

Die Handlungsschritte 1 bis 5 beziehen sich auf die folgende Ausgangssituation:

Sie sind Mitarbeiter/-in der ITRES GmbH.

Die ITRES GmbH plant, ihr Unternehmensnetzwerk neu zu strukturieren.

Sie sollen vier der folgenden fünf Handlungsschritte bearbeiten:

1. Netzwerkgeräte konfigurieren und überprüfen
2. Die WLAN-Verfügbarkeit optimieren
3. Die Benutzerverwaltung automatisieren
4. Die Datensicherheit im Unternehmen erhöhen
5. Das zentrale Speichersystem erweitern

1. Handlungsschritt (25 Punkte)

Das Administratorenteam der ITRES GmbH plant, den Zugang zum Netzwerk direkt an den Switchen abzusichern. Jeder Benutzer soll bereits bei der Anmeldung am Netzwerk einem VLAN dynamisch zugeordnet werden. Dazu wurden die folgenden VLANs eingerichtet:

ID	Name	Beschreibung	IP-Adresskreis
1	Verwaltung	Mitarbeiter der Verwaltung	192.168.1.0/24
2	Produktion	Mitarbeiter der Produktion	192.168.2.0/24
9	Administration	IT-Administratoren	192.168.9.0/28
99	Gast	Kunden und Gäste	192.168.99.0/24

Die Netzwerkkonfiguration ist im Netzwerkplan der ITRES GmbH dargestellt, siehe perforierte Anlage.

- a) Erläutern Sie, wie viele IP-Adressen im VLAN „Administration“ vergeben werden können.

Der Rechenweg ist anzugeben.

3 Punkte

[illegible]

- b) Erläutern Sie, warum Frames auf den Verbindungen zwischen den Switchen getagged werden müssen.

4 Punkte

- c) Die IP-Konfiguration für die Clients in den einzelnen VLANs soll über einen zentralen DHCP-Server erfolgen. Dazu wurden auf dem DHCP-Server die einzelnen Adresspools mit den entsprechenden Bereichsoptionen (Gateway, DNS) eingerichtet. Bei der Überprüfung der IP-Konfiguration an einem Client im VLAN Produktion (192.168.2.0/24) erhalten Sie folgende Ausgabe:

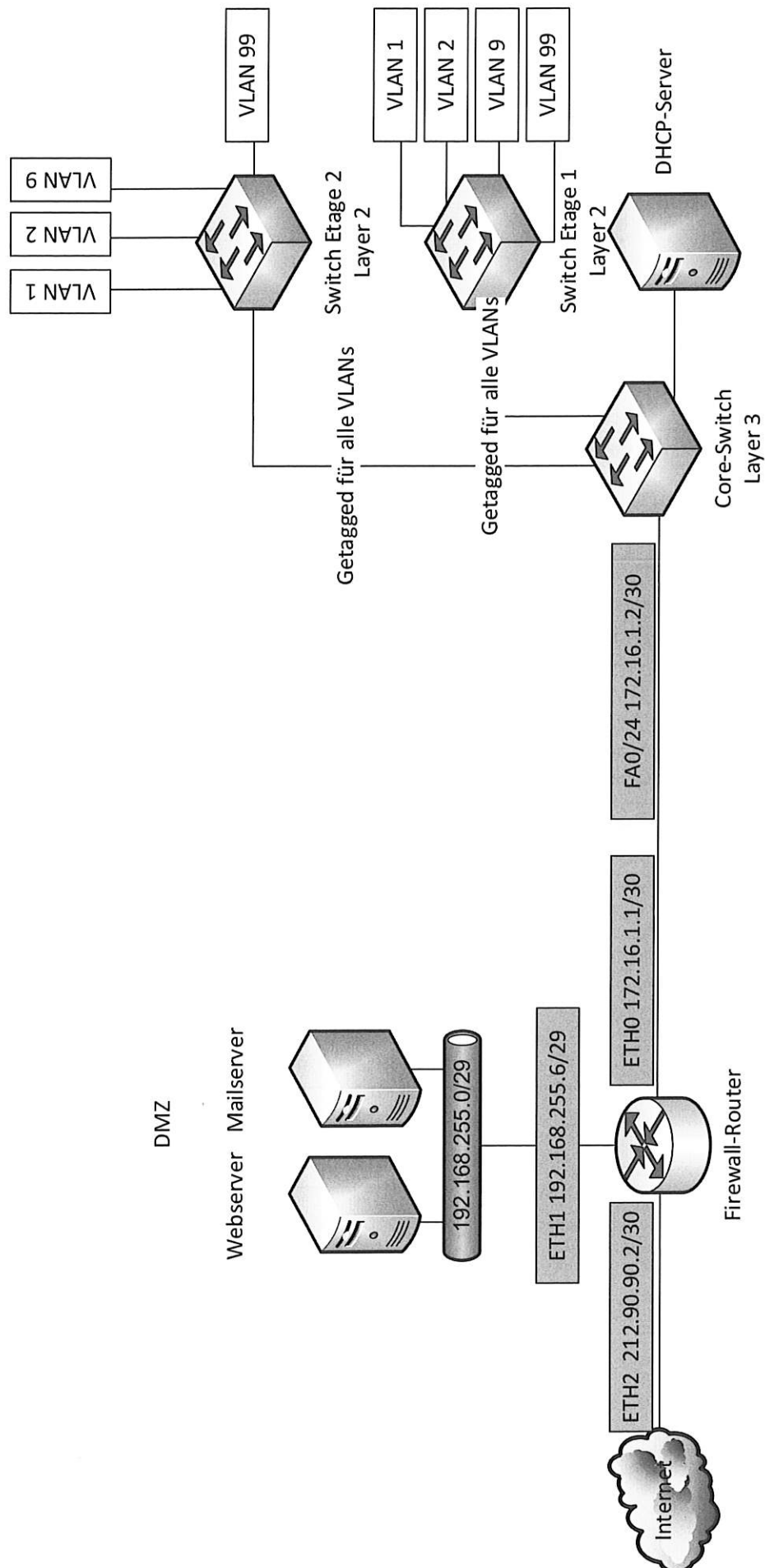
IP Address...: 169.254.60.24

Subnet Mask...: 255.255.0.0

Bei den Clients in den anderen VLANs funktioniert die IP-Konfiguration per DHCP dagegen tadellos.

- ca) Erläutern Sie, warum der Client diese IP-Adresse generiert hat.

2 Punkte



cb) Der Client soll vom DHCP-Server eine korrekte IP-Adresse aus dem Bereich seines VLANs erhalten.

Korrekturrand

Unterbreiten Sie dazu einen Vorschlag.

2 Punkte

d) Das Routing im Netzwerk muss konfiguriert werden.

da) Dazu wurde auf dem Core-Switch die folgende Routingtabelle angelegt.

Ergänzen Sie in folgender Tabelle die notwendige Default-Route.

3 Punkte

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop Adresse
192.168.1.0	255.255.255.0	VLAN1
192.168.2.0	255.255.255.0	VLAN2
192.168.9.0	255.255.255.240	VLAN9
192.168.99.0	255.255.255.0	VLAN99
		

db) Bei einem Ping-Test von einem Rechner im Verwaltungsnetz zum Webserver erhalten Sie einen Time-Out. Der Ping-Test auf die IP 172.16.1.2 funktioniert ohne Probleme. Daraufhin überprüfen Sie die Routingtabelle des Firewall-Routers:

Netzwerk	Subnetzmaske	Schnittstelle	Next-Hop Adresse
172.16.1.0	255.255.255.252	ETH0
192.168.2.0	255.255.255.0	172.16.1.2
192.168.9.0	255.255.255.240	172.16.1.2
192.168.99.0	255.255.255.0	172.16.1.2
192.168.255.0	255.255.255.248	ETH1
212.90.90.0	255.255.255.252	ETH2
0.0.0.0	0.0.0.0	ETH2

Erläutern Sie, welcher Fehler vorliegt und wie Sie diesen Fehler beheben können.

4 Punkte

Fortsetzung 1. Handlungsschritt →

Fortsetzung 1. Handlungsschritt

Korrekturrand

e) Zur Absicherung des Netzes wurden auf dem Core-Switch die folgenden Firewall-Regeln aufgestellt:

Nr	Aktion	Protokoll	Quell-IP	Ziel-IP	Q-Port	Z-Port	Von Interface	Nach Interface
1	Permit	IP	192.168.9.0/28	Any	-	-	VLAN9	ANY
2	Permit	TCP	192.168.1.0/24	Any	>1023	80	VLAN1	FA0/24
3	Permit	TCP	192.168.1.0/24	Any	>1023	443	VLAN1	FA0/24
4	Permit	TCP	192.168.1.0/24	Any	>1023	25	VLAN1	FA0/24
5	Permit	TCP	192.168.1.0/24	Any	>1023	110	VLAN1	FA0/24
6	Permit	UDP	192.168.1.0/24	Any	>1023	53	VLAN1	FA0/24
...								
N	Deny	IP	Any	Any	-	-	Internet	IN

Erläutern Sie die Regeln 1 – 6 und N mit eigenen Worten.

7 Punkte

Regel	Erläuterung
1	
2	
3	
4	
5	
6	
N	

2. Handlungsschritt (25 Punkte)

Korrekturrand

Die ITRES GmbH möchte für ihre Mitarbeiter und Kunden einen Internetzugang über ein WLAN-Netzwerk einrichten.

a) Der WLAN-Access-Point wird im Infrastruktur-Modus betrieben.

Erläutern Sie den Begriff „Infrastruktur-Modus“.

3 Punkte

b) Für die Anmeldung an das WLAN soll ein RADIUS-Dienst (Remote Authentication Dial-In User Service) genutzt werden. In diesem Zusammenhang fällt der Begriff Triple-A-System.

Nennen Sie die drei Begriffe, nach denen das AAA-System benannt ist.

3 Punkte

c) Erläutern Sie, ob das Verbergen der SSID die Sicherheit des WLANs erhöht.

3 Punkte

Fortsetzung 2. Handlungsschritt

d) Bei der Recherche zum Thema RADIUS-Authentifizierung finden Sie folgenden Textauszug:

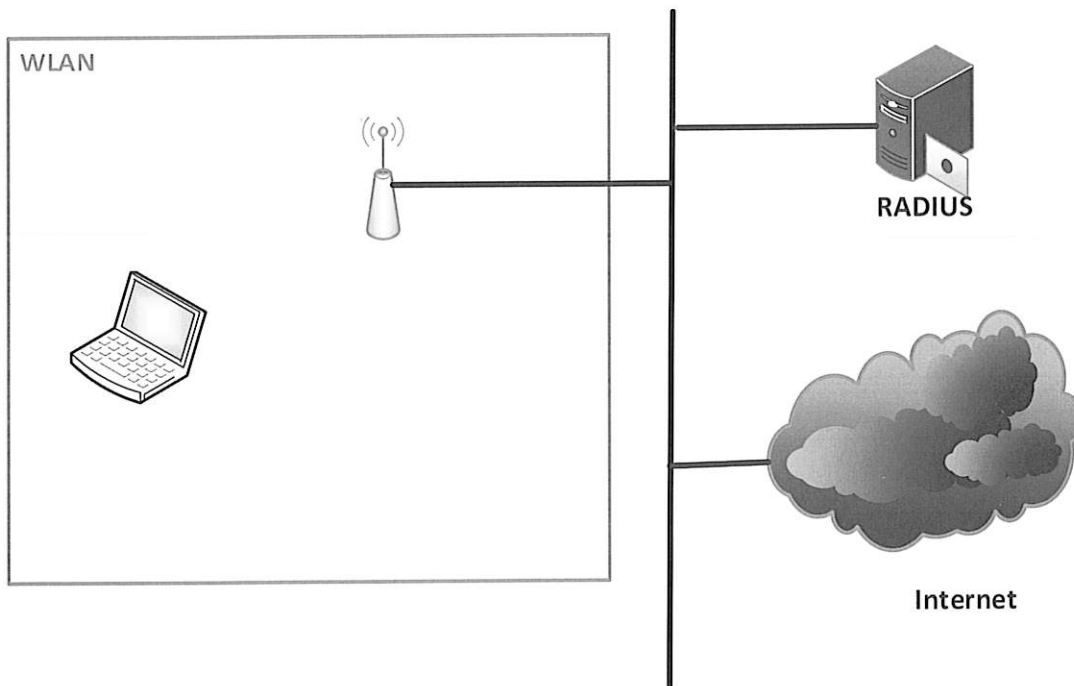
802.1X authentication involves three parties: a supplicant, an authenticator, and an authentication server. The supplicant is a client device (such as a laptop) that wishes to attach to the LAN/WLAN. The authenticator is a network device, such as an Ethernet switch or wireless access point; and the authentication server is typically a host running software supporting the RADIUS and EAP protocols.

The authenticator acts like a security guard to a protected network. The supplicant (i. e., client device) is not allowed access through the authenticator to the protected side of the network until the supplicant's identity has been validated and authorized. With 802.1X port-based authentication, the supplicant provides credentials, such as user name/password or digital certificate, to the authenticator, and the authenticator forwards the credentials to the authentication server for verification. If the authentication server determines the credentials are valid, the supplicant (client device) is allowed to access resources located on the protected side of the network.

Ergänzen Sie die folgende Skizze, indem Sie

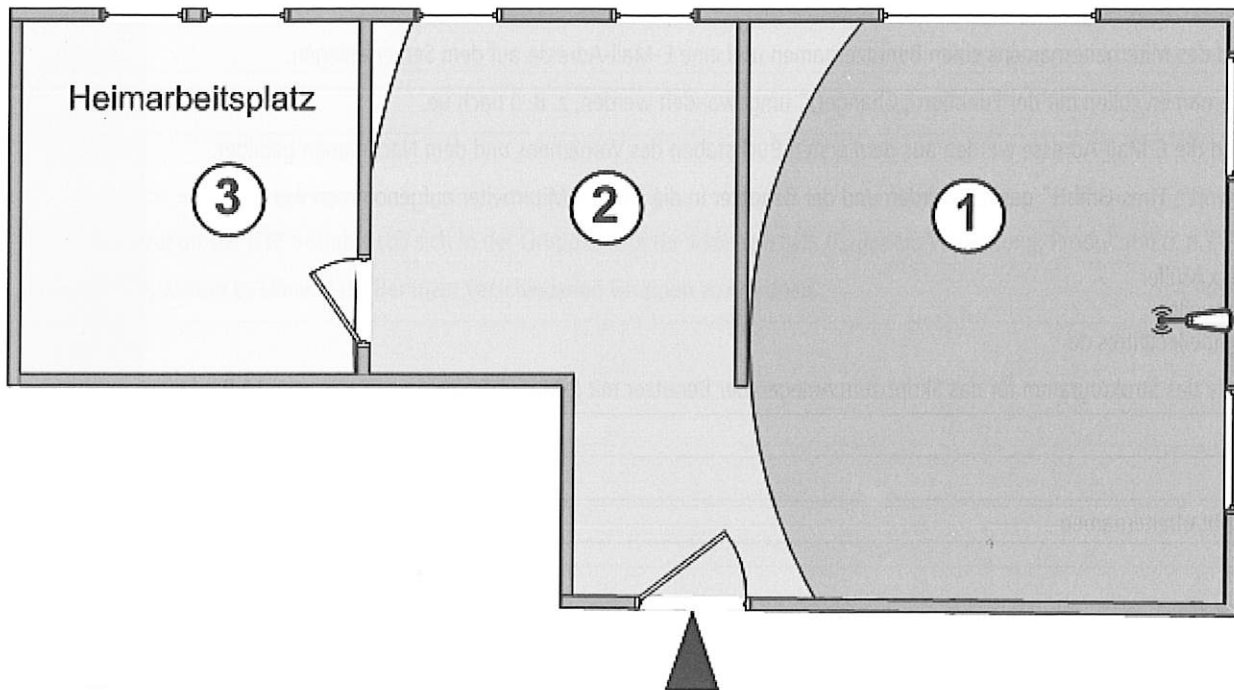
- die Komponenten „supplicant“, „authenticator“, „authentication server“ mithilfe des Textauszuges bezeichnen.
- die Kommunikationswege des EAP-Protokolls in Form gerichteter Pfeile einzeichnen.

7 Punkte



- e) Eine Messung der WLAN-Ausleuchtung im Heimarbeitsplatz eines Mitarbeiters ergibt folgendes Ergebnis. Der Bereich 1 bietet den besten, der Bereich 2 einen akzeptablen und der Bereich 3 den schlechtesten WLAN-Empfang.

Korrekturrand



- ea) Nennen Sie vier Faktoren, welche die Qualität des WLAN-Signals mindern.

4 Punkte

- eb) Nennen Sie drei Maßnahmen, mit denen der Empfang in der gesamten Wohnung (Bereiche 2 und 3) verbessert werden kann.

3 Punkte

- ec) Markieren Sie in der Grafik zwei Positionen, an denen Sie den WLAN-Empfang mit entsprechenden Komponenten verbessern können.

2 Punkte

Es soll das Startkennwort „1tres-GmbH“ gesetzt werden und der Benutzer in die Gruppe Mitarbeiter aufgenommen werden.

Beispiel:

Vorname Name: Max Müller

Benutzername: mmueller

E-Mail: mmueller@itres.de

a) Vervollständigen Sie das Struktogramm für das Skript zum Anlegen der Benutzer mit E-Mail-Adresse.

14 Punkte

Benutzeranlage
Start
Öffne Datei mit Mitarbeiternamen
Ende

b) Erläutern Sie, warum es nicht sinnvoll ist, E-Mail-Adressen mit Umlauten zu benutzen.

4 Punkte

Korrekturrand

c) Die VLAN-Struktur der ITRES GmbH soll sich in der Gruppenstruktur widerspiegeln (Gruppen: Verwaltung, Produktion u. a.).

Erläutern Sie, warum es sinnvoll ist, Benutzer verschiedenen Gruppen zuzuordnen.

4 Punkte

d) Nennen Sie drei Regeln, mit denen die Sicherheit von Benutzerkennwörtern erhöht wird.

3 Punkte

4. Handlungsschritt (25 Punkte)

Die ITRES GmbH will ihre Datensicherheit verbessern.

- a) Bei der Datensicherheit in der ITRES GmbH sind die in folgender Tabelle aufgeführten Aspekte zu betrachten. Sie sollen zu diesen Aspekten entsprechende Maßnahmen zur Datensicherheit einführen.

Vervollständigen Sie die folgende Tabelle, indem Sie zu den vier Aspekten *Logisch*, *Elektrisch*, *Organisatorisch* und *Physikalisch* jeweils eine entsprechende Maßnahme und die Erläuterung dieser Maßnahme eintragen. 8 Punkte

Aspekt	Maßnahme	Erläuterung
Logisch	Netzwerk-Firewall	Schutz vor Angriffen aus dem Netz, da nur definierte Ports/Adressen zugelassen sind.
Logisch		
Elektrisch	Einbau einer USV	Schutz vor Stromausfall. Server laufen ohne Unterbrechung weiter.
Elektrisch		
Organisatorisch	Benutzerschulung	Durchführung einer Datenschutzunterweisung; die Mitarbeiter wissen, wie mit Daten umgegangen werden muss.
Organisatorisch		
Physikalisch	Backup-Server in anderem Brandabschnitt	Bei Brand im Gebäude sind die Daten noch an einem anderen Ort vorhanden.
Physikalisch		

- b) Sie erhalten den Auftrag, für die Mitarbeiter der ITRES GmbH eine Schulung zum Umgang mit sensiblen internen Daten und Kundendaten vorzubereiten.

Nennen Sie fünf Aspekte, die Sie bei der Vorbereitung und Durchführung der Schulung beachten sollten.

5 Punkte

- c) Die ITRES GmbH sichert ein Serversystem mit einer USV. Die USV hat einen Anschluss, über den der Ladestand des Akkus in Prozent abgefragt werden kann.

Der zu 100 % geladene Akku kann bei einer Last von 100 VA eine Stunde Stromausfall überbrücken. Zur Schonung des eingebauten Akkus soll der Ladezustand 40 % nicht unterschreiten. Der angeschlossene Server hat einen Leistungsbedarf von 300 Watt.

Um die laufenden Serverdienste sicher zu beenden und das Betriebssystem herunterzufahren, benötigt der Server fünf Minuten.

Berechnen Sie den Ladestand in Prozent, bei dem der Shutdown des Servers eingeleitet werden muss. Der Rechenweg ist anzugeben.

Hinweis: Rechnen Sie mit $1 \text{ VA} = 1 \text{ Watt}$.

6 Punkte

[illegible]

- d) Für die Sicherung des ERP-Systems (10 TiByte) der ITRES GmbH wird von einem Kollegen vorgeschlagen, Snapshots anzufertigen.

- da) Erläutern Sie, warum ein Snapshot auf einem einzelnen Speichersystem keine verlässliche Datensicherung von Unternehmensdaten darstellt. 2 Punkte

2 Punkte

- db) Zur Sicherung der Datenbank des ERP-Systems wird eine Kombination aus Erstellung eines Snapshots und anschließender Bandsicherung vorgeschlagen.

Erläutern Sie, warum dieser Vorschlag sinnvoll ist.

4 Punkte

c) Auf NAS-2 soll der zur Verfügung stehende Speicherplatz durch „Data Deduplication“ optimiert werden.

Zu „Data Deduplication“ steht Ihnen folgender Text zur Verfügung.

Data deduplication has the goal to store more data in less space. It works by segmenting files into small variable-sized chunks (32–128 KiByte), identifying duplicate chunks, and maintaining a single copy of each chunk. Redundant copies of the chunk are replaced by a reference to the single copy. The chunks are stored in a special container file.

Erläutern Sie die prinzipielle Arbeitsweise von „Data Deduplication“.

5 Punkte

d) Um den Betrieb der NAS-Systeme zu optimieren, wurden folgende Regeln aufgestellt:

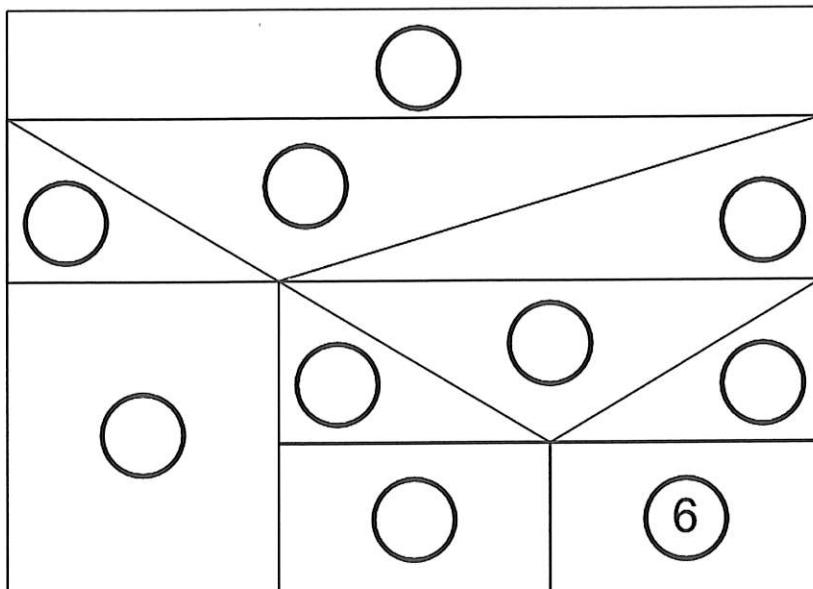
Regeln:

- Wenn die Speicherbelegung von NAS-1 weniger als 50 % beträgt, dann sollen alle Dateien, auf die seit mindestens 90 Tagen nicht zugegriffen wurde, von NAS-1 auf NAS-2 verschoben werden.
- Wenn die Speicherbelegung von NAS-1 zwischen einschließlich 50 % und 75 % beträgt, dann sollen alle Dateien, auf die seit mindestens 30 Tagen nicht zugegriffen wurde, von NAS-1 auf NAS-2 verschoben werden.
- Wenn die Speicherbelegung von NAS-1 über 75 % beträgt, dann sollen alle Dateien, auf die seit mindestens sieben Tagen nicht zugegriffen wurde, von NAS-1 auf NAS-2 verschoben werden.

Die Regeln sollen mithilfe eines Algorithmus umgesetzt werden.

Vervollständigen Sie das folgende Struktogramm, indem Sie in die Kreise die Ziffern vor den entsprechenden Angaben eintragen.
8 Punkte

- 1 Verschiebe alle Dateien nach NAS-2, auf die seit mindestens 90 Tagen nicht mehr zugegriffen wurde.
- 2 Liegt die Speicherbelegung von NAS-1 unter 50 %?
- 3 Ermittle die Speicherbelegung von NAS-1.
- 4 Ja
- 5 Liegt die Speicherbelegung von NAS-1 über 75 %?
- 6 Verschiebe alle Dateien nach NAS-2, auf die seit mindestens sieben Tagen nicht mehr zugegriffen wurde.
- 7 Nein
- 8 Verschiebe alle Dateien nach NAS-2, auf die seit mindestens 30 Tagen nicht mehr zugegriffen wurde.



bitte wenden!