

## Server Installation

### Netzwerkeinrichtung

Nach der Installation müssen die Netzwerkeinstellungen vorgenommen werden. Hierzu wird eine feste IP-Adresse sowie der Servername eingetragen.

**Beispiel:**

IP-Adresse: 192.168.1.1

Server-Name: server1

### DNS und DHCP Server

Sobald das Betriebssystem installiert und das Netzwerk eingerichtet ist können die Server-Komponenten installiert werden. Da wir einen DNS und DHCP Server benötigen werden diese nun installiert.

### Servicepack

Bevor weitere Software installiert wird die nicht zum Betriebssystem gehört und wir beginnen den Server zu konfigurieren wird ein Servicepack installiert.

Wichtig ist, dass die Service-Packs bereits im laufenden Betrieb auf Stabilität und Kompatibilität geprüft worden sind.

### DHCP (Dynamic Host Configuration Protocol)

Der DHCP Server ermöglicht die automatische Zuweisung von Netzwerkadressen und weitere Netzwerkooptionen an Computer. Der Vorteil liegt darin, bei Änderungen der Netzwerkkonfiguration nicht jeden Rechner umstellen zu müssen, sondern dies auf dem Server zu verwalten was per DHCP dann zugewiesen wird.

### Zonen

Die Zone (Netzwerkbezeichnung) die der DHCP-Server verwalten soll nennen wir einfach wie die Domäne.

**Beispiel:** firmenname.local (intern)  
firmenname.de (extern)

## **Bereichsoptionen**

Hier werden zusätzliche Parameter an die Clients übergeben, in unserem Fall sind das das Standard-Gateway, DNS-Server und Domänen-Suffix.

Standard-Gateway ist der nächste Router in fremde Netzwerke (meist zum Internet).

Das Standard-Gateway ermöglicht den Übergang in fremde Netze, hier in das Internet. Alle Anfragen die außerhalb des Netzes liegen in dem sich der Rechner selbst befindet werden an das Standard-Gateway, einen Router, geleitet.

DNS-Server ist der Server selbst, das Domänen-Suffix der Domänen-Name.

## **Ausschlüsse**

Da wir im Bereich der Workstations keine festen IP-Adressen vergeben möchten, gibt es in diesem Bereich keine Ausschlüsse.

In manchen Netzen, vor allem in bereits bestehenden Netzen, kann es manchmal nötig sein, bestimmte Adressbereiche von der automatischen Konfiguration auszuschließen. Beispiele sind Netzwerkdrucker oder Server die immer unter der selben Adresse erreichbar sein müssen.

## **DNS (Domain Name Service)**

In einem DNS Server werden Computernamen und ihre zugehörigen Netzwerkadressen hinterlegt. Somit ist es möglich einen Rechner über seinen Namen zu kontaktieren, der dabei beteiligte DNS Server löst dabei den Namen in die zugehörige IP-Adresse auf.

## **Dynamische Aktualisierung**

Damit die Namen der Rechner die ihre IP-Adresse automatisch via DHCP zugewiesen bekommen haben ebenfalls aufgelöst werden können, muss man im DNS-Server die dynamische Aktualisierung aktivieren.

Dabei wird für jeden Rechner der eine IP-Adresse vom DHCP-Server zugewiesen bekommen hat einen Datensatz in der Forward-Lookup-Zone und Reverse-Lookup-Zone angelegt.

Es existieren zwei Tabellen mit Rechnernamen und Netzwerkadressen. In der Forward-Lookup Zone können Rechnernamen in ihre Netzwerkadresse aufgelöst werden was am häufigsten benötigt wird, seltener benötigt man die umgekehrte Funktion der Reverse-Lookup-Zone, in der mit einer IP-Adresse den Namen des zugehörigen Rechners abgefragt werden kann.

