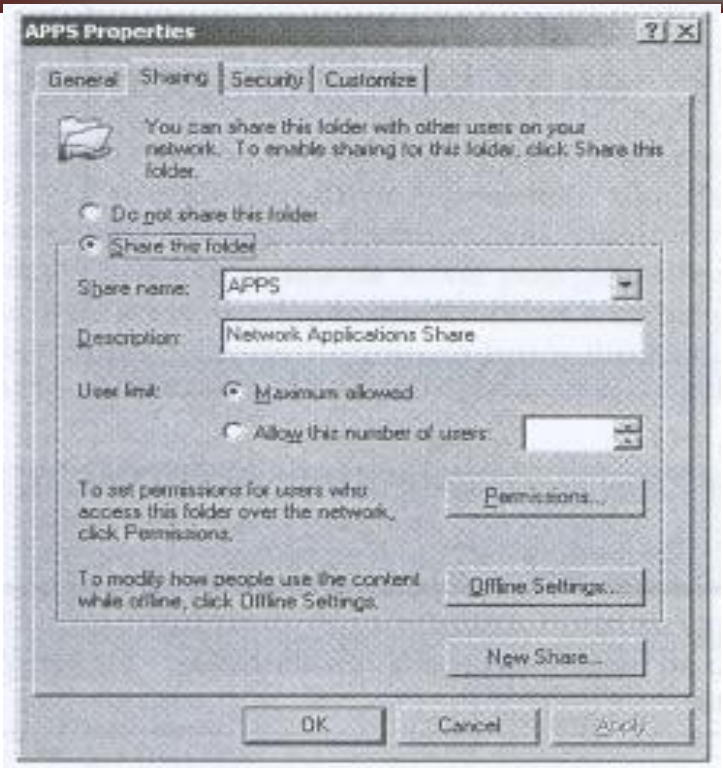
9.1 Deljenje datoteka

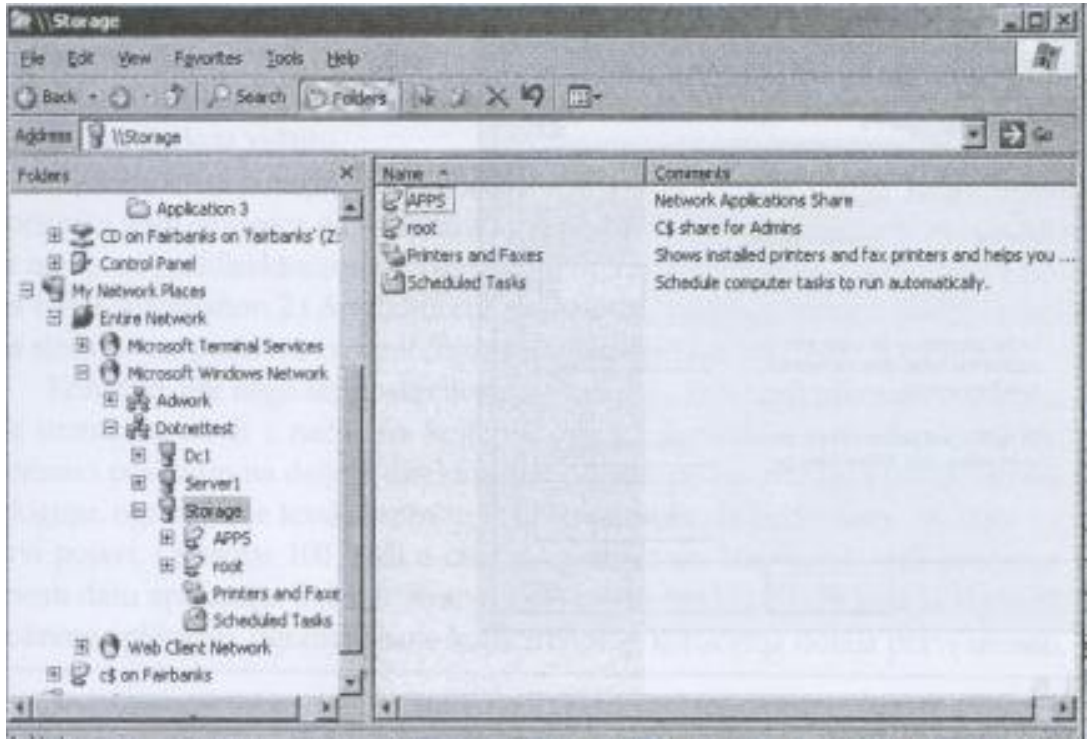
- Da biste mogli da kreirate deljeni direktorijum, morate da imate odgovarajuća prava a to znači da ste ili administrator ili Power User.
- Deljene direktorijume možete da kreirate na nekoliko načina: preko Explorera, upravljačkom konzolom ili korišćenjem **Server Manager-a**

Kreiranje deljenih direktorijuma iz Explorera

- Ako sedite za serverom, Explorer omogućava jednostavno i direktno kreiranje i kontrolu svih svojstava deljenih direktorijuma.
- Potrebno je da desnim tasterom označimo željeni direktorijum (APPS) koji želimo da delimo i iz menija biramo opciju ***Sharing and Security***
- Ovo otvara novu stranicu sa svojstvima direktorijuma APPS, sa već prikazanom karticom ***Sharing***.
- Za deljenje ovog direktorijuma preko mreže kliknite radio dugme ***Share This Folder***.
- Opcija ***Share Name*** predstavlja najznačajniji podatak na ovoj stranici jer će ime koje ovde date biti vidljivo svim korisnicima mreže
- Polje ***Description*** omogućava unos detaljnijih opisnih informacija o ovom direktorijumu i ono nema neki značaj na serveru ili klijentu.

