12.6 Logauswertung, Monitoring und Dokumentation bei Netzwerkfehlern

Logs und Monitoring sind wichtige Hilfsmittel bei der Fehlersuche.

Ein Paketmitschnitt zeigt, welche Pakete übertragen werden.

Logs zeigen, was Systeme, Dienste, Firewalls und Anwendungen entschieden oder gemeldet haben.

Monitoring zeigt, ob Systeme und Dienste dauerhaft verfügbar und leistungsfähig sind.

Merksatz:

```
Mitschnitt zeigt Verkehr.
Logs zeigen Ereignisse.
Monitoring zeigt Zustand über Zeit.
```

Warum Logs wichtig sind

Viele Fehler sind ohne Logs schwer zu verstehen.

Beispiele:

```
Benutzer kann sich nicht anmelden.
Firewall blockiert Verbindung.
Webserver liefert HTTP 500.
Datenbank lehnt Verbindung ab.
Zertifikat wird abgelehnt.
VPN-Verbindung wird getrennt.
DHCP vergibt keine Adresse.
DNS liefert falsche Antwort.
```

Ohne Logs sieht man oft nur das Symptom.

Merksatz:

```
Logs liefern Hinweise auf die Ursache.
```

Was ist ein Log?

Ein Log ist ein Ereignisprotokoll.

Darin steht, was ein System oder Dienst festgestellt hat.

Typische Angaben:

- Zeitpunkt
- Quelle
- Ziel
- Benutzer
- Dienst
- Aktion
- Fehlercode
- Meldung
- Schweregrad
- betroffene Komponente

Merksatz:

Ein Log ist ein technisches Ereignistagebuch.

Typische Logquellen

Wichtige Logquellen in Netzwerken:

- Firewall-Logs
- Router-Logs
- Switch-Logs
- DNS-Logs
- DHCP-Logs
- VPN-Logs
- Webserver-Logs
- Reverse-Proxy-Logs
- Authentifizierungslogs
- Mailserver-Logs
- Datenbank-Logs
- Betriebssystem-Logs

```
- Anwendungslogs
- Cloud-Logs
- Monitoring-Alarme
```

Merksatz:

```
Die richtige Logquelle hängt vom Fehlerbild ab.
```

Firewall-Logs

Firewall-Logs zeigen, ob Verkehr erlaubt oder blockiert wurde.

Wichtige Informationen:

```
- Quelle
- Ziel
- Quellport
- Zielport
- Protokoll
- Aktion
- Regelname
- Interface
- Zone
- NAT-Übersetzung
- Zeit
```

Beispiele für Aktionen:

```
allow
deny
drop
reject
```

Merksatz:

```
Firewall-Logs zeigen,
welche Regel wirklich gegriffen hat.
```

Firewall-Log richtig lesen

Bei Firewall-Logs prüft man:

```
Kommt der Verkehr an der Firewall an?
Welche Quelle sieht die Firewall?
Welches Ziel sieht die Firewall?
Welcher Port wird genutzt?
TCP oder UDP?
Wird erlaubt oder blockiert?
Welche Regel trifft?
Ist NAT sichtbar?
Gibt es Rückverkehr?
```

Merksatz:

```
Nicht die gedachte Regel zählt,
sondern die tatsächlich getroffene Regel.
```

Keine Firewall-Logs sichtbar

Wenn kein passender Logeintrag sichtbar ist, kann das bedeuten:

```
Verkehr kommt gar nicht bei der Firewall an.
falsche Firewall wird geprüft.
falsches Interface wird geprüft.
Logging ist deaktiviert.
DNS zeigt auf ein anderes Ziel.
Route geht anderen Weg.
Client sendet keine Anfrage.
vorgeschaltetes Gerät blockiert.
Zeitfilter ist falsch gesetzt.
```

Merksatz:

```
Kein Log heißt nicht automatisch:
Firewall ist unschuldig.
```

Router-Logs

Router-Logs helfen bei:

- Routingproblemen
- Verbindungsabbrüchen
- WAN-Störungen
- VPN-Tunneln
- Interface-Fehlern
- Nachbarschaftsproblemen
- Routing-Protokollen

Typische Hinweise:

- Interface up/down
- Route geändert
- Tunnel down
- Paket verworfen
- Gateway nicht erreichbar

Merksatz:

> Router-Logs zeigen Wege und Verbindungszustände.

Switch-Logs

Switch-Logs sind wichtig für Schicht 2.

