DNS Management

Part 2: Managing A-Records, CNAME Records, and Local DNS Cache

Microsoft Active Directory

1 Introduction

1.1 What is a DNS? And why is it needed?

Following my successful implementation of Active Directory on Azure, I am now embarking on the crucial task of managing Domain Name System (DNS) services. This project will document my journey in configuring and managing a DNS server using Azure Virtual Machines (Windows 10 and Server 2022), DNS Manager, and Command Prompt.

DNS is a fundamental component of network infrastructure, acting as the 'phonebook' of the Internet. It translates human-readable domain names into IP addresses, enabling efficient communication between devices. Proper DNS management is vital for several reasons:

1. Network performance optimisation
2. Enhanced security through proper name resolution
3. Simplified network administration
4. Improved user experience with faster web browsing
5. Support for other network services and applications

By configuring my own DNS server in conjunction with the previously established Active Directory environment, I aim to gain hands-on experience in:

1. Creating and managing DNS records
2. Integrating DNS with Active Directory for seamless name resolution

This project will not only enhance my understanding of DNS management but also provide valuable insights into the interplay between various network services in a Windows Server environment. Through this endeavour, I will further develop my skills in network administration and infrastructure management, cementing my knowledge for future IT challenges.

1.2 Resources and Software tools we'll be using

The Azure resources we'll be creating and working with:

- Azure Virtual Machines (Windows Server 2022 and Windows 10)

Software/Tools we'll be using to configure Active Directory:

- DNS Manager
- Command Prompt

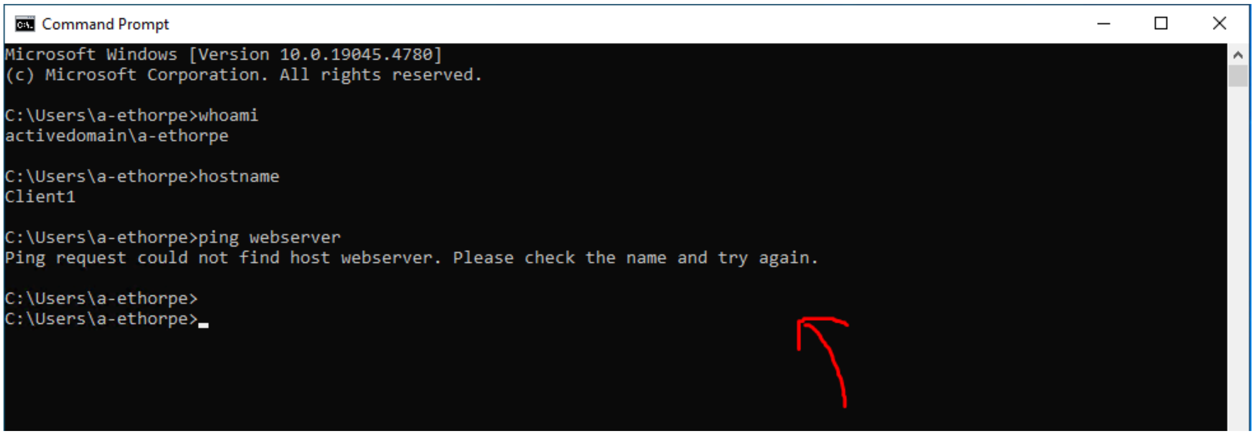
2 Setting up an A-Record

A-Records (Address Records) are crucial for translating human-friendly domain names into IP addresses that computers use to communicate over the internet. When a user types a website name into their browser, an A-Record maps that domain name to the corresponding IP address, enabling the browser to locate and connect to the correct web server.

This mapping simplifies network communication, making it easier for users and systems to access and interact with online services and resources. By providing a consistent way to link domain names to IP addresses, A-Records play a vital role in ensuring reliable and efficient network operations.

2.1 Testing Client Machine

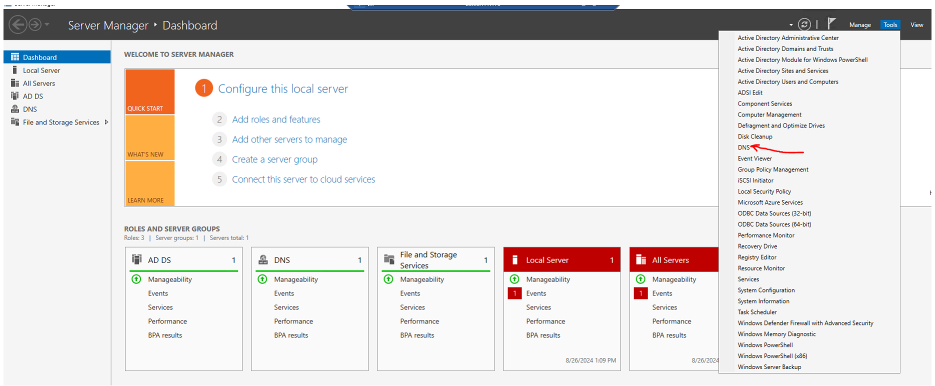
First we'll be testing out Client Machine, just to make sure everything is correct and that we cannot ping to an A-Record we will later set up.



