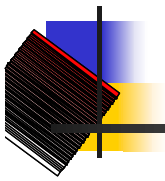
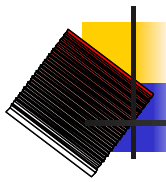


Reti e Domini Windows 2000

Corso di Amministrazione di Reti
A.A. 2002/2003

Materiale preparato utilizzando dove possibile materiale AIPA
http://www.aipa.it/attivita[2/formazione[6/corsi[2/materiali/Reti%20di%20Calcolatori/welcome.htm

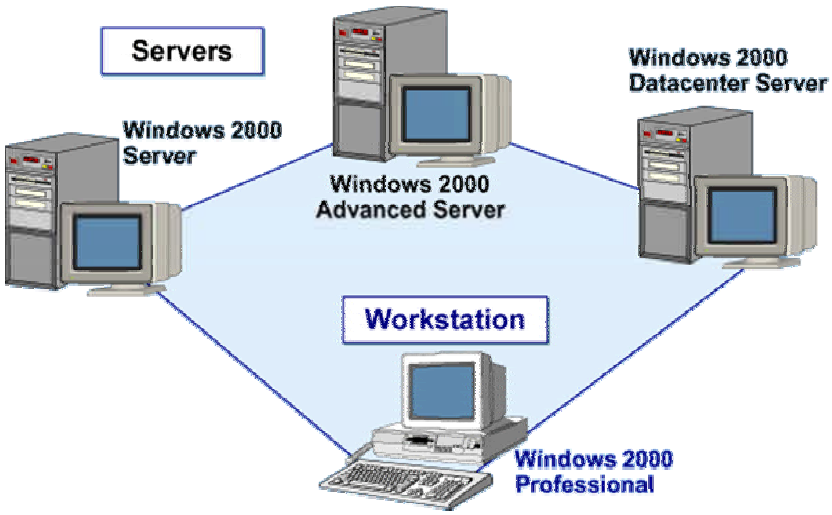
Giorgio Calarco - DEIS



Argomenti

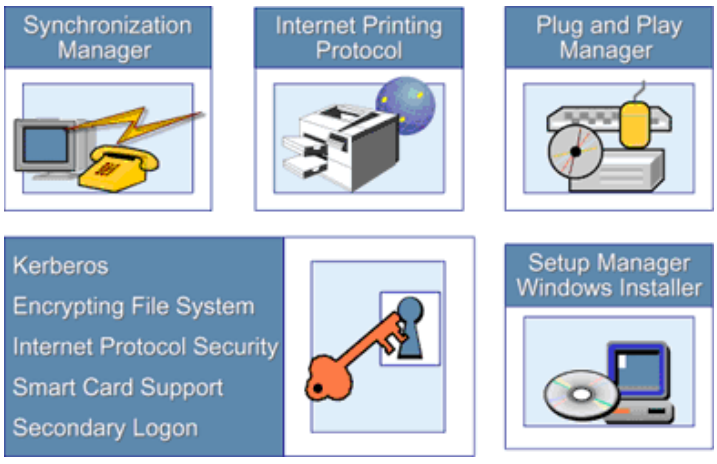
- Cenni di architettura Reti Windows 2000
  - Client e Server
  - Workgroup e Domini
- Domini Windows 2000
  - Introduzione ai Directory Services di Windows 2000
  - Active Directory
  - Supporto a protocolli standard e non proprietari
  - Spazio dei nomi
  - Active Directory e DNS

La famiglia Microsoft Windows 2000



Sistemi Client: Windows 2000 Professional

- **Semplicità d'Uso.** Oltre ai miglioramenti relativi all'interfaccia utente, offre il Supporto per Utenti Remoti: **Network Connestion Wizard**, per configurare l'accesso remoto (connessione dial-up, connessione ad Internet, connessione VPN, connessione via cavo); Supporto per Virtual Private Network (**VPN**)
- **Gestione dei Files.** File System **NTFS**, File System **FAT32**, deframmentazione dei dischi e utility di Backup
- **Sicurezza.** Ricordiamo le seguenti funzionalità:**Kerberos 5** (protocollo standard di autenticazione), **Encrypting File System** (permette di cifrare i file memorizzati su disco), Internet Protocol Security (**IPSec**) (permette di specificare politiche di cifratura per flussi di dati sulla rete).



Windows 2000 Server

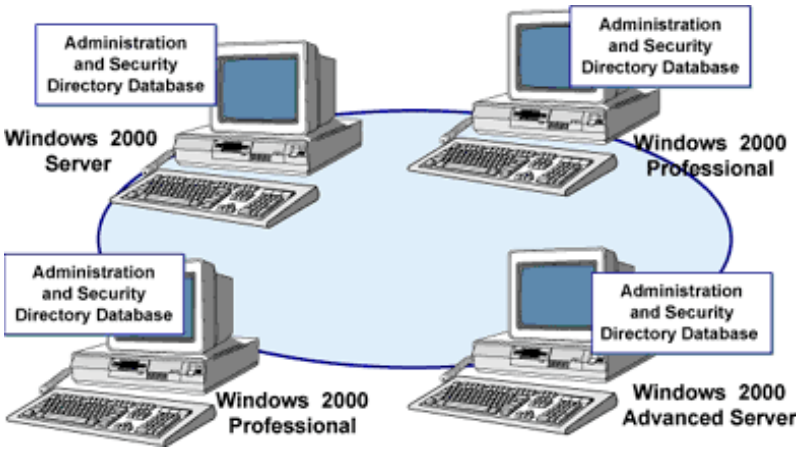
- Piattaforma che offre tutte le funzionalità di Microsoft Windows 2000 Professional + le funzionalità che ne ottimizzano le performance per le funzionalità di file server, print server ed application server.
- Servizio di Active Directory: che permette di centralizzare la gestione di utenti, gruppi, sicurezza e risorse di rete.
- Buona soluzione per l'implementazione di soluzioni enterprise in realtà medio-piccole: file server, print server, web server, Terminal Services server, server di accesso remoto.
- Requisiti hardware minimi per l'installazione di Microsoft Windows 2000 Server:
  - Processor: 32-bit Pentium 133 MHz.
  - Memory: 64 MB per eti di meno di 5 computer; 128 MB è il minimo raccomandato per tutte le altre situazioni.
  - uno o più dischi con un minimo di 680 MB (raccomandati 2 GB) Sulla partizione che conterrà i file di sistema

Windows 2000 Advanced Server

- Elevata disponibilità e bilanciamento dei carichi di lavoro (**Cluster**).
- Microsoft Windows 2000 Datacenter è la soluzione server ottimizzata per data warehouse, **o**n**l**ine **t**ransaction **p**rocessing (OLTP), simulazioni in real-.time, Web hosting. Microsoft Windows 2000 Datacenter ha tutte le caratteristiche di Microsoft Windows 2000 Advanced Server, ma supporta fino a 64 GB di memoria RAM e fino a 32 processori SMP.

