4.0 Server- und Dienstfehler systematisch analysieren

Server- und Dienstfehler liegen vor, wenn ein benötigter Dienst nicht startet, unerwartet beendet wird, nicht erreichbar ist oder zwar Verbindungen annimmt, aber fehlerhafte Ergebnisse liefert.

Dieses Kapitel behandelt die systematische Analyse von Diensten und Serveranwendungen unter Windows, Linux und macOS. Dazu gehören unter anderem Webserver, Datenbanken, Datei- und Druckdienste, Anwendungsserver sowie Hintergrunddienste.

> **Grundsatz:**
> Ein erreichbarer Server ist nicht automatisch ein funktionierender Server. Netzwerkverbindung, Port, Dienstprozess und Anwendungsfunktion müssen getrennt geprüft werden.

Ziele dieses Kapitels

Nach Abschluss dieses Kapitels sollst du:

- den betroffenen Dienst eindeutig identifizieren können,
- zwischen Netzwerk-, Port-, Dienst- und Anwendungsfehlern unterscheiden können,
- Dienststatus und Startart überprüfen können,
- Prozesse, Abhängigkeiten und verwendete Ports ermitteln können,
- Protokolle verschiedener Betriebssysteme auswerten können,
- Konfigurationsfehler erkennen können,
- Berechtigungs-, Ressourcen- und Zertifikatsprobleme untersuchen können,
- Dienste kontrolliert testen und neu starten können,
- wiederkehrende Dienstabbrüche analysieren können,
- Diagnoseergebnisse nachvollziehbar dokumentieren können.

Sicherheits- und Risikokennzeichnungen

Kennzeichnung	Bedeutung
`[RO]`	Rein lesender Befehl; verändert normalerweise nichts
`[TEST]`	Führt eine aktive Prüfung oder Verbindungsanfrage aus
`[PRIV]`	Erfordert möglicherweise Administrator- oder Rootrechte
`[FILE]`	Liest eine Datei oder schreibt eine Ausgabe in eine Datei
`[SENS]`	Ausgabe kann sensible Informationen enthalten

Kennzeichnung	Bedeutung
[CHANGE]	Verändert Einstellungen, Zustände oder Konfigurationen
[DISRUPT]	Kann einen Dienst oder laufenden Betrieb unterbrechen

> Befehle mit [CHANGE] oder [DISRUPT] dürfen erst nach Prüfung der Auswirkungen und möglichst innerhalb eines abgestimmten Wartungsfensters ausgeführt werden.

---

1. Diagnosemodell für Server- und Dienstfehler

Ein Dienst wird schrittweise von außen nach innen geprüft:

Ebene	Leitfrage	Typische Prüfung
1. Benutzer	Was funktioniert aus Sicht des Benutzers nicht?	Fehlermeldung und Zeitpunkt aufnehmen
2. Client	Ist nur ein Gerät oder Benutzer betroffen?	Vergleich mit anderem Client
3. Namensauflösung	Wird der richtige Servername aufgelöst?	DNS-Abfrage durchführen
4. Netzwerk	Ist der Server erreichbar?	Route und Erreichbarkeit prüfen
5. Transport	Ist der benötigte TCP- oder UDP-Port erreichbar?	Porttest durchführen
6. Betriebssystem	Läuft das Betriebssystem stabil?	Ressourcen und Ereignisse prüfen
7. Dienst	Läuft der benötigte Dienst?	Dienststatus und Prozess prüfen
8. Abhängigkeiten	Funktionieren abhängige Dienste und Systeme?	Datenbank, DNS, Speicher oder Authentifizierung prüfen
9. Konfiguration	Ist der Dienst korrekt konfiguriert?	Konfigurationsdateien und Startparameter prüfen
10. Anwendung	Liefert der Dienst fachlich korrekte Ergebnisse?	Anwendungsspezifischen Funktionstest durchführen

Wichtig: `ping` prüft nicht, ob ein Anwendungsdienst funktioniert. Ein Server kann ICMP-Anfragen beantworten, obwohl beispielsweise der Web-, Datenbank- oder Dateidienst ausgefallen ist.

---

2. Vier grundlegende Dienstzustände unterscheiden

Zustand	Beschreibung	Typische Ursache
Server nicht erreichbar	Bereits die Netzwerkverbindung scheitert	Routing, VLAN, Firewall, Stromversorgung oder Netzwerkkarte
Port nicht erreichbar	Server ist erreichbar, aber der Dienstport nicht	Dienst gestoppt, falscher Port oder Firewall
Port erreichbar, Anwendung fehlerhaft	Verbindung wird aufgebaut, die Anfrage schlägt jedoch fehl	Konfiguration, Berechtigung, Datenbank oder Anwendung
Dienst funktioniert teilweise	Nur bestimmte Benutzer oder Funktionen sind betroffen	Rechte, Mandant, Backend, Datenbestand oder Lastproblem

Diese Zustände dürfen nicht miteinander verwechselt werden. Die Fehlersuche beginnt immer bei der niedrigsten noch nicht nachgewiesenen Funktionsebene.

