20.13 Trainer – Gemischte Fehlersuche nach dem OSI-Modell

Diese Trainer-Seite wiederholt die systematische Fehlersuche nach dem OSI-Modell.

Ziel ist, Fehlerbilder nicht wild zu raten, sondern sauber einzuordnen:

- Welche Schicht ist betroffen?
- Was funktioniert noch?
- Was funktioniert nicht?
- Welche Prüfung passt als nächstes?
- Welche Ursache ist am wahrscheinlichsten?

Merksatz:

Gute Fehlersuche beginnt nicht mit Vermutung,
sondern mit Eingrenzung.

Lernziele

Nach dieser Seite solltest du sicher können:

- Fehler systematisch nach OSI-Schichten eingrenzen
- typische Fehlerbilder erkennen
- passende Prüfwerkzeuge auswählen
- IP,
  DNS,
  Gateway,
  Firewall,
  Port,
  Dienst
  und Rechte unterscheiden
- aus Symptomen wahrscheinliche Ursachen ableiten
- prüfungssichere Antworten formulieren

Grundprinzip der Fehlersuche

Bei Netzwerkproblemen immer fragen:

1. Gibt es eine physische Verbindung?

2. Ist die lokale Verbindung korrekt?

3. Stimmt die IP-Konfiguration?

4. Ist das Zielnetz erreichbar?

5. Ist der Port oder Dienst erreichbar?

6. Funktioniert die Anwendung?

7. Gibt es Berechtigungs- oder Authentifizierungsprobleme?

Merksatz:

Erst Verbindung prüfen,
dann Adresse,
dann Dienst,
dann Anwendung.

OSI-Fehlersuche im Überblick

Schicht	Thema	Typische Prüfung
1	Kabel, Signal, Link	Link-LED, Kabel, Port
2	MAC, VLAN, Switch	VLAN, MAC-Tabelle, ARP
3	IP, Gateway, Routing	IP-Konfiguration, ping, traceroute
4	TCP, UDP, Ports	Porttest, Dienst lauscht?
5	Sitzung	Session, Timeout, Cookie
6	TLS, Zertifikat	Zertifikat, Verschlüsselung
7	Anwendung	DNS, HTTP, Dienst, Logs

Merksatz:

Jede Schicht hat eigene Fehlerbilder.

Aufgabe 1

Ein Client hat keine Link-LED am Netzwerkanschluss.

Welche Schicht ist zuerst betroffen?

Antwort anzeigen

Zuerst betroffen ist:

OSI-Schicht 1

Begründung:

Keine Link-LED deutet auf ein physisches Problem hin.

Prüfen:

Kabel

Stecker

Netzwerkdose

Switchport

Netzwerkkarte

Gegenstelle

Merksatz:

Kein Link:
Schicht 1 prüfen.

Aufgabe 2

Ein Client hat die IP-Adresse:

```
169.254.23.10
```

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
DHCP-Problem
```

Begründung:

```
169.254.x.x ist eine APIPA-Adresse.
Der Client hat wahrscheinlich keine gültige IP-Adresse vom DHCP-Server erhalten.
```

Prüfen:

```
DHCP-Server

VLAN

DHCP-Scope

DHCP-Relay

Netzwerkverbindung
```

Merksatz:

```
169.254.x.x:
DHCP nicht erreicht.
```

Aufgabe 3

Ein Client kann Geräte im gleichen Netz erreichen, aber keine externen Netze.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
Gateway,
Routing,
NAT
oder Firewall
```

Erste Prüfung:

```
Standardgateway
```

Begründung:

```
Lokale Kommunikation funktioniert.
Der Fehler liegt wahrscheinlich beim Weg in andere Netze.
```

Merksatz:

```
Lokal ja,
extern nein:
Gateway prüfen.
```

Aufgabe 4

Ein Client erreicht eine Webseite per IP-Adresse, aber nicht per Namen.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

DNS-Problem

Begründung:

Die IP-Kommunikation funktioniert.
Nur die Namensauflösung funktioniert nicht.

Prüfen:

DNS-Server

DNS-Eintrag

DNS-Cache

DNS-Suffix

Split-DNS

Merksatz:

IP ja,
Name nein:
DNS.

Aufgabe 5

Ein Server ist per ping erreichbar, aber SSH funktioniert nicht.

Was ist wahrscheinlich?

Antwort anzeigen

Ping prüft ICMP. SSH nutzt TCP 22.

