Securizarea fişierelor

10 Mai

Cuprins

- Partajarea resurselor
- Offline files
- DFS
- Shadow copy
- Permisiuni NTFS
- EFS
- Disk quotas

Partajarea resurselor

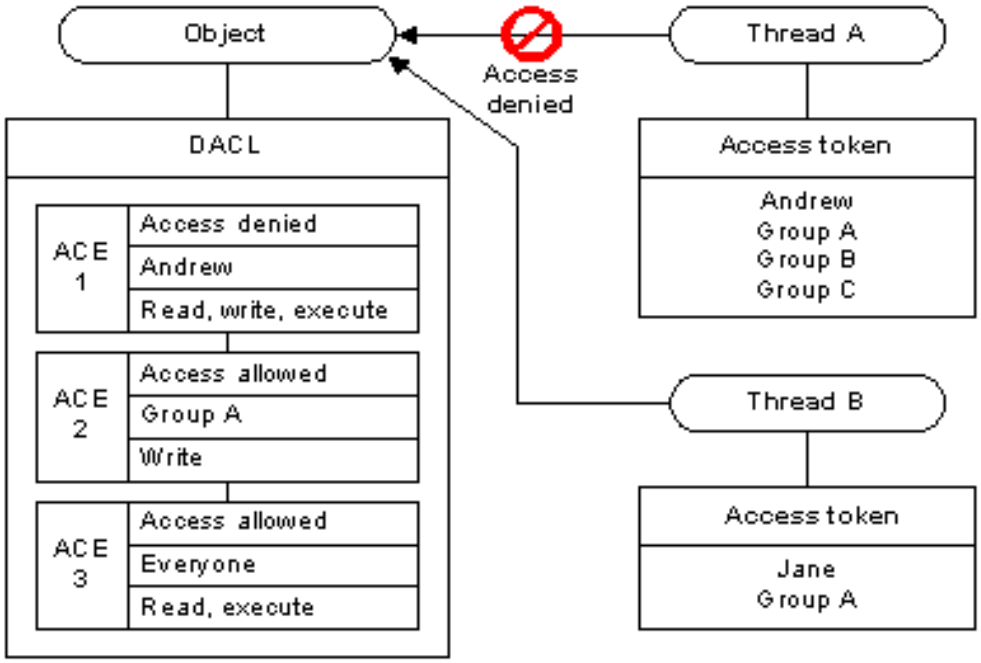
- De ce?
  - sneakernet – all over again?
- Ce?
  - fişier
    - resursă disponibilă clienţilor autorizaţi prin intermediul unei reţele
- Cine poate partaja?
  - membru al unuia din grupurile
    - Administrators, Power Users, Server Operators
- Cum?
  - Windows Explorer interface
  - Computer Management console

Partajarea resurselor

- Se pot partaja resurse pe orice tip de sistem de operare
  - client sau server
- Sistemele de operare client au o limita la numărul de conexiuni
  - net config server pentru a vedea numărul maxim
  - Ex. 20 pentru Windows 7
- Accesarea resurselor se face folosind UNC
  - Universal Naming Convention
- Pentru a ascunde un fişier partajat adăugaţi semnul $ la sfârşitul fişierului

Partajarea resurselor

- Foloseşte liste de acces per fişier
  - discretionary access control list (DACL)
  - access control entries (ACEs)
- Lista de acces blochează în mod implicit accesul la resursă



Drepturi asupra fişierelor partajate

- se aplică doar atunci când fişierul este accesat prin reţea
- sunt moştenite de către fişierele din interiorul directorului partajat
- sunt cumulative
  - dacă un utilizator face parte din mai multe grupuri, se adună drepturile “primite” pentru fiecare grup
  - !! dacă un tip de acces este blocat explicit, această regulă suprascrie orice altă regulă

Tipuri de acces

- Două metode de atribuire de permisiuni
  - Atribuirea unui rol pentru un utilizator/grup
  - Atribuirea de permisiuni pentru utilizator/grup

Permisie	Rol	Descriere
Read	Reader	• Browse • Open • Copy from • Run programs
Change	Contributor	• Toate acţiunile de Read • Write • Change file attributes • Create • Copy to • Delete
Full control	Owner Co-owner	• Toate acţiunile de Read şi Change • Configurarea permisiunilor de partajare

