Windows Server 2012

Active Directory Services (ADS)

Domain Name Service (DNS)

Was wird behandelt?

- Einführung in Active Directory Services (ADS)
- Strukturelemente von Domänen
- Organisation von Domänen
- Domain Name Service (DNS)
- AD-Management

Was ist ADS?

- Verzeichnisdient zur Verwaltung aller Ressourcen eines Netzwerkes
  (z.B. Benutzer, Drucker, Dienste, Anwendungen, Daten, Geräte usw.)
- gemeinsame einheitliche hierarchische Datenbank
- Sicherheit durch Authentifizierung nach Kerberos und verschiedene weitere Sicherheitskonzepte

Was leistet Active Directory?

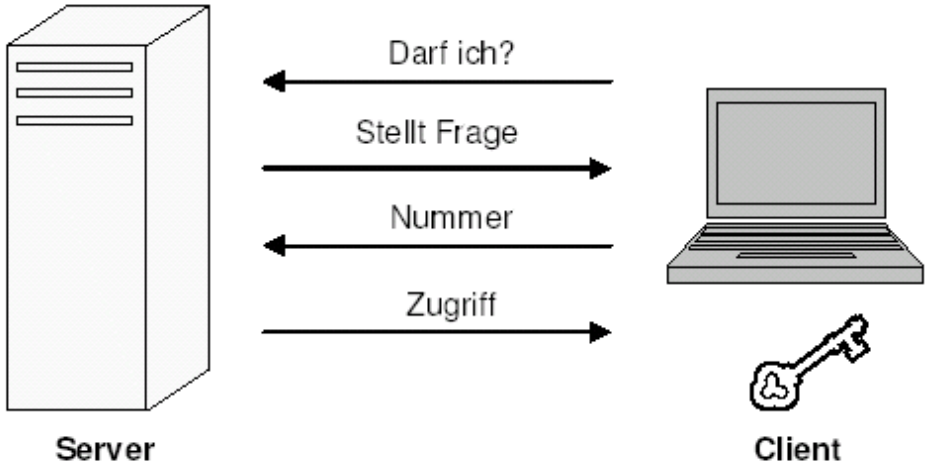
- Anzahl der verwalteten Objekte
- Sicherheit
- Verwaltung
- Erweiterbarkeit
- Flexibilität
- Performance
- Interoperabilität

Wie sicher ist Active Directory?

- Anmeldeauthentifizierung
- Gruppenrichtlinien
- Zugriffsberechtigungen
- Freigaben
- Verschlüsselung von Daten (EFS)
- Sichere Protokolle (Ipsec)
- Kerberos V5

Was bedeutet Kerberos?

- Sicheres Authentifizierungsverfahren des MIT für die Verwendung auf unsicheren Medien
- Verschlüsselte Übertragung für die Kommunikation zwischen Client und Server



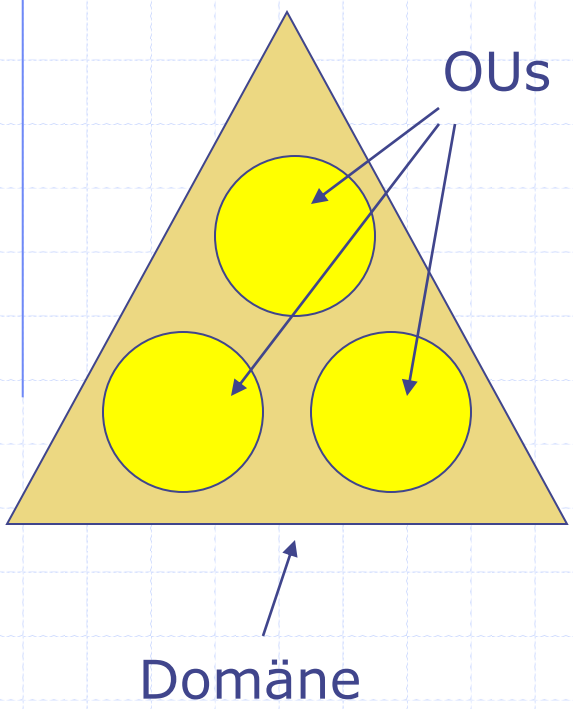
Der Client besitzt einen Schlüssel für mathem. Funktionen, die aus der Frage des Servers eine Nummer erzeugen.

zurück

Was ist eine Domäne?

- Grundbaustein des Active Directory
- beinhaltet alle Objekte eines bestimmten Administrativen Bereichs.
- Entspricht häufig einem physischen Standort
- Domänen können mit Hilfe von Organisatorischen Einheiten (OUs) weiter untergliedert werden.
- Mehrere Domänen können zu einem Active Directory Tree zusammengefasst werden.

