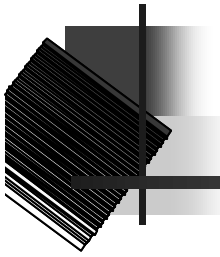
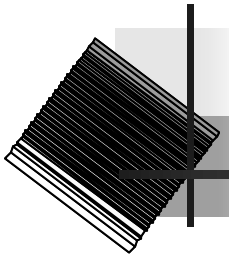


Struttura di Active Directory

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

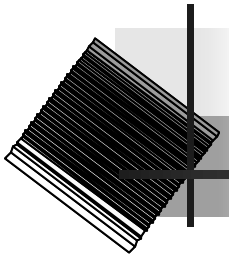
Materiale preparato utilizzando dove possibile materiale AIPA
http://www.aipa.it/attivita[2/formazione[6/corsi[2/materiali/Reti%20di%20Calcolatori/welcome.htm

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

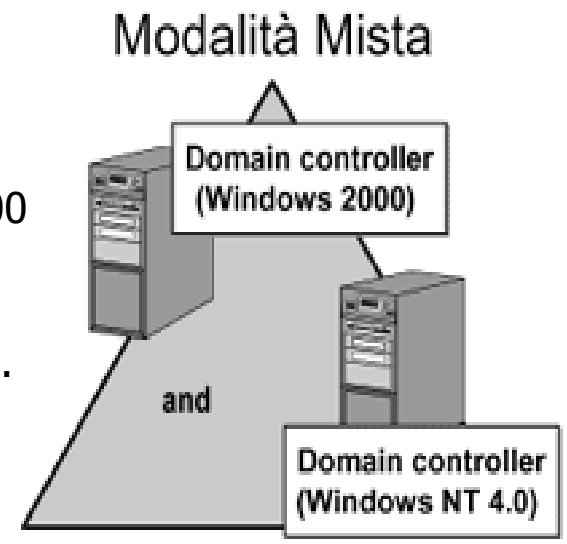
Un dominio può essere visto come:

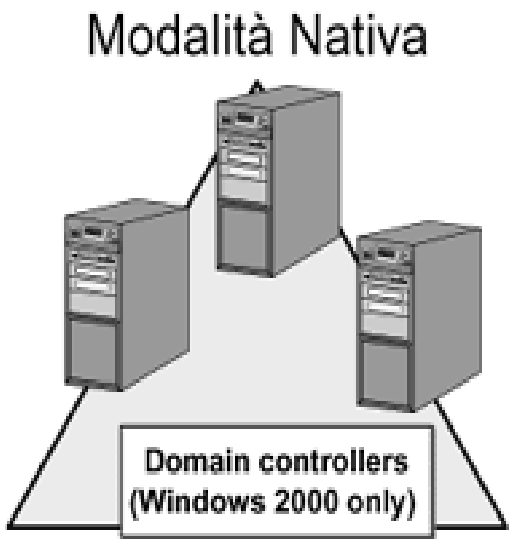
Contesto di Sicurezza. In una rete basata su Microsoft Windows 2000, un dominio costituisce un contesto di sicurezza separato. L'amministratore di un dominio ha tutti i permessi e diritti necessari per svolgere qualsiasi attività all'interno del proprio dominio, ma non ha nessun permesso né nessun diritto 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.

