7.3 „Name geht nicht, IP geht“

Ist ein Ziel über seine IP-Adresse erreichbar, aber nicht über seinen Namen, liegt der Fehler wahrscheinlich im Bereich der Namensauflösung.

Beispiel:

```
ping 192.0.2.25
```

funktioniert, aber:

```
ping server01.example.local
```

scheitert.

Damit ist jedoch noch nicht automatisch bewiesen, dass ausschließlich der DNS-Server fehlerhaft ist. Auch folgende Ursachen sind möglich:

- falscher DNS-Server am Client,
- falscher oder unvollständiger Zielname,
- fehlendes DNS-Suffix,
- falscher DNS-Eintrag,
- veralteter positiver oder negativer Cacheeintrag,
- unterschiedliche Antworten mehrerer DNS-Server,
- fehlende Zonenreplikation,
- fehlerhafter Forwarder oder Conditional Forwarder,
- defekte Delegation,
- blockiertes UDP oder TCP auf Port 53,
- falsche `hosts`-Datei,
- VPN- oder NRPT-Regel,
- Split-DNS,
- DNS over HTTPS,
- nur fehlerhafter A- oder AAAA-Eintrag.

Dieser Entscheidungsbaum dient der schnellen Eingrenzung. Die ausführliche DNS-Analyse befindet sich im Netzwerk- und Verbindungsfehler-Kapitel.

---

1. Zuerst die Ausgangslage bestätigen

Zunächst prüfen, ob die Verbindung zur Ziel-IP tatsächlich funktioniert.

```
Test-NetConnection -ComputerName <ziel-ip> -InformationLevel Detailed
```

Für einen konkreten Dienst:

```
Test-NetConnection -ComputerName <ziel-ip> -Port <port>
```

Danach denselben Test mit dem Namen durchführen:

```
Test-NetConnection -ComputerName <zielname> -Port <port>
```

Bewertung

Ergebnis	Bedeutung
IP und Name funktionieren	DNS-Fehler aktuell nicht reproduzierbar
IP funktioniert, Name wird nicht aufgelöst	DNS-Pfad untersuchen
Name wird aufgelöst, aber Verbindung scheitert	Dienst, Port, Firewall, Routing oder falsche Zieladresse prüfen
IP und Name scheitern	nicht nur DNS untersuchen; Netzwerkpfad oder Zielsystem prüfen
Kurzname scheitert, FQDN funktioniert	DNS-Suffix oder Suchliste prüfen
FQDN scheitert ebenfalls	DNS-Server, Zone, Eintrag oder Weiterleitung prüfen
Name liefert falsche IP-Adresse	Record, Cache, Replikation oder Split-DNS prüfen
nur einzelne Anwendungen scheitern	Anwendungscache, Proxy, DoH oder anwendungseigene Namensauflösung prüfen

Ein erfolgreicher Ping auf die IP-Adresse bestätigt nicht, dass der benötigte Dienst erreichbar ist. Deshalb sollte nach Möglichkeit derselbe Zielport einmal über die IP-Adresse und einmal über den Namen getestet werden.

---

2. Schneller Hauptentscheidungsbaum

```
START: Name geht nicht, IP geht
|
+-- Ist die Ziel-IP über den benötigten Port erreichbar?
|   |
|   +-- Nein -> Dienst, Firewall, Routing oder Zielsystem prüfen
|   |
```

```
|   +-- Ja
|
+-- Wurde der richtige Zielname verwendet?
|   |
|   +-- Unklar -> Schreibweise, Domäne und erwarteten FQDN prüfen
|   |
|   +-- Ja
|
+-- Funktioniert der vollständige FQDN?
|   |
|   +-- Ja, aber Kurzname nicht
|   |         -> DNS-Suffix und Suchliste prüfen
|   |
|   +-- Nein
|
+-- Sind die vorgesehenen DNS-Server eingetragen und erreichbar?
|   |
|   +-- Nein -> DHCP, Adapter, VPN, Routing oder Firewall prüfen
|   |
|   +-- Ja
|
+-- Antworten alle eingetragenen DNS-Server gleich?
|   |
|   +-- Nein -> Zone, Record, Replikation oder Serverzustand prüfen
|   |
|   +-- Ja
|
+-- Liefert die Abfrage einen passenden A- oder AAAA-Eintrag?
|   |
|   +-- Nein -> Zone, Record, Forwarder oder Delegation prüfen
|   |
|   +-- Ja
|
+-- Ist die zurückgegebene IP-Adresse korrekt und erreichbar?
|   |
|   +-- Nein -> falschen oder veralteten Record beziehungsweise Cache prüfen
|   |
|   +-- Ja
|
```

```
+-- Funktioniert die Anwendung trotzdem nicht?
   |
   +-- Ja  -> Anwendungscache, Proxy, TLS, VPN, NRPT,
   |          DoH oder Hosts-Datei prüfen
   |
   +-- Nein -> DNS-Auflösung funktioniert
```

---

3. Den verwendeten Namen genau dokumentieren

Vor weiteren Tests erfassen:

- eingegebener Zielname,
- erwarteter vollständiger DNS-Name,
- Groß- und Kleinschreibung bei nachgelagerten Anwendungen,
- verwendete Anwendung,
- genaue Fehlermeldung,
- Zeitpunkt der Abfrage,
- erwartete IP-Adresse,
- tatsächlich gelieferte IP-Adresse,
- interne oder externe Domäne,
- Verbindung mit oder ohne VPN.

Beispiele:

```
server01
server01.example.local
portal.example.com
files.example.local
```

Ein Kurzname wie `server01` ist nicht dasselbe wie der vollständige Name:

```
server01.example.local
```

Der Kurzname kann nur funktionieren, wenn der Client ihn mithilfe eines DNS-Suffixes zu einem vollständigen Namen ergänzt oder ein anderes vorgesehenes Namensauflösungsverfahren verwendet.