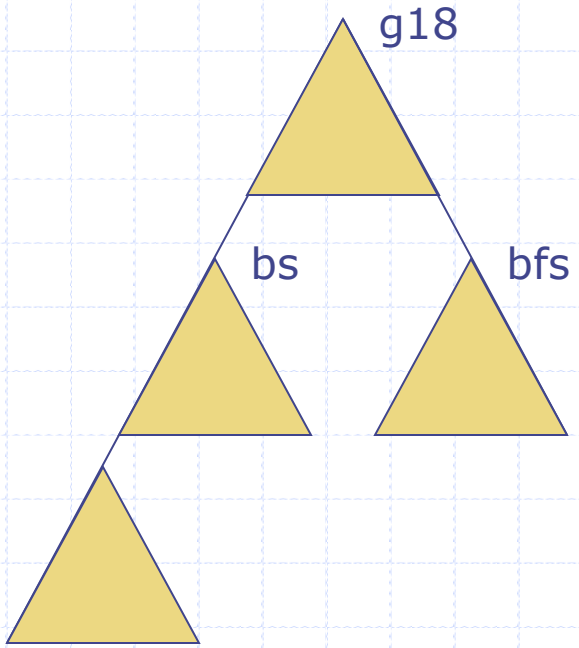
Was sind OUs?



- Aufteilung der Gesamtdomäne in einzelne Abschnitte - die OUs.
- Gruppierung bestimmter Objekttypen oder
- Untergliederung nach firmeninterner Organisationsstruktur
- Anwendung von Systemrichtlinien
- Delegationsmöglichkeit für Administrationsaufgaben

Was ist ein AD – Tree?

- Ein Tree enthält alle in einem Namensraum (z. B. g18.de) zusammengefügten Domänen.
- Domänen sind innerhalb des Trees hierarchisch aufgebaut,
- transitive Vertrauensstellungen zwischen Domänen eines Trees.
- Alle Domänen eines Trees haben einen gemeinsamen globalen Katalog (zentrale Datenbank).
- Mehrere Trees können zu einem Forest zusammengeführt werden.



it (relativer Name)

it.bs.g18 (absoluter Name)

Was ist ein Forest?

- Die höchste Ebene einer Active Directory Struktur (Gesamtstruktur).
- Ein Forest beinhaltet einen oder mehrere Active Directory Trees.
- Zwischen den Trees werden automatisch Vertrauensstellungen aufgebaut.
- Die in einem Forest enthaltenen Active Directory Trees verfügen über unterschiedliche Namensräume (z. B. g18.de und g18.com).
- Ein Active Directory enthält immer mindestens einen Forest - auch dann, wenn nur ein Tree vorhanden ist.
- Alle Trees innerhalb eines Forest besitzen das gleiche Active Directory Schema.

Was ist ein AD - Schema?

- Es beschreibt den Aufbau aller Objekte innerhalb des Active Directory (z.B. Drucker, Benutzer oder Computer)
- Das Schema ist auf allen Domänen-Controllern innerhalb des Forests gespeichert. Es ist innerhalb des gesamten Forests einheitlich.
- Das Schema kann modifiziert werden.
- Es können neue Attribute und Objekte erzeugt werden.
- Objekte können nur hinzugefügt werden können, nicht aber wieder gelöscht werden.

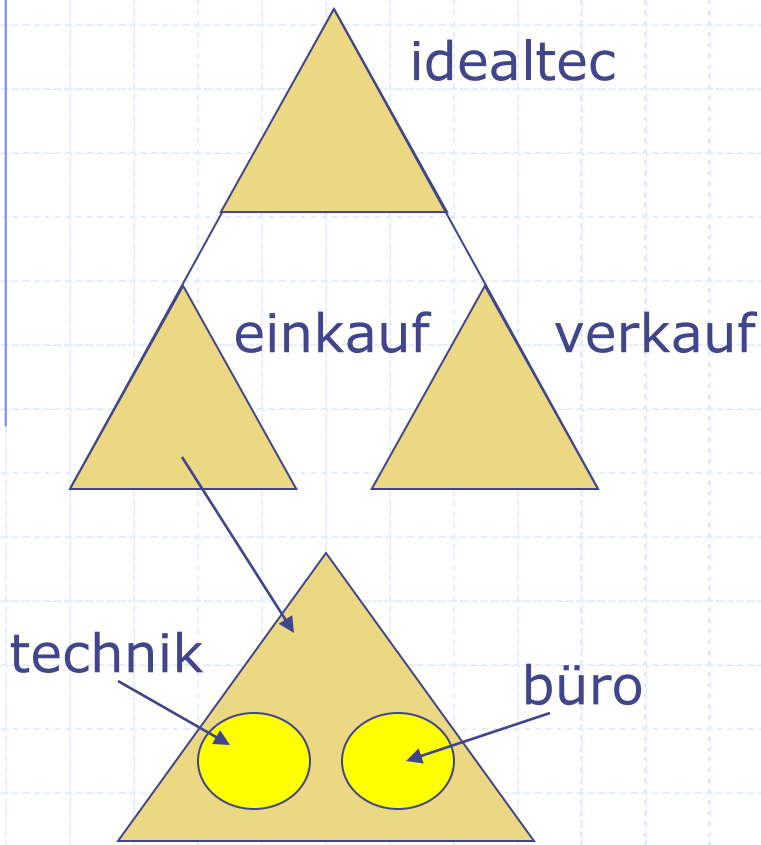
zurück

Domänenorganisation

- Organisationsbasierte Hierarchie
- Funktionsbasierte Hierarchie
- Mischhierarchie nach Standort und Organisation
- Mischhierarchie nach Organisation und Standort

