

Landesberufsschule 4 Salzburg

Übungen im

Laboratorium für Systemtechnik

DNS

für die Übung Nr. 1

Katalog - Nr.: 1

Name : Valentin Adlgasser

Jahrgang : 2020

Datum der Übung : 17.09.2020

Inhalt

1. Anweisung der Übung:	3
2. Einleitung.....	3
3. Inventarliste.....	3
4. Übungsdurchführung	4
a. Begriffserklärung	4
b. VM erstellen	5
c. DNS Suffix vergeben	5
d. DNS Rolle installieren	6
e. Forward-Lookup-Zone installieren	6
f. Host erstellen	7
g. Reverse-Lookup-Zone erstellen.....	8
h. PTR-Eintrag erstellen	9
i. CNAME-Eintrag erstellen.....	10
j. Weiterleitung.....	10
5. Einsatzgebiet	10
6. Erkenntnisse	10
7. Abbildungsverzeichnis.....	11

1. Anweisung der Übung:

In dieser Übung werden zuerst Fragen über DNS beantwortet und danach eine Virtuelle Maschine erstellt, welcher als DNS fungieren soll.

2. Einleitung

Ein Domain Name System (DNS) ist ein System zur Auflösung von IP-Adressen in, von Menschen lesbare, Namen. Ein DNS ist also grob beschrieben eine Datenbank, welche Namen zu IP-Adressen gespeichert hat. Dieser Service wurde eingeführt, weil es für normale PC Benutzer extrem schwierig ist, sich IP Adressen zu merken, Namen allerdings sind leicht merkbar und aussagekräftiger.

3. Inventarliste

- VirtualBox (Version 6.1.10)
- VM Windows Server 2016
- 4GB Ram
- 50GB VHD

4. Übungsdurchführung

a. Begriffserklärung

- **Domain-Name-Service:** Ein Domain-Name-Service ist ein Service, welcher IP-Adressen in Namen auflöst, oder umgekehrt.
- **TLD und FQDN:** Eine Top-Level-Domain (TLD) ist der letzte Teil eines Domainnamens (*www.zufaelligeurl.com*) und ist damit die oberste Ebene einer Domain. FQDN (Fully Qualified Domain Name) bezeichnet den vollständigen Namen einer Domain, z.B. *www.zufaelligeurl.com*.
- **Forward-Lookup-Zone / Reverse-Lookup-Zone:** Wenn eine DNS-Abfrage Anfrage vom Client an den DNS-Server geschickt wird, schickt der Client meist einen Domainnamen und der Server antwortet mit der IP-Adresse. Dieser Vorgang nennt sich Forward-Lookup. Der Server hat dafür eine eigene Datenbank, in welcher die Domainnamen als Name gespeichert werden und die IP-Adressen als Daten. Wenn der Client allerdings eine Anfrage mit einer IP-Adresse an den Server schickt, dann soll der DNS-Server einen Domainnamen zurückschicken. Dafür hat der Server eine zweite Datenbank eingerichtet, in welcher die IP-Adressen als Namen gespeichert sind und die Domainnamen als Daten. Diese Datenbank nennt sich Reverse-Lookup-Zone.
- **Zonen-Dateien:** Der DNS-Server speichert die IP-Adressen und Domainnamen, sowie weitere Details in sogenannten Zonen-Dateien (DNS-Records). Diese legt der Server entweder in der Forward-Lookup-Zone oder in der Reverse-Lookup-Zone ab.
- **PTR, SOA und CNAME Resource Record:** PTR (Pointer) Resource Records sind Bestandteile einer Zonen Datei. Sie ordnen im DNS einer IP-Adresse eine oder mehrere Hostnamen zu.
SOA (Start of Authority) Resource Record ist ein weiterer Bestandteil einer Zonen-Datei. Es beinhaltet wichtige, administrative Informationen über die Zone, in welcher sich der Hostname befindet.
CNAME (Canonical Name) Resource Record ist dazu vorgesehen, einer Domäne weitere Namen zuzuordnen.
- **A und AAAA Resource Record:** A Resource Records werden dazu benötigt, um IPv4-Adressen zu Hostnamen zu mappen. AAAA Resource Records werden benutzt um IPv6-Adressen zu mappen.
- **Unterschiede bei Auflösungsanfragen:**
 - Rekursiv: Der DNS-Server holt sich die benötigten Daten von einem anderen DNS-Server und leitet die Daten an den Client weiter.
 - Autoritativ: Der Server holt sich die benötigten Daten aus einer lokalen Zonendatei.
 - Iterativ: Der Server antwortet dem Client mit einem oder mehreren Verweisen zu einem anderen Server.
- **Resolver ablauf anhand eines Beispiels:** Der Resolver ist die Schnittstelle zwischen Programm und DNS-Server. Der Resolver übernimmt die Anfrage und ergänzt sie, falls notwendig, zu einem FQDN. Danach leitet er die FQDN an einen Nameserver weiter. Der Server antwortet daraufhin entweder mit dem angeforderten Datensatz oder antwortet mit einem Verweis auf einen anderen Nameserver. Der Resolver arbeitet sich also von DNS-Server zu DNS-Server durch, bis er entweder den richtigen

