Teil D Verzeichnisdienst (Active Directory) aufbauen

13 Was ist ein Verzeichnisdienst?

Lernziele

Nach der Bearbeitung dieses Kapitels können Sie …

- die wichtigsten Kategorien von Informationen nennen, die in einem Directory Service enthalten sind.
- anhand von Beispielen erläutern, wie diese Informationskategorien zu einem effizienten und sicheren Betrieb eines Systems führen.
- die Vorteile eines Directory Service erklären.
- die wichtigsten Begriffe rund um das Active Directory aufzählen und erläutern.

Schlüsselbegriffe

Betriebsmasterrolle, Canonical Name, digitale Signatur, Directory Information Base, Directory Information Tree, Directory System Agent, Directory User Agent, Distinguished Name, Domäne, Domänenkontroller, Gesamtstruktur (Forest), Globaler Katalog (GC), Kerberos, LDAP, Namenskonvention, Netzwerkressourcen, Objekt, Objektklasse, Organisationseinheit, OU, Private Key, Public Key, Relative Distinguished Name, Replikationsmodell, Schema, Struktur (Tree), Subnetz, User Principal Name, Vertrauensstellung, X.500, Verzeichnisdienst

Um alle Netzwerkressourcen und -dienste optimal verwalten zu können, sind Sie auf ein gut organisiertes **Ablagesystem** angewiesen. Sie können das Ablagesystem mit einem Kleiderschrank vergleichen. Wenn Sie alles einfach nur hineinschmeissen, verlieren Sie früher oder später den Überblick und können Ihre Kleidungsstücke nicht mehr finden. Gleich verhält es sich in einer Netzwerkumgebung. Sie müssen Ablagen schaffen, die flexibel und skalierbar sind, damit die Ressourcen und Dienste effizient genutzt und übersichtlich verwaltet werden können. In diesem Kapitel werden die notwendigen Grundlagen dafür vermittelt.

13.1 Bedeutung des Active Directory

Ein **Verzeichnisdienst (Directory Service)** ist für die Systemadministration von zentraler Bedeutung. Über den Verzeichnisdienst können Sie die **gesamte IT-Infrastruktur** mit allen Rechnerkonten und Sicherheitseinstellungen verwalten. Aber auch andere Dienste und Anwendungen wie beispielsweise Mailserver oder Datenbanken nutzen die Informationen des Verzeichnisdienstes. In diesem Zusammenhang kann z. B. das Anmeldeverfahren nach dem **Single-Sign-on-Prinzip**[1] genannt werden.

Aus technischer Sicht ist der Verzeichnisdienst nichts anderes als eine grosse Datenbank zur **Speicherung und Verwaltung von Netzwerkressourcen**. Solche Ressourcen können sein:

- Benutzer
- Computer
- E-Mail-Adressen (Kontakte)
- Freigaben (Shares)
- Gruppen

Hinweis

Vorreiter im Bereich des Verzeichnisdiensts war Novell mit dem Novell Directory Service (NDS), der auch unter dem Namen eDirectory bekannt ist.

Im Jahr 1999 brachte Microsoft zusammen mit dem neuen Serverbetriebssystem Windows 2000 das **Active Directory** auf den Markt. Dieser Verzeichnisdienst beruht auf diversen

[1] Hier im Sinne von: einmal anmelden und danach alle Anwendungen verwenden.

öffentlichen Standards (vgl. nächstes Unterkapitel) und vereinfacht die Verwaltung von Objekten sowohl für Grossfirmen als auch für KMU-Betriebe. Dies wird durch einen streng hierarchischen und somit skalierbaren Aufbau des Verzeichnisdienstes möglich. Das Active Directory lässt sich anhand folgender **Merkmale** beschreiben:

- **Skalierbarkeit:** Dies erlaubt Ihnen eine gezielte Anpassung an Ihr Unternehmen. Neue Mitarbeitende, Standorte, Drucker etc. können ohne grosse Änderung der bestehenden Struktur hinzugefügt werden.
- **Erweiterbarkeit:** Es können problemlos neue Objekttypen wie Firmenfahrzeuge hinzugefügt und bequem verwaltet werden. Ein gutes Beispiel für die Erweiterbarkeit ist die Installation einer Exchange-Messaging-Umgebung. Hier wird der Verzeichnisdienst vor der Installation um etliche neue Objekte erweitert, um die für den E-Mail-Betrieb notwendigen Werte mitzugeben.
- **Sicherheit:** Durch die Verwendung von sogenannten Zugriffssteuerungslisten (ACL) wird genau festgelegt, welche Benutzer in welcher Form (lesen, schreiben, ausführen) auf Objekte innerhalb des Verzeichnisdienstes zugreifen dürfen.
- **Verfügbarkeit:** Durch die Verwendung von zwei oder mehr Domänencontrollern ist auch bei einem Ausfall eines solchen der Betrieb weiterhin gewährleistet.
- **Performance:** Das ganze Verzeichnis ist darauf ausgelegt, die verlangten Informationen schnell an jedem Platz einer weltweit tätigen Unternehmung zur Verfügung zu stellen.

13.2 Der X.500-Standard

Um die Kompatibilität zwischen unterschiedlichen Directory Services und auch gegenüber anderen Betriebssystemen wie Unix zu gewährleisten, wurden diverse offene Standards verwendet. Dies erleichtert auch den Betrieb von Active Directory in einer heterogenen (gemischten) Umgebung. Die **X.500-Spezifikation** fasst internationale Standards für einen plattformunabhängigen, verteilten Verzeichnisdienst zusammen. Das Active Directory setzt nicht alle Eigenschaften dieser Spezifikation um, verwendet aber dasselbe Datenmodell, die gleichen Namenskonventionenen und einige Konzepte daraus.

Weshalb wurde der X.500-Standard etwickelt? Den Ausschlag für die Entwicklung gab die Problematik, welche der WHOIS[1]-Dienst mit seiner **zentralen Datenbank** verursachte. In dieser Datenbank wurden in den 1980er-Jahren alle Domänennamen und IP-Bereiche verwaltet. Zusätzlich wurden darin alle weiteren Daten aufgenommen, die vom Defense Data Network Network Information Center (DDNNIC) sowieso bearbeitet werden mussten. Dies führte zu immer längeren Antwortzeiten und riesigen Datenmengen. Als zudem der Internetboom einsetzte, war es nicht mehr möglich, mit einer einzigen Datenbank zu arbeiten. Die Arbeit mit mehreren Datenbanken wurde unumgänglich. Die Suche nach einer Lösung war aber nicht einfach, weil die beteiligten Gremien der International Standards Organisation (ISO) und der International Telecommunication Union (IT) jeweils eigene Interessen vertraten. 1988 schafften sie es dennoch, mit **X.500 Bluebook** (entspricht der **ISO-Norm 9594**) einen allgemeingültigen Standard zu verabschieden.

Die wichtigsten **Merkmale des X.500-Standards** lauten wie folgt:

- Dezentralisierte Verwaltung
- Erweiterte Suche
- Globaler Namenskontext
- Strukturierte Informationsbasis (Schema)

[1] Engl. für: Wer ist? Protokoll, mit dem von einem verteilten Datenbanksystem aus Informationen über Internetdomänen und IP-Adressen sowie deren Eigentümer abgefragt werden können.

13.2.1 Directory System Agent und Directory User Agent

In einem Verzeichnis werden bestimmte **Objekte** und deren **Attribute** gespeichert. Wenn Sie als Systemadministrator z. B. einen neuen Mitarbeiter erfassen, wird dieser automatisch unter dem angegebenen Namen am richtigen Ort im Verzeichnis abgelegt. Auch bei der Suche nach einem bestimmten Objekt liest automatisch der richtige Server die richtige Information. Wer sorgt dafür, dass dies richtig abläuft?

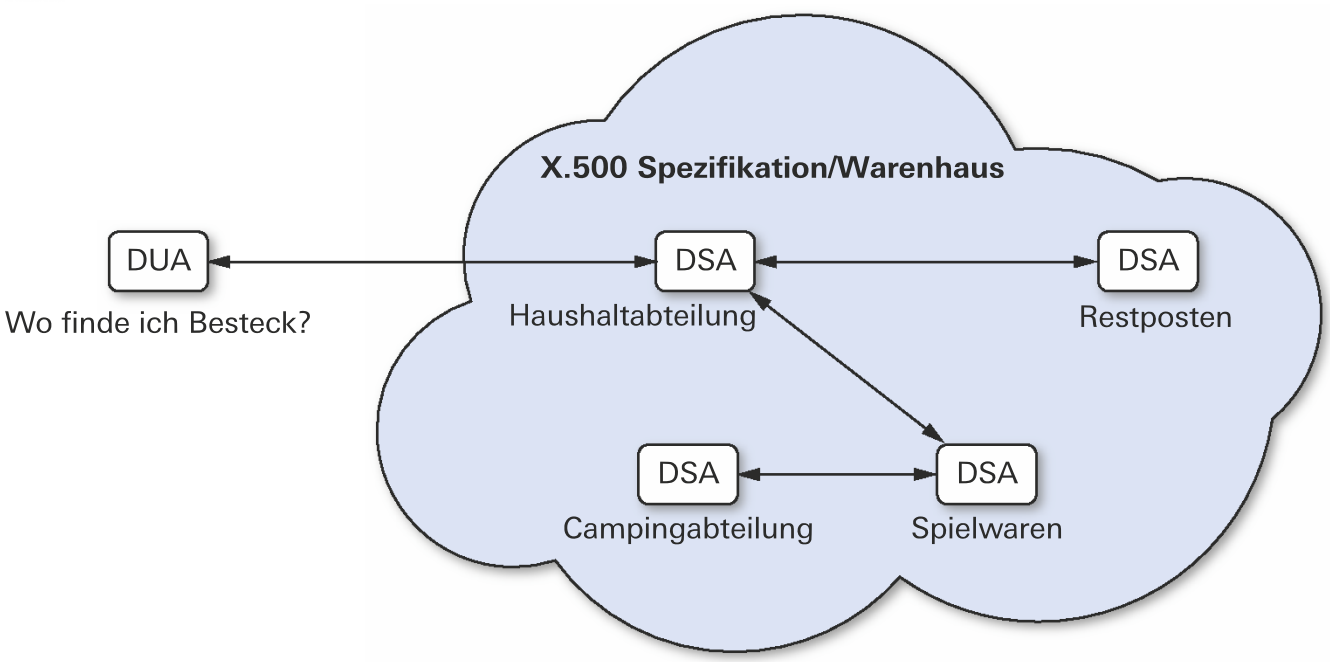
Bei der Abfrage eines Verzeichnisses nach bestimmten Informationen dient der **Directory User Agent (DUA)** als Schnittstelle zwischen dem Benutzer und dem Verzeichnis. Er übersetzt die Anfrage quasi in die richtige Systemsprache. Der Directory User Agent selber hat keinen direkten Zugriff auf die Objekte, sondern muss den sogenannten **Directory System Agent (DSA)** anfragen. Dieser ist mit dem Mitarbeiter eines Warenhauses vergleichbar, der für einen bestimmten Bereich des Gesamtsortiments zuständig ist und über dieses Teilsortiment rasch und korrekt Auskunft geben kann. Auch der DSA kennt nur einen Teil des Gesamtverzeichnisses. Der Mitarbeiter im Warenhaus kann zudem mit anderen Mitarbeitern aus anderen Bereichen Kontakt aufnehmen, um Informationen zu erhalten. Dies gilt auch für den DSA.

Beispiel

Sie fragen die Mitarbeiterin eines Warenhauses, wo sich das Essbesteck aus Aluminium befindet. Die Mitarbeiterin ist für die Haushaltsabteilung zuständig und weiss, dass es sowohl in ihrer Abteilung als auch in der Campingabteilung entsprechende Artikel gibt. Sicherheitshalber fragt sie auch noch in der Restpostenabteilung nach, ob es dort evtl. vergünstigte Essbestecke gibt.

Folgende Grafik soll dieses Zusammenspiel verdeutlichen:

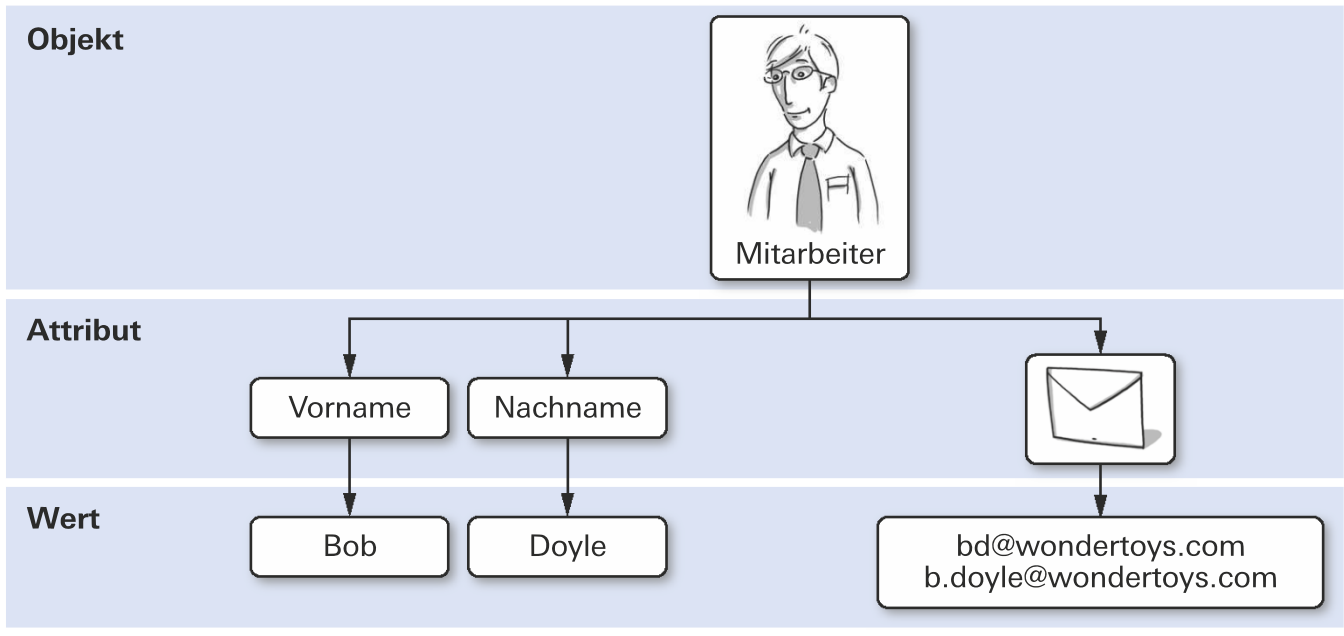
Abb. [13-1] **Zusammenspiel zwischen DUA und DSA**



13.2.2 Directory Information Base

Alle Informationen in einem Verzeichnis werden generell als **Directory Information Base (DIB)** bezeichnet. Aus Benutzersicht bestehen die Daten eines Verzeichnisses aus Objekten. Ein Objekt besteht wiederum aus mehreren Attributen, die einen bestimmten Wert besitzen. Folgende Grafik soll den **Zusammenhang zwischen Objekt, Attribut und Wert** verdeutlichen:

Abb. [13-2] Zusammenhang zwischen Objekt, Attribut und Wert

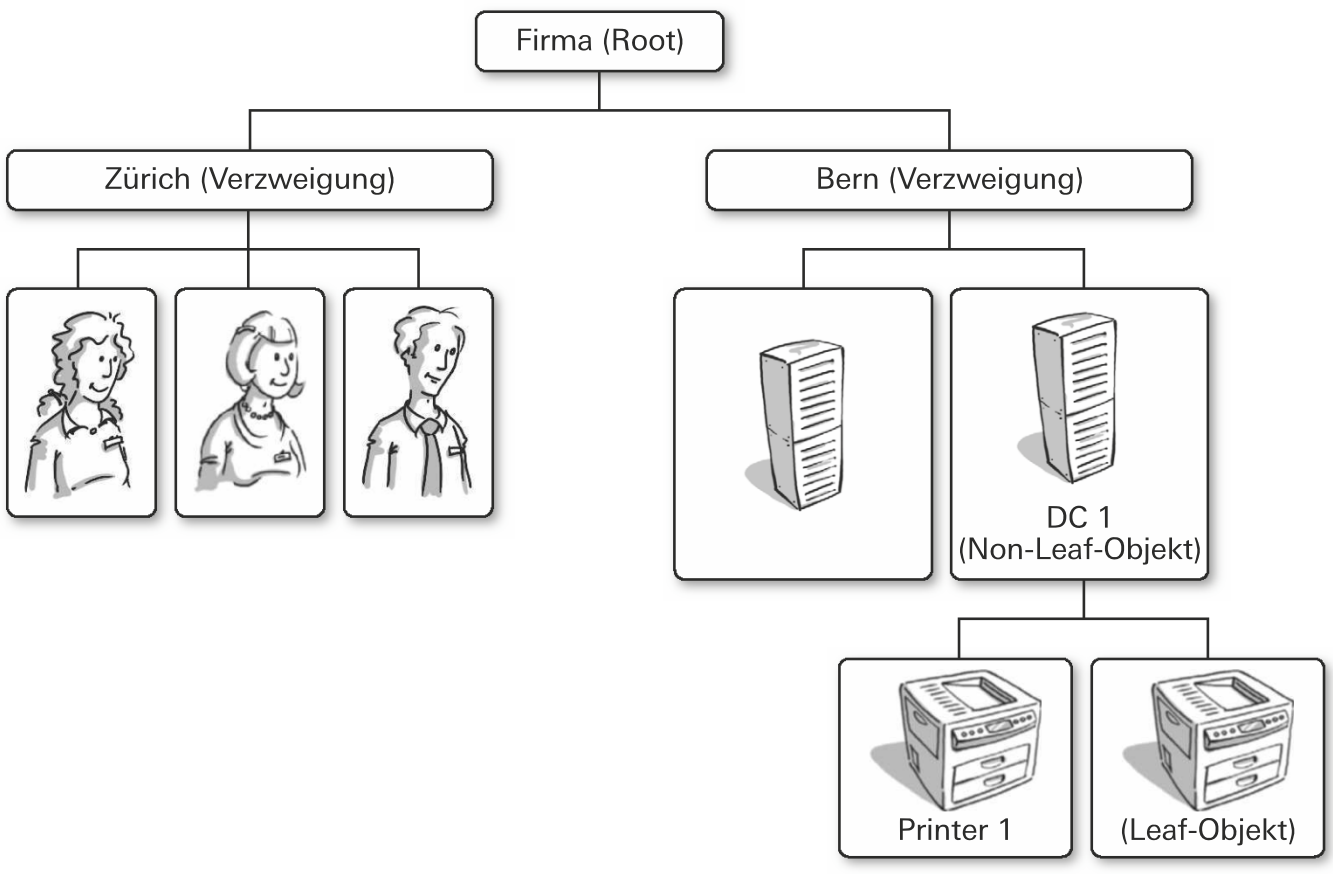


Jedes Objekt ist mit einem Namen gekennzeichnet. Dieser Name ist innerhalb eines Verzeichnisses einzigartig. Man spricht deshalb auch vom **Distinguished Name**[1] **(DN).**

13.2.3 Directory Information Tree

Die Einträge in der DIB sind in Form eines umgekehrten Baums hierarchisch strukturiert und bilden den sogenannten **Directory Information Tree**. Zuoberst befindet sich die **Root**[2], an der alles aufgehängt ist. Sie ist innerhalb des Verzeichnisses einmalig. Neben Objekten wie User und Computer gibt es auch Organisationseinheiten, Standorte, Domänen etc. Zudem haben Objekte meist untergeordnete Objekte. In diesem Fall wird innerhalb des Verzeichnisses eine logische Verbindung eingerichtet. Die folgende Abbildung soll den **Aufbau eines Directory Information Tree** verdeutlichen:

Abb. [13-3] Root, Verzweigungen und Verbindungen



[1] Engl. für: definierter Name.
[2] Engl. für: Wurzel.

Der **Directory Information Tree (DIT)** beschreibt die Datenbankstruktur, also die Hierarchie der Datenbank. Bei den Verzweigungspunkten wird zwischen Leaf-Objekten und Non-Leaf-Objekten unterschieden. **Leaf-Objekte** besitzen keine Unterobjekte. In der obigen Grafik wäre ein Leaf-Objekt beispielsweise der Printer 1. Objekte mit weiteren Unterobjekten werden als **Non-Leaf-Objekte** bezeichnet. In der obigen Grafik wäre ein Non-Leaf-Objekt beispielsweise der DC 1.

Hinweis

Vom Begriff «Directory Information Tree» stammt auch die Endung der Datenbankdatei **NTDS.DIT** (New Technologies Directory Services Directory Information Tree) beim Active Directory.

