

RODC

Read-Only Domain Controller

RODC

- O RODC é um controlador de domínio que mantém todas as funções de um ADDC (Active Directory Domain Controller) porém não tem permissão para alterar os dados do diretório
- A principal recomendação de uso deste tipo de controlador de domínio é em situações onde seja necessário um ADDC mas não há estrutura de segurança e suporte local



RODC

- Exemplo de um ambiente:
 - A empresa XYZ tem 2 filiais e uma matriz as filiais conectam-se por uma linha de baixa velocidade e não tem equipe de TI local para suporte de informática
- Neste caso um RODC colocado na filial permitirá que os usuários da filial façam logon no servidor local
- Ainda assim a segurança dos dados do diretório estará assegurada pela característica somente leitura do servidor



RODNS

- Além do serviço de RODC este servidor pode oferecer também o serviço de RODNS
- O RODNS (Read Only Domain Name Server) é um serviço de DNS que também é apenas de leitura
- Assim os clientes locais podem consultar este servidor local que mantém a estrutura do DNS principal, apenas para consulta
- Para isso o RODC irá replicar as partes do diretório referentes ao DNS



RODC

- O primeiro controlador de domínio da floresta deve ser um controlador comun
- A partir deste podemos definir outros controladores que sejam RODC
- É importante diferenciar um RODC de um Controlador de domínio secundário
- O controlador secundário tem as mesmas funções de qualquer controlador de domínio enquanto o RODC é usado apenas para armazenar informação do AD e efetuar o logon de usuários.



RODC

- O RODC normalmente não armazena senhas de usuários localmente
- Ele pode porém, armazenar em cache algumas dessas senhas que sejam definidas pelo administrador do domínio
- É possível ainda permitir que um usuário do domínio tenha acesso a este servidor, mas sem permissão para editar as informações do domínio
 - Este usuário pode fazer tarefas como instalar ou atualizar hardware e softwares, mas não poderá alterar o AD



Replicação de dados no RODC

- A replicação de dados entre servidores ADDC é bidirecional, ou seja:
 - Alterações feitas em qualquer servidor são enviadas e recebidas por todos os controladores
- No caso dos RODC essa replicação é unidirecional:
 - O RODC apenas recebe alterações e não as envia para nenhum controlador de domínio



Autenticação

- O RODC precisa enviar os pedidos de autenticação para um servidor ADDC comum
- Esse servidor ADDC deve estar rodando pelo menos o Windows server 2008
- É possível fazer esta autenticação no próprio RODC, desde que isto esteja definido no ADDC correspondente.
- Se for assim, o RODC guardará em cache a senha dos usuários definidos



Requisitos

- É preciso ter ao menos um servidor windows server 2008 que seja controlador de domínio comum.
- O nível funcional da floresta e do domínio precisa ser windows 2003 ou superior
- Para usar o RODNS é necessário executar o comando: **adprep /rodcprep** no controlador da floresta para atualizar as permissões do DNS



Dependência do ADDC

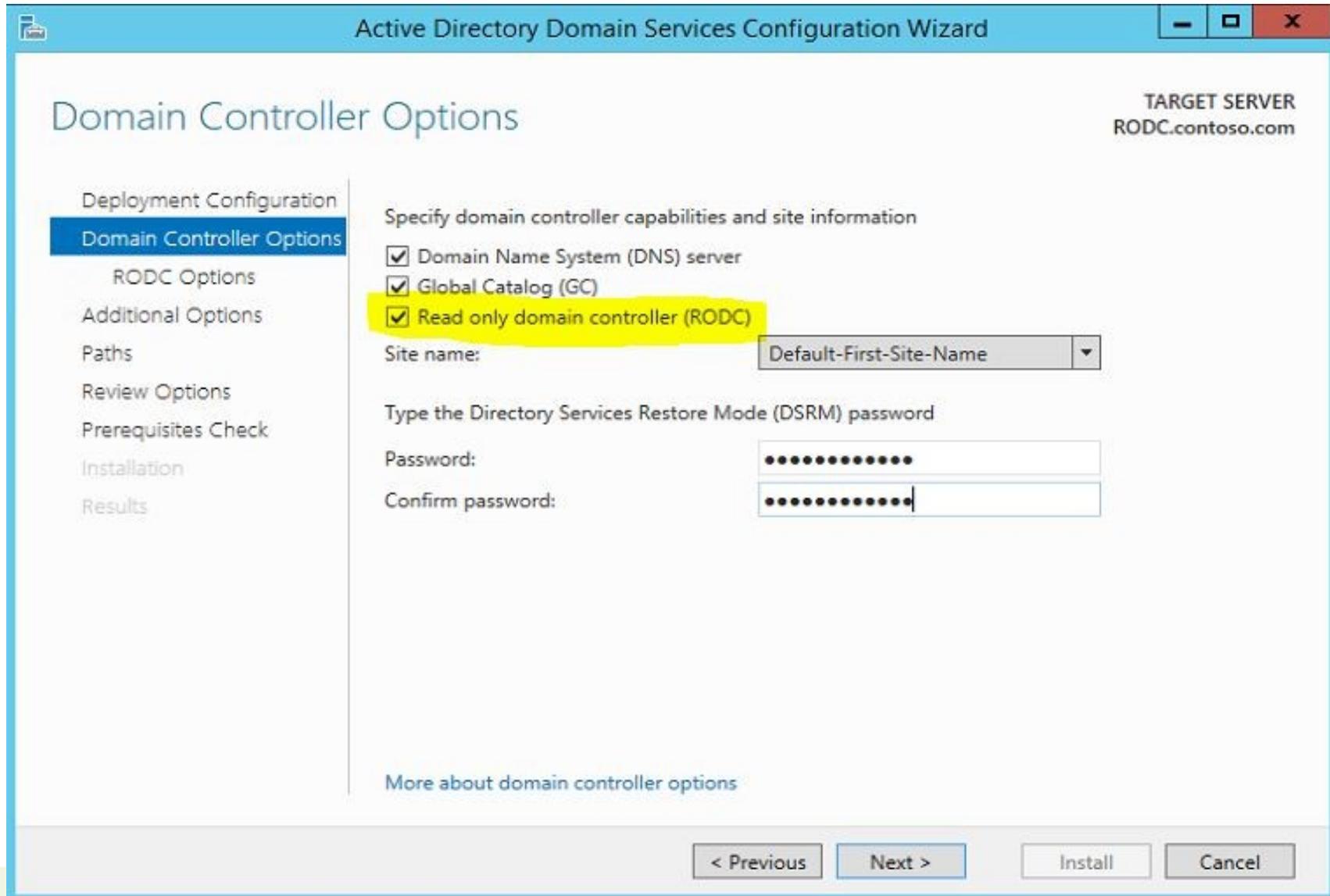
- Apesar de funcionar como um controlador de domínio secundário o RODC tem algumas limitações.
- Em caso de falta de contato com o ADDC as seguintes operações falharão:
 - Troca de senha
 - Ingressar um novo computador no domínio
 - Renomear um computador
 - Autenticação de um usuário que não esteja no cache do RODC
 - Atualização das políticas de grupo usando **gpupdate /force**



