7.7 Netzwerk oder Anwendung ist langsam

1. Ziel dieser Seite

Die Meldung „Das Netzwerk ist langsam“ beschreibt zunächst nur die Wahrnehmung des Benutzers. Die tatsächliche Ursache kann unter anderem im Client, im Netzwerk, auf dem Server, im Storage, in der Datenbank oder in der Anwendung liegen.

Diese Seite zeigt, wie ein Leistungsproblem systematisch eingegrenzt wird.

Ziel ist die Unterscheidung zwischen:

- langsamem Client,
- langsamem Netzwerk,
- hoher Latenz,
- Paketverlust,
- geringer verfügbarer Bandbreite,
- ausgelastetem WLAN,
- langsamem VPN,
- überlastetem Server,
- hoher Storage-Latenz,
- blockierter Datenbank,
- langsamem DNS,
- fehlerhaftem Serverknoten,
- Anwendungs- oder Schnittstellenproblem.

---

2. „Langsam“ messbar beschreiben

Ungeeignet:

```
Das Netzwerk ist langsam.
```

Besser:

```
Das Öffnen einer 20-MB-Datei vom Dateiserver dauert seit 09:30 Uhr
ungefähr 45 Sekunden. Normalerweise dauert es weniger als 5 Sekunden.
Betroffen sind drei Benutzer im zweiten Obergeschoss.
Internetseiten und das Standardgateway reagieren normal.
```

Zu erfassen sind:

- genaue Benutzeraktion,

- betroffene Anwendung,
- betroffene Datei oder Funktion,
- Startzeitpunkt,
- Dauer,
- Häufigkeit,
- betroffene Benutzer,
- betroffene Clients,
- Standort,
- LAN, WLAN oder VPN,
- internes oder externes Ziel,
- erwartete Dauer,
- tatsächlich gemessene Dauer,
- Fehlermeldungen,
- durchgeführte Änderungen.

Beispiel

Merkmal	Beobachtung
Aktion	Öffnen einer Datei vom Dateiserver
Dateigröße	20 MB
Normalzustand	3 bis 5 Sekunden
aktueller Zustand	40 bis 50 Sekunden
Beginn	seit ungefähr 09:30 Uhr
Betroffene	drei Benutzer
Standort	zweites Obergeschoss
Verbindung	WLAN
Internet	normal
Gateway	normal erreichbar
Dateiserver	hohe Antwortzeit

Erst durch einen solchen Vergleich wird aus einer subjektiven Meldung ein messbares Problem.

---

3. Wichtige Leistungsbegriffe unterscheiden

Begriff	Bedeutung
Latenz	Zeit, die ein Datenpaket oder eine Anfrage bis zur Antwort benötigt
Paketverlust	Anteil der Pakete, die ihr Ziel nicht erreichen
Bandbreite	theoretisch oder technisch verfügbare Übertragungskapazität

Begriff	Bedeutung
Durchsatz	tatsächlich übertragene Datenmenge pro Zeiteinheit
Jitter	Schwankung der Laufzeit aufeinanderfolgender Pakete
Antwortzeit	gesamte Dauer einer Anfrage aus Benutzersicht
IOPS	Anzahl der Ein- und Ausgabeoperationen eines Speichers pro Sekunde
Storage-Latenz	Wartezeit einer Speicheroperation
CPU-Auslastung	Anteil der aktuell verwendeten Prozessorleistung
Arbeitsspeicherauslastung	Belegung des physischen Arbeitsspeichers
Warteschlange	Anforderungen, die auf Verarbeitung oder Übertragung warten
Retransmission	erneute Übertragung verlorener oder nicht bestätigter TCP-Daten
Applikationslatenz	Zeit, welche die Anwendung für die Verarbeitung benötigt

Eine schnelle Netzwerkverbindung garantiert keinen hohen Anwendungsdurchsatz.

Beispiel

```
Verbindungsgeschwindigkeit: 1 Gbit/s
tatsächlicher Dateidurchsatz: 8 Mbit/s
```

Die angezeigte Verbindungsgeschwindigkeit beschreibt nur die ausgehandelte Verbindung. Sie beweist nicht, dass die gesamte Strecke oder das Zielsystem diese Datenrate bereitstellen kann.

---

4. Mögliche Ursachenbereiche

```
Benutzeraktion
    ↓
Client
    ↓
lokale Verbindung
    ↓
Switch, WLAN oder VPN
    ↓
Routing, Firewall oder WAN
    ↓
Server
```

```
    ↓
Anwendung
    ↓
Datenbank oder Storage
```

Eine Verzögerung kann an jeder Stelle dieser Kette entstehen.

Client

- hohe CPU-Auslastung,
- unzureichender Arbeitsspeicher,
- langsamer Datenträger,
- Hintergrundprogramme,
- Virenscanner,
- fehlerhafter Netzwerktreiber,
- Energiesparmodus,
- Browsererweiterungen,
- lokaler DNS-Cache,
- defekte Netzwerkkarte.

Netzwerk

- Paketverlust,
- hohe Latenz,
- Interface-Fehler,
- Duplex- oder Geschwindigkeitsproblem,
- ausgelasteter Uplink,
- Queue Drops,
- fehlerhaftes Kabel,
- überlastetes WLAN,
- Roaming,
- VPN-Überlastung,
- MTU-Problem,
- fehlerhaftes Routing,
- langsame Namensauflösung.

Server

- hohe CPU-Auslastung,
- zu wenig Arbeitsspeicher,
- Paging oder Swapping,
- hohe Storage-Latenz,
- volle Datenträger,
- überlastete Netzwerkschnittstelle,
- zu viele gleichzeitige Sitzungen,

- blockierte Prozesse,
- Virenscan,
- Backup,
- Snapshot,
- überlasteter Hypervisor.

Anwendung und Datenbank

- langsame Datenbankabfrage,
- fehlender Datenbankindex,
- Datenbanksperre,
- erschöpfter Verbindungspool,
- langsame API,
- externer Dienst,
- fehlerhafter Serverknoten,
- Anwendungsfehler,
- ungeeignete Zeitüberschreitung,
- große oder ineffiziente Abfrage,
- überlastete Hintergrundverarbeitung.

