

Windows server – Group Policy



Fin dal rilascio di Windows Server 2000, la funzionalità **Group Policy Object (GPO)** ha permesso agli amministratori di rete di poter configurare in maniera centralizzata i computer della propria organizzazione. Infatti, in un ambiente di lavoro che è completamente gestito da un' infrastruttura basata sulle Group Policy, l'amministratore non ha bisogno di configurare singolarmente i computer e le impostazioni gli utenti.

Le Group policy possono essere associate ad un intero sito di Active Directory, al dominio oppure possono essere associate alle singole Organizational Unit (OU).

Tantissimo è stato scritto in questi anni a proposito delle GPO e quello che mi propongo di scrivere in questa breve guida è rispondere alle domande più frequenti che sono venuti fuori durante i miei corsi.

Le **Group Policy** sono un potentissimo strumento che permette di poter imporre le configurazioni sia agli utenti che ai computer, in particolar modo configurazioni che riguardano la sicurezza, le applicazioni desktop, la gestione e la distribuzione del software e le configurazioni relative alla rete.

In particolar modo, gli Administrative Templates delle GPO modificano chiavi di registro di Windows, sia nel ramo utente che nel ramo computer, che contengono la parola **Policies**.

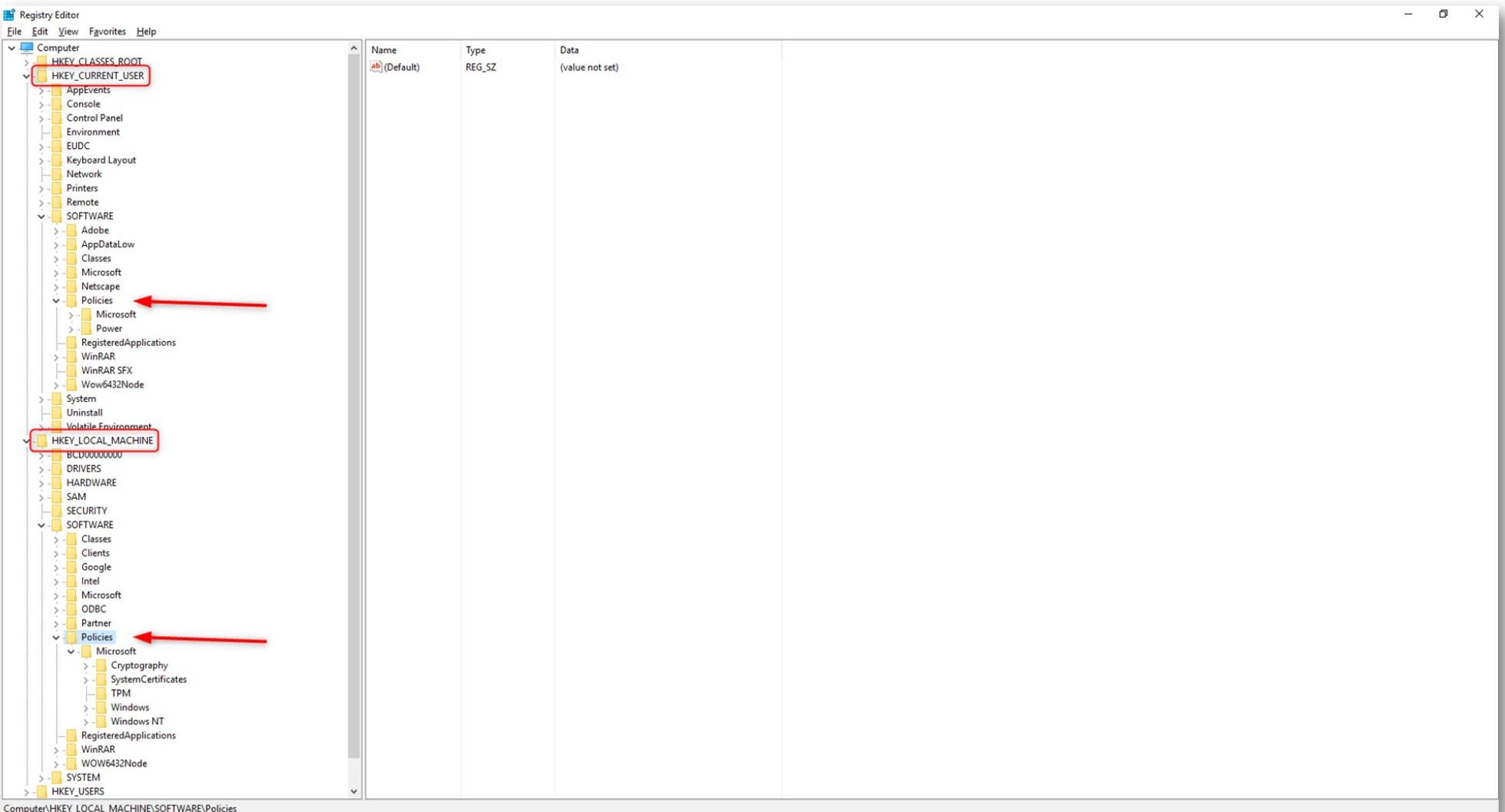


Figura 1: Le Group Policy modificano le chiavi registro di Windows

Gestione delle Group Policy: console e tools

Per gestire le Group policy abbiamo a disposizione alcune console come la **Group Policy Management Console** e il **Group Policy Management Editor**. Ma ci sono anche diversi strumenti a riga di comando come **GPUpdate** e **GPRResult**

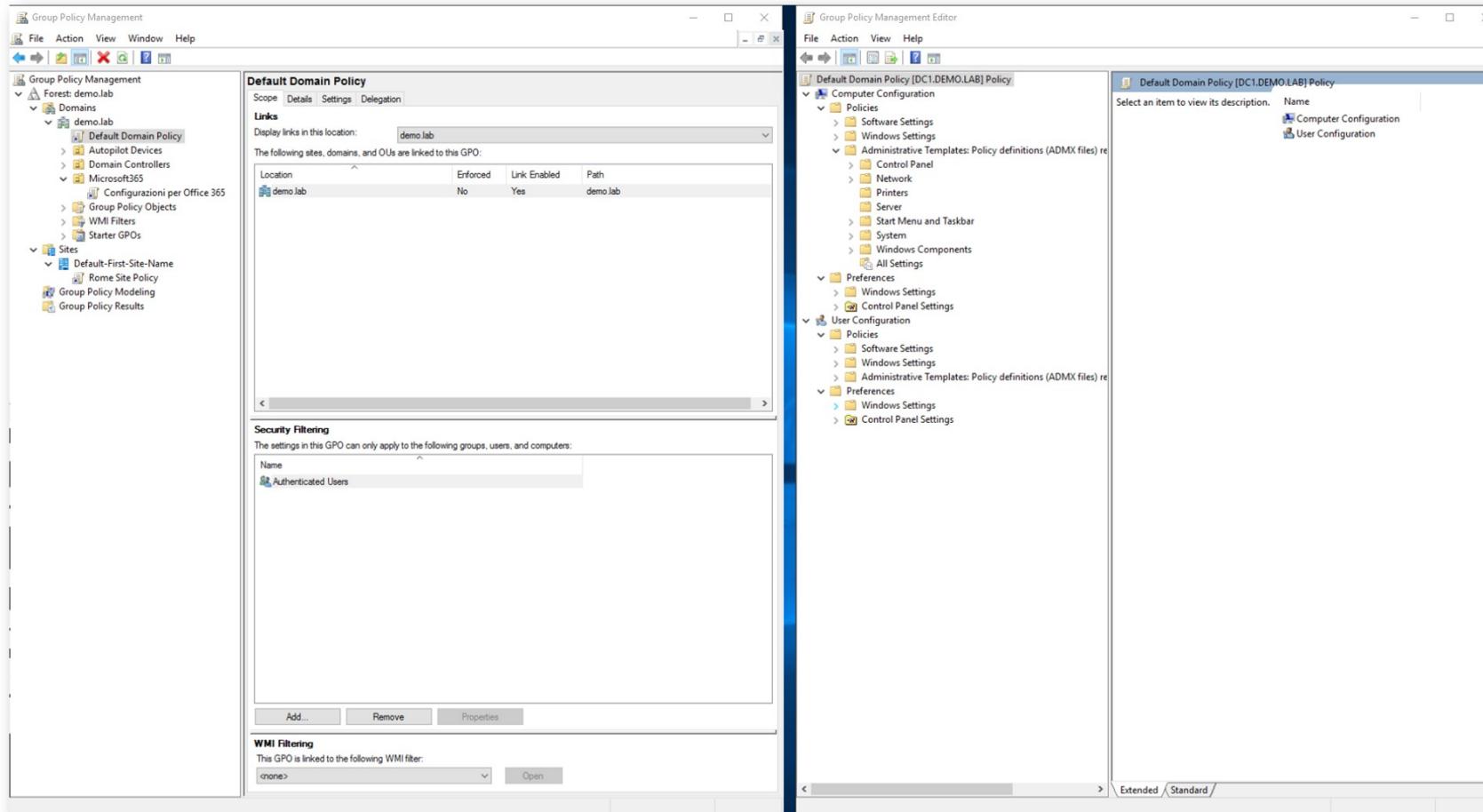


Figura 2: Strumenti per la gestione delle Group Policy: Group Policy Management Console e Group Policy Editor

Il comando **GResult** permette di ottenere informazioni sulle Group Policy applicate all'utente sulla macchina su cui è connesso in quel momento. Con il comando GResult /h <nome file>.htm è possibile ottenere un report in formato HTML delle policy applicate. Per maggiori informazioni potete consultare la pagina <https://docs.microsoft.com/it-it/windows-server/administration/windows-commands/gresult>

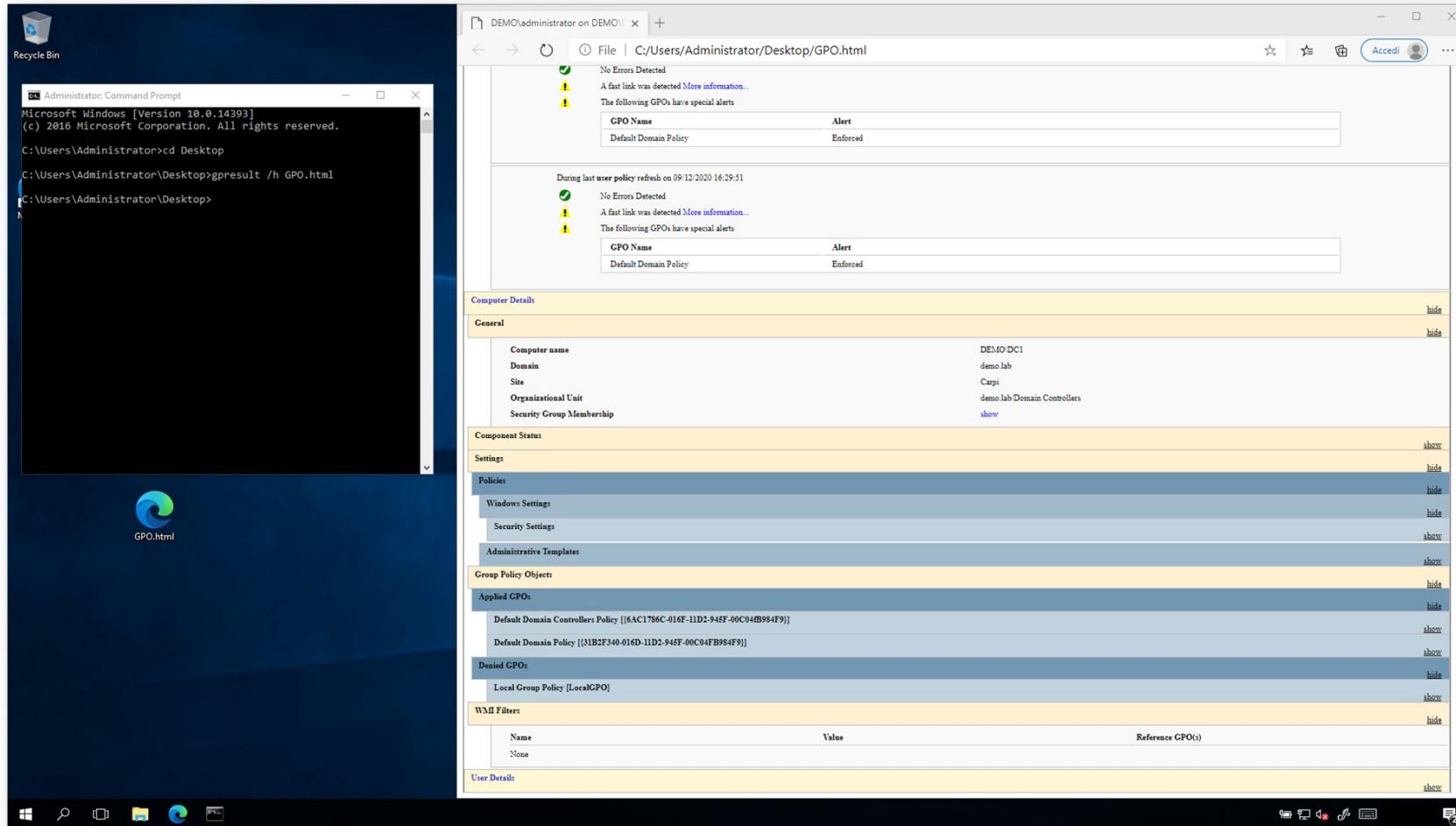


Figura 3: Risultato dell'esecuzione del comando **gpresult**

Applicazione delle Group Policy

Uno dei vantaggi delle **Group Policy** è che vengono applicate in background senza l'intervento dell'amministratore e vengono riapplicate in maniera automatica ogni 5 minuti per i domain controller e ogni 90 minuti + 30 minuti per i computer del dominio. L'impostazione è modificabile cambiando i valori del ramo Computer Configuration à Policies à Administrative Templates à System à Group Policy e configurando le due policy **Set Group Policy refresh interval for domain controllers** e **Set Group Policy refresh interval for computers**

