6.3 IP-Adresse erreichbar, Name nicht – DNS- und Namensauflösungsfehler

Wenn ein Ziel über seine IP-Adresse erreichbar ist, der Zugriff über den Namen jedoch scheitert, funktioniert die grundlegende IP-Kommunikation wahrscheinlich. Der Fehler liegt dann häufig bei der Namensauflösung, ihrer Konfiguration oder einem davon abhängigen Dienst.

Typische Meldungen sind:

- „Die Website ist nicht erreichbar.“
- „Der Server wurde nicht gefunden.“
- „Der Netzwerkname wurde nicht gefunden.“
- „Der Hostname kann nicht aufgelöst werden.“
- „Mit der IP-Adresse funktioniert es.“
- „Internet geht, aber interne Anwendungen nicht.“
- „Einige Namen funktionieren, andere nicht.“

Die Aussage „IP geht, Name geht nicht“ grenzt den Fehlerbereich ein. Sie beweist aber noch nicht, dass ausschließlich der DNS-Server defekt ist.

---

1. Technischer Zusammenhang

Anwendungen verwenden häufig Namen statt IP-Adressen.

```
Benutzer oder Anwendung
        ↓
fragt nach server.example.test
        ↓
Namensauflösung
        ↓
liefert eine IP-Adresse
        ↓
Verbindung zur IP-Adresse
```

Beispiel:

```
intranet.example.test → 192.0.2.40
```

Kann der Client `192.0.2.40` erreichen, den Namen `intranet.example.test` jedoch nicht auflösen, müssen insbesondere folgende Bereiche untersucht werden:

- DNS-Konfiguration des Clients,
- Erreichbarkeit des DNS-Servers,
- DNS-Dienst,
- zuständige Zone,
- benötigter Resource Record,
- Weiterleitung oder Rekursion,
- Suchsuffix,
- lokale Namensquellen,
- Cache,
- Firewallregeln für DNS,
- DNSSEC,
- Split-DNS,
- VPN- oder standortspezifische DNS-Konfiguration.

---

2. Fehlerbild zuerst bestätigen

Die Benutzeraussage muss durch konkrete Tests bestätigt werden.

Zu dokumentieren sind:

- exakter Name,
- vollständiger Name oder Kurzname,
- bekannte Ziel-IP-Adresse,
- betroffene Anwendung,
- Fehlermeldung,
- Zeitpunkt,
- betroffener Client,
- verwendete Netzwerkverbindung,
- verwendeter DNS-Server,
- interne oder externe Namensauflösung,
- Vergleich mit einem funktionierenden Client.

Beispiel:

```
Name: fileserver.example.test
IP-Adresse: 192.0.2.40
IP-Adresse erreichbar: ja
Name auflösbar: nein
DNS-Server: 192.0.2.10
Betroffener Client: PC-023
Vergleichsclient: PC-024 funktioniert
```

Ein Test mit einer IP-Adresse muss denselben Zielsystem- und Netzwerkpfad sinnvoll prüfen. Der Aufruf irgendeiner erreichbaren IP-Adresse ist kein ausreichender Vergleich.

3. IP-Erreichbarkeit und Namensauflösung getrennt prüfen

Zuerst wird geprüft, ob das Ziel grundsätzlich per IP erreichbar ist.

Windows

```
ping <ip-adresse>
Test-NetConnection <ip-adresse>
Test-NetConnection <ip-adresse> -Port <port>
```

Linux und macOS

```
ping <ip-adresse>
traceroute <ip-adresse>
nc -vz <ip-adresse> <port>
```

Danach wird derselbe Dienst über den Namen getestet.

Windows

```
ping <name>
Resolve-DnsName <name>
Test-NetConnection <name> -Port <port>
```

Linux und macOS

```
ping <name>
dig <name>
host <name>
nslookup <name>
```

Mögliche Einordnung

Ergebnis	mögliche Einordnung
IP und Name funktionieren	Fehler liegt möglicherweise bei Anwendung, Port, Authentifizierung oder zeitweiligem Zustand
IP funktioniert, Name wird nicht aufgelöst	Namensauflösung untersuchen
Name wird korrekt aufgelöst, Verbindung scheitert	Zieladresse, Port, Firewall, Routing oder Anwendung untersuchen

Ergebnis	mögliche Einordnung
IP und Name scheitern	grundlegende IP-Verbindung, Routing, Firewall oder Zielsystem untersuchen
Name liefert eine falsche IP-Adresse	DNS-Daten, Cache, Hosts-Datei oder Split-DNS untersuchen
nur der Kurzname scheitert	DNS-Suffix oder Suchliste untersuchen
vollständiger Name und Kurzname scheitern	DNS-Server, Zone, Record oder Transport untersuchen

> Eine erfolgreiche Namensauflösung beweist nicht, dass der Zielservice erreichbar ist. Sie bestätigt zunächst nur, dass eine Antwort für den Namen geliefert wurde.

---

4. Vollständigen Namen verwenden

Bei der Fehlersuche sollte zwischen Kurzname und Fully Qualified Domain Name unterschieden werden.

Beispiel:

```
Kurzname:
fileserver

Vollständiger Name:
fileserver.example.test
```

Funktioniert der vollständige Name, der Kurzname jedoch nicht, sind häufig folgende Bereiche betroffen:

- DNS-Suffix fehlt,
- falsches DNS-Suffix,
- falsche Suchreihenfolge,
- VPN stellt keine benötigte Suchdomäne bereit,
- DHCP verteilt eine falsche Domänenoption,
- Kurzname wird über eine andere Auflösungsmethode gesucht,
- mehrere gleichnamige Geräte existieren in verschiedenen Domänen.