weiter

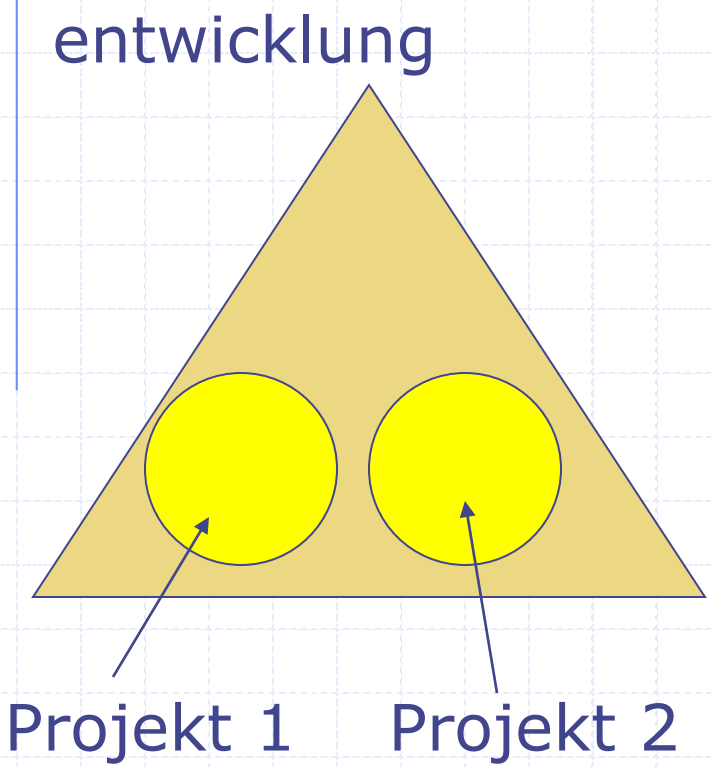
Organisationsbasierte Hierarchie



- Reflektiert das Geschäfts-modell
- Hoher Änderungsaufwand bei Umstrukturierung
- Autonomie der Abteilungen
- Offen für Zusammen-schlüsse und Erweiterungen
- Geeignet für dezentrale IT-Organisation

weiter

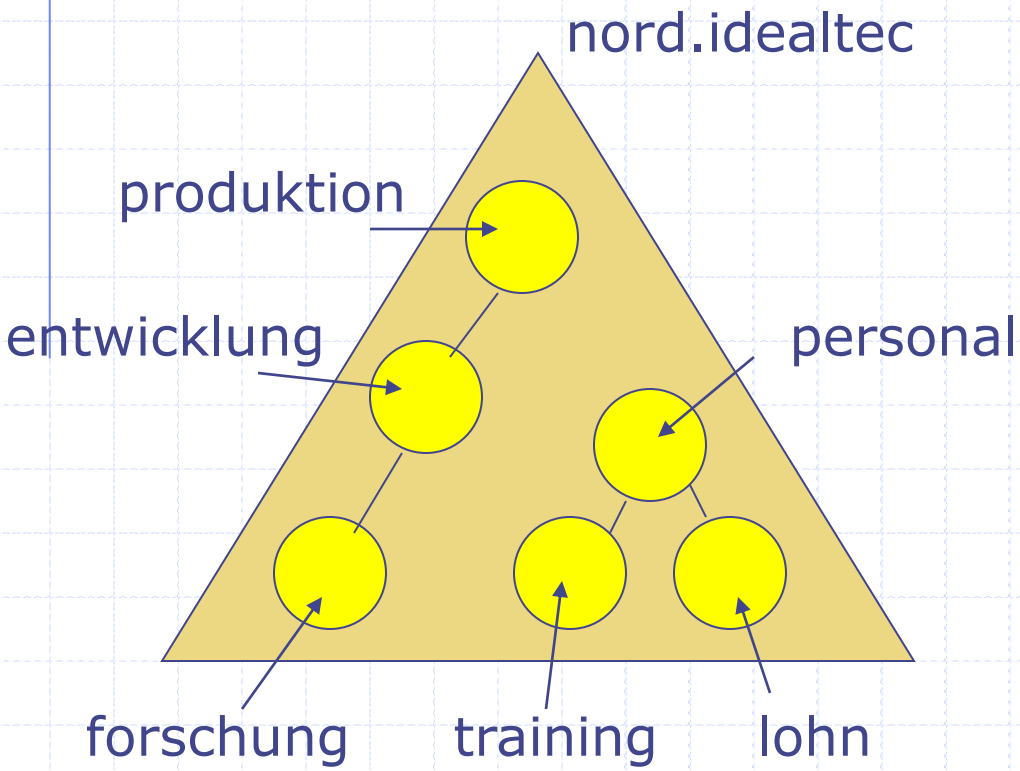
Funktionsbasierte Hierarchie



- Nur für kleine Organisationen geeignet
- Keine Änderungen bei Umstrukturierungen erforderlich
- Für dezentrale IT-Organisation
- Gut für abteilungs-übergreifende Teams