---

4. DNS-Konfiguration des Clients prüfen

Vollständige Netzwerkkonfiguration anzeigen:

```
ipconfig /all
```

Gezielt die konfigurierten DNS-Server anzeigen:

```
Get-DnsClientServerAddress
```

Nur IPv4-DNS-Server:

```
Get-DnsClientServerAddress -AddressFamily IPv4
```

DNS-Clientkonfiguration der Adapter anzeigen:

```
Get-DnsClient
```

Globale DNS-Einstellungen und Suffixsuchliste anzeigen:

```
Get-DnsClientGlobalSetting
```

Zu prüfen sind:

- welcher Adapter aktiv verwendet wird,
- welche DNS-Server am aktiven Adapter eingetragen sind,
- ob die DNS-Server per DHCP oder statisch gesetzt wurden,
- ob ein VPN-Adapter eigene DNS-Server einträgt,
- ob virtuelle Adapter beteiligt sind,
- ob öffentliche DNS-Server an einem Domänenclient eingetragen sind,
- ob IPv4 und IPv6 unterschiedliche DNS-Server verwenden,
- ob ein verbindungsspezifisches DNS-Suffix vorhanden ist,
- ob die DNS-Suffixsuchliste korrekt ist.

Typische Fehlerbilder

Beobachtung	Mögliche Ursache
DNS-Serverfeld ist leer	fehlerhafte DHCP-Option oder statische Konfiguration
falscher interner DNS-Server	DHCP-, Adapter- oder VPN-Konfiguration
öffentlicher DNS-Server am Domänenclient	interne Namen können nicht aufgelöst werden
alter DNS-Server eingetragen	veraltete statische Konfiguration
VPN-DNS nur bei bestehender Verbindung erreichbar	VPN-Verbindung oder Routing fehlt

Beobachtung	Mögliche Ursache
mehrere Adapter besitzen unterschiedliche DNS-Server	falscher Adapter oder unerwarteter DNS-Pfad
IPv6-DNS verweist auf einen anderen Server	unterschiedliche Antwortwege möglich
nur ein Client betroffen	lokale Konfiguration, Cache, `hosts`, VPN oder Richtlinie prüfen
mehrere Clients betroffen	DHCP-Option, DNS-Dienst, Zone, Replikation oder Netzwerkpfad prüfen

Die DNS-Server eines Unternehmensclients dürfen nicht versuchsweise durch öffentliche DNS-Server ersetzt werden. Dadurch können interne Namen, Active Directory und unternehmensinterne Dienste zusätzlich gestört werden.

---

5. DNS-Server auf Erreichbarkeit prüfen

Zuerst die IP-Erreichbarkeit des vorgesehenen DNS-Servers prüfen:

```
ping <dns-server-ip>
```

Ein fehlgeschlagener Ping beweist keinen Ausfall, da ICMP blockiert sein kann.

TCP-Port 53 prüfen:

```
Test-NetConnection -ComputerName <dns-server-ip> -Port 53
```

Wichtig

Dieser Befehl testet nur TCP-Port 53. Klassische DNS-Abfragen verwenden häufig zunächst UDP-Port 53. Größere Antworten, Zonentransfers und bestimmte weitere Fälle können TCP verwenden.

Ein erfolgreicher TCP-Test bestätigt deshalb nicht vollständig:

- dass UDP 53 funktioniert,
- dass der DNS-Dienst korrekte Antworten liefert,
- dass die richtige Zone vorhanden ist,
- dass der gewünschte Record existiert.

Die eigentliche DNS-Funktion muss mit einer DNS-Abfrage geprüft werden.

---

6. Den Namen gezielt abfragen

Standardabfrage mit dem aktuell verwendeten DNS-Pfad:

```
Resolve-DnsName <zielname>
```

Beispiel:

```
Resolve-DnsName server01.example.local
```

Gezielt einen bestimmten DNS-Server abfragen:

```
Resolve-DnsName <zielname> -Server <dns-server-ip>
```

Alternativ:

```
nslookup <zielname>
```

Bestimmten DNS-Server abfragen:

```
nslookup <zielname> <dns-server-ip>
```

Zu dokumentieren sind:

- abgefragter Name,
- verwendeter DNS-Server,
- Rückgabecode,
- zurückgegebene IP-Adresse,
- Record-Typ,
- autoritative oder nicht autoritative Antwort,
- TTL,
- Unterschiede zwischen mehreren DNS-Servern.

`nslookup` und `Resolve-DnsName` sind wichtige Diagnosetests. Sie bilden jedoch nicht in jedem Fall exakt denselben Auflösungsweg ab, den eine konkrete Anwendung verwendet. Anwendungen können beispielsweise eigene Caches, Browser-DoH, Proxyauflösung oder andere Bibliotheken benutzen.

---

7. Jeden konfigurierten DNS-Server einzeln testen

Sind mehrere DNS-Server eingetragen, muss jeder einzeln abgefragt werden.

Beispiel:

```
Resolve-DnsName server01.example.local -Server 192.0.2.10
```

```
Resolve-DnsName server01.example.local -Server 192.0.2.11
```

Bewertung

DNS-Server 1	DNS-Server 2	Mögliche Ursache
richtige Antwort	richtige Antwort	Serverantworten sind konsistent
richtige Antwort	keine Antwort	zweiter Server, Dienst oder Netzwerkpfad gestört
richtige Antwort	falsche IP	Replikations-, Zonen- oder Recordproblem
Record vorhanden	`NXDOMAIN`	Zone oder Record fehlt auf einem Server
beide keine Antwort	gemeinsame Erreichbarkeit, Firewall oder Dienst prüfen	
beide `NXDOMAIN`	Name, Zone, Delegation oder Forwarder prüfen	
unterschiedliche TTL	kann durch unterschiedliche Cachezustände entstehen	
unterschiedliche Record-Sätze	Replikation, Split-DNS oder Lastverteilung prüfen	

Wenn nur einer von mehreren DNS-Servern fehlerhaft antwortet, kann das Problem scheinbar zufällig auftreten. Abhängig vom verwendeten Server funktioniert die Namensauflösung dann zeitweise oder nur auf bestimmten Clients.

