

Protokoll zu DNS Task

Inhaltsverzeichnis

Aufgabenstellung (Records):.....	2
Script:	2
„A“:	3
„MX“:	3
„NS“:	4
Ergebnis:.....	4
Aufgabenstellung (Namensauflösung):.....	5
Script:	5
Ergebnis:.....	6

Aufgabenstellung (Records):

- Lege die Einträge der csv-Datei als Records auf deinem DNS-Serve an.
- Schreibe ein Powershell-Script für die Anlage.

Script:

```
$list = Import-CSV -Path "C:\dns_records.csv" -Delimiter ";"

foreach($csv in $list){

    $name = $csv.name
    $ipv4 = $csv.ipv4
    $type = $csv.type

    if($type -eq "A"){
        Add-DnsServerResourceRecordA -Name $name -ZoneName "suljevic.at" -AllowUpdateAny -
IPv4Address $ipv4 -TimeToLive 01:00:00
    }

    if($type -eq "MX"){
        Add-DnsServerResourceRecordMX -Preference 10 -Name $name -TimeToLive 01:00:00 -
MailExchange $ipv4 -ZoneName "suljevic.at"
    }

    if($type -eq "NS"){
        Add-DnsServerResourceRecordA -IPv4Address $ipv4 -Name $name -ZoneName
"suljevic.at";
        Add-DnsServerResourceRecord -NS -ZoneName suljevic.at -Name suljevic.at -NameServer
$($name + ".suljevic.at.");
    }
}
```

Der Inhalt von der CSV Datei wird ausgelesen:

```
$list = Import-CSV -Path "C:\dns_records.csv" -Delimiter ";"
```

Danach wird der Inhalt in eine foreach Schleife durchgegangen

Die if Abfragen schauen, ob der **\$type** gleich einem **A**, **MX** oder **NS** entspricht

„A“:

```
Add-DnsServerResourceRecordA -Name $name -ZoneName "suljevic.at" -  
AllowUpdateAny -IPv4Address $ipv4 -TimeToLive 01:00:00
```

- Name** → Gibt einen Hostnamen an
- ZoneName** → Gibt den Namen einer DNS-Zone an
- AllowUpdateAny** → Gibt an, dass jeder authentifizierte Benutzer einen Ressourceneintrag mit demselben Eigentümernamen aktualisieren kann.
- IPv4Address** → Gibt ein Array von IPv4-Adressen an.
- TimeToLive** → Gibt den Time to Live in Sekunden für einen Ressourceneintrag an. Andere DNS-Server verwenden diese Zeitspanne, um zu bestimmen, wie lange ein Datensatz zwischengespeichert werden soll.

„MX“:

```
Add-DnsServerResourceRecordMX -Preference 10 -Name $name -TimeToLive 01:00:00  
-MailExchange $ipv4 -ZoneName "suljevic.at"
```

- Name** → Gibt den Namen der Host- oder untergeordneten Domäne für den Mail-Exchange-Datensatz an.
- ZoneName** → Gibt den Namen einer DNS-Zone an
- TimeToLive** → Gibt den Time to Live in Sekunden für einen Ressourceneintrag an. Andere DNS-Server verwenden diese Zeitspanne, um zu bestimmen, wie lange ein Datensatz zwischengespeichert werden soll.
- Preference** → Gibt eine Priorität von 0 bis 65535 für diesen MX-Ressourceneintrag an. Ein Dienst versucht, Mail-Server in der bevorzugten Reihenfolge vom niedrigsten Prioritätswert zum höchsten Prioritätswert zu kontaktieren.
- MailExchange** → Gibt einen FQDN für einen Mail-Exchanger an

„NS“:

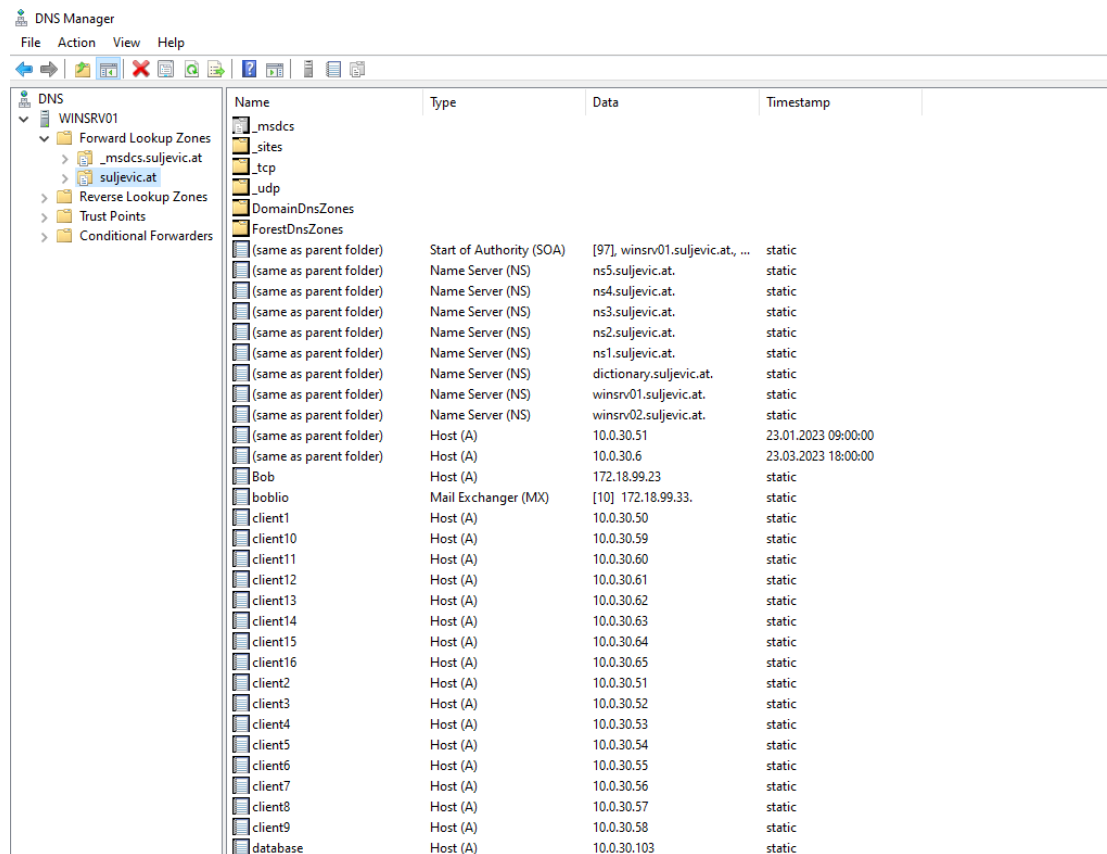
Da es keinen **Add-DnsServerResourceRecordNS** gibt muss man stattdessen **Add-DnsServerResourceRecordA** und **Add-DnsServerResourceRecord** nutzen

```
Add-DnsServerResourceRecordA -IPv4Address $ipv4 -Name $name -ZoneName "suljevic.at";
Add-DnsServerResourceRecord -NS -ZoneName suljevic.at -Name suljevic.at -NameServer $($name + ".suljevic.at.");
```

-NameServer → Gibt den Nameserver einer Domäne an.

Ergebnis:

Das fertige Ergebnis kann man dann unter **DNS→Forward Looking Zone** → **suljevic.at/ebertz.at** sehen



Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[97]. winsrv01.suljevic.at, ...	static
(same as parent folder)	Name Server (NS)	ns5.suljevic.at.	static
(same as parent folder)	Name Server (NS)	ns4.suljevic.at.	static
(same as parent folder)	Name Server (NS)	ns3.suljevic.at.	static
(same as parent folder)	Name Server (NS)	ns2.suljevic.at.	static
(same as parent folder)	Name Server (NS)	ns1.suljevic.at.	static
(same as parent folder)	Name Server (NS)	dictionary.suljevic.at.	static
(same as parent folder)	Name Server (NS)	winsrv01.suljevic.at.	static
(same as parent folder)	Name Server (NS)	winsrv02.suljevic.at.	static
(same as parent folder)	Host (A)	10.0.30.51	23.01.2023 09:00:00
(same as parent folder)	Host (A)	10.0.30.6	23.03.2023 18:00:00
Bob	Host (A)	172.18.99.23	static
boblio	Mail Exchanger (MX)	[10] 172.18.99.33.	static
client1	Host (A)	10.0.30.50	static
client10	Host (A)	10.0.30.59	static
client11	Host (A)	10.0.30.60	static
client12	Host (A)	10.0.30.61	static
client13	Host (A)	10.0.30.62	static
client14	Host (A)	10.0.30.63	static
client15	Host (A)	10.0.30.64	static
client16	Host (A)	10.0.30.65	static
client2	Host (A)	10.0.30.51	static
client3	Host (A)	10.0.30.52	static
client4	Host (A)	10.0.30.53	static
client5	Host (A)	10.0.30.54	static
client6	Host (A)	10.0.30.55	static
client7	Host (A)	10.0.30.56	static
client8	Host (A)	10.0.30.57	static
client9	Host (A)	10.0.30.58	static
database	Host (A)	10.0.30.103	static

Abbildung 1- DNS Manager

Aufgabenstellung (Namensauflösung):

- Schreibe ein Powershell-Script, dass einen FQDN auflöst und den Ablauf der Namensauflösung beginnend bei einem DNS-Root-Server im Detail beschreibt.

Beim Beispiel wurde www.amazon.de als FQDN genutzt

Script:

```
$address = "www.amazon.de"

nslookup $address 8.8.8.8

nslookup.exe -type=NS . 8.8.8.8
nslookup.exe -type=A b.root-servers.net 8.8.8.8

#Damit man die Ip-Adresse in eine Variable speichert
$firstOutput = nslookup.exe -type=A b.root-servers.net 8.8.8.8 | Select-String
-Pattern "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}" | Select-Object -Last 1
$ip_address = $firstOutput -replace
".*?(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*", '$1'

nslookup.exe -type=NS de. $ip_address

$output = nslookup.exe -type=A c.gtld-servers.net 8.8.8.8 | Select-String -
Pattern "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}" | Select-Object -Last 1
$ip_address = $output -replace ".*?(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*",
'$1'

nslookup.exe -type=NS amazon.de. $ip

$Secondoutput = nslookup.exe -type=A ns4.p31.dynect.net 8.8.8.8 | Select-
String -Pattern "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}" | Select-Object -Last 1
$ip_address = $Secondoutput -replace
".*?(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*", '$1'

nslookup.exe -type=A www.amazon.de. $ipAddress
```

Mit dem Befehl wird die IP-Adresse, die man von `nslookup.exe -type=A c.gtld-servers.net 8.8.8.8`, in eine Variable gespeichert

```
$output = nslookup.exe -type=A c.gtld-servers.net 8.8.8.8 | Select-String -
Pattern "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}" | Select-Object -Last 1

$ip_address = $output -replace ".*?(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}).*",
'$1'
```

Ergebnis:

```

PS C:\Users\bsulj\Desktop\SYT\DNS Task> .\FQDN_Aufgabe.ps1
Server:  dns.google
Address:  8.8.8.8

Nicht autorisierende Antwort:
Name:      e15317.dsca.akamaiedge.net
Addresses: 2a02:26f0:dc:390::3bd5
           2a02:26f0:dc:386::3bd5
           23.62.221.174
Aliases:   www.amazon.de
           tp.abe2c2f23-frontier.amazon.de
           www.amazon.de.edgekey.net

Server:  dns.google
Address:  8.8.8.8

Nicht autorisierende Antwort:
(root) nameserver = a.root-servers.net
(root) nameserver = b.root-servers.net
(root) nameserver = c.root-servers.net
(root) nameserver = d.root-servers.net
(root) nameserver = e.root-servers.net
(root) nameserver = f.root-servers.net
(root) nameserver = g.root-servers.net
(root) nameserver = h.root-servers.net
(root) nameserver = i.root-servers.net
(root) nameserver = j.root-servers.net
(root) nameserver = k.root-servers.net
(root) nameserver = l.root-servers.net
(root) nameserver = m.root-servers.net
Server:  dns.google
Address:  8.8.8.8

Nicht autorisierende Antwort:
Name:      b.root-servers.net
Address:    199.9.14.201