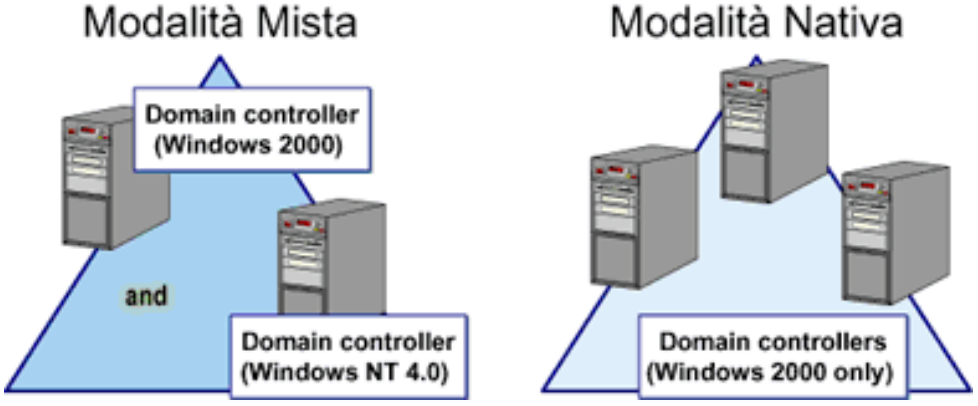
Workgroup

- Microsoft Windows 2000 permette di implementare **due ambienti di rete** in cui gli utenti possano condividere risorse (file, stampanti, applicazioni) indipendentemente dalle dimensioni della rete: i **workgroup** ed i **domini**.
- Un workgroup è chiamato anche rete **Peer-to-Peer** (paritetica) per evidenziare quella che è la sua caratteristica saliente: tutti i computer che appartengono ad un workgroup sono "uguali", senza che ci sia un server dedicato alla gestione della sicurezza. Ogni computer che esegua sia Microsoft Windows 2000 Professional sia Microsoft Windows 2000 Server gestisce **un proprio security database locale**, cioè una lista di utenti ed impostazioni di sicurezza inerenti il computer che ospita tale database: dunque in un workgroup le **gestione degli utenti e della sicurezza** è **decentralizzata**



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)

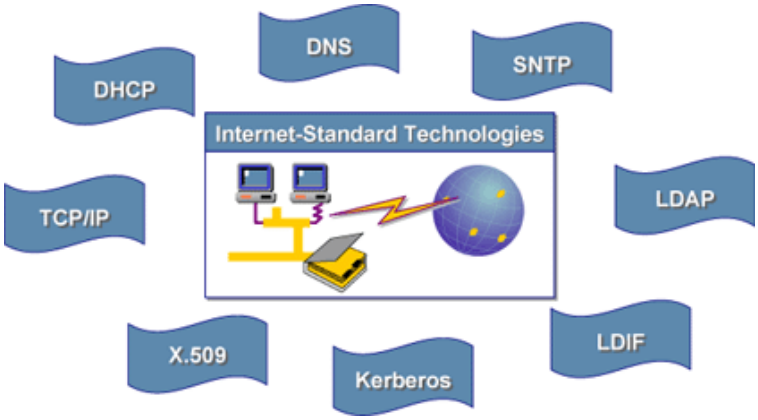


Domini Windows 2000: Active Directory

Active Directory è il Directory Services di Microsoft Windows 2000. Il Directory Service è un **servizio di rete** che ha lo scopo di gestire tutte le informazioni inerenti le risorse di rete per renderle accessibili agli utenti ed alle applicazioni; permette di identificare, descrivere, localizzare, accedere, gestire e rendere sicure tali risorse. Dunque Active Directory fornisce le funzionalità per **organizzare, gestire e controllare in maniera centralizzata l'accesso alle risorse di rete**, in maniera trasparente rispetto alla topologia di rete ed al protocollo utilizzato. Tramite Active Directory è possibile memorizzare ed organizzare un numero praticamente illimitato di oggetti.

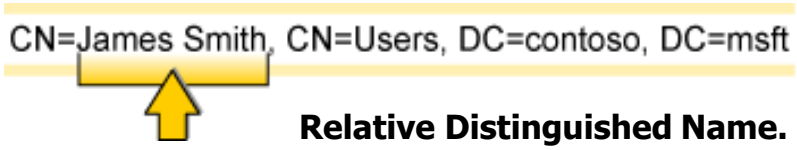
Tecnologie Supportate

I protocolli e le tecnologie più importanti su cui Active Directory si basa: **D**ynamic **H**ost **C**onfiguration **P**rotocol (**DHCP**): gestione centralizzata ed automatica dei parametri di indirizzamento IP; **DNS** dynamic update protocol: creazione dinamica dei record A e PTR in una zona DNS; **S**imple **N**etwork **T**ime **P**rotocol (**SNTP**): per la sincronizzazione dell'ora;**L**ightweight **D**irectory **A**ccess **P**rotocol (**LDAP**): protocollo per l'accesso client al directory service; **Kerberos V5**: protocollo di autenticazione; **X.509** v3 : standard per l'utilizzo di certificati digitali per la cifratura e la firma digitale; **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol (**TCP/IP**)



Spazio dei nomi

- Per localizzare una risorsa, sia l'utente che le applicazioni, devono conoscerne o alcune proprietà o il nome, per cui è fondamentale conoscere la convenzione che è alla base dello spazio dei nomi di Active Directory.
- Active Directory supporta diverse convenzioni dei nomi, per cui è possibile utilizzare quella che si ritiene più conveniente.
  - **Distinguished Name.** Ogni oggetto in Active Directory ha un suo "Distinguished Name" che indica il dominio in cui l'oggetto è localizzato oltre che il path completo all'interno del dominio. Ad esempio, il Distinguished Name "CN=James Smith,CN=Users,DC=contoso,DC=msft" identifica l'oggetto "James Smith" contenuti nel contenitore "Users" contenuto nel dominio "contoso.msft". In tale sintassi le abbreviazioni più utilizzate sono CN="Common Name", OU="Organizational Unit", DC="Domain Component".



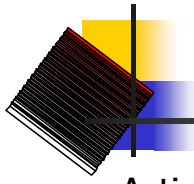
Relative Distinguished Name. E' un sottoinsieme del Distinguished Name che identifica un oggetto una volta che si sia focalizzata l'attenzione su un certo livello della gerarchia.

Spazio dei nomi

- **User Principal Name.** Lo "user principal name (UPN)" di un oggetto utente è composto dal "logon name" e dal dominio in cui tale logon name risiede. Può essere utilizzato per effettuare il logon. Ad esempio , l'utente "James Smith" nel dominio "contoso.msft" ha come UPN "JamesS@contoso.msft".