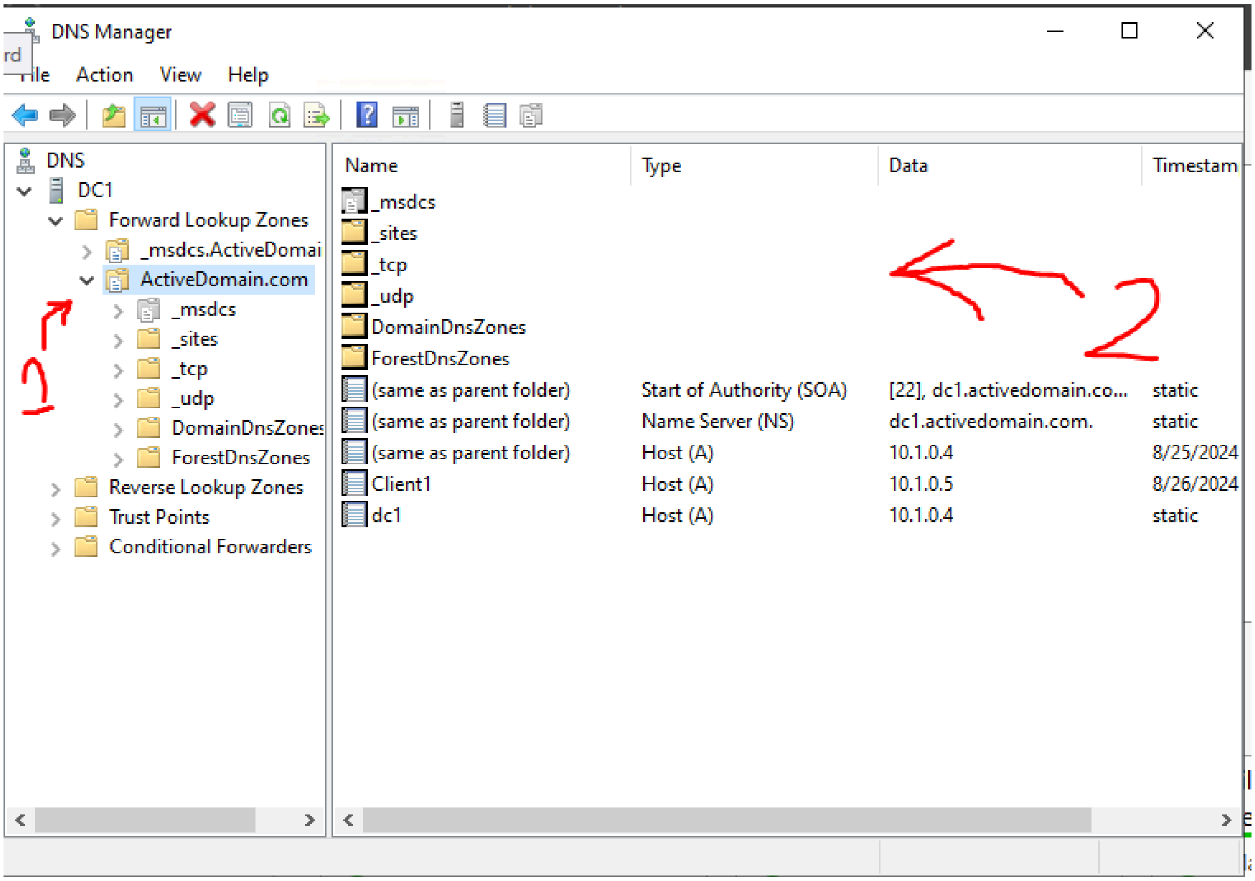
```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\a-ethorpe>whoami
activedomain\a-ethorpe

C:\Users\a-ethorpe>hostname
Client1

C:\Users\a-ethorpe>ping webserver
Ping request could not find host webserver. Please check the name and try again.

C:\Users\a-ethorpe>
C:\Users\a-ethorpe>
```

- 1. we'll just test to see if we are a domain under the domain server
    - Type "whoami"
- 2. we'll check the hostname, just to make sure it's Client1
- 3. Type in "ping webserver". We'll see that we cannot find this host. We'll now setup a webserver A-Record

2.2 Setting up an A-Record



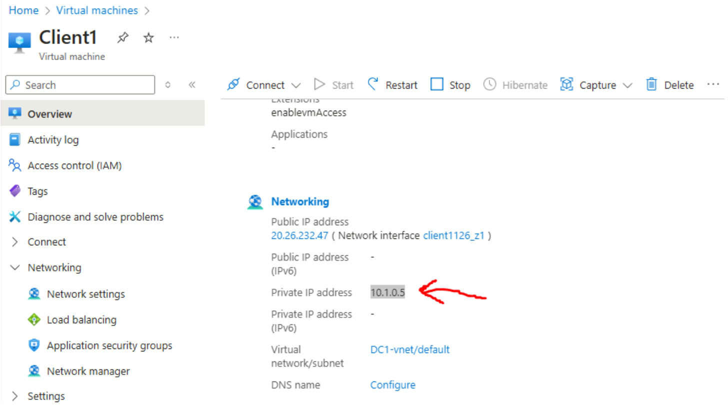
- Go to Tools > Select DNS



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[22], dc1.activedomain.co...	static
(same as parent folder)	Name Server (NS)	dc1.activedomain.com.	static
(same as parent folder)	Host (A)	10.1.0.4	8/25/2024
Client1	Host (A)	10.1.0.5	8/26/2024
dc1	Host (A)	10.1.0.4	static

- Go to our DNS Manager
- 1. Go to ActiveDomain.com by going through DNS>DC1>Forward Lookup Zones>ActiveDomain.com
- 2. Here you'll find all your A-Records. The reason why Client1 couldn't ping webserver is because it couldn't find any records called "webserver"

Now we’re going to set up our new A-Record. Before doing so, we need to find our Private IP address for our Client machine.



Extensions
enablevmAccess

Applications
-

Networking

Public IP address
20.26.232.47 (Network interface client1126_z1)