13.2.4 Namenskonventionen bei X.500

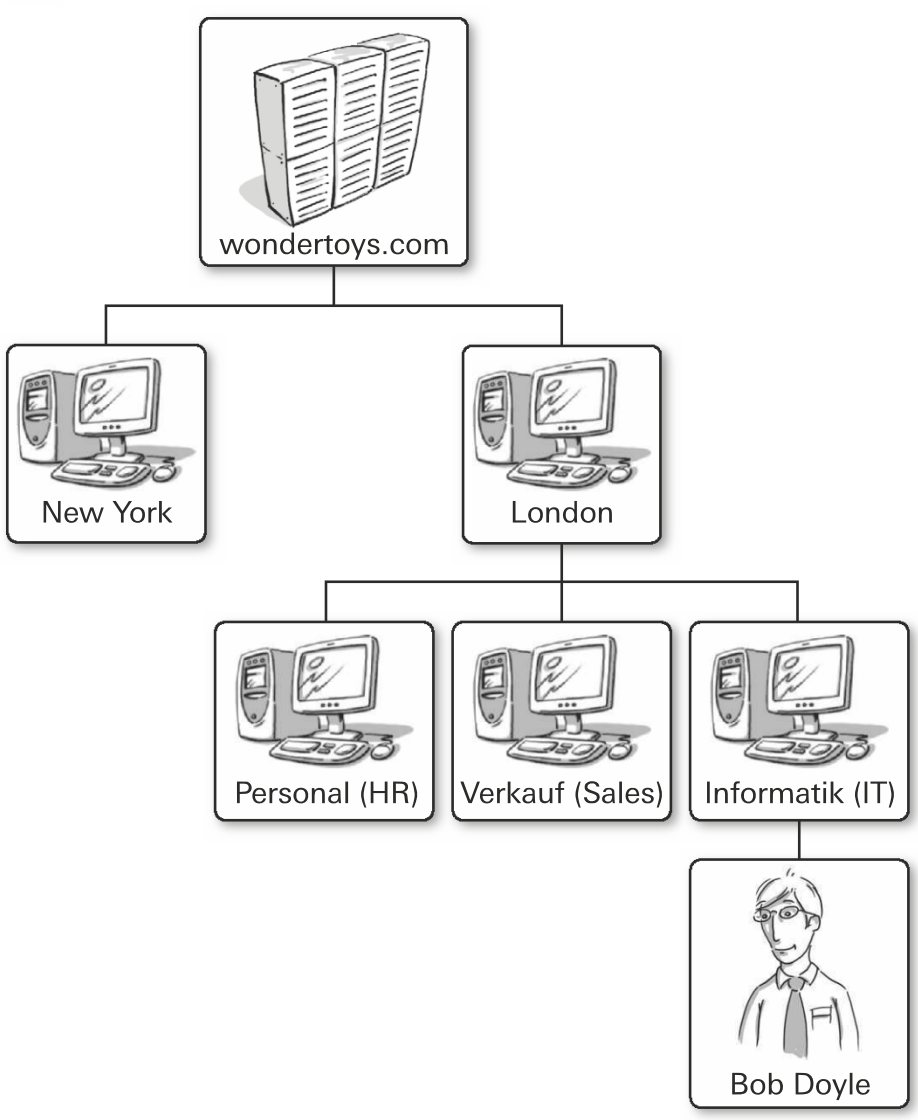
Wie bereits erwähnt hat jedes Objekt innerhalb des DIT einen eindeutigen Namen. Er muss eindeutig sein, um das Objekt zweifelsfrei identifizieren zu können. Ein Objekt besitzt meist mehrere eindeutige Namen. Dies kommt daher, dass unterschiedliche Anwendungen und Dienste unter verschiedenen Namenskonventionen auf diese Informationen zurückgreifen. Es wird unterschieden zwischen **Distinguished Name (DN), Relativ Distinguished Name (RDN), User Principal Name (UPN)** und **Canonical Name (CNAME)**.

Beispiel

Stellen Sie sich folgende Situation vor: Bob Doyle ist neuer Administrator der Firma wondertoys.com am Standort in London. Der Hauptstandort befindet sich in New York. Als Systemadministrator ist er für die Pflege und Betreuung der Server vor Ort zuständig. Bauen Sie dieses Szenario mithilfe von Objekten innerhalb des DIT auf.

In der folgenden Grafik sehen Sie den Aufbau und den Standort von Bob Doyle innerhalb des Unternehmens, das logisch im DIT nachgebildet wurde:

Abb. [13-4] **Bob Doyle innerhalb des DIT**



Aus dem obigen Beispiel ergeben sich gemäss X.500-Namenskonvention folgende Werte:

- **DN:** cn[1]=Bob Doyle, ou[2]=IT, ou= London, dc[3]=wondertoys, dc=com
- **RDN:** cn=Bob Doyle
- **UPN:** b.doyle@wondertoys.com
- **CNAME:** wondertoys.com/London/IT/Bob Doyle

Hinweis

Für die Zusammenstellung des DN empfiehlt es sich, jeweils beim zu benennenden Objekt zu beginnen und sich dann nach oben zu arbeiten. Dabei darf kein Objekt ausgelassen werden. Genaue Kenntnisse über den Kontext und Aufbau erleichtern Ihnen den Umgang mit diversen Tools und Befehlszeilenprogrammen bei der Bearbeitung des Objekts.

13.2.5 Active Directory Schema

Sie haben gesehen, dass Sie innerhalb des DIT unterschiedliche Objekte erstellen und diesen bestimmte Eigenschaften und Werte zuweisen können. Wer aber sagt Ihnen, welche Objekte Sie wo erstellen können und welche Attribute Sie zuweisen dürfen? Sie brauchen also eine Vorlage, welche genau das regelt. In Active Directory erfüllt das **Schema** diese Aufgabe. Dieses Schema ist eine Art Regelbuch mit folgenden Inhalten:

1. **Namensregeln:** Wie muss der DN oder der RDN aufgebaut werden?
2. **Strukturregeln:** Wie ist die Hierarchie, des DIT aufgebaut?
3. **Objektregeln:** Welche Objektklassen dürfen mit welchen Attributen versehen werden?
4. **Attributregeln:** Darf ein Attribut mehrere Werte besitzen? Welche Syntax und Schreibweise muss der Wert haben? Ist zwingend ein Wert einzugeben oder darf das Attribut leer bleiben?

Hinweis

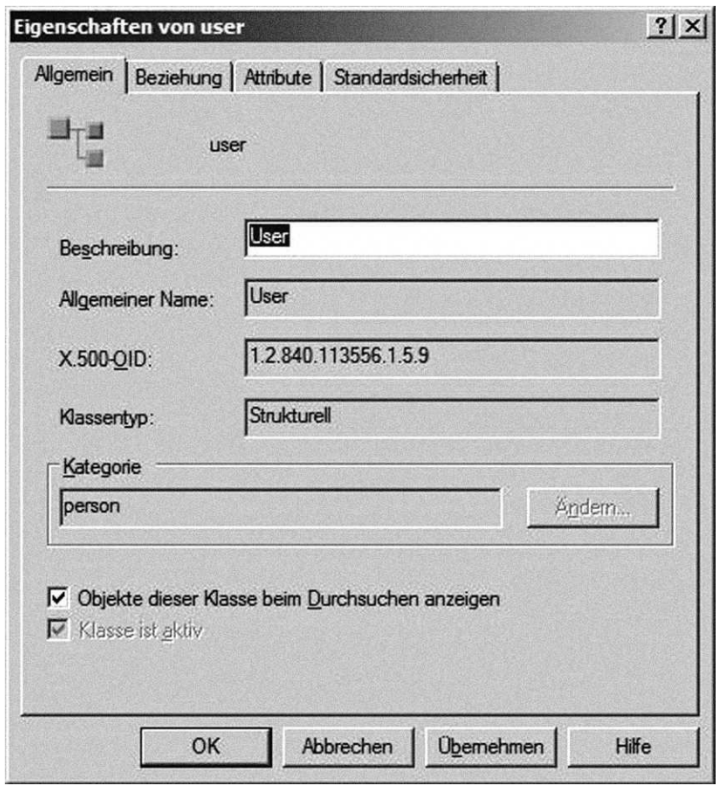
Das Schema ist ein zentrales Element innerhalb des Active Directory. Beschädigungen am Schema können nur unter speziellen Umständen behoben werden. In den meisten Fällen muss die Domäne neu aufgebaut werden. Im Umgang mit dem Schema ist deshalb grösste Vorsicht geboten.

13.2.6 Objektklassen

Eine **Objektklasse** definiert die Regeln für die Einträge in ein Objekt und beschreibt, welche Attribute einem Objekt zugewiesen werden können. Zur eindeutigen Identifizierung wird allen Objektklassen ein sogenannter **Object Identifier (OID)** zugewiesen. Das folgende Bild zeigt beispielhaft, wie ein solcher OID aussieht:

[1] Abk. für Common Name (allgemeiner Name).
[2] Abk. für Organizational Unit (Organisationseinheit).
[3] Abk. für Domain Component (Domänenkomponente).

Abb. [13-5] OID der Benutzerklasse USER (Beispiel)



Bei den Objektklassen werden folgende **Typen** unterschieden:

- **Abstract:** Diese Klasse dient als Vorlage für andere Objektklassen und wird nicht im DIT eingetragen (Beispiel: Klasse top).
- **Structural:** Diese Klasse dient als Vorlage für die Erzeugung der hauptsächlichen Objekte von Active Directory. Damit wird u. a. festgelegt, wo (innerhalb des DIT) Objekte dieser Klasse hinzugefügt werden dürfen und welche Attribute dazugehören.
- **Auxiliary:** Diese Klasse dient zur Erweiterung der Klassentypen Abstract und Structural und enthält Attribute, die diesen Klassen zugewiesen werden können.

13.2.7 Sicherheitsaspekte

Sie kennen nun den grundsätzlichen Aufbau und die Funktionsweise von Verzeichnisdiensten und wissen, welche Objektklassen es gibt und welche Objekte damit erzeugt werden können. Eine wichtige Frage ist aber, wie Sie diese Daten vor unberechtigtem Zugriff schützen können. Bevor Benutzer auf Objekte innerhalb des Verzeichnisdienstes zugreifen dürfen, werden sie authentifiziert. Dabei lassen sich folgende **Authentifizierungsarten** unterscheiden:

- **Einfache Authentifizierung:** Bei dieser Art der Authentifizierung wird der Benutzer einmal am Server angemeldet. Er übermittelt dabei Benutzername und Passwort, welche mit den Angaben in der Datenbank des Servers verglichen werden.
- **Strenge Authentifizierung:** Damit sich ein Benutzer nicht immer wieder aufs Neue bei einem DSA anmelden muss, werden digitale Signaturen verwendet. Dadurch wird zwischen dem Benutzer und dem DSA eine Vertrauensbasis geschaffen, die so lange dauert, bis sich der Benutzer wieder vom System abmeldet.

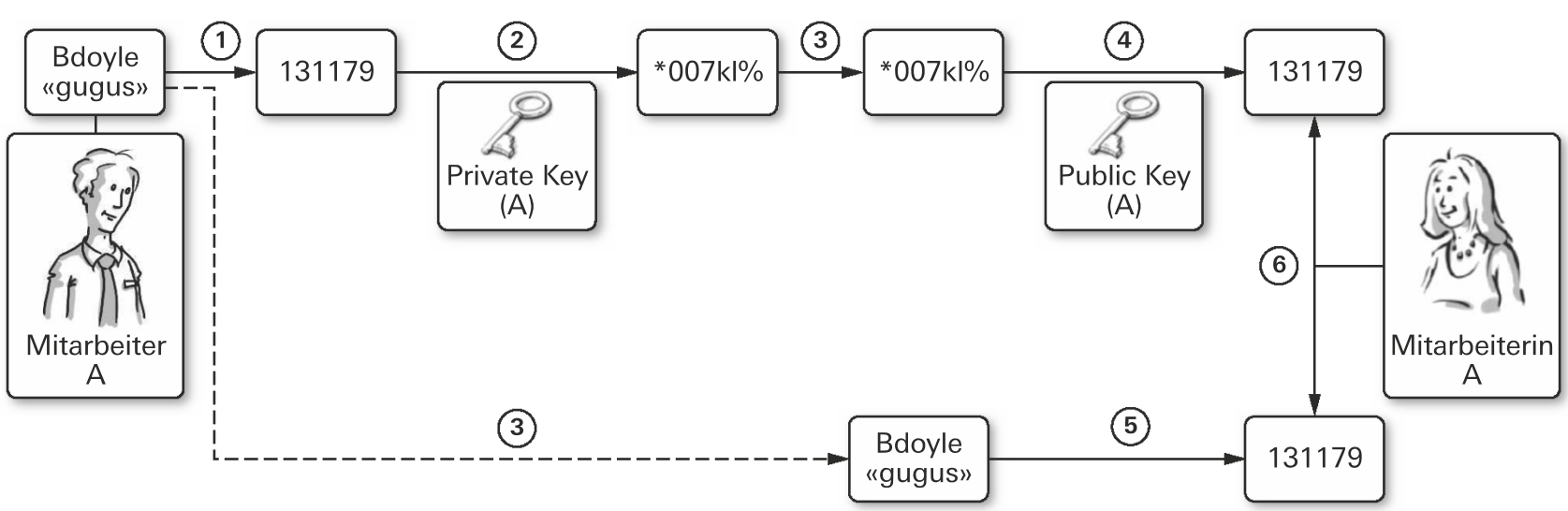
Wenn Sie mit verteilten Datenbanken arbeiten und sich die gesuchten Objekte nicht immer auf dem Server befinden, an dem Sie gerade angemeldet sind, müssen Sie mit einer einfachen Authentifizierung den Benutzernamen und das Passwort immer wieder aufs Neue übermitteln. Abhilfe schafft hier die strenge Authentifizierung.

Digitale Signaturen gewährleisten, dass ein Benutzer, der sich am System anmeldet, wirklich diejenige Person ist, die er vorgibt. Digitale Signaturen basieren auf einer **asymmetrischen Verschlüsselung.** Dabei wird jeweils ein Schlüsselpaar generiert: Public Key und Private Key. Der **Public Key** ist als öffentlicher Schlüssel für alle zugänglich. Der **Private Key** ist als privater Schlüssel nur dem Besitzer des Schlüsselpaares bekannt. Das Prinzip der asymmetrischen Verschlüsselung lässt sich anhand folgender **Schritte** beschreiben:

1. Ein Hashwert[1] wird auf der Nachricht generiert.
2. Der Hashwert wird mittels Private Key verschlüsselt (= Signatur).
3. Die unverschlüsselte Nachricht wird zusammen mit der Signatur übermittelt.
4. Der Empfänger entschlüsselt mit dem Public Key die Signatur.
5. Der Empfänger erzeugt auf der Nachricht einen Hashwert.
6. Die beiden Hashwerte werden miteinander verglichen.

Folgende Grafik verdeutlicht diesen Ablauf:

Abb. [13-6] **Prinzip der asymmetrischen Verschlüsselung**



Digitale Signaturen reichen nicht aus, um den Zugriff auf Objekte einzuschränken. Zum Schutz der Objekte werden deshalb auch **Access Control Lists (ACL)** verwendet, in denen festgehalten wird, welcher Benutzer in welchem Umfang auf das gewünschte Objekt zugreifen darf (z. B. nur lesen oder ändern).

13.2.8 Replikation der Daten

Der X.500-Standard basiert auf dem **Single-Master-Replikationsmodell.** Änderungen am Verzeichnis werden dabei von einem zentralen Dienst geregelt und auf die anderen Server übertragen. Dieses Modell hat aber seine Tücken. Wenn der Masterserver ausfällt, können in dieser Zeit keine Mutationen an den Objekten durchgeführt werden. Ausserdem kann die Datenbank des Masters nicht beliebig gross sein.

Mit Windows 2003 Active Directory wurde die **Multi-Master-Replikation** eingeführt. Hier kann jeder Server, der am Verzeichnis beteiligt ist, Änderungen entgegennehmen. Sie sind quasi gleichberechtigt. Ein **Replikationsdienst** sorgt dafür, dass die Änderungen auf alle anderen Server übertragen werden. Beim Ausfall eines Servers stehen also grundsätzlich alle anderen Server für Mutationen zur Verfügung.

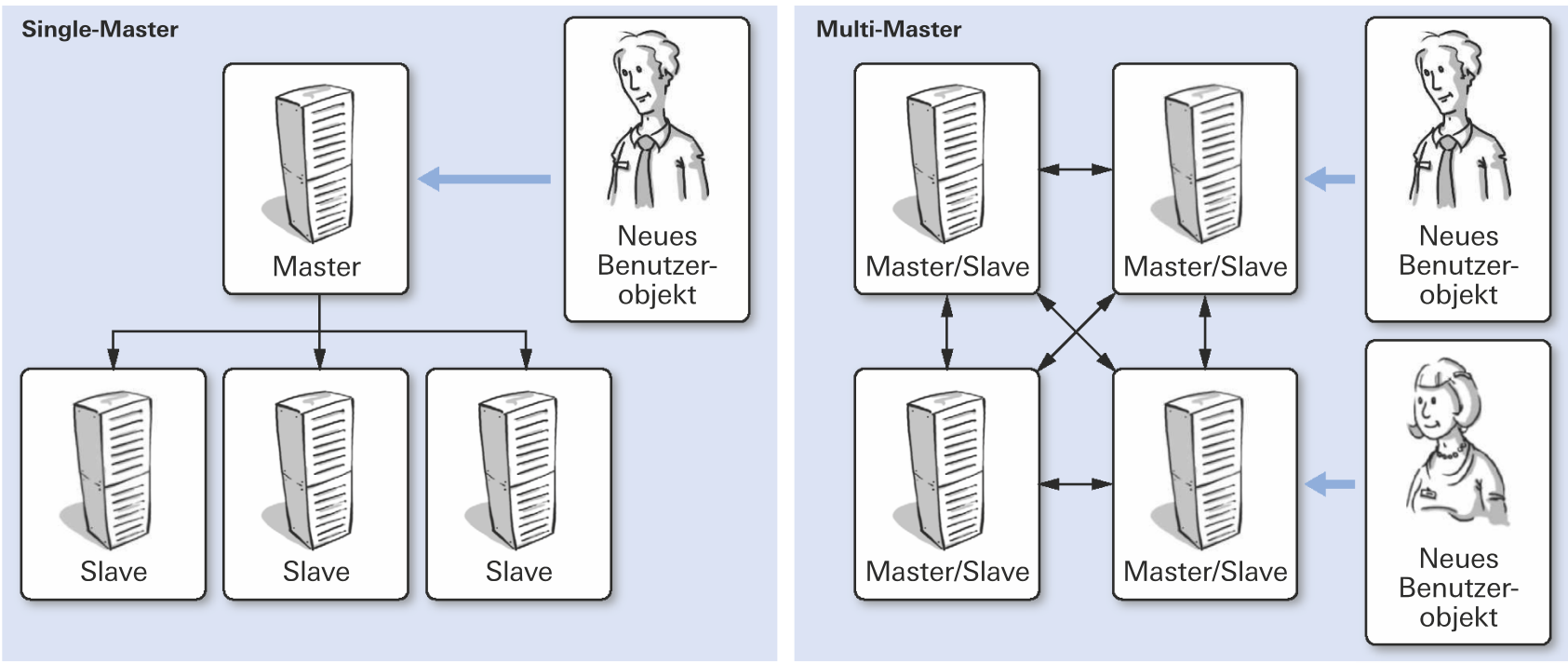
[1] Ein Hashwert wird auch als Fingerprint bezeichnet, da er eine grössere Datenmenge nahezu eindeutig kennzeichnet, ähnlich wie ein Fingerabdruck einen Menschen fast eindeutig identifiziert.

Hinweis

Die Aussage, dass beim Multi-Master-Replikationsmodell alle Server gleichberechtigt sind, gilt nicht für sämtliche Änderungen. Spezielle Änderungsvorgänge können im Active Directory nur von einem bestimmten Server vorgenommen werden, der die Betriebsmasterrolle innehat. Vergleichen Sie dazu auch das Kapitel 13.6.1, S. 102.