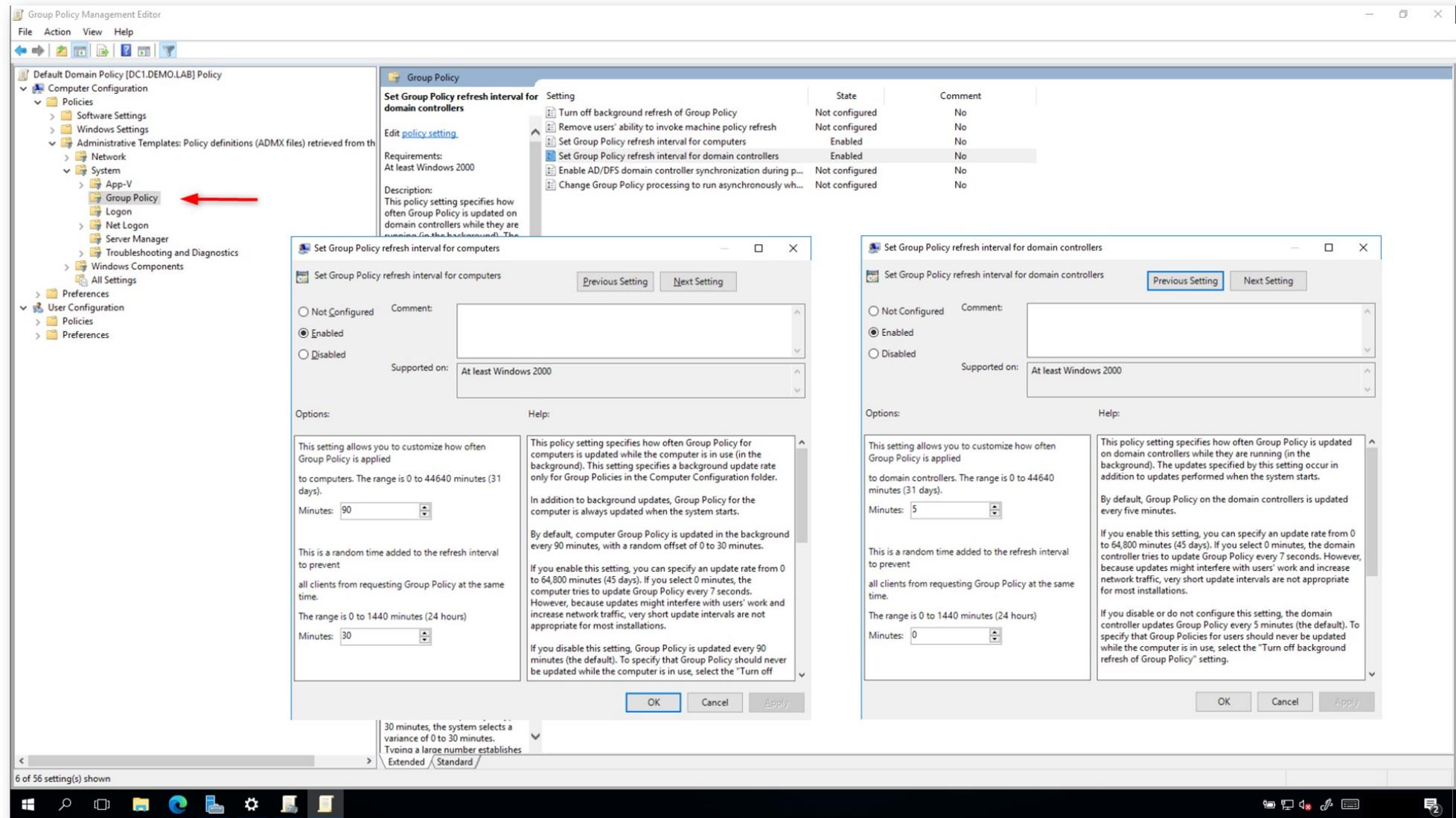


Figura 4: Configurazione degli intervalli di refresh delle GPO per i computer e per i domain controller

Opzioni disponibili per le Policy

Tutte le policy hanno 3 "stati"

1. **Not Configured**: Questa è la modalità **predefinita** di tutti i settings. In questa modalità le configurazioni previste non vengono applicate e sono ignorate.

2. **Enabled**: In questa modalità vengono attivate le configurazioni previste dal setting

3. **Disabled**: Questa opzione viene utilizzata per contraddirre una configurazione a livello più alto. Se ad un livello più alto (Domain oppure OU) il setting è configurato con **Enabled** e ad un livello più basso (OU o sotto OU) lo stesso setting è configurato su **Disabled** allora le due configurazioni si annullano a vicenda. Quindi rimane la configurazione predefinita dal sistema operativo o dal software che state configurando tramite Administrative Templates con la GPO.

NOTA: Controllate sempre nella guida del Setting cosa succede nel caso del **Disabled**. A volte mettere il Setting in modalità **Disabled** equivale al **Not Configured**, ma potrebbero esserci Settings che in modalità **Disabled** impediscono anche all'utente di modificare la configurazione sul proprio PC.

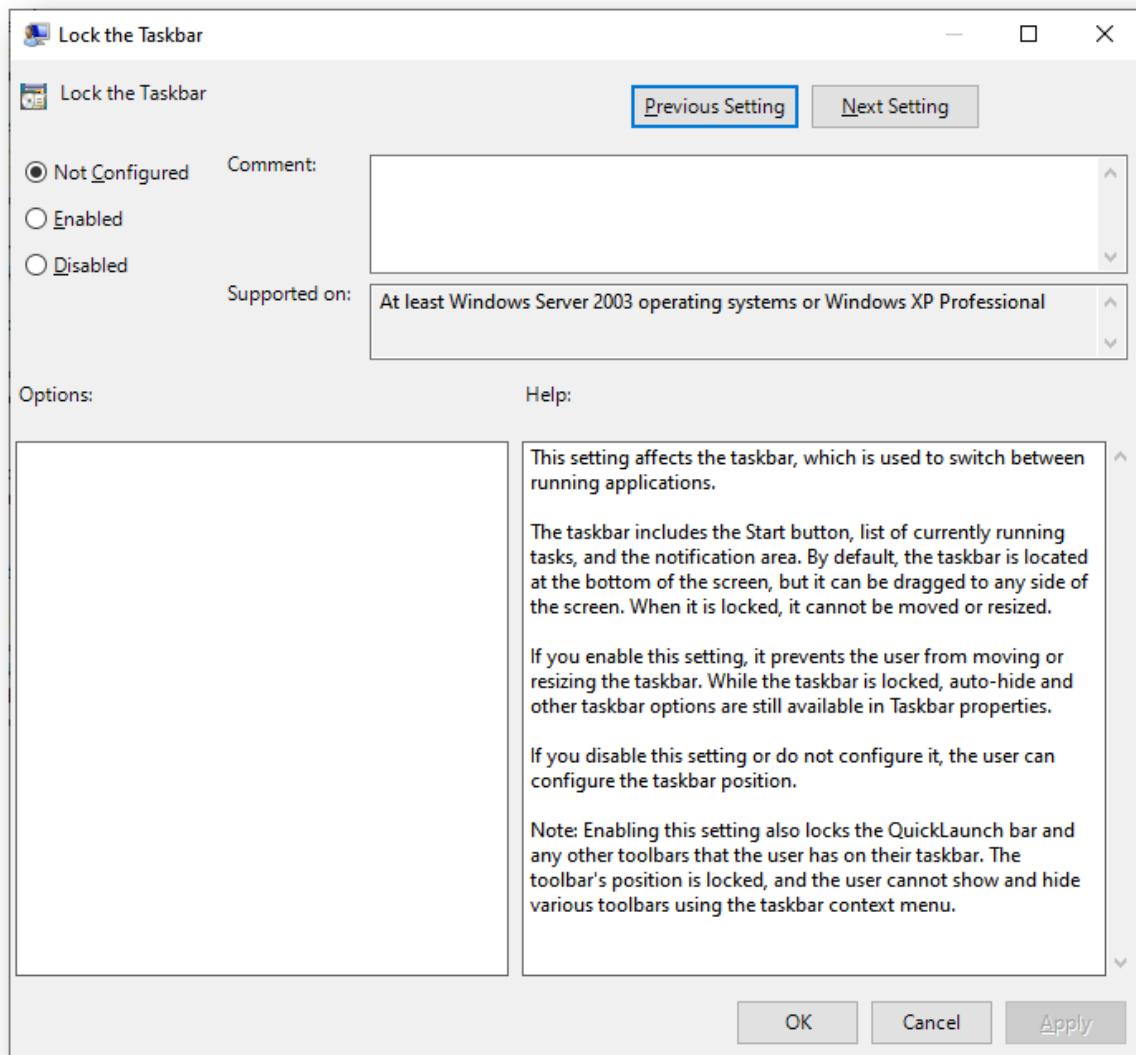


Figura : Opzioni disponibili per i settings delle GPO

Administrative Templates

Come già scritto prima, gli **Administrative Templates** delle Group Policy modificano i rami del registro computer **HKEY_LOCAL_MACHINE** e dell'utente **HKEY_CURRENT_USER**. Questi file, originariamente creati in formato .ADM e successivamente in Windows Server 2008 creati in formato .ADMX, permettono di configurare un notevole numero di parametri del sistema operativo, ma anche di alcuni applicativi. Infatti, è possibile aggiungere ulteriori administrative templates alle nostre group policy per poter configurare in ambiente enterprise prodotti come Microsoft Office, Adobe Acrobat Reader, Google Chrome, Mozilla Firefox e tanti altri. Dopo essersi procurati sul sito del produttore dell'applicativo i diversi file ADMX, è sufficiente copiarli nella cartella **C:\Windows\PolicyDefinitions** del domain controller.

Se, ad esempio, volete aggiungere gli **Administrative Templates** per poter gestire le Microsoft 365 Apps for enterprise, Office 2019 oppure Office 2016, potete scaricarli dal link <https://www.microsoft.com/en-us/download/details.aspx?id=49030> . Dopo averli estratti sarà sufficiente copiarli nella cartella **C:\Windows\PolicyDefinitions** del domain controller. Riaprodo successivamente il Group Policy Editor per qualsiasi GPO, le nuove configurazioni saranno disponibili e potranno essere utilizzate per poter gestire le applicazioni Office, come mostrato nelle figure sotto. Ricordatevi anche di copiare la cartella degli ADML (language pack degli ADMX) della stessa lingua del domain controller!

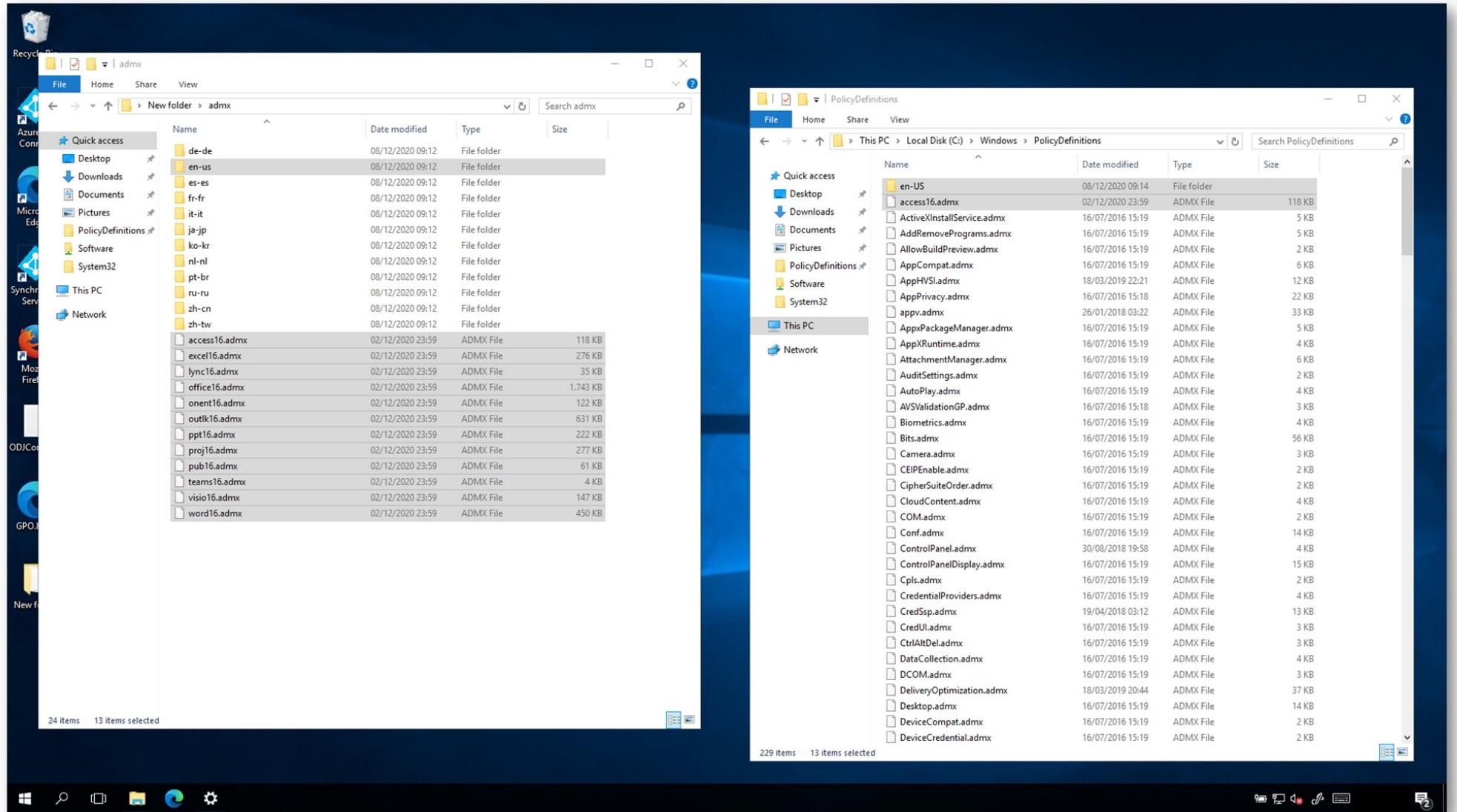


Figura 5: Aggiunta degli Administrative Templates di Office alle policy di dominio

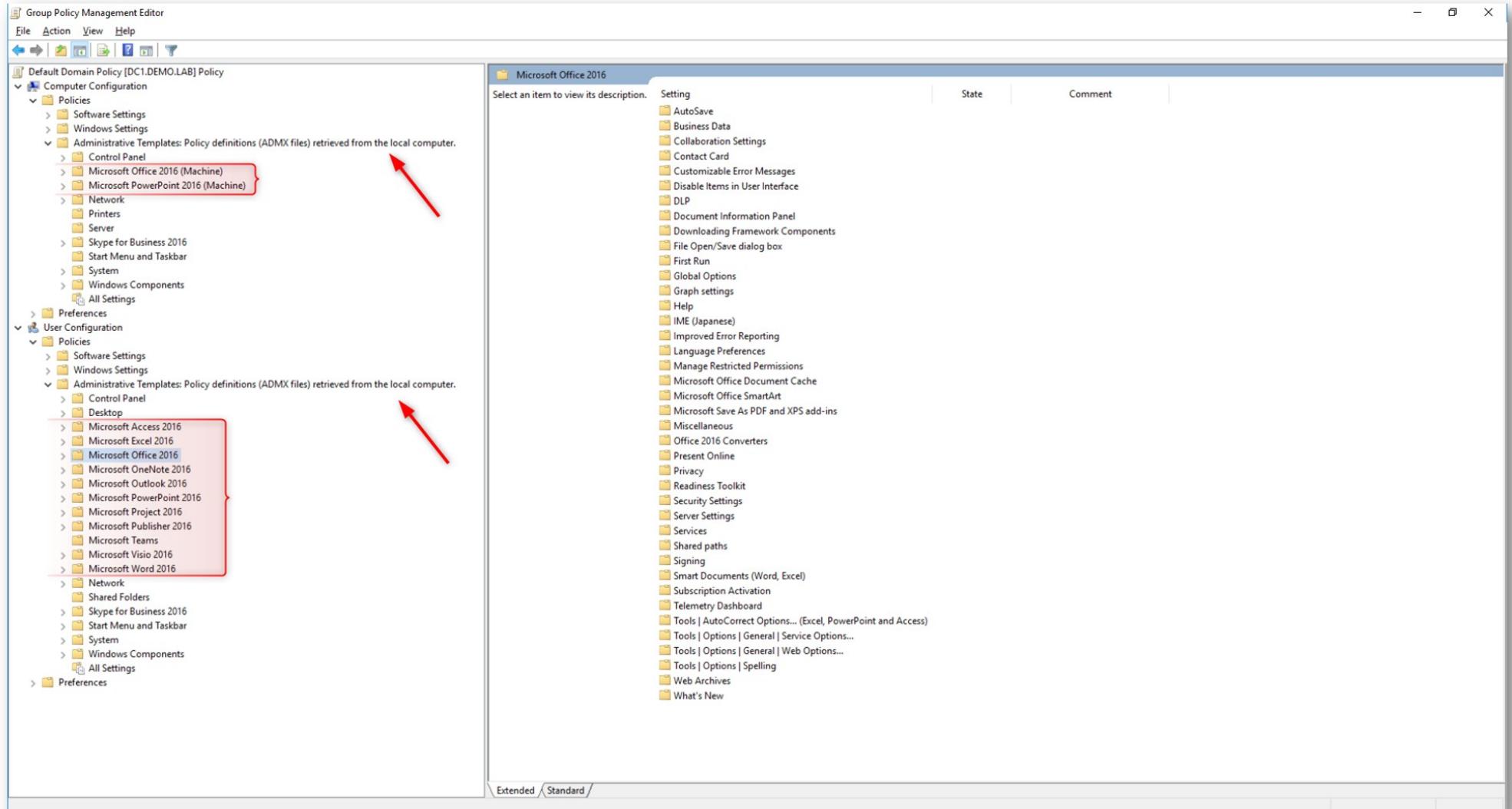


Figura 6: Gestione delle applicazioni Office utilizzando le Group Policy

Come si può vedere dalla figura sopra, gli **Administrative Templates** sono stati incollati nella cartella **C:\Windows\PolicyDefinitions** del domain controller e la console ci mostra che sono stati presi dal computer locale (la freccia lo evidenzia nell'immagine). Di default, quando aprite la Group Policy Management Console viene contattato non un domain controller qualsiasi ma quello che ha il ruolo FSMO (Flexible Single Master Operation) di **PDC Emulator**. Se avete più domain controller, come è giusto che sia, e se sono anche distribuiti in diversi Site di Active Directory, sarà necessario copiare gli Administrative Templates in tutte le cartelle **C:\Windows\PolicyDefinitions** di tutti i domain controller in modo tale da poterlo configurare da qualsiasi DC e non necessariamente dal DC che ha il ruolo di **PDC Emulator**. Per ovviare a questa incombenza è possibile utilizzare il **Central Store** delle GPO, disponibile da Windows Server 2008.

