VWA Diplomarbeit

**Vorteile einer Microsoft®
Active Directory Implementierung
im globalen Unternehmen**

von

Stefan Schmidt

Diese Diplomarbeit wurde mit 1,0 bewertet.

*Die Adresse im Deckblatt habe ich abgeändert.

Diese Seite ist nicht Bestandteil der Diplomarbeit!

Verwaltungs- und Wirtschafts-Akademie

Studiengang zum Betriebswirt (VWA)

Vorteile einer Microsoft® Active Directory Implementierung im globalen Unternehmen

Betreuer: Dr. Jürgen Bartnick

Stefan Schmidt
Einestrasse 99*

12345 Eindorf*

Abgabetermin: 15. Dezember 2005

Inhalt

Abkürzungsverzeichnis

Abb.	Abbildung
AD	(Windows) Active Directory
BDC	Backup Domain Controller
DC	Domain Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
dt.	Deutsch
etc.	et cetera
engl.	Englisch
evtl.	eventuell
FR	Frame Relay Protocol
FSMO	Flexible Single Master Operation
GC	Global Catalogue
GPO	Group Policy, Group Policy Object
i.d.R.	in der Regel
IT	Informationstechnologie, auch IT-Abteilung
LDAP	Lightweight Directory Access Protocol
MS	Microsoft
NT	New Technology (Windows Betriebssystem)
o.ä.	oder ähnlich
OU	Organizational Unit
PDC	Primary Domain Controller
RID	Relative Identifier
SID	Security Identifier
SSL	Secure Sockets Layer
s.u.	siehe unten
TCP/IP	Transmission Control Protocol / Internet Protocol
u.A.	unter Anderem
UDP	User Datagram Protocol
u.U.	unter Umständen
usw.	und so weiter
u.v.m.	und vieles mehr
vgl.	vergleiche
VPN	Virtual Private Network
z.B.	zum Beispiel

Begriffe:

Im IT Bereich stammen die meisten Begriffe aus dem Englischen. Nicht immer gibt es eine sinnvolle deutsche Übersetzung oder das Wort wurde eingedeutscht (z.B. „downloaden“). Im nachfolgenden Dokument werden englische und deutsche Begriffe deshalb substitutiv verwendet.

Abbildungs- und Tabellenverzeichnis

Einleitung

Globale Unternehmen benötigen Informationsnetzwerke, die den Zugriff auf beliebige Daten an beliebigen Orten im Unternehmen gewährleisten. Fortschreitende Globalisierung hat meist auch größere Dezentralisierung der Datenbestände (Geschäftsdatenbanken, Informationsdatenbanken, Dateien, Emails, etc.) zur Folge, da diese meist regional verteilt vorliegen und nur mit erheblichem Aufwand zentral gehalten und verwaltet werden könnten. Die Konzeption, Administration und Weiterentwicklung solcher Informationsnetzwerke ist deshalb eine der zentralen Aufgaben der IT-Abteilung.

Die nachfolgende Studie basiert auf einem realen Projekt, durchgeführt in einem mittelständischen Unternehmen mit etwa 4.500 Mitarbeitern an etwa 55 Standorten in 30 Ländern. Der Ausgangspunkt lag in einer strategischen Management-Entscheidung, den Mitarbeitern Zugriff von jedem Standort zu jedem Standort zu gewährleisten. Die globale IT-Abteilung beschloss, Microsoft Active Directory (MS AD) als zentrales Tool zur Netzwerkadministration einzusetzen, um dieses hochgesteckte Ziel zu erreichen. Die mit der Migration verbundenen Anforderungen, Erwartungen, Probleme und Ergebnisse sollen anhand dieser Studie aufgezeigt werden. Dabei werden die Auswirkungen nicht nur aus der Administrationsperspektive sondern auch aus betriebswirtschaftlicher Sicht beleuchtet.

1 Technischer Hintergrund

1.1 Datennetzwerke

Datennetzwerke bestehen aus zwei Hauptkomponenten: Hardware und Software. Die Hardware (Netzwerkkarten, Kabel, Router, Switche, etc.) bildet die Plattform für die physikalische Übertragung der Daten in einem Netzwerk. Abb. 1.1.1 zeigt ein typisches Netzwerkdiagramm (Netzwerkplan) mit den zugehörigen Hardwarekomponenten.

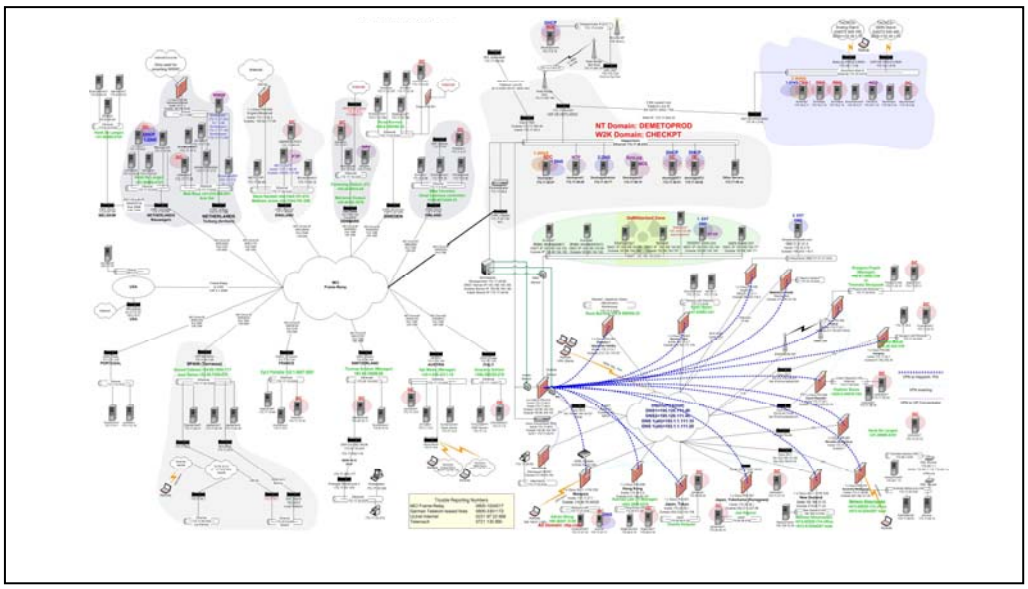


Abb. 1.1.1: Netzwerkplan des betrachteten Unternehmens (Europa + Asien)

Die Netzwerk Software – man spricht in diesem Zusammenhang vom Network Operating System (NOS) – stellt die notwendige „Intelligenz“ im Netzwerk zur Verfügung. Das NOS ist verantwortlich für die Verwaltung der User, Computer, Drucker, sowie anderer Netzwerkobjekte. Das NOS übernimmt auch Steuerung und Zugangskontrolle (Authentisierung) der jeweiligen Netzwerkobjekte. Dazu gehört (u.A.) die Rechtevergabe auf Dateiebene oder die Verwaltung und Überprüfung der Benutzerkennwörter.

1.2 Entwicklung des MS Netzwerk Betriebssystem

Mit der Einführung von Windows NT 3.0 im Jahre 1990 hatte Microsoft ein leistungsfähiges NOS entwickelt, das – nicht zuletzt aufgrund der bestehenden starken Marktanteile des Windows Client Operatingsystems – innerhalb kürzester Zeit größte Verbreitung fand. Mit NT stellte Microsoft das erste „echte“ eigene NOS vor. Bis dahin gab es nur Netzwerkunterstützung für andere Betriebssysteme und das Microsoft Workgroup[1] Konzept. Der damalige Marktführer Novell[2] wurde bis heute fast vollständig vom Markt verdrängt, obwohl sein Betriebssystem technisch ausgereifter war[3]. Trotz der heute starken Verbreitung war und ist Windows nicht unumstritten. Zahlreiche Sicherheitslücken sorgen regelmäßig für Schlagzeilen und in den letzten Jahren wurde Linux von Experten vermehrt als sichere und leistungsfähige Alternative angesehen, die Windows bald ablösen sollte.

Seit der Einführung von Active Directory 1997 mit Windows 2000 Server bietet Microsoft ein leistungsfähiges Netzwerk OS mit stärkerer Sicherheit, stabilerem Laufverhalten und verbesserter Skalierbarkeit. Microsoft Server stellen heute bereits den Industriestandard für Netzwerke dar (siehe Abb. 1.2.1). Bis zum Jahr 2008 prognostiziert IDC[4] für Windows einen weltweiten Marktanteil von etwa 60% im Serverbereich. Ohne Zweifel konnte Linux seinen Markt ausbauen und ist heute insbesondere im Bereich der Webserver weit verbreitet. Linux wird IDC zufolge bis 2008 immerhin 29% des Servermarktes abdecken, jedoch Windows Server OS nicht – wie noch jüngst von vielen Experten erwartet – vom Markt verdrängen.

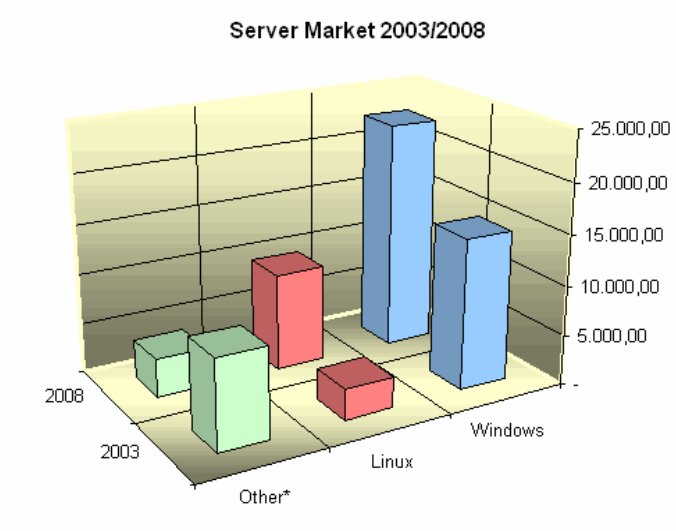
---

[1] Microsoft Workgroups (Arbeitsgruppen) gab es seit Windows 3.11 und ist auch im aktuellen Windows XP enthalten. Es handelt sich dabei um eine einfache Netzwerkverbindung zum Datenaustausch zwischen Client-Gruppen – ohne Domäne, starke Authentisierung oder Sicherheitsmechanismen.

[2] Novell hatte Ende der 80er Jahre Marktanteile von über 80% im NOS Segment.

[3] Novell bot bereits Anfang der 90er Jahre einen aktiven Verzeichnisdienst, sowie bereits seit Novell ELS II (ca. 1986) granulare Rechtevergabe auf Verzeichnisebene.

[4] IDC ist ein auf Informations Technologie spezialisierter Markt Analyst (www.idc.com). Die Zahlen wurden Sekundärliteratur von *Golem* und *Webhosting.info* entnommen, die sich auf IDC Studien beziehen.



Quelle: Eigene Grafik erstellt mit Zahlen von IDC

Abb. 1.2.1: Marktanteile Windows Server

Ein wesentlicher Grund ist wohl darin zu sehen, dass die neuen Windows Netzwerkbetriebssysteme sehr leistungsfähig und wesentlich stabiler geworden sind. Durch automatisiertes Patchmanagement wurde auch die Sicherheit gegenüber NT wesentlich erhöht. Der Anreiz zu Linux zu wechseln ist somit insgesamt geringer geworden.

1.3 Was ist ein Active Directory?

Um die Vorteile von Active Directory verstehen zu können, muss man sich zunächst mit der dahinter stehenden Technologie auseinandersetzen. An dieser Stelle soll ein grundsätzliches Verständnis der MS AD Komponenten vermittelt werden, um den Zusammenhang der teilweise sehr komplexen Vorgänge im Active Directory erkennen und die in der Studie beschriebenen Strategien und Vorgehensweisen besser nachvollziehen zu können.

Active Directory (AD) wird ins Deutsche übersetzt mit (aktiver) Verzeichnisdienst (vgl. *Knecht-Thurmann*, S. 35). Es handelt sich dabei um eine Datenbank, die alle relevanten Objekte des Netzwerks verwaltet.

Aktiv ist dieses Verzeichnis deshalb, weil die Daten nicht statisch sind, sondern sich dynamisch an Veränderungen anpassen. Werden zum Beispiel neue Computer oder Drucker an das Netzwerk angeschlossen, so erscheinen diese automatisch auch im Verzeichnis des Active Directory. Die Verzeichnisstruktur kann dabei nahezu beliebige Organisationsformen annehmen, die durch so genannte Organisatorische Einheiten (engl. Organizational Units = OUs) unterteilt werden. Auf OUs und deren Organisationsformen wird im Folgenden noch genauer eingegangen.