weiter

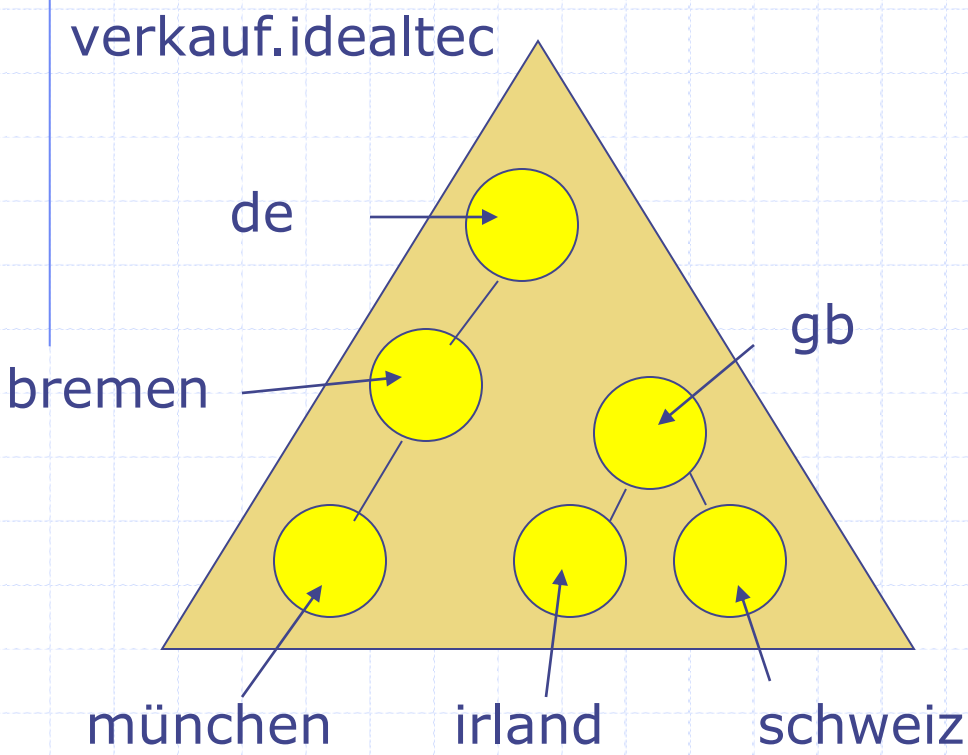
Mischhierarchie nach Standort und Organisation



- Gestattet geographisches Wachstum
- Ermöglicht unterschiedliche Sicherheits-grenzen
- Geeignet für zentralisierte IT-Organisation

weiter

Mischhierarchie nach Organisation und Standort



- Für große, stark verteilte Organisationen mit physisch verteilten Geschäftsbereichen
- Verwaltungsfunktionen können scharf getrennt werden
- Aufwendige Umstrukturierungen
- Keine effektive Netzwerknutzung durch Domäne an mehreren Standorten

zurück

Domain Name Service

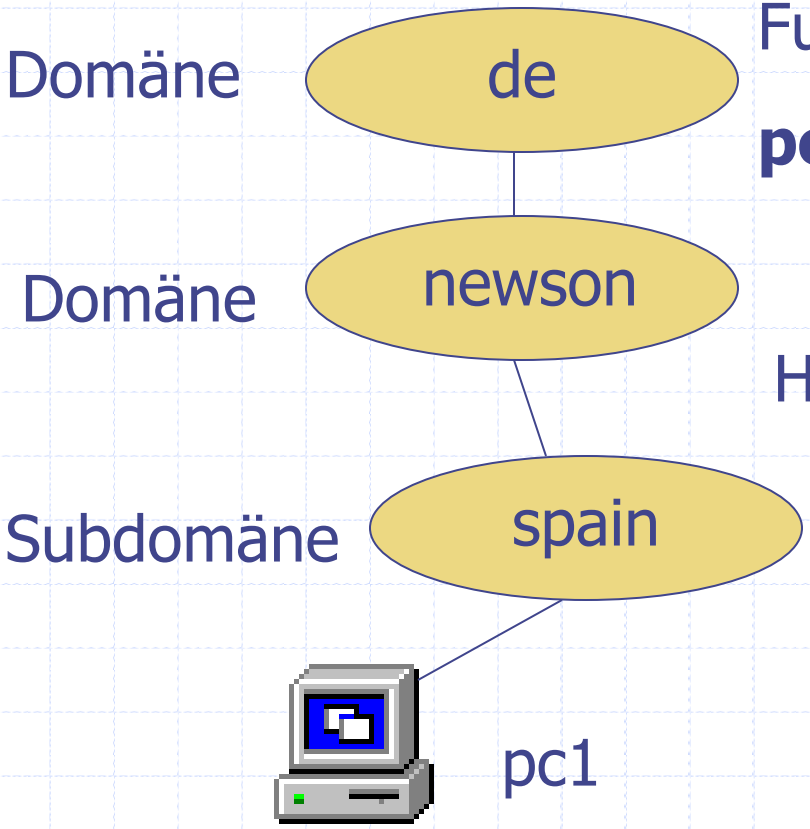
- Grundlagen
- DNS-Adressen
- Richtlinien
- Namensauflösung
- Client-/Servermodell

zurück

Was ist DNS?