---

8. FQDN und Kurzname vergleichen

Vollständigen Namen testen:

```
Resolve-DnsName server01.example.local
```

Kurznamen testen:

```
Resolve-DnsName server01
```

Entscheidung

```
Funktioniert der FQDN?
|
+-- Nein
|   -> DNS-Server, Zone, Record, Weiterleitung oder Delegation prüfen
|
+-- Ja
    |
    +-- Funktioniert auch der Kurzname?
        |
        +-- Ja  -> Suffixauflösung funktioniert
        |
        +-- Nein
            -> DNS-Suffix und Suchliste prüfen
```

DNS-Clientinformationen anzeigen:

```
Get-DnsClient
```

Globale Suffixsuchliste anzeigen:

```
Get-DnsClientGlobalSetting
```

In `ipconfig /all` insbesondere prüfen:

```
Primäres DNS-Suffix
Verbindungsspezifisches DNS-Suffix
DNS-Suffixsuchliste
```

Mögliche Ursachen bei „FQDN geht, Kurzname geht nicht“

- kein DNS-Suffix vorhanden,
- falsches verbindungsspezifisches Suffix,
- falsche globale Suchliste,
- VPN ändert die Suffixsuchliste,
- DHCP-Option liefert ein falsches Suffix,
- Gruppenrichtlinie setzt eine falsche Suchliste,
- Anwendung ergänzt keinen DNS-Suffix,
- Kurzname ist mehrdeutig.

Für Diagnose und Dokumentation ist der FQDN grundsätzlich aussagekräftiger als ein Kurzname.

9. A- und AAAA-Einträge getrennt prüfen

IPv4-Eintrag abfragen:

```
Resolve-DnsName <zielname> -Type A
```

IPv6-Eintrag abfragen:

```
Resolve-DnsName <zielname> -Type AAAA
```

Mit `nslookup`:

```
nslookup -type=A <zielname>
```

```
nslookup -type=AAAA <zielname>
```

Bewertung

Ergebnis	Mögliche Ursache
richtiger A-Eintrag, kein AAAA-Eintrag	nur IPv4 vorgesehen; nicht automatisch ein Fehler
richtiger AAAA-Eintrag, kein A-Eintrag	nur IPv6 vorgesehen; Umgebung prüfen
A-Eintrag zeigt auf alte IP	veralteter Record oder Cache
AAAA-Eintrag zeigt auf nicht erreichbares Ziel	veralteter IPv6-Record oder fehlerhafter IPv6-Pfad
mehrere A- oder AAAA-Einträge	Lastverteilung oder mehrere Zielsysteme möglich
nur eine der gelieferten Adressen funktioniert	einzelnen Record und Zielpfad prüfen
CNAME verweist auf nicht auflösbaren Namen	Ziel des CNAME prüfen
`NXDOMAIN`	Name oder Zone existiert laut befragtem Server nicht
`SERVFAIL`	Server konnte die Anfrage nicht korrekt verarbeiten

Wenn ein Name mehrere Adressen liefert, müssen alle zurückgegebenen Ziele berücksichtigt werden. Ein einzelner funktionierender Record beweist nicht, dass jeder mögliche Verbindungsversuch erfolgreich ist.

---

10. Zurückgegebene IP-Adresse überprüfen

Nach erfolgreicher Auflösung prüfen, ob die Antwort dem erwarteten Ziel entspricht.

```
Resolve-DnsName <zielname>
```

Danach den benötigten Port an der gelieferten Adresse testen:

```
Test-NetConnection -ComputerName <zurückgegebene-ip> -Port <port>
```

Zu klären sind:

- gehört die IP-Adresse zum vorgesehenen Server,
- ist die Adresse noch aktuell,
- existieren mehrere A- oder AAAA-Einträge,
- verweist ein CNAME auf das richtige Ziel,
- stammt die Antwort aus einer internen oder externen Zone,
- liefert das VPN eine andere Antwort,
- verwendet der Client möglicherweise einen alten Cacheeintrag?

Wichtig

„Der Name wird aufgelöst“ bedeutet nur, dass eine DNS-Antwort vorliegt. Die Antwort kann trotzdem falsch, veraltet oder für den aktuellen Netzwerkstandort ungeeignet sein.

---

11. DNS-Clientcache untersuchen

Cacheeinträge anzeigen:

```
ipconfig /displaydns
```

Alternativ:

```
Get-DnsClientCache
```

Gezielt nach einem Namen suchen:

```
Get-DnsClientCache | Where-Object Entry -Like "*<zielname>*"
```

Zu prüfen sind:

- gespeicherter Name,
- Record-Typ,
- gespeicherte Adresse,

- verbleibende TTL,
- negativer Cacheeintrag,
- Unterschied zur direkten Abfrage des DNS-Servers.

Vergleich

```
Resolve-DnsName <zielname>
```

und anschließend gezielt:

```
Resolve-DnsName <zielname> -Server <dns-server-ip>
```

Unterscheiden sich Cache und direkte Serverantwort, kann ein veralteter Cacheeintrag vorliegen.

Cache erst nach der Dokumentation leeren:

```
Clear-DnsClientCache
```

Alternativ:

```
ipconfig /flushdns
```

Danach denselben Test erneut durchführen:

```
Resolve-DnsName <zielname>
```

Negativer Cache

Auch eine zuvor fehlgeschlagene Namensauflösung kann zwischengespeichert werden. Wurde der DNS-Eintrag erst danach angelegt, kann der Client bis zum Ablauf des negativen Cacheeintrags weiterhin melden, dass der Name nicht existiert.

Das Leeren des Caches ist nur dann ein aussagekräftiger Test, wenn vorher und nachher dieselbe Abfrage dokumentiert wird.

---

12. `hosts`-Datei prüfen

Unter Windows befindet sich die Datei hier:

```
C:\Windows\System32\drivers\etc\hosts
```

Inhalt mit PowerShell anzeigen:

```
Get-Content "$env:SystemRoot\System32\drivers\etc\hosts"
```

Relevante aktive Zeilen anzeigen:

```
Get-Content "$env:SystemRoot\System32\drivers\etc\hosts" |
    Where-Object { $_ -notmatch '^\s*#' -and $_ -notmatch '^\s*$' }
```

Mögliche Fehler:

- Name verweist auf eine alte IP-Adresse,
- Tippfehler im Hostnamen,
- Testeintrag wurde nicht entfernt,
- Sicherheitssoftware hat einen Eintrag ergänzt,
- Anwendung erreicht dadurch ein anderes Ziel,
- ein lokaler Eintrag verdeckt die erwartete DNS-Antwort.