Folgende Grafik vergleicht die beiden **Replikationsmodelle** miteinander:

Abb. [13-7] **Replikationsmodelle im Vergleich**

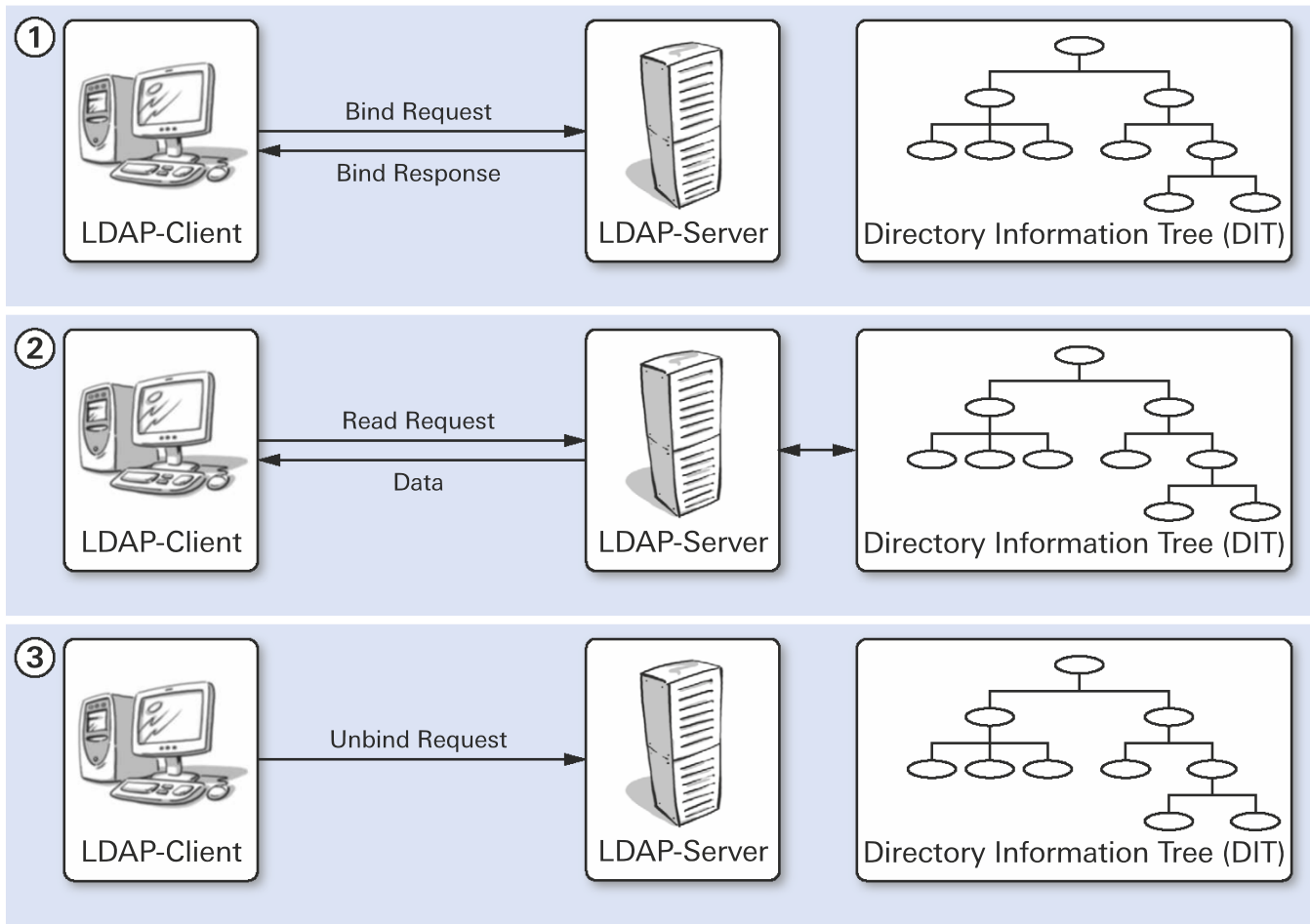


13.3 Lightweight Directory Access Protocol (LDAP)

Um Objekte in einem Verzeichnis zu speichern und von dort abzurufen, braucht es eine gemeinsame Sprache zwischen Mensch und Maschine. Diese gemeinsame Sprache wird als **Lightweight Directory Access Protocol (LDAP)** bezeichnet. Es handelt sich um eine abgespeckte Version des **Directory Access Protocol (DAP).** Dieses Kommunikationsprotokoll wurde bei der Erarbeitung des X.500-Standards definiert, hat aber einige Schwächen. So ist es zum Beispiel Ressourcen-intensiv. Die Entwicklung von DAP zu LDAP (und weiter zur LDAPv3) war ein langer Weg, der 1990 seinen Anfang nahm und bis 1997 dauerte. Viele Fachleute und Universitäten waren daran beteiligt, das Protokoll schlanker und schneller zu machen und den heutigen Bedürfnissen anzupassen.

LDAP kann textorientierte Abfragen von einem LDAP-Client zu einem LDAP-Server **über das TCP/IP-Protokoll** abwickeln. Die LDAP-Kommunikation lässt sich in drei Schritte gliedern und wie folgt darstellen:

Abb. [13-8] LDAP-Kommunikation



In der obigen Grafik können Sie gut erkennen, dass der **Verbindungsauf- und -abbau** vom Client ausgelöst wird. Beim einleitenden **Bind Request** werden Benutzername und Passwort mittels strenger Authentifizierung überprüft. Erst nach erfolgreicher Authentifizierung werden die gewünschten Daten aus dem Verzeichnis gelesen und an den LDAP-Client übermittelt. Da 99 % der Zugriffe auf Verzeichnisse über Suchabfragen erfolgen, wurde die Kommunikation entsprechend optimiert.

Bei **Suchabfragen** können Sie auf folgende Funktionen zugreifen:

- `BaseObject`: entspricht dem Startpunkt der Suchabfrage (beliebiger Knoten im Verzeichnis).
- `Scope`: definiert die Tiefe der Suche (Suche nur innerhalb BaseDN oder untergeordnete Objekte mit einbeziehen).
- `SearchFilter`: bezieht sich auf die Kriterien, die ein Attribut oder ein Eintrag besitzen muss («=» gleich, «<» kleiner als, «>» grösser als).
- `BooleanOperator`: erlauben komplexe Suchabfragen («`and`», «`or`», «`not`»).
- `SizeLimit`: legt fest, wie viele Objekte ausgegeben werden sollen (Achtung: grosse Suchabfragen können das System verlangsamen oder zum Absturz bringen).
- `TimeLimit`: definiert die Zeit, wie lange auf eine Antwort vom Server gewartet wird.

Bei der Durchführung von Änderungen stehen folgende Funktionen zur Verfügung:

- `Add`: erstellt einen Eintrag im Verzeichnis (ein Eintrag kann dabei aus mehreren Attributen bestehen).
- `Delete`: löscht einen Eintrag im aus dem Verzeichnis (gilt sowohl für Objekte als auch für Attribute und Werte).
- `Modify`: ermöglicht das Löschen, Bearbeiten und Hinzufügen bestehender Attribute.
- `Modify DN`: ermöglicht das Verschieben von Teilbäumen innerhalb des Verzeichnisses (dies gilt aber nur innerhalb desselben Servers).

Hinweis

Diese Funktionen werden häufig über eine grafische Benutzeroberfläche (GUI) angewendet und nur selten müssen Sie LDAP-Abfragen selber konstruieren. **LDP.EXE** ist ein Tool, das alle Funktionen vereint. Installieren Sie dazu die Support-Tools. Diese finden Sie auf der CD des Serverbetriebssystems.

Für den Zugriff auf LDAP-Ressourcen werden auch URLs verwendet (ähnlich wie im WWW). Wenn Sie sich beispielsweise aus dem Verzeichnis alle Mitarbeitenden der Abteilung Marketing anzeigen lassen möchten, können Sie folgende **URL** verwenden:

Ldap://server1.wondertoys.com/ou=Marketing/o=ORG?User?Department=Marketing

13.4 Kerberos

Kerberos ersetzt das **NTLM**[1]**-Protokoll,** das vor Windows 2000 für die Authentifizierung der Benutzer zuständig war. Das neue, standardisierte **Kerberos-Protokoll** basiert auf dem **Ticket-Prinzip.** Wenn Sie ein Konzert besuchen, erhalten Sie ein Ticket, das Ihnen den Zutritt in die Zone gewährt, in der sich Ihr Sitzplatz befindet. Genauso verhält es sich mit Kerberos. Bevor Sie auf eine Ressource zugreifen dürfen, erhalten Sie ein entsprechendes Ticket. Damit können Sie auf die zuvor angegebene Ressource (und nur auf diese) zugreifen. Alles andere ist nicht erlaubt. Die wichtigsten Funktionen zur Authentifizierung sind im **Key Distribution Center (KDC)** zusammengefasst. Dieses beinhaltet folgende Dienste:

- **Authentification Service (AS):** Der Authentifizierungsdienst identifiziert den Benutzer und stellt Ticket Granting Tickets (TGTs) aus, die der Client für Sitzungstickets benötigt.
- **Ticket Granting Service (TGS):** Der Ticket-Garantiedienst stellt Sitzungstickets aus, die auf Informationen beruhen, die der Client mittels TGT zugestellt hat.

Hinweis

Diese beiden Dienste laufen nicht unter eigenem Namen, sondern sind Subprozesse des im Taskmanager ersichtlichen **ISASS.EXE.** Dieser Prozess läuft nicht nur auf den Servern, sondern auch auf allen Clients. Clientseitig übernimmt dieser Prozess die Interaktion zwischen dem Benutzer und dem KDC.

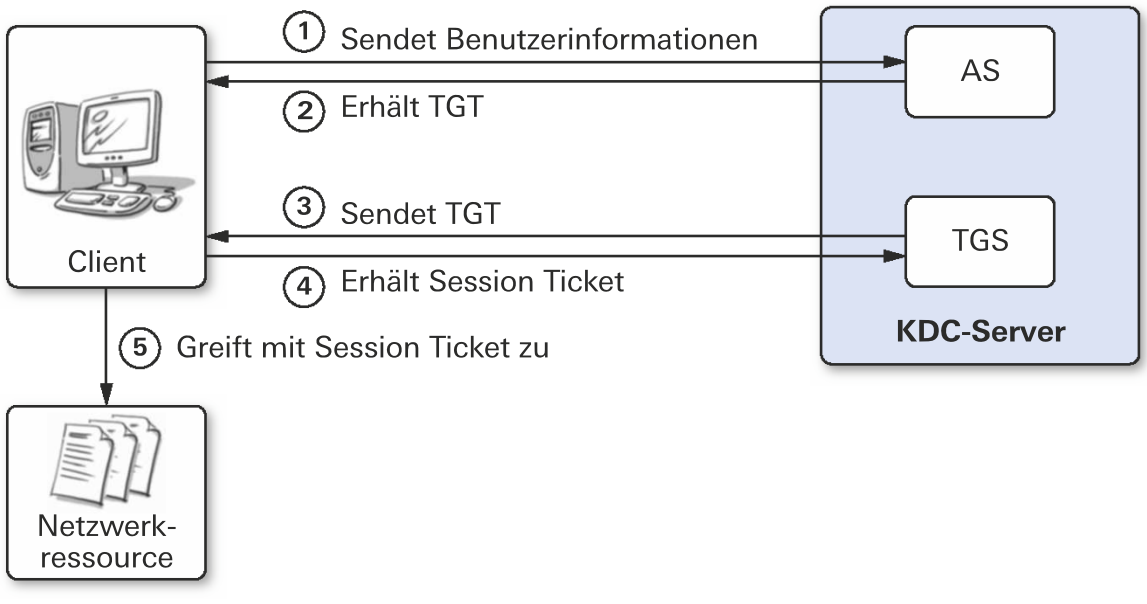
Der Authentifizierungsdienst sorgt dafür, dass sich der Benutzer gegenüber einem System eindeutig ausweist. In einem Netzwerk geschieht dies in der Regel über einen Benutzernamen und einem nur dem Benutzer bekannten Passwort. Das **Prinzip der Authentifizierung** lässt sich anhand folgender Schritte erläutern:

1. Der Benutzer authentifiziert sich mittels AS beim KDC. Die Benutzerinformationen werden dabei mit denen im Verzeichnis verglichen.
2. Stimmen Benutzername und Passwort überein, stellt der AS dem Benutzer ein TGT aus.
3. Wenn der Benutzer nun auf eine Ressource im Netzwerk, einen Share zum Beispiel, zugreifen möchte, schickt der Benutzer dem TGS sein TGT mit der Aufforderung, ihm ein passendes Ticket zu senden für den Zugriff auf diese Ressource.
4. Der TGS erstellt für den Client ein passendes Session Ticket.
5. Der Benutzer kann nun mit diesem Session Ticket auf die gewünschte Netzwerkressource, also den Server mit dem gewünschten Share, zugreifen.

[1] Abk. für: NT LAN Manager, steht für ein Authentifizierungsverfahren.

Folgende Grafik verdeutlicht diesen Ablauf:

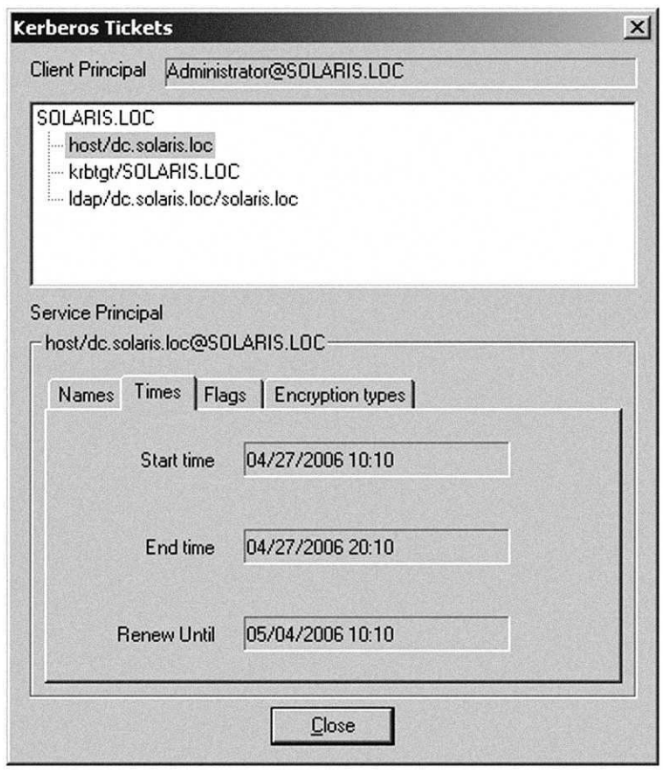
Abb. [13-9] Ablauf einer Authentifizierung



Ein **Sitzungsticket** enthält folgende Informationen:

- Versionsnummer des Tickets
- Name der Domäne, die das Ticket ausgestellt hat
- Name des Servers, auf dem es gültig ist
- Sitzungsschlüssel
- Name der Domäne des Clients
- Name des Clients
- Ausstellungszeitpunkt
- Gültigkeitsdauer

Abb. [13-10] Kerberos-Ticket (Beispiel)



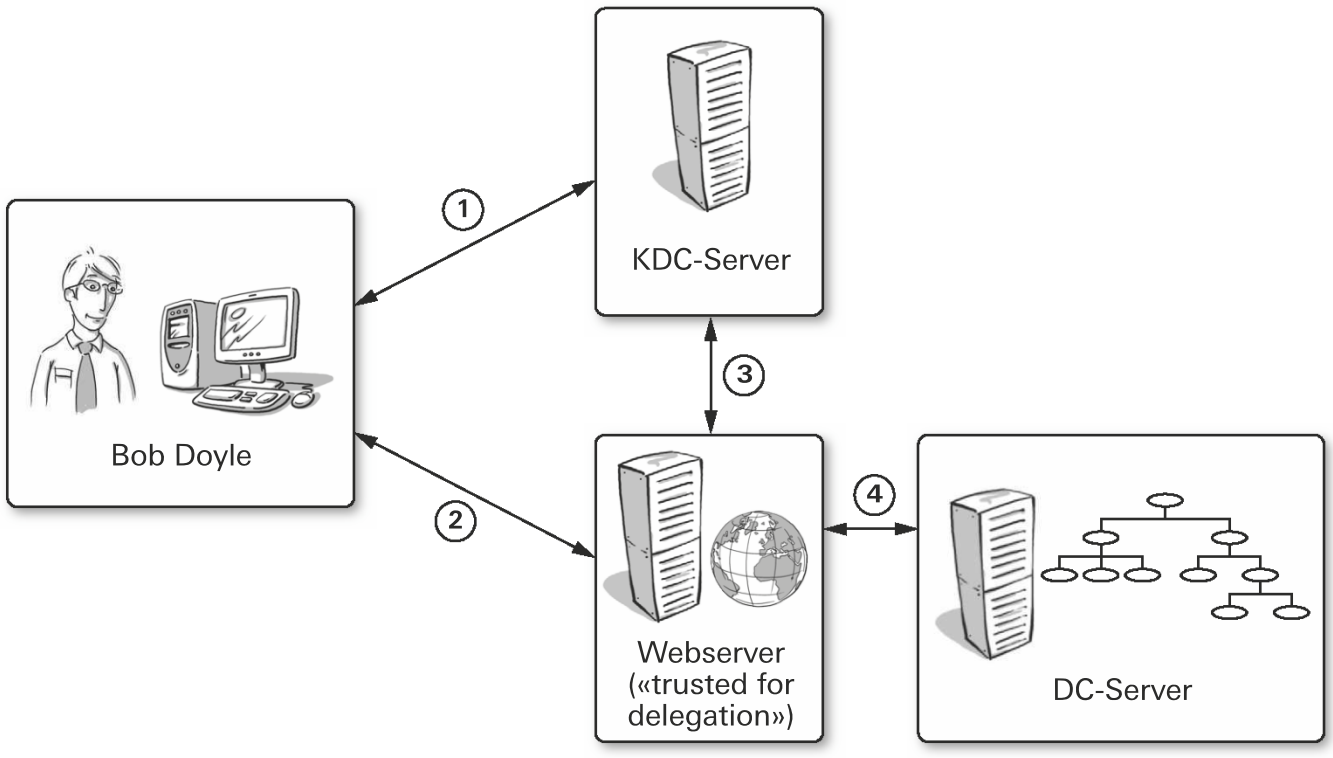
Mit Kerberos lassen sich Aufgaben delegieren. Ein gutes Beispiel dafür ist ein webbasiertes Adressbuch, das die Informationen aus dem Active Directory holt. Man spricht in diesem Zusammenhang auch von einer **Multi-Tier-Anwendung.** Eine Multi-Tier-Anwendung ist eine Erweiterung der Client-Server-Architektur, in der Client-PCs und Server direkt (d. h. ohne Zwischenrechner) miteinander kommunizieren. Indem eine oder mehrere Serverstufen dazwischengeschaltet werden, lassen sich rechenintensive Vorgänge wie z. B. der Bildschirmaufbau auf einen vorgelagerten Server (Front-End) auslagern. Kerberos stellt die Authentifizierung sicher, sodass alle involvierten Server problemlos miteinander kommunizieren können.

Die **Aufgabendelegation** lässt sich an folgendem Beispiel erläutern:

1. Bob Doyle holt sich beim KDC ein Ticket, um auf den Webservice zugreifen zu können.
2. Mithilfe des Session Ticket kann er auf den Webserver zugreifen und seine Suchanfrage eingeben.
3. Das vom Benutzer gesendete Ticket ist aber nur für den Webserver gültig. Damit die gesuchten Daten vom Domänenkontroller geholt werden dürfen, muss sich der Benutzer dort ebenfalls authentifizieren. Dies macht aber der Webserver für ihn, da er «trusted for delegation» ist.
4. Der Webserver schickt im Auftrag von Bob Doyle das Ticket zum DC und darf die angeforderte Suche ausführen.

Folgende Grafik verdeutlicht den beschriebenen Ablauf:

Abb. [13-11] **Delegation bei Multi-Tier-Anwendungen**



13.5 Die logische Sicht auf Active Directory

Active Directory ist eine **verteilte Datenbank,** deren Inhalte über verschiedene Dienste auf den Domänencontrollern zur Verfügung gestellt werden. Diese Datenbank lässt sich aus einer logischen und einer physikalischen Sicht betrachten. Die **logische Sicht** umfasst Aspekte wie Umfang und Delegation der Benutzerrechte. Die **physikalische Sicht** beschreibt den Aufbau und das Netzwerk. Diese Betrachtungsweisen erlauben ein passendes Design, je nachdem, ob administrative Delegation oder Domänenkontroller und Netzwerkverbindungen geplant werden müssen.

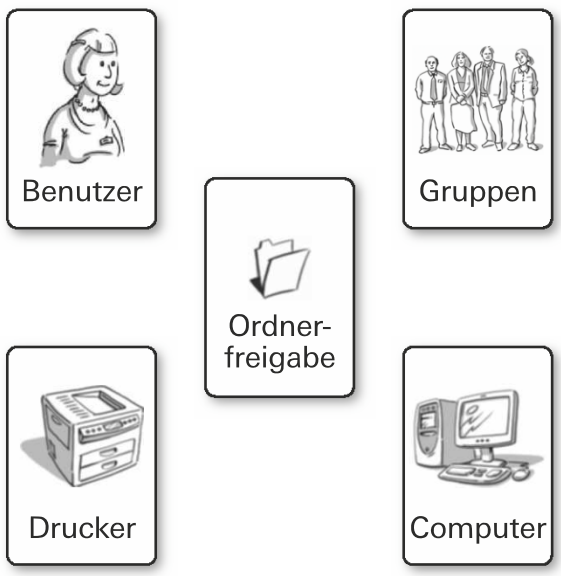
Nachfolgend wird zunächst die **logische Sicht** behandelt. Diese erlaubt die Strukturierung der Verwaltungs- und Organisationsanforderungen und umfasst folgende **Komponenten:**

- Objekte (Benutzer, Computer, Gruppen, Drucker, Freigaben etc.)
- Organisationseinheiten (OU)
- Domäne
- Struktur (Tree)
- Gesamtstruktur (Forest)
- Vertrauensstellungen

13.5.1 Objekte

Als Objekte werden im Active Directory **Netzwerkressourcen** angelegt. Alle Objekte haben einen eindeutigen Namen und eine definierte Anzahl von Attributen. Hier die gebräuchlichsten Objekte im Überblick:

Abb. [13-12] **Objekte im AD**



Hinweis

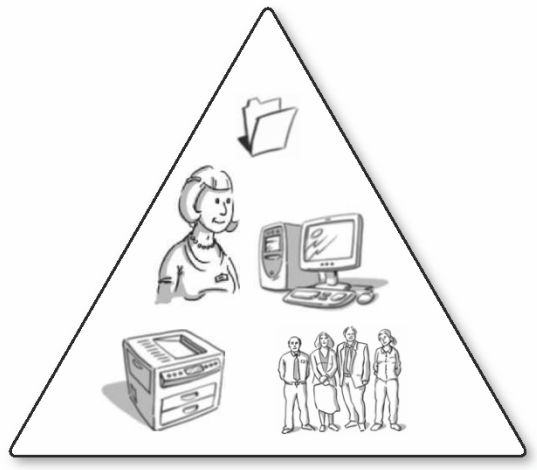
Auch OUs und Richtlinien sind AD-Objekte. Aufgrund ihrer Besonderheiten werden sie aber an dieser Stelle nicht aufgeführt.