```

Abbildung 3 - Namensauflösung von www.amazon.de

```

Nicht autorisierende Antwort:
in-addr.arpa  nameserver = a.in-addr-servers.arpa
in-addr.arpa  nameserver = b.in-addr-servers.arpa
in-addr.arpa  nameserver = c.in-addr-servers.arpa
in-addr.arpa  nameserver = d.in-addr-servers.arpa
in-addr.arpa  nameserver = e.in-addr-servers.arpa
in-addr.arpa  nameserver = f.in-addr-servers.arpa
a.in-addr-servers.arpa  internet address = 199.180.182.53
a.in-addr-servers.arpa  AAAA IPv6 address = 2620:37:e000::53
b.in-addr-servers.arpa  internet address = 199.253.183.183
b.in-addr-servers.arpa  AAAA IPv6 address = 2001:500:87::87
c.in-addr-servers.arpa  internet address = 196.216.169.10
c.in-addr-servers.arpa  AAAA IPv6 address = 2001:43f8:110::10
d.in-addr-servers.arpa  internet address = 200.10.60.53
d.in-addr-servers.arpa  AAAA IPv6 address = 2001:13c7:7010::53
e.in-addr-servers.arpa  internet address = 203.119.86.101
e.in-addr-servers.arpa  AAAA IPv6 address = 2001:dd8:6::101
f.in-addr-servers.arpa  internet address = 193.0.9.1
f.in-addr-servers.arpa  AAAA IPv6 address = 2001:67c:e0::1
Server:  Unknown
Address:  199.9.14.201

de      nameserver = a.nic.de
de      nameserver = f.nic.de
de      nameserver = l.de.net
de      nameserver = n.de.net
de      nameserver = s.de.net
de      nameserver = z.nic.de
a.nic.de      internet address = 194.0.0.53
a.nic.de      AAAA IPv6 address = 2001:678:2::53
f.nic.de      internet address = 81.91.164.5
f.nic.de      AAAA IPv6 address = 2a02:568:0:2::53
z.nic.de      internet address = 194.246.96.1
z.nic.de      AAAA IPv6 address = 2a02:568:fe02::de
l.de.net      internet address = 77.67.63.105
l.de.net      AAAA IPv6 address = 2001:668:1f:11::105
n.de.net      internet address = 194.146.107.6
n.de.net      AAAA IPv6 address = 2001:67c:1011:1::53
s.de.net      internet address = 195.243.137.26
s.de.net      AAAA IPv6 address = 2003:8:14::53

```

Abbildung 2 - Namensauflösung von www.amazon.de

```
Nicht autorisierende Antwort:
Server: UnKnown
Address: fe80::8e59:c3ff:fe35:fb01

Nicht autorisierende Antwort:
amazon.de      nameserver = ns2.p31.dynect.net
amazon.de      nameserver = pdns6.ultradns.co.uk
amazon.de      nameserver = pdns1.ultradns.net
amazon.de      nameserver = ns1.p31.dynect.net
amazon.de      nameserver = ns4.p31.dynect.net
amazon.de      nameserver = ns3.p31.dynect.net
Nicht autorisierende Antwort:
Server: UnKnown
Address: fe80::8e59:c3ff:fe35:fb01

Nicht autorisierende Antwort:
Name:          djvbdzlobemzo.cloudfront.net
Address:       18.66.21.162
Aliases:       www.amazon.de
               tp.abe2c2f23-frontier.amazon.de

PS C:\Users\bsulj\Desktop\SYT\DNS Task> |
```

Abbildung 4 - Ergebnis der Namensauflösung

Am Ende ist die IP-Adresse von www.amazon.de zu sehen 18.66.21.162