Offline files

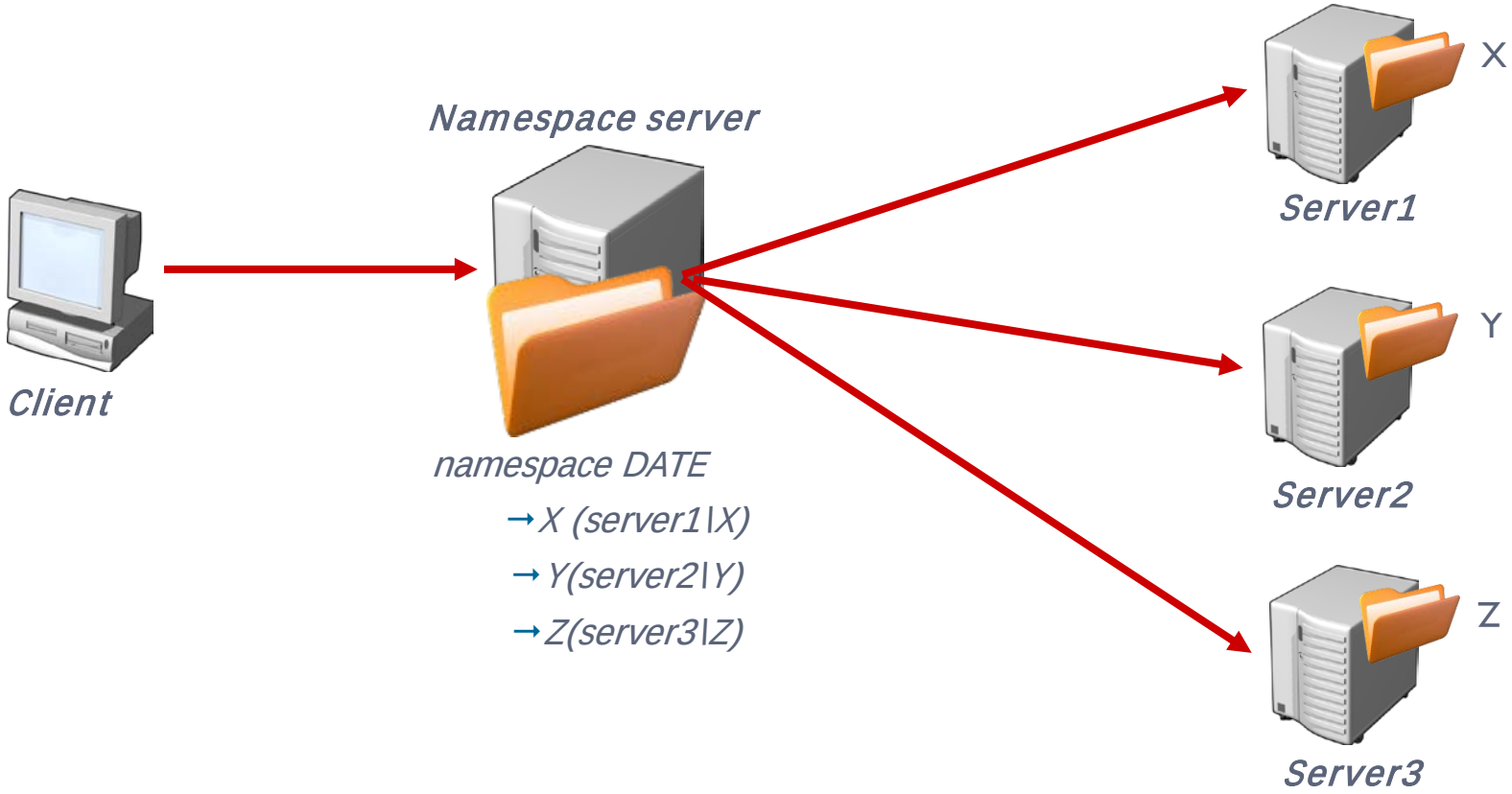
- Fişierele partajate vor fi copiate pe hard local
  - limită pentru spaţiul ocupat
- Accesarea fişierelor offline se face similar cu accesarea fişierelor partajate
- Serviciul este activat permanent
  - (implicit) utilizatorul specifică ce fişiere să fie disponibile offline
  - toate fişierele deschise vor fi disponibile offline
  - fişierele nu sunt accesibile offline
- Fişierele descărcate local pot fi criptate