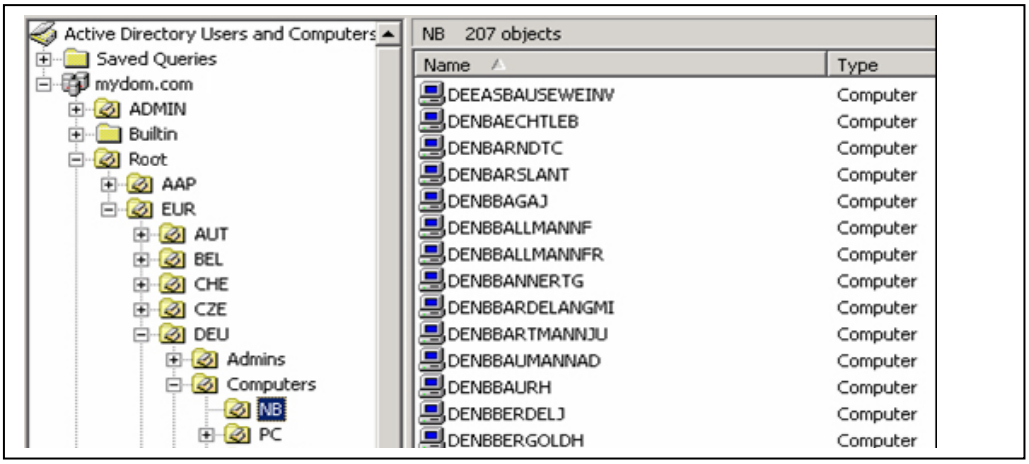


Abb. 1.3.1: OUs und Computerobjekte im AD

1.4 Objektorientierte Datenbank

Die Datenbank des MS Active Directories gehört zur Generation der objektorientierten Datenbanken. Dabei werden die Daten nicht mehr – wie bei konventionellen sequentiellen oder relationalen Datenbanken – in Tabellen oder Formularen angezeigt, sondern als Objekt (Icon) in einer frei definierbaren hierarchischen Struktur (Organizational Units) dargestellt (siehe Abb. 1.3.1). Das bedeutet, dass alle Objekte ähnlich wie in einer Verzeichnis- oder Baumstruktur[5] zugegriffen, angelegt, gelöscht, geändert und verschoben werden können. Zudem gibt es für jeden Objekttyp eine entsprechende Objektklasse, die alle notwendigen Objektattribute (Objekteigenschaften) definiert. Die Objektklassen sind also die Vorlagen für die eigentlichen Objekte (ähnlich eines Bauplans) – sie enthalten selbst keine Daten.

[5] Directory Information Tree (DIT)

Soll unter AD beispielsweise ein neuer Drucker angelegt werden, so wird im Schema nach der entsprechenden Objektklasse für Drucker gesucht und das neue Objekt nach dessen Vorlage (Bauplan) angelegt. Die Objektklasse Drucker enthält (u.A.) die Attribute für den Namen des Druckers, den Standort, das Papierformat und spezielle Informationen über Farbdruckeigenschaften oder Druckauflösung. Jedes neu angelegte Druckerobjekt wird immer genau diese vordefinierten Attribute enthalten. Unter AD kann man bestehende Objektklassen (respektive deren Attribute) ändern oder auch völlig neue Objektklassen erstellen. Alle Objektklassen sind im so genannten Schema abgelegt. Das Schema selbst ist – wie die eigentlichen Objekte auch – im Verzeichnis enthalten. Objekteigenschaften werden i.d.R. durch gesonderte Eingabemasken angezeigt, eingegeben oder geändert (siehe Abb. 1.4.1).

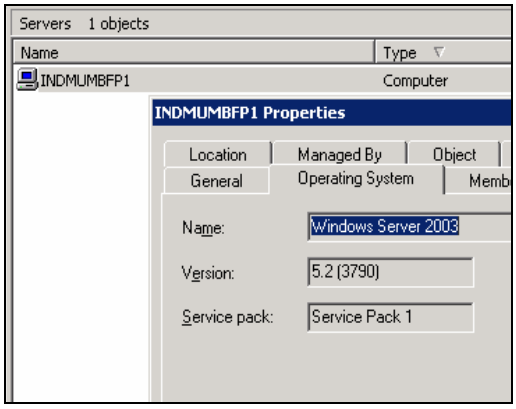


Abb. 1.4.1: Objekteigenschaften

Das Prinzip der Objektklassen wird bereits seit längerem auch im Bereich der objektorientierten Programmiersprachen benutzt (z.B. C++, Visual Basic). Wie bei den Programmiersprachen, können auch unter AD Objektattribute vererbt werden. Dadurch wird es beispielsweise möglich, neue Objektklassen mit Attributen bestehender Objektklassen zu erstellen, ohne für jedes neue Objekt alle Attribute neu erstellen zu müssen (vgl. *Michela, Palme*, S. 33ff.).

1.4.1 Organizational Units

Organizational Units (OUs) sind organisatorische Einheiten für administrative Zwecke. Sie werden im AD als Ordner dargestellt und enthalten weitere OUs oder Objekte wie Computer, Server, User, etc.. Die Organisationsform der OUs kann dabei – wie bei einem Ordnerverzeichnis auf der Festplatte – vom Administrator frei bestimmt werden und ist anforderungsspezifisch. Die Organisation von Netzwerkobjekten in OUs haben zwei wesentliche Vorteile: Zum einen kann man verschiedenen OUs unterschiedliche Administratoren zuweisen und so granulare Berechtigungen im Netzwerk vergeben. Ein typisches Beispiel wäre ein lokaler Administrator, der nur die Objekte in seinem regionalen Bereich administrieren soll – jedoch nicht die gesamte Domäne. Zum anderen kann man den OUs so genannte Gruppenrichtlinien (engl. group policies, GPOs) zuweisen. Group policies sind Einstellungen, die allen Objekten einer bestimmten OU (typischerweise Computern oder Usern) zugeordnet werden (vgl. *Spealman, Hudson, Craft*, S. 377ff.). Die GPO setzt dann im Betriebssystem auf den ausgewählten Objekten bestimmte Registry-Einträge[6], um die vom Administrator gewünschten Einstellungen am System zu erzwingen. Ein typisches Beispiel wäre die Aktivierung der Windows Firewall oder der automatische Update von Windows Komponenten.

Microsoft unterscheidet drei grundlegende Organisationsformen für OUs (vgl. *Spealman, Hudson, Craft*, S. 377ff.), auf die hier kurz eingegangen werden soll:

- **Organisation nach Standort**
  Diese Organisationsform bietet sich an, wenn eine komplexe Standortstruktur vorliegt (z.B. globale, zahlreiche Standorte) und die Administration nach bestimmten Standorten erfolgen soll. Dadurch wird es möglich, lokalen Administratoren alle notwendigen Berechtigungen für „ihre“ OU zu geben.

[6] Die Windows Registry ist eine Datei (bzw. einfache Datenbank), in der alle Systemrelevanten Einstellungen verwaltet werden (Hardware-, Software-, sowie Benutzereinstellungen).

- **Organisation nach Geschäftsfunktion**
  Dies ist dann relevant, wenn die Administration nach Geschäftsbereichen (z.B. Abteilungen: Fertigung, Vertrieb, Kundendienst) erfolgen soll. Hier würde beispielsweise ein Abteilungsleiter spezielle Berechtigungen für seine Abteilungs-OU erhalten.

- **Organisation nach Objekttyp**
  Wenn die Verwaltung vorwiegend nach Objekten (z.B. Computer, Drucker, User, etc.) erfolgt und andere Organisationskriterien weniger relevant sind kann diese Strukturierung benutzt werden (Beispiel: bestimmte Mitarbeiter sollen nur Benutzer anlegen, andere Mitarbeiter sollen nur Computer migrieren, o.ä.).

Um die individuellen Firmengegebenheiten besser abzubilden, findet man in der Praxis eher Mischformen dieser Grundtypen.

1.4.2 Active Directory Datenbank Engine

Obwohl die Verzeichnisdatenbank des AD objektorientiert arbeitet, ist die eigentliche Datenbank Engine auf einer „klassischen" relationalen Microsoft JET (Joint Engine Technologie) Datenbank aufgebaut, die in ihrer ursprünglichen Form bereits 1992 mit MS Access eingeführt wurde (vgl. *Wikipedia* [Microsoft Jet Engine]). Die mit Access eingeführte Datenbank wird auch als JET red bezeichnet. Active Directory nutzt die aktuelle ESE (Extensible Storage Engine) Version, die auch als JET blue bekannt ist. Technisch haben diese beiden Versionen jedoch nur noch wenig gemeinsam und sind nicht kompatibel (vgl. *Microsoft Developer Network* [Extensible Storage Engine]). ESE hat sich bereits bei MS Exchange bewährt und ist für sehr große Datenmengen ausgelegt. Die theoretische Größe der ESE Datenbank liegt bei 16 Terrabytes und wurde bereits mit 40 Millionen (bzw. 60 Millionen[7]) Objekten unter AD getestet (vgl. *Microsoft TechNet* [What Is the Data Storage], sowie *Microsoft TechNet* [How the Data Storage Works]).

[7] Bezüglich der genauen Zahl gibt es in den beiden MS TechNet Dokumenten unterschiedliche Angaben.

1.4.3 Verzeichnisdienst Protokoll LDAP

Wesentlicher Bestandteil des Verzeichnisdienstes ist – neben der Datenbank – das Lightweight Directory Access Protocol (LDAP), das für den Datenaustausch und zum Abrufen von Informationen der Verzeichnisdatenbank benutzt wird (vgl. *Microsoft Corporation* [Microsoft Windows 2000 Active Directory planen und einführen] S. 234ff.). LDAP basiert auf dem Directory Access Protokoll (DAP), das von der International Organization of Standardisation (ISO) und der International Telecommunication Union (ITU) Ende der 80er Jahre als X.500 Protokoll definiert wurde. DAP stellt die Übertragungen aller Verzeichnisinformationen im Netzwerk sicher. Da DAP viele Funktionen unterstützt, die für die meisten Anwendungen nicht genutzt wurden, hat die University Of Michigan Anfang der 90er Jahre das Lightweight Directory Access Protocol entwickelt. LDAP kommt mit wesentlich geringeren Datenmengen aus und wird in der heutigen Form u.A. von Microsoft, Novell, Sun oder Netscape genutzt. Microsoft Active Directory nutzt ausschließlich LDAP für den Verzeichnisdienst. Dabei wird Port 389 und 636 (SSL Verschlüsselung) für die Verbindung zum DC verwendet (vgl. *Microsoft Corporation* [Microsoft Windows 2000 Active Directory planen und einführen] S. 239ff.). Um auf Objekte im LDAP zuzugreifen besteht eine einfache hierarchische Struktur. Dabei werden sog. Attribut Typen (vgl. *IETF* [RFC 2253]) benutzt, wie die Tabelle oben zeigt.

X.500 String	AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

Tabelle 1.1: Attributtypen aus RFC 2253

Ein typischer LDAP Pfad im Active Directory sieht folgendermaßen aus:

LDAP://*cn*=Donald Duck, *ou*=users, *dc*=MyDomain, *dc*=com

Dabei beschreibt der Name hinter *cn* in diesem Falle einen User, der sich in der Organizational Unit (*ou*) names „users“ befindet. Hinter *dc* steht die zugehörige Domänenstruktur.

1.5 Multimaster-Replikation

1.5.1 Redundanz durch Replikation

Die Objekte im AD werden nicht mehr zentral – wie unter Windows NT – auf einem einzigen Master Domain Controller (unter NT PDC[8] genannt) verwaltet, sondern über Multimaster-Replikation auf beliebige Domain Controller im Netzwerk repliziert. Unter Windows NT besteht die Redundanz der Domain Controller darin, dass der Service eines ausgefallenen Primary Domain Controllers (PDC) von einem Backup Domain Controller (BDC) übernommen wird. Dies kann auch standortübergreifend erfolgen (Ein BDC in London übernimmt – über die WAN-Strecke – die Benutzerauthentisierung für einen User in Paris). Grundsätzlich werden unter NT jedoch alle Änderungen der Domain-Objekte immer auf dem PDC durchgeführt und von dort auf die BDCs repliziert (Singlemaster-Replikation). Ist ein ausgefallener PDC nicht mehr zu reaktivieren, so muss ein vorhandener BDC (zeitnah) zu einem PDC heraufgestuft werden, um die Replikation zwischen den Domaincontrollern zu gewährleisten. Geschieht dies nicht, können unter NT keine neuen Objekte mehr angelegt und Objektänderungen nicht mehr durchgeführt werden.

