Utenti, gruppi e permessi nei s.o. Microsoft

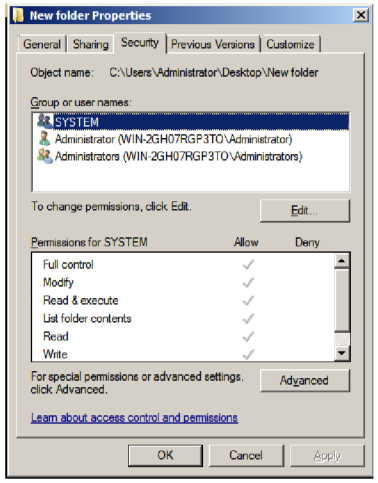
- Generalità NTFS
- Implementare la sicurezza di NTFS
- Implementare la condivisione di risorse
- Permessi locali e permessi sulle condivisioni NTFS
- Utenti e loro proprietà
- Tipi di gruppi
- Estensione dei gruppi sui domini
- Gruppi predefiniti

Filesystem in ambiente Microsoft®

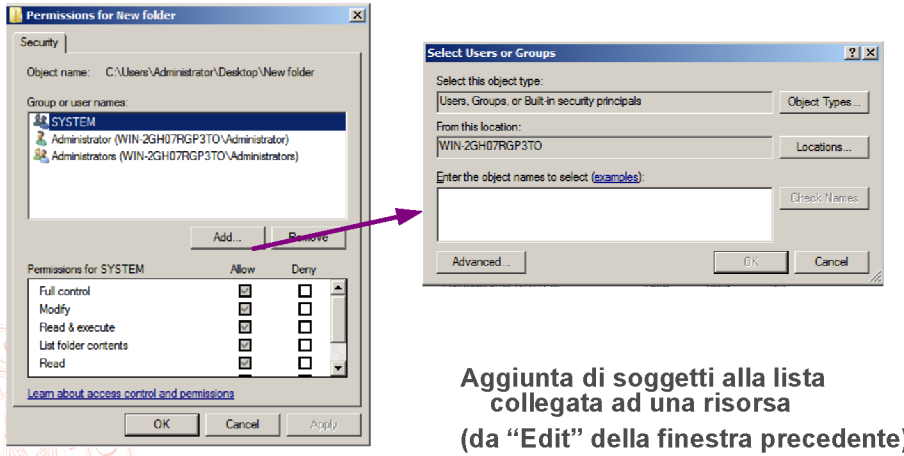
- FAT (File Allocation Table)
  - Origine: 1977, floppy disks
  - Molto semplice, basso overhead
  - 3 evoluzioni per superare via via I limiti di dimensioni (FAT12 – 32MB, FAT16 – 4GB, FAT32 – 8TB)
  - Nomi "8.3" → estensione LFN per memorizzare nomi lunghi
  - *Progettato per sistemi monoutente → no controllo dell'accesso*
- NTFS (New Technology File System)
  - Origine: 1993, Windows NT 3.1
  - Journaled, indicizzato con B+trees
  - *Supporta il controllo dell'accesso associando un'ACL a ogni risorsa*
- ReFS (Resilient File System)
  - Origine: Windows Server 2012
  - Integra tutte le funzionalità di rilevazione danni e gestione ridondanza
  - Stesse ACL di NTFS
  - In via di completamento (ad oggi: 2017) e graduale adozione

Controllo dell'accesso

- Le autorizzazioni sono assegnate sotto forma di ACL: ad ogni risorsa è associata una lista di soggetti (utenti o gruppi) e dei relativi permessi che essi detengono sulla risorsa
- Le ACL sono disponibili
  - su partizioni NTFS
  - sulle condivisioni di risorse in rete
- Per modificare le ACL è necessario
  - o detenere l'Ownership
  - o che nell'ACL medesima siano assegnati i permessi 'Full Control' o 'Change Permissions'



Esempio di modifica delle ACL



Aggiunta di soggetti alla lista collegata ad una risorsa

(da "Edit" della finestra precedente)

Ownership ed autorizzazioni

- Ownership
  - L'Owner di files e directories ha il pieno controllo (Full Control)
  - Administrator può sempre prendere l'ownership
  - L'Owner può assegnare le permissions per prendere l'Ownership
  - Nota: gli utenti che creano un file o una directory ne detengono l' Ownership
- Autorizzazioni NTFS predefinite
  - Ad Everyone viene assegnato automaticamente Full Control
  - I nuovi file ereditano le autorizzazioni della cartella in cui vengono creati (questo vale anche per i files che vengono copiati in un direttorio)