Beispiel eines problematischen Eintrags:

```
192.0.2.40 server01.example.local
```

Wenn der Server inzwischen die Adresse `192.0.2.50` verwendet, kann der Client trotz korrektem DNS-Eintrag weiterhin das alte Ziel verwenden.

Ein Eintrag darf erst nach Sicherung und Freigabe kontrolliert geändert oder entfernt werden. Nicht jede Anwendung verwendet zwingend den identischen Windows-Auflösungsweg.

---

13. Zone und Resource Record auf dem DNS-Server prüfen

Auf einem autorisierten Windows-DNS-Server können die vorhandenen Zonen angezeigt werden:

```
Get-DnsServerZone
```

Bestimmte Zone prüfen:

```
Get-DnsServerZone -Name "<zone>"
```

Resource Record suchen:

```
Get-DnsServerResourceRecord -ZoneName "<zone>" -Name "<hostname>"
```

A- und AAAA-Records der Zone anzeigen:

```
Get-DnsServerResourceRecord -ZoneName "<zone>" -RRType A
```

```
Get-DnsServerResourceRecord -ZoneName "<zone>" -RRType AAAA
```

Zu prüfen sind:

- existiert die richtige Zone,
- ist die Zone geladen,
- ist der Record vorhanden,
- stimmt der Record-Typ,
- stimmt die gespeicherte IP-Adresse,
- existiert ein alter zusätzlicher Record,
- verweist ein CNAME auf einen gültigen Zielnamen,
- ist der Record statisch oder dynamisch registriert,
- stimmt der Zeitstempel,
- ist die TTL plausibel,
- befindet sich der Record auf allen zuständigen DNS-Servern,
- wird möglicherweise eine gleichnamige, aber falsche Zone verwendet?

Beispiel

Der Client fragt ab:

```
server01.example.local
```

Dafür müssen mindestens folgende Bestandteile stimmen:

```
Zone: example.local
Name: server01
Typ: A oder AAAA
Wert: vorgesehene IP-Adresse
```

Ein korrekt aussehender Record auf einem DNS-Server genügt nicht, wenn Clients auch andere DNS-Server verwenden.

---

14. TTL und veraltete Antworten berücksichtigen

Die TTL bestimmt, wie lange ein Resolver einen DNS-Record zwischenspeichern darf.

TTL mit PowerShell prüfen:

```
Resolve-DnsName <zielname>
```

Ausführlich mit `nslookup`:

```
nslookup -debug <zielname>
```

Mögliche Situation:

1. ein Record zeigte auf eine alte IP-Adresse,
2. der Record wurde auf dem DNS-Server korrigiert,
3. ein Client oder zwischengeschalteter Resolver besitzt noch die alte Antwort,
4. der Client verwendet diese bis zum Ablauf der TTL weiter.

Zu berücksichtigen sind:

- lokaler Clientcache,
- Cache des DNS-Servers,
- Forwarder-Cache,
- Anwendungscache,
- Browsercache,
- Proxy- oder Sicherheitsgateway,
- negative Cacheeinträge.

Eine kurze TTL löst keine falsche Zonen- oder Replikationskonfiguration. Eine lange TTL ist ebenfalls nicht automatisch fehlerhaft, verlängert aber die mögliche Nutzungsdauer eines veralteten Cacheeintrags.

---

15. Zonenreplikation prüfen

Bei Active-Directory-integrierten Zonen prüfen:

- Replikationsbereich der Zone,
- Zustand der Active-Directory-Replikation,
- Vorhandensein des Records auf allen zuständigen DNS-Servern,
- Zeitpunkt der letzten Änderung,
- Erreichbarkeit der Replikationspartner,
- Ereignisprotokolle von DNS und Active Directory.

Zone auf mehreren Servern gezielt vergleichen:

```
Get-DnsServerResourceRecord `
   -ComputerName <dns-server-1> `
   -ZoneName "<zone>" `
   -Name "<hostname>"
```

```
Get-DnsServerResourceRecord `
   -ComputerName <dns-server-2> `
   -ZoneName "<zone>" `
   -Name "<hostname>"
```

Hinweise auf ein Replikationsproblem

- ein DNS-Server liefert die neue IP-Adresse,
- ein anderer DNS-Server liefert die alte IP-Adresse,
- ein Server besitzt den Record, ein anderer meldet `NXDOMAIN`,
- Fehler tritt nur an einem Standort auf,
- Fehler tritt abhängig vom verwendeten DNS-Server auf,
- eine kürzlich angelegte Zone oder ein Record fehlt auf einzelnen Servern.

Die Zone oder der Record sollte nicht einfach auf jedem Server manuell nachgebaut werden. Zuerst muss geklärt werden, warum die vorgesehene Replikation nicht funktioniert.

---

16. Forwarder und Conditional Forwarder prüfen

Forwarder auf einem Windows-DNS-Server anzeigen:

```
Get-DnsServerForwarder
```

Conditional Forwarder anzeigen:

```
Get-DnsServerZone |
   Where-Object ZoneType -EQ "Forwarder"
```

Details einer Weiterleitungszone prüfen:

```
Get-DnsServerConditionalForwarderZone -Name "<zone>"
```

Zu prüfen sind:

- wird die betroffene Domäne lokal autoritativ beantwortet,
- existiert ein Conditional Forwarder für die Domäne,
- zeigen dessen Zieladressen auf die richtigen DNS-Server,
- sind diese Server erreichbar,
- antworten sie auf die betreffende Anfrage,
- funktioniert UDP und TCP 53,
- besteht der erforderliche VPN- oder Standortpfad,
- ist die Weiterleitungszone korrekt repliziert,
- greift unbeabsichtigt eine lokale Zone statt des Forwarders?

