

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.**

You need to **verify requirements** for installing a RODC in your environment. One of the important requirement is the forest functional level, **verify that your forest functional level is set to Windows Server 2003 or newer**. In my case, my forest functional level is already set to Windows Server 2012 R2.

To verify the forest functional level, log in to your AD Server, open Active Directory Users and Computers, right-click the Local domain, and then click **Raise domain functional level** and confirm that the Current domain functional level is set to Windows Server 2012 R2...

Server Manager

Local Server

Manage Tools View Help

- Dashboard
- Local Server**
- All Servers
- File and Storage Services >

PROPERTIES
For compha

Computer name	compha	
Workgroup	WORKGROUP	
Windows Firewall	Private: On	Windows E
Remote management	Enabled	Customer E
Remote Desktop	Enabled	IE Enhance
NIC Teaming	Disabled	Time zone
Ethernet	<input checked="" type="checkbox"/> IPv6 enabled	Product ID
Operating system version	Microsoft Windows Server 2012 Standard	Processors
Hardware information	Microsoft Corporation Virtual Machine	Installed m
		Total disk s



Before you begin

DESTINATION SERVER
compha

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

Skip this page by default

< Previous

Next >

Install

Cancel



Select installation type

DESTINATION SERVER
compha

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

Role-based or feature-based installation

Configure a single server by adding roles, role services, and features.

Remote Desktop Services installation

Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

< Previous

Next >

Install

Cancel



Select destination server

DESTINATION SERVER
compha

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select a server or a virtual hard disk on which to install roles and features.

- Select a server from the server pool
- Select a virtual hard disk

Server Pool

Filter:

Name	IP Address	Operating System
compha		Microsoft Windows Server 2012 Standard

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

< Previous

Next >

Install

Cancel

Select server roles

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

Select one or more roles to install on the selected server.

Roles

- Active Directory Certificate Services
- Active Directory Domain Services
- Active Directory Federation Services
- Active Directory Lightweight Directory Services
- Active Directory Rights Management Services
- Application Server
- DHCP Server
- DNS Server
- Fax Server
- ▶ File And Storage Services (Installed)
- Hyper-V
- Network Policy and Access Services
- Print and Document Services
- Remote Access
- Remote Desktop Services

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



Active Directory Domain Services

DESTINATION SERVER
compha

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

Active Directory Domain Services (AD DS) stores information about users, computers, and other devices on the network. AD DS helps administrators securely manage this information and facilitates resource sharing and collaboration between users. AD DS is also required for directory-enabled applications such as Microsoft Exchange Server and for other Windows Server technologies such as Group Policy.

Things to note:

- To help ensure that users can still log on to the network in the case of a server outage, install a minimum of two domain controllers for a domain.
- AD DS requires a DNS server to be installed on the network. If you do not have a DNS server installed, you will be prompted to install the DNS Server role on this machine.
- Installing AD DS will also install the DFS Namespaces, DFS Replication, and File Replication services which are required by AD DS.

[Learn more about AD DS](#)

< Previous

Next >

Install

Cancel



Installation progress

DESTINATION SERVER
compha

Before You Begin

Installation Type

Server Selection

Server Roles

Features

AD DS

Confirmation

Results

View installation progress

i Feature installation

Configuration required. Installation succeeded on compha.

Active Directory Domain Services

Additional steps are required to make this machine a domain controller.

[Promote this server to a domain controller](#)

Group Policy Management

Remote Server Administration Tools

Role Administration Tools

AD DS and AD LDS Tools

Active Directory module for Windows PowerShell

AD DS Tools

Active Directory Administrative Center

AD DS Snap-Ins and Command-Line Tools



You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

[Export configuration settings](#)

< Previous

Next >

Close

Cancel



Deployment Configuration

TARGET SERVER
compha

Deployment Configuration

Domain Controller Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Root domain name:

Virtualha.com

[More about deployment configurations](#)

< Previous

Next >

Install

Cancel

Domain Controller Options

TARGET SERVER
compha

Deployment Configuration

Domain Controller Options

DNS Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Select functional level of the new forest and root domain

