18.4 Merksätze und Prüfungswissen zur Prüfungsvorbereitung

Diese Seite fasst die wichtigsten Punkte zur Prüfungsvorbereitung zusammen.

Sie dient als Abschluss für das Kapitel Prüfungsvorbereitung und Wiederholung.

Im Mittelpunkt stehen:

- Aufgaben richtig lesen
- Operatoren beachten
- Signalwörter erkennen
- Fehlerbilder einordnen
- Fachbegriffe sauber verwenden
- Rechenaufgaben systematisch lösen
- Antworten kurz und prüfungssicher formulieren

Merksatz:

Prüfungsvorbereitung heißt:
Wissen verstehen,
anwenden
und sauber formulieren.

Wichtigste Grundregel

Die wichtigste Regel in der Prüfung lautet:

Erst die Aufgabe verstehen,
dann antworten.

Nicht sofort auf bekannte Stichwörter reagieren.

Immer prüfen:

Was wird wirklich gefragt?

Welche Informationen sind gegeben?

Welche Einschränkungen stehen in der Aufgabe?

Wie viele Antworten werden verlangt?

Soll ich nennen,
erklären,
begründen,
vergleichen
oder berechnen?

Merksatz:

Die Aufgabenstellung entscheidet,
wie die Antwort aussehen muss.

Operatoren sicher beachten

Operator	Erwartung
nennen	kurze Begriffe oder Stichpunkte
beschreiben	sachlich darstellen
erklären	Zusammenhang deutlich machen
begründen	Warum nennen
vergleichen	Unterschiede und Gemeinsamkeiten darstellen
berechnen	rechnerisch ermitteln
bewerten	fachlich einschätzen
zuordnen	passend einordnen

Merksatz:

Wer den Operator ignoriert,
beantwortet schnell die falsche Frage.

Antworten nach Operator formulieren

Beispiel „nennen“:

Zwei Vorteile von VLANs sind logische Netztrennung
und kleinere Broadcast-Domänen.

Beispiel „erklären“:

VLANs trennen ein physisches Netzwerk logisch in mehrere getrennte Netzbereiche.
Dadurch können Geräte verschiedener Abteilungen oder Sicherheitszonen getrennt werden.

Beispiel „begründen“:

VLANs erhöhen die Struktur und Sicherheit,
weil Broadcastverkehr begrenzt
und Zugriffe zwischen Netzbereichen gezielter geregelt werden können.

Merksatz:

Gleicher Begriff,
andere Antworttiefe je nach Operator.

Signalwörter erkennen

Signalwörter zeigen oft direkt die Richtung der Lösung.

Signalwort oder Fehlerbild	Wahrscheinliches Thema
IP erreichbar, Name nicht	DNS
169.254.x.x	DHCP
lokal erreichbar, extern nicht	Gateway, NAT, Firewall
Host erreichbar, Dienst nicht	Port, Dienst, Firewall
Anmeldung fehlgeschlagen	Authentifizierung
Zugriff verweigert	Autorisierung, Rechte
Zertifikatswarnung	Zertifikat, Hostname, Zeit
nur ein VLAN betroffen	VLAN, Routing, Firewall
nach Update defekt	Change, Version, Kompatibilität
viele fehlgeschlagene Logins	Brute Force, Passwortangriff
verschlüsselte Dateien	Ransomware

Signalwort oder Fehlerbild	Wahrscheinliches Thema
gestohlene Zugangsdaten	Phishing, Credential Theft
Backup nicht lesbar	Restore-Test, Konsistenz, Schlüssel

Merksatz:

> Signalwörter sind Hinweise,
> keine Zufälle.

Typische Fehlerbilder sicher zuordnen

Fehlerbild	Erste Prüfung
kein Netzwerk	Kabel, WLAN, Link, IP
kein Internet	Gateway, DNS, NAT, Firewall
Name funktioniert nicht	DNS
falsche automatische IP	DHCP
Dienst nicht erreichbar	Port, Dienststatus, Firewall
Datei nicht zugreifbar	Rechte, Gruppe, ACL
Login nicht möglich	Konto, Passwort, MFA, Verzeichnisdienst
Webseite 404	URL, Pfad, Webserver
Webseite 500	Anwendung, Backend, Logs
Zertifikatsfehler	Ablaufdatum, Hostname, Kette, Uhrzeit
langsame Verbindung	Latenz, Paketverlust, Last, DNS

Merksatz:

> Fehlerbild zuerst einordnen,
> dann gezielt prüfen.