Sie zeigen zum Beispiel:

- Port up/down
- VLAN-Fehler
- STP-Änderungen
- Loop-Erkennung
- Port-Security-Verletzungen
- Duplex- oder Speed-Probleme
- MAC-Flapping
- PoE-Probleme
- Trunk-Probleme

Merksatz:

```
Switch-Logs helfen bei lokalen Netz- und VLAN-Problemen.
```

MAC-Flapping

MAC-Flapping bedeutet:

```
dieselbe MAC-Adresse erscheint schnell wechselnd an verschiedenen Switchports.
```

Mögliche Ursachen:

```
- Netzwerkschleife
- falsch angeschlossener Switch
- falsche Link Aggregation
- virtuelle Umgebung
- fehlerhafte Redundanz
- Loop über Patchkabel
```

Merksatz:

```
MAC-Flapping ist ein Warnzeichen für Schicht-2-Probleme.
```

STP-Logs

STP steht für:

```
Spanning Tree Protocol
```

STP verhindert Schleifen in Layer-2-Netzen.

STP-Logs zeigen zum Beispiel:

```
Topology Change
Port Blocking
Port Forwarding
Root Bridge Wechsel
```

Loop erkannt

Merksatz:

STP-Logs sind wichtig bei Schleifen und Broadcast-Stürmen.

DNS-Logs

DNS-Logs zeigen Namensauflösungen.

Wichtige Fragen:

Welcher Client fragt?
Welcher Name wird gefragt?
Welche Antwort wird geliefert?
Gibt es NXDOMAIN?
Gibt es SERVFAIL?
Wird intern oder extern gefragt?
Gibt es ungewöhnlich viele Anfragen?

Merksatz:

DNS-Logs zeigen,
welche Namen tatsächlich aufgelöst werden.

DHCP-Logs

DHCP-Logs zeigen, wie IP-Adressen vergeben werden.

Wichtige Informationen:

- Client-MAC-Adresse
- angebotene IP-Adresse
- vergebene IP-Adresse
- Lease-Zeit
- Scope
- DHCP-Optionen
- Konflikte

- Fehlermeldungen

Typische Fehler:

Scope voll
falscher Scope
DHCP-Relay fehlt
Lease-Konflikt
unbekannter Client

Merksatz:

DHCP-Logs erklären,
warum ein Client welche IP bekommt oder nicht bekommt.

VPN-Logs

VPN-Logs zeigen, ob ein Tunnel aufgebaut wird und warum er scheitert.

Wichtige Hinweise:

Benutzername
Client-IP
VPN-IP
Authentifizierung erfolgreich oder fehlgeschlagen
Zertifikatsfehler
MFA-Fehler
Gruppenrichtlinie
zugewiesene Routen
Tunnel aufgebaut oder getrennt
Fehlercode

Merksatz:

VPN verbunden heißt nicht automatisch:
Zugriff auf interne Systeme erlaubt.

Webserver-Logs

Webserver-Logs zeigen HTTP-Anfragen und Antworten.

Typische Angaben:

```
- Client-IP
- Zeitpunkt
- Methode
- Pfad
- Statuscode
- User-Agent
- Antwortgröße
- Bearbeitungszeit
```

Beispiele:

```
GET /index.html 200
POST /login 401
GET /admin 403
GET /missing 404
GET /app 500
```

Merksatz:

```
Webserver-Logs zeigen,
was die Anwendung oder der Webserver geantwortet hat.
```

Reverse-Proxy-Logs

Reverse-Proxy-Logs sind besonders wichtig bei veröffentlichten Webdiensten.

Sie zeigen:

```
- externer Client
- Hostname
- Pfad
- Backend-Ziel
- HTTP-Status
- TLS-Informationen
- Weiterleitungsfehler
```

- Timeout
- 502 oder 504
- ausgewähltes Backend

Merksatz:

Reverse-Proxy-Logs zeigen den Übergang vom Client zum Backend.

Authentifizierungslogs

Authentifizierungslogs zeigen, ob eine Anmeldung erfolgreich war oder nicht.

Typische Hinweise:

- Benutzername
- Quelle
- Zeitpunkt
- Erfolg oder Fehler
- falsches Passwort
- Konto gesperrt
- MFA erforderlich
- Token ungültig
- Gruppenmitgliedschaft
- Kerberos- oder LDAP-Fehler

Merksatz:

Authentifizierungslogs beantworten:
Wer wollte sich anmelden,
und warum ging es nicht?

Autorisierungsfehler in Logs

Autorisierung bedeutet:

Ein Benutzer ist bekannt,
hat aber nicht die nötigen Rechte.