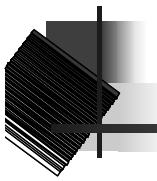
JamesS@contoso.msft

- **Globally Unique Identifier.** Il "**g**lobally **u**nique **id**entifier (GUID)" è una stringa di 128 caratteri esadecimali che Windows 2000 assegna all'oggetto all'atto della creazione. Per garantirne l'unicità l'algoritmo di creazione si basa su informazioni relative al momento della creazione (data e ora) cui vengono naggiunte informazioni di tipo casuale. Il GUID non cambia se cambia il Distinguished Name. Il GUID è unico per definizione.



Active Directory e DNS

- Active Directory utilizza il DNS per garantire principalmente tre funzionalità:
  - **Risoluzione dei Nomi.** DNS fornisce ad Active Directory il servizio che permette di associare ad un nome il corrispondente indirizzo IP.
  - **Definizione dello Spazio dei Nomi.** I domini Microsoft Windows 2000 vengono denominati utilizzando la convenzione dei nomi su cui si basa il DNS. Dunque un nome di dominio Windows 2000 è un nome DNS. Ad esempio "azienda.com" è sia un nome di dominio DNS valido che un nome di dominio Windows 2000 valido.
  - **Localizzazione delle Componenti di Active Directory.** Per effettuare il logon sulla rete e/o eseguire ricerche in Active Directory, una macchina basata su Microsoft Windows 2000 deve innanzitutto localizzare un controllore di dominio (per il processo di autenticazione) e/o un server "global catalog" (per eseguire la ricerca). Per quanto detto ai due punti precedenti il server contiene nel proprio database tutte le informazioni necessarie ad individuare quali macchine svolgano, sulla rete, il ruolo di controllore di dominio o global catalog.

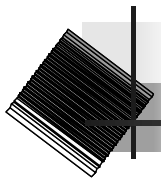


Struttura di Active Directory

Corso di Amministrazione di Reti
A.A. 2002/2003

Materiale preparato utilizzando dove possibile materiale AIPA
http://www.aipa.it/attivita[2/formazione[6/corsi[2/materiali/Reti%20di%20Calcolatori/welcome.htm

Giorgio Calarco - DEIS



Argomenti

- Domini e Unità Organizzative
- Alberi e Foreste
- Schema
- Trust Relationships

Domini

Iniziamo ad analizzare la struttura logica di Active Directory partendo da quello che è l'elemento di base:

il **Dominio:** un insieme di computer, comunicanti tra loro e che condividono un directory database comune

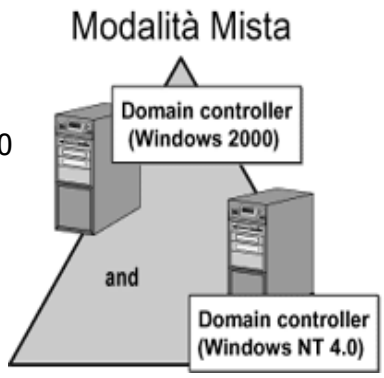
Un dominio può essere visto come:

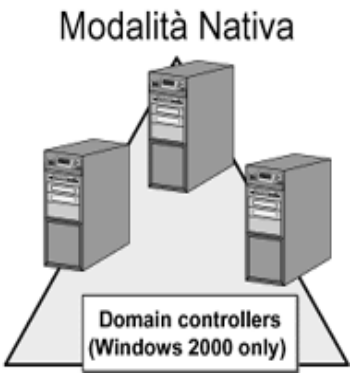
Contesto di Sicurezza. In una rete basata su Microsoft Windows 2000, un dominio costituisce un contesto di sicurezza separato. L'amministratore di un dominio ha tutti i permessi e diritti necessari per svolgere qualsiasi attività all'interno del proprio dominio, ma non ha nessun permesso né nessun diritto in altri domini a meno che non gli vengano esplicitamente garantiti. Ogni dominio ha le proprie politiche di sicurezza (ad esempio, controllo sulla composizione delle password e sul tempo di vita degli account utente).

Domini

Unità di Replica. I Domini sono anche Unità di Replica. Tutti i Controllori di Dominio hanno una copia completa delle informazioni di directory del proprio dominio e replicano tra loro le modifiche.Il modello di replica è di tipo "Multi-Master": tutti i controllori di dominio hanno accesso in lettura scrittura alla copia delle informazioni di directory in loro possesso, replicano le modifiche a tali informazioni agli altri controllori di dominio e ricevono le modifiche apportate dagli altri.

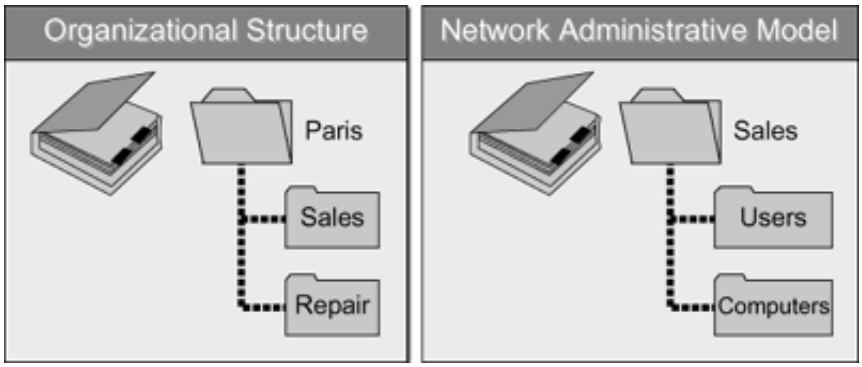
Al momento dell'installazione, il dominio ed Active Directory vengono eseguiti in "**Modalità Mista**" cioè permettono la presenza di controllori di dominio basati sia su Windows 2000 che su Windows NT 4.0. In tale modalità non è possibile usufruire di tutte le funzionalità di Windows 2000.





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 Organizzativa" 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 e comunque tale struttura è trasparente 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 su specifici oggetti contenuti in una "Unità Organizzativa" o su un sottoinsieme dei loro attributi.
- 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.

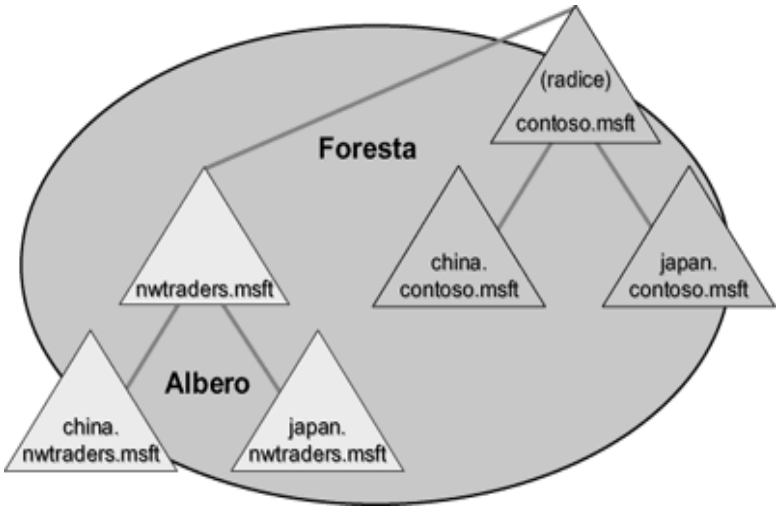
Alberi e Foreste

- 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.

