

READ ONLY DOMAIN CONTROLLER

RODCs offer improved security, faster logon times, and more efficient access to local resources. RODC administration can be delegated to users or groups that do not have administrative rights in the domain.

- **benefits of using an RODC**
- **Installing an RODC in a branch office.**
- **Configuring a Password Replication Policy.**
- **Using Administrative Role Separation.**

- **RODC's provide 3 main security benefits which satisfy needs of many branch offices.**
 - **By default RODC's do not maintain password properties for any users.**
 - **No changes can be made to the AD database on the RODC.**
 - **RODC's have local a Administrator group which allows users in the branch office to administrate the computer without having privileges to the domain.**

Installing a Read Only Domain Controller.

This is going to be the same process we used to install a Domain Controller.

1. Go to Add Roles
2. Active Directory Domains and Services and install the role.
3. Launch the dcpromo wizard





Windows Server 2008 domain controllers have a new more secure default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0." This setting prevents Microsoft Windows and non-Microsoft SMB "clients" from using weaker NT 4.0 style cryptography algorithms when establishing security channel sessions against Windows Server 2008 domain controllers. As a result of this new default, operations or applications that require a security channel serviced by Windows Server 2008 domain controllers might fail.

Platforms impacted by this change include Windows NT 4.0, as well as non-Microsoft SMB "clients" and network-attached storage (NAS) devices that do not support stronger cryptography algorithms. Some operations on clients running versions of Windows earlier than Vista with Service Pack 1 are also impacted, including domain join operations performed by the Active Directory Migration Tool or Windows Deployment Services.

For more information about this setting, see Knowledge Base article 942564 (<http://go.microsoft.com/fwlink/?LinkId=104751>).

< Back

Next >

Cancel

Choose a Deployment Configuration

You can create a domain controller for an existing forest or for a new forest.



- Existing forest
 - 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 in a new forest

More about [possible deployment configurations](#)

< Back

Next >

Cancel

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.



Type the name of any domain in the forest where you plan to install this domain controller:

Specify the account credentials to use to perform the installation:

My current logged on credentials (GLOBOMANTICS\administrator)

Alternate credentials:

More about [who can install Active Directory Domain Services](#)

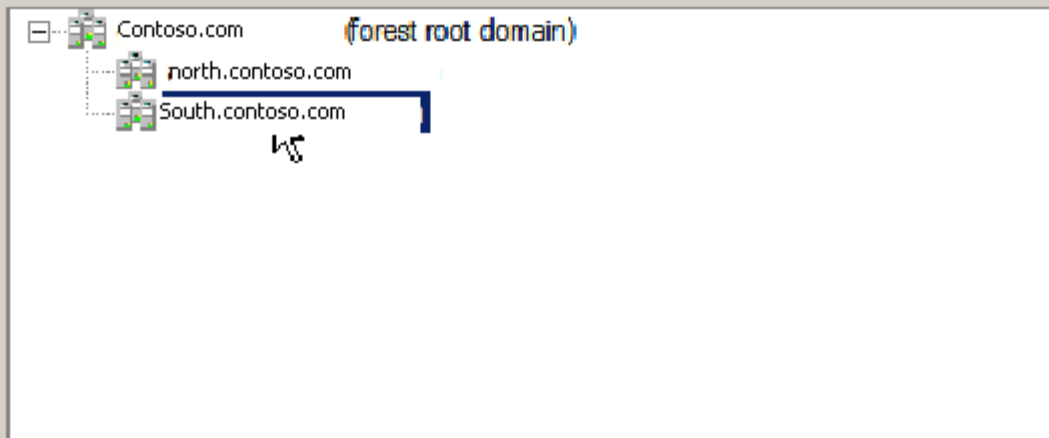
Active Directory Domain Services Installation Wizard

Select a Domain



Select a domain for this additional domain controller.

Domains:



Active Directory Domain Services Installation Wizard

Select a Site

Select a site for the new domain controller.



Use the site that corresponds to the IP address of this computer.

Sites:

Site	Description
Default-First-Site-Name	Used to control replication from office to office

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

Delegation of RODC Installation and Administration



The user or group that you specify will be able to attach a server to the RODC account that you are creating now and complete the RODC installation. They will also have local administrative permissions on this RODC.

