7.12 Systematischer DNS-Diagnoseablauf

> **Kurz erklärt**
>
> DNS-Störungen dürfen nicht durch wahlloses Leeren von Caches, Ändern von DNS-Servern oder Neuerstellen von Einträgen diagnostiziert werden.
>
> Der sichere Ablauf beginnt beim exakten Fehlerbild und verfolgt die Namensauflösung schrittweise vom Client über den verwendeten Resolver, den Transportweg und rekursive DNS-Server bis zum autoritativen Server und den tatsächlichen Zonendaten.

7.12.1 Ziel des Diagnoseablaufs

Der Diagnoseablauf soll eindeutig bestimmen:

- welcher Name oder welche IP-Adresse betroffen ist;
- welcher Datensatztyp benötigt wird;
- welcher Client und welche Anwendung betroffen sind;
- welcher Resolverweg tatsächlich verwendet wird;
- welcher DNS-Server die Anfrage erhält;
- ob eine Antwort eintrifft;
- welcher Antwortcode zurückgegeben wird;
- ob die Antwort korrekt und aktuell ist;
- ob die Antwort aus einem Cache oder einer autoritativen Zone stammt;
- an welcher Stelle eine Verzögerung oder ein Fehler entsteht;
- welche einzelne Maßnahme die nachgewiesene Ursache behebt;
- wie die vollständige Funktion anschließend verifiziert wird.

DNS-Diagnose bedeutet nicht nur, irgendeine erfolgreiche Antwort zu erhalten. Die Antwort muss vom vorgesehenen DNS-Pfad stammen, fachlich korrekt sein und innerhalb einer angemessenen Zeit eintreffen.

7.12.2 Grundregeln

1. Zuerst beobachten und dokumentieren.
2. Den exakten Namen und Datensatztyp verwenden.
3. Clientverhalten und direkte DNS-Abfrage unterscheiden.
4. Den tatsächlich verwendeten DNS-Server bestimmen.
5. Antwortcode und Antwortinhalt getrennt bewerten.
6. Positive, negative und ausgebliebene Antworten unterscheiden.

7. Cache-, rekursive und autoritative Antworten trennen.
8. UDP, TCP, DoH und DoT nicht gleichsetzen.
9. Pro Versuch nur eine relevante Variable verändern.
10. Vor jeder Änderung Risiko und Rückweg dokumentieren.
11. Nach der Maßnahme denselben Test wiederholen.
12. Erst nach technischer Verifikation den Vorgang abschließen.

Folgende Maßnahmen sind keine geeigneten ersten Diagnoseschritte:

- DNS-Cache sofort löschen;
- öffentlichen DNS-Server eintragen;
- DNS-Dienst neu starten;
- Zone neu erstellen;
- DNS-Einträge vorsorglich löschen;
- Forwarder verändern;
- Scavenging aktivieren;
- Client erneut in die Domäne aufnehmen;
- Firewall oder DNSSEC deaktivieren;
- VPN-, NRPT- oder DoH-Richtlinien entfernen.

7.12.3 Fehleraufnahme

Vor dem ersten Test sind mindestens folgende Angaben zu erfassen:

Angabe	Beispiel
Zeitpunkt	`2026-08-02 14:35:20`
Client	`client25.example.test`
Benutzer beziehungsweise Dienst	betroffene Sitzung oder Dienstkonto
Anwendung	Browser, RDP, Mail, Dateifreigabe, AD-Anmeldung
eingegebener Name	`app.example.test`
erwarteter FQDN	`app.example.test.`
erwarteter Datensatztyp	A, AAAA, CNAME, PTR, SRV, MX oder TXT
erwartetes Ergebnis	vorgesehene IP-Adresse oder Zielname
tatsächliches Ergebnis	Fehlertext oder falsche Antwort
verwendetes Netzwerk	LAN, WLAN, VPN oder Mobilfunk
Quell-IP-Adresse	aktive Clientadresse
konfigurierte DNS-Server	Reihenfolge und Schnittstelle
Fehlerumfang	einzelner Client, Standort, Zone oder alle Systeme
letzte Änderung	DNS, DHCP, VPN, Firewall, Server, Zertifikat oder Netzwerk

Kennwörter, Zugangsdaten und unnötige personenbezogene Daten dürfen nicht in die Fehlerdokumentation übernommen werden.

7.12.4 Störung einordnen

Fehlerklasse	Typisches Symptom
vollständiger Ausfall	keine DNS-Abfrage funktioniert
namensbezogener Fehler	nur ein bestimmter Name schlägt fehl
zonenbezogener Fehler	alle Namen einer Zone schlagen fehl
datensatzbezogener Fehler	A funktioniert, SRV oder PTR jedoch nicht
resolverbezogener Fehler	nur ein bestimmter DNS-Server liefert Fehler
clientbezogener Fehler	derselbe Name funktioniert an anderen Clients
anwendungsbezogener Fehler	direkte DNS-Abfrage funktioniert, Anwendung nicht
standortbezogener Fehler	Fehler tritt nur in einem Netz oder VPN auf
zeitabhängiger Fehler	Fehler tritt nur zeitweise auf
leistungsbezogener Fehler	Antwort ist korrekt, aber zu langsam
datenbezogener Fehler	DNS liefert eine falsche oder veraltete Antwort
transportbezogener Fehler	UDP, TCP, DoH oder DoT verhalten sich unterschiedlich
validierungsbezogener Fehler	DNSSEC führt zu `SERVFAIL` oder Validierungsfehler
reversebezogener Fehler	IP-Adresse lässt sich nicht korrekt in einen Namen auflösen

Diese Einordnung bestimmt, welche Vergleichstests aussagekräftig sind.

7.12.5 Geeignete Testdaten festlegen

Für reproduzierbare Tests müssen folgende Werte feststehen:

- exakter FQDN;
- gewünschter Datensatztyp;
- erwarteter Wert;
- vorgesehener DNS-Server;
- autoritativer DNS-Server;
- Vergleichsname, der sicher funktioniert;
- Vergleichsname, der sicher nicht existiert;
- vorgesehene Antwortzeit oder vorhandene Baseline.

Ein kurzer Name wie:

```
server01
```

ist für eine eindeutige DNS-Diagnose ungeeignet, solange nicht feststeht, welches DNS-Suffix ergänzt wird.

Besser:

```
server01.example.test.
```

Der abschließende Punkt kennzeichnet einen vollständig qualifizierten absoluten DNS-Namen. Viele Werkzeuge funktionieren auch ohne diesen Punkt, können dann jedoch abhängig von Suchsuffixen zusätzliche Namen prüfen.

7.12.6 DNS-Auflösung als Kette betrachten

Eine Namensauflösung kann folgende Stationen durchlaufen:

Station	Aufgabe
Anwendung	fordert eine Namensauflösung an oder verwendet eigenen Resolver
lokale Namensquelle	Hosts-Datei oder anwendungseigener Cache
Betriebssystemresolver	wertet Cache, Suffixe, Richtlinien und DNS-Server aus
lokaler Stub-Resolver	nimmt Anfragen lokal entgegen und leitet sie weiter
VPN-, Container- oder Sicherheitsresolver	beeinflusst den Abfrageweg
rekursiver DNS-Server	beschafft die vollständige Antwort für den Client
Forwarder	übernimmt weitergeleitete Anfragen
DNS-Hierarchie	verweist schrittweise auf zuständige Server
autoritativer DNS-Server	liefert die maßgeblichen Zonendaten
Cache auf dem Rückweg	speichert positive oder negative Antworten

Die Diagnose folgt dieser Kette vom Client in Richtung autoritativer Datenquelle.

