# Active Directory

# Domini Windows

Un dominio Windows è un insieme di computer logicamente collegati e “gestiti” da uno o più domain controller.

Un domain controller è un computer in cui è installato una versione di Windows Server e su cui sono attivati i servizi di Active Directory.

Active Directory è una directory in cui sono registrati gli oggetti che compongono il dominio, a partire dai computer e dagli utenti.

La directory è memorizzata nel Domain Controller.

# Gestione centralizzata

L’infrastruttura di Active Directory consente la gestione centralizzata degli utenti e della sicurezza:

- single sign on
- gestione delle politiche di sicurezza per l’intera organizzazione, assegnando permessi a:
  - utenti (quali risorse possono essere utilizzate)
  - computer (quali computer possono accedere al dominio, limitazioni al s/w utilizzabile o alle risorse accessibili,...)
  - gruppi
  - unità organizzative

# Active directory

La struttura della directory si chiama “schema”, definisce i tipi di oggetti che si possono registrare e i campi associati a ciascun oggetto.

Lo schema è estensibile.

Gli oggetti di base sono:

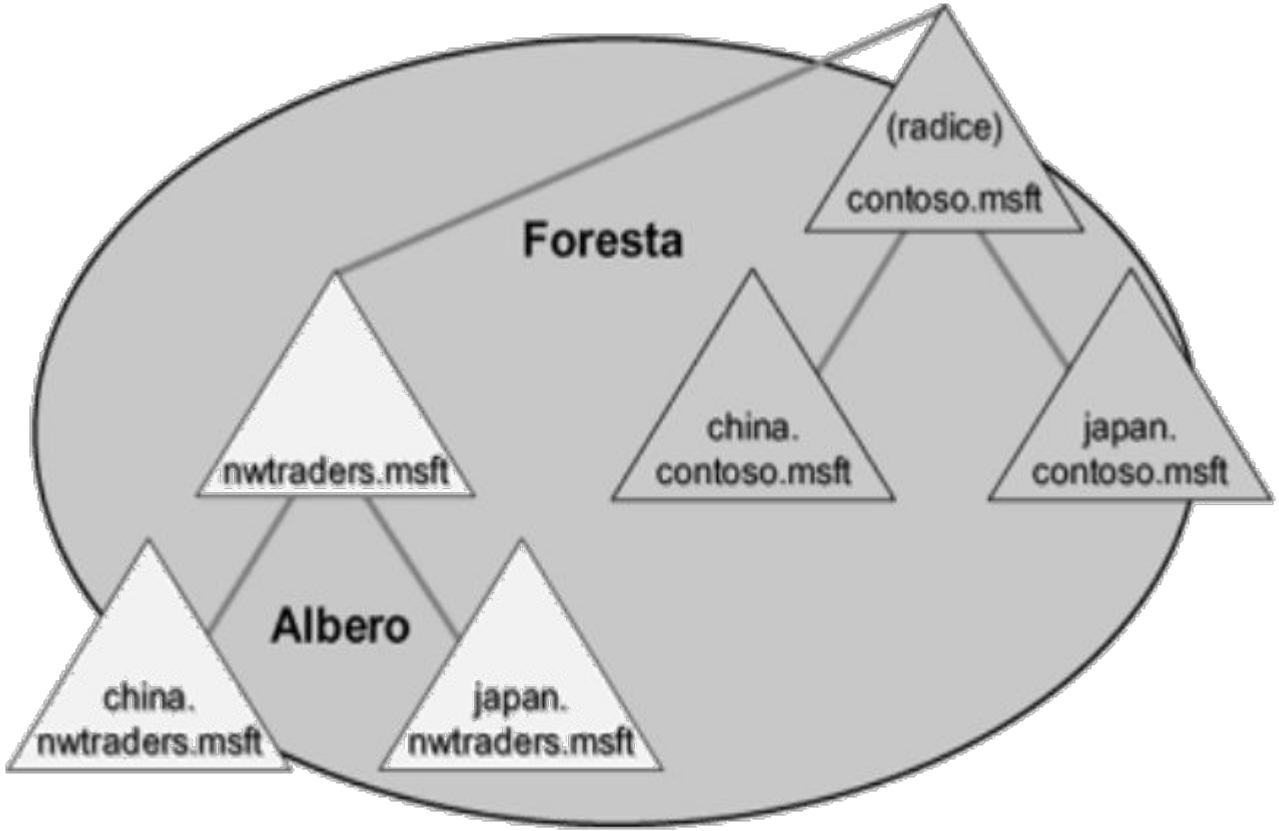
- user account;
- computer account.