Gezielte Prüfung des Zielservers:

```
Resolve-DnsName <zielname> -Server <forwarder-ip>
```

Entscheidung

```
Betrifft der Fehler nur Namen einer bestimmten Domäne?
|
+-- Nein
|   -> allgemeinen DNS-Dienst und Clientpfad prüfen
|
+-- Ja
    |
    +-- Ist der lokale DNS-Server für die Zone autoritativ?
        |
        +-- Ja  -> Zone, Record und Replikation prüfen
        |
        +-- Nein
            |
            +-- Existiert ein Conditional Forwarder oder eine Delegation?
                |
                +-- Nein -> vorgesehene Namensarchitektur prüfen
                |
                +-- Ja  -> Zielserver, Erreichbarkeit und Antwort prüfen
```

---

17. Delegation prüfen

Bei einer delegierten untergeordneten Zone müssen die übergeordnete Zone und die zuständigen Nameserver korrekt auf die untergeordnete Zone verweisen.

Nameserver abfragen:

```
Resolve-DnsName <untergeordnete-zone> -Type NS
```

SOA-Eintrag prüfen:

```
Resolve-DnsName <untergeordnete-zone> -Type SOA
```

Zu prüfen sind:

- existiert die Delegation in der übergeordneten Zone,
- sind die richtigen NS-Records eingetragen,
- lassen sich die Nameservernamen auflösen,
- stimmen benötigte Glue Records,
- sind die delegierten DNS-Server erreichbar,
- hosten diese Server die untergeordnete Zone,
- liefern sie den erwarteten Record?

Typisches Fehlerbild

```
host.abteilung.example.local
```

Die Zone:

```
abteilung.example.local
```

wurde auf separate DNS-Server delegiert. Die übergeordnete Zone kennt jedoch einen alten Nameserver. Dadurch funktioniert die übrige Domäne, während nur Namen unterhalb der delegierten Zone scheitern.

---

18. UDP und TCP auf Port 53 unterscheiden

DNS verwendet sowohl UDP als auch TCP.

Typische Gründe für TCP-Nutzung:

- Antwort ist für UDP zu groß,
- DNSSEC vergrößert die Antwort,
- Zonentransfer,
- Server fordert Wiederholung über TCP,
- bestimmte Netzwerk- oder Serverkonfigurationen.

Nur TCP testen:

```
Test-NetConnection -ComputerName <dns-server-ip> -Port 53
```

Eine tatsächliche DNS-Abfrage ausführen:

```
Resolve-DnsName <zielname> -Server <dns-server-ip>
```

Abfrage ausdrücklich über TCP erzwingen:

```
Resolve-DnsName <zielname> -Server <dns-server-ip> -TcpOnly
```

Bewertung

Normale Abfrage	Abfrage mit `-TcpOnly`	Mögliche Eingrenzung
funktioniert	funktioniert	UDP und TCP wahrscheinlich nutzbar
scheitert	funktioniert	UDP 53 oder UDP-Antwortpfad untersuchen
funktioniert	scheitert	TCP 53 untersuchen
beide scheitern	DNS-Dienst, Erreichbarkeit, Firewall oder Name prüfen	
kleine Antworten funktionieren, große nicht	Fragmentierung, MTU, EDNS oder TCP-Fallback prüfen	

Firewallregeln dürfen nicht pauschal deaktiviert werden. Stattdessen sind erlaubte und blockierte DNS-Verbindungen gezielt anhand von Quelle, Ziel, Protokoll und Port zu prüfen.

---

19. Split-DNS berücksichtigen

Bei Split-DNS liefert derselbe Name abhängig vom verwendeten DNS-System unterschiedliche Antworten.

Beispiel:

```
portal.example.com
```

Intern:

```
10.10.20.25
```

Extern:

```
198.51.100.25
```

Vergleichsabfragen:

```
Resolve-DnsName portal.example.com -Server <interner-dns-server>
```

```
Resolve-DnsName portal.example.com -Server <vorgesehener-externer-dns-server>
```

Zu prüfen sind:

- ist der Client intern oder extern,
- besteht eine VPN-Verbindung,
- verwendet der Client den internen DNS-Server,
- existiert eine interne Zone mit demselben Namen,
- enthält die interne Zone den benötigten Record,
- liefert ein öffentlicher Resolver absichtlich eine andere Adresse,
- ist die interne Zieladresse vom aktuellen Standort erreichbar?

Typisches Fehlerbild

Die interne Zone `example.com` existiert, enthält aber keinen Record für `portal`. Der interne DNS-Server fragt deshalb möglicherweise nicht extern weiter, sondern beantwortet die Anfrage aus seiner eigenen autoritativen Zone mit einem negativen Ergebnis.

---

20. VPN, NRPT und DNS-Routing prüfen

VPN-Clients können abhängig von ihrer Konfiguration:

- eigene DNS-Server erhalten,
- nur bestimmte DNS-Domänen über das VPN auflösen,
- eine DNS-Suffixsuchliste erhalten,
- Split-Tunneling verwenden,
- die Name Resolution Policy Table verwenden,
- interne und externe Anfragen unterschiedlich behandeln.

DNS-Konfiguration vor und nach der VPN-Verbindung vergleichen:

```
Get-DnsClientServerAddress
```

```
Get-DnsClientGlobalSetting
```

NRPT-Regeln anzeigen:

```
Get-DnsClientNrptPolicy
```

Zusätzlich, abhängig von der Windows-Version:

```
Get-DnsClientNrptRule
```

Zu prüfen sind:

- tritt der Fehler nur mit VPN auf,
- tritt der Fehler nur ohne VPN auf,
- ist der interne DNS-Server über den Tunnel erreichbar,
- wird das interne Präfix über das VPN geroutet,
- greift die vorgesehene NRPT-Regel,
- verwendet die betroffene Domäne den richtigen DNS-Server,
- überschreibt der VPN-Client die Suffixsuchliste,
- besteht eine Überschneidung interner und lokaler Netze?

Vergleich

Zustand	Ergebnis	Eingrenzung
ohne VPN fehlerhaft, mit VPN erfolgreich	interner DNS nur über VPN vorgesehen	
ohne VPN erfolgreich, mit VPN fehlerhaft	VPN-DNS, NRPT oder Tunnelrouting prüfen	
nur interne Namen fehlerhaft	internen DNS-Pfad und Suffix prüfen	
interne und externe Namen fehlerhaft	VPN-DNS-Konfiguration oder allgemeine Erreichbarkeit prüfen	
FQDN funktioniert, Kurzname nicht	Suffixänderung durch VPN prüfen	

---

21. DNS over HTTPS berücksichtigen

Bei DNS over HTTPS, kurz DoH, werden DNS-Abfragen verschlüsselt über HTTPS übertragen. Dadurch kann eine Anwendung oder der Windows-DNS-Client einen anderen DNS-Pfad verwenden als bei klassischem DNS über Port 53.