7.12.7 Umfang der Störung bestimmen

Kontrollierte Vergleiche:

Vergleich	Aussage
gleicher Name, anderer Client	clientbezogenen Fehler prüfen

Vergleich	Aussage
gleicher Client, anderer Name	namens- oder zonenbezogenen Fehler prüfen
gleicher Name, anderer DNS-Server	resolverbezogenen Fehler prüfen
gleiche Abfrage, direkt gegen autoritativen Server	Rekursion und Autorität trennen
gleiche Abfrage mit und ohne VPN	VPN-, NRPT- oder Split-DNS-Fehler prüfen
gleiche Abfrage über UDP und TCP	Transportfehler prüfen
direkte DNS-Abfrage und Anwendung	DNS- und Anwendungsfehler trennen
Vorwärts- und Rückwärtsauflösung	A/AAAA und PTR getrennt prüfen
erste und wiederholte Abfrage	Cachewirkung prüfen
interner und externer Name	interne Zone und Rekursion trennen

Erst nach diesen Vergleichen sollte eine konkrete Ursache angenommen werden.

7.12.8 Clientidentität und Netzwerkzustand prüfen

Windows

```
Get-NetIPConfiguration
```

```
ipconfig /all
```

Linux

```
ip address
```

```
ip route
```

macOS

```
ifconfig
```

```
route -n get default
```

Zu prüfen sind:

- aktive Schnittstelle;
- IPv4- und IPv6-Adresse;
- Subnetz beziehungsweise Präfix;
- Standardgateway;
- DNS-Server;
- DHCP- oder statische Konfiguration;
- Verbindungssuffix;
- VPN-Schnittstelle;
- unerwartete zusätzliche Schnittstellen;
- Container-, Hypervisor- oder Sicherheitsadapter.

Eine vorhandene IP-Adresse beweist nicht, dass der vorgesehene DNS-Server erreichbar ist.

7.12.9 DNS-Server und Resolverkonfiguration ermitteln

Windows

```
Get-DnsClientServerAddress
```

```
Get-DnsClient
```

Linux

```
cat /etc/resolv.conf
```

Bei `systemd-resolved`:

```
resolvectl status
```

macOS

```
scutil --dns
```

Zu prüfen sind:

- DNS-Server pro Schnittstelle;
- Reihenfolge der DNS-Server;
- DNS-Suffixe;
- Suchliste;
- VPN-spezifische Resolver;

- IPv4- und IPv6-DNS-Server;
- lokale Stub-Adressen;
- namensraumabhängige Resolver.

`/etc/resolv.conf` kann lediglich auf einen lokalen Stub-Resolver verweisen. In diesem Fall müssen die tatsächlichen Upstream-DNS-Server über den zuständigen Resolverdienst ermittelt werden.

7.12.10 Interne Clients und öffentliche DNS-Server

Domänenmitglieder und interne Clients müssen für interne Namensräume die vorgesehenen internen DNS-Server verwenden.

Das Eintragen eines öffentlichen DNS-Servers wie eines Resolverdienstes im Internet kann:

- interne Zonen unauflösbar machen;
- Active-Directory-SRV-Einträge verbergen;
- Split-DNS umgehen;
- interne Namen an externe Resolver übertragen;
- Anmeldungen, Gruppenrichtlinien und Dienstsuche beeinträchtigen;
- zu wechselnden Ergebnissen führen.

Ein öffentlicher DNS-Server darf deshalb nicht als pauschale Reparatur für einen internen DNS-Fehler eingetragen werden.

7.12.11 Hosts-Datei und lokale Namensquellen prüfen

Hosts-Dateien:

Betriebssystem	Pfad
Windows	`C:\Windows\System32\drivers\etc\hosts`
Linux	`/etc/hosts`
macOS	`/etc/hosts`

Zu prüfen sind:

- existiert ein Eintrag für den betroffenen Namen?
- stimmt die eingetragene IP-Adresse?
- existieren doppelte oder auskommentierte Varianten?
- verwendet die Anwendung einen eigenen lokalen Namensspeicher?
- stammt die erfolgreiche Auflösung überhaupt aus DNS?

Eine direkte Abfrage mit ausdrücklich angegebenem DNS-Server kann erfolgreich sein, während eine Anwendung wegen eines falschen lokalen Eintrags eine andere Adresse verwendet.

7.12.12 Kurznamen und DNS-Suffixe prüfen

Wenn ein Benutzer nur folgenden Namen verwendet:

```
server01
```

kann der Resolver abhängig von seiner Suchliste nacheinander verschiedene Namen bilden:

```
server01.example.test
server01.branch.example.test
server01.other.example.test
```

Windows-Konfiguration prüfen:

```
Get-DnsClient
```

Linux mit `systemd-resolved`:

```
resolvectl status
```

macOS:

```
scutil --dns
```

Mögliche Fehler:

- falsches Verbindungssuffix;
- fehlende Suchdomäne;
- zu lange Suchliste;
- unerwartete Reihenfolge;
- unterschiedliche Suffixe zwischen LAN und VPN;
- ein Kurzname trifft unbeabsichtigt auf eine andere Zone;
- Suchanfragen erzeugen zusätzliche Verzögerungen.

Für die technische Diagnose sollte zuerst der vollständige FQDN verwendet werden.

7.12.13 Tatsächlichen Windows-Resolverpfad bestimmen

Unter Windows können NRPT, VPN-Richtlinien und verschlüsseltes DNS den Abfrageweg verändern.

Wirksame NRPT-Richtlinien:

```
Get-DnsClientNrptPolicy
```

Konfigurierte NRPT-Regeln:

```
Get-DnsClientNrptRule
```

DNS-Clientzustand:

```
netsh dnsclient show state
```

Globale verschlüsselte DNS-Einstellungen:

```
netsh dnsclient show global
```

Konfigurierte DoH- oder DoT-Endpunkte:

```
netsh dnsclient show encryption
```

Wichtig:

- `Resolve-DnsName` kann den Windows-Resolverpfad einschließlich NRPT verwenden.
- `nslookup` verwendet einen eigenen Abfrageweg und eignet sich nicht allein zur Prüfung der NRPT.
- Browser oder andere Anwendungen können eigene DoH-Resolver verwenden.
- Eine direkte Abfrage mit `-Server` prüft den angegebenen DNS-Server, aber nicht zwingend die gesamte normale Resolverauswahl der Anwendung.

Deshalb müssen Systemauflösung und direkte Serverabfrage getrennt getestet werden.

7.12.14 Anwendung und DNS voneinander abgrenzen

Folgende Ergebnisse sind getrennt zu prüfen:

1. Kann die Ziel-IP-Adresse direkt erreicht werden?
2. Liefert eine direkte DNS-Abfrage die erwartete Adresse?
3. Liefert der normale Betriebssystemresolver dieselbe Adresse?
4. Verwendet die Anwendung dieselbe Adresse?
5. Ist der eigentliche Dienst auf der Zieladresse erreichbar?

Beispiel:

```
Resolve-DnsName "app.example.test"
```

Direkte Abfrage gegen einen bestimmten DNS-Server:

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Type A `
  -Server "192.0.2.53" `
  -DnsOnly
```

Wenn DNS die richtige IP-Adresse liefert, die Anwendung aber weiterhin fehlschlägt, müssen unter anderem Anwendungscache, Proxy, TLS-Zertifikat, Dienstport und Anwendungsrichtlinien geprüft werden.

Ein erfolgreicher DNS-Test beweist nicht, dass der Zielservice funktioniert.

7.12.15 Direkte DNS-Abfragen durchführen

Windows PowerShell

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Type A `
  -Server "192.0.2.53" `
  -DnsOnly
```

Windows Eingabeaufforderung

```
nslookup app.example.test 192.0.2.53
```

Linux und macOS

```
dig @192.0.2.53 app.example.test A
```

Bei jedem Test sind zu dokumentieren:

- Abfragename;

- Datensatztyp;
- verwendeter DNS-Server;
- Antwortcode;
- Antwortinhalt;
- TTL;
- Antwortzeit;
- Flags;
- autoritative oder rekursive Antwort;
- zusätzliche CNAME-Ziele.