Public IP address (IPv6) -

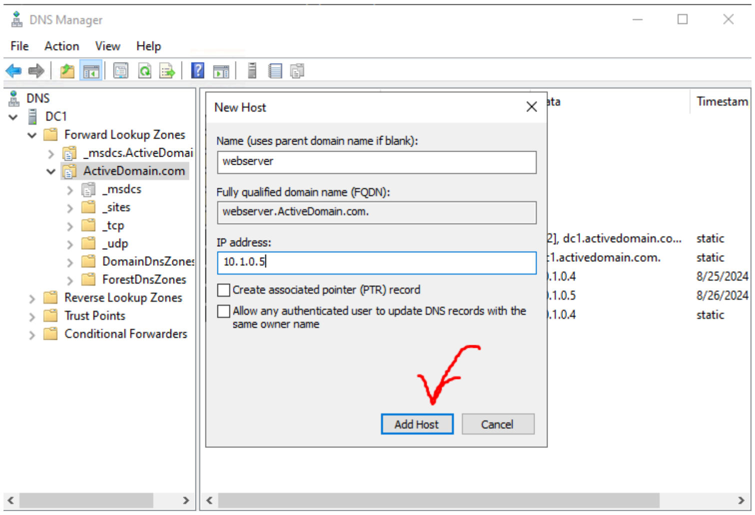
Private IP address 10.1.0.5

Private IP address (IPv6) -

Virtual network/subnet DC1-vnet/default

DNS name Configure

- Copy this IP Address



New Host

Name (uses parent domain name if blank):
webserver

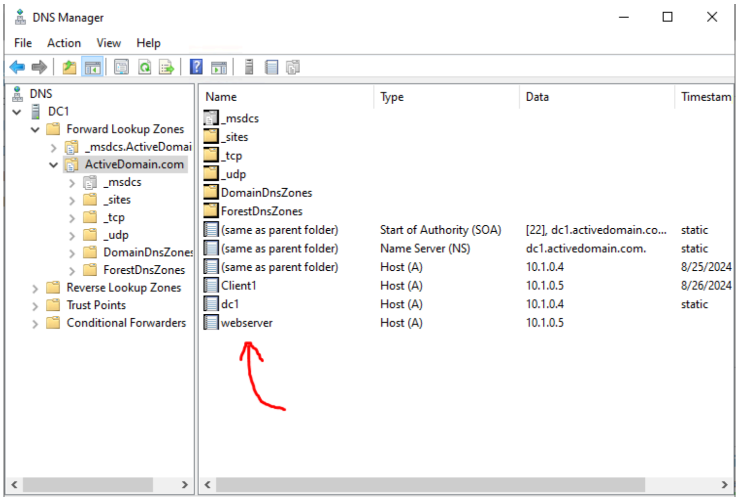
Fully qualified domain name (FQDN):
webserver.ActiveDomain.com.

IP address:
10.1.0.5

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

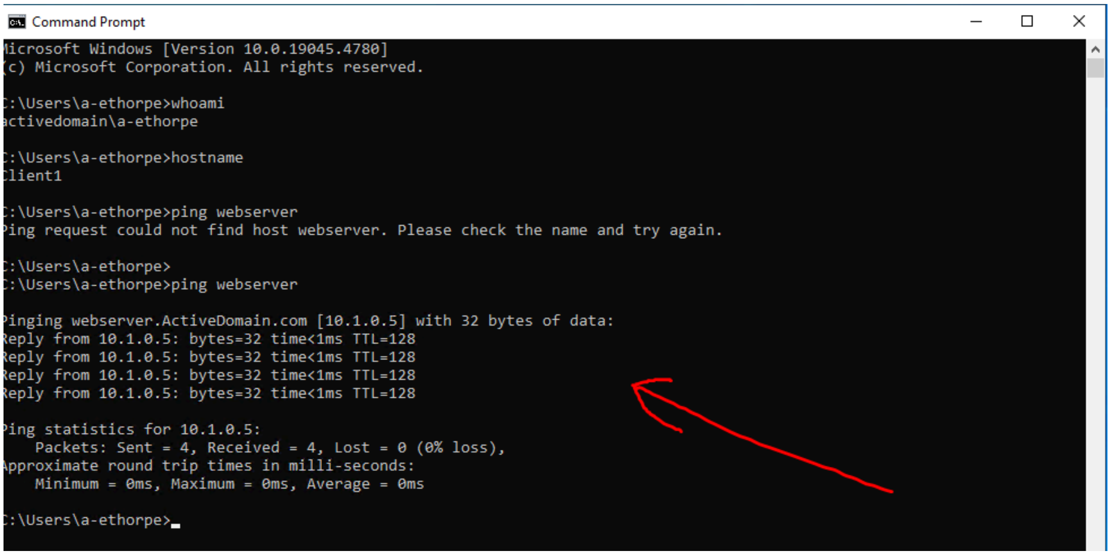
- Set the name “webserver” or whatever you’d like to call the A-Record
- Paste the IP address
- Add Host



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[22], dc1.activedomain.co...	static
(same as parent folder)	Name Server (NS)	dc1.activedomain.com.	static
(same as parent folder)	Host (A)	10.1.0.4	8/25/2024
Client1	Host (A)	10.1.0.5	8/26/2024
dc1	Host (A)	10.1.0.4	static
webserver	Host (A)	10.1.0.5	

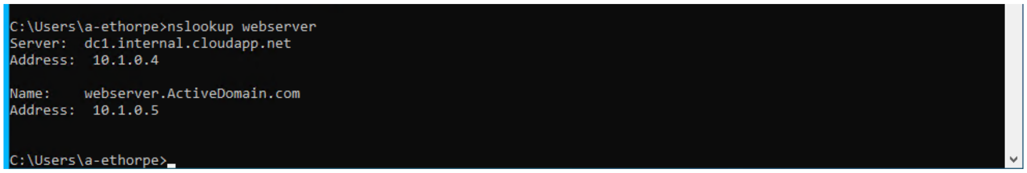
- webserver

2.2.1 Testing A-Record



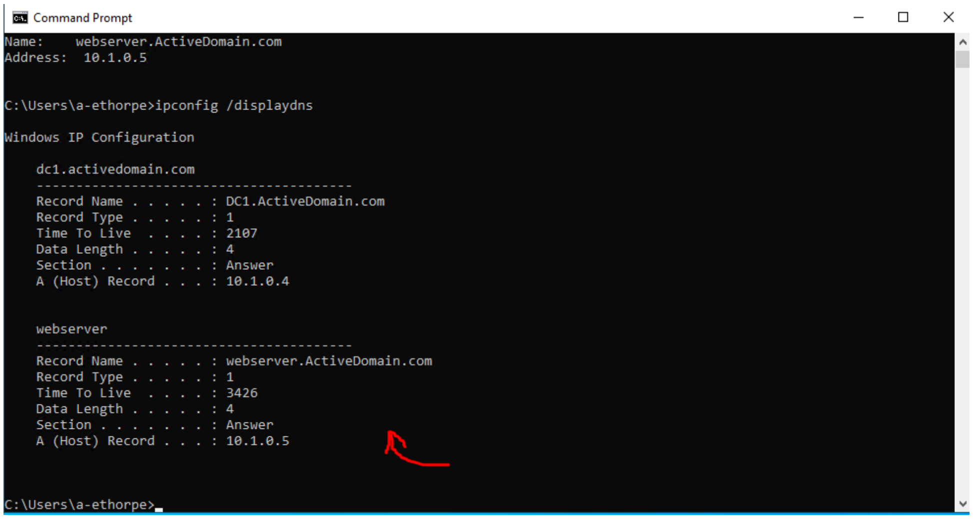
```
icrosoft Windows [Version 10.0.19045.4780]
c) Microsoft Corporation. All rights reserved.

:\Users\a-ethorpe>whoami
ctivedomain\a-ethorpe

:\Users\a-ethorpe>hostname
lient1

:\Users\a-ethorpe>ping webserver
ing request could not find host webserver. Please check the name and try again.

:\Users\a-ethorpe>
:\Users\a-ethorpe>ping webserver

inging webserver.ActiveDomain.com [10.1.0.5] with 32 bytes of data:
eply from 10.1.0.5: bytes=32 time<1ms TTL=128
eply from 10.1.0.5: bytes=32 time<1ms TTL=128
eply from 10.1.0.5: bytes=32 time<1ms TTL=128
eply from 10.1.0.5: bytes=32 time<1ms TTL=128

ing statistics for 10.1.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\a-ethorpe>_
```

