Lab Guide

Implementing and maintaining DNS

Install DNS role

We have a running DNS service on DC1, which got installed when we installed the first domain controller in the domain "lab.local"

We will install another DNS server on DC2, and use it to get hands on experience in configuring and maintaining DNS service in Windows server environment.

1- Open the Server Manager on DC2 and click on "Add Roles and Features", then click "Next".



2- Keep the selection on "Role-based or Feature-based installation, and click "Next"



3- Make sure DC2 is selected and click "Next".

Select destinat	ion server			DESTINAT	ION SERVI DC2.lab.loc
Before You Begin	Select a server or a vi	rtual hard disk on whicl	h to install roles and features.		
Installation Type	 Select a server fro 	m the server pool			
Server Selection	O Select a virtual ha	rd disk			
Server Roles	Server Pool				
Features					
	Filter:				
Results	Name	IP Address	Operating System		
	DC2.lab.local	10.10.10.2	Microsoft Windows Server	2022 Datacenter	
	DC2.lab.local	10.10.10.2	Microsoft Windows Server	2022 Datacenter	
	DC2.lab.local	10.10.10.2	Microsoft Windows Server	2022 Datacenter	
	DC2.lab.local	10.10.10.2	Microsoft Windows Server	2022 Datacenter	

4- Check on DNS, and click "Next", then a message will popup asking to add the required features, click "Add Feature", then click "Next".



5- Click "Next" twice, and finally "Install".

Now DNS role will be installed, the next step is to configure the server in order to make it able to serve client DNS queries.

DNS can respond to click queries by either checking its own "DNS Zone", or be getting help from other DNS servers.

6- At first, you can configure the server as a forwarder which gets clients requests and forward them to anther server you specify.To do that, go to "Server Manager", click on "Tools" then select "DNS" from the menu Then will open the DNS console, right-click on the server's name and choose "Properties"

🍰 DNS Manager		_	×
File Action View Help			
🗢 🔿 🙍 📷 🗙 🖾 🧟 🗟 📷 📲 🚳			
 DNS Name Configure a DNS Server F Create Default Application Directory Partitions 1 New Zone C Set Aging/Scavenging for All Zones Scavenge Stale Resource Records Update Server Data Files 			
Clear Cache Launch nslookup			
All Tasks	>		
View	>		
Delete Refresh Export List			
-> Properties			
Help			
Opens the properties dialog box for the current selection.			

7- In the "Properties" page click on "Forwarders" tap, then add DC1 as shown in the picture

DC2 Properties		? ×				
Debug Logging Event Loggin Interfaces Forwarders	ng Monitoring Advanced	Security Root Hints				
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.						
IP Address	Server FQDN					
10.10.10.1	DC1					
Use root hints if no forwarders are a	available	Edit				
Note: If conditional forwarders are defi used instead of server-level forwarders forwarders, navigate to the Conditiona	Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.					
		_				
OK Cano	xel Apply	Help				

Now DC2 will respond the client queries by forwarding the query to DC1, getting the response, and send back the response to the client.

Primary and Secondary zones

Let's go further with the next step which is to add a new zone to DC2 to make it able to respond to client queries by itself.

At first, we will create a Primary zone and configure zone transfer with a secondary zone on another DNS server.

8- In DNS console on DC2, make sure forward lookup zone to selected, then right-click on it, and choose "New Zone"



9- In the "New zone wizard" click "Next", then leave the default selection on "Primary zone", and uncheck the option down the window, which says "Store the zone in Active Directory, (this option is available only of DC2 is already and domain controller. Then click "Next"

Zone Type

The DNS server supports various types of zones and storage.

Cusatas	one	ومراقبة والمراجعة والمراجع	this serves	
Creates a	copy of a zone that can b	be updated directly or	i this server.	
<u>○</u> Secondar	y zone			
Creates a the proce	a copy of a zone that exists essing load of primary serv	s on another server. Vers and provides fau	This option helps ba It tolerance.	lance
⊖ Stub zone	2			
 Stub zone Creates a (SOA), ar authorita 	e a copy of a zone containing nd possibly glue Host (A) re tive for that zone.	g only Name Server (I ecords. A server cont	NS), Start of Authori aining a stub zone i	ty s not
 Stub zone Creates a (SOA), ar authorita Store the controller 	e a copy of a zone containing nd possibly glue Host (A) re tive for that zone. zone in <u>A</u> ctive Directory (a)	g only Name Server (l ecords. A server cont available only if DNS se	NS), Start of Authori aining a stub zone i erver is a writeable	ty s not domain

10- Enter the new zone name "abc.local" and click next.