Forest functional level:

Domain functional level:

Specify domain controller capabilities

Domain Name System (DNS) server

Global Catalog (GC)

Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous

Next >

Install

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](#)

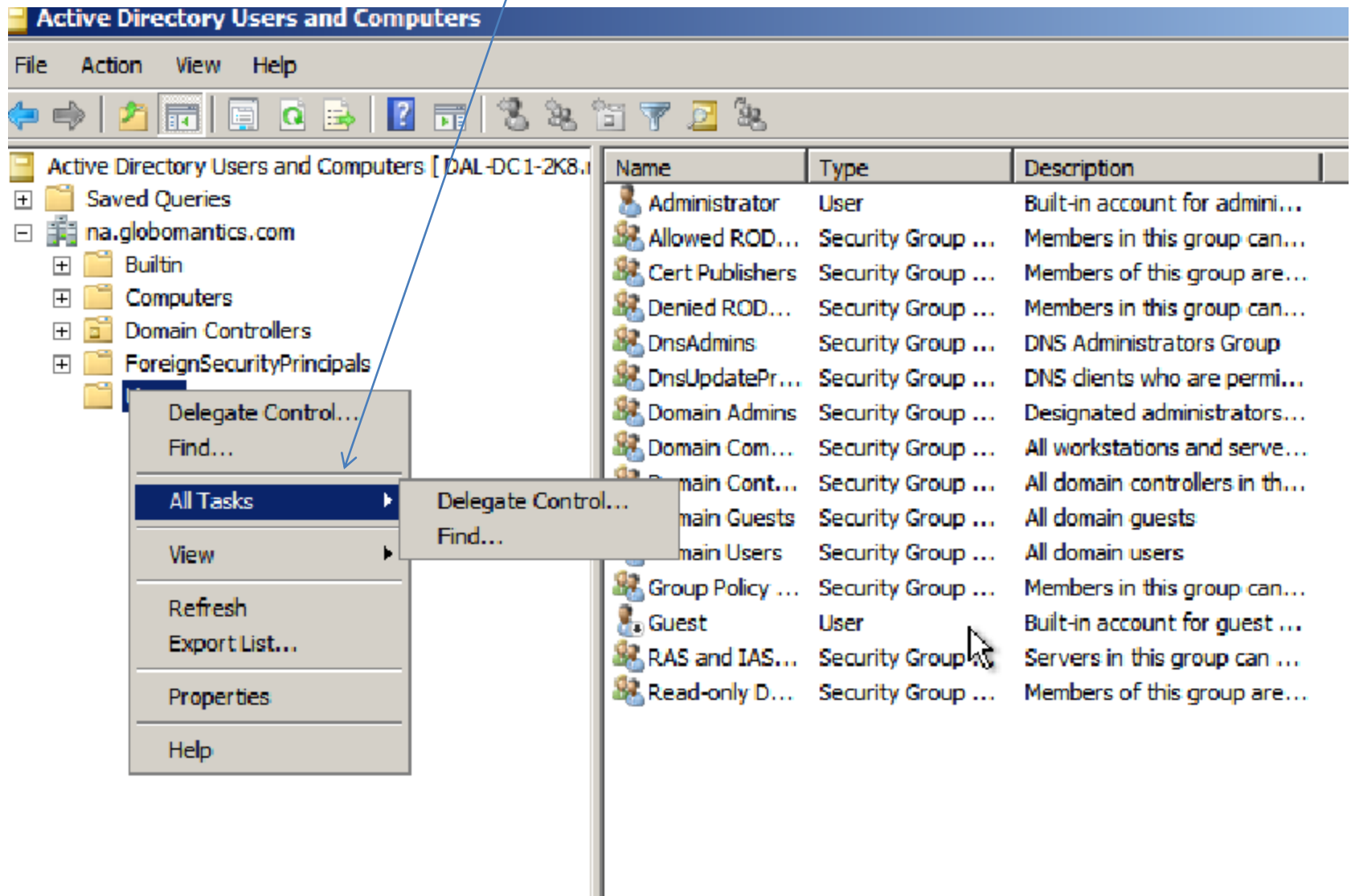