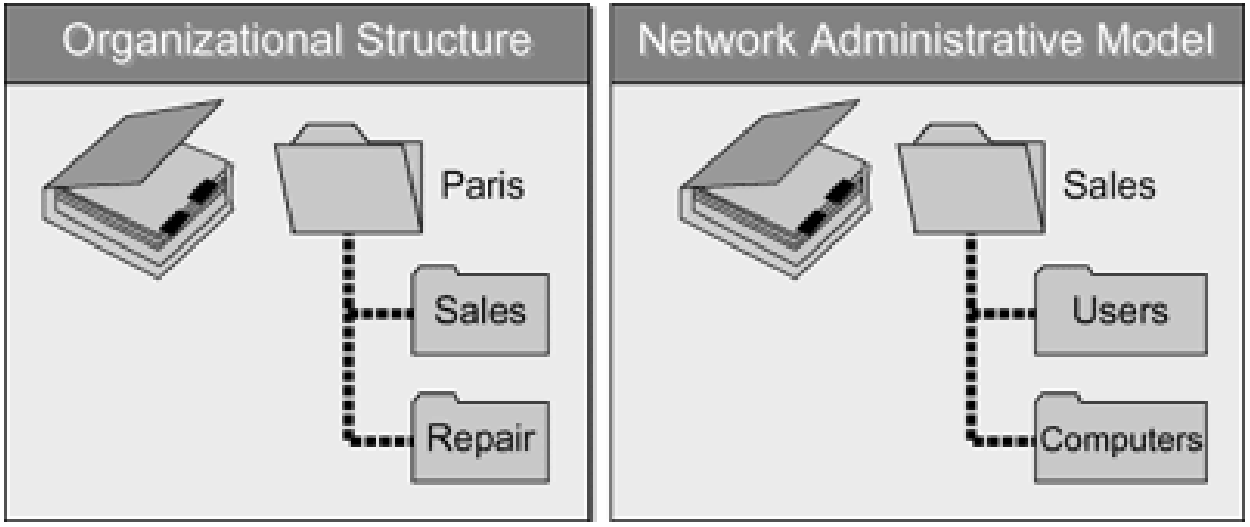
Al momento dell'installazione, il dominio ed Active Directory vengono eseguiti in "**Modalità Mista**" cioè permettono la presenza di controllori di dominio basati sia su Windows 2000 che su Windows NT 4.0. In tale modalità non è possibile usufruire di tutte le funzionalità di Windows 2000.



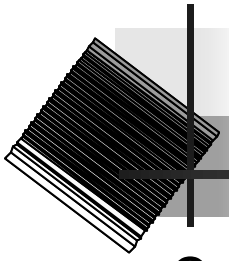


Unità Organizzative

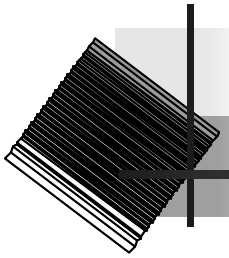
- Una "Unità Organizzativa" (OU – **Organizational Unit**) è un contenitore che ha lo scopo di organizzare oggetti (account utente, account di gruppo, computers, stampanti…) di Active Directory all'interno di un dominio.
- Utilizzando le "Unità Organizzativa" è possibile raggruppare oggetti di Active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