Unter Active Directory gibt es nur noch gleichberechtigte Domain Controller (Multimaster). Objekte können nun an beliebigen Domain Controllern an beliebigen Standorten angelegt oder geändert werden. Von jedem Domain Controller zu jedem Domain Controller können somit Objekte ausgetauscht (bzw. repliziert) werden (Microsoft nennt das Multimaster-Replikation). In der Praxis bedeutet dies, dass z.B. ein französischer User auf dem Domain Controller in London (und umgekehrt) angelegt werden kann und diese Information nach erfolgter Replikation auch auf dem Domain Controller in Paris (bzw. umgekehrt in London) verfügbar ist. Gleiches gilt für Passwortänderungen, Löschung von Accounts, etc.. Aufgrund der Multimaster-Replikation werden diese Objektänderungen (und nur die Änderungen) auf alle übrigen DCs verteilt (repliziert). In Abb. 1.5.1 sieht man einen User (John) in London, dessen lokaler DC ausgefallen ist. Er authentisiert sich über das WAN in Paris und kann ohne Unterbrechung weiterarbeiten.

[8] Primary Domain Controller

Fällt ein lokaler DC unter AD aus, so kann man Objekte auch weiterhin an anderen DCs bearbeiten. In Abb. 1.5.1 genanntem Beispiel könnte man die Eigenschaften von User John auch von London aus auf dem DC in Paris ändern. Zudem könnte auch ein völlig neuer Benutzer (von London aus) am DC in Paris angelegt werden und sich über die WAN-Strecke authentisieren.

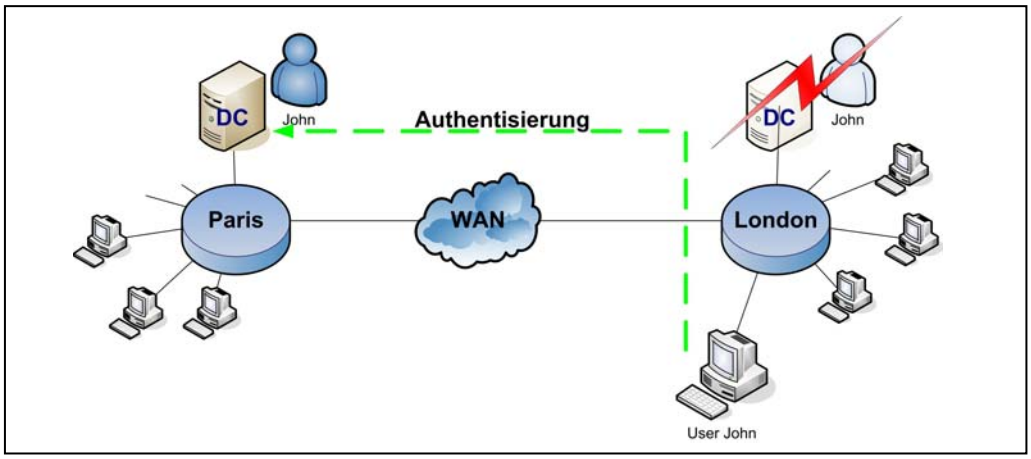


Abb. 1.5.1: Redundanz durch WAN Authentisierung

Das Aufsetzen eines neuen lokalen DCs ist (wenn man von der möglichen Leitungsbelastung durch die Authentisierung über die WAN-Strecke absieht) zeitunkritisch. Es muss kein BDC heraufgestuft werden, da Objekte weiterhin angelegt, geändert und repliziert werden können. Sonderfälle stellen DCs mit Betriebsmastern dar, auf die später noch eingegangen wird.

Zu beachten ist jedoch in diesem Zusammenhang, dass die Services der entfernten DCs nicht mehr zur Verfügung stehen, sobald die WAN Strecke ausfällt. Praktisch bedeutet dies, dass sich User nicht mehr am Netzwerk anmelden können, wenn gleichzeitig der lokale DC und die WAN Leitung ausfallen.

1.5.2 Replikationstopologie

In der Praxis stellt die Replikationstopologie für komplexe und große Netzwerke eine besondere Herausforderung dar. Grundsätzlich unterscheidet man standortinterne und standortübergreifende Replikation (vgl. *Spealman, Hudson, Craft*, S. 25ff.). Die standortinterne Replikation wird automatisch vom AD Dienst KCC [9] sichergestellt. Dabei wird nach vordefinierten Kriterien (Qualitätsmerkmalen) eine Ringstruktur mit mindestens zwei direkten Replikationsverbindungen eingerichtet.

Die externe Replikation wird über Verbindungsobjekte (Inter-Site Transports [10]) gesteuert. Dabei wird für jede Verbindung (Leitung) ein Kostenfaktor zugeordnet. Die Replikation erfolgt dann immer über die „günstigste" Leitung und nur bei einem Leitungsausfall über eine teurere (alternative) Leitung. Durch diesen Steuermechanismus sind komplexe Replikationsstrukturen möglich. Damit wird aber auch deutlich, dass solch eine Struktur genau geplant werden muss und bei fehlerhafter (oder fehlender) Planung unnötige Daten über die Leitungen laufen oder – im ungünstigsten Falle – Replikationsverzögerungen durch „Umwege" entstehen. Für die damit verbundenen Problematiken wird in Kapitel 7 ein kurzes Beispiel genannt.

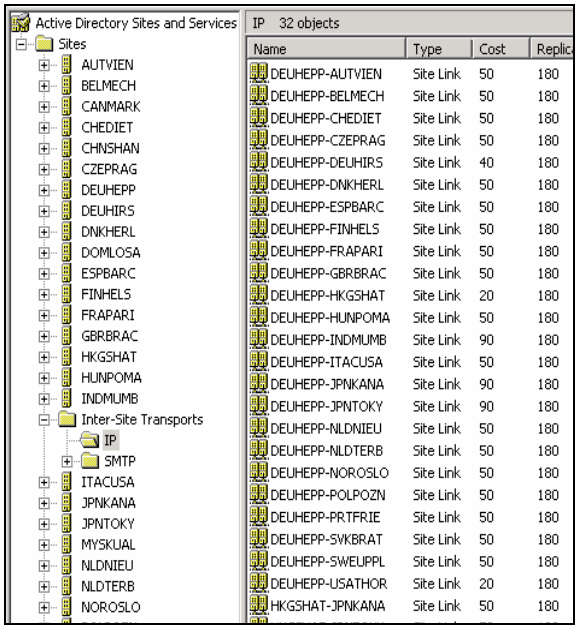


Abb. 1.5.2: Inter-Site Transport Objekte

[9] Der MS Konsistenzprüfungsdienst (KCC) konfiguriert automatisch die Replikationstopologie innerhalb eines Standorts. Dabei werden Verbindungsobjekte automatisch angelegt oder den Anforderungen entsprechend geändert.

[10] Inter Site Transports sind Verbindungsobjekte im AD Verzeichnis. Sie verbinden zwei Standorte (virtuell) miteinander und ermöglichen so die Replikation zwischen Domain Controllern.

1.6 Globaler Katalog

Der globale Katalog (engl. global catalogue, GC) dient dazu, Objekte im AD schneller zu finden. Er enhält die wichtigsten Informationen (Attribute) aller Objekte im Verzeichnis, aus denen im GC Indizes für Suchanfragen erstellt werden. Eine typische Objektanfrage wäre beispielsweise die Suche nach einem Drucker, der bestimmte Eigenschaften besitzen muss (z.B. Standort, Raum, Papierformat, Farbdrucker, etc.).

Abb. 1.6.1: Suche im Globalen Katalog

Welche Informationen (Attribute) im GC gespeichert sind, kann vom Administrator frei bestimmt werden. Bestehen in einer Gesamtstruktur mehrere Domänen, so hält der GC auch Informationen über Objekte aus den anderen Domänen vor. Dabei werden jedoch nur wenige Attribute gespeichert, um das Datenvolumen gering zu halten (vgl. *Spealman, Hudson, Craft*, S. 18ff.).

Der GC wird mit dem LDAP Protokoll über TCP/UDP Port 3268 angesprochen (vgl. *Knecht-Thurmann*, S. 64ff., sowie *Microsoft Corporation* [Microsoft Windows 2000 Active Directory planen und einführen] S. 260ff). Per Voreinstellung wird der GC auf dem ersten Domain Controller der Domäne installiert. Dieser DC wird deshalb auch globaler Katalogserver genannt.

1.7 Betriebsmasterrollen des Active Directory

Neben den Multimaster Servern des Verzeichnisdienstes gibt es spezielle Betriebsmaster, die im AD besondere Rollen übernehmen (Flexible Single Master Operations[11]). Man unterscheidet gesamtstrukturweite und domainweite Betriebsmaster (vgl. *Allen, Lowe-Norris*, S. 22ff., sowie *Spealman, Hudson, Craft*, S. 218ff. oder *Michela, Palme*, S. 111ff.). Gesamtstrukturweite Betriebsmaster dürfen in einer gesamten AD Struktur nur einmal vorkommen (siehe dazu Abb. 1.7.1). Domainweite Betriebsmaster können in der Gesamtstruktur mehrmals vorkommen, in jeder Domäne der Gesamtstruktur jedoch nur einmal.

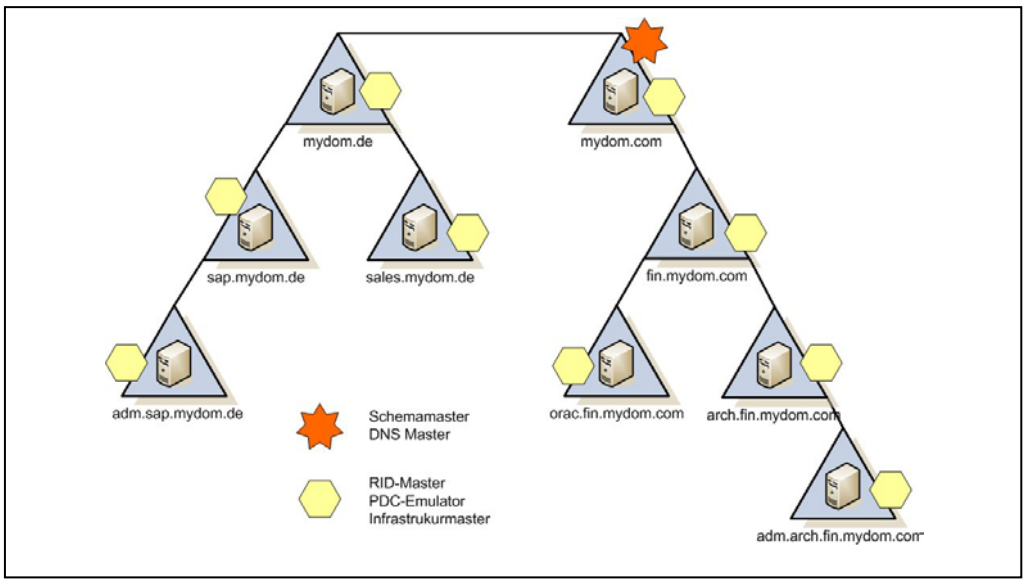


Abb. 1.7.1: Gesamtstrukturweite und domainweite Betriebsmaster

1.7.1 Verteilung der Betriebsmaster

Betriebsmaster können jederzeit auf beliebige DCs transferiert werden. Beliebige DCs können (ohne Transferierung) zu bestimmten Betriebsmastern heraufgestuft werden, wenn sich ein bisheriger Betriebsmaster nicht mehr wiederherstellen lässt. In komplexen Infrastrukturen mit vielen Domain Controllern empfiehlt es sich, die Standorte der Betriebsmaster zu planen und diese von vornherein auf verschiedene DCs zu verteilen. Dadurch werden einzelne DCs entlastet und im Falle eines Hardwarecrashs fallen nicht alle

[11] Je nach Literatur wird von Betriebsmaster oder FSMO (Flexible Single Master Operation) Besitzern gesprochen.

Betriebsmaster gleichzeitig aus. Auch die Wiederherstellung des Systems wird im Ernstfall beschleunigt, wenn nur ein einzelner Betriebsmaster wiederherzustellen ist. Auch wenn man die Betriebsmaster nicht individuell auf DCs verteilt, ist es empfehlenswert, die jeweiligen Standorte der Betriebsmaster zu dokumentieren. Fällt ein Domain Controller mit Betriebsmasterfunktionen aus, kann dies verheerende Folgen haben. Um bei Systemausfall schnell reagieren zu können (Betriebsmaster transferieren oder DC heraufstufen) sind diese Informationen für einen reibungslosen Netzwerkbetrieb von grundsätzlicher Bedeutung.