pre-staging of RODC installation

< Back

Next >

Cancel

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

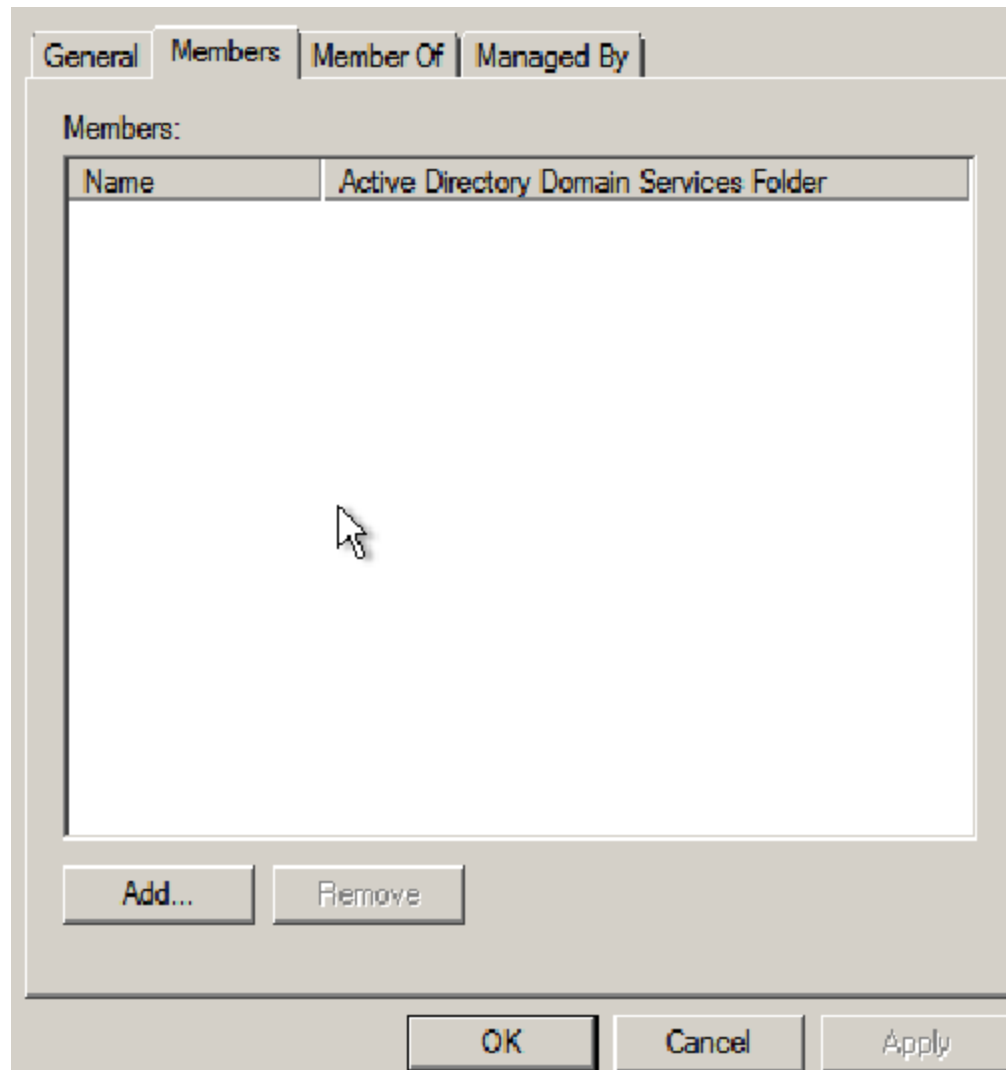
On the writable domain controller we could create a group and a user
Who will administer the RODC. We could then add the group to the