Mögliche Ursachen:

TCP 22 blockiert

SSH-Dienst läuft nicht

SSH lauscht auf anderem Port

lokale Firewall blockiert

Netzwerkfirewall blockiert

Benutzer oder Schlüssel falsch

Merksatz:

ping geht,
Dienst nicht:
Port,
Dienst
und Firewall prüfen.

Aufgabe 6

Ein Webserver ist per ping erreichbar, aber HTTPS funktioniert nicht.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

TCP 443 erreichbar?

Webserver läuft?

Dienst lauscht auf Port 443?

```
Firewall erlaubt TCP 443?

Reverse Proxy korrekt?

TLS-Zertifikat korrekt?

Anwendung läuft?
```

Merksatz:

```
ping ist kein HTTPS-Test.
```

Aufgabe 7

Ein Browser zeigt HTTP 404.

Was bedeutet das?

Antwort anzeigen

HTTP 404 bedeutet:

```
nicht gefunden
```

Die angeforderte Ressource existiert unter dieser Adresse nicht oder ist dort nicht erreichbar.

Prüfen:

```
URL

Pfad

Routing der Webanwendung

Webserver-Konfiguration

Reverse Proxy
```

Merksatz:

```
404 = Ressource nicht gefunden.
```

Aufgabe 8

Ein Browser zeigt HTTP 500.

Was bedeutet das?

Antwort anzeigen

HTTP 500 bedeutet:

```
interner Serverfehler
```

Das Problem liegt eher auf Serverseite.

Prüfen:

```
Anwendungslogs

Webserverlogs

Backend

Datenbank

Konfiguration

Berechtigungen
```

Merksatz:

```
500 = Server,
Anwendung
oder Backend prüfen.
```

Aufgabe 9

Ein Browser zeigt HTTP 502.

Was bedeutet das häufig?

Antwort anzeigen

HTTP 502 bedeutet:

```
Bad Gateway
```

Typisch bei:

```
Reverse Proxy

Load Balancer

Gateway
```

Mögliche Ursachen:

```
Backend nicht erreichbar

Backend-Port falsch

Backend-Dienst läuft nicht

DNS intern falsch

Proxy-Konfiguration falsch
```

Merksatz:

```
502:
Proxy oder Gateway erreicht Backend nicht korrekt.
```

Aufgabe 10

Ein Benutzer kann sich anmelden, aber nicht auf eine Datei zugreifen.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
Autorisierungs- oder Berechtigungsproblem
```

Begründung:

```
Die Anmeldung funktioniert.
Der Zugriff auf die Ressource ist aber nicht erlaubt.
```

Prüfen:

```
Gruppenmitgliedschaft

ACLs

Freigaberechte

Dateisystemrechte

Rollen
```

Merksatz:

```
Login ja,
Zugriff nein:
Rechte prüfen.
```

Aufgabe 11

Ein Benutzer kann sich gar nicht anmelden.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
Authentifizierungsproblem
```

Mögliche Ursachen:

```
falsches Passwort

Konto gesperrt

MFA-Problem

Verzeichnisdienst nicht erreichbar

Zertifikat abgelaufen

Zeitproblem
```

Merksatz:

```
Anmeldung scheitert:
Authentifizierung prüfen.
```

Aufgabe 12

Ein Client bekommt eine IP-Adresse aus dem falschen Netz.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

falsches VLAN

Begründung:

Wenn ein Client im falschen VLAN landet,
erhält er eventuell eine Adresse aus dem falschen DHCP-Scope.

Prüfen:

Access-VLAN am Switchport

Trunk-Konfiguration

DHCP-Scope

Dokumentation

Merksatz:

Falsches Netz:
VLAN prüfen.

Aufgabe 13

Mehrere VLANs funktionieren über eine Switch-Verbindung nicht.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

Trunk-Port aktiv?

VLANs erlaubt?

VLANs auf beiden Switches vorhanden?

802.1Q-Tagging korrekt?

Native VLAN passend?

Gegenstelle korrekt konfiguriert?

Merksatz:

Mehrere VLANs betroffen:
Trunk prüfen.

Aufgabe 14

Ein einzelner Client kann keine Verbindung herstellen, andere Clients im gleichen Raum funktionieren.

Was ist wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

Patchkabel defekt

Netzwerkdose defekt

Switchport deaktiviert

falsches Access-VLAN

Netzwerkkarte deaktiviert

Port Security blockiert

Client-Konfiguration falsch

Merksatz:

Nur ein Gerät betroffen:
lokal am Gerät,
Kabel
oder Port suchen.