## **Weiterleitung**

Um Anfragen über PC Namen die nicht im eigenen Netz liegen und somit im eigenen DNS Server nicht eingetragen sind zu beantworten gibt es zwei Möglichkeiten:

- **Root-Zone:**  
Über die Root-Zone (.-Zone) kann der DNS-Server einen Root-Server abfragen und die Namensauflösung selbst erledigen.  
Ein Root-Server ist einer der 13 obersten DNS-Server die in der ganzen Welt verteilt sind. Sie beinhalten die DNS-Server für alle vorhandenen Topleveldomains. Bei einer Anfrage unseres DNS-Server wird erst der Root-Server angefragt, der daraus resultierende DNS Server für die gewünschte Topleveldomain wird dann nach dem Domännennamen angefragt. Als Ergebnis erhält er den DNS-Server für die gewünschte Domäne. Dieser kann dann den Rechnernamen auflösen.
- **Weiterleitung:**  
Einfacher zu konfigurieren und zu warten ist es einen DNS-Servers eines Internet-Providers zu verwenden der die Abfragen selbst durchführt und das Ergebnis zurückgibt.  
In unserem Fall tragen wir den DNS-Server von T-Online ein, 194.25.2.129.

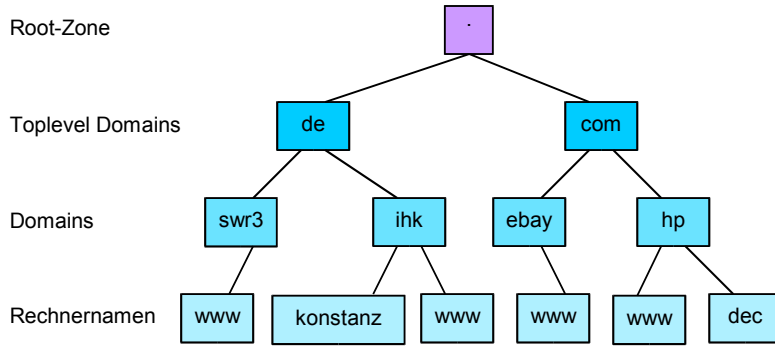


Abb. 1: Illustration: Struktur der DNS-Server im Internet

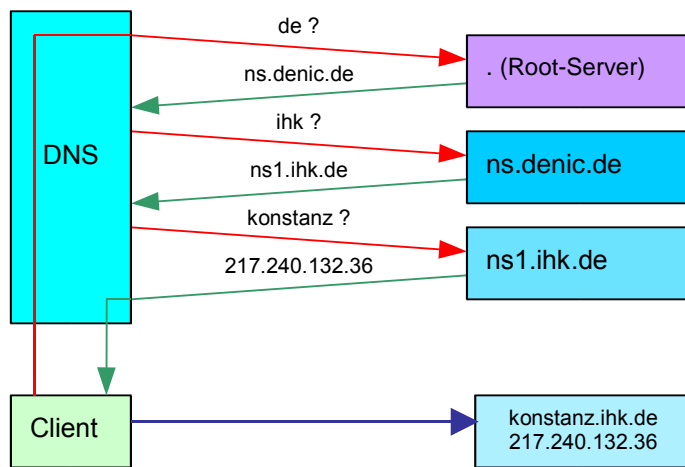


Abb. 2: Beispiel: Auflösung des Rechnernamens konstanz.ihk.de

## Active Directory

Um eine Windows 2000 Domäne auf einem Server zu installieren wird ein Active Directory als Verzeichnisdienst installiert. Das Active Directory basiert auf einer LDAP Datenbank und speichert Benutzer, Gruppen, Rechner und sämtliche anderen Objekte einer Domäne inklusive deren Eigenschaften.

Bei Windows NT gab es die sogenannten „SAM-Datenbank“. In dieser wurden Benutzer, Gruppen und deren Eigenschaften gespeichert. Seit Windows 2000 hat man sich für ein Datenbanksystem entschieden, dass es erlaubt den Daten-Baum einer Domäne in einen „Forest“ mit vielen Domänen zu integrieren und jederzeit auf jedes beliebige Objekt und jede Eigenschaft Zugriff zu haben.