---

5. Zuerst den Umfang bestimmen

Zu klären ist:

1. Ist nur ein Benutzer betroffen?
2. Sind mehrere Benutzer betroffen?
3. Ist nur ein Standort betroffen?
4. Sind nur WLAN-Benutzer betroffen?
5. Sind auch kabelgebundene Clients betroffen?
6. Ist nur eine Anwendung langsam?
7. Sind mehrere Dienste desselben Servers betroffen?
8. Sind interne und externe Ziele betroffen?
9. Tritt das Problem zu einer bestimmten Uhrzeit auf?
10. Tritt es nur bei einer bestimmten Datenmenge auf?

Schnelle Eingrenzung

Beobachtung	Wahrscheinlicher Prüfbereich
nur ein Client betroffen	Client, Treiber, Kabel, WLAN oder lokale Software
mehrere Clients gleichzeitig betroffen	gemeinsame Infrastruktur oder zentraler Dienst
nur ein Standort betroffen	Standortanbindung, Switch, WLAN oder WAN
nur WLAN betroffen	Funkstrecke, Access Point, Kanal oder Roaming
LAN und WLAN betroffen	gemeinsamer Netzwerkpfad, Server oder Anwendung

Beobachtung	Wahrscheinlicher Prüfbereich
nur eine Anwendung betroffen	Anwendung, Datenbank, API oder Sitzung
mehrere Dienste eines Servers betroffen	Server, Betriebssystem, Storage oder Hypervisor
alle internen Dienste langsam	Netzwerk, DNS, Firewall oder zentrale Infrastruktur
nur Internet langsam	WAN, Provider, Proxy oder externe Ziele
nur große Dateien langsam	Durchsatz, Paketverlust, Storage oder Übertragungsweg
kleine Anfragen bereits langsam	Latenz, DNS, Anwendung oder Datenbank

---

6. Vergleich mit einer funktionierenden Referenz

Ein Vergleichssystem sollte möglichst ähnlich sein:

- gleicher Standort,
- gleiches Netzwerk,
- gleiche Anwendung,
- gleiche Berechtigung,
- gleiche Datenmenge,
- gleicher Server,
- ähnliche Hardware,
- möglichst gleicher Zeitpunkt.

Beispiel

Prüfung	betroffener Client	Vergleichsclient
Gateway-Latenz	2 ms	2 ms
Server-Latenz	3 ms	3 ms
Dateiübertragung	4 MB/s	85 MB/s
CPU-Auslastung	15 %	20 %
Datenträgerauslastung	100 %	8 %

In diesem Beispiel ist der Netzwerkpfad zunächst unauffällig. Die lokale Datenträgerauslastung des betroffenen Clients ist dagegen auffällig.

---

7. Baseline festlegen

Ein Messwert ist nur aussagekräftig, wenn bekannt ist, welcher Wert normalerweise erreicht wird.

Beispiel

```
Normale Antwortzeit:       200 bis 400 ms
Aktuelle Antwortzeit:      4 bis 8 Sekunden
Normale Dateiübertragung:  80 bis 95 MB/s
Aktuelle Übertragung:      5 bis 12 MB/s
Normale Storage-Latenz:    2 bis 8 ms
Aktuelle Storage-Latenz:   80 bis 250 ms
```

Mögliche Baselines:

- Antwortzeit einer Anwendung,
- Laufzeit einer Datenbankabfrage,
- Ping-Latenz,
- Paketverlust,
- DNS-Antwortzeit,
- Dateidurchsatz,
- CPU-Auslastung,
- Speicherauslastung,
- Storage-Latenz,
- Anzahl gleichzeitiger Sitzungen,
- Fehlerrate,
- Warteschlangenlänge.

Messungen sollten möglichst unter vergleichbaren Bedingungen erfolgen.

---

8. Lokalen Client prüfen

Unter Windows:

```
Get-Process |
    Sort-Object CPU -Descending |
    Select-Object -First 10 Name, CPU, WorkingSet
```

Netzwerkadapter anzeigen:

```
Get-NetAdapter |
    Format-Table Name, Status, LinkSpeed, InterfaceDescription
```

Adapterstatistiken:

```
Get-NetAdapterStatistics
```

Aktuelle IP-Konfiguration:

```
ipconfig /all
```

Unter Linux:

```
top
```

Alternativ, sofern installiert:

```
htop
```

Arbeitsspeicher:

```
free -h
```

Datenträgerbelegung:

```
df -h
```

Netzwerkschnittstellen:

```
ip link show
```

Statistiken:

```
ip -s link show
```

Zu prüfen sind:

- CPU-Spitzen,
- Speicherdruck,
- Paging oder Swapping,
- Datenträgerauslastung,
- Hintergrundprozesse,
- Synchronisationsprogramme,
- Virenscanner,
- Softwareupdates,
- Treiberstatus,

- ausgehandelte Verbindungsgeschwindigkeit,
- Interface-Fehler,
- Energiesparzustände.

Ein ausgelasteter Client kann eine langsame Anwendung verursachen, obwohl Netzwerk und Server ordnungsgemäß arbeiten.

---

9. Latenz und Paketverlust messen

Unter Windows:

```
ping -t <ziel>
```

Beispiel:

```
ping -t 192.0.2.10
```

Unter Linux oder macOS:

```
ping <ziel>
```

Es sollten mehrere Ziele verglichen werden:

```
Client → Standardgateway
Client → interner Server
Client → externes Referenzziel
```

Auswertung

Gateway	interner Server	externes Ziel	Mögliche Eingrenzung
langsam	langsam	langsam	Clientzugang oder lokales Netzwerk
normal	langsam	normal	interner Pfad oder Servernetz
normal	normal	langsam	WAN, Provider oder externer Pfad
normal	normal	normal	Anwendung, Port, Serverprozess oder Datenbank

Gateway	interner Server	externes Ziel	Mögliche Eingrenzung
Paketverlust	Paketverlust	Paketverlust	lokale Verbindung oder gemeinsamer Uplink

Ping prüft ICMP-Erreichbarkeit. Eine normale Ping-Antwort beweist nicht, dass die Anwendung schnell arbeitet.

---

10. Netzwerkpfad untersuchen

Unter Windows:

```
tracert <ziel>
```

Unter Linux:

```
traceroute <ziel>
```

Unter macOS:

```
traceroute <ziel>
```

Falls vorhanden, kann eine fortlaufende Pfadanalyse durchgeführt werden:

```
mtr <ziel>
```

Zu prüfen sind:

- auffällige Latenzsprünge,
- wechselnde Pfade,
- Paketverlust,
- Routingänderungen,
- Unterschiede zwischen betroffenen und funktionierenden Clients.