- Domain Name System
- Wird im Internet zur Namensauswertung benutzt.
- ist eine verteilte hierarchische Datenbank
- ordnet Computernamen IP-Adressen zu
- DNS-Domäne ist ein hierarchischer Namensraum für Computer, Dienste und DNS-Subdomänen eines Netzwerkes.
- Eine DNS-Domäne besitzt einen eigenen Namen

Aufbau einer DNS-Adresse



Full qualified Domain Name FQDN:

pc1.spain.newson.de

Hostname DNS-Domänenname

Bedeutung:

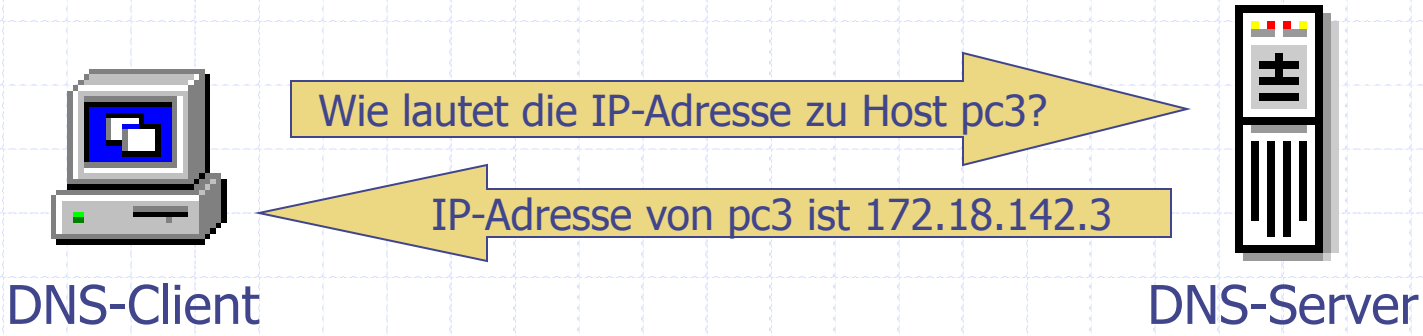
Der Computer *pc1* ist Host in der DNS-Domäne *spain.newson.de*

Richtlinien für DNS

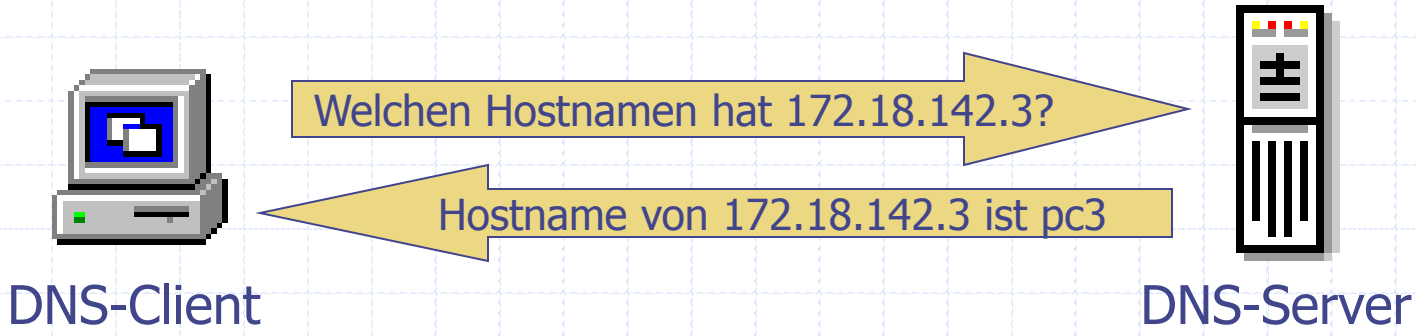
- Maximal 5 Ebenen
- Eindeutige Namen für Subdomänen
- Kurze, aussagekräftige Namen verwenden
- Maximal 63 Zeichen für Domänennamen einschließlich der Punkte
- Gesamtlänge des FQDN maximal 255 Zeichen
- DNS Standardzeichen sind: a-z, 0-9 und Bindestrich
- Großbuchstaben werden automatisch durch Kleinbuchstaben ersetzt