9.1 Deljenje datoteka





- ***User Limit*** konfigurišete broj korisnika koji istovremeno mogu da koriste deljeni direktorijum – važi za kompletan direktorijum
- Kada direktorijum učinite deljivim, ponovo možete da posetite stranicu sa svojstvima, desnim klikom i biranjem opcije ***Sharing and Security***.
- Iako izgleda kao i prethodna stranica sa svojstvima, imamo još jednu opciju, ***New Share***, koja može da dodeli direktorijumu drugo ime
- Izborom ***Permissions*** definišemo različite dozvole za deljenje

9.2 Upravljanje dozvolama

- Potrebno je zaštititi deljene resurse od neovlašćenog pristupa
- Postoje razni načini, pomoću rutera ili *firewala*, ali znatno veće mogućnosti imamo ako se koristimo dozvolama za rad sa resursima
- Postoje ***dozvole za rad sa deljenim direktorijumima*** i ***dozvole za rad sa fajlovima i direktorijumima*** (**NTFS dozvole**).
- Pomoću ovih dozvola možemo da kontrolišemo ko ima pristup našim podacima i šta može da radi sa njima.

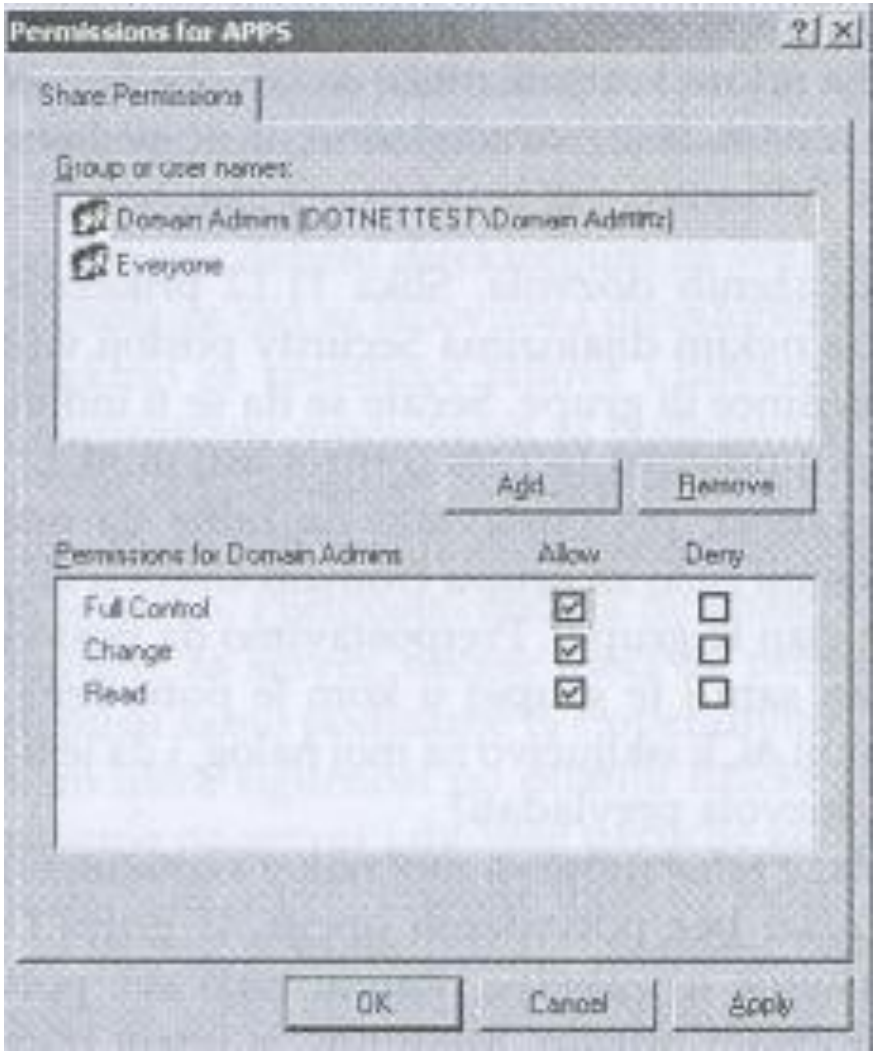
1. Dozvole za rad sa deljenim direktorijumima

- Dozvole za rad sa deljenim direktorijumima predstavljaju jednostavan oblik kontrole pristupa kada radite sa Windows Serverom OS.
- Ove dozvole imaju efekat samo kada računaru pristupamo preko mreže
- Definisanjem dozvola za deljene direktorijume možemo da definišemo nivo pristupa za sve korisnike još na samom ulazu u fajl sistem
- Nivo dozvole predstavlja samo *maksimalni* nivo pristupa koji dobijate kada dospete u unutrašnjost a to znači da dalja ograničenja unutar direktorijuma možete da postignete dozvolama na nivou fajla (NTFS) kojima dobijamo punu kontrolu nad direktorijumom

9.2 Upravljanje dozvolama

- Prikazano je polje ***Group or User Names*** koje navodi listu korisnika i grupa dodeljenih deljenom direktorijumu
- Kada se selektuje korisnik ili grupa, prikazuju se i njima dodeljene dozvole.
- Možemo postaviti sledeće dozvole:

1. ***Full Control*** - grupa može da izvršava sve funkcije nad svim fajlovima i direktorijumima u okviru deljenog direktorijuma.
2. ***Change*** - Dodeljena grupa može da čita i izvršava, kao i da menja i briše fajlove i direktorijume u okviru deljenog direktorijuma.
3. ***Read*** - Dodeljena grupa može da čita i izvršava fajlove i direktorijume, ali ne može da menja ili briše bilo šta što se nalazi u okviru direktorijuma



9.2 Upravljanje dozvolama

Razumevanje opcija *Allow* i *Deny*

- ✓ Administrator može da odobri ili zabrani pristup za bilo koga, ili može da izbriše obe opcije, i ***Allow*** i ***Deny***, ostavljajući korisnika i bez dopuštenja i bez zabrane konkretne dozvole.
- ✓ Ako korisnik nema dozvolu, ni odobrenje ni zabranu, onda uopšte nema nikakav pristup objektu.
- ✓ Ako je kod dozvole potvrđena opcija ***Allow***, korisnik može da isproba dozvolu; ako je potvrđena opcija ***Deny***, ne može.
- ➢ Objekti mogu da imaju više pridruženih dozvola za iste direktorijume.
- ➢ OS traži sve ACL ulaze za nalog i izračunava ih na sledeći način:

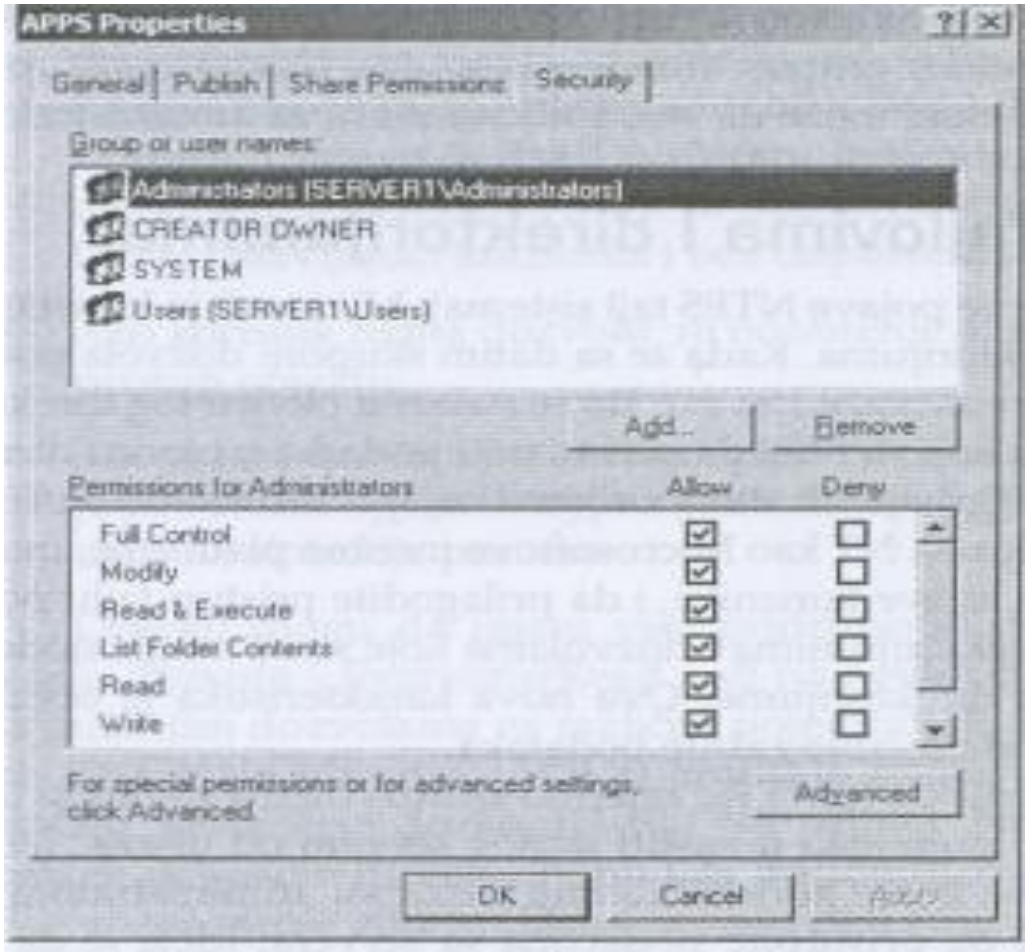
1. najpre se ignorišu svi ulazi bez potvrđenih opcija
2. traži sve potvrđene opcije ***Allow*** i ako ih nema, nema pristupa resursu
3. traže se sve potvrđene opcije ***Deny*** i ako se pronađe makar jedna, pristup resursu je zabranjen.

Pristup resursu se dobija samo ako ima barem jedna potvrđena opciju Allow, bez potvrđenih opcija Deny.

Ako je potvrđena bar jedna opcija Deny pristup resursu je zabranjen

9.3 NTFS dozvole za rad sa fajlovima

- Ako imamo 1000 korisnika koji su hteli da privatizuju podatke u okviru direktorijuma,moramo da kreiramo 1000 deljenih direktorijuma
- NTFS dozvole - dozvole koje su se mogle dodeljivati direktno za specifične fajlove i direktorijume što obezbeđuje neograničene mogućnosti.



9.3 NTFS dozvole za rad sa fajlovima

- Dozvole koje vidite na slici formirane su od dozvola nižeg nivoa.
- Na primer, dozvola višeg nivoa ***List Folder Contents*** sadrži pet dozvola nižeg nivoa:
    1. *Traverse Folder/Execute File*,
    2. *List Folder/Read Data*,
    3. *Read Attributes*,
    4. *Read Extended Attributes*
    5. *Read Permissions*.
- Sve dozvole možemo podeliti na "**molekularne**" i "**atomske**" dozvole.
- NTFS ima 13 atomskih dozvola.
- Ostale vrste objekata mogu da imaju manji ili veći broj atomskih dozvola; na primer, bilo koji objekat AD (korisnički nalog, nalog mašine, OJ, objekat grupne polise i td.) ima više od 35 atomskih dozvola.
- Svi AD objekti dele isti skup atomskih dozvola.
- Na sledećoj slici pokazano je kako se grupisanjem atomskih dozvola kreiraju molekularne dozvole.

9.3 NTFS dozvole za rad sa fajlovima

Atomske dozvole	*Write*	*Read*	*List Folder Contents*	*Read and Execute*	*Modify*	*Full Control*
Traverse Folder/Execute File			x	x	x	x
List Folder/Read Data		x	x	x	x	x
Read Attributes		x	x	x	x	x
Read Extended Attributes		x	x	x	x	x
Create Files/Write Data	x				x	x
Create Folders/Append Data	x				x	x
Write Attributes	x				x	x
Write Extended Attributes	x				x	x
Delete Subfolders and Files						x
Delete					x	x
Read Permissions	x	x	x	x	x	x
Change Permissions						x
Take Ownership						x

9.4 Atomske dozvole

Traverse Folder/Execute File - omogućuje preskakanje nekoliko nivoa zaštite da bi došli do ciljnog direktorijuma gde dozvole stvarno važe a Execute File izvršavanje fajla.

List Folder/Read Data - Dozvola *List Folder* omogućava prikazivanje naziva *fajlova* i *direktorijuma* u okviru datog direktorijuma a dozvola *Read Data* omogućava prikazivanje sadržaja fajla.