- If we go back to our Client Machine and ping to webserver, we'll now see it works!



```
C:\Users\a-ethorpe>nslookup webserver
Server:  dc1.internal.cloudapp.net
Address:  10.1.0.4

Name:    webserver.ActiveDomain.com
Address:  10.1.0.5

C:\Users\a-ethorpe>_
```

- We can type "nslookup webserver" to look up the information regarding webserver.
- "nslookup" is a command-line tool used to query DNS (Domain Name System) servers to obtain information about domain names and IP addresses.

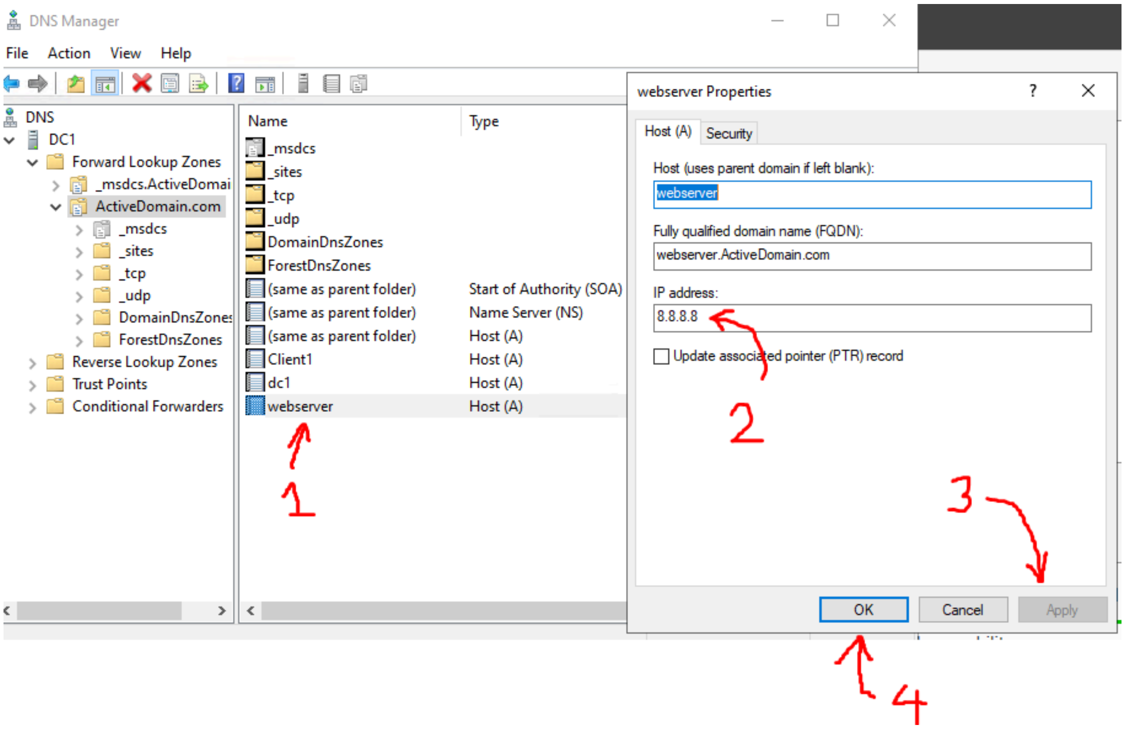


```
Name:    webserver.ActiveDomain.com
Address:  10.1.0.5


C:\Users\a-ethorpe>ipconfig /displaydns

Windows IP Configuration

    dc1.activedomain.com
    ----------------------------------------
    Record Name . . . . . : DC1.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 2107
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.4


    webserver
    ----------------------------------------
    Record Name . . . . . : webserver.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 3426
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.5


C:\Users\a-ethorpe>_
```

- We can then check to see all the DNS ip addresses we have.
- Type ipconfig /displaydns
- As shown by the arrow, the webserver IP information showcases everything is as we intended.

2.2.2 Changing IP Address

Something we can do is change the IP address of our A-Record. We'll change it to 8.8.8.8 which is one of Google's public DNS servers, which provides a free, fast, and reliable DNS resolution service for users around the world.



Name	Type
_msdcs	
_sites	
_tcp	
_udp	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of Authority (SOA)
(same as parent folder)	Name Server (NS)
(same as parent folder)	Host (A)
Client1	Host (A)
dc1	Host (A)
webserver	Host (A)