Typische Hinweise:

```
Access denied
Forbidden
Permission denied
Insufficient privileges
Missing role
Group required
Scope missing
```

Merksatz:

```
Authentifizierung prüft Identität.
Autorisierung prüft Rechte.
```

Mailserver-Logs

Mailserver-Logs helfen bei E-Mail-Problemen.

Sie zeigen:

```
- eingehende Verbindung
- ausgehende Verbindung
- Absender
- Empfänger
- SMTP-Statuscode
- Spamfilter-Entscheidung
- TLS-Fehler
- Zustellversuch
- Bounce
- Queue-Status
```

Merksatz:

```
Mailserver-Logs zeigen,
wo eine E-Mail hängen bleibt oder abgelehnt wird.
```

Datenbank-Logs

Datenbank-Logs helfen bei Anwendungsfehlern.

Typische Hinweise:

```
- Verbindung fehlgeschlagen
- Benutzer nicht berechtigt
- Passwort falsch
- Datenbank nicht erreichbar
- SQL-Fehler
- langsame Abfragen
- Locking-Probleme
- Speicher- oder Verbindungsgrenze erreicht
```

Merksatz:

```
HTTP 500 kann seine Ursache in der Datenbank haben.
```

Betriebssystem-Logs

Betriebssystem-Logs zeigen Systemereignisse.

Beispiele:

```
Dienst gestartet
Dienst gestoppt
Dienst abgestürzt
Speicher voll
Festplatte voll
Netzwerkinterface down
Treiberfehler
Berechtigungsfehler
Zeitproblem
Zertifikatproblem
```

Merksatz:

```
Systemlogs zeigen,
ob das Betriebssystem selbst Probleme meldet.
```

Anwendungslogs

Anwendungslogs sind oft die wichtigste Quelle bei Schicht-7-Problemen.

Sie zeigen zum Beispiel:

```
Konfigurationsfehler
fehlende Datei
Datenbankfehler
API-Fehler
Berechtigungsfehler
ungültiges Datenformat
ungültige Session
Fehler beim Start
Stacktrace
Timeout zu Backend
```

Merksatz:

```
Wenn Netzwerk steht,
aber Anwendung fehlschlägt,
Anwendungslogs prüfen.
```

Cloud-Logs

In Cloud-Umgebungen gibt es zusätzliche Logquellen.

Beispiele:

```
- Security Groups
- Network Security Groups
- Load Balancer Logs
- Cloud Firewall Logs
- IAM Logs
- Audit Logs
- DNS Logs
- API Gateway Logs
- Container Logs
- Kubernetes Events
```

Merksatz:

```
In Cloud-Umgebungen liegen Netzwerkentscheidungen oft in mehreren Diensten.
```

Container-Logs

Container-Logs zeigen Ausgaben der Anwendung im Container.

Typische Hinweise:

```
Dienst startet nicht.
Port ist belegt.
Datenbank nicht erreichbar.
Umgebungsvariable fehlt.
Berechtigung fehlt.
Volume fehlt.
DNS-Name im Docker-Netz falsch.
Backend nicht erreichbar.
Zertifikat fehlt.
```

Merksatz:

```
Container-Logs zeigen,
was die Anwendung im Container meldet.
```

Zeitstempel in Logs

Zeitstempel sind entscheidend.

Man muss prüfen:

```
Stimmen Uhrzeiten der Systeme?
Welche Zeitzone wird verwendet?
Ist NTP korrekt?
Passt der Fehlerzeitpunkt?
Sind Logs in UTC oder lokaler Zeit?
Sind Client,
Server
```

und Firewall zeitlich vergleichbar?

Merksatz:

Ohne korrekte Zeit sind Logs schwer vergleichbar.

NTP und Logs

NTP sorgt für korrekte Zeitsynchronisation.

Falsche Uhrzeiten verursachen Probleme bei:

Logvergleich
Zertifikaten
Kerberos
MFA
Tokens
Monitoring
Vorfallanalyse

Merksatz:

Korrekte Zeit ist Grundlage für sinnvolle Logauswertung.

Schweregrade in Logs

Logs haben oft Schweregrade.

Typische Stufen:

Stufe	Bedeutung
Debug	sehr detaillierte Diagnoseinformationen
Info	normale Information
Warning	Warnung, mögliches Problem
Error	Fehler
Critical	schwerer Fehler
Alert	sofortige Aufmerksamkeit nötig

Stufe	Bedeutung
Emergency	System praktisch nicht mehr nutzbar

Merksatz:

```
Nicht jede Warnung ist die Ursache,
aber jede Warnung ist ein Hinweis.
```

Debug-Logs

Debug-Logs sind sehr detailliert.