Read Attributes – omogućava prikaz osnovnih atributa fajla kao što su *Read-Only, Hidden, System i Archive*.

Read Extended Attributes - određeni programi za svoje tipova fajlova uključuju neke druge atribute koji se razlikuju od programa do programa

Write Attributes - omogućava izmenu osnovnih atributa fajla.

Write Extended Attributes - omogućava izmenu dodatnih atributa fajla.

Create Files/Write Data - *Create Files* omogućava postavljanje novih fajlova u okviru direktorijuma a *Write Data* omogućava prepisivanje postojećih podataka u okviru fajla.

9.4 Atomske dozvole

Create Folders/Append Data - *Create Folders* omogućava kreiranje direktorijuma u okviru postojećeg direktorijuma a *Append Data* omogućava dodavanje podataka na kraj postojećeg fajla.

Delete Subfolders and Files - brisanje poddirektorijuma i fajlova

Delete - omogućava brisanje objekta.

Read Permissions - omogućava prikazivanje svih NTFS dozvola dodeljenih fajlu ili direktorijumu, ali bez mogućnosti za promenu

Change Permissions - Ova atomska dozvola omogućava promenu dozvola koje su dodeljene fajlu ili direktorijumu.

Take Ownership - Ova atomska dozvola omogućava preuzimanje vlasništva nad fajlom. Kada postanete vlasnik, nasleđujete prava za promenu dozvola za rad sa fajlom. Podrazumeva se da administratori uvek mogu da preuzmu vlasništvo nad fajlom ili direktorijumom.

9.5 Molekularne dozvole

Read - omogućava prikazivanje sadržaja, dozvola i atributa dodeljenih objektu. Ako je reč o fajlu, možete da prikažete fajl, a ako je reč o direktorijumu, dozvola omogućava prikazivanje sadržaja direktorijuma.

Write – dozvola za direktorijum omogućava kreiranje novog poddirektorijuma u okviru datog direktorijuma a za promenu fajla, pored dozvole Write morate imati i dozvolu *Read*.

Read and Exccute Dozvola *Read and Execute* je identična dozvoli Read, ali dodaje atomsku privilegiju prolaska do direktorijuma.

Modify - kombinacija dozvola Read and Execute i Write.

Full Control - predstavlja kombinaciju prethodno pominjanih dozvola, sa mogućnošću da menjate dozvole i preuzimate vlasništvo

List Folder Contents - slična prava kao i dozvola Read and Execute, ali važi samo u slučaju direktorijuma.

Special Permissions - je jednostavno prilagođena grupa atomskih prava koju kreirate kada neka od standardnih atomskih dozvola nije prikladna za datu situaciju.

9.6 Obezbeđivanje fajl sistema

- Windows Server OS sve svoje podatke smešta u fajl sistem, tj. svi korisnički podaci, aplikacije i fajlovi OS nalaze se u fajl sistemu.
- Da bi fajl sistem bio bezbedan, ovi fajlovi se moraju obezbediti.
- Spoljašnje pretnje mreži, slučajno brisanje fajl sistema ili pristup neke od neovlašćenih internih grupa mogu rezultirati gubitkom podataka

Blokiranje fajl sistema preko NTFS-a - NTFS je predstavljao veliku prekretnicu u odnosu na FAT fajl sistem, u mnogim oblastima. Podržavanje većih diskova, podržavanje nestandardnih veličina bloka za dodeljivanje memorije i mogućnost definisanja bezbednosti na nivou fajla ili direktorijuma - sve su to velike prednosti NTFS-a.

Blokiranje grupnog članstva - Jedan od najbitnijih načina za bezbednost mreže je da se korisnicima ne garantuje članstvo u grupama koje bi im obezbedile više prava nego što im je zaista neophodno.

Držanje korisnika dalje od sistemskih fajlova - Korumpiranje ili brisanje sistemskih fajlova vrlo brzo može da onesposobi server. Ako ne računamo bezbednosne zakrpe, ne postoji nijedan drugi razlog da administrator ima pravo upisivanja za sistemske fajlove.

