Modul 123

Serverdienste in Betrieb nehmen

Lernziele

- Sie kennen den Ablauf einer DNS Abfrage
- Sie können einen Windows DNS Server in Betrieb nehmen
- Sie können einen Windows DNS Server testen
- Sie können die Funktionalität eines DNS Servers auf einem Windows Client testen

Konfigurationseinstellungen

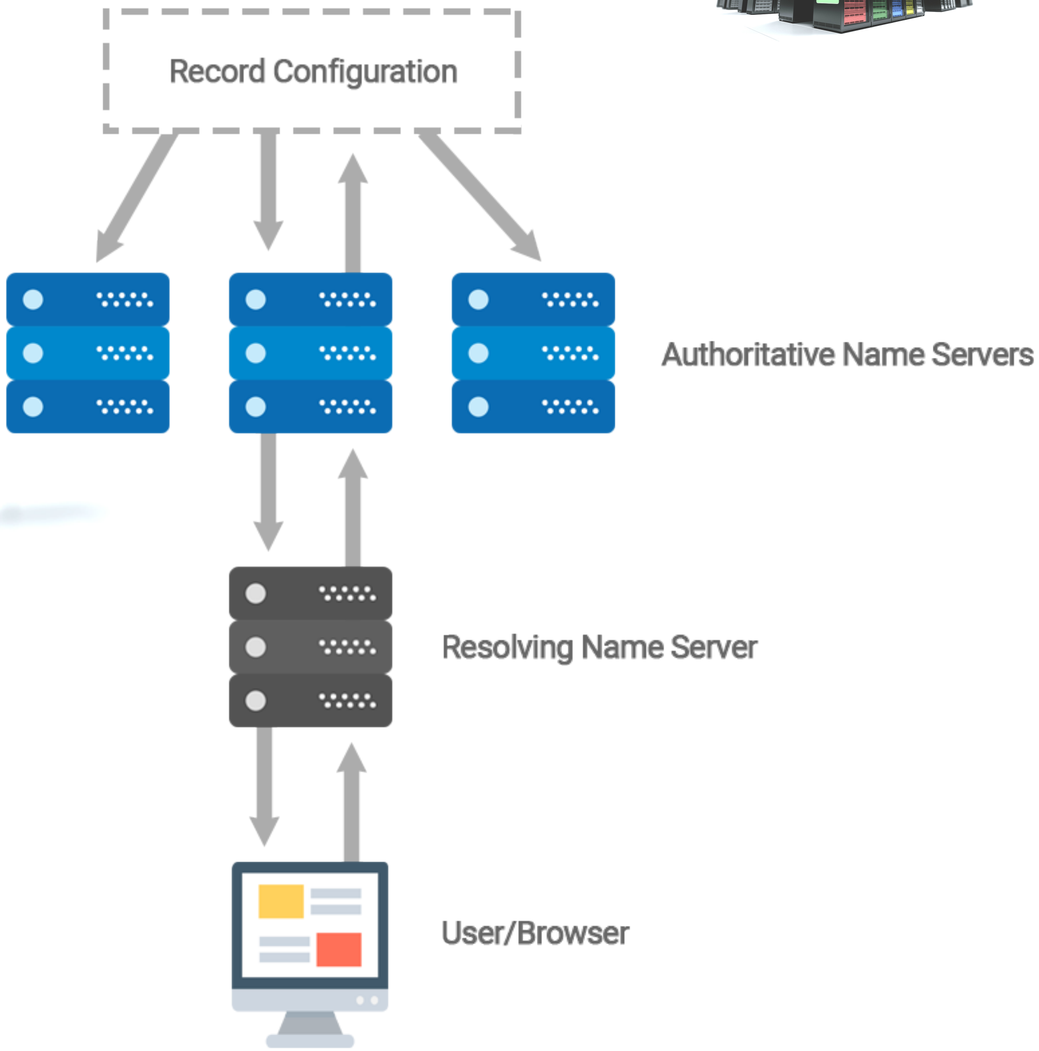
- Gateway 192.168.220.2
- Server: 192. 168.20.101
- ServerName: SRV01
- Serverlogin erfolgt via ein Password zb: Gibz1234!