Sincronizare

- Sincronizare automată la conectarea la reţea sau forţată de către utilizator
- Pentru metoda de sincronizare se foloseşte data la care a fost modificat un fişier
- Acţiunii în cazul unei desincronizări
  - păstrarea versiunii de pe server
  - folosirea versiunii modificate de către utilizator
  - păstrarea ambelor versiuni

Distributed file system

- Accesarea centralizată a resurselor partajate
- Permite controlul centralizat al tipului de acces



DFS – Fapte

- Directorul principal poarta denumirea de namespace
- Două posibile configuraţii pentru servere DFS
  - domain-based
    - accesarea se face folosind \\domainname\namespace
    - datele despre namespace sunt stocate in AD
    - pot exista mai multe servere fizice cu același namespace
    - se pot replica datele din fişierele destinaţie, dacă acestea sunt pe calculatoare ce rulează cel Windows Server 2003 R2 sau 2008
      - topologii de tip hub şi spoke, full mesh sau custom
  - stand-alone
    - accesarea se face folosind \\servername\namespace
    - datele despre namespace sunt stocate în registru
- Fişierele destinaţie trebuie să fie pe o partiţie NTFS

Shadow copy

- Copierea incrementală a fişierelor la intervale regulate de timp
- Nu este o soluţie de backup
- Activarea serviciului permite
  - recuperarea datelor şterse
  - recuperarea unei versiunii anterioare
  - compararea versiunilor existente
- Activarea se face per partiţie
  - În Windows 7 activarea se face prin activarea serviciului System Protection

Shadow copy

- Salvează maxim 64 de versiuni
- Şterge versiunile mai vechi
- Permite planificarea intervalului pentru salvarea datelor
- Implicit datele sunt salvate pe aceeaşi partiţie
  - nu poate fi folosit un alt calculator
  - recomandată folosirea unui alt hard intern
- Permisiunile NTFS sunt păstrate la recuperarea datelor
- Utilitarul folosit pentru management *vssadmin*

Reguli pentru acces la fişiere

- Doar pentru partiţiile NTFS
- Sunt cumulative
  - un utilizator acumulează toate drepturile grupurilor din care face parte
- Drepturile pe un director sunt moştenite implicit
  - această regulă poate fi dezactivată per director
- Drepturile care blochează accesul suprascriu orice drepturi care permit accesul
- Drepturile pot fi configurate pentru
  - fişiere
  - directoare

Drepturile standard

Permisiune	Descriere
Read	Vizualizare detalii şi atribute director. Vizualizare atribute fişier şi deschiderea unui fişier.
Write	Modificarea directoarelor sau a fişierelor, si a atributelor.
List Folder Contents	Acţiunile din Read plus abilitatea de listare a conţinutului unui director.
Read & Execute	Acţiunile din Read şi abilitatea de a executa programe.
Modify	Acţiunile din Read & Execute şi Write, plus abilitatea de a adăuga sau şterge fişiere.
Full Control	Toate acţiunile plus abilitatea de deveni owner şi a modifica permisiunile.
Special permissions	Folosite atunci când se folosesc drepturile mai specifice.

Drepturi speciale

- Permit o mai mare granularitate de declarare a drepturilor
- Folosite pentru controlul drepturilor moştenite
- Pentru un director pot controla modul în care sunt moştenite drepturile
  - pot suprascrie drepturile moştenite de la directorul părinte
  - pot suprascrie drepturile doar pentru anumite fişiere copil
    - This folder only
    - This folder, subfolders, and files (default)
    - This folder and subfolders
    - This folder and files
    - Subfolders and files only
    - Subfolders only
    - Files only

Drepturi speciale

Permisiune	Descriere
Traverse Folder/Execute File	Parcurgerea conţinutului unui director, sau executarea unui program.
List Folder/Read Data	Vizualizarea unui director, citirea datelor dintr-un fişier.
Read Attributes	Vizualizarea atributelor unui fişier sau director.
Read Extended Attributes	Vizualizarea atributelor extinse(definite de programul care a creat acel fişier) ale unui fişier sau director.
Create Files/Write Data	Crearea de fişiere într-un director sau modificarea unui fişier.
Create Folders/Append Data	Crearea de directoare într-un director şi adăugarea de date la sfârşitul unui fişier.
Write Attributes	Modificarea atributelor pentru fişiere sau directoare, precum Read-Only.
Write Extended Attributes	Modificarea atributelor extinse pentru fişiere sau directoare.
Delete Subfolders and Files	Ştergerea de directoare sau fişiere din directorul curent.
Delete	Ştergerea de directoare sau fişiere curente.
Read Permissions	Vizualizarea permisiunilor standard.
Change Permissions	Modificarea permisiunilor standard.
Take Ownership	Poate deveni owner pe un fişier sau director. Un owner poate modifica permisiunile unui fişier, indiferent de celelalte permisiunii existente.