Accesso ed auditing

- Le ACL per il controllo dell'accesso fanno sì che, ad ogni tentativo di utilizzo di una risorsa, il sistema risponda autorizzando o negando l'operazione
- Ad ogni risorsa è inoltre associata una SACL utilizzata per l'auditing, che si presenta come una normale ACL, ma permette di tracciare gli esiti dei tentativi di utilizzo
- Le regole nella SACL possono essere impostate in modo che
  - quando un determinato soggetto tenta un'operazione e, grazie alla configurazione della ACL standard, *riesce*, questo evento sia registrato
  - quando un determinato soggetto tenta un'operazione e, grazie alla configurazione della ACL standard, *viene bloccato*, questo evento sia registrato

Autorizzazioni standard e speciali

- L'obiettivo del sistema di controllo delle autorizzazioni è duplice
  - elevata precisione nel controllo dell'accesso
    - in termini di tipo di azioni da concedere/negare
    - in termini di gestione delle complesse relazioni tra utenti e gruppi che possono essere titolari delle autorizzazioni
  - facilità d'uso
    - il sistema è Discretionary Access Control (DAC), quindi consente ad ogni utente anche non tecnico di manipolare le autorizzazioni sulle proprie risorse
    - anche l'utente più esperto per il 90% del tempo fa cose semplici

Autorizzazioni standard e speciali (cont.)

- La soluzione ai due problemi è realizzata con un sistema che prevede tre strati di interfaccia utente per "svelare" all'occorrenza i dettagli che servono:
  - a basso livello il sistema supporta
    - molte autorizzazioni (*autorizzazioni speciali*) --> possibilità di controllo fine sui permessi
    - con una logica a tre valori (*allow, deny, not set*) --> possibilità di definire regole di interazione quando diverse ACL vengono combinate
  - le autorizzazioni speciali sono aggregate in un set più ridotto di *autorizzazioni standard*
  - le autorizzazioni standard possono essere visualizzate a due valori (*allow, not set*) o mostrando esplicitamente i tre valori

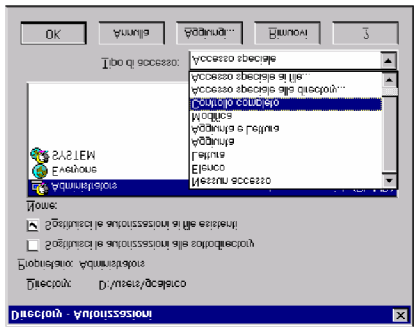
Autorizzazioni standard (elenco)

Abbreviation	Type	Description
R	Read	Provides the designated user or group the ability to read the file or the contents of the folder.
W	Write	Provides the designated user or group the ability to create or write files and folders.
RX	Read & Execute	Provides the designated user or group the ability to read file and folder attributes, view folder contents, and read files within the folder. If this permission is applied to a folder, files with inheritance set will inherit it (see the inheritance discussion).
L	List Folder Contents	Same as Read & Execute, but not inherited by files within a folder. However, newly created subfolders will inherit this permission.
M	Modify	Provides the ability to delete, write, read, and execute.
F	Full Control	Provides the ability to perform any action, including taking ownership and changing permissions. When applied to a folder, the user or group may delete subfolders and files within a folder.

Corrispondenza tra autorizzazioni standard e speciali

Types	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
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	
Change Permissions	X					
Take Ownership	X					

Esempio di manipolazione delle ACL (vecchia interfaccia semplificata)



Nelle nuove versioni di Windows, tutte le interfacce mostrano le colonne Allow e Deny, nelle vecchie esisteva una vista ancor più semplificata per scegliere

- una delle autorizzazioni standard (implicitamente equivalente a settare “Allow” su tutte le autorizzazioni speciali corrispondenti)
- oppure “Nessun accesso”, equivalente a deny su tutti i permessi