To simplify administration, you should specify a group and then add individual users to the group.

Group or user:

Set...

Other accounts can also inherit permissions on this RODC, but those accounts will not have local administrative permissions on this RODC unless you add those accounts explicitly.

More about [delegation for read-only domain controller installation and administration](#)

pre-staging of RODC installation

< Back

Next >

Cancel

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.



For better performance and recoverability, store the database and log files on separate volumes.

Database folder:

Log files folder:

SYSVOL folder:

More about [placing Active Directory Domain Services files](#)



The Directory Services Restore Mode Administrator account is **different** from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

Password:

Confirm password:

More about [Directory Services Restore Mode password](#)

< Back

Next >

Cancel

Review your selections:

Configure this server as a domain na.globomantics.

Site: Default-First-Site-Name

Additional Options:

Read-only domain controller: No
Global catalog: Yes
DNS Server: Yes

Update DNS Delegation: No

Source domain controller: No

To change an option, click the option.

These settings can be exported to a file for use in other unattended operations.
More about [using an answer file](#).

Active Directory Domain Services Installation Wizard

The wizard is configuring Active Directory Domain Services. This process can take from a few minutes to several hours, depending on your environment and the options that you selected.



Waiting for DNS installation to finish



Cancel

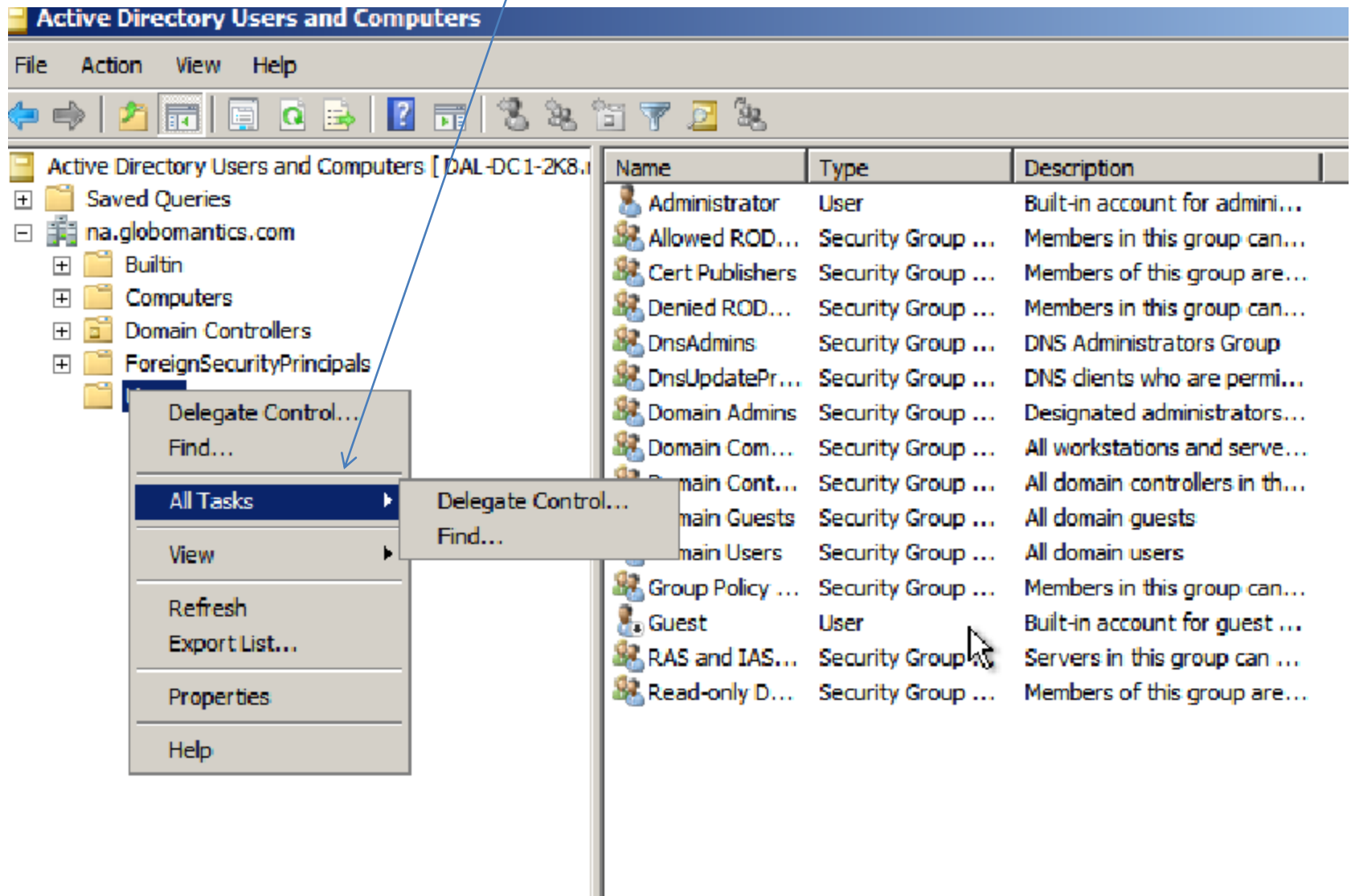
Reboot on completion

< Back

Next >

Cancel

RODC Note that all the objects are missing we cannot create anything **new**. The **NEW** tab missing.



Changes can only be made on the writable domain controller

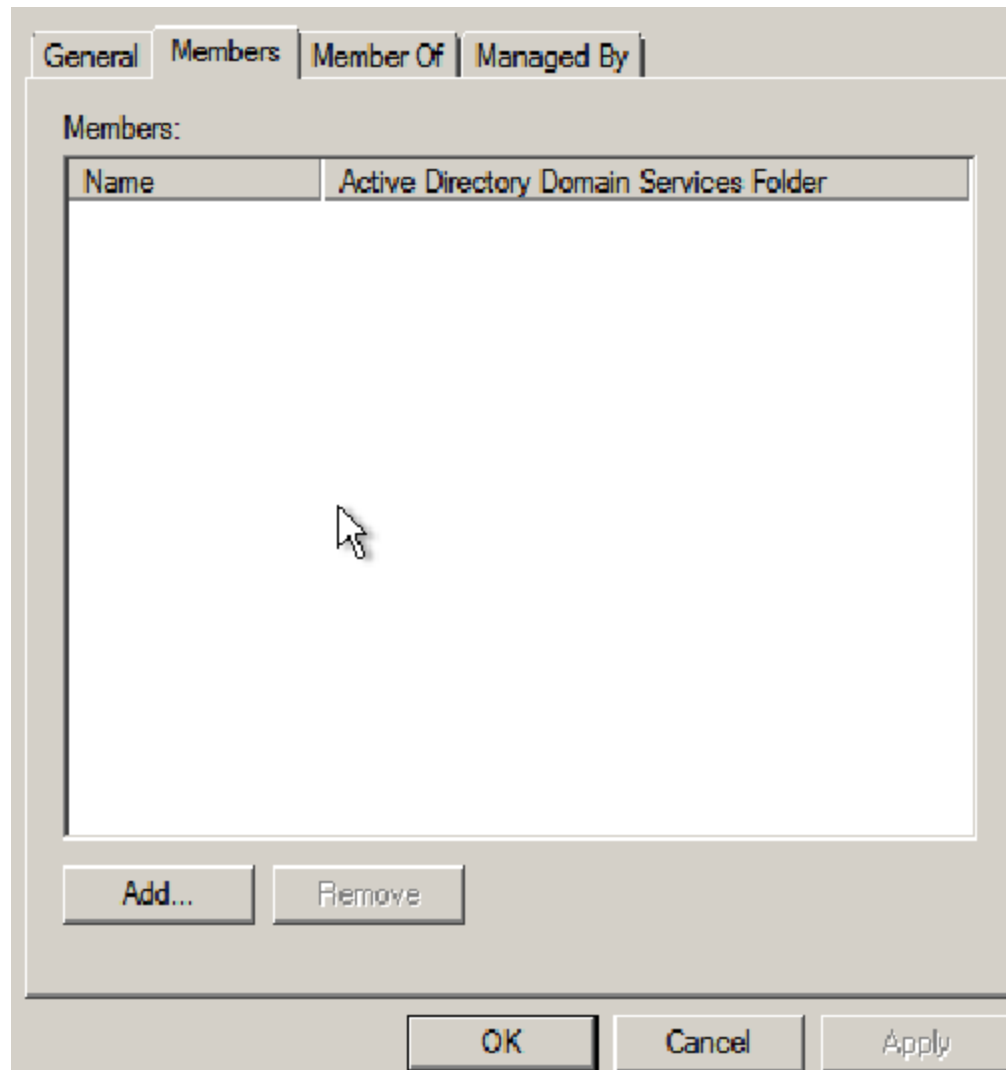
On the writable domain controller we could create a group and a user
Who will administer the RODC. We could then add the group to the