Host (uses parent domain if left blank): webserver

Fully qualified domain name (FQDN): webserver.ActiveDomain.com

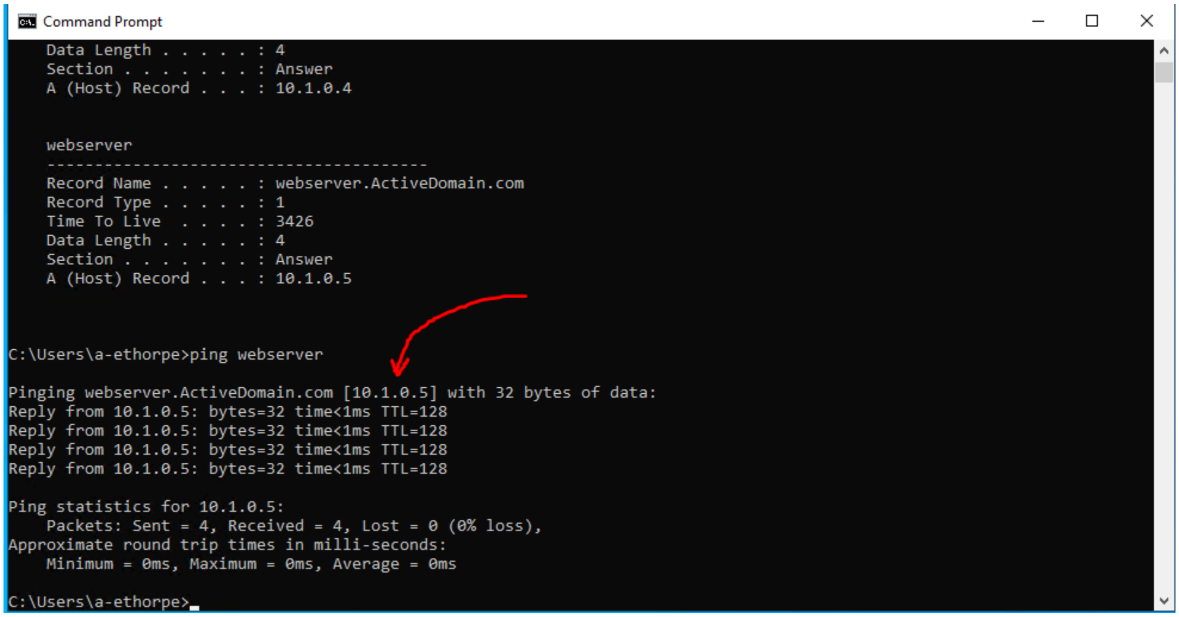
IP address: 8.8.8.8

☐ Update associated pointer (PTR) record

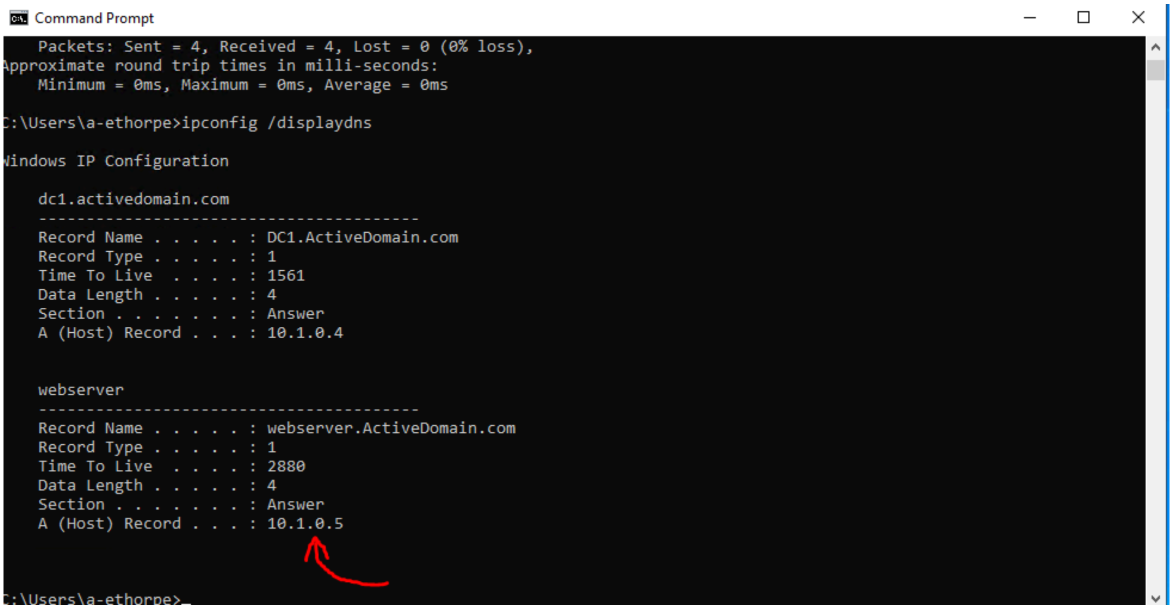
- 1. Right click webserver and select Properties
- 2. Change the IP address to 8.8.8.8
- 3. Click Apply
- 4. Click OK