Autorizzazioni di accesso alle cartelle

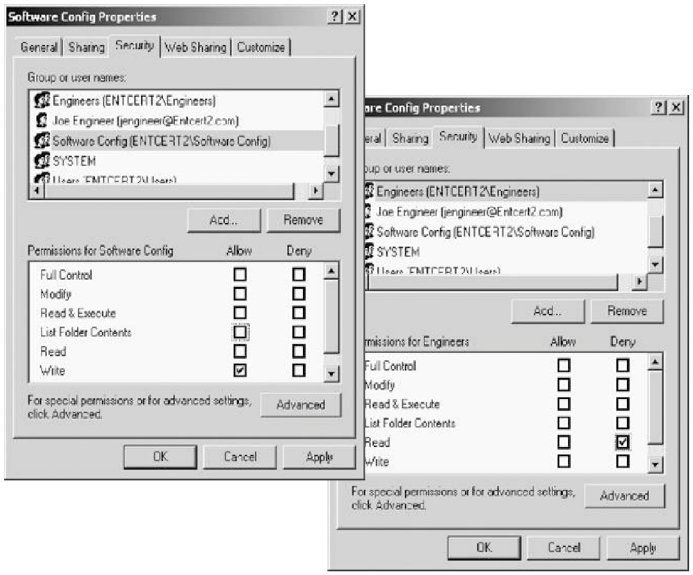
- Sulle cartelle è possibile impostare una delle seguenti autorizzazioni standard:
  - Nessun accesso
  - Elenco
  - Lettura
  - Aggiunta
  - Aggiunta e Lettura
  - Modifica
  - Controllo completo
- Nota: I gruppi o gli utenti a cui è stata concessa l'autorizzazione ‘Controllo completo’ su una cartella sono in grado di eliminarne i file, indipendentemente dall'autorizzazione che li protegge.

Autorizzazioni di accesso ai file

- Sui file è possibile impostare le seguenti autorizzazioni standard:
  - Nessun accesso
  - Lettura
  - Modifica
  - Controllo completo
- Impostando le autorizzazioni di accesso a un file sarà possibile specificare il tipo di accesso al file consentito a un gruppo o a un utente. Altrimenti, un file eredita le autorizzazioni proprie della cartella in cui è stato creato.
- Nota I gruppi o gli utenti cui si concede l'autorizzazione Controllo completo su una cartella possono eliminarne i file, indipendentemente dall'autorizzazione che li protegge.

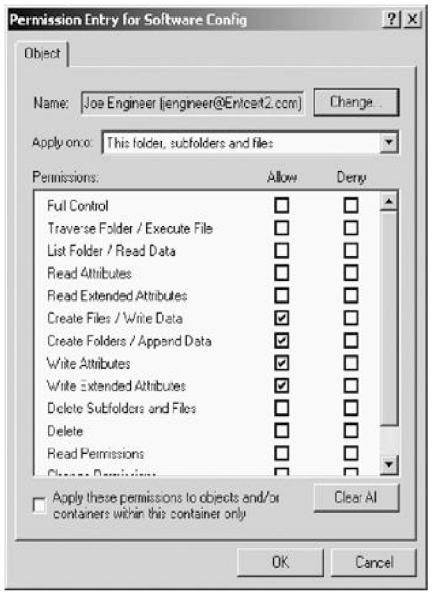
Esempio di manipolazione delle ACL (interfaccia completa su permessi standard)

Permette ancora di manipolare solo le autorizzazioni standard, non semplicemente scegliendone una dall'elenco, ma piuttosto impostando esplicitamente *allow, deny* o nessuno dei due valori per ciascuna.



Esempio di manipolazione delle ACL (interfaccia completa su permessi speciali)

Permette di settare ciascuna delle proprietà di basso livello ad uno dei tre valori *allow*, *deny*, o non impostata.



Composizione dei permessi

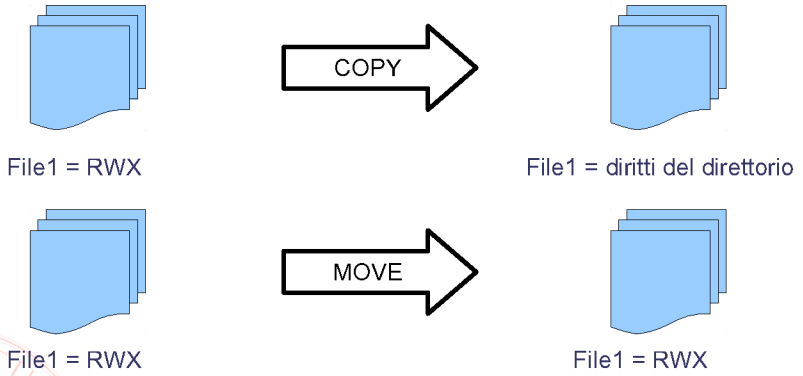
- Come visto, ogni diritto può essere esplicitamente concesso (ALLOW), esplicitamente negato (DENY), o non impostato (nè concesso nè negato)
  - In quest'ultimo caso, se l'utente non eredita il permesso per altra via, l'accesso è negato → "not set" == "soft deny"
- Questa logica a tre valori è fondamentale per effettuare la combinazione di permessi nel caso un soggetto sia coinvolto in più ACL
  - es. un utente membro di vari gruppi può essere soggetto di una ACL, così come i gruppi di cui fa parte, ed ogni entry potrebbe assegnargli permessi diversi
- La logica di base è che i permessi sono *cumulativi*, per cui un utente "somma tutte le crocette" che derivano dalle varie entry dell'ACL
  - nel caso questo porti, per una certa autorizzazione, ad avere sia *allow* che *deny*, quest'ultimo prevale → "deny" == "hard deny"

