Abschlussprüfung Sommer 2013
Lösungshinweise

IHK

Fachinformatiker/Fachinformatikerin
Systemintegration
1197

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)

a) 9 Punkte

Fehler 1: Client 1 hat ein falsches Gateway eingetragen, richtig ist 192.168.0.254.
Fehler 2: Client N hat eine falsche IP-Adresse eingetragen, richtig ist eine IP-Adresse im Netz 192.168.0.0./24
Fehler 3: Beim Webserver ist die Broadcastadresse als Gateway eingetragen, richtig wäre eine Adresse zwischen 212.12.12.10 – 14.

b) 4 Punkte

Der Client hat keine IP-Adresse erhalten, da er den DHCP-Server nicht erreichen kann.

Grund ist die Tatsache, dass der DHCP-Discover als Broadcast ins Netz geschickt, vom Router aber nicht weitergeleitet bzw. beantwortet wurde (z. B. kein DHCP-Server auf dem Router installiert, kein DHCP-Relay installiert).

Ein weiterer Grund wäre die falsche Konfiguration der Routerschnittstelle.

Weitere sinnvolle Lösungen möglich

ca) 4 Punkte

Eine Stateful Packet Inspection ist ein erweiterter Paketfilter, der neben IP, Protokoll und Port weitere Kriterien (z. B. Segmentnummer) für die Filterung heranzieht. Deswegen werden Antworten auf erlaubte Verbindungen (sog. States) automatisch zugelassen und müssen nicht separat konfiguriert werden.

cb) 8 Punkte

- Paket wird verworfen, da ICPM von außen nicht zugelassen wird.
- Paket wird durchgelassen, da es eine http-Anfrage für den Webserver in der DMZ ist.
- Paket wird durchgelassen, da es eine Antwort auf eine Anfrage des Proxys ist.
- Paket wird verworfen, da der Port 22 (SSH) aus dem Internet nicht erlaubt ist.

2. Handlungsschritt (25 Punkte)

a) 6 Punkte, 3 x 2 Punkte

- Plattformunabhängigkeit, da virtuelle Server auf jeder Hardware eingesetzt werden können
- Energieeinsparung, da mehrere virtuelle Server auf einer physikalischen Maschine betrieben werden können
- Bessere Auslastung der physischen Hardware
- Vereinfachung der Serververwaltung durch Managementkonsole der Hypervisorsoftware
- u. a.

ba) 4 Punkte

- Hardware des Wirts wird von Hypervisor verwaltet.
- Hypervisor weist virtuellen Maschinen Hardware-Recourcen zu.
- Virtuelle Maschinen besitzen jeweils ein Gast-Betriebssystem.

Vorteile gegenüber gehosteter Architektur

- Höhere Performance, da direkte Kommunikation mit den I/O-Geräten möglich
- Kein Host-OS erforderlich
- Höhere Sicherheit, da der Hypervisor die komplette Hardwareverwaltung übernimmt
- u. a.

bb) 4 Punkte

- Hardware des Wirts wird von einem Wirt-Betriebssystem verwaltet.
- Wirt-Betriebssystem weist den Virtuellen Maschinen Hardware-Recourcen zu.
- Hypervisor arbeitet als Mittler zwischen Wirt- und Gast-Betriebssystem
- Hypervisor und Gast-Betriebssystem laufen als Anwendungen des Host-Betriebssystems.

Vorteile gegenüber Bare Metal

- Einfache Installation auf vorhandenem OS möglich
- In der Regel kostengünstiger
- u. a.

c) 8 Punkte

- Festlegung der Standardkonfiguration für eine virtuelle Maschine (VM)
- Installation einer Standard-VM (ggf. für jede Abteilung einen eigenen VM-Build anlegen)
- Erstellen einer VM
- Installation eines Server-Betriebssystems
- Installation eines Thin-Client-Betriebssystems
- (Installation ggf. auch unter einem physischen Betriebssystem)
- Kopieren, Klonen der VM (unter Beachtung der vorhandenen Lizenzbedingungen)
- Starten der VM
- Erstellen der Thin-Client-Server-Verbindungsprofile für jeden Build (Beim Verbindungsprofil einer Abteilung müssen die IP-Adressen der virtuellen Desktops dem Build der Abteilung zugewiesen werden.)
- Festlegung, wie die physischen Clients gestartet werden sollen (z. B. PXE-Boot, Festplatte oder CD-ROM)

d) 3 Punkte

Erläuterung:
Exakte Kopie eines Datenstandes zu einem bestimmten Zeitpunkt

Begründung:
Schnelle Systemwiederherstellung nach Fehlern oder Änderungen

3. Handlungsschritt (25 Punkte)

a) 3 Punkte

- Besserer Ausnutzungsgrad der Festplatten
- Energieersparnis, weil insgesamt weniger Festplatten benötigt werden
- Geringerer Administrationsaufwand durch zentrale Verwaltung
- Mehr Flexibilität, da Servern gegebenenfalls mehr Speicher aus dem Speicherpool zugewiesen werden kann
- Schnelle Erweiterbarkeit
- u. a.

b) 4 Punkte

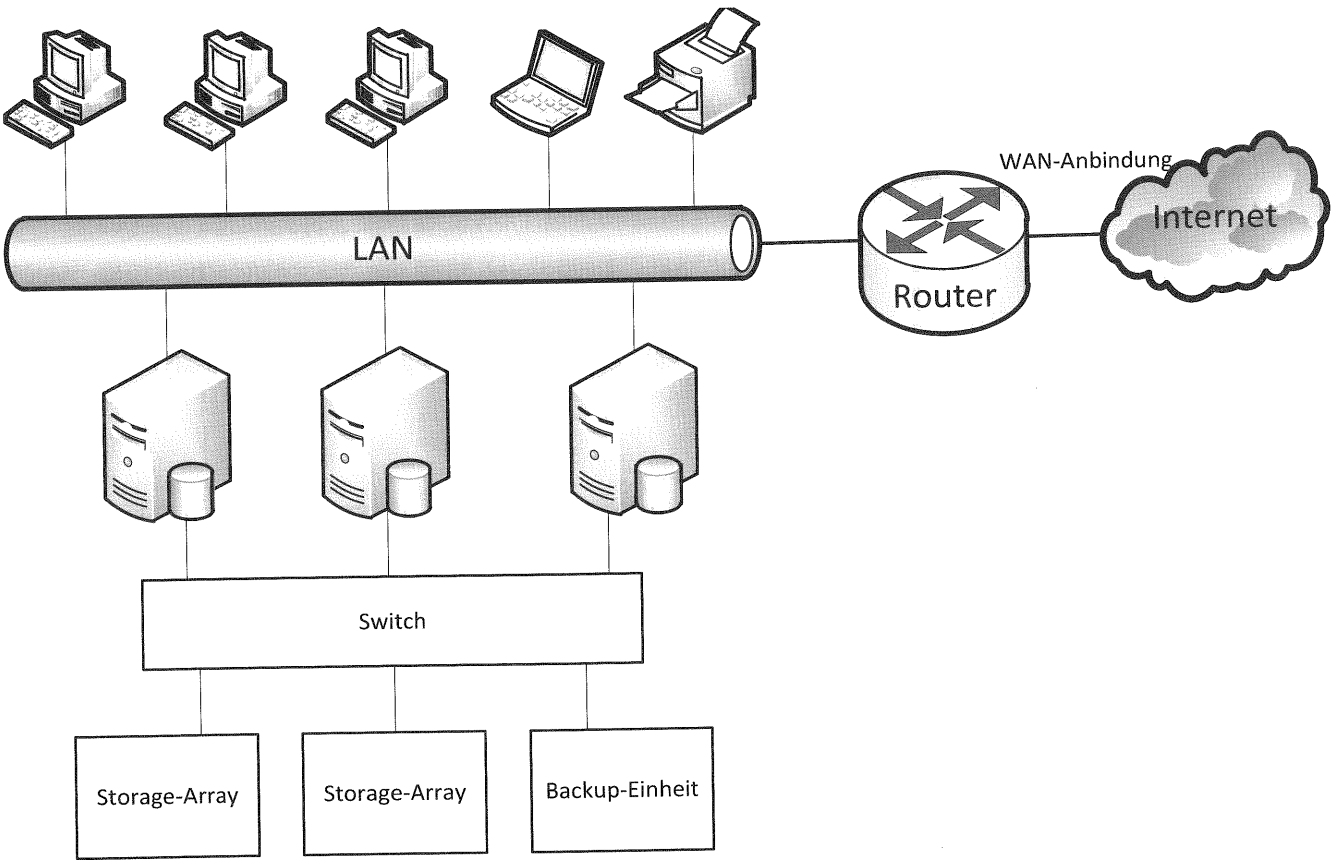
iSCSI:

- Weiterentwicklung der bewährten SCSI-Technik, bei der der Datentransport auf bestehender Netzwerktechnik geschieht
- SCSI-Daten werden in TCP/IP-Pakete gekapselt und z. B. über eine Ethernet-Verbindung übertragen.

(2 Punkte)
Zutreffende Sachverhalte zur Fibre-Channel-Technik

c) 4 Punkte

2 Punkte für Serveranschluss
2 Punkte für Switchanschluss



3. Handlungsschritt (25 Punkte)

da) 7 Punkte

RAID 5 und RAID 1:
3.724 GiByte ((7 - 1) x 450 GiByte + (2 - 1) x 1.024 GiByte = 2.700 GiByte + 1.024 GiByte)

5 Punkte für:
nur RAID 5:
3.600 GiByte ((9 - 1) x 450 GiByte)

Teilpunkte entsprechend dem Lösungsansatz.

db) 2 Punkte

Dezimalpräfixe
Beispiele
- ISDN 64 kbit/s
- USB 2.0 480 Mbit/s
- Ethernet 1000BaseT 1000 Mbit/s

Dezimalpräfixe wie Kilo, Mega usw. beziehen sich als Exponent auf die Zahl 10 und werden bei Datenübertragungsraten benutzt.

Binarpräfixe:
Beispiele
- Arbeitsspeicher: 4 GiB;
- Dateigröße: 34,12 MiB;
- Festplatte: 1 TiB

Binärpräfixe wie Kibi, Mebi usw. beziehen sich als Exponent auf die Zahl 2 und werden bei der Angabe von Speichergrößen benutzt.

e) 5 Punkte

38 Minuten

Vor der Erweiterung:
1,3 Stunden (18 · 12 V · 4,5 Ah / 750 VA)
78 Minuten (1,3 h · 60 min/h)

Nach der Erweiterung:
0,67 Stunden (18 · 12 V · 4,5 Ah / 1.450 VA)
40 Minuten (0,67 h · 60 min/h)

Differenz:
38 Minuten (78 – 40)

4. Handlungsschritt (25 Punkte)

a) 6 Punkte

Eine Demilitarisierte Zone (DMZ) ist ein separierter Netzwerkabschnitt zwischen zwei Netzwerken, in der Regel zwischen einem internen Netz und dem Internet. Funktionell ist die DMZ durch zwei (logische oder physikalische) Firewalls von Internet und internem Netz getrennt. In diesen Abschnitt werden Dienste platziert, die von außen erreichbar sein sollen, aber aus Sicherheitsaspekten nicht im internen Netz betrieben werden sollen. Bei einer Kompromittierung eines Dienstes ist das interne Netz durch die zweite Firewall geschützt.

Andere Lösung möglich

ba) 6 Punkte

Bei einer DNS-Spoofing-Attacke wird der DNS-Eintrag verändert, so kann man eine Verbindung bei der DNS-Abfrage über einen weiteren Host umleiten. Dieser könnte als Art Proxy die Verbindung an den ursprünglich angefragten Server weiterleiten, sodass der verbindungsaufbauende Host nichts merkt. Dieser bekommt die richtige Seite angezeigt. Der „man in the middle" kann aber den gesamten Datenverkehr aufzeichnen und die Daten (Benutzer, Passwörter und sonstige Angaben) für „eigene Zwecke" verwenden.

Andere Lösung möglich

bb) 2 Punkte

- Fester Eintrag in die „Hosts"-Datei
- Feste Einträge in den lokalen DNS-Server
- Konfiguration des DNS-Servers, dass dynamische Veränderungen der DNS-Einträge nur mittels Key funktionieren (rndc.key)

Andere Lösung möglich

c) 6 Punkte

Lokale „man in the middle"-Attacke auf Basis eines arp-Poisoning
Dabei werden verfälschte arp-Requests oder arp-Responses an einen Host gesendet, um die arp-Tabelle in dem Rechnern so zu verändern, dass die Netzwerkpakete über den Host des Angreifers gesendet werden. Der Angreifer gelangt so an die Daten des Angegriffenen.

Andere Lösung möglich

d) 5 Punkte

Überwachung der Netzwerktätigkeiten mittels passiver Überwachung oder aktiver Remoteabfrage von Netzwerkdaten. Bei Auffälligkeiten im Netzwerk (z. B. Portscan, doppelte Einträge in arp-Tabellen) werden festgelegte Aktionen ausgeführt: E-Mail an den Administrator, Abschaltung/Sperrung von Netzwerkelementen (z. B. Switch-Ports), Herunterfahren sicherheitskritischer Anwendungen u. a.

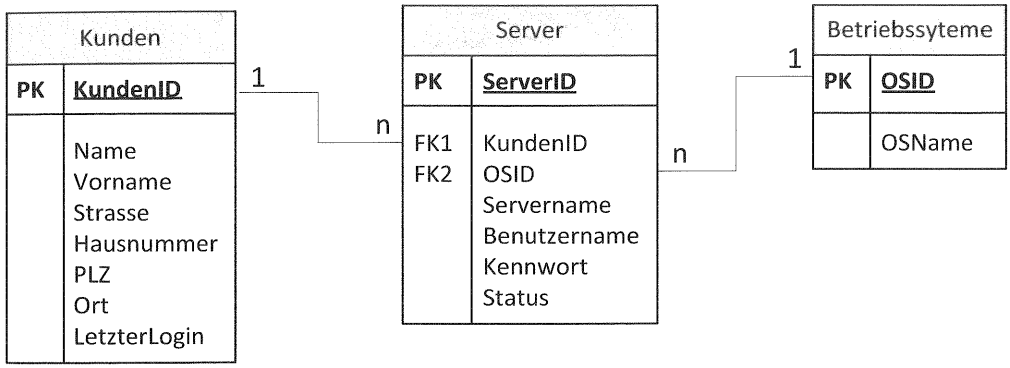
Andere Lösung möglich

5. Handlungsschritt (25 Punkte)

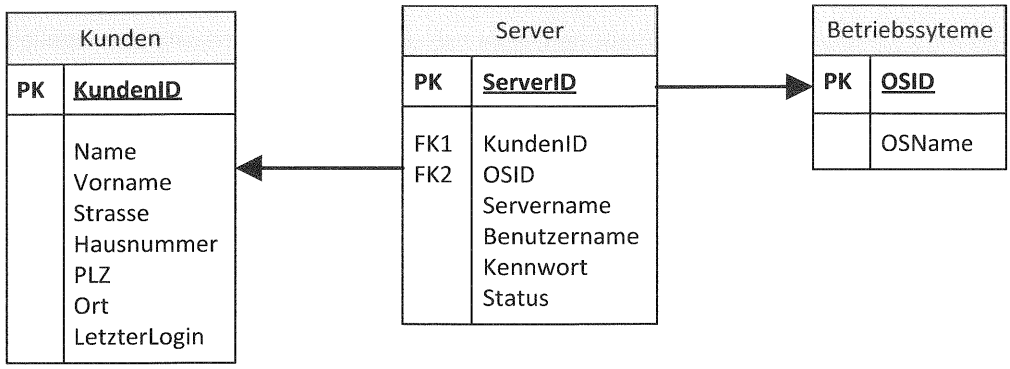
a) 16 Punkte

3 Punkte, 3 x 1 Punkt je Primärschlüssel
2 Punkte, 2 x 1 Punkt je Fremdschlüssel
3 Punkte, 3 x 1 Punkt je Entität
2 Punkte, 2 x 1 Punkt je Beziehung
6 Punkte, 6 x 1 Punkt je Attribut

Version 1



Version 2



b) 3 Punkte
3 x 1 Punkt je Fachbegriff (Tupel, Record, Attribut)

Eine relationale Datenbank besteht aus mehreren Tabellen die zueinander in einer Beziehung stehen. In jeder Zeile (Tupel) der Tabelle steht ein Datensatz (Record). Jede Zeile besteht aus einer Reihe von Eigenschaften (Attributes).

c) 6 Punkte

Die Datenbank/Dateien müssen in einem konsistenten Zustand vor dem Speichern der Dateien versetzt werden. Dazu gibt es die folgenden Möglichkeiten:

Die Datenbank wird geschlossen und heruntergefahren. Danach werden die Datenbankdateien gesichert.

Die Datenbank wird in einen Backup-Modus versetzt. Hierbei werden die Tabellen und Dateien geschlossen und die Datenbank nicht heruntergefahren. Die Datenbankdateien können nun normal gesichert werden. Je nach Datenbanksystem ist die Datenbank in diesem Zustand „nur lesbar" oder eventuelle Änderungen werden temporär zwischengespeichert und nach Beendigung des Backup-Modus in die Datenbank geschrieben.

Hinweis für Korrektor:
„Online-Backups" mit „recovery-files" (z. B. Oracle) oder „dump-files" (mySQL) stellen kein Voll-Backup dar!