Namensauflösung

- Forward-Lookup



- Reverse-Lookup

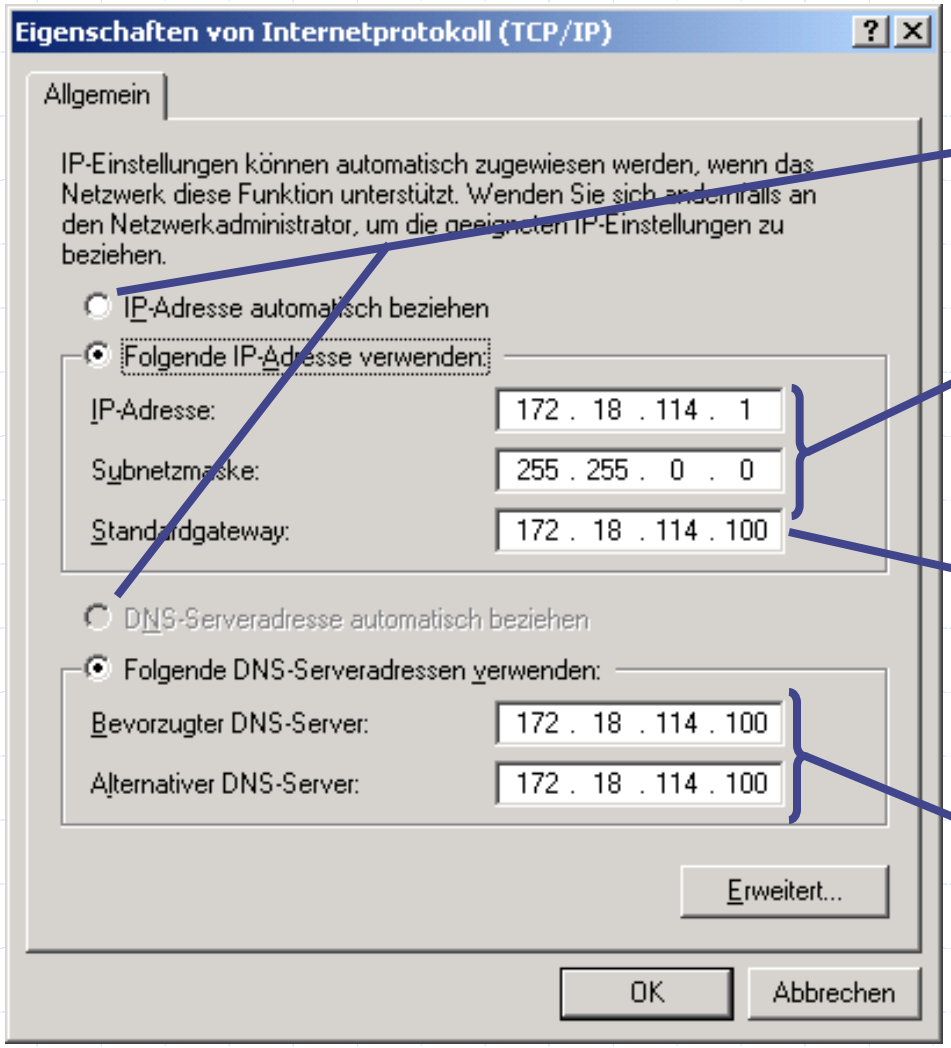


Client-/Servermodell

- DNS-Namensserver übernehmen den Serverpart.
- Zum Client wird ein Computer durch Eintragen der IP-Adresse des zuständigen Namensservers in die TCP/IP-Protokollkonfiguration auf dem betreffenden Computer.
- Ein DNS-Server kann nur Namen auflösen, für die er autorisiert ist.
- Client-Anfragen, die nicht aufgelöst werden können, werden an einen anderen Namensserver übergeben (Internet-Prinzip)