Ad 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 multi-domain 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.

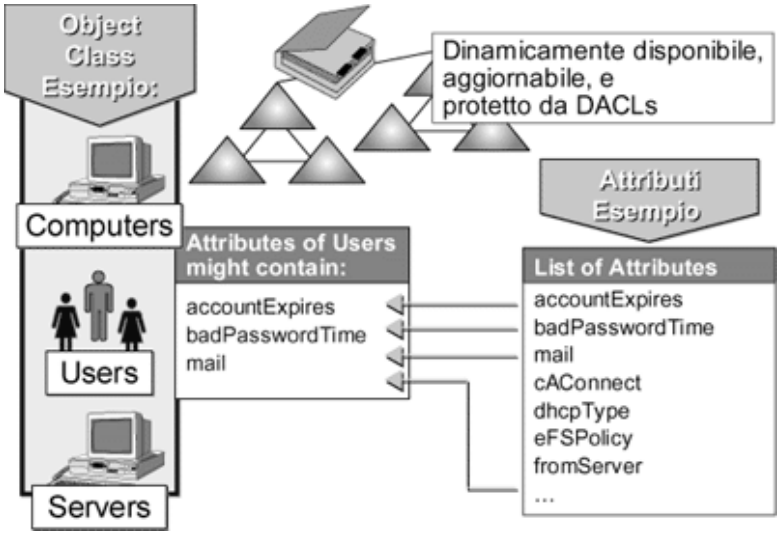
Schema

- In una Foresta, indipendentemente dal numero di Domini ed Alberi da cui è formata, tutti i domini condividono le informazioni di configurazione:
  - Catalogo Globale
  - Schema
- Lo "**Schema**" di Active Directory è una struttura che contiene le definizioni di tutti gli oggetti (utenti, computer, gruppi….) che è possibile creare in Active Directory, e può contenere due tipi di definizioni: le "Classi" e gli "Attributi".

Schema

Le 'Classi' (Object Classes) descrivono i possibili oggetti che possono essere creati. Ogni classe è un insieme di 'Attributi' che vengono definiti separatamente dalla Classe. Dunque ogni Attributo viene definito una sola volta e può essere utilizzato in più Classi. Ad esempio l'attributo "Descrizione" viene definito una sola volta ma poi può essere utilizzato in più Classi.

E' possibile individuare oggetti in Active Directory effettuando la ricerca basandosi sul valore di un certo Attributo.



Schema

- Per quanto detto, in Active Directory, esiste **un solo Schema comune** a tutta la Foresta e questo ci garantisce che tutti gli oggetti creati sottostanno alle stesse regole. Le modifiche fatte allo Schema vengono replicate tra tutti I Controllori di Dominio della Foresta indipendentemente dal dominio di appartenenza.

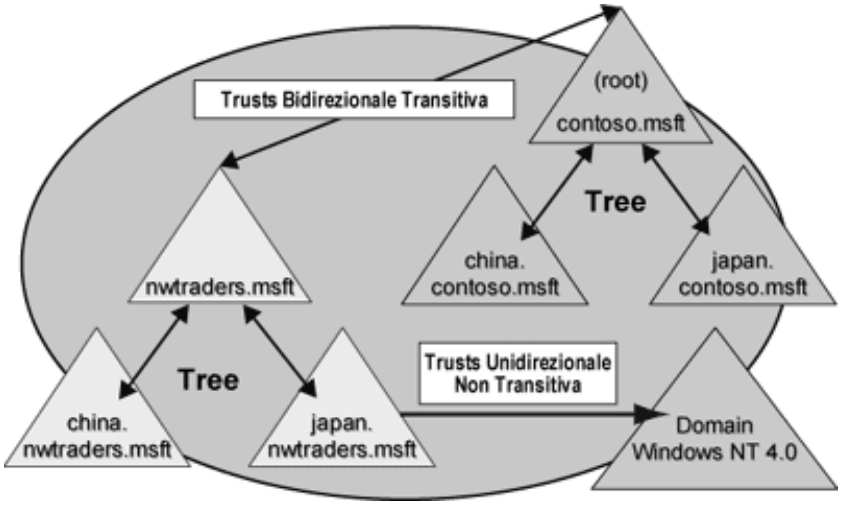
- Lo schema è contenuto nel database di Active Directory, il che permette di:
  - Renderlo dinamicamente disponibile alle applicazioni
  - Renderlo dinamicamente aggiornabile
  - E' possibile assegnare permessi che definiscono con esattezza chi può modificarne il contenuto

Lo Schema è come un oggetto di Active Directory, il cui Distinguished Name è "CN=schema, CN=configuration, DC=domain_name, DC=domain_root".

Fisicamente il database di Active Directory è contenuto in "systemroot\Ntds\Ntds.dit", dove "systemroot" è la cartella di sistema (ad esempio, C:\WINNT). Oltre allo Schema, contiene tutte le altre informazioni relative ad Active Directory.

Trust Relationship

- "Trust Relationship" (relazioni di fiducia): 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, transitivo".