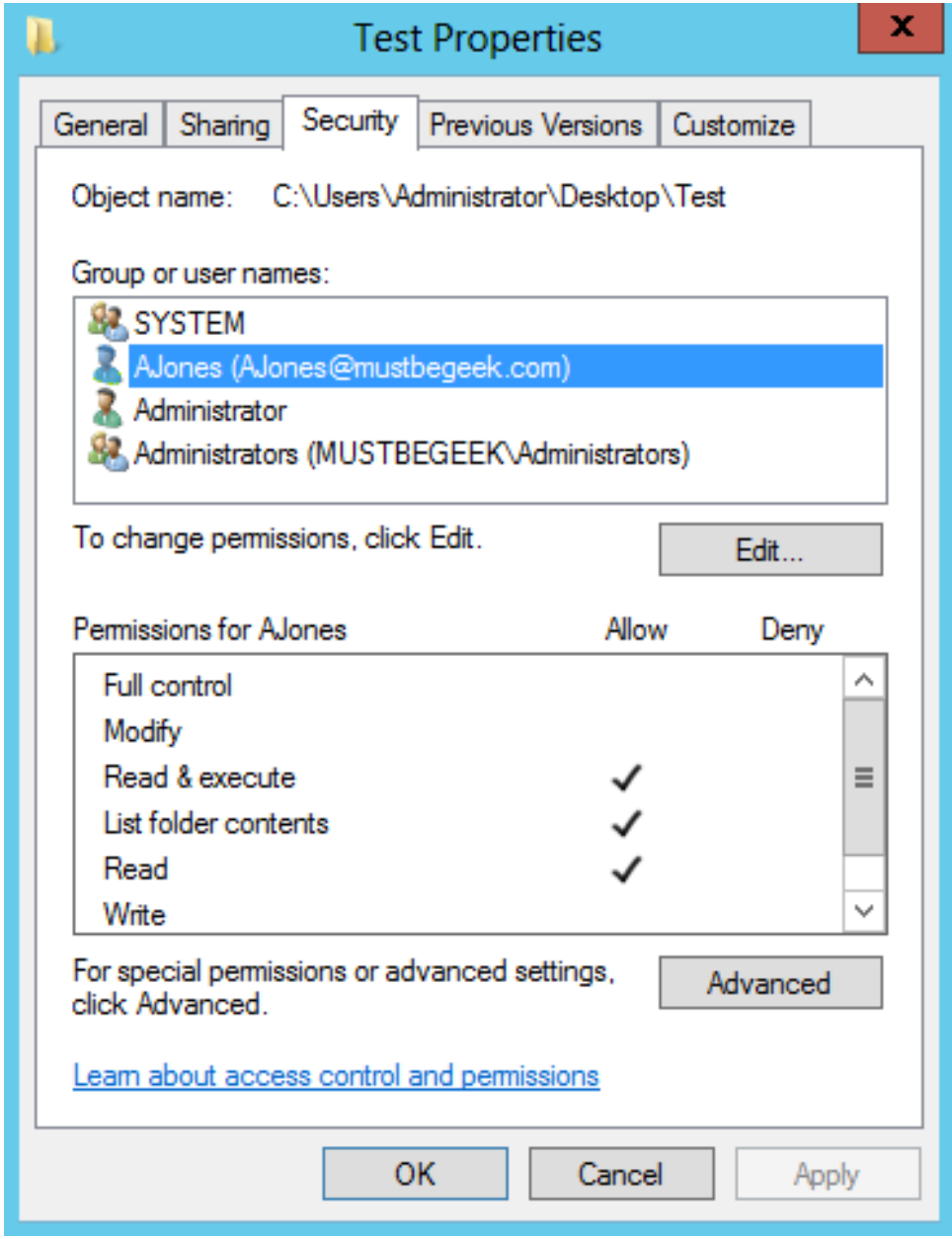
9.6 Obezbeđivanje fajl sistema

Održavanje tajnosti fajlova pomoću EFS-a - *Encrypting File System* na NTFS volumenima omogućava korisniku da šifruje fajl tako da samo on može da mu pristupi. Kada počne da koristi EFS za šifrovanje fajla, korisniku se dodeljuje par ključeva (javni i privatni ključ). Ključevi se generišu pomoću servisa sertifikata ili ih EFS samostalno potpisuje, u zavisnosti od toga da li je CA prisutan.

Samostalna upotreba EFS-a - Windows Server ima sposobnost da generiše sopstveni par ključeva za EFS ukoliko nemaju na raspolaganju sertifikat na nivou domena. EFS na mašini koja ne pripada domenu se dosta razlikuje od onog na mašini koja je član domena. Ako korisnik šifruje fajl i izgubi oba spremišta sertifikata, korisničkog i lokalnog DRA-a, neće moći da dešifruje fajl. Slično tome, usled nedostatka centralne baze podataka ključeva za korisnike EFS-a na računaru koji ne pripada domenu, korisnik može namerno da izbriše DRA sertifikat i spremište sertifikata, pa će takvi fajlovi biti neupotrebljivi.