7.12.16 Datensatztypen gezielt prüfen

Aufgabe	Datensatz
IPv4-Adresse ermitteln	A
IPv6-Adresse ermitteln	AAAA
Alias verfolgen	CNAME
Mailserver ermitteln	MX
Dienst und Port ermitteln	SRV
IP-Adresse rückwärts auflösen	PTR
Zonenautorität prüfen	SOA
autoritative Server ermitteln	NS
Richtlinien- oder Verifikationstext prüfen	TXT
DNSSEC-Schlüssel prüfen	DNSKEY
Delegationssignatur prüfen	DS

Beispiele:

```
Resolve-DnsName "app.example.test" -Type A
```

```
Resolve-DnsName "alias.example.test" -Type CNAME
```

```
Resolve-DnsName "_service._tcp.example.test" -Type SRV
```

```
Resolve-DnsName "example.test" -Type SOA
```

```
Resolve-DnsName "example.test" -Type NS
```

Bei CNAME, MX und SRV muss zusätzlich geprüft werden, ob der zurückgegebene Zielname über A oder AAAA auflösbar ist.

7.12.17 DNS-Antwortcodes auswerten

Ergebnis	Bedeutung	Nächster Schritt
`NOERROR` mit Antwort	Abfrage erfolgreich	Inhalt, TTL und Quelle prüfen
`NOERROR` ohne gesuchten Datensatz	Name kann existieren, Datensatztyp fehlt	anderen Datensatztyp und SOA prüfen
`NXDOMAIN`	abgefragter Name existiert laut Antwort nicht	Name, Zone, Autorität und negativen Cache prüfen
`SERVFAIL`	Server konnte keine verwertbare Antwort erzeugen	Delegation, DNSSEC, Forwarder und Serverprotokolle prüfen
`REFUSED`	Server verweigert die Abfrage	ACL, Rekursion, Richtlinie und Quellnetz prüfen
`FORMERR`	DNS-Nachricht wurde als fehlerhaft bewertet	Client, Server und Netzwerkgerät prüfen
`NOTIMP`	angeforderte Funktion wird nicht unterstützt	Abfragefunktion und Serverfähigkeit prüfen
Timeout	keine verwertbare Antwort innerhalb der Wartezeit	Netzwerk, Transport und Serververfügbarkeit prüfen
`TC` gesetzt	UDP-Antwort wurde abgeschnitten	erneuten Versuch über TCP prüfen

Wichtige Unterscheidungen:

- `NODATA` ist kein eigener RCODE, sondern beschreibt typischerweise `NOERROR` ohne den angefragten Datensatz.
- Timeout ist keine DNS-Antwort.
- `SERVFAIL` beweist nicht, dass der Name nicht existiert.
- `NXDOMAIN` und ein fehlender einzelner Datensatztyp sind nicht dasselbe.
- Extended DNS Errors können zusätzliche Hinweise liefern, werden aber nicht von jedem Resolver oder Diagnosewerkzeug angezeigt.

7.12.18 Antwortflags berücksichtigen

Typische DNS-Flags:

Flag	Bedeutung
`AA`	Antwort ist für die beantwortete Zone autoritativ

Flag	Bedeutung
`RD`	Client hat Rekursion angefordert
`RA`	Server bietet Rekursion an
`TC`	Antwort wurde abgeschnitten
`AD`	Resolver kennzeichnet Daten als DNSSEC-validiert
`CD`	Client fordert an, Validierungsfehler nicht als Sperre zu verwenden

Ein gesetztes `AD`-Flag muss im Zusammenhang mit dem verwendeten validierenden Resolver bewertet werden. Das bloße Anfordern von DNSSEC-Daten beweist keine erfolgreiche Validierung.

7.12.19 Antwortzeit messen

Windows

```
Measure-Command {
    Resolve-DnsName `
      -Name "app.example.test" `
      -Type A `
      -Server "192.0.2.53" `
      -DnsOnly
}
```

Linux und macOS

```
dig @192.0.2.53 app.example.test A +stats
```

Zu vergleichen sind:

- erste Abfrage;
- unmittelbar wiederholte Abfrage;
- vorhandener Name;
- nicht vorhandener Name;
- interner Name;
- externer Name;
- primärer DNS-Server;
- alternativer DNS-Server;
- rekursiver DNS-Server;
- autoritativer DNS-Server;
- UDP;

- TCP;
- mit und ohne VPN.

`Measure-Command` enthält auch den PowerShell-Befehlsaufwand. Es eignet sich deshalb vor allem für Vergleiche unter denselben Bedingungen.

7.12.20 Cachezustand prüfen

Windows-Clientcache

```
Get-DnsClientCache
```

Alternativ:

```
ipconfig /displaydns
```

Linux mit systemd-resolved

```
resolvectl statistics
```

Windows-DNS-Servercacheeinstellungen

```
Get-DnsServerCache
```

`Get-DnsServerCache` zeigt Cacheeinstellungen des Windows-DNS-Servers und nicht einfach eine vollständige Liste aller zwischengespeicherten Antworten.

Zu prüfen sind:

- positiver oder negativer Cacheeintrag;
- Datensatztyp;
- gespeicherter Wert;
- verbleibende TTL;
- Herkunft des Eintrags;
- Verhalten nach Ablauf der TTL;
- Unterschiede zwischen Anwendung, Client und DNS-Server.

Cachelöschung verändert Beweisdaten und darf erst nach der Dokumentation als kontrollierter Vergleich erfolgen.

7.12.21 Positive und negative Zwischenspeicherung unterscheiden

Positive Antworten können A-, AAAA-, CNAME-, PTR- oder andere Datensätze zwischenspeichern.

Negative Zwischenspeicherung kann unter anderem betreffen:

- nicht vorhandenen Namen;
- vorhandenen Namen ohne angefragten Datensatztyp;
- vorübergehende Auflösungsfehler, abhängig vom Resolververhalten.

Mögliche Folge:

1. Ein Name wird abgefragt und liefert `NXDOMAIN`.
2. Der fehlende Datensatz wird anschließend angelegt.
3. Der Client oder rekursive Resolver liefert zunächst weiterhin die gespeicherte negative Antwort.
4. Erst nach Ablauf oder kontrollierter Löschung des Cacheeintrags wird der neue Datensatz sichtbar.

Deshalb müssen SOA-Daten, negative TTL und alle beteiligten Cacheebenen berücksichtigt werden.

7.12.22 DNS-Server vergleichen

Eine identische Abfrage muss gezielt an jeden vorgesehenen DNS-Server gesendet werden.

Windows

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Type A `
  -Server "192.0.2.53" `
  -DnsOnly
```

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Type A `
  -Server "192.0.2.54" `
  -DnsOnly
```

Linux und macOS

```
dig @192.0.2.53 app.example.test A
```

```
dig @192.0.2.54 app.example.test A
```

Zu vergleichen sind:

- Antwortcode;
- Datensatzwert;
- TTL;
- CNAME-Kette;
- Antwortzeit;
- Autoritätsflag;
- SOA- und NS-Daten;
- DNSSEC-Verhalten.

Unterschiedliche Antworten können auf Cache-, Zonen-, Replikations-, Zonentransfer- oder Konfigurationsprobleme hinweisen.

7.12.23 UDP und TCP prüfen

Klassische DNS-Abfragen verwenden häufig UDP-Port `53`. TCP-Port `53` wird unter anderem benötigt:

- bei abgeschnittenen UDP-Antworten;
- bei größeren Antworten;
- bei bestimmten DNSSEC-Antworten;
- bei Zonentransfers;
- wenn TCP ausdrücklich angefordert wird.

TCP-Erreichbarkeit unter Windows:

```
Test-NetConnection "192.0.2.53" -Port 53
```

Dieser Befehl prüft nur TCP.

