Elementi di base dei sistemi Microsoft

Preparato con il contributo di Giorgio Calarco e del materiale AIPA
(http://www.aipa.it/attivita[2/formazione[6/corsi[2/materiali/Reti%20di%20Calcolatori/welcome.htm)

Le generazioni dei sistemi operativi Microsoft

Pre-rete

DOS, Windows fino a 3.10 (1980-1992 / fine supporto 2001)

→ soluzioni di comunicazione realizzate ad-hoc e prive di integrazione con il sistema operativo

Basate su workgroup

Windows 3.11 for Workgroups, Windows 95/98/ME (1993-2000 / fine supporto 2006)

*Windows NT fino a 3.51 - Windows XP Home (1993-2001 / fine supporto 2001-**2014**)*

→ protocolli di comunicazione proprietari ma integrati nativamente

nessun supporto alla distribuzione di credenziali utente

Basate su domini

*Windows NT 4.0 - XP Professional (1996-2001 / fine supporto 2004-**2014**)*

→ centralizzazione di informazioni utili per la gestione e la mobilità degli utenti

Basate su directory

Windows 2000 Server / Server 2003 / Server 2008 / Server 2012

Windows Vista / 7 / 8 (2000-oggi)

→ evoluzione delle funzioni di gestione dei domini e delle informazioni centralizzate

→ possibilità di costruire reti multi-dominio

Le generazioni dei sistemi server Microsoft

Riassumiamo le principali innovazioni introdotte con le diverse generazioni:

Server 2000 *(2000-2010)* → Active Directory, NTFS3, DFS

Server 2003 *(2003-2015)* → 64 bit, embrione di command line

Server 2008 *(2008-2020)* → Server Core, Roles, Clustering, Hyper-V, Windows Server Resource Manager, Self-Healing NTFS

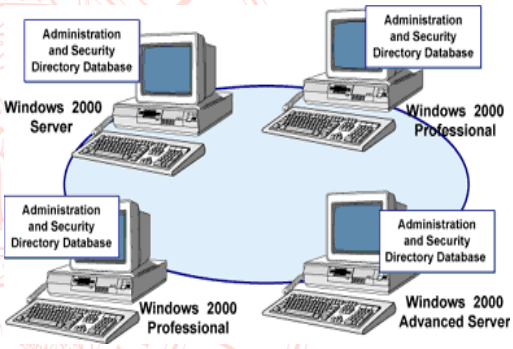
Server 2012 *(2012-2023)* → Core/GUI commutabile senza reinstallare, Core il default suggerito, IP address manager, ReFS

Modelli di licenza

- In funzione della licenza acquistata, possono essere interamente disattivate alcune feature, e/o limitato il loro utilizzo
- Con riferimento alla versione 2012:
  - *Foundation*: 1 CPU, 32GB RAM, 15 utenti, 50 conn., no HyperV
    - la licenza è "per server"
  - *Essentials*: 2 CPU, 64GB RAM, 25 utenti, 50/250 conn., no HyperV
    - la licenza è "per server"
  - *Standard*: 64CPU, 4TB RAM, max 2 VM
    - la licenza è "per coppia di CPU + per numero di client"
  - *Datacenter*: 64CPU, 4TB RAM, VM illimitate
    - la licenza è "per coppia di CPU + per numero di client"

Workgroup

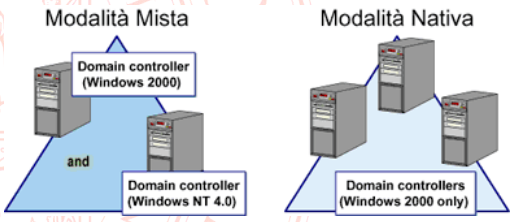
Un workgroup è chiamato anche rete **Peer-to-Peer** (paritetica) per evidenziare quella che è la sua caratteristica saliente: tutti i computer che appartengono ad un workgroup sono "uguali", senza che ci sia un server dedicato alla gestione della sicurezza. Ogni computer gestisce **un proprio security 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 20xx. 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

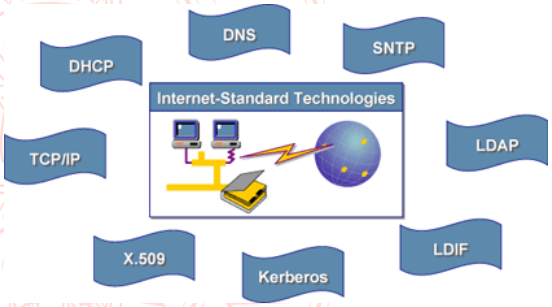
- Il modello di distribuzione dei dati in NT era di tipo MONOMASTER
  - PDC = Primary Domain Controller (RW)
  - BDC = Backup Domain Controller (RO)
  - Rielezione PDC in caso di gasto
- Dall'avvento di Active Directory il modello è diventato MULTIMASTER
  - Tutti i DC sono paritetici
  - Sincronizzazione 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*

Domini Windows 20xx: Active Directory

Active Directory è il Directory Service introdotto da Microsoft con 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.

