

# 1

## Ganzheitliche Aufgabe I Fachqualifikationen

### Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.). Wird eine bestimmte Anzahl verlangt (z. B. „Nennen Sie fünf Merkmale ...“), so ist bei Aufzählung von fünf richtigen Merkmalen die volle vorgesehene Punktzahl zu geben, auch wenn im Lösungshinweis mehr als fünf Merkmale genannt sind. Bei Angabe von Teilpunkten in den Lösungshinweisen sind diese auch für richtig erbrachte Teilleistungen zu geben.

In den Fällen, in denen vom Prüfungsteilnehmer

- keiner der sechs Handlungsschritte ausdrücklich als „nicht bearbeitet“ gekennzeichnet wurde,
- der 6. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 5 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 6. Handlungsschritt soll in diesen Fällen allein wegen des Verstoßes gegen die Formvorschrift nicht erfolgen!

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1 =	100 – 92 Punkte	Note 2 =	unter	92 – 81 Punkte
Note 3 =	unter 81 – 67 Punkte	Note 4 =	unter	67 – 50 Punkte
Note 5 =	unter 50 – 30 Punkte	Note 6 =	unter	30 – 0 Punkte

## 1. Handlungsschritt (20 Punkte)

a) 2 Punkte, 2 x 1 Punkt

Netzwerkschicht (3)

Transportschicht (4)

ba) 2 Punkte

ETH0 (oder: die äußere, dem Internet zugewandte Netzwerkkarte)

bb) 4 Punkte

egal: Verbindungsanfrage aus dem Internet möglich (Aufbau einer TCP-Verbindung)

ja: Verbindungsanfrage aus dem Internet nicht möglich (nur Antworten)

bc) 6 Punkte, 6 x 1 Punkt

Nr.

Regel

- 1 Verbindungsanfrage eines Internet-Clients an den Web-Server weiterleiten
- 2 Antwort des Web-Servers an einen Internet-Client weiterleiten
- 3 Verbindungsanfrage eines LAN-Clients zum Versand von E-Mails an den Mail-Server weiterleiten
- 4 Antwort des Mail-Servers beim Versand von E-Mails an den LAN-Client weiterleiten
- 5 Verbindungsanfrage eines LAN-Clients zum Abruf von E-Mails an den Mail-Server weiterleiten
- 6 Antwort des Mail-Servers beim Abruf von E-Mails an den LAN-Client weiterleiten
- 9 Alle anderen Datenpakete blockieren

bd) 6 Punkte

Nr.	Richtung	Quell-IP	Ziel-IP	Protokoll	Quell-Port	Ziel-Port	Ack-Flag	Aktion
7	rein	egal	DMZ-www	TCP	> 1023	21	egal	weiterleiten
8	raus	DMZ-www	egal	TCP	21	> 1023	ja	weiterleiten

## 2. Handlungsschritt (20 Punkte)

a) 4 Punkte

- Auf dem Terminal-Server sind alle Anwendungsprogramme installiert und werden dort ausgeführt.
- Ein Terminal-Client ist nur Ein- und Ausgabegerät.

b) 4 Punkte

Anwendungsprogramme müssen nur auf dem Terminal-Server installiert und gepflegt werden.

c) 4 Punkte

Da die Programme auf dem Server ausgeführt werden, ist eine Aufrüstung der Terminal-Clients nicht erforderlich.

d) 4 Punkte

Fällt der Terminal-Server oder das Netzwerk aus, kann an den Clients nicht mehr lokal gearbeitet werden, da auf den Clients keine Anwendungsprogramme installiert sind.

e) 4 Punkte

39 Terminal-Clients

$$1\,024\text{ MB} \cdot 0,7 = 716,8\text{ MB}$$

$$(716,8\text{ MB} - 128\text{ MB}) / 15\text{ MB} = 39,25 \Rightarrow 39\text{ Benutzer}$$



### 3. Handlungsschritt (20 Punkte)

aa) 2 Punkte, 2 x 1 Punkt

Vorteile

- Kein spezieller Raid-Controller notwendig
- Festplatten-Cache bleibt aktiviert

Nachteile

- Abhängigkeit vom Betriebssystem
- Datenverlust bei Systemabsturz

ab) 3 Punkte, 3 x 1 Punkt

Beispiel:IDE
– Fibre Channel
– SCSI
– iSCSI
– S-ATA
– SAS
– FICON, ESCON

b) 2 Punkte

Aufteilung der Platten in zusammenhängende, gleich große Blöcke. Die Anordnung der Blöcke zu einer großen „Festplatte“ ist alternierend auf den realen Festplatten. Dadurch höhere Transferraten der Daten durch paralleles Schreiben und Lesen auf mehreren zusammengeschlossenen Festplatten.