Esempio di composizione di permessi

Permessi di Michael	Permessi di Research	Permessi di Development	Permessi di Michael (effettivi)
Read	Read	-	Read
Write	-	Read	Change
Take Ownership	Read	Change	Take Ownership & Change
No Access	Read	Change	No Access
Change	No Access	Change	No Access

RWX = Read, Write, Execute
DPO = Delete, Permissions, Ownership
Change = RWXD

Permessi dopo un copy/move di file

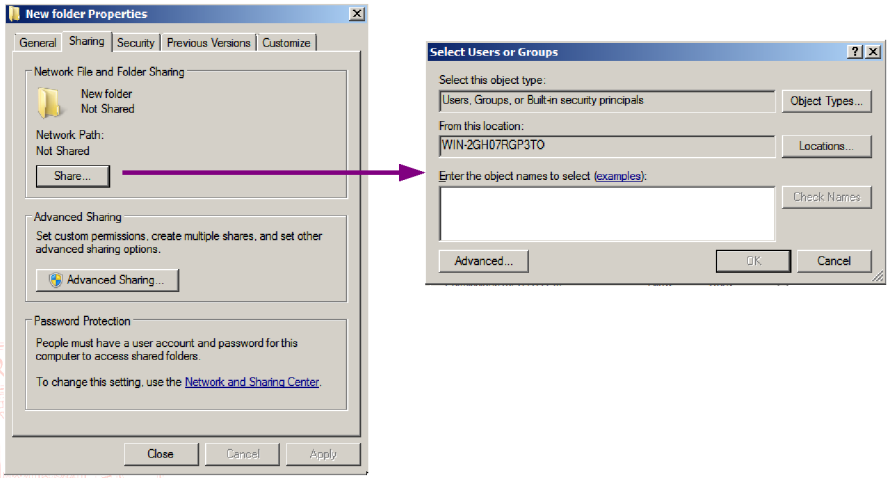


NOTA: MOVE verso una partizione diversa dalla sorgente = COPY (+delete)!

Condivisione di risorse

- Share = directory (folder) condivisa
- I diritti necessari per attivare le condivisioni sono concessi di default ai gruppi
  - Administrators
  - Server Operators (se in un dominio)
  - Power Users (se in un workgroup)
- Gli Users devono avere almeno il permesso List per fruire della directory condivisa

Condividere una cartella



Permessi locali vs. Permessi sulla condivisione

	Permessi assegnati	Permessi di Michael
Permessi Share	Everyone: Read Michael: Change	Change (RWXD)
Permessi locali	Everyone: Read Michael: Read	Read (RX)
Permessi effettivi		Read (RX)

Le ACL di Share si comportano come quelle di NTFS in termini di composizione di permessi, però vengono applicate in serie una all'altra, per cui complessivamente l'autorizzazione effettiva è quella più restrittiva tra le due

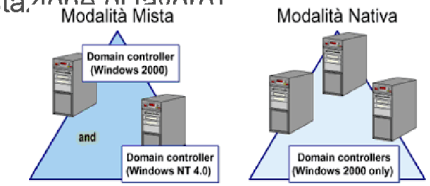
Organizzazione degli utenti e dei gruppi

- **Nell'uso più comune, i sistemi Microsoft sono raggruppati in un *dominio*: un insieme di computer, comunicanti tra loro e che condividono un directory database comune**
- **Gli utenti e I gruppi possono essere definiti**
  - **Localmente a ogni macchina**
  - **Nello stesso dominio della macchina su cui si trova la risorsa a cui vogliono accedere**
  - **In un altro dominio col quale intercorra una *relazione di fiducia***

Domini

I computer **condividono un directory database centralizzato**, cioè un database che contiene la definizione degli user account, dei gruppi e tutte le impostazioni inerenti la sicurezza. Tale database è chiamato "Directory" ed è una parte di Active Directory che è il directory services di Windows 2000. Tale database è contenuto su un server "particolare" denominato "**Domain Controller**".