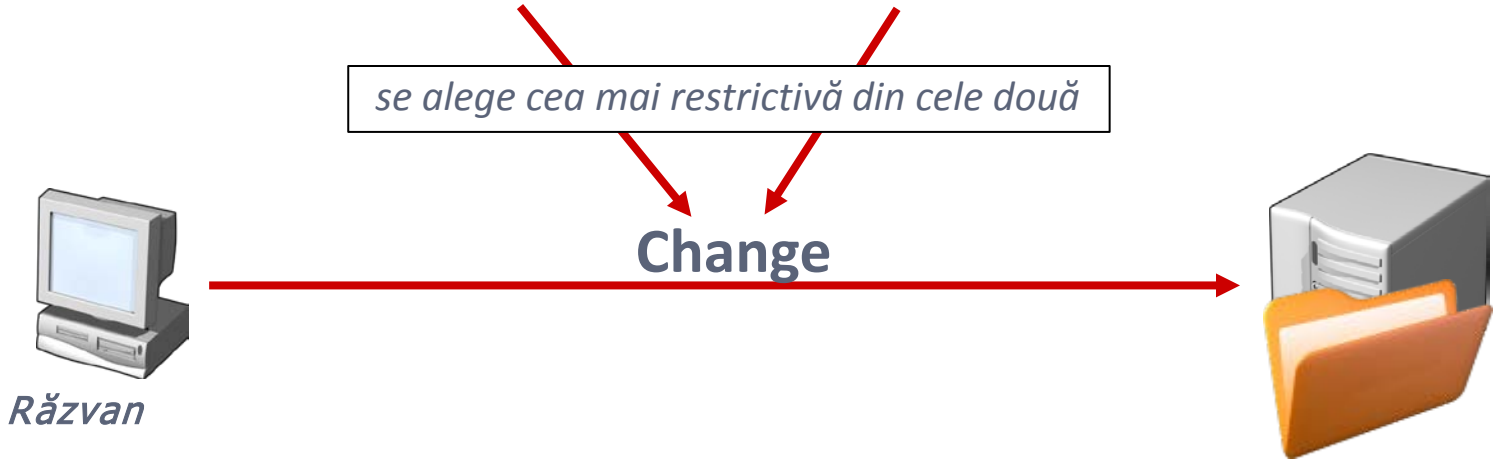
Calcularea permisiunilor

- Permisiunea efectivă este o sumă formată din:
  - drepturile explicite aplicate pentru utilizator
  - drepturile explicite aplicate pentru grupurile din care face parte un utilizator
  - drepturile moştenite de la obiectul părinte
- tab-ul Effective Permissions este folosit pentru vizualizarea drepturilor unui utilizator

Drepturile fişierelor partajate

- Răzvan face parte din trei grupuri

Grup	Drepturi NTFS	Drepturi partajare
MSSR	Modify	Read
Profi	Full control	Change
Consiliu	Read	Read
Suma (+)	Full control	Change



