

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 fünf Handlungsschritte ausdrücklich als „nicht bearbeitet“ gekennzeichnet wurde,
- der 5. Handlungsschritt bearbeitet wurde,
- einer der Handlungsschritte 1 bis 4 deutlich erkennbar nicht bearbeitet wurde,

ist der tatsächlich nicht bearbeitete Handlungsschritt von der Bewertung auszuschließen.

Ein weiterer Punktabzug für den bearbeiteten 5. 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 (25 Punkte)

aa) 2 Punkte, 2 x 1 Punkt

LAN: 255.255.252.0

DMZ: 255.255.255.248

ab) 6 Punkte, 6 x 1 Punkt

	Netz-ID	Erster Host	Letzter Host	Broadcast
LAN	10.10.0.0	10.10.0.1	10.10.3.254	10.10.3.255
DMZ	192.168.199.0	192.168.199.1	192.168.199.6	192.168.199.7

ba) 4 Punkte, 2 x 2 Punkte

- VoIP VLAN ist deswegen sinnvoll, weil die Performance, z. B. durch QoS erhöht wird.
- Eigenes VLAN für Admin-Notebooks ist sinnvoll, um die Sicherheit zu erhöhen.

Andere Lösungen sind möglich.

bb) 2 Punkte

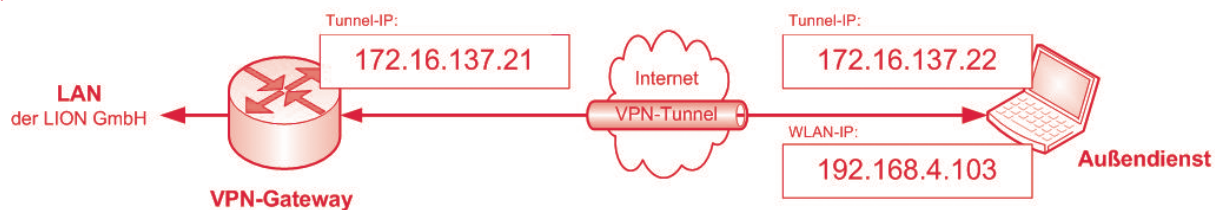
Switch, Layer 2

bc) 4 Punkte

Dynamische VLAN-Zuordnung erfolgt anhand des Benutzernamens, z. B. über einen RADIUS-Dienst oder Netzwerkrichtlinien-Server. Damit kann sich der Administrator an jedem beliebigen Switchport anmelden und wird immer dem Management-VLAN zugeordnet.

Andere Lösungen sind möglich.

ca) 3 Punkte



cb) 4 Punkte

Es fehlt die Route in das Netz der Zentrale. Folgende Route ergänzen:

10.10.0.0 255.255.252.0 172.16.137.21

2. Handlungsschritt (25 Punkte)

a) 4 Punkte, 4 x 1 Punkt

- Bessere Administrierbarkeit der mobilen Geräte
- Verbesserung des Sicherheitsstandards
- Senkung von Verwaltungskosten
- Einfacheres Lizenzmanagement
- Abbildung eines Life Cycle Managements möglich
- u. a.

b) 4 Punkte, 4 x 1 Punkt

- Schulung von Mitarbeitern
- Festlegen von Berechtigungen
- Verschlüsselung von Daten bzw. Datenträgern
- Passwortrichtlinien
- Bring-your-own-device: dienstliche Nutzung privater Geräte
- Privatnutzung dienstlicher Geräte
- Klassifizierung von Daten in Schutzklassen
- Erfassung und Speicherung von Bewegungsdaten
- u. a.

c) 3 Punkte

- Zwischen Endgeräten mit diesem Feature ist eine direkte Kommunikation möglich.
- Eines der beiden Geräte übernimmt Host-Funktionalität.
- Wird üblicherweise zum Verbinden von Druckern und Digitalkameras mit einem PC verwendet.
- u. a.

da) 3 Punkte

- Eigene Dateien
- Eigene Dokumente
- Kontakte
- E-Mails
- u. a.

db) 5 Punkte, 2 x 2,5 Punkte

USB-3.0-Schnittstelle: 20 Sek

Rechenweg

$$8 \text{ GiB} * 1.024^3 \text{ Byte} / 450 * 1.000^3 \text{ Byte/Sek} = 19,09 \text{ Sek} \sim 20 \text{ Sek}$$

SATA II-Schnittstelle: 29 Sek

Rechenweg

$$8 \text{ GiB} * 1.024^3 \text{ Byte} / 300 * 1.000^3 \text{ Byte/Sek} = 28,63 \text{ Sek} \sim 29 \text{ Sek}$$

e) 6 Punkte, 3 x 2 Punkte

TPM ist ein Chip, der mit einer Smartcard verglichen werden kann. Der Chip kann Passwörter, Zertifikate und Verschlüsselungsschlüssel speichern.