Aufgabe 15

Alle Clients in einem VLAN haben kein Internet.

Was ist wahrscheinlicher als ein einzelnes defektes Patchkabel?

Antwort anzeigen

Wahrscheinlicher sind zentrale Ursachen:

Gateway des VLANs

Firewall-Regel

Routing

NAT

DHCP-Konfiguration

VLAN-Trunk

DNS,
falls nur Namen betroffen sind

Merksatz:

Viele Geräte betroffen:
zentrale Komponente prüfen.

Aufgabe 16

Ein Client kann externe IP-Adressen erreichen, aber keine Webseiten per Domain.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
DNS-Problem
```

Begründung:

```
Der Weg ins Internet funktioniert.
Nur die Namensauflösung funktioniert nicht.
```

Prüfen:

```
DNS-Server

DNS-Erreichbarkeit

DNS-Einträge

DNS-Cache
```

Merksatz:

```
Externe IP ja,
Domain nein:
DNS.
```

Aufgabe 17

Ein Dienst funktioniert intern, aber nicht von außen über das Internet.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

```
öffentliche IP

DNS

Portweiterleitung

Router-Firewall

lokale Firewall

Dienststatus

Dienstport

doppeltes NAT

CGNAT

Provider-Portblockade
```

Merksatz:

```
Intern ja,
extern nein:
NAT,
Firewall,
DNS
und öffentliche IP prüfen.
```

Aufgabe 18

Ein Dienst funktioniert von außen, aber intern nicht über die öffentliche Domain.

Was ist wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

```
Hairpin NAT fehlt

Split-DNS fehlt

interne DNS-Auflösung falsch

Firewall-Regel für internen Zugriff fehlt
```

Merksatz:

```
Externe Domain intern:
Hairpin NAT oder Split-DNS prüfen.
```

Aufgabe 19

VPN ist verbunden, aber interne Namen funktionieren nicht.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

```
VPN-DNS-Problem
```

Prüfen:

```
interner DNS-Server gesetzt?

DNS-Server über VPN erreichbar?

DNS-Suffix vorhanden?
```

Split-DNS korrekt?

DNS-Cache veraltet?

Merksatz:

VPN-IP ja,
VPN-Name nein:
VPN-DNS prüfen.

Aufgabe 20

VPN ist verbunden, aber interne IP-Ziele sind nicht erreichbar.

Was ist wahrscheinlich?

Antwort anzeigen

Mögliche Ursachen:

VPN-Route fehlt

Zielnetz nicht erlaubt

Firewall blockiert

Rückroute fehlt

IP-Adresskonflikt

Berechtigung fehlt

Merksatz:

```
VPN verbunden heißt nicht automatisch:
Routen und Regeln stimmen.
```

Aufgabe 21

Ein Heimnetz und Firmennetz nutzen beide 192.168.1.0/24.

Warum ist das bei VPN problematisch?

Antwort anzeigen

Problem:

```
Der Client kann nicht eindeutig entscheiden,
ob 192.168.1.x lokal
oder über VPN erreichbar sein soll.
```

Folge:

```
Routingprobleme

interne Dienste nicht erreichbar
```

Merksatz:

```
Gleiche Netze lokal und remote verursachen VPN-Probleme.
```

Aufgabe 22

Ein Zertifikat ist abgelaufen.

Welches typische Fehlerbild entsteht?

Antwort anzeigen

Typisches Fehlerbild:

```
Browser oder Client zeigt Zertifikatswarnung.
```

Mögliche Folgen:

```
HTTPS-Verbindung wird blockiert

Benutzer erhält Sicherheitswarnung

API-Clients lehnen Verbindung ab
```

Prüfen:

```
Ablaufdatum

Hostname

Zertifikatskette

Systemzeit
```

Merksatz:

```
Zertifikatswarnung:
Ablauf,
Name,
Kette
und Zeit prüfen.
```

Aufgabe 23

Ein HTTPS-Zertifikat passt nicht zum Hostnamen.

Was ist die Ursache?

Antwort anzeigen

Ursache:

Der aufgerufene Name steht nicht passend im Zertifikat.

Prüfen:

Common Name

Subject Alternative Name

verwendete Domain

Reverse Proxy

falsches Zertifikat

Merksatz:

Zertifikat muss zum aufgerufenen Namen passen.

Aufgabe 24

Ein Dienst startet nach einem Restore nicht.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

Abhängigkeiten

Datenbank erreichbar?

Rechte korrekt?