- Vorbedingungen
- Ping Gateway: 192.168.220.2
- DNS Auflösung funktioniert z.B nslookup www.gibz.ch

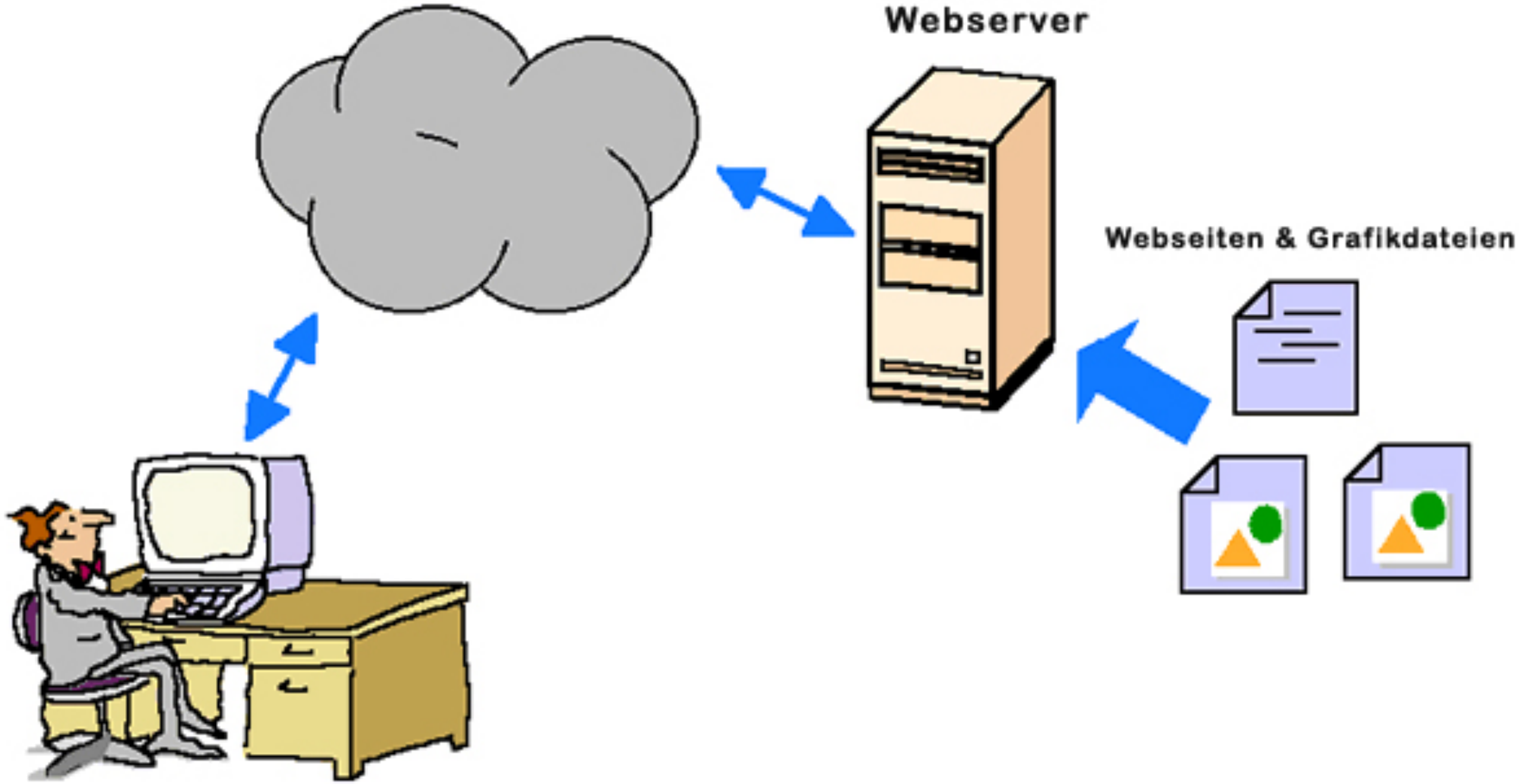
