Pool 5: Systemkonzeption und Beschaffungsprozesse

Ich übernehme keine Verantwortung für fehlende oder falsche Informationen.

Active Directory

Das Active Directory ist ein Verzeichnisdienst für den Microsoft Windows Server, durch welchen Information über Objekte in einem Netzwerk gespeichert werden. Diese Objekte können Benutzer, Drucker, Telefone etc. sein. Durch das Active Directory ist die Strukturierung und die Administration von Objekten vereinfacht worden und eine wirklichkeitsgetreue Darstellung einer Organisation möglich.

1. Was sind Active Directory Objekte?

Die Informationen über Benutzer, Drucker usw. werden in Objekten gespeichert. Ein Objekt ist ein individueller Attributsatz mit Informationen. Spezielle Objekte, welche andere Objekte enthalten können, nennt man Container. Eine Domäne ist zum Beispiel ein Container, da sie Benutzer, Drucker etc. beinhaltet.

2. Was ist ein Active Directory Schema?

Das Schema definiert Objekte, die ins AD aufgenommen werden können. Es beschreibt, welche Art von Objekten und welche Art von Informationen zu einem AD-Objekt gespeichert werden können. Das Schema wird in Schemaklassen und Schemaattribute unterteilt. Die Schemaklasse beschreibt die Objekte und hat eine Auflistung von Schemaattributen.

3. Wie sieht der logische Aufbau der Komponenten aus?

Domänen: Das ist die wichtigste Komponente zur Strukturierung. In einer Domäne können Millionen von Objekten gespeichert werden. Sie enthält nur Informationen über Objekte, die auch in ihr enthalten sind. Zusätzlich stellt sie eine Sicherheitsbarriere dar, da mit Berechtigungen klargestellt wird, welcher Benutzer Zugriff auf welche Objekte mit welchem Umfang hat. Die Domäne spiegelt die Struktur des Unternehmens wieder.

Organisationseinheiten (OU): Das ist ein Container, mit dessen Hilfe eine Domäne in logische, administrative Gruppen gegliedert werden kann. OUs können weitere OUs beinhalten, wodurch sich eine Hierarchie innerhalb der Domäne ergibt. Jede OU kann eigene Berechtigungen haben. Wenn aber zwei oder mehr OUs eine übergeordnete OU haben, erben diese standardgemäß die Berechtigungen der Übergeordneten.

Strukturen (Tree): Eine Struktur ist eine hierarchische Anordnung von Domänen. Die Domänen einer Struktur nutzen einen gemeinsamen zusammenhängenden Namespace. Eine untergeordnete Domäne hat einen Eigennamen, an welchem der Name der übergeordneten Domäne angehängt wird.

Gesamtstruktur (Forest): Das sind mehrere Strukturen, die vollständig und separat voneinander sind. Alle Domänen eines Forests basieren auf dem gleichen Schema, besitzen denselben Global Catalog (siehe Frage 5), sind durch Vertrauensstellungen verknüpft und agieren unabhängig.

4. Wie sieht der physische Aufbau der Komponenten aus?
Standorte / Sites: Das ist ein Subnetz oder eine Kombi aus mehreren IP-Subnetzen.
Sites sind nicht Teil des Namespace. Die Sites enthalten nur Computer und Verbindungsobjekte, welche zur Replikation zwischen den Standorten genutzt werden. Unterschiedliche Sites können in eine Domäne und umgekehrt.

Domänencontroller (DC): Das ist ein Computer/Server, auf welchem ein Replikat des Domänenverzeichnisses gespeichert ist. Ein Domänencontroller gehört nur zu einer Domäne, diese kann aber mehrere Domänencontroller haben. Er authentifiziert auch Anmeldeversuche und verwaltet Sicherheitsrichtlinien für Domänen. Änderungen der Informationen werden an einem Domänencontroller vorgenommen. Dieser repliziert dann die Änderungen auf allen anderen Controllern innerhalb der Domäne. Mehr Domänencontroller sind besser, um Fehler zu vermeiden.

5. Was ist der Global Catalog?
Der Global Catalog beinhaltet Informationen zu Objekten aus allen Domänen. Dieser Katalog wird auf einem Domänencontroller, meist auf dem ersten Controller der ersten Domäne gespeichert. Durch den Globalen Katalog können Informationen im Verzeichnis gefunden werden, egal welche Domäne diese Informationen erhält.

6. Welche Serverrollen gibt es im Active Directory?
- **File-Server:** Das ist ein Rechner, der Dateisysteme oder zumindest einen Teil eines Dateisystems in einem Rechnernetz zur Verfügung stellt.
- **Domänencontroller:** Siehe Frage 4.
- **DHCP (Dynamic Host Configuration Protocol)-Server:** Dieser übernimmt dir Vergabe der IP-Adressen beim Hochfahren eines Rechners. Ein Domänencontroller kann auch als DHCP-Server funktionieren.
- **DNS (Domain Name Service)-Server:** Dieser ist für die Namensauflösung zuständig. Er wandelt also eine URL/Namen in die richtige IP (forward lookup) um und umgekehrt (reverse lookup). Der DNS kann ins Internet weiterschalten oder lokal bleiben.

7. Was sind FSMO (Flexible Single Master Operations)?
Das sind spezielle Aufgaben, die Domänencontroller innerhalb ADs übernehmen. Die Aufgaben können auf verschiedene Server verteilt werden, jedoch darf keine dieser Rollen von mehreren Servern gleichzeitig übernommen werden.

Gesamtstrukturweite Rollen:
- **Schema Master:** Er ist für Änderungen des Schemas im AD verantwortlich und wird daher bei Änderungen oder beim Hinzufügen von Objekten ins Schema benutzt.
- **Domain Naming Master:** Dieser ist für die Namensgebung zuständig. Falls versucht wird, eine neue Domäne oder einen Domänencontroller in die Struktur einzubinden, funktioniert das nur, wenn der Domain Naming Master den Namen der neuen Domäne kontrolliert und freigegeben hat.

Domänenweite Rollen:
- **RID (Relative ID)-Master:** Die SID (automatisch vergebener Sicherheits-Identifikator) muss eindeutig sein deswegen legt der RID-Master für jeden anderen Domänencontroller RID-Pools aus welchen dann bei neu erstellten Objekten gewählt wird.

- **PDC (Primary Domain Controller) -Emulator:** Da die Speicherung von Daten in die Datenbank 20 Minuten dauern kann, werden geänderte Benutzerpasswörter auf dem PDC gespeichert. Wenn ein DC einen fehlerhaften Anmeldeversuch feststellt, frägt er erst beim PDC nach, bevor er den Benutzer zurückweist.
- **Domain Infrastructure Master:** Er sorgt dafür, dass wenn Änderungen eines Objektes auch ein anderes betreffen, dieses die Änderungen auch mitbekommt. Das ganze muss domänenübergreifend funktionieren.

8. Was ist Replikation und wie funktioniert sie?
Dadurch wird sichergestellt, dass Informationen, die an einem Domänencontroller durchgeführt wurden, auch auf allen anderen Controllern vorgenommen werden. Die Änderungen werden auf Controllern innerhalb eines Standortes, aber auch außerhalb repliziert.