Ein Router muss ICMP-Antworten nicht mit derselben Priorität wie weitergeleiteten Verkehr behandeln. Ein auffälliger Zwischenknoten allein beweist deshalb noch keinen Fehler. Entscheidend ist, ob die Beeinträchtigung auch an nachfolgenden Zielen sichtbar bleibt.

---

11. TCP-Port getrennt prüfen

Unter Windows:

```
Test-NetConnection <server> -Port <port>
```

Beispiel:

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

Weitere Beispiele:

```
Test-NetConnection webserver.example.local -Port 443
```

```
Test-NetConnection dbserver.example.local -Port 1433
```

Unter Linux oder macOS, sofern Netcat vorhanden ist:

```
nc -vz <server> <port>
```

Beispiel:

```
nc -vz webserver.example.local 443
```

Damit wird geprüft, ob der TCP-Verbindungsaufbau möglich ist. Die tatsächliche Antwortzeit der Anwendung wird dadurch noch nicht vollständig gemessen.

---

12. Anwendungsantwort mit curl messen

Gesamte Antwortzeit:

```
curl \
    -o /dev/null \
    -s \
    -w "DNS: %{time_namelookup}\nTCP: %{time_connect}\nTLS: %{time_appconnect}\nErstes Byte: %{time_starttransfer}\nGesamt: %{time_total}\n" \
    https://example.com/
```

Beispielausgabe:

```
DNS:         0.012
TCP:         0.028
TLS:         0.071
Erstes Byte: 3.842
Gesamt:      3.901
```

Interpretation:

- DNS langsam: Namensauflösung untersuchen,
- TCP langsam: Netzwerkpfad oder Zielsystem prüfen,
- TLS langsam: Zertifikatsprüfung, Proxy oder Serverlast prüfen,
- erstes Byte langsam: Anwendung, Server oder Datenbank prüfen,
- Download nach dem ersten Byte langsam: Durchsatz oder Datenmenge prüfen.

Vergleich

```
DNS:         0,012 Sekunden
TCP:         0,028 Sekunden
TLS:         0,071 Sekunden
Erstes Byte: 3,842 Sekunden
```

Das Netzwerk baut die Verbindung schnell auf. Die lange Wartezeit bis zum ersten Byte weist eher auf die Verarbeitung im Zielsystem hin.

---

13. DNS-Antwortzeit prüfen

Unter Windows:

```
Measure-Command {
   Resolve-DnsName <hostname>
}
```

Einzelne DNS-Abfrage:

```
Resolve-DnsName <hostname>
```

Unter Linux oder macOS, sofern `dig` vorhanden ist:

```
dig <hostname>
```

Kurze Ausgabe:

```
dig <hostname> +stats
```

Zu prüfen sind:

- Antwortzeit,
- verwendeter DNS-Server,
- unterschiedliche Antworten,
- Zeitüberschreitungen,
- fehlerhafte Weiterleitung,
- IPv4- und IPv6-Verhalten,
- Suchdomänen,
- Split-DNS,
- mehrere Zieladressen.

Beispiel

```
Aufruf über IP-Adresse:  0,4 Sekunden
Aufruf über Hostnamen:   5,2 Sekunden
```

Dieser Unterschied weist auf die Namensauflösung hin. Er beweist noch nicht, welcher DNS-Server oder welche DNS-Konfiguration die Verzögerung verursacht.

---

14. Durchsatz messen

Für eine kontrollierte Netzwerkmessung kann `iperf3` verwendet werden. Dafür wird auf einem autorisierten Zielsystem ein `iperf3`-Server benötigt.

Server:

```
iperf3 -s
```

Client:

```
iperf3 -c <server-ip>
```

Messung in Gegenrichtung:

```
iperf3 -c <server-ip> -R
```

Mehrere parallele Verbindungen:

```
iperf3 -c <server-ip> -P 4
```

UDP-Tests dürfen nur kontrolliert und mit begrenzter Bandbreite durchgeführt werden:

```
iperf3 -c <server-ip> -u -b 10M
```

Zu vergleichen sind:

- Senderichtung,
- Empfangsrichtung,
- LAN,
- WLAN,
- VPN,
- betroffener Client,
- Referenzclient,
- verschiedene Zeitpunkte.

Wichtig

Ein unkontrollierter Durchsatztest kann produktive Verbindungen beeinträchtigen. Zielsystem, Testdauer und erzeugte Last müssen abgestimmt sein.

---

15. Dateitransfer richtig bewerten

Ein Dateitransfer misst nicht ausschließlich das Netzwerk.

Beteiligt sind:

```
Quelldatenträger
    ↓
Quellsystem
    ↓
Netzwerk
    ↓
Zielsystem
    ↓
Zieldatenträger
```

Mögliche Begrenzungen:

- langsamer Quelldatenträger,
- langsamer Zieldatenträger,
- Virenscanner,
- Dateisystem,
- Verschlüsselung,
- SMB- oder NFS-Konfiguration,
- viele kleine Dateien,
- Kompression,
- CPU-Auslastung,
- Netzwerkdurchsatz,
- Storage-Latenz.

Beispiel

```
Eine Datei mit 10 GB:          80 MB/s
100.000 sehr kleine Dateien:    8 MB/s
```

Viele kleine Dateien erzeugen wesentlich mehr Verwaltungs- und Speicheroperationen. Die niedrigere Übertragungsrate beweist deshalb nicht automatisch ein Netzwerkproblem.

---

16. Interface-Fehler und Drops prüfen

Unter Windows:

```
Get-NetAdapterStatistics
```

Unter Linux:

```
ip -s link show
```

Auf einem verwalteten Switch müssen die herstellerspezifischen Diagnosebefehle verwendet werden.

Zu beobachten sind:

- CRC-/FCS-Fehler,
- Input Errors,
- Output Errors,
- Discards,
- Queue Drops,
- Interface Resets,
- Kollisionen,

- Link-Flaps,
- Geschwindigkeits- und Duplexaushandlung.

Zähler müssen als Verlauf betrachtet werden.