DNS


DNS

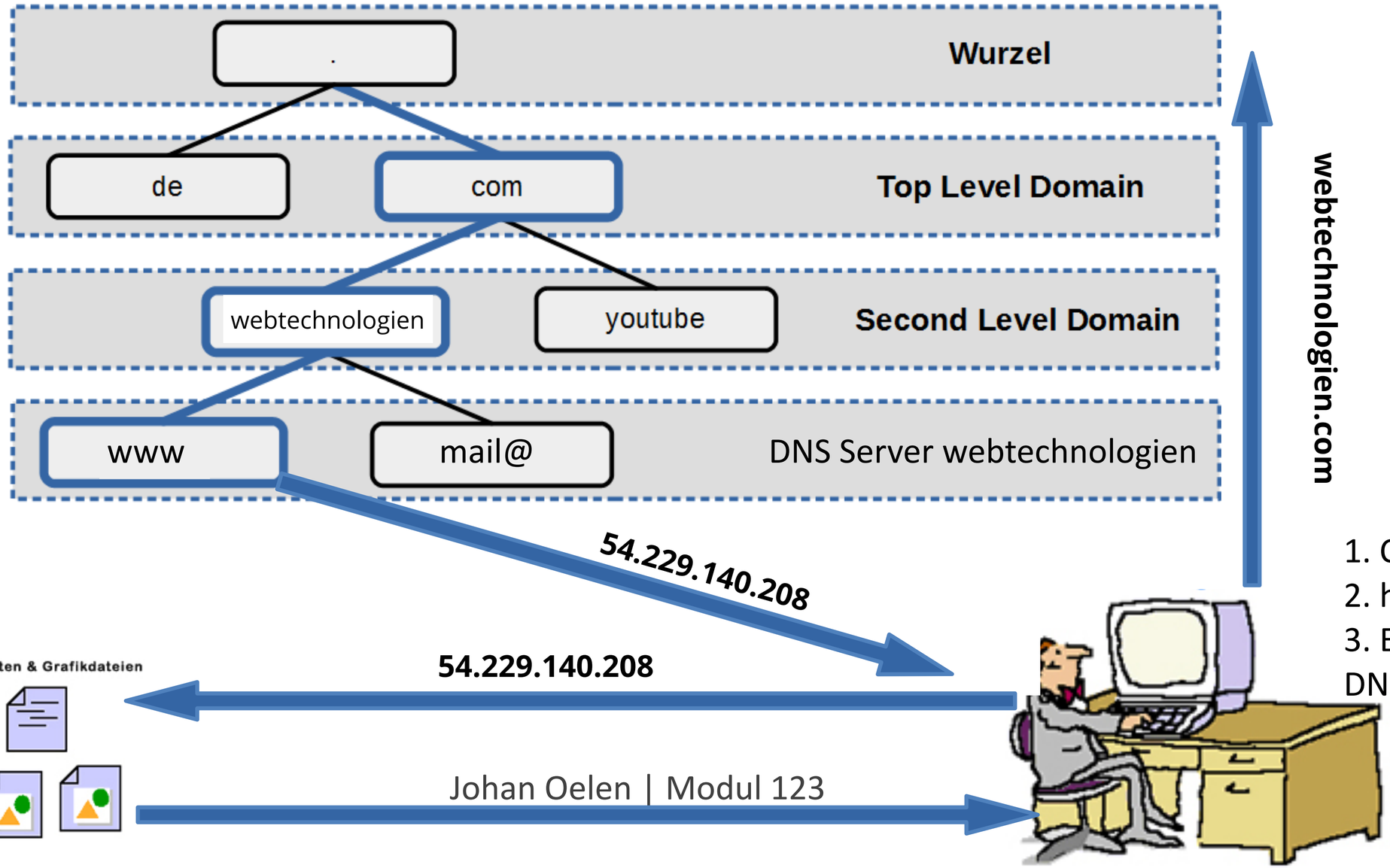

DNS


Record Configuration
Authoritative Name Servers
Resolving Name Server
User/Browser