Windows

```
ipconfig /all
Get-DnsClientGlobalSetting
Get-DnsClient
```

Linux

```
cat /etc/resolv.conf
resolvectl status
```

macOS

```
scutil --dns
```

Zu prüfen sind:

- primäres DNS-Suffix,
- verbindungsspezifisches DNS-Suffix,
- DNS-Suffixsuchliste,
- Reihenfolge der Suchdomänen,
- aktive Netzwerkschnittstelle,
- vom DHCP-Server gelieferte Einstellungen,
- vom VPN-Client ergänzte Einstellungen.

---

5. Konfigurierte DNS-Server prüfen

Ein Client muss die vorgesehenen DNS-Server verwenden.

Windows

```
ipconfig /all
Get-DnsClientServerAddress
```

Linux

```
resolvectl status
cat /etc/resolv.conf
nmcli device show
```

macOS

```
scutil --dns
networksetup -getdnsservers <netzwerkdienst>
```

Zu prüfen sind:

- richtige DNS-Serveradressen,
- Reihenfolge der DNS-Server,
- IPv4- und IPv6-Konfiguration,
- statische oder dynamische Konfiguration,
- DNS-Angaben aus DHCP,
- DNS-Einstellungen des VPN-Clients,
- lokale Resolver,
- Sicherheitssoftware oder DNS-Filter,
- unerwünschte öffentliche DNS-Server.

In einer Active-Directory-Umgebung dürfen Clients für interne AD-Namen normalerweise nicht ausschließlich beliebige öffentliche DNS-Resolver verwenden. Ein öffentlicher Resolver kennt die internen DNS-Zonen nicht.

---

6. Jeden DNS-Server einzeln abfragen

Sind mehrere DNS-Server eingetragen, muss jeder Server gezielt getestet werden.

Windows

```
Resolve-DnsName <name> -Server <dns-server-1>
Resolve-DnsName <name> -Server <dns-server-2>
```

Alternativ:

```
nslookup <name> <dns-server-1>
nslookup <name> <dns-server-2>
```

Linux und macOS

```
dig @<dns-server-1> <name>
dig @<dns-server-2> <name>
```

Beispielhafte Auswertung

DNS-Server 1	DNS-Server 2	mögliche Einordnung

richtige Antwort	richtige Antwort	DNS-Server grundsätzlich konsistent
richtige Antwort	keine Antwort	zweiter Server, Netzwerkpfad oder Firewall
richtige Antwort	falsche Antwort	abweichende Zone, Replikation oder veraltete Daten
keine Antwort	keine Antwort	Erreichbarkeit, Dienst, Firewall oder Clientkonfiguration
`NXDOMAIN`	richtige Antwort	inkonsistente Zonen oder verschiedene DNS-Sichten
unterschiedliche IP-Adressen	möglicherweise Split-DNS, Replikationsfehler oder abweichende Records	

> Ein Client wechselt nicht in jedem Fall zum nächsten DNS-Server, nur weil der erste Server eine fachlich falsche Antwort liefert. Eine erhaltene negative oder falsche Antwort ist etwas anderes als ein nicht antwortender Server.

---

7. Bedeutung häufiger DNS-Ergebnisse

DNS-Abfragen können unterschiedliche Rückmeldungen liefern.

Ergebnis	Bedeutung	möglicher Untersuchungsbereich
`NOERROR` mit Antwort	Name wurde beantwortet	zurückgegebene Daten auf Richtigkeit prüfen
`NOERROR` ohne passende Antwort	Name oder Typ besitzt möglicherweise keinen entsprechenden Record	Record-Typ, Zone oder Alias prüfen
`NXDOMAIN`	angefragter Name existiert aus Sicht des antwortenden Servers nicht	Schreibweise, Zone, Record, Cache oder falscher DNS-Server
`SERVFAIL`	Server konnte die Anfrage nicht erfolgreich bearbeiten	DNSSEC, Delegation, Upstream-Server oder Serverfehler
`REFUSED`	Server verweigert die Anfrage	Richtlinie, Rekursion, ACL oder nicht erlaubter Client
Zeitüberschreitung	keine rechtzeitige DNS-Antwort	Erreichbarkeit, Port 53, Überlastung oder Dienst
falsche IP-Adresse	Antwort vorhanden, aber ungeeignet	Record, Cache, Hosts-Datei, Split-DNS oder Replikation
`CNAME` ohne erreichbares Endziel	Alias vorhanden, Zielname problematisch	CNAME-Kette und Zielzone untersuchen

Die Meldung `NXDOMAIN` bedeutet nicht automatisch, dass der gesamte DNS-Dienst ausgefallen ist. Der Server hat geantwortet, kennt den angefragten Namen jedoch nicht.

---

8. Record-Typ gezielt prüfen

DNS enthält verschiedene Resource Records.

Typ	Aufgabe
`A`	Name zu IPv4-Adresse
`AAAA`	Name zu IPv6-Adresse
`CNAME`	Alias auf einen anderen Namen
`PTR`	IP-Adresse zu Name bei Rückwärtsauflösung
`MX`	zuständiger Mailserver
`NS`	autoritativer Nameserver einer Zone
`SOA`	Verwaltungsinformationen einer Zone
`SRV`	Dienst und zuständiger Server
`TXT`	Textinformationen, Prüf- und Richtliniendaten

Windows

```
Resolve-DnsName <name> -Type A
Resolve-DnsName <name> -Type AAAA
Resolve-DnsName <name> -Type CNAME
Resolve-DnsName <domain> -Type NS
Resolve-DnsName <domain> -Type SOA
Resolve-DnsName <dienstname> -Type SRV
```

Linux und macOS

```
dig A <name>
dig AAAA <name>
dig CNAME <name>
dig NS <domain>
dig SOA <domain>
dig SRV <dienstname>
```

Wenn eine Anwendung einen bestimmten Record-Typ benötigt, reicht die erfolgreiche Abfrage eines anderen Typs nicht aus.

