Active Directory

Hierarchischer Windows-Verzeichnisdienst
für die zentrale Verwaltung von Objekten (Benutzer, Gruppen, Computer, Drucker, ..) in Domänen.

Bezeichnungen

Server 2000, 2003, 2008: Active Directory (**AD**)
Server 2008R2 : Active Directory Domain Services (**ADDS**)

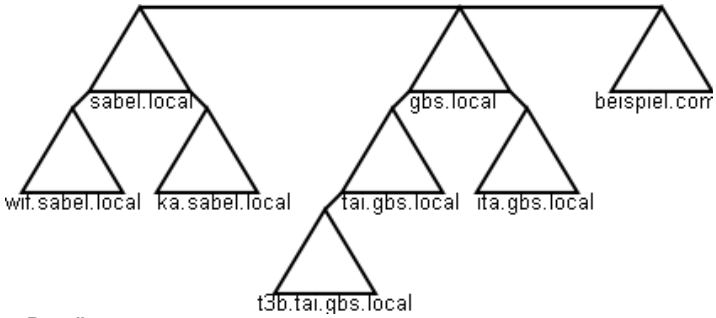
Verwendete Protokolle

- **TCP/IP**: Netz
- **DNS**: Namensauflösung
- **Kerberos**: Authentifizierung
- **LDAP**: Abfrage und Modifikation der Verzeichnisdaten

Hierarchische Struktur

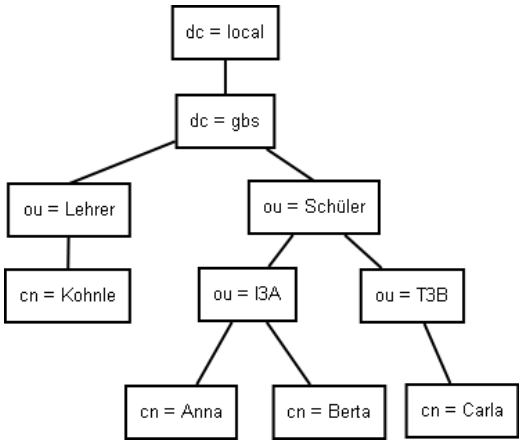
- **Forest** (Gesamtstruktur): ein einheitliches Schema, enthält mindestens einen Tree
- **Tree** (Baum): einheitlicher Namensraum, enthält mindestens eine Domäne und evtl. Subdomänen
- **Domain** (Domäne): enthält mindestens einen Domaincontroller und folgende Objekte
  - **Organizational Unit** (Organisationseinheit): Container für Objekte
  - **Domänencontroller** (DC)
  - **Memberserver**: kein DC, sonstige Dienste
  - PCs
  - Benutzer
  - Gruppen
  - ...

Aufbau einer Gesamtstruktur (Forest)

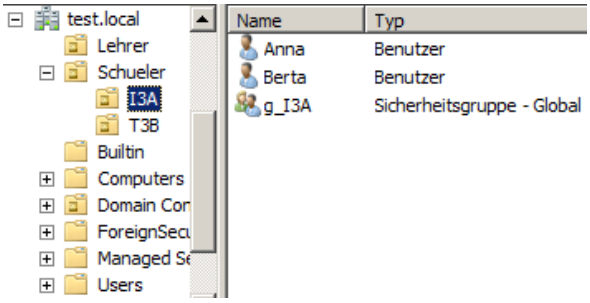


Struktur einer Domäne

LDAP-Datenstruktur



Anzeige im mmc-Snap-In Active Directory-Benutzer und -Computer



Replikation

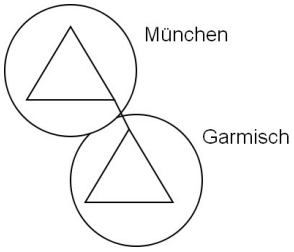
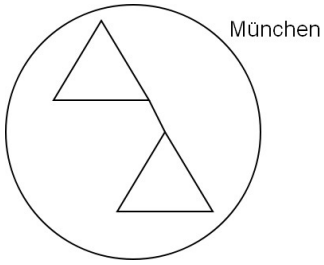
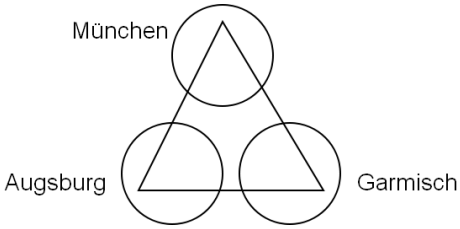
Synchronisation der Daten mehrerer Domänencontroller

