Ermanno Goletto
*Microsoft MVP Alumni - MCSA – MCITP – MCTS - MCP*


# Active Directory - Security groups deep dive

## Introduzione

Come descritto in Active Directory security groups | Microsoft Learn **Active Directory prevede due entità di sicurezza**: **gli Account Utente e gli Account Computer** che rappresentano rispettivamente una persona o un computer. Gli account utente possono poi anche essere utilizzati come account di servizio dedicato per alcune applicazioni.

**Active Directory prevede poi due tipi di gruppi**: i **Gruppi di sicurezza** usati per assegnare le autorizzazioni alle risorse condivise e i **Gruppi di distribuzione** utilizzati per creare liste di distribuzione di posta elettronica..

## Argomenti

## Gruppi di sicurezza e gruppi di distribuzione

Nei sistemi operativi Windows vi sono diversi account e gruppi di sicurezza built-in preconfigurati con appropriati diritto ed autorizzazioni che permettono l'esecuzione di attività specifiche.

In Active Directory il modello amministrativo è stato progettato per suddividere le attività amministrative in due tipologie di amministratori:

- **Service administrators**: responsabili della manutenzione e distribuzione di Active Directory Domain Services (AD DS), inclusa la gestione dei controller di dominio e la configurazione di AD DS.
- **Data administrators**: responsabili della gestione dei dati archiviati in Active Directory e nei server e nelle workstation membri del dominio.

**Active Directory prevede due tipi di gruppi**: i **Gruppi di sicurezza** usati per assegnare le autorizzazioni alle risorse condivise e i **Gruppi di distribuzione** utilizzati per creare liste di distribuzione di posta elettronica.
I gruppi di sicurezza nello specifico possono essere utilizzati per eseguire le seguenti attività:

- **Assegnare diritti utente** ai gruppi di sicurezza in Active Directory **per determinare quali attività possono eseguire i membri di tale gruppo nell'ambito di un dominio o di una foresta**. I diritti utente vengono assegnati automaticamente ad alcuni gruppi di sicurezza quando viene installata Active Directory, a riguardo si veda Default Active Directory security groups. Ad esempio, un utente aggiunto al gruppo Backup Operators in Active Directory può eseguire il backup e il ripristino di file e directory che si trovano in ogni controller di dominio nel dominio. E' possibile utilizzare le Group Policies per assegnare diritti utente ai gruppi di sicurezza in modo da delegare attività specifiche, a riguardo si veda User Rights Assignment.

- **Assegnare autorizzazioni** ai gruppi di sicurezza per le risorse. **Le autorizzazioni, che si differenziano dai diritti utente, vengono assegnate a un gruppo di sicurezza per una risorsa condivisa e determinano chi può accedere alla risorsa e a quale livello di accesso** (ad esempio Controllo completo o Lettura). Alcune autorizzazioni che sono impostate su oggetti di dominio sono assegnate automaticamente per consentire vari livelli di accesso ai gruppi di sicurezza predefiniti (ad esempio il gruppo Account Operators o il gruppo Domain Admins). I gruppi di sicurezza sono elencati in Discretionary Access Control Lists (DACLs) che definiscono le autorizzazioni per risorse e oggetti e **gli amministratori quando assegnano autorizzazioni per risorse come condivisioni file o stampanti, dovrebbero assegnare tali autorizzazioni ad un gruppo di sicurezza anziché a singoli utenti**. In questo modo le autorizzazioni vengono assegnate una sola volta al gruppo anziché più volte a ogni singolo utente.

Per quanto riguarda i gruppi di distribuzione è possibile utilizzarli solo per inviare messaggi di posta elettronica a elenchi di utenti tramite un'applicazione di posta elettronica (ad esempio Exchange Server). **I gruppi di distribuzione non sono abilitati per la sicurezza**, quindi non è possibile includerli in DACLs (Discretionary Access Control List).
Viceversa **è possibile usare un gruppo di sicurezza come entità di posta elettronica** e l'invio di un messaggio di posta elettronica a un gruppo di sicurezza invia il messaggio a tutti i membri del gruppo esattamente come accade per i gruppi di distribuzione.

