### Lesson 16: Configuring Domain Controllers

MOAC 70-411: Administering Windows Server 2012



WILEY

### Overview

- Exam Objective 5.2: Configure Domain Controllers
- Understanding Domain Controllers
- Installing and Configuring an RODC
- Cloning a Domain Controller

### Understanding Domain Controllers

Lesson 16: Configuring Domain Controllers

## Active Directory Logical Components



## Active Directory Physical Components



### **Domain Controllers**

- A **domain controller** is a Windows server that stores a replica of the account and security information for the domain and defines the domain boundaries.
- To make a computer running Windows Server 2012 a domain controller, you must install the AD DS and execute dcpromo from Server Manager.
- Each domain has its own set of domain controllers.
- For fault tolerance, a site should have two or more domain controllers.

## **Global Catalogs**

- As a domain controller, a global catalog stores a full copy of all objects in the domain.
- In addition, as a global catalog, it also has a partial copy of all objects for all other domains in the forest.
- The partial copy of all objects is used for logon, object searches, and universal group membership.
- A global catalog is created automatically on the first domain controller in the forest.
- Optionally, other domain controllers can be configured to serve as global catalogs.

## Global Catalogs and Universal Groups

- One of the primary functions of a global catalog is to provide search capability of any object in the forest.
- Another function of global catalog is to resolve User Principal Names (UPNs).
- Membership of universal groups is stored only in the global catalog and is replicated across the forest.
- When a user logs on, the domain controller must be able to view the membership of the universal groups, so that it can be determined whether a user is allowed or denied logon based on the membership of the universal group.

## Universal Group Membership Caching

- If the membership of the universal groups cannot be determined, a user's logon request denies the request, and the user cannot log on.
- The only exception to this is that the Administrator account can always log on.
- Therefore, for all other users to log on, there must be at least one domain controller acting as a global catalog available or you need Universal Group Membership Caching enabled.

#### **Enable Global Catalogs**

Activ	Active Directory Sites and Services				
File Action View Help					
🗢 🔿 📶 🦸 🔀 🖾 🔒 🛛 🖬 🖉					
👷 Active Directory Sites and Services [WIN20]	Name	Туре	Description		
⊿ 🚞 Sites	🚏 NTDS Settings	Domain Controller Settings			
▷ iii Subnets					
Inter-Site Transports					
🛛 📔 Default-First-Site-Name					
⊿ 🧮 Servers					
⊿ WIN2012SRV					
🚏 NTDS Settings					
< III >	<	Ш	>		

Navigating to domain controllers

### **Enable Global Catalogs**

NTDS Settings Properties ? X					
General Connections Object Security Attribute Editor					
NTDS Settings					
Description:					
Query Policy:					
DNS Alias: 987AF834-E236-4DA3-82F3-F0A21609D5E9msdcs.cr					
Global Catalog					
The amount of time it will take to publish the Global Catalog varies depending on your replication topology.					
OK Cancel Apply Help					

Opening the NTDS Settings Properties dialog box

### Universal Group Membership Caching (UGMC)

- Universal group membership caching (UGMC) allows the local domain controller to store the membership of the universal groups in its local cache indefinitely.
- The cache is refreshed by default every eight hours. As a result, domain controllers can process a logon or resource request without the presence of a global catalog server.
- UGMC provides better logon performance and minimizes WAN usage.
- UGMC is enabled on a per-site basis.

### Enable Universal Group Membership Caching

NTDS Site Set	tings Properties ? X
Site Settings Object Security Attr	ibute Editor
NTDS Site Settings	
Description:	
Change Schedule	
Inter-Site Topology Generator	
Server: WIN2012SRV	
Site: Default-First-Site-Na	me
Universal Group Membership Cach	ing
Enable Universal Group Membe	ership Caching
Refresh cache from:	<default></default>
OK Can	cel Apply Help