Im Active Directory können außerdem beliebige Objekte und Eigenschaften gespeichert werden wie zum Beispiel der Standort eines Druckers, dessen Benutzer und sonstige Daten. Externe Software hat zusätzlich die Möglichkeit eigene Objekte oder Eigenschaften für existierende Objekte hinzuzufügen, während früher jede Software ihre eigene Datenbank mitbringen musste.

Die Installation von Active Directory wird auf einem Windows 2000 Server vorgenommen mit dem Aufruf von „dcpromo“. Während der Installation des Active Directorys muss zwingend eine Netzwerkverbindung bestehen, eine Verbindung zu einem Hub oder Switch ist hierfür ausreichend.

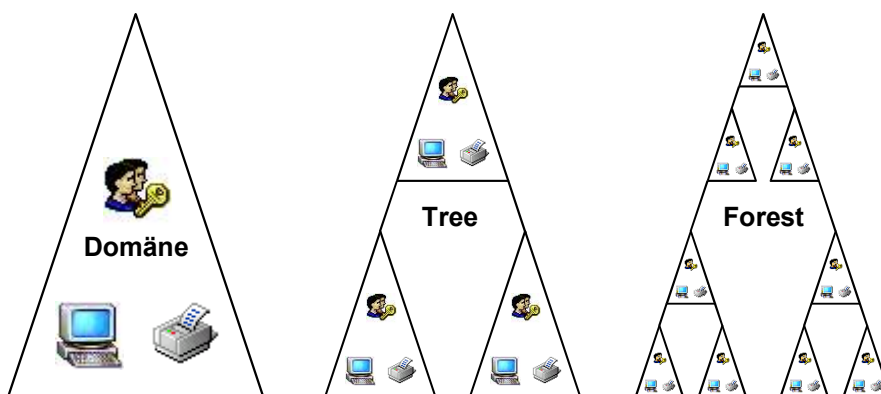


Abb. 3: Illustration: Active Directory - Domäne, Tree, Forest

## DHCP Autorisierung

Nach der Installation von Active Directory muss der zur Domäne gehörige DHCP Server autorisiert werden damit er in der Lage ist den Domänencomputern IP-Adressen zu zuweisen und diese im DNS einzutragen.

**LDAP-Verzeichnis**

Wie bereits erwähnt basiert das Active Directory auf einem modifizierten LDAP-Verzeichnis. Ein LDAP-Verzeichnis ist eine Datenbank die anstelle von Tabellen, Feldern und Datensätzen Objekte beinhaltet.

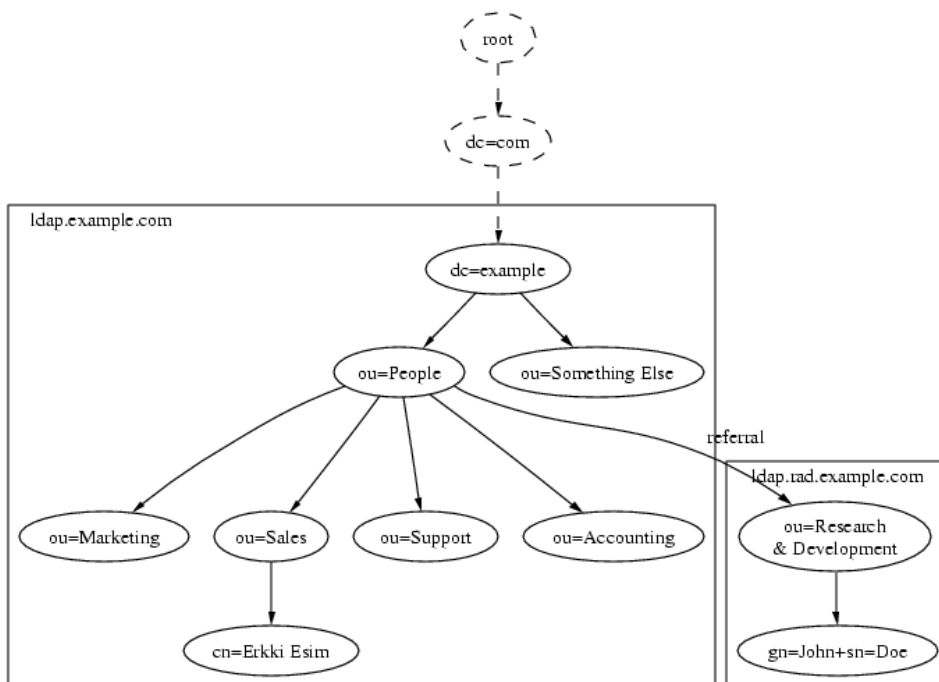
Ein Objekt im Verzeichnis hat einen Namen, mit dem es referenziert werden kann (cn=common name). Die oberste Ebene eines Verzeichnisses ist der Ländercode (c oder dc), darunter die entsprechende Domain (dc). Somit ist das LDAP-Verzeichnis nach dem gleichen System wie das DNS hierarchisch aufgebaut. Der oberste Punkt eines Verzeichnisses nennt sich root-dn.