Normale DNS-Abfrage:

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Server "192.0.2.53" `
  -DnsOnly
```

TCP erzwingen:

```
Resolve-DnsName `
  -Name "app.example.test" `
  -Server "192.0.2.53" `
  -DnsOnly `
  -TcpOnly
```

Mit `dig`:

```
dig @192.0.2.53 app.example.test A
```

```
dig @192.0.2.53 app.example.test A +tcp
```

Wenn UDP fehlschlägt und TCP funktioniert, sind Firewall, Paketverlust, EDNS, MTU und Fragmentierung zu prüfen.

7.12.24 EDNS, MTU und Fragmentierung prüfen

Hinweise auf ein Größen- oder Transportproblem:

- einfache A-Abfrage funktioniert;
- größere TXT-, DNSKEY- oder DNSSEC-Antwort schlägt fehl;
- Fehler tritt nur über VPN oder Tunnel auf;
- UDP endet im Timeout;
- dieselbe Abfrage funktioniert über TCP;
- Netzwerkaufzeichnung zeigt fragmentierte oder verlorene Pakete.

Vergleich:

```
dig @192.0.2.53 example.com A +dnssec
```

```
dig @192.0.2.53 example.com A +dnssec +tcp
```

Test ohne EDNS:

```
dig @192.0.2.53 example.com A +noedns
```

Das testweise Unterdrücken von EDNS dient nur der Eingrenzung. EDNS darf nicht dauerhaft deaktiviert werden, um einen fehlerhaften Netzwerkpfad zu verdecken.

7.12.25 Verschlüsseltes DNS prüfen

DNS over HTTPS und DNS over TLS verändern den Transportweg.

Zu prüfen sind:

- verwendetes Protokoll;
- Resolveradresse;
- DoH-URI beziehungsweise DoT-Hostname;
- TCP-Port;
- TLS-Zertifikat;
- Zertifikatsname;
- Vertrauenskette;
- Fallback auf klassisches DNS;
- Firewall- und Proxyweg;
- Anwendung mit eigenem DoH-Resolver;
- Erreichbarkeit interner Zonen.

Windows-Zustand:

```
netsh dnsclient show state
```

```
netsh dnsclient show encryption
```

Bei verschlüsseltem DNS kann eine klassische Paketaufzeichnung den DNS-Inhalt nicht ohne zusätzliche, autorisierte Entschlüsselungsinformationen anzeigen.

Ein erfolgreicher Test gegen UDP- oder TCP-Port `53` beweist nicht, dass ein DoH- oder DoT-Endpunkt funktioniert.

7.12.26 Rekursiven und autoritativen DNS-Server unterscheiden

Ein rekursiver DNS-Server beschafft die Antwort im Auftrag des Clients.

Ein autoritativer DNS-Server verwaltet die maßgeblichen Daten einer Zone.

Diagnosevergleich:

1. Client fragt vorgesehenen rekursiven DNS-Server.
2. Rekursiver Server liefert Fehler oder langsame Antwort.
3. Autoritativer DNS-Server wird direkt abgefragt.
4. Ergebnisse werden verglichen.

Wenn der autoritative Server korrekt und schnell antwortet, liegt die Ursache wahrscheinlich bei:

- Rekursion;
- Forwarder;
- Cache;
- DNSSEC-Validierung;
- Netzwerkpfad;
- Richtlinie des rekursiven Servers.

Wenn bereits der autoritative Server falsche Daten liefert, sind Zone, Datensatz, Delegation und Replikation zu prüfen.

7.12.27 SOA-, NS- und Delegationsdaten prüfen

SOA prüfen:

```
Resolve-DnsName `
  -Name "example.test" `
  -Type SOA `
  -Server "192.0.2.53" `
  -DnsOnly
```

NS prüfen:

```
Resolve-DnsName `
  -Name "example.test" `
  -Type NS `
  -Server "192.0.2.53" `
  -DnsOnly
```

Mit `dig`:

```
dig @192.0.2.53 example.test SOA
```

```
dig @192.0.2.53 example.test NS
```

Öffentliche Delegationskette verfolgen:

```
dig app.example.test A +trace
```

Zu prüfen sind:

- richtige Zonengrenze;
- zuständige autoritative Server;
- Erreichbarkeit aller autoritativen Server;
- korrekte NS-Einträge;
- erforderliche Glue Records;
- SOA-Seriennummer;
- widersprüchliche Antworten;
- veraltete Delegation;
- fehlende oder falsche Child-Zone.

`dig +trace` folgt der öffentlichen DNS-Hierarchie. Interne Split-DNS-Zonen, bedingte Forwarder und private Namensräume müssen über den internen DNS-Pfad geprüft werden.

7.12.28 Forwarder, bedingte Forwarder und Rekursion prüfen

Auf einem Windows-DNS-Server:

```
Get-DnsServerForwarder
```

```
Get-DnsServerRecursion
```

```
Get-DnsServerRootHint
```

Zonen und bedingte Weiterleitungen:

```
Get-DnsServerZone
```

Zu prüfen sind:

- Erreichbarkeit aller Forwarder;
- Antwortzeit jedes Forwarders;
- bedingter Forwarder für den betroffenen Namensraum;
- aktuelle Zieladressen;
- Replikationsbereich eines AD-integrierten bedingten Forwarders;
- aktivierte oder deaktivierte Rekursion;
- Root-Hint-Verwendung;
- DNS-Richtlinien und Rekursionsbereiche;
- Timeout- und Fallbackverhalten.

Ein nicht erreichbarer erster Forwarder kann Verzögerungen verursachen, bevor ein weiterer Auflösungspfad verwendet wird.

7.12.29 Reverse-Lookups prüfen

Windows

```
Resolve-DnsName `
  -Name "192.0.2.25" `
  -Type PTR `
  -Server "192.0.2.53" `
  -DnsOnly
```

Linux und macOS

```
dig @192.0.2.53 -x 192.0.2.25
```

Danach muss der PTR-Zielname wieder vorwärts geprüft werden:

```
Resolve-DnsName `
  -Name "host25.example.test" `
  -Type A `
  -Server "192.0.2.53" `
  -DnsOnly
```

Zu prüfen sind:

- Reverse-Zone;
- Delegation;
- PTR-Eintrag;
- Zielname;
- TTL;
- Vorwärts-Rückwärts-Konsistenz;
- veraltete Einträge;
- öffentliche oder private Zuständigkeit;
- dynamische Aktualisierung.

Ein fehlender PTR-Eintrag beweist keinen vollständigen DNS-Ausfall.

7.12.30 DNSSEC systematisch abgrenzen

DNSSEC-Daten anfordern:

```
Resolve-DnsName `
  -Name "example.com" `
  -Type A `
  -Server "192.0.2.53" `
  -DnsOnly `
  -DnssecOk
```

Mit `dig`:

```
dig @192.0.2.53 example.com A +dnssec
```

Zu prüfen sind:

- tritt `SERVFAIL` nur bei signierten Zonen auf?
- funktioniert die Abfrage über einen nicht validierenden Vergleichspfad?
- existieren DS- und DNSKEY-Datensätze?
- sind Signaturen gültig?
- stimmt die Systemzeit?
- ist der Trust Anchor vorhanden?
- verlangt die NRPT DNSSEC-Validierung?
- zeigt der Resolver einen Extended DNS Error an?
- besteht ein Größen- oder Transportproblem?

`-DnssecOk` und `+dnssec` fordern DNSSEC-bezogene Daten an. Diese Optionen beweisen allein keine erfolgreiche Validierung.

`nslookup` ist nicht für eine vollständige DNSSEC-Diagnose geeignet.

7.12.31 Windows-DNS-Serverzustand prüfen

Dienststatus:

```
Get-Service -Name DNS
```

Zonen:

```
Get-DnsServerZone
```

Bestimmte Zone:

```
Get-DnsServerZone `
  -Name "example.test"
```

Datensätze:

```
Get-DnsServerResourceRecord `
  -ZoneName "example.test"
```

Serverstatistiken:

```
Get-DnsServerStatistics
```

Verfügbare Leistungsindikatoren:

```
Get-Counter -ListSet DNS
```

Zu prüfen sind:

- Dienststatus;
- geladene und angehaltene Zonen;
- primäre, sekundäre, Stub- oder AD-integrierte Zone;
- Replikationsbereich;
- dynamische Updates;
- Zonentransfer;
- Serverfehler;
- Rekursionsfehler;
- Abfragerate;
- CPU, Speicher und Netzwerk;
- Unterschiede zwischen DNS-Servern.

Ein laufender DNS-Dienst beweist nicht, dass eine bestimmte Zone korrekt geladen oder repliziert wurde.

7.12.32 Active-Directory-DNS prüfen

LDAP-SRV-Einträge:

```
Resolve-DnsName `
  -Name "_ldap._tcp.dc._msdcs.<AD-DNS-Domäne>" `
```

```
  -Type SRV
```

Kerberos-SRV-Einträge:

```
Resolve-DnsName `
  -Name "_kerberos._tcp.<AD-DNS-Domäne>" `
  -Type SRV
```

DNS-Test eines Domänencontrollers:

```
dcdiag /test:DNS /v /s:<DC-Name>
```

Replikationsübersicht:

```
repadmin /replsummary
```

Replikationsdetails:

```
repadmin /showrepl
```

Zu prüfen sind:

- verwendet der Client ausschließlich vorgesehene AD-DNS-Server?
- existieren die benötigten SRV-Einträge?
- sind die SRV-Zielhosts über A oder AAAA auflösbar?
- sind die veröffentlichten Dienste erreichbar?
- existiert die Zone auf allen vorgesehenen DNS-Servern?
- funktioniert AD-Replikation?
- stimmen Standort- und Subnetzzuordnung?
- liefern verschiedene DCs unterschiedliche Antworten?

Eine manuelle Neuerstellung von SRV-Einträgen ist keine erste Maßnahme. Zuerst müssen Registrierung, Netlogon, Zone, Berechtigungen und Replikation geprüft werden.

7.12.33 Dynamische Updates und DHCP prüfen

Vor einer erneuten Registrierung sind vorhandene Datensätze, Zeitstempel und Ereignisse zu dokumentieren.

Verändernde Clientregistrierung:

```
Register-DnsClient
```

Alternativ:

```
ipconfig /registerdns
```

Zu prüfen sind:

- Existenz der Forward- und Reverse-Zone;
- erlaubte Aktualisierungsart;
- sichere dynamische Updates;
- Client- oder DHCP-Verantwortung;
- DHCP-Lease;
- DNS-Optionen des DHCP-Bereichs;
- Aktualisierung von A- und PTR-Einträgen;
- Datensatzeigentümer;
- Berechtigungen;
- statische Altbestände;
- DHCP-Failover;
- DNS- und DHCP-Ereignisse.

Das wiederholte Registrieren behebt keine fehlende Zone, falsche Berechtigung oder fehlerhafte DHCP-DNS-Konfiguration.

7.12.34 Aging und Scavenging prüfen

Zu prüfen sind:

- Aging-Einstellung der Zone;
- Scavenging-Einstellung des Servers;
- No-Refresh-Intervall;
- Refresh-Intervall;
- Scavenging-Zyklus;
- Zeitstempel des Datensatzes;
- statischer oder dynamischer Eintrag;
- DHCP-Leasezeit;
- Zeitpunkt der letzten Aktualisierung;
- unerwartet gelöschte Datensätze.

Scavenging beinhaltet Löschvorgänge und darf nicht spontan aktiviert oder erzwungen werden, um einzelne veraltete Einträge zu beseitigen.

7.12.35 Ereignisse und Protokolle auswerten

Vorhandene DNS-Protokolle unter Windows anzeigen:

```
Get-WinEvent -ListLog "*DNS*"
```

Mögliche Bereiche:

- DNS-Client-Protokolle;
- DNS-Server-Audit-Protokoll;
- DNS-Server-Analytical-Protokoll;
- Systemprotokoll;
- DHCP-Serverprotokoll;
- Verzeichnisdienstprotokoll;
- anwendungsspezifische Protokolle.

Zu korrelieren sind:

- genauer Zeitpunkt;
- Clientadresse;
- Abfragename;
- Datensatztyp;
- Antwortcode;
- verwendeter Server;
- dynamische Aktualisierung;
- Zonenladen;
- Replikation;
- DNSSEC;
- DoH;
- Dienststart oder Dienstfehler.

Analytische DNS-Protokollierung muss gezielt und zeitlich begrenzt aktiviert werden. Sie kann bei hohen Abfrageraten die Leistung beeinflussen und enthält schützenswerte interne Namensinformationen.

7.12.36 Netzwerkaufzeichnung gezielt einsetzen

Eine Netzwerkaufzeichnung ist sinnvoll, wenn unklar bleibt:

- ob die Abfrage den Client verlässt;
- welcher DNS-Server angesprochen wird;
- ob eine Antwort zurückkommt;
- ob Wiederholungen stattfinden;
- ob UDP oder TCP verwendet wird;
- ob die UDP-Antwort abgeschnitten ist;
- ob anschließend TCP verwendet wird;
- ob Fragmentierung oder Paketverlust auftritt;

- wie lang die Antwort tatsächlich benötigt;
- ob der Client zu einem anderen DNS-Server wechselt.

Bei DoH und DoT ist der DNS-Inhalt verschlüsselt. Sichtbar bleiben unter anderem Zieladresse, Port, TLS-Verbindung und Zeitverhalten, nicht jedoch ohne Weiteres der eigentliche DNS-Nachrichteninhalt.

Aufzeichnungen müssen auf die betroffenen Systeme, Namen und Zeiträume begrenzt sowie geschützt gespeichert werden.

7.12.37 Hypothese und Gegenbeweis formulieren

Beispiel:

```
Hypothese:
Der erste konfigurierte DNS-Forwarder ist nicht erreichbar und verursacht die Verzögerung.

Erwarteter Befund:
Direkte Abfragen gegen den ersten Forwarder laufen in einen Timeout.
Direkte Abfragen gegen den zweiten Forwarder funktionieren sofort.