Vantaggi: Amministrazione Centralizzata, Accesso Universale alle Risorse, Scalabilità, One User One Account (con un unico username ed un'unica password l'utente accede al dominio da qualsiasi postazione di lavoro)



Domini NT vs. 2000

Il modello di distribuzione dei dati in NT era di tipo MONOMASTER

PDC = Primary Domain Controller (RW)

BDC = Backup Domain Controller (RO)

Rielezione PDC in caso di gasto

Dall'avvento di Active Directory il modello è diventato MULTIMASTER

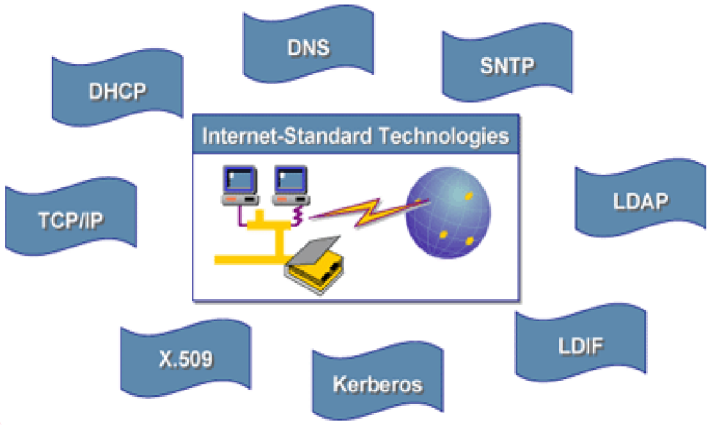
Tutti i DC sono paritetici

Sincronizzazione e replica ottimizzate per mezzo della configurazione di ***sites***

I sites servono anche a permettere la personalizzazione di determinate politiche sulla base della località geografica ed alle workstation per scegliere il "miglior" server cui rivolgersi (DC, logon, accesso a DFS, ...)

Compatibilità tra reti NT4.0 e 2000 (modalità mista): il primo DC ad andare online svolge la funzione di *PDC emulator*

Tecnologie Supportate

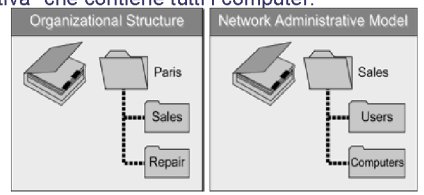


Unità Organizzative

Una "Unità Organizzativa" (OU – Organizational Unit) è un contenitore che ha lo scopo di organizzare oggetti (account utente, account di gruppo, computers, stampanti…) di Active Directory all'interno di un dominio.

Utilizzando le "Unità Organizzative" è possibile raggruppare oggetti di Active Directory in una struttura gerarchica, che meglio rappresenta la nostra organizzazione e che si basa su aspetti diversi della nostra organizzazione:

- Dislocazione Territoriale o Organizzazione Interna
- Responsabilità Amministrative. Ad esempio un utente è responsabile dell'amministrazione degli utenti ed un altro utente è responsabile dell'amministrazione dei computers. In tal caso creeremo un "Unità Organizzativa" che contiene tutti gli account utente ed una "Unità Organizzativa" che contiene tutti i computer.



Unità Organizzative

Ogni dominio può avere una sua gerarchia di "Unità Organizzative", indipendente da quella di altri domini della foresta

- nello spirito dell'organizzazione gerarchica, ogni oggetto può appartenere ad una ed una sola OU

Tale struttura è trasparente (ed invisibile) agli utenti ed ha l'unico scopo di facilitare l'amministratore nelle sue attività e nella delega di privilegi.

- E' infatti possibile delegare ad utenti o gruppi di utenti privilegi sugli oggetti contenuti in una "Unità Organizzativa" o su un sottoinsieme dei loro attributi.
- Non è possibile il contrario, cioè dire che una data OU (= gli utenti ad essa appartenenti) possiede o meno certi privilegi su altri oggetti

Poichè un dominio Active Directory può contenere un numero praticamente infinito di oggetti, grazie alle "Unità Organizzative" che permettono di organizzare in maniera anche molto strutturata tali oggetti e permettono di implementare meccanismi di delega molto sofisticati e dettagliati, spariscono molte delle motivazioni che in ambiente Microsoft Windows NT 4.0 costringerebbero ad implementare realtà multi dominio.