2.2.3 Testing New IP Address

Now we'll test the new IP address

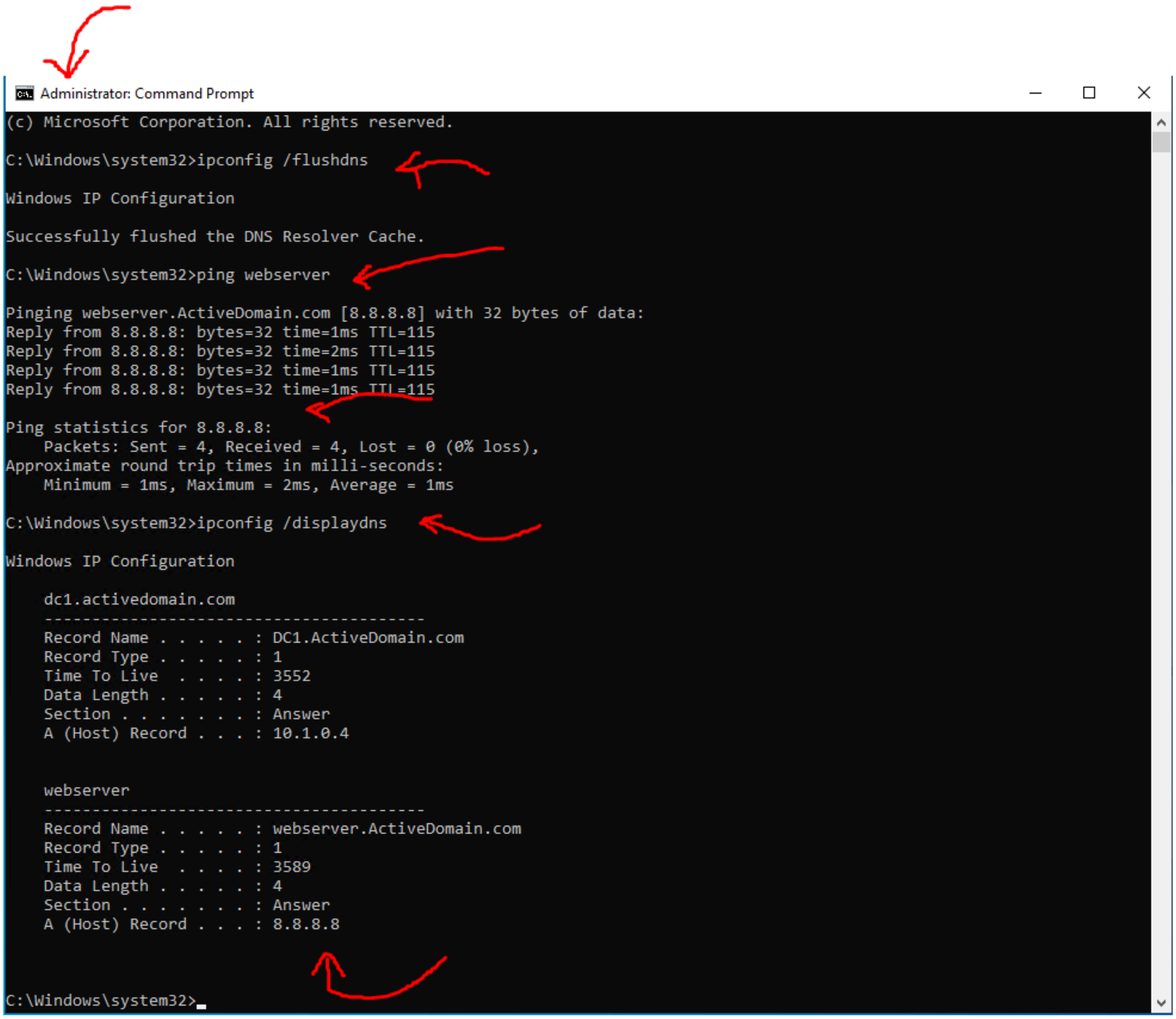


```
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.4


    webserver
    ----------------------------------------
    Record Name . . . . . : webserver.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 3426
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.5


C:\Users\a-ethorpe>ping webserver

Pinging webserver.ActiveDomain.com [10.1.0.5] with 32 bytes of data:
Reply from 10.1.0.5: bytes=32 time<1ms TTL=128
Reply from 10.1.0.5: bytes=32 time<1ms TTL=128
Reply from 10.1.0.5: bytes=32 time<1ms TTL=128
Reply from 10.1.0.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\a-ethorpe>_
```



```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

:\Users\a-ethorpe>ipconfig /displaydns

Windows IP Configuration

    dc1.activedomain.com
    ----------------------------------------
    Record Name . . . . . : DC1.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 1561
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.4


    webserver
    ----------------------------------------
    Record Name . . . . . : webserver.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 2880
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.5


:\Users\a-ethorpe>_
```

- As we see here, when we ping to our webserver, it still shows 10.1.0.5 - our old IP address
- The reason for this is because the ip config is current cached, so the new IP address would not be assigned. In order to fix this, we'll have to use flushdns



```
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig /flushdns

Windows IP Configuration

Successfully flushed the DNS Resolver Cache.

C:\Windows\system32>ping webserver

Pinging webserver.ActiveDomain.com [8.8.8.8] with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=1ms TTL=115
Reply from 8.8.8.8: bytes=32 time=2ms TTL=115
Reply from 8.8.8.8: bytes=32 time=1ms TTL=115
Reply from 8.8.8.8: bytes=32 time=1ms TTL=115

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Windows\system32>ipconfig /displaydns

Windows IP Configuration

    dc1.activedomain.com
    ----------------------------------------
    Record Name . . . . . : DC1.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 3552
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 10.1.0.4


    webserver
    ----------------------------------------
    Record Name . . . . . : webserver.ActiveDomain.com
    Record Type . . . . . : 1
    Time To Live  . . . . : 3589
    Data Length . . . . . : 4
    Section . . . . . . . : Answer
    A (Host) Record . . . : 8.8.8.8


C:\Windows\system32>
```

- 1. To do this we'll have to first open a new command line and run as Administrator
- 2. Type "ipconfig /flushdns"
- 3. Type "ping webserver"
- 4. You'll see that we're getting a ping back from 8.8.8.8 - as intended
- 5. Type "ipconfig /displaydns"
- 6. You'll see we are getting a DNS ip address of 8.8.8.8 - also, as intended

We have successfully made AND changed a A-Record!

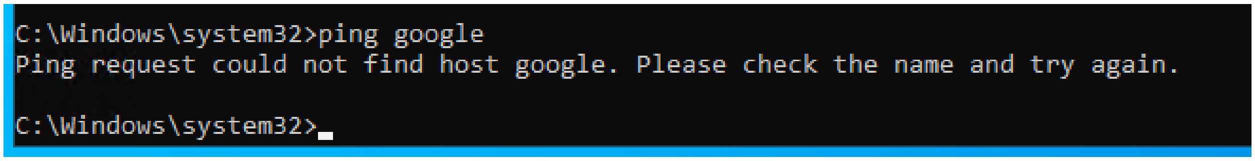
3 Setting up a CNAME Record

CNAME Records (Canonical Name Records) are used in DNS to create an alias for a domain name. Unlike A-Records, which map a domain directly to an IP address, CNAME records point one domain name to another domain name. This allows multiple domain names to resolve to the same IP address indirectly, using the primary domain's A-Record.

Key Differences:

1. **Purpose:**
    - **CNAME Record:** Used to alias one domain name to another. For example, www.example.com might point to example.com, so both domains resolve to the same IP address.
    - **A-Record:** Directly maps a domain name to an IP address. For example, example.com is directly mapped to 192.168.1.1.
2. **Flexibility:**
    - **CNAME Record:** Useful for managing subdomains and providing a single point of configuration. If the IP address of the primary domain changes, only the A-Record for that domain needs to be updated, and all CNAME-alias domains will automatically follow the change.
    - **A-Record:** Directly associates a domain with an IP address, which can be less flexible if multiple domains need to point to the same IP address. Each domain with its own A-Record would need to be updated separately if the IP address changes.