```
Konfiguration vorhanden?

Zertifikate vorhanden?

DNS korrekt?

Ports frei?

Logs auswerten

Restore-Reihenfolge eingehalten?
```

Merksatz:

```
Restore braucht Abhängigkeiten und Reihenfolge.
```

Aufgabe 25

Nach einem Update funktioniert ein Dienst nicht mehr.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

```
Änderungsprotokoll

Konfigurationsänderungen

Dienststatus

Logs

Ports

Abhängigkeiten
```

```
Berechtigungen

Kompatibilität

Rollback-Möglichkeit
```

Merksatz:

```
Nach Änderung:
Change,
Logs
und Rollback prüfen.
```

Aufgabe 26

Ein Backup ist vorhanden, aber die Wiederherstellung schlägt fehl.

Was wurde wahrscheinlich versäumt?

Antwort anzeigen

Wahrscheinlich:

```
Restore-Test
```

Weitere mögliche Ursachen:

```
Backup beschädigt

Schlüssel fehlt

Rechte fehlen

Datenbank nicht konsistent gesichert
```

Backup-Kette unvollständig

Dokumentation fehlt

Merksatz:

Backup ohne Restore-Test ist unsicher.

Aufgabe 27

Ein Server ist sehr langsam, aber nicht komplett ausgefallen.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

CPU-Auslastung

RAM

Festplatten-I/O

Speicherplatz

Netzwerkfehler

Paketverluste

Latenz

Logs

laufende Prozesse

Datenbanklast

Merksatz:

```
Langsamkeit braucht Messwerte,
nicht nur Vermutung.
```

Aufgabe 28

Ein Dienst ist nicht erreichbar. Der Port lauscht aber lokal auf 127.0.0.1.

Warum kann das ein Problem sein?

Antwort anzeigen

127.0.0.1 ist localhost.

Wenn ein Dienst nur auf 127.0.0.1 lauscht, ist er nur lokal auf dem Server erreichbar, nicht von anderen Systemen.

Prüfen:

```
Bind-Adresse

Dienstkonfiguration

Firewall
```

Merksatz:

```
127.0.0.1 heißt:
nur lokal erreichbar.
```

Aufgabe 29

Ein Dienst lauscht auf 0.0.0.0.

Was bedeutet das?

Antwort anzeigen

0.0.0.0 bedeutet bei einem lauschenden Dienst:

```
Der Dienst lauscht auf allen IPv4-Schnittstellen des Systems.
```

Wichtig:

```
Ob er wirklich erreichbar ist,
hängt zusätzlich von Firewall,
Routing
und Netzwerk ab.
```

Merksatz:

```
0.0.0.0 heißt:
alle IPv4-Interfaces.
```

Aufgabe 30

Ein Porttest schlägt fehl, obwohl der Dienst läuft.

Was kann die Ursache sein?

Antwort anzeigen

Mögliche Ursachen:

```
Dienst lauscht nur auf localhost

lokale Firewall blockiert

Netzwerkfirewall blockiert

falscher Port
```

falsches Protokoll TCP/UDP

NAT-Regel fehlt

Routingproblem

Ziel-IP falsch

Merksatz:

Dienst läuft heißt nicht automatisch:
Dienst ist von außen erreichbar.

Aufgabe 31

Ein DNS-Eintrag wurde geändert, aber Clients nutzen noch die alte IP.

Was ist wahrscheinlich?

Antwort anzeigen

Wahrscheinlich:

DNS-Cache oder TTL

Prüfen:

Client-DNS-Cache

DNS-Server-Cache

TTL des Eintrags

welcher DNS-Server gefragt wird

Merksatz:

DNS-Änderungen wirken nicht immer sofort.

Aufgabe 32

Ein Client erhält keine IP-Adresse, aber nur in einem bestimmten VLAN.

Was sollte geprüft werden?

Antwort anzeigen

Prüfen:

DHCP-Scope für dieses VLAN

DHCP-Relay

Gateway im VLAN

VLAN-Trunk

Firewall-Regeln

DHCP-Server erreichbar?

Merksatz:

DHCP pro VLAN braucht passenden Scope und Weg zum Server.

Aufgabe 33

Ein Client kann den DNS-Server nicht erreichen.

Welche Folgen kann das haben?

Antwort anzeigen

Folgen:

Namen werden nicht aufgelöst

Webseiten per Domain funktionieren nicht

interne Dienste per Name funktionieren nicht

Anmeldung oder Dienste können verzögert sein

Anwendungen finden Backend-Systeme nicht

Merksatz:

Ohne DNS funktionieren viele Dienste scheinbar nicht,
obwohl IP-Kommunikation möglich sein kann.

Aufgabe 34

Ein Benutzer meldet: „Das Internet geht nicht.“

Welche Rückfragen oder Prüfungen sind sinnvoll?

Antwort anzeigen

Sinnvoll prüfen:

Betrifft es nur eine Webseite oder alle?

Geht Zugriff per IP?

Geht DNS-Auflösung?

IP-Adresse korrekt?

Gateway erreichbar?