Navigating to a site

### Enable Universal Group Membership Caching

Description:			
Change Sch	nedule		
Inter-Site T	opology General	tor	
Server:	WIN2012SF	RV	
Site:	Default-First	:-Site-Name	
- Universal G	àroup Membersh	ip Caching	
🗌 Enable	Universal Group	Membership Caching	
Refresh ca	iche from:	<default></default>	~

Opening the NTDS Site Settings Properties dialog box



### Managing Operations Masters

Guidelines for placing the Operations Master roles:

- Place the domain-level roles on high-performance domain controllers.
- Do not place the infrastructure master on a global catalog server unless you have only one domain or all the domain controllers in your forest are also global catalogs.
- The Schema Master and Domain Naming Master should be on domain controllers in the forest-root domain.
- If the Primary Domain Controller (PDC) Emulator becomes overworked, you should offload non-AD DS roles to other servers, upgrade the PDC Emulator, or move the PDC Emulator to a more powerful computer.

### Viewing the Operations Masters Role Holders

- The easiest way to view the holders of all Operations Masters at once: netdom query fsmo
- To view the RID Masters, PDC Emulators, or Infrastructure Master, use the Active Directory Users and Computers console.

### **Viewing Operations Masters**



#### Viewing the holders of the Operations Masters roles at the command prompt

### Viewing the Operations Masters Role Holders

- To view the holder of the Domain Naming Master role, use the Active Directory Domains and Trusts console.
- To view the holder of the Schema Master role, use the Active Directory Schema.

#### View the Holders of RID Master, PDC Emulator, or Infrastructure Master

Active Directory Users and Computers						
File Action View Help						
Active Directory Users and Com       Name         ▷ Saved Queries       Builtin         ▷ Contoso.com       Computer         ▷ Built       Delegate Control         ▷ Con       Find BitLocker recovery password         ▷ Dire       Find         ▷ Don       Change Domain         ▷ Lost       Change Domain Controller         ▷ Mar       Raise domain functional level         ▷ Syst       Operations Masters	s nts	Type builtinDomain Container Organizational Unit Container IostAndFound nts Container Container Container Container msDS-QuotaContainer msTPM-InformationObjectsContainer	Description Default containe Default containe Default containe Default containe Default containe Default location Builtin system se Default containe			
D 🖆 User New ► D 🖆 NTC All Tasks ►				Quota specificat		
D 🚞 TPN	View	•	InfrastructureUpdate			
	Refresh Export List					
	Properties					
	Help					
<			Ш			
Domain operations n	Domain operations masters					

Selecting Operations Masters

### View the Holders of RID Master, PDC Emulator, or Infrastructure Master

Operations Masters ? X				
RID PDC Infrastructure				
The operations master manages the allocation of RID pools to other Domain Controllers. Only one server in the domain performs this role.				
Operations master:				
WIN2012SRV.contoso.com				
To transfer the operations master role to the following Change				
WIN2012SRV.contoso.com				
<b>Close</b> Cancel				

Using the Active Directory Users and Computers console to view the holders of the domain-based Operation Masters roles

#### View the Domain Naming Operations Master Role Holder

Operations Master	x
The domain naming operations master ensures that domain names are unique. Only one Active Directory Domain Controller in the enterprise performs this role.	
Domain naming operations master:	
WIN2012SRV.contoso.com	
To transfer the domain naming master role to the Change.	
WIN2012SRV.contoso.com	
Close	

Using the Active Directory Domains and Trusts console to view the holders of the Domain Naming Operations Master

#### View the Schema Master Operations Master Role Holder

nap-in Active Directory Do	Vendor Microsoft Cor	^		Console Root	Edit Extensions
Active Directory Sch Active Directory Site	Microsoft Cor Microsoft Cor	≡			Remove
Active Directory Use ActiveX Control	Microsoft Cor Microsoft Cor				Move Up
ADSI Edit Authorization Manager	Microsoft Cor Microsoft Cor		Add >		Move Down
Certificate Templates Certificates	Microsoft Cor Microsoft Cor				
Certification Authority Component Services	Microsoft Cor				
Computer Managem Device Manager	Microsoft Cor Microsoft Cor	_			Advanced
OFS Management	Microsoft Cor		]		

Opening the Add or Remove Snap-in dialog box

## Transferring the Operations Masters Role

Reasons to transfer the Operations Master:

- Planned maintenance
- Retiring a domain controller that holds a role of Operations Master
- Moving a role of Operations Master to a domain controller with more resources

Transferring a FSMO role requires that the source domain controller and the target domain controller be online.