Beispiel

```
09:00 Uhr:  15 CRC-Fehler
09:30 Uhr:  15 CRC-Fehler
10:00 Uhr:  15 CRC-Fehler
```

Der Zähler steigt nicht. Die Fehler können aus einem früheren Zeitraum stammen.

```
09:00 Uhr:    15 CRC-Fehler
09:30 Uhr:   280 CRC-Fehler
10:00 Uhr: 4.500 CRC-Fehler
```

Der Zähler nimmt aktuell zu und weist auf ein Problem des physischen Übertragungswegs hin.

---

17. Duplex und Verbindungsgeschwindigkeit prüfen

Mögliche Symptome:

- geringer Durchsatz,
- hohe Anzahl von Fehlern,
- Kollisionen,
- stark unterschiedliche Sende- und Empfangsleistung,
- Verbindung handelt nur 100 Mbit/s statt 1 Gbit/s aus.

Zu prüfen sind:

- Clientadapter,
- Switchport,
- Kabelkategorie,
- Stecker,
- Dockingstation,
- Medienkonverter,
- Transceiver,
- automatische Aushandlung.

Geschwindigkeit und Duplex dürfen nicht wahllos fest eingestellt werden. Beide Seiten müssen zusammenpassen und die Änderung muss dokumentiert sowie freigegeben sein.

---

18. WLAN-Leistung untersuchen

Bei WLAN-Verbindungen sind zusätzlich zu betrachten:

- Signalstärke,
- Signal-Rausch-Abstand,
- Kanalauslastung,
- Retry-Rate,
- verwendetes Frequenzband,
- Kanalbreite,
- Anzahl aktiver Clients,
- Airtime,
- Roaming,
- Access-Point-Auslastung,
- DFS-Kanalwechsel,
- Störquellen,
- AP-Uplink,
- PoE-Versorgung.

Unter Windows:

```
netsh wlan show interfaces
```

WLAN-Bericht:

```
netsh wlan show wlanreport
```

Wichtiger Vergleich:

Test	LAN	WLAN	Eingrenzung
Anwendung	schnell	langsam	WLAN oder Access Point
Anwendung	langsam	langsam	gemeinsamer Pfad, Server oder Anwendung
nur ein WLAN-Client langsam	–	betroffen	Client, Treiber, Standort oder Funkband
alle Clients eines AP langsam	–	betroffen	Access Point, Kanal, Uplink oder PoE

Ein hoher angezeigter WLAN-Verbindungswert entspricht nicht automatisch dem tatsächlichen Nutzdurchsatz.

---

19. VPN-Verbindung untersuchen

Mögliche Ursachen:

- hohe Internetlatenz,
- Paketverlust,
- überlastetes VPN-Gateway,
- Verschlüsselungslast,
- ungeeignete MTU,
- getunnelter Internetverkehr,
- langsamer DNS-Server,
- geografische Entfernung,
- WLAN-Probleme des Benutzers,
- Bandbreitenbegrenzung,
- Neuaufbau des Tunnels.

Zu vergleichen sind:

```
ohne VPN → internes Testziel, sofern autorisiert erreichbar
mit VPN  → internes Testziel
mit VPN  → Standardgateway des lokalen Netzes
mit VPN  → VPN-Gateway
```

Außerdem sollte geprüft werden:

- betrifft es alle VPN-Benutzer,
- betrifft es nur einen Internetanbieter,
- tritt es nur zu bestimmten Zeiten auf,
- ist nur eine Anwendung betroffen,
- sind Senden und Empfangen unterschiedlich langsam,
- steigt die CPU-Auslastung des VPN-Gateways,
- treten Tunnelabbrüche oder Neuverbindungen auf.

VPN- oder Sicherheitsfunktionen dürfen nicht zur Diagnose umgangen werden.

---

20. Serverressourcen prüfen

Wichtige Messwerte:

- CPU-Auslastung,
- CPU-Warteschlange,
- Arbeitsspeicher,
- Paging oder Swapping,
- Datenträgerauslastung,
- Storage-Latenz,
- freie Speicherkapazität,

- Netzwerkauslastung,
- aktive Sitzungen,
- Prozessanzahl,
- Container- oder VM-Grenzen,
- Hypervisor-Auslastung.

Unter Linux:

```
uptime
```

```
free -h
```

```
df -h
```

```
top
```

Falls installiert:

```
vmstat 1
```

```
iostat -xz 1
```

Unter Windows können Task-Manager, Ressourcenmonitor, Leistungsüberwachung und PowerShell verwendet werden.

Beispiel für Prozesse mit hoher CPU-Zeit:

```
Get-Process |
    Sort-Object CPU -Descending |
    Select-Object -First 10 Name, CPU, WorkingSet
```

Ein einzelner aktueller Messwert reicht bei sporadischen Problemen nicht aus. Die Werte müssen während der tatsächlichen Verzögerung aufgezeichnet werden.

---

21. CPU-Auslastung richtig interpretieren

Eine hohe CPU-Auslastung kann auf einen Engpass hinweisen, muss aber im Zusammenhang betrachtet werden.

Zu prüfen sind:

- Gesamtauslastung,
- Auslastung einzelner Kerne,
- Prozess mit hoher CPU-Nutzung,
- Laufzeit der hohen Last,
- Warteschlangen,
- virtuelle CPU-Zuteilung,
- CPU-Limits von Containern,
- Steal Time bei virtuellen Systemen,
- thermische Drosselung.

Beispiel

```
Gesamtauslastung: 35 %
Anwendungsprozess: ein Prozesskern dauerhaft bei 100 %
```

Eine nicht ausreichend parallelisierte Anwendung kann bereits durch einen vollständig ausgelasteten Kern begrenzt werden, obwohl die Gesamtauslastung unauffällig wirkt.

---

22. Arbeitsspeicher und Paging prüfen

Hohe Speicherbelegung allein beweist keinen Fehler. Betriebssysteme nutzen freien Arbeitsspeicher häufig als Cache.

Wichtiger sind:

- verfügbarer Arbeitsspeicher,
- Paging oder Swapping,
- Speicherdruck,
- Speicherwachstum eines Prozesses,
- Out-of-Memory-Ereignisse,
- Container- oder VM-Limits,
- wiederholte Prozessabbrüche.

Typische Wirkung

```
Arbeitsspeicher reicht nicht aus
        ↓
Auslagerung auf Datenträger
        ↓
Storage-Latenz steigt
        ↓
```

```
Anwendung reagiert langsam
```

Deshalb müssen Arbeitsspeicher- und Storage-Messwerte gemeinsam betrachtet werden.