---

3. Schnellprüfung unter Windows, Linux und macOS

Die folgenden Befehle liefern eine erste Übersicht. `<DIENST>` und `<PORT>` müssen durch die tatsächlichen Werte ersetzt werden.

Aufgabe	Windows	Linux	macOS
Rechnername	`[RO] hostname`	`[RO] hostnamectl`	`[RO] scutil --get ComputerName`
Systemlaufzeit	`[RO] (Get-CimInstance Win32_OperatingSystem).LastBootUpTime`	`[RO] uptime`	`[RO] uptime`
Dienststatus	`[RO] Get-Service -Name "<DIENST>"`	`[RO] systemctl status <DIENST> --no-pager`	`[RO] launchctl print system/<DIENST>`
Alle laufenden Dienste	`[RO] Get-Service | Where-Object Status -eq "Running"`	`[RO] systemctl list-units --type=service --state=running`	`[RO] launchctl list`
Prozess suchen	`[RO] Get-Process -Name "<PROZESS>" -ErrorAction SilentlyContinue`	`[RO] pgrep -a <PROZESS>`	`[RO] pgrep -alf <PROZESS>`
TCP-Listener anzeigen	`[RO] Get-NetTCPConnection -State Listen`	`[RO][PRIV] sudo ss -lntp`	`[RO][PRIV] sudo lsof -nP -iTCP -sTCP:LISTEN`
Bestimmten Port prüfen	`[RO] Get-NetTCPConnection -LocalPort <PORT> -ErrorAction SilentlyContinue`	`[RO][PRIV] sudo ss -lntp "sport = :<PORT>"`	`[RO][PRIV] sudo lsof -nP -iTCP:<PORT> -sTCP:LISTEN`
Remote-TCP-Port testen	`[TEST] Test-NetConnection <SERVER> -Port <PORT>`	`[TEST] nc -vz <SERVER> <PORT>`	`[TEST] nc -vz <SERVER> <PORT>`

Aufgabe	Windows	Linux	macOS
CPU und Arbeitsspeicher	`[RO] Get-Process | Sort-Object CPU -Descending | Select-Object -First 10`	`[RO] top`	`[RO] top -o cpu`
Freien Speicherplatz prüfen	`[RO] Get-Volume`	`[RO] df -hT`	`[RO] df -h`

> “ `launchctl print system/<DIENST>` benötigt das Dienstlabel und nicht zwingend den sichtbaren Namen einer Anwendung. Benutzerbezogene LaunchAgents befinden sich außerdem nicht in der Systemdomäne.

---

4. Reihenfolge der praktischen Fehlersuche

1. Störung und betroffene Funktion genau beschreiben.
2. Zeitpunkt und Dauer der Störung erfassen.
3. Prüfen, welche Benutzer, Clients und Standorte betroffen sind.
4. Letzte Änderungen und bekannte Wartungsarbeiten ermitteln.
5. Servername und Zielsystem eindeutig bestimmen.
6. DNS-Auflösung und Netzwerkpfad überprüfen.
7. Erreichbarkeit des benötigten Ports testen.
8. Dienststatus, Prozess und Startart kontrollieren.
9. Kontrollieren, auf welcher Adresse und welchem Port der Dienst lauscht.
10. Abhängige Dienste und externe Systeme überprüfen.
11. System- und Anwendungsprotokolle für den Störungszeitraum auswerten.
12. CPU, Arbeitsspeicher, Datenträger und offene Dateien prüfen.
13. Konfiguration, Berechtigungen und Zertifikate kontrollieren.
14. Einen gezielten Funktionstest durchführen.
15. Erst danach eine geeignete Maßnahme planen.
16. Nach der Maßnahme Funktion und Nebenwirkungen überprüfen.
17. Ursache, Maßnahme und Ergebnis dokumentieren.

---

5. Kapitelübersicht

Seite	Thema	Inhalt
4.0	Server- und Dienstfehler systematisch analysieren	Kapitelübersicht und Diagnosemodell