Datensatz erhält oder eine negative Antwort erhält.

z.B. Anwendung schickt „lbs4.salzburg.at“ an Resolver -> Resolver ergänzt den Hostnamen zu einem vollständigen FQDN „www.lbs4.salzburg.at.“ -> Resolver schickt Anfrage an DNS Server und erhält die Antwort: 193.170.247.144.

b. VM erstellen

Das Aufsetzen der VM werde ich hier nicht beschreiben, da man diesen Vorgang bereits in vielen anderen Protokollen nachlesen. Man muss nur darauf aufpassen, dass die Netzwerkkarte auf Host-Only gestellt ist.

c. DNS Suffix vergeben

Um den DNS Suffix zu vergeben öffnet man zuerst den Server-Manager, dort klickt man auf die Option „Systemeigenschaften ändern“. Danach klickt man auf den Link „Computernamen“, in dem geöffneten Fenster klickt man nun auf „ändern...“. Danach klickt man unterhalb des Computernamens auf „Weitere...“. Hier kann man nun einfach das DNS-Suffix eintragen. Nachdem man das Suffix geändert hat muss man den Server neustarten.

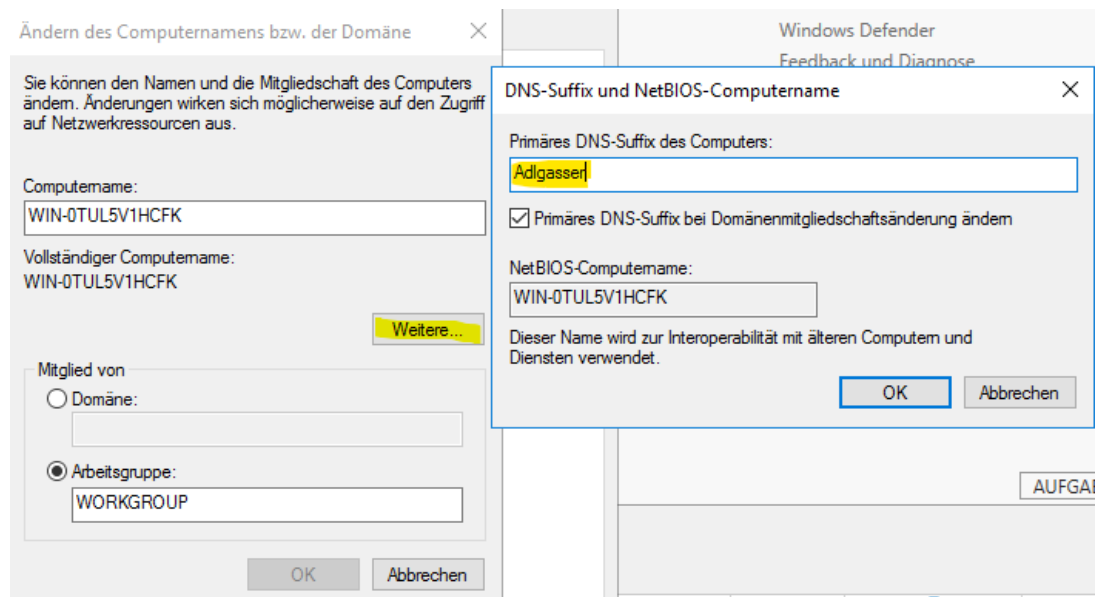


Abbildung 1 | DNS Suffix vergeben

d. DNS Rolle installieren

Um die DNS Rolle zu installieren muss man zuerst eine Powershell Applikation als Administrator starten. Danach gibt man folgenden Befehl ein:

Install-WindowsFeature -Name DNS -IncludeManagementTools

Die Installation läuft danach einfach durch und die DNS Rolle ist installiert. Ist die DNS-Rolle erstellt, muss man noch in den Adapteroptionen die IP-Adresse des DNS-Servers eintragen, in meinem Fall 192.168.56.101, da sonst der Resolver nicht weiß an welchen DNS er die Requests schicken soll.

```
PS C:\Users\Administrator> Install-WindowsFeature -Name DNS -includeManagementTools
WARNUNG: Die folgende empfohlene Bedingung wird für DNS nicht erfüllt: Auf diesem Computer wurden keine statischen IP-Adressen gefunden. Wenn die IP-Adresse geändert wird, können Clients möglicherweise keine Verbindungen mehr mit diesem Server herstellen. Installieren Sie den DNS-Server erst, nachdem Sie eine statische IP-Adresse auf dem Computer konfiguriert haben.

Success Restart Needed Exit Code      Feature Result
-----
True      No                Success      {DNS-Server, Remoteserver-Verwaltungstools...
```

Abbildung 2 | DNS Rolle installieren

e. Forward-Lookup-Zone installieren

Nachdem der Server installiert worden ist kann man die Forward-Lookup-Zone installieren. Dazu klickt man im Server-Manager unter Tools auf den Eintrag „DNS“. Danach einen Rechtsklick auf den Servernamen und „DNS-Server konfigurieren...“ auswählen. Im ersten Schritt entscheidet man ob man eine Forward-Lookup-Zone erstellen will oder eine Forward- und Reverse-Lookup-Zone. In diesem Protokoll erstellt man zuerst nur eine Forward-Lookup-Zone.

Im nächsten Schritt wählt man aus ob der Server DNS-Daten lokal speichern soll. In diesem Protokoll verwaltet der Server die Daten selbst also wählt man „Dieser Server verwaltet die Zone“ aus.

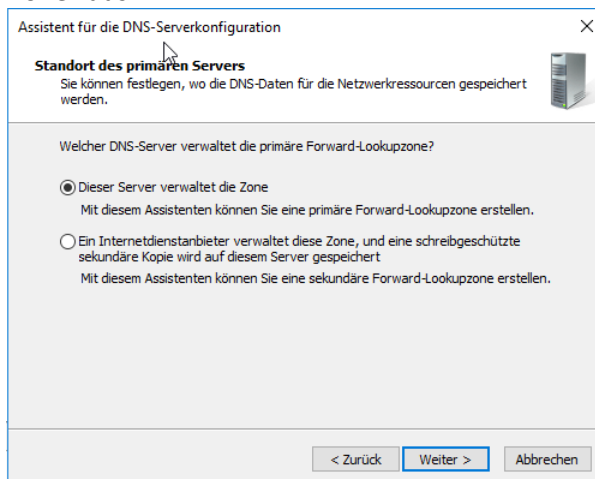


Abbildung 3 | Server verwaltet DNS-Daten

Nachdem man weiter geklickt hat, gibt man nun den Zonennamen an. In meinem Fall lautet der Zonename „test.com“.

#

Abbildung 4 | Zonename

Im nächsten Schritt gibt man an ob eine neue Zonendatei erstellt werden soll. In unserem Fall soll eine neue Zonendatei erstellt werden. Also wählt man „Neue Date mit diesem Dateinamen erstellen:“ aus und gibt den Namen der Zone an.

Auf der nächsten Seite muss man nur noch angeben ob man Updates von Clients zulassen will oder nicht. Danach klickt man auf „Weiter“ und auf „Fertigstellen“.

f. Host erstellen

Um einen A oder AAAA Host zu erstellen muss man im DNS-Manager einen Rechtsklick auf die gerade erstellte Forward-Lookup-Zone machen und danach „Neuer Host (A oder AAAA)...“ auswählen.

Danach gibt man den Hostnamen an und die IP-Adresse. Das Programm erkennt eigenständig ob es sich um eine IPv4- oder IPv6-Adresse handelt und erstellt den richtigen Host. Wenn bereits eine Reverse-Lookup-Zone existiert kann man noch einen hacken bei „Verknüpften PTR-Eintrag erstellen“ um gleich einen PTR-Eintrag zu erstellen.

Um zu testen ob der Host auch wirklich funktioniert gibt man in der CMD den Befehl „nslookup“ ein und danach den Namen des Hosts. Wenn man eine Antwort erhält funktioniert der DNS.

Abbildung 6 | A-Host erstellen

```
C:\Users\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
Standardserver: UnKnown
Address: 192.168.56.101

> test.test
Server: UnKnown
Address: 192.168.56.101

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
Name: test.test
Address: 10.0.0.5
```

Abbildung 5 | nslookup A-Host

g. Reverse-Lookup-Zone erstellen

Um eine Reverse-Lookup-Zone zu erstellen muss man wieder in den DNS-Manager wechseln. Hier macht man einen Rechtsklick auf „Reverse-Lookupzonen“ und wählt „Neue Zone erstellen“ aus.

