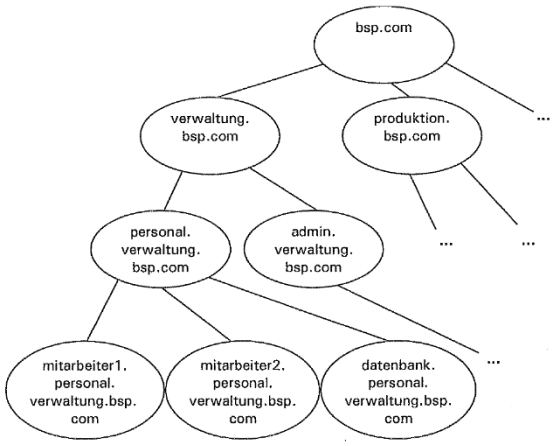
M159 ZF I

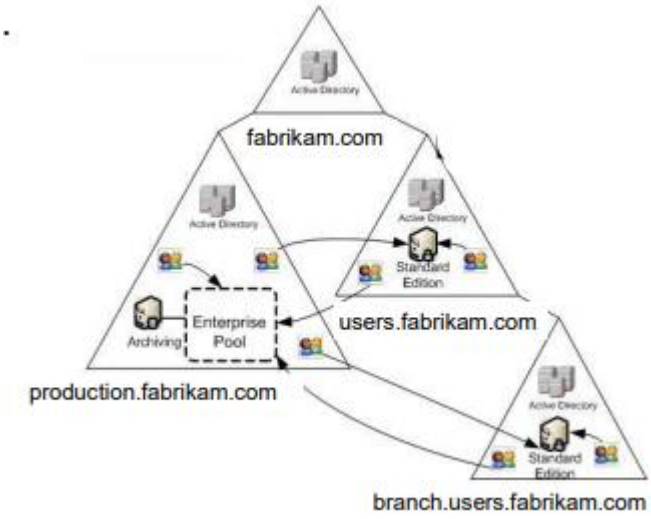
1. Was ist ein Verzeichnisdienst
    - Funktionsweise
        - Grosse Datenbank zum Speichern von Netzwerkressourcen
            - Benutzer
            - Gruppen
            - Computer
            - Freigaben
    - Einsatz
        - Zentrale Verwaltung von Infrastruktur, Policys und Netzwerkressourcen
    - Eigenschaften
        - Skalierbarkeit
            - Gezielte Anpassung
            - Neue Ressourcen können ohne Änderungen hinzugefügt werden
        - Erweiterbarkeit
            - Zusätzliche Objekttypen können hinzugefügt werden
        - Sicherheit
            - Zugriff auf Daten nur für autorisierte Personen möglich
        - Verfügbarkeit
            - User können auf ständig auf aktuelle Daten zugreifen
        - Performance
            - Zugriff auf die Daten erfolgt schnell und zuverlässig
    - Standards und deren Aufgaben
        - X.500
            - Bildet konzeptionelle Grundlage der AD
            - Ist ein Standard für den Aufbau eines AD
        - DNS
            - Dient als «Telefonbuch» für den Client -> damit dieser Domäne findet
        - LDAP
            - Bereitstellung zentraler Ort für Authentifizierung
            - Zugriff von Fremdsystemen auf AD
2. X.500 Standard
    - Eigenschaften
        - Nach diesem Standard kann global auf die AD zugegriffen werden
        - Daten aufgrund vorgegebener Struktur abgelegt
        - Einheitlicher Namenskontext
        - Dezentraler Aufbau
    - Zusammenhänge der Namensbildung (DN, RDN)
        - Distinguished Name (DN) = setzt sich aus mehreren Ebenen zusammen
            - Z.B. CN=Max Mustermann, OU= Users, OU=Riethüesli, DC=GBS.local
        - Relative Distinguished Name (RDN) = Name einer Ebene
            - Z.B. CN= Max Mustermann
    - Klassen
        - Definieren Eigenschaften von Objekten, z.B.
            - Computer
            - Benutzer

