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).

Add Roles Wizard		<u>×</u>	1
Select Server Ro	les		
Before You Begin Select Server Roles Active Directory Domain Services Confirm Installation Selections Installation Progress Installation Results	Select one or more roles to install on this server. Roles: Active Directory Certificate Services Active Directory Federation Services Active Directory Federation Services Active Directory Rights Management Services Bervices Bervice	Description: Active Directory Domain Services (AD) DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.	
	< Previous Next	> Install Cancel	

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.

\overline Active Directory Domain	Services Installation Wizard	×
	Welcome to the Active Directory Domain Services Installation Wizard	
	This wizard helps you install Active Directory Domain Services (AD DS) on this server, making the server an Active Directory domain controller. To continue, click Next.	
	Use advanced mode installation Learn more about the additional options that are available in <u>advanced mode installation</u> .	
	More about <u>Active Directory Domain Services</u>	
	< Back Next > Cancel	

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).

Active Directory Domain Services Installation Wizard	×
Choose a Deployment Configuration You can create a domain controller for an existing forest or for a new forest.	
Existing forest	
C Add a domain controller to an existing domain.	
Create a new domain in an existing forest.	
This server will become the first domain controller in the new domain.	
Create a new domain tree root instead of a new child domain.	
C Create a new domain in a new forest.	
More about possible deployment configurations	
< Back Next >	Cancel

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).

a Active Directory Domain Services Installation Wizard	×	
Network Credentials Specify the name of the forest where the installation will occur and account credentials that have sufficient privileges to perform the installation.		
The security	×	
Network Credentials Specify the account credentials to use to perform the installation: Administrator ••••••• Domain: contoso.com	-	
OK Cancel		
More about who can install Active Directory Domain Services		
< Back Next > 0	Cancel	

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**.

Active Directory Domain Services Installation Wizard	×
Additional Domain Controller Options	
Select additional options for this domain controller.	
DNS server	
🔽 Global catalog	
Read-only domain controller (RODC)	
Additional information:	
There is currently 1 DNS server that is registered as an authoritative name server for this domain.	
More about additional domain controller options	
< Back Next >	Cancel

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.

a Active Directory Domain Se	ervices Installation Wiz	ard	X	
Specify the Password Replication Policy In the password replication policy, you can specify whose passwords are allowed to replicate to the read-only domain controller (RODC) or whose accounts are denied from replicating to the RODC.				
Add or remove any accounts whose passwords you want to allow to replicate to this RODC or whose passwords you want to deny from replication to this RODC. Groups, users and computers:				
Name	Active Directory Doma	Setting	Add	
Administrators	Contoso.com/Builtin	Deny		
Server Operators	Contoso.com/Builtin	Deny	Remove	
Backup Operators	Contoso.com/Builtin	Deny		
Account Operators	Contoso.com/Builtin	Deny		
Denied RODC Passwo	Contoso.com/Users	Deny		
Allowed RODC Passw	Contoso.com/Users	Allow		
More about the password re	eplication policy			
	< Bac	k Next >	Cancel	

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).

area Active Directory Domain Services Installation Wizard	×
Install from Media	
Select one of the following options, depending on whether you want to replicate domain data over the network from an existing domain controller or you want to replicate domain data from media created from an existing domain controller (install from media). In either case, the existing domain controller must be in the same domain as the new domain controller.	
 Replicate data over the network from an existing domain controller Replicate data from media at the following location If you select this option, some data is still copied over the network. Location: C:\NTDSRestore 	
< Back Next > Ca	incel

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.

C Active Directory Domain Services Installation Wizard	×
Source Domain Controller	
Select any writable domain controller or a specific domain co to use for sending and receiving domain data during installati Some data must be copied from and written to this source do chose to install from media. Select a source domain controller for installation: Any writable domain controller This specific domain controller:	ntroller in this same domain on of this domain controller. main controller even if you
Domain Controller Name	Site Name
SEA-DC1.Contoso.com	Default-First-Site-Name
More about <u>selecting an installation partner</u>	
< Back	Next > Cancel

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).

\overline Active Directory Domain Services Installation Wizard	X
Summary	
Review your selections: Configure this server as an additional Active Directory domain controller for the domain Contoso.com. Site: Default-First-Site-Name Additional Options: Read-only DC: Yes Global Catalog: Yes DNS Server: Yes Update DNS Delegation: No Source DC: any writable domain controller To change an option, click Back. To begin the operation, click Next.	
These settings can be exported to an answer file for use with other unattended operations. More about <u>using an answer file</u>	
< Back Next > Ca	ncel

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:

SEA-SRV1 Properties		<u>? ×</u>		
General Operating System Member Of Delegation Password Replication Policy Location Managed By Dial-in This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC. Groups, users and computers;				
Name	Active Directory Dom	Setting		
Account Operators	Contoso.com/Builtin	Deny		
Administrators	Contoso.com/Builtin	Deny		
Allowed RODC Passw	Contoso.com/Users	Allow		
Backup Operators	Contoso.com/Builtin	Deny		
Denied RODC Passwo	Contoso.com/Users	Deny		
Server Uperators	Contoso.com/Builtin	Deny		
	R			
Advanced	Add	Remove		
ОК	Cancel	Apply Help		

Figura 12 - Proprietà del RODC

Cliccando sul pulsante **Advanced** è possibile sapere in tempo reale quali sono gli utenti è 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 **Prepolulate Passwords**, inserire nel database del RODC alcuni account prima ancora che questi facciano il logon per la prima volta.

dvanced Password F	Replication Policy for SEA-SR	¥1	×
Policy Usage Result	ant Policy		
Display users and co	mputers that meet the following crit	iteria:	
Accounts whose pa	sswords are stored on this Read-or	nly Domain Controller	
 Accounts whose pase Accounts that have 	sswords are stored on this Read-or been authenticated to this Read-o	nly Domain Controller	
Name	Domain Services Folder	Password Last Changed Password Expires	
👗 krbtgt_28957	Contoso.com/Users	4/18/2007 6:36:24 PM	
💽 SEA-SRV1	Contoso.com/Domain	4/18/2007 6:36:33 PM	
Export	Prepopulate Passwords		
		Help Close	

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 utlizzando 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.

Dele	ting Domain Controller	×
	The computer object you want to delete represents this Read-only Domain Controller:	
	SEA-SRV1	
	If the Read-only Domain Controller was stolen or compromised, it is recommended that you reset the passwords of the accounts that were stored on this Read-only Domain Controller.	
	🗹 Reset all passwords for user accounts that were cached on this Read-only Domain Controller.	
	Warning! This operation will require these users to contact your helpdesk to obtain a new password.	
	\square Reset all passwords for computer accounts that were cached on this Read-only Domain Controller.	
	Warning! This operation will disjoin these computers from the domain and they will need to b rejoined.	e
	Export the list of accounts that were cached on this Read-only Domain Controller View List	1
	Location:	
	Browse	
	Delete Cancel]

Figura 15 - Eliminazione di un RODC

Per poter configurare la separazione del ruolo amministrativo sul nostro RODC utilizzeremo il tool a riga di comando dsmgmt.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



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 sopratutto 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.