Im Folgenden sollen die Funktionen der jeweiligen Betriebsmaster näher erläutert werden. Die Darstellung soll sich hier jedoch nur auf die wesentlichen Informationen beschränken und ein Grundverständnis der Dienste vermitteln.

1.7.2 Gesamtstrukturweite Betriebsmaster

Nachfolgende Betriebsmaster dürfen in einer Active Directory Gesamtstruktur nur einmal vorkommen:

- **Schemamaster**

  Das AD Schema enthält alle Informationen über die Objekte des Verzeichnisdienstes. Änderungen am Schema (z.B. das Hinzufügen neuer Objektklassen, etc.) müssen am Schemamaster erfolgen (vgl. dazu 1.4). Der Schemamaster ist nur einmalig in der gesamten AD Struktur vorhanden.

- **DNS Master**

  Da die gesamte Namensauflösung unter Active Directory auf DNS (Domain Name Service) basiert, ist DNS fester Bestandteil von AD. Grundsätzlich können beliebig viele DNS Server innerhalb einer Domäne aufgesetzt werden. Der Domänennamenmaster darf jedoch nur einmal in der gesamten AD-Struktur vorhanden sein, da über ihn das Hinzufügen und Entfernen von Domänen kontrolliert wird. Üblicherweise liegt der DNS Master auf dem ersten DC der ersten Domäne.

1.7.3 Domainweite Betriebsmaster

Nachfolgende Betriebsmaster dürfen in einer Active Directory Gesamtstruktur je Domäne nur einmal vorkommen:

- **Infrastrukturmaster**

  Der Infrastrukturmaster verwaltet die Zuordnungen zwischen Benutzern und Gruppen. Bei Änderungen an den Benutzern (z.B. Name, Eigenschaften), aktualisiert dieser die Verknüpfungen zu den jeweiligen Gruppen. Die Aktualisierungen werden dann per Multimaster-Replikation an die anderen Domain Controller weitergegeben.

- **RID Master**

  Der Relative ID Master (RID Master) verteilt die universellen IDs für die Objekte im Verzeichnis. Die eindeutige SID (Sicherheits-ID) eines jeden Domänenobjekts, setzt sich aus der Domänen-ID und der RID zusammen. Um die Eindeutigkeit der RIDs zu gewährleisten, darf je Domäne nur ein RID Master existieren. Alle DCs erhalten regelmäßig Kontingente (Pools) von RIDs zugewiesen, die von keinem anderen DC mehr benutzt werden. Die DCs greifen bei der Anlage neuer Objekte also nur auf ihre eigene RID Liste zu. Somit können selbst beim (kurzfristigen) Ausfall des RID Masters weiterhin Objekte im Netzwerk angelegt werden[12].

  Beispiele für SIDs:

  ```
  S-1-5-21-1455577082-173041108-1221738049-4206
  S-1-5-21-1455577082-173041108-1221738049-1061
  S-1-5-21-1451215950-3219338060-852893066-1140
  S-1-5-21-733294735-28373578-245764625-22763
  ```

- **PDC Emulator**

  Der PDC Emulator ist erforderlich, wenn ein Trust zu einer NT Domäne besteht (z.B. während einer AD Migration). Dieser sorgt für die Authentisierung zwischen AD Objekten und NT Objekten.

[12] Erst wenn der RID Master für längere Zeit ausfällt und der lokale RID-Vorrat des DCs erschöpft ist, können keine neuen Objekte mehr angelegt werden.

2 Ausgangssituation

Im Folgenden wird ein globales Unternehmen mit vielen Standorten in vielen Ländern betrachtet. Die Unternehmensstruktur war durch zahlreiche Firmenzukäufe, Merges und lokale Unterschiede in Organisation und ICT Infrastruktur stark heterogen. Besonders im IT-Bereich bestanden zahlreiche Insellösungen, deren einzige gemeinsame Basis das Windows NT Betriebssystem darstellte. Dabei hatte jedes Land ein eigenes Windows Netzwerk mit einer eigenen NT 4 Domäne, die jeweils lokal administriert wurde. Die Länder waren untereinander nur nach Bedarf mit Standleitungen (Frame Relay[13]) oder VPN (Virtual Private Network[14]) verbunden worden. Domänen-Trusts (Vertrauensstellungen[15]) zwischen den einzelnen Domänen gab es nur vereinzelt und waren lediglich nach besonderem Bedarf eingerichtet. Es fehlte ein ganzheitliches, strukturiertes TCP/IP Netzwerk, ein einheitliches Domänen- und Authentisierungsmodell, sowie ein globales Konzept für IT-Prozesse und -Organisation. Insbesondere für reisende Mitarbeiter, die an anderen Standorten im Unternehmen arbeiten wollten, gab es grundsätzlich Verbindungs- und Zugriffsprobleme. Email, Internet, sowie Datenzugriff auf Fileserver waren außerhalb des eigenen Standorts oftmals gar nicht mehr – oder nur durch Anpassung der lokalen IT möglich. Aus Management-Sicht war dieser Zustand nicht länger akzeptabel. Um die Unternehmensziele zu erreichen, musste die Verfügbarkeit und Erreichbarkeit der Informationssysteme von und zu allen Standorten gewährleistet werden. Neben einer Restrukturierung des TCP/IP Netzwerkes sollte Microsoft Active Directory als Tool zur Umsetzung eines global administrierbaren Netzwerks eingesetzt werden.

---

[13] Frame Relay ist ein Standardprotokoll für Standleitungen (leased lines). Es wird heute mehr und mehr durch MPLS abgelöst.

[14] VPNs basieren auf verschlüsselten Punkt zu Punkt Verbindungen, die über das öffentliche Internet erstellt werden. Aufgrund der Verschlüsselung werden diese Verbindungen als sehr sicher angesehen. Der Vorteil von VPNs sind die geringen Kosten, da jede beliebige Internetverbindung dafür genutzt werden kann. Der Nachteil von VPNs ist die nicht garantierte Bandbreite bei der Datenübertragung, da zwischen zwei Standorten die verschiedenen Wege der Datenpakete nicht beeinflußt werden können (unterschiedliche Provider und Datenleitungen, sowie nicht kontrollierbare Nutzung anderer Benutzer).

[15] Vertrauensstellungen zwischen Domänen sind notwendig um Zugang zu anderen Domänen (z.B. zum Datenaustausch) zu erhalten.

3 Erwartungen

Aufgrund des zu erwartenden Kosten- und Zeitaufwands einer AD Implementierung, waren die Anforderungen an den Nutzen aus IT- und aus betriebswirtschaftlicher Sicht sehr hoch. Neben dem globalen Zugriff auf Netzwerkobjekte (Server, Computer, Dateien, Drucker, etc.) sollte auch die allgemeine Administration erleichtert werden. Zudem erwartete man durch ein zentralisiertes Netzwerkmanagement verbesserte Übersicht, Kontrolle und mehr Sicherheit im Netzwerk. Auf die wichtigsten Punkte wird nachfolgend eingegangen. Inwieweit diese Erwartungen erfüllt werden konnten, wird im Kapitel 5 und 6 beleuchtet.

- **Globaler Zugriff**

  Primäres Ziel war die überregionale Verfügbarkeit der Systeme und Services. Von jedem Standort sollte den Benutzern – ohne besondere IT-Kenntnisse – der Zugriff auf Netzwerkobjekte eines jeden anderen Standorts möglich sein – insbesondere auch für reisende Mitarbeiter.

- **Simple sign-on**

  Praktisch bedeutet simple sign-on, dass sich ein Anwender nur einmal am Arbeitsplatz anmeldet und Zugriff auf mehrere Systeme (Email, Warenwirtschaft, etc.) erhält, ohne sich erneut anmelden zu müssen. Mit Active Directory erhoffte man sich wenigstens die vereinfachte Anmeldung für die Hauptsysteme wie Netzwerk, Email, SAP und Remote Einwahl zu realisieren.

- **Single Administration**

  Durch die Verknüpfung von Active Directory zu anderen X.500 (bzw. LDAP) fähigen Systemen, sollte die Administration wichtiger Applikationen (Netzwerk, Email, SAP ERP[16]) vereinfacht werden. Insbesondere die Synchronisation von Benutzerdatenbanken sollte zu erheblicher Zeiteinsparung bei gleichzeitiger Steigerung der Aktualität und Präzision der Daten führen. Das Prinzip der „Single Administration" beruht darauf, dass beispielsweise ein User unter AD angelegt wird und über das LDAP Protokoll diese Informationen automatisch in die Email- oder SAP-Datenbank einfließen. Der User muss also nur einmal angelegt werden und erscheint mit den identischen Informationen in „allen" Systemen (siehe Beispiel Notes in Abb. 3.1).

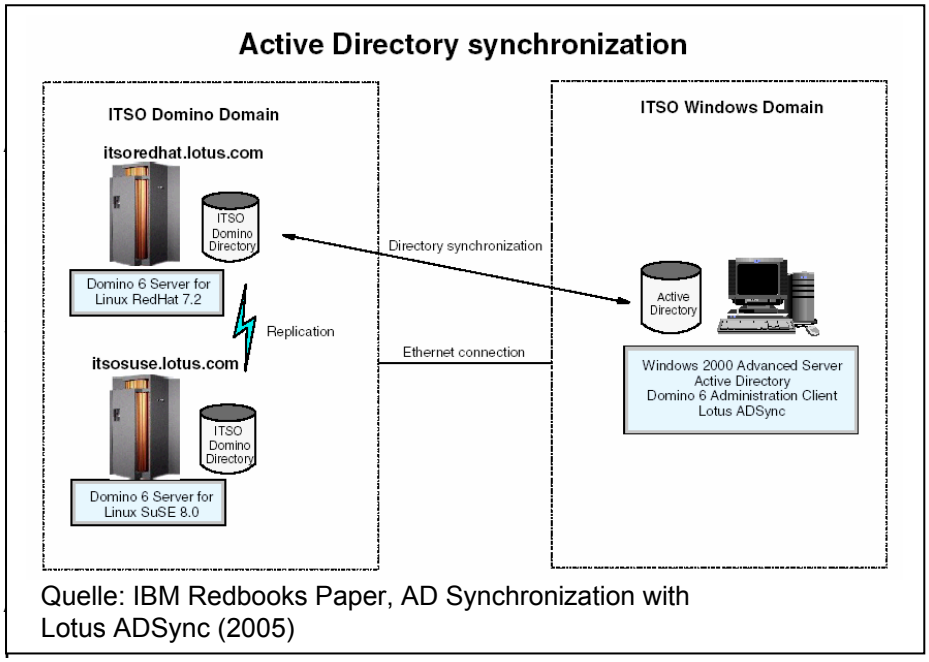


Abb. 3.1: LDAP Synchronisation mit Lotus Notes

[16] ERP = Electronic Ressource Planning. Darunter versteht man komplexe Softwareanwendungen, die es dem Unternehmen ermöglichen, Zugriff auf alle wichtigen Unternehmensdaten zu erhalten. Dazu zählen Warenwirtschafts-, Buchhaltungs- oder beispielsweise Kundenmanagementsysteme, wie sie von der Firma SAP angeboten werden.

- **Inventarisierung**

  Ziel war es, durch das globale Verzeichnis die Übersicht und Transparenz im Netzwerk zu erhöhen und die genaue Inventarisierung der Netzwerkobjekte sicherzustellen. Durch Gruppierungen in OUs wollte man die strukturierte Zuordnung der Objekte zu den Standorten ermöglichen. Auch die Befolgung der Namenskonventionen sollte so besser überwacht werden können.

- **Zentrale und dezentrale Administration**

  Die bis dahin nur unzureichend (über NT Domain-Trusts) verbundenen Standorte sollten ein Netzwerk aus „einem Guss" erhalten und zentral administrierbar sein. Das Management der Netzwerkbenutzer (Anlegen, Ändern, Rechtevergabe, Deaktivierung) wollte man zentral koordinieren und überwachen können. Zudem plante man eine dezentrale Administration für zwei Fälle:

  - **„Follow the sun" support**

    Für reisende Mitarbeiter oder Mitarbeiter, die außerhalb der üblichen Helpdeskzeiten[17] Unterstützung benötigten, sollte die Möglichkeit gegeben werden nicht nur beim lokalen Support, sondern am Helpdesk einer beliebigen Zeitzone Hilfe zu erhalten.