### Transfer the Holders of RID Master, PDC Emulator, or Infrastructure Master

Active Directory Users and Computers						
File Action View Help						
🗢 🔿 📶 📋 🗐 🖉 🖬	浅 📚 🛅 💎 .	2 (k				
Active Dire Saved Saved Change Domain Change Domain Controller. All Tasks Refresh Help Manag Program System Users NTDS C TPM Do Infrastr		Type builtinDomain Container Organizational Unit Organizational Unit Container IostAndFound Container Container Container Container msDS-QuotaContainer msTPM-InformationObjectsContainer infrastructureUpdate	Description Default containe Default containe Default containe Default containe Default containe Default location Builtin system se Default containe Quota specificat			
< III > <		Ш	>			
Choose a specific Domain Controller to connect t	:0					

#### Selecting the Change Domain Controller option

#### Transfer the Holders of RID Master, PDC Emulator, or Infrastructure Master

Change Directory Server							
Curren WIN Chang • A O T	t Directory Server: 2012SRV.contoso.com e to: wy writable Domain Controller 'his Domain Controller or AD LDS instance						
	Name	Site	DC Type	DC Version	Status		
	<type a="" directory="" here="" name[:port]="" server=""> WIN2012SRV.contoso.com Win2012Srv2.contoso.com</type>	Default-First-Site-Name Default-First-Site-Name	GC GC	Windows Windows	Online Online		
Sa Sa	Save this setting for the current console						
			OK	Cancel	Help		

#### Selecting a domain controller to transfer the role to

### Seizing the Operations Masters Role

- If a domain controller that holds an Operations Master role has an unrecoverable failure, you cannot transfer roles because the current domain controller is not online. Therefore, you need to seize the role.
- Seizing a FSMO role is a drastic measure that should be performed only in the event of a permanent role holder failure.
- To seize a role of an Operations Master, you use the ntdsutil.exe utility.

#### Seize the Role of an Operations Master Holder

CA.	Administrator: Command Prompt - ntdsutil	_ <b>D</b> X
C:\>ntdsutil ntdsutil: roles fsmo maintenance: conne server connections: con Binding to win2012srv2. Connected to win2012srv2. Server connections: qui fsmo maintenance: seize Attempting safe transfe FSMO transferred succes Server "win2012srv2.cor Schema - CN=NTDS Settin Schema - CN=NTDS Settin Sites, CN=Configuration Name, CN=Sites, CN=Config PDC - CN=NTDS Settings, ites, CN=Configuration, I RID - CN=NTDS Settings, tes, CN=Configuration, DC	ections nect to server win2012srv2.contoso.com .contoso.com 2.contoso.com using credentials of locally log it e pdc er of PDC FSMO before seizure. ssfully - seizure not required. toso.com" knows about 5 roles hgs,CN=WIN2012SRU,CN=Servers,CN=Default-First-S h,DC=contoso,DC=com CN=WIN2012SRU2,CN=Servers,CN=Default-First-Sit Quration,DC=contoso,DC=com CN=WIN2012SRU2,CN=Servers,CN=Default-First-Sit DC=contoso,DC=com CN=WIN2012SRU2,CN=Servers,CN=Default-First-Site C=contoso,DC=com CN=WIN2012SRU2,CN=Servers,CN=Default-First-Site C=contoso,DC=com CN=WIN2012SRU2,CN=Servers,CN=Default-First-Site C=contoso,DC=com	ged on user ite-Name,CN First-Site- e-Name,CN=S -Name,CN=Si -Rivst-Site
-Name,CN=Sites,CN=Confi fsmo maintenance: _	iguration,DC=contoso,DC=com	v

#### Seizing the PDC Emulator role

### Installing and Configuring an RODC

Lesson 16: Configuring Domain Controllers

## Read-Only Domain Controller (RDOC)

The Read-Only Domain Controller (RODC):

- Contains a full replication of the domain database.
- Was created to be used in places where a domain controller is needed but the physical security of the domain controller could not be guaranteed.