Alberi e Foreste

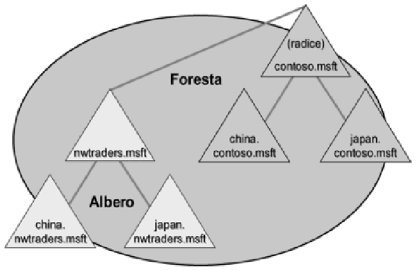
Nonostante l'utilizzo delle "Unità Organizzative", anche in Windows 2000 esiste una numerosa serie di situazioni in cui definiamo comunque degli ambienti multi dominio. Ad esempio:

- Avere ambiti di sicurezza separati
- Avere politiche di controllo delle password e di sicurezza diverse
- Avere uno spazio dei nomi che abbia una sua struttura gerarchica abbastanza complessa
- Controllo migliore della replica
- Amministrazione Decentralizzata

Alberi e Foreste

A differenza di Microsoft Windows NT 4.0, in Windows 2000 esiste esplicitamente una struttura comprendente più domini che prende il nome di "Foresta", che può essere formata da uno o più "Alberi".

Un "Albero" è una struttura gerarchica di Domini AD che condividono uno spazio dei nomi "contiguo". Quando si aggiunge un dominio ad un albero esistente, tale dominio sarà il dominio "figlio" di un dominio "padre" esistente, ed il suo nome si ottiene concatenandolo a quello del padre ed ottenendo in tal modo il suo nome DNS.



Alberi e Foreste

Una "Foresta" è un insieme di Alberi che non condividono uno spazio dei nomi contiguo.

Ogni albero ha il suo dominio Radice ed il primo domino Radice creato è anche il Dominio "Radice della Foresta" ("Forest Root Domain"): il suo nome identifica tutta la Foresta.

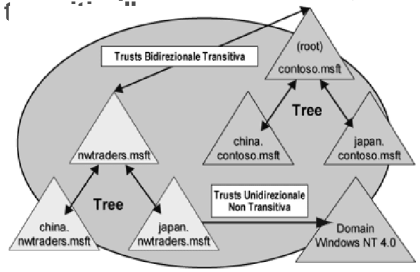
Esempio: la società "Azienda1" acquisisce la società "Azienda2" e, nonostante voglia che le due società condividano informazioni nello stesso tempo vuole realizzare una struttura Active Directory in cui lo spazio dei nomi sia formato da nomi non contigui. Per cui realizzerà la foresta formata dai due alberi "Azienda1.com" ed "Azienda2.com".

Quindi l'unica differenza tra un ambiente single-domain ed un ambiente multidomain è lo spazio dei nomi risultante. All'interno di una Foresta, sia che essa sia formata da un unico Dominio sia che essa sia formata da più Domini organizzati in uno o più Alberi, un utente appartenente a qualsiasi Dominio della Foresta può accedere a risorse appartenenti ad un qualsiasi altro Dominio, previa concessione di permessi.

Trust Relationship

"Trust Relationship" (relazioni di fiducia): consentono ad un controllore di dominio di utilizzare, considerandole appunto fidate, le informazioni in possesso di un altro DC. In questo modo gli utenti di un dominio sono riconosciuti da ogni altro dominio con cui esiste una TR, ed autorizzabili all'uso delle risorse

A differenza di Windows NT 4.0 che supportava solo relazioni di fiducia di tipo "unidirezionale, non transitivo", Active Directory supporta sia Relazioni di Fiducia di tipo "unidirezionale, non transitivo" ma anche "bidirezionale, t



Trust Relationship

Unidirezionale, Non Transitivo.

In una Relazione di Fiducia "Unidirezionale" se il Dominio A concede fiducia al Dominio B, non è vero che il Dominio B dia fiducia a Dominio A.

In una Relazione di Fiducia "Non Transitiva" se Dominio A concede fiducia a Dominio B che a sua volta dà fiducia a Dominio C, questo non implica che Dominio A dia fiducia a Dominio C.

In Active Directory è possibile definire manualmente Relazioni di Fiducia di questo tipo tra Active Directory e Domini Windows NT 4.0, ma anche tra domini Active Directory (ad esempio domini di foreste diverse).

Bidirezionale, Transitivo.

In una Relazione di Fiducia "Bidirezionale" se il Dominio A dà fiducia al Dominio B, è vero anche che Dominio B dà fiducia a Dominio A.