Vorteil:

```
liefern viele Informationen
```

Nachteil:

```
erzeugen große Datenmengen
können sensible Informationen enthalten
können Leistung beeinflussen
sind schwerer zu lesen
```

Debug sollte oft nur gezielt und zeitlich begrenzt aktiviert werden.

Merksatz:

```
Debug nur gezielt und vorübergehend nutzen.
```

Logrotation

Logrotation bedeutet:

```
alte Logdateien werden archiviert,
komprimiert
oder gelöscht,
damit Speicherplatz nicht voll läuft.
```

Wichtig:

```
Logs dürfen nicht unkontrolliert wachsen.
```

Problem:

```
Wenn Speicher voll läuft,
können Dienste ausfallen.
```

Merksatz:

```
Logrotation schützt vor volllaufenden Systemen.
```

Logaufbewahrung

Logaufbewahrung beschreibt, wie lange Logs gespeichert werden.

Dabei spielen eine Rolle:

```
- gesetzliche Vorgaben
- Datenschutz
- Sicherheitsanforderungen
- Speicherplatz
- Vorfallanalyse
- Unternehmensrichtlinien
```

Merksatz:

```
Logs so lange wie nötig,
aber nicht unnötig lange speichern.
```

Datenschutz bei Logs

Logs können personenbezogene oder sensible Daten enthalten.

Beispiele:

```
Benutzername
IP-Adresse
E-Mail-Adresse
Standort
Login-Zeit
Gerät
Fehlerdetails
Tokens
Session-Informationen
```

Deshalb:

```
Zugriff beschränken
Zweck beachten
Aufbewahrung regeln
sensible Daten vermeiden
Logs sicher speichern
```

Merksatz:

```
Logs sind oft personenbezogen und müssen geschützt werden.
```

Zentrale Logsammlung

In größeren Umgebungen werden Logs zentral gesammelt.

Vorteile:

```
- einheitliche Suche
- bessere Korrelation
- langfristige Auswertung
- Alarmierung
- Schutz vor Manipulation auf Einzelsystem
- bessere Vorfallanalyse
```

Beispiele für Konzepte:

```
Syslog
SIEM
Logserver
zentraler Monitoring-Stack
```

Merksatz:

```
Zentrale Logs erleichtern Analyse und Sicherheit.
```

Syslog

Syslog ist ein verbreitetes Verfahren, um Logs von Netzwerkgeräten und Servern zentral zu sammeln.

Typische Quellen:

```
Router
Switches
Firewalls
Linux-Systeme
Appliances
```

Merksatz:

```
Syslog sammelt Ereignisse zentral.
```

SIEM

SIEM steht für:

```
Security Information and Event Management
```

Ein SIEM sammelt, korreliert und bewertet sicherheitsrelevante Ereignisse.

Es kann helfen bei:

Angriffserkennung
Compliance
Vorfallanalyse
Alarmierung
Korrelation von Ereignissen
ungewöhnlichem Verhalten

Merksatz:

SIEM verbindet Logs zu sicherheitsrelevanten Erkenntnissen.

Korrelation

Korrelation bedeutet:

Ereignisse aus mehreren Quellen werden zusammen betrachtet.

Beispiel:

Firewall meldet blockierte Verbindung.
Webserver meldet viele 404.
Auth-Log meldet viele Loginfehler.
IDS meldet Angriffsmuster.

Zusammen kann daraus ein Angriff erkennbar werden.

Merksatz:

Einzelne Logs sind Hinweise,
korrelierte Logs ergeben Zusammenhang.

Monitoring

Monitoring überwacht Systeme und Dienste dauerhaft.

Es beantwortet Fragen wie:

```
Ist der Dienst erreichbar?
Ist der Server ausgelastet?
Ist Speicherplatz knapp?
Läuft der Prozess?
Ist das Zertifikat bald abgelaufen?
Ist die Latenz erhöht?
Gibt es Paketverlust?
Ist ein Standort offline?
```

Merksatz:

```
Monitoring erkennt Probleme,
bevor Benutzer sie melden.
```

Monitoring-Arten

Typische Monitoring-Arten:

```
- Verfügbarkeitsmonitoring
- Performance-Monitoring
- Netzwerkmonitoring
- Dienstmonitoring
- Logmonitoring
- Sicherheitsmonitoring
- Zertifikatsmonitoring
- Kapazitätsmonitoring
```

Merksatz:

```
Monitoring kann Verfügbarkeit,
Leistung,
Sicherheit
und Kapazität prüfen.
```

Verfügbarkeitsmonitoring

Verfügbarkeitsmonitoring prüft, ob ein System oder Dienst erreichbar ist.