OSI-Modell als Prüfungswerkzeug

Das OSI-Modell hilft, Fehler strukturiert einzugrenzen.

Schicht	Typische Fehler
1	Kabel defekt, kein Link, falscher Stecker
2	VLAN falsch, MAC-Problem, ARP, Switchport

Schicht	Typische Fehler
3	IP falsch, Gateway falsch, Routingfehler
4	Port blockiert, TCP/UDP-Problem
5	Sitzung abgelaufen, Sessionproblem
6	TLS, Zertifikat, Codierung
7	DNS, DHCP, HTTP, SMTP, SMB

Merksatz:

> Von unten nach oben prüfen:
> physisch,
> Netzwerk,
> Dienst,
> Anwendung.

MAC, IP und Port nicht verwechseln

Begriff	Schicht	Aufgabe
MAC-Adresse	2	lokale Zustellung im LAN
IP-Adresse	3	logische Adressierung über Netze
Port	4	Zuordnung zu einem Dienst

Merksatz:

> MAC findet lokal.
> IP findet das Zielnetz.
> Port findet den Dienst.

DNS und DHCP nicht verwechseln

DNS:

> löst Namen in IP-Adressen auf

DHCP:

verteilt IP-Konfiguration automatisch

Beispiel DNS-Problem:

IP funktioniert,
Name nicht.

Beispiel DHCP-Problem:

Client erhält 169.254.x.x
oder keine passende IP-Konfiguration.

Merksatz:

DNS beantwortet:
Wie heißt die IP?

DHCP beantwortet:
Welche IP bekomme ich?

Gateway und DNS unterscheiden

Gateway:

Weg in andere Netze

DNS:

Namensauflösung

Typisches Gateway-Problem:

lokales Netz erreichbar,
Internet nicht

Typisches DNS-Problem:

IP erreichbar,

Name nicht

Merksatz:

Gateway ist der Weg.

DNS ist das Telefonbuch.

TCP und UDP sicher unterscheiden

Merkmal	TCP	UDP
Verbindung	verbindungsorientiert	verbindungslos
Zustellung	zuverlässig	keine eingebaute Garantie
Reihenfolge	wird gesichert	nicht garantiert
Overhead	höher	geringer
Einsatz	vollständige Datenübertragung	schnelle oder zeitkritische Kommunikation

Merksatz:

TCP = zuverlässig.

UDP = schlank.

Wichtige Ports sicher können

Dienst	Port
FTP	TCP 21
SSH	TCP 22
Telnet	TCP 23
SMTP	TCP 25
DNS	UDP/TCP 53
DHCP Server	UDP 67
DHCP Client	UDP 68
HTTP	TCP 80
POP3	TCP 110

Dienst	Port
IMAP	TCP 143
HTTPS	TCP 443
SMB	TCP 445
SMTPS	TCP 465
IMAPS	TCP 993
POP3S	TCP 995
RDP	TCP 3389

Merksatz:

> Ports immer mit Dienst und Protokoll lernen.

Subnetting-Prüfungswissen

Bei Subnetting immer gleich vorgehen:

> 1. Präfix bestimmen.
> 2. Hostbits berechnen.
> 3. Adressanzahl berechnen.
> 4. nutzbare Hosts berechnen.
> 5. Blockgröße bestimmen.
> 6. Netzadresse finden.
> 7. Broadcastadresse finden.
> 8. erste und letzte nutzbare Adresse bestimmen.

Formel:

> nutzbare Hosts = 2 hoch Hostbits minus 2

Merksatz:

> Subnetting wird einfacher,
> wenn die Reihenfolge immer gleich bleibt.

Subnetting-Merksätze

IPv4 hat 32 Bit.

Präfix gibt die Netzbits an.

Hostbits = 32 minus Präfix.

Mehr Netzbits bedeuten kleinere Netze.

Mehr Hostbits bedeuten mehr Hosts.

Netzadresse ist die erste Adresse.

Broadcastadresse ist die letzte Adresse.

Erste nutzbare Adresse = Netzadresse plus 1.

Letzte nutzbare Adresse = Broadcastadresse minus 1.

Pro zusätzlichem Netzbit halbiert sich die Hostanzahl.

Pro zusätzlichem Hostbit verdoppelt sich die Hostanzahl.

Merksatz:

Präfix größer:
Netz kleiner.