Active Directory Users and Computers [CHI-DC1-2K8.r

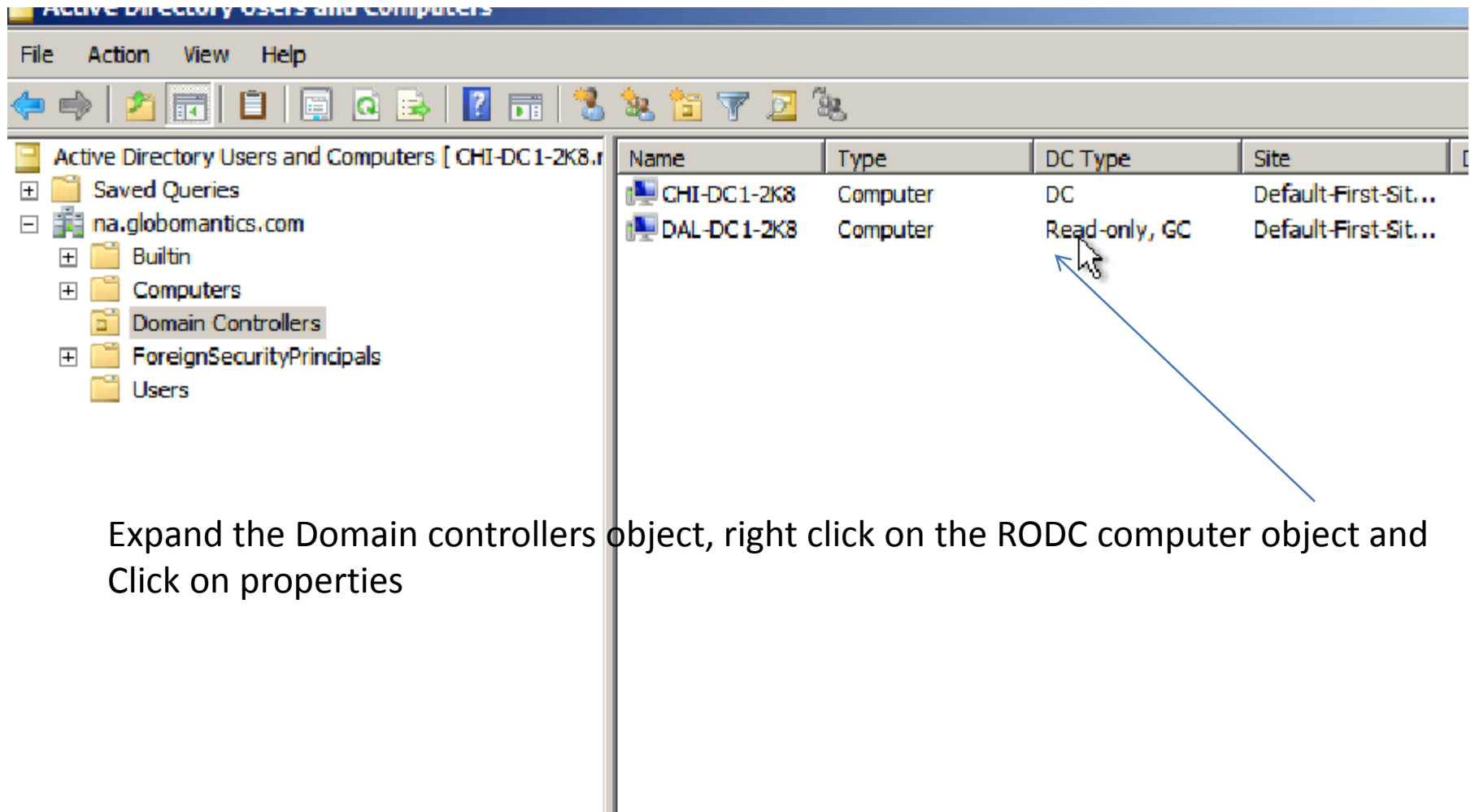
- na.globomantics.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Users