Welche Informationen werden repliziert?
Die Informationen werden in Partitionen unterteilt.

- **Schemapartition:** Darauf befindet sich das Schema, also die Regeln für die Objekte und Attribute.
- **Konfigurationspartition:** Sie beschreibt den logischen Aufbau der Domänen.
- **Domänenpartition:** Sie beschreibt alle Objekte der Domäne. Diese Informationen sind domänenspezifisch und werden nur auf Controllern der Domäne repliziert.
- **Anwendungsverzeichnispartition:** Hier werden dynamische, anwendungsspezifische Daten des ADs gespeichert.

Wie werden Informationen repliziert?

- **Standortinterne Replikation:** Dabei kommt ein Dienst namens Konsistenzprüfung (KCC) zum Einsatz. Er wird auf allen Controllern ausgeführt und definiert den Pfad der Verzeichnisaktualisierung so, dass diese von einem zum nächsten Controller weitergeleitet wird. Die Topologie entspricht einer Ringstruktur, daher gibt es immer zwei Replikationspfade pro DC. Wenn ein DC ausfällt, bekommen immer noch alle anderen die Aktualisierung mit.
- **Standortübergreifende Replikation (Site-to-Site):** Dabei müssen die Standorte durch Standortverknüpfungen manuell verbunden sein. Ein KCC pro Standort erstellt alle Verbindungen zwischen Standorten.

9. Was ist eine Vertrauensstellung?
Wenn eine Vertrauensstellung zwischen Domäne A und Domäne B herrscht und sich ein Benutzer bei Domäne A authentifiziert, ist dieser auch automatisch auf Domäne B authentifiziert. Der Benutzer hat aber auf Domäne B nicht die gleichen Berechtigungen wie auf Domäne A.
Vertrauensstellungen können auch transitiv sein (A vertraut B, B vertraut C, dann vertraut A auch C).

10. Was sind Group Policies?
Das sind Zusammenstellungen von Benutzer- und Computerkonfigurationseinstellungen, welche mit Computer, Domänen und OUs verknüpft werden können. Durch diese Richtlinien kann unter anderem eingestellt werden, welche Programme welcher Benutzer anwenden kann. Diese Richtlinien können lokal oder nicht-lokal sein.

Die Gruppenrichtlinien werden in folgender Reihenfolge angewendet:

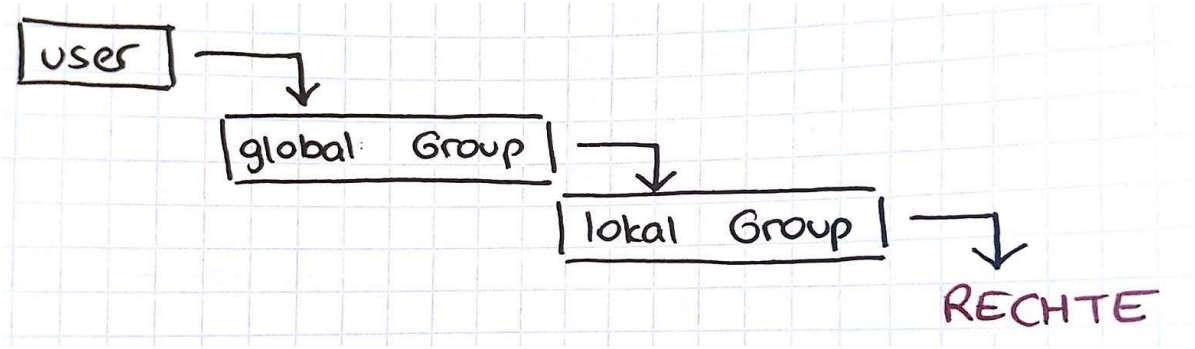
- Lokale GPO

- Mit Standort verknüpfte GPOs
- Mit Domänen verknüpfte GPOs
- Mit Organisationseinheit verknüpfte GPOs

Benutzern sollte man niemals direkt Rechte geben oder ihnen diese verweigern. Es sollten Gruppen erstellt werden, die bestimmte Rechte haben.

- **Globale Gruppen:** Diese Gruppen können Benutzerkonten oder andere globale Gruppen beinhalten. Darin werden User mit gleichen Anforderungen zusammengefasst.
- **Lokale Gruppen:** Diese existieren nur in der jeweiligen Domäne und beschreiben nicht die Mitglieder, sondern die Rechte.
- **Universelle Gruppen:** Die Universellen Gruppen sind überall bekannt und können von jedem verwendet werden.

Die Rechtevergabe sollte auf Ebene der „Lokalen Gruppen“ passieren. Benutzer sollte man in globale Gruppen geben, welche dann in die lokale Gruppe importiert wird. Erst dann sollte die Rechtevergabe erfolgen. Durch dieses System hat man mehr Übersicht und muss bei Änderungen nur die Rechte der Gruppen verändern. Man hat keine eigenen User-Rechte, was Arbeit erspart.



11. Was ist HSM (Hardware Security Module)?
HSM lagert Daten, die lange nicht gebraucht wurden, auf einen externen Datenträger (billiges Langzeitmedium) aus. Bei Gebrauch werden sie automatisch zurück geladen.

12. Was ist EFS (Encrypting File System)?
Das ist ein Verschlüsselungsdienst um Dateiinhalte zu verschlüsseln. Die Schlüsselübertragung erfolgt asymmetrisch mit **public** und **private key**. Die mit dem öffentlichen public key verschlüsselten Daten können nur mit dem private key verschlüsselt werden. Man kann Daten auch mit dem private key verschlüsseln und versenden.

13. Was ist DFS (Distributed File System)?
Damit ist es möglich, auf Verzeichnisse zuzugreifen, ohne den tatsächlichen Speicherort zu kennen. Das DFS trennt dabei physikalischen Speicherort einer Datei von dem Namen, dadurch ist es möglich eine Verzeichnisstruktur zu erzeugen, obwohl die Verzeichnisse auf verschiedenen Speicherorten liegen.

14. Was ist der Kerberos?
ist eine Authentifikationsdienst, welcher dazu dient, eine sichere Authentifikation zu ermöglichen.
Ablauf:

1. Der Kerberos authentifiziert den Server gegenüber dem Client und umgekehrt. Zusätzlich authentifiziert er sich selbst gegenüber beiden.
2. Der Client meldet sich am Kerberos Server an und fordert ein Ticket an.
3. Wird ein Dienst aufgerufen, wird das Ticket an den Dienst gesendet.

Die Kommunikation zwischen Client und Kerberos erfolgt asymmetrisch.

15. Was ist LDAP?
LDAP beschreibt dabei die Kommunikation zwischen dem Client und dem Verzeichnisdienst. Wenn ein Client den Dienst anstößt, erzeugt er dabei eine LDAP-Abfrage, diese wird zum Server gesendet, welcher dann eine Antwort formuliert. Das Protokoll unterstützt alle Funktionen welche notwendig sind: Anmeldungen, Suchanfragen und Änderungen von Daten.