Zo	one Name What is the name of the new zone?	The second second
	The zone name specifies the portion of the DNS namespace for which this authoritative. It might be your organization's domain name (for example, a portion of the domain name (for example, newzone.microsoft.com). The the name of the DNS server.	server is microsoft.com) or zone name is not
	Zone name:	
	abc.local	
		1

X

11- In the zone file name accept the default, and click "Next"

Zone File You can create a new zone file or use a file	e copied from another DNS server.	III IIII
Do you want to create a new zone file or us another DNS server?	se an existing file that you have copie	ed from
• Create a new file with this file name:		
abc.local.dns		
O Use this existing file:		
To use this existing file, ensure that it ha %SystemRoot%\system32\dns on this s	as been copied to the folder server, and then click Next.	
	< Back Next >	Cancel

12- In the "Dynamic Update" window change the selection allow both secure and nonsecure dynamic updates, and click "Next"

Dynamic Update			
You can specify that this DNS zone accept updates.	s secure, nonsecure	, or no dynamic	Interest
Dynamic updates enable DNS client compu resource records with a DNS server when	uters to register and ever changes occur	dynamically updat	e their
Select the type of dynamic updates you wa	ant to allow:		
Allow only secure dynamic updates (re-	commended for Acti	ve Directory)	
This option is available only for Active D	Directory-integrated	zones.	
Allow both nonsecure and secure dyna	mic updates		
Dynamic updates of resource records	are accepted from a	any client.	
This option is a significant securi from untrusted sources.	ity vulnerability beca	use updates can b	e accepted
O Do not allow dynamic updates			
Dynamic updates of resource records a these records manually.	are not accepted by	this zone. You mu	st update

13- Click "Finish" to create the zone.

Now the zone is created as a primary zone, and we need to create a secondary zone on another server, which will be read-only zone, and will transfer it is records from the primary (the master)

We will use DC1 for this step

14-, Go to DC1, Open the DNS console then r-click on the server's name and choose "New Zone", and select secondary, then click "Next"

Zone Type		31
The DNS server supports various types	s of zones and storage.	in the second se
Select the type of zone you want to cre	ate:	
O Primary zone		
Creates a copy of a zone that can b	be updated directly on this serv	er.
Secondary zone		
Creates a copy of a zone that exists the processing load of primary serv	s on another server. This optio vers and provides fault tolerand	n helps balance ce.
🔿 Stub zone		
Creates a copy of a zone containing (SOA), and possibly glue Host (A) re authoritative for that zone.	g only Name Server (NS), Start ecords. A server containing a s	of Authority tub zone is not
Store the zone in Active Directory (a controller)	wailable only if DNS server is a	writeable domain

15- Enter the zone name "abc.local", then click "Next"

New Zone Wizard	×
Zone Name What is the name of the new zone?	and the second se
The zone name specifies the portion of the authoritative. It might be your organization a portion of the domain name (for example the name of the DNS server.	DNS namespace for which this server is s domain name (for example, microsoft.com) or e, newzone.microsoft.com). The zone name is not
Zone name:	
abc.local	
	< Back Next > Cancel

16- Enter the IP address or the name of the DNS server which holds the primary zone, in our case it is DC2.

The secondary zone is	s copied from one or	r more DNS servers.	
Specify the DNS serve	rs from which you w	ant to copy the zone.	Servers are contacted
in the order shown.			
Master Servers:			
IP Address	Server FQDN	Validated	Delete
<click here="" td="" to<=""><td></td><td></td><td></td></click>			
0 10.10.10.2	DC2	OK	Up
- ICHIOIL			
1			Down

17- Finally click finish the create the zone.

Now the zone is created but we need to allow zone transfer from DC2 (the master) to DC1, before allowing zone transfer from the master, the secondary zone will not work.

18- Go to DC2, r-click on "abc.local" zone and choose properties.