Beispielsweise können Active-Directory-Dienste von SRV-Records abhängig sein. Ein vorhandener A-Record des Domain Controllers beweist nicht, dass alle benötigten SRV-Records korrekt vorhanden sind.

---

9. DNS-Transport und Port 53 prüfen

DNS verwendet grundsätzlich:

- UDP Port 53,
- TCP Port 53.

UDP wird häufig für normale Abfragen verwendet. TCP kann unter anderem bei größeren, abgeschnittenen oder bestimmten serverseitigen Übertragungen erforderlich sein.

Zu prüfen sind:

- Client erreicht DNS-Server per IP,
- UDP Port 53 ist erlaubt,
- TCP Port 53 ist erlaubt,
- lokale Firewall blockiert nicht,
- Netzwerk-Firewall blockiert nicht,
- VPN erlaubt DNS-Verkehr,
- DNS-Server lauscht auf der vorgesehenen Adresse,
- Antwortpakete erreichen den Client,
- NAT oder Sicherheitsfilter verändern den Verkehr nicht.

Windows

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

Dieser Test prüft TCP Port 53. Er ersetzt keine Prüfung von UDP-DNS.

Linux und macOS

```
dig @<dns-server> <name>
dig +tcp @<dns-server> <name>
```

Mögliche Beobachtungen

Beobachtung	mögliche Einordnung
UDP-Abfrage funktioniert, TCP-Abfrage scheitert	Firewall oder Dienstkonfiguration für TCP 53
kleine Antworten funktionieren, größere nicht	TCP-Fallback, Fragmentierung, EDNS oder MTU

Beobachtung	mögliche Einordnung
Anfrage verlässt Client, keine Antwort sichtbar	DNS-Server, Rückweg oder Filter
Antwort erreicht Netzwerkschnittstelle, Anwendung erhält sie nicht	lokale Firewall, Resolver oder Sicherheitssoftware
DNS-Server ist per IP erreichbar, Port 53 antwortet nicht	Dienst, Firewall oder falsche Zieladresse

---

10. Lokalen DNS-Cache prüfen

Clients und Resolver speichern DNS-Antworten für eine bestimmte Zeit. Auch negative Antworten können zwischengespeichert werden.

Mögliche Symptome:

- ein Client erhält eine alte Adresse,
- andere Clients funktionieren bereits,
- nach einer DNS-Änderung bleibt der Fehler bestehen,
- der Name funktioniert nach Ablauf einer gewissen Zeit,
- eine direkte Abfrage beim DNS-Server ist korrekt, die Anwendung verwendet aber weiterhin eine alte Antwort.

Windows

```
ipconfig /displaydns
Clear-DnsClientCache
```

Alternativ:

```
ipconfig /flushdns
```

Linux mit systemd-resolved

```
resolvectl statistics
sudo resolvectl flush-caches
```

macOS

Die verwendeten Cache-Mechanismen können von der macOS-Version und dem aktiven Resolver abhängen. Vor einer Cache-Bereinigung sollte deshalb zuerst geprüft werden, ob eine direkte DNS-Abfrage bereits die korrekte Antwort liefert.

> Das Leeren des Cache ist eine Prüf- oder Korrekturmaßnahme für zwischengespeicherte Daten. Es behebt keine fehlenden Records, falschen Zonen oder nicht erreichbaren DNS-Server.

---

11. Hosts-Datei berücksichtigen

Vor oder neben DNS können lokale Namensquellen eine Rolle spielen. Eine fehlerhafte Hosts-Datei kann DNS-Ergebnisse überlagern.

Windows

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

Linux und macOS

```
/etc/hosts
```

Zu prüfen sind:

- Eintrag für den betroffenen Namen,
- veraltete IP-Adresse,
- Schreibfehler,
- doppelte Einträge,
- Einträge durch Softwareverteilung,
- Manipulation durch Schadsoftware,
- abweichender Eintrag nur auf einzelnen Clients.

Die Hosts-Datei sollte nicht ungeprüft als dauerhafte Ersatzlösung für einen fehlerhaften DNS-Eintrag verwendet werden. Dadurch würde die zentrale Ursache verborgen und eine schwer wartbare Sonderkonfiguration geschaffen.

---

12. Zuständige Zone und autoritative Server prüfen

Für einen internen Namen muss die zuständige DNS-Zone vorhanden und auf den vorgesehenen Servern verfügbar sein.

Zu prüfen sind:

- existiert die Zone?
- ist sie geladen?
- enthält sie den benötigten Record?
- ist der Record aktiviert und korrekt geschrieben?

- zeigt der Record auf die richtige Adresse?
- besitzt die Zone korrekte NS-Einträge?
- ist die Delegation korrekt?
- stimmen primäre und sekundäre Kopien überein?
- funktioniert die Replikation?
- ist die Seriennummer plausibel?
- bestehen abgelaufene oder veraltete Zonendaten?
- ist eine bedingte Weiterleitung erforderlich?
- antwortet der abgefragte Server autoritativ?

Windows-DNS-Server

```
Get-DnsServerZone
Get-DnsServerResourceRecord -ZoneName <zone>
Get-DnsServerForwarder
```

Allgemeine Abfragen

```
dig NS <domain>
dig SOA <domain>
dig +trace <domain>
```

`dig +trace` zeigt eine schrittweise Auflösung über die DNS-Hierarchie. Für rein interne Zonen ist dieser Test nicht in derselben Weise geeignet wie für öffentlich delegierte Zonen.

---

13. Rekursion und Weiterleitungen prüfen

Ein interner DNS-Server kennt nicht automatisch alle externen Namen. Er verwendet je nach Konfiguration:

- Rekursion,
- Root Hints,
- allgemeine Forwarder,
- Conditional Forwarder,
- Stub-Zonen,
- interne Delegationen.