16. Wie kommt der Hypervisor im Active Directory zum Einsatz?
Kein Ahnung.

Ausschreibung

Eine Ausschreibung ist ein öffentliche und schriftliche Aufforderung, Angebote für eine Lieferung oder Leistung abzugeben. Organisationen des öffentlichen Sektors (z.B.: Schulen) sind verpflichtet auszuschreiben, Private können es machen, um ihre Kosten möglichst gering zu halten. Ausschreibungen halten den Wettbewerb zwischen den Anbietern aufrecht, außerdem bietet das Ausschreibungsverfahren eine höhere Transparenz.

1. Was sind die Bestandteile einer Ausschreibung?

- Beschreibung der geforderten Leistung
- Nachweise, mit der die Anbieter ihre Eignung zeigen können
- Ansprechpartner
- Preis mit Aufgliederung
- Sicherstellungen (Vadium – siehe Frage…)
- Angebotsfrist
- Zeit und Ort der Angebotsöffnung

2. Wie läuft eine Ausschreibung ab?

1. **Bekanntmachung:** Die Ausschreibung wird erstellt und je nach Verfahren öffentlich gemacht oder an ausgewählte Unternehmer gesendet.
2. **Angebotsfrist:** Innerhalb der Frist müssen die Angebote eingehen.
3. **Angebotsöffnung:** Bei der formalen Öffnung der Angebote dürfen Vertreter der Unternehmer teilnehmen. Ein Notar muss anwesend sein.
4. **Zuschlagsfrist:** Innerhalb von max. 5 Monaten muss sie der Auftraggeber entscheiden.
5. **Stillhaltefrist:** Innerhalb von 14 Tagen nach der Bekanntgabe des Siegers kann ein anderer Bieter ein Veto einlegen. Das kann passieren, wenn die Ausschreibung beispielsweise aufgrund eines Fehlers ungültig ist. Erst danach erfolgen die Bestellung, der Abschluss eines Vertrages und die Bezahlung.

3. Welche Arten der Vergabeverfahren gibt es?

Grundsätzlich unterscheidet man:

- **Einstufiges Verfahren:** Dabei können alle Unternehmen in der EU teilnehmen, die die Kriterien erfüllen. Nach der Angebotslegung wird der beste Bieter genommen.
- **Zweistufiges Verfahren:** Dabei bestimmt man einen Bieterkreis. Die Bestimmung kann beispielsweise aufgrund der Größe oder des jährlichen Umsatzes erfolgen. Jeder Bieter wird einzeln zu Hearings eingeladen und kann über die Spezifikationen verhandeln. Der Bestbietendste wird genommen.

Weiters:

- **Offenes Verfahren:** Ein einstufiges Vergabeverfahren, für Aufträge über den Schwellenwerten (siehe Frage 11). Es wird EU-weit ausgeschrieben. Bei diesem Verfahren wird eine unbeschränkte Anzahl von Unternehmern eingeladen Angebote abzugeben. Diese müssen ihre Eignung nachweisen. Die Ausschreibung muss an das Amtsblatt der EU geschickt werden.
- **Nicht offenes Verfahren:**
    - **Mit vorhergehender Bekanntmachung:** Es wird eine unbeschränkte Anzahl von Unternehmen öffentlich zur Abgabe von Teilnahmeanträgen eingeladen. Aus den

erhaltenen Teilnahmeanträgen werden die am besten geeigneten Bieter (mind. 5) ausgewählt. Diese geben ihre Angebote ab, der Zuschlag geht an das beste Angebot.
    - **Ohne vorhergehender Bekanntmachung:** Eine beschränkte Anzahl von Unternehmen wird zur Abgabe von Angeboten aufgefordert. Die Auswahl dieser Unternehmer darf nicht diskriminierend sein. Der Zuschlag geht an das beste Angebot. Die Angebotsfrist ist geringer als beim ersten Verfahren.
- **Verhandlungsverfahren:** Dieses muss angewendet werden wenn es sich um eine geistige Wertschöpfung handelt. Nach der Auswahl der besten Bieter werden diese zu Hearings geladen, wobei nicht über den Preis gesprochen werden darf. Mit jedem Bieter werden die gleichen Fragen durchgearbeitet. Sollte nach dem ersten Hearing kein Zuschlag möglich sein, kann es zu weiteren kommen. Sollte ein Zuschlag erfolgen, müssen alle Bieter benachrichtigt werden. Dieses Verfahren unterscheidet man wieder in **„mit vorhergehende Bekanntmachung“** und **„ohne vorhergehende Bekanntmachung“**.
- **Freihändige Vergabe / Direktvergabe:** Das ist nur erlaubt, wenn es sich um einen Folgeauftrag handelt, der ca. 10% des ursprünglichen Preises nicht überschreitet.
- **Dynamisches Beschaffungssystem:** Eine unbeschränkte Anzahl von Firmen wird öffentlich eingeladen, unverbindliche Erklärungen zur Leistungserbringung abzugeben. Diese werden dann zu einem vollelektronischen Beschaffungsprozess zugelassen.
- **Wettbewerblicher Dialog:** Eine unbeschränkte Anzahl von Bietern kann sich beteiligen. Aus diesen wird ein Kreis ausgewählt, ein Gespräch geführt und somit der Bestbieter ermittelt.

4. Was sind Eignungskriterien?

Eignungskriterien beschreiben Mindestanforderungen, die ein Bieter erfüllen muss. Dabei überprüft der Ausschreibende die Befugnis, Zuverlässigkeit und die finanzielle, wirtschaftliche und technische Leistungsfähigkeit. Es müssen alle Elemente erfüllt sein.

Merkmale:

- Sie dürfen nicht diskriminierend sein.
- Sie müssen unternehmensbezogen sein.
- Sie können nur erfüllt oder nicht erfüllt sein.
- Sie können nicht als Auswahl- oder Zuschlagskriterien verwendet werden.

5. Woraus besteht ein Angebot?

- Name des Bieters
- Geschäftssitz des Bieters
- Bevollmächtigte bei Arbeitsgemeinschaften
- Teilleistungen die der Bieter an Subunternehmen weitergeben will
- Adresse
- Nachweis des Vadiums (siehe Frage …)
- Preis mit Aufgliederung

6. Wie funktioniert die Angebotsabgabe?

- **Offenes Verfahren:** Die Unternehmer können innerhalb der Frist ihre Angebote einreichen.
- **Nicht offenes Verfahren**
    - **mit Bekanntmachung:** Ausgewählte Unternehmen erhalten gleichzeitig die Aufforderung, Angebote abzugeben.
    - **ohne Bekanntmachung:** Es werden Angebote von den in Aussicht kommenden Unternehmen eingeholt.

7. Was sind Zuschlagskriterien?
Diese Kriterien ermitteln das technisch und wirtschaftlich beste Angebot (Bestbieterprinzip). Sie dürfen nicht diskriminierend sein und müssen auftragsbezogen sein. Diese Kriterien müssen im relativen Verhältnis zueinander oder in der Reihenfolge ihrer Bedeutung angegeben werden. Sind die Grundlage für die Entscheidung des Auftraggebers und in der Ausschreibung anzugeben.
Zuschlagskriterien können sein:

- Qualität
- Preis
- Technischer Wert
- Rentabilität
- Lieferzeitpunkt
- Betriebskosten
- etc.