  - **Lokale Administration**

    Ein weiteres Ziel war es, den regionalen Administratoren in den Ländern weitgehende Befugnisse für die Verwaltung ihrer Standorte zu geben. Dafür sollten sie alle notwendigen Berechtigungen für ihren lokalen Bereich erhalten, jedoch nicht auf der gesamten Domänenebene.

[17] Die regionalen Helpdeskzeiten des betrachteten Unternehmens beschränken sich üblicherweise auf normale Bürozeiten.

- **Zertifikate**

  Durch die Möglichkeit im Verzeichnis eine PKI (Public Key Infrastructure[18]) aufbauen zu können, bot es sich an, über die Verteilung von Zertifikaten nachzudenken. Als zukünftiger Schritt, war angedacht, Zertifikate zur Authentisierung (u.A. im Zusammenhang mit „Simple sing on“) oder Email-Sicherheit zu nutzen.

- **Verbesserte Netzwerksicherheit**

  Durch die Implementierung von globalen Gruppenrichtlinien (GPOs) wollte man regionale und globale Einstellungen an allen PCs im Unternehmen kontrollieren und somit zur Sicherheit der Systeme beitragen. Lokale PC-Firewalleinstellungen, Sicherheits- und Softwareupdates, sowie zahlreiche weitere sicherheitsrelevante Einstellungen sollten damit unternehmensweit und individuell gesteuert werden können. Zudem plante man eine Passwort Policy, die starke Benutzerkennwörter erzwingen würde. Es wurde außerdem erwartet, dass durch Redundanz der DC Verzeichnisdatenbanken die Ausfallsicherheit im Netz erhöht wird. Fällt ein Domain Controller unter AD aus, so kann vorübergehend ein beliebiger anderer Domain Controller die Aufgaben übernehmen (siehe dazu auch 1.5.1).

- **Prozessoptimierung**

  Insgesamt sollte Active Directory zur Unterstützung und Transparenz von IT-Prozessen beitragen. Viele Abläufe (Zugang/Abgang von Mitarbeitern, Softwarenutzung, gemeinsame Ressourcennutzung, etc.) sollten global vereinheitlicht werden.

[18] PKI basiert auf einem Authentisierungsverfahren, das auf einem privaten (geheimen) und einem öffentlichen Schlüssel beruht. Darauf lassen sich u.A. Zertifikats- und Authentisierungsdienste aufbauen (vgl. Microsoft, Entwerfen und Einführen von Active Directory- und Sicherheitsdiensten für Windows Server 2003, S.671 ff.).

4 Projektierung

Nachdem die IT-Strategie festgelegt und die Entscheidung für Active Directory als Tool gefallen war, wurde das Projekt vorbereitet. Das Migrationsteam wurde international mit zwei Netzwerkarchitekten und einem Netzwerkingenieur besetzt. In der Vorbereitungsphase wurden zunächst Informationen über Active Directory gesammelt und evaluiert, um einen möglichst guten Überblick über den Zeit- und Kostenaufwand zu erhalten. Danach wurde die Grobplanung für das Projekt erstellt:

Consulting	1 Monat
Planung	1 Monat
Testphase	2 Monate
Implementierung	12 Monate

4.1 Consultingphase

Hierbei ging es vorwiegend darum, alle sinnvollen Migrationsstrategien zu verstehen, um grobe Fehler in der Architektur zu vermeiden. Es sollte verhindert werden, ein eventuell falsches Migrationskonzept zu spät zu erkennen und dann auf irreversible – oder nur mit sehr hohem Aufwand zu lösende – Probleme zu stoßen. Dabei sollte ein kompetentes Consultingunternehmen (Microsoft Goldpartner) mit großer Praxiserfahrung beratend zur Seite stehen.

Zunächst wurden die verschiedenen Möglichkeiten aufgezeigt, mit denen man ein NT Netzwerk in ein AD Netzwerk überführen (migrieren) kann. Es ergaben sich zwei grundsätzliche Ansätze: Harter Schnitt oder fließender Übergang. Es stellte sich schnell heraus, dass ein harter Schnitt aufgrund der Unternehmensgröße und der Unüberschaubarkeit der Systeme und den damit verbundenen Konsequenzen nicht sinnvoll war. Man entschied sich letztlich für einen schrittweisen Übergang auf Active Directory. Dabei sollte Standort für

Standort in das globale Netzwerk eingebunden werden. Auch die Standortmigration selbst, musste nicht auf einmal erfolgen, sondern konnte Maschine für Maschine umgestellt werden. Das Konzept, das zusammen mit den Beratern entwickelt wurde, sah folgende Migrationsstrategie vor:

Erstellung einer einzigen globalen Domäne (hier: mydom.com) mit einer einzigen AD integrierten DNS Zone[19], um die Namensauflösung der Server global zu gewährleisten. Für die User Maschinen in den Ländern plante man eine lokale primary DNS Zone[20] einzurichten, da die Namensauflösung der User PCs nicht global verfügbar sein musste. Die OU Struktur wollte man hierarchisch nach Standorten aufzubauen. Dabei waren drei übergeordnete OUs für die Regionen und unterhalb der Regionen die Länder und Standorte vorgesehen (siehe Abb. 4.1.1). Es war geplant, die Standorte einzeln bzw. nacheinander umzustellen. Dabei sollte ein Domänentrust zwischen der bestehenden NT-Domäne und der neuen AD-Domäne die nahtlose Migration gewährleisten. Durch den Trust konnte PC für PC umgestellt werden, ohne dass Zugriffsprobleme auftreten. Außerdem entschied man sich dazu, die Migration vom unternehmensinternen IT-Team umsetzen zu lassen, um das Know-how möglichst im Hause zu behalten. Die Umsetzung vor Ort in den Ländern sollte ebenfalls von internen Ressourcen erfolgen um dem Ziel „Netzwerk aus einem Guss“ Rechnung zu tragen. Ziel war dabei, die Migration der User und Computer von lokalen IT-Ressourcen der Standorte unterstützen zu lassen.

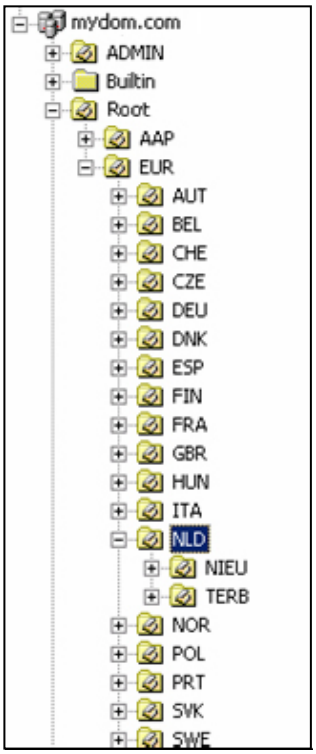


Abb. 4.1.1: OU Struktur

[19] AD integrierte DNS Zonen werden auf alle DCs repliziert. Maschinen, die sich dort anmelden, erscheinen innerhalb der Replikationszeit auf jedem DNS Server der Zone.
[20] Primary DNS Zonen werden nicht im AD repliziert. Angemeldete Maschinen erscheinen nur im lokalen DNS.

4.2 Planungsphase

Der Übergang zwischen Consultingphase und Planung erfolgte fließend. Auch bei der Projektplanung wurde das Beratungsunternehmen regelmäßig einbezogen um von deren Erfahrung vergangener Projekte zu profitieren und Best Practices[21] zu berücksichtigen. Neben der eigentlichen Projektplanung (zeitlicher Ablauf) galt es insbesondere die Struktur des künftigen Active Directories zu formulieren. Dabei war die grundsätzlichen Migrationsstrategie und die benötigte Struktur zahlreicher AD Services zu berücksichtigen:

- **Migrationsstrategie**

  Die Planung sah eine schrittweise Migration der Standorte vor. Dazu sollte für jede bestehende NT Domäne ein Trust zur neuen AD Domäne hergestellt werden. Man wollte dadurch sicherstellen, dass Benutzer der alten Domäne weiterhin Berechtigungen und Zugang zu Objekten (z.B. Servern) in der neuen AD Domäne haben. Ziel war es, zunächst einen lokalen AD DC zu implementieren und dann die User einzeln in die neue Domäne zu migrieren. Nach erfolgter User Migration sollte der letzte Schritt die Server-Migration sein. Anschließend war geplant, den jeweiligen NT PDC abzuschalten.

- **Positionierung und Dimensionierung von DCs**

  Aufgrund der unterschiedlichen Standortgrößen mussten individuelle Ressourcen für Domain Controller eingeplant werden. Dabei entschied man, für die drei IT-Hubs (New Jersey, Deutschland, Hong Kong), sowie für große Standorte (> 100 User) redundante Domain Controller zu implementieren. Für mittlere Standorte war ein einfacher Domain Controller (Standardserverhardware) und für sehr kleine (< 5 User) kein Domain Controller sondern Authentisierung über WAN vorgesehen.

[21] Best Practices sind beste Praktiken, die in der Industrie allgemein anerkannte Standardprozeduren darstellen.

- **TCP/IP Routing und Subnetting**

  Um dem Replikationsmodell des AD Verzeichnisdienstes Rechnung zu tragen, musste sichergestellt werden, dass eine gültige Netzwerkverbindung von jedem Standort zu jedem Standort bestand. Man war sich bereits im Vorfeld darüber im Klaren, dass eine Restrukturierung des bestehenden IP Netzwerks unumgänglich war, um IP Routing von jedem Standort zu jedem Standort zu gewährleisten. Fast alle größeren Standorte verfügten bereits über Frame Relay Standleitungen, die vollständig gemashed[22] waren. Die Routingtabellen wurden über EIGRP[23] ausgetauscht, sodass der Zugriff zwischen allen Frame Relay Standorten gewährleistet war. Zahlreiche kleinere Standorte verfügten jedoch lediglich über „Punkt zu Punkt" VPN Verbindungen, deren Routing auf die jeweiligen lokalen Subnetze beschränkt war – von dort war standortübergreifendes IP-Routing nicht möglich. Die Planung konzentrierte sich deshalb auf noch nicht ins Firmennetz eingebundene bzw. bisher über VPN verbundene Standorte. Im Wesentlichen bestand die Planung darin, die bestehenden Subnetze in ein einheitliches Konzept einzubinden (Umstellung der IP Adressen von Subnetzen) und die VPN Verbindungen mittelfristig in ein gemashtes und voll geroutetes[24] Netzwerk zu überführen.

  Man entschied sich dazu, mittelfristig alle bisher intern administrierten VPN Verbindungen an einen Provider abzugeben, der das Routing für alle Standorte sicherstellt. Bis dahin wurde das Replikationsmodell der Domain Controller so gewählt, dass die VPN Standorte direkt über die VPN Verbindung lediglich zum nächsten Hub replizieren. Das Ziel, Zugriff auf Daten beliebiger Standorte zu erhalten konnte für diese VPN Standorte zu diesem Zeitpunkt nicht vollständig realisiert werden.

[22] In diesem Falle bedeutet gemashed (eingedeutscht aus dem engl. mashed, dt. vermascht), dass alle FR Standorte mit jedem anderen FR Standort direkt verbunden sind und IP Routing zwischen allen Standorten besteht.
[23] EIGRP ist ein Routingprotokoll, das Informationen über Subnetze und Datenwege austauscht.
[24] Bei einer einfachen VPN Verbindung besteht nur ein IP Tunnel zwischen zwei Standorten. Soll von diesen Standorten zu weiteren Subnetzen geroutet werden, müssen alle Subnetze manuell oder per Routingprotokoll bekannt gemacht werden. Dies erfordert einen sehr hohen Administrationsaufwand und war bis dato aufgrund begrenzter IT Ressourcen nicht möglich.

DC Replikationsstruktur

Zu Planungszeitpunkt hat man dem Replikationskonzept nur eine untergeordnete Rolle beigemessen. Es sollte ein dreistündiges Replikationsintervall eingerichtet werden, bei dem alle DCs mit anderen DCs replizieren, die über Site-Transports (siehe 1.5.2) verbunden sind. Auf die damit verbundene Problematik wird im Kapitel 6.2 noch eingegangen.

- **Organizational Unit Struktur**

  Einen erheblichen Teil des Planungsaufwandes verwandte man für die OUs. Dabei entschied man sich für das bereits erwähnte Konzept der regionalen Strukturierung (siehe dazu 1.4.1), um dem geplanten Administratorkonzept (s.u.) Rechnung zu tragen.