Beispiele:

```
Ping erfolgreich?
TCP-Port offen?
HTTP-Status 200?
DNS antwortet?
VPN-Tunnel up?
Datenbank erreichbar?
```

Merksatz:

```
Verfügbarkeit bedeutet:
Dienst antwortet grundsätzlich.
```

Performance-Monitoring

Performance-Monitoring prüft Leistungswerte.

Beispiele:

```
CPU-Auslastung
RAM-Auslastung
Festplatten-I/O
Netzwerklast
Latenz
Paketverlust
Antwortzeit
Datenbankabfragezeit
```

Merksatz:

```
Performance-Monitoring zeigt,
ob ein Dienst langsam oder überlastet ist.
```

Netzwerkmonitoring

Netzwerkmonitoring prüft Netzwerkkomponenten.

Beispiele:

Switchports
Router
Firewalls
Access Points
VPN-Tunnel
WAN-Leitungen
Bandbreite
Interface-Fehler
Paketverlust
Latenz

Merksatz:

Netzwerkmonitoring zeigt Zustand der Infrastruktur.

Dienstmonitoring

Dienstmonitoring prüft konkrete Dienste.

Beispiele:

Webserver läuft?
Datenbank erreichbar?
DNS antwortet?
DHCP verfügbar?
Mailqueue wächst?
Reverse Proxy antwortet?
API liefert erwarteten Status?

Merksatz:

Dienstmonitoring prüft,
ob ein Dienst fachlich nutzbar ist.

Zertifikatsmonitoring

Zertifikatsmonitoring prüft TLS-Zertifikate.

Wichtige Fragen:

```
Wann läuft das Zertifikat ab?
Passt der Hostname?
Ist die Zertifikatskette gültig?
Wird das richtige Zertifikat ausgeliefert?
Ist die CA vertrauenswürdig?
```

Merksatz:

```
Zertifikate sollten überwacht werden,
bevor sie ablaufen.
```

Kapazitätsmonitoring

Kapazitätsmonitoring prüft, ob Ressourcen knapp werden.

Beispiele:

```
Speicherplatz
RAM
CPU
Bandbreite
Datenbankgröße
Loggröße
Anzahl Verbindungen
DHCP-Leases
Lizenzgrenzen
```

Merksatz:

```
Kapazitätsprobleme kündigen sich oft vorher an.
```

Alarmierung

Monitoring ist nur hilfreich, wenn wichtige Probleme auch gemeldet werden.

Alarmierung kann erfolgen über:

E-Mail
SMS
App
Dashboard
Ticket
Chat
Pager

Wichtig:

Nicht zu viele unnötige Alarme,
sonst werden wichtige Alarme ignoriert.

Merksatz:

Gute Alarmierung ist relevant,
verständlich
und handlungsfähig.

False Positive und False Negative

False Positive:

Alarm,
obwohl kein echtes Problem vorliegt.

False Negative:

Kein Alarm,
obwohl ein echtes Problem vorliegt.

Beides ist problematisch.

Merksatz:

Monitoring muss sinnvoll eingestellt und regelmäßig geprüft werden.

Schwellwerte

Schwellwerte legen fest, wann ein Alarm ausgelöst wird.

Beispiele:

```
CPU über 90 Prozent
Speicherplatz unter 10 Prozent frei
Zertifikat läuft in 14 Tagen ab
Ping-Verlust über 5 Prozent
Antwortzeit über 2 Sekunden
HTTP-Status nicht 200
```

Merksatz:

```
Schwellwerte müssen zum Dienst passen.
```

Trends

Monitoring zeigt nicht nur aktuelle Werte, sondern auch Entwicklungen.

Beispiele:

```
Speicherplatz wird jede Woche knapper.
Antwortzeiten steigen langsam.
Bandbreite ist montags überlastet.
Logdateien wachsen ungewöhnlich stark.
DHCP-Leases reichen bald nicht mehr.
```

Merksatz:

```
Trends helfen,
Probleme vor dem Ausfall zu erkennen.
```

Baseline

Eine Baseline beschreibt, was für ein System normal ist.