        - Gruppe
        - Drucker-Warteschlange
    - Attribute
        - Definieren Eigenschaften (Wert) von Feldern, z.B.
            - Byte
            - Numerisch
            - Unicode-Zeichenfolge
            - Case-Sensitive (ja/nein)
            - Zeit
            - SID
            - Adresse
    - OID
        - Object Identifier ID
        - Für Klassen
    - Single-Master Replikation
        - Ein Server macht Änderungen auf Daten
        - Kopien der Änderungen werden an Slave-Server übertragen
        - Änderungen nur auf Master-Server möglich
    - Multi-Master Replikation
        - Mehrere Computer machen Änderungen an Daten
        - Jeder Übernimmt die Änderungen des anderen
3. Domain Name System
    - Hierarchischer Aufbau



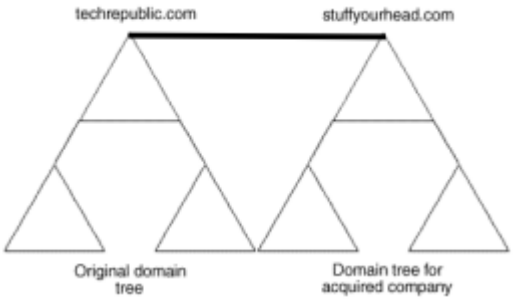
    - Eigenschaften
        - Basiert auf TCP/IP
        - DNS-Domäne ist eine Verwaltungseinheit, die Sub-Domänen enthalten kann
        - Kann Mitglied einer übergeordneten Domäne sein
    - Zonentypen
        - Forward-Lookup-Zone
            - FQND -> IP
        - Reverse-Lookup-Zone
            - IP -> FQND
        - Primäre Zone
            - Enthält originale Zonendaten (Webserver-Name, -IP
        - Sekundär Zone

        - Erhält Kopie der Daten
        - Frägt periodisch neue Daten ab
4. Domäne und Standort
    - Logische Sicht
        - Mit dreiecken
        - Grundsätzlich nur eine Domäne
        - Empfehlung 2 DC pro domäne
        - Weitere Domänen nur bei
            - Schemaschutz
            - Autonome oder eigenständige Verwaltung
            - Eigener Sicherheitsbereich
    - Physische Sicht
        - Durch Elipsen dargestellt
        - Bei üblicher WAN verbindung -> 1 DC pro standort
        - Bei Hochgeschw. 1 DC und 1 standort
    - Schutzschema
    - Sicherheitsgrenzen
        - Domänengrenzen sind auch Sicherheitsgrenzen
        - Admin von übergeordneter Domäne hat nicht zwinged Admin Rechte
        - Benutzergruppen können übergreifende Berechtungen haben
    - Replikation DC
        - Vermeiden von SPOF
        - Jeder DC schreibt auf AD
        - Jeder DC enthält alle Objekte aller Domänen
    - RODC
        - Read Only DC
        - Nicht alle Objekte werden repliziert
    - Strukturierungsmöglichkeiten mittels OU
        - Firmenstuktur
        - Zuweisen von Verwaltungstätigkeiten
        - Gruppenrichtlinen
        - Skalierbarkeit
    - Verschiedene Modelle
        - Singledomain
            - Geeignet für meisten Fälle
            - Einzelner DC
            - Beinhaltet alle Netzwerkressourcen
        - Tree



- Nur nötig bei
  - Unabhängier Verwaltung
  - Stämmdomäne keine Produktionsobjekte enthalten soll
- Dinge können auf Domänenebene getrennt werden

- Multi-Forest
  - Mehere Stammdomänen -> unterschiedliche Schemas
  - Domänen sind paralell zueinander
  - Zwei verbundene ADs



- Forest
  - AD beherbergt alle Domänen
  - Unterschiedliche DNS-Domänen lassen sich mischen