Mögliche Fehlerbilder:

- interne Namen funktionieren, externe nicht,
- externe Namen funktionieren, eine Partnerdomäne nicht,
- nur Namen einer bestimmten internen Zone scheitern,
- Abfragen an den internen DNS-Server liefern `SERVFAIL`,

- direkte Abfragen an einen öffentlichen Resolver funktionieren,
- ein Forwarder ist nicht erreichbar,
- eine bedingte Weiterleitung zeigt auf veraltete Server.

Abgrenzung

Ergebnis	möglicher Bereich
interne und externe Namen scheitern	Client, DNS-Server, Dienst oder Transport
interne Namen funktionieren, externe nicht	Rekursion, Forwarder, Root Hints oder Firewall
externe Namen funktionieren, interne nicht	interne Zone, falscher DNS-Server oder Split-DNS
nur eine Partnerdomäne scheitert	Conditional Forwarder, Delegation oder Partner-DNS
nur einzelne Records fehlen	Zone, Replikation oder Record-Verwaltung

---

14. Split-DNS berücksichtigen

Bei Split-DNS kann derselbe Name abhängig vom verwendeten DNS-Server oder Standort unterschiedliche Antworten liefern.

Beispiel:

```
intern:
portal.example.test → 192.0.2.50

extern:
portal.example.test → 198.51.100.50
```

Zu prüfen sind:

- befindet sich der Client intern, extern oder im VPN?
- welcher DNS-Server beantwortet die Anfrage?
- wird die interne oder externe Zone verwendet?
- ist die interne Adresse aus dem aktuellen Netz erreichbar?
- wird über das VPN der richtige DNS-Server bereitgestellt?
- verwendet der Browser oder die Anwendung einen eigenen DNS-Dienst?
- existieren widersprüchliche Records?

Ein korrekt funktionierender öffentlicher DNS-Eintrag beweist nicht, dass der interne Eintrag korrekt ist.

---

15. VPN und mehrere Netzwerkschnittstellen

VPN-Verbindungen können DNS-Einstellungen gezielt verändern.

Mögliche Fehlerbilder:

- interne Namen funktionieren nur mit aktivem VPN,
- externe Namen funktionieren, interne nicht,
- nach dem Trennen des VPN bleibt eine ungeeignete DNS-Konfiguration aktiv,
- der Client fragt den DNS-Server der falschen Schnittstelle,
- Split-Tunneling und Split-DNS passen nicht zusammen,
- lokale und entfernte Netze verwenden dieselbe Domäne,
- mehrere aktive Adapter besitzen widersprüchliche DNS-Suffixe.

Zu prüfen sind:

- DNS-Server jeder Schnittstelle,
- Schnittstellenmetrik,
- DNS-Suffixe,
- vom VPN übermittelte Suchdomänen,
- Routen zum internen DNS-Server,
- Erreichbarkeit des DNS-Servers durch den Tunnel,
- Richtlinien des VPN-Clients,
- Zustand nach erneutem Verbindungsaufbau.

Windows

```
Get-NetIPConfiguration
Get-DnsClient
Get-DnsClientServerAddress
Get-NetRoute
```

Linux

```
ip address
ip route
resolvectl status
```

macOS

```
ifconfig
netstat -rn
scutil --dns
```

---

16. IPv4 und IPv6 getrennt betrachten

Ein Name kann sowohl einen A- als auch einen AAAA-Record besitzen.

Mögliche Fehlerbilder:

- A-Record ist korrekt, AAAA-Record ist falsch,
- Client bevorzugt IPv6, der IPv6-Pfad funktioniert jedoch nicht,
- Anwendung erhält nur eine IPv6-Adresse,
- DNS funktioniert, aber die zurückgegebene Adressfamilie ist nicht erreichbar,
- IPv6-DNS-Server ist eingetragen, aber nicht erreichbar.

Zu prüfen sind:

```
Resolve-DnsName <name> -Type A
Resolve-DnsName <name> -Type AAAA
```

```
dig A <name>
dig AAAA <name>
ping -4 <name>
ping -6 <name>
```

Das pauschale Deaktivieren von IPv6 ist keine fachgerechte Standardlösung. Zuerst muss bestätigt werden, ob tatsächlich ein fehlerhafter AAAA-Record, IPv6-DNS-Server oder IPv6-Datenpfad vorliegt.

---

17. DNSSEC prüfen

DNSSEC ermöglicht die Prüfung signierter DNS-Daten. Fehler bei Signaturen oder Vertrauenskette können zu `SERVFAIL` führen.

Mögliche Ursachen:

- abgelaufene Signatur,
- fehlerhafter DS-Record,
- nicht passende Schlüssel,
- unvollständige Vertrauenskette,
- falsche Systemzeit,
- fehlerhafte Zone nach Schlüsselwechsel,
- validierender Resolver verwirft die Antwort.

Linux und macOS mit dig

```
dig +dnssec <name>
dig +trace <name>
```

Bei DNSSEC-Problemen sollten geprüft werden:

- exakter Antwortcode,
- gesetzte DNSSEC-Flags,
- Systemzeit,
- Signaturgültigkeit,
- Delegation,
- Verhalten eines validierenden und eines nicht validierenden Resolvers.

DNSSEC darf nicht pauschal deaktiviert werden, ohne den Fehler einzugrenzen und die Sicherheitsauswirkung zu bewerten.

---

18. Browser und verschlüsseltes DNS

Ein Browser oder eine Sicherheitsanwendung kann einen eigenen DNS-Auflösungsweg verwenden, beispielsweise DNS over HTTPS.

Mögliche Beobachtungen:

- `Resolve-DnsName` oder `dig` liefert eine richtige Antwort,
- nur ein bestimmter Browser verwendet eine falsche oder keine Antwort,
- Browser und Betriebssystem zeigen unterschiedliche Ergebnisse,
- interne Namen funktionieren in einer Anwendung, im Browser jedoch nicht,
- DNS-Filter oder Proxy beeinflusst nur Webverkehr.