Beispiel:

```
normale CPU-Auslastung
normale Antwortzeit
normale Anzahl Verbindungen
normale DNS-Anfragen
normale Bandbreite
```

Ohne Baseline weiß man schwer, ob ein Wert auffällig ist.

Merksatz:

```
Baseline = normales Verhalten als Vergleichswert.
```

Dokumentation

Dokumentation beschreibt, wie ein System aufgebaut ist und wie es betrieben wird.

Wichtige Inhalte:

```
- Netzplan
- IP-Adressplan
- VLAN-Plan
- Firewall-Regeln
- NAT-Regeln
- DNS-Zonen
- DHCP-Scopes
- Serverrollen
- Dienste
- Zugangspfade
- Ansprechpartner
- Änderungen
- Notfallverfahren
```

Merksatz:

```
Gute Dokumentation beschleunigt Fehlersuche.
```

Netzplan

Ein Netzplan zeigt, wie Netzbereiche und Geräte verbunden sind.

Er enthält zum Beispiel:

```
Router
Switches
Firewalls
Server
VLANs
Standorte
VPNs
DMZ
Internetanschluss
IP-Netze
```

Merksatz:

```
Netzplan zeigt,
wie das Netzwerk aufgebaut ist.
```

IP-Adressplan

Ein IP-Adressplan zeigt, welche Netze und Adressen verwendet werden.

Beispiele:

```
192.168.10.0/24 Clients
192.168.20.0/24 Server
192.168.30.0/24 DMZ
192.168.40.0/24 Management
192.168.50.0/24 Gäste
```

Merksatz:

```
IP-Adressplan verhindert Verwechslungen und Doppelvergaben.
```

VLAN-Dokumentation

Eine VLAN-Dokumentation enthält:

VLAN-ID
Name
Subnetz
Gateway
DHCP-Scope
Zweck
zugehörige Switchports
Trunks
Firewall-Zone

Merksatz:

VLANs ohne Dokumentation führen schnell zu Fehlkonfigurationen.

Firewall- und NAT-Dokumentation

Dokumentiert werden sollten:

Quelle
Ziel
Dienst
Port
Protokoll
Richtung
Zone
NAT-Ziel
Zweck
Verantwortlicher
Ticket
Ablaufdatum bei temporären Regeln

Merksatz:

Firewall-Regeln ohne Zweck sind später schwer bewertbar.

DNS-Dokumentation

DNS-Dokumentation enthält:

Zonen
A-Records
AAAA-Records
CNAMEs
MX-Records
TXT-Records
interne und externe Namen
Split-DNS-Regeln
TTL
zuständige Systeme

Merksatz:

DNS-Dokumentation verhindert falsche Zielauflösungen.

DHCP-Dokumentation

DHCP-Dokumentation enthält:

Scope
Adressbereich
Ausschlüsse
Reservierungen
Lease-Zeit
Gateway-Option
DNS-Option
Relay-Adresse
VLAN-Zuordnung

Merksatz:

DHCP-Dokumentation erklärt,
warum Clients welche Konfiguration bekommen.

Änderungsdokumentation

Änderungen sollten nachvollziehbar sein.

Wichtige Angaben:

```
Was wurde geändert?
Warum wurde es geändert?
Wann wurde es geändert?
Wer hat es geändert?
Welche Systeme sind betroffen?
Wie wurde getestet?
Gibt es Rollback?
Gibt es ein Ticket?
```

Merksatz:

```
Ohne Änderungsdokumentation ist Fehlersuche nach Änderungen schwer.
```

Incident-Dokumentation

Bei Störungen sollte dokumentiert werden:

```
Startzeit
Endezeit
betroffene Systeme
betroffene Benutzer
Fehlerbild
Ursache
Maßnahmen
Lösung
Workaround
Kommunikation
Nacharbeiten
```

Merksatz:

```
Incident-Dokumentation hilft,
aus Fehlern zu lernen.
```

Root Cause Analysis

Root Cause Analysis bedeutet:

```
die eigentliche Ursache eines Problems finden.
```

Nicht nur:

```
Dienst neu starten
```

Sondern fragen:

```
Warum ist der Dienst abgestürzt?
Warum war Speicher voll?
Warum gab es keinen Alarm?
Warum wurde die Logrotation nicht eingerichtet?
```

Merksatz:

```
Root Cause Analysis sucht die Ursache hinter dem Symptom.
```

Post-Mortem

Ein Post-Mortem ist eine Nachbesprechung nach einer Störung.