13.5.2 Domäne

In einer **Domäne** können Millionen von Objekten gespeichert und verwaltet werden. Active Directory umfasst im Minimum einen einzigen Forest mit einer einzigen Domäne. Eine Domäne ist eine unabhängige Verwaltungseinheit, in der der **Domänenadministrator** weitgehende Rechte ausübt. Jede Domäne hat ihre eigenen Sicherheitseinstellungen, die unabhängig von weiteren Domänen konfiguriert und verwaltet werden können.

Der **Administrator einer Forest Root**[1] hat weitgehende Rechte über alle später hinzugefügten Domänen. Bei der Erstellung einer Domäne erhält diese einen Namen, der sich an der DNS-Struktur orientiert (z. B. wondertoys.com). Auf diese Weise wird sichergestellt, dass für die Namensauflösung kein zusätzlicher Dienst (ausser DNS) notwendig ist.

Abb. [13-13] **Domäne im AD**



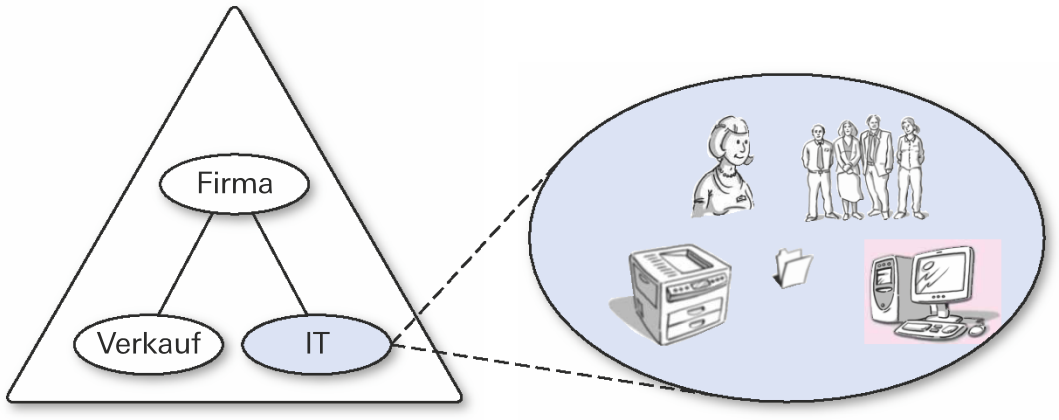
[1] Erste in einem Forest erstellte Domäne.

13.5.3 Organisationseinheit

Organisationseinheiten (OUs[1]**)** dienen zur Strukturierung der Objekte innerhalb einer Domäne, zur besseren Delegation der Verwaltungsaufgaben und zur Implementierung der Gruppenrichtlinien. Sie können mit den Fächern eines Kleiderschranks verglichen werden. Objekte, die untereinander in einer bestimmten Beziehung stehen, können über OUs einfach zusammengefasst und schnell wieder gefunden werden.

Die **OU-Struktur** ist ebenfalls hierarchisch aufgebaut und kann von Domäne zu Domäne unterschiedlich sein. Mehr über den Aufbau und die Verwendung von OU-Strukturen erfahren Sie in Kapitel 14.6, S. 109.

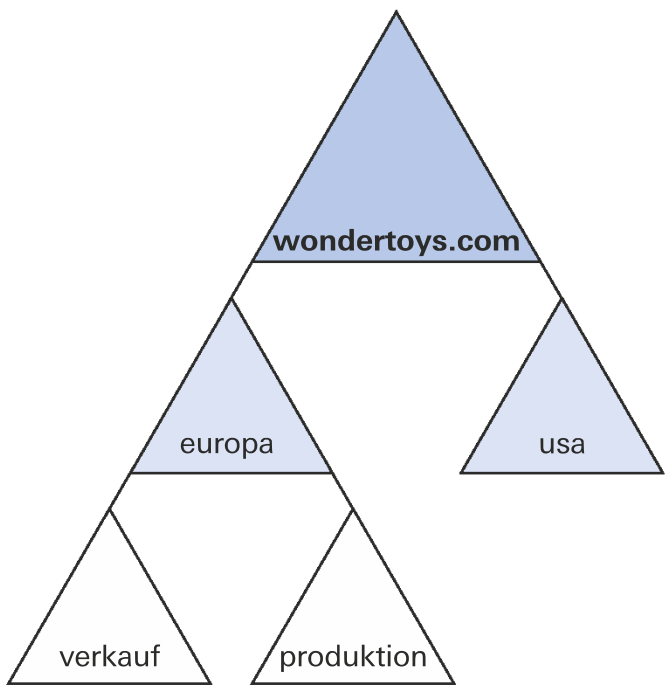
Abb. [13-14] **OUs als Strukturierungsgrundlage**



13.5.4 Tree (Struktur)

Unter **Tree** oder Struktur wird die hierarchische Anordnung einer oder mehrerer AD-Domänen im selben DNS-Namespace verstanden. Was auf den ersten Blick etwas verwirrend klingt, ist die Tatsache, dass auch eine einzelne Domäne bereits eine Struktur darstellt. Die erste Domäne, die Sie erstellen, trägt die Bezeichnung **Stammdomäne (Root Domain).** An ihr können beliebig viele Unterdomänen angehängt werden. Einzige Bedingung zu einem Tree ist, dass sie zum gleichen Namespace gehören müssen.

Abb. [13-15] **Tree (Struktur)**

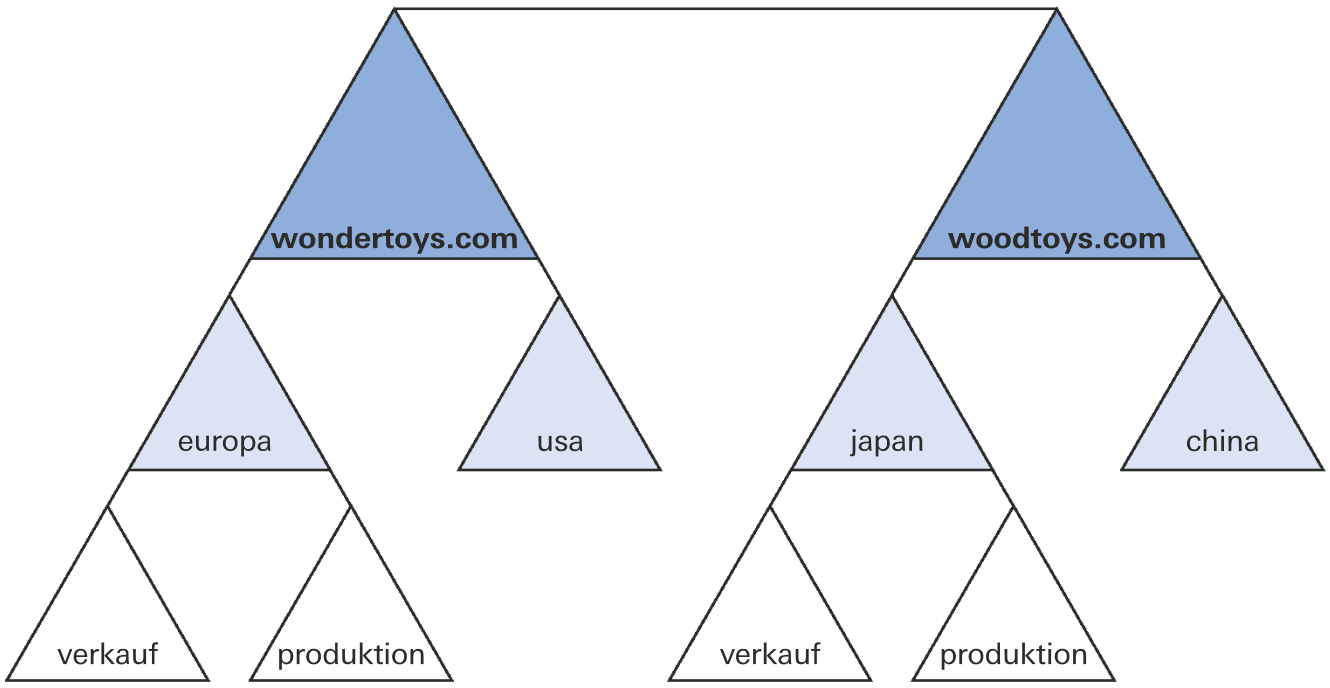


[1] Die Abkürzung OU kommt aus dem Englischen und bedeutet Organizational Unit.

13.5.5 Forest (Gesamtstruktur)

Mit **Forest** oder Gesamtstruktur ist das komplette Verzeichnis gemeint. Ein Verzeichnis kann sowohl aus einer einzelnen Domäne als auch aus mehreren Strukturen bestehen. Wenn Sie die englischen Begriffe «tree» (für Struktur) und «forest» (für Gesamtstruktur) heranziehen, wird das Hierarchieprinzip klar; mehrere Bäume ergeben einen Wald. Vergleichen Sie dazu die folgende Abbildung:

Abb. [13-16] **Gesamtstruktur (Forest)**



Eine Gesamtstruktur ist durch folgende **Merkmale** gekennzeichnet:

- Alle Domänen innerhalb einer Gesamtstruktur basieren auf demselben Schema.
- Alle Domänen nutzen einen gemeinsamen globalen Katalog[1].
- Die einzelnen Strukturen weisen einen eigenen Namespace auf.
- Jede Domäne in einer Gesamtstruktur ist weitgehend unabhängig, dennoch können sie miteinander kommunizieren.

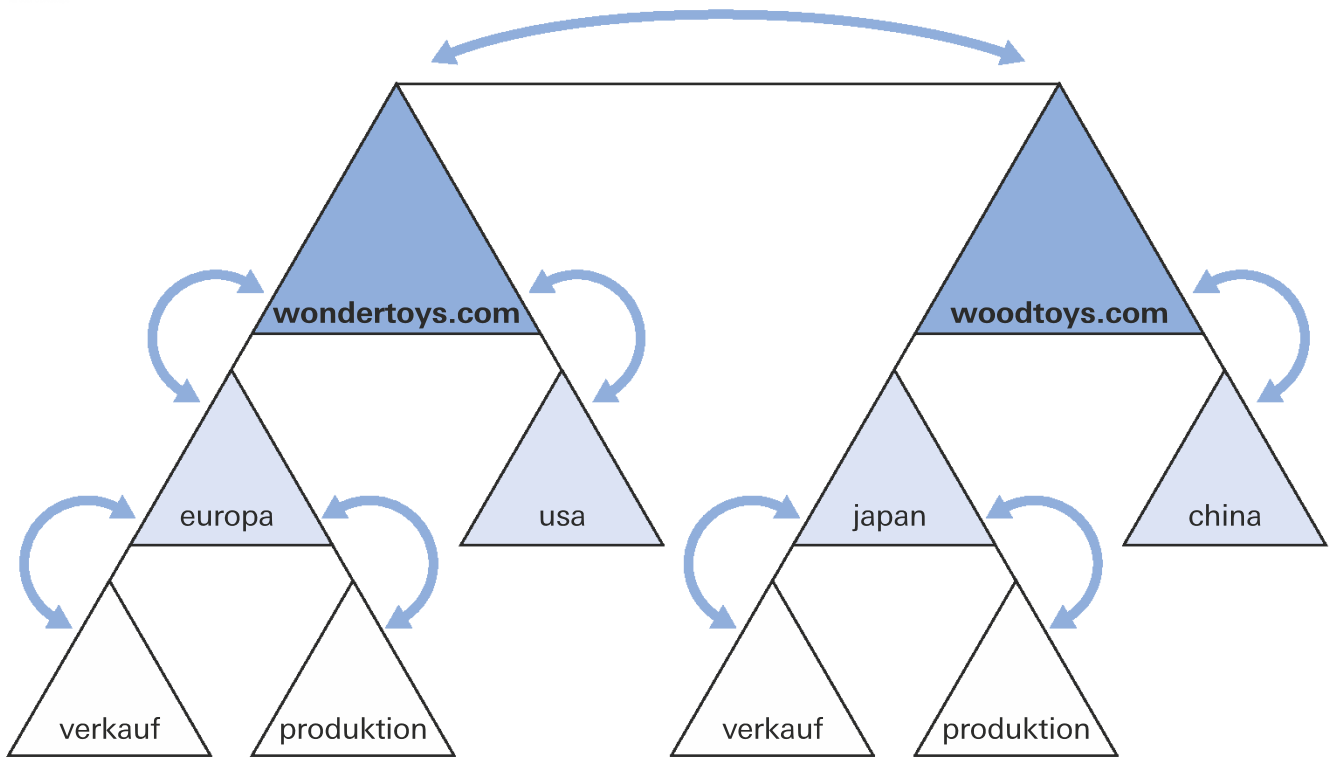
13.5.6 Vertrauensstellungen

Da jede Domäne eine eigene, unabhängige Verwaltungseinheit darstellt, braucht es zwischen ihnen Schnittstellen, die es ermöglichen, über die gesamte Struktur hinweg auf Ressourcen zuzugreifen. Diese Schnittstelle wird als **Vertrauensstellung** bzw. **Trust** bezeichnet.

Vertrauensstellungen existieren zwischen jeder über- und untergeordneten Domäne, aber auch zwischen den einzelnen Trees bzw. Strukturen. Vergleichen Sie dazu die folgende Grafik.

[1] Beim globalen Katalog handelt es sich um ein Suchverzeichnis für die DIB. Vergleichen Sie dazu das Kapitel 13.7, S. 104.

Abb. [13-17] Vertrauensstellungen (Trusts)



⟷ Vertrauensstellung

In Windows 2008 lassen sich folgende **Arten von Vertrauensstellungen** unterscheiden:

- Überordnungs-Unterordnungs-Vertrauensstellung (Parent-Child Trust)
- Strukturstamm-Vertrauensstellung (Tree-Root Trust)
- Externe Vertrauensstellung (External Trust)
- Shortcut-Vertrauensstellung (Shortcut Trust bzw. Shortlink Trust)
- Bereichsvertrauensstellung (Realm Trust)
- Gesamtstrukturvertrauensstellung (Forest Trust)

Hinweis Der Einfachheit halber wird in diesem Lehrmittel generell von Vertrauensstellung gesprochen.

13.6 Die physikalische Sicht auf Active Directory

Die physikalische Sicht des Active Directory umfasst im Wesentlichen den **Domänenkontroller** und die **Standorte**. Jeder Standort (Site) ist mit folgenden **Merkmalen** verbunden:

- Replikationsverbindungen (Inter- und Intra-Site)
- Standortverknüpfungen
- Standortverknüpfungsbrücken (Site Link Bridge)
- Subnetze

13.6.1 Domänenkontroller

Der **Domänenkontroller (DC)** ist ein Server, auf dem Windows Server mit Active Directory installiert ist, und bildet die Basis jeder Domäne. Auf dem DC wird die AD-Datenbank gespeichert. Er verwaltet die Replikation der Datenbank mit anderen DCs der gleichen oder anderer Domänen der gleichen Struktur oder Gesamtstruktur. Der DC ist auch für die Authentifizierung der Clients zuständig und beantwortet Benutzeranfragen bezüglich Netzwerkressourcen wie Drucker, Freigaben, Mailadressen etc.

Die DCs arbeiten zwar mit einem Multi-Master-Replikations-Modell. Für spezielle Aufgaben wird aber ein spezieller DC zur Ausführung bestimmt. Solche Aufgaben, die einem einzigen DC zugewiesen werden, werden unter dem Begriff **Betriebsmasterrolle** zusammengefasst. Es können folgende Betriebsmasterrollen unterschieden werden:

Betriebsmasterrolle	Aufgaben
Schema-Master (1x pro Gesamtstruktur)	Diese Rolle übernimmt der erste Domänenkontroller in der Gesamtstruktur. Dieser verwaltet alle Änderungen am Schema, wie das Hinzufügen von neuen Objektklassen oder Attributen. Ein typisches Beispiel aus der Praxis in Bezug auf eine Schemaerweiterung ist die Installation eines Exchange Servers. AD-Objekte werden dabei um Messaging-spezifische Attribute erweitert.
Domänennamen-Master (1x pro Gesamtstruktur)	Diese Rolle verwaltet das Hinzufügen und Entfernen von Domänen und Strukturen. Wenn Sie eine neue Domäne erstellen möchten, muss dieser Dienst verfügbar sein.
RID[1]-Master (1x pro Domäne)	Diese Rolle verwaltet die Pools der Relativ-IDs. Die RID ist eine Nummer, die jedem neuen Objekt innerhalb einer Domäne zugewiesen wird. Zusammen mit der Domänen-ID ergibt es die SID, die eine eindeutige Identifikation eines Objektes erlaubt.
PDC[2]-Emulator (1x pro Domäne)	Diese Rolle emuliert unter anderem einen Windows NT 4.0 PDC. Er hilft bei der Authentifizierung von älteren Clients, die nicht auf normalem Weg mit Active Directory kommunizieren können. Das sind alle Clients vor Windows 2000. Zudem ist der für die Zeitsynchronisation und Passwortänderungen zuständig.
Infrastruktur-Master (1x pro Domäne)	Diese Rolle ist für die Updates von Referenzen über Domänengrenzen hinweg zuständig, z. B. wenn ein Objekt seinen DN wechselt. Auch normale Objektänderungen wie das Hinzufügen einer Telefonnummer zu einem Benutzerobjekt laufen darüber. Er sorgt ebenfalls dafür, dass keine veralteten Objekte auf den globalen Katalogservern vorhanden sind. Des Weiteren aktualisiert er die Zuordnung von Benutzern zu Gruppen, wenn diese umbenannt wurden.

[1] Abk. für: Relativ-ID.
[2] Primary Domain Controller.

Hinweis

Die Betriebsmasterrollen werden im Englischen als Flexible Single Master Operations (FSMO) bezeichnet. In der Praxis werden Sie deshalb oft auch den Ausdruck FSMO-Rollen hören.

13.6.2 Standorte und Subnetze

Unter **Standort** wird eine Gruppe von Domänenkontrollern verstanden, die in einem oder in mehreren **IP-Subnetzen** vorhanden sind und durch eine schnelle Leitung (mind. 1 Mbit/s) miteinander verbunden sind. Zu jedem Standort gehören eines oder mehrere Subnetze. Damit Informationen auf den Domänenkontrollern standortübergreifend repliziert werden können, sind **Standortverknüpfungen** notwendig. Standardmässig ist der Vorgabewert **Site Link** vorgegeben, dessen Einstellungen für alle Replikationsverbindungen übernommen werden, sofern keine eigenen Standortverknüpfungen eingerichtet sind.

Abb. [13-18] **Standorte und Subnetze**

13.7 Globaler Katalogserver

Der **Global Catalog (GC)** ist eine weitere spezielle Funktion, die ein DC übernehmen kann. Der GC ist der Speicher für alle Objekte einer Struktur bzw. Gesamtstruktur und gilt deshalb als die **zentrale Suchmaschine für Abfragen innerhalb des Active Directory.** Um effiziente Abfragen auch bei Millionen von Objekten noch zu gewährleisten, werden zwar alle Objekte gespeichert, aber nur mit einer limitierten Anzahl von Attributen. Damit sind Attribute gemeint wie zum Beispiel Benutzername, Telefonnummer, Abteilung, die für eine Suche sinnvoll sind. Über das Schema wird geregelt, welche Attribute auf dem GC gespeichert werden. Im Wesentlichen erfüllt der globale Katalogserver folgende **Funktionen:**

- Hilft bei Benutzeranmeldungen, weil er als einziger Server die Teilnehmer in universellen Gruppen kennt.
- Ist bei Suchanfragen der Benutzer oder Anwendungen für das Auffinden der gesuchten Objekte verantwortlich.