```
andere Clients betroffen?

WLAN oder Kabel?

Proxy oder VPN aktiv?

Firewall oder Filter?
```

Merksatz:

```
„Internet geht nicht“ erst in konkrete Symptome zerlegen.
```

Aufgabe 35

Ein Benutzer meldet: „Der Server ist nicht erreichbar.“

Welche Eingrenzung ist sinnvoll?

Antwort anzeigen

Sinnvoll prüfen:

```
Welcher Server?

per Name oder IP?

ping erreichbar?

Port erreichbar?

Dienst läuft?

nur ein Benutzer betroffen?

Rechteproblem?

DNS korrekt?
```

Firewall-Regel geändert?

Logs vorhanden?

Merksatz:

Server nicht erreichbar kann DNS,
Routing,
Port,
Dienst
oder Rechte bedeuten.

Aufgabe 36

Ordne Fehlerbilder den Themen zu.

Fehlerbild	Thema
keine Link-LED	?
169.254.x.x	?
IP geht, Name nicht	?
ping geht, HTTPS nicht	?
HTTP 500	?
Login geht, Zugriff nicht	?

Antwort anzeigen

Fehlerbild	Thema
keine Link-LED	Schicht 1 / physische Verbindung
169.254.x.x	DHCP
IP geht, Name nicht	DNS
ping geht, HTTPS nicht	TCP 443, Webdienst, Firewall, TLS
HTTP 500	Server, Anwendung, Backend
Login geht, Zugriff nicht	Autorisierung / Rechte

Merksatz:

> Fehlerbild zuerst genau einordnen.

Aufgabe 37

Welche Antwort ist besser?

Aufgabe:

> Ein Client erreicht externe IP-Adressen,
> aber keine Domains.
> Nennen Sie eine wahrscheinliche Ursache.

Antwort A:

> Internet ist kaputt.

Antwort B:

> Wahrscheinlich liegt ein DNS-Problem vor,
> da externe IP-Adressen erreichbar sind,
> aber Namen nicht aufgelöst werden.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort leitet die Ursache aus dem Fehlerbild ab
> und nennt DNS als konkrete Prüfung.

Merksatz:

> Ursache aus Symptom ableiten.

Aufgabe 38

Welche Antwort ist besser?

Aufgabe:

```
Ein Dienst ist per ping erreichbar,
aber der Port 443 ist nicht erreichbar.
Was prüfen Sie?
```

Antwort A:

```
Den Monitor.
```

Antwort B:

```
Ich prüfe,
ob der Webdienst läuft,
ob er auf TCP 443 lauscht,
ob lokale oder zentrale Firewalls TCP 443 blockieren
und ob NAT oder Portweiterleitung korrekt eingerichtet sind.
```

Antwort anzeigen

B ist besser.

Begründung:

```
Die Antwort trennt Host-Erreichbarkeit von Dienst-Erreichbarkeit
und nennt konkrete Prüfungen.
```

Merksatz:

```
ping ist kein Porttest.
```

Aufgabe 39

Welche Antwort ist besser?

Aufgabe:

> Nach einem Update funktioniert ein Dienst nicht mehr.
> Was tun Sie?

Antwort A:

> Alles neu installieren.

Antwort B:

> Ich prüfe Dienststatus,
> Logs,
> geänderte Konfigurationen,
> Abhängigkeiten,
> Ports
> und Berechtigungen.
> Falls nötig,
> nutze ich den vorbereiteten Rollback-Plan.

Antwort anzeigen

B ist besser.

Begründung:

> Die Antwort ist systematisch
> und berücksichtigt Change Management.

Merksatz:

> Nach Änderung:
> gezielt prüfen,
> nicht blind neu installieren.

Aufgabe 40

Welche Antwort ist besser?

Aufgabe:

```
Warum ist systematische Fehlersuche besser als Raten?
```

Antwort A:

```
Weil das professioneller klingt.
```

Antwort B:

```
Systematische Fehlersuche grenzt den Fehler anhand von Schichten,
Symptomen
und Messwerten ein.
Dadurch werden Ursachen schneller gefunden
und unnötige Änderungen vermieden.
```

Antwort anzeigen

B ist besser.

Begründung:

```
Die Antwort erklärt den Nutzen:
Eingrenzung,
Messbarkeit
und Vermeidung unnötiger Änderungen.
```

Merksatz:

```
Fehlersuche braucht Struktur.
```

Mini-Prüfung: typische Fehlerbilder

Fehlerbild	Wahrscheinlichstes Thema

keine Link-LED	Kabel, Port, Schicht 1
Link ja, aber falsches Netz	VLAN oder DHCP
169.254.x.x	DHCP nicht erreicht
lokale Kommunikation ja, Internet nein	Gateway, Routing, NAT, Firewall
externe IP ja, Name nein	DNS
ping ja, SSH nein	TCP 22, SSH-Dienst, Firewall
ping ja, HTTPS nein	TCP 443, Webdienst, Firewall, TLS
HTTP 401	Authentifizierung
HTTP 403	Autorisierung
HTTP 404	Ressource nicht gefunden
HTTP 500	Anwendung oder Server
HTTP 502	Proxy, Gateway oder Backend
VPN verbunden, IP ja, Name nein	VPN-DNS
Restore schlägt fehl	Restore-Test, Backup, Schlüssel, Rechte

Mini-Prüfung: passende Werkzeuge

Prüfung	Werkzeug oder Ort
IP-Konfiguration prüfen	ipconfig, ip addr
Gateway prüfen	route print, ip route
Erreichbarkeit per ICMP	ping
Weg zum Ziel prüfen	tracert, traceroute
DNS prüfen	nslookup, dig
offene Ports prüfen	ss, netstat, Porttest
HTTP prüfen	Browser, curl
Dienststatus prüfen	systemctl, Diensteverwaltung
Logs prüfen	journalctl, Event Viewer, Anwendungslogs
Firewall prüfen	Firewall-Regeln und Logs
Rechte prüfen	Gruppen, ACLs, Rollen
Backup prüfen	Backup-Job, Restore-Test

IHK-sichere Kurzformulierung

Systematische Fehlersuche bedeutet, ein Problem anhand von Symptomen, Schichten und Messwerten einzugrenzen. Zuerst wird geprüft, ob eine physische Verbindung besteht. Danach folgen lokale Kommunikation, IP-Konfiguration, Gateway, Routing, DNS, Ports, Dienste, Anwendung und Berechtigungen. Typische Fehlerbilder helfen bei der Einordnung: 169.254.x.x deutet auf DHCP hin, IP erreichbar aber Name nicht deutet auf DNS hin, lokale Kommunikation aber kein Internet deutet auf Gateway, Routing, NAT oder Firewall hin. ping prüft nur ICMP und ersetzt keinen Port- oder Diensttest. Gute Prüfungsantworten nennen eine wahrscheinliche Ursache, begründen sie mit dem Fehlerbild und nennen eine passende Prüfung.

Merksätze

Fehlersuche beginnt mit Eingrenzung.

Erst Schicht 1,
dann höhere Schichten.

Kein Link:
Kabel,
Port,
Gegenstelle prüfen.

Falsches Netz:
VLAN oder DHCP prüfen.

169.254.x.x:
DHCP nicht erreicht.

Lokal ja,
extern nein:
Gateway,
Routing,
NAT
oder Firewall.

IP ja,
Name nein:
DNS.

ping ja,
Dienst nein:
Port,

Dienst
und Firewall.

ping ist kein Porttest.

HTTP 401:
nicht authentifiziert.

HTTP 403:
verboten.

HTTP 404:
nicht gefunden.

HTTP 500:
interner Serverfehler.

HTTP 502:
Gateway,
Proxy
oder Backend.

VPN verbunden heißt nicht:
Routen,
DNS
und Rechte stimmen.

Login ja,
Zugriff nein:
Rechte.

Anmeldung scheitert:
Authentifizierung.

Nach Änderung:
Change,
Logs
und Rollback prüfen.

Backup ohne Restore-Test ist unsicher.

Viele Geräte betroffen:
zentrale Komponente prüfen.

Ein Gerät betroffen:
lokales Problem prüfen.

Gute Antwort:
Ursache,
Begründung,
Prüfung.

Nicht raten,
sondern messen.