- **DNS Struktur**

  Das ursprünglich geplante Konzept einer Subzonen Struktur hat man wieder verworfen, da regionale Server von Reisenden nur mit zusätzlichem Administrationsaufwand zugänglich gewesen wären. Es war geplant, zunächst für die verschiedenen Regionen AD integrierte Subzonen zu erstellen (**usa**.domain.com, **eur**.domain.com, **pac**.domain.com). Bei der Namensauflösung wäre jedoch beispielsweise ein Zugriff von USA auf einen Server in Europa nicht direkt möglich gewesen, da die Subzonen sich auf dem gleichen Level befinden. Die von Microsoft empfohlenen Maßnahmen zur Lösung dieses Problems[25] stellten sich als nicht befriedigend dar und hätten einen erheblichen Mehraufwand an Administration bedeutet. Letztendlich entschied man sich für ein Modell, bei dem alle Server (aller Standorte) in der AD integrierten Rootzone stehen und nur die User PCs in den jeweiligen regionalen Primary Zonen enthalten sind (siehe dazu auch 4.1).

[25] Eine in Betracht gezogene Lösung war beispielsweise, den Clients (über GPOs) weitere DNS Suffix Einträge für die Zonen zu vergeben.

- **DHCP Konzept**

  Die Planung sah hier vor, auf jedem DC auch einen DHCP[26] Server zu installieren, der die Clients mit allen notwendigen Netzwerkeinstellungen (IP Adresse, Gateway, DNS Server) versorgt. Auch Adress-Reservierungen für bestimmte Clients waren vorgesehen. Von der ursprünglichen Planung, auch die Server über DHCP mit festen IP Adressen zu versorgen, hat man aufgrund einiger Probleme (ungültige oder nicht eindeutig zuzuordnende MAC Adressen, doppelte IP Vergabe, Ausfall von DHCP Servern) wieder abgesehen.

- **Namenskonventionen**

  Für die Namenskonventionen hat man einen Großteil der Planungszeit aufgewandt. Es sollte ein einheitliches, global genutztes Konzept zur Benennung von Netzwerkobjekten entstehen. Dabei waren zahlreiche Abgleichungsrunden mit den regionalen IT-Administratoren notwendig, um allen Ansprüchen gerecht zu werden und Einwände oder erkannte Probleme zu berücksichtigen. Die Namenskonventionen enthielten schließlich Vorgaben für die Benennung von Ländern, Städten, Standorten, Servern, Computern, Druckern und Usern. Wichtig war dabei, dass Netzwerkobjekte anhand des Namens eindeutig identifiziert werden konnten, ohne weitere Datenbanken zur Identifizierung bemühen zu müssen. Für Computer hat man – insbesondere unter dem Aspekt der reisenden Mitarbeiter – Wert darauf gelegt, dass der Computername direkten Aufschluss über Herkunft (Land) und zugehörigen User gibt. Die entsprechende Konvention sah deshalb zwingend eine genau definierte Länderkennung und eine Userbezeichnung vor.

[26] DHCP (dynamic host configuration protocol) erlaubt Clients die automatische Zuweisung grundlegender Netzwerkinformationen wie IP Adresse, Standard Gateway, DNS Server, etc..

- **Administratorkonzept**

  Die Planung sah vor, dass die regionalen IT-Mitarbeiter ihre Standorte weitgehend selbst administrieren. Dabei sollten diese keine Domain-Administrator Berechtigung besitzen, um die Sicherheit der Domäne nicht zu gefährden. Versehentlichem Löschen von OU-Strukturen oder anderen wichtigen Elementen der Active Directory wollte man so vorbeugen. Da für die User- und Computer-Migration jedoch zwingend Domain-Admin Berechtigungen notwendig sind und die lokalen Administratoren an der Migration beteiligt werden sollten, hat man ihnen für den Zeitraum der Migration die Berechtigungen des Domain-Administrators vergeben. Dieses Risiko wurde bewusst in Kauf genommen, da die Migration aus Ressourcengründen anders nicht bewältigt werden konnte.

4.3 Testphase

In der Testphase wurde in Deutschland[27] eine Active Directory Domäne gemäß den Spezifikationen der Migrationsstrategie aufgesetzt und ein Trust zur bestehenden NT-Domäne erstellt. Zur Evaluierung wurden einige Test-Workstations und -User migriert. Dazu wurden die von Microsoft zur Verfügung gestellten Standard-Tools benutzt (z.B. AD Migration Tool). Es wurde insbesondere geprüft, ob die Zugriffsberechtigungen zu Objekten der alten NT Domäne auch aus der neuen AD Domäne bestehen. Dies war die Voraussetzung für eine nahtlose Migration, die es erlaubte, Computer für Computer und User für User in die neue Domäne zu übernehmen. Nach erfolgreichen Tests, sowie Erstellung der notwendigen Dokumentation und Prozeduren begann man mit der eigentlichen Implementierung.

[27] Deutschland wurde als IT-Hub für Europa aufgrund der IT-Ressourcen (Know-how, Manpower) zum Teststandort ausgewählt.

4.4 Implementierungsphase

Nach erfolgreichem Test und Optimierung der Anforderungen und Prozesse wurde die produktive Domäne erstellt und im Netzwerk verfügbar gemacht. Schließlich wurden die ersten User und Computer erfolgreich in die produktive AD Domäne migriert.

4.4.1 Migrationsplan

Bereits in der Testphase wurden umfangreiche Dokumentationen erstellt, die Schritt für Schritt die Vorgehensweise der AD Implementierung vor Ort beschreiben. Vor der eigentlichen Migration wurde diese Dokumentation weiter optimiert und aufgrund der ständig neuen Erfahrungen auch später immer wieder angepasst. Der Migrationsplan beinhaltete im Wesentlichen folgende Punkte mit jeweils detaillierten Prozeduren:

- Vorbereitung in AD (neuen Standort und IP Subnet in AD anlegen)
- Domänentrust zwischen alter NT Domäne und AD erstellen
- DNS und DHCP auf neuem DC konfigurieren
- DC Promo ausführen um Server zum Domain Controller heraufzustufen
- Einrichtung der regionalen DNS Zone
- DHCP auf DC konfigurieren
- Administrator Accounts für lokale Administratoren anlegen
- AD-Tools und zusätzliche Software auf dem DC installieren
- Scripts für SID Transfer ausführen
- Testuser migrieren
- Test PC migrieren
- Standard GPOs für Standort OU einrichten
- Sowie diverse kleinere Prozeduren für Testwerkzeuge

Die Prozeduren des Migrationsplans wurden dann von einem Mitglied des Migrationsteams vor Ort abgearbeitet (siehe auch 4.4.3).

4.4.2 Vorbereitung der Standorte

Für die Migration der Standorte wurde eine detaillierte Checkliste erstellt, die dem lokalen IT-Verantwortlichen im Vorfeld zugeschickt wurde. Enthalten waren Hardwarespezifikationen für den Domain Controller, sowie spezifische Installationsanweisungen zur Grundinstallation des Betriebssystems. Für die späteren Arbeiten vor Ort wurde vorab ein grober Projektplan mit den lokalen Mitarbeitern abgestimmt (Zeitpunkt, Dauer, Ort, Ablauf, benötigte Ressourcen, Anreisemodalitäten, etc.).

Die künftigen Domain Controller wurden gemäß den Vorgaben bestellt und vom lokalen IT-Team vorkonfiguriert. Überprüfungen per Fernzugriff ergaben, dass bei der Installation von den lokalen Kollegen sehr kreativ vorgegangen wurde und man sich oftmals nicht an die Vorgaben hielt, bzw. darüber hinausging. Hier galt es, sehr detailliert alle systemrelevanten Einstellungen auf Abweichungen zu prüfen, um spätere Probleme zu vermeiden. Beispiele für inakzeptable Abweichungen waren falsche Partitionsgrößen, Installation als Fileserver, Antivirus- oder Remote Zugriff Installationen, sowie Installation diverser Software.

Je nach Zeitplan wurde der Domänentrust zwischen der bestehenden NT Domäne und AD ebenfalls remote vorgenommen, da hier erfahrungsgemäß die meisten Probleme entstanden. So konnten bereits im Vorfeld eventuelle Schwierigkeiten ohne Zeitdruck ausgeräumt werden. Außerdem wurde geprüft, ob das lokale Subnetz dem globalen IP Schema entsprach, da u.U. Vorlaufzeiten für Änderungen beim Provider der Frame Relay Standorte[28] einkalkuliert werden mussten.

[28] Für die FR Standorte musste das Routing vom Provider mit entsprechenden Vorlaufzeiten umkonfiguriert werden.

4.4.3 Migration vor Ort

Für die eigentliche Implementierung teilte man das Migrationsteam in zwei regionale Zuständigkeiten auf: Ein Teil betreute Nord- und Südamerika, der andere Teil betreute die Region Europa und Asien. Dabei sollte immer ein Mitglied des Migrationsteams die Implementierung vor Ort am Standort überwachen. Zum einen ging es darum, sich ein genaues Bild der Situation vor Ort zu machen, zum anderen sollte das notwendige Know-how zu Active Directory möglichst direkt aus dem Team vermittelt werden. Wichtig war hier auch ein echter Austausch zwischen globaler und lokaler IT, um eventuelle lokale Probleme oder Hindernisse erkennen und ausräumen zu können.

Erste Aufgabe vor Ort war es, sich ein Bild über das bestehende Netzwerk zu machen. In der Vergangenheit hatte sich regelmäßig gezeigt, dass das Verständnis für relevante Informationen der Netzwerkinfrastruktur lokal völlig unterschiedlich war. Die verfügbare Dokumentation war oftmals unvollständig oder enthielt – aus Netzwerksicht – völlig unbrauchbare Informationen. In Zusammenarbeit mit dem lokalen Team wurden alle relevanten Netzwerkkomponenten wie Server, Router, Switches, Verkabelung, VPN und Firewall behandelt und ein detaillierter Netzwerkplan erstellt. In diesem Rahmen wurden auch Komponenten wie Wireless LAN[29], Anti-Virus,[30] Ad- und Spyware[31], sowie generelle Sicherheitsthemen angesprochen. Einige Standorte betrieben lokale (schlecht geschützte) Internet Gateways, die es mittelfristig abzuschalten galt. Hier musste ein praktikables Konzept gefunden werden, den Internet Zugriff über den regionalen IT Hub (z.B. Deutschland oder Hong Kong) zu routen.

In den meisten Fällen ergab sich auch genereller Handlungsbedarf zur Optimierung des Netzwerks (z.B. Optimierung der Switches, Verkabelung, Patch Management, OS- oder Softwareupdates, etc.).

---

[29] Hier gab es bereits eine bestehende Policy, sowie ein geplantes globales Projekt.
[30] Obwohl eine globale Lizenzierung einer Corporate Antivirus Version existierte, hatten zahlreiche Länder ihre eigenen Lösungen implementiert, was unnötige Kosten verursachte.
[31] Bisher gab es diesbezüglich keine einheitliche Lösung, da ein unternehmensweites Konzept bis dato von keinem bekannten Hersteller zufrieden stellend unterstützt wurde. Es sollte jedoch für das Thema sensibilisiert und die geplanten Projekte in diesem Bereich vorgestellt werden.

Ein wichtiges Anliegen der globalen IT-Abteilung war der Informationstransfer zu Active Directory. Als wichtigste Inhalte sind zu nennen:

- Grundkonzept Active Directory
- Vorteile der AD (Simple Sign-on, globaler Datenzugriff, Administration, Sicherheit, etc.)
- Organizational Units (OUs)
- Group Policies (GPOs)
- Globale Namenskonventionen
- Administration unter AD

Im nächsten Schritt wurde der Ablauf der Migration abgestimmt. Zunächst wurde der Domain Controller eingerichtet und mit der AD Domäne repliziert. An manchen Standorten musste das IP Subnetz an das globale IP Schema angepasst werden. Dabei wurde DHCP für die User umgestellt, sowie neue IP Adressen für Server und Netzwerkkomponenten vergeben. Das globale Routing musste in den Routingtabellen der VPN Komponenten eingetragen bzw. für Standorte mit Standleitung beim Provider neu beantragt werden. Anschließend erfolgte die Migration gemäß Migrationsplan (siehe 4.4.1). Es sei an dieser Stelle darauf hingewiesen, dass sich bei fast jedem der etwa 35 Standorte in Europa und Asien individuelle Komplikationen bei der Migration ergaben, die im Vorhinein nicht zu ersehen waren (z.B. an einem Standort wurde eine AD Domäne vorgefunden – statt einer erwarteten NT Domäne, ein anderer Standort benutzte einen Domänennamen zu dem kein Trust erstellt werden konnte, andere hatten im Nachhinein die Konfiguration des DCs geändert, u.v.m.).