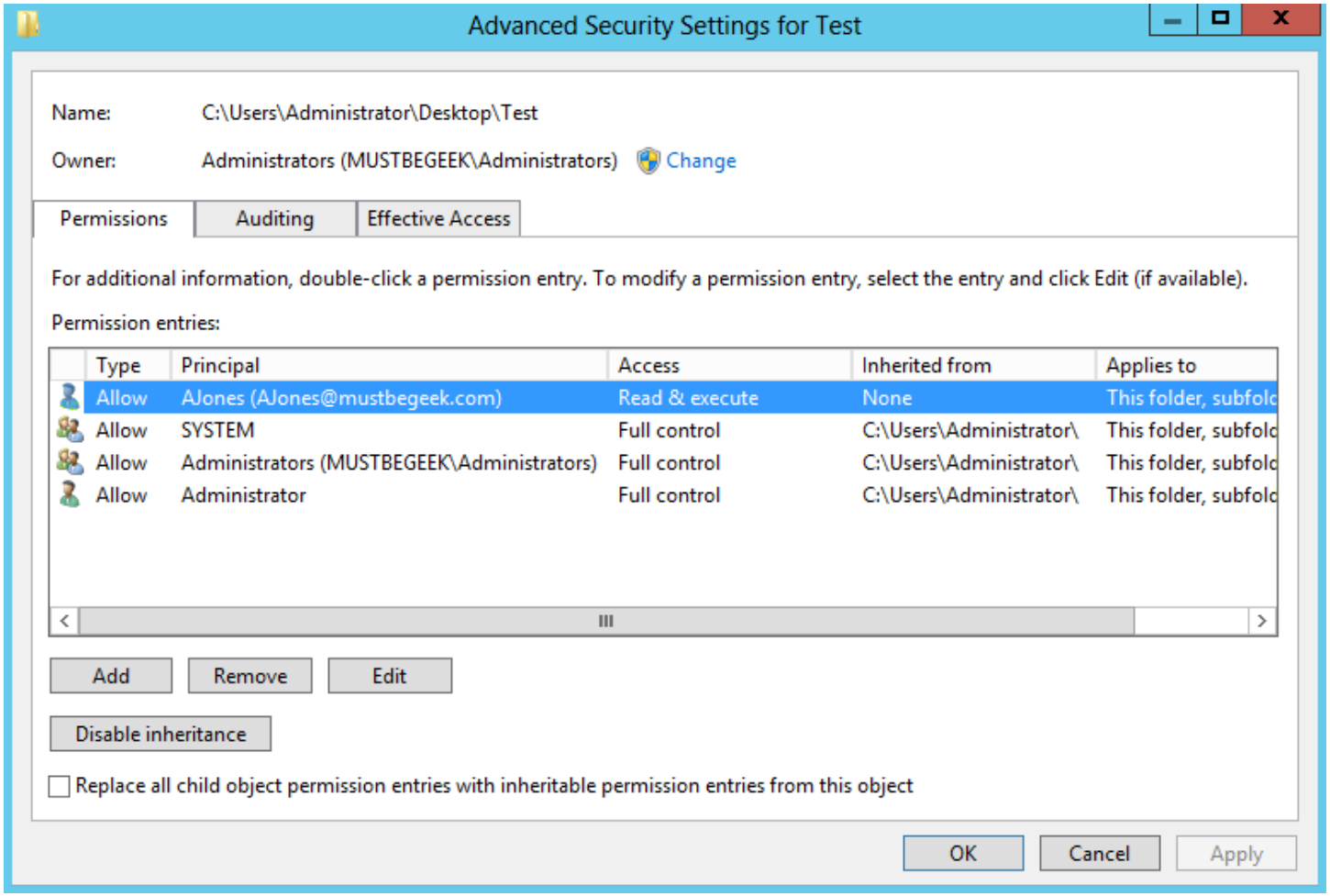
9.7 NTFS File i Folder dozvole

1. Da bi konfigurisali NTFS dozvole za foldere ili fajlove otvorite **Properties** za taj objekat
2. Izaberite **Security** opciju
3. U prozoru **Group or user names**, izaberite ili dodajte grupu ili korisnika.
4. U prozoru **Permissions**, dozvoli ili zabrani dozvolu.
5. Postoje dva tipa NTFS dozvola: standardne i specijalne.
6. Standardne dozvole su prikazane u prozoru **Permissions**
7. Za specijalne dozvole potrebno je da izaberete opsiju **Advanced**.



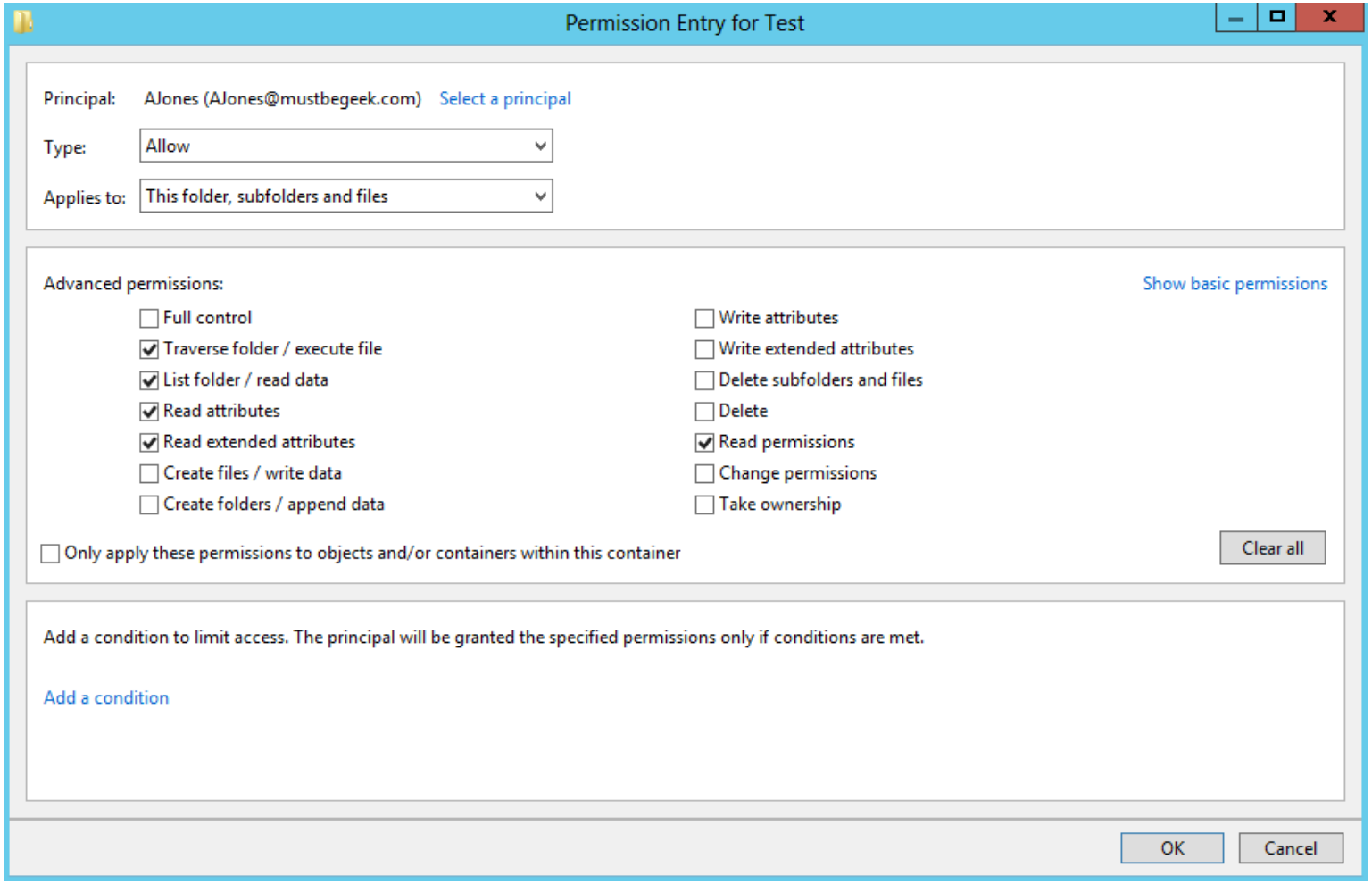
9.7 NTFS File i Folder dozvole

8. Sada možete da dodate novu grupu ili korisnika (**Add**) za koga će važiti podešene NTFS dozvole ili obristai neki objekat (**Remove**).
9. Takođe možete da izaberete već postojeće korisnike ili grupe i biranjem opcije **Edit** izvršiti konfigurisanje specijalnih NTFS dozvola.