In una Relazione di Fiducia "Transitiva" se Dominio A da fiducia a Dominio B che da a sua volta fiducia a Dominio C, questo implica che Dominio A da fiducia a Dominio C.

Tale tipo di Relazione di Fiducia è quella di default in Active Directory ed è quella che viene creata automaticamente tra un dominio padre ed un dominio figlio all'interno di un albero e tra i domini radice dei vari alberi che formano una foresta ed il dominio radice della foresta.

Utenti

- Local user accounts
  - ristretti al sistema su cui sono creati
  - possono avere moderati permessi amministrativi (che non si estendono alla possibilità di accedere ai dati di altri utenti) --> Power Users Group
- Domain user accounts
  - appartiene ad un dominio
  - profilo memorizzato in AD
  - può accedere a risorse non locali, limitatamente ai privilegi che gli sono concessi
    - del proprio dominio
    - dei domini trusted

Proprietà dell'utente

- Sono moltissime,accessibili dai *tab* del wizard qui elencati:
  - Member Of — The user's defined group membership
  - Dial-in — Remote access and callback options
  - General — User's first name, last name, display name description, office location, telephone, e-mail, and Web pages
  - Address — User's post office mailing address
  - Account — Logon name, domain, logon hours, logon to server name, account options, and account expiration date
  - Profile — User profile path, profile script, home directory path and server, and shared document folder location
  - Telephones/Notes — Home, pager, and mobile phone numbers and comments on where to contact user
  - Organization — Job title, company, department, manager, and people who report to user
  - Environment — Applications to run from Terminal server client
  - Sessions — Timeouts for Terminal Services
  - Remote Control — Permissions for monitoring Terminal Service sessions
  - Terminal Service Profile — Location for Terminal Service home directory

Gruppi

- Ogni oggetto di AD può essere membro di uno o più gruppi (di tipo e scope appropriato)
- Distribution Groups
  - possono essere usati da qualsiasi applicazione abbia bisogno di una lista di utenti
  - il sistema operativo non li utilizza
    - non appesantiscono il logon ticket dell'utente
- Security Groups
  - come i DG, ma possono essere soggetti nelle regole che controllano l'accesso alle risorse del sistema
- In Windows 2003 funzionante in Native Mode è possibile la conversione da un tipo all'altro

Group scopes

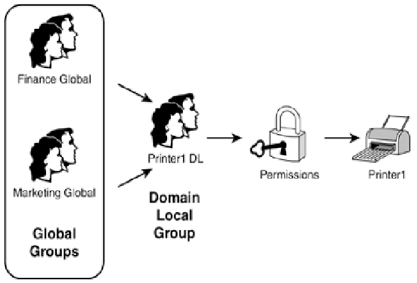
- Sia per i Distribution Group che per i Security Group vale il concetto di *scope* (estensione), che definisce
  - oggetti di quali domini possono far parte del gruppo
  - in quali domini può essere usato un gruppo per definire regole d'accesso
- La prima suddivisione è tra
  - Machine Local (locali ad una singola macchina)
  - Gruppi validi nel dominio
    - Domain Local
    - Global
    - Universal
- Nesting: è possibile *solo in native mode* rendere gruppi membri di altri gruppi

Group scopes

	Può contenere	Può essere membro di	Gli possono essere assegnati permessi su
Domain Local Group (DLG)	Utenti, GG, UG, computer di qualsiasi dominio, DLG dello stesso dominio	Altri DLG dello stesso dominio	Risorse dello stesso dominio
Global Group (GG)	Utenti ed altri GG dello stesso dominio	Qualsiasi DLG e UG, GG dello stesso dominio	Risorse di qualsiasi dominio
Universal Group (UG)	Utenti, GG, UG di qualsiasi dominio	DLG e UG di qualsiasi dominio	Risorse di qualsiasi dominio

Utilizzo tipico e consigliato

- Sebbene sia possibile assegnare diritti su risorse direttamente a UG e GG, la struttura consigliata è (caso più semplice):
  - individuare in ogni dominio utenti con esigenze analoghe e metterli in un GG
  - rendere i GG membro degli opportuni DLG
  - assegnare i permessi d'uso delle risorse ai DLG