Waren die Vorarbeiten abgeschlossen, erfolgten die ersten Testmigrationen der User und Computer. Typische Migrationsprobleme (z.B. Firewall aktiv, unzureichender Festplattenplatz auf dem Client, etc.) wurden aufgezeigt und gegebenenfalls korrigiert. Die weitere Migration erfolgte anschließend durch lokale IT-Ressourcen.

5 Resultierende Vorteile

Nachdem die Migration zum jetzigen Zeitpunkt zu etwa 95% abgeschlossen ist[32], lässt sich der Projekterfolg relativ genau bewerten. In allen großen Standorten wird AD bereits seit über einem Jahr eingesetzt, sodass sich sehr zuverlässige Aussagen treffen lassen. In diesem Kapitel soll auf die entstandenen Vorteile der AD-Implemetierung eingegangen werden. Das nachfolgende Kapitel beleuchtet die Probleme, die sich in diesem Zusammenhang ergaben.

5.1 Administration

Zusammenfassend lässt sich vorweg nehmen, dass die Administration unter Active Directory erhebliche Vorteile gebracht hat. Durch die hohe Flexibilität und die Vielzahl der Tools kann das Netzwerk – je nach Bedarf – global oder lokal administriert werden. Dabei verliert die übergeordnete globale IT-Abteilung niemals die Kontrolle über die lokalen Standorte.

- **Globaler Zugriff**

  Wenn man von den VPN Standorten absieht[33], hat sich AD unter dem Aspekt des globalen Zugriffs als sehr erfolgreich erwiesen. Seitdem das IP Routing angepasst und kleinere DNS Probleme beseitigt wurden, können Benutzer nun global von jedem Standort auf ihre Heim- und Emailserver zugreifen. Reisende haben problemlos Zugang zu allen Informationen im Netzwerk, ohne jedes Mal den lokalen Helpdesk bemühen zu müssen.

[32] An einigen (wenigen) Standorten existieren noch NT PDCs, sowie einige wenige Clients, die bisher nicht in AD migriert werden konnten (Außendienstmitarbeiter). Ferner wurde die Migration der Standorte in Malaysia und Australien aus organisatorischen Gründen auf das nächste Jahr verschoben.

[33] Die VPN Standorte werden erst im kommenden Jahr vom Provider in das globale Routing übernommen.

- **Organizational Units**

  Zwar ist die Planung und Administration von OUs zunächst sehr zeitaufwändig, jedoch wird dadurch die Strukturierung und Übersicht im Netzwerk wesentlich erhöht. Objekte sind leichter aufzufinden und Eigenschaften strukturiert zuzuordnen. Nicht zuletzt können für die Objekte einer OU Gruppenrichtlinien (GPOs) vergeben werden, die erhebliche Vorteile bei Administration und Sicherheit bringen.

- **Gruppenrichtlinien (GPOs)**

  Die Group Policies können beliebigen OUs und somit nahezu beliebigen Objekten (i.d.R. Computern oder Usern) im AD zugeordnet werden. Sie sorgen für die vom Unternehmen gewünschten Einstellungen auf Computern (siehe dazu 1.5.2) oder anderen Objekten und tragen so erheblich zur Vereinheitlichung der Systeme und zur Gesamtsicherheit im Netzwerk bei. User können nicht mehr so leicht „aus der Reihe tanzen“, da diese Einstellungen erzwungen werden können. Durch GPOs konnten die Firewall Einstellungen für alle User kontrolliert werden, sowie die Updates für (von der IT-Abteilung als sinnvoll erachtete) Windows Sicherheits-Patches erzwungen werden. Spezielle GPOs für Notebooks und Desktop Computer wurden eingerichtet um spezifische Einstellungen (z.B. Offline-Files, Server-Profiles, etc.) vorzunehmen.

- **Namenskonvention**

  Durch die Namenskonvention haben sich erhebliche Vorteile in Struktur und Transparenz des Netzwerks ergeben. Durch die selbsterklärenden Bezeichnungen können Maschinen nun leicht zugeordnet und User problemlos identifiziert werden. Für die Administration entstanden dadurch in der Praxis erhebliche Erleichterungen.

Simple sign-on

Aufgrund mangelnder IT-Ressourcen wurde die Implementierung von Simple sign-on zunächst verschoben (siehe dazu auch 6.2). Die Anbindung an Notes ist für das kommende Jahr geplant.

- **Inventarisierung**

  Durch das strukturierte OU-Konzept, sowie der objektorientierten Datenbank, können alle Netzwerkobjekte im Verzeichnis leicht aufgefunden und zugeordnet werden. Die Inventarisierung wurde erheblich vereinfacht, da nun alle Objekte (User, Computer, Server, etc.) in Echtzeit aufgelistet werden.

5.2 Sicherheit

Unter AD ergeben sich zahlreiche sicherheitsrelevante Verbesserungen, auf die hier nur grob und aus subjektiver Sicht des Projekts eingegangen werden kann:

- **Hacking**

  Durch zahlreiche Verbesserungen an Authentisierung und Verschlüsselung (Kerberos, mutual authentication, Passwortverschlüsselung), wurden Einbruchsversuche und das Abfangen von Passwörtern erheblich erschwert, sowie die Gesamtsicherheit des Systems erhöht.

- **Benutzerkennwörter**

  Durch die (gegenüber NT) wesentlich bessere Granulierung von Passwortrichtlinien lassen sich sehr komplexe und sichere Kriterien für die Vergabe von Passwörtern einstellen. So kann man beispielsweise untersagen, dass Teile des eigenen Namens als Teil des Passworts verwendet werden dürfen. Die regelmäßige Erneuerung des Passworts erfolgt komfortabler als unter NT. Die Erstellung komplexer Passwort-Anforderungen war Voraussetzung für Simple-sign-on.

- **GPOs**

  Durch GPOs lassen sich zahlreiche grundsätzliche Sicherheitseinstellungen an den Clients vornehmen. Dadurch konnte beispielsweise das Patchmanagement erheblich verbessert werden oder Einstellungen für Firewall, Offline Files und Server Profiles kontrolliert werden.

- **DC Redundanz**

  Da es auf den Netzwerkbetrieb nahezu keine Auswirkung hat, wenn ein DC ausfällt, ist die Kontinuität des Geschäftsbetriebs gewährleistet. Anders als unter NT können weiterhin Objekte angelegt und geändert werden. Die Beschaffung von Ersatzhardware und Neuinstallation ist somit nicht mehr zeitkritisch. Dies ist insbesondere aus Unternehmenssicht ein großer Vorteil, da keine Ausfallzeiten entstehen und IT Ressourcen flexibler verplant werden können.

Größter Vorteil von Active Directory ist wohl die globale – oder je nach Bedarf auch lokale – Administration. So können globale Richtlinien über GPOs auf jeden Computer im Unternehmen konfiguriert werden oder lokale Administratoren ihre eigenen regional spezifischen GPOs erstellen. Weiterhin können durch die granulare Berechtigung die Administrationsrechte bis auf OU- oder sogar auf Objektebene heruntergebracht werden.

5.3 Vorteile aus betriebswirtschaftlicher Sicht

Für das Unternehmen ergeben sich durch Active Directory mehrere Vorteile:

- **Sicherheit und Steuerung**

  Durch die zahlreichen Sicherheitsoptimierungen (komplexe Passwörter, GPOs, Verschlüsselung, Zertifikate) wurde die Gesamtsicherheit im Unternehmen deutlich erhöht, Sicherheitslöcher geschlossen und firmeninterne Daten besser vor Fremdzugriff geschützt. Die Steuerung der Client-Berechtigungen wird durch AD wesentlich vereinfacht.

- **Effizienz durch globalen Datenzugriff**

  Aus Sicht des Managements war der Zugriff auf Daten von jedem Standort zu jedem Standort eines der Hauptziele der AD Migration. Dieses Ziel wurde weitgehend erreicht und wird vollständig erreicht sein, nach Integration der VPN Standorte in das globale Routing. Durch den vereinfachten Datenaustausch wurde die Effektivität der Kommunikation (z.B. Email) und des Datenaustauschs zwischen den Standorten deutlich gesteigert. Reisende Mitarbeiter können nun problemlos Daten und Mails abrufen.

- **Übersicht der Ressourcen**

  Durch die strukturierte Inventarisierung des Verzeichnisdienstes hat nicht nur die IT-Abteilung, sondern auch die Geschäftsführung jederzeit genauen Überblick über die Verteilung der Ressourcen.

- **Erhöhte Produktivität**

  Die Gesamtproduktivität wurde durch verbesserte Administration, höhere Ausfallsicherheit (z.B. DC Redundanz) und Systemverfügbarkeit, globale Sicherheitsrichtlinien, sowie durch den bereits erwähnten überregionalen Datenzugriff erheblich gesteigert. Es entstehen durch die weitgehend global administrierten Updates für Antivirus und Windows Patches wesentlich weniger Clientausfälle.

- **Audit compliance**

  Als amerikanisches Unternehmen unterliegen alle Standorte (weltweit) dem Sarbanes Oxley Act [34] für US börsennotierte Unternehmen. Dies bedeutet regelmäßige Auditorien im Finanz- und IT-Bereich. Um dem Audit gerecht zu werden müssen umfangreiche Prozess- und Sicherheitskriterien erfüllt werden. Active Directory war ein wesentlicher Beitrag zur Erfüllung dieser Kriterien.

[34] Der „Sarbanes-Oxley Act of 2002“ (auch bekannt als SOX) ist ein nach den selbigen Senatoren benanntes US-Gesetz, das Betrug in amerikanischen Unternehmen vorbeugen und die Aktionäre schützen soll.

6 Grenzen

Trotz der zahlreichen Möglichkeiten werden dem Nutzer von Active Directory Grenzen aufgezeigt. Wir unterscheiden zwischen organisatorischen Grenzen, die meist personell begründet sind, sowie technischen Einschränkungen, die systembedingte Grenzen darstellen. Die organisatorischen Herausforderungen sind vorwiegend in der mangelnden Disziplin oder der fehlenden Qualifikation der Mitarbeiter begründet. Auch Firmenkultur und regionale Mentalität können erheblichen Einfluss auf den Arbeitsstil und somit auf die organisatorischen und strukturellen Probleme haben. Organisatorische Schwächen lassen sich durch Training, Motivation oder durch Prozessvorgaben weitgehend in den Griff bekommen, jedoch sind dazu langfristige und dauerhafte Maßnahmen notwendig. Technische Grenzen sind vom System vorgegeben und nur – wenn überhaupt – durch „Workarounds“ zu kompensieren oder als gegeben hinzunehmen. Beide Bereiche sollen hier anhand der praktischen Erfahrung dieses Projekts beleuchtet werden und sind somit subjektiv.

6.1 Organisatorische Herausforderungen

Grundsätzlich stellt sich in einer komplexen Infrastruktur das Problem der administrativen Disziplin. In einem globalen System mit vielen Administratoren ist es essentiell, dass bestimmte Konventionen und Prozesse eingehalten werden, um eine einheitliche Nutzung und Interpretation der Daten zu gewährleisten. Die Vorarbeit einer Active Directory Einführung muss demnach großen Wert auf Namenskonventionen und Prozessdefinitionen legen. Im globalen Umfeld haben sich vor allem fehlenden Sanktionsmöglichkeiten als Hindernis erwiesen, bestimmte Prozesse und Konventionen zu erzwingen. Da die lokalen IT-Abteilungen disziplinarisch dem lokalen Management unterstellt sind – und nicht der globalen IT Abteilung – gibt es keine direkten Steuerungsmöglichkeiten. Verletzungen der Richtlinien müssen dem lokalen Management deshalb über den CIO gemeldet werden. Dieses Problem wurde im Unternehmen noch nicht dauerhaft gelöst.

- **Lokale Administratoren**

  Ein wesentliches Problem ist die Kontrolle der lokalen IT-Mitarbeiter in den Ländern. Zwar kann deren Befugnis stark eingeschränkt werden, jedoch können durch deren lokale Berechtigungen diverse Prozesse – zumindest für deren Bereich – meist umgangen werden (Globale Prozeduren werden missachtet, Namenskonventionen nicht eingehalten, etc.). Zwar erleichtert AD die Überprüfung dieser Regeln, jedoch ist ein entsprechender Kontroll- und Korrekturmechanismus notwendig.