zurück

IP- und DNS-Konfiguration



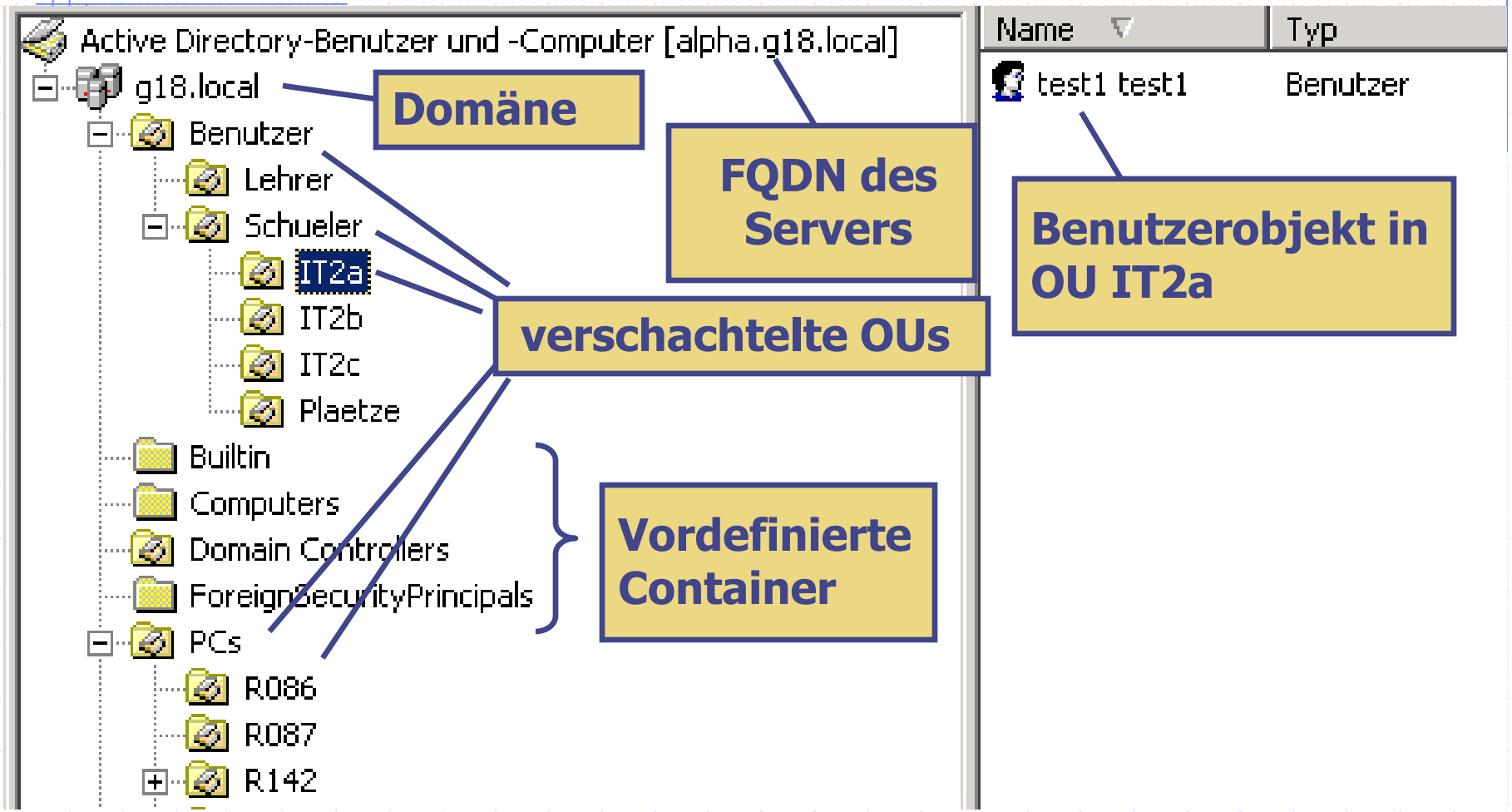
IP-/DNS-Adresse über DHCP-Server beziehen

Feste IP-Adresse und Subnetzmaske

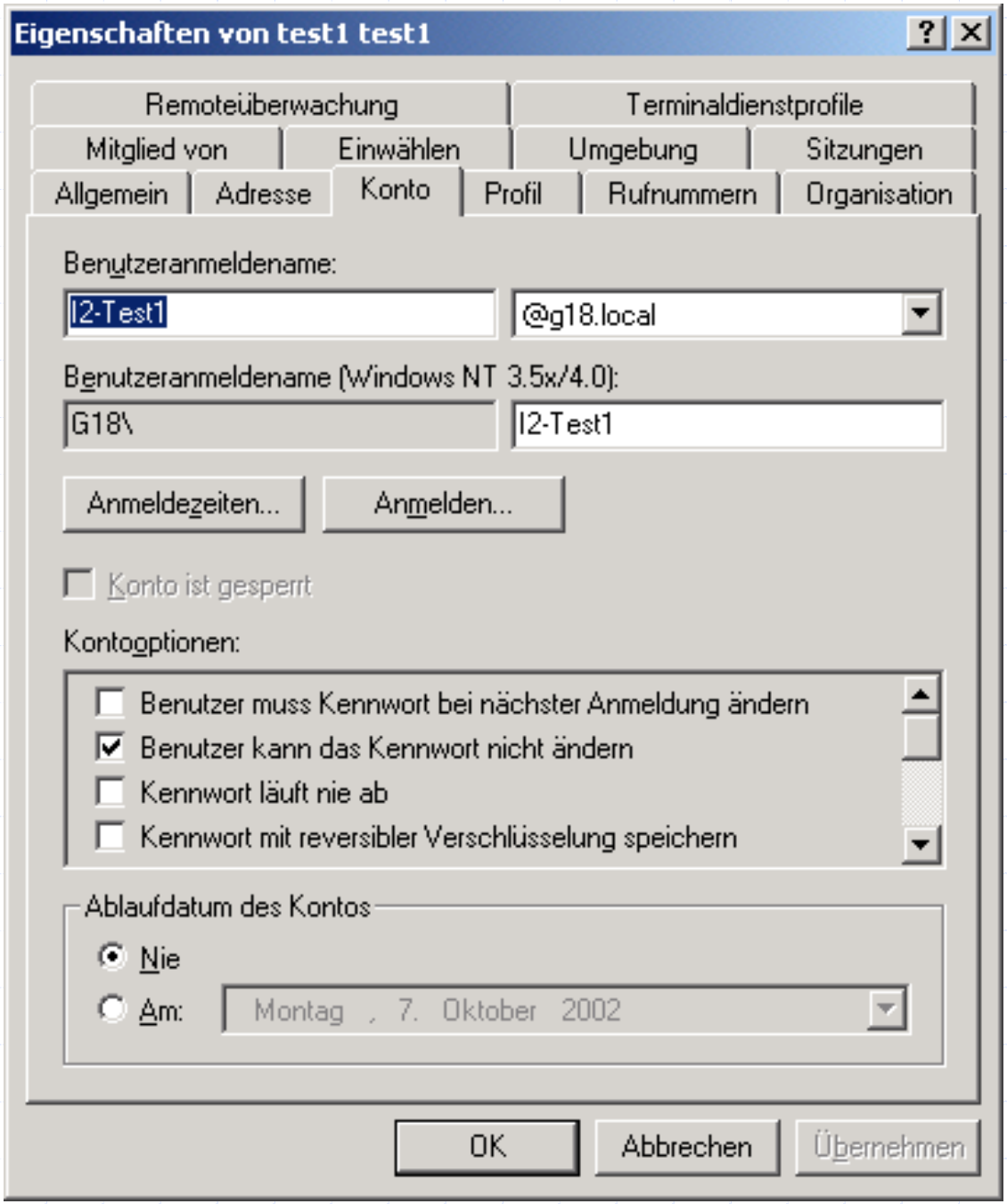
Gateway für Internetzugang (Proxyserver)