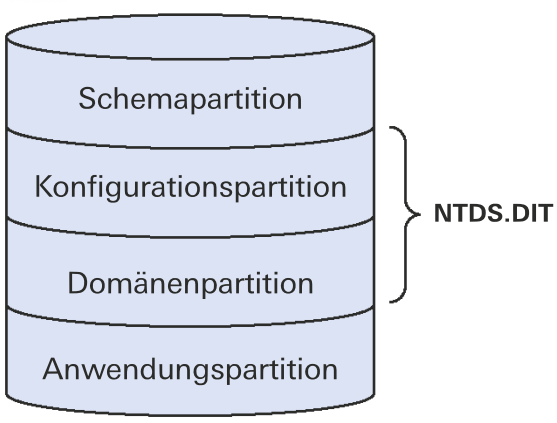
Hinweis

In grossen Domänen mit einer Vielzahl von Benutzern müssen aus Sicherheitsgründen mindestens zwei DCs die Funktion als globaler Katalogserver übernehmen, damit die universellen Gruppen auch überprüft werden können, wenn einer ausfällt.

13.8 Active-Directory-Datenbank

Die Active-Directory-Datenbank ist im Grunde nichts anderes als eine Datei, die auf jedem Domänenkontroller unter **C:\WINDOWS\NTDS\NTDS.DIT** hinterlegt ist. Die logische Struktur dieser Datenbank lässt sich wie folgt darstellen:

Abb. [13-19] **Struktur der Active-Directory-Datenbank**



In der folgenden Tabelle werden die einzelnen **Partitionsbereiche** näher erläutert:

Partitionsbereich	Beschreibung
Schemapartition	Hier werden die einzelnen Objektklassen und Attribute gespeichert. Änderungen am Schema beziehen sich immer auf diesen Abschnitt. Die Informationen aus diesem Bereich der Datenbank werden auf alle Domänenkontroller in der Gesamtstruktur repliziert.
Konfigurations-partition	In diesem Bereich werden Informationen gespeichert zu den Standorten, den installierten Diensten und den Standortverknüpfungen. Die Informationen aus diesem Bereich der Datenbank werden auf alle Domänenkontroller in der Gesamtstruktur repliziert.
Domänenpartition	Hier werden die Netzwerkressourcen wie Benutzer, Computer, Drucker etc. gespeichert. Wie der Name schon sagt, handelt es sich um Informationen der jeweiligen Domäne. Aus diesem Grund werden die Informationen nur auf Domänenkontroller repliziert, die sich auch in derselben Domäne befinden.
Anwendungs-partition	Bis jetzt wird dieser Bereich erst von DNS genutzt. Er ist dafür vorgesehen, Informationen nur auf die Domänenkontroller einer Gesamtstruktur zu replizieren, auf denen sie effektiv benötigt werden, d. h. unabhängig von deren Zugehörigkeit zu einer Domäne. Microsoft hält sich die Option offen, diesen Bereich in Zukunft auch für andere Anwendungen zu gebrauchen.

13.9 SYSVOL-Ordner

Bei der Installation des Active Directory wird neben dem Ordner **C:\Windows\NTDS** auch der Ordner **C:\Windows\SYSVOL** angelegt. Dieser wird für folgende Aufgaben verwendet:

- Speicherung der Gruppenrichtlinien für die entsprechende Domäne
- Speicherung der Login-Scripts und deren Bereitstellung über den NETLOGON-Share

Der **SYSVOL-Ordner** ist auf dem System als versteckter Share freigegeben. Diese Freigabe wird benötigt, damit die Gruppenrichtlinien und Login-Scripts auf die anderen DCs repliziert werden können.

Zusammenfassung

Um innerhalb eines Firmennetzwerks Hunderte oder gar Tausende von Objekten verwalten zu können, braucht es einen **Verzeichnisdienst** wie beispielsweise das Active Directory von Microsoft. Active Directory beruht auf dem **Prinzip der verteilten Datenbank** und dem **X.500-Standard.** Hier sind alle Spezifikationen für einen skalierbaren, leistungsfähigen, sicheren, verfügbaren und erweiterbaren Verzeichnisdienst enthalten.

Der Aufbau des Active Directory ist streng **hierarchisch.** Dadurch wird eine effiziente Suche gewährleistet. Um Daten in und aus dem Verzeichnis zu lesen bzw. zu schreiben, wird eine passende Schnittstelle benötigt. Diese Schnittstelle liefert das **Lightweight Directory Access Protocol.** Dank diversen Funktionen ist **LDAP** optimal auf Suchvorgänge abgestimmt. Bevor ein Benutzer auf Daten eines Verzeichnisses zugreifen darf, muss er authentifiziert werden. Eine sichere Authentifizierung wird mittels **Kerberos-Protokoll** gewährleistet. Dabei werden die Benutzerangaben verschlüsselt übertragen und der Benutzer erhält ein Ticket, das ihm den Zugriff auf Netzwerkressourcen erlaubt.

Bei jedem Verzeichnisdienst kann eine logische und eine physikalische Sicht unterschieden werden. Die **logische Sicht** von **Active Directory** umfasst Objekte, Domäne, Organisationseinheiten, Trees (Strukturen), Forests (Gesamtstrukturen) und Vertrauensstellungen. Die **physikalische Sicht** besteht aus Domänenkontrollern, Standorten und Subnetzen.

Jeder **Domänenkontroller (DC)** ist in der Lage, die Funktion des globalen Katalogservers zu übernehmen. Aus Sicherheitsgründen sollten mindestens zwei DCs vorhanden sein und jeder DC eine Kopie der Active-Directory-Datenbank aufweisen. Die Datenbank **NTDS.DIT** besteht aus vier Partitionsbereichen mit Informationen entweder für die Domäne oder den Forest.

Der **SYSVOL-Ordner** ist ebenfalls Bestandteil jedes DC und für die Replikation von Informationen unter den DCs zuständig. Er beinhaltet aber die Login-Scripts, die bei der Anmeldung der Clients ausgeführt werden.

Aufgaben

37	Nennen Sie fünf entscheidende Vorteile, die ein Verzeichnisdienst mit sich bringt.
38	Welches sind die Hauptmerkmale des X.500-Standards?
39	Erklären Sie die Funktionen des Schemas in Active Directory.

14 Active-Directory-Struktur planen

Lernziele

Nach der Bearbeitung dieses Kapitels können Sie …

- die Kriterien zur Überprüfung der Aussagekraft von Kundenanforderungen nennen.
- aufzeigen, welche Konsequenzen der Erfüllungsgrad dieser Kriterien auf die Qualität der Erhebung hat.
- die wichtigsten Kategorien von Informationen bezeichnen, die in einem Directory Service enthalten sind.
- anhand von Beispielen erläutern, wie diese Informationskategorien zu einem effizienten und sicheren Systembetrieb beitragen.
- die grundlegenden Schritte darlegen, die bei der Planung und Einführung eines Directory Service durchlaufen werden müssen.
- aufzeigen, welchen Beitrag diese Schritte zu einem funktionsfähigen System leisten.

Schlüsselbegriffe

Abteilungsmodell, Benennungsstrategie, Benutzerkonten, Container, Forest, Gesamtstruktur, Kombinationsmodell, Mehrdomänenmodell, Objektmodell, Organisationseinheit, Rechnerkonten, Richtlinien, Standortmodell, Struktur, Tree, Einzeldomäne

Um eine Active-Directory-Struktur zu planen, benötigen Sie neben einem Netzwerkdiagramm auch Angaben über Sicherheitsanforderungen bezüglich des Zugriffs auf Ressourcen. Ferner brauchen Sie auch Angaben über die Organisation der Verwaltungsaufgaben der Ressourcen, die im Active Directory gespeichert werden sollen. Auf Basis dieser Informationen können Sie anschliessend bestimmen, wie viele Gesamtstrukturen, Strukturen und Domänen notwendig sein werden.

14.1 Einzeldomänen-Modell

Die einfachste Active-Directory-Struktur ist die Einzeldomäne. Das **Einzeldomänen-Modell** reicht für die meisten Unternehmen aus und zeichnet sich dadurch aus, dass die Verwaltung von Benutzern, Gruppen, Richtlinien usw. stark vereinfacht wird. Einfach bedeutet weniger Aufwand bei der Planung, Verwaltung und Fehlerbehebung. Diese Faktoren wirken sich auch positiv auf die Kosten aus.

Bei NT 4.0 gab es folgende Gründe, die für ein **Mehrdomänen-Modell** sprachen:

- **Delegation der Verwaltungsaufgaben:** Wenn Objekte in unterschiedlichen Bereichen angelegt wurden, musste für jeden Bereich eine eigene Domäne erstellt werden.
- **Limitierte Anzahl Objekte:** Pro Domäne konnten lediglich 40 000 Objekte verwaltet werden. Grosse Unternehmen mussten deshalb meist mehrere Domänen verwalten.

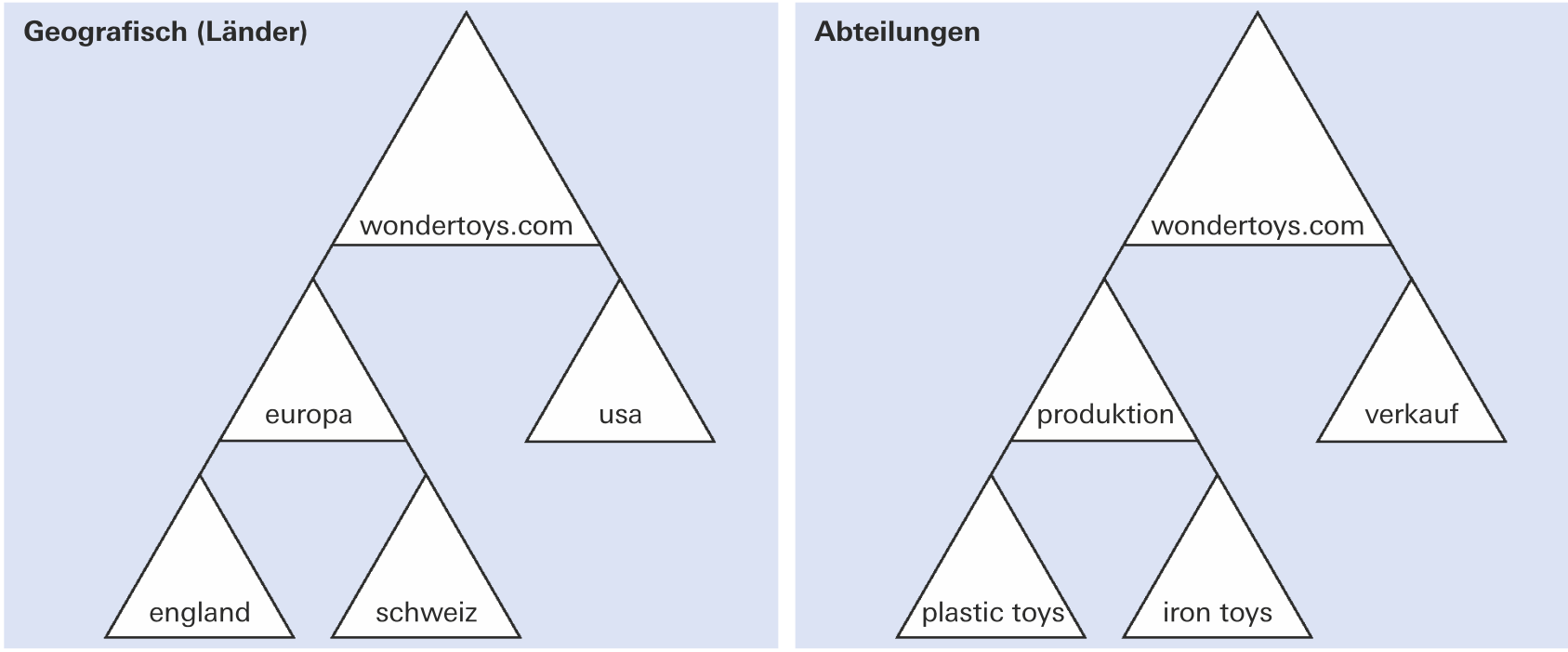
Heute bestehen diese Einschränkungen bei Einzeldomänen nicht mehr. Für die Delegation von Verwaltungsaufgaben können Organisationseinheiten benutzt und pro Domäne mehrere Millionen Objekte verwaltet werden. Versuchen Sie also, Ihre Bedürfnisse in einer einzigen Domäne abzubilden, und widerstehen Sie der Versuchung einer Untergliederung in mehrere Domänen und Subdomänen.

14.2 Mehrdomänen-Modell

In Ausnahmesituationen müssen ggf. mehrere Domänen eingesetzt werden. Versuchen Sie in solchen Fällen **alle Domänen in derselben Struktur** unterzubringen. Dies hat den Vorteil, dass Sie nur einen Namespace verwalten müssen.

Sie legen die **Grenzen mehrerer Domänen** fest, indem Sie die Domänen entsprechend den Unternehmensgrenzen gliedern. Dabei empfiehlt es sich, die Standorte und nicht die Abteilungen des Unternehmens als Gliederungskriterium zu verwenden. Der Grund dafür: Es ist wahrscheinlicher, dass sich Abteilungen verändern als dass Standorte von einem Tag auf den anderen verlegt werden oder komplett verschwinden. Hier zwei Beispiele für Strukturen im Mehrdomänen-Modell:

Abb. [14-1] **Domänenstrukturen geografisch und nach Abteilungen**



Folgende **Gründe** sprechen für ein Mehrdomänen-Modell:

- Unterschiedliche Anforderungen an die Sicherheitsrichtlinie. Die Richtlinien bezüglich Passwortlänge, Kerberos-Tickets, Überwachung, IPSec usw. können nur zentral auf Domänenebene erstellt und verwaltet werden. Wenn andere Standorte oder Abteilungen eigene Anforderungen an diese Sicherheitseinstellungen haben, wird der Einsatz von mehreren Domänen unabdingbar.
- Dezentrale Verwaltung kann mit ein Grund sein, mehrere Domänen einzusetzen. Insbesondere dann, wenn jeder Standort eine eigene IT-Abteilung besitzt mit der Vollmacht, neue DCs zu installieren und eigene Sätze von Richtlinien zu definieren.
- Bessere Optimierung der Replikation unter den Standorten. Wenn eine WAN-Verbindung so langsam und unzuverlässig ist, dass eine Replikation von Objekten schwierig ist, macht es Sinn, an diesem Standort eine eigene Domäne zu errichten.
- Ein Grund für mehrere Domänen kann sein, dass eine bestehende Domänenstruktur übernommen und beibehalten werden muss. Sei dies aus NT-4.0- oder Windows-2000-Zeiten.
- Zum Schutz des Schemas und der Enterprise-Admins. Dabei wird eine leere Domäne erstellt mit zwei DCs, die nur das Schema verwalten. Es finden sich keine weiteren betriebsspezifischen Objekte in dieser Domäne (Empty Root Domain).

Je mehr Domänen angelegt werden, desto mehr Domänenkontroller sind notwendig. Dies erhöht nicht nur die Kosten für die Hardware, sondern auch für die Systemadministration. Wenn Sie eine komplexe IT-Infrastruktur aufbauen möchten, reicht für deren Betreuung ein mit Grundkenntnissen ausgebildeter Systemadministrator nicht mehr aus.

14.3 Ein- oder Mehrstruktur-Modell?

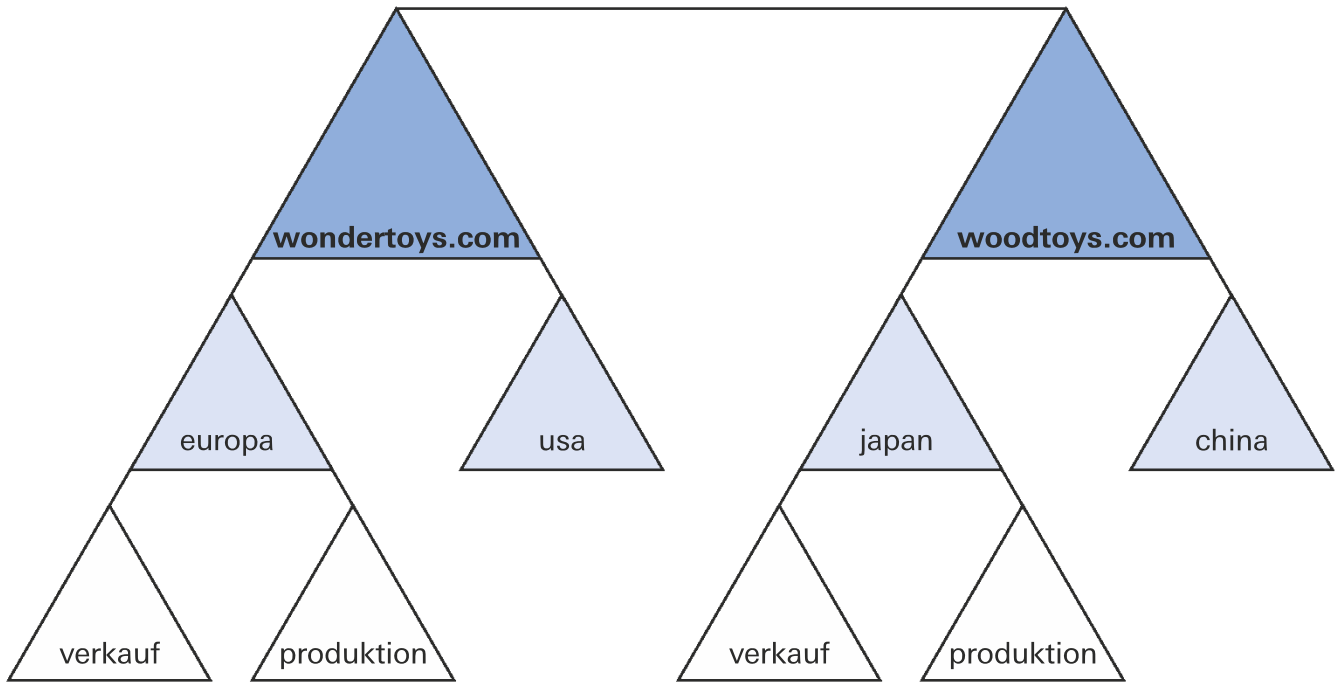
Mehrere Strukturen (Trees) sind nur dann nötig, wenn unterschiedliche DNS-Namespaces unterstützt werden sollen.

Beispiel

Die Firma Wondertoys.com besitzt eine Tochtergesellschaft mit dem Namen Woodtoys.com. Diese ist voll in das Unternehmen integriert, tritt aber unter eigenem Namen auf dem Markt auf.

Betreffend der **AD-Funktionalität** spielt es keine Rolle, ob in einem Forest alle Domänen in einem einzigen Tree oder in mehreren Trees angeordnet sind. Nur in der Forest-Root-Domain sind die Enterprise- und Schema-Admins mit weitgehenden Rechten vorhanden. Die Root-Domain einer zusätzlichen Struktur ist allen anderen Domänen innerhalb der Gesamtstruktur gleichgestellt. Eine zusätzliche Struktur muss also nur dann angelegt werden, wenn innerhalb des Forests ein separater DNS-Namensraum benötigt wird.

Abb. [14-2] **Mehrstruktur-Modell**



14.4 Ein- oder Mehrgesamtstruktur-Modell

Gesamtstrukturen stellen die äussere Sicherheitsbarriere dar. Sie können nur zusammenarbeiten, wenn dies ausdrücklich verlangt wird. Mit dem Forest Trust konnte die Komplexität reduziert und die Kosten planbar gemacht werden, was die Zusammenarbeit mehrerer Gesamtstrukturen deutlich vereinfacht. Auch wenn Sie mehrere Gesamtstrukturen vermeiden sollten, gibt es Fälle, bei denen mehrere Gesamtstrukturen vorteilhaft sind. Solche Fälle sind etwa:

- Fusion von Unternehmen: Wenn zwei oder mehrere Unternehmen, die über eine eigene Active-Directory-Struktur verfügen, zusammengeführt werden sollen, können sie über eine Gesamtstrukturvertrauensstellung vereint werden. Danach können alle Ressourcen unternehmensweit eingesetzt werden.
- Isolation einer Organisationseinheit: Geschäftsbereiche oder Abteilungen, die ein hohes Mass an Autonomie brauchen und/oder hohe Anforderungen an die IT-Sicherheit stellen, können in einer separaten Gesamtstruktur geführt werden.

14.5 Namenskonvention für Domänen

Da Active Directory und DNS eng miteinander verknüpft sind und die meisten Unternehmen ihr Netzwerk ans Internet anschliessen, muss eine **Namenskonvention für Domänen** gefunden und eingehalten werden. Folgende Ansätze sind denkbar:

- Sie benutzen den **registrierten Namen des Unternehmens** für das Active Directory. Dies ist nicht die beste Lösung. Der Grund liegt im DNS-Splitting, d. h., Sie konfigurieren einen DNS-Server für den internen Gebrauch und einen für den externen Gebrauch. Auf beiden werden unterschiedliche Informationen über die Domäne eingetragen. Die Verwaltung ist schwieriger und Fehler können dazu führen, dass Bereiche Ihres internen Netzwerks offengelegt werden.
- Sie verwenden eine **Subdomäne** für das Active Directory. Sie registrieren beispielsweise wondertoys.com als externe Domäne und für das Active Directory erstellen Sie eine Domäne mit dem Namen intern.wondertoys.com. Aus Sicht des DNS ist dies schon einfacher als das vorangegangene Beispiel.
- Sie verwenden **intern und extern unterschiedliche Domänen** (z. B. extern wondertoys.com und intern wondertoys.local). Bei zwei Domänennamen ist auf den ersten Blick klar, welche DNS-Einträge intern bzw. extern sind. Bei DNS extern = DNS intern ist dies wesentlich schwieriger zu verstehen und zu verwalten. Sie helfen also auf diese Art und Weise Ihren Mitarbeitenden, sich zurechtzufinden.