UEFI

Für 64-Bit-Systeme entwickelter Nachfolger des PC-BIOS. Zentrale Schnittstelle zwischen der Firmware, den einzelnen Komponenten eines Rechners und dem Betriebssystem.

Secure Boot

Secure Boot Modus verhindert den Start bzw. Installation nicht gewünschter Betriebssysteme, auch z. B. von USB-Sticks etc.

3. Handlungsschritt (25 Punkte)

a) 8 Punkte, 4 x 2 Punkte

Sicherheitsmerkmal	Erläuterung
Integrierte Firewall	Schutz des Rechners vor netzinternen Angriffen, Schutz des internen Netzes vor kompromittierten Rechnern
Sichere Anmeldung	Kennwortrichtlinien konfigurierbar, Anmeldung mit Biometrie-Funktionen
Dateisystem	erlaubt die Verschlüsselung der Daten auf den Speichermedien
Logfunktionen	hält sicherheitsrelevante Vorgänge in Log-Dateien fest
Benutzerverwaltung	erlaubt die gezielte Vergabe von Berechtigungen
Updatefunktion	warnt und schließt umgehend Sicherheitslücken

Hinweis für Prüferin/Prüfer:

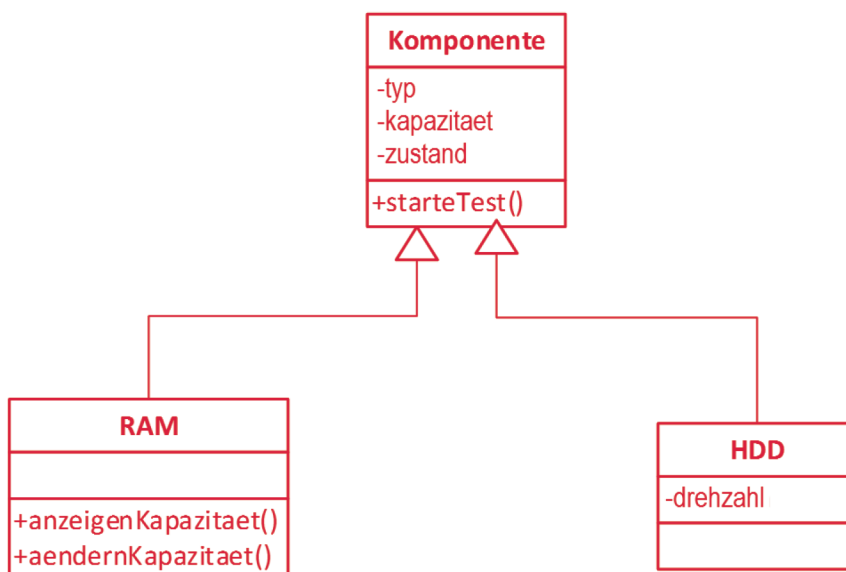
Weitere Sicherheitsmerkmale, wie z. B. TPM, UEFI und Zertifikate mit zutreffender Erläuterung sind auch als richtig zu bewerten.

ba) 9 Punkte

4 Punkte für Klasse Komponente: 4 x 1 Punkt je Attribut und Methode

3 Punkte für Klasse RAM: 1 Punkt für Klasse und Beziehung, 2 x 1 Punkt je Methode

2 Punkte für Klasse HDD: 1 Punkt für Klasse und Beziehung, 1 Punkt für Attribut



bb) 4 Punkte

1 Punkt Umrechnung GiB in Byte

1 Punkt Methodenaufruf *aendernKapazitaet()*

2 Punkte Methodenaufruf *anzeigenKapazitaet()* und Zuweisung

17.179.869.184 Byte (16 GiB * 1.024³)

CRAM.aendernKapazitaet(17179869184)

aktuelleKapazitaet = CRAM.anzeigenKapazitaet()

bc) 4 Punkte

2 Punkte für $(a_F * 100 / a_Z) > 0.1$

1 Punkt für $(a_Z \geq 100000)$

1 Punkt für (Bedingung 1) **&&** (Bedingung 2)

```
if (((a_F * 100 / a_Z) > 0.1) && (a_Z >= 100000)) err1 = true;
```

4. Handlungsschritt (25 Punkte)

a) 3 Punkte, 3 x 1 Punkt

DRAFT

Speicherort für E-Mails, die noch nicht versendet worden sind (Entwürfe)

SENT

Speicherort für versendete E-Mails (gesendete Objekte)

TRASH

Speicherort für gelöschte E-Mails der Klassen gesendete und empfangene Objekte

Andere Lösungen sind möglich.

ba) 6 Punkte, 3 x 2 Punkte

SMTP

Simple Message Transport Protocol

Wird verwendet, um eine E-Mail an den nächsten MTA (Mail-Server bzw. Mail Transport Agent) weiterzuleiten.