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

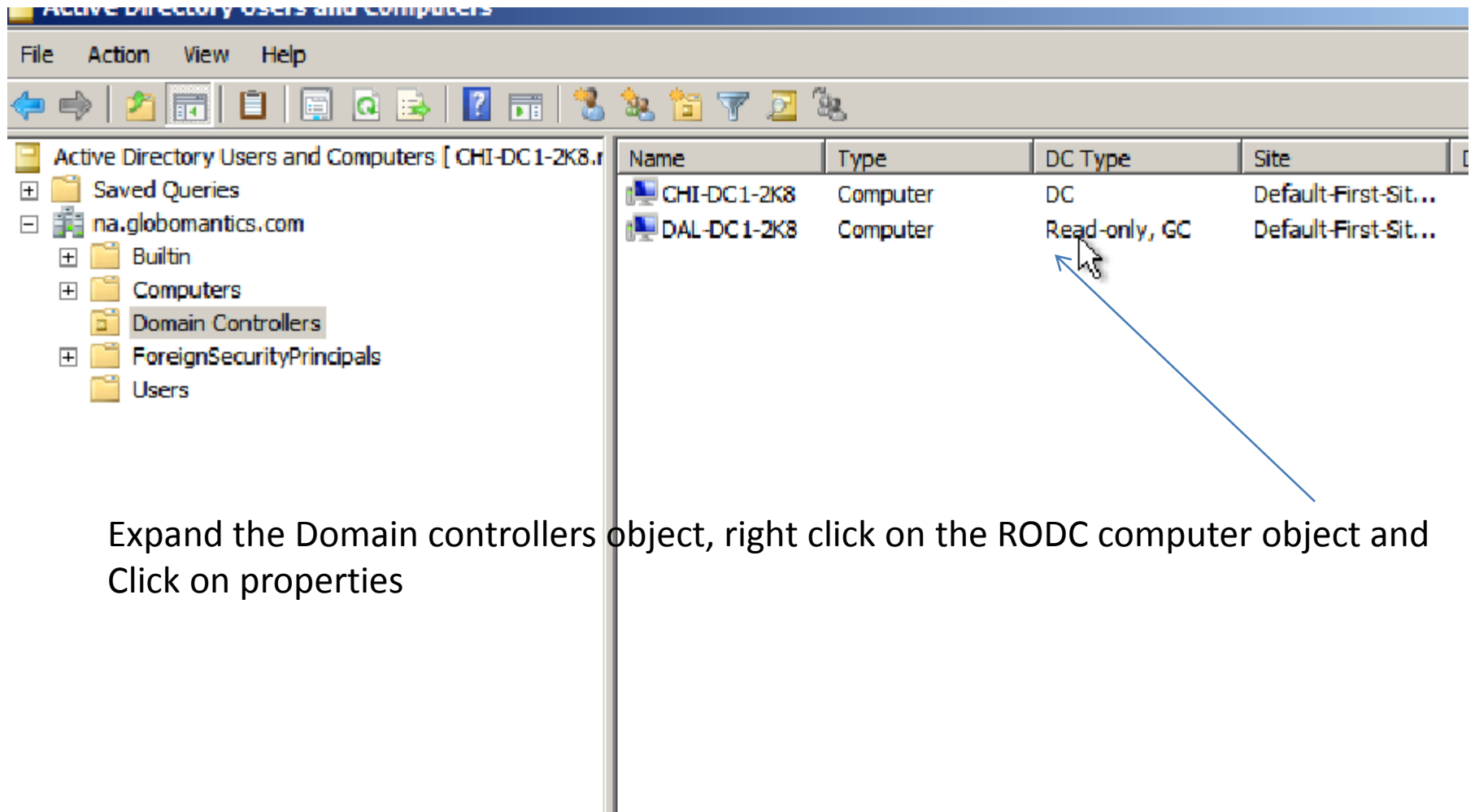
- na.globomantics.com
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Users

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 under '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

General Operating System Member Of Delegation
Password Replication Policy Location Managed By Dial-in