Egal welchen Ansatz Sie wählen, Sie müssen die Bezeichnung vor Gebrauch bei der zuständigen Behörde bzw. Organisation **registrieren** (in der Schweiz unter http://www.switch.ch). Dadurch wird garantiert, dass niemand denselben Namen benutzen kann, auch wenn zurzeit noch keine Pläne bestehen, die Domäne ans Internet anzuschliessen.

Bei der Wahl des Domänennamens müssen Sie sich zudem an die **DNS-Richtlinien** halten, die folgende **Regeln** vorsehen:

- Verwenden Sie kurze, aussagekräftige Namen, die auch den Anforderungen von NETBIOS genügen (maximal 15 Zeichen).
- Registrieren Sie den Domänennamen vor Gebrauch.
- Benutzen Sie nur die Zeichen A–Z, a–z, 0–9 und den Bindestrich (-).

14.6 Mithilfe von Organisationseinheiten strukturieren

Organisationseinheiten (OUs) sind wichtige Bestandteile einer Active-Directory-Umgebung. Wie lassen sich OUs charakterisieren und wie lässt sich die Struktur korrekt planen und umsetzen?

14.6.1 Grundlagen zu Organisationseinheiten

OUs werden oft mit Containern verglichen. Der Unterschied ist aber klar. Container sind vom System vordefinierte Ordner. Auf solche Ordner lassen sich keine GPOs[1] linken. OUs sind dagegen Erweiterungen eines Containers und dienen unter anderem dazu, GPOs darauf zu verlinken oder Verwaltungsaufgaben zu delegieren.

- Computer
- Gruppen
- Benutzer

[1] Abk. für Group Policy Object. Engl. für: Gruppenrichtlinienobjekte. Objekte für die Steuerung der Benutzerumgebung. Vergleichen Sie dazu Teil G, S. 161.

- Drucker
- Richtlinien
- Freigegebene Ordner (Shares)
- Andere
- OUs

OUs stellen ein **Verwaltungstool** dar, die dem Systemadministrator u. a. dabei helfen, die Ressourcen schnell und leicht wieder zu finden. Der Benutzer merkt nichts von den OUs, da sie in keiner Weise mit DNS zusammenhängen. OUs erfüllen aber noch weitere Zwecke wie:

- Verwaltungsaufgaben delegieren
- Objekte verstecken
- Gruppenrichtlinien gezielt implementieren

Hinweis

Die OUs, die Sie erstellen, gelten immer nur domänenweit. Sie können also nur Objekte aufnehmen, die sich tatsächlich in Ihrer Domäne befinden.

14.6.2 OU-Struktur planen

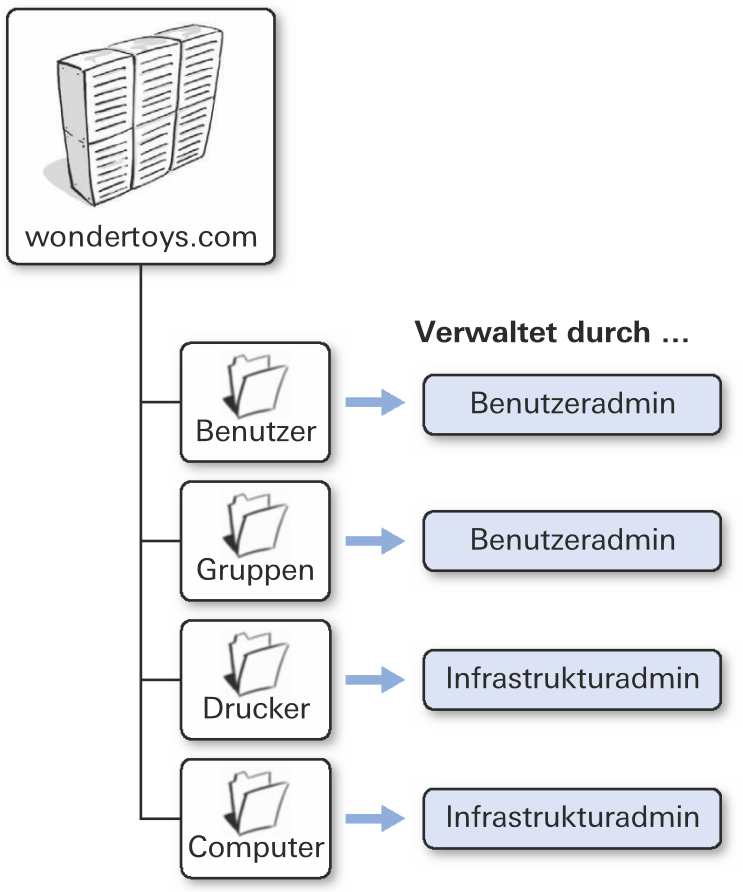
Wie schon erwähnt, sollen OUs die Verwaltung von Ressourcen erleichtern. Nehmen Sie sich also die Zeit und überlegen Sie, wer wie und wo die einzelnen Objekte verwalten soll. Anhand der entsprechenden Antworten lässt sich eine geeignete Struktur abbilden, die die Arbeitsweise in Ihrem Unternehmen widerspiegelt.

14.6.3 OUs für die Delegation von Verwaltungsaufgaben

Wenn Sie OUs für die Delegation von Verwaltungsaufgaben erstellen, können Sie zwischen einem objektbasierten Ansatz oder einem aufgabenbasierten Ansatz wählen.

Beim **objektbasierten Ansatz** ordnen Sie die Ressourcen nach Objekttyp (Mitarbeitende, Gruppen, Admins). Anschliessend weisen Sie den OUs die Gruppen bzw. Benutzerkonten zu, die für die Administration dieser Objekte zuständig sind.

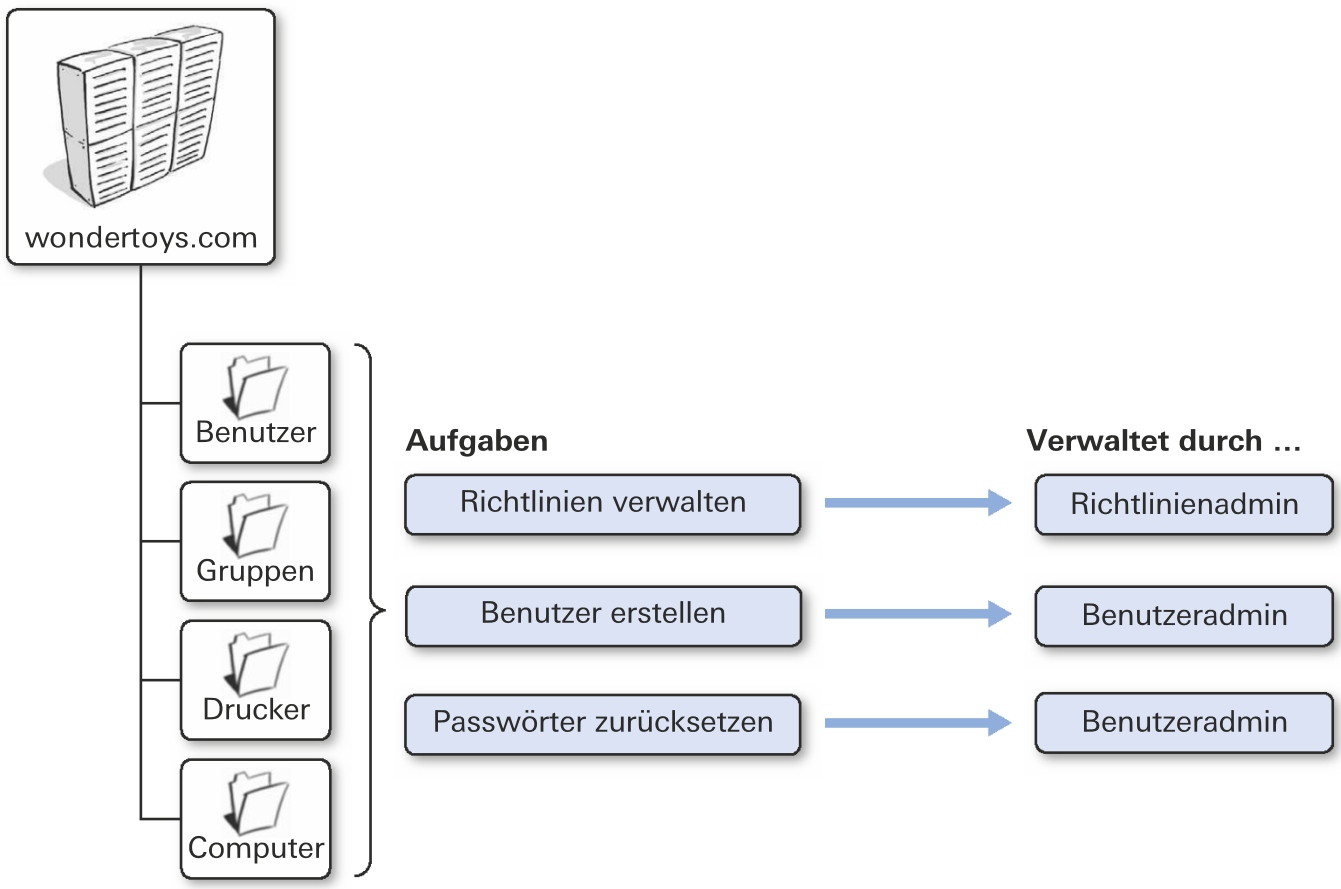
Abb. [14-3] **Objektbasierter Ansatz (Beispiel)**



In der obigen Grafik können Sie sehen, dass es unterschiedliche Administratoren in einem Netzwerk geben kann, die ihren eigenen Zuständigkeitsbereich haben. So ist der Benutzeradmin für die Benutzerkonten und die Gruppen zuständig. Der Infrastrukturadmin verwaltet die Drucker und Computer.

Beim **aufgabenbasierten Ansatz** werden unterschiedliche Aufgaben wie Benutzerkonten erstellen, Rechnerkonten löschen, Richtlinien verwalten, Passwort zurücksetzen etc. auf den einzelnen OUs definiert. Auch hier können Sie wie im Beispiel oben dieselben Objekte in der gleichen OU speichern. Dagegen ist nun nicht mehr eine Gruppe oder eine Person für die ganze Verwaltung der Objekte zuständig, sondern je nach Aufgabengebiet tut dies eine andere Person. Dabei ist zu beachten, dass auf der OU die Verwaltungsrechte entsprechend den zugewiesenen Aufgaben einzeln konfiguriert werden müssen.

Abb. [14-4] **Aufgabenbasierter Ansatz**

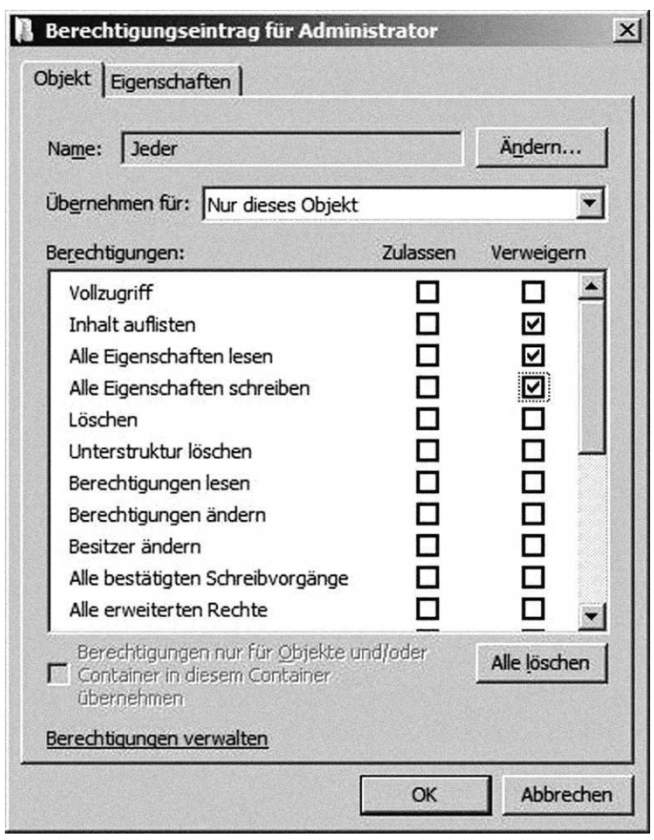


14.6.4 Objekte verstecken

Das **Verstecken von Objekten** kommt eher selten zur Anwendung. Es kann aber sein, dass Sie aus politischen, gesetzlichen oder Sicherheitsgründen dazu gezwungen sind, bestimmte Objekte im Active Directory vor Benutzergruppen zu verbergen. Erstellen Sie dazu eine OU und platzieren Sie alle Objekte darin. Passen Sie anschliessend die ACL der OU so an, dass die Benutzergruppen, die die Objekte nicht sehen dürfen, die Objekte nicht auflisten können. Dabei müssen Sie folgende Punkte beachten:

- Sie können keine Administratorenkonten verstecken. Die entsprechenden Berechtigungen werden stündlich zurückgesetzt (adminSDHolder). Dies dient dem Schutz vor Manipulationen.
- Ein explizites «Allow» überschreibt ein vererbtes «Deny». Seien Sie beim Verändern der Berechtigungen also vorsichtig.

Abb. [14-5] Objekte verstecken



Hinweis Damit die Registerkarte «Sicherheit» unter den Eigenschaften der OU erscheint, müssen Sie in der Konsole die erweiterte Ansicht aktivieren.

14.6.5 Richtlinien implementieren

Richtlinien dienen dazu, die Benutzerumgebung einzuschränken. Sie fassen mit OUs die Benutzer zusammen, die denselben Einschränkungen unterliegen sollen. Dies bedingt, dass Sie sich schon zuvor Gedanken über mögliche Gruppenrichtlinien gemacht haben.

Hinweis Gruppenrichtlinien werden entweder auf Benutzer- oder Rechnerkonten angewendet. Fassen Sie also nicht einzelne Gruppenkonten in einer OU zusammen in der Hoffnung, Sie können auf dieser dann Gruppenrichtlinien implementieren.

14.6.6 OU-Strukturansätze

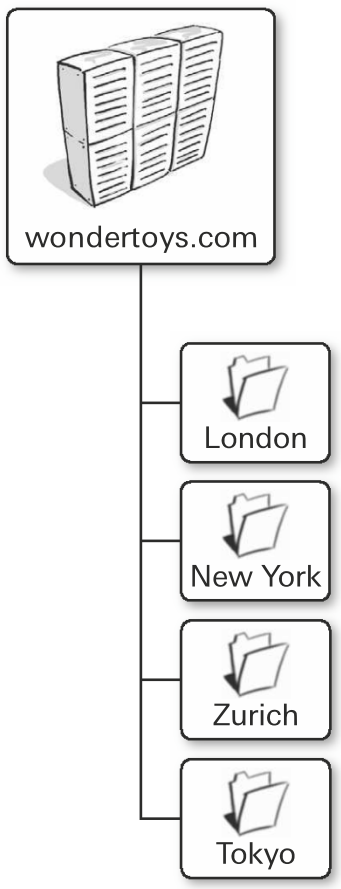
Beim Entwurf der OU-Struktur spielt die erste Ebene eine entscheidende Rolle. Diese Ebene sollte so statisch wie möglich sein, also keinen direkten Änderungen unterliegen. Hierfür gibt es vier Ansätze:

- Standortmodell
- Abteilungsmodell
- Objektmodell
- Kombination aus allem

A] Standortmodell

Beim **Standortmodell** werden OUs für alle geografischen Standorte erstellt. Die zugehörigen Objekte werden also entsprechend ihrem Standort gegliedert. Hier ein Beispiel dazu:

Abb. [14-6] Standortmodell (Beispiel)



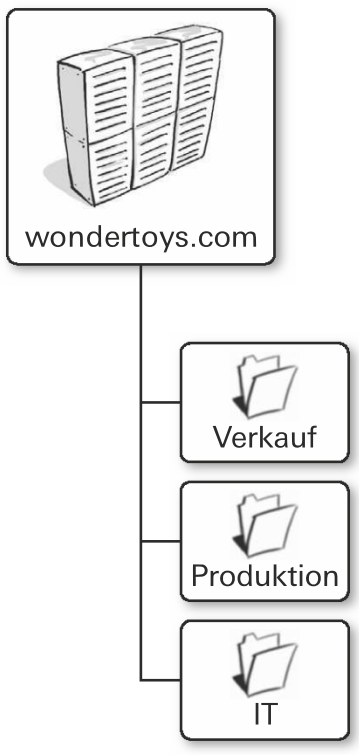
Die **Vorteile des Standortmodells** lassen sich wie folgt zusammenfassen:

- Bei der Umstrukturierung von Abteilungen bleiben die OUs erhalten.
- Standortbezogene Ressourcen werden schnell gefunden.
- Bei Fusionen oder neuen Standorten kann einfach eine zusätzliche OU angelegt werden.

B] Abteilungsmodell

Beim **Abteilungsmodell** erhält jede Abteilung gemäss Organigramm eine OU. Objekte aus diesen Abteilungen werden dann innerhalb dieser OUs verwaltet. Hier ein Beispiel dazu:

Abb. [14-7] Abteilungsmodell (Beispiel)



Die **Vorteile des Abteilungsmodells** liegen in folgenden Bereichen:

- Es erlaubt ein genaues Abbild der Unternehmensstruktur.
- Abteilungsbezogene Ressourcen werden schnell gefunden.
- Neue Abteilungen oder Zusammenschlüsse können einfach verwaltet werden.

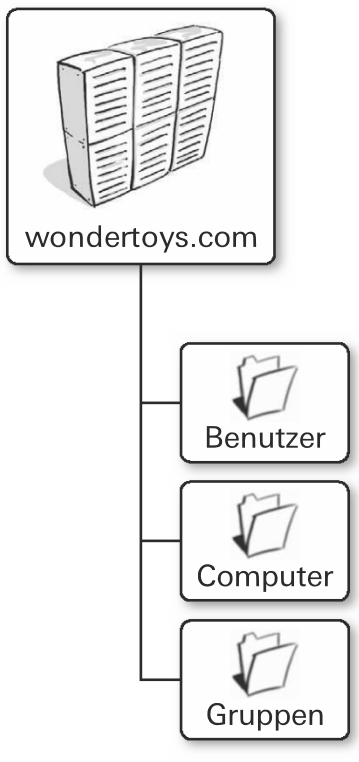
Die **Nachteile dieses Modells** lauten wie folgt:

- Es wird unübersichtlich, wenn Abteilungen auf mehrere Standorte verteilt sind.
- Die Verwaltung gestaltet sich schwierig. Dies könnte ein Problem sein, wenn Sie aus Sicht der IT dezentral organisiert sind.

C] Objektmodell

Beim **Objektmodell** werden alle Objekte des gleichen Typs in einer OU gespeichert. Hier ein Beispiel dazu:

Abb. [14-8] **Objektmodell (Beispiel)**



Die **Vorteile des Objektmodells** liegen in folgenden Bereichen:

- Es hat eine extrem flache Hierarchie.
- Fusionen oder Zusammenschlüsse haben keinen grossen Einfluss auf die OU-Struktur.

Aber auch dieses Modell hat ein paar **Nachteile:**

- Bei vielen Objekten wird das Ganze schnell unübersichtlich.
- Delegation von Verwaltungsaufgaben ist nicht mehr so einfach.
- Gruppenrichtlinien können nur noch mittels Filter gezielt angewendet werden.