Windows-Konfiguration unterstützter DoH-Server anzeigen:

```
Get-DnsClientDohServerAddress
```

Zu prüfen sind:

- ist DoH auf dem Client aktiviert,
- welcher DoH-Server wird verwendet,
- verwendet der Browser einen eigenen sicheren DNS-Dienst,
- umgeht die Anwendung den internen DNS-Server,
- kann der DoH-Server interne Namen überhaupt auflösen,
- blockiert eine Unternehmensrichtlinie nicht vorgesehene DoH-Verbindungen,
- funktioniert die Namensauflösung im Betriebssystem, aber nicht im Browser,
- funktioniert sie im Browser, aber nicht in anderen Anwendungen?

Typische Hinweise

Beobachtung	Mögliche Ursache
`Resolve-DnsName` funktioniert, Browser nicht	Browsercache, Browser-DoH, Proxy oder Anwendung prüfen
Browser funktioniert, andere Anwendungen nicht	Browser verwendet möglicherweise eigenen Resolver oder DoH
interne Namen nur im Browser fehlerhaft	Browser-DoH umgeht möglicherweise internen DNS
klassischer DNS-Port 53 blockiert, DoH funktioniert	unterschiedliche DNS-Pfade
Fehler nur nach Aktivierung von sicherem DNS	DoH-Konfiguration oder verwendeten Resolver prüfen

DoH sollte nicht ungeprüft deaktiviert oder umkonfiguriert werden. Zuerst ist festzustellen, welcher Auflösungsweg tatsächlich vorgesehen ist.

---

22. DNS-Servercache berücksichtigen

Auch ein DNS-Server kann veraltete positive oder negative Antworten zwischenspeichern.

Cacheeinträge eines autorisierten Windows-DNS-Servers anzeigen:

```
Show-DnsServerCache
```

Gezielt sollte geprüft werden:

- enthält der Server eine alte IP-Adresse,
- wurde zuvor eine negative Antwort gespeichert,
- liefert der autoritative Server inzwischen eine andere Antwort,
- verwenden mehrere DNS-Server unterschiedliche Cachezustände,
- funktioniert eine direkte Abfrage des autoritativen Servers?

Beispiel:

```
Resolve-DnsName <zielname> -Server <lokaler-dns-server>
```

```
Resolve-DnsName <zielname> -Server <autoritativ-dns-server>
```

Der Servercache darf nicht als erste Maßnahme vollständig geleert werden. Vorher müssen betroffene Einträge, TTL, Serverantworten und Zeitpunkt dokumentiert werden.

---

23. CNAME-Ketten vollständig prüfen

CNAME-Abfrage:

```
Resolve-DnsName <zielname> -Type CNAME
```

Normale Abfrage:

```
Resolve-DnsName <zielname>
```

Beispiel:

```
portal.example.local
   CNAME -> webfarm.example.local
   A     -> 192.0.2.80
```

Zu prüfen sind:

- existiert der CNAME,
- ist dessen Zielname korrekt geschrieben,
- lässt sich der Zielname auflösen,
- verweist die Kette auf eine gültige Adresse,
- besteht eine Schleife,
- liegt das Ziel in einer anderen Zone,
- funktioniert die Weiterleitung zu dieser Zone,
- existieren widersprüchliche Records?

Ein vorhandener CNAME genügt nicht. Die gesamte Kette bis zum abschließenden A- oder AAAA-Record muss funktionieren.

---

24. DNS-Antwortcodes richtig bewerten

Antwort	Bedeutung	Nächster Schritt
`NOERROR` mit Antwort	Abfrage wurde erfolgreich beantwortet	Record und Adresse prüfen
`NOERROR` ohne gesuchten Record	Name kann existieren, aber der angefragte Typ fehlt	Record-Typ und Zonendaten prüfen
`NXDOMAIN`	der abgefragte Name existiert laut antwortendem Server nicht	Schreibweise, Zone, Record, Cache und Replikation prüfen
`SERVFAIL`	Server konnte die Anfrage nicht erfolgreich verarbeiten	DNSSEC, Weiterleitung, Delegation, Serverprotokolle oder Erreichbarkeit prüfen
`REFUSED`	Server lehnt die Anfrage ab	Richtlinie, Rekursion, ACL oder Serverrolle prüfen
Zeitüberschreitung	keine rechtzeitige Antwort	Dienst, Netzwerkpfad, Firewall, UDP/TCP oder Auslastung prüfen

Ein `NXDOMAIN` ist eine DNS-Antwort und nicht dasselbe wie eine Zeitüberschreitung. Bei `NXDOMAIN` hat ein DNS-Server geantwortet, konnte den Namen jedoch in seinem Auflösungspfad nicht als vorhanden bestätigen.

---

25. Anwendungen getrennt vom DNS-System testen

Wenn Befehlszeilentests funktionieren, die Anwendung jedoch weiterhin scheitert, prüfen:

- Anwendung vollständig neu gestartet,
- anwendungseigener DNS-Cache,
- Browsercache,
- Proxykonfiguration,
- Browser-DoH,
- fest konfigurierte Zieladresse,
- Zertifikat stimmt nicht zum Namen,
- Anwendung verwendet einen Alias oder anderen Hostnamen,
- Load-Balancer oder Reverse Proxy,
- Verbindung über IPv4 oder IPv6,
- lokale Sicherheitssoftware,
- PAC-Datei oder Webproxy,
- Container, VM oder WSL mit eigener DNS-Konfiguration.

Vergleichstests

```
Resolve-DnsName <zielname>
```

```
Test-NetConnection -ComputerName <zielname> -Port <port>
```

```
Test-NetConnection -ComputerName <aufgelöste-ip> -Port <port>
```

Wenn diese Tests erfolgreich sind, muss der konkrete Auflösungs- und Verbindungsweg der Anwendung untersucht werden.