**I gruppi di sicurezza sono quindi un modo per raccogliere account utente, account computer e altri gruppi in unità gestibili**.

## Ambito dei gruppi di Active Directory

**Ogni gruppo ha un ambito che identifica come il gruppo viene applicato nel dominio o nella foresta Active Directory**, sono disponibili i **tre ambiti di gruppo** seguenti:

- **Domain Local**
- **Global**
- **Universal**

Per la precisione oltre a questi tre ambiti esiste anche l'ambito Builtin Local, ma quest'ambito è destinato ai soli i gruppi predefiniti presenti nel contenitore Builtin, su tali gruppi predefiniti non è possibile modificare né lo scope, nè il tipo di gruppo.

**I gruppi di sicurezza, in base al proprio ambito, posso concedere permessi nel dominio, nella foresta o in domini esterni trusted** come descritto nello schema seguente:

| Ambito | Può concedere permessi nello stesso dominio | Può concedere permessi in un altro dominio nella stessa foresta | Può concedere permessi in un dominio esterno trusted |
|---|---|---|---|
| **Domain Local** | **Sì** | **No** | **No** |
| **Global** | **Sì** | **Sì** | **Sì** |
| **Universal** | **Sì** | **Sì** | **Sì** |

I **membri ammessi da ciascun gruppo suddivisi per ambito** sono elencati nello schema seguente:

| Ambito | Membri dello stesso dominio | Membri da un altro dominio nella stessa foresta | Membri da un dominio esterno trusted |
|---|---|---|---|
| **Domain Local** | • Account<br>• Gruppi Global<br>• Gruppi Universal<br>• Gruppi Domain Local | • Account<br>• Gruppi Global<br>• Gruppi Universal | • Account<br>• Gruppi Global<br>• Gruppi Universal |
| **Global** | • Account<br>• Gruppi Global | **Non ammessi** | **Non ammessi** |
| **Universal** | • Account<br>• Gruppi Global<br>• Gruppi Universal | • Account<br>• Gruppi Global<br>• Gruppi Universal | **Non ammessi** |

Le **appartenenze dei gruppi suddivisi per ambito** sono elencate nello schema seguente:

| Ambito | Membro di nello stesso dominio | Membro di in un altro dominio nella stessa foresta | Membro di in un dominio esterno trusted |
|---|---|---|---|
| **Domain Local** | • Gruppi locali su computer (esclusi i gruppi Built-In con identificatori di sicurezza noti (SID)<br>• Gruppi Domain Local | **Non ammesso** | **Non ammesso** |
| **Global** | • Gruppi Domain Local<br>• Gruppi Global<br>• Gruppi Universal | • Gruppi Domain Local<br>• Gruppi Universal | • Gruppi Domain Local |
| **Universal** | • Gruppi locali su computer<br>• Gruppi Domain Local<br>• Gruppi Universal | • Gruppi locali su computer<br>• Gruppi Domain Local<br>• Gruppi Universal | • Gruppi locali su computer<br>• Gruppi Domain Local |

Le **conversioni ammesse dei gruppi suddivisi per ambito** sono elencate nello schema seguente:

| Ambito | Domain Local | Global | Universal |
|---|---|---|---|
| **Domain Local** | - | **No** | **Se il gruppo non contiene Gruppi Domain Local** |
| **Global** | **No** | - | **Se il gruppo non contiene Gruppi Global** |
| **Universal** | **Se il gruppo non contiene Gruppi Universal** | **Se il gruppo non contiene Gruppi Universal** | - |

## Quando utilizzare i gruppi Domain Local

Come riportato in When to use groups with domain local scope **i gruppi Domain Local consentono di definire e gestire l'accesso alle risorse all'interno di un singolo dominio**. Per gestire l'assegnazione dei diritti di accesso a risorse di rete, come ad esempio stampanti o share, è possibile **creare un gruppo Domain Local assegnandogli l'autorizzazione per accedere alla risorsa di rete, inserire gli account utente in un gruppo Global e quindi aggiungere questo gruppo al gruppo Domain Local**. In questo modo gli accessi non saranno definiti sui singoli utenti e quando sarà necessario assegnare a tali utenti accessi ad altre risorse si potrà fare rifermento al gruppo Global semplificando questo tipo di attività amministrative di routine.