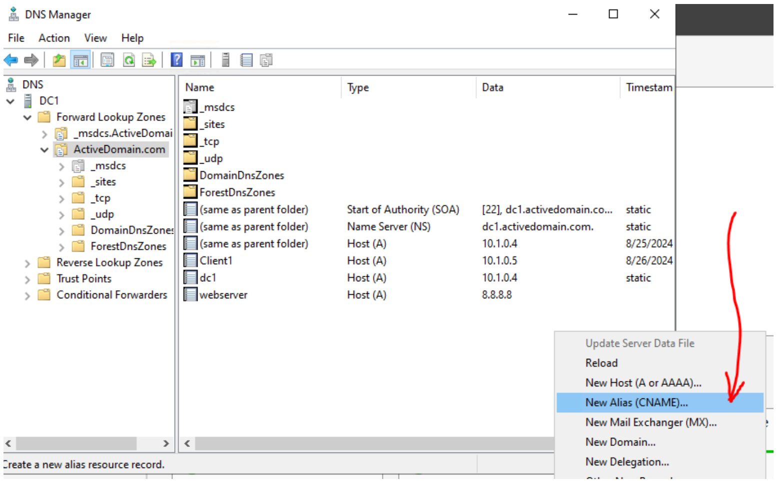
For this, we'll set up a CNAME for Google. As shown below, if we ping to "google", it won't be able to find the host.



```
C:\Windows\system32>ping google
Ping request could not find host google. Please check the name and try again.

C:\Windows\system32>_
```

3.1 Set up CNAME

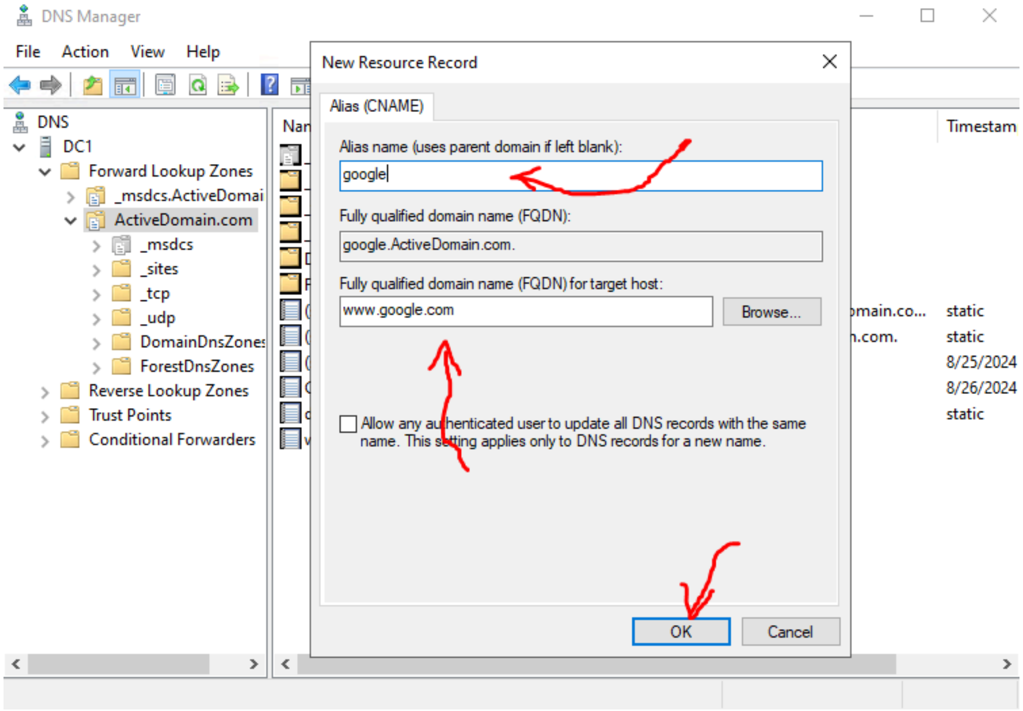
First, we'll go back to our Windows Server 2022



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[22], dc1.activedomain.co...	static
(same as parent folder)	Name Server (NS)	dc1.activedomain.com.	static
(same as parent folder)	Host (A)	10.1.0.4	8/25/2024
Client1	Host (A)	10.1.0.5	8/26/2024
dc1	Host (A)	10.1.0.4	static
webserver	Host (A)	8.8.8.8	

Create a new alias resource record.

- Right click in an empty area within ActiveDomain.com DNS manager
- Click "New Alias (CNAME)"



Alias name (uses parent domain if left blank): google

Fully qualified domain name (FQDN): google.ActiveDomain.com.

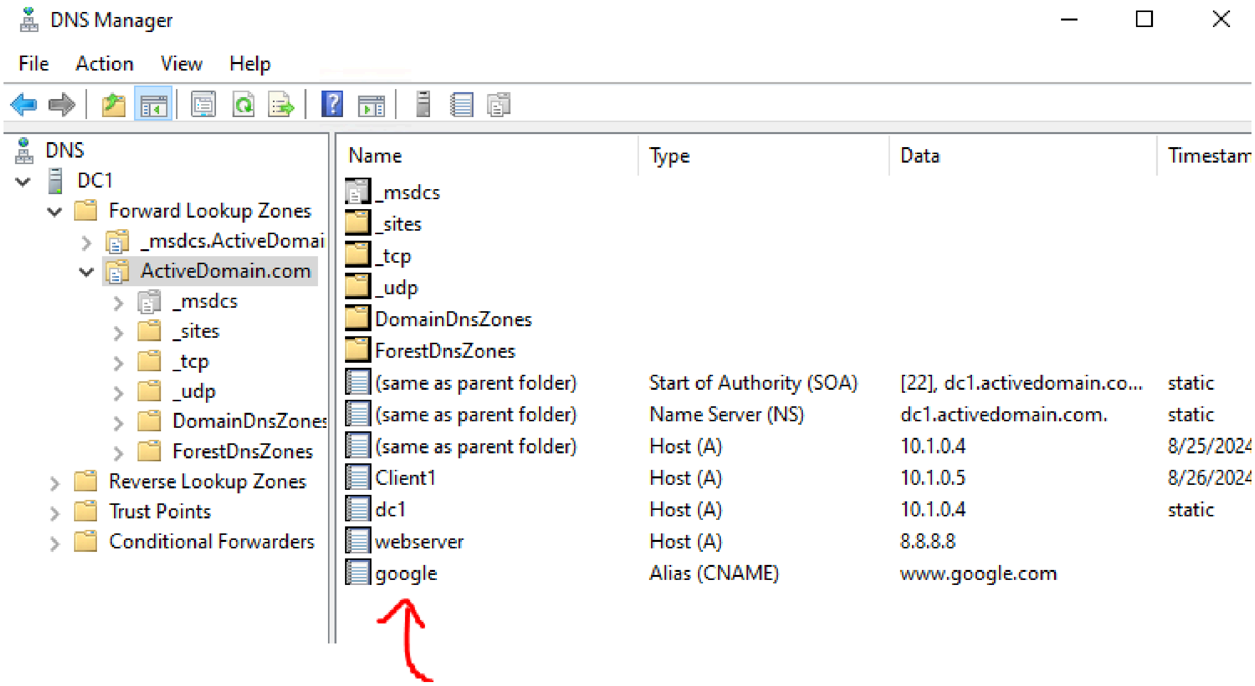
Fully qualified domain name (FQDN) for target host: www.google.com