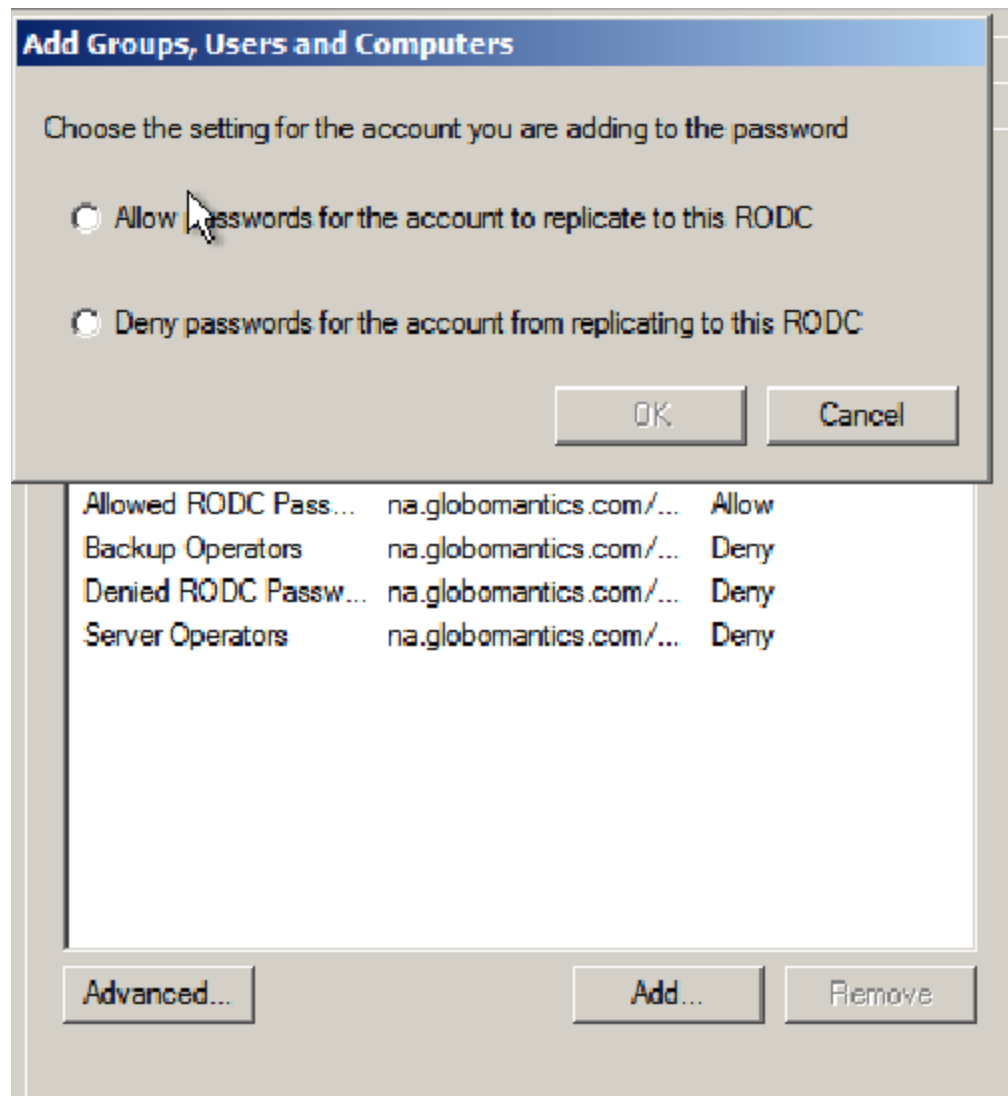
This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
Account Operators	na.globomantics.com/...	Deny
Administrators	na.globomantics.com/...	Deny
Allowed RODC Passw...	na.globomantics.com/...	Allow
Backup Operators	na.globomantics.com/...	Deny
Denied RODC Passwo...	na.globomantics.com/...	Deny
Server Operators	na.globomantics.com/...	Deny

Advanced... Add... Remove

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

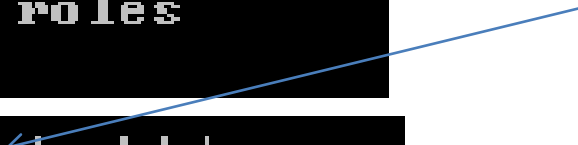
ROLE SEPARATION

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 - dsimgmt
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.`