## Installing an RDOC

When you install an RODC, you need to define a delegated administrator that has local administrative permission to the RODC, even though the account is not a member of the Domain Admin or domain built-in Administrators group.

# Deploying an RDOC:

- Ensure that the forest functional level is Windows Server 2003 or higher.
- Deploy at least one writable domain controller running Windows Server 2008 or higher.

## Configuring an RDOC

You can configure each RODC to have its own Password Replication Policy (PRP).

To allow enterprise-wide configuration of the RODC PRP, Windows Server 2008 creates the following security groups:

- Denied RODC Password Replication Group
- Allowed RODC Password Replication Group

2	Server Manager	_ <b>_</b> ×
Server M	anager 🕨 AD DS 🛛 🗸 🕫 🖍 Manage	Tools View Help
<ul> <li>Dashboard</li> <li>Local Server</li> <li>All Servers</li> <li>AD DS</li> <li>AD LDS</li> <li>DNS</li> <li>File and Storage Services ▷</li> <li>IIS</li> <li>Remote Access</li> </ul>	SERVERS All servers   1 total Configuration required for Active Directory Domain Services at WIN2012SRV2 Filter P E Server Name IPv4 Address Manageability WIN2012SRV2 10.1.1.25,192.168.3.121 Online - Data retrieval failures occurred I I I I I I I I I I I I I	TASKS       ▼         More       ×         ✓       ✓         Last Update       9/28/2012 4:34:57 PN         >       >

#### Installing AD DS on a new computer

Filter	م م		• (R) •		۲
Status	Task Name	Stage	Message	Action	Notifications
	Post-deployment Configuration	Not Sta	Configuration required for Active Directory Do	Promote this server to a domain	1
<			101		
< Status	Notification		III	Time Stamp	

#### Promoting the server to a domain controller

B	Active Directory Domain Services	Configuration Wizard	_ <b>_</b> ×
Deployment Cont	figuration		TARGET SERVER Win2012Srv2.contoso.com
Domain Controller Options Additional Options	<ul> <li>Select the deployment operation</li> <li>Add a domain controller to an existin</li> <li>Add a new domain to an existing for</li> <li>Add a new forest</li> </ul>	ng domain rest	
Parns Review Options Prerequisites Check	<ul> <li>Add a new forest</li> <li>Specify the domain information for this</li> <li>Domain:</li> </ul>	operation contoso.com	Select
Results	Supply the credentials to perform this o CONTOSO\administrator (Current user)	peration	Change
	More about deployment configurations		
	< Pr	evious Next >	Install

#### Adding a domain controller to an existing domain

<b>b</b>	Active Directory Domain Servic	es Configuration Wizard	_ <b>□</b> ×
Domain Controller	<sup>r</sup> Options		TARGET SERVER Win2012Srv2.contoso.com
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation	Specify domain controller capabilitie Domain Name System (DNS) ser Global Catalog (GC) Read only domain controller (RC Site name: Type the Directory Services Restore Password: Confirm password:	es and site information ver DDC) Default-First-Site-Name Mode (DSRM) password	<b>v</b>
Results	More about domain controller optic	ons	Install
		< Previous Next >	Install Cancel

#### Selecting an RODC

à	Active Directory Domain Services Configuration Wizard
RODC Options	TARGET SERVER Win2012Srv2.contoso.com
Deployment Configuration Domain Controller Options RODC Options Additional Options	Delegated administrator account <not provided=""> Select Accounts that are allowed to replicate passwords to the RODC</not>
Paths Review Options Prerequisites Check Installation	CONTOSO\Allowed RODC Password Replication Group <u>Add</u> Remove
Results	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