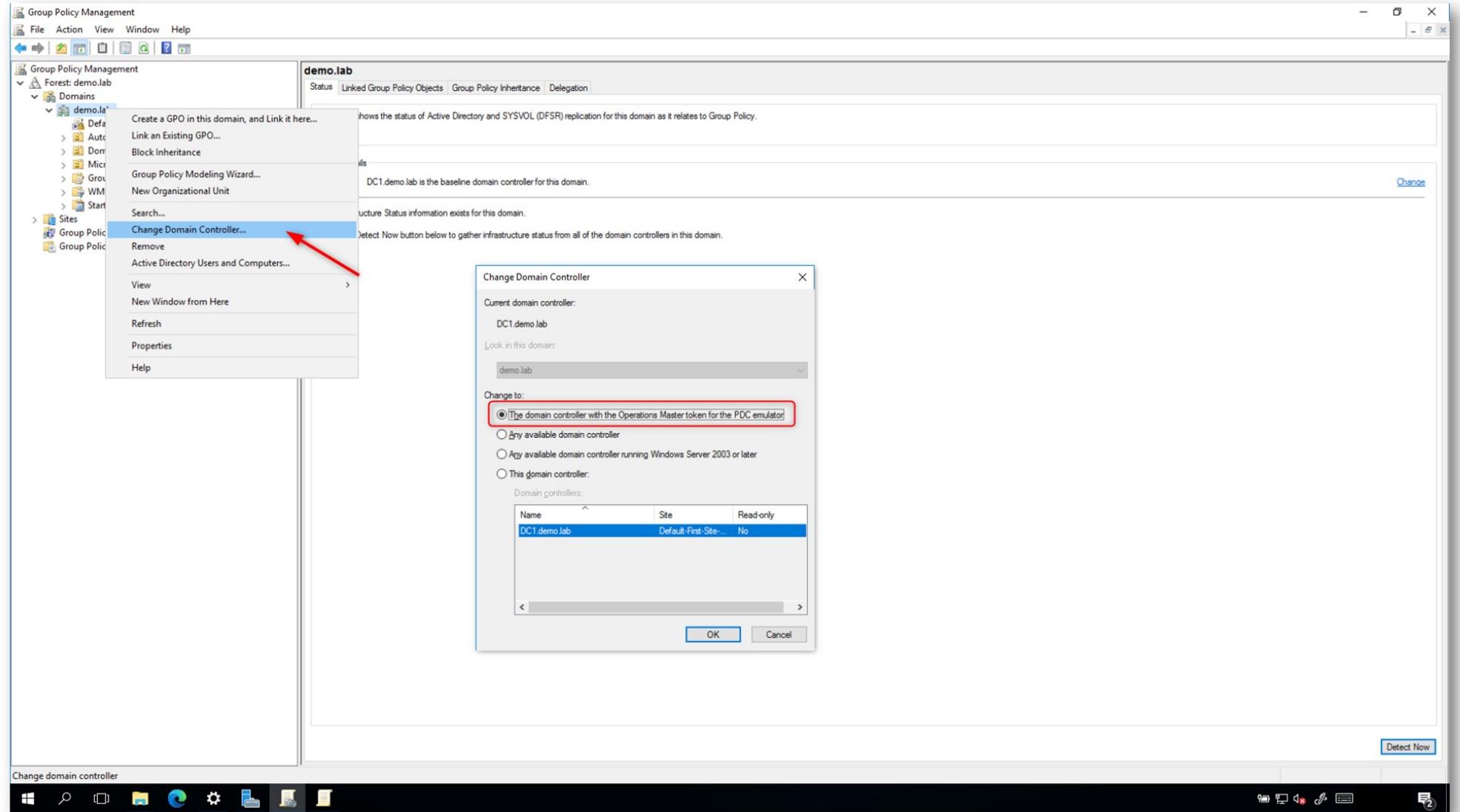


Figura 7: La Group Policy Management Console si collega in maniera predefinita al domain controller con il ruolo di PDC Emulator

Utilizzo del Central Store

Per poter gestire le Group Policy collegandovi con le console di amministrazione a qualsiasi domain controller e non necessariamente da quello che il ruolo di **PDC Emulator**, soprattutto se aggiungete Administrative Templates che non sono inclusi in Windows Server, è possibile utilizzare il **Central Store** delle GPO, introdotto In Windows Server 2012 R2. Tutta la cartella **C:\Windows\PolicyDefinitions** di uno dei domain controller deve essere copiata nel percorso **\<nome dominio>\SYSVOL\<nome dominio>\Policies**. Va da sé che d'ora in poi tutti gli Administrative Templates da aggiungere dovranno essere copiati nella cartella centralizzata della SYSVOL e non più nella cartella locale dei domain controller.

In particolar modo dovranno essere anche copiati gli Administrative Templates per le versioni più recenti di Windows Server e Windows Client, come ampiamente trattato nella guida ufficiale <https://docs.microsoft.com/it-it/troubleshoot/windows-client/group-policy/create-and-manage-central-store>

- Modelli amministrativi (con estensione ADMX) per l'aggiornamento a Windows 10 maggio 2020 (2004)
- Modelli amministrativi (con estensione ADMX) per l'aggiornamento a Windows 10 novembre 2019 (1909)
- Modelli amministrativi (con estensione ADMX) per l'aggiornamento a Windows 10 maggio 2019 (1903)
- Modelli amministrativi (con estensione ADMX) per l'aggiornamento a Windows 10 ottobre 2018 (1809)
- Modelli amministrativi (con estensione ADMX) per Windows 10, versione 1803 (aggiornamento 2018 di aprile)
- Modelli amministrativi (con estensione ADMX) per Windows 10, versione 1709 (Fall Creators Update)
- Modelli amministrativi (con estensione ADMX) per Windows 10, versione 1703 (Creators Update)
- Modelli amministrativi (con estensione ADMX) per Windows 10, versione 1607 e Windows Server 2016
- Modelli amministrativi (con estensione ADMX) per Windows 10 e Windows 10, versione 1511
- Modelli amministrativi (con estensione ADMX) per l'aggiornamento a Windows 8,1 e Windows Server 2012 R2
- Modelli amministrativi (con estensione ADMX) per Windows 8,1 e Windows Server 2012 R2

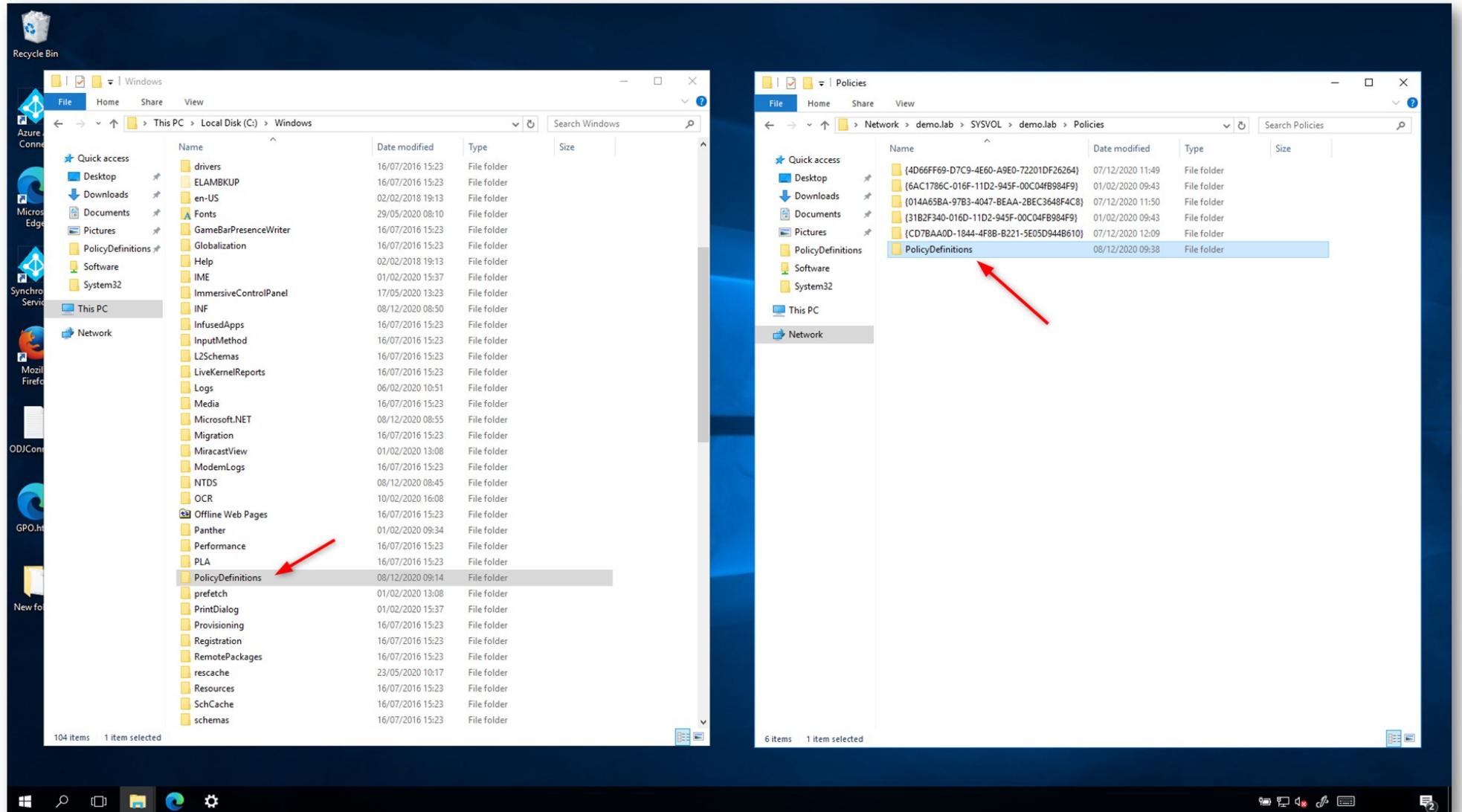


Figura 8: Configurazione del Central Store per le GPO

Come si può vedere dalla figura sotto, il Group Policy Editor fa riferimento al **Central Store** per il caricamento e la visualizzazione degli Administrative Templates.

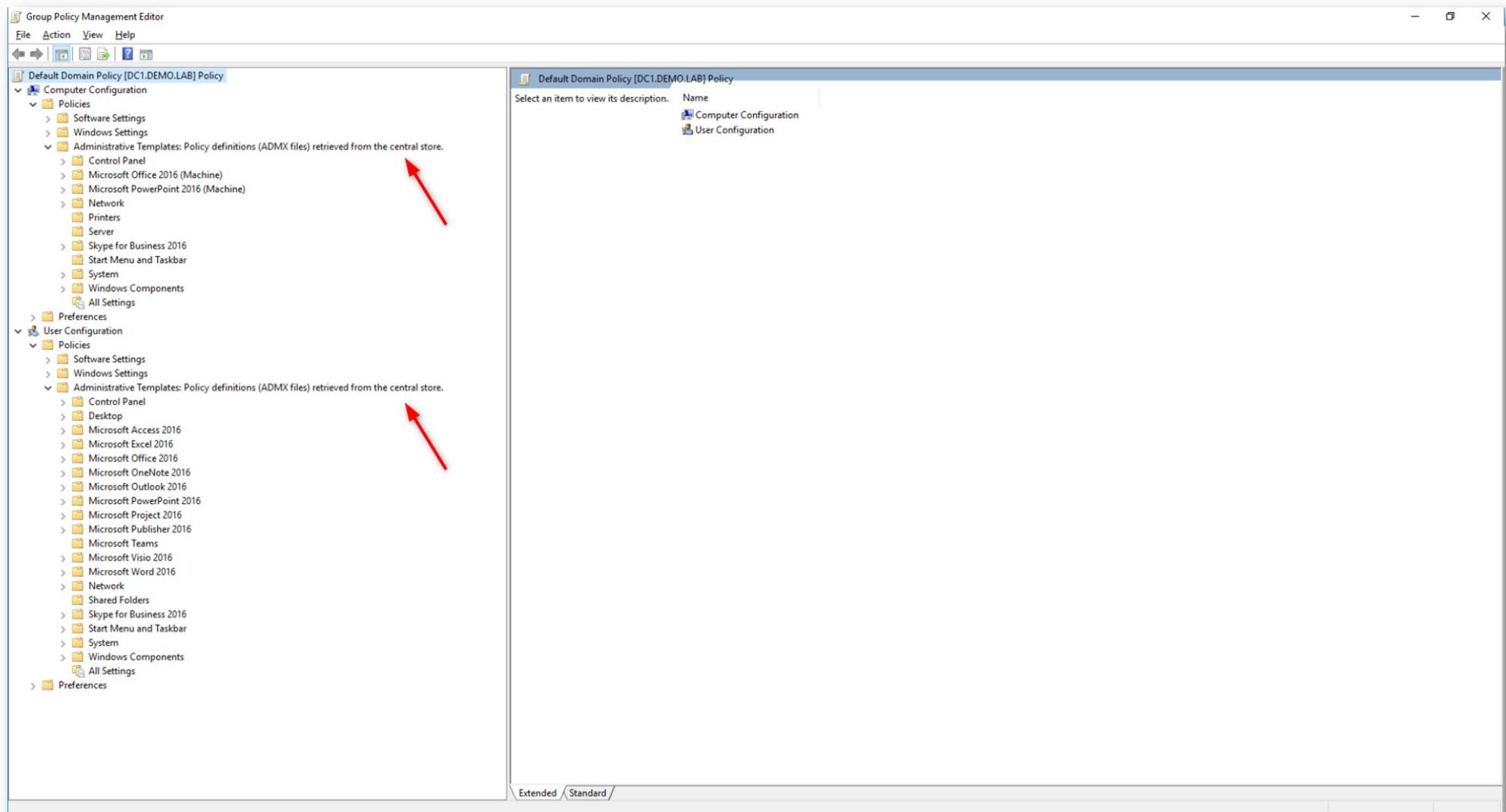


Figura 9: Il Central Store viene utilizzato per caricare gli Administrative Templates

Group Policy Processing order

Quello che spesso sfugge è l'ordine con cui le Group policy vengono applicate all'interno della nostra organizzazione . Infatti, è molto importante considerare l'ordine di precedenza in quanto, nonostante l'applicazione delle configurazioni sia **cumulativa**, l'ultima policy sovrascriverà la configurazione applicata da una policy precedente:

Ordine di precedenza: Local à Site à Domain à OU à Child OU à ...