IP-Adressen der DNS-Server

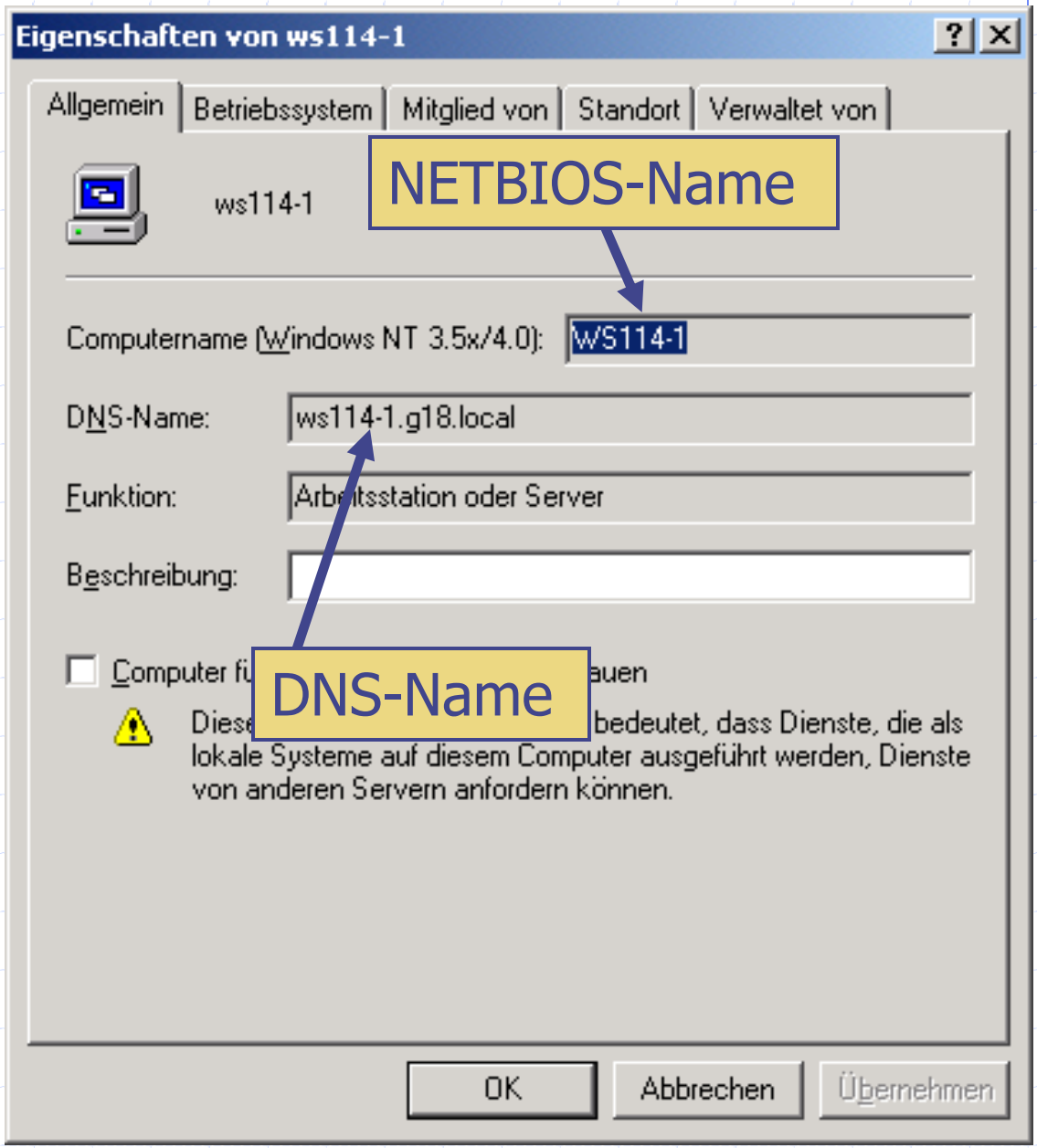
AD-Managementkonsole



Benutzer-verwaltung im Active Directory



Computer-verwaltung



zurück