**I gruppi Domai Local dovrebbero quindi essere utilizzati per descrivere il livello di assegnazione dei diritti su una risorsa di rete del dominio**, come ad esempio l'accesso in lettura o in scrittura ad una share o i diritti di utilizzare o amministrare una stampante.

## Quando utilizzare i gruppi Global

Come riportato in When to use groups with global scope **i gruppi Global consentono di gestire oggetti Active Directory che richiedono una manutenzione giornaliera** come account computer e account utente. Dal momento che **i gruppi Global non vengono replicati all'esterno del proprio dominio è possibile modificare frequentemente gli account contenuti nel gruppo senza generare traffico di replica verso il Global Catalog**.

Sebbene le assegnazioni di diritti e autorizzazioni su un gruppo Global siano valide solo all'interno del dominio in cui sono assegnate, **utilizzando gruppi Global in modo uniforme uniformemente nei domini è possibile consolidare i riferimenti ad account con scopi simili semplificando e razionalizzando la gestione dei gruppi tra i domini.** P*er meglio comprendere questo concetto si consideri, ad esempio, un'infrastruttura Active Directory costituita da una foresta di due domini denominati Europa e Stati Uniti, se in tale infrastruttura esiste un gruppo Global nel dominio Stati Uniti denominato SG-Accounting e destinato agli utenti della contabilità creare un gruppo Global denominato SG-Accounting anche nel dominio Europa (a meno che la funzione di contabilità non esista in tale dominio) per razionalizzare la gestione dei gruppi nei due domini*.

E' quindi fortemente consigliato l'utilizzo di gruppi Global o Universal invece di gruppi Domain Local quando si specificano autorizzazioni su oggetti di Active Directory replicati nel Global Catalog.

**I gruppi Global dovrebbero quindi essere utilizzati per descrivere i ruoli aziendali o le funzioni lavorative all'interno del dominio**.

## Quando utilizzare i gruppi Universal

Come riportato in When to use groups with universal scope **i gruppi Universal vengono usati per consolidare gruppi che si estendono su più domini**. A tale scopo, aggiungere gli account ai gruppi Global quindi nidificare questi gruppi all'interno di gruppi Universal in questo modo le modifiche all'appartenenza nei gruppi Global non influiscono sui gruppi Universal. *Per meglio comprendere questo concetto si consideri, ad esempio, un'infrastruttura Active Directory costituita da una foresta di due domini denominati Europa e Stati Uniti, se in tale infrastruttura esiste un gruppo Global in ciascun dominio denominato SG-Accounting e destinato agli utenti della contabilità creare un gruppo*

*Universal denominato SU-Accounting che abbia come membri i due gruppi SG-Accounting, Stati Uniti\SG-Accounting ed Europa\SG-Accounting, in questo modo il gruppo SU-Accounting potrà essere utilizzato ovunque nell'infrastruttura Active Directory aziendale ed eventuali modifiche nell'appartenenza dei singoli gruppi SG-Accounting non causeranno la replica del gruppo SU-Accounting.*

**I gruppi Universal dovrebbero quindi essere utilizzati per descrivere i ruoli aziendali o le funzioni lavorative comuni a tutti i dominii della foresta Active Directory**.