L'ordine è visibile nel tab **Group Policy Inheritance** della Group Policy Management Console. L'impostazione che vincerà è quella applicata alla Child OU, perchè è stata creata appositamente per gestire in maniera diversa gli utenti ed i computer che si trovano in quella OU.

Questo tipo di comportamento, che è quello predefinito, può essere modificato configurando la policy precedente in modalità **Enforced** e, nel caso vengano configurate **le stesse impostazioni**, quella che vince è quella applicata a livello più alto. Ripeto infatti che tutte le configurazioni vengono sommate (sono cumulative) e che stiamo solo decidendo il comportamento nel caso in cui due policy diverse vadano a modificare la stessa impostazione.

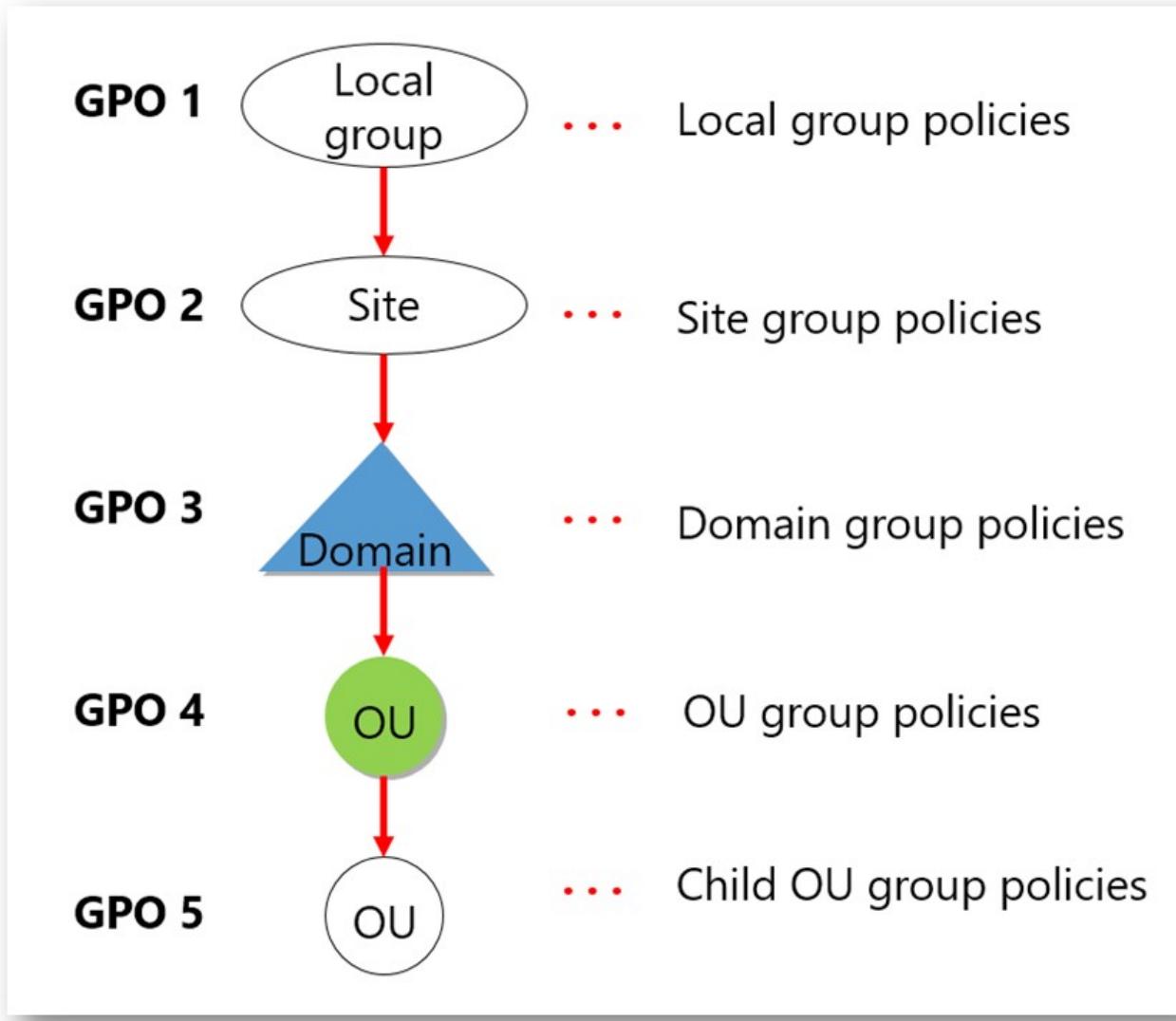


Figura 10: Group Policy processing order

Si tenga presente che più è basso il numero della precedenza nella scheda **Group Policy Inheritance** à Più in alto verrà visualizzata la policy nella lista –à La policy più in alto avrà la **precedenza**

Lower number à Higher on list à Precedence

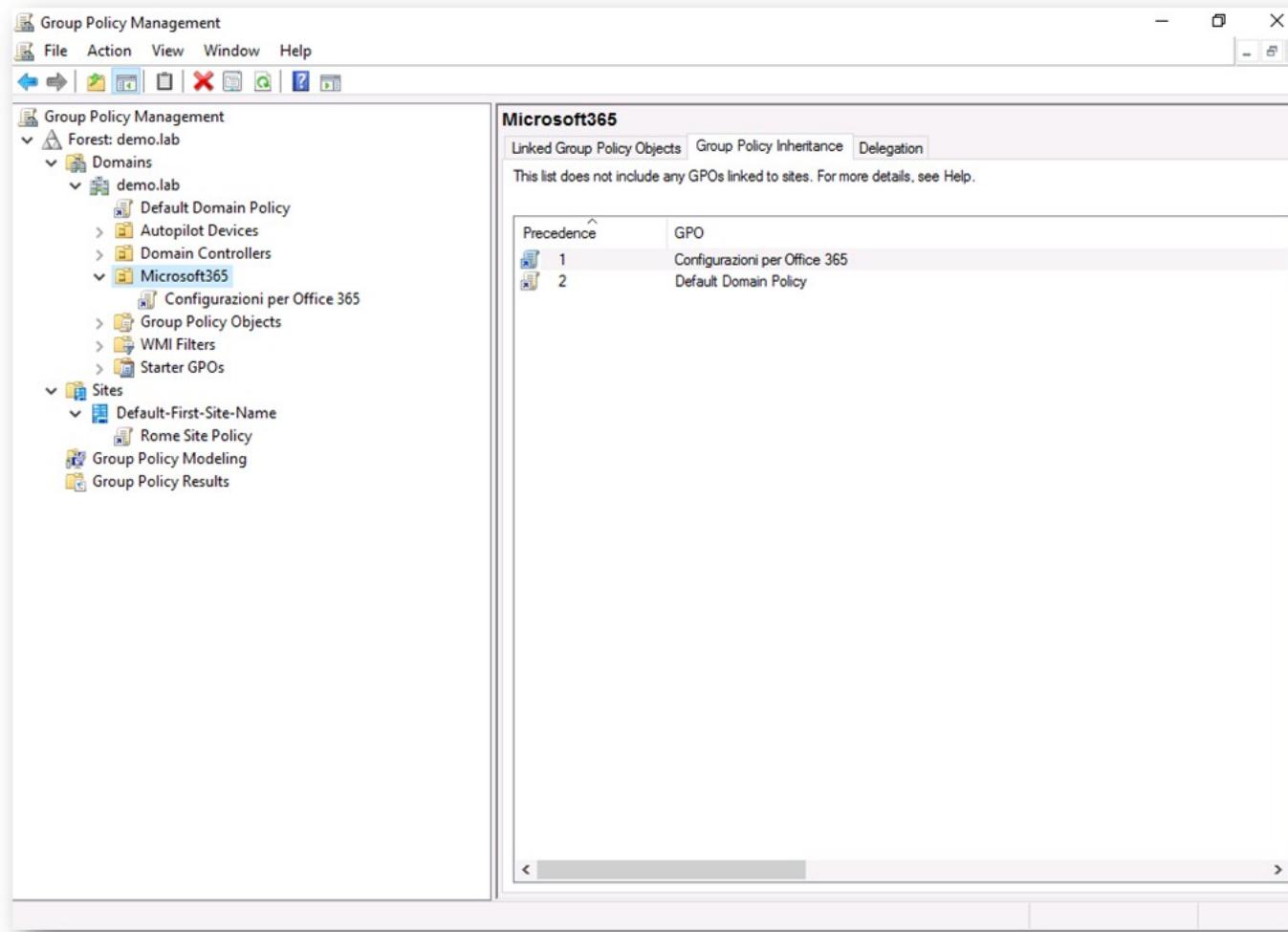


Figura 11: Esempio di Group Policy Inheritance

L'eredità può anche essere bloccata, cliccando col tasto destro sulla OU e scegliendo **Block Inheritance**. L'icona della Organization Unit avrà un punto esclamativo bianco su base blu, che permetterà di evidenziare meglio questo tipo di configurazione. Con il blocco dell'ereditarietà delle GPO verranno applicate solo le GPO associate a quella OU ed ignorate tutte le altre applicate "a monte". Se ci sono delle Child OU, queste invece erediteranno dalla OU padre, a meno che non blocchiate l'ereditarietà anche per loro, agendo singolarmente su ogni OU.

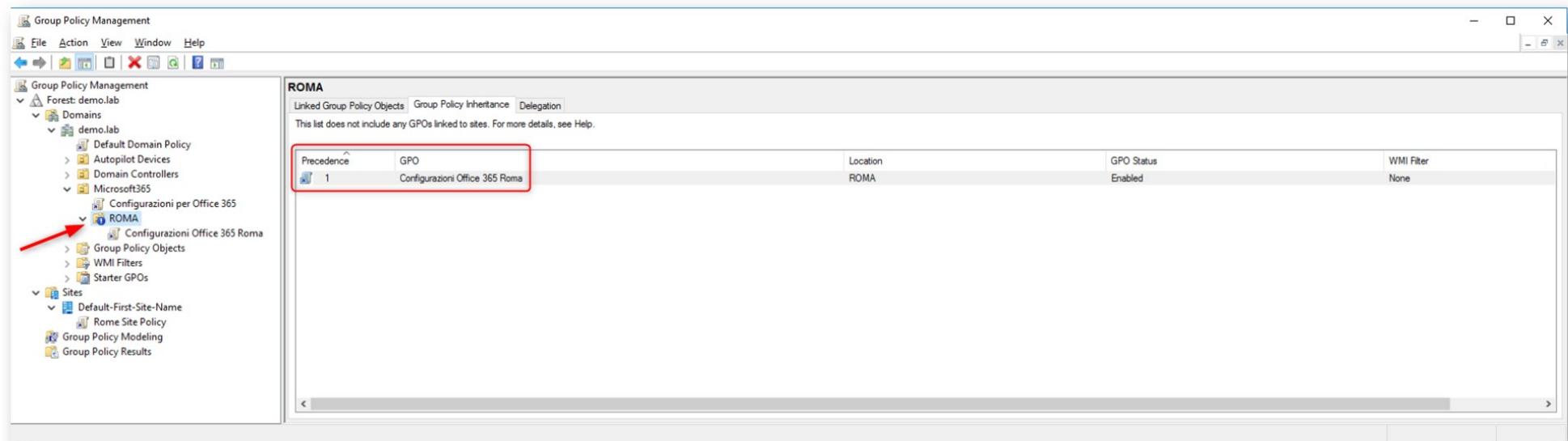


Figura 12: Blocco dell'ereditarietà per una OU

In ogni caso, ricordatevi che se a livello più alto una GPO è **Enforced**, vincerà sempre. Per "forzare" una GPO è sufficiente cliccare con il tasto destro sul link della GPO e scegliere la voce **Enforced**. Sul link della GPO apparirà il simbolo di un lucchetto, come mostrato nella figura sotto. Nella figura si può inoltre notare che la Default Domain Policy è stata forzata e viene applicata anche nel caso alla OU chiamata ROMA abbia applicato il blocco dell'ereditarietà, come mostrato nella scheda Group Policy Inheritance della OU chiamata ROMA.

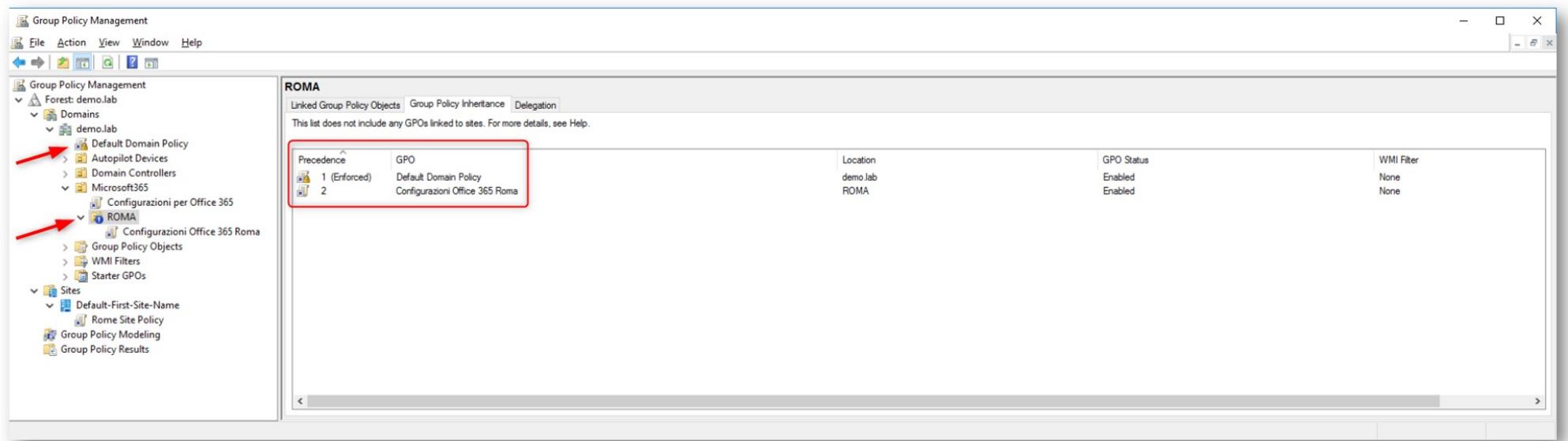


Figura 13: Enforcement di una GPO in modo tale da impedire le modifiche apportate da una GPO ad un livello più basso, in caso di contrasto