ca) 3 Punkte, 3 x 1 Punkte

- Übertragung von Fehlern auch auf Spiegelplatte
- Beschädigung der Spiegelung bei Systemabsturz möglich
- Inkonsistente Daten durch Transaktionsabbruch
- Versehentliche Löschung von Daten
- Zerstörung von Festplatten (z. B. durch Brand)
- Diebstahl von Festplatten

cb) 2 Punkte

Höherer Kapazitätsverlust (immer 50 %), bei RAID 5 von Anzahl der Festplatten abhängig, jedoch maximal 33 %

da) 1 Punkt

1 Festplatte

db) 3 Punkte

- Der Inhalt einer unsicheren Platte wird auf eine Hot-Spare-Platte geschrieben, damit die unsichere Platte ausgewechselt werden kann, ohne dass der Betrieb unterbrochen werden muss.
- S.M.A.R.T. ermittelt anhand der Fehlerkorrekturstatistik Platten, bei denen ein Ausfall droht.

dc) 2 Lösungen möglich

Lösung A (4 Punkte)

320 GB

$$160 \text{ GB} \cdot (3 - 1) = 320 \text{ GB}$$

$$\text{Gesamtkapazität} = s \cdot (n - 1)$$

s = kleinste Platte im Array

n = Anzahl der Platten im Array

Lösung B (2 Punkte)

228 GB

$$76 \text{ GB} \cdot (4 - 1) = 228 \text{ GB}$$

$$\text{Gesamtkapazität} = s \cdot (n - 1)$$

s = kleinste Platte im Array

n = Anzahl der Platten im Array

#### 4. Handlungsschritt (20 Punkte)

a) 4 Punkte

Mit den Nutzdaten werden u. a. übertragen

- Protokolldaten Overhead
- Header-Informationen
- Redundante Daten zur Fehlerkorrektur

b) 2 Punkte

Übertragungsgeschwindigkeit von 480 MBit/s wird garantiert.

c) 2 Punkte

- 2 Kabel a 5 m verbunden mit einem aktiven USB-Hub.

Oder:

- Einsatz einer aktiven USB-Verlängerung mit integriertem Signalverstärker.

da) 4 Punkte

$$(100\text{mA} + 100\text{mA} + 150\text{mA} + 450\text{mA}) \cdot 5\text{V} = 4\,000\text{ mW} = 4\text{ W}$$

db) 2 Punkte

$$0,5\text{ A} \times 5\text{ V} = 2,5\text{ W}$$

dc) 2 Punkte

Die Festplatte alleine oder die restlichen drei Geräte zusammen anschließen.

e) 4 Punkte

- Direkter Austausch von Daten zwischen zwei USB-Geräten möglich
- USB on-the-go-Gerät kann Host-Funktion übernehmen
- Verbindung von Digitalkamera zu Drucker u. a.
- Gerätekennzeichnung: USB-Logo mit grünem Pfeil und on-the-go-Schriftzug

## 5. Handlungsschritt (20 Punkte)

aa) 3 Punkte, 2 x 1,5 Punkte

- Switch gegen Hub austauschen (nur für kleine Netze praktikabel)
- oder Port Mirroring anwenden
- oder ARP-Request senden
- oder VLAN deaktivieren

ab) 1 Punkt

Promiscuous Mode

b) 4 Punkte

Der Switch wird mit „spoofed“ ARP-Paketen überflutet, sodass die interne MAC-Tabelle des Switches an die Kapazitätsgrenze stößt. Der Switch verhält sich wie ein Hub, sodass der Datenverkehr im Netz leicht abgehört werden kann.

ca) 3 Punkte, 3 x 1 Punkt

- Port 110
- Port 25
- Port 143
- Port 993 (IMAP 4 over TLS/SSL)
- Port 995 (POP3 over TLS/SSL)

cb) 3 Punkte, 3 x 1 Punkt

- POP3 (Post Office Protocol Version 3)
- FTP (File Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- IMAP (Internet Message Access Protocol)
- SIP (Session Initiation Protocol)
- u. a.

d) 6 Punkte

- PC mit Sniffer im Promiscuous Mode
- Dadurch Verarbeitung aller ankommenden Datenpakete
- Dadurch höhere Latenzzeit bei Ping und ICMP-Echo-Anfragen



## **6. Handlungsschritt (20 Punkte)**

aa) 2 Punkte

Port 443: HTTPS

ab) 4 Punkte

Bei Port 443 handelt es sich um eine verschlüsselte Übertragung. Um den Inhalt zu überprüfen, müssten die Daten entschlüsselt werden, was einer Datenmanipulation gleichkommt und dem Sinn der Verbindung entgegensteht.

ac) 4 Punkte

- Whitelist mit erlaubten Adressen auf dem Proxy installieren
- Whitelist mit vertrauenswürdigen Zertifikaten und Authentifizierungsstellen (ca = certificate authority) für Zertifikate auf dem Proxy installieren
- Port 443 schließen (unpraktikabel, weil dadurch z. B. Online-Banking unmöglich wird)

b) 10 Punkte

Handshake-Protokoll:

- Client kontaktiert Server und schickt ihm Verschlüsselungsverfahren.
- Server identifiziert sich gegenüber Client durch ein Zertifikat (optional).
- Server wählt Verschlüsselungsverfahren aus und schickt Client seinen öffentlichen Schlüssel.
- Client generiert Sitzungsschlüssel und schickt ihn - verschlüsselt mit dem öffentlichen Schlüssel - an den Server.
- Server entschlüsselt Session Key mit privatem Schlüssel.
- (Symmetrische Ver- und Entschlüsselung der Daten mit Session Key.)