19- Click on "zone transfer" tap, it says that transfer is allowed to server that are listed on "Name Servers" tap

abc.local Properties			?	×
General	5	Start of Authority (S	SOA)	
Name Servers	WINS	Zone	Transfers	
A zone transfer sends a copy copy. Allow zone transfers: To any server Only to servers listed o	of the zone t	to the servers that Servers tab	request a	
IP Address		Server FQDN		
			Edit	
To specify secondary serv updates, click Notify.	ers to be no	tified of zone	Notify	
ОК	Cancel	Apply	Hel	p

20- The point is "Name Servers" tap has only DC2, and we need to add DC1 (which has the secondary zone) in it.

abc.local Properties ?						
General	Star	t of Authority (SO	A)			
Name Servers	WINS	Zone T	ransfers			
To add name servers to the list, click Add.						
Name servers:	Name servers:					
Server Fully Qualified Don	nain Name (FQDN)	IP Addres	55			
dc1.lab.local.		[10.10.10	0.1]			
	dc2.lab.local. [10.10.10.2]					
Add Edit.	Remov	e				
Add Edit Remove * represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.						
OK	Cancel	Apply	Help			

- 21- Wait a minute for the transfer to happen, and you can refresh the zone on DC1 to see that transfer has been successful.
- 22- Create a new "Host (a)" record on the primary zone, and check if the zone transfer has been successful in the secondary zone.
- 23- Try to create a new record on the secondary zone, you won't find the option to do so. As this copy of the zone is read only.

Active Directory Integrated Zone

Benefits of DNS integrated Active Directory

- Multimaster update and enhanced security based on the capabilities of Active Directory.
- Zones are replicated and synchronized to new domain controllers automatically whenever a new one is added to an Active Directory domain.
- Directory replication is faster and more efficient and secure than standard DNS replication.
- Multiple masters are created for DNS replication. Therefore, any domain controller in the domain running the DNS Server service can write updates to the Active Directory-integrated DNS zones.
- Secure dynamic updates are supported.
- A forest-wide application directory partition is available in this scenario, called ForestDnsZones.
- Domain-wide application directory partitions for each domain in the forest, named DomainDnsZones.

To get the benefits of DNS integrated Active Directory, the steps are very simple, we will delete the secondary zone "abc.local" from DC1. Then convert the primary zone on DC2 to an Active Directory integrated zone.

Please notice that both DC1 and DC2 are domain controllers.

24- Delete the secondary zone from DC1

D Zones D Zones D Cal Name as parent folder) (same as parent folder) (same as parent folder)	Type Start of Authority (SOA) Name Server (NS) Name Server (NS)	Data [4], dc2.lab.local, hostmaste dc2.lab.local. dc1.lab.local.	Timestamp static static static	
Reload Transfer from Master Transfer new copy of zone from Master All Tasks	>			
View				
Delete Refresh Export List				
Properties				
Help				
	Zones cal (same as parent folder) (same as	Zones cal (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) Name Server (NS) Name Serve	Zones cal (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) (same as parent folder) Name Server (NS) Name Server (NS) All Calablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. tselection. Start of Authority (SOA) Name Server (NS) (dcllablocal. dcllablocal. (dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. dcllablocal. same as a second the se	Zones cal (same as parent folder) (same as parent folder) Name Server (NS) Name Server (NS) Name Server (NS) (d.lab.local. dcllab.local. (d.lab.local

25- Open DNS on DC1 and r-click on the zone and choose properties, then click on "Change"

🛔 DNS Manager

File Action View	Help							
🗢 🄿 🙍 🏹	t 🖻 🗟 🗟 🖪 📰	1						
Abc.local Properties				? ×				
DC2 Forward Lo	Name Servers WINS General Start of Author			Zone Transfers ority (SOA)				
> 📑 Iab.loca	Status: Running			Pause				
 Reverse Loc Trust Points 	Type: Primary		\rightarrow	Change				
> 📔 Conditiona	Replication: Not an Active	Directory-integra	ated zone	Change				
	Zone file name:							
	abc.local.dns							
	Dynamic updates:	Nonse	Nonsecure and secure $\qquad \lor$					
	Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted sources.							
	To set aging/scavenging properties, click Aging. Aging							
			_					
	ОК	Cancel	Apply	Help				

26- Check on the option to store the zone in Active Directory, then click "OK".

Change Zone Type	×
Select a zone type:	
Primary zone	
Stores a copy of the zone that can be updated directly.	
O Secondary zone	
Stores a copy of an existing zone. This option helps balance the pr servers and provides fault tolerance.	ocessing load of primary
Stub zone Stores a copy of a zone containing only NS, SOA, and possibly glue A records. A server containing a stub zone is not authoritative for that zone.	2
Store the zone in Active Directory (available only if DNS server is a c	domain controller)
	OK Cancel

- 27- In the confirmation message, click "Yes"
- 28- Click "Ok" to close the properties window.
- 29- Now, we just have to wait just minutes for the replication to take place, and the zone will appear on DC1 with the latest updates with no further configuration.