DNS

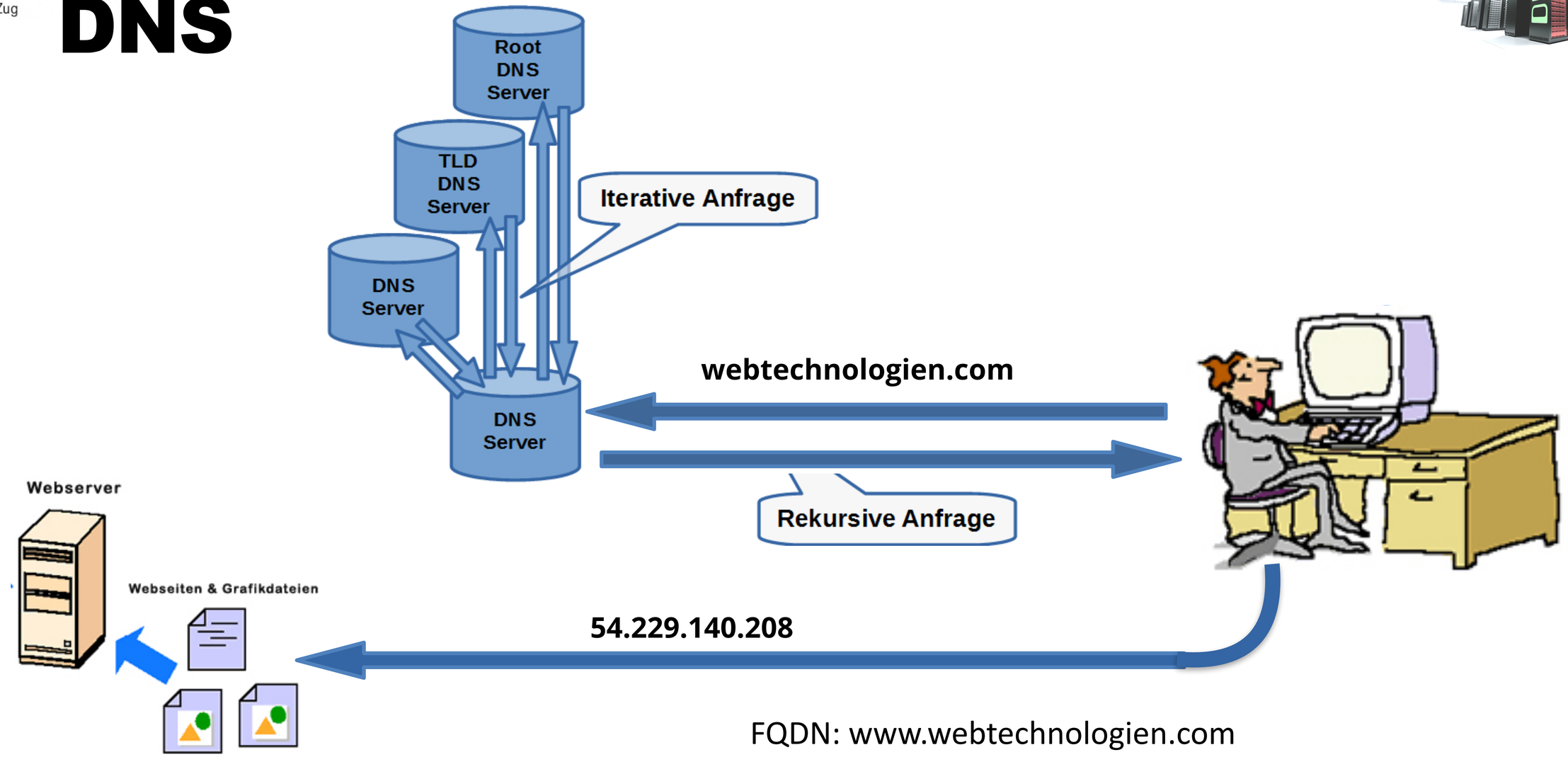


4_ Struktur von DNS



1. Cache
2. host Datei
3. Eingetragene DNS

DNS



FQDN: www.webtechnologien.com

DNS: Domain Name System_ Zusammenfassung

- DNS löst sprechende Namen (URL) in eindeutige IP-Adressen auf
- DNS ist ein Protokoll und arbeitet mit Port 53 UDP

- DNS Name: www.sbb.ch (FQDN) = Fully Qualified Domain Name

  Auflösungsprozess

  1. lokaler DNS Cache überprüft
  2. host Datei
  3. Bevorzugter DNS anfragen

  Öffentlicher Auflösungsprozess

  4. "." Root DNS Server (13 Stk)
  5. "ch" DNS Server TLD
  6. "sub" DNS Server SLD

GIBZ Gewerblich-industrielles
Bildungszentrum Zug

Kanton Zug

5_DNS Abschluss

öffentliche TLD : .ch
.de
.org

↳ Domains, welche registriert werden müssen (z.B. www.switchplus.ch

private TLD : .local
.intra
.test

⇒ interne Domains
⇒ existieren nur intern

Tools für DNS:

Whois Abfrage : wem gehört diese Domäne (z.B. switchplus.ch/whois)

DNS Abfrage : Alle Einträge einer Domain abfragen (z.B. www.ultratools.com)
DNS Lookup

4_DNS Manager

Root Hints: Root DNS Server (13 stk)

Forwarders: Weiterleitungsserver für DNS Abfragen
"wenn unser DNS die Anfrage nicht auflösen kann"

Zone = Domäne

Forward Lookup Zone = Name in IP auflösen
z.B. www.gayle.ch 217.13.14.16

Reverse Lookup Zone = IP Adresse in Namen auflösen
z.B. 13.14.100.17 mail.microsoft.com