Präfix kleiner:
Netz größer.

NAT, PAT und Portweiterleitung unterscheiden

NAT:

übersetzt IP-Adressen

PAT:

übersetzt zusätzlich Ports,
damit mehrere interne Clients eine öffentliche IP nutzen können

Portweiterleitung:

leitet eingehenden Verkehr auf einen internen Dienst weiter

Merksatz:

NAT übersetzt Adressen.
PAT unterscheidet über Ports.
Portweiterleitung veröffentlicht einen Dienst.

Firewall-Prüfungswissen

Eine Firewall filtert Verkehr anhand von Regeln.

Typische Regelbestandteile:

Quelle
Ziel
Port
Protokoll
Richtung
Aktion
Zustand
Zweck

Sichere Grundregel:

Default Deny

Das bedeutet:

Standardmäßig blockieren,
nur benötigten Verkehr erlauben.

Merksatz:

Firewall-Regeln so eng wie möglich formulieren.

VPN-Prüfungswissen

Remote-Access-VPN:

einzelner Benutzer verbindet sich mit einem Netzwerk

Site-to-Site-VPN:

zwei Netzwerke oder Standorte werden verbunden

Wichtig:

VPN verschlüsselt den Transportweg,
ersetzt aber keine Rechteverwaltung.

Merksatz:

VPN schützt Verbindung,
nicht automatisch jede Berechtigung.

Cloud-Prüfungswissen

IaaS:

virtuelle Infrastruktur

PaaS:

Plattform für Anwendungen

SaaS:

fertige Anwendung

Public Cloud:

öffentlich angebotene Cloud

Private Cloud:

Cloud für eine Organisation

Hybrid Cloud:

Kombination aus lokal und Cloud

Multi Cloud:

Nutzung mehrerer Cloud-Anbieter

Merksatz:

IaaS,
PaaS
und SaaS beschreiben Servicemodelle.

Public,
Private,
Hybrid
und Multi Cloud beschreiben Bereitstellungsmodelle.

Shared Responsibility

Beim Shared-Responsibility-Modell teilen sich Cloud-Anbieter und Kunde die Verantwortung.

Anbieter:

Infrastruktur der Cloud

Kunde:

Daten
Identitäten
Zugriffe
Konfigurationen
Anwendungen je nach Modell

Merksatz:

Cloud-Anbieter übernimmt nicht automatisch alles.

Sicherheitsbegriffe sicher unterscheiden

Begriff	Bedeutung
Vertraulichkeit	Schutz vor unberechtigtem Lesen
Integrität	Schutz vor unbemerkter Veränderung
Verfügbarkeit	Nutzbarkeit von Systemen und Daten
Authentizität	Echtheit einer Identität oder Nachricht
Nichtabstreitbarkeit	Nachweisbarkeit einer Handlung
Schwachstelle	ausnutzbare Lücke
Bedrohung	mögliches schädliches Ereignis
Risiko	Wahrscheinlichkeit und Auswirkung
Maßnahme	reduziert Risiko

Merksatz:

Schwachstelle ist die Lücke.
Bedrohung ist das Ereignis.
Risiko ist die bewertete Gefahr.

Angriffe sicher zuordnen

Angriff	Typisches Ziel
Phishing	Zugangsdaten, Identitäten
Ransomware	Verfügbarkeit, oft auch Vertraulichkeit

Angriff	Typisches Ziel
DDoS	Verfügbarkeit
Man-in-the-Middle	Vertraulichkeit und Integrität
SQL Injection	Datenbank
XSS	Browser anderer Benutzer
CSRF	gültige Sitzung
Brute Force	Passwort
Credential Stuffing	wiederverwendete Zugangsdaten
Spoofing	Identität oder Herkunft

Merksatz:

> Angriff immer dem Ziel und Schutzziel zuordnen.

Schutzmaßnahmen sicher zuordnen

Risiko	passende Maßnahme
gestohlenes Passwort	MFA
zu viele Rechte	Least Privilege
Malware	EDR, Patchmanagement
Ransomware	Backup, Immutable Backup, Segmentierung
DDoS	DDoS-Schutz, CDN, Rate Limiting
unsichere Freigaben	Rechteprüfung, Ablaufdatum
fehlende Nachvollziehbarkeit	Logging, SIEM
Fehlkonfiguration	Change Management
unsichere Benutzer	Schulung, Awareness
veraltete Software	Patchmanagement

Merksatz:

> Maßnahme muss direkt zum Risiko passen.