POP3

Post Office Protocol Version 3

Wird verwendet, um E-Mails bei einem Server (MDA Mail Delivery Agent) abzuholen.

IMAP

Internet Message Access Protocol

Der Client lädt je nach Einstellung nur die Kopfzeilen neuer E-Mails oder die E-Mails vollständig herunter. Die E-Mail-Ordner werden zwischen Client und Server synchronisiert.

bb) 3 Punkte

Da die E-Mails im Postfach auf dem Server verwaltet werden, kann von verschiedenen Clients auf das Postfach zugegriffen werden. Lokal ist nur die Kopie vorhanden.

bc) 3 Punkte

Der Einsatz von sicheren Mail-Protokollen wie SMTPs und POP3s stellt sicher, dass die Mails zwischen Client und Mailserver verschlüsselt übertragen werden.

u. a.

ca) 4 Punkte, 2 x 2 Punkte

Blacklist

Eine Liste von unerwünschten Absendern (Domains oder Mailboxen), die abgewiesen werden. Absender, die nicht auf der Liste stehen, werden bearbeitet.

Whitelist

Eine Liste von erwünschten Absendern, die weitergeleitet werden. Alle anderen Absender werden zurückgewiesen.

cb) 4 Punkte für einen vollständigen Fall

Fall 1:

Es werden immer alle Regeln abgearbeitet:

mail from @domain.de reject (evtl. deny oder drop – Blacklist-Regel)

mail from kontakt@domain.de accept (Whitelist-Regel)

oder

Fall 2:

Bei der ersten gültigen Regel wird diese angewendet.

mail from kontakt@domain.de accept (Whitelist-Regel)

mail from @domain.de reject (evtl. deny oder drop – Blacklist-Regel)

Hinweis für Prüferin/Prüfer

reject:

Die höfliche Form, weil eine Nachricht gesendet wird, dass der ursprüngliche Absender „blacklistet“ ist. Sollte bevorzugt verwendet werden, damit die Gegenstelle mitbekommt, dass diese „blacklistet“ ist, um Gegenmaßnahmen einzuleiten.

deny oder drop:

Bei deny oder drop werden die Mails nicht bearbeitet.

Sollte gar nicht oder nur bei hartnäckigen Fällen angewandt werden, da eine Nichtbearbeitung evtl. im Gegensatz zum Postgeheimnis steht.

Andere Lösungen sind möglich.

d) 2 Punkte

Der Filter hat eine ausführbare Datei (.exe) im E-Mail-Anhang entdeckt und diese aus Sicherheitsgründen blockiert.

5. Handlungsschritt (25 Punkte)

aa) 4 Punkte

9,4 TiB

Rechenweg

Altdateien	7.373 GiB	8 TiB * 0,9 * 1024
Datenzuwachs in 5 Jahren	2.250 GiB	450 GiB/Jahr x 5 Jahre
Benötigter Speicherplatz	9.623 GiB	7.373 GiB + 2.250 GiB
Umrechnung in TiB	9,4 TiB	9.623 GiB / 1.024 = 9,3975

ab) 3 Punkte

Anzahl Festplatten: 12

Herleitung

9,4 TiB ~ 10 TiB

10 x 1 TiB Festplatten für Daten + 2 x 1 TiB Festplatten für Parität

ac) 3 Punkte

Eine Hot-Spare-Festplatte ist eine in einem System nicht verwendete Festplatte. Fällt eine andere Platte aus, wird die Hot-Spare-Platte im laufenden Betrieb automatisch anstelle der defekten Platte eingebunden.

ba) 6 Punkte

Inkrementelle Sicherung

Sichert alle veränderten Daten seit der letzten Sicherung (inkrementell oder Vollsicherung)

Differentielle Sicherung

Sichert alle veränderten Daten ab einem Basistag (z. B. Tag der letzten Vollsicherung)

bb) 3 Punkte

Zur Unterscheidung von veränderten Dateien setzen manche Dateisysteme spezielle Dateiattribute ein (Archivbit), die bei einer Veränderung automatisch vom System gesetzt werden.

oder

Sollte kein Archivbit möglich sein, kann das System Datumsvergleiche vornehmen oder Prüfsummen bilden.

c) 6 Punkte, 2 x 3 Punkte

Recovery Time Objective (RTO)

Bezeichnet die Zeitspanne, für die ein System ausfallen kann. Es handelt es sich um die Zeit, die vom Zeitpunkt des Schadens bis zur vollständigen Wiederherstellung vergehen darf.

Recovery Point Objective (RPO)

Bezeichnet die Zeitspanne, für die ein Datenverlust in Kauf genommen werden kann. Bei der Recovery Point Objective handelt es sich um den Zeitraum, der zwischen zwei Datensicherungen liegen darf.

Andere Lösungen sind möglich.