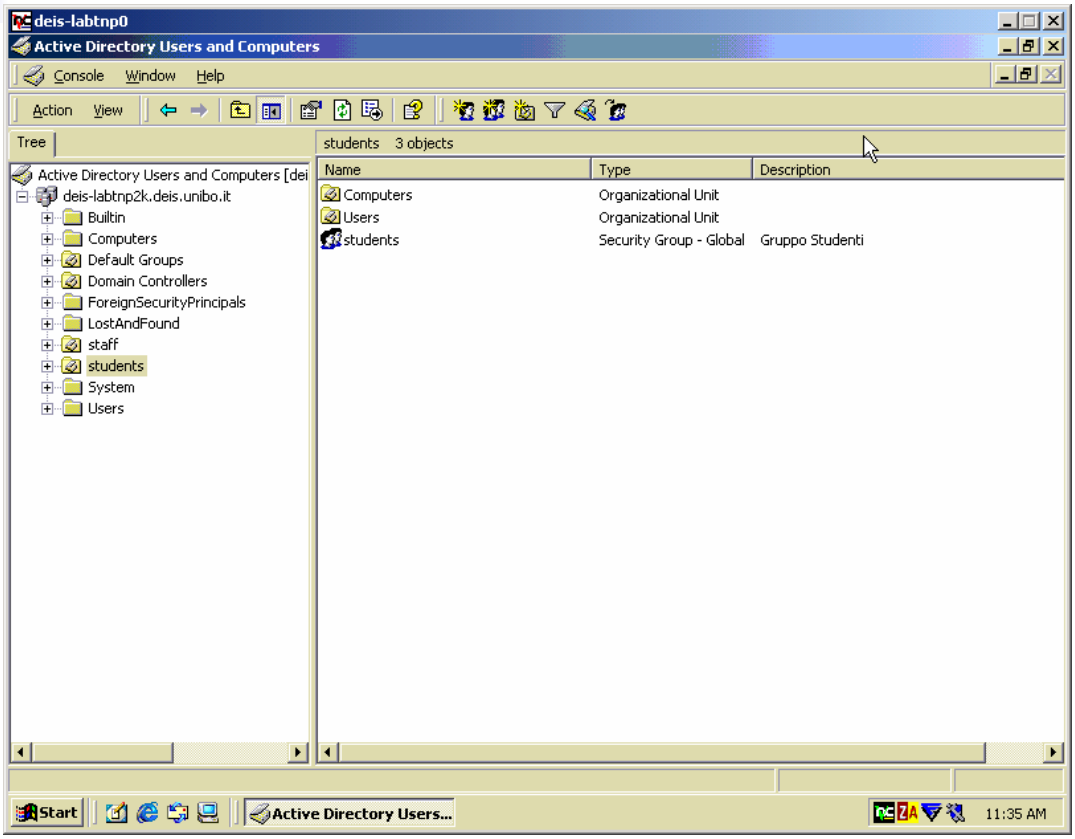
Trust Relationship

- **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.

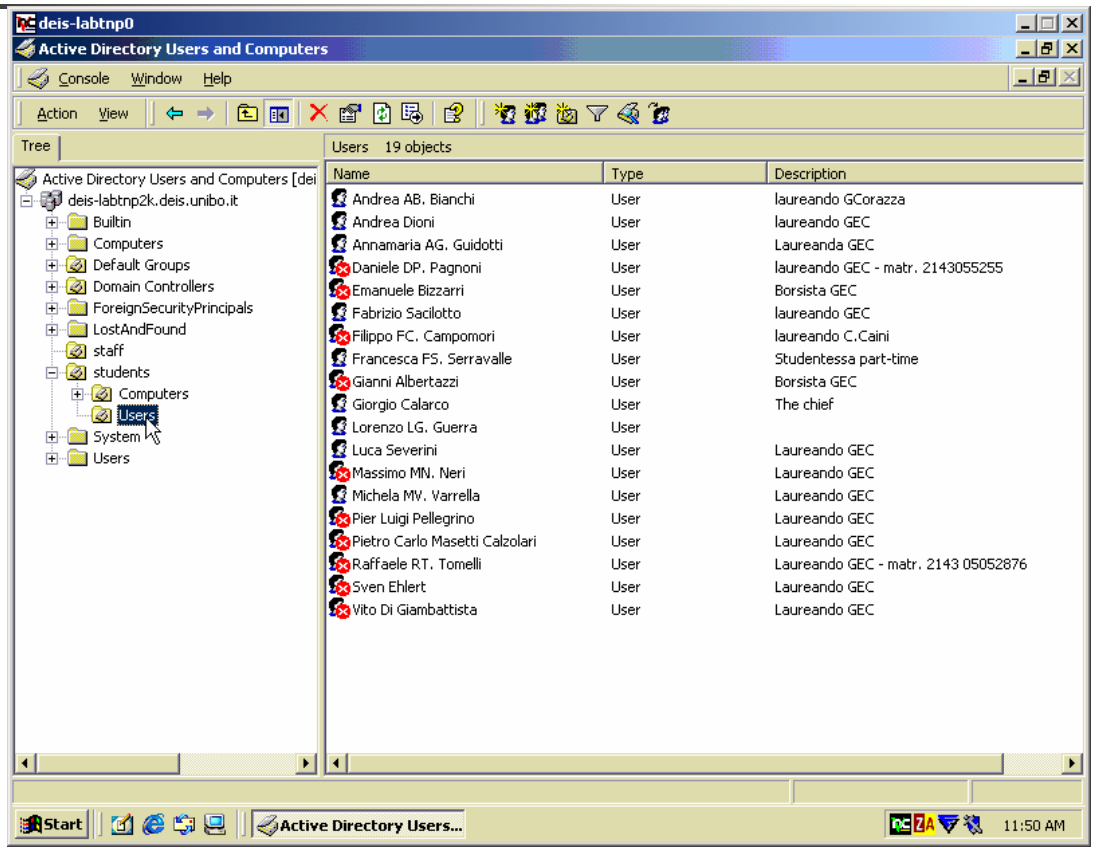
Active Directory – alcuni esempi

Corso di Amministrazione di Reti
A.A.2002/2003

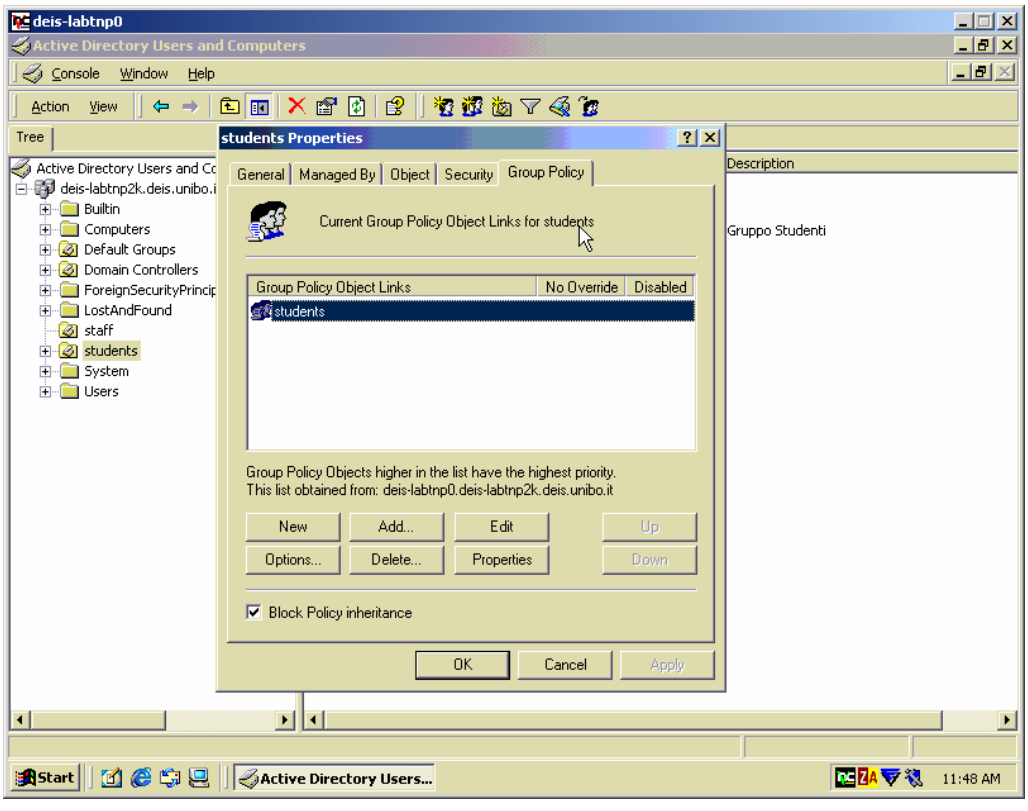
Sul Domain Controller: Active Directory Users & Computers per creare/muovere/cancellare le OU