Authentifizierung und Autorisierung

Authentifizierung:

Wer bist du?

Autorisierung:

Was darfst du?

Beispiel:

Benutzer meldet sich mit Passwort und MFA an.
Danach wird geprüft,
ob er auf einen Ordner zugreifen darf.

Merksatz:

Erst Identität,
dann Rechte.

Least Privilege und Need to Know

Least Privilege:

nur notwendige Rechte

Need to Know:

nur notwendige Informationen

Beispiel:

Ein Supportmitarbeiter braucht vielleicht Zugriff auf Gerätedaten,
aber nicht auf Gehaltsdaten.

Merksatz:

Least Privilege begrenzt Rechte.
Need to Know begrenzt Informationen.

Backup, Replikation und Synchronisation unterscheiden

Backup:

wiederherstellbare Sicherung alter Zustände

Replikation:

aktuelle Kopie auf anderem System

Synchronisation:

Abgleich zwischen Speicherorten

Risiko:

Fehler,
Löschung
oder Ransomware können bei Replikation oder Synchronisation mit übertragen werden.

Merksatz:

Sync und Replikation sind kein Backup.

RPO und RTO

RPO:

maximal akzeptabler Datenverlust

RTO:

maximal akzeptable Wiederherstellungszeit

Beispiel:

RPO 1 Stunde:
maximal 1 Stunde Datenverlust

RTO 4 Stunden:
Dienst soll spätestens nach 4 Stunden wieder laufen

Merksatz:

RPO = Datenverlust.
RTO = Zeit bis Wiederherstellung.

Logging, Monitoring und Alerting unterscheiden

Logging:

Ereignisse werden aufgezeichnet

Monitoring:

Zustände werden überwacht

Alerting:

bei kritischen Zuständen wird alarmiert

Reporting:

Zustände werden über einen Zeitraum ausgewertet

Merksatz:

Logs zeigen Ereignisse.
Monitoring zeigt Zustände.
Alerting meldet Probleme.

Wichtige Befehle sicher einordnen

Aufgabe	Werkzeug
IP-Konfiguration Windows	ipconfig
IP-Konfiguration Linux	ip addr
Routing Windows	route print
Routing Linux	ip route
DNS prüfen	nslookup, dig
Erreichbarkeit prüfen	ping
Weg verfolgen	tracert, traceroute
Verbindungen anzeigen	netstat, ss
Webdienst prüfen	curl
Linux-Dienst prüfen	systemctl
Linux-Logs prüfen	journalctl
Windows-Logs prüfen	Ereignisanzeige

Merksatz:

> Befehle liefern Fakten,
> keine Vermutungen.

Typische Prüfungsfallen

> DNS und DHCP verwechseln.
>
> Gateway und DNS verwechseln.
>
> MAC,
> IP
> und Port verwechseln.
>
> TCP und UDP verwechseln.
>
> NAT,
> PAT
> und Portweiterleitung verwechseln.
>
> VLAN und Subnetz gleichsetzen.

Firewall und Router verwechseln.

Authentifizierung und Autorisierung verwechseln.

Backup,
Replikation
und Synchronisation verwechseln.

RPO und RTO verwechseln.

SFTP und FTPS verwechseln.

IDS und IPS verwechseln.

Redundanz als Backup bezeichnen.

Snapshot als vollständiges Backup bezeichnen.

ping als vollständigen Diensttest verstehen.

Merksatz:

Prüfungsfallen sind oft Begriffsfallen.

Gute Antwortstruktur bei Fehlersuche

Struktur:

Ursache
Begründung
Prüfung

Beispiel:

Wahrscheinlich liegt ein DNS-Problem vor,
da die IP-Adresse erreichbar ist,
der Name aber nicht aufgelöst wird.

Der DNS-Server und der DNS-Eintrag sollten mit nslookup oder dig geprüft werden.

Merksatz:

Fehlerantwort:
Ursache,
Begründung,
Prüfung.

Gute Antwortstruktur bei Sicherheitsfragen

Struktur:

Risiko
Maßnahme
Wirkung

Beispiel:

Das Risiko besteht im Missbrauch gestohlener Zugangsdaten.
Durch MFA reicht ein gestohlenes Passwort allein nicht mehr aus.
Dadurch wird die Wahrscheinlichkeit eines unberechtigten Zugriffs reduziert.

Merksatz:

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Gute Antwortstruktur bei Vergleichen

Struktur:

Gemeinsamkeit
Unterschied
Beispiel

Beispiel:

```
TCP und UDP sind Transportprotokolle.
TCP ist verbindungsorientiert und zuverlässig,
UDP ist verbindungslos und hat weniger Overhead.
TCP wird zum Beispiel bei HTTPS genutzt,
UDP häufig bei DNS oder VoIP.
```

Merksatz:

```
Vergleich:
Gemeinsamkeit,
Unterschied,
Beispiel.
```

Gute Antwortstruktur bei Berechnungen

Struktur:

```
gegebene Werte
Formel oder Regel
Rechenschritt
Ergebnis mit Einheit
Plausibilitätsprüfung
```

Beispiel:

```
Bei /27 gibt es 5 Hostbits.
2 hoch 5 ergibt 32 Adressen.
Davon sind 30 nutzbar,
weil Netzadresse und Broadcastadresse nicht für Hosts genutzt werden.
```

Merksatz:

```
Berechnung immer mit Bedeutung des Ergebnisses angeben.
```

Letzte Prüfungsminute

Kurz vor Abgabe prüfen:

```
Habe ich alle Teilfragen beantwortet?

Habe ich die geforderte Anzahl genannt?

Habe ich Einheiten ergänzt?

Habe ich Fachbegriffe sauber verwendet?

Habe ich DNS und DHCP nicht verwechselt?

Habe ich RPO und RTO nicht verwechselt?

Habe ich bei Subnetting Netzadresse und Broadcast geprüft?

Habe ich bei Sicherheitsfragen die Maßnahme begründet?

Habe ich bei Fehlersuche eine Prüfung genannt?
```

Merksatz:

```
Die letzte Kontrolle verhindert einfache Punktverluste.
```

IHK-sichere Gesamtformulierung

Für die Prüfung ist entscheidend, Aufgabenstellungen genau zu lesen, Operatoren zu beachten und technische Hinweise richtig einzuordnen. Netzwerkfehler sollten systematisch nach OSI-Modell geprüft werden: physische Verbindung, IP-Konfiguration, Gateway, DNS, Routing, Firewall, Dienst und Anwendung. Wichtige Begriffe wie MAC-Adresse, IP-Adresse, Port, DNS, DHCP, TCP, UDP, NAT, PAT, Authentifizierung, Autorisierung, Backup, Replikation, RPO und RTO müssen sauber unterschieden werden. Gute Antworten sind kurz, fachlich korrekt und begründet. Bei Fehlersuche werden Ursache, Begründung und Prüfung genannt. Bei Sicherheitsfragen werden Risiko, Maßnahme und Wirkung verbunden.

Wichtigste Merksätze

```
Erst Aufgabe verstehen,
dann antworten.
```

Operator beachten.

Signalwörter erkennen.

Fehlerbild einordnen.

OSI als Fehlersuche nutzen.

MAC ist lokal.

IP ist logisch.

Port ist Dienst.

DNS löst Namen auf.

DHCP verteilt Konfiguration.

Gateway führt in andere Netze.

TCP ist zuverlässig.

UDP ist schlank.

NAT übersetzt Adressen.

PAT nutzt Ports.

Portweiterleitung veröffentlicht Dienste.

Firewall filtert Verkehr.

VPN schützt Verbindung.

Cloud bedeutet geteilte Verantwortung.

Vertraulichkeit schützt vor Mitlesen.

Integrität schützt vor Manipulation.

Verfügbarkeit schützt Nutzbarkeit.

MFA schützt gegen Passwortmissbrauch.

Least Privilege begrenzt Rechte.

Backup ist Wiederherstellungsvorsorge.

Replikation ist kein Backup.

Synchronisation ist kein Backup.

RPO ist Datenverlust.

RTO ist Wiederherstellungszeit.

Logging zeigt Ereignisse.

Monitoring zeigt Zustände.

Alerting meldet Probleme.

Befehle liefern Fakten.

Prüfungsfallen sind oft Begriffsfallen.

Fehlerantwort:
Ursache,
Begründung,
Prüfung.

Sicherheitsantwort:
Risiko,
Maßnahme,
Wirkung.

Vergleich:
Gemeinsamkeit,
Unterschied,

Beispiel.

Berechnung:
Regel,
Ergebnis,
Einheit.

Kurz,
fachlich,
begründet.