---

26. Beispiel für eine schnelle Diagnose

Symptom

Ein Benutzer kann den internen Fileserver über seine IP-Adresse erreichen:

```
\\192.0.2.25\Freigabe
```

Der Zugriff über den Namen scheitert:

```
\\fileserver.example.local\Freigabe
```

IP-Prüfung

```
Test-NetConnection -ComputerName 192.0.2.25 -Port 445
```

Ergebnis:

```
TcpTestSucceeded : True
```

Namensprüfung

```
Resolve-DnsName fileserver.example.local
```

Ergebnis:

```
Name       : fileserver.example.local
Type       : A
IPAddress  : 192.0.2.20
```

Bewertung

- SMB-Port 445 ist an der tatsächlichen Serveradresse erreichbar.
- Der Name wird aufgelöst.
- Die gelieferte Adresse ist jedoch veraltet.
- Es liegt kein allgemeiner Netzwerkausfall vor.
- DNS-Record, Cache und Replikation müssen geprüft werden.

Vergleich der DNS-Server

```
Resolve-DnsName fileserver.example.local -Server 192.0.2.10
```

Ergebnis:

```
IPAddress : 192.0.2.25
```

```
Resolve-DnsName fileserver.example.local -Server 192.0.2.11
```

Ergebnis:

```
IPAddress : 192.0.2.20
```

Festgestellte Ursache

Der aktualisierte A-Record wurde aufgrund einer gestörten Active-Directory-Replikation noch nicht auf den zweiten DNS-Server übertragen.

Kontrollierte Maßnahme

- Replikationsfehler untersucht und behoben,
- Replikation des DNS-Records bestätigt,
- beide DNS-Server liefern anschließend dieselbe Adresse,
- alter Clientcache erst nach der Dokumentation geleert.

Nachprüfung

```
Resolve-DnsName fileserver.example.local -Server 192.0.2.10
```

```
Resolve-DnsName fileserver.example.local -Server 192.0.2.11
```

Beide Server liefern:

```
IPAddress : 192.0.2.25
```

Zusätzlich:

```
Test-NetConnection -ComputerName fileserver.example.local -Port 445
```

Ergebnis:

```
TcpTestSucceeded : True
```

Die Freigabe funktioniert anschließend wieder über den vorgesehenen Namen.

---

27. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- öffentliche DNS-Server am Unternehmensclient eintragen,
- DNS-Server wahllos austauschen,
- DNS-Cache vor der Dokumentation löschen,
- DNS-Servercache vollständig leeren,
- `hosts`-Datei ungeprüft bearbeiten,
- einen neuen DNS-Record zusätzlich anlegen, ohne vorhandene Records zu prüfen,
- mehrere widersprüchliche A-Records erstellen,
- DNS-Zone auf jedem Server manuell nachbauen,
- DNS-Dienst oder Domain Controller sofort neu starten,
- VPN-Client ungeprüft deinstallieren,
- NRPT-Regeln ungeprüft löschen,
- DoH pauschal deaktivieren,
- IPv6 vollständig deaktivieren,
- Firewall vollständig abschalten,
- TTL ohne Ursachenanalyse stark verkürzen,
- mehrere DNS-Änderungen gleichzeitig durchführen,
- ausschließlich mit `ping` testen,
- erfolgreiche IP-Erreichbarkeit mit vollständiger Anwendungsfunktion gleichsetzen.

Solche Maßnahmen können den ursprünglichen Zustand verändern, Beweise beseitigen oder zusätzliche Fehler in Active Directory, VPN und internen Anwendungen verursachen.

---

28. Vollständige Schnellprüfreihenfolge

1. genaue Fehlermeldung und Uhrzeit erfassen.
2. verwendeten Namen exakt dokumentieren.
3. erwartete Ziel-IP und Zielport feststellen.
4. Zielport über die IP-Adresse prüfen.
5. Zielport über den Namen prüfen.
6. FQDN und Kurzname getrennt testen.
7. aktive Netzwerkadapter ermitteln.
8. konfigurierte DNS-Server dokumentieren.
9. DNS-Suffix und Suchliste prüfen.
10. VPN und virtuelle Adapter berücksichtigen.
11. jeden eingetragenen DNS-Server einzeln abfragen.
12. Antworten und TTL miteinander vergleichen.
13. A- und AAAA-Records getrennt prüfen.
14. CNAME-Kette untersuchen.
15. zurückgegebene IP-Adressen einzeln testen.
16. Clientcache anzeigen und dokumentieren.
17. negative Cacheeinträge berücksichtigen.
18. `hosts`-Datei kontrollieren.
19. Zone und Resource Record auf dem DNS-Server prüfen.
20. Record auf allen zuständigen DNS-Servern vergleichen.
21. Zonen- oder AD-Replikation untersuchen.
22. Forwarder und Conditional Forwarder prüfen.
23. Delegation und Nameserver prüfen.
24. UDP und TCP 53 unterscheiden.
25. Split-DNS berücksichtigen.
26. VPN-Routing, DNS-Zuweisung und NRPT prüfen.
27. DoH und anwendungseigene Resolver berücksichtigen.
28. genau eine Hypothese formulieren.
29. genau eine kontrollierte Maßnahme durchführen.
30. dieselben Abfragen erneut ausführen.
31. jeden vorgesehenen DNS-Server erneut testen.
32. den benötigten Dienst über den Namen prüfen.
33. Vergleichsclient oder Vergleichsstandort testen.
34. temporäre Diagnoseänderungen entfernen.
35. Ursache, Maßnahme und Nachweis dokumentieren.

---

29. Checkliste „Name geht nicht, IP geht“

- [ ] genaue Fehlermeldung wurde dokumentiert.
- [ ] Zeitpunkt der fehlerhaften Abfrage ist bekannt.
- [ ] verwendeter Zielname wurde exakt übernommen.
- [ ] erwarteter FQDN ist bekannt.
- [ ] erwartete Ziel-IP ist bekannt.