Wenn man mehrere Faktoren berücksichtigt, muss man ein Punkteschema einführen.

Beispiel:
Maximale Punkte (Faktor): 30
Zu berücksichtigendes Zuschlagskriterium: Preis
Bieter:

1. Bieter: 100,-
2. Bieter: 150,-
3. Bieter: 200,-

1. Dreieckssatz:

$$Punkte = \frac{bester\ Bieter}{aktueller\ Bieter} * Faktor$$

1. Bieter mit 100,- = 100 / 100 * 30 = 30 Punkte
2. Bieter mit 150,- = 100 / 150 * 30 = 20 Punkte
3. Bieter mit 200,- = 100 / 200 * 30 = 15 Punkte

2. Zweite Art der Berechnung:

$$Punkte = \frac{schlechtester\ Bieter - aktueller\ Bieter}{schlechtester\ Bieter - bester\ Bieter} * Faktor$$

1. Bieter mit 100,- = (200 - 100) / (200 - 100) * 30 = 30 Punkte
2. Bieter mit 150,- = (200 - 150) / (200 - 100) * 30 = 15 Punkte
3. Bieter mit 200,- = (200 - 200) / (200 - 100) * 30 = 0 Punkte

8. Was sind Beurteilungskriterien?
Beurteilungskriterien sind die vom Auftraggeber in der Reihenfolge ihrer Bedeutung festgelegten, nicht diskriminierenden Kriterien, nach welchen das Preisgericht bei Wettbewerben seine Entscheidungen trifft.
Das Preisgericht hat diese Auswahl aufgrund von Wettbewerbsarbeiten, die anonym vorgelegt werden, und nur aufgrund der Beurteilungskriterien zu treffen.

9. Welche Kostenarten gibt es?

- **Regiepreis:** Das ist der Preis für den tatsächlichen Aufwand, der dann bei der Leistung erfolgt.
- **Pauschalpreis:** Das ist der pauschale Preis unabhängig vom Mehraufwand.
- **Festpreis:** Dieser bleibt auch gleich, wenn sich bei Preisgrundlagen etwas ändert.
- **Variabler Preis:** Dieser kann bei Änderungen der Preisgrundlagen geändert werden.
- **Einheitspreis:** Das ist der Preis pro Stück, Meter, Stunde, Kilogramm, usw.

10. Welche Sicherstellungen gibt es?

- **Vadium:** Es dient als Sicherstellung für den Fall, dass der Bieter während der Zuschlagsfrist von seinem Angebot zurücktritt. Es darf 10% des geschätzten Auftragswertes nicht überschreiten und geht, wenn der Bieter das Angebot zurückzieht, an den Ausschreibenden über. Es muss in der Ausschreibung angeführt sein.
- **Kaution:** Diese wird nach der Vorgabe des Angebots verlangt, für den Fall dass der Bieter seine Leistungen nicht erbringt. Sie muss ebenfalls in der Ausschreibung angeführt sein.
- **Deckungsrücklass:** Der Ausschreibende zahlt bei Teilrechnungen nur einen gewissen Prozentsatz (z.B. 95%). Sollte am Ende, bei der Bezahlung der Schlussrechnung, alles in Ordnung sein, zahlt er den Deckungsrücklass zurück. Er muss in der Ausschreibung angeführt sein.
- **Haftungsrücklass:** Der Ausschreibende bezahlt, für den Fall, dass der Auftragnehmer seine Gewährleistung nicht erfüllt, nur einen gewissen Teil der Schlussrechnung (mind. 95%). Nach Ablauf der Gewährleistung bekommt der Auftragnehmer den Betrag zurück. Er muss in der Ausschreibung angeführt sein.

11. Welche Schwellwerte gibt es?

- **Oberschwellbereich:** Werden diese überschritten, muss im öffentlichen Bereich europaweit ausgeschrieben werden.
    - **Für Liefer- und Dienstleistungsaufträge:** 209.000,-
    - **Für Bauaufträge:** 5.225.000,-
- **Unterschwellbereich:** Eine Direktvergabe ist nur bei einem Auftragswert von 100.000,- möglich. Es ist ebenfalls möglich, ein Verhandlungsverfahren ohne vorherige Bekanntmachung anzuwenden solange der geschätzte Auftragswert 100.000 € nicht überschreitet. Es müssen mindestens 3 Angebote eingeholt werden.

12. Wann kann man einen Bieter ausschließen?

Der Ausschluss eines Bieters kann aufgrund von gesetzlichen Übertretungen erfolgen, zum Beispiel aufgrund von Bestechungen oder Steuerhinterziehung.

13. Welche Vor- und Nachteile hat eine Ausschreibung?

Vorteile:

- Man erhält für einen genau definierten Auftrag mehrere Angebote und kann das Beste daraus wählen.
- Ausschreibungen halten den Wettbewerb zwischen den Anbietern aufrecht.
- Ausschreibungen bieten eine hohe Transparenz.

Nachteile:

- Man kann sich seine Auftragnehmer nicht mehr aussuchen, sondern muss das „beste“ Angebot (abhängig von den angewandten Entscheidungskriterien) akzeptieren.
- Gute Ausschreibungen sind aufwändig und teuer; sowohl für die Behörde als auch die Auftragnehmer. Daher ist es nicht verwunderlich, dass es bei Ausschreibungen bisweilen zu

einem Kandidatenmangel kommt. Oligopolbildung ist die Folge, Preisabsprachen sind leicht möglich.

- Bei Ausschreibungen werden möglichst viele Parameter fixiert, sie sind daher unflexibel. Auf kurzfristige Veränderungen kann nur schwer reagiert werden.

Storage Systeme

Storage beschreibt Speicherlösungen im IT-Umfeld, bestehend aus technischen Komponenten und permanenten Speichermedien zur Speicherung digitaler Daten.

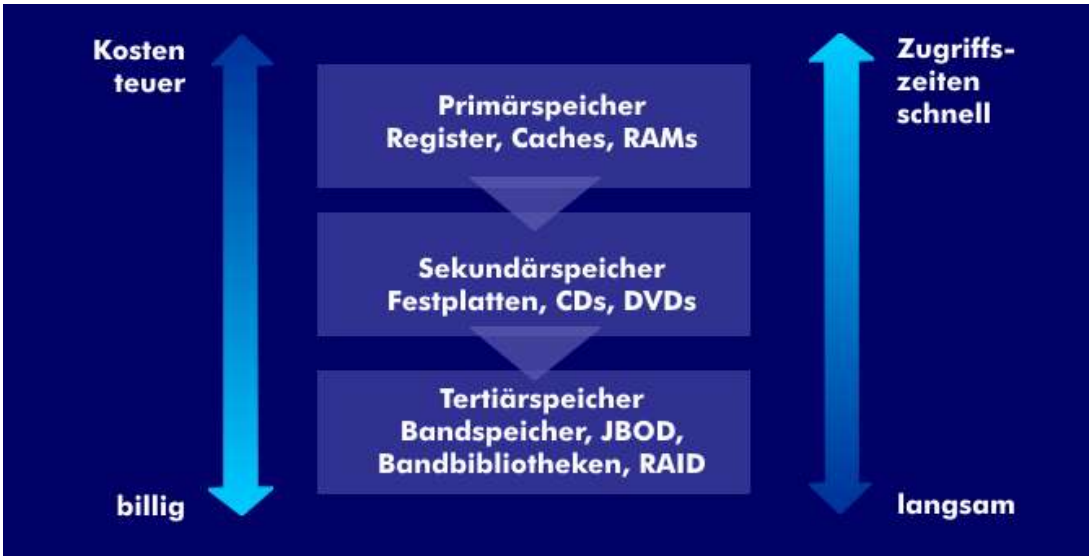
1. Welche Komponenten kann Storage enthalten?