I gruppi universali sono anche gli unici indicato per i gruppi di distribuzione in un'infrastruttura con Exchange come indicato in Exchange Server - Recipients - Manage distribution groups:

*«You can create or mail-enable only universal distribution groups. To convert a domain-local or a global group to a universal group, you can use the Set-Group cmdlet using the Exchange Management Shell. You may have mail-enabled groups that were migrated from previous versions of Exchange that are not universal groups. You can use the EAC or the Exchange Management Shell to manage these groups»*

## Conclusioni

**Dal punto di vista della sicurezza utilizzare gruppi Domain Local per concedere permessi a risorse specifiche permette di concedere ai membri di altri domini e foreste l'accesso alla risorsa**, mediante la nidificazione di gruppi Global o Universal, **senza dover concedere accesso diretto al resto del dominio in cui risiede la risorsa**.

Da quanto visto possiamo trarre le seguenti best practices per l'utilizzo degli Active Directory security groups.

**Best Practice 1: Non assegnare le autorizzazioni agli account utente o computer, ma i gruppi di sicurezza** per evitare di assegnare più volte le autorizzazioni, per gestire in modo organizzato le autorizzazioni ed evitare che quando gli utenti cambiano ruolo sia necessario intervenire sui diritti puntuali a loro assegnati col rischio di mantenere diritti di accesso non più necessari.

**Best Practice 2: Semplificare le attività amministrative di assegnazione dei diritti di accesso alle risorse di rete svincolandosi dall'assegnazione dei diritti di accesso agli utenti, utilizzando gruppi nidificati**. In questo modo i diritti di accesso sono assegnati a gruppi che contengono a loro volta gruppi omogenei di utenti, in questo modo si evita che il singolo utente abbia diritti di accesso ad assegnazione diretta difficili e onerosi da gestire e si struttura l'assegnazione l'attività amministrativa di gestione dei diritti.

**Best Practice 3: Utilizzare i gruppi Domain Local per descrivere il livello di assegnazione dei diritti su una risorsa del dominio**.

**Best Practice 4: Utilizzare i gruppi Global per descrivere i ruoli aziendali o le funzioni lavorative all'interno del dominio dal momento che tali gruppi sono soggetti a manutenzione frequente e che i gruppi Global non sono replicati all'esterno del dominio di appartenenza** e di conseguenza le modifiche a tali gruppi a gruppi non causa traffico di replica verso il Global Catalog. Inoltre **l'utilizzo dei gruppi Global consentono di consolidare i riferimenti ad account con scopi simili semplificando e razionalizzando la gestione dei gruppi tra i domini**.

**Best Practice 5: Utilizzare i gruppi Universal quando si ha la necessità di consolidare i ruoli aziendali o le funzioni lavorative che si estendono su più domini.** Utilizzando i gruppi Universal per contenere gruppi Global le modifiche eseguite sui gruppi Global non causeranno traffico di replica verso i Global Catalog dei rispettivi domini. Inoltre i Global Catalog contengono nella cache i gruppi Universal e non i gruppi Global rendendo le ricerche più veloci soprattutto se i domini sono collegati via WAN o VPN.

**Best Practice 6: Se l'infrastruttura Active Directory è una foresta composta da un singolo dominio assegnare i diritti di accesso alle risorse di rete a gruppi Domain Local che conterranno gruppi Global** che a loro volta raggruppano gli utenti che necessitano dell'accesso alla risorsa condivisa con i diritti conferiti al gruppo Domain Local. **Ovvero implementare il role-based access controls** (RBAC) **tramite l'approccio AGDLP** (Account, Global, Domain Local, Permission).