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

-

- First we type the alias name "google"
- Select the fully qualified domain name "www.google.com"
- Press "OK"

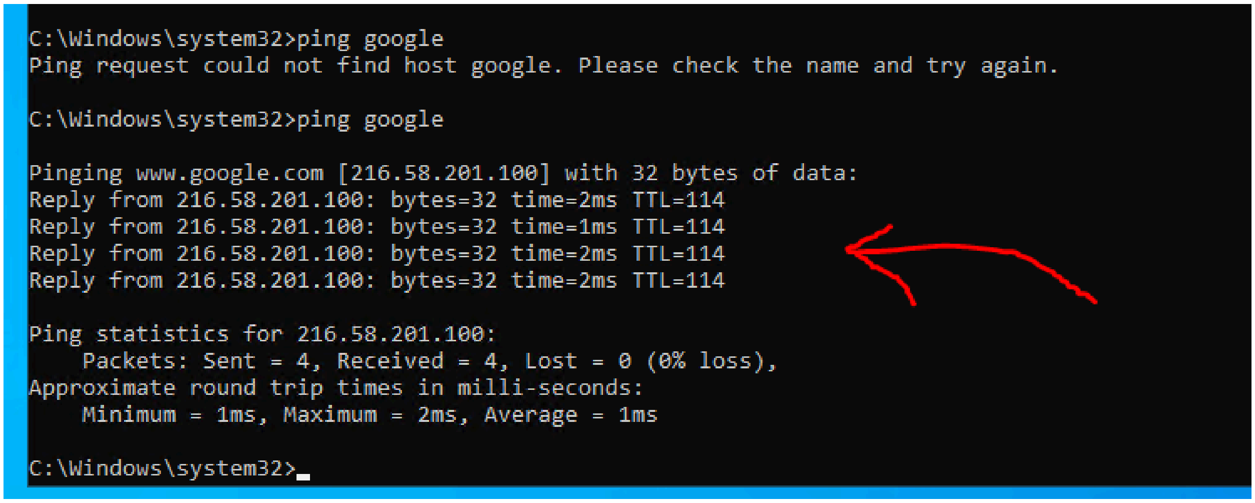
3.2 Testing new CNAME



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[22], dc1.activedomain.co...	static
(same as parent folder)	Name Server (NS)	dc1.activedomain.com.	static
(same as parent folder)	Host (A)	10.1.0.4	8/25/2024
Client1	Host (A)	10.1.0.5	8/26/2024
dc1	Host (A)	10.1.0.4	static
webserver	Host (A)	8.8.8.8	
google	Alias (CNAME)	www.google.com	

- Now we can see Google as an Alias.

When we go back to the client machine, we can check to see if we can ping to this new Alias and see if it pings to www.google.com



```
C:\Windows\system32>ping google
Ping request could not find host google. Please check the name and try again.

C:\Windows\system32>ping google

Pinging www.google.com [216.58.201.100] with 32 bytes of data:
Reply from 216.58.201.100: bytes=32 time=2ms TTL=114
Reply from 216.58.201.100: bytes=32 time=1ms TTL=114
Reply from 216.58.201.100: bytes=32 time=2ms TTL=114
Reply from 216.58.201.100: bytes=32 time=2ms TTL=114

Ping statistics for 216.58.201.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\Windows\system32>_
```

- As shown here. It works! We have successfully made a CNAME.

4 Conclusion

In this project, I successfully delved into DNS management, building upon my previous work with Active Directory deployment on Azure. The key accomplishments include:

1. Setting up and managing A-Records, demonstrating their crucial role in translating domain names to IP addresses.

2. Creating an A-Record for a 'webserver' and testing its functionality using ping and nslookup commands.

3. Modifying the A-Record's IP address and observing the effects, including the need to flush the DNS cache for immediate updates.

4. Establishing a CNAME Record to create an alias for Google, showcasing the flexibility of DNS in managing domain name associations.

5. Utilising various tools such as DNS Manager and Command Prompt to configure and test DNS settings.

6. Gaining hands-on experience in troubleshooting DNS-related issues and understanding the importance of proper DNS management in network infrastructure.

This practical exercise has significantly enhanced my understanding of DNS operations within a Windows Server environment and its integration with Active Directory.

Moving forward, I plan to expand this project to simulate a more comprehensive, real-life Active Directory environment. The next phase will focus on:

1. Creating a more complex organisational unit structure, reflects a typical enterprise setup.
2. Implementing robust user and object management practices.
3. Establishing and testing password reset procedures.
4. Creating and managing service accounts for various network services and applications.

By undertaking these advanced tasks, I aim to further solidify my skills in network administration and gain a deeper insight into the complexities of managing a large-scale Active Directory infrastructure. This experience will be invaluable in preparing me for real-world IT challenges and enhancing my capabilities as an IT professional.