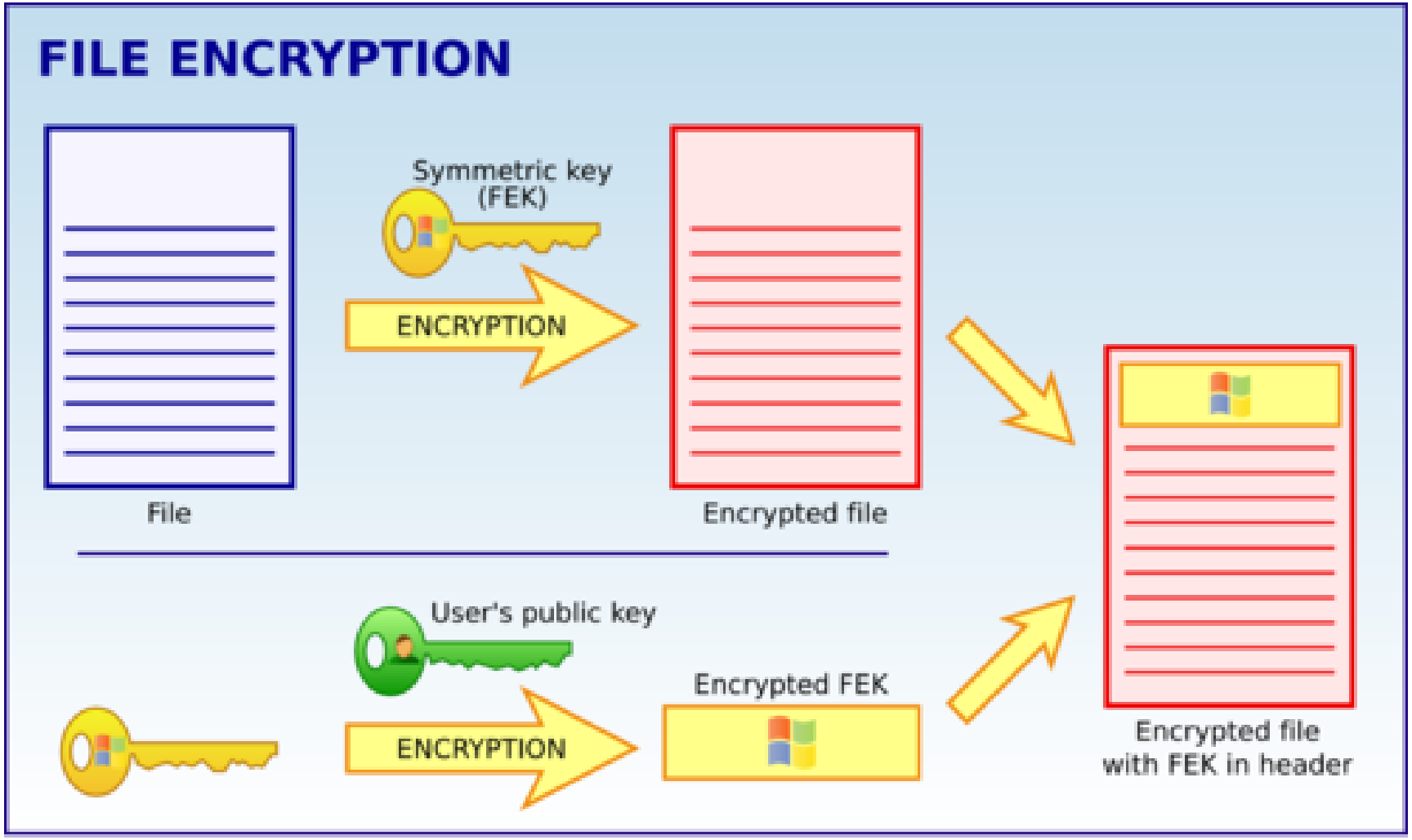
Encrypting File System

- Metodă de securizare a fişierelor sau directoarelor
- Foloseşte chei simetrice şi asimetrice pentru criptarea fişierelor
- Nu poate fi folosit împreună cu comprimarea fişierelor
- Necesită drepturi de scriere pentru criptare
- Foloseşte următoarele structuri
  - File encryption key (FEK)
    - cheie simetrică folosită pentru criptare
  - Data decryption field (DDF)
    - antet folosit pentru păstrarea cheii simetrice criptate de cheia publica a utilizatorului cu acces
  - Data recovery filed (DRF)
    - antet folosit pentru păstrarea cheii simetrice criptate de cheia publica a agentului de recuperare

EFS - Fapte

- Designed recovery agents
  - Agent folosit pentru recuperarea datelor
  - Începând cu Windows XP nu există un DRA implicit
  - Folosirea comenzii cipher /r creează un certificat
  - Prin intermediul “Local Security Policy” se creează un DRA folosind certificatul generat anterior
- Implicit este folosit algoritmul AES 256 biți pentru criptarea fişierului
- Se folosesc certificate pentru criptarea cheilor simetrice