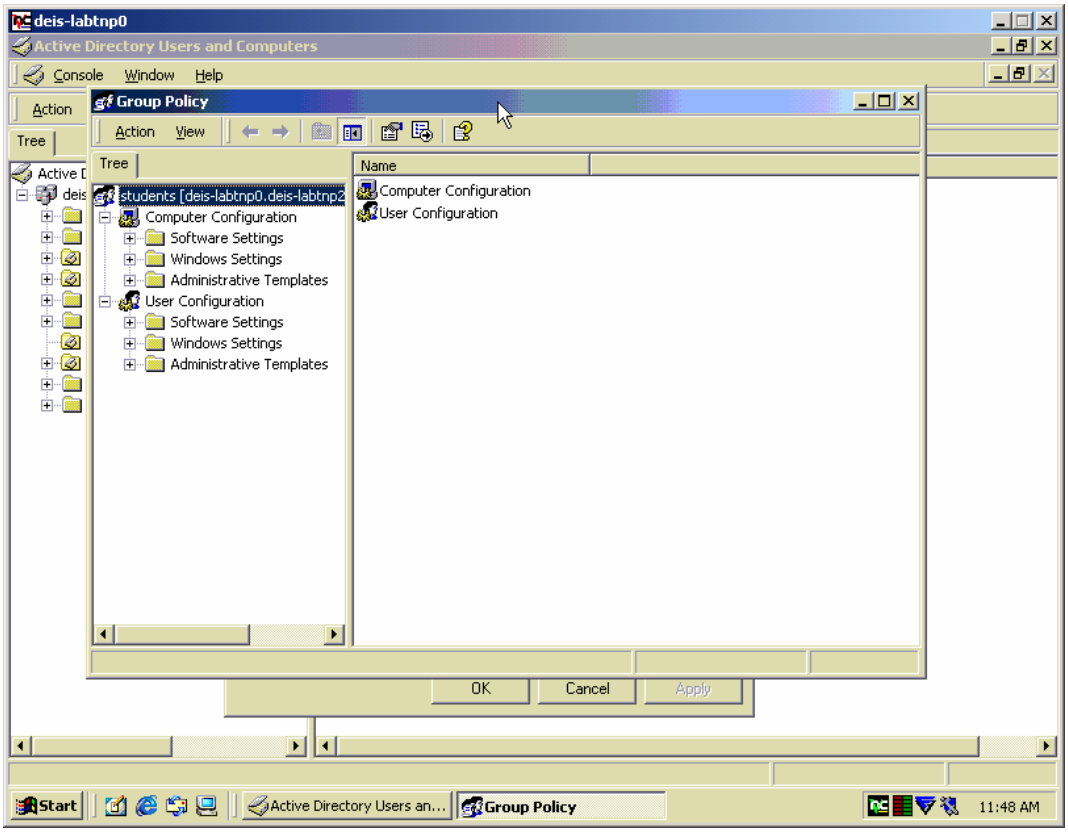
Visualizzo gli oggetti e le OU contenute all'interno di una OU



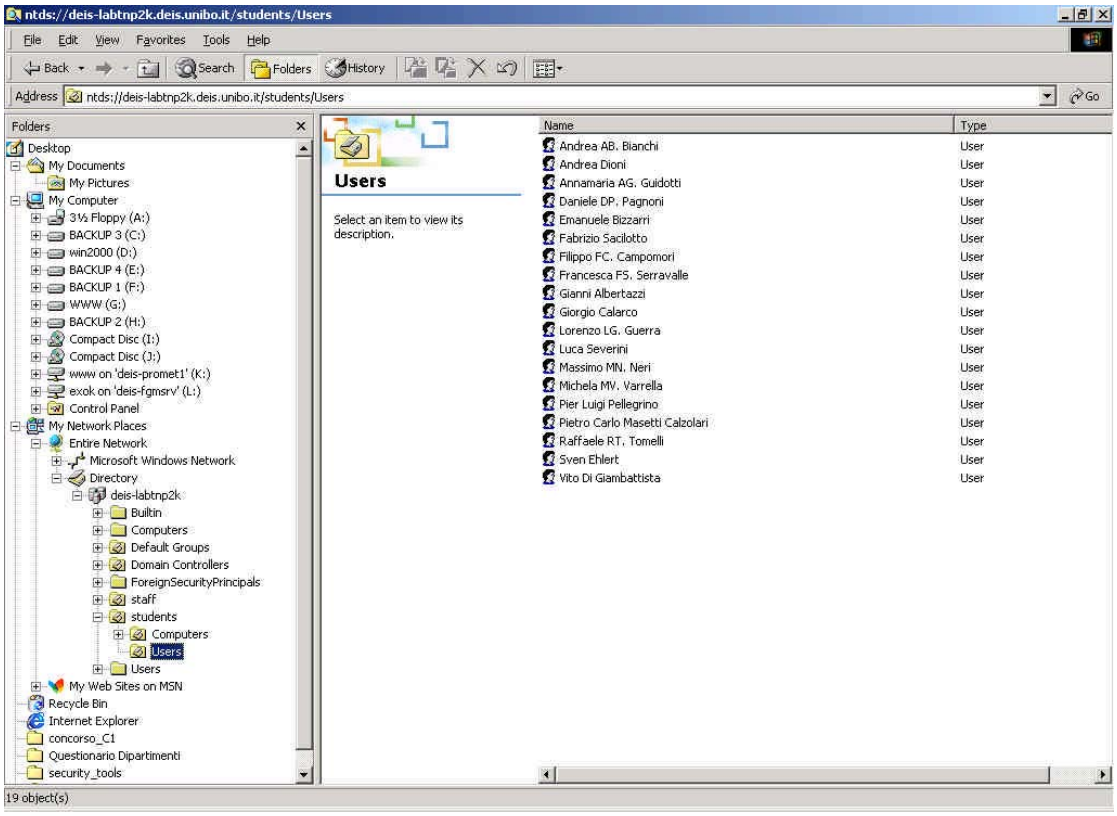
Seleziono una OU e ne visualizzo le proprietà, ad es. le Policy