Zu prüfen sind:

- verwendet die Anwendung den Systemresolver?
- ist verschlüsseltes DNS aktiviert?
- welcher Resolver wird dabei verwendet?
- kann dieser Resolver interne Zonen kennen?
- besteht ein Proxy?
- besitzt die Anwendung einen eigenen Cache?
- greift eine Sicherheitsrichtlinie ein?

Ein funktionierender Kommandozeilentest beweist daher nicht in jedem Fall, dass die betroffene Anwendung denselben Resolver und dieselben DNS-Daten verwendet.

---

19. mDNS, LLMNR und NetBIOS nicht mit DNS verwechseln

Kurznamen und lokale Gerätenamen können abhängig vom Betriebssystem auch über andere Verfahren aufgelöst werden.

Mögliche Verfahren:

- DNS,
- lokale Hosts-Datei,
- Multicast DNS,
- Link-Local Multicast Name Resolution,
- NetBIOS Name Service,
- anwendungseigene Verzeichnisse.

Wenn ein Kurzname funktioniert, ist damit nicht automatisch bewiesen, dass DNS funktioniert. Der Name könnte über ein anderes Verfahren aufgelöst worden sein.

Für eine eindeutige DNS-Prüfung sollten gezielte Werkzeuge verwendet werden:

```
Resolve-DnsName <vollständiger-name> -Server <dns-server>
```

```
dig @<dns-server> <vollständiger-name>
```

---

20. Reverse DNS getrennt prüfen

Die Rückwärtsauflösung ordnet einer IP-Adresse einen Namen zu. Dafür werden PTR-Records verwendet.

Beispiel:

```
192.0.2.40 → fileserver.example.test
```

Windows

```
Resolve-DnsName <ip-adresse> -Type PTR
```

Linux und macOS

```
dig -x <ip-adresse>
```

Eine fehlende Rückwärtsauflösung verhindert nicht grundsätzlich jede Verbindung zur IP-Adresse. Bestimmte Anwendungen, Protokollierungen, Authentifizierungsverfahren oder

Sicherheitsprüfungen können jedoch von einem korrekten PTR-Record abhängen.

Vorwärts- und Rückwärtsauflösung sind deshalb getrennt zu prüfen.

---

21. Active Directory und DNS

Active Directory ist stark von DNS abhängig.

DNS-Fehler können unter anderem beeinträchtigen:

- Domänenanmeldung,
- Auffinden von Domain Controllern,
- Gruppenrichtlinien,
- Kerberos,
- LDAP,
- Replikation,
- Datei- und Druckdienste,
- Zertifikatsdienste,
- Verwaltungswerkzeuge.

Benötigt werden unter anderem SRV-Records.

Beispielhafte Prüfung:

```
Resolve-DnsName _ldap._tcp.dc._msdcs.<domain> -Type SRV
Resolve-DnsName _kerberos._tcp.<domain> -Type SRV
```

Zu prüfen sind:

- verwendet der Client ausschließlich vorgesehene interne DNS-Server?
- sind SRV-Records vorhanden?
- sind die eingetragenen Domain Controller erreichbar?
- stimmen Systemzeit und Domänenzugehörigkeit?
- sind DNS-Zonen zwischen Domain Controllern repliziert?
- existieren alte Records nicht mehr vorhandener Systeme?
- funktioniert die dynamische DNS-Registrierung?

---

22. Dynamische DNS-Registrierung

Clients und Server können ihre Records dynamisch registrieren.

Mögliche Fehlerbilder:

- neuer Client besitzt noch keinen Record,

- Record zeigt auf eine alte Adresse,
- DHCP aktualisiert DNS nicht,
- Client darf den Record nicht aktualisieren,
- alter Record wurde nicht entfernt,
- Gerät besitzt mehrere Schnittstellen und registriert eine ungeeignete Adresse,
- Replikation verteilt den aktualisierten Record nicht.

Windows-Client

```
ipconfig /registerdns
```

Vor der Verwendung ist zu prüfen:

- soll der Client den Record selbst registrieren?
- übernimmt DHCP die Registrierung?
- besitzt der Client eine gültige DNS-Konfiguration?
- ist die Zone für dynamische Updates eingerichtet?
- bestehen ausreichende Berechtigungen?
- existiert bereits ein Record mit abweichendem Besitzer?

`ipconfig /registerdns` ist keine Lösung für einen falsch eingerichteten DNS-Server oder eine fehlende Zone.

---

23. Zeitabhängige und sporadische Fehler

Sporadische Namensauflösungsfehler können entstehen durch:

- inkonsistente DNS-Server,
- fehlerhafte Replikation,
- abwechselnd richtige und falsche Antworten,
- instabile Netzwerkverbindung,
- Paketverlust,
- überlasteten DNS-Server,
- ablaufende oder erneuerte Cache-Einträge,
- DNS-Round-Robin,
- einen fehlerhaften Server hinter einem Load Balancer,
- unterschiedliche VPN-Zustände,
- zeitweise nicht erreichbare Forwarder.

Sinnvoll sind wiederholte, zeitgestempelte Abfragen.

PowerShell

```
1..10 | ForEach-Object {
    Get-Date
    Resolve-DnsName <name> -Server <dns-server>
    Start-Sleep -Seconds 2
}
```

Bash

```
for i in {1..10}; do
    date
    dig @<dns-server> <name>
    sleep 2
done
```

Zu vergleichen sind:

- Antwortcode,
- Antwortadresse,
- antwortender Server,
- TTL,
- Laufzeit,
- Häufigkeit von Zeitüberschreitungen.

---

24. Paketaufzeichnung für DNS

Eine Paketaufzeichnung kann zeigen:

- ob der Client eine Anfrage sendet,
- welchen DNS-Server er verwendet,
- welcher Name und Record-Typ angefragt wird,
- ob die Anfrage UDP oder TCP verwendet,
- ob eine Antwort zurückkommt,
- welcher Antwortcode geliefert wird,
- ob Wiederholungen auftreten,
- ob verschiedene DNS-Server angesprochen werden,
- ob die Antwort abgeschnitten ist,
- ob der Client die Antwort verwirft.