Name	Type	Description
Administrator	User	Built-in accou
Allowed RODC Password Replication Group	Security Group ...	Members in th
Cert Publishers	Security Group ...	Members of t
Dallas Administrator	User	
DallasUsers	Security Group ...	
Denied RODC Password Replication Group	Security Group ...	Members in th
DnsAdmins	Security Group ...	DNS Administ
DnsUpdateProxy	Security Group ...	DNS clients w
Domain Admins	Security Group ...	Designated a
Domain Computers	Security Group ...	All workstatio
Domain Controllers	Security Group ...	All domain coi
Domain Guests	Security Group ...	All domain gu
Domain Users	Security Group ...	All domain usi
Group Policy Creator Owners	Security Group ...	Members in th
Guest	User	Built-in accou
RAS and IAS Servers	Security Group ...	Servers in thi
Read-only Domain Controllers	Security Group ...	Members of t

Any one who is a member of
This group will have their pass
words cached on the RODC. This
means that these passwords will
not only be cached on this RODC
but any RODC in the Domain



If we wanted the passwords to be cached only on the specific RODC that we are dealing with
Then we Would have to connect to that RODC and add the users to the Allowed RODC
Password Replication Group on that RODC.



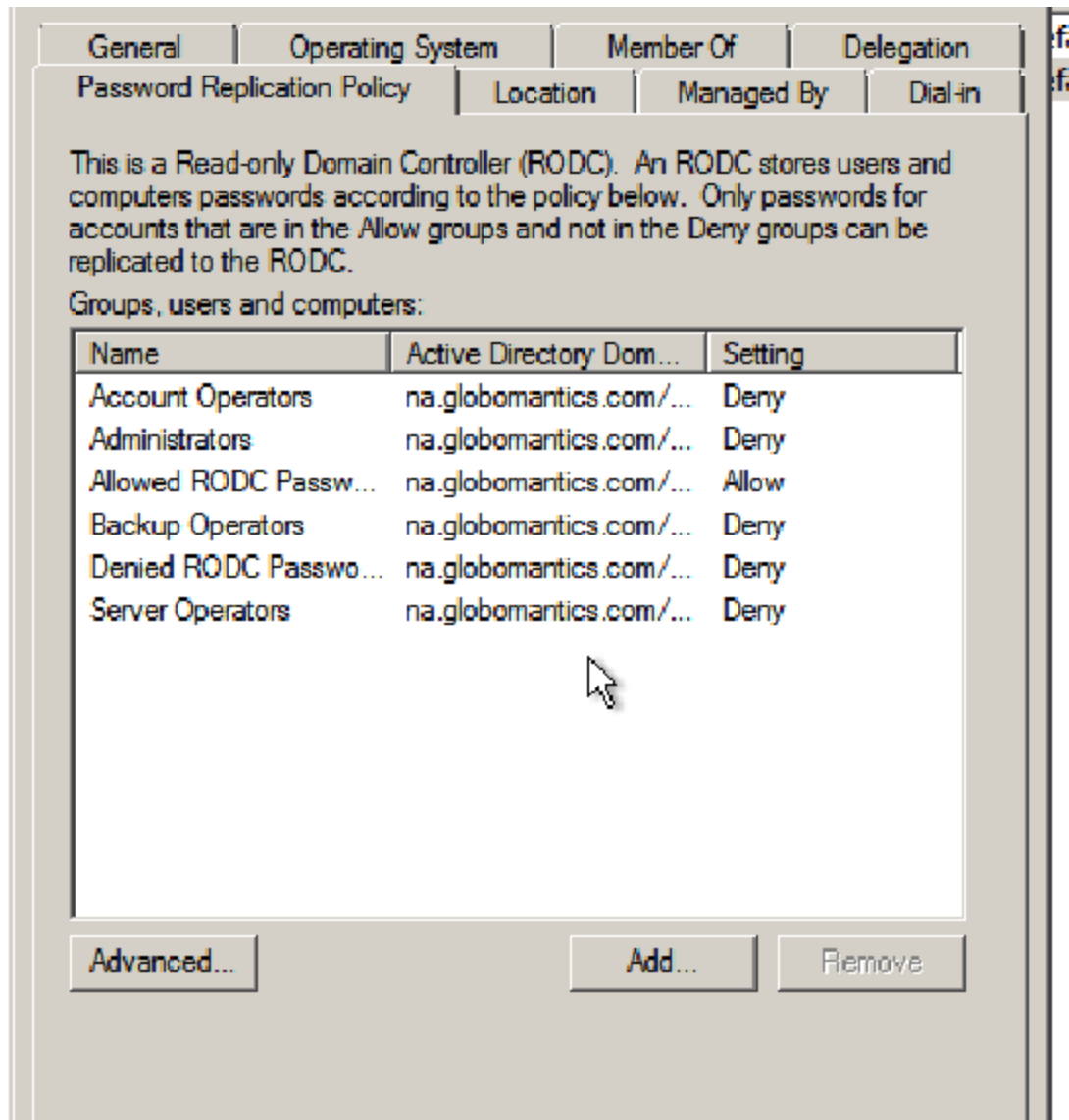
The screenshot shows the Active Directory Users and Computers console. The left pane displays the tree structure for the domain na.globomantics.com, with 'Domain Controllers' expanded. The right pane shows a table of domain controllers:

Name	Type	DC Type	Site
CHI-DC1-2K8	Computer	DC	Default-First-Sit...
DAL-DC1-2K8	Computer	Read-only, GC	Default-First-Sit...

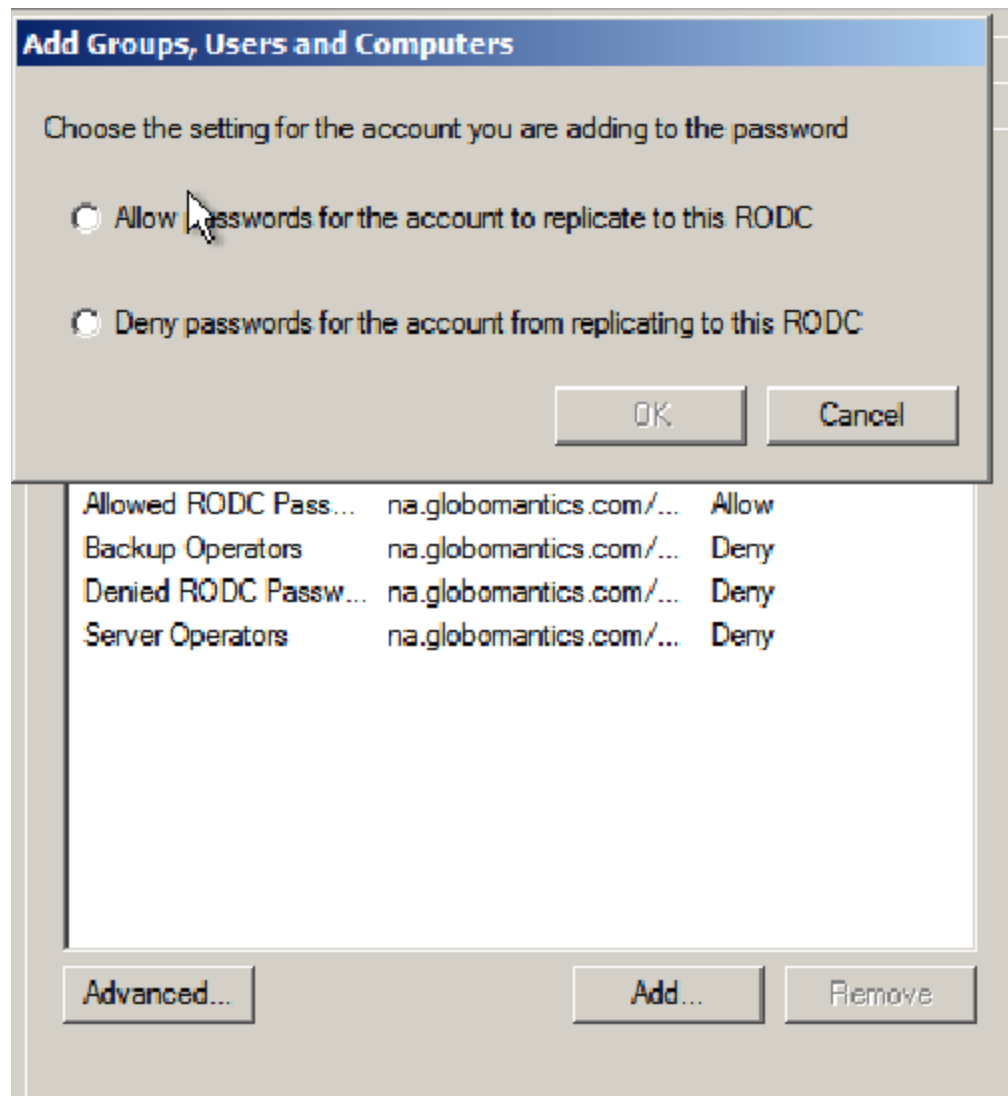
A blue arrow points from the text below to the 'DAL-DC1-2K8' entry in the table.