- [ ] benötigter Zielport wurde bestimmt.
- [ ] Zielport ist über die IP-Adresse erreichbar.
- [ ] Zielport wurde auch über den Namen getestet.
- [ ] FQDN und Kurzname wurden getrennt geprüft.
- [ ] aktive Netzwerkadapter wurden ermittelt.
- [ ] konfigurierte DNS-Server wurden dokumentiert.
- [ ] DHCP- oder statische DNS-Konfiguration wurde unterschieden.
- [ ] DNS-Suffix wurde geprüft.
- [ ] DNS-Suffixsuchliste wurde geprüft.
- [ ] VPN-Adapter wurden berücksichtigt.
- [ ] virtuelle Adapter wurden berücksichtigt.
- [ ] jeder DNS-Server wurde einzeln abgefragt.
- [ ] Antworten mehrerer DNS-Server wurden verglichen.
- [ ] A-Record wurde geprüft.
- [ ] AAAA-Record wurde geprüft.
- [ ] CNAME-Kette wurde geprüft.
- [ ] zurückgegebene IP-Adressen wurden auf Plausibilität geprüft.
- [ ] alle gelieferten Zieladressen wurden berücksichtigt.
- [ ] TTL wurde dokumentiert.
- [ ] Clientcache wurde vor dem Leeren untersucht.
- [ ] negativer Cache wurde berücksichtigt.
- [ ] `hosts`-Datei wurde geprüft.
- [ ] zuständige DNS-Zone wurde ermittelt.
- [ ] Resource Record wurde serverseitig geprüft.
- [ ] mehrere zuständige DNS-Server wurden verglichen.
- [ ] Zonenreplikation wurde berücksichtigt.
- [ ] Active-Directory-Replikation wurde bei Bedarf geprüft.
- [ ] Forwarder wurden geprüft.
- [ ] Conditional Forwarder wurden geprüft.
- [ ] Delegationen wurden berücksichtigt.
- [ ] UDP und TCP 53 wurden unterschieden.
- [ ] Split-DNS wurde berücksichtigt.
- [ ] VPN-DNS und NRPT wurden berücksichtigt.
- [ ] DNS over HTTPS wurde berücksichtigt.

- [ ] anwendungseigene DNS-Auflösung wurde berücksichtigt.
- [ ] vor Änderungen wurden Antworten und Cachezustände gesichert.
- [ ] nur eine kontrollierbare Änderung wurde durchgeführt.
- [ ] dieselben Abfragen wurden anschließend wiederholt.
- [ ] alle vorgesehenen DNS-Server liefern konsistente Antworten.
- [ ] der benötigte Dienst funktioniert wieder über den Namen.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

30. Schnellreferenz

Ergebnis	Nächster Schritt
IP und Zielport funktionieren, Name nicht	DNS-Pfad untersuchen
IP funktioniert, Zielport nicht	Dienst oder Firewall prüfen
FQDN funktioniert, Kurzname nicht	DNS-Suffix und Suchliste prüfen
kein DNS-Server eingetragen	DHCP- oder Adapterkonfiguration prüfen
falscher DNS-Server eingetragen	vorgesehene Clientkonfiguration prüfen
DNS-Server nicht erreichbar	Routing, VPN, Firewall oder Server prüfen
ein DNS-Server antwortet, ein anderer nicht	zweiten Server oder Netzwerkpfad prüfen
DNS-Server liefern unterschiedliche IPs	Record, Replikation oder Split-DNS prüfen
A korrekt, AAAA falsch	IPv6-Record und IPv6-Pfad prüfen
AAAA korrekt, A falsch	IPv4-Record und IPv4-Pfad prüfen
Name liefert alte IP	Record, TTL und Cache prüfen
direkte Serverabfrage korrekt, Clientantwort falsch	Clientcache, `hosts` oder Resolverpfad prüfen
`NXDOMAIN`	Name, Zone, Record, Replikation oder Weiterleitung prüfen
`SERVFAIL`	Server, DNSSEC, Forwarder oder Delegation prüfen
FQDN in bestimmter Domäne scheitert	Conditional Forwarder oder Delegation prüfen
nur intern fehlerhaft	interne Zone, Split-DNS oder internen Resolver prüfen
nur extern fehlerhaft	Forwarder, Rekursion oder externen DNS-Pfad prüfen
nur mit VPN fehlerhaft	VPN-DNS, NRPT, Suffix oder Routing prüfen
nur ohne VPN fehlerhaft	interner DNS möglicherweise nur über VPN erreichbar
PowerShell funktioniert, Browser nicht	Browsercache, DoH, Proxy oder Anwendung prüfen
normale Abfrage scheitert, `-TcpOnly` funktioniert	UDP 53 oder UDP-Antwortpfad prüfen
TCP-Abfrage scheitert	TCP 53, Firewall oder DNS-Dienst prüfen

Ergebnis	Nächster Schritt
CNAME vorhanden, Ziel nicht auflösbar	vollständige CNAME-Kette prüfen
Fehler nur auf einem Client	Cache, `hosts`, Adapter, VPN oder DoH prüfen
Fehler auf mehreren Clients	DNS-Dienst, DHCP-Option, Zone oder Replikation prüfen

---

Merksatz

> Wenn die IP-Adresse funktioniert, der Name aber nicht, wird von unten nach oben geprüft: richtiger Name, FQDN, Client-DNS, einzelner DNS-Server, A und AAAA, Cache, Zone, Record, Replikation und Weiterleitung. Eine DNS-Antwort ist erst dann brauchbar, wenn sie vom vorgesehenen Server kommt und auf das richtige erreichbare Ziel verweist.

Quellen und weiterführende Dokumentation

- Microsoft Learn – DNS Client PowerShell module
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – Get-DnsClientServerAddress
- Microsoft Learn – Get-DnsClient
- Microsoft Learn – Get-DnsClientGlobalSetting
- Microsoft Learn – Get-DnsClientCache
- Microsoft Learn – Clear-DnsClientCache
- Microsoft Learn – Get-DnsClientDohServerAddress
- Microsoft Learn – Secure DNS Client over HTTPS
- Microsoft Learn – nslookup
- Microsoft Learn – ipconfig
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – DNS zones
- Microsoft Learn – Manage DNS zones
- Microsoft Learn – DNS forwarding
- Microsoft Learn – Get-DnsServerZone
- Microsoft Learn – Get-DnsServerResourceRecord
- Microsoft Learn – Get-DnsServerForwarder
- Microsoft Learn – Get-DnsServerConditionalForwarderZone
- Microsoft Learn – Best practices for DNS client settings