Security Filtering

Le Group Policy possono essere anche applicate a gruppi specifici di Active Directory utilizzando il **Security Filtering**. Dalla scheda **Scope** della GPO è infatti possibile decidere di non applicare la policy agli Authenticated Users (una special identity che contiene anche i computer), ma ad un unico utente, ad un gruppo di utenti, ad un unico computer o ad un gruppo di computer. Ad esempio, potremmo collegare la policy a livello di dominio e decidere di applicarla solo al gruppo dei Domain Admins, senza preoccuparci in quale OU si trovino gli amministratori di dominio. È necessario però almeno lasciare i permessi di lettura al gruppo Authenticated Users, altrimenti riceverete un errore come quello mostrato nella figura sotto:

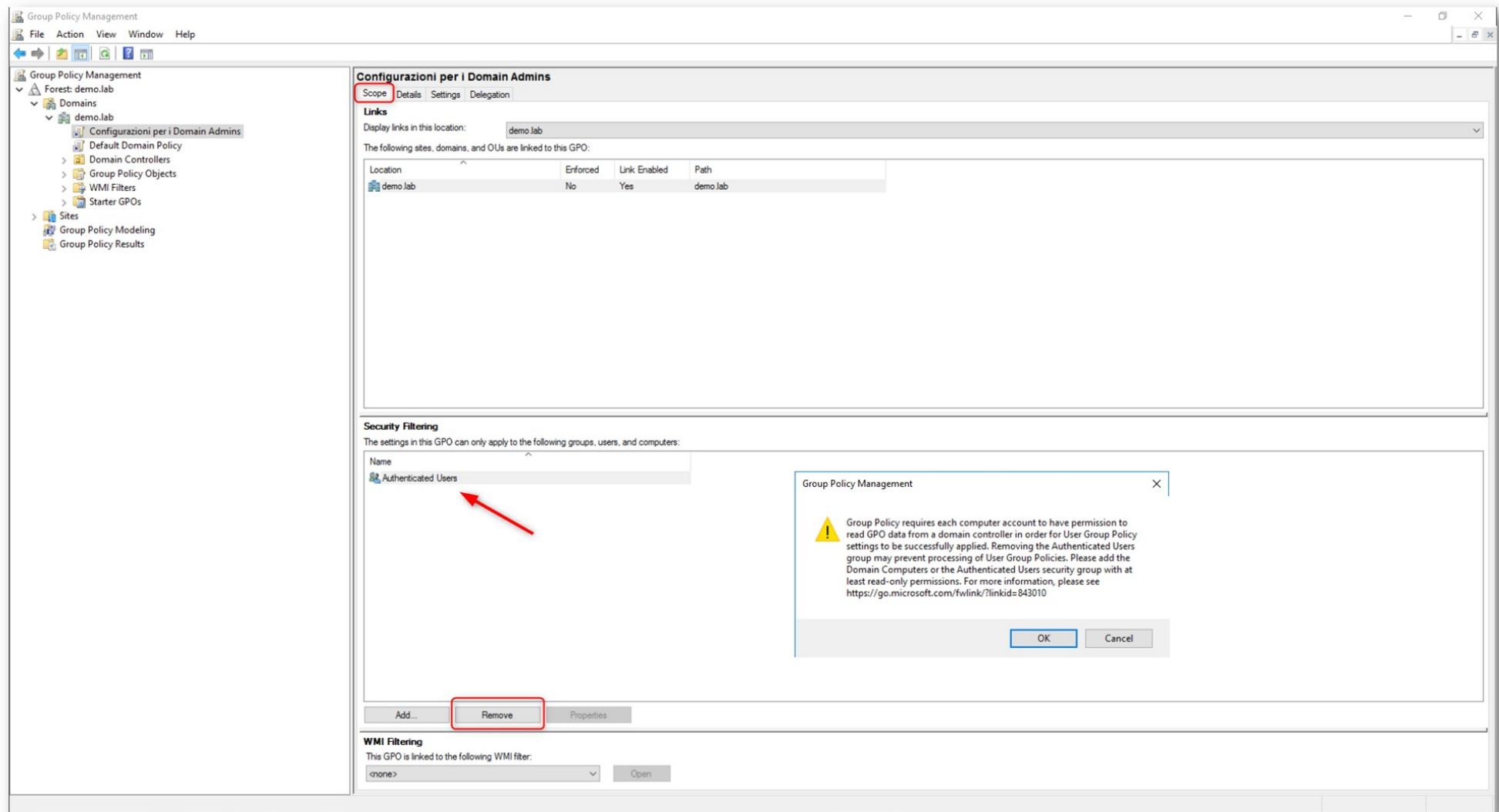


Figura 14: Rimozione degli Authenticated Users dalla Group Policy

Procedete quindi a rimuovere il permesso di **Apply Group Policy** per il gruppo **Authenticated Users** selezionando la scheda **Delegation** della GPO, poi **Advanced** e dai **Settings** della GPO rimuovete il segno di spunta come mostrato nella figura sotto.

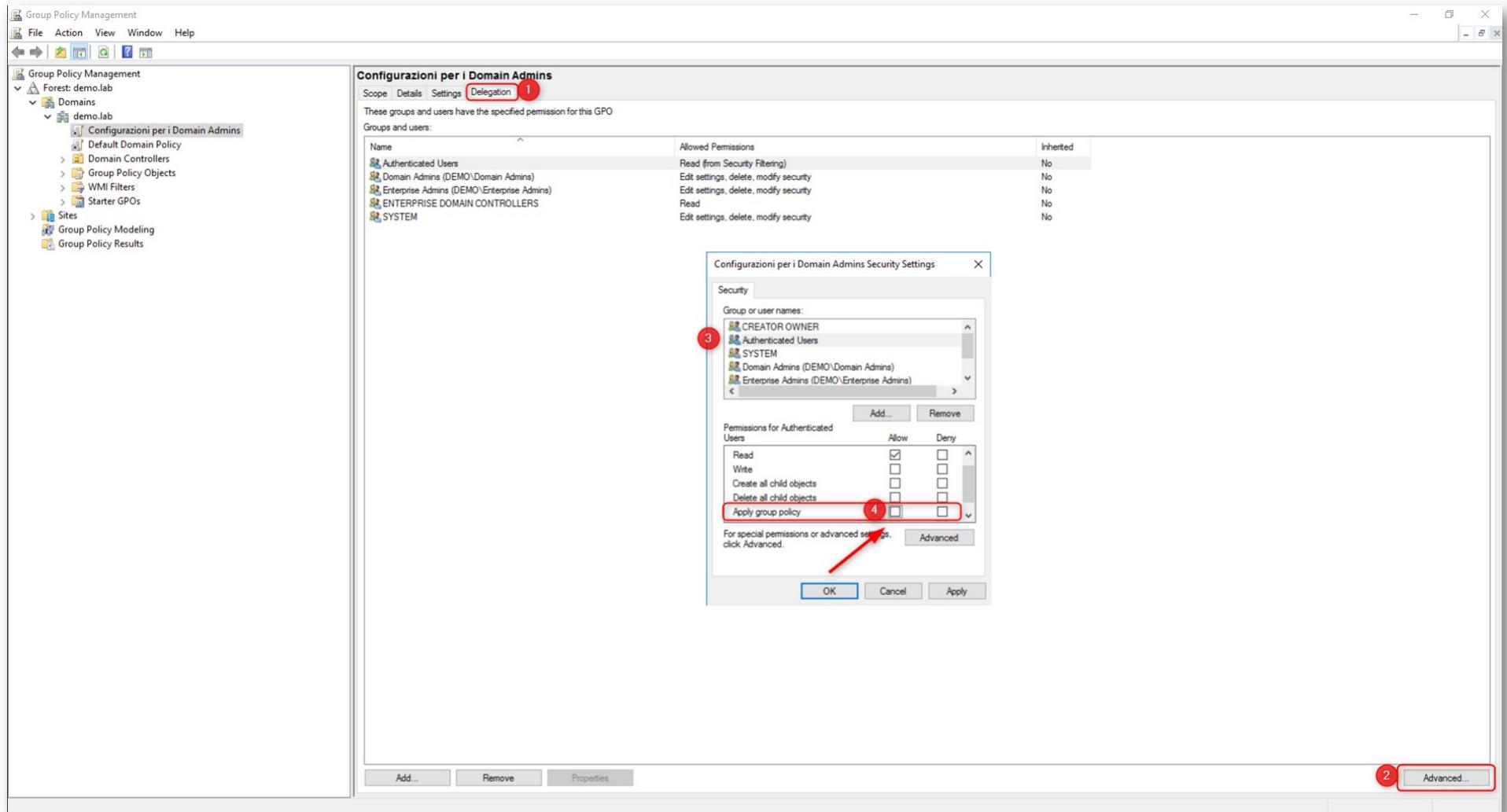


Figura 15: Rimozione dei permessi di applicazione della Group Policy al gruppo **Authenticated Users**

Vedrete a questo punto che il gruppo **Authenticated Users** non sarà più visibile nei Security Settings della GPO

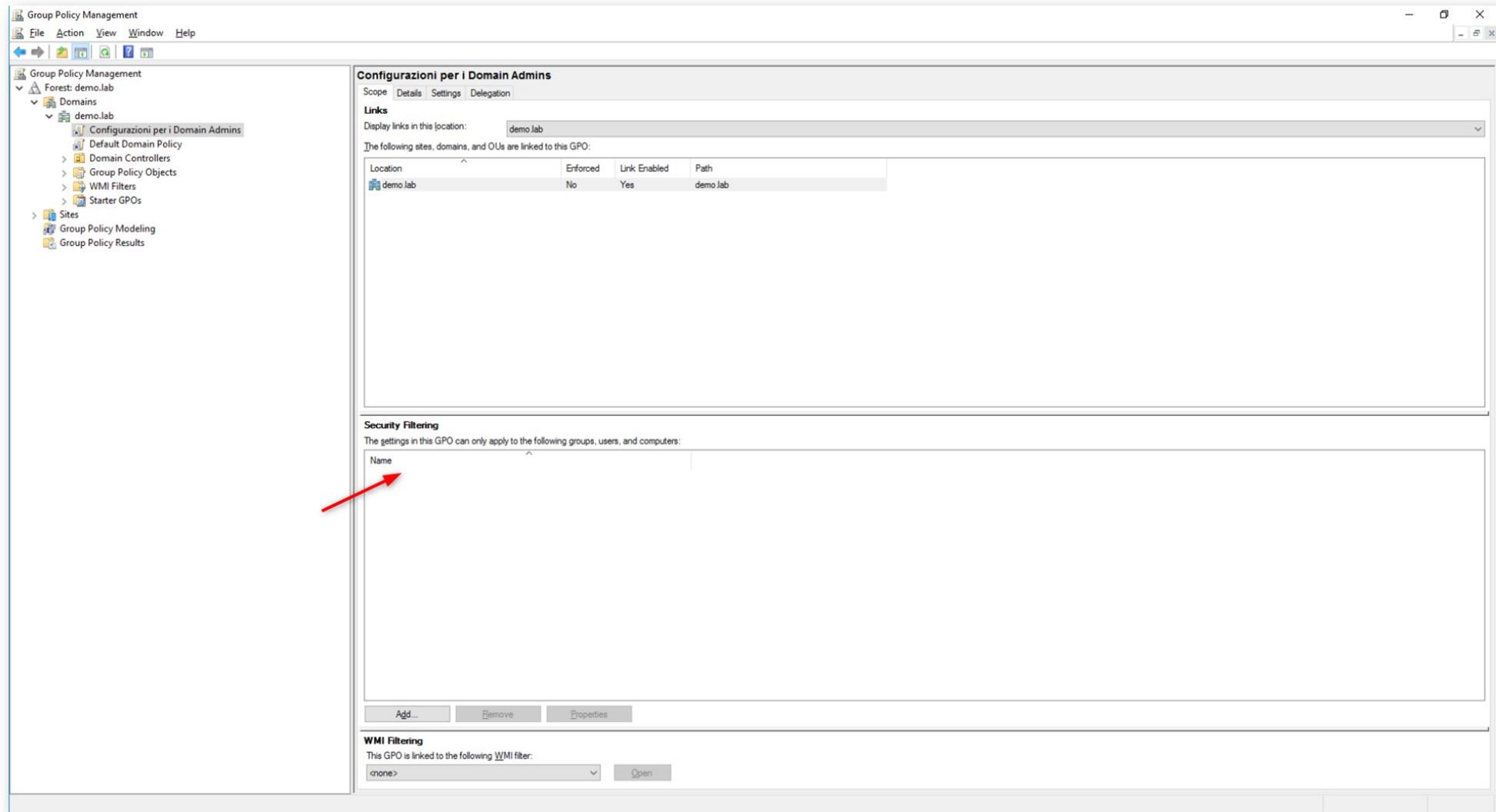


Figura 16: il gruppo Authenticated Users non è più visibile nei Security Settings della GPO

Procedete quindi ad aggiungere il gruppo a cui volete applicare la GPO cliccando sul pulsante **Add**

