

Implementare i Read Only Domain Controller

di Nicola Ferrini

MCT – MCSA – MCSE – MCTS – MCITP

Introduzione

I Read Only Domain Controller (RODC) sono dei domain controller che hanno una copia in sola lettura del database di Active Directory. Uno dei principali motivi per avere un RODC è che un'organizzazione abbia una o più sedi remote in cui non ci siano amministratori locali per poter gestire un Domain Controller oppure non ci siano server room sicure dove poterli tenere.

Le caratteristiche principali di un RODC sono: database di AD in sola lettura, replica unidirezionale dai DC, caching delle credenziali dei soli utenti che si sono loggati sul RODC remoto.

Di default i RODC conservano le password del proprio account computer e la password dell'account KRBTGT, l'account Kerberos che si occupa di rilasciare i Ticket Granting Ticket (TGT) che vengono utilizzati per potersi autenticare ed accedere alle risorse di rete.

Nonostante sui RODC sia permesso installare il servizio DNS, tutti i record inseriti nella zona replicata sono di sola lettura.

E' necessario installare i RODC in Windows Server 2008 ma è possibile inserirli anche in un'infrastruttura di AD già esistente e basata su Windows Server 2003, a patto che il Primary Domain Controller (PDC) Emulator sia Windows Server 2008 e che il livello funzionale della foresta (forest functional level) sia almeno Windows Server 2003. I RODC possono anche essere Global Catalog, ma non possono avere nessun ruolo FSMO.

Password Replication Policies

Quando decidiamo di installare un RODC dobbiamo configurare una *password replication policy* su un DC del nostro dominio. Questa policy serve a stabilire se un RODC può o meno fare caching delle password degli utenti.

Poiché di default non viene messa nella cache del RODC nessuna password, questo assicura un notevole grado di sicurezza nel momento in cui dovessimo perdere un RODC a causa di un furto oppure a causa di un attacco informatico volto ad enumerare gli account della nostra infrastruttura AD.

Spiegazione

Installazione di un RODC

Vediamo adesso nello specifico come installare il ruolo RODC su un nuovo domain controller Windows Server 2008. Dal *Server Manager* aggiungiamo il nuovo ruolo (Figura 1):

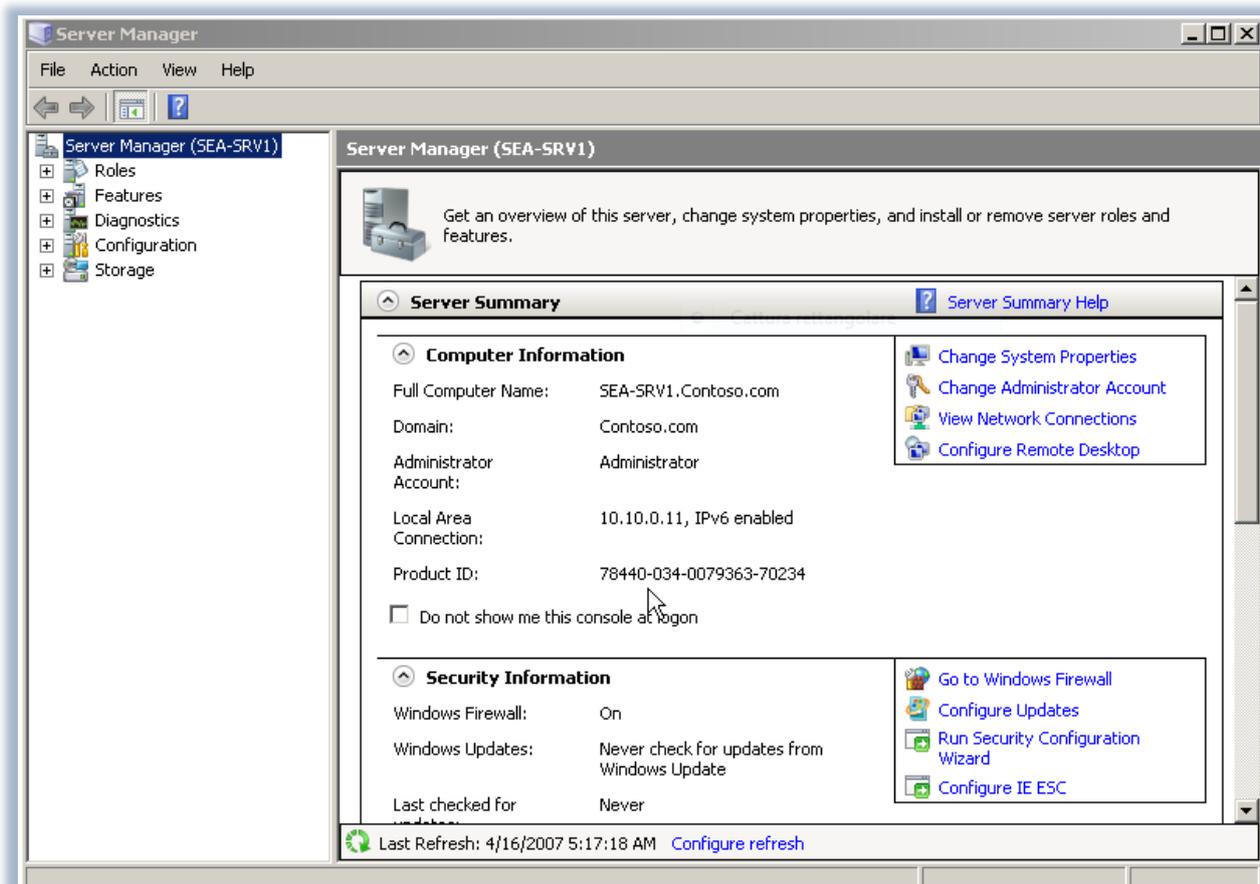


Figura 1 - Schermata iniziale del Server Manager

Dal menù di sinistra scegliamo di aggiungere un nuovo ruolo . In particolare scegliamo Active Directory Domain Services e seguiamo le indicazioni fornite dal wizard, che ci aiuterà a configurare il nostro server come Domain Controller (Figura 2).