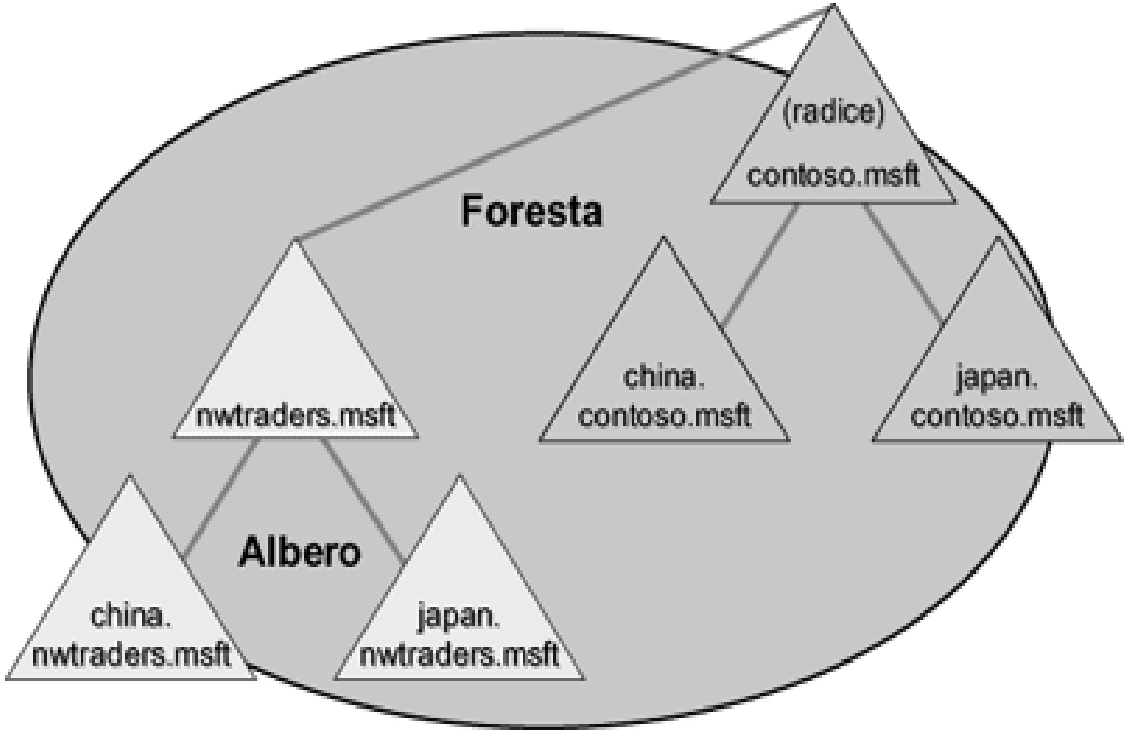
Alberi e Foreste

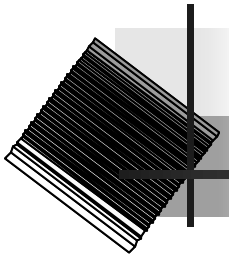
- Nonostante l'utilizzo delle "Unità Organizzative", anche in Windows 2000 esiste una numerosa serie di situazioni in cui definiamo comunque degli ambienti multi dominio. Ad esempio:
  - Avere ambiti di sicurezza separati
  - Avere politiche di controllo delle password e di sicurezza diverse
  - Avere 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.



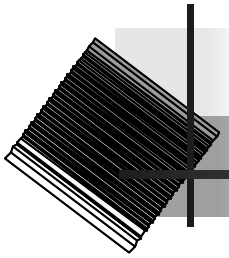


Alberi e Foreste

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.