Posso fare modifiche: seleziono Edit e visualizzo le Group Policy



Dai client del Dominio: posso visualizzare il contenuto dell'AD



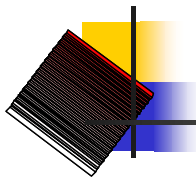
ACL

Corso di Amministrazione di Reti
A.A.2002/2003

Giorgio Calarco - DEIS

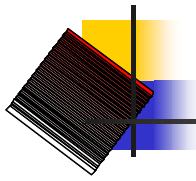
Argomenti

- Generalità NTFS
- Implementare la sicurezza di NTFS
- Implementare la condivisione di risorse
- Permessi locali e permessi sulle condivisioni NTFS
- Solaris: comandi “setfacl” e “getfacl”



File system supportati da Windows NT

- File system FAT 16
  - Supporta i nomi di file lunghi
  - NON prevede alcuna protezione locale, ogni utente può accedere a tutti i files e directories
  - Dimensione massima partizioni/file: 2.047 MByte
- File system NTFS
  - Supporta i nomi di file lunghi
  - Supporta la protezione locale
  - Dimensione massima partizioni:
    - 16 esabyte (teorici)
    - 2 terabyte (effettivi)



Implementare la sicurezza di NTFS

- Settare Directory o File Permissions
- Auditing

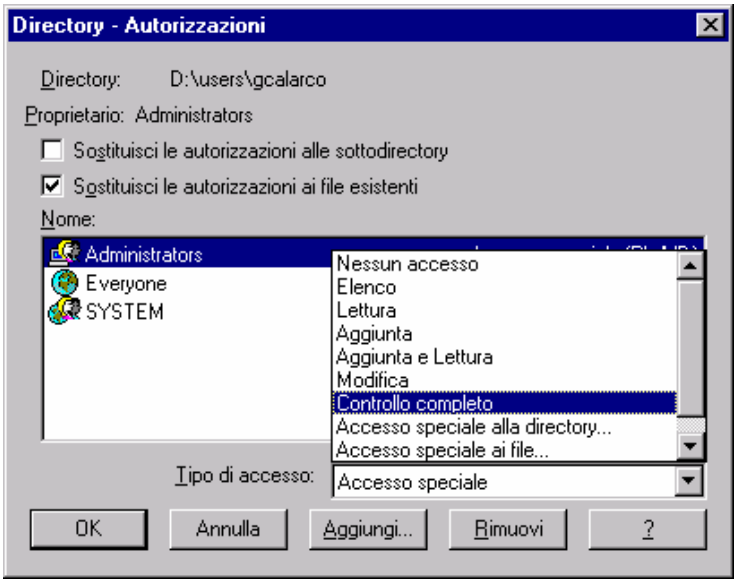
Sicurezza NTFS: requisiti

- Disponibile solo su partizioni NTFS
- Settare le Permissions richiede:
  - 'Full Control'
  - 'Change Permissions'
  - 'Ownership'

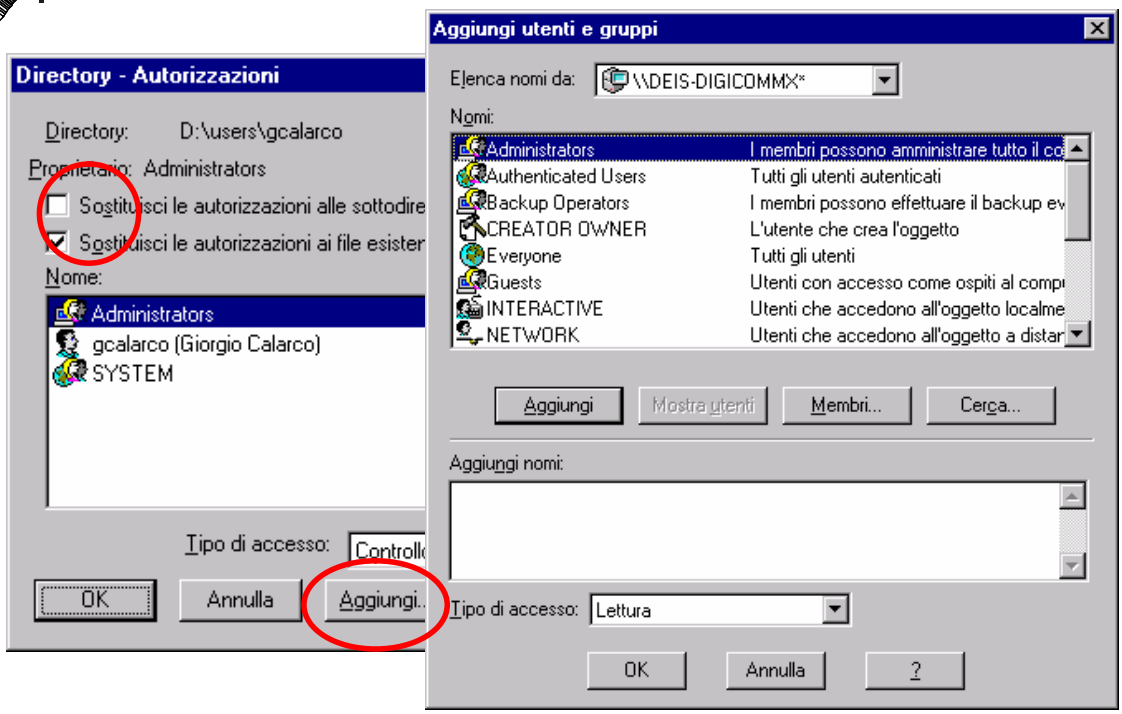
Autorizzazioni di accesso alle cartelle

- Sulle cartelle è possibile impostare le seguenti **autorizzazioni standard**:
  - Nessun accesso (Nessuno)(Nessuno)
  - Elenco (RX)(Non specificato)
  - Lettura (RX)(RX)
  - Aggiunta (WX)(Non specificato)
  - Aggiunta e Lettura (RWX)(RX)
  - Modifica (RWXD)(RWXD)
  - Controllo completo (Tutti)(Tutti)
- Le autorizzazioni sono **cumulative**, ad eccezione dell'autorizzazione 'No Access' che ha la precedenza su tutte le altre. Se ad esempio un utente è membro di un gruppo a cui è stata concessa l'autorizzazione Lettura e di un gruppo a cui è stata concessa l'autorizzazione Modifica, l'utente disporrà dell'autorizzazione Modifica.
- **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.