Wireshark-Filter

```
dns
udp.port == 53
tcp.port == 53
dns.qry.name == "<name>"
ip.addr == <dns-server>
```

Typische Beobachtungen

Paketaufzeichnung	mögliche Einordnung
keine DNS-Anfrage	Anwendungscache, Hosts-Datei, anderer Resolver oder Anwendung sendet nicht
Anfrage an falschen Server	Client-, DHCP-, VPN- oder Schnittstellenkonfiguration
Anfrage, keine Antwort	Server, Transport, Firewall oder Rückweg
Antwort `NXDOMAIN`	Server kennt den Namen nicht
Antwort `SERVFAIL`	serverseitige Auflösung, DNSSEC oder Delegation
richtige Antwort, Anwendung scheitert	Cache, Anwendung, Zielservice oder Datenpfad
wiederholte Anfragen an mehrere Server	Antwortausfall oder Zeitüberschreitung
UDP-Antwort abgeschnitten, TCP scheitert	TCP Port 53, Firewall oder MTU

Paketaufzeichnungen dürfen nur mit entsprechender Berechtigung erstellt und müssen geschützt gespeichert werden.

---

25. Praxisfall A: Nur ein Client kann einen internen Namen nicht auflösen

Symptom

- Server ist per IP erreichbar,
- vollständiger interner Name funktioniert auf anderen Clients,
- nur ein Client ist betroffen,
- externe Namen funktionieren.

Prüfung

1. DNS-Server des betroffenen Clients prüfen.
2. mit funktionierendem Client vergleichen.
3. vollständigen Namen gezielt abfragen.
4. jeden eingetragenen DNS-Server einzeln testen.
5. DNS-Cache prüfen.
6. Hosts-Datei kontrollieren.
7. VPN- und Schnittstellenkonfiguration prüfen.
8. Paketaufzeichnung bei Bedarf durchführen.

Mögliche Ursache

Der Client verwendet aufgrund einer statischen Alt-Konfiguration einen öffentlichen DNS-Server. Dieser kann die interne Zone nicht auflösen.

Nachprüfung

- interner DNS-Server ist eingetragen,
- vollständiger Name wird korrekt aufgelöst,
- Kurzname funktioniert mit richtigem Suffix,
- externe Namen funktionieren weiterhin,
- ursprüngliche Anwendung ist erreichbar.

---

26. Praxisfall B: Interne Namen funktionieren, externe Namen nicht

Symptom

- interne Servernamen werden korrekt aufgelöst,
- externe Namen liefern `SERVFAIL` oder Zeitüberschreitungen,
- Internetziele sind per IP erreichbar,
- mehrere Clients sind betroffen.

Prüfung

1. DNS-Server direkt abfragen.
2. interne und externe Namen vergleichen.
3. allgemeine Forwarder prüfen.
4. Erreichbarkeit der Forwarder untersuchen.
5. Rekursion und Root Hints kontrollieren.
6. Firewallregeln für UDP und TCP Port 53 prüfen.
7. Serverprotokolle auswerten.
8. DNSSEC-Fehler ausschließen.

Mögliche Ursache

Der interne DNS-Server kann interne Zonen selbst beantworten. Der konfigurierte Forwarder für externe Namen ist jedoch nicht mehr erreichbar.

Nachprüfung

- interne Namen funktionieren,
- externe Namen funktionieren,
- mehrere externe Domänen wurden geprüft,
- UDP- und TCP-Abfragen sind möglich,
- redundante Weiterleitung wurde bewertet,
- Monitoring erkennt externe Auflösungsfehler.

27. Praxisfall C: Vollständiger Name funktioniert, Kurzname nicht

Symptom

```
fileserver.example.test → funktioniert
fileserver → funktioniert nicht
```

Prüfung

1. DNS-Suffixsuchliste anzeigen.
2. verbindungsspezifisches Suffix prüfen.
3. DHCP-Optionen kontrollieren.
4. VPN-Konfiguration untersuchen.
5. mit funktionierendem Client vergleichen.
6. tatsächlich angefragte Namen in einer Paketaufzeichnung prüfen.

Mögliche Ursache

Nach einer DHCP-Änderung wird das interne DNS-Suffix nicht mehr an neue Clients verteilt.

Nachprüfung

- vollständiger Name funktioniert,
- Kurzname wird um das richtige Suffix ergänzt,
- neue DHCP-Lease enthält die vorgesehene Konfiguration,
- andere Namensräume funktionieren weiterhin.

---

28. Praxisfall D: Einige Clients erhalten eine falsche IP-Adresse

Symptom

- derselbe Name liefert unterschiedliche Adressen,
- ein Teil der Clients erreicht den Dienst,
- andere Clients verbinden sich mit einem alten Server,
- beide DNS-Server antworten.

Prüfung

1. beide DNS-Server einzeln abfragen.
2. Records und TTL vergleichen.
3. Zone und Replikationszustand prüfen.
4. Cache auf Clients und Resolvern berücksichtigen.
5. Hosts-Dateien ausschließen.
6. Split-DNS-Konfiguration prüfen.

7. Anwendung nach Korrektur erneut testen.

Mögliche Ursache

Ein DNS-Server besitzt aufgrund einer Replikationsstörung noch einen alten A-Record.

Nachprüfung

- alle vorgesehenen DNS-Server liefern dieselbe korrekte Antwort,
- Replikation funktioniert,
- alte Records sind entfernt,
- Clients erreichen den vorgesehenen Dienst,
- Ursache der Replikationsstörung ist dokumentiert.