---

23. Storage-Latenz untersuchen

Eine hohe Datenträgerauslastung bedeutet nicht automatisch einen hohen Datendurchsatz. Viele kleine oder zufällige Operationen können einen Datenträger vollständig auslasten.

Zu prüfen sind:

- Lese- und Schreiblatenz,
- Warteschlangentiefe,
- IOPS,
- Durchsatz,
- freie Kapazität,
- Dateisystem,
- RAID-Zustand,
- Controllerzustand,
- Cache,
- SAN- oder NAS-Verbindung,
- Snapshots,
- Replikation,
- Backup,
- Virenscan,
- Thin Provisioning,
- Storage-Überbelegung.

Beispiel

```
Netzwerkauslastung:  12 %
CPU-Auslastung:      30 %
Storage-Latenz:     180 ms
Anwendungsantwort:    8 s
```

Die niedrige Netzwerkauslastung spricht gegen einen reinen Bandbreitenengpass. Die hohe Storage-Latenz ist dagegen auffällig.

Hersteller- und betriebssystemspezifische Grenzwerte müssen anhand der jeweiligen Dokumentation und des normalen Betriebszustands bewertet werden.

---

24. Datenbank als Ursache untersuchen

Mögliche Ursachen:

- langsame Abfrage,
- fehlender Index,
- Datenbanksperre,
- Deadlock,
- zu viele gleichzeitige Verbindungen,
- erschöpfter Verbindungspool,
- hohe Storage-Latenz,
- Statistik- oder Wartungsproblem,
- große Ergebnismenge,
- ungeeigneter Ausführungsplan,
- Replikationsverzögerung.

Zu vergleichen sind:

- Dauer der Benutzeranfrage,
- Dauer der zugehörigen Datenbankabfrage,
- Wartezeiten,
- Sperren,
- Anzahl aktiver Verbindungen,
- CPU- und Storage-Auslastung,
- Zeitpunkt von Wartungsaufgaben,
- Verhalten vergleichbarer Abfragen.

Beispiel

```
TCP-Verbindung zum Webserver:      20 ms
Antwort des Webservers:             6 s
Datenbankabfrage:                   5,7 s
```

Das Netzwerk ist in diesem Beispiel nicht der größte Zeitanteil. Die Datenbankabfrage bestimmt nahezu die gesamte Antwortzeit.

Produktive Abfragen dürfen nicht unkontrolliert wiederholt oder verändert werden. Datenbankdiagnosen müssen mit den vorgesehenen Werkzeugen und Berechtigungen erfolgen.

---

25. Anwendungs- und API-Abhängigkeiten prüfen

Eine Anwendung kann von mehreren Diensten abhängig sein:

```
Client
  ↓
```

```
Webanwendung
  ↓
Authentifizierungsdienst
  ↓
API
  ↓
Datenbank
  ↓
Storage
```

Zu prüfen sind:

- Antwortzeit jeder Abhängigkeit,
- externe APIs,
- Authentifizierungsdienst,
- Verzeichnisdienst,
- DNS,
- Proxy,
- Nachrichtenwarteschlange,
- Datenbank,
- Storage,
- Cache,
- Rate Limits,
- Zeitüberschreitungen.

Beispiel

```
Anwendung selbst:        100 ms
externe API:           4.800 ms
Gesamtantwort:         5.100 ms
```

Aus Benutzersicht ist die Anwendung langsam. Die eigentliche Verzögerung entsteht jedoch bei einer externen API.

---

26. Load Balancer und mehrere Serverknoten prüfen

Bei verteilten Anwendungen kann nur ein einzelner Knoten langsam sein.

Beispiel

Zielknoten	Antwortzeit
Webserver 1	250 ms

Zielknoten	Antwortzeit
Webserver 2	230 ms
Webserver 3	8.400 ms
Zugriff über Load Balancer	wechselnd zwischen schnell und langsam

Mögliche Ursachen des einzelnen Knotens:

- andere Konfiguration,
- fehlerhafte Softwareversion,
- hohe CPU-Auslastung,
- langsames Storage,
- fehlerhaftes Zertifikat,
- fehlende Verbindung zur Datenbank,
- defekter Cache,
- Hintergrundprozess,
- ungleiche Lastverteilung.

Alle Knoten müssen einzeln verglichen werden. Ein gelegentlich langsamer Zugriff über den Load Balancer kann entstehen, wenn nur ein Teil der Anfragen an den fehlerhaften Knoten gelangt.

---

27. Zeitgesteuerte Last berücksichtigen

Leistungsprobleme können regelmäßig mit anderen Prozessen zusammenfallen:

- Backup,
- Snapshot,
- Replikation,
- Virenscan,
- Softwareverteilung,
- Update,
- Datenimport,
- Export,
- Berichterstellung,
- Indexierung,
- Datenbankwartung,
- Logrotation,
- Cloud-Synchronisation.

Beispiel

```
02:00:00 Backup startet
02:00:12 Storage-Latenz steigt
02:00:18 Datenbankabfragen werden langsamer
```

```
02:00:25 Anwendung überschreitet Zeitlimit
02:20:00 Backup endet
02:20:15 Storage-Latenz normalisiert sich
```

Eine gemeinsame Zeitleiste zeigt die mögliche Abhängigkeit.

Der zeitliche Zusammenhang ist ein Hinweis. Die Ursache muss durch Messwerte und gegebenenfalls eine kontrollierte Änderung bestätigt werden.

---

28. Paketmitschnitt gezielt einsetzen

Ein Paketmitschnitt kann unter anderem zeigen:

- TCP-Retransmissions,
- Verbindungsabbrüche,
- verzögerte Bestätigungen,
- DNS-Zeitüberschreitungen,
- lange Pausen zwischen Anfrage und Antwort,
- wiederholte Verbindungsaufbauten,
- TCP-Zero-Window-Ereignisse,
- TLS-Verbindungsaufbau,
- unterschiedliche Serverziele.