Die im Verzeichnis enthaltenen Objekte werden in Organisationseinheiten (ou=organizational unit) strukturiert. Eine ou kann wiederum weitere ous enthalten.

Die genaue Bezeichnung eines Objekts in Verzeichnis nennt man dn=distinguished name. Ein dn enthält den gesamten Pfad vom Objekt bis zur root-dn des Verzeichnisses.

**Beispiel:**

cn=Benutzername,ou=Abteilung,ou=Mitarbeiter,dc=firmenname,dc=de



**Abb. 4: Illustration: Struktur eines LDAP-Verzeichnisses**

**Schemen**

Jedes Objekt in einem solchen Verzeichnis beinhaltet verschiedene Eigenschaften:

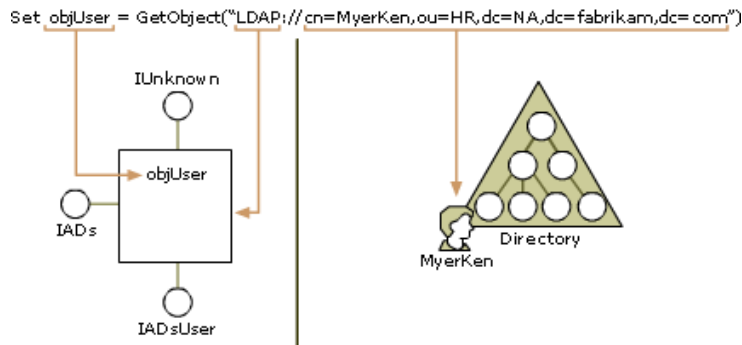
- cn: Nachname
- sn: Vorname
- mail: no-spam@spam.de
- departmentNumber: pr14
- preferredLanguage: german
- homePhone: 01231234567
- homePostalAddress: hauptstrasse 1
- roomNumber: 301
- mobile: 0170 1234567

Die Eigenschaften eines solchen Objekts werden in Schemen festgelegt. Ein Objekt wird dann einer Klasse zugeordnet, Beispiel inetorgPerson und muss somit die Eigenschaften der Klasse inetorgPerson besitzen. Ein Objekt kann gleichzeitig mehreren Klassen zugehörig sein, ausserdem können Klassen ihre Eigenschaften an Unterklassen vererben -> s. objektorientierte Programmierung.

Diese Schemen sind zu einem Teil standardisiert worden und somit im Lieferumfang eines LDAP-Servers enthalten.

**Schemenerweiterungen**

Das Active Directory nutzt eigene Schemen zum speichern seiner Objekte wie Benutzer, Computer, Gruppen etc.



**Abb. 5: Beispiel: Abfrage von Benutzerneigenschaften aus dem Active Directory**

Wollen nun Applikationen wie Microsoft Exchange den Objekten eigene Eigenschaften hinzufügen (Beispiel: E-Mail-Adresse), dann werden Schemenerweiterungen installiert (Fachjargon Microsoft). Das bedeutet nichts anderes, als dass die vorhandenen Schemen entweder ersetzt werden oder neue hinzugefügt werden die dann für die Objekte verwendet werden können.