---

29. Praxisfall E: DNS-Abfrage funktioniert, Browser nicht

Symptom

- Systemwerkzeug liefert die richtige Adresse,
- nur ein Browser kann den internen Namen nicht öffnen,
- andere Anwendungen funktionieren,
- der Browser verwendet verschlüsseltes DNS.

Prüfung

1. Ergebnis des Systemresolvers dokumentieren.
2. Browser-DNS-Konfiguration prüfen.
3. verwendeten verschlüsselten Resolver bestimmen.
4. Browsercache berücksichtigen.
5. Proxy- und Sicherheitsrichtlinien kontrollieren.
6. vollständigen Namen im Browser testen.

Mögliche Ursache

Der Browser sendet DNS-over-HTTPS-Abfragen an einen öffentlichen Resolver, der die interne Zone nicht kennt.

Nachprüfung

- Browser verwendet die vorgesehene Unternehmensrichtlinie,
- interne Namen werden aufgelöst,
- externe Namen funktionieren,
- System- und Browserauflösung liefern konsistente Ergebnisse.

---

30. Ungeeignete Sofortmaßnahmen

Problematisch sind insbesondere:

- DNS-Server ungeprüft neu starten,
- öffentliche DNS-Server dauerhaft auf internen Clients eintragen,
- DNSSEC pauschal deaktivieren,
- IPv6 pauschal deaktivieren,
- Firewall für Port 53 vollständig öffnen,
- fehlende Records durch lokale Hosts-Einträge auf vielen Clients ersetzen,
- komplette Zonen neu erstellen,
- Replikation ohne Sicherung zurücksetzen,
- Caches löschen, ohne vorher den Ausgangszustand zu dokumentieren,
- mehrere DNS-Server gleichzeitig verändern,
- produktive Records ohne Prüfung löschen,
- den DNS-Server als Ursache festlegen, obwohl der Name korrekt aufgelöst wird.

Vor Änderungen sind zu sichern beziehungsweise zu dokumentieren:

- aktuelle Clientkonfiguration,
- verwendete DNS-Server,
- Abfrageergebnisse,
- zuständige Zone,
- vorhandene Records,
- TTL,
- Replikationszustand,
- Weiterleitungen,
- Zeitpunkt und Umfang der Störung.

---

31. Vollständige Prüfreihenfolge

1. exakten betroffenen Namen erfassen.
2. Kurzname und vollständigen Namen unterscheiden.
3. bekannte Ziel-IP-Adresse dokumentieren.
4. Ziel per IP-Adresse und benötigtem Port prüfen.
5. denselben Dienst über den Namen testen.
6. Fehlermeldung und Zeitpunkt dokumentieren.
7. betroffene und funktionierende Clients vergleichen.
8. konfigurierte DNS-Server feststellen.
9. jeden DNS-Server einzeln abfragen.
10. Antwortcode und zurückgegebene Records bewerten.
11. A- und AAAA-Records getrennt prüfen.
12. DNS-Suffix und Suchliste kontrollieren.
13. lokale Hosts-Datei prüfen.
14. Cache nur nach Dokumentation berücksichtigen.
15. Erreichbarkeit des DNS-Servers prüfen.
16. UDP und TCP Port 53 berücksichtigen.

17. zuständige Zone und Record untersuchen.
18. autoritative Server und Delegation prüfen.
19. Replikation zwischen DNS-Servern kontrollieren.
20. Rekursion, Forwarder oder Conditional Forwarder untersuchen.
21. Split-DNS und aktuellen Standort berücksichtigen.
22. VPN und mehrere Schnittstellen prüfen.
23. anwendungseigene Resolver oder verschlüsseltes DNS berücksichtigen.
24. bei Bedarf eine autorisierte Paketaufzeichnung erstellen.
25. konkrete Hypothese formulieren.
26. genau eine kontrollierbare Änderung durchführen.
27. DNS-Abfrage erneut testen.
28. ursprüngliche Anwendung erneut testen.
29. interne und externe Namen prüfen.
30. zweiten DNS-Server und Vergleichsclient prüfen.
31. Ursache, Maßnahme und Ergebnis dokumentieren.
32. Monitoring oder Präventionsmaßnahme festlegen.

---

32. Dokumentationsbeispiel

```
Ticket: INC-20631
Beginn: 02.08.2026, etwa 10:35 Uhr
Umfang: neu verbundene VPN-Clients
Betroffen: interne Servernamen
Nicht betroffen: externe DNS-Namen und direkte IP-Verbindungen

Symptom:
Der Server fileserver.example.test ist über 192.0.2.40 erreichbar.
Der Name kann auf betroffenen VPN-Clients nicht aufgelöst werden.

Ausgangszustand:
- VPN-Tunnel aktiv
- Route zum internen Server vorhanden
- Server per IP und TCP Port 445 erreichbar
- externe Namen werden aufgelöst
- betroffene Clients verwenden einen öffentlichen DNS-Server
- interne DNS-Server werden vom VPN nicht bereitgestellt
- funktionierende interne Clients verwenden 192.0.2.10 und 192.0.2.11

Hypothese:
Die VPN-Konfiguration übermittelt nicht die für interne Zonen
zuständigen DNS-Server.
```

Prüfung:
- Resolve-DnsName über Standardkonfiguration liefert NXDOMAIN
- direkte Abfrage an 192.0.2.10 liefert 192.0.2.40
- interne DNS-Server sind durch den Tunnel erreichbar
- VPN-Profil besitzt keine DNS-Serverzuweisung
- Änderung des VPN-Profils zum Fehlerzeitpunkt festgestellt

Ursache:
Bei einer Änderung des VPN-Profils wurden die internen DNS-Server und die interne Suchdomäne nicht übernommen.

Maßnahme:
Interne DNS-Server und Suchdomäne nach Freigabe wieder in das VPN-Profil aufgenommen.