Danach entscheidet man ob man eine primäre, sekundäre oder Stubzone erstellen will. In unserem Beispiel wählt man Primäre Zone aus.

Im nächsten Fenster entscheidet man ob man eine IPv4 oder IPv6 Reverse-Lookup-Zone erstellen will. In diesem Protokoll erstellen wir eine IPv4-Zone.

Danach gibt man die Netzwerk-ID oder den Namen der Reverse-Lookup-Zone an. In unserem Fall gibt man die Netzwerk-ID ein, welche aus den ersten drei Stellen der IPv4-Adresse des DNS-Servers besteht. In unserem Fall sieht dies so aus:

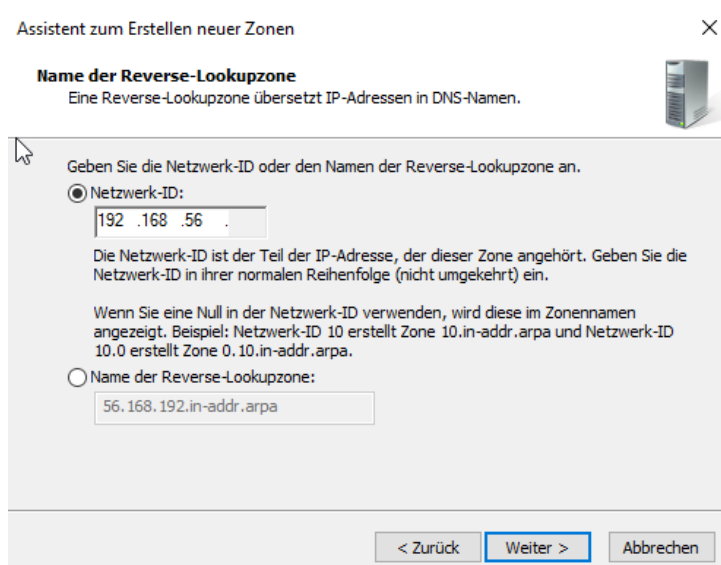


Abbildung 7 | Netzwerk-ID eingeben

Im nächsten Fenster gibt man wieder an ob dynamische Updates erlaubt werden sollen oder nicht. In unserem Fall erlauben wir diese nicht.

Danach kann man die Erstellung wieder abschließen.

h. PTR-Eintrag erstellen

Um einen PTR-Eintrag zu erstellen geht man ähnlich vor wie beim Erstellen eines A-Hosts. Man macht einen Rechtsklick auf die gerade erstellte Reverse-Lookup-Zone und wählt „Neuer Zeiger (PTR)...“ aus.

Im neu geöffneten Fenster gibt man nun die Host-IP-Adresse an und den dazugehörigen Hostnamen.

Danach testet man den Reverse-Lookup wieder in der CMD mit dem Befehl „nslookup“. Erhält man ein Ergebnis zurück, hat alles richtig funktioniert.