Seite	Thema	Inhalt
4.1	Störung und betroffenen Dienst eingrenzen	Benutzer, Clients, Standorte und Zeiträume
4.2	Dienststatus und Startart prüfen	Windows-Dienste, systemd und launchd
4.3	Prozesse und Prozesszustände analysieren	PID, Elternprozess, Laufzeit und Ressourcen
4.4	Listener, Ports und Bindungsadressen prüfen	TCP, UDP, IPv4, IPv6 und Loopback
4.5	Dienstabhängigkeiten untersuchen	Abhängige Dienste, Backends und Startreihenfolge
4.6	System- und Dienstprotokolle auswerten	Ereignisanzeige, Journal und Unified Logging
4.7	Dienststartfehler analysieren	Exitcodes, Zeitüberschreitungen und Abstürze
4.8	Konfigurationsfehler untersuchen	Syntax, Pfade, Parameter und Umgebungsvariablen
4.9	Benutzer-, Dienstkonto- und Berechtigungsfehler	Konten, Dateirechte und Zugriffstoken
4.10	Ressourcenengpässe erkennen	CPU, RAM, Datenträger und Dateideskriptoren
4.11	Speicherplatz- und Dateisystemfehler	Volumes, Inodes, Quotas und schreibgeschützte Dateisysteme
4.12	Zertifikats- und TLS-Probleme	Gültigkeit, Vertrauenskette, Name und Protokoll
4.13	Webserver und HTTP-Dienste analysieren	HTTP-Statuscodes, Header, Logs und virtuelle Hosts
4.14	Datenbankverbindungen analysieren	Port, Anmeldung, Berechtigungen und Verbindungspools
4.15	Datei- und Freigabedienste analysieren	SMB, NFS, Berechtigungen und Sperren
4.16	Druckdienste und Warteschlangen analysieren	Spooler, Druckaufträge, Treiber und Erreichbarkeit
4.17	Wiederkehrende Dienstabbrüche untersuchen	Crash-Loops, Neustartregeln und Ursachenanalyse
4.18	Dienste kontrolliert neu starten	Risikoanalyse, Abhängigkeiten und Funktionstest
4.19	Befehlsübersicht – Server- und Dienstdiagnose	Vergleichstabelle für Windows, Linux und macOS

6. Entscheidungsweg bei einem nicht erreichbaren Dienst

Prüfschritt	Ergebnis	Nächste Aktion
Wird der richtige Servername verwendet?	Nein	Zielsystem und Dokumentation korrigieren
Wird der Name korrekt aufgelöst?	Nein	DNS-Konfiguration untersuchen
Ist der Server über das Netzwerk erreichbar?	Nein	Netzwerkpfad, VLAN, Routing und Firewall prüfen
Ist der benötigte Port erreichbar?	Nein	Listener, Dienststatus und Paketfilter prüfen
Läuft der Dienstprozess?	Nein	Startfehler und Protokolle untersuchen
Lauscht der Prozess auf dem erwarteten Port?	Nein	Bindungsadresse und Konfiguration prüfen
Antwortet das Anwendungsprotokoll?	Nein	Dienstprotokoll, TLS und Abhängigkeiten prüfen
Funktioniert die Anmeldung?	Nein	Konto, Kennwort, Berechtigungen und Identitätsdienst prüfen
Funktioniert die gewünschte Aktion?	Nein	Anwendung, Backend und Datenbestand untersuchen
Funktioniert alles wieder?	Ja	Ursache und Lösung dokumentieren

---

7. Wichtige Informationen vor einem Dienstneustart

Vor einem Neustart müssen mindestens folgende Fragen beantwortet werden:

- Welche Benutzer und Anwendungen verwenden den Dienst?
- Gibt es laufende Transaktionen oder Dateioperationen?
- Hängen weitere Dienste von diesem Dienst ab?
- Wird der Dienst automatisch wieder gestartet?
- Existiert ein Cluster, Loadbalancer oder Failover-System?
- Gehen durch den Neustart Diagnoseinformationen verloren?
- Wurden die relevanten Protokolle bereits gesichert?
- Ist der Neustart betrieblich freigegeben?
- Wie wird die Funktion anschließend getestet?
- Gibt es eine Rückfallmöglichkeit?

> Ein Neustart kann die Verfügbarkeit kurzfristig wiederherstellen, beseitigt aber nicht automatisch die eigentliche Fehlerursache. Vorher sollten Zustand, Zeitstempel, Fehlermeldungen und relevante Protokolle erfasst werden.

---

8. Mindestdokumentation eines Dienstfehlers

Information	Beispiel
Betroffener Dienst	Intranet-Webanwendung
Server	`srv-web01.example.local`
Betriebssystem	Windows Server beziehungsweise Linux-Distribution und Version
Beginn der Störung	Datum und genaue Uhrzeit mit Zeitzone
Betroffene Benutzer	Alle Benutzer am Standort Berlin
Fehlerbild	HTTP-Verbindung wird aufgebaut, Antwortcode 503
Dienststatus	Dienst läuft beziehungsweise ist beendet
Prozess	Prozessname und PID
Port und Bindungsadresse	TCP 443 auf einer bestimmten IP-Adresse
Relevante Protokollmeldung	Ereignis-ID, Exitcode oder Fehlermeldung
Letzte Änderung	Aktualisierung oder Konfigurationsänderung
Durchgeführte Prüfungen	DNS-, Port-, Dienst- und Funktionstest
Maßnahme	Konfiguration korrigiert und Dienst kontrolliert neu gestartet
Funktionstest	Anmeldung und Beispielabfrage erfolgreich
Ursache	Technische Grundursache
Vorbeugung	Monitoring, Dokumentation oder Konfigurationsprüfung

---

Merksatz

> **Erreichbarkeit beweist nur den Netzwerkweg. Ein offener Port beweist nur einen Listener. Erst ein erfolgreicher Anwendungstest beweist die Funktion des Dienstes.**

Weiterführende Quellen

- Microsoft Learn – sc.exe query
- Microsoft Learn – Get-Service
- systemd – systemctl
- systemd – journalctl
- Apple – Einführung in die App „Konsole“
- Apple – Handbuchseite zu launchctl