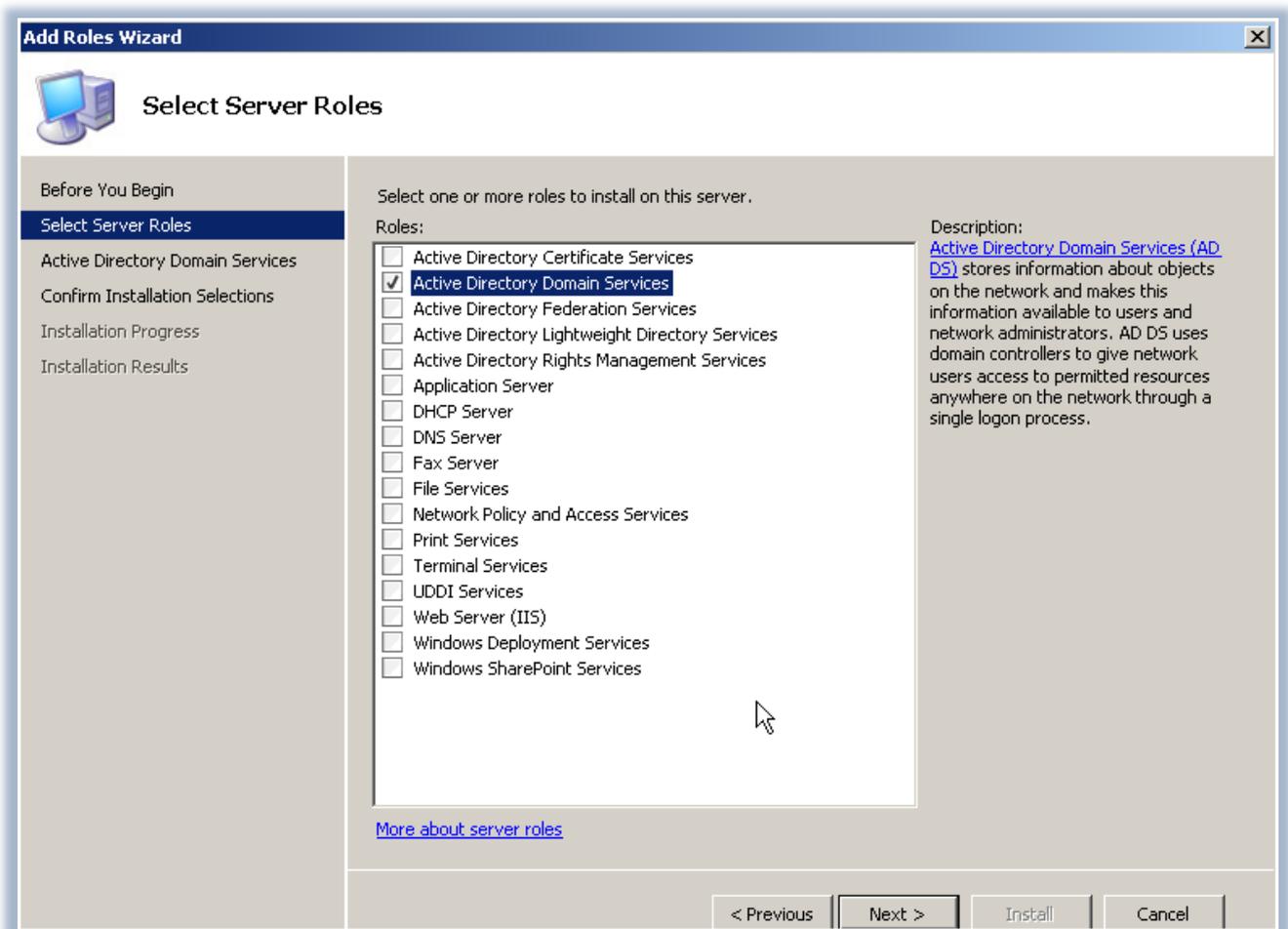


Figura 2 - Aggiunta dei servizi di Active Directory

Terminata l'installazione dei servizi possiamo lanciare da riga di comando il tool DCPROMO, come avveniva anche nelle precedenti versioni di Windows Server. Per poter installare un RODC dobbiamo selezionare l'opzione **Use advanced mode installation** (Figura 3). Se non selezioniamo questa opzione verrà installato un normale Domain Controller.



Figura 3 - Advanced mode installation

Il wizard ci chiederà successivamente se vogliamo installare il server per usarlo in una nuova foresta oppure aggiungerlo ad una foresta esistente (Figura 4).

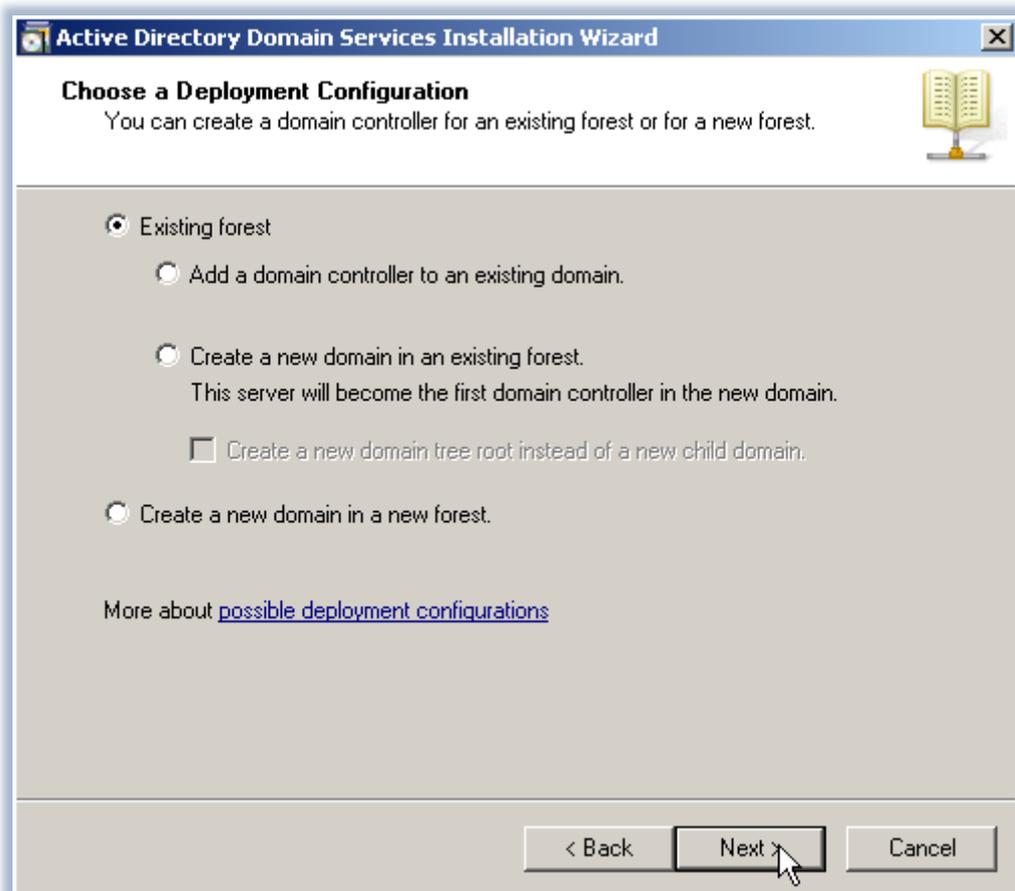


Figura 4 - Creazione del DC in una foresta esistente

Sarà necessario a questo punto inserire le credenziali di un utente che abbia i privilegi per installare gli Active Directory Domain Services sulla macchina, ma soprattutto che abbia le credenziali per aggiungere il nuovo domain controller al dominio esistente (Figura 5).