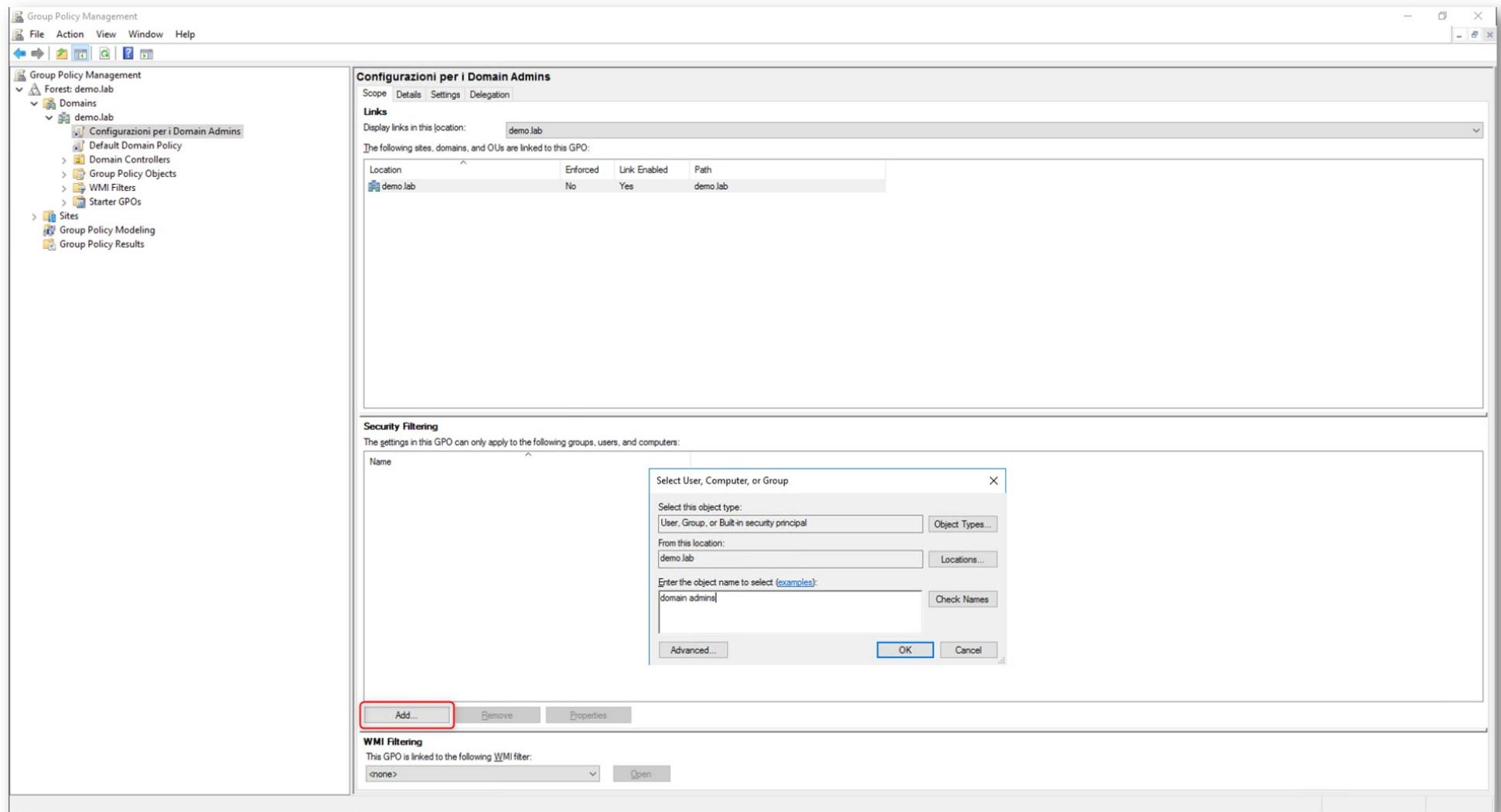


Figura 17: Aggiunta del gruppo di Active Directory a cui applicare la GPO

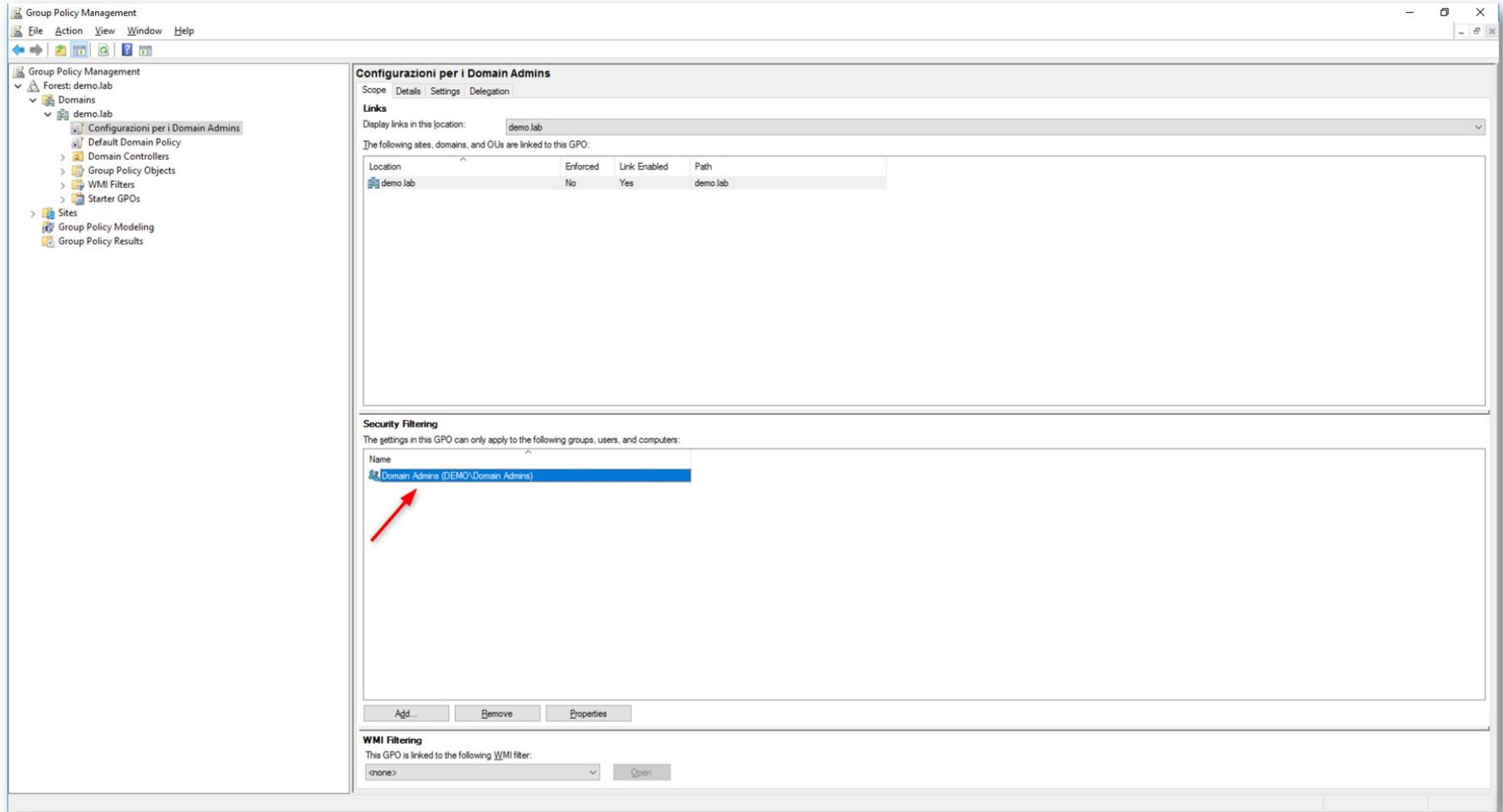


Figura 18: Il nuovo gruppo di Active Directory è stato aggiunto al Security Filtering della GPO

È possibile verificare la presenza del gruppo appena aggiunto anche andando nella scheda **Delegation** della GPO e cliccando su **Advanced**, come mostrato nella figura sotto:

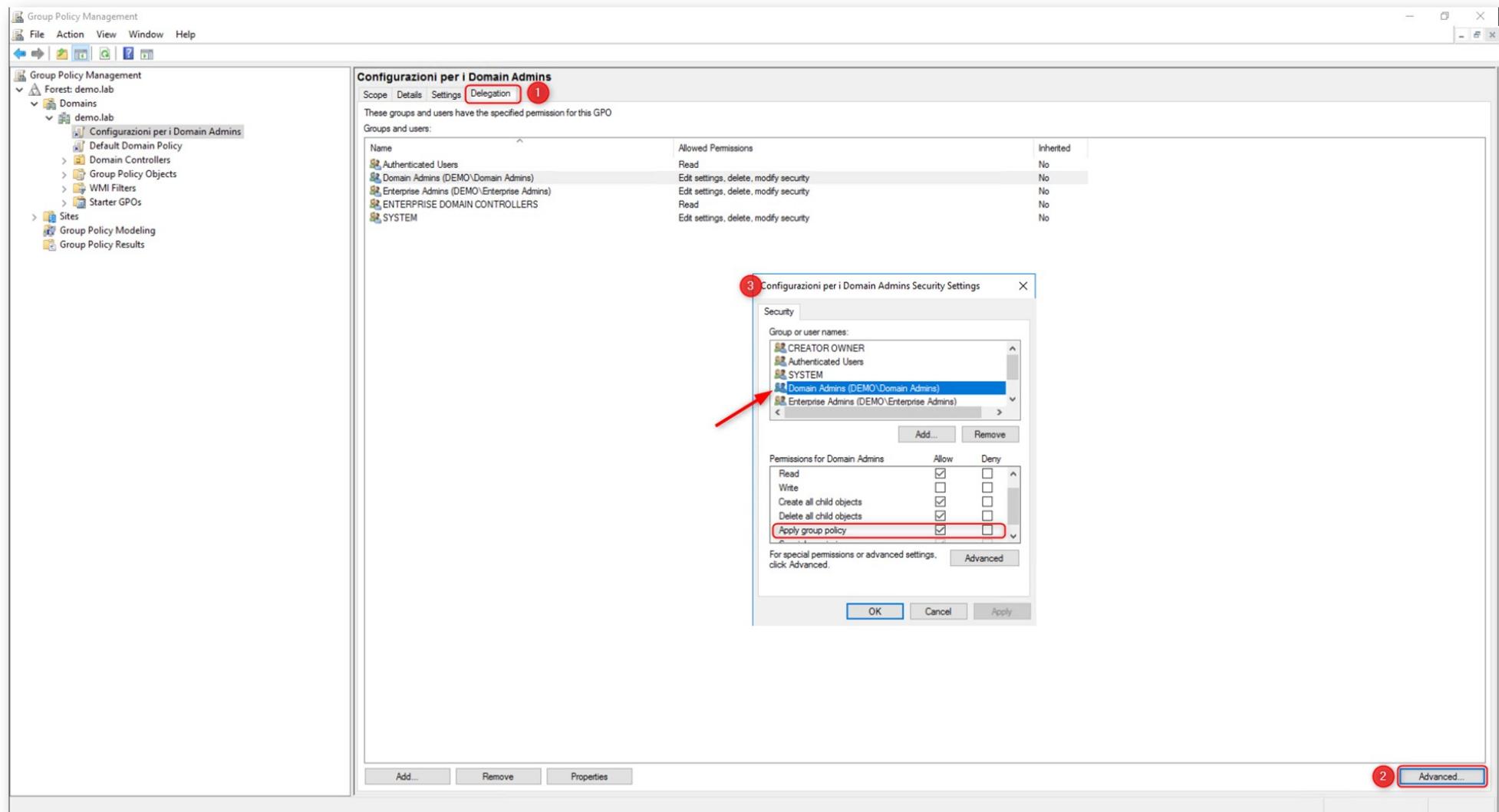


Figura 19: Verifica delle permission di accesso alla GPO

Se volete impedire ad un utente che si trova nel gruppo che avete aggiunto al Security Filtering della GPO di essere configurato tramite la policy è possibile configurare il tab Security della policy ed utilizzare il **Deny** sul permesso di **Apply Group Policy**, come mostrato nella figura:

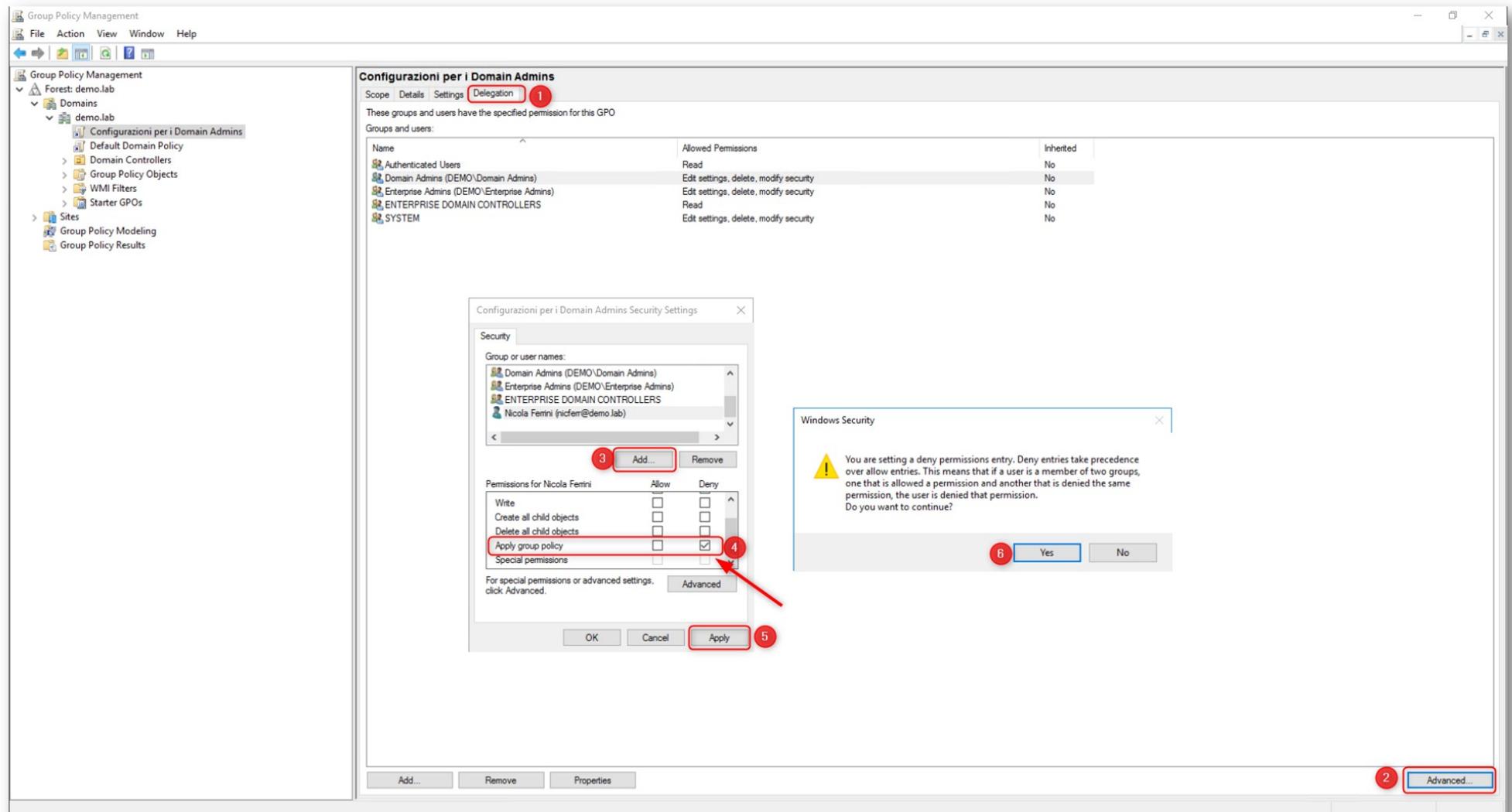


Figura 20: Esclusione di un utente dall'applicazione di una Group Policy

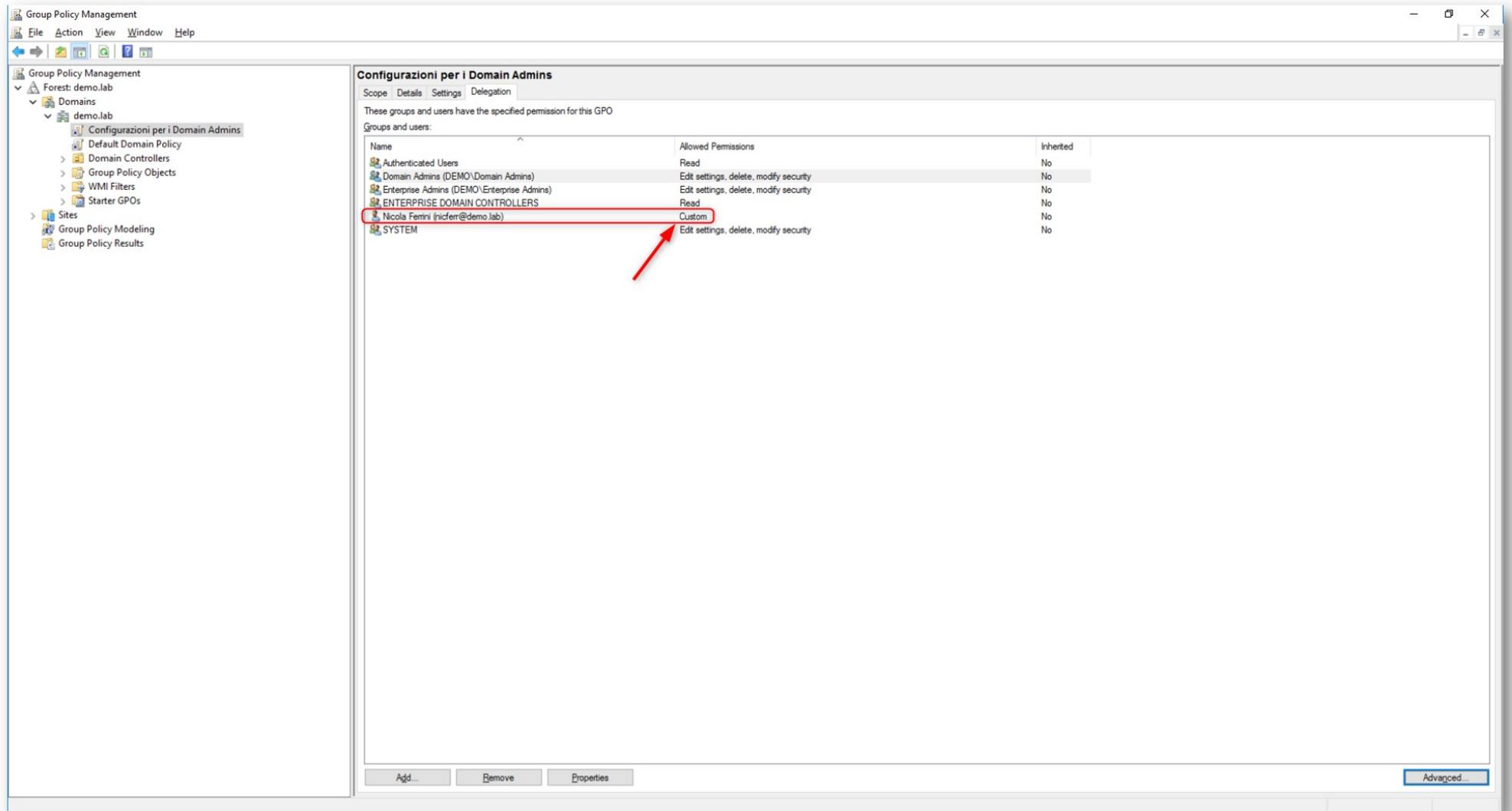


Figura 21: Utente con permessi personalizzati per la GPO

Loopback Processing Mode

Ho già avuto modo di scrivere del Loopback Processing Mode nell'articolo [Come funziona il Loopback Processing Mode nelle Group Policy](#). Molti di voi sapranno già che le Group Policy hanno la possibilità di configurare sia i computer che gli utenti e le configurazioni utente vengono applicate indipendentemente dal computer dove l'utente si logga.

Ci sono casi, tuttavia, dove questo tipo di comportamento potrebbe non andare bene; ad esempio se un utente si logga su un Remote Desktop Session Host (Terminal Server), che è una macchina condivisa da più persone, vorrei evitare che si porti dietro alcune configurazioni.

Per ovviare a questo comportamento di default è necessario abilitare **il Loopback Processing mode**. Per abilitare il Loopback Processing Mode è necessario configurare la Policy scegliendo **Computer Configuration/Administrative Templates/System/Group Policy** e modificare il parametro **Configure user Group Policy loopback processing mode**

Se si abilita questa impostazione, è possibile selezionare una delle modalità seguenti nella casella Modalità:

- “Sostituisci” indica che le impostazioni utente definite negli oggetti Criteri di gruppo del computer sostituiscono le impostazioni utente generalmente applicate all’utente.
- “Unisci” indica che le impostazioni utente definite negli oggetti Criteri di gruppo del computer e le impostazioni utente normalmente applicate all’utente vengono combinate. In caso di conflitto, le impostazioni utente degli oggetti Criteri di gruppo del computer avranno la precedenza sulle impostazioni normali dell’utente.

Se si disabilita o non si configura questa impostazione, gli oggetti Criteri di gruppo dell’utente determineranno le impostazioni utente valide.

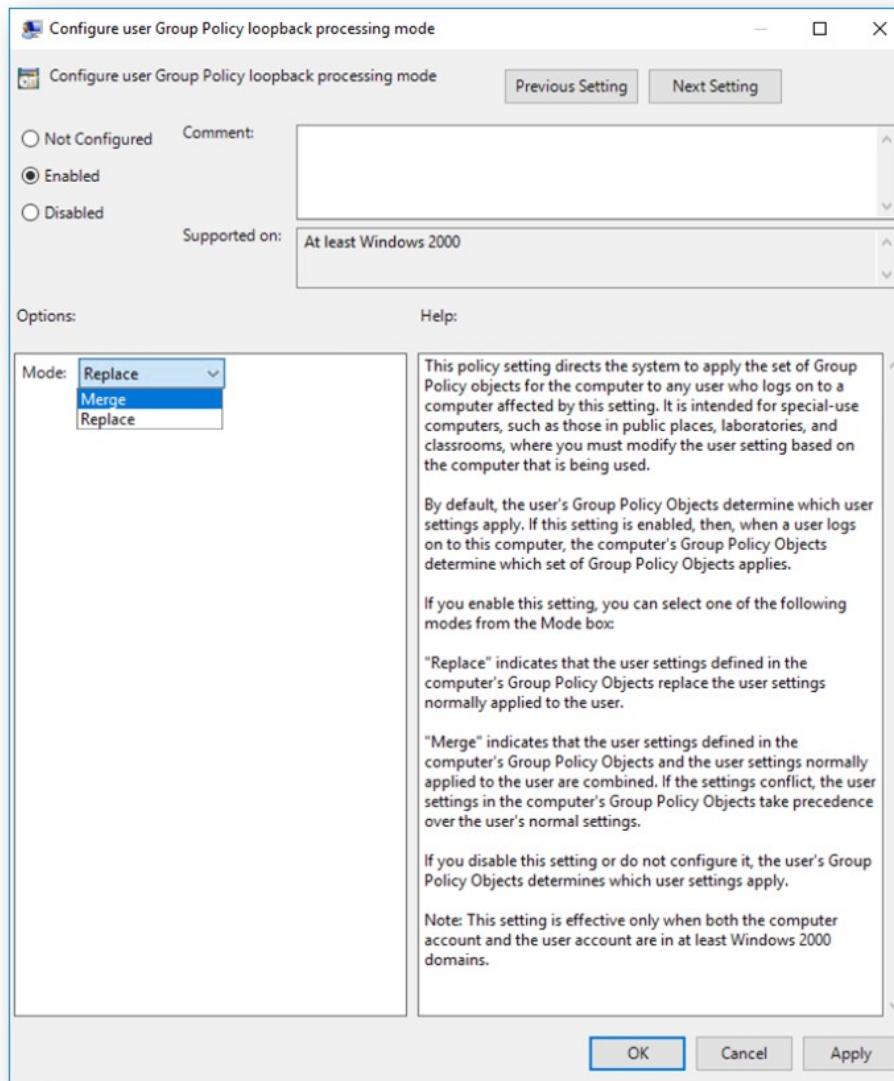


Figura 22: Loopback Processing Mode

Group Policy Preferences

Un discorso a parte lo meritano le **Group Policy Preferences**, introdotte in Windows Server 2008. Tramite le **Group Policy Preferences** è possibile distribuire e gestire le configurazioni del sistema operativo e degli applicativi, che non possono essere gestiti utilizzando le **Group Policy**. Alcuni esempi di Group Policy Preferences includono la mappatura dei dischi di rete, la creazione e la configurazione di operazioni pianificate, la creazione di utenti e gruppi locali e la modifica delle chiavi di registro utilizzate dalle applicazioni. La maggior parte delle volte offrono una valida alternativa agli script di logon degli utenti o di startup delle macchine.

Mentre infatti le GPO, grazie agli Administrative Templates, lavorano su chiavi di registro apposite (che contengono il ramo **Policies**) e che devono essere previste dallo sviluppatore, le Group Policy Preferences modificano le chiavi utilizzate dall'applicazione. Un esempio è ben descritto nell'articolo [Gestione centralizzata di Java Virtual Machine in ambienti distribuiti e con l'utilizzo delle Group Policy Preferences](#)

C'è da considerare anche che nonostante le Group Policy Preferences utilizzino lo stesso intervallo di refresh delle classiche Group Policy, non hanno esattamente lo stesso comportamento. Infatti, se scollegate una Group Policy da un Organizational Unit (OU), le configurazioni applicate dalla Group Policy verranno anch'esse rimosse. Invece le configurazioni applicate delle **Group Policy Preferences** rimarranno e dovranno essere eliminate con uno script oppure con una Group Policy Preferences che faccia l'operazione di rimozione (Delete).

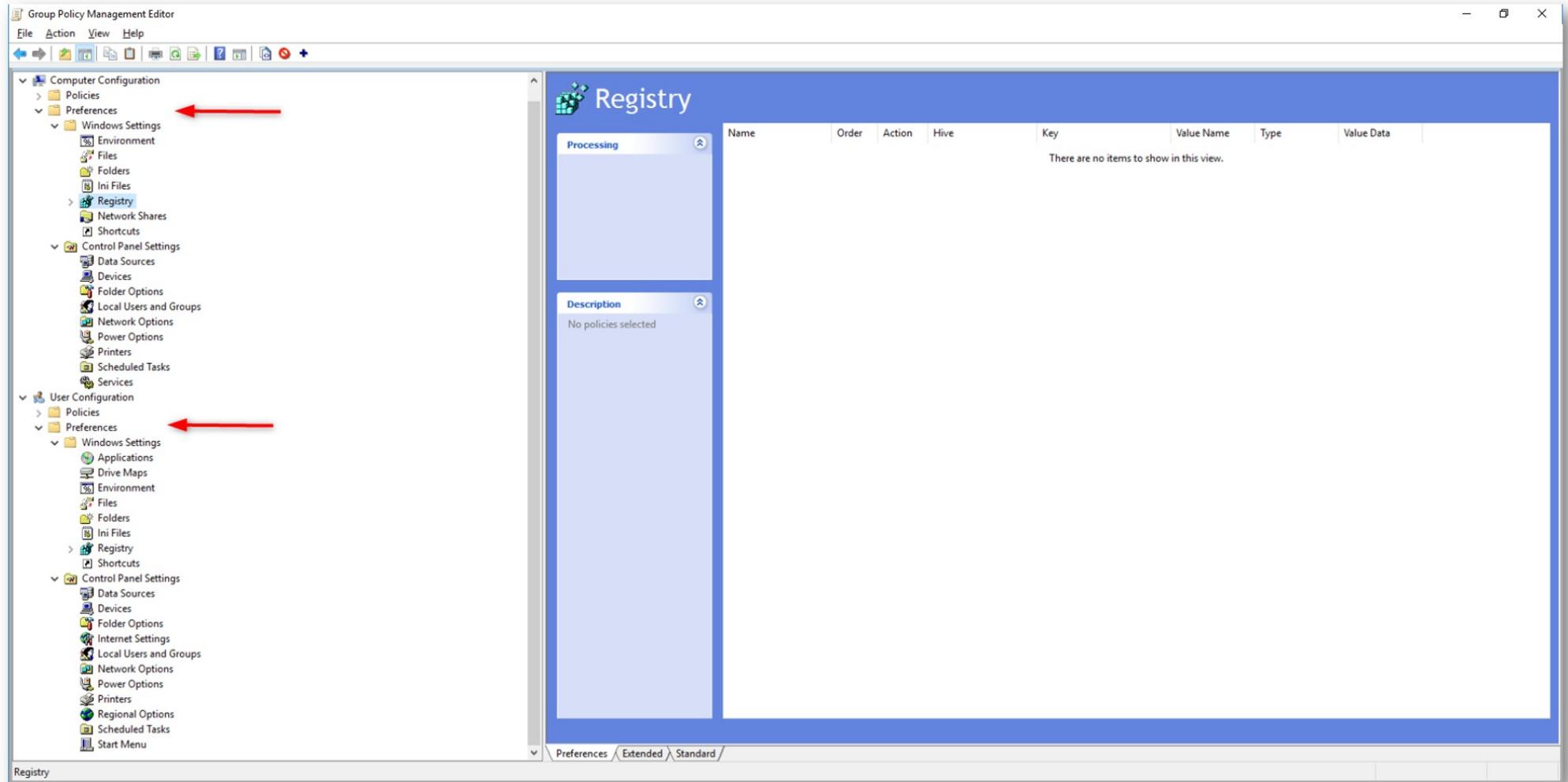


Figura 23: Group Policy Preferences

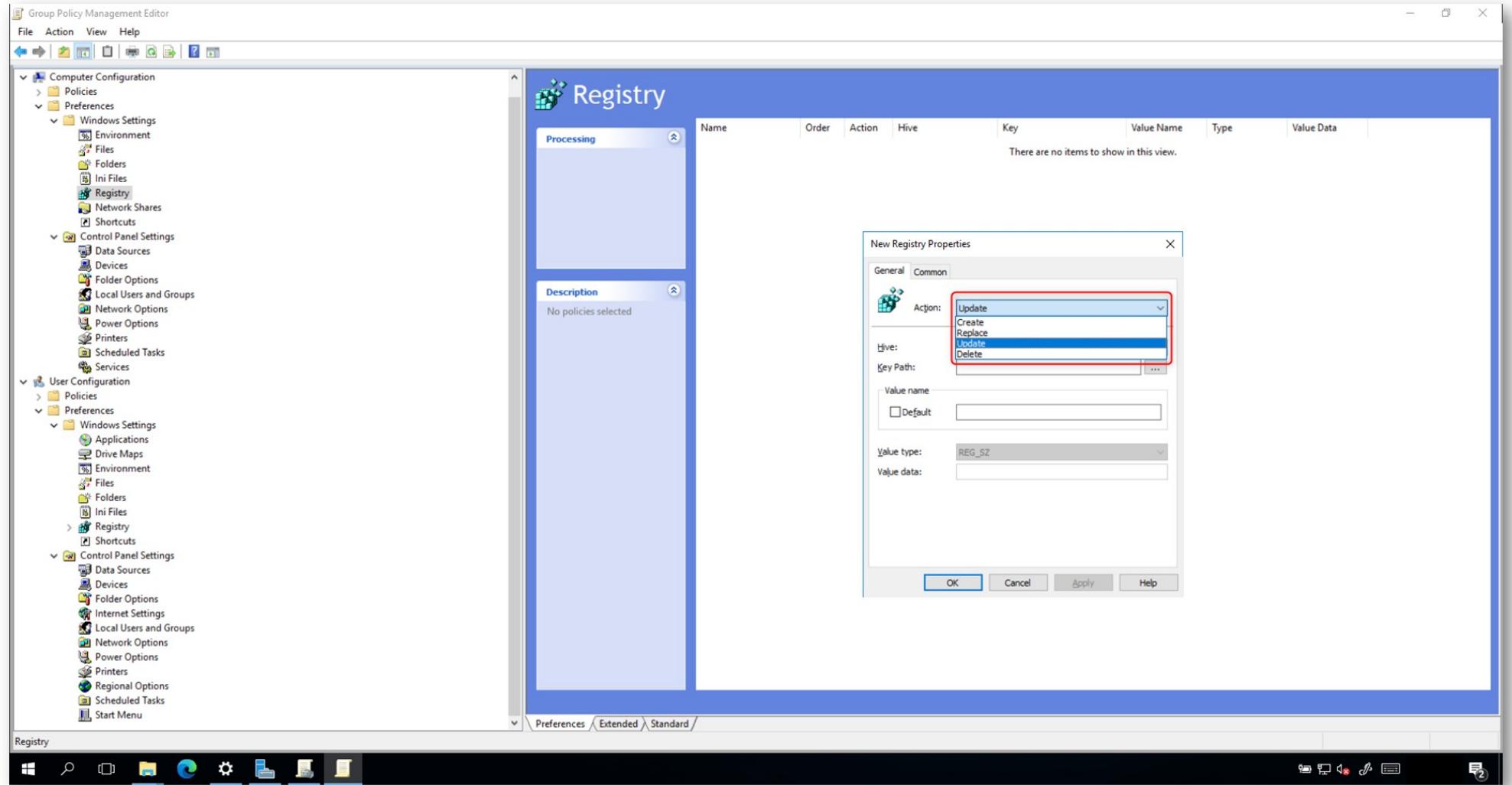


Figura 24: Operazioni consentite dalle configurazioni delle Group Policy Preferences