=> SPAM Erkennung

DNS Records

Record Type	
Forwarder	
SOA	Start of Autority
A Record	ordnet einem DNS Namen eine IPv4 Adresse zu
NS Record	definiert welche Name Server für diese Zone zuständig sind
PTR	ordnet eine IP Adresse einen oder mehrere Hostnames zu
CNAME	properiert welche IP basierende Dienste in einer Domäne Angebogen werden

4_DNS Forward Lookup Zone

Wir arbeiten mit der Zone (domain) myad.local

Ressource Record = DNS Eintrag

SOA - Eintrag

Starteintrag der Domäne

Serial = ID

unterschiedliche Zeitintervalle (Refresh, TTL, ...)

NS - Eintrag

NS = Name Server

Inhaber der Zone

⇒ verantwortlich für diese Domäne

A - Eintrag

Name zu IP Auflösung

Host-Eintrag

CNAME - Eintrag

Name zu Name Auflösung

Alias Eintrag

DNS im praktischen Beispiel

Hinweis: Nach Installation wird der DNS auf localhost gesetzt (127.0.0.1) => eigene IP hinterlegen

cmd Tool: ipconfig /all

ipconfig /displaydns => lokaler Cache

ipconfig /flushdns => bereinigen DNS Cache

DNS Testen

Test	
DNS Delegation/ forwarder	nslookup tagi.ch
SOA	nslookup set q=soa ad.myad.local
A Record	nslookup set q=a desktop-01
NS Record	nslookup set q=ns tagi.ch
PTR-Record	nslookup 192.168.15.11
MX-Record	nslookup set q=mx

DNS Test Forwarder

Test: DNS Forwarder ==>1. Test mit IP V 6 aktiviert. 2. Test ohne IP V 6 Aktivierung auf dem Netzwerkadapter