Specifying the delegated administrator

<b>b</b>	Active Directory Domain Services	Configuration Wizard	_ 🗆 X
Additional Option	IS		TARGET SERVER Win2012Srv2.contoso.com
Deployment Configuration Domain Controller Options RODC Options	Specify Install From Media (IFM) Option	S	
Additional Options	Specify additional replication options		
Paths Review Options Prerequisites Check Installation Results	Replicate from:	Any domain controller	T
	More about additional options		
	< Pr	evious Next >	Install Cancel

#### Selecting additional options

	WIN20125	RV2 Properties	s L	? X
Security	Dial-in /	Attribute Editor	BitLocker Re	covery
Delegation F	Password Replication Po	ing System blicy Location	Member Managed By	Obiect
This is a Read-or computers passw accounts that are replicated to the I Groups, users an	nly Domain Controller (Ri ords according to the p e in the Allow groups and RODC. d computers:	DDC). An RODC sto olicy below. Only pa d not in the Deny gro	ores users and isswords for oups can be	
Name		Active Directory Do	om Settinc	
Account Opera	tors	contoso.com/Builtir	n Deny	
Administrators		contoso.com/Builtir	n Deny	
Allowed RODC	Password Replicatio	contoso.com/Users	s Allow	
Backup Operat	ors	contoso.com/Builtir	n Deny	
Denied RODC I	Password Replication	contoso.com/Users	s Deny	
Server Operato	18	contoso.com/Builtir	n Deny	
<	III		>	
Advanced		Add	Remove	

Configuring the Password Replication Policy

### Cloning a Domain Controller

Lesson 16: Configuring Domain Controllers

## **Domain Controller Clones**

- Starting with Windows Server 2012, you can safely virtualize a domain controller and rapidly deploy virtual domain controllers through cloning.
- It allows you to quickly restore domain controllers when a failure occurs and to rapidly provision a test environment when you need to deploy and test new features or capabilities before you apply the features or capabilities to production.

### Deploying a Cloned Domain Controller

Deploying a cloned virtualized domain controller:

- 1. Grant the source virtualized domain controller the permission to be cloned by adding the source virtualized domain controller to the Cloneable Domain Controllers group.
- 2. Run Get-ADDCCloningExcludedApplicationList cmdlet in Windows PowerShell to determine which services and applications on the domain controller are not compatible with the cloning.
- 3. Run New-ADDCCloneConfigFile to create the clone configuration file, which is stored in the C:\Windows\NTDS.
- 4. In Hyper-V, export and then import the virtual machine of the source domain controller.

		Н	yper-V Manag	ger		_ <b>_</b> ×
File Action View Help						
🗢 🏟 🖄 📰 🛽 🗊						
Hyper-V Manager					~	Actions
	virtual Machines					WIN2012SRV2
	Name	State	CPU Usage	Assigned Memory	Uptir	New
	DC02	Running	0%	650 MB	00:47	💫 Import Virtual Machine
	<	Ш				👔 Hyper-V Settings
	Snapshots					🙀 Virtual Switch Manager
						🖳 🖳 Virtual SAN Manager
		No virti	ual machine select	ed.	=	💋 Edit Disk
						🖳 Inspect Disk
					_	Stop Service
	Details					🗙 Remove Server
		N	lo item selected.			🔉 Refresh
						View 🕨
						🛿 🕜 Help
					~	
	<	III			>	