- **Lokale Organisatorische Einheiten (OUs)**

  Da regionalen Administratoren volle Berechtigung zum Erstellen eigener OUs zugestanden wird, kann hier – insbesondere in Verbindung mit GPOs – entsprechend viel „Unsinn" administriert werden. Ein unerfahrener Administrator kann z.B. lokale GPOs erstellen, die andere Einstellungen ungünstig beeinflussen oder unbrauchbar machen.

- **Namenskonventionen**

  Wenn die globalen Namenskonventionen nicht von allen Administratoren unterstützt und genutzt werden, wird sich auf Dauer keine einheitliche Struktur abbilden lassen. Dies gilt für die Bezeichnungen von OUs genauso wie für die Vergabe von Server- oder Benutzernamen. In der Praxis hat sich gezeigt, dass insbesondere Computer nur schwer zuzuordnen sind, wenn sie den Namenskonventionen nicht entsprechen.

- **Anlegen neuer Objekte**

  Problematisch ist der Umstand, dass Active Directory neue Computer (die der Domäne beitreten) zunächst in der Root OU „Computer" ablegt. Von dort müssen diese manuell in die jeweiligen Länder-OUs verschoben werden. Wird dies vom anlegenden Administrator vergessen, so füllt sich die Root OU und die Computer werden nicht durch die notwendigen GPOs kontrolliert. Es handelt sich im ungünstigsten Falle um „einstellungslose" Computer, denen wichtige Firewall-, DNS- bzw. Securitypatch-Einstellungen fehlen.

6.2 Technische Probleme

Neben den Herausforderungen bei der Migration selbst (siehe 4.4.3), stellten sich im Nachhinein einige generelle Einschränkungen des Systems heraus, auf die hier näher eingegangen werden soll.

- **Simple Sign-On**

  Die Einbindung von anderen Systemen in die Active Directory Authentisierung hat sich als recht aufwändig erwiesen. Für manche Systeme muss erst die globale AD Migration abgeschlossen werden, bevor die Authentisierung über AD erfolgen kann[35]. Erste Versuche, die VPN Einwahl über AD zu authentisieren sind trotz Einbeziehung einer großen externen Beratungsfirma fehlgeschlagen. Zum jetzigen Zeitpunkt (AD-Migration zu 95% abgeschlossen) ist es vermutlich noch zu früh, um eine endgültige Aussage zu treffen. Es ist davon auszugehen, dass die Einbindung der AD für Notes und VPN unter Zuhilfenahme von externer Beratung in naher Zukunft erfolgen wird.

- **DHCP auf Domain Controller**

  Als kleinen Nachteil hat sich erwiesen, den DHCP Service auch auf dem DC zu installieren. Bricht der DC weg, fällt auch der DHCP aus. Während sich User weiterhin über die WAN Strecke an der AD Domäne authentisieren können, erhalten neue Clients keine gültigen IP Adressen[36] (bzw. bestehende Clients keine Erneuerung der IP Lease) und können generell keine Netzwerkverbindung aufbauen. Dadurch wird (indirekt) die Redundanz der Domain Controller eingeschränkt. Bei einer typischen IP-Lease Dauer von etwa 7-8 Tagen sollte dies jedoch nur in wenigen Fällen zu Beeinträchtigungen führen.

[35] Es macht beispielsweise keinen großen Sinn, die AD Useradministration mit Notes zu verbinden, solange noch nicht alle User im AD angelegt wurden.
[36] Das DHCP Protokoll wird standardmäßig nicht über Router und somit auch nicht über WAN-Strecken geroutet (weitergeleitet). Die Clientanfrage nach einer IP-Adresse kann demnach nur im lokalen Subnetz beantwortet werden.

- **Fehlende Redundanz kritischer Betriebsmaster**

  Fällt derjenige Domain Controller aus, der PDC-Emulator oder RID-Betriebsmaster ist, so stellt dies unter Umständen ein kritisches Problem dar. Die Erfahrung hat gezeigt, dass während dieser Zeit das Einrichten neuer Objekte problematisch ist. Bei der Installation von neuen Domain Controllern ohne Verbindung zu oben genannten Betriebsmastern gab es erhebliche Schwierigkeiten, die letztendlich eine komplette Neuinstallation der DCs notwendig machten.

- **Wiederherstellung gelöschter AD Objekte**

  Als nicht zu unterschätzendes Problem hat sich die Wiederherstellung von gelöschten Objekten im Verzeichnis herausgestellt. Eine versehentlich gelöschte OU kann beispielsweise zahlreiche Objekte oder ganze Regionen „arbeitsunfähig" machen. Die Wiederherstellung vom AD Datenbank Backup ist zwar grundsätzlich vorgesehen, hat sich jedoch in der Praxis als sehr komplexes Thema erwiesen, da beim Auftreten von Problemen umfangreiches Know-how der AD Komponenten notwendig ist[37]. Es sei an dieser Stelle explizit empfohlen, sich im Vorfeld mit den Recovery Funktionen vertraut zu machen, um in zeitkritischen Situationen entsprechend routiniert reagieren zu können.

- **Granulierung der Administrationsberechtigungen**

  Zwar lässt sich der Zugriff auf OUs oder einzelne Objekte im Verzeichnis sehr detailliert definieren, jedoch geht dieser Zugriff nicht auf das entsprechende Objekt über. Praktisch bedeutet dies, dass man einem Administrator beispielsweise die volle Berechtigung für eine OU „Server" vergeben kann, er deshalb aber noch keine Administratorrechte an dem entsprechenden Server selbst hat. Er kann also nur Objekte und deren Eigenschaften administrieren – nicht aber das dahinter stehende reale Gerät.

[37] In einem Falle war die gesamte AD-Replikation blockiert, da nach der Datenwiederherstellung der Schlüssel für die Replikationsverbindung ungültig (veraltet) war. Der Schlüssel mußte manuell zurückgesetzt werden, um die Replikation wieder herzustellen.

Eine entsprechende Granulierung kann nur mit der Definition von Domänen-Gruppen erfolgen, die dann jedem Objekt „von Hand“ oder über GPOs zugeordnet werden müssen. Ein ausreichend granulares Administrationskonzept ist demnach entsprechend aufwändig

- **Replikationsmodell**

  Obwohl unter AD die Replikation der Verzeichnisdaten auch ohne weitere Konfiguration funktioniert, ergeben sich bei komplexen Netzwerken unter Umständen Replikationsprobleme. Beim Erstellen von Verbindungsobjekten (Inter-Site Transports) wird der Kostenfaktor standardmäßig immer auf 100 gesetzt. Wird an den Voreinstellungen nichts verändert, so ist keine Bevorzugung bestimmter Verbindungen definiert (siehe dazu auch 1.5.2). In einer globalen Infrastruktur entsteht dadurch sehr schnell ein unüberschaubares Replikationsschema, das unkontrollierten Datenverkehr oder auch starke Replikationsverzögerungen durch unnötige (zusätzliche) oder ungünstige Hops mit sich bringt[38].

- **Fehlendes Konzept für Event Logging**

  In der Praxis hat sich das Konzept des lokalen Windows Event Logging als problematisch erwiesen, wenn es darum geht, Vorgänge im AD zu rekonstruieren. Da Objektänderungen im AD (theoretisch) von jedem DC ausgeführt werden können, ist die Nachverfolgung der Änderungen umso schwieriger, je mehr DCs im Netzwerk vorhanden sind. Man kann Vorgänge nur dann eindeutig lokalisieren, wenn man auf jedem DC in die Event Logs schaut. Zudem muss das Logging auf jedem Domain Controller individuell aktiviert bzw. auf die jeweiligen Bedürfnisse angepasst werden. Microsoft bietet für dieses Problem keine integrierte Lösung an. Man ist deshalb auf Zusatzlösungen[39] oder Lösungen von Drittanbietern[40] angewiesen.

[38] In einem Falle stellte sich heraus, dass zwischen zwei Standorten bis zu 4 Hops bestanden und die Replikation dadurch fast einen ganzen Tag benötigte.
[39] Microsoft bietet den MOM (Microsoft Operation Manager) an.
[40] Beispielsweise netiQ Security Manager oder RippleTech LogCaster.

7 Schlussbetrachtung

Active Directory stellt sich nach der Implementierung nicht als „das“ perfekte Network Operating System dar, wie man es aufgrund der Features und der Vielzahl der Verbesserungen gegenüber NT vielleicht erwarten würde. Doch es enthält zahlreichen Optimierungen, die es positiv von NT und anderen Netzwerk Betriebssystemen abhebt. Und obwohl sich nach der AD Implementierung zahlreiche Unzulänglichkeiten herausgestellt haben, hat die Migration die meisten Erwartungen erfüllt. – Wenn auch zunächst erst einige Erfahrungen gemacht und zahlreiche Probleme aus dem Weg geräumt werden mussten. – Die vielen Vorteile der AD überwiegen eindeutig die wenigen Nachteile und für die meisten Unzulänglichkeiten oder aufgetretenen Probleme hat man akzeptable Workarounds gefunden.

Es hat sich gezeigt, dass erhebliches Know-how der AD-Komponenten notwendig ist, um eine komplexe Netzwerklandschaft reibungslos betreiben zu können und bei scheinbar nicht nachvollziehbaren Problemen die Ursache und somit eine entsprechende Lösung zu finden. Die Einbeziehung eines kompetenten, erfahrenen Beratungsunternehmens in den gesamten Migrationsprozess scheint nach den gemachten Erfahrungen als unumgänglich.

Langfristig zahlt sich der enorme Planungs- und Migrationsaufwand einer Active Directory Implementierung aus. Die Administration, Kontrolle und Sicherheit im Netzwerk wird drastisch erhöht. Dies führt zu weniger Ausfallzeiten und zu mehr Produktivität im gesamten Unternehmen. Die Möglichkeit der globalen Administration von zentraler Stelle erlaubt es, flexibel auf Umwelteinflüsse zu reagieren und die Kontinuität der Geschäftsprozesse zu gewährleisten. Somit ist Active Directory auch aus betriebswirtschaftlicher Sicht[41] absolut empfehlenswert.

[41] Vgl. dazu 5.3, Vorteile aus betriebswirtschaftlicher Sicht

Literaturverzeichnis

Allen, R., Lowe-Norris, A., Active Directory, Köln, 2004

Boykin, B., Tulisalo, T., IBM, Redbooks Paper. Active Directory Synchronization with Lotus ADSync, 2005

Golem, IDC: Windows und Linux legen im Server-Bereich zu, 18.06.2004, http://www.golem.de/0406/31837.html (abgerufen 17.11.2005)

Internet Engineering Task Force (IETF), RFC 2253 von 1997, http://rfc.net/rfc2253.html (abgerufen 15.11.2005)

Knecht-Thurmann, S., Active Directory, München, 2004

Michela, F., Palme, M., Active Directory, Unterschleißheim, 2000

Microsoft Corporation, Microsoft Windows 2000 Active Directory planen und einführen, Unterschleißheim, 2000

Microsoft Developer Network (MSDN), Extensible Storage Engine, 2005, http://msdn.microsoft.com/library/default.asp, Win32 and COM Development, Data Access and Storage, Extensible Storage Engine (abgerufen 24.10.2005)

Microsoft TechNet, What Is the Data Store?, 2003, http://technet2.microsoft.com/WindowsServer/en/Library/ff822bf5-9fd6-43b8-962d-666baaeb713a1033.mspx (abgerufen 24.10.2005)

Microsoft TechNet, How the Data Store Works, 2003, http://technet2.microsoft.com/WindowsServer/en/Library/54094485-71f6-4be8-8ebf-faa45bc5db4c1033.mspx (abgerufen 24.10.2005)

Spealman, J., Hudson, K., Craft, M., Microsoft Windows Server 2003 Active Directory-Infrastruktur, Unterschleißheim, 2003

Webhosting.info, IDC Expects Return to Growth in the U.S. Server Market, (14.09.2003), http://news.webhosting.info/t-121/ (abgerufen 17.11.2005)

Wikipedia, Microsoft Jet Engine, 2005, http://wikipedia.de
Artikel: „Microsoft Jet Engine“, (abgerufen 24.10.2005)

Eidesstattliche Erklärung

Hiermit versichere ich, dass die vorliegende Arbeit von mir selbständig und ohne unerlaubte Hilfe angefertigt worden ist, insbesondere, dass ich alle Stellen, die wörtlich oder annähernd aus Veröffentlichungen übernommen sind, durch Zitate als solche kenntlich gemacht habe.

Eindorf*, den 15.12.2005

Stefan Schmidt