Instalação de um RODC

- A instalação se dá no mesmo modo que para um ADDC padrão,
- Porém durante a promoção a DC na tela de opções do ADDC é necessário marcar a opção RODC

Instalação de um RODC



Active Directory Domain Services Configuration Wizard

TARGET SERVER
RODC.contoso.com

Domain Controller Options

Deployment Configuration

Domain Controller Options

RODC Options

Additional Options

Paths

Review Options

Prerequisites Check

Installation

Results

Specify domain controller capabilities and site information

- Domain Name System (DNS) server
- Global Catalog (GC)
- Read only domain controller (RODC)

Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

[More about domain controller options](#)

< Previous Next > Install Cancel



Instalação de um RODC

- Na próxima janela é possível definir os usuários ou grupos de usuários, que serão permitidos ficar em cache neste RODC
- É possível também definir usuários ou grupos de usuários que estão proibidos de ficar em cache neste RODC

Instalação de um RODC

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the text 'Active Directory Domain Services Configuration Wizard' and standard window control buttons. The main window is titled 'RODC Options' and has a sidebar on the left with the following menu items: 'Deployment Configuration', 'Domain Controller Options', 'RODC Options' (highlighted), 'Additional Options', 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main content area is for the 'TARGET SERVER RODC.contoso.com'. It contains three sections: 1. 'Delegated administrator account' with a text box containing '<Not provided>' and a 'Select...' button. 2. 'Accounts that are allowed to replicate passwords to the RODC' with a list box containing 'CONTOSO\Allowed RODC Password Replication Group' and 'Add...' and 'Remove' buttons. 3. 'Accounts that are denied from replicating passwords to the RODC' with a list box containing 'BUILTIN\Administrators', 'BUILTIN\Server Operators', and 'BUILTIN\Backup Operators', and 'Add...' and 'Remove' buttons. Below the denied list is the text 'If the same account is both allowed and denied, denied takes precedence.' and a link 'More about RODC options'. At the bottom of the wizard are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

Active Directory Domain Services Configuration Wizard

RODC Options

TARGET SERVER
RODC.contoso.com

Deployment Configuration
Domain Controller Options
RODC Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

Delegated administrator account
<Not provided>

Accounts that are allowed to replicate passwords to the RODC

CONTOSO\Allowed RODC Password Replication Group

Accounts that are denied from replicating passwords to the RODC

BUILTIN\Administrators
BUILTIN\Server Operators
BUILTIN\Backup Operators

If the same account is both allowed and denied, denied takes precedence.

[More about RODC options](#)

< Previous Next > Install Cancel



Instalação de um RODC

- Na próxima tela é possível definir um servidor específico do qual este RODC irá receber suas atualizações
- Ou podemos deixar que ele receba-as de qualquer controlador de domínio deste domínio

Instalação de um RODC

The screenshot shows the 'Active Directory Domain Services Configuration Wizard' window. The title bar includes the text 'Active Directory Domain Services Configuration Wizard' and standard window control buttons. The main content area is titled 'Additional Options' and shows the 'TARGET SERVER' as 'RODC.contoso.com'. A left-hand navigation pane lists several steps: 'Deployment Configuration', 'Domain Controller Options', 'RODC Options', 'Additional Options' (which is highlighted in blue), 'Paths', 'Review Options', 'Prerequisites Check', 'Installation', and 'Results'. The main pane contains the following options:

- Specify Install From Media (IFM) Options**
 - Install from media
- Specify additional replication options**
 - Replicate from: Any domain controller (dropdown menu)

At the bottom of the wizard, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. A link 'More about additional options' is also visible at the bottom of the main content area.