Expand the Domain controllers object, right click on the RODC computer object and
Click on properties

Is



As you can see everyone else is set to deny except the Allowed RODC password replication Group.



If you wanted to add a specific person you would click on Add and select the option to allow passwords for the accounts to replicate to this RODC



- Active Directory Users and Computers
- Saved Queries
- na.globomantics.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Users

DAL-DC1-2K8 Properties

Select Users, Computers, or Groups

Select this object type:
Users, Computers, Groups, or Built-in security principals

From this location:
na.globomantics.com

Enter the object names to select (examples):
Dallas Users

So now any users in the Dallas Users group
Will be able to catch their password on the
Dallas RODC Domain Controller

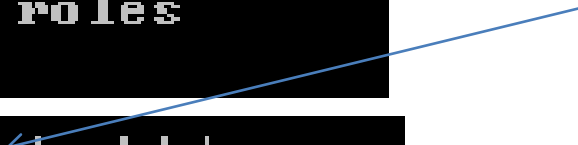
ROLE SEPARATION

On a RODC if we want to make someone an Administrator (local – because a member on a RODC cannot be a domain Administrator) we have to do it from the command Prompt.

```
dsmgmt: local roles
local roles:
```

```
local roles: add daladmin administrators
Successfully updated local role.
local roles: █
```

The user we created on the Writable DC



```
Administrator: Command Prompt - dsmgmt
local roles: list roles
    Administrators

Available roles:
    Administrators
    Users
    Guests
    Remote Desktop Users
    Network Configuration Operators
    Performance Monitor Users
    Performance Log Users
    Distributed COM Users
    IIS_IUSRS
    Cryptographic Operators
    Event Log Readers
    Certificate Service DCOM Access
    Terminal Server License Servers
    Pre-Windows 2000 Compatible Access
    Windows Authorization Access Group
    Replicator
    Account Operators
    Backup Operators
    Server Operators
    Print Operators
local roles:
```

the list roles command
Gives you a list of all
The local roles
Available on the sever

If you want to make someone a member of a specific type of local group so as to manage the individual server but without having Active Directory specific privileges, then this is how you do it. This is called Administrative Role Separation.

RODC AND DNS

If a DNS server is installed on an RODC, clients can send name resolution queries as they would to any other DNS server.

However, the DNS server on an RODC does not support client updates directly and does not register name server (NS) resource records for any Active Directory–integrated zone that it hosts.

When a client attempts to update its DNS records against an RODC, the server returns a referral to a writable DNS server. The RODC then requests the updated DNS record (only a single record) from the writable DNS server. The entire list of changed zone or domain data does not get replicated during this special replicate-single-object request.`