# Gruppi e unità organizzative

I gruppi sono oggetti di active directory che si utilizzano per impostazioni di sicurezza, impostando policy di accesso comuni a gruppi di utenti o computer.

Ad esempio, tutti gli utenti del gruppo “marketing” hanno accesso a una determinata condivisione sul server.

Le unità organizzative (strutturate ad albero) si impostano per esigenze amministrative e consentono ad esempio di delegare ad un utente la gestione, eventualmente parziale, dell’unità organizzativa.


(radice)
contoso.msft
Foresta
nwtraders.msft
china.
contoso.msft
japan.
contoso.msft
Albero
china.
nwtraders.msft
japan.
nwtraders.msft

# Alberi

Al dominio principale possono essere aggiunti dei sottodomini, a formare un albero.

I sottodomini ereditano lo schema del dominio “padre”, che potranno successivamente modificare.

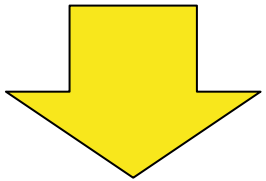
Tra dominio principale e sottodomini si determina la “two ways implicit transitive trust”, per cui un utente di un qualsiasi dominio dell’albero può accedere a tutti gli altri.

# Foreste

Una foresta è formata da due o più alberi collegati in cui però un’eventuale relazione di “fiducia” deve essere stabilita esplicitamente (explicit one way trust).

# Repliche

Il domain controller ha il controllo centralizzato dell'intera rete (utenti, computer,...) ed è opportuno evitare di avere un "single point of failure".



È opportuno che ogni dominio abbia un cluster (fault tolerance, load balancing) di domain controller.

La strategia di replica specifica la modalità con cui i dati vengono copiati tra i diversi domain controller.

# Sites

I siti consentono di distribuire geograficamente le repliche dei domain controller.

In questo modo ogni computer del dominio ha un controller nella propria LAN.

Le repliche appartenenti allo stesso sito sono in cluster, hanno collegamenti veloci e possono di fatto avere esattamente la stessa versione della directory.

La strategia di replica tra controllori in siti diversi specifica ogni quanto tempo va effettuato la sincronizzazione della directory.

I collegamenti tra siti si chiamano site link, mentre i site link bridgeheads sono collegamenti ridondanti che consentono di evitare single point of failure nella sincronizzazione.

# Roaming profile

Con questa impostazione, il profilo dell'utente è salvato in una condivisione in rete e quindi l'utente lo ritroverà su ogni computer del dominio.

1. creare sul server (o su un qualsiasi file server del dominio) una cartella in cui verranno poi creati i profili utente (es, PROFILES). Il permesso di share deve essere read+write per Everybody
2. in gestione dell'utente, scheda "profile" modificare la directory del profilo a:

   *\\server\PROFILES\%username%*

# Permessi

I permessi determinano come gli utenti possono interagire con le risorse del dominio. Sono assegnati dal proprietario della risorsa.

Nella gestione di un dominio complesso, è opportuno assegnare i permessi ai gruppi di utenti e non ai singoli utenti.

Se un utente appartiene a più di un gruppo:

- i permessi “assegnati” si sommano;
- anche i permessi “negati” si sommano, e in caso di conflitto hanno prevalenza su quelli “assegnati”.

# Group policy objects

Si applicano alle Unità Organizzative e possono essere utilizzati per la gestione della sicurezza.

Tramite i GPO è possibile:

- abilitare/disabilitare applicazioni;
- impostare la connessione automatica a risorse condivise;
- impostare l'esecuzione automatica di script/progrmmi;
- ....

per tutti gli utenti di una OU.