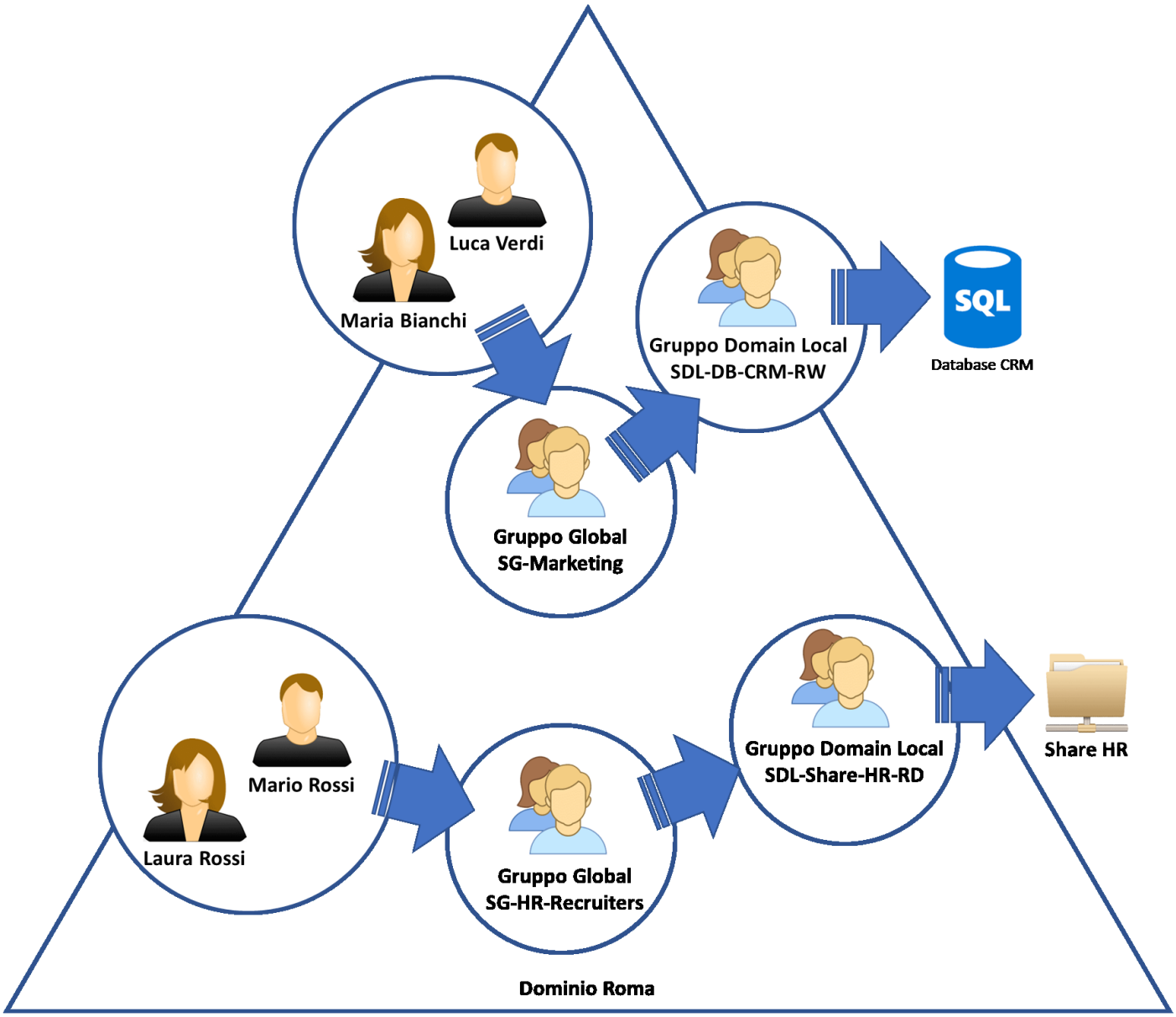


**Figura 1**: *Strategia AGDPL (Account, Global, Domain Local, Permission)*

**Best Practice 7: Se l'infrastruttura Active Directory è una foresta composta da più domini e/o da foreste trusted assegnare i diritti di accesso alle risorse di rete a gruppi Domain Local che conterranno gruppi Universal che consolidano gruppi Global** che a loro volta raggruppano gli utenti che necessitano dell'accesso alla risorsa condivisa con i diritti conferiti al gruppo Domain Local**. Ovvero implementare il role-based access controls (RBAC) tramite l'approccio AGUDLP** (Account, Global, Universal, Domain Local, Permission).