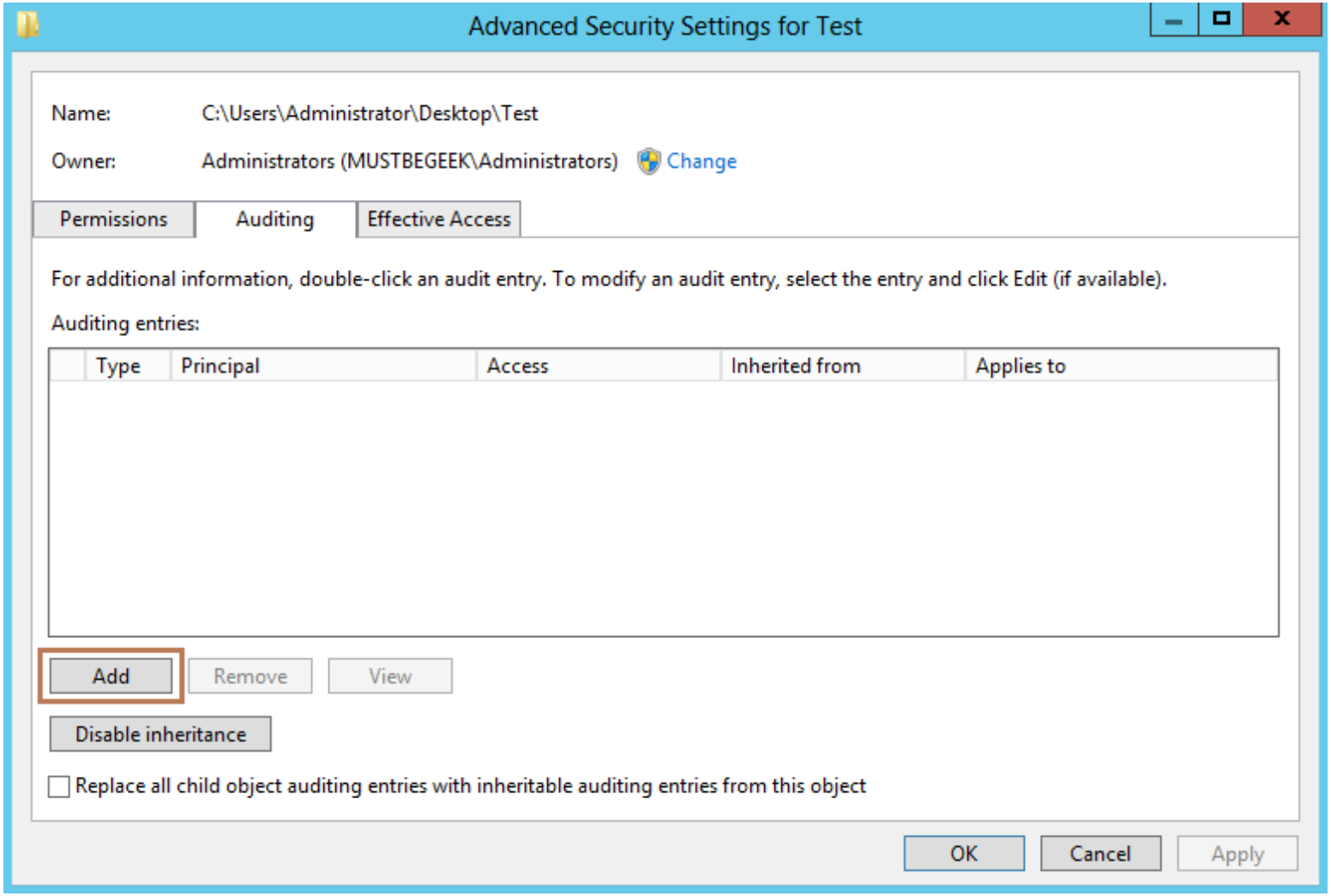
9.7 NTFS File i Folder dozvole

10. Pojaviće se sledeći prozor u kome možete da podesite specijalne NTFS dozvole.



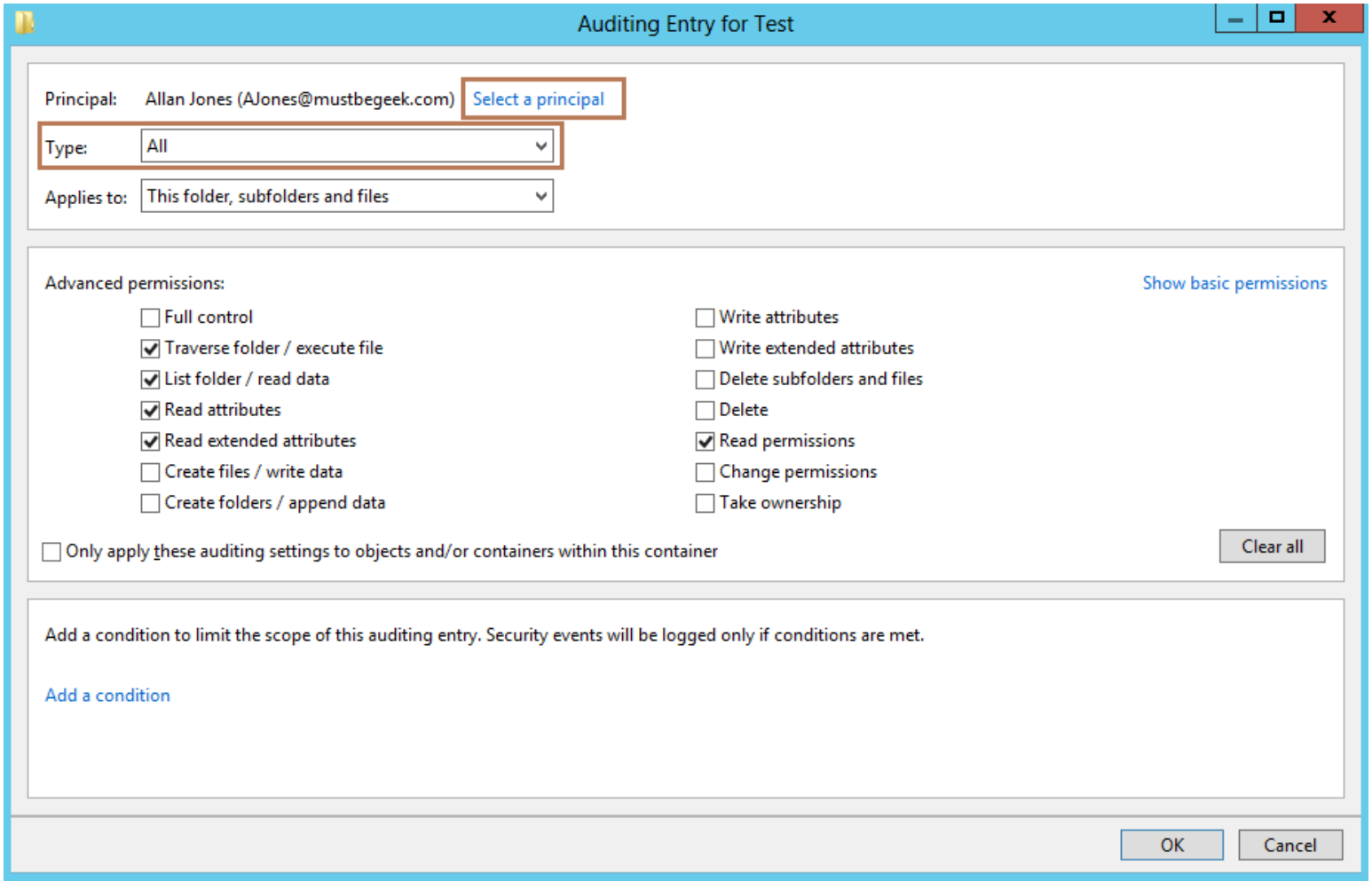
9.7 NTFS File i Folder dozvole

11. Opcija **Auditing** omogućava nam da obeležimo objekte za koje hoćemo da pratimo ko pristupa tom objektu (pravljenje log izveštaja za taj objekat). Biramo opciju **Add** za dodavanje novog objekta.



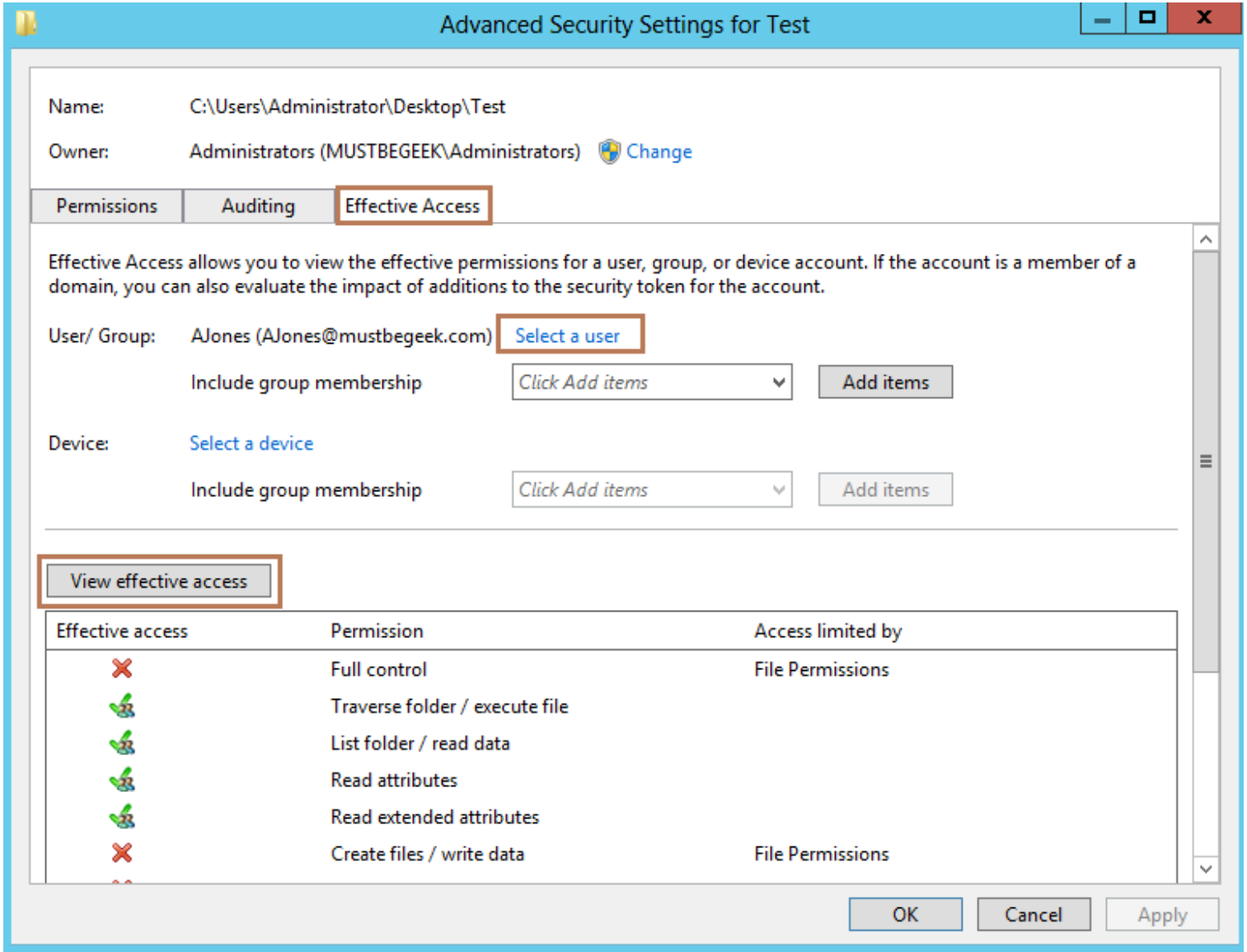
9.7 NTFS File i Folder dozvole

12. Izaberite **Select a principal** da bi konfigurisali **auditing option** za korisnike ili grupe. U prozoru **Type**, birate **All** ako želite da se beleže i uspešni i neuspešni pristupi obeleženom objektu, ali samo za izabranog korisnika ili grupu (**principal**). Pritisnite **OK** da bi sistem prihvatio to.



9.7 NTFS File i Folder dozvole

13. Opcija **Effective access** omogućava nam da testiramo i proverimo NTFS dozvole koje smo ranije postavili za određene objekte i korisnike.



Hvala na pažnji !!!

Pitanja

? ? ?