Checkliste DNS Server

- Netzwerkadapter: DNS ändern von 127.0.0.1 zu 192.168.20.101 (DNS Server)
- Forwarder einrichten 8.8.8.8
- Reverse Lookup Zone einrichten
- PTR erstellen

- Server Testen
- Forwarder nslookup www.google.com
- PTR Record nslookup -q=ptr 192.168.220.10
- A Record nslookup -q=a myaddc01
- NS Record nslookup -q=ns myad.local
- SOA Record nslookup -q=soa myad.local

- Client Testen

Clientseitige Post-Installations tests

Post Installationstests auf dem Client

✓ nslookup www.google.com ==> forwarder
✓nslookup 192.168.20.126 ==> PTR-Record
✓nslookup CLwin01 ==> A-Record

Post Installationstests auf dem Server
A-Record des Clients ist eingetragen auf dem DNS Server
PTR Record des Clients ist eingetragen auf dem DNS Server

DNS Test Forwarder


```
C:\Users\Administrator>nslookup www.swiss.com
Server:  srv01.demo.local
Address:  192.168.220.20

Non-authoritative answer:
Name:    e2809.a.akamaiedge.net
Address:  2.22.152.85
Aliases:  www.swiss.com
          www.swiss.com.edgekey.net
          www.swiss.com.edgekey.net.globalredir.akadns.net
```

Falls IPV6 auf dem Netzwerkadapter aktiviert ist erscheint hier ebenfalls eine IPv6 Adresse.

DNS testen

Test: SOA_Start of Authority

```
C:\Users\Administrator>nslookup
Default Server:  srv01.demo.local
Address:  192.168.220.20

> set q=soa
> demo.local
Server:  srv01.demo.local
Address:  192.168.220.20

demo.local
        primary name server = srv01.demo.local
        responsible mail addr = hostmaster
        serial  = 6
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
srv01.demo.local        internet address = 192.168.220.20
```

Test: NS Record wird mit dem FQDN getestet

```
C:\Users\Administrator>nslookup srv01.demo.local
Server:  srv01.demo.local
Address:  192.168.220.20

Name:    srv01.demo.local
Address:  192.168.220.20
```

DNS testen

Test: A Record.

```
C:\Users\Administrator>nslookup srv01
Server:  srv01.demo.local
Address:  192.168.220.20

Name:    srv01.demo.local
Address:  192.168.220.20
```

```
C:\Users\Administrator>nslookup
Default Server:  srv01.demo.local
Address:  192.168.220.20

> set q=a
> srv01
Server:  srv01.demo.local
Address:  192.168.220.20

Name:    srv01.demo.local
Address:  192.168.220.20
```

Jeder PC in einer Domäne erhält ein A-Record Eintrag in der DNS Server. Ein A-Record kann mit Namen des Geräts getestet werden

DNS testen

Test: A Record

```
> set q=a
> srv01
Server:  demo.local
Address:  192.168.220.20

*** demo.local can't find srv01: Non-existent domain
```

Fehlermeldung

Test: PTR Record

```
C:\Users\Administrator>nslookup 192.168.220.20
Server:  demo.local
Address:  192.168.220.20

Name:    demo.local
Address:  192.168.220.20
```

```
C:\Users\Administrator>nslookup
Default Server:  demo.local
Address:  192.168.220.20

> set q=ptr
> 192.168.220.20
Server:  demo.local
Address:  192.168.220.20

20.220.168.192.in-addr.arpa     name = demo.local
```

Clientseitige Post-Installations tests

Vorbedingungen

✓ Der DHCP Server wurde installiert und getestet.

✓Der DHCP Server wurde autorisiert

✓ Der neue DNS Server wurde auf dem DHCP eingetragen

✓Der Client ist im gleichen Netzwerk wie der Server ping 192.167.20.101 funktioniert.