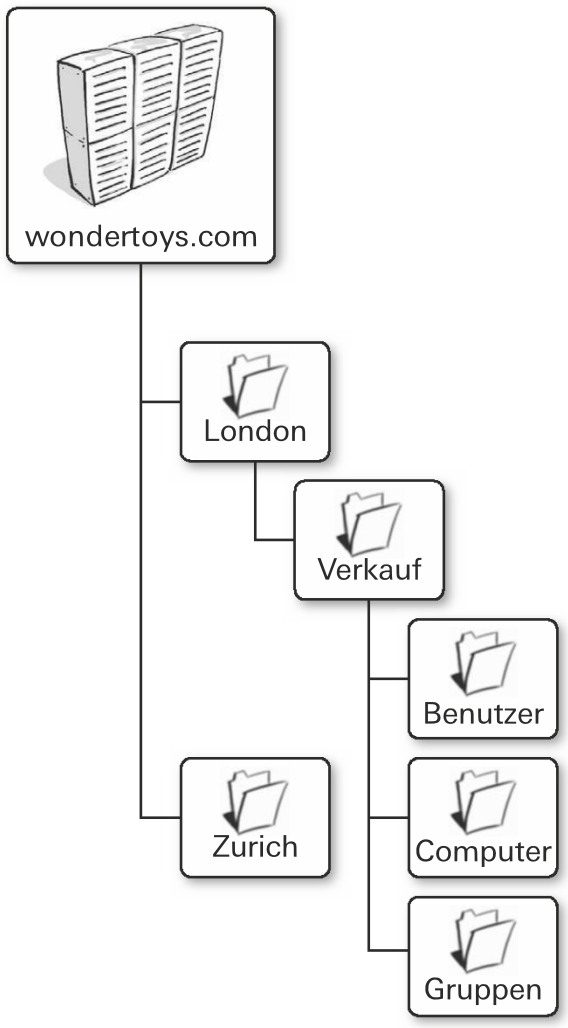
D] Kombinationsmodell

Die wohl beste Lösung ist das **Kombinationsmodell**. Dies bietet Übersichtlichkeit, Transparenz und ein Höchstmass an Flexibilität. In der Praxis werden beim OU-Design folgende Ansätze miteinander kombiniert:

- Verwaltungsaufgaben delegieren
- Objekte auffinden
- Gruppenrichtlinien gezielt implementieren

Zunächst wird für jeden Ansatz unabhängig von den anderen Ansätzen ein optimales OU-Modell entworfen. Danach werden diese sinnvoll kombiniert. Dies zeigt sich meist in einer Struktur, wie Sie in der folgenden Abbildung sehen können:

Abb. [14-9] **Kombinationsmodell**



Zusammenfassung

In **Active Directory** werden Netzwerkressourcen wie Benutzer, Gruppen, Drucker, Richtlinien usw. gespeichert und verwaltet. Der **Domänenkontroller** bildet damit das Herzstück einer Domäne und stellt die zugehörigen Informationen in der **Active-Directory-Datenbank** bereit. Bei der Planung von Active Directory gilt der Grundsatz: So einfach als möglich. Also zuerst immer nur eine Domäne in Betracht ziehen und nur in Ausnahmefällen auf mehrere Domänen, Strukturen oder Gesamtstrukturen ausweichen.

Organisationseinheiten (OUs) vereinfachen dem Administrator die Systemverwaltung, indem sie das Auffinden der Netzwerkressourcen vereinfachen. Darüber hinaus erfüllen OUs folgende Zwecke:

- Verwaltungsaufgaben delegieren
- Objekte verstecken
- Gruppenrichtlinien gezielt implementieren

Beim **Entwurf der OU-Struktur** spielt die erste Ebene eine entscheidende Rolle. Diese Ebene sollte so statisch als möglich sein, also keine direkten Änderungen ermöglichen. Folgende Ansätze werden beim Strukturentwurf unterschieden:

- Standortmodell
- Abteilungsmodell
- Objektmodell
- Kombination aus allem

In der Praxis hat sich das **Kombinationsmodell** bewährt. Dabei werden sowohl die Standorte als auch die Abteilungen und Objekte berücksichtigt.

Aufgaben

40	Welche AD-Struktur sollten Sie bei mehreren Domänen wählen: eine Struktur nach Ländern oder nach Abteilungen? Begründen Sie Ihre Antwort.
41	Nennen Sie zwei Gründe für die Implementierung mehrerer Domänen.
42	Worauf können zwei oder mehr Gesamtstrukturen zurückzuführen sein?

15 Active Directory installieren und konfigurieren

Lernziele

Nach der Bearbeitung dieses Kapitels können Sie …

- die Konfigurationsaspekte eines Corporate Directory darlegen und deren Auswirkungen auf die Funktionalität beispielhaft aufzeigen.
- die grundlegenden Schritte bei einer Einführung eines Directory Service und deren Beitrag zu einem funktionsfähigen System aufzeigen.
- die unterschiedlichen Domänen-Funktionsebenen von Active Directory erklären.
- erläutern, welche Anpassungen nach der Installation von Active Directory bei einem DNS-Server notwendig sind.

Schlüsselbegriffe

AD-Datenbank, DCPROMO.EXE, DDNS, Domänen-Funktionsebene, DSRM-Passwort, Gesamtstruktur-Funktionsebene, Protokolldateien, SYSVOL-Verzeichnis, Domänenkontroller

15.1 Voraussetzungen für die Installation

Für die Installation von Active Directory müssen folgende **technische Voraussetzungen** erfüllt sein:

- DNS-Infrastruktur
- TCP/IP-Protokoll mit einer fixen IP-Adresse
- NTFS-Dateisystem
- Administratorrechte auf dem Server
- Genügend Platz auf der Festplatte:
  - 15 MB freier Speicherplatz auf der Partition für die Systeminstallation
  - 250 MB freier Speicherplatz für die Active-Directory-Datenbank **(NTDS.DIT)**
  - 50 MB freier Speicherplatz für die ESENT-Protokolldateien. Bei ESENT (Extensible Storage Engine Transaction) handelt es sich um ein transaktives Datenbanksystem, das anhand von Protokolldateien die Rollbacksemantik unterstützt, um das Übernehmen von Transaktionen in die Datenbank sicherzustellen

15.2 Der erste Domänenkontroller

Aus Gründen der Sicherheit installieren Sie immer mindestens **zwei Domänenkontroller.** Das Vorgehen bei der Installation des ersten DC wird im Folgenden separat erläutert, weil es sich vom Vorgehen für die weiteren Domänenkontroller unterscheidet.

15.2.1 Installation starten und erste Schritte durchführen

Mit dem Befehl **DCPROMO.EXE** starten Sie den Installationsassistenten, um Ihre Domäne und den darin enthaltenen Domänenkontroller zu konfigurieren. Die Installation wird grafisch unterstützt und jeder Schritt genauestens beschrieben. Ein häufiger Fehler liegt darin, dass Informationen am falschen Ort ein- bzw. angegeben werden.

Wichtig ist, dass Sie dem Installationsassistenten zu Beginn mitteilen, dass es sich um eine neue Domäne in einer neuen Gesamtstruktur (Forest) handelt. Damit steuern Sie, welche Angaben als Nächstes gemacht werden müssen.

Zuerst geben Sie den FQDN für Ihre Domäne an. Dabei handelt es sich um die Angabe der Domäne ohne Host-Bezeichnung (z. B. sbb.ch oder meinefirma.com). Wenn Sie zuvor eine entsprechende Zone im DNS für Ihre Domäne erstellt haben, müssen Sie darauf achten, den Domänennamen ohne Schreibfehler zu übernehmen.

15.2.2 Funktionsebenen und ihre Bedeutung

Während der Installation der Domäne bzw. des Domänenkontrollers müssen Sie auch die **Funktionsebene** angeben. Dadurch wird sichergestellt, dass auch ältere Domänenkontroller (z. B. solche unter Windows Server 2003 oder Windows 2000) miteinander kommunizieren und die zusätzlichen Funktionen und Verbesserungen genutzt werden können.

Bei den Funktionsebenen wird zwischen Gesamtstruktur und Domäne differenziert. Folgende Tabelle gibt Auskunft über **Gesamtstruktur-Funktionsebenen** und ihre Unterschiede:

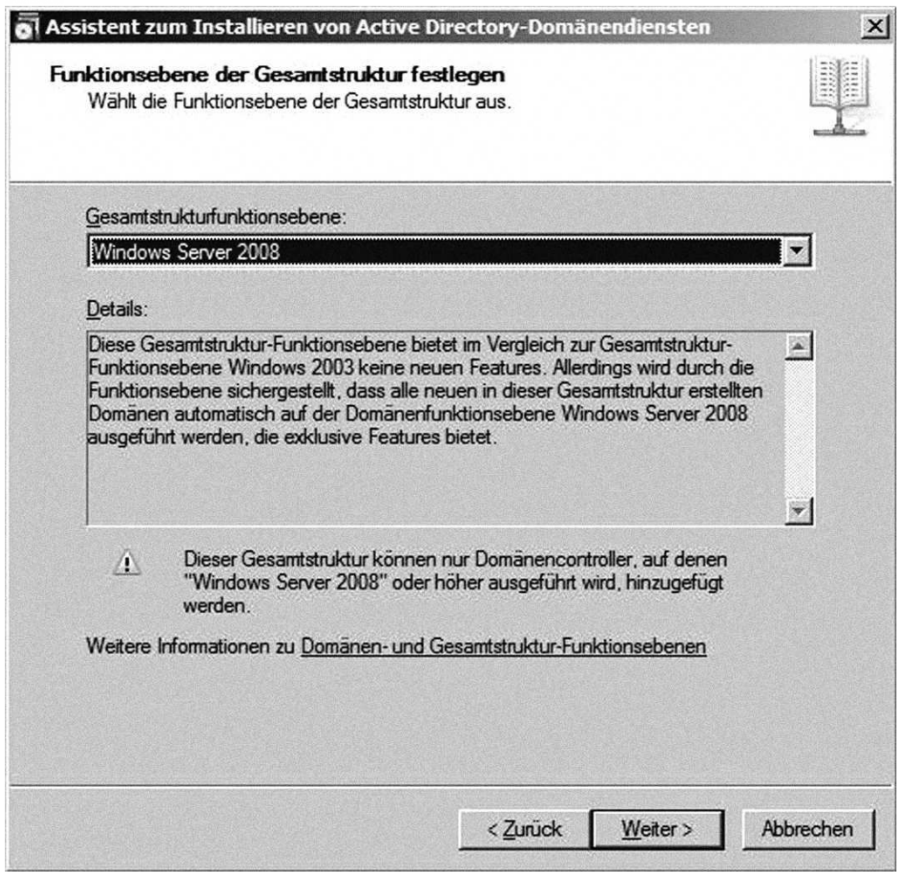
Gesamtstruktur-Funktionsebene	Verfügbare Funktionen	Unterstützte Domänenkontroller
Windows 2000 einheitlich	Es stehen alle standardmässigen Active-Directory-Funktionen zur Verfügung.	• Windows Server 2008 • Windows Server 2003 • Windows 2000
Windows Server 2003	Es stehen alle standardmässigen Active-Directory-Funktionen zur Verfügung plus die folgenden Erweiterungen, welche mit Windows Server 2003 eingeführt wurden: • Gesamtstrukturvertrauensstellungen • Domänenumbenennung • Replikation verknüpfter Werte • Bereitstellung schreibgeschützter Domänenkontroller • Verbesserte KCC-Algorithmen (Knowledge Consistency Checker) • Deaktivierung und Neudefinition von Attributen und Klassen im Schema	• Windows Server 2008 • Windows Server 2003
Windows Server 2008	Es stehen alle für die Windows-Server-2003-Gesamtstruktur-Funktionsebene verfügbaren Funktionen zur Verfügung, jedoch keine zusätzlichen. Alle Domänen, die zur Gesamtstruktur hinzugefügt werden, werden automatisch mit der Domänen-Funktionsebene Windows Server 2008 ausgeführt.	• Windows Server 2008

Hinweis

Auf eine ausführliche Beschreibung der Funktionen wird in diesem Lehrmittel verzichtet. Nähere Informationen finden Sie bei Bedarf auf dem Microsoft Technet. Vergleichen Sie dazu das Linkverzeichnis im Anhang, S. 228.

Im folgenden Bild sehen Sie, wie Sie die Funktionsebenen unter Windows Server 2008 R2 konfigurieren können:

Abb. [15-1] Funktionsebene der Gesamtstruktur festlegen



Die Gesamtstruktur-Funktionsebene ist von der **Domänen-Funktionsebene** abhängig. Eine grundlegende Voraussetzung für eine Gesamtstruktur-Funktionsebene Windows Server 2008 besteht darin, dass alle darin enthaltenen Domänen ebenfalls auf der Windows-Server-2008-Funktionsebene betrieben werden.

Folgende Tabelle gibt Auskunft über verschiedene Domänen-Funktionsebenen und deren Unterschiede:

Domänen-Funktionsebene	Verfügbare Funktionen	Unterstützte Domänenkontroller
Windows 2000 einheitlich	Es stehen alle standardmässigen AD-Funktionen zur Verfügung wie: • Universelle Gruppen für Verteiler- und Sicherheitsgruppen • Gruppenverschachtelungen • Gruppenkonvertierung, wodurch eine Konvertierung zwischen Sicherheits- und Verteilergruppen ermöglicht wird • SID[1]-Verlauf	• Windows Server 2008 • Windows Server 2003 • Windows 2000
Windows Server 2003	Es stehen alle standardmässigen AD-Funktionen zur Verfügung, die die Domänen-Funktionsebene Windows 2000 einheitlich bietet, ergänzt durch die Erweiterungen durch Windows Server 2003: • Domänen mit dem Befehl `netdom.exe` umbenennen • Anmeldezeitstempel aktualisieren • Eingeschränkte Delegierung • Ausgewählte Authentifizierung	• Windows Server 2008 • Windows Server 2003
Windows Server 2008	Es stehen alle zuvor erwähnten Funktionen zur Verfügung, erweitert durch Funktionen von Windows Server 2008: • Unterstützung der DFS-Replikation (Distributed File System) für das Windows-Server-2003-Systemvolume (SYSVOL) • Die DFS-Replikation bietet eine stabilere AES-128- und AES-256-Unterstützung (Advanced Encryption Standard) für das Kerberos-Protokoll • Information zur letzten interaktiven Anmeldung • Fein abgestimmte Kennwortrichtlinien	• Windows Server 2008

[1] Abk. für: Security Identifier. Weil das System Zahlen besser versteht, erhält jedes Objekt (neben dem vom Administrator festgelegten Namen) eine eindeutige, automatisch generierte, 32-stellige Zahl.

Hinweis

Weiterführende Informationen zu diesen Funktionen finden Sie bei Bedarf auf dem Microsoft Technet. Vergleichen Sie dazu das Linkverzeichnis, S. 228.

Was bedeutet das für Sie? Wenn Sie «auf der grünen Wiese» eine neue Domäne aufbauen, müssen Sie sich über die Funktionsebenen keine grossen Gedanken machen, sondern nehmen einfach die höchstmögliche (also Windows Server 2008). Wenn Sie aber in einem grösseren Unternehmen bzw. Netzwerksystem mit mehreren Domänen und unzähligen Domänenkontrollern mit unterschiedlichen Betriebssystemen arbeiten, müssen Sie über die Kombinationsmöglichkeiten und deren Auswirkungen auf das Gesamtsystem Bescheid wissen. Es kann fatale Folgen haben, wenn Sie die Funktionsebene der Domäne oder der Gesamtstruktur in einer Liveumgebung ändern, bevor alle Domänenkontroller auf die gewünschte Version aktualisiert worden sind. Dies kann zur Folge haben, dass die Replikation von Benutzerinformationen oder anderen wichtigen Objekten innerhalb von Active Directory nicht mehr gewährleistet ist und Mitarbeitende sich zum Beispiel nicht mehr anmelden oder auf ihre Dokumente zugreifen können.

Hinweis

- Die Änderung von Funktionsebenen ist ein Vorgang, der nicht mehr rückgängig gemacht werden kann. Bei falscher Anwendung müssen die Gesamtstruktur oder einzelne Domänen neu aufgebaut werden.
- Machen Sie sich auch mit den oben erwähnten Funktionen der unterschiedlichen Funktionsebenen vertraut. Diese geben Ihnen unter Umständen wichtige Argumentationspunkte, wenn es darum geht, eine bestehende Umgebung auf eine neue Betriebssystemversion zu aktualisieren.

15.2.3 Datenspeicherorte

Während der Installation werden Sie zur Angabe eines Speicherorts für die Active-Directory-Datenbank **NTDS.DIT,** für die Protokolldateien und für das **SYSVOL-Verzeichnis** gebeten. Der Assistent schlägt Ihnen vor, alle Daten in den System-Ordner **\windows** zu speichern. Dies empfiehlt sich nur bei kleinen Active-Directory-Installationen mit einem Standort, einer Domäne und weniger als 1000 Objekten. Da Sie zum Zeitpunkt der Erstellung von Active Directory nur schwer abschätzen können, wie sich Ihr Unternehmen in den nächsten fünf Jahren entwickeln wird, ist es von Vorteil, die Daten auf einer getrennten Partition unterzubringen. Damit ersparen Sie sich ein späteres manuelles Verschieben der Daten. Ein weiterer Vorteil liegt in der besseren Performance. Die Daten liegen auf einer Partition, auf die neben dem Active-Directory-Dienst keine weiteren Dienste zugreifen werden. Dadurch finden keine zusätzlichen Lese- und Schreibzugriffe statt.

15.2.4 Installation abschliessen

Ein wichtiger Punkt, der gerne unterschätzt wird, ist die Angabe des **DSRM[1]-Passworts**. Dieses Passwort hat nichts mit dem Domänenpasswort des Administrators zu tun. Es handelt sich dabei um das Passwort, das benötigt wird, wenn Sie den Server über die erweiterten Bootfunktionen in den Active-Directory-Wiederherstellungsmodus (DSRM) booten. Denn nur so kann im Notfall das Active-Directory mithilfe einer Sicherung wiederhergestellt werden. Notieren Sie sich dieses Passwort gut und bewahren Sie es an einem sicheren Ort auf.

Hinweis

Sollten Sie dennoch mal das Wiederherstellungspasswort vergessen haben, können Sie es mithilfe von **NTDSUTIL.EXE** wieder zurücksetzen. Machen Sie dies aber, noch bevor der Server ein Problem verursacht und wiederhergestellt werden muss.

[1] Abk. für: Directory Service Restore Mode.

Nachdem Sie alle Angaben gemacht haben, wird Active Directory installiert. Dies dauert ca. 5 bis 15 Minuten (je nach Hardware). Das heisst, die Ordnerstruktur ist angelegt, die Datenbank mit dem Schema erstellt und die Verwaltungstools sind bereitgestellt. Nach Abschluss der Installation ist ein Neustart erforderlich. Und erschrecken Sie nicht, denn der erste Neustart des DC dauert in der Regel immer etwas länger.

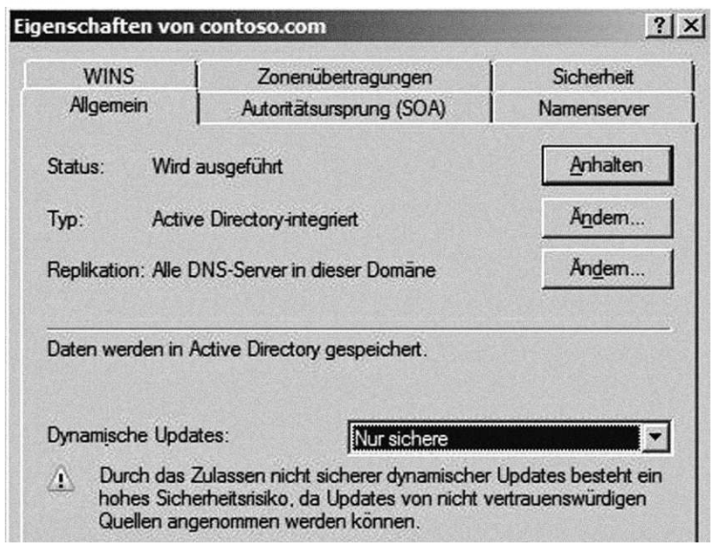
15.2.5 DNS anpassen

Nach der erfolgreichen Installation von Active Directory können Sie Ihre DNS-Konfiguration noch optimieren. Denn jetzt ist es an der Zeit, die Zonen, die noch als primäre und sekundäre aufgesetzt sind, in Active-Directory-integrierte zu konvertieren. Sie können die Zonen auf einem DNS-Server im laufenden Betrieb ändern. Ein Neustart des Servers ist nicht notwendig. Das folgende Bild zeigt, wie Sie den **Zonentyp auf dem DNS-Server** unter Windows Server 2008 R2 anpassen können:

Abb. [15-2] **Zonentyp auf dem DNS-Server ändern**

Achten Sie darauf, **DDNS** so anzupassen, dass nur sichere Updates möglich sind. Im folgenden Bild sehen Sie, wie Sie den DDNS unter Windows Server 2008 R2 anpassen können:

Abb. [15-3] **DDNS anpassen**



Hinweis

Führen Sie diese Schritte erst aus, nachdem Sie den Domänenkontroller auf korrektes Funktionieren hin überprüft haben. Details, wie Sie die Installation überprüfen können, finden Sie im Kapitel 8, S. 60.

15.3 Weitere Domänenkontroller, Domänen und Strukturen installieren

Sie können mit **DCPROMO.EXE** jederzeit weitere Domänenkontroller hinzufügen, neue Domänen erstellen oder gleich eine neue Struktur. Wählen Sie dazu einfach die entsprechende Option im Installationsassistenten. Wenn Sie weitere DCs installieren, denken Sie daran, die TCP/IP-Eigenschaften so einzustellen, dass der Server, welcher zum DC heraufgestuft wird, auf einen bereits laufenden DNS-Server zurückgreifen kann. Nach der Installation können Sie auch auf dem zweiten Server den DNS installieren. Passen Sie die TCP/IP-Eigenschaften danach wieder an, damit der Server sich selber als DNS benutzt.