Opening the Hyper-V Manager

		H	yper-V Mana	ger				Ŀ	- 1	2	x
File Action View Help											
🗢 🏟 🞽 🖬 👔											
📑 Hyper-V Manager						~	Act	ions			
WIN2012SRV2	Virtual Mach	lines					W	N2012SRV2		-	^
	Name 🔻	State	CPU Usage	Assigned Merr	nory Uptir			New		•	
	DC02	Connect	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	650 MB	00:49		1	Import Virtual Machin	ie		
	<	Settings					1	Hyper-V Settings			
	Spanshot	Turn Off						Virtual Switch Manage	er		
	Shapshot	Shut Down						Virtual SAN Manager.			=
		Save	achine has r	io snapshots.		=		Edit Disk			-
		Pause					4	Inspect Disk			
		Reset						Stop Service			*
	DC02	Snapshot					×	Remove Server			
		Move				1	Q	Refresh			
	1. gene	Rename	1	Clustered: N	No			View		•	
	100 E	Enable Replication		Heartbeat: L	UK (Application Healthy)	r i	?	Help			
		Help									
								.uz		_	
Γ.	<				>	-		Connect			-
Turns off the selected virtual ma	achine.						p mw-1	Vertind(			

#### Turning off a virtual machine

2	Import Virtual Machine	x
Locate Folder		
Before You Begin	Specify the folder containing the virtual machine to import.	
Locate Folder Select Virtual Machine Choose Import Type Summary	Folder: Browse	
	< Previous Next > Finish Cancel	

Specifying the virtual machine to import

2	Import Virtual Machine	x
Choose Impo	ort Type	
Before You Begin	Choose the type of import to perform:	
Locate Folder	Register the virtual machine in-place (use the existing unique ID)	
Select Virtual Machine	O Restore the virtual machine (use the existing unique ID)	
Choose Import Type	O Copy the virtual machine (create a new unique ID)	
Summary		
	< Previous Next > Finish Cancel	

#### Choosing the import type

2	Import Virtual Machine	x
Choose Folde	ers for Virtual Machine Files	
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.  If I store the virtual machine in a different location Virtual machine configuration folder:  C:\ProgramData\Microsoft\Windows\Hyper-V3 Browse Smart Paging folder:  C:\ProgramData\Microsoft\Windows\Hyper-V3 Browse	····
	< Previous Next > Finish Canc	el

#### Choosing where to store the virtual machine files

2	Import Virtual Machine	x
Choose Folde	ers to Store Virtual Hard Disks	
Before You Begin Locate Folder Select Virtual Machine Choose Import Type Choose Destination Choose Storage Folders Summary	Where do you want to store the imported virtual hard disks for this virtual machine?         Location:       C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\         Browse.	
	< Previous Next > Finish Cance	

Choosing where to store the virtual hard disks

## Lesson Summary

- A domain is an administrative boundary for users and computers that are stored in a common directory database. A single domain can span multiple physical locations or sites and can contain millions of objects.
- Domain controllers are servers that contain the Active Directory databases.
- A global catalog stores a full copy of all objects in the domain.
- Universal group membership caching (UGMC) is one method to use to avoid placing a global catalog at every site and to avoid going over a WAN link for login information.
- Operations masters, sometimes referred to as Flexible Single Master Operations (FMSO), are specialized domain controllers that perform certain tasks that can be handled only by a single domain controller in a multi-master environment.

## Lesson Summary

- Primary Domain Controller (PDC) Emulator coordinates password changes, account lockouts, and time synchronization; manages edits to Group Policy Objects (GPOs); and acts as a domain master browser (provides a list of workgroups and domains when you browse).
- Infrastructure Master is used to track which objects belong to which domain because it is responsible for reference updates from its domain objects to other domains.
- Relative Identifier (RID) Master is responsible for assigning relative identifiers to domain controllers in the domain.
- Schema Master controls all the updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master.

## Lesson Summary

- Domain Naming Master holds the Domain Naming Master role that controls the addition or removal of domains in the forest.
- If you are planning to do maintenance where a domain controller that holds the Operations Master will be down for an extended period of time, you are going to retire a domain controller that holds a role of Operations Master or you need to move the role to a domain controller with more resources, you will need to transfer the Operations Master.
- The Read-Only Domain Controller (RODC) contains a full replication of the domain database and cannot be modified directly.
- Starting with Windows Server 2012, you can safely virtualize a domain controller and rapidly deploy virtual domain controllers through cloning.

#### Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