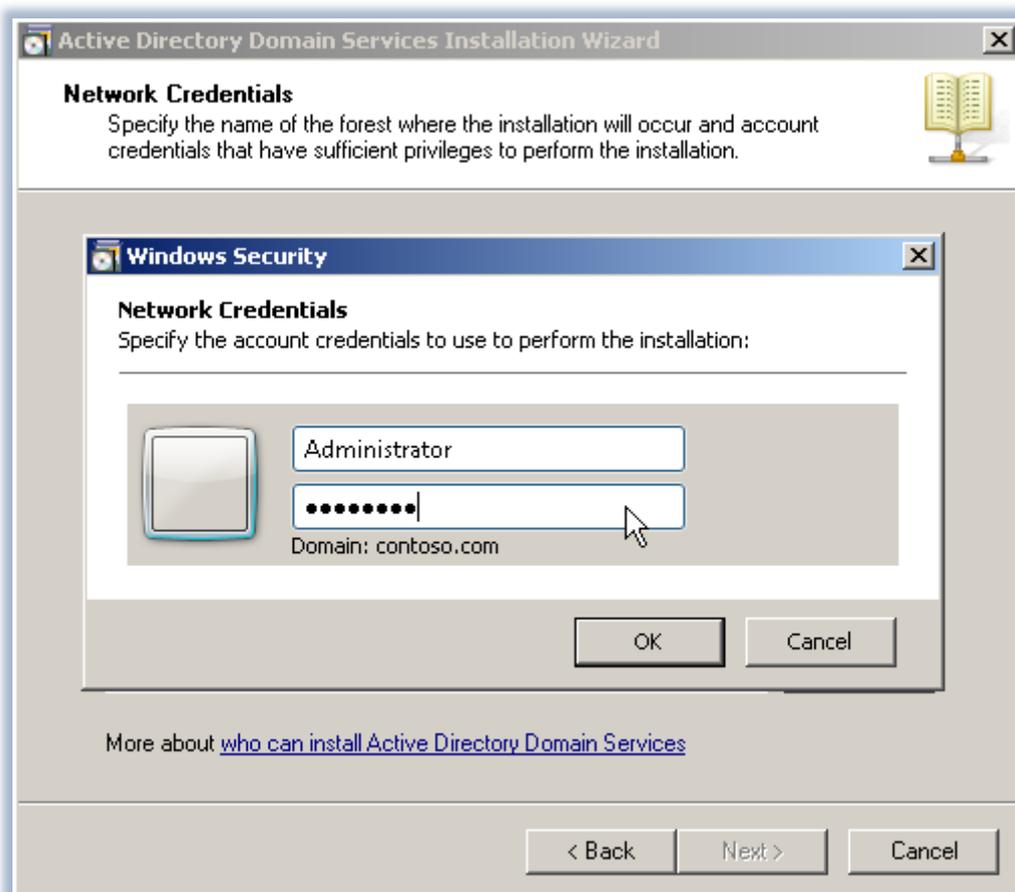


Figura 5 - Inserimento credenziali

Una volta scelto il dominio al quale vogliamo aggiungere il nuovo DC e il *site* in cui inserirlo, ci apparirà la schermata mostrata in Figura 6. Da questa schermata potremo scegliere se installare anche il servizio DNS e se vogliamo rendere il nuovo RODC un **Global Catalog**.

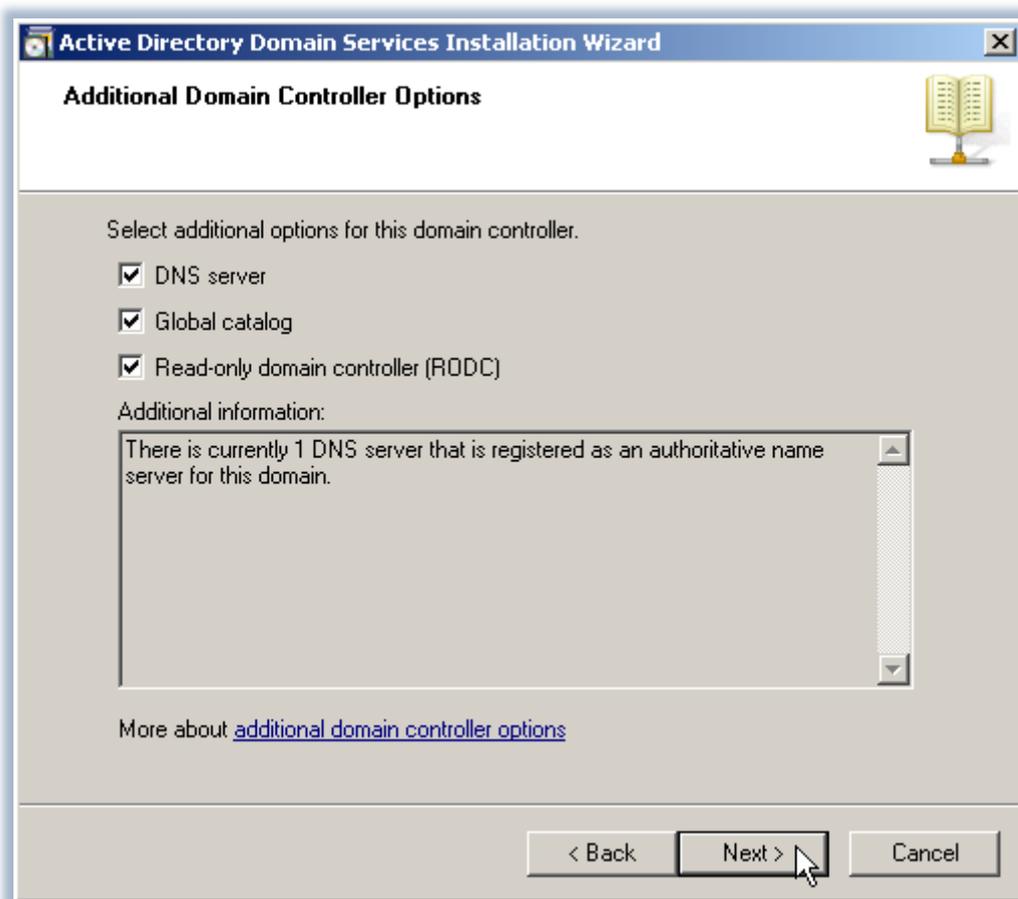


Figura 6 - Scelta delle opzioni

La schermata successiva , *Specify Password Policy* (Figura 7), ci permetterà di aggiungere o eliminare gli account le cui password non vogliamo vengano replicate sul RODC.