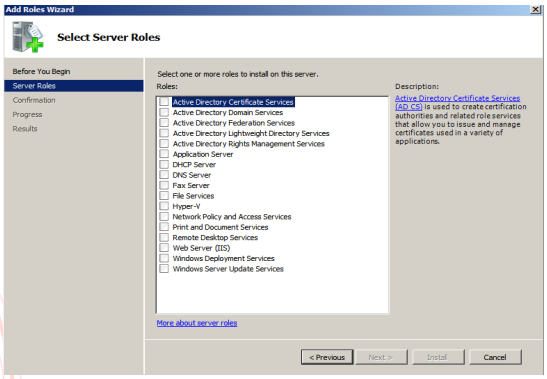
Tecnologie Supportate

I protocolli e le tecnologie più importanti su cui Active Directory si basa: Dynamic Host Configuration Protocol (**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; Simple Network Time Protocol (**SNTP**): per la sincronizzazione dell'ora;Lightweight Directory Access Protocol (**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; Transmission Control Protocol/Internet Protocol (**TCP/IP**)



Server Roles

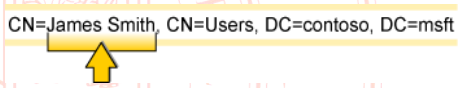
- I servizi di base di AD sono implementati attivando *ruoli* per il server



- Gestione dei ruoli in Windows Server 2008
  - http://technet.microsoft.com/en-us/library/dd283014(v=ws.10).aspx
- Gestione di Windows Server 2012
  - http://technet.microsoft.com/en-us/windowsserver/hh534429

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".

Globally Unique Identifier. Il "globally unique identifier (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 20xx è un nome DNS. Ad esempio "azienda.com" è sia un nome di dominio DNS valido che un nome di dominio Windows 20xx 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 20xx 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

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:

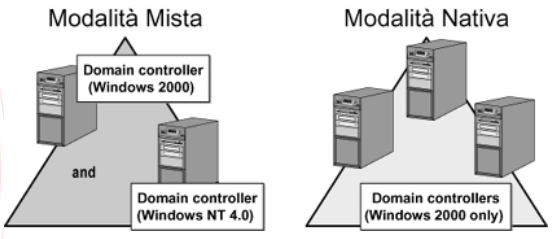
Parte dello spazio DNS. I nomi e l'organizzazione dei domini corrispondono allo spazio di nomi DNS assegnato all'utilizzatore.

Contesto di Sicurezza. In una rete basata su Windows 20xx, 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 (cont.)

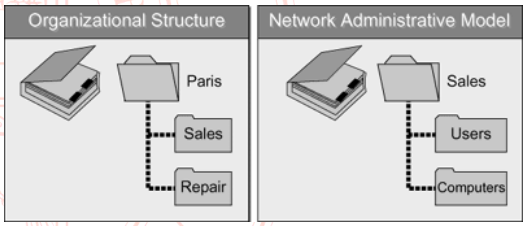
Unità di Replica. I Domini sono anche Unità di Replica. Tutti i Controllori di Dominio hanno una copia completa delle informazioni di directory del proprio dominio e replicano tra loro le modifiche.Il modello di replica è di tipo "Multi-Master“: tutti i controllori di dominio hanno accesso in lettura 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 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

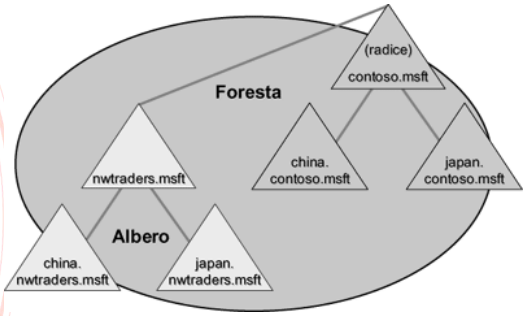
Nonostante l'utilizzo delle "Unità Organizzative", anche in Windows 2000 esiste una numerosa serie di situazioni in cui definiamo comunque degli ambienti multi dominio. Ad esempio:

- 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.

Schema e Global Catalog

In una Foresta, indipendentemente dal numero di Domini ed Alberi da cui è formata, tutti i domini condividono le informazioni di configurazione:

- Catalogo Globale (o Global Catalog, **GC**)
- Schema

Il GC è un “sottoinsieme trasversale” dell'intera AD utilizzato per ottimizzare le ricerche degli oggetti:

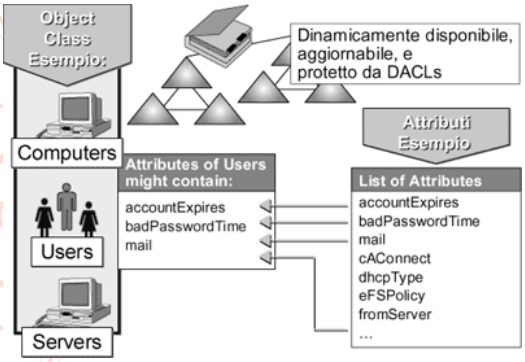
- contiene **poche informazioni essenziali** su **tutti** gli oggetti di AD
- è collocato su un sottoinsieme dei DC
- è derivato dal database principale, ed è in sola lettura

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

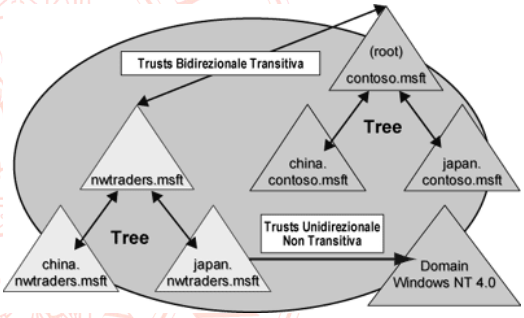
Lo Schema è come un oggetto di Active Directory, il cui Distinguished Name è "CN=schema, CN=configuration, DC=domain_name, DC=domain_root".

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): 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, 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.