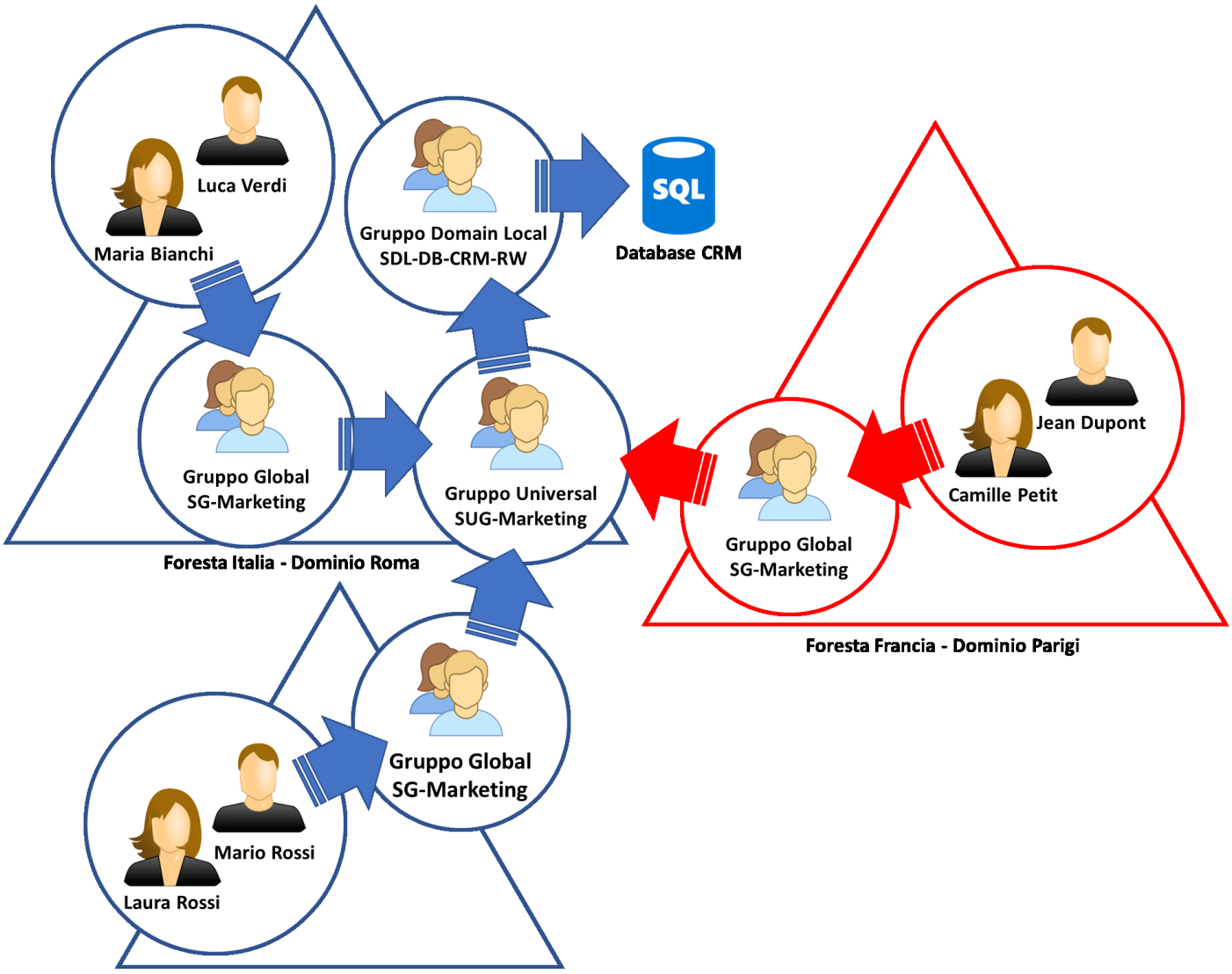


**Figura 2**: *Strategia AGUDPL (Account, Global, Universal, Domain Local, Permission)*

**Best Practice 8: Utilizzare i gruppi Universal per creare gruppi di distribuzione in infrastrutture con Exchange.**

## Riferimenti

- Active Directory security groups | Microsoft Learn
- Windows Server 2003 Product Help - Understanding Active Directory - Group scope