Gegenbeweis:
Der erste Forwarder antwortet unter denselben Bedingungen schnell und korrekt.
```

Eine belastbare Hypothese enthält:

- vermutete Ursache;
- erwarteten messbaren Befund;
- möglichen Gegenbeweis;
- Testmethode;
- Erfolgskriterium;
- Risiko des Tests.

Erst danach sollte eine Änderung vorgenommen werden.

7.12.38 Kontrollierte Maßnahmen

Maßnahme	Voraussetzung	Risiko
DNS-Serveradresse korrigieren	falscher Resolver nachgewiesen	andere Namensräume können beeinflusst werden
Suffix oder NRPT-Regel korrigieren	falscher Abfrageweg nachgewiesen	VPN- und Split-DNS-Verhalten ändert sich

Maßnahme	Voraussetzung	Risiko
DNS-Datensatz korrigieren	autoritative Daten sind nachweislich falsch	Anwendungen können auf neues Ziel wechseln
PTR-Eintrag korrigieren	falscher Reverse-Eintrag bestätigt	Protokoll- oder Sicherheitszuordnung ändert sich
Forwarder korrigieren	nicht erreichbarer oder falscher Forwarder bestätigt	externe oder interne Rekursion betroffen
Delegation korrigieren	falsche NS- oder Glue-Daten bestätigt	gesamte Zone kann betroffen sein
dynamische Updates korrigieren	Updatefehler und Berechtigung nachgewiesen	viele Clients können Einträge verändern
Cache kontrolliert löschen	falscher Cacheeintrag dokumentiert	Beweisdaten gehen verloren
DNSSEC-Konfiguration korrigieren	Validierungsfehler nachgewiesen	Vertrauenskette und Sicherheit betroffen
Aging oder Scavenging anpassen	Fehlkonfiguration nachgewiesen	gültige Datensätze können gelöscht werden
Replikationsfehler beheben	AD-Replikationsfehler bestätigt	mehrere Verzeichnisdaten betroffen

Vor der Maßnahme sind zu dokumentieren:

- Ausgangszustand;
- betroffene Systeme und Zonen;
- Berechtigung;
- Risiko;
- Rückweg;
- Erfolgskriterium;
- vorgesehenes Testverfahren.

7.12.39 Vollständiger Diagnoseablauf

1. **Exakte Fehlermeldung aufnehmen**
   Wortlaut, Anwendung, Benutzer, Client und Uhrzeit dokumentieren.
2. **Betroffenen Namen bestimmen**
   Kurzname, FQDN oder IP-Adresse unterscheiden.
3. **Erwarteten Datensatztyp bestimmen**
   A, AAAA, CNAME, PTR, SRV, MX, TXT, NS oder SOA festlegen.
4. **Erwartetes Ergebnis dokumentieren**
   Vorgesehene IP-Adresse, Zielname oder Dienstinformation festhalten.
5. **Umfang bestimmen**
   Einzelnen Client, Standort, DNS-Server, Namen, Zone oder alle Systeme unterscheiden.
6. **Anwendung und DNS abgrenzen**
   Direkte IP-Verbindung, Systemresolver und Anwendung getrennt prüfen.
7. **Netzwerkzustand erfassen**
   Schnittstelle, Adresse, Gateway, VPN und Routing dokumentieren.

8. **Konfigurierte DNS-Server erfassen**
   DNS-Server pro Schnittstelle und Reihenfolge bestimmen.
9. **Suffixe und lokale Namensquellen prüfen**
   Suchliste, Hosts-Datei und Anwendungscache berücksichtigen.
10. **Resolverrichtlinien prüfen**
    NRPT, Split-DNS, Container-DNS und Sicherheitsresolver berücksichtigen.
11. **Verschlüsselten DNS-Pfad bestimmen**
    Klassisches DNS, DoH und DoT unterscheiden.
12. **Normale Systemauflösung testen**
    Prüfen, welches Ergebnis die Anwendung grundsätzlich erhalten kann.
13. **Direkte Abfrage durchführen**
    Vorgesehenen DNS-Server und Datensatztyp ausdrücklich angeben.
14. **Antwortcode auswerten**
    `NOERROR`, `NXDOMAIN`, `SERVFAIL`, `REFUSED` oder Timeout unterscheiden.
15. **Antwortinhalt auswerten**
    Wert, TTL, CNAME-Kette und Flags prüfen.
16. **Antwortzeit messen**
    Erste und wiederholte Abfrage vergleichen.
17. **Alternativen DNS-Server prüfen**
    Unterschiede zwischen vorgesehenen Resolvern dokumentieren.
18. **Cachezustand prüfen**
    Positive und negative Einträge auf allen relevanten Ebenen berücksichtigen.
19. **UDP und TCP vergleichen**
    Transportabhängige Fehler bestimmen.
20. **EDNS, MTU und Fragmentierung prüfen**
    Besonders bei großen Antworten oder VPN-Verbindungen.
21. **Rekursiven und autoritativen Server unterscheiden**
    Abfrageweg in einzelne Ebenen zerlegen.
22. **SOA, NS und Delegation prüfen**
    Zuständigkeit und Zonengrenze bestätigen.
23. **Autoritative Server direkt vergleichen**
    Datensatz, TTL, Seriennummer und Antwortcode auswerten.
24. **Forwarder und Rekursion prüfen**
    Erreichbarkeit, Richtlinien und Timeoutpfad untersuchen.
25. **DNSSEC prüfen**
    Signaturen, DS, DNSKEY, Trust Anchor und Validierungsfehler berücksichtigen.
26. **Reverse-Lookup prüfen**
    PTR, Reverse-Zone, Delegation und Vorwärtskonsistenz auswerten.
27. **DNS-Serverzustand prüfen**
    Dienst, Zonen, Statistiken, Last und Ereignisse untersuchen.
28. **AD-DNS und Replikation prüfen**
    Wenn AD-integrierte Zonen oder SRV-Einträge beteiligt sind.
29. **Dynamische Updates und DHCP prüfen**
    Registrierung, Eigentümer, Berechtigungen und Leasezustand auswerten.
30. **Aging und Scavenging prüfen**
    Bei veralteten oder unerwartet fehlenden Einträgen.

31. **Protokolle korrelieren**
    Client, DNS-Server, DHCP und Anwendung auf denselben Versuch begrenzen.
32. **Bei Bedarf Netzwerkaufzeichnung durchführen**
    Nur zeitlich und technisch begrenzt.
33. **Hypothese und Gegenbeweis formulieren**
    Ursache vor der Änderung messbar beschreiben.
34. **Eine kontrollierte Maßnahme ausführen**
    Risiko, Rückweg und Erfolgskriterium beachten.
35. **Identischen Test wiederholen**
    Antwortcode, Wert und Zeit mit dem Ausgangszustand vergleichen.
36. **Alternativen Pfad erneut prüfen**
    Weitere Clients, Resolver oder autoritative Server kontrollieren.
37. **Anwendung verifizieren**
    Nicht nur das Diagnosewerkzeug testen.
38. **Temporäre Änderungen zurücknehmen**
    Logging, Testregeln und Ausnahmen entfernen.
39. **Ursache dokumentieren**
    Technischen Nachweis und betroffenen Pfad festhalten.