Ziele:

```
Ursache verstehen
Ablauf rekonstruieren
Verbesserungen finden
Schuldzuweisungen vermeiden
Maßnahmen ableiten
Wiederholung verhindern
```

Merksatz:

```
Post-Mortem soll Systeme verbessern,
nicht Personen beschuldigen.
```

Lessons Learned

Lessons Learned sind Erkenntnisse aus einer Störung.

Beispiele:

```
Monitoring muss erweitert werden.
Zertifikate müssen überwacht werden.
Firewall-Regeln müssen dokumentiert werden.
Backups müssen getestet werden.
Change-Prozess muss angepasst werden.
Runbook muss erstellt werden.
```

Merksatz:

```
Lessons Learned machen aus Störungen Verbesserungen.
```

Runbook

Ein Runbook ist eine Schritt-für-Schritt-Anleitung für wiederkehrende Aufgaben oder Störungen.

Beispiele:

```
Webdienst neu starten
Zertifikat erneuern
VPN-Tunnel prüfen
DHCP-Scope erweitern
Firewall-Regel prüfen
Backup wiederherstellen
```

Merksatz:

```
Runbooks machen wiederkehrende Arbeiten sicherer und schneller.
```

Checkliste für Logauswertung

```
1. Fehlerzeitpunkt bestimmen.
2. Betroffene Systeme bestimmen.
```

3. Passende Logquelle auswählen.
4. Zeitfilter setzen.
5. Fehlermeldungen suchen.
6. Schweregrad beachten.
7. Ereignisse vor und nach dem Fehler prüfen.
8. Logs mehrerer Systeme vergleichen.
9. Zeitabweichungen beachten.
10. Ergebnis dokumentieren.

Merksatz:

Logs immer zeitlich und fachlich einordnen.

Checkliste für Monitoring

1. Wird der Dienst überwacht?
2. Wird der richtige Port geprüft?
3. Wird die Anwendung geprüft oder nur Ping?
4. Gibt es sinnvolle Schwellwerte?
5. Gibt es Alarmierung?
6. Werden Zertifikate überwacht?
7. Werden Ressourcen überwacht?
8. Werden Trends betrachtet?
9. Gibt es zu viele Fehlalarme?
10. Werden Alarme bearbeitet?

Merksatz:

Monitoring muss den Dienst wirklich abbilden.

Checkliste für Dokumentation

1. Netzplan aktuell?
2. IP-Adressplan aktuell?
3. VLANs dokumentiert?
4. Firewall-Regeln dokumentiert?
5. NAT-Regeln dokumentiert?

6. DNS-Einträge dokumentiert?
7. DHCP-Scopes dokumentiert?
8. Verantwortliche bekannt?
9. Änderungen dokumentiert?
10. Notfallverfahren vorhanden?

Merksatz:

Dokumentation ist ein Werkzeug,
nicht nur Verwaltung.

Typische Fehler bei Logs und Monitoring

Häufige Fehler:

Logs werden nicht aktiviert.
Logs werden zu kurz gespeichert.
Logs laufen voll.
Zeitstempel stimmen nicht.
falsche Zeitzone wird übersehen.
Monitoring prüft nur Ping.
Zertifikate werden nicht überwacht.
Alarme gehen an niemanden.
zu viele Fehlalarme entstehen.
Dokumentation ist veraltet.
Änderungen werden nicht dokumentiert.
Root Cause wird nicht gesucht.

Merksatz:

Logs und Monitoring müssen gepflegt werden.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Warum sind Logs bei der Fehlersuche wichtig?
- Welche Informationen enthält ein Firewall-Log?
- Warum ist die Uhrzeit bei Logs wichtig?
- Warum ist NTP für Logauswertung wichtig?
- Was ist Monitoring?
- Was ist der Unterschied zwischen Verfügbarkeits- und Performance-Monitoring?
- Warum reicht Ping-Monitoring nicht immer aus?
- Was ist ein Schwellwert?
- Was ist eine Baseline?
- Warum müssen Zertifikate überwacht werden?
- Was gehört in eine Netzwer dokumentation?
- Warum ist Änderungsdokumentation wichtig?
- Was ist eine Root Cause Analysis?
- Was ist ein Runbook?
- Warum können Logs personenbezogene Daten enthalten?

Typische Prüfungsfallen

Logs zeigen Ereignisse,
nicht automatisch die Ursache.

Monitoring zeigt Zustand über Zeit.

Ping-Monitoring reicht nicht für Anwendungserfolg.

Firewall-Logs zeigen getroffene Regeln.

Kein Log kann auch falschen Weg bedeuten.

Zeitstempel müssen vergleichbar sein.