Utilizzo tipico e consigliato

- In realtà molto ampie è possibile sfruttare gli UG per aggiungere un livello di nesting che consenta all'*enterprise administrator* di raggruppare i GG
  - individuare in ogni dominio utenti con esigenze analoghe e metterli in un GG
    - in questo modo si delega al *domain administrator* che conosce bene la propria realtà il compito di popolare i GG
  - raggruppare i GG omologhi in un UG
    - in questo modo si evita che alla riorganizzazione dei domini, o in generale alla comparsa/scomparsa di GG, i singoli amministratori delle risorse debbano agire sui DLG, ripopolandoli di conseguenza. Sarà l'*enterprise administrator* a sapere quali GG è opportuno assegnare agli UG, mentre questi ultimi saranno creati o distrutti solo in casi eccezionali.
  - rendere l'UG membro degli opportuni DLG
  - assegnare i permessi d'uso delle risorse ai DLG
    - gli amminstratori delle singole risorse possono scegliere i soggetti (GG e UG) preconfigurati ai passi precedenti come membri di DLG, anzichè come soggetti cui attribuire direttamente permessi, in modo che l'aggiunta o la rimozione di un UG/GG da un DLG si applichi automaticamente a tutte le risorse su cui tale DLG può operare

Gruppi predefiniti – domain local

Gruppo	Caratteristiche
Administrators	Controllo completo della macchina locale con tutti i provilegi; membri di default comprendono i Domain Admins, gli Enterprise Admins, e l'account Administrator.
Account Operators	Amministrazione degli utenti del dominio.
Backup Operators	Back up e restore dei file sulla macchina locale indipendentemente dai permessi ad essi associati; log on e shut down. Le Group policies possono limitare questi privilegi di default.
Guests	Logon/shutdown limitato sulla macchina locale.
Print Operators	Amministrazione delle stampanti locali.
Replicator	Gestione delle funzioni e dei servizi di replica di Active Directory.
Server Operators	Amministrazione del sistema locale.
Users	Esecuzione di applicazioni, accesso alle stampanti, logon/shutdown/locking, creazione e modifica fi gruppi locali; tutti gli utenti del dominio sono membri di default.

Gruppi predefiniti – global

Gruppo	Caratteristiche
Domain Admins	Privilegi di amministrazione su tutti i sistemi appartenenti al dominio
Domain Computers	Tutti i computer del dominio
Domain Controllers	Tutti i domain controller
Domain Guests	Appartiene al DLG "Guest"
Domain Users	Appartiene al DLG "Users"
Enterprise Admins	Appartiene al gruppo "Domain Admins" di ciascun dominio, concedendo quindi i privilegi di amministrazione a livello di foresta.
Group Policy Creators Owners	Ai membri è consentito modificare le group policy
Schema Admins	Ai membri è consentito modificare lo schema di Active Directory

Group Policy

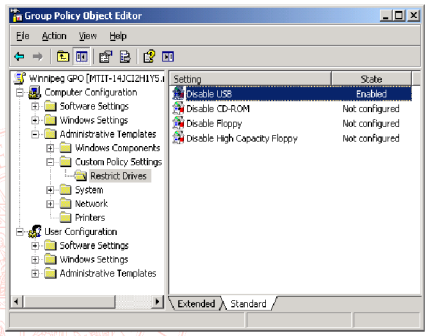
- Group Policy fornisce un quadro di riferimento per controllare l'ambiente di utenti e computer, cioè per assegnare quel tipo di privilegi o restrizioni che non sono legati a risorse fisiche ovvie quali file, cartelle, ecc.
- Le regole vengono definite in un Group Policy Object, che può essere collegato a qualsiasi contenitore di oggetti (una OU, un Site, un Domain) per applicarle a tutti gli oggetti in esso contenuti.
- Ogni GPO contiene due sezioni distinte
  - impostazioni per gli utenti (user settings)
  - impostazioni per i computer (computer settings)
- In ciascuna delle due sezioni le impostazioni sono ulteriormente classificate in:
  - impostazioni software (software settings)
  - impostazioni di Windows (Windows settings)
  - modelli per l'amministrazione (administrative templates)

Group Policy - impostazioni

Categoria	Finalità	Disponibile per computer?	Disponibile per utenti?
Software settings	Installare, aggiornare, rimuovere applicazioni	Sì	Sì
Windows settings	Definire scripts ed impostazioni di sicurezza (vedi colonne a fianco)	Start-up e shutdown scripts, numerose impostazioni di sicurezza	Logon e logoff scripts, alcune impostazioni di sicurezza, impostazioni di Internet Explorer, folder redirection
Administrative templates	Definire in modo centralizzato le impostazioni del registro di sistema	Sì	Sì

Group Policy - esempi

Limitare l'uso di una intera categoria di dispositivi, come le porte USB



Configurare il contenuto del desktop o del menu avvio