Zusammenfassung

Der **Installationsassistent von Active Directory** ist das wichtigste Werkzeug für die Installation dieses Verzeichnisdienstes. Gestartet wird er über den Befehl **DCPROMO.EXE.** Dieser Befehl wird sowohl für die Erstellung der ersten Domäne mit Domänenkontroller als auch für das Hinzufügen weiterer Domänen, Strukturen oder Domänenkontrollern verwendet. Er wird auch benötigt, um einen bestehenden DC von seinen Aufgaben zu entbinden und ihn wieder zu einem «normalen» Mitgliedsserver der Domäne zu machen.

Während der AD-Installation gibt es folgende **Aufgaben** zu erledigen:

- Die **Gesamtstruktur-Funktionsebene** und die **Domänen-Funktionsebene** müssen festgelegt werden. Damit wird sichergestellt, dass auch ältere (bereits bestehende Domänenkontroller) mit den neuen DCs richtig funktionieren. Die DC-Ebenen unterscheiden sich nicht nur in den unterstützten Windows-Server-Versionen, sondern auch in zusätzlichen Funktionen, welche das AD zur Verfügung stellen kann. Dabei gilt: Je höher die Version, desto mehr nützliche Funktionen können verwendet werden.
- Die **Datenspeicherorte für die AD-Datenbank, Replikationslogs und Sysvol-Ordner** sind von der Systempartition **C:\windows** auf eine andere Partition zu verschieben. Dies wirkt sich positiv auf die Performance aus und die Speicherorte müssen später nicht wieder verschoben werden.
- Das Wiederherstellungspasswort muss festgelegt werden. Dieses wird benötigt, um sich am Server im sogenannten Directory Service Restore Mode anzumelden. Dabei handelt es sich um einen Status, um das Active Directory im Fehlerfall wiederherstellen zu können.

Nach erfolgreicher Installation können Sie die **DNS-Einstellungen optimieren,** um auch hier von den Vorteilen von Active Directory zu profitieren.

Aufgaben

43	Sie verfügen über eine Domäne mit einem DC basierend auf Windows Server 2003. Welche Gesamtstruktur-Funktionsebene und welche Domänen-Funktionsebene sind aktuell? Wenn Sie nun eine weitere Domäne mit einem Windows Server 2008 DC hinzufügen; welche Funktionsebene wählen Sie für die neue Domäne?
44	Um Active Directory wiederherstellen zu können, brauchen Sie ein eigenes Passwort. Dieses Passwort wird im DSRM abgefragt. Wie starten Sie den Server in diesem Modus?
45	Warum ändern Sie die DNS-Konfiguration auf «Nur sichere, dynamische Updates zulassen»?

16 Active-Directory-Installation testen und Probleme aufdecken

Lernziele

Nach der Bearbeitung dieses Kapitels können Sie …

- die Ereignisanzeige in Bezug auf Probleme mit der Replikation richtig interpretieren.
- die Möglichkeiten zum Testen der Replikation von Active Directory aufzeigen.
- die Managementkonsole für den Zugriff auf das Active-Directory-Schema einrichten.

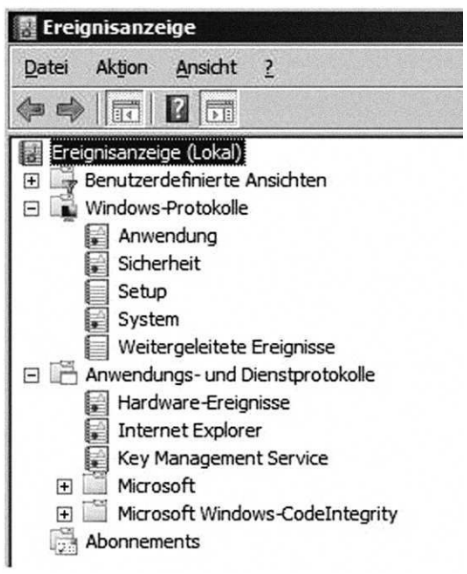
Schlüsselbegriffe

DCdiag, Ereignisanzeige, Netdiag, Replikationsdienst, Schema, SRV-Einträge

16.1 Ereignisanzeige

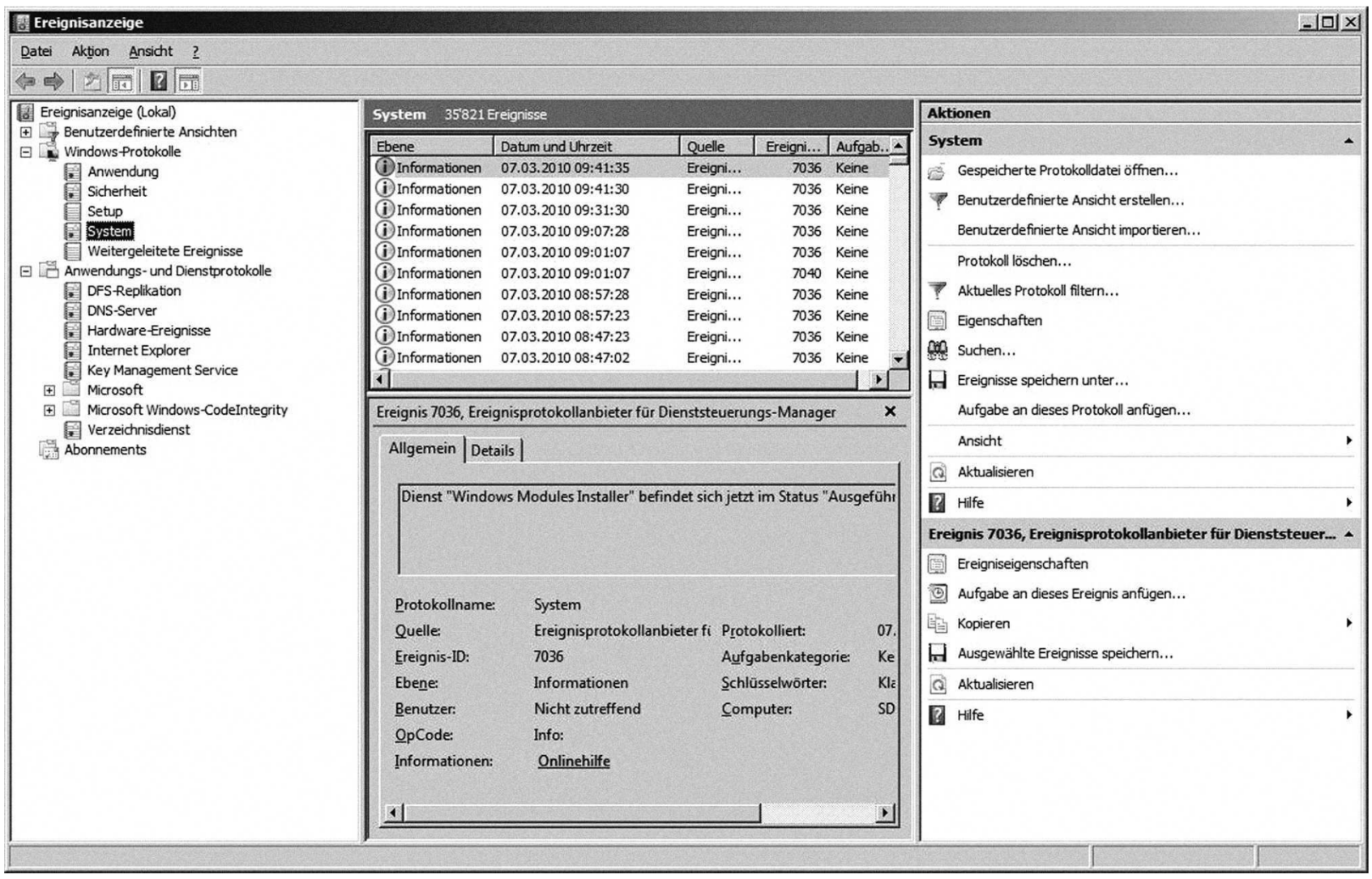
Mit der Installation des Active Directory wird die **Ereignisanzeige** um wichtige Informationen erweitert, die den Replikationsdienst, den DNS und die Verzeichnisdienste betreffen. Das folgende Bild zeigt die Ereignisanzeige unter Windows Server 2008 R2 vor der AD-Installation:

Abb. [16-1] Ereignisanzeige vor der Installation des Active Directory



Und so sieht die Ereignisanzeige unter Windows Server 2008 R2 nach der AD-Installation aus:

Abb. [16-2] Ereignisanzeige nach der Installation des Active Directory



Kontrollieren Sie alle Bereiche auf Fehler in Bezug auf den DNS oder das Active Directory. Wenn Sie nur einen Domänenkontroller betreiben, können Sie den Bereich **Dateireplikationsdienst** vernachlässigen.

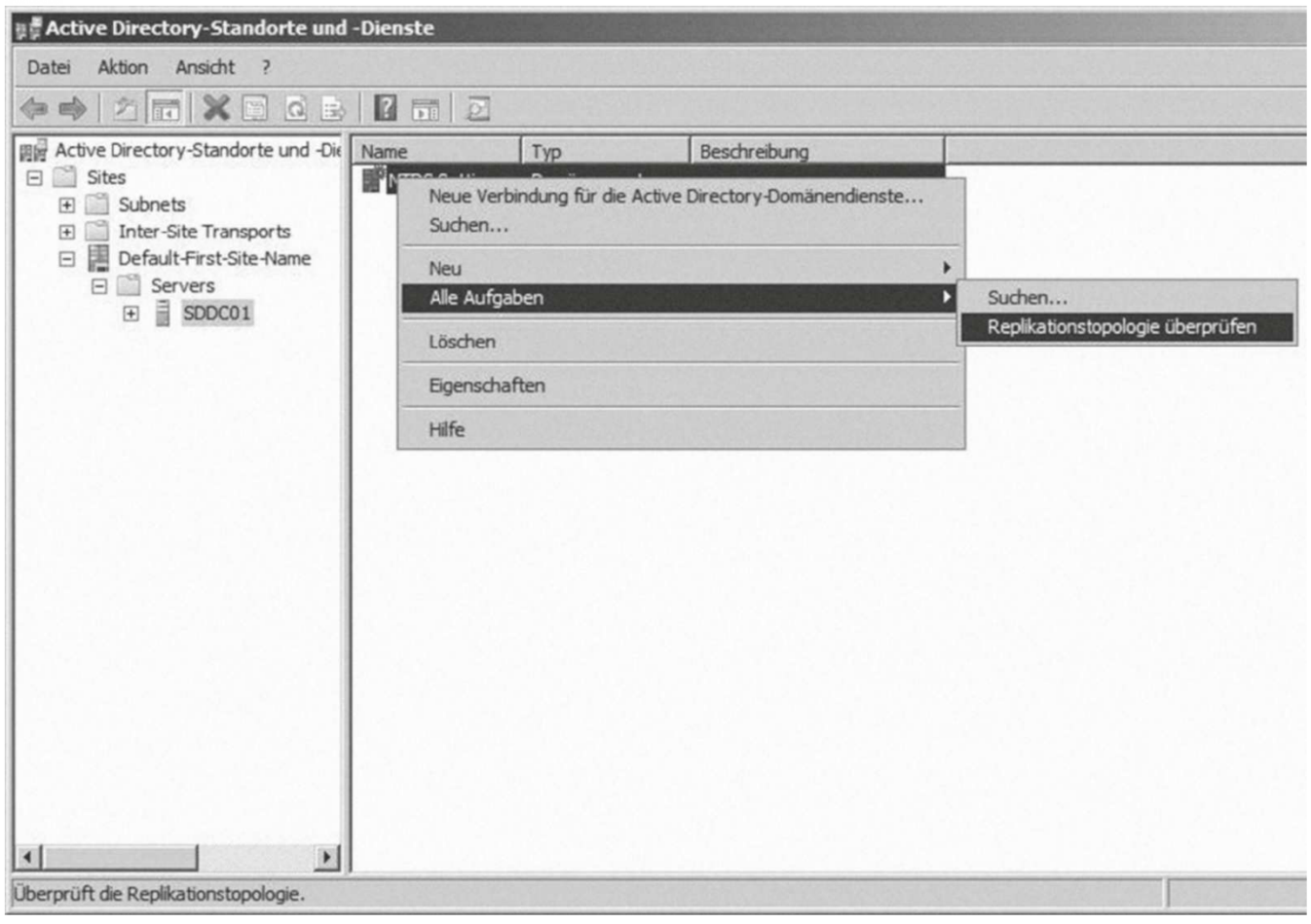
Hinweis

Wenn Sie mehrere Domänenkontroller betreiben, halten Sie Ausschau nach einem Fehler mit der Event ID: 1265. Tritt dieses Ereignis auf, hat Ihr Active Directory ein schwerwiegendes Problem. Dieser Fehler sagt aus, dass die Replikation der Domänenkontroller nicht mehr funktioniert. Dieses Verhalten ist häufig auf ein DNS-Problem zurückzuführen.

16.2 Replikation testen

Wenn Sie mindestens zwei Domänenkontroller haben, können Sie versuchen, eine manuelle Replikation auszulösen. Wenn dies klappt, haben Sie ebenfalls Gewissheit, dass beide DCs gut funktionieren. Verwenden Sie hierfür am besten die Verwaltungskonsole «Active Directory Standorte und Dienste». Im folgenden Bildschirmfenster sehen Sie die entsprechende Funktion zur Überprüfung der Replikation:

Abb. [16-3] Replikation testen



Bevor Sie die Replikation testen, sollten Sie den Servern mindestens 15 Minuten Zeit geben, um sich einzurichten. Die **Replikationstopologie** muss zuerst durch einen internen Dienst erstellt werden. Dies dauert zu Beginn seine Zeit. Sollte Replikation dennoch fehlschlagen, starten Sie den ganzen Domänenkontroller neu und kontrollieren Sie anschliessend die Ereignisanzeige. Meist liegt das Problem beim DNS, also der Namensauflösung. Stellen Sie sicher, dass alle Server über den FQDN erreichbar sind. Sie können auch das Tool **REPLMON** zu Hilfe nehmen. Dieses Tool zeigt zudem, ob alle FSMO-Rollen korrekt funktionieren.

16.3 NETDIAG.EXE und DCDIAG.EXE

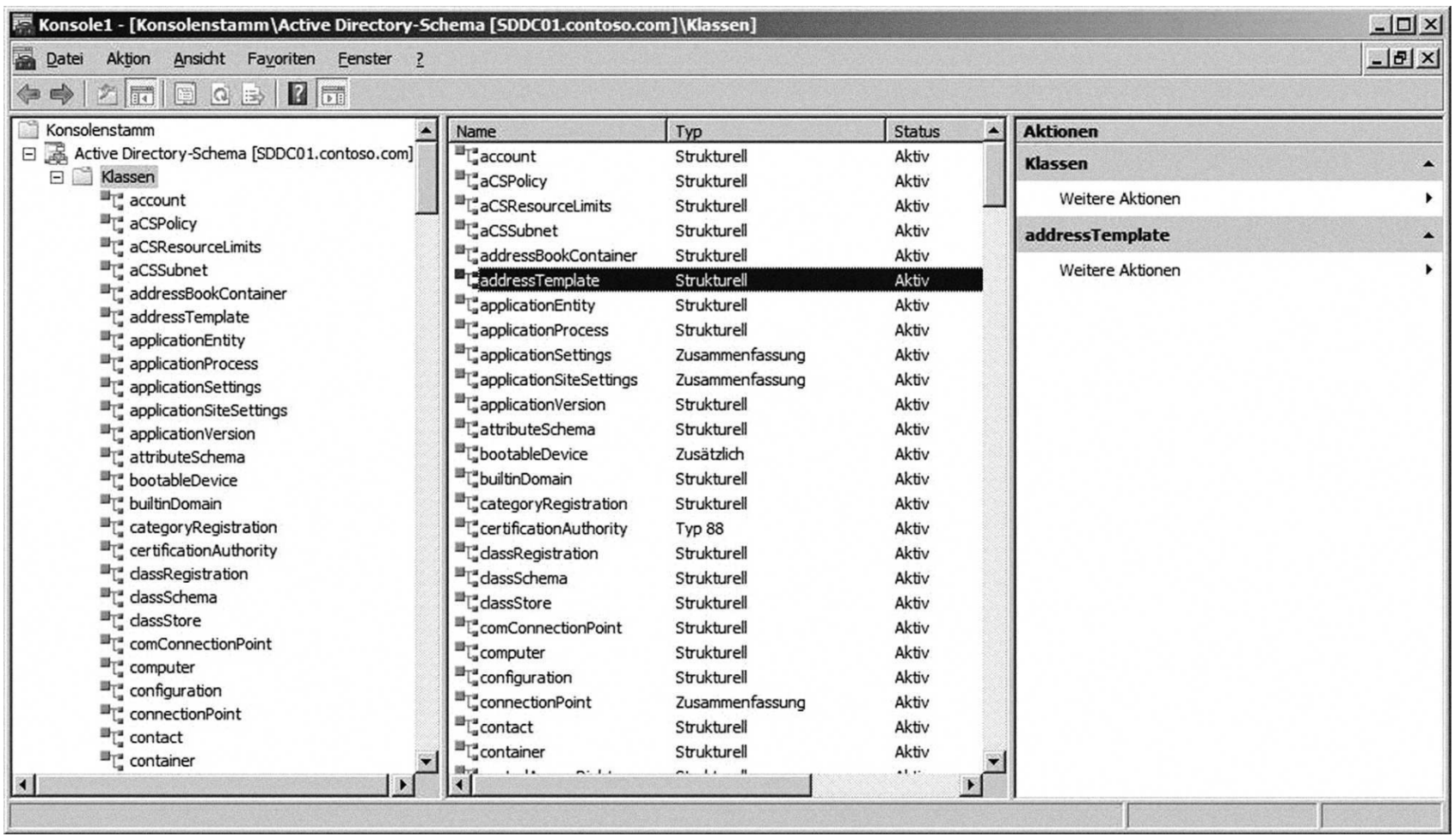
Sofern Sie die Support-Tools installiert haben, können Sie mit **NETDIAG.EXE** und **DCDIAG.EXE** den DC auf etwaige Fehler untersuchen. Kleinere Probleme können Sie mit der entsprechenden Option auch gleich beheben lassen.

16.4 Zugriff auf das Schema

Mit der **Schema-Verwaltungskonsole** von Microsoft haben Sie eine weitere Möglichkeit, um zu testen, ob Active Directory ordnungsgemäss installiert ist. Diese Konsole müssen Sie zuerst mit dem Befehl `regsvr32.exe schmmgmt.dll` installieren. Danach erhalten Sie ein weiteres **Snap-in**[1] für die Managementkonsole. Mit diesem Verwaltungstool erhalten Sie Zugriff auf das Schema, das in der Active-Directory-Datenbank hinterlegt ist. Wenn Sie einzelne Objektklassen sehen und die Attribute aufrufen können, können Sie davon ausgehen, dass Active Directory richtig funktioniert. Zudem haben Sie mit diesem Verwaltungstool die Möglichkeit, den Aufbau der einzelnen AD-Objekte zu studieren. Hier die entsprechende Bildschirmmaske dazu:

[1] Engl. für: Auf-/Eingestecktes. Erweiterung der Managementkonsole zur Verwaltung unterschiedlicher Dienste auf einem Server. Pro Dienst gibt es ein eigenes Snap-in.

Abb. [16-4] Schemaverwaltungskonsole



16.5 SRV-Einträge im DNS-Server prüfen

Nach einer erfolgreichen Active-Directory-Installation finden sich in der korrespondierenden DNS-Zone alle notwendigen SRV-Einträge. Sie erkennen diese am führenden Unterstrich (_). Über diese Einträge werden die DCs mit den Active-Directory-Diensten lokalisiert.

Zusammenfassung

Die korrekte Installation und Konfiguration von Active Directory kann mit ein paar einfachen Tools schnell und sicher überprüft werden. Als Erstes sollte die **Ereignisanzeige** in den Bereichen Active Directory, Replikation und DNS auf Fehler oder Warnungen überprüft werden.

Wird nichts Aussergewöhnliches festgestellt, ist die **Replikation** mithilfe der Befehle `replmon.exe` und `dcdiag.exe` zu testen. Die **Netzwerkeinstellungen** des Domänenkontrollers werden mit dem Befehl `netdiag.exe` kontrolliert.

Der Zugriff auf das **Schema** und die darin enthaltenen Objekte kann aufzeigen, dass die AD-Installation erfolgreich war. Es schadet auch nichts, sich die **DNS-Zone der Domäne** genauer anzusehen. Darin sollten die **Service Records** ersichtlich sein, die am vorangestellten Unterstrich (_) erkennbar sind.

Aufgaben

46	Welches ist der häufigste Grund für eine fehlerhafte Replikation?
47	Wie lautet der Befehl, um alle Domänenkontroller in einem Unternehmen zu testen und die erweiterten Informationen der Tests in der Datei **DCTEST.TXT** zu speichern?
48	Beschreiben Sie einen möglichen Lösungsweg für Replikationsprobleme zwischen DCs.