NTP ist wichtig für Logs,
Zertifikate
und Authentifizierung.

Debug-Logs nur gezielt aktivieren.

Logs können sensible Daten enthalten.

Logrotation verhindert volle Datenträger.

Zentrale Logsammlung erleichtert Analyse.

SIEM korreliert sicherheitsrelevante Ereignisse.

Monitoring braucht sinnvolle Schwellwerte.

Zu viele Fehlalarme führen zu Alarmmüdigkeit.

Baseline zeigt normales Verhalten.

Dokumentation muss aktuell sein.

Änderung ohne Dokumentation erschwert Fehlersuche.

Root Cause ist wichtiger als nur Neustart.

Runbooks helfen bei wiederkehrenden Aufgaben.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Log	Ereignisprotokoll
Logquelle	System oder Dienst, der Logs erzeugt
Firewall-Log	Protokoll von erlaubtem oder blockiertem Verkehr
Systemlog	Betriebssystemereignisse
Anwendungslog	Meldungen einer Anwendung
Debug-Log	sehr detaillierte Diagnoseausgabe
Logrotation	Archivieren oder Löschen alter Logs
Logaufbewahrung	Zeitraum der Speicherung
Syslog	Verfahren zur zentralen Logsammlung
SIEM	System zur Sicherheitsauswertung von Logs
Korrelation	Zusammenführen mehrerer Ereignisse
Monitoring	dauerhafte Überwachung

Begriff	Kurze Erklärung
Schwellwert	Grenze für Alarmierung
False Positive	Fehlalarm
False Negative	fehlender Alarm trotz Problem
Baseline	normales Verhalten als Vergleich
Netzplan	grafische Netzdokumentation
IP-Adressplan	Übersicht verwendeter Netze und Adressen
Änderungsdokumentation	Nachweis von Änderungen
Incident	Störung oder Sicherheitsvorfall
Root Cause Analysis	Suche nach eigentlicher Ursache
Post-Mortem	Nachbesprechung nach Störung
Lessons Learned	Erkenntnisse zur Verbesserung
Runbook	Schritt-für-Schritt-Anleitung

IHK-sichere Kurzformulierung

Logs, Monitoring und Dokumentation sind zentrale Bestandteile der Netzwerkfehlersuche. Logs zeigen Ereignisse und Entscheidungen von Systemen, Diensten, Firewalls, Anwendungen und Betriebssystemen. Monitoring überwacht Verfügbarkeit, Leistung, Kapazität und Sicherheit über einen längeren Zeitraum und kann Probleme frühzeitig melden. Wichtig sind korrekte Zeitstempel, NTP, sinnvolle Schwellwerte, Logrotation, Datenschutz und zentrale Logsammlung. Dokumentation wie Netzplan, IP-Adressplan, VLAN-Plan, Firewall-Regeln, NAT-Regeln, DNS-Einträge und DHCP-Scopes hilft, Fehler schneller einzugrenzen. Nach Störungen sollten Ursache, Maßnahmen und Verbesserungen dokumentiert werden.

Merksätze

Mitschnitt zeigt Verkehr.

Logs zeigen Ereignisse.

Monitoring zeigt Zustand über Zeit.

Dokumentation zeigt Aufbau und Änderungen.

Firewall-Logs zeigen getroffene Regeln.

DNS-Logs zeigen Namensauflösung.

DHCP-Logs zeigen Adressvergabe.

VPN-Logs zeigen Tunnel und Anmeldung.

Webserver-Logs zeigen HTTP-Antworten.

Reverse-Proxy-Logs zeigen Backend-Probleme.

Authentifizierungslogs zeigen Loginprobleme.

Anwendungslogs zeigen Schicht-7-Fehler.

Zeitstempel müssen stimmen.

NTP ist wichtig für Logvergleich.

Debug nur gezielt aktivieren.

Logs können sensible Daten enthalten.

Logrotation verhindert volle Datenträger.

Zentrale Logs erleichtern Analyse.

SIEM korreliert Sicherheitsereignisse.

Monitoring erkennt Probleme früh.

Ping-Monitoring reicht oft nicht.

Schwellwerte müssen sinnvoll sein.

Baseline zeigt normales Verhalten.

Zertifikate überwachen.

Netzplan aktuell halten.

IP-Adressplan aktuell halten.

Firewall- und NAT-Regeln dokumentieren.

Änderungen dokumentieren.

Root Cause suchen,
nicht nur Symptom beheben.

Runbooks helfen bei wiederkehrender Fehlersuche.