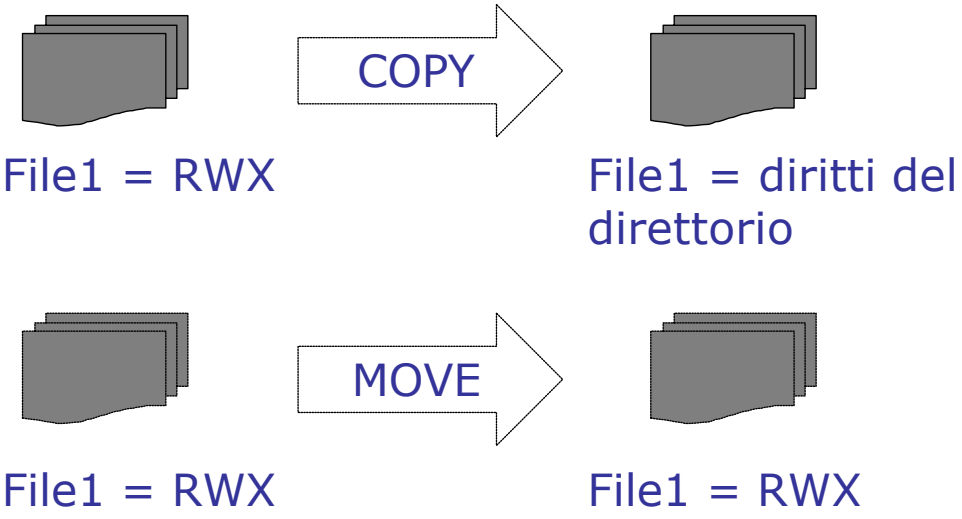
Settare i permessi di cartelle



Assegnazione di autorizzazioni



Permessi dopo un copy/move di file (e directory)



Autorizzazioni di accesso ai files

- Sui file è possibile impostare le seguenti **autorizzazioni standard**:
  - Nessun accesso (Nessuno)
  - Lettura (RX)
  - Modifica (RWXD)
  - Controllo completo (Tutti)

- 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.
- Le autorizzazioni sono **cumulative**, ad eccezione dell'autorizzazione 'Nessun accesso' che ha la precedenza su tutte le altre. Se ad esempio un utente è membro di un gruppo a cui è stata concessa l'autorizzazione Lettura e di un gruppo a cui è stata concessa l'autorizzazione Modifica, l'utente disporrà dell'autorizzazione Modifica.

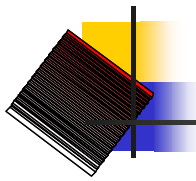
Autorizzazioni di accesso ai files

- Quando si imposta un'autorizzazione standard, accanto a questa viene visualizzato un insieme di **autorizzazioni individuali**. Quando ad esempio per un file viene impostata l'autorizzazione Lettura, verrà visualizzata la sigla (RX), indicante le autorizzazioni Lettura e Esecuzione sul file.
- **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.

Interazione permessi utente e gruppi

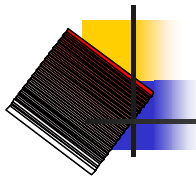
Permessi di Michael	Permessi di Research	Permessi di Development	Permessi di Michael (effettivi)
Read	Read	-	Read
Write	-	Read	Read & Write
-	Change	Read	Change
Take Ownership	Read	Change	Take Ownership & Change
No Access	Read	Change	No Access
Change	No Access	Change	No Access

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



Ownership di files e directories

- 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 bene:
  - Gli utenti che creano un file o una directory ne detengono l' Ownership



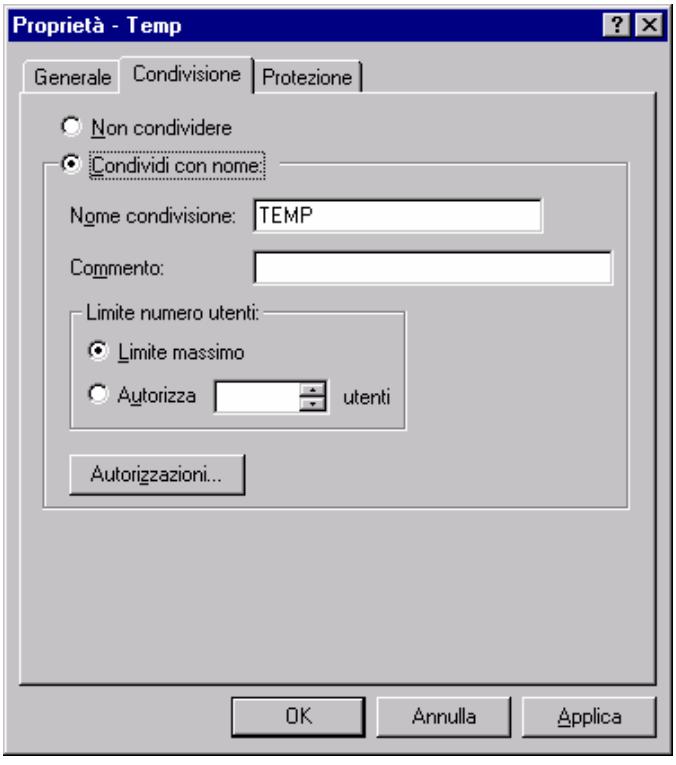
Assegnazione di autorizzazioni NTFS

- Autorizzazioni NTFS predefinite:
  - A 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)

Condivisione di risorse

- Share = directory (folder) condivisa
- Diritti necessari per attivare le condivisioni:
  - 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 un direttorio

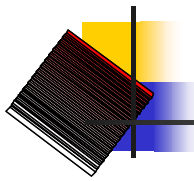


Permessi di una share

Permessi locali vs. Permessi sulla condivisione

	Permessi Assegnati	Permessi di Michael
Permessi Share C:\temp	Everyone: Read Michael: Change	**Change** (RWXD)
Permessi locali	Everyone: Read Michael: Read	**Read** (RX)
Permessi effettivi		**Read** (RX)

L'autorizzazione effettiva è quella più restrittiva !

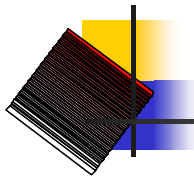


Setfacl

- Modifica l'Access Control List (ACL)

  Sintassi: setfacl -s acl_entries file
- acl_entries sono ACL separate da virgole
- Affinché l'ACL venga effettivamente applicata occorre essere l'owner del file

- Es.: setfacl –s user:www:rwx,user::rwx,group::r-x,mask:rwx,other:r-x download/
- Attenzione a mask: filtra i diritti di user aggiuntivo e group. Se user:www:rw- e mask:r-- -> l'effetto è che www:r--
- Più comoda l'opzione –m, che aggiunge l'acl ai diritti preesistenti. Es. setfacl –m user:www:rwx foo



Getfacl

- Sintassi: getfacl file
- Esempio: getfacl download/

```
# file: download/
# owner: help
# group: suexec
user::rwx
user:www:rwx            #effective:rwx
group::r-x              #effective:r-x
mask:rwx
other:r-x
```