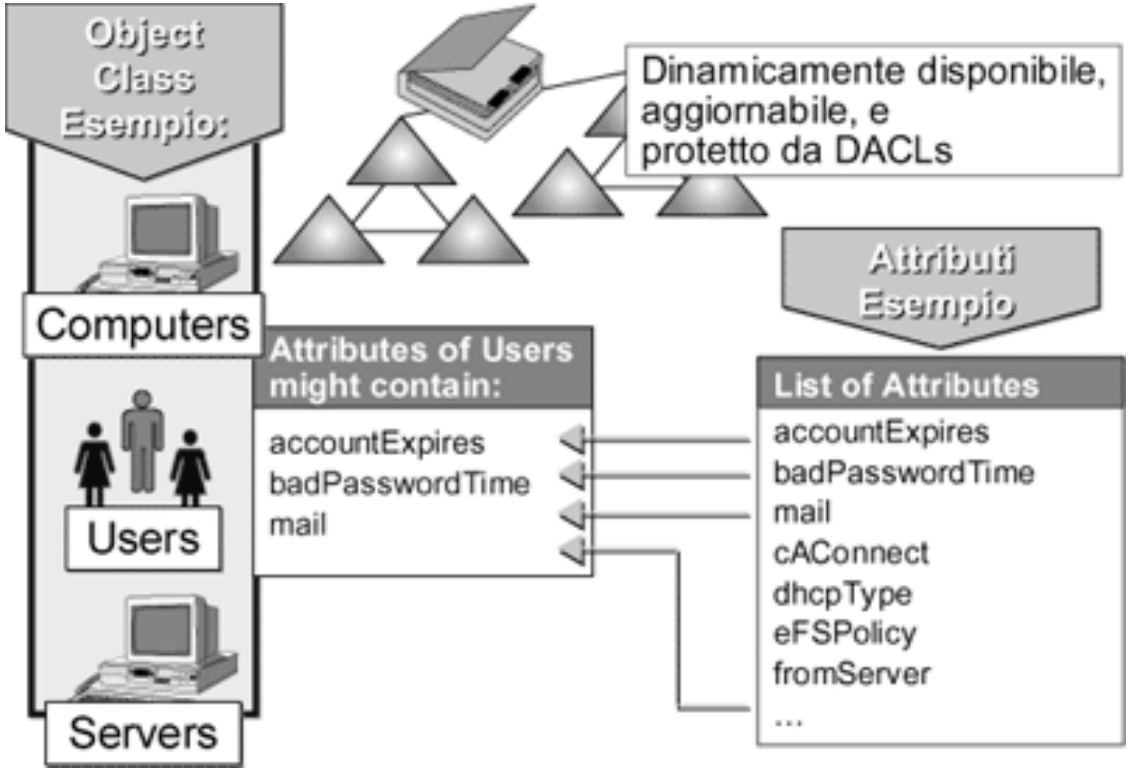
Schema

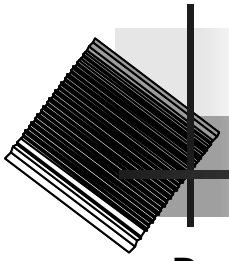
- In una Foresta, indipendentemente dal numero di Domini ed Alberi da cui è formata, tutti i domini condividono le informazioni di configurazione:
  - Catalogo Globale
  - Schema
- Lo "**Schema**" di Active Directory è una struttura che contiene le definizioni di tutti gli oggetti (utenti, computer, 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.

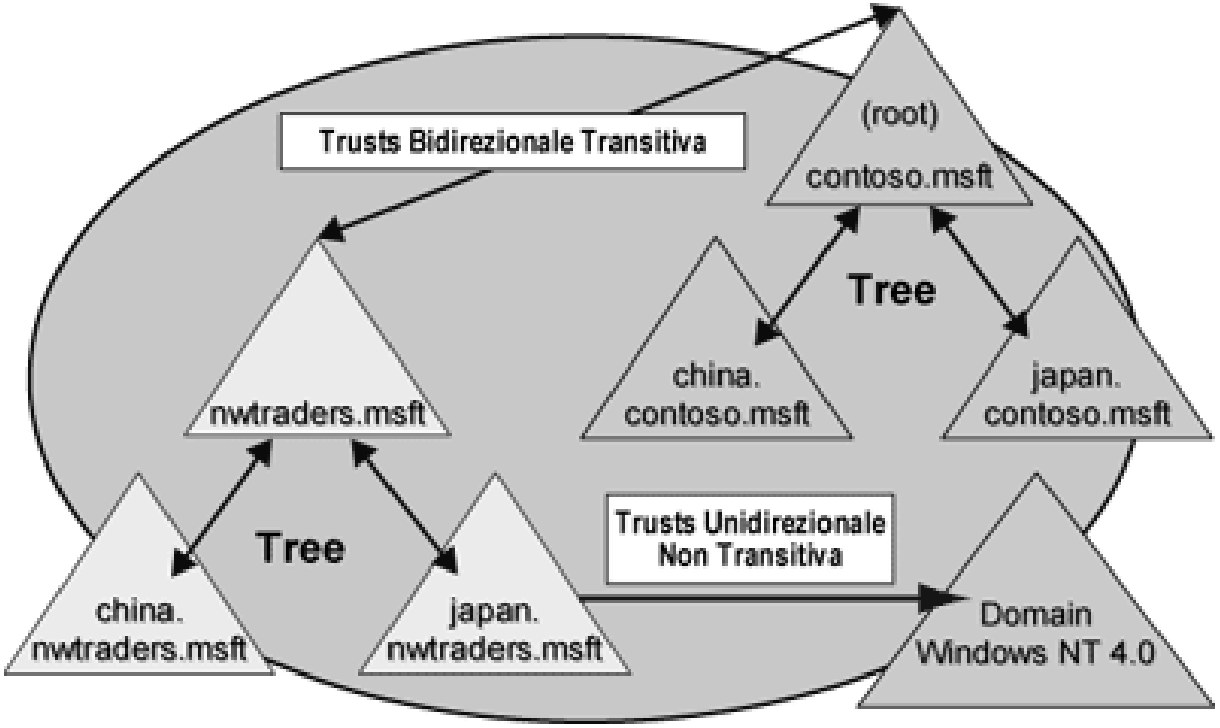
- Lo schema è contenuto nel database di Active Directory, il che permette di:
  - Renderlo dinamicamente disponibile alle applicazioni
  - Renderlo dinamicamente aggiornabile
  - E' possibile assegnare permessi che definiscono con esattezza chi può modificarne il contenuto

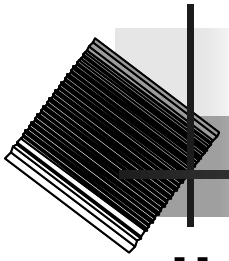
Lo Schema è come un oggetto di Active Directory, il cui Distinguished Name è "CN=schema, CN=configuration, DC=domain_name, DC=domain_root".

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.