Decisamente interessante per quanto riguarda le **Group Policy Preferences** è la possibilità di poter applicare le configurazioni solo se si verificano determinate condizioni. Utilizzando infatti l'**Item-level targeting** possiamo decidere le caratteristiche della macchina di

destinazione della nostra configurazione, filtrando la lingua, il sistema operativo, il range di indirizzi IP della macchina, lo spazio disco disponibile, la RAM, ecc. come mostrato nella figura sotto:

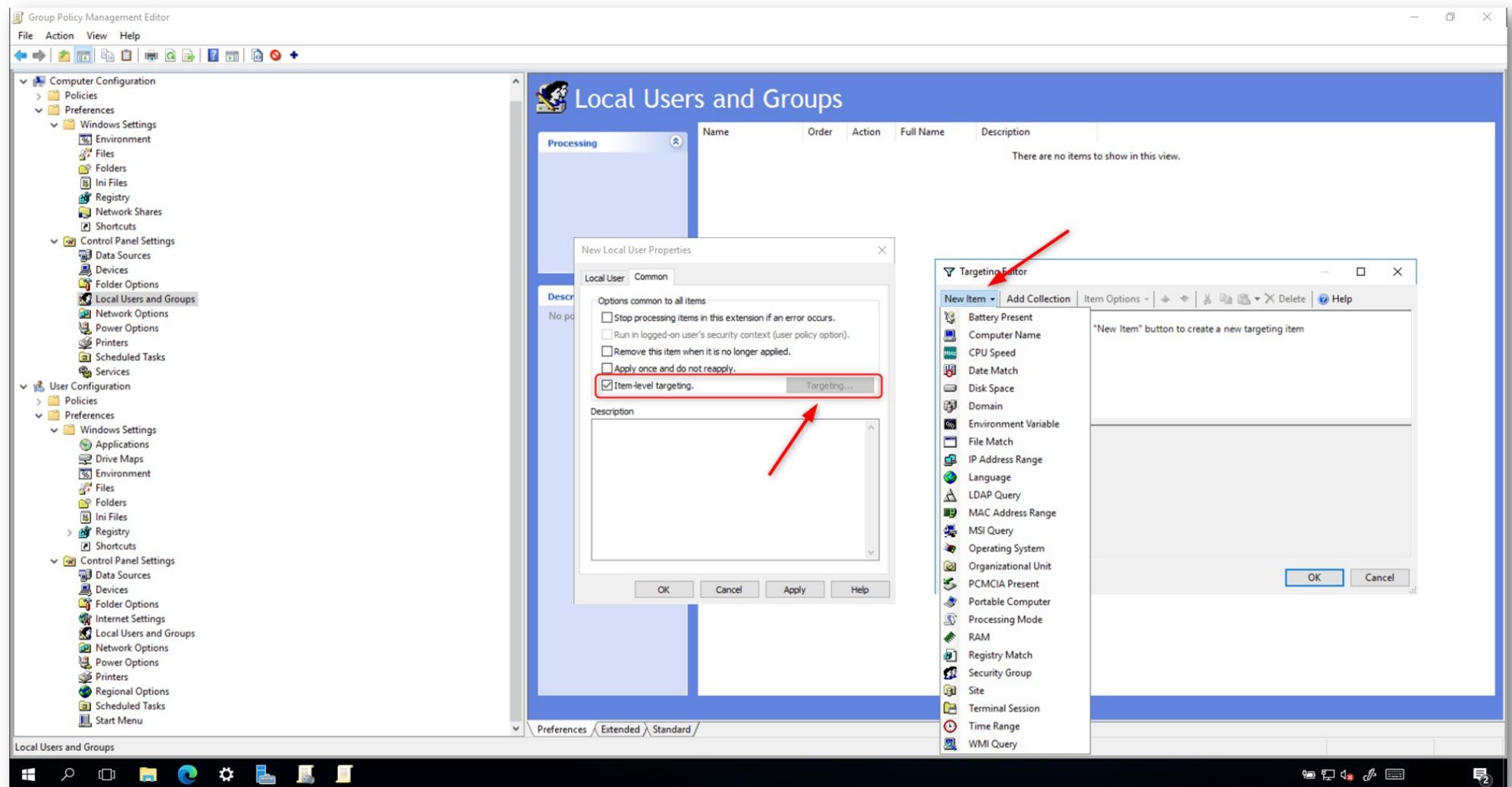


Figura 25: Configurazione dell'Item-level targeting per le Group Policy Preferences

Se nella definizione delle **Group Policy Preference** abbiamo a disposizione la funzione di **Item Level Targeting** per determinare con precisione dove applicare le impostazioni della GPO, in una Group Policy “tradizionale” questo strumento non è presente e dovremo impiegare altre modalità di selezione o filtraggio per quanto riguarda l’applicazione o meno di una determinata GPO. Nella guida Gestione avanzata delle Group Policy in Windows Server: Filtri WMI, backup e restore trovate maggiori informazioni.

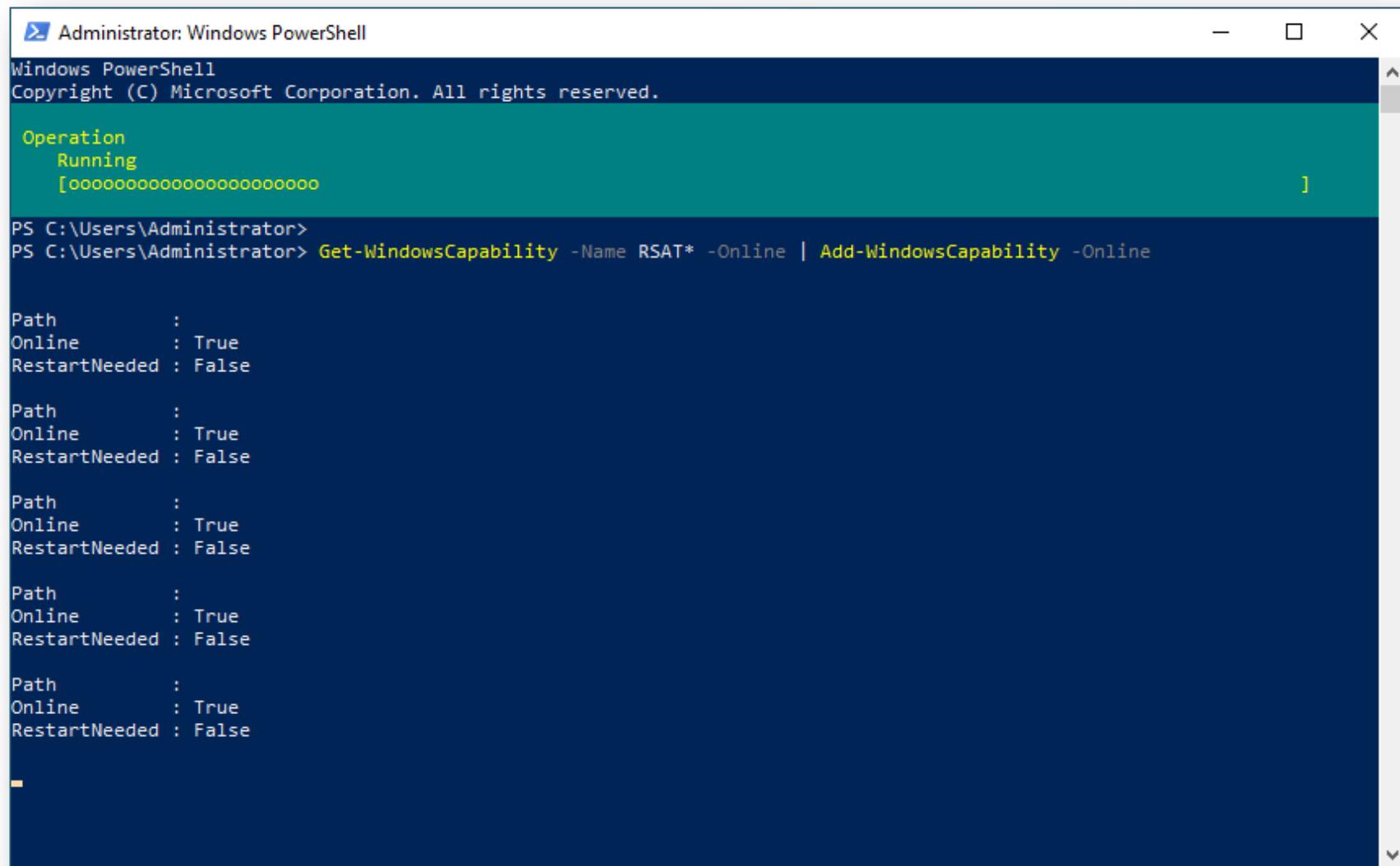
Amministrazione remota

Per motivi di sicurezza e per **best practice** è sempre raccomandato non gestire direttamente le configurazioni di dominio e accedere alle console di gestione collegandosi direttamente o in desktop remoto ai domain controller. Potete utilizzare delle postazioni di lavoro remote su cui avete installato i **Remote Server Administration Tool (RSAT)**. Potete scaricare i **Remote Server Administration Tool (RSAT)** utilizzando PowerShell oppure, a partire dall’aggiornamento di Windows 10 di ottobre 2018, utilizzando le Features on Demands, come vi ho già mostrato nell’articolo Installare le Features on Demand (FODs) in Windows 10.

Maggiori informazioni sono disponibili alla guida <https://docs.microsoft.com/it-it/windows-server/remote/remote-server-administration-tools>

Se volete utilizzare PowerShell e se la macchina con Windows 10 dispone di un collegamento ad Internet potete utilizzare il comando:

```
Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online
```



The screenshot shows an Administrator Windows PowerShell window. The command entered was `Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online`. The output indicates that multiple operations are running, each with a progress bar showing 100% completion. The properties for each operation are listed as follows:

```
Operation
  Running
  [ooooooooooooooooooooooo]

PS C:\Users\Administrator>
PS C:\Users\Administrator> Get-WindowsCapability -Name RSAT* -Online | Add-WindowsCapability -Online

Path      :
Online    : True
RestartNeeded : False

Path      :
Online    : True
RestartNeeded : False
```

Figura 26: Installazione dei Remote Server Administration Tools in Windows 10

Dopo aver installato gli RSAT (mettetevi comodi perché ci possono volere oltre 50 minuti!) potete aprire le console cliccando su Start e cercando Group Policy Management, come mostrato nella figura sotto. Ovviamente la console dovrà essere lanciata con i privilegi di un utente che possa gestire le GPO nel dominio.

NOTA: Se vi interessa installare solo la GRoup Policy Management console potete lanciare il comando **Get-WindowsCapability -Name Rsat.GroupPolicy.Management.Tools* -Online | Add-WindowsCapability -Online**

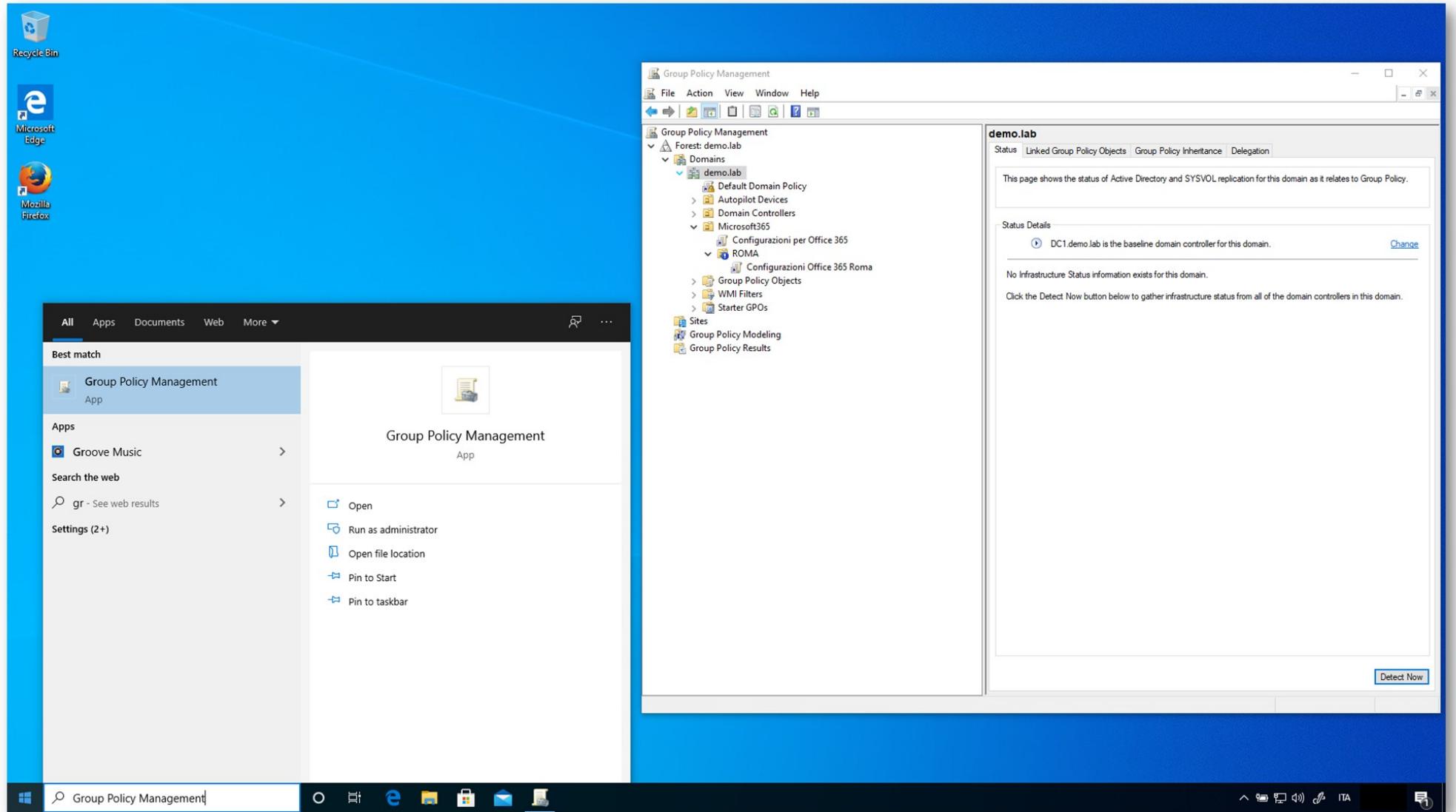


Figura 27: Group Policy Management console eseguita su Windows 10

Conclusioni

L'intento di questo articolo è quello di fissare solo alcuni concetti relativi alla Group Policy, che dovranno comunque essere approfonditi. Avere ben chiaro il comportamento e le modalità di applicazione delle GPO sono un ottimo strumento per configurare la nostra infrastruttura e per poter effettuare poi il troubleshooting in maniera corretta nel caso di problematiche.

FONTE:

[ICT POWER](#)