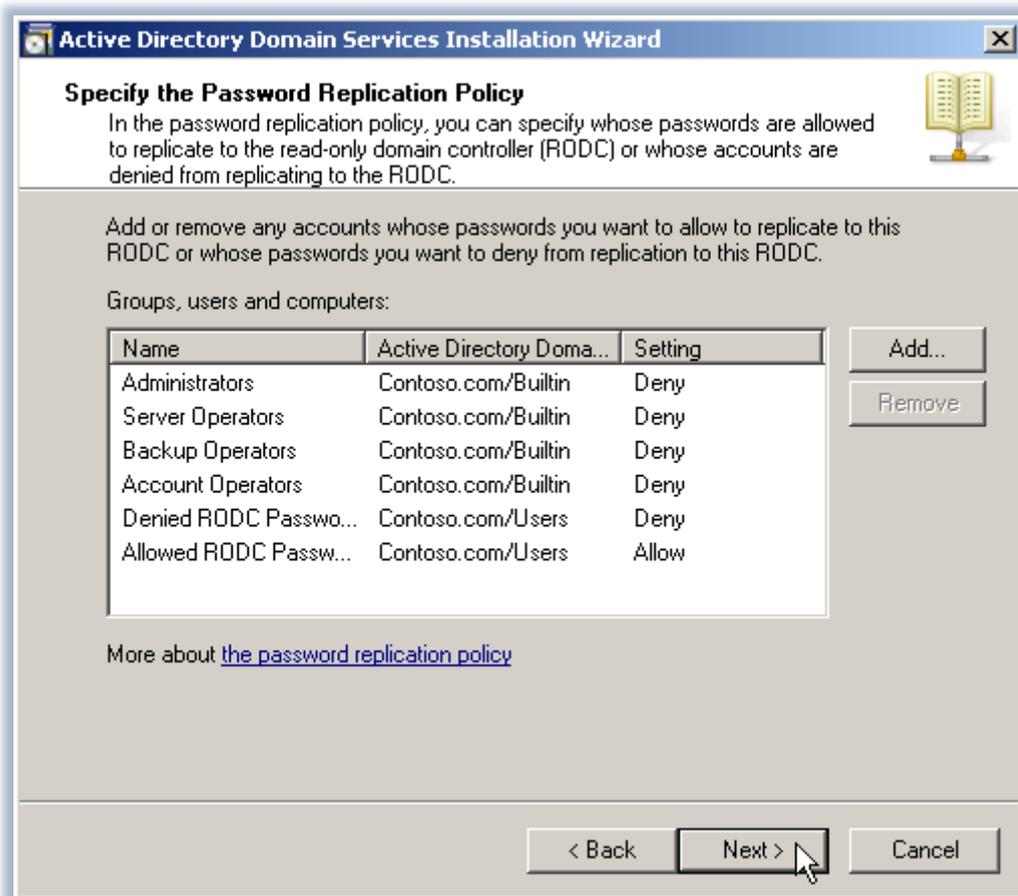


Figura 7 - Password Replication Policy

Altra significativa novità consiste nel fatto che è possibile selezionare un utente od un gruppo a cui siano concessi privilegi amministrativi sul server. In questo modo se ci dovessero essere problemi sul server e fosse necessario effettuare delle manutenzioni che richiedono privilegi amministrativi, avremmo delegato la possibilità di farlo a persone di nostra fiducia.

Come succedeva anche in passato abbiamo la possibilità di effettuare la promozione a DC di una macchina partendo dal backup di un altro DC, nel caso per esempio non fosse disponibile una connessione di rete (Figura 8).

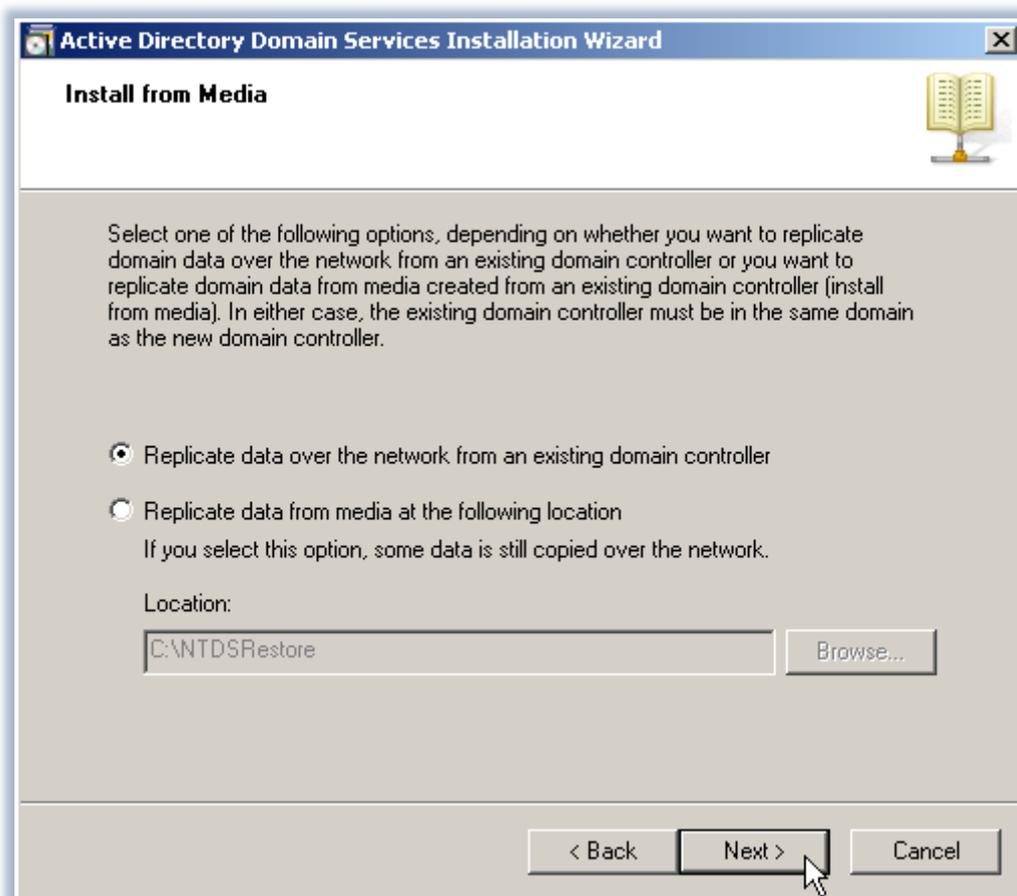


Figura 8 - Installazione da Media

Poiché la replica delle informazioni contenute nel database di Active Directory avviene attraverso la rete, durante l'installazione è possibile scegliere da quale altro domain controller effettuarla, in modo da assicurare il massimo delle performance, come mostrato in Figura 9.