EFS – How it works



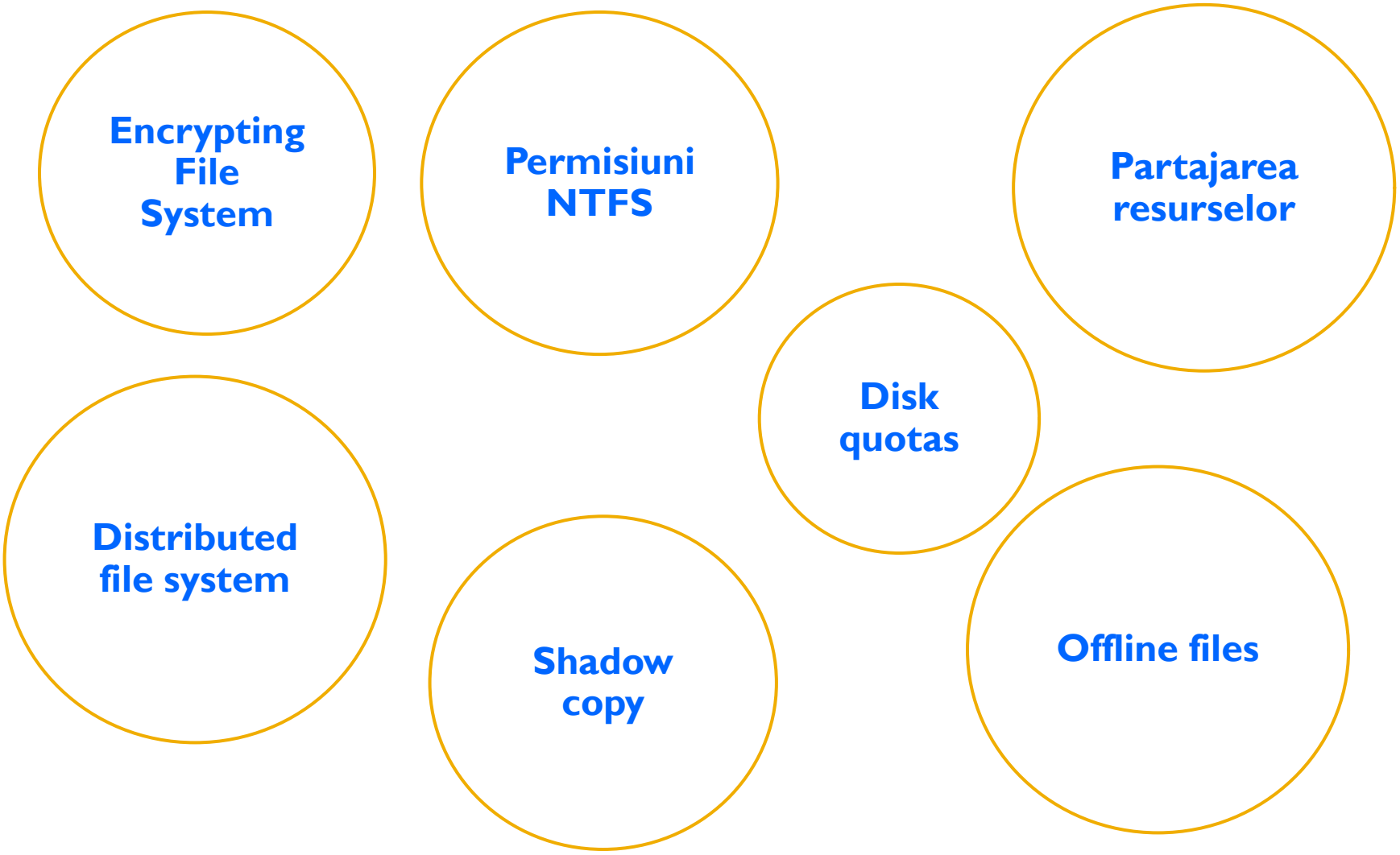
Reguli de mutare a fişierelor

- Mutarea/copierea unui fişier criptat pe o partiţie non-NTFS duce la pierderea criptării
- Mutarea/copierea unui fişier criptat pe o partiţie NTFS păstrează criptarea
- Mutarea unui fişier necriptat într-un director criptat duce la decriptarea fişierului
- Copierea unui fişier necriptat într-un director criptat duce la criptarea fişierului
- Criptarea este păstrată atunci când se realizează un backup

Disk quotas

- Restricţionează spaţiul folosit de un utilizator pe o anumită partiţie
- Poate fi configurat doar pentru partiţii de tip NTFS
- Se calculează dimensiunea pentru care utilizatorul este owner
  - compresia fişierelor nu este luată în calcul
- Implicit limita este configurată pentru toţi utilizatori, se pot crea excepţii de la reguli
  - utilizatorul Administrator nu poate avea limită de spaţiu
- Se poate configura o limită de avertizare

Overview


Encrypting File System
Permisiuni NTFS
Partajarea resurselor
Disk quotas
Distributed file system
Shadow copy
Offline files