Beispiel mit `dumpcap`:

```
dumpcap \
  -i 1 \
  -f "host 192.0.2.45" \
  -b duration:300 \
  -b files:12 \
  -w langsame-anwendung.pcapng
```

Dabei gelten folgende Regeln:

- Mitschnitt autorisieren lassen,
- richtige Schnittstelle auswählen,
- Capture-Filter begrenzen,
- Speicherbedarf begrenzen,
- Datenschutz berücksichtigen,
- Zeitpunkt des Problems dokumentieren,
- Mitschnitt nach der Diagnose beenden,
- Dateien geschützt speichern,
- Dateien anschließend geregelt löschen.

Ein Mitschnitt auf dem Client zeigt nicht automatisch alle Pakete anderer Systeme oder Netzwerksegmente.

---

29. TCP-Retransmissions bewerten

TCP überträgt verlorene Daten erneut. Viele erneute Übertragungen können den Durchsatz erheblich reduzieren.

Mögliche Ursachen:

- Paketverlust,
- fehlerhaftes Kabel,
- WLAN-Störungen,
- überlastete Warteschlangen,
- WAN-Probleme,
- fehlerhafter Netzwerkadapter,
- MTU-Problem,
- überlastetes Zielsystem.

Vereinfachtes Beispiel

```
Datenpaket wird gesendet
        ↓
Paket geht verloren
        ↓
Bestätigung bleibt aus
        ↓
TCP wartet
        ↓
Daten werden erneut übertragen
```

Die Bandbreite kann technisch hoch sein, während der tatsächlich nutzbare Durchsatz durch Paketverlust stark sinkt.

---

30. Ursache und Wartezeit trennen

Eine langsame Anwendung kann in verschiedene Zeitanteile zerlegt werden.

Beispiel

Verarbeitungsschritt	Dauer
DNS-Auflösung	20 ms

Verarbeitungsschritt	Dauer
TCP-Verbindungsaufbau	25 ms
TLS-Verbindungsaufbau	70 ms
Webserververarbeitung	180 ms
Datenbankabfrage	4.800 ms
Übertragung der Antwort	90 ms
Gesamtdauer	5.185 ms

Die Datenbankabfrage beansprucht den größten Teil der Gesamtdauer.

Dadurch kann die Diagnose auf den Bereich mit dem größten Zeitanteil konzentriert werden.

---

31. Mehrere Systeme auf einer Zeitleiste vergleichen

Zeit	Client	Netzwerk	Server	Storage	Anwendung
09:59:50	normal	normal	normal	4 ms	300 ms
10:00:00	Anfrage startet	normal	CPU 40 %	8 ms	400 ms
10:00:05	wartet	normal	CPU 45 %	170 ms	5 s
10:00:10	wartet	normal	CPU 48 %	240 ms	10 s
10:00:15	Antwort	normal	CPU 42 %	12 ms	normal

In diesem Beispiel steigen die Netzwerklatenz und CPU-Auslastung nicht auffällig. Die Storage-Latenz steigt dagegen zeitgleich mit der langsamen Anwendung.

---

32. Hypothese messbar formulieren

Ungeeignet:

```
Der Server ist wahrscheinlich überlastet.
```

Besser:

```
Wenn die Anwendung erneut länger als fünf Sekunden benötigt,
steigt vermutlich gleichzeitig die Storage-Latenz des Datenbankservers
auf mehr als 100 ms.
```

Prüfung:

```
Anwendungsantwortzeit messen
Storage-Latenz aufzeichnen
Datenbankwartezeiten erfassen
Zeitstempel vergleichen
```

Eine gute Hypothese enthält:

- konkrete Komponente,
- erwarteten Messwert,
- erwartete Veränderung,
- Zeitfenster,
- Möglichkeit der Widerlegung.

---

33. Kontrollierte Änderung durchführen

Erst nach ausreichender Eingrenzung wird genau eine Änderung vorgenommen.

Mögliche Änderungen:

- defektes Kabel ersetzen,
- vorgesehenen Treiber aktualisieren,
- fehlerhaften Switchport wechseln,
- ungeeignete Sicherungszeit verschieben,
- fehlerhaften Serverknoten aus der Verteilung nehmen,
- abgestimmte Bandbreitensteuerung einrichten,
- Datenbankabfrage optimieren,
- fehlenden Index nach Prüfung ergänzen,
- Ressourcenlimit korrigieren,
- defekten Datenträger oder Access Point ersetzen.

Ungeeignet:

```
Treiber aktualisieren, Kabel ersetzen, DNS ändern und Server neu starten.
```

Wenn mehrere Änderungen gleichzeitig durchgeführt werden, kann die wirksame Maßnahme nicht mehr eindeutig bestimmt werden.

---

34. Rollback festlegen

Vor jeder Änderung dokumentieren:

- ursprüngliche Konfiguration,

- ursprüngliche Version,
- Ausgangsmesswerte,
- verantwortliche Person,
- Änderungsfenster,
- erwartete Wirkung,
- Abbruchkriterium,
- Rückweg.

Beispiel

Änderung:

Fehlerhaften Webserver 3 kontrolliert aus dem Load Balancer nehmen.

Erwartung:

Die wechselnden Antwortzeiten verschwinden.

Rollback:

Webserver 3 mit der ursprünglichen Gewichtung wieder aufnehmen.

Abbruchkriterium:

Verbleibende Knoten überschreiten die zulässige Auslastung.

---

35. Verifikation

Nach der Änderung müssen dieselben Messungen wie vorher wiederholt werden.

Zu prüfen sind:

- ursprüngliche Benutzeraktion,
- Antwortzeit,
- Latenz,
- Paketverlust,
- Durchsatz,
- Fehlerzähler,
- CPU-Auslastung,
- Arbeitsspeicher,
- Storage-Latenz,
- Datenbankwartezeit,
- Protokolle,
- Nebenwirkungen,
- Verhalten abhängiger Systeme.

Beispiel

```
Vorher:
Antwortzeit:       6 bis 12 Sekunden
Storage-Latenz:    120 bis 260 ms
Fehlerhäufigkeit:  20 bis 30 Ereignisse pro Stunde

Nachher:
Antwortzeit:       250 bis 400 ms
Storage-Latenz:    3 bis 8 ms
Fehlerhäufigkeit:  0 Ereignisse in 48 Stunden
```

Ein einzelner erfolgreicher Test reicht nicht aus, wenn das Problem vorher nur gelegentlich auftrat.

---

36. Beispiel „Netzwerk angeblich langsam“

Symptom

Mehrere Benutzer melden, dass das Öffnen von Kundendatensätzen am Vormittag mehrere Sekunden dauert.