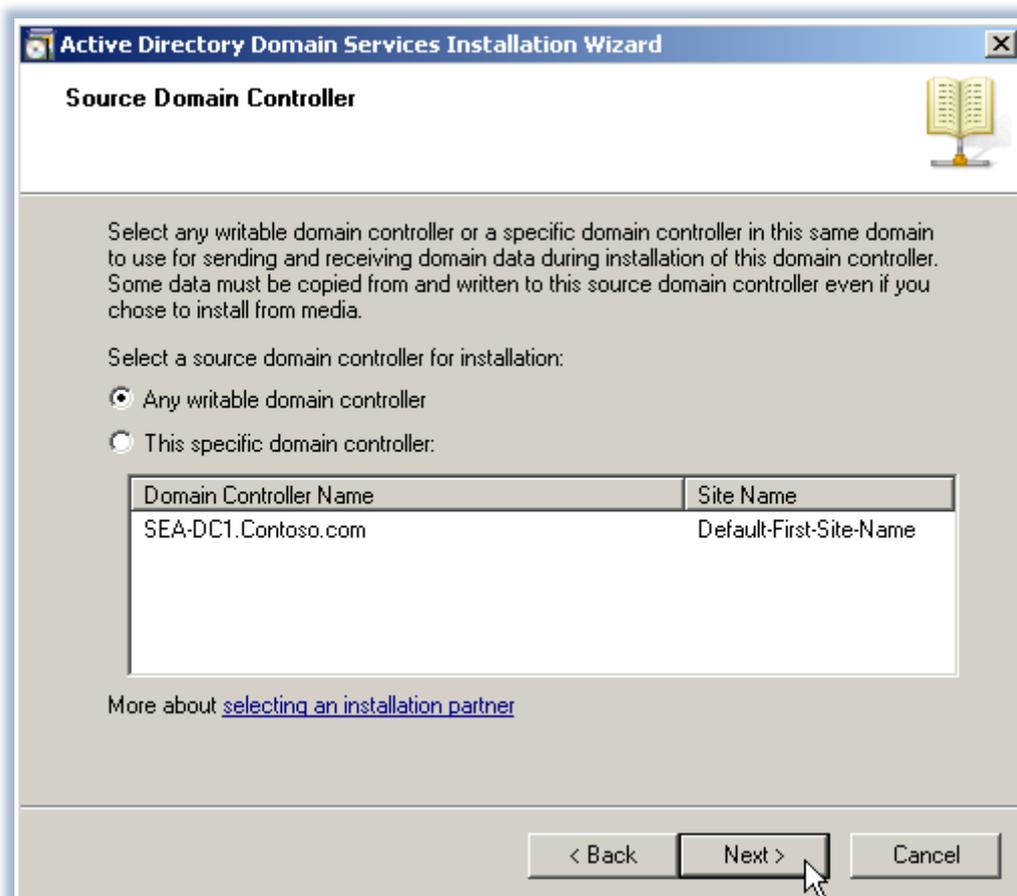


Figura 9 - Scelta del domain controller da cui effettuare la replica delle informazioni di AD

Nelle schermate successive verrà poi chiesto dove conservare i database di Active Directory (si consiglia per il massimo delle performance di memorizzare il database e i file di log su dischi diversi) e una password da poter utilizzare nell' Active Directory Restore Mode, proprio come avveniva nel passato.

A questo punto ci verrà presentata una schermata riassuntiva, che potrà essere utilizzata anche per esportare i settaggi in un file, in modo tale da poterlo utilizzare per realizzare una installazione non assistita di un nuovo RODC (Figura 10).

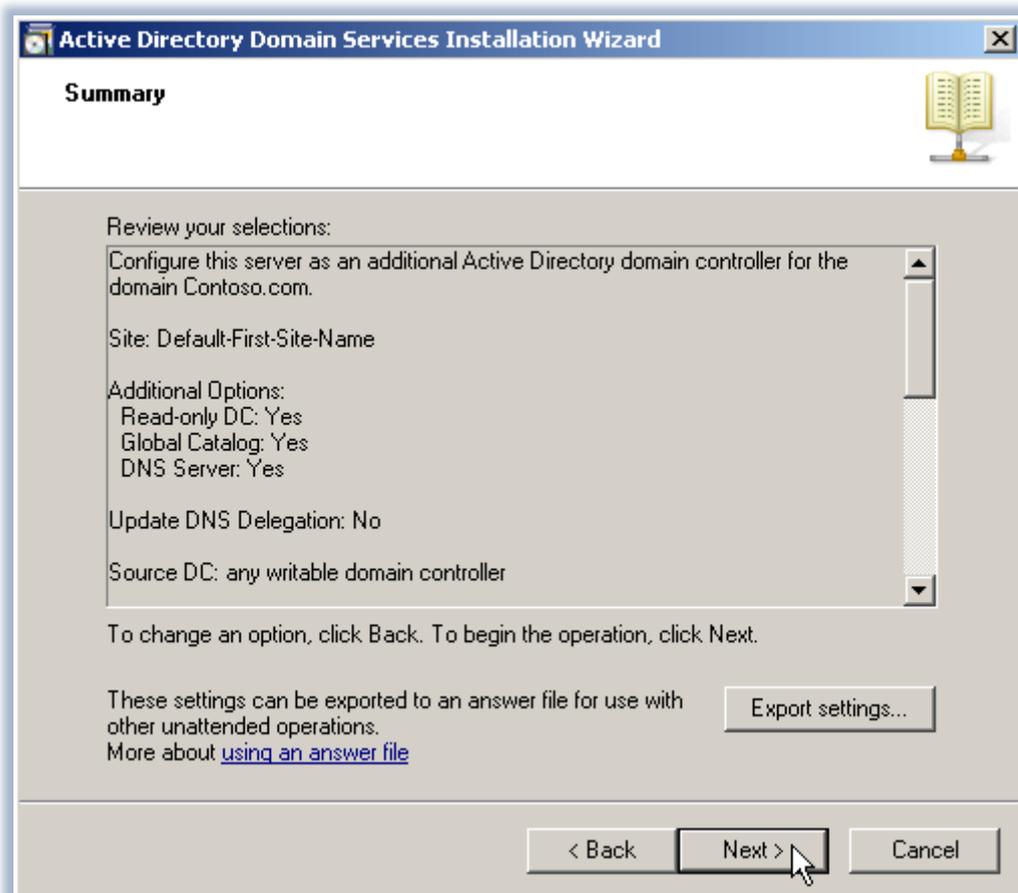


Figura 10 - Schermata riassuntiva

Per completare l'installazione sarà necessario riavviare il server. Non è possibile aggiungere o rimuovere ulteriori ruoli fino a quando il server non sarà riavviato.