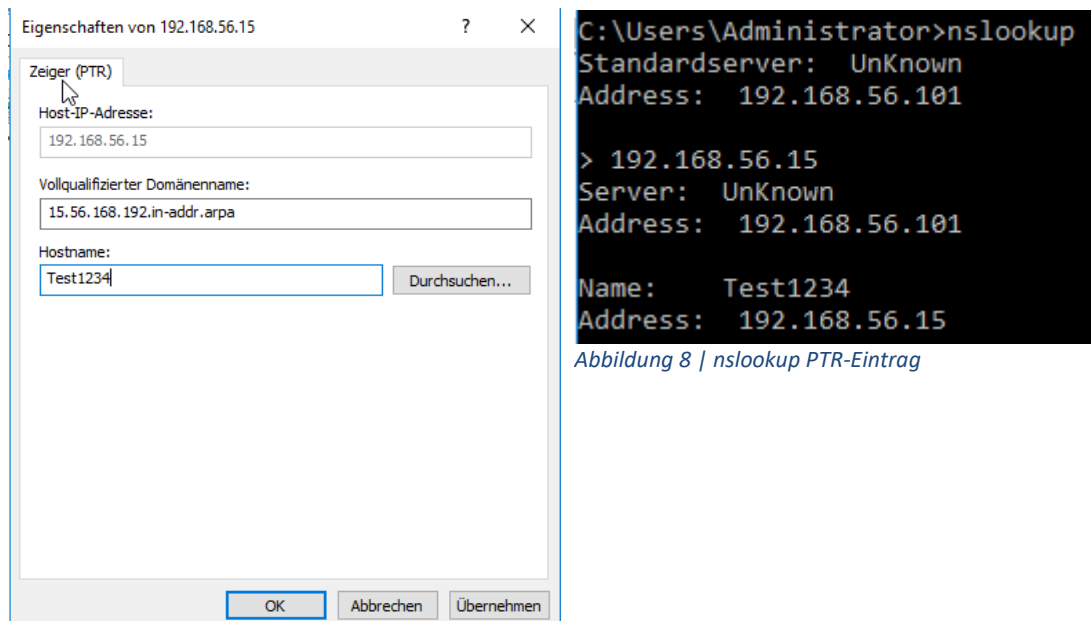


Abbildung 8 | nslookup PTR-Eintrag

Abbildung 9 | PTR-Eintrag erstellen

i. CNAME-Eintrag erstellen

Zum Erstellen eines CNAME-Eintrages geht man wieder fast gleich vor wie beim Erstellen eines A- oder AAAA-Hosts.

Zuerst ein Rechtsklick auf die Forward-Lookup-Zone und „Neuer CNAME...“ auswählen.

Danach gibt man den Aliasnamen ein und klickt weiter unten auf „Durchsuchen...“. Nun wählt man den Zielhost aus und schon ist der CNAME-Eintrag erstellt.

Danach kann man wieder mit dem CMD-Befehl „nslookup“ testen ob auch alles richtig funktioniert hat, indem man den Vollqualifizierten Aliasnamen eingibt.

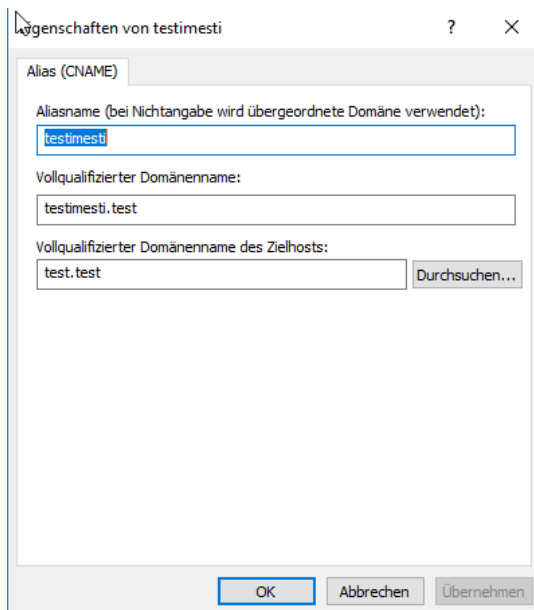


Abbildung 11 | CNAME-Eintrag erstellen

```
C:\Users\Administrator>nslookup
Standardserver: UnKnown
Address: 192.168.56.101

> testimesti.test
Server: UnKnown
Address: 192.168.56.101

DNS request timed out.
  timeout was 2 seconds.
DNS request timed out.
  timeout was 2 seconds.
Name: test.test
Address: 10.0.0.5
Aliases: testimesti.test
```

Abbildung 10 | nslookup CNAME-Eintrag

j. Weiterleitung

Die Weiterleitung wird dazu verwendet, dass wenn der DNS-Server keinen Eintrag zu der geschickten Domain hat, er die Anfrage einfach an einen anderen DNS-Server weiterleitet.

Diese Funktion kann man aktivieren, in dem man im DNS-Manager einen Rechtsklick auf „Bedingte Weiterleitung“ macht und danach „Neue bedingte Weiterleitung“ auswählt. Danach gibt man einfach die Domain des DNS-Servers ein oder dessen IP-Adresse.

5. Einsatzgebiet

Grundsätzlich gibt es viele Einsatzmöglichkeiten für einen eigenen DNS. In vielen Firmen zum Beispiel wird ein eigener DNS verwendet, damit Firmen kontrollieren können wo Anfragen hingeschickt werden und keine man in the middle Attacks stattfinden können.

6. Erkenntnisse

Einen DNS-Server aufzusetzen ist nicht schwierig. Die Schwierigkeit kommt erst dadurch, dass man alle IPs und Domainnamen manuell eintragen muss.

7. Abbildungsverzeichnis

Abbildung 1 DNS Suffix vergeben	5
Abbildung 2 DNS Rolle installieren	6
Abbildung 3 Server verwaltet DNS-Daten	6
Abbildung 4 Zonenname.....	7
Abbildung 5 nslookup A-Host	7
Abbildung 6 A-Host erstellen.....	7
Abbildung 7 Netzwerk-ID eingeben.....	8
Abbildung 8 nslookup PTR-Eintrag	9
Abbildung 9 PTR-Eintrag erstellen	9
Abbildung 10 nslookup CNAME-Eintrag.....	10
Abbildung 11 CNAME-Eintrag erstellen.....	10