40. **Prävention festlegen**
    Monitoring, Standardisierung oder Konfigurationsverbesserung umsetzen.

7.12.40 Befundmatrix

Befund	Mögliche Einordnung	Nächster Nachweis
IP-Verbindung funktioniert, Name nicht	DNS oder lokaler Resolverpfad	direkte A-/AAAA-Abfrage
direkter DNS-Test funktioniert, Anwendung nicht	Anwendungscache, Proxy oder eigener Resolver	Anwendungsresolver und Zieladresse prüfen
nur Kurzname schlägt fehl	Suffix- oder Suchlistenproblem	FQDN und Suffixkonfiguration vergleichen
nur ein Client betroffen	lokale Konfiguration, Cache oder Hosts-Datei	anderen Client und direkte Serverabfrage vergleichen
nur ein DNS-Server betroffen	Zone, Cache, Dienst oder Replikation	DNS-Server direkt vergleichen
ganze Zone liefert `NXDOMAIN`	falscher Resolver oder fehlende Delegation	SOA, NS und autoritative Server prüfen
`NOERROR`, aber keine A-Antwort	Name vorhanden, Datensatztyp fehlt	CNAME, AAAA und SOA prüfen
`SERVFAIL`	Rekursion, DNSSEC oder Serverfehler	autoritative Abfrage und Protokolle
`REFUSED`	Richtlinie, ACL oder deaktivierte Rekursion	Serverkonfiguration und Quellnetz prüfen
Timeout	fehlende Antwort	Transport, Netzwerk und Serverlast prüfen

Befund	Mögliche Einordnung	Nächster Nachweis
UDP schlägt fehl, TCP funktioniert	Firewall, MTU, Fragmentierung oder EDNS	Netzwerkaufzeichnung und große Antwort prüfen
erste Abfrage langsam, zweite schnell	Cacheeffekt	kalte und warme Abfrage vergleichen
externe Namen langsam	Forwarder oder Rekursion	Forwarder direkt prüfen
interne Namen langsam	interne Delegation, Forwarder oder AD-DNS	interne autoritative Server prüfen
mit VPN falsche Antwort	NRPT oder Split-DNS	Resolver vor und nach VPN vergleichen
Browser und System liefern verschiedene Antworten	Browser-DoH oder Anwendungscache	Browserresolver und Systemresolver vergleichen
PTR fehlt, A funktioniert	Reverse-Zone oder PTR fehlt	Reverse-Delegation prüfen
unterschiedliche Antworten je DC	AD-Replikation	`repadmin` und direkte DNS-Abfragen
nur große Antworten scheitern	EDNS-, MTU- oder Fragmentierungsproblem	UDP/TCP-Vergleich
nur signierte Zonen scheitern	DNSSEC-Validierungsfehler	DS-, DNSKEY- und EDE-Auswertung
neuer Datensatz bleibt unsichtbar	positiver oder negativer Cache	TTL und Cacheebenen prüfen
SRV vorhanden, Dienst nicht erreichbar	Zielhost, Port oder Dienst fehlerhaft	SRV-Ziel und Dienstport prüfen

---

7.12.41 Typische Diagnosefehler

- Fehlermeldung nicht vollständig dokumentieren.
- Kurzname und FQDN verwechseln.
- Den benötigten Datensatztyp nicht bestimmen.
- `ping` als vollständigen DNS-Test verwenden.
- Einen erfolgreichen Ping als Nachweis des Dienstes betrachten.
- Nur `nslookup` verwenden.
- NRPT mit `nslookup` prüfen.
- Anwendung und direkten DNS-Test gleichsetzen.
- Den tatsächlich verwendeten DNS-Server nicht bestimmen.
- Öffentlichen DNS-Server auf einem Domänenclient eintragen.
- Cache vor der Beweissicherung löschen.
- `NXDOMAIN`, `NODATA`, `SERVFAIL` und Timeout gleich behandeln.
- Nur den Antwortcode, aber nicht den Antwortinhalt prüfen.
- Nur den Antwortwert, aber nicht TTL und Quelle prüfen.
- Rekursiven und autoritativen DNS-Server verwechseln.
- Nur einen DNS-Server testen.
- UDP und TCP nicht getrennt prüfen.
- TCP-Port `53` als UDP-Nachweis verwenden.
- EDNS, MTU und Fragmentierung ignorieren.

- DoH oder DoT über einen klassischen DNS-Test als funktionsfähig bewerten.
- DNSSEC allein mit `nslookup` prüfen.
- `+dnssec` als vollständigen Validierungsnachweis interpretieren.
- Öffentliche `+trace`-Abfrage für eine interne Split-DNS-Zone verwenden.
- CNAME-, MX- oder SRV-Zielnamen nicht weiter auflösen.
- Erfolgreichen SRV-Lookup mit erreichbarem Dienst gleichsetzen.
- PTR-Fehler als vollständigen DNS-Ausfall bewerten.
- Forwarder verändern, ohne ihr Verhalten direkt zu testen.
- DNS-Dienst vorsorglich neu starten.
- Zone vorsorglich neu erstellen.
- Einträge löschen, ohne Eigentümer, TTL und Replikation zu prüfen.
- Scavenging unkontrolliert aktivieren.
- AD-Replikationsfehler durch manuelle DNS-Änderungen verdecken.
- Pro Diagnoseversuch mehrere Variablen verändern.
- Nur das Diagnosewerkzeug, aber nicht die Anwendung verifizieren.
- Temporäre Logging- oder Firewalländerungen aktiv lassen.

7.12.42 Verifikation

Nach einer Maßnahme müssen mindestens folgende Punkte geprüft werden:

- Client besitzt eine gültige Netzwerkkonfiguration;
- vorgesehene DNS-Server sind eingetragen;
- richtige Schnittstelle und VPN-Regel werden verwendet;
- Suffixe und Suchliste sind korrekt;
- Hosts-Datei enthält keinen widersprüchlichen Eintrag;
- NRPT und Split-DNS funktionieren wie vorgesehen;
- DoH oder DoT funktioniert, sofern vorgesehen;
- exakter FQDN wird korrekt aufgelöst;
- benötigter Datensatztyp ist vorhanden;
- Antwortcode ist korrekt;
- Antwortwert entspricht dem Sollzustand;
- TTL ist plausibel;
- rekursive und autoritative Antworten sind konsistent;
- alle vorgesehenen DNS-Server liefern den richtigen Wert;
- UDP und TCP funktionieren;
- DNSSEC-Validierung funktioniert, sofern vorgesehen;
- Vorwärts- und Rückwärtsauflösung stimmen überein, sofern erforderlich;
- SRV-, MX- und CNAME-Ziele sind vollständig auflösbar;
- AD-SRV-Einträge sind vorhanden;
- AD-Replikation ist fehlerfrei;
- dynamische Aktualisierung funktioniert, sofern vorgesehen;
- keine neuen DNS-, DHCP- oder Replikationsfehler entstehen;
- Antwortzeit entspricht der Baseline;
- ursprüngliche Anwendung funktioniert;

- weitere repräsentative Clients funktionieren;
- temporäre Diagnoseänderungen wurden zurückgenommen;
- Ursache, Maßnahme und Prävention wurden dokumentiert.

Eine einzelne erfolgreiche Cacheabfrage ist keine ausreichende Verifikation.

7.12.43 Dokumentationsvorlage