Erste Messungen

```
Gateway-Latenz:            1 ms
Webserver-Latenz:          2 ms
Paketverlust:              0 %
TCP-Verbindungsaufbau:     20 ms
Zeit bis zum ersten Byte:  7 s
```

Servermessungen

```
CPU-Auslastung:            35 %
Arbeitsspeicher:           unauffällig
Netzwerkauslastung:        10 %
Storage-Latenz:            6 ms
```

Datenbankmessung

```
Abfragedauer:              6,7 s
Warteursache:              Datenbanksperre
```

Festgestellte Ursache

Ein zeitgleich laufender Import hielt eine Datenbanksperre. Netzwerk und Webserver waren nicht die Ursache.

Kontrollierte Maßnahme

Der Importprozess wurde nach Prüfung so angepasst, dass die Sperre kürzer gehalten wird.

Verifikation

```
Antwortzeit:              300 bis 450 ms
Paketverlust:             weiterhin 0 %
Datenbanksperren:         keine auffällige Wartezeit
Import:                   weiterhin erfolgreich
```

---

37. Beispiel „Dateiserver ist langsam“

Symptom

Ein Benutzer erreicht beim Kopieren großer Dateien nur ungefähr 8 MB/s.

Vergleich

Messung	betroffener Client	Referenzclient
Verbindung	1 Gbit/s	1 Gbit/s
Ping zum Server	2 ms	2 ms
`iperf3`	920 Mbit/s	925 Mbit/s
Dateiübertragung	8 MB/s	90 MB/s
lokale Datenträgerauslastung	100 %	15 %

Festgestellte Ursache

Der lokale Zieldatenträger des betroffenen Clients war der Engpass. Die Netzwerkverbindung erreichte im kontrollierten Durchsatztest einen normalen Wert.

Lehre

```
Ein langsamer Dateitransfer ist nicht automatisch ein langsames Netzwerk.
```

---

38. Beispiel „WLAN ist langsam“

Symptom

Benutzer in einem Besprechungsraum melden am Nachmittag langsame Anwendungen und Videokonferenzen.

Vergleich

```
LAN:                        normal
WLAN außerhalb des Raums:   normal
WLAN im Besprechungsraum:   langsam
```

Messwerte

```
Signalstärke:               ausreichend
Kanalauslastung:            sehr hoch
Retry-Rate:                 stark erhöht
aktive Clients:             42
AP-Uplink:                  unauffällig
```

Festgestellte Ursache

Der Funkkanal war stark ausgelastet. Viele erneute Übertragungen reduzierten den tatsächlichen Durchsatz.

Kontrollierte Maßnahme

Die Funkplanung wurde anhand der vorgesehenen WLAN-Managementfunktionen angepasst.

Verifikation

```
Retry-Rate:                 deutlich reduziert
Anwendungsantwortzeit:      normal
Videokonferenzen:           stabil
```

---

39. Ungeeignete Sofortmaßnahmen

Nicht als erste Maßnahme verwenden:

- Server ohne vorherige Messung neu starten,
- Netzwerkgerät wahllos neu starten,
- DNS-Cache vor der Bestandsaufnahme löschen,
- alle Netzwerkadapter zurücksetzen,

- mehrere Kabel und Ports gleichzeitig wechseln,
- Sicherheitssoftware ohne Freigabe deaktivieren,
- VPN umgehen,
- Firewallregeln pauschal ändern,
- WLAN-Kanäle wahllos wechseln,
- unbegrenzten Paketmitschnitt starten,
- produktives Netzwerk unkontrolliert auslasten,
- Datenbankabfragen ungeprüft verändern,
- Serverressourcen ohne Messwerte erhöhen,
- Zeitüberschreitungen pauschal verlängern,
- aus einem einzelnen Ping eine Ursache ableiten,
- hohe Bandbreite mit hoher Anwendungsleistung gleichsetzen.

Solche Maßnahmen können Beweise vernichten, neue Fehler verursachen oder die eigentliche Ursache verdecken.

---

40. Vollständige Prüfreihenfolge

1. genaue Benutzeraktion erfassen.
2. erwartete und tatsächliche Dauer dokumentieren.
3. Startzeitpunkt, Häufigkeit und Dauer bestimmen.
4. betroffene Benutzer, Clients und Standorte erfassen.
5. LAN, WLAN und VPN unterscheiden.
6. einzelne Anwendung und allgemeines Systemverhalten vergleichen.
7. betroffenen Client mit Referenzclient vergleichen.
8. normalen Leistungsbereich als Baseline bestimmen.
9. lokale CPU-, Speicher- und Datenträgerauslastung prüfen.
10. Verbindungsgeschwindigkeit und Adapterstatus prüfen.
11. Gateway, internes Ziel und externes Ziel messen.
12. Latenz und Paketverlust getrennt betrachten.
13. Netzwerkpfad untersuchen.
14. TCP-Port prüfen.
15. DNS-Antwortzeit messen.
16. Anwendungsantwort in einzelne Zeitanteile zerlegen.
17. kontrollierten Durchsatztest durchführen.
18. Interface-Fehler, Drops und Retransmissions prüfen.
19. WLAN-Auslastung und Retry-Rate berücksichtigen.
20. VPN-Pfad und VPN-Gateway prüfen.
21. Server-CPU und Arbeitsspeicher überwachen.
22. Paging, Swapping und Ressourcenlimits prüfen.
23. Storage-Latenz und Warteschlangen untersuchen.
24. Datenbankabfragen, Sperren und Verbindungen prüfen.
25. APIs und externe Abhängigkeiten untersuchen.
26. alle Serverknoten einzeln vergleichen.
27. geplante Aufgaben und Hintergrundprozesse prüfen.

28. Messwerte auf einer gemeinsamen Zeitleiste darstellen.
29. größten Zeitanteil bestimmen.
30. Ursache und Folge unterscheiden.
31. genau eine messbare Hypothese formulieren.
32. Ausgangszustand und Rollback dokumentieren.
33. genau eine freigegebene Änderung durchführen.
34. ursprüngliche Messung wiederholen.
35. ausreichend lange Verifikation durchführen.
36. Nebenwirkungen kontrollieren.
37. temporäre Diagnosemaßnahmen entfernen.
38. Ursache, Maßnahme und Nachweis dokumentieren.