Schema

Datenbankstruktur des AD. Definiert, welche Klassen von Objekten es gibt (z.B. Benutzer) und welche Attribute die Objekte haben (z.b. E-Mail-Adresse). Alle Domänen innerhalb einer Gesamtstruktur (Forest) verwenden dasselbe Schema.

Standort (Site)

- wird durch ein oder mehrere IP-Netze definiert
- Verwaltung: „Active Directory -Standorte und -Dienste“
- Verknüpfung: Name – IP-Subnet

a) Jeder Standort eine Domäne	b) Mehrere Domänen an einem Standort	c) Eine Domäne über mehrere Standorte verteilt
		

Namen von Objekten

LDAP (Lightweight Directory Access Protocol)

Protokoll zur Abfrage und Modifikation der Verzeichnisdaten einer Baumstruktur.
Es gibt verschiedenen Objektklassen:

- Domain Component (DC)
- Organizational Unit (OU)
- Common Name (CN)
- ...

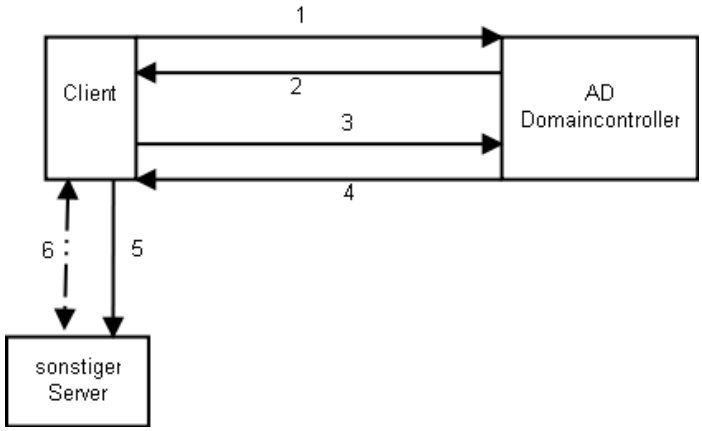
Jedes Objekt wird im Verzeichnisbaum eindeutig durch seinen **Distinguished Name** (DN) identifiziert.
Jedes Objekt hat auch einen **kanonischen Namen**.
Jeder Benutzer hat auch einen **User Principal Name** (UPN).

LDAP-Name: **Distinguished Name** (DN)	**kanonischer Name**	**Anmeldename:** **User Principal Name** (UPN)
`cn=Kohnle,ou=Lehrer,dc=gbs,dc=local`	`gbs.local/Lehrer/kohnle`	`kohnle@gbs.local`
`cn=Anna,ou=I3A,ou=Schüler,dc=gbs,dc=local`	`gbs.local/Schüler/I3A/Anna`	`anna@gbs.local`

Da im UPN keine OUs vorkommen, müssen **Benutzernamen** innerhalb einer Domäne **einmalig** sein!

Kerberos

Protokoll zur Authentifizierung.



1. Client schickt Anmeldedaten und fordert vom Domaincontroller TGT (Ticket Granting Ticket) an.
2. Domaincontroller überprüft Anmeldedaten und sendet TGT an Client => Client ist authentifiziert.
3. Client fordert mit seinem TGT ein ST (Service Ticket) speziell für den Zugriff auf sonstigen Server an.
4. Domaincontroller überprüft Anmeldedaten und sendet ST.
5. Client sendet das vom Domaincontroller zertifizierte ST an den sonstigen Server => sonstiger Server weiß nun ,dass der Domaincontroller bestätigt hat, dass der Client derjenige ist, der er behauptet zu sein.
6. Die eigentliche Kommunikation zwischen Client und sonstigem Server kann beginnen