```
Störung:
<exakte Beschreibung>

Zeitpunkt:
<Datum und Uhrzeit>

Betroffener Client:
<Hostname und IP-Adresse>

Betroffene Anwendung:
<Anwendung oder Dienst>

Abfragename:
<FQDN oder IP-Adresse>

Datensatztyp:
<A, AAAA, CNAME, PTR, SRV, MX, TXT, NS oder SOA>

Erwartetes Ergebnis:
<Sollwert>

Tatsächliches Ergebnis:
<Istwert, Antwortcode und Antwortzeit>

Verwendeter Resolver:
<DNS-Server und Schnittstelle>

Resolverpfad:
<klassisches DNS, NRPT, VPN, DoH, DoT oder Anwendungsresolver>

Vergleichstests:
<anderer Client, DNS-Server, Transport oder autoritativer Server>
```

```
Nachgewiesene Ursache:
<technischer Befund>

Gegenbeweis ausgeschlossen durch:
<Test und Ergebnis>

Durchgeführte Maßnahme:
<genau eine kontrollierte Änderung>

Risiko und Rückweg:
<Beschreibung>

Verifikation:
<identischer Test, Anwendungstest und weitere Systeme>

Präventionsmaßnahme:
<Monitoring, Standardisierung oder Konfigurationsänderung>
```

7.12.44 Checkliste

- [ ] exakte Fehlermeldung dokumentiert
- [ ] Datum und Uhrzeit erfasst
- [ ] betroffenen Client erfasst
- [ ] betroffene Anwendung erfasst
- [ ] Kurzname, FQDN und IP-Adresse unterschieden
- [ ] benötigten Datensatztyp bestimmt
- [ ] erwartetes Ergebnis dokumentiert
- [ ] Fehlerumfang bestimmt
- [ ] aktive Netzwerkschnittstelle geprüft
- [ ] IP-Adresse und Gateway geprüft
- [ ] VPN-Zustand dokumentiert
- [ ] konfigurierte DNS-Server erfasst
- [ ] DNS-Serverreihenfolge geprüft
- [ ] DNS-Suffixe und Suchliste geprüft
- [ ] Hosts-Datei geprüft
- [ ] Anwendungscache berücksichtigt

- [ ] NRPT geprüft
- [ ] Split-DNS berücksichtigt
- [ ] DoH oder DoT berücksichtigt
- [ ] normalen Systemresolver getestet
- [ ] direkte DNS-Abfrage durchgeführt
- [ ] DNS-Server ausdrücklich angegeben
- [ ] Antwortcode dokumentiert
- [ ] Antwortinhalt dokumentiert
- [ ] TTL dokumentiert
- [ ] Antwortflags berücksichtigt
- [ ] Antwortzeit gemessen
- [ ] erste und wiederholte Abfrage verglichen
- [ ] positiven Cache geprüft
- [ ] negativen Cache geprüft
- [ ] alternativen DNS-Server getestet
- [ ] UDP getestet
- [ ] TCP getestet
- [ ] EDNS und MTU berücksichtigt
- [ ] rekursiven Server bestimmt
- [ ] autoritativen Server bestimmt
- [ ] SOA geprüft
- [ ] NS-Einträge geprüft
- [ ] Delegation geprüft
- [ ] autoritative Server direkt verglichen
- [ ] Forwarder geprüft
- [ ] bedingte Forwarder geprüft
- [ ] Rekursion geprüft
- [ ] A- und AAAA-Einträge geprüft
- [ ] CNAME-Kette geprüft
- [ ] SRV- oder MX-Ziele bei Bedarf geprüft
- [ ] Reverse-Lookup geprüft
- [ ] DNSSEC bei Bedarf geprüft
- [ ] DNS-Serverdienst geprüft
- [ ] Zonenstatus geprüft

- [ ] Serverstatistiken geprüft
- [ ] Serverlast geprüft
- [ ] DNS-Ereignisse ausgewertet
- [ ] AD-SRV-Einträge bei Bedarf geprüft
- [ ] AD-Replikation bei Bedarf geprüft
- [ ] dynamische Updates bei Bedarf geprüft
- [ ] DHCP-DNS-Aktualisierung bei Bedarf geprüft
- [ ] Aging und Scavenging bei Bedarf geprüft
- [ ] Hypothese formuliert
- [ ] Gegenbeweis festgelegt
- [ ] Risiko und Rückweg dokumentiert
- [ ] nur eine kontrollierte Maßnahme durchgeführt
- [ ] identischen Test wiederholt
- [ ] ursprüngliche Anwendung getestet
- [ ] weitere repräsentative Systeme geprüft
- [ ] temporäre Änderungen zurückgenommen
- [ ] Ursache und Prävention dokumentiert

7.12.45 Schnellreferenz

Aufgabe	Befehl
Windows-Netzwerkkonfiguration	`Get-NetIPConfiguration`
vollständige Windows-IP-Konfiguration	`ipconfig /all`
Windows-DNS-Serveradressen	`Get-DnsClientServerAddress`
Windows-DNS-Clientkonfiguration	`Get-DnsClient`
Linux-Resolverzustand	`resolvectl status`
macOS-Resolverzustand	`scutil --dns`
wirksame NRPT-Richtlinie	`Get-DnsClientNrptPolicy`
konfigurierte NRPT-Regeln	`Get-DnsClientNrptRule`
verschlüsselter DNS-Clientzustand	`netsh dnsclient show state`
verschlüsselte DNS-Endpunkte	`netsh dnsclient show encryption`
Systemauflösung unter Windows	`Resolve-DnsName <Name>`
direkte A-Abfrage	`Resolve-DnsName <Name> -Type A -Server <DNS-IP> -DnsOnly`
direkte AAAA-Abfrage	`Resolve-DnsName <Name> -Type AAAA -Server <DNS-IP> -DnsOnly`

Aufgabe	Befehl
CNAME prüfen	`Resolve-DnsName <Name> -Type CNAME -Server <DNS-IP> -DnsOnly`
SRV prüfen	`Resolve-DnsName <SRV-Name> -Type SRV -Server <DNS-IP> -DnsOnly`
PTR prüfen	`Resolve-DnsName <IP> -Type PTR -Server <DNS-IP> -DnsOnly`
SOA prüfen	`Resolve-DnsName <Zone> -Type SOA -Server <DNS-IP> -DnsOnly`
NS prüfen	`Resolve-DnsName <Zone> -Type NS -Server <DNS-IP> -DnsOnly`
direkte Abfrage mit `dig`	`dig @<DNS-IP> <Name> <Typ>`
Reverse-Abfrage mit `dig`	`dig @<DNS-IP> -x <IP>`
öffentliche Delegation verfolgen	`dig <Name> <Typ> +trace`
TCP-DNS unter Windows	`Resolve-DnsName <Name> -Server <DNS-IP> -DnsOnly -TcpOnly`
TCP-DNS mit `dig`	`dig @<DNS-IP> <Name> <Typ> +tcp`
DNSSEC-Daten anfordern	`dig @<DNS-IP> <Name> <Typ> +dnssec`
Windows-Clientcache	`Get-DnsClientCache`
Windows-DNS-Dienst	`Get-Service DNS`
Windows-DNS-Zonen	`Get-DnsServerZone`
Windows-DNS-Datensätze	`Get-DnsServerResourceRecord -ZoneName <Zone>`
Windows-DNS-Forwarder	`Get-DnsServerForwarder`
Windows-DNS-Rekursion	`Get-DnsServerRecursion`
Windows-DNS-Statistiken	`Get-DnsServerStatistics`
DNS-Leistungsindikatoren	`Get-Counter -ListSet DNS`
vorhandene Windows-DNS-Protokolle	`Get-WinEvent -ListLog "*DNS*"`
AD-DNS-Test	`dcdiag /test:DNS /v /s:<DC-Name>`
AD-Replikationsübersicht	`repadmin /replsummary`
AD-Replikationsdetails	`repadmin /showrepl`

Ändernde Befehle, die nicht als erste Diagnose verwendet werden dürfen:

```
Clear-DnsClientCache
Clear-DnsServerCache
Register-DnsClient
ipconfig /flushdns
ipconfig /registerdns
Set-DnsClientServerAddress
```

```
Set-DnsServerForwarder
Set-DnsServerRecursion
Set-DnsServerCache
Set-DnsServerZoneAging
Start-DnsServerScavenging
Add-DnsServerPrimaryZone
Add-DnsServerResourceRecord
Remove-DnsServerResourceRecord
Restart-Service DNS
```

7.12.46 Quellen

Offizielle Microsoft-Dokumentation

- Microsoft Learn – Guidance for troubleshooting DNS
- Microsoft Learn – Troubleshooting DNS clients
- Microsoft Learn – Troubleshooting DNS servers
- Microsoft Learn – Troubleshoot DNS client name resolution issues
- Microsoft Learn – Troubleshoot DNS name resolution on the Internet
- Microsoft Learn – DNS queries and lookups
- Microsoft Learn – DNS architecture
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – DnsClient PowerShell module
- Microsoft Learn – DnsServer PowerShell module
- Microsoft Learn – Test-NetConnection
- Microsoft Learn – Best practices for DNS client settings
- Microsoft Learn – Forwarders and conditional forwarders resolution timeouts
- Microsoft Learn – Dynamic DNS Update in Windows and Windows Server
- Microsoft Learn – DNS scavenging setup
- Microsoft Learn – Enable DNS logging and diagnostics
- Microsoft Learn – Validate and secure DNS responses using DNSSEC
- Microsoft Learn – Secure DNS Client over HTTPS
- Microsoft Learn – DNS encryption using DNS over HTTPS
- Microsoft Learn – netsh dnsclient
- Microsoft Learn – Dcdiag
- Microsoft Learn – Verify DNS functionality to support directory replication

Offizielle Projektdokumentation

- ISC BIND 9 – dig manual page
- ISC BIND 9 – Troubleshooting
- systemd – resolvectl
- systemd – systemd-resolved

Standards

- RFC 1034 – Domain Names: Concepts and Facilities
- RFC 1035 – Domain Names: Implementation and Specification
- RFC 2308 – Negative Caching of DNS Queries
- RFC 4033 – DNS Security Introduction and Requirements
- RFC 4035 – Protocol Modifications for DNS Security Extensions
- RFC 6891 – Extension Mechanisms for DNS
- RFC 7766 – DNS Transport over TCP
- RFC 7858 – DNS over Transport Layer Security
- RFC 8484 – DNS Queries over HTTPS
- RFC 8499 – DNS Terminology
- RFC 8914 – Extended DNS Errors
- RFC 9520 – Negative Caching of DNS Resolution Failures

Für diese Seite wurden keine Community-Berichte, Hersteller-Social-Media-Aussagen oder eigenen Laborergebnisse als Nachweis verwendet.