---

41. Checkliste „Netzwerk oder Anwendung ist langsam“

- [ ] genaue Benutzeraktion wurde dokumentiert.
- [ ] erwartete Dauer wurde erfasst.
- [ ] tatsächliche Dauer wurde gemessen.
- [ ] Zeitpunkt und Häufigkeit wurden dokumentiert.
- [ ] betroffene Benutzer wurden bestimmt.
- [ ] betroffene Clients wurden bestimmt.
- [ ] betroffene Standorte wurden bestimmt.
- [ ] LAN, WLAN und VPN wurden unterschieden.
- [ ] interner und externer Zugriff wurden verglichen.
- [ ] betroffener Client wurde mit einer Referenz verglichen.
- [ ] Baseline wurde bestimmt.
- [ ] lokale CPU-Auslastung wurde geprüft.
- [ ] lokaler Arbeitsspeicher wurde geprüft.
- [ ] lokaler Datenträger wurde geprüft.
- [ ] Hintergrundprozesse wurden geprüft.
- [ ] Verbindungsgeschwindigkeit wurde geprüft.
- [ ] Adapterstatistiken wurden geprüft.
- [ ] Gateway-Latenz wurde gemessen.
- [ ] Server-Latenz wurde gemessen.
- [ ] Paketverlust wurde geprüft.
- [ ] Netzwerkpfad wurde untersucht.
- [ ] TCP-Port wurde geprüft.
- [ ] DNS-Antwortzeit wurde gemessen.

- [ ] Zeit bis zum ersten Byte wurde gemessen.
- [ ] tatsächlicher Durchsatz wurde geprüft.
- [ ] beide Übertragungsrichtungen wurden berücksichtigt.
- [ ] Interface-Fehler wurden geprüft.
- [ ] Drops und Discards wurden geprüft.
- [ ] TCP-Retransmissions wurden berücksichtigt.
- [ ] WLAN-Kanalauslastung wurde geprüft.
- [ ] WLAN-Retry-Rate wurde geprüft.
- [ ] VPN-Verbindung wurde berücksichtigt.
- [ ] Server-CPU wurde überwacht.
- [ ] Serverarbeitsspeicher wurde überwacht.
- [ ] Paging oder Swapping wurde geprüft.
- [ ] Storage-Latenz wurde gemessen.
- [ ] Datenträgerwarteschlangen wurden berücksichtigt.
- [ ] Datenbankabfragen wurden geprüft.
- [ ] Datenbanksperren wurden berücksichtigt.
- [ ] APIs und externe Abhängigkeiten wurden geprüft.
- [ ] alle Serverknoten wurden verglichen.
- [ ] Backups und Snapshots wurden berücksichtigt.
- [ ] Virenscans und Updates wurden berücksichtigt.
- [ ] gemeinsame Zeitleiste wurde erstellt.
- [ ] größter Zeitanteil wurde bestimmt.
- [ ] Ursache und Folge wurden unterschieden.
- [ ] messbare Hypothese wurde formuliert.
- [ ] Ausgangszustand wurde dokumentiert.
- [ ] Rollback wurde festgelegt.
- [ ] nur eine kontrollierte Änderung wurde durchgeführt.
- [ ] Messungen wurden anschließend wiederholt.
- [ ] ausreichend lange Verifikation wurde durchgeführt.
- [ ] Nebenwirkungen wurden geprüft.
- [ ] Ursache und Nachweis wurden dokumentiert.

---

42. Schnellreferenz

Beobachtung	Nächster Prüfbereich

nur ein Client langsam	Client, Treiber, Datenträger oder lokale Software
alle Clients langsam	gemeinsame Infrastruktur, Server oder Anwendung
Gateway bereits langsam	lokaler Zugang, WLAN, Kabel oder Switch
Gateway normal, Server langsam	interner Pfad, Servernetz oder Server
Ping normal, Anwendung langsam	Anwendung, Datenbank, API oder Storage
DNS langsam	DNS-Server, Weiterleitung oder Namensauflösung
TCP-Aufbau langsam	Netzwerkpfad, Firewall oder Zielsystem
erstes Byte langsam	Server, Anwendung oder Datenbank
Download nach erstem Byte langsam	Durchsatz, Paketverlust oder Datenmenge
`iperf3` schnell, Dateiübertragung langsam	Datenträger, Dateisystem, Virenscanner oder Protokoll
CRC-/FCS-Fehler steigen	Kabel, Stecker, Port oder Transceiver
Output Drops steigen	Auslastung oder nachgelagerter Engpass
nur WLAN langsam	Funkkanal, Retry-Rate, Roaming oder Access Point
nur VPN langsam	Internetpfad, VPN-Gateway, MTU oder Verschlüsselung
nur ein Serverknoten langsam	Konfiguration oder Ressource dieses Knotens
CPU dauerhaft hoch	Prozess, Last oder unzureichende Rechenleistung
CPU unauffällig, Storage-Latenz hoch	Storage, Backup, Snapshot oder Datenträger
Speicherdruck und Paging	Arbeitsspeicher, Prozess oder Ressourcenlimit
Anwendung während Backup langsam	Storage-, Netzwerk- und CPU-Auslastung vergleichen
Fehler nur bei großen Datenmengen	Durchsatz, Paketverlust, Storage oder Zeitlimit
Fehler nur bei vielen kleinen Dateien	IOPS, Dateisystem und Virenscanner
Monitoring zeigt nichts	Messintervall, Maximum und kurzfristige Spitzen prüfen

---

Merksatz

> „Langsam“ ist zunächst nur ein Symptom. Erst durch den Vergleich von Latenz, Paketverlust, Durchsatz, Anwendungsantwortzeit, Serverressourcen, Storage und Datenbankwartezeiten lässt sich bestimmen, an welcher Stelle die tatsächliche Verzögerung entsteht.

Quellen und weiterführende Dokumentation

- Microsoft Learn – Test-Connection
- Microsoft Learn – Test-NetConnection

- Microsoft Learn – Get-NetAdapter
- Microsoft Learn – Get-NetAdapterStatistics
- Microsoft Learn – Resolve-DnsName
- Microsoft Learn – netsh wlan
- Microsoft Learn – Windows Performance Monitor
- curl – Write-Out Variables
- iperf3 – Documentation
- Wireshark – User’s Guide
- Wireshark – TCP Analysis
- Wireshark – dumpcap Manual Page
- systemd – journalctl