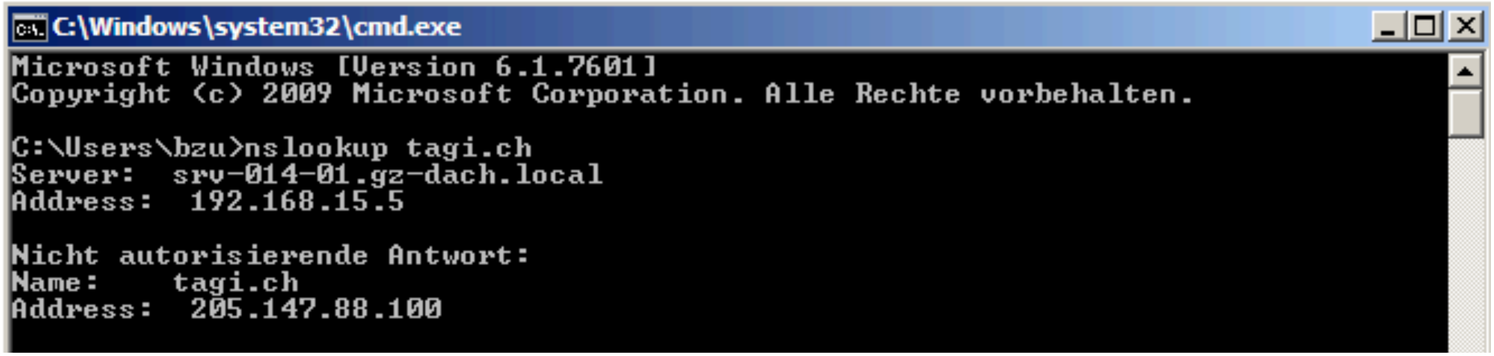
✓Der Clients ist im gleichen Netzwerk wie der Gateway ping 192.168.20.2 funktioniert

✓Gemäss ipconfig ist der DNS Server 192.168.20.101

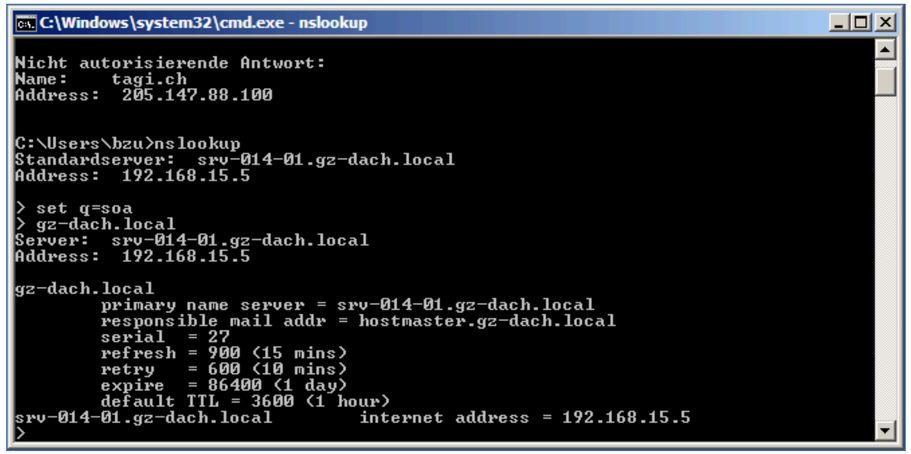
✓Der Client hat den Namen CLWin01

DNS auf dem Client testen

Test: Client- Test Forwarder



Test: Client- Test SOA



DNS test vom Client

Test: A Record

Testen Sie den A-Record des Clients.
Sollte den Client nicht mt A-Record im DNS Server erfasst sein erstellen Sie manuel ein A-Record für den Client

Test: PTR Record

Installieren Sie eine Windows DNS

1. Installieren Sie eine Windows DNS
2. Testen Sie den DNS Server
3. Konfigurieren Sie einen Windows Desktop als DNS-Client
4. Testen Sie den DNS Client
5. Testen Sie welche Client Records im DNS -Server eingetragen wurden

GIBZ Gewerblich-industrielles Bildungszentrum Zug

Kanton Zug