Nachprüfung:
- vollständiger interner Name wird korrekt aufgelöst
- Kurzname funktioniert über die vorgesehene Suchdomäne
- Dateidienst ist über den Namen erreichbar
- externe Namensauflösung funktioniert
- erneuter VPN-Verbindungsaufbau erfolgreich
- zweiter DNS-Server geprüft
- mehrere VPN-Clients erfolgreich getestet

Prävention:
- DNS-Funktion in den VPN-Abnahmetest aufnehmen
- interne und externe Testnamen überwachen
- Änderungen an VPN-Profilen durch Peer-Review prüfen

---

33. Checkliste „Name geht nicht, IP geht“

- [ ] der exakte betroffene Name wurde dokumentiert.
- [ ] Kurzname und vollständiger Name wurden getrennt getestet.
- [ ] die bekannte Ziel-IP-Adresse wurde geprüft.
- [ ] der benötigte Zielport wurde berücksichtigt.
- [ ] die Fehlermeldung wurde dokumentiert.
- [ ] ein funktionierender Vergleichsclient wurde geprüft.

- [ ] die verwendeten DNS-Server wurden festgestellt.
- [ ] jeder DNS-Server wurde einzeln abgefragt.
- [ ] Antwortcodes wurden ausgewertet.
- [ ] A- und AAAA-Records wurden getrennt geprüft.
- [ ] CNAME-Ketten wurden bei Bedarf verfolgt.
- [ ] DNS-Suffix und Suchliste wurden kontrolliert.
- [ ] DHCP- und VPN-DNS-Einstellungen wurden berücksichtigt.
- [ ] die Hosts-Datei wurde geprüft.
- [ ] der DNS-Cache wurde vor einer Bereinigung bewertet.
- [ ] die Erreichbarkeit des DNS-Servers wurde geprüft.
- [ ] UDP und TCP Port 53 wurden berücksichtigt.
- [ ] die zuständige Zone wurde bestimmt.
- [ ] der benötigte Resource Record wurde geprüft.
- [ ] autoritative Server wurden ermittelt.
- [ ] Delegation und Replikation wurden berücksichtigt.
- [ ] Rekursion und Weiterleitungen wurden geprüft.
- [ ] Split-DNS wurde berücksichtigt.
- [ ] IPv4 und IPv6 wurden getrennt betrachtet.
- [ ] DNSSEC wurde bei `SERVFAIL` berücksichtigt.
- [ ] anwendungseigene oder verschlüsselte DNS-Auflösung wurde geprüft.
- [ ] eine Paketaufzeichnung erfolgte nur mit Berechtigung.
- [ ] vor Änderungen wurde der Ausgangszustand dokumentiert.
- [ ] nur eine kontrollierbare Änderung wurde durchgeführt.
- [ ] die DNS-Abfrage wurde nach der Änderung wiederholt.
- [ ] die ursprüngliche Anwendung wurde erneut getestet.
- [ ] weitere interne und externe Namen wurden geprüft.
- [ ] Ursache, Maßnahme und Nachweis wurden dokumentiert.

---

34. Schnellreferenz

Fehlerbild	wahrscheinlicher Untersuchungsbereich
IP funktioniert, vollständiger Name nicht	DNS-Server, Zone, Record oder DNS-Transport
vollständiger Name funktioniert, Kurzname nicht	DNS-Suffix oder Suchliste
interne Namen funktionieren, externe nicht	Forwarder, Rekursion, Root Hints oder Firewall

Fehlerbild	wahrscheinlicher Untersuchungsbereich
externe Namen funktionieren, interne nicht	falscher DNS-Server, interne Zone oder Split-DNS
nur ein Client betroffen	Clientkonfiguration, Cache, Hosts-Datei oder Anwendung
alle Clients betroffen	zentraler DNS-Dienst, Zone, Netzwerkpfad oder Firewall
nur VPN-Clients betroffen	VPN-DNS, Suchdomäne, Route oder Split-DNS
ein DNS-Server liefert falsche Daten	Zone, Replikation oder veralteter Record
`NXDOMAIN`	Name aus Sicht des antwortenden Servers nicht vorhanden
`SERVFAIL`	Serververarbeitung, Delegation, Forwarder oder DNSSEC
Zeitüberschreitung	Erreichbarkeit, Port 53, Überlastung oder Rückweg
richtige IP wird geliefert, Dienst scheitert	kein reiner DNS-Fehler; Port, Firewall, Anwendung oder Zielsystem
A funktioniert, AAAA führt zum Fehler	IPv6-Record oder IPv6-Datenpfad
Kommandozeile funktioniert, Browser nicht	Browsercache, Proxy oder verschlüsseltes DNS
wechselnde Antworten	mehrere DNS-Server, Round-Robin, Split-DNS oder Replikation
Reverse Lookup scheitert	PTR-Record oder Reverse-Lookup-Zone

Merksatz

> Wenn die IP-Adresse funktioniert, der Name aber nicht, wird die Namensauflösung gezielt und schichtweise geprüft: verwendeter DNS-Server, vollständiger Name, Antwortcode, Record, Zone, Weiterleitung und tatsächlicher Resolver. Eine erreichbare IP-Adresse grenzt den Fehler ein, beweist aber weder einen DNS-Server-Ausfall noch die Funktionsfähigkeit des angesprochenen Dienstes.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Guidance for troubleshooting DNS
- Microsoft Learn – Troubleshooting DNS clients
- Microsoft Learn – Troubleshoot DNS client name resolution issues
- Microsoft Learn – Troubleshooting DNS servers
- Microsoft Learn – DNS forwarder-related resolution failures
- Microsoft Learn – Best practices for DNS client settings
- RFC 1034 – Domain Names: Concepts and Facilities

- RFC 1035 – Domain Names: Implementation and Specification
- RFC 2181 – Clarifications to the DNS Specification
- RFC 9499 – DNS Terminology
- Wireshark – Display Filter Reference: DNS