Password Replication Policy

Per poter modificare la **Password Replication Policy** per il nuovo RODC appena creato sarà necessario utilizzare lo snap-in *Active Directory Users and Computers* su un altro Domain Controller (Figura 11). Infatti nessuna modifica può essere effettuata sui RODC. Il nostro RODC conserverà le password solo degli utenti i cui account appartengono ai vari gruppi che hanno i permessi settati ad **Allow**.

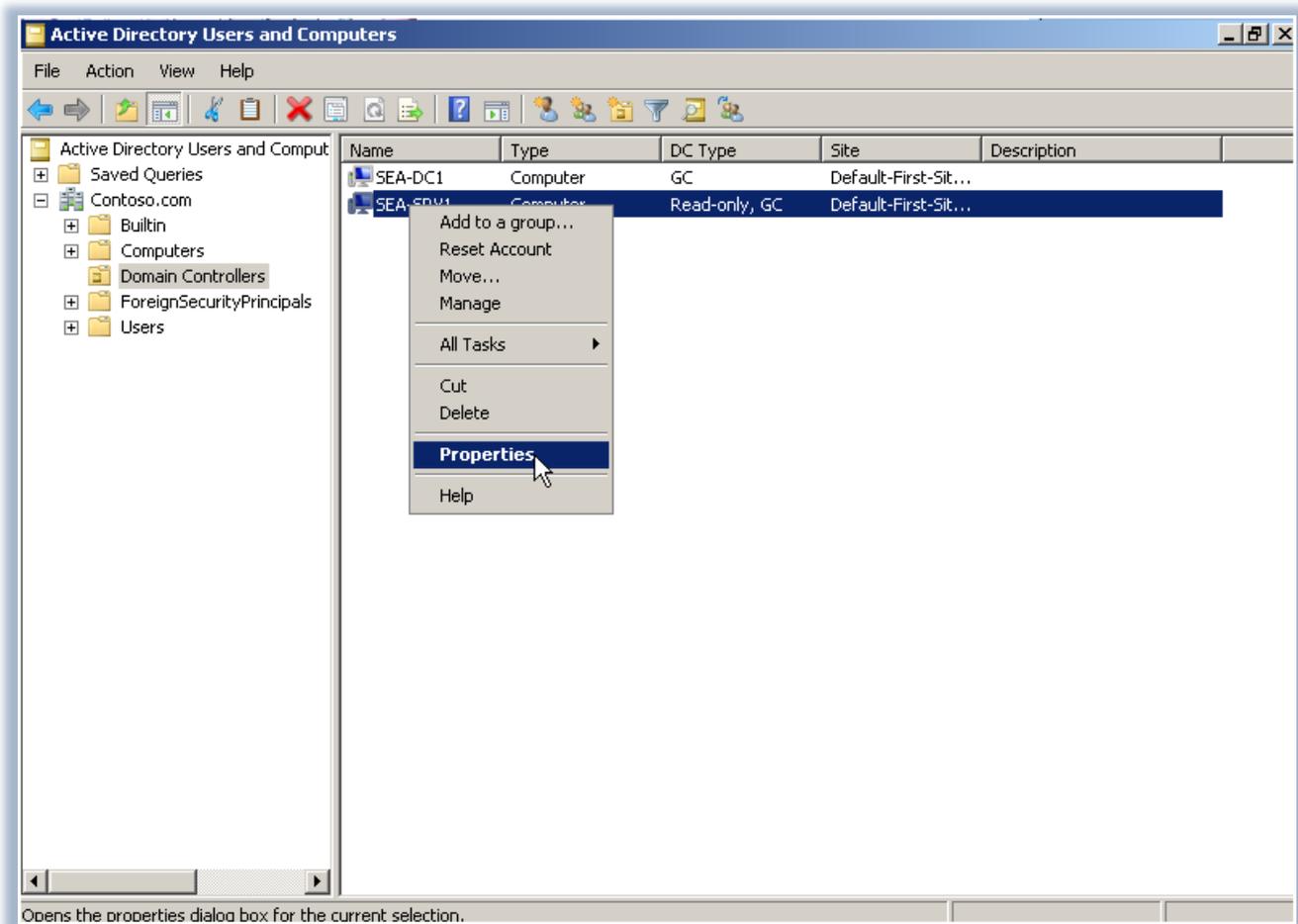


Figura 11 - Il RODC è stato aggiunto al dominio

Nelle proprietà del RODC sarà possibile in qualsiasi momento decidere a quali gruppi è permessa la replica delle password, come mostrato nella Figura 12:

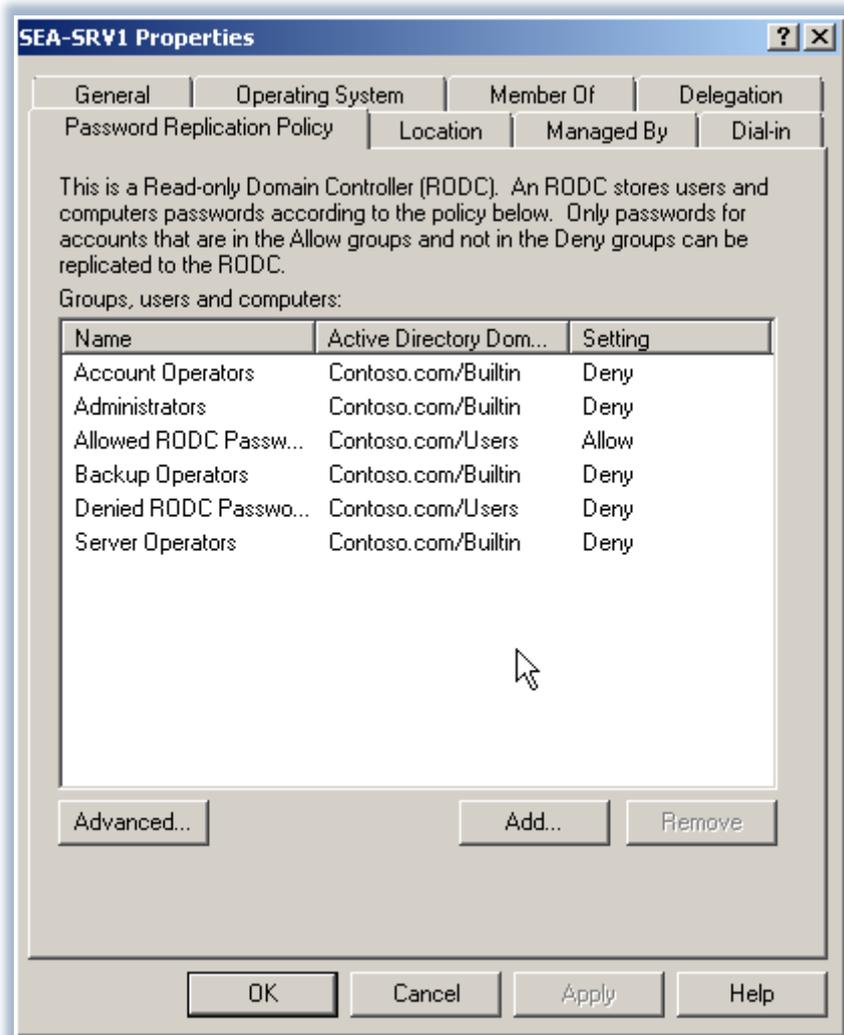


Figura 12 - Proprietà del RODC

Cliccando sul pulsante **Advanced** è possibile sapere in tempo reale quali sono gli utenti e i computer che hanno le password in cache sul RODC oppure gli account che si sono già autenticati (Figura 13). Questo perché è possibile, utilizzando il pulsante **Prepopulate Passwords**, inserire nel database del RODC alcuni account prima ancora che questi facciano il logon per la prima volta.

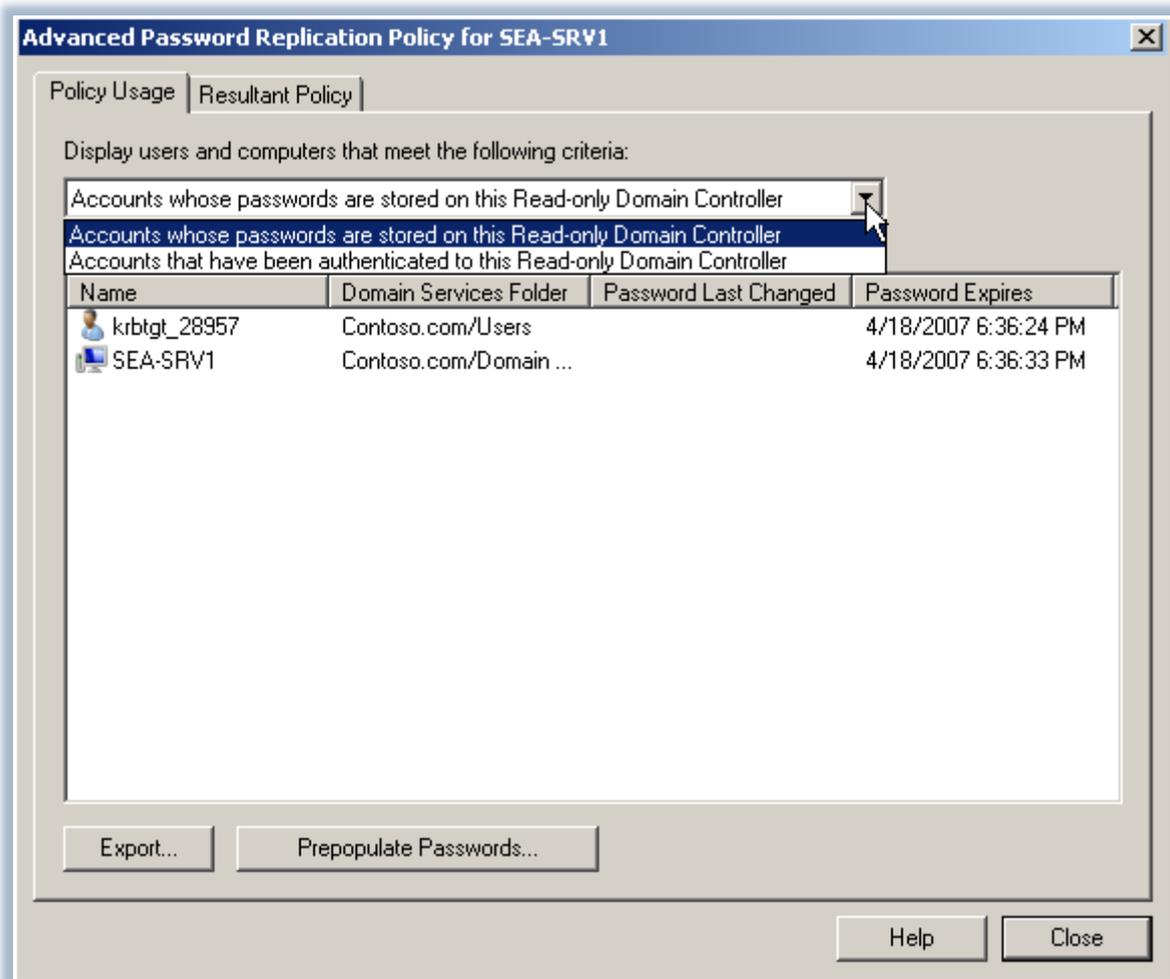


Figura 13: Proprietà avanzate del RODC

Sarà possibile in qualsiasi momento modificare la *Password Replication Policy* scegliendo dal pulsante **Add** quali gruppi inserire nella policy, come mostrato in Figura 14:



Figura 14 - Aggiunta dei nuovi account

Se il domain controller RODC viene perso o rubato, si potranno resettare le password degli accounts che erano conservate nella cache del Read Only Domain Controller (RODC). Questa operazione verrà effettuata utilizzando lo snap-in di *Active Directory Users and Computers* e scegliendo la voce **Elimina**.

A questo punto apparirà una finestra (Figura 15) dalla quale sceglieremo se resettare le password degli account compromessi oppure esportare la lista degli stessi account.

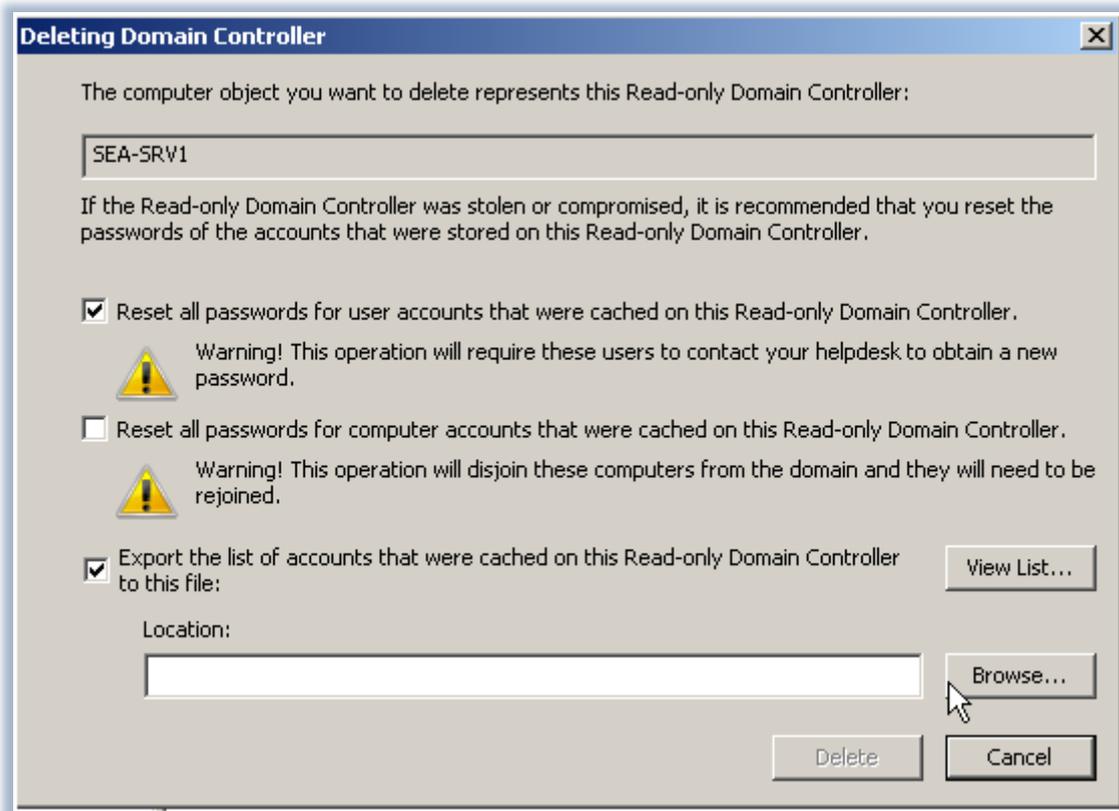
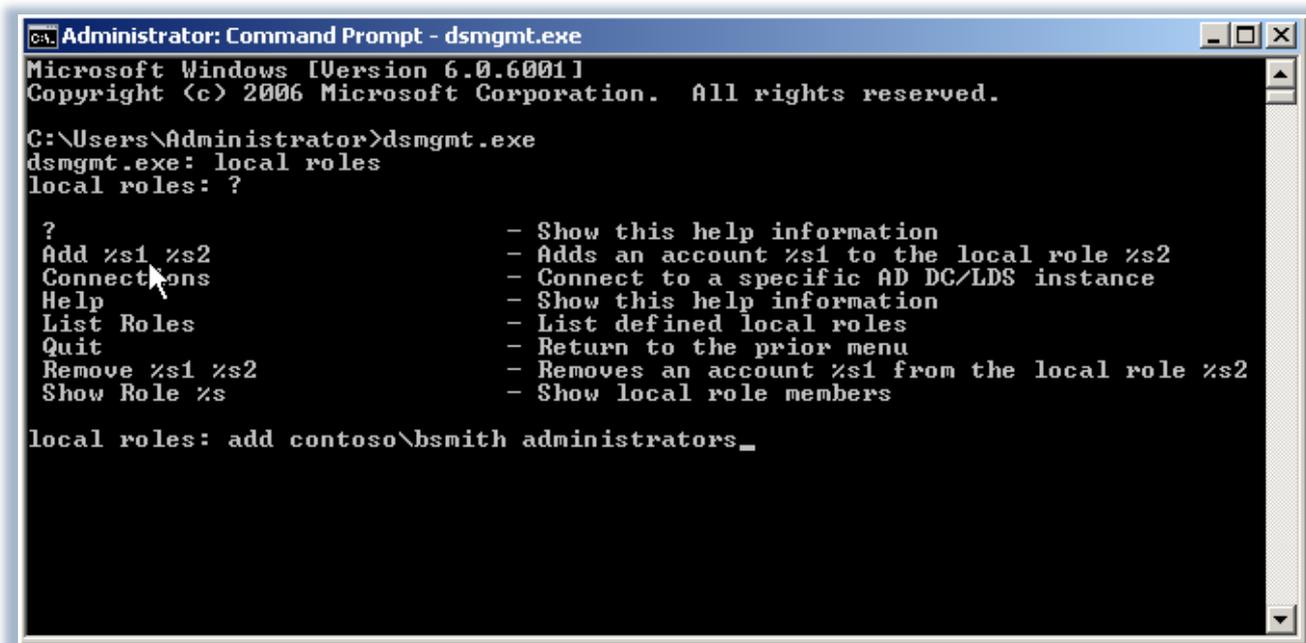


Figura 15 - Eliminazione di un RODC

Per poter configurare la separazione del ruolo amministrativo sul nostro RODC utilizzeremo il tool a riga di comando `dsmsgmt.exe`. Questo tool ci permetterà di modificare alcuni settaggi di AD che non sono accessibili in tool quali Active Directory Users and Computers. Utilizzando l'opzione **local roles** possiamo configurare le *administrative permission* sul RODC, come si vede in Figura 16



```
C:\Users\Administrator>dsmsgmt.exe
dsmsgmt.exe: local roles
local roles: ?

? - Show this help information
Add %s1 %s2 - Adds an account %s1 to the local role %s2
Connections - Connect to a specific AD DC/LDS instance
Help - Show this help information
List Roles - List defined local roles
Quit - Return to the prior menu
Remove %s1 %s2 - Removes an account %s1 from the local role %s2
Show Role %s - Show local role members

local roles: add contoso\bsmith administrators_
```

Figura 16 - Il comando DSMGMT

In questo esempio abbiamo aggiunto un utente con account **bsmith** del dominio **contoso.com** al gruppo *Administrators* locali della macchina.

Conclusioni

La nuova funzionalità offerta da Windows Server 2008 è sicuramente interessante ed offre una gestione avanzata ma soprattutto sicura dei Branch Office. Ritengo davvero utilissima la possibilità di poter resettare le password degli account compromessi e di poter esportare in un file le configurazioni in modo tale da poter avere delle “unattended installations” per gli altri RODC da installare nell’infrastruttura di dominio.