Ein Storage ist eine eigenständige Server-Hardware, welche folgende Komponenten enthalten kann:

- Netzwerkkarten
- RAID-Controller
- Festplatten

2. Welche Arten von Speichern gibt es?

- **Primärspeicher:** Darin sind die Programme und Daten abgelegt, die die Zentralarbeit (CPU) abarbeitet und auf die sie direkt zugreifen muss. Es sind schnelle, flüchtige Speicher, mit vergleichsweise wenig Kapazität, aber hohen Kosten pro Speichereinheit. Dazu gehören beispielsweise die **Register des Caches** und der **Arbeitsspeicher**.
- **Sekundärspeicher:** Dazu gehören **HDD, SSD**, **Flash-Speicher**, **Disketten** und die optischen Speichermedien **CD** und **DVD**. Auf ihnen werden Daten, die nicht für den aktiven Rechenvorgang benötigt werden, ausgelagert. Er hat eine wesentlich höhere Kapazität als der Primärspeicher und kann langfristig Daten speichern. Die Zugriffszeit ist aber langsamer.
- **Tertiärspeicher:** Technisch werden sie durch **Bandlaufwerke** und **Magnetbänder**, durch **Bandbibliotheken**, **Automated Tape Libraries (ATL)**, **RAID-Systeme** und **RAIT-Systeme** realisiert. Sie haben sehr hohe Kapazitäten und sind für die langfristige Archivierung von Daten gedacht. Die Kosten pro Speicherzeiten sind gering, die Zugriffszeiten aber sehr hoch.



3. Was sind Tiers?

Tiers geben an wie schnell ein Speichersystem ist. Je schneller ein Medium ist des teuer ist es normalerweise. Je öfter man auf Daten zugreift, umso schneller sollte das Speicher System sein, auf dem es gelagert wird.

- **Tier 0 Storage:** Es ist das schnellste und teuerste Speichersystem und sollte nur für Daten genutzt werden, die wenig Ausfallzeit und Delay zulassen.
- **Tier 1 Storage:** Dieser beinhaltet unternehmenskritische Anwendungen, kürzlich aufgerufene Daten und top-secret-Files. Es wird auf teuren, hoch qualitativen Medien gespeichert. Prioritäten sind schnelle Read- und Write-Zugriffe.

Auch wenn Tier 1 Daten in schnelleren Systemen gespeichert werden, wird meist gleichzeitig ein Back-Up auf sekundäre Tier Systeme geschrieben.

- **Tier 2 Storage:** . Tier 2 Daten enthalten meistens historische Finanz-Daten, Klassifizierte Files und selten verwendete Daten. Es wird auf billigeren Speichermedien in SAN Systemen gespeichert (siehe Frage 7).
- **Tier 3 Storage:** Tier 3 Speicher bilden das Archiv. Die Archiv Schicht kann event-basierte oder selten benutzte Daten auf langsamen HDDs oder Bändern enthalten.

4. Welche Speichertechnologien gibt es?

1. **Block-Storage:** Darin erfolgen die Zugriffe blockbasierend. Mehrere Blöcke bilden eine Datei/Datensatz. Ein Block enthält eine Adresse. Anhand dieser kann eine Anwendung auf den Block zugreifen.
2. **Grid-Storage:** Dabei werden die Ressourcen unabhängig von dem Ort gespeichert. Bei diesem Speicherkonzept kann die Auslastung, Verfügbarkeit und Speicherkapazität flexibel und dynamisch angepasst werden. Der Zugriff ist unabhängig von der Netzinfrastruktur und dem benutzten Netzwerkprotokoll.
3. **Storage-Virtualisierung:** Der Festplatten-Speicher erscheint nur virtuell, muss also nicht zwingend entlang der physischen Grenzen (pro Festplatte; pro Speichereinheit) aufgeteilt sein. Damit können mehrere Speichersysteme für den Nutzer als eines erscheinen, oder umgekehrt.
4. **Unified-Storage:** Das ist ein Speichersystem, mit dem Dateien und Anwendungen von einem einzigen Gerät aus ausgeführt und verwaltet werden können. Dieses ermöglicht die Speicherung von Dateidaten und verwaltet gleichzeitig den blockbasierten Zugriff von Anwendungen.
5. **Flash-Speicher:** Sie gewährleisten eine nichtflüchtige Speicherung von Daten bei niedrigem Energieverbrauch. Flash-Speicher sind gegenüber Festplatten robuster und weniger störanfällig. Die Daten werden nicht auf mechanischen, sondern auf Flash-Speicher Bauteilen gespeichert.

5. Was ist DAS (Direct Attached Storage)?

DAS bezeichnet an einen einzelnen Host (Rechner, Server…) angeschlossene Festplatten, die sich in einem separaten Gehäuse befinden. Es wird mit Punkt-zu-Punkt-Verbindungen angebracht.

Vorteile:

- DAS bietet einen kostengünstigen Einstieg.
- Es sind keine zusätzlichen Switches oder Verwaltungseinheiten nötig.
- Es ist performant (geringe Laufzeiten, Latenzen, kein Protokoll-Overhead).

Nachteile:

- Es kann nur aufskaliert werden.
- DAS kann nur in geringer Entfernung zum Host angebracht werden.
- DAS kann nur an einen Host angebracht werden.

6. Was ist NAS (Network Attached Storage)?

NAS-Speicher sind zentrale Server, die einen gemeinsamen Speicher für alle dem jeweiligen Rechnernetz zugehörenden Nutzer zur Verfügung stellen. Es wird eingesetzt, um ohne hohen Aufwand unabhängige Speicherkapazität in einem Rechnernetz bereitzustellen. Es via Ethernet-Switch an die bestehende IT-Infrastruktur angeschlossen. NAS arbeitet auf File-Basis.

Vorteile:

- NAS ist einfach einzubinden.

- NAS stellt Daten zentral für alle Nutzer zur Verfügung.
- Je nach Modell ist der Speicher erweiterbar.
- Den Nutzern kann ein bestimmter Speicherplatz zur Verfügung gestellt werden.

Nachteile:

- Die Zugriffszeiten sind höher als beim DAS.
- Es gibt zusätzliche Stromkosten.
- Es führt zu höherer Belastung des LANs.
- Das TCP/IP-Protokoll ist nicht für Storage-Traffic optimiert, da ein relativ großer Protokoll-Overhead entsteht. Es kann aber durch die Verwendung von Jumbo-Frames optimiert werden.

7. Was ist SAN (Storage Area Network)?

Das sind dedizierte Speichernetze, die Server und Speichersysteme über Breitbandnetze wie Fibre Channel miteinander verbinden und gegenseitig entkoppeln. Es bildet eine Erweiterung zum DAS und arbeitet daher blockbasiert. Ein einfaches SAN besteht aus einem Fibre-Channel-Switch, einem oder mehreren Festplattensubsystemen und den Servern, die über so genannte Host Bus Adapter, mit dem SAN-Switch verbunden werden.

Vorteile:

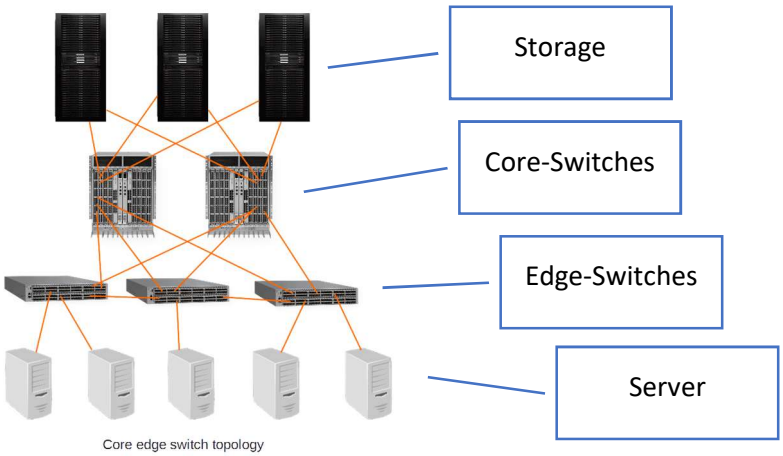
- Ein Vorteil eines SANs ist die direkte Erreichbarkeit aller ins SAN integrierten Komponenten untereinander. Dies heißt, jeder Server kann jedes Storage-System und jedes Tapelaufwerk ansprechen.
- Die Verteilung auf mehrere physische Datenspeicher garantiert eine hohe Daten-Sicherheit.
- Man kann mehrere physische Datenspeicher zu einer großen (virtuellen) Einheit zusammenfassen.

Nachteile:

- Die Anschaffung ist extrem teuer.
- SAN ist nicht leicht richtig aufzubauen und zu managen.
- In SAN kommen viele versch. Komponenten zum Einsatz. Diese sind nicht immer miteinander kompatibel.

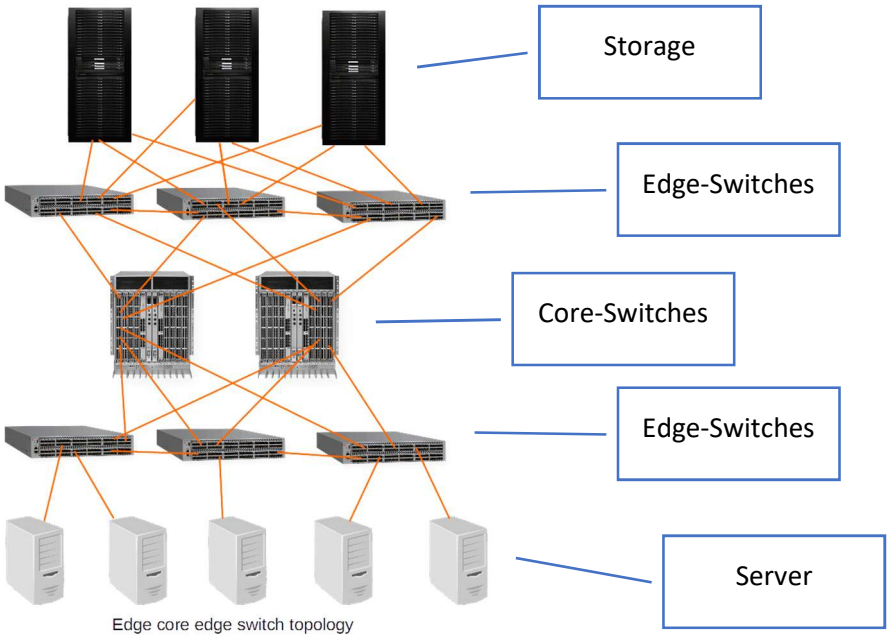
SAN-Topologien:

- **Edge-Core Topology:** Diese Topologie positioniert Speicher auf der Core-Schicht (im „Netzwerkkern“) und Server auf der Edge-Schicht (am „Netzwerkrand“). Da sich Speicher und Server auf völlig unterschiedlichen Switches befinden, bietet diese Topologie eine einfache Verwaltung und eine gute Leistung.



Core edge switch topology

- **Edge-Core-Edge Topology:** Diese Topologie positioniert Server auf einer Edge-Schicht und Speicher auf einer anderen Edge-Schicht, sodass der Kern für Switch-Verbindungen oder die Verknüpfung von Geräten mit netzwerkweitem Geltungsbereich verbleibt.



Edge core edge switch topology

- **Weitere mögliche Topologien:**
  - Single Switch Topology (mit nur einem Switch)
  - Arbitrated Loop (Ring-Topologie)
  - Point-to-Point (Direktverbindung zwischen Speicher und Server)

8. Was sind Bandlaufwerke?
Sie speichern ihre Daten auf Magnetbändern, die sich in Cartridges befinden. Die Datenspeicherung erfolgt sequentiell auf Blockebene, wobei die Informationsblöcke möglichst groß sein sollten. Zur Reduzierung der Datenmenge arbeiten alle Magnetbandspeicher mit Datenkompression. Sie werden hauptsächlich zur Archivierung verwendet.

9. Was ist eine HDD (Hard Disk Drive)?
Das ist eine ganz normale Festplatte mit magnetischem Speichersystem. Dabei kommen rotierende Scheiben zum Einsatz, auf deren Oberfläche die Daten gespeichert werden.
Beim Schreiben von Informationen wird die magnetische Oberfläche der Scheiben dauerhaft und ohne Berührung magnetisiert.
Beim Lesen der Daten tastet ein Sensor diese Magnetisierung der Scheibe berührungslos ab und verwandelt die Werte wieder in lesbare Daten.
Die Daten werden in Blöcken gespeichert.

10. Was ist eine SSD (Solid State Drive)?
Diese arbeiten mit Flash-Speichern. Jedes einzelne Bit wird in Form einer elektrischen Ladung auf einem sogenannten Floating-Gate-Transistor gespeichert. Diese speziellen Transistoren enthalten eine elektrisch isolierte Elektrode, das „Floating Gate“, auf dem die Ladung permanent gespeichert werden kann. Wird eine positive Spannung an das Floating Gate gelegt, so wird die Ladung

gespeichert. Um sie wieder zu entladen, muss eine negative Spannung angelegt werden – daher geht keine Information verloren, wenn die Stromzufuhr abgebrochen wird.
SSDs sind schneller als HDDs und geräuschlos.

11. Was sind Hybrid-Festplatten?
Das ist eine Kombi aus HDD und SSD. Der Flash-Speicher der Festplatte dient der Datenpufferung. Die Daten werden solange in den Flash-Speicher geschrieben, bis dessen Speicherkapazität keine weiteren Daten aufnehmen kann. Danach erst wird der Inhalt des Flash-Speichers auf die Festplatte gelesen.

12. Was ist ein SSA (Solid-State -Array)?
Das ist eine gegliederte Anordnung von mehreren SSDs, auf die viele Server über das SAN zugreifen können.

13. Was ist ein RAID-System?
Siehe Pool 4 – Redundante Systeme.

14. Was ist Cloud-Storage?
Das ist ein Dienst bei dem Daten vom Anbieter gespeichert, verwaltet und dem Kunden über das Internet zur Verfügung gestellt werden. Der Cloud-Dienst ist kostenpflichtig und wird nach unterschiedlichen Tarifierungsmodellen berechnet, beispielsweise auf Basis der zur Verfügung gestellten Speicherkapazität oder abhängig von der Nutzung.

15. Was ist SaaS (Storage as a Service)?
Mit diesem Business-Modell des Cloud-Storage mieten Unternehmen Speicherplatz in der Storage-Cloud und haben damit Zugriff auf unbegrenzte Speicherressourcen.

Virtualisierung

Virtualisierung bildet eine Schicht zwischen Software und Hardware oder Software und Software. Diese bezeichnet man als Anwender und Resource, manchmal auch Wirt und Gast. Hauptsächlich wird Virtualisierung genutzt, um einem Anwender eine Umgebung vorzutäuschen.

1. Warum virtualisiert man?

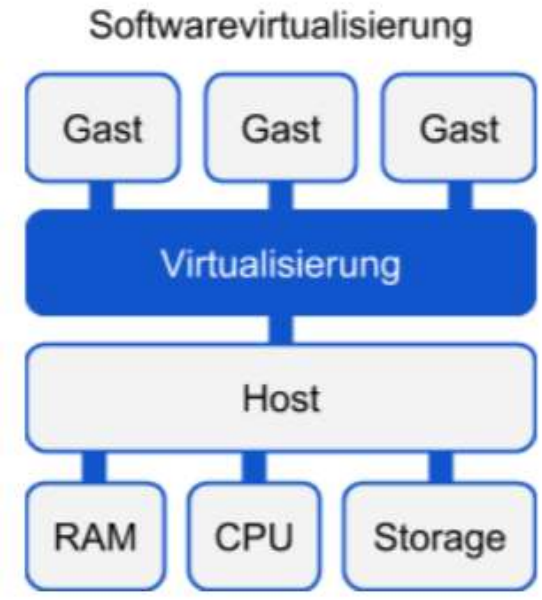
- Hardwareunabhängigkeit auf Grund der Virtualsierungsebene
- Verringerung der Administrations- und Serverwartungskosten
- Optimierung des Platzbedarfs
- Verbesserung der Ausfallsicherheit und des Disaster Recovery
- Erhöhung und Verbesserung der Flexibilität und Skalierbarkeit
- Verbesserung des Energieverbrauchs und der Wärmeentwicklung (z.B. USV, Klimaanlage)
- und viele mehr

2. Welche Arten von Virtualisierung gibt es?

- Softwarevirtualisierung
    - Containervirtualisierung
    - Virtuelle Maschinen
- Hardwarevirtualisierung
    - Systemvirtualisierung
    - Partitionierung and Pooling
    - Domaining
    - Prozessorvirtualisierung
    - Speichervirtualisierung
- Netzwerkvirtualisierung

3. Was ist Softwarevirtualisierung?

Bei dieser Art der Virtualisierung werden Gastsysteme auf einem Host-System betrieben. Diese Gastsysteme können von einzelnen Anwendungen bis zu ganzen Betriebssystemen reichen. Die Virtualisierung täuscht Umgebungen vor und bildet eine zusätzliche Schutzschicht.



4. Was ist Containervirtualisierung (Betriebssystemvirtualisierung)?
Dabei werden Gastsysteme in Containern ausgeführt und im Idealfall komplett vom Host isoliert. Auf dem Host werden mehrere virtuelle Laufzeitumgebungen erzeugt (Jails), die für die laufenden Programme als normale Betriebssysteme wirken. Die Applikationen sehen nur die Applikationen, mit denen sie ihre virtuelle Umgebung teilen.
Vorteil: Es ist leichter Programme zu transportieren und ihren einwandfreien Betrieb zu garantieren.
Beispiele: FreeBSD Jails, Solaris Zone/Container, Linux VServer, Open VZ und Virtuozzo

5. Was sind virtuelle Maschinen?
Durch virtuelle Maschinen ist es möglich ein Betriebssystem in einem Betriebssystem zu starten. Dazu wird ein sogenannter Hypervisor(Typ 2) (siehe Frage 6) verwendet.

Systembasierte virtuelle Maschinen:
Diese bilden einen realen Rechner so vollständig nach, dass normale Betriebssysteme, die für reale Rechner entworfen sind auf der virtuellen Maschine laufen.
Vorteile:

- Betrieb von mehreren Betriebssystemen gleichzeitig
- Plattformunabhängigkeit
- Höhere Effizienz (der Hardwarenutzung) im Parallelbetrieb
- Sicherheit
- Wartbarkeit

Nachteile:

- Effizienzverlust (durch den Betrieb des Hypervisors)
- Die virtuellen Maschinen beeinflussen sich, da sie sich die Hardware teilen

Prozessbasierte virtuelle Maschinen (Anwendungsvirtualisierung):
Diese ermöglichen es, einzelne Anwendungen unabhängig vom Host-System auszuführen. Der bekannteste Vertreter dieser Art ist das **JRE** (Java Runtime Environment) das Java plattformunabhängig macht.
Vorteile:

- Plattformunabhängigkeit
- Dynamische Optimierung (weil die VM für die Ausführung verantwortlich ist und nicht das OS)

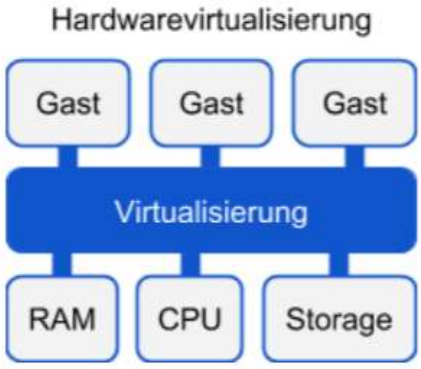
Nachteile:

- Geschwindigkeitsverlust

6. Was ist ein Hypervisor?
Er bildet eine abstrahierende Schicht zwischen tatsächlicher Hardware bzw. dem Host-System und den Gastsystemen. Er ist dafür zuständig, dem Gastsystem Ressourcen zur Verfügung zu stellen. Dadurch ist es möglich den Gästen eine bestimmte Umgebung vorzutäuschen die nicht der realen Umgebung entspricht.

- **Typ 1 (nativer Hypervisor):** Dieser setzt direkt auf der Hardware auf und braucht bestimmte Treiber für den Hardwarezugriff.
- **Typ 2 (hosted Hypervisor):** Dieser setzt auf einem Hostsystem auf und nutzt Gerätetreiber für den Hardwarezugriff.

7. Was ist Hardwarevirtualisierung?
Dabei wird direkt von der Hardware virtualisiert, anstatt auf einem Hostsystem.



8. Was ist Systemvirtualisierung?
Das ist die Trennung eines Computersystems in eigenständige OS, d.h. auf einem einzelnen Rechner laufen mehrere (verschiedene) Betriebssysteme. Die Systemvirtualisierung findet heute vielfach in Form der Server-Partitionierung Einsatz, besonders in Rechenzentren.
Alle Systeme teilen sich dieselbe Hardware. Diese wird durch einen Hypervisor, nach Bedarf, den Systemen zugewiesen.
Vorteile sind geringe Kosten wegen effizienterer Nutzung der Hardware, geringer Platzbedarf und erhöhte Wartbarkeit.

9. Was sind Partitionierung and Pooling?
Hierbei wird eine große Hardwarekomponente virtuell auf mehrere kleine abgebildet.

10. Was ist Domaining (Virtual Hosting)?
Das ist ein Verfahren das es ermöglicht mehrere Domains auf einem physischen Server anzubieten.
Vorteile sind die Kostenersparnis und man kann mehrere Domains mit sprechenden Namen auf einem Server anlegen.

- **Name-based:** Dabei laufen mehrere Domains auf einer IP. Der Client muss den Host-Header setzen um die richtige Domain anzusprechen.
- **IP-based:** Jede Domain erhält eine eigene IP-Adresse, dadurch kann jedes beliebige Protokoll verwendet werden. Es läuft komplett serverseitig ab, da der Client nur die IP braucht.
- **Port-based:** Jede Domain erhält ihren eigenen Port.

Die wichtigste Anwendung von Virtual Domaining is das **Shared Web Hosting**, wobei eine große Anzahl verschiedener Websites auf dem selben System angeboten werden.

11. Was ist Prozessorvirtualisierung?
Befehle werden nicht an den Prozessor, sondern an einen Hypervisor, der die Befehle an die native Hardware anpasst und an den Prozessor weiterleitet. Das ermöglicht eine schnellere Kommunikation zwischen Gast-System und Hardware da sich der Prozessor um die Unterscheidung zwischen Gast- und Host-System kümmert. Manche Prozessoren unterstützen dies automatisch (AMD-V, VT-x).

12. Was ist Speichervirtualisierung?
Der Zugriff auf den Speicher erfolgt nicht mehr direkt, der angezeigte Speicher muss nicht mit dem physischen Speicher übereinstimmen. Beispiel: RAID-Systeme.

Vorteile:

- für den Anwender: angepasste Verzeichnisstruktur
- für den Anbieter: höhere Effizienz.

Block-Virtualisierung:
Es wird ein logisches Interface geschaffen über das man auf den gesamten Speicher zugreifen kann. Diese Trennung der Hardware vom Zugriff bringt erhöhte Flexibilität in der Speicherverwaltung. Ressourcen erhalten eine Logical Unit Numbers (LUN) und eine Logical Block Address (LBA), über die sie angesprochen werden.

Erforderliche Schritte:

- **Speicher-Neuzuordnung:** Die User-Ansicht ergibt sich aus mehreren Virtualisierungsschichten. Im Hintergrund werden alle Speichermedien zu einem Storage Pool zusammengefasst.
- **Metadaten:** Der Zugriff erfolgt nicht mehr über den realen Pfad, also müssen Metadaten angelegt werden, um diese wiederzufinden und zu verwalten (mit Mapping-Table, Hashing).
- **I/O-Umleitung:** Das virtualisierte System erhält Zugriffsanfragen, findet den tatsächlichen Speicherort und liefert die geforderten Daten zurück.

Block-Virtualisierung kann auf drei Arten geschehen:

- **Host-basiert:** Ein Softwarelayer zwischen Anwender und Hardware abstrahiert den Speicher. Moderne OS unterstützen dies automatisch.
- **Speicher-basiert:** Die Speichermedien werden zusammengefasst und zusätzlich wird Replikation und erhöhte Performance angeboten (bei RAID-Systemen).
- **Netzwerk-basiert:** Die Virtualisierung passiert zwischen einem Storage Area Network und den Nutzern. Das ist besonders nützlich da es einen einzelnen Zugriffspunkt für den gesamten Speicher definiert.

Die **Replikation** muss die Virtualisierungsschicht passieren.

- **Mirroring:** Jeder Zugriff/jede Veränderung wird sofort repliziert.
- **Snapshots:** An einem Zeitpunkt wird das gesamte System repliziert.

Vorteile:

- Sichere Speicherverwaltung
- Speicheroptimierung

Nachteile:

- erhöhte Komplexität
- Geschwindigkeitsverlust

Datei-Virtualisierung:
Es ermöglicht den einheitlichen Zugriff auf unterschiedlichste File-Systeme. So kann man zum Beispiel auf eine lokale Datei genau gleich zugreifen, wie auf ein Netzwerk-Datei.

13. Was ist Netzwerkvirtualisierung?
Durch Netzwerkvirtualisierung werden die physischen Netzwerkressourcen in logische Einheiten geteilt, d.h. die Virtualisierungsschicht liegt im Netzwerk. Durch diese Trennung von Hardware und Logik ist es möglich mehrere Netzwerke auf derselben Hardware einzurichten und so leichter zu verwalten. Dazu gehören **VLAN** und **VPN**. **Siehe dazu Pool 4 – Ethernet und VPN.**

14. Was ist Paravirtualisierung?
Dabei handelt es sich um eine Virtualisierungstechnologie bei der nur Instanzen virtualisiert werden.
Der Gast braucht einen Kernel, der direkt mit der Virtualisierungsschicht kommuniziert und nicht direkt mit der physikalischen Hardware (keine Ahnung, ob das stimmt lol).

15. Was ist Desktopvirtualisierung?
Dabei wird der Desktop virtualisiert. Dieser läuft vollständig auf einer Server und wird zum Client gestreamt. Der Client benötigt nur einen Loader, der den Stream entgegen nimmt.

16. Was ist der Unterschied zwischen einer Desktopvirtualisierung und einem Terminalserver?
Desktopvirtualisierung: Die Applikation wird vollständig gestreamt (Registerinhalt wird mitübertragen).
Terminalserver: Dieser liefert nur die Bildschirmdarstellung, Maus und Tastatur.

17. Was ist der Unterschied zwischen einer Virtualisierung und einer Emulation?
Emulation: Das ist das funktionelle Nachbilden eines Systems durch ein anderes, ohne direkte Unterstützung durch das Betriebssystem oder den Prozessor. Das nachbildende System (Emulator) verhält sich im Idealfall wie das originale System hat aber keinen direkten Zugriff auf die Hardware, sondern nutzt wie jede andere Software die Funktionen des Betriebssystems.

Virtualisierung: Das ist eine zusätzliche Abstraktionsschicht zwischen Wirtssystem und Gast und kommt ohne die direkte Unterstützung durch den